目 录

1 Portal

说明

VLAN 接口上的 Portal 不支持计费，其它类型接口上的 Portal 支持计费。

1.1 Portal简介

1.1.1 Portal概述

Portal 在英语中是入口的意思。Portal 认证通常也称为 Web 认证，一般将 Portal 认证网站称为门户网站。

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

用户可以主动访问已知的 Portal 认证网站，输入用户名和密码进行认证，这种开始 Portal 认证的方式称作主动认证。反之，如果用户试图通过 HTTP 访问其他外网，将被强制访问 Portal 认证网站，从而开始 Portal 认证过程，这种方式称作强制认证。

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

1.1.2 Portal扩展功能

Portal 的扩展功能主要是指通过强制接入终端实施补丁和防病毒策略，加强网络终端对病毒攻击的主动防御能力。具体扩展功能如下：

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

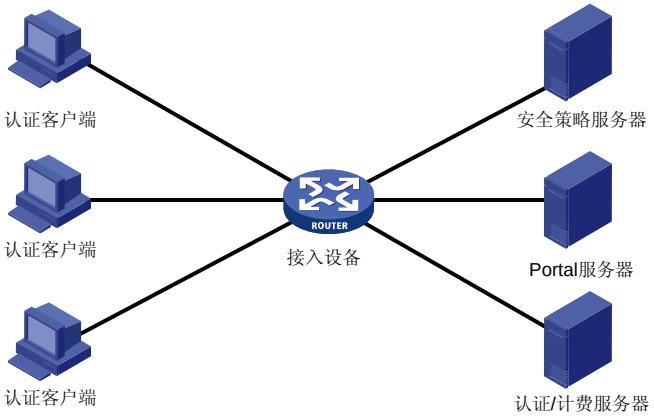
1.1.3 Portal的系统组成

Portal的典型组网方式如 图 1-1 所示，它由五个基本要素组成：认证客户端、接入设备、Portal服务器、认证/计费服务器和安全策略服务器。

说明

由于 Portal 服务器可以是接入设备之外的独立实体，也可以是存在于接入设备之内的内嵌实体，本文称之为“本地 Portal 服务器”，因此下文中除对本地支持的 Portal 服务器做特殊说明之外，其它所有 Portal 服务器均指独立的 Portal 服务器，请勿混淆。

图1-1 Portal 系统组成示意图



1. 认证客户端

安装于用户终端的客户端系统，为运行 HTTP/HTTPS 协议的浏览器或运行 Portal 客户端软件的主机。对接入终端的安全性检测是通过 Portal 客户端和安全策略服务器之间的信息交流完成的。

2. 接入设备

交换机、路由器等宽带接入设备的统称，主要有三方面的作用：

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

3. Portal服务器

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

4. 认证/计费服务器

与接入设备进行交互，完成对用户的认证和计费。

5. 安全策略服务器

与 Portal 客户端、接入设备进行交互，完成对用户的安全认证，并对用户进行授权操作。

以上五个基本要素的交互过程为：

(1) 未认证用户访问网络时，在 Web 浏览器地址栏中输入一个互联网的地址，那么此 HTTP 请求在经过接入设备时会被重定向到 Portal 服务器的 Web 认证主页上；若需要使用 Portal 的扩展认证功能，则用户必须使用 Portal 客户端。

(1) 用户在认证主页/认证对话框中输入认证信息后提交，Portal 服务器会将用户的认证信息传递给接入设备；

(2) 然后接入设备再与认证/计费服务器通信进行认证和计费；

(3) 认证通过后，如果未对用户采用安全策略，则接入设备会打开用户与互联网的通路，允许用户访问互联网；如果对用户采用了安全策略，则客户端、接入设备与安全策略服务器交互，对用户的安全检测通过之后，安全策略服务器根据用户的安全性授权用户访问非受限资源。

说明

- 无论是 Web 客户端还是 H3C iNode 客户端发起的 Portal 认证，均能支持 Portal 认证穿越 NAT，即 Portal 客户端位于私网、Portal 服务器位于公网，接入设备上启用 NAT 功能的组网环境下，NAT 地址转换不会对 Portal 认证造成影响，但建议在此组网环境下，将发送 Portal 报文的源地址配置为接口的公网 IP 地址。
- 目前支持 Portal 认证的远端认证/计费服务器为 RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）服务器。
- 目前通过访问 Web 页面进行的 Portal 认证不能对用户实施安全策略检查，安全检查功能的实现需要与 H3C iNode 客户端配合。

1.1.4 Portal的认证方式

Portal 的三层认证方式支持在接入设备连接用户的三层接口上开启 Portal 认证功能。三层接口 Portal 认证又可分为三种不同的认证方式：直接认证方式、二次地址分配认证方式和可跨三层认证方式。直接认证方式和二次地址分配认证方式下，认证客户端和接入设备之间没有三层转发；可跨三层认证方式下，认证客户端和接入设备之间可以跨接三层转发设备。

1. 直接认证方式

用户在认证前通过手工配置或 DHCP 直接获取一个 IP 地址，只能访问 Portal 服务器，以及设定的免费访问地址；认证通过后即可访问网络资源。认证流程相对二次地址较为简单。

2. 二次地址分配认证方式

用户在认证前通过 DHCP 获取一个私网 IP 地址，只能访问 Portal 服务器，以及设定的免费访问地址；认证通过后，用户会申请到一个公网 IP 地址，即可访问网络资源。该认证方式解决了 IP 地址规划和分配问题，对未认证通过的用户不分配公网 IP 地址。例如运营商对于小区宽带用户只在访问小区外部资源时才分配公网 IP。

说明

使用本地 Portal 服务器的 Portal 认证不支持二次地址分配认证方式。

3. 可跨三层认证方式

和直接认证方式基本相同，但是这种认证方式允许认证用户和接入设备之间跨越三层转发设备。

对于以上三种认证方式，IP 地址都是用户的唯一标识。接入设备基于用户的 IP 地址下发 ACL 对接口上通过认证的用户报文转发进行控制。由于直接认证和二次地址分配认证下的接入设备与用户之

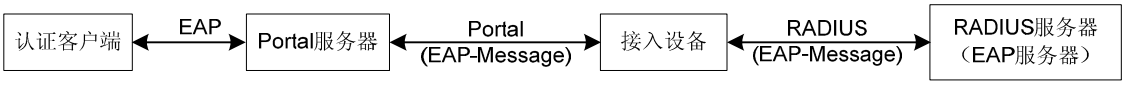
间未跨越三层转发设备，因此接口可以学习到用户的 MAC 地址，接入设备可以利用学习到 MAC 地址增强对用户报文转发的控制力度。

1.1.5 Portal支持EAP认证

在对接入用户身份可靠性要求较高的网络应用中，传统的基于用户名和口令的用户身份验证方式存在一定的安全问题，基于数字证书的用户身份验证方式通常被用来建立更为安全和可靠的网络接入认证机制。

EAP（Extensible Authentication Protocol，可扩展认证协议）可支持多种基于数字证书的认证方式（例如 EAP-TLS），它与 Portal 认证相配合，可共同为用户提供基于数字证书的接入认证服务。

图1-2 Portal 支持 EAP 认证协议交互示意图



如 图 1-2 所示，在Portal支持EAP认证的实现中，客户端与Portal服务器之间交互EAP认证报文，Portal服务器与接入设备之间交互携带EAP-Message属性的Portal协议报文，接入设备与RADIUS服务器之间交互携带EAP-Message属性的RADIUS协议报文，由具备EAP服务器功能的RADIUS服务器处理EAP-Message属性中封装的EAP报文，并给出EAP认证结果。整个EAP认证过程中，接入设备只是对Portal服务器与RADIUS服务器之间的EAP-Message属性进行透传，并不对其进行任何处理，因此接入设备上无需任何额外配置。

说明

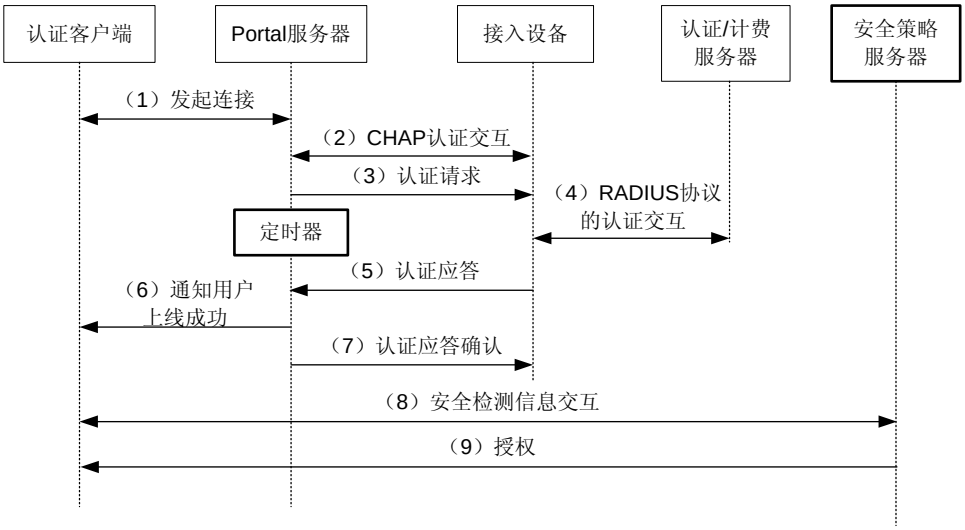
- 该功能仅能与 H3C iMC 的 Portal 服务器以及 H3C iNode Portal 客户端配合使用。
- 目前，仅使用远程 Portal 服务器的三层 Portal 认证支持 EAP 认证。

1.1.6 三层Portal认证过程

直接认证和可跨三层 Portal 认证流程相同。二次地址分配认证流程因为有两次地址分配过程，所以其认证流程和另外两种认证方式有所不同。

1. 直接认证和可跨三层Portal认证的流程（CHAP/PAP认证方式）

图1-3 直接认证/可跨三层 Portal 认证流程图



直接认证/可跨三层 Portal 认证流程：

(1) Portal 用户通过 HTTP 协议发起认证请求。HTTP 报文经过接入设备时，对于访问 Portal 服务器或设定的免费访问地址的 HTTP 报文，接入设备允许其通过；对于访问其它地址的 HTTP 报文，接入设备将其重定向到 Portal 服务器。Portal 服务器提供 Web 页面供用户输入用户名和密码来进行认证。

(2) Portal 服务器与接入设备之间进行 CHAP（Challenge Handshake Authentication Protocol，质询握手验证协议）认证交互。若采用 PAP（Password Authentication Protocol，密码验证协议）认证则直接进入下一步骤。

(3) Portal 服务器将用户输入的用户名和密码组装成认证请求报文发往接入设备，同时开启定时器等待认证应答报文。

(4) 接入设备与 RADIUS 服务器之间进行 RADIUS 协议报文的交互。

(5) 接入设备向 Portal 服务器发送认证应答报文。

(6) Portal 服务器向客户端发送认证通过报文，通知客户端认证（上线）成功。

(7) Portal 服务器向接入设备发送认证应答确认。

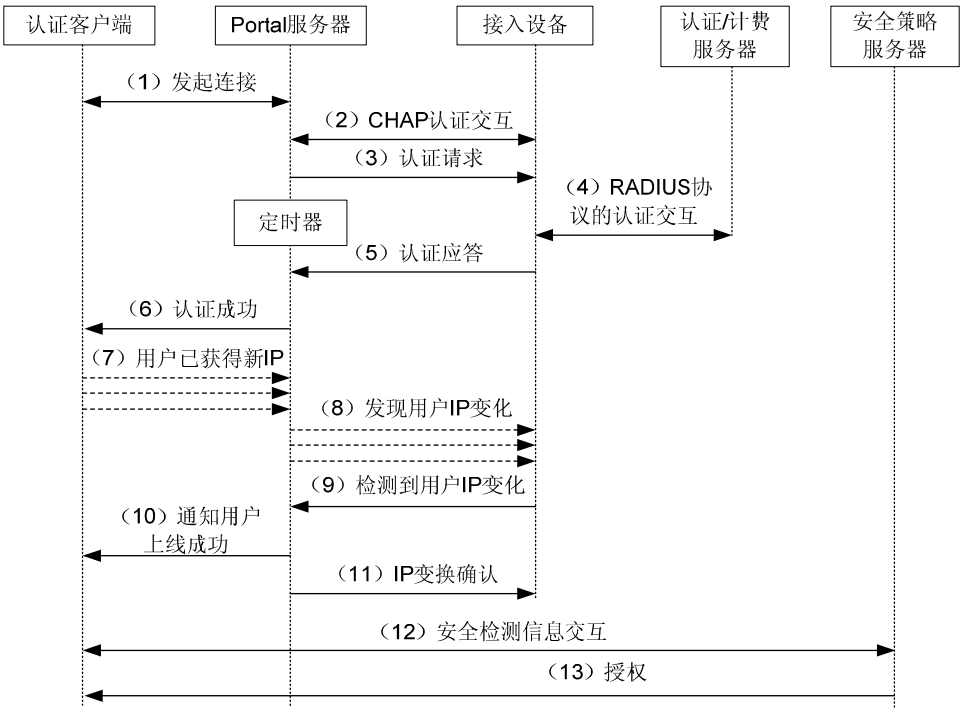
(8) 客户端和安全策略服务器之间进行安全信息交互。安全策略服务器检测接入终端的安全性是否合格，包括是否安装防病毒软件、是否更新病毒库、是否安装了非法软件、是否更新操作系统补丁等。

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

步骤(8)、(9)为 Portal 认证扩展功能的交互过程。

2. 二次地址分配认证方式的流程（CHAP/PAP认证方式）

图1-4 二次地址分配认证方式流程图



二次地址分配认证流程：

(1)～(6)同直接/可跨三层 Portal 认证中步骤（1）～（6）。客户端收到认证通过报文后，通过 DHCP 获得新的公网 IP 地址，并通知 Portal 服务器用户已获得新 IP 地址。

(8) Portal 服务器通知接入设备客户端获得新公网 IP 地址。

(9) 接入设备通过检测 ARP 协议报文发现了用户 IP 变化，并通告 Portal 服务器已检测到用户 IP 变化。

(10) Portal 服务器通知客户端上线成功。

(11) Portal 服务器向接入设备发送 IP 变化确认报文。

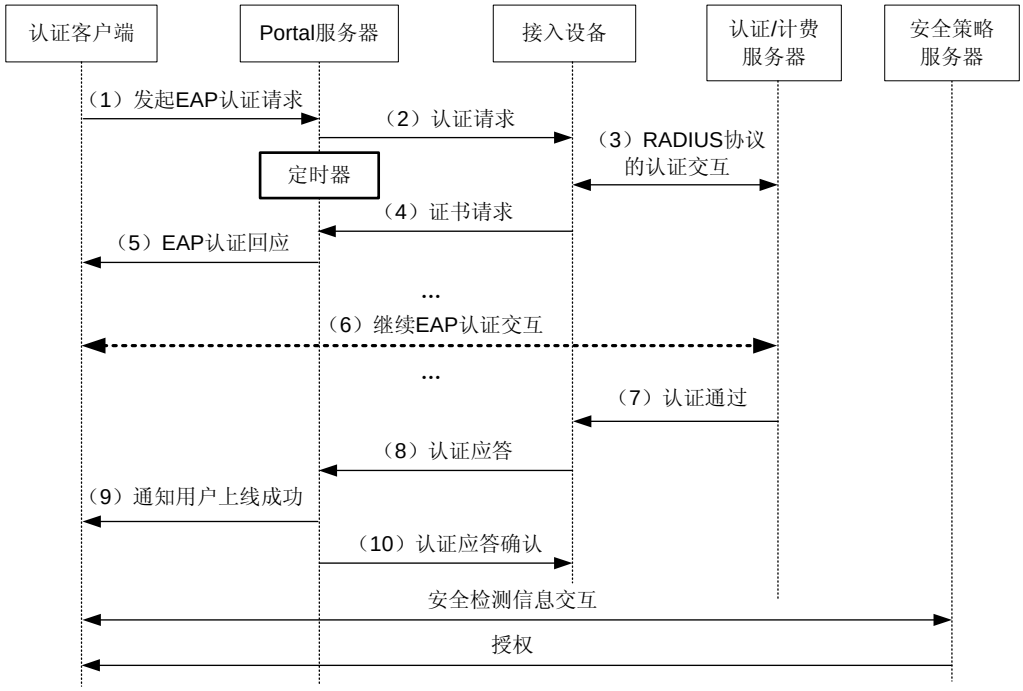
(12) 客户端和安全策略服务器之间进行安全信息交互。安全策略服务器检测接入终端的安全性是否合格，包括是否安装防病毒软件、是否更新病毒库、是否安装了非法软件、是否更新操作系统补丁等。

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

步骤(12)、(13)为 Portal 认证扩展功能的交互过程。

3. Portal支持EAP认证流程

图1-5 Portal 支持 EAP 认证流程图



支持 EAP 认证的 Portal 认证流程如下（各 Portal 认证方式下 EAP 认证的处理流程相同，此处仅以直接方式的 Portal 认证为例）：

(1) Portal 客户端发起 EAP 认证请求，向 Portal 服务器发送 Identity 类型的 EAP 请求报文。

(2) Portal 服务器向接入设备发送 Portal 认证请求报文，同时开启定时器等待 Portal 认证应答报文，该认证请求报文中包含若干个 EAP-Message 属性，这些属性用于封装 Portal 客户端发送的 EAP 报文，并可携带客户端的证书信息。

(3) 接入设备接收到 Portal 认证请求报文后，构造 RADIUS 认证请求报文与 RADIUS 服务器进行认证交互，该 RADIUS 认证请求报文的 EAP-Message 属性值由接入设备收到的 Portal 认证请求报文中的 EAP-Message 属性值填充。

(4) 接入设备根据 RADIUS 服务器的回应信息向 Portal 服务器发送证书请求报文，该报文中同样会包含若干个 EAP-Message 属性，可用于携带 RADIUS 服务器的证书信息，这些属性值由 RADIUS 认证回应报文中的 EAP-Message 属性值填充。

(5) Portal 服务器接收到证书请求报文后，向 Portal 客户端发送 EAP 认证回应报文，直接将 RADIUS 服务器响应报文中的 EAP-Message 属性值透传给 Portal 客户端。

(6) Portal 客户端继续发起的 EAP 认证请求，与 RADIUS 服务器进行后续的 EAP 认证交互，期间 Portal 认证请求报文可能会出现多次。后续认证过程与第一个 EAP 认证请求报文的交互过程类似，仅 EAP 报文类型会根据 EAP 认证阶段发展有所变化，此处不再详述。

(7) EAP 认证通过后，RADIUS 服务器向接入设备发送认证通过响应报文，该报文的 EAP-Message 属性中封装了 EAP 认证成功报文（EAP-Success）。

(8) 接入设备向 Portal 服务器发送认证应答报文，该报文的 EAP-Message 属性中封装了 EAP 认证成功报文。

(9) Portal 服务器根据认证应答报文中的认证结果通知 Portal 客户端认证成功。

(10) Portal 服务器向接入设备发送认证应答确认。

后续为 Portal 认证扩展功能的交互过程，可参考 CHAP/PAP 认证方式下的认证流程介绍，此处略。

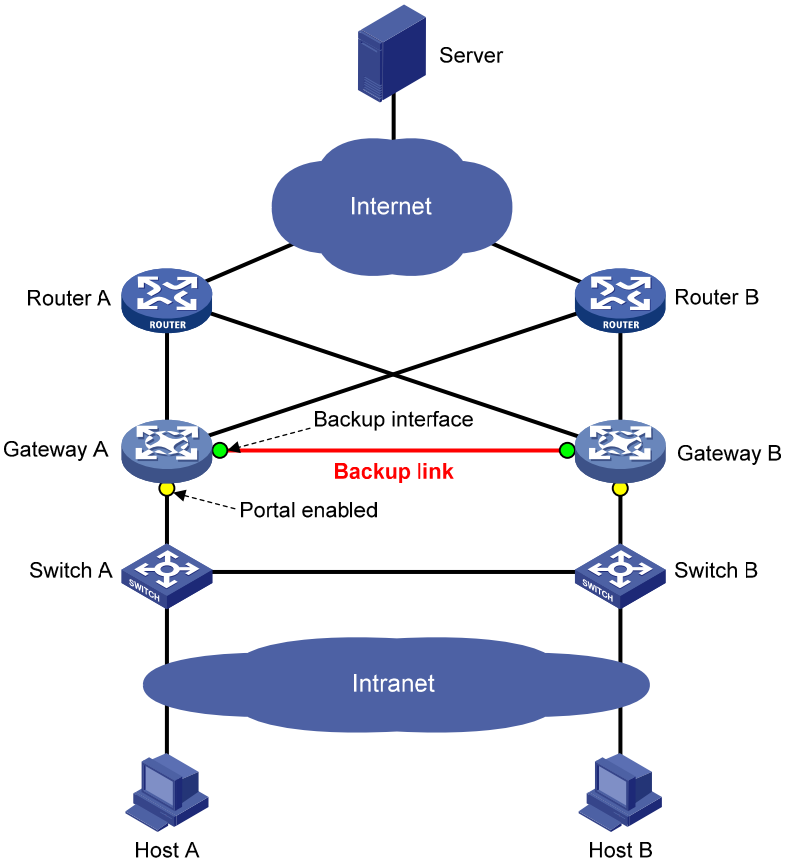
1.1.7 Portal支持双机热备

1. 概述

在当前的组网应用中，用户对网络可靠性的要求越来越高，特别是在一些重点的业务入口或接入点上需要保证网络业务的不间断性。双机热备技术可以保证这些关键业务节点在单点故障的情况下，信息流仍然不中断。

所谓双机热备，其实是双机业务备份。可以分别指定两台设备上的任意一个支持备份接口功能的以太网接口为备份接口，两个备份接口直接相连，不通过交换机。在设备正常工作时，对业务信息进行主备同步；在设备故障后，利用 VRRP 机制实现业务流量切换到备份设备，由备份设备继续处理业务，从而保证了当前的业务不被中断。关于双机热备的详细介绍请参见“可靠性配置指导”中的“双机热备”。

图1-6 双机热备组网图



如 图 1-6 所示，在一个典型的Portal双机热备组网环境中，用户通过Portal认证接入网络，为避免接入设备单机故障的情况下造成的Portal业务中断，接入设备提供了Portal支持双机热备功能。该功能是指，接入设备Gateway A和Gateway B通过备份链路互相备份两台设备上的Portal在线用户信息，

实现当其中一台设备发生故障时，另外一台设备可以对新的Portal用户进行接入认证，并能够保证所有已上线Portal用户的正常数据通信。

2. 基本概念

(1) 设备的工作状态

- 独立运行状态：设备未与其它设备建立备份连接时所处的一种稳定状态。
- 同步运行状态：设备与对端设备之间成功建立备份连接，可以进行数据备份时所处的一种稳定状态。

(2) 用户的工作模式

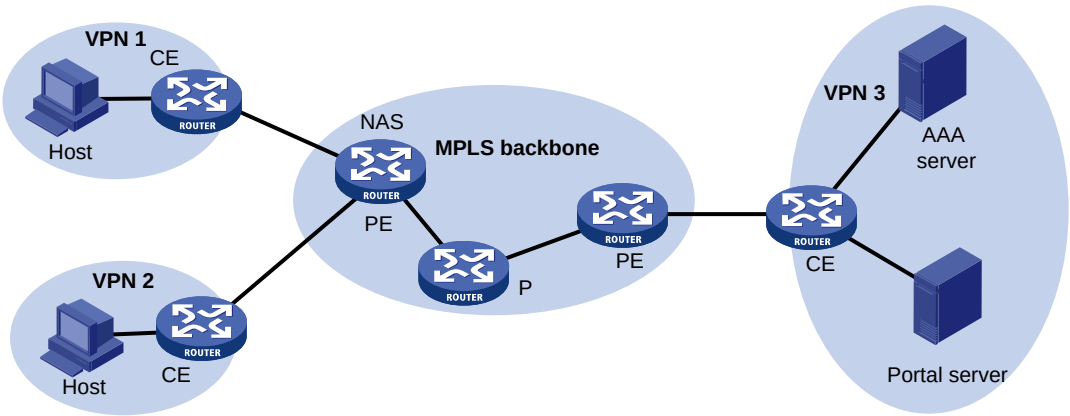
- Stand-alone：表示用户数据只在一台设备上存在。当前设备处于独立运行状态，或者当前设备处于同步运行状态但用户数据还未同步。
- Primary：表明用户是由本端设备上线，用户数据由本端设备生成。本端设备处于同步运行状态，可以处理并接收服务器发送的报文。
- Secondary：表明用户是由对端设备上线，用户数据是由对端设备同步到本端设备上的。本端设备处于同步运行状态，只接收并处理同步消息，不处理服务器发送的报文。

1.1.8 Portal支持多实例

实际组网应用中，某企业的各分支机构属于不同的 VPN，且各 VPN 之间的业务相互隔离。如果各分支机构的 Portal 用户要通过位于总部 VPN 中的服务器进行统一认证，则需要 Portal 支持多实例。

通过 Portal 支持多实例，可实现 Portal 认证报文通过 MPLS VPN 进行交互。如下图所示，连接客户端的 PE 设备作为 NAS，通过 MPLS VPN 将私网客户端的 Portal 认证报文透传给网络另一端的私网服务器，并在 AAA 支持多实例的配合下，实现对私网 VPN 客户端的 Portal 接入认证，满足了私网 VPN 业务隔离情况下的客户端集中认证，且各私网的认证报文互不影响。

图1-7 Portal 支持多实例典型组网图



说明

- 在 MCE 设备上进行的 Portal 接入认证也可支持多实例功能。关于 MCE 的相关介绍请见参见“MPLS 配置指导”中的“MPLS L3VPN”。
- 关于 AAA 支持多实例的相关介绍请参见“安全配置指导”中的“AAA”。
- 本特性不支持多 VPN 间的地址重叠。
- 本特性不支持在网关模式下工作。

1.2 Portal配置任务简介

表1-1 三层 Portal 配置任务简介

配置任务		说明	详细配置
指定三层Portal认证的Portal服务器		必选	1.4
使能三层Portal认证		必选	1.5
控制Portal用户的接入	配置免认证规则	可选	1.6.1
	配置源认证网段		1.6.2
	配置目的认证网段		1.6.3
	配置Portal最大用户数		1.6.4
	指定Portal用户使用的认证域		1.6.5
配置接口发送RADIUS报文的相关属性	配置接口发送RADIUS报文的NAS-ID	可选	1.7.1
	配置接口的NAS-Port-Type		1.7.2
	配置接口的NAS-Port-ID		1.7.3
	配置接口的NAS-ID Profile		1.7.4 1.7.3 1.7.3
配置接口发送Portal报文使用的源地址		可选	1.8
配置Portal支持双机热备		可选	1.9
指定Portal用户认证成功后认证页面的自动跳转目的网站地址		可选	1.10
配置Portal探测功能	配置三层Portal用户的在线探测功能	可选	1.11.1
	配置Portal服务器探测功能		1.11.2
	配置Portal用户信息同步功能		1.11.3
强制Portal用户下线		可选	1.12

1.3 配置准备

Portal 提供了一个用户身份认证和安全认证的实现方案，但是仅仅依靠 Portal 不足以实现该方案。接入设备的管理者需选择使用 RADIUS 认证方法，以配合 Portal 完成用户的身份认证。Portal 认证的配置前提：

- Portal 服务器、RADIUS 服务器已安装并配置成功。本地 Portal 认证无需单独安装 Portal 服务器。
- 若采用二次地址分配认证方式，接入设备需启动 DHCP 中继的安全地址匹配检查功能，另外需要安装并配置好 DHCP 服务器。
- 用户、接入设备和各服务器之间路由可达。
- 如果通过远端 RADIUS 服务器进行认证，则需要在 RADIUS 服务器上配置相应的用户名和密码，然后在接入设备端进行 RADIUS 客户端的相关设置。RADIUS 客户端的具体配置请参见“安全配置指导”中的“AAA”。
- 如果需要支持 Portal 的扩展功能，需要安装并配置 CAMS EAD/iMC EAD。同时保证在接入设备上的 ACL 配置和安全策略服务器上配置的受限资源 ACL 号、非受限资源 ACL 号对应。接入设备上的安全策略服务器配置请参见“安全配置指导”中的“AAA”。

说明

- 安全策略服务器的配置请参考 CAMS EAD 安全策略组件联机帮助/iMC EAD 安全策略组件联机帮助。
- 受限资源 ACL、非受限资源 ACL 分别对应安全策略服务器中的隔离 ACL 与安全 ACL。
- 如果接入设备上的授权 ACL 配置被修改，则修改后的 ACL 不对已经在线的 Portal 用户生效，只能对新上线的 Portal 用户有效。

1.4 指定三层Portal认证的Portal服务器

本配置用于指定 Portal 服务器的相关参数，主要包括服务器 IP 地址、共享加密密钥、服务器端口号以及服务器提供的 Web 认证地址。

表1-2 指定三层 Portal 认证的 Portal 服务器

操作	命令	说明
进入系统视图	**system-view**	-
指定三层Portal认证的Portal服务器	**portal server** *server-name* **ip** *ip-address* [**key** [**cipher** | **simple**] *key-string* | **port** *port-id* | **server-type** { **cmcc** | **imc** } | **url** *url-string* | **vpn-instance** *vpn-instance-name*] *	必选 缺省情况下，没有指定三层Portal认证的Portal服务器

说明

- 已配置的 Portal 服务器参数仅在该 Portal 服务器未被接口引用时才可以被删除或修改。
- 为保证设备能够向 MPLS VPN 私网中的 Portal 服务器发送报文，指定 Portal 服务器时需指定服务器所属的 VPN 且必须和该服务器所在的 VPN 保持一致。

1.5 使能三层Portal认证

只有在接口上使能了 Portal 认证，对接入用户的 Portal 认证功能才能生效。

在使能三层 Portal 认证之前，需要满足以下要求：

- 使能 Portal 的接口已配置或者获取了合法的 IP 地址；
- 使能 Portal 的接口未加入聚合组；
- 接口上引用的 Portal 服务器名已经存在；

表1-3 使能三层 Portal 认证

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	- 只能是三层接口
在接口上使能三层Portal认证	**portal server** *server-name* **method** { **direct** | **layer3** | **redhcp** }	必选 缺省情况下，没有使能三层Portal认证

说明

- 在部分设备的三层接口上可以同时使能直接或可跨三层方式的 Portal 认证和 802.1X 认证，且只要用户通过任何一种类型的认证，都可成功接入网络。若在三层接口上同时使能二次地址方式的 Portal 认证和 802.1X 认证，Portal 认证会失效。关于 802.1X 的配置介绍请参见“安全配置指导”中的 “802.1X”。
- 设备向 Portal 服务器主动发送报文时使用的目的端口号必须与远程 Portal 服务器实际使用的端口号保持一致。
- 已配置的 Portal 服务器及其参数仅在该 Portal 服务器未被接口引用时才可以被删除或修改。
- 对于跨三层设备支持 Portal 认证的应用只能配置可跨三层 Portal 认证方式（**portal server** *server-name* **method layer3**），但可跨三层 Portal 认证方式不要求接入设备和 Portal 用户之间必需跨越三层设备。
- 在二次地址分配认证方式下，允许用户在未通过 Portal 认证时以公网地址向外发送报文，但相应的回应报文则受限制。

1.6 控制Portal用户的接入

1.6.1 配置免认证规则

通过配置免认证规则(free-rule)可以让特定的用户不需要通过 Portal 认证即可访问外网特定资源，这是由免认证规则中配置的源信息以及目的信息决定的。

免认证规则的匹配项包括 IP 地址、TCP/UDP 端口号、MAC 地址、所连接设备的接口和 VLAN，只有符合免认证规则的用户报文才不会触发 Portal 认证，因此这些报文所属的用户才可以直接访问网络资源。

表1-4 配置免认证规则

操作	命令	说明
进入系统视图	**system-view**	-
配置Portal的免认证规则	**portal free-rule** *rule-number* { **destination** { **any** | **ip** { *ip-address* **mask** { *mask-length* | *mask* } | **any** } [**tcp** *tcp-port-number* [**to** *tcp-port-number*] | **udp** *udp-port-number* [**to** *udp-port-number*]] } | **source** { **any** | [**interface** *interface-type interface-number* | **ip** { *ip-address* **mask** { *mask-length* | *mask* } | **any** } [**tcp** *tcp-port-number* [**to** *tcp-port-number*] | **udp** *udp-port-number* [**to** *udp-port-number*]] | **mac** *mac-address* | **vlan** *vlan-id*]] * } } *	必选

说明

- 如果免认证规则中同时配置了 **vlan** 和 **interface** 项，则要求 **interface** 属于该 VLAN，否则该规则无效。
- 相同内容的免认证规则不能重复配置，否则提示免认证规则已存在或重复。
- 无论接口上是否使能 Portal 认证，只能添加或者删除免认证规则，不能修改。
- 加入聚合组的二层接口不能被指定为免认证规则的源接口，反之亦然。

1.6.2 配置源认证网段

说明

本特性仅三层 Portal 认证支持。

通过配置源认证网段实现只允许在源认证网段范围内的用户 HTTP 报文才能触发 Portal 认证。如果未认证用户的 HTTP 报文既不满足免认证规则又不在源认证网段内，则将被接入设备丢弃。

表1-5 配置源认证网段

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置源认证网段	**portal auth-network** *network-address* { *mask-length* | *mask* }	可选 缺省情况下，源认证网段为0.0.0.0/0，表示对来自任意网段的用户都进行Portal认证

说明

- 源认证网段配置仅对可跨三层 Portal 认证有效。直接认证方式的认证网段为任意源 IP，二次地址分配方式的认证网段为由接口私网 IP 决定的私网网段。
- 可通过多次执行本命令，配置多个源认证网段，最多允许配置的源认证网段和目的认证网段总数为 16。
- 如果接口下同时配置了源认证网段和目的认证网段，则源认证网段的配置无效。

1.6.3 配置目的认证网段

说明

本特性仅三层 Portal 认证支持。

通过配置目的认证网段实现仅要求访问指定目的网段（除免认证规则中指定的目的 IP 地址或网段）的用户进行 Portal 认证，其它用户访问外部网络时无需认证。

表1-6 配置目的认证网段

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置目的认证网段	**portal auth-network destination** *network-address* { *mask-length* | *mask* }	可选 缺省情况下，目的认证网段为0.0.0.0/0，表示对访问任意网段的用户都进行Portal认证

说明

- 可通过多次执行本命令，配置多个目的认证网段，最多允许配置的源认证网段和目的认证网段总数为 16。
- 如果接口下同时配置了源认证网段和目的认证网段，则源认证网段的配置无效。

1.6.4 配置Portal最大用户数

通过该配置可以控制系统中的 Portal 接入用户总数。

表1-7 配置 Portal 最大用户数

操作	命令	说明
进入系统视图	**system-view**	-
配置Portal最大用户数	**portal max-user** *max-number*	必选 缺省情况下，Portal最大用户数为系统支持的最大值

说明

如果配置的 Portal 最大用户数小于当前已经在线的 Portal 用户数，则该命令可以执行成功，且在线 Portal 用户不受影响，但系统将不允许新的 Portal 用户接入。

1.6.5 指定Portal用户使用的认证域

通过在指定接口上配置 Portal 用户使用的认证域，使得所有从该接口接入的 Portal 用户被强制使用指定的认证域来进行认证、授权和计费。即使 Portal 用户输入的用户名中携带的域名相同，接入设备的管理员也可以通过该配置对不同接口指定不同的认证域，从而增加了管理员部署 Portal 接入策略的灵活性。

表1-8 指定 Portal 用户使用的认证域

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
指定Portal用户使用的认证域	**portal domain** *domain-name*	必选 缺省情况下，未指定Portal用户使用的认证域

说明

从指定接口上接入的 Portal 用户将按照如下先后顺序选择认证域：接口上指定的 ISP 域-->用户名中携带的 ISP 域-->系统缺省的 ISP 域。关于缺省 ISP 域的相关介绍请参见“安全配置指导”中的“AAA”。

1.7 配置接口发送RADIUS报文的相关属性

说明

本特性仅三层 Portal 认证支持。

1.7.1 配置接口发送RADIUS报文的NAS-ID

若设备使用 RADIUS 服务器对 Portal 用户进行认证/授权/计费，则当接口上有 Portal 用户上线时，设备会向 RADIUS 服务器发送 RADIUS 请求报文，并使用 RADIUS 请求报文中携带的 NAS-Identifier 属性来向 RADIUS 服务器标识自己。该属性值可在系统视图下或者接口视图下进行配置，接口上的配置优先，若接口上没有配置，则使用系统视图下的全局配置。

表1-1 配置接口发送 RADIUS 报文的 NAS-ID

操作		命令	说明
进入系统视图		**system-view**	-
配置接口发送RADIUS报文的NAS-ID	系统视图	**portal nas-id** *nas-identifier*	必选 缺省情况下，使用命令**sysname**配置的设备名作为接口发送RADIUS报文的NAS ID **sysname**的具体配置请参见“基础配置命令参考”中的“设备管理”
	接口视图	**interface** *interface-type interface-number*	
		portal nas-id *nas-identifier*	

1.7.2 配置接口的NAS-Port-Type

RADIUS 标准属性 NAS-Port-Type 用于表示用户接入的端口类型。当接口上有 Portal 用户上线时候，若该接口上配置了 NAS-Port-Type，则使用本命令配置的值作为向 RADIUS 服务器发送的 RADIUS 请求报文的 NAS-Port-Type 属性值，否则使用接入设备获取到的用户接入的端口类型填充该属性。

若作为 Portal 认证接入设备的 BAS（Broadband Access Server，宽带接入服务器）与 Portal 客户端之间跨越了多个网络设备，则可能无法正确获取到接入用户的实际端口信息。

表1-9 配置接口的 NAS-Port-Type

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
进入接口视图	**interface** *interface-type interface-number*	-
配置接口的NAS-Port-Type	**portal nas-port-type** { **ethernet** | **wireless** }	必选 缺省情况下，未指定接口的NAS-Port-Type

1.7.3 配置接口的NAS-Port-ID

Portal 用户进行 RADIUS 认证时，设备发送给 RADIUS 服务器的请求请求报文中需要携带 NAS-Port-ID 属性。该属性值的使用情况与具体的 Portal 服务器配置相关。

表1-1 配置接口的 NAS-Port-ID

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置接口的NAS-Port-ID	**portal nas-port-id** *nas-port-id-value*	必选 缺省情况下，未指定接口的NAS-Port-ID，RADIUS请求报文中的NAS-Port-ID属性值为接入设备获取到的Portal用户接入的物理接口信息

1.7.4 配置接口的NAS-ID Profile

在某些组网环境下，依靠 VLAN 来确定用户的接入位置，网络运营商需要使用 NAS-Identifier 来标识用户的接入位置。当接口上有 Portal 用户上线时，若该接口上指定了 NAS-ID Profile，则接入设备会根据指定的 Profile 名字和用户接入的 VLAN 来获取与此 VLAN 绑定的 NAS-ID，此 NAS-ID 的值将作为向 RADIUS 服务器发送的 RADIUS 请求报文中的 NAS-Identifier 属性值。

本特性中指定的 Profile 名字用于标识 VLAN 和 NAS-ID 的绑定关系，该绑定关系由 AAA 中的 **nas-id** *id-value* **bind vlan** *vlan-id* 命令生成，有关该命令的具体情况请参见“安全命令参考”中的“AAA”。

在接口上未指定 NAS-ID Profile 或指定的 Profile 中没有找到匹配的绑定关系的情况下，若接口上已通过命令 **portal nas-id** 命令配置了 NAS-ID，则使用该 NAS-ID 作为接口的 NAS-ID；若接口上不支持或未配置 **portal nas-id** 命令，则使用设备名作为接口的 NAS-ID。

表1-10 配置接口的 NAS-ID Profile

操作	命令	说明
进入系统视图	**system-view**	-
创建NAS-ID Profile，并进入NAS-ID-Profile视图	**aaa nas-id profile** *profile-name*	必选 该命令的具体情况请参见“安全命令参考”中的“AAA”

操作	命令	说明
设置NAS-ID与VLAN的绑定关系	**nas-id** *nas-identifier* **bind vlan** *vlan-id*	必选 该命令的具体情况请参见“安全命令参考”中的“AAA”
退出当前视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
指定接口的NAS-ID Profile	**portal nas-id-profile** *profile-name*	必选 缺省情况下，未指定NAS-ID Profile

1.8 配置接口发送Portal报文使用的源地址

说明

本特性仅三层 Portal 认证支持。

通过在使能 Portal 的接口上配置发送 Portal 报文使用的源地址，可以保证接入设备以此 IP 地址为源地址向 Portal 服务器发送报文，且 Portal 服务器向接入设备回应的报文以此 IP 地址为目的地址。

表1-11 配置接口发送 Portal 报文使用的源地址

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置接口发送Portal报文使用的源地址	**portal nas-ip** *ip-address*	可选 缺省情况下，未指定源地址，即以接入用户的接口地址作为发送Portal报文的源地址 在NAT组网环境下，此地址建议配置为接口的公网IP地址

1.9 配置Portal支持双机热备

说明

本特性仅三层 Portal 认证支持。

SR6600/SR6600-X 路由器各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	特性	描述
SR6602	配置Portal支持双机热	支持

型号	特性	描述
SR6602-X	备	不支持
SR6604/SR6608/SR6616		不支持
SR6604-X/SR6608-X/SR6616-X		不支持

为实现 Portal 支持双机热备，在保证实现业务流量切换的 VRRP 机制工作正常的前提下，还需要完成以下配置任务：

- 指定备份 Portal 业务所涉及的接口，（与传输状态协商报文和备份数据的备份接口相区别）本文简称为业务备份接口，并在该业务备份接口上使能 Portal。
- 配置业务备份接口所属的 Portal 备份组，两台设备上有备份关系的业务备份接口属于同一个 Portal 备份组。
- 配置双机热备模式下的设备 ID，保证设备上用户的全局唯一性，该设备 ID 必须不同于对端的设备 ID。
- 配置设备发送 RADIUS 报文的备份源 IP 地址，使得对端设备也能够收到服务器发送的报文。备份源 IP 地址必须指定为对端设备发送 RADIUS 报文使用的源 IP 地址。（此配置可选）
- 指定备份接口，并使能双机热备功能，相关配置请参考“可靠性配置指导”的“双机热备”。

对端设备上也需要完成以上配置，才能保证双机热备环境下的 Portal 业务备份正常进行。

当双机工作状态由独立运行状态转换为同步运行状态，且 Portal 备份组已生效时，两台设备上已经上线的 Portal 用户数据会开始进行相互的备份。

表1-12 配置 Portal 支持双机热备

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置业务备份接口所属的Portal备份组	**portal backup-group** *group-id*	必选 缺省情况下，业务备份接口不属于任何Portal备份组 相互备份的两台设备上业务备份接口所属的Portal备份组必须相同
退回系统视图	**quit**	-
配置双机热备模式下的设备ID	**nas device-id** *device-id*	必选 缺省情况下，设备运行在单机模式下，无设备ID 具体配置请参考“安全命令参考”中的“AAA”
指定设备发送RADIUS报文使用的备份源IP地址	**radius nas-backup-ip** *ip-address* [**vpn-instance** *vpn-instance-name*]	二者可选其一 缺省情况下，未指定发送RADIUS报

操作	命令	说明
	radius scheme *radius-scheme-name* **nas-backup-ip** *ip-address*	文使用的备份源IP地址 若将设备发送RADIUS报文使用的源IP地址指定为VRRP上行链路所在备份组的虚拟IP地址，则不需要本配置 具体配置请参考“安全命令参考”中的“AAA”

- 双机热备模式下，设备不支持业务备份接口使能二次地址方式的 Portal 认证。
- 工作于双机热备模式下的任何一台设备上的用户被强制下线，都会导致另外一台设备上的相同用户信息同时被删除。设备和 Portal 服务器上均可执行强制用户下线操作，例如，设备上可通过执行命令 **cut connetion**、**portal delete-user** 来强制用户下线。
- 互为备份的两台设备上的 AAA 及 Portal 的相关配置必须保持一致，比如两台设备上都必须配置相同的 Portal 服务器。

- 由于配置或改变设备的设备 ID 会导致设备上所有在线用户被强制下线，因此需慎重操作，并建议该配置成功执行后，保存配置并重启设备。
- 在双机热备运行的情况下，不要删除已配置的备份源 IP 地址，否则可能会导致备份设备上的在线用户无法收到服务器发送的报文。

1.10 指定Portal用户认证成功后认证页面的自动跳转目的网站地址

在未认证用户登录到 Portal 认证页面进行认证的情况下，当用户输入正确的认证信息且认证成功后，若设备上指定了认证页面的自动跳转目的网站地址，则认证成功的用户将被强制登录到该指定的目的网站页面。

表1-13 指定 Portal 用户认证成功后认证页面的自动跳转目的 URL

配置步骤	命令	说明
进入系统视图	**system-view**	-
指定Portal用户认证成功后认证页面的自动跳转目的网站地址	**portal redirect-url** *url-string*	必选 缺省情况下，用户认证成功后认证页面将会跳转到用户初始访问的网站页面

说明

对于三层远程 Portal 认证，该特性需要与支持自动跳转页面功能的 iMC Portal 服务器配合使用。

1.11 配置Portal探测功能

说明

本特性仅直接和二次地址分配方式的三层 Portal 认证支持。

1.11.1 配置三层Portal用户在线探测功能

SR6600/SR6600-X 路由器各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	特性	描述
SR6602	配置三层Portal用户在线探测功能	支持
SR6602-X		支持
SR6604/SR6608/SR6616		不支持
SR6604-X/SR6608-X/SR6616-X		不支持

在接口上配置 Portal 用户在线探测功能后，设备会定期向从该接口上线的 Portal 在线用户发送探测报文（目前支持发送 ARP 请求），来确认该用户是否在线，以便及时发现异常离线用户。

- 若设备在指定的探测次数之内收到了该 Portal 用户的响应报文，则认为此用户在线，并通过继续发送探测报文，来持续确认该用户的在线状态。
- 若设备在指定的探测次数之后仍然未收到该 Portal 用户的响应报文，则认为此用户已经下线，则停止发送探测报文，并删除该用户。

表1-14 配置三层 Portal 用户在线探测功能

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置三层Portal用户在线探测功能	**access-user detect type arp retransmit** *number* **interval** *interval*	必选 缺省情况下，未配置三层Portal用户在线探测功能

说明

探测报文的发送次数和发送间隔请根据网络的实际情况进行调整。

1.11.2 配置Portal服务器探测功能

在 Portal 认证的过程中，如果接入设备与 Portal 服务器的通信中断，则会导致新用户无法上线，已经在线的 Portal 用户无法正常下线的问题。为解决这些问题，需要接入设备能够及时探测到 Portal 服务器可达状态的变化，并能触发执行相应的操作来应对这种变化带来的影响。例如，当接入设备发现 Portal 服务器不可达时，可打开网络限制，允许 Portal 用户不需经过认证即可访问网络资源，也就是通常所说的 Portal 逃生功能，该功能为一种灵活的用户接入方案。

通过配置本特性，设备可以对指定 Portal 服务器的可达状态进行探测，具体配置包括如下几项：

(1) 探测方式（可以选择其中一种或同时使用两种）

- 探测 HTTP 连接：接入设备定期向 Portal 服务器的 HTTP 服务端口发起 TCP 连接，若连接成功建立则表示此服务器的 HTTP 服务已开启，就认为一次探测成功且服务器可达。若连接失败则认为一次探测失败。
- 探测 Portal 心跳报文：支持 Portal 逃生心跳功能的 Portal 服务器（目前仅 iMC 支持）会定期向接入设备发送 Portal 心跳报文，设备通过检测此报文来判断服务器的可达状态：若设备在指定的周期内收到 Portal 心跳报文或者其它认证报文，且验证其正确，则认为此次探测成功且服务器可达，否则认为此次探测失败。

(2) 探测参数

- 探测间隔：进行探测尝试的时间间隔。
- 失败探测的最大次数：允许连续探测失败的最大次数。若连续探测失败数目达到此值，则认为服务器不可达。

(3) 可达状态改变时触发执行的操作（可以选择其中一种或同时使用多种）

- 发送 Trap：Portal 服务器可达或者不可达的状态改变时，向网管服务器发送 Trap 信息。Trap 信息中记录了 Portal 服务器名以及该服务器的当前状态。
- 发送日志：Portal 服务器可达或者不可达的状态改变时，发送日志信息。日志信息中记录了 Portal 服务器名以及该服务器状态改变前后的状态。
- 打开网络限制（Portal 逃生）：Portal 服务器不可达时，暂时取消端口进行的 Portal 认证，允许该端口接入的所有 Portal 用户访问网络资源。之后，若设备收到 Portal 服务器的心跳报文，或者收到其它认证报文（上线报文、下线报文等），则恢复该端口的 Portal 认证功能。

对于以上配置项，可根据实际情况进行组合使用，但需要注意以下几点：

- 如果同时指定了两种探测方式，则只要使用任何一种探测方式进行探测的失败次数达到最大值就认为服务器不可达。在服务器不可达状态下，只有使用两种探测方式的探测都成功才能认为服务器恢复为可达状态。
- 如果同时指定了多种操作，则 Portal 服务器可达状态改变时系统可并发执行多种操作。
- 对指定 Portal 服务器配置的探测功能，只有接口上使能了 Portal 认证并引用该 Portal 服务器之后才能生效。

表1-15 配置 Portal 服务器探测功能

操作	命令	说明
进入系统视图	**system-view**	-
配置对Portal服务器的探测功能	**portal server** *server-name* **server-detect method** { **http** | **portal-heartbeat** } * **action** { **log** | **permit-all** | **trap** } * [**interval** *interval*] [**retry** *retries*]	必选 缺省情况下，未配置对Portal服务器的探测功能 本命令中指定的Portal服务器必须已经存在

只有对于支持 Portal 逃生心跳功能（目前仅 iMC 的 Portal 服务器支持）的 Portal 服务器，**portal-heartbeat** 类型的探测方法才有效。为了配合此类型的探测，还需要在 Portal 服务器上选择支持逃生心跳功能，并要求此处的 **interval** 与 **retry** 参数值的乘积大于等于 Portal 服务器上的逃生心跳间隔时长，其中 **interval** 取值最好大于 Portal 服务器的逃生间隔时长。

1.11.3 配置Portal用户信息同步功能

为了解决接入设备与 Portal 服务器通信中断后，两者的 Portal 用户信息不一致问题，设备提供了一种 Portal 用户信息同步功能。该功能利用了 Portal 同步报文的发送及检测机制，具体实现如下：

(1) 由 Portal 服务器周期性地（周期为 Portal 服务器上指定的用户心跳间隔值）将在线用户信息通过用户同步报文发送给接入设备；

(2) 接入设备检测到该用户同步报文后，将其中携带的用户信息与自己的用户信息进行对比，如果发现同步报文中有设备上不存在的用户信息，则将这些自己没有的用户信息反馈给 Portal 服务器，Portal 服务器将删除这些用户信息；如果发现接入设备上的某用户信息在连续 N（N 为 **retry** 参数的取值）个周期内，都未在该 Portal 服务器发送过来的用户同步报文中出现过，则认为 Portal 服务器上已不存在该用户，设备将强制该用户下线。

表1-16 配置 Portal 用户同步功能

操作	命令	说明
进入系统视图	**system-view**	-
配置Portal用户同步功能	**portal server** *server-name* **user-sync** [**interval** *interval*] [**retry** *retries*]	必选 缺省情况下，未配置Portal用户同步功能 本命令中指定的Portal服务器必须已经存在 只有在指定的Portal服务器已经在接口上使能的情况下，本功能才能生效

说明

- 只有在支持 Portal 用户心跳功能(目前仅 iMC 的 Portal 服务器支持)的 Portal 服务器的配合下，本功能才有效。为了实现该功能，还需要在 Portal 服务器上选择支持用户心跳功能，并要求此处的 **interval** 与 **retry** 参数值的乘积应该大于等于 Portal 服务器上的用户心跳间隔时长，其中 **interval** 取值最好大于 Portal 服务器的用户心跳间隔时长。
- 对于设备上多余的用户信息，即在 N 个周期后被判定为 Portal 服务器上已不存在的用户信息，设备会在第 N + 1 个周期内的某时刻将其删除掉。

1.12 强制Portal用户下线

通过配置强制用户下线可以终止对指定 IP 地址用户的认证过程，或者将已经通过认证的指定 IP 地址的用户删除。

表1-17 配置强制用户下线

操作	命令	说明
进入系统视图	**system-view**	-
强制接入设备上的用户下线	**portal delete-user** { *ip-address* | **all** | **interface** *interface-type interface-number* }	必选

1.13 Portal显示和维护

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

在用户视图下执行 **reset** 命令可以清除 Portal 统计信息。

表1-18 Portal 显示和维护

操作	命令
显示接口上Portal的ACL信息	**display portal acl** { **all** | **dynamic** | **static** } **interface** *interface-type interface-number* [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示接口上Portal的连接统计信息	**display portal connection statistics** { **all** | **interface** *interface-type interface-number* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示Portal的免认证规则信息	**display portal free-rule** [*rule-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示指定接口的Portal配置信息	**display portal interface** *interface-type interface-number* [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示Portal服务器信息	**display portal server** [*server-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

操作	命令
显示接口上Portal服务器的统计信息	**display portal server statistics** { **all** | **interface** *interface-type interface-number* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示TCP仿冒统计信息	**display portal tcp-cheat statistics** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示Portal用户的信息	**display portal user** { **all** | **interface** *interface-type interface-number* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除接口上Portal的连接统计信息	**reset portal connection statistics** {**all** | **interface** *interface-type interface-number* }
清除接口上Portal服务器的统计信息	**reset portal server statistics** { **all** | **interface** *interface-type interface-number* }
清除TCP仿冒统计信息	**reset portal tcp-cheat statistics**

1.14 Portal典型配置举例

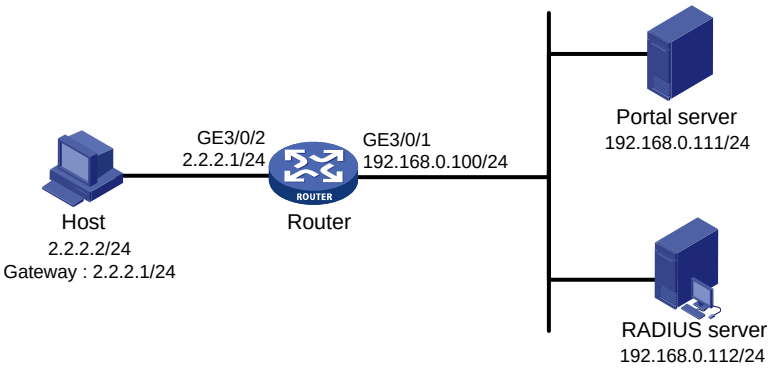
1.14.1 Portal直接认证配置举例

1. 组网需求

- 用户主机与接入设备 Router 直接相连，采用直接方式的 Portal 认证。用户通过手工配置或 DHCP 获取的一个公网 IP 地址进行认证，在通过 Portal 认证前，只能访问 Portal 服务器；在通过 Portal 认证后，可以使用此 IP 地址访问非受限的互联网资源。
- 采用 RADIUS 服务器作为认证/计费服务器。

2. 组网图

图1-8 配置 Portal 直接认证组网图



3. 配置步骤

说明

- 按照组网图配置设备各接口的 IP 地址，保证启动 Portal 之前各主机、服务器和设备之间的路由可达。
- 完成 RADIUS 服务器上的配置，保证用户的认证/计费功能正常运行。

(1) 配置 Portal server（iMC PLAT 3.20）

说明

下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 3.20-R2602P13、iMC UAM 3.60-E6301），说明 Portal server 的基本配置。

配置 Portal 服务器。

登录进入 iMC 管理平台，选择“业务”页签，单击导航树中的[Portal 服务器管理/服务器配置]菜单项，进入服务器配置页面。

- 根据实际组网情况调整以下参数，本例中使用缺省配置。

图1-9 Portal 服务器配置页面

配置 IP 地址组。

单击导航树中的[Portal 服务器管理/IP 地址组配置]菜单项，进入 Portal IP 地址组配置页面，在该页面中单击<增加>按钮，进入增加 IP 地址组配置页面。

- 填写 IP 地址组名；
- 输入起始地址和终止地址。用户主机 IP 地址必须包含在该 IP 地址组范围内。；
- 选择业务分组，本例中使用缺省的“未分组”；
- 选择 IP 地址组的类型为“普通”。

图1-10 增加 IP 地址组配置页面

增加 Portal 设备。

单击导航树中的[Portal 服务器管理/设备配置]菜单项，进入 Portal 设备配置页面，在该页面中单击<增加>按钮，进入增加设备信息配置页面。

- 填写设备名；
- 指定 IP 地址为与接入用户相连的设备接口 IP；
- 输入密钥，与接入设备 Router 上的配置保持一致；
- 选择是否进行二次地址分配，本例中为直接认证，因此为否；
- 选择是否支持逃生心跳功能和用户心跳功能，本例中不支持。

图1-11 增加设备信息配置页面

Portal 设备关联 IP 地址组

在 Portal 设备配置页面中的设备信息列表中，点击 NAS 设备的<端口组信息管理>链接，进入端口组信息配置页面。

图1-12 设备信息列表

在端口组信息配置页面中点击<增加>按钮，进入增加端口组信息配置页面。

- 填写端口组名；
- 选择 IP 地址组，用户接入网络时使用的 IP 地址必须属于所选的 IP 地址组；
- 其它参数采用缺省值。

图1-13 增加端口组信息配置页面

最后单击导航树中的[业务参数配置/系统配置手工生效]菜单项，使以上 Portal 服务器配置生效。

(2) 配置 Portal server（iMC PLAT 5.0）

说明

下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 5.0(E0101)、iMC UAM 5.0(E0101)），说明 Portal server 的基本配置。

配置 Portal 服务器。

登录进入 iMC 管理平台，选择“业务”页签，单击导航树中的[Portal 服务器管理/服务器配置]菜单项，进入服务器配置页面。

- 根据实际组网情况调整以下参数，本例中使用缺省配置。

图1-1 Portal 服务器配置页面

配置 IP 地址组。

单击导航树中的[Portal 服务器管理/IP 地址组配置]菜单项，进入 Portal IP 地址组配置页面，在该页面中单击<增加>按钮，进入增加 IP 地址组配置页面。

- 填写 IP 地址组名；
- 输入起始地址和终止地址。用户主机 IP 地址必须包含在该 IP 地址组范围内；
- 选择业务分组，本例中使用缺省的“未分组”；
- 选择 IP 地址组的类型为“普通”。

图1-2 增加 IP 地址组配置页面

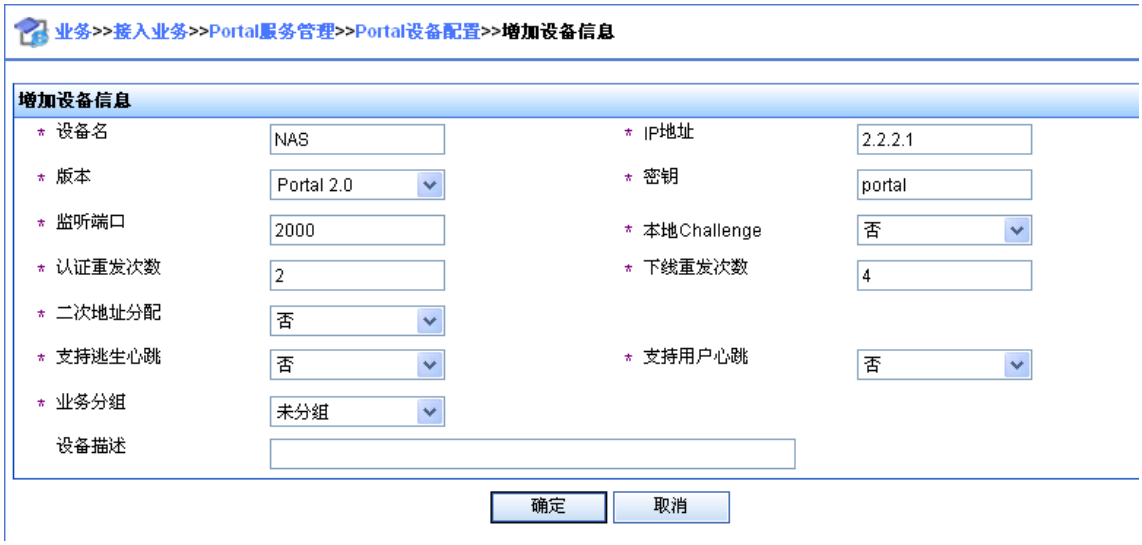
增加 Portal 设备。

单击导航树中的[Portal 服务器管理/设备配置]菜单项，进入 Portal 设备配置页面，在该页面中单击<增加>按钮，进入增加设备信息配置页面。

- 填写设备名；

- 指定 IP 地址为与接入用户相连的设备接口 IP；
- 输入密钥，与接入设备 Router 上的配置保持一致；
- 选择是否进行二次地址分配，本例中为直接认证，因此为否；
- 选择是否支持逃生心跳功能和用户心跳功能，本例中不支持。

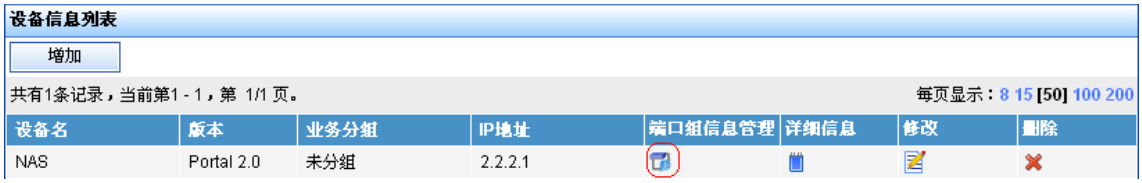
图1-3 增加设备信息配置页面



Portal 设备关联 IP 地址组

在 Portal 设备配置页面中的设备信息列表中，点击 NAS 设备的<端口组信息管理>链接，进入端口组信息配置页面。

图1-4 设备信息列表



在端口组信息配置页面中点击<增加>按钮，进入增加端口组信息配置页面。

- 填写端口组名；
- 选择 IP 地址组，用户接入网络时使用的 IP 地址必须属于所选的 IP 地址组；
- 其它参数采用缺省值。

图1-5 增加端口组信息配置页面

最后单击导航树中的[业务参数配置/系统配置手工生效]菜单项，使以上 Portal 服务器配置生效。

(3) 配置 Router

- 配置 RADIUS 方案

创建名字为 rs1 的 RADIUS 方案并进入该方案视图。

```
<Router> system-view
[Router] radius scheme rs1
```

配置 RADIUS 方案的服务器类型。使用 CAMS/iMC 服务器时，RADIUS 服务器类型应选择 **extended**。

```
[Router-radius-rs1] server-type extended
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[Router-radius-rs1] primary authentication 192.168.0.112
[Router-radius-rs1] primary accounting 192.168.0.112
[Router-radius-rs1] key authentication radius
[Router-radius-rs1] key accounting radius
```

配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[Router-radius-rs1] user-name-format without-domain
[Router-radius-rs1] quit
```

- 配置认证域

创建并进入名字为 dm1 的 ISP 域。

```
[Router] domain dm1
```

配置 ISP 域使用的 RADIUS 方案 rs1。

```
[Router-isp-dm1] authentication portal radius-scheme rs1
[Router-isp-dm1] authorization portal radius-scheme rs1
[Router-isp-dm1] accounting portal radius-scheme rs1
[Router-isp-dm1] quit
```

配置系统缺省的 ISP 域 dm1，所有接入用户共用此缺省域的认证和计费方式。若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方案。

```
[Router] domain default enable dm1
```

- 配置 Portal 认证

配置 Portal 服务器：名称为 newpt，IP 地址为 192.168.0.111，密钥为明文 portal，端口为 50100，URL 为 http://192.168.0.111:8080/portal。（Portal 服务器的 URL 请与实际环境中的 Portal 服务器配置保持一致，此处仅为示例）

```
[Router] portal server newpt ip 192.168.0.111 key simple portal port 50100 url
http://192.168.0.111:8080/portal
```

在与用户 Host 相连的接口上使能 Portal 认证。

```
[Router] interface gigabitethernet 3/0/2
[Router-GigabitEthernet3/0/2] portal server newpt method direct
[Router-GigabitEthernet3/0/2] quit
```

4. 验证配置结果

以上配置完成后，通过执行以下显示命令可查看 Portal 配置是否生效。

```
[Router] display portal interface gigabitethernet 3/0/2
 Portal configuration of GigabitEthernet3/0/2
 IPv4:
    Status: Portal running
    Portal server: newpt
    Portal backup-group: None
    Authentication type: Direct
    Authentication domain:
    Authentication network:
```

用户既可以使用 H3C 的 iNode 客户端，也可以通过网页方式进行 Portal 认证。用户在通过认证前，只能访问认证页面 http://192.168.0.111:8080/portal，且发起的 Web 访问均被重定向到该认证页面，在通过认证后，可访问非受限的互联网资源。

认证通过后，可通过执行以下显示命令查看 Router 上生成的 Portal 在线用户信息。

```
[Router] display portal user interface gigabitethernet 3/0/2
 Index:19
 State:ONLINE
 SubState:NONE
 ACL:NONE
 Work-mode:stand-alone
 MAC              IP               Vlan   Interface
 --------------------------------------------------------------------------
 0015-e9a6-7cfe   2.2.2.2          0      GigabitEthernet3/0/2
 On interface GigabitEthernet3/0/2:total 1 user(s) matched, 1 listed.
```

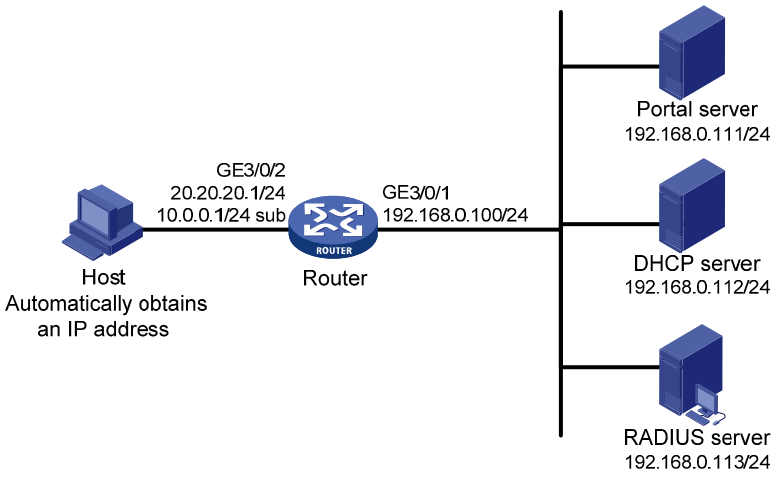
1.14.2 Portal二次地址分配认证配置举例

1. 组网需求

- 用户主机与接入设备 Router 直接相连，采用二次地址分配方式的 Portal 认证。用户通过 DHCP 服务器获取 IP 地址，Portal 认证前使用分配的一个私网地址；通过 Portal 认证后，用户申请到一个公网地址，才可以访问非受限互联网资源。
- 采用 RADIUS 服务器作为认证/计费服务器。

2. 组网图

图1-14 配置 Portal 二次地址分配认证组网图



3. 配置步骤

说明

- Portal 二次地址分配认证方式应用中，DHCP 服务器上需创建公网地址池（20.20.20.0/24）及私网地址池（10.0.0.0/24），具体配置略。
- Portal 二次地址分配认证方式应用中，接入设备上需要配置 DHCP 中继来配合 Portal 认证，且启动 Portal 的接口需要配置主 IP 地址（公网 IP）及从 IP 地址（私网 IP）。关于 DHCP 中继的详细配置请参见“三层技术-IP 业务配置指导”中的“DHCP 中继”。
- 请保证在 Portal 服务器上添加的 Portal 设备的 IP 地址为与用户相连的接口的公网 IP 地址（20.20.20.1），且与该 Portal 设备关联的 IP 地址组中的转换前地址为用户所在的私网网段（10.0.0.0/24）、转换后地址为公网网段（20.20.20.0/24）。
- 按照组网图配置设备各接口的 IP 地址，保证启动 Portal 之前各主机、服务器和设备之间的路由可达。
- 完成 RADIUS 服务器上的配置，保证用户的认证/计费功能正常运行。

在 Router 上进行以下配置。

(1) 配置 RADIUS 方案

创建名字为 rs1 的 RADIUS 方案并进入该方案视图。

```
<Router> system-view
[Router] radius scheme rs1
```

配置 RADIUS 方案的服务器类型。使用 CAMS/iMC 服务器时，RADIUS 服务器类型应选择 **extended**。

```
[Router-radius-rs1] server-type extended
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[Router-radius-rs1] primary authentication 192.168.0.113
```

```
[Router-radius-rs1] primary accounting 192.168.0.113
[Router-radius-rs1] key authentication radius
[Router-radius-rs1] key accounting radius
```

配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[Router-radius-rs1] user-name-format without-domain
[Router-radius-rs1] quit
```

(2) 配置认证域

创建并进入名字为 dm1 的 ISP 域。

```
[Router] domain dm1
```

配置 ISP 域的 RADIUS 方案 rs1。

```
[Router-isp-dm1] authentication portal radius-scheme rs1
[Router-isp-dm1] authorization portal radius-scheme rs1
[Router-isp-dm1] accounting portal radius-scheme rs1
[Router-isp-dm1] quit
```

配置系统缺省的 ISP 域 dm1，所有接入用户共用此缺省域的认证和计费方式。若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方案。

```
[Router] domain default enable dm1
```

(3) 配置 Portal 认证

配置 Portal 服务器：名称为 newpt，IP 地址为 192.168.0.111，密钥为明文 portal，端口为 50100，URL 为 http://192.168.0.111:8080/portal（请根据 Portal 服务器的实际情况配置，此处仅为示例）。

```
[Router] portal server newpt ip 192.168.0.111 key simple portal port 50100 url
http://192.168.0.111:8080/portal
```

配置 DHCP 中继，并启动 DHCP 中继的安全地址匹配检查功能。

```
[Router] dhcp enable
[Router] dhcp relay server-group 0 ip 192.168.0.112
[Router] interface gigabitethernet 3/0/2
[Router–GigabitEthernet3/0/2] ip address 20.20.20.1 255.255.255.0
[Router–GigabitEthernet3/0/2] ip address 10.0.0.1 255.255.255.0 sub
[Router-GigabitEthernet3/0/2] dhcp select relay
[Router-GigabitEthernet3/0/2] dhcp relay server-select 0
[Router-GigabitEthernet3/0/2] dhcp relay address-check enable
```

在与用户 Host 相连的接口上使能 Portal 认证。

```
[Router–GigabitEthernet3/0/2] portal server newpt method redhcp
[Router–GigabitEthernet3/0/2] quit
```

1.14.3 可跨三层Portal认证配置举例

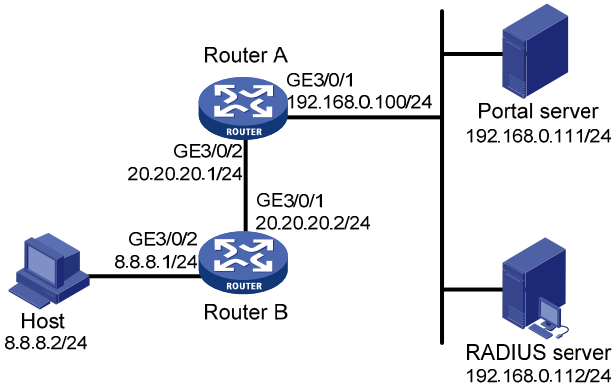
1. 组网需求

Router A 支持 Portal 认证功能。用户 Host 通过 Router B 接入到 Router A。

- 配置 Router A 采用可跨三层 Portal 认证。用户在未通过 Portal 认证前，只能访问 Portal 服务器；用户通过 Portal 认证后，可以访问非受限互联网资源。
- 采用 RADIUS 服务器作为认证/计费服务器。

2. 组网图

图1-15 配置可跨三层 Portal 认证组网图



3. 配置步骤

说明

- 请保证在 Portal 服务器上添加的 Portal 设备的 IP 地址为与用户相连的接口 IP 地址(20.20.20.1),且与该 Portal 设备关联的 IP 地址组为用户所在网段（8.8.8.0/24）。
- 按照组网图配置设备各接口的 IP 地址，保证启动 Portal 之前各主机、服务器和设备之间的路由可达。
- 完成 RADIUS 服务器上的配置，保证用户的认证/计费功能正常运行。

在 Router A 上进行以下配置。

(1) 配置 RADIUS 方案

创建名字为 rs1 的 RADIUS 方案并进入该方案视图。

```
<RouterA> system-view
[RouterA] radius scheme rs1
```

配置 RADIUS 方案的服务器类型。使用 CAMS/iMC 服务器时，RADIUS 服务器类型应选择 **extended**。

```
[RouterA-radius-rs1] server-type extended
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[RouterA-radius-rs1] primary authentication 192.168.0.112
[RouterA-radius-rs1] primary accounting 192.168.0.112
[RouterA-radius-rs1] key authentication radius
[RouterA-radius-rs1] key accounting radius
```

配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[RouterA-radius-rs1] user-name-format without-domain
[RouterA-radius-rs1] quit
```

(2) 配置认证域

创建并进入名字为 dm1 的 ISP 域。

```
[RouterA] domain dm1
```

配置 ISP 域的 RADIUS 方案 rs1。

```
[RouterA-isp-dm1] authentication portal radius-scheme rs1
[RouterA-isp-dm1] authorization portal radius-scheme rs1
[RouterA-isp-dm1] accounting portal radius-scheme rs1
[RouterA-isp-dm1] quit
```

配置系统缺省的 ISP 域 dm1，所有接入用户共用此缺省域的认证和计费方式。若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方案。

```
[Router] domain default enable dm1
```

(3) 配置 Portal 认证

配置 Portal 服务器：名称为 newpt，IP 地址为 192.168.0.111，密钥为 portal，端口为 50100，URL 为 http://192.168.0.111:8080/portal（请根据 Portal 服务器的实际情况配置，此处仅为示例）。

```
[RouterA] portal server newpt ip 192.168.0.111 key portal port 50100 url
http://192.168.0.111:8080/portal
```

在与 Router B 相连的接口上使能 Portal 认证。

```
[RouterA] interface gigabitethernet 3/0/2
[RouterA-GigabitEthernet3/0/2] portal server newpt method layer3
[RouterA-GigabitEthernet3/0/2] quit
```

Router B 上需要配置到 192.168.0.0/24 网段的缺省路由，下一跳为 20.20.20.1，具体配置略。

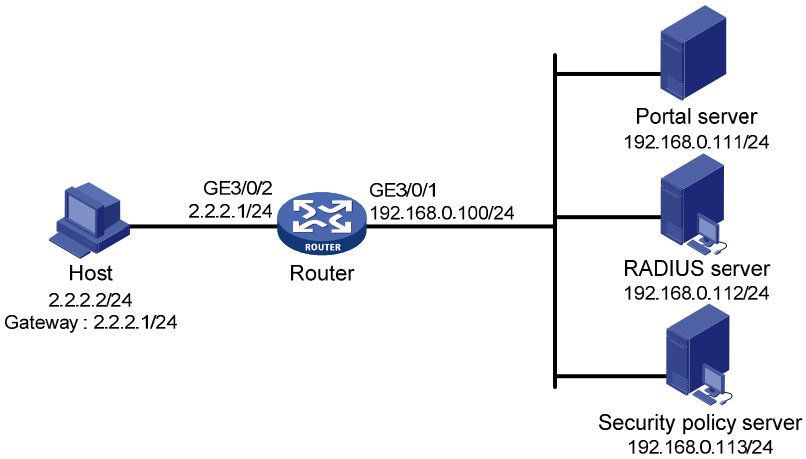
1.14.4 Portal直接认证扩展功能配置举例

1. 组网需求

- 用户主机与接入设备 Router 直接相连，采用直接方式的 Portal 认证。用户通过手工配置或 DHCP 获取的一个公网 IP 地址进行认证，在通过身份认证而没有通过安全认证时可以访问 192.168.0.0/24 网段；在通过安全认证后，可以使用此 IP 地址访问非受限互联网资源。
- 采用 RADIUS 服务器作为认证/计费服务器。

2. 组网图

图1-16 配置 Portal 直接认证扩展功能组网图



3. 配置步骤

说明

- 按照组网图配置设备各接口的 IP 地址，保证启动 Portal 之前各主机、服务器和设备之间的路由可达。
- 完成 RADIUS 服务器上的配置，保证用户的认证/计费功能正常运行。

在 Router 上进行以下配置。

(1) 配置 RADIUS 方案

创建名字为 rs1 的 RADIUS 方案并进入该方案视图。

```
<Router> system-view
[Router] radius scheme rs1
```

配置 RADIUS 方案的服务器类型。使用 CAMS/iMC 服务器时，RADIUS 服务器类型应选择 **extended**。

```
[Router-radius-rs1] server-type extended
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[Router-radius-rs1] primary authentication 192.168.0.112
[Router-radius-rs1] primary accounting 192.168.0.112
[Router-radius-rs1] key accounting simple radius
[Router-radius-rs1] key authentication simple radius
[Router-radius-rs1] user-name-format without-domain
```

配置 RADIUS 方案的安全策略服务器 IP。

```
[Router-radius-rs1] security-policy-server 192.168.0.113
[Router-radius-rs1] quit
```

(2) 配置认证域

创建并进入名字为 dm1 的 ISP 域。

```
[Router] domain dm1
```

配置 ISP 域的 RADIUS 方案 rs1。

```
[Router-isp-dm1] authentication portal radius-scheme rs1
[Router-isp-dm1] authorization portal radius-scheme rs1
[Router-isp-dm1] accounting portal radius-scheme rs1
[Router-isp-dm1] quit
```

配置系统缺省的 ISP 域 dm1，所有接入用户共用此缺省域的认证和计费方式。若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方案。

```
[Router] domain default enable dm1
```

(3) 配置受限资源对应的 ACL 为 3000，非受限资源对应的 ACL 为 3001

说明

安全策略服务器上需要将 ACL 3000 和 ACL 3001 分别指定为隔离 ACL 和安全 ACL。

```
[Router] acl number 3000
[Router-acl-adv-3000] rule permit ip destination 192.168.0.0 0.0.0.255
```

```
[Router-acl-adv-3000] rule deny ip
[Router-acl-adv-3000] quit
[Router] acl number 3001
[Router-acl-adv-3001] rule permit ip
[Router-acl-adv-3001] quit
```

(4) 配置 Portal 认证

配置 Portal 服务器：名称为 newpt，IP 地址为 192.168.0.111，密钥为明文 portal，端口为 50100，URL 为 http://192.168.0.111:8080/portal（请根据 Portal 服务器的实际情况配置，此处仅为示例）。

```
[Router] portal server newpt ip 192.168.0.111 key simple portal port 50100 url
http://192.168.0.111:8080/portal
```

在与用户 Host 相连的接口上使能 Portal 认证。

```
[Router] interface gigabitethernet 3/0/2
[Router-GigabitEthernet3/0/2] portal server newpt method direct
[Router-GigabitEthernet3/0/2] quit
```

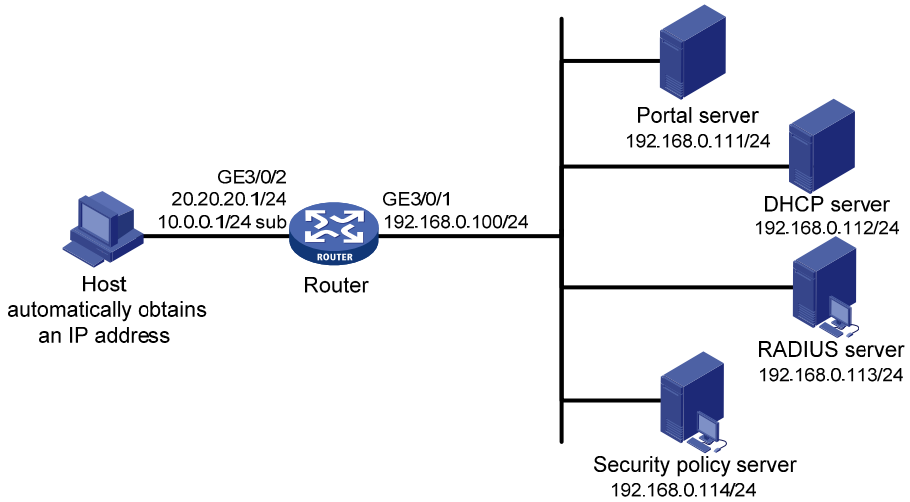
1.14.5 Portal二次地址分配认证扩展功能配置举例

1. 组网需求

- 用户主机与接入设备 Router 直接相连，采用二次地址分配方式的 Portal 认证。用户通过 DHCP 服务器获取 IP 地址，Portal 认证前使用分配的一个私网地址；通过 Portal 认证后，用户申请到一个公网地址。
- 用户在通过身份认证而没有通过安全认证时可以访问 192.168.0.0/24 网段；在通过安全认证后，可以访问非受限互联网资源。
- 采用 RADIUS 服务器作为认证/计费服务器。

2. 组网图

图1-17 配置 Portal 二次地址分配认证扩展功能组网图



3. 配置步骤

说明

- Portal 二次地址分配认证方式应用中，DHCP 服务器上需创建公网地址池（20.20.20.0/24）及私网地址池（10.0.0.0/24），具体配置略。
- Portal 二次地址分配认证方式应用中，接入设备需要配置 DHCP 中继来配合 Portal 认证，且启动 Portal 的接口需要配置主 IP 地址（公网 IP）及从 IP 地址（私网 IP）。关于 DHCP 中继的详细配置请参见“三层技术-IP 业务配置指导”中的“DHCP 中继”。
- 请保证在 Portal 服务器上添加的 Portal 设备的 IP 地址为与用户相连的接口的公网 IP 地址（20.20.20.1），且与该 Portal 设备关联的 IP 地址组中的转换前地址为用户所在的私网网段（10.0.0.0/24）、转换后地址为公网网段（20.20.20.0/24）。
- 按照组网图配置设备各接口的 IP 地址，保证启动 Portal 之前各主机、服务器和设备之间的路由可达。
- 完成 RADIUS 服务器上的配置，保证用户的认证/计费功能正常运行。

在 Router 上进行以下配置。

(1) 配置 RADIUS 方案

创建名字为 rs1 的 RADIUS 方案并进入该方案视图。

```
<Router> system-view
[Router] radius scheme rs1
```

配置 RADIUS 方案的服务器类型。使用 CAMS/iMC 服务器时，RADIUS 服务器类型应选择 **extended**。

```
[Router-radius-rs1] server-type extended
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[Router-radius-rs1] primary authentication 192.168.0.113
[Router-radius-rs1] primary accounting 192.168.0.113
[Router-radius-rs1] key authentication simple radius
[Router-radius-rs1] key accounting simple radius
[Router-radius-rs1] user-name-format without-domain
```

配置 RADIUS 方案的安全策略服务器 IP。

```
[Router-radius-rs1] security-policy-server 192.168.0.114
[Router-radius-rs1] quit
```

(2) 配置认证域

创建并进入名字为 dm1 的 ISP 域。

```
[Router] domain dm1
```

配置 ISP 域的 RADIUS 方案 rs1。

```
[Router-isp-dm1] authentication portal radius-scheme rs1
[Router-isp-dm1] authorization portal radius-scheme rs1
[Router-isp-dm1] accounting portal radius-scheme rs1
[Router-isp-dm1] quit
```

配置系统缺省的 ISP 域 dm1，所有接入用户共用此缺省域的认证和计费方式。若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方案。

```
[Router] domain default enable dm1
```

(3) 配置受限资源对应的 ACL 为 3000，非受限资源对应的 ACL 为 3001

说明

安全策略服务器上需要将 ACL 3000 和 ACL 3001 分别指定为隔离 ACL 和安全 ACL。

```
[Router] acl number 3000
[Router-acl-adv-3000] rule permit ip destination 192.168.0.0 0.0.0.255
[Router-acl-adv-3000] rule deny ip
[Router-acl-adv-3000] quit
[Router] acl number 3001
[Router-acl-adv-3001] rule permit ip
[Router-acl-adv-3001] quit
```

(4) 配置 Portal 认证

配置 Portal 服务器：名称为 newpt，IP 地址为 192.168.0.111，密钥为明文 portal，端口为 50100，URL 为 http://192.168.0.111:8080/portal（请根据 Portal 服务器的实际情况配置，此处仅为示例）。

```
[Router] portal server newpt ip 192.168.0.111 key simple portal port 50100 url
http://192.168.0.111:8080/portal
```

配置 DHCP 中继，并启动 DHCP 中继的安全地址匹配检查功能。

```
[Router] dhcp enable
[Router] dhcp relay server-group 0 ip 192.168.0.112
[Router] interface gigabitethernet 3/0/2
[Router–GigabitEthernet3/0/2] ip address 20.20.20.1 255.255.255.0
[Router–GigabitEthernet3/0/2] ip address 10.0.0.1 255.255.255.0 sub
[Router-GigabitEthernet3/0/2] dhcp select relay
[Router-GigabitEthernet3/0/2] dhcp relay server-select 0
[Router-GigabitEthernet3/0/2] dhcp relay address-check enable
```

在与用户 Host 相连的接口上使能 Portal 认证。

```
[Router–GigabitEthernet3/0/2] portal server newpt method redhcp
[Router–GigabitEthernet3/0/2] quit
```

1.14.6 可跨三层Portal认证扩展功能配置举例

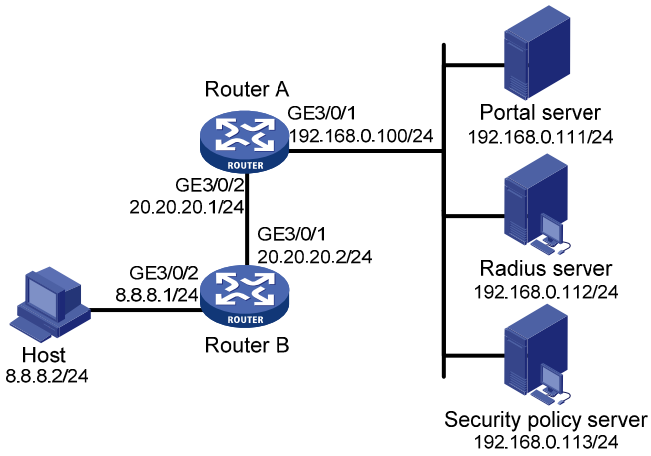
1. 组网需求

Router A 支持 Portal 认证功能。用户 Host 通过 Router B 接入到 Router A。

- 配置 Router A 采用可跨三层 Portal 认证。用户在通过身份认证而没有通过安全认证时可以访问 192.168.0.0/24 网段；在通过安全认证后，可以访问非受限互联网资源。
- 采用 RADIUS 服务器作为认证/计费服务器。

2. 组网图

图1-18 配置可跨三层 Portal 认证扩展功能组网图



3. 配置步骤

说明

- 请保证在 Portal 服务器上添加的 Portal 设备的 IP 地址为与用户相连的接口 IP 地址(20.20.20.1)，且与该 Portal 设备关联的 IP 地址组为用户所在网段（8.8.8.0/24)。
- 按照组网图配置设备各接口的 IP 地址，保证启动 Portal 之前各主机、服务器和设备之间的路由可达。
- 完成 RADIUS 服务器上的配置，保证用户的认证/计费功能正常运行。

在 Router A 上进行以下配置。

(1) 配置 RADIUS 方案

创建名字为 rs1 的 RADIUS 方案并进入该方案视图。

```
<RouterA> system-view
[RouterA] radius scheme rs1
```

配置 RADIUS 方案的服务器类型。使用 CAMS/iMC 服务器时，RADIUS 服务器类型应选择 **extended**。

```
[RouterA-radius-rs1] server-type extended
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[RouterA-radius-rs1] primary authentication 192.168.0.112
[RouterA-radius-rs1] primary accounting 192.168.0.112
[RouterA-radius-rs1] key authentication simple radius
[RouterA-radius-rs1] key accounting simple radius
[RouterA-radius-rs1] user-name-format without-domain
```

配置 RADIUS 方案的安全策略服务器 IP。

```
[RouterA-radius-rs1] security-policy-server 192.168.0.113
[RouterA-radius-rs1] quit
```

(2) 配置认证域

创建并进入名字为 dm1 的 ISP 域。

```
[RouterA] domain dm1
```

配置 ISP 域的 RADIUS 方案 rs1。

```
[RouterA-isp-dm1] authentication portal radius-scheme rs1
[RouterA-isp-dm1] authorization portal radius-scheme rs1
[RouterA-isp-dm1] accounting portal radius-scheme rs1
[RouterA-isp-dm1] quit
```

配置系统缺省的 ISP 域 dm1，所有接入用户共用此缺省域的认证和计费方式。若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方案。

```
[RouterA] domain default enable dm1
```

(3) 配置受限资源对应的 ACL 为 3000，非受限资源对应的 ACL 为 3001

说明

安全策略服务器上需要将 ACL 3000 和 ACL 3001 分别指定为隔离 ACL 和安全 ACL。

```
[RouterA] acl number 3000
[RouterA-acl-adv-3000] rule permit ip destination 192.168.0.0 0.0.0.255
[RouterA-acl-adv-3000] rule deny ip
[RouterA-acl-adv-3000] quit
[RouterA] acl number 3001
[RouterA-acl-adv-3001] rule permit ip
[RouterA-acl-adv-3001] quit
```

(4) 配置 Portal 认证

配置 Portal 服务器：名称为 newpt，IP 地址为 192.168.0.111，密钥为明文 portal，端口为 50100，URL 为 http://192.168.0.111:8080/portal（请根据 Portal 服务器的实际情况配置，此处仅为示例）。

```
[RouterA] portal server newpt ip 192.168.0.111 key simple portal port 50100 url
http://192.168.0.111:8080/portal
```

在与 Router B 相连的接口上使能 Portal 认证。

```
[RouterA] interface gigabitethernet 3/0/2
[RouterA-GigabitEthernet3/0/2] portal server newpt method layer3
[RouterA-GigabitEthernet3/0/2] quit
```

Router B 上需要配置到 192.168.0.0/24 网段的缺省路由，下一跳为 20.20.20.1，具体配置略。

1.14.7 Portal支持双机热备配置举例（仅SR6602 和SR6602-X支持）

1. 组网需求

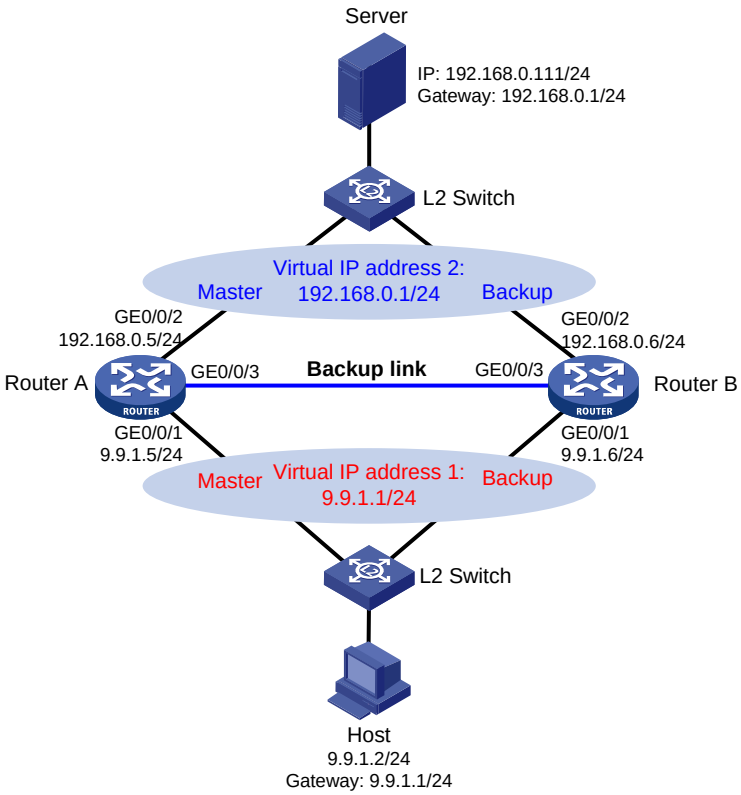
接入设备 Router A 和 Router B 之间存在备份链路，使用 VRRP 协议实现双机热备的流量切换，且两台设备均支持 Portal 认证功能。现要求 Router A 和 Router B 支持双机热备运行情况下的 Portal 用户数据备份，具体为：

- Router A 正常工作的情况下，Host 通过 Router A 进行 Portal 认证接入到外网。Router A 发生故障的情况下，Host 通过 Router B 接入到外网，并且在 VRRP 监视上/下行链路接口功能的配合下，保证业务流量切换不被中断。

- 采用 RADIUS 服务器作为认证/计费服务器。（本例中 Portal 服务器和 RADIUS 服务器的功能均由 Server 实现）
- Router A 和 Router B 之间通过单独的物理链路传输双机热备报文。

2. 组网图

图1-19 配置 Portal 支持双机热备组网图



3. 配置步骤

说明：

- 按照组网图配置设备各接口的 IP 地址，保证启动 Portal 之前各主机、服务器和设备之间的路由可达。
- 保证启动 Portal 之前主机可以分别通过 Router A 和 Router B 访问认证服务器。
- 配置 VRRP 备份组 1 和 VRRP 备份组 2 分别实现下行、上行链路的备份。VRRP 配置的相关介绍请参见“可靠性配置指导”中的“VRRP”。
- 双机热备配置的相关介绍请参见“可靠性配置指导”中的“双机热备”。

(1) 配置 Portal 服务器（iMC PLAT 3.20）

说明

下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 3.20-R2606P13、iMC UAM 3.60-E6301），说明 Portal server 的相关配置。

配置 Portal 服务器。

登录进入 iMC 管理平台，选择“业务”页签，单击导航树中的[Portal 服务器管理/服务器配置]菜单项，进入服务器配置页面。

- 根据实际组网情况调整以下参数，本例中使用缺省配置。

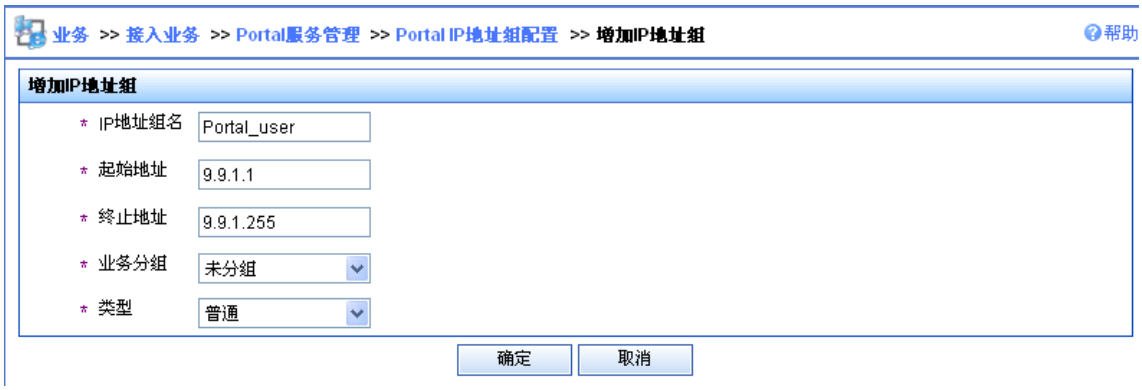
图1-20 Portal 服务器配置页面

配置 IP 地址组。

单击导航树中的[Portal 服务器管理/IP 地址组配置]菜单项，进入 Portal IP 地址组配置页面，在该页面中单击<增加>按钮，进入增加 IP 地址组配置页面。

- 填写 IP 地址组名；
- 输入起始地址和终止地址。用户主机 IP 地址必须包含在该 IP 地址组范围内；
- 选择业务分组，本例中使用缺省的“未分组”；
- 选择 IP 地址组的类型为“普通”。

图1-21 增加 IP 地址组配置页面



增加 Portal 设备。

单击导航树中的[Portal 服务器管理/设备配置]菜单项，进入 Portal 设备配置页面，在该页面中单击<增加>按钮，进入增加设备信息配置页面。

- 填写设备名；
- 指定主机 IP 地址为使能 Portal 的接口所在的 VRRP 组的虚拟 IP 地址；
- 输入密钥，与接入设备 Router 上的配置保持一致；
- 选择是否进行二次地址分配，本例中为直接认证，因此为否；
- 选择是否支持逃生心跳功能和用户心跳功能，本例中不支持。

图1-22 增加设备信息配置页面

Portal 设备关联 IP 地址组

在 Portal 设备配置页面中的设备信息列表中，点击 NAS 设备的<端口组信息管理>链接，进入端口组信息配置页面。

图1-23 设备信息列表

在端口组信息配置页面中点击<增加>按钮，进入增加端口组信息配置页面。

- 填写端口组名；
- 选择 IP 地址组，用户接入网络时使用的 IP 地址必须属于所选的 IP 地址组；
- 其它参数采用缺省值。

图1-24 增加端口组信息配置页面

最后单击导航树中的[业务参数配置/系统配置手工生效]菜单项，使以上 Portal 服务器配置生效。

(2) 配置 Portal 服务器（iMC PLAT 5.0）

说明

下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 5.0(E0101)、iMC UAM 5.0(E0101)），说明 Portal server 的基本配置。

配置 Portal 服务器。

登录进入 iMC 管理平台，选择“业务”页签，单击导航树中的[Portal 服务器管理/服务器配置]菜单项，进入服务器配置页面。

- 根据实际组网情况调整以下参数，本例中使用缺省配置。

图1-6 Portal 服务器配置页面

配置 IP 地址组。

单击导航树中的[Portal 服务器管理/IP 地址组配置]菜单项，进入 Portal IP 地址组配置页面，在该页面中单击<增加>按钮，进入增加 IP 地址组配置页面。

- 填写 IP 地址组名；
- 输入起始地址和终止地址。用户主机 IP 地址必须包含在该 IP 地址组范围内；
- 选择业务分组，本例中使用缺省的“未分组”；
- 选择 IP 地址组的类型为“普通”。

图1-7 增加 IP 地址组配置页面

增加 Portal 设备。

单击导航树中的[Portal 服务器管理/设备配置]菜单项，进入 Portal 设备配置页面，在该页面中单击<增加>按钮，进入增加设备信息配置页面。

- 填写设备名；
- 指定主机 IP 地址为使能 Portal 的接口所在的 VRRP 组的虚拟 IP 地址；
- 输入密钥，与接入设备 Router 上的配置保持一致；
- 选择是否进行二次地址分配，本例中为直接认证，因此为否；
- 选择是否支持逃生心跳功能和用户心跳功能，本例中不支持。

图1-8 增加设备信息配置页面

Portal 设备关联 IP 地址组

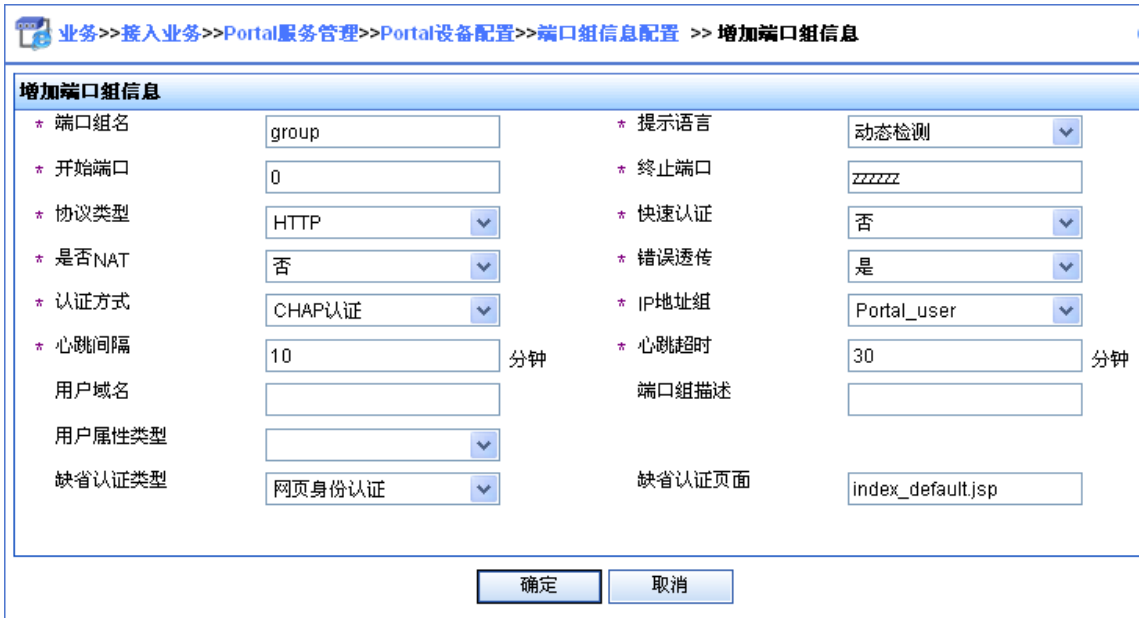
在 Portal 设备配置页面中的设备信息列表中，点击 NAS 设备的<端口组信息管理>链接，进入端口组信息配置页面。

图1-9 设备信息列表

在端口组信息配置页面中点击<增加>按钮，进入增加端口组信息配置页面。

- 填写端口组名；
- 选择 IP 地址组，用户接入网络时使用的 IP 地址必须属于所选的 IP 地址组；
- 其它参数采用缺省值。

图1-10 增加端口组信息配置页面



最后单击导航树中的[业务参数配置/系统配置手工生效]菜单项，使以上 Portal 服务器配置生效。

(3) 配置 Router A

- 配置 VRRP

创建 VRRP 备份组 1，并配置 VRRP 备份组 1 的虚拟 IP 地址为 9.9.1.1。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 0/0/1
[RouterA-GigabitEthernet0/0/1] vrrp vrid 1 virtual-ip 9.9.1.1
```

配置接口 GigabitEthernet0/0/1 在 VRRP 备份组 1 中的优先级为 200。

```
[RouterA-GigabitEthernet0/0/1] vrrp vrid 1 priority 200
```

在接口 GigabitEthernet0/0/1 上配置监视接口 GigabitEthernet0/0/2，当接口 GigabitEthernet0/0/2 状态为 Down 或 Removed 时，接口 GigabitEthernet0/0/1 在备份组 1 中的优先级降低 150。

```
[RouterA-GigabitEthernet0/0/1] vrrp vrid 1 track interface gigabitethernet 0/0/2 reduced 150
[RouterA-GigabitEthernet0/0/1] quit
```

创建 VRRP 备份组 2，并配置 VRRP 备份组 2 的虚拟 IP 地址为 192.168.0.1。

```
[RouterA] interface gigabitethernet 0/0/2
[RouterA-GigabitEthernet0/0/2] vrrp vrid 2 virtual-ip 192.168.0.1
```

配置接口 GigabitEthernet0/0/2 在 VRRP 备份组 2 中的优先级为 200。

```
[RouterA-GigabitEthernet0/0/2] vrrp vrid 2 priority 200
```

在接口 GigabitEthernet0/0/2 上配置监视接口 GigabitEthernet0/0/1，当接口 GigabitEthernet0/0/1 状态为 Down 或 Removed 时，接口 GigabitEthernet0/0/2 在备份组 2 中的优先级降低 150。

```
[RouterA-GigabitEthernet0/0/2] vrrp vrid 2 track interface gigabitethernet 0/0/1 reduced 150
[RouterA-GigabitEthernet0/0/2] quit
```

- 配置 RADIUS 方案

创建名字为 rs1 的 RADIUS 方案并进入该方案视图。

```
[RouterA] radius scheme rs1
```

配置 RADIUS 方案的服务器类型。使用 iMC 服务器时，RADIUS 服务器类型应选择 **extended**。

```
[RouterA-radius-rs1] server-type extended
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[RouterA-radius-rs1] primary authentication 192.168.0.111
[RouterA-radius-rs1] primary accounting 192.168.0.111
[RouterA-radius-rs1] key authentication simple expert
[RouterA-radius-rs1] key accounting simple expert
```

配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。（可选，请根据实际应用需求调整）

```
[RouterA-radius-rs1] user-name-format without-domain
[RouterA-radius-rs1] quit
```

- 配置认证域

创建并进入名字为 dm1 的 ISP 域。

```
[RouterA] domain dm1
```

配置 ISP 域的 RADIUS 方案 rs1。

```
[RouterA-isp-dm1] authentication portal radius-scheme rs1
[RouterA-isp-dm1] authorization portal radius-scheme rs1
[RouterA-isp-dm1] accounting portal radius-scheme rs1
[RouterA-isp-dm1] quit
```

配置系统缺省的 ISP 域 dm1，所有接入用户共用此缺省域的认证和计费方式。若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方案。

```
[RouterA] domain default enable dm1
```

- 接口使能 Portal

配置 Portal 服务器：名称为 newpt，IP 地址为 192.168.0.111，密钥为明文 portal，端口为 50100，URL 为 http://192.168.0.111:8080/portal。（Portal 服务器的 URL 请与实际环境中的 Portal 服务器配置保持一致，此处仅为示例）

```
[RouterA] portal server newpt ip 192.168.0.111 key simple portal port 50100 url
http://192.168.0.111:8080/portal
```

在与用户 Host 相连的接口上使能 Portal 认证。

```
[RouterA] interface gigabitethernet 0/0/1
[RouterA–GigabitEthernet0/0/1] portal server newpt method layer3
```

指定发送 Portal 报文的源 IP 地址为 VRRP 组 1 的虚拟 IP 地址 9.9.1.1。

```
[RouterA–GigabitEthernet0/0/1] portal nas-ip 9.9.1.1
```

- 配置 Portal 支持双机热备

配置接口 GigabitEthernet0/0/1 属于 Portal 备份组 1。

```
 [RouterA–GigabitEthernet0/0/1] portal backup-group 1
[RouterA–GigabitEthernet0/0/1] quit
```

配置双机热备模式下的设备 ID 为 1。

```
[RouterA] nas device-id 1
```

配置发送 RADIUS 报文的源 IP 地址为 VRRP 组 2 的虚拟 IP 地址 192.168.0.1。

```
[RouterA] radius nas-ip 192.168.0.1
```

说明

请保证 RADIUS 服务器上成功添加了 IP 地址为 192.168.0.1 的接入设备。

- 配置双机热备

配置备份接口为接口 GigabitEthernet0/0/3。

```
[RouterA] dhbk interface gigabitethernet0/0/3
```

使能双机热备功能，且支持对称路径。

```
[RouterA] dhbk enable backup-type symmetric-path
```

(4) 配置 Router B

- 配置 VRRP

创建 VRRP 备份组 1，并配置 VRRP 备份组 1 的虚拟 IP 地址为 9.9.1.1。

```
<RouterB> system-view
[RouterB] interface gigabitethernet 0/0/1
[RouterB–GigabitEthernet0/0/1] vrrp vrid 1 virtual-ip 9.9.1.1
```

配置接口 GigabitEthernet0/0/1 在 VRRP 备份组 1 中的优先级为 150。

```
[RouterB–GigabitEthernet0/0/1] vrrp vrid 1 priority 150
[RouterB–GigabitEthernet0/0/1] quit
```

创建 VRRP 备份组 2，并配置 VRRP 备份组 2 的虚拟 IP 地址为 192.168.0.1。

```
[RouterB] interface gigabitethernet 0/0/2
[RouterB–GigabitEthernet0/0/2] vrrp vrid 2 virtual-ip 192.168.0.1
```

配置接口 GigabitEthernet0/0/2 在 VRRP 备份组 2 中的优先级为 150。

```
[RouterB–GigabitEthernet0/0/2] vrrp vrid 2 priority 150
[RouterB–GigabitEthernet0/0/2] quit
```

- 配置 RADIUS 方案

创建名字为 rs1 的 RADIUS 方案并进入该方案视图。

```
[RouterB] radius scheme rs1
```

配置 RADIUS 方案的服务器类型。使用 iMC 服务器时，RADIUS 服务器类型应选择 **extended**。

```
[RouterB-radius-rs1] server-type extended
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[RouterB-radius-rs1] primary authentication 192.168.0.111
[RouterB-radius-rs1] primary accounting 192.168.0.111
[RouterB-radius-rs1] key authentication simple expert
[RouterB-radius-rs1] key accounting simple expert
```

配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。（可选，请根据实际应用需求调整）

```
[RouterB-radius-rs1] user-name-format without-domain
[RouterB-radius-rs1] quit
```

- 配置认证域

创建并进入名字为 dm1 的 ISP 域。

```
[RouterB] domain dm1
```

配置 ISP 域的 RADIUS 方案 rs1。

```
[RouterB-isp-dm1] authentication portal radius-scheme rs1
[RouterB-isp-dm1] authorization portal radius-scheme rs1
```

```
[RouterB-isp-dm1] accounting portal radius-scheme rs1
[RouterB-isp-dm1] quit
```

配置系统缺省的 ISP 域 dm1，所有接入用户共用此缺省域的认证和计费方式。若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方案。

```
[RouterB] domain default enable dm1
```

- 配置接口使能 Portal

配置 Portal 服务器：名称为 newpt，IP 地址为 192.168.0.111，密钥为明文 portal，端口为 50100，URL 为 http://192.168.0.111:8080/portal。（Portal 服务器的 URL 请与实际环境中的 Portal 服务器配置保持一致，此处仅为示例）

```
[RouterB] portal server newpt ip 192.168.0.111 key simple portal port 50100 url
http://192.168.0.111:8080/portal
```

在与用户 Host 相连的接口上使能 Portal 认证。

```
[RouterB] interface gigabitethernet 0/0/1
[RouterB-GigabitEthernet0/0/1] portal server newpt method layer3
```

指定发送 Portal 报文的源 IP 地址为 VRRP 组 1 的虚拟 IP 地址 9.9.1.1。

```
[RouterB-GigabitEthernet0/0/1] portal nas-ip 9.9.1.1
```

- 配置 Portal 支持双机热备

配置接口 GigabitEthernet0/0/1 属于 Portal 备份组 1。

```
 [RouterB-GigabitEthernet0/0/1] portal backup-group 1
[RouterB-GigabitEthernet0/0/1] quit
```

配置双机热备模式下的设备 ID 为 2。

```
[RouterB] nas device-id 2
```

配置发送 RADIUS 报文的源 IP 地址为 VRRP 组 2 的虚拟 IP 地址 192.168.0.1。

```
[RouterB] radius nas-ip 192.168.0.1
```

说明

请保证 RADIUS 服务器上成功添加了 IP 地址为 192.168.0.1 的接入设备。

- 配置双机热备

配置备份接口为接口 GigabitEthernet0/0/3。

```
[RouterB] dhbk interface gigabitethernet0/0/3
```

使能双机热备功能。

```
[RouterB] dhbk enable backup-type symmetric-path
```

4. 验证配置结果

用户 Host 从 Router A 成功上线后，在 Router A 和 Router B 上均可以通过命令 **display portal user** 查看该用户的认证情况。

```
[RouterA] display portal user all
Index:3
 State:ONLINE
 SubState: NONE
 ACL:NONE
 Work-mode: primary
 VPN instance:NONE
```

```
 MAC                 IP                  Vlan    Interface
 --------------------------------------------------------------------------
 000d-88f8-0eac      9.9.1.2             0       GigabitEthernet0/0/1
 Total 1 user(s) matched, 1 listed.
[RouterB] display portal user all
Index:2
 State:ONLINE
 SubState: NONE
 ACL:NONE
 Work-mode: secondary
 VPN instance:NONE
 MAC                 IP                  Vlan    Interface
 --------------------------------------------------------------------------
 000d-88f8-0eac      9.9.1.2             0       GigabitEthernet0/0/1
 Total 1 user(s) matched, 1 listed.
```

通过以上显示信息可以看到，Router A 和 Router B 上均有 Portal 用户 Host 的信息，且 Router A 上的用户模式为 primary，Router B 上的用户模式为 secondary，表示该用户是由 Router A 上线并被同步到 Router B 上的。

1.14.8 Portal服务器探测和用户同步功能配置举例

1. 组网需求

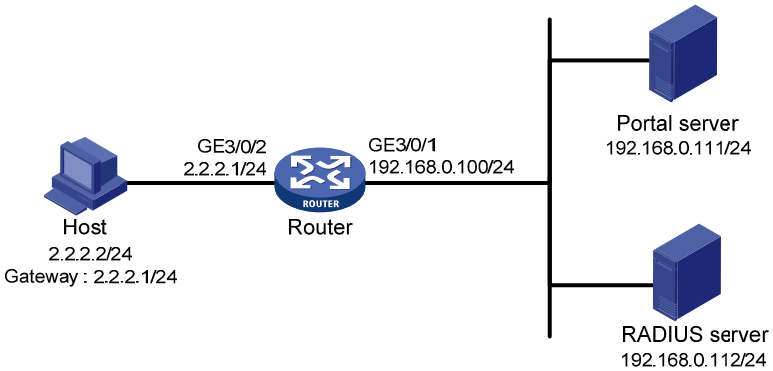
用户主机与接入设备 Router 直接相连，通过 Portal 认证接入网络，并采用 RADIUS 服务器作为认证/计费服务器。

具体要求如下：

- 用户通过手工配置或 DHCP 获取的一个公网 IP 地址进行认证，在通过 Portal 认证前，只能访问 Portal 服务器；在通过 Portal 认证后，可以使用此 IP 地址访问非受限的互联网资源。
- 接入设备能够探测到 Portal 服务器是否可达，并输出可达状态变化的 Trap 信息，在服务器不可达时（例如，网络连接中断、网络设备故障或服务器无法正常提供服务等情况），取消 Portal 认证，使得用户仍然可以正常访问网络。
- 接入设备能够与服务器定期进行用户信息的同步。

2. 组网图

图1-25 Portal 服务器探测和用户同步功能配置组网图



3. 配置思路

(1) 配置 Portal 服务器，并启动逃生心跳功能和用户心跳功能；

(2) 配置 RADIUS 服务器，实现正常的认证及计费功能；

(3) 接入设备通过接口 GigabitEthernet3/0/2 与用户主机直接相连，在该接口上配置直接方式的 Portal 认证；

(4) 接入设备上配置 Portal 服务器探测功能，在与 Portal 服务器的逃生心跳功能的配合下，对 Portal 服务器的可达状态进行探测；

(5) 接入设备上配置 Portal 用户同步功能，在与 Portal 服务器的用户心跳功能的配合下，与 Portal 服务器上的用户信息进行同步。

4. 配置步骤

说明

- 按照组网图配置设备各接口的 IP 地址，保证启动 Portal 之前各主机、服务器和设备之间的路由可达。
- 完成 RADIUS 服务器上的配置，保证用户的认证/计费功能正常运行。

(1) 配置 Portal 服务器（iMC PLAT 3.20）

说明

下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 3.20-R2606P13、iMC UAM 3.60-E6301），说明 Portal server 的相关配置。

配置 Portal 服务器。

登录进入 iMC 管理平台，选择“业务”页签，单击导航树中的[Portal 服务器管理/服务器配置]菜单项，进入服务器配置页面。

- 配置逃生心跳间隔时长及用户心跳间隔时长；
- 其它参数使用缺省配置。

图1-26 Portal 服务器配置页面

配置 IP 地址组。

单击导航树中的[Portal 服务器管理/IP 地址组配置]菜单项，进入 Portal IP 地址组配置页面，在该页面中单击<增加>按钮，进入增加 IP 地址组配置页面。

- 填写 IP 地址组名；
- 输入起始地址和终止地址。用户主机 IP 地址必须包含在该 IP 地址组范围内；
- 选择业务分组，本例中使用缺省的“未分组”；
- 选择 IP 地址组的类型为“普通”。

图1-27 增加 IP 地址组配置页面

增加 Portal 设备。

单击导航树中的[Portal 服务器管理/设备配置]菜单项，进入 Portal 设备配置页面，在该页面中单击<增加>按钮，进入增加设备信息配置页面。

- 填写设备名；
- 指定 IP 地址为与接入用户相连的设备接口 IP；
- 输入密钥，与接入设备 Router 上的配置保持一致；
- 选择是否进行二次地址分配，本例中为直接认证，因此为否；
- 选择支持逃生心跳功能和用户心跳功能。

图1-28 增加设备信息配置页面

Portal 设备关联 IP 地址组

在 Portal 设备配置页面中的设备信息列表中，点击 NAS 设备的<端口组信息管理>链接，进入端口组信息配置页面。

图1-29 设备信息列表

在端口组信息配置页面中点击<增加>按钮，进入增加端口组信息配置页面。

- 填写端口组名；
- 选择 IP 地址组，用户接入网络时使用的 IP 地址必须属于所选的 IP 地址组；
- 其它参数采用缺省值。

图1-30 增加端口组信息配置页面

最后单击导航树中的[业务参数配置/系统配置手工生效]菜单项，使以上 Portal 服务器配置生效。

(2) 配置 Portal 服务器（iMC PLAT 5.0）

说明

下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 5.0(E0101)、iMC UAM 5.0(E0101)），说明 Portal server 的基本配置。

配置 Portal 服务器。

登录进入 iMC 管理平台，选择“业务”页签，单击导航树中的[Portal 服务器管理/服务器配置]菜单项，进入服务器配置页面。

- 配置逃生心跳间隔时长及用户心跳间隔时长；
- 其它参数使用缺省配置。

图1-11 Portal 服务器配置页面

配置 IP 地址组。

单击导航树中的[Portal 服务器管理/IP 地址组配置]菜单项，进入 Portal IP 地址组配置页面，在该页面中单击<增加>按钮，进入增加 IP 地址组配置页面。

- 填写 IP 地址组名；
- 输入起始地址和终止地址。用户主机 IP 地址必须包含在该 IP 地址组范围内；
- 选择业务分组，本例中使用缺省的“未分组”；
- 选择 IP 地址组的类型为“普通”。

图1-12 增加 IP 地址组配置页面

增加 Portal 设备。

单击导航树中的[Portal 服务器管理/设备配置]菜单项，进入 Portal 设备配置页面，在该页面中单击<增加>按钮，进入增加设备信息配置页面。

- 填写设备名；

- 指定 IP 地址为与接入用户相连的设备接口 IP；
- 输入密钥，与接入设备 Router 上的配置保持一致；
- 选择是否进行二次地址分配，本例中为直接认证，因此为否；
- 选择支持逃生心跳功能和用户心跳功能。

图1-13 增加设备信息配置页面

Portal 设备关联 IP 地址组

在 Portal 设备配置页面中的设备信息列表中，点击 NAS 设备的<端口组信息管理>链接，进入端口组信息配置页面。

图1-14 设备信息列表

在端口组信息配置页面中点击<增加>按钮，进入增加端口组信息配置页面。

- 填写端口组名；
- 选择 IP 地址组，用户接入网络时使用的 IP 地址必须属于所选的 IP 地址组；
- 其它参数采用缺省值。

图1-15 增加端口组信息配置页面

最后单击导航树中的[业务参数配置/系统配置手工生效]菜单项，使以上 Portal 服务器配置生效。

(3) 配置 Router

- 配置 RADIUS 方案

创建名字为 rs1 的 RADIUS 方案并进入该方案视图。

```
<Router> system-view
[Router] radius scheme rs1
```

配置 RADIUS 方案的服务器类型。使用 iMC 服务器时，RADIUS 服务器类型应选择 **extended**。

```
[Router-radius-rs1] server-type extended
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[Router-radius-rs1] primary authentication 192.168.0.112
[Router-radius-rs1] primary accounting 192.168.0.112
[Router-radius-rs1] key authentication simple radius
[Router-radius-rs1] key accounting simple radius
```

配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[Router-radius-rs1] user-name-format without-domain
[Router-radius-rs1] quit
```

- 配置认证域

创建并进入名字为 dm1 的 ISP 域。

```
[Router] domain dm1
```

配置 ISP 域的 RADIUS 方案 rs1。

```
[Router-isp-dm1] authentication portal radius-scheme rs1
[Router-isp-dm1] authorization portal radius-scheme rs1
[Router-isp-dm1] accounting portal radius-scheme rs1
[Router-isp-dm1] quit
```

配置系统缺省的 ISP 域 dm1，所有接入用户共用此缺省域的认证和计费方式。若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方案。

```
[Router] domain default enable dm1
```

- 使能 Portal 认证

配置 Portal 服务器：名称为 newpt，IP 地址为 192.168.0.111，密钥为明文 portal，端口为 50100，URL 为 http://192.168.0.111:8080/portal。（Portal 服务器的 URL 请与实际环境中的 Portal 服务器配置保持一致，此处仅为示例）

```
[Router] portal server newpt ip 192.168.0.111 key simple portal port 50100 url
http://192.168.0.111:8080/portal
```

在与用户 Host 相连的接口上使能 Portal 认证。

```
[Router] interface gigabitethernet 3/0/2
[Router-GigabitEthernet3/0/2] portal server newpt method direct
[Router-GigabitEthernet3/0/2] quit
```

- 配置 Portal 服务器探测功能

配置对 Portal 服务器 newpt 的探测功能：探测方式为探测 Portal 心跳报文，每次探测间隔时间为 40 秒，若连续二次探测均失败，则发送服务器不可达的 Trap 信息，并打开网络限制，允许未认证用户访问网络。

```
[Router] portal server newpt server-detect method portal-heartbeat action trap permit-all
interval 40 retry 2
```

说明

此处 interval 与 retry 的乘积应该大于等于 Portal 服务器的逃生心跳间隔时长，且推荐 interval 取值大于 Portal 服务器的逃生心跳间隔时长。

- 配置 Portal 用户信息同步功能

配置对 Portal 服务器 newpt 的 Portal 用户同步功能，检测用户同步报文的时间间隔为 600 秒，如果设备中的某用户信息在连续两个探测周期内都未在该 Portal 服务器发送的同步报文中出现，设备将强制该用户下线。

```
[Router] portal server newpt user-sync interval 600 retry 2
```

说明

此处 interval 与 retry 的乘积应该大于等于 Portal 服务器上的用户心跳间隔时长，且推荐 interval 取值大于 Portal 服务器的用户心跳间隔时长。

5. 验证配置结果

以上配置完成后，可以通过执行以下命令查看到 Portal 服务器的状态为 Up，说明当前 Portal 服务器可达。

```
<Router> display portal server newpt
 Portal server:
  1)newpt:
      IP   : 192.168.0.111
      Key  : ******
      Port : 50100
      URL  : http://192.168.0.111:8080/portal
```

```
Status  : Up
```

之后，若接入设备探测到 Portal 服务器不可达了，可通过以上显示命令查看到 Portal 服务器的状态为 Down，同时，设备会输出表示服务器不可达的 Trap 信息“portal server newpt lost”，并取消对该接口接入的用户的 Portal 认证，使得用户可以直接访问外部网络。

1.14.9 可跨三层Portal认证支持多实例配置举例

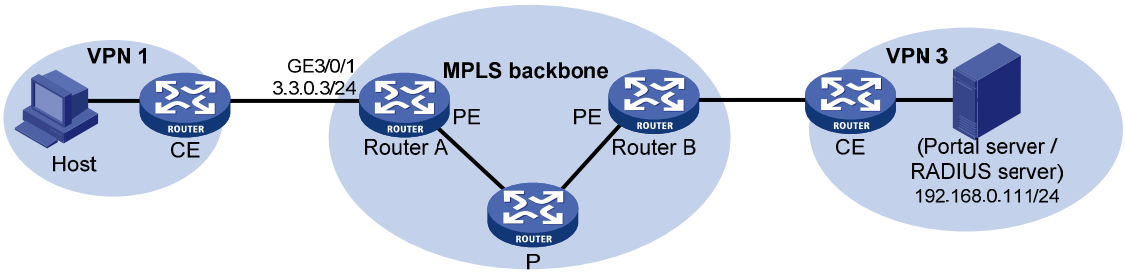
1. 组网需求

连接客户端的 PE 设备 Rourer A 对私网 VPN 1 中的用户 Host 进行 Portal 接入认证，RADIUS 服务器和 Portal 服务器位于私网 VPN 3 中。

- 配置 Rourer A 采用可跨三层 Portal 认证。用户在通过身份认证后，可以访问非受限网络资源。
- RADIUS 服务器和 Portal 服务器由同一台服务器承担。

2. 组网图

图1-31 配置可跨三层 Portal 认证支持多实例组网图



3. 配置步骤

说明

- 启动 Portal 之前，需要首先配置 MPLS L3VPN 功能，通过为 VPN 1 和 VPN 3 指定匹配的 VPN Target，确保 VPN 1 和 VPN 3 可以互通。本例仅介绍连接客户端的 PE 上接入认证的相关配置，其它配置请参考“MPLS 配置指导”中的“MPLS L3VPN”。
- 完成 RADIUS 服务器上的配置，保证用户的认证/计费功能正常运行。

在 Router A 上进行以下配置。

(1) 配置 RADIUS 方案

创建名字为 rs1 的 RADIUS 方案并进入该方案视图。

```
<RouterA> system-view
[RouterA] radius scheme rs1
```

配置 RADIUS 方案所属的 VPN 实例为 vpn3。

```
[RouterA-radius-rs1] vpn-instance vpn3
```

配置 RADIUS 方案的服务器类型。使用 CAMS/iMC 服务器时，RADIUS 服务器类型应选择 **extended**。

```
[RouterA-radius-rs1] server-type extended
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[RouterA-radius-rs1] primary authentication 192.168.0.111
[RouterA-radius-rs1] primary accounting 192.168.0.111
[RouterA-radius-rs1] key accounting simple radius
[RouterA-radius-rs1] key authentication simple radius
```

配置向 RADIUS 服务器发送的用户名不携带域名。

```
[RouterA-radius-rs1] user-name-format without-domain
```

配置发送 RADIUS 报文使用的源地址为 3.3.0.3。

```
[RouterA-radius-rs1] nas-ip 3.3.0.3
[RouterA-radius-rs1] quit
```

说明

建议通过命令 **nas-ip** 指定设备发送 RADIUS 报文的源地址，并与服务器上指定的接入设备 IP 保持一致，避免未指定源地址的情况下，设备选择的源地址与服务器上指定的接入设备 IP 不一致，而造成认证失败。

(2) 配置认证域

创建并进入名字为 dm1 的 ISP 域。

```
[RouterA] domain dm1
```

配置 ISP 域的 RADIUS 方案 rs1。

```
[RouterA-isp-dm1] authentication portal radius-scheme rs1
[RouterA-isp-dm1] authorization portal radius-scheme rs1
[RouterA-isp-dm1] accounting portal radius-scheme rs1
[RouterA-isp-dm1] quit
```

配置系统缺省的 ISP 域 dm1，所有接入用户共用此缺省域的认证和计费方式。若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方案。

```
[RouterA] domain default enable dm1
```

(3) 配置 Portal 认证

配置 Portal 服务器：名称为 newpt，IP 地址为 192.168.0.111，所属的 VPN 为 vpn3，密钥为明文 portal，端口为 50100，URL 为 http://192.168.0.111:8080/portal。

```
[RouterA] portal server newpt ip 192.168.0.111 vpn-instance vpn3 key simple portal port 50100
url http://192.168.0.111:8080/portal
```

在与客户端相连的接口上使能 Portal 认证。

```
[RouterA] interface gigabitethernet 3/0/1
[RouterA-GigabitEthernet3/0/1] portal server newpt method layer3
[RouterA-GigabitEthernet3/0/1] quit
```

4. 验证配置结果

以上配置完成后，通过执行命令 **display portal server** 可查看 Portal 配置是否生效。用户认证通过后，通过执行命令 **display portal user** 查看 Router A 上生成的 Portal 在线用户信息。

```
[RouterA] display portal user all
 Index:2
 State:ONLINE
 SubState:NONE
```

```
ACL:NONE
Work-mode:stand-alone
VPN instance:vpn1
MAC              IP               Vlan   Interface
--------------------------------------------------------------------------------
000d-88f7-c268   3.3.0.1          0      GigabitEthernet3/0/1
Total 1 user(s) matched, 1 listed.
```

1.15 常见配置错误举例

1.15.1 接入设备和Portal服务器上的密钥不一致

1. 故障现象

用户被强制去访问 Portal 服务器时没有弹出 Portal 认证页面，也没有错误提示，登录的 Portal 认证服务器 Web 页面为空白。

2. 故障分析

接入设备上配置的 Portal 密钥和 Portal 服务器上配置的密钥不一致，导致 Portal 服务器报文验证出错，Portal 服务器拒绝弹出认证页面。

3. 处理过程

使用 **display portal server** 命令查看接入设备上配置的 Portal 服务器密钥，并在系统视图中使用 **portal server** 命令修改密钥，或者在 Portal 服务器上查看对应接入设备的密钥并修改密钥，直至两者的密钥设置一致。

1.15.2 接入设备上服务器端口配置错误

1. 故障现象

用户通过 Portal 认证后，在接入设备上使用 **portal delete-user** 命令强制用户下线失败，但是使用客户端的“断开”属性可以正常下线。

2. 故障分析

在 Portal 上使用 **portal delete-user** 命令强制用户下线时，由接入设备主动发送下线请求报文到 Portal 服务器，Portal 服务器默认的报文监听端口为 50100，但是因为接入设备上配置的服务器监听端口错误（不是 50100），即其发送的下线请求报文的目的端口和 Portal 服务器真正的监听端口不一致，故 Portal 服务器无法收到下线请求报文，Portal 服务器上的用户无法下线。

当使用客户端的“断开”属性让用户下线时，由 Portal 服务器主动向接入设备发送下线请求，其源端口为 50100，接入设备的下线应答报文的目的端口使用请求报文的源端口，避免了其配置上的错误，使得 Portal 服务器可以收到下线应答报文，从而 Portal 服务器上的用户成功下线。

3. 处理过程

使用 **display portal server** 命令查看接入设备对应服务器的端口，并在系统视图中使用 **portal server** 命令修改服务器的端口，使其和 Portal 服务器上的监听端口一致。