H3C MSR 系列路由器 典型配置案例集(Web)

新华三技术有限公司
http://www.h3c.com/

软件版本：R6728
资料版本：6W100-20221108

环境保护

本产品符合关于环境保护方面的设计要求，产品的存放、使用和弃置应遵照相关国家法律、法规要求进行。

前 言

本配置指导主要介绍 H3C MSR 系列路由器 Web 典型配置案例。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... }*	表示从多个选项中至少选取一个。
[x | y | ...]*	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
说明	对操作内容的描述进行必要的补充和说明。
窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

1 典型配置举例 导读

H3C MSR 系列路由器 典型配置案例集(Web)共包括 9 个文档，介绍了 MSR 系列路由器常用特性的典型配置举例，包含组网需求、配置步骤和验证配置等内容。

1.1 适用款型及软件版本

本手册所描述的内容适用于 H3C MSR 系列路由器 Release 6728 及其以上版本。

1.2 内容简介

手册包含的文档列表如下：

编号	名称
1	H3C MSR系列路由器登录Web界面典型配置举例
2	H3C MSR系列路由器管理账户典型配置举例
3	H3C MSR系列路由器静态路由典型配置举例
4	H3C MSR系列路由器如何连接云平台配置举例
5	H3C MSR系列路由器系统升级典型配置举例
6	H3C MSR系列路由器端口映射典型配置举例
7	H3C MSR系列路由器IPsec VPN典型配置举例
8	H3C MSR系列路由器L2TP VPN典型配置举例
9	H3C MSR系列路由器无线AC典型配置举例

目 录

1 简介

本文档介绍登录路由器 Web 界面的典型配置举例。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

3 使用限制

- 建议使用 Internet Explorer 10 及以上版本、Chrome 57 及以上版本、Firefox 35 及以上版本的浏览器访问 Web 管理界面。
- 使用的浏览器必须要设置能接受第一方 Cookie（即来自站点的 Cookie），并启用活动脚本（或 JavaScript），才能正常访问 Web。以上功能在不同浏览器中的名称及设置方法可能不同，请以实际情况为准。
- 使用 Internet Explorer 浏览器时，还必须启用以下两个功能才能正常访问 Web：对标记为可安全执行脚本的 ActiveX 控件执行脚本、运行 ActiveX 控件和插件。
- 更改设备的软件版本后，建议在登录 Web 管理界面之前先清除浏览器的缓存，以便正确地显示 Web 页面。
- 本举例适用于首次登录设备 Web 管理界面。

4 使用版本

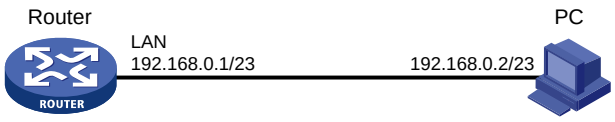
本配置举例是在 MSR830-10HI 路由器 Release 6728P19 版本上进行配置和验证的。

5 配置举例

5.1 组网需求

如图 1 所示，Host 与设备通过直连方式相连。通过本配置，使 Host 可以通过 Web 方式登录设备。

图1 登录 Web 界面配置组网图



5.2 配置步骤

1. 给设备上电

给设备上电，让设备正常启动运行。操作步骤如下：

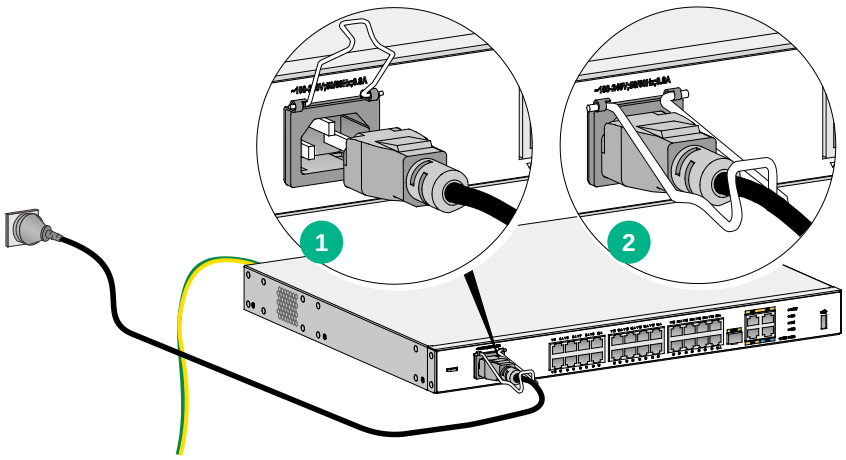
(1) 将电源线一端插入到设备的电源接口。

(2) 用卡扣固定住电源线。

(3) 将另一端连接到外部的交流电源插座上。

(4) 待设备系统指示灯（SYS）为绿色闪烁时，表示设备已正常运行。

图2 给设备上电



2. 连接设备和 Host

用网线将 Host 网口和设备上的 LAN 接口相连。

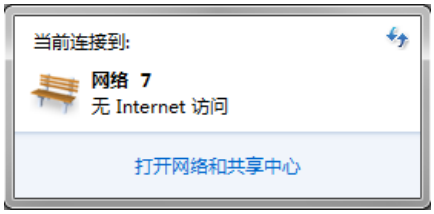
3. 配置 Host 网卡

说明

配置 Host 网卡为自动获取 IP 地址，或手工配置 Host 网卡的 IP 地址为 192.168.0.2/23（即与设备 IP 地址在同一网段），保证其能与设备互通。

本例采用手工配置 Host 网卡 IP 地址（以装有 Win7 系统的 PC 为例），配置步骤如下：

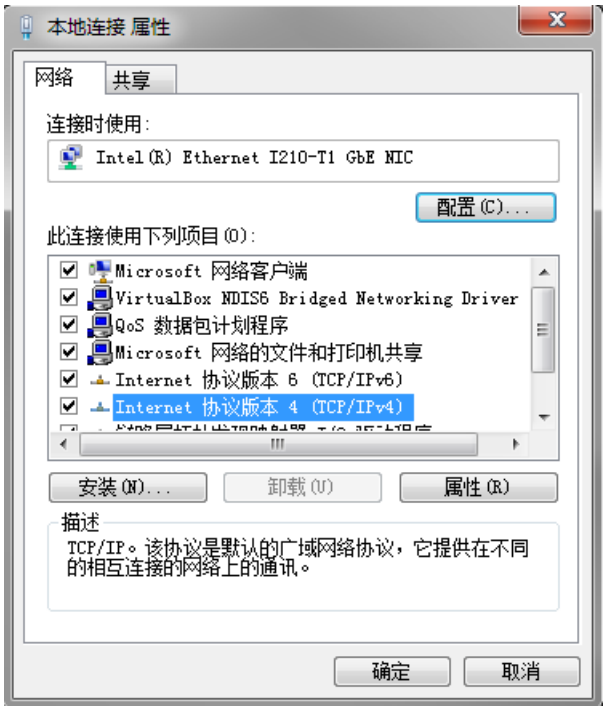
(1) 单击桌面右下角（即任务栏中）的网络图标，选择“打开网络和共享中心”选项，进入网络和共享中心页面。



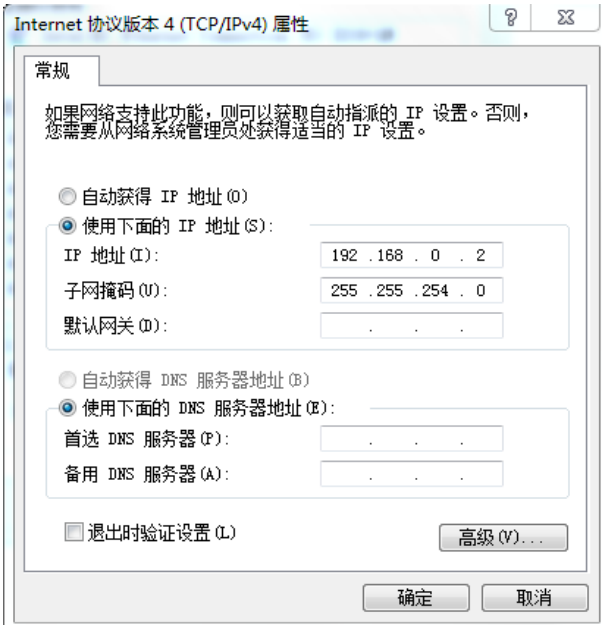
(2) 单击“本地连接”链接，进入本地连接状态页面。

(3) 单击<属性>按钮，进入本地连接属性页面。

(4) 双击“Internet 协议版本 4（TCP/IPv4）”选项，进入 Internet 协议版本 4（TCP/IPv4）属性页面。



(5) 选择“使用下面的 IP 地址（S）”选项，在 IP 地址（I）配置项处，输入 192.168.0.2，在子网掩码配置项处，输入 255.255.254.0。



(6) 单击<确定>按钮，完成配置。

4. 登录设备

说明

设备缺省的登录地址为是 http://192.168.0.1 或 https://192.168.0.1。缺省的登录用户名是 admin，密码是 admin。首次登录后，需要修改密码。

本例使用缺省登录地址“http://192.168.0.1”登录设备，配置步骤如下：

(1) 在 Host 上启动浏览器，在浏览器的地址栏中输入“http://192.168.0.1”，然后回车，进入设备的 Web 登录页面。

(2) 在“用户名”配置项处输入 admin；在“密码”配置项处输入 admin。

(3) 单击<登录>按钮，弹出修改密码页面。

图3 Web 登录页面

(4) 在“旧密码”配置项处，输入 admin。

(5) 在“新密码”配置项处，输入设置的新密码。

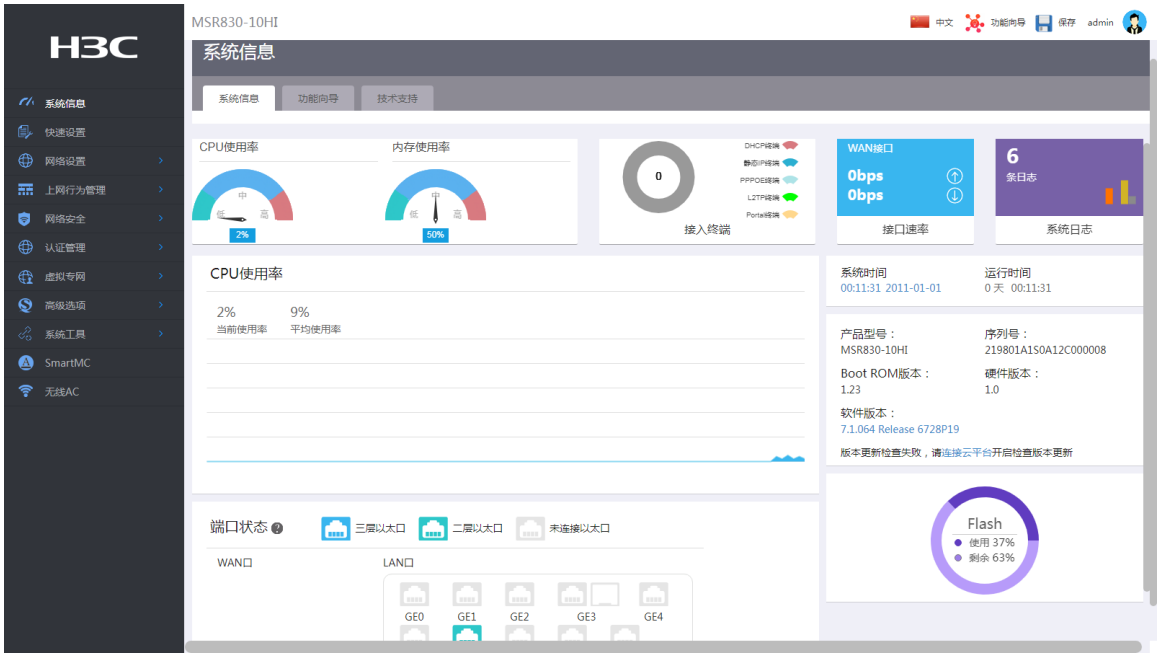
(6) 在“密码确认”配置项处，再次输入设置的新密码。

(7) 单击<确定>按钮，完成登录密码的修改。

图4 修改缺省 Web 登录密码

登录密码修改后，系统会自动跳转到设备 Web 管理界面，Web 登录成功。

图5 成功登录设备 Web 管理界面



目 录

1 简介

本文档介绍管理账户的配置方式。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解管理员和远程管理特性。

3 使用版本

本配置举例是在 MSR830-10HI 路由器 Release 6728P19 版本上进行配置和验证的。

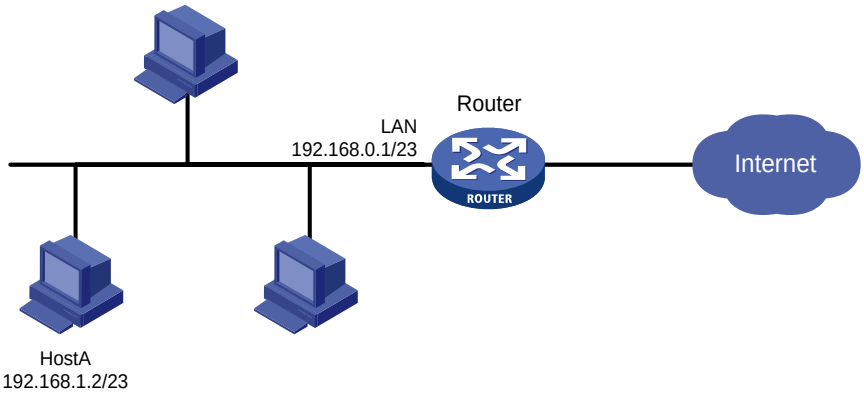
4 配置举例

4.1 组网需求

如图 1 所示，缺省情况下，LAN（VLAN1）接口下的所有 PC 都可以使用 admin 账户登录 Router 的 Web 管理界面。现为方便管理，要求如下：

- 添加管理员用户名为 webuser，密码为 router123456，删除缺省管理员账户 admin。
- 只允许 LAN 接口下的 Host A 访问设备 Web 管理界面。

图1 管理账户组网图



4.2 配置步骤

1. 添加管理员用户名和密码

本例将添加一个设备的管理员账户，用户名为 webuser，密码为 router123456。配置步骤如下：

(1) 登录设备 Web 管理界面，设备 Web 管理界面导航栏中选择“系统工具>管理账户”，进入管理账户配置页面。

(2) 点击<添加>按钮，进入添加管理员页面。

(3) 在“用户名”配置项处，输入 webuser。

(4) 在“密码”配置项处，输入 router123456。

(5) 在“确认密码”配置项处，再次输入 router123456。

(6) 在“角色”配置项处，选择 Administrator。

(7) 在“可用服务”配置项处，选择 WEB。

(8) 单击<确定>按钮，完成配置。

图2 添加管理员用户名和密码

2. 删除缺省管理员账户 admin

本例将删除设备的缺省管理员账户 admin。配置步骤如下：

(1) 在设备 Web 管理界面导航栏中选择“系统工具>管理账户”，进入管理账户配置页面。

(2) 在用户行的“操作”区域，点击删除按钮，删除缺省管理员账户 admin。

(3) 在弹出的“确认提示”对话框中，点击<是>按钮，完成删除操作。

3. 配置管理 IP 地址

本例将允许访问设备 Web 管理界面的 IP 地址设置为 Host A 的 IP 地址 192.168.1.2。注意：设置完成后，其它 IP 地址将不可以访问设备 Web 管理界面。

(1) 在设备 Web 管理页面，单击执行区域右上角“管理员”图标，在下拉框中选择“退出”。

(2) 在弹出的“确认提示”对话框中，点击<是>按钮，完成退出操作。

(3) 使用新的用户名和密码登录设备 Web 管理界面。

(4) 在设备 Web 管理界面导航栏中选择“系统工具>远程管理”，进入远程管理界面。

(5) 单击“HTTP/HTTPS”页签，进入 HTTP/HTTPS 配置页面。

(6) 点击<添加>按钮，进入添加管理员 IP 地址页面。

(7) 单击“IP 地址段（默认推荐）192.168.1.2-192.168.1.254”后的删除图标，删除之前可登录设备 Web 管理界面的 IP 地址段。

(8) 在“IP 地址”配置项处，输入 Host A 的 IP 地址 192.168.1.2。

(9) 点击配置项右侧的<→→>按钮，提交配置的地址内容。

(10) 单击<确定>按钮，完成配置。

图3 修改管理 IP 地址

4.3 验证配置

仅在 Host A（IP 地址为 192.168.1.2/23）上可以使用用户名 webuser，密码 router123456 登录设备 Web 管理界面，能够成功登录，说明配置验证成功。

目 录

1 简介

本文档介绍路由器静态路由典型配置举例。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解静态路由特性。

3 使用限制

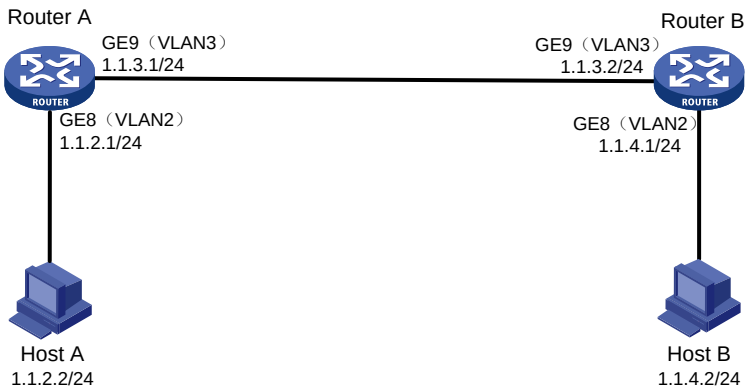
静态路由的配置必须确保下一跳网络可达，并且下一跳设备也必须存在到本设备和目的地址的路由。

4 配置举例

4.1 组网需求

如图 1 所示，在 Router A、Router B 上配置静态路由，实现 Host A 以及 Host B 的相互访问。

图1 静态路由配置组网图



4.2 使用版本

本配置举例是在 MSR830-10HI 路由器 Release 6728P19 版本上进行配置和验证的。

4.3 配置思路

在 Router A 上，需要进行如下配置：

- 划分 VLAN2 和 VLAN3，并配置 VLAN 接口 IP 地址。
- 将 GE8 接口划分 VLAN2，将 GE9 接口划分到 VLAN3。
- 添加到 Host B 所在子网 1.1.4.1/24 的静态路由。

在 Router B 上，需要进行如下配置：

- 划分 VLAN2 和 VLAN3，并配置 VLAN 接口 IP 地址。
- 将 GE8 接口划分 VLAN2，将 GE9 接口划分到 VLAN3。
- 添加到 Host A 所在子网 1.1.2.1/24 的静态路由。

4.4 配置步骤

4.4.1 配置 Router A

1. 划分 VLAN2，并配置接口 IP 地址

在 Router A 上添加 VLAN2，其接口 IP 地址为 1.1.2.1,配置步骤如下:

(1) 在设备 Web 管理界面导航栏中选择“网络设置 > LAN 配置”，进入 LAN 配置页面。

(2) 单击<添加>按钮，进入添加 LAN 页面。

(3) 在“LAN 接口类型”配置项处，选择 VLAN 接口。

(4) 在“VLAN ID”配置项处，输入 2。

(5) 在“接口 IP 地址”配置项处，输入 1.1.2.1。

(6) 在“子网掩码”配置项处，输入 255.255.255.0。

(7) 其它配置项保持默认配置，单击<确定>按钮，完成配置。

图2 配置 VLAN2

2. 划分 VLAN3，并配置接口 IP 地址

在 Router A 上添加 VLAN3，其接口 IP 地址为 1.1.3.1，配置步骤如下:

(1) 在设备 Web 管理界面导航栏中选择“网络设置 > LAN 配置”，进入 LAN 配置页面。

(2) 单击<添加>按钮，进入添加 LAN 页面。

(3) 在“LAN 接口类型”配置项处，选择 VLAN 接口。

(4) 在“VLAN ID”配置项处，输入 3。

(5) 在“接口 IP 地址”配置项处，输入 1.1.3.1。

(6) 在“子网掩码”配置项处，输入 255.255.255.0。

(7) 其它配置项保持默认配置，单击<确定>按钮，完成配置。

图3 配置 VLAN3

3. 将 GE8 接口划分到 VLAN2

(1) 在设备 Web 管理界面导航栏中选择“网络设置 > LAN 配置”，进入 VLAN 划分页面。

(2) 单击 GE8 对应的操作列编辑图标，进入详细端口配置页面。

(3) 在“PVID”配置项处，选择 2。

(4) 单击<确认>按钮，完成配置。

图4 将 GE 接口划分到指定的 VLAN

4. 将 GE9 接口划分到 VLAN3

(1) 在设备 Web 管理界面导航栏中选择“网络设置 > LAN 配置”，进入 VLAN 划分页面。

(2) 单击 GE9 对应的操作列编辑图标，进入详细端口配置页面。

(3) 在“PVID”配置项处，选择 3。

(4) 单击<确定>按钮，完成配置。

图5 将 GE 接口划分到指定的 VLAN

5. 配置静态路由

在 Router A 上添加目的 IP 地址为 1.1.4.0，下一跳 IP 地址为 1.1.3.2 的 IPv4 静态路由。

(1) 在设备 Web 管理界面导航栏中选择“高级选项 > 静态路由”，进入静态路由配置页面。

(2) 单击<添加>按钮，进入添加 IPv4 静态路由页面。

(3) 在“目的 IP 地址”配置项处，输入 1.1.4.0。

(4) 在“掩码长度”配置项处，输入 24。

(5) 在“下一跳”配置项处，取消出接口前方的勾选，在“下一跳 IP 地址”配置项处，输入 1.1.3.2。

(6) 单击<确定>按钮，完成配置。

图6 配置静态路由

4.4.2 配置 Router B

1. 划分 VLAN2，并配置接口 IP 地址

在 Router B 上添加 VLAN2，其接口 IP 地址为 1.1.4.1。配置步骤请参见 “4.4.1 1. 划分 VLAN2，并配置接口 IP 地址”。

2. 划分 VLAN3，并配置接口 IP 地址

在 Router B 上添加 VLAN3，其接口 IP 地址为 1.1.3.2。配置步骤请参见 “4.4.1 2. 划分 VLAN3，并配置接口 IP 地址”。

3. 将 GE8 接口划分到 VLAN2

在 Router B 上将 GE8 接口划分到 VLAN2。配置步骤请参见“4.4.1 3. 将 GE8 接口划分到 VLAN2”。

4. 将 GE9 接口划分到 VLAN3

在 Router B 上将 GE9 接口划分到 VLAN3。配置步骤请参见“4.4.1 4. 将 GE9 接口划分到 VLAN3”。

5. 配置静态路由

在 Router B 上添加到 Host A 所在子网 1.1.2.1/24 的静态路由，下一跳 IP 地址为 1.1.3.1。配置步骤请参见 “4.4.1 5. 配置静态路由”。

5 验证配置

在 Host A 主机上 ping Host B 主机的 IP 地址 1.1.4.2，如果能够 Ping 通，则说明配置成功。

```
C:\Users\abc>ping 1.1.4.2

正在 Ping 1.1.4.2 具有 32 字节的数据:
来自 1.1.4.2 的回复: 字节=32 时间=1ms TTL=252
来自 1.1.4.2 的回复: 字节=32 时间=1ms TTL=252
来自 1.1.4.2 的回复: 字节=32 时间=1ms TTL=252
来自 1.1.4.2 的回复: 字节=32 时间=1ms TTL=252

1.1.4.2 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms，最长 = 1ms，平均 = 1ms
```

目 录

1 简介

本文档介绍路由器远程管理-云服务的配置方法。

当网络管理员需要远程监管或运维设备时，可以通过设备 Web 页面上的云服务功能将设备绑定到 H3C 云简网络平台（以下简称云平台）来实现。

H3C 云简网络是主要面向中小企业用户的轻量级多业务平台，适用于中小企业办公网络，中小型商业网络以及分支连锁场景。云简网络为以上类型场景提供场景化解决方案，包括开局部署，设备监管，无线运维，数据对接与应用等。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解远程管理-云服务特性。

3 使用版本

本配置举例是在 MSR3610-X1 路由器 Release 6728P22 版本上进行配置和验证的。

4 配置准备

首次登录 H3C 云简网络平台需要注册账户，相关操作可以参考 https://www.h3c.com/cn/Service/Document_Software/Document_Center/Oasis/Catalog/Oasis_Platform/Oasis_Platform/Guide_Manual/Oasis_Guide/H3C_BS_Manual-6W104/中的云简网络账户注册方法，或者参考下文“6.2.2 注册云平台账户”章节。

5 配置注意事项

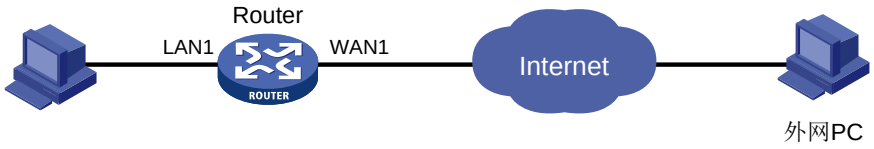
MSR 系列路由器当前仅支持绑定到 H3C 云简网络平台。

6 配置举例

6.1 组网需求

如图 1 所示，某企业要求将公司出口路由器绑定到云平台，方便远程对设备进行监管和运维。

图1 云服务配置举例



6.2 配置步骤

6.2.1 启用远程管理-云服务功能

#确认设备 Web 管理界面的云服务功能为开启状态，步骤如下：

(1) 在设备 Web 管理界面导航栏中选择“系统工具 > 远程管理”，进入远程管理配置页面。

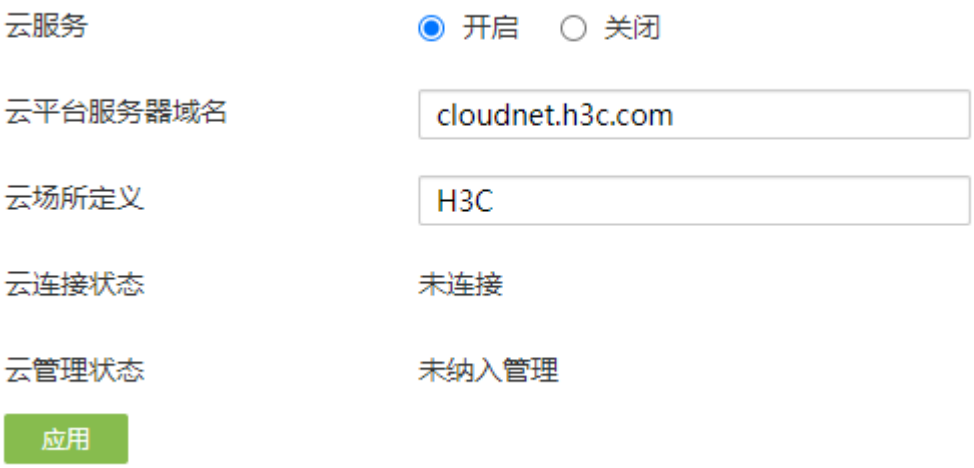
(2) 单击“云服务”页签，进入云服务配置页面。

(3) 在“云服务”配置项处，选择开启。（缺省就为开启状态，该步骤可省略）

(4) “云平台服务器域名”配置项处默认配置为 H3C 云简网络平台域名，保持默认配置即可。

(5) “云场所定义”配置项处默认配置为“H3C”，可自定义修改。

图2 开启远程管理-云服务功能



6.2.2 注册云平台账户

#云平台的服务器域名为“cloudnet.h3c.com”,建议使用谷歌、火狐或 Edge 浏览器打开，首次登录需要进行账户注册。配置步骤如下：

(1) 在浏览器地址栏输入 http://cloudnet.h3c.com/，进入云简网络平台登录页面。

图3 云简网络登录页

(2) 单击“还没有账户立即注册”选项，进入用户注册页面。

(3) 在“用户名”配置项处，输入自定义的用户名。

(4) 在“验证码”配置项处，输入该配置项后面显示的验证码。

(5) 在“手机号”配置项处，输入手机号。

(6) 单击<获取验证码>按钮，验证码会以短信的形式发送到您注册的手机上。

(7) 在“手机验证码”配置项处，输入短信获取的验证码。

(8) 在“登录密码”配置项处，输入自定义的登录密码。

(9) 在“确认密码”配置项处，再次输入自定义的密码。

(10) 勾选“同意《用户条款》《隐私政策》”前方的单选框，同意相关协议。

(11) 单击<完成注册>按钮，完成账户注册。

图4 注册页

6.2.3 登录云简网络平台

(1) 返回云简网络平台登录页面。

(2) 在“用户名/手机号/邮箱”配置项处，输入注册的用户名或手机号。

(3) 在“密码”配置项处，输入注册的密码。

(4) 单击<登录>按钮，进入云简网络平台首页。

图5 云简网络平台首页

6.2.4 划分分支和增加场所

说明

场所为存放网络设备的虚拟容器，一般同一场所仅能存放同一产品类型、同一设备类型的网络设备；分支为存放场所的虚拟容器，一般会根据一定的规划划分分支，例如地区，品牌等。

#本例在云平台划分名称为“浙江”的分支，然后在该分支下增加名称为“杭州”的场所。配置步骤如下：

(1) 在云简网络平台首页顶部导航栏中选择“网络管理”选项，然后选择左侧导航栏中的“网络-组织”，进入组织页面。

(2) 单击左侧<+增加>按钮，弹出添加分支对话框。

(3) 在分支名称配置项处，输入浙江。

(4) 单击<确认>按钮，完成分支的划分。

(5) 单击右侧<+增加>按钮，弹出增加场所对话框，场所类型选择“通用”。

图6 场景类型配置

(6) 单击<下一步>按钮，进行场所名称配置。

(7) 在“场所名称”配置项处，输入杭州。

(8) 在“分支”配置项处，选择“浙江”。

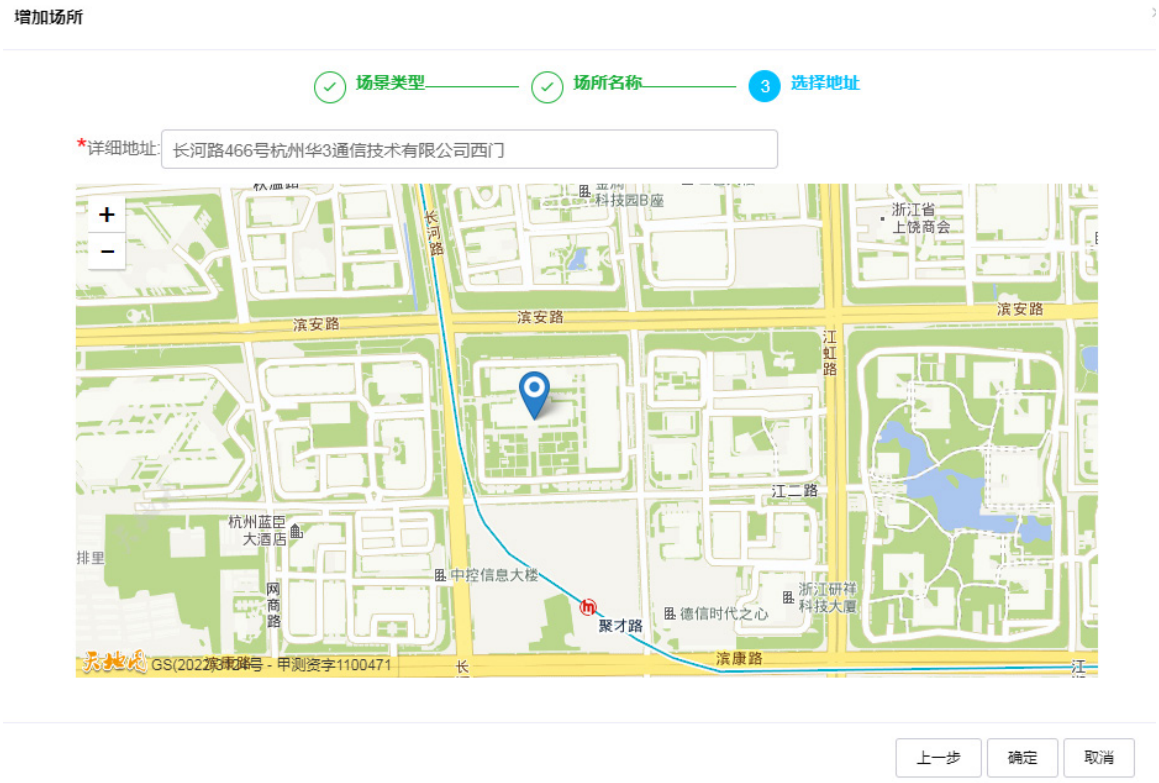
(9) 在“所属行业”配置项处，选择其他（可根据实际情况选择行业类型）。

图7 场所名称配置

(10) 单击<下一步>按钮，在详细地址配置项处输入设备的详细地址。

(11) 单击<确定>按钮，完成场所的添加。

图8 场所名称配置



6.2.5 在场所中添加设备

将本例中的出口路由器添加到“杭州”场所，增加设备之前需在路由器 Web 管理界面“系统信息”页面中查看设备序列号。配置步骤如下：

(1) 在云简网络平台首页顶部导航栏中选择“网络管理”选项，然后选择左侧导航栏中的“网络-设备”。

(2) 单击<增加设备>按钮，进入增加设备页面。

(3) 在“场所”配置项处，选择“杭州”。

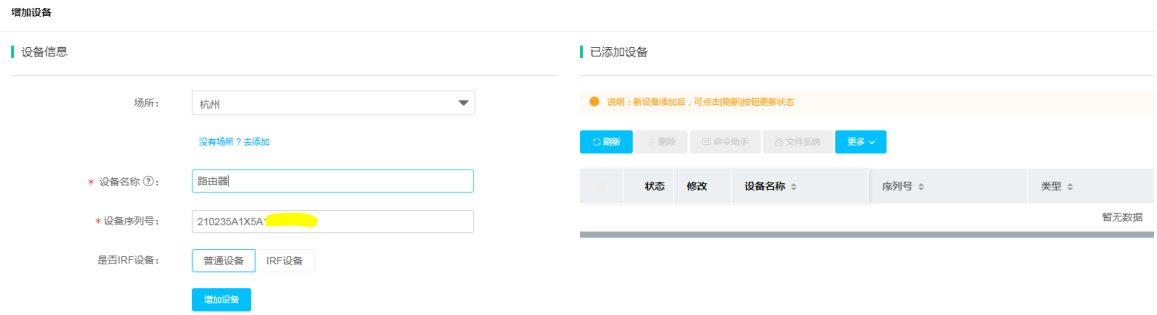
(4) 在“设备名称”配置项处，输入路由器。（可根据需要自定义）

(5) 在“设备系列号”配置项处，输入出口路由器的序列号。

(6) 在“设备类型”配置项处，选择“普通设备”。

(7) 单击<添加>按钮，完成设备的增加。

图9 增加设备

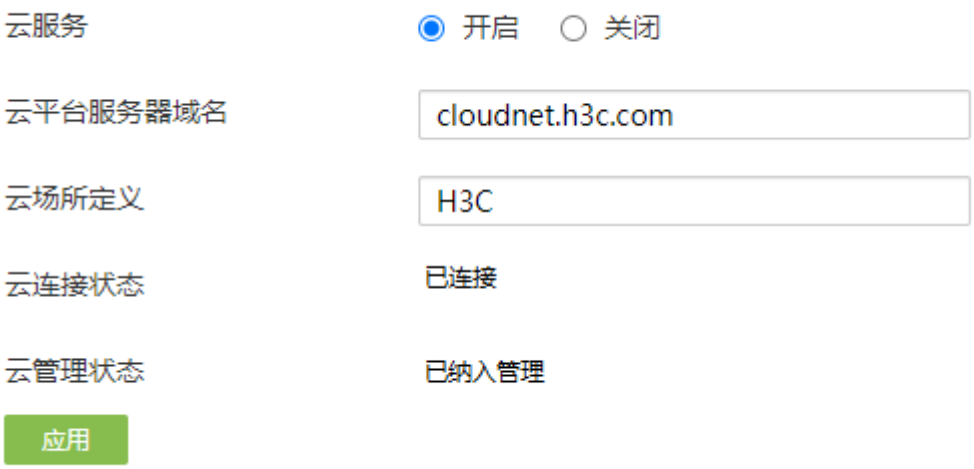


6.3 验证配置

(1) 登录路由器 Web 管理界面，选择“系统工具 > 远程管理”，进入远程管理配置页面。

(2) 单击“云服务”页签，进入云服务配置页面，查看云连接状态为“已连接”、云管理状态为“已纳入管理”，说明设备已成功绑定云简网络平台，配置成功。如显示“未连接”，请重新检查配置或设备网络的连通性。

图10 验证配置



目 录

1 简介

本文档介绍路由器系统升级的配置方法。

您可以根据实际的应用环境，选择下面两种升级方法中的一种进行系统升级操作：

- 手动升级系统软件：通过特定路径下的系统软件文件对设备的系统软件进行升级，具体配置请参见“4.3.1 手动升级系统软件”。
- 自动升级系统软件：设备将通过云平台对设备的系统软件进行升级，具体步骤请参见“4.3.2 自动升级系统软件”。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解系统升级特性。

3 使用版本

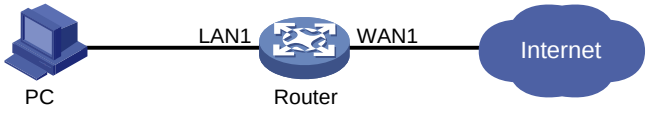
本配置举例是在 MSR3610-X1 路由器 Release 6728P22 版本上进行配置和验证的。

4 配置举例

4.1 组网需求

如图 1 所示，某企业需要对出口路由器（MSR3610-X1）进行系统升级，设备当前软件版本为 Release 6728P22，要求升级到最新的软件版本 Release 6749l01。

图1 系统升级配置组网图



4.2 配置注意事项

- 在进行系统软件升级之前，建议备份当前设备配置文件。
- 系统升级过程中，设备请勿断电。升级成功后设备会自动重启，为防止业务中断，升级过程中，不要随便切换网页，直至完成升级。
- 进行自动升级前，需确保云连接状态为已连接，可以进入设备 Web 管理界面“系统工具 > 远程管理 > 云服务”页面，查看云连接状态。

4.3 配置方法

4.3.1 手动升级系统软件

说明

进行手工升级前，请根据软件版本说明书找到和本设备匹配的软件包（必须为 IPE 文件），并将它保存到您的登录终端。您可以从 https://www.h3c.com/cn/Service/Document_Software/Software_Download/Router/获得最新的软件版本。

(1) 在设备 Web 管理界面导航栏中选择“系统工具 > 系统升级”，进入系统升级配置页面.

(2) 单击“版本升级”页签，进入软件升级页面。

(3) 单击<手动升级系统软件>按钮，进入手工升级系统软件配置页面。

(4) 单击<选择文件>按钮，选择从 H3C 官网下载的软件版本（IPE 文件,如果下载的文件是压缩包，则需要解压缩获取 IPE 文件）,并勾选“立即重启设备”选项。

(5) 单击<确定>按钮，系统会自动上传软件版本，然后进行升级。

图2 手动升级系统软件

4.3.2 自动升级系统软件

(1) #在设备 Web 管理界面导航栏中选择“系统工具 > 系统升级”，进入系统升级页面。

(2) 单击“版本升级”页签，进入软件升级页面。

(3) 单击<自动升级系统软件>按钮，进入升级系统软件页面。

(4) 单击<确定>按钮，系统将进行自动升级。

图3 自动升级系统软件

目 录

1 简介

本文档介绍路由器端口映射的配置方法。

当外网用户（例如出差员工）想要访问搭建在企业内网的服务器时，可以通过配置端口映射（即Web 管理界面中 NAT 配置-虚拟服务器功能）实现。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 NAT 配置-虚拟服务器特性。

3 使用版本

本配置举例是在 MSR3610-X1 路由器 Release 6728P22 版本上进行配置和验证的。

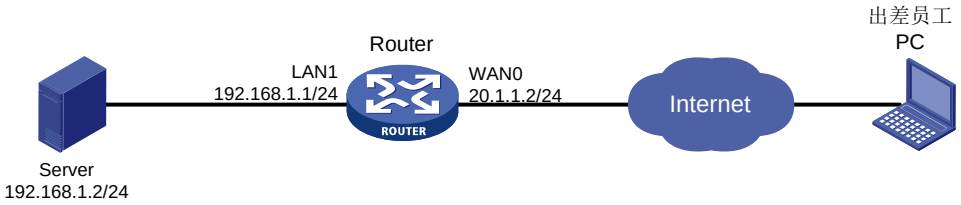
3.1 组网需求

如图 1 所示，Router 为某企业的出口网关，通过 WAN0 接口连接 Internet，WAN0 接口的连接模式为固定地址，IP 地址为 20.1.1.2/24，网关地址为 20.1.1.1。

因企业在外出差员工需要访问搭建在内网的 OA 服务器，因此需要在 Router 上配置端口映射。OA 服务器的信息如下：

- 协议类型：TCP
- IP 地址：192.168.1.2
- 内部端口：80

图1 端口映射典型配置组网图



3.2 配置注意事项

本例中映射的仅是服务器的 Web 服务，外部端口选择自定义端口，起始端口号和结束端口号需要保持一致，建议输入 10000 及以上端口号。本例输入 10000。

3.3 配置步骤

3.3.1 配置路由器上网

本例中外网的接口模式为单 WAN 模式，WAN 接口的连接模式为固定地址。配置步骤如下：

(1) 在设备 Web 管理界面导航栏中选择“网络设置 > 外网配置”，进入外网配置页面。

(2) 在“场景定义”页签下选择单 WAN 模式，单击<应用>按钮使得配置生效。

图2 配置 WAN 场景

(3) 单击“WAN 配置”页签，进入 WAN 配置页面。

(4) 单击 WAN0 接口对应操作列编辑图标，进入修改 WAN 配置页面。

(5) 在“连接模式”配置项处，选择固定地址。

(6) 在“IP 地址”配置项处，输入 20.1.1.2。

(7) 在“子网掩码”配置项处，输入 255.255.255.0。

(8) 在“网关地址”配置项处，输入 20.1.1.1。

(9) 在“NAT 地址转换”配置项处，选择启用。

(10) 其它参数保持默认配置即可，单击<确定>按钮保存配置。

图3 配置 WAN0 接口连接 Internet

3.3.2 配置虚拟服务器（端口映射）

本例外部端口选择自定义端口，起始端口号和结束端口号保持一致，输入 10000。配置步骤如下：

(1) 在设备 Web 管理界面中选择“网络设置 > NAT 配置”，进入 NAT 配置页面。

(2) 在“端口映射”页签下，单击<添加>按钮，进入添加 NAT 端口映射页面。

(3) 在“接口”配置项处，选择当前接口 WAN0。

(4) 在“协议类型”配置项处，选择 TCP。

(5) 在“外部地址”配置项处，选择当前接口 IP 地址。

(6) 在“外部端口”配置项处，选择“自定义端口”，并在起始端口号配置项处输入 10000，结束端口号配置项处输入 10000。

(7) 在“内部地址”配置项处，输入 192.168.1.2（服务器的 IP 地址）。

(8) 在“内部端口”配置项处，起始端口号配置项处输入 80。

(9) 单击<确定>按钮完成配置。

图4 添加 NAT 端口映射

3.4 验证配置

使用出差员工 PC，在浏览器中输入 http://20.1.1.2:10000，可以访问企业内部 OA 服务器网页，配置验证成功。

目 录

1 简介

本文档分别介绍路由器采用主模式和野蛮模式建立 IPsec VPN 的配置方法。

- 主模式：适用于企业和分支路由器外网均有固定公网 IP 地址的场景。
- 野蛮模式：适用于企业和分支路由器其中一端外网无固定公网 IP 地址（例如以 DHCP 方式连接 Internet）的场景。

请根据您的实际组网，参考主模式配置举例或野蛮模式配置举例进行配置。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 IPsec VPN 特性。

3 使用版本

本配置举例是在 MSR3610-X1 路由器 Release 6728P22 版本和 MSR3640-X1-HI 路由器 Release 6728P22 版本上进行配置和验证的。

4 主模式配置举例

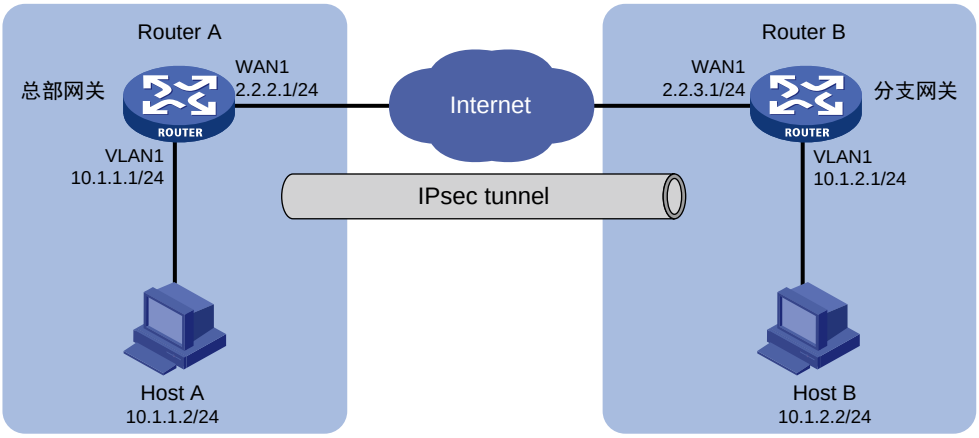
4.1 组网需求

如图 14 所示，Router A 为企业总部网关，Router B 为企业分支网关，Router A 和 Router B 的外网接口模式均为单 WAN 模式，且以固定地址方式连接 Internet。分支与总部通过公网建立通信。

出于安全因素，需要对企业分支与总部之间相互访问的数据流进行安全保护，因此需要在 Router A 和 Router B 之间建立一条 IPsec 隧道。具体要求如下：

- 两端通过预共享秘钥（123456TESTplat&!）进行认证。
- IKE 协商采用的加密算法为 3DES-CBC，认证算法为 MD5。
- IPsec 隧道的封装模式为隧道模式，安全协议为 ESP。

图1 IPsec VPN（主模式）典型配置组网图



4.2 配置思路

采用如下的配置思路：

(1) 完成 WAN 和 LAN 的基本配置

a. 配置 Router A 和 Router B 的 WAN 接口 IP 地址和网关地址等参数。

b. 修改 Router A 和 Router B 的 VLAN1 接口缺省 IP 地址。

(2) 添加 IPsec 策略

由于 Router A 和 Router B 的 WAN 接口均以固定公网 IP 地址连接 Internet，因此 IPsec 策略中的 IKE 协商模式选择主模式。

4.3 配置注意事项

- 修改 VLAN1 接口的 IP 地址后，会导致 Web 管理界面登录异常，需要使用修改后的 IP 地址重新登录 Web 管理界面，才能进行接下来的配置。
- 若您的组网是双 WAN 或多 WAN 接入时，需要在 Router 上需配置一条静态路由，将访问对端内网的流量指向 IPsec 策略中所选用的 WAN 接口。本例中 Router A 和 Router B 均为单 WAN 接入，设备自动生成一条缺省路由，将所有流量指向出接口的网关，所以本例中该步骤可省略。
- IPsec 隧道两端设备的预共享秘钥、安全协议、加密/认证算法以及封装模式需保持一致。

4.4 配置步骤

4.4.1 配置 Router A

1. 修改 VLAN1 接口的 IP 地址

将 VLAN1 接口的 IP 地址修改为 10.1.1.1/24。配置步骤如下：

(1) 在设备 Web 管理界面导航栏中选择“网络设置 > LAN 配置”，进入 LAN 配置页面。

(2) 单击“LAN 配置”页签，进入 LAN 配置页面。

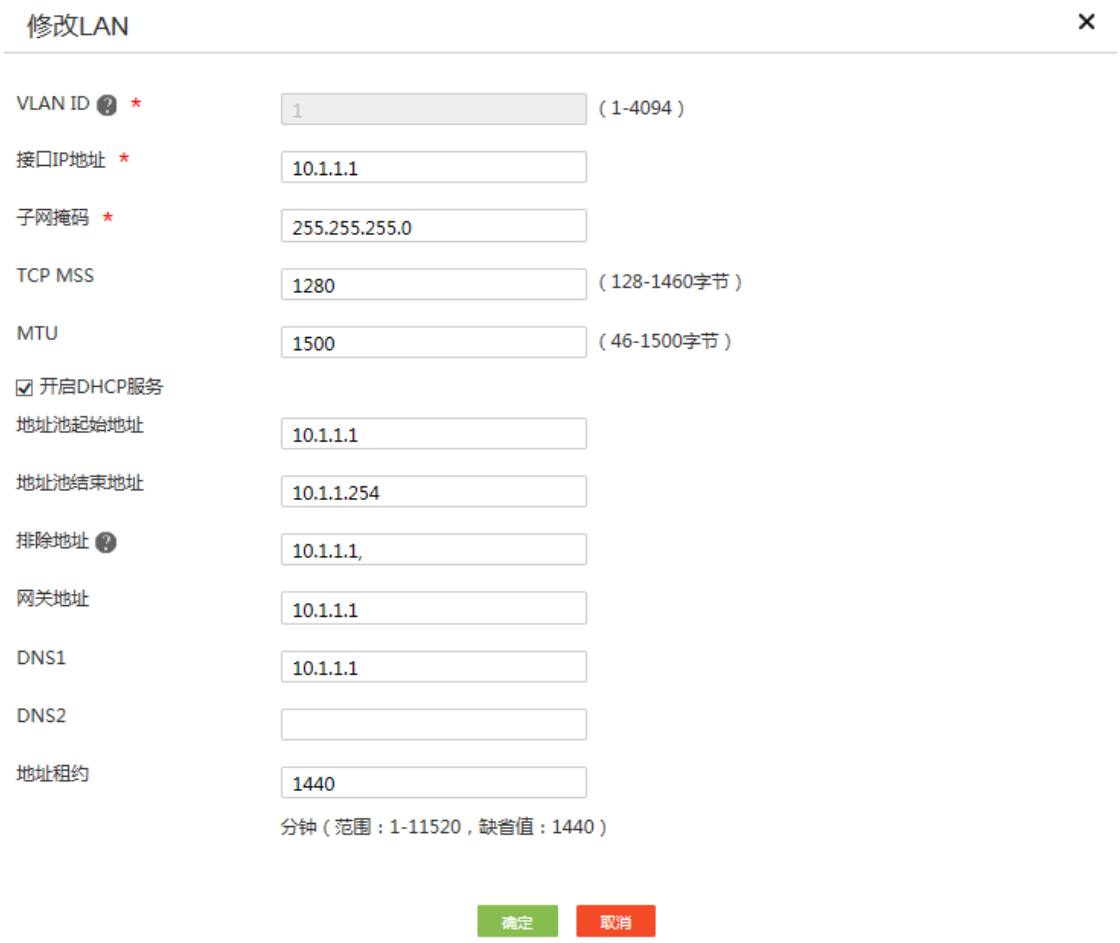
(3) 单击 VLAN1 对应的操作列编辑图标，进入修改 LAN 配置页面。

(4) 在“接口 IP 地址”配置项处，输入 10.1.1.1。

(5) 在“子网掩码”配置项处，输入 255.255.255.0。

(6) 其它配置项均保持默认情况即可，单击<确定>按钮保存配置。

图2 修改 LAN 配置



2. 配置 WAN1 接口连接 Internet

本例中 Router A 外网的接口模式选择单 WAN 模式，WAN 接口的连接模式为固定地址。配置步骤如下：

(1) 在设备 Web 管理界面导航栏中选择“网络设置 > 外网配置”，进入外网配置页面。

(2) 在“场景定义”页签下选择单 WAN 场景，选择线路 1 为 WAN1，单击<应用>按钮使得配置生效。

(3) 单击“WAN 配置”页签，进入 WAN 配置页面。

(4) 单击 WAN1 对应的操作列编辑图标，进入修改 WAN 配置页面。

(5) 在“连接模式”配置项处，选择固定地址。

(6) 在“IP 地址”配置相处，输入 2.2.2.1。

(7)　在“子网掩码”配置项处，输入 255.255.255.0。

(8)　在“网关地址”配置项处，输入 2.2.2.254。

(9)　其它配置项均保持默认情况即可，单击<确定>按钮保存配置。

图3 配置 WAN 场景

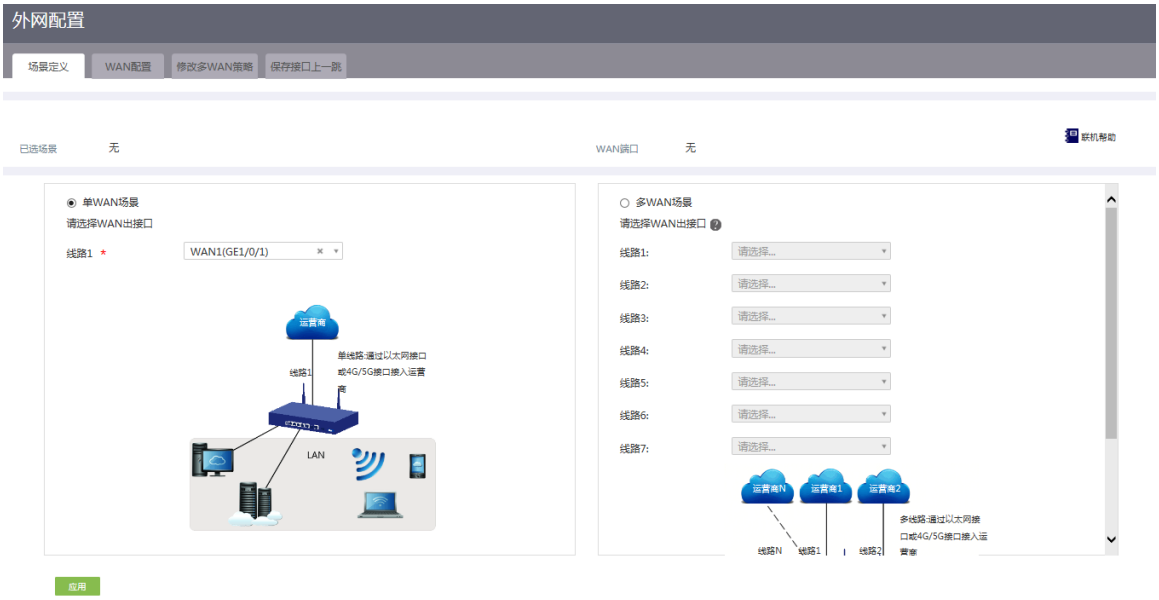
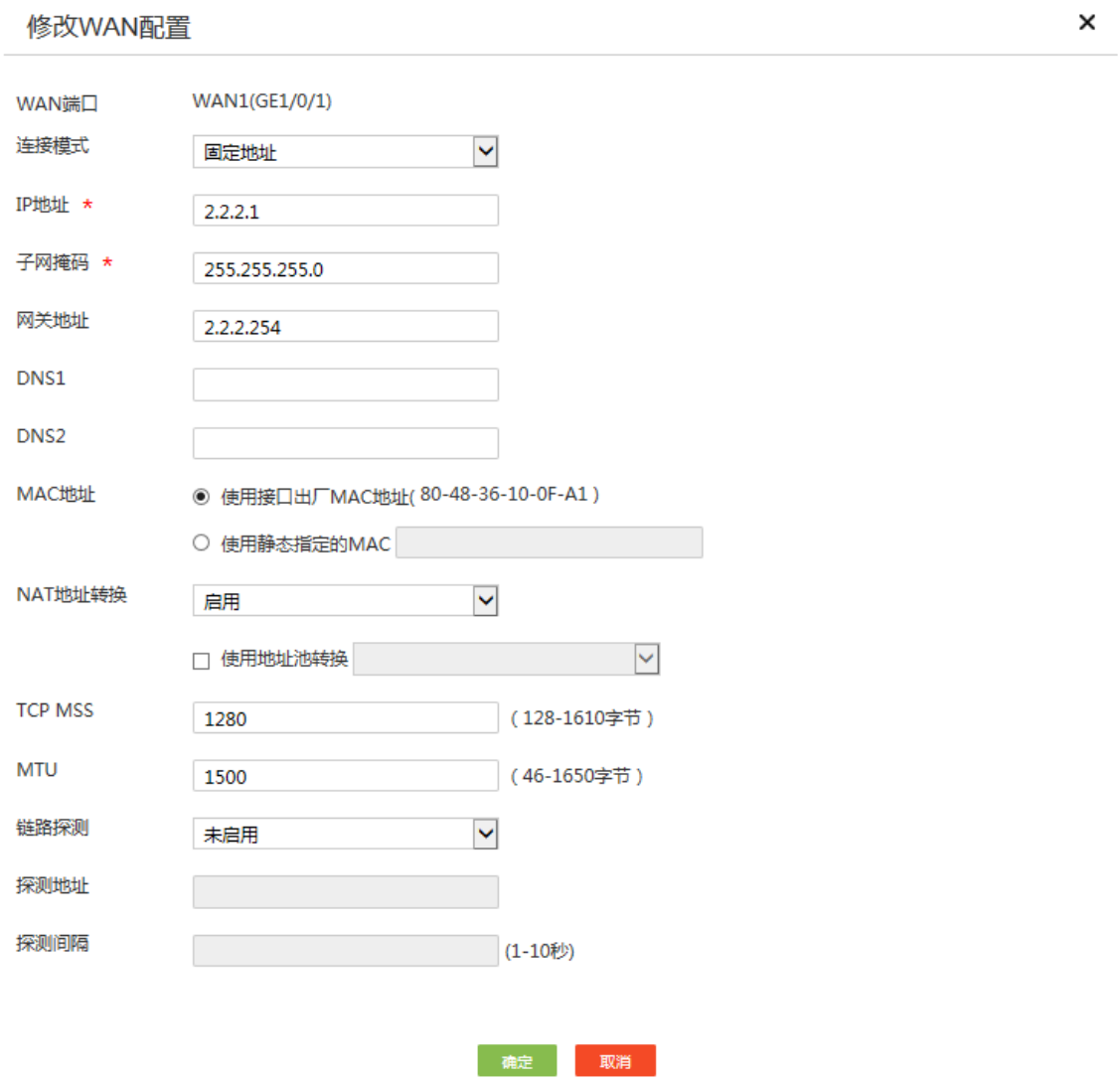


图4 修改 WAN 配置



3. 配置 IPsec 策略

Router A 的 IPsec 策略中的组网方式选择中心节点，IKE 协商模式选择主模式。配置步骤如下：

(1) 在设备 Web 管理界面导航栏中选择“虚拟专网（VPN） > IPsec VPN”，进入 IPsec 策略配置页面。

(2) 单击<添加>按钮，进入添加 IPsec 策略页面，配置如下参数：

- 名称：输入 map1
- 接口：选择 WAN1
- 组网方式：选择中心节点
- 预共享密钥：输入 123456TESTplat&!

图5 配置 IPsec 策略

(3) 单击<显示高级配置>按钮，进入 IKE 配置页面，配置如下参数：

- 协商模式：选择主模式
- 本端身份类型：选择 IP 地址，输入 2.2.2.1
- 对等体存活检测（DPD）：选择开启，超时时间配置为 30（该功能缺省是关闭状态，建议您开启此功能，使设备能够及时获悉 IPsec 隧道的可用情况）
- 算法组合：选择自定义
- 认证算法：选择 MD5
- 加密算法：选择 3DES-CBC
- 其它参数保持缺省配置即可。

图6 IKE 配置

(4) 单击“IPsec 配置”页签，进入 IPsec 配置页面，配置如下参数：

- 算法组合：选择自定义
- 安全协议：选择 ESP
- ESP 认证算法：选择 MD5
- ESP 加密算法：选择 3DES-CBC
- 封装模式：选择隧道模式
- 其它参数保持缺省配置即可

(5) 单击<返回基本设置>按钮，再单击<确定>按钮，完成配置。

图7 IPsec 配置

4.4.2 配置 Router B

1. 修改 VLAN1 接口的 IP 地址

将 VLAN1 接口的 IP 地址修改为 10.1.2.1/24。配置步骤如下：

(1) 在设备 Web 管理界面导航栏中选择“网络设置 > LAN 配置”，进入 LAN 配置页面。

(2) 单击“LAN 配置”页签，进入 LAN 配置页面。

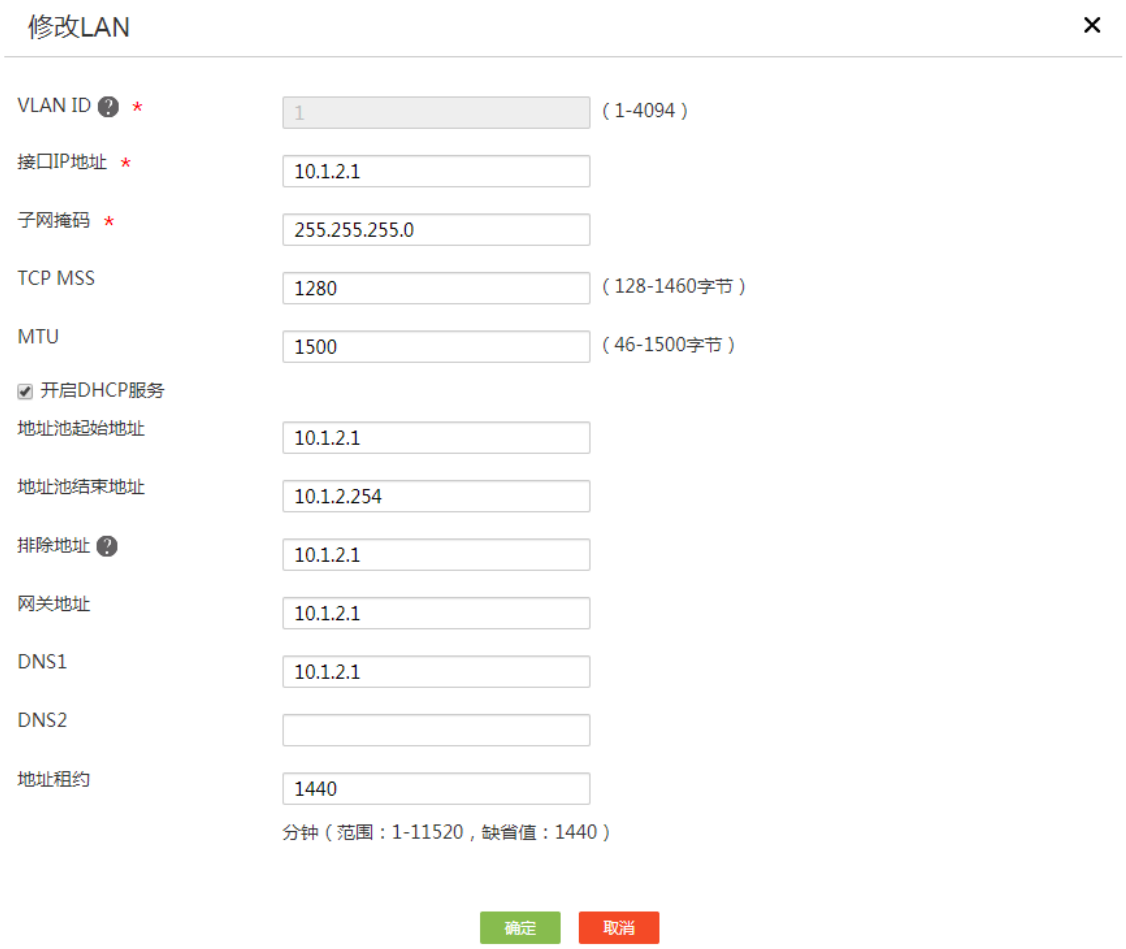
(3) 单击 VLAN1 对应的操作列编辑图标，进入修改 LAN 配置页面。

(4) 在“接口 IP 地址”配置项处，输入 10.1.2.1。

(5) 在“子网掩码”配置项处，输入 255.255.255.0。

(6) 其它配置项均保持默认配置即可，单击<确定>按钮保存配置。

图8 修改 LAN 配置



2. 配置 WAN1 接口连接 Internet

本例中 Router B 外网的接口模式选择单 WAN 模式，WAN 接口的连接模式为固定地址。配置步骤如下：

(1) 在设备 Web 管理界面导航栏中选择“网络设置 > 外网配置”，进入外网配置页面。

(2) 在“场景定义”页签下选择单 WAN 场景，线路 1 选择 WAN1，单击<应用>按钮使得配置生效。

(3) 单击“WAN 配置”页签，进入 WAN 配置页面。

(4) 单击 WAN1 对应的操作列编辑图标，进入修改 WAN 配置页面。

(5) 在“连接模式”配置项处，选择固定地址。

(6) 在“IP 地址”配置相处，输入 2.2.3.1。

(7) 在“子网掩码”配置项处，输入 255.255.255.0。

(8) 在“网关地址”配置项处，输入 2.2.3.254。

(9) 其它配置项均保持默认情况即可，单击<确定>按钮保存配置。

图9 修改 WAN 配置

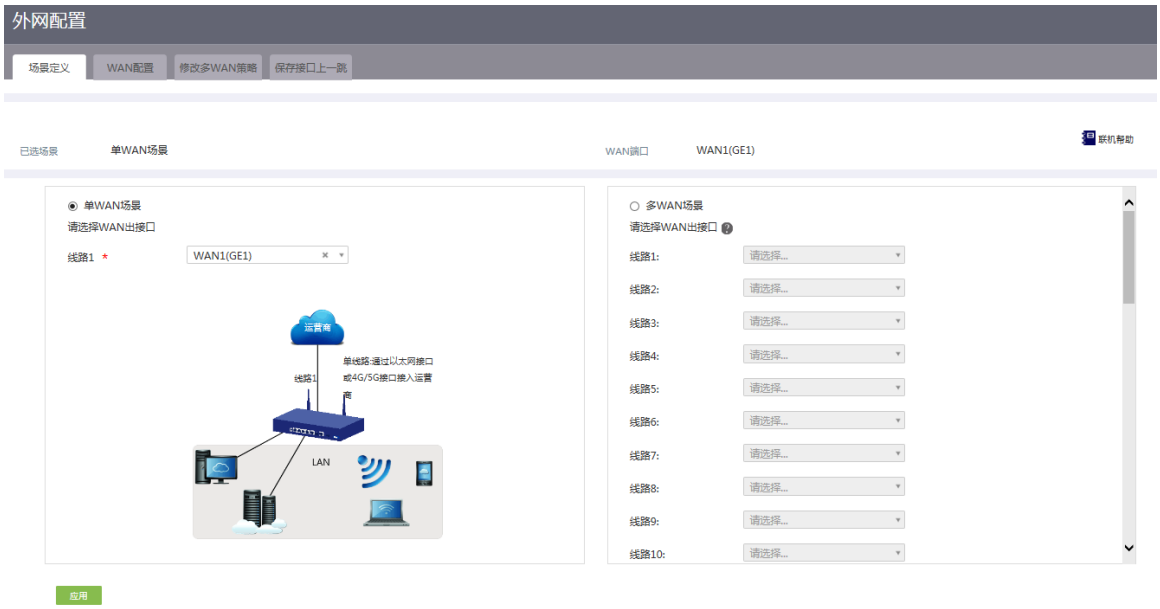
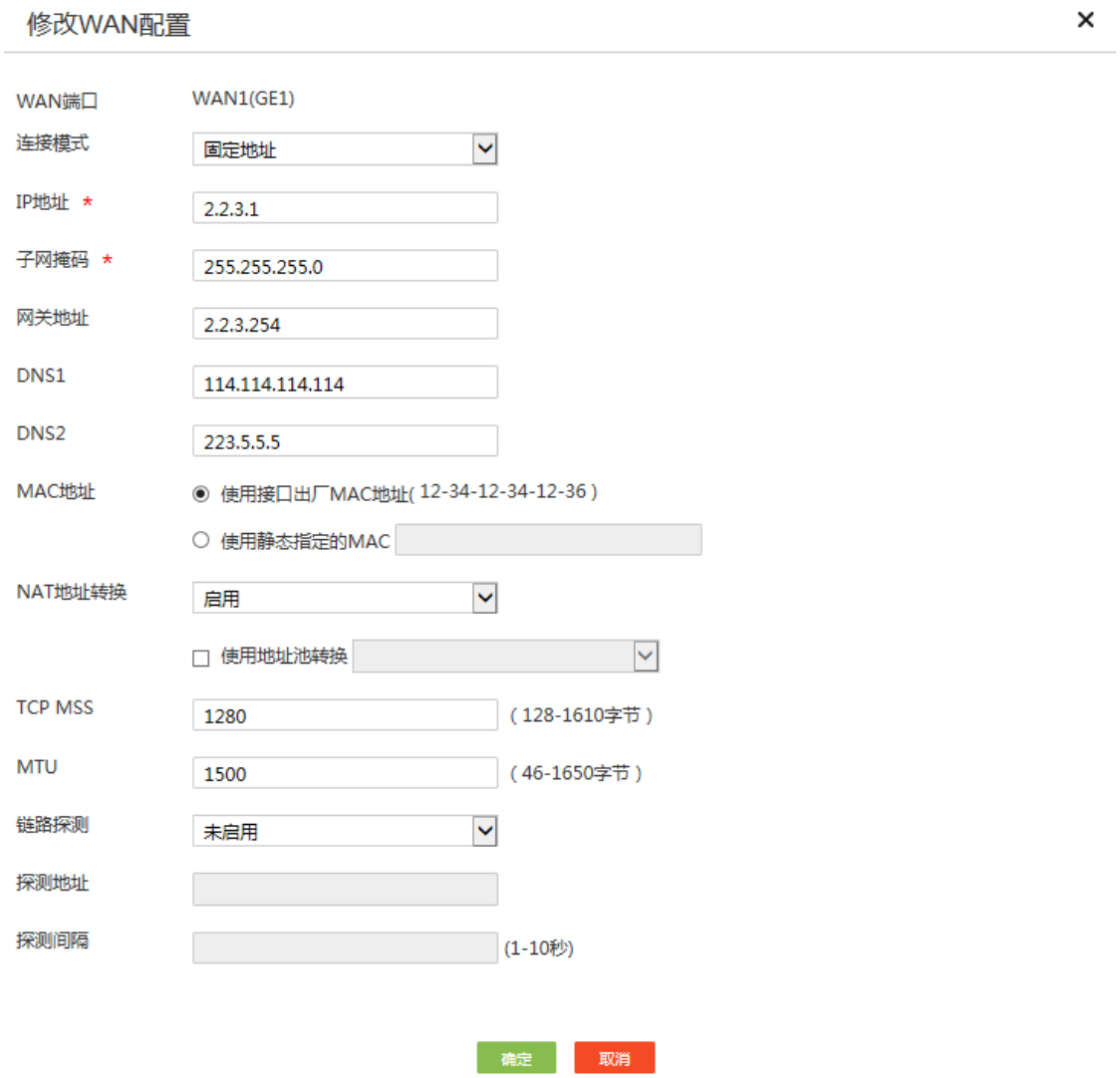

外网配置
场景定义
WAN配置
修改多WAN策略
保存接口上一跳
已选场景
单WAN场景
WAN端口
WAN1(GE1)
联机帮助
单WAN场景
请选择WAN出接口
线路1 *
WAN1(GE1)
运营商
线路1
单线路:通过以太网接口或4G/5G接口接入运营商
LAN
多WAN场景
请选择WAN出接口
线路1:
线路2:
线路3:
线路4:
线路5:
线路6:
线路7:
线路8:
线路9:
线路10:
请选择...
应用

图10 修改 WAN 配置



3. 配置 IPsec 策略

Router B 的 IPsec 策略中的组网方式选择分支节点，IKE 协商模式选择主模式。配置步骤如下：

(1) 在设备 Web 管理界面导航栏中选择“虚拟专网（VPN） > IPsec VPN”，进入 IPsec 策略配置页面。

(2) 单击<添加>按钮，进入添加 IPsec 策略页面，配置如下参数：

- 名称：输入 map1
- 接口：选择 WAN1
- 组网方式：选择分支节点
- 对端网关地址：输入 2.2.2.1
- 预共享密钥：输入 123456TESTplat&!
- 保护措施流：受保护协议选择 IP，本端受保护网段/掩码输入 10.1.2.0/24，对端受保护网段/掩码输入 10.1.1.0/24，单击<+>按钮，完成保护流的添加。

图11 配置 IPsec 策略

(3) 单击<显示高级配置>按钮，进入 IKE 配置页面，配置如下参数：

- 协商模式：选择主模式
- 本端身份类型：选择 IP 地址，输入 2.2.3.1
- 对端身份类型：选择 IP 地址，输入 2.2.2.1
- 对等体存活检测（DPD）：选择开启，超时时间设置为 30
- 算法组合：选择自定义
- 认证算法：选择 MD5
- 加密算法：选择 3DES-CBC
- 其它参数保持缺省配置即可。

图12 IKE 配置

(4) 单击“IPsec 配置”页签，进入 IPsec 配置页面，配置如下参数：

- 算法组合：选择自定义
- 安全协议：选择 ESP
- ESP 认证算法：选择 MD5
- ESP 加密算法：选择 3DES-CBC
- 封装模式：选择隧道模式
- 其它参数保持缺省配置即可

(5) 单击<返回基本设置>按钮，再单击<确定>按钮，完成配置。

图13 IPsec 配置

4.5 验证配置

(1) 用 Host A 主机 ping Host B 主机 IP 地址，可以 ping 通。

```
C:\Users\abc>ping 10.1.2.2
Ping 10.1.2.2 (10.1.2.2): 56 data bytes, press CTRL_C to break
56 bytes from 10.1.2.2: icmp_seq=0 ttl=254 time=2.137 ms
56 bytes from 10.1.2.2: icmp_seq=1 ttl=254 time=2.051 ms
56 bytes from 10.1.2.2: icmp_seq=2 ttl=254 time=1.996 ms
56 bytes from 10.1.2.2: icmp_seq=3 ttl=254 time=1.963 ms
56 bytes from 10.1.2.2: icmp_seq=4 ttl=254 time=1.991 ms

--- Ping statistics for 10.1.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.963/2.028/2.137/0.062 ms
C:\Users\abc>
```

(2) 完成上述配置后，在设备 Web 管理界面选择“虚拟专网(VPN) > IPsec VPN”，单击“监控信息”页签，进入监控信息页面，可以看到建立成功的 IPsec 隧道信息，状态列显示为 Active，说明配置验证成功。

5 野蛮模式配置举例

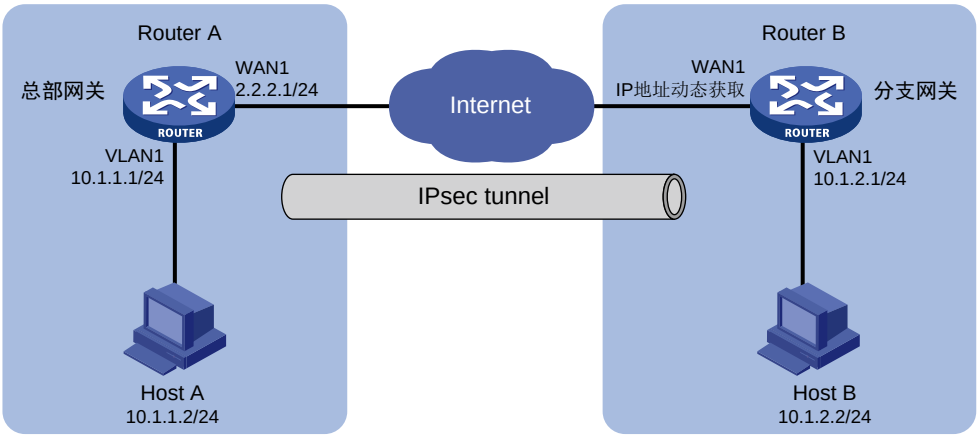
5.1 组网需求

如图 14 所示，Router A 为企业总部网关，外网接口模式为单 WAN 模式且以固定地址方式连接 Internet。Router B 为企业分支网关，外网接口模式为单 WAN 模式且以 DHCP 方式连接 Internet。分支与总部通过公网建立通信。

出于安全因素，需要对总部子网与分支组子网之间相互访问的流量进行安全保护，因此需要在 Router A 和 Router B 之间建立一条 IPsec 隧道，具体要求如下：

- 两端通过预共享秘钥（123456TESTplat&!）进行认证。
- IKE 协商采用的加密算法为 3DES-CBC，认证算法为 MD5。
- IPsec 隧道的封装模式为隧道模式，安全协议为 ESP。

图14 IPsec VPN（野蛮模式）典型配置组网图



5.2 配置思路

采用如下的配置思路：

(1) 完成 WAN 和 LAN 的基本配置

a. 配置 Router A 和 Router B 的 WAN 接口连接 Internet。

b. 修改 Router A 和 Router B 的 VLAN1 接口缺省 IP 地址。

(2) 添加 IPsec 策略

由于 Router B 的 WAN 接口采用 DHCP 方式获取地址，因此 IPsec 策略中的 IKE 协商模式选择野蛮模式。

5.3 配置注意事项

- 修改 VLAN1 接口的 IP 地址后，会导致 Web 管理界面登录异常，需要使用修改后的 IP 地址重新登录 Web 管理界面，才能进行接下来的配置。

- 若您的组网是双 WAN 或多 WAN 接入时，需要在 Router 上需配置一条静态路由，将访问对端内网的流量指向 IPsec 策略中所选用的 WAN 接口。本例中 Router A 和 Router B 均为单 WAN 接入，设备自动生成一条缺省路由，将所有流量指向出接口的网关，所以本例中该步骤可省略。
- IPsec 隧道两端设备的预共享秘钥、安全协议、加密/认证算法以及封装模式需保持一致。

5.4 配置步骤

5.4.1 配置 Router A

1. 修改 VLAN1 接口的 IP 地址

将 VLAN1 接口的 IP 地址修改为 10.1.1.1/24。配置步骤如下：

(1) 在设备 Web 管理界面导航栏中选择“网络设置 > LAN 配置”，进入 LAN 配置页面。

(2) 单击“LAN 配置”页签，进入 LAN 配置页面。

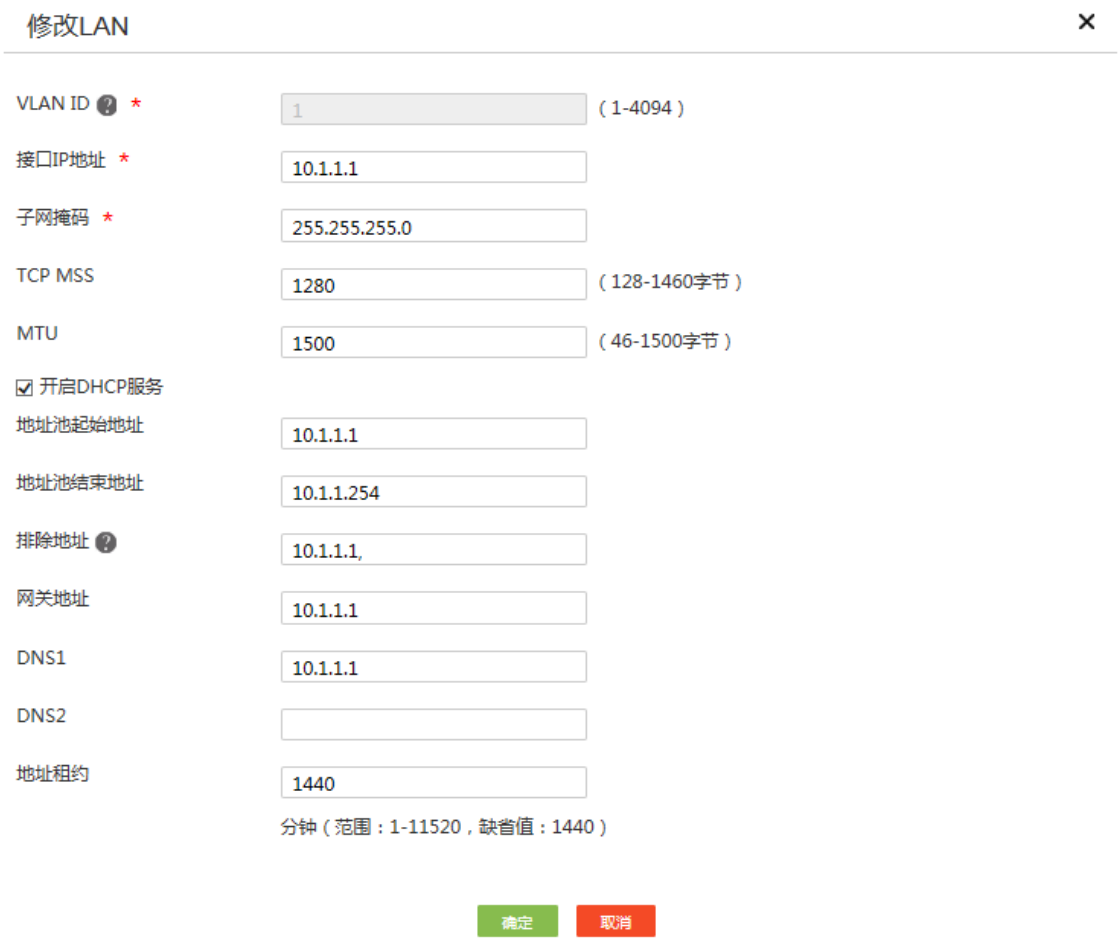
(3) 单击 VLAN1 对应的操作列编辑图标，进入修改 LAN 配置页面。

(4) 在“接口 IP 地址”配置项处，输入 10.1.1.1。

(5) 在“子网掩码”配置项处，输入 255.255.255.0。

(6) 其它配置项均保持默认情况即可，单击<确定>按钮保存配置。

图15 修改 VLAN 配置



2. 配置 WAN1 接口连接 Internet

本例中 Router A 外网的接口模式选择单 WAN 模式，WAN 接口的连接模式为固定地址。配置步骤如下：

(1) 在设备 Web 管理界面导航栏中选择“网络设置 > 外网配置”，进入外网配置页面。

(2) 在“场景定义”页签下选择单 WAN 场景，线路 1 选择 WAN1，单击<应用>按钮使得配置生效。

(3) 单击“WAN 配置”页签，进入 WAN 配置页面。

(4) 单击 WAN1 对应的操作列编辑图标，进入修改 WAN 配置页面。

(5) 在“连接模式”配置项处，选择固定地址。

(6) 在“IP 地址”配置相处，输入 2.2.2.1。

(7) 在“子网掩码”配置项处，输入 255.255.255.0。

(8) 在“网关地址”配置项处，输入 2.2.2.254。

(9) 其它配置项均保持默认情况即可，单击<确定>按钮保存配置。

图16 配置 WAN 场景

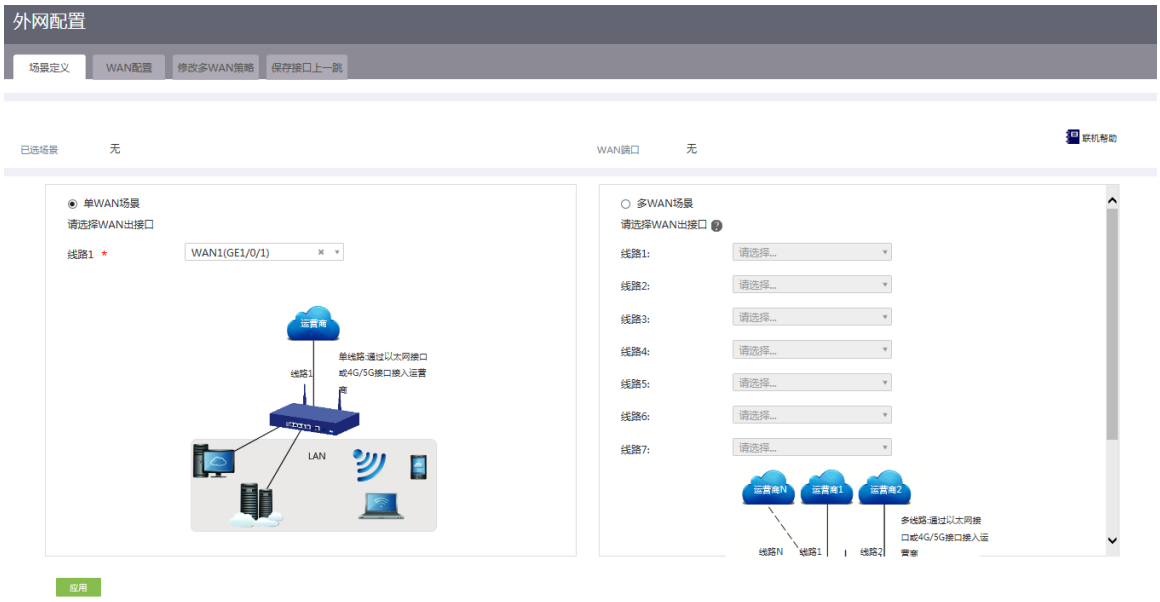
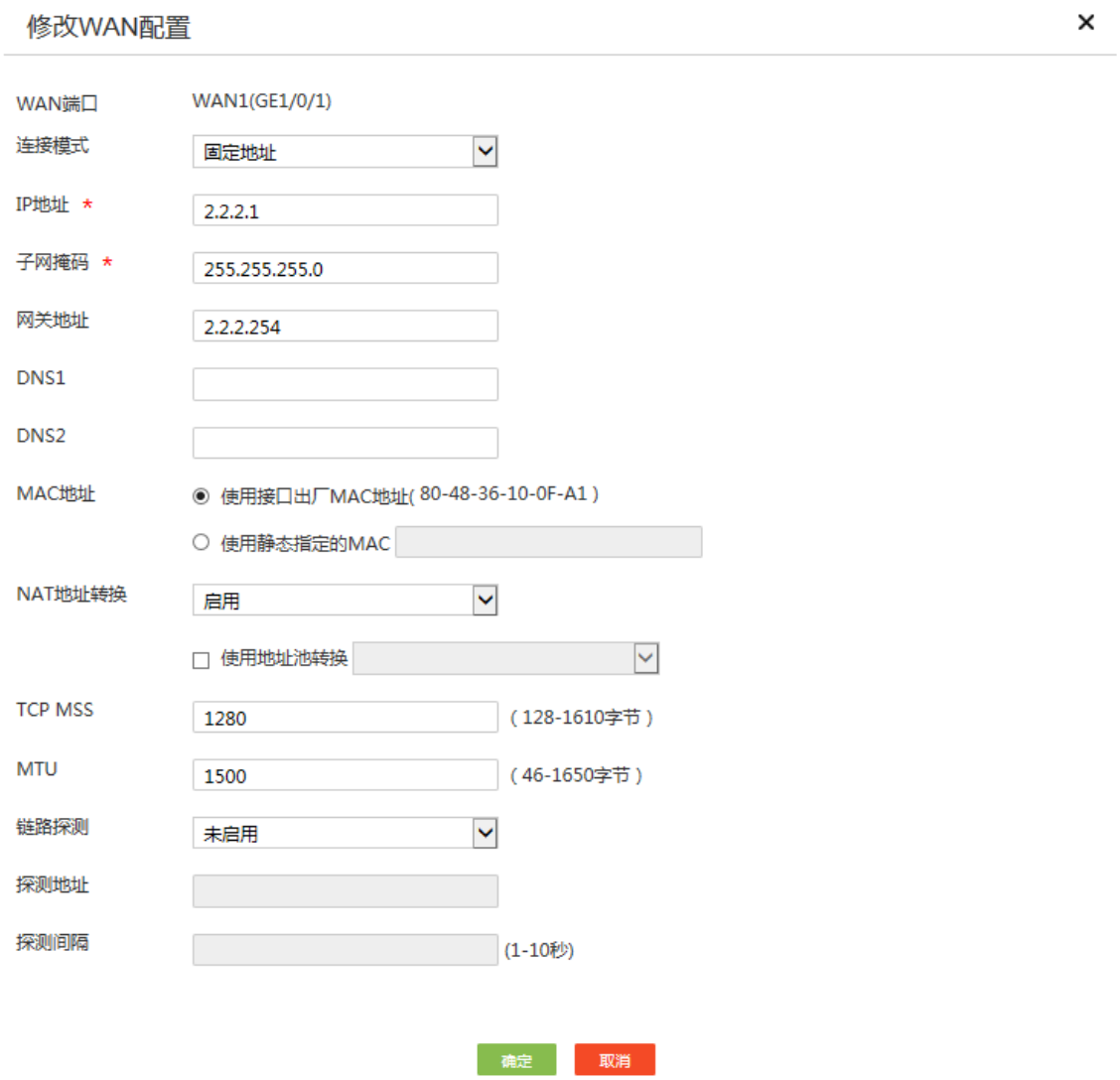

外网配置
场景定义
WAN配置
修改多WAN策略
保存接口上一跳
已选场景
无
WAN端口
无
联机帮助
单WAN场景
请选择WAN出接口
线路1 *
WAN1(GE1/0/1)
运营商
单线路:通过以太网接口或4G/5G接口接入运营商
线路1
LAN
多WAN场景
请选择WAN出接口
线路1:
线路2:
线路3:
线路4:
线路5:
线路6:
线路7:
请选择...
运营商N
运营商1
运营商2
多线路:通过以太网接口或4G/5G接口接入运营商
线路N
线路1
线路2
应用

图17 修改 WAN 配置



3. 配置 IPsec 策略

IPsec 策略中的组网方式选择中心节点，IKE 协商模式选择野蛮模式。配置步骤如下：

(1) 在设备 Web 管理界面导航栏中选择“虚拟专网（VPN） > IPsec VPN”，进入 IPsec 策略配置页面。

(2) 单击<添加>按钮，进入添加 IPsec 策略页面，配置如下参数：

- 名称：输入 map1
- 接口：选择 WAN1
- 组网方式：选择中心节点
- 预共享密钥：输入 123456TESTplat&!

图18 配置 IPsec 策略

(3) 单击<显示高级配置>按钮，进入 IKE 配置页面，配置如下参数：

- 协商模式：选择野蛮模式
- 本端身份类型：选择 FQDN，输入 www.test.com（自定义即可）
- 对等体存活检测（DPD）：选择开启，超时时间设置为 30（该功能缺省是关闭状态，建议您开启此功能，使设备能够及时获悉 IPsec 隧道的可用情况。）
- 算法组合：选择自定义
- 认证算法：选择 MD5
- 加密算法：选择 3DES-CBC
- 其它参数保持缺省配置即可。

图19 IKE 配置

(4) 单击“IPsec 配置”页签，进入 IPsec 配置页面，配置如下参数：

- 算法组合：选择自定义
- 安全协议：选择 ESP
- ESP 认证算法：选择 MD5
- ESP 加密算法：选择 3DES-CBC
- 封装模式：选择隧道模式
- 其它参数保持缺省配置即可

(5) 单击<返回基本设置>按钮，再单击<确定>按钮，完成配置。

图20 IPsec 配置

5.4.2 配置 Router B

1. 修改 VLAN1 接口的 IP 地址

将 VLAN1 接口的 IP 地址修改为 10.1.2.1/24。配置步骤如下：

(1) 在设备 Web 管理界面导航栏中选择“网络设置 > LAN 配置”，进入 LAN 配置页面。

(2) 单击“LAN 配置”页签，进入 LAN 配置页面。

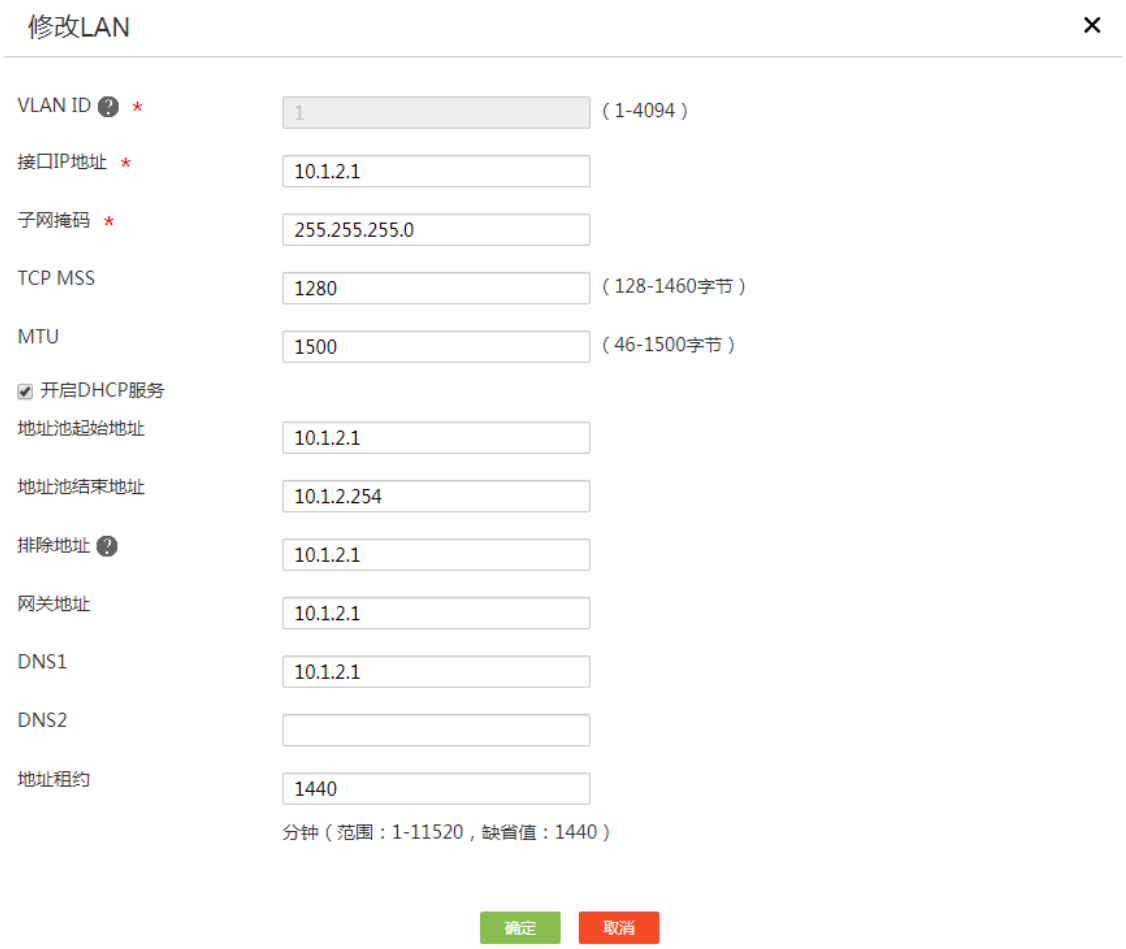
(3) 单击 VLAN1 对应的操作列编辑图标，进入修改 LAN 配置页面。

(4) 在“接口 IP 地址”配置项处，输入 10.1.2.1。

(5) 在“子网掩码”配置项处，输入 255.255.255.0。

(6) 其它配置项均保持默认配置即可，单击<确定>按钮保存配置。

图21 修改 VLAN 配置



2. 配置 WAN1 接口连接 Internet

本例中 Router B 外网的接口模式选择单 WAN 模式，WAN 接口的连接模式为 DHCP。配置步骤如下：

(1) 在设备 Web 管理界面导航栏中选择“网络设置 > 外网配置”，进入外网配置页面。

(2) 在“场景定义”页签下选择单 WAN 场景，线路 1 选择 WAN1，单击<应用>按钮使得配置生效。

(3) 单击“WAN 配置”页签，进入 WAN 配置页面。

(4) 单击 WAN1 对应的操作列编辑图标，进入修改 WAN 配置页面。

(5) 在“连接模式”配置项处，选择 DHCP。

(6) 其它配置项均保持默认情况即可，单击<确定>按钮保存配置。

图22 配置 WAN 场景

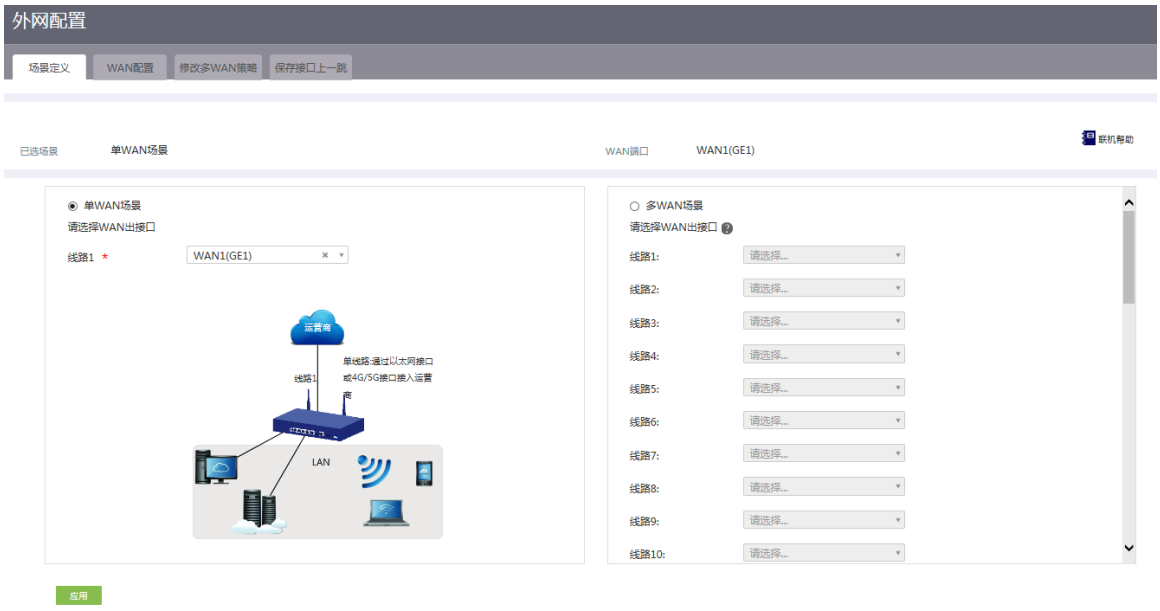


图23 修改 WAN 配置

3. 配置 IPsec 策略

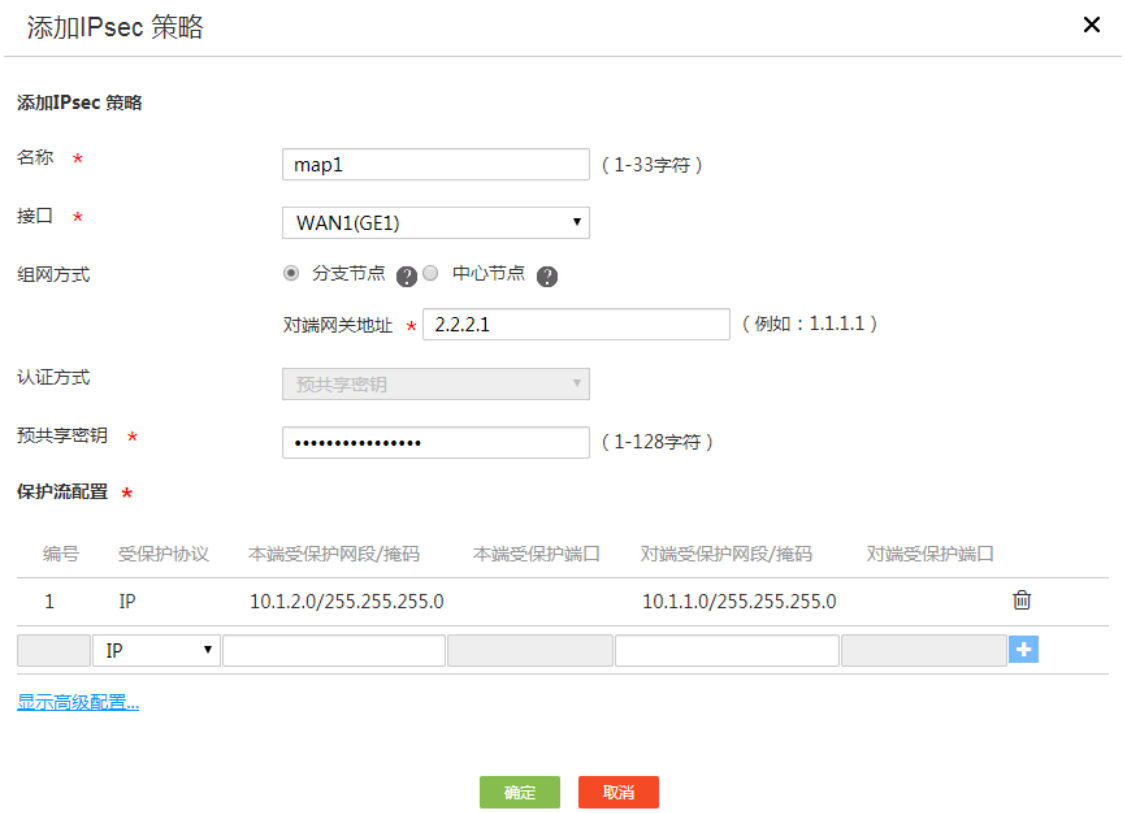
IPsec 策略中的组网方式选择分支节点，IKE 协商模式选择野蛮模式。配置步骤如下：

(1) 在设备 Web 管理界面导航栏中选择“虚拟专网（VPN） > IPsec VPN”，进入 IPsec 策略配置页面。

(2) 单击<添加>按钮，进入添加 IPsec 策略页面，配置如下参数

- 名称：输入 map1
- 接口：选择 WAN1
- 组网方式：选择分支节点
- 对端网关地址：输入 2.2.2.1
- 预共享密钥：输入 123456TESTplat&!
- 保护措施流：受保护协议选择 IP，本端受保护网段/掩码输入 10.1.2.0/24，对端受保护网段/掩码输入 10.1.1.0/24，单击<+>按钮，完成保护流的添加。

图24 配置 IPsec 策略



(3) 单击<显示高级配置>按钮，进入 IKE 配置页面，配置如下参数：

- 协商模式：选择野蛮模式
- 本端身份类型：选择 FQDN，输入 www.test1.com（自定义）
- 对端身份类型：选择 FQDN，输入 www.test.com
- 对等体存活检测（DPD）：选择开启，超时时间设置为 30

- 算法组合：选择自定义
- 认证算法：选择 MD5
- 加密算法：选择 3DES-CBC
- 其它参数保持缺省配置即可

图25 IKE 配置

(4) 单击“IPsec 配置”页签，进入 IPsec 配置页面，配置如下参数：

- 算法组合：选择自定义
- 安全协议：选择 ESP
- ESP 认证算法：选择 MD5
- ESP 加密算法：选择 3DES-CBC
- 封装模式：选择隧道模式
- 其它参数保持缺省配置即可

(5) 单击<返回基本设置>按钮，再单击<确定>按钮，完成配置。

图26 IPsec 配置

5.5 验证配置

(1) 用 Host A 主机 ping Host B 主机 IP 地址，可以 ping 通。

```
C:\Users\abc>ping 10.1.2.2
Ping 10.1.2.2 (10.1.2.2): 56 data bytes, press CTRL_C to break
56 bytes from 10.1.2.2: icmp_seq=0 ttl=254 time=2.137 ms
56 bytes from 10.1.2.2: icmp_seq=1 ttl=254 time=2.051 ms
56 bytes from 10.1.2.2: icmp_seq=2 ttl=254 time=1.996 ms
56 bytes from 10.1.2.2: icmp_seq=3 ttl=254 time=1.963 ms
56 bytes from 10.1.2.2: icmp_seq=4 ttl=254 time=1.991 ms

--- Ping statistics for 10.1.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.963/2.028/2.137/0.062 ms
C:\Users\abc>
```

(2) 完成上述配置后，在设备 Web 管理界面选择“虚拟专网(VPN) > IPsec VPN”，单击“监控信息”页签，进入监控信息页面，可以看到建立成功的 IPsec 隧道信息，状态列显示为 UP，说明配置验证成功。

目 录

1 简介

本文档介绍路由器 L2TP VPN 的配置方法。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 L2TP VPN 特性。

3 使用版本

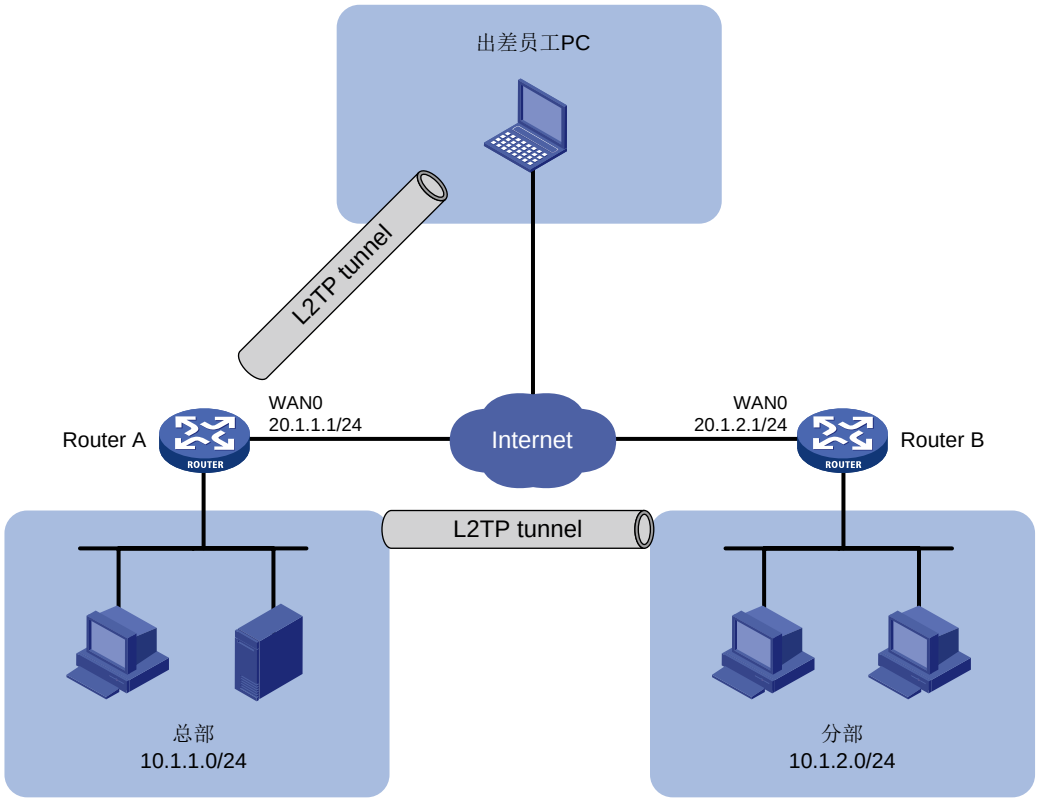
本配置举例是在 MSR3610-X1 路由器 Release 6728P22 版本上进行配置和验证的。

4 配置举例

4.1 组网需求

如图 1 所示，某企业要求通过创建 L2TP 隧道来实现出差员工和分部公司员工可以访问搭建在总部内网的服务器。

图1 L2TP VPN 典型配置组网图



4.2 配置思路

(1) 配置总部路由器 Router A 连接 Internet，启用 L2TP 服务器端。

(2) 配置分部路由器 Router B 连接 Internet，启用 L2TP 客户端。

(3) 在出差员工 PC 上设置 L2TP 客户端。

4.3 配置步骤

4.3.1 配置 Router A

1. 配置 WAN0 接口连接 Internet

说明

本例中 Router A 外网的接口模式为单 WAN 模式，WAN 接口的连接模式为固定地址。

选择“网络设置 > 外网配置”，进入外网配置页面：

(1) 在“配置接口模式”页面中勾选“单 WAN 模式”，单击“应用”按钮完成配置；

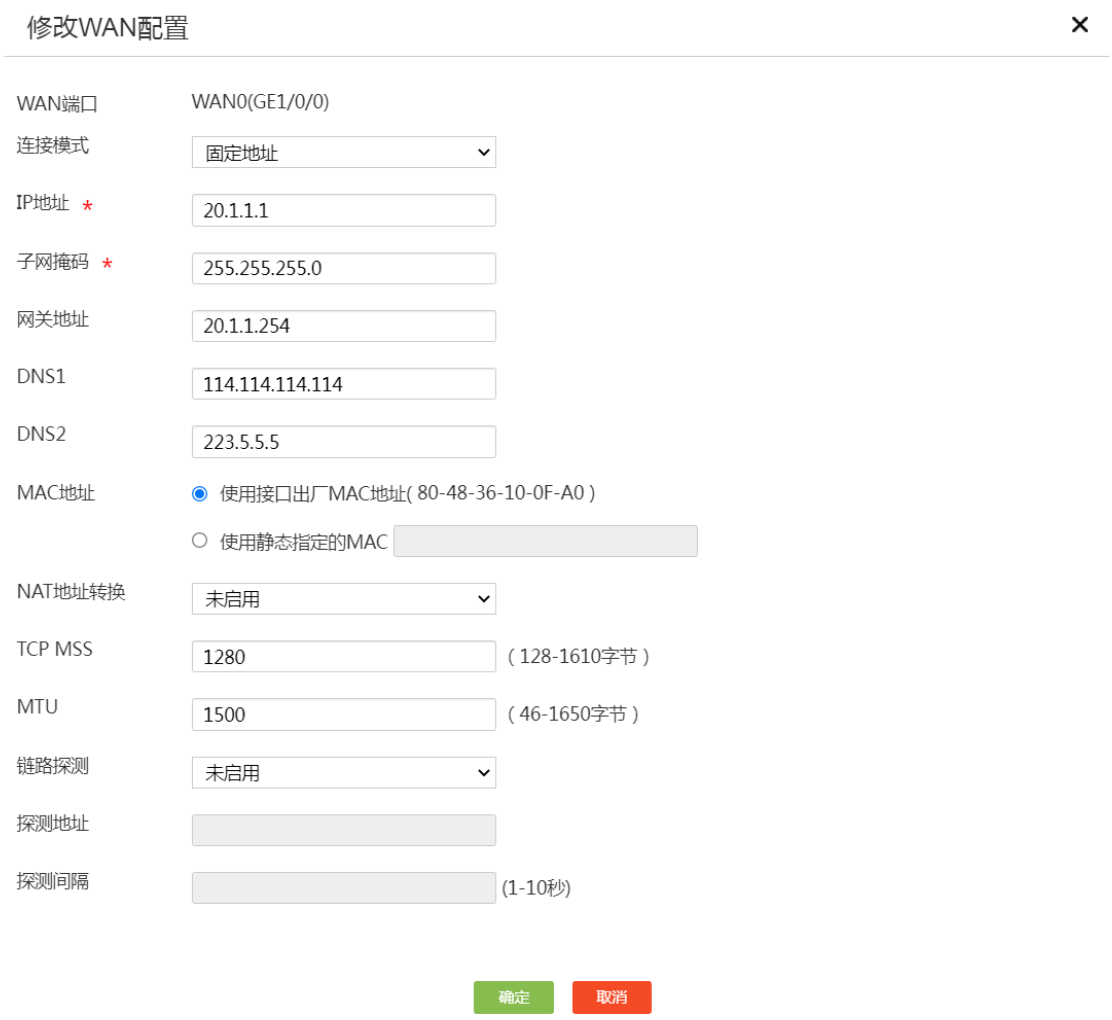
(2) 单击“WAN 配置”页签，进入 WAN 配置页面；

(3) 单击 WAN0 接口对应操作列编辑图标，进入修改 WAN 配置页面，配置如下参数：

- 连接模式：固定地址
- IP 地址：20.1.1.1
- 子网掩码：255.255.255.0
- 网关地址：20.1.1.254
- DNS1：114.114.114.114
- DNS2：223.5.5.5
- 其它参数保持默认配置

(4) 单击“确定”按钮保存配置。

图2 配置 WAN0 接口连接 Internet



2. 启用并配置 L2TP 服务器

说明

本例需要创建两个 L2TP 组（隧道）分别供出差员工 PC 和分部路由器连接，名称分别为 LNS1 和 LNS2。

#选择“虚拟专网（VPN）>L2TP 服务器端”，进入 L2TP 配置页面，勾选 L2TP 服务器端的“开启”选项，完成 L2TP 服务器的启用。

(1) 配置 LNS1（供出差员工 PC 连接）

#在 L2TP 配置页面，单击“添加”按钮，进入“新建 L2TP 组”配置页面，完成如下参数配置：

- 对端隧道名称：不勾选复选框，无需配置（若勾选，需填写出差员工计算机名称）
- 本端隧道名称：LNS1
- 隧道验证：选择“禁用”（使用 PC 作为 L2TP 客户端，不建议启用隧道验证功能）
- PPP 认证方式：选择“CHAP”
- 虚拟模板接口地址：172.16.10.1（根据实际情况输入，不要和内网 IP 地址相同）
- 子网掩码：255.255.255.0（根据实际情况输入）
- 用户地址池：172.16.10.2-172.16.10.5（根据实际情况输入）
- 其它参数保持默认配置
- 单击“确定”按钮，完成 LNS1 的添加

图3 配置 LNS1

(2) 配置 LNS2（供分部路由器连接）

#在 L2TP 配置页面，单击“添加”按钮，进入“新建 L2TP 组”配置页面，完成如下参数配置：

- 对端隧道名称：LAC（根据情况自定义）
- 本端隧道名称：LNS2
- 隧道验证：选择“启用”，并输入隧道验证密码“abc123”
- PPP 认证方式：选择“CHAP”
- 虚拟模板接口地址：172.16.20.1（根据实际情况输入，不要和内网 IP 地址在同一网段）
- 子网掩码：255.255.255.0（根据实际情况输入）
- 用户地址池：172.16.20.2-172.16.20.5（根据情况输入）
- 其它参数保持默认配置
- 单击“确认”按钮，完成 LNS2 的添加

图4 配置 LNS2


新建L2TP组
L2TP配置
对端隧道名称
LAC
(1-31字符)
本端隧道名称
LNS2
(1-31字符)
隧道验证
启用
禁用
隧道验证密码
(1-16字符)
PPP认证配置
PPP认证方式
CHAP
PPP地址配置
虚拟模板接口地址 *
172.16.20.1
子网掩码 *
255.255.255.0
用户地址池 *
172.16.20.2-172.16.20.5
可以是单个地址，
也可以是一个地址范围
如:192.168.1.100-192.168.1.200
LNS用户管理
* 需要添加指定接入的PPP用户，完成本页设置后请到"认证管理 - 用户管理"页面添加
隐藏高级设置...
高级配置
Hello报文间隔
60
秒(60-1000,缺省值为60)
AVP数据隐藏
流量控制
强制本端CHAP认证
强制LCP重协商
确定
取消

图5 L2TP 组配置

3. 添加 L2TP 用户

说明

L2TP 用户设置主要是为 L2TP 客户端拨号时提供账号名和密码。

(1) 为分部路由器做客户端添加账号名和密码

#选择“认证管理>用户管理”，单击“用户设置”页签，进入用户设置页面，单击“添加”按钮，进入添加用户页面，配置下面参数：

- 账号名：vpdn1（根据实际情况自定义即可）
- 状态：选择“可用”
- 密码：user123（根据实际情况自定义即可）
- 可用服务：选择“PPP”
- MAC 地址：选择“不绑定”
- 最大用户数：1（根据实际需要设置该账号同时可支持多少 L2TP 客户端连接）
- 有效日期：不配置（若选择“配置”，则需要在日期选择框中选则账号权限到期日期）
- 单击“确定”按钮，完成配置

图6 添加 L2TP 用户

(2) 为出差员工 PC 添加账号名和密码

按照同样的步骤为出差员工添加账号名为 vpdnuser，密码为：user1234。

4.3.2 配置 Router B

1. 配置 WAN0 接口连接 Internet

说明

本例中 Router B 外网的接口模式为单 WAN 模式，WAN 接口的连接模式为固定地址。

选择“网络设置 > 外网配置”，进入外网配置页面：

(1) 在“配置接口模式”页面中勾选“单 WAN 模式”，单击“应用”按钮完成配置；

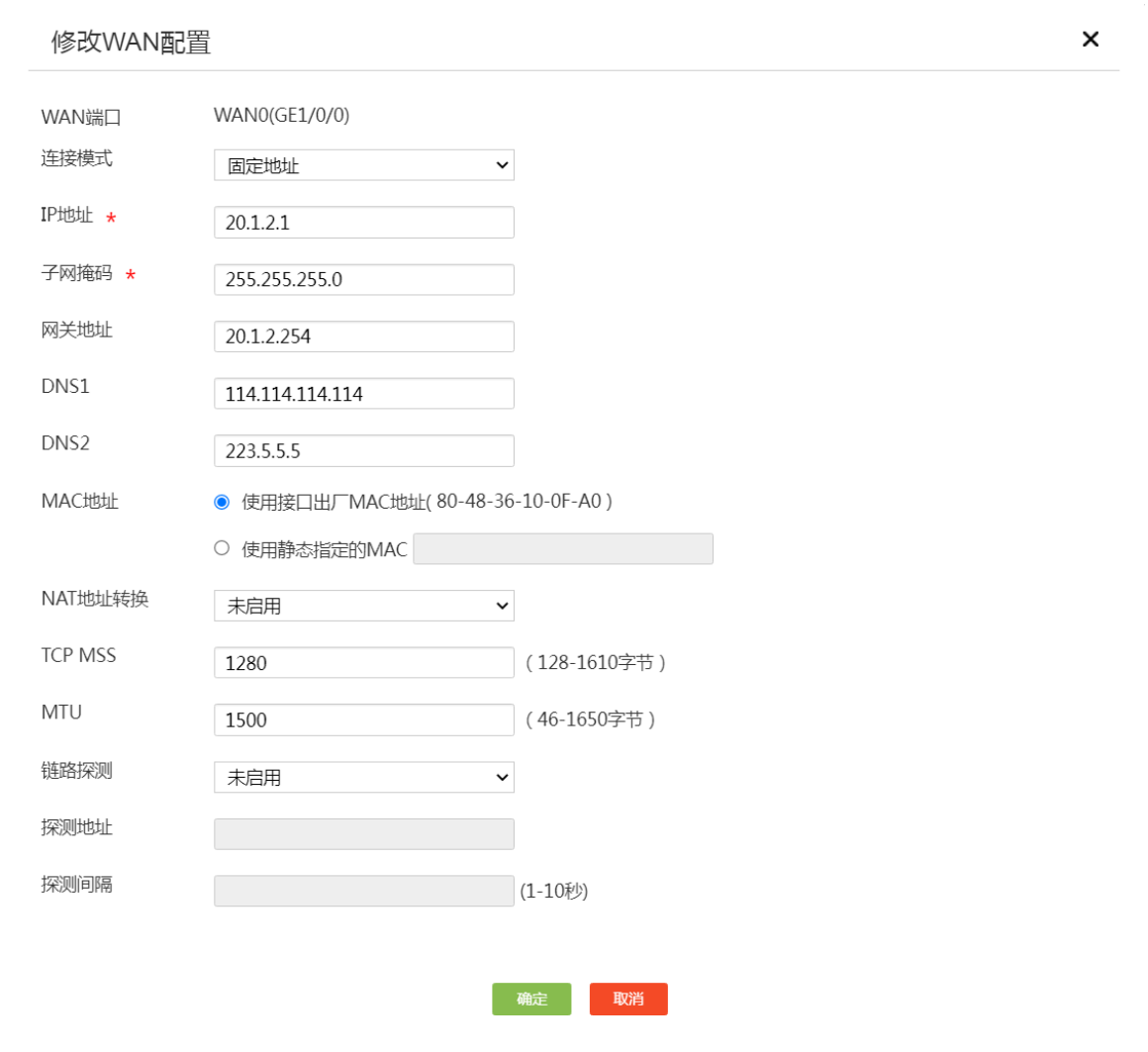
(2) 单击“WAN 配置”页签，进入 WAN 配置页面，单击 WAN0 接口对应操作列编辑图标，进入修改 WAN 配置页面，配置如下参数：

- 连接模式：固定地址
- IP 地址：20.1.2.1
- 子网掩码：255.255.255.0

- 网关地址：20.1.2.254
- DNS1：114.114.114.114
- DNS2：223.5.5.5
- 其它参数保持默认配置即可

(3) 单击“确定”按钮保存配置。

图7 配置 WAN0 接口连接 Internet



2. 启用并配置 L2TP 客户端

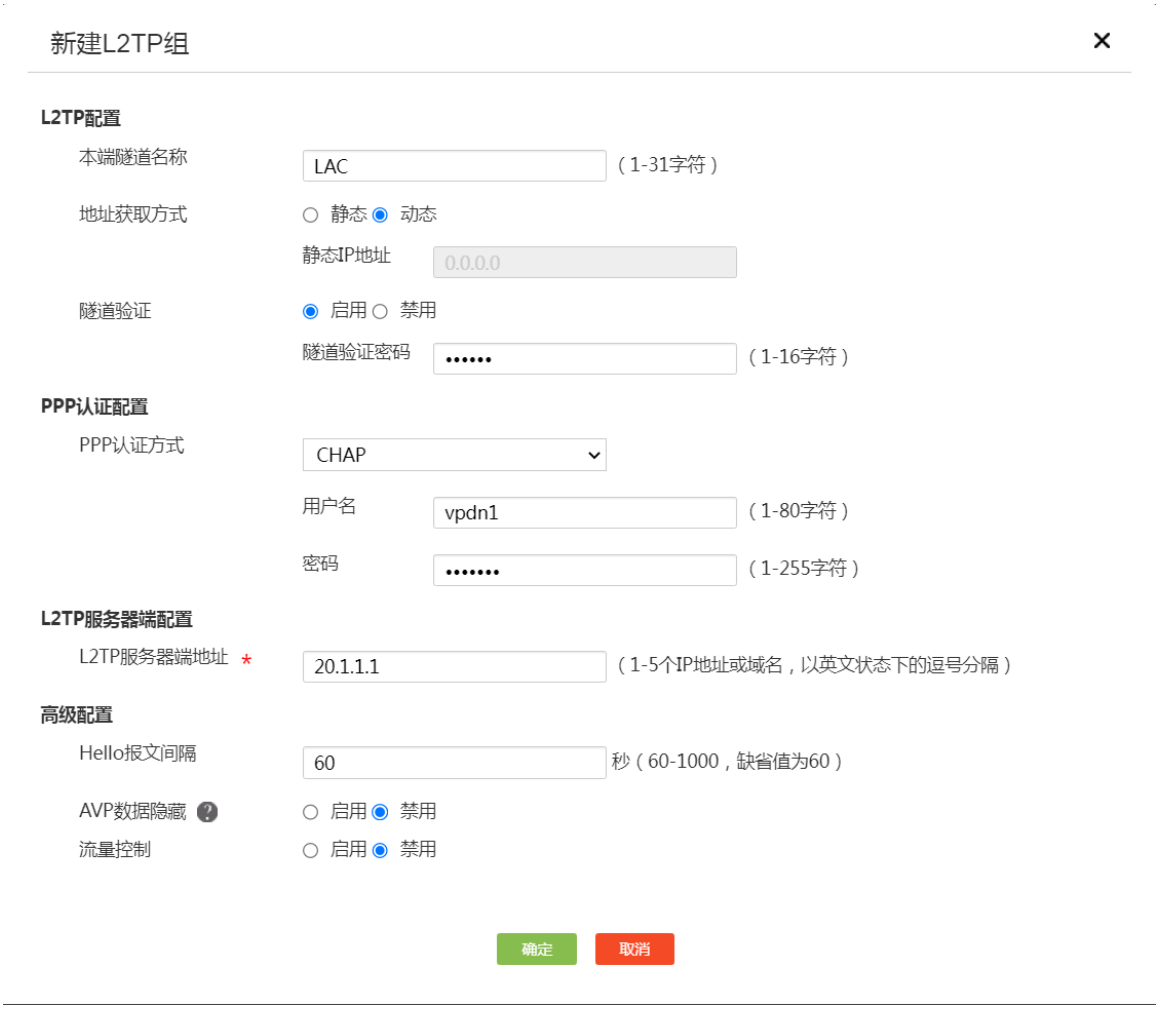
说明

配置 L2TP 客户端时相关信息需要和 L2TP 服务器端保持一致。

#选择“虚拟专网（VPN）>L2TP 客户端”，单击“L2TP 客户端”页签，进入 L2TP 客户端配置页面，选择 L2TP 客户端“开启”选项，完成 L2TP 客户端的启用。单击“添加”按钮，进入“新建 L2TP 组”页面，配置下面参数：

- 本端隧道名称：LAC
- 地址获取方式：选择“动态”
- 隧道验证：选择“启用”，并输入 LNS2 中设置的密码 abc123
- PPP 认证方式：选择“CHAP”，用户名配置项处输入 vpdn1，密码配置项处输入 user123
- L2TP 服务器端地址：20.1.1.1（总部 WAN0 接口 IP 地址）
- 其它参数保持默认配置即可
- 单击“确定”按钮，完成配置

图8 配置 L2TP 客户端



3. 配置静态路由

说明

当使用路由器做 L2TP 客户端时，需要添加到 L2TP 服务器端子网（10.1.1.0/24）的静态路由。

#选择“高级选项>静态路由”，进入静态路由配置页面，单击“添加”按钮，进入“添加 IPv4 静态路由”页面，配置下面参数：

- 目的 IP 地址：10.1.1.0
- 子网掩码：24
- 下一跳：GE1/0/0（对应的 L2TP 隧道接口）
- 其它选项保持默认即可，单击“确定”按钮，完成配置

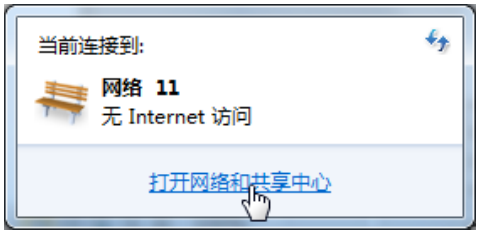
图9 配置静态路由

4.3.3 配置出差员工 PC

说明

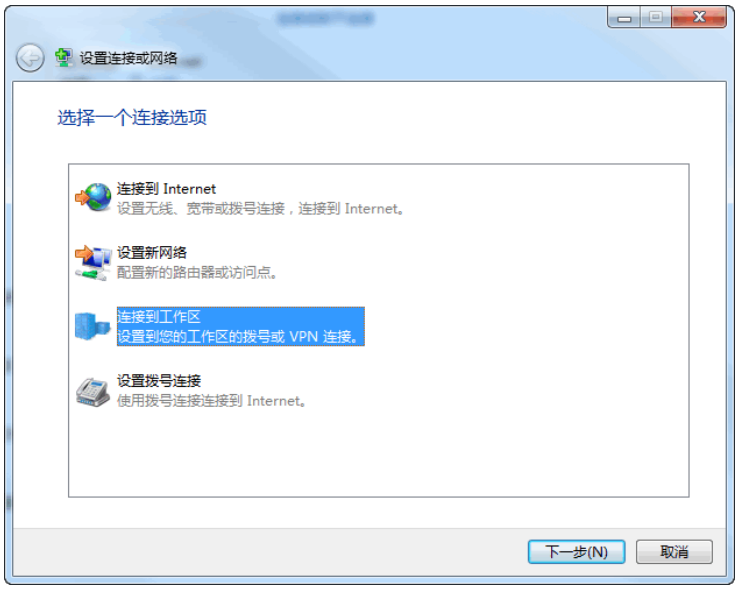
在出差员工 PC 上配置 L2TP 客户端，本例以装有 Window 7 系统的 PC 为例。

#登录出差员工 PC 桌面，单击桌面右下角（即任务栏中）的网络图标，选择“打开网络和共享中心”。

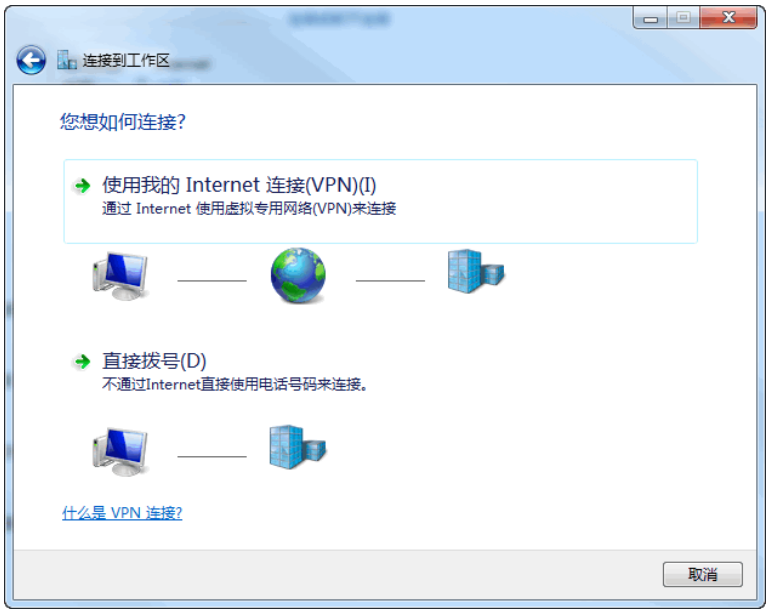


单击“设置新的连接或网络”选项，创建一个 L2TP 客户端。

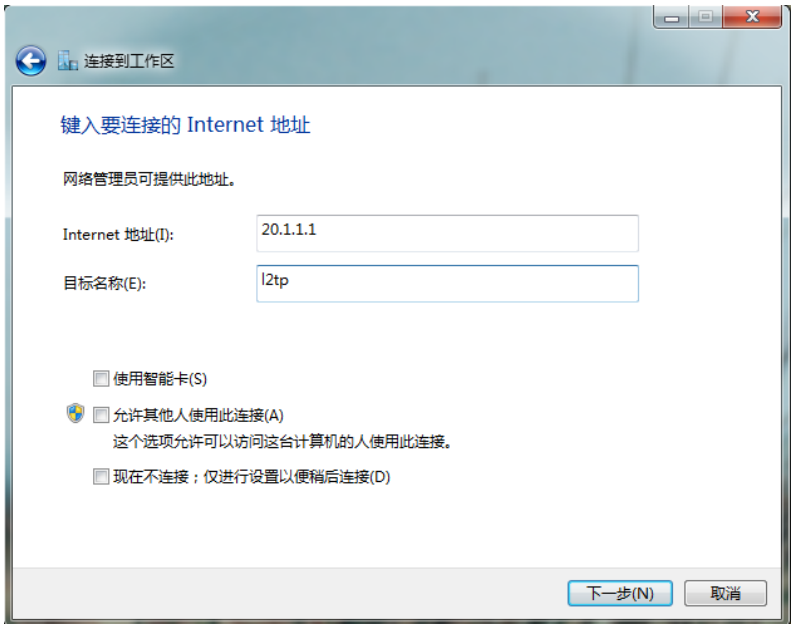
在弹出的设置连接或网络对话框中，选择“连接到工作区”选项，单击“下一步”按钮。



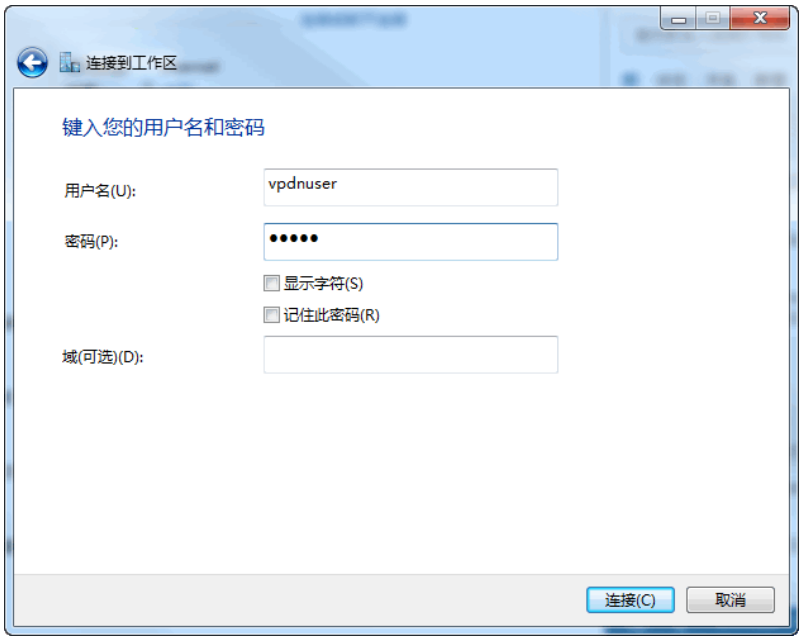
选择“使用我的 Internet 连接(VPN)(I)”选项，开始配置连接的 Internet 地址。



在 Internet 连接(T)配置项中，输入要连接到的 L2TP 服务器段 WAN0 接口的 IP 地址，本例为 20.1.1.1；在目的名称配置项中，输入该 L2TP 客户端的连接的名称，本例为 l2tp，单击“下一步”按钮。

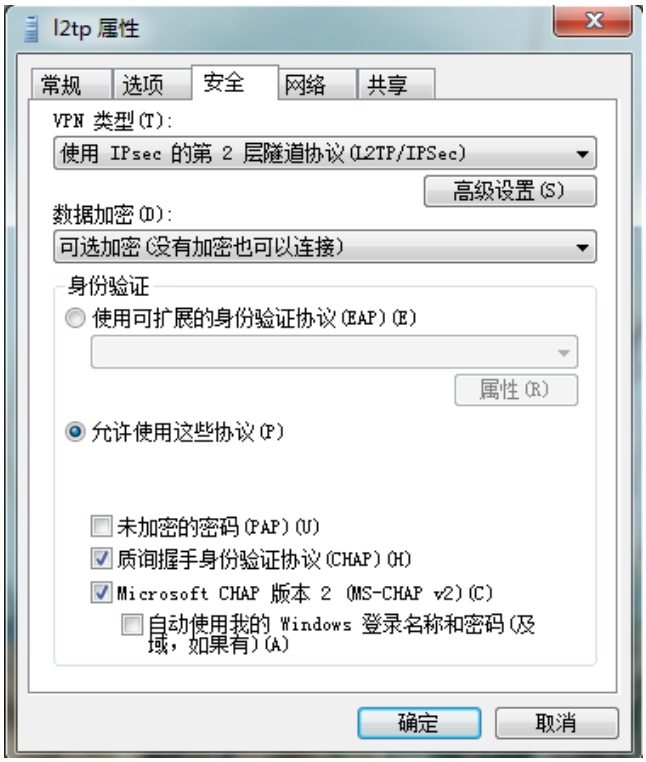


在用户名和密码配置项中，分别输入 L2TP 服务器端设置的用户名和密码，本例用户名为 vpdnuser，密码为 user1234，单击“连接”按钮进行连接。



单击桌面右下角的网络图标，右键单击 L2TP 客户端名称（如“l2tp”），选择“属性”选项。

在弹出属性对话框中，选择“安全”页签，在“VPN 类型(T)”中选择“使用 IPsec 的第 2 层隧道协议(L2TP/IPSec)”，在“数据加密(D)”中选择“可选加密（没有加密也可以连接）”，单击“确定”按钮使得配置生效。



打开 L2TP 协议的拨号终端窗口，在弹出连接对话框中输入用户名：vpdnuser，密码：uesr1234，单击“连接”按钮进行连接。

4.3.4 验证配置

出差员工 PC 和分部员工 PC 都可以访问总部服务器，配置验证成功。登录总部路由器 RouterA Web 管理界面，选择“虚拟专网（VPN）>L2TP 服务器端”，单击“隧道信息”页签，可以查看对应的 L2TP 隧道信息。

目 录

1 简介

本文档介绍无线 AC 的配置方法。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解无线 AC 特性。

3 使用版本

本配置举例是在 MSR3610-X1 路由器 Release 6728P22 版本上进行配置和验证的。

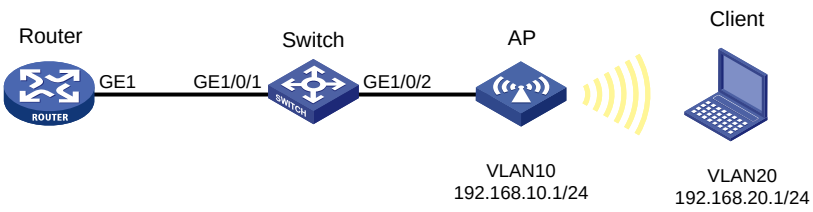
4 配置举例

4.1 组网需求

如图 1 所示，AP 通过二层交换机连接到 Router（AC），现要求：

- Client 能通过 AP 下发的 2.4G 和 5G 无线网络接入 Router，且能自动获取 VLAN20 网段的 IP 地址。
- AP 能自动获取 VLAN10 网段的 IP 地址。
- 二层交换机通过 PoE 方式给 AP 供电。

图1 WLAN AC 典型配置组网图



4.2 配置思路

- 需要在 Router 上配置 2.4G 和 5G 无线服务模板，本例中，为给 Client 提供更好的无线体验，结合 AP 周围的环境，具体参数设置如下：

无线服务模板	SSID	工作模式	工作信道	最大传输速率
2.4G	service1	802.11g	6	19dm
5G	service2	802.11ac	157	19dm

- 需要在 Router 上划分 VLAN10 和 VLAN20，其中 VLAN10 用于 Router 与 AP 之间的报文交互，VLAN20 和 2.4G、5G 无线服务模板绑定。
- 需要在 Router 上开启 DHCP Server 功能，使得 AP 和 Client 都能通过 DHCP Server 自动获取 IP 地址。

4.3 配置注意事项

- 无线的工作模式、工作信道和最大传输速率可以根据无线实际的使用情况进行调整。
- Router 与交换机之间互联的接口，以及交换机上连接 AP 的接口，需要设置为 Trunk，允许 AP 的管理 VLAN 和业务 VLAN 通过，且缺省的 VLAN 为 AP 的管理 VLAN。
- 您可以选择创建手工 AP 或配置自动 AP 使得 AP 上线。本例选择创建手工 AP，AP 的序列号可以通过 AP 设备背面的标签获取。

4.4 配置步骤

4.4.1 配置 Router（AC）

1. 划分 VLAN10

划分 VLAN10，并配置接口的 IP 地址，开启接口的 DHCP 服务。

(1) 在设备 Web 管理界面导航栏中选择“网络设置 > LAN 配置”，进入 LAN 配置页面。

(2) 单击<添加>按钮，进入添加 LAN 配置页面。

(3) 在“LAN 接口类型”配置项处，选择 VLAN 接口。

(4) 在“VLAN ID”配置项处，输入 10。

(5) 在“接口 IP 地址”配置项处，输入 192.168.10.1。

(6) 在“子网掩码”配置项处，输入 255.255.255.0。

(7) 勾选“开启 DHCP 服务”前方的单选框，开启接口的 DHCP 服务。

(8) 其它配置项保持缺省配置，单击<确定>按钮保存配置。

图2 划分 VLAN10

2. 划分 VLAN20

划分 VLAN20，并配置接口的 IP 地址，开启接口的 DHCP 服务。

(1) 在设备 Web 管理界面导航栏中选择“网络设置 > LAN 配置”，进入 LAN 配置页面。

(2) 单击<添加>按钮，进入添加 LAN 配置页面。

(3) 在“LAN 接口类型”配置项处，选择 VLAN 接口。

(4) 在“VLAN ID”配置项处，输入 20。

(5) 在“接口 IP 地址”配置项处，输入 192.168.20.1。

(6) 在“子网掩码”配置项处，输入 255.255.255.0。

(7) 勾选“开启 DHCP 服务”前方的单选框，开启接口的 DHCP 服务。

(8) 其它配置项保持缺省配置，单击<确定>按钮保存配置。

图3 划分 VLAN20

3. 配置 GE1 接口

配置 GE1 接口同时通过 VLAN10 和 VLAN20，并设置接口的 PVID（缺省 VLAN）为 10。

(1) 在设备 Web 管理界面导航栏中选择“网络设置 > LAN 配置”，进入 LAN 配置页面。

(2) 单击“VLAN 划分”页签，进入 VLAN 划分配置页面。

(3) 单击 GE1 接口对应的操作列编辑图标，进入详细端口配置页面。

(4) 在“PVID”配置项处，选择 10。

(5) 单击待选 VLAN 框中的 VLAN20，将 VLAN20 加入已选 VLAN 框。

(6) 单击<确定>按钮保存配置。

图4 配置 GE1 接口

4. 配置无线 AC

手工创建 AP，使得 AP 和 AC 之间可以建立连接。

(1) 在设备 Web 管理界面导航栏中选择无线 AC，进入无线 AC 配置页面。

(2) 在左侧导航栏中选择“快速配置 > 新增 AP”，进入新增 AP 页面。

(3) 在“AP 名称”配置项处，输入 ap1（自定义即可）。

(4) 在“AP 型号”配置项处，选择 WA4320H。（选择使用的 AP 型号）

(5) 在“AP 序列号”配置项处，输入 219801A0YG819BE005JC。（选择使用的 AP 序列号）

(6) 其它选项保持缺省配置，单击<确定>按钮，完成 AP 创建。

图5 新增 AP

配置 2.4G 射频，指定工作模式为 802.11g，工作信道为 6，最大传输功率为 19dBm。

(7) 在无线 AC 界面左侧导航栏中选择“无线配置 > 射频配置”，进入射频配置页面。

(8) 单击“所有 AP 的射频”对应行的更多按钮，进入所有 AP 的射频页面。

(9) 单击 2.4G 射频对应行的操作按钮，进入 AP 的射频配置页面。

(10) 单击<修改射频模式>按钮，进入修改射频模式页面。

(11) 在“射频模式”配置项处，选择 802.11g。

(12) 在“配置信道”配置项处，选择 6。

(13) 在“最大功率”配置项处，输入 19。

(14) 其它选项保持缺省配置，单击<确定>按钮，完成 2.4G 射频设置。

图6 配置 2.4G 射频

配置 5G 射频，指定工作模式为 802.11ac，工作信道为 157，最大传输功率为 19dBm。

(15) 在 AP 射频页面，单击 5G 射频对应行的操作按钮，进入 AP 的射频配置页面。

(16) 单击<修改射频模式>按钮，进入修改射频模式页面。

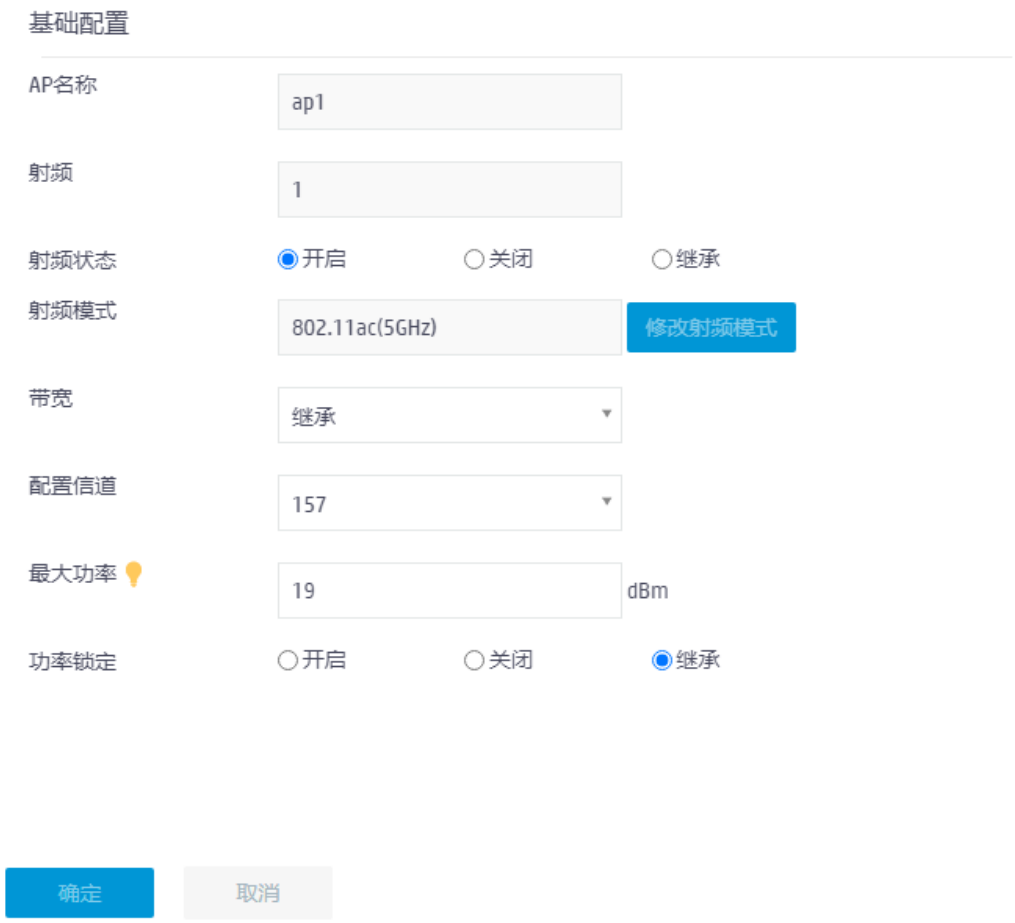
(17) 在“射频模式”配置项处，选择 802.11g。

(18) 在“配置信道”配置项处，选择 6。

(19) 在“最大功率”配置项处，输入 19。

(20) 其它选项保持缺省配置，单击<确定>按钮，完成 5G 射频设置。

图7 配置 5G 射频



创建 2.4G 无线服务模板 map1，配置 SSID 为 service1，配置客户端从无线服务模板 map1 上线后将被加入到 VLAN 20，并开启无线服务模板。

(21) 在无线 AC 配置界面左侧导航栏中选择“快速配置 > 新增无线服务”，进入新增无线服务页面。

(22) 在“无线服务名称”配置项处，输入 map1。

(23) 在“SSID”配置项处，选择 service1。

(24) 在“无线服务”配置项处，选择开启。

(25) 在“缺省 VLAN”配置项处，输入 20。

图8 2.4G 无线服务名称基础设置

将无线服务模板 map1 与 2.4G 射频绑定。

(26) 在新增无线服务页面，单击<确定并进入高级设置>按钮，进入高级设置页面。

(27) 单击页面中的<绑定>按钮，进入绑定页面。

(28) 单击待选项框中的 ap1（Radio2 2.4G），将 ap1（Radio2 2.4G）移动至已选项框。

(29) 单击<确定>按钮，完成无线服模板和射频的绑定。

图9 2.4G 无线服务名称高级设置

创建 5G 无线服务模板 map2，配置 SSID 为 service2，配置客户端从无线服务模板 map1 上线后将被加入到 VLAN 20，并开启服务模板。

(30) 在无线 AC 配置界面左侧导航栏中选择“快速配置 > 新增无线服务”，进入新增无线服务页面。

(31) 在“无线服务名称”配置项处，输入 map2。

(32) 在“SSID”配置项处，选择 service2。

(33) 在“无线服务”配置项处，选择开启。

(34) 在“缺省 VLAN”配置项处，输入 20。

图10 5G 无线服务名称基础设置

将无线服务模板 map2 与 5G 射频绑定。

(35) 在新增无线服务页面，单击<确定并进入高级设置>按钮，进入高级设置页面。

(36) 单击页面中的<绑定>按钮，进入绑定页面。

(37) 单击待选项框中的 ap1（Radio1 5G），将 ap1（Radio1 5G）移动至已选项框。

(38) 单击<确定>按钮，完成无线服模板和射频的绑定。

图11 5G 无线服务名称高级设置

4.4.2 配置二层交换机

配置 VLAN 及接口。

```
<L2 switch> system-view
[L2 switch] vlan 10
[L2 switch-vlan100] quit
[L2 switch] vlan 20
[L2 switch-vlan201] quit
[L2 switch] interface gigabitethernet 1/0/1
[L2 switch-GigabitEthernet1/0/1] port link-type trunk
[L2 switch-GigabitEthernet1/0/1] port trunk pvid vlan 10
[L2 switch-GigabitEthernet1/0/1] port trunk permit vlan 10 20
[L2 switch-GigabitEthernet1/0/1] quit
[L2 switch] interface gigabitethernet 1/0/2
[L2 switch-GigabitEthernet1/0/2] port link-type trunk
[L2 switch-GigabitEthernet1/0/2] port trunk pvid vlan 10
[L2 switch-GigabitEthernet1/0/2] port trunk permit vlan 10 20
[L2 switch-GigabitEthernet1/0/2] quit
[L2 switch]
```

开启 PoE 接口远程供电功能。

```
[L2 switch] interface gigabitethernet 1/0/2
[L2 switch-GigabitEthernet1/0/2] poe enable
[L2 switch-GigabitEthernet1/0/2] quit
```

4.5 验证配置

查看 AP 的详细信息，可以看到 AP 与 AC 成功建立隧道连接并进入 Run 状态。

```
[Router]display wlan ap name ap1 verbose
AP name                         : ap1
AP ID                           : 1
AP group name                   : default-group
State                           : Run
Backup type                     : Master
```

```
Online time                   : 0 days 4 hours 7 minutes 27 seconds
System uptime                 : 0 days 4 hours 17 minutes 4 seconds
Model                         : WA4320H
Region code                   : CN
Region code lock              : Disabled
Serial ID                     : 219801A0YG819BE005JC
MAC address                   : 9429-2f93-14c0
IP address                    : 192.168.0.4
UDP control port number       : 25930
UDP data port number          : 25930
H/W version                   : Ver.B
S/W version                   : R2439P01
Boot version                  : 7.21
USB state                     : Disabled
Power level                   : N/A
Power info                    : N/A
Description                   : Not configured
Priority                      : 4
Echo interval                 : 10 seconds
Echo count                    : 3 counts
```

.....显示信息略.....

Client 可以分别通过 service1 和 service2 的无线信号连接到 2.4G 和 5G 网络，说明配置验证成功。可使用命令 **display wlan client verbose** 查看到上线用户的连接情况。

```
[Router]display wlan client verbose
Total number of clients: 2

 MAC address                    : 424a-b9db-91bf
 IPv4 address                   : 192.168.20.3
 IPv6 address                   : N/A
 Username                       : N/A
 AID                            : 2
 AP ID                          : 1
 AP name                        : ap1
 Radio ID                       : 2
 SSID                           : service1
 BSSID                          : 9429-2f93-14d0
 VLAN ID                        : 20
 Sleep count                    : 22
 Wireless mode                  : 802.11g
 Supported rates                : 1, 2, 5.5, 6, 9, 11,
                                  12, 18, 24, 36, 48, 54 Mbps
 QoS mode                       : WMM
 Listen interval                : 20
 RSSI                           : 54
 Rx/Tx rate                     : 0/0 Mbps
 Speed                          : N/A
 Authentication method          : Open system
 Security mode                  : PRE-RSNA
```

```
AKM mode                          : Not configured
Cipher suite                      : N/A
User authentication mode          : Bypass
WPA3 status                       : N/A
Authorization CAR                 : N/A
Authorization ACL ID              : N/A
Authorization user profile        : N/A
Roam status                       : N/A
Key derivation                    : N/A
PMF status                        : N/A
Forwarding policy name            : Not configured
Online time                       : 0days 0hours 0minutes 6seconds
FT status                         : Inactive
```

.....显示信息略.....