目 录

1 AAA

1.1 AAA简介

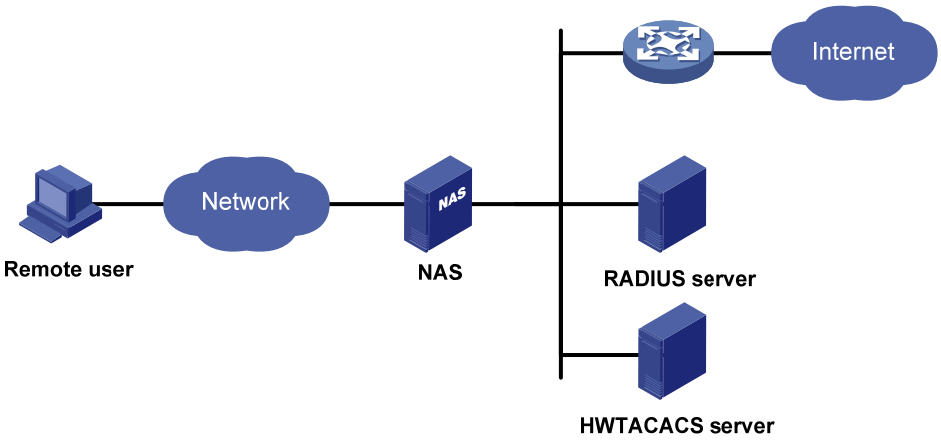
1.1.1 概述

AAA（Authentication、Authorization、Accounting，认证、授权、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。

- 认证：确认访问网络的远程用户的身份，判断访问者是否为合法的网络用户。
- 授权：对不同用户赋予不同的权限，限制用户可以使用的服务。例如，管理员授权办公用户才能对服务器中的文件进行访问和打印操作，而其它临时访客不具备此权限。
- 计费：记录用户使用网络服务过程中的所有操作，包括使用的服务类型、起始时间、数据流量等，用于收集和记录用户对网络资源的使用情况，并可以实现针对时间、流量的计费需求，也对网络起到监视作用。

AAA采用客户端/服务器结构，客户端运行于NAS（Network Access Server，网络接入服务器）上，负责验证用户身份与管理用户接入，服务器上则集中管理用户信息。AAA的基本组网结构如 图 1-1。

图1-1 AAA 基本组网结构示意图



当用户想要通过 NAS 获得访问其它网络的权利或取得某些网络资源的权利时，首先需要通过 AAA 认证，而 NAS 就起到了验证用户的作用。NAS 负责把用户的认证、授权、计费信息透传给服务器。服务器根据自身的配置对用户的身份进行判断并返回相应的认证、授权、计费结果。NAS 根据服务器返回的结果，决定是否允许用户访问外部网络、获取网络资源。

AAA 可以通过多种协议来实现，这些协议规定了 NAS 与服务器之间如何传递用户信息。目前设备支持 RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）协议、HWTACACS（HW Terminal Access Controller Access Control System，HW 终端访问控制器控制系统协议）协议和 LDAP（Lightweight Directory Access Protocol，轻量级目录访问协议）协议，在实际应用中，最常使用 RADIUS 协议。

图 1-1 的AAA基本组网结构中有两台服务器，用户可以根据实际组网需求来决定认证、授权、计费功能分别由使用哪种协议类型的服务器来承担。例如，可以选择HWTACACS服务器实现认证和授权，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。例如，公司仅仅想让员工在访问某些特定资源时进行身份认证，那么网络管理员只要配置认证服务器就可以了。但是若希望对员工使用网络的情况进行记录，那么还需要配置计费服务器。

目前，设备支持动态口令认证机制。

1.1.2 RADIUS协议简介

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/服务器结构的信息交互协议，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。RADIUS 协议合并了认证和授权的过程，它定义了 RADIUS 的报文格式及其消息传输机制，并规定使用 UDP 作为封装 RADIUS 报文的传输层协议，UDP 端口 1812、1813 分别作为认证/授权、计费端口。

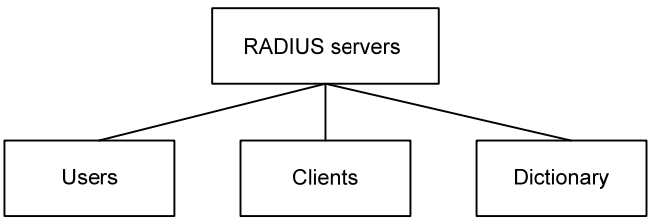
RADIUS 最初仅是针对拨号用户的 AAA 协议，后来随着用户接入方式的多样化发展，RADIUS 也适应多种用户接入方式，如以太网接入、ADSL 接入。它通过认证授权来提供接入服务，通过计费来收集、记录用户对网络资源的使用。

1. 客户端/服务器模式

- 客户端：RADIUS 客户端一般位于 NAS 上，可以遍布整个网络，负责将用户信息传输到指定的 RADIUS 服务器，然后根据服务器返回的信息进行相应处理（如接受/拒绝用户接入）。
- 服务器：RADIUS 服务器一般运行在中心计算机或工作站上，维护用户的身份信息和与其相关的网络服务信息，负责接收 NAS 发送的认证、授权、计费请求并进行相应的处理，然后给 NAS 返回处理结果（如接受/拒绝认证请求）。另外，RADIUS 服务器还可以作为一个代理，以 RADIUS 客户端的身份与其它的 RADIUS 认证服务器进行通信，负责转发 RADIUS 认证和计费报文。

RADIUS服务器通常要维护三个数据库，如 图 1-2 所示：

图1-2 RADIUS 服务器的组成



- “Users”：用于存储用户信息（如用户名、口令以及使用的协议、IP 地址等配置信息）。
- “Clients”：用于存储 RADIUS 客户端的信息（如 NAS 的共享密钥、IP 地址等）。
- “Dictionary”：用于存储 RADIUS 协议中的属性和属性值含义的信息。

2. 安全的消息交互机制

RADIUS 客户端和 RADIUS 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的。共享密钥是一个带外传输的客户端和服务器都知道的字符串，不需要单独进行网络传输。RADIUS 报文中有

一个 16 字节的验证字字段，它包含了对整个报文的数字签名数据，该签名数据是在共享密钥的参与下利用 MD5 算法计算出的。收到 RADIUS 报文的一方要验证该签名的正确性，如果报文的签名不正确，则丢弃它。通过这种机制，保证了 RADIUS 客户端和 RADIUS 服务器之间信息交互的安全性。另外，为防止用户密码在不安全的网络上传递时被窃取，在 RADIUS 报文传输过程中还利用共享密钥对用户密码进行了加密。

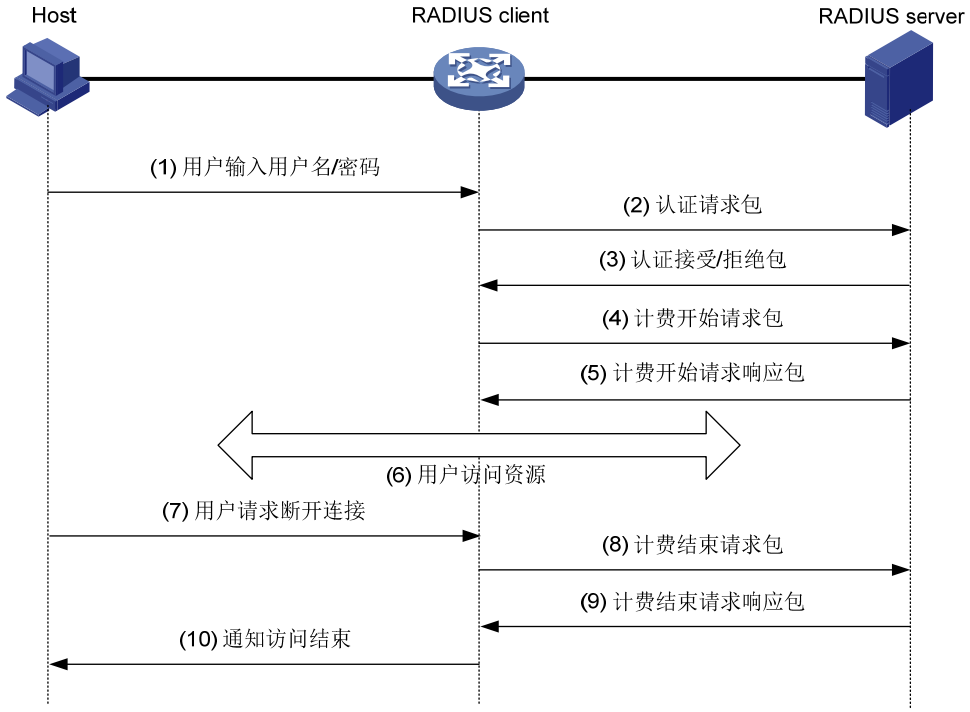
3. 用户认证机制

RADIUS 服务器支持多种方法来认证用户，例如 PAP（Password Authentication Protocol，密码认证协议）、CHAP（Challenge Handshake Authentication Protocol，质询握手认证协议）以及 EAP（Extensible Authentication Protocol，可扩展认证协议）。

4. RADIUS的基本消息交互流程

用户、RADIUS客户端和RADIUS服务器之间的交互流程如 图 1-3 所示。

图1-3 RADIUS 的基本消息交互流程



消息交互流程如下：

(1) 用户发起连接请求，向 RADIUS 客户端发送用户名和密码。

(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），其中的密码在共享密钥的参与下利用 MD5 算法进行加密处理。

(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）；如果认证失败，则返回认证拒绝包（Access-Reject）。由于 RADIUS 协议合并了认证和授权的过程，因此认证接受包中也包含了用户的授权信息。

(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 RADIUS 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。

(8) RADIUS 客户端向 RADIUS 服务器发送计费停止请求包（Accounting-Request）。

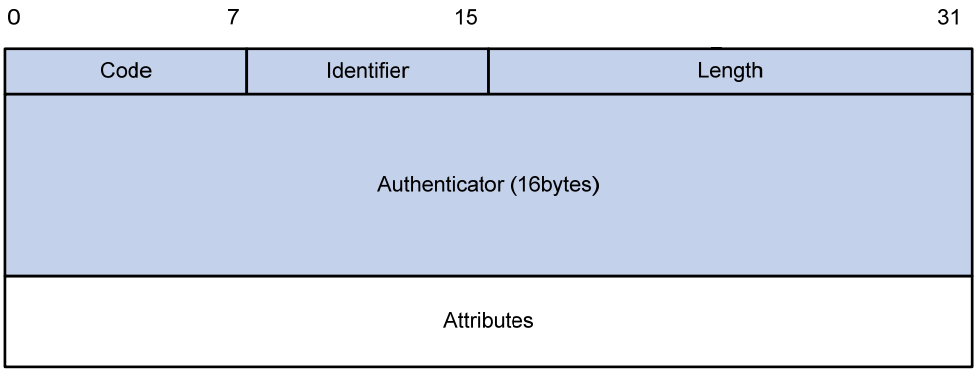
(9) RADIUS 服务器返回计费结束响应包（Accounting-Response），并停止计费。

(10) 通知用户结束访问网络资源。

5. RADIUS报文结构

RADIUS采用UDP报文来传输消息，通过定时器机制、重传机制、备用服务器机制，确保RADIUS服务器和客户端之间交互消息的正确收发。RADIUS报文结构如 图 1-4 所示。

图1-4 RADIUS 报文结构



各字段的解释如下：

(1) Code 域

长度为 1 个字节，用于说明RADIUS报文的类型，如 表 1-1 所示。

表1-1 Code 域的主要取值说明

Code	报文类型	报文说明
1	Access-Request认证请求包	方向Client->Server，Client将用户信息传输到Server，请求Server对用户身份进行验证。该报文中必须包含User-Name属性，可选包含NAS-IP-Address、User-Password、NAS-Port等属性
2	Access-Accept认证接受包	方向Server->Client，如果Access-Request报文中的所有Attribute值都可以接受（即认证通过），则传输该类型报文
3	Access-Reject认证拒绝包	方向Server->Client，如果Access-Request报文中存在任何无法被接受的Attribute值（即认证失败），则传输该类型报文
4	Accounting-Request计费请求包	方向Client->Server，Client将用户信息传输到Server，请求Server开始/停止计费。该报文中的Acct-Status-Type属性用于区分计费开始请求和计费结束请求
5	Accounting-Response计费响应包	方向Server->Client，Server通知Client已经收到Accounting-Request报文，并且已经正确记录计费信息

(2) Identifier 域

长度为 1 个字节，用于匹配请求包和响应包，以及检测在一段时间内重发的请求包。对于类型一致且属于同一个交互过程的请求包和响应包，该 Identifier 值相同。

(3) Length 域

长度为 2 个字节，表示 RADIUS 数据包（包括 Code、Identifier、Length、Authenticator 和 Attribute）的长度，单位为字节。超过 Length 域的字节将作为填充字符被忽略。如果接收到的包的实际长度小于 Length 域的值时，则包会被丢弃。

(4) Authenticator 域

长度为 16 个字节，用于验证 RADIUS 服务器的应答报文，另外还用于用户密码的加密。Authenticator 包括两种类型：Request Authenticator 和 Response Authenticator。

(5) Attribute 域

不定长度，用于携带专门的认证、授权和计费信息。Attribute 域可包括多个属性，每一个属性都采用（Type、Length、Value）三元组的结构来表示。

- 类型（Type）：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决定。

表 1-2 列出了RADIUS认证、授权、计费常用的属性，这些属性由RFC 2865、RFC 2866、RFC 2867和RFC 2868 所定义。常用RADIUS标准属性的介绍请参见“1.1.7 1. 常用RADIUS标准属性”。

表1-2 RADIUS 属性

属性编号	属性名称	属性编号	属性名称
1	User-Name	45	Acct-Authentic
2	User-Password	46	Acct-Session-Time
3	CHAP-Password	47	Acct-Input-Packets
4	NAS-IP-Address	48	Acct-Output-Packets
5	NAS-Port	49	Acct-Terminate-Cause
6	Service-Type	50	Acct-Multi-Session-Id
7	Framed-Protocol	51	Acct-Link-Count
8	Framed-IP-Address	52	Acct-Input-Gigawords
9	Framed-IP-Netmask	53	Acct-Output-Gigawords
10	Framed-Routing	54	(unassigned)
11	Filter-ID	55	Event-Timestamp
12	Framed-MTU	56-59	(unassigned)
13	Framed-Compression	60	CHAP-Challenge
14	Login-IP-Host	61	NAS-Port-Type
15	Login-Service	62	Port-Limit
16	Login-TCP-Port	63	Login-LAT-Port
17	(unassigned)	64	Tunnel-Type
18	Reply-Message	65	Tunnel-Medium-Type
19	Callback-Number	66	Tunnel-Client-Endpoint
20	Callback-ID	67	Tunnel-Server-Endpoint

属性编号	属性名称	属性编号	属性名称
21	(unassigned)	68	Acct-Tunnel-Connection
22	Framed-Route	69	Tunnel-Password
23	Framed-IPX-Network	70	ARAP-Password
24	State	71	ARAP-Features
25	Class	72	ARAP-Zone-Access
26	Vendor-Specific	73	ARAP-Security
27	Session-Timeout	74	ARAP-Security-Data
28	Idle-Timeout	75	Password-Retry
29	Termination-Action	76	Prompt
30	Called-Station-Id	77	Connect-Info
31	Calling-Station-Id	78	Configuration-Token
32	NAS-Identifier	79	EAP-Message
33	Proxy-State	80	Message-Authenticator
34	Login-LAT-Service	81	Tunnel-Private-Group-id
35	Login-LAT-Node	82	Tunnel-Assignment-id
36	Login-LAT-Group	83	Tunnel-Preference
37	Framed-AppleTalk-Link	84	ARAP-Challenge-Response
38	Framed-AppleTalk-Network	85	Acct-Interim-Interval
39	Framed-AppleTalk-Zone	86	Acct-Tunnel-Packets-Lost
40	Acct-Status-Type	87	NAS-Port-Id
41	Acct-Delay-Time	88	Framed-Pool
42	Acct-Input-Octets	89	(unassigned)
43	Acct-Output-Octets	90	Tunnel-Client-Auth-id
44	Acct-Session-Id	91	Tunnel-Server-Auth-id

6. RADIUS扩展属性

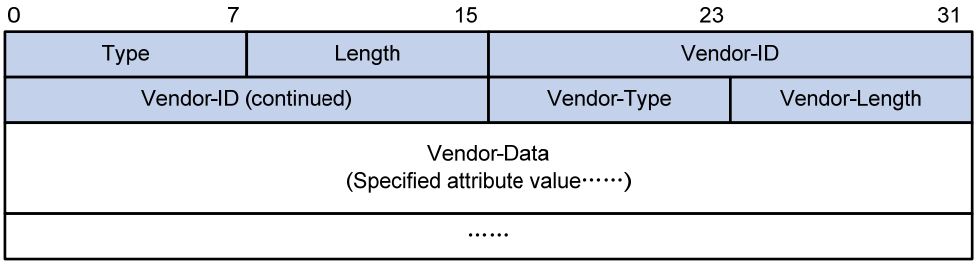
RADIUS 协议具有良好的可扩展性，RFC 2865 中定义的 26 号属性（Vendor-Specific）用于设备厂商对 RADIUS 进行扩展，以实现标准 RADIUS 没有定义的功能。

设备厂商可以在 26 号属性中封装多个自定义的（Type、Length、Value）子属性，以提供更多的扩展功能。26 号属性的格式如 图 1-5 所示：

- Vendor-ID，表示厂商代号，最高字节为 0，其余 3 字节的编码见 RFC 1700。H3C 公司的 Vendor-ID 是 25506。
- Vendor-Type，表示子属性类型。
- Vendor-Length，表示子属性长度。
- Vendor-Data，表示子属性的内容。

关于H3C RADIUS扩展属性的介绍请参见“1.1.7 2. H3C RADIUS扩展属性”。

图1-5 26 号属性的格式



1.1.3 HWTACACS协议简介

HWTACACS（HW Terminal Access Controller Access Control System，HW 终端访问控制器控制系统协议）是在 TACACS（RFC 1492）基础上进行了功能增强的安全协议。该协议与 RADIUS 协议类似，采用客户端/服务器模式实现 NAS 与 HWTACACS 服务器之间的通信。

HWTACACS 协议主要用于 PPP（Point-to-Point Protocol，点对点协议）和 VPDN（Virtual Private Dial-up Network，虚拟专用拨号网络）接入用户及终端用户的认证、授权和计费。其典型应用是对需要登录到 NAS 设备上进行操作的终端用户进行认证、授权以及对终端用户执行的操作进行记录。设备作为 HWTACACS 的客户端，将用户名和密码发给 HWTACACS 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，HWTACACS 服务器上会记录用户对设备执行过的命令。

1. HWTACACS协议与RADIUS协议的区别

HWTACACS协议与RADIUS协议都实现了认证、授权和计费功能，它们有很多相似点：结构上都采用客户端/服务器模式；都使用共享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。两者之间存在的主要区别如 表 1-3 所示。

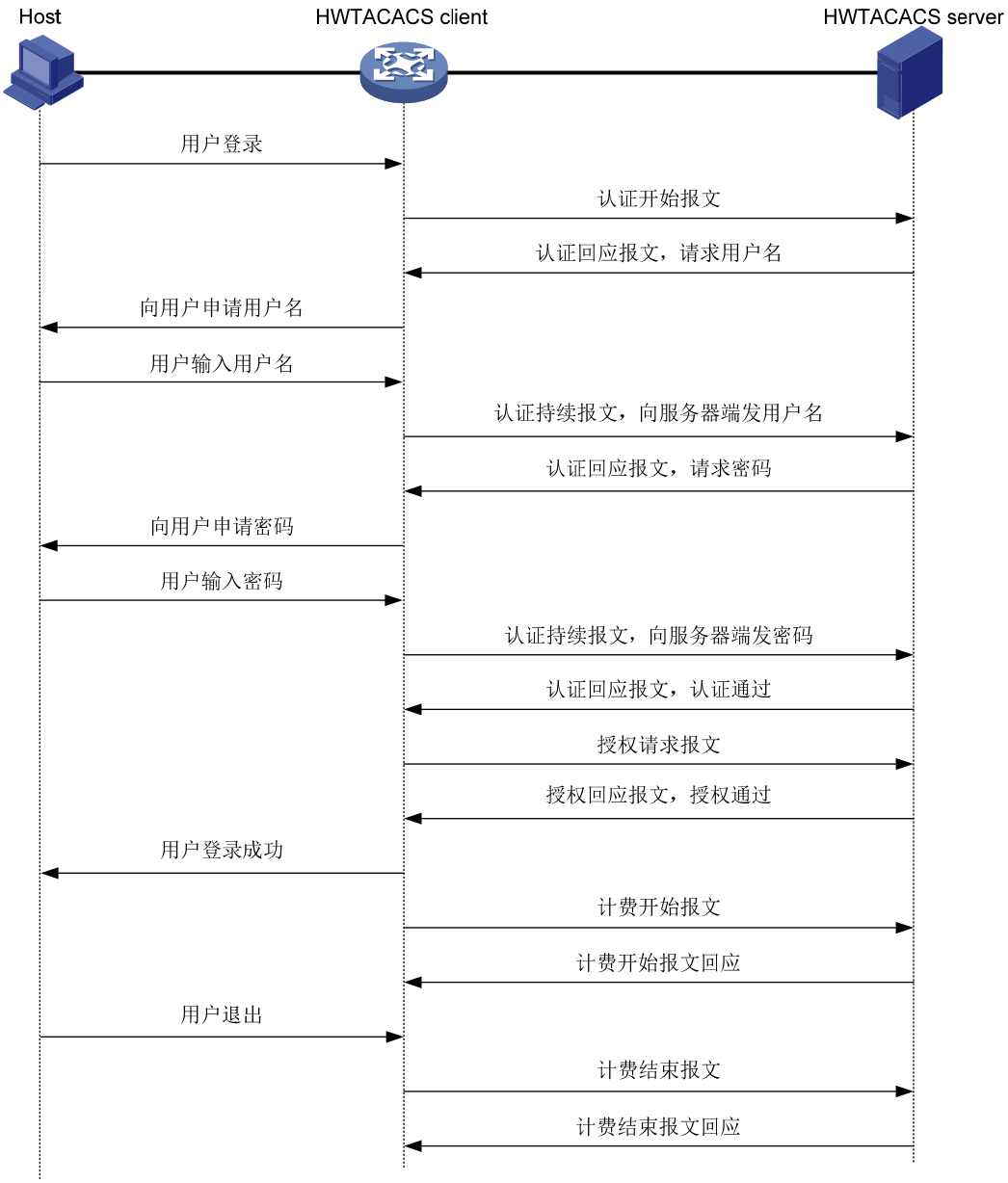
表1-3 HWTACACS 协议和 RADIUS 协议区别

HWTACACS 协议	RADIUS 协议
使用TCP，网络传输更可靠	使用UDP，网络传输效率更高
除了HWTACACS报文头，对报文主体全部进行加密	只对认证报文中的密码字段进行加密
协议报文较为复杂，认证和授权分离，使得认证、授权服务可以分离在不同的服务器上实现。例如，可以用一个HWTACACS服务器进行认证，另外一个HWTACACS服务器进行授权	协议报文比较简单，认证和授权结合，难以分离
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角色和AAA授权的双重限制，某角色的用户输入的每一条命令都需要通过HWTACACS服务器授权，如果授权通过，命令就可以被执行	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所具有的角色决定，关于用户角色的相关介绍请参见“基础配置指导”中的“RBAC”

2. HWTACACS的基本消息交互流程

下面以Telnet用户为例，说明使用HWTACACS对用户进行认证、授权和计费的过程。基本消息交互流程图如 图 1-6 所示。

图1-6 Telnet 用户认证、授权和计费流程图



基本消息交互流程如下：

(1) Telnet 用户请求登录设备。

(2) HWTACACS 客户端收到请求之后，向 HWTACACS 服务器发送认证开始报文。

(3) HWTACACS 服务器发送认证回应报文，请求用户名。

(4) HWTACACS 客户端收到回应报文后，向用户询问用户名。

(5) 用户输入用户名。

(6) HWTACACS 客户端收到用户名后，向 HWTACACS 服务器发送认证持续报文，其中包括了用户名。

(7) HWTACACS 服务器发送认证回应报文，请求登录密码。

(8) HWTACACS 客户端收到回应报文，向用户询问登录密码。

(9) 用户输入密码。

(10) HWTACACS 客户端收到登录密码后，向 HWTACACS 服务器发送认证持续报文，其中包括了登录密码。

(11) 如果认证成功，HWTACACS 服务器发送认证回应报文，指示用户通过认证。

(12) HWTACACS 客户端向 HWTACACS 服务器发送授权请求报文。

(13) 如果授权成功，HWTACACS 服务器发送授权回应报文，指示用户通过授权。

(14) HWTACACS 客户端收到授权成功报文，向用户输出设备的配置界面，允许用户登录。

(15) HWTACACS 客户端向 HWTACACS 服务器发送计费开始报文。

(16) HWTACACS 服务器发送计费回应报文，指示计费开始报文已经收到。

(17) 用户请求断开连接。

(18) HWTACACS 客户端向 HWTACACS 服务器发送计费结束报文。

(19) HWTACACS 服务器发送计费结束报文，指示计费结束报文已经收到。

1.1.4 LDAP协议简介

LDAP（Lightweight Directory Access Protocol，轻量级目录访问协议）是一种目录访问协议，用于提供跨平台的、基于标准的目录服务。它是在 X.500 协议的基础上发展起来的，继承了 X.500 的优点，并对 X.500 在读取、浏览和查询操作方面进行了改进，适合于存储那些不经常改变的数据。

LDAP 协议的典型应用是用来保存系统中的用户信息，如 Microsoft 的 Windows 操作系统就使用了 Active Directory Server（一种 LDAP 服务器软件）来保存操作系统的用户、用户组等信息，用于用户登录 Windows 时的认证和授权。

1. LDAP目录服务

LDAP 中使用目录记录并管理系统中的组织信息、人员信息以及资源信息。目录按照树型结构组织，由多个条目（Entry）组成的。条目是具有 DN（Distinguished Name，识别名）的属性（Attribute）集合。属性用来承载各种类型的数据信息，例如用户名、密码、邮件、计算机名、联系电话等。

LDAP 协议基于 Client/Server 结构提供目录服务功能，所有的目录信息数据存储在 LDAP 服务器上。目前，Microsoft 的 Active Directory Server、IBM 的 Tivoli Directory Server 和 Sun 的 Sun ONE Directory Server 都是常用的 LDAP 服务器软件。

2. 使用LDAP协议进行认证和授权

AAA 可以使用 LDAP 协议对用户提供认证和授权服务。LDAP 协议中定义了多种操作来实现 LDAP 的各种功能，用于认证和授权的操作主要为绑定和查询。

- 绑定操作的作用有两个：一是与 LDAP 服务器建立连接并获取 LDAP 服务器的访问权限。二是用于检查用户信息的合法性。
- 查询操作就是构造查询条件，并获取 LDAP 服务器的目录资源信息的过程。

使用 LDAP 协议进行认证时，其基本的工作流程如下：

(1) LDAP 客户端使用 LDAP 服务器管理员 DN 与 LDAP 服务器进行绑定，与 LDAP 服务器建立连接并获得查询权限。

(2) LDAP 客户端使用认证信息中的用户名构造查询条件，在 LDAP 服务器指定根目录下查询此用户，得到用户的 DN。

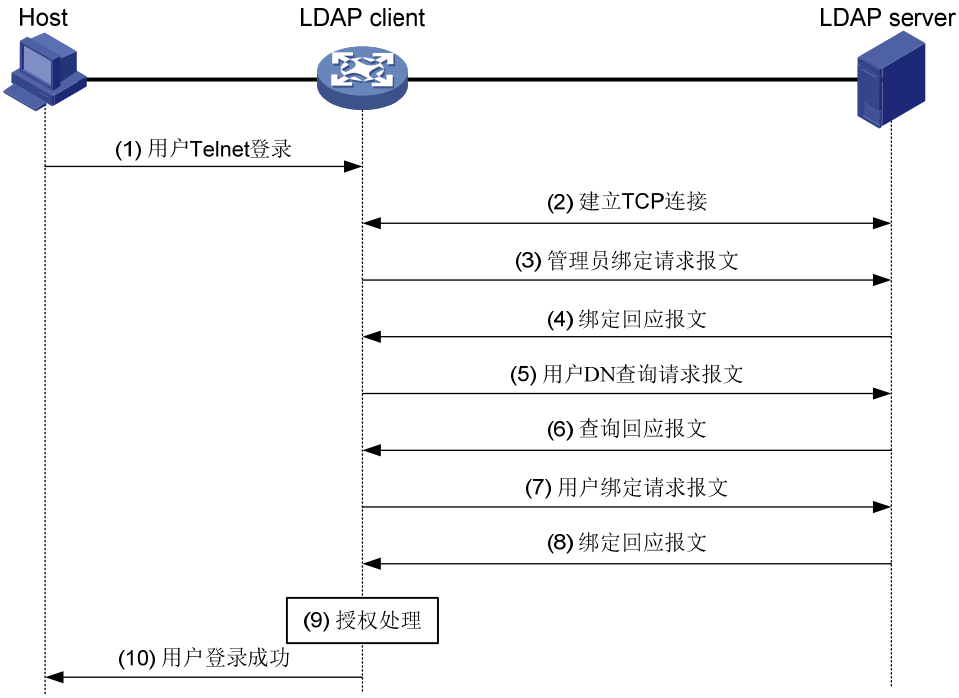
(3) LDAP 客户端使用用户 DN 和用户密码与 LDAP 服务器进行绑定，检查用户密码是否正确。

使用 LDAP 协议进行授权的过程与认证过程相似，首先必须通过与 LDAP 服务器进行绑定，建立与服务器的连接，然后在此连接的基础上通过查询操作得到用户的授权信息。与认证过程稍有不同的是，授权过程不仅仅会查询用户 DN，还会同时查询相应的 LDAP 授权信息。

3. LDAP认证的基本消息交互流程

下面以Telnet用户登录设备为例，说明如何使用LDAP认证服务器来对用户进行认证。用户的LDAP认证基本消息交互流程如 图 1-7 所示。

图1-7 LDAP 认证的基本消息交互流程



基本消息交互流程如下：

(1) 用户发起连接请求，向 LDAP 客户端发送用户名和密码。

(2) LDAP 客户端收到请求之后，与 LDAP 服务器建立 TCP 连接。

(3) LDAP 客户端以管理员 DN 和管理员 DN 密码为参数向 LDAP 服务器发送管理员绑定请求报文（Administrator Bind Request）获得查询权限。

(4) LDAP 服务器进行绑定请求报文的处理。如果绑定成功，则向 LDAP 客户端发送绑定成功的回应报文。

(5) LDAP 客户端以输入的用户名为参数，向 LDAP 服务器发送用户 DN 查询请求报文（User DN Search Request）。

(6) LDAP 服务器收到查询请求报文后，根据报文中的查询起始地址、查询范围、以及过滤条件，对用户 DN 进行查找。如果查询成功，则向 LDAP 客户端发送查询成功的回应报文。查询得到的用户 DN 可以是一或多个。

(7) LDAP 客户端以查询得到的用户 DN 和用户输入的密码为参数，向 LDAP 服务器发送用户 DN 绑定请求报文（User DN Bind Request），检查用户密码是否正确。

(8) LDAP 服务器进行绑定请求报文的处理。

- 如果绑定成功，则向 LDAP 客户端发送绑定成功的回应报文。
- 如果绑定失败，则向 LDAP 客户端发送绑定失败的回应报文。LDAP 客户端以下一个查询到的用户 DN（如果存在的话）为参数，继续向服务器发送绑定请求，直至有一个 DN 绑定成功，或者所有 DN 均绑定失败。如果所有用户 DN 都绑定失败，则 LDAP 客户端通知用户登录失败并拒绝用户接入。

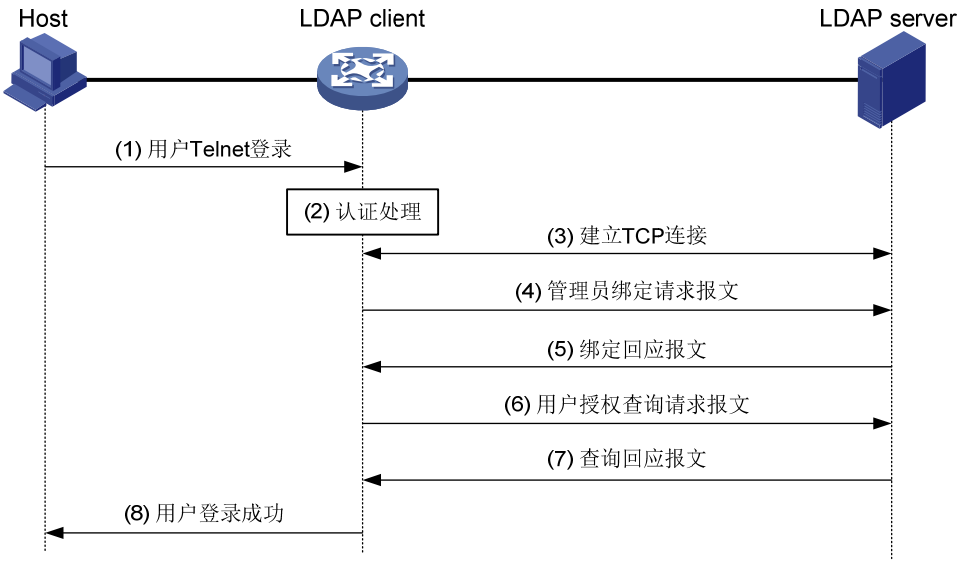
(9) LDAP客户端保存绑定成功的用户DN，并进行授权处理。如果设备采用LDAP授权方案，则进行 图 1-8 所示的用户授权交互流程；如果设备采用非LDAP的授权方案，则执行其它协议的授权处理流程，此处略。

(10) 授权成功之后，LDAP 客户端通知用户登录成功。

4. LDAP授权的基本消息交互流程

下面以Telnet用户登录设备为例，说明如何使用LDAP服务器来对用户进行授权。用户的LDAP授权基本消息交互流程如 图 1-8 所示。

图1-8 LDAP 授权的基本消息交互流程



(1) 用户发起连接请求，向 LDAP 客户端发送用户名和密码。

(2) LDAP客户端收到请求之后，进行认证处理。如果设备采用LDAP认证方案，则按照 图 1-7 所示进行LDAP认证。LDAP认证流程完成之后，如果已经和该LDAP授权服务器建立了绑定关系，则直接转到步骤（6），否则转到步骤（4）；如果设备采用非LDAP认证方案，则执行其它协议的认证处理流程，之后转到步骤（3）。

(3) LDAP 客户端与 LDAP 服务器建立 TCP 连接。

(4) LDAP 客户端以管理员 DN 和管理员 DN 密码为参数向 LDAP 服务器发送管理员绑定请求报文（Administrator Bind Request）获得查询权限。

(5) LDAP 服务器进行绑定请求报文的处理。如果绑定成功，则向 LDAP 客户端发送绑定成功的回应报文。

(6) LDAP 客户端以输入的用户名为参数（如果用户认证使用的是相同 LDAP 服务器，则以保存的绑定成功的用户 DN 为参数），向 LDAP 服务器发送授权查询请求报文。

(7) LDAP 服务器收到查询请求报文后，根据报文中的查询起始地址、查询范围、过滤条件以及 LDAP 客户端关心的 LDAP 属性，对用户信息进行查找。如果查询成功，则向 LDAP 客户端发送查询成功的回应报文。

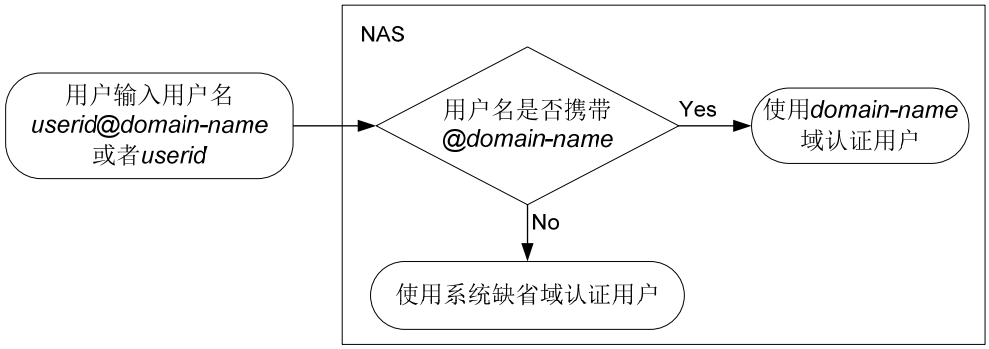
(8) 授权成功后，LDAP 客户端通知用户登录成功。

1.1.5 设备的AAA实现

1. 基于域的用户管理

NAS对用户的管理是基于ISP（Internet Service Provider，互联网服务提供商）域的，每个用户都属于一个ISP域。一般情况下，用户所属的ISP域是由用户登录时提供的用户名决定的，如 图 1-9 所示。

图1-9 用户名决定域名



为便于对不同接入方式的用户进行区分管理，提供更为精细且有差异化的认证、授权、计费服务，AAA 将用户划分为以下几个类型：

- lan-access 用户：LAN 接入用户，如 802.1X 认证、MAC 地址认证用户。
- login 用户：登录设备用户，如 SSH、Telnet、FTP、终端接入用户（即从 Console 口登录的用户）。
- Portal 接入用户。
- PPP 接入用户。
- IKE 用户：使用 IKE 扩展认证的用户。
- Web 用户：使用 HTTP 或 HTTPS 服务登录设备 Web 界面的用户。

对于某些接入方式，用户最终所属的 ISP 域可由该相应的认证模块（例如 802.1X）提供命令行来指定，用于满足一定的用户认证管理策略。

2. 实现AAA的方法

在具体实现中，一个 ISP 域对应着设备上一套实现 AAA 的配置策略，它们是管理员针对该域用户制定的一套认证、授权、计费方法，可根据用户的接入特征以及不同的安全需求组合使用。

AAA 支持以下认证方法：

- 不认证：对用户非常信任，不对其进行合法性检查，一般情况下不采用这种方法。
- 本地认证：认证过程在接入设备上完成，用户信息（包括用户名、密码和各种属性）配置在接入设备上。优点是速度快，可以降低运营成本；缺点是存储信息量受设备硬件条件限制。
- 远端认证：认证过程在接入设备和远端的服务器之间完成，接入设备和远端服务器之间通过 RADIUS、HWTACACS 或 LDAP 协议通信。优点是用户信息集中在服务器上统一管理，可实现大容量、高可靠性、支持多设备的集中式统一认证。当远端服务器无效时，可配置备选认证方式完成认证。

AAA 支持以下授权方法：

- 不授权：接入设备不请求授权信息，不对用户可以使用的操作以及用户允许使用的网络服务进行授权。此时，认证通过的 login 用户只有系统给予的缺省用户角色 level-0，其中 FTP/SFTP/SCP 用户的工作目录是设备的根目录，但并无访问权限；认证通过的非 login 用户，可直接访问网络。关于用户角色 level-0 的详细介绍请参见“基础配置指导”中的“RBAC”。
- 本地授权：授权过程在接入设备上进行，根据接入设备上为本地用户配置的相关属性进行授权。
- 远端授权：授权过程在接入设备和远端服务器之间完成。RADIUS 协议的认证和授权是绑定在一起的，不能单独使用 RADIUS 进行授权。RADIUS 认证成功后，才能进行授权，RADIUS 授权信息携带在认证回应报文中下发给用户。HWTACACS 协议的授权与认证相分离，在认证成功后，HWTACACS 授权信息通过授权报文进行交互。当远端服务器无效时，可配置备选授权方式完成授权。

AAA 支持以下计费方法：

- 不计费：不对用户计费。
- 本地计费：计费过程在接入设备上完成，实现了本地用户连接数的统计和限制，并没有实际的费用统计功能。
- 远端计费：计费过程在接入设备和远端的服务器之间完成。当远端服务器无效时，可配置备选计费方式完成计费。

除此之外，对于 login 用户，AAA 还可以对其提供以下服务，用于提高对设备操作的安全性：

- 命令行授权：用户执行的每一条命令都需要接受授权服务器的检查，只有授权成功的命令才被允许执行。关于命令行授权的详细介绍请参考“基础配置指导”中的“配置用户通过 CLI 登录设备”。
- 命令行计费：若未开启命令行授权功能，则计费服务器对用户执行过的所有有效命令进行记录；若开启了命令行授权功能，则计费服务器仅对授权通过的命令进行记录。关于命令行计费的详细介绍请参考“基础配置指导”中的“配置用户通过 CLI 登录设备”。
- 用户角色切换认证：在不退出当前登录、不断开当前连接的前提下，用户将当前的用户角色切换为其它用户角色时，只有通过服务器的认证，该切换操作才被允许。关于用户角色切换的详细介绍请参考“基础配置指导”中的“RBAC”。

1.1.6 协议规范

与 AAA、RADIUS、HWTACACS、LDAP 相关的协议规范有：

- RFC 2865：Remote Authentication Dial In User Service (RADIUS)
- RFC 2866：RADIUS Accounting
- RFC 2867：RADIUS Accounting Modifications for Tunnel Protocol Support
- RFC 2868：RADIUS Attributes for Tunnel Protocol Support
- RFC 2869：RADIUS Extensions
- RFC 5176：Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)
- RFC 1492：An Access Control Protocol, Sometimes Called TACACS
- RFC 1777：Lightweight Directory Access Protocol
- RFC 2251：Lightweight Directory Access Protocol (v3)

1.1.7 RADIUS属性

1. 常用RADIUS标准属性

表1-4 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认证方式时，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的消息摘要。在采用CHAP认证方式时，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采用本地一个接口的IP地址来唯一的标识自己，这就是NAS-IP-Address。该属性指示当前发起请求的Client的NAS-IP-Address。该字段仅出现在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
7	Framed-Protocol	用户Frame类型业务的封装协议
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
12	Framed-MTU	用户与NAS之间数据链路的MTU（Maximum Transmission Unit，最大传输单元）值。例如在802.1X的EAP方式认证中，NAS通过Framed-MTU值指示Server发送EAP报文的最大长度，防止EAP报文大于数据链路MTU导致的报文丢失
14	Login-IP-Host	用户登录设备的接口IP地址
15	Login-Service	用户登录设备时采用的业务类型
18	Reply-Message	服务器反馈给用户的纯文本描述，可用于向用户显示认证失败的原因

属性编号	属性名称	描述
26	Vendor-Specific	厂商自定义的私有属性。一个报文中可以有一个或者多个私有属性，每个私有属性中可以有一个或者多个子属性
27	Session-Timeout	会话结束之前，给用户提供服务的最大时间，即用户的最大可用时长
28	Idle-Timeout	会话结束之前，允许用户持续空闲的最大时间，即用户的限制切断时间
31	Calling-Station-Id	NAS用于向Server告知标识用户的号码，在我司设备提供的lan-access业务中，该字段填充的是用户的MAC地址
32	NAS-Identifier	NAS用来向Server标识自己的名称
40	Acct-Status-Type	计费请求报文的类型 • 1：Start • 2：Stop • 3：Interim-Update • 4：Reset-Charge • 7：Accounting-On（3GPP 中有定义） • 8：Accounting-Off （3GPP 中有定义） • 9-14：Reserved for Tunnel Accounting • 15：Reserved for Failed
45	Acct-Authentic	用户采用的认证方式，包括RADIUS，Local以及Remote
60	CHAP-Challenge	在CHAP认证中，由NAS生成的用于MD5计算的随机序列
61	NAS-Port-Type	NAS认证用户的端口的物理类型 • 15：以太网 • 16：所有种类的 ADSL • 17：Cable（有线电视电缆） • 19：WLAN-IEEE 802.11 • 201：VLAN • 202：ATM 如果在ATM或以太网端口上还划分VLAN，则该属性值为201
79	EAP-Message	用于封装EAP报文，实现RADIUS协议对EAP认证方式的支持
80	Message-Authenticator	用于对认证报文进行认证和校验，防止非法报文欺骗。该属性在RADIUS协议支持EAP认证方式被使用
87	NAS-Port-Id	用字符串来描述的认证端口信息

2. H3C RADIUS扩展属性

表1-5 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

子属性编号	子属性名称	描述
2	Input-Average-Rate	用户接入到NAS的平均速率，以bps为单位
3	Input-Basic-Rate	用户接入到NAS的基本速率，以bps为单位
4	Output-Peak-Rate	从NAS到用户的峰值速率，以bps为单位
5	Output-Average-Rate	从NAS到用户的平均速率，以bps为单位
6	Output-Basic-Rate	从NAS到用户的基本速率，以bps为单位
15	Remanent_Volume	表示该连接的剩余可用总流量。对于不同的服务器类型，此属性的单位不同
20	Command	用于会话控制，表示对会话进行操作，此属性有五种取值 • 1：Trigger-Request • 2：Terminate-Request • 3：SetPolicy • 4：Result • 5：PortalClear
24	Control_Identifier	服务器重发报文的标识符，对于同一会话中的重发报文，本属性必须相同。不同的会话的报文携带的该属性值可能相同。相应的客户端响应报文必须携带该属性，其值不变 在开始、停止或中间上报流量的Accounting-Request报文中，若带有Control_Identifier属性，此时的Control_Identifier属性无实际意义
25	Result_Code	表示Trigger-Request或SetPolicy的结果，0表示成功，非0表示失败
26	Connect_ID	用户连接索引
28	Ftp_Directory	FTP/SFTP/SCP用户工作目录 对于FTP/SFTP/SCP用户，当RADIUS客户端作为FTP/SFTP/SCP服务器时，该属性用于设置RADIUS客户端上的FTP/SFTP/SCP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，表示从1970年1月1日UTC 00:00:00以来的秒数
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”，IP地址和MAC地址之间以空格分开
61	User_Notify	服务器需要透传到客户端的信息
62	User_HeartBeat	802.1X用户认证成功后下发的32字节的Hash字符串，该属性值被保存在设备的用户列表中，用于校验802.1X客户端的握手报文 该属性仅出现在Access-Accept和Accounting-Request报文中
111	Longitude-Latitude	NAS的经度和纬度信息
201	Input-Interval-Octets	两次实时计费间隔的输入的字节差，以Byte为单位
202	Output-Interval-Octets	两次实时计费间隔的输出的字节差，以Byte为单位
203	Input-Interval-Packets	两次计费间隔的输入的包数，单位由设备上的配置决定
204	Output-Interval-Packets	两次计费间隔的输出的包数，单位由设备上的配置决定

子属性编号	子属性名称	描述
205	Input-Interval-Gigawords	两次计费间隔的输入的字节差是4G字节的多少倍
206	Output-Interval-Gigawords	两次计费间隔的输出的字节差是4G字节的多少倍
207	Backup-NAS-IP	NAS发送RADIUS报文的备份源IP地址
255	Product_ID	产品名称

1.2 AAA配置思路及配置任务简介

在作为 AAA 客户端的接入设备（实现 NAS 功能的网络设备）上，AAA 的基本配置思路如下：

(1) 配置 AAA 方案：根据不同的组网环境，配置相应的 AAA 方案。

- 本地认证：由 NAS 自身对用户进行认证、授权和计费。需要配置本地用户，即 local user 的相关属性，包括手动添加用户的用户名和密码等。
- 远程认证：由远程 AAA 服务器来对用户进行认证、授权和计费。需要配置 RADIUS、HWTACACS 或 LDAP 方案。

(2) 配置实现 AAA 的方法：在用户所属的 ISP 域中分别指定实现认证、授权、计费的方法。其中，远程认证、授权、计费方法中均需要引用已经配置的 RADIUS、HWTACACS 或 LDAP 方案。

- 认证方法：可选择不认证（none）、本地认证（local）或远程认证（scheme）；
- 授权方法：可选择不授权（none）、本地授权（local）或远程授权（scheme）；
- 计费方法：可选择不计费（none）、本地计费（local）或远程计费（scheme）。

图1-10 AAA 基本配置思路流程图

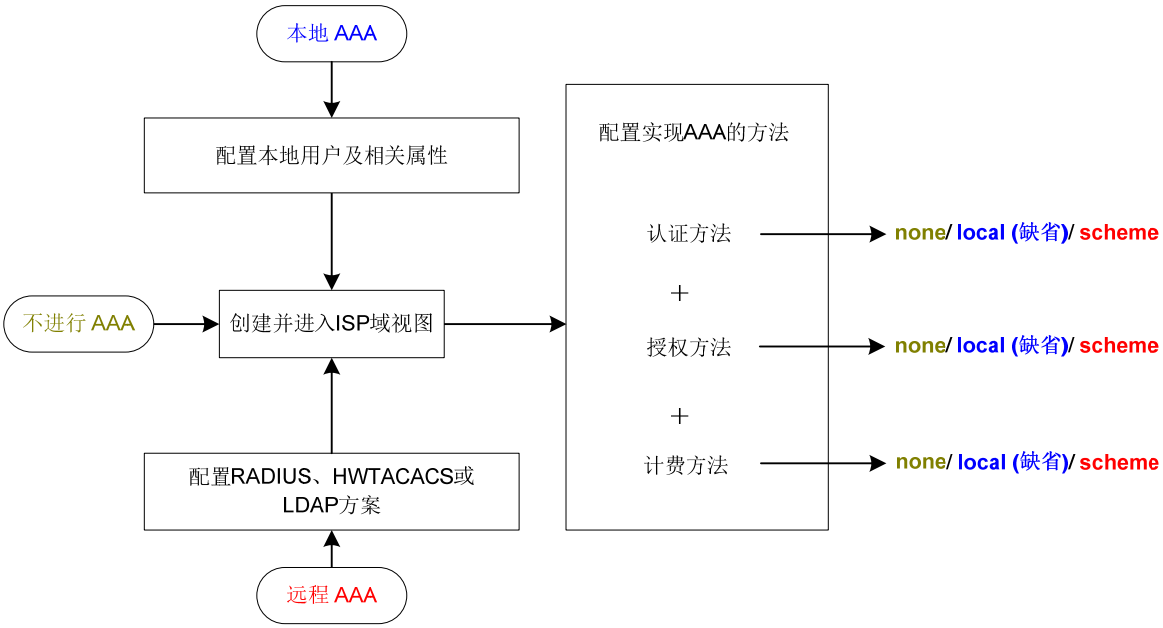


表1-6 AAA 配置任务简介

配置任务		说明	详细配置
配置AAA方案	配置本地用户	四者至少选其一	1.3.1
	配置RADIUS方案		1.3.2
	配置HWTACACS方案		1.3.3
	配置LDAP方案		1.3.4
在ISP域中配置实现AAA的方法	创建ISP域	必选	1.4.2
	配置ISP域的属性	可选	1.4.3
	配置ISP域的AAA认证方法	三者至少选其一	1.4.4
	配置ISP域的AAA授权方法		1.4.5
	配置ISP域的AAA计费方法		1.4.6
配置RADIUS session control功能		可选	1.5
配置RADIUS DAE服务器功能		可选	1.6
配置RADIUS协议报文的DSCP优先级		可选	1.7
限制同时在线的最大用户连接数		可选	1.8
配置本地BYOD授权		可选	1.9
配置ITA业务策略		可选	1.10
配置NAS-ID与VLAN的绑定		可选	1.11

1.3 配置AAA方案

1.3.1 配置本地用户

当选择使用本地认证、本地授权、本地计费方法对用户进行认证、授权或计费时，应在设备上创建本地用户并配置相关属性。

所谓本地用户，是指在本地设备上设置的一组用户属性的集合。该集合以用户名和用户类别为用户的唯一标识。本地用户分为两类，一类是设备管理用户；另一类是网络接入用户。设备管理用户供设备管理员登录设备使用，网络接入用户供通过设备访问网络服务的用户使用。

网络接入用户中还存在一种来宾用户，供临时接入网络的访客使用。来宾用户可以支持的服务类型为 lan-access 和 Portal。

为使某个请求网络服务的用户可以通过本地认证，需要在设备上的本地用户数据库中添加相应的表项。具体步骤是，创建一个本地用户并进入本地用户视图，然后在本地用户视图下配置相应的用户属性，可配置的用户属性包括：

- 描述信息
- 服务类型

用户可使用的网络服务类型。该属性是本地认证的检测项，如果没有用户可以使用的服务类型，则该用户无法通过认证。

支持的服务类型包括：FTP、HTTP、HTTPS、IKE、lan-access、Portal、PPP、SSH、Telnet、Terminal。

- 用户状态

用于指示是否允许该用户请求网络服务器，包括 active 和 block 两种状态。active 表示允许该用户请求网络服务，block 表示禁止该用户请求网络服务。

- 最大用户数

使用当前用户名接入设备的最大用户数目。若当前该用户名的接入用户数已达最大值，则使用该用户名的新用户将被禁止接入。

- 所属的用户组

每一个本地用户都属于一个本地用户组，并继承组中的所有属性（密码管理属性和用户授权属性）。关于本地用户组的介绍和配置请参见“1.3.1 2. 配置用户组属性”。

- 绑定属性

用户认证时需要检测的属性，用于限制接入用户的范围。若用户的实际属性与设置的绑定属性不匹配，则不能通过认证，因此在配置绑定属性时要考虑该用户是否需要绑定某些属性。可绑定的属性包括：ISDN用户的主叫号码、用户IP地址、用户接入端口、用户MAC地址、用户所属VLAN。各属性的使用及支持情况请见 表 1-8。

- 用户授权属性

用户认证通过后，接入设备下发给用户的授权属性。支持的授权属性请见 表 1-8。由于可配置的授权属性都有其明确的使用环境和用途，因此配置授权属性时要考虑该用户是否需要某些属性。例如，PPP接入用户不需要授权的目录，因此就不要设置PPP用户的工作目录属性。

本地用户的授权属性在用户组和本地用户视图下都可以配置，且本地用户视图下的配置优先级高于用户组视图下的配置。用户组的配置对组内所有本地用户生效。

- 密码管理属性

用户密码的安全属性，可用于对设备管理类本地用户的认证密码进行管理和控制。可设置的策略包括：密码老化时间、密码最小长度、密码组合策略、密码复杂度检查策略和用户登录尝试次数限制策略。

本地用户的密码管理属性在系统视图（具有全局性）、用户组视图和本地用户视图下都可以配置，其生效的优先级顺序由高到底依次为本地用户、用户组、全局。全局配置对所有本地用户生效，用户组的配置对组内所有本地用户生效。有关密码管理以及全局密码配置的详细介绍请参见“安全配置指导”中的“Password Control”。

表1-7 配置任务简介

配置任务	说明	详细配置
配置本地用户属性	必选	1.3.1 1.
配置用户组属性	可选	1.3.1 2.
配置本地来宾用户属性	可选	1.3.1 3.
配置本地来宾用户管理	可选	1.3.1 4.
本地用户及本地用户组显示与维护	可选	1.3.1 5.

1. 配置本地用户属性

配置本地用户属性时，有以下配置限制和指导：

- 使能全局密码管理功能（通过命令 **password-control enable**）后，设备上将不显示配置的本地用户密码。
- 授权属性可以在本地用户视图和用户组视图下配置，各视图下的配置优先级顺序从高到底依次为：本地用户视图-->用户组视图。
- 在绑定接口属性时要考虑绑定接口类型是否合理。对于不同接入类型的用户，请按照如下方式进行绑定接口属性的配置：
  - 802.1X 用户：配置绑定的接口为使能 802.1X 的二层以太网接口；
  - MAC 地址认证用户：配置绑定的接口为使能 MAC 地址认证的二层以太网接口；
  - Portal 用户：若使能 Portal 的接口为 VLAN 接口，且没有通过 **portal roaming enable** 命令配置 Portal 用户漫游功能，则配置绑定的接口为用户实际接入的二层以太网接口；其它情况下，配置绑定的接口均为使能 Portal 的接口。

表1-8 配置本地用户的属性

操作		命令	说明
进入系统视图		**system-view**	-
添加本地用户，并进入本地用户视图		**local-user** *user-name* [**class** { **manage** | **network** }]	缺省情况下，不存在本地用户
（可选）设置本地用户的密码	对于网络接入类（**network**）本地用户	**password** { **cipher** | **simple** } *password*	缺省情况下，不存在本地用户密码，即本地用户认证时无需输入密码，只要用户名有效且其它属性验证通过即可认证成功
	对于设备管理类（**manage**）本地用户	**password** [{ **hash** | **simple** } *password*]	
设置本地用户可以使用的服务类型	对于网络接入类（**network**）本地用户	**service-type** { **ike** | **lan-access** | **portal** | **ppp** }	缺省情况下，本地用户不能使用任何服务类型
	对于设备管理类（**manage**）本地用户	**service-type** { **ftp** | { **http** | **https** | **ssh** | **telnet** | **terminal** } * }	
（可选）设置本地用户的状态		**state** { **active** | **block** }	缺省情况下，本地用户处于活动状态，即允许该用户请求网络服务
（可选）设置使用当前本地用户名接入设备的最大用户数		**access-limit** *max-user-number*	缺省情况下，不限制使用当前本地用户名接入的用户数 由于FTP/SFTP/SCP用户不支持计费，因此FTP/SFTP/SCP用户不受此属性限制
（可选）设置本地用户的绑定属性		**bind-attribute** { **call-number** *call-number* [**:** *subcall-number*] | **ip** *ip-address* | **location interface** *interface-type interface-number* | **mac** *mac-address* | **vlan** *vlan-id* } *	缺省情况下，未设置本地用户的任何绑定属性

操作		命令	说明
（可选）设置本地用户的授权属性		**authorization-attribute** { **acl** *acl-number* | **callback-number** *callback-number* | **idle-cut** *minute* | **ip** *ipv4-address* | **ip-pool** *ipv4-pool-name* | **ipv6** *ipv6-address* | **ipv6-pool** *ipv6-pool-name* | **ipv6-prefix** *ipv6-prefix prefix-length* | { **primary-dns** | **secondary-dns** } { **ip** *ip-address* | **ipv6** *ipv6-address* } | **session-timeout** *minutes* | **url** *url-string* | **user-profile** *profile-name* | **user-role** *role-name* | **vlan** *vlan-id* | **work-directory** *directory-name* } *	缺省情况下，授权FTP/SFTP/SCP用户可以访问的目录为设备的根目录，但无访问权限。由用户角色为network-admin或者level-15的用户创建的本地用户被授权用户角色network-operator
（可选）设置设备管理类本地用户的密码管理属性	密码老化时间	**password-control aging** *aging-time*	缺省情况下，采用本地用户所属用户组的密码管理策略 仅设备管理类的本地用户支持本地用户密码管理功能
	密码最小长度	**password-control length** *length*	
	密码组合策略	**password-control composition type-number** *type-number* [**type-length** *type-length*]	
	密码的复杂度检查策略	**password-control complexity** { **same-character** | **user-name** } **check**	
	用户登录尝试次数以及登录尝试失败后的行为	**password-control login-attempt** *login-times* [**exceed** { **lock** | **lock-time** *time* | **unlock** }]	
（可选）设置本地用户所属的用户组		**group** *group-name*	缺省情况下，本地用户属于用户组system
（可选）设置网络接入类本地用户的描述信息		**description** *text*	缺省情况下，未配置网络接入类本地用户的描述信息

2. 配置用户组属性

为了简化本地用户的配置，增强本地用户的可管理性，引入了用户组的概念。用户组是一个本地用户属性的集合，某些需要集中管理的属性可在用户组中统一配置和管理，用户组内的所有本地用户都可以继承这些属性。目前，用户组中可以管理的用户属性为授权属性。

每个新增的本地用户都默认属于一个系统自动创建的用户组 system，且继承该组的所有属性。本地用户所属的用户组可以通过本地用户视图下的 **group** 命令来修改。

表1-9 配置用户组的属性

操作	命令	说明
进入系统视图	**system-view**	-
创建用户组，并进入用户组视图	**user-group** *group-name*	缺省情况下，存在一个用户组，名称为system

操作		命令	说明
设置用户组的授权属性		**authorization-attribute** { **acl** *acl-number* | **callback-number** *callback-number* | **idle-cut** *minute* | **ipv6-pool** *ipv6-pool-name* | **ipv6-prefix** *ipv6-prefix prefix-length* | { **primary-dns** | **secondary-dns** } { **ip** *ip-address* | **ipv6** *ipv6-address* } | **session-timeout** *minutes* | **url** *url-string* | **user-profile** *profile-name* | **vlan** *vlan-id* | **work-directory** *directory-name* } *	缺省情况下，未设置用户组的授权属性
（可选）设置用户组的密码管理属性	密码老化时间	**password-control aging** *aging-time*	缺省情况下，采用全局密码管理策略 全局密码管理策略的相关配置请参见“安全配置指导”中的“Password Control”
	密码最小长度	**password-control length** *length*	
	密码组合策略	**password-control composition type-number** *type-number* [**type-length** *type-length*]	
	密码的复杂度检查策略	**password-control complexity** { **same-character** | **user-name** } **check**	
	用户登录尝试次数以及登录尝试失败后的行为	**password-control login-attempt** *login-times* [**exceed** { **lock** | **lock-time** *time* | **unlock** }]	

3. 配置本地来宾用户属性

为使临时接入网络的访客可以通过本地认证并方便管理员对访客的访问权限进行管理，需要在设备上的本地用户数据库中添加相应的本地来宾用户表项。具体步骤是，创建一个本地来宾用户并进入本地来宾用户视图，然后在该视图下配置相应的来宾用户属性，可配置的属性包括：

- 密码。
- 描述信息。
- 个人信息：姓名、公司、电话号码以及 Email 地址（用于向来宾发送本地来宾用户用户名和密码的通知邮件）。
- 接待人信息：接待人姓名、接待人所在部门以及接待人 Email 地址（用于向来宾接待人发送本地来宾用户用户名和密码的通知邮件）。
- 有效期：来宾使用用户名和密码只能在有效期内认证通过。
- 用户组：本地来宾用户的授权属性继承所属用户组的属性。

完成本地来宾用户属性的配置后，可向来宾或来宾接待人发送包含用户名、密码、有效期的通知邮件。

表1-10 配置本地来宾用户属性

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
创建本地来宾用户，并进入本地来宾用户视图	**local-user** *user-name* **class network guest**	缺省情况下，不存在本地来宾用户
配置本地来宾用户的密码	**password** { **cipher** | **simple** } *password*	缺省情况下，未配置本地来宾用户的密码
配置本地来宾用户的描述信息	**description** *user-info*	缺省情况下，未配置本地来宾用户的描述信息
配置本地来宾用户的姓名	**full-name** *name-string*	缺省情况下，未配置本地来宾用户的姓名
配置本地来宾用户所属公司	**company** *company-name*	缺省情况下，未配置本地来宾用户所属公司
配置本地来宾用户的电话号码	**phone** *phone-number*	缺省情况下，未配置本地来宾用户电话号码
配置本地来宾用户的Email地址	**email** *email-string*	缺省情况下，未配置本地来宾用户的Email地址
配置本地来宾用户的接待人姓名	**sponsor-full-name** *name-string*	缺省情况下，未配置本地来宾用户的接待人姓名
配置本地来宾用户接待人所属部门	**sponsor-department** *department-string*	缺省情况下，未配置本地来宾用户接待人所属部门
配置本地来宾用户接待人的Email地址	**sponsor-email** *email-string*	缺省情况下，未配置本地来宾用户接待人的Email地址
配置本地来宾用户的有效期	**validity-datetime** *start-date start-time* **to** *expiration-date expiration-time*	缺省情况下，未限制本地来宾用户的有效期，该用户始终有效
配置本地来宾用户所属的用户组	**group** *group-name*	缺省情况下，本地来宾用户属于系统默认创建的用户组system
退回系统视图	**quit**	-

4. 配置本地来宾管理功能

随着无线智能终端的快速发展，对于来公司参观的访客，公司需要提供一些网络服务。这些访客成员通常为供应商、贵宾、听众或者是其他合作伙伴等。当访客用自己的手机、笔记本、IPAD 等终端接入公司网络时，涉及到用户账号注册，以及访问权限控制的问题。为了简化访客的注册和审批流程，以及对访客权限的管理控制，提供了本地来宾用户管理功能，具体包括：

- 来宾用户过期自动删除功能：设备定时检查本地来宾用户是否过期并自动删除过期的用户。
- 本地来宾用户的注册与审批，具体过程如下：

(1) 来宾用户通过设备推出的 Portal Web 页面填写注册信息，主要包括用户名、密码和 Email 地址，并提交该信息。

(2) 设备收到来宾用户的注册信息后，记录该注册信息，并向来宾管理员发送一个注册申请通知邮件。

(3) 来宾管理员收到注册申请通知邮件之后，在设备的 Web 页面上对该帐户进行编辑和审批。

(4) 如果该帐户在等待审批时间超时前被来宾管理员审批通过，则设备将自动在本地创建一个本地来宾用户，并生成该用户的相关属性。若该帐户在等待审批时间超时后还未被审批通过，则设备将会删除本地记录的该用户注册信息。

(5) 本地来宾用户创建之后，设备将自动发送邮件通知本地来宾用户或来宾接待人用户注册成功，向他们告知本地来宾用户的密码及有效期信息。

(6) 本地来宾用户收到注册成功通知后，将可以使用注册的帐户访问网络。

- 邮件通知功能：向来宾、来宾接待人、来宾管理员发送帐户审批、密码信息的邮件。
- 批量创建本地来宾用户：在设备上批量生成一系列本地来宾帐户，这些账户的用户名和密码按照指定规律生成。
- 导入本地来宾用户信息：将指定路径 CSV 文件的本地来宾帐户信息导入到设备上，并生成相应的本地来宾用户。导入操作成功后，该类帐户可直接用于访问网络。
- 导出本地来宾用户信息：将设备上的本地来宾帐户信息导出到指定路径 CSV 文件中供其它设备使用

表1-11 配置本地来宾用户管理功能

操作	命令	说明
进入系统视图	**system-view**	-
配置本地来宾用户的邮件格式	**local-guest email format to** { **guest** | **manager** | **sponsor** } { **body** *body-string* | **subject** *sub-string* }	缺省情况下，未配置本地来宾用户的邮件格式
配置本地来宾用户的发件人Email地址	**local-guest email sender** *email-address*	缺省情况下，未配置本地来宾用户的发件人Email地址
配置本地来宾用户发送Email使用的SMTP服务器	**local-guest email smtp-server** *url-string*	缺省情况下，未配置本地来宾用户发送Email使用的SMTP服务器
配置来宾管理员的Email地址	**local-guest manager-email** *email-address*	缺省情况下，未配置来宾管理员的Email地址。
（可选）配置本地来宾用户的等待审批超时定时器	**local-guest timer waiting-approval** *time-value*	缺省情况下，来宾注册信息等待审批超时定时器的值为24小时
（可选）从指定路径的文件中导入用户信息并创建本地来宾用户	**local-user-import class network guest url** *url-string* **validity-datetime** *start-date start-time* **to** *expiration-date expiration-time* [**auto-create-group** | **override** | **start-line** *line-number*] *	本命令用于将指定文件的本地来宾帐户信息导入到接入设备上，并生成相应的本地来宾用户。导入操作成功后，该类帐户可直接用于访问网络
（可选）批量创建本地来宾用户	**local-guest generate username-prefix** *name-prefix* [**password-prefix** *password-prefix*] **suffix** *suffix-number* [**group** *group-name*] **count** *user-count* **validity-datetime** *start-date start-time* **to** *expiration-date expiration-time*	本命令用于在设备上批量生成一系列本地来宾帐户，这些账户的用户名和密码等属性按照指定规律生成。批量创建成功后，该类帐户可直接用于访问网络
（可选）从设备导出本地来宾用户信息到指定路径的CSV文件	**local-user-export class network guest url** *url-string*	本命令用于将设备上的本地来宾帐户信息导出到文件中供其它设备使用
（可选）开启来宾用户过期自动删除功能	**local-guest auto-delete enable**	缺省情况下，来宾用户过期自动删除功能处于关闭状态

操作	命令	说明
退回用户视图	**quit**	-
向本地来宾用户邮箱和来宾接待人邮箱发送邮件	**local-guest send-email user-name** *user-name* **to** { **guest** | **sponsor** }	可以通过执行本命令向相关人发送通知邮件，邮件中包含用户名、密码以及有效期信息

5. 本地用户及本地用户组显示与维护

完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后本地用户及本地用户组的运行情况，通过查看显示信息验证配置的效果。

表1-12 本地用户及本地用户组显示和维护

操作	命令
显示本地用户的配置信息和在线用户数的统计信息	**display local-user** [**class** { **manage** | **network** [**guest**] } | **idle-cut** { **disable** | **enable** } | **service-type** { **ftp** | **http** | **https** | **ike** | **lan-access** | **portal** | **ppp** | **ssh telnet** | **terminal** } | **state** { **active** | **block** } | **user-name** *user-name* **class** { **manage** | **network** [**guest**] } | **vlan** *vlan-id*]
显示本地用户组的相关配置	**display user-group** { **all** | **name** *group-name* [**byod-authorization**] }
显示待审批来宾用户注册信息	**display local-guest waiting-approval** [**username** *user-name*]
清除待审批的来宾用户注册信息	**reset local-guest waiting-approval** [**username** *username*]

1.3.2 配置RADIUS方案

RADIUS 方案中定义了设备和 RADIUS 服务器之间进行信息交互所必需的一些参数，主要包括 RADIUS 服务器的 IP 地址、UDP 端口号、报文共享密钥、服务类型等。

1. RADIUS配置任务简介

表1-13 RADIUS 配置任务简介

配置任务	说明	详细配置
配置RADIUS服务器探测模版	可选	1.3.2 2.
创建RADIUS方案	必选	1.3.2 3.
配置RADIUS认证服务器	必选	1.3.2 4.
配置RADIUS计费服务器及相关参数	可选	1.3.2 5.
配置RADIUS报文的共享密钥	可选	1.3.2 6.
配置发送给RADIUS服务器的用户名格式和数据统计单位	可选	1.3.2 7.
配置发送RADIUS报文的最大尝试次数	可选	1.3.2 8.
配置RADIUS服务器的状态	可选	1.3.2 9.
配置发送RADIUS报文使用的源地址	可选	1.3.2 10.
配置RADIUS服务器的定时器	可选	1.3.2 11.

配置任务	说明	详细配置
配置RADIUS的accounting-on功能	可选	1.3.2 12.
配置RADIUS Attribute 25的CAR参数解析功能	可选	1.3.2 13.
配置RADIUS Attribute 15的检查方式	可选	1.3.2 14.
配置RADIUS Remanent_Volume属性的流量单位	可选	1.3.2 15.
配置RADIUS Attribute 31中的MAC地址格式	可选	1.3.2 16.
配置RADIUS告警功能	可选	1.3.2 17.
RADIUS显示和维护	可选	1.3.2 18.

2. 配置RADIUS服务器探测模版

RADIUS 服务器探测功能是指，设备周期性发送探测报文探测 RADIUS 服务器是否可达：如果服务器不可达，则置服务器状态为 **block**，如果服务器可达，则置服务器状态为 **active**。该探测功能不依赖于实际用户的认证过程，无论是否有用户向 RADIUS 服务器发起认证，无论是否有用户在线，设备都会自动对指定的 RADIUS 服务器进行探测，便于及时获得该服务器的可达状态。

RADIUS 服务器探测模板用于配置探测用户名以及探测周期，并且可以被 RADIUS 方案视图下的 RADIUS 服务器配置引用。只有一个 RADIUS 服务器配置中成功引用了一个已经存在的服务器探测模板，设备才会启动对该 RADIUS 服务器的探测功能。

RADIUS 服务器探测报文是一种模拟的认证请求报文，服务器探测模板中配置的探测用户名即为该探测报文中的认证用户名。设备会在配置的探测周期内选择随机时间点向引用了服务器探测模板的 RADIUS 服务器发送探测报文，且每次收到的探测应答消息仅能说明当前探测周期内该 RADIUS 服务器可达。服务器探测功能启动后，周期性的探测过程会一直执行，直到相关的配置发生变化（包括：删除该 RADIUS 服务器配置、取消对服务器探测模板的引用、删除对应的服务器探测模板、将该 RADIUS 服务器的状态手工置为 **block**、删除当前 RADIUS 方案）。

表1-14 配置 RADIUS 服务器探测模版

操作	命令	说明
进入系统视图	**system-view**	-
配置RADIUS服务器探测模版	**radius-server test-profile** *profile-name* **username** *name* [**interval** *interval*]	缺省情况下，不存在RADIUS服务器探测模板 系统支持最多同时存在多个RADIUS服务器探测模板

3. 创建RADIUS方案

在进行 RADIUS 的其它配置之前，必须先创建 RADIUS 方案并进入其视图。系统最多支持配置 16 个 RADIUS 方案。一个 RADIUS 方案可以同时被多个 ISP 域引用。

表1-15 创建 RADIUS 方案

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
创建RADIUS方案，并进入RADIUS方案视图	**radius scheme** *radius-scheme-name*	缺省情况下，不存在RADIUS方案

4. 配置RADIUS认证服务器

由于 RADIUS 服务器的授权信息是随认证应答报文发送给 RADIUS 客户端的，RADIUS 的认证和授权功能由同一台服务器实现，因此 RADIUS 认证服务器相当于 RADIUS 认证/授权服务器。通过在 RADIUS 方案中配置 RADIUS 认证服务器，指定设备对用户进行 RADIUS 认证时与哪些服务器进行通信。

一个RADIUS方案中最多允许配置一个主认证服务器和16个从认证服务器。当主服务器不可达时，设备根据从服务器的配置顺序由先到后查找状态为 **active** 的从服务器并与之交互。建议在不需要备份的情况下，只配置主 RADIUS 认证服务器即可。

在实际组网环境中，可以指定一台服务器既作为某个 RADIUS 方案的主认证服务器，又作为另一个 RADIUS 方案的从认证服务器。

表1-16 配置 RADIUS 认证服务器

操作	命令	说明
进入系统视图	**system-view**	-
进入RADIUS方案视图	**radius scheme** *radius-scheme-name*	-
配置主RADIUS认证服务器	**primary authentication** { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **test-profile** *profile-name*] *	二者至少选其一 缺省情况下，未配置主认证服务器和从认证服务器 在同一个方案中指定的主认证服务器和从认证服务器的IP地址、端口号不能完全相同，并且各从认证服务器的IP地址、端口号也不能完全相同
配置从RADIUS认证服务器	**secondary authentication** { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **test-profile** *profile-name*] *	

5. 配置RADIUS计费服务器及相关参数

通过在 RADIUS 方案中配置 RADIUS 计费服务器，指定设备对用户进行 RADIUS 计费时与哪些服务器进行通信。

一个RADIUS方案中最多允许配置一个主计费服务器和16个从计费服务器。当主服务器不可达时，设备根据从服务器的配置顺序由先到后查找状态为 **active** 的从服务器并与之交互。建议在不需要备份的情况下，只配置主 RADIUS 计费服务器即可。

在实际组网环境中，可以指定一台服务器既作为某个 RADIUS 方案的主计费服务器，又作为另一个 RADIUS 方案的从计费服务器。

当用户请求断开连接或者设备强行切断用户连接的情况下，设备会向 RADIUS 计费服务器发送停止计费请求。通过在设备上配置发起实时计费请求的最大尝试次数，允许设备向 RADIUS 服务器发出的实时计费请求没有得到响应的次数超过指定的最大值时切断用户连接。

目前 RADIUS 不支持对 FTP/SFTP/SCP 用户进行计费。

表1-17 配置 RADIUS 计费服务器及相关参数

操作	命令	说明
进入系统视图	**system-view**	-
进入RADIUS方案视图	**radius scheme** *radius-scheme-name*	-
配置主RADIUS计费服务器	**primary accounting** { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string*] *	二者至少选其一 缺省情况下，未配置主/从计费服务器 在同一个方案中指定的主计费服务器和从计费服务器的IP地址、端口号不能完全相同，并且各从计费服务器的IP地址、端口号也不能完全相同
配置从RADIUS计费服务器	**secondary accounting** { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string*] *	
（可选）设置允许发起实时计费请求的最大尝试次数	**retry realtime-accounting** *retry-times*	缺省情况下，允许发起实时计费请求的最大尝试次数为5

6. 配置RADIUS报文的共享密钥

RADIUS 客户端与 RADIUS 服务器使用 MD5 算法并在共享密钥的参与下生成验证字，接受方根据收到报文中的验证字来判断对方报文的合法性。只有在共享密钥一致的情况下，彼此才能接收对方发来的报文并作出响应。

由于设备优先采用配置 RADIUS 认证/计费服务器时指定的报文共享密钥，因此，本配置中指定的 RADIUS 报文共享密钥仅在配置 RADIUS 认证/计费服务器时未指定相应密钥的情况下使用。

表1-18 配置 RADIUS 报文的共享密钥

操作	命令	说明
进入系统视图	**system-view**	-
进入RADIUS方案视图	**radius scheme** *radius-scheme-name*	-
配置RADIUS报文的共享密钥	**key** { **accounting** | **authentication** } { **cipher** | **simple** } *string*	缺省情况下，未配置RADIUS报文的共享密钥 必须保证设备上设置的共享密钥与RADIUS服务器上的完全一致

7. 配置发送给RADIUS服务器的用户名格式和数据统计单位

接入用户通常以“*userid@isp-name*”的格式命名，“@”后面的部分为 ISP 域名，设备通过该域名决定将用户归于哪个 ISP 域。由于有些较早期的 RADIUS 服务器不能接受携带有 ISP 域名的用户名，因此就需要设备首先将用户名中携带的 ISP 域名去除后再传送给该类 RADIUS 服务器。通过设置发送给 RADIUS 服务器的用户名格式，就可以选择发送 RADIUS 服务器的用户名中是否要携带 ISP 域名，以及是否保持用户输入的原始用户名格式。

设备通过发送计费报文，向 RADIUS 服务器报告在线用户的数据流量统计值，该值的单位可配，为保证 RADIUS 服务器计费的准确性，设备上设置的发送给 RADIUS 服务器的数据流或者数据包的单位应与 RADUIS 服务器上的流量统计单位保持一致。

需要注意的是，如果要在两个乃至两个以上的 ISP 域中引用相同的 RADIUS 方案，建议设置该 RADIUS 方案允许用户名中携带 ISP 域名，使得 RADIUS 服务器端可以根据 ISP 域名来区分不同的用户。

表1-19 配置发送给 RADIUS 服务器用户名格式和数据统计单位

操作	命令	说明
进入系统视图	**system-view**	-
进入RADIUS方案视图	**radius scheme** *radius-scheme-name*	-
设置发送给RADIUS服务器的用户名格式	**user-name-format { keep-original | with-domain | without-domain }**	缺省情况下，发送给RADIUS服务器的用户名携带ISP域名
设置发送给RADIUS服务器的数据流或者数据包的单位	**data-flow-format { data { byte | giga-byte | kilo-byte | mega-byte } | packet { giga-packet | kilo-packet | mega-packet | one-packet } } ***	可选 缺省情况下，数据流的单位为字节，数据包的单位为包

8. 配置发送RADIUS报文的最大尝试次数

由于RADIUS协议采用UDP报文来承载数据，因此其通信过程是不可靠的。如果设备在应答超时定时器规定的时长内（由**timer response-timeout**命令配置）没有收到RADIUS服务器的响应，则设备有必要向RADIUS服务器重传RADIUS请求报文。如果发送RADIUS请求报文的累计次数已达到指定的最大尝试次数而RADIUS服务器仍旧没有响应，则设备将尝试与其它服务器通信，如果不存在状态为**active**的服务器，则认为本次认证或计费失败。关于RADIUS服务器状态的相关内容，请参见“1.3.2 9. 配置RADIUS服务器的状态”。

表1-20 配置发送 RADIUS 报文的最大尝试次数

操作	命令	说明
进入系统视图	**system-view**	-
进入RADIUS方案视图	**radius scheme** *radius-scheme-name*	-
设置发送RADIUS报文的最大尝试次数	**retry** *retry-times*	缺省情况下，发送RADIUS报文的最大尝试次数为3次

9. 配置RADIUS服务器的状态

RADIUS 方案中各服务器的状态（**active**、**block**）决定了设备向哪个服务器发送请求报文，以及设备在与当前服务器通信中断的情况下，如何转而与另外一个服务器进行交互。在实际组网环境中，可指定一个主 RADIUS 服务器和多个从 RADIUS 服务器，由从服务器作为主服务器的备份。通常情况下，设备上主从服务器的切换遵从以下原则：

- 当主服务器状态为 **active** 时，设备首先尝试与主服务器通信，若主服务器不可达，设备更改主服务器的状态为 **block**，并启动该服务器的 **quiet** 定时器，然后按照从服务器的配置先后顺序依次查找状态为 **active** 的从服务器进行认证或者计费。如果状态为 **active** 的从服务器也不可达，则将该从服务器的状态置为 **block**，同时启动该服务器的 **quiet** 定时器，并继续查找状态为 **active** 的从服务器。当服务器的 **quiet** 定时器超时，或者手动将服务器状态置为 **active** 时，该服务器将恢复为 **active** 状态。在一次认证或计费过程中，如果设备在尝试与从服务器

通信时，之前已经查找过的服务器状态由 **block** 恢复为 **active**，则设备并不会立即恢复与该服务器的通信，而是继续查找从服务器。如果所有已配置的服务器都不可达，则认为本次认证或计费失败。

- 如果在认证或计费过程中删除了当前正在使用的服务器，则设备在与该服务器通信超时后，将会立即从主服务器开始依次查找状态为 **active** 的服务器并与之进行通信。
- 当主/从服务器的状态均为 **block** 时，设备尝试与主服务器进行通信，若未配置主服务器，则设备尝试与首个配置的从服务器通信。
- 只要存在状态为 **active** 的服务器，设备就仅与状态为 **active** 的服务器通信，即使该服务器不可达，设备也不会尝试与状态为 **block** 的服务器通信。
- 一旦服务器状态满足自动切换的条件，则所有 RADIUS 方案视图下该服务器的状态都会相应地变化。
- 将认证服务器的状态由 **active** 修改为 **block** 时，若该服务器引用了 RADIUS 服务器探测模板，则关闭对该服务器的探测功能；反之，将认证服务器的状态由 **block** 更改为 **active** 时，若该服务器引用了一个已存在的 RADIUS 服务器探测模板，则开启对该服务器的探测功能。

缺省情况下，设备将配置了 IP 地址的各 RADIUS 服务器的状态均置为 **active**，认为所有的服务器均处于正常工作状态，但有些情况下用户可能需要通过以下配置手工改变 RADIUS 服务器的当前状态。例如，已知某服务器故障，为避免设备认为其 **active** 而进行无意义的尝试，可暂时将该服务器状态手工置为 **block**。

表1-21 配置 RADIUS 服务器的状态

操作	命令	说明
进入系统视图	**system-view**	-
进入RADIUS方案视图	**radius scheme** *radius-scheme-name*	-
设置主RADIUS认证服务器的状态	**state primary authentication** { **active** | **block** }	四者可选其一 缺省情况下，RADIUS服务器的状态为**active** 设置的服务器状态不能被保存在配置文件中，可通过**display radius scheme**命令查看。设备重启后，各服务器状态将恢复为缺省状态**active**
设置主RADIUS计费服务器的状态	**state primary accounting** { **active** | **block** }	
设置从RADIUS认证服务器的状态	**state secondary authentication** [{ *ipv4-address* | **ipv6** *ipv6-address* } [*port-number*] *] { **active** | **block** }	
设置从RADIUS计费服务器的状态	**state secondary accounting** [{ *ipv4-address* | **ipv6** *ipv6-address* } [*port-number*] *] { **active** | **block** }	

10. 配置发送RADIUS报文使用的源地址

RADIUS 服务器上通过 IP 地址来标识接入设备，并根据收到的 RADIUS 报文的源 IP 地址是否与服务器所管理的接入设备的 IP 地址匹配，来决定是否处理来自该接入设备的认证或计费请求。若 RADIUS 服务器收到的 RADIUS 认证或计费报文的源地址在所管理的接入设备 IP 地址范围内，则会进行后续的认证或计费处理，否则直接丢弃该报文。因此，为保证认证和计费报文可被服务器正常接收并处理，接入设备上发送 RADIUS 报文使用的源地址必须与 RADIUS 服务器上指定的接入设备的 IP 地址保持一致。

通常，该地址为接入设备上与 RADIUS 服务器路由可达的接口 IP 地址。

设备发送 RADIUS 报文时，根据以下顺序查找使用的源地址：

(1) 若当前所使用的 RADIUS 方案中配置了发送 RADIUS 报文使用源地址，则使用该地址。

(2) 否则，根据当前使用的服务器所属的 VPN 查找系统视图下通过 **radius nas-ip** 命令配置的私网源地址，对于公网服务器则直接查找该命令配置的公网源地址。

(3) 若系统视图下没有配置相应的源地址，则使用通过路由查找到的报文出接口地址。

此配置可以在系统视图和 RADIUS 方案视图下进行，系统视图下的配置将对所有 RADIUS 方案生效，RADIUS 方案视图下的配置仅对本方案有效，并且具有高于前者的优先级。

表1-22 为所有 RADIUS 方案配置发送 RADIUS 报文使用的源地址

操作	命令	说明
进入系统视图	**system-view**	-
设置设备发送RADIUS报文使用的源地址	**radius nas-ip** { *ipv4-address* | **ipv6** *ipv6-address* }	缺省情况下，未指定发送RADIUS报文使用的源地址，设备将以发送报文的接口地址作为源地址

表1-23 为 RADIUS 方案配置发送 RADIUS 报文使用的源地址

操作	命令	说明
进入系统视图	**system-view**	-
进入RADIUS方案视图	**radius scheme** *radius-scheme-name*	-
设置设备发送RADIUS报文使用的源地址	**nas-ip** { *ipv4-address* | **ipv6** *ipv6-address* }	缺省情况下，使用系统视图下由命令**radius nas-ip**指定的源地址，若系统视图下未指定源地址，则使用发送RADIUS报文的接口地址

11. 配置RADIUS服务器的定时器

在与 RADIUS 服务器交互的过程中，设备上可启动的定时器包括以下几种：

- 服务器响应超时定时器（**response-timeout**）：如果在 RADIUS 请求报文发送出去一段时间后，设备还没有得到 RADIUS 服务器的响应，则有必要重传 RADIUS 请求报文，以保证用户尽可能地获得 RADIUS 服务，这段时间被称为 RADIUS 服务器响应超时时间。
- 服务器恢复激活状态定时器（**quiet**）：当服务器不可达时，设备将该服务器的状态置为 **block**，并开启超时定时器，在设定的一定时间间隔之后，再将该服务器的状态恢复为 **active**。这段时间被称为 RADIUS 服务器恢复激活状态时长。
- 实时计费间隔定时器（**realtime-accounting**）：为了对用户实施实时计费，有必要定期向服务器发送实时计费更新报文，通过设置实时计费的时间间隔，设备会每隔设定的时间向 RADIUS 服务器发送一次在线用户的计费信息。

设置 RADIUS 服务器的定时器时，请遵循以下配置原则：

- 要根据配置的从服务器数量合理设置发送 RADIUS 报文的最大尝试次数和 RADIUS 服务器响应超时时间，避免因为超时重传时间过长，在主服务器不可达时，出现设备在尝试与从服务器通信的过程中接入模块（例如 Telnet 模块）的客户端连接已超时的现象。但是，有些接入模块的客户端的连接超时时间较短，在配置的从服务器较多的情况下，即使将报文重传次数

和 RADIUS 服务器响应超时时间设置的很小，也可能会出现上述客户端超时的现象，并导致初次认证或计费失败。这种情况下，由于设备会将不可达服务器的状态设置为 **block**，在下次认证或计费时设备就不会尝试与这些状态为 **block** 的服务器通信，一定程度上缩短了查找可达服务器的时间，因此用户再次尝试认证或计费就可以成功。

- 要根据配置的从服务器数量合理设置服务器恢复激活状态的时间。如果服务器恢复激活状态时间设置得过短，就会出现设备反复尝试与状态 **active** 但实际不可达的服务器通信而导致的认证或计费频繁失败的问题；如果服务器恢复激活状态设置的过长，则会导致已经恢复激活状态的服务器暂时不能为用户提供认证或计费服务。
- 实时计费间隔的取值对设备和 RADIUS 服务器的性能有一定的相关性要求，取值小，会增加网络中的数据流量，对设备和 RADIUS 服务器的性能要求就高；取值大，会影响计费的准确性。因此要结合网络的实际情况合理设置计费间隔的大小，一般情况下，建议当用户量比较大（大于等于 1000）时，尽量把该间隔的值设置得大一些。

表1-24 设置 RADIUS 服务器的定时器

操作	命令	说明
进入系统视图	**system-view**	-
进入RADIUS方案视图	**radius scheme** *radius-scheme-name*	-
设置RADIUS服务器响应超时时间	**timer response-timeout** *seconds*	缺省情况下，RADIUS服务器响应超时定时器为3秒
设置服务器恢复激活状态的时间	**timer quiet** *minutes*	缺省情况下，服务器恢复激活状态前需要等待5分钟
设置实时计费间隔	**timer realtime-accounting** *minutes interval* [**second**]	缺省情况下，实时计费间隔为12分钟

12. 配置RADIUS的accounting-on功能

使能了 accounting-on 功能后，集中式设备或分布式设备单板会在重启后主动向 RADIUS 服务器发送 accounting-on 报文来告知自己已经重启，并要求 RADIUS 服务器停止计费且强制通过本设备或单板上线的用户下线。该功能可用于解决集中式设备或分布式设备单板重启后，重启前的原在线用户因被 RADIUS 服务器认为仍然在线而短时间内无法再次登录的问题。若集中式设备或分布式设备单板发送 accounting-on 报文后 RADIUS 服务器无响应，则会在按照一定的时间间隔（**interval** *seconds*）尝试重发几次（**send** *send-times*）。分布式设备单板重启时，accounting-on 功能的实现需要和 H3C IMC 网管系统配合使用。

对于插卡类设备，PPP 和 lan-access 类型的用户数据均保存在用户接入的单板上。开启 accounting-on 扩展功能后，当此类用户接入的单板重启时（整机未重启），设备会向 RADIUS 服务器发送携带设备以及单板标识的 accounting-on 报文，用于通知 RADIUS 服务器对该单板的用户停止计费且强制用户下线。其它类型的用户数据保存在主控板上，只需要开启 accounting-on 功能即可，无需开启 accounting-on 扩展功能。

只有在 accounting-on 功能开启的情况下，accounting-on 扩展功能才能生效。

表1-25 配置 RADIUS 的 accounting-on 功能

操作	命令	说明
进入系统视图	**system-view**	-
进入RADIUS方案视图	**radius scheme** *radius-scheme-name*	-
配置accounting-on功能	**accounting-on enable** [**interval** *seconds* | **send** *send-times*] *	缺省情况下，accounting-on功能处于关闭状态
（可选）开启accounting-on扩展功能	**accounting-on extended**	缺省情况下，accounting-on扩展功能处于关闭状态

13. 配置RADIUS Attribute 25 的CAR参数解析功能

RADIUS 的 25 号属性为 class 属性，该属性由 RADIUS 服务器下发给设备，但 RFC 中并未定义具体的用途，仅规定了设备需要将服务器下发的 class 属性再原封不动地携带在计费请求报文中发送给服务器即可，同时 RFC 并未要求设备必须对该属性进行解析。目前，某些 RADIUS 服务器利用 class 属性来对用户下发 CAR 参数，为了支持这种应用，可以通过本特性来控制设备是否将 RADIUS 25 号属性解析为 CAR 参数，解析出的 CAR 参数可被用来进行基于用户的流量监管控制。

表1-26 配置 RADIUS Attribute 25 的 CAR 参数解析功能

操作	命令	说明
进入系统视图	**system-view**	-
进入RADIUS方案视图	**radius scheme** *radius-scheme-name*	-
开启RADIUS Attribute 25的CAR参数解析功能	**attribute 25 car**	缺省情况下，RADIUS Attribute 25的CAR参数解析功能处于关闭状态

14. 配置RADIUS Attribute 15 的检查方式

RADIUS 15 号属性为Login-Service属性，该属性携带在Access-Accept报文中，由RADIUS服务器下发给设备，表示认证用户的业务类型，例如属性值 0 表示Telnet业务。设备检查用户登录时采用的业务类型与服务器下发的Login-Service属性所指定的业务类型是否一致，如果不一致则用户认证失败 。由于RFC中并未定义SSH、FTP和Terminal这三种业务的Login-Service属性值，因此设备无法针对SSH、FTP、Terminal用户进行业务类型一致性检查，为了支持对这三种业务类型的检查，H3C为Login-Service属性定义了 表 1-27 所示的扩展取值。

表1-27 扩展的 Login-Service 属性值

属性值	描述
50	用户的业务类型为SSH
51	用户的业务类型为FTP
52	用户的业务类型为Terminal

可以通过配置设备对 RADIUS 15 号属性的检查方式，控制设备是否使用扩展的 Login-Service 属性值对用户进行业务类型一致性检查。

- 严格检查方式：设备使用标准属性值和扩展属性值对用户业务类型进行检查，对于 SSH、FTP、Terminal 用户，当 RADIUS 服务器下发的 Login-Service 属性值为对应的扩展取值时才能够通过认证。
- 松散检查方式：设备使用标准属性值对用户业务类型进行检查，对于 SSH、FTP、Terminal 用户，在 RADIUS 服务器下发的 Login-Service 属性值为 0（表示用户业务类型为 Telnet）时才能够通过认证。

由于某些 RADIUS 服务器不支持自定义的属性，无法下发扩展的 Login-Service 属性，若要使用这类 RADIUS 服务器对 SSH、FTP、Terminal 用户进行认证，建议设备上对 RADIUS 15 号属性值采用松散检查方式。

表1-28 配置 RADIUS Attribute 15 的检查方式

操作	命令	说明
进入系统视图	**system-view**	-
进入RADIUS方案视图	**radius scheme** *radius-scheme-name*	-
配置RADIUS Attribute 15的检查方式	**attribute 15 check-mode** { **loose** | **strict** }	缺省情况下，RADIUS Attribute 15的检查方式为strict方式

15. 配置RADIUS Remanent_Volume属性的流量单位

Remanent_Volume 属性为 H3C 自定义 RADIUS 属性，携带在 RADIUS 服务器发送给接入设备的认证响应或实时计费响应报文中，用于向接入设备通知在线用户的剩余流量值。设备管理员设置的 Remanent_Volume 属性流量单位应与 RADIUS 服务器上统计用户流量的单位保持一致，否则设备无法正确使用 Remanent_Volume 属性值对用户进行计费。

表1-29 配置 RADIUS Remanent_Volume 属性的流量单位

操作	命令	说明
进入系统视图	**system-view**	-
进入RADIUS方案视图	**radius scheme** *radius-scheme-name*	-
配置RADIUS Remanent_Volume属性的流量单位	**attribute remanent-volume unit** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** }	缺省情况下，Remanent_Volume属性的流量单位是千字节

16. 配置RADIUS Attribute 31 中的MAC地址格式

不同的 RADIUS 服务器对填充在 RADIUS Attribute 31 中的 MAC 地址有不同的格式要求，为了保证 RADIUS 报文的正常交互，设备发送给服务器的 RADIUS Attribute 31 号属性中 MAC 地址的格式必须与服务器的要求保持一致。

表1-30 配置 RADIUS Attribute 31 中的 MAC 地址格式

操作	命令	说明
进入系统视图	**system-view**	-
进入RADIUS方案视图	**radius scheme** *radius-scheme-name*	-
配置RADIUS Attribute 31中的MAC地址格式	**attribute 31 mac-format section** { **six** | **three** } **separator** *separator-character* { **lowercase** | **uppercase** }	缺省情况下，RADIUS Attribute 31中的MAC地址为大写字母格式，且被分隔符“-”分成6段，即为HH-HH-HH-HH-HH-HH的格式。

17. 配置RADIUS告警功能

开启相应的 RADIUS 告警功能后，RADIUS 模块会生成告警信息，用于报告该模块的重要事件：

- 当 NAS 向 RADIUS 服务器发送计费或认证请求没有收到响应时，会重传请求，当重传次数达到最大传送次数时仍然没有收到响应时，NAS 认为该服务器不可达，并发送表示 RADIUS 服务器不可达的告警信息。
- 当 **timer quiet** 定时器设定的时间到达后，NAS 将服务器的状态置为激活状态并发送表示 RADIUS 服务器可达的告警信息。
- 当 NAS 发现认证失败次数与认证请求总数的百分比超过阈值时，会发送表示认证失败次数超过阈值的告警信息。

生成的告警信息将发送到设备的 SNMP 模块，通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关属性。有关告警信息的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。

表1-31 配置 RADIUS 告警功能

操作	命令	说明
进入系统视图	**system-view**	-
开启RADIUS告警功能	**snmp-agent trap enable radius** [**accounting-server-down** | **authentication-error-threshold** | **authentication-server-down** | **accounting-server-up** | **authentication-server-up**] *	缺省情况下，所有类型的RADIUS 告警功能均处于关闭状态

18. RADIUS显示和维护

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

在用户视图下，执行 **reset** 命令可以清除相关统计信息。

表1-32 RADIUS 显示和维护

操作	命令
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**

操作	命令
清除RADIUS协议的统计信息	**reset radius statistics**

1.3.3 配置HWTACACS方案

1. HWTACACS配置任务简介

表1-33 HWTACACS 配置任务简介

配置任务	说明	详细配置
创建HWTACACS方案	必选	1.3.3 2.
配置HWTACACS认证服务器	必选	1.3.3 3.
配置HWTACACS授权服务器	可选	1.3.3 4.
配置HWTACACS计费服务器	可选	1.3.3 5.
配置HWTACACS报文的共享密钥	可选	1.3.3 6.
配置发送给HWTACACS服务器的用户名格式和数据统计单位	可选	1.3.3 7.
配置发送HWTACACS报文使用的源地址	可选	1.3.3 8.
配置HWTACACS服务器的定时器	可选	1.3.3 9.
HWTACACS显示和维护	可选	1.3.3 10.

2. 创建HWTACACS方案

在进行 HWTACACS 的其它相关配置之前，必须先创建 HWTACACS 方案并进入其视图。系统最多支持配置 16 个 HWTACACS 方案。一个 HWTACACS 方案可以同时被多个 ISP 域引用。

表1-34 创建 HWTACACS 方案

操作	命令	说明
进入系统视图	**system-view**	-
创建HWTACACS方案并进入其视图	**hwtacacs scheme** *hwtacacs-scheme-name*	缺省情况下，不存在HWTACACS方案

3. 配置HWTACACS认证服务器

通过在 HWTACACS 方案中配置 HWTACACS 认证服务器，指定设备对用户进行 HWTACACS 认证时与哪个服务器进行通信。

一个 HWTACACS 方案中最多允许配置一个主认证服务器和 16 个从认证服务器。当主服务器不可达时，设备根据从服务器的配置顺序由先到后查找状态为 **active** 的从服务器并与之交互。建议在不需要备份的情况下，只配置主 HWTACACS 认证服务器即可。

在实际组网环境中，可以指定一台服务器既作为某个 HWTACACS 方案的主认证服务器，又作为另一个 HWTACACS 方案的从认证服务器。

表1-35 配置 HWTACACS 认证服务器

操作	命令	说明
进入系统视图	**system-view**	-
进入HWTACACS方案视图	**hwtacacs scheme** *hwtacacs-scheme-name*	-
配置主HWTACACS认证服务器	**primary authentication** { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection**] *	二者至少选其一 缺省情况下，未配置主/从认证服务器 在同一个方案中指定的主认证服务器和从认证服务器的IP地址、端口号不能完全相同，并且各从认证服务器的IP地址、端口号也不能完全相同
配置从HWTACACS认证服务器	**secondary authentication** { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection**] *	

4. 配置HWTACACS授权服务器

通过在 HWTACACS 方案中配置 HWTACACS 授权服务器，指定设备对用户进行 HWTACACS 授权时与哪个服务器进行通信。

一个 HWTACACS 方案中最多允许配置一个主授权服务器和 16 个从授权服务器。当主服务器不可达时，设备根据从服务器的配置顺序由先到后查找状态为 **active** 的从服务器并与之交互。建议在不需要备份的情况下，只配置主 HWTACACS 授权服务器即可。

在实际组网环境中，可以指定一台服务器既作为某个 HWTACACS 方案的主授权服务器，又作为另一个 HWTACACS 方案的从授权服务器。

表1-36 配置 HWTACACS 授权服务器

操作	命令	说明
进入系统视图	**system-view**	-
进入HWTACACS方案视图	**hwtacacs scheme** *hwtacacs-scheme-name*	-
设置主HWTACACS授权服务器	**primary authorization** { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection**] *	二者至少选其一 缺省情况下，未配置主/从授权服务器 在同一个方案中指定的主授权服务器和从授权服务器的IP地址、端口号不能完全相同，并且各从授权服务器的IP地址、端口号也不能完全相同
设置从HWTACACS授权服务器	**secondary authorization** { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection**] *	

5. 配置HWTACACS计费服务器

通过在 HWTACACS 方案中配置 HWTACACS 计费服务器，指定设备对用户进行 HWTACACS 计费时与哪个服务器进行通信。

一个 HWTACACS 方案中最多允许配置一个主计费服务器和 16 个从计费服务器。当主服务器不可达时，设备根据从服务器的配置顺序由先到后查找状态为 **active** 的从服务器并与之交互。建议在不需要备份的情况下，只配置主 HWTACACS 计费服务器即可。

在实际组网环境中，可以指定一台服务器既作为某个 HWTACACS 方案的主计费服务器，又作为另一个 HWTACACS 方案的从计费服务器。

目前 HWTACACS 不支持对 FTP/SFTP/SCP 用户进行计费。

表1-37 配置 HWTACACS 计费服务器

操作	命令	说明
进入系统视图	**system-view**	-
进入HWTACACS方案视图	**hwtacacs scheme** *hwtacacs-scheme-name*	-
设置HWTACACS主计费服务器	**primary accounting** { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection**] *	二者至少选其一 缺省情况下，未配置主/从计费服务器 在同一个方案中指定的主计费服务器和从计费服务器的IP地址、端口号不能完全相同，并且各从计费服务器的IP地址、端口号也不能完全相同
设置HWTACACS从计费服务器	**secondary accounting** { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection**] *	

6. 配置HWTACACS报文的共享密钥

HWTACACS 客户端与 HWTACACS 服务器使用 MD5 算法并在共享密钥的参与下加密 HWTACACS 报文。只有在密钥一致的情况下，彼此才能接收对方发来的报文并作出响应。

由于设备优先采用配置 HWTACACS 认证/授权/计费服务器时指定的报文共享密钥，因此，本配置中指定的 HWTACACS 报文共享密钥仅在配置 HWTACACS 认证/授权/计费服务器时未指定相应密钥的情况下使用。

表1-38 配置 HWTACACS 报文的共享密钥

操作	命令	说明
进入系统视图	**system-view**	-
进入HWTACACS方案视图	**hwtacacs scheme** *hwtacacs-scheme-name*	-
配置HWTACACS认证、授权、计费报文的共享密钥	**key** { **accounting** | **authentication** | **authorization** } { **cipher** | **simple** } *string*	缺省情况下，未设置HWTACACS报文的共享密钥 必须保证设备上设置的共享密钥与HWTACACS服务器上的完全一致

7. 配置发送给HWTACACS服务器的用户名格式和数据统计单位

接入用户通常以“*userid@isp-name*”的格式命名，“@”后面的部分为 ISP 域名，设备通过该域名决定将用户归于哪个 ISP 域的。由于有些 HWTACACS 服务器不能接受携带有 ISP 域名的用户名，因此就需要设备首先将用户名中携带的 ISP 域名去除后再传送给该类 HWTACACS 服务器。通过设置发送给 HWTACACS 服务器的用户名格式，就可以选择发送 HWTACACS 服务器的用户名中是否要携带 ISP 域名。

设备通过发送计费报文，向HWTACACS服务器报告在线用户的数据流量统计值，该值的单位可配，为保证 HWTACACS 服务器计费的准确性，设备上设置的发送给 HWTACACS 服务器的数据流或者数据包的单位应与 HWTACACS 服务器上的流量统计单位保持一致。

需要注意的是，如果要在两个乃至两个以上的 ISP 域中引用相同的 HWTACACS 方案，建议设置该 HWTACACS 方案允许用户名中携带 ISP 域名，使得 HWTACACS 服务器端可以根据 ISP 域名来区分不同的用户。

表1-39 配置发送给 HWTACACS 服务器的用户名格式和数据统计单位

操作	命令	说明
进入系统视图	**system-view**	-
进入HWTACACS方案视图	**hwtacacs scheme** *hwtacacs-scheme-name*	-
设置发送给HWTACACS服务器的用户名格式	**user-name-format { keep-original | with-domain | without-domain }**	缺省情况下，发送给HWTACACS服务器的用户名携带ISP域名
设置发送给HWTACACS服务器的数据流或者数据包的单位	**data-flow-format { data { byte | giga-byte | kilo-byte | mega-byte } | packet { giga-packet | kilo-packet | mega-packet | one-packet } } ***	可选 缺省情况下，数据流的单位为字节，数据包的单位为包

8. 配置发送HWTACACS报文使用的源地址

HWTACACS 服务器上通过 IP 地址来标识接入设备，并根据收到的 HWTACACS 报文的源 IP 地址是否与服务器所管理的接入设备的 IP 地址匹配，来决定是否处理来自该接入设备的认证、授权或计费请求。若 HWTACACS 服务器收到的 HWTACACS 认证或计费报文的源地址在所管理的接入设备 IP 地址范围内，则会进行后续的认证或计费处理，否则直接丢弃该报文。因此，为保证认证、授权和计费报文可被服务器正常接收并处理，接入设备上发送 HWTACACS 报文使用的源地址必须与 HWTACACS 服务器上指定的接入设备的 IP 地址保持一致。

通常，该地址为接入设备上与 HWTACACS 服务器路由可达的接口 IP 地址。

设备发送 HWTACACS 报文时，根据以下顺序查找使用的源地址：

- 若当前所使用的 HWTACACS 方案中配置了发送 HWTACACS 报文使用源地址，则使用该地址。
- 否则，根据当前使用的服务器所属的 VPN 查找系统视图下通过 **hwtacacs nas-ip** 命令配置的私网源地址，对于公网服务器则直接查找该命令配置的公网源地址。
- 若系统视图下没有配置相应的源地址，则使用通过路由查找到的报文出接口地址。

此配置可以在系统视图和 HWTACACS 方案视图下进行，系统视图下的配置将对所有 HWTACACS 方案生效，HWTACACS 方案视图下的配置仅对本方案有效，并且具有高于前者的优先级。

表1-40 为所有 HWTACACS 方案配置发送 HWTACACS 报文使用的源地址

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
设置设备发送HWTACACS报文使用的源地址	**hwtacacs nas-ip** { *ipv4-address* | **ipv6** *ipv6-address* }	缺省情况下，未设置发送HWTACACS报文使用的源地址，设备将以发送报文的接口地址作为源地址

表1-41 为 HWTACACS 方案配置发送 HWTACACS 报文使用的源地址

操作	命令	说明
进入系统视图	**system-view**	-
进入HWTACACS方案视图	**hwtacacs scheme** *hwtacacs-scheme-name*	-
设置设备发送HWTACACS报文使用的源地址	**nas-ip** { *ipv4-address* | **ipv6** *ipv6-address* }	缺省情况下，使用系统视图下由命令**hwtacacs nas-ip**指定的源地址，若系统视图下未指定源地址，则使用发送HWTACACS报文的接口地址

9. 配置HWTACACS服务器的定时器

在与 HWTACACS 服务器交互的过程中，设备上可启动的定时器包括以下几种：

- 服务器响应超时定时器（**response-timeout**）：如果在 HWTACACS 请求报文传送出去一段时间后，设备还没有得到 HWTACACS 服务器的响应，则会将该服务器的状态置为 **block**，并向下一个 HWTACACS 服务器发起请求，以保证用户尽可能得到 HWTACACS 服务，这段时间被称为 HWTACACS 服务器响应超时时长。
- 实时计费间隔定时器（**realtime-accounting**）：为了对用户实施实时计费，有必要定期向服务器发送用户的实时计费信息，通过设置实时计费的时间间隔，设备会每隔设定的时间向 HWTACACS 服务器发送一次在线用户的计费信息。
- 服务器恢复激活状态定时器（**quiet**）：当服务器不可达时，设备将该服务器的状态置为 **block**，并开启超时定时器，在设定的一定时间间隔之后，再将该服务器的状态恢复为 **active**。这段时间被称为服务器恢复激活状态时长。

关于 HWTACACS 服务器的状态：

HWTACACS 方案中各服务器的状态（**active**、**block**）决定了设备向哪个服务器发送请求报文，以及设备在与当前服务器通信中断的情况下，如何转而与另外一个服务器进行交互。在实际组网环境中，可指定一个主 HWTACACS 服务器和多个从 HWTACACS 服务器，由从服务器作为主服务器的备份。通常情况下，设备上主从服务器的切换遵从以下原则：

- 当主服务器状态为 **active** 时，设备首先尝试与主服务器通信，若主服务器不可达，设备更改主服务器的状态为 **block**，并启动该服务器的 **quiet** 定时器，然后按照从服务器的配置先后顺序依次查找状态为 **active** 的从服务器进行认证或者计费。如果状态为 **active** 的从服务器也不可达，则将该从服务器的状态置为 **block**，同时启动该服务器的 **quiet** 定时器，并继续查找状态为 **active** 的从服务器。当服务器的 **quiet** 定时器超时，该服务器将恢复为 **active** 状态。在一次认证或计费过程中，如果设备在尝试与从服务器通信时，之前已经查找过的服务器状态由 **block** 恢复为 **active**，则设备并不会立即恢复与该服务器的通信，而是继续查找从服务器。如果所有已配置的服务器都不可达，则认为本次认证或计费失败。

- 如果在认证或计费过程中删除了当前正在使用的服务器，则设备在与该服务器通信超时后，将会立即从主服务器开始依次查找状态为 **active** 的服务器并与之进行通信。
- 当主/从服务器的状态均为 **block** 时，设备尝试与主服务器进行通信，若未配置主服务器，则设备尝试与首个配置的从服务器通信。
- 只要存在状态为 **active** 的服务器，设备就仅与状态为 **active** 的服务器通信，即使该服务器不可达，设备也不会尝试与状态为 **block** 的服务器通信。
- 一旦服务器状态满足自动切换的条件，则所有 HWTACACS 方案视图下该服务器的状态都会相应地变化。

需要注意的是，实时计费间隔的取值对设备和 HWTACACS 服务器的性能有一定的相关性要求，取值越小，对设备和 HWTACACS 服务器的性能要求越高。建议当用户量比较大（大于等于 1000）时，尽量把该间隔的值设置得大一些。

表1-42 配置 HWTACACS 服务器的定时器

操作	命令	说明
进入系统视图	**system-view**	-
进入HWTACACS方案视图	**hwtacacs scheme** *hwtacacs-scheme-name*	-
设置HWTACACS服务器响应超时时间	**timer response-timeout** *seconds*	缺省情况下，服务器响应超时时间为5秒
设置实时计费的时间间隔	**timer realtime-accounting** *minutes*	缺省情况下，实时计费间隔为12分钟
设置服务器恢复激活状态的时间	**timer quiet** *minutes*	缺省情况下，服务器恢复激活状态前需要等待5分钟

10. HWTACACS显示和维护

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

在用户视图下，执行 **reset** 命令可以清除相关统计信息。

表1-43 HWTACACS 显示和维护

操作	命令
查看所有或指定HWTACACS方案的配置信息或统计信息	**display hwtacacs scheme** [*hwtacacs-server-name* [**statistics**]]
清除HWTACACS协议的统计信息	**reset hwtacacs statistics** { **accounting** | **all** | **authentication** | **authorization** }

1.3.4 配置LDAP方案

1. LDAP配置任务简介

表1-44 LDAP 配置任务简介

配置任务		说明	详细配置
配置LDAP服务器	创建LDAP服务器	必选	1.3.4 2.
	配置LDAP服务器IP地址	必选	1.3.4 3.
	配置LDAP版本号	可选	1.3.4 4.
	配置LDAP服务器的连接超时时间	可选	1.3.4 5.
	配置具有管理员权限的用户属性	必选	1.3.4 6.
	配置LDAP用户属性参数	必选	1.3.4 7.
配置LDAP属性映射表		可选	1.3.4 8.
创建LDAP方案		必选	1.3.4 9.
指定LDAP认证服务器		必选	1.3.4 10.
指定LDAP授权服务器		可选	1.3.4 11.
引用LDAP属性映射表		可选	1.3.4 12.
LDAP显示和维护		可选	1.3.4 13.

2. 创建LDAP服务器

表1-45 创建 LDAP 服务器

操作	命令	说明
进入系统视图	**system-view**	-
创建LDAP服务器并进入LDAP服务器视图	**ldap server** *server-name*	缺省情况下，不存在LDAP服务器

3. 配置LDAP服务器IP地址

表1-46 配置 LDAP 服务器 IP 地址

操作	命令	说明
进入系统视图	**system-view**	-
进入LDAP服务器视图	**ldap server** *server-name*	-
配置LDAP服务器IP地址	{ **ip** *ip-address* | **ipv6** *ipv6-address* } [**port** *port-number*]	缺省情况下，未配置LDAP服务器IP地址 LDAP服务器视图下仅能同时存在一个IPv4地址类型的LDAP服务器或一个IPv6地址类型的LDAP服务器。多次配置，后配置的生效

4. 配置LDAP版本号

配置 LDAP 认证中所支持的 LDAP 协议的版本号，目前设备支持 LDAPv2 和 LDAPv3 两个协议版本。设备上配置的 LDAP 版本号需要与服务器支持的版本号保持一致。

表1-47 配置 LDAP 版本号

操作	命令	说明
进入系统视图	**system-view**	-
进入LDAP服务器视图	**ldap server** *server-name*	-
配置LDAP版本号	**protocol-version** { **v2** | **v3** }	缺省情况下，LDAP版本号为LDAPv3 Microsoft的LDAP服务器只支持LDAPv3版本

5. 配置LDAP服务器的连接超时时间

设备向 LDAP 服务器发送绑定请求、查询请求，如果经过指定的时间后未收到 LDAP 服务器的回应，则认为本次认证、授权请求超时。若使用的 ISP 域中配置了备份的认证、授权方案，则设备会继续尝试进行其他方式的认证、授权处理，否则本次认证、授权失败。

表1-48 配置 LDAP 服务器的连接超时时间

操作	命令	说明
进入系统视图	**system-view**	-
进入LDAP服务器视图	**ldap server** *server-name*	-
配置LDAP服务器的连接超时时间	**server-timeout** *time-interval*	缺省情况下，LDAP服务器的连接超时时间为10秒

6. 配置具有管理员权限的用户属性

配置 LDAP 认证过程中绑定服务器所使用的用户 DN 和用户密码，该用户具有管理员权限。

表1-49 配置具有管理员权限的用户属性

操作	命令	说明
进入系统视图	**system-view**	-
进入LDAP服务器视图	**ldap server** *server-name*	-
配置具有管理员权限的用户DN	**login-dn** *dn-string*	缺省情况下，未配置具有管理员权限的用户DN 配置的管理员权限的用户DN必须与LDAP服务器上管理员的DN一致
配置具有管理员权限的用户密码	**login-password** { **ciper** | **simple** } *password*	缺省情况下，未配置具有管理权限的用户密码

7. 配置LDAP用户属性参数

要对用户进行身份认证，就需要以用户 DN 及密码为参数与 LDAP 服务器进行绑定，因此需要首先从 LDAP 服务器获取用户 DN。LDAP 提供了一套 DN 查询机制，在与 LDAP 服务器建立连接的基础上，按照一定的查询策略向服务器发送查询请求。该查询策略由设备上指定的 LDAP 用户属性定义，具体包括以下几项：

- 用户 DN 查询的起始节点（search-base-dn）
- 用户 DN 查询的范围（search-scope）
- 用户名称属性（user-name-attribute）
- 用户名称格式（user-name-format）
- 用户对象类型（user-object-class）

LDAP 服务器上的目录结构可能具有很深的层次，如果从根目录进行用户 DN 的查找，耗费的时间将会较长，因此必须配置用户查找的起始点 DN，以提高查找效率。

表1-50 配置 LDAP 用户属性参数

操作	命令	说明
进入系统视图	**system-view**	-
进入LDAP服务器视图	**ldap server** *server-name*	-
配置用户查询的起始DN	**search-base-dn** *base-dn*	缺省情况下，未指定用户查询的起始DN
（可选）配置用户查询的范围	**search-scope** { **all-level** | **single-level** }	缺省情况下，用户查询的范围为**all-level**
（可选）配置用户查询的用户名属性	**user-parameters user-name-attribute** { *name-attribute* | **cn** | **uid** }	缺省情况下，用户查询的用户名属性为**cn**
（可选）配置用户查询的用户名格式	**user-parameters user-name-format** { **with-domain** | **without-domain** }	缺省情况下，用户查询的用户名格式为**without-domain**
（可选）配置用户查询的自定义用户对象类型	**user-parameters user-object-class** *object-class-name*	缺省情况下，未指定自定义用户对象类型，根据使用的LDAP服务器的类型使用各服务器缺省的用户对象类型

8. 配置LDAP属性映射表

在用户的 LDAP 授权过程中，设备会通过查询操作得到用户的授权信息，该授权信息由 LDAP 服务器通过若干 LDAP 属性下发给设备。若设备从 LDAP 服务器查询得到某 LDAP 属性，则该属性只有在被设备的 AAA 模块解析之后才能实际生效。如果某 LDAP 服务器下发给用户的属性不能被 AAA 模块解析，则该属性将被忽略。因此，需要通过配置 LDAP 属性映射表来指定要获取哪些 LDAP 属性，以及 LDAP 服务器下发的这些属性将被 AAA 模块解析为什么类型的 AAA 属性，具体映射为哪种类型的 AAA 属性由实际应用需求决定。

每一个 LDAP 属性映射表项定义了一个 LDAP 属性与一个 AAA 属性的对应关系。将一个 LDAP 属性表在指定的 LDAP 方案视图中引用后，该映射关系将在 LDAP 授权过程中生效。

表1-51 配置 LDAP 属性映射表

操作	命令	说明
进入系统视图	**system-view**	-
创建LDAP的属性映射表，并进入属性映射表视图	**ldap attribute-map** *map-name*	缺省情况下，不存在LDAP属性映射表
配置LDAP属性映射表项	**map ldap-attribute** *ldap-attribute-name* [**prefix** *prefix-value* **delimiter** *delimiter-value*] **aaa-attribute** { **user-group** | **user-profile** }	缺省情况下，不存在LDAP属性映射关系

9. 创建LDAP方案

系统最多支持配置 16 个 LDAP 方案。一个 LDAP 方案可以同时被多个 ISP 域引用。

表1-52 创建 LDAP 方案

操作	命令	说明
进入系统视图	**system-view**	-
创建LDAP方案并进入其视图	**ldap scheme** *ldap-scheme-name*	缺省情况下，不存在LDAP方案

10. 指定LDAP认证服务器

表1-53 指定 LDAP 认证服务器

操作	命令	说明
进入系统视图	**system-view**	-
进入LDAP方案视图	**ldap scheme** *ldap-scheme-name*	-
指定LDAP认证服务器	**authentication-server** *server-name*	缺省情况下，未指定LDAP认证服务器

11. 指定LDAP授权服务器

表1-54 指定 LDAP 授权服务器

操作	命令	说明
进入系统视图	**system-view**	-
进入LDAP方案视图	**ldap scheme** *ldap-scheme-name*	-
指定LDAP授权服务器	**authorization-server** *server-name*	缺省情况下，未指定LDAP认证服务器

12. 引用LDAP属性映射表

在使用 LDAP 授权方案的情况下，可以通过在 LDAP 方案中引用 LDAP 属性映射表，将 LDAP 授权服务器下发给用户的 LDAP 属性映射为 AAA 模块可以解析的某类属性。

一个 LDAP 方案视图中只能引用一个 LDAP 属性映射表，后配置的生效。

表1-55 引用 LDAP 属性映射表

操作	命令	说明
进入系统视图	**system-view**	-
进入LDAP方案视图	**ldap scheme** *ldap-scheme-name*	-
引用LDAP属性映射表	**attribute-map** *map-name*	缺省情况下，未引用任何LDAP属性映射表

13. LDAP显示和维护

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

表1-56 LDAP 显示和维护

操作	命令
查看所有或指定LDAP方案的配置信息	**display ldap scheme** [*ldap-scheme-name*]

1.4 在ISP域中配置实现AAA的方法

通过在 ISP 域视图下引用预先配置的认证、授权、计费方案来实现对用户的认证、授权和计费。如果用户所属的 ISP 域下未应用任何认证、授权、计费方法，系统将使用缺省的认证、授权、计费方法，分别为本地认证、本地授权和本地计费。

1.4.1 配置准备

- 若采用本地认证方案，则请先完成本地用户的配置。有关本地用户的配置请参见“1.3.1 配置本地用户”。
- 若采用远端认证、授权或计费方案，则请提前创建RADIUS方案、HWTACACS方案或LDAP方案。有关RADIUS方案的配置请参见“1.3.2 配置RADIUS方案”。有关HWTACACS方案的配置请参见“1.3.3 配置HWTACACS方案”。有关LDAP方案的配置请参见“1.3.4 配置LDAP方案”。

1.4.2 创建ISP域

在多 ISP 的应用环境中，不同 ISP 域的用户有可能接入同一台设备。而且各 ISP 用户的用户属性（例如用户名及密码构成、服务类型/权限等）有可能不相同，因此有必要通过设置 ISP 域把它们区分开，并为每个 ISP 域单独配置一套 AAA 方法及 ISP 域的相关属性。

对于设备来说，每个接入用户都属于一个 ISP 域。系统中最多可以配置 16 个 ISP 域，包括一个系统缺省存在的名称为 system 的 ISP 域。如果某个用户在登录时没有提供 ISP 域名，系统将把它归于缺省的 ISP 域。系统缺省的 ISP 域可以手工修改为一个指定的 ISP 域。

用户认证时，设备将按照如下先后顺序为其选择认证域：接入模块指定的认证域-->用户名中指定的 ISP 域-->系统缺省的 ISP 域。其中，仅部分接入模块支持指定认证域，例如 802.1X、Portal、MAC

地址认证。如果根据以上原则决定的认证域在设备上不存在，但设备上为未知域名的用户指定了 ISP 域，则最终使用该指定的 ISP 域认证，否则，用户将无法认证。

需要注意的是：

- 一个 ISP 域被配置为缺省的 ISP 域后，将不能够被删除，必须首先使用命令 **undo domain default enable** 将其修改为非缺省 ISP 域，然后才可以被删除。
- 系统缺省存在的 system 域只能被修改，不能被删除。

表1-57 创建 ISP 域

操作	命令	说明
进入系统视图	**system-view**	-
创建ISP域并进入其视图	**domain** *isp-name*	缺省情况下，存在一个ISP域，名称为system
返回系统视图	**quit**	-
（可选）手工配置缺省的ISP域	**domain default enable** *isp-name*	缺省情况下，系统缺省的ISP域为system
（可选）配置未知域名的用户的ISP域	**domain if-unknown** *isp-domain-name*	缺省情况下，没有为未知域名的用户指定ISP域

1.4.3 配置ISP域的属性

一个 ISP 域中可配置以下属性，这些属性对于接入该域的所有用户均生效：

- ISP 域的状态：通过域的状态（active、block）控制是否允许该域中的用户请求网络服务。
- ISP 域的用户授权属性：用户认证成功之后，对于 ACL、IP 地址池、IPv6 地址前缀、IPv6 地址池、DNS 服务器、强制 URL、可同时点播的节目最大数、User Profile、User Group 授权属性，用户优先采用服务器下发的属性值，其次采用 ISP 域下配置的属性值；对于用户闲置切断授权属性，用户优先采用 ISP 域下配置的属性值，其次采用服务器下发的属性值。
  - 授权 ACL：用户认证成功后，将仅被授权访问匹配指定 ACL 的网络资源。对于 Portal 用户，若在认证之前被授权了认证域，则将被授权访问指定的 ACL。
  - 用户闲置切断时间：用户上线后，设备会周期性检测用户的流量，若 ISP 域内某用户在指定的闲置检测时间内产生的流量小于指定的数据流量，则会被强制下线。
  - IP 地址池：认证成功的 PPP 用户可以从指定的地址池中分配得到一个 IP 地址。
  - 授权 User Profile：用户认证成功后，其访问行为将受到该 User Profile 中预设配置的限制。对于 Portal 用户，若在认证之前被授权了认证域，则其访问行为将受到该域中的 User Profile 配置的限制。
  - 授权会话超时时间：如果用户在线时长超过该值，设备会强制该用户下线。
  - 授权 IPv6 地址前缀：认证成功的 PPP 用户使用该前缀作为自己的 IPv6 地址前缀。
  - IPv6 地址池：认证成功的 PPP 用户可以从指定的地址池中分配得到一个 IPv6 地址。
  - DNS 服务器地址：认证成功的 PPP 用户使用该 DNS 服务器提供的 DNS 服务。
  - 强制 URL：PPP 用户认证成功后，此 URL 将被推送至 PPP 客户端。
  - 授权用户组：用户认证成功后，将继承该用户组中的所有属性。

- 点播的最大节目数：PPP 用户认证成功后，用户可以同时点播的最大节目数受此限制。

- 设备上传到服务器的用户在线时间中保留闲置切断时间：当用户异常下线时，上传到服务器上的用户在线时间中包含了一定的闲置切断检测间隔或用户在线探测间隔（该在线探测机制目前仅 Portal 认证支持），此时服务器上记录的用户时长将大于用户实际在线时长。
- 用户采用的 ITA 业务策略，用于实现根据用户访问的不同目的地址进行不同级别的流量计费。用户优先采用 AAA 服务器下发的 ITA 业务策略，其次采用 ISP 域下配置的 ITA 业务策略。
- 用户主业务依赖的 IP 地址类型.：如果 PPPoE 用户主业务依赖的 IP 地址分配失败，则不允许该用户上线。
- 用户等待 DHCPv6 分配 IPv6 地址的最大时长：PPPoE 用户与设备完成 IPv6CP 协商之后，设备等待 DHCPv6 为用户分配 IP 地址的时长。

表1-58 配置 ISP 域的属性

操作	命令	说明
进入系统视图	**system-view**	-
进入ISP域视图	**domain** *isp-name*	-
设置ISP域的状态	**state** { **active** | **block** }	缺省情况下，当前ISP域处于活动状态，即允许任何属于该域的用户请求网络服务
设置当前ISP域下的用户授权属性	**authorization-attribute** { **acl** *acl-number* | **idle-cut** *minute* [*flow*] | **igmp max-access-number** *number* | **ip-pool** *pool-name* | **ipv6-pool** *ipv6-pool-name* | **ipv6-prefix** *ipv6-prefix prefix-length* | **mld max-access-number** *number* | { **primary-dns** | **secondary-dns** } { **ip** *ip-address* | **ipv6** *ipv6-address* } | **session-timeout** *minutes* | **url** *url-string* | **user-group** *user-group-name* **| user-profile** *profile-name* }	缺省情况下，未对当前ISP域下的用户设置任何授权属性，其中用户闲置切换功能处于关闭状态
设置设备上传到服务器的用户在线时间中保留闲置切断时间	**session-time include-idle-time**	缺省情况下，设备上传到服务器的用户在线时间中扣除闲置切断时间
设置当前ISP域下的用户地址类型	**user-address-type** { **ds-lite** | **ipv6** | **nat64** | **public-ds** | **public-ipv4 | private-ipv4** | **private-ds** | **private-ipv4** }	缺省情况下，未配置用户地址类型
设置当前ISP域的业务类型	**service-type** { **hsi** | **stb** | **voip** }	缺省情况下，当前ISP域的业务类型为**hsi**
设置当前ISP域采用的ITA业务策略	**ita-policy** *policy-name*	缺省情况下，当前ISP域中未采用ITA业务策略
设置PPPoE用户主业务依赖的IP地址类型	**basic-service-ip-type** { **ipv4** | **ipv6** | **ipv6-pd** } *	缺省情况下，PPPoE用户主业务不依赖于任何IP地址类型
设置PPPoE用户等待DHCPv6分配IPv6地址的最大时长	**dhcpv6-follow-ipv6cp time-out** *delay-time*	缺省情况下，PPPoE接入用户等待DHCPv6分配IPv6地址的最大时长为60秒

1.4.4 配置ISP域的AAA认证方法

配置 ISP 域的 AAA 认证方法时，需要注意的是：

- 当选择了 RADIUS 协议的认证方案以及非 RADIUS 协议的授权方案时，AAA 只接受 RADIUS 服务器的认证结果，RADIUS 授权的信息虽然在认证成功回应的报文中携带，但在认证回应的处理流程中不会被处理。
- 当使用 HWTACACS 方案进行用户角色切换认证时，系统使用用户输入的用户角色切换用户名进行角色切换认证；当使用 RADIUS 方案进行用户角色切换认证时，系统使用 RADIUS 服务器上配置的“$enab*n*$”形式的用户名进行用户角色切换认证，其中 *n* 为用户希望切换到的用户角色 level-*n* 中的 *n*。

配置前的准备工作：

(1) 确定要配置的接入方式或者服务类型。AAA 可以对不同的接入方式和服务类型配置不同的认证方案。

(2) 确定是否为所有的接入方式或服务类型配置缺省的认证方法，缺省的认证方法对所有接入用户都起作用，但其优先级低于为具体接入方式或服务类型配置的认证方法。

表1-59 配置 ISP 域的 AAA 认证方法

操作	命令	说明
进入系统视图	**system-view**	-
进入ISP域视图	**domain** *isp-name*	-
为当前ISP域配置缺省的认证方法	**authentication default** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **ldap-scheme** *ldap-scheme-name* [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }	缺省情况下，当前ISP域的缺省认证方法为**local**
为IKE扩展认证配置认证方法	**authentication ike** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	缺省情况下，IKE扩展认证采用缺省的认证方法
为lan-access用户配置认证方法	**authentication lan-access** { **ldap-scheme** *ldap-scheme-name* [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	缺省情况下，lan-access用户采用缺省的认证方法
为login用户配置认证方法	**authentication login** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **ldap-scheme** *ldap-scheme-name* [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }	缺省情况下，login用户采用缺省的认证方法
为Portal用户配置认证方法	**authentication portal** { **ldap-scheme** *ldap-scheme-name* [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	缺省情况下，Portal用户采用缺省的认证方法
为PPP用户配置认证方法	**authentication ppp** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	缺省情况下，PPP用户采用缺省的认证方法

操作	命令	说明
配置用户角色切换认证方法	**authentication super** { **hwtacacs-scheme** *hwtacacs-scheme-name* | **radius-scheme** *radius-scheme-name* } *	缺省情况下，用户角色切换认证采用缺省的认证方法

1.4.5 配置ISP域的AAA授权方法

配置 ISP 域的 AAA 授权方法时，需要注意的是：

- 目前设备暂不支持使用 LDAP 进行授权。
- 在一个 ISP 域中，只有 RADIUS 授权方法和 RADIUS 认证方法引用了相同的 RADIUS 方案，RADIUS 授权才能生效。若 RADIUS 授权未生效或者 RADIUS 授权失败，则用户认证会失败。

配置前的准备工作：

(1) 确定要配置的接入方式或者服务类型，AAA 可以按照不同的接入方式和服务类型进行 AAA 授权的配置。

(2) 确定是否为所有的接入方式或服务类型配置缺省的授权方法，缺省的授权方法对所有接入用户都起作用，但其优先级低于为具体接入方式或服务类型配置的授权方法。

表1-60 配置 ISP 域的 AAA 授权方法

操作	命令	说明
进入系统视图	**system-view**	-
进入ISP域视图	**domain** *isp-name*	-
为当前ISP域配置缺省的授权方法	**authorization default** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }	缺省情况下，当前ISP域的缺省授权方法为**local**
配置命令行授权方法	**authorization command** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local** [**none**] | **local** [**none**] | **none** }	缺省情况下，命令行授权采用缺省的授权方法
为IKE扩展认证配置授权方法	**authorization ike** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	缺省情况下，IKE扩展认证采用缺省的授权方法
为lan-access用户配置授权方法	**authorization lan-access** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	缺省情况下，lan-access用户采用缺省的授权方法
为login用户配置授权方法	**authorization login** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }	缺省情况下，login用户采用缺省的授权方法
为Portal用户配置授权方法	**authorization portal** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	缺省情况下，Portal用户采用缺省的授权方法

操作	命令	说明
为PPP用户配置授权方法	**authorization ppp** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	缺省情况下，PPP用户采用缺省的授权方法

1.4.6 配置ISP域的AAA计费方法

配置 ISP 域的 AAA 认证方法时，需要注意的是：

- 不支持对 FTP 类型 login 用户进行计费。
- 本地计费仅用于配合本地用户视图下的 **access-limit** 命令来实现对本地用户连接数的限制功能。

配置前的准备工作：

(1) 确定要配置的接入方式或者服务类型，AAA 可以按照不同的接入方式和服务类型进行 AAA 计费的配置。

(2) 确定是否为所有的接入方式或服务类型配置缺省的计费方法，缺省的计费方法对所有接入用户都起作用，但其优先级低于为具体接入方式或服务类型配置的计费方法。

表1-61 配置 ISP 域的 AAA 计费方法

操作	命令	说明
进入系统视图	**system-view**	-
进入ISP域视图	**domain** *isp-name*	-
为当前ISP域配置缺省的计费方法	**accounting default** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }	缺省情况下，当前ISP域的缺省计费方法为**local**
配置命令行计费方法	**accounting command hwtacacs-scheme** *hwtacacs-scheme-name*	缺省情况下，命令行计费采用缺省的计费方法
为lan-access用户配置计费方法	**accounting lan-access** { **broadcast** **radius-scheme** *radius-scheme-name1* **radius-scheme** *radius-scheme-name2* [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	缺省情况下，lan-access用户采用缺省的计费方法
为login用户配置计费方法	**accounting login** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }	缺省情况下，login用户采用缺省的计费方法
为Portal用户配置授权方法	**accounting portal** { **broadcast** **radius-scheme** *radius-scheme-name1* **radius-scheme** *radius-scheme-name2* [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	缺省情况下，Portal用户采用缺省的计费方法

操作	命令	说明
为PPP用户配置计费方法	**accounting ppp** { **broadcast** **radius-scheme** *radius-scheme-name1* **radius-scheme** *radius-scheme-name2* [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	缺省情况下，PPP用户采用缺省的计费方法
配置用户计费开始失败策略	**accounting start-fail** { **offline** | **online** }	缺省情况下，如果用户计费开始失败，则允许用户保持在线状态
配置用户计费更新失败策略	**accounting update-fail** { [**max-times** *times*] **offline** | **online** }	缺省情况下，如果用户计费更新失败，允许用户保持在线状态
用户计费流量配额耗尽策略	**accounting quota-out** { **offline** | **online** }	缺省情况下，用户的计费流量配额耗尽后将被强制下线

1.5 配置RADIUS session control功能

H3C 的 IMC RADIUS 服务器使用 session control 报文向设备发送授权信息的动态修改请求以及断开连接请求。开启 RADIUS session control 功能后，设备会打开知名 UDP 端口 1812 来监听并接收 RADIUS 服务器发送的 session control 报文。

当设备收到 session control 报文时，通过 session control 客户端配置验证 RADIUS session control 报文的合法性。

需要注意的是，该功能仅能和 H3C 的 IMC RADIUS 服务器配合使用。

表1-62 使能 RADIUS session control 服务

操作	命令	说明
进入系统视图	**system-view**	-
使能RADIUS session control功能	**radius session-control enable**	缺省情况下，RADIUS session control功能处于关闭状态
指定session control客户端	**radius session-control client** { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**key** { **cipher** | **simple** } *string*] *	缺省情况下，未指定session control客户端

1.6 配置RADIUS DAE服务器功能

DAE（Dynamic Authorization Extensions，动态授权扩展）协议是 RFC 5176 中定义的 RADIUS 协议的一个扩展，它用于强制认证用户下线，或者更改在线用户授权信息。DAE 采用客户端/服务器通信模式，由 DAE 客户端和 DAE 服务器组成。

- DAE 客户端：用于发起 DAE 请求，通常驻留在一个 RADIUS 服务器上，也可以为一个单独的实体。
- DAE 服务器：用于接收并响应 DAE 客户端的 DAE 请求，通常为一个 NAS（Network Access Server，网络接入服务器）设备。

DAE 报文包括以下两种类型：

- DMs（Disconnect Messages）：用于强制用户下线。DAE 客户端通过向 NAS 设备发送 DM 请求报文，请求 NAS 设备按照指定的匹配条件强制用户下线。
- COA（Change of Authorization）Messages：用于更改用户授权信息。DAE 客户端通过向 NAS 设备发送 COA 请求报文，请求 NAS 设备按照指定的匹配条件更改用户授权信息。

在设备上使能 RADIUS DAE 服务后，设备将作为 RADIUS DAE 服务器在指定的 UDP 端口监听指定的 RADIUS DAE 客户端发送的 DAE 请求消息，然后根据请求消息进行用户授权信息的修改或断开用户连接，并向 RADIUS DAE 客户端发送 DAE 应答消息。

表1-63 配置 RADIUS DAE 服务器

操作	命令	说明
进入系统视图	**system-view**	-
使能RADIUS DAE服务，并进入RADIUS DAE服务器视图	**radius dynamic-author server**	缺省情况下，RADIUS DAE服务处于关闭状态
指定RADIUS DAE客户端	**client** { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**key** { **cipher** | **simple** } *string*] *	缺省情况下，未指定RADIUS DAE客户端
指定RADIUS DAE服务端口	**port** *port-number*	缺省情况下，RADIUS DAE服务端口为3799

1.7 配置RADIUS报文的DSCP优先级

DSCP 携带在 IP 报文中的 ToS 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。通过本命令可以指定设备发送的 RADIUS 报文携带的 DSCP 优先级的取值。配置 DSCP 优先级的取值越大，RADIUS 报文的优先级越高。

表1-64 配置 RADIUS 报文的 DSCP 优先级

操作	命令	说明
进入系统视图	**system-view**	-
配置RADIUS报文的DSCP优先级	**radius** [**ipv6**] **dscp** *dscp-value*	缺省情况下，RADIUS报文的DSCP优先级为0

1.8 限制同时在线的最大用户连接数

通过配置同时在线的最大用户连接数，可以限制采用指定登录方式（FTP、SSH、Telnet 等）同时接入设备的在线用户数。

该配置对于通过任何一种认证方式（none、password 或者 scheme）接入设备的用户都生效。

表1-65 配置同时在线的最大用户连接数

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
配置同时在线的最大用户连接数	**aaa session-limit** { **ftp** | **http** | **https** | **ssh** | **telnet** } *max-sessions*	缺省情况下，最大用户连接数为32

1.9 配置本地BYOD授权

BYOD（Bring Your Own Device）指携带自己的设备办公，这些设备主要是指个人电脑、手机、平板电脑等终端设备。BYOD 解决方案可以为企业和用户提供基于用户身份信息、终端信息、接入场景的认证、授权服务。

本地 BYOD 授权是指，用户通过本地认证之后，设备通过匹配该用户的终端特征来给用户授予相关的网络访问权限。本地 BYOD 授权是通过用户组实现的。每一个本地用户都属于一个用户组，用户组中定义了基于终端类型的授权属性。用户在认证过程中，接入设备通过本地的 BYOD 终端类型识别规则来识别用户的终端类型，并根据识别出的终端类型为其授权相应的授权属性。

1.9.1 配置BYOD终端类型的识别规则

BYOD 终端类型的识别规则是用户终端特征与用户终端类型的一种映射关系。在用户认证的过程中，接入设备获取到用户终端的相关特征（例如 DHCP Option 55 指纹信息）后，可根据定义的识别规则识别出用户所使用的终端类型。

目前 BYOD 授权支持的用户终端特征包括：DHCP Option 55 指纹、HTTP User Agent 指纹和 MAC 地址指纹。

- DHCP Option55 指纹：DHCP 请求参数列表选项，终端利用该选项指明需要从服务器获取哪些网络配置参数。
- HTTP UserAgent 指纹：属于 HTTP 请求报文头域的一部分，用于携带终端访问 Web 页面时所使用的操作系统（包括版本号）、浏览器（包括版本号）等信息。
- MAC 地址指纹：终端的 MAC OUI 信息或终端所属的 MAC 地址范围。

每种特征只能对应一种终端类型，但一种终端类型可以对应多个同类特征。不同终端特征的识别优先级可以通过命令 **byod rule-order** 配置。

系统中已经预定义了一系列常用的 BYOD 终端类型识别规则，用户也可以根据实际组网需求通过命令行添加规则。

表1-66 配置 BYOD 终端类型的识别规则

操作	命令	说明
进入系统视图	**system-view**	-
配置BYOD终端类型的识别规则	**byod rule** { **dhcp-option** *option-string* | **http-user-agent** *agent-string* | **mac-address** *mac-address* **mask** *mac-mask* } **device-type** *type-name*	缺省情况下，不存在BYOD终端类型的识别规则
配置BYOD终端类型识别规则的类型和优先级	**byod rule-order** { **dhcp-option** | **http-user-agent** | **mac-address** } *	缺省情况下，设备采用三种终端类型识别规则，它们的优先级由高到低为：DHCP Option 55规则、HTTP User Agent规则、MAC地址规则

1.9.2 配置基于终端类型的授权属性

设备支持对网络接入类本地用户进行基于终端类型的 BYOD 授权。基于终端类型的授权属性在用户组视图下配置，且优先级高于用户组视图下的通用授权属性配置，以及本地用户视图下的授权属性配置。如果用户组中配置了基于终端类型的授权属性，则在用户认证过程中，设备将优先查找用户所属终端类型的授权属性配置并进行授权；如果用户组中没有该用户所属的终端类型对应的授权属性配置，则该用户将被授予用户组中的通用授权属性，或用户所属的本地用户视图下的授权属性。

表1-67 配置基于终端类型的授权属性

操作	命令	说明
进入系统视图	**system-view**	-
创建用户组，并进入用户组视图	**user-group** *group-name*	缺省情况下，存在一个名称为system的用户组
配置基于终端类型的授权属性	**byod authorization device-type** *type-name* { **acl** *acl-number* | **callback-number** *callback-number* | **idle-cut** *minute* | **ip-pool** *ipv4-pool-name* | **ipv6-pool** *ipv6-pool-name* | **ipv6-prefix** *ipv6-prefix prefix-length* | { **primary-dns** | **secondary-dns** } { **ip** *ipv4-address* | **ipv6** *ipv6-address* } | **session-timeout** *minutes* | **url** *url-string* | **user-profile** *profile-name* | **vlan** *vlan-id* } *	缺省情况下，未配置基于终端类型的授权属性

1.9.3 本地BYOD授权显示与维护

完成上述配置后，在任意视图下执行 **display** 命令可以显示 BYOD 终端类型的相关配置。

表1-68 显示 BYOD 指纹信息规则

操作	命令
显示BYOD终端类型识别规则	**display byod rule** { **dhcp-option** [*option-string*] | **http-user-agent** [*agent-string* | **mac-address** [*mac-address*] }
显示基于终端类型的授权属性信息	**display user-group name** *group-name* **byod-authorization**
显示BYOD终端类型识别规则的类型和优先级	**display byod rule-order**

1.10 配置ITA业务策略

ITA（Intelligent Target Accounting，智能靶向计费）表示根据接入用户访问的不同目的地址定义不同的计费级别，实现基于目的地址的差别化计费。例如在校园网中，可以通过在用户的接入设备上

应用 ITA 业务策略对访问教育网内的用户流量不收费或者收很低的费用，而对于访问教育网外 Internet 的用户流量收取较高的费用。目前，仅 Portal、PPP 类型的用户支持 ITA 业务。

在部署了 ITA 业务策略的组网环境中，我们将标记了计费级别的用户流量称为 ITA 业务流量，其它的用户流量称做非 ITA 业务流量。这样，根据每个用户是否有 ITA 业务流量可以将该用户的总计费流量将分成两种情况：一，总计费流量仅由非 ITA 业务流量组成；二，总计费流量是 ITA 业务流量和非 ITA 业务流量的和。用户的总计费流量是否包含 ITA 业务流量可以通过配置进行控制。各个级别的 ITA 业务流量可以独立于用户的总流量进行计费，可以与总计费流量采用不同的计费方案。

需要通过以下几个步骤完成 ITA 业务策略的部署：

(1) 配置 QoS 策略：通过配置流行为将访问不同目的地址的流量重标记为多个流量级别。流量重标记的详细配置请参见“ACL 和 QoS 配置指导”中的“QoS”。

(2) 定义 User Profile，并在 User Profile 内应用用于标记流量级别的 QoS 策略，User Profile 的详细配置请参见“安全配置指导”中的“User Profile”。

(3) 配置授权 User Profile，有以下两种配置方式：

- 在 RADIUS 服务器或设备上(取决于采用远程认证还是本地认证)为用户指定授权 User Profile 属性。当用户通过认证后，由 RADIUS 服务器或设备为接入用户下发 User Profile。
- 在用户的认证域中指定授权 User Profile 属性。若 AAA 服务器或设备未给用户下发 User Profile，则将使用用户认证域中指定的授权 User Profile。

(4) 定义ITA业务策略，主要包括指定计费方案和流量计费级别，具体如 表 1-69 所示。

(5) 配置授权 ITA 业务策略。可在 RADIUS 服务器上或用户认证域中指定授权的 ITA 业务策略。当用户通过认证后，若 RADIUS 服务器为当前用户授权了 ITA 业务策略，将使用 RADIUS 服务器授权的 ITA 业务策略，否则使用用户认证域中指定的 ITA 业务策略。

表1-69 配置并应用 ITA 业务策略

操作	命令	说明
进入系统视图	**system-view**	-
创建ITA业务策略	**ita policy** *policy-name*	缺省情况下，不存在ITA业务策略
指定ITA业务使用的计费方案	**accounting-method** { **none** | **radius-scheme** *radius-scheme-name* [**none**] }	缺省情况下，使用的计费方案为**none**，即不计费
指定需要进行计费的流量计费级别	**accounting-level** *level* { **ipv4** | **ipv6** }	缺省情况下，未指定需要计费的流量计费级别
（可选）开启统一计费功能	**accounting-merge enable**	缺省情况下，统一计费功能处于关闭状态
（可选）配置ITA业务流量配额耗尽策略	**traffic-quota-out** { **offline** | **online** }	缺省情况下，流量配额耗尽后用户不能访问授权的目的地址段
（可选）开启ITA业务流量与用户总计费流量分离功能	**traffic-separate enable**	缺省情况下，ITA业务流量与用户总计费流量分离功能处于关闭状态

1.11 配置NAS-ID与VLAN的绑定

在某些应用环境中，网络运营商需要使用接入设备发送给 RADIUS 服务器的 NAS-Identifier 属性值来获知用户的接入位置，而用户的接入 VLAN 可标识用户的接入位置，因此接入设备上可通过建立用户接入 VLAN 与指定的 NAS-ID 之间的绑定关系来实现接入位置信息的映射。这样，当用户上线时，设备会将与用户接入 VLAN 匹配的 NAS-ID 填充在 RADIUS 请求报文中的 NAS-Identifier 属性中发送给 RADIUS 服务器。

表1-70 配置 NAS-ID 与 VLAN 的绑定

操作	命令	说明
进入系统视图	**system-view**	-
创建NAS-ID Profile，并进入NAS-ID-Profile视图	**aaa nas-id profile** *profile-name*	缺省情况下，不存在NAS-ID Profile 本NAS-ID Profile将被使能Portal或端口安全相应特性进行引用，具体应用请参见“安全配置指导”中的“Portal”或“端口安全”
设置NAS-ID 与VLAN的绑定关系	**nas-id** *nas-identifier* **bind vlan** *vlan-id*	缺省情况下，不存在NAS-ID与VLAN的绑定关系

1.12 AAA显示和维护

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

表1-71 ISP 域显示和维护

操作	命令
显示所有或指定ISP域的配置信息	**display domain** [*isp-name*]

1.13 AAA典型配置举例

1.13.1 SSH用户的HWTACACS认证、授权、计费配置

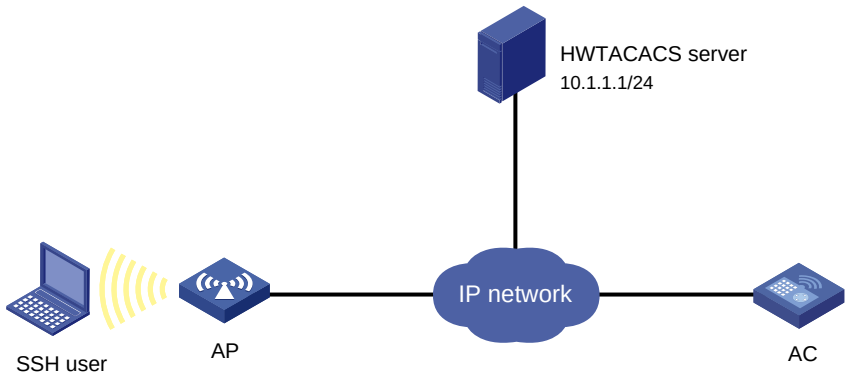
1. 组网需求

通过配置无线控制器 AC 实现使用 HWTACACS 服务器对 SSH 登录 AC 的用户进行认证、授权、计费。

- 由一台 HWTACACS 服务器担当认证、授权、计费服务器的职责，服务器 IP 地址为 10.1.1.1/24。
- AC 与认证、授权、计费 HWTACACS 服务器交互报文时的共享密钥均为 expert，向 HWTACACS 服务器发送的用户名中不带域名。
- SSH 用户登录 AC 时使用 HWTACACS 服务器上配置的用户名以及密码进行认证，认证通过后具有缺省的用户角色 network-operator。

2. 组网图

图1-11 SSH 用户 HWTACACS 认证、授权和计费配置组网图



3. 配置步骤

(1) 配置 HWTACACS 服务器

在 HWTACACS 服务器上设置与 AC 交互报文时的共享密钥为 expert；添加 SSH 用户名及密码。（略）

(2) 配置 AC

配置各接口的 IP 地址（略）。

创建 HWTACACS 方案 hwtac。

```
<AC> system-view
[AC] hwtacacs scheme hwtac
```

配置主认证服务器的 IP 地址为 10.1.1.1，认证端口号为 49。

```
[AC-hwtacacs-hwtac] primary authentication 10.1.1.1 49
```

配置主授权服务器的 IP 地址为 10.1.1.1，授权端口号为 49。

```
[AC-hwtacacs-hwtac] primary authorization 10.1.1.1 49
```

配置主计费服务器的 IP 地址为 10.1.1.1，计费端口号为 49。

```
[AC-hwtacacs-hwtac] primary accounting 10.1.1.1 49
```

配置与认证、授权、计费服务器交互报文时的共享密钥均为明文 expert。

```
[AC-hwtacacs-hwtac] key authentication simple expert
[AC-hwtacacs-hwtac] key authorization simple expert
[AC-hwtacacs-hwtac] key accounting simple expert
```

配置向 HWTACACS 服务器发送的用户名不携带域名。

```
[AC-hwtacacs-hwtac] user-name-format without-domain
[AC-hwtacacs-hwtac] quit
```

创建 ISP 域 bbb，为 login 用户配置 AAA 认证方法为 HWTACACS 认证/授权/计费。

```
[AC] domain bbb
[AC-isp-bbb] authentication login hwtacacs-scheme hwtac
[AC-isp-bbb] authorization login hwtacacs-scheme hwtac
[AC-isp-bbb] accounting login hwtacacs-scheme hwtac
[AC-isp-bbb] quit
```

创建本地 RSA 及 DSA 密钥对。

```
[AC] public-key local create rsa
```

```
[AC] public-key local create dsa
```

使能 SSH 服务器功能。

```
[AC] ssh server enable
```

设置 SSH 用户登录用户线的认证方式为 AAA 认证。

```
[AC] line vty 0 31
[AC-line-vty0-31] authentication-mode scheme
[AC-line-vty0-31] quit
```

使能缺省用户角色授权功能，使得认证通过后的 SSH 用户具有缺省的用户角色 network-operator。

```
[AC] role default-role enable
```

4. 验证配置

用户向 AC 发起 SSH 连接，按照提示输入正确用户名及密码后，可成功登录 AC，并具有用户角色 network-operator 所拥有的命令行执行权限。

1.13.2 SSH用户的local认证、HWTACACS授权、RADIUS计费配置

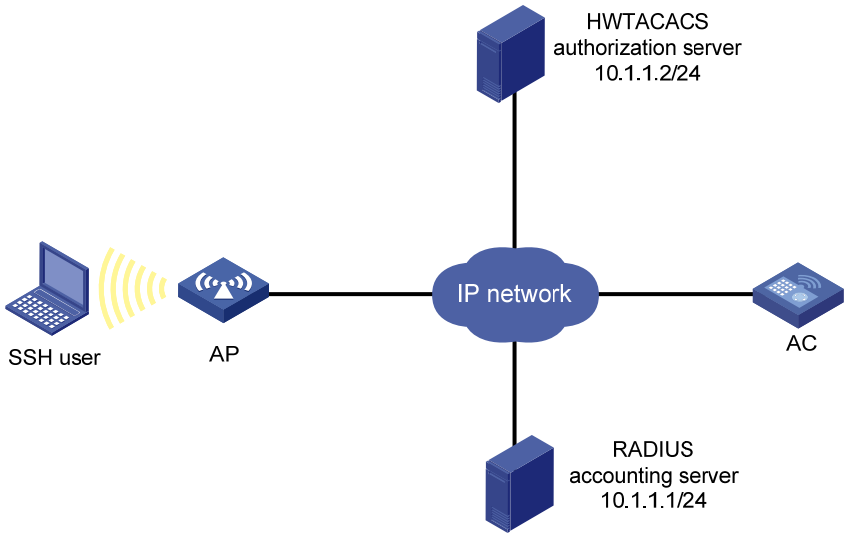
1. 组网需求

通过配置 AC 实现 local 认证，HWTACACS 授权和 RADIUS 计费。SSH 用户的用户名和密码为 hello。

- 一台 HWTACACS 服务器（担当授权服务器的职责）与 AC 相连，服务器 IP 地址为 10.1.1.2。AC 与授权 HWTACACS 服务器交互报文时的共享密钥均为 expert，发送给 HWTACACS 服务器的用户名中不带域名。
- 一台 RADIUS 服务器（担当计费服务器的职责）与 AC 相连，服务器 IP 地址为 10.1.1.1。AC 与计费 RADIUS 服务器交互报文时的共享密钥为 expert。
- 认证通过后的 SSH 用户具有缺省的用户角色 network-operator。

2. 组网图

图1-12 SSH 用户 local 认证、HWTACACS 授权和 RADIUS 计费配置组网图



3. 配置步骤

(1) 配置 HWTACACS 服务器（略）

(2) 配置 RADIUS 服务器（略）

(3) 配置 AC

配置各接口的 IP 地址（略）。

创建本地 RSA 及 DSA 密钥对。

```
<AC> system-view
[AC] public-key local create rsa
[AC] public-key local create dsa
```

使能 SSH 服务器功能。

```
[AC] ssh server enable
```

设置 SSH 用户登录用户线的认证方式为 AAA 认证。

```
[AC] line vty 0 31
[AC-line-vty0-31] authentication-mode scheme
[AC-line-vty0-31] quit
```

配置 HWTACACS 方案。

```
[AC] hwtacacs scheme hwtac
[AC-hwtacacs-hwtac] primary authorization 10.1.1.2 49
[AC-hwtacacs-hwtac] key authorization simple expert
[AC-hwtacacs-hwtac] user-name-format without-domain
[AC-hwtacacs-hwtac] quit
```

配置 RADIUS 方案。

```
[AC] radius scheme rd
[AC-radius-rd] primary accounting 10.1.1.1 1813
[AC-radius-rd] key accounting simple expert
[AC-radius-rd] user-name-format without-domain
[AC-radius-rd] quit
```

创建设备管理类本地用户 hello。

```
[AC] local-user hello class manage
```

配置该本地用户的服务类型为 SSH。

```
[AC-luser-manage-hello] service-type ssh
```

配置该本地用户密码为明文 123456TESTplat&!。

```
[AC-luser-manage-hello] password simple 123456TESTplat&!
[AC-luser-manage-hello] quit
```

创建 ISP 域 bbb，为 login 用户配置 AAA 认证方法为本地认证、HWTACACS 授权、RADIUS 计费。

```
[AC] domain bbb
[AC-isp-bbb] authentication login local
[AC-isp-bbb] authorization login hwtacacs-scheme hwtac
[AC-isp-bbb] accounting login radius-scheme rd
[AC-isp-bbb] quit
```

使能缺省用户角色授权功能，使得认证通过后的 SSH 用户具有缺省的用户角色 network-operator。

```
[AC] role default-role enable
```

4. 验证配置

用户向 AC 发起 SSH 连接，按照提示输入用户名 hello@bbb 及正确的密码后，可成功登录 AC，并具有用户角色 network-operator 拥有的命令行执行权限。

1.13.3 SSH用户的RADIUS认证和授权配置

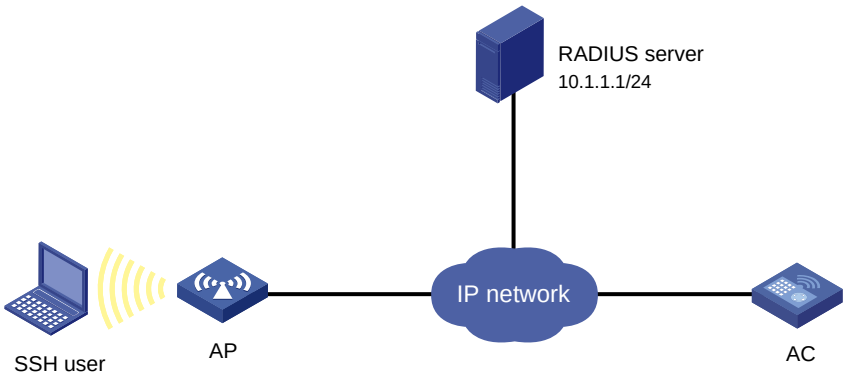
1. 组网需求

如 图 1-13 所示，配置AC实现使用RADIUS服务器对登录AC的SSH用户进行认证和授权。

- 由一台 iMC 服务器担当认证/授权 RADIUS 服务器的职责，服务器 IP 地址为 10.1.1.1/24。
- AC 与 RADIUS 服务器交互报文时使用的共享密钥为 expert，向 RADIUS 服务器发送的用户名带域名。服务器根据用户名携带的域名来区分提供给用户的服务。
- SSH 用户登录 AC 时使用 RADIUS 服务器上配置的用户名 hello@bbb 以及密码进行认证，认证通过后具有缺省的用户角色 network-operator。

2. 组网图

图1-13 SSH 用户 RADIUS 认证/授权配置组网图



3. 配置步骤

(1) 配置 RADIUS 服务器（iMC PLAT 5.0）

说明

下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 5.0(E0101)、iMC UAM 5.0(E0101)），说明 RADIUS 服务器的基本配置。

增加接入设备。

登录进入 iMC 管理平台，选择“业务”页签，单击导航树中的[接入业务/接入设备管理/接入设备配置]菜单项，进入接入设备配置页面，在该页面中单击“增加”按钮，进入增加接入设备页面。

- 设置与 AC 交互报文时使用的认证、计费共享密钥为“expert”；
- 设置认证及计费的端口号分别为“1812”和“1813”；
- 选择业务类型为“设备管理业务”；
- 选择接入设备类型为“H3C”；
- 选择或手工增加接入设备，添加 IP 地址为 10.1.1.2 的接入设备；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

说明

添加的接入设备 IP 地址要与 AC 发送 RADIUS 报文的源地址保持一致。缺省情况下，设备发送 RADIUS 报文的源地址是发送 RADIUS 报文的接口 IP 地址。

- 若设备上通过命令 **nas-ip** 或者 **radius nas-ip** 指定了发送 RADIUS 报文的源地址，则此处的接入设备 IP 地址就需要修改并与指定源地址保持一致。
- 若设备使用缺省的发送 RADIUS 报文的源地址，例如，本例中为 AC 与 RADIUS 服务器连接接口的 IP 地址 10.1.1.2，则此处接入设备 IP 地址就选择 10.1.1.2。

图1-14 增加接入设备

增加设备管理用户。

选择“用户”页签，单击导航树中的[接入用户视图/设备管理用户]菜单项，进入设备管理用户列表页面，在该页面中单击<增加>按钮，进入增加设备管理用户页面。

- 输入用户名“hello@bbb”和密码；
- 选择服务类型为“SSH”；
- 添加所管理设备的 IP 地址，IP 地址范围为“10.1.1.0～10.1.1.255”；
- 单击<确定>按钮完成操作。

说明

添加的所管理设备的 IP 地址范围要包含添加的接入设备的 IP 地址。

图1-15 增加设备管理用户

(2) 配置 AC

配置各接口的 IP 地址（略）。

生成 RSA 及 DSA 密钥对。

```
[AC] public-key local create rsa
[AC] public-key local create dsa
```

使能 SSH 服务器功能。

```
[AC] ssh server enable
```

设置 SSH 用户登录用户线的认证方式为 AAA 认证。

```
[AC] line vty 0 31
[AC-line-vty0-31] authentication-mode scheme
[AC-line-vty0-31] quit
```

使能缺省用户角色授权功能，使得认证通过后的 SSH 用户具有缺省的用户角色 network-operator。

```
[AC] role default-role enable
```

创建 RADIUS 方案 rad。

```
[AC] radius scheme rad
```

配置主认证服务器的 IP 地址为 10.1.1.1，认证端口号为 1812。

```
[AC-radius-rad] primary authentication 10.1.1.1 1812
```
配置与认证服务器交互报文时的共享密钥为明文 expert。
```
[AC-radius-rad] key authentication simple expert
```
配置向 RADIUS 服务器发送的用户名要携带域名。
```
[AC-radius-rad] user-name-format with-domain
[AC-radius-rad] quit
```
创建 ISP 域 bbb，为 login 用户配置 AAA 认证方法为 RADIUS 认证/授权、不计费。
```
[AC] domain bbb
[AC-isp-bbb] authentication login radius-scheme rad
[AC-isp-bbb] authorization login radius-scheme rad
[AC-isp-bbb] accounting login none
[AC-isp-bbb] quit
```
4. 验证配置

用户向 AC 发起 SSH 连接，按照提示输入用户名 hello@bbb 及正确的密码后，可成功登录 AC，并具有用户角色 network-operator 所拥有的命令行执行权限。

1.13.4 SSH用户的LDAP认证配置

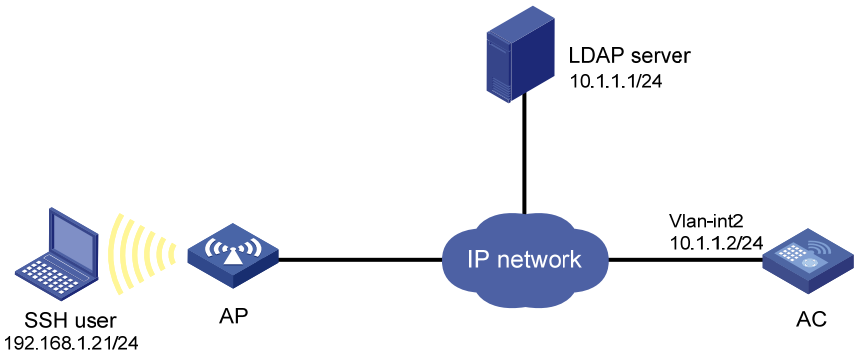
1. 组网需求

如 图 1-16 所示，配置AC实现使用LDAP服务器对登录AC的SSH用户进行认证，且认证通过后具有缺省的用户角色network-operator。

- 一台 LDAP 认证服务器与 AC 相连，服务器 IP 地址为 10.1.1.1。服务器域名为 ldap.com。
- 在 LDAP 服务器上设置管理员 administrator 的密码为 admin!123456；并添加用户名为 aaa 的用户，密码为 ldap!123456。

2. 组网图

图1-16 SSH 用户 LDAP 认证配置组网图



3. 配置步骤

(1) 配置 LDAP 服务器

说明

本文以 Microsoft Windows 2003 Server 的 Active Directory 为例，说明该例中 LDAP 服务器的基本配置。

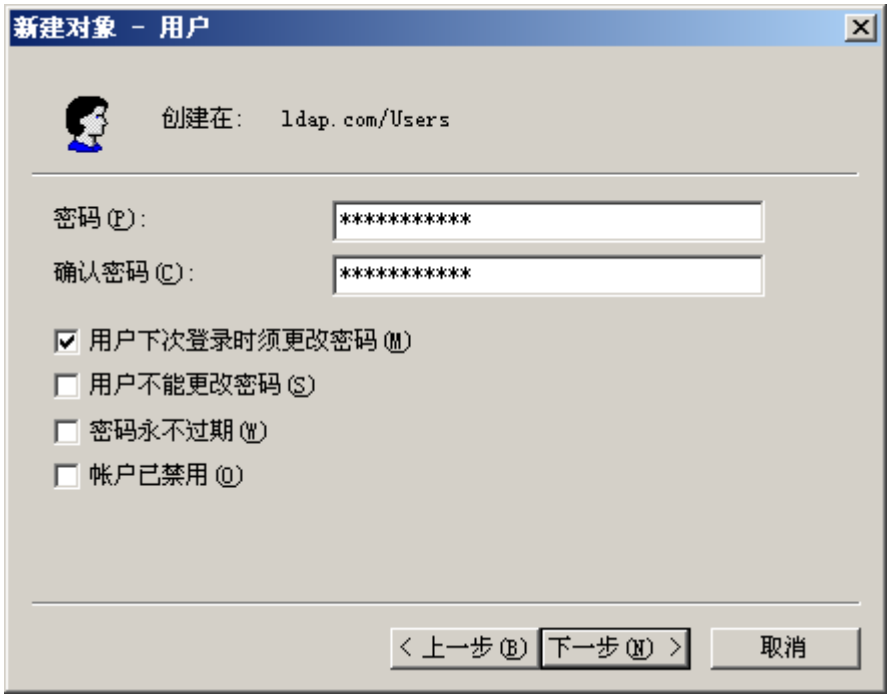
添加用户 aaa。

- 在 LDAP 服务器上，选择[开始/管理工具]中的[Active Directory 用户和计算机]，打开 Active Directory 用户管理界面；
- 在 Active Directory 用户管理界面的左侧导航树中，点击 ldap.com 节点下的“Users”按钮；
- 选择[操作/新建/用户]，打开[新建对象-用户]对话框；
- 在对话框中输入用户登录名 aaa，并单击<下一步>按钮。

图1-17 新建用户 aaa

- 在弹出的对话框的“密码”区域框内输入用户密码 ldap!123456，并单击<下一步>按钮。用户帐户的其它属性（密码的更改方式、密码的生存方式、是否禁用帐户）请根据实际情况选择配置，图中仅为示例。

图1-18 设置用户密码

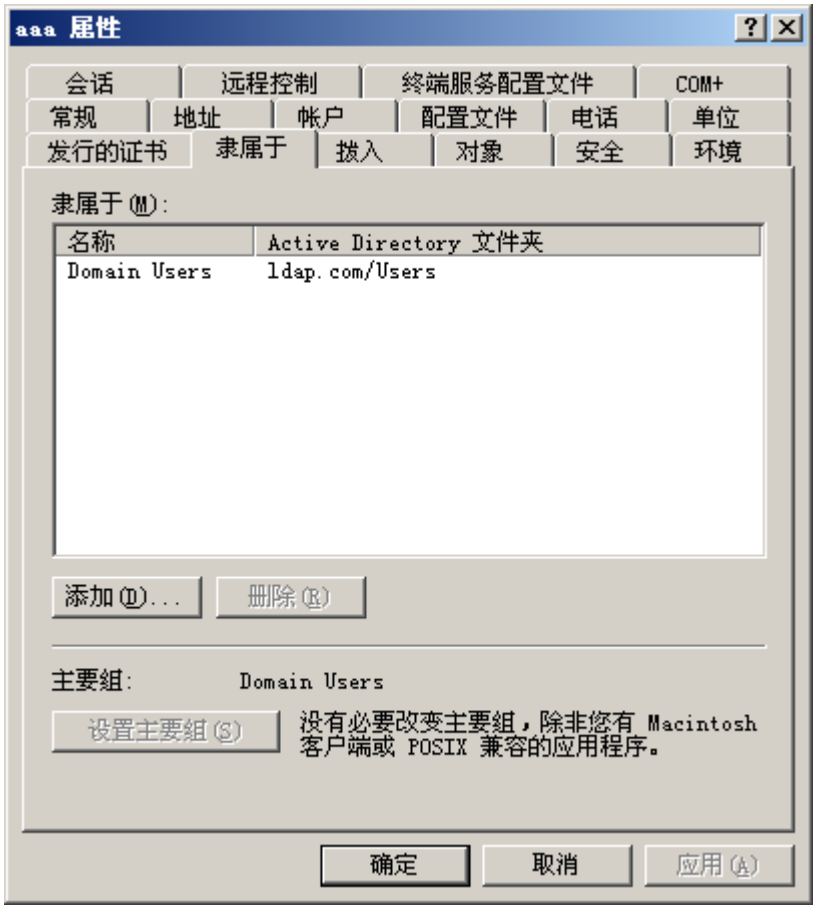


- 单击<完成>按钮，创建新用户 aaa。

将用户 aaa 加入 Users 组。

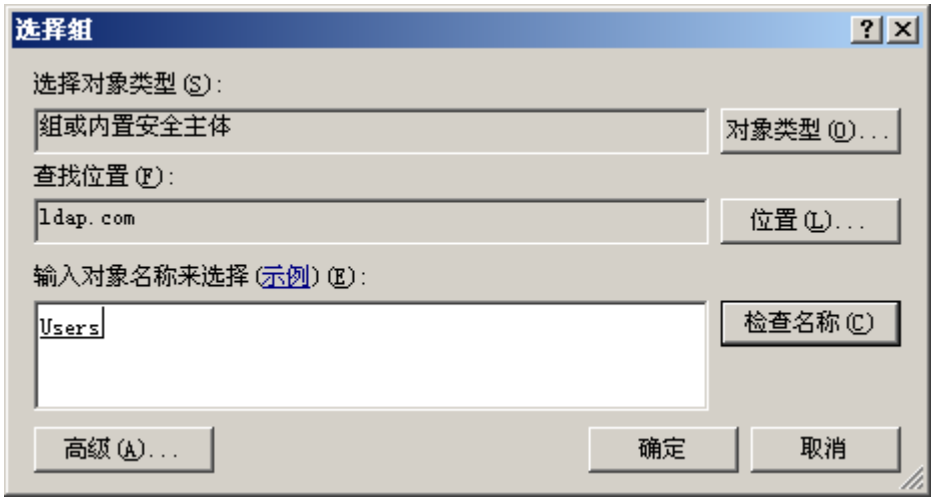
- 在 Active Directory 用户管理界面的左侧导航树中，点击 ldap.com 节点下的“Users”按钮；
- 在右侧的 Users 信息框中右键单击用户 aaa，选择“属性”项；
- 在弹出的[aaa 属性]对话框中选择“隶属于”页签，并单击<添加(D)...>按钮。

图1-19 修改用户属性



- 在弹出的[选择组]对话框中的可编辑区域框中输入对象名称“Users”，单击<确定>，完成用户 aaa 添加到 Users 组。

图1-20 添加用户 aaa 到用户组 Users



完成用户 aaa 的添加之后，还需要配置管理员用户 administrator 的密码为 admin!123456。

- 在右侧的 Users 信息框中右键单击管理员用户 administrator，选择“设置密码(S)...”项；
- 在弹出的密码添加对话框中设置管理员密码，详细过程略。

(2) 配置 AC

配置与 LDAP 服务器连接的 VLAN 2 的 IP 地址为 10.1.1.2/24。

```
[AC] vlan 2
[AC-vlan2] quit
[AC] interface vlan-interface 2
[AC-Vlan-interface2] ip address 10.1.1.2 24
[AC-Vlan-interface2] quit
```

生成本地 RSA 及 DSA 密钥对。

```
[AC] public-key local create rsa
[AC] public-key local create dsa
```

使能 SSH 服务器功能。

```
[AC] ssh server enable
```

设置 SSH 用户登录用户线的认证方式为 AAA 认证。

```
[AC] line vty 0 31
[AC-line-vty0-31] authentication-mode scheme
[AC-line-vty0-31] quit
```

使能缺省用户角色授权功能，使得认证通过后的 SSH 用户具有缺省的用户角色 network-operator。

```
[AC] role default-role enable
```

创建 LDAP 服务器。

```
[AC] ldap server ldap1
```

配置 LDAP 认证服务器的 IP 地址。

```
[AC-ldap-server-ldap1] ip 10.1.1.1
```

配置具有管理员权限的用户 DN。

```
[AC-ldap-server-ldap1] login-dn cn=administrator,cn=users,dc=ldap,dc=com
```

配置具有管理员权限的用户密码。

```
[AC-ldap-server-ldap1] login-password simple admin!123456
```

配置查询用户的起始目录。

```
[AC-ldap-server-ldap1] search-base-dn dc=ldap,dc=com
[AC-ldap-server-ldap1] quit
```

创建 LDAP 方案。

```
[AC] ldap scheme ldap-shm1
```

配置 LDAP 认证服务器。

```
[AC-ldap-ldap-shm1] authentication-server ldap1
[AC-ldap-ldap-shm1] quit
```

创建 ISP 域 bbb，为 login 用户配置 AAA 认证方法为 LDAP 认证、不授权、不计费。

```
[AC] domain bbb
[AC-isp-bbb] authentication login ldap-scheme ldap-shm1
[AC-isp-bbb] authorization login none
[AC-isp-bbb] accounting login none
[AC-isp-bbb] quit
```

4. 验证配置

用户向 AC 发起 SSH 连接，按照提示输入用户名 aaa@bbb 及正确的密码 ldap!123456 后，可成功登录 AC，并具有用户角色 network-operator 所拥有的命令行执行权限。

1.13.5 802.1X用户的RADIUS认证、授权和计费配置

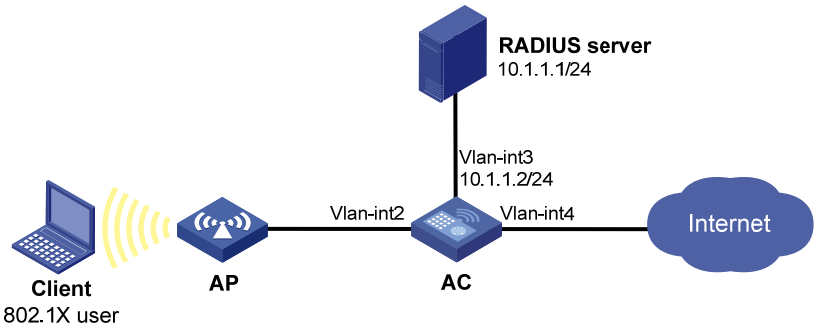
1. 组网需求

在图 1-21 所示的组网环境中，需要实现使用RADIUS服务器对通过AC接入的802.1X用户进行认证、授权和计费。

- 在接入端口 GigabitEthernet1/0/1 上对接入用户进行 802.1X 认证，并采用基于 MAC 地址的接入控制方式，即该端口下的所有用户都需要单独认证；
- AC 与 RADIUS 服务器交互报文时使用的共享密钥为 expert，认证/授权、计费的端口号分别为 1812 和 1813，向 RADIUS 服务器发送的用户名携带域名；
- 用户认证时使用的用户名为 dot1x@bbb。
- 用户认证成功后，认证服务器授权下发 VLAN 4，将用户所在端口加入该 VLAN，允许用户访问该 VLAN 中的网络资源。
- 对 802.1X 用户进行包月方式计费，费用为 120 元/月，以月为周期对用户上网服务的使用量按时长进行统计，允许每月最大上网使用量为 120 个小时。

2. 组网图

图1-21 802.1X 用户 RADIUS 认证、授权和计费配置组网图



3. 配置步骤

说明

请按照组网图完成端口和 VLAN 的配置，并保证用户在通过认证后，能够及时更新客户端 IP 地址与授权 VLAN 中的资源互通。

(1) 配置 RADIUS 服务器（iMC PLAT 5.0）

说明

下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 5.0(E0101)、iMC UAM 5.0(E0101)、iMC CAMS 5.0(E0101)），说明 RADIUS 服务器和 Portal 服务器的基本配置。

增加接入设备。

登录进入 iMC 管理平台，选择“业务”页签，单击导航树中的[接入业务/接入设备配置]菜单项，进入接入设备配置页面，在该页面中单击“增加”按钮，进入增加接入设备页面。

- 设置与 AC 交互报文时的认证、计费共享密钥为“expert”；
- 设置认证及计费的端口号分别为“1812”和“1813”；
- 选择业务类型为“LAN 接入业务”；
- 选择接入设备类型为“H3C”；
- 选择或手工增加接入设备，添加 IP 地址为 10.1.1.2 的接入设备；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

说明

添加的接入设备 IP 地址要与 AC 发送 RADIUS 报文的源地址保持一致。缺省情况下，设备发送 RADIUS 报文的源地址是发送 RADIUS 报文的接口 IP 地址。

- 若设备使用缺省的发送 RADIUS 报文的源地址，例如，本例中为接口 Vlan-interface3 的 IP 地址 10.1.1.2，则此处接入设备 IP 地址就选择 10.1.1.2。
- 若设备上通过命令 **nas-ip** 或者 **radius nas-ip** 指定了发送 RADIUS 报文的源地址，则此处的接入设备 IP 地址就需要修改并与指定源地址保持一致。

图1-22 增加接入设备

增加计费策略。

选择“业务”页签，单击导航树中的[计费业务/计费策略管理]菜单项，进入计费策略管理页面，在该页面中单击<增加>按钮，进入计费策略配置页面。

- 输入计费策略名称“UserAcct”；
- 选择计费策略模板为“包月类型计费”；
- 设置包月基本信息：计费方式为“按时长”、计费周期为“月”、周期内固定费用为“120 元”；
- 设置包月使用量限制：允许每月最大上网使用量为 120 个小时。
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

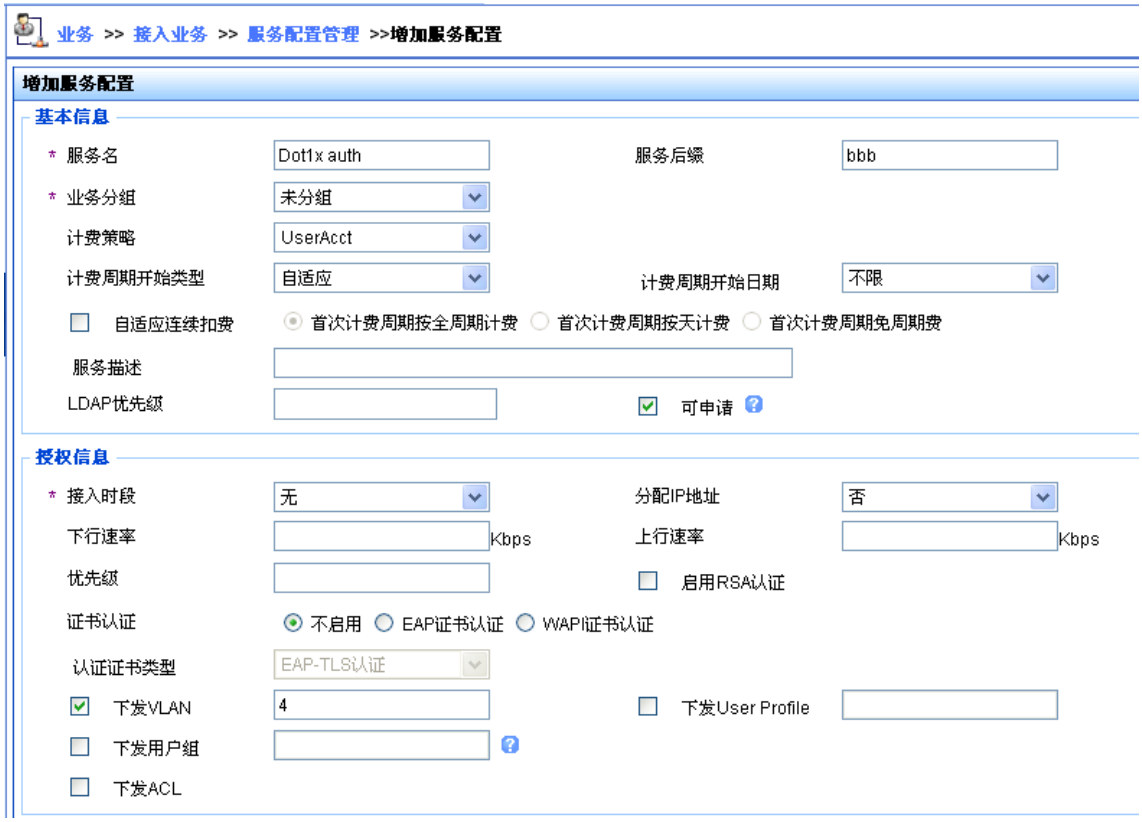
图1-23 增加计费策略

增加服务配置。

选择“业务”页签，单击导航树中的[接入业务/服务配置管理]菜单项，进入服务器配置管理页面，在该页面中单击<增加>按钮，进入增加服务配置页面。

- 输入服务名为“Dot1x auth”、服务后缀为“bbb”，此服务后缀为 802.1X 用户使用的认证域。指定服务后缀的情况下，RADIUS 方案中必须指定向服务器发送的用户名中携带域名；
- 选择计费策略为“UserAcct”；
- 配置授权下发的 VLAN ID 为“4”；
- 本配置页面中还有其它服务配置选项，请根据实际情况选择配置；
- 单击<确定>按钮完成操作。

图1-24 增加服务配置



增加接入用户。

选择“用户”页签，单击导航树中的[接入用户视图/所有接入用户]菜单项，进入接入用户列表页面，在该页面中单击<增加>按钮，进入增加接入用户页面。

- 选择或者手工增加用户姓名为“test”；
- 输入帐号名“dot1x”和密码；
- 选择该用户所关联的接入服务为“Dot1x auth”；
- 本配置页面中还有其它服务配置选项，请根据实际情况选择配置；
- 单击<确定>按钮完成操作。

图1-25 增加接入用户

(2) 配置 AC

- 配置 RADIUS 方案

创建名字为 rad 的 RADIUS 方案并进入该方案视图。

```
<AC> system-view
[AC] radius scheme rad
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[AC-radius-rad] primary authentication 10.1.1.1
[AC-radius-rad] primary accounting 10.1.1.1
[AC-radius-rad] key authentication simple expert
[AC-radius-rad] key accounting simple expert
```

配置发送给 RADIUS 服务器的用户名携带 ISP 域名。

```
[AC-radius-rad] user-name-format with-domain
[AC-radius-rad] quit
```

- 配置认证域

创建并进入名字为 bbb 的 ISP 域。

```
[AC] domain bbb
```

为 lan-access 用户配置 AAA 认证方法为 RADIUS 认证/授权/计费，且均使用 RADIUS 方案 rad。

```
[AC-isp-bbb] authentication lan-access radius-scheme rad
[AC-isp-bbb] authorization lan-access radius-scheme rad
[AC-isp-bbb] accounting lan-access radius-scheme rad
[AC-isp-bbb] quit
```

- 配置 802.1X 认证

开启全局的端口安全特性。

```
[AC] port-security enable
```

配置无线 dot1x 用户的认证方式。

```
[AC] dot1x authentication-method eap
```

创建服务模板 1。

```
[AC] wlan service-template 1
```
配置无线服务的 SSID 为 sectest。
```
[AC-wlan-st-1] ssid sectest
[AC-wlan-st-1] vlan 2
```
配置 AKM 为 802.1X。
```
[AC-wlan-st-1] akm mode dot1x
```
配置用户接入方式为 802.1X 认证。
```
[AC-wlan-st-1] client-security authentication-mode dot1x
```
配置 TKIP 为加密套件，配置 wpa 为安全信息元素。
```
[AC-wlan-st-1] cipher-suite tkip
[AC-wlan-st-1] security-ie wpa
```
配置强制认证域为 bbb。
```
[AC-wlan-st-1] dot1x domain bbb
```
配置使能无线服务模板。
```
[AC-wlan-st-1] service-template enable
```
创建 AP 的模板，名称为 ap1，选择 AP 的型号并配置序列号。
```
[AC] wlan ap ap1 model WA5320E-WiNet
[AC-wlan-ap-ap1] serial-id 219801A1FF8171E00361
```
将服务模板 1 绑定到 AP 的 radio 1 口。
```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] type dot11an
[AC-wlan-ap-ap1-radio-1] service-template 1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```
4. 验证配置


说明

- 若使用 Windows XP 的 802.1X 客户端，则需要正确设置此连接的网络属性：在网络属性的“验证”页签中，确保选中“启用此网络的 IEEE 802.1x 验证”，并选择要用于此连接的 EAP 认证类型为“受保护的 EAP(PEAP)”。
- 若使用 iNode 802.1X 客户端，则无需启用任何高级认证选项。

对于使用 iNode 802.1X 客户端的用户，在客户端的用户属性中输入正确的用户名“dot1x@bbb”和密码后，通过主动发起连接可成功通过认证；对于使用 Windows XP 802.1X 客户端的用户，在系统自动弹出的认证对话框中输入正确的用户名“dot1x@bbb”和密码后，可成功通过认证。认证通过后，服务器向该用户所在端口授权下发了 VLAN 4。

可以通过如下命令查看该连接的详细信息，其中授权下发 VLAN 为 VLAN 4。
```
[AC] display dot1x connection
User MAC address           : 0015-e9a6-7cfe
AP name                    : ap1
Radio ID                   : 1
SSID                       : sectest
```

```
BSSID                      : 8434-9701-0b74
Username                   : dot1x@bbb
Authentication domain      : bbb
Authentication method      : EAP
Initial VLAN               : 2
Authorization VLAN         : 4
Authorization ACL number   : N/A
Authorization user profile : N/A
Termination action         : N/A
Session timeout period     : N/A
Online from                : 2015/06/01 17:15:46
Online duration            : 0h 0m 14s

Total connections: 1
```

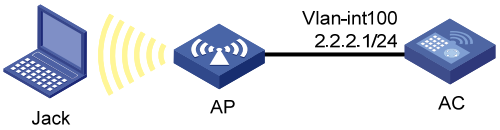
1.13.6 本地来宾用户管理配置举例

1. 组网需求

在 AC 上配置来宾管理功能，并为来宾 Jack 创建本地来宾用户 user1。具体要求如下：

- 开启来宾用户过期删除功能。
- 配置设备为来宾用户业务发送 Email 使用的 SMTP 服务器地址、发件人地址、来宾管理员的 Email 地址。
- 配置设备发送给来宾用户、来宾接待人、来宾管理员的邮件标题和内容。
- 为来宾 Jack 创建一个本地来宾用户 user1，并设置密码、所属用户组、个人相关信息、有效期、以及接待人信息。
- 创建本地来宾用户之后，向来宾接待人和来宾用户分别发送通知邮件。

2. 组网图



3. 配置步骤

- 配置来宾管理功能

开启来宾用户过期删除功能。

```
<AC> system-view
[AC] local-guest auto-delete enable
```

配置发送 Email 使用的 SMTP 服务器地址为 smtp://192.168.0.112/smtp。

```
[AC] local-guest email smtp-server smtp://192.168.0.112/smtp
```

配置 Email 发件人地址为 bbb@ccc.com。

```
[AC] local-guest email sender bbb@ccc.com
```

配置来宾管理员的 Email 地址为 guest-manager@ccc.com。

```
[AC] local-guest manager-email guest-manager@ccc.com
```

配置发送给来宾用户的邮件标题为 Guest account information，邮件内容为 A guest account has been created for your use. The username, password, and valid dates for the account are given below.。

```
[AC] local-guest email format to guest subject Guest account information
[AC] local-guest email format to guest body A guest account has been created for your use. The username, password, and valid dates for the account are given below.
```

配置发送给来宾接待人的邮件标题为Guest account information，邮件内容为A guest account has been created. The username, password, and valid dates for the account are given below.。

```
[AC] local-guest email format to sponsor subject Guest account information
[AC] local-guest email format to sponsor body A guest account has been created for your use. The username, password, and valid dates for the account are given below.
```

配置发送给来宾管理员的邮件标题为 Guest register information，邮件内容为 A guest account has been registered. The username for the account is given below. Please approve the register information.。

```
[AC] local-guest email format to manager subject Guest register information
[AC] local-guest email format to manager body A guest account has been registered. The username for the account is given below. Please approve the register information.
```

- 配置本地来宾用户

创建用户组 guest1。

```
[AC] user-group guest1
[AC-ugroup-guest1] quit
```

创建本地来宾用户 user1。

```
[AC] local-user user1 class network guest
```

配置本地来宾用户密码为明文 123456。

```
[AC-luser-network(guest)-user1] password simple 123456
```

指定本地来宾用户所属的用户组为 guest1。

```
[AC-luser-network(guest)-user1] group guest1
```

配置本地来宾用户的姓名为 Jack。

```
[AC-luser-network(guest)-user1] fullname Jack
```

配置本地来宾用户的公司为 cc。

```
[AC-luser-network(guest)-user1] company cc
```

配置本地来宾用户的 Email 地址为 Jack@cc.com。

```
[AC-luser-network(guest)-user1] email Jack@cc.com
```

配置本地来宾用户的电话为 131129237。

```
[AC-luser-network(guest)-user1] phone 131129237
```

配置本地来宾用户的描述信息为 A guest from company cc。

```
[AC-luser-network(guest)-user1] description A guest from company cc
```

配置本地来宾用户的有效期为 2015/4/1 8:00 ~ 2015/4/3 18:00。

```
[AC-luser-network(guest)-user1] validity-datetime 2015/4/1 08:00:00 to 2015/4/3 18:00:00
```

配置本地来宾用户的接待人姓名为 Sam。

```
[AC-luser-network(guest)-user1] sponsor-full-name Sam
```

配置本地来宾用户的接待人 Email 地址为 Sam@aa.com。

```
[AC-luser-network(guest)-user1] sponsor-email Sam@aa.com
```

配置本地来宾用户的接待人部门为 security。

```
[AC-luser-network(guest)-user1] sponsor-department security
[AC-luser-network(guest)-user1] quit
```

- 给来宾接待人和来宾用户分别发送通知邮件

给来宾接待人发送通知邮件。

```
[AC] local-guest send-email username user1 to sponsor
```

给来宾发送通知邮件。

```
[AC] local-guest send-email username user1 to guest
```

4. 验证配置

以上配置完成后，通过执行如下显示命令可查看本地来宾用户 user1 的配置信息。

```
[AC] display local-user user1 class network guest
Network access guest user user1:
  State:                      Active
  Service type:               LAN access/Portal
  User group:                 guest1
  Full name:                  Jack
  Company:                    cc
  Email:                      Jack@cc.com
  Phone:                      131129237
  Description:                A guest from company cc
  Sponsor full name:          Sam
  Sponsor department:         security
  Sponsor email:              Sam@aa.com
  Period of validity:
    Start date and time:      2015/04/01-08:00:00
    Expiration date and time:2015/04/03-18:00:00
```

Jack 使用用户名 user1 和密码 123456 在 2015/4/1 8:00 ~ 2015/4/3 18:00 内进行本地认证，可以认证通过。

1.14 AAA常见配置错误举例

1.14.1 RADIUS认证/授权失败

1. 故障现象

用户认证/授权总是失败。

2. 故障分析

(1) 设备与 RADIUS 服务器之间存在通信故障。

(2) 用户名不是“*userid@isp-name*”的形式，或设备上没有正确配置用于认证该用户的 ISP 域。

(3) RADIUS 服务器的数据库中没有配置该用户。

(4) 用户侧输入的密码不正确。

(5) RADIUS 服务器和设备的报文共享密钥不同。

3. 处理过程

(1) 使用 **ping** 命令检查设备与 RADIUS 服务器是否可达。

(2) 使用正确形式的用户名或在设备上确保正确配置了用于该用户认证的 ISP 域。

(3) 检查 RADIUS 服务器的数据库以保证该用户的配置信息确实存在。

(4) 确保接入用户输入正确的密码。

(5) 检查两端的共享密钥，并确保两端一致。

1.14.2 RADIUS报文传送失败

1. 故障现象

RADIUS 报文无法传送到 RADIUS 服务器。

2. 故障分析

(1) 设备与 RADIUS 服务器之间的通信存在故障。

(2) 设备上没有设置相应的 RADIUS 服务器 IP 地址。

(3) 认证/授权和计费服务的 UDP 端口设置不正确。

(4) RADIUS 服务器的认证/授权和计费端口被其它应用程序占用。

3. 处理过程

(1) 确保线路通畅。

(2) 确保正确设置 RADIUS 服务器的 IP 地址。

(3) 确保与 RADIUS 服务器提供服务的端口号一致。

(4) 确保 RADIUS 服务器上的认证/授权和计费端口可用。

1.14.3 RADIUS计费功能异常

1. 故障现象

用户认证通过并获得授权，但是计费功能出现异常。

2. 故障分析

(1) 计费端口号设置不正确。

(2) 计费服务器和认证服务器不是同一台机器，设备却要求认证和计费功能属于同一个服务器（IP 地址相同）。

3. 处理过程

(1) 正确设置 RADIUS 计费端口号。

(2) 确保设备的认证服务器和计费服务器的设置与实际情况相同。

1.14.4 HWTACACS常见配置错误举例

HWTACACS 的常见配置错误举例与 RADIUS 基本相似，可以参考以上内容。

1.14.5 LDAP常见配置错误举例

1. 故障现象

用户认证失败。

2. 故障分析

(1) 设备与 LDAP 服务器之间存在通信故障。

(2) 配置的认证/授权服务器 IP 地址或端口号不正确。

(3) 用户名不是“*userid@isp-name*”的形式，或设备上没有正确配置用于认证该用户的 ISP 域。

(4) LDAP 服务器目录中没有配置该用户。

(5) 用户输入的密码不正确。

(6) 具有管理员权限的用户 DN 或密码没有配置。

(7) 设备上配置的用户参数（如用户名属性）与服务器上的配置不对应。

(8) 认证操作时，没有配置 LDAP 方案用户查询的起始 DN。

3. 处理过程

(1) 使用 **ping** 命令检查设备与 LDAP 服务器是否可达。

(2) 确保配置的认证服务器 IP 地址与端口号与 LDAP 服务器实际使用的 IP 地址和端口号相符。

(3) 使用正确形式的用户名或在设备上确保正确配置了用于该用户认证的 ISP 域。

(4) 检查 LDAP 服务器目录以保证该用户的配置信息确实存在。

(5) 确保输入用户密码正确。

(6) 确保配置了正确的管理员用户 DN 和密码。

(7) 确保设备上的用户参数（如用户名属性）配置与 LDAP 服务器上的配置相同。

(8) 认证操作时，确保配置了用户查询的起始 DN。