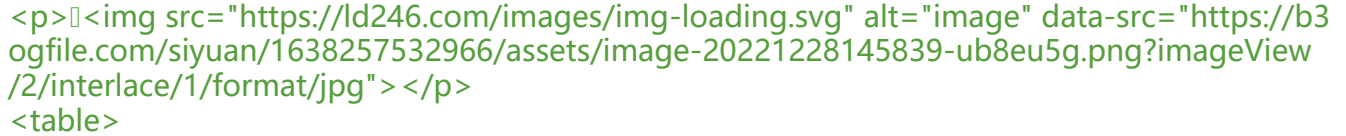
AAA 原理与配置

作者：DNA
原文链接：https://ld246.com/article/1672805041537
来源网站：链滴

<h2 id="前言">前言</h2>
对于任何网络，用户管理都是最基本的安全管理要求之一。
AAA（Authentication, Authorization, and Accounting）是一种管理框架</strong，它提供了授权部分用户访问指定资源和记录这些用户操作行为的安全机制。因其具有良好的可扩展，并且容易实现用户信息的集中管理而被广泛使用。AAA 可以通过多种协议来现，在实际应用中，最常使用 RADIUS （Remote Authentication Dial-In User Service）协议或 HTACACS（Huawei Terminal Access Controller Access Control System）思科的是 TACACS+。</>
本章将介绍 AAA 基本概念、AAA 的实现方式、AAA 的基本配置以及常见 AAA 应用场景。
<h2 id="目标">目标</h2>
学完本课程后，您将能够：

掌握 AAA 的基本原理
描述 AAA 的应用场景
描述 RADIUS 的基本原理
掌握 AAA 的基本配置

<h2 id="AAA-概述">AAA 概述</h2>
<h2 id="为什么使用-AAA">为什么使用 AAA</h2>
<table>
<thead>
<tr>
<th align="center">需求</th>
<th align="left">描述</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">设备的数量</td>
<td align="left">大量的网络设备、VPN 服务器、无线 AP 要做身份验证。</td>
</tr>
<tr>
<td align="center">人员的数量</td>
<td align="left">大量的员工需要在各种设备上做身份验证。</td>
</tr>
<tr>
<td align="center">人员的变动</td>
<td align="left">员工的入职、升职、离职，需要对相关账户属性或权限做修改。</td>
</tr>
<tr>
<td align="center">计费的需要</td>
<td align="left">记录访问时间、操作过程等行为，产生日志或相关费用。</td>
</tr>
</tbody>
</table>
因此，AAA 给企业网络提供一种集中式、标准化、可扩展、灵活的解决方。
<h2 id="AAA-基本概念">AAA 基本概念</h2>
AAA 是 Authentication（认证）、Authorization（授权）和 Accounting（计费）的简称，是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。

<table>

<thead>
<tr>
<th align="center">名词</th>
<th align="center">描述</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">认证</td>
<td align="center"></td>
</tr>
<tr>
<td align="center">Authentication</td>
<td align="center"></td>
</tr>
<tr>
<td align="center">Who are you？你是谁？</td>
<td align="center"></td>
</tr>
<tr>
<td align="center">确认用户的身份，判断访问者是否为合法的网络用户。</td>
<td align="center"></td>
</tr>
<tr>
<td align="center"></td>
<td align="center"></td>
</tr>
<tr>
<td align="center">授权</td>
<td align="center"></td>
</tr>
<tr>
<td align="center">Authorization</td>
<td align="center"></td>
</tr>
<tr>
<td align="center">What can you do？ 你能做什么？</td>
<td align="center"></td>
</tr>
<tr>
<td align="center">对不同用户赋予不同的权限，限制用户可以使用的服务。</td>
<td align="center"></td>
</tr>
<tr>
<td align="center"></td>
<td align="center"></td>
</tr>
<tr>
<td align="center">计费</td>
<td align="center"></td>
</tr>
<tr>
<td align="center">Accounting</td>
<td align="center"></td>

</tr>
<tr>
<td align="center">What did you do? 你做过什么？ </td>
<td align="center"></td>
</tr>
<tr>
<td align="center">记录用户使用网络服务过程中的所有操作</td>
<td align="center"></td>
</tr>
<tr>
<td align="center"></td>
<td align="center"></td>
</tr>
</tbody>
</table>

<h2 id="AAA-常见架构">AAA 常见架构</h2>
AAA 常见网络架构中包括用户、NAS（Network Access Server）、AAA 服务器（AAA Server
。采用 C/S（客户端/服务器）架构
AAA 可以通过多种协议来实现，目前设备支持基于 RADIUS 或 HWTACACS 协议来实现 AAA
在实际应用中，最常使用 RADIUS 协议。
<table>
<thead>
<tr>
<th align="center">角色</th>
<th align="left">描述</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">用户</td>
<td align="left">每个用户都属于某一个域。用户属于哪个域是由用户名中的域名分隔符 @ 后的字
串决定。例如，如果用户名是 user1@<a href="https://ld246.com/member/" aria-name="" clas
="tooltipped__user" target="_blank">domain1，则用户属于 domain1 域。如果用户名后
带有 @，则用户属于系统缺省域。</td>
</tr>
<tr>
<td align="center">AAA 客户端</td>
<td align="left">开启 AAA，通常为网络设备、服务器、无线 AP 等</td>
</tr>
<tr>
<td align="center">通常被称为 NAS（ Network Access Server，网络接入服务器）</st
ong></td>
<td align="left"></td>
</tr>
<tr>
<td align="center">NAS 基于域来对用户进行管理，每个域都可以配置不同的认证、授权和计费方
，用于对该域下的用户进行认证、授权和计费。</td>
<td align="left"></td>
</tr>
<tr>
<td align="center"></td>

<td align="left"></td>
</tr>
<tr>
<td align="center">AAA 服务器</td>
<td align="left">负责 AAA，通常为各个厂商开发的不同产品</td>
</tr>
</tbody>
</table>

<blockquote>
注：AAA 框架使用协议的交互都是在 AAA 客户端和 AAA 服务器之间完成的。也就是说用户和 AA 客户端之间没有运行 AAA 框架调用协议的交互。
</blockquote>

<h2 id="AAA工作原理">AAA 工作原理</h2>
<h2 id="认证-Authentication-">认证（Authentication）</h2>
AAA 支持三种认证方式
<table>
<thead>
<tr>
<th align="center">认证方式</th>
<th align="left">Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">不认证</td>
<td align="left">完全信任用户，不对用户身份进行合法性检查。鉴于安全考虑，这种认证方式很少采用。华为不允许不认证。</td>
</tr>
<tr>
<td align="center">本地认证</td>
<td align="left">将本地用户信息（包括用户名、密码和各种属性）配置在 NAS 上，此时路由器即是NAS 也是 AAA Server。</td>
</tr>
<tr>
<td align="center">本地认证的优点是处理速度快、运营成本低；缺点是存储信息量受设备硬件条限制。</td>
<td align="left"></td>
</tr>
<tr>
<td align="center">这种认证方式常用于对用户登录设备进行管理，如 Telnet，FTP 用户等。</td>
<td align="left"></td>
</tr>
<tr>
<td align="center"></td>
<td align="left"></td>
</tr>

<tr>
<td align="center">远端认证</td>
<td align="left">将用户信息（包括用户名、密码和各种属性）配置在认证服务器上。</td>
</tr>
<tr>
<td align="center">支持通过 RADIUS 协议或 HWTACACS 协议进行远端认证。</td>
<td align="left"></td>
</tr>
<tr>
<td align="center">NAS 作为客户端，与 RADIUS 服务器或 HWTACACS 服器进行通信。</td>
<td align="left"></td>
</tr>
<tr>
<td align="center"></td>
<td align="left"></td>
</tr>
</tbody>
</table>

注：认证方案中可以指定一种或者多种认证方法：按照配置顺序，仅前一方法无响应时（不是失败），NAS 设备才尝试使用下一个认证方法。如果某种证方法回应认证失败，则意味着 AAA 服务器拒绝用户接入，用户身份认证过程被停止，并且不会尝试后面的认证方法。
<h2 id="授权-Authorization-">授权（Authorization）</h2>
AAA 授权功能赋予用户访问的特定网络或设备的权限。授权信息包括：

所属用户组
所属 VLAN
ACL 编号

AAA 支持三种授权方式：
<table>
<thead>
<tr>
<th align="center">方法</th>
<th align="left">Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">不授权</td>
<td align="left">不对用户进行授权处理。</td>
</tr>
<tr>
<td align="center">本地授权</td>
<td align="left">根据 NAS 上对应域下的配置进行授权。</td>
</tr>
<tr>
<td align="center">远端授权</td>
<td align="left">支持由 RADIUS 服务器授权或 HWTACAS 服务器授权。</td>
</tr>

</tbody>
</table>

HWTACACS 授权，使用 HWTACACS 服务器对所有用户授权。
RADIUS 授权，只支持对通过 RADIUS 服务器认证的用户授权。RADIUS 协议的认证和授权是定在一起的，不能单独使用 RADIUS 进行授权。
当采用远端授权时，用户可以同时从授权服务器和 NAS 获取授权信息。NAS 配置的授权信息优先级授权服务器下发的授权信息低。
|

<p>注：可以指定一种或多种授权方法：按照配置顺序，仅前一种授权方法<strng>无响应时（不是失败），后面的授权方法才会被启用。如果前面的授权方法<strong回应授权失败，表示 AAA 服务器拒绝为用户提供服务。此时，授权结束，后面授权方法不会被启用。</p>
<h2 id="计费-Accouting-">计费（Accouting）</h2>
计费功能用于监控授权用户的网络行为和网络资源的使用情况。AAA 支持两种计费方式：
<table>
<thead>
<tr>
<th align="center">计费方式</th>
<th align="left">说明</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">不计费</td>
<td align="left">为用户提供免费上网服务，不产生相关活动日志。</td>
</tr>
<tr>
<td align="center">远端计费</td>
<td align="left">支持通过 RADIUS 服务器或 HWTACACS 服务器进行远端计费。</td>
</tr>
</tbody>
</table>

注：只能指定一种计费方法。
<h2 id="AAA-协议">AAA 协议</h2>
<h3 id="AAA-常用协议">AAA 常用协议</h3>
运行在 AAA 客户端和服务端之间，在实际应用中，最常使用 RADIUS 协议。HWTACACS 完全<trong>兼容思科、华三使用的 TACACS+，制完全一致。
<table>
<thead>
<tr>
<th align="center">AAA 协议</th>
<th align="center">封装</th>
<th align="center">端口号</th>
<th align="center">安全程度</th>
<th align="center">标准</th>

<th align="center">命令授权</th>
<th align="center">组成</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">RADIUS</td>
<td align="center">UDP</td>
<td align="center">1812、1813</td>
<td align="center">只加密密码</td>
<td align="center">IETF 公开标准</td>
<td align="center">不支持</td>
<td align="center">认证和授权一起</td>
</tr>
<tr>
<td align="center">HWTACACS</td>
<td align="center">TCP</td>
<td align="center">49</td>
<td align="center">加密整个包</td>
<td align="center">华为私有</td>
<td align="center">支持对设备上的配置命令进行授权使用</td>
<td align="center">认证和授权独立</td>
</tr>
<tr>
<td align="center">TACACS+</td>
<td align="center">TCP</td>
<td align="center">49</td>
<td align="center">加密整个包</td>
<td align="center">Cisco Private</td>
<td align="center">支持对设备上的配置命令进行授权使用</td>
<td align="center">认证和授权独立</td>
</tr>
</tbody>
</table>
注：授权一般都是厂商私有，所以 RADIUS 只能做认证和计费。
<h3 id="RADIUS-工作原理">RADIUS 工作原理</h3>
设备作为 RADIUS 客户端，负责收集用户信息（例如：用户名、密码等），并将这些信息发送到 RADIUS 服务器。RADIUS 服务器则根据这些信息完成用户身份认证以及认证通过后的用户授权和计。用户、RADIUS 客户端和 RADIUS 服务器之间的交互流程如图 1 所示。

<table>
<thead>
<tr>
<th align="center">第几步</th>
<th align="left">详细过程</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">1</td>
<td align="left">当用户接入网络时，用户发起连接请求，向 RADIUS 客户端（即设备）发送用户和密码。</td>

</tr>
<tr>
<td align="center">2</td>
<td align="left">RADIUS 客户端向 RADIUS 服务器发送包含用户名和密码信息的认证请求报文。</d>
</tr>
<tr>
<td align="center">3</td>
<td align="left">RADIUS 服务器对用户身份的合法性进行检验：</td>
</tr>
</tbody>
</table>

如果用户身份合法，RADIUS 服务器向 RADIUS 客户端返回认证接受报文，允许用户进行下一步作。由于 RADIUS 协议合并了认证和授权的过程，因此认证接受报文中也包含了用户的授权信息。</l>
如果用户身份不合法，RADIUS 服务器向 RADIUS 客户端返回认证拒绝报文，拒绝用户访问接入络。|
|4|RADIUS 客户端通知用户认证是否成功。|
|5|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ADIUS 服务器发送计费开始请求报文。|
|6|RADIUS 服务器返回计费开始响应报文，并开始计费。|
|7| 用户开始访问网络资源。|
|8|（可选）在使能实时计费功能的情况下，RADIUS 客户端会定时向 RADIUS 服务器发送实时计费求报文，以避免因付费用户异常下线导致的不合理计费。|
|9|（可选）RADIUS 服务器返回实时计费响应报文，并实时计费。|
|10| 用户发起下线请求，请求停止访问网络资源。|
|11|RADIUS 客户端向 RADIUS 服务器提交计费结束请求报文。|
|12|RADIUS 服务器返回计费结束响应报文，并停止计费。|
|13|RADIUS 客户端通知用户访问结束，用户结束访问网络资源。|

<h3 id="HWTACACS-工作原理">HWTACACS 工作原理</h3>
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。基本消交互流程图如图 1 所示。

<td align="left">HWTACACS 客户端收到请求之后，向 HWTACACS 服务器发送认证开始报文。</d>
</tr>
<tr>
<td align="center">3</td>
<td align="left">HWTACACS 服务器发送认证回应报文，请求用户名。</td>
</tr>
<tr>
<td align="center">4</td>
<td align="left">HWTACACS 客户端收到回应报文后，向用户询问用户名。</td>
</tr>
<tr>
<td align="center">5</td>
<td align="left">用户输入用户名。</td>
</tr>
<tr>
<td align="center">6</td>
<td align="left">HWTACACS 客户端收到用户名后，向 HWTACACS 服务器发送认证持续报文，中包括了用户名。</td>
</tr>
<tr>
<td align="center">7</td>
<td align="left">HWTACACS 服务器发送认证回应报文，请求密码。</td>
</tr>
<tr>
<td align="center">8</td>
<td align="left">HWTACACS 客户端收到认证回应报文，向用户询问密码。</td>
</tr>
<tr>
<td align="center">9</td>
<td align="left">用户输入密码。</td>
</tr>
<tr>
<td align="center">10</td>
<td align="left">HWTACACS 客户端收到密码后，向 HWTACACS 服务器发送认证持续报文，其包括了密码信息。</td>
</tr>
<tr>
<td align="center">11</td>
<td align="left">HWTACACS 服务器发送认证回应报文，指示用户通过认证。</td>
</tr>
<tr>
<td align="center">12</td>
<td align="left">HWTACACS 客户端向 HWTACACS 服务器发送授权请求报文。</td>
</tr>
<tr>
<td align="center">13</td>
<td align="left">HWTACACS 服务器发送授权回应报文，指示用户通过授权。</td>
</tr>
<tr>
<td align="center">14</td>
<td align="left">HWTACACS 客户端收到授权回应报文，向用户输出设备的配置界面。</td>
</tr>
<tr>

<td align="center">15</td>
<td align="left">HWTACACS 客户端向 HWTACACS 服务器发送计费开始请求报文。</td>
</tr>
<tr>
<td align="center">16</td>
<td align="left">HWTACACS 服务器发送计费开始回应报文，指示计费开始请求报文已经收到。</d>
</tr>
<tr>
<td align="center">17</td>
<td align="left">用户请求断开连接。</td>
</tr>
<tr>
<td align="center">18</td>
<td align="left">HWTACACS 客户端向 HWTACACS 服务器发送计费结束请求报文。</td>
</tr>
<tr>
<td align="center">19</td>
<td align="left">HWTACACS 服务器发送计费结束回应报文，指示计费结束请求报文已经收到。</d>
</tr>
</tbody>
</table>

<h2 id="AAA-域">AAA 域</h2>
<h3 id="简介">简介</h3>
NAS 设备对用户的管理是基于域的，每个用户都属于一个域，一个域是由属于同一个域的用户成的群体。简单地说，用户属于哪个域就使用哪个域下的 AAA 配置信息。
使用域的目的，为了防止同名的存在，有了域即使同名但域名是唯一的。
用户输入的用户名决定域，完整格式：用户名 @ 域名后缀

如图 1 所示，域统一管理 AAA 方案、服务器模板和授权等配置信息

AAA 方案：分为认证方案、授权方案和计费方案，用来定义认证、授权和计费的方法及每种方的生效顺序
服务器模板：用来配置认证、授权或计费使用的服务器。配置服务器授权时，用户从服务器和域获取授权信息，详见图 2。
如果使用本地认证或授权，需要配置本地用户的相关信息。
域下的授权信息：域下还可以配置授权信息。

授权信息分为两类：服务器下发的授权信息和域下的授权信息。用户从何处获取授权与授权方案配置的授权方法有关。如图 2 所示：

授权方法为本地授权时，用户从域下获取授权信息。
授权方法为服务器授权时，用户从服务器和域下获取授权信息。域下配置的授权信息比服务器下的授权信息优先级低，如果两者的授权信息冲突，则服务器下发的授权优先生效；如果两者的授权信不冲突，则两者的授权信息同时生效。这样处理可以通过域管理进行灵活授权，而不必受限于服务器供的授权。

<h3 id="用户所属的域">用户所属的域</h3>
如<a href="https://ld246.com/forward?goto=http%3A%2F%2Flocalhost%3A7890%2Fpages%2FAZL1024J%2F01%2FAZL1024J%2F01%2Fresources%2Fdc%2Fdc_cfg_aaa_6022.html%3Ft%3D0%26fe%3D10%26hib%3D7.1.14.2.2.1%26id%3DZH-CN_CONCEPT_0176366033%23ZH-N_CONCEPT_0176366033__fig_dc_cfg_aaa_602201" target="_blank" rel="nofollow ugc">图 3 /a> 所示，用户所属的域是由用户登录到 NAS 设备时提供的用户名决定的，当户名中没有携带域名或者携带的域名在 NAS 设备上未配置时，NAS 设备无法确认用户所属的域，此，NAS 设备根据用户的类型将用户加入到默认域中。

注：本地认证作用的
为了提供更为精细且有差异化的认证、授权、计费服务，AAA 将用户划分为管理员用户和接入户两种类型。NAS 设备存在两个全局默认域：全局默认管理域 <code>default_admin</code> 和局默认普通域 <code>default</code>，分别作为 <code>管理员用户</code> 和 <code>接入户</code> 的全局默认域，两个全局默认域下的缺省配置也不同。
| 用户分类 | 用户接入方式
| 使用的全局默认域 | 全局默认域下的缺省配置
（认证方案）| 全局默认域下的缺省配置
<table>
<thead>
<tr>
<th align="center">（计费方案）</th>
<th align="center"></th>
<th align="center"></th>
<th align="center"></th>
<th align="center"></th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">管理员用户</td>
<td align="center">又称为 Login 用户，指可以登录设备的用户。</td>
<td align="center"></td>
<td align="center"></td>
<td align="center"></td>
</tr>
<tr>
<td align="center">包括通过 FTP、HTTP、SSH、Telnet 和 Console 方式登录设备的用户。</td

<td align="center"></td>
<td align="center"></td>

<td align="center"></td>
<td align="center"></td>
</tr>
<tr>
<td align="center">缺省本地认证</td>
<td align="center"></td>
<td align="center"></td>
<td align="center"></td>
<td align="center"></td>
</tr>
<tr>
<td align="center">default_admin</td>
<td align="center">default（本地认证）</td>
<td align="center">default（不计费）</td>
<td align="center"></td>
<td align="center"></td>
</tr>
<tr>
<td align="center">接入/普通用户</td>
<td align="center">包括 NAC 用户（包括 802.1X 认证用户、MAC 认证用户、Portal 认证用户、PPoE 认证用户）。</td>
<td align="center"></td>
<td align="center"></td>
<td align="center"></td>
</tr>
<tr>
<td align="center">缺省本地认证</td>
<td align="center"></td>
<td align="center"></td>
<td align="center"></td>
<td align="center"></td>
</tr>
<tr>
<td align="center">default</td>
<td align="center">radius（本地认证）</td>
<td align="center">default（不计费）</td>
<td align="center"></td>
<td align="center"></td>
</tr>
</tbody>
</table>
<pre><code class="language-powershell highlight-chroma">#查看设备当前配置的全局默认普通域和全默认管理域
 display aaa onfiguration
  Domain Name Delimiter : @
  Domainname parse direction : <span class="highlight-

">Left to right</spa
>
 <span class="hi
hlight-n">Domainname location <span
lass="highlight-err">: After-delimiter
 <span class="hi
hlight-n">Administrator user <span class="highl
ght-k">default domain<span class="highlight-e
r">: default_admin <span class="highlight-p"
//全局默认管理域
 <span class="hi
hlight-n">Normal user <span class="highlight-k
>default domain <span class="highlight-err
>: default //</spa
>全局默认普通域
</code></pre>
注

两个全局默认域缺省都绑定了名称为 default 的计费方案，修改该计费方案会同时影响这两个域配置。
两个全局默认域均不能删除，只能修改。

<h2 id="AAA-常见应用场景">AAA 常见应用场景</h2>

<h2 id="AAA-服务器产品">AAA 服务器产品</h2>
<h2 id="思科-AAA-服务器产品">思科 AAA 服务器产品</h2>
ACS：Secure Access Control Server，安全访问控制服务器
ISE：Identity Services Engine，身份服务引擎。

<h2 id="Windows-上-801-x-认证">Windows 上 801.x 认证</h2>

启动上面的服务后会多出一个选项页面，这就是 802.1x 认证。

2/interlace/1/format/jpg">□
□
□
<h2 id="AAA-配置实现">AAA 配置实现</h2>
<h2 id="配置流程">配置流程</h2>
创建配置服务器模板 :箭头/Arrow_96px:
创建配置 AAA 方案 :箭头/Arrow_96px:
创建配置域方案 :箭头/Arrow_96px:
在域下应用 AAA 方案、RADIUS 服务器模板和授权信息
□
□

<table>
<thead>
<tr>
<th align="center">默认参数</th>
<th align="left">缺省值</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">本地用户</td>
<td align="left">名称*：admin*</td>
</tr>
<tr>
<td align="center">接入方式：SSH、HTTP（用于 Web 网管方式登录设备）</td>
<td align="left"></td>
</tr>
<tr>
<td align="center"></td>
<td align="left"></td>
</tr>
<tr>
<td align="center">全局默认普通域</td>
<td align="left">default：默认绑定认证方案 radius 和计费方案 default、未绑定授权方案。</td>
</tr>
<tr>
<td align="center">全局默认管理域</td>
<td align="left">default_admin：默认绑定认证方案 default 和计费方案 default、未绑定授权方
。</td>
</tr>
<tr>
<td align="center">认证方案</td>
<td align="left">default：默认认证方式为本地认证。radius：默认认证方式为 RADIUS 认证。</t
>
</tr>
<tr>
<td align="center">授权方案</td>
<td align="left">default：默认授权方式为本地授权。</td>
</tr>
<tr>
<td align="center">计费方案</td>

<td align="left">default：默认不计费。</td>
</tr>
</tbody>
</table>
<h2 id="配置本地认证">配置本地认证</h2>
背景信息
AAA 认证、授权可以在 NAS 设备上完成，也可以交由服务器完成。如果在 NAS 上完成 AAA 证和授权，则相当在 NAS 上配置一个本地的 AAA 服务器。本地认证的优点是速度快，可以为运营低成本，缺点是存储信息量受设备硬件条件限制。
配置本地服务器，需要在设备上配置用户的认证和授权信息，包括配置本地用户和配置本地授权个步骤。
<h3 id="配置本地认证-">配置本地认证</h3>
背景信息
配置本地用户时，可以配置本地用户允许建立的连接数目、本地用户级别、闲置切断时间以及本地用上线时间等功能，同时支持本地用户修改密码功能。
说明

为充分保证设备安全，请用户不要关闭密码复杂度检查功能，并定期修改密码。

更改本地账号的权限（密码、接入类型、FTP 目录、级别等）后，已经在线的用户权限不会被更，新上线的用户则以新的权限为准。

本地用户的接入类型分为以下两类：

管理类：包括 ftp、http、ssh、telnet、x25-pad 和 terminal。
普通类：包括 8021x、bind、ppp、sslvpn 和 web。

登录方式为 Telnet 和 FTP 时存在安全风险，建议使用 STelnet 和 SFTP，此时，用户的接入类配置为 SSH。
缺省情况下，HTTP 采用随机生成的自签名证书支持 HTTPS。由于自签名证书存在安全风险，因此建用户替换为官方授信的数字证书。

操作步骤
（1）创建本地用户（AAA 视图下）
<table>
<thead>
<tr>
<th align="center">步骤</th>
<th align="center">命令</th>
<th align="left">说明</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">（可选）使能对密码进行复杂度检查功能</td>
<td align="center">user-password complexity-check [three-of kinds]</td>
<td align="left">缺省情况下，设备对密码进行复杂度检查。用户设置的密码至少包含“大写字母、

写字母、数字和特殊字符”中的两种，才能通过密码复杂度检查。</td>
</tr>
<tr>
<td align="center">创建本地用户名和密码(选择一种方式创建本地用户名和密码)</td>
<td align="center"></td>
<td align="left"></td>
</tr>
<tr>
<td align="center">local-user user-name passwor
</td>
<td align="center">缺省情况下：本命令为交互式命令，当用户输入密码时，直接以明文形式输入在安全风险，建议用户以交互式方式输入。如果用户名中带域名分隔符（如“@”、“|”、“%”等号），并且没有执行命令 domainname-parse-direction right-to-le
t 设置域名解析方向，则认为分隔符前面的部分是纯用户名，后面部分是域名。如果没有隔符，则整个字符串为用户名，普通用户默认到 default 域认证，管理用户默到 default_admin 域进行认证。</td>
<td align="left"></td>
</tr>
<tr>
<td align="center"></td>
<td align="center"></td>
<td align="left"></td>
</tr>
<tr>
<td align="center"></td>
<td align="center">local-user user-name passwor
 { cipher | irreversible-cipher } passw
rd</td>
<td align="left"></td>
</tr>
<tr>
<td align="center">配置本地用户的允许接入类型</td>
<td align="center">local-user user-name service-t
pe { 8021x | bind | ftp |
http | ppp | ssh | sslvpn
/strong> | telnet | terminal | web |
x25-pad } ^*^</td>
<td align="left">缺省情况下，本地用户关闭所有的接入类型。如果为 Portal 接入用户，则配置的入类型为 web。配置本地用户的接入类型前，如果用户已经存在，需注意：</t
>
</tr>
</tbody>
</table>

如果密码使用的是不可逆加密算法，则只允许配置管理类的接入类型。
如果密码使用的是可逆加密算法，则允许配置普通类或者管理类的接入类型，不允许配置普通类管理类的混合类接入类型，并且当配置为管理类的接入类型时，加密算法自动转换成不可逆加密算法

|
|（可选）为本地用户分配固定的 IP 地址 |local-user user-name
bind-ip ip-address| 缺省情况下，系统没有为本地用户分配固的 IP 地址。|

（2）（可选）配置用户级别、所属用户组、接入时间段、闲置切断功能及可建立的连接数目

<table>
<thead>
<tr>
<th align="center">步骤</th>
<th align="center">命令</th>
<th align="left">说明</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">配置本地用户级别</td>
<td align="center">local-user user-name privileg
 level level</td>
<td align="left">缺省情况下，本地用户的级别为 0 级。</td>
</tr>
<tr>
<td align="center">配置本地用户所属的组</td>
<td align="center">local- user user-name user-gr
up group-name</td>
<td align="left">缺省情况下，本地用户不属于任何用户组。</td>
</tr>
<tr>
<td align="center">配置本地账号的接入时间段</td>
<td align="center">local-user user-name</e
> time-range time-name</td>
<td align="left">缺省情况下，未配置本地账号的接入时间段，即任意时间都允许接入。</td>
</tr>
<tr>
<td align="center">配置指定用户的闲置切断时间</td>
<td align="center">local-user user-name idle-tim
out minutes [seconds]</td>
<td align="left"></td>
</tr>
<tr>
<td align="center">或者 local-user user-name idle
cut</td>
<td align="center"></td>
<td align="left"></td>
</tr>
<tr>
<td align="center">指定用户界面的超时时间。本地用户闲置时间超过设定时间，则用户自动下线
设置用户连接的超时时间为 0 或者过长会导致终端一直处于登录状态，存在安全风险，建议用户执行
令 lock 锁定当前连接。如果对普通用户（NAC 或 PPP 用户等）进行闲置切断
则执行命令 local-user user-name idle-cut
进行配置，如果需要对管理用户进行闲置切断，请执行命令 local-user u
er-name idle-timeout minutes [seconds
]进行配置。</td>
<td align="center"></td>
<td align="left"></td>
</tr>
<tr>
<td align="center">配置指定用户可建立的连接数目</td>

<td align="center">local-user user-name access-limit max-number</td>
<td align="left">缺省情况下，不限制用户可建立的连接数目。如果需要设置本地账号只能在唯一终登录，可通过设置 max-number 的值为 1 实现该功能。</td>
</tr>
</tbody>
</table>

（3）配置本地用户安全性（可选）
| 步骤
<table>
<thead>
<tr>
<th align="left"></th>
<th>命令</th>
<th align="left">说明</th>
<th align="left"></th>
</tr>
</thead>
<tbody>
<tr>
<td align="left">使能本地帐号锁定功能并配置用户的重试时间间隔、连续认证失败的限制次数及帐锁定时间</td>
<td></td>
<td align="left"></td>
<td align="left"></td>
</tr>
<tr>
<td align="left"></td>
<td>local-aaa-user wrong-password retry-interval retry-interval retry-time retry-time bloc-time block-time</td>
<td align="left">缺省情况下，本地帐号锁定功能处于使能状态，用户的重试时间间隔为 5 分钟、续输入错误密码的限制次数为 3 次，帐号锁定时间为 5 分钟。</td>
<td align="left"></td>
</tr>
<tr>
<td align="left">配置在用户账号锁定期间，允许该用户使用指定的 IP 地址访问网络</td>
<td></td>
<td align="left"></td>
<td align="left"></td>
</tr>
<tr>
<td align="left"></td>
<td>aaa-quiet administrator except-list { *ipv4-address</td>
<td align="left">ipv6-address* } <1-32></td>
<td align="left">缺省情况下，用户在账号锁定期间不能访问网络。通过命令 display aaa quiet administrator except-list，可以查询以上配置的 IP 地址信息。</td>
</tr>
<tr>
<td align="left">配置本地接入用户密码策略</td>
<td></td>
<td align="left"></td>
<td align="left"></td>

</tr>
<tr>
<td align="left">使能本地接入用户的密码策略功能并进入本地接入用户密码策略视图。</td>
<td>local-aaa-user password policy access-user</td>

<td align="left">缺省情况下，本地接入用户的密码策略功能处于使能状态。</td>
<td align="left"></td>
</tr>
<tr>
<td align="left"></td>
<td></td>
<td align="left"></td>
<td align="left"></td>
</tr>
<tr>
<td align="left"></td>
<td>配置每个用户密码的历史记录的最大条数。</td>
<td align="left">password history record number <m>number</td>
<td align="left">缺省情况下，每个用户密码的历史记录的最大条数是 5 条。</td>
</tr>
<tr>
<td align="left"></td>
<td>退出本地接入用户密码策略视图。</td>
<td align="left">quit</td>
<td align="left"></td>
</tr>
<tr>
<td align="left">配置本地管理员密码策略</td>
<td></td>
<td align="left"></td>
<td align="left"></td>
</tr>
<tr>
<td align="left">使能本地管理员的密码策略功能并进入本地管理员密码策略视图。</td>
<td>local-aaa-user password policy administrator</t
>
<td align="left">缺省情况下，本地管理员的密码策略功能处于已使能状态。</td>
<td align="left"></td>
</tr>
<tr>
<td align="left"></td>
<td>使能密码过期提醒功能并配置密码过期前的提醒时间。</td>
<td align="left">password alert before-expire day</td>
<td align="left">缺省情况下，密码过期前的提醒时间为 30 天。</td>
</tr>
<tr>
<td align="left"></td>
<td>使能初始密码提醒功能。</td>
<td align="left">password alert original</td>
<td align="left">缺省情况下，初始密码修改提醒功能处于使能状态。</td>
</tr>
<tr>
<td align="left"></td>

<td>使能密码过期功能并配置密码过期时间。</td>
<td align="left">password expire day</
d>
<td align="left">缺省情况下，密码过期时间为 90 天。</td>
</tr>
<tr>
<td align="left"></td>
<td>配置每个用户密码的历史记录的最大条数。</td>
<td align="left">password history record number <
m>number</td>
<td align="left">缺省情况下，每个用户密码的历史记录的最大条数是 5 条。</td>
</tr>
<tr>
<td align="left"></td>
<td>退出本地管理员密码策略视图。</td>
<td align="left">quit</td>
<td align="left"></td>
</tr>
</tbody>
</table>

（4）本地用户访问权限相关配置（可选）
<table>
<thead>
<tr>
<th align="left">步骤</th>
<th align="left">命令</th>
<th align="left">说明</th>
</tr>
</thead>
<tbody>
<tr>
<td align="left">配置允许 FTP 用户访问的 FTP 目录</td>
<td align="left">local-user user-name ftp-director
 directory</td>
<td align="left">缺省情况下，允许 FTP 用户访问的 FTP 目录为空。若配置本地用户的接入类型为 F
P 方式，则必须配置本地用户的 FTP 目录，且本地用户的级别不能低于管理级，否则 FTP 用户无法
录。</td>
</tr>
<tr>
<td align="left">配置本地用户的状态</td>
<td align="left">local-user user-name state</stro
g> { **active</td>
<td align="left">block** }</td>
</tr>
</tbody>
</table>

若用户状态为激活态，将接收该用户的认证请求并做进一步处理。
若用户状态为阻塞态，将拒绝该用户的认证请求。
|
| 配置本地账号的有效期 |local-user user-name expir
-date expire-date| 缺省情况下，本地账号永久有效。|
| 配置本地用户的账户类型 |local-user user-name acc

unt-type cmcc-tr069| 缺省情况下，未配置本地用户的账户类型。
如果未通过命令 set operator-code cmcc 开启设备的 TR069 功能，则本命令无法执行。
|

（5）本地管理员用户修改密码时，去使能与用户进行交互确认的功能
<pre><code class="language-powershell highlight-chroma">[R-aaa] undo local-user password change-offline enable

</code></pre>
缺省情况下，本地管理员用户在 AAA 视图下通过命令 local-user user-name password 修改密码时，已使能与用户进行交互确认的功能，备会提示用户账号将被注销，需要重新登录。

（6）修改本地用户登录密码（可选）
<table>
<thead>
<tr>
<th align="center">步骤</th>
<th align="center">命令</th>
<th align="center">说明</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">返回用户视图</td>
<td align="center">return</td>
<td align="center">-</td>
</tr>
<tr>
<td align="center">修改本地用户登录密码</td>
<td align="center">local-user change-password</td>
<td align="center">-</td>
</tr>
</tbody>
</table>

<h3 id="配置授权规则">配置授权规则</h3>
<h3 id="配置AAA方案">配置 AAA 方案</h3>
背景信息
如果需要采用本地方式进行认证和授权，需要在认证方案中配置认证模式为本地认证，在授权方中配置授权模式为本地授权。
缺省情况下，设备对用户进行本地认证和授权。
注：如果使用 authentication-mode 命令配置认证方式为不认证，则当户上线时，用户输入任意的用户名和密码后都会认证成功。因此，为保护设备或网络安全，建议开启证方式，保证用户经过认证后才可以访问设备或网络。
<h4 id="-1-配置认证方案">【1】配置认证方案</h4>

（1）进入 AAA 视图
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">[R1] <span class="highlight-n
>aaa
</code></pre>

（2）创建一个认证方案并进入认证方案视图，或者直接进入一个已经存在的认证方案视图
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">[R
-aaa] authenticatio
-scheme
</code></pre>
缺省情况下，设备中有两个认证方案，认证方案名称分别是 default 和 radius，default 和 radiu
方案均不能删除，只能修改方案下的参数。

（3）配置认证模式为本地认证
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">#配置为RADIUS认证
<span class="high
ight-p">[R1-aaa-au
hen-rz] authenticat
on-mode local

<span class="high
ight-c">#如果需要配置本地认证为备份认证模式，请执行命令
<span class="high
ight-p">[R1-aaa-au
hen-rz] authenticat
on-mode { radius</
pan> local | <span c
ass="highlight-nb">local-case }
</code></pre>
缺省情况下，认证模式为本地认证。

（4）在当前认证模板下，配置对用户提升级别进行认证时采用的认证模式（可选）
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">[R
-aaa-authen-rz]</sp
n> authentication-super [</
pan> hwtacacs | <sp
n class="highlight-n">super] <span class="high
ight-p">* none
</code></pre>
缺省情况下，用户提升级别时认证模式为 super，即本地认证模式。

（5）配置域名解析的方向，从左向右或从右向左（可选）
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">[R
-aaa] domainname
parse-direction {</s
an> left-to-right <
pan class="highlight-p">| right-to<span class=
highlight-n">-left }
</code></pre>

缺省情况下，域名解析方向为从左向右。

（6）配置认证旁路时间（可选）
<pre><code class="language-powershell highlight-chroma">[R1] aaa-authen-bypass enable time time-value
</code></pre>
缺省情况下，未启用旁路认证功能。
<table>
<thead>
<tr>
<th align="center">参数</th>
<th align="center">参数说明</th>
<th align="center">取值</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">enable</td>
<td align="center">使能远端认证旁路功能。</td>
<td align="center">-</td>
</tr>
<tr>
<td align="center">time time-value</td>
<td align="center">指定认证旁路时间。</td>
<td align="center">整数形式，单位为分钟，取值范围为 1～1440。</td>
</tr>
</tbody>
</table>
<pre><code class="language-powershell highlight-chroma"># 配置认证旁路时间为3分钟。
[Huawei] aaa-authen-bypass enable time 3
</code></pre>

<h4 id="-2-配置授权方案">【2】配置授权方案</h4>

（1）进入 AAA 视图
<pre><code class="language-powershell highlight-chroma">[R1] aaa
</code></pre>

（2）创建授权方案，并进入授权方案视图或直接进入一个已存在的授权方案视图
<pre><code class="language-powershell highlight-chroma">[R-aaa] authorization scheme
</code></pre>
缺省情况下，设备有一个授权方案，授权方案配置名是 default，不能删除，只能修改。

（3）配置授权模式
<pre><code class="language-powershell highlight-chroma">[R-aaa-authorization-sq] authorization-mode local [none]
</code></pre>
缺省情况下，授权模式为本地授权模式。

（4）配置授权服务器下发的用户授权信息的生效模式（可选）
<pre><code class="language-powershell highlight-chroma">[R-aaa] authorization modify mode { modify | overlay }
</code></pre>
缺省情况下，授权服务器下发的用户授权信息的生效模式为 overlay 模式
<table>
<thead>
<tr>
<th align="center">参数</th>
<th align="center">参数说明</th>
<th align="center">取值</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">modify</td>
<td align="center">指定授权服务器下发的用户授权信息的生效模式为修改模式。</td>
<td align="center">-</td>
</tr>
<tr>
<td align="center">overlay</td>
<td align="center">指定授权服务器下发的用户授权信息的生效模式为覆盖模式。</td>
<td align="center">-</td>
</tr>
</tbody>
</table>

（5）配置认证旁路时间（可选）
<pre><code class="language-powershell highlight-chroma">[R1] aaa-authen-bypass enable time time-alue
</code></pre>
缺省情况下，未启用旁路认证功能。
<table>
<thead>
<tr>

<th align="center">参数</th>
<th align="center">参数说明</th>
<th align="center">取值</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">enable</td>
<td align="center">使能远端认证旁路功能。</td>
<td align="center">-</td>
</tr>
<tr>
<td align="center">time time-value</td>
<td align="center">指定认证旁路时间。</td>
<td align="center">整数形式，单位为分钟，取值范围为 1～1440。</td>
</tr>
</tbody>
</table>
<pre><code class="language-powershell highlight-chroma"># 配置认证旁路时间为3分钟。
[Huawei] aaa-authen-bypass enable time 3
</code></pre>

<h3 id="在域下应用AAA方案">在域下应用 AAA 方案</h3>
背景信息
创建的认证和授权方案，只有在域下应用后才能生效。采用本地方式进行认证和授权时，采用缺省的费方案，即不计费。
操作步骤
（1）创建域并进入域视图或进入一个已存在的域视图
<pre><code class="language-powershell highlight-chroma">[R-aaa] domain [domain-index domain-index]
</code></pre>
缺省情况下，设备存在两个域：“default”和“default_admin”。“default”用于普通接入户的域，“default_admin”用于管理员的域。
说明

用户认证时，如果输入不带域名的用户名，将到默认域认证，因此设备需通过 domain domain-name [admin]命令设置 domain-name 为全局默认域。
用户认证时，如果输入带域名的用户名，需要带上正确的域名domain-name。

（2）配置域的 AAA 方案
<table>
<thead>
<tr>
<th align="left">步骤</th>

<th align="left">命令</th>
<th align="left">说明</th>
</tr>
</thead>
<tbody>
<tr>
<td align="left">配置域的认证方案</td>
<td align="left">authentication-scheme authentication-scheme-name</td>
<td align="left">缺省情况下，“default”域使用名为“radius”的认证方案，“default_admin域使用名为“default”的认证方案，其他域使用名为“radius”的认证方案。</td>
</tr>
<tr>
<td align="left">配置域的授权方案</td>
<td align="left">authorization-scheme authorization-scheme-nam</td>
<td align="left">缺省情况下，域下没有绑定授权方案。</td>
</tr>
</tbody>
</table>

（3）配置本地授权规则（可选）
<table>
<thead>
<tr>
<th align="left">步骤</th>
<th align="left">命令</th>
<th align="left">说明</th>
</tr>
</thead>
<tbody>
<tr>
<td align="left">（可选）配置对域下的用户下发用户组授权。</td>
<td align="left">user-group group-name</td>
<td align="left">缺省情况下，未配置对域下的用户下发用户组授权。</td>
</tr>
<tr>
<td align="left">（可选）配置域的业务方案</td>
<td align="left">service-scheme service-scheme-name</td>
<td align="left">缺省情况下，域下没有配置任何业务方案。</td>
</tr>
</tbody>
</table>

（4）配置域的状态和流量统计功能（可选）
<table>
<thead>
<tr>
<th align="left">步骤</th>
<th align="left">命令</th>
<th align="left">说明</th>
</tr>
</thead>

<tbody>
<tr>
<td align="left">配置域的状态</td>
<td align="left">state { **active</td>

<td align="left">block** [time-range time-name <1–4>] }</td>
</tr>
</tbody>
</table>

（5）使能域用户的流量统计功能（可选）
<pre><code class="language-powershell highlight-chroma">[R-aaa-domain-test] statistic enable</code></pre>
缺省情况下，域用户的流量统计功能处于未使能状态。

（6）配置域名解析方案（如果在 AAA 视图和认证模板视图下都配置了域名解析，则优先使用认证模板上的配置。认证模板下的配置仅适用于无线用户）（可选）
| 步骤
<table>
<thead>
<tr>
<th align="left"></th>
<th align="left">命令</th>
<th>说明</th>
<th align="left"></th>
</tr>
</thead>
<tbody>
<tr>
<td align="left">AAA 视图</td>
<td align="left"></td>
<td></td>
<td align="left"></td>
</tr>
<tr>
<td align="left">退出域视图</td>
<td align="left">quit</td>
<td></td>
<td align="left"></td>
</tr>
<tr>
<td align="left"></td>
<td align="left">配置域名解析的方向</td>
<td>domainname-parse-direction { left-to-right | right-to-left }</td>
<td align="left">域名解析的方向可以是从左到右，或者从右到左。缺省情况下，域名解析方向为从右向右。</td>
</tr>

<tr>
<td align="left"></td>
<td align="left">配置域名分隔符</td>
<td>domain-name-delimiter delimiter</td>
<td align="left">域名分隔符可以是 \ / : < > | @ ' % 中的某一个。缺省情况下，域名分隔符为@。</td>
</tr>
<tr>
<td align="left"></td>
<td align="left">配置域名的位置</td>
<td>domain-location { after-delimiter | befre-delimiter }</td>
<td align="left">缺省情况下，域名在分隔符后。</td>
</tr>
<tr>
<td align="left"></td>
<td align="left">配置安全字符串分隔符</td>
<td>security-name-delimiter delimiter</td>
<td align="left">缺省情况下，安全字符串分隔符为*。</td>
</tr>
</tbody>
</table>

<h2 id="配置基于RADIUS远程认证">配置基于 RADIUS 远程认证</h2>
<h3 id="配置RADIUS服务器模板">配置 RADIUS 服务器模板</h3>
背景信息
设备通过 RADIUS 服务器模板来指定与其对接的 RADIUS 服务器，RADIUS 服务器模板内包含服务的 IP 地址、端口号、源接口、共享密钥等配置。
RADIUS 服务器模板下的配置要与 RADIUS 服务器上的配置一致。
操作步骤
【1】配置 RADIUS 服务模板名字
<pre><code class="language-powershell highlight-chroma">[NSA] radius-server template template-name
</code></pre>
缺省情况下，设备上存在一个名为“default”的 RADIUS 服务器模板，只能修改，不能删除。
【2】配置 RADIUS 认证服务器
<pre><code class="language-powershell highlight-chroma">#IPv4 RADIUS认证
[R1-radiusDNA] radius-serve authentication ipv-address port [vpn-instance vpn-instace-name | source { loopback interface-number <span class="ass="highlight-p">| ip-address ipv4-address | vlanif interface-number <span class="hi

hlight-p">} | weight
/span> weight-value]</spa
> *

<span class="high
ight-c">#IPv6 RADIUS认证
<span class="high
ight-p">[R1-radius
DNA] radius-serve
 authentication ipv
-address port [</sp
n> source { <span cl
ss="highlight-n">loopback interface-number
span class="highlight-p">| ip-address <span cl
ss="highlight-nb">ipv6-address | <span class="
ighlight-n">vlanif interface-number <span clas
="highlight-p">} | w
ight weight-value]
/span> *
</code></pre>
缺省情况下，未配置 RADIUS 认证服务器。
<table>
<thead>
<tr>
<th align="center">参数</th>
<th align="left">参数说明</th>
<th align="left">取值</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">ipv4-address</td>
<td align="left">指定 RADIUS 认证服务器的 IPv4 地址。</td>
<td align="left">点分十进制格式，必须是合法的单播地址。</td>
</tr>
<tr>
<td align="center">ipv6-address</td>
<td align="left">指定 RADIUS 认证服务器的 IPv6 地址。</td>
<td align="left">32 位 16 进制数，格式为 X:X:X:X:X:X:X:X。</td>
</tr>
<tr>
<td align="center">port</td>
<td align="left">指定 RADIUS 认证服务器的端口号。</td>
<td align="left">整数形式，取值范围是 1～65535。</td>
</tr>
<tr>
<td align="center">vpn-instance vpn-instance-name</td>
<td align="left">指定绑定的 VPN 实例名称。</td>
<td align="left">必须是已存在的 VPN 实例。</td>
</tr>
<tr>
<td align="center">source loopback interface-number</td

<td align="left">指定 Loopback 接口的 IP 地址作为源 IP 地址。其中，interface-number<

em> 表示 Loopback 接口编号。</td>
<td align="left">必须是已存在的 Loopback 接口。</td>
</tr>
<tr>
<td align="center">source ip-address ipv4-address</td>
<td align="left">指定 IPv4 地址作为向 RADIUS 认证服务器发送 RDIUS 报文时使用的源 IPv4 地址。如果没有配置此参数，则使用出接口的 IPv4 地址作为向RADIUS 认证服务器发送 RADIUS 报文时使用的源 IPv4 址。</td>
<td align="left">点分十进制格式，必须是合法的单播地址。</td>
</tr>
<tr>
<td align="center">source ip-address ipv6-address</td>
<td align="left">指定 IPv6 地址作为向 RADIUS 认证服务器发送 RDIUS 报文时使用的源 IPv6 地址。如果没有配置此参数，则使用出接口的 IPv6 地址作为向RADIUS 认证服务器发送 RADIUS 报文时使用的源 IPv6 址。该地址不能为 VRRP6 虚地址。</td>
<td align="left">32 位 16 进制数，格式为 X:X:X:X:X:X:X:X。</td>
</tr>
<tr>
<td align="center">source vlanif interface-number</td>
<td align="left">指定 VLANIF 接口的 IP 地址作为源 IP 地址。其中，interface-number</m> 表示 VLANIF 接口编号。</td>
<td align="left">必须是已存在的 VLANIF 接口。</td>
</tr>
<tr>
<td align="center">weight weight-value</td>
<td align="left">指定 RADIUS 认证服务器的权重值。当配置了多个服务器时设备优先通过权重值大的服务器进行认证。当权重值相等时，设备则优先通过先配置的服务器进行认。</td>
<td align="left">整数形式，取值范围是 0～100，缺省值为 80。</td>
</tr>
</tbody>
</table>
<pre><code class="language-powershell highlight-chroma"><pan class="highlight-cl"># 配置主用RADIUS认证服务器的IP地址为10163.155.13，端口号为1812。
[R1-radiusDNA] radius-serve authentication 10</pan>.163.15513 1812

配置备用RADIUS认证服务器的IP地址为10.163.155.15，端口号为1812，权重为50。</san>
[R1-radiusDNA] radius-serve authentication 10</pan>.163.155

15 1812 <s
an class="highlight-n">weight 50
</code></pre>
【3】配置 RADIUS 计费服务器
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">配置<span class="highlight-n
>IPv4 RADIUS计费
务器
<span class="high
ight-p">[R1-radius
DNA] radius-serve
 accounting ipv4-a
dress port [
vpn-instance vpn-instance
/span>-name | <spa
class="highlight-n">source { <span class="highl
ght-n">loopback interface-number <span clas
="highlight-p">| ip-address <span class="highl
ght-nb">ipv4-address | <span class="highlight-
">vlanif interface-number <span class="highli
ht-p">} | weight</sp
n> weight-value]
span class="highlight-p">*

<span class="high
ight-err">配置IPv6 R
DIUS计费服务器
<span class="high
ight-p">[R1-radius
DNA] radius-serve
 accounting ipv6-a
dress port [
source { <span class
"highlight-n">loopback interface-number <sp
n class="highlight-p">| ip-address <span class
"highlight-nb">ipv6-address | <span class="high
ight-n">vlanif interface-number <span class="
ighlight-p">} | weigh
 weight-value]</s
an> *
</code></pre>
<table>
<thead>
<tr>
<th align="center">参数</th>
<th align="left">参数说明</th>
<th align="left">取值</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">ipv4-address</td>
<td align="left">指定 RADIUS 计费服务器的 IPv4 地址。</td>
<td align="left">点分十进制格式。必须是合法的单播地址。</td>

</tr>
<tr>
<td align="center">ipv6-address</td>
<td align="left">指定 RADIUS 计费服务器的 IPv6 地址。</td>
<td align="left">32 位 16 进制数，格式为 X:X:X:X:X:X:X:X。</td>
</tr>
<tr>
<td align="center">port</td>
<td align="left">指定服务器的端口号。</td>
<td align="left">整数形式，取值范围是 1～65535。</td>
</tr>
<tr>
<td align="center">vpn-instance vpn-instance-name</td>
<td align="left">指定绑定的 VPN 实例名称。</td>
<td align="left">必须是已存在的 VPN 实例名称。</td>
</tr>
<tr>
<td align="center">source loopback interface-number</td

<td align="left">指定 Loopback 接口的编号。</td>
<td align="left">必须是已存在的 Loopback 接口。</td>
</tr>
<tr>
<td align="center">source ip-address ipv4-address</td>
<td align="left">指定计费服务器的源 IPv4 地址。</td>
<td align="left">点分十进制格式，必须是合法的单播地址。</td>
</tr>
<tr>
<td align="center">source ip-address ipv6-address</td>
<td align="left">指定计费服务器的源 IPv6 地址。该地址不能为 VRRP6 虚地址。</td>
<td align="left">32 位 16 进制数，格式为 X:X:X:X:X:X:X:X。</td>
</tr>
<tr>
<td align="center">source vlanif interface-number</td>
<td align="left">指定 VLANIF 接口的 IP 地址作为源 IP 地址。其中，interface-number</
m> 表示 VLANIF 接口编号。</td>
<td align="left">必须是已存在的 VLANIF 接口。</td>
</tr>
<tr>
<td align="center">weight weight-value</td>
<td align="left">指定计费服务器的权重值。当配置了多个服务器时，设备优先通过权重值大的服务
进行计费。当权重值相等时，设备则优先通过先配置的服务器进行计费。</td>
<td align="left">整数形式，取值范围是 0～100。</td>
</tr>
</tbody>
</table>
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl"># 配置RADIUS主用计费服务器。
<span class="high
ight-p">[R1-radius
DNA] radius-serve
 accounting 10</spa
>.163<span class="h
ghlight-p">.155.</s

an>12 1813

<span class="high
ight-c"># 配置备用RADIUS计费服务器。
<span class="high
ight-p">[R1-radius
DNA] radius-serve
 accounting 10</spa
>.163<span class="h
ghlight-p">.155.</s
an>15 1813 <span c
ass="highlight-n">weight 50
</code></pre>
【4】配置 RADIUS 服务器的共享密钥
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">[R
-radius-DNA]</spa
> radius-server shared-ke
 cipher key-string<
span>
</code></pre>
<table>
<thead>
<tr>
<th align="center">参数</th>
<th align="left">参数说明</th>
<th align="left">取值</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">cipher</td>
<td align="left">以密文形式显示共享密钥。</td>
<td align="left">-</td>
</tr>
<tr>
<td align="center">key-string</td>
<td align="left">指定 RADIUS 共享密钥。</td>
<td align="left">字符串形式，不支持空格、单引号和问号，区分大小写。key***-str
ng***可以是长度为 1～128 位的明文形式，也可以是长度为 48、68、88、108、128、148、168 或
188 位的密文形式。</td>
</tr>
</tbody>
</table>
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl"># 配置RADIUS服务器的共享密钥为YsHsjx_
02206，以密文形式显示。
<span class="high
ight-p">[R1-radius
DNA] radius-serve
 shared-key cipher
/span> YsHsjx_202206
</code></pre>
同一个 RADIUS 服务器同时配置在多个 RADIUS 服务器模板下时：

如果不同 RADIUS 服务器模板下的共享密钥不同，则需要在每个 RADIUS 服务器模板视图下分配置。
如果所有 RADIUS 服务器模板下的共享密钥相同，则可以在系统视图下配置。配置命令为 radius-server ip-address { ipv4-address | ipv6-address } shared-key cipher <key-string>。
RADIUS 服务器模板视图下和系统视图下都配置 RADIUS 服务器的密钥时，系统视图下配置的 RADIUS 服务器密钥优先生效。

【5】配置 RADIUS 服务器的运算法则（可选）
当 RADIUS 服务器模板下配置多台认证或者计费服务器时，设备根据配置的运算法则和权重参数 weight，决定如何选择 RADIUS 服务器：

若选择主备算法，则权重参数 weight 决定主备，weight 值较大者为主，如果 weight 值相同，则先配置的服务器为主服务器。
如选择负载均衡算法，则权重参数 weight 决定报文的分配。

<pre><code class="language-powershell highlight-chroma">radius-server algorithm { loading-share | master-backup } [based-user]
</code></pre>
缺省情况下，RADIUS 服务器采用基于单个用户的主备运算法则。
<table>
<thead>
<tr>
<th align="center">参数</th>
<th align="left">参数说明</th>
<th align="center">取值</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">loading-share</td>
<td align="left">指定 RADIUS 服务器的运算法则为负载均衡运算法则。</td>

<td align="center">-</td>
</tr>
<tr>
<td align="center">master-backup</td>
<td align="left">指定 RADIUS 服务器的运算法则为主备运算法则。</td>
<td align="center">-</td>
</tr>
<tr>
<td align="center">based-user</td>
<td align="left">指定 RADIUS 服务器的运算法则为基于单个用户的运算法则如不指定该参数，则表示 RADIUS 服务器的运算法则为基于报文的运算法则。<td>
<td align="center">-</td>
</tr>
</tbody>

</table>
<pre><code class="language-powershell highlight-chroma"># 配置RADIUS服务器使用负载均衡运算法。
 system-view
[Huawei] radius-server template template1
[Huawei-radius-template1] radius-server algorithm loading-share
</code></pre>
【6】RADIUS 请求报文的超时重传次数和超时时间（可选）
<pre><code class="language-powershell highlight-chroma">[R-radius-DNA] radius-server { retransmit retry-times | timeout time-value } *
</code></pre>
缺省情况下，RADIUS 认证请求报文的超时重传次数为 3，超时时间是 5 秒。
<table>
<thead>
<tr>
<th align="center">参数</th>
<th align="left">参数说明</th>
<th align="left">取值</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">retransmit retry-times</td>
<td align="left">指定超时重传次数。这里的报文超时重传次数是指报文的发送次数。</td>
<td align="left">整数形式，取值范围是 1～5。</td>
</tr>
<tr>
<td align="center">timeout time-value</td>
<td align="left">指定超时时间。</td>
<td align="left">整数形式，取值范围是 1～10，单位是秒。</td>
</tr>
</tbody>
</table>
<pre><code class="language-powershell highlight-chroma"># 配置RADIUS认证请求报文的超时重传次为3，重传超时时间为2秒。
 system-view
[Huawei] radius-server <span class="highlight-

highlight-n">template test1
<span class="high
ight-p">[Huawei-radius<span class="highlight
n">-test1] radius-s
rver retransmit 3</s
an> timeout 2
</code></pre>
【7】配置设备向 RADIUS 服务器发送的报文中的用户名的格式（可选）<
p>
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">#配置设备向RADIUS服务器发送的报文中
用户名包含域名。
<span class="high
ight-p">[R1-radius
DNA] radius-serve
 user-name doma
n-included

<span class="high
ight-c">#配置设备向RADIUS服务器发送的报文中的用户名为用户原始输入的用户名，设备不对其
行修改。
<span class="high
ight-p">[R1-radius
DNA] radius-serve
 user-name origina

<span class="high
ight-c">#配置设备向RADIUS服务器发送的报文中的用户名不包含域名。
<span class="high
ight-p">[R1-radius
DNA] undo
radius-server user-name</
pan> domain-included

<span class="high
ight-c">#配置设备向RADIUS服务器发送的报文中的用户名不包含域名（除EAP认证外的其他认证方
，AR1000V无使用场景，建议不使用该命令）。
<span class="high
ight-p">[R1-radius
DNA] undo
radius-server user-name</
pan> domain-included ex
ept-eap
</code></pre>
缺省情况下，设备向 RADIUS 服务器发送的报文中的用户名为用户原始输入的用户名，设备不
其进行修改。
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl"># 设置用户名格式中不包含域名。
 <span class="hig
light-nb">system-view
<span class="high
ight-no">[Huawei] radius-server <span class=
highlight-n">template template1

[Huawei-radius-template1] undo radius-server user-name domain-included
</code></pre>
【8】配置 RADIUS 服务器的流量单位（可选）
<pre><code class="language-powershell highlight-chroma">[R-radius-DNA] radius-server traffic-unit { byte | kbyte | mbyte | gbyte }
</code></pre>
缺省情况下，设备以（byte）作为 RADIUS 流量单位。
<pre><code class="language-powershell highlight-chroma"># 使用千字节作为RADIUS流量单位。
 system-view
[Huawei] radius-server template template1
[Huawei-radius-template1] radius-server traffic-unit kbyte
</code></pre>
【9】配置重认证方式为只重认证不重授权（可选）
<pre><code class="language-powershell highlight-chroma">[R-radius-DNA] radius-attribute service-type with-authenonlyreauthen
</code></pre>
缺省情况下，重认证方式为重认证和重授权。
当 RADIUS 服务器的 Service-Type 属性为 Authenticate Only 时，该功能才可以生效。
<pre><code class="language-powershell highlight-chroma"># 配置重认证方式为只重认证不重授权。
 system-view
[Huawei] radius-server template test
[Huawei-radius-test] radius-attribute service-type with-authenonly-reauthen

</code></pre>

【10】启用 Framed-IP-Address 的功能（可选）
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">[R
-radius-DNA]</spa
> radius-server framed-ip
/span>-address no-user</s
an>-ip enable
</code></pre>
缺省情况下，当用户发送的 RADIUS 认证请求报文中没有携带用户 IP 地址时，未使能设备在 RA
IUS 认证请求报文中封装 RADIUS 属性 Framed-IP-Address 的功能。
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl"># 当用户发送的RADIUS认证请求报文中没
携带用户IP地址时，使能设备在RADIUS认证请求报文中封装RADIUS属性Framed-IP-Address的功
。
 <span class="hig
light-nb">system-view
<span class="high
ight-no">[Huawei] radius-server <span class=
highlight-n">template template1
<span class="high
ight-p">[Huawei-radius<span class="highlight
n">-template1] rad
us-server framed-ip
address no-user-ip
/span> enable
</code></pre>
<h3 id="配置AAA方案-">配置 AAA 方案</h3>
背景信息
用户使用的认证、授权和计费方法通过 AAA 方案来定义。如果使用 RADIUS 方式进行认证、授权和
费，需要在认证方案中配置认证模式为 RADIUS 认证，在计费方案中配置计费模式为 RADIUS 计费。
ADIUS 认证与授权结合，不能分离，认证成功授权也成功。所以不需要配置授权方案</str
ng>，仅需配置认证方案和计费方案。
为避免单一认证模式无响应而造成的认证失败，一般会在认证方案中配置本地认证或不认证为备
认证模式。
注：如果使用 <code>authentication-mode</code>命令配置认证方式为不认证，则当用户
线时，用户输入任意的用户名和密码后都会认证成功。因此，为保护设备或网络安全，建议开启认证
式，保证用户经过认证后才可以访问设备或网络。
<h4 id="-1-配置认证方案-">【1】配置认证方案</h4>
（1）进入 AAA 视图
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">[R1] <span class="highlight-n
>aaa
</code></pre>

（2）创建一个认证方案并进入认证方案视图，或者直接进入一个已经存在的认证方案视图
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">[R
-aaa] authenticatio
-scheme scheme-name
</code></pre>
缺省情况下，设备中有两个认证方案，认证方案名称分别是 default 和 radius，default 和 radiu
方案均不能删除，只能修改方案下的参数。

（3）配置认证模式为 RADIUS 认证
<pre><code class="language-powershell highlight-chroma">#配置为RADIUS认证
[R1-aaa-authen-rz] authentication-mode radius

#如果需要配置本地认证为备份认证模式，请执行命令
[R1-aaa-authen-rz] authentication-mode radius local | local-case }
</code></pre>
缺省情况下，认证模式为本地认证。

（4）配置用户在服务器认证无响应转入本地认证后，设备不发送计费或授权报文（可选）
<pre><code class="language-powershell highlight-chroma">[R-aaa-authen-rz] undo server no-response { accounting | authorization }
</code></pre>
缺省情况下，在配置了服务器计费的情况下，用户在服务器认证无响应转入本地认证后，设备不送计费报文。

（5）配置管理员用户在 RADIUS 认证拒绝后转入本地认证（可选）
该功能仅对管理员用户生效。实现该功能认证模式必须为 RADIUS+ 本地认证。
<pre><code class="language-powershell highlight-chroma">[R-aaa-authen-rz] radius-reject local
</code></pre>
缺省情况下，未配置管理员用户在 RADIUS 认证拒绝后转入本地认证。在 RADIUS 认证拒绝后即 RADIUS 服务器回应 Access-Reject 报文），认证流程结束，用户认证失败。

（6）配置账号锁定功能（可选）
<pre><code class="language-powershell highlight-chroma">#开启接入用户远端认证失败后账号锁定功

[R1-aaa]access-user remote authen-fail retry-interval retry-interval retry-time retry-time block-time block-time

<span class="high
ight-c">#开启管理员用户远端认证失败后账号锁定功能
<span class="high
ight-p">[R1-aaa]</
pan>administrator remote</
pan> authen-fail retry-inte
val retry-interval r
try-time retry-time <span class="highlight-nb"
block-time block-time
</code></pre>
缺省情况下，接入用户远端认证失败后账号锁定功能处于关闭状态；管理员用户远端认证失败后
号锁定功能处于开启状态，并且，远端认证失败后用户的重试时间间隔为 5 分钟，连续认证失败的限
次数为 30 次，账号锁定时间为 5 分钟。
<table>
<thead>
<tr>
<th align="center">参数</th>
<th align="center">参数说明</th>
<th align="center">取值</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">retry-interval retry-interval</td>
<td align="center">指定远端认证失败后用户的重试时间间隔。</td>
<td align="center">整数形式，取值范围为 5～65535，单位为分钟。</td>
</tr>
<tr>
<td align="center">retry-time retry-time</td>
<td align="center">指定接入用户连续认证失败的限制次数。</td>
<td align="center">整数形式，取值范围为 3～65535。</td>
</tr>
<tr>
<td align="center">block-time block-time</td>
<td align="center">指定接入用户帐号的锁定时间。</td>
<td align="center">整数形式，取值范围为 5～65535，单位为分钟。</td>
</tr>
</tbody>
</table>
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl"># 开启接入和管理员用户远端认证失败后账
锁定功能：
<span class="high
ight-c"># - 远端认证失败后用户的重试时间间隔为5分钟
<span class="high
ight-c"># - 连续认证失败的限制次数为3次、账号锁定时间为5分钟

<span class="high
ight-no">[Huawei] aaa
<span class="high
ight-p">[Huawei-aaa<span class="highlight-p
>] access-user rem
te authen-fail retr

-interval 5 retry-ti
e 3 block-time</sp
n> 5
<span class="high
ight-p">[Huawei-aaa<span class="highlight-p
>] administrator re
ote authen-fail ret
y-interval 5 retry-t
me 3 block-time</
pan> 5
</code></pre>

<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">#配置在用户账号锁定期间，允许该用户使
指定的IP地址访问网络
<span class="high
ight-p">[R1-aaa]</
pan> aaa-quiet administrat
r except-list {</spa
> ipv4-address | <
pan class="highlight-nb">ipv6-address } <1<span class="hi
hlight-p">-32></
pan>
</code></pre>
缺省情况下，用户在账号锁定期间不能访问网络。

<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">#将认证失败的远端认证账号解锁
<span class="high
ight-p">[R1-aaa]</
pan> remote-user authen-
ail unblock {
all | <span class="hi
hlight-n">username username <span class="hi
hlight-p">}
</code></pre>

（7）配置当 RADIUS 服务器下发的 Session-Timeout 为 0 时，设备不对用户进行下线或重认
（可选）
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">[R
-aaa] aaa-author</
pan> session-timeout inval
d-value enable
</code></pre>
缺省情况下，当 Radius 服务器下发的 Session-Timeout 属性值为 0 时，该属性不生效。

（8）配置认证旁路时间（可选）
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">[R1] <span class="highlight-n
">aaa-authen-bypass <span class="highlight-n
>enable time time-
alue

</code></pre>
缺省情况下，未启用旁路认证功能。
<table>
<thead>
<tr>
<th align="center">参数</th>
<th align="center">参数说明</th>
<th align="center">取值</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">enable</td>
<td align="center">使能远端认证旁路功能。</td>
<td align="center">-</td>
</tr>
<tr>
<td align="center">time time-value</td>
<td align="center">指定认证旁路时间。</td>
<td align="center">整数形式，单位为分钟，取值范围为 1～1440。</td>
</tr>
</tbody>
</table>
<pre><code class="language-powershell highlight-chroma"># 配置认证旁路时间为3分钟。
[Huawei] aaa-authen-bypass enable time 3
</code></pre>

<h4 id="-2-配置计费方案">【2】配置计费方案</h4>

（1）进入 AAA 视图
<pre><code class="language-powershell highlight-chroma">[R1] aaa
</code></pre>

（2）创建一个计费方案，并进入计费方案视图或直接进入一个已存在的计费方案视图
<pre><code class="language-powershell highlight-chroma">[R-aaa] accounting-scheme
</code></pre>
缺省情况下，设备中有一个计费方案，计费方案配置名是 default，default 方案不能删除，只修改 default 方案下的参数。

（3）配置计费模式为 RADIUS 计费
<pre><code class="language-powershell highlight-chroma">[R-aaa-accounting-jf] accounting-mode radius

</code></pre>
缺省情况下，不计费，即计费模式为 none。

（4）配置计费失败策略

开始计费失败策略

<pre><code class="language-powershell highlight-chroma">#配置开始计费失败策略
[R1-aaa-accounting-jf] accounting start-fail { offline | online }
</code></pre>
缺省情况下，如果开始计费失败，不允许用户上线。

实时计费失败策略

<pre><code class="language-powershell highlight-chroma">#使能实时计费并设置计费间隔
[R1-aaa-accounting-jf] accounting realtime
</code></pre>
缺省情况下，设备按时长计费，未使能实时计费功能。
<pre><code class="language-powershell highlight-chroma">#配置允许的实时计费请求最大无响应次数以及实时计费失败后采取的策略
[R1-aaa-accounting-jf] accounting interim-fail [max-times times] { offline | online }
</code></pre>
缺省情况下，允许的实时计费请求最大无响应次数为 3 次，实时计费失败后允许用户在线。

结束计费失败策略

<pre><code class="language-powershell highlight-chroma">#进入RADIUS服务器模板视图
[R1] radius-server template
</code></pre>
<pre><code class="language-powershell highlight-chroma">#配置计费结束报文的重传功能以及可重发计费结束报文个数
<span class="high

ight-p">[R1-radius-addius-server] radis-server accounting-stop-packet resend
 resend-times]</san>
</code></pre>
缺省情况下，允许重发计费结束报文，且计费结束报文的重发次数为 3。

<h3 id="创建域和配置域">创建域和配置域</h3>
背景信息
NAS 设备对用户的管理是基于域的，每个用户都属于一个域，一个域是由属于同一个域的用户成的群体。简单地说，用户属于哪个域就使用哪个域下的 AAA 配置信息。
设备根据用户名决定用户所属的域。对用户进行认证、授权和计费前，需要先创建用户所属的域
操作步骤
（1）进入 AAA 视图
<pre><code class="language-powershell highlight-chroma"><pan class="highlight-cl">[R1] aaa
</code></pre>
（2）用来创建域，并进入域视图
<pre><code class="language-powershell highlight-chroma"><pan class="highlight-cl">[R-aaa] domain</spa> domain-name [span class="highlight-nb">domain-index domain-inde]
</code></pre>
缺省情况下，设备上存在名为“default”和“default_admin”两个域。可以修改这两个域下的置，但是不能删除这两个域。
<table>
<thead>
<tr>
<th align="center">参数</th>
<th align="center">参数说明</th>
<th align="center">取值</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">domain-name</td>
<td align="center">指定域名。</td>
<td align="center">字符串形式，不区分大小写，长度范围是 1～64，不支持空格，不能仅配置为“”或“--”，且不能包含字符“*” “?” “”” 。</td>
</tr>
<tr>
<td align="center">domain-index domain-index</td>
<td align="center">指定域的索引。</td>
<td align="center">整数形式，取值范围是 0～255。</td>
</tr>
</tbody>
</table>
<pre><code class="language-powershell highlight-chroma"><

pan class="highlight-cl">#创建名称为domain1的域，并进入域视图<
span>
 <span class="hig
light-nb">system-view
<span class="high
ight-no">[Huawei] aaa
<span class="high
ight-p">[Huawei-aaa<span class="highlight-p
>] domain domain1
/span>
<span class="high
ight-p">[Huawei-aaa<span class="highlight-n
>-domain-domain1]
</code></pre>

（3）配置域的状态（可选）
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">[H
awei-aaa-domain-domain1<span class="highlig
t-p">] state {</span
active | <span class
"highlight-n">block [<span class="highlight-nb
>time-range time-name <span class="highligh
-p">&<1<span class="highlight-err">-<
span>4> <span c
ass="highlight-p">] }
</code></pre>
缺省情况下，域创建后处于激活状态。当域处于阻塞状态时，属于该域的用户不能登录。
<table>
<thead>
<tr>
<th align="center">参数</th>
<th align="center">参数说明</th>
<th align="center">取值</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">active</td>
<td align="center">指定域为激活态。</td>
<td align="center">-</td>
</tr>
<tr>
<td align="center">block</td>
<td align="center">指定域为阻塞态。</td>
<td align="center">-</td>
</tr>
<tr>
<td align="center">time-range time-name</td>
<td align="center">指定域为阻塞态的时间段。其中，time-name 表示域为阻塞状
的时间段名称。如果不指定时间段，表示任何时间都为阻塞态。</td>
<td align="center">字符串形式，区分大小写，必须以英文字母开头，长度范围是 1～32。但为避
混淆，时间段的名字不可以使用英文单词 all。</td>
</tr>

</tbody>
</table>
（4）使能域用户的流量统计功能（可选）
<pre><code class="language-powershell highlight-chroma">[Hawei-aaa-domain-domain1] statistic enable
</code></pre>
缺省情况下，域用户的流量统计功能处于未使能状态。

（5）配置域名解析方案，对设备上所有域都有效（可选）
<pre><code class="language-powershell highlight-chroma">[Hawei-aaa] domainname-parse-direction { left-to-right | right-to-left }
</code></pre>
缺省情况下，域名解析方向为从左向右。
<table>
<thead>
<tr>
<th align="center">参数</th>
<th align="center">参数说明</th>
<th align="center">取值</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">left-to-right</td>
<td align="center">指定域名解析方向为从左向右。</td>
<td align="center">-</td>
</tr>
<tr>
<td align="center">right-to-left</td>
<td align="center">指定域名解析方向为从右向左。</td>
<td align="center">-</td>
</tr>
</tbody>
</table>
（6）配置域名分隔符和位置（可选）
<pre><code class="language-powershell highlight-chroma">#配置域名分隔符（默认为@）
[R1-aaa]domain-name-delimiter delimiter
#配置域名的位置（缺省情况下，域名在分隔符后）
[R1-aaa]domain-location {</sp

n> after-delimiter |
before-delimiter }
</code></pre>
注：认证模板下也支持配置域名方案，如果在 AAA 视图和认证模板视图下都配置了域名解析方
，则优先使用认证模板下的配置。认证模板下的配置仅适用于无线用户。
<table>
<thead>
<tr>
<th align="center">参数</th>
<th align="center">参数说明</th>
<th align="center">取值</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">delimiter</td>
<td align="center">指定安全字符串分隔符。</td>
<td align="center">枚举类型，只能是 1 位，取值范围： “\”， “/”， “:”， “<”， “>
，”｜“， “%”， “@”， “*”， “'” </td>
</tr>
<tr>
<td align="center">after-delimiter</td>
<td align="center">指定域名在分隔符后。</td>
<td align="center">-</td>
</tr>
<tr>
<td align="center">before-delimiter</td>
<td align="center">指定域名在分隔符前。</td>
<td align="center">-</td>
</tr>
</tbody>
</table>

（7）配置安全字符串功能（可选）
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">#使能安全字符串功能（默认启用）</span

<span class="high
ight-p">[R1-aaa]</
pan> security-name enable
/span>

<span class="high
ight-c">#配置安全字符串分隔符（默认为*，Identifier character \ / : < > | @ ' % * ）</spa
>
<span class="high
ight-p">[R1-aaa]</
pan> security-name-delimit
r delimiter
</code></pre>
注：认证模板下也支持配置安全字符串，如果在 AAA 视图和认证模板视图下都配置了安全字符
，则优先使用认证模板下的配置。认证模板下的配置仅适用于无线用户。
<table>
<thead>

<tr>
<th align="center">参数</th>
<th align="center">参数说明</th>
<th align="center">取值</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">delimiter</td>
<td align="center">指定安全字符串分隔符。</td>
<td align="center">枚举类型，只能是 1 位，取值范围：“\”，“/”，“:”，“<”，“>”，”｜”，“%”，“@”，“*”，“'”</td>
</tr>
</tbody>
</table>

<h3 id="配置全局默认域">配置全局默认域</h3>
背景信息
设备根据用户的用户名决定用户所属的域。当用户名中没有携带域名、设备无法确认用户所属的域时将用户加入到全局默认域中。根据用户类型的不同（接入用户或者管理员用户），全局默认域又分为局默认普通域和全局默认管理域。
操作步骤
（1）配置全局默认域
<pre><code class="language-powershell highlight-chroma">#配置全局默认普通域
[R1]domain domain-name

#配置全局默认管理域
[R1]domain domain-name admin
</code></pre>
缺省情况下，全局默认域有两个：全局默认普通域“default”和全局默认管理域“default_admin”。
<table>
<thead>
<tr>
<th align="center">参数</th>
<th align="center">参数说明</th>
<th align="center">取值</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">domain-name</td>
<td align="center">指定全局默认域的域名。</td>
<td align="center">必须是已存在的域名。</td>
</tr>
<tr>
<td align="center">admin</td>
<td align="center">表示配置指定的域为管理域。如果不指定此参数，则表示配置全局默认普通域</td>

</td>
<td align="center">-</td>
</tr>
</tbody>
</table>
注：全局默认普通域和全局默认管理域可以配置为同一个域。

<h3 id="在域下应用AAA方案-RADIUS服务器模板和授权信息">在域下应用 AAA 方案、RADIUS 务器模板和授权信息</h3>
背景信息
域统一管理 AAA 方案、服务器模板等配置信息，另外，域下还可以配置授权信息。用户属于哪个域使用哪个域下的 AAA 配置信息。
操作步骤

（1）创建域并进入域视图或进入一个已存在的域视图
<pre><code class="language-powershell highlight-chroma"><pan class="highlight-cl">[R-aaa] domain</spa> domain-name [span class="highlight-nb">domain-index domain-inde]
[R1-aaa-domain-yu]
</code></pre>
缺省情况下，设备存在两个域：“default”和“default_admin”。“default”用于普通接入户的域，“default_admin”用于管理员的域。

（2）配置域下应用的认证方案
<pre><code class="language-powershell highlight-chroma"><pan class="highlight-cl">[R-aaa-domain-yu]</san> authentication-scheme <span class="highlight-nb>scheme-name
</code></pre>
缺省情况下，“default”域使用名为“radius”的认证方案，“default_admin”域使用名为“efault”的认证方案，其他域使用名为“radius”的认证方案。

（3）配置域下应用的计费方案
<pre><code class="language-powershell highlight-chroma"><pan class="highlight-cl">[R-aaa-domain-yu]</san> accounting-scheme acounting-scheme-name
</code></pre>
缺省情况下，域使用名为“default”的计费方案。“default”计费方案的策略为：计费模式为计费，关闭实时计费开关。

（4）配置域下应用的 RADIUS 服务器模板
<pre><code class="language-powershell highlight-chroma"><pan class="highlight-cl">[R-aaa-domain-yu]</san> radius-server templat-name

</code></pre>
缺省情况下，“default”域下绑定了名为“default”的 RADIUS 服务器模板，“default_admi
”域下没有绑定 RADIUS 服务器模板，其他域下绑定了名为“default”的 RADIUS 服务器模板。</
>

（5）开启 RADIUS 计费报文抄送功能并配置二级计费 RADIUS 服务器模板（可选）
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">[R
-aaa-domain-yu]</s
an> accounting-copy radi
s-server template-name
</code></pre>
缺省情况下，未开启 RADIUS 计费报文抄送功能。

（6）域下配置授权信息
<pre><code class="highlight-chroma"><span class="highlight
cl"> :字母/Number_1_96px: 配置对域下的用户下发用户组授权
</code></pre>
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">[R
-aaa-domain-yu]</s
an> user-group group-na
e
</code></pre>
缺省情况下，未配置对域下的用户下发用户组授权。

<pre><code class="highlight-chroma"><span class="highlight
cl"> :字母/Number_2_96px: 配置对域下的用户下发业务方案授权
</code></pre>
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">[R
-aaa-domain-yu]</s
an> service-scheme servic
-scheme-name
</code></pre>
缺省情况下，未配置对域下的用户下发业务方案授权。
<h2 id="验证命令">验证命令</h2>
<h3 id="查看RADIUS服务器模板的配置信息">查看 RADIUS 服务器模板的配置信息</h3>
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">display <span class="highlight-
b">radius-server configuration <span class="hi
hlight-p">[template <span class="highlight-nb
>template-name]
</code></pre>
<table>
<thead>
<tr>
<th align="center">参数</th>
<th align="center">参数说明</th>
<th align="center">取值</th>
</tr>
</thead>
<tbody>
<tr>

```
<td align="center"><strong>template</strong> <em>template-name</em></td>
<td align="center">指定 <strong>RADIUS</strong> 服务器模板的名称。如果不指定此参数则
示所有 <strong>RADIUS</strong> 服务器模板的配置信息。</td>
<td align="center">必须是已存在的 <strong>RADIUS</strong> 服务器模板名称。</td>
</tr>
</tbody>
</table>
<pre><code class="language-powershell highlight-chroma"><span class="highlight-line"><
pan class="highlight-cl"><span class="highlight-c"># 查看名称为shiva的RADIUS服务器模板
配置信息。</span>
</span></span><span class="highlight-line"><span class="highlight-cl">
</span></span><span class="highlight-line"><span class="highlight-cl"> <span class="hig
light-n">display</span> <span class="highlight-nb">radius-server</span> <span class="hi
hlight-n">configuration</span> <span class="highlight-n">template</span> <span class="
ighlight-n">shiva</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-p">------------------------------------------------------------------------------</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Server-template</span><span class="highlight-n">-name</span>        <span c
ass="highlight-err">:</span>  <span class="highlight-n">shiva</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Server-template</span><span class="highlight-n">-index</span>        <span cl
ss="highlight-err">:</span>  <span class="highlight-n">1</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Protocol-version</span>            <span class="highlight-err">:</span>  <span c
ass="highlight-n">standard</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Traffic-unit</span>                <span class="highlight-err">:</span>  <span clas
="highlight-n">B</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Shared-secret</span><span class="highlight-n">-key</span>           <span clas
="highlight-err">:</span>  <span class="highlight-p">******</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Group-filter</span>               <span class="highlight-err">:</span>  <span clas
="highlight-n">class</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Timeout-interval</span><span class="highlight-p">(</span><span class="highl
ght-k">in</span> <span class="highlight-n">second</span><span class="highlight-p">)</
pan>  <span class="highlight-err">:</span>  <span class="highlight-n">5</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-n">Retransmission</span>             <span class="highlight-err">:</span>  <span cla
s="highlight-n">2</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-n">EndPacketSendTime</span>           <span class="highlight-err">:</span>  <span
class="highlight-n">0</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-n">Dead</span> <span class="highlight-n">time</span><span class="highlight-p">
</span><span class="highlight-k">in</span> <span class="highlight-n">minute</span><s
an class="highlight-p">)</span>         <span class="highlight-err">:</span>  <span class="
ighlight-n">5</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Domain-included</span>             <span class="highlight-err">:</span>  <span
lass="highlight-n">YES</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
```

hlight-nb">NAS-IP-Address <span clas
="highlight-err">: -
 <span class="hi
hlight-nb">Calling-station-id <span class="highl
ght-nb">MAC-format : <span class="highligh
-nb">xxxx-xxxx-xxxx
 <span class="hi
hlight-nb">Called-station-id <span class="highl
ght-nb">MAC-format : <span class="highligh
-n">XX.XX<
pan class="highlight-p">.XX<span class="highli
ht-p">.XX.<
pan class="highlight-n">XX.<span class="highli
ht-n">XX
 <span class="hi
hlight-nb">NAS-Port-ID <span class="highlight
n">format : <span class="highlight-n"
New
 <span class="hi
hlight-nb">Service-type : <span cla
s="highlight-p">-
 <span class="hi
hlight-nb">NAS-IPv6-Address <span cla
s="highlight-err">: ::
 <span class="hi
hlight-n">Server algorithm <span class
"highlight-err">: master-backup
 <span class="hi
hlight-nb">Detect-interval(<span class="highlig
t-k">in second)</sp
n> : 60
 <span class="hi
hlight-n">Detect up-server<span class="highli
ht-p">(in second</s
an>) : <span clas
="highlight-n">0
 <span class="hi
hlight-n">Detect timeout<span class="highlight
p">(in second</spa
>) : <span class
"highlight-n">3
 <span class="hi
hlight-nb">Testuser-username : <span
class="highlight-n">test
 <span class="hi
hlight-nb">Testuser-ciperpwd : <span
lass="highlight-p">%^%#.5*EDl^j_WXg[#Z>plj8;k|8.s*
u<_F~g9k`0*9%^%#
 <span class="hi
hlight-nb">Chargeable-user-identity <span c
ass="highlight-err">: Not <span class="highlig
t-n">Support
 <span class="hi
hlight-n">CUI Not re

ect : No<
span>
  <span class="hi
hlight-n">Enable framed-ip<span class="highl
ght-n">-address : <span class="highlight-
">Yes
  <span class="hi
hlight-n">Authentication Server <span class="h
ghlight-n">1 :
0.7<span cl
ss="highlight-p">.66
66 Port<
pan class="highlight-err">:1812 <span class="h
ghlight-n">Weight:<span class="highlight-n"
80 [up]

  Vrf:<span class=
highlight-p">- LoopBack<span class="highlight
err">:NULL Vlanif</
pan>:NULL

  Source IP<span cl
ss="highlight-err">: ::
  <span class="hi
hlight-n">Authentication Server <span class="h
ghlight-n">2 :
0.7<span cl
ss="highlight-p">.66
67 Port<
pan class="highlight-err">:1812 <span class="h
ghlight-n">Weight:<span class="highlight-n"
80 [up]

  Vrf:<span class=
highlight-p">- LoopBack<span class="highlight
err">:NULL Vlanif</
pan>:NULL

  Source IP<span cl
ss="highlight-err">: ::
  <span class="hi
hlight-n">Accounting Server <span class="hi
hlight-n">1 : 1
.7<span cla
s="highlight-p">.66
66 Port<
pan class="highlight-err">:1813 <span class="h
ghlight-n">Weight:<span class="highlight-n"
80 [up]

  Vrf:<span class=
highlight-p">- LoopBack<span class="highlight
err">:NULL Vlanif</
pan>:NULL

```
</span></span><span class="highlight-line"><span class="highlight-cl">
    <span class="highlight-n">Source</span> <span class="highlight-n">IP</span><span cl
ss="highlight-err">:</span> <span class="highlight-p">::</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-n">Accounting</span> <span class="highlight-n">Server</span>     <span class="hi
hlight-n">2</span>       <span class="highlight-err">:</span>  <span class="highlight-n">1
</span><span class="highlight-p">.</span><span class="highlight-n">7</span><span cla
s="highlight-p">.</span><span class="highlight-n">66</span><span class="highlight-p">
</span><span class="highlight-n">67</span>     <span class="highlight-n">Port</span><
pan class="highlight-err">:</span><span class="highlight-n">1813</span>  <span class="h
ghlight-n">Weight</span><span class="highlight-err">:</span><span class="highlight-n"
80</span>  <span class="highlight-no">[up]</span>
</span></span><span class="highlight-line"><span class="highlight-cl">
    <span class="highlight-n">Vrf</span><span class="highlight-err">:</span><span class=
highlight-p">-</span> <span class="highlight-n">LoopBack</span><span class="highlight
err">:</span><span class="highlight-n">NULL</span> <span class="highlight-n">Vlanif</
pan><span class="highlight-err">:</span><span class="highlight-n">NULL</span>
</span></span><span class="highlight-line"><span class="highlight-cl">
    <span class="highlight-n">Source</span> <span class="highlight-n">IP</span><span cl
ss="highlight-err">:</span> <span class="highlight-p">::</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-p">------------------------------------------------------------------------------</span>
</span></span></code></pre>
<table>
<thead>
<tr>
<th align="center">项目</th>
<th align="left">描述</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center"><strong>Server</strong>-template-name</td>
<td align="left"><strong>RADIUS</strong> 服务器模板的名称。通过 <strong>radius</stron
>-<em>server template</em> 命令配置。</td>
</tr>
<tr>
<td align="center"><strong>Server</strong>-template-index</td>
<td align="left"><strong>RADIUS</strong> 服务器模板的索引。</td>
</tr>
<tr>
<td align="center">Protocol-version</td>
<td align="left"><strong>RADIUS</strong> 协议的版本：</td>
</tr>
</tbody>
</table>
<ul>
<li>standard</li>
<li>huawei</li>
<li>iphotel</li>
<li>portal<br>
|<br>
|Traffic-unit|<strong>RADIUS</strong> 服务器模板的流量单位：</li>
<li>B：字节</li>
```

KB：千字节
MB：兆（Mega）字节
GB：吉（Giga）字节
通过 radius-server traffic-unit 命令配置。
|
|Shared-secret-key|RADIUS 服务器模板的共享密钥。通过 radius-server shared-key 配置。|
|Group-filter| 用户组过滤字段，目前仅支持使用 class 字段作为组过滤字段。|
|Timeout-interval(in second)|RADIUS 应答超时时间。通过 radius-server retransmit timeout 命令配置。|
|Retransmission|RADIUS 重传次数。通过 radius-server retransmit timeout 命令配置。|
|EndPacketSendTime|RADIUS 计费停止报文重传次数。通过 radius-server accounting-stop-packet resend 命令配置。|
|Dead time(in minute)|RADIUS 主用服务器恢复激活状态的时间。通过 radius-server retransmit timeout 命令配置。|
|Domain-included|RADIUS 用户名格式，指定用户名是否包含域名。
YES：表示用户名包含域名。
NO：表示用户名不包含域名。
Original：用户原始输入的用户名，设备不对其进行修改。
通过 radius-server user-name domain-included 命令配置。
|
|NAS-IP-Address|RADIUS 报文中 NAS-IP-Address 属性值。|
|Calling-station-id MAC-format|RADIUS 报文 calling-station-id 属性 MAC 地址的封装格式。|
|Called-station-id MAC-format|RADIUS 报文 called-station-id 属性 MAC 址的封装格式。通过 called-station-id mac-format 命令配置。|
|NAS-Port-ID format|RADIUS 服务器 NAS 端口 ID 的形式。
New：指定采用新的 NAS 端口 ID 形式。
Old：指定采用旧的 NAS 端口 ID 形式。
通过 radius-server nas-port-id-format 命令配置。
|
|Service-type| 服务类型。|
|NAS-IPv6-Address|RADIUS 报文中 NAS-IPv6-Address 属性值。|
|Server algorithm|RADIUS 服务器的运算法则。
master-backup：表示 RADIUS 服务器的运算法则为基于报文的主备运算则。
master-backup based-user：表示 RADIUS 服务器的运算法则为基于单用户的主备运算法则。
loading-share：表示 RADIUS 服务器的运算法则为基于报文的负载均衡算法则。
loading-share based-user：表示 RADIUS 服务器的运算法则为基于单个户的负载均衡运算法则。
通过 radius-server algorithm 命令配置。
|
|Detect-interval(in second)| 对 Down 状态的 RADIUS 服务器的自动探测周。通过 radius-server ****detect-****serve 命令配置。|
|Detect up-server(in second)| 对 Up 状态的 RADIUS 务器的自动探测周期。通过 radius-server detect-server up-server inteval 命令配置。|
|Detect timeout(in second)|RADIUS 服务器自动探测报文的超时等待时间。过 radius-server detect-server timeout 命令配置。|

|Chargeable-user-identity| 设备是否支持 CUI 属性。取值包括：
Not Support：设备不支持 CUI 属性。
Support：设备支持 CUI 属性。
通过 radius-server support chargeable-user-identity 令配置。
|
|CUI Not reject| 设备是否不处理 CUI 属性。取值包括：
No：设备处理 CUI 属性。
Yes：设备不处理 CUI 属性。
通过 radius-server support chargeable-user-identity 命令配。
|
|Enable framed-ip-address| 当用户发送的 RADIUS 认证请求报文中没有携带户 IP 地址时，是否使能设备在 RADIUS 认证请求报文中封装 RADIU 属性 Framed-IP-Address 的功能。取值包括：
No：未使能。
Yes：已使能。
通过 radius-server framed-ip-address no-user-ip enable 命配置。
|
|Testuser-username|RADIUS 服务器自动探测用户名。通过 radius-server testuser 命令配置。|
|Testuser-ciperpwd|RADIUS 服务器自动探测用户密码。通过 radiu-server testuser 命令配置。|
|Authentication Server 1|RADIUS 主用认证服务器的 IP 地址、端口号、权重值、状态、VPN 实例、源接口以及源 IP 地址。通过 radius server authentication 命令配置。|
|Authentication Server 2|RADIUS 备用认证服务器的 IP 地址、端口号、权重值、状态、VPN 实例、源接口以及源 IP 地址。通过 radius server authentication 命令配置。|
|Accounting Server 1|RADIUS 主用计费服务器的 IP 地、端口号、权重值、状态、VPN 实例、源接口以及源 IP 地址。通过 radius-<m>server accounting 命令配置。|
|Accounting Server 2|RADIUS 备用计费服务器的 IP 地、端口号、权重值、状态、VPN 实例、源接口以及源 IP 地址。通过 radius-<m>server accounting 命令配置。|

<h3 id="查看RADIUS服务器会话管理功能的配置信息">查看 RADIUS 服务器会话管理功能的配置息</h3>

<h3 id="测试RADIUS服务器的连通性">测试 RADIUS 服务器的连通性</h3>
<pre><code class="language-powershell highlight-chroma"><pan class="highlight-cl">#(所有视图)测试设备与认证服务器或计费务器的连通性，认证服务器或计费服务器是否可以正常对用户进行认证或计费。
test-aaa user-name user-password radius-template <san class="highlight-nb">template-name [chap | pap]

test-aaa user-name user-password radius-template <s

an class="highlight-nb">template-name [accounting [start | realtime | stop]]

test-aaa user-name user-password hwtacacs-template template-name [accounting [start | realtime | stop]]
</code></pre>

参数	参数说明	取值
user-name	指定用户名。	字符串形式，不区分大小写，长度范围是 1～253。
	说明：探测 HWTACACS 服务器或 RADIUS 服务器时，用户名中不支持空。	
user-password	指定用户密码。	字符串形式，区分大小写，长度范围是 1～128。
radius-template template-name	指定 RADIUS 服务器模板名称。	RADIUS 服务器模板必须已经存在。
chap	指定认证方式为 CHAP 认证。NAS 设备把用户名和加密后的密码，以及一个 16	节随机码传给 RADIUS 服务器。RADIUS 服务器根据用户名查找数据库得到密码，然后根据收到的 16

字节的随机码对密码进行加密，将其结果与传来的密码作比较，如果相同表明验证通过，如果不相同明验证失败。另外如果验证成功，RADIUS 服务器同样可以生成一个 16 字节的随机码对用户进行询（Challenge）。</td>
<td align="center">-</td>
</tr>
<tr>
<td align="center">pap</td>
<td align="left">指定认证方式为 PAP 认证。NAS 设备把用户名和加密后的密码放到验证请求包的应属性中传递给 RADIUS 服务器。根据 RADIUS 服务器的返回结果来决定是否允许用户上线。</td>
<td align="center">-</td>
</tr>
<tr>
<td align="center">accounting</td>
<td align="left">指定计费。默认发送的计费报文是开始计费报文。</td>
<td align="center">-</td>
</tr>
<tr>
<td align="center">start</td>
<td align="left">指定发送的报文是开始计费报文。</td>
<td align="center">-</td>
</tr>
<tr>
<td align="center">realtime</td>
<td align="left">指定发送的报文是实时计费报文。</td>
<td align="center">-</td>
</tr>
<tr>
<td align="center">stop</td>
<td align="left">指定发送的报文是停止计费报文。</td>
<td align="center">-</td>
</tr>
<tr>
<td align="center">hwtacacs-template template-name</t
>
<td align="left">指定 HWTACACS 服务器模板名称。</td>
<td align="center">HWTACACS 服务器模板必须已经存在。</td>
</tr>
</tbody>
</table>
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">
<span class="high
ight-c">#前提：（已在RADIUS服务器上配置了测试用户wakin@huawei.com，用户密码为wakin）

<span class="high
ight-c">#测试用户wakin@huawei.com是否能够通过R1-radius的认证
<span class="high
ight-nb">test-aaa wakin<span class="highlight-
v">@huawei.com</
pan> wakin radius-templat
 R1-radius

<span class="high
ight-n">Info: Acco

nt test succeed</sp
n>.

<span class="high
ight-c">#不正确的情况
<span class="high
ight-nb">test-aaa aaa<span class="highlight-nv
>@huawei.com</sp
n> aaa radius-template</sp
n> R1-radius

<span class="high
ight-n">Info: User
/span> name or <sp
n class="highlight-n">password is <span class=
highlight-n">wrong.
</code></pre>
<h3 id="查看-AAA-的概要信息">查看 AAA 的概要信息</h3>
（1）查看 AAA 的概要信息，如域、认证方案、授权方案、计费方案的使
情况（所有视图）
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl"> display <span class="highlight
n">aaa configuration

<span class="high
ight-c"># 查看AAA的概要信息。

 <span class="hig
light-n">display aaa
onfiguration
 <span class="hi
hlight-n">Domain Name <span class="highlight
n">Delimiter : <span class="highlig
t-p">@
 <span class="hi
hlight-n">Domainname parse <span class="high
ight-n">direction : <span class="highli
ht-n">Left to right</
pan>
 <span class="hi
hlight-n">Domainname location <s
an class="highlight-err">: After-delimiter

 <span class="hi
hlight-n">Administrator user <span class="highl
ght-k">default domain <span class="highli
ht-err">: default_admin
 <span class="hi
hlight-n">Normal user <span class="highlight-k
>default domain <span class="highlight
err">: default
 <span class="hi
hlight-n">Domain : <span
class="highlight-n">total: <span class="highli

ht-n">256 used:
/span> 2
  <span class="hi
hlight-nb">Authentication-scheme :
total: <span class=
highlight-n">33 used<span class="highlight-
rr">: 2
  <span class="hi
hlight-nb">Accounting-scheme :
total: <span class=
highlight-n">32 used<span class="highlight-
rr">: 1
  <span class="hi
hlight-nb">Authorization-scheme :
total: <span class=
highlight-n">32 used<span class="highlight-
rr">: 1
  <span class="hi
hlight-nb">Service-scheme : <
pan class="highlight-n">total: <span class="hi
hlight-n">256 used<span class="highlight-err
>: 1
  <span class="hi
hlight-nb">Recording-scheme :
span class="highlight-n">total: <span class="h
ghlight-n">32 used<span class="highlight-er
">: 0
  <span class="hi
hlight-nb">Local-user : <spa
 class="highlight-n">total: <span class="highli
ht-n">512 used:
/span> 3
  <span class="hi
hlight-nb">Local-user block <span class="highli
ht-nb">retry-interval : <span class="highl
ght-n">5 Min(</spa
>s)
  <span class="hi
hlight-nb">Local-user block <span class="highli
ht-nb">retry-time : <span class="highli
ht-n">3
  <span class="hi
hlight-nb">Local-user block <span class="highli
ht-n">time : <span class="highlight
n">5 Min(<
pan class="highlight-n">s)
  <span class="hi
hlight-nb">Remote-admin-user <span class="h
ghlight-n">block retry-interval <span class="h
ghlight-err">: 5 Min
/span>(s<span clas
="highlight-p">)
  <span class="hi
hlight-nb">Remote-admin-user <span class="h

ghlight-n">block retry-time <span class="h
ghlight-err">: 30
 <span class="hi
hlight-nb">Remote-admin-user <span class="h
ghlight-n">block time <span class="highl
ght-err">: 5 Min</s
an>(s<span class="h
ghlight-p">)
 <span class="hi
hlight-n">Session timeout <span class="highlig
t-n">invalid enable <span class="highlight
err">: No
</code></pre>
<table>
<thead>
<tr>
<th align="center">项目</th>
<th align="left">描述</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">Domain Name Delimiter</td>
<td align="left">域名分隔符，可以是 \ / : < > | @ ' %中的某一个。缺省是 @。</td>
</tr>
<tr>
<td align="center">通过 domain-name-delimiter 命令配置。</td>
<td align="left"></td>
</tr>
<tr>
<td align="center"></td>
<td align="left"></td>
</tr>
<tr>
<td align="center">Domain</td>
<td align="left">域的数目。</td>
</tr>
</tbody>
</table>

total：可以创建的域总数。
used：已经创建的域数目。
|
|Domainname parse direction| 域名的解析方向。
Left to right：从左到右解析。
Right to left：从右到左解析。
通过 domainname-parse-direction 命令配置。
|
|Domainname location| 域名的位置。
After-delimiter：域名在分隔符后。
Before-delimiter：域名在分隔符前。
通过 domain-location 命令配置。
|
|Administrator user default domain| 管理用户默认域。|

|Normal user default domain| 普通用户默认域。|
|Authentication-scheme| 认证方案数目。
total：可以创建的认证方案总数。
used：已经创建的认证方案数目。
|
|Accounting-scheme| 计费方案数目。
total：可以创建的计费方案总数。
used：已经创建的计费方案数目。
|
|Authorization-scheme| 授权方案数目。
total：可以创建的授权方案总数。
used：已经创建的授权方案数目。
|
|Service-scheme| 业务方案数目。
total：可以创建的业务方案总数。
used：已经创建的业务方案数目。
|
|Recording-scheme| 记录方案数目。
total：可以创建的记录方案总数。
used：已经创建的记录方案数目。
|
|Local-user| 本地用户数目。
total：可以创建的本地用户总数。
used：已经创建的本地用户数目。
|
|Local-user block retry-interval| 本地账号用户的重试时间间隔。
通过 local-aaa-user wrong-password 命令配置。
|
|Local-user block retry-time| 本地账号连续认证失败的限制次数。
通过 local-aaa-user wrong-password 命令配置。
|
|Local-user block time| 本地账号的锁定时间。
通过 local-aaa-user wrong-password 命令配置。
|
|Remote-access-user block retry-interval| 远端认证失败的接入用户的重试时间间隔。
通过 access-user remote authen-fail 命令配置。
|
|Remote-access-user block retry-time| 远端认证失败的接入用户连续认证失败的限制次数。
通过 access-user remote authen-fail 命令配置。
|
|Remote-access-user block time| 远端认证失败的接入用户的锁定时间。
通过 access-user remote authen-fail 命令配置。
|
|Remote-admin-user block retry-interval| 远端认证失败的管理员用户的重试时间间隔。
通过 administrator remote authen-fail 命令配置。
|
|Remote-admin-user block retry-time| 远端认证失败的管理员用户连续认证失败的限制次数。
通过 administrator remote authen-fail 命令配置。
|
|Remote-admin-user block time| 远端认证失败的管理员用户的锁定时间。
通过 administrator remote authen-fail 命令配置。
|
|Session timeout invalid enable| 通过 aaa-author session-timeout invalid-value enab
e 命令配置。

Yes：当 Radius 服务器下发的 Session-Timeout 为 0 时，设备不对用户进行下线或重认证。</l
>
No：当 Radius 服务器下发的 Session-Timeout 为 0 时，设备对用户进行下线或重认证。
|
|Navigator first login state| 出厂设备首次登录状态。|

<h3 id="查看认证方案的配置信息">查看认证方案的配置信息</h3>
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">display <span class="highlight-
b">authentication-scheme [<span class="highl
ght-nb">authentication-scheme-name <span cl
ss="highlight-p">]
</code></pre>
<table>
<thead>
<tr>
<th align="center">参数</th>
<th align="center">参数说明</th>
<th align="center">取值</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">authentication***-scheme</em
-name*</td>
<td align="center">指定查看的认证方案名称。</td>
<td align="center">必须为已存在的认证方案名称。</td>
</tr>
</tbody>
</table>
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl"># 查看所有认证方案的摘要信息。
 <span class="hig
light-n">display authentication-scheme
 <span class="hi
hlight-p">---
 <span class="hig
light-nb">Authentication-scheme-name <
pan class="highlight-nb">Authentication-method sc
eme-index
 <span class="hi
hlight-p">---
 <span class="hi
hlight-k">default Local
0
 <span class="hi
hlight-n">radius RADIUS
1
 <span class="hi
hlight-p">---
 <span class="hi
hlight-n">Total of au
hentication scheme
 2

```
</span></span><span class="highlight-line"><span class="highlight-cl">
</span></span><span class="highlight-line"><span class="highlight-cl"><span class="high
ight-c"># 查看配置名为default的认证方案的详细配置信息。</span>
</span></span><span class="highlight-line"><span class="highlight-cl"> <span class="hig
light-n">display</span> <span class="highlight-nb">authentication-scheme</span> <span
lass="highlight-k">default</span>
</span></span><span class="highlight-line"><span class="highlight-cl">

</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Authentication-scheme</span><span class="highlight-n">-name</span>
span class="highlight-err">:</span> <span class="highlight-k">default</span>

</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Authentication-method</span>              <span class="highlight-err">:</span>
span class="highlight-n">Local</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-n">server</span> <span class="highlight-nb">no-response</span> <span class="hi
hlight-n">accounting</span>      <span class="highlight-err">:</span> <span class="highli
ht-n">NO</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-n">server</span> <span class="highlight-nb">no-response</span> <span class="hi
hlight-n">authorization</span>    <span class="highlight-err">:</span> <span class="highl
ght-n">NO</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-n">Location</span> <span class="highlight-n">after</span> <span class="highlight
n">radius</span> <span class="highlight-n">reject</span>      <span class="highlight-err
>:</span> <span class="highlight-n">None</span>
</span></span></code></pre>
<table>
<thead>
<tr>
<th align="center">项目</th>
<th align="left">描述</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center"><strong>scheme</strong>-index</td>
<td align="left">方案索引。</td>
</tr>
<tr>
<td align="center"><strong>Authentication</strong>-<strong>scheme</strong>-name</
d>
<td align="left">认证方案的名称。通过**authentication-scheme（AAA 视图）**命令配置。</t
>
</tr>
<tr>
<td align="center"><strong>Authentication</strong>-method</td>
<td align="left">认证方案的认证模式。通过 <strong>authentication</strong>-mode（认证方
视图）命令配置。</td>
</tr>
<tr>
<td align="center">server no-response accounting</td>
<td align="left">用户在服务器认证无响应转入本地认证后，设备是否继续发送计费报文。取值包括
```

</td>
</tr>
</tbody>
</table>

YES：设备继续发送计费报文。
NO：设备不发送计费报文。
通过 server no-response accounting 命令配置。
|
|server no-response authorization| 用户在服务器认证无响应转入本地认证后，设备是否继续发送权报文。取值包括：
YES：设备继续发送授权报文。
NO：设备不发送授权报文。
通过 server no-response authorization 命令配置。
|
|Location after radius reject|RADIUS 认证拒绝后，转入的下一种认证方式。取值包括：
None：未配置下一种认证方式，认证结束。
Local：转入本地认证。
通过 radius-reject local 命令配置。
|

<p></p>
<h3 id="查看计费方案的配置情况">查看计费方案的配置情况</h3>
<pre><code class="language-powershell highlight-chroma">display accounting-scheme [accounting-scheme-name]
</code></pre>
<table>
<thead>
<tr>
<th align="center">参数</th>
<th align="center">参数说明</th>
<th align="center">取值</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">accounting-scheme-name</td>
<td align="center">指定查看的计费方案名称。</td>
<td align="center">必须为已存在的计费方案名称。</td>
</tr>
</tbody>
</table>
<pre><code class="language-powershell highlight-chroma"># 查看所有计费方案的摘要信息。
 display accounting-scheme

 Accounting-scheme-name   Accounting-method   <span class="highlight-nb">sc

```
eme-index</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-p">----------------------------------------------------------------</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-k">default</span>                    <span class="highlight-n">None</span>
        <span class="highlight-n">0</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-n">radius</span><span class="highlight-p">-</span><span class="highlight-n">1<
span>                  <span class="highlight-n">RADIUS</span>                  <span clas
="highlight-n">1</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-n">tacas</span><span class="highlight-p">-</span><span class="highlight-n">1</
pan>                  <span class="highlight-n">HWTACACS</span>                  <span cl
ss="highlight-n">3</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-n">haca</span><span class="highlight-p">-</span><span class="highlight-n">1</s
an>                  <span class="highlight-n">HACA</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-p">----------------------------------------------------------------</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-n">Total</span> <span class="highlight-n">of</span> <span class="highlight-nb">
ccounting-scheme</span><span class="highlight-err">:</span> <span class="highlight-n"
4</span>
</span></span><span class="highlight-line"><span class="highlight-cl">
</span></span><span class="highlight-line"><span class="highlight-cl">
</span></span><span class="highlight-line"><span class="highlight-cl"><span class="high
ight-c"># 查看系统缺省的计费方案的详细配置信息。</span>
</span></span><span class="highlight-line"><span class="highlight-cl">display accounting-scheme default
</span></span><span class="highlight-line"><span class="highlight-cl">
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Accounting-scheme</span><span class="highlight-n">-name</span>
span class="highlight-err">:</span> <span class="highlight-k">default</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Accounting-method</span>                  <span class="highlight-err">:</span>
span class="highlight-n">None</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Realtime-accounting</span><span class="highlight-n">-switch</span>          <
pan class="highlight-err">:</span> <span class="highlight-n">Disabled</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Realtime-accounting</span><span class="highlight-n">-interval</span><span c
ass="highlight-p">(</span><span class="highlight-n">min</span><span class="highlight-
">)</span>    <span class="highlight-err">:</span> <span class="highlight-p">-</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Start-accounting</span><span class="highlight-n">-fail-policy</span>          <s
an class="highlight-err">:</span> <span class="highlight-n">Offline</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Realtime-accounting</span><span class="highlight-n">-fail-policy</span>
span class="highlight-err">:</span> <span class="highlight-n">Online</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Realtime-accounting</span><span class="highlight-n">-failure-retries</span>
<span class="highlight-err">:</span> <span class="highlight-n">3</span>
</span></span></code></pre>
```

<table>
<thead>
<tr>
<th align="center">项目</th>
<th align="left">描述</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">scheme-index</td>
<td align="left">方案索引。</td>
</tr>
<tr>
<td align="center">Accounting-scheme-name</td>
<td align="left">计费方案的名称。通过**accounting-scheme（AAA 视图）**命令创建。</td>
</tr>
<tr>
<td align="center">Accounting-method</td>
<td align="left">此计费方案配置的计费模式。计费模式如下：</td>
</tr>
</tbody>
</table>

HWTACACS：HWTACACS 服务器计费。
None：不计费。
RADIUS：RADIUS 服务器计费。
HACA：HACA 服务器计费。
通过 accounting-mode 命令配置。
|
|Realtime-accounting-switch| 是否启用实时计费功能。实时计费开关有两种状态：
Disabled：关闭，不进行实时计费。
Enabled：打开，进行实时计费。
通过 accounting realtime 命令配置。
|
|Realtime-accounting-interval(min)| 实时计费间隔。通过 accounting realtime</stron
> 命令配置。|
|Start-accounting-fail-policy| 开始计费失败后对用户采取的策略：
Offline：使用户下线。
Online：保持用户在线。
通过 accounting start-fail 命令配置。
|
|Realtime-accounting-fail-policy| 实时计费失败后对用户采取的策略：
Offline：使用户下线。
Online：保持用户在线。
通过 accounting interim-fail 命令配置。
|
|Realtime-accounting-failure-retries| 确认为实时计费失败前系统尝试实时计费的次数。通过 <stro
g>accounting interim-fail 命令配置。|

<h3 id="查看授权方案的配置信息">查看授权方案的配置信息</h3>
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">display <span class="highlight-
b">authorization-scheme [<span class="highli

ht-nb">authorization-scheme-name <span clas
="highlight-p">]
</code></pre>
<table>
<thead>
<tr>
<th align="center">参数</th>
<th align="center">参数说明</th>
<th align="center">取值</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">authorization-scheme-name</td>
<td align="center">指定查看的授权方案名称。</td>
<td align="center">必须为已存在的授权方案名称。</td>
</tr>
</tbody>
</table>
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl"># 查看授权方案的摘要信息。
 <span class="hig
light-n">display authorization-scheme
 <span class="hi
hlight-p">---
 <span class="hi
hlight-nb">Authorization-scheme-name <
pan class="highlight-nb">Authorization-method s
heme-index
 <span class="hi
hlight-p">---
 <span class="hi
hlight-k">default Local
0
 <span class="hi
hlight-n">scheme0 Local
1
 <span class="hi
hlight-p">---
 <span class="hi
hlight-n">Total of
uthorization-scheme: <span class="highlight-n
>2

<span class="high
ight-c"># 查看名为scheme0的授权方案的详细配置信息。
 <span class="hig
light-n">display authorization-scheme <span c
ass="highlight-n">scheme0
<span class="high
ight-p">---
 <span class="hig
light-nb">Authorization-scheme-name <span c

ass="highlight-err">: scheme0
 <span class="hig
light-nb">Authorization-method : <span c
ass="highlight-n">Local
 <span class="hig
light-nb">Authorization-cmd level <span class
"highlight-n">0 :
isabled
 <span class="hig
light-nb">Authorization-cmd level <span class
"highlight-n">1 :
isabled
 <span class="hig
light-nb">Authorization-cmd level <span class
"highlight-n">2 :
isabled
 <span class="hig
light-nb">Authorization-cmd level <span class
"highlight-n">3 :
isabled
 <span class="hig
light-nb">Authorization-cmd level <span class
"highlight-n">4 :
isabled
 <span class="hig
light-nb">Authorization-cmd level <span class
"highlight-n">5 :
isabled
 <span class="hig
light-nb">Authorization-cmd level <span class
"highlight-n">6 :
isabled
 <span class="hig
light-nb">Authorization-cmd level <span class
"highlight-n">7 :
isabled
 <span class="hig
light-nb">Authorization-cmd level <span class
"highlight-n">8 :
isabled
 <span class="hig
light-nb">Authorization-cmd level <span class
"highlight-n">9 :
isabled
 <span class="hig
light-nb">Authorization-cmd level <span class=
highlight-n">10 : <span class="highlight-n"
Disabled
 <span class="hig
light-nb">Authorization-cmd level <span class=
highlight-n">11 : <span class="highlight-n"
Disabled
 <span class="hig
light-nb">Authorization-cmd level <span class=

highlight-n">12 : <span class="highlight-n"
Disabled
 <span class="hig
light-nb">Authorization-cmd level <span class=
highlight-n">13 : <span class="highlight-n"
Disabled
 <span class="hig
light-nb">Authorization-cmd level <span class=
highlight-n">14 : <span class="highlight-n"
Disabled
 <span class="hig
light-nb">Authorization-cmd level <span class=
highlight-n">15 : <span class="highlight-n"
Disabled
 <span class="hig
light-nb">Authorization-cmd no-response<sp
n class="highlight-n">-policy : <span class=
highlight-n">Online
<span class="high
ight-p">---
</code></pre>
<table>
<thead>
<tr>
<th align="center">项目</th>
<th align="left">描述</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">scheme-index</td>
<td align="left">方案索引。</td>
</tr>
<tr>
<td align="center">Authorization-scheme-name</td>
<td align="left">授权方案的名称。通过**authorization-scheme（AAA 视图）**命令配置。</td>
</tr>
<tr>
<td align="center">Authorization-method</td>
<td align="left">授权方案配置的授权模式。通过 authorization-mode 命令
置。</td>
</tr>
<tr>
<td align="center">Authorization-cmd level</td>
<td align="left">该级别用户是否使能了按命令行授权功能。</td>
</tr>
</tbody>
</table>

Disabled：没有使能按命令行授权功能。
Enabled：使能了按命令行授权功能。
通过 authorization-cmd 命令配置。
|
|Authorization-cmd no-response-policy| 按命令行授权失败时的策略：允许用户上线。|

<h3 id="查看认证失败的远端认证账号的信息">查看认证失败的远端认证账号的信息</h3>
<pre><code class="language-powershell highlight-chroma">display remote-user authen-fail [blocked | username username]
</code></pre>
<table>
<thead>
<tr>
<th align="center">参数</th>
<th align="center">参数说明</th>
<th align="center">取值</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">blocked</td>
<td align="center">显示所有已被锁定的远端认证账号。</td>
<td align="center">-</td>
</tr>
<tr>
<td align="center">username username</td>
<td align="center">显示指定的认证失败的远端认证账号的详细信息。如果不指定 username 参数，表示显示所有认证失败的远端认证账号的基本信息。</td>
<td align="center">字符串形式，不支持空格，不区分大小写，长度范围是 1～253。</td>
</tr>
</tbody>
</table>
<pre><code class="language-powershell highlight-chroma"># 查看所有认证失败的AAA远端认证账号。
display remote-user authen-fail
Interval: Retry Interval(Mins)
TimeLeft: Retry Time Left
BlockDuration: Block Duration(Mins)

```
hlight-n">Username</span>                <span class="highlight-n">Interval</span>  <span c
ass="highlight-n">TimeLeft</span>  <span class="highlight-n">BlockDuration</span>  <sp
n class="highlight-n">UserType</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-p">-------------------------------------------------------------------------------
/span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-n">www</span><span class="highlight-nv">@test</span>                <span class="
ighlight-n">0</span>       <span class="highlight-n">0</span>       <span class="highligh
-n">65414</span>       <span class="highlight-n">administrator</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-p">-------------------------------------------------------------------------------
/span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-n">Total</span> <span class="highlight-n">1</span><span class="highlight-p">,</
pan> <span class="highlight-n">1</span> <span class="highlight-n">printed</span>
</span></span><span class="highlight-line"><span class="highlight-cl">
</span></span><span class="highlight-line"><span class="highlight-cl"><span class="high
ight-c"># 查看所有被锁定的AAA远端认证账号。</span>
</span></span><span class="highlight-line"><span class="highlight-cl"> <span class="hig
light-n">display</span> <span class="highlight-nb">remote-user</span> <span class="hig
light-nb">authen-fail</span> <span class="highlight-n">blocked</span>
</span></span><span class="highlight-line"><span class="highlight-cl"><span class="high
ight-n">Interval</span><span class="highlight-err">:</span> <span class="highlight-n">Re
ry</span> <span class="highlight-n">Interval</span><span class="highlight-p">(</span><
pan class="highlight-n">Mins</span><span class="highlight-p">)</span>
</span></span><span class="highlight-line"><span class="highlight-cl"><span class="high
ight-n">TimeLeft</span><span class="highlight-err">:</span> <span class="highlight-n">
etry</span> <span class="highlight-n">Time</span> <span class="highlight-n">Left</spa
>
</span></span><span class="highlight-line"><span class="highlight-cl"><span class="high
ight-n">BlockDuration</span><span class="highlight-err">:</span> <span class="highlight
n">Block</span> <span class="highlight-n">Duration</span><span class="highlight-p">(<
span><span class="highlight-n">Mins</span><span class="highlight-p">)</span>
</span></span><span class="highlight-line"><span class="highlight-cl"><span class="high
ight-p">-------------------------------------------------------------------------------
----------</span>
</span></span><span class="highlight-line"><span class="highlight-cl"><span class="high
ight-n">Username</span>                <span class="highlight-n">Interval</span>  <span cl
ss="highlight-n">TimeLeft</span>  <span class="highlight-n">BlockDuration</span>  <spa
 class="highlight-n">BlockTime</span>                <span class="highlight-n">UserType</sp
n>
</span></span><span class="highlight-line"><span class="highlight-cl"><span class="high
ight-p">-------------------------------------------------------------------------------
----------</span>
</span></span><span class="highlight-line"><span class="highlight-cl"><span class="high
ight-n">www</span><span class="highlight-nv">@test</span>                <span class="hi
hlight-n">0</span>       <span class="highlight-n">0</span>       <span class="highlight-
">65414</span>       <span class="highlight-n">2018</span><span class="highlight-p">
</span><span class="highlight-n">04</span><span class="highlight-p">-</span><span cl
ss="highlight-n">23</span> <span class="highlight-n">17</span><span class="highlight-e
r">:</span><span class="highlight-n">22</span><span class="highlight-err">:</span><spa
n class="highlight-n">09</span><span class="highlight-p">+</span><span class="highlig
t-n">08</span><span class="highlight-err">:</span><span class="highlight-n">00</span>
```

administrator
<span class="high
ight-p">----------
<span class="high
ight-n">Total 1,</sp
n> 1 printed

<span class="high
ight-c"># 查看认证失败的AAA远端认证账号“test”的详细信息。
 <span class="hig
light-n">display remote-user <span class="hig
light-nb">authen-fail username <span class="hi
hlight-n">test
 <span class="hi
hlight-n">The contents <span class="highlight-
">of the user</span
:
 <span class="hi
hlight-nb">User-type : <span class="hi
hlight-n">Administrator
 <span class="hi
hlight-n">Retry interval<span class="highlight-
">(Mins) <
pan class="highlight-err">: 29
 <span class="hi
hlight-n">Retry time
eft : 4
 <span class="hi
hlight-n">Block time <span class="highlight-n"
left(Mins<s
an class="highlight-p">) : <span class="highli
ht-n">0
 <span class="hi
hlight-n">User state <span class="highli
ht-err">: Block
</code></pre>
<table>
<thead>
<tr>
<th align="center">项目</th>
<th align="left">描述</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">Username</td>
<td align="left">用户名。</td>
</tr>
<tr>
<td align="center">Interval 或 Retry interval(Mins)</td>
<td align="left">用户的重试时间间隔，单位是分钟。通过命令 access-user remote aut
en-fail 或命令 administrator remote authen-fail 配置。</td>

</tr>
<tr>
<td align="center">TimeLeft 或 Retry Time Left</td>
<td align="left">用户连续认证失败的剩余限制次数。通过命令 access-user remote aut
en-fail 或命令 administrator remote authen-fail 配置。 </td>
</tr>
<tr>
<td align="center">BlockDuration 或 Block time left(Mins)</td>
<td align="left">用户帐号的锁定时间，单位是分钟。通过命令 access-user remote aut
en-fail 或命令 administrator remote authen-fail 配置。 </td>
</tr>
<tr>
<td align="center">UserType</td>
<td align="left">用户类型，取值包括： </td>
</tr>
</tbody>
</table>

administrator：管理员用户。
access-user：接入用户。
|
|BlockTime| 用户帐号的锁定时刻。|
|Block time left(Mins)| 用户帐号的剩余锁定时间。|
|User-state| 用户的状态：
Block：该用户处于锁定状态。
Active：该用户处于活跃状态。
|

<h3 id="查看在用户账号锁定期间-允许该用户访问网络使用的IP地址">查看在用户账号锁定期间，
许该用户访问网络使用的 IP 地址</h3>
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">display <span class="highlight-
b">aaa-quiet administrator <span class="highli
ht-nb">except-list
<span class="high
ight-c"># 查看在用户账号锁定期间，允许该用户访问网络使用的IP地址。

 <span class="hig
light-n">display aaa-quiet <span class="highli
ht-n">administrator except-list
 <span class="hig
light-p">----------
 <span class="hig
light-n">Admin silent <span class="highlight-n
>whitelist #白名单内配置的IP地址
 <span class="hig
light-p">----------
 <span class="hig
light-n">10.2</spa
>.2<span class="hig
light-p">.1
 <span class="hig

light-n">10.2</spa
>.2<span class="hig
light-p">.2
 <span class="hig
light-p">--
 <span class="hig
light-n">Total: 2</
pan>, printed<span
lass="highlight-err">: 2
</code></pre>
<h3 id="查看按照指定标准查看在线用户的概要信息">查看按照指定标准查看在线用户的概要信息</
3>
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">display <span class="highlight-
b">access-user [do
ain domain-name |
/span> interface interface-t
pe interface-number <span class="highlight-p
>[vlan vlan-id</sp
n> [qinq <span clas
="highlight-nb">qinq-vlan-id <span class="high
ight-p">]] |
ip-address ip-address</sp
n> [vpn-instance
span class="highlight-nb">vpn-instance-name
span class="highlight-p">] | <span class="highli
ht-nb">ipv6-address ipv6-address <span class
"highlight-p">| access-slot <span class="highli
ht-nb">slot-id | use
-group user-group
name | username</s
an> user-name] <
pan class="highlight-p">[detail <span class="h
ghlight-p">] 、
<span class="high
ight-n">display access-user <span class="highl
ght-p">[mac-address <span class="highlight-
b">mac-address | s
rvice-scheme service-scheme<span class="high
ight-n">-name | us
r-id user-id |</spa
> statistics | <span c
ass="highlight-n">ssid ssid-name <span class
"highlight-p">]
<span class="high
ight-n">display access-user <span class="highl
ght-nb">access-type { <span class="highlight-n
>admin [ftp
| ssh <span class="h
ghlight-p">| telnet |
/span> terminal | <s
an class="highlight-n">web] <span class="highl
ght-p">| ppp |</spa
> l2tp } <span class

"highlight-p">[username <span class="highligh
-nb">user-name]
</code></pre>
<table>
<thead>
<tr>
<th align="center">参数</th>
<th align="left">参数说明</th>
<th align="center">取值</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">domain domain-name</td>
<td align="left">指定根据域名查看用户信息。</td>
<td align="center">必须是已存在的域名。</td>
</tr>
<tr>
<td align="center">interface interface-type interface
number</td>
<td align="left">指定根据接口查看用户信息。</td>
<td align="center"></td>
</tr>
</tbody>
</table>

interface-type：接口类型。
<table>
<thead>
<tr>
<th>interface-number：接口编号。</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan vlan-id [qinq qinq-vlan-
d]</td>
</tr>
</tbody>
</table>

vlan-id：VLAN ID。如果是 QinQ VLAN，表示内层 VLAN ID。
qinq-vlan-id：表示外层 VLAN ID。
|vlan-id 和 qinq-vlan-id：整数形式，取值范围是 1～4094。|
|ip-address ip-address| 指定根据 IP 地址查看用户信息。
说明：当用户类型为 NAC 用户时，则显示详细用户信息；其他类型用户则显示简要用户信息。<b
>
| 点分十进制格式。|
|vpn-instance vpn-instance-name| 指定 IP 地址所属的 VPN
例。| 必须是已存在的 VPN 实例。|
|ipv6-address ipv6-address| 指定根据 IPv6 地址查看用户信息。
总长度为 128 位，通常分为 8 组，每组为 4 个 16 进制数的形式，格式为 X:X:X:X:X:X:X:X。|
|mac-address mac-address| 指定根据 MAC 地址查看用户信息
| 格式为 H-H-H。其中 H 为 4 位的十六进制数。|

|service-scheme service-scheme-name| 根据业务方案查看用。| 必须为已经存在的业务方案。|
|access-slot slot-id| 指定根据接口板查看用户信息。| 接口板槽号，取值范围根据设备的型号确定。|
|ssid ssid-name| 指定服务组合识别码。| 已存在的 SSID 名。|
|statistics| 指定查看设备上用户的统计信息：
Historical wireless user statistics：指定查看设备上历史的 WLAN 用户的统计信息。
<table>
<thead>
<tr>
<th>Current online user statistics：指定查看设备上当前在线的所有用户的统计信息。</th>
</tr>
</thead>
<tbody>
<tr>
<td>user-group user-group-name</td>
</tr>
<tr>
<td>user-id user-id</td>
</tr>
<tr>
<td>username user-name</td>
</tr>
<tr>
<td>detail</td>
</tr>
<tr>
<td>access-type</td>
</tr>
<tr>
<td>admin [ftp | ssh | elnet | terminal | web]</td>
</tr>
<tr>
<td> ftp：FTP 用户。</td>
</tr>
<tr>
<td> ssh：SSH 用户。</td>
</tr>
<tr>
<td> telnet：Telnet 用户。</td>
</tr>
<tr>
<td> terminal：Terminal 用户。</td>
</tr>
<tr>
<td> web：Web 用户。</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>

```
</tr>
<tr>
<td><strong>ppp</strong></td>
</tr>
<tr>
<td><strong>l2tp</strong></td>
</tr>
</tbody>
</table>
</li>
</ul>
<h3 id="查看域的配置信息">查看域的配置信息</h3>
<pre><code class="language-powershell highlight-chroma"><span class="highlight-line"><
pan class="highlight-cl"><span class="highlight-n">display</span> <span class="highlight-
">domain</span> <span class="highlight-p">[</span> <span class="highlight-n">name</
pan> <span class="highlight-nb">domain-name</span> <span class="highlight-p">]</spa
>
</span></span></code></pre>
<table>
<thead>
<tr>
<th align="center">参数</th>
<th align="center">参数说明</th>
<th align="center">取值</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center"><strong>name</strong> <em>domain-name</em></td>
<td align="center">指定查看的域名。如果不指定域名，则显示所有域的摘要信息。</td>
<td align="center">必须为已存在的域名。</td>
</tr>
</tbody>
</table>
<pre><code class="language-powershell highlight-chroma"><span class="highlight-line"><
pan class="highlight-cl"><span class="highlight-c"># 查看当前所有存在的域的配置信息。</sp
n>
</span></span><span class="highlight-line"><span class="highlight-cl">
</span></span><span class="highlight-line"><span class="highlight-cl"> <span class="hig
light-n">display</span> <span class="highlight-n">domain</span>
</span></span><span class="highlight-line"><span class="highlight-cl"> <span class="hi
hlight-p">------------------------------------------------------------------------</span>
</span></span><span class="highlight-line"><span class="highlight-cl"> <span class="hi
hlight-n">index</span> <span class="highlight-n">DomainName</span>
</span></span><span class="highlight-line"><span class="highlight-cl"> <span class="hi
hlight-p">------------------------------------------------------------------------</span>
</span></span><span class="highlight-line"><span class="highlight-cl"> <span class="hi
hlight-n">0</span> <span class="highlight-k">default</span>
</span></span><span class="highlight-line"><span class="highlight-cl"> <span class="hi
hlight-n">1</span> <span class="highlight-n">default_admin</span>
</span></span><span class="highlight-line"><span class="highlight-cl"> <span class="hi
hlight-p">------------------------------------------------------------------------</span>
</span></span><span class="highlight-line"><span class="highlight-cl"> <span class="hi
hlight-n">Total</span><span class="highlight-err">:</span> <span class="highlight-n">2<
```

span>
</code></pre>
<table>
<thead>
<tr>
<th align="center">项目</th>
<th align="left">描述</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">index</td>
<td align="left">域的索引。通过**domain（AAA 视图）**命令置。</td>
</tr>
<tr>
<td align="center">DomainName</td>
<td align="left">域的名称。通过**domain（AAA 视图）**命令置。</td>
</tr>
</tbody>
</table>
<pre><code class="language-powershell highlight-chroma"><pan class="highlight-cl"># 查看default域的配置信息。
 display domain name default

  Domain-name   : <spanlass="highlight-k">default
  Domain-index   : 0
  Domain-state   : Active
  Authentication-scheme-name   <san class="highlight-err">: default
  Accounting-scheme-name   <spn class="highlight-err">: default
  Authorization-scheme-name   <san class="highlight-err">: -
  Service-scheme-name   <span

```
class="highlight-err">:</span> <span class="highlight-p">-</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">RADIUS-server</span><span class="highlight-n">-template</span>          <span
class="highlight-err">:</span> <span class="highlight-p">-</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">HWTACACS-server</span><span class="highlight-n">-template</span>        <s
an class="highlight-err">:</span> <span class="highlight-p">-</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">User-group</span>                    <span class="highlight-err">:</span> <span cl
ss="highlight-p">-</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Push-url</span><span class="highlight-n">-address</span>               <span cla
s="highlight-err">:</span> <span class="highlight-p">-</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-n">Domain</span> <span class="highlight-n">auto</span> <span class="highlight-
">block</span> <span class="highlight-nb">Time-range</span>    <span class="highlight-
rr">:</span> <span class="highlight-n">asd</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Flow-statistic</span>                <span class="highlight-err">:</span> <span cla
s="highlight-n">enable</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Tariff-level</span>
</span></span><span class="highlight-line"><span class="highlight-cl">   <span class="hi
hlight-nb">Qos-profile</span>                   <span class="highlight-err">:</span> <span cla
s="highlight-n">huawei</span>
</span></span><span class="highlight-line"><span class="highlight-cl">   <span class="hi
hlight-nb">Accounting-flag</span>               <span class="highlight-err">:</span> <span c
ass="highlight-n">enable</span>
</span></span></code></pre>
<table>
<thead>
<tr>
<th align="center">项目</th>
<th align="left">描述</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">Domain-name</td>
<td align="left">域的名称。</td>
</tr>
<tr>
<td align="center">通过**domain（AAA 视图）**命令配置。</td>
<td align="left"></td>
</tr>
<tr>
<td align="center"></td>
<td align="left"></td>
</tr>
<tr>
<td align="center">Domain-index</td>
<td align="left">域的索引。</td>
</tr>
<tr>
```

<td align="center">通过**domain（AAA 视图）**命令配置。</td>
<td align="left"></td>
</tr>
<tr>
<td align="center"></td>
<td align="left"></td>
</tr>
<tr>
<td align="center">Domain-state</td>
<td align="left">域的状态，其中：</td>
</tr>
</tbody>
</table>

Active 表示激活状态。
Block 表示阻塞状态。
通过 state（AAA 域视图）命令配置。
|
|Authentication-scheme-name| 域使用的认证方案名称。
通过authentication-scheme（AAA 域视图）命令配置。
|
|Accounting-scheme-name| 域使用的计费方案名称。
通过accounting-scheme（AAA 域视图）命令配置。
|
|Authorization-scheme-name| 域使用的授权方案名称。
通过authorization-scheme（AAA 域视图）命令配置。
|
|Service-scheme-name| 域使用的业务方案名称。
通过service-scheme（AAA 域视图）命令配置。
|
|RADIUS-server-template| 域使用的 RADIUS 服务器模板名称。
通过radius-server（AAA 域视图）命令配置。
|
|HWTACACS-server-template| 域使用的 HWTACACS 服务器模板名称。
通过hwtacacs-server命令配置。
|
|User-group| 域使用的用户组授权。
通过**user-group（AAA 域视图）**命令配置。
|
|Push-url-address| 域使用的强推 URL。|
|Domain auto block Time-range| 域自动阻塞的时间段。|
|Flow-statistic| 域用户的流量统计功能是否使能：
enable：使能。
-：未使能。
通过**statistic enable（AAA 域视图）**命令配置。
|
|Tariff-level| 费率级别。|
|Qos-profile| 费率级别对应的 QoS 模板。|
|Accounting-flag| 费率级别对应的计费功能是否使能：
enable：使能。
disable：未使能。
|

<h3 id="查看本地用户的属性信息">查看本地用户的属性信息</h3>

<pre><code class="language-powershell highlight-chroma">display local-user [domain domain-name | state { active | block } | username username] *
</code></pre>

参数	参数说明	取值
domain *domain-name*	查看指定域下的本地用户属性。	必须是已存在的域名。
state { **active**	**block** }	根据状态查看本地用户属性。	

- **active**：激活态。
- **block**：阻塞态。
||
|**username** *user-name*| 查看指定用户名的本地用户属性。| 必是已存在的用户名。|

<pre><code class="language-powershell highlight-chroma"># 查看所有本地用户的概要信息。
 display local-user

  User-name   State AuthMask AdminLevel
  ----
  user-a   A   A   0
  user-c   A   A

```
s="highlight-n">A</span>        <span class="highlight-n">0</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-p">--------------------------------------------------------------------------------</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-n">Total</span> <span class="highlight-n">2</span> <span class="highlight-n">us
r</span><span class="highlight-p">(</span><span class="highlight-n">s</span><span cla
s="highlight-p">)</span>
</span></span><span class="highlight-line"><span class="highlight-cl">
</span></span><span class="highlight-line"><span class="highlight-cl"><span class="high
ight-c"># 查看本地用户user-a的详细信息。</span>
</span></span><span class="highlight-line"><span class="highlight-cl"> <span class="hig
light-n">display</span> <span class="highlight-nb">local-user</span> <span class="highli
ht-n">username</span> <span class="highlight-nb">user-a</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-n">The</span> <span class="highlight-n">contents</span> <span class="highlight-
">of</span> <span class="highlight-n">local</span> <span class="highlight-n">user</spa
><span class="highlight-p">(</span><span class="highlight-n">s</span><span class="hig
light-p">)</span><span class="highlight-err">:</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-n">Password</span>          <span class="highlight-err">:</span> <span class="high
ight-p">****************</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-n">State</span>             <span class="highlight-err">:</span> <span class="highli
ht-n">active</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Service-type</span><span class="highlight-n">-mask</span>    <span class="h
ghlight-err">:</span> <span class="highlight-n">A</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-n">Privilege</span> <span class="highlight-n">level</span>      <span class="highli
ht-err">:</span> <span class="highlight-p">-</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Ftp-directory</span>       <span class="highlight-err">:</span> <span class="hi
hlight-p">-</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Access-limit</span>        <span class="highlight-err">:</span> <span class="hi
hlight-n">Yes</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Access-limit</span><span class="highlight-n">-max</span>    <span class="hi
hlight-err">:</span> <span class="highlight-n">4294967295</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Accessed-num</span>        <span class="highlight-err">:</span> <span class=
highlight-n">0</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Idle-timeout</span>        <span class="highlight-err">:</span> <span class="hi
hlight-p">-</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">User-group</span>          <span class="highlight-err">:</span> <span class="h
ghlight-p">-</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Account-type</span>        <span class="highlight-err">:</span> <span class="h
ghlight-nb">cmcc-tr069</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Original-password</span>   <span class="highlight-err">:</span> <span class=
highlight-n">No</span>
```

  <span class="hi
hlight-nb">Password-set-time <span class="h
ghlight-err">: 2019-
/span>12-<span cla
s="highlight-n">01 18<span class="highlight-er
">:42:<sp
n class="highlight-n">57+<span class="highlig
t-n">01:00
DST
  <span class="hi
hlight-nb">Password-expired : <span class=
highlight-n">No
  <span class="hi
hlight-nb">Password-expire-time <span class="
ighlight-err">: -
  <span class="hi
hlight-nb">Account-expire-time <span class="h
ghlight-err">: -
  <span class="hi
hlight-n">Bind IP <span class="highligh
-err">: 10.<
pan class="highlight-n">1.<span class="highlig
t-n">1.1
</code></pre>
注：登录失败未被锁定的本地用户会显示剩余可以尝试登录的次数 Retry-time-left</s
rong>，修改初始密码失败的本地用户会显示剩余可以尝试登录的次数 Change password
etry-count-left。当连续登录失败或者修改初始密码失败的次数达到命令 local-
aa-user wrong-password 配置的次数限制，用户会被锁定。
用户登录失败或者修改初始密码失败的次数未达到命令 local-aaa-user wrong-passw
rd 配置的次数限制时，用户不会被锁定。如果，通过命令 local-aaa-user wron
-password 修改了次数限制，且修改后的次数小于用户已经登录失败或者修改初始密码失
的次数时，用户还有一次尝试登录或者修改密码的机会，此时，字段 Retry-time-left</str
ng> 或者 Change password retry-count-left 显示 1。
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl"># 查看登录失败的本地用户user1的信息。<
span>
 <span class="hig
light-n">display local-user <span class="highli
ht-n">username user1

  <span class="hi
hlight-n">The contents <span class="highlight-
">of local user</spa
>(s<span class="hig
light-p">):

  <span class="hi
hlight-n">Password : <span class="high
ight-p">****************
  <span class="hi
hlight-n">State : <span class="highli
ht-n">active
  <span class="hi
hlight-nb">Service-type-mask <span class="h

ghlight-err">: T

  <span class="hi
hlight-n">Privilege level   <span class="highli
ht-err">: 0

  <span class="hi
hlight-nb">Ftp-directory   : <span class="hi
hlight-p">-
  <span class="hi
hlight-nb">Access-limit   : <span class="hi
hlight-p">-
  <span class="hi
hlight-nb">Accessed-num   : <span class=
highlight-n">0
  <span class="hi
hlight-nb">Idle-timeout   : <span class="hi
hlight-p">-
  <span class="hi
hlight-nb">Retry-interval   : <span class="hi
hlight-n">4 Min(</s
an>s)

  <span class="hi
hlight-nb">Retry-time-left   <span class="high
ight-err">: 1

  <span class="hi
hlight-nb">Original-password   : <span class=
highlight-n">Yes
  <span class="hi
hlight-nb">Password-set-time   <span class="h
ghlight-err">: 2019-
/span>01-<span cla
s="highlight-n">27 13<span class="highlight-er
">:26:<sp
n class="highlight-n">55+<span class="highlig
t-n">08:00

  <span class="hi
hlight-nb">Password-expired   : <span class=
highlight-n">No
  <span class="hi
hlight-nb">Password-expire-time <span class="
ighlight-err">: -

  <span class="hi
hlight-nb">Account-expire-time <span class="h
ghlight-err">: -

<span class="high
ight-c"># 查看修改初始密码失败的本地用户user1的信息。
 <span class="hig
light-n">display local-user <span class="highli

ht-n">username user1
  <span class="hi
hlight-n">The contents <span class="highlight-
">of local user</spa
>(s<span class="hig
light-p">):

  <span class="hi
hlight-n">Password   : <span class="high
ight-p">****************
  <span class="hi
hlight-n">State   : <span class="highli
ht-n">active
  <span class="hi
hlight-nb">Service-type-mask   <span class="h
ghlight-err">: T

  <span class="hi
hlight-n">Privilege level   <span class="highli
ht-err">: 0

  <span class="hi
hlight-nb">Ftp-directory   : <span class="hi
hlight-p">-
  <span class="hi
hlight-nb">Access-limit   : <span class="hi
hlight-p">-
  <span class="hi
hlight-nb">Accessed-num   : <span class=
highlight-n">1
  <span class="hi
hlight-nb">Idle-timeout   : <span class="hi
hlight-p">-
  <span class="hi
hlight-n">Change password <span class="highl
ght-nb">retry-interval : <span class="highligh
-n">4 Min(
span class="highlight-n">s)

  <span class="hi
hlight-n">Change password <span class="highl
ght-nb">retry-count-left<span class="highlight
err">: 3

  <span class="hi
hlight-nb">Original-password   : <span class=
highlight-n">Yes
  <span class="hi
hlight-nb">Password-set-time   <span class="h
ghlight-err">: 2019-
/span>01-<span cla
s="highlight-n">27 13<span class="highlight-er
">:26:<sp
n class="highlight-n">55+<span class="highlig

t-n">08:00

  <span class="hi
hlight-nb">Password-expired   : <span class=
highlight-n">No
  <span class="hi
hlight-nb">Password-expire-time <span class="
ighlight-err">: -

  <span class="hi
hlight-nb">Account-expire-time <span class="h
ghlight-err">: -

<span class="high
ight-c"># 查看处于锁定状态的本地用户信息。
 <span class="hig
light-n">display local-user <span class="highli
ht-n">state block
  <span class="hi
hlight-p">--

  <span class="hi
hlight-nb">User-name   State <span
class="highlight-n">AuthMask AdminLevel <s
an class="highlight-n">BlockTime
  <span class="hi
hlight-p">--

  <span class="hi
hlight-n">test2   B   <span class
"highlight-n">T   0   <span class="highl
ght-n">2018-04</s
an>-10 <span class
"highlight-n">01:5
:11<span c
ass="highlight-p">-00<span class="highlight-er
">:00
  <span class="hi
hlight-p">--
  <span class="hi
hlight-n">Total 1 us
r(s<span cla
s="highlight-p">)

<span class="high
ight-c"># 查看处于锁定状态的本地用户test2的信息。
 <span class="hig
light-n">display local-user <span class="highli
ht-n">state block us
rname test2
  <span class="hi
hlight-n">The contents <span class="highlight-
">of local user</spa
>(s<span class="hig

```
light-p">)</span><span class="highlight-err">:</span>

</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-n">Password</span>            <span class="highlight-err">:</span> <span class="high
ight-p">***************</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-n">State</span>               <span class="highlight-err">:</span> <span class="highli
ht-n">block</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Service-type</span><span class="highlight-n">-mask</span>    <span class="h
ghlight-err">:</span> <span class="highlight-n">T</span>

</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-n">Privilege</span> <span class="highlight-n">level</span>      <span class="highli
ht-err">:</span> <span class="highlight-n">0</span>

</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Ftp-directory</span>       <span class="highlight-err">:</span> <span class="hi
hlight-p">-</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Access-limit</span>        <span class="highlight-err">:</span> <span class="hi
hlight-p">-</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Accessed-num</span>        <span class="highlight-err">:</span> <span class=
highlight-n">0</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Idle-timeout</span>        <span class="highlight-err">:</span> <span class="hi
hlight-p">-</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Block-time</span><span class="highlight-n">-left</span>      <span class="high
ight-err">:</span> <span class="highlight-n">8</span> <span class="highlight-n">Min</s
an><span class="highlight-p">(</span><span class="highlight-n">s</span><span class="h
ghlight-p">)</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Original-password</span>    <span class="highlight-err">:</span> <span class=
highlight-n">Yes</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Password-set</span><span class="highlight-n">-time</span>    <span class="h
ghlight-err">:</span> <span class="highlight-n">2019</span><span class="highlight-p">-
/span><span class="highlight-n">01</span><span class="highlight-p">-</span><span cla
s="highlight-n">27</span> <span class="highlight-n">13</span><span class="highlight-er
">:</span><span class="highlight-n">26</span><span class="highlight-err">:</span><sp
n class="highlight-n">55</span><span class="highlight-p">+</span><span class="highlig
t-n">08</span><span class="highlight-err">:</span><span class="highlight-n">00</span>

</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Password-expired</span>    <span class="highlight-err">:</span> <span class=
highlight-n">No</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Password-expire</span><span class="highlight-n">-time</span> <span class="
ighlight-err">:</span> <span class="highlight-p">-</span>

</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Account-expire</span><span class="highlight-n">-time</span>  <span class="h
```

ghlight-err">: -
</code></pre>
<table>
<thead>
<tr>
<th align="center">项目</th>
<th align="left">描述</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">User-name</td>
<td align="left">本地用户的用户名。通过 local-user 命令配置。</td>
</tr>
<tr>
<td align="center">State</td>
<td align="left">本地用户的状态：</td>
</tr>
</tbody>
</table>

A：Active
B：Block
通过 local-user 命令配置。
|
|AuthMask| 本地用户的接入类型，包括如下几种类型：
T：Telnet 用户。
M：终端用户，通常指 Console 用户。
S：SSH 用户。
F：FTP 用户。
W：WEB 用户。
B：IP Session 用户。
X：802.1X 用户。
A：All，表示用户可以使用所有接入类型。
H：HTTP 用户。
D：X25-PAD 用户。
P：PPP 用户。
组合类型：例如 MH，表示用户既可以是终端用户，也可以是 HTTP 用户。
通过 local-user service-type 命令配置。
|
|AdminLevel| 本地用户的级别。
通过 local-user 命令配置。
当没有配置 local-user 命令时，admin 用户显示的级别为“-”。
|
|Password| 本地用户的密码。
通过 local-user 命令配置。
|
|Service-type-mask| 本地用户的服务类型，和 AuthMask 的类型一致。
通过 local-user service-type 命令配置。
|
|Privilege level| 本地用户的级别。
通过 local-user 命令配置。
|
|Ftp-directory| 本地用户的 FTP 目录。

通过 local-user 命令配置。
|
|Access-limit| 是否配置了本地用户的连接限制数。
通过 local-user 命令配置。
|
|Access-limit-max| 本地用户的连接限制数。
通过 local-user 命令配置。
|
|Accessed-num| 本地用户已建立的连接数。|
|Idle-timeout| 本地用户的闲置切断时间。
通过 local-user 命令配置。
|
|User-group| 本地用户绑定的用户组。
通过 local-user 命令配置。
|
|Account-type| 本地用户的账户类型。
通过命令 local-user account-type 配置本地用户的账户类型为 CMCC-TR069 协议用户。
|
|Original-password| 本地用户的密码是否是初始密码：
Yes
No
通过 password alert original 命令配置。
|
|Password-set-time| 本地用户的密码创建时间，该时间格式为本地时间附带夏令时时区。|
|Password-expired| 本地用户的密码是否过期：
Yes
No
|
|Password-expire-time| 本地用户的密码过期时间，该时间格式为本地时间附带夏令时时区。
通过 password expire 命令配置。
|
|Account-expire-time| 本地用户的账号过期时间，该时间格式为本地时间附带夏令时时区。
通过 local-user expire-date 命令配置。
|
|Bind IP| 本地用户绑定的 IP 地址。
通过 local-user bind-ip 命令配置。
|
|BlockTime 或 Block-time-left| 本地用户被锁定（由于连续输入错误密码导致本地用户被锁定）的余时间。|
|Retry-interval| 本地用户被锁定前，可以尝试登录的重试时间间隔。
通过 local-aaa-user wrong-password 命令配置。
|
|Retry-time-left| 本地用户被锁定前，剩余可尝试登录的次数。
通过 local-aaa-user wrong-password 命令配置。
|
|Change password retry-interval| 本地用户被锁定前，可以尝试修改初始密码的重试时间间隔。

通过 local-aaa-user wrong-password 命令配置。
|
|Change password retry-count-left| 本地用户被锁定前，剩余可尝试修改初始密码的次数。
通过 local-aaa-user wrong-password 命令配置。
|


```
<p></p>
<p></p>
<h3 id="查看本地用户的过期时间">查看本地用户的过期时间</h3>
<pre><code class="language-powershell highlight-chroma"><span class="highlight-line"><
pan class="highlight-cl"><span class="highlight-n">display</span> <span class="highlight-
b">local-user</span> <span class="highlight-nb">expire-time</span>
</span></span><span class="highlight-line"><span class="highlight-cl">
</span></span><span class="highlight-line"><span class="highlight-cl"><span class="high
ight-c"># 查看本地用户的过期时间。</span>
</span></span><span class="highlight-line"><span class="highlight-cl">
</span></span><span class="highlight-line"><span class="highlight-cl"> <span class="hig
light-n">display</span> <span class="highlight-nb">local-user</span> <span class="highli
ht-nb">expire-time</span>
</span></span><span class="highlight-line"><span class="highlight-cl"> <span class="hig
light-p">--------------------------------------------------------------------------------</span>
</span></span><span class="highlight-line"><span class="highlight-cl"> <span class="hig
light-n">Username</span>              <span class="highlight-nb">Password-expire</span>
   <span class="highlight-nb">Account-expire</span>           <span class="highlight-n">Expi
ed</span>
</span></span><span class="highlight-line"><span class="highlight-cl"> <span class="hig
light-p">--------------------------------------------------------------------------------</span>
</span></span><span class="highlight-line"><span class="highlight-cl"> <span class="hig
light-n">zsh</span>                   <span class="highlight-n">2014</span><span class="high
ight-p">-</span><span class="highlight-n">12</span><span class="highlight-p">-</span
<span class="highlight-n">01</span> <span class="highlight-n">21</span><span class="h
ghlight-err">:</span><span class="highlight-n">25</span><span class="highlight-err">:</
pan><span class="highlight-n">44</span>    <span class="highlight-p">-</span>
      <span class="highlight-n">NO</span>
</span></span><span class="highlight-line"><span class="highlight-cl"> <span class="hig
light-n">mm001</span>                 <span class="highlight-n">2014</span><span class="h
ghlight-p">-</span><span class="highlight-n">12</span><span class="highlight-p">-</s
an><span class="highlight-n">01</span> <span class="highlight-n">21</span><span clas
="highlight-err">:</span><span class="highlight-n">29</span><span class="highlight-err
>:</span><span class="highlight-n">58</span>    <span class="highlight-p">-</span>
              <span class="highlight-n">NO</span>
</span></span><span class="highlight-line"><span class="highlight-cl"> <span class="hig
light-p">--------------------------------------------------------------------------------</span>
</span></span><span class="highlight-line"><span class="highlight-cl"> <span class="hig
light-n">Total</span><span class="highlight-err">:</span> <span class="highlight-n">2</
pan><span class="highlight-p">,</span> <span class="highlight-n">printed</span><span
lass="highlight-err">:</span> <span class="highlight-n">2</span>
</span></span></code></pre>
<table>
<thead>
<tr>
<th align="center">项目</th>
<th align="left">描述</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">Username</td>
<td align="left">本地用户的用户名。通过**local-user（AAA 视图）**命令配置。</td>
</tr>
```

<tr>
<td align="center">Password-expire</td>
<td align="left">密码过期时间。通过 password expire 命令配置。</td>
</tr>
<tr>
<td align="center">Account-expire</td>
<td align="left">账号过期时间。通过 local-user expire-date 命令配置。</t
>
</tr>
<tr>
<td align="center">Expired</td>
<td align="left">本地用户是否已经过期：</td>
</tr>
</tbody>
</table>

YES
NO
说明：由于显示值可能与实际值存在一分钟以内的误差，所以可能出现当前密码已经过期，但仍然显
为 NO 的情形。当本地用户的账号或密码过期时，表示本地用户已经过期。
|

<h3 id="查看本地用户的密码策略信息">查看本地用户的密码策略信息</h3>
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">display <span class="highlight-
b">local-aaa-user pa
sword policy {</spa
> access-user | <sp
n class="highlight-n">administrator }
</code></pre>
<table>
<thead>
<tr>
<th align="center">参数</th>
<th align="center">参数说明</th>
<th align="center">取值</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">access-user</td>
<td align="center">显示本地接入用户的密码策略信息。</td>
<td align="center">-</td>
</tr>
<tr>
<td align="center">administrator</td>
<td align="center">显示本地管理员的密码策略信息。</td>
<td align="center">-</td>
</tr>
</tbody>
</table>
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl"># 查看本地接入用户的密码策略信息。</sp
n>

 <span class="hig
light-n">display local-aaa<span class="highlig
t-n">-user password <span class="highlight-n"
policy access-user
 <span class="hi
hlight-n">Password control <span cla
s="highlight-err">: Enable
 <span class="hi
hlight-n">Password history <span cl
ss="highlight-err">: Enable <span class="highli
ht-p">(history reco
ds:5<span
class="highlight-p">)
</code></pre>
<table>
<thead>
<tr>
<th align="center">项目</th>
<th align="left">描述</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">Password control</td>
<td align="left">密码控制功能的开启状态：</td>
</tr>
</tbody>
</table>

Enable：开启
Disable：关闭该参数可以
通过命令 local-aaa-user password policy access-user 配置。
|
|Password history| 密码历史记录功能的开启状态和每个用户密码的历史记录的最大条数。
该参数可以通过命令 password history record number 配置。
|

<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl"># 查看本地管理员的密码策略信息。</spa
>
 <span class="hig
light-n">display local-aaa<span class="highlig
t-n">-user password <span class="highlight-n"
policy administrator
 <span class="hi
hlight-n">Password control <span cla
s="highlight-err">: Enable
 <span class="hi
hlight-n">Password expiration <span cl
ss="highlight-err">: Enable <span class="highli
ht-p">(180 days</s
an>)
 <span class="hi
hlight-n">Password history <span cl

ss="highlight-err">: Enable <span class="highli
ht-p">(history reco
ds:5<span
class="highlight-p">)
 <span class="hi
hlight-n">Password alert <span class="highlight
n">before expiration <span class="highlight-err
>: 30 days

 <span class="hi
hlight-n">Password alert <span class="highlight
n">original :
nable
</code></pre>
<table>
<thead>
<tr>
<th align="center">项目</th>
<th align="left">描述</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">Password control</td>
<td align="left">密码控制功能的开启状态：</td>
</tr>
</tbody>
</table>

Enable：开启
Disable：关闭
该参数可以通过命令 local-aaa-user password policy administrator 配置。<
r>
|
|Password expiration| 密码过期功能的开启状态和密码过期时间。该参数可以通过命令 pa
sword expire 配置。|
|Password history| 密码历史记录功能的开启状态和每个用户密码的历史记录的最大条数。该参数可
通过命令 password history record number 配置。|
|Password alert before expiration| 密码过期前的提醒时间。该参数可以通过命令 passwo
d alert before-expire 配置。|
|Password alert original| 初始密码修改提醒功能的开启状态：
Enable：开启
Disable：关闭
该参数可以通过命令 password alert original 配置。
|

<h3 id="查看认证请求数">查看认证请求数</h3>
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">display <span class="highlight-
">aaa statistics acc
ss-type-authenreq
</code></pre>

<h3 id="查看业务方案配置信息">查看业务方案配置信息</h3>
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">display <span class="highlight-
b">service-scheme [<span class="highlight-n"
name name]</span

</code></pre>
<table>
<thead>
<tr>
<th align="center">参数</th>
<th align="center">参数说明</th>
<th align="center">取值</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">name name</td>
<td align="center">指定业务方案名称。</td>
<td align="center">必须是已存在的业务方案名称。</td>
</tr>
</tbody>
</table>
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl"># 查看所有业务方案信息。
 <span class="hig
light-n">display service-scheme
 <span class="hi
hlight-p">--
 <span class="hi
hlight-nb">service-scheme-name <
pan class="highlight-nb">scheme-index
 <span class="hi
hlight-p">--
 <span class="hi
hlight-n">svcscheme1 0
 <span class="hi
hlight-n">svcscheme2 1
 <span class="hi
hlight-p">--
 <span class="hi
hlight-n">Total of se
vice scheme:</spa
> 2

<span class="high
ight-c"># 查看名为svcscheme1的业务方案配置信息。
 <span class="hig
light-n">display service-scheme <span class="
ighlight-n">name svcscheme1

```
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">service-scheme</span><span class="highlight-n">-name</span>          <span c
ass="highlight-err">:</span> <span class="highlight-n">svcscheme1</span>

</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">service-scheme</span><span class="highlight-n">-dns-name</span>      <span
class="highlight-err">:</span> <span class="highlight-p">-</span>

</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">service-scheme</span><span class="highlight-n">-primary-dns</span>    <span
class="highlight-err">:</span> <span class="highlight-p">-</span>

</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">service-scheme</span><span class="highlight-n">-secondary-dns</span>  <sp
n class="highlight-err">:</span> <span class="highlight-p">-</span>

</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">service-scheme</span><span class="highlight-n">-adminlevel</span>    <span
class="highlight-err">:</span> <span class="highlight-n">15</span>

</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">service-scheme</span><span class="highlight-n">-dhcpgroup</span>     <spa
 class="highlight-err">:</span> <span class="highlight-p">-</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">service-scheme</span><span class="highlight-n">-ippool</span>         <span c
ass="highlight-err">:</span> <span class="highlight-p">-</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">service-scheme</span><span class="highlight-n">-primary-wins</span>   <spa
 class="highlight-err">:</span> <span class="highlight-p">-</span>

</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">service-scheme</span><span class="highlight-n">-secondary-wins</span> <sp
n class="highlight-err">:</span> <span class="highlight-p">-</span>

</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">service-scheme</span><span class="highlight-n">-update-config</span>  <sp
n class="highlight-err">:</span> <span class="highlight-p">-</span>

</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">service-scheme</span><span class="highlight-n">-update-version</span> <sp
n class="highlight-err">:</span> <span class="highlight-p">-</span>

</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">service-scheme</span><span class="highlight-n">-acl-number</span>    <span
class="highlight-err">:</span> <span class="highlight-p">-</span>

</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">service-scheme</span><span class="highlight-n">-interface-flag</span> <span
class="highlight-err">:</span> <span class="highlight-p">-</span>    <span class="highlig
t-nb">service-scheme</span><span class="highlight-n">-qosprofile</span>    <span class
"highlight-err">:</span> <span class="highlight-p">-</span>
</span></span></code></pre>
<table>
<thead>
```

<tr>
<th align="center">项目</th>
<th align="left">描述</th>
</tr>
</thead>
<tbody>
<tr>
<td align="center">service-scheme-name</td>
<td align="left">业务方案名称。通过**service-scheme（AAA 视图）**命令配置。</td>
</tr>
<tr>
<td align="center">scheme-index</td>
<td align="left">业务方案索引。</td>
</tr>
<tr>
<td align="center">service-scheme-dns-name</td>
<td align="left">业务方案下的 DNS 缺省域名。</td>
</tr>
<tr>
<td align="center">service-scheme-primary-dns</td>
<td align="left">主用 DNS 服务器地址。</td>
</tr>
<tr>
<td align="center">service-scheme-secondary-dns</td>
<td align="left">备用 DNS 服务器地址。</td>
</tr>
<tr>
<td align="center">service-scheme-adminlevel</td>
<td align="left">管理员用户级别。通过 admin-user privilege level 命令配
。</td>
</tr>
<tr>
<td align="center">service-scheme-dhcpgroup</td>
<td align="left">DHCP 服务器组。</td>
</tr>
<tr>
<td align="center">service-scheme-ippool</td>
<td align="left">业务方案下的 IP 地址池。</td>
</tr>
<tr>
<td align="center">service-scheme-primary-wins</td>
<td align="left">主用 wins 服务器地址。</td>
</tr>
<tr>
<td align="center">service-scheme-secondary-wins</td>
<td align="left">备用 wins 服务器地址。</td>
</tr>
<tr>
<td align="center">service-scheme-update-config</td>
<td align="left">升级包的 URL 路径。</td>
</tr>
<tr>
<td align="center">service-scheme-update-version</td>
<td align="left">升级包的版本号。</td>

</tr>
<tr>
<td align="center">service-scheme-acl-number</td>
<td align="left">推送给对端的本端子网信息。</td>
</tr>
<tr>
<td align="center">service-scheme-interface-flag</td>
<td align="left">推送给对端的绑定 IPSec 的接口 IP 地址。</td>
</tr>
<tr>
<td align="center">service-scheme-qosprofile</td>
<td align="left">绑定的 QoS 模板名称。通过**qos-profile（业务方案视图）**命令配置。</td>
</tr>
<tr>
<td align="center">service-scheme-idlecut-time</td>
<td align="left">闲置切断时间，单位是分钟。通过**idle-cut（业务方案视图）**命令配置。</td>
</tr>
<tr>
<td align="center">service-scheme-idlecut-flow</td>
<td align="left">闲置切断的流量阈值，单位是 Kbyte。通过**idle-cut（业务方案视图）**命令配
。</td>
</tr>
<tr>
<td align="center">service-scheme-idlecut-direct</td>
<td align="left">闲置切断的对流量生效的方向。取值包括：</td>
</tr>
</tbody>
</table>

Inbound：表示闲置切断对上行流量生效。
Outbound：表示闲置切断对下行流量生效。
Inbound and Outbound：表示闲置切断对上行流量和下行流量都生效。
通过 idle-cut（业务方案视图）命令配置。
|
|Tariff-level| 费率级别。|
|Qos-profile| 费率级别对应的 QoS 模板。通过tariff-level命令配置。|
|Accounting-flag| 费率级别对应的计费功能是否使能：
enable：使能。
disable：未使能。
通过 tariff-level 命令配置。
|

<h2 id="维护-AAA">维护 AAA</h2>

<h2 id="配置主备RADIUS案例">配置主备 RADIUS 案例</h2>
组网需求
如图 1 所示，用户同处于 huawei 域，Router 作为目的网络接入服务器。用户需要通过服务器的远
认证才能通过 Router 访问目的网络。在 Router 上的远端认证方式如下：

Router 对接入用户先用 RADIUS 服务器进行认证，如果认证没有响应，再使用本地认证。
RADIUS 服务器 10.7.66.66/24 作为主用认证服务器和计费服务器，RADIUS 服务器 10.7.66.67/
4 作为备用认证服务器和计费服务器，认证端口号缺省为 1812，计费端口号缺省为 1813。

<img src="https://ld246.com/images/img-loading.svg" alt="image" title="图1 采用RADIS协议对用户进行认证和计费组网图" data-src="https://b3logfile.com/siyuan/1638257532966/assets/image-20230101121400-jgozhx1.png?imageView2/2/interlace/1/format/jpg">
配置思路
用如下的思路配置采用 RADIUS 协议对用户进行认证和计费。

配置 RADIUS 服务器模板。
配置认证方案、计费方案。
在域下应用 RADIUS 服务器模板、认证方案和计费方案。

说明

配置前请确保各设备之间路由可达。
请确保 RADIUS 服务器模板内的共享密钥和 RADIUS 服务器上的配置保持一致。
如果 RADIUS 服务器不接受包含域名的用户名，可以在 RADIUS 服务器模板视图下，配置命令 <trong>undo radius-server user-name domain-included 使设备向 RADIUS 服务器发的报文中的用户名不包含域名。
域被配置成全局默认域之后，用户的用户名中携带该域名或者不携带域名时，会使用全局默认域的 AAA 配置信息。
配置命令 undo radius-server user-name domain-included 后，设备仅会修改发送报文中的户名格式，不会影响用户所属的域。例如，配置该命令后，用户名为“user@huawei.com”的用户使用 huawei.com 域下的 AAA 配置信息。

操作步骤
（1）配置 VTY
<pre><code class="language-powershell highlight-chroma"><pan class="highlight-cl">user-interface vty 0 4</pan>
 authentication-mode aaa
 user privilege <span class="highlight-n>level 15
 protocol inbound all
</code></pre>
（2）配置 RADIUS 服务器模板
<pre><code class="language-powershell highlight-chroma"><pan class="highlight-cl"># 配置RADIUS服务器模板shiva。
 system-view
[Huawei] sysname Router
[Router] radius-server template shiva

配置RADIUS主用认证服务器和计费服务器的IP地址、端口。
[Router-radius<span class="highlight-

```
">-shiva</span><span class="highlight-p">]</span> <span class="highlight-nb">radius-se
ver</span> <span class="highlight-n">authentication</span> <span class="highlight-n">1
</span><span class="highlight-p">.</span><span class="highlight-n">7</span><span cla
s="highlight-p">.</span><span class="highlight-n">66</span><span class="highlight-p">
</span><span class="highlight-n">66</span> <span class="highlight-n">1812</span> <s
an class="highlight-n">weight</span> <span class="highlight-n">80</span>
</span></span><span class="highlight-line"><span class="highlight-cl"><span class="high
ight-p">[</span><span class="highlight-nb">Router-radius</span><span class="highlight-
">-shiva</span><span class="highlight-p">]</span> <span class="highlight-nb">radius-se
ver</span> <span class="highlight-n">accounting</span> <span class="highlight-n">10</
pan><span class="highlight-p">.</span><span class="highlight-n">7</span><span class=
highlight-p">.</span><span class="highlight-n">66</span><span class="highlight-p">.</s
an><span class="highlight-n">66</span> <span class="highlight-n">1813</span> <span c
ass="highlight-n">weight</span> <span class="highlight-n">80</span>
</span></span><span class="highlight-line"><span class="highlight-cl">
</span></span><span class="highlight-line"><span class="highlight-cl"><span class="high
ight-c"># 配置RADIUS备用认证服务器和计费服务器的IP地址、端口。</span>
</span></span><span class="highlight-line"><span class="highlight-cl"><span class="high
ight-p">[</span><span class="highlight-nb">Router-radius</span><span class="highlight-
">-shiva</span><span class="highlight-p">]</span> <span class="highlight-nb">radius-se
ver</span> <span class="highlight-n">authentication</span> <span class="highlight-n">1
</span><span class="highlight-p">.</span><span class="highlight-n">7</span><span cla
s="highlight-p">.</span><span class="highlight-n">66</span><span class="highlight-p">
</span><span class="highlight-n">67</span> <span class="highlight-n">1812</span> <s
an class="highlight-n">weight</span> <span class="highlight-n">40</span>
</span></span><span class="highlight-line"><span class="highlight-cl"><span class="high
ight-p">[</span><span class="highlight-nb">Router-radius</span><span class="highlight-
">-shiva</span><span class="highlight-p">]</span> <span class="highlight-nb">radius-se
ver</span> <span class="highlight-n">accounting</span> <span class="highlight-n">10</
pan><span class="highlight-p">.</span><span class="highlight-n">7</span><span class=
highlight-p">.</span><span class="highlight-n">66</span><span class="highlight-p">.</s
an><span class="highlight-n">67</span> <span class="highlight-n">1813</span> <span c
ass="highlight-n">weight</span> <span class="highlight-n">40</span>
</span></span><span class="highlight-line"><span class="highlight-cl">
</span></span><span class="highlight-line"><span class="highlight-cl"><span class="high
ight-c"># 配置RADIUS服务器密钥、重传次数，以及设备向RADIUS服务器发送的报文中的用户名
包含域名。</span>
</span></span><span class="highlight-line"><span class="highlight-cl"><span class="high
ight-p">[</span><span class="highlight-nb">Router-radius</span><span class="highlight-
">-shiva</span><span class="highlight-p">]</span> <span class="highlight-nb">radius-se
ver</span> <span class="highlight-nb">shared-key</span> <span class="highlight-n">cip
er</span> <span class="highlight-n">YsHsjx_202206</span>
</span></span><span class="highlight-line"><span class="highlight-cl"><span class="high
ight-p">[</span><span class="highlight-nb">Router-radius</span><span class="highlight-
">-shiva</span><span class="highlight-p">]</span> <span class="highlight-nb">radius-se
ver</span> <span class="highlight-n">retransmit</span> <span class="highlight-n">2</sp
n>
</span></span><span class="highlight-line"><span class="highlight-cl"><span class="high
ight-p">[</span><span class="highlight-nb">Router-radius</span><span class="highlight-
">-shiva</span><span class="highlight-p">]</span> <span class="highlight-n">undo</sp
n> <span class="highlight-nb">radius-server</span> <span class="highlight-nb">user-nam
</span> <span class="highlight-nb">domain-included</span>
</span></span><span class="highlight-line"><span class="highlight-cl"><span class="high
ight-p">[</span><span class="highlight-nb">Router-radius</span><span class="highlight-
```

">-shiva] quit</spa
>
</code></pre>
（3）配置认证方案、计费方案。
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl"># 配置认证方案auth，认证模式为先进行R
DIUS认证，后进行本地认证。
<span class="high
ight-no">[Router] aaa
<span class="high
ight-p">[Router-aaa<span class="highlight-p"
] authentication-scheme <span class="highligh
-n">auth
<span class="high
ight-p">[Router-aaa<span class="highlight-n"
-authen-auth] auth
ntication-mode radius <span class="highlight-n
>local
<span class="high
ight-p">[Router-aaa<span class="highlight-n"
-authen-auth] quit<
span>

<span class="high
ight-c"># 配置计费方案abc，计费模式为RADIUS，并配置当开始计费失败时，允许用户上线。</sp
n>
<span class="high
ight-p">[Router-aaa<span class="highlight-p"
] accounting-scheme <span class="highlight-n
>abc
<span class="high
ight-p">[Router-aaa<span class="highlight-n"
-accounting-abc] a
counting-mode radius
<span class="high
ight-p">[Router-aaa<span class="highlight-n"
-accounting-abc] ac
ounting start-fail on
ine
<span class="high
ight-p">[Router-aaa<span class="highlight-n"
-accounting-abc] qui

</code></pre>
（4）配置 huawei 域，在域下应用认证方案 auth、计费方案 abc、RADIUS 服务器模板 shiva<
p>
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">[R
uter-aaa] domain</
pan> huawei
<span class="high
ight-p">[Router-aaa<span class="highlight-n"
-domain-huawei] a

thentication-scheme auth
<span class="high
ight-p">[Router-aaa<span class="highlight-n"
-domain-huawei] a
counting-scheme abc
<span class="high
ight-p">[Router-aaa<span class="highlight-n"
-domain-huawei] r
dius-server shiva
<span class="high
ight-p">[Router-aaa<span class="highlight-n"
-domain-huawei] qui

<span class="high
ight-p">[Router-aaa<span class="highlight-p"
] quit
</code></pre>
（5）配置 huawei 域为全局默认域
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">[Router] <span class="highlig
t-n">domain huawei
<span class="high
ight-no">[Router] domain <span class="highlig
t-n">huawei admin
</code></pre>
（6）配置 AAA 本地认证
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">[Router] <span class="highlig
t-n">aaa
<span class="high
ight-p">[Router-aaa<span class="highlight-p"
] local-user user1</
pan> password irreversible-
ipher YsHsjx_202207
<span class="high
ight-p">[Router-aaa<span class="highlight-p"
] local-user user1</
pan> service-type http</sp
n>
<span class="high
ight-p">[Router-aaa<span class="highlight-p"
] local-user user1</
pan> privilege level
span class="highlight-n">15
<span class="high
ight-p">[Router-aaa<span class="highlight-p"
] quit
</code></pre>
（7）验证配置结果
<pre><code class="language-powershell highlight-chroma"><
pan class="highlight-cl">
<span class="high
ight-c"># 在Router上执行命令display radius-server configuration template template-name，
以观察到该RADIUS服务器模板的配置与要求一致。

```
</span></span><span class="highlight-line"><span class="highlight-cl"><span class="high
ight-no">[Router]</span> <span class="highlight-n">display</span> <span class="highligh
-nb">radius-server</span> <span class="highlight-n">configuration</span> <span class="h
ghlight-n">template</span> <span class="highlight-n">shiva</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-p">----------------------------------------------------------------------</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Server-template</span><span class="highlight-n">-name</span>        <span c
ass="highlight-err">:</span>  <span class="highlight-n">shiva</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Server-template</span><span class="highlight-n">-index</span>       <span cl
ss="highlight-err">:</span>  <span class="highlight-n">1</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Protocol-version</span>            <span class="highlight-err">:</span>  <span c
ass="highlight-n">standard</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Traffic-unit</span>              <span class="highlight-err">:</span>  <span clas
="highlight-n">B</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Shared-secret</span><span class="highlight-n">-key</span>          <span clas
="highlight-err">:</span>  <span class="highlight-p">******</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Group-filter</span>              <span class="highlight-err">:</span>  <span clas
="highlight-n">class</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Timeout-interval</span><span class="highlight-p">(</span><span class="highl
ght-k">in</span> <span class="highlight-n">second</span><span class="highlight-p">)</
pan>  <span class="highlight-err">:</span>  <span class="highlight-n">5</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-n">Retransmission</span>             <span class="highlight-err">:</span>  <span cla
s="highlight-n">2</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-n">EndPacketSendTime</span>          <span class="highlight-err">:</span>  <span
class="highlight-n">3</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-n">Dead</span> <span class="highlight-n">time</span><span class="highlight-p">
</span><span class="highlight-k">in</span> <span class="highlight-n">minute</span><s
an class="highlight-p">)</span>       <span class="highlight-err">:</span>  <span class="
ighlight-n">5</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Domain-included</span>           <span class="highlight-err">:</span>  <span
lass="highlight-n">NO</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">NAS-IP</span><span class="highlight-n">-Address</span>             <span clas
="highlight-err">:</span>  <span class="highlight-p">-</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Calling-station</span><span class="highlight-n">-id</span> <span class="highl
ght-nb">MAC-format</span> <span class="highlight-err">:</span>  <span class="highligh
-nb">xxxx-xxxx</span><span class="highlight-n">-xxxx</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
hlight-nb">Called-station</span><span class="highlight-n">-id</span> <span class="highl
ght-nb">MAC-format</span>  <span class="highlight-err">:</span>  <span class="highligh
-nb">XX-XX</span><span class="highlight-n">-XX-XX-XX-XX</span>
</span></span><span class="highlight-line"><span class="highlight-cl">  <span class="hi
```

hlight-nb">NAS-Port-ID <span class="highlight
n">format : <span class="highlight-n"
New
 <span class="hi
hlight-nb">Service-type : <span cla
s="highlight-p">-
 <span class="hi
hlight-nb">NAS-IPv6-Address <span cla
s="highlight-err">: ::
 <span class="hi
hlight-n">Server algorithm <span class
"highlight-err">: master-backup
 <span class="hi
hlight-nb">Detect-interval(<span class="highlig
t-k">in second)</sp
n> : 60
 <span class="hi
hlight-n">Authentication Server <span class="h
ghlight-n">1 :
0.7<span cl
ss="highlight-p">.66
66 Port<
pan class="highlight-err">:1812 <span class="h
ghlight-n">Weight:<span class="highlight-n"
80 [UP]

Vrf:<span class=
highlight-p">- LoopBack<span class="highlight
err">:NULL Vlanif</
pan>:NULL

Source IP<span cl
ss="highlight-err">: ::
 <span class="hi
hlight-n">Authentication Server <span class="h
ghlight-n">2 :
0.7<span cl
ss="highlight-p">.66
67 Port<
pan class="highlight-err">:1812 <span class="h
ghlight-n">Weight:<span class="highlight-n"
40 [UP]

Vrf:<span class=
highlight-p">- LoopBack<span class="highlight
err">:NULL Vlanif</
pan>:NULL

Source IP<span cl
ss="highlight-err">: ::
 <span class="hi
hlight-n">Accounting Server <span class="hi
hlight-n">1 : 1
.7<span cla

s="highlight-p">.66
66 Port<
pan class="highlight-err">:1813 <span class="h
ghlight-n">Weight:<span class="highlight-n"
80 [UP]

  Vrf:<span class=
highlight-p">- LoopBack<span class="highlight
err">:NULL Vlanif</
pan>:NULL

  Source IP<span cl
ss="highlight-err">: ::
  <span class="hi
hlight-n">Accounting Server <span class="hi
hlight-n">2 : 1
.7<span cla
s="highlight-p">.66
67 Port<
pan class="highlight-err">:1813 <span class="h
ghlight-n">Weight:<span class="highlight-n"
40 [UP]

  Vrf:<span class=
highlight-p">- LoopBack<span class="highlight
err">:NULL Vlanif</
pan>:NULL

  Source IP<span cl
ss="highlight-err">: ::
  <span class="hi
hlight-p">--
</code></pre>

<h2 id="思考题-">思考题？</h2>
<blockquote>
AAA 支持的认证、授权和计费方式分别有哪几种？
</blockquote>
认证：不认证、本地认证、远端认证
授权：不授权、本地授权、远端授权
计费：不计费、远端计费

<blockquote>
当创建本地认证的普通用户时，没有关联自定义的域，则该用户属于哪个域?
</blockquote>
如果创建用户时未指定用户所属的域，用户会自动关联缺省域 default（管理用户关联到 default admin 域）。

<h2 id="本章总结">本章总结</h2>
AAA 技术为了提高企业网络的安全性，防止非法用户登录，需要对企业内部员工，外部客户等行身份的认证，可访问资源的授权和上网为行为的监控。

认证（Authentication）：验证用户是否可以获得访问权，确定哪些用户可以访问网络。

授权（Authorization）：授权用户可以使用哪些服务。
计费（Accounting）：记录用户使用网络资源的情况。

AAA 技术可以本地实现，也可以通过远端服务器实现。
AAA 可以用多种协议来实现，最常用的是 RADIUS 协议。
<h2 id="FAQ">FAQ</h2>
<blockquote>
RADIUS、HWTACAS 协议运行在谁和谁之间？
</blockquote>
运行在 NAS/AAA Client 和 AAA 服务器之间

<h2 id="WinRADIUS使用">WinRADIUS 使用</h2>
<h2 id="设置NAS密钥和RADIUS端口">设置 NAS 密钥和 RADIUS 端口</h2>

<h2 id="创建ODBC数据库">创建 ODBC 数据库</h2>

<h2 id="创建RAIDUS表">创建 RAIDUS 表</h2>

<h2 id="添加RADIUS用户">添加 RADIUS 用户</h2>

<h2 id="查询">查询</h2>

ogfile.com/siyuan/1638257532966/assets/image-20221230153252-g9cziwc.png?imageView2/2/interlace/1/format/jpg">
<img src="https://ld246.com/images/img-loading.svg" alt="image" data-src="https://b3ogfile.com/siyuan/1638257532966/assets/image-20221230153241-hilwb5n.png?imageView2/2/interlace/1/format/jpg">

修改

<img src="https://ld246.com/images/img-loading.svg" alt="image" data-src="https://b3ogfile.com/siyuan/1638257532966/assets/image-20221230153601-kon0izd.png?imageView2/2/interlace/1/format/jpg">
<img src="https://ld246.com/images/img-loading.svg" alt="image" data-src="https://b3ogfile.com/siyuan/1638257532966/assets/image-20221230153611-996umvd.png?imageView/2/interlace/1/format/jpg">
<img src="https://ld246.com/images/img-loading.svg" alt="image" data-src="https://b3ogfile.com/siyuan/1638257532966/assets/image-20221230153252-g9cziwc.png?imageView2/2/interlace/1/format/jpg">
<img src="https://ld246.com/images/img-loading.svg" alt="image" data-src="https://b3ogfile.com/siyuan/1638257532966/assets/image-20221230153620-i1xpvg8.png?imageView2/2/interlace/1/format/jpg">