H3C ER G3 系列路由器

端口映射典型配置举例

新华三技术有限公司
http://www.h3c.com

资料版本：6W102-20221021

1.1 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 ER G3 系列路由器-端口映射 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. 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。

2. 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。

3. 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。

4. 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！

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 管理页面中 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 ER3200G3 路由器 Release 0114 版本上进行配置和验证的。

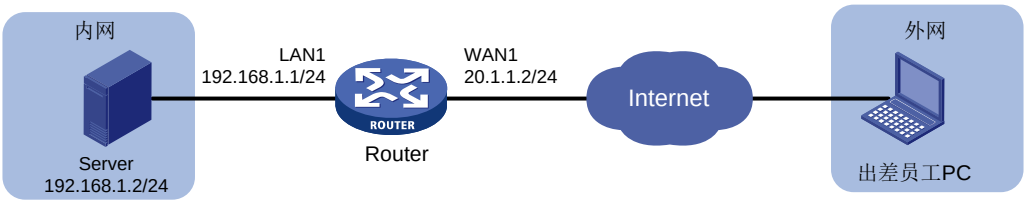
3.1 组网需求

如图 3-1 所示，Router 为某企业的出口网关，通过 WAN1 接口连接 Internet，WAN1 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3-1 端口映射典型配置组网图



3.2 配置注意事项

由于本例中映射的仅是服务器的 Web 服务，所以外部端口选择自定义端口，且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

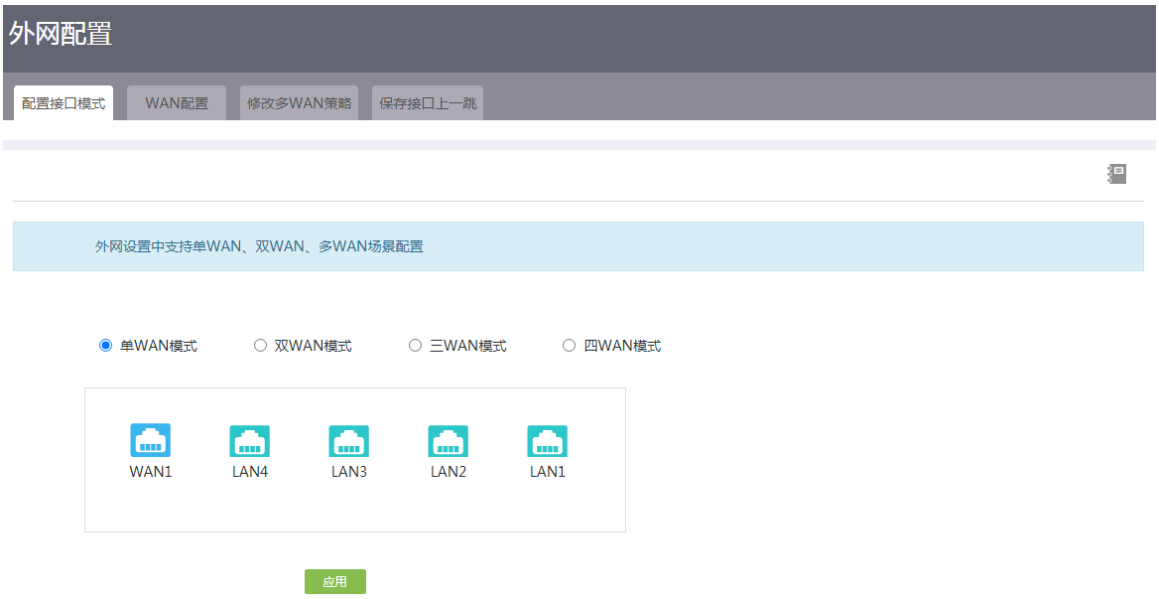
3.3.1 配置路由器上网

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“配置接口模式”页签下选择单 WAN 模式，单击<应用>按钮使得配置生效。

图3-2 配置 WAN 场景



(3) 单击“WAN 配置”页签，进入 WAN 配置页面。

(4) 单击 WAN1 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) 其它参数保持默认配置即可，单击<确定>按钮保存配置。

图3-3 配置 WAN1 接口连接 Internet

3.3.2 配置虚拟服务器（端口映射）

由于本例中映射的仅是服务器的 Web 服务，所以外部端口选择自定义端口，且起始端口号和结束端口号保持一致，建议输入 10000 及以上端口号。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) 单击<添加>按钮，进入添加 NAT 端口映射页面。

(3) 在“协议类型”配置项处，选择 TCP。

(4) 在“外部地址”配置项处，选择当前接口 IP 地址。

(5) 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。

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

(7) 在“内部端口”配置项处，起始端口号配置项处输入 80

(8) 在“是否启用”配置项处，勾选启用选项前方单选框，启用端口映射功能。

(9) 单击<确定>按钮完成配置。

图3-4 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。

H3C ER G3 系列路由器

IPsec VPN 典型配置举例

新华三技术有限公司
http://www.h3c.com

资料版本：6W102-20221021

1.1 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 ER G3 系列路由器-IPsec VPN 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. 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。

2. 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。

3. 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。

4. 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！

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 ER3200G3 路由器的 Release 0123 版本上进行配置和验证的。

4 主模式配置举例

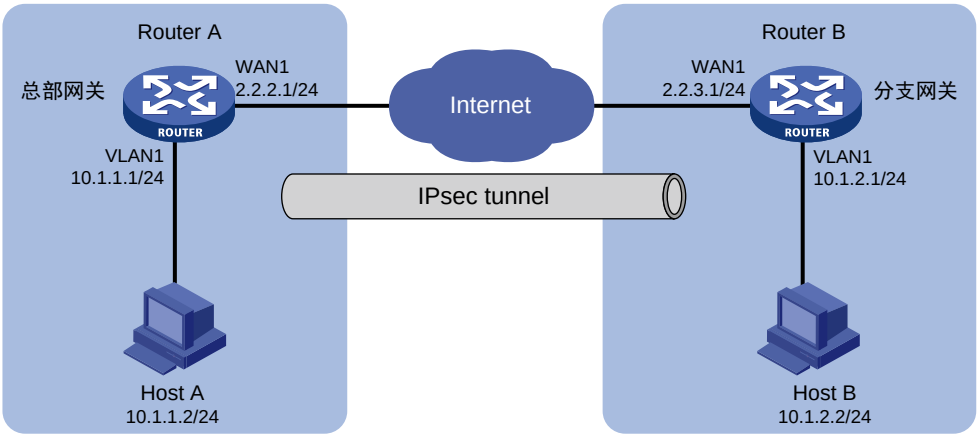
4.1 组网需求

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“VLAN 配置”页签，进入 VLAN 配置页面。

(3) 单击 VLAN1 对应的操作列编辑图标，进入修改 VLAN 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 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“配置接口模式”页签下选择单 WAN 模式，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

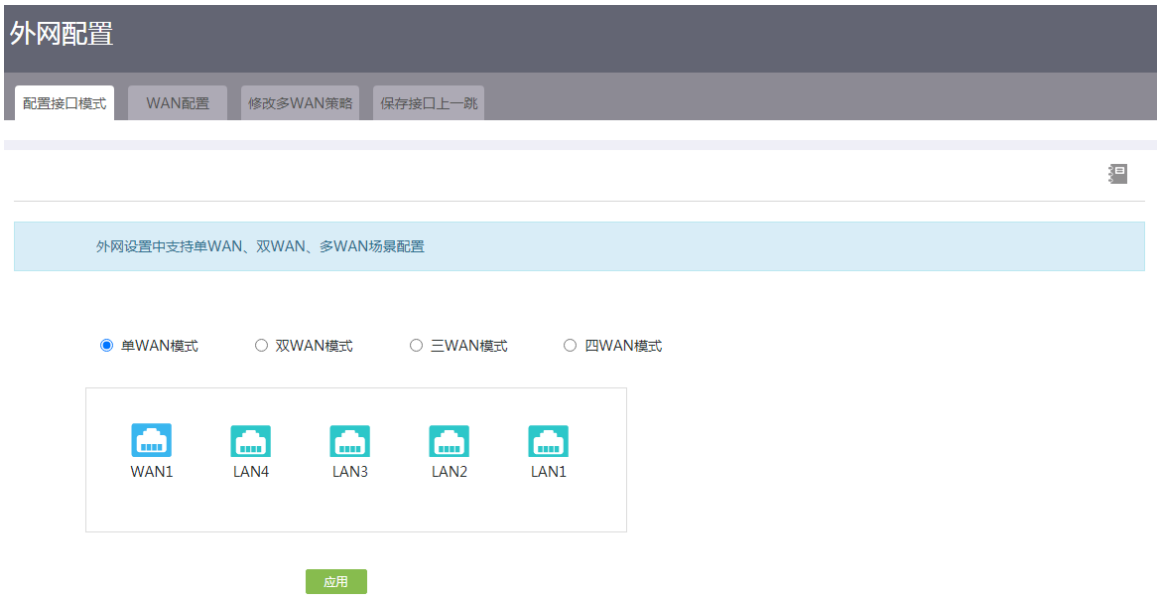


图4 修改 WAN 配置

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：

- IKE 版本：选择 V1
- 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，探测时间和超时时间保持缺省配置即可（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“VLAN 配置”页签，进入 VLAN 配置页面。

(3) 单击 VLAN1 对应的操作列编辑图标，进入修改 VLAN 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“配置接口模式”页签下选择单 WAN 模式，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
配置接口模式
WAN配置
修改多WAN策略
保存接口上一跳
外网设置中支持单WAN、双WAN、多WAN场景配置
单WAN模式
双WAN模式
三WAN模式
四WAN模式
WAN1
LAN4
LAN3
LAN2
LAN1
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：

- IKE 版本：选择 V1
- 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，探测时间和超时时间保持缺省配置即可
- 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 UP，说明配置验证成功。

5 野蛮模式配置举例

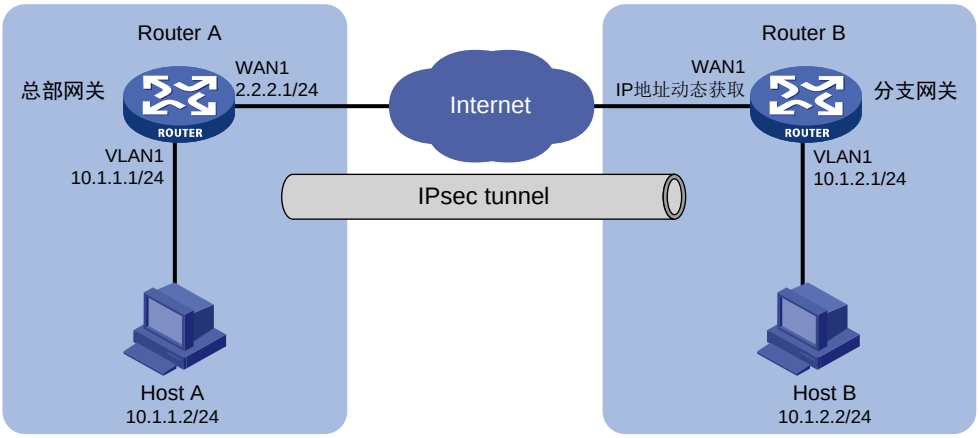
5.1 组网需求

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“VLAN 配置”页签，进入 VLAN 配置页面。

(3) 单击 VLAN1 对应的操作列编辑图标，进入修改 VLAN 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“配置接口模式”页签下选择单 WAN 模式，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

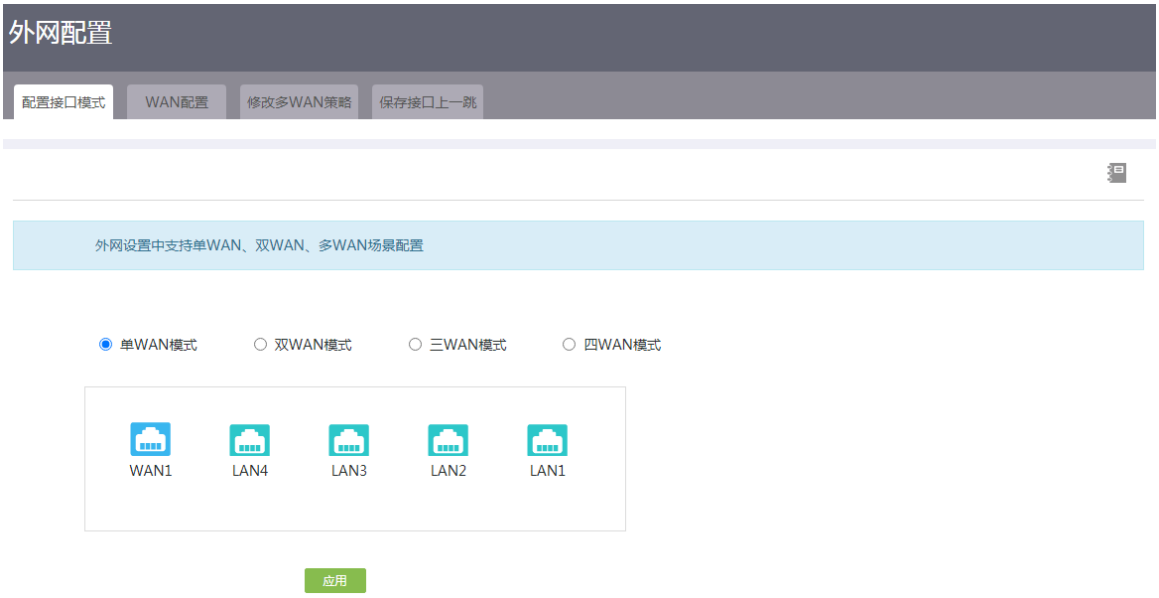

外网配置
配置接口模式
WAN配置
修改多WAN策略
保存接口上一跳
外网设置中支持单WAN、双WAN、多WAN场景配置
单WAN模式
双WAN模式
三WAN模式
四WAN模式
WAN1
LAN4
LAN3
LAN2
LAN1
应用

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：

- IKE 版本：选择 V1
- 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，探测时间和超时时间保持缺省配置即可（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“VLAN 配置”页签，进入 VLAN 配置页面。

(3) 单击 VLAN1 对应的操作列编辑图标，进入修改 VLAN 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“配置接口模式”页签下选择单 WAN 模式，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) 在“DNS1”配置项处，输入 114.114.114.114。

(7) 在“DNS2”配置项处，输入 223.5.5.5。

(8) 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


外网配置
配置接口模式
WAN配置
修改多WAN策略
保存接口上一跳
外网设置中支持单WAN、双WAN、多WAN场景配置
单WAN模式
双WAN模式
三WAN模式
四WAN模式
WAN1
LAN4
LAN3
LAN2
LAN1
应用

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：

- IKE 版本：选择 V1
- 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，探测时间和超时时间保持缺省配置即可
- 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。

H3C ER G3 系列路由器

L2TP VPN 典型配置举例

新华三技术有限公司
http://www.h3c.com

资料版本：6W102-20221021

1.1 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 ER G3 系列路由器-L2TP VPN 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. 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。

2. 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。

3. 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。

4. 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！

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

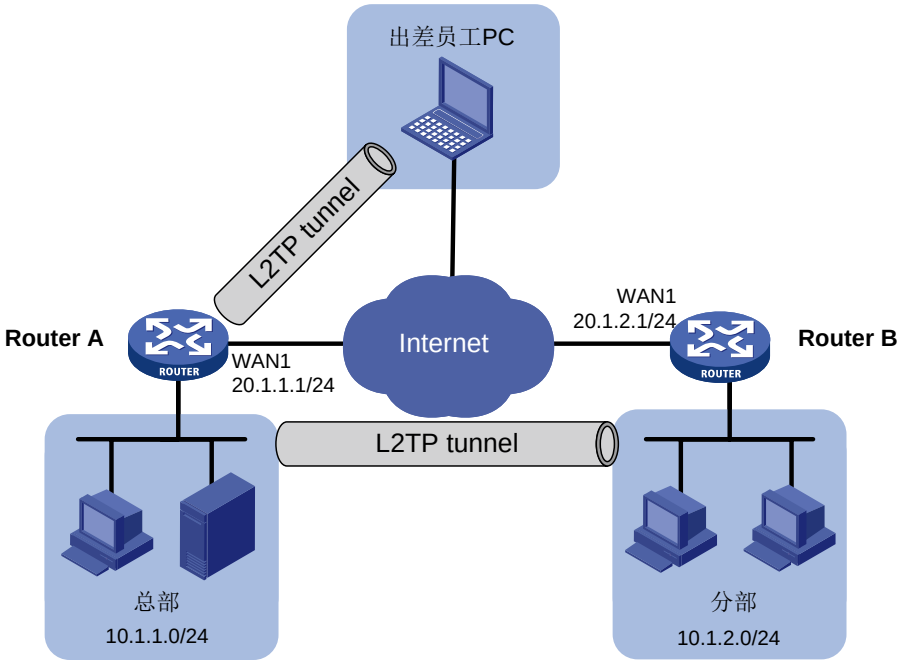
本配置举例是在 ER3200G3 系列路由器 Release 0118 版本上进行配置和验证的。

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 WAN1 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；

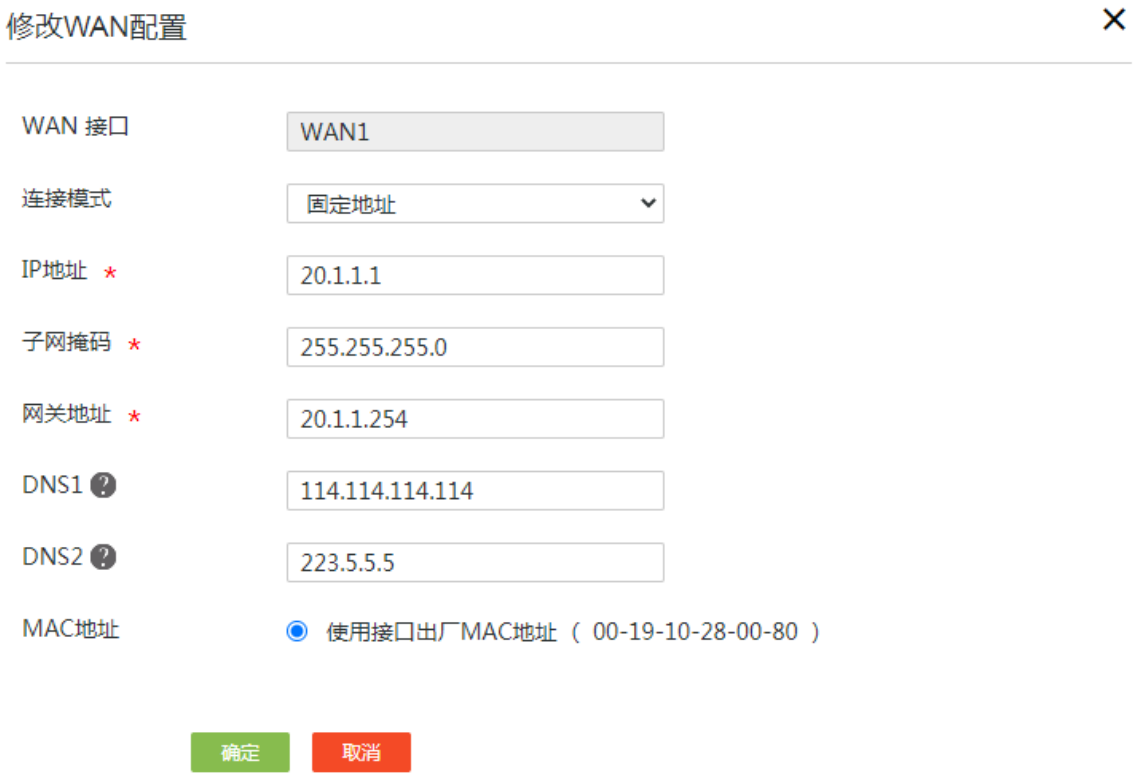
(2) 单击“WAN 配置”页签，进入 WAN 配置页面；

(3) 单击 WAN1 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
- 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 WAN1 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“启用 L2TP 服务器端”选项，单击“确定”按钮，完成 L2TP 服务器的启用。

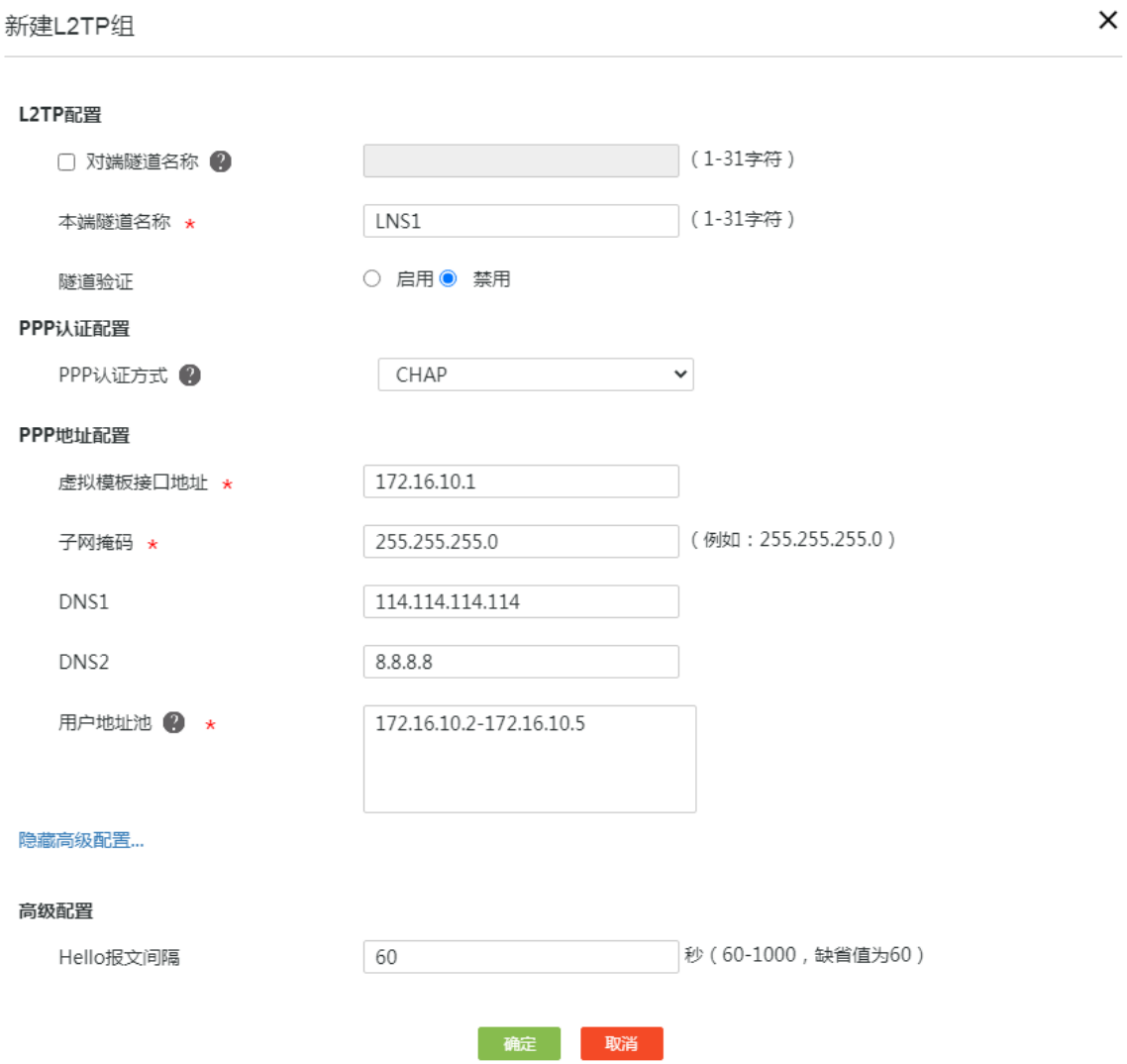
(1) 配置 LNS1（供出差员工 PC 连接）

#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）
- DNS1：114.114.114.114（输入可用 DNS 即可）
- DNS2：8.8.8.8（输入可用 DNS 即可）
- 用户地址池：172.16.10.2-172.16.10.5（根据实际情况输入）

- Hello 报文间隔：保持缺省值 60 秒
- 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）
- DNS1：114.114.114.114（输入可用 DNS 即可）
- DNS2：8.8.8.8（输入可用 DNS 即可）

- 用户地址池：172.16.20.2-172.16.20.5（根据情况输入）
- Hello 报文间隔：保持缺省值 60 秒
- 单击“确认”按钮，完成 LNS2 的添加

图4 配置 LNS2

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“虚拟专网（VPN）>L2TP 服务器端”，单击“L2TP 用户”页签，进入 L2TP 用户配置页面，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）
- 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 WAN1 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；

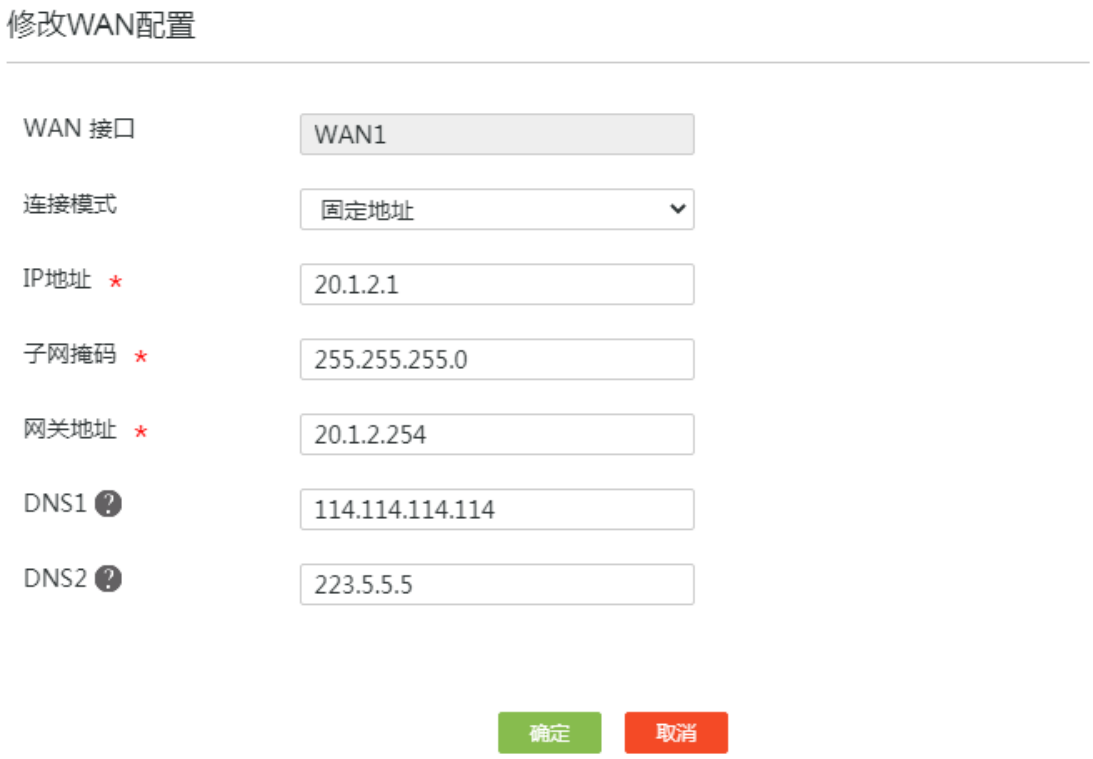
(2) 单击“WAN 配置”页签，进入 WAN 配置页面，单击 WAN1 接口对应操作列编辑图标，进入修改 WAN 配置页面，配置如下参数：

- 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
- 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 WAN1 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“启用 L2TP 客户端”选项，单击“确定”按钮，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
- NAT 地址转换：选择“启用”（若选择“不启用”，需要总部添加到分部的静态路由）

- L2TP 服务器端地址：20.1.1.1（总部 WAN1 接口 IP 地址）
- Hello 报文间隔：保持缺省 60 秒
- 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：L2TP1（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

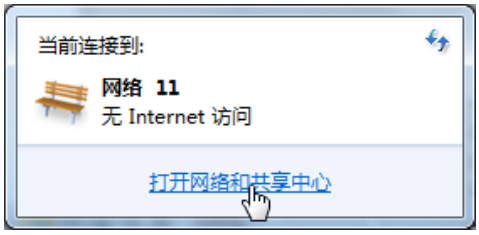
图9 配置静态路由

4.3.3 配置出差员工 PC

说明

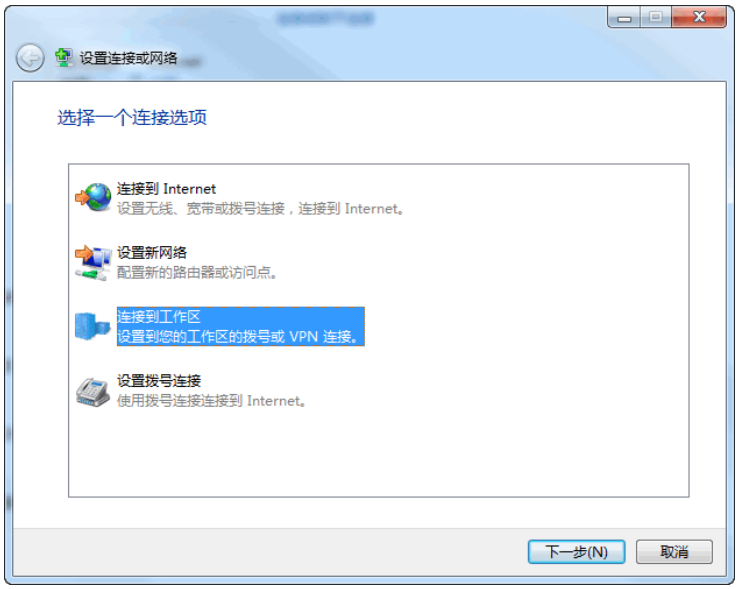
在出差员工 PC 上配置 L2TP 客户端，本例以装有 Window 7 系统的 PC 为例。

#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”。

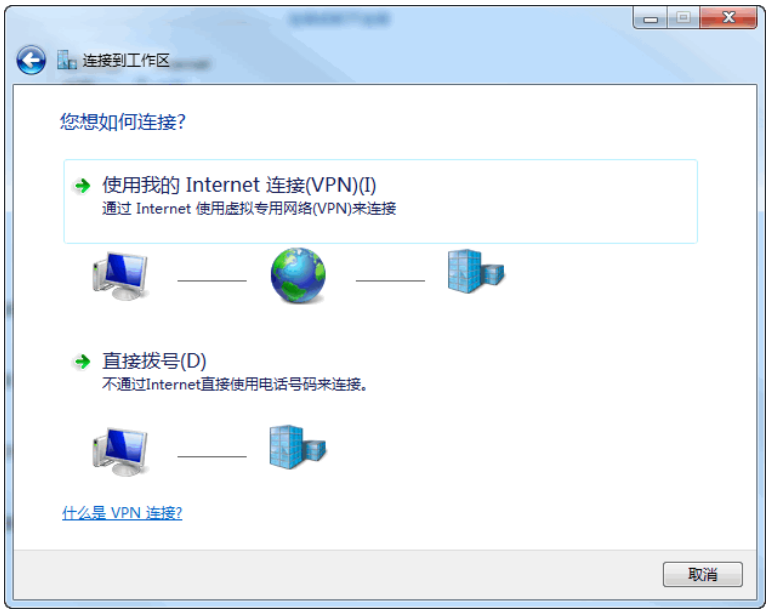


单击“设置新的连接或网络”选项，创建一个 L2TP 客户端。

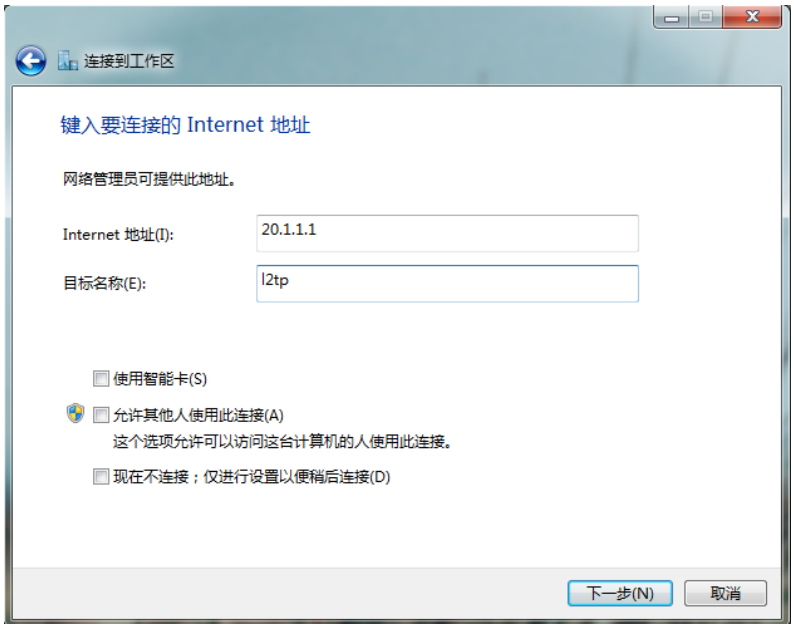
在弹出的设置连接或网络对话框中，选择“连接到工作区”选项，单击“下一步”按钮。



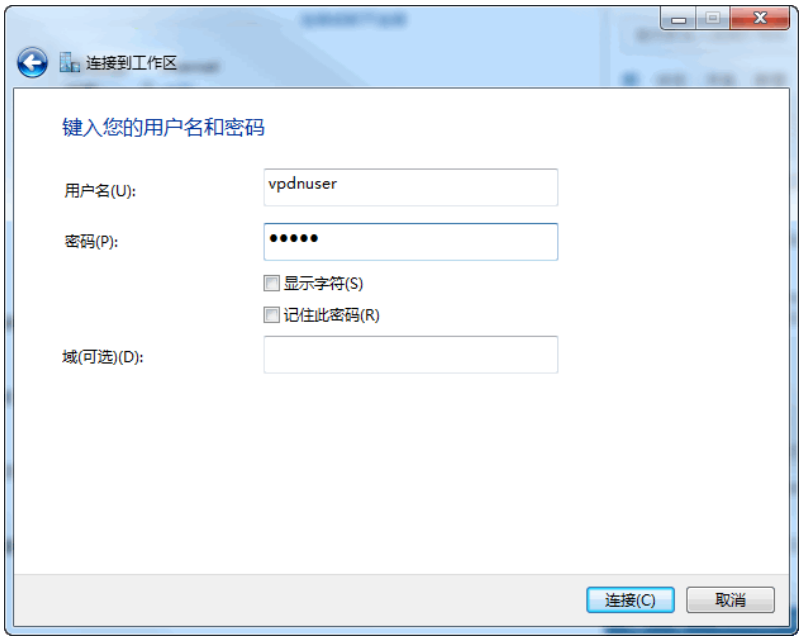
选择“使用我的 Internet 连接(VPN)(I)”选项，开始配置连接的 Internet 地址。



在 Internet 连接(T)配置项中，输入要连接到的 L2TP 服务器段 WAN1 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。

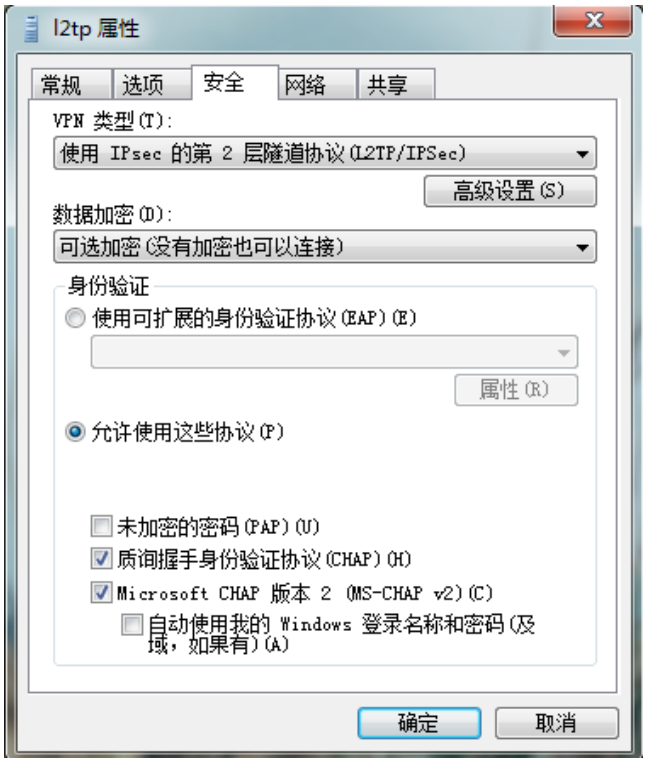


在用户名和密码配置项中，分别输入 L2TP 服务器端设置的用户名和密码，本例用户名为 vpdnuser，密码为 user1234，单击“连接”按钮进行连接。



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。

图10 隧道信息

H3C ER G3 系列路由器

MiniAP 典型配置举例

新华三技术有限公司
http://www.h3c.com

资料版本：6W102-20221021

1.1 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 ER G3 系列路由器-MiniAP 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. 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。

2. 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。

3. 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。

4. 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！

目 录

1 简介

本文档介绍 MiniAP 管理的配置方法。

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 MiniAP 管理特性。

3 使用版本

本配置举例是在 ER3200G3 路由器 Release 0124 版本上进行配置和验证的。

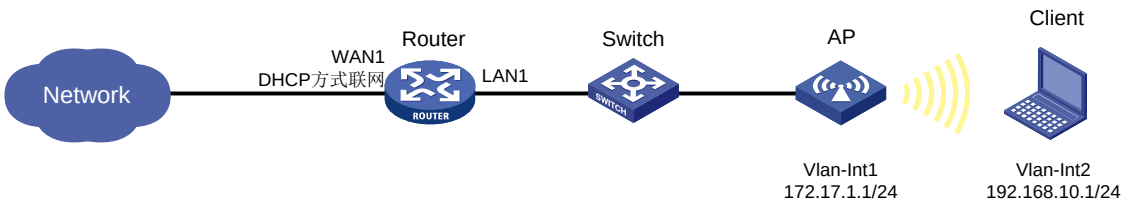
4 配置举例

4.1 组网需求

如图 1 所示 Router 为某企业的出口网关，通过 WAN1 接口连接外网，接口的连接模式为 DHCP。AP 通过 PoE 交换机（非管理型）连接 Router 的 LAN1 接口，,Router 作为 DHCP server 为 AP 和 Client 分配 IP 地址。现需要实现 Client 通过 AP 下发的无线连接到外网，具体要求如下：

- AP 的管理 VLAN 为 VLAN1，IP 地址为 172.17.1.1/24。
- Client 接入的无线名称为 service1（2.4G 网络）和 service2（5G 网络），密码均为 service@123。
- Client 获取的 IP 地址为 192.168.10.1/24 网段，用 VLAN2 标识。

图1 AP 管理典型配置组网图



4.2 配置注意事项

- 设备支持的无线加密方式有如下两种：
  - WPA-PSK/WPA2-PSK 加密：若无线终端支持 WIFI5 无线协议，推荐使用该方式加密。
  - WPA2-PSK/WPA3-PSK 加密：若无线终端支持 WIFI6 无线协议，推荐使用该方式加密。

请根据您的实际使用场景，选择对应的加密方式，本例选择 WPA-PSK/WPA2-PSK 加密。

- 您可以根据需要修改无线的网络模式、频宽、信道、发射功率，本例均保持缺省配置。
- 您可以根据需要修改 AP 的管理 VLAN 以及 AP 管理地址，本例保持缺省的 VLAN1，IP 地址为 172.17.1.1/24
- Router 上连接 AP 接口的 PVID 需要和 AP 的管理 VLAN ID 一致。本例 AP 的管理 VLAN 为 VLAN 1，则 GE2/0 接口的 PVID 需要设置为 1。

4.3 配置思路

- 在 Router 上划分 VLAN2，且设置 LAN1 接口同时通过 VLAN1 和 VLAN2。
- 创建无线服务模板，在模板中添加无线 2.4G 和 5G 的无线名称和密码，并与 VLAN2 进行绑定。
- 将创建的无线服务模板下发给 AP。

4.4 配置步骤

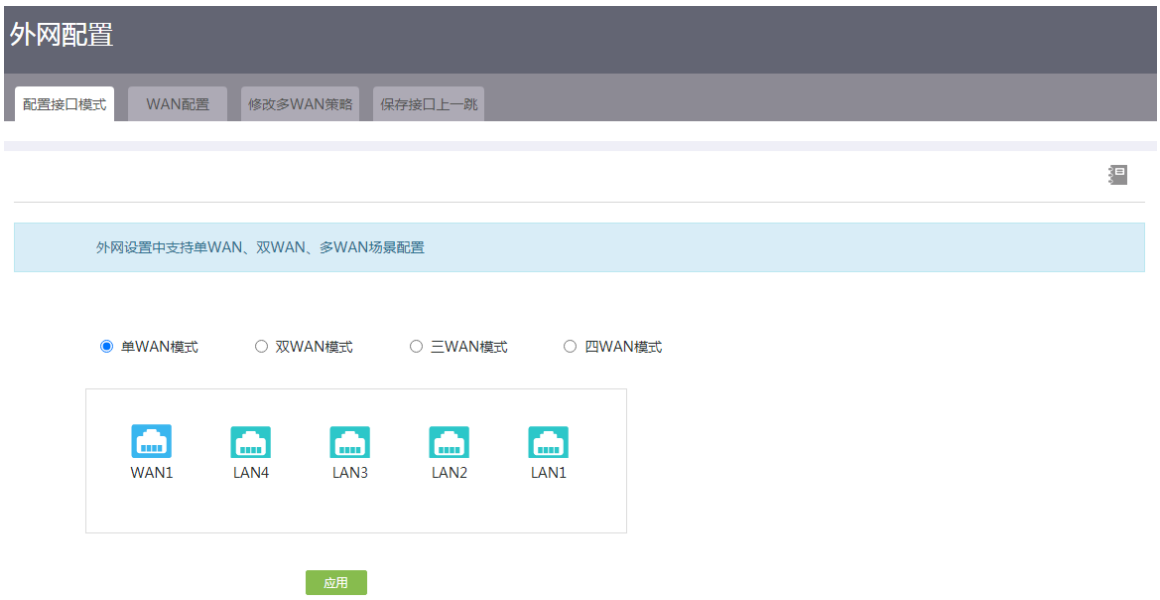
4.4.1 配置 WAN1 接口连接 Internet

本例 Router 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“配置接口模式”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 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) 在“DNS1”配置项处，输入 114.114.114.114。

(7) 在“DNS2”配置项处，输入 223.5.5.5。

(8) 其它配置项均保持缺省配置，单击<确定>按钮保存配置。

图3 修改 WAN 配置

4.4.2 划分 VLAN

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 192.168.10.1/24。

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

(2) 单击<添加>按钮，进入添加 VLAN 页面。

(3) 在“VLAN ID”配置项处，输入 2。

(4) 在“接口 IP 地址”配置项处，输入 192.168.10.1。

(5) 在“子网掩码”配置项处，输入 255.255.255.0。

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

(7) 其它配置项保持默认配置，单击<确定>按钮，完成配置。

图4 配置 VLAN2

2. 允许 LAN1 接口通过 VLAN2

LAN1 接口缺省情况下仅允许通过 VLAN1，本例需要同时通过 VLAN1 和 VLAN2。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。

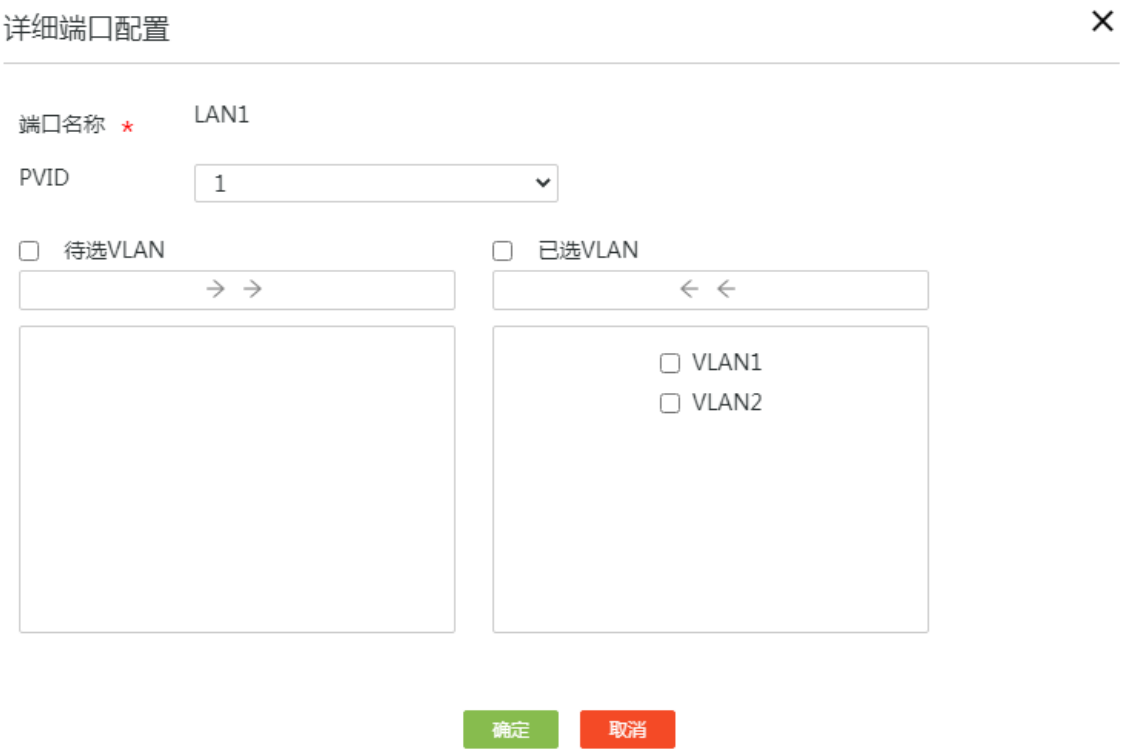
(2) 单击<VLAN 划分>页签，进入 VLAN 划分配置页面。

(3) 单击 LAN1 接口对应的操作列编辑图标，进入详细端口配置页面

(4) 勾选待选 VLAN 框中 VLAN2 前方的单选框，单击<→→>按钮，将 VLAN2 加入已选 VLAN 框。

(5) 单击<确定>按钮，完成配置。

图5 允许 LAN1 接口通过 VLAN2



4.4.3 启用 AP 管理功能

启用 AP 管理功能，使得 AP 上线。配置步骤如下：

(1) 在设备 Web 管理界面导航栏中选择“MiniAP 管理 > AP 管理设置”，进入 AP 管理设置页面。

(2) 在“AP 管理功能”配置项处，选择启用。

(3) 其它选择保持缺省配置，单击<确定>按钮，完成配置。

图6 启用 AP 管理功能

4.4.4 配置无线服务模板

#您可以选择在设备缺省的 default 模板中配置 2.4G 和 5G 的无线名称和密码。本例选择创建新的名称为 map1 的无线服务模板，配置步骤如下：

(1) 在设备 Web 管理界面导航栏中选择“MiniAP 管理 > 配置管理”，进入配置管理页面。

(2) 单击“配置模板管理”页签，进入配置模板管理页面。

(3) 单击“添加”按钮，进入添加配置模板页面。

(4) 在“模板名称”配置项处，输入 map1。

图7 创建模板

(5) 在“2.4G 配置”配置项处，单击<添加>按钮，进入添加 SSID 配置页面

(6) 勾选“启用 SSID”前方的单选框，启用 SSID 功能。

(7) 在“SSID 名称”配置项处，输入 service1。

(8) 在“加密方式”配置项处。选择 WPA-PSK/WPA2-PSK。

(9) 在“共享密钥”配置项处。设置 service@123。

(10) 勾选“高级设置”前方单选框，进行高级功能设置。

(11) 在“桥接 VLAN”配置项处，输入 2。

(12) 其它选择保持缺省配置，单击<确定>按钮，完成 2.4G 无线配置。

图8 无线 2.4G 配置

(13) 在“5G 配置”配置项处，单击<添加>按钮，进入添加 SSID 配置页面。

(14) 勾选“启用 SSID”前方的单选框，启用 SSID 功能。

(15) 在“SSID 名称”配置项处，输入 service2。

(16) 在“加密方式”配置项处。选择 WPA-PSK/WPA2-PSK。

(17) 在“共享密钥”配置项处。设置 service@123。

(18) 勾选“高级设置”前方单选框，进行高级功能设置。

(19) 在“桥接 VLAN”配置项处，输入 2。

(20) 其它选择保持缺省配置，单击<确定>按钮，完成 5G 无线配置。

图9 无线 5G 配置

(21) 其它选择保持缺省配置，单击<确定>按钮，完成配置模板添加。

4.4.5 下发无线服务模板

缺省情况下，上线 AP 绑定的为 default 模板，本例需要将创建的 map1 模板下发给在线 AP，配置步骤如下：

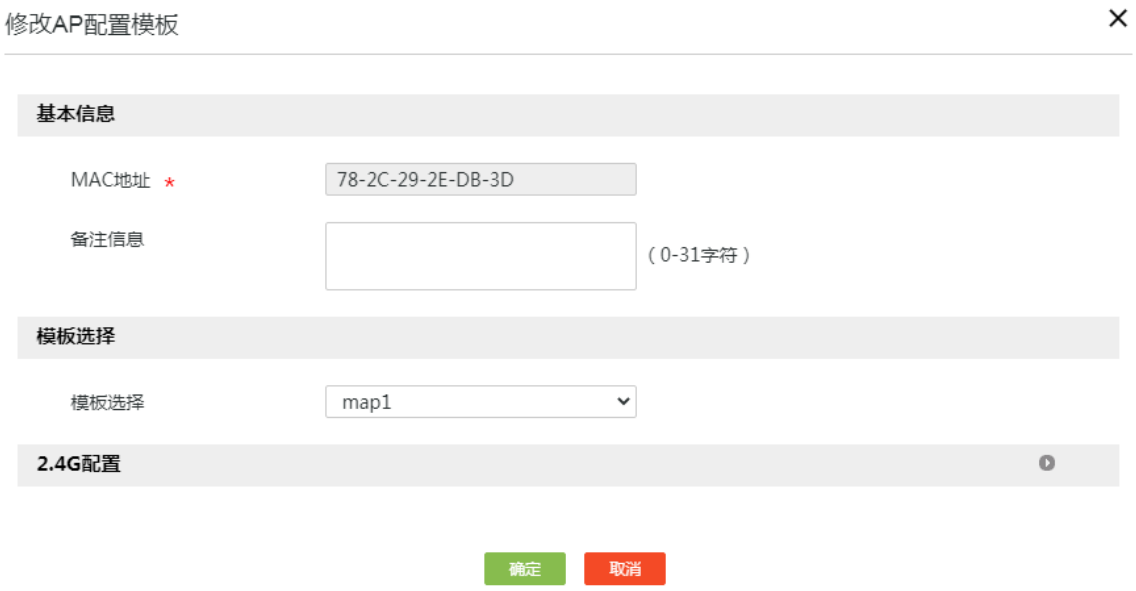
(1) 在设备 Web 管理界面导航栏中选择“MiniAP > 配置管理”，进入配置管理页面。

(2) 单击<AP 配置管理>页签，进入 AP 配置管理页面。

(3) 单击 AP MAC 地址对应的操作列编辑图标，进入 AP 模板修改页面，在模板选择配置相处，选择“map1”

(4) 单击“确认”按钮，完成配置的下发

图10 AP 配置管理



4.5 验证配置

Client 可以通过无线名称为“service1”或“service2”的无线信号连接到互联网，且获取到 IP 地址为 192.168.10.1/24 网段，说明配置验证成功。

H3C ER G3 系列路由器

Portal 认证典型配置举例

新华三技术有限公司
http://www.h3c.com

资料版本：6W102-20221021

1.1 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 ER G3 系列路由器-Portal 认证 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. 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。

2. 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。

3. 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。

4. 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！

目 录

1 简介

当网络管理员需要对接入设备的用户身份进行验证时，可以通过配置设备 Web 管理界面上的 Portal 认证功能来实现。

- 设备的Portal认证方式为云端认证，采用云端服务器（H3C 云简网络平台，以下简称云平台）来同时承担 Portal 认证服务器和 Portal Web 服务器的职责。
- 设备当前可结合云平台对用户进行微信公众号、短信登录、账号登录和一键上网等认证方式，本文档采用一键上网认证方式进行配置举例。
- 您可以为不需要通过 Portal 认证即可访问网络资源的用户设置免认证规则，免认证规则的匹配项包括 MAC 地址和 IP 地址。

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 Portal 认证特性。

3 使用版本

本配置举例是在 ER3200G3 路由器 Release 0114 版本上进行配置和验证的。

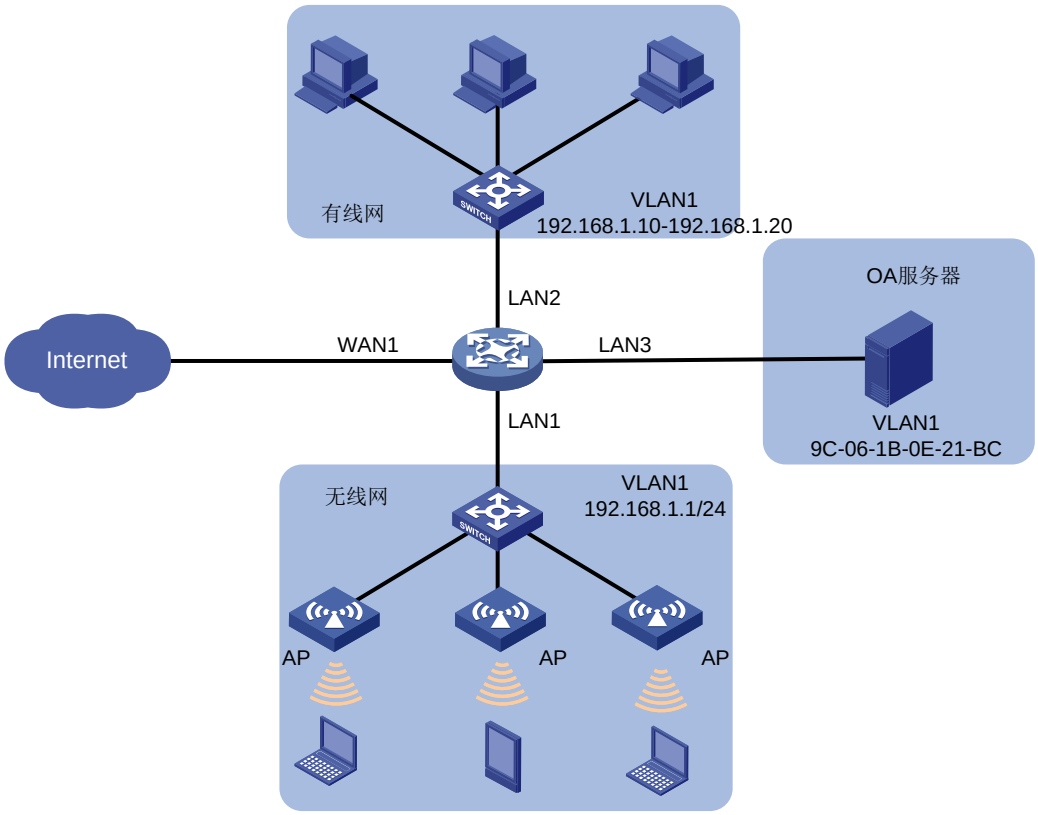
4 配置举例

4.1 组网需求

如图 4-1 所示，某酒店出于营销需求，需要在 Router 上进行如下配置：

- 所有无线终端上网时需要进行一键上网认证。
- 有线上网的 PC 上网时无需认证，免认证方式采用 IP 地址。
- 部署在内网的 OA 服务器上网时无需认证，免认证方式采用 MAC 地址。

图4-1 Portal 认证典型配置组网图



4.2 配置注意事项

- 配置 Portal 认证前，需要将设备绑定到云平台。
- 在云平台进行认证配置时，您可以选择自己创建模板，或着选择云平台提供的默认模板。本例选择云平台默认的酒店模板。

4.3 配置步骤

4.3.1 将 Router 绑定云平台

本例选择将 Router 绑定在云平台中我的网络分支下的杭州场所，设备名称为 ER G3。具体配置步骤参见《H3C ER G3 系列路由器如何连接云平台配置举例》，本文档不再描述。

绑定完成后，在设备 Web 管理界面的导航栏中选择“系统工具 > 远程管理”，进入远程管理配置页面。单击“云服务”页签，云管理状态为已纳入管理，说明设备已成功绑定云平台。

图4-2 将设备绑定云简网络

4.3.2 在云平台进行认证配置

1. 配置认证模板

本例选择云平台默认的酒店模板，配置步骤如下：

(1) 登录云简网络平台，选择“网络管理 > 配置 > ER G3 路由器 > 认证配置”，进入认证配置页面。

(2) 单击<添加>按钮，进入认证配置页面。

(3) 在分支场所框中选择“我的网络”。

(4) 在场所框中选择“杭州”

(5) 在设备切换框中选择当前 ER G3 设备

(6) 单击<+添加>按钮，弹出的选择模板页面中选择“酒店模板”。

(7) 单击<选择>按钮，弹出模板信息页面。

(8) 在“模板名称”配置项处，输入 test。

(9) 在“接口名称”配置项处，选择 VLAN1。（终端所属的 VLAN）

(10) 单击<应用>按钮，完成模板配置。

图4-3 增加认证模板

2. 配置一键认证

(1) 在认证配置页面，单击已创建的“test”模板后的绘制按钮，进入绘制页面。

(2) 在“定制移动端页面”页签下，单击<登录>按钮，进入认证配置页面。

(3) 点开“认证方式”伸缩栏，开启“一键上网功能”，其它配置项保持默认即可。

(4) 点开“高级配置”伸缩栏，可对上网时长等做出限制，本例保持默认配置。

(5) 单击<完成>按钮，完成一键认证的配置并发布。

图4-4 配置一键认证

4.3.3 启用云认证功能

需要在路由器 Web 管理界面启用云认证功能，步骤如下：

(1) 在设备 Web 管理界面导航栏中选择“认证管理 > Portal 认证”，进入 Portal 认证页面。

(2) 单击“云认证”页签进入云认证配置页面，

(3) 单击 VLAN1 对应的云认证功能列的按钮，使得按钮状态为“开启”，开启云认证功能。

图4-5 启用云认证功能

4.3.4 配置有线终端进行免认证

1. 配置地址组

将有线网区域 PC 的 IP 地址段设置为一个地址组，方便在设置免认证时引用。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 > 地址组”，进入地址组配置页面。

(2) 单击<添加>按钮，进入添加地址组配置页面。

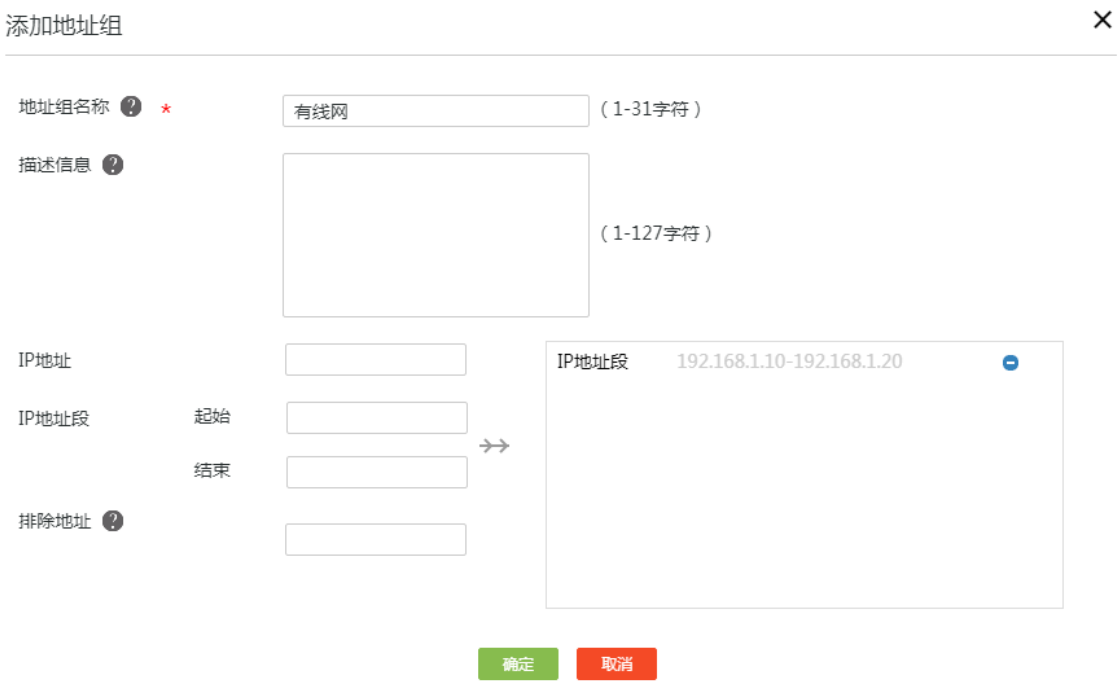
(3) 在“地址组名称”配置项处，输入有线网。

(4) 在“IP 地址段”配置项处，起始框输入 192.168.1.10，结束框输入 192.168.1.20。

(5) 单击<→→>按钮，提交配置的地址组内容

(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4-6 配置地址组



2. 配置免认证

(1) 在设备 Web 管理界面导航中选择“认证管理 > Portal 认证”，进入 Portal 认证页面。

(2) 单击“免认证 IP 地址”页签，进入免认证 IP 地址配置页面。

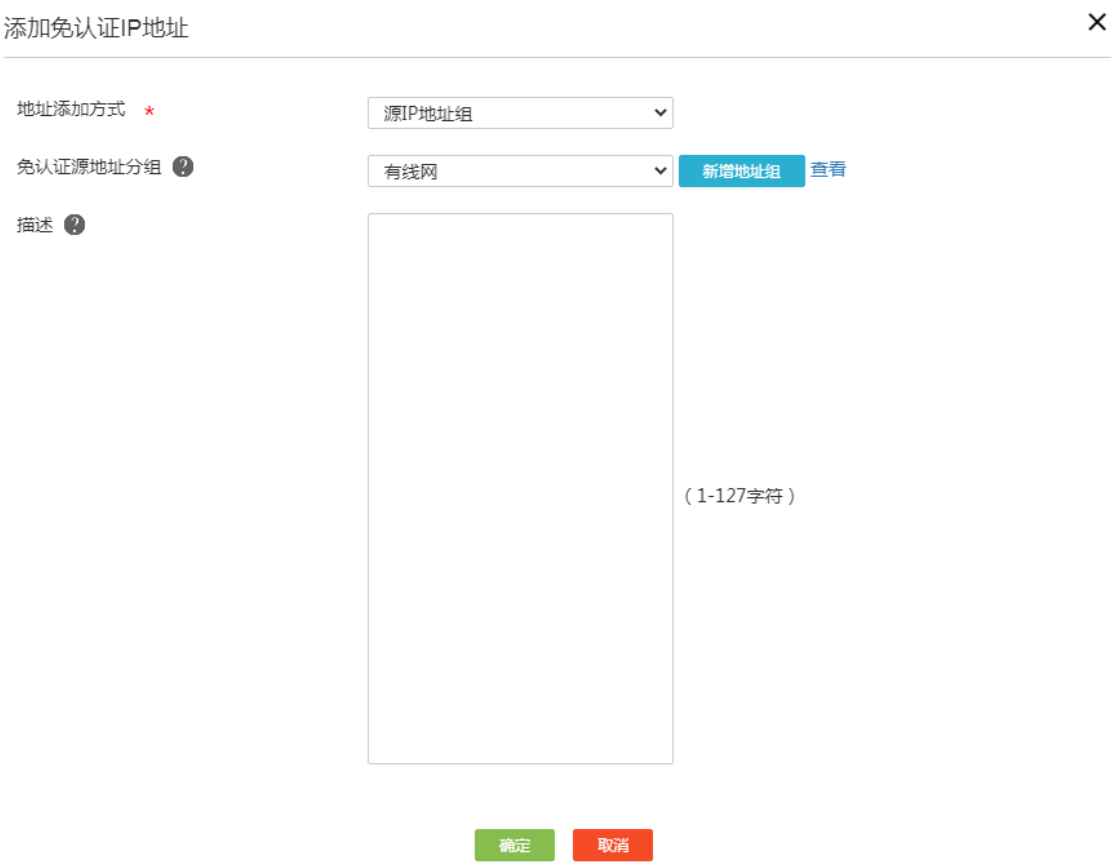
(3) 单击<添加>按钮，进入“添加免认证 IP 地址”页面。

(4) 在“地址组添加方式”配置项处，选择“源 IP 地址组”。

(5) 在“免认证源地址分组”配置项处，选择刚创建的有线网地址组。

(6) 单击<确定>按钮，完成配置。

图4-7 配置免认证 IP 地址



4.3.5 配置 OA 服务器进行免认证

(1) 在设备 Web 管理界面导航中选择“认证管理 > Portal 认证”，进入 Portal 认证页面。

(2) 单击“免认证 MAC 地址”页签，进入免认证 MAC 地址配置页面。

(3) 单击<添加>按钮，进入“添加免认证 MAC 地址”页面。

(4) 在“MAC 地址”配置项处，输入 9C-06-1B-0E-21-BC（OA 服务器的 MAC 地址）。

(5) 单击<确定>按钮，完成配置

图4-8 配置免认证 MAC 地址

4.4 验证配置

酒店内有线网终端和 OA 服务器上网时无需认证，使用手机连接酒店 WiFi，可以弹出一键上网认证界面，配置验证成功。

图4-9 认证页面


15:46
4G
oasisauth.h3c.com
H3C
登录
取消
主题酒店
便利设施：110V电压插座、空调、书桌、保险箱、衣柜/衣橱、电吹风机、电熨烫机...
便利设施：衣柜/衣橱、电吹风机、电熨烫机...
点我上网
同意《Wi-Fi使用协议》

H3C ER G3 系列路由器

防火墙典型配置举例

新华三技术有限公司
http://www.h3c.com

资料版本：6W102-20221021

1.1 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 ER G3 系列路由器-防火墙 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. 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。

2. 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。

3. 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。

4. 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！

目 录

1 简介

本文档介绍路由器防火墙功能的典型配置举例。

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防火墙特性。

3 使用版本

本配置举例是在 ER3200G3 路由器 Release 0118 版本上进行配置和验证的。

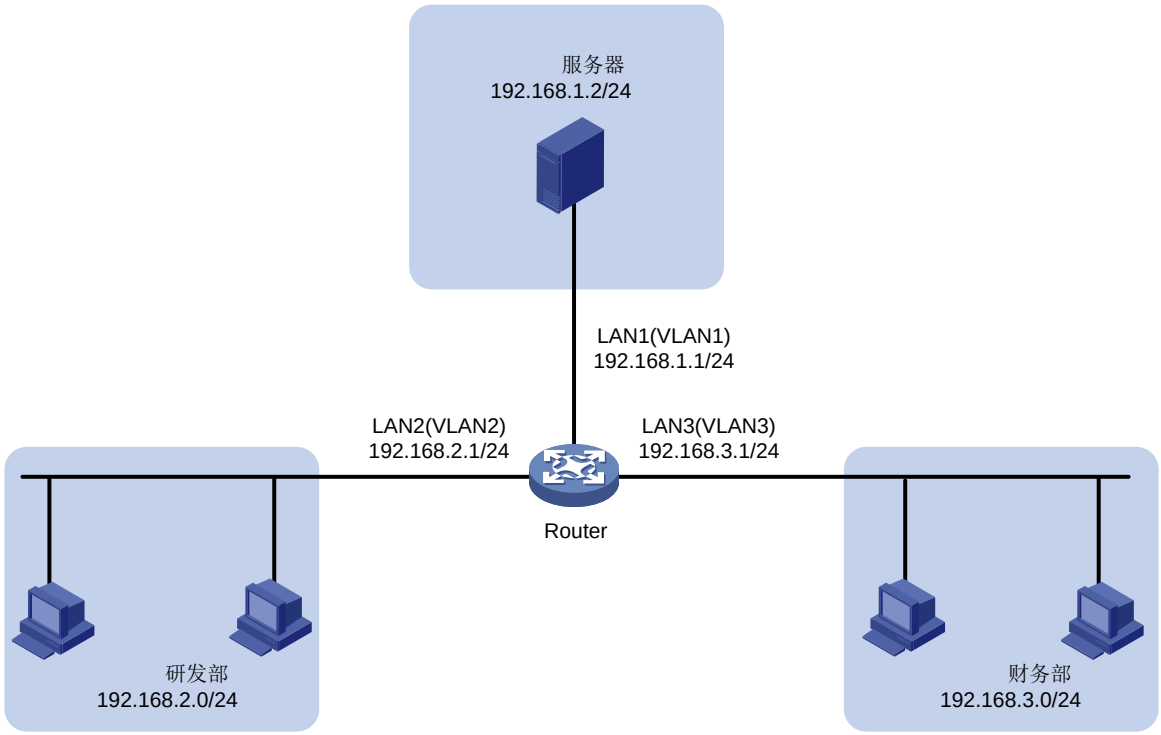
4 配置举例

4.1 组网需求

如图 4-1 所示，某企业通过 Router 连接了服务器与内网中各部门的 PC，需要根据各部门的业务对访问服务器的权限进行控制。具体要求如下：

- 研发部的 PC 仅允许在工作时间内（周一至周五 9:00~18:00）访问服务器。
- 不允许财务部的 PC 在任何时间访问服务器。

图4-1 防火墙典型配置组网图



4.2 配置思路

需要在 Router 上进行如下配置：

(1) 划分 VLAN2 和 VLAN3，并配置接口 IP 地址。

(2) 将 LAN2 接口划分到 VLAN2，LAN3 接口划分到 VLAN3。

(3) 将研发部所在的子网（192.168.2.1/24）设置为名称为“研发部”的地址组，将财务部所在子网（192.168.3.1/24）设置为名称为“财务部”的地址组，将服务器 IP 地址（192.168.1.2）设置为名称为“服务器”的地址组。

(4) 将工作时间段（周一至周五 9:00~18:00）设置为名称为“工作时间”的时间组。

(5) 开启防火墙功能并配置以下防火墙规则：

- 不允许研发部的 PC 在任何时间访问服务器；
- 允许研发部的 PC 在工作时间访问服务器；
- 不允许财务部的 PC 在任何时间访问服务器。

4.3 配置注意事项

- 当启用设备防火墙功能后，可通过配置“缺省过滤规则”来对未匹配任何安全规则的报文进行处理：
  - 若设置为允许，用户不需要配置任何安全规则，接入当前设备的所有终端都可以相互访问，且可以访问外网。

  - 如果用户需要限制指定终端访问特定外网的权限，可根据需求配置指定的 VLAN 接口与 WAN 接口之间的安全规则。
  - 如果用户需要限制指定终端访问其它 VLAN 下终端的权限，可根据需求配置指定的 VLAN 接口到 VLAN 接口的安全规则。
- 若设置为禁止，如果用户未配置任何安全规则，所有终端不能访问外网，不同 VLAN 下的终端不能相互访问。
  - 如果用户需要允许指定终端可以访问特定外网，则需要根据需求配置指定 VLAN 接口与 WAN 接口之间的安全规则，且必须配置双向规则，即出站方向和入站方向各一条。
  - 如果用户需要让指定终端能够访问其它 VLAN 下的终端，则需要配置指定本端 VLAN 接口与对端 VLAN 接口之间的安全规则，且必须配置双向规则。

本例防火墙的缺省规则设置为允许。

- 当一个接口上配置了多条防火墙的安全规则时，报文会按照规则的优先级（数值越小优先级越高）从高到低与这些规则进行匹配，一旦匹配上某条规则便结束匹配过程，并对此报文执行规则中的动作。

4.4 配置步骤

1. 划分 VLAN2，并配置接口 IP 地址

在路由器上划分 VLAN2，并配置接口 IP 地址为 192.168.2.1/24，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”，单击“VLAN 配置”页签，进入 VLAN 配置页面。

(2) 单击<添加>按钮，进入添加 VLAN 页面。

(3) 在“VLAN ID”配置项处，输入 2。

(4) 在“接口 IP 地址”配置项处，输入 192.168.2.1。

(5) 在“子网掩码”配置项处，输入 255.255.255.0。

(6) 勾选“开启 DHCP 服务”复选框，开启设备的 DHCP 服务。

(7) 其它配置项保持默认配置，单击<确定>按钮，完成配置。

图4-2 划分 VLAN2

2. 划分 VLAN3 并配置接口的 IP 地址。

在路由器上划分 VLAN3，并配置接口 IP 地址为 192.168.3.1/24，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”，单击“VLAN 配置”页签，进入 VLAN 配置页面。

(2) 单击<添加>按钮，进入添加 VLAN 页面。

(3) 在“VLAN ID”配置项处，输入 3。

(4) 在“接口 IP 地址”配置项处，输入 192.168.3.1。

(5) 在“子网掩码”配置项处，输入 255.255.255.0。

(6) 勾选“开启 DHCP 服务”复选框，开启设备的 DHCP 服务。

(7) 其它配置项保持默认配置，单击<确定>按钮，完成配置。

图4-3 划分 VLAN3

3. 将 LAN2 接口划分到 VLAN2

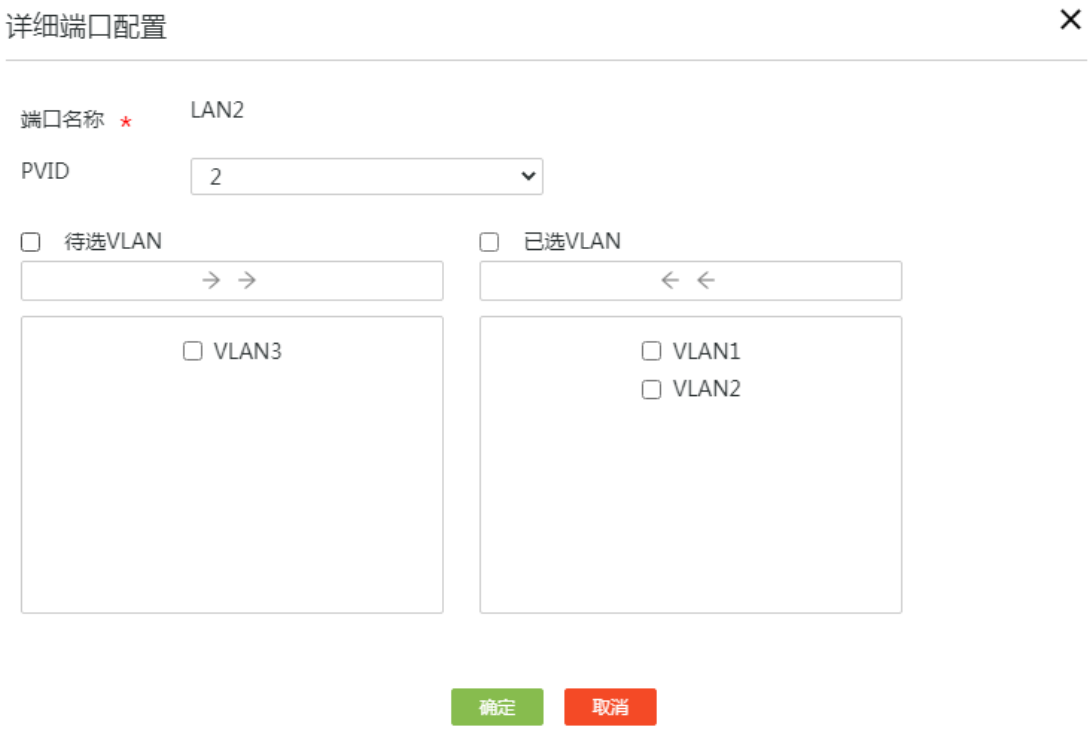
(1) 在设备 Web 管理界面导航栏中选择“网络设置>LAN 配置”，进入 VLAN 划分页面。

(2) 单击 LAN2 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<确定>按钮，完成配置。

图4-4 将 LAN2 接口划分到 VLAN2



4. 将 LAN3 接口划分到 VLAN3

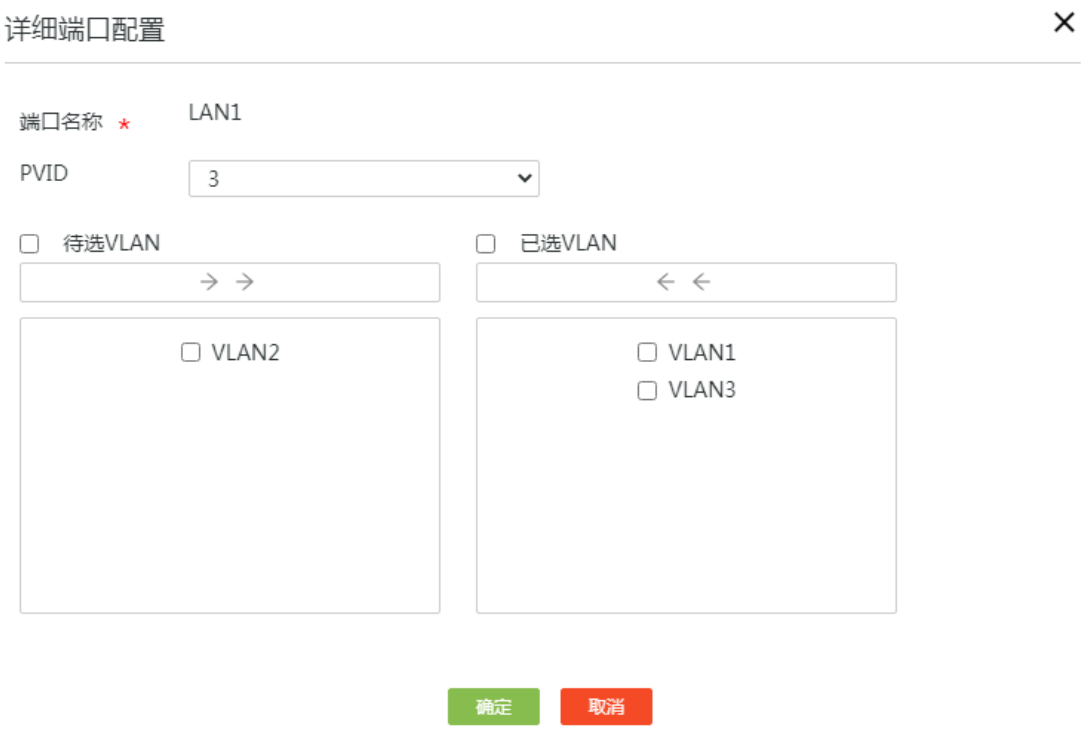
(1) 在设备 Web 管理界面导航栏中选择“网络设置>LAN 配置”，进入 VLAN 划分页面。

(2) 单击 LAN2 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4-5 将 LAN3 接口划分到 VLAN3



5. 配置地址组

将研发部所在子网（192.168.2.1/24）设置为名称为“研发部”的地址组，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 > 地址组”，进入地址组配置页面。

(2) 单击<添加>按钮，进入添加地址组配置页面。

(3) 在“地址组”名称配置项处，输入研发部。

(4) 在“IP 地址段”配置项处，起始框中输入 192.168.2.2，结束框中输入 192.168.2.254。

(5) 单击<→→>按钮，提交配置的地址组内容。

(6) 单击<确定>按钮，完成地址组创建。

图4-6 配置名称为研发部的地址组

参见“研发部”地址组的配置步骤，将财务部所在的子网（192.168.3.1/24）设置为名称为“财务部”的地址组。

参见“研发部”地址组的配置步骤，将服务器的 IP 地址（192.168.1.2）设置为名称为“服务器”的地址组。

6. 配置时间组

将工作时间段周一至周五 9:00~18:00 设置为名称为“工作时间”的时间组，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 > 时间组”，进入时间组配置页面。

(2) 单击<添加>按钮，进入新建时间组配置页面。

(3) 在“时间组名称”配置项处，输入工作时间。

(4) 在“生效时间”配置项处，选择周期性生效。

(5) 时间段设置为周一到周五 9:00~18:00。

(6) 单击<+>按钮，提交设置的生效时间段。

(7) 单击<确定>按钮完成配置。

图4-7 配置时间组

7. 开启防火墙功能并配置防火墙规则

开启防火墙功能后，为完成组网要求需创建如下 3 条规则：

- 不允许研发部的 PC 在任何时间访问服务器；
- 允许研发部的 PC 在工作时间访问服务器；
- 不允许财务部的 PC 在任何时间访问服务器。

配置步骤如下：

(1) 在设备 Web 管理界面导航栏中选择“网络安全 > 防火墙”，进入防火墙配置页面。

(2) 勾选“开启防火墙”选项，开启防火墙功能。

(3) 在“缺省过滤规则”配置项处，保持缺省配置为允许。

(4) 创建“不允许研发部的 PC 在任何时间访问服务器”规则：

a. 单击<添加>按钮，弹出创建安全规则对话框。

b. 在“接口”配置项处，选择研发部所在的 VLAN2。

c. 在“协议”配置项处，选择所有协议。

d. 在“源地址分组”配置项处，选择“研发部”地址组。

e. 在“目的地址分组”配置项处，选择“服务器”地址组。

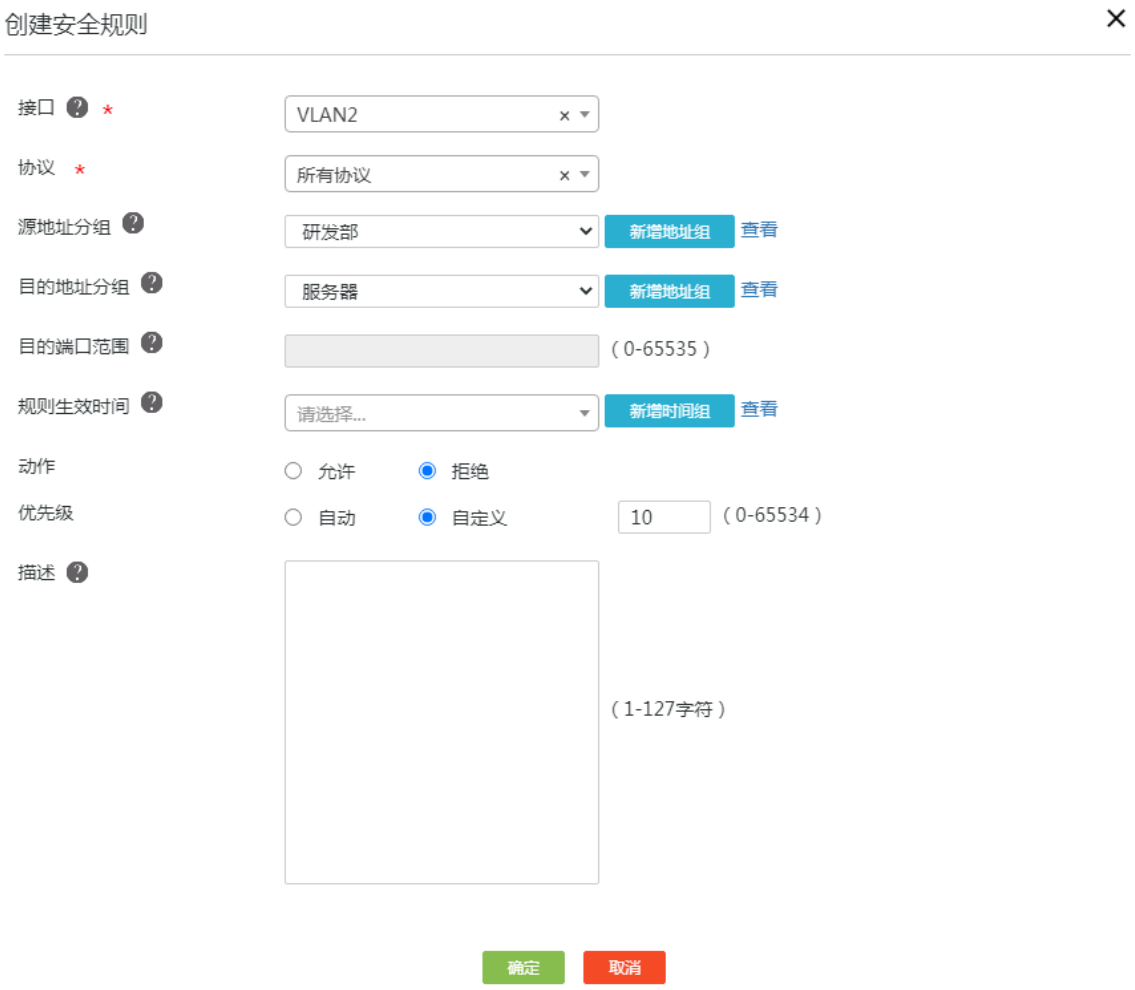
f. 在“规则生效时间”配置项处，保持缺省配置（表示所有时间段）。

g. 在“动作”配置项处，选择拒绝。

h. 在“优先级”配置项处，选择自定义，优先级配置为 10。

i. 单击<确定>按钮，完成配置。

图4-8 配置规则“不允许研发部在任何时间访问服务器”



(5) 创建“允许研发部的 PC 在工作时间访问服务器”规则：

a. 在防火墙配置页面，单击<添加>按钮，弹出创建安全规则对话框。

b. 在“接口”配置项处，选择研发部所在的 VLAN2。

c. 在“协议”配置项处，选择所有协议。

d. 在“源地址分组”配置项处，选择“研发部”地址组。

e. 在“目的地址分组”配置项处，选择“服务器”地址组。

f. 在“规则生效时间”配置项处，选择“工作时间”时间组。

g. 在“动作”配置项处，选择允许。

h. 在“优先级”配置项处，选择自定义，优先级配置为 5。（注意：需要比规则“不允许研发部 PC 在任何时间访问服务器”的优先级数值小）。

i. 单击<确定>按钮，完成配置。

图4-9 配置规则“允许研发部在工作时间访问服务器”

(6) 创建“不允许财务部的 PC 在任何时间访问服务器”规则：

a. 在防火墙配置页面，单击<添加>按钮，弹出创建安全规则对话框。

b. 在“接口”配置项处，选择财务部所在的 VLAN3。

c. 在“协议”配置项处，选择所有协议。

d. 在“源地址分组”配置项处，选择“财务部”地址组。

e. 在“目的地址分组”配置项处，选择“服务器”地址组。

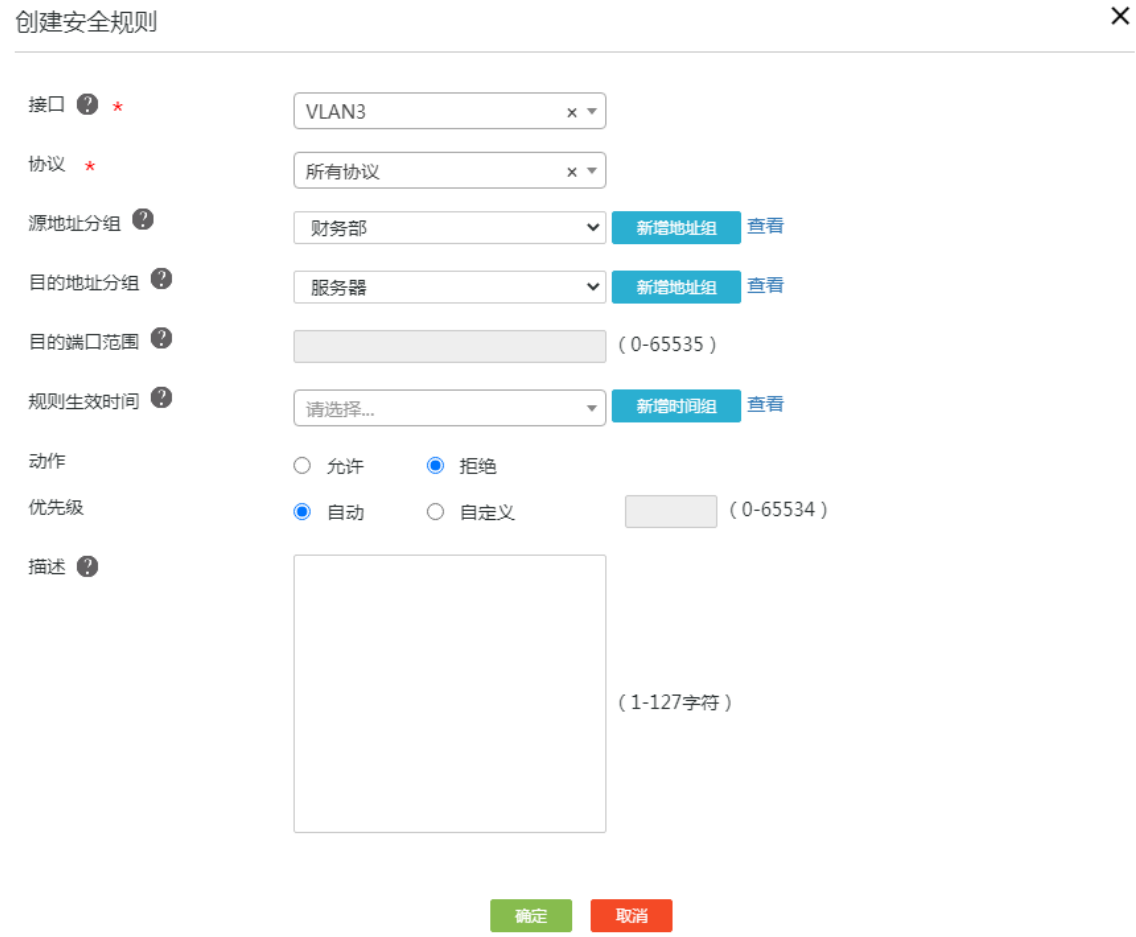
f. 在“规则生效时间”配置项处，保持缺省配置（表示所有时间段）。

g. 在“动作”配置项处，选择拒绝。

h. 在“优先级”配置项处，选择自动。

i. 单击<确定>按钮，完成配置。

图4-10 配置规则“不允许财务部的 PC 在任何时间访问服务器”



(7) 确认防火墙规则创建完成。

如图 4-11 所示，完成上述配置后，防火墙配置页面生成相应表项。

图4-11 防火墙规则表项

4.5 验证配置

(1) 在工作时间段内，用研发部 PC 去 ping 服务器 IP 地址，能够 ping 通。

```
C:\Users\abc>ping 192.168.1.2
Ping 192.168.1.2 (192.168.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.1.2: icmp_seq=0 ttl=254 time=0.320 ms
56 bytes from 192.168.1.2: icmp_seq=1 ttl=254 time=0.213 ms
56 bytes from 192.168.1.2: icmp_seq=2 ttl=254 time=0.194 ms
56 bytes from 192.168.1.2: icmp_seq=3 ttl=254 time=0.160 ms
56 bytes from 192.168.1.2: icmp_seq=4 ttl=254 time=0.187 ms

--- Ping statistics for 192.168.1.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.160/0.215/0.320/0.055 ms
```

(2) 在任何时间段内，用财务部 PC 去 ping 服务器 IP 地址，ping 不通。

```
C:\Users\abc>ping 192.168.1.2
Ping 192.168.1.2 (192.168.1.2): 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out
```

通过上述验证说明防火墙配置成功。

H3C ER G3 系列路由器

策略路由典型配置举例

新华三技术有限公司
http://www.h3c.com

资料版本：6W102-20221021

1.1 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 ER G3 系列路由器-策略路由 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. 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。

2. 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。

3. 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。

4. 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！

目 录

1 简介

本文档介绍路由器策略路由的配置方法。

当网络管理员需要在某个时间段将局域网指定的主机的上网流量从指定的 WAN 口发送出去时，可以通过配置策略路由来实现。

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策略路由特性。

3 使用版本

本配置举例是在 ER3200G3 路由器 Release 0114 版本上进行配置和验证的。

4 配置举例

4.1 组网需求

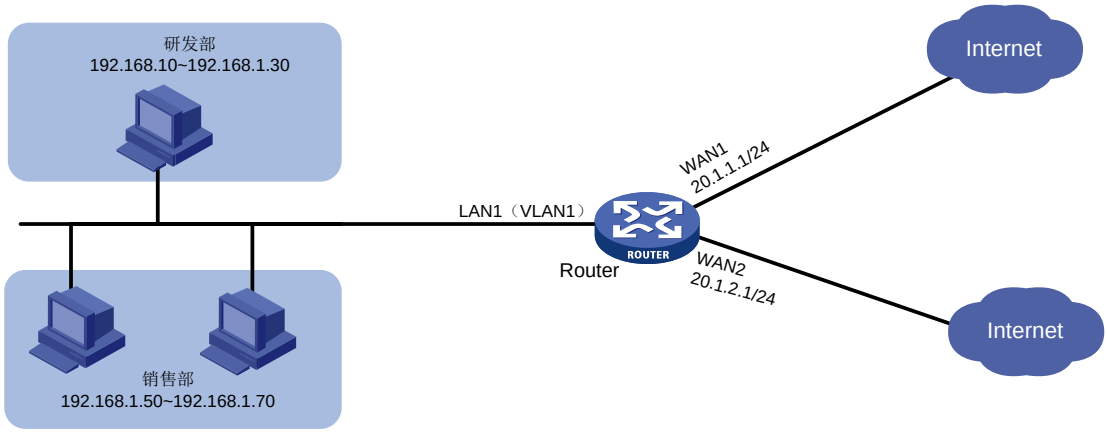
如图 4-1 所示，Router 为某企业的出口网关，通过 WAN1 和 WAN2 接口连接 Internet，WAN1 和 WAN2 接口的连接模式都为固定地址，其中 WAN1 接口的 IP 地址为 20.1.1.1/24，网关地址为 20.1.1.254。

WAN2 接口的 IP 地址为 20.1.2.1/24，网关地址为 20.1.2.254。

现企业为实现在工作时间段内（周一至周五 8:30-18:00）进行业务分流，需要在 Router 上进行如下配置：

- 研发部所有员工 PC 上网流量走 WAN1 接口发送出去。
- 销售部所有员工 PC 上网流量走 WAN2 接口发送出去。

图4-1 策略路由典型配置组网图



4.2 配置注意事项

配置策略路由的策略时，优先级若选择“自动”，策略路由就会按照配置顺序生效，即先配置的策略路由的优先级高于后配置的策略路由优先级；若选择“自定义”，则配置的数值越小优先级越高。

4.3 配置步骤

4.3.1 配置 Router 上网

本例 Router 外网的接口模式选择双 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“配置接口模式”页签下选择双 WAN 模式，单击<应用>按钮使得配置生效。

图4-2 配置 WAN 场景

(3) 单击“WAN 配置”页签，进入 WAN 配置页面。

(4) 单击 WAN1 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。

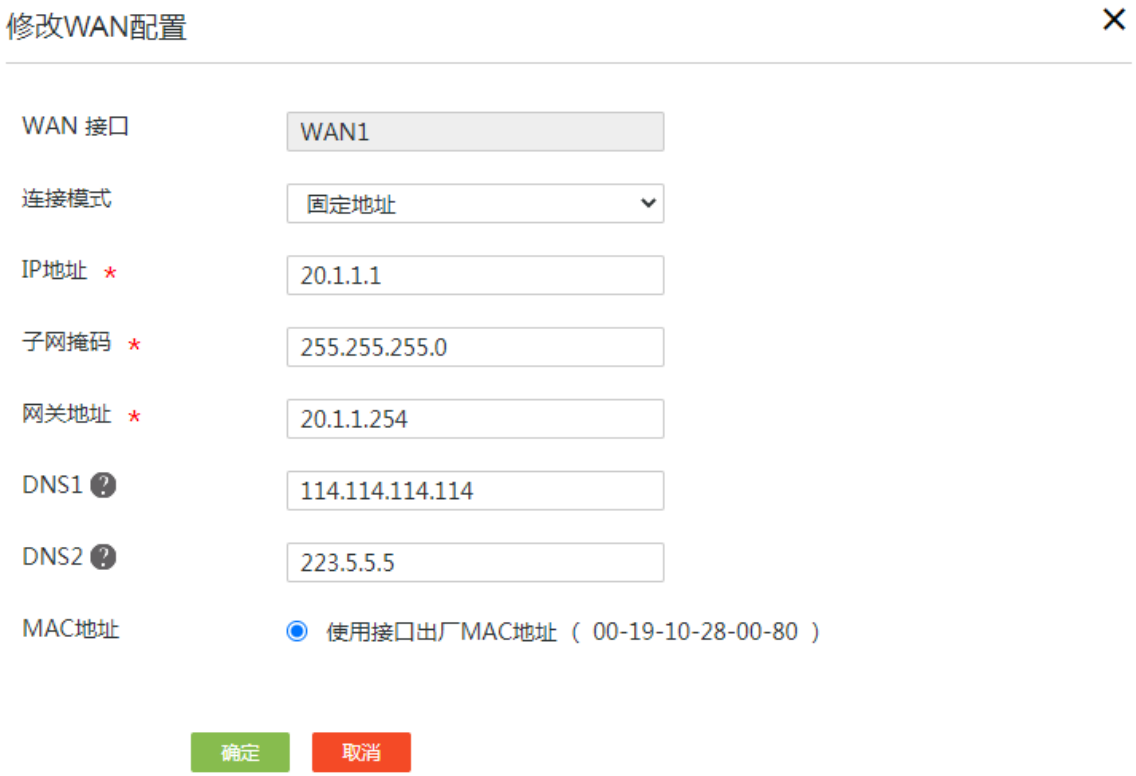
(6) 在“IP 地址”配置项处，输入 20.1.1.1。

(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 20.1.1.254。

(9) 其它参数保持默认配置即可，单击<确定>按钮保存配置

图4-3 配置 WAN1 接口连接 Internet



(10) 单击 WAN2 接口对应操作列编辑图标，进入修改 WAN 配置页面。

(11) 在“连接模式”配置项处，选择固定地址。

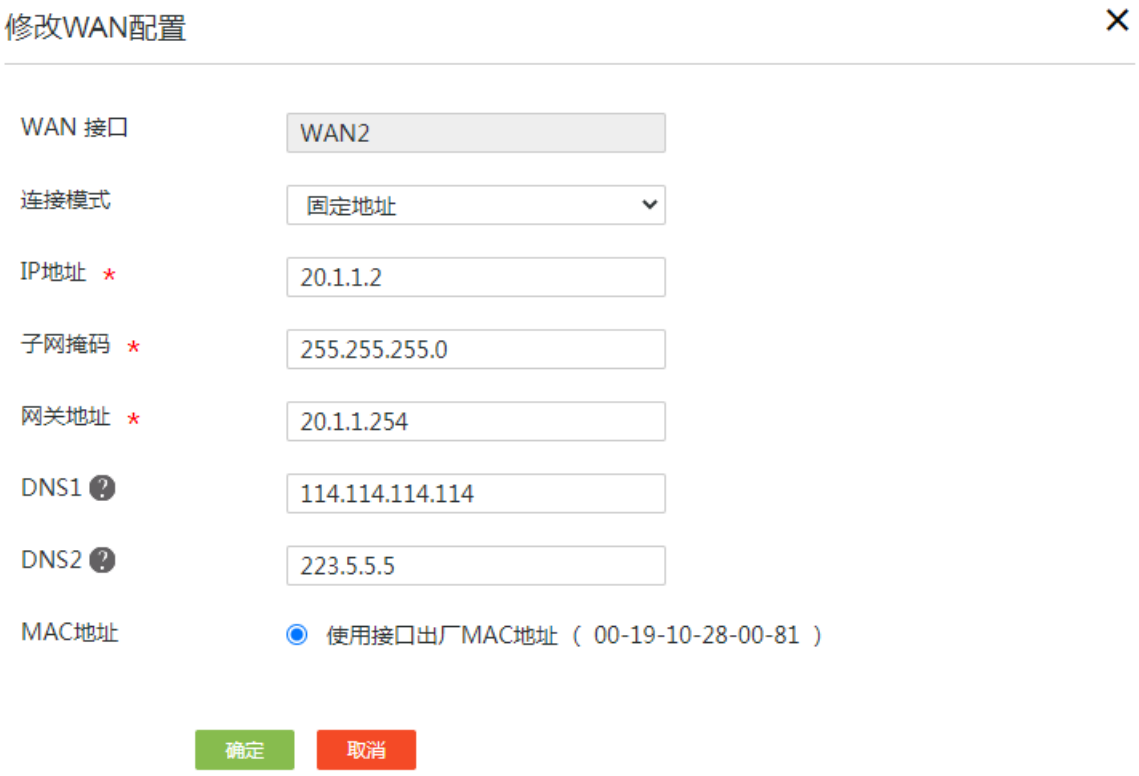
(12) 在“IP 地址”配置项处，输入 20.1.2.1。

(13) 在“子网掩码”配置项处，输入 255.255.255.0。

(14) 在“网关地址”配置项处，输入 20.1.2.254。

(15) 其它参数保持默认配置即可，单击<确定>按钮保存配置

图4-4 配置 WAN2 接口连接 Internet



4.3.2 配置时间组

将本例中工作时间段（周一至周五 8:30-18:00）设置为一个时间组，方便在添加策略路由时引用。配置步骤如下：

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

(2) 单击<添加>按钮，进入新建时间组配置页面。

(3) 在“时间组名称”配置项处，输入 time。

(4) 在“生效时间”配置项处，选择周期性生效，并在下面设置具体的时间段为周一至周五 8：30-18:00。

(5) 单击<＋>按钮，完成时间段的配置。

(6) 单击<确定>按钮保存配置。

图4-5 新建时间组

4.3.3 配置策略路由

1. 配置研发部策略路由

(1) 在设备 Web 管理界面导航中 选择“高级选项 > 策略路由”，进入策略路由配置页面。

(2) 单击<添加>按钮，进入新增策略路由列表。

(3) 在“接口”配置项处，选择 VLAN1。

(4) 在“协议类型”配置项处，选择 IP。

(5) 在“源 IP 地址段”配置项处，输入 192.168.1.10-192.168.1.30。

(6) 在“目的 IP 地址段”配置项处，输入 0.0.0.0-255.255.255.0（所有地址）。

(7) 在“生效时间”配置项处，time。

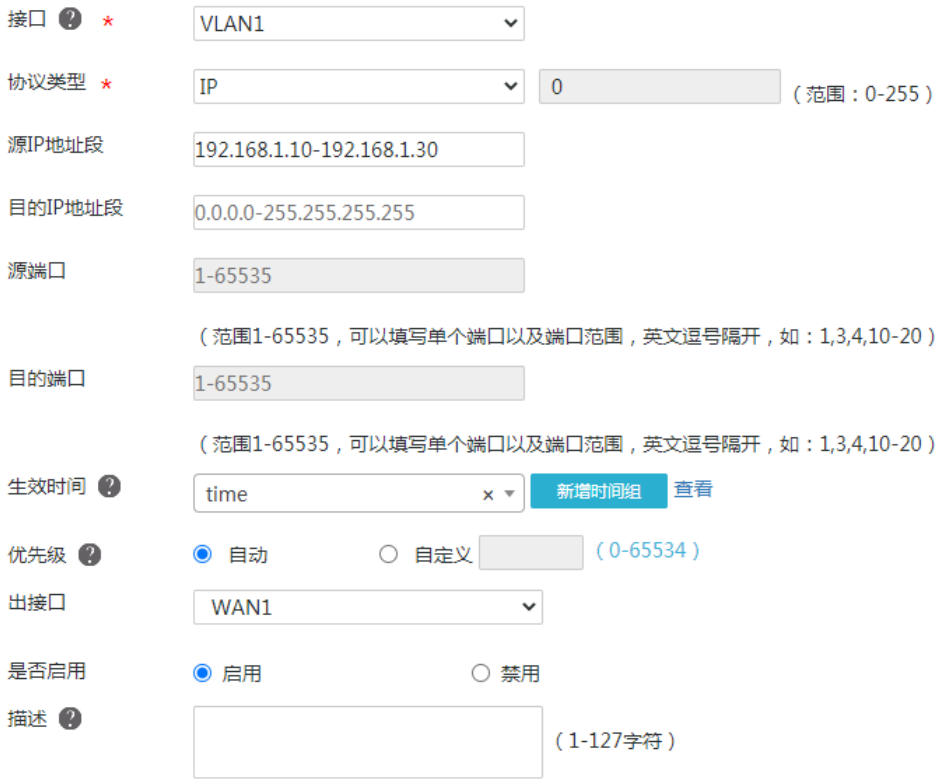
(8) 在“优先级”配置项处，选择自动。

(9) 在“出接口”配置项处，选择 WAN1。

(10) 在“是否启用”配置项处，勾选“启用”前方单选框，启用策略路由功能。

(11) 其它参数保持默认即可，单击<确定>按钮，完成配置。

图4-6 配置研发部策略路由



2. 配置销售部策略路由

(1) 在设备 Web 管理界面导航中 选择“高级选项 > 策略路由”，进入策略路由配置页面。

(2) 单击<添加>按钮，进入新增策略路由列表。

(3) 在“接口”配置项处，选择 VLAN1。

(4) 在“协议类型”配置项处，选择 IP。

(5) 在“源 IP 地址段”配置项处，输入 192.168.1.50-192.168.1.70。

(6) 在“目的 IP 地址段”配置项处，输入 0.0.0.0-255.255.255.0（所有地址）。

(7) 在“生效时间”配置项处，time。

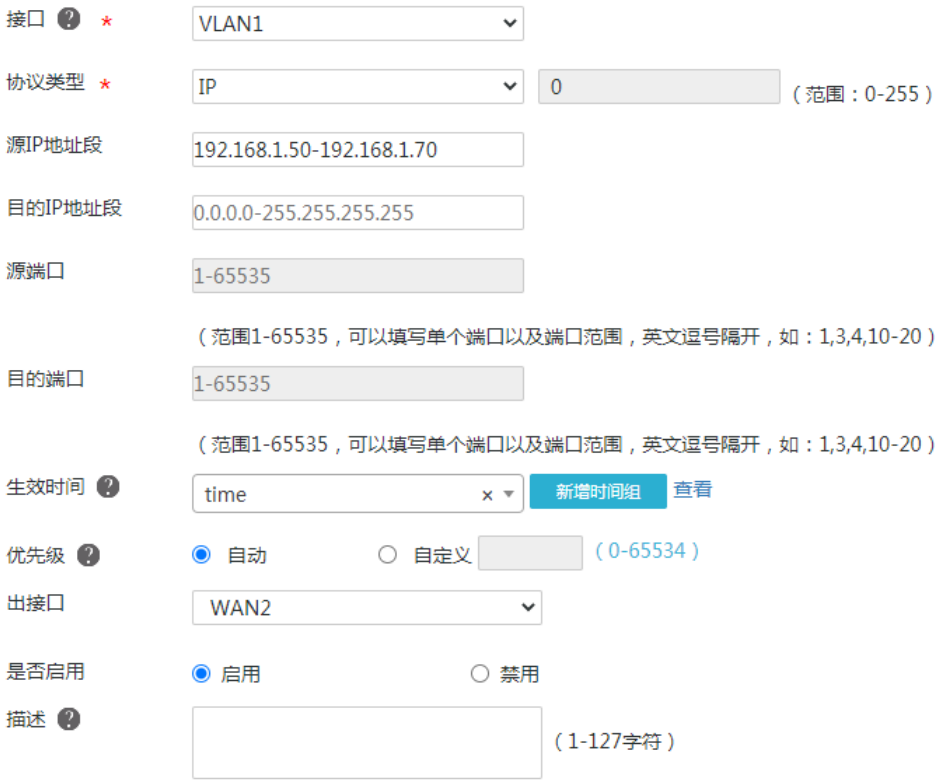
(8) 在“优先级”配置项处，选择自动。

(9) 在“出接口”配置项处，选择 WAN2。

(10) 在“是否启用”配置项处，勾选“启用”前方单选框，启用策略路由功能。

(11) 其它参数保持默认即可，单击<确定>按钮，完成配置。

图4-7 配置研发部策略路由



4.4 验证配置

(1) 登录研发部员工 PC 界面，tracert 目标 IP 地址 200.1.1.1，查看路由路径：

```
C:\Users\abc>tracert 200.1.1.1

通过最多 30 个跃点跟踪到 200.1.1.1 的路由
1        <1 毫秒      1ms     1ms    erlogin.cn[192.168.1.1]
2        <1 毫秒      <1 毫秒     <1 20.1.1.254
3        <1 毫秒      <1 毫秒     <1 200.1.1.1

跟踪完成。
```

(2) 登录销售部员工 PC 界面，tracert 目标 IP 地址 200.1.1.1，查看路由路径：

```
C:\Users\cbd>tracert 200.1.1.1

通过最多 30 个跃点跟踪到 200.1.1.1 的路由
1        <1 毫秒      1ms     1ms    erlogin.cn[192.168.1.1]
2        <1 毫秒      <1 毫秒     <1 20.1.2.254
3        <1 毫秒      <1 毫秒     <1 200.1.1.1

跟踪完成。
```

由路由路径可知，研发部 PC 访问外网时路由的下一跳为 WAN1 口网关，销售部 PC 访问外网时路由的下一跳为 WAN2 口网关，策略路由配置成功。

H3C ER G3 系列路由器

应用控制典型配置举例

新华三技术有限公司
http://www.h3c.com

资料版本：6W102-20221021

1.1 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 ER G3 系列路由器-应用控制 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. 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。

2. 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。

3. 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。

4. 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！

目 录

1 简介

本文档介绍路由器上网行为管理-应用控制的配置方法。

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上网行为管理-应用控制特性。

3 使用版本

本举例是在 ER3200G3 路由器的 Release 0123 版本上进行配置和验证的。

4 配置举例

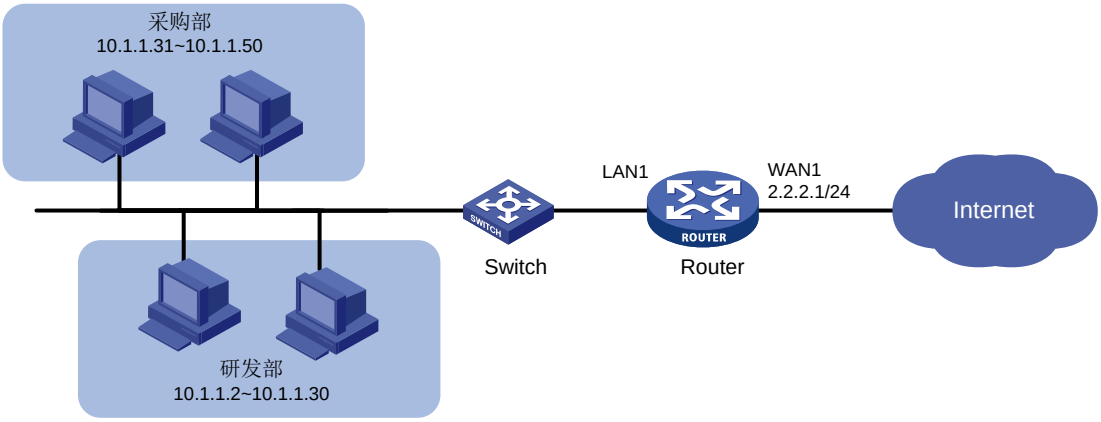
4.1 组网需求

如图 4-1 所示，Router 为企业的出口网关，通过 WAN1 接口连接 Internet，WAN1 接口连接模式为固定地址，IP 地址为 2.2.2.1/24，网关地址为 2.2.2.254，DNS1 服务器地址为 114.114.114.114，DNS2 服务器地址为 223.5.5.5。企业内部各部门 PC 通过 Switch 连接到 Router 的 LAN1 接口，LAN1 接口属于 VLAN1，VLAN1 的接口 IP 地址为 10.1.1.1/24。

WAN1 接口的上行带宽为 100M，下行带宽为 200M，企业为确保公司各部门业务稳定运行，需配置如下策略：

- 禁止研发部上班时间段使用迅雷软件。
- 对采购部上班时间段（周一至周五 9:00-18:00）内访问淘宝的流量进行限速，上行 100kbps，下行 200kbps。

图4-1 上网行为管理-应用控制配置组网图



4.2 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。

4.3 配置步骤

4.3.1 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“VLAN 配置”页签，进入 VLAN 配置页面。

(3) 单击 VLAN1 对应的操作列编辑图标，进入修改 VLAN 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4-2 修改 VLAN 配置

4.3.2 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“配置接口模式”页签下选择单 WAN 模式，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) 在“网络上行带宽”配置项处，输入 100。

(10) 在“网络下行带宽”配置项处，输入 200。

(11) 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4-3 配置 WAN 场景

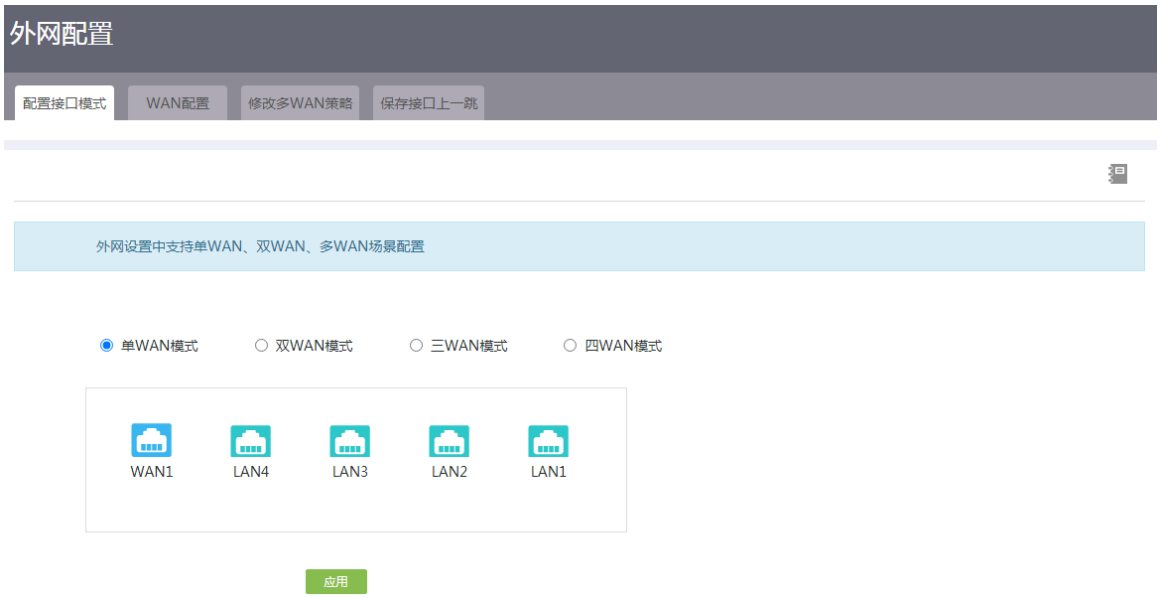


图4-4 修改 WAN 配置


修改WAN配置
WAN 接口
WAN1
连接模式
固定地址
IP地址 *
2.2.2.1
子网掩码 *
255.255.255.0
网关地址 *
2.2.2.254
DNS1
114.114.114.114
DNS2
223.5.5.5
MAC地址
使用接口出厂MAC地址（ 00-19-10-28-00-80 ）
使用静态指定的MAC
网络上行带宽
100
（Mbps）
网络下行带宽
200
（Mbps）
NAT地址转换
启用
使用地址池转换
新增地址池
TCP MSS
1280
（128-1610字节，默认：1280字节）
MTU
1500
（576-1650字节）
链路探测
未启用
探测地址
探测间隔
（1-10秒）
探测次数
（默认3次）
确定
取消

4.3.3 配置地址组

1. 配置研发部员工 PC 的地址组

将研发部门员工 PC 的 IP 地址段设置为名称为“研发部”的地址组。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 > 地址组”，进入地址组配置页面。

(2) 单击<添加>按钮，进入添加地址组配置页面。

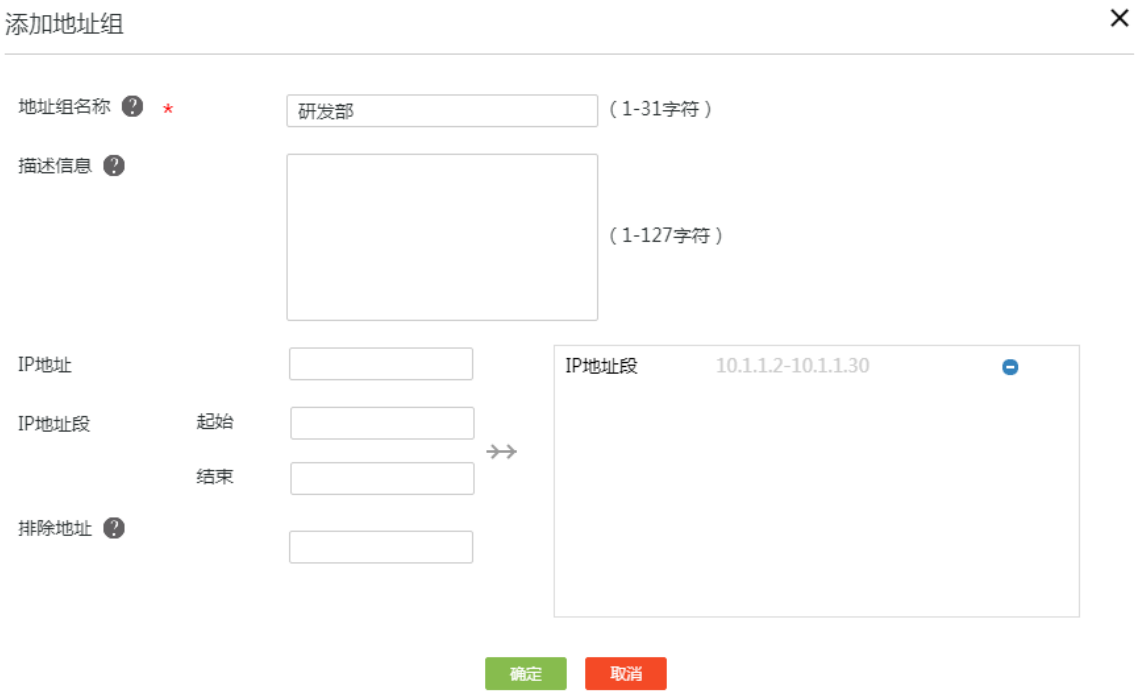
(3) 在“地址组名称”配置项处，输入研发部。

(4) 在“IP 地址段”配置项处，起始框输入 10.1.1.2，结束框输入 10.1.1.30。

(5) 点击配置项右侧的<→→>按钮，提交配置的地址组内容。

(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4-5 配置研发部地址组



2. 配置采购部员工 PC 的地址组

将采购部员工 PC 的 IP 地址段设置为名称为“采购部”的地址组。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 > 地址组”，进入地址组配置页面。

(2) 单击<添加>按钮，进入添加地址组配置页面。

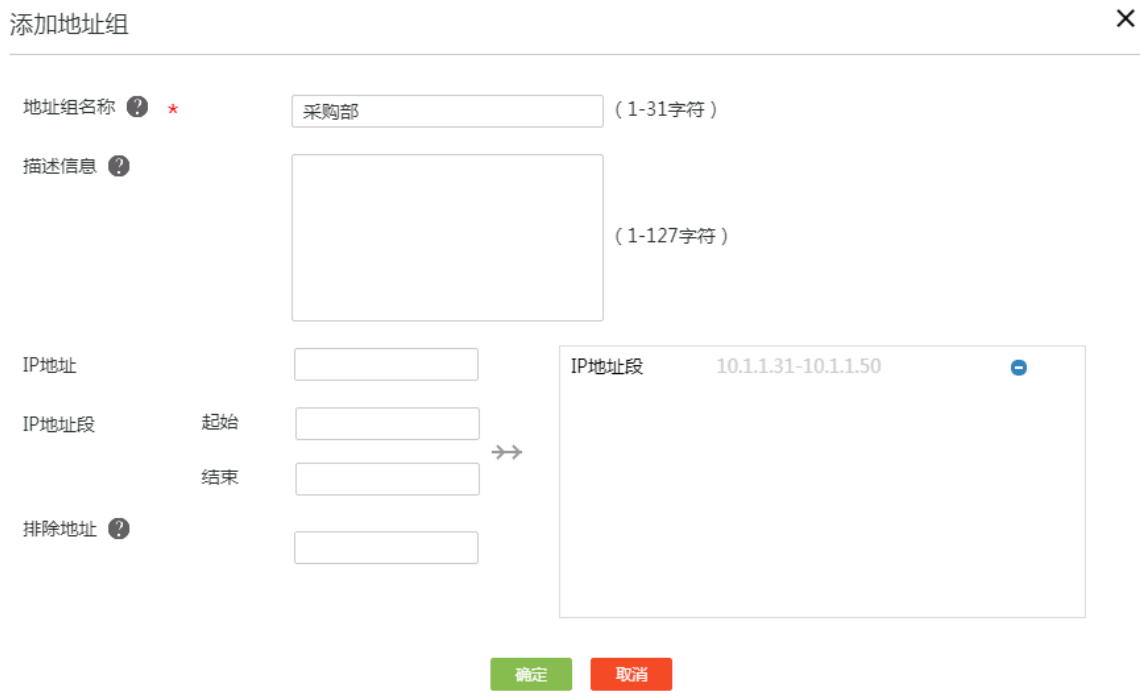
(3) 在“地址组名称”配置项处，输入采购部。

(4) 在“IP 地址段”配置项处，起始框输入 10.1.1.31，结束框输入 10.1.1.50。

(5) 点击配置项右侧的<→→>按钮，提交配置的地址组内容。

(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4-6 配置采购部地址组



4.3.4 配置时间组

将上班时间段设置为名称为“上班时间”的时间组。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 > 时间组”，进入时间组配置页面。

(2) 单击<添加>按钮，进入新建时间组配置页面。

(3) 在“时间组名称”配置项处，输入上班时间。

(4) 在“生效时间”配置项处，选择周期性生效，并设置具体的时间段为周一至周五 9:00-18:00，单击<+>按钮，提交配置的时间段。

(5) 单击<确定>按钮保存配置。

图4-7 新建时间组

4.3.5 配置应用控制策略

1. 禁止研发部使用迅雷软件

(1) 在设备 Web 管理界面导航栏中选择“上网行为管理 > 上网行为管理”，进入上网行为管理配置页面。

(2) 单击“应用控制”页签，进入应用控制配置页面。

(3) 勾选“开启应用控制”，单击<确定>按钮，开启应用控制功能。

(4) 单击“添加”按钮，进入应用控制配置页面。

(5) 在“策略名称”配置项处，输入 policy1。

(6) 在“用户范围”配置项处，选择现有分组研发部。

(7) 在“限制时段”配置项处，选择现有时间组上班时间。

(8) 在“应用控制”配置项处，单击选择网络应用行的详情按钮，进入选择网络应用配置页面。

(9) 单击 P2P 选项前方的<+>按钮，弹出具体的 P2P 应用选项。

(10) 勾选迅雷所在行的“阻断”选项。

(11) 单击<确定>按钮返回应用控制配置页面。

(12) 单击<确定>按钮保存配置。

图4-8 配置应用控制

图4-9 选择网络应用

2. 对采购部使用淘宝软件进行限速

(1) 在设备 Web 管理界面导航栏中选择“上网行为管理 > 上网行为管理”，进入上网行为管理配置页面。

(2) 单击“应用控制”页签，进入应用控制配置页面。

(3) 勾选“开启应用控制”，单击<确定>按钮，开启应用控制功能。

(4) 单击“添加”按钮，进入应用控制配置页面。

(5) 在“策略名称”配置项处，输入 policy2。

(6) 在“用户范围”配置项处，选择现有分组采购部。

(7) 在“限制时段”配置项处，选择现有时间组上班时间。

(8) 在“应用控制”配置项处，单击选择网络应用行的详情按钮，进入选择网络应用配置页面。

(9) 单击“购物”选项前方的<+>按钮，弹出具体的应用选项。

(10) 勾选淘宝（PC）所在行的“限速”选项，在上行带宽输入框中输入 100，在下行带宽输入框中输入 200。

(11) 单击<确定>按钮返回应用控制配置页面。

(12) 单击<确定>按钮保存配置。

图4-10 配置应用控制

图4-11 选择网络应用

4.4 验证配置

上班时间段内，研发部员工 PC 无法使用迅雷软件，采购部员工 PC 访问淘宝的流量受限，说明配置验证成功。

H3C ER G3 系列路由器

网址控制典型配置举例

新华三技术有限公司
http://www.h3c.com

资料版本：6W102-20221021

1.1 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 ER G3 系列路由器-网址控制 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. 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。

2. 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。

3. 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。

4. 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！

目 录

1 简介

本文档分别介绍路由器通过网址黑名单和网址白名单的方式进行网址控制的配置方法。

- 网址黑名单：开启该功能，设备会禁止指定的用户在指定的时间段内访问自定义网址分类中指定的网址；对于不在网址分类中的网址，则可以正常访问。
- 网址白名单：开启该功能，设备只允许指定的用户在指定的时间段内访问自定义网址分类中指定的网址；对于不在网址分类中的网址，则无法访问。

请根据您的实际需求，参考黑名单配置举例或白名单配置举例进行配置。

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上网行为管理-网址控制的特性。

3 使用版本

本举例是在 ER3200G3 路由器的 Release 0123 版本上进行配置和验证的。

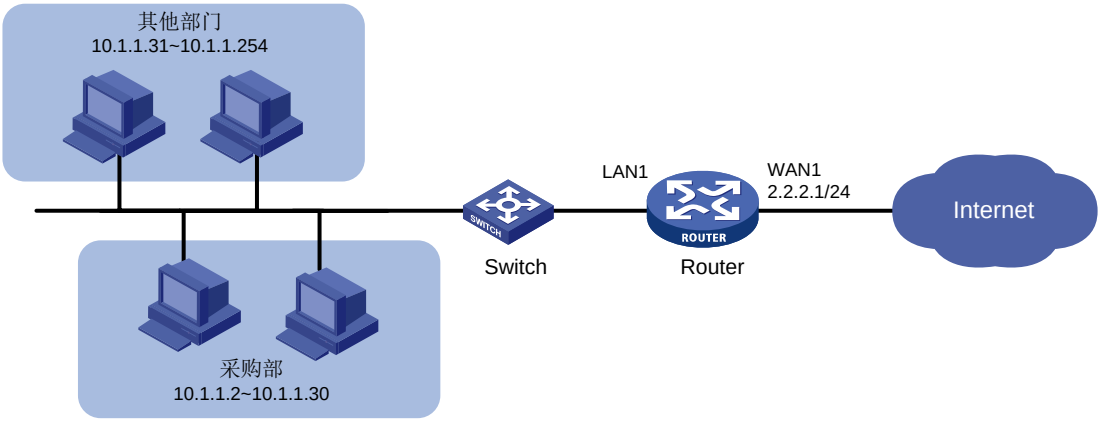
4 白名单配置举例

4.1 组网需求

如图 4-1 所示，Router 为企业的出口网关，通过 WAN1 接口连接 Internet，WAN1 接口连接模式为固定地址，IP 地址为 2.2.2.1/24，网关地址为 2.2.2.254，DNS1 服务器地址为 114.114.114.114，DNS2 服务器地址为 223.5.5.5。企业内部各部门 PC 通过 Switch 连接到 Router 的 LAN1 接口，LAN1 接口属于 VLAN1，VLAN1 的接口 IP 地址为 10.1.1.1/24。

现出于业务需求，企业要求采购部的 PC 在上班时间段（周一至周五 9:00-18:00）仅可以访问淘宝网，其他部门 PC 在上班时间段访问任何网址不受限制。

图4-1 网址白名单典型配置组网图



4.2 配置思路

需要开启网址白名单功能，并配置以下两条白名单策略来达到需求：

- 允许采购部 PC 在上班时间段内访问淘宝网。
- 允许其他部分 PC 在上班时间段内访问任何网址。

4.3 配置注意事项

- 开启网址白名单功能后，报文的匹配规则举例如下：

网址白名单名称	网址分类名称	地址组名称
白名单A	网址组A	用户组A
白名单B	网址组B	用户组B

  - 如果用户 User1 同时属于用户组 A 和用户组 B，则用户 User1 只允许访问网址组 A 和网址组 B 中的网址；
  - 如果用户 User2 仅属于用户组 A，则用户 User2 只允许访问网址组 A 中的网址；
  - 如果用户 User3 既不属于用户组 A 也不属于用户组 B，则用户 User3 不允许访问任何网址。
- 配置网址关键字时：
  - 若需匹配所有网址配置，可将网址关键字设置为“.”，即英文句号。
  - 若设置的网址关键字不加通配符*时，网址控制策略将根据关键字做精确匹配，例如 www.baidu.com；关键字添加通配符*时，网址控制策略将根据关键字做模糊匹配，例如 *.baidu.com、www.baidu*或*baidu*。
- 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。

4.4 配置步骤

4.4.1 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“VLAN 配置”页签，进入 VLAN 配置页面。

(3) 单击 VLAN1 对应的操作列编辑图标，进入修改 VLAN 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4-2 修改 VLAN 配置

4.4.2 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“配置接口模式”页签下选择单 WAN 模式，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4-3 配置 WAN 场景

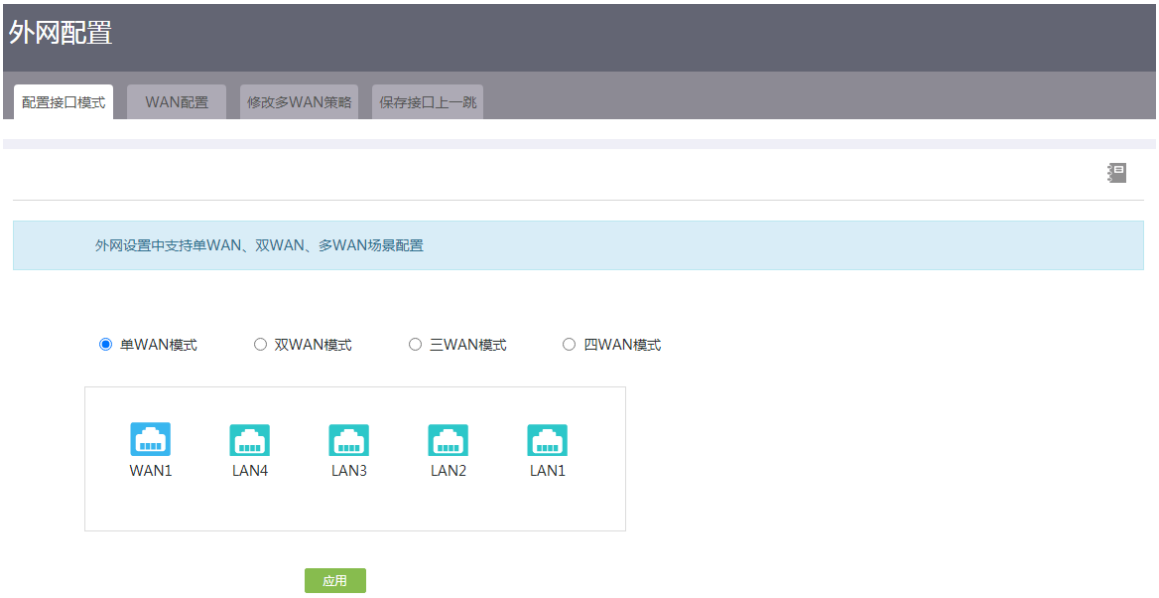


图4-4 修改 WAN 配置


修改WAN配置
WAN 接口
WAN1
连接模式
固定地址
IP地址 *
2.2.2.1
子网掩码 *
255.255.255.0
网关地址 *
2.2.2.254
DNS1
114.114.114.114
DNS2
223.5.5.5
MAC地址
使用接口出厂MAC地址（ 00-19-10-28-00-80 ）
使用静态指定的MAC
网络上行带宽
（Mbps）
网络下行带宽
（Mbps）
NAT地址转换
启用
使用地址池转换
新增地址池
TCP MSS
1280
（128-1610字节，默认：1280字节）
MTU
1500
（576-1650字节）
链路探测
未启用
探测地址
探测间隔
（1-10秒）
探测次数
（默认3次）
确定
取消

4.4.3 配置地址组

1. 配置采购部员工 PC 的地址组

将采购部门员工 PC 的 IP 地址段设置为名称为“采购部”的地址组。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 > 地址组”，进入地址组配置页面。

(2) 单击“添加”按钮，进入添加地址组配置页面。

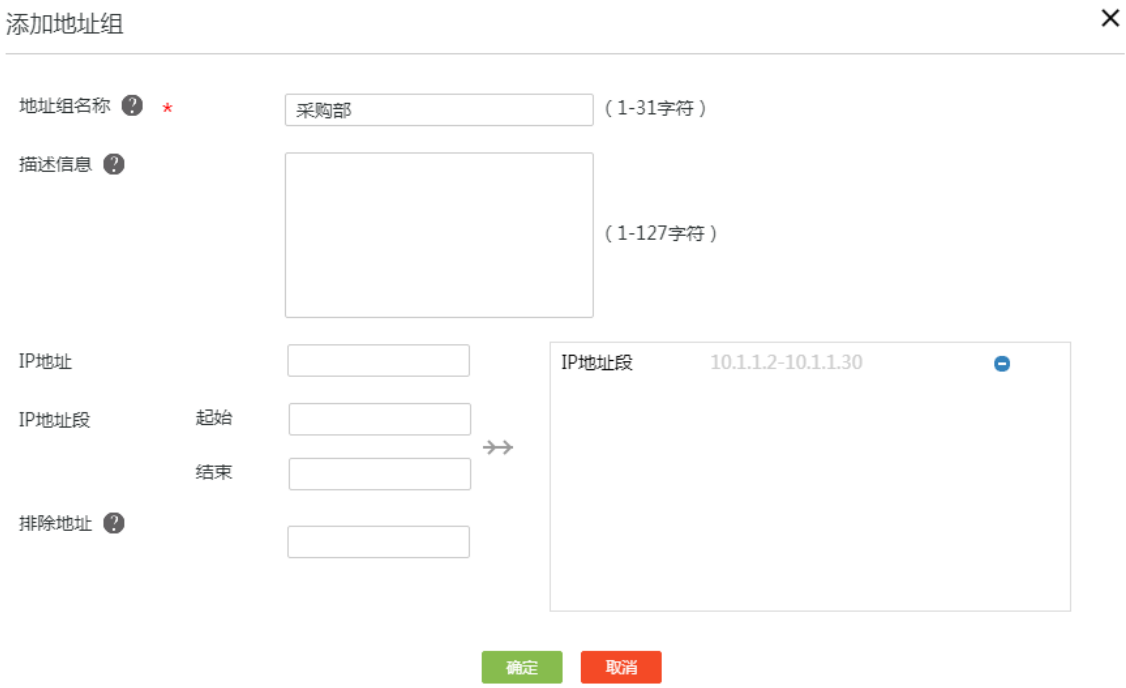
(3) 在“地址组名称”配置项处，输入采购部。

(4) 在“IP 地址段”配置项处，起始框输入 10.1.1.2，结束框输入 10.1.1.30。

(5) 点击配置项右侧的<→→>按钮，提交配置的地址组内容。

(6) 其它配置项均保持缺省配置即可，单击<确定>按钮保存配置。

图4-5 配置采购部地址组



2. 配置其他部门 PC 的地址组

将其他部门员工 PC 的 IP 地址段设置为名称为“其他部门”的地址组。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 > 地址组”，进入地址组配置页面。

(2) 单击<添加>按钮，进入添加地址组配置页面。

(3) 在“地址组名称”配置项处，输入其他部门。

(4) 在“IP 地址段”配置项处，起始框输入 10.1.1.31，结束框输入 10.1.1.254。

(5) 点击配置项右侧的<→→>按钮，提交配置的地址组内容。

(6) 其它配置项均保持缺省配置即可，单击<确定>按钮保存配置。

图4-6 配置其他部门地址组

4.4.4 配置时间组

将上班时间段设置为名称为“上班时间”的时间组。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 > 时间组”，进入时间组配置页面。

(2) 单击<添加>按钮，进入新建时间组配置页面。

(3) 在“时间组名称”配置项处，输入上班时间。

(4) 在“生效时间”配置项处，选择周期性生效，并设置具体的时间段为周一至周五 9:00-18:00，单击<+>按钮，提交配置的时间段。

(5) 单击<确定>按钮保存配置。

图4-7 新建时间组

4.4.5 配置网址白名单策略

1. 设置采购部上班时间段允许访问淘宝网

(1) 在设备 Web 管理界面导航栏中选择“上网行为管理 > 上网行为管理”，进入上网行为管理配置页面。

(2) 单击“网址控制”页签，进入网址控制配置页面。

(3) 勾选“网址白名单模式”，单击<确定>按钮，开启网址白名单功能。

(4) 在“网址分类”列对应的配置项处，输入新建网址控制策略的网址分类名称“policy1”。

(5) 在“地址组”列对应的配置项处，选择“采购部”地址组。

(6) 在“时间组”列对应的配置项处，选择“上班时间”时间组。

(7) 单击右侧<+>按钮，名称为“policy1”的网址分类成功。

(8) 单击“policy1”网址分类操作列对应的详情图标，进入设置网址关键字页面。

(9) 在“网址关键字”输入框中输入淘宝网关键字“*taobao*”。

(10) 单击右侧<+>按钮，提交网址关键字。

(11) 单击<确定>按钮，完成网址关键字添加。

图4-8 配置网址控制

图4-9 设置网址关键字

2. 设置其他部门 PC 上班时间段允许访问所有网址

(1) 在“网址分类”列对应的配置项处，输入新建网址控制策略的网址分类名称“policy2”。

(2) 在“地址组”列对应的配置项处，选择“其他部门”地址组。

(3) 在“时间组”列对应的配置项处，选择“上班时间”时间组。

(4) 单击右侧<+>按钮，名称为“policy2”的网址分类成功。

(5) 单击“policy2”网址分类操作列对应的详情图标，进入设置网址关键字页面。

(6) 在“网址关键字”输入框中输入关键字“.”（表示所有网址）。

(7) 单击右侧<+>按钮，提交网址关键字。

(8) 单击<确定>按钮，完成添加网址关键字。

图4-10 配置网址控制

图4-11 设置网址关键字

4.5 验证配置

上班时间段内，使用采购部员工 PC 可以正常打开淘宝网，其它网页无法打开，其他部门 PC 可以正常访问任何网址，说明配置验证成功。

图4-12 淘宝网页面

图4-13 百度网页面

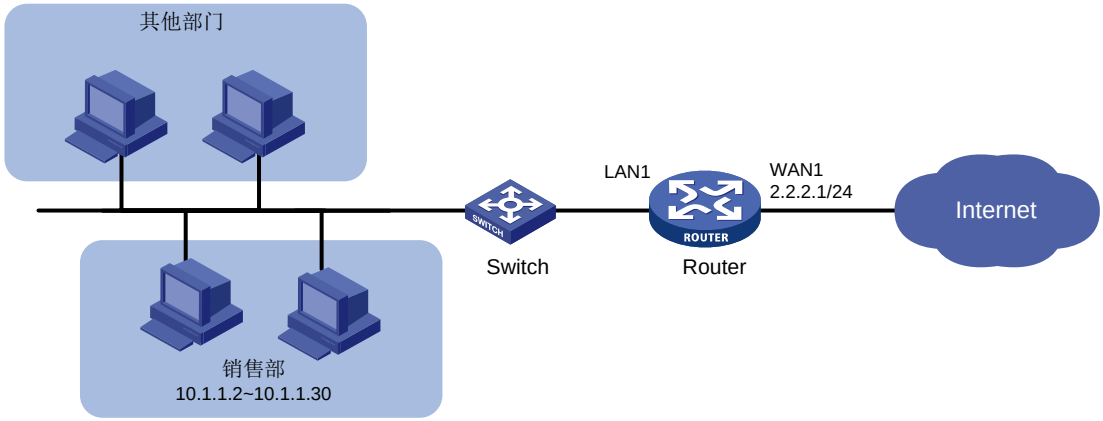
5 黑名单配置举例

5.1 组网需求

如图 5-1 所示，Router 为企业的出口网关，通过 WAN1 接口连接 Internet，WAN1 接口连接模式为固定地址，IP 地址为 2.2.2.1/24，网关地址为 2.2.2.254，DNS1 服务器地址为 114.114.114.114，DNS2 服务器地址为 223.5.5.5。企业内部各部门 PC 通过 Switch 连接到 Router 的 LAN1 接口，LAN1 接口属于 VLAN1，VLAN1 的接口 IP 地址为 10.1.1.1/24。

现出于业务需求，需禁止销售部的 PC 在上班时间段（周一至周五 9:00-18:00）访问优酷网，其他部门 PC 在上班时间段访问任何网址不受限制。

图5-1 网址黑名单典型配置组网图



5.2 配置思路

需要启用网址黑名单功能，并配置一条禁止销售部 PC 在上班时间内访问优酷网的策略来达到需求。

5.3 配置注意事项

- 开启网址黑名单功能后，报文的匹配规则举例如下：

网址黑名单名称	网址分类名称	地址组名称
黑名单A	网址组A	用户组A

  - 如果用户 User1 属于用户组 A，则用户 User1 不允许访问网址组 A 中的网址；
  - 如果用户 User2 不属于用户组 A，则用户 User2 允许访问任何网址。
- 配置网址关键字时：
  - 若需匹配所有网址配置，可将网址关键字设置为“.”，即英文句号。
  - 若设置的网址关键字不加通配符*时，网址控制策略将根据关键字做精确匹配，例如 www.baidu.com；关键字添加通配符*时，网址控制策略将根据关键字做模糊匹配，例如 *.baidu.com、www.baidu*或*baidu*。
- 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。

5.4 配置步骤

5.4.1 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“VLAN 配置”页签，进入 VLAN 配置页面。

(3) 单击 VLAN1 对应的操作列编辑图标，进入修改 VLAN 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5-2 修改 VLAN 配置

5.4.2 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“配置接口模式”页签下选择单 WAN 模式，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5-3 配置 WAN 场景

图5-4 修改 WAN 配置


修改WAN配置
WAN 接口
WAN1
连接模式
固定地址
IP地址 *
2.2.2.1
子网掩码 *
255.255.255.0
网关地址 *
2.2.2.254
DNS1
114.114.114.114
DNS2
223.5.5.5
MAC地址
使用接口出厂MAC地址（ 00-19-10-28-00-80 ）
使用静态指定的MAC
网络上行带宽
（Mbps）
网络下行带宽
（Mbps）
NAT地址转换
启用
使用地址池转换
新增地址池
TCP MSS
1280
（128-1610字节，默认：1280字节）
MTU
1500
（576-1650字节）
链路探测
未启用
探测地址
探测间隔
（1-10秒）
探测次数
（默认3次）
确定
取消

5.4.3 配置地址组

将销售部门员工 PC 的 IP 地址段设置为名称为“销售部”的地址组。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 > 地址组”，进入地址组配置页面。

(2) 单击<添加>按钮，进入添加地址组配置页面。

(3) 在“地址组名称”配置项处，输入销售部。

(4) 在“IP 地址段”配置项处，起始框输入 10.1.1.2，结束框输入 10.1.1.30。

(5) 点击配置项右侧的<→→>按钮，提交配置的地址组内容。

(6) 其它配置项均保持缺省配置即可，单击<确定>按钮保存配置。

图5-5 配置地址组

5.4.4 配置时间组

将上班时间段设置为名称为“上班时间”的时间组。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 > 时间组”，进入时间组配置页面。

(2) 单击<添加>按钮，进入新建时间组配置页面。

(3) 在“时间组名称”配置项处，输入上班时间。

(4) 在“生效时间”配置项处，选择周期性生效，并设置具体的时间段为周一至周五 9:00-18:00，单击<+>按钮，提交配置的时间段。

(5) 单击<确定>按钮保存配置。

图5-6 新建时间组

5.4.5 配置网址黑名单策略

配置一条销售部 PC 在上班时间内禁止访问优酷网的策略。配置步骤如下：

(1) 在设备 Web 管理界面导航栏中选择“上网行为管理 > 上网行为管理”，进入上网行为管理配置页面。

(2) 单击“网址控制”页签，进入网址控制配置页面。

(3) 勾选“网址黑名单模式”，单击<确定>按钮，开启网址黑名单功能。

(4) 在“网址分类”列对应的配置项处，输入新建网址控制策略的网址分类名称“policy2”。

(5) 在“地址组”列对应的配置项处，选择“销售部”地址组。

(6) 在“时间组”列对应的配置项处，选择“上班时间”时间组。

(7) 单击右侧<+>按钮，名称为“policy1”的网址分类成功。

(8) 单击“policy1”网址分类操作列对应的详情图标，进入设置网址关键字页面。

(9) 在“网址关键字”输入框中输入关键字“www.youku.com”。

(10) 单击右侧<+>按钮，提交网址关键字。

(11) 单击<确定>按钮，完成添加网址关键字。

图5-7 配置黑名单策略

图5-8 设置网址关键字

5.5 验证配置

上班时间段内，使用销售部员工 PC 无法访问优酷网，其它网页正常访问，其他部门 PC 可以正常访问任何网址，说明配置验证成功。

H3C ER G3 系列路由器

如何连接云平台典型配置举例

新华三技术有限公司
http://www.h3c.com

资料版本：6W102-20221021

1.1 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 ER G3 系列路由器-如何连接云平台典型配置案例。

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. 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。

2. 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。

3. 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。

4. 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！

目 录

1 简介

当网络管理员需要远程监管或运维路由器时，可以通过路由器 Web 管理界面上的云服务功能将路由器绑定到 H3C 云简网络平台（以下简称云平台）来实现。

本文档介绍云服务功能的配置方法。

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远程管理-云服务特性。

3 使用版本

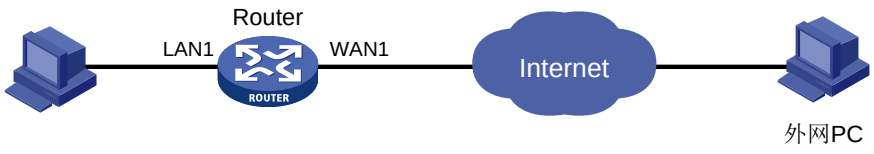
本配置举例是在 ER3200G3 路由器 Release 0114 版本上进行配置和验证的。

4 配置举例

4.1 组网需求

如图 4-1 所示，某企业要求将公司出口路由器绑定到云平台，方便远程对路由器进行监管和运维。

图4-1 云服务配置举例



4.2 配置注意事项

- ER G3 系列路由器当前仅支持绑定到 H3C 云简网络平台。
- 将路由器绑定到云平台之前，请确保路由器已连接互联网。

4.3 配置步骤

4.3.1 启用远程管理-云服务功能

#确认路由器 Web 管理界面的云服务功能为开启状态，步骤如下：

(1) 在路由器 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，单击按钮，使得按钮状态为“ON”，开启云服务。（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4-2 开启远程管理-云服务功能

4.3.2 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，进入云平台登录页面。

图4-3 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。（可以选择手机号或邮箱注册，本文以手机号注册为例）

(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4-4 手机号注册页

4.3.3 登录云平台

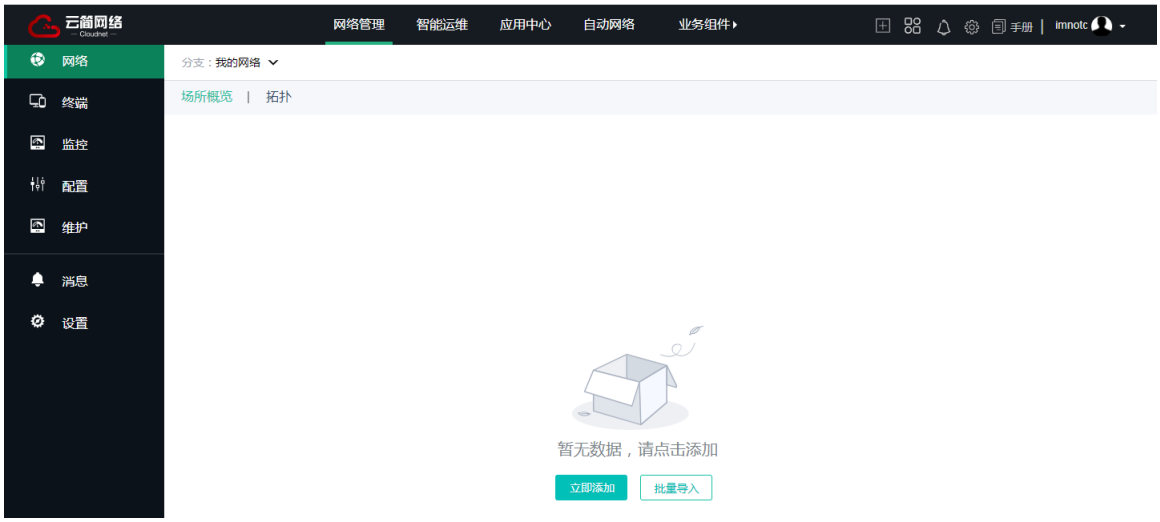
(1) 返回云平台登录页面。

(2) 在“用户名/手机号/邮箱”配置项处，输入注册的用户名。

(3) 在“密码”配置项处，输入密码。

(4) 单击<登录>按钮，进入云平台首页。

图4-5 云平台首页



4.3.4 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。

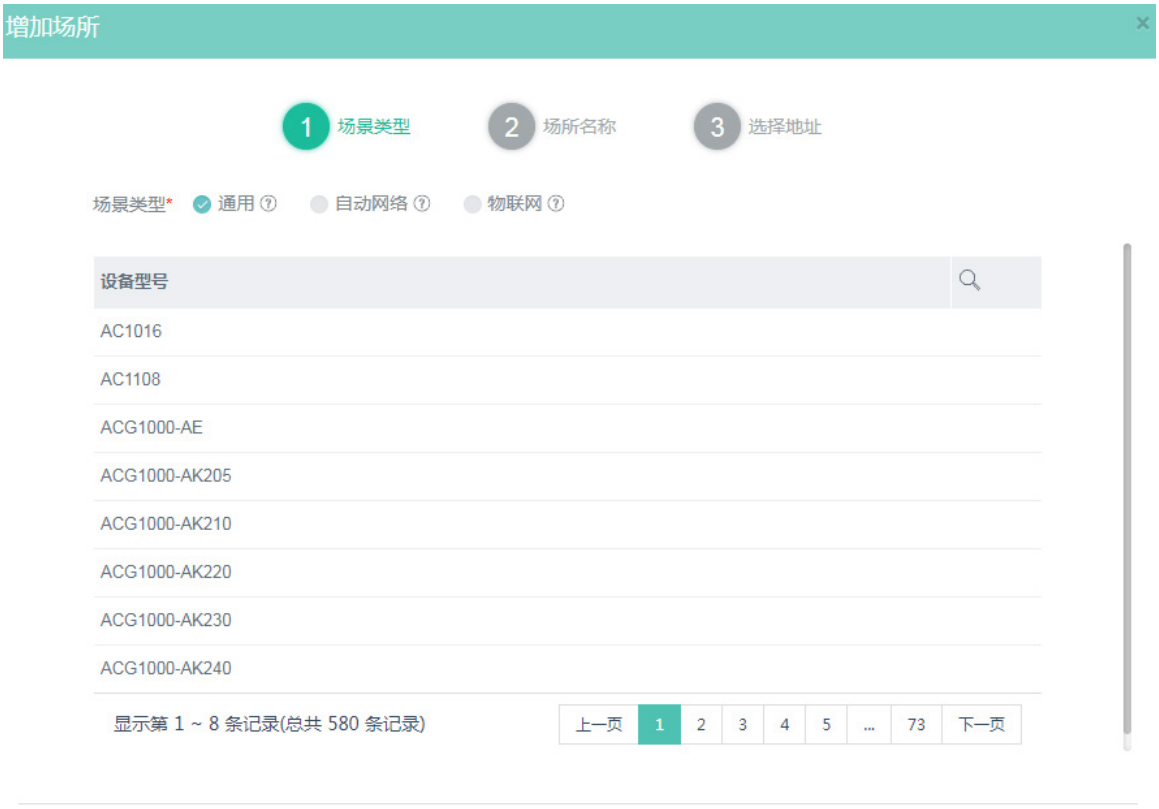
(2) 单击左侧<+增加>按钮，弹出添加分支对话框。

(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4-6 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4-7 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4-8 场所名称配置

4.3.5 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-监控”。

(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”。

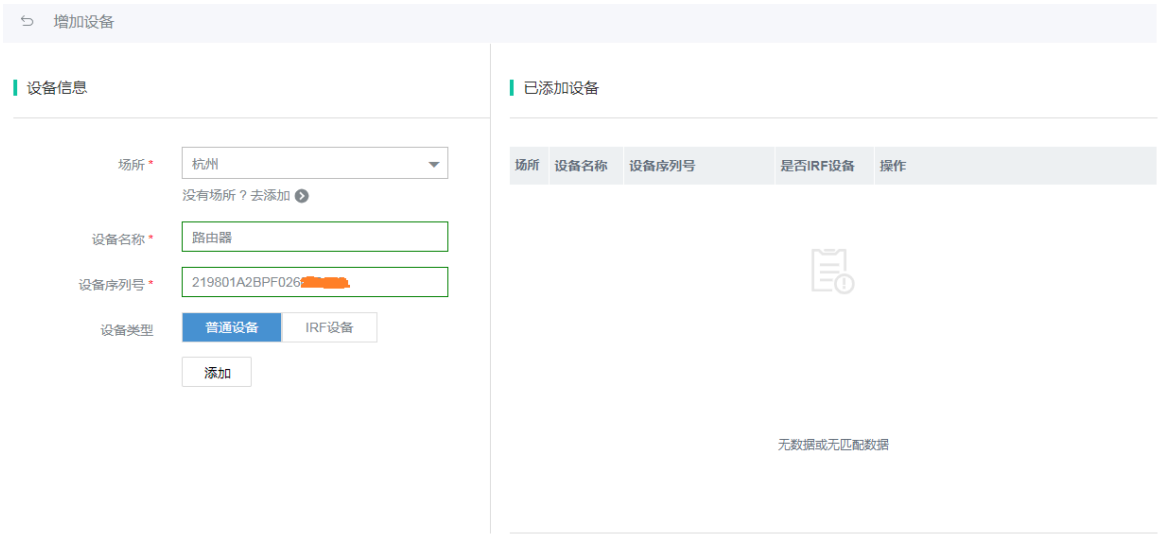
(4) 在“设备名称”配置项处，输入路由器。（可根据需要自定义）

(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4-9 增加设备



4.4 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，云管理状态为“已纳入管理”，说明设备已成功绑定云平台，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4-10 验证配置