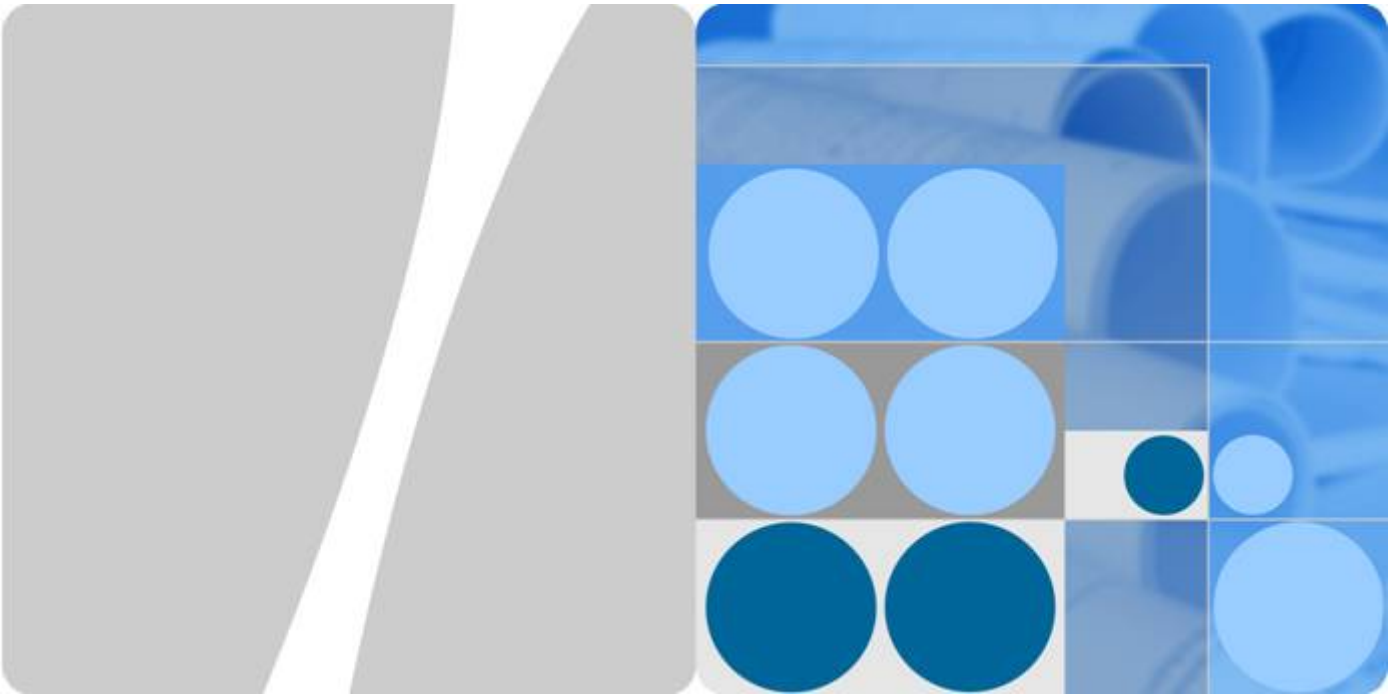


HUAWEI NetEngine20E-X6 高端业务路由器
V600R003C00

配置指南-用户接入

文档版本　01

发布日期　2011-05-15

华为技术有限公司

商标声明


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

注意

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

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

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 0755-28560000 4008302118

客户服务传真： 0755-28560111

前 言

概述

本文档针对用户接入业务，从基本原理、配置过程、配置方法几个方面介绍了 AAA、用户管理、DHCPv4、等特性。

本文档提供了用户接入业务的配置方法与步骤。

读者对象

本文档主要适用于以下工程师：

- 调测工程师
- 数据配置工程师
- 网络监控工程师
- 系统维护工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
 危险	以本标志开始的文本表示有高度潜在危险，如果不能避免，会导致人员死亡或严重伤害。
 警告	以本标志开始的文本表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。
 注意	以本标志开始的文本表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
窍门	以本标志开始的文本能帮助您解决某个问题或节省您的时间。
说明	以本标志开始的文本是正文的附加信息，是对正文的强调和补充。

修订记录

修改记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本 01 (2011-05-15)

第一次正式发布。

目 录

插图目录

1 AAA 配置

关于本章

通过 AAA 的配置，实现对用户进行本地认证、授权和计费，或者进行远端的认证、授权和计费。

1.1 AAA 简介
配置 AAA 所要理解的知识，包括 AAA 方案、RADIUS 服务器模板、HWTACAS 服务器模板以及配置域所要理解的知识。

1.2 配置 AAA 方案
通过配置 AAA 方案，可以确定对用户进行的认证、授权和计费方式。

1.3 配置 RADIUS 服务器
当对用户的认证、计费通过远端 RADIUS 服务器时需要配置 RADIUS 服务器。

1.4 配置 HWTACACS 服务器
当对用户的认证、计费通过远端 HWTACACS 服务器时需要配置 HWTACACS 服务器。

1.5 配置话单本地保存
话单本地保存是对远端计费服务器的备份，防止远端服务器故障，计费信息丢失。

1.6 配置域
所有的本地用户和接入用户都是基于域属性进行管理。

1.7 维护 AAA
维护 AAA 包括清除 HWTACACS 统计信息，调试 RADIUS 或者 HWTACACS。

1.8 配置举例
介绍 AAA 配置的各种示例。配置示例中包括组网需求、配置注意事项和配置思路等。

1.1 AAA 简介

配置 AAA 所要理解的知识，包括 AAA 方案、RADIUS 服务器模板、HWTACAS 服务器模板以及配置域所要理解的知识。

1.1.1 AAA 概述

远端认证、授权和计费协议包括 RADIUS 和 HWTACACS，所有的认证、授权和计费都要通过对域用户实现。

AAA

AAA 是 Authentication（认证）、Authorization（授权）和 Accounting（计费）的简称。它提供对用户进行认证、授权和计费三种安全功能。具体如下：

- 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 一般采用“客户端—服务器”结构。这种结构既具有良好的可扩展性，又便于用户信息的集中管理。

AAA 支持的认证方式包括不认证、本地认证、远端认证。其中远端认证支持通过 RADIUS（Remote Authentication Dial In User Service）协议或 HWTACACS（HuaWei Terminal Access Controller Access Control System）协议进行。

AAA 支持的授权方式包括直接授权、本地授权、HWTACACS 授权、if-authenticated 授权。

说明

RADIUS 协议的认证和授权是绑定在一起的，不能单独使用 RADIUS 进行授权。

经过 HWTACACS 认证的用户，可以主动发起修改保存在 TACACS 服务器上的用户密码。

AAA 支持的计费方式包括不计费、远端计费。

用户的认证、授权、计费都需要在域下执行。

基于域的用户管理

网络接入服务器对用户的管理包括两种方式。

- 通过域来进行用户管理，域下可以进行缺省授权配置、RADIUS/HWTACACS 模板配置、认证和计费方案的配置等。
- 通过帐号进行用户管理。

在目前 AAA 的实现中，所有用户都属于某个域。用户属于哪个域是由用户名中带的“@”后的字符串来决定的，比如“user@hua”，就属于“hua”域；如果用户名中没有带“@”，就属于系统缺省的域，default0、default1、default_admin 域。

除了系统缺省的 default0、default1、default_admin 域外，AAA 允许用户最多创建 1021 个域。

所有对于用户的认证、授权、计费都是在域视图下应用认证方案、授权方案、计费方案来实现的，在 AAA 视图下分别预先配置相应的认证模式、计费模式、授权模式。

域下配置的授权信息较 AAA 服务器的授权信息优先级低，即，优先使用 AAA 服务器下发的授权属性，在 AAA 服务器无该项授权或不支持该项授权时，域的授权属性生效。这样处理的优点是：可以凭借域管理灵活增加业务，而不必受限于 AAA 服务器提供的属性。

1.1.2 NE20E-X6 支持的 AAA

NE20E-X6 支持本地和远端的认证、授权和计费，支持 HWTACACS 用户修改密码。

NE20E-X6 支持如下的认证、授权和计费方案，并支持对用户通过域进行管理。

1. 认证方式

   AAA 支持的认证方式包括不认证、本地认证、远端认证。其中远端认证支持通过 RADIUS（Remote Authentication Dial In User Service）协议或 HWTACACS（HuaWei Terminal Access Controller Access Control System）协议进行。

   这几种认证方式可以按照命令行配置的认证组合方式进行认证。如果采用第一种认证模式进行认证时无响应（包括远端服务器无响应等），可以改用另外一种认证模式进行认证（按照配置认证模式的先后依次进行）。比如先后按照 radius、local、none 的方式进行认证。

2. 授权方式

   AAA 支持的授权方式包括直接授权、本地授权、HWTACACS 授权、if-authenticated 授权。

   说明

   RADIUS 协议的授权和认证是绑定在一起的，不能单独使用 RADIUS 进行授权。

   用户在线时，NE20E-X6 支持动态修改用户的授权信息，称为 CoA（Change of Authorization）。网络管理员可在保持用户在线的情况下，修改 RADIUS 服务器上相应的业务属性，然后通过 CoA 报文动态改变用户使用的服务，这种授权称为动态授权。

3. 计费方式

   AAA 支持的计费方式包括不计费和远端计费。

   用户完成认证授权之后，就已经上线成功，从访问业务开始就要进行计费。对用户进行计费可以根据用户上线的时长、用户流量或者是混合时长和流量进行计费。用户的计费过程包括 NE20E-X6 对用户的上网时长和上下行流量信息进行统计，然后把这些统计信息按照 RADIUS 协议或者 HWTACACS 协议规定的格式发送到 RADIUS 服务器或者 HWTACACS 服务器，服务器向 NE20E-X6 返回计费是否成功的信息。

说明

用户的认证、授权、计费都需要在域下执行。

对于 HWTACACS 用户，经过认证后，NE20E-X6 既支持服务器端发起，使用户修改密码，也支持用户通过命令行主动修改用户密码。

HWTACACS 支持 VPN 实例转发，当运营商的 TACACS 服务器部署在私网，而 NE20E-X6 位于公网时，HWTACACS 支持通过 VPN 实例与 TACACS 服务器进行交互，实现对用户的认证、授权和计费。

1.2 配置 AAA 方案

通过配置 AAA 方案，可以确定对用户进行的认证、授权和计费方式。

1.2.1 建立配置任务

介绍配置 AAA 方案的应用环境，以及配置 AAA 方案需要提前完成的任务和准备的数据。

应用环境

在需要为合法用户提供网络接入服务，同时对敏感的网络设备进行保护，防止非授权访问和抵赖行为的环境下，可以在路由器上配置 AAA。

说明

AAA 在网络接入服务器上始终处于使能状态。

在配置地址池的时候，A 类地址中的 XXX.255.255.255 和 XXX.0.0.0、B 类地址中的 XXX.XXX.255.255 和 XXX.XXX.0.0、C 类地址中的 XXX.XXX.XXX.255 和

XXX.XXX.XXX.0 都不能够作为合法的地址池起始、结束地址。如果地址池里面含有这些地址，这些地址也不会被分配。

说明

IP 地址协商的配置需要在客户端与服务器端分别进行。

前置任务

在配置 AAA 方案之前，需完成以下任务：

配置接口的链路层协议参数和 IP 地址，使接口的链路协议状态为 Up。

数据准备

在配置 AAA 方案之前，需要准备以下数据。

序号	数据
1	认证方案名称、认证模式
2	（可选）授权方案名称、授权模式、HWTACACS 按命令行授权的用户级别、命令授权超时时间
3	计费方案名称、计费模式、实时计费的时间间隔、开始计费失败策略、实时计费失败策略、实时计费失败次数
4	（可选）记录方案名称、与记录模式关联的 HWTACACS 服务器模板的名称、需要记录的事件
5	服务器端和用户端的接口类型和编号、在采用地址池时需要确定地址池编号、IP 地址范围，不采用地址池时需要确定为用户分配的 IP 地址

1.2.2 （可选）使能 RADIUS/HWTACACS 协议功能

打开应用层联动模块中 RADIUS 或 HWTACACS 的协议开关，用户发送的认证、授权和计费请求报文将被转发。关闭 RADIUS/HWTACACS 协议功能时，用户发送的认证、授权和计费请求报文将被丢弃。

背景信息

请在路由器上进行如下配置：

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 使能 RADIUS/HWTACACS 协议功能，可选择执行其中之一：

- 执行命令 **radius enable**，使能 RADIUS 协议功能；
- 执行命令 **hwtacacs enable**，使能 HWTACACS 协议功能。

缺省情况下，RADIUS/HWTACACS 协议使能。

----结束

1.2.3 配置认证方案

配置认证方式后，应该在认证服务器上配置相关用户信息，否则用户不能通过认证。

背景信息

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **authentication-scheme** *scheme-name*，创建认证方案。

步骤 4 执行命令 **authentication-mode** { **hwtacacs** | **radius** | **local** } *[**none**]配置认证模式。

NE20E-X6 支持的认证模式包括 HWTACACS 认证、RADIUS 认证、本地认证和不认证。另外，NE20E-X6 支持二次认证，如果采用第一种认证模式进行认证时无响应（包括远端服务器无响应或者本地未配置该用户等），可以改用另外一种认证模式进行认证。

NE20E-X6 中固定有三个认证方案 default、default0、default1，不能删除，只能修改。

- default0 认证方案的认证模式缺省为不认证。
- default1 的认证模式缺省为 RADIUS 认证。
- default 的认证模式缺省为先本地认证后 RADIUS 认证。

步骤 5 （可选）执行命令 **authening authen-fail** { **offline** | **online authen-domain** *domain-name* }，用户配置认证失败后的处理策略。

认证失败后的处理策略是指当用户认证失败后，NE20E-X6 对用户的处理策略。缺省情况下，当用户认证失败后，NE20E-X6 直接使用户下线；如果希望给用户二次认证的机会（例如用户在 PPP 认证失败后再使用 Web 认证），则可以保持用户的在线状态，并将用户归入缺省域（默认为 default0 域）。

步骤 6 （可选）执行命令 **authentication-super** { [**hwtacacs** | **super**] * | **none** } *，配置操作用户的管理级别切换认证方法。

操作用户管理级别切换认证方式主要是为解决操作用户在线后修改本身的管理级别问题，比如：一个 telnet 级别为 2 的用户上线后想切换到级别 3。

NE20E-X6 支持的操作用户管理级别切换的认证方式包括不认证、HWTACACS 认证、Super 认证。NE20E-X6 支持二次级别切换认证，如果当前级别切换认证方法为 Super 认证，但 NE20E-X6 上没有配置 Super 密码，或者当前级别切换认证方法为 HWTACACS 认证，但 HWTACACS 服务器无响应，可以根据配置改用另外一种认证方法。

步骤 7 （可选）执行命令 **authening authen-redirect online authen-domain** *domain-name*，配置重定向域。

配置重定向域可使认证成功和实际认证不成功的用户最终分别从不同的域上线。

实际应用中，通过在重定向域中配置私网 IP 地址池、基于用户 ACL 的访问权限、安全域等，使得对于用户的公/私网地址分配、访问权限、是否做 NAT 等功能都可以按照用

户域进行差异化配置和隔离，从而可节省公网 IP 地址资源，并防止非法攻击占用大量公网 IP 地址资源。

----结束

1.2.4 （可选）配置授权方案

授权方案缺省是本地授权，RADIUS 的认证和授权绑定在一起，HWTACACS 的认证和授权分离。HWTACACS 授权除了针对用户名进行授权外，还包括按命令行进行授权。

背景信息

在路由器上进行如下配置。

说明

在配置 HWTACACS 按命令行授权时需要注意：

- 只有在使用 HWTACACS 协议时，才可以配置某级别的用户按命令行授权。
- HWTACACS 按命令行授权和授权模式（**authorization-mode**）之间并没有联系。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **authorization-scheme** *authorization-scheme-name*，创建授权方案，并进入授权方案视图。

缺省情况下，有一个授权方案，授权方案配置名是 default，不能删除，只能修改。

步骤 4 执行命令 **authorization-mode** { **hwtacacs** | **if-authenticated** | **local** } *[**none**]配置授权模式。

缺省情况下，授权模式为本地授权模式。

如果采用 HWTACACS 授权模式，必须配置 HWTACACS 服务器模板，然后在用户所属域的视图下应用该服务器模板。

步骤 5 执行命令 **authorization-cmd** *privilege-level* **hwtacacs** [**local**]，配置某级别的用户按命令行授权。

缺省情况下，按命令行授权功能处于禁止状态。

如果使能按命令行授权功能，必须配置 HWTACACS 服务器模板，然后在用户所属域的视图下应用该服务器模板。

步骤 6 执行命令 **authorization-cmd no-response-policy** { **online** | **offline** [**max-times** *max-times-value*] }，配置 TACACS 服务器不可用或本地未配置用户而无响应的失败策略。

步骤 7 执行命令 **quit**，退回至 AAA 视图。

步骤 8 执行命令 **quit**，退回至系统视图。

步骤 9 执行命令 **hwtacacs-server template** *template-name*，进入 HWTACACS 服务器模板视图。

步骤 10 执行命令 **hwtacacs-server timer response-timeout** *timeout-value*，配置定时器响应超时时间。

----结束

1.2.5 配置计费方案

配置计费方案是对用户计费的前提。

背景信息

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **accounting-scheme** *scheme-name*，创建计费方案。

NE20E-X6 中固定有两个计费方案 default0、default1，不能删除，只能修改。

- default0 计费方案的计费模式缺省为不计费。
- default1 和自定义的计费方案的计费模式缺省为 RADIUS 计费。

步骤 4 执行命令 **accounting-mode** { **hwtacacs** | **none** | **radius** }，配置计费模式。

NE20E-X6 支持的计费模式包括 RADIUS 计费、HWTACACS 计费和不计费。

步骤 5 （可选）执行命令 **accounting interim interval** *interval* [**second**]，配置实时计费间隔。

实时计费功能是指用户在线过程中，NE20E-X6 定时生成计费报文传送给远端服务器。通过实时计费功能，NE20E-X6 可以在其和远端服务器通信中断时，最大程度的减少计费异常的时间。

实时计费间隔时间单位可配置为分钟或秒。缺省情况下，实时计费间隔时间单位为分钟。

步骤 6 （可选）执行命令 **accounting start-fail** { **offline** | **online** }，配置开始计费失败的处理策略。

开始计费失败策略是指 NE20E-X6 向远端计费服务器发送开始计费报文后，收不到对方响应报文时采取的处理策略，包括保持用户在线和强制用户下线。

缺省情况下，开始计费失败后，NE20E-X6 使用户下线。

步骤 7 （可选）执行命令 **accounting interim-fail** [**max-times** *times*] { **offline** | **online** }，配置实时计费失败的处理策略。

实时计费失败策略是指 NE20E-X6 向远端计费服务器发送的实时计费报文超过重传次数后，仍然收不到对方响应报文时的处理策略，包括保持用户在线和强制用户下线。

缺省情况下，实时计费报文重传次数为 3 次，实时计费失败后保持用户在线。

步骤 8 （可选）执行命令 **accounting send-update**，设置实时计费用户在收到开始计费回应之后立即发送实时计费报文功能。

NE20E-X6 在收到计费服务器计费回应报文后可根据配置决定是否立即发送实时计费报文。

缺省情况下，NE20E-X6 在收到计费服务器计费回应报文后不立即发送实时计费报文。

----结束

1.2.6 （可选）配置记录方案

只有在使用 HWTACACS 协议时，才可以配置记录功能。记录用户执行过的命令、连接次数、系统事件。

背景信息

在路由器上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **recording-scheme** *recording-scheme-name*，创建记录方案，并进入记录方案视图。

缺省情况下，NE20E-X6 中没有记录方案。

步骤 4 执行命令 **recording-mode hwtacacs** *template-name*，配置记录模式。

缺省情况下，记录方案不与 HWTACACS 服务器模板相关联。

步骤 5 执行命令 **quit**，退回至 AAA 视图。

步骤 6 执行命令 **cmd recording-scheme** *recording-scheme-name*，记录用户在路由器上执行过的命令。

步骤 7 执行命令 **outbound recording-scheme** *recording-scheme-name*，记录连接信息。

步骤 8 （可选）执行命令 **system recording-scheme** *recording-scheme-name*，记录系统级事件。

----结束

1.2.7 配置为用户分配 IP 地址

对单个用户可以直接分配 IP 地址，不需要配置地址池，对多个用户分配 IP 地址时，需要配置地址池进行分配。

背景信息

在路由器上进行如下配置。

说明

在只有一个用户的情况下，可以不必配置地址池，直接为其分配指定的 IP 地址，这时可以省略步骤 2、3、4。第 6 步的命令应运行于 POS 等支持 PPP 协议的接口

若接口封装了 PPP，本端接口还未配置 IP 地址而对端已有 IP 地址时，可为本端接口配置 IP 地址可协商属性，使本端接口接受 PPP 协商产生的由对端分配的 IP 地址。在配置 IP 地址协商时，有以下几点需要注意：

- 因 PPP 支持 IP 地址的协商，所以只有当接口封装了 PPP 时，才能设置接口 IP 地址的协商，当 PPP 协议 Down 时，协商产生的 IP 地址将被删除。
- 配置接口 IP 地址协商后，不需再给该接口配 IP 地址，IP 地址由协商获得。若接口原来配有地址，原 IP 地址将被删除。
- 配置接口 IP 地址协商后，再次配置该接口协商，原协商产生的 IP 地址将被删除，接口再次协商获得 IP 地址。
- 在协商地址被删除后，接口将处于无地址状态。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令，配置本地系统 IP 地址池。

步骤 4 执行命令 **quit**，退回至 AAA 视图。

步骤 5 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 6 执行命令 **remote address** { *ip-address* | **pool** [*pool-number*] }，在服务器端为对端用户分配 IP 地址。在客户端执行命令 **ip address ppp-negotiate**，配置接口 IP 地址为可协商。

----结束

1.2.8 检查配置结果

AAA 方案配置完成后，可以查看认证、授权、计费和记录方案的配置信息，以及用户在线的基本信息。

前提条件

已经完成 AAA 方案的所有配置。

操作步骤

- 执行命令查看 AAA 的概要信息。
- 执行 [*accounting-scheme-name*]命令查看计费方案的配置情况。
- 执行 [*authentication-scheme-name*]命令查看认证方案的配置情况。
- 执行 [*authorization-scheme-name*]命令查看授权方案的配置情况。
- 执行 **display recording-scheme** [*recording-scheme-name*]命令查看记录方案的配置情况。
- 执行 **display ip pool** { **global** | **domain** *domain-name* }命令查看地址池使用情况。

----结束

任务示例

执行 **display aaa configuration** 命令，查看 AAA 的概要信息。

```
<HUAWEI> display aaa configuration
  ------------------------------------------------------------------------------
  AAA configuration information :
  ------------------------------------------------------------------------------
  Domain                : total: 255   used: 2
  Authentication-scheme : total: 16    used: 2
  Authorization-scheme  : total: 16    used: 2
  Accounting-scheme     : total: 128   used: 2
  Recording-scheme      : total: 128   used: 0
  AAA-access-user       : total: 384   used: 0
  Access-user-state     : authen: 0    author: 0    accounting: 0
  ------------------------------------------------------------------------------
```

执行 **display authentication-scheme** 命令，查看认证方案的配置信息。

```
<HUAWEI> display authentication-scheme scheme0
  ------------------------------------------------------------------------------
  Authentication-scheme-name   : scheme0
  Authentication-method        : Local authentication
  Authentication-super method  : Super authentication-super
  ------------------------------------------------------------------------------
```

执行 **display authorization-scheme** 命令查看授权方案的配置信息。

```
<HUAWEI> display authorization-scheme scheme0
------------------------------------------------------------------------------
 Authorization-scheme-name   : scheme0
 Authorization-method         : Local authorization
 Authorization-cmd level 0   : disabled
 Authorization-cmd level 1   : disabled
 Authorization-cmd level 2   : enabled  ( Hwtacacs  )
 Authorization-cmd level 3   : disabled
 Authorization-cmd level 4   : disabled
 Authorization-cmd level 5   : disabled
 Authorization-cmd level 6   : disabled
 Authorization-cmd level 7   : disabled
 Authorization-cmd level 8   : disabled
 Authorization-cmd level 9   : disabled
 Authorization-cmd level 10   : disabled
 Authorization-cmd level 11   : disabled
 Authorization-cmd level 12   : disabled
 Authorization-cmd level 13   : disabled
 Authorization-cmd level 14   : disabled
 Authorization-cmd level 15   : disabled
 Authorization-cmd no-response-policy    : Online
------------------------------------------------------------------------------
```

执行 **display accounting-scheme** 命令查看计费方案的配置信息。

```
<HUAWEI> display accounting-scheme scheme0
  ------------------------------------------------------------------------------
  Accounting-scheme-name                : scheme0
  Accounting-method                     : RADIUS accounting
  Realtime-accounting-switch            : Open
  Realtime-accounting-interval(min)     : 5
  Start-accounting-fail-policy          : Cut user
  Realtime-accounting-fail-policy       : Cut user
  Realtime-accounting-failure-retries   : 3

------------------------------------------------------------------------------
```

执行 **display recording-scheme** 命令，查看记录方案的配置信息。

```
<HUAWEI> display recording-scheme scheme0
------------------------------------------------------------------------------
```

```
  Recording-scheme-name       : scheme0
  HWTACACAS-template-name     : template0
------------------------------------------------------------------------------
```

执行 **display ip pool global** 命令，查看全局地址池是用情况。

```
<HUAWEI> display ip pool global
  ------------------------------------------------------------------------------
  Pool-number  Pool-start-addr   Pool-end-addr   Pool-length  Used-addr-number
  ------------------------------------------------------------------------------
      2        10.1.1.1          10.1.1.10          10             0
  ------------------------------------------------------------------------------
  Total pool number:    1
```

1.3 配置 RADIUS 服务器

当对用户的认证、计费通过远端 RADIUS 服务器时需要配置 RADIUS 服务器。

1.3.1 建立配置任务

在进行 RADIUS 服务器配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

1.3.2 创建 RADIUS 服务器组

RADIUS 服务器组是一组具有相同属性（IP 地址和端口号除外）、采用主备备份或负荷分担方式工作的 RADIUS 服务器的集合。

1.3.3 配置 RADIUS 认证/计费服务器

RADIUS 认证服务器和计费服务器使用一台服务器时应使用不同的端口。

1.3.4 （可选）配置 RADIUS 服务器的选择算法

当 RADIUS 服务器组中的认证/计费服务器多于一个时，可配置选择服务器的算法，包括负荷分担和主备备份两种。

1.3.5 （可选）配置 RADIUS 服务器的协商参数

RADIUS 服务器的协商参数是指 RADIUS 服务器和 NE20E-X6 通信时，双方对 RADIUS 协议以及消息格式的参数约定。

1.3.6 （可选）配置 RADIUS 属性禁用

必须先使能 RADIUS 属性解释功能，属性禁用功能才能生效。

1.3.7 （可选）配置 RADIUS 属性转换功能

通过使能 RADIUS 属性转换功能，NE20E-X6 可以对接不同厂家的 RADIUS 服务器。

1.3.8 （可选）配置 RADIUS 服务器下发隧道密码方式

RADIUS 服务器下发隧道密码的方式包括明文方式和密文方式。

1.3.9 （可选）配置使用 Class 属性携带 CAR 值

通过配置 Class 属性是否携带 CAR 值以适应不同的 RADIUS 服务器。

1.3.10 （可选）配置 NAS-Port 相关属性格式

通过配置 NAS-Port 相关属性格式以适应不同厂商设备。

1.3.11 （可选）配置 RADIUS 服务器源接口

当设备连接多个 RADIUS 服务器时，配置 RADIUS 服务器源接口可明确设备与 RADIUS 服务器连接的路由。

1.3.12 （可选）配置 RADIUS 授权服务器

可配置多个 RADIUS 授权服务器，主要用于动态业务的业务授权。

1.3.13 （可选）配置 RADIUS 服务器状态参数

通过 RADIUS 服务器状态参数配置实现监控 RADIUS 服务器状态的目的。

1.3.14 （可选）配置 RADIUS 扩展源端口
如果不想使用默认扩展源端口来收发 RADIUS 报文的话,需要改变 RADIUS 扩展源端口。

1.3.15 检查配置结果
完成 RADIUS 服务器配置后，您可以查看到 RADIUS 服务器的配置信息、系统支持的 RADIUS 属性、RADIUS 报文统计信息。

1.3.1 建立配置任务

在进行 RADIUS 服务器配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

当在路由器配置 AAA 使用的是 RADIUS 协议时，需要配置 RADIUS 服务器相关信息。

NE20E-X6 中使用 RADIUS 服务器组对 RADIUS 服务器进行管理，RADIUS 服务器组是一组具有相同属性（IP 地址和端口号除外）、采用主备备份或负荷分担方式工作的 RADIUS 服务器的集合。

说明

- 在 RADIUS 的配置中，几乎都有缺省配置，用户也可以根据实际组网需求进行配置。
- RADIUS 服务器组不论是否有用户使用，都可以修改或者删除，并且原来的用户不受影响。

前置任务

使能 RADIUS 协议功能。

数据准备

在配置 RADIUS 服务器之前，请根据网络规划，准备好以下数据。

序号	数据
1	RADIUS 服务器组名称
2	（可选）RADIUS 服务器的选择算法
3	RADIUS 认证服务器的 IP 地址、端口号
4	RADIUS 计费服务器的 IP 地址、端口号
5	（可选）RADIUS 服务器的协议版本
6	（可选）RADIUS 服务器的密钥
7	（可选）RADIUS 服务器的用户名格式
8	（可选）RADIUS 服务器的流量单位
9	（可选）RADIUS 服务器应答超时时间、RADIUS 报文的重传次数
10	（可选）需要禁用的 RADIUS 属性

序号	数据
11	（可选）是否启用 RADIUS 属性转换功能以及转换的源 RADIUS 属性和目的 RADIUS 属性
12	（可选）是否在 RADIUS 报文中使用 Class 属性携带 CAR 值
13	（可选）RADIUS 授权服务器的 IP 地址、VPN 实例、共享密钥、所在 RADIUS 服务器组、授权回应报文的保留时长
14	（可选）判定 RADIUS 服务器异常的连续无响应次数、恢复 RADIUS 服务器状态的等待时间
15	（可选）RADIUS 服务器扩展源端口数、起始扩展源端口号

1.3.2 创建 RADIUS 服务器组

RADIUS 服务器组是一组具有相同属性（IP 地址和端口号除外）、采用主备备份或负荷分担方式工作的 RADIUS 服务器的集合。

背景信息

NE20E-X6 中一共可配置 128 个 RADIUS 服务器组。

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **radius-server group** *group-name*，创建 RADIUS 服务器组。

创建 RADIUS 服务器组后，系统进入 RADIUS 服务器组视图。如果 RADIUS 服务器组已经存在，则执行上述步骤直接进入 RADIUS 服务器组视图。

----结束

1.3.3 配置 RADIUS 认证/计费服务器

RADIUS 认证服务器和计费服务器使用一台服务器时应使用不同的端口。

背景信息

配置 RADIUS 认证/计费服务器需要指定以下参数：

- 认证/计费服务器的 IP 地址；
- 认证/计费服务器所属的 VPN 实例，缺省为公网 VPN 实例 public；
- 认证/计费服务器的端口号，缺省值为 1812 和 1813；
- 认证/计费服务器的权重，只对负荷分担方式有效，缺省为 0。

说明

RADIUS 认证服务器和计费服务器可以使用相同的 IP 地址，即同一台服务器既可以是认证服务器也可以是计费服务器。

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **radius-server group** *group-name*，进入 RADIUS 服务器组视图。

步骤 3 执行命令 **radius-server authentication** { *ip-address* [**vpn-instance** *instance-name*] | *ipv6-address* } *port* [**weight** *weight-value*]，配置 RADIUS 认证服务器。

步骤 4 执行命令 **radius-server accounting** { *ip-address* [**vpn-instance** *instance-name*] | *ipv6-address* } *port* [**weight** *weight-value*]，配置 RADIUS 计费服务器。

步骤 5 （可选）执行命令 **radius-server accounting-stop-packet resend** [*resend-times*]，配置计费服务器的计费结束报文的重发次数。

缺省情况下，计费结束报文的重发次数为 0。

----结束

1.3.4 （可选）配置 RADIUS 服务器的选择算法

当 RADIUS 服务器组中的认证/计费服务器多于一个时，可配置选择服务器的算法，包括负荷分担和主备备份两种。

背景信息

- 负荷分担：多台设备根据各服务器的权重，按比例进行负荷分配。
- 主备备份：配置的第一个服务器为主用服务器，其余的为备用服务器。

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **radius-server group** *group-name*，进入 RADIUS 服务器组视图。

步骤 3 执行命令 **radius-server algorithm** { **loading-share** | **master-backup** }，配置 RADIUS 服务器的选择算法。

缺省情况下，RADIUS 服务器的选择算法为主备备份。

----结束

1.3.5 （可选）配置 RADIUS 服务器的协商参数

RADIUS 服务器的协商参数是指 RADIUS 服务器和 NE20E-X6 通信时，双方对 RADIUS 协议以及消息格式的参数约定。

背景信息

RADIUS 服务器的协商参数主要包括：

- RADIUS 协议版本

  NE20E-X6 支持标准 RADIUS、RADIUS+1.0、RADIUS+1.1 协议。

- IP Hotel 型服务器支持 RADIUS+1.0 协议。
- Portal 型服务器支持 RADIUS+1.1 协议。

- 密钥

  密钥用于加密用户口令和生成回应认证符（Response Authenticator）。RADIUS 服务器发送认证报文时，对口令等重要信息使用 MD5 加密，确保认证信息在网络中传输的安全性。

  为了确保认证双方的身份合法性，要求 NE20E-X6 上的密钥与 RADIUS 服务器上的密钥相同。密钥对大小写敏感。

- 用户名格式

  用户名格式为“user@domain”。某些 RADIUS 服务器只支持纯用户名格式，而有的服务器支持包含域名的格式。根据 RADIUS 服务器的不同，需设置 NE20E-X6 传送给 RADIUS 服务器的用户名中是否包含域名。

- 流量单位

  各种 RADIUS 服务器使用的流量单位不尽相同，NE20E-X6 支持多种流量单位，以保证能和各种 RADIUS 服务器的设置相同。

  NE20E-X6 中支持字节、千字节、兆字节、吉字节四种流量单位。

- 重传参数

  当 NE20E-X6 向 RADIUS 服务器发送报文后，如果在指定时间内未收到服务器的响应，NE20E-X6 会重传报文，以避免因短暂的网络拥塞导致认证/计费信息丢失。

  RADIUS 服务器的重传参数包括超时等待时间和重传次数。

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **radius-server group** *group-name*，进入 RADIUS 服务器组视图。

步骤 3 执行命令 **radius-server type** { **standard** | **plus10** | **plus11** }，配置 RADIUS 服务器的协议版本。

缺省情况下，RADIUS 服务器的协议版本为 **standard** 版本。

步骤 4 执行命令 **radius-server shared-key** *key-string* [**authentication** | **accounting**] *ip-address* [**vpn-instance** *instance-name*] *port-number* [**weight** *weight*]，配置 RADIUS 服务器的密钥。

NE20E-X6 可以对每个 RADIUS 服务器的密钥进行设置。

缺省情况下，RADIUS 服务器的密钥为 huawei。

步骤 5 执行命令 **radius-server user-name** { **domain-included** | **original** }，配置 RADIUS 报文用户名格式。

缺省情况下，RADIUS 服务器的用户名格式中包含域名。

步骤 6 执行命令 **radius-server traffic-unit** { **byte** | **gbyte** | **kbyte** | **mbyte** }，配置 RADIUS 报文流量单位。

本配置对非字节的流量单位以及使用标准 RADIUS 协议的服务器无效。

缺省情况下，RADIUS 服务器的流量单位为字节。

步骤 7 执行命令 **radius-server timeout** *timeout-value*，配置 RADIUS 服务器的重传超时时间。

缺省情况下，重传超时时间为 5 秒。

步骤 8 执行命令 **radius-server retransmit** *retry-times*，配置 RADIUS 报文重传参数。

缺省情况下，重传次数为 3。

步骤 9 执行命令 **radius-attribute agent-circuit-id format** { **cn** | **tr-101** }，配置 RADIUS 报文通知上游设备线路 ID 的格式。

缺省情况下，报文采用 cn 格式进行发送。

步骤 10 执行命令 **radius-server calling-station-id include option82**，配置 RADIUS 公有 31 号属性 Calling-Station-Id 属性的构造方式。

缺省情况下，RADIUS 公有 31 号属性的构造方式没有配置。

----结束

1.3.6 （可选）配置 RADIUS 属性禁用

必须先使能 RADIUS 属性解释功能，属性禁用功能才能生效。

背景信息

RADIUS 属性禁用功能配置在 RADIUS 服务器组下，因此只对该 RADIUS 服务器组下的 RADIUS 服务器生效。每个组下最多可以配置 64 个属性禁用。

NE20E-X6 支持同时配置发送方和接收方的属性禁用。

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **radius-server group** *group-name*，进入 RADIUS 服务器组视图。

步骤 3 执行命令 **radius-server attribute translate**，使能 RADIUS 属性转换功能。

步骤 4 执行命令 **radius-attribute disable** *attribute-name* { { **access-accept** | **access-request** | **account** } * | { **receive** | **send** } * }配置 RADIUS 属性禁用或者执行命令 **radius-attribute disable extend** *attribute-description* { **access-accept** | { **access-request** | **account** } * }，配置扩展 RADIUS 属性禁用。

----结束

1.3.7 （可选）配置 RADIUS 属性转换功能

通过使能 RADIUS 属性转换功能，NE20E-X6 可以对接不同厂家的 RADIUS 服务器。

背景信息

不同厂家的 RADIUS 服务器所支持的 RADIUS 属性集以及对某些属性的定义均存在差异，这种差异增加了 NE20E-X6 和 RADIUS 服务器对接的难度。NE20E-X6 提供 RADIUS 属性转换功能适应上述情况。

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **radius-server group** *group-name*，进入 RADIUS 视图。

步骤 3 执行命令 **radius-server attribute translate**，使能 RADIUS 属性转换功能。

步骤 4 执行命令 **radius-attribute translate** *src-attr-description dest-attr-description* { { **access-accept** | **access-request** | **account** } * | { **receive** | **send** } * }或者执行命令 **radius-attribute translate extend** *src-attr-descriptiondest-attr-description* { **access-accept** | { **access-request** | **account** } * }，配置 RADIUS 属性转换。

radius-attribute translate extend 用于配置私有 RADIUS 属性的转换。

当使能并配置了 RADIUS 属性转换功能后，NE20E-X6 在发送和接收 RADIUS 报文时，使用 *dest-attribute* 的属性格式来封装或解析 *src-attribute* 的属性值，以便和不同设备进行对接。

该功能经常用于同一属性值有多种格式的情况。例如 **nas-port-id** 属性有新旧两种格式，NE20E-X6 采用新格式，如果 RADIUS 服务器采用旧格式，则可在 NE20E-X6 上配置 **radius-attribute translate nas-port-id nas-port-identify-old receive send** 命令。

说明

在 NE20E-X6 上最多可配置 64 个不同属性的转换关系。

----结束

1.3.8 （可选）配置 RADIUS 服务器下发隧道密码方式

RADIUS 服务器下发隧道密码的方式包括明文方式和密文方式。

背景信息

虽然 RADIUS 协议规定从 RADIUS 服务器下发的隧道密码必须为密文，但目前很多 RADIUS 服务器并没有严格遵循。因此 NE20E-X6 支持的隧道密码的方式需要可配置，以便适用于各种对接的 RADIUS 服务器。

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **radius-server group** *group-name*，进入 RADIUS 视图。

步骤 3 执行命令 **radius-attribute tunnel-password** { **cipher** | **simple** }，配置 RADIUS 下发隧道密码的方式。

缺省情况下，NE20E-X6 支持 RADIUS 服务器以密文方式下发隧道密码。

----结束

1.3.9 （可选）配置使用 Class 属性携带 CAR 值

通过配置 Class 属性是否携带 CAR 值以适应不同的 RADIUS 服务器。

背景信息

在标准 RADIUS 协议中，在 RADIUS 服务器发送给客户端认证报文（Access-Accept）中的 Class 属性，必须由客户端在计费报文（Accounting-Request）中不加修改的发送给计费服务器。

NE20E-X6 在标准协议的基础上进行了扩展，增加传送 CAR（Committed Access Rate）值的功能，即在实现 Class 属性（RADIUS 25 号属性）时携带 Class 字段中的 CAR 值。

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **radius-server group** *group-name*，进入 RADIUS 视图。

步骤 3 执行命令 **radius-server class-as-car** [**enable-pir**]，配置使用 Class 属性携带 CAR 值。

缺省情况下，RADIUS 服务器不使用 Class 属性携带 CAR 值。

说明

为了适应不同的 RADIUS 服务器，NE20E-X6 可通过 RADIUS 的 25 号属性传送 CAR 值给 RADIUS 服务器（如通过上述命令），也可通过 RADIUS 的 26 号属性来传送。

----结束

1.3.10 （可选）配置 NAS-Port 相关属性格式

通过配置 NAS-Port 相关属性格式以适应不同厂商设备。

背景信息

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **radius-server group** *group-name*，进入 RADIUS 视图。

步骤 3 执行命令 **radius-server format-attribute** { **nas-port** *format-string* | **nas-port-idvendor** *vendor-id* }，配置 NAS-Port 属性和 NAS-Port-Id 属性的格式。

说明

配置 NAS-Port-Id 属性格式时：

- 如果指定厂商标识为 2352，NE20E-X6 按照 Redback 厂商的默认格式封装 NAS-Port-Id 属性。
- 如果指定厂商标识为 2636，NE20E-X6 按照 Juniper 厂商的默认格式封装 NAS-Port-Id 属性。
- 如果指定厂商标识为 9，NE20E-X6 按照 Cisco 厂商的默认格式封装 NAS-Port-Id 属性。
- 如果指定为其他厂商标识，NE20E-X6 按照原来的格式封装 NAS-Port-Id 属性。

----结束

1.3.11 （可选）配置 RADIUS 服务器源接口

当设备连接多个 RADIUS 服务器时，配置 RADIUS 服务器源接口可明确设备与 RADIUS 服务器连接的路由。

背景信息

NE20E-X6 支持将和 RADIUS 服务器连接的接口配置成源接口。NE20E-X6 允许在系统模式下和不同的 RADIUS 服务器组下配置源接口。这样 NE20E-X6 在与 RADIUS 交互报文时，如果 RADIUS 服务器组下配置了源接口，则该 RADIUS 服务器组中的 RADIUS 服务器与 NE20E-X6 通信时，使用该组下配置的源接口，否则使用全局 RADIUS 服务器源接口。

请在路由器上进行如下配置

操作步骤

- 配置全局 RADIUS 服务器源接口
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **radius-server source interface** *interface-type interface-number*，配置全局 RADIUS 服务器源接口。
- 配置 RADIUS 服务器组的源接口
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **radius-server group** *group-name*，进入 RADIUS 视图。
  3. 执行命令 **radius-server source interface** *interface-type interface-number*，配置 RADIUS 服务器组的源接口。

----结束

1.3.12 （可选）配置 RADIUS 授权服务器

可配置多个 RADIUS 授权服务器，主要用于动态业务的业务授权。

背景信息

对于动态选择的业务，需要配置 RADIUS 授权服务器，以便在用户进行动态业务选择时对业务进行动态授权。

请在路由器上进行以下配置

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **radius-server authorization** *ip-address* [**vpn-instance** *instance-name*] { **shared-key** *key* | **server-group** *groupname* } * [**ack-reserved-interval** *interval*]，配置全局的 RADIUS 授权服务器。

如果要保留 RADIUS 授权回应报文以用于回应 RADIUS 授权服务器的重传报文，在配置 RADIUS 授权服务器的时候需要配置授权回应报文保留时长。

----结束

1.3.13 （可选）配置 RADIUS 服务器状态参数

通过 RADIUS 服务器状态参数配置实现监控 RADIUS 服务器状态的目的。

背景信息

本配置对所有 RADIUS 服务器有效。

请在路由器上进行以下配置

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **radius-server** { **dead-count** *times* | **dead-interval** *interval* | **dead-time** *time* }，配置 RADIUS 服务器的状态参数。

缺省情况下，判定 RADIUS 服务器异常的连续无响应次数为 10 次，从第一个没有响应报文到设置的 **dead-count** 个数的没有响应报文之间的时间间隔为 5 秒，恢复 RADIUS 服务器状态的等待时间为 3 分钟。

当 NE20E-X6 向 RADIUS 服务器连续发送若干次（通过本命令设置）RADIUS 报文，均收不到 RADIUS 服务器的响应报文时，且从第一个没有响应报文到设置的 **dead-count** 个数的没有响应报文之间的时间间隔大于设置的 **dead-interval** 时，NE20E-X6 判定该 RADIUS 服务器工作异常，并将 RADIUS 服务器的状态置为 Down。

当 NE20E-X6 将 RADIUS 的状态置为 Down 后，等待若干时间（通过本命令配置），NE20E-X6 会重新将 RADIUS 服务器的状态置为 UP，并尝试和 RADIUS 服务器重新建立连接。如果连接失败，重新将 RADIUS 服务器的状态置为 Down。

----结束

1.3.14 （可选）配置 RADIUS 扩展源端口

如果不想使用默认扩展源端口来收发 RADIUS 报文的话,需要改变 RADIUS 扩展源端口。

背景信息

配置 RADIUS 扩展源端口，可在一定时间内增加 NE20E-X6 向 RADIUS 服务器发送的非重复的报文数。

配置后，NE20E-X6 使用扩展源端口收发 RADIUS 报文。其中，扩展源端口的前一半用来收发 RADIUS 认证报文，后一半用来收发 RADIUS 计费报文。若配置的扩展源端口数为奇数，则收发认证报文的端口比收发计费报文的端口多一个。

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **radius-server extended-source-ports** [**start-port** *star-port-number*] **port-number** *port-number*,配置 RADIUS 扩展源端口

缺省情况下，系统没有配置 RADIUS 扩展源端口。此时，NE20E-X6 使用默认的 1812 端口收发 RADIUS 认证报文，1813 端口收发 RADIUS 计费报文。

说明

如果配置时不指定扩展源端口的起始端口号，则由系统分配指定数目（即配置的扩展源端口数）的有效的扩展源端口。

----结束

1.3.15 检查配置结果

完成 RADIUS 服务器配置后，您可以查看到 RADIUS 服务器的配置信息、系统支持的 RADIUS 属性、RADIUS 报文统计信息。

前提条件

已经完成服务器模板的所有配置。

操作步骤

- 执行 **display radius-server authorization configuration** 命令，查看 RADIUS 授权服务器的配置信息。
- 执行 **display radius-server configuration** [**group** *groupname*]命令，查看 RADIUS 服务器组的配置信息。
- 执行 **display radius-attribute** [**name** *attribute-name* | { **type** { **3gpp** | **dsl** | **huawei** | **microsoft** | **redback** | **standard** } [*attribute-number*] }]命令或者 **display radius-attribute** [*attribute-name*]命令，查看系统所支持的 RADIUS 属性。
- 执行 **display radius-client configuration** 命令，查看所有 RADIUS 客户端的配置信息。
- 执行 **display radius-server packet ip-address** *ip-address* [*vpn-instance*] { **accounting** | **authentication** }命令，查看指定 IP 地址的 RADIUS 服务器的报文的统计信息。

----结束

任务示例

执行命令 **display radius-server authorization configuration**，查看 RADIUS 授权服务器的配置信息。

```
<HUAWEI> display radius-server authorization configuration
  ------------------------------------------------------------------------------
  IP-Address         Secret-key         Group                          Ack-r
eserved-interval
  ------------------------------------------------------------------------------
  192.168.7.100      huawei             rd1                            20
    Vpn : --
  ------------------------------------------------------------------------------
  1 Radius authorization server(s) in total
```

执行 **display radius-server configuration** 命令，查看 RADIUS 服务器组的配置信息。

```
<HUAWEI> display radius-server configuration
  RADIUS source interface            : LoopBack20
  RADIUS no response packet count    : 30
  RADIUS auto recover time(Min)      : 100
  RADIUS authentication source ports :
         IPv4: 1812
         IPv6: 1812
  RADIUS accounting source ports     :
         IPv4: 1813
         IPv6: 1813
```

```
  ------------------------------------------------------
  Server-group-name    :  chen
  Authentication-server:  IP:1.3.4.144 Port:1812 Weight[0] [UP]
                          Vpn: -
  Accounting-server    :  IP:1.3.4.144 Port:1814 Weight[0] [UP]
                          Vpn: -
  Protocol-version     :  radius
  Shared-secret-key    :  huawei
  Retransmission       :  3
  Timeout-interval(s)  :  5
  Acct-Stop-Packet Resend  :  NO
  Acct-Stop-Packet Resend-Times  :  0
  ------------------------------------------------------
  Are you sure to display next (y/n)[y]:y
  ------------------------------------------------------
  Server-group-name    :  huawei
  Authentication-server:  IP:10.1.1.1 Port:1820 Weight[50] [UP]
                          Vpn: -
  Accounting-server    :  IP:10.1.1.1 Port:1823 Weight[0] [UP]
                          Vpn: -
  Accounting-server    :  IP:10.1.1.2 Port:20 Weight[20] [UP]
                          Vpn: -
                          share-key:  huawei
  Protocol-version     :  radius
  Shared-secret-key    :  huawei
  Retransmission       :  2
  Timeout-interval(s)  :  8
  Acct-Stop-Packet Resend  :  YES
  Acct-Stop-Packet Resend-Times  :  100
  ------------------------------------------------------
  Total 2,2 printed
```

执行命令 **display radius-attribute** [**name** *attribute-name* | { **type** { **3gpp** | **dsl** | **huawei** | **microsoft** | **redback** | **standard** } [*attribute-number*] } 查看 NE20E-X6 当前版本支持的 RADIUS 标准属性。

```
<HUAWEI> display radius-attribute type standard 1
 Radius Attribute Type        : 1
 Radius Attribute Name        : User-Name
 Radius Attribute Description : This Attribute indicates the name of the user to
 be authenticated.
 Supported Packets            : Auth Request, Acct Request, Session Control, COA
 Request, COA Ack
```

执行 **display radius-client configuration** 命令，查看所有 RADIUS 客户端的配置信息。

```
<HUAWEI> display radius-client configuration
-------------------------------------------------------------------------------
  IP-Address         Secret-key        Group
-------------------------------------------------------------------------------
  172.194.0.10       huawei            sim3
  172.194.0.20       huawei            sim3
  7.0.200.10         huawei            sim3
  1.1.1.1            1                 xzn
    Vpn : dsg
-------------------------------------------------------------------------------
  4 Radius client(s) in total
```

执行 **display radius-server packet ip-address** *ip-address* [*vpn-instance*] **accounting** 命令，查看指定 IP 地址的 RADIUS 服务器的计费报文的统计信息。

```
<HUAWEI>display radius-server packet ip-address 74.1.1.2 accounting
  Account Requests   : 1          Account Retransmissions     : 19
  Account Responses  : 0          Malformed Account Responses : 0
  Bad Authenticators : 0         Pending Requests           : 0
  Timeouts           : 20          Unknown Types              : 0
  Packets Dropped    : 0
```

执行 **display radius offline-sub-reason** [**subcode** *subcode-number*]命令，查看指定设备上送给 RADIUS 服务器的停止计费报文中的用户下线原因的编号对应的描述信息。

```
<HUAWEI> display radius offline-sub-reason subcode 1
--------------------------------------------------------------------------------
Subcode     description of offline sub reason
--------------------------------------------------------------------------------
1           User request to offline
--------------------------------------------------------------------------------
```

1.4 配置 HWTACACS 服务器

当对用户的认证、计费通过远端 HWTACACS 服务器时需要配置 HWTACACS 服务器。

1.4.1 建立配置任务
在进行 HWTACACS 服务器配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

1.4.2 创建 HWTACACS 服务器模板
创建 HWTACACS 服务器模板是配置 HWTACACS 服务器的必备条件。

1.4.3 配置 HWTACACS 认证/计费/授权服务器
主认证服务器和备用认证服务器的 IP 地址和绑定的 VPN 实例不能完全相同，否则将提示配置不成功。

1.4.4 配置 HWTACACS 服务器的源 IP 地址
HWTACACS 服务器的源 IP 地址，是指当 NE20E-X6 向 HWTACACS 服务器发送报文时，报文所使用的源 IP 地址。

1.4.5 （可选）配置 HWTACACS 服务器的协商参数
通信双方对 HWTACACS 协议以及消息格式的参数约定必须一致。

1.4.6 （可选）配置 HWTACACS 服务器的定时器
配置 HWTACACS 服务器的定时器是一种检测检测服务器工作是否正常的方式，在网络调整优化时才需要配置。

1.4.7 （可选）配置计费结束报文的重传功能
只有在网络状况不理想时才需要进行配置计费结束报文的重传功能。

1.4.8 （可选）配置 HWTACACS 用户主动修改用户密码
配置 HWTACACS 用户主动修改用户密码使运营商能提供更方便、快捷的服务。

1.4.9 检查配置结果
完成 HWTACACS 服务器配置后，您可以查看到 HWTACACS 服务器的配置信息。

1.4.1 建立配置任务

在进行 HWTACACS 服务器配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

当 AAA 使用 HWTACACS 协议时，需要配置 HWTACACS 服务器。

NE20E-X6 中使用 RADIUS 服务器组对 RADIUS 服务器进行管理，RADIUS 服务器组是一组具有相同属性（IP 地址和端口号除外）、采用主备备份或负荷分担方式工作的 RADIUS 服务器的集合。

说明

- 除删除服务器外，HWTACACS 的大部分属性在改变配置时都不检查当前是否有用户在使用此模板。
- HWTACACS 服务器缺省没有密钥。

前置任务

无

数据准备

在配置 HWTACACS 服务器之前，请根据网络规划，准备好以下数据。

序号	数据
1	HWTACACS 服务器模板名称
2	HWTACACS 主认证、授权、计费服务器的 IP 地址和端口号及需要绑定的 VPN 实例
3	HWTACACS 备份认证、授权、计费服务器的 IP 地址、端口号
4	计费结束报文重传次数或禁止重传
5	HWTACACS 服务器的源 IP 地址
6	（可选）HWTACACS 服务器的密钥
7	（可选）HWTACACS 服务器的用户名格式
8	（可选）HWTACACS 服务器的流量单位
9	（可选）HWTACACS 服务器应答超时时间
10	（可选）HWTACACS 主服务器的恢复激活时间

1.4.2 创建 HWTACACS 服务器模板

创建 HWTACACS 服务器模板是配置 HWTACACS 服务器的必备条件。

背景信息

NE20E-X6 中一共可配置 128 个 HWTACACS 服务器模板。

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **hwtacacs-server template** *template-name*，创建 HWTACACS 服务器模板，并进入 HWTACACS 服务器模板视图。

如果 HWTACACS 服务器模板已经存在，则执行上述命令直接进入 HWTACACS 视图。

----结束

1.4.3 配置 HWTACACS 认证/计费/授权服务器

主认证服务器和备用认证服务器的 IP 地址和绑定的 VPN 实例不能完全相同，否则将提示配置不成功。

背景信息

请在路由器上进行以下配置。

操作步骤

- 配置 HWTACACS 的认证服务器
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **hwtacacs-server template** *template-name*，进入 HWTACACS 服务器模板视图。
  3. 执行命令 **hwtacacs-server authentication** *ip-address* [*port*] [**vpn-instance** *vpn-instance-name*]，配置 HWTACACS 的主认证服务器。

     缺省情况下，主用 HWTACACS 认证服务器的 IP 地址为 0.0.0.0，不绑定 VPN 实例。
  4. 执行命令 **hwtacacs-server authentication** *ip-address* [*port*] [**vpn-instance** *vpn-instance-name*] **secondary**，配置 HWTACACS 的备份认证服务器。

     缺省情况下，备用 HWTACACS 认证服务器的 IP 地址为 0.0.0.0，不绑定 VPN 实例。
- 配置 HWTACACS 的授权服务器
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **hwtacacs-server template** *template-name*，进入 HWTACACS 服务器模板视图。
  3. 执行命令 **hwtacacs-server authorization** *ip-address* [*port*] [**vpn-instance** *vpn-instance-name*]，配置 HWTACACS 的主授权服务器。

     缺省情况下，主用 HWTACACS 授权服务器的 IP 地址为 0.0.0.0，不绑定 VPN 实例。
  4. 执行命令 **hwtacacs-server authorization** *ip-address* [*port*] [**vpn-instance** *vpn-instance-name*] **secondary**，配置 HWTACACS 的备份授权服务器。

     缺省情况下，备用 HWTACACS 授权服务器的 IP 地址为 0.0.0.0，不绑定 VPN 实例。
- 配置 HWTACACS 的计费服务器
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **hwtacacs-server template** *template-name*，进入 HWTACACS 服务器模板视图。
  3. 执行命令 **hwtacacs-server accounting** *ip-address* [*port*] [**vpn-instance** *vpn-instance-name*]，配置 HWTACACS 的主计费服务器。

缺省情况下，主用 HWTACACS 计费服务器的 IP 地址为 0.0.0.0，不绑定 VPN 实例。

4. 执行命令 **hwtacacs-server accounting** *ip-address* [*port*] [**vpn-instance** *vpn-instance-name*] **secondary**，配置 HWTACACS 的备份计费服务器。

   缺省情况下，备用 HWTACACS 计费服务器的 IP 地址为 0.0.0.0，不绑定 VPN 实例。

----结束

1.4.4 配置 HWTACACS 服务器的源 IP 地址

HWTACACS 服务器的源 IP 地址，是指当 NE20E-X6 向 HWTACACS 服务器发送报文时，报文所使用的源 IP 地址。

背景信息

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **hwtacacs-server template** *template-name*，进入 HWTACACS 视图。

步骤 3 执行命令 **hwtacacs-server source-ip** *ip-address*，配置 HWTACACS 服务器的源 IP 地址。

缺省情况下，HWTACACS 源 IP 地址是 0.0.0.0，此时 NE20E-X6 使用实际出接口的 IP 地址作为 HWTACACS 报文的源 IP 地址。

指定 HWTACACS 源 IP 地址后，使用该 HWTACACS 模板与服务器通信时，报文的源 IP 地址为指定的 IP 地址。此时，服务器也将使用指定的 IP 地址与 NE20E-X6 通信。

----结束

1.4.5 （可选）配置 HWTACACS 服务器的协商参数

通信双方对 HWTACACS 协议以及消息格式的参数约定必须一致。

背景信息

HWTACACS 服务器的协商参数是指 HWTACACS 服务器和 NE20E-X6 通信时，双方对 HWTACACS 协议以及消息格式的参数约定，主要包括：

- HWTACACS 协议密钥

  使用密钥可以提高 NE20E-X6 与 HWTACACS 服务器通信的安全性。

  为了确保认证双方的身份合法性，要求 NE20E-X6 上的密钥与 HWTACACS 服务器上的密钥相同。

  密钥对大小写敏感。

- 用户名格式

  NE20E-X6 中的用户名格式为“user@domain”。如果 HWTACACS 服务器不接收带域名的用户名格式，可以将去掉域名后的纯用户名格式传送 HWTACACS 服务器。

- 流量单位

  NE20E-X6 中支持字节、千字节、兆字节、吉字节四种流量单位，以保证能和 HWTACACS 服务器的设置相同。

请在路由器上进行以下配置。

操作步骤

- （可选）配置 HWTACACS 服务器的密钥
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **hwtacacs-server template** *template-name*，进入 HWTACACS 服务器模板视图。
  3. 执行命令 **hwtacacs-server shared-key***key-string*，配置 HWTACACS 服务器的密钥。

     缺省情况下，HWTACACS 共享密钥为空。

     设置密钥可以提高 NE20E-X6 与 HWTACACS 服务器通信的安全性。

     说明

     为了确保认证双方的身份合法性，要求路由器上的密钥与 HWTACACS 服务器的密钥必须相同。
- （可选）配置 HWTACACS 服务器的用户名格式
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **hwtacacs-server template** *template-name*，进入 HWTACACS 服务器模板视图。
  3. 执行命令 **hwtacacs-server user-name domain-included**，配置 HWTACACS 服务器的用户名格式。

     缺省情况下，HWTACACS 用户名格式为用户名包含域名。

     如果 HWTACACS 服务器不接受带域名的用户名时，可以配置将用户名中的域名去掉后再传送给 HWTACACS 服务器。

     说明

     用户名通常采用“纯用户名@域名”格式，@后面的部分为域名。
- （可选）配置 HWTACACS 服务器的流量单位
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **hwtacacs-server template** *template-name*，进入 HWTACACS 服务器模板视图。
  3. 执行命令 **hwtacacs-server traffic-unit** { **byte** | **kbyte** | **mbyte** | **gbyte** }，配置 HWTACACS 服务器的流量单位。

     缺省情况下，NE20E-X6 使用字节做为流量单位（byte）。

----结束

1.4.6 （可选）配置 HWTACACS 服务器的定时器

配置 HWTACACS 服务器的定时器是一种检测检测服务器工作是否正常的方式，在网络调整优化时才需要配置。

背景信息

NE20E-X6 向 HWTACACS 服务器发送报文后，在指定的等待时间内未收到服务器的响应报文，则认为连接已经断开。上述的等待时间即为 HWTACACS 服务器应答超时时间。

说明

由于 HWTACACS 是基于 TCP 实现的，因此，服务器应答超时或 TCP 超时都可能导致 NE20E-X6 与 HWTACACS 服务器的连接断开。

当 NE20E-X6 判断和 HWTACACS 主服务器的连接已经断开时，NE20E-X6 会等待指定的时间，然后重新尝试和主服务器建立连接。上述的等待时间即为 HWTACACS 主服务器恢复激活时间。

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **hwtacacs-server template** *template-name*，进入 HWTACACS 视图。

步骤 3 执行命令 **hwtacacs-server timer response-timeout** *value*，配置 HWTACACS 服务器应答超时时间。

缺省情况下，HWTACACS 服务器应答超时时间为 5 秒。

步骤 4 执行命令 **hwtacacs-server timer quiet** *value*，配置 HWTACACS 主服务器恢复激活时间。

缺省情况下，HWTACACS 主服务器恢复激活时间为 5 分钟。

----结束

1.4.7 （可选）配置计费结束报文的重传功能

只有在网络状况不理想时才需要进行配置计费结束报文的重传功能。

背景信息

使用 HWTACACS 计费模式时，用户下线后，NE20E-X6 会生成计费结束报文传送给 HWTACACS 服务器。如果网络状况不是非常理想，可以配置计费结束报文的重传功能，以保证计费信息不会丢失。

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **hwtacacs-server accounting-stop-packet resend** { **disable** | **enable** *number* }，配置计费结束报文的重传功能。

可以配置是否启用计费结束报文的重传功能以及报文的重传次数。缺省情况下，NE20E-X6 启用计费结束报文的重传功能，报文的重传次数为 100。

计费停止报文用来通知服务器停止计费。如果计费服务器没有收到该报文将持续对用户进行计费。

如果计费服务器没有收到计费停止报文，NE20E-X6 可以重传该报文，直到服务器收到该报文或达到指定的重传次数。

----结束

1.4.8 （可选）配置 HWTACACS 用户主动修改用户密码

配置 HWTACACS 用户主动修改用户密码使运营商能提供更方便、快捷的服务。

背景信息

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **hwtacacs-user change-password hwtacacs-server** *template-name*，修改 HWTACACS 用户的密码。

说明

- 登录设备的用户必须经过 HWTACACS 认证，且服务器模板必须已经存在。
- 只有在 TACACS 服务器上保存的用户名和密码没有过期的情况下，才允许用户主动使用该命令修改密码。
- 对于密码已经过期的用户，登录设备时，TACACS 服务器将返回认证不成功，不允许用户主动更改密码。

----结束

1.4.9 检查配置结果

完成 HWTACACS 服务器配置后，您可以查看到 HWTACACS 服务器的配置信息。

前提条件

已经完成服务器模板的所有配置。

操作步骤

- 执行 **display hwtacacs-server template** [*template-name* [**verbose**]]命令查看 TACACS 服务器模板的配置信息。
- 执行 **display hwtacacs-server accounting-stop-packet** { **all** | *number* | **ip***ip-address* }命令查看 TACACS 服务器的计费停止报文情况。

----结束

任务示例

执行命令 **display hwtacacs-server template**，可以查看 TACACS 服务器信息。

```
<HUAWEI> display hwtacacs-server template
  ------------------------------------------------------------
  HWTACACS-server template name   : 123
  Primary-authentication-server   : 0.0.0.0:0:-
  Primary-authorization-server    : 0.0.0.0:0:-
  Primary-accounting-server       : 0.0.0.0:0:-
  Secondary-authentication-server : 0.0.0.0:0:-
  Secondary-authorization-server  : 0.0.0.0:0:-
  Secondary-accounting-server     : 0.0.0.0:0:-
```

```
Current-authentication-server   : 0.0.0.0:0:-
Current-authorization-server    : 0.0.0.0:0:-
Current-accounting-server       : 0.0.0.0:0:-
Source-IP-address               : 0.0.0.0
Shared-key                      : -
Quiet-interval(min)             : 5
Response-timeout-Interval(sec)  : 5
Domain-included                 : Yes
Traffic-unit                    : B
-------------------------------------------------------------
Are you sure to display more information (y/n)[y]:y
-------------------------------------------------------------
HWTACACS-server template name   : test1
Primary-authentication-server   : 1.1.11.1:49:vpna
Primary-authorization-server    : 0.0.0.0:0:-
Primary-accounting-server       : 1.1.1.1:49:vpna
Secondary-authentication-server : 0.0.0.0:0:-
Secondary-authorization-server  : 1.1.1.1:12:vpna
Secondary-accounting-server     : 0.0.0.0:0:-
Current-authentication-server   : 1.1.11.1:49:vpna
Current-authorization-server    : 1.1.1.1:12:vpna
Current-accounting-server       : 1.1.1.1:49:vpna
Source-IP-address               : 1.1.1.1
Shared-key                      : -
Quiet-interval(min)             : 5
Response-timeout-Interval(sec)  : 5
Domain-included                 : Yes
Traffic-unit                    : B
-------------------------------------------------------------
Total 2,2 printed
```

1.5 配置话单本地保存

话单本地保存是对远端计费服务器的备份，防止远端服务器故障，计费信息丢失。

1.5.1 建立配置任务
在进行话单本地保存配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

1.5.2 创建本地话单池
创建本地话单池是实现话单本地保存功能的前提。

1.5.3 配置缓存中话单备份模式
缺省情况下缓存中的话单保存到 CF 卡，但 CF 卡容量有限，配置缓存的话单备份模式可更改话单保存路径。

1.5.4 （可选）配置将 CF 卡中的话单保存到话单服务器
因为 CF 卡容量有限，应该将 CF 卡中的话单保存到话单服务器，避免 CF 卡中的话单超过告警阈值，计费信息丢失。

1.5.5 （可选）配置将缓存中的话单保存到话单服务器
因为缓存和 CF 容量都较小，强烈建议将缓存中的话单保存到话单服务器。

1.5.6 检查配置结果
完成话单本地保存配置后，您可以查看到话单本地保存的配置信息。

1.5.1 建立配置任务

在进行话单本地保存配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

当远端计费服务器出现异常时，不能和接入设备正常连接的时候，为防止计费信息丢失，可应用话单本地保存功能，将生成的话单保存在本地。

应用话单本地保存功能后，NE20E-X6 会将生成的话单先保存在缓存中。用户可选择将缓存中的话单保存到 CF 卡，或者通过 TFTP 方式保存到话单服务器中。CF 卡中的话单也可备份到话单服务器中。

NE20E-X6 可通过命令创建或删除本地话单池。话单本地保存功能是以本地话单池的存在为前提的，如果没有本地话单池，话单本地保存功能随之失效，也不会进行话单备份。

前置任务

无

数据准备

在配置本地计费之前，请根据网络规划，准备好以下数据。

序号	数据
1	话单服务器 IP 地址和文件名
2	（可选）CF 卡、缓存中的话单告警阈值
3	（可选）CF 卡、缓存中的话单自动备份的时间间隔
4	（可选）缓存中的话单备份模式

1.5.2 创建本地话单池

创建本地话单池是实现话单本地保存功能的前提。

背景信息

NE20E-X6 支持通过命令创建或删除本地话单池。只有创建了本地话单池，才会有话单本地保存功能。若删除本地话单池，本地话单池中的本地话单也会被删除，因此删除本地话单池前需手动备份本地话单。

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **local-aaa-server**，进入本地 AAA 服务器视图。

步骤 3 执行命令 **local-bill-pool enable**，使能本地话单池功能。

缺省情况下 NE20E-X6 没有使能本地话单池功能。

----结束

1.5.3 配置缓存中话单备份模式

缺省情况下缓存中的话单保存到 CF 卡，但 CF 卡容量有限，配置缓存的话单备份模式可更改话单保存路径。

背景信息

缓存中的话单备份模式包括三种：备份到 CF 卡、通过 TFTP 备份到话单服务器、不备份。

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **local-aaa-server**，进入本地 AAA 视图。

步骤 3 执行命令 **local-bill cache backup-mode** { **cfcard** | **none** | **tftp** }，配置缓存的话单备份模式。

缺省情况下，缓存中的话单保存到 CF 卡。即当缓存中的话单超过告警阈值后，经过固定的时间间隔，缓存中的话单就会自动保存到 CF 卡中并清空缓存中的话单。但是受 CF 卡容量所限，经过一段时间后就必须将 CF 卡中的话单再保存到话单服务器中。建议直接将缓存中的话单保存到话单服务器中。

----结束

1.5.4 （可选）配置将 CF 卡中的话单保存到话单服务器

因为 CF 卡容量有限，应该将 CF 卡中的话单保存到话单服务器，避免 CF 卡中的话单超过告警阈值，计费信息丢失。

背景信息

说明

缺省情况下，缓存中的话单自动保存到 CF 中，但是 CF 卡的容量有限，所以必须将 CF 卡中的话单保存到话单服务器。

请在路由器上进行以下配置。

操作步骤

- 配置话单服务器
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **local-aaa-server**，进入本地 AAA 服务器视图。
  3. 执行命令 **bill-server** *ip-address* **filename** *file-name*，配置备份话单服务器。

     在 NE20E-X6 上配置话单服务器，需要指定话单服务器的 IP 地址，以及话单的文件名前缀。话单的格式为“文件名前缀-时间-编号.lam”。例如文件名前缀为“backupfile”，备份时间为 2005 年 3 月 15 日 15 点 26 分，备份时生成 10 个文件，那么第五个文件的名称为“backupfile-200503151526-5.lam”。

说明

NE20E-X6 使用 TFTP 协议登录话单服务器，进行话单文件保存操作。因此在话单服务器上必须运行 TFTP 服务器程序，并指定工作目录。

- 配置 CF 卡中话单的告警阈值
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **local-aaa-server**，进入本地 AAA 服务器视图。
  3. 执行命令 **local-bill cfcard alarm-threshold** *threshold*，配置 CF 卡的话单告警阈值。

     缺省情况下，CF 卡中的话单告警阈值为 75%。

  当 CF 卡中的话单超过告警阈值的时候，需要将 CF 中的话单保存到话单服务器。保存方式分为自动和手动两种。缺省情况下是自动保存，即经过固定的时间间隔后，系统自动将 CF 卡中的话单保存到话单服务器；如果用户希望自己手动保存，可通过配置命令 **local-bill cfcard backup** [*file-name*]实现。那么当 CF 卡中的话单超过告警阈值的时候，系统会向网管系统和终端发送告警，提醒用户手动将 CF 卡中的话单保存到话单服务器。
- 配置话单自动备份的时间间隔
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **local-aaa-server**，进入本地 AAA 服务器视图。
  3. 执行命令 **local-bill cfcard backup-interval** *interval*，配置 CF 卡的话单自动备份的时间间隔。

     缺省情况下，CF 卡的话单自动备份的时间间隔为 1440 分钟。
- 配置 CF 卡中的话单手动保存到话单服务器
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **local-aaa-server**，进入本地 AAA 服务器视图。
  3. 执行命令 **local-bill cfcard backup** [*file-name*]，配置 CF 卡的话单手动保存到话单服务器。
- （可选）清除 CF 卡中所有的话单数据
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **local-aaa-server**，进入本地 AAA 视图。
  3. 执行命令 **local-bill cfcard reset**，清除 CF 卡中所有的话单数据。

     执行此命令后，CF 卡中的话单数据将全部被清除，不可恢复。

----结束

1.5.5 （可选）配置将缓存中的话单保存到话单服务器

因为缓存和 CF 容量都较小，强烈建议将缓存中的话单保存到话单服务器。

背景信息

NE20E-X6 使用 TFTP 协议登录话单服务器，进行话单文件保存操作。因此在话单服务器上必须运行 TFTP 服务器程序，并指定工作目录。

请在路由器上进行以下配置。

操作步骤

- 配置话单服务器
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **local-aaa-server**，进入本地 AAA 服务器视图。
  3. 执行命令 **bill-server** *ip-address* **filename** *file-name*，配置备份话单服务器。

     在 NE20E-X6 上配置话单服务器，需要指定话单服务器的 IP 地址，以及话单的文件名前缀。在 NE20E-X6 中，话单的格式为“文件名前缀-时间-编号.lam”。

     例如文件名前缀为“backupfile”，备份时间为 2005 年 3 月 15 日 15 点 26 分，备份时生成 10 个文件，其中第五个文件的名称为“backupfile-200503151526-5.lam”。
- 配置缓存中话单的告警阈值
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **local-aaa-server**，进入本地 AAA 服务器视图。
  3. 执行命令 **local-bill cache alarm-threshold** *threshold*，配置缓存的话单告警阈值。

     缺省情况下，缓存中的话单告警阈值为 75%。

  缓存中的容量是有限的，所以当缓存中的话单达到一定数量的时候，需要按照用户配置的备份方式保存到其他位置。保存方式分为自动和手动两种。缺省情况下话单是自动保存方式，即经过一定的时间间隔，系统自动将话单保存到相应位置。如果用户希望自己手动保存，可通过配置命令 **local-bill cache backup** 实现手动方式，那么当缓存中的话单超过告警阈值的时候，系统会向网管系统和终端发送告警，提醒用户手动将缓存中的话单保存到话单服务器。
- 配置话单自动备份的时间间隔
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **local-aaa-server**，进入本地 AAA 服务器视图。
  3. 执行命令 **local-bill cache backup-interval** *interval*，配置缓存的话单自动备份的时间间隔。

     缺省情况下，缓存的话单自动备份的时间间隔为 1440 分钟。
- 配置缓存中的话单手动备份到话单服务器
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **local-aaa-server**，进入本地 AAA 服务器视图。
  3. 执行命令 **local-bill cache backup**，手动备份缓存的话单。

----结束

1.5.6 检查配置结果

完成话单本地保存配置后，您可以查看到话单本地保存的配置信息。

操作步骤

- 使用 **display local-bill** { **cache** *start-no count* | **configuration** | **information** }命令，查看话单本地保存的配置信息。

----结束

任务示例

配置完成后，执行命令 **display local-bill** { **cache** *start-no count* | **configuration** | **information** }可以查看话单本地保存的配置信息。例如：

```
<HUAWEI> display local-bill cache 0 2
  Contents of Bill 1:
  ------------------------------------------------------------
  Bill-No   :  1
  Session-Id:  NE20E-X6-1007002000000100ee7075000024
  User-name :  user1@huawei
  Start-Time:  2007/11/24 18:04:42
  Stop-Time :  2007/11/24 18:06:17     Elapse     : 0:01:35
  IP-Addr   :  192.168.7.186           MAC        : 0016-ecb7-a879
  IPv6-Addr :  ::
  Auth-Type :  PPP                     Access-Type: PPPoE
  Port-No   :  1/0/2                   VLAN       : 100
  Status    :  2(offline)              Code    : 6,   Ref: 98
  Acc Data before Tariff Switch,
  1 Priority :
  0  : User-received:  Bytes=0                    , Pkts=0
       User-sent:      Bytes=0                    , Pkts=0
  Acc Data after Tariff Switch,
  1 Priority :
  0  : User-received:  Bytes=0                    , Pkts=0
       User-sent:      Bytes=0                    , Pkts=0
  ------------------------------------------------------------
  Total printed 1 bills from cache.
```

1.6 配置域

所有的本地用户和接入用户都是基于域属性进行管理。

1.6.1 建立配置任务

在进行域配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

1.6.2 创建域

AAA 对用户的管理是通过域来实现的，域是用户管理的最小单位，通常可以是某个 ISP 的名字或 ISP 的某种业务名字。

1.6.3 配置域的 AAA 方案

配置域的 AAA 方案实现对域用户认证、授权和计费方案配置。

1.6.4 配置域的服务器

配置域的服务器包括指定 RADIUS 服务器、hwtacacs 服务器、DNS 服务器、COPS 等各种服务器，可根据业务需求灵活进行配置。

1.6.5 指定域的 IPv4 地址池

指定域的 IPv4 地址池后用户才能从此地址池中获取地址。

1.6.6 （可选）配置域的最大接入用户数

通过在域下配置接入限制数可达到控制用户接入数的目的。

1.6.7 （可选）配置帐号允许的最大 Session 数目

配置域帐号下允许接入的最大用户数即对同一用户名接入的 session 个数进行限制，相同用户名的用户可共享 QoS 资源。

1.6.8 （可选）配置域用户的优先级

配置域用户的优先级可实现不同优先级的用户或业务得到不同的服务。

1.6.9 （可选）指定域所属的分组
指定域所属的分组包括指定域属于 L2TP 组、所属的 VPN 实例等、灵活实现域与各种业务的关联。

1.6.10 （可选）指定域的模板和策略
指定域的模板和策略包括指定域的 802.1X 模板、QoS 模板、组播模板、增值业务策略等，灵活实现域与各种业务的关联。

1.6.11 （可选）配置域用户业务类型
配置域用户业务类型一般是指配置用户接入 Internet 或数字机顶盒接入。

1.6.12 （可选）配置预留带宽
配置预留带宽一般应用于同一家庭中存在 STB 用户和通终端用户，为保证 STB 用户带宽优于 PC 上网带宽时进行配置。

1.6.13 （可选）配置域的附加功能
除基本业务管理功能外，域还包括许多附加功能如：强制 Portal、时间段控制、策略路由、流量统计、IP 地址告警等功能。

1.6.14 （可选）激活域
域处于阻塞状态时，用户不能接入。当某域不希望被继续使用，可以将此域设置为阻塞状态。

1.6.15 检查配置结果
完成域配置后，您可以查看到所有域的配置信息。

1.6.1 建立配置任务

在进行域配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

当需要通过域来对接入用户进行 AAA 等管理时需要配置域。

前置任务

在配置域之前，需要完成以下任务。

- 配置认证方案、计费方案、授权方案
- 如果采用 RADIUS 认证、计费，配置 RADIUS 服务器组
- 如果采用 HWTACACS 认证、计费和授权，配置 HWTACACS 服务器模板
- 配置 IPv4 地址池

数据准备

在配置域之前，请根据网络规划，准备好以下数据。

序号	数据
1	域的名称
2	认证方案、计费方案、授权方案的名称

序号	数据
3	RADIUS 服务器组名称、HWTACACS 服务器模板名称、COPS 服务器组名称、强制 Web 认证服务器的 IP 地址/URL/模式、DNS 服务器的 IP 地址
4	IPv4 地址池名称
5	（可选）最大接入用户数、每秒钟可建立的最大连接数
6	（可选）所属的用户组、GRE 组、L2TP 组、VPN 实例、安全区域
7	（可选）使用的 802.1X 认证模板名称、QoS 模板名称、增值业务策略名称
8	（可选）是否使用强制 Portal 功能、时间段控制功能、闲置切断功能、强制 PPP 认证功能、策略路由功能、IP 地址告警功能、流量统计功能、计费报文抄送功能及相关的参数

说明

域下配置的用户属性，包括用户优先级、用户所属分组、闲置切断参数、时间段 QoS 控制功能、QoS 模板、队列模板、增值业务策略、策略路由功能、组播参数、最大重认证时长等，只对新上线用户有效，对于在线用户，需要重新上线后才能生效。

1.6.2 创建域

AAA 对用户的管理是通过域来实现的，域是用户管理的最小单位，通常可以是某个 ISP 的名字或 ISP 的某种业务名字。

背景信息

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **domain** *domain-name*，创建域，并进入域视图。

NE20E-X6 中一共可创建 1024 个域。系统中存在 default0、default1、default_admin 三个缺省域。

- default0 域是认证前用户的归属域。用户刚接入 NE20E-X6 且尚未进行认证时，NE20E-X6 不能获知用户归属域，因此默认用户属于 default0 域。此域下的用户缺省使用 default0 认证方案、default0 计费方案。
- default1 域是认证时用户的缺省归属域。如果在用户认证时输入的用户名中未包含域名，则 NE20E-X6 默认该用户属于 default1 域。该域下的用户缺省使用 default1 认证方案、default1 计费方案。
- default_admin 域是管理用户的缺省归属域。当操作用户通过 Telnet 或者 SSH 等方式登录 NE20E-X6 时，如果认证时输入的用户名中未包含域名，则 NE20E-X6 默认该操作用户属于 default_admin 域。该域下的用户缺省采用 default 认证方案，default0 计费方案。此域下的用户先本地认证后 RADIUS 认证，也不计费。

----结束

1.6.3 配置域的 AAA 方案

配置域的 AAA 方案实现对域用户认证、授权和计费方案配置。

背景信息

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **domain** *domain-name*，进入域视图。

步骤 4 执行命令 **authentication-scheme** *scheme-name*，指定域的认证方案。

缺省情况下，自定义的域使用 default1 认证方案，default0 域使用 default0 认证方案，default1 域使用 default1 认证方案，default_admin 域使用 default 认证方案。缺省的认证方案使用命令 **display authentication-scheme** 可以查看到详细信息。

缺省情况下，自定义的域使用 default0 认证方案，default_admin 域使用 default0 认证方案。缺省的认证方案使用命令 **display authentication-scheme** 可以查看到详细信息。

步骤 5 执行命令 **accounting-scheme** *scheme-name*，指定域的计费方案。

缺省情况下，自定义的域使用 default1 计费方案，default0 域使用 default0 计费方案，default1 域使用 default1 计费方案，default_admin 域使用 default0 计费方案。

步骤 6 执行命令 **authorization-scheme** *scheme-name*，指定域的授权方案。

缺省情况下，域没有指定授权方案。

----结束

1.6.4 配置域的服务器

配置域的服务器包括指定 RADIUS 服务器、hwtacacs 服务器、DNS 服务器、COPS 等各种服务器，可根据业务需求灵活进行配置。

背景信息

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **domain** *domain-name*，进入域视图。

步骤 4 请根据实际需要，可选择配置域的服务器。

- 执行命令 **hwtacacs-server** *template-name*，指定域 HWTACACS 服务器模板。
- 执行命令 **radius-server group** *group-name*，指定域的 RADIUS 服务器组。

- 执行命令 **cops-server group** *group-name*，指定域的 COPS 服务器组。

  域下只能绑定类型为 SIG 的服务器。
- 执行命令 **web-server** { *ip-address* | **mode** { **get** | **post** } | **redirect-key** { **mscg-ip** *mscg-ip-key* | **user-ip-address** *user-ip-key* | **user-location***user-location-key* } | **url** *url* | **user-first-url-key** { *key-name* | **default-name** } }，指定域的强制 Web 认证服务器。
- 执行命令 **dns** { **primary-ip** |**second-ip** } *ip-address*，指定域的主/备 DNS 服务器

  说明

  如果地址池下也配置了主/备 DNS 服务器，则优先选择地址池下配置的 DNS 服务器

缺省情况下，未指定域的 HWTACACS 服务器模板、RADIUS 服务器组、COPS（Common Open Policy Service）服务器组、强制 Web 认证服务器、主/备 DNS 服务器。

----结束

1.6.5 指定域的 IPv4 地址池

指定域的 IPv4 地址池后用户才能从此地址池中获取地址。

背景信息

域的 IPv4 地址池可以是本地地址池或远端地址池。

一个域可以指定多个 IPv4 地址池（最多 1024 个），一个地址池也可用于多个域。域下配置的 IPv4 地址池的位置可以移动，可移动的范围与域下已配置的地址池数相关，比如域下已配置了 10 个地址池，则域下已配置的地址池的可移动范围为 1 ～ 10。

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **domain** *domain-name*，进入域视图。

步骤 4 执行命令 **ip-pool** *pool-name* [**move-to** *position*]，指定域的 IPv4 地址池。

----结束

1.6.6 （可选）配置域的最大接入用户数

通过在域下配置接入限制数可达到控制用户接入数的目的。

背景信息

为了保证 NE20E-X6 的处理性能，可以对一个域中所能接入的用户总数进行限制，超过限定值后，新接入的用户将被拒绝。

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **domain** *domain-name*，进入域视图。

步骤 4 执行命令 **access-limit** *max-number*，配置域的最大接入用户数。

缺省情况下，域最大接入用户数为 279552。

----结束

1.6.7 （可选）配置帐号允许的最大 Session 数目

配置域帐号下允许接入的最大用户数即对同一用户名接入的 session 个数进行限制，相同用户名的用户可共享 QoS 资源。

背景信息

为了保证 NE20E-X6 的处理性能，可以对一个帐号所能接入的用户总数进行限制，超过限定值后，新接入的用户将被拒绝。

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **domain** *domain-name*，进入域视图。

步骤 4 执行命令 **user-max-session** *max-session-number*，配置一个帐号允许的最大 Session 数目。

缺省情况下，域下用户没有帐号 Session 数目限制。

----结束

1.6.8 （可选）配置域用户的优先级

配置域用户的优先级可实现不同优先级的用户或业务得到不同的服务。

背景信息

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **domain** *domain-name*，进入域视图。

步骤 4 执行命令 **user-priority** { **upstream** | **downstream** } { **priority** | **trust-8021p-inner** | **trust-8021p-outer** | **trust-dscp** | **trust-dscp-inner** | **trust-dscp-outer** | **unchangeable** | **trust-exp-inner** | **trust-exp-outer** }，配置域用户的优先级。

目前域下只支持配置一个用户优先级。

- **priority**：用户优先级，取值范围 0 ～ 7。
- **trust-8021p-inner**：使用用户二层报文的内层 802.1p 值作为用户优先级。
- **trust-8021p-outer**：使用用户二层报文的外层 802.1p 值作为用户优先级。
- **trust-dscp**：使用用户报文的 DSCP 值作为用户优先级。
- **trust-dscp-inner**：使用用户报文的 DSCP 值作为用户优先级。
- **trust-dscp-outer**：使用用户报文的 DSCP 值作为用户优先级。
- **unchangeable**：用户优先级不变。
- **trust-exp-inner**：使用 MPLS 内层标签的 EXP 值作为用户优先级。
- **trust-exp-outer**：使用 MPLS 外层标签的 EXP 值作为用户优先级。

缺省情况下，上下行的用户优先级均为 0。

----结束

1.6.9 （可选）指定域所属的分组

指定域所属的分组包括指定域属于 L2TP 组、所属的 VPN 实例等、灵活实现域与各种业务的关联。

背景信息

可配置域属于以下分组：

- 用户组

  用户组是用于控制用户访问权限的分组，是进行用户 ACL 控制的条件之一。NE20E-X6 支持最多配置 255 个用户组。
- L2TP 组
- VPN 实例

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **domain** *domain-name*，进入域视图。

步骤 4 请根据实际需要，选择执行以下命令：

- 执行命令 **user-group** *group-name*，指定域所属的用户组。

  缺省情况下，未指定域的用户组。
-
- 执行命令 **vpn-instance** *instance-name*，指定域所属的 VPN 实例。

  缺省情况下，未指定域所属的 VPN 实例。

----结束

1.6.10 （可选）指定域的模板和策略

指定域的模板和策略包括指定域的 802.1X 模板、QoS 模板、组播模板、增值业务策略等，灵活实现域与各种业务的关联。

背景信息

可在域下引用如下模板与策略：

- 802.1X 模板

  有关 802.1X 模板，请参见**配置 802.1X 接入业务**。
- QoS 模板

  有关 QoS 模板，请参见《HUAWEI NetEngine20E-X6 高端业务路由器 配置指南-QoS》。

  每个域可同时引用作用于普通用户的 QoS 模板和作用于 LNS 端 L2TP 用户的 QoS 模板，但分别只能引用一个。
- 队列模板

  有关队列模板，请参见《HUAWEI NetEngine20E-X6 高端业务路由器 配置指南-QoS》。
- 组播模板

  有关组播模板，请参见《HUAWEI NetEngine20E-X6 高端业务路由器 配置指南-IP 组播》。
- 增值业务策略

  有关增值业务策略，请参见《HUAWEI NetEngine20E-X6 高端业务路由器 配置指南-增值业务》。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **domain** *domain-name*，进入域视图。

步骤 4 根据需要选择执行以下命令为域指定相应模板:

- 执行命令 **dot1x-template** *dot1x-template-number*，指定域的 802.1X 模板。

  缺省情况下，域使用 802.1X 模板 1。
- 执行命令 **qos-profile** *qos-profile-name* [[**inbound** | **outbound**] **lns-gts**],指定域的 QoS 模板。

  缺省情况下，域下引用的作用于普通用户的 QoS 模板为 default，但不引用作用于 LNS 端 L2TP 用户的 QoS 模板。

  说明

  inbound、**outbound**、**lns-gts** 等参数仅对 LNS 端的 L2TP 用户生效。
- 执行命令 **queue-profile** *queue-profile-name*，指定域的队列模板。
- 执行命令 **value-added-service policy** *policy-name*，指定域的增值业务策略。
- 执行命令 **value-added-service accounting-type** { **cops** *group-name* | **default** | **none** | **radius** *group-name* }，指定域的增值业务计费方式。

----结束

1.6.11 （可选）配置域用户业务类型

配置域用户业务类型一般是指配置用户接入 Internet 或数字机顶盒接入。

背景信息

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **domain** *domain-name*，进入域视图。

步骤 4 执行命令 **service-type** { **hsi** | **stb** }，配置用户业务类型。

缺省情况下，用户属于 HSI 业务。

HSI（High Speed Internet）业务指 PPP、DHCP、802.1x、专线、静态等普通用户接入业务，STB 业务主要指使用数字机顶盒接入的 DHCP 接入业务。

对于普通 DHCP 用户和二层专线下用户，如果域下配置的业务类型是 STB，则用户类型是 STB。

对于三层专线、静态用户、PPP 用户、802.1x 用户，无论域下配置的业务类型是什么，用户类型均强制为 HSI。

HSI 业务用户掉线后，可重新获取 IP 地址上线，但不支持用户信息的远端备份；STB 业务用户断线后不会重新主动上线，支持用户信息远端备份。

----结束

1.6.12 （可选）配置预留带宽

配置预留带宽一般应用于同一家庭中存在 STB 用户和通终端用户，为保证 STB 用户带宽优于 PC 上网带宽时进行配置。

背景信息

需要在非 STB 用户的域下配置此命令，STB 用户域下不能配置此命令。

同一家庭允许的最大 STB 用户数和 HSI 用户数均为 8 个。

说明

- 只有 BAS 接口下配置了 **client-option82** 和 **iptv shaping** 命令，且 STB 用户上线时携带了 option82 信息，STB 用户预留带宽功能才能实现。
- 只有相同接口、相同 VLAN、相同 option82 信息的用户才归为一个家庭。

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **domain** *domain-name*，进入域视图。

步骤 4 执行命令 **bandwidth-tune cir** *cir-value* [**pir** *pir-value*]，配置为 STB 用户预留的带宽。

缺省情况下，域下不为 STB 用户预留带宽。

为保证 STB 用户带宽优于 PC 上网带宽，当 STB 用户上线时，同一家庭中若存在其它的普通终端用户，则按照该配置数值减少普通用户的带宽。即使普通终端用户的带宽小于 STB 用户的预留带宽，STB 用户也能上线。

当普通终端用户上线时，同一家庭中若存在 STB 用户且配置了预留带宽，则普通终端用户以减少后的带宽上线。

----结束

1.6.13 （可选）配置域的附加功能

除基本业务管理功能外，域还包括许多附加功能如：强制 Portal、时间段控制、策略路由、流量统计、IP 地址告警等功能。

背景信息

域的附加功能有：

- 强制 Portal

  强制 Portal，是指用户认证通过后第一次访问外部网络时，由 NE20E-X6 将其访问请求强制重定向到某一服务器（通常为运营商的 Portal 服务器），使用户访问 Internet 的第一站就是运营商站点的一项业务。

- 时间段控制功能

  域的时间段控制功能是指在指定的时间段内，域自动进入阻塞状态（block），域中的用户不能再接入，已接入的用户将被强制下线。当时间过了该时间段规定的范围后，域再自动恢复为激活状态，并允许用户上线。

- 闲置切断功能

  闲置切断（Idle-Cut）是指当用户在某一个时长内业务流量小于某一个阈值时，NE20E-X6 认为该用户处于闲置状态，从而切断用户连接的功能。配置闲置切断功能需要指定时长和流量两个参数。

  域下的闲置切断功能只对用户的基本流量进行控制。组播业务的流量以及没有配置 summary 的增值业务的流量不计算在用户的基本流量中，因而域下的闲置切断功能对组播业务的流量以及没有配置 summary 的增值业务的流量无效。

- 策略路由功能

  策略路由功能是指 NE20E-X6 在转发用户的报文时，依据用户所属的域中所指定的地址来决定转发出口的功能，而不是像通常的路由转发中是根据报文的目的地址来决定其转发出口。

- IP 地址告警功能

  设置了 IP 地址使用告警阈值（百分比）后，当域中的 IP 地址使用超过阈值（百分比）时，NE20E-X6 向网管系统上报告警信息。如果不设置 IP 地址使用告警阈值，则无论域中的 IP 地址使用情况如何，NE20E-X6 均不会告警。

- 流量统计功能

  流量统计功能包括域的总流量统计功能和用户的上下行流量统计功能。

- 计费报文抄送功能

  计费报文抄送是指在计费过程中，将计费信息同步发送给两台 RADIUS 服务器，并分别等待回应的功能。

  计费报文抄送功能主要在需要多处保存原始计费信息的场合使用（如多运营商共同组网）。在这种情况下，计费报文需要同步发送给两台 RADIUS 服务器，在后续的结算中作为原始计费信息。

- 最大重认证时长

  最大重认证时长用于三层预连接用户，当三层预连接用户在设置的最大重认证时长后仍然没有认证通过，NE20E-X6 切断与该用户的连接。

- 用户配额用完策略

  用户配额用完策略指用户配额（如用户流量、session-time）用完后 NE20E-X6 对在线用户采取的策略，包括强制用户下线、保持用户下线、强制重定向用户三种策略。

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **domain** *domain-name*，进入域视图。

步骤 4 执行命令 **portal-server** { *ip-address* | **redirect-limit** *times* | **url** *url-string* }和 **pppoe-url** *url-string*，设置域的强制 Portal 功能。

缺省情况下，域未启用强制 Portal 功能。

强制重定向的 URL 解析后的 IP 地址和 Portal 服务器的 IP 地址应该保持一致。

步骤 5 执行命令 **time-range domain-block** { *range-name* | **enable** }，设置域的时间段控制功能。

一个域可设置四个时间段，时间段之间的作用平等。

缺省情况下，域的时间段控制功能关闭。

步骤 6 执行命令 **idle-cut** *idle-time-length idle-rate* ，设置域的闲置切断功能。

缺省情况下，域的闲置切断时长为 0，即不启用闲置切断功能。

步骤 7 执行命令 **policy-route** *next-hop-ip-address*，设置域的策略路由功能。

缺省情况下，域中未启用策略路由功能。

步骤 8 执行命令 **ip-warning-threshold** *threshold*，设置域的 IP 地址使用告警功能。

缺省情况下，域中未设置 IP 地址使用告警阈值。

步骤 9 执行命令 **flow-bill**，打开域的总流量统计开关。

缺省情况下，域的总流量统计开关关闭，用户的上下行流量统计开关均打开。

步骤 10 执行命令 **flow-statistic** { **down** | **up** } *，打开域的用户流量统计开关。

步骤 11 执行命令 **accounting-copy radius-server** *radius-name*，设置域的计费报文抄送功能。

缺省情况下，域中未设置计费抄送功能。

步骤 12 执行命令 **max-ipuser-reauthtime** *time-value*，设置域的最大重认证时长。

缺省情况下，最大重认证时长为 300 秒。

步骤 13 执行命令 **quota-out** { **offline** | **online** | **redirect url** *url-string* }，设置用户配额用完后对在线用户采取的策略。

缺省情况下，用户配额用完后 NE20E-X6 强制用户下线。

步骤 14 执行命令 **radius-no-response lease-time** *time*，设置 DHCP 用户在 RADIUS 服务器无响应时的租期。

缺省情况下，DHCP 用户在服务器无响应时直接下线。

----结束

1.6.14 （可选）激活域

域处于阻塞状态时，用户不能接入。当某域不希望被继续使用，可以将此域设置为阻塞状态。

背景信息

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **domain** *domain-name*，进入域视图。

步骤 4 执行命令 **block**，设置当前域为阻塞状态。

缺省情况下，域创建后处于激活状态。

----结束

1.6.15 检查配置结果

完成域配置后，您可以查看到所有域的配置信息。

前提条件

已经完成域的所有配置。

操作步骤

步骤 1 执行 **display domain** [*domain-name*]，命令查看域的配置信息。

----结束

任务示例

配置完成后，执行命令 **display domain**，可以查看所有域的简要配置信息，例如：

```
<HUAWEI> display domain
  ------------------------------------------------------------------------------
  Domain name           State        CAR Access-limit   Online  BODNum RptVSMNum
  ------------------------------------------------------------------------------
  default0              Active         0       279552        0       0         0
  default1              Active         0       279552        0       0         0
  default_admin         Active         0       279552        0       0         0
  default               Active         0       279552        0       0         0
  isp1                  Active         0       279552        0       0         0
  ------------------------------------------------------------------------------
  Total 5,5 printed
<HUAWEI> display domain default
 ------------------------------------------------------------------------------
  Domain-name                     : default
  Domain-state                    : Active
  Authentication-scheme-name      : default1
  Accounting-scheme-name          : default1
  Authorization-scheme-name       :
  Primary-DNS-IP-address          : -
  Second-DNS-IP-address           : -
  Web-server-URL-parameter        : No
  Portal-server-URL-parameter     : No
  Primary-NBNS-IP-address         : -
  Second-NBNS-IP-address          : -
  User-group-name                 : -
  Idle-data-attribute (time,flow) : 0, 60
  Install-BOD-Count               : 0
  Report-VSM-User-Count           : 0
  Value-added-service             : COPS
  User-access-limit               : 279552
  Online-number                   : 0
  Web-IP-address                  : -
  Web-URL                         : -
  Portal-server-IP                : -
  Portal-URL                      : -
  Portal-force-times              : 2
  PPPoE-user-URL                  : Disable
  IPUser-ReAuth-Time(second)      : 300
  mscg-name-portal-key            : -
  Portal-user-first-url-key       : -
  Ancp auto qos adapt             : Disable
  RADIUS-server-template          : -
  Two-acct-template               : -
  HWTACACS-server-template        : -
  Bill Flow                       : Disable
  Tunnel-acct-2867                : Disabled
  Qos-profile-name inbound        : -
  Qos-profile-name outbound       : -

  Flow Statistic:
  Flow-Statistic-Up               : Yes
  Flow-Statistic-Down             : Yes
  Source-IP-route                 : Disable
  IP-warning-threshold            : -
  Multicast Forwarding            : Yes
  Multicast Virtual               : No
  Max-multilist num               : 4
  Multicast-profile               : -
  Quota-out                     : Offline
```

1.7 维护 AAA

维护 AAA 包括清除 HWTACACS 统计信息，调试 RADIUS 或者 HWTACACS。

1.7.1 清除 AAA 统计信息

清除 AAA 统计信息包括清除认证、计费、授权服务器和计费停止报文的统计信息。

1.7.1 清除 AAA 统计信息

清除 AAA 统计信息包括清除认证、计费、授权服务器和计费停止报文的统计信息。

背景信息


注意

清除统计信息后，以前的统计信息将无法恢复，务必仔细确认。

操作步骤

- 在确认需要清除统计信息后,请在用户视图下执行 **reset hwtacacs-server statistics** { **all** | **accounting** | **authentication** | **authorization** }命令。
- 在确认需要清除统计信息后,请在用户视图下执行 **reset hwtacacs-server accounting-stop-packet** { **all** | **ip** *ip-address* }命令。

----结束

1.8 配置举例

介绍 AAA 配置的各种示例。配置示例中包括组网需求、配置注意事项和配置思路等。

1.8.1 配置采用 RADIUS 协议对用户进行认证和计费示例
介绍一个采用 RADIUS 协议对用户进行认证和计费示例，结合配置组网图来理解业务的配置过程。配置示例包括组网需求、思路准备、操作步骤和配置文件。

1.8.2 配置采用 HWTACACS 协议对用户进行认证、授权和计费示例
HWTACACS 认证、授权和计费在具体组网中的应用。使 huawei 域的用户使用 HWTACACS 进行认证、授权和计费。

1.8.3 配置在 MPLS VPN 网络中使用 HWTACACS 认证、授权示例
HWTACACS 认证、授权和计费报文穿越 VPN 在具体组网中的应用。能够使公网中的管理员到私网的服务器上进行认证授权和计费。

1.8.1 配置采用 RADIUS 协议对用户进行认证和计费示例

介绍一个采用 RADIUS 协议对用户进行认证和计费示例，结合配置组网图来理解业务的配置过程。配置示例包括组网需求、思路准备、操作步骤和配置文件。

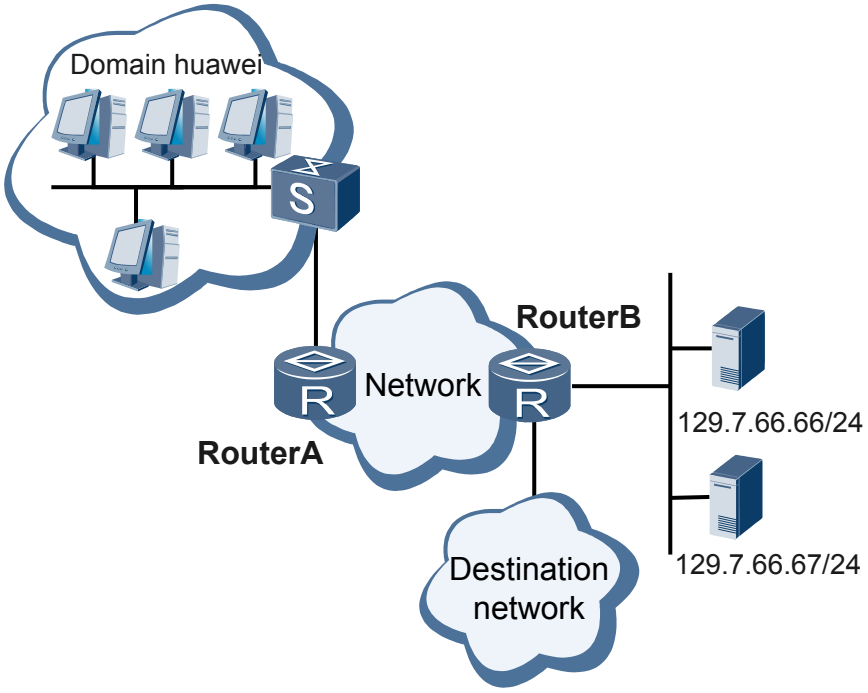
组网需求

如**图 1-1** 所示。用户通过 RouterA 访问网络，用户同处于 huawei 域。RouterB 作为目的网络的网络接入服务器。用户如果要访问目的网络，首先需要穿越 RouterA 和 RouterB 所在的网络，然后通过服务器的远端认证才能通过 RouterB 访问网络。在 RouterB 上的远端认证方式如下：

- 用 RADIUS 服务器对接入用户进行认证、计费。

- RADIUS 服务器 129.7.66.66/24 作为主认证服务器和计费服务器，RADIUS 服务器 129.7.66.67/24 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。

图 1-1 配置采用 RADIUS 协议对用户进行认证和计费组网图



配置思路

在 RouterB 上用如下的思路配置采用 RADIUS 协议对用户进行认证和计费。

1. 配置 RADIUS 服务器组、认证方案、计费方案。
2. 在域下应用 RADIUS 服务器组、认证方案和计费方案。

数据准备

为完成此配置例，需准备以下数据：

- Radius 主（备）认证服务器的 IP 地址。
- Radius 主（备）计费服务器的 IP 地址。

操作步骤

步骤 1 配置 RADIUS 服务器组、认证方案、计费方案

配置 RADIUS 服务器组 shiva。

```
<HUAWEI> system-view
[HUAWEI] radius-server group shiva
```

配置 RADIUS 主认证、计费服务器 IP 地址和端口。

```
[HUAWEI-radius-shiva] radius-server authentication 129.7.66.66 1812
```

```
[HUAWEI-radius-shiva] radius-server accounting 129.7.66.66 1813
```

配置 RADIUS 备认证、计费服务器 IP 地址和端口。

```
[HUAWEI-radius-shiva] radius-server authentication 129.7.66.67 1812
[HUAWEI-radius-shiva] radius-server accounting 129.7.66.67 1813
```

配置 RADIUS 服务器密钥、重传次数。

```
[HUAWEI-radius-shiva] radius-server shared-key it-is-my-secret
[HUAWEI-radius-shiva] radius-server retransmit 2
[HUAWEI-radius-shiva] quit
```

进入 AAA 视图。

```
[HUAWEI] aaa
```

配置认证方案 1，认证方法为 RADIUS。

```
[HUAWEI-aaa] authentication-scheme 1
[HUAWEI-aaa-authen-1] authentication-mode radius
[HUAWEI-aaa-authen-1] quit
```

配置计费方案 1，计费方法为 RADIUS。

```
[HUAWEI-aaa] accounting-scheme 1
[HUAWEI-aaa-accounting-1] accounting-mode radius
[HUAWEI-aaa-accounting-1] quit
```

步骤 2 配置 huawei 域，在域下应用认证方案 1、计费方案 1、shiva 的 RADIUS 服务器组

```
[HUAWEI-aaa] domain huawei
[HUAWEI-aaa-domain-huawei] authentication-scheme 1
[HUAWEI-aaa-domain-huawei] accounting-scheme 1
[HUAWEI-aaa-domain-huawei] radius-server group shiva
```

步骤 3 检查配置结果

采用 RADIUS 协议对用户进行认证和计费一般应用于 BRAS 接入，如果接入配置也正确，用户能够通过认证，正常上线，并且被正常计费。

在路由器上执行 **display radius-server configuration group shiva** 命令后，可以看到该 RADIUS 服务器组的配置与要求一致。

```
<HUAWEI> display radius-server configuration group shiva
  ----------------------------------------------------
  Server-group-name    :  shiva
  Authentication-server:  IP:129.7.66.66 Port:1812 Weight[0] [UP]
                          Vpn: -
  Authentication-server:  IP:129.7.66.67 Port:1812 Weight[0] [UP]
                          Vpn: -
  Authentication-server:  -
  Authentication-server:  -
  Authentication-server:  -
  Authentication-server:  -
  Authentication-server:  -
  Authentication-server:  -
  Accounting-server    :  IP:129.7.66.66 Port:1813 Weight[0] [UP]
                          Vpn: -
  Accounting-server    :  IP:129.7.66.67 Port:1813 Weight[0] [UP]
                          Vpn: -
  Accounting-server    :  -
  Accounting-server    :  -
  Accounting-server    :  -
  Accounting-server    :  -
  Accounting-server    :  -
  Accounting-server    :  -
  Protocol-version     :  radius
  Shared-secret-key    :  it-is-my-secret
  Retransmission       :  2
```

```
  Timeout-interval(s)  :  5
  Acct-Stop-Packet Resend  :  NO
  Acct-Stop-Packet Resend-Times  :  0
  Traffic-unit         :  B
  ClassAsCar           :  NO
  User-name-format     :  Domain-included
  Option82 parse mode  :  -
  Attribute-translation:  NO
  Packet send algorithm:  Master-Backup
  Tunnel password      :  cipher
```

在路由器上执行 **display domain** *domain-name* 命令后，可以查看域的配置。

```
<HUAWEI> display domain huawei
  ------------------------------------------------------------------------------
  Domain-name                     : huawei
  Domain-state                    : Active
  Authentication-scheme-name      : 1
  Accounting-scheme-name          : 1
  Authorization-scheme-name       :
  Primary-DNS-IP-address          : -
  Second-DNS-IP-address           : -
  Primary-NBNS-IP-address         : -
  Second-NBNS-IP-address          : -
  User-group-name                 : -
  Idle-data-attribute (time,flow) : 0, 60
  Install-BOD-Count               : 0
  Report-VSM-User-Count           : 0
  Value-added-service             : COPS
  User-access-limit               : 279552
  Online-number                   : 0
  Web-IP-address                  : -
  Web-URL                         : -
  Portal-server-IP                : -
  Portal-URL                      : -
  Portal-force-times              : 2
  PPPoE-user-URL                  : Disable
  IPUser-ReAuth-Time(second)      : 300
  Ancp auto qos adapt             : Disable
  Service-type                    : STB
  RADIUS-server-template          : shiva
  Two-acct-template               : -
  HWTACACS-server-template        : -
  Bill Flow                       : Disable
  Tunnel-acct-2867                : Disabled

  Flow Statistic:
  Flow-Statistic-Up               : Yes
  Flow-Statistic-Down             : Yes
  Source-IP-route                 : Disable
  IP-warning-threshold            : -
  Multicast Forwarding            : Yes
  Multicast Virtual               : No
  Max-multilist num               : 4
  Multicast-profile               : -
  Quota-out                     : Offline
  ------------------------------------------------------------------------------
```

----结束

配置文件

```
#
sysname HUAWEI
#
aaa
  authentication-scheme 1
  authentication-mode radius
 #
```

```
 authorization-scheme default
 #
  accounting-scheme 1
  accounting-mode radius
 #
domain huawei
 authentication-scheme 1
 accounting-scheme 1
  radius-server group shiva
#
radius-server group shiva
 radius-server authentication 129.7.66.66 1812 weight 0
 radius-server authentication 129.7.66.67 1812 weight 0
 radius-server accounting 129.7.66.66 1813 weight 0
 radius-server accounting 129.7.66.67 1813 weight 0
 radius-server shared-key it-is-my-secret
 radius-server retransmit 2
#
return
```

1.8.2 配置采用 HWTACACS 协议对用户进行认证、授权和计费示例

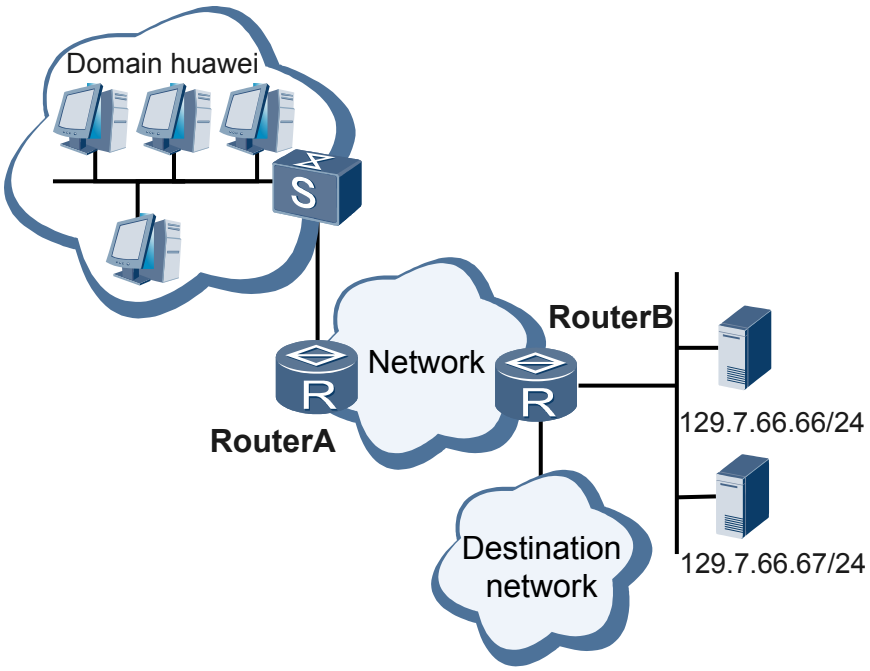
HWTACACS 认证、授权和计费在具体组网中的应用。使 huawei 域的用户使用 HWTACACS 进行认证、授权和计费。

组网需求

如图 1-2 所示。用户通过 RouterA 访问网络，用户同处于 huawei 域。RouterB 作为目的网络的网络接入服务器。用户如果要访问目的网络，首先需要穿越 RouterA 和 RouterB 所在的网络，然后通过服务器的远端认证才能通过 RouterB 访问网络。在 RouterB 上的认证方式如下：

- 对接入用户先用本地进行认证，如果认证没有响应，再使用 HWTACACS 服务器进行认证。
- 接入的用户进行用户等级提升时，要求先使用 HWTACACS 对其进行认证，如果 HWTACACS 认证没有响应，再使用本地认证。
- 对接入用户采用 HWTACACS 授权。
- 对所有用户都需要计费。
- HWTACACS 服务器 129.7.66.66/24 为主服务器，认证端口号为 49，授权端口号为 49，计费端口号为 49；HWTACACS 服务器 129.7.66.67/24 为备服务器，认证端口号缺省为 49，授权端口号缺省为 49，计费端口号缺省为 49。

图 1-2 配置对用户使用本地和 HWTACACS 认证、HWTACACS 授权和进行实时计费组网图



配置思路

采用如下的思路配置对用户使用本地和 HWTACACS 认证、HWTACACS 授权和进行实时计费。

1. 配置 HWTACACS 服务器模板。
2. 配置认证方案、授权方案、计费方案。
3. 在域上引用 HWTACACS 服务器模板、认证方案、授权方案、计费方案。

数据 准备

为完成此配置例，需准备以下数据：

- HWTACACS 主（备）认证服务器的 IP 地址。
- HWTACACS 主（备）授权服务器的 IP 地址。
- HWTACACS 主（备）计费服务器的 IP 地址。

操作步骤

步骤 1 配置 HWTACACS 服务器模板

配置 HWTACACS 服务器模板 ht。

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template ht
```

配置 HWTACACS 主认证、授权、计费服务器 IP 地址和端口。

```
[HUAWEI-hwtacacs-ht] hwtacacs-server authentication 129.7.66.66 49
```

```
[HUAWEI-hwtacacs-ht] hwtacacs-server authorization 129.7.66.66 49
[HUAWEI-hwtacacs-ht] hwtacacs-server accounting 129.7.66.66 49
```

配置 HWTACACS 备认证、授权、计费服务器 IP 地址和端口。

```
[HUAWEI-hwtacacs-ht] hwtacacs-server authentication 129.7.66.67 49 secondary
[HUAWEI-hwtacacs-ht] hwtacacs-server authorization 129.7.66.67 49 secondary
[HUAWEI-hwtacacs-ht] hwtacacs-server accounting 129.7.66.67 49 secondary
```

配置 HWTACACS 服务器密钥。

```
[HUAWEI-hwtacacs-ht] hwtacacs-server shared-key it-is-my-secret
[HUAWEI-hwtacacs-ht] quit
```

步骤 2 配置认证方案、授权方案、计费方案

进入 AAA 视图。

```
[HUAWEI] aaa
```

配置认证方案 l-h，认证方法为先进行本地认证，后进行 HWTACACS 认证。用户级别提升方为先进行 HWTACACS 认证，后进行本地认证。

```
[HUAWEI-aaa] authentication-scheme l-h
[HUAWEI-aaa-authen-l-h] authentication-mode local hwtacacs
[HUAWEI-aaa-authen-l-h] authentication-super hwtacacs super
[HUAWEI-aaa-authen-l-h] quit
```

配置授权方案 hwtacacs，授权方法为 HWTACACS。

```
[HUAWEI-aaa] authorization-scheme hwtacacs
[HUAWEI-aaa-author-hwtacacs] authorization-mode hwtacacs
[HUAWEI-aaa-author-hwtacacs] quit
```

配置计费方案 hwtacacs，计费方法为 HWTACACS。

```
[HUAWEI-aaa] accounting-scheme hwtacacs
[HUAWEI-aaa-accounting-hwtacacs] accounting-mode hwtacacs
```

步骤 3 配置 huawei 域，在域下采用 l-h 认证方案、HWTACACS 授权方案、HWTACACS 计费方案、ht 的 HWTACACS 模板

```
[HUAWEI-aaa] domain huawei
[HUAWEI-aaa-domain-huawei] authentication-scheme l-h
[HUAWEI-aaa-domain-huawei] authorization-scheme hwtacacs
[HUAWEI-aaa-domain-huawei] accounting-scheme hwtacacs
[HUAWEI-aaa-domain-huawei] hwtacacs-server ht
[HUAWEI-aaa-domain-huawei] quit
[HUAWEI-aaa] quit
```

步骤 4 检查配置结果

在路由器上执行 **display hwtacacs-server template** 命令后，可以观察到该 hwtacacs 服务器模板的配置与要求一致。

```
<HUAWEI> display hwtacacs-server template ht
  ------------------------------------------------------------------------------
  HWTACACS-server template name   : ht
  Primary-authentication-server   : 129.7.66.66:49
  Primary-authorization-server    : 129.7.66.66:49
  Primary-accounting-server       : 129.7.66.66:49
  Secondary-authentication-server : 129.7.66.67:49
  Secondary-authorization-server  : 129.7.66.67:49
  Secondary-accounting-server     : 129.7.66.67:49
  Current-authentication-server   : 129.7.66.66:49
  Current-authorization-server    : 129.7.66.66:49
  Current-accounting-server       : 129.7.66.66:49
  Source-IP-address               : 0.0.0.0
  Shared-key                      : it-is-my-secret
```

```
  Quiet-interval(min)             : 5
  Response-timeout-Interval(sec)  : 5
  Domain-included                 : Yes
  Traffic-unit                    : B
-----------------------------------------------------------------------------
```

同时在路由器上执行 **display domain** 命令后，可以观察到该域的配置与要求一致

```
<HUAWEI>display domain huawei
```

----结束

配置文件

```
#
Sysname HUAWEI
#
hwtacacs-server template ht
 hwtacacs-server authentication 129.7.66.66 49
 hwtacacs-server authentication 129.7.66.67 49 secondary
 hwtacacs-server authorization 129.7.66.66 49
 hwtacacs-server authorization 129.7.66.67 49 secondary
 hwtacacs-server accounting 129.7.66.66 49
 hwtacacs-server accounting 129.7.66.67 49 secondary
 hwtacacs-server shared-key it-is-my-secret
#
aaa
 authentication-scheme default
 authentication-scheme l-h
  authentication-mode  local  hwtacacs
#
 authorization-scheme default
 authorization-scheme hwtacacs
  authorization-mode  hwtacacs
 #
 accounting-scheme default
 accounting-scheme hwtacacs
  accounting-mode hwtacacs
 #
 domain default
 domain huawei
  authentication-scheme  l-h
  authorization-scheme hwtacacs
  accounting-scheme hwtacacs
  hwtacacs-server ht
 #
return
```

1.8.3 配置在 MPLS VPN 网络中使用 HWTACACS 认证、授权示例

HWTACACS 认证、授权和计费报文穿越 VPN 在具体组网中的应用。能够使公网中的管理员到私网的服务器上进行认证授权和计费。

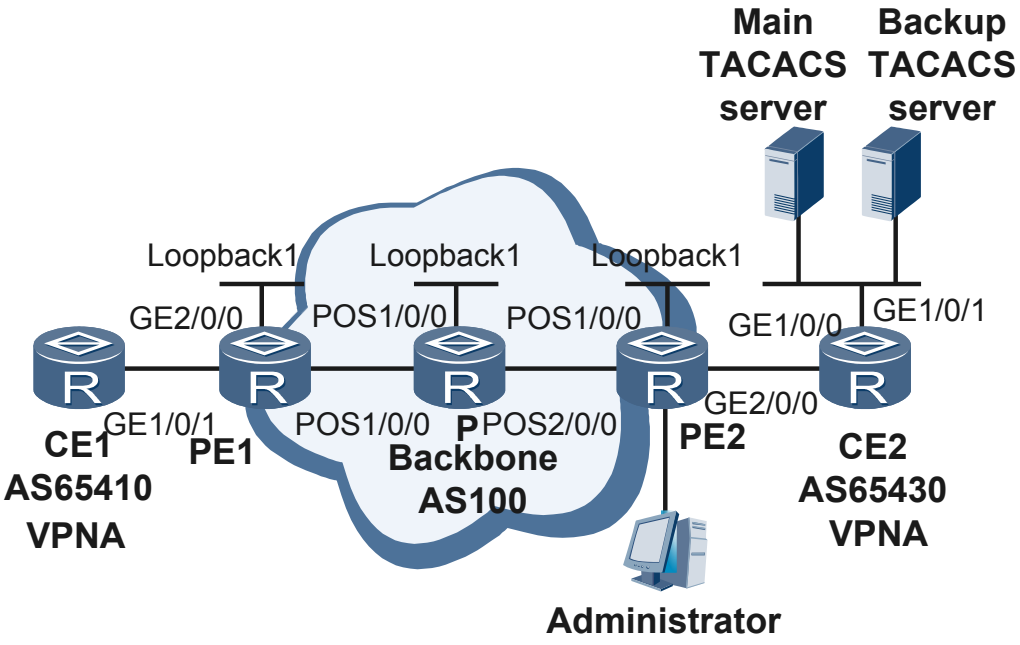
组网需求

如图 1-3 所示。CE1、CE2 同属于 VPN-A，VPN-A 使用的 VPN-target 属性为 111:1。公网中管理员通过 Console 口直接登录 PE，或者通过公网中的 PC、其他路由器、Telnet 客户端等登录 PE2，经过 HWTACACS 认证/授权后对 PE2 进行管理，PE2 的一些系统事件、管理员动作等信息也会发往 TACACS 服务器记录。TACACS 服务器位于私网中，需要 HWTACACS 报文经过 VPN 实例发送。

- 在 PE2 上对管理员用户使用 TACACS 服务器进行 HWTACACS 认证。
- 在 PE2 上对管理员用户采用 HWTACACS 授权。

- TACACS 服务器 160.1.1.100/24 为主服务器，认证端口号为 49，授权端口号为 49，计费端口号为 49；TACACS 服务器 160.1.1.101/24 为备服务器，认证端口号缺省为 49，授权端口号缺省为 49，计费端口号缺省为 49。

图 1-3 配置对管理员用户使用 HWTACACS 认证和授权组网图



设备名称	接口名称	IP 地址
CE1	GE1/0/1	10.1.1.2/24
PE1	Loopback1	1.1.1.9/32
	GE2/0/0	10.1.1.1/24
	POS1/0/0	100.1.1.1/24
P	Loopback1	3.3.3.9/32
	POS1/0/0	100.1.1.2/24
	POS2/0/0	200.1.1.1/24
PE2	Loopback1	2.2.2.9/32
	GE2/0/0	10.2.1.2/24
	POS1/0/0	200.1.1.2/24
CE2	GE1/0/0	10.2.1.1/24
	GE1/0/1	160.1.1.1/24
Main TACACS server		160.1.1.100/24
Backup TACACS server		160.1.1.101/24

配置思路

采用如下的思路配置对管理员用户进行 HWTACACS 认证和授权。

1. 配置基本的 BGP/MPLS IP VPN，使网络互通。
2. 配置 HWTACACS 服务器模板。
3. 配置认证方案、授权方案。
4. 在域上引用 HWTACACS 服务器模板、认证方案、授权方案。

数据准备

为完成此配置例，需准备以下数据：

- HWTACACS 主（备）认证服务器的 IP 地址。
- HWTACACS 主（备）授权服务器的 IP 地址。
- HWTACACS 主（备）计费服务器的 IP 地址。

操作步骤

步骤 1 配置 BGP/MPLS IP VPN。

在网络上配置 IGP 协议，实现骨干网 PE 和 P 的互通，发布 CE 下节点的 IP 地址。

配置 PE1。

```
<HUAWEI> system-view
[HUAWEI] sysname PE1
[PE1] interface loopback 1
[PE1-LoopBack1] ip address 1.1.1.9 32
[PE1-LoopBack1] quit
[PE1] interface pos1/0/0
[PE1-Pos1/0/0] ip address 100.1.1.1 24
[PE1-Pos1/0/0] quit
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

配置 P。

```
<HUAWEI> system-view
[HUAWEI] sysname P
[P] interface loopback 1
[P-LoopBack1] ip address 3.3.3.9 32
[P-LoopBack1] quit
[P] interface pos 1/0/0
[P-Pos1/0/0] ip address 100.1.1.2 24
[P-Pos1/0/0] quit
[P] interface pos 2/0/0
[P-Pos2/0/0] ip address 200.1.1.1 24
[P-Pos2/0/0] quit
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 200.1.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

配置 PE2。

```
<HUAWEI> system-view
[HUAWEI] sysname PE2
[PE2] interface loopback 1
[PE2-LoopBack1] ip address 2.2.2.9 32
[PE2-LoopBack1] quit
[PE2] interface pos 1/0/0
[PE2-Pos1/0/0] ip address 200.1.1.2 24
[PE2-Pos1/0/0] quit
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 200.1.1.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

配置 CE1。

```
<HUAWEI> system-view
[HUAWEI] sysname CE1
[CE1] interface gigabitethernet 1/0/1
[CE1-GigabitEthernet1/0/1] ip address 10.1.1.2 24
[CE1-GigabitEthernet1/0/1] quit
```

配置 CE2。

```
<HUAWEI> system-view
[HUAWEI] sysname CE2
[CE2] interface gigabitethernet 1/0/0
[CE2-GigabitEthernet1/0/0] ip address 10.2.1.1 24
[CE2-GigabitEthernet1/0/0] quit
[CE2] interface gigabitethernet 1/0/1
[CE2-GigabitEthernet1/0/1] ip address 160.1.1.1 24
[CE2-GigabitEthernet1/0/1] quit
[CE2] ospf
[CE2-ospf-1] area 0
[CE2-ospf-1-area-0.0.0.0] network 160.1.1.0 0.0.0.255
[CE2-ospf-1-area-0.0.0.0] quit
[CE2-ospf-1] quit
```

配置完成后，PE1、P、PE2 之间应能建立 OSPF 邻居关系，执行 **display ospf peer** 命令可以看到邻居状态为 Full。执行 **display ip routing-table** 命令可以看到 PE 之间学习到对方的 Loopback1 路由。

以 PE1 的显示为例：

```
[PE1] display ip routing-table
Route Flags: R - relied, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9        Routes : 9
Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface
      1.1.1.9/32  Direct 0    0           D  127.0.0.1       InLoopBack0
      2.2.2.9/32  OSPF   10   3125        D  100.1.1.2       Pos1/0/0
      3.3.3.9/32  OSPF   10   1563        D  100.1.1.2       Pos1/0/0
    127.0.0.0/8   Direct 0    0           D  127.0.0.1       InLoopBack0
    127.0.0.1/32  Direct 0    0           D  127.0.0.1       InLoopBack0
    100.1.1.0/24  Direct 0    0           D  100.1.1.1       Pos1/0/0
    100.1.1.1/32  Direct 0    0           D  127.0.0.1       InLoopBack0
    100.1.1.2/32  Direct 0    0           D  100.1.1.2       Pos1/0/0
    200.1.1.0/24  OSPF   10   3124        D  100.1.1.2       Pos1/0/0
[PE1] display ospf peer
          OSPF Process 1 with Router ID 1.1.1.9
                  Neighbors
 Area 0.0.0.0 interface 100.1.1.1(Pos1/0/0)'s neighbors
 Router ID: 3.3.3.9        Address: 100.1.1.2        GR State: Normal
   State: Full  Mode:Nbr is  Master  Priority: 1
   DR: None   BDR: None   MTU: 1500
   Dead timer due in 38  sec
   Neighbor is up for 00:02:44
```

```
  Authentication Sequence: [ 0 ]
```

在 MPLS 骨干网上配置 MPLS 基本能力和 MPLS LDP，建立 LDP LSP。

配置 PE1。

```
[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls
[PE1-mpls] lsp-trigger all
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] interface pos 1/0/0
[PE1-Pos3/0/0] mpls
[PE1-Pos3/0/0] mpls ldp
[PE1-Pos3/0/0] quit
```

配置 P。

```
[P] mpls lsr-id 3.3.3.9
[P] mpls
[P-mpls] lsp-trigger all
[P-mpls] quit
[P] mpls ldp
[P-mpls-ldp] quit
[P] interface pos 1/0/0
[P-Pos1/0/0] mpls
[P-Pos1/0/0] mpls ldp
[P-Pos1/0/0] quit
[P] interface pos 2/0/0
[P-Pos2/0/0] mpls
[P-Pos2/0/0] mpls ldp
[P-Pos2/0/0] quit
```

配置 PE2。

```
[PE2] mpls lsr-id 2.2.2.9
[PE2] mpls
[PE2-mpls] lsp-trigger all
[PE2-mpls] quit
[PE2] mpls ldp
[PE2-mpls-ldp] quit
[PE2] interface pos 1/0/0
[PE2-Pos3/0/0] mpls
[PE2-Pos3/0/0] mpls ldp
[PE2-Pos3/0/0] quit
```

上述配置完成后，PE1 与 P、P 与 PE2 之间应能建立 LDP 会话，执行 **display mpls ldp session** 命令可以看到显示结果中 Status 项为“Operational”。执行 **display mpls ldp lsp** 命令，可以看到 LDP LSP 的建立情况。

以 PE1 的显示为例：

```
[PE1] display mpls ldp session
              LDP Session(s) in Public Network
 ------------------------------------------------------------------------------
 Peer-ID            Status      LAM  SsnRole  SsnAge      KA-Sent/Rcv
 ------------------------------------------------------------------------------
 3.3.3.9:0          Operational DU   Passive  000:00:01   7/7
 ------------------------------------------------------------------------------
 TOTAL: 1 session(s) Found.
 LAM : Label Advertisement Mode      SsnAge Unit : DDD:HH:MM
[PE1] display mpls ldp lsp
                          LDP LSP Information
 -------------------------------------------------------------------
 SN  DestAddress/Mask   In/OutLabel  Next-Hop     In/Out-Interface
 -------------------------------------------------------------------
 1   1.1.1.9/32         3/NULL       127.0.0.1     Pos1/0/0/InLoop0
 2   2.2.2.9/32         NULL/1027    100.1.1.2     -------/Pos1/0/0
```

```
3    3.3.3.9/32          NULL/3        100.1.1.2      -------/Pos1/0/0
------------------------------------------------------------------------------
TOTAL: 3 Normal LSP(s) Found.
TOTAL: 0 Liberal LSP(s) Found.
A '*' before an LSP means the LSP is not established
A '*' before a Label means the USCB or DSCB is stale
```

在 PE 设备上配置 VPN 实例，将 CE 接入 PE。

配置 PE1。

```
[PE1] ip vpn-instance vpna
[PE1-vpn-instance-vpna] route-distinguisher 100:1
[PE1-vpn-instance-vpna] vpn-target 111:1 both
[PE1-vpn-instance-vpna] quit
[PE1] interface gigabitethernet 2/0/0
[PE1-GigabitEthernet2/0/0] ip binding vpn-instance vpna
[PE1-GigabitEthernet2/0/0] ip address 10.1.1.1 24
[PE1-GigabitEthernet2/0/0] quit
```

配置 PE2。

```
[PE2] ip vpn-instance vpna
[PE2-vpn-instance-vpna] route-distinguisher 200:1
[PE2-vpn-instance-vpna] vpn-target 111:1 both
[PE2-vpn-instance-vpna] quit
[PE2] interface gigabitethernet 2/0/0
[PE2-GigabitEthernet2/0/0] ip binding vpn-instance vpna
[PE2-GigabitEthernet2/0/0] ip address 10.2.1.2 24
[PE2-GigabitEthernet2/0/0] quit
```

配置完成后，在 PE 设备上执行 **display ip vpn-instance verbose** 命令可以看到 VPN 实例的配置情况。各 PE 能 ping 通自己接入的 CE。

说明

当 PE 上有多个绑定了同一个 VPN 的接口，则使用 **ping -vpn-instance** 命令 ping 对端 PE 接入的 CE 时，要指定源 IP 地址，即要指定 **ping -vpn-instance** *vpn-instance-name* **-a** *source-ip-address dest-ip-address* 命令中的参数**-a** *source-ip-address*，否则可能 ping 不通。

以 PE1 和 CE1 为例：

```
[PE1] display ip vpn-instance verbose
  Total VPN-Instances configured : 1
  VPN-Instance Name and ID : vpna, 1
  Create date : 2008/09/27 15:24:40
  Up time : 0 days, 00 hours, 05 minutes and 19 seconds
  Route Distinguisher : 100:1
  Export VPN Targets :  111:1
  Import VPN Targets :  111:1
  Label policy: label per route
  The diffserv-mode Information is : uniform
  The ttl-mode Information is : pipe
  Interfaces : GigabitEthernet1/0/0
[PE1] ping -vpn-instance vpna 10.1.1.2
  PING 10.1.1.2: 56  data bytes, press CTRL_C to break
    Reply from 10.1.1.2: bytes=56 Sequence=1 ttl=255 time=56 ms
    Reply from 10.1.1.2: bytes=56 Sequence=2 ttl=255 time=4 ms
    Reply from 10.1.1.2: bytes=56 Sequence=3 ttl=255 time=4 ms
    Reply from 10.1.1.2: bytes=56 Sequence=4 ttl=255 time=52 ms
    Reply from 10.1.1.2: bytes=56 Sequence=5 ttl=255 time=3 ms
  --- 10.1.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/23/56 ms
```

在 PE 与 CE 之间建立 EBGP 对等体关系，引入 VPN 路由。

配置 CE1。

```
[CE1] bgp 65410
[CE1-bgp] peer 10.1.1.1 as-number 100
[CE1-bgp] import-route direct
```

说明

另外 1 个 CE 设备（CE2）配置与 CE1 设备配置类似，配置过程省略。

配置 PE1。

```
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpna
[PE1-bgp-vpna] peer 10.1.1.2 as-number 65410
[PE1-bgp-vpna] import-route direct
[PE1-bgp-vpna] quit
```

说明

PE2 的配置与 PE1 类似，配置过程省略。

配置完成后，在 PE 设备上执行 **display bgp vpnv4 vpn-instance peer** 命令，可以看到 PE 与 CE 之间的 BGP 对等体关系已建立，并达到 Established 状态。

以 PE1 与 CE1 的对等体关系为例：

```
[PE1] display bgp vpnv4 vpn-instance vpna peer
 BGP local router ID : 1.1.1.9
 Local AS number : 100
 Total number of peers : 1           Peers in established state : 1
  Peer            V    AS  MsgRcvd  MsgSent    OutQ  Up/Down    State        PrefRcv
  10.1.1.2        4   65410  11     9          0     00:06:37   Established  1
```

在 PE 之间建立 MP-IBGP 对等体关系。

配置 PE1。

```
[PE1] bgp 100
[PE1-bgp] peer 2.2.2.9 as-number 100
[PE1-bgp] peer 2.2.2.9 connect-interface loopback 1
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpnv4] peer 2.2.2.9 enable
[PE1-bgp-af-vpnv4] quit
[PE1-bgp] quit
```

配置 PE2。

```
[PE2] bgp 100
[PE2-bgp] peer 1.1.1.9 as-number 100
[PE2-bgp] peer 1.1.1.9 connect-interface loopback 1
[PE2-bgp] ipv4-family vpnv4
[PE2-bgp-af-vpnv4] peer 1.1.1.9 enable
[PE2-bgp-af-vpnv4] quit
```

配置完成后，在 PE 设备上执行 **display bgp peer** 或 **display bgp vpnv4 all peer** 命令，可以看到 PE 之间的 BGP 对等体关系已建立，并达到 Established 状态。

```
[PE1] display bgp peer
 BGP local router ID : 1.1.1.9
 Local AS number : 100
 Total number of peers : 1          Peers in established state : 1
  Peer            V    AS  MsgRcvd  MsgSent    OutQ  Up/Down    State        PrefRcv
  2.2.2.9         4   100   2       6          0     00:00:12   Established   0
[PE1] display bgp vpnv4 all peer
BGP local router ID : 1.1.1.9
 Local AS number : 100
 Total number of peers : 2                 Peers in established state : 2
  Peer            V    AS  MsgRcvd  MsgSent    OutQ  Up/Down    State        PrefRcv
  2.2.2.9         4   100   12      18         0     00:09:38   Established   0
```

```
Peer of vpn instance:
vpn instance vpna :
10.1.1.2        4   65410  25     25         0     00:17:57   Established   1
```

步骤 2 在 PE2 上配置 HWTACACS 服务器模板

配置 HWTACACS 服务器模板 ht。

```
<PE2> system-view
[PE2] hwtacacs-server template ht
```

配置 HWTACACS 主认证、授权、计费服务器 IP 地址和端口，并绑定服务器所在的 VPN 实例。

```
[PE2-hwtacacs-ht] hwtacacs-server authentication 160.1.1.100 49 vpn-instance vpna
[PE2-hwtacacs-ht] hwtacacs-server authorization 160.1.1.100 49 vpn-instance vpna
```

配置 HWTACACS 备认证、授权、计费服务器 IP 地址和端口，并绑定服务器所在的 VPN 实例。

```
[PE2-hwtacacs-ht] hwtacacs-server authentication 160.1.1.101 49 vpn-instance vpna secondary
[PE2-hwtacacs-ht] hwtacacs-server authorization 160.1.1.101 49 vpn-instance vpna secondary
```

配置 TACACS 服务器密钥。

```
[PE2-hwtacacs-ht] hwtacacs-server shared-key it-is-my-secret
[PE2-hwtacacs-ht] quit
```

步骤 3 配置认证方案、授权方案、计费方案

进入 AAA 视图。

```
[PE2] aaa
```

配置认证方案 l-h，认证方法 HWTACACS 认证。

```
[PE2-aaa] authentication-scheme l-h
[PE2-aaa-authen-l-h] authentication-mode hwtacacs
[PE2-aaa-authen-l-h] quit
```

配置授权方案 hwtacacs，授权方法为 HWTACACS。

```
[PE2-aaa] authorization-scheme hwtacacs
[PE2-aaa-author-hwtacacs] authorization-mode hwtacacs
[PE2-aaa-author-hwtacacs] quit
```

步骤 4 配置 huawei 域，在域下采用 l-h 认证方案、HWTACACS 授权方案、HWTACACS 计费方案、ht 的 HWTACACS 模板

```
[PE2-aaa] domain huawei
[PE2-aaa-domain-huawei] authentication-scheme l-h
[PE2-aaa-domain-huawei] authorization-scheme hwtacacs
[PE2-aaa-domain-huawei] hwtacacs-server ht
[PE2-aaa-domain-huawei] quit
[PE2-aaa] quit
```

步骤 5 检查配置结果

在路由器上执行 **display hwtacacs-server template** 命令后，可以观察到该 hwtacacs 服务器模板的配置与要求一致。

```
<PE2> display hwtacacs-server template ht
-------------------------------------------------------------------------
HWTACACS-server template name   : ht
Primary-authentication-server   : 160.1.1.100:49:vpna
Primary-authorization-server    : 160.1.1.100:49:vpna
Primary-accounting-server       : 0.0.0.0:0:-
Secondary-authentication-server : 160.1.1.101:49:vpna
Secondary-authorization-server  : 160.1.1.101:49:vpna
```

```
  Secondary-accounting-server     : 0.0.0.0:0:-
  Current-authentication-server   : 160.1.1.100:49:vpna
  Current-authorization-server    : 160.1.1.100:49:vpna
  Current-accounting-server       : 0.0.0.0:0:-
  Source-IP-address               : 0.0.0.0
  Shared-key                      : it-is-my-secret
  Quiet-interval(min)             : 5
  Response-timeout-Interval(sec)  : 5
  Domain-included                 : Yes
  Traffic-unit                    : B
-----------------------------------------------------------------------------
```

同时在路由器上执行 **display domain** 命令后，可以观察到该域的配置与要求一致。

```
<CE1> display domain huawei
  -----------------------------------------------------------------------
  Domain-name                     : huawei
  Domain-state                    : Active
  Authentication-scheme-name      : l-h
  Accounting-scheme-name          : default
  Authorization-scheme-name       : hwtacacs
  User-CAR                        : -
  Web-IP-address                  : -
  Next-hop                        : -
  Primary-DNS-IP-address          : -
  Second-DNS-IP-address           : -
  Primary-NBNS-IP-address         : -
  Second-NBNS-IP-address          : -
  Acl-number                      : -
  Idle-data-attribute (time,flow) : 0, 60
  User-priority                   : -
  Online-number                   : 0
  RADIUS-server-template          : -
  HWTACACS-server-template        : ht
  -----------------------------------------------------------------------
```

----结束

配置文件

- PE1 的配置文件

```
#
 sysname PE1
#
ip vpn-instance vpna
 route-distinguisher 100:1
 vpn-target 111:1 export-extcommunity
 vpn-target 111:1 import-extcommunity
#
 mpls lsr-id 1.1.1.9
 mpls
  lsp-trigger all
#
mpls ldp
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip binding vpn-instance vpna
 ip address 10.1.1.1 255.255.255.0
#
interface Pos1/0/0
 link-protocol ppp
undo shutdown
ip address 100.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
```

```
 ip address 1.1.1.9 255.255.255.255
#
bgp 100
 peer 2.2.2.9 as-number 100
 peer 2.2.2.9 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 2.2.2.9 enable
#
 ipv4-family vpnv4
  policy vpn-target
  peer 2.2.2.9 enable
 #
 ipv4-family vpn-instance vpna
  import-route direct
  peer 10.1.1.2 as-number 65410
#
ospf 1
 area 0.0.0.0
  network 100.1.1.0 0.0.0.255
  network 1.1.1.9 0.0.0.0
#
return
```

- P 的配置文件

```
#
 sysname P
#
 mpls lsr-id 3.3.3.9
 mpls
  lsp-trigger all
#
mpls ldp
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 100.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 200.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 3.3.3.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 100.1.1.0 0.0.0.255
  network 200.1.1.0 0.0.0.255
  network 3.3.3.9 0.0.0.0
#
return
```

- PE2 的配置文件

```
#
 sysname PE2
#
ip vpn-instance vpna
 route-distinguisher 200:1
 vpn-target 111:1 export-extcommunity
 vpn-target 111:1 import-extcommunity
#
hwtacacs-server template ht
```

```
 hwtacacs-server authentication 160.1.1.100 49 vpn-instance vpna
 hwtacacs-server authentication 160.1.1.101 49 vpn-instance vpna secondary
 hwtacacs-server authorization 160.1.1.100 vpn-instance vpna
 hwtacacs-server authorization 160.1.1.101 vpn-instance vpna secondary
 hwtacacs-server shared-key it-is-my-secret
#
 mpls lsr-id 2.2.2.9
 mpls
  lsp-trigger all
#
mpls ldp
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip binding vpn-instance vpna
 ip address 10.2.1.2 255.255.255.0
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 200.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 2.2.2.9 255.255.255.255
#
bgp 100
 peer 1.1.1.9 as-number 100
 peer 1.1.1.9 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 1.1.1.9 enable
 #
 ipv4-family vpnv4
  policy vpn-target
  peer 1.1.1.9 enable
 #
 ipv4-family vpn-instance vpna
  peer 10.2.1.1 as-number 65430
  import-route direct
#
aaa
 authentication-scheme default
 authentication-scheme l-h
  authentication-mode hwtacacs
#
 authorization-scheme default
 authorization-scheme hwtacacs
  authorization-mode  hwtacacs
#
  accounting-scheme default
 #
 domain default
 domain huawei
  authentication-scheme  l-h
  authorization-scheme hwtacacs
  hwtacacs-server ht
 #
ospf 1
 area 0.0.0.0
  network 200.1.1.0 0.0.0.255
  network 2.2.2.9 0.0.0.0
 #
return
```

- CE1 的配置文件

```
#
 sysname CE1
```

```
#
interface GigabitEthernet1/0/1
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
#
bgp 65410
 peer 10.1.1.1 as-number 100
 #
 ipv4-family unicast
  undo synchronization
  import-route direct
  peer 10.1.1.1 enable
#
return
```

- CE2 的配置文件

```
#
 sysname CE2
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.2.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 undo shutdown
 ip address 160.1.1.1 255.255.255.0
#
bgp 65430
 peer 10.2.1.2 as-number 100
 #
 ipv4-family unicast
  undo synchronization
  import-route direct
  peer 10.2.1.2 enable
 #
ospf 1
 area 0.0.0.0
  network 160.1.1.0 0.0.0.255
#
return
```

2 DHCPv4 配置

关于本章

在 IPv4 网络中，用户动态获取 IP 地址需要配置 DHCPv4。

2.1 DHCPv4 概述
DHCPv4 是一种终端自动配置协议，客户端可获取一个动态合法的 IPv4 地址。

2.2 NE20E-X6 支持的 DHCPv4 特性
NE20E-X6 支持 DHCP Relay、DHCP Server 为用户分配地址。

2.3 配置 IPv4 地址池
配置地址池后，用户才可以从地址池中获得 IPv4 地址。

2.4 配置 DHCPv4 服务器组
只有使用远端地址池为 BAS 侧用户分配地址时才需要配置 DHCPv4 服务器组。

2.5 配置 DHCPv4 中继
当客户端与 DHCPv4 服务器不在同一网段时，通过在中继设备实现提供 IPv4 地址的服务。

2.6 调整 DHCPv4 服务参数
通过调整 DHCPv4 服务参数达到提高 DHCPv4 服务安全性的目的。

2.7 维护
维护 DHCPv4 包括清除 DHCPv4 统计信息、DHCPv4 运行状况和调试 DHCPv4。

2.8 配置举例
介绍 DHCPv4 配置的各种示例。配置示例中包括组网需求、配置注意事项和配置思路等。

2.1 DHCPv4 概述

DHCPv4 是一种终端自动配置协议，客户端可获取一个动态合法的 IPv4 地址。

随着网络规模的扩大和网络复杂度的提高，网络配置越来越复杂，经常出现计算机位置变化（如便携机或无线终端）和计算机数量超过可分配的 IP 地址的情况。动态主机配置协议 DHCPv4（Dynamic Host Configuration Protocol）就是为满足这些需求而发展起来的。

2.2 NE20E-X6 支持的 DHCPv4 特性

NE20E-X6 支持 DHCP Relay、DHCP Server 为用户分配地址。

NE20E-X6 支持基于全局地址池的 DHCPv4 应用，提供 DHCPv4 Relay、DHCPv4 Server 等功能，并可以提供保证 DHCPv4 服务安全的特性。用户可以通过内置的 DHCPv4 Server 功能获取 IP 地址，也可以通过 DHCPv4 Relay 功能从外部的 DHCPv4 Server 获得 IP 地址。

NE20E-X6 还支持 DHCPv4 扩展功能，包括 DHCPv4 Option 和 DHCPv4 广播。

2.3 配置 IPv4 地址池

配置地址池后，用户才可以从地址池中获得 IPv4 地址。

2.3.1 建立配置任务
在进行 IPv4 地址池配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

2.3.2 配置地址池
配置地址池类型、名称、网关、地址段是地址池的必备元素。

2.3.3 （可选）配置用于静态地址绑定的地址池
配置用于静态地址绑定的地址池是指配置包含有特殊 IP 地址的地址池，一般用于需要固定 IP 地址的服务器或有特殊需要的用户。

2.3.4 （可选）配置 DHCPv4 客户端的 DNS 服务
配置 DHCPv4 客户端的 DNS 服务使用户自动获得 DNS 服务，用户就可以使用便于记忆的、有意义的域名，而不必去记忆复杂的 IP 地址。

2.3.5 （可选）配置 DHCPv4 客户端的 NetBIOS 服务
配置 DHCPv4 客户端的 NetBIOS 服务使用户自动获得 NetBIOS 服务，用户就可以使用便于记忆的的主机名，而不必去记忆复杂的 IP 地址。

2.3.6 （可选）配置 DHCPv4 客户端的 SIP 服务
配置 DHCPv4 客户端的 SIP 服务，主要应用于多媒体通信如多媒体会议、Internet 电话、远程教育以及远程医疗等。

2.3.7 （可选）配置 DHCPv4 自定义选项
通过配置 DHCPv4 自定义选项可以给客户端提供更多的控制信息和参数。

2.3.8 （可选）设置地址池保护
设置地址池保护是在一些特殊情况下对地址池锁定、禁用 IP 地址或地址段、设置冲突或回收 IP 地址的处理。

完成 IPv4 地址池配置后，您可以查看到所有 IP 地址池和指定地址池的配置信息。

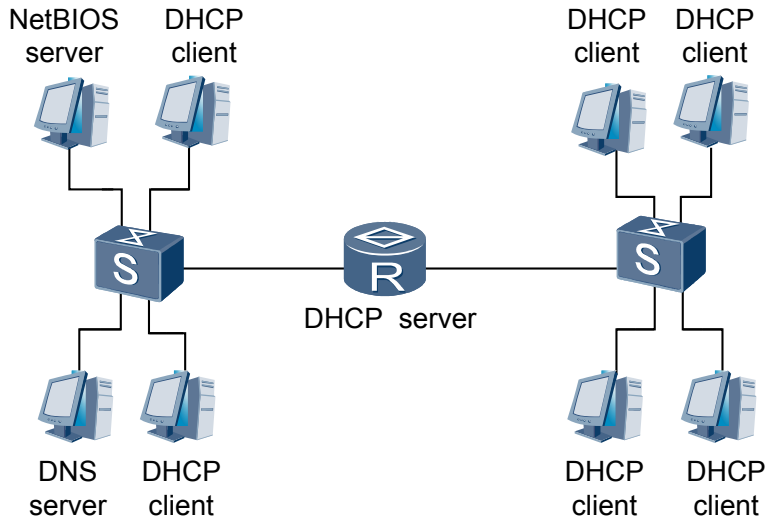
2.3.1 建立配置任务

在进行 IPv4 地址池配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

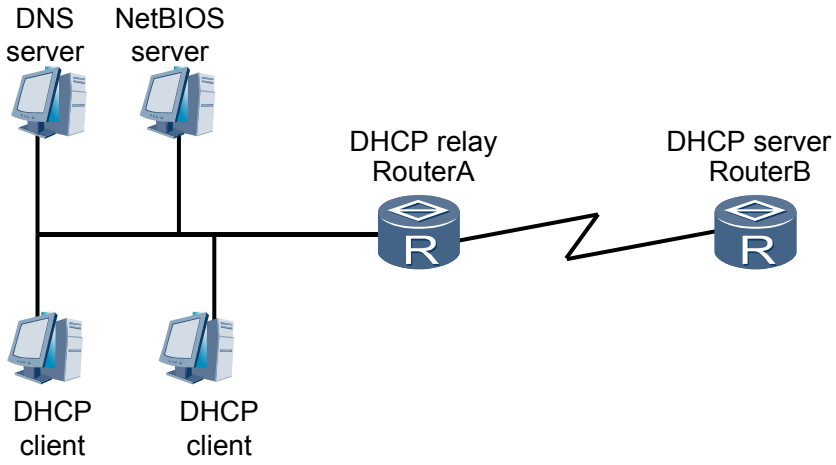
在一个较大的网络里，如果网络中的计算机不能与路由设备通过以太网接口直接相连，而要穿过其他的设备，在这种情况下，为了让计算机从路由设备动态获取 IPv4 地址，通常需要配置网络侧 DHCPv4 服务器，如图 2-1 所示。

图 2-1 以太网用户 IP 地址分配－无中继设备组网图



网络侧的 DHCPv4 服务器通常与 DHCPv4 Relay Agent 协同工作，如图 2-2 所示。

图 2-2 以太网用户 IP 地址分配－包含中继设备组网图



当需要为接入用户分配 IP 地址时，需要配置 BAS 侧地址池。如果由 NE20E-X6 为用户分配 IP 地址，需要配置本地地址池，如图 2-3 所示；如果由 DHCPv4/BOOTP 服务器为用户分配 IP 地址，需要在 NE20E-X6 上配置远端地址池，如图 2-4 所示。

图 2-3 使用本地地址池为接入用户分配地址组网图

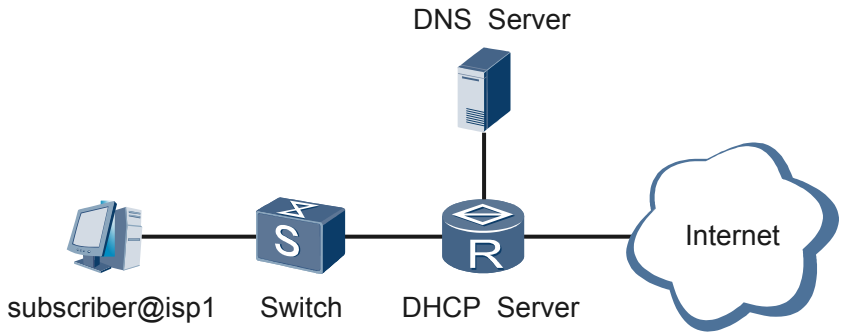
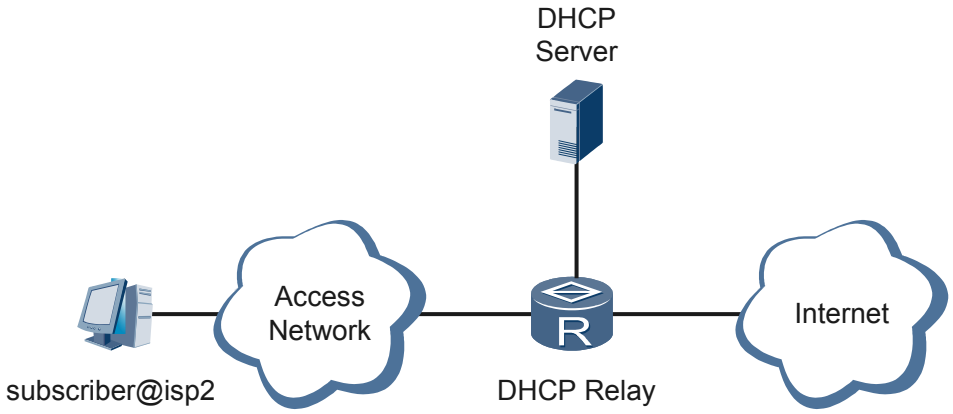


图 2-4 使用远端地址池为接入用户分配地址组网图



前置任务

在配置 IP 地址池之前，需要完成以下任务。

- 如果使用远端地址池，请**配置 DHCPv4 服务器组**

说明

如果两个远端地址池指向同一 DHCP Server，但 DHCP Server 配置与远端地址池配置不一致的情况，可能导致第二个地址池不能使用，应保证配置一致或指向不同 DHCP Server。

数据准备

在配置 IP 地址池之前，请准备好以下数据。

序号	数据
1	地址池名称以及网关地址
2	地址段个数以及每个地址段的开始地址和结束地址
3	（可选）地址池的租期、IP 地址的续租时间、VPN 实例
4	（可选）需要静态绑定的 IP 地址和 MAC 地址表项
5	（可选）地址池的 DNS 服务器地址、DNS 后缀、NetBIOS 服务器地址、SIP 服务器地址
6	（可选）DHCPv4 自定义选项
7	（可选）地址池中禁用的 IP 地址或地址段、地址池中标识为冲突的 IP 地址或地址段、需要回收的 IP 地址

2.3.2 配置地址池

配置地址池类型、名称、网关、地址段是地址池的必备元素。

背景信息

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip pool** *pool-name* [**bas** { **local** | **remote** | **rui-slave** } | **server**]，创建地址池并进入地址池视图。

系统最多可配置 4096 个地址池，包括接入侧地址池和网络侧地址池。所有类型的地址池不能重名。

步骤 3 执行命令 **gateway** *ip-address mask*，配置地址池的网关地址。

地址池网关地址和子网掩码用于检查地址段的地址是否和网关在一个子网内。因此必须先配置地址池的网关地址和掩码，再配置地址段。

步骤 4 执行命令 **section** *section-num start-ip-address* [*end-ip-address*]，配置地址段。

一个地址池中可配置 256 个地址段，每个地址段最多可配置 65536 个地址，每个地址段中的地址不可重叠。

步骤 5 （可选）执行命令 **lease** *days* [*hours* [*minutes*]]，配置地址池租期。

缺省情况下，地址池中的 IP 地址的租期为 3 天，如果租期设置为 0，表示租期无限。

步骤 6 （可选）执行命令 **rebinding-time** *days* [*hours* [*minutes*]]，配置 IP 地址的重绑定时间。

缺省情况下，IP 地址的重绑定时间是地址池租期的 87.5%。

步骤 7 （可选）执行命令 **renewal-time** *days* [*hours* [*minutes*]]，配置 IP 地址的更新时间。

缺省情况下，IP 地址的更新时间是地址池租期的 50%。

步骤 8 （可选）执行命令 **recycle** *start-ip-address* [*end-ip-address*]，配置 IP 地址的状态为空闲。

当某 IP 地址的状态为占用，但用户不在线时，可用该命令手动回收地址。

步骤 9 （可选）执行命令 **reserved ip-address** { **lease** | **mac** }，配置用户 IP 地址的预留类型。

缺省情况下，不进行地址预留。当用户下线时就将用户的 IP 地址回收。

如果用户第一次上线时给它分配的租期是 4 天，用户下线后，在这 4 天内再次上线，可以再次使用第一次分配的 IP 地址，即按租期预留。

如果用户第一次上线会记录用户的 MAC 地址和分配给用户的 IP 地址，用户下线后再次上线后，可以再次使用第一次申请的 IP 地址分配给用户，即按 MAC 地址预留。

步骤 10 （可选）执行命令 **vpn-instance** *instance-name*，配置地址池所属的 VPN 实例。

----结束

2.3.3 （可选）配置用于静态地址绑定的地址池

配置用于静态地址绑定的地址池是指配置包含有特殊 IP 地址的地址池，一般用于需要固定 IP 地址的服务器或有特殊需要的用户。

背景信息

根据客户端的实际需要，可以选择采用静态地址绑定方式或动态地址分配方式。

动态地址分配需要指定用于分配的地址范围，而静态地址绑定则可以看做是只包含一个地址的特殊的 DHCPv4 地址池。

请在作为 DHCPv4 服务器的设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip pool** *pool-name* **bas local**，创建地址池并进入地址池视图。

步骤 3 执行命令 **excluded-ip-address** *start-ip-address* [*end-ip-address*]，禁用指定 IP 地址，以便这些地址不会被分配给用户。

步骤 4 执行命令 **static-bind ip-address** *ip-address* **mac-address** *mac-address*，配置静态绑定的 IP-MAC 地址对。

----结束

后续处理

某些客户端可能需要固定的 IP 地址，即将客户端的 MAC 地址与某个 IP 地址绑定。当此 MAC 地址的客户端申请 DHCPv4 地址时，服务器根据客户端 MAC 地址寻找到对应的固定 IP 地址分配给客户端。

2.3.4 （可选）配置 DHCPv4 客户端的 DNS 服务

配置 DHCPv4 客户端的 DNS 服务使用户自动获得 DNS 服务，用户就可以使用便于记忆的、有意义的域名，而不必去记忆复杂的 IP 地址。

背景信息

当作为 DHCPv4 服务器的设备需要为 DHCPv4 客户端提供 DNS 服务时，请在设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip pool** *pool-name* [**bas** { **local** | **remote** } | **server**]，创建地址池并进入地址池视图。

步骤 3 执行命令 **dns-suffix** *suffix-name*，配置地址池的 DNS 后缀名。

说明

该命令仅适用于本地和 Server 地址池的配置。

步骤 4 执行命令 **dns-server** *ip-address* &<1-8>，配置地址池分配给客户端的 DNS 服务器的 IP 地址。

----结束

后续处理

在 DHCPv4 服务器上，可以为每个地址池分别指定客户端使用的 DNS 后缀名。

主机通过 DNS 后缀名访问 Internet 时，需要将 DNS 后缀名解析为 IP 地址，这是通过域名系统 DNS（Domain Name System）实现的。因此，为了使 DHCPv4 客户端成功接入 Internet，DHCPv4 服务器应在为客户端分配 IP 地址的同时指定 DNS 服务器地址。

为了提高网络的可靠性，可配置多个 DNS 服务器。

2.3.5 （可选）配置 DHCPv4 客户端的 NetBIOS 服务

配置 DHCPv4 客户端的 NetBIOS 服务使用户自动获得 NetBIOS 服务，用户就可以使用便于记忆的的主机名，而不必去记忆复杂的 IP 地址。

背景信息

当作为 DHCPv4 服务器的设备需要为 DHCPv4 客户端提供 NetBIOS 服务时，请在设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip pool** *pool-name* [**bas** { **local** | **remote** } | **server**]，创建地址池并进入地址池视图。

步骤 3 执行命令 **netbios-name-server** *ip-address* &<1-8>，配置地址池客户端的 NetBIOS 服务器地址。

步骤 4 执行命令 **netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** }，配置 DHCPv4 客户端的 NetBIOS 节点类型。

缺省情况下，不指定客户端的节点类型。

----结束

后续处理

对于使用 Microsoft 操作系统的客户端，由 WINS（Windows Internet Naming Service）服务器为通过 NetBIOS 协议通信的主机提供主机名到 IP 地址的解析。所以，大部分 Windows 网络客户端需要进行 WINS 的设置。

DHCPv4 客户端在广域网上使用 NetBIOS 协议通信时，需要在主机名和 IP 地址之间建立映射关系。根据获取映射关系的方式不同，NetBIOS 节点分为四种。

- b 类节点（b-node）：“b”代表广播（broadcast），即，此类节点采用广播的方式获取映射关系。
- h 类节点（h-node）：“h”代表混合（hybrid），是具备“端对端”通信机制的 b 类节点。
- m 类节点（m-node）：“m”代表混合（mixed），是具有部分广播特性的 p 类节点。
- p 类节点（p-node）：“p”代表端到端（peer-to-peer），即，此类节点采用与 NetBIOS 服务器通信的方式获取映射关系。

2.3.6 （可选）配置 DHCPv4 客户端的 SIP 服务

配置 DHCPv4 客户端的 SIP 服务，主要应用于多媒体通信如多媒体会议、Internet 电话、远程教育以及远程医疗等。

背景信息

当作为 DHCPv4 服务器的设备需要为 DHCPv4 客户端提供 SIP 服务时，请在设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip pool** *pool-name* [**bas local** | **server**]，创建地址池并进入地址池视图。

步骤 3 执行命令 **sip-server** { { **ip-address** *ip-address* } &<1~2> | { **list** *server-name* } &<1~2> }，配置 SIP 服务器的 IP 地址或名称。

缺省情况下，没有指定 SIP 服务器。

----结束

2.3.7 （可选）配置 DHCPv4 自定义选项

通过配置 DHCPv4 自定义选项可以给客户端提供更多的控制信息和参数。

背景信息

请在作为 DHCPv4 服务器的设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip pool** *pool-name* [**bas local** | **server**]，创建地址池并进入地址池视图。

步骤 3 执行命令 **option** *code* { **ip** *ip-address* | **string** *string* }，配置 DHCPv4 选项。

----结束

后续处理

DHCPv4 报文中的 Option 字段可以用来存放某些普通协议中没有定义的控制信息和参数。如果用户在 DHCPv4 服务器端配置了 Option，DHCPv4 客户端在申请 IP 地址的时候，会通过服务器端回应的 DHCPv4 报文获得 Option 字段中的配置信息。

用户可以通过手工定义的方式将选项添加到 DHCPv4 服务器的属性列表中。例如：

- 如果想配置 Log Server 地址为 10.110.204.1，可以使用命令：**option 7 ip 10.110.204.1**；
- 如果想配置 DHCPv4 服务器选项代码 129 代表字符串“huawei”，可以使用命令：**option 129 string huawei**。

说明

常用的 Option（如 DNS、租期）的选项 Option 的数值是一定的，包括 3，6，15，44，46，50-54，57-59。如果再配置该选项 Option 的数值，会提示不允许配置。

option 命令用于将指定选项内容通过服务器端回应的 DHCPv4 报文进行携带。

使用该命令前，需要明确选项功能。如 Option 77 用于 DHCPv4 客户端，用于识别用户或应用所属的类型，根据 Option 字段中所携带的用户类型（User Class），DHCPv4 服务器选择适当的地址池为客户端分配 IP 地址以及相关配置参数。Option77 一般在客户端由用户进行配置，而不必要用 Option 命令在服务器端配置。

2.3.8 （可选）设置地址池保护

设置地址池保护是在一些特殊情况下对地址池锁定、禁用 IP 地址或地址段、设置冲突或回收 IP 地址的处理。

背景信息

地址池保护方法包括：

- 锁定地址池

  地址池可以通过命令锁定，锁定后该地址池中的 IP 地址不再分配。

  本方法经常用于地址池由于有用户在线使用无法删除的情况，此时先锁定地址池，不再继续分配，待所有的用户下线后，地址池中的 IP 地址全部得到释放，再删除地址池。
- IP 地址禁用

  在复杂的网络规划中，可能需要对其中的部分 IP 地址进行禁用。
- IP 地址回收

  当地址池中的 IP 地址出现异常时，即没有用户在使用，但 IP 地址处于被使用的状态，该 IP 地址无法被继续使用。此时可以通过 IP 地址强行回收命令进行回收。

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip pool** *pool-name* [**bas** { **local** | **remote** } | **server**]，创建地址池并进入地址池视图。

步骤 3 执行命令 **lock**，锁定地址池。

或执行命令 **excluded-ip-address** *start-ip-address* [*end-ip-address*]，禁用 IP 地址或地址段。

说明

在配置静态 IP 地址用户时需用到此命令。

或执行命令 **recycle** *start-ip-address* [*end-ip-address*]，回收 IP 地址。

----结束

2.3.9 检查配置结果

完成 IPv4 地址池配置后，您可以查看到所有 IP 地址池和指定地址池的配置信息。

前提条件

已经完成 IPv4 地址池的所有配置。

操作步骤

- 使用 **display ip pool** [**name** *pool-name* [*section-num* [*start-ip-address* [*end-ip-address*]] | **all** | **used**]] [**vpn-instance** *instance-name*]命令，查看 IP 地址池的配置信息。

----结束

任务示例

执行 **display ip pool** 命令，可以看到系统配置的所有地址池。

```
<HUAWEI> display ip pool
  ------------------------------------------------------------------------
  Pool-Name      : test
  Pool-No        : 1
  Position       : Local           Status           : Unlocked
  Gateway        : 89.0.0.1        Mask             : 255.0.0.0
  Vpn instance   : --
  ------------------------------------------------------------------------
  Pool-Name      : test1
  Pool-No        : 6
  Position       : Local           Status           : Unlocked
  Gateway        : 40.50.60.1      Mask             : 255.255.255.0
  Vpn instance   : --
  IP address pool Statistic
    Local       :2          Remote    :0          Relay    :0
  IP address Statistic
    Total       :51695
    Used        :0          Free      :51695
Conflicted  :0          Disable   :0
```

执行命令 **display ip pool** [**name** *pool-name* [*section-num* [*start-ip-address* [*end-ip-address*]] | **all** | **used**]] [**vpn-instance** *instance-name*]命令，可以看到指定地址池的详细信息。例如：

```
<HUAWEI> display ip pool name huawei
Pool-Name      : huawei
  Pool-No        : 0
  Lease          : 3 Days 0 Hours 0 Minutes
  NetBois Type   : N-Node
  DNS-Suffix     : -

  DNS1          :10.10.10.1
  Position       : Local           Status           : Unlocked
  Gateway        : 10.10.10.2      Mask             : 255.255.255.0
  Vpn instance   : --
  Profile-Name   : -               Server-Name      : -
  Codes: CFLCT(conflicted)
  ------------------------------------------------------------------------------
---------
  ID           start             end total  used  idle CFLCT disable reserved st
atic-bind
  ------------------------------------------------------------------------------
---------
   0       10.10.10.3     10.10.10.100     98      0     98      0        0         0
         0
  ------------------------------------------------------------------------------
---------
```

2.4 配置 DHCPv4 服务器组

只有使用远端地址池为 BAS 侧用户分配地址时才需要配置 DHCPv4 服务器组。

2.4.1 建立配置任务
在进行 DHCPv4 服务器组配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

2.4.2 配置 DHCPv4 服务器组
DHCPv4 服务器可以是负荷分担或主备方式进行工作。

2.4.3 配置 IP 地址池与 DHCPv4 服务器组关联
只有使用远端地址池才需要关联 IP 地址池和 DHCPv4 服务器组。

2.4.4 检查配置结果
完成 DHCPv4 服务器组配置后，您可以查看到所有 DHCPv4 服务器组的配置信息。

2.4.1 建立配置任务

在进行 DHCPv4 服务器组配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

NE20E-X6 可以作为 DHCPv4 服务器为用户分配 IP 地址，也可以使用外置 DHCPv4 服务器为用户分配地址。

当使用外置 DHCPv4 服务器为用户分配 IP 地址时，如**图 2-4** 所示，需要在 NE20E-X6 上配置该 DHCPv4 服务器的 IP 地址等参数，便于 NE20E-X6 和 DHCPv4 服务器进行通讯。在 NE20E-X6 中，使用 DHCPv4 服务器组对 DHCPv4 服务器进行管理。

说明

只有使用远端地址池为 BAS 侧用户分配地址时才需要配置 DHCPv4 服务器组。

前置任务

无

数据准备

在配置 DHCPv4 服务器之前，请根据网络规划，准备好以下数据。

序号	数据
1	DHCPv4 服务器组名称
2	主备 DHCPv4 服务器的 IP 地址、所属的 VPN 实例、权重值
3	（可选）是否使用 DHCPv4 Release 代理功能

2.4.2 配置 DHCPv4 服务器组

DHCPv4 服务器可以是负荷分担或主备方式进行工作。

背景信息

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dhcp-server group** *group-name*，创建 DHCPv4 服务器组并进入 DHCPv4 服务器组视图。

步骤 3 执行命令 **dhcp-server** *ip-address* [**vpn-instance** *vpn-instance*] [**weight** *weight-value*]，配置 DHCPv4 服务器。

一个 DHCPv4 服务器组可以配置一主一备两台 DHCPv4 服务器。

步骤 4 （可选）执行命令 **dhcp-server algorithm** { **loading-share** | **master-backup** }，配置 DHCPv4 服务器的选择算法。

当 DHCPv4 服务器组中的服务器为两个时，配置选择服务器的算法才能生效，包括负荷分担和主备备份两种。

- 负荷分担：NE20E-X6 根据各服务器的权重，按比例进行负荷分配。
- 主备备份：配置的第一个服务器为主用服务器，另外一个为备用服务器。

缺省情况下，DHCPv4 服务器的选择算法为主备备份。

步骤 5 （可选）执行命令 **release-agent**，配置 DHCPv4 Release 代理功能。

缺省情况下，DHCPv4 服务器组启用 DHCPv4 Release 代理功能。

DHCPv4 Release 代理是指用户下线时，NE20E-X6 会代替用户向 DHCPv4 服务器发送 DHCPv4 Release 报文。

----结束

2.4.3 配置 IP 地址池与 DHCPv4 服务器组关联

只有使用远端地址池才需要关联 IP 地址池和 DHCPv4 服务器组。

背景信息

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip pool** *pool-name* **bas remote**，进入远端地址池视图。

步骤 3 执行命令 **dhcp-server group** *group-name*，配置与 DHCPv4 服务器组关联。

----结束

2.4.4 检查配置结果

完成 DHCPv4 服务器组配置后，您可以查看到所有 DHCPv4 服务器组的配置信息。

前提条件

已经完成 DHCPv4 服务器组的所有配置。

操作步骤

- 使用 **display dhcp-server group** [*group-name*]命令查看 DHCPv4 服务器组的配置信息。

----结束

任务示例

执行 **display dhcp-server group** 命令，可以看到所有 DHCPv4 服务器组的信息。

```
<HUAWEI> display dhcp-server group
  Group-Name          : remote
  Release-Agent       : Support
  Primary-Server      : -
    Vpn instance      : --
  Weight              : 0
  Status              : -
  Secondary-Server    : -
    Vpn instance      : --
  Weight              : 0
  Status              : -
  Algorithm           : master-backup
  Source              : --
  Giaddr              : --
  Group-Name          : g1
  Release-Agent       : Support
  Primary-Server      : -
    Vpn instance      : --
```

```
Weight              : 0
Status              : -
Secondary-Server    : -
  Vpn instance      : --
Weight              : 0
Status              : -
Algorithm           : master-backup
Source              : --
Giaddr              : --
2 DHCP server group(s) in total
```

2.5 配置 DHCPv4 中继

当客户端与 DHCPv4 服务器不在同一网段时，通过在中继设备实现提供 IPv4 地址的服务。

2.5.1 建立配置任务
在进行 DHCPv4 中继配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

2.5.2 配置中继功能
配置中继功能包括使能中继功能、DHCPv4 服务器地址以及实现 DHCP 服务器根据不同的客户端分配不同网段的 IP 地址。

2.5.3 检查配置结果
完成 DHCPv4 中继配置后，您可以查看到 DHCPv4 中继的配置信息和统计信息。

2.5.1 建立配置任务

在进行 DHCPv4 中继配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如果本地网络没有配置 DHCPv4 服务器，可以在网段内的其他设备上启动 DHCPv4 中继功能，从客户端发送的 DHCPv4 请求可通过中继代理传到 DHCPv4 服务器，如**图 2-2** 所示。

说明

DHCPv4 服务器和客户端之间的中继代理不能超过 4 次，否则 DHCPv4 报文将被丢弃。

前置任务

在配置 DHCPv4 中继代理之前，需完成以下任务：

- 配置 DHCPv4 服务器
- 配置中继代理的接口
- 配置中继代理到 DHCPv4 服务器的路由

数据准备

在配置 DHCPv4 中继之前，需准备以下数据。

序号	数据
1	DHCPv4 服务器的 IP 地址
2	需要启动 DHCPv4 中继代理功能的接口编号
3	需要启动 DHCPv4 中继功能的 VLAN 编号
4	（可选）需要释放的 IP 地址和对应的 MAC 地址
5	（可选）DHCP option 的编号
6	中继代理地址

2.5.2 配置中继功能

配置中继功能包括使能中继功能、DHCPv4 服务器地址以及实现 DHCP 服务器根据不同的客户端分配不同网段的 IP 地址。

背景信息

当客户端与 DHCPv4 服务器不在同一网段时，通过在中继设备上配置其接口所代理的 DHCPv4 服务器地址，可以将客户端的请求报文转发到此 DHCPv4 服务器，实现提供 IP 地址的服务。

可以分别在接口视图下、系统视图下配置中继功能。

说明

由于 DHCPv4 客户端在 DHCPv4 配置的某些阶段发送的报文为广播报文，因此启动中继功能的接口应当支持广播方式。接口的 IP 地址应和地址池中的 IP 地址属于同一网段。每个接口最多可以配置 20 个该接口所代理的 DHCPv4 服务器地址。

请在中继设备上进行以下配置。

操作步骤

- 在接口视图下配置 DHCPv4 中继功能
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **ip address** *ip-address* { *mask* | *mask-length* }，配置接口的主 IP 地址。
  4. 执行命令 **dhcp select relay**，使能接口的 DHCPv4 中继功能。
  5. 执行命令 **ip relay address** *ip-address* [**dhcp-option** { **60** [*option-text*] | *code* }]，配置该接口所代理的 DHCPv4 服务器地址。
  6. 执行命令 **ip relay giaddr** *ip-address* [**dhcp-option** { **60** [*option-text*] | *code* }]，配置 DHCP option 与中继代理地址的关联，从而实现 DHCP 服务器根据不同的客户端分配不同网段的 IP 地址。
- 在系统视图下配置 DHCPv4 中继功能
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dhcp select relay** { **all** | **interface** *interface-type interface-number.sub-interface-number1* [**to** *interface-type interface-number.sub-interface-number2*] |

interface *interface-type interface-number* | **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> }，系统视图下使能接口的 DHCPv4 中继功能。

3. 执行命令 **ip relay address** *ip-address* { **all** | **interface** *interface-type interface-number.sub-interface-number1* [**to** *interface-type interface-number.sub-interface-number2*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* }，配置多个接口所代理的 DHCPv4 服务器地址。

----结束

2.5.3 检查配置结果

完成 DHCPv4 中继配置后，您可以查看到 DHCPv4 中继的配置信息和统计信息。

前提条件

已经完成 DHCPv4 中继的所有配置。

操作步骤

- 使用 **display dhcp relay statistics** 命令查看中继代理的相关统计信息。
- 使用 **display dhcp relay address** { **all** | **interface** *interface-type interface-number* | **vlan** *vlan-id* }命令用来查看启动中继代理功能接口的 DHCPv4 配置情况。

----结束

任务示例

执行命令 **display dhcp relay address all**，可以查看所有接口的 DHCPv4 配置情况。

```
<HUAWEI> display dhcp relay address all
**  GigabitEthernet0/0/0 DHCP Relay Address  **
 Dhcp Option          Relay Agent IP       Server IP
 *                    -                    10.10.1.2

    **  GigabitEthernet2/0/0 DHCP Relay Address  **
 Dhcp Option          Relay Agent IP       Server IP
 *                    -                    10.10.1.2

    **  GigabitEthernet2/0/0.100 DHCP Relay Address  **
 Dhcp Option          Relay Agent IP       Server IP
 *                    -                    10.10.1.2

    **  GigabitEthernet2/0/1 DHCP Relay Address  **
 Dhcp Option          Relay Agent IP       Server IP
 *                    -                    10.10.1.2
```

执行命令 **display dhcp relay statistics**，可以看到 DHCPv4 中继的统计信息，包括错误的报文数、各种 DHCPv4 报文数。

```
<HUAWEI> display dhcp relay statistics
    Bad Packets received:                   0
    DHCP packets received from clients:     2
        DHCP DISCOVER packets received:     1
        DHCP REQUEST packets received:      1
        DHCP INFORM packets received:       0
        DHCP DECLINE packets received:      0
    DHCP packets received from servers:     2
        DHCP OFFER packets received:        1
        DHCP ACK packets received:          1
        DHCP NAK packets received:          0
```

```
DHCP packets sent to servers:            1
DHCP packets sent to clients:            1
    Unicast packets sent to clients:     0
    Broadcast packets sent to clients:   0
```

2.6 调整 DHCPv4 服务参数

通过调整 DHCPv4 服务参数达到提高 DHCPv4 服务安全性的目的。

2.6.1 建立配置任务
在调整 DHCPv4 服务参数前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

2.6.2 配置 DHCPv4 全局参数
DHCPv4 全局参数包括对指定单板允许接入 DHCPv4 用户数进行限制和对 DHCPv4 服务器组发送的报文进行限速。

2.6.3 配置 DHCPv4 报文透传功能
配置 DHCPv4 报文透传功能一般用于机顶盒用户快速关机再重启只发送一次 DHCPv4 Discover 报文的情况。

2.6.4 启动服务器的非法 DHCPv4 服务器检测功能
启动服务器的非法 DHCPv4 服务器检测功能可以防止其他非法 DHCPv4 服务器为客户端分配不合法的 IP 地址。

2.6.5 使能 IP 地址冲突检测功能
DHCPv4 服务器通过发送 Ping 报文探测地址的使用情况，进行 IP 地址冲突检测。

2.6.6 保存 DHCPv4 数据
保存 DHCPv4 数据到存储设备后，在发生故障时可以从存储设备恢复数据。

2.6.7 恢复 DHCPv4 数据
恢复 DHCPv4 数据可以恢复出系统保存的正常的地址租借信息和地址冲突信息。

2.6.8 检查配置结果
完成 DHCPv4 服务参数调整后，您可以查看到 DHCPv4 服务器的信息和 DHCPv4 数据库的存放路径。

2.6.1 建立配置任务

在调整 DHCPv4 服务参数前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

在配置 DHCPv4 服务器后，为了提高 DHCPv4 服务的安全性，防止其他非法 DHCPv4 服务器为客户端分配不合法的 IP 地址，需要配置 DHCPv4 服务的安全功能。网络管理员通过查看日志，判断是否有非法的 DHCPv4 服务器为客户端分配 IP 地址。

前置任务

在调整 DHCPv4 服务参数之前，需完成以下任务：

- 配置 DHCPv4 服务器

数据准备

在调整 DHCPv4 服务参数之前，需准备以下数据。

序号	数据
1	单板允许接入 DHCPv4 用户的最大数量
2	DHCPv4 服务器的 IP 地址
3	单位时间里允许发送的报文数目
4	是否使用非法 DHCPv4 服务器检测功能以及非法 DHCPv4 服务器检测的时间间隔
5	启动防止 IP 地址重复分配功能时 Ping 包的间隔和次数
6	保存 DHCPv4 数据的间隔

2.6.2 配置 DHCPv4 全局参数

DHCPv4 全局参数包括对指定单板允许接入 DHCPv4 用户数进行限制和对 DHCPv4 服务器组发送的报文进行限速。

背景信息

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dhcp** *slot-id* **max-sessions** *user-number*，配置设备上的指定单板允许接入 DHCPv4 用户的最大数量。

缺省情况下，指定单板允许接入 DHCPv4 用户的最大数量由 License 文件决定。

步骤 3 执行命令 **dhcp-server** *ip-address* [**vpn-instance** *vpn-instance*] **send-discover-speed** *packet-number time*，配置对 DHCPv4 服务器组发送的报文进行限速。

缺省情况下，不对 DHCPv4 服务器组发送的报文进行限速。

----结束

2.6.3 配置 DHCPv4 报文透传功能

配置 DHCPv4 报文透传功能一般用于机顶盒用户快速关机再重启只发送一次 DHCPv4 Discover 报文的情况。

背景信息

在机顶盒用户快速关机再重启时，NE20E-X6 感知不到用户下线，用户表项还在。收到机顶盒再重启发送的 DHCPv4 Discover 报文时，NE20E-X6 会先让用户下线，等待用户再次发起 DHCPv4 Discover 报文获取 DHCPv4 地址的过程。

而有些机顶盒关机再启动时，只发送一次 DHCPv4 Discover 报文，这就导致这些用户不能重新上线。

配置 DHCPv4 报文透传功能可解决上述问题。请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dhcp through-packet** ，配置 DHCPv4 报文透传功能。

缺省情况下，设备没有配置 DHCPv4 报文透传功能。

----结束

2.6.4 启动服务器的非法 DHCPv4 服务器检测功能

启动服务器的非法 DHCPv4 服务器检测功能可以防止其他非法 DHCPv4 服务器为客户端分配不合法的 IP 地址。

背景信息

在网络中，如果有私自架设的 DHCPv4 服务器，当其他用户申请 IP 地址时，这台 DHCPv4 服务器就会与 DHCPv4 客户端进行交互，导致用户获得错误的 IP 地址，无法正常上网，这种私设的 DHCPv4 服务器称为非法 DHCPv4 服务器。

网络管理员通过查看日志文件，可以看到所有为客户端提供 IP 地址的 DHCPv4 服务器的 IP 地址，进而可以判断是否存在非法 DHCPv4 服务器。

请在作为 DHCPv4 服务器的设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dhcp server detect**，使能服务器的非法 DHCPv4 服务器检测功能。

缺省情况下，禁止服务器的非法 DHCPv4 服务器检测功能。

说明

该功能只能在网络侧设备上配置。

步骤 3 执行命令 **dhcp invalid-server-detecting** [*interval*]，配置非法 DHCPv4 服务器检测的时间间隔。

如果非法 DHCPv4 服务器检测的时间间隔设置为 0，则表示不进行检测。

说明

该功能只能在 BAS 侧设备上配置。

----结束

2.6.5 使能 IP 地址冲突检测功能

DHCPv4 服务器通过发送 Ping 报文探测地址的使用情况，进行 IP 地址冲突检测。

背景信息

为防止 IP 地址重复分配导致地址冲突，DHCPv4 服务器为客户端分配地址前，需要先对该地址进行探测。

说明

该功能只能在网络侧设备上配置。

请在作为 DHCPv4 服务器的网络侧设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dhcp server ping timeout** *milliseconds*，配置 DHCPv4 服务器发送 Ping 包的最长等待响应时间。

步骤 3 执行命令 **dhcp server ping packets** *number*，配置 DHCPv4 服务器发送 Ping 包的最大数量。

缺省情况下，发送 Ping 包的最大数量为 2，等待 Ping 响应的最长时间为 500 毫秒。

----结束

后续处理

地址探测是通过 **Ping** 命令实现的，检测是否能在指定时间内得到 Ping 应答。如果没有得到应答，则继续发送 Ping 报文，直到发送 Ping 包数量达到最大值，如果仍然超时，则可以认为本网段内没有设备使用该 IP 地址，从而确保客户端被分得的 IP 地址是唯一的。

2.6.6 保存 DHCPv4 数据

保存 DHCPv4 数据到存储设备后，在发生故障时可以从存储设备恢复数据。

背景信息

请在作为 DHCPv4 服务器的设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dhcp server database enable**，使能 DHCPv4 数据保存到存储设备的功能。

步骤 3 （可选）执行命令 **dhcp server database write-delay** *seconds*，设置保存时延。

缺省情况下，不启用 DHCPv4 数据保存到存储设备的功能。如果启用此功能，缺省情况下，每隔 300 秒保存一次当前的 DHCPv4 数据，并覆盖之前的数据文件。

----结束

后续处理

系统将当前的 DHCPv4 数据保存到存储设备上，并可以在发生故障时从存储设备恢复数据。

DHCPv4 数据以固定的文件名保存在存储设备上，正常的地址租借信息保存在文件 lease.txt 中，地址冲突信息则保存在文件 conflict.txt 中。由于这两个文件会被定期覆盖，建议用户在必要时将生成的文件备份到其它位置。

2.6.7 恢复 DHCPv4 数据

恢复 DHCPv4 数据可以恢复出系统保存的正常的地址租借信息和地址冲突信息。

背景信息

请在作为 DHCPv4 服务器的设备上进行以下配置。

说明

必须使能 DHCPv4 数据保存的功能之后，才能将保存的 DHCPv4 数据恢复。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dhcp server database recover**，从存储设备恢复 DHCPv4 数据。

----结束

2.6.8 检查配置结果

完成 DHCPv4 服务参数调整后，您可以查看到 DHCPv4 服务器的信息和 DHCPv4 数据库的存放路径。

前提条件

已经完成 DHCPv4 服务参数调整的所有配置。

操作步骤

- 使用 **display dhcp-server item** *ip-address* [**vpn-instance** *vpn-instance*]命令查看 DHCPv4 服务器的信息。
- 使用 **display dhcp server database** 命令查看 DHCPv4 数据库的存放路径和文件信息。

----结束

任务示例

执行命令 **display dhcp-server item** *ip-address*，可以看到 DHCPv4 服务器的信息。

```
<HUAWEI> display dhcp-server item 1.2.3.4
  IPAddress  : 1.2.3.4
  State      :  UP
  Speed Limit : 0 packets / 0 seconds
```

执行命令 **display dhcp server database**，可以看到 DHCPv4 数据库的存放路径。

```
<HUAWEI> display dhcp server database
Status: disable
 Recover from files after reboot: disable
 File saving lease items: cfcard:/dhcp/lease.txt
```

```
File saving conflict items: cfcard:/dhcp/conflict.txt
Save Interval: 300 (seconds)
```

2.7 维护

维护 DHCPv4 包括清除 DHCPv4 统计信息、DHCPv4 运行状况和调试 DHCPv4。

2.7.1 清除 DHCPv4 统计信息
清除 DHCPv4 统计信息包括清除 DHCPv4 中继的统计信息。

2.7.2 监控 DHCPv4 运行状况
通过查看 IPv4 地址池、DHCPv4 服务器、DHCPv4 数据的存放路径和文件信息达到监控 DHCPv4 运行状况的目的。

2.7.1 清除 DHCPv4 统计信息

清除 DHCPv4 统计信息包括清除 DHCPv4 中继的统计信息。

背景信息

注意

清除 DHCPv4 的统计信息后，以前的统计信息将无法恢复，务必仔细确认。

操作步骤

- 在确认需要清除 DHCPv4 中继的统计信息后，请在用户视图下执行 **reset dhcp relay statistics** 命令。

----结束

2.7.2 监控 DHCPv4 运行状况

通过查看 IPv4 地址池、DHCPv4 服务器、DHCPv4 数据的存放路径和文件信息达到监控 DHCPv4 运行状况的目的。

前提条件

在日常维护工作中，可以在任意视图下选择执行以下命令，了解 DHCPv4 的运行情况。

操作步骤

- 在任意视图下执行 **display ip pool** [**name** *pool-name* [*section-num* [*start-ip-address* [*end-ip-address*]] | **all** | **used**]] [**vpn-instance** *vpn-instance-name*]命令查看 IPv4 地址池的配置信息。
- 在任意视图下执行 **display dhcp-server group** [*group-name*]命令查看 DHCPv4 服务器组的配置信息。
- 在任意视图下执行 **display dhcp-server item** *ip-address* [**vpn-instance** *vpn-instance*] 命令查看 DHCPv4 服务器的信息。

- 在任意视图下执行 **display dhcp-server statistics** *ip-address* [**vpn-instance** *vpn-instance*]命令查看 DHCPv4 服务器的统计信息。
- 在任意视图下执行 **display dhcp server database** 命令，查看 DHCPv4 数据库的存放路径和文件信息。
- 在任意视图下执行 **display dhcp relay address** { **all** | **interface** *interface-type interface-number* | **vlan** *vlan-id* } [| **count**] [| { **begin** | **exclude** | **include** } *regular-expression*]命令，查看 DHCPv4 中继地址配置。

----结束

2.8 配置举例

介绍 DHCPv4 配置的各种示例。配置示例中包括组网需求、配置注意事项和配置思路等。

背景信息

说明

实际组网环境中，需要加载 License，请参见《HUAWEI NetEngine20E-X6 高端业务路由器 配置指南-系统管理》。

2.8.1 配置本地地址池为接入用户分配地址示例
介绍一个本地地址池为用户分配 IPv4 地址配置示例，结合配置组网图来理解业务的配置过程。配置示例包括组网需求、思路准备、操作步骤和配置文件。

2.8.2 配置远端地址池为接入用户分配地址示例
介绍一个远端地址池为接入用户分配 IPv4 地址示例，结合配置组网图来理解业务的配置过程。配置示例包括组网需求、思路准备、操作步骤和配置文件。

2.8.3 配置三层 DHCPv4 用户接入示例
介绍一个三层 DHCPv4 用户接入示例，结合配置组网图来理解业务的配置过程。配置示例包括组网需求、思路准备、操作步骤和配置文件。

2.8.4 配置以太网用户 IP 地址分配示例（无中继设备）
介绍一个以太网用户 IP 地址分配示例（无中继设备），结合配置组网图来理解业务的配置过程。配置示例包括组网需求、思路准备、操作步骤和配置文件。

2.8.5 配置以太网用户 IP 地址分配示例（包含中继设备）
介绍一个以太网用户 IP 地址分配示例（包含中继设备），结合配置组网图来理解业务的配置过程。配置示例包括组网需求、思路准备、操作步骤和配置文件。

2.8.1 配置本地地址池为接入用户分配地址示例

介绍一个本地地址池为用户分配 IPv4 地址配置示例，结合配置组网图来理解业务的配置过程。配置示例包括组网需求、思路准备、操作步骤和配置文件。

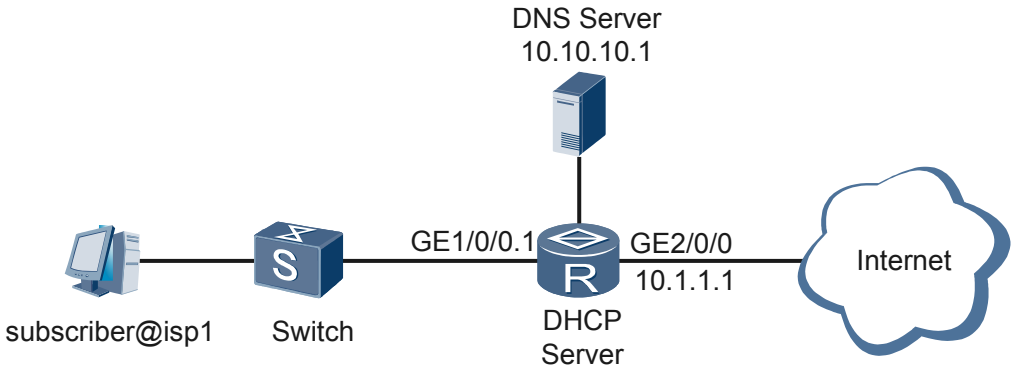
组网需求

如**图 2-5** 所示，配置本地地址池为接入用户分配地址的组网需求为：

- 使用本地地址池为 isp1 域的用户分配地址。
- 地址池的 IP 地址为 10.10.10.3 ～ 10.10.10.100，网关地址为 10.10.10.2。
- 地址池的 DNS 服务器地址为 10.10.10.1。

- 用户采用的认证策略为不认证，计费策略为不计费。

图 2-5 配置本地地址池为接入用户分配地址组网图



配置思路

说明

接入用户包括 IPoE 用户和 PPPoE 用户，本地地址池为 IPoE 和 PPPoE 用户分配地址的不同之处在于接入方式的不同，本节只介绍与 IPv4 地址池相关的配置，有关 IPoE 接入方式的配置请参见**配置普通 IPoE 接入 VPN 示例**，有关 PPPoE 接入方式的配置请参见**配置 PPPoE 接入示例**。

DHCPv4 服务器的配置思路如下：

1. 配置本地地址池，包括网关地址、地址范围和 DNS 服务器地址。
2. 配置用户所在的域 isp1，包括认证方式和计费方式。
3. 配置 BAS 接口，包括用户的接入方式。

数据准备

完成此配置举例，需要准备以下数据：

- 地址池名称、范围、网关地址和 DNS 服务器地址
- 用户所在域的名称
- 认证方式和计费方式

操作步骤

步骤 1 在 DHCPv4 服务器上进行配置

配置地址池。

```
<HUAWEI> system-view
[HUAWEI] ip pool pool1 bas local
[HUAWEI-ip-pool-pool1] gateway 10.10.10.2 255.255.255.0
[HUAWEI-ip-pool-pool1] section 0 10.10.10.3 10.10.10.100
[HUAWEI-ip-pool-pool1] dns-server 10.10.10.1
[HUAWEI-ip-pool-pool1] quit
```

配置 isp1 域。

```
[HUAWEI] aaa
[HUAWEI-aaa] domain isp1
```

```
[HUAWEI-aaa-domain-isp1] authentication-scheme default0
[HUAWEI-aaa-domain-isp1] accounting-scheme default0
[HUAWEI-aaa-domain-isp1] ip-pool pool1
[HUAWEI-aaa-domain-isp1] quit
[HUAWEI-aaa] quit
```

配置 BAS 接口。

```
[HUAWEI] interface gigabitEthernet 1/0/0.1
[HUAWEI-GigabitEthernet1/0/0.1] user-vlan 1
[HUAWEI-GigabitEthernet1/0/0.1-vlan-1-1] bas
[HUAWEI-GigabitEthernet1/0/0.1-bas] access-type layer2-subscriber
[HUAWEI-GigabitEthernet1/0/0.1-bas] authentication-method bind
[HUAWEI-GigabitEthernet1/0/0.1-bas] default-domain authentication isp1
[HUAWEI-GigabitEthernet1/0/0.1-bas] quit
[HUAWEI-GigabitEthernet1/0/0.1] quit
```

步骤 2 验证配置结果

查看本地地址池 pool1 的配置。

```
[HUAWEI] display ip pool name pool1

  Pool-Name      : pool1
  Pool-No        : 19
  Lease          : 3 Days 0 Hours 0 Minutes
  NetBois Type   : N-Node
  DNS-Suffix     : -,
  DNS1          :10.10.10.1
  Position       : Local           Status          : Unlocked
  Gateway        : 10.10.10.2      Mask            : 255.255.255.0
  Vpn instance   : --
  Profile-Name   : -               Server-Name     : -
  Codes: CFLCT (conflicted)

  ------------------------------------------------------------------------------
  ID           start             end total  used  idle CFLCT disable reserved static-bind
  ------------------------------------------------------------------------------
   0       10.10.10.3     10.10.10.100    98     0    98     0       0        0           0
  ------------------------------------------------------------------------------
```

查看域 isp1 的配置。

```
[HUAWEI] display domain isp1
 ------------------------------------------------------------------------------
  Domain-name                    : isp1
  Domain-state                   : Active
  Authentication-scheme-name     : default0
  Accounting-scheme-name         : default0
  Authorization-scheme-name      :
  Primary-DNS-IP-address         : -
  Second-DNS-IP-address          : -
  Web-server-URL-parameter       : No
  Portal-server-URL-parameter    : No
  Primary-NBNS-IP-address        : -
  Second-NBNS-IP-address         : -
  User-group-name                : -
  Idle-data-attribute (time,flow) : 0,60
  Install-BOD-Count              : 0
  Report-VSM-User-Count          : 0
  Value-added-service            : COPS
  User-access-limit              : 279552
  Online-number                  : 0
  Web-IP-address                 : -
  Web-URL                        : -
  Portal-server-IP               : -
  Portal-URL                     : -
  Portal-force-times             : 2
  PPPoE-user-URL                 : Disable
  IPUser-ReAuth-Time (second)      : 300
```

```
  mscg-name-portal-key           : -
  Portal-user-first-url-key      : -
  Ancp auto qos adapt            : Disable
  Service-type                   : STB
  RADIUS-server-template         : -
  Two-acct-template              : -
  HWTACACS-server-template       : -
  Bill Flow                      : Disable
  Tunnel-acct-2867               : Disabled
  Flow Statistic:
  Flow-Statistic-Up              : Yes
  Flow-Statistic-Down            : Yes
  Source-IP-route                : Disable
  IP-warning-threshold           : -
  Multicast Forwarding           : Yes
  Multicast Virtual              : No
  Max-multilist num              : 4
  Multicast-profile              : -
  IP-address-pool-name           : pool1
  Quota-out                    : Offline
  ---------------------------------------------------------------------------
```

----结束

配置文件

HUAWEI 的配置文件

```
#
 sysname HUAWEI
#
ip pool pool1 bas local
 gateway 10.10.10.2 255.255.255.0
 section 0 10.10.10.3 10.10.10.100
 dns-server 10.10.10.1
#
aaa
 authentication-scheme default0
 #
 accounting-scheme default0
 #
domain isp1
 authentication-scheme default0
 accounting-scheme default0
 ip-pool pool1
 #
interface GigabitEthernet1/0/0.1
 user-vlan 1
 bas
 #
  access-type layer2-subscriber default-domain authentication isp
1
  authentication-method bind
#
return
```

2.8.2 配置远端地址池为接入用户分配地址示例

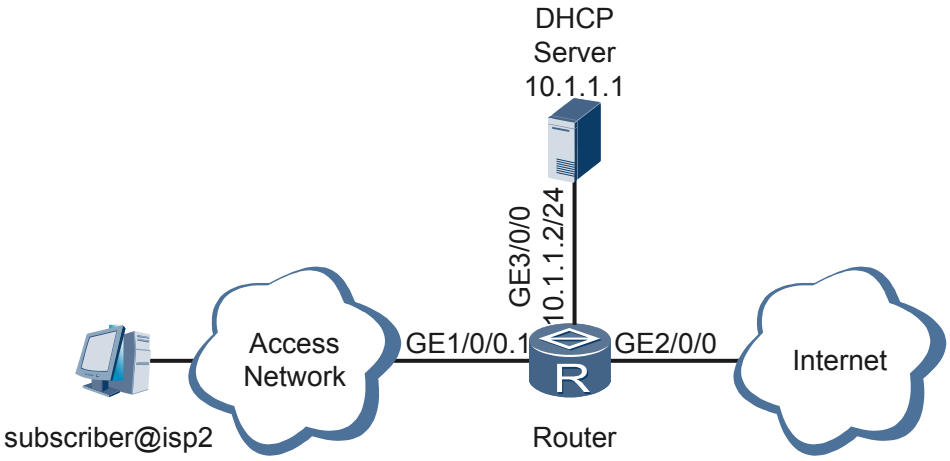
介绍一个远端地址池为接入用户分配 IPv4 地址示例，结合配置组网图来理解业务的配置过程。配置示例包括组网需求、思路准备、操作步骤和配置文件。

组网需求

如图 2-6 所示，配置远端地址池为接入用户分配地址的组网需求为：

- 使用远端地址池为 isp2 域的用户分配地址。
- 路由器作为 relay 设备，通过接口 GE3/0/0 与 DHCPv4 服务器相连。接口 GE3/0/0 的 IP 地址为 10.1.1.2/24。
- 远端地址池对应的 DHCPv4 服务器地址为 10.1.1.1，没有备用 DHCPv4 服务器。
- 用户采用的认证策略为不认证，计费策略为不计费。

图 2-6 配置远端地址池为接入用户分配地址组网图



配置思路

DHCPv4 服务器的配置思路如下：

1. 创建 DHCPv4 服务器组、远端地址池，并将地址池绑定到 DHCPv4 服务器组。
2. 配置用户所在的域 isp2，包括认证方式和计费方式。
3. 配置 BAS 接口，包括用户的接入方式。

数据准备

完成此配置举例，需要准备以下数据：

- 地址池名称
- 网关地址
- 用户所在域的名称
- 与服务器相连的接口的 IP 地址
- 用户的接入方式

操作步骤

步骤 1 在路由器上进行配置

创建 DHCPv4 服务器组。

```
<HUAWEI> system-view
[HUAWEI] dhcp-server group group1
[HUAWEI-dhcp-server-group-group1] dhcp-server 10.1.1.1
```

```
[HUAWEI-dhcp-server-group-group1] quit
```

创建远端地址池，绑定 DHCPv4 服务器组。

```
[HUAWEI] ip pool pool2 bas remote
[HUAWEI-ip-pool-pool2] gateway 10.10.10.1 24
[HUAWEI-ip-pool-pool2] dhcp-server group group1
[HUAWEI] quit
```

配置 isp2 域。

```
[HUAWEI] aaa
[HUAWEI-aaa] domain isp2
[HUAWEI-aaa-domain-isp2] authentication-scheme default0
[HUAWEI-aaa-domain-isp2] accounting-scheme default0
[HUAWEI-aaa-domain-isp2] ip-pool pool2
[HUAWEI-aaa-domain-isp2] quit
[HUAWEI-aaa] quit
```

配置接入用户的接口。

```
[HUAWEI] interface gigabitEthernet1/0/0.1
[HUAWEI-GigabitEthernet1/0/0.1] user-vlan 1
[HUAWEI-GigabitEthernet1/0/0.1-vlan-1-1] bas
[HUAWEI-GigabitEthernet1/0/0.1-bas] access-type layer2-subscriber
[HUAWEI-GigabitEthernet1/0/0.1-bas] authentication-method bind
[HUAWEI-GigabitEthernet1/0/0.1-bas] default-domain authentication isp2
[HUAWEI-GigabitEthernet1/0/0.1-bas] quit
[HUAWEI-GigabitEthernet1/0/0.1] quit
```

配置与服务器相连的接口。

```
[HUAWEI] interface GigabitEthernet 3/0/0
[HUAWEI-GigabitEthernet3/0/0] ip address 10.1.1.2 255.255.255.0
```

步骤 2 验证配置结果

查看 DHCP 服务器组 group1 的配置。

```
[HUAWEI] display dhcp-server group group1
  Group-Name          : group1
  Release-Agent       : Support
  Primary-Server      : 10.1.1.1
    Vpn instance      : --
  Weight              : 0
  Status              : up
  Secondary-Server    : -
    Vpn instance      : --
  Weight              : 0
  Status              : -
  Algorithm           : master-backup
  Source              : --
  Giaddr              : --
```

查看远端地址池 pool2 的配置。

```
[HUAWEI] display ip pool name pool2

  Pool-Name      : pool2
  Pool-No        : 0
  DHCP-Group     : group1
  Position       : Remote          Status           : Unlocked
  Gateway        : 10.10.10.1      Mask             : 255.255.255.0
  Vpn instance   : --
  Profile-Name   : -               Server-Name      : -
  Codes: CFLCT (conflicted)

  ------------------------------------------------------------------------------
  ID           start             end total  used  idle CFLCT disable reserved static-bind
  ------------------------------------------------------------------------------
```

```
  0        10.10.10.0      10.10.10.255    256       0    256       0         0         0             0
------------------------------------------------------------------------------
```

查看域 isp2 的配置。

```
[HUAWEI] display domain isp2
------------------------------------------------------------------------------
  Domain-name                     : isp2
  Domain-state                    : Active
  Authentication-scheme-name      : default0
  Accounting-scheme-name          : default0
  Authorization-scheme-name       :
  Primary-DNS-IP-address          : -
  Second-DNS-IP-address           : -
  Primary-NBNS-IP-address         : -
  Second-NBNS-IP-address          : -
  User-group-name                 : -
  Idle-data-attribute (time,flow) : 0, 60
  Install-BOD-Count               : 0
  Report-VSM-User-Count           : 0
  Value-added-service             : COPS
  User-access-limit               : 279552
  Online-number                   : 0
  Web-IP-address                  : -
  Web-URL                         : -
  Portal-server-IP                : -
  Portal-URL                      : -
  Portal-force-times              : 2
  PPPoE-user-URL                  : Disable
  IPUser-ReAuth-Time(second)      : 300
  Ancp auto qos adapt             : Disable
  RADIUS-server-template          : -
  Two-acct-template               : -
  HWTACACS-server-template        : -
  Bill Flow                       : Disable
  Tunnel-acct-2867                : Disabled

  Flow Statistic:
  Flow-Statistic-Up               : Yes
  Flow-Statistic-Down             : Yes
  Source-IP-route                 : Disable
  IP-warning-threshold            : -
  Multicast Forwarding            : Yes
  Multicast Virtual               : No
  Max-multilist num               : 4
  Multicast-profile               : -
  IP-address-pool-name            : pool2
  Quota-out                     : Offline
  ------------------------------------------------------------------------------
```

----结束

配置文件

路由器的配置文件

```
#
 sysname HUAWEI
#
dhcp-server group group1
 dhcp-server 10.1.1.1
#
ip pool pool2 bas remote
 gateway 10.10.10.1 255.255.255.0
 dhcp-server group group1
#
aaa
 authentication-scheme default0
 #
```

```
 accounting-scheme default0
 #
domain isp2
 authentication-scheme default0
 accounting-scheme default0
 ip-pool pool2
 #
interface GigabitEthernet1/0/0.1
 undo shutdown
 user-vlan 1
 bas
 #
  access-type layer2-subscriber default-domain authentication
 isp2
  authentication-method bind
#
interface GigabitEthernet3/0/0
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
#
return
```

2.8.3 配置三层 DHCPv4 用户接入示例

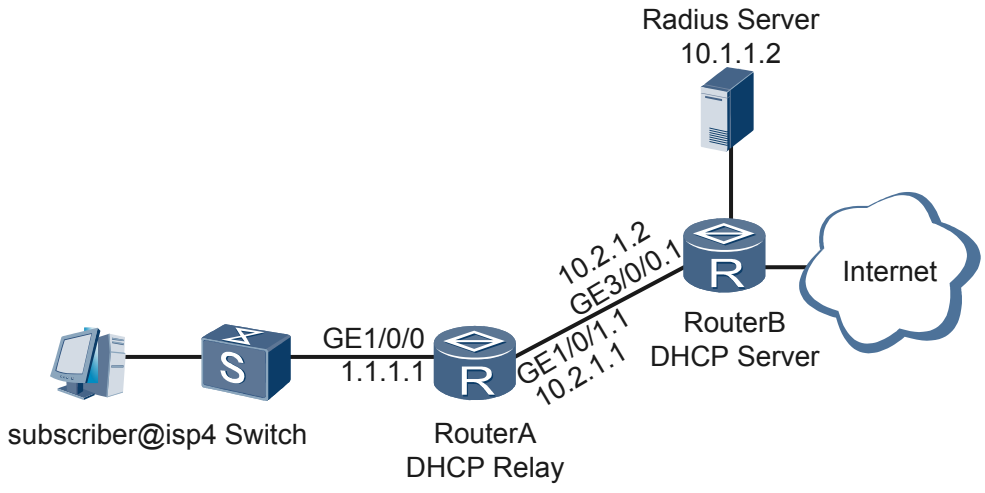
介绍一个三层 DHCPv4 用户接入示例，结合配置组网图来理解业务的配置过程。配置示例包括组网需求、思路准备、操作步骤和配置文件。

组网需求

如图 2-7 所示，配置三层 DHCPv4 用户接入的组网需求为：

- 用户归属于 isp4 域，通过 RouterA 接入 RouterB，其中用户与 RouterA 连接接口为 GE1/0/0。
- RouterB 作为 DHCPv4 服务器，通过接口 GE3/0/0.1 与 RouterA 相连。接口 GE3/0/0.1 的 IP 地址为 10.2.1.2/24。
- 用户采用 web 认证，并采用 RADIUS 认证模式和 RADIUS 计费模式。
- RADIUS 服务器地址为 10.1.1.2，认证和计费端口分别是 1812 和 1813，采用标准 RADIUS 协议，密钥为 hello。

图 2-7 配置三层 DHCPv4 用户接入组网图



配置思路

DHCPv4 服务器的配置思路如下：

1. 配置地址池，包括网关地址和地址范围。
2. 配置认证方案和计费方案。
3. 配置 RADIUS 服务器组，包括 RADIUS 服务器地址、认证端口和计费端口。
4. 配置用户所在的域 isp4，包括认证方式和计费方式。
5. 配置 BAS 接口，包括用户的接入方式。

数据准备

完成此配置举例，需要准备以下数据：

- 地址池名称、范围以及网关地址
- 认证方案和计费方案
- RADIUS 服务器地址、认证端口和计费端口
- 用户所在域的名称

操作步骤

步骤 1 在 RouterA 上进行配置

配置接口 GE1/0/0。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterA
[RouterA] interface gigabitEthernet 1/0/0
[RouterA-GigabitEthernet1/0/0] undo shutdown
[RouterA-GigabitEthernet1/0/0] dhcp select relay
[RouterA-GigabitEthernet1/0/0] ip address 1.1.1.1 24
[RouterA-GigabitEthernet1/0/0] ip relay address 10.2.1.2
[RouterA-GigabitEthernet1/0/0] quit
```

配置接口 GE1/0/1.1。

```
[RouterA] interface gigabitEthernet 1/0/1.1
[RouterA-GigabitEthernet1/0/1.1] undo shutdown
[RouterA-GigabitEthernet1/0/1.1] vlan-type dot1q 1
[RouterA-GigabitEthernet1/0/1.1] ip address 10.2.1.1 24
```

步骤 2 在 RouterB 上进行配置

配置地址池。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterB
[RouterB] ip pool pool4 bas local
[RouterB-ip-pool-pool4] gateway 1.1.1.1 255.255.255.0
[RouterB-ip-pool-pool4] section 0 1.1.1.2 1.1.1.200
[RouterB-ip-pool-pool4] quit
```

配置认证方案。

```
[RouterB] aaa
[RouterB-aaa] authentication-scheme auth4
[RouterB-aaa-authen-auth4] authentication-mode radius
[RouterB-aaa-authen-auth4] quit
```

配置计费方案。

```
[RouterB-aaa] accounting-scheme acct4
[RouterB-aaa-accounting-acct4] accounting-mode radius
[RouterB-aaa-accounting-acct4] quit
[RouterB-aaa] quit
```

配置 RADIUS 服务器组。

```
[RouterB] radius-server group rd4
[RouterB-radius-rd4] radius-server authentication 10.1.1.2 1812
[RouterB-radius-rd4] radius-server accounting 10.1.1.2 1813
[RouterB-radius-rd4] radius-server type standard
[RouterB-radius-rd4] radius-server shared-key hello
[RouterB-radius-rd4] quit
```

配置 isp4 域。

```
[RouterB] aaa
[RouterB-aaa] domain isp4
[RouterB-aaa-domain-isp4] authentication-scheme auth4
[RouterB-aaa-domain-isp4] accounting-scheme acct4
[RouterB-aaa-domain-isp4] radius-server group rd4
[RouterB-aaa-domain-isp4] quit
[RouterB-aaa] quit
```

配置 BAS 接口。

```
[RouterB] interface gigabitEthernet 3/0/0.1
[RouterB-GigabitEthernet3/0/0.1] undo shutdown
[RouterB-GigabitEthernet3/0/0.1] ip address 10.2.1.2 24
[RouterB-GigabitEthernet3/0/0.1] vlan-type dot1q 1
[RouterB-GigabitEthernet3/0/0.1] bas
[RouterB-GigabitEthernet3/0/0.1-bas] access-type layer3-subscriber
[RouterB-GigabitEthernet3/0/0.1-bas] default-domain authentication isp4
[RouterB-GigabitEthernet3/0/0.1-bas] quit
[RouterB-GigabitEthernet3/0/0.1] quit
[RouterB] ip route-static 1.1.1.1 255.255.255.255 10.2.1.1
```

步骤 3 验证配置结果

查看本地地址池 pool4 的配置。

```
[RouterB] display ip pool name pool4
  Pool-Name      : pool4
  Pool-No        : 0
  Lease          : 3 Days 0 Hours 0 Minutes
  NetBois Type   : N-Node
  DNS-Suffix     : -
  Position       : Local          Status           : Unlocked
  Gateway        : 1.1.1.1    Mask             : 255.255.255.0
  Vpn instance   : --
  Profile-Name   : -              Server-Name      : -
  Codes: CFLCT(conflicted)
  ------------------------------------------------------------------------------
  ID           start             end total  used  idle CFLCT disable reserved
  ------------------------------------------------------------------------------
   0        1.1.1.2       1.1.1.200    199     0   199     0       0        0
  ------------------------------------------------------------------------------
```

查看域 isp4 的配置。

```
[RouterB] display domain isp4
  ------------------------------------------------------------------------------
  Domain-name                    : isp4
  Domain-state                   : Active
  Authentication-scheme-name     : auth4
  Accounting-scheme-name         : acct4
  Authorization-scheme-name      :
  Primary-DNS-IP-address         : -
  Second-DNS-IP-address          : -
  Primary-NBNS-IP-address        : -
```

```
  Second-NBNS-IP-address          : -
  User-group-name                 : -
  Idle-data-attribute (time,flow) : 0, 60
  Install-BOD-Count               : 0
  Report-VSM-User-Count           : 0
  Value-added-service             : COPS
  User-access-limit               : 279552
  Online-number                   : 0
  Web-IP-address                  : -
  Web-URL                         : -
  Portal-server-IP                : -
  Portal-URL                      : -
  Portal-force-times              : 2
  PPPoE-user-URL                  : Disable
  IPUser-ReAuth-Time(second)      : 300
  Ancp auto qos adapt             : Disable
  RADIUS-server-template          : rd4
  Two-acct-template               : -
  HWTACACS-server-template        : -
  IP-warning-threshold            : -
  Max-multilist num               : 4
  Multicast-profile               : -
  Quota-out                     : Offline
  ------------------------------------------------------------------------------
```

----结束

配置文件

RouterA 的配置文件

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 1.1.1.1 255.255.255.0
 ip relay address 10.2.1.2
 dhcp select relay
#
interface GigabitEthernet1/0/1.1
 undo shutdown
 vlan-type dot1q 1
 ip address 10.2.1.1 255.255.255.0
#
```

RouterB 的配置文件

```
#
 sysname RouterB
#
radius-server group rd4
 radius-server authentication 10.1.1.2 1812 weight 0
 radius-server accounting 10.1.1.2 1813 weight 0
 radius-server shared-key hello
#
ip pool pool4 bas local
 gateway 1.1.1.1 255.255.255.0
 section 0 1.1.1.2 10.1.1.200
#
aaa
 authentication-scheme auth4
  authentication-mode  radius
 #
 accounting-scheme acct4
  accounting-mode radius
 #
domain isp4
 authentication-scheme auth4
```

```
 accounting-scheme acct4
  radius-server group rd4
#
interface GigabitEthernet3/0/0.1
 vlan-type dotlq 1
 ip address 10.2.1.2 255.255.255.0
 bas
 #
  access-type layer3-subscriber default-domain authentication isp4
  authentication-method web
  ip-trigger
#
ip route-static 1.1.1.1 255.255.255.255 10.2.1.1
#
return
```

2.8.4 配置以太网用户 IP 地址分配示例（无中继设备）

介绍一个以太网用户 IP 地址分配示例（无中继设备），结合配置组网图来理解业务的配置过程。配置示例包括组网需求、思路准备、操作步骤和配置文件。

组网需求

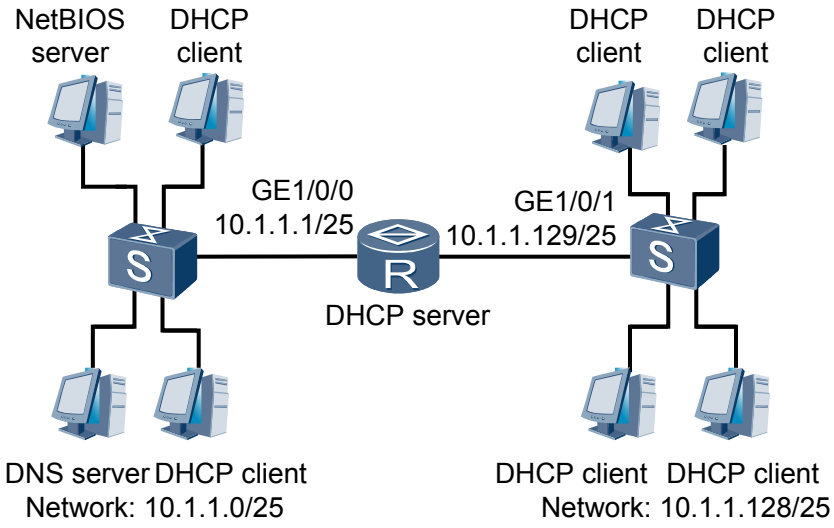
在一个较大的网络里，如果网络中的计算机不能与路由设备通过以太网接口直接相连，而要穿过其他的设备，在这种情况下，为了让计算机从路由设备动态获取 IP 地址，通常需要配置网络侧 DHCPv4 服务器。

如图 2-8 所示，DHCPv4 服务器为同一网段中的客户端动态分配 IP 地址，地址池网段 10.1.1.0/24 分为两个网段：10.1.1.0/25 和 10.1.1.128/25。DHCPv4 服务器两个 GigabitEthernet 接口的 IP 地址分别为 10.1.1.1/25 和 10.1.1.129/25。

网段 10.1.1.0/25 内的地址租用期限为 10 天 12 小时，DNS 后缀名为 huawei.com，DNS 服务器地址为 10.1.1.2，无 NetBIOS 地址，网关地址为 10.1.1.1；

网段 10.1.1.128/25 内的地址租用期限为 5 天，DNS 后缀名为 huawei.com，DNS 服务器地址为 10.1.1.2，NetBIOS 地址为 10.1.1.4，网关地址为 10.1.1.129。

图 2-8 以太网用户 IP 地址分配－无中继设备组网图



配置思路

DHCPv4 服务器的配置思路如下：

1. 配置接口的 IP 地址。
2. 配置地址池，包括网关地址、地址范围、DNS 后缀名、地址租用期限和不参与自动分配的 IP 地址，一般包括 DNS 服务器地址、NetBIOS 和网关地址等。

   此配置举例介绍的是配置两个地址池的情况。

数据准备

完成此配置举例，需要准备以下数据：

- 接口的 IP 地址
- 地址池编号及范围
- 禁止分配的 IP 地址
- DNS 后缀名、DNS 服务器地址和地址租用期限

操作步骤

步骤 1 在 DHCPv4 服务器上进行配置

配置接口 GE1/0/0 的 IP 地址。

```
[HUAWEI] interface gigabitethernet 1/0/0
[HUAWEI-GigabitEthernet1/0/0] ip address 10.1.1.1 255.255.255.128
[HUAWEI-GigabitEthernet1/0/0] undo shutdown
[HUAWEI-GigabitEthernet1/0/0] quit
```

配置接口 GE1/0/1 的 IP 地址。

```
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] ip address 10.1.1.129 255.255.255.128
[HUAWEI-GigabitEthernet1/0/1] undo shutdown
[HUAWEI-GigabitEthernet1/0/1] quit
```

配置 DHCPv4 地址池 1 的属性（网关地址、地址池范围、DNS 后缀名、DNS 服务器地址和地址租用期限）。

```
[HUAWEI] ip pool 1 server
[HUAWEI-ip-pool-1] gateway 10.1.1.1 255.255.255.128
[HUAWEI-ip-pool-1] section 0 10.1.1.2 10.1.1.126
[HUAWEI-ip-pool-1] excluded-ip-address 10.1.1.2
[HUAWEI-ip-pool-1] excluded-ip-address 10.1.1.4
[HUAWEI-ip-pool-1] dns-suffix huawei.com
[HUAWEI-ip-pool-1] dns-server 10.1.1.2
[HUAWEI-ip-pool-1] lease 10 12
[HUAWEI-ip-pool-1] quit
```

配置 DHCPv4 地址池 2 的属性（地址池范围、网关、NetBIOS 地址和地址租用期限）。

```
[HUAWEI] ip pool 2 server
[HUAWEI-ip-pool-2] gateway 10.1.1.129 255.255.255.128
[HUAWEI-ip-pool-2] section 0 10.1.1.130 10.1.1.254
[HUAWEI-ip-pool-2] dns-suffix huawei.com
[HUAWEI-ip-pool-2] dns-server 10.1.1.2
[HUAWEI-ip-pool-2] lease 5
[HUAWEI-ip-pool-2] netbios-name-server 10.1.1.4
[HUAWEI-ip-pool-2] quit
```

步骤 2 验证配置结果

配置完后，在 DHCPv4 服务器上使用 **display ip pool** 命令查看 DHCPv4 地址池信息。

```
<HUAWEI> display ip pool
  ------------------------------------------------------------------------
  Pool-Name      : 1
  Pool-No        : 1
  Position       : Relay           Status           : Unlocked
  Gateway        : 10.1.1.1        Mask             : 255.255.255.128
  Vpn instance   : --

  ------------------------------------------------------------------------
  Pool-Name      : 2
  Pool-No        : 2
  Position       : Relay           Status           : Unlocked
  Gateway        : 10.1.1.129    Mask             : 255.255.255.128
  Vpn instance   : --


  IP address pool Statistic
    Local       :0          Remote    :0          Server   :2

  IP address Statistic
    Total       :152
    Used        :0          Free      :152
    Conflicted  :0          Disable   :0
    Designated       :0
```

----结束

配置文件

HUAWEI 的配置文件

```
#
 sysname HUAWEI
#
ip pool 1 server
 gateway 10.1.1.1 255.255.255.128
 secton 0 10.1.1.2 10.1.1.126
 excluded-ip-address 10.1.1.2
 excluded-ip-address 10.1.1.4
 dns-server 10.1.1.2
 dns-suffix huawei.com
 lease 10 12
#
ip pool 2 server
 gateway 10.1.1.129 255.255.255.128
 secton 0 10.1.1.130 10.1.1.254
 dns-server 10.1.1.2
 dns-suffix huawei.com
 netbios-name-server 10.1.1.4
 lease 5
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.1 255.255.255.128
#
interface GigabitEthernet1/0/1
 undo shutdown
 ip address 10.1.1.129 255.255.255.128
#
return
```

2.8.5 配置以太网用户 IP 地址分配示例（包含中继设备）

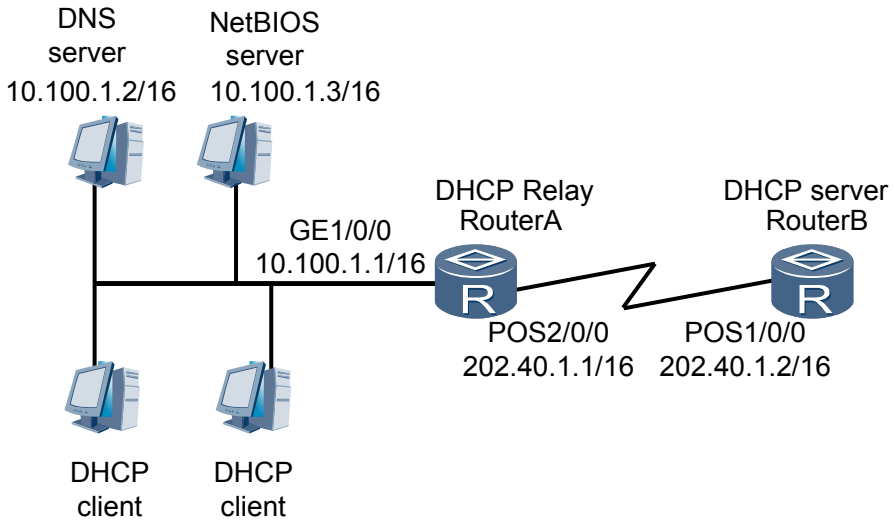
介绍一个以太网用户 IP 地址分配示例（包含中继设备），结合配置组网图来理解业务的配置过程。配置示例包括组网需求、思路准备、操作步骤和配置文件。

组网需求

网络侧的 DHCPv4 服务器通常与 DHCPv4 Relay Agent 协同工作。如图 2-9，DHCPv4 客户端所在的网段为 10.100.0.0/16，而 DHCPv4 服务器所在的网段为 202.40.0.0/16。需要通过带 DHCPv4 中继功能的路由设备转发 DHCPv4 报文，使得 DHCPv4 客户端可以从 DHCPv4 服务器上申请到 IP 地址等相关配置信息。

DHCPv4 服务器应当配置一个网络侧的 IP 地址池，DNS 服务器地址为 10.100.1.2/16，NetBIOS 服务器地址 10.100.1.3/16，网关地址 10.100.1.1，并且 DHCPv4 服务器上应当配置有到 10.100.0.0/16 网段的路由。

图 2-9 以太网用户 IP 地址分配-包含中继设备组网图



配置思路

DHCPv4 服务器的配置思路如下：

1. 配置要实现 DHCPv4 中继功能的接口 POS2/0/0
2. 在接口 GE1/0/0 配置该接口所代理的 DHCPv4 服务器地址并使能接口的 DHCPv4 中继功能
3. 配置 DHCPv4 服务器 RouterB 到 RouterA 的接口 GE1/0/0 的路由
4. 配置 RouterB 的接口 POS1/0/0 下的客户端从地址池中获取 IP 地址
5. 在 RouterB 上配置网络侧的地址池

数据准备

完成此配置举例，需要准备以下数据：

- 要实现 DHCPv4 中继功能的接口的 IP 地址
- DHCPv4 服务器的地址
- DHCPv4 地址池（包括网关地址、地址池范围、不参与自动分配的 IP 地址、DNS 后缀名、DNS 地址、地址租用期）

操作步骤

步骤 1 在 DHCPv4 中继上进行配置

配置接口 POS2/0/0 接口地址。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterA
[RouterA] interface pos 2/0/0
[RouterA-Pos2/0/0] ip address 202.40.1.1 255.255.0.0
[RouterA-Pos2/0/0] undo shutdown
[RouterA-Pos2/0/0] quit
```

进入要实现 DHCPv4 中继功能的接口，为其配置 IP 地址、子网掩码和该接口所代理的 DHCPv4 服务器地址。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 10.100.1.1 255.255.0.0
[RouterA-GigabitEthernet1/0/0] dhcp select relay
[RouterA-GigabitEthernet1/0/0] ip relay address 202.40.1.2
[RouterA-GigabitEthernet1/0/0] undo shutdown
[RouterA-GigabitEthernet1/0/0] quit
```

步骤 2 在 DHCPv4 服务器上进行配置

配置 RouterB 到 RouterA 与客户端相连接口 GE1/0/0 的路由。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterB
[RouterB] ip route-static 10.100.0.0 255.255.0.0 202.40.1.1
```

配置接口 POS1/0/0 下的 IP 地址。

```
[RouterB] interface pos 1/0/0
[RouterB-Pos1/0/0] ip address 202.40.1.2 255.255.0.0
[RouterB-Pos1/0/0] undo shutdown
[RouterB-Pos1/0/0] quit
```

配置 DHCPv4 地址池 1 属性（网关地址、地址池范围、不参与自动分配的 IP 地址、DNS 后缀名、DNS 地址、地址租用期）。

```
[RouterB] ip pool 1 server
[RouterB-ip-pool-1] gateway 10.100.1.1 255.255.0.0
[RouterB-ip-pool-1] section 0 10.100.1.5 10.100.1.100
[RouterB-ip-pool-1] dns-suffix huawei.com
[RouterB-ip-pool-1] dns-server 10.100.1.2
[RouterB-ip-pool-1] netbios-name-server 10.100.1.3
[RouterB-ip-pool-1] lease 10 12
[RouterB-ip-pool-1] quit
```

步骤 3 验证配置结果

在 DHCPv4 服务器上使用 **display ip pool** 命令用来查看 DHCPv4 地址池的树状结构信息，其中包括配置的 DNS 服务、地址租用期限、Option 参数等信息。

```
[RouterB] display ip pool
  ------------------------------------------------------------------------
  Pool-Name      : 1
  Pool-No        : 1
  Position       : Server          Status          : Unlocked
```

```
Gateway        : 10.100.1.1      Mask            : 255.255.0.0
Vpn instance   : --

------------------------------------------------------------------------


IP address pool Statistic
  Local       :0          Remote    :0          Server   :1

IP address Statistic
  Total       :96
  Used        :0          Free      :96
  Conflicted  :0          Disable   :0
  Designated       :0
```

在 DHCPv4 中继上，使用 **display dhcp relay address** 命令用来查看接口的 DHCPv4 配置情况。

```
[RouterA] display dhcp relay address all
  **  GigabitEthernet1/0/0 DHCP Relay Address  **
 Dhcp Option          Relay Agent IP       Server IP
 *                    -                    202.40.1.2
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.100.1.1 255.255.0.0
 ip relay address 202.40.1.2
 dhcp select relay
#
interface Pos 2/0/0
 link-protocol ppp
 undo shutdown
 ip address 202.40.1.1 255.255.0.0
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
ip pool 1 server
 gateway 10.100.1.1 255.255.0.0
 section 0 10.100.1.5 10.100.1.100
 dns-server 10.100.1.2
 dns-suffix huawei.com
 netbios-name-server 10.100.1.3
 lease 10 12
#
interface Pos 1/0/0
 link-protocol ppp
 undo shutdown
ip address 202.40.1.2 255.255.0.0
#
ip route-static 10.100.0.0 255.255.0.0 202.40.1.1
#
return
```

3 配置 BRAS 接入

关于本章

通过配置 BRAS 接入实现多种接入方式的业务控制和管理。

3.1 简介
BRAS 接入认证通过用户报文的协议栈来区分用户，对应不同的用户，灵活地选择不同的认证方式。

3.2 配置认证方式
认证技术指用户终端与设备之间进行认证交互、提交用户名和密码的方法，NE20E-X6 提供了多种认证技术。

3.3 配置 IPoX 接入业务
IPoX 接入方式下，接入用户只需通过报文触发的方式接入 Internet，无需安装客户端拨号软件、无需拨号。

3.4 配置专线接入业务
专线接入一般用于需要同时接入多个用户，这些用户使用统一的认证计费、带宽控制、访问权限控制以及 QoS 控制。

3.5 配置和管理用户
BRAS 对用户的管理通过域和用户帐号实现。

3.6 配置 BoD 增值业务
BOD(Bandwidth on Demand)是一种动态分配带宽的业务。

3.7 维护
通过维护 BRAS 认证可以实现监控 BRAS 接入认证运行状况、实现清除接入用户上下线统计数据和出现故障时调试的目的。

3.8 配置举例
介绍 BRAS 接入认证的各种示例。配置示例中包括组网需求、配置注意事项和配置思路等。

3.1 简介

BRAS 接入认证通过用户报文的协议栈来区分用户，对应不同的用户，灵活地选择不同的认证方式。

3.1.1 BRAS 接入认证概述

在进行 BRAS 接入认证配置之前了解如 Web 认证、端口绑定认证、快速认证等基本概念，有助于快速和准确的完成 BRAS 接入认证配置。

用户物理接入方式的差异通常在接入设备上被屏蔽，NE20E-X6 也无需关心终端用户的接入方式。NE20E-X6 上可见用户报文的封装格式，并依据报文的协议栈来区分用户。

对于用户认证，目前存在以下几种认证方式：

- Web 认证：是指用户通过访问 Web 认证服务器的认证页面，交互输入用户名和密码进行身份认证的一种认证方法。
- 快速认证：一种简化的 Web 认证方法，是指用户访问 Web 页面，但是无需输入用户名和密码，直接提交认证，由设备根据用户接入的 BAS（Broadband Access Server）接口信息自动生成用户名和密码（vlan）进行认证。
- 强制 Web 认证：是指当需要 Web 认证或快速认证的用户，在未认证前试图访问其无权访问的地址时，NE20E-X6 将其访问请求强制重定向到强制 Web 认证服务器，让用户进行认证。
- 绑定认证：是指 NE20E-X6 根据用户接入的位置信息自动生成用户名和密码进行认证。

3.1.2 NE20E-X6 支持的接入认证特性

NE20E-X6 支持的接入特性包括用户接入识别和用户认证方式。

NE20E-X6 支持个人用户、专线用户通过各种方式接入 Internet 网（有关个人用户的介绍请参见《HUAWEI NetEngine20E-X6 高端业务路由器 特性描述-BRAS 业务》）。这些接入用户的协议栈分为以下几类：

- IPoX（IPoE、IPoEoVLAN、IPoEoQ）

NE20E-X6 支持以下认证方式：

- Web 认证
- 快速认证
- 强制 Web 认证
- 绑定认证

3.2 配置认证方式

认证技术指用户终端与设备之间进行认证交互、提交用户名和密码的方法，NE20E-X6提供了多种认证技术。

3.2.1 建立配置任务
在进行认证方式配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

3.2.2 配置 Web 认证方式或快速认证方式
Web 认证是指用户通过访问 Web 认证服务器的认证页面，交互输入用户名和密码进行身份认证的一种认证方式。快速认证是指用户访问 Web 页面，但是无需输入用户名和密码，直接提交认证。

3.2.3 配置其他认证方式
用户认证不通过 web 页面，通过用户物理信息绑定认证等方式进行认证。

3.2.4 检查配置结果
完成认证方式的配置后，您可以通过查看域配置信息获知认证方式。

3.2.1 建立配置任务

在进行认证方式配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

Web 认证是指用户通过访问 Web 认证服务器的认证页面，交互输入用户名和密码进行身份认证的一种认证方法。

Web 认证还有一种简化的方法，称为快速认证，是指用户访问 Web 页面，但是无需输入用户名和密码，直接提交认证，由 NE20E-X6 根据用户接入的 BAS（Broadband Access Server）接口信息自动生成用户名和密码（vlan）进行认证。

绑定认证是指 NE20E-X6 根据用户接入的位置信息自动生成用户名和密码进行认证。

前置任务

在配置认证方式之前，需要完成以下任务：

- 加载 BRAS License，请参见《HUAWEI NetEngine20E-X6 高端业务路由器 配置指南-系统管理》。
- 配置 ACL（针对 Web 认证）。

数据准备

在配置认证方式之前，请根据网络规划，准备好以下数据。

序号	数据
1	Web 认证服务器的 IP 地址、端口号、所属的 VPN 实例、共享密钥
2	Portal 协议版本号、NE20E-X6 的侦听端口号、源接口

序号	数据
3	是否透传 RADIUS 认证结果消息给 Web 认证服务器
4	BAS 接口下 Web 认证用户的认证前缺省域
5	（可选）是否使用强制 Web 认证

3.2.2 配置 Web 认证方式或快速认证方式

Web 认证是指用户通过访问 Web 认证服务器的认证页面，交互输入用户名和密码进行身份认证的一种认证方式。快速认证是指用户访问 Web 页面，但是无需输入用户名和密码，直接提交认证。

背景信息

配置 Web 认证方式或快速认证方式包括以下参数：

- 服务器的 IP 地址以及所属的 VPN 实例
- 服务器的端口号
- 服务器的共享密钥
- NE20E-X6 是否向服务器上报自己的 IP 地址
- 配置 Portal 协议时的 Portal 版本号、侦听端口号、发送报文的源接口
- 强制重定向的页面

请在 NE20E-X6 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 （可选）执行命令 **web-auth-server version v2**，设置 Portal 版本号。

- 或执行命令 **web-auth-server listening-port** *port*，配置 NE20E-X6 的侦听端口号。缺省情况下，NE20E-X6 使用端口 2000 侦听 Web 认证服务器的消息。
- 或执行命令 **web-auth-server source interface** *interface-type interface-number*，配置 NE20E-X6 发送报文的源接口。缺省情况下，NE20E-X6 中未配置发送 Portal 报文的源接口，即直接使用报文出接口的 IP 地址作为源 IP 地址。
- 或执行命令 **web-auth-server reply-message**，配置透传 RADIUS 消息。缺省情况下，NE20E-X6 透传 RADIUS 消息给 Web 认证服务器。

步骤 3 执行命令 **web-auth-server** *ip-address* [**vpn-instance** *instance-name*] [**port** *port-number*] [**key** *key-string*] [**nas-ip-address**]，配置 Web 认证服务器。

缺省情况下，NE20E-X6 中未配置 Web 认证服务器。配置 Web 认证服务器后，缺省的端口号为 50100、共享密钥为空、NE20E-X6 不向 Web 认证服务器上报 IP 地址。

步骤 4 （可选）执行命令 **aaa**，进入 AAA 视图。

步骤 5 （可选）执行命令 **domain** *domain-name*，进入域视图（认证前缺省域）。

步骤 6 （可选）执行命令 **web-server** { **url** *url* | *ip-address* | **mode** { **get** | **post** } | **redirect-key** { **mscg-ip** *mscg-ip-key* | **mscg-name** *mscg-name* | **user-ip-address** *user-ip-key* | **user-location** *user-*

location-key } | **user-first-url-key** { *key-name* | **default-name** } | **url-parameter** }，配置强制Web认证服务器。

强制重定向的 URL 的形式为“http://www.isp.com/index.htm”。NE20E-X6 支持两种 HTTP 页面访问模式，即 get 和 post 模式。两者模式分别规定了不同的 NE20E-X6 与 HTTP 页面交互的报文格式。

步骤 7 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 8 执行命令 **bas**，进入 BAS 接口视图。

步骤 9 执行命令 **access-type layer2-subscriber**，设置用户接入类型为二层用户。

步骤 10 执行命令 **default-domain pre-authentication** *domain-name*，指定认证前缺省域。

缺省情况下，BAS 接口下的认证前缺省域为 default0。

步骤 11 执行命令 **default-domain authentication** [**force** | **replace**] *domain-name*，指定认证时缺省域。

缺省情况下，BAS 接口下的认证时缺省域为 default1。

步骤 12 执行命令 **authentication-method** { **web** | **fast** }，配置 Web 认证方式或快速认证方式。

----结束

3.2.3 配置其他认证方式

用户认证不通过 web 页面，通过用户物理信息绑定认证等方式进行认证。

背景信息

请在 NE20E-X6 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **bas**，进入 BAS 接口视图。

步骤 4 执行命令 **access-type layer2-subscriber**，设置用户接入类型为二层用户。

步骤 5 执行命令 **default-domain pre-authentication** *domain-name*，指定认证前缺省域。

缺省情况下，BAS 接口下的认证前缺省域为 default0。

步骤 6 执行命令 **default-domain authentication** [**force** | **replace**] *domain-name*，指定认证时缺省域。

缺省情况下，BAS 接口下的认证时缺省域为 default1。

步骤 7 执行命令 **authentication-method** ，配置绑定认证方式。

只有接入用户类型为二层用户的 BAS 接口可以设置其认证方法。各种认证方法可以组合使用，但有以下的约束关系：

- Web 认证和快速认证互斥；

- 绑定认证和其他认证方式都互斥。

----结束

3.2.4 检查配置结果

完成认证方式的配置后，您可以通过查看域配置信息获知认证方式。

操作步骤

- 使用 **display web-auth-server configuration** 命令，查看 Web 服务器的配置信息。
- 使用 **display domain** [*domain-name*]命令，查看域的配置信息。

----结束

任务示例

配置完成后，执行命令 **display web-auth-server configuration** 命令可以查看 Web 服务器的配置信息，例如：

```
<HUAWEI> display web-auth-server configuration
  Source interface      : -
  Listening port        : 2000
  Portal                : version 1, version 2
  Display reply message : enabled
  ------------------------------------------------------------------------------
           Server  Share-Password     Port  NAS-IP  Vpn-instance
  ------------------------------------------------------------------------------
    192.168.3.140  huawei            50100   NO
  ------------------------------------------------------------------------------
  1 Web authentication server(s) in total
```

配置完成后，执行命令 **display domain** *domain-name* 可以查看域与用户组的绑定信息，例如：

```
<HUAWEI> display domain isp1
  Domain-name                    : isp1
  Domain-state                   : Active
  Domain-type                    : Normal domain
  Service-type                   : HSI
  Authentication-scheme-name     : default1
  Accounting-scheme-name         : default1
  Authorization-scheme-name      : -
  RADIUS-server-group            : -
  Accounting-copy-RADIUS-group   : -
  Hwtacacs-server-template       : -
  Tunnel-acct-2867               : Disabled
  User-group-name                : -
  Policy-route                   : Disabled
  Policy-route-nexthop           : -
  AdminUser-priority             : -
  Web-server-IP-address          : -
  Web-URL                        : -
  Web-server-work-mode           : Get
  Primary dns-IP-address         : -
  Secondary dns-IP-address       : -
  Queue-profile-name             : -
  User-priority-up               : 0
  User-priority-down             : 0
  PPPoe-URL                      : Disabled
  Portal-server-URL              : -
  Portal-server-IP-Address       : -
  Portal-force-times             : 2
  Quota-out                      : Offline
```

```
Force-Auth-Type                 : -
Idle-data-attribute (time,rate) : 3 minute, 100 Kbyte/minute
User-access-limit               : 147456
Online-user-total               : 0
User-session-limit              : -
Flow-Statistic-Up               : Yes
Flow-Statistic-Down             : Yes
Time-range                      : Disabled
GRE-group-name                  : -
L2TP-group-name                 : -
L2TP-user RADIUS Force          : Disabled
Dot1x-template-index            : 1
Realloc-IP-address              : Disabled
Bill Flow                       : Disabled
Multicast flow statistic        : Disabled
VPN-instance-name               : --
Value-service-name              : -
DPI-policy-group                : -
Multicast-profile               : -
IPUser-ReAuth-Time              : 300 second
IP-Warning-Percent              : -
Qos-profile-name                : default
Zone-name                       : -
Ancp auto qos adapt             : Disabled
TimeRange-Qos                   : Disabled
Val-added-srv-account           : Default
Multicast Forwarding            : Yes
Multicast Virtual               : No
Multivirtual cir                : -
Multivirtual pir                : -
Max-multilist num               : 4
L2TP-QosProfile-inbind          : -
L2TP-QosProfile-outbind         : -
```

3.3 配置 IPoX 接入业务

IPoX 接入方式下，接入用户只需通过报文触发的方式接入 Internet，无需安装客户端拨号软件、无需拨号。

3.3.1 建立配置任务
在配置 IPoX 接入之前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

3.3.2 创建静态用户
当用户需要固定 IP 地址时，可以配置其为静态用户。

3.3.3 配置子接口下绑定 VLAN
当设备接入的用户报文携带 VLAN 标签时，对不同的用户有不同的处理方式，确保此类报文能够正确被转发。

3.3.4 配置 BAS 接口
当某个接口用于接入宽带用户时，需要将该接口配置为 BAS 接口，并指定该接口的用户接入类型及相关属性。

3.3.5 检查配置结果
用户通过相应的 display 命令，可以查看已经配置的 IPoX 接入相关信息。

3.3.1 建立配置任务

在配置 IPoX 接入之前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

IPoX 接入业务是一种接入认证业务。在普通 IPoX 接入业务中，用户通过以太网、ADSL 等方式接入，通过配置固定 IP 地址或者 DHCP 方式动态获取 IP 地址，通过 Web 认证、快速认证或绑定认证方法进行身份验证。

根据组网方式的不同，普通 IPoX 接入业务可以分为 IPoE、IPoEoVLAN、IPoEoQ。

说明

IPoE 用户使用动态 QinQ 接入时，IPoEoQ 用户上线 MAC 地址与 chaddr 地址不同,用户无法上线。

前置任务

在配置普通 IPoX 接入业务之前，需要完成以下任务：

- 加载 BRAS License，请参见《HUAWEI NetEngine20E-X6 高端业务路由器 配置指南-系统管理》。
- 配置 AAA 方案。
- 配置服务器模板。
- 配置 IPv4 地址池。
- 配置域。

数据准备

在配置普通 IPoX 接入业务之前，请根据网络规划，准备好以下数据。

序号	数据
1	（可选）静态用户所属域的名称
2	静态用户的 IP 地址、所属 VPN 实例（可选）、MAC 地址（可选）、接入 NE20E-X6 的接口号（可选）
3	使用的认证方案、计费方案、授权方案（针对 HWTACACS 服务器）名称
4	使用的 RADIUS 服务器组或 HWTACACS 服务器模板名称
5	使用的 IPv4 地址池名称
6	用户所在域
7	（可选）Web 认证服务器的相关参数
8	用户侧 VLAN（仅对 IPoEoVLAN、IPoEoQ 接入）
9	BAS 接口的相关参数

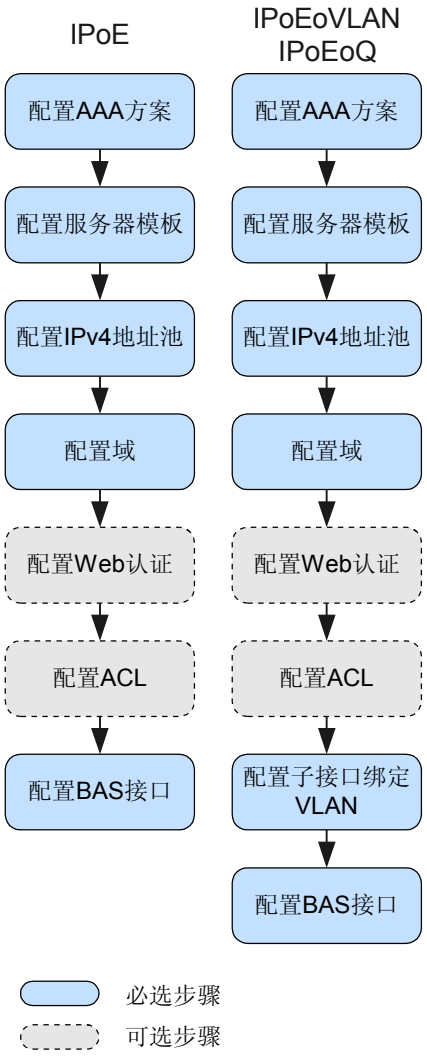
配置过程

要完成配置普通 IPoX 接入业务的任务，需要执行如下的配置过程。

说明

“**配置 AAA 方案**”，“**配置 RADIUS 服务器组**”，“**配置 IPv4 地址池**“，“**配置域**“，在其它章节已说明，这里不再重复。

图 3-1 IPoX 配置过程



3.3.2 创建静态用户

当用户需要固定 IP 地址时，可以配置其为静态用户。

背景信息

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **static-user** *start-ip-address* [*end-ip-address*] **gateway** *ip-address* [**vpn-instance** *instance-name*] [**domain-name** *domain-name* | **interface** *interface-type interface-number* [**vlan** *vlan-id* [**qinq** *qinq-vlan*] | **pvc** *vpi/vci*] | **mac-address** *mac-address* | **detect**] *，创建静态用户。

创建静态用户时，可以指定其 IP 地址（可设置 IP 地址所属的 VPN 实例）、接入 NE20E-X6 的接口（只能是 FE、GE、Eth-Trunk、VE 接口）、所属的域、MAC 地址。

detect 参数表示 NE20E-X6 主动探测静态用户是否在线，如果不配置该参数，则需要用户计算机发送 ARP 报文才能触发上线。

缺省情况下，NE20E-X6 中未创建静态用户。

----结束

3.3.3 配置子接口下绑定 VLAN

当设备接入的用户报文携带 VLAN 标签时，对不同的用户有不同的处理方式，确保此类报文能够正确被转发。

背景信息

对于从子接口接入的用户，需要在子接口下绑定 VLAN。

子接口可以绑定 VLAN 或 QinQ，配置子接口绑定 VLAN 包括以下参数：

- 子接口的编号
- VLAN ID
- QinQ ID

说明

- 每个主接口下只允许配置一个 any-other 子接口。同一个子接口下 **any-other** 不能与 *start-vlan* 或 **qinq** 同时配置。
- 子接口上已经配置了 dot1q 终结或 QinQ 终结或 qinq stacking 或 vlan-type dot1q，则不能再配置 **user-vlan** 命令。
- 不同的子接口下不能配置 VLAN ID 相同的 user-vlan。

请在 NE20E-X6 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number.subinterface-number*，创建并进入子接口视图。

步骤 3 当用户接入类型为二层普通用户接入时：执行命令 **user-vlan** { *start-vlan* [*end-vlan*] [**qinq** *start-qinq-id* [*end-qinq-id*]] | **any-other** }，创建用户侧 VLAN。

当用户接入类型为三层普通用户接入时：执行命令 **dot1q** *vlan-id*，创建用户侧 VLAN。

----结束

3.3.4 配置 BAS 接口

当某个接口用于接入宽带用户时，需要将该接口配置为 BAS 接口，并指定该接口的用户接入类型及相关属性。

背景信息

配置 BAS 接口包括以下参数：

- BAS 接口的编号

- 用户的接入类型和认证方法
- （可选）BAS 接口接入的最大用户数、指定 VLAN 接入的最大用户数
- （可选）BAS 接口的缺省域、漫游域和允许用户接入的域
- （可选）是否启用 ARP 代理功能、DHCP 广播功能、计费报文抄送功能、IP 报文触发上线功能、按用户复制组播报文功能功能
- （可选）是否信任客户端上报的 DHCP Option82 信息、用户探测参数、非 PPP 用户所属的 VPN 实例、BAS 接口名字、接入设备的类型

请在 NE20E-X6 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number* [*.subinterface-number*]，进入接口视图。

步骤 3 执行命令 **bas**，创建 BAS 接口并进入 BAS 接口视图。

当在一个接口视图下执行 **bas** 命令时，可以将该接口设置为 BAS 接口。可以设置为 BAS 接口的接口类型包括以太接口、Eth-Trunk 接口以及这些接口的子接口。

步骤 4 执行命令 **access-type layer2-subscriber** [**default-domain** { [**authentication** [**force** | **replace**] *dname*] [**pre-authentication** *predname*] }]，配置二层普通用户接入类型及相关属性。

或执行命令 **access-type layer3-subscriber** [**default-domain** { [**pre-authentication** *predname*] **authentication** [**force** | **replace**] *dname* }]，配置三层普通用户接入类型及相关属性。

在设置 BAS 接口的用户接入类型时，还可以一起设置和该种用户类型相关的业务属性，这些属性也可以在后续的配置中逐项配置。

在配置三层普通用户时，可以在系统视图下执行命令 **layer3-subscriber** *start-ip-address end-ip-address* [**vpn-instance** *instance-name*] **domain-name** *domain-name* 指定所在 IP 地址段以及相关联的认证域的域名。

对于已经被 Eth-Trunk 接口包含的以太网接口，不能配置其用户接入类型，而只能在相应的 Eth-Trunk 接口下配置用户接入类型。

步骤 5 （可选）执行命令 **access-limit** *number*，设置接口级用户数限制。

缺省情况下，BAS 接口未设置用户数限制。

步骤 6 （可选）执行命令 **default-domain pre-authentication** *domain-name*，指定认证前缺省域。缺省情况下，BAS 接口的认证前缺省域为 default0。

- 或执行命令 **default-domain authentication** [**force** | **replace**] *domain-name*，指定认证缺省域。缺省情况下，BAS 接口的认证缺省域为 default1。
- 或执行命令 **permit-domain** *domain-name* &<1->，指定允许接入的域。缺省情况下，BAS 接口的未设置允许接入的域，所有的域都可以接入。

步骤 7 （可选）执行命令 **client-option82** [**basinfo-insert cn-telecom**]，配置路由器信任客户端上报的 Option82 信息。缺省情况下，路由器不信任客户端上报的 Option82 信息。

或执行命令 **vbas**，启用 VBAS（Virtual BAS）方式的用户定位功能。缺省情况下，系统不启用 VBAS 方式的用户定位功能。

步骤 8 （可选）执行命令 **client-option60**，配置路由器信任客户端上报的 Option60 信息。缺省情况下，路由器不信任客户端上报的 Option60 信息。

如果从 option60 获取用户域，在 option60 字符串中选择域名分割符（默认@）后面的所有字符串做域名，如果没有寻找到用户域则按照下面顺序继续寻找，如果没有域名分隔符按照配置的模糊还是精确的方式进行匹配。如果获取到用户域信息，流程不再往下进行。

1. BAS 接口下配置的 **client-option60**
2. BAS 接口下配置了业务识别策略，业务识别策略视图下配置了 **service-identify dhcp-option60**，匹配方式按照命令 **option60 partial-match** 确定是精确匹配还是部分匹配。
3. 系统视图下配置的 **dhcp option-60**
4. 如果是静态用户，命令 **static-user** *start-ip-address* [*end-ip-address*] **gateway** *ip-address* [**vpn-instance** *instance-name*] [**domain-name** *domain-name*]配置的静态用户所属域。
5. BAS 接口配置的认证域

步骤 9 （可选）执行命令 **accounting-copy radius-server** *radius-name*，启用计费报文抄送功能。缺省情况下，BAS 接口的计费报文抄送功能关闭。

步骤 10 执行命令 **ip-trigger**，启用 IP 报文触发上线功能。缺省情况下，BAS 接口的 IP 报文触发上线功能关闭。

或执行命令 **arp-trigger**，启用 ARP 报文触发上线功能。缺省情况下，BAS 接口的 ARP 报文触发上线功能关闭。

步骤 11 （可选）执行命令 **user detect retransmit** *number* **interval** *time*，设置用户探测参数。缺省情况下，用户探测的次数为 5，时间间隔为 30 秒。

步骤 12 （可选）执行命令 **block**，设置 BAS 接口的阻塞状态。

步骤 13 （可选）执行命令 **dhcp-forcerenew**，配置强制 renew 使能，强制 renew 报文的重传延时和次数。

该功能应用在用户异常掉线的情况下，用于触发客户端重新申请地址。

----结束

3.3.5 检查配置结果

用户通过相应的 display 命令，可以查看已经配置的 IPoX 接入相关信息。

操作步骤

- 使用 **display web-auth-server configuration** 命令，查看 Web 服务器的配置信息。
- 使用 **display domain** 命令，查看域的配置信息。
- 使用 **display acl** 命令，查看 ACL 的配置信息。

----结束

任务示例

配置完成后，执行命令 **display web-auth-server configuration** 命令可以查看 Web 服务器的配置信息，例如：

```
<HUAWEI> display web-auth-server configuration
  Source interface      : -
  Listening port        : 2000
  Portal                : version 1, version 2
  Display reply message : enabled
  ------------------------------------------------------------------------------
           Server  Share-Password     Port  NAS-IP  Vpn-instance
  ------------------------------------------------------------------------------
    192.168.3.140  huawei            50100   NO
  ------------------------------------------------------------------------------
  1 Web authentication server(s) in total
```

配置完成后，执行命令 **display domain** 可以查看域与用户组的绑定信息，例如：

```
<HUAWEI> display domain isp1
  Domain-name                     : isp1
  Domain-state                    : Active
  Domain-type                     : Normal domain
  Authentication-scheme-name      : default1
  Accounting-scheme-name          : default1
  Authorization-scheme-name       : -
  RADIUS-server-group             : -
  Accounting-copy-RADIUS-group    : -
  Hwtacacs-server-template        : -
  Tunnel-acct-2867                : Disabled
  User-group-name                 : -
  Policy-route                    : Disabled
  Policy-route-nexthop            : -
  AdminUser-priority              : -
  Web-server-IP-address           : -
  Web-URL                         : -
  Web-server-work-mode            : Get
  Primary dns-IP-address          : -
  Secondary dns-IP-address        : -
  Queue-profile-name              : -
  User-priority-up                : 0
  User-priority-down              : 0
  PPPoe-URL                       : Disabled
  Portal-server-URL               : -
  Portal-server-IP-Address        : -
  Portal-force-times              : 2
  Quota-out                       : Offline
  Force-Auth-Type                 : -
  Idle-data-attribute (time,rate) : 3 minute, 100 Kbyte/minute
  User-access-limit               : 147456
  Online-user-total               : 0
  User-session-limit              : -
  Flow-Statistic-Up               : Yes
  Flow-Statistic-Down             : Yes
  Time-range                      : Disabled
  GRE-group-name                  : -
  L2TP-group-name                 : -
  L2TP-user RADIUS Force          : Disabled
  Dot1x-template-index            : 1
  Realloc-IP-address              : Disabled
  Bill Flow                       : Disabled
  Multicast flow statistic        : Disabled
  VPN-instance-name               : --
  Value-service-name              : -
  DPI-policy-group                : -
  Multicast-profile               : -
  IPUser-ReAuth-Time              : 300 second
  IP-Warning-Percent              : -
  Qos-profile-name                : default
```

```
  Zone-name                      : -
  Ancp auto qos adapt            : Disabled
  TimeRange-Qos                  : Disabled
  Val-added-srv-account          : Default
  Multicast Forwarding           : Yes
  Multicast Virtual              : No
  Multivirtual cir               : -
  Multivirtual pir               : -
  Max-multilist num              : 4
  L2TP-QosProfile-inbind         : -
  L2TP-QosProfile-outbind        : -
```

配置完成后，执行命令 **display acl** 命令可以查看 ACL 的配置信息，例如：

```
<HUAWEI> display acl 3100
Advanced ACL  3100, 3 rules,
 rule 0 permit icmp (2 times matched)
 rule 1 permit ip source 1.1.1.1 0 destination 2.2.2.2 0 (0 times matched)
 rule 2 permit tcp source 10.110.0.0 0.0.255.255 (0 times matched)
```

3.4 配置专线接入业务

专线接入一般用于需要同时接入多个用户，这些用户使用统一的认证计费、带宽控制、访问权限控制以及 QoS 控制。

3.4.1 建立配置任务
在进行专线接入业务配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

3.4.2 配置用户侧 VLAN
当设备接入的用户报文携带 VLAN 标签时，对不同的专线用户有不同的处理方式，确保此类报文能够正确被转发。

3.4.3 配置 BAS 接口
当某个接口用于接入宽带用户时，需要将该接口配置为 BAS 接口，并指定该接口的用户接入类型及相关属性。

3.4.4 检查配置结果
完成专线接入业务的配置后，您可以通过查看到 BAS 接口的信息检查专线接入业务的配置。

3.4.1 建立配置任务

在进行专线接入业务配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

专线（Leased Line）接入业务是指将 NE20E-X6 的某个以太网接口或者接口下的某些 VLAN 整体出租给一组用户使用的业务。一条专线下可以接入多台计算机，但是在 NE20E-X6 上只表现为一个用户，NE20E-X6 对专线进行统一的认证计费、带宽控制、访问权限控制以及 QoS 控制。

根据专线接入业务的组网方式以及业务的处理方式，专线可以分为二层 VPN 专线，二层专线、三层专线。

二层专线，三层专线，二层 VPN 专线默认做 CAR，cir 为 128kbps，pir 为 1000000kbps，cbs 为 23936bytes，pbs 为 18700000bytes。

前置任务

在配置专线接入业务之前，需要完成以下任务：

- 加载 BRAS License，请参见《HUAWEI NetEngine20E-X6 高端业务路由器 配置指南-系统管理》
- 配置 AAA 方案
- 配置服务器模板
- 配置 IPv4 地址池（二层专线）
- 配置域

数据准备

在配置专线接入业务之前，请根据网络规划，准备好以下数据。

序号	数据
1	使用的认证方案、计费方案、授权方案（仅对 HWTACACS 授权）名称
2	使用的 RADIUS 服务器组或 HWTACACS 服务器模板名称
3	使用的 IPv4 地址池名称（只对二层专线需要）
4	用户所在域
5	用户侧 VLAN（仅对以太网子接口下的专线接入）
6	BAS 接口的相关参数
7	专线的用户名和密码
8	用户网段地址（只对三层专线需要）

3.4.2 配置用户侧 VLAN

当设备接入的用户报文携带 VLAN 标签时，对不同的专线用户有不同的处理方式，确保此类报文能够正确被转发。

背景信息

配置用户侧 VLAN 包括以下参数：

- 子接口的编号
- 用户侧 VLAN 的编号
- QinQ VLAN 的编号（可选）

说明

此配置仅适用于以太网子接口下的专线接入方式。

请在 NE20E-X6 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 （针对三层专线接入）执行命令 **interface** *interface-type interface-number*，进入接收用户报文的以太网主接口视图。

步骤 3 （针对三层专线接入）执行命令 **mode user-termination**，配置接口模式为用户终结模式。

在主接口下使用该命令时，需要保证该主接口下没有配置子接口。

步骤 4 执行命令 **interface** *interface-type sub-interface-number*，进入子接口视图。

步骤 5 （针对非三层专线接入）执行命令 **user-vlan** { *start-vlan* [*end-vlan*] [**qinq** *start-qinq-id* [*end-qinq-id*]] | **any-other** }，创建用户侧 VLAN。

步骤 6 （针对三层专线接入）执行命令 **control-vid** *vid* **dot1q-termination** [**rt-protocol**]，配置控制 VLAN 与 Dot1q 终结子接口之间的对应关系。

或执行命令 **control-vid** *vid* **qinq-termination** [**dynamic** [**rt-protocol**] | **local-switch** | **rt-protocol** [**dynamic**]]，配置控制 VLAN 与 QinQ 终结子接口之间的对应关系。

步骤 7 （针对三层专线接入）执行命令 **dot1q termination vid** *low-pe-vid* [**to** *high-pe-vid*] { **8021p** { *8021p-value1* [**to** *8021p-value2*] } &<1-10> | **dscp** { *dscp-value1* [**to** *dscp-value2*] } &<1-10> | **eth-type** *eth-type-value* | **default** } [**vlan-group** *group-id*]，配置一层 Tag 报文终结功能。

当子接口需要终结接收到的带有一层 Tag 的用户报文时，需要在子接口上使用 **dot1q termination vid** 命令配置。配置后，接收的用户报文的 Tag 值应该在命令中指定的 pe-vid 值的范围内。

或执行命令 **qinq termination pe-vid** *pe-vid* **ce-vid** { *low-ce-vid* [**to** *high-ce-vid*] | **any** } [**vlan-group** *group-id*]，配置两层 Tag 报文终结功能。

当子接口需要终结接收到的带有两层 Tag 的用户报文时，需要在子接口上使用 **qinq termination pe-vid** 命令配置。配置后，用户报文的外层 Tag 应该为命令中指定的 PE 的 VLAN ID 值；内层 Tag 应该在命令中指定的 CE 的 VLAN ID 指定的范围之内。

----结束

3.4.3 配置 BAS 接口

当某个接口用于接入宽带用户时，需要将该接口配置为 BAS 接口，并指定该接口的用户接入类型及相关属性。

背景信息

配置 BAS 接口包括以下参数：

- BAS 接口的编号
- 用户的接入类型和认证方法
- （可选）BAS 接口接入的最大用户数、指定 VLAN 接入的最大用户数
- （可选）BAS 接口的缺省域、漫游域和允许用户接入的域
- （可选）是否启用 ARP 代理功能、DHCP 广播功能、计费报文抄送功能、IP 报文触发上线功能、按用户复制组播报文功能

- （可选）是否信任客户端上报的 DHCP Option82 信息、用户探测参数、非 PPP 用户所属的 VPN 实例、BAS 接口名字、接入设备的类型

请在 NE20E-X6 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number* [*.subinterface-number*]，进入接口视图。

步骤 3 执行命令 **bas**，创建 BAS 接口并进入 BAS 接口视图。

当在一个接口视图下执行 **bas** 命令时，可以将该接口设置为 BAS 接口。可以设置为 BAS 接口的接口类型包括 FE（Ethernet）接口、GE（GigabitEthernet）接口、VE 接口、Eth-Trunk 接口以及这些接口的子接口。

步骤 4 执行命令 **access-type l2vpn-leased-line user-name** *uname* **password** { **cipher** | **simple** } *password* [**default-domain authentication** *dname*]，配置二层 VPN 专线用户接入类型及相关属性。

- 或执行命令 **access-type layer2-leased-line user-name** *uname* **password** { **cipher** | **simple** } *password* [**default-domain authentication** *dname*]，配置二层专线用户接入类型及相关属性。
- 或执行命令 **access-type layer3-leased-line user-name** *uname* **password** { **cipher** | **simple** } *password* [**default-domain authentication** *dname*]，配置三层专线用户接入类型及相关属性。

在设置 BAS 接口的用户接入类型时，还可以一起设置和该种用户类型相关的业务属性。

对于已经被 Eth-Trunk 接口包含的以太网接口，不能配置其用户接入类型，而只能在相应的 Eth-Trunk 接口下配置用户接入类型。

有用户在线时，只有当用户类型是专线用户时，可以在线修改 BAS 接口的用户接入类型，其他情况不能修改。

当用户类型配置为专线用户后，NE20E-X6 立即对该专线用户进行认证。

步骤 5（可选）执行命令 **access-limit** *number*，设置接口级用户数限制。

缺省情况下，BAS 接口未设置用户数限制。

步骤 6（可选）对于二层专线接入，执行命令 **ip-trigger**，启用 IP 报文触发上线功能。缺省情况下，BAS 接口的 IP 报文触发上线功能关闭。

或执行命令 **arp-trigger**，启用 ARP 报文触发上线功能。缺省情况下，BAS 接口的 ARP 报文触发上线功能关闭。

步骤 7（可选）对于二层专线接入，执行命令 **user detect retransmit** *number* **interval** *time*，设置用户探测参数。缺省情况下，用户探测的次数为 5，时间间隔为 30 秒。

步骤 8（可选）执行命令 **block**，设置 BAS 接口的阻塞状态。

----结束

3.4.4 检查配置结果

完成专线接入业务的配置后，您可以通过查看到 BAS 接口的信息检查专线接入业务的配置。

操作步骤

- 使用 **display bas-interface** 命令，查看 BAS 接口的配置信息。

----结束

任务示例

配置完成后，执行命令 **display bas-interface** 命令可以查看 BAS 接口的配置信息，例如：

```
<HUAWEI> display bas-interface
--------------------------------------------------------------------------------
    Interface              AccessIF-Identification-mode          user-num
--------------------------------------------------------------------------------
 GigabitEthernet2/0/1                   host                        0
 GigabitEthernet2/0/2                   none                        0
--------------------------------------------------------------------------------
Total 2 AccessIf is configured
```

3.5 配置和管理用户

BRAS 对用户的管理通过域和用户帐号实现。

3.5.1 建立配置任务
在进行配置和管理用户前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

3.5.2 配置用户名解析
域名与用户名之间位置以及先后关系可以灵活配置满足多种需要。

3.5.3 创建本地用户帐号
在 AAA 视图创建用户，可以携带域名，本地用户不带域名时缺省属于 default_admin 域。

3.5.4 配置用户名生成方式和密码
对于绑定认证用户、快速认证用户等用户上线，不需要输入用户名和密码，NE20E-X6 提供配置用户名生成方式和密码的功能。

3.5.5 配置本地用户的状态
本地用户分为激活态或者阻塞态，激活态用户可以进行认证、阻塞态用户则不能进行认证。

3.5.6 配置用户的接入限制
通过该配置可以控制用户连接数目。

3.5.7 切断在线用户的连接
NE20E-X6 提供了根据用户的 IP 地址、MAC 地址、接入端口、域等多种条件切断在线用户连接的功能。

3.5.8 配置用户上下线记录功能
通过用户上下线记录可以获知用户上下线原因和时间。

完成管理用户的配置后，可以查看到用户名生成方式、域解析相关配置。

3.5.1 建立配置任务

在进行配置和管理用户前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

NE20E-X6 支持根据域名分隔符和 realm 名分隔符解析出用户名和域名。利用该功能，系统能够根据需要对用户名和域名进行解析。

当用户已经在线时，管理员可以在 NE20E-X6 上对在线用户进行管理，包括查看在线用户和切断用户连接。

前置任务

在配置和管理用户之前，需要完成以下任务：

- 加载 License，请参见《HUAWEI NetEngine20E-X6 高端业务路由器 配置指南-系统管理》
- 配置 BAS 接口的接入方式和认证方法

数据准备

在配置和管理用户之前，请根据网络规划，准备好以下数据。

序号	数据
1	域名分隔符、位置、解析方向
2	（可选）realm 名分隔符、域名位置、解析方向
3	解析优先级
4	在线用户的用户名、域名、接口名或接口类型/接口编号、VLAN 号、IP 地址、IP 地址所在的地址池、所属的 VPN 实例、MAC 地址、用户 ID、所在的槽位号

3.5.2 配置用户名解析

域名与用户名之间位置以及先后关系可以灵活配置满足多种需要。

背景信息

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **domain-name-delimiter** *delimiter*，配置域名分隔符。

缺省情况下，域名分隔符为@。

步骤 4 执行命令 **domain-location** { **after-delimiter** | **before-delimiter** }，设置域名位置。

缺省情况下，域名的位置在域名分隔符后面。

步骤 5 执行命令 **domainname-parse-direction** { **left-to-right** | **right-to-left** }，设置域名解析方向。

缺省情况下，域名解析方向为从左到右。

步骤 6 （可选）执行命令 **realm-name-delimiter** *delimiter*，设置 realm 名分隔符。

缺省情况下，realm 名分隔符为空。

步骤 7 （可选）执行命令 **realm-location** { **after-delimiter** | **before-delimiter** }，配置 realm 域名位置。

缺省情况下，realm 域名在 realm 名分隔符前面。

步骤 8 （可选）执行命令 **realmname-parse-direction** { **left-to-right** | **right-to-left** }，设置 realm 名解析方向。

缺省情况下，realm 名解析方向为从左到右。

步骤 9 执行命令 **parse-priority** { **domain-first** | **realm-first** }，配置解析优先级。

如果解析优先级为 **domain-first**，则去除 realm 域名部分。

缺省情况下，系统解析优先级为 **domain-first**。

----结束

3.5.3 创建本地用户帐号

在 AAA 视图创建用户，可以携带域名，本地用户不带域名时缺省属于 default_admin 域。

背景信息

在网络接入路由器上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **local-user** *user-name* **password** { **simple** | **cipher** } *password*，创建本地用户帐号。

如果用户名中带@，则认为@前面的部分是用户名，后面部分是域名。如果没有@，则整个字符串为用户名，域名为 default_admin。

----结束

3.5.4 配置用户名生成方式和密码

对于绑定认证用户、快速认证用户等用户上线，不需要输入用户名和密码，NE20E-X6 提供配置用户名生成方式和密码的功能。

背景信息

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **default-user-name** [**template** *template-name*] **include** { **gateway-address** | **ip-address** | **mac-address** | **option12** | **option60** | **option61** | **option82** | **sysname** } *，配置根据用户连接请求报文中携带的相关信息生成 IPoX 用户的纯用户名的方式。

或执行命令 **vlanpvc-to-username** { **standard** | **turkey** | **version10** | **version20** }，配置原有 IPoX 用户的纯用名生成格式。缺省情况下，原有 IPoX 用户名的纯用户名生成格式为 **version20** 规定的格式。

步骤 4 执行命令 **default-password** { **cipher** *cipher-password* | **simple** *simple-password* }，配置 IPoX 用户的密码。

cipher 和 **simple** 的区别在于：

- 设置为 **cipher** 后，无论输入的是加密的密码，还是不加密的密码，配置文件中显示的密码是密文形式。
- 设置为 **simple** 后，配置文件中显示的密码为明文形式。

----结束

3.5.5 配置本地用户的状态

本地用户分为激活态或者阻塞态，激活态用户可以进行认证、阻塞态用户则不能进行认证。

背景信息

在网络接入路由器上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **local-user** *user-name* **state** { **active** | **block** }，配置本地用户的状态。

缺省情况下，本地用户的状态为激活态。

----结束

后续处理

对处于激活态和阻塞态用户的处理方式如下：

- 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。

3.5.6 配置用户的接入限制

通过该配置可以控制用户连接数目。

背景信息

在网络接入路由器上进行如下配置。

操作步骤

- 本地用户的接入限制
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **aaa**，进入 AAA 视图。
  3. 执行命令 **local-user** *user-name* **access-limit** *max-number*，配置本地用户的接入限制。

     缺省情况下，不限制指定用户名可建立的连接数目。
- DHCP 用户接入限制
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dhcp-user-slot-warning-threshold**，配置业务单板 DHCP 接入用户数告警的阈值，当单板 DHCP 接入用户数比例超过这个设定的阈值时，设备会发出告警。
  3. 执行命令 **dhcp-user-warning-threshold**，配置整机 DHCP 接入用户数告警的阈值，当 NE20E-X6 整机的 DHCP 接入用户数比例超过这个设定的阈值时，设备会发出告警。
  4. 执行命令 **dhcp_connection_chasten** *request-sessions request-period blocking-period*，配置 DHCP 接入用户限制。
     - 使用 **display dhcp chasten-number** 命令，查看被限制 DHCP 用户数目。
     - 使用 **display dhcp chasten-user** 命令，查看被限制用户的 MAC 地址。
     - 使用 **display dhcp connection-chasten** 命令查看当前系统限制的 DHCP 用户连接的配置信息。
     - 使用命令 **dhcp reset chasten-number** 命令清除已经限制用户总数的计数。
- 单板接入用户限制
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **slot-warning-threshold**，配置单板接入用户数告警的阈值，当单板接入用户数比例超过这个设定的阈值时，设备会发出告警。

----结束

3.5.7 切断在线用户的连接

NE20E-X6 提供了根据用户的 IP 地址、MAC 地址、接入端口、域等多种条件切断在线用户连接的功能。

背景信息

请在路由器上进行以下操作。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **cut access-user username** *user-name* { **all** | **hwtacacs** | **local** | **none**| **radius** }，按用户名切断在线用户。

或执行命令 **cut access-user domain** *domain-name*，按域名切断在线用户。

或执行命令 **cut access-user mac-address** *mac-address*，按 MAC 地址切断在线用户。

或执行命令 **cut access-user ipv6-address** *ipv6-address* [**vpn-instance** *instance-name*]，按 IPv6 地址切断在线用户。

或执行命令 **cut access-user ip-address** *ip-address* [**vpn-instance** *instance-name*]，按 IP 地址切断在线用户。

或执行命令 **cut access-user interface** *interface-type interface-number* [**pevlan** *vlan-id*] [**cevlan** *vlan-id*]，按接口切断在线用户。

或执行命令 **cut access-user user-id** *start-no* [*end-no*]，按用户 ID 切断在线用户。

或执行命令 **cut access-user ip-pool** *pool-name*，按 IP 地址池切断在线用户。

或执行命令 **cut access-user slot** *slot-id*，切断指定槽号的单板上的所有用户连接。

----结束

3.5.8 配置用户上下线记录功能

通过用户上下线记录可以获知用户上下线原因和时间。

背景信息

在路由器上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa offline-record**，使能产生用户下线记录的功能。

缺省情况下，产生用户下线记录。

步骤 3 执行命令 **aaa online-fail-record**，使能产生用户上线失败记录的功能。

缺省情况下，产生用户上线失败记录。

步骤 4 执行命令 **aaa_abnormal-offline-record**，使能产生用户异常下线记录。

缺省情况下，系统会生成用户异常下线记录。

----结束

3.5.9 配置用户业务跟踪功能

操作步骤

步骤 1 执行命令 **trace access-user object** *object-id* { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address* | **ce-vlan** *ce-vlan-id* | **pe-vlan** *pe-vlan-id* } * [**output** [**file** *file-name* | **syslog-server** *ip-address* | **vty**] | [**-t** *time*]] *，使能用户业务跟踪功能。

缺省情况下，使能用户业务跟踪功能。跟踪信息向 VTY 终端屏幕输出，对对象的跟踪时间为 15 分钟。

使用业务跟踪功能将使 NE20E-X6 的性能有一定程度的下降，因此建议只在需要进行问题定位时启用，正常情况下不开启该功能。如果在大量用户状态变化时使用此命令，请注意配置的跟踪对象尽可能的精确，避免消耗大量的设备资源，造成用户正常的业务无法开展。

----结束

3.5.10 检查配置结果

完成管理用户的配置后，可以查看到用户名生成方式、域解析相关配置。

操作步骤

- 使用 **display static-user** 命令，查看配置的静态用户信息。
- 使用 **display aaa configuration** 命令，查看域名解析相关的配置信息。
- 使用 **display vlanpvc-to-username** 命令，查看生成 IPoX 用户名版本格式的配置信息。
- 使用 **display call rate** 命令，查看各类用户的呼叫接通率。

----结束

任务示例

配置完成后，执行命令 **display static-user** 命令可以查看配置的静态用户信息，例如：

```
<HUAWEI> display static-user
--------------------------------------------------------------------------------
 Interface         VLAN-ID/PVC     IP-address       MAC-address       VPN
--------------------------------------------------------------------------------
 -                 -               10.10.10.2       -                 --
 GE1/0/2           -               10.10.10.5       -                 --
--------------------------------------------------------------------------------
 Total 2 item(s) matched
```

配置完成后，执行命令 **display aaa configuration** 命令可以查看域名解析相关的配置信息，例如：

```
<HUAWEI> display aaa configuration
------------------------------------------------------------------------------
AAA configuration information :
------------------------------------------------------------------------------
Parse Priority                   : Domain first
Domain Name Delimiter            : @
Domainname parse direction       : Left to right
Domainname location              : After-delimiter
Realm name delimiter             : -
Realmname parse direction        : Left to right
Realmname location               : Before-delimiter
Domain                : total: 1024  used: 7
Authentication-scheme : total: 32    used: 4
Authorization-scheme  : total: 16    used: 2
Accounting-scheme     : total: 128   used: 4
Recording-scheme      : total: 128   used: 1
AAA-access-user       : total: 279552 used: 0
Access-user-state     : authen: 0    author: 0    accounting: 0
Transition-step                  : -
Min-Delay-time                   : -
Max-Delay-time                   : -
Access speed                     : -
Account-session-id-version       : Version1
------------------------------------------------------------------------------
```

配置完成后，执行命令 **display vlanpvc-to-username** 可以查看生成 IPoX 用户名版本格式的配置信息，例如：

```
<HUAWEI> display vlanpvc-to-username
  Version of vlan and pvc model in username : Version2.0
```

配置完成后，执行命令 **display call rate** 查看各类用户的呼叫接通率，例如：

```
<HUAWEI> display call rate
 User callrate:
 ------------------------------------------------------------
 Usertype      Calltime      Callcompletion      Rate
 ------------------------------------------------------------
 PPP             127              127          100.00%
 Dot1X           324              324          100.00%
 Web/Fast        7                7            100.00%
 Bind            0                0            0.00%
 Total           458              458          100.00%
```

3.6 配置 BoD 增值业务

BOD(Bandwidth on Demand)是一种动态分配带宽的业务。

3.6.1 建立配置任务

在配置 BOD 增值业务之前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

3.6.2 配置 COPS 服务器源接口

当使用 COPS 服务器下发增值业务的业务策略时，需要在 NE20E-X6 上配置 COPS 服务器。并且必须配置 COPS 报文的源接口，COPS 连接才能建立。

3.6.3 （可选）配置 COPS Open 消息超时时间

在网络状态存在不稳定因素的情况下，建议适当延长 COPS Open 消息超时时间。

3.6.4 创建 COPS 服务器组

创建 COPS 服务器组包括配置 COPS 服务器的 IP 地址、服务器的端口号、客户端的端口号、服务器所属的 VPN 实例以及权重。

3.6.5 使能全局增值业务功能

3.6.1 建立配置任务

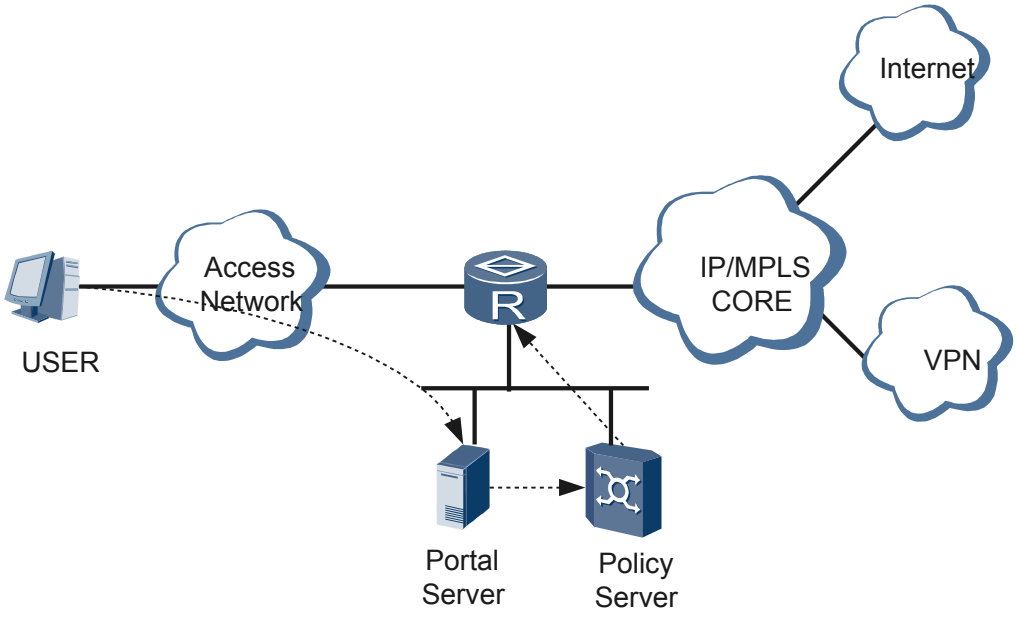
在配置 BOD 增值业务之前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

BOD(Bandwidth on Demand)是一种动态分配带宽的业务，在用户有带宽调整需求时，可以通过 Portal Server 自助选择 BOD 业务的动态激活和注销，不需要运营商通过更改配置完成带宽更改，同时也给运营商提供了更为灵活的基于业务的计费方式。

如图 3-2 所示，用户通过 Portal Server 请求带宽更改，Portal Server 将带宽参数传递给策略服务器，策略服务器给接入设备下发业务带宽，接入设备带宽参数生效，计费服务器根据新的带宽进行计费。

图 3-2 BOD 业务应用组网图



NE20E-X6 支持专线用户、二三层接入用户、二三层 VPN 用户的 BOD。

前置任务

在配置 BOD 增值业务之前，需完成以下任务：

- 配置认证、计费方案、RADIUS 服务器组

- 配置域，域下绑定认证、计费方案、地址池、RADIUS 服务器组
- 配置地址池
- 配置 BAS 接口

数据准备

在配置 BOD 增值业务之前，需要准备以下数据。

序号	数据
1	COPS 服务器组名称
2	COPS 服务器的 IP 地址、所属的 VPN 实例（可选）、服务器端口号、客户端端口号、权重
3	COPS 客户端的标识
4	（可选）COPS 客户端与服务器连接断开后流保持的时间
5	（可选）COPS 服务器的密钥
6	（可选）COPS Open 消息超时时间
7	设备与 COPS 服务器交互报文的源接口（根据需要选择全局的或 COPS 服务器组的源接口）
8	用户组名、用户域名
9	增值业务的计费方案

3.6.2 配置 COPS 服务器源接口

当使用 COPS 服务器下发增值业务的业务策略时，需要在 NE20E-X6 上配置 COPS 服务器。并且必须配置 COPS 报文的源接口，COPS 连接才能建立。

背景信息

请在路由器上进行以下配置。

说明

COPS 服务器源接口为设备与 COPS 服务器之间交互报文的接口。可根据需要选择配置全局的 COPS 服务器源接口或者 COPS 服务器组的源接口，但必须保证配置其中一个，否则设备与 COPS 服务器之间不能建立 COPS 连接。

设备在与 COPS 服务器交互 COPS 报文时，优先选取 COPS 服务器组的源接口，如果 COPS 服务器所在的 COPS 服务器组下没有配置源接口，则选取全局的 COPS 服务器源接口。

操作步骤

步骤 1 配置全局 COPS 服务器源接口

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 *interface-type interface-number*，配置发送 COPS 报文的源接口。

缺省情况下，系统未配置全局的 COPS 服务器源接口。

步骤 2 配置 COPS 服务器组的源接口

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 *group-name*，进入 COPS 服务器组视图。
3. 执行命令 *interface-type interface-number*，配置 COPS 服务器组的源接口。

   缺省情况下，COPS 服务器组下没有配置源接口。

----结束

3.6.3 （可选）配置 COPS Open 消息超时时间

在网络状态存在不稳定因素的情况下，建议适当延长 COPS Open 消息超时时间。

背景信息

请在路由器上进行以下配置。

说明

Open 消息超时时间是指设备向 COPS 服务器发送 Open 消息后，等待响应的超时时间。当设备在该时间内无法收到 COPS 服务器的响应时，设备将重发 Open 报文。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 *time*，配置 COPS Open 消息超时时间。

缺省情况下，Open 消息超时时间为 15 秒。

----结束

3.6.4 创建 COPS 服务器组

创建 COPS 服务器组包括配置 COPS 服务器的 IP 地址、服务器的端口号、客户端的端口号、服务器所属的 VPN 实例以及权重。

背景信息

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 *group-name* **client-type ssg**，创建 COPS 服务器组，并进入服务器组视图。

创建 COPS 服务器组后，进入 COPS 服务器组视图。如果 COPS 服务器组已经存在，则执行上述步骤直接进入 COPS 服务器组视图。

创建 COPS 服务器组时，必须指定该 COPS 服务器组的客户端类型，即指定客户端（路由器）是为开展何种业务而连接 COPS 服务器的。

步骤 3 执行命令 **cops-server** *ip-address* [*server-port* | **client-port** *client-port* | **vpn-instance** *vpn-instance-name* | **shared-key** *shared-key* | **weight** *value*] *，配置 COPS 服务器。

配置 COPS 服务器时，可以指定 COPS 服务端口号、服务器所属的 VPN 实例以及权重。

步骤 4 （可选）执行命令 **cops-server pep-id** *client-id*，配置 COPS 客户端标识。

步骤 5 （可选）执行命令 **cops-server flow-keeping-time** *time*，配置 COPS 服务器的流保持时间。

步骤 6 （可选）执行命令 **cops-server shared-key** *key-string*，配置 COPS 服务器的密钥。

密钥用于对 COPS 报文进行加密。在设备和 COPS 服务器上必须配置相同密钥。

步骤 7 执行命令 **active**，激活 COPS 服务器组中的所有服务器。

说明

只有当 COPS 服务器组为激活状态时，设备才会试图和 COPS 服务器建立连接。

----结束

3.6.5 使能全局增值业务功能

背景信息

请在路由器上进行以下配置。

说明

在配置 BOD 增值业务之前，必须在全局下使能增值业务。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **value-added-service enable**，配置使能全局增值业务。

----结束

3.6.6 配置域下绑定 COPS 服务器组

背景信息

请在路由器上进行以下配置。

说明

如果用户的接入类型支持配置 BOD 特性，那么在用户域下绑定 COPS 服务器组后，用户上下线的信息会上报给 COPS 服务器。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **domain** *domain-name*，进入域视图。

步骤 4 执行命令 **cops-server group** *group-name*，配置在域下绑定 COPS 服务器组。

----结束

3.6.7 配置增值业务计费方式

针对不同用户运营商可配置灵活的业务和资费政策。

背景信息

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **value-added-service accounting individual**，配置下发增值业务后，基本业务停止计费。

步骤 4 执行命令 **domain** *domain-name*，进入域视图。

步骤 5 执行命令 **value-added-service accounting** { **none** | **cops** | **radius** *template-name* }，配置增值业务的计费方式。

缺省情况下，对增值业务不计费。

----结束

3.6.8 配置用户组

背景信息

请在路由器上进行以下配置。

说明
增值业务必须有用户组才能生效。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **user-group** *group-name*，创建用户组。

步骤 3 执行命令 **aaa**，进入 AAA 视图。

步骤 4 执行命令 **domain** *domain-name*，进入域视图。

步骤 5 执行命令 **user-group** *group-name*，指定域所属的用户组。

----结束

3.6.9 检查配置结果

操作步骤

- 使用 **display cops-server configuration** [**group** *group-name*]命令，查看 COPS 服务器的配置信息。

- 使用 **display domain** [*domain-name*]命令，查看域的配置信息。

----结束

任务示例

配置完成后，执行命令 **display cops-server configuration** 可以查看接入用户的状态信息，例如：

```
<HUAWEI> display cops-server configuration group huawei
-- Cops group table display ------------------------------------------------
    Group index                 : 52
    Group name                  : huawei
    Client type                 : iptn
    Group up or down flag       : Down
    Group active state          : Inactive
    Secret key                  : huawei
    Flow keeping time (second)  : 300
    PEP ID                      : huawei
[state][server IPv4 addr][server port][client port][weight][vpn name]
-- End cops group table ----------------------------------------------------
```

3.7 维护

通过维护 BRAS 认证可以实现监控 BRAS 接入认证运行状况、实现清除接入用户上下线统计数据和出现故障时调试的目的。

3.7.1 显示 BRAS 接入运行信息
查看 BRAS 接入的运行信息包括查看用户上下线记录信息和相关配置信息。

3.7.2 清除 BRAS 接入运行信息
如果用户上下线记录信息太多，可以清除 BRAS 接入运行信息再进行查看。

3.7.1 显示 BRAS 接入运行信息

查看 BRAS 接入的运行信息包括查看用户上下线记录信息和相关配置信息。

背景信息

在完成 BRAS 接入认证的配置后，在任意视图下执行下面的 **display** 命令，查看 BRAS 接入认证的运行信息，检查配置的效果。运行信息的详细解释请参考《HUAWEI NetEngine20E-X6 高端业务路由器 命令参考》。

操作步骤

步骤 1 在任意视图下执行命令 **display web-auth-server configuration**，查看 Web 认证服务器配置信息。

步骤 2 在任意视图下执行命令 **display bas-interface**，查看 BAS 接口的配置信息。

步骤 3 任意视图下执行命令 **display aaa online-fail-record**，查看用户上线失败记录信息。

步骤 4 任意视图下执行命令 **display aaa offline-record** ，查看用户下线的记录信息。

步骤 5 任意视图下执行命令 **display aaa abnormal-offline-record**，查看用户异常下线的记录信息。

步骤 6 任意视图下执行命令 **display access-user**，查看在线用户信息。

----结束

3.7.2 清除 BRAS 接入运行信息

如果用户上下线记录信息太多，可以清除 BRAS 接入运行信息再进行查看。

背景信息

注意

清除 BRAS 接入运行信息后，此前的运行信息将无法恢复。

请执行下面的 **reset** 命令，清除运行信息。

操作步骤

步骤 1 在确认清除系统当前所有的用户上线失败记录后，请在用户视图执行命令 **reset aaa online-fail-record**。

步骤 2 在确认清除系统当前所有的用户下线记录后，请用户视图在执行命令 **reset aaa offline-record**。

步骤 3 在确认清除系统当前所有的用户异常下线记录，请用户视图在执行命令 **reset aaa abnormal offline-record**。

----结束

3.8 配置举例

介绍 BRAS 接入认证的各种示例。配置示例中包括组网需求、配置注意事项和配置思路等。

3.8.1 配置普通 IPoE 接入 VPN(web 认证)示例
介绍一个 IPoE 接入 VPN(web 认证)业务的配置示例，结合配置组网图来理解业务的配置过程。配置示例包括组网需求、思路准备、操作步骤和配置文件。

3.8.2 配置普通 IPoEoVLAN 接入示例
介绍一个 IPoEoVLAN 接入业务的配置示例，结合配置组网图来理解业务的配置过程。配置示例包括组网需求、思路准备、操作步骤和配置文件。

3.8.3 配置普通 IPoEoQ 接入示例
介绍一个 IPoEoQ 接入业务的配置示例，结合配置组网图来理解业务的配置过程。配置示例包括组网需求、思路准备、操作步骤和配置文件。

3.8.4 配置以太网二层专线接入示例
介绍一个以太网二层专线接入业务的配置示例，结合配置组网图来理解业务的配置过程。配置示例包括组网需求、思路准备、操作步骤和配置文件。

3.8.5 配置以太网三层专线接入示例

介绍一个以太网三层专线接入业务的配置示例，结合配置组网图来理解业务的配置过程。配置示例包括组网需求、思路准备、操作步骤和配置文件。

3.8.6 配置 VPN 二层专线接入示例
介绍一个 VPN 二层专线接入业务的配置示例，结合配置组网图来理解业务的配置过程。配置示例包括组网需求、思路准备、操作步骤和配置文件。

3.8.7 配置远端认证静态用户示例
介绍一个远端认证静态用户的配置示例，结合配置组网图来理解业务的配置过程。配置示例包括组网需求、思路准备、操作步骤和配置文件。

3.8.8 配置本地认证静态用户示例
介绍一个本地认证静态用户的配置示例，结合配置组网图来理解业务的配置过程。配置示例包括组网需求、思路准备、操作步骤和配置文件。

3.8.1 配置普通 IPoE 接入 VPN(web 认证)示例

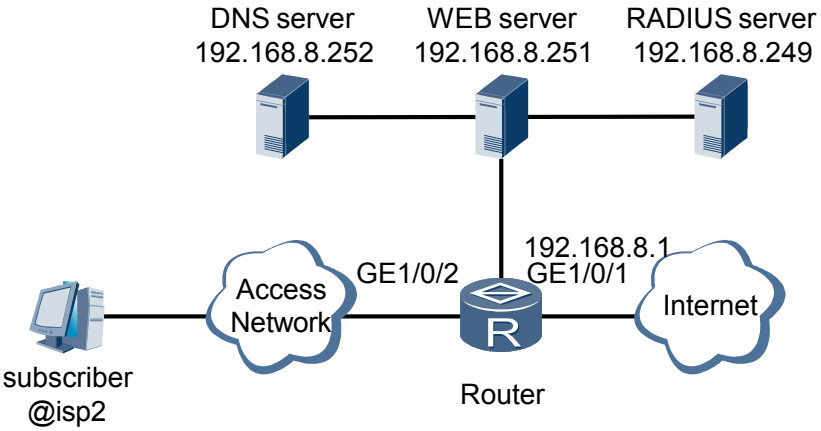
介绍一个 IPoE 接入 VPN(web 认证)业务的配置示例，结合配置组网图来理解业务的配置过程。配置示例包括组网需求、思路准备、操作步骤和配置文件。

组网需求

如图 3-3 所示，普通 IPoE 接入组网需求为：

- 用户归属于 isp2 域，从路由器的 GE1/0/2 接口下以普通 IPoE 方式接入。
- 用户采用 Web 认证，并采用 RADIUS 认证模式和 RADIUS 计费模式。
- RADIUS 服务器地址为 192.168.8.249，认证和计费端口分别是 1812 和 1813，采用标准 RADIUS 协议，密钥为 hello。
- 用户为 VPN 用户，所属 VPN 实例为 vpn1。
- DNS 服务器地址为 192.168.8.252。
- Web 认证服务器地址为 192.168.8.251，密钥为 webvlan。
- 网络侧接口为 GE1/0/1。

图 3-3 普通 IPoE 配置举例组网图



配置思路

普通 IPoE 接入 VPN 的配置思路如下：

1. 配置 VPN 实例
2. 配置认证方案和计费方案
3. 配置 RADIUS 服务器组
4. 配置地址池
5. 配置 Web 认证的认证前域和认证域
6. 配置 Web 认证服务器
7. 配置 ACL 规则和流量管理策略
8. 配置 BAS 接口和上行接口

数据准备

完成此配置举例，需要准备以下数据：

- VPN 实例名称、RD 及 VPN-Target
- 认证模板的名称和认证方式
- 计费模板的名称和计费方式
- RADIUS 服务器组名称，RADIUS 认证服务器和 RADIUS 计费服务器的 IP 地址、端口号
- 地址池名称、网关地址、DNS 服务器地址
- 域的名称
- Web 认证服务器地址
- ACL 规则
- 流量管理策略
- BAS 接口参数

操作步骤

步骤 1 配置 VPN 实例

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] route-distinguisher 100:1
[HUAWEI-vpn-instance-vpn1] vpn-target 100:1 both
[HUAWEI-vpn-instance-vpn1] quit
```

步骤 2 配置 AAA 方案

配置认证方案。

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] authentication-scheme auth2
[HUAWEI-aaa-authen-auth2] authentication-mode radius
[HUAWEI-aaa-authen-auth2] quit
```

配置计费方案

```
[HUAWEI-aaa] accounting-scheme acct2
[HUAWEI-aaa-accounting-acct2] accounting-mode radius
[HUAWEI-aaa-accounting-acct2] quit
```

```
[HUAWEI-aaa] quit
```

步骤 3 配置 RADIUS 服务器组

```
[HUAWEI] radius-server group rd2
[HUAWEI-radius-rd2] radius-server authentication 192.168.8.249 1812
[HUAWEI-radius-rd2] radius-server accounting 192.168.8.249 1813
[HUAWEI-radius-rd2] radius-server type standard
[HUAWEI-radius-rd2] radius-server shared-key hello
[HUAWEI-radius-rd2] quit
```

步骤 4 配置地址池

```
[HUAWEI] ip pool pool2 bas local
[HUAWEI-ip-pool-pool2] gateway 172.82.1.1 255.255.255.0
[HUAWEI-ip-pool-pool2] section 0 172.82.1.2 172.82.1.200
[HUAWEI-ip-pool-pool2] dns-server 192.168.8.252
[HUAWEI-ip-pool-pool2] vpn-instance vpn1
[HUAWEI-ip-pool-pool2] quit
```

步骤 5 配置域

配置 default0 域，作为 Web 认证的认证前域。

```
[HUAWEI] user-group huawei
[HUAWEI] aaa
[HUAWEI-aaa] domain default0
[HUAWEI-aaa-domain-default0] ip-pool pool2
[HUAWEI-aaa-domain-default0] user-group huawei
[HUAWEI-aaa-domain-default0] web-server 192.168.8.251
[HUAWEI-aaa-domain-default0] web-server url http://192.168.8.251
[HUAWEI-aaa-domain-default0] vpn-instance vpn1
[HUAWEI-aaa-domain-default0] quit
```

配置 isp2 域，作为 Web 认证的认证域。

```
[HUAWEI-aaa] domain isp2
[HUAWEI-aaa-domain-isp2] authentication-scheme auth2
[HUAWEI-aaa-domain-isp2] accounting-scheme acct2
[HUAWEI-aaa-domain-isp2] radius-server group rd2
[HUAWEI-aaa-domain-isp2] vpn-instance vpn1
[HUAWEI-aaa-domain-isp2] quit
[HUAWEI-aaa] quit
```

步骤 6 配置 Web 认证服务器

```
[HUAWEI] web-auth-server 192.168.8.251 key webvlan
```

步骤 7 配置 ACL

配置 ACL 规则。

```
[HUAWEI] acl number 6000
[HUAWEI-acl-ucl-6000] acl number 6001
[HUAWEI-acl-ucl-6001] rule permit ip source user-group huawei destination ip-address 192.168.8.251
0
[HUAWEI-acl-ucl-6001] rule permit ip source user-group huawei destination ip-address 192.168.8.252
0
[HUAWEI-acl-ucl-6001] quit
```

配置流量管理策略。

```
[HUAWEI] traffic classifier c1
[HUAWEI-classifier-c1] if-match acl 6000
[HUAWEI-classifier-c2] quit
[HUAWEI] traffic classifier c2
[HUAWEI-classifier-c2] if-match acl 6001
[HUAWEI-classifier-c2] quit
[HUAWEI] traffic behavior deny1
[HUAWEI-behavior-deny1] traffic behavior perm1
[HUAWEI-behavior-perm1] permit
```

```
[HUAWEI-behavior-perm1] quit
[HUAWEI] traffic policy action1
[HUAWEI-policy-action1] classifier c2 behavior perm1
[HUAWEI-policy-action1] classifier c1 behavior deny1
[HUAWEI-policy-action1] quit
```

在全局下应用策略。

```
[HUAWEI] traffic-policy action1 inbound
[HUAWEI] traffic-policy action1 outbound
```

步骤 8 配置接口

配置 BAS 接口。

```
[HUAWEI-GigabitEthernet1/0/2] bas
[HUAWEI-GigabitEthernet1/0/2-bas] access-type layer2-subscriber
[HUAWEI-GigabitEthernet1/0/2-bas] authentication-method web
[HUAWEI-GigabitEthernet1/0/2-bas] default-domain authentication isp2
[HUAWEI-GigabitEthernet1/0/2-bas] quit
[HUAWEI-GigabitEthernet1/0/2] quit
```

配置上行接口。

说明

上行接口连接 MPLS 网络，详细配置请参见《NE20E-X6 配置指南-VPN》中 BGP/MPLS IP VPN 配置章节，此处略。

```
[HUAWEI] interface GigabitEthernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] ip address 192.168.8.1 255.255.255.0
```

----结束

配置文件

```
#
 sysname HUAWEI
#
 user-group huawei
#
ip vpn-instance vpn1
 route-distinguisher 100:1
 vpn-target 100:1 export-extcommunity
 vpn-target 100:1 import-extcommunity
#
 radius-server group rd2
 radius-server authentication 192.168.8.249 1812 weight 0
 radius-server accounting 192.168.8.249 1813 weight 0
 radius-server shared-key hello
#
acl number 6000
#
acl number 6001
 rule 5 permit ip source user-group huawei destination ip-address 192.168.8.251 0
 rule 10 permit ip source user-group huawei destination ip-address 192.168.8.252 0
#
traffic classifier c2 operator and
 if-match acl 6001
traffic classifier c1 operator and
 if-match acl 6000
#
traffic behavior perm1
traffic behavior deny1
#
traffic policy action1
 classifier c2 behavior perm1
 classifier c1 behavior deny1
traffic-policy action1 inbound
```

```
traffic-policy action1 outbound
#
interface GigabitEthernet1/0/2
 bas
  access-type layer2-subscriber  default-domain  authentication isp2
  authentication-method  web
#
interface GigabitEthernet1/0/1
 ip address 192.168.8.1 255.255.255.0
#
ip pool pool2 bas local
 vpn-instance vpn1
 gateway 172.82.1.1 255.255.255.0
 section 0 172.82.1.2 172.82.1.200
 dns-server  192.168.8.252
#
aaa
 authentication-scheme  auth2
 accounting-scheme  acct2
 domain  default0
  web-server  192.168.8.251
  web-server url  http://192.168.8.251
  user-group   huawei
  vpn-instance  vpn1
  ip-pool   pool2
 domain  isp2
  authentication-scheme   auth2
  accounting-scheme   acct2
  radius-server group  rd2
#
return
```

3.8.2 配置普通 IPoEoVLAN 接入示例

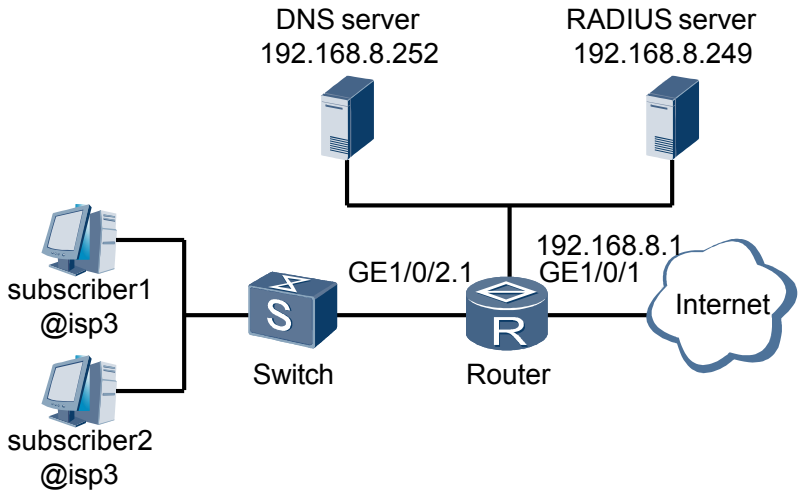
介绍一个 IPoEoVLAN 接入业务的配置示例，结合配置组网图来理解业务的配置过程。配置示例包括组网需求、思路准备、操作步骤和配置文件。

组网需求

如图 3-4 所示，普通 IPoEoVLAN 接入组网需求为：

- 用户归属于 isp3 域，从路由器的 GE1/0/2.1 接口下以普通 IPoEoVLAN 方式接入，Switch 使用 VLAN 1 和 VLAN 2 对用户报文进行标记。
- 用户采用绑定认证，并采用 RADIUS 认证模式和 RADIUS 计费模式。
- RADIUS 服务器地址为 192.168.8.249，认证和计费端口分别是 1812 和 1813，采用标准 RADIUS 协议，密钥为 hello。
- DNS 服务器地址为 192.168.8.252。
- 网络侧接口为 GE1/0/1。

图 3-4 普通 IPoEoVLAN 配置举例组网图



配置思路

普通 IPoEoVLAN 接入的配置思路如下：

1. 配置认证方案和计费方案
2. 配置 RADIUS 服务器组
3. 配置地址池
4. 配置认证域
5. 配置 BAS 接口和上行接口

数据准备

完成此配置举例，需要准备以下数据：

- 认证模板的名称和认证方式
- 计费模板的名称和计费方式
- RADIUS 服务器组名称，RADIUS 认证服务器和 RADIUS 计费服务器的 IP 地址、端口号
- 地址池名称、网关地址、DNS 服务器地址
- 域的名称
- BAS 接口参数

操作步骤

步骤 1 配置 AAA 方案

配置认证方案。

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] authentication-scheme auth3
[HUAWEI-aaa-authen-auth3] authentication-mode radius
[HUAWEI-aaa-authen-auth3] quit
```

配置计费方案。

```
[HUAWEI-aaa] accounting-scheme acct3
[HUAWEI-aaa-accounting-acct3] accounting-mode radius
[HUAWEI-aaa-accounting-acct3] quit
[HUAWEI-aaa] quit
```

步骤 2 配置 RADIUS 服务器组

```
[HUAWEI] radius-server group rd3
[HUAWEI-radius-rd3] radius-server authentication 192.168.8.249 1812
[HUAWEI-radius-rd3] radius-server accounting 192.168.8.249 1813
[HUAWEI-radius-rd3] radius-server type standard
[HUAWEI-radius-rd3] radius-server shared-key hello
[HUAWEI-radius-rd3] quit
```

步骤 3 配置地址池

```
[HUAWEI] ip pool pool3 bas local
[HUAWEI-ip-pool-pool3] gateway 172.82.2.1 255.255.255.0
[HUAWEI-ip-pool-pool3] section 0 172.82.2.2 172.82.2.200
[HUAWEI-ip-pool-pool3] dns-server 192.168.8.252
[HUAWEI-ip-pool-pool3] quit
```

说明

由于绑定认证在用户上线时自动进行认证，因此无需配置认证前缺省域，此处配置的地址池用于用户认证后的域。

步骤 4 配置认证域

```
[HUAWEI] aaa
[HUAWEI-aaa] domain isp3
[HUAWEI-aaa-domain-isp3] authentication-scheme auth3
[HUAWEI-aaa-domain-isp3] accounting-scheme acct3
[HUAWEI-aaa-domain-isp3] radius-server group rd3
[HUAWEI-aaa-domain-isp3] ip-pool pool3
[HUAWEI-aaa-domain-isp3] quit
[HUAWEI-aaa] quit
```

说明

由于绑定认证是获取 IP 地址时自动进行认证，因此无需对认证前的用户进行 ACL 限制，配置 ACL 只需配置其认证后的网络权限即可，此处不作详述。

步骤 5 配置接口

配置 BAS 接口。

```
[HUAWEI] interface GigabitEthernet 1/0/2.1
[HUAWEI-GigabitEthernet1/0/2.1] user-vlan 1 2
[HUAWEI-GigabitEthernet1/0/2.1-vlan-1-2] quit
[HUAWEI-GigabitEthernet1/0/2.1] bas
[HUAWEI-GigabitEthernet1/0/2.1-bas] access-type layer2-subscriber
[HUAWEI-GigabitEthernet1/0/2.1-bas] authentication-method bind
[HUAWEI-GigabitEthernet1/0/2.1-bas] default-domain authentication isp3
[HUAWEI-GigabitEthernet1/0/2.1-bas] quit
[HUAWEI-GigabitEthernet1/0/2.1] quit
```

说明

- 由于绑定认证的用户名是根据用户接入 NE20E-X6 的位置以及域名自动生成的，因此在 RADIUS 服务器上必须根据生成规则来配置用户名，密码为 vlan。
- 有关绑定认证的用户名生成格式请参见《HUAWEI NetEngine20E-X6 高端业务路由器 命令参考》中 **vlanpvc-to-username** 命令的描述。

配置上行接口。

```
[HUAWEI] interface GigabitEthernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] ip address 192.168.8.1 255.255.255.0
```

----结束

配置文件

```
#
 sysname HUAWEI
#
radius-server group rd3
 radius-server authentication 192.168.8.249 1812 weight 0
 radius-server accounting 192.168.8.249 1813 weight 0
 radius-server shared-key hello
#
interface GigabitEthernet1/0/2.1
 user-vlan 1 2
 bas
  access-type layer2-subscriber  default-domain  authentication isp3
  authentication-method  bind
#
interface GigabitEthernet1/0/1
 ip address 192.168.8.1 255.255.255.0
#
ip pool pool3 bas local
 gateway 172.82.2.1 255.255.255.0
 section 0 172.82.2.2 172.82.2.200
 dns-server  192.168.8.252
#
aaa
authentication-scheme  auth3
accounting-scheme  acct3
domain  isp3
 authentication-scheme   auth3
 accounting-scheme   acct3
 radius-server group  rd3
 ip-pool   pool3
#
return
```

3.8.3 配置普通 IPoEoQ 接入示例

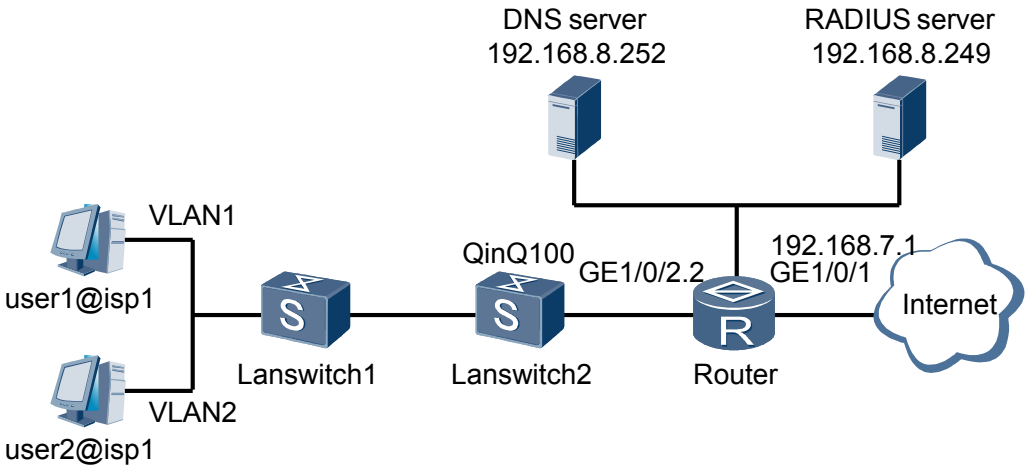
介绍一个 IPoEoQ 接入业务的配置示例，结合配置组网图来理解业务的配置过程。配置示例包括组网需求、思路准备、操作步骤和配置文件。

组网需求

如图 3-5 所示，普通 IPoEoQ 接入组网需求为：

- 用户从路由器的 GE1/0/2.2 接口下以普通 IPoEoQ 方式接入。LAN Switch1 使用 VLAN 1 和 VLAN 2 对用户报文进行标记，LAN Switch2 使用 QinQ100 对用户报文进行标记。
- 用户归属于 isp1 域，采用绑定认证和 RADIUS 计费。
- RADIUS 服务器地址为 192.168.7.249，认证和计费端口分别是 1812 和 1813，采用 RADIUS 标准协议，密钥为 itellin。
- DNS 服务器地址为 192.168.7.252。

图 3-5 普通 IPoEoQ 接入配置组网图



配置思路

普通 IPoEoQ 接入的配置思路如下：

1. 配置认证方案和计费方案
2. 配置 RADIUS 服务器组
3. 配置地址池
4. 配置认证域
5. 配置 BAS 接口和上行接口

数据准备

完成此配置举例，需要准备以下数据：

- 认证模板的名称和认证方式
- 计费模板的名称和计费方式
- RADIUS 服务器组名称，RADIUS 认证服务器和 RADIUS 计费服务器的 IP 地址、端口号
- 地址池名称、网关地址、DNS 服务器地址
- 域的名称
- BAS 接口参数

操作步骤

步骤 1 配置 AAA 方案

配置认证方案。

```
[HUAWEI] aaa
[HUAWEI-aaa] authentication-scheme auth1
[HUAWEI-aaa-authen-auth1] authentication-mode radius
[HUAWEI-aaa-authen-auth1] quit
```

配置计费方案。

```
[HUAWEI-aaa] accounting-scheme acct1
[HUAWEI-aaa-accounting-acct1] accounting-mode radius
[HUAWEI-aaa-accounting-acct1] quit
[HUAWEI-aaa] quit
```

步骤 2 配置 RADIUS 服务器组

```
[HUAWEI] radius-server group rd1
[HUAWEI-radius-rd1] radius-server authentication 192.168.7.249 1812
[HUAWEI-radius-rd1] radius-server accounting 192.168.7.249 1813
 [HUAWEI-radius-rd1] radius-server shared-key itellin
[HUAWEI-radius-rd1] quit
```

步骤 3 配置地址池

```
[HUAWEI] ip pool pool1 bas local
[HUAWEI-ip-pool-pool1] gateway 172.82.0.1 255.255.255.0
[HUAWEI-ip-pool-pool1] section 0 172.82.0.2 172.82.0.200
[HUAWEI-ip-pool-pool1] dns-server 192.168.7.252
[HUAWEI-ip-pool-pool1] quit
```

步骤 4 配置认证域

```
[HUAWEI] aaa
[HUAWEI-aaa] domain isp1
[HUAWEI-aaa-domain-isp1] authentication-scheme auth1
[HUAWEI-aaa-domain-isp1] accounting-scheme acct1
[HUAWEI-aaa-domain-isp1] radius-server group rd1
[HUAWEI-aaa-domain-isp1] ip-pool pool1
[HUAWEI-aaa-domain-isp1] quit
[HUAWEI-aaa] quit
```

步骤 5 配置以太网接口

配置用户侧 VLAN。

```
[HUAWEI] interface GigabitEthernet 1/0/2.2
[HUAWEI-GigabitEthernet1/0/2.2] user-vlan 1 2 qinq 100
[HUAWEI-GigabitEthernet1/0/2.2] quit
```

配置 BAS。

```
[HUAWEI-GigabitEthernet1/0/2.2] bas
[HUAWEI-GigabitEthernet1/0/2.2-bas] access-type layer2-subscriber
[HUAWEI-GigabitEthernet1/0/2.2-bas] default-domain authentication isp1
[HUAWEI-GigabitEthernet1/0/2.2-bas] authentication-method bind
[HUAWEI-GigabitEthernet1/0/2.2-bas] quit
[HUAWEI-GigabitEthernet1/0/2.2] quit
```

配置上行接口。

```
[HUAWEI] interface GigabitEthernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] ip address 192.168.7.1 255.255.255.0
```

步骤 6 检查配置结果。

完成上述配置后，使用命令 **display access-user domain** 查看域下用户在线情况，用户能够正常上线。

```
<HUAWEI> display access-user domain isp1
--------------------------------------------------------------------------------
  UserID  Username               Interface      IP address       MAC
          IPv6 address
--------------------------------------------------------------------------------
  20      user1@isp1               GE1/0/2.2      172.82.0.5         0002-0101-0101
          -
  21      user2@isp1               GE1/0/2.2      172.82.0.6          0002-0101-0102
          -
--------------------------------------------------------------------------------
  Total users                       : 2
```

----结束

配置文件

```
#
 sysname HUAWEI
#
radius-server group rd1
 radius-server authentication 192.168.7.249 1812 weight 0
 radius-server accounting 192.168.7.249 1813 weight 0
 radius-server shared-key itellin
#
interface GigabitEthernet1/0/2.2
 user-vlan 1 2 qinq 100
 bas
  access-type layer2-subscriber  default-domain  authentication isp1
  authentication-method  bind
#
interface GigabitEthernet1/0/1
 ip address 192.168.7.1 255.255.255.0
#
ip pool pool1 bas local
 gateway 172.82.0.1 255.255.255.0
 section 0 172.82.0.2 172.82.0.200
 dns-server  192.168.7.252
#
aaa
authentication-scheme  auth1
accounting-scheme  acct1
domain  default0
domain  default1
domain  default_admin
domain  isp1
 authentication-scheme   auth1
 accounting-scheme   acct1
 radius-server group  rd1
 ip-pool   pool1
#
return
```

3.8.4 配置以太网二层专线接入示例

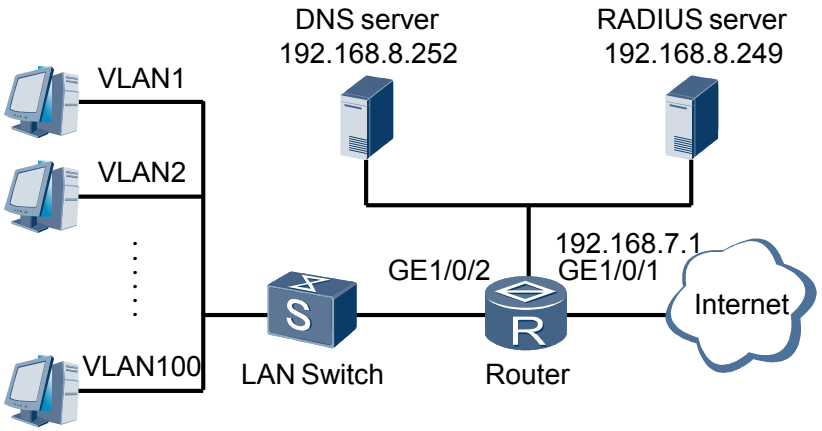
介绍一个以太网二层专线接入业务的配置示例，结合配置组网图来理解业务的配置过程。配置示例包括组网需求、思路准备、操作步骤和配置文件。

组网需求

如图 3-6 所示，以太网二层专线接入组网需求为：

- 以太网二层专线从 GE1/0/2.1 下接入。
- 专线的用户名为 layer2lease1@isp1，密码为 hello。
- 专线用户的 VLAN 为 1 ～ 100。
- 专线用户通过 DHCP 从路由器获取 IP 地址。
- 采用 RADIUS 认证和 RADIUS 计费。RADIUS 服务器地址为 192.168.7.249，认证和计费端口分别是 1645 和 1646，采用 RADIUS+1.1 协议，密钥为 itellin。
- DNS 服务器地址为 192.168.7.252。
- 网络侧接口为 GE1/0/1。

图 3-6 以太网二层专线配置举例组网图



配置思路

以太网二层专线接入的配置思路如下：

1. 配置认证方案和计费方案
2. 配置 RADIUS 服务器组
3. 配置地址池
4. 配置认证域
5. 配置上线接口

数据准备

完成此配置举例，需要准备以下数据：

- 认证模板的名称和认证方式
- 计费模板的名称和计费方式
- RADIUS 服务器组名称，RADIUS 认证服务器和 RADIUS 计费服务器的 IP 地址、端口号
- 地址池名称、网关地址、DNS 服务器地址
- 域的名称
- BAS 接口参数

操作步骤

步骤 1 配置认证方案。

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] authentication-scheme auth1
[HUAWEI-aaa-authen-auth1] authentication-mode radius
[HUAWEI-aaa-authen-auth1] quit
```

步骤 2 配置计费方案。

```
[HUAWEI-aaa] accounting-scheme acct1
[HUAWEI-aaa-accounting-acct1] accounting-mode radius
[HUAWEI-aaa-accounting-acct1] quit
```

```
[HUAWEI-aaa] quit
```

步骤 3 配置 RADIUS 服务器组。

```
[HUAWEI] radius-server group rd1
[HUAWEI-radius-rd1] radius-server authentication 192.168.7.249 1645
[HUAWEI-radius-rd1] radius-server accounting 192.168.7.249 1646
[HUAWEI-radius-rd1] radius-server type plus11
[HUAWEI-radius-rd1] radius-server shared-key itellin
[HUAWEI-radius-rd1] quit
```

步骤 4 配置地址池。

```
[HUAWEI] ip pool pool1 bas local
[HUAWEI-ip-pool-pool1] gateway 172.82.0.1 255.255.0.0
[HUAWEI-ip-pool-pool1] section 0 172.82.0.2 172.82.0.200
[HUAWEI-ip-pool-pool1] dns-server 192.168.7.252
[HUAWEI-ip-pool-pool1] quit
```

步骤 5 配置域。

```
[HUAWEI] aaa
[HUAWEI-aaa] domain isp1
[HUAWEI-aaa-domain-isp1] authentication-scheme auth1
[HUAWEI-aaa-domain-isp1] accounting-scheme acct1
[HUAWEI-aaa-domain-isp1] radius-server group rd1
[HUAWEI-aaa-domain-isp1] ip-pool pool1
[HUAWEI-aaa-domain-isp1] quit
[HUAWEI-aaa]quit
```

步骤 6 配置上线接口。

注意

如果接入接口为以太网子接口则必须要配置 VLAN，如果接入接口为以太网主接口则不能配置 VLAN。

可以为在二层专线的接口下配置多个 VLAN。

```
[HUAWEI] interface GigabitEthernet 1/0/2.1
[HUAWEI-GigabitEthernet1/0/2.1] user-vlan 1 100
[HUAWEI-GigabitEthernet1/0/2.1-vlan-1-100] quit
[HUAWEI-GigabitEthernet1/0/2.1] bas
[HUAWEI-GigabitEthernet1/0/2.1-bas] access-type layer2-leased-line
user-name layer2lease1 password simple hello default-domain authentication isp1
[HUAWEI-GigabitEthernet1/0/2.1-bas] quit
[HUAWEI-GigabitEthernet1/0/2.1] quit
```

----结束

配置文件

```
#
 sysname HUAWEI
#
radius-server group rd1
 radius-server authentication 192.168.7.249 1645 weight 0
 radius-server accounting 192.168.7.249 1646 weight 0
 radius-server shared-key itellin
 radius-server type plus11
 radius-server traffic-unit kbyte
#
interface GigabitEthernet1/0/2.1
 user-vlan 1 100
 bas
```

```
 access-type layer2-leased-line user-name layer2lease1 password simple hello default-domain
authentication isp1
#
interface GigabitEthernet1/0/1
 ip address 192.168.7.1 255.255.255.0
#
ip pool pool1 bas local
 gateway 172.82.0.1 255.255.255.0
 section 0 172.82.0.2 172.82.0.200
 dns-server  192.168.7.252
#
aaa
authentication-scheme  auth1
accounting-scheme  acct1
domain  default0
domain  default1
domain  default_admin
domain  isp1
 authentication-scheme   auth1
 accounting-scheme   acct1
 radius-server group  rd1
 ip-pool   pool1
#
return
```

3.8.5 配置以太网三层专线接入示例

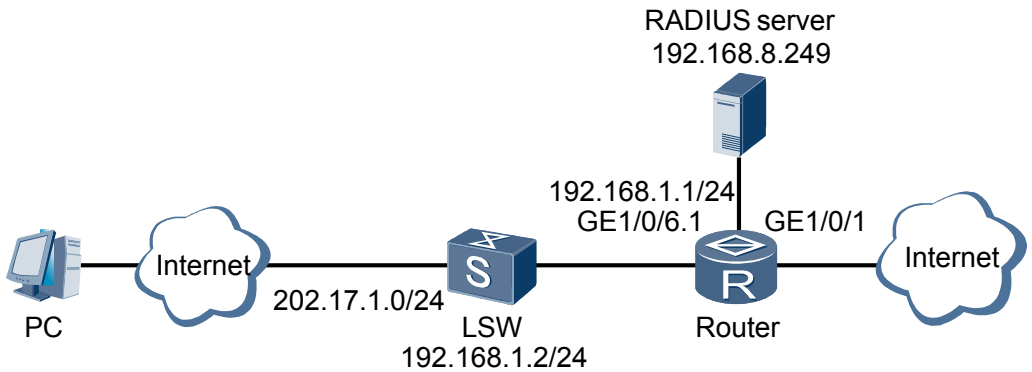
介绍一个以太网三层专线接入业务的配置示例，结合配置组网图来理解业务的配置过程。配置示例包括组网需求、思路准备、操作步骤和配置文件。

组网需求

如图 3-7 所示，以太网三层专线接入组网需求为：

- 以太网三层专线从 GE1/0/6.1 下接入。
- 专线的用户名为 layer3lease1@isp1。
- 三层专线的用户网段为 202.17.1.0/24。
- 采用 RADIUS 认证和 RADIUS 计费。RADIUS 服务器地址为 192.168.7.249，认证和计费端口分别是 1645 和 1646，采用 RADIUS+1.1 协议，密钥为 itellin。
- 网络侧接口为 GE1/0/1。

图 3-7 以太网三层专线配置举例组网图



配置思路

以太网三层专线接入的配置思路如下：

1. 配置认证方案和计费方案
2. 配置 RADIUS 服务器组
3. 配置认证域
4. 配置子接口 VLAN 和 IP 地址
5. 配置 BAS 接口和上行接口
6. 配置静态路由

数据准备

完成此配置举例，需要准备以下数据：

- 认证模板的名称和认证方式
- 计费模板的名称和计费方式
- RADIUS 服务器组名称，RADIUS 认证服务器和 RADIUS 计费服务器的 IP 地址、端口号
- 网关地址、DNS 服务器地址
- 域的名称
- 子接口 VLAN 和 IP 地址
- BAS 接口参数
- 静态路由

操作步骤

步骤 1 配置认证方案。

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] authentication-scheme auth1
[HUAWEI-aaa-authen-auth1] authentication-mode radius
[HUAWEI-aaa-authen-auth1] quit
```

步骤 2 配置计费方案。

```
[HUAWEI-aaa] accounting-scheme acct1
[HUAWEI-aaa-accounting-acct1] accounting-mode radius
[HUAWEI-aaa-accounting-acct1] quit
[HUAWEI-aaa] quit
```

步骤 3 配置 RADIUS 服务器组。

```
[HUAWEI] radius-server group rd1
[HUAWEI-radius-rd1] radius-server authentication 192.168.7.249 1812
[HUAWEI-radius-rd1] radius-server accounting 192.168.7.249 1813
[HUAWEI-radius-rd1] radius-server type standard
[HUAWEI-radius-rd1] radius-server shared-key itellin
[HUAWEI-radius-rd1] quit
```

步骤 4 配置域。

```
[HUAWEI] aaa
[HUAWEI-aaa] domain isp1
[HUAWEI-aaa-domain-isp1] authentication-scheme auth1
[HUAWEI-aaa-domain-isp1] accounting-scheme acct1
[HUAWEI-aaa-domain-isp1] radius-server group rd1
[HUAWEI-aaa-domain-isp1] quit
```

```
[HUAWEI-aaa]quit
```

步骤 5 配置 VLAN

- 如果接入接口为以太网子接口则必须要配置 VLAN，如果接入接口为以太网主接口则不能配置 VLAN。
- 三层专线只能配置一个 VLAN。

```
[HUAWEI] interface GigabitEthernet 1/0/6
[HUAWEI-GigabitEthernet1/0/6] mode user-termination
[HUAWEI-GigabitEthernet1/0/6] interface GigabitEthernet 1/0/6.1
[HUAWEI-GigabitEthernet1/0/6.1] control-vid 1 dot1q-termination
[HUAWEI-GigabitEthernet1/0/6.1] dot1q termination vid 3
```

步骤 6 配置 IP 地址

```
[HUAWEI-GigabitEthernet1/0/6.1] ip address 192.168.1.1 255.255.255.0
```

步骤 7 配置 BAS 接口

```
[HUAWEI-GigabitEthernet1/0/6.1] bas
[HUAWEI-GigabitEthernet1/0/6.1-bas] access-type layer3-leased-line user-name layer3lease1 password
simple hello default-domain authentication isp1
[HUAWEI-GigabitEthernet1/0/6.1-bas] quit
[HUAWEI-GigabitEthernet1/0/6.1] quit
```

步骤 8 配置静态路由

```
[HUAWEI] ip route-static 202.17.1.0 255.255.255.0 192.168.1.2
```

----结束

配置文件

```
#
 sysname HUAWEI
#
#
radius-server group rd1
 radius-server authentication 192.168.7.249 1645 weight 0
 radius-server accounting 192.168.7.249 1646 weight 0
 radius-server shared-key itellin
 radius-server type plus11
 radius-server traffic-unit kbyte
#
interface GigabitEthernet1/0/6
 mode user-termination
#
interface GigabitEthernet1/0/6.1
 control-vid 1 dot1q-termination
 dot1q termination vid 3
 ip address 192.168.1.1 255.255.255.0
 bas
 access-type layer3-leased-line user-name layer3lease1 password simple hello default-domain
authentication isp1
#
interface GigabitEthernet1/0/1
 ip address 192.168.7.1 255.255.255.0
#
aaa
authentication-scheme  auth1
accounting-scheme  acct1
domain  default0
```

```
domain  default1
domain  default_admin
domain  isp1
 authentication-scheme   auth1
 accounting-scheme   acct1
 radius-server group  rd1
#
ip route-static 202.17.1.0 255.255.255.0 192.168.1.2
#
return
```

3.8.6 配置 VPN 二层专线接入示例

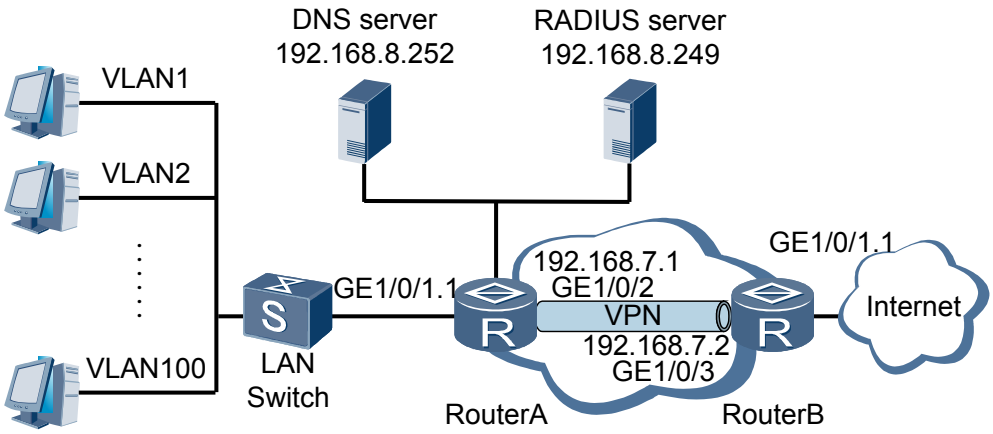
介绍一个 VPN 二层专线接入业务的配置示例，结合配置组网图来理解业务的配置过程。配置示例包括组网需求、思路准备、操作步骤和配置文件。

组网需求

如图 3-8 所示，L2VPN 专线接入组网需求为：

- L2VPN 专线从 GE1/0/1 下接入。
- 专线用户的用户名为 l2vpn-leased-line1@isp1，密码为 hello。
- 专线用户的 VLAN 为 10，通过 DHCP 从 RouterA 获取 IP 地址。
- 采用 RADIUS 认证和 RADIUS 计费。RADIUS 服务器地址为 192.168.7.249，认证和计费端口分别是 1645 和 1646，采用 RADIUS+1.1 协议，密钥为 itellin。
- DNS 服务器地址为 192.168.7.252。
- 网络侧接口为 GE1/0/2。

图 3-8 VPN 二层专线配置举例组网图



配置思路

L2VPN 专线接入的配置思路如下：

1. 配置认证方案和计费方案
2. 配置 RADIUS 服务器组
3. 配置地址池

4. 配置认证域
5. 在设备上使能 MPLS 基本能力
6. 在设备之间建立 LSP 隧道
7. 在设备上使能 MPLS L2VPN
8. 配置 BAS 接口

数据准备

完成此配置举例，需要准备以下数据：

- 认证模板的名称和认证方式
- 计费模板的名称和计费方式
- RADIUS 服务器组名称，RADIUS 认证服务器和 RADIUS 计费服务器的 IP 地址、端口号
- 地址池名称、网关地址、DNS 服务器地址
- 域的名称
- 接口的 IP 地址
- PW 两端的 VSI ID（必须一致）
- 设备上的 MPLS LSR-ID
- 设备上的 VSI 名称
- 子接口 VLAN 和 IP 地址
- BAS 接口参数

操作步骤

步骤 1 配置认证方案。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterA
[RouterA] aaa
[RouterA-aaa] authentication-scheme auth1
[RouterA-aaa-authen-auth1] authentication-mode radius
[RouterA-aaa-authen-auth1] quit
```

步骤 2 配置计费方案。

```
[RouterA-aaa] accounting-scheme acct1
[RouterA-aaa-accounting-acct1] accounting-mode radius
[RouterA-aaa-accounting-acct1] quit
[RouterA-aaa] quit
```

步骤 3 配置 RADIUS 服务器组。

```
[RouterA] radius-server group rd1
[RouterA-radius-rd1] radius-server authentication 192.168.7.249 1812
[RouterA-radius-rd1] radius-server accounting 192.168.7.249 1813
[RouterA-radius-rd1] radius-server type standard
[RouterA-radius-rd1] radius-server shared-key itellin
[RouterA-radius-rd1] quit
```

步骤 4 配置地址池。

```
[RouterA] ip pool pool1 local
[RouterA-ip-pool-pool1] gateway 172.82.0.1 255.255.0.0
[RouterA-ip-pool-pool1] section 0 172.82.0.2 172.82.0.200
[RouterA-ip-pool-pool1] dns-server 192.168.7.252
[RouterA-ip-pool-pool1] quit
```

步骤 5 配置域。

```
[RouterA] aaa
[RouterA-aaa] domain isp1
[RouterA-aaa-domain-isp1] authentication-scheme auth1
[RouterA-aaa-domain-isp1] accounting-scheme acct1
[RouterA-aaa-domain-isp1] radius-server group rd1
[RouterA-aaa-domain-isp1] ip-pool pool1
[RouterA-aaa-domain-isp1] quit
[RouterA-aaa]quit
```

步骤 6 配置 RouterA 的 GE1/0/1 接口

注意

- 如果接入接口为以太网子接口则必须要配置 VLAN，如果接入接口为以太网主接口则不能配置 VLAN。

```
[RouterA] interface gigabitethernet 1/0/1.1
[RouterA-GigabitEthernet1/0/1.1] vlan-type dot1q 10
[RouterA-GigabitEthernet1/0/1.1] quit
```

步骤 7 配置 IGP，本示例中使用 OSPF

配置 RouterA

```
[RouterA] interface loopback 1
[RouterA-LoopBack1] ip address 1.1.1.9 32
[RouterA-LoopBack1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-gigabitethernet1/0/2] ip address 192.168.7.1 24
[RouterA-gigabitethernet1/0/2] undo shutdown
[RouterA-gigabitethernet1/0/2] quit
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[RouterA-ospf-1-area-0.0.0.0] network 192.168.7.0 0.0.0.3
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

配置 RouterB

```
<HUAWEI> system-view
[HUAWEI] sysname RouterB
[RouterB] interface loopback 1
[RouterB-LoopBack1] ip address 2.2.2.9 32
[RouterB-LoopBack1] quit
[RouterB] interface gigabitethernet 1/0/3
[RouterB-gigabitethernet1/0/3] ip address 192.168.7.2 24
[RouterB-gigabitethernet1/0/3] undo shutdown
[RouterB-gigabitethernet1/0/3] quit
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[RouterB-ospf-1-area-0.0.0.0] network 192.168.7.0 0.0.0.3
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

步骤 8 使能 MPLS 基本能力和 LDP

配置 RouterA

```
[RouterA] mpls lsr-id 1.1.1.9
[RouterA] mpls
[RouterA-mpls] lsp-trigger all
```

```
[RouterA-mpls] quit
[RouterA] mpls ldp
[RouterA-mpls-ldp] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-gigabitethernet1/0/2] mpls
[RouterA-gigabitethernet1/0/2] mpls ldp
[RouterA-gigabitethernet1/0/2] quit
```

配置 RouterB

```
[RouterB] mpls lsr-id 2.2.2.9
[RouterB] mpls
[RouterB-mpls] lsp-trigger all
[RouterB-mpls] quit
[RouterB] mpls ldp
[RouterB-mpls-ldp] quit
[RouterB] interface gigabitethernet 1/0/3
[RouterB-gigabitethernet1/0/3] mpls
[RouterB-gigabitethernet1/0/3] mpls ldp
[RouterB-gigabitethernet1/0/3] quit
```

步骤 9 使能 MPLS L2VPN，创建 VSI 并指定 VSI 的信令为 LDP

配置 RouterA

```
[RouterA] mpls l2vpn
[RouterA-l2vpn] quit
[RouterA] vsi ldp1 static
[RouterA-vsi-ldp1] pwsignal ldp
[RouterA-vsi-ldp1-ldp] vsi-id 2
[RouterA-vsi-ldp1-ldp] peer 2.2.2.9
```

配置 RouterB

```
[RouterB] mpls l2vpn
[RouterB-l2vpn] quit
[RouterB] vsi ldp1 static
[RouterB-vsi-ldp1] pwsignal ldp
[RouterB-vsi-ldp1-ldp] vsi-id 2
[RouterB-vsi-ldp1-ldp] peer 1.1.1.9
[RouterB-vsi-ldp1-ldp] quit
[RouterB-vsi-ldp1] quit
```

步骤 10 配置 BAS 接口，绑定 VSI

```
[RouterA-GigabitEthernet1/0/1.1] bas
[RouterA-GigabitEthernet1/0/1.1-bas] access-type l2vpn-leased-line user-name l2vpn-leased-line1
password simple hello default-domain authentication isp1
[RouterA-GigabitEthernet1/0/1.1-bas] quit
[RouterA-GigabitEthernet1/0/1.1] l2 binding vsi ldp1
[RouterB] interface gigabitethernet 1/0/1.1
[RouterB-GigabitEthernet1/0/1.1] vlan-type dot1q 10
[RouterB-GigabitEthernet1/0/1.1] l2 binding vsi ldp1
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
mpls lsr-id 1.1.1.9
mpls
lsp-trigger all
mpls l2vpn
#
vsi ldp1 static
 pwsignal ldp
```

```
 vsi-id 2
 peer 2.2.2.9
#
mpls ldp
#
interface LoopBack1
 ip address 1.1.1.9 255.255.255.255
#
interface GigabitEthernet1/0/1.1
 vlan-type dot1q 10
 l2 binding vsi ldp1
 bas
 access-type l2vpn-leased-line user-name l2vpn-leased-line1 password simple hello default-domain
authentication isp1
#
interface GigabitEthernet1/0/2
 undo shutdown
 ip address 192.168.7.1 255.255.255.0
 mpls
 mpls ldp
#
 ospf 1
 area 0.0.0.0
 network 1.1.1.9 0.0.0.0
 network 192.168.7.0 0.0.0.3
#
ip pool pool1 local
 gateway 172.82.0.1 255.255.0.0
 section 0 172.82.0.2 172.82.0.200
 dns-server  192.168.7.252
#
aaa
authentication-scheme  auth1
accounting-scheme  acct1
domain  default0
domain  default1
domain  default_admin
domain  isp1
 authentication-scheme   auth1
 accounting-scheme   acct1
 radius-server group  rd1
 ip-pool pool1
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
mpls lsr-id 2.2.2.9
mpls
lsp-trigger all
mpls l2vpn
#
vsi ldp1 static
 pwsignal ldp
 vsi-id 2
 peer 1.1.1.9
#
mpls ldp
#
interface LoopBack1
 ip address 2.2.2.9 255.255.255.255
#
interface GigabitEthernet1/0/1.1
 vlan-type dot1q 10
 l2 binding vsi ldp1
#
interface GigabitEthernet1/0/3
 undo shutdown
```

```
 ip address 192.168.7.2 255.255.255.0
 mpls
 mpls ldp
#
 ospf 1
 area 0.0.0.0
 network 2.2.2.9 0.0.0.0
 network 192.168.7.0 0.0.0.3
#
return
```

3.8.7 配置远端认证静态用户示例

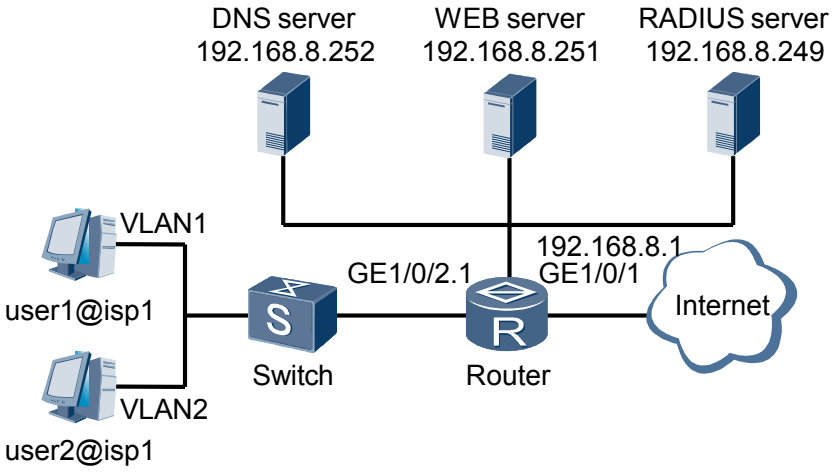
介绍一个远端认证静态用户的配置示例，结合配置组网图来理解业务的配置过程。配置示例包括组网需求、思路准备、操作步骤和配置文件。

组网需求

如图 3-9 所示。

- 用户 user1@isp1 和用户 user2@isp1 同属于域 isp1，从路由器的 1/0/2.1 接口下以静态用户方式接入。LAN Switch 使用 VLAN 1 和 VLAN 2 对用户报文进行标记。
- 两个用户均使用 Web 认证，并采用 RADIUS 认证方式和 RADIUS 计费方式。
- 用户 user1@isp1 的固定 IP 地址为 172.82.1.100，用户 user2@isp1 的固定 IP 地址为 172.82.2.200。
- 两个静态用户都为 VPN 用户，VPN 实例名为 VPN1，将用户加入到 VPN 实例，并允许 VPN1 接入。
- RADIUS 服务器地址为 192.168.8.249，认证和计费端口分别是 1812 和 1813，采用标准 RADIUS 协议，密钥为 hello。
- Web 认证服务器地址为 192.168.8.251，密钥为 webvlan。

图 3-9 远端认证静态用户配置组网图



配置思路

远端认证静态用户的配置思路如下：

1. 配置 VPN 实例
2. 配置认证方案和计费方案
3. 配置 Web 认证服务器
4. 配置 RADIUS 服务器组
5. 配置 DHCP 服务器组
6. 配置 ACL 规则和流量管理策略
7. 配置地址池
8. 配置认证域
9. 配置 BAS 接口和上行接口
10. 配置静态用户

数据准备

完成此配置举例，需要准备以下数据：

- VPN 实例名称、RD 及 VPN-Target
- 认证模板的名称和认证方式
- 计费模板的名称和计费方式
- Web 认证服务器地址
- RADIUS 服务器组名称，RADIUS 认证服务器和 RADIUS 计费服务器的 IP 地址、端口号
- DHCP 服务器组地址
- ACL 规则
- 流量管理策略
- 地址池名称、网关地址、DNS 服务器地址
- 域的名称
- BAS 接口参数

操作步骤

步骤 1 配置 VPN 实例。

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] route-distinguisher 100:1
[HUAWEI-vpn-instance-vpn1] vpn-target 100:1 both
[HUAWEI-vpn-instance-vpn1] quit
```

步骤 2 配置认证方案。

```
[HUAWEI] aaa
[HUAWEI-aaa] authentication-scheme auth1
[HUAWEI-aaa-authen-auth1] authentication-mode radius
[HUAWEI-aaa-authen-auth1] quit
```

步骤 3 配置计费方案。

```
[HUAWEI-aaa] accounting-scheme acct1
[HUAWEI-aaa-accounting-acct1] accounting-mode radius
[HUAWEI-aaa-accounting-acct1] quit
[HUAWEI-aaa] quit
```

步骤 4 配置 Web 认证服务器。

```
[HUAWEI] web-auth-server 192.168.8.251 key webvlan
```

步骤 5 配置 RADIUS 服务器组。

```
[HUAWEI] radius-server group rd1
[HUAWEI-radius-rd1] radius-server authentication 192.168.8.249 1812
[HUAWEI-radius-rd1] radius-server accounting 192.168.8.249 1813
[HUAWEI-radius-rd1] radius-server type standard
[HUAWEI-radius-rd1] radius-server shared-key hello
[HUAWEI-radius-rd1] quit
```

步骤 6 配置 ACL，使用户 Web 认证前只能访问 Web 服务器

配置用户组

```
[HUAWEI] user-group Huawei
```

配置 ACL 规则

```
[HUAWEI] acl 6000 match-order auto
[HUAWEI-acl-ucl-6000] rule deny ip source user-group huawei destination ip-add
ress any
[HUAWEI-acl-ucl-6000] rule permit ip source user-group huawei destination ip-add
Ress 192.168.8.251 0.0.0.255
[HUAWEI-acl-ucl-6000] quit
```

配置流分类器

```
[HUAWEI] traffic classifier c1
[HUAWEI-classifier-c1] if-match acl 6000
[HUAWEI-classifier-c1] quit
```

配置流动作

```
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] permit
[HUAWEI-behavior-b1] quit
```

配置流量策略

```
[HUAWEI] traffic policy policy
[HUAWEI-trafficpolicy-policy] classifier c1 behavior b1
[HUAWEI-trafficpolicy-policy] quit
```

全局下应用流量策略

```
[HUAWEI] traffic-policy policy inbound
[HUAWEI] traffic-policy policy outbound
```

步骤 7 配置地址池。

```
[HUAWEI] ip pool pool1 bas local
[HUAWEI-ip-pool-pool1] gateway 172.82.1.1 255.255.255.0
[HUAWEI-ip-pool-pool1] section 0 172.82.1.2 172.82.1.200
[HUAWEI-ip-pool-pool1] excluded-ip-address 172.82.1.100
[HUAWEI-ip-pool-pool1] vpn-instance vpn1
[HUAWEI-ip-pool-pool1] quit
[HUAWEI] ip pool pool2 bas local
[HUAWEI-ip-pool-pool2] gateway 172.82.2.1 255.255.255.0
[HUAWEI-ip-pool-pool2] section 0 172.82.2.2 172.82.2.200
[HUAWEI-ip-pool-pool2] vpn-instance vpn1
[HUAWEI-ip-pool-pool2] quit
```

步骤 8 配置域。

配置认证前域 default0。

```
[HUAWEI] aaa
[HUAWEI-aaa] domain default0
[HUAWEI-aaa-domain-default0] ip-pool pool1
[HUAWEI-aaa-domain-default0] ip-pool pool2
```

```
[HUAWEI-aaa-domain-default0] user-group huawei
[HUAWEI-aaa-domain-default0] vpn-instance vpn1
[HUAWEI-aaa-domain-default0] quit
```

配置认证后域 isp1。

```
[HUAWEI-aaa] domain isp1
[HUAWEI-aaa-domain-isp1] authentication-scheme auth1
[HUAWEI-aaa-domain-isp1] accounting-scheme acct1
[HUAWEI-aaa-domain-isp1] radius-server group rd1
[HUAWEI-aaa-domain-isp1] vpn-instance vpn1
[HUAWEI-aaa-domain-isp1] quit
[HUAWEI-aaa] quit
```

步骤 9 配置 BAS 接口。

```
[HUAWEI] interface GigabitEthernet 1/0/2.1
[HUAWEI-GigabitEthernet1/0/2.1] user-vlan 1 2
[HUAWEI-GigabitEthernet1/0/2.1-vlan-1-2] quit
[HUAWEI-GigabitEthernet1/0/2.1] bas
[HUAWEI-GigabitEthernet1/0/2.1-bas] access-type layer2-subscriber default-domain authentication isp1
[HUAWEI-GigabitEthernet1/0/2.1-bas] authentication-method web
[HUAWEI-GigabitEthernet1/0/2.1-bas] vpn-instance vpn1
[HUAWEI-GigabitEthernet1/0/2.1-bas] ip-trigger
[HUAWEI-GigabitEthernet1/0/2.1-bas] arp-trigger
[HUAWEI-GigabitEthernet1/0/2.1-bas] quit
[HUAWEI-GigabitEthernet1/0/2.1] quit
```

步骤 10 配置静态用户

```
[HUAWEI] static-user 172.82.1.100 172.82.1.100 vpn-instance vpn1  interface GigabitEthernet1/0/2.1
vlan 1 detect domain-name isp1
[HUAWEI] static-user 172.82.2.200 172.82.2.200 vpn-instance vpn1  interface GigabitEthernet1/0/2.1
vlan 2 domain-name isp1
```

步骤 11 配置上行接口。

```
[HUAWEI] interface GigabitEthernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] ip address 192.168.8.1 255.255.255.0
```

----结束

配置文件

```
#
 sysname HUAWEI
#
 user-group huawei
#
ip vpn-instance vpn1
 route-distinguisher 100:1
 vpn-target 100:1 export-extcommunity
 vpn-target 100:1 import-extcommunity
#
radius-server group rd1
 radius-server authentication 192.168.8.249 1812 weight 0
 radius-server accounting 192.168.8.249 1813 weight 0
 radius-server shared-key hello
#
acl number 6000 match-order auto
  rule 5 permit ip source user-group huawei destination ip-address 192.168.8.0 0.
0.0.255
 rule 10 deny ip source user-group huawei destination ip-address any
#
traffic classifier c1 operator or
 if-match acl 6000
#
traffic behavior b1
#
traffic policy policy
 classifier c1 behavior b1
```

```
traffic-policy policy inbound
traffic-policy policy outbound
#
interface GigabitEthernet1/0/2.1
 user-vlan 1 2
 bas
  access-type layer2-subscriber default-domain authentication isp1
  authentication-method  web
  vpn-instance vpn1
  ip-trigger
  arp-trigger
#
interface GigabitEthernet1/0/1
 ip address 192.168.8.1 255.255.255.0
#
ip pool pool1 bas local
 vpn-instance vpn1
 gateway 172.82.1.1 255.255.255.0
 section 0 172.82.1.2 172.82.1.200
 excluded-ip-address  172.82.1.100
#
ip pool pool2 bas local
 vpn-instance vpn1
 gateway 172.82.2.1 255.255.255.0
 section 0 172.82.2.2 172.82.2.200
#
aaa
authentication-scheme  auth1
accounting-scheme  acct1
domain  default0
 user-group huawei
 vpn-instance  vpn1
 ip-pool pool1
 ip-pool pool2
domain  isp1
 authentication-scheme   auth1
 accounting-scheme   acct1
 radius-server group  rd1
 vpn-instance vpn1
#
 web-auth-server 192.168.8.251 port 50100 key webvlan
#
 static-user 172.82.1.100 172.82.1.100 vpn-instance vpn1  interface GigabitEther
net1/0/2.1 vlan 1 detect domain-name isp1
 static-user 172.82.2.200 172.82.2.200 vpn-instance vpn1  interface GigabitEther
net1/0/2.1 vlan 2 domain-name isp1
#
return
```

3.8.8 配置本地认证静态用户示例

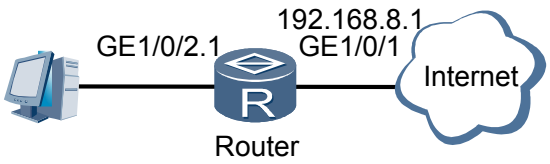
介绍一个本地认证静态用户的配置示例，结合配置组网图来理解业务的配置过程。配置示例包括组网需求、思路准备、操作步骤和配置文件。

组网需求

如图 3-10 所示。

- 用户从路由器的 1/0/2.1 接口下以静态用户方式接入，固定 IP 地址为 172.192.0.8。
- 用户使用本地认证模式。
- 使用用户报文携带的 IP 地址生成用户名。

图 3-10 本地认证静态用户配置组网图



配置思路

本地认证静态用户的配置思路如下：

1. 配置认证方案
2. 配置地址池
3. 配置认证域
4. 配置 BAS 接口和上行接口
5. 配置静态用户

数据准备

完成此配置举例，需要准备以下数据：

- 认证模板的名称和认证方式
- 地址池名称、网关地址、DNS 服务器地址
- 域的名称
- BAS 接口参数

操作步骤

步骤 1 配置认证方案

```
[HUAWEI] aaa
[HUAWEI-aaa] authentication-scheme local
[HUAWEI-aaa-authen-local] authentication-mode local
[HUAWEI-aaa-authen-local] quit
```

步骤 2 配置用户名生成方式和密码

```
[HUAWEI-aaa] default-user-name include ip-address .
[HUAWEI-aaa] default-password simple test
[HUAWEI-aaa] quit
```

步骤 3 配置本地帐号

```
[HUAWEI] local-aaa-server
[HUAWEI-local-aaa-server] user 172.192.0.8@isp1 password simple test authentication-type b
[HUAWEI-local-aaa-server] quit
```

步骤 4 配置地址池

```
[HUAWEI] ip pool pool1 bas local
[HUAWEI-ip-pool-pool1] gateway 172.192.0.1 255.255.255.0
[HUAWEI-ip-pool-pool1] section 0 172.192.0.2 172.192.0.200
[HUAWEI-ip-pool-pool1] excluded-ip-address 172.192.0.8
[HUAWEI-ip-pool-pool1] quit
```

步骤 5 配置域

```
[HUAWEI] aaa
```

```
[HUAWEI-aaa] domain isp1
[HUAWEI-aaa-domain-isp1] authentication-scheme local
[HUAWEI-aaa-domain-isp1] accounting-scheme default0
[HUAWEI-aaa-domain-isp1] ip-pool pool1
[HUAWEI-aaa-domain-isp1] quit
[HUAWEI-aaa] quit
```

步骤 6 配置 BAS 接口

```
[HUAWEI-GigabitEthernet1/0/2] interface GigabitEthernet 1/0/2.1
[HUAWEI-GigabitEthernet1/0/2.1] user-vlan 100
[HUAWEI-GigabitEthernet8/0/2.1-vlan-1-2] quit
[HUAWEI-GigabitEthernet1/0/2.1] bas
[HUAWEI-GigabitEthernet1/0/2.1-bas] access-type layer2-subscriber
[HUAWEI-GigabitEthernet1/0/2.1-bas] authentication-method bind
[HUAWEI-GigabitEthernet1/0/2.1-bas] default-domain authentication isp1
[HUAWEI-GigabitEthernet1/0/2.1-bas] ip-trigger
[HUAWEI-GigabitEthernet1/0/2.1-bas] arp-trigger
[HUAWEI-GigabitEthernet1/0/2.1-bas] quit
[HUAWEI-GigabitEthernet1/0/2.1] quit
```

步骤 7 配置静态用户

```
[HUAWEI] static-user 172.192.0.8 interface GigabitEthernet 1/0/2.1 vlan 100 detect
```

步骤 8 配置上行接口

```
[HUAWEI] interface GigabitEthernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] ip address 192.168.8.1 255.255.255.0
```

步骤 9 验证配置结果。

完成上述配置后，使用命令 **display access-user domain** 查看域下用户在线情况，用户能够正常上线。

```
<HUAWEI> display access-user domain isp1
------------------------------------------------------------------------------
  UserID  Username                Interface      IP address       MAC
          IPv6 address
  ------------------------------------------------------------------------------
  20      172.192.0.8@isp1                GE1/0/2.1      172.192.0.8         0002-0101-0101
          -
  ------------------------------------------------------------------------------
  Total users                         : 1
```

----结束

配置文件

```
#
 sysname HUAWEI
#
interface GigabitEthernet1/0/1
 undo shutdown
 ip address 192.168.8.1 255.255.255.0
#
interface GigabitEthernet1/0/2.1
 user-vlan 100
 bas
  access-type layer2-subscriber  default-domain  authentication isp1
  ip-trigger
  arp-trigger
  authentication-method  bind
#
ip pool pool1 bas local
 gateway 172.192.0.1 255.255.255.0
 section 0 172.192.0.2 172.192.0.200
 excluded-ip-address  172.192.0.8
#
aaa
```

```
 default-user-name include ip-address .
 default-password simple test
authentication-scheme  local
 authentication-mode local
domain  ispl
 authentication-scheme   local
 accounting-scheme   default0
 ip-pool pool1
#
local-aaa-server
 user 172.192.0.8@ispl password simple test authentication-type B
#
 static-user 172.192.0.8 172.192.0.8 interface GigabitEthernet1/0/2.1 vlan 100 detect
#
return
```

A RADIUS、HWTACACS 属性列表

列出本手册中的 RADIUS、HWTACACS 属性列表。

A.1 RADIUS 属性
列出本手册中的 RADIUS 列表。

A.2 HWTACACS 属性
列出本手册中 HWTACACS 属性列表。

A.1 RADIUS 属性

列出本手册中的 RADIUS 列表。

A.1.1 标准 RADIUS 属性

列出本手册中的标准 RADIUS 属性列表

编码	名称	描述
1	User-Name	进行认证的用户名
2	Password	进行认证的用户密码，仅对 PAP 认证有效
3	Challenge-Password	进行认证的用户密码，仅对 CHAP 认证有效
4	NAS-IP-Address	设备 IP 地址，如果 RADIUS 服务器组绑定了接口地址，则取绑定的接口地址，否则取发送报文的接口地址
5	NAS-Port	用户接入端口，格式为“4 位槽位号+2 位卡号+5 位端口号+21 位 VLAN”
6	Service-Type	用户业务类型，接入用户为 2，操作用户为 6
7	Framed-Protocol	固定为 1，表示 PPP 类型
8	Framed-IP-Address	RADIUS 服务器为用户分配的 IP 地址，0xFFFFFFFE 表示 RADIUS 服务器不分配地址，而由设备为用户分配 IP 地址
9	Framed-Netmask	RADIUS 服务器为用户分配的 IP 地址掩码
11	Filter-ID	表示用户组
14	Login-IP-Host	Login 连接用户的主机 IP 地址
15	Login-Service	Login 业务类型----Telnet，Rlogin，TCP Clear，PortMaster (proprietary)，LAT
18	Reply-Message	认证成功或拒绝消息
22	Framed-route	RADIUS 服务器为 NAS 的用户提供路由信息
24	State	如果 RADIUS 服务器发送给设备的接入质询报文中包含该值，则设备在后续的接入请求报文中必须包含相同的值

编码	名称	描述
25	Class	如果 RADIUS 服务器发送给设备的认证接受报文中包含该值，则设备在后续的计费请求报文中必须包含相同的值；对于标准 RADIUS 服务器，设备可以使用 Class 属性表示 CAR 参数
27	Session-Timeout	用户可用的剩余时间，以秒为单位；在 EAP 质询报文中作为用户的重认证时长
28	Idle-Timeout	用户的闲置切断时间，以秒为单位
29	Termination-Action	指定的业务终止方式，重认证或者强制用户下线等
30	Called-Station-Id	允许 NAS 发送被叫号码
31	Calling-Station-Id	允许 NAS 发送主叫号码
32	NAS-Identifier	设备主机名
33	Proxy-State	在 COA、DM 请求回应报文中使用，回应和请求保持一致
40	Acct-Status-Type	计费报文类型，1 表示开始计费报文，2 表示停止计费报文，3 表示实时计费报文
41	Acct-Delay-Time	生成计费报文花费的时间，以秒为单位
42	Acct-Input-Octets	上行字节数，单位为 Byte、kbyte、Mbyte、Gbyte，具体使用何种单位可通过命令配置
43	Acct-Output-Octets	下行字节数，单位为 Byte、kbyte、Mbyte、Gbyte，具体使用何种单位可通过命令配置
44	Acct-Session-Id	计费的连接号，对于同一个连接的开始计费、实时计费和停止计费报文，其中的连接号必须相同
45	Acct-Authentic	用户的认证模式，1 表示 RADIUS 认证，2 表示本地认证
46	Acct-Session-Time	用户的上线时间，以秒为单位
47	Acct-Input-Packets	上行的报文数
48	Acct-Output-Packets	下行的报文数

编码	名称	描述
49	Terminate-Cause	用户连接中断的原因： ● User-Request(1)：用户主动下线 ● Lost Carrier(2)：握手失败，如 ARP 探测失败、PPP 握手失败等 ● Lost Service(3)：LNS 发起拆除连接指令 ● Idle Timeout(4)：闲置切断 ● Session Timeout(5)：时间限制切断或流量限制切断 ● Admin Reset(6)：管理员发起拆除连接指令 ● Admin Reboot(7)：管理员复位设备 ● Port Error(8)：端口错误 ● NAS Error(9)：设备发生内部错误 ● NAS Request(10)：设备由于资源变化拆除连接 ● NAS Reboot(11)：设备自动复位 ● Port Unneeded(12)：端口 Down ● Port Suspended(14)：端口挂起 ● Service Unavailable(15)：业务不可用 User Error ● (17)：用户认证失败或超时 ● Host Request (18)：收到服务器的 Decline 报文
50	Acct-Multi-Session-ID	多会话 ID，用于识别日志中的相关会话
52	Acct-Input-Gigawords	表示上行字节数是 4G(2^{32})Byte、kbyte、Mbyte、Gbyte（单位取何值由命令配置决定）的多少倍
53	Acct-Output-Gigawords	表示下行字节数是 4G(2^{32})Byte、kbyte、Mbyte、Gbyte（单位取何值由命令配置决定）的多少倍
55	Event-Timestamp	生成计费报文的时间，以秒为单位，表示从 1970 年 1 月 1 日零点零分零秒以来的绝对秒数
60	CHAP-Challenge	CHAP 认证的质询字，只用于 CHAP 认证
61	NAS-Port-Type	NAS 的端口类型，可在 BAS 接口视图下配置
62	Port-Limit	端口用户数，目前通过该属性限制一个帐号下的用户数
64	Tunnel-Type	隧道的协议类型，固定为 3，表示 L2TP 隧道
65	Tunnel-Medium-Type	隧道承载的媒介类型，固定为 1，表示 IPv4
66	Tunnel-Client-Endpoint	隧道本地端的 IP 地址

编码	名称	描述
67	Tunnel-Server-Endpoint	隧道服务器端的 IP 地址
68	Acct-Tunnel-Connection	隧道服务器计费 ID
69	Tunnel-Password	隧道验证的密码，前两字节为 SALT，后 16 字节为加密后的密码
77	connect-info	作为 LNS 时，通过 RADIUS connect-info 上报 L2TP Transmit (TX) Speed（avp24）和 RX Speed
79	EAP-Message	用于携带 EAP 报文，EAP 报文长度超过 253 时支持封装成多个属性
80	Message-Authenticator	用于携带 EAP 报文加密信息，EAPoR 认证时使用
82	Tunnel-Assignment-ID	隧道标识名
83	Tunnel-Preference	隧道优先级
85	Acct-Interim-Interval	实时计费的间隔，以秒为单位
86	Acct-Tunnel-Packets-Lost	在一个指定连接上丢失的报文数
87	NAS-Port-Id	用户接入的端口号，格式为“slot=XX;subslot=XX;port=XXX;VLANID=XXXX;”或者“slot=XX;subslot=XX;port=XXX;VPI=XXX;VCI=XXXX”
88	Framed-Pool	地址池的名称和地址段号，只对从设备的本地地址池为 PPP 分配 IP 地址有效，格式为“地址池名#地址段号”
90	Tunnel-Client-Auth-ID	隧道认证中传递的本端用户名
91	Tunnel_Server_Auth_id	隧道认证中传递的服务器端用户名
95	NAS-Ipv6-Address	NAS 的 IPv6 地址
96	Framed-Interface-Id	分配给用户的接口 ID，目前只有 PPPv6 用户使用
97	Framed-Ipv6-Prefix	分配给用户的 IPv6 前缀，目前支持 PPPv6 用户和 ND 用户
101	Error-Cause	RFC3576 下线原因

编码	名称	描述
123	Delegated-Ipv6-Prefix	分配给路由模式 CPE 的 ipv6 pd 前缀

A.1.2 华为 RADIUS 属性

编码	名称	描述
26-1	Input-Peak-Rate	上行峰值速率，以 bit/s 为单位
26-2	Input-Average-Rate	上行平均速率，以 bit/s 为单位
26-3	Input-Basic-Rate	上行基本速率，以 bit/s 为单位
26-4	Output-Peak-Rate	下行峰值速率，以 bit/s 为单位
26-5	Output-Average-Rate	下行平均速率，以 bit/s 为单位
26-6	Output-Basic-Rate	下行基本速率，以 bit/s 为单位
26-7	In-Kb-Before-T-Switch	费率切换前接收的流量，以 kbyte 为单位。如果实时计费周期内未发生费率切换，则本属性表示整个实时计费周期内设备接收到的用户流量；如果在实时计费周期内发生费率切换，则本属性表示从实时计费开始到费率切换时刻设备接收到的用户流量本属性只用于 Portal 型（RADIUS+1.1）的 RADIUS 服务器
26-8	Out-Kb-Before-T-Switch	费率切换前发送的流量，以 kbyte 为单位。如果实时计费周期内未发生费率切换，则本属性表示整个实时计费周期内设备发送出的用户流量；如果在实时计费周期内发生费率切换，则本属性表示从实时计费开始到费率切换时刻设备发送出的用户流量本属性只用于 Portal 型（RADIUS+1.1）的 RADIUS 服务器
26-9	In-Pkt-Before-T-Switch	费率切换前接收的报文数。如果实时计费周期内未发生费率切换，则本属性表示整个实时计费周期内设备接收到的报文数；如果在实时计费周期内发生费率切换，则本属性表示从实时计费开始到费率切换时刻设备接受到的报文数本属性只用于 Portal 型（RADIUS+1.1）的 RADIUS 服务器
26-10	Out-Pkt-Before-T-Switch	费率切换前发送的报文数。如果实时计费周期内未发生费率切换，则本属性表示整个实时计费周期内设备发送出的报文数；如果在实时计费周期内发生费率切换，则本属性表示从实时计费开始到费率切换时刻设备发送出的报文数本属性只用于 Portal 型（RADIUS+1.1）的 RADIUS 服务器

编码	名称	描述
26-11	In-Kb-After-T-Switch	费率切换后接收的流量，以 kbyte 为单位。如果实时计费周期内未发生费率切换，则本属性表示整个实时计费周期内设备接收到的用户流量；如果在实时计费周期内发生费率切换，则本属性表示从费率切换时刻到实时计费结束设备接收到的用户流量本属性只用于 Portal 型（RADIUS+1.1）的 RADIUS 服务器
26-12	Out-Kb-After-T-Switch	费率切换后发送的流量，以 kbyte 为单位。如果实时计费周期内未发生费率切换，则本属性表示整个实时计费周期内设备发送出的用户流量；如果在实时计费周期内发生费率切换，则本属性表示从费率切换时刻到实时计费结束设备发送出的用户流量本属性只用于 Portal 型（RADIUS+1.1）的 RADIUS 服务器
26-13	In-Pkt-After-T-Switch	费率切换后接收的报文数。如果实时计费周期内未发生费率切换，则本属性表示整个实时计费周期内设备接收到的报文数；如果在实时计费周期内发生费率切换，则本属性表示从费率切换时刻到实时计费结束设备接受到的报文数本属性只用于 Portal 型（RADIUS+1.1）的 RADIUS 服务器
26-14	Out-Pkt-After-T-Switch	费率切换后发送的报文数。如果实时计费周期内未发生费率切换，则本属性表示整个实时计费周期内设备发送出的报文数；如果在实时计费周期内发生费率切换，则本属性表示从费率切换时刻到实时计费结束设备发送出的报文数本属性只用于 Portal 型（RADIUS+1.1）的 RADIUS 服务器
26-15	Remanent-Volume	用户的剩余可用流量，单位为千字节
26-16	Tariff-Switch-Interval	最近的费率切换时刻与当前时间的时间间隔，以秒为单位本属性只用于 Portal 型（RADIUS+1.1）的 RADIUS 服务器
26-20	Command	用于会话控制报文，表示对会话进行操作，取值如下：1：会话触发请求 2：会话中断请求 3：设置策略 4：结果本属性只用于 Portal 型（RADIUS+1.1）的 RADIUS 服务器
26-22	Priority	用户业务的优先级，有效值范围 1 ～ 9
26-24	Control-Identifier	服务器重发报文的标识符，对于同一会话中的重发报文，本属性必须相同；客户端响应的报文中，该值必须原样返回在开始计费、实时计费和结束计费报文中，该值无意义本属性只用于 Portal 型（RADIUS+1.1）的 RADIUS 服务器
26-25	Result-Code	当 26-20 属性设置为 3 或 4 时有效，0 表示成功，非 0 表示失败本属性只用于 Portal 型（RADIUS+1.1）的 RADIUS 服务器
26-26	Connect-ID	用户连接的索引本属性只用于 Portal 型（RADIUS+1.1）的 RADIUS 服务器
26-27	Portal-URL	PPP 用户强制 Portal 业务的 URL 本属性只用于 Portal 型（RADIUS+1.1）的 RADIUS 服务器
26-28	Ftp-directory	FTP 用户的初始目录
26-29	Exec-Privilege	Telnet 等操作用户的优先级，有效值范围 0 ～ 3

编码	名称	描述
26-30	Radius-Mp-VT-Number	MP 用户所用的 Virtual-template 号
26-31	VPN-instance	VPN 用户所属的 VPN-instance 名字
26-32	VT-number	VPN 用户所属的 Virtual-template 号
26-59	Startup-stamp	设备的启动时间，以秒为单位，表示从 1970 年 1 月 1 日零点零分零秒设备启动时间的绝对秒数
26-60	Ip-Host-Address	认证和计费报文中携带的用户 IP 地址和 MAC 地址，格式为“A.B.C.D HH:HH:HH:HH:HH:HH”，IP 地址和 MAC 地址之间以空格分割
26-135	Primary-DNS	用户认证成功后，RADIUS 下发的主 DNS 服务器地址
26-136	Secondary-DNS	用户认证成功后，RADIUS 下发的备 DNS 服务器地址
26-254	Version	设备的软件版本号
26-255	Product-ID	产品名称

A.2 HWTACACS 属性

列出本手册中 HWTACACS 属性列表。

名称	描述
Acl	代表一个连接的 ACL；仅当 service=shell, cmd=NULL 时使用
Idletime	连接的空闲 timeout, 单位是分钟。0 表示没有 timeout
Autocmd	一个要自动运行的命令；仅当 service=shell, cmd=NULL 时使用
Priv-lvl	赋予的特权级别，范围是 0-3.
Ftpdir	FTP 用户的初始目录
Callback-line	服务器传递过来可以显示给用户的信息，如移动电话号码等
Nocallback-verify	回呼之后不需要验证
Nohangup	在一个自动运行的命令之后不断开连接；仅当 service=shell, cmd=NULL 时使用
Addr	网络地址
Addr-pool	指定一个地址池，NAS 必须从该地址池分配出地址
Dns-servers	DNS 服务器

名称	描述
Tunnel-type	隧道类型
Ip-addresses	LNS 的 IP 地址，最多支持 5 个，IP 地址之间以','或者';'分隔
Tunnel-id	隧道 ID
L2tp-hello-interval	L2TP Hello 报文的间隔时间
L2tp-hidden-avp	L2TP 的隐藏属性值对 AVP（Attribute Value Pair）
L2tp-nosession-timeout	L2TP 无会话时切断时间
L2tp-tos-reflect	L2TP 的 TOS 的值
L2tp-tunnel-authen	是否进行 L2TP 的隧道认证
Gw-password	网关密码
L2tp-udp-checksum	L2TP 的 UDP 包的检验和
Source-ip	源 IP 地址
L2tp-group-num	L2TP 组号
Upaverage	上行平均速率，单位 bps
Uppeak	上行峰值速率，以 bit/s 为单位
Dnaverage	下行平均速率，单位 bps
Dnpeak	下行峰值速率，以 bit/s 为单位
Task_id	任务 ID
Timezone	时区
Service	主要的服务。是要授权或者计费的服务，例如：“slip”，“ppp”，“arap”，“shell”，“tty-daemon”，“connection”，“system”以及“firewall”。
Protocol	协议是服务的子集，例如“lcp”，“ip”，“ipx”，“atalk”，“vines”，“lat”，“xremote”，“tn3270”，“telnet”，“rlogin”，“pad”，“vpdn”，“ftp”，“http”，“deccp”，“osicp”以及“unknown”。
Mlp_links_max	MP 的最大捆绑连接数

名称	描述
Mlp_links_current	MP 的当前连接数
Disc_cause	下线原因
Disc_cause_ext	下线原因的扩展
Elapsed_time	用户的在线时长
Nas_rx_speed	NAS 的输出速度
Nas_tx_speed	NAS 的输入速度

B 术语

列出了本手册中使用的术语，及对应的英文全称和中文解释。

B

BRAS	Broadband Remote Access Server，是运行在 NE20E-X6 上的功能组件，用于为宽带用户提供接入服务。
本地地址池	本地地址池是 NE20E-X6 自行管理的地址池， NE20E-X6 负责对地址池中的 IP 地址资源进行分配、续租、回收等管理。
本地认证	在 NE20E-X6 上配置用户信息（用户名、密码及其他属性等），由 NE20E-X6 完成对用户的认证。本地认证的优点是速度快，可以降低运营成本；缺点是存储信息量受设备硬件条件限制。
绑定认证	指 NE20E-X6 根据用户接入的位置信息自动生成用户名和密码进行认证。
本地授权	根据 NE20E-X6 配置的用户属性对用户进行授权。
不计费	NE20E-X6 不对用户进行计费。
不认证	表示运营商对用户非常信任，NE20E-X6 对用户不进行合法性检查。一般情况下不建议采用此模式。

D

DHCP 客户端	NE20E-X6 作为 DHCP 客户端，向外部 DHCP/BOOTP 服务器申请 IP 地址，并将申请到的 IP 地址分配给 PPP 用户。
DHCP 服务器	NE20E-X6 作为 DHCP 服务器，从本地地址池中为用户侧用户分配 IP 地址。从中继地址池为网络侧经过 DHCP 代理的用户分配 IP 地址。
DHCP 代理	NE20E-X6 作为 DHCP 代理，将用户的 DHCP 请求转发给外部 DHCP/BOOTP 服务器，由 DHCP/BOOTP 服务器为用户分配 IP 地址。

H

HWTACACS	Huawei TACACS，在 TACACS（RFC 1492）基础上进行了功能增强的一种安全协议。该协议与 RADIUS 协议类似，主要是通过 C/S 模式与 HWTACACS 服务器通信，来实现多种用户的 AAA 功能。
HWTACACS 计费	NE20E-X6 将计费报文送往 HWTACACS 服务器，由 HWTACACS 服务器完成对用户的计费。
HWTACACS 授权	由 HWTACACS 服务器对用户进行授权。
HWTACACS 认证	NE20E-X6 作为客户端，与 HWTACACS 服务器通信。在 HWTACACS 服务器上配置用户信息，NE20E-X6 将用户名和密码通过 HWTACACS 协议传送给 HWTACACS 服务器， HWTACACS 服务器完成对用户的认证并将认证结果反馈给 NE20E-X6。

J

接入业务	提供用户访问网络的基本能力。当用户使用接入业务时，运营商只需针对用户，按流量或时长进行基本的计费即可。
静态用户	指使用固定 IP 地址的用户。用户在自己的计算机上设置固定的 IP 地址，而操作员在 NE20E-X6 上配置该 IP 地址属于合法的用户。

K

快速认证	Web 认证还有一种简化的方法，称为快速认证，是指用户访问 Web 页面，但是无需输入用户名和密码，直接提交认证，由 NE20E-X6 根据用户接入的 BAS（Broadband Access Server）接口信息自动生成用户名和密码（vlan）进行认证。

O

Option 60 选项	某些终端设备（例如数字电视的机顶盒）在接入网络时，NE20E-X6 无法通过用户名方式获知其所属域，也就不能为其分配 IP 地址。此时，可配置该终端设备在发起 DHCP 请求时，通过 Option 60 携带域信息。NE20E-X6 收到 DHCP 报文时，可根据 Option 60 中携带的域信息来分配 IP 地址。
Option 82 信息	外置 DHCP/BOOTP 服务器收到 DHCP 报文时，无法得知用户的物理位置信息，只能在地址池中按顺序为用户分配 IP 地址，无法实现根据用户分配 IP 地址的需求。NE20E-X6 作为 DHCP 代理，在代理用户 DHCP 报文时，可在 Option 82 中填写用户的物理位置信息，通知 DHCP 服务器按此信息对为用户分配 IP 地址。

P

Portal 协议	由华为公司开发，主要用于 Web 服务器和其他设备之间的信息交互。Portal 协议基于客户端/服务器结构，采用 UDP 作为传输协议

Q

强制 Web 认证	强制 Web 认证是指当需要 Web 认证或快速认证的用户，在未认证前试图访问其无权访问的地址时，NE20E-X6 将其访问请求强制重定向到强制 Web 认证服务器，让用户进行认证。

R

RADIUS 计费	NE20E-X6 将计费报文送往 RADIUS 服务器，由 RADIUS 服务器完成对用户的计费。
RADIUS 授权	RADIUS 协议的认证和授权是绑定在一起的，不能单独使用 RADIUS 进行授权。用户认证成功后给将得到授权。
RADIUS 认证	NE20E-X6 作为客户端，与 RADIUS 服务器通信。在 RADIUS 服务器上配置用户信息，NE20E-X6 将用户名和密码通过 RADIUS 协议传送给 RADIUS 服务器， RADIUS 服务器完成对用户的认证并将认证结果反馈给 NE20E-X6。

W

Web 认证	指用户通过访问 Web 认证服务器的认证页面，交互输入用户名和密码进行身份认证的一种认证方法。

Y

域	NE20E-X6 基于域来管理接入用户。每个用户都归属于某个域，同一个域的用户具有相同的业务属性。NE20E-X6 中的用户名格式为“username@domain”，用户所属的域由“@”前或者后的字符串决定。
远端地址池	远端地址池是外部 DHCP（Dynamic Host Configuration Protocol）/BOOTP（Boot Protocol）服务器的一个映像，里面并不配置实际的 IP 地址，只是指明该地址池对应的 DHCP/BOOTP 服务器。使用远端地址池时，NE20E-X6 可以代理用户发起请求或者中继用户的请求，向 DHCP/BOOTP 服务器申请、续组或释放地址。

Z

增值业务	如 VoD、Gaming、Triple Play 等，是用户访问运营商的 Portal 服务器所选择的业务。当用户使用增值业务时，运营商可针对具体业务，按流量或时长进行差异化计费。

直接授权	表示运营商对用户非常信任，直接授权。
中继地址池	中继地址池为网络侧通过中继请求 IP 地址的用户提供 IP 地址。NE20E-X6 负责对地址池中的 IP 地址资源进行分配、续租、回收等管理。

C 缩略语

列出了本手册中使用的缩略语，及对应的英文全称和中文解释。

A

AAA	Authentication, Authorization and Accounting	认证、授权和计费
ACL	Access Control List	访问控制列表
ADSL	Asymmetric Digital Subscriber Line	不对称数字用户线
AP	Access Point	接入点
ARP	Address Resolution Protocol	地址解析协议

B

BAS	Broadband Access Server	宽带接入服务器
BOOTP	Bootstrap Protocol	引导协议
BRAS	Broadband Remote Access Server	宽带远端接入服务器

C

CAR	Committed Access Rate	接入速率限制
CF	Compressed Flash	压缩闪存
CHAP	Challenge Handshake Authentication Protocol	握手认证协议
CLI	Command Line Interface	命令行接口
CMTS	Cable Modem Terminal System	线缆调制解调器终端系统
CoA	Change of Authorization	授权变更
COPS	Common Open Policy Service	公共开放策略服务

D

DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DNS	Domain Name Server	域名服务器
DSLAM	Digital Subscriber Line Access Multiplexer	数字用户线接入复接器

E

EAP	Extensible Authentication Protocol	扩展认证协议
EAPoL	EAP over LAN	局域网承载 EAP

F

FE	Fast Ethernet	快速以太网

G

GE	Gigabit Ethernet	千兆以太网
GRE	Generic Routing Encapsulation	通用路由封装

H

HDLC	High level Data Link Control	高级数据链路控制
HFC	Hybrid Fiber-Coaxial	光纤/同轴混合网
HWTACACS	Huawei TACACS	华为 TACACS

I

IEEE	Institute of Electrical and Electronics Engineers	电气和电子工程师学会
IP	Internet Protocol	网际协议
IPCP	Internet Protocol Control Protocol	IP 控制协议
IPoE	IP over Ethernet	以太网承载 IP 协议
IPoEoVLAN	IP over Ethernet over VLAN	VLAN 标记化的 IPoE
IPoX	IP over X	某种方式承载 IP 协议
IPTN	IP Telecommunication Network	IP 电信网
ISP	Internet Service Provider	Internet 服务提供商

L

LAN	Local Area Network	局域网
LCP	Link Control Protocol	链路控制协议
L2TP	Layer 2 Tunneling Protocol	二层隧道协议
LTS	L2TP Tunnel Switch	L2TP 隧道交换

M

MAC	Media Access Control	媒体接入控制
MSCHAP	Microsoft CHAP	微软 CHAP 协议

N

NCP	Network Control Protocol	网络控制协议
ND	Neighbor Discovery	邻居发现
NetBIOS	Network Basic Input/Output System	网络基本输入输出系统

P

PAP	Password Authentication Protocol	密码验证协议
PDP	Policy Decision Point	策略决策点
PEP	Policy Enforcement Point	策略执行点
PPP	Point-to-Point Protocol	点到点协议
PPPoE	Point-to-Point Protocol over Ethernet	以太网承载 PPP 协议
PPPoEoVLAN	PPPoE over VLAN	VLAN 标记 PPPoE 协议
PPPoX	PPP over X	某种方式承载 PPP 协议
PSTN	Public Switched Telekeywordone Network	公共交换电话网

Q

QinQ	802.1Q in 802.1Q	双层 VLAN tag 封装
QoS	Quality of Service	服务质量

R

RADIUS	Remote Authentication Dial in User Service	远端用户拨入鉴权服务
RFC	Requirement for Comments	征求意见稿
S		
SIG	Safe Immunity Gateway	安全免疫网关
SIM	Subscriber Identity Module	用户标识模块
DSG	Dynamic Service Gateway	业务选择网关
SSH	Secure Shell	安全外壳
T		
TACACS	Terminal Access Controller Access Control System	终端接入控制器接入控制系统
TCP	Transmission Control Protocol	传输控制协议
TFTP	Trivial File Transfer Protocol	简单文件传输协议
U		
UDP	User Datagram Protocol	用户数据包协议
URL	Universal Resource Locator	统一资源定位器
V		
VLAN	Virtual LAN	虚拟局域网
VoD	Video On Demand	视频点播
VPN	Virtual Private Network	虚拟私有网