H3C NR-1200W 企业级无线宽带路由器

用户手册

新华三技术有限公司
http://www.h3c.com

资料版本：5W100-20181010

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

《H3C NR-1200W 企业级无线宽带路由器 用户手册》将会详细地指导您如何通过 Web 设置页面或命令行对设备进行本地管理。

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！

目 录

1 您想了解什么？

如果您想？	您可以查看
初识产品的大致形态、业务特性或者它在实际网络应用中的定位	“产品概述”
通过搭建Web环境来管理设备，同时想进一步熟悉其设置页面	“登录Web设置页面”和“熟悉Web设置页面”
通过Web设置页面来设置设备WAN口的上网参数、LAN口相关功能、VLAN应用、DHCP功能等	“接口管理”
通过Web设置页面来设置设备的无线参数和AP参数，进行无线网络管理	“无线管理”
通过Web设置页面来设置对用户登录设备的上网行为管理	“上网管理”
通过Web设置页面来设置云WiFi，进行注册、绑定和升级	“云WiFi”
通过Web设置页面来实现设备及网络环境的安全性，比如：ARP安全、接入控制、防火墙等	“安全专区”
通过Web设置页面来实现设备IPSec VPN功能和L2TP VPN功能	“设置IPSec VPN”和“设置L2TP特性”
通过Web设置页面来设置设备WAN口的带宽、IP流量限制、网络连接限数等	“设置QoS”
通过Web设置页面来实现设备的高级业务功能，比如：NAT、虚拟服务器、路由管理等	“高级设置”
通过Web设置页面对设备进行维护管理，比如：软件升级、用户管理等	“设备管理”
通过Web设置页面对设备当前的设置状态进行查询或对系统运行情况进行监控等	“系统监控”
通过具体的典型组网举例来进一步理解设备的关键特性	“典型组网配置举例”
通过命令行来简单地维护设备	“附录 - 命令行设置”
定位或排除使用设备过程中遇到的问题	“附录 - 故障排除”
获取设备重要的缺省出厂配置信息	“附录 - 缺省设置”

2 产品概述

本章节主要包含以下内容：

2.1 产品简介

感谢您选择了 H3C NR-1200W 企业级无线宽带路由器（以下简称路由器），它们主要适用于 SMB（Small and Medium Business，中小企业）、政府/企业机构等需要高速有线及无线接入的中小型网络环境。

设备提供丰富的软件特性（比如：IP 流量限制、多 WAN 口负载均衡、策略路由、ARP 绑定、ARP 防护、防攻击、QQ 应用限制、IPSec/L2TP VPN 等功能），可以帮您快速地完成各功能特性需求的配置。

表2-1 路由器列表

产品	描述

NR-1200W	• 提供 1 个固定 LAN 口和 1 个固定 WAN 口，3 个 WAN/LAN 可变口，所有端口均为全千兆端口
	• 外置 4 根 5dBi 高增益全向天线，支持 2.4GHz 和 5GHz 双频覆盖
	• 工作频段：
	  ○ 802.11b/g/n：2.4GHz-2.483GHz（中国）
	  ○ 802.11ac/a/n：5.15GHz-5.35GHz，5.725GHz-5.850GHz（中国）
	• 无线传输速率：1200Mbps

说明

- 各产品间的软件特性基本类似，若存在区别，本手册会在具体特性描述时给出相关的说明。
- 本手册中所涉及的 Web 设置页面仅供参考，请以实际为准。此外，手册中所描述的功能特性规格可能随产品的升级而发生改变，恕不另行通知。详情您可以向 H3C 公司市场人员或技术支援人员咨询获取。

2.2 主要特性

2.2.1 强大的功能特性

- 丰富的无线特性

支持多个 SSID，可为公司不同部门设置不同的 SSID，并可通过启用访客网络功能，使得来访宾客使用的无线网络与公司内网完全隔离，保障内网信息安全。

- 多 WAN 口

全千兆的多 WAN 口（默认双 WAN 口）支持带宽的负载均衡及线路备份功能。满足企业多运营商接入的组网需求，可让用户根据线路实际带宽分配网络流量，充分利用带宽；同时，保障网络稳定性，在其中一条运营商线路出现故障时，其他线路也能正常工作。

- 无线 AP 扩展

支持 AP 管理功能，可自动发现并统一管理多达 8 台 H3C Mini 系列无线 AP 产品，实现 AP 接入后零配置功能，即插即用。

- 企业级 VPN

通过 VPN 安全连接，最多支持 50 路 IPSec 连接到办公网络。同时，支持 L2TP VPN 服务器和客户端模式。

- ARP 双重防护

通过 ARP 静态绑定和动态绑定功能，有效防止 ARP 欺骗引起的内网通讯中断问题；在遭受 ARP 欺骗时，提供毫秒级的免费 ARP 定时发送机制，有效地避免局域网内主机中毒后引发的 ARP 攻击，有效保障上网体验。

- 高性能防火墙

内置高性能防火墙，可防护外部多种专业的攻击手段，如 DDOS 攻击、端口扫描等行为。

内置内网异常流量防护模块，对局域网内各主机流量进行检查，并根据所选的防护等级（支持高、中、低三种）进行相应的处理，确保网络在遭受此类异常攻击时仍能正常工作。

- VLAN

支持多局域网功能，您可以方便的划分局域网为多个网段，降低广播域和 ARP 病毒的影响。针对每个局域网可以配置单独的 DHCP Server 和防火墙规则。

- 网络流量监控

提供流量实时监控和排序功能，同时提供多种安全日志，包括内/外网攻击实时日志、地址绑定日志、流量告警日志和会话日志，为网络管理员实时监控网络运行状态和安全状态提供了更快捷的窗口。

- 网络流量限速

通过基于 IP 的网络流量限速功能，可以有效地控制指定用户的上/下行流量，限制了 P2P 软件对网络带宽的过度占用。同时，提供弹性带宽功能，在网络空闲时可以智能地提升用户的限制带宽，既充分地提升了网络带宽的利用率，又保证了网络繁忙时带宽的可用性。

- 策略路由

实现按照用户制定的策略选择路由，如出接口的选择等。

- 访问控制

通过设置出站和入站通信策略，可允许或禁止特定应用数据流经过路由器；同时，支持基于用户组和时间段配置策略，实现精细化管理。

- 业务控制

QQ 等即时通讯软件的大量普及，可能会引起员工办公效率低下，无法集中精力。路由器独有的应用控制功能，可以方便地限制内网用户对 QQ 等应用的使用；同时还支持对大智慧/分析家/同花顺/广发至强/光大证券/国元证券等金融软件的应用控制功能。另外，您还可以通过对特权用户组的设置保证关键用户的使用不受影响。

- USB 管理

支持 USB 快速备份和快速恢复功能；还支持设备启动的时候从 USB 中加载并恢复配置的功能。

2.2.2 友好的用户界面

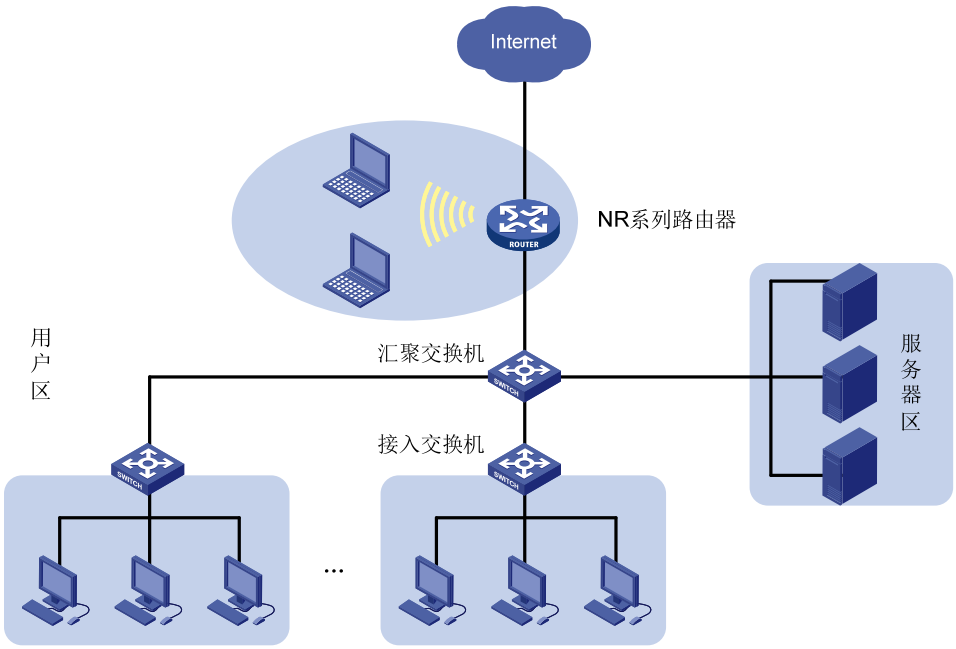
- 提供非常简便的 Web 设置页面，配置直观、易操作。
- 每个 Web 设置页面均提供详细的联机帮助，有效降低配置难度。

2.2.3 丰富的统计诊断功能和管理方式

- 提供了丰富的统计信息和状态信息显示功能，使您对路由器当前的运行状态一目了然。
- 支持通过本地和远程 Web 方式对路由器进行详细的配置和管理。
- 支持通过 Telnet 方式对路由器进行简单的命令行管理。

2.3 典型组网应用

图2-1 组网应用



3 登录Web设置页面

说明

本章节仅介绍如何本地登录路由器的Web设置页面。如果您想实现远程登录路由器进行管理，需要先本地登录路由器，并开启其远程管理功能，相关的介绍请参见“14.3 远程管理”。

本章节主要包含以下内容：

3.1 准备工作

完成硬件安装后（安装过程请参见《H3C NR-1200W 企业级无线宽带路由器 快速入门》），在登录路由器的 Web 设置页面前，您需要确保管理计算机和网络满足一些基本要求。

3.1.1 管理计算机要求

请确认管理计算机已安装了以太网卡。

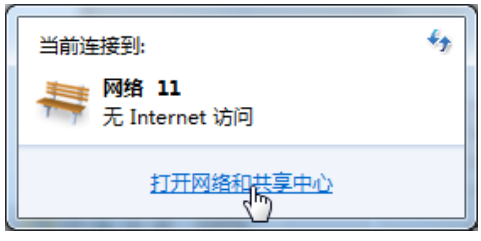
3.1.2 建立网络连接

1. 设置管理计算机的IP地址

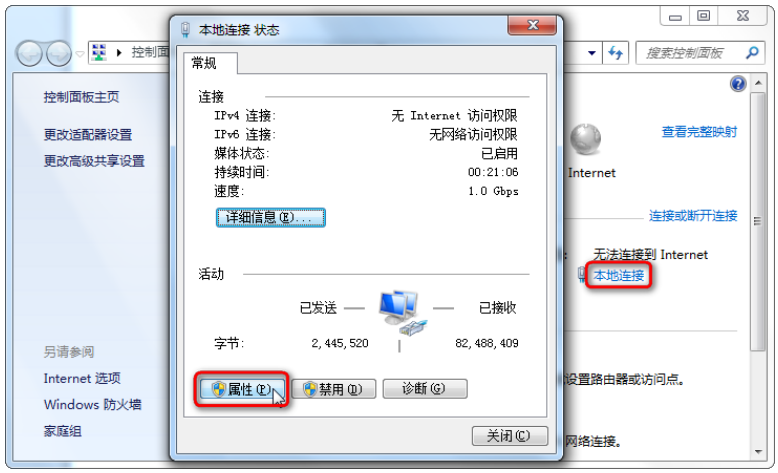
- 自动获取 IP 地址（推荐使用）：请将管理计算机设置成“自动获得 IP 地址”和“自动获得 DNS 服务器地址”（计算机系统的缺省配置），由路由器自动为管理计算机分配 IP 地址。
- 设置静态 IP 地址：请将管理计算机的 IP 地址与路由器的 LAN 口 IP 地址设置在同一网段内（LAN 口缺省的 IP 地址为 192.168.1.1，子网掩码为 255.255.255.0）。

操作步骤如下（以 Windows 7 系统为例）：

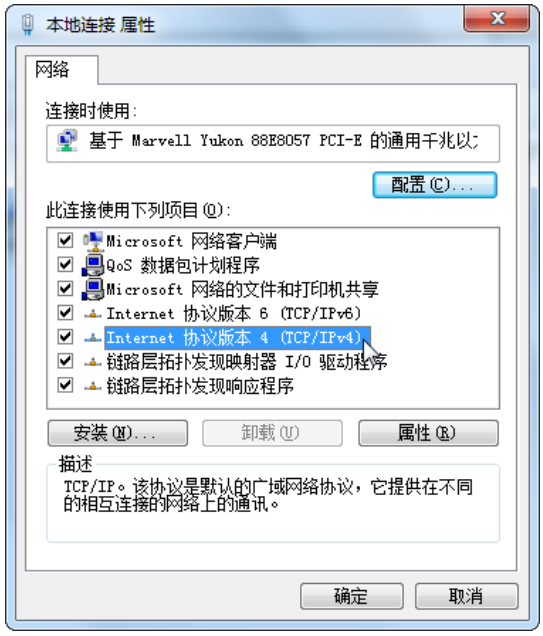
1. 单击桌面右下角的网络图标，如  ，选择“打开网络和共享中心”



2. 单击“本地连接”，单击<属性>按钮，进入“本地连接属性”窗口



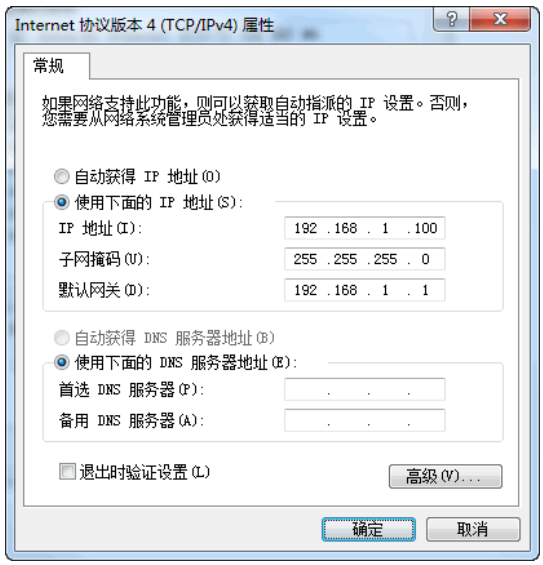
3. 双击“Internet 协议版本 4（TCP/IPv4）”



4. 配置电脑的 IP 地址

- 当路由器开启 DHCP 功能时，可选择自动获取 IP 地址和 DNS 服务器地址，或通过手动配置电脑 IP 地址，与路由器 IP 地址（缺省 192.168.1.1）保持同一网段
- 当路由器关闭 DHCP 功能时，只能通过手动配置电脑 IP 地址，与路由器 IP 地址（缺省 192.168.1.1）保持同一网段

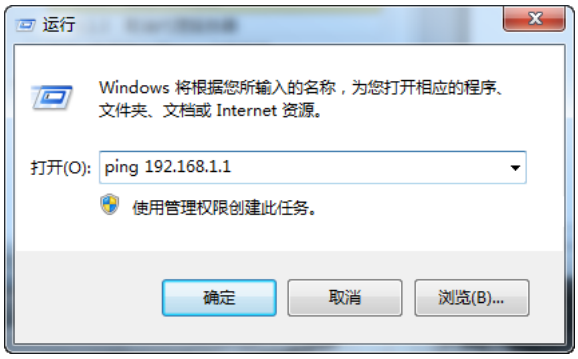
设置好IP地址后，单击<确定>按钮，返回[本地连接 属性]对话框，再单击<确定>按钮



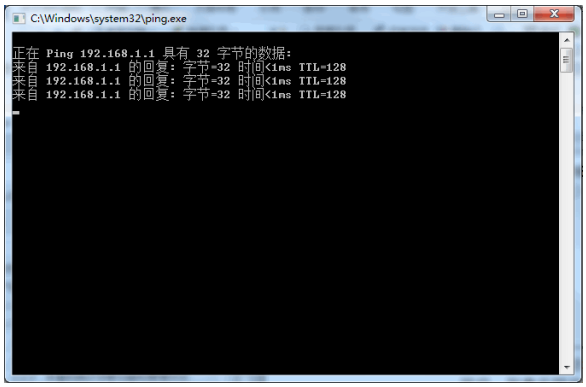
2. 确认管理计算机和路由器之间的网络是否连通

操作步骤如下：

1. 单击屏幕左下角<开始>按钮进入[开始]菜单，选择“运行”，弹出“运行”对话框
2. 输入“ping 192.168.1.1（设备的 IP 地址，此处是缺省 IP 地址）”，单击<确定>按钮



3. 如果在弹出的对话框中显示了从设备侧返回的回应，则表示网络连通；否则请检查网络连接

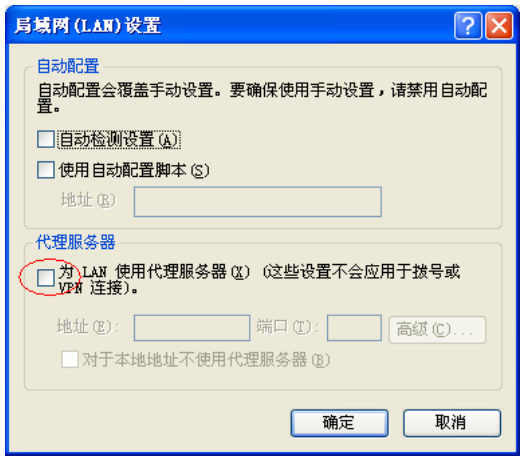


3.1.3 取消代理服务器

如果当前管理计算机使用代理服务器访问因特网，则必须取消代理服务，操作步骤如下：

1. 在浏览器窗口中，选择[工具/Internet 选项]进入“Internet 选项”窗口

2. 选择“连接”页签，并单击<局域网设置（L）>按钮，进入“局域网（LAN）设置”页面。请确认未选中“为 LAN 使用代理服务器”选项；若已选中，请取消并单击<确定>按钮



3.2 登录路由器Web设置页面

运行Web浏览器，在地址栏中输入“http://192.168.1.1”，回车后跳转到Web登录页面，如 图 3-1 所示。输入用户名、密码（缺省均为admin，区分大小写），单击<登录>按钮或直接回车即可进入Web设置页面。

图3-1 登录路由器 Web 设置页面

说明

- 同一时间，路由器最多允许五个用户通过 Web 设置页面进行管理。当对路由器进行多用户管理时，建议不要同时对其进行配置操作，否则可能会导致数据配置不一致。
- 为了安全起见，建议您首次登录后修改缺省的登录密码，并保管好密码信息。

4 熟悉Web设置页面

路由器提供非常简便的 Web 设置页面，您可以通过该设置页面快速地完成所需功能的配置。本章将带领您先了解和熟悉 Web 设置页面。

本章节主要包含以下内容：

4.1 Web设置页面介绍

图4-1 Web 设置页面示意图

4.2 常用页面控件介绍

以下控件是 Web 设置页面中经常出现的，有关它们的用途请参见下表。

表4-1 常见页面控件说明

页面控件	描述
	文本框，用于输入文本
使用设备MAC： 手工输入MAC：	单选按钮，用于从多个选项中选择一项
启用DHCP服务器	复选框，用于开启（选中）和关闭（未选中）该功能或服务
PPPoE（大部分的宽带网或xDSL） 静态地址（手工配置地址） 动态地址（从DHCP服务器自动获取） PPPoE（大部分的宽带网或xDSL） 禁用	下拉列表框，用于选择相应的列表项
应用	当您完成了某页面设置项的操作后，必须单击该页面上的<应用>按钮，设置才能生效
启用	如果页面中出现类似的蓝色字体项，您可以通过单击它来跳转到相应的页面进行设置修改
刷新　自动刷新：禁止 秒	单击<刷新>按钮，您可以手动对设置页面的数据进行更新；在“自动刷新”列表框中选择刷新频率后，页面的数据会自动根据该刷新频率进行更新

4.3 页面列表操作介绍

路由器的Web设置页面中经常会出现类似 图 4-2 的页面，此处对其操作进行统一的介绍，以下不再赘述。

图4-2 页面列表举例

表4-2 页面列表操作介绍

界面项	描述
查询	您可通过设置关键字，单击<查询>按钮来查看符合条件的列表项
显示全部	单击<显示全部>按钮，您可查看所有的列表项
全选	单击<全选>按钮，您可选中所有的列表项对其进行批量操作 说明 您也可以通过单击各列表项的方式来选中指定表项进行批量操作

界面项	描述
新增 删除	单击<新增>按钮，您可在弹出的对话框中添加一个新的表项。添加完成后，您可以通过该页面中的查询功能来确认刚添加的表项是否已存在 选中指定的列表项，单击<删除>按钮，您可将该列表项删除
	单击该图标，您可在弹出的对话框中对该列表项进行修改  说明 双击某列表项，同样也可在弹出的对话框中对该列表项进行修改

4.4 Web用户超时处理

当您长时间没有操作Web设置页面时，系统超时并将注销本次登录，返回到Web设置登录页面（如图 3-1 所示）。

 说明

Web用户登录的超时时间缺省为 5 分钟。如果您想修改此超时时间，相关操作请参见“14.4.1 登录管理”。

4.5 退出Web设置页面

单击导航栏中的 退出，确认后即可退出 Web 设置页面。

5 接口管理

说明

路由器能自动进行拨号，您无需使用操作系统自带的拨号软件（如 PPPoE 拨号软件）或其他客户端拨号软件。

本章节主要包含以下内容：

5.1 设置WAN

5.1.1 接口转换

路由器缺省为双 WAN 口，支持 WAN/LAN 口转换，您可设置 WAN 口的数目。当 WAN 口数量更改时，会自动增加/删除接口相关的条目。

页面向导：接口管理→WAN 设置→接口转换

本页面为您提供如下主要功能：

配置WAN口数目	

页面中关键项的含义如下表所示。

表5-1 页面关键项描述

页面关键项	描述
WAN口数目	设置路由器WAN口的数目。根据接入因特网的链路个数配置相应的WAN出口个数

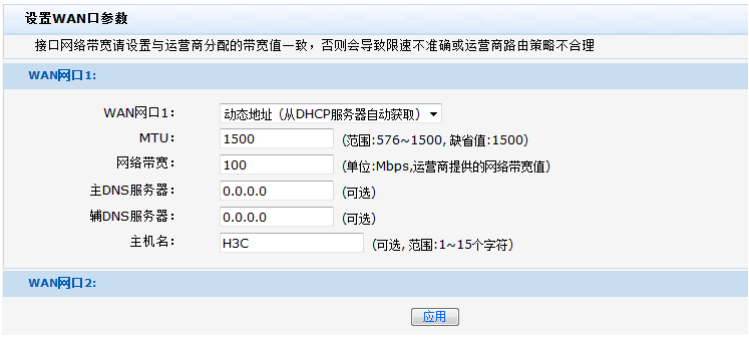
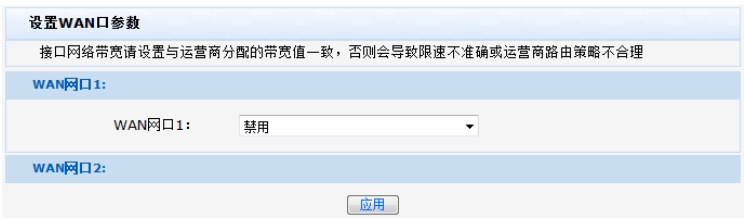
5.1.2 连接到因特网

路由器支持静态地址、动态地址、PPPoE 三种连接方式。具体选择何种方式请咨询当地运营商。

- 静态地址：手动为 WAN 口设置 IP 地址和子网掩码。
- 动态地址：设置 WAN 口作为 DHCP 客户端，使用 DHCP 方式获取 IP 地址。
- PPPoE：设置 WAN 口作为 PPPoE 客户端，使用 PPPoE 用户名和密码拨号连接获取 IP 地址。

页面向导：接口管理→WAN 设置→连接到因特网

本页面为您提供如下主要功能：

通过静态地址连接到因特网	
通过动态地址连接到因特网	
通过PPPoE连接到因特网	
关闭指定WAN口连接到因特网的功能	

页面中关键项的含义如下表所示。

表5-2 页面关键项描述

页面关键项	描述
IP地址	设置路由器WAN口的IP地址。由运营商提供
子网掩码	设置路由器WAN口的IP地址子网掩码。由运营商提供
缺省网关	设置路由器WAN口的缺省网关地址。由运营商提供
MTU	设置路由器WAN口允许通过的最大传输单元，单位为字节。建议您使用缺省值
网络带宽	连接至设备WAN口的线路出口带宽
主DNS服务器	设置路由器主域名服务器的地址，用于将便于记忆的、有意义的域名解析为正确的IP地址。由运营商提供
辅DNS服务器	设置路由器辅域名服务器的地址，当主域名服务器失效时，可以由它来完成解析。由运营商提供
主机名	设置在路由器使用DHCP方式获取IP地址时，DHCP服务器侧显示的路由器主机名
PPPoE用户名	设置PPPoE拨号上网时，身份验证使用的用户名。由运营商提供
PPPoE密码	设置PPPoE拨号上网时，身份验证使用的密码。由运营商提供
服务器名	设置PPPoE服务器的名称。由运营商提供
服务名	设置PPPoE服务器的服务名称。由运营商提供
LCP主动检测	设置PPPoE拨号上网时的链路检测方式，缺省情况为“是”： • 选择“是”，设备会主动发送 LCP 请求，即时检测链路状态 • 选择“否”，设备如果在等待时间内没有收到服务器的 LCP 请求，才会进行 LCP 检测

说明

- 当您需要设置运营商分配给您的带宽时，相关操作请参见“12.1 设置IP流量限制”。
- 设置完成后，您可以通过查看 基本信息页面中的“WAN网口状态”来验证设置是否已生效。

5.1.3 设置多WAN工作模式

路由器的多 WAN 工作模式包括同运营商接入和不同运营商接入两种。

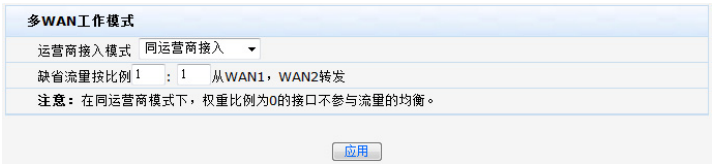
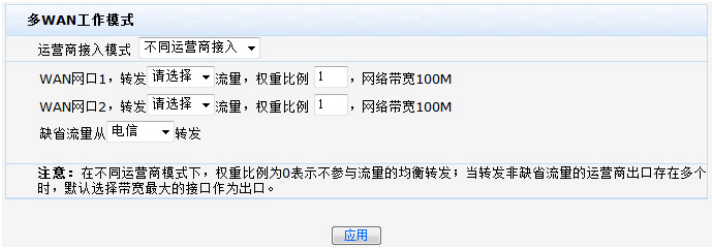
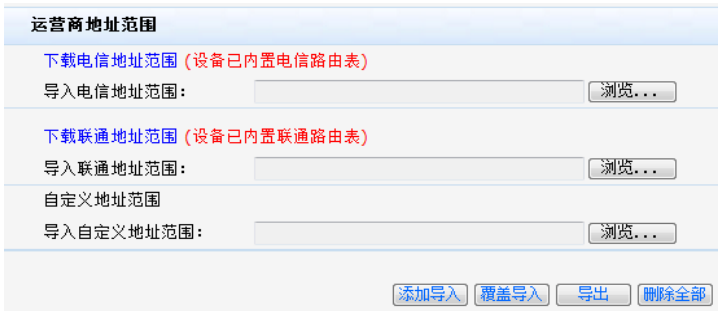
表5-3 多 WAN 工作模式描述

工作模式	描述
同运营商接入模式	正常情况下，允许多条链路同时工作，流量会先根据路由表进行选择链路，其它流量根据设置的比例将网络连接分担到各个WAN口上 同运营商接入模式主要应用于同一运营商接入网场景，流量根据设置的比例转发 设置的流量比例为0的WAN口只转发路由表选择的链路，不转发其他流量

工作模式	描述
不同运营商接入模式	正常情况下，允许多条链路同时工作，接口转发配置的运营商流量，其他流量根据配置的缺省运营商WAN口转发 不同运营商接入模式主要应用于多路不同的运营商接入场景，根据地址范围配置实现“电信走电信，网通走网通”功能 设置的流量比例为0的WAN口只转发路由表选择的链路，不转发其他流量

页面向导：接口管理→WAN 设置→多 WAN 工作模式

本页面为您提供如下主要功能：

设置多WAN同运营商接入模式	
设置多WAN不同运营商接入模式	
导入运营商地址池	

页面中关键项的含义如下表所示。

表5-4 页面关键项描述

页面关键项	描述
添加导入	在原来的均衡路由表基础上，将已编辑好的均衡路由表文件（.cfg格式）导入 说明 cfg 文件的格式是“目的 IP 地址/子网掩码”。其中： ● “目的 IP 地址”：输入网段地址，到该网段的报文会从指定的出接口转发 ● “子网掩码”：目的 IP 地址的子网掩码，表示方式为网络地址位数 举例如下： 58.32.0.0/13 58.40.0.0/16 58.42.0.0/16

页面关键项	描述
覆盖导入	删除原来的运营商地址池表项，然后再将已编辑好的均衡路由表文件（.cfg格式）导入
导出	将当前的运营商地址池文件导出到本地保存
删除全部	删除运营商地址池中的所有表项

说明

- 当您选择了均衡模式或者手动模式后，可以通过设置均衡路由表，使访问特定目的 IP 地址的报文按指定的链路进行转发。比如：在手动模式下，您可以通过导入新联通的均衡路由表，使访问新联通的流量都通过 WAN2 转发；然后再指定缺省链路为 WAN1，使非访问新联通的流量都通过 WAN1 转发，从而达到不同运营商流量在不同的链路上转发的目的。
- 设置完成后，您可以通过查看 基本信息页面中的“WAN网口模式”来验证设置是否已生效。

5.1.4 设置链路检测

如果您需要实时监控线路状态，保证一条线路故障时能切换到另一条线路，您就需要设置路由器的线路检测功能。路由器支持灵活的检测机制，并提供多种线路检测方法供您选择（包括 PING 检测、DNS 检测和 NTP 检测三种方式），以满足实际应用的需要。

- 启用 WAN 口线路检测后，如果您指定了一种或多种检测方式，路由器将只使用指定的检测方式。为了检测的有效性，建议您同时使用多种检测方式。
- 启用 WAN 口线路检测后，如果您没有指定检测方式，路由器将使用缺省的检测方式（PING 检测），即向 WAN 口对应的网关发送 Ping 报文，以检测通信是否正常。

说明

- 缺省情况下，路由器不进行 WAN 口线路检测。
- 由于运营商侧的 PPPoE 服务器可能不响应 Ping 报文，因此，在 PPPoE 拨号方式下，如果您启用了 WAN 口线路检测功能且检测方式为“PING 检测”时，请勿将“PING 检测”的目的地址设置为 WAN 口对应的网关地址。否则路由器将判断这个链路存在故障。
- 检测结果您可通过查看 基本信息页面中的“链路状态”来获取。

页面向导：接口管理→WAN 设置→链路检测

本页面为您提供如下主要功能：

设置WAN口线路检测

页面中关键项的含义如下表所示。

表5-5 页面关键项描述

页面关键项	描述
PING检测	选中“PING检测”复选框，输入目的IP地址，单击<应用>按钮，路由器会通过Ping报文来检测与目的IP地址的连通性，有响应则认为线路正常
DNS检测	选中“DNS检测”复选框，输入需要DNS解析的域名，路由器会通过DNS报文来检测与DNS服务器的连通性，有响应认为线路正常
NTP检测	选中“NTP检测”复选框，输入NTP服务器的IP地址，路由器会通过NTP报文来检测与NTP服务器的连通性，有响应认为线路正常

5.1.5 设置MAC地址克隆

路由器出厂时，各 WAN 口都有一个缺省的 MAC 地址，一般情况下，无需改变。但是，比如：有些运营商要求只有注册过的路由器才能连接到因特网，此时，您就需要使用路由器 WAN 口 MAC 地址克隆功能，将 WAN 口 MAC 地址修改为在运营商侧注册过的 MAC 地址。

页面向导：接口管理→WAN 设置→MAC 地址克隆

本页面为您提供如下主要功能：

设置WAN口MAC地址克隆

页面中关键项的含义如下表所示。

表5-6 页面关键项描述

页面关键项	描述
使用本设备的MAC地址	选中该项，使用路由器出厂时的MAC地址
使用这台PC的MAC地址	选中该项，使用用来设置路由器的管理计算机的MAC地址
手工输入MAC地址	选中该项，输入在运营商侧注册过的MAC地址

说明

- 当进行 WAN 口 MAC 地址克隆设置时，如果更换了 MAC 地址，则 WAN 口会重新进行初始化。在此过程中，转发的流量会因为接口地址和路由的变化，会重新选择出接口。待接口初始化完成以后，新建立的转发业务才会按照您所设置的方式进行转发。
- 设置完成后，您可以通过查看 基本信息页面中的“MAC地址”来验证设置是否已生效。

5.1.6 设置网口模式

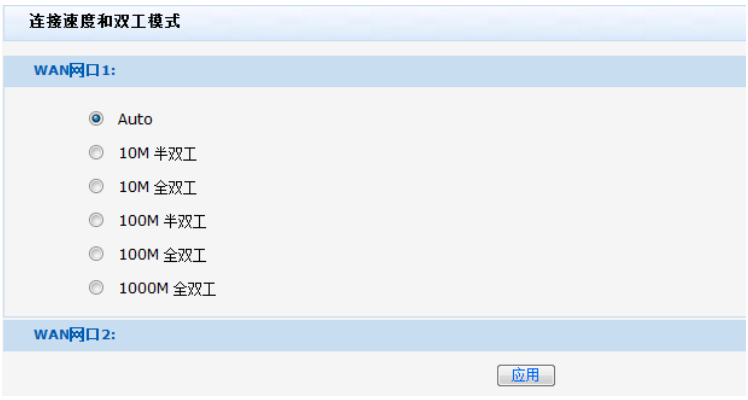
路由器的 WAN 口支持以下几种速率和双工模式的组合。

表5-7 WAN 口的速率和双工模式

项目	描述
Auto	WAN口的双工和速率状态均由本端口和对端端口自动协商而定 说明 缺省情况下，WAN 口采用 Auto 模式
10M半双工	WAN口工作在10Mbps速率下，且端口同一时刻只能发送数据包或接收数据包
10M全双工	WAN口工作在10Mbps速率下，且端口在发送数据包的同时可以接收数据包
100M半双工	WAN口工作在100Mbps速率下，且端口同一时刻只能发送数据包或接收数据包
100M全双工	WAN口工作在100Mbps速率下，且端口在发送数据包的同时可以接收数据包
1000M全双工	WAN口工作在1000Mbps速率下，且端口在发送数据包的同时可以接收数据包

页面向导：接口管理→WAN 设置→网口模式

本页面为您提供如下主要功能：

选择WAN口的速率和双工模式	

说明

- 除了 Auto 模式外，路由器 WAN 口的速率和双工模式需要与对端设备保持一致。
- 设置完成后，您可以通过查看 端口流量 页面中的“链路状态”来验证设置是否已生效。

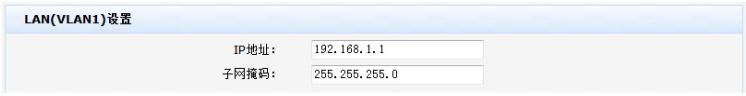
5.2 设置LAN

5.2.1 修改IP地址

当您修改了路由器 LAN 口的 IP 地址后，您需要在浏览器中输入新的 IP 地址重新登录，才能对路由器继续进行配置和管理。比如：某企业事先已经将整个 IP 地址段均已规划好，因此，您需要根据已规划好的 IP 地址来修改路由器 LAN 口的 IP 地址，以适应实际环境。

页面向导：接口管理→LAN 设置→局域网设置

本页面为您提供如下主要功能：

修改LAN口的IP地址（缺省情况下，路由器LAN口的IP地址为192.168.1.1，子网掩码为255.255.255.0）	

说明

修改 LAN 口 IP 地址后，其他页面中和 IP 地址相关的配置可能需要相应修改（如 IP/MAC 绑定表中的 IP 地址等），保持和 LAN 口 IP 在同一网段。

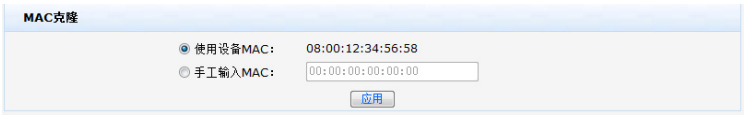
5.2.2 设置MAC地址克隆

路由器出厂时，LAN 口均有一个缺省的 MAC 地址，一般情况下，无需改变。但是，比如：某企业之前为了防止 ARP 攻击，给局域网内的主机均设置了网关的静态 ARP 表项。此时，如果企业想升级设备，将原来的网关换成了路由器（网关地址保持不变），局域网内的主机则无法学习到路由器的 MAC 地址。因此，您需要逐个修改局域网内主机的静态 ARP 表项，才可使局域网内的主机恢复正常上网，这样维护效率会很低。

路由器的 LAN 口 MAC 克隆功能可以使您免除这样的重复劳动，只需将路由器的 LAN 口 MAC 地址设为原来网关的 MAC 地址，局域网内的主机即可正常上网了。

页面向导：接口管理→LAN 设置→局域网设置

本页面为您提供如下主要功能：

设置LAN口MAC地址克隆	

页面中关键项的含义如下表所示。

表5-8 页面关键项描述

页面关键项	描述
使用设备MAC	选中该项，使用路由器LAN口出厂时的MAC地址
手工输入MAC	选中该项，输入原网关的MAC地址

5.2.3 设置基本属性

路由器 LAN 口的基本属性包括端口的速率/双工模式、广播风暴抑制和流控功能。

1. 速率/双工模式

路由器的 LAN 口支持以下几种速率和双工模式的组合。

表5-9 LAN 口的速率和双工模式

项目	描述
Auto	LAN口的双工和速率状态均由本端口和对端端口自动协商而定 说明 缺省情况下，LAN 口采用 Auto 模式
10M半双工	LAN口工作在10Mbps速率下，且端口同一时刻只能发送数据包或接收数据包
10M全双工	LAN口工作在10Mbps速率下，且端口在发送数据包的同时可以接收数据包
100M半双工	LAN口工作在100Mbps速率下，且端口同一时刻只能发送数据包或接收数据包
100M全双工	LAN口工作在100Mbps速率下，且端口在发送数据包的同时可以接收数据包
1000M全双工	LAN口工作在1000Mbps速率下，且端口在发送数据包的同时可以接收数据包

2. 广播风暴抑制

如果局域网内存在大量的广播报文流量（可能由病毒导致）时，将会影响网络的正常通信。您可以通过设置路由器 LAN 口的广播风暴抑制功能，可以有效地抑制大量广播报文的传播，避免网络拥塞，保证网络业务的正常运行。

路由器允许您设置四种 LAN 口的广播风暴抑制状态级别：不抑制、低、中、高。这四个级别允许通过的报文流量依次减少，您可根据实际需求进行相应的设置。缺省情况下，LAN 口的广播风暴抑制功能处于关闭状态（即不抑制）。

3. 流控

一般仅在网络拥塞比较严重时，才开启路由器 LAN 口的流控功能。

当路由器和对端设备都开启了流量控制功能后，如果路由器发生拥塞：

(1) 路由器将向对端设备发送消息，通知对端设备暂时停止发送报文或减慢发送报文的速度。

(2) 对端设备在接收到该消息后，将暂停向路由器发送报文或减慢发送报文的速度，从而避免了报文丢失现象的发生，保证了网络业务的正常运行。

缺省情况下，路由器 LAN 口的流控功能处于关闭状态。

页面向导：接口管理→LAN 设置→端口设置

本页面为您提供如下主要功能：

设置LAN口的基本属性	

 说明

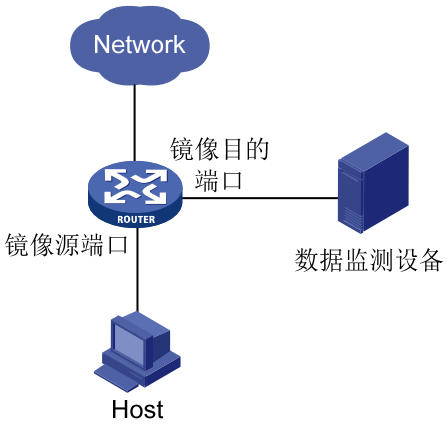
- 除了 Auto 模式外，路由器 LAN 口的速率和双工模式需要与对端设备保持一致。
- 设置完成后，您可以通过查看 端口流量 页面中的“链路状态”来验证端口模式设置是否已生效。

5.2.4 设置本地端口镜像

端口镜像是将指定镜像源端口的报文复制到镜像目的端口，镜像目的端口会与数据监测设备相连，用户利用这些数据监测设备来分析复制到目的端口的报文，进行网络监控和故障排除。

路由器提供本地端口镜像功能，即镜像源端口和镜像目的端口在同一台设备上。

图5-1 本地端口镜像示意图



页面向导：接口管理→LAN 设置→端口镜像

本页面为您提供如下主要功能：

通过设置镜像源端口（被镜像端口）和镜像目的端口（镜像端口）来实现路由器的本地端口镜像	

说明

设置完成后，您可以通过查看 端口流量 页面中的“端口镜像信息”来验证设置是否已生效。

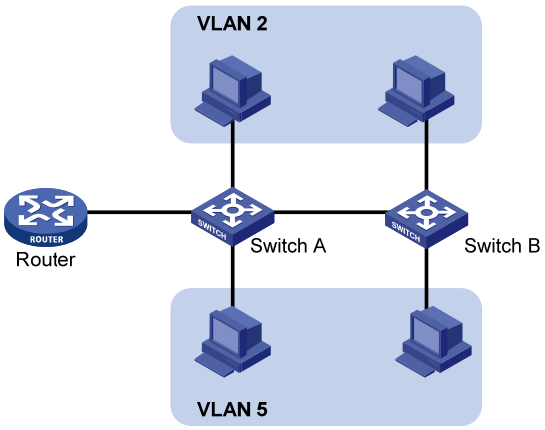
5.3 设置VLAN

5.3.1 VLAN简介

1. VLAN概述

以太网是一种基于CSMA/CD的共享通讯介质的数据网络通讯技术，当主机数目较多时会导致冲突严重、广播泛滥、性能显著下降甚至使网络不可用等问题。在这种情况下出现了VLAN技术，这种技术可以把一个LAN划分成多个逻辑的LAN——VLAN，每个VLAN是一个广播域。VLAN内的主机间通信就和在一个LAN内一样，而VLAN间则不能直接互通，这样，广播报文被限制在一个VLAN内，如 图 5-2 所示。

图5-2 VLAN 示意图



2. VLAN的优点

与传统以太网相比，VLAN 具有如下的优点：

- 控制广播域的范围：局域网内的广播报文被限制在一个 VLAN 内，节省了带宽，提高了网络处理能力。
- 增强了 LAN 的安全性：由于报文在数据链路层被 VLAN 划分的广播域所隔离，因此各个 VLAN 内的主机间不能直接通信，需要通过路由器或三层网络设备对报文进行三层转发。
- 灵活创建虚拟工作组：使用 VLAN 可以创建跨物理网络范围的虚拟工作组，当用户的物理位置在虚拟工作组范围内移动时，不需要更改网络配置即可以正常访问网络。

3. VLAN接口

不同 VLAN 间的主机不能直接通信，需要通过路由器或三层网络设备进行转发。

VLAN 接口是一种三层模式下的虚拟接口，主要用于实现 VLAN 间的三层互通，它不作为物理实体存在于设备上。每个 VLAN 对应一个 VLAN 接口，该接口可以为本 VLAN 内端口收到的报文根据其目的 IP 地址在网络层进行转发。通常情况下，由于 VLAN 能够隔离广播域，因此每个 VLAN 也对应一个 IP 网段，VLAN 接口将作为该网段的网关对需要跨网段转发的报文进行基于 IP 地址的三层转发。

4. VLAN类型

目前，路由器支持基于端口的 VLAN。

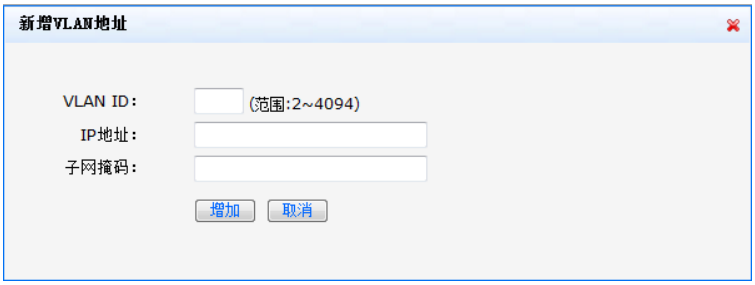
基于端口的 VLAN 是最简单的一种 VLAN 划分方法。您可以将设备上的端口划分到不同的 VLAN 中，此后从某个端口接收的报文将只能在相应的 VLAN 内进行传输，从而实现广播域的隔离和虚拟工作组的划分。

基于端口的 VLAN 具有实现简单，易于管理的优点，适用于连接位置比较固定的用户。

5.3.2 设置VLAN

页面向导：接口管理→VLAN 设置→VLAN 设置

本页面为您提供如下主要功能：

显示和修改已添加的VLAN接口（主页面）	
创建新的VLAN接口（单击主页面上的<新增>按钮，在弹出的对话框中输入相应的VLAN接口信息，单击<增加>按钮完成操作）	

5.3.3 设置Trunk口

Trunk 类型是以太网端口的链路类型之一。此类型的端口可以属于多个 VLAN，可以接收和发送多个 VLAN 的报文，一般用于连接交换机。

表5-10 Trunk 端口收发报文的处理

接收报文时的处理		发送报文时的处理
当接收到的报文不带 Tag 时	当接收到的报文带有 Tag 时	
• 当缺省 VLAN ID（即 PVID）在端口允许通过的 VLAN ID 列表里时：接收该报文，且给报文添加缺省 VLAN 的 Tag • 当缺省 VLAN ID 不在端口允许通过的 VLAN ID 列表里时：丢弃该报文	• 当 VLAN ID 在端口允许通过的 VLAN ID 列表里时：接收该报文 • 当 VLAN ID 不在端口允许通过的 VLAN ID 列表里时：丢弃该报文	• 当 VLAN ID 与缺省 VLAN ID 相同，且是该端口允许通过的 VLAN ID 时：去掉 Tag，发送该报文 • 当 VLAN ID 与缺省 VLAN ID 不同，且是该端口允许通过的 VLAN ID时：保持原有Tag，发送该报文

页面向导：接口管理→VLAN 设置→Trunk 口设置

本页面为您提供如下主要功能：

设置指定端口的Trunk相关参数（PVID和端口允许通过的VLAN）	

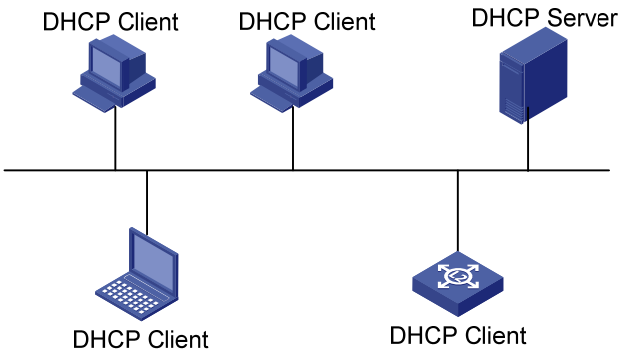
5.4 设置DHCP

5.4.1 DHCP简介

DHCP 采用“客户端/服务器”通信模式，由客户端向服务器提出配置申请，服务器返回为客户端分配的 IP 地址等配置信息，以实现网络资源的动态配置。

在DHCP的典型应用中，一般包含一台DHCP服务器和多台DHCP客户端（比如：PC和便携机），如图 5-3 所示。

图5-3 DHCP 典型应用



5.4.2 DHCP的IP地址分配

1. IP地址分配策略

路由器作为 DHCP 服务器，提供两种 IP 地址分配策略：

- 手工分配地址：由管理员为特定客户端静态绑定 IP 地址。通过 DHCP 将配置的固定 IP 地址分配给客户端。
- 动态分配地址：DHCP 为客户端分配具有一定有效期限的 IP 地址，当使用期限到期后，客户端需要重新申请地址。

2. IP地址分配机制

(1) 路由器接收到 DHCP 客户端申请 IP 地址的请求时，首先查找手工设置的 DHCP 静态表，如果这台 DHCP 客户端的 MAC 地址在 DHCP 静态表中，则把对应的 IP 地址分配给该 DHCP 客户端。

(2) 如果申请 IP 地址的 DHCP 客户端 MAC 地址不在 DHCP 静态表中，或者 DHCP 客户端申请的 IP 地址与 LAN 口的 IP 地址不在同一网段，路由器会从地址池中选择一个在局域网中未被使用的 IP 地址分配给该主机。

(3) 如果地址池中没有任何可分配的 IP 地址，则主机获取不到 IP 地址。

说明

如果主机离线（比如：主机关机了），路由器不会马上把之前分给它的 IP 地址分配出去，只有在地址池中没有其他可分配的 IP 地址，且该离线主机 IP 地址的租约过期时，才会分配出去。

5.4.3 设置DHCP服务器

页面向导：接口管理→DHCP 设置→DHCP 设置

本页面为您提供如下主要功能：

显示和修改已创建的DHCP服务器信息（主页面）

创建新的DHCP服务器（单击主页面中的<新增>按钮，在弹出的对话框中选择需要启用DHCP服务器功能的VLAN接口，并设置DHCP服务相关参数，单击<增加>按钮完成操作）

页面中关键项的含义如下表所示。

表5-11 页面关键项描述

页面关键项	描述
VLAN接口	选择启用DHCP服务器功能的VLAN接口，且一个VLAN接口上只能创建一个DHCP服务器
启用DHCP服务器	缺省情况下，DHCP服务器功能处于开启状态
地址池起始地址	DHCP服务器地址池的起始地址
地址池结束地址	DHCP服务器地址池的结束地址，且地址池结束地址要大于起始地址
地址租约	设置DHCP服务器分配给客户端IP地址的租借期限。当租借期满后，DHCP服务器会收回该IP地址，客户端必须重新申请（客户端一般会自动申请） 缺省情况下，地址租约为1440分钟
客户端域名	设置DHCP服务器分配给客户端使用的域名地址后缀
主DNS服务器	设置DHCP服务器分配IP地址时所携带的主DNS服务器地址 缺省情况下，DNS服务器地址为网关地址
辅DNS服务器	设置DHCP服务器分配IP地址时所携带的辅DNS服务器地址 缺省情况下，DNS服务器地址为网关地址

5.4.4 设置DHCP静态表

如果您想让路由器给某些特定的客户端分配固定的 IP 地址，可以事先通过 DHCP 静态表将客户端的 MAC 地址和 IP 地址进行绑定，使其成为一对一的分配关系。

说明

当您设置路由器通过DHCP方式为客户端分配IP地址的同时又设置了 ARP绑定，此时，请确保DHCP静态表项与ARP绑定表项不冲突，否则对应的客户端可能无法上网。建议您可以将 ARP绑定表导出，然后再将其导入到DHCP静态表中。

页面向导：接口管理→DHCP 设置→DHCP 静态表

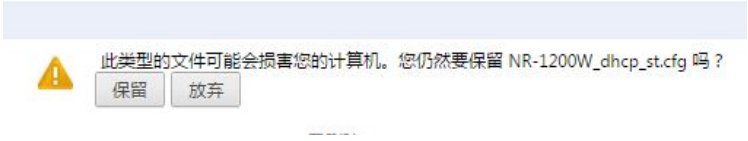
本页面为您提供如下主要功能：

显示和修改已添加的DHCP静态表项（主页面）

单个添加DHCP静态表项（单击主页面上的<新增>按钮，在弹出的对话框中设置相应的参数，并单击<增加>按钮完成操作）

批量添加DHCP静态表项（您可以先在本地编辑一个.cfg文件，内容格式为“MAC地址 IP地址 描述”（比如：00:0A:EB:7F:AA:AB 192.168.1.2 zhangsan），且每条静态表项之间需换行。单击主页面上的<导入>按钮，在弹出的对话框中选择该文件将其导入即可）

将路由器当前的DHCP静态表项备份保存（.cfg文件），且您可用“记事本”程序打开该文件进行编辑（单击主页面上的<导出>按钮，确认后即可将其导出到本地）



5.4.5 显示和维护DHCP客户列表

页面向导：接口管理→DHCP 设置→DHCP 客户列表

本页面为您提供如下主要功能：

- 显示已分配的 DHCP 客户列表信息
- 释放并回收指定客户端的 IP 地址，使该 IP 地址可以重新被分配（选择指定的客户项，比如：已关机客户 PC，单击<释放>按钮即可）

6 无线管理

本章节主要包含以下内容：

6.1 无线服务简介

WLAN 技术是当今通信领域的热点之一，使用 WLAN 解决方案，网络运营商和企业能够为用户提供方便的无线接入服务，主要包括：

- 应用具有无线局域网功能的设备建立无线网络，通过该网络，用户可以访问局域网或因特网；
- 使用不同认证和加密方式，提供安全的无线网络接入服务；
- 在无线网络内，用户可以在网络覆盖区域内自由移动，彻底摆脱有线束缚。

无线 AP 基于 WLAN 技术，实现了 802.11 无线网络标准中的无线接入功能。开启本功能后，无线客户端（带有无线网卡的 PC 或智能移动终端等）可通过无线方式方便快捷地连接到无线局域网，实现高速率的数据通信，部署灵活，免去了有线连接的繁琐。同时，无线 AP 支持多种加密功能，有效地保证了数据通信的安全性。

6.2 无线管理

6.2.1 基本设置

1. 设置内部网络

您可以通过本页面设置内部网络基础 SSID，内网用户可以管理设备，但是无法与访客网络客户端通信。

页面向导：无线管理→基本设置→内部网络

本页面为您提供如下主要功能：

- 开启/关闭 2.4G 和 5G 无线网络功能
- 设置 2.4G 和 5G 基础 SSID 的信息（设置 2.4G 和 5G 射频的内部网络基础 SSID 名称，并选择加密方式，单击<应用>按钮生效）

页面中关键项的含义如下表所示。

表6-1 页面关键项描述

页面关键项	描述
启用无线网络	启用/禁用整个无线网络功能，包括访客网络功能 默认启用无线网络功能
SSID名称	配置2.4G和5G的基础SSID名称，2.4G的SSID-1名称默认为H3C，5G的SSID-2名称默认为H3C_5G
加密方式	设置2.4G和5G的基本SSID的加密方式，可以设置为不加密或WPA-PSK/WPA2-PSK加密，默认为不加密
共享密钥	如果选择加密，则输入此密钥才能连接上SSID，长度范围为8～63个字符

2. 设置访客网络

您可以通过本页面设置访客网络 SSID，通过访客网络，您的客人可以访问外网资源，但是无法管理设备，也无法与内网客户端通信。

页面向导：无线管理→基本设置→访客网络

本页面为您提供如下主要功能：

- 开启/关闭 2.4G 和 5G 无线访客网络功能
- 设置 2.4G 和 5G 访客网络 SSID 的信息（设置 2.4G 和 5G 射频的访客网络 SSID 名称，并选择加密方式，单击<应用>按钮生效）

页面中关键项的含义如下表所示。

表6-2 页面关键项描述

页面关键项	描述
启用SSID	启用/禁用访客网络功能 默认启用该功能
SSID名称	配置2.4G和5G的访客网络SSID名称，2.4G的SSID的名称默认为H3C_GUEST，5G的SSID的名称默认为H3C_5G_GUEST
加密方式	设置2.4G和5G访客网络的基本SSID的加密方式，可以设置为不加密或WPA-PSK/WPA2-PSK加密，默认为不加密
共享密钥	如果选择加密，则输入此密钥才能连接上SSID，长度范围为8～63个字符

6.2.2 高级设置

1. 多SSID设置

您可以通过本页面添加多个 SSID 并进行管理。

说明

SSID 设置时，需注意同射频下的 SSID 名称不能相同。

页面向导：无线管理→高级设置→多 SSID 设置

本页面为您提供如下主要功能：

- 设置 2.4G SSID 的基本信息（在主页面中双击待配置的 SSID 表项，进入[SSID 配置]页面）
- 设置 SSID 加密方式（可以设置为不加密或 WPA-PSK/WPA2-PSK 加密）

页面中关键项的含义如下表所示。

表6-3 页面关键项描述

页面关键项	描述
启用SSID	选择是否启用该SSID 缺省情况下，启用该功能
SSID射频	新增SSID时，可以选择在2.4G或5G射频上创建
SSID名称	设置无线网络使用的SSID名称 不同的SSID用于区分不同的无线网络
桥接VLAN	SSID工作在桥接模式，设置该SSID（无线接口）与哪个VLAN桥接在一起，即将无线接口和VLAN放在同一个桥下 缺省情况下，SSID与VLAN1桥接在一起

页面关键项	描述
客户端隔离	选择与某个SSID建立连接的无线客户端之间是否可以互相通信 • 禁用：允许无线客户端之间进行通信 • 启用：禁止无线客户端之间进行通信 缺省情况下，禁用客户端隔离功能 注意 启用客户端隔离后，无线客户端与有线客户端之间依然无法隔离
SSID广播	选择是否广播SSID • 如果启用本功能，当无线客户端搜寻本地可以接入的无线网络时，将检测到广播的SSID，从而可以建立连接 • 如果禁用该功能，则需要管理员向用户知会其 SSID 名称和密码，用户才可以根据 SSID 名称接入无线网络 缺省情况下，启用SSID广播
允许接入客户端数	设置允许多少个无线客户端接入该SSID，取值范围为0～32 缺省情况下，允许接入的客户端数为 32 个 说明 如您配置了中文 SSID，会同时支持 UTF-8 和 GB2312 两种编码格式，每种编码格式的 SSID 都支持所设置的允许接入客户端数
加密方式	选择加密方式，不加密或WPA-PSK/WPA2-PSK加密。建议选择WPA-PSK/WPA2-PSK加密，以提供更高的网络安全性 缺省情况下，不加密 说明 如您选择加密方式为“不加密”时，则无需设置共享密钥、加密协议与群组密钥更新周期
共享密钥	如果选择加密，则输入此密钥才能连接上SSID，长度范围为8～63个字符
加密协议（选择Mixed WPA/WPA2-个人加密时）	选择加密协议 • TKIP：暂时密钥完整性协议 • AES：先进加密标准 • TKIP+AES：使用多种加密方式 缺省情况下，加密协议为AES
群组密钥更新周期	设备会根据所设定的时间定期更新密钥，单位为秒 缺省情况下，群组密钥更新周期为3600

2. 接入控制

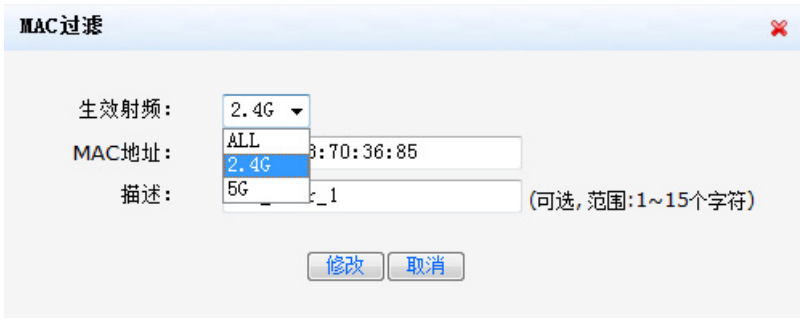
您可以通过本页面设置无线网络的 MAC 地址接入控制功能。本页面配置仅对设备本身的无线网络生效，不对设备的下接 AP 生效。

页面向导：无线管理→高级设置→接入控制

本页面为您提供如下主要功能：

开启/关闭MAC地址接入控制功能（选中“启用MAC地址接入控制功能”，并选择相应的MAC接入无线网络功能，单击<应用>按钮生效）

添加MAC地址（单击主页面上的<新增>按钮，在弹出的对话框中选择生效射频并输入MAC地址和描述信息，单击<增加>按钮生效）



从接入客户端列表导入MAC地址（单击主页面上的<从接入客户列表导入>按钮，在弹出的对话框中选择生效的射频并选择待导入的表项，单击<导入到MAC地址过滤表>按钮生效）

页面中关键项的含义如下表所示。

表6-4 页面关键项描述

页面关键项	描述
启用MAC地址接入控制功能	选中该项启用MAC地址过滤功能，否则允许所有客户端计算机接入无线网络
仅允许MAC地址列表中的MAC接入	选中该项表示仅允许MAC地址表中的客户端计算机接入无线网络
仅禁止MAC地址列表中的MAC接入	选中该项表示仅禁止MAC地址表中的客户端计算机接入无线网络
生效射频	用于控制MAC表项中的地址在哪个射频上生效，可以选择在2.4G射频上或5G射频上生效，也可以选择在两个射频上同时生效 缺省情况下，在两个射频上同时生效
MAC地址	客户端计算机的MAC地址，输入格式为xx:xx:xx:xx:xx:xx（或xx-xx-xx-xx-xx-xx、或xxxx-xxxx-xxxx），且不区分大小写
描述	MAC地址的说明信息

3. 高级参数设置

页面向导：无线管理→高级设置→高级参数设置

本页面为您提供如下主要功能：

无线网络高级设置

- 设置 2.4G 和 5G 无线网络的高级属性（比如：无线网络模式、无线网络信道频宽、无线信道、发射功率、二层漫游、信号切换阈值、禁止弱信号客户端接入、禁止接入信号强度、广播探测等）
- 单击标题栏切换 2.4G 和 5G 配置列表，单击<应用>按钮生效

页面中关键项的含义如下表所示。

表6-5 页面关键项描述

页面关键项	描述

无线网络模式	• 选择 2.4G 无线网络工作模式：
	  ○ b-only 模式：设备工作在 802.11b 模式下
	  ○ g-only 模式：设备工作在 802.11g 模式下
	  ○ b+g 模式：设备工作在 802.11b/g 的混合模式下
	  ○ n-only 模式：设备工作在 802.11n 模式下
	  ○ b+g+n 模式：设备工作在 802.11b/g/n 的混合模式下
	• 选择 5G 无线网络工作模式：
	  ○ a+n 模式：设备工作在 802.11a/n 的混合模式下
	  ○ a+n+ac 模式：设备工作在 802.11a/n/ac 的混合模式下
	缺省情况下，2.4G无线网络模式为b+g+n模式，5G无线网络模式为a+n+ac模式

无线网络频宽	• 选择 2.4G 无线网络的工作频宽：
	  ○ 当无线模式选择“b+g+n”或“n-only”时，可选 20MHz、20/40MHz 或 40MHz
	  ○ 其余工作模式下均为 20MHz
	• 选择 5G 无线网络的工作频宽：
	  ○ 当无线模式选择“a+n”时，可选 20MHz、20/40MHz 或 40MHz
	  ○ 当无线模式选择“a+n+ac”时，可选 20MHz、20/40MHz、40MHz 或 80MHz
	缺省情况下，2.4G和5G的网络频宽均为20MHz

页面关键项	描述
无线信道	选择无线网络的工作信道（频道） 为了提升网络性能，请尽量选择设备工作环境中未被使用的信道 缺省情况下，无线信道为AUTO 说明 在 AUTO 模式下，设备会自动选择一个合适的无线信道
发射功率	调节无线发射功率，值越大，覆盖范围越大，信号越好 缺省情况下，发射功率为100%
二层漫游	启用/禁用二层漫游功能，启用二层漫游功能可以让无线客户端切换到较强信号的AP上 缺省情况下，二层漫游功能禁用
信号切换阈值	若启用二层漫游功能，则需设置信号切换阈值，主要用于无线客户端在不同的AP之间切换。当客户端的信号强度低于此阈值时，客户端会被踢下线，去尝试连接信号强的AP 缺省情况下，信号切换阈值为-75dBm
禁止弱信号客户端接入	启用/禁用禁止弱信号客户端接入功能，启用禁止弱信号客户端接入功能可以让弱信号的无线客户端无法接入到AP上 缺省情况下，禁止弱信号客户端接入功能禁用
禁止接入信号强度	若启用禁止弱信号客户端接入功能，则需设置禁止接入信号强度值。当无线客户端的信号强度低于此值时，客户端将无法连接上AP 缺省情况下，禁止接入信号强度为-80dBm
广播探测	启用/禁用广播探测功能，启用广播探测功能，AP会响应客户端的探测 缺省情况下，广播探测功能为启用

6.2.3 AP管理

1. AP管理设置

通过 AP 管理设置开启管理 AP 功能，如果启用管理 AP 功能，需要设置管理 VLAN。

提示

如需设置 AP 管理相关功能（如在线 AP 管理、配置管理等），请先启用 AP 管理功能，否则 AP 管理相关功能处于关闭状态。

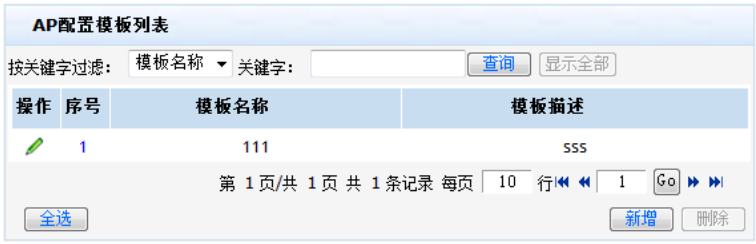
页面向导：无线管理→AP 管理→AP 管理设置

启用AP管理功能，选择AP管理使用VLAN，单击<应用>按钮，完成设置	

2. AP模板管理

设备的无线配置会作为默认模板下发给 AP。如 AP 需要更多不同的配置，您可以通过配置本页面，添加不同的 AP 配置模板。当有 AP 上线时，可以绑定某一个 AP 配置模板。

页面向导：无线管理→AP 管理→AP 模板管理

在AP配置模板列表中查看、新增或删除模板 • 单击<新增>按钮，可以添加新的 AP 配置模板 • 选择要删除的配置模板，单击<删除>按钮，再单击<确定>按钮便可删除该配置模板	
添加新的AP配置模板 • 单击<新增>按钮，弹出 AP 配置模板页面 • 设置模板名称和模板描述 • 设置无线网络模式、频宽、无线信道、发射功率等无线参数 • 单击<新增>按钮，在弹出的页面中 设置无线网络SSID • 单击<添加>按钮，完成 AP 配置模板设置	

设置无线网络SSID

- 设置 SSID 名称和加密方式，如果 SSID 输入了中文，会弹出中文编码格式供选择，且可以点击了解编码详情
- 勾选“高级设置”后，可设置客户端隔离、SSID 广播、客户端数量、桥接 VLAN 等参数
- 单击<增加>按钮，完成 SSID 设置

注意

- 因为 802.11n 不支持 TKIP 加密协议，所以当无线网络模式设置为“n-only”模式时，无法选用 TKIP。此外，当无线网络模式设置为“b+g+n”时，推荐您把加密设置为 AES，而不是 TKIP，否则无线 AP 将不能提供 802.11n 的高速率数据传输服务。
- 当您发现无线网络运行不稳定时，请尝试换用其他的无线信道。

页面中关键项的含义如下表所示。

表6-6 页面关键项描述

页面关键项	描述
模板名称	配置模板的名称
模板描述	配置模板的描述信息

无线网络模式	• 选择 2.4G 无线网络工作模式：
	  ○ b-only 模式：设备工作在 802.11b 模式下
	  ○ g-only 模式：设备工作在 802.11g 模式下
	  ○ b+g 模式：设备工作在 802.11b/g 的混合模式下
	  ○ n-only 模式：设备工作在 802.11n 模式下
	  ○ b+g+n 模式：设备工作在 802.11b/g/n 的混合模式下
	• 选择 5G 无线网络工作模式：
	  ○ a+n 模式：设备工作在 802.11a/n 的混合模式下
	  ○ a+n+ac 模式：设备工作在 802.11a/n/ac 的混合模式下
	缺省情况下，2.4G无线网络模式为b+g+n模式，5G无线网络模式为a+n+ac模式

页面关键项	描述

无线网络频宽	• 选择 2.4G 无线网络的工作频宽：
	  ○ 当无线模式选择“b+g+n”或“n-only”时，可选 20MHz、20/40MHz 或 40MHz
	  ○ 其余工作模式下均为 20MHz
	• 选择 5G 无线网络的工作频宽：
	  ○ 当无线模式选择“a+n”时，可选 20MHz、20/40MHz 或 40MHz
	  ○ 当无线模式选择“a+n+ac”时，可选 20MHz、20/40MHz、40MHz 或 80MHz
	缺省情况下，2.4G和5G的网络频宽均为20MHz

无线信道	选择无线网络的工作信道（频道） 为了提升网络性能，请尽量选择设备工作环境中未被使用的信道。AP的2.4G所有SSID共用同一个信道，5G所有SSID共用同一个信道 缺省情况下，无线信道为AUTO 说明 在 AUTO 模式下，AP 会自动选择一个合适的无线信道
发射功率	调节无线发射功率，值越大，覆盖范围越大，信号越好
SSID名称	设置无线网络使用的SSID名称 不同的SSID用于区分不同的无线网络
中文编码选择	配置SSID名称时，若输入中文，需要选择相应的编码格式GB2312或UTF-8 不同的客户端对中文编码格式支持情况不同，部分客户端仅支持GB2312或UTF-8其中一种编码格式，具体信息可通过点击了解编码详情获取 缺省情况下，输入中文后，编码格式为UTF-8
加密方式	选择加密方式 建议使用WPA-PSK/WPA2-PSK加密方式，以提供更高的网络安全性 缺省情况下，不加密
共享密钥	WPA共享密钥，输入一个8～63字符的字符串
加密协议	选择加密协议 • TKIP：暂时密钥完整性协议 • AES：先进加密标准 • TKIP+AES：自动协商使用 TKIP 或 AES 缺省情况下，加密协议为AES
群组密钥更新周期	设备会根据时间定期更新密钥，单位为秒 缺省情况下，群组密钥更新周期为3600
客户端隔离	选择与某个SSID建立连接的无线客户端之间是否可以互相通信 • 禁用：允许无线客户端之间进行通信 • 启用：禁止无线客户端之间进行通信 缺省情况下，禁用客户端隔离功能 注意 启用客户端隔离后，无线客户端与有线客户端之间依然无法隔离

页面关键项	描述
SSID广播	选择是否广播SSID • 启用本功能，当无线客户端搜寻本地可以接入的无线网络时，将检测到广播的 SSID，从而可以建立连接 • 禁用该功能，则需要管理员向用户知会其 SSID 名称和密码，用户才可以根据 SSID 名称接入无线网络 缺省情况下，启用SSID广播
客户端数量	SSID最大能够接入的无线客户端数量，默认值为AP的客户端默认数量值 若无线管理器上配置的值大于AP允许接入的客户端最大值，则以AP允许接入的客户端最大值为准
桥接VLAN	设置AP桥接VLAN的值，取值范围为1～4094，默认为VLAN 1

3. AP版本管理

AP 版本信息显示管理器上是否上传了或从云平台上下载了 AP 的最新版本。如果上传了或下载了，则会显示当前的版本信息，并且可以通过<删除>按钮，删除该版本。

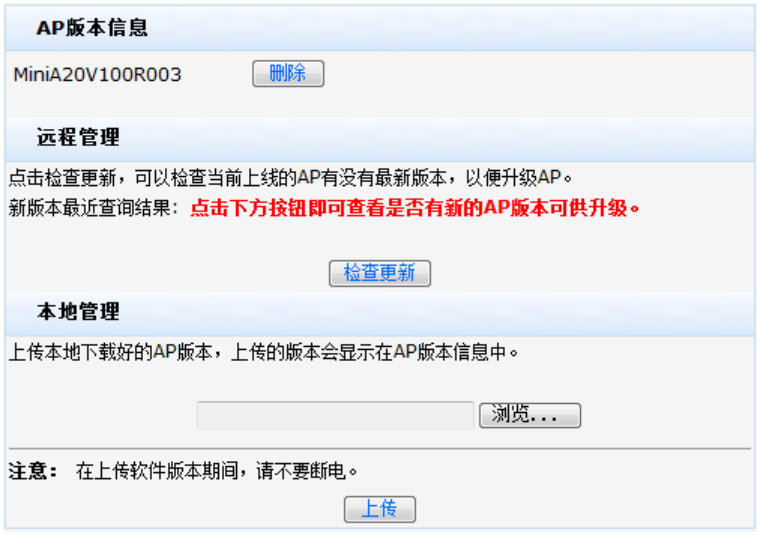
您可以通过远程管理功能，将最新的 AP 版本从云平台上下载至管理器。也可通过本地管理功能，将最新的 AP 版本上传至管理器。

说明

远程管理或本地管理的 AP 版本均保存在设备内存中，在设备重启后，该版本会丢失。

页面向导：无线管理→AP 管理→AP 版本管理

- AP 版本信息，单击<删除>按钮便可删除相应的 AP 版本
- 远程管理，单击<检查更新>按钮，可以检查在线 AP 是否有最新版本，若有便可将版本下载至管理器
- 本地管理，单击<浏览...>按钮，在弹出的对话框中选择需要上传的 AP 版本文件，单击<上传>按钮便可上传该软件版本）
- 关于当前最新 AP 版本，可咨询 H3C 技术支持人员



页面中关键项的含义如下表所示。

表6-7 页面关键项描述

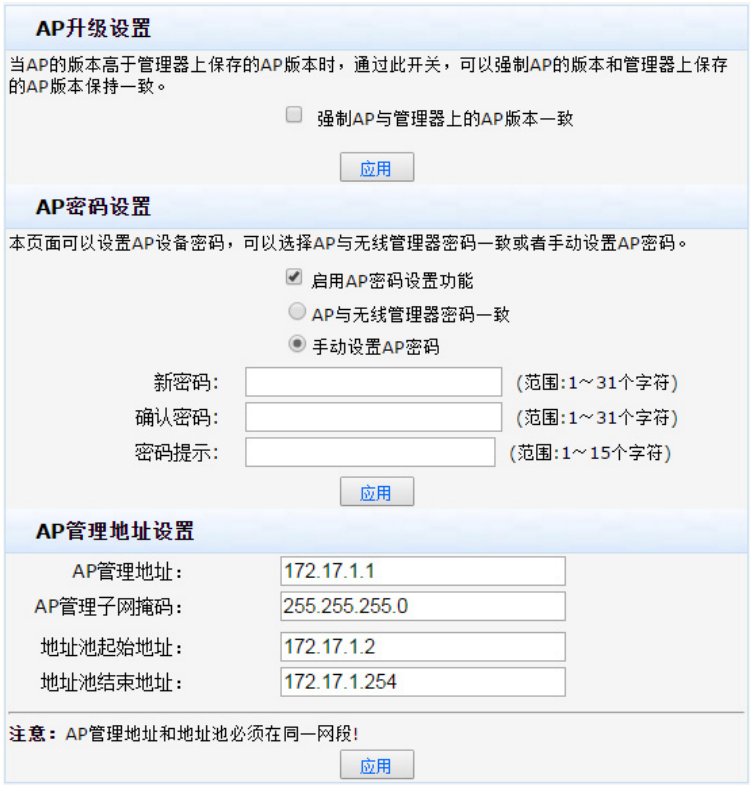
页面关键项	描述
AP版本信息	管理器上保存的AP版本
远程管理	通过云平台将AP软件版本下载到管理器
本地管理	将本地的AP软件版本上传到管理器

4. AP高级管理

- AP 升级设置：当 AP 上运行的版本高于管理器上保存的 AP 版本时，通过强制 AP 与管理器上的 AP 版本一致功能，可以将 AP 的版本强制升级为管理器上的 AP 版本。
- AP 密码设置：用于集中管理 AP 的登录密码。当启用 AP 密码设置功能后，可以选择 AP 与管理器密码一致，也可以手动设置 AP 密码。
- AP 管理地址设置：用于为 AP 分配管理地址。

页面向导：无线管理→AP 管理→AP 高级管理

- AP 升级设置（启用强制 AP 与管理器上的 AP 版本一致，单击<应用>按钮生效）
- AP 密码设置（启用 AP 密码设置功能，选择 AP 与无线管理器密码一致或选择手动设置 AP 密码，并输入新密码，单击<应用>按钮生效）
- AP 管理地址设置
  - 设置管理器管理 AP 的私有管理地址，可以通过该地址登录管理器管理页面，进行管理操作。注意该地址不能与现网路由器地址冲突
  - 设置 AP 注册成功后分配的 IP 地址池起始地址。注意 AP 注册成功后不能使用默认地址访问，必须使用管理器分配的 IP 地址访问



页面中关键项的含义如下表所示。

表6-8 页面关键项描述

页面关键项	描述
强制AP与管理器上的AP版本一致	将AP上运行的版本强制升级成与管理器上的AP版本一致
启用AP密码设置功能	开启AP密码管理功能

页面关键项	描述
AP与无线管理器密码一致	选择AP的密码与无线管理器的密码一致
手动设置AP密码	手动设置AP的密码
AP管理地址	设置AP管理地址
AP管理子网掩码	设置AP管理地址对应的子网掩码
地址池起始地址	设置地址池的起始地址，必须与AP管理地址设置在同一子网内
地址池结束地址	设置地址池的结束地址，必须与AP管理地址设置在同一子网内。地址池结束地址不能小于地址池起始地址

6.2.4 在线列表

1. 在线AP列表

在线 AP 列表包括 AP 统计信息和在线 AP 列表。通过 AP 统计信息，可以知道管理器最大支持 AP 数量，以及当前已接入的 AP 数量。在线 AP 列表中，你可以查看所有在线或离线的 AP 信息，包括 IP 地址、MAC 地址、状态、配置模板、信道等。其中红色条目指表项异常，如：检测到 AP 的状态显示为版本升级异常、配置同步异常或离线。

页面向导：无线管理→在线列表→在线 AP 列表

- 如果 AP 的版本低于当前管理器上的 AP 版本，或 AP 显示版本升级异常，通过<版本升级>按钮，可以给一个或多个在线 AP 手动升级到最新的版本
- 如果 AP 显示配置同步异常，通过<配置同步>按钮，可以给一个或多个在线 AP 手动进行配置同步
- 通过<删除离线记录>按钮，可以删除一个或多个离线 AP 的配置信息记录

- 查看在线 AP 的详细接入信息（单击主页面列表中的<详细>按钮，单击<关闭>按钮完成操作）

页面中关键项的含义如下表所示。

表6-9 页面关键项描述

页面关键项	描述
AP型号	显示当前接入的AP型号
IP地址	显示管理AP的私有IP地址
条码SN	显示在线AP的条码SN
AP版本号	显示在线AP的版本号
MAC	显示在线AP的MAC地址
状态	显示当前AP注册运行过程中的各种操作状态，包括正常、初始化、版本升级、版本升级异常、配置同步、配置同步异常和离线
配置模板	显示在线AP使用的模板信息
信道	显示AP的2.4G的工作信道
5G信道	显示AP的5G的工作信道
AP客户端数量	显示接入当前AP的客户端数量，点击可查看该AP的无线客户端接入信息
AP端口状态	显示AP的端口速率和双工模式
备注	用户对AP的自定义管理信息
详细	点击详细，用户可以查看到该在线AP的详细接入信息

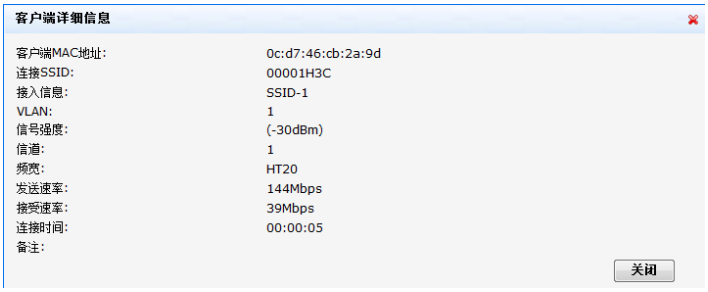
2. 客户端列表

通过客户端列表查看所有通过无线网络接入的客户端信息。包括客户端 MAC 地址、连接 SSID、接入信息、VLAN、信号强度、发送/接收速率、连接时间等。

页面向导：无线管理→在线列表→客户端列表

- 查看无线客户端的接入信息
- 选择需要释放的无线客户端，单击<释放>按钮，在弹出的页面中单击<确定>，完成释放操作

- 查看无线客户端的详细接入信息（单击主页面列表中的<详细>按钮，单击<关闭>按钮完成操作）



页面中关键项的含义如下表所示。

表6-10 页面关键项描述

页面关键项	描述
客户端MAC地址	连接到AP的无线客户端的MAC地址
连接SSID	无线客户端连接到AP的SSID名称
接入信息	无线客户端连接的AP信息或无线管理器的SSID信息
VLAN	无线客户端连接的SSID桥接的VLAN，表示客户端在这个VLAN内通信
信号强度	表示AP跟客户端之间的无线信号质量
信道	AP无线网络的工作信道
频宽	无线客户端跟AP之间协商的工作频宽
发送速率	无线AP的实时发送速率
接收速率	无线客户端的实时发送速率
连接时间	无线客户端连接到AP的总时长
备注	无线客户端连接的AP的备注信息
详细	点击详细，用户可以查看到该无线客户端的详细接入信息

7 上网管理

本章节主要包含以下内容：

7.1 简介

7.1.1 背景介绍

伴随互联网的应用越来越广泛，传统的 WEB 服务承载了越来越多的业务，各种各样的信息通过 WEB 方式提供给用户。WEB 使用者通过网络获取了大量的信息，同样不法之徒也通过网络将非法信息和内容进行传播，基于上网行为的管理技术越来越成为各个企业管理者关注的部分。通过对上网行为的管理，对访问行为进行过滤，使得企业内部的信息得到保护，更使得企业管理者时刻掌握着 WEB 服务的安全性和合法性，因此上网行为管理成为了各类网络产品中必不可少的功能之一。

7.1.2 特性介绍

上网管理主要实现如下功能：

1. 组管理

- 支持用户组管理，包括列表显示、新增、编辑和删除。
- 支持时间段管理，包括列表显示、新增、编辑和删除。

2. 行为策略管理

支持行为策略管理，包括列表显示、新增、编辑和删除：

- 支持适用用户组的设置，可设置零个或多个用户组。
- 支持适用时间段的设置，可设置零个或多个时间段。
- 支持应用软件的设置，可设置某些金融软件（同花顺、广发至强与国元证券、大智慧与分析家、光大证券）的禁用。
- 支持 IM 软件的设置，可设置 QQ 的禁用。
- 在启用 IM 软件且禁用 QQ 上线的情况下，行为策略管理支持 QQ 特权号码的设置。
- 支持网站过滤的设置。
- 支持文件类型过滤的设置。

3. 行为策略信息

- 支持列表显示行为控制的状态信息。
- 支持通过查询一个 IP 地址或者用户组，把该 IP 地址所属的用户组或者用户组配置的所有行为控制策略通过列表显示出来。
- 支持以用户组为单位显示行为控制状态的详细信息，包括应用控制、IM 软件、网站过滤和文件类型过滤状态的详细信息。

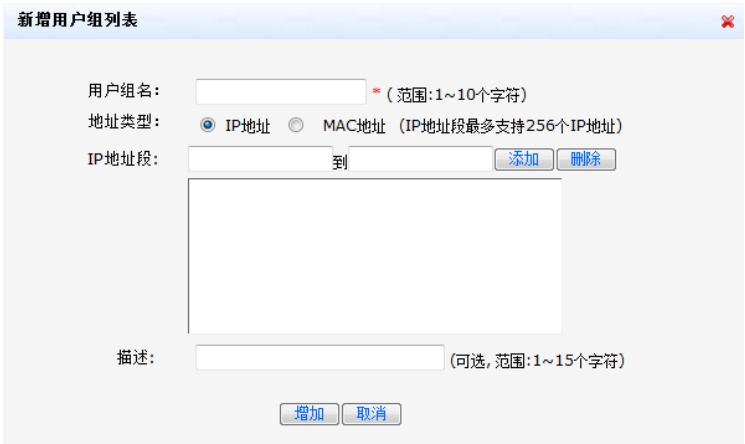
7.2 设置上网管理

7.2.1 组管理

1. 用户组设置

用户组管理设置页面，可以设置用户组名，一条或者多条 IP/MAC 地址以及描述信息。

页面向导：上网管理→组管理→用户组管理

显示和修改已创建的用户组信息（主页面）	
创建新的一条用户组（单击主页面中的<新增>按钮，在弹出的对话框中添加用户组名、IP/MAC地址、描述信息，单击<增加>按钮完成操作）	

页面中关键项的含义如下表所示。

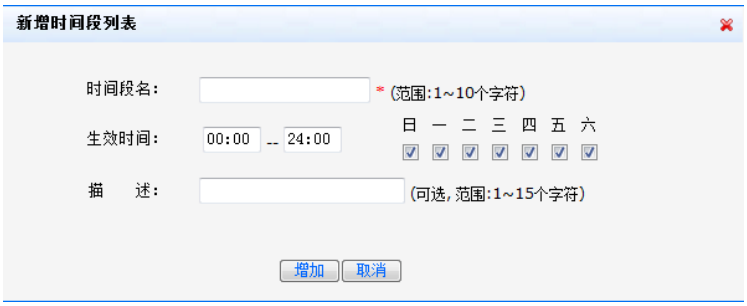
表7-1 页面关键项描述

页面关键项	描述
用户组名	设置用户组的名字。该名字可以提示用户该用户组中的用户特征
地址类型	选择区分该用户所使用的地址类型，可以选择“IP地址”或者“MAC地址”
IP地址段	输入用于标识该用户的IP地址，仅当地址类型选择为“IP地址”类型时，才会显示此配置项
MAC地址	输入用于标识该用户的MAC地址，仅当地址类型选择为“MAC地址”类型时，才会显示此配置项
描述	设置用户组的描述信息

2. 时间段设置

时间段管理设置页面，可以设置时间段名、生效时间以及描述信息。

页面向导：上网管理→组管理→时间段管理

显示和修改已创建的时间段信息（主页面）	
创建新的一条时间段（单击主页面中的<新增>按钮，在弹出的对话框中添加时间段名、生效时间、描述信息，单击<增加>按钮完成操作）	

页面中关键项的含义如下表所示。

表7-2 页面关键项描述

页面关键项	描述
时间段名	设置时间段的名字。该名字可以提示用户该时间段中的时间段特征
生效时间	设置该时间段的生效时间段范围；生效时间包括两部分内容：在一天中生效的时间段，时间使用24小时制，起始时间应早于结束时间，00:00～24:00表示该规则在一天内任何时间都生效；一周中哪些天规则生效
描述	设置该时间段的描述信息

7.2.2 策略管理

策略管理页面，对内网计算机访问外网资源的行为进行统一管理，可以设置包括策略使能、表项序号、策略名称、策略描述、适用用户组、适用时间段、应用软件、IM 软件、QQ 特权号码、网站和文件过滤。

页面向导：上网管理→策略管理→行为策略管理

显示和修改已创建的行为策略管理信息（主页面）	

创建新的一条行为管理策略规则（单击主页面中的<新增>按钮，在弹出的对话框中勾选“启用该策略”，并设置行为管理策略的相关参数，单击<完成策略配置>按钮完成操作）

1. 设置适用用户组

设置该条行为策略的适用用户组，可以设置零条或者多条（零条默认为所有用户组）。

页面向导：上网管理→策略管理→行为策略管理→适用用户组

在弹出的对话框页面中点击“适用用户组”，在所有用户组中双击想要添加的用户组，或者单击想要添加的用户组，再点击 >> 按钮

2. 设置适用时间段

设置该条行为策略的适用时间段，可以设置零条或者多条（零条默认为所有时间段）。

页面向导：上网管理→策略管理→行为策略管理→适用时间段

在弹出的对话框页面中点击“适用时间段”或者单击<下一步>按钮，在所有时间段中双击想要添加的时间段，或者单击想要添加的时间段，再点击 >> 按钮

3. 设置应用软件

设置该条行为策略是否禁用某种应用软件，包括同花顺、广发至强与国元证券、大智慧与分析家、光大证券。

页面向导：上网管理→策略管理→行为策略管理→应用软件

在弹出的对话框页面中点击“应用软件”或者单击<下一步>按钮，勾选“启用应用软件控制功能”复选框，并设置相应参数

4. 设置IM软件

设置该条行为策略是否禁用 IM 软件（QQ）。并且可以设置 RTX 服务器地址。

页面向导：上网管理→策略管理→行为策略管理→IM 软件

在弹出的对话框页面中点击“IM软件”或者单击<下一步>按钮，勾选“启用IM软件控制功能”，并设置相应参数

5. 设置特权QQ号码

如果该条行为策略开启禁止 QQ 上线功能，可以设置是否启用 QQ 特权号码，可以新增、编辑、删除特权 QQ 号码。

页面向导：上网管理→策略管理→行为策略管理→QQ 特权号码

- 在弹出的对话框页面中点击“QQ特权号码”或者单击<下一步>按钮
- 如果在 IM 软件中勾选“禁止 QQ 上线功能”，在该页面中勾选“启用特权 QQ 号码”，并设置相应参数

6. 设置网站过滤

设置该条行为策略是否启用网站过滤功能、网站过滤模式和新增、编辑或者删除网站过滤列表。

页面向导：上网管理→策略管理→行为策略管理→网站过滤

在弹出的对话框页面中点击“网站过滤”或者单击<下一步>按钮，勾选“启用网站过滤功能”，并设置相应参数

7. 设置文件过滤

设置该条行为策略是否启用文件过滤功能和新增、编辑或者删除文件过滤列表。

页面向导：上网管理→策略管理→行为策略管理→文件类型过滤

在弹出的对话框页面中点击“文件类型过滤”或者单击<下一步>按钮，勾选“启用文件类型过滤功能”，并设置相应参数

页面中关键项的含义如下表所示。

表7-3 页面关键项描述

页面关键项	描述
适用用户组	配置适用该行为策略的用户组，可以配置零条或多条，当配置零条时，则默认为所有用户生效
适用时间段	配置适用该行为策略的时间段，可以配置零条或多条，当配置零条时，则默认为所有时间生效
启用应用软件控制功能	选中该项，可以限制内网计算机使用应用软件功能。缺省情况下，不启用该功能
禁止同花顺	选中该项，启用禁止同花顺股票软件的功能，内网的计算机将不能使用同花顺股票软件

页面关键项	描述
禁止广发至强与国元证券	选中该项，启用禁止广发至强版和国元证券软件的功能，内网的计算机将不能使用广发至强版和国元证券软件
禁止大智慧与分析家	选中该项，启用禁止大智慧股票软件和分析家的功能，内网的计算机将不能使用大智慧和分析家
禁止光大证券	选中该项，启用光大证券软件（网上行情）的功能，内网的计算机将不能使用光大证券软件（网上行情）
启用IM软件控制功能	选中该项，可以限制内网计算机使用IM软件功能。缺省情况下，不启用该功能
禁止QQ上线	选中该项，启用禁止应用QQ的功能，内网的计算机将不能登录QQ服务器。缺省情况下，不启用该功能
RTX服务器IP地址	腾讯通RTX（Real Time eXchange）是腾讯公司推出的企业级即时通信平台。RTX与QQ属于类似业务，如需禁止QQ上线但仍需使用RTX，请配置允许访问的RTX服务器IP地址
启用QQ特权号码	选中该项，启用特权QQ号码功能，在“特权号码”列表中的QQ号码被允许使用QQ。缺省情况下，不启用该功能
QQ特权号码	添加到“特权号码”列表的QQ号码被称为“特权号码”。特权号码用户允许使用QQ，非特权号码用户不允许使用QQ
启用网站过滤功能	选中该项，可以通过网站地址对局域网内计算机进行上网控制。缺省情况下，不启用该功能
仅允许访问列表中的网站地址	选中该项，仅允许访问列表中的网站地址。如果您想让局域网内的计算机仅能访问固定的某些网站，可以选中此功能，然后添加相应的网站地址
仅禁止访问列表中的网站地址	选中该项，仅禁止访问列表中的网站地址。如果您想让局域网内的计算机不能访问某些网站（比如：黑客、色情、反动等网站），可以选中此功能，然后添加相应的网站地址
匹配方式	网站地址的匹配方式，可分为精确匹配和模糊匹配
网站地址	需要控制的站点域名或IP地址
导入文件的格式	导入文件必须是.cfg文件。您可以先在本地编辑一个.cfg文件，内容格式为“匹配方式 网站地址 描述”（比如：0(1) www.abc.com desc）  说明 每条表项必须单独为一行，并且行尾不能存在空格
启用文件类型功能	选中该项，可以限制内网的计算机下载的文件类型。缺省情况下，不启用该功能
文件后缀	添加文件类型过滤的后缀名，用于限制该类型文件的下载

7.2.3 策略查看

行为控制信息页面，可以查看以用户组为单位配置的行为管理策略信息。

页面向导：上网管理→策略查看→行为策略状态

显示以组为单位创建的行为策略管理信息（主页面）

查看某个用户组的行为管理策略信息（单击主页面列表中的<详细>按钮，单击<关闭>按钮完成操作）

页面中关键项的含义如下表所示。

表7-4 页面关键项描述

页面关键项	描述
用户组	查看行为策略使用的各个适用用户组组名
应用控制	查看该条用户组应用控制是否开启
IM软件	查看该条用户组IM软件是否开启
网站过滤	查看该条用户组网站过滤是否开启
文件类型过滤	查看该条用户组文件类型过滤是否开启
详细	点击详细，用户可以查看到该条用户组相关的行为管理策略信息

8 云WiFi

本章节主要包含以下内容：

8.1 云WiFi简介

云 WiFi 主要面向企业和公众用户，通过手机号可以注册一个商户账号，该账号可对分散在不同位置的路由器进行统一管理，实现远程监控、远程管理、业务推送、用户管理等功能，适用于无线网络的业务部署。

接入 Internet 网络后，单击设备 Web 管理页面的<注册>按钮进行注册。完成账户注册和设备注册激活后，可通过云管理平台（gate.h3c.com）对用户进行访问控制以及业务推送。

8.2 设置云WiFi

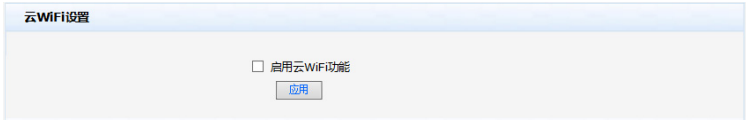
注意

云 WiFi 不支持静态 ARP，请勿执行 ARP 绑定操作。

8.2.1 启用云WiFi功能

页面向导：云 WiFi→云 WiFi 设置→云 WiFi

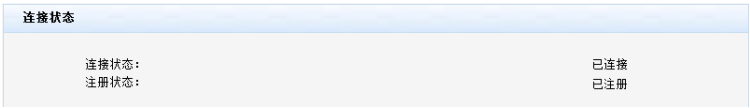
本页面为您提供如下主要功能：

启用云WiFi功能（选中“启用云WiFi功能”复选框，单击<应用>按钮生效）	

8.2.2 查看连接状态

页面向导：云 WiFi→云 WiFi 设置→云 WiFi

本页面为您提供如下主要功能：

显示设备的连接状态和注册状态	

页面中关键项的含义如下表所示。

表8-1 页面关键项描述

页面关键项	描述
连接状态	显示服务器连接状态 • 已连接：设备与服务器连接成功 • 未连接：设备未与服务器建立连接或者与服务器连接失败
注册状态	显示设备注册状态 • 已注册：设备在云管理平台注册成功 • 未注册：设备未在云管理平台注册或者注册失败

8.2.3 注册WiFi管理平台

页面向导：云 WiFi→云 WiFi 设置→云 WiFi

本页面为您提供如下主要功能：

1. 注册 WiFi 管理平台

单击<注册>按钮，弹出云平台注册页面

2. 新设备注册

- 新用户请点击“注册新账户”，进行账户注册
- 已有账户的用户可以直接输入用户名（即注册时使用的手机号）、密码，单击<注册激活>按钮完成设备注册

3. 注册新账户

- 填写手机号、密码并确认密码后，单击<发送验证码>按钮，获取手机验证码后进行填写，并单击<下一步>按钮
- 填写姓名、邮箱、商户名、商户描述等信息。勾选“我同意服务条款和隐私政策”复选框。单击<注册>按钮，完成新账户注册，并跳转至 2新设备注册

4. 注册成功 注册完成后点击“H3C云平台网站”，跳转至云平台页面并自动登录注册账户	

说明

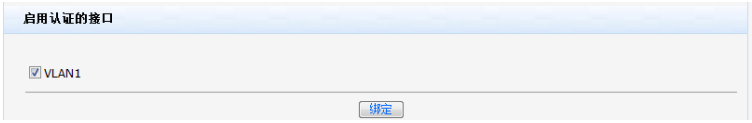
- 注册新账户时只能通过用户输入的手机号进行注册，且该手机号作为账户的用户名使用。
- 一个账户可以注册激活多台设备。

8.2.4 启用认证的接口

接口启用认证后，通过该接口接入的客户端需要通过云 WiFi 认证才能上网。

页面向导：云 WiFi→云 WiFi 设置→云 WiFi

本页面为您提供如下主要功能：

启用认证的接口（选择需要启用认证的接口，单击<绑定>按钮，完成设置）	

9 安全专区

本章节主要包含以下内容：

9.1 设置ARP安全

9.1.1 ARP简介

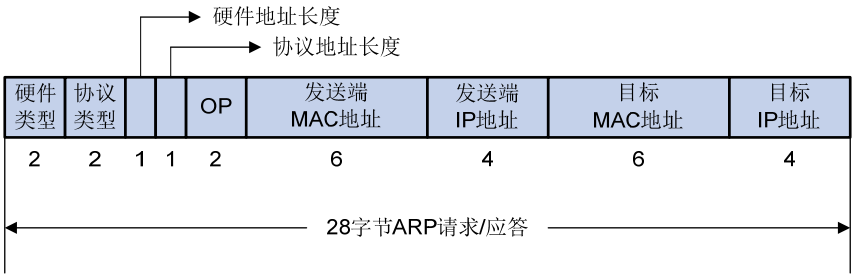
1. ARP作用

ARP 是将 IP 地址解析为以太网 MAC 地址（或称物理地址）的协议。

在局域网中，当主机或其他网络设备有数据要发送给另一个主机或设备时，它必须知道对方的网络层地址（即 IP 地址）。但是仅仅有 IP 地址是不够的，因为 IP 数据报文必须封装成帧才能通过物理网络发送。因此发送方还必须有接收方的物理地址，需要一个从 IP 地址到物理地址的映射。ARP 就是实现这个功能的协议。

2. ARP报文结构

图9-1 ARP 报文结构



- 硬件类型：表示硬件地址的类型。它的值为 1 表示以太网地址。
- 协议类型：表示要映射的协议地址类型。它的值为 0x0800 即表示 IP 地址。
- 硬件地址长度和协议地址长度分别指出硬件地址和协议地址的长度，以字节为单位。对于以太网上 IP 地址的 ARP 请求或应答来说，它们的值分别为 6 和 4。
- 操作类型（OP）：1 表示 ARP 请求，2 表示 ARP 应答。
- 发送端 MAC 地址：发送方设备的硬件地址。
- 发送端 IP 地址：发送方设备的 IP 地址。
- 目标 MAC 地址：接收方设备的硬件地址。
- 目标 IP 地址：接收方设备的 IP 地址。

3. ARP地址解析过程

假设主机A和B在同一个网段，主机A要向主机B发送信息。如 图 9-2 所示，具体的地址解析过程如下：

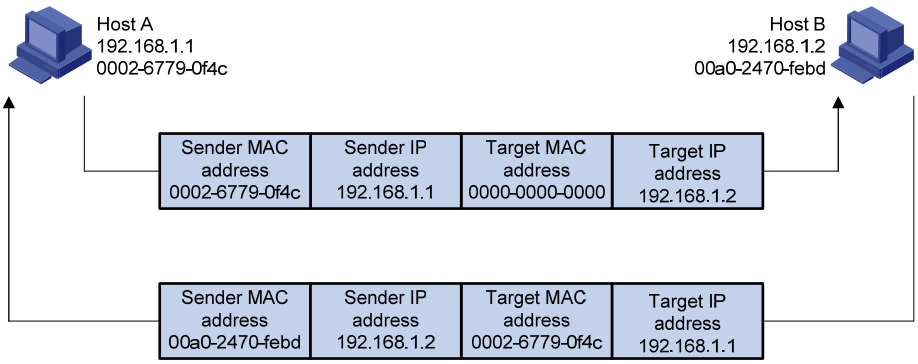
(1) 主机 A 首先查看自己的 ARP 表，确定其中是否包含有主机 B 对应的 ARP 表项。如果找到了对应的 MAC 地址，则主机 A 直接利用 ARP 表中的 MAC 地址，对 IP 数据包进行帧封装，并将数据包发送给主机 B。

(2) 如果主机 A 在 ARP 表中找不到对应的 MAC 地址，则将缓存该数据报文，然后以广播方式发送一个 ARP 请求报文。ARP 请求报文中的发送端 IP 地址和发送端 MAC 地址为主机 A 的 IP 地址和 MAC 地址，目标 IP 地址和目标 MAC 地址为主机 B 的 IP 地址和全 0 的 MAC 地址。由于 ARP 请求报文以广播方式发送，该网段上的所有主机都可以接收到该请求，但只有被请求的主机（即主机 B）会对该请求进行处理。

(3) 主机 B 比较自己的 IP 地址和 ARP 请求报文中的目标 IP 地址，当两者相同时进行如下处理：将 ARP 请求报文中的发送端（即主机 A）的 IP 地址和 MAC 地址存入自己的 ARP 表中。之后以单播方式发送 ARP 响应报文给主机 A，其中包含了自己的 MAC 地址。

(4) 主机 A 收到 ARP 响应报文后，将主机 B 的 MAC 地址加入到自己的 ARP 表中以用于后续报文的转发，同时将 IP 数据包进行封装后发送出去。

图9-2 ARP 地址解析过程



当主机 A 和主机 B 不在同一网段时，主机 A 就会先向网关发出 ARP 请求，ARP 请求报文中的目标 IP 地址为网关的 IP 地址。当主机 A 从收到的响应报文中获得网关的 MAC 地址后，将报文封装并发给网关。如果网关没有主机 B 的 ARP 表项，网关会广播 ARP 请求，目标 IP 地址为主机 B 的 IP 地址，当网关从收到的响应报文中获得主机 B 的 MAC 地址后，就可以将报文发给主机 B；如果网关已经有主机 B 的 ARP 表项，网关直接把报文发给主机 B。

4. ARP表

设备通过 ARP 解析到目的 MAC 地址后，将会在自己的 ARP 表中增加 IP 地址到 MAC 地址的映射表项，以用于后续到同一目的地报文的转发。

ARP 表项分为动态 ARP 表项和静态 ARP 表项。

- 动态 ARP 表项

动态 ARP 表项由 ARP 协议通过 ARP 报文自动生成和维护，会被新的 ARP 报文所更新。

- 静态 ARP 表项

静态 ARP 表项需要通过手工配置和维护，不会被动态的 ARP 表项所覆盖。

配置静态 ARP 表项可以增加通信的安全性。它可以限制和指定 IP 地址的设备通信时只使用指定的 MAC 地址，此时攻击报文无法修改此表项的 IP 地址和 MAC 地址的映射关系，从而保护了本设备和指定设备间的正常通信。

9.1.2 设置ARP绑定

通过设置 ARP 绑定，可以有效地防止路由器的 ARP 表项受到攻击，保证了网络的安全。

1. 设置动态ARP绑定

为了防止通过 DHCP 方式获取 IP 地址的主机在路由器上的 ARP 表项被篡改，您可以开启动态 ARP 绑定功能，使得所有通过 DHCP 服务器分配出去的 IP 地址和其对应的 MAC 地址自动绑定。且动态绑定的表项在地址租约到期后不会被删除。

页面向导：安全专区→ARP 安全→ARP 绑定

页面为您提供如下主要功能：

设置动态ARP绑定（选中“对DHCP分配的地址进行ARP保护”复选框，单击<应用>按钮生效）

说明

开启动态 ARP 绑定后，路由器通过 DHCP 方式获取到的 ARP 表项状态为“动态绑定”。反之，则为“未绑定”。

2. 设置静态ARP绑定

静态 ARP 绑定即需要通过手工配置和维护。建议您将局域网内所有主机都添加到路由器的静态 ARP 表项中。

页面向导：安全专区→ARP 安全→ARP 绑定

本页面为您提供如下主要功能：

- 显示和修改 ARP 表项（主页面）
- 将动态获取到的 ARP 表项进行绑定（选中动态获取到的表项，单击<静态绑定>按钮即可完成绑定。此时，ARP 表项状态则为“静态绑定”）

单个添加静态ARP表项（单击主页上的<新增>按钮，在弹出的对话框中设置相应的参数，并单击<增加>按钮完成操作）

批量添加静态ARP表项（您可以在本地用“记事本”程序创建一个.cfg文件，内容格式为“MAC地址 IP地址 描述”（比如：00:0A:EB:7F:AA:AB 192.168.1.2 zhangsan），且每条绑定项之间需换行。单击主页面上的<导入>按钮，在弹出的对话框中选择该文件将其导入即可）	
将路由器当前的ARP静态表项备份保存（.cfg文件），且您可用“记事本”程序打开该文件进行编辑（单击主页面上的<导出>按钮，确认后即可将其导出到本地）	

说明

您还可以通过路由器自动搜索在线主机功能来获取ARP表项，然后再将其批量绑定添加到路由器的ARP静态表中。相关操作请参见“9.1.3 设置ARP检测”。

9.1.3 设置ARP检测

通过 ARP 检测功能，您可以快速地搜索到局域网内所有在线的主机，获取相应的 ARP 表项。同时，系统会检测这些表项当前的绑定状态以及是否存在异常（比如：获取的表项是否和路由器的静态 ARP 表项存在冲突等），并在页面的列表中以不同的颜色加以标明，帮助您更直观地对 ARP 表项进行判断和维护。

页面向导：安全专区→ARP 安全→ARP 检测

本页面为您提供如下主要功能：

• 搜索在线主机，获取 ARP 表项（输入指定的地址范围，单击<扫描>按钮即可。如果您想清除当前的搜索结果，请单击<清除结果>按钮） • 将获取到的、未绑定的 ARP 表项进行批量绑定(选中未绑定项，单击<静态绑定>按钮即可）	

9.1.4 设置发送免费ARP

免费 ARP 报文是一种特殊的 ARP 报文，该报文中携带的发送端 IP 地址和目标 IP 地址都是本机 IP 地址，报文源 MAC 地址是本机 MAC 地址，报文的目的 MAC 地址是广播地址。

设备通过对外发送免费 ARP 报文来实现以下功能：

- 确定其他设备的 IP 地址是否与本机的 IP 地址冲突。当其他设备收到免费 ARP 报文后，如果发现报文中的 IP 地址和自己的 IP 地址相同，则给发送免费 ARP 报文的设备返回一个 ARP 应答，告知该设备 IP 地址冲突。
- 设备改变了硬件地址，通过发送免费 ARP 报文通知其他设备更新 ARP 表项。

路由器支持定时发送免费 ARP 功能，这样可以及时通知其他设备更新 ARP 表项或者 MAC 地址表项，主要应用场景如下：

- 防止仿冒网关的 ARP 攻击

如果攻击者仿冒网关发送免费 ARP 报文，就可以欺骗同网段内的其他主机，使得被欺骗的主机访问网关的流量，被重定向到一个错误的 MAC 地址，导致其他用户无法正常访问网络。

为了尽量避免这种仿冒网关的 ARP 攻击，可以在网关的接口上开启定时发送免费 ARP 功能。开启该功能后，网关接口上将按照配置的时间间隔周期性发送接口主 IP 地址的免费 ARP 报文。这样，每台主机都可以学习到正确的网关，从而正常访问网络。

- 防止主机 ARP 表项老化

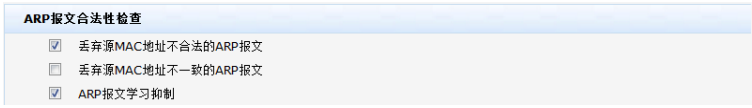
在实际环境中，当网络负载较大或接收端主机的 CPU 占用率较高时，可能存在 ARP 报文被丢弃或主机无法及时处理接收到的 ARP 报文等现象。这种情况下，接收端主机的动态 ARP 表项会因超时而被老化，在其重新学习到发送设备的 ARP 表项之前，二者之间的流量就会发生中断。

为了解决上述问题，您可以在路由器的接口上开启定时发送免费 ARP 功能。开启该功能后，路由器接口上将按照配置的时间间隔周期性地发送接口主 IP 地址的免费 ARP 报文。这样，接收端主机可以及时更新 ARP 映射表，从而防止了上述流量中断现象。

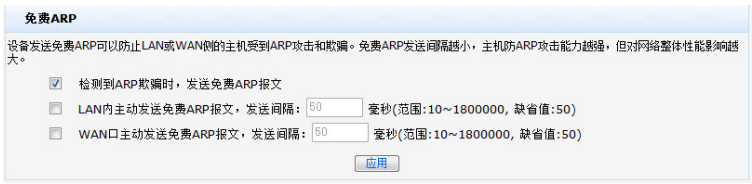
页面向导：安全专区→ARP 安全→ARP 防护

本页面为您提供如下主要功能：

- 设置路由器丢弃源 MAC 地址不合法的 ARP 报文，即选中该功能后，当设备接收到的 ARP 报文的源 MAC 地址为 0、组播 MAC 地址或广播 MAC 地址时，则直接将其丢弃不对其进行 ARP 学习（缺省情况下，此功能处于开启状态）
- 设置路由器丢弃源 MAC 地址不一致的报文，即选中该功能后，当设备接收到的 ARP 报文的源 MAC 地址与该报文的二层源 MAC 地址不一致时（通常情况下，认为存在 ARP 欺骗），则直接将其丢弃，不对其进行 ARP 学习（缺省情况下，此功能处于关闭状态）
- 设置路由器 ARP 报文学习抑制，即选中该功能后，设备在一段时间内只学习第一个返回的 ARP 响应报文，丢弃其他响应报文，从而防止有过多的 ARP 响应报文返回造成 ARP 表项异常（缺省情况下，此功能处于开启状态）



- 设置路由器检测到 ARP 欺骗时，LAN 口或 WAN 口会主动发送免费 ARP（缺省情况下，此功能处于开启状态）
- 设置路由器 LAN 口主动定时发送免费 ARP（缺省情况下，此功能处于关闭状态）
- 设置路由器 WAN 口主动定时发送免费 ARP（缺省情况下，此功能处于关闭状态）



9.2 设置接入控制

9.2.1 设置MAC过滤

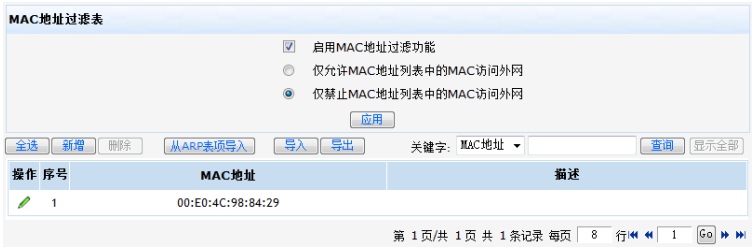
通过 MAC 过滤功能，您可以有效地控制局域网内的主机访问外网。路由器为您提供两种 MAC 过滤功能：

- 仅允许 MAC 地址列表中的 MAC 访问外网：如果您仅允许局域网内的某些主机访问外网，可以选中此功能，并添加相应的主机 MAC 地址表项。
- 仅禁止 MAC 地址列表中的 MAC 访问外网：如果您想禁止局域网内的某些主机访问外网，可以选中此功能，并添加相应的主机 MAC 地址表项。

页面向导：安全专区→接入控制→MAC 过滤

本页面为您提供如下主要功能：

根据实际需求启用相应的MAC过滤功能（主页面。选择相应的MAC过滤功能后，单击<应用>按钮生效）



单个添加MAC过滤表项（单击主页面上的<新增>按钮，在弹出的对话框中添加一个需要过滤的MAC地址，单击<增加>按钮完成操作）

通过导入路由器的ARP绑定表来批量添加MAC过滤表项（单击主页面上的<从ARP表项导入>按钮，在弹出的对话框中选择需要过滤的MAC地址，单击<导入到MAC地址过滤表>按钮完成操作）

通过配置文件批量添加MAC过滤表项（您可以在本地用“记事本”程序创建一个.cfg文件，内容格式为“MAC地址 描述”，且每条过滤项之间需要换行。单击主页面上的<导入>按钮，在弹出的对话框中选择该文件将其导入即可）

将当前您需要进行过滤处理的MAC地址保存（.cfg文件），且您可用“记事本”程序打开该文件进行编辑（单击主页面上的<导出>按钮，确认后即可将其导出到本地）

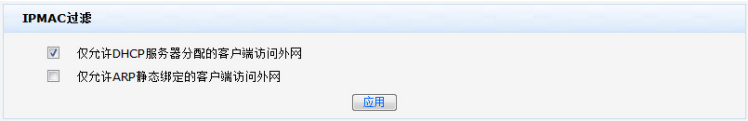
9.2.2 设置IPMAC过滤

IPMAC 过滤功能可以同时对报文中的源 MAC 地址和源 IP 地址进行匹配，仅当源 MAC 地址和源 IP 地址均符合条件的主机才允许访问外网。IPMAC 过滤功能支持以下两种匹配方式：

- 仅允许 DHCP 服务器分配的客户端访问外网：即开启此功能后，不在路由器 DHCP 服务器分配的客户列表中的用户将无法访问外网。此方式可以运用于企业环境中，因为企业通常使用 DHCP 方式为客户端分配 IP 地址。
- 仅允许 ARP 静态绑定的客户端访问外网：即开启此功能后，不在 ARP 静态绑定表中的客户端将无法访问外网。此方式可以运用于网吧环境中，因为网吧通常为客户端设置静态 IP 地址。

页面向导：安全专区→接入控制→IPMAC 过滤

本页面为您提供如下主要功能：

设置IPMAC过滤功能（选择相应的IPMAC过滤匹配方式，单击<应用>按钮生效）	

9.3 设置防火墙

路由器的防火墙功能为您实现了根据报文的内容特征（比如：协议类型、源/目的 IP 地址等），来对入站方向（从因特网发向局域网的方向）和出站方向（从局域网发向因特网的方向）的数据流进行相应的控制，保证了路由器和局域网内主机的安全运行。

9.3.1 开启/关闭防火墙功能

仅当防火墙功能开启后，您定制的防火墙出站和入站通信策略才能生效。

页面向导：安全专区→防火墙→防火墙设置

本页面为您提供如下主要功能：

开启/关闭防火墙功能	

9.3.2 设置出站通信策略

页面向导：安全专区→防火墙→出站通信策略

本页面为您提供如下主要功能：

设置报文在出站方向上未匹配任何您预先设定的规则时，系统所采取的策略（主页面。在“出站通信缺省策略”下拉框中选择指定的方式，单击<应用>按钮生效）

添加匹配规则来控制指定的报文（在主页面上单击<新增>按钮，在弹出的对话框中设置相应的匹配项，单击<增加>按钮完成操作）

页面中关键项的含义如下表所示。

表9-1 页面关键项描述

页面关键项	描述
出站通信缺省策略	• “允许”：允许内网主动发起的访问报文通过 • “禁止”：禁止内网主动发起的访问报文通过 缺省情况下，出站通信缺省策略为“允许” **说明** • 当缺省策略是“允许”时，您手动添加的策略即为“禁止”，反之亦然 • 缺省策略更改后，所有已配置的出站通信策略将会被清空，且仅对新建立的访问连接生效 • 当您手动添加了出站通信策略后，系统会优先根据该策略对主机进行访问控制，如果未匹配手动添加的策略，则遵循缺省策略
源接口	设置报文的来源接口，即可以对从某一LAN侧接口收到的报文进行控制
源地址	设置需要进行控制的源地址类型： • IP 地址段：通过源 IP 地址范围对局域网中的主机进行控制 • MAC 地址：通过源 MAC 地址对局域网中的主机进行控制 • 用户组：通过您预先划分好的用户组对局域网中的主机进行控制

页面关键项	描述
起始IP/结束IP（源IP地址范围）	输入需要匹配的报文的源IP地址段 说明 • 起始 IP 地址不能大于结束 IP 地址 • 如果无需匹配报文的源 IP 地址，您可以将起始 IP 地址设置为 0.0.0.0，结束 IP 地址设置为 255.255.255.255
源端口范围	输入需要匹配的报文的源端口范围 说明 如果无需匹配报文的源端口号，您可以将其设置为 1～65535
起始IP/结束IP（目的IP地址范围）	输入需要匹配的报文的目的IP地址段 说明 • 起始 IP 地址不能大于目的 IP 地址 • 如果无需匹配报文的目的 IP 地址，您可以将起始 IP 地址设置为 0.0.0.0，结束 IP 地址设置为 255.255.255.255
服务类型	选择局域网中主机访问因特网资源的服务类型 说明 缺省情况下，系统预定义了常用的服务类型。如果您需要自定义服务类型，相关操作请参见“9.3.4 设置服务类型”
生效时间	设置此新增规则的生效时间 说明 生效时间需要您指定具体的时间段，比如：某天的某个时间段
是否启用	在下拉列表框中选择“启用”，表示此匹配策略生效；选择“禁用”，表示此匹配策略不生效
描述	对此新增规则进行简单的描述

9.3.3 设置入站通信策略

页面向导：安全专区→防火墙→入站通信策略

本页面为您提供如下主要功能：

设置报文在入站方向上未匹配任何您预先设定的规则时，系统所采取的策略（主页面。在“入站通信缺省策略”下拉框中选择指定的方式，单击<应用>按钮生效）	

添加匹配规则来控制指定的报文（在主页面上单击<新增>按钮，在弹出的对话框中设置相应的匹配项，单击<增加>按钮完成操作）	

页面中关键项的含义如下表所示。

表9-2 页面关键项描述

页面关键项	描述
入站通信缺省策略	• “禁止”：禁止外网主动发起的访问报文通过 • “允许”：允许外网主动发起的访问报文通过 说明 • 当路由器工作于NAT模式下时（即开启了NAT功能），入站通信缺省策略不允许配置，且仅为“禁止”；当路由器工作于路由模式下时（即关闭了NAT功能），入站通信缺省策略才允许选择配置，且缺省情况下为“允许” • 当缺省策略是“禁止”时，您手动添加的策略即为“允许”，反之亦然 • 缺省策略更改后，所有已配置的出站通信策略将会被清空，且仅对新建立的访问连接生效 • 当您手动添加了入站通信策略后，路由器会优先根据该策略对主机进行访问控制，如果未匹配手动添加的策略，则遵循缺省策略
源接口	设置报文的来源接口，即可以对从某一WAN侧接口收到的报文进行控制
起始IP/结束IP（源IP地址范围）	输入需要匹配的报文的源IP地址段 说明 • 起始 IP 地址不能大于结束 IP 地址 • 如果无需匹配报文的源 IP 地址，您可以将起始 IP 地址设置为 0.0.0.0，结束 IP 地址设置为 255.255.255.255
源端口范围	输入需要匹配的报文的源端口范围 说明 如果无需匹配报文的源端口号，您可以将其设置为 1～65535
目的IP地址（目的IP地址范围）	输入需要匹配的报文的目的IP地址 说明 当路由器工作于NAT模式下时（即开启了NAT功能），仅允许设置单个目的IP地址；当路由器工作于路由模式下时（即关闭了NAT功能），允许设置目的IP地址范围

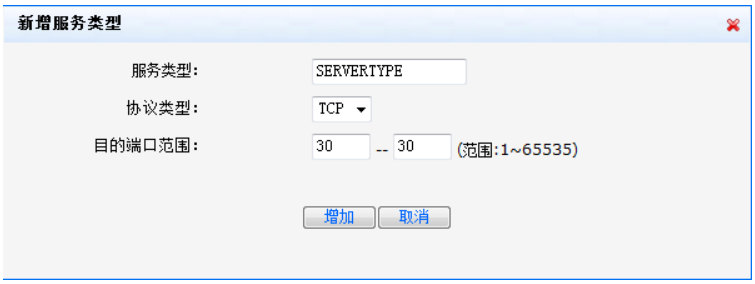
页面关键项	描述
服务类型	选择因特网中的主机访问局域网资源的服务类型 说明 缺省情况下，系统预定义了常用的服务类型。如果您需要自定义服务类型，相关操作请参见“9.3.4 设置服务类型”
生效时间	设置此新增规则的生效时间 说明 生效时间需要您指定具体的时间段，比如：某天的某个时间段
是否启用	在下拉列表框中选择“启用”，表示此匹配策略生效；选择“禁用”，表示此匹配策略不生效
描述	对此新增规则进行简单的描述

9.3.4 设置服务类型

为了让您能够在定制防火墙策略时比较方便地指定需要过滤的协议和端口号，路由器提供了服务类型管理功能。每一个服务类型均由协议和端口号两部分构成，系统预定义一些常用的服务类型（比如：HTTP、FTP、TELNET 等）；同时，您也可以根据实际需求添加自定义的服务类型。

页面向导：安全专区→防火墙→服务类型

本页面为您提供如下主要功能：

显示和修改已定义的服务类型（主页面。系统预定义的服务类型均不可修改和删除）	
自定义服务类型（单击主页面上的<新增>按钮，在弹出的对话框中设置服务类型名称、协议类型及目的端口范围，单击<增加>按钮完成操作）	

9.4 设置防攻击

在复杂网络环境中，常常由于主机异常或中毒，导致其不断地发送一些攻击报文，造成路由器资源和网络带宽不必要的消耗。防攻击主要的目的就是发现并丢弃非法的报文，以保证整体网络的稳定性。

9.4.1 防攻击方式

路由器为您提供了以下三种防攻击方式：

- IDS 防范

IDS 防范主要用于发现一些常见的攻击类型报文对路由器的扫描和一些常见的 DOS 攻击，并丢弃相应的报文。在一定程度上，可以有效地保证路由器的正常运行。

- 报文源认证

攻击类型的报文多种多样，除了 ARP 欺骗外，最主要的是伪装 IP 地址的报文和伪装 MAC 地址的报文。您通过设置路由器的静态路由表和 ARP 表项，可以在很大程度上认证内网发送的报文的合法性。比如：当报文的源 IP 地址属于不可达网段，报文的源 IP 地址/源 MAC 地址和静态 ARP 表项存在冲突等，则路由器会认为该报文是非法伪装的报文，会直接将其丢弃。

- 异常流量防护

在网络实际应用中，往往会由于单台主机中毒或异常，导致这台主机大量发送数据包。而这些报文并不能被路由器的报文源认证功能确定为非法的报文，此时会大量地消耗路由器的资源。开启该功能后，路由器会对各台主机的流量进行检查，并根据您所选择的防护等级（包括：高、中、低三种）进行相应的处理，以确保路由器受到此类异常流量攻击时仍可正常工作。

9.4.2 设置IDS防范

页面向导：安全专区→防攻击→IDS 防范

本页面为您提供如下主要功能：

开启指定攻击类型报文的IDS防范（选中您需要防范的攻击类型，单击<应用>按钮生效）	

说明

- 本页面中的各攻击类型的介绍请参见路由器的在线联机帮助。
- 仅当您选择了“丢弃攻击报文，并记入日志”选项，路由器才会对攻击事件以日志的形式记录。日志信息的查看，请参见“15.2.1 查看日志信息”。

9.4.3 设置报文源认证

页面向导：安全专区→防攻击→报文源认证

本页面为您提供如下主要功能：

选择基于哪个表项（静态路由表、静态ARP表、动态ARP表）来对报文进行源认证（选中相应的功能项，单击<应用>按钮生效）	

页面中关键项的含义如下表所示。

表9-3 页面关键项描述

页面关键项	描述
启用基于静态路由的报文源认证功能	开启该功能后，路由器将根据静态路由表对所有报文的源IP地址进行检查。如果静态路由表中存在到该源IP地址的表项，则转发该报文；否则丢弃该报文 比如：路由器LAN口下挂的设备接口地址为192.168.1.5/24，内网为192.200.200.0/24网段。同时，您设置静态路由目的地址为192.200.200.0/24，下一跳为192.168.1.5，出接口为LAN口。此时，路由器允许从192.200.200.0/24网段转发过来的报文通过
启用基于ARP绑定、DHCP分配ARP防护下的报文源认证功能	开启该功能后，路由器将根据静态ARP表的绑定关系及DHCP分配列表中的对应关系，来认证内网的报文。如果报文的源IP地址/MAC地址与静态ARP表中的IP地址/MAC地址对应关系存在冲突，则路由器将其直接丢弃 比如：您设置了一条ARP静态绑定项（将源IP地址：192.168.1.100与源MAC地址：08:00:12:00:00:01绑定）。当路由器LAN侧收到一个报文，其源IP地址为192.168.1.100，但源MAC地址为08:00:12:00:00:02，路由器会将该报文丢弃
启用基于动态ARP的报文源认证功能	开启该功能，路由器将会根据动态ARP表的对应关系，来认证内网的报文。如果报文的源IP地址/MAC地址与已确认合法的动态ARP表的IP地址/MAC地址对应关系存在冲突，则路由器将其直接丢弃 比如：路由器动态学习到一条ARP表项（源IP地址：192.168.1.100，源MAC地址：08:00:12:00:00:01），当路由器LAN侧在该ARP表项老化之前收到一个报文，其源IP地址为192.168.1.100，但源MAC地址为08:00:12:00:00:02，路由器会将该报文丢弃

说明

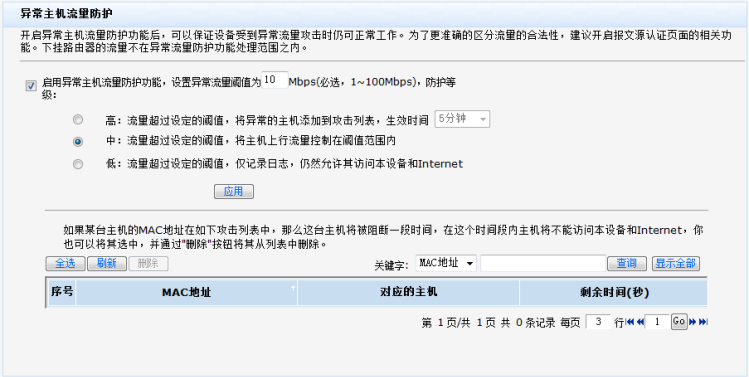
如果您想查看源认证失败的报文的个数，请参见“15.3.3 安全统计”。

9.4.4 设置异常流量防护

页面向导：安全专区→防攻击→异常流量防护

本页面为您提供如下主要功能：

选择防护等级来对异常主机流量进行防护（选中“启用异常主机流量防护功能”复选框，并选择相应的防护等级，单击<应用>按钮生效）



页面中关键项的含义如下表所示。

表9-4 页面关键项描述

页面关键项	描述
高	选中该单选框，路由器会把检查到的攻击主机添加到本页面下方的攻击列表中，并在一段时间内（即您所选择的“生效时间”）禁止其访问路由器和因特网
中	选中该单选框，路由器会把检查到的攻击主机的上行流量限制在异常流量阈值范围内
低	选中该单选框，路由器仅对上行流量超过异常流量阈值的攻击主机以事件的形式记入日志

10 设置IPSec VPN

本章节主要包含以下内容：

10.1 IPSec VPN简介

VPN 是近年来随着 Internet 的广泛应用而迅速发展起来的一种新技术，用以实现在公用网络上构建私人专用网络。“虚拟”主要指这种网络是一种逻辑上的网络。

10.1.1 IPSec简介

IPSec 是 IETF 制定的三层隧道加密协议，它为 Internet 上数据的传输提供了高质量的、可互操作的、基于密码学的安全保证。特定的通信方之间在 IP 层通过加密与数据源认证等方式，可以获得以下的安全服务：

- 数据机密性（Confidentiality）：IPSec 发送方在通过网络传输包前对包进行加密。
- 数据完整性（Data Integrity）：IPSec 接收方对发送方发送来的包进行认证，以确保数据在传输过程中没有被篡改。
- 数据来源认证（Data Authentication）：IPSec 接收方可以认证 IPSec 报文的发送方是否合法。
- 防重放（Anti-Replay）：IPSec 接收方可检测并拒绝接收过时或重复的报文。

可以通过 IKE 为 IPSec 提供自动协商交换密钥、建立和维护 SA 的服务，以简化 IPSec 的使用和管理。IKE 协商并不是必须的，IPSec 所使用的策略和算法等也可以手工协商。

1. IPSec的实现

IPSec 通过如下两种协议来实现安全服务：

- AH 是认证头协议，协议号为 51。主要提供的功能有数据源认证、数据完整性校验和防报文重放功能，可选择的认证算法有 MD5、SHA-1 等。AH 报文头插在标准 IP 包头后面，保证数据包的完整性和真实性，防止黑客截获数据包或向网络中插入伪造的数据包。
- ESP 是报文安全封装协议，协议号为 50。与 AH 协议不同的是，ESP 将需要保护的用户数据进行加密后再封装到 IP 包中，以保证数据的机密性。常见的加密算法有 DES、3DES、AES 等。同时，作为可选项，用户可以选择 MD5、SHA-1 算法保证报文的完整性和真实性。

AH 和 ESP 可以单独使用，也可以联合使用。设备支持的 AH 和 ESP 联合使用的方式为：先对报文进行 ESP 封装，再对报文进行 AH 封装，封装之后的报文从内到外依次是原始 IP 报文、ESP 头、AH 头和外部 IP 头。

2. IPSec基本概念

(1) SA

IPSec 在两个端点之间提供安全通信，端点被称为 IPSec 对等体。

SA 是 IPSec 的基础，也是 IPSec 的本质。SA 是通信对等体间对某些要素的约定，例如，使用哪种协议（AH、ESP 还是两者结合使用）、协议的封装模式（传输模式和隧道模式）、加密算法（DES、3DES 和 AES）、特定流中保护数据的共享密钥以及密钥的生存周期等。

SA 是单向的，在两个对等体之间的双向通信，最少需要两个 SA 来分别对两个方向的数据流进行安全保护。同时，如果两个对等体希望同时使用 AH 和 ESP 来进行安全通信，则每个对等体都会针对每一种协议来构建一个独立的 SA。

SA 由一个三元组来唯一标识，这个三元组包括 SPI（Security Parameter Index，安全参数索引）、目的 IP 地址、安全协议号（AH 或 ESP）。

SPI 是为唯一标识 SA 而生成的一个 32 比特的数值，它在 AH 和 ESP 头中传输。在手工配置 SA 时，需要手工指定 SPI 的取值；使用 IKE 协商产生 SA 时，SPI 将随机生成。

SA 是具有生存周期的，且只对通过 IKE 方式建立的 SA 有效。生存周期到达指定的时间或指定的流量，SA 就会失效。SA 失效前，IKE 将为 IPSec 协商建立新的 SA，这样，在旧的 SA 失效前新的 SA 就已经准备好。在新的 SA 开始协商而没有协商好之前，继续使用旧的 SA 保护通信。在新的 SA 协商好之后，则立即采用新的 SA 保护通信。

(2) 验证算法与加密算法

【验证算法】:

验证算法的实现主要是通过杂凑函数。杂凑函数是一种能够接受任意长的消息输入，并产生固定长度输出的算法，该输出称为消息摘要。IPSec 对等体计算摘要，如果两个摘要是相同的，则表示报文是完整未经篡改的。

IPSec 使用以下两种验证算法：

表10-1 验证算法

验证算法	描述
MD5	MD5通过输入任意长度的消息，产生128bit的消息摘要 与SHA-1相比：计算速度快，但安全强度略低
SHA-1	SHA-1通过输入长度小于2的64次方bit的消息，产生160bit的消息摘要 与MD5相比：计算速度慢，但安全强度更高

【加密算法】:

加密算法实现主要通过对称密钥系统，它使用相同的密钥对数据进行加密和解密。

IPSec 支持以下三种加密算法：

表10-2 加密算法

加密算法	描述
DES	使用64bit的密钥对一个64bit的明文块进行加密
3DES	使用三个64bit的DES密钥（共192bit密钥）对明文进行加密
AES	使用128bit、192bit或256bit密钥长度的AES算法对明文进行加密

说明

这三个加密算法的安全性由高到低依次是：AES、3DES、DES，安全性高的加密算法实现机制复杂，但运算速度慢。对于普通的安全要求，DES 算法就可以满足需要。

(3) 协商方式

有如下两种协商方式建立 SA：

- 手工方式配置比较复杂，创建 SA 所需的全部信息都必须手工配置，而且不支持一些高级特性（例如定时更新密钥），但优点是可以不依赖 IKE 而单独实现 IPSec 功能。
- IKE 自动协商方式相对比较简单，只需要配置好 IKE 协商安全策略的信息，由 IKE 自动协商来创建和维护 SA。

当与之进行通信的对等体设备数量较少时，或是在小型静态环境中，手工配置 SA 是可行的。对于中、大型的动态网络环境中，推荐使用 IKE 协商建立 SA。

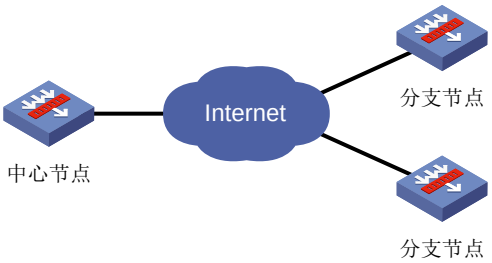
(4) 安全隧道

安全隧道是建立在本端和对端之间可以互通的一个通道，它由一对或多对 SA 组成。

10.1.2 IPSec VPN常见的组网模式

- 中心/分支模式应用在一对多网络中，如 图 10-1 所示。中心/分支模式的网络采用野蛮模式进行IKE协商，可以使用安全网关名称或IP地址作为本端ID。在中心/分支模式的网络中，中心节点不会发起IPSec SA的协商，需要由分支节点首先向中心节点发起IPSec SA的协商。路由器通常作为分支节点的VPN接入设备使用。

图10-1 中心/分支模式组网



- 对等模式应用在一对一网络中，如 图 10-2 所示。在对等模式的网络中，两端的设备互为对等节点，都可以向对端发起IPSec SA的协商。

图10-2 对等模式组网

10.2 设置虚接口

IPSec 是同虚接口进行绑定的，数据流首先通过静态路由或者策略路由引入到虚接口，然后才会匹配规则进行 IPSec 加密处理。

虚接口需要映射到物理接口，只有需要进行 IPSec 处理的报文才会通过虚接口发送，其他报文仍然从实接口转发，另外路由加虚接口的配置模式使得 VPN 的配置更加灵活。

页面向导：VPN→IPSEC VPN→虚接口

本页面为您提供如下主要功能：

显示和修改已创建的虚接口（主页面）	
创建虚接口（单击主页面上的<新增>按钮，在弹出的对话框中选择一个虚接口通道以及映射的实际物理接口，单击<增加>完成操作）	

10.3 设置IKE

在实施 IPSec 的过程中，可以使用 IKE 协议来建立 SA。该协议建立在由 Internet SA 和密钥管理协议 ISAKMP 定义的框架上。IKE 为 IPSec 提供了自动协商交换密钥、建立 SA 的服务，能够简化 IPSec 的使用和管理。

IKE 不是在网络上直接传输密钥，而是通过一系列数据的交换，最终计算出双方共享的密钥，并且即使第三者截获了双方用于计算密钥的所有交换数据，也不足以计算出真正的密钥。

1. IKE简介

(1) IKE 的安全机制

IKE 具有一套自保护机制，可以在不安全的网络上安全地认证身份、分发密钥、建立 IPSec SA。

【数据认证】:

数据认证有如下两方面的概念：

- 身份认证：身份认证确认通信双方的身份，支持预共享密钥认证。
- 身份保护：身份数据在密钥产生之后加密传送，实现了对身份数据的保护。

【DH】:

DH 算法是一种公共密钥算法。通信双方在不传输密钥的情况下通过交换一些数据，计算出共享的密钥。即使第三者（如黑客）截获了双方用于计算密钥的所有交换数据，由于其复杂度很高，不足以计算出真正的密钥。所以，DH 交换技术可以保证双方能够安全地获得公有信息。

【PFS】：

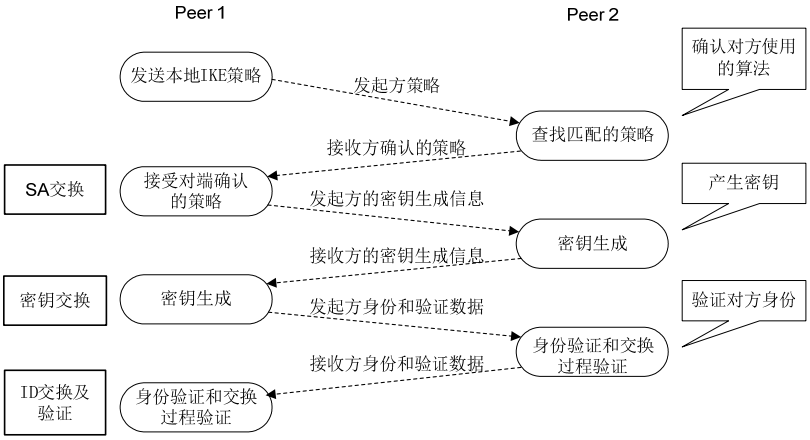
PFS 特性是一种安全特性，指一个密钥被破解，并不影响其他密钥的安全性，因为这些密钥间没有派生关系。对于 IPSec，是通过在 IKE 阶段 2 协商中增加一次密钥交换来实现的。PFS 特性是由 DH 算法保障的。

(2) IKE 的交换过程

IKE 使用了两个阶段为 IPSec 进行密钥协商并建立 SA：

- 第一阶段，通信各方彼此间建立了一个已通过身份认证和安全保护的通道，即建立一个 ISAKMP SA。第一阶段有主模式和野蛮模式两种 IKE 交换方法。
- 第二阶段，用在第一阶段建立的安全隧道为 IPSec 协商安全服务，即为 IPSec 协商具体的 SA，建立用于最终的 IP 数据安全传输的 IPSec SA。

图10-3 主模式交换过程



如 图 10-3 所示，第一阶段主模式的IKE协商过程中包含三对消息：

- 第一对叫 SA 交换，是协商确认有关安全策略的过程；
- 第二对消息叫密钥交换，交换 Diffie-Hellman 公共值和辅助数据（如：随机数），密钥材料在这个阶段产生；
- 最后一对消息是 ID 信息和认证数据交换，进行身份认证和对整个 SA 交换进行认证。

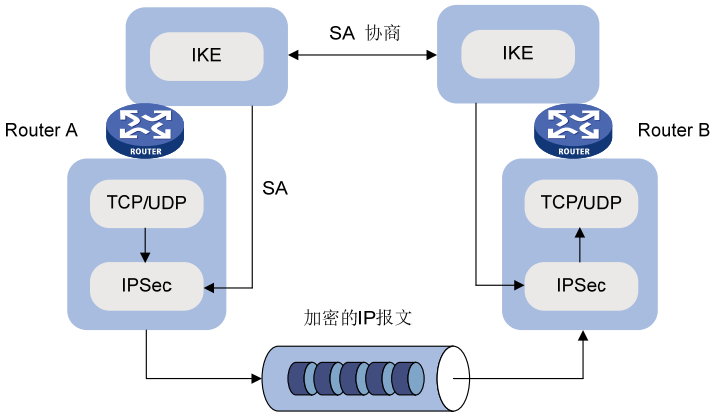
野蛮模式交换与主模式交换的主要差别在于，野蛮模式不提供身份保护，只交换 3 条消息。在对身份保护要求不高的场合，使用交换报文较少的野蛮模式可以提高协商的速度；在对身份保护要求较高的场合，则应该使用主模式。

(3) IKE 在 IPSec 中的作用

- 因为有了 IKE，IPSec 很多参数（如：密钥）都可以自动建立，降低了手工配置的复杂度。
- IKE 协议中的 DH 交换过程，每次的计算和产生的结果都是不相关的。每次 SA 的建立都运行 DH 交换过程，保证了每个 SA 所使用的密钥互不相关。
- IPSec 使用 AH 或 ESP 报文头中的序列号实现防重放。此序列号是一个 32 比特的值，此数溢出后，为实现防重放，SA 需要重新建立，这个过程需要 IKE 协议的配合。
- 对安全通信的各方身份的认证和管理，将影响到 IPSec 的部署。IPSec 的大规模使用，必须有认证机构或其他集中管理身份数据的机构的参与。
- IKE 提供端与端之间动态认证。

(4) IPSec 与 IKE 的关系

图10-4 IPSec 与 IKE 的关系图



从 图 10-4 中我们可以看出IKE和IPSec的关系：

- IKE 是 UDP 之上的一个应用层协议，是 IPSec 的信令协议；
- IKE 为 IPSec 协商建立 SA，并把建立的参数及生成的密钥交给 IPSec；
- IPSec 使用 IKE 建立的 SA 对 IP 报文加密或认证处理。

2. 设置安全提议

安全提议定义了一套属性数据来描述 IKE 协商怎样进行安全通信。配置 IKE 提议包括选择加密算法、选择验证算法、选择 Diffie-Hellman 组标识。

页面向导：VPN→IPSEC VPN→IKE 安全提议

本页面为您提供如下主要功能：

显示和修改已添加的IKE安全提议（主页面）	
添加一条新的IKE安全提议（单击主页面上的<新增>按钮，在弹出的对话框中设置相应的参数，并单击<增加>按钮完成操作）	

页面中关键项的含义如下表所示。

表10-3 页面关键项描述

页面关键项	描述
安全提议名称	输入安全提议的名称
IKE验证算法	选择IKE所使用的验证算法 缺省情况下，使用MD5
IKE加密算法	选择IKE所使用的加密算法 缺省情况下，使用3DES
IKE DH组	选择IKE所使用的DH算法 • DH1：768 位 DH 组 • DH2：1024 位 DH 组 • DH5：1536 位 DH 组 • DH14：2048 位 DH 组 缺省情况下，使用DH2

3. 设置对等体

对等体定义了协商的双方，包括本端发起协商接口、对端地址、采用的安全提议、协商模式、ID 类型等信息。只有经定义的双方才能够进行协商通信。

页面向导：VPN→IPSEC VPN→IKE 对等体

本页面为您提供如下主要功能：

显示和修改已添加的IKE对等体（主页面）

添加一个新的IKE对等体单击主页面上的<新增>按钮，在弹出的对话框中设置相应的参数，并单击<增加>按钮完成操作）

页面中关键项的含义如下表所示。

表10-4 页面关键项描述

页面关键项	描述
对等体名称	输入对等体的名称
虚接口	选择本端发起协商的出接口
对端地址	设置对等体对端的地址信息 说明 如果对端地址不是固定地址而是动态地址，建议通过将对端地址配置为动态域名的方式进行连接
协商模式	选择协商模式。主模式一般应用于点对点的对等组网模式；野蛮模式一般应用于中心/分支组网模式 缺省情况下，使用主模式
ID类型、本端ID、对端ID	此设置项需在野蛮模式下进行 当ID类型为NAME类型时，还需要指定相应的本端ID与对端ID
安全提议	选择对等体需要引用的IKE安全提议
预共享密钥（PSK）	设置IKE认证所需的预共享密钥（pre-shared-key）
生命周期	设置IKE SA存在的生命周期（IKE SA实际的周期以协商结果为准）
DPD开启	DPD用于IPsec邻居状态的检测。启动DPD功能后，当接收端在触发DPD的时间间隔内收不到对端的IPSec加密报文时，会触发DPD查询，主动向对端发送请求报文，对IKE对等体是否存在进行检测
DPD周期	指定对等体DPD检测周期，即触发DPD查询的间隔时间
DPD超时时间	指定对等体DPD检测超时时间，即等待DPD应答报文超时的时间

10.4 设置IPSec

1. 设置安全提议

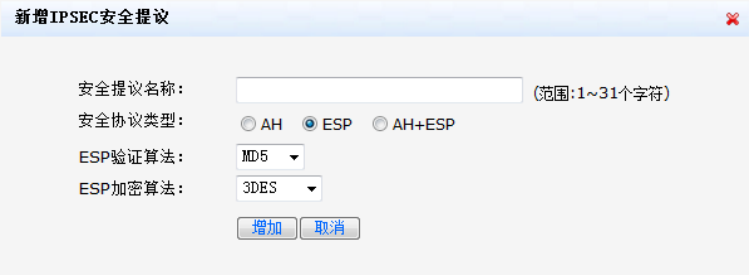
安全提议保存 IPSec 需要使用的特定安全性协议，以及加密/验证算法，为 IPSec 协商 SA 提供各种安全参数。为了能够成功的协商 IPSec 的 SA，两端必须使用相同的安全提议。

页面向导：VPN→IPSEC VPN→IPSec 安全提议

本页面为您提供如下主要功能：

显示和修改已添加的IPSec安全提议（主页面）	

添加一条新的IPSec安全提议（单击主页面上的<新增>按钮，在弹出的对话框中设置相应的参数，并单击<增加>按钮完成操作）



页面中关键项的含义如下表所示。

表10-5 页面关键项描述

页面关键项	描述
安全提议名称	输入安全提议的名称
安全协议类型	选择安全协议类型来实现安全服务 缺省情况下，使用ESP
AH验证算法	选择AH验证算法 缺省情况下，使用MD5
ESP验证算法	选择ESP验证算法 缺省情况下，使用MD5
ESP加密算法	选择ESP加密算法 缺省情况下，使用3DES

2. 设置安全策略

安全策略规定了对什么样的数据流采用什么样的安全提议。安全策略分为手工安全策略和 IKE 协商安全策略。前者需要用户手工配置密钥、SPI 等参数；后者则由 IKE 自动协商生成这些参数。

页面向导：VPN→IPSEC VPN→IPSec 安全策略

本页面为您提供如下主要功能：

开启IPSec功能、显示和修改已添加的安全策略（主页面）

设置使用IKE协商方式建立SA（单击主页面上的<新增>按钮，在弹出的对话框中选择“协商类型”为IKE协商并设置相应的参数，单击<增加>按钮完成操作）	
设置使用手动协商方式建立SA（单击主页面上的<新增>按钮，在弹出的对话框中选择“协商类型”为手动模式并设置相应的参数，单击<增加>按钮完成操作）	

页面中关键项的含义如下表所示。

表10-6 页面关键项描述

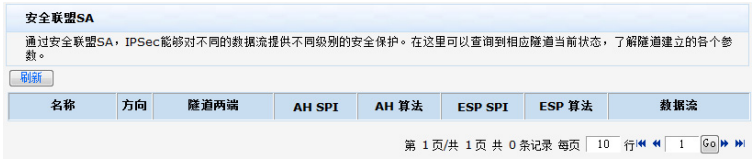
页面关键项	描述
启用IPSec	选中“启用IPSec”，开启IPSec功能 缺省情况下，禁用IPSec功能
安全策略名称	设置安全策略的名称，后面的复选框可以设置该安全策略的使用状态
本地子网IP/掩码	本地子网IP/掩码和对端子网IP/掩码，两个配置项组成一个访问控制规则。IPSec通过此访问控制规则来定义需要保护的数据流，访问控制规则匹配的报文将会被保护
对端子网IP/掩码	本地子网IP/掩码和对端子网IP/掩码分别用来指定IPSec VPN隧道本端和对端的子网网段
协商类型	选择IPSec协商方式 缺省情况下，使用IKE协商方式

页面关键项			描述
IKE协商模式	对等体		选择需要引用的IKE对等体
	安全提议		选择需要引用的IPSec安全提议 说明 此模式下，一条安全策略最多可以引用四个安全提议，根据组网需求可以灵活的加以配置
	PFS		PFS特性是一种安全特性，指一个密钥被破解，并不影响其他密钥的安全性，因为这些密钥间没有派生关系。IKE在使用安全策略发起一个协商时，可以进行一个PFS交换。如果本端设置了PFS特性，则发起协商的对端也必须设置PFS特性，且本端和对端指定的DH组必须一致，否则协商会失败 • 禁止：关闭 PFS 特性 • DH1：768 位 DH 组 • DH2：1024 位 DH 组 • DH5：1536 位 DH 组 • DH14：2048 位 DH 组 缺省情况下，PFS特性处于关闭状态
	生命周期		设置IPSec SA存在的生命周期 缺省情况下，生命周期为28800秒
	触发模式		用来指定隧道的触发模式 • 流量触发：IKE 隧道配置下发后，不会自动建立隧道，会等待兴趣流来触发隧道建立 • 长连模式：IKE 隧道配置下发后或隧道异常断开后，会自动触发隧道建立，并且保证隧道长时间建立，不需等待兴趣流触发
手动模式	虚接口		指定与当前策略绑定的虚接口
	对端地址		指定IPSec对等体另外一端的IP地址
	安全提议		选择需要引用的IPSec安全提议
	入/出SPI值		在安全隧道的两端设置的SA参数必须是完全匹配的。本端入方向SA的SPI必须和对端出方向SA的SPI一样；本端出方向SA的SPI必须和对端入方向SA的SPI一样。SPI具有唯一性，不允许输入相同的SPI值
	安全联盟使用的密钥	入/出ESP MD5密钥	在安全隧道的两端设置的SA参数必须是完全匹配的。本端入方向SA的密钥必须和对端出方向SA的密钥一样；本端出方向SA的密钥必须和对端入方向SA的密钥一样
		入/出ESP 3DES密钥	

10.5 查看VPN状态

页面向导：VPN→IPSEC VPN→安全联盟

本页面为您提供如下主要功能：

单击<刷新>按钮，您可以查看已建立的VPN隧道及对应的安全策略信息	

说明

IPSec VPN隧道建立后，路由器会自动添加一条路由信息（目的地址为IPSec VPN对端网段地址，出接口为IPSec VPN虚接口）。您可以通过单击“静态路由”页面中的<查看路由信息表>按钮来获知。

10.6 一对一IPSec VPN配置举例

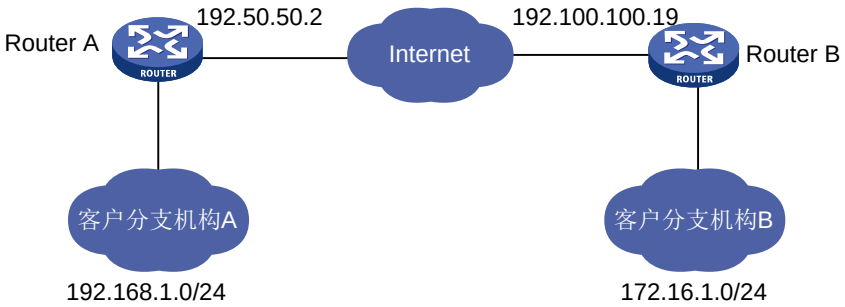
10.6.1 组网需求

在 Router A（采用 NR-1200W）和 Router B（采用 NR-1200W）之间建立一个安全隧道，对客户分支机构 A 所在的子网（192.168.1.0/24）与客户分支机构 B 所在的子网（172.16.1.0/24）之间的数据流进行安全保护。

安全协议采用 ESP 协议，加密算法采用 3DES，认证算法采用 SHA1。

10.6.2 组网图

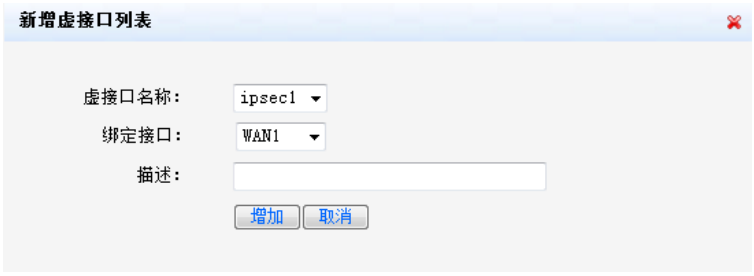
图10-5 组网示意图



10.6.3 设置步骤

1. 设置Router A

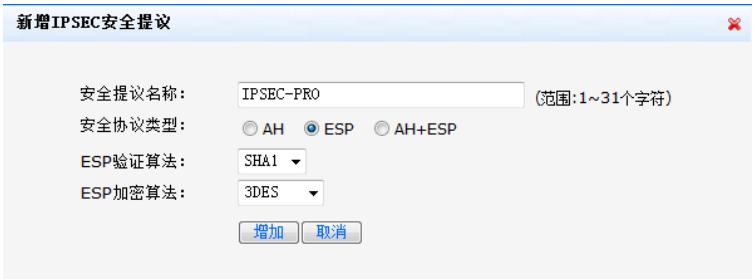
1. 选择“VPN→IPSEC VPN→虚接口”。单击<新增>按钮，在弹出的对话框中选择一个虚接口通道，并将其与对应的出接口进行绑定（此处假设为 WAN1），单击<增加>按钮完成操作



2. 选择“VPN→IPSEC VPN→IKE安全提议”。单击<新增>按钮，在弹出的对话框中输入安全提议名称，并设置验证算法和加密算法分别为 SHA1、3DES，单击<增加>按钮完成操作

3. 选择“VPN→IPSEC VPN→IKE对等体”。单击<新增>按钮，在弹出的对话框中输入对等体名称，选择对应的虚接口 ipsec1。在“对端地址”文本框中输入 Router B 的 IP 地址，并选择已创建的安全提议等信息，单击<增加>按钮完成操作

4. 选择“VPN→IPSEC VPN→IPSec 安全提议”。单击<新增>按钮，在弹出的对话框中输入安全提议名称，选择安全协议类型为 ESP，并设置验证算法和加密算法分别为 SHA1、3DES，单击<增加>按钮完成操作



5. 选择“VPN→IPSEC VPN→IPSec 安全策略”。选中“启用 IPSec 功能”复选框，单击<应用>按钮生效。单击<新增>按钮，在弹出的对话框中输入安全策略名称，在“本地子网 IP/掩码”和“对端子网 IP/掩码”文本框中分别输入客户分支机构 A 和 B 所处的子网信息，并选择协商类型为“IKE 协商”、对等体为“IKE-d1”、安全提议为“IPSEC-PRO”，单击<增加>按钮完成操作

6. 为经过 IPSec VPN 隧道处理的报文设置路由，才能使隧道两端互通（一般情况下，只需要为隧道报文配置静态路由即可）。选择“高级设置→路由设置→静态路由”，单击<新增>按钮，在弹出的对话框中，设置目的地址、子网掩码等参数，单击<增加>按钮完成操作

2. 设置Router B

在对端 Router B 上，IPSec VPN 的配置与 Router A 是相互对应的。因此，除了对等体的对端地址以及安全策略中的本地子网、对端子网需要做相应修改，其他的设置均一致。此处略。

3. 查看VPN状态

两端均设置完成后，您可以通过选择路由器的“VPN→IPSEC VPN→安全联盟”页面，并单击<刷新>按钮来查看相应的隧道是否已成功建立。

11 设置L2TP特性

本章节主要包含以下内容：

11.1 L2TP特性简介

11.1.1 概述

VPDN（Virtual Private Dial-up Network，虚拟专用拨号网络）是指利用公共网络（如 ISDN 或 PSTN）的拨号功能接入公共网络，实现虚拟专用网，从而为企业、小型 ISP、移动办公人员等提供接入服务。即，VPDN 为远端用户与私有企业网之间提供了一种经济而有效的点到点连接方式。

VPDN 采用隧道协议在公共网络上为企业建立安全的虚拟专网。企业驻外机构和出差人员可从远程经由公共网络，通过虚拟隧道实现和企业总部之间的网络连接，而公共网络上其它用户则无法穿过虚拟隧道访问企业网内部的资源。

VPDN 隧道协议主要包括以下三种：

- PPTP（Point-to-Point Tunneling Protocol，点到点隧道协议）
- L2F（Layer 2 Forwarding，二层转发）
- L2TP（Layer 2 Tunneling Protocol，二层隧道协议）

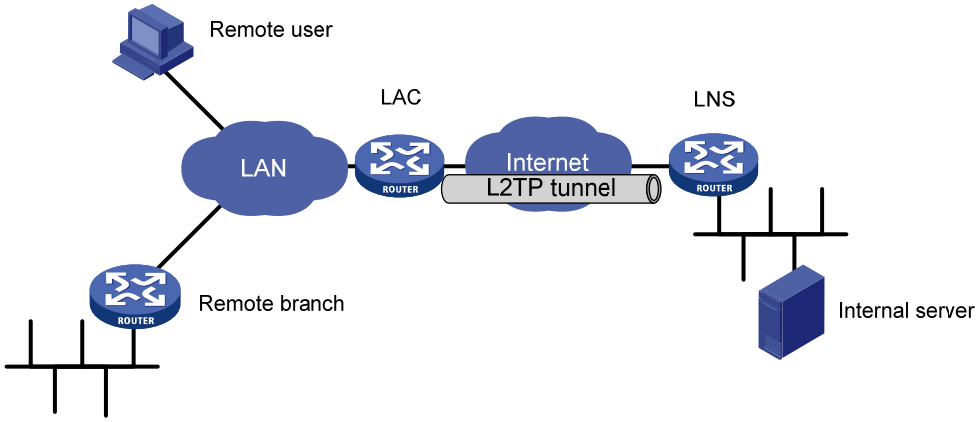
L2TP 结合了 L2F 和 PPTP 的各自优点，是目前使用最为广泛的 VPDN 隧道协议。

L2TP（RFC 2661）是一种对 PPP 链路层数据包进行封装，并通过隧道进行传输的技术。L2TP 允许连接用户的二层链路端点和 PPP 会话终点驻留在通过分组交换网络连接的不同设备上，从而扩展了 PPP 模型，使得 PPP 会话可以跨越分组交换网络，如 Internet。

11.1.2 L2TP典型组网应用

使用L2TP协议构建的VPDN应用的典型组网如 图 11-1 所示。

图11-1 应用 L2TP 构建的 VPDN 服务



在 L2TP 构建的 VPDN 中，网络组件包括以下三个部分：

- 远端系统

远端系统是要接入 VPDN 网络的远地用户和远地分支机构，通常是一个拨号用户的主机或私有网络的一台路由设备。

- LAC（L2TP Access Concentrator，L2TP 访问集中器）

LAC 是具有 PPP 和 L2TP 协议处理能力的设备，通常是一个当地 ISP 的 NAS（Network Access Server，网络接入服务器），主要用于为 PPP 类型的用户提供接入服务。

LAC 作为 L2TP 隧道的端点，位于 LNS 和远端系统之间，用于在 LNS 和远端系统之间传递信息包。它把从远端系统收到的信息包按照 L2TP 协议进行封装并送往 LNS，同时也将从 LNS 收到的信息包进行解封装并送往远端系统。

VPDN 应用中，LAC 与远端系统之间通常采用 PPP 链路。

- LNS（L2TP Network Server，L2TP 网络服务器）

LNS 既是 PPP 端系统，又是 L2TP 协议的服务器端，通常作为一个企业内部网的边缘设备。

LNS 作为 L2TP 隧道的另一侧端点，是 LAC 的对端设备，是 LAC 进行隧道传输的 PPP 会话的逻辑终止端点。通过在公网中建立 L2TP 隧道，将远端系统的 PPP 连接由原来的 NAS 在逻辑上延伸到了企业网内部的 LNS。

11.1.3 L2TP消息类型及封装结构

L2TP 中存在两种消息：

- 控制消息：用户隧道和会话连接的建立、维护和拆除。它的传输是可靠传输，并且支持对控制消息的流量控制和拥塞控制。
- 数据消息：用于封装 PPP 帧，并在隧道上传输。它的传输是不可靠传输，若数据报文丢失，不予重传，不支持对数据消息的流量控制和拥塞控制。

控制消息和数据消息共享相同的报文头，通过报文头中的 Type 字段来区分控制消息和数据消息。

图 11-2 描述了控制通道以及PPP帧和数据通道之间的关系。PPP帧在不可靠的L2TP数据通道上进行传输，控制消息在可靠的L2TP控制通道内传输。

图11-2 L2TP 协议结构

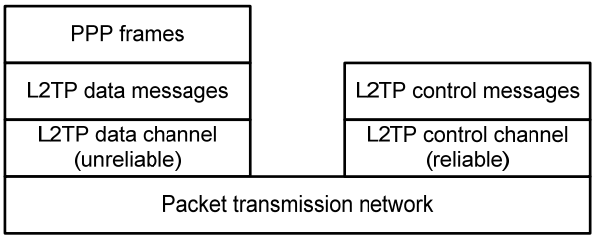


图 11-3 描述了LAC与LNS之间的L2TP数据报文的封装结构。通常L2TP数据以UDP报文的形式发送。L2TP注册了UDP 1701 端口，但是这个端口仅用于初始的隧道建立过程中。L2TP隧道发起方任选一个空闲的端口（未必是 1701）向接收方的 1701 端口发送报文；接收方收到报文后，也任选一个空闲的端口（未必是 1701），给发送方的指定端口回送报文。至此，双方的端口选定，并在隧道保持连通的时间段内不再改变。

图11-3 L2TP 报文封装结构图

11.1.4 L2TP隧道和会话

在一个 LNS 和 LAC 对之间存在着两种类型的连接。

- 隧道（Tunnel）连接：它对应了一个 LNS 和 LAC 对。
- 会话（Session）连接：它复用在隧道连接之上，用于表示承载在隧道连接中的每个 PPP 会话过程。

在同一对 LAC 和 LNS 之间可以建立多个 L2TP 隧道，隧道由一个控制连接和一个或多个会话连接组成。会话连接必须在隧道建立（包括身份保护、L2TP 版本、帧类型、硬件传输类型等信息的交换）成功之后进行，每个会话连接对应于 LAC 和 LNS 之间的一个 PPP 数据流。

控制消息和 PPP 数据报文都在隧道上传输。L2TP 使用 Hello 报文来检测隧道的连通性。LAC 和 LNS 定时向对端发送 Hello 报文，若在一段时间内未收到 Hello 报文的应答，隧道断开。

11.1.5 L2TP隧道模式及隧道建立过程

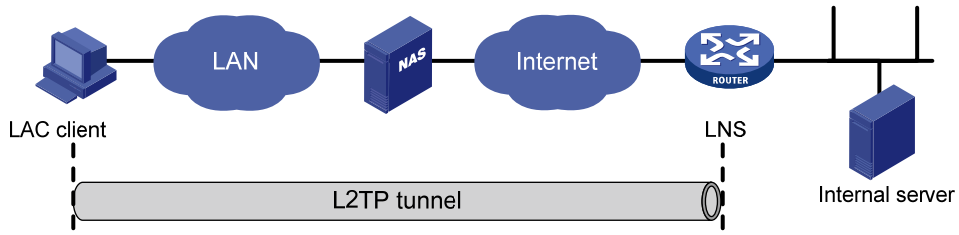
L2TP 隧道的建立支持以下两种典型模式。

- Client-Initiated

如 图 11-4 所示，直接由LAC客户（指本地支持L2TP协议的用户）发起L2TP隧道连接。LAC客户获得Internet访问权限后，可直接向LNS发起隧道连接请求，无需经过一个单独的LAC设备建立隧道。LAC客户的私网地址由LNS分配。

在 Client-Initiated 模式下，LAC 客户需要具有公网地址，能够直接通过 Internet 与 LNS 通信。

图11-4 Client-Initiated L2TP 隧道模式



说明

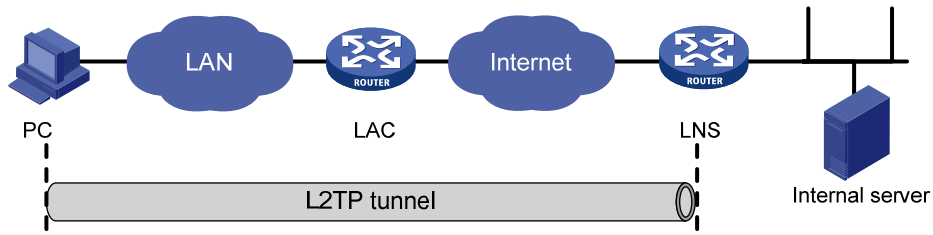
在该模式中，由路由器设备担当 LNS 角色。

- LAC-Auto-Initiated

如 图 11-5 所示， LAC上创建一个虚拟的PPP用户， LAC将自动向LNS发起建立隧道连接的请求，为该虚拟PPP用户建立L2TP隧道。远端系统访问LNS连接的内部网络时，LAC将通过L2TP隧道转发这些访问数据。

在该模式下，远端系统和 LAC 之间可以是任何基于 IP 的连接，不局限于拨号连接。

图11-5 LAC-Auto-Initiated L2TP 隧道模式



说明

在该模式中，由路由器设备担当 LAC 角色。

11.1.6 协议规范

与 L2TP 相关的协议规范有：

- RFC 1661：The Point-to-Point Protocol （PPP）
- RFC 1918：Address Allocation for Private Internets
- RFC 2661：Layer Two Tunneling Protocol “L2TP”

11.2 设置L2TP特性

支持 L2TP 特性的设备，既可以担任 L2TP 客户端（LAC）的角色，又可以担任 L2TP 服务端（LNS）的角色，下面将对这两种应用场景分别进行介绍。

11.2.1 设置L2TP客户端（设备作为LAC时的配置）

页面向导：VPN→L2TP VPN→L2TP 客户端

本页面为您提供如下主要功能：

设置L2TP客户端（LAC）	

页面中关键项的含义如下表所示。

表11-1 页面关键项描述

页面关键项	描述
启用LAC	启用或禁用LAC功能 缺省情况下，LAC处于禁用状态
L2TP用户名	LNS管理的允许建立会话的用户名（由远端的LNS管理员分配）
L2TP密码	LNS管理的允许建立会话的用户密码（由远端的LNS管理员分配）
L2TP服务器地址	LNS的公网地址（由远端的LNS管理员分配）
本端名称	标记该L2TP客户端的名称
地址获取方式	选择LAC会话建立成功后PPP接口的IP地址获取方式： • 动态：由 LNS 分配 • 静态：LAC 端手工设置一个 IP 地址 缺省情况下，地址获取方式为动态获取
静态IP地址	LAC手工设置的IP，只有在地址获取方式选择静态时起作用（由远端的LNS管理员分配）
启用隧道认证	设置是否启用L2TP隧道认证功能，当启用隧道认证时需要设置隧道认证密码 隧道认证请求可由LAC或LNS任何一侧发起。只要有一端启用了隧道认证，则只有在对端也启用了隧道认证，两端密码完全一致且不为空的情况下，隧道才能建立；否则本端将自动断开隧道连接。若隧道两端都禁止了隧道认证，隧道认证的密码一致与否将不起作用 缺省情况下，未启用隧道认证
隧道认证密码	为了保证隧道安全，建议用户启用隧道认证功能。如果为了进行网络连通性测试或者接收不知名对端发起的连接，则也可不进行隧道认证（隧道认证的密码由远端的LNS管理员分配）

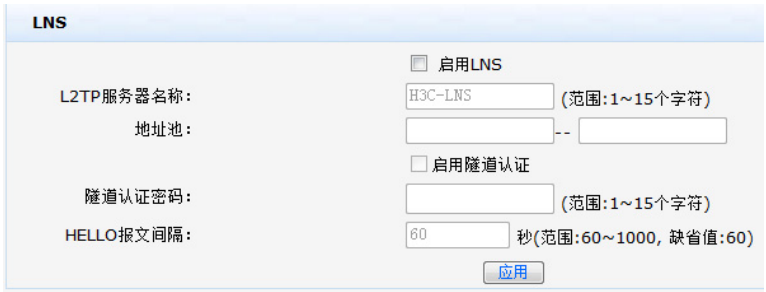
页面关键项	描述
HELLO报文间隔	设置发送Hello报文的时间间隔，单位为秒 为了检测LAC和LNS之间隧道的连通性，LAC和LNS会定期向对端发送Hello报文，接收方接收到Hello报文后会进行响应。当LAC或LNS在指定时间间隔内未收到对端的Hello响应报文时，重复发送，如果重复发送6次仍没有收到对端的响应信息则认为L2TP隧道已经断开，需要重新建立隧道连接 LNS端可以配置与LAC端不同的Hello报文间隔 缺省情况下，Hello报文间隔为60秒
绑定接口	用来指定l2tp0虚接口绑定的实接口信息

11.2.2 设置L2TP服务端（设备作为LNS时的配置）

1. 设置L2TP服务端

页面向导：VPN→L2TP VPN→L2TP 服务端

本页面为您提供如下主要功能：

设置L2TP服务端（LNS）	

页面中关键项的含义如下表所示。

表11-2 页面关键项描述

页面关键项	描述
启用LNS	启用或禁用LNS功能 缺省情况下，LNS处于禁用状态
L2TP服务器名称	标识该L2TP网络服务的名称
地址池	设置给L2TP客户端分配地址所用的地址池 设置地址池的开始IP地址和结束IP地址 开始和结束地址之间的地址数不能超过100 起始地址和结束地址前24位要一致，即输入地址格式： x1.x2.x3.y～x1.x2.x3.y1，即起始与结束地址x1.x2.x3要一致，如：地址池设置为10.5.100.100～10.5.100.155，要确保起始地址和结束地址10.5.100一致即可 说明 结束地址被 LNS 的 PPP 接口使用，不分配给接入客户端

页面关键项	描述
启用隧道认证	设置是否在该组中启用L2TP隧道认证功能，当启用隧道认证时需要设置隧道认证密码 隧道认证请求可由LAC侧发起。只要有一端启用了隧道认证，则只有在对端也启用了隧道认证，两端密码完全一致且不为空的情况下，隧道才能建立；否则本端将自动断开隧道连接。若隧道两端都禁止了隧道认证，隧道认证的密码一致与否将不起作用 缺省情况下，未启用隧道认证 说明 当 PC 作为 LAC，设备作为 LNS 时，建议不要启用 LNS 端的隧道认证功能
隧道认证密码	为了保证隧道安全，建议启用隧道认证功能。如果为了进行网络连通性测试或者接收不知名对端发起的连接，则也可不进行隧道认证
HELLO报文间隔	设置发送Hello报文的时间间隔，单位为秒 为了检测LAC和LNS之间隧道的连通性，LAC和LNS会定期向对端发送Hello报文，接收方接收到Hello报文后会进行响应。当LAC或LNS在指定时间间隔内未收到对端的Hello响应报文时，重复发送，如果重复发送6次仍没有收到对端的响应信息则认为L2TP隧道已经断开，需要重新建立隧道连接 LNS端可以配置与LAC端不同的Hello报文间隔 缺省情况下，Hello报文间隔为60秒

2. 设置LNS用户管理

页面向导：VPN→L2TP VPN→LNS 用户管理

本页面为您提供如下主要功能：

LNS用户查询（关键字过滤选择用户名或状态，在关键字中输入用户名或选择用户状态，单击<查询>按钮生效）	
LNS新增用户（单击主页面上的<新增>按钮，在弹出的对话框中输入用户名、密码和选择用户状态，单击<增加>按钮生效）	
修改用户信息（双击主页面上的列表中的用户项或者单击 图标，在弹出的对话框中修改密码和用户状态，单击<修改>按钮生效）	

页面中关键项的含义如下表所示。

表11-3 页面关键项描述

页面关键项	描述
用户名	LNS管理的用户，LAC与该LNS建立会话时要使用的用户名
密码	LNS管理的用户，LAC与该LNS建立会话时要使用的用户密码
状态	LNS管理的用户状态 启用：LNS允许远端的L2TP客户端使用该用户建立会话 禁用：LNS不允许远端的L2TP客户端使用该用户建立会话

3. 查看L2TP状态

页面向导：VPN→L2TP VPN→L2TP 状态

本页面为您提供如下主要功能：

- 显示当前 L2TP 客户端信息
- 连接或断开 L2TP 客户端连接
- 显示当前作为 LNS 时已建立会话和隧道的信息

页面中关键项的含义如下表所示。

表11-4 页面关键项描述

页面关键项	描述
链路状态	显示L2TP客户端当前的连接状态
本端IP地址	显示当前L2TP客户端，本端PPP接口的IP地址
对端IP地址	显示当前L2TP客户端，对端PPP接口的IP地址
用户名	显示LNS服务中，当前接入客户端建立会话使用的用户名
对端地址	显示LNS服务中，当前接入客户端的公网IP地址
对端主机名称	显示LNS服务中，当前接入客户端的主机名称
本端隧道ID	显示LNS服务中，当前已建立隧道的本端ID
对端隧道ID	显示LNS服务中，当前已建立隧道的对端ID

11.3 L2TP典型配置举例

11.3.1 设备作为L2TP客户端的配置举例

1. 组网需求

VPN 用户访问公司总部过程如下：

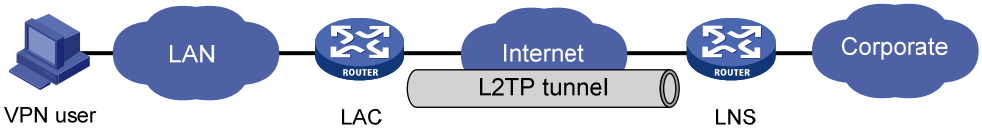
(1) LAC 上创建虚拟 PPP 用户，LAC 自动向 LNS 发起建立隧道连接的请求，为该虚拟 PPP 用户建立 L2TP 隧道。

(2) VPN 用户通过 LAN 将访问公司总部的报文发送给 LAC。

(3) LAC 封装该报文，并通过已经建立的 L2TP 隧道将报文发送给 LNS，VPN 用户与公司总部间的通信都通过 LAC 与 LNS 之间的隧道进行传输。

2. 组网图

公司办事处通过 L2TP 客户端，与远端的公司总部的 LNS 进行连接。



3. 组网配置方案

- 将路由器的 WAN 口接公网线路；
- 设置 WAN 口通过静态方式连接到因特网；
- 设置 L2TP 客户端为启用状态；
- 设置公司总部提供的 LNS 的 IP 地址、L2TP 隧道密码以及提供建立 PPP 连接的用户名、密码；
- 设置 L2TP 客户端地址获取方式为动态获取。

4. 设置步骤

说明

此典型配置案例中所涉及的设置均在路由器缺省配置的基础上进行。如果您之前已经对路由器做过相应的配置，为了保证效果，请确保当前配置和以下配置不冲突。

(1) LAC 侧配置

在管理计算机的Web浏览器地址栏中输入http://192.168.1.1，回车。输入缺省的用户名：admin，密码：admin，单击<登录>按钮后便可进入Web设置页面

设置WAN口IP：192.16.100.19，网关地址：192.16.100.11（静态IP和网关都是由运营商分配）	
配置LAC信息（启用LAC功能，输入用户名：vpdnuser，密码：hello，L2TP服务器IP：192.16.100.31，地址方式选择动态获取，启用隧道认证，隧道认证密码：tunnel-auth，单击<应用>按钮后发起L2TP连接请求）	

(2) LNS 侧配置

公司总部的 LNS 服务器运行正常，并提供 LNS 侧配置信息，如下表所示。

表11-5 LNS 管理员提供的配置

关键项	内容
用户名	vpdnuser
密码	hello
隧道认证是否开启	开启隧道认证模式
隧道认证密码	tunnel-auth
LNS的公网IP地址	192.16.100.31

(3) 验证配置结果

选择“VPN→L2TP VPN→L2TP状态→L2TP客户端信息”来查看L2TP客户端连接情况，当链路状态为已连接时，则可正常访问公司总部的资源了

11.3.2 设备作为L2TP服务端的配置举例

1. 组网需求

VPN 用户访问公司总部过程如下：

(1) 配置用户侧主机的 IP 地址和路由，确保用户侧主机和 LNS 之间路由可达。

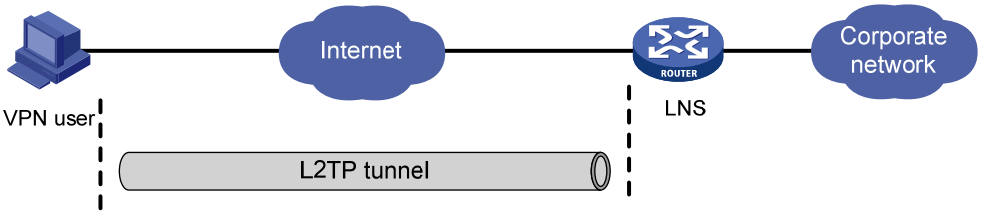
(2) 由用户向 LNS 发起 Tunnel 连接的请求。

(3) 在 LNS 接受此连接请求之后，VPN 用户与 LNS 之间就建立了一条虚拟的 L2TP tunnel。

(4) 用户与公司总部间的通信都通过 VPN 用户与 LNS 之间的隧道进行传输。

2. 组网图

公司办事处员工通过 Windows 7 的 L2TP 客户端接入公司总部的设置 L2TP 服务端，来访问内部资源。



3. 组网配置方案

- 将路由器的 WAN 口接公网线路；
- 设置 WAN 口通过静态方式连接到因特网；
- 设置 LNS 服务为启用状态，并配置信息；
- 添加允许接入的用户信息。

4. 设置步骤

说明

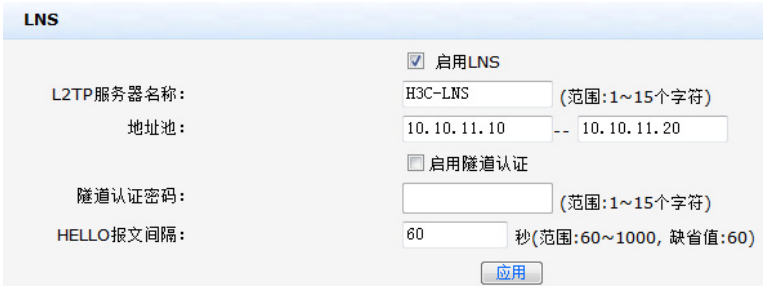
此典型配置案例中所涉及的设置均在路由器缺省配置的基础上进行。如果您之前已经对路由器做过相应的配置，为了保证效果，请确保当前配置和以下配置不冲突。

(1) LNS 侧配置

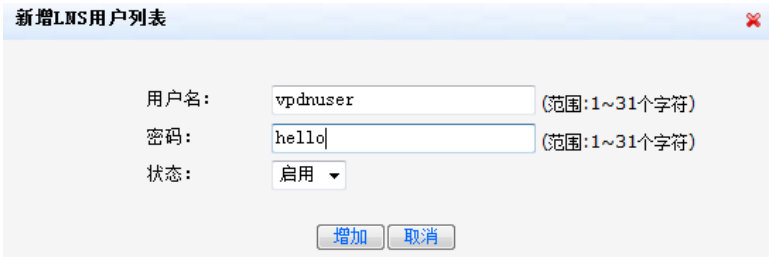
在管理计算机的Web浏览器地址栏中输入http://192.168.1.1，回车。输入缺省的用户名：admin，密码：admin，单击<登录>按钮后便可进入Web设置页面

设置WAN口IP：192.16.100.31，网关地址：192.16.100.11（静态IP和网关都是由运营商分配）

配置LNS信息（启用LNS，输入L2TP服务器名称：H3C-LNS，地址池：10.10.11.10～10.10.11.20，单击<应用>按钮生效）



新增用户（单击主LNS用户管理页面上的<新增>按钮，在弹出的对话框中输入用户名：vpdnuser，密码：hello，用户状态：启用，单击<增加>按钮生效）



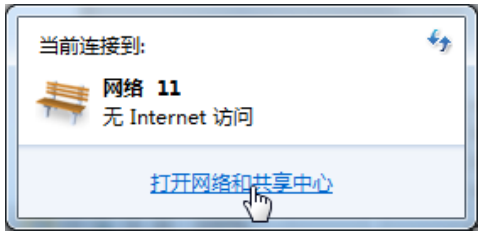
完成以上所有设置后，您可以通过下列操作来查看当前 LNS 配置情况：

选择“VPN→L2TP VPN→L2TP服务端”来查看当前LNS配置信息

选择“VPN→L2TP VPN→LNS用户管理”来查看允许L2TP客户端使用的用户信息

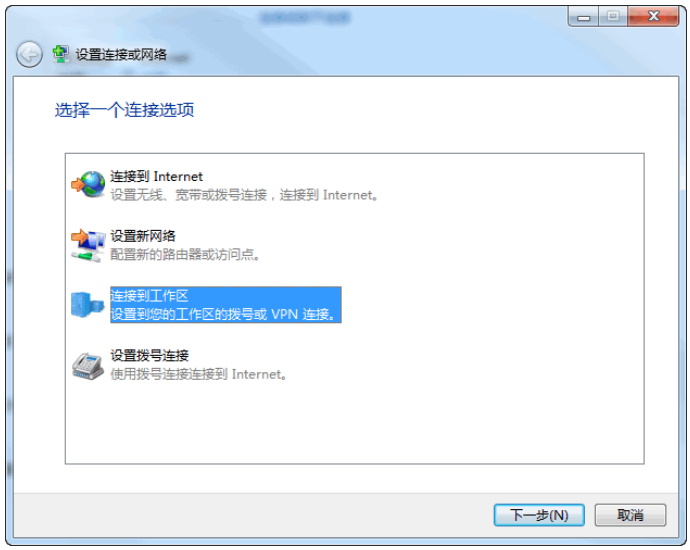
(2) 设置 Windows 7 的 L2TP 客户端

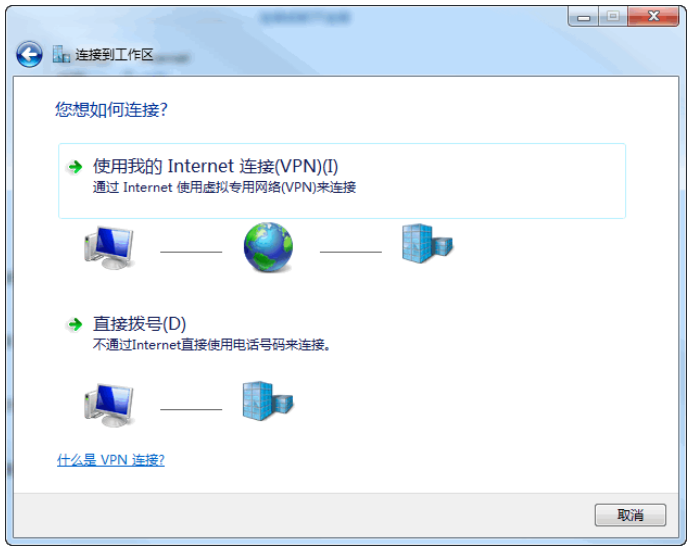
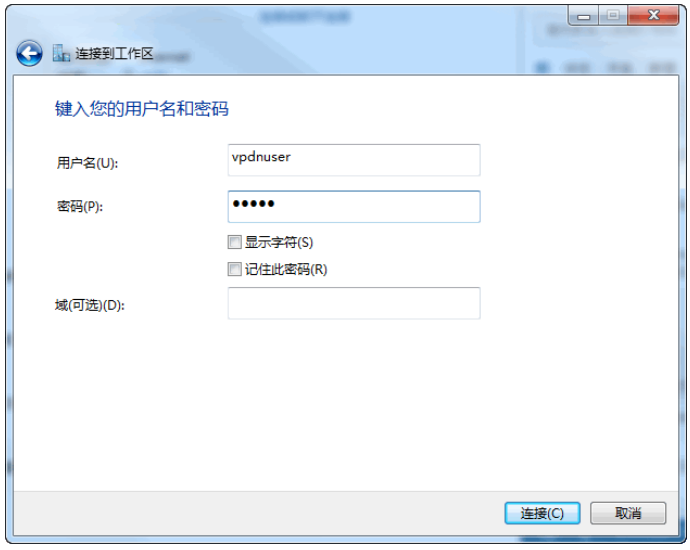
单击桌面右下角的网络图标，如  ，选择“打开网络和共享中心”



单击“设置新的连接或网络”，创建一个L2TP客户端

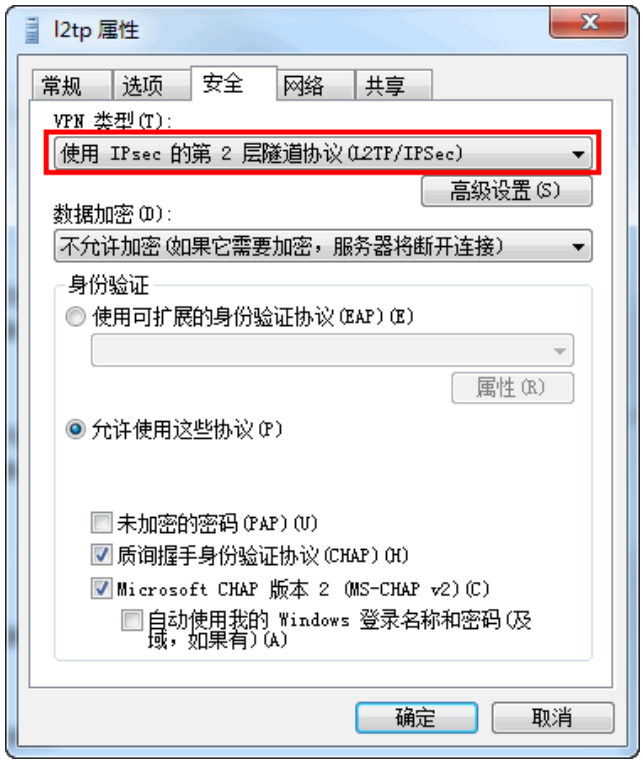
弹出“设置连接或网络”，选择“连接到工作区”选项，单击<下一步>按钮



选择“使用我的Internet连接(VPN)(I)”选项	
输入要连接到的L2TP服务器的IP地址和该L2TP客户端的连接的名称，单击<下一步>按钮	
输入用户名：vpdnuser，密码：hello，单击<连接>按钮进行连接	

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

在弹出窗口中，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)”，单击<确定>按钮生效

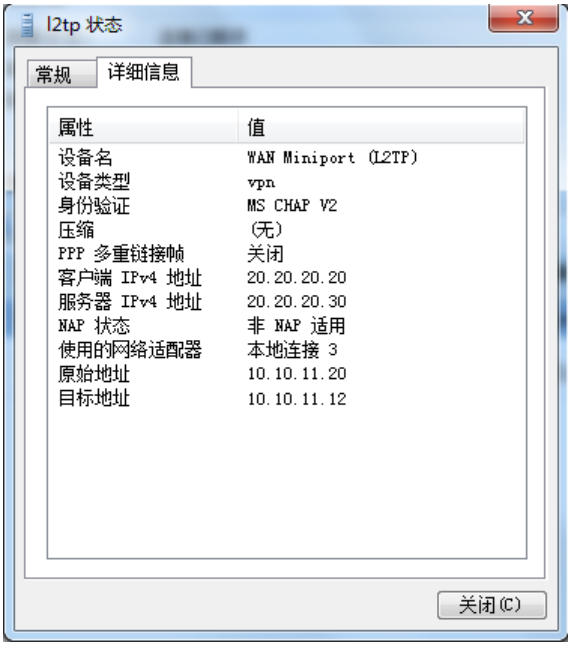


打开L2TP协议的拨号终端窗口，在弹出的窗口中输入用户名：vpdnuser，密码：hello，单击<连接>按钮进行连接

(3) 验证配置结果

LNS侧，通过选择“VPN→L2TP VPN→L2TP状态”来查看当前的LNS服务端会话信息

打开Windows 7的L2TP客户端，通过选择L2TP协议连接终端的状态选项，来查看当前的连接情况



12 设置QoS

QoS 是指针对网络中各种应用不同的需求，提供不同的服务质量，比如：提供专用带宽、减少报文丢失率、降低报文传送时延及抖动。

本章节主要包含以下内容：

12.1 设置IP流量限制

某些应用（比如：P2P 下载等）在给用户带来方便的同时，也占用了大量的网络带宽。一个网络的总带宽是有限的，如果这些应用过度占用网络带宽，必将会影响其他用户正常使用网络。

为了保证局域网内所有用户都能正常使用网络资源，您可以通过 IP 流量限制功能对局域网内指定主机的流量进行限制。

路由器支持以下两种 IP 流量限制方式：

- 允许每 IP 通道借用空闲的带宽（推荐使用）：即弹性带宽限制，在带宽使用不紧张时，允许每台主机可以使用系统空闲带宽，其实际流量可以超过限速值。
- 每 IP 通道只能使用预设的带宽：即固定带宽限制，每台主机的实际流量不能超过限速值。即使系统还有空闲的带宽，也不能利用。

说明

一般情况下，上网流量都通过正常通道来转发（正常通道是指除了绿色专用通道和限制专用通道以外的通道），IP流量限制仅对该通道中的流量生效。正常通道的带宽 = 接口带宽（从运营商申请到的实际带宽）－绿色专用通道的带宽。

页面向导：QoS 设置→流量管理→IP 流量限制

本页面为您提供如下主要功能：

启用IP流量限制功能，并设置您所需的限制方式（主页面。选中“启用IP流量限制”复选框，选择相应的限制方式，并设置正确的接口带宽（否则可能发生掉线），单击<应用>按钮生效）	

添加限速规则（单击<新增>按钮，在弹出的对话框中设置限速规则，单击<增加>按钮完成操作）	

页面中关键项的含义如下表所示。

表12-1 页面关键项描述

页面关键项	描述
启用IP流量限制	开启路由器的IP流量限制功能 缺省情况下，IP流量限制功能处于关闭状态
允许每IP通道借用空闲的带宽 每IP通道只能使用预设的带宽	选择路由器的IP流量限制方式 缺省情况下，路由器采用每IP通道只能使用预设的带宽 **说明** 以出口带宽为 30M，带机量为 150 台为例：每 IP 上行和下行流量上限均可设置为 200Kbps，同时开启使用允许每 IP 通道借用空闲的带宽
表项序号	由于系统会根据表项的序号来顺序匹配，因此您可以通过此选项来调整该表项的匹配优先级 缺省情况下，新增的表项会排在最后
IP起始地址	输入局域网内需要进行流量限制的主机的起始IP地址
IP结束地址	输入局域网内需要进行流量限制的主机的结束IP地址
带宽共享方式	选择需要进行流量限制的计算机的带宽共享方式，当受限地址类型为IP地址范围时可选择独占或共享，为IP网段时，系统自动设定为共享，无法修改 • 独占：受限地址范围内的每台计算机各自占有给定的带宽（即流量上限），如 IP 地址范围为 192.168.1.2～192.168.1.11，流量上限为 1000Kbps，表示此 IP 范围内的每台计算机的流量上限为 1000Kbps • 共享：受限地址范围内的所有计算机共享给定的带宽，如 IP 地址范围为 192.168.1.2～192.168.1.11，流量上限为 1000Kbps，表示此 IP 范围内的所有主机的流量之和的上限为 1000Kbps
限速接口	选择IP流量限速所应用的接口 • WAN1：仅当流量从 WAN1 口出入时，才进行限速 • WAN2：仅当流量从 WAN2 口出入时，才进行限速

页面关键项	描述
限速方向	选择IP流量限速方向： • “上行限速”：限制由局域网发送到因特网的数据流速率（比如：局域网内主机向因特网上的 FTP 服务器上传文件） • “下行限速”：限制由因特网发送到局域网的数据流速率（比如：局域网内主机从因特网上的 FTP 服务器下载文件） • “双向限速”：同时限制上行、下行两个方向上的数据流速率
上行流量上限	输入最大上行流量 说明 此最大上行流量限制值是在“IP 起始地址”和“IP 结束地址”地址段中各个主机的上行带宽，而不是 IP 地址段内所有主机的共享上行带宽
下行流量上限	输入最大下行流量 说明 此最大下行流量限制值是在“IP 起始地址”和“IP 结束地址”地址段中各个主机的下行带宽，而不是 IP 地址段内所有主机的共享下行带宽
生效时间	选择IP流量限制的生效时间。生效时间包括两部分内容：在一天中生效的时间段，时间使用24小时制，起始时间应早于结束时间，00:00～24:00表示该规则在一天内任何时间都生效；星期选择表示一周中哪些天规则生效。请为设备配置正确的系统时间
描述	对此条新增限速规则进行描述

说明

当对相同的单个 IP 地址或 IP 地址网段，在同一个限速接口上进行限速时，先添加的限速规则生效。比如：

- 先添加规则 1：设置用户（192.168.0.2）在 WAN1 接口上的 IP 流量限速为 300Kbps。
- 后添加规则 2：设置用户（192.168.0.2）在 WAN1 接口上的 IP 流量限速为 400Kbps。

生效情况：规则 1 生效。

未设置限速规则的用户，带宽不做限制，只受系统转发能力的限制；当路由器开启弹性带宽后，系统为了合理地分配带宽，限速的用户可以占用一定的弹性带宽。

12.2 设置专用通道

路由器为您提供了绿色专用通道和限制专用通道的设置：

- 绿色专用通道：您可以将特定的数据业务流通过绿色通道转发，从而可以保证对时延要求较高的应用（比如：网络游戏）有足够带宽。在绿色专用通道中，路由器支持根据您设置的报文长度大小和协议端口号来匹配数据流。
- 限制专用通道：您可以将特定的数据业务流通过限制通道转发，从而可以限制大流量 P2P 应用的带宽。在限制通道中，路由器支持根据您设置的报文协议端口号来匹配数据流。

比如：某网吧的实际带宽为 10Mbps，有 100 人在上网，其中大部分用户都在玩某类游戏，还有部分用户在使用 P2P 软件下载影片。此时，您可以为玩某类游戏的用户设置绿色专用通道，为 P2P 下载影片的用户设置限制专用通道。从而保证即使线路存在拥塞时，游戏数据包仍然能得到及时转发，并可以限制 P2P 下载过度占用带宽。

12.2.1 设置绿色专用通道

页面向导：QoS 设置→流量管理→绿色通道管理

本页面为您提供如下主要功能：

启用绿色通道功能，并设置相关参数（主页面。选中“启用绿色专用通道”复选框，设置此绿色通道的每接口上/下行流量限速，并选择数据流匹配方式，单击<应用>按钮生效）	
添加用于匹配数据流的协议端口号（单击主页面上的<新增>按钮，在弹出的对话框中设置匹配项，单击<增加>按钮完成操作）	

页面中关键项的含义如下表所示。

表12-2 页面关键项描述

页面关键项	描述
启用绿色专用通道	缺省情况下，绿色专用通道处于关闭状态
每接口上行流量上限	输入每个WAN接口所占用的绿色专用通道的最大上行流量
每接口下行流量上限	输入每个WAN接口所占用的绿色专用通道的最大下行流量
启用数据包长度选择	选中该复选框，并设置报文长度，路由器会根据报文的长度来识别需要发送到绿色专用通道的流量 缺省情况下，此功能处于关闭状态
启用端口选择	选中该复选框，路由器会根据协议端口来识别需要发送到绿色专用通道的流量 缺省情况下，此功能处于关闭状态
应用名称	设置需要识别的端口组的描述名称，可以为空

页面关键项	描述
端口号	设置需要识别的协议端口号 说明 对局域网发送到因特网的流量，路由器匹配目的端口号；对因特网发送到局域网的流量，路由器匹配源端口号

说明

如果报文长度选择和端口选择同时开启时，只要匹配其中一项即可识别成功，且报文长度选择优先匹配。

12.2.2 设置限制专用通道

页面向导：QoS 设置→流量管理→限制通道管理

本页面为您提供如下主要功能：

启用限制通道功能，并设置相关参数（主页面。选中“启用限制通道”复选框，设置此限制通道的每接口上/下行流量限速，单击<应用>按钮生效）	
添加用于匹配数据流的协议端口号（单击主页面上的<新增>按钮，在弹出的对话框中设置匹配项，单击<增加>按钮完成操作）	

页面中关键项的含义如下表所示。

表12-3 页面关键项描述

页面关键项	描述
启用限制通道	缺省情况下，限制通道处于关闭状态
每接口上行流量上限	输入每个WAN接口所占用的限制通道的最大上行流量
每接口下行流量上限	输入每个WAN接口所占用的限制通道的最大下行流量
应用名称	设置需要识别的端口组的描述名称，可以为空

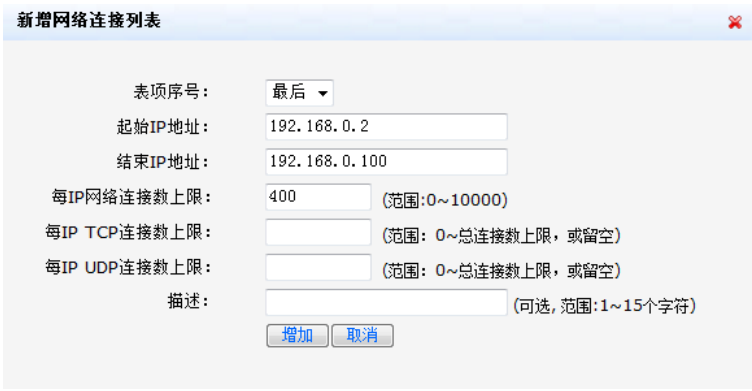
页面关键项	描述
端口号	设置需要识别的协议端口号 说明 对局域网发送到因特网的流量，路由器匹配目的端口号；对因特网发送到局域网的流量，路由器匹配源端口号

12.3 设置网络连接限数

当局域网内的主机遭受 NAT 攻击时，主机的网络连接数可能会超过几万个，从而会严重影响业务的正常运行或出现网络掉线现象。此时，您可对指定主机的最大网络连接数进行限制，保证网络资源的有效利用。

页面向导：QoS 设置→连接限制→网络连接限数

本页面为您提供如下主要功能：

启用网络连接限数功能（主页面。选中“启用网络连接限数”复选框，单击<应用>按钮生效）	
添加指定IP地址范围内每台主机同时发起的最大网络连接数（单击主页面上的<新增>按钮，在弹出的对话框中设置相应参数，单击<增加>按钮完成操作）	

页面中关键项的含义如下表所示。

表12-4 页面关键项描述

页面关键项	描述
启用网络连接限数	缺省情况下，网络连接限数功能处于关闭状态
表项序号	由于系统会根据表项的序号来顺序匹配，因此您可以通过此选项来调整该表项的匹配优先级 缺省情况下，新增的表项会排在最后
IP起始地址	输入对局域网内进行网络连接限数的主机的起始IP地址
IP结束地址	输入对局域网内进行网络连接限数的主机的结束IP地址

页面关键项	描述
每IP网络连接数上限	输入指定主机的网络连接数上限值
每IP TCP连接数上限	允许指定IP范围的每台主机同时向WAN侧发起的最大TCP连接数，可留空
每IP UDP连接数上限	允许指定IP范围的每台主机同时向WAN侧发起的最大UDP连接数，可留空
描述	对此网络连接限数项进行描述

说明

当对相同的单个 IP 地址或 IP 地址网段进行网络连接限数时，先添加的限数规则生效。比如：

- 先添加规则 1：设置 192.168.0.1～192.168.0.100 网段中的用户网络连接数上限为 40。
- 后添加规则 2：设置 192.168.0.1～192.168.0.100 网段中的用户网络连接数上限为 50。

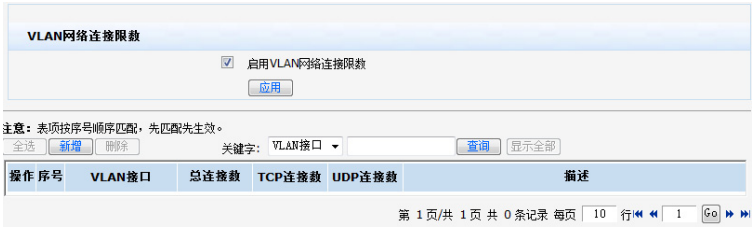
生效情况：规则 1 生效。

12.4 设置VLAN网络连接限数

VLAN 网络连接限数即通过设置每个 VLAN 的连接数上限，从而有效解决了部分 VLAN 占用大量网络连接资源的问题，实现了网络资源的合理利用。设置网络连接数时，除总连接数上限以外，您还可以设置 TCP 连接数上限和 UDP 连接数上限。通过设置 UDP 连接数上限，您可以有效解决 BT 和视频播放等软件建立过多 UDP 连接，导致网页访问缓慢等问题（连接数过多，TCP 连接无法建立）。

页面向导：QoS 设置→连接限制→VLAN 网络连接限数

本页面为您提供如下主要功能：

启用VLAN网络连接限数功能（主页面。选中“启用VLAN网络连接限数”复选框，单击<应用>按钮生效）	
添加指定VLAN的总连接数上限（单击主页面上的<新增>按钮，在弹出的对话框中设置相应参数，单击<增加>按钮完成操作）	

页面中关键项的含义如下表所示。

表12-5 页面关键项描述

页面关键项	描述
启用VLAN网络连接限数	开启和关闭VLAN内网络连接限数功能
VLAN接口	需要进行网络连接限数的VLAN接口名称
总连接数	指定VLAN允许占用的最大网络连接数，避免个别VLAN占用过多的资源
TCP连接数	指定VLAN允许占用的最大TCP连接数
UDP连接数	指定VLAN允许占用的最大UDP连接数
描述	对此VLAN网络连接限数项进行描述

13 高级设置

本章节主要包含以下内容：

13.1 地址转换

13.1.1 NAT设置

NAT 可以实现局域网内的多台主机通过 1 个或多个公网 IP 地址接入因特网，即用少量的公网 IP 地址代表较多的私网 IP 地址，节省公网的 IP 地址。

说明

私网 IP 地址是指内部网络或主机的 IP 地址，公网 IP 地址是指在因特网上全球唯一的 IP 地址。

RFC 1918 为私网预留出了三个 IP 地址块，如下：

- A 类：10.0.0.0 ~ 10.255.255.255
- B 类：172.16.0.0 ~ 172.31.255.255
- C 类：192.168.0.0 ~ 192.168.255.255

上述三个范围内的地址不会在因特网上被分配，因此可以不必向运营商或注册中心申请而在公司或企业内部自由使用。

路由器支持提供以下三种 NAT 转换方式：

- 一对一 NAT：将局域网内主机的 IP 地址一对一转换为指定的公网 IP 地址，即对应主机访问因特网时有自己的公网 IP 地址。在这种方式下，局域网内的其他主机及因特网上的主机都可以通过访问对应的公网 IP 地址来访问该主机。
- 多对一 NAT：当路由器拥有单个公网 IP 地址时，如果局域网内的主机访问外网，其私网 IP 地址均自动转换为对应的 WAN 接口的 IP 地址。
- 多对多 NAT：当路由器拥有多个公网 IP 地址时，如果局域网内的主机访问外网，其私网 IP 地址会自动转换为公网 IP 地址池中的其中一个 IP 地址。

比如：某企业申请了一条电信线路，分配的公网 IP 地址范围是 218.3.55.20～218.3.55.30。该企业需要对外开放 Web 服务器（IP 地址为 192.168.1.5）、Mail 服务器（IP 地址为 192.168.1.6）和 FTP 服务器（IP 地址为 192.168.1.7）。此时，您可以使用一对一 NAT 方式将服务器 IP 地址与公网 IP 地址建立一对一地址转换，其他主机上网时可使用公网 IP 地址池中的其他 IP 地址，从而可以充分利用所有的公网 IP 地址。

1. 设置NAT功能状态

仅当开启了 NAT 功能后，您所设置的一对一 NAT、多对一 NAT 和多对多 NAT 才会生效。

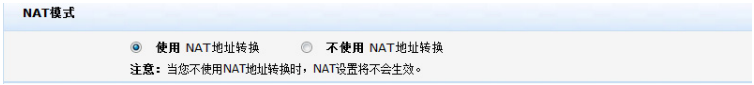
说明

当您需要将设备作为普通的路由器使用时，可以关闭 NAT 功能。

页面向导：高级设置→地址转换→NAT 设置

本页面为您提供如下主要功能：

- 开启 NAT 功能（选中“使用 NAT 地址转换”单选按钮，单击<应用>按钮生效）
- 关闭 NAT 功能（选中“不使用 NAT 地址转换”单选按钮，单击<应用>按钮生效）



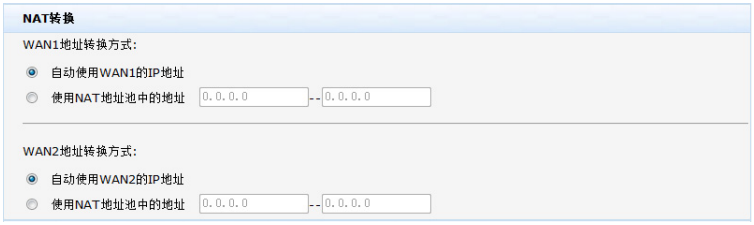
2. 设置多对一NAT和多对多NAT

在您设置多对一和多对多 NAT 前，请先开启 NAT 功能。

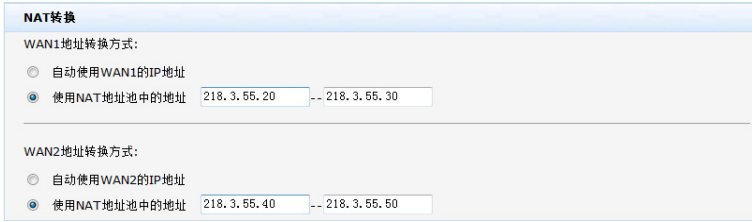
页面向导：高级设置→地址转换→NAT 设置

本页面为您提供如下主要功能：

设置多对一NAT（根据您实际所连接的线路，选择相应的“自动使用WAN1的IP地址”或“自动使用WAN2的IP地址”单选按钮，单击<应用>按钮生效）



设置多对多NAT（根据您实际所连接的线路，设置相应WAN口的NAT地址池范围，单击<应用>按钮生效）



3. 设置网络连接参数

说明

建议您在 H3C 技术人员的指导下对网络连接参数进行操作。

页面向导：高级设置→地址转换→NAT 设置

本页面为您提供如下主要功能：

- 设置路由器支持的网络连接总数，即会话总数（一般情况下，请保留缺省值。比如：局域网内PC 遭受病毒攻击从而建立大量无用的连接，您可以修改该参数来减少路由器资源的浪费）
- 清除指定接口的网络连接（一般情况下，如果路由器运行正常，请勿执行此操作。因为，清除网络连接会导致现有的业务重新选择出接口，可能会影响现有业务的正常运行）

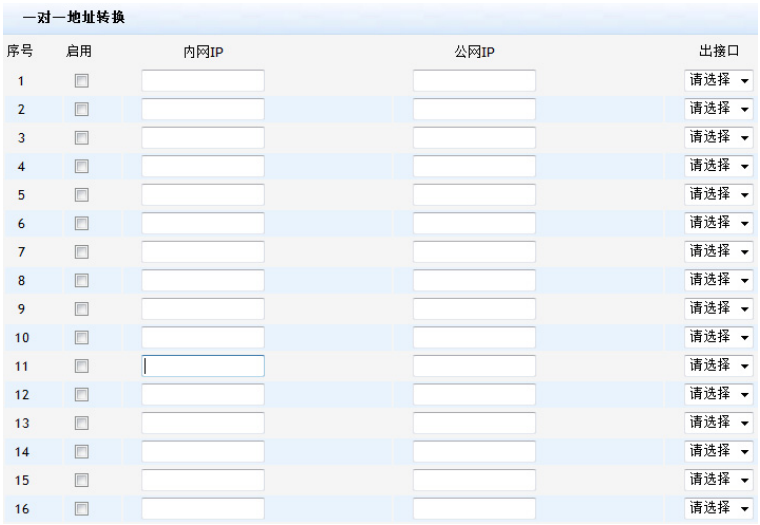
13.1.2 设置一对一NAT

在您设置一对一 NAT 前，请先开启 NAT 功能。

页面向导：高级设置→地址转换→一对一 NAT

本页面为您提供如下主要功能：

设置一对一NAT（选中“启用”复选框，设置指定的内网IP与公网IP的映射关系，并选择相应的WAN出接口，单击<应用>按钮生效）



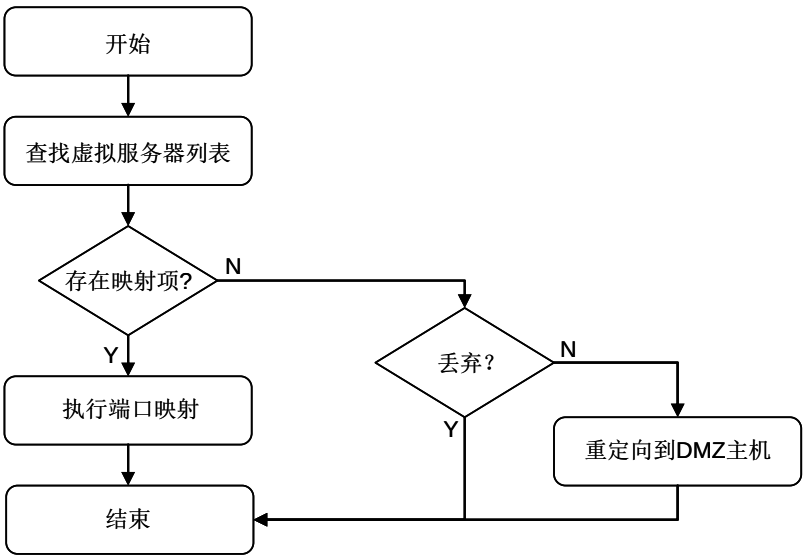
13.1.3 设置虚拟服务器

为保证局域网的安全，路由器会阻断从因特网主动发起的连接请求。因此，如果您想让因特网用户能够访问局域网内的服务器（比如：Web 服务器、Email 服务器、FTP 服务器等），需要设置虚拟服务器。

虚拟服务器也可称为端口映射，它可以将 WAN 口 IP 地址、外部端口号和局域网内服务器 IP 地址、内部端口号建立映射关系，使所有对该 WAN 口某服务端口的访问重定向到指定的局域网内服务器的相应端口。

路由器会根据以下步骤来进行端口映射：

图13-1 端口映射



页面向导：高级设置→地址转换→虚拟服务器

本页面为您提供如下主要功能：

设置当虚拟服务器列表中如果不存在对应的映射项时，对报文的处理方式（主页面。选择“丢弃”或“重定向到DMZ主机”，单击<应用>按钮生效）	
添加虚拟服务器列表项（单击主页面上的<新增>按钮，在弹出的对话框中设置相应的虚拟服务器参数，单击<增加>按钮完成操作）	

页面中关键项的含义如下表所示。

表13-1 页面关键项描述

页面关键项	描述
预置设置	路由器提供一些常用服务的预置设置选项，比如：FTP、Web等服务 在下拉列表框中选择某服务，服务名称、外部端口、内部端口项均将自动完成设置 **说明** • 如果路由器提供的预设服务没有您需要的，您可以自行设置服务信息 • 预设服务的端口号是常用端口号，如果需要，您可以自行修改 • 对于FTP、TFTP服务等，您需要开启对应的ALG项，且内部端口必须设置为标准端口号。例如：WAN侧客户端通过PASV模式（被动FTP）访问局域网内的FTP服务器，内部端口必须设置为 21
服务名称	输入虚拟服务器设置项的名称
外部端口	输入客户端访问虚拟服务器所使用的端口。取值范围：1～65535，端口范围必须从小到大。如果只有一个端口，则左右两边的文本框请填写同一端口号 **说明** 各设置项的外部端口不能重复，且内部端口和外部端口的设定个数必须一样，即内部端口和外部端口一一对应。比如：设置某个虚拟服务器，外部端口为 100～102，内部端口为 10～12。如果路由器收到外部 101 端口的访问请求，则路由器会把报文转发到内部服务器的 11 端口
内部端口	输入内部服务器上真实开放的服务端口。取值范围：1～65535，端口范围必须从小到大。如果只有一个端口，则左右两边的文本框请填写同一端口号 **说明** 各设置项的内部端口允许重复，且内部端口和外部端口的设定个数必须一样，即内部端口和外部端口一一对应
内部服务器IP	输入内部服务器的IP地址
是否启用	在下拉列表框中选择“启用”，表示此虚拟服务器生效；选择“禁用”，表示此虚拟服务器不生效

13.1.4 设置端口触发

当局域网内的客户端访问因特网上的服务器时，对于某些应用（比如：IP 电话、视频会议等），客户端向服务器主动发起连接的同时，也需要服务器向客户端发起连接请求。而缺省情况下，路由器收到 WAN 侧主动连接的请求都会拒绝，此时通信会被中断。

通过设置路由器的端口触发规则，当客户端访问服务器并触发规则后，路由器会自动开放服务器需要向客户端请求的端口，从而可以保证通信正常。当客户端和路由器长时间没有数据交互时，路由器会自动关闭之前对外开放的端口，最大限度地保证了局域网的安全。

页面向导：高级设置→地址转换→端口触发

本页面为您提供如下主要功能：

显示和修改当前您已添加的端口触发规则（主页面）	

添加端口触发规则（单击主页面上的<新增>按钮，在弹出的对话框中设置相应的参数，单击<增加>按钮完成操作）	

页面中关键项的含义如下表所示。

表13-2 页面关键项描述

页面关键项	描述
应用名称	输入端口触发设置项的名称
触发端口	输入局域网内的客户端向外网服务器发起请求的端口。取值范围：1～65535，端口范围必须从小到大。如果只有一个端口，则左右两边的文本框请填写同一端口号 **说明** 当局域网内的客户端通过触发端口与外部网络建立连接时，其相应的外来端口也将被打开。此时，外部网络的主机可以通过这些端口来访问局域网
外来端口	输入外网服务器需要主动向局域网内客户端请求的端口。取值范围：1～65535，可设置单一端口、端口范围或两者的组合，端口间用英文逗号“,”隔开，比如：100,200-300,400，表示请求端口为端口100，400及200到300之间的端口
是否启用	在下拉列表框中选择“启用”，表示此端口触发生效；选择“禁用”，表示此端口触发不生效

13.1.5 设置ALG应用

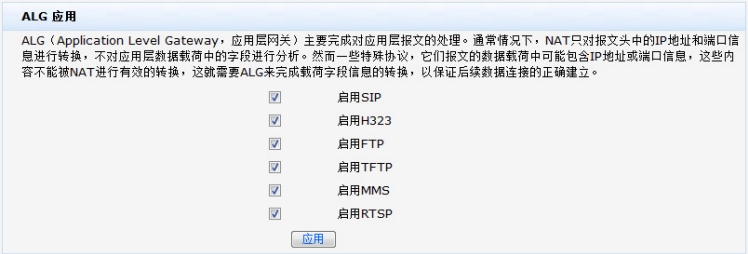
通常情况下，NAT 只对报文头中的 IP 地址和端口信息进行转换，不对应用层数据载荷中的字段进行分析。

然而，对于一些特殊的协议（比如：FTP、TFTP 等），它们报文的数据载荷中可能包含 IP 地址或端口信息，这些内容不能被 NAT 进行有效地转换，就可能会出现问题。比如：FTP 应用是由数据连接和控制连接共同完成的，而且数据连接的建立由控制连接中的载荷字段信息动态地决定，这就需要 ALG 来完成载荷字段信息的转换，以保证后续数据连接的正确建立。

针对需要 ALG 的一些应用层协议，您在使用时只需要在路由器上开启相应的项即可。

页面向导：高级设置→地址转换→ALG 应用

本页面为您提供如下主要功能：

设置ALG应用（缺省情况下，应用层协议的ALG应用均已经开启，建议您保留缺省设置）	

13.2 路由设置

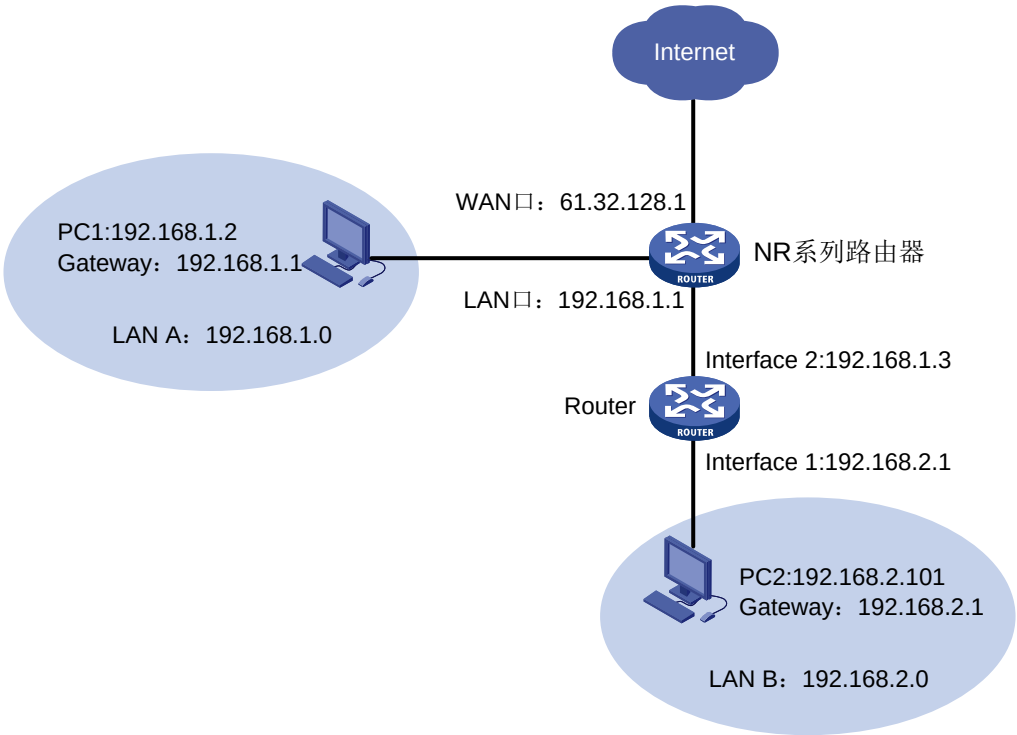
13.2.1 设置静态路由

静态路由是一种特殊的路由，需要您手工设置。设置静态路由后，去往指定目的地的报文将按照您指定的路径进行转发。在组网结构比较简单的网络中，只需设置静态路由就可以实现网络互通。恰当地设置和使用静态路由可以改善网络的性能，并可为重要的网络应用保证带宽。

静态路由的缺点在于：不能自动适应网络拓扑结构的变化，当网络发生故障或者拓扑发生变化后，可能会出现路由不可达，导致网络中断。此时必须由您手工修改静态路由的设置。

比如：如 图 13-2 所示，如果您希望LAN A中PC1 与LAN B中PC2 可以相互访问或LAN B中PC2 通过NR设备访问因特网，则可以在NR设备上设置一条静态路由（目的网段：192.168.2.0，下一跳地址：192.168.1.3）。

图13-2 静态路由设置举例组网图



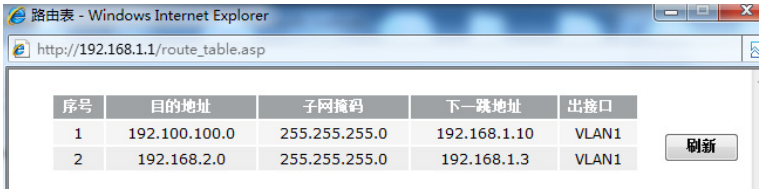
页面向导：高级设置→路由设置→静态路由

本页面为您提供如下主要功能：

显示和修改当前您已添加的静态路由（主页面）

添加静态路由（主页面。单击<新增>按钮，在弹出的对话框中设置相应的参数，单击<增加>按钮完成操作）

查看所添加的静态路由的生效情况（单击主页面上的“查看路由信息表”按钮，您即可在弹出的页面中查看已经生效的静态路由信息。如果您添加了一条错误的静态路由，该路由不会生效。您可以通过对比主页面的静态路由表和此处的路由信息，判断您是否添加了错误路由）



页面中关键项的含义如下表所示。

表13-3 页面关键项描述

页面关键项	说明
目的地址	输入需要到达的目的IP地址
子网掩码	输入需要到达的目的地址的子网掩码
下一跳地址	输入数据在到达目的地址前，需要经过的下一个路由器的IP地址
出接口	选择静态路由的出接口 **说明** 您必须选择正确的出接口，所添加的静态路由才能生效
描述	对此静态路由表项进行描述

13.2.2 设置策略路由

策略路由是一种依据您所制定的策略进行路由选择的机制。路由器提供独特的策略路由功能，可以根据报文的某些字段（比如：源/目的 IP 地址、协议类型等）来区分数据流，并从指定的接口发送出去，起到业务分流的作用。

比如：某企业拥有两条带宽大小不同的因特网线路，并设置了普通用户区（IP 地址范围是 192.168.1.2～192.168.1.100）和管理层用户区（IP 地址范围是 192.168.1.101～192.168.1.200）。此时，您可以通过策略路由功能（根据源 IP 地址段区分）来将带宽比较小的线路分配给普通区用户，将带宽比较大的线路分配给管理层用户。

页面向导：高级设置→路由设置→策略路由

本页面为您提供如下主要功能：

显示和修改当前您已添加的策略路由（主页面）	
添加策略路由（单击主页面上的<新增>按钮，在弹出的对话框中设置相应的参数，单击<增加>按钮完成操作）	

页面中关键项的含义如下表所示。

表13-4 页面关键项描述

页面关键项	描述
表项序号	由于系统会根据表项的序号来顺序匹配，因此您可以通过此选项来调整该表项的匹配优先级 缺省情况下，新增的表项会排在最后
协议类型	选择需要匹配的报文的协议类型（或输入对应的协议号）

页面关键项	描述
源端口	输入需要匹配的报文的源端口号（只有选择或者设置协议TCP/UDP之后，源端口才可配置） 源端口支持散列端口和端口范围两种输入方式： • 散列端口：格式为[!] n,m • 端口范围：格式为[!] n-m 缺省情况下，源端口号为1-65535，表示匹配所有的源端口  说明 “!”表示取反的意思（可选），即匹配除了所设置端口外的其他端口。比如：您设置源端口为!3-300，表示源端口在 3～300 范围内的报文均不会被匹配，其他源端口的报文都会被匹配。以下若涉及此“!”参数，意义相同，不再赘述
源IP地址段	输入需要匹配的报文的源IP地址段 源IP地址段支持三种输入方式： • 单独的 IP 地址：格式为[!] a.b.c.d • IP 地址网段：格式为[!] a.b.c.d/mask，mask 表示网络掩码长度，取值范围为 0～32 • IP 地址范围：格式为[!] a.b.c.d-e.f.g.h 缺省情况下，源IP地址段为0.0.0.0-255.255.255.255，表示匹配所有的源IP地址
目的端口	输入需要匹配的报文的目的端口号（只有选择或者设置协议TCP/UDP之后，源端口才可配置） 目的端口支持散列端口和端口范围两种输入方式： • 散列端口：格式为[!] n,m • 端口范围：格式为[!] n-m 缺省情况下，目的端口号为1-65535，表示匹配所有的目的端口
目的IP地址段	输入需要匹配的报文的目的IP地址段 目的IP地址段支持三种输入方式： • 单独的 IP 地址：格式为[!] a.b.c.d • IP 地址网段：格式为[!] a.b.c.d/mask，mask 表示网络掩码长度，取值范围为 0～32 • IP 地址范围：格式为[!] a.b.c.d-e.f.g.h 缺省情况下，目的IP地址段为0.0.0.0-255.255.255.255，表示匹配所有的目的IP地址
出接口	指定策略路由表项的出口 如果不选中“强制”复选框，当该出接口不可用时，匹配该策略的报文仍进行选路转发；如果选中“强制”复选框，当该出接口不可用时，匹配该策略的报文会直接被丢弃
生效时间	设置此策略路由项生效的时间段
是否启用	设置当前策略路由的状态 选择启用，表示使用此策略路由；选择禁用，表示不使用此策略路由
描述	对此策略路由项进行说明

13.3 应用服务

13.3.1 设置DDNS

当路由器通过 PPPoE 方式或动态方式连接到因特网时，所获取到的 IP 地址是不固定的。因此，给想访问本局域网内服务器的因特网用户带来很大的不便。

开启 DDNS 功能后，路由器会在 DDNS 服务器上建立一个 IP 与域名的映射表。当 WAN 口 IP 地址变化时，路由器会自动向指定的 DDNS 服务器发起更新请求，DDNS 服务器会更新域名与 IP 地址的映射关系。所以，无论路由器的 WAN 口 IP 地址如何改变，因特网上的用户仍可以通过域名对本局域网内的服务器进行访问。

说明

路由器的 DDNS 功能是作为 DDNS 服务的客户端工具，需要与 DDNS 服务器协同工作。使用该功能之前，请先到 www.pubyun.com 去申请注册一个域名。

页面向导：高级设置→应用服务→DDNS

本页面为您提供如下主要功能：

设置WAN口的DDNS	

页面中关键项的含义如下表所示。

表13-5 页面关键项描述

页面关键项	描述
WAN1 / WAN2 DDNS	开启或关闭对应WAN口的DDNS功能 缺省情况下，WAN口的DDNS功能处于关闭状态
用户名	输入在DDNS服务器上申请到的登录用户名
密码	输入在DDNS服务器上申请到的登录密码
注册的主机名	输入在DDNS服务器上申请的主机名，例如：ddnstest.3322.org
DDNS服务器地址	选择DDNS服务器地址
当前地址	显示对应WAN口当前的IP地址

页面关键项	描述
状态	显示当前对应WAN口的DDNS工作状态 • 未连接：与 DDNS 服务器连接失败 • 注册成功：向 DDNS 服务器注册成功 • 注册失败：DDNS 服务器认证没有通过，可能是用户名或密码错误

13.3.2 设置UPnP

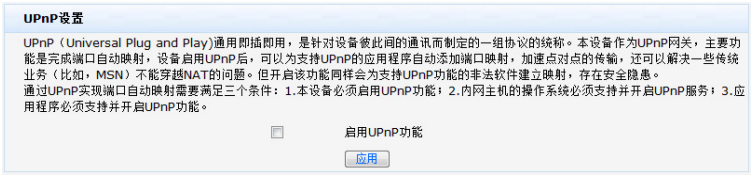
UPnP 主要用于实现设备的智能互联互通，无需用户参与和使用主服务器，能自动发现和控制来自各家厂商的各种网络设备。

启用 UPnP 功能，路由器可以实现 NAT 穿越：当局域网内的主机通过路由器与因特网通信时，路由器可以根据需要自动增加、删除 NAT 映射表，从而解决一些传统的业务不能穿越 NAT 的问题。

如需与 UPnP 功能配合使用，您所使用的计算机操作系统和应用程序均需要支持 UPnP 功能（比如：操作系统：Windows 7，应用程序：MSN）。

页面向导：高级设置→应用服务→UPnP

本页面为您提供如下主要功能：

开启UPnP功能（选中“启用UPnP功能”，单击<应用>按钮生效。缺省情况下，UPnP功能处于关闭状态）	

13.3.3 设置DNS Server

本设备支持静态 DNS Server 功能，通过手动指定网络设备的域名和 IP 的对应关系可实现域名解析的目的。

页面向导：高级设置→应用服务→DNS Server

本页面为您提供如下主要功能：

设置静态域名	
单击<新增>按钮，在弹出的对话框中设置静态dns，单击<增加>完成操作	

页面中关键项的含义如下表所示。

表13-6 页面关键项描述

页面关键项	描述
域名	网络设备的域名，域名不区分大小写。格式为：“XXXX.XXXX.XXXX”；例如：“myserver.com”
IP	网络设备的IP地址
描述	对此静态域名表项进行描述

14 设备管理

本章节主要包含以下内容：

14.1 基本管理

14.1.1 配置管理

页面向导：设备管理→基本管理→配置管理

本页面为您提供如下主要功能：

- 将当前路由器的设置信息以.cfg文件的形式备份到本地（比如：当您发生误操作或其他情况导致路由器的系统设置信息丢失时，您可用此备份文件进行恢复操作，保证路由器的正常运行）
- 将路由器当前的设置恢复到您之前备份过的设置
- 将路由器恢复到出厂设置(比如：当您从一个网络环境切换到另一个不同的网络环境的情况，可将路由器恢复到出厂设置，然后再进行重新设置，以适应当前的组网）

注意

- 请不要编辑备份在本地的设置文件。因为，设置文件经过加密，修改后不能再次恢复到路由器中。
- 恢复到出厂设置后，当前的设置将会丢失。如果您不希望丢失当前设置信息，请先对路由器进行备份操作。
- 恢复出厂设置后，路由器将会重新启动。在此期间请勿断开设备的电源。

14.1.2 设置系统时间

路由器支持通过 NTP 服务器来自动获取系统时间和手工设置系统时间两种方式。

1. 通过NTP服务器自动获取系统时间（推荐）

NTP 是由 RFC 1305 定义的时间同步协议，用来在分布式时间服务器和客户端之间进行时间同步。NTP 基于 UDP 报文进行传输，使用的 UDP 端口号为 123。

使用 NTP 的目的是对网络内所有具有时钟的设备进行时钟同步，使网络内所有设备的时钟保持一致，从而使设备能够提供基于统一时间的多种应用。对于运行 NTP 的本地系统，既可以接受来自其他时钟源的同步，又可以作为时钟源同步其他的时钟。

对于网络中的各台设备来说，如果单依靠管理员手工修改系统时间，不但工作量巨大，而且也不能保证时钟的精确性。通过 NTP，可以很快将网络中设备的时钟同步，同时也能保证很高的精度。

当路由器连接到因特网后，会自动从路由器缺省的 NTP 服务器或您手工设置的 NTP 服务器中获取时间。当通过 NTP 成功获取到系统时间后，该时间还会根据您选择的时区做相应的调整。

说明

如果路由器无法通过NTP服务器获取系统时间，则路由器会在 基本信息 页面中的“系统时间”处显示“网络未获取时间”，此时您需要手工设置系统时间。

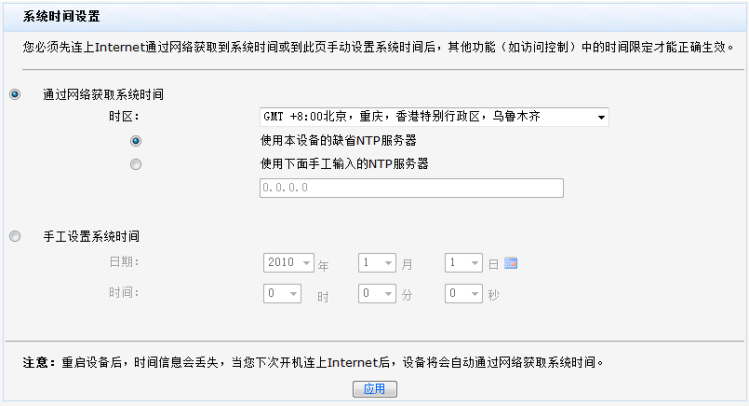
2. 手工设置系统时间

手工设置的系统时间不会与其他设备同步，也不支持时区的切换。当路由器重新启动后，手工设置的系统时间会丢失，并且路由器将恢复成了通过 NTP 服务器来自动获取系统时间。此时，如果您将路由器连接到因特网后，它会通过缺省的 NTP 服务器来获取系统时间。

页面向导：设备管理→基本管理→时间设置

本页面为您提供如下主要功能：

- 通过 NTP 服务器来自动获取系统时间（单击“通过网络获取系统时间”单选按钮，并指定相应的 NTP 服务器及时区，单击<应用>按钮生效）
- 手工设置系统时间（单击“手工设置系统时间”单选按钮，设置具体的时间参数，单击<应用>按钮生效）



说明

设置完成后，您可以通过查看 基本信息 页面中的“系统时间”来验证设置是否已生效。

14.1.3 软件升级

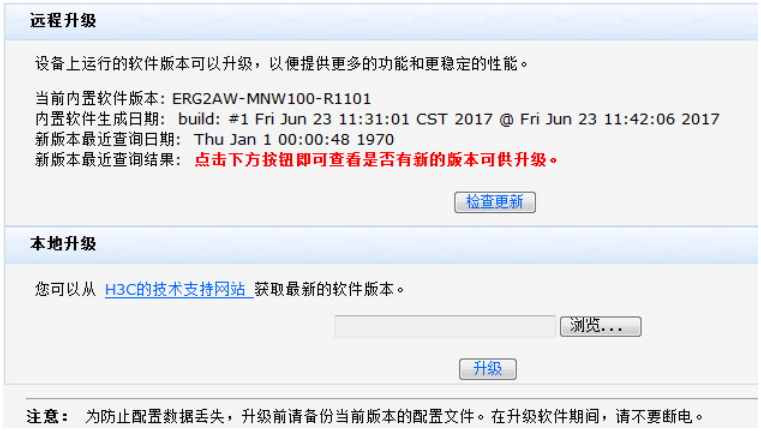
通过软件升级，您可以加载最新版本的软件到路由器，以便获得更多的功能和更为稳定的性能。

注意

- 请您在软件升级之前备份路由器当前的设置信息。如果升级过程中出现问题，您可以用其来恢复到原来的设置。
- 升级过程中请勿断开路由器的电源，否则可能会造成路由器不能正常工作。
- 路由器升级成功后，将会重新启动。

页面向导：设备管理→基本管理→软件升级

本页面为您提供如下主要功能：

升级软件 • 通过远程升级（单击<检查更新>按钮，查看是否有新版本可供升级，如检测到新版本，<检测更新>按钮将变成<升级>，单击<升级>按钮，即可开始升级） • 通过本地升级（单击页面上的“H3C 的技术支持网站”链接下载对应产品的最新软件版本，保存到本地主机。然后，单击<浏览>按钮，选择相应的升级软件。最后，单击<升级>按钮，即可开始升级）	

说明

软件升级后，您可以通过查看 基本信息页面中“软件版本”来验证当前运行的版本是否正确。

14.1.4 重新启动路由器

注意

- 重新启动期间，请勿断开路由器的电源。
- 重新启动期间，网络通信将暂时中断。

页面向导：设备管理→基本管理→重启动

单击页面上的<重启动>按钮，确认后，路由器重新启动。

14.2 USB管理

页面向导：设备管理→USB 管理→快速备份和恢复

本页面为您提供如下主要功能：

- 当插上 U 盘等存储设备，USB 接口会显示已连接，并根据设备类型，USB 模式会显示为存储模式。缺省情况下，USB 接口上没有插任何设备，USB 状态和 USB 模式均显示未连接
- 将当前路由器的配置信息以.cfg 文件的形式快速备份到 USB 设备上（比如：当您发生误操作或其他情况导致路由器的系统配置信息丢失时，您可用此备份文件进行恢复操作，保证路由器的正常运行）
- 将路由器当前的配置从 USB 设备上恢复到您之前备份过的配置
- 设备启动的时候，可以从 USB 设备加载并恢复您之前备份过的配置

说明

插上USB设备后，您可以通过查看 基本信息 页面中“软件版本”来验证当前运行的版本是否正确。

注意

- 请不要编辑备份在 USB 设备上的配置文件。因为配置文件经过加密，修改后不能再次恢复到路由器中。
- 恢复到出厂配置后，当前的配置将会丢失。如果您不希望丢失当前配置信息，请先对路由器进行备份操作。
- 恢复出厂配置后，路由器将会重新启动。在此期间请勿断开设备的电源。

14.3 远程管理

路由器为您提供了远程登录管理的功能，即因特网上的主机可以通过路由器的 WAN 口来实现 Web 或 Telnet 登录。

远程 Web 管理支持 HTTP 和 HTTPS 两种访问方式。HTTPS 相对于 HTTP，在安全性方面有所增强，它将 HTTP 和 SSL 结合，通过 SSL 对客户端身份和服务器进行验证，对传输的数据进行加密，从而实现了对设备的安全管理。

HTTPS 通过 SSL 协议，从以下几方面提高了安全性：

- 客户端通过数字证书对服务器进行身份验证，保证客户端访问正确的服务器；
- 服务器通过数字证书对客户端进行身份验证，保证合法客户端可以安全地访问设备，禁止非法的客户端访问设备；

- 客户端与设备之间交互的数据需要经过加密，保证了数据传输的安全性和完整性，从而实现了对设备的安全管理。

说明

- 同一时间，路由器最多允许五个用户远程通过 Web 或 Telnet 进行管理和设置。
- 缺省情况下，路由器的远程 Web 管理和远程 Telnet 管理均处于关闭状态。

页面向导：设备管理→远程管理→远程管理

本页面为您提供如下主要功能：

- 开启远程 Web 管理功能（选中“启用远程 web 管理”复选框，选择访问方式，并设置相关的参数，单击<应用>按钮生效）
- 开启远程 Telnet 管理功能（选中“启用远程 telnet 管理”复选框，设置相关的参数，单击<应用>按钮生效）

页面中关键项的含义如下表所示。

表14-1 页面关键项描述

页面关键项	描述
访问方式	当选择HTTP访问方式时，远程用户需要在浏览器的地址栏中输入http://xxx.xxx.xxx.xxx:port登录路由器；当选择HTTPS访问方式时，远程用户需要在浏览器的地址栏输入https://xxx.xxx.xxx.xxx:port登录路由器 说明 • xxx.xxx.xxx.xxx 是指路由器 WAN 口的 IP 地址，port 是指您所指定的“设备的远程管理端口” • 如果您使用 HTTPS 方式访问路由器，路由器会向您发放一份证书。此证书可能因为不受信任而被浏览器阻止，您只要选择信任此证书，继续操作便可进入路由器的 Web 登录页面
远程管理PC的IP范围	设置远程用户的IP地址范围，仅在该指定范围内的用户才允许远程管理路由器 缺省情况下，允许所有用户对路由器进行远程管理
设备的远程管理端口号	设置对路由器进行远程管理的端口号

14.4 用户管理

14.4.1 登录管理

页面向导：设备管理→用户管理→登录管理

本页面为您提供如下主要功能：

- 设置局域网内允许管理路由器的用户 IP 地址范围（在“LAN 内管理 PC 的 IP 范围”文本框中输入允许管理路由器的 IP 地址范围，单击<应用>按钮生效。此限制功能仅对 http/https、telnet 访问有效）
- 设置 Web 用户超时时间（在“超时时间”文本框中输入时间参数，单击<应用>按钮生效）
- 开启/关闭 Web 登录页面验证码功能（选择功能状态，单击<应用>按钮生效）
- 查看当前已登录的用户信息
- 注销已登录用户（单击某用户所对应的<注销>按钮，即可将该用户强制退出。如需登录，需要重新认证）

说明

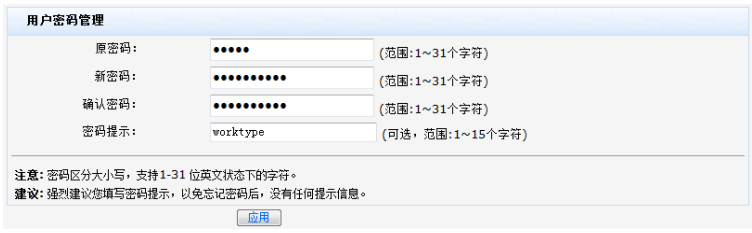
- 当由于误操作而未将自身的IP划入到允许管理路由器的用户IP地址范围内，导致无法登录路由器时，您可以通过 **admin acl default**命令将其恢复为缺省设置（缺省情况下，允许局域网内所有用户访问路由器）。
- 验证码功能会使您的系统安全性更高。如果您想在登录路由器 Web 设置页面时不需要输入验证码，可禁用验证码功能。

14.4.2 密码管理

页面向导：设备管理→用户管理→密码管理

本页面为您提供如下主要功能：

修改路由器的登录密码



15 系统监控

本章节主要包含以下内容：

15.1 查看运行信息

15.1.1 查看基本信息

页面向导：系统监控→运行信息→基本信息

本页面为您提供如下主要功能：

- 查看设备基本信息（比如：当前运行的软件版本号、CPU/内存使用率、运行时间等）
- 查看 WAN 口当前的状态信息（比如：WAN 口的工作模式、连接因特网的方式、IP 地址等）
- 查看设备具体的无线网络状态（比如：2.4G 无线状态、5G 无线状态）

页面中关键项的含义如下表所示。

表15-1 页面关键项描述

页面关键项	描述
生产序列号	显示路由器的序列号
软件版本	显示路由器当前的软件版本 说明 页面中的软件版本信息仅作参考，请以路由器加载软件版本后的最终显示为准
Bootrom版本	显示路由器当前的Bootrom版本
硬件版本	显示路由器当前的硬件版本
系统资源	显示路由器 CPU及内存的使用百分比，您可以通过该参数值来简单判断路由器当前是否运行正常
运行时间	显示路由器从上一次通电后到现在的总运行时间
系统时间	显示路由器当前的系统时间和系统时间设置方式
USB状态	显示路由器当前的USB接口状态信息
连接方式	显示路由器WAN口连接到因特网的方式
链路状态	显示路由器WAN口当前的链路状态 • 已连接：WAN 口工作正常 • 物理连接已断开：WAN 口物理链路出现故障 • 线路检测失败：WAN 口检测没有成功。此时，WAN 口不能转发任何报文 • WAN 口禁用：当前 WAN 口被禁用 • 接口空闲：接口物理链路正常，但该接口不进行工作。比如：在主备模式下，主接口工作正常时，备份接口处于空闲状态 • 连接中：在 PPPoE、DHCP 连接方式下，路由器正在与服务器建立连接 • 服务器没响应：在 PPPoE、DHCP 连接方式下，对应的服务器无响应或线路异常 • IP 地址已释放：在 DHCP 连接方式下，单击页面上的<释放>按钮主动断开连接，显示此状态。此状态下，接口不再尝试与服务器进行连接 • 连接已断开：在 PPPoE 连接方式下，单击页面上的<释放>按钮主动断开连接，显示此状态。此状态下，接口不再尝试与服务器进行连接 • 用户名或密码错误：在 PPPoE 连接方式下，输入的用户名和密码错误
IP地址	显示WAN口当前的IP地址
子网掩码	显示WAN口当前的子网掩码
网关地址	显示WAN口当前的网关地址
主DNS服务器	显示WAN口的主DNS服务器地址
辅DNS服务器	显示WAN口的辅DNS服务器地址
DHCP剩余时间	显示DHCP租约的剩余时间 说明 仅当连接方式为 DHCP 方式时才显示

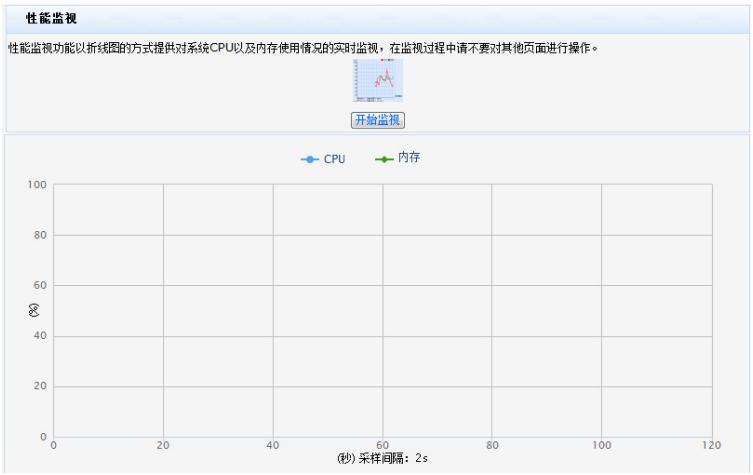
页面关键项	描述
MAC地址	显示WAN口当前生效的MAC地址 说明 当您设置了 WAN 口的 MAC 地址克隆后，此 MAC 地址会出现相应的变化
连接	单击此按钮建立WAN口的链路连接 说明 仅当连接方式为 PPPoE、DHCP 时才显示此按钮
释放	单击此按钮释放当前路由器WAN口动态获取到的IP地址 说明 仅当连接方式为 PPPoE、DHCP 时才显示此按钮

15.1.2 实时监视性能状态

当您开启性能实时监视功能后，系统会对路由器 CPU 和内存的使用进行实时采样，并通过一个直观的滚动折线图来显示数据变化，供您及时了解 CPU 和内存的使用率是否过高，波动是否正常。

页面向导：系统监控→运行信息→性能监视

本页面为您提供如下主要功能：

单击页面中的<开始监视>按钮，您即可在弹出的页面中实时监视路由器CPU和内存的使用状态	

15.1.3 技术支持信息

页面向导：系统监控→运行信息→技术支持

本页面为您提供了路由器相关的技术支持类信息，比如：客服热线、H3C 公司网站/技术论坛链接等。

15.2 查看和管理日志信息

路由器能够记录当前运行过程中的设置状态变化、网络攻击等信息，可以帮助您快速定位设备故障、了解网络情况及对网络攻击进行定位。

路由器还支持把日志信息实时发送给日志服务器的功能，以免路由器重新启动后，所有记录的日志都会丢失。

说明

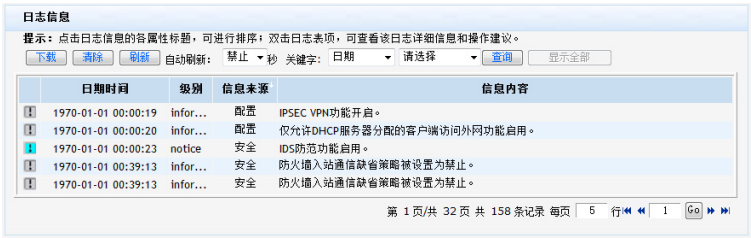
当路由器中的日志信息存满后，新的日志将会覆盖最早被记录的日志信息。因此，为了避免日志信息遗漏，建议您使用日志服务器来记录日志信息。此时，需要您预先在局域网内或外网建立相应的日志服务器，且与路由器保持连通。

15.2.1 查看日志信息

页面向导：系统监控→系统日志→日志信息

本页面为您提供如下主要功能：

- 显示和查询路由器上电启动以来所产生的日志信息
- 将路由器所记录的日志信息下载到本地（单击<下载>按钮，可将日志信息导出到本地保存）
- 清除路由器所记录的日志信息（单击<清除>按钮即可完成操作）



15.2.2 管理日志信息

页面向导：系统监控→系统日志→日志管理

本页面为您提供如下主要功能：

- 控制日志信息输出的等级(在“日志记录等级”下拉框中选择某个等级，单击<应用>按钮生效。此时，仅不大于该等级的日志信息才被路由器记录或允许发送到日志服务器。日志等级的具体描述请参见“表 15-2”)
- 控制日志信息输出的来源（选择您需要关注的日志信息来源，单击<应用>按钮生效。日志信息来源描述请参见“表 15-3”）
- 将日志信息同步输出到日志服务器（选中“发送到日志服务器”复选框，输入服务器地址，单击<应用>按钮生效）
- 开启/关闭路由器日志信息记录功能（选中“本地不记录日志”复选框，单击<应用>按钮，本地记录日志信息功能关闭。反之，开启）

表15-2 日志信息等级描述

严重等级	数值	描述
emergency	0	系统不可用
alert	1	需要立即做出反应的信息
critical	2	严重信息
error	3	错误信息
warning	4	告警信息
notice	5	正常出现但是重要的信息
informational	6	需要记录的通知信息
debug	7	调试过程产生的信息

表15-3 日志信息来源描述

日志来源	描述
系统	所有路由器功能运行的日志信息。比如：您使用PPPoE方式连接因特网时，路由器会输出相应的日志信息
配置	当更改了路由器的配置操作时输出的日志信息。比如：功能的开启或关闭
安全	路由器进行防攻击、报文过滤等操作时输出的日志信息

日志来源	描述
流量信息	路由器流量统计时输出的日志信息。比如：局域网内的某台主机的网络连接数超过限速值时，路由器会输出相应的日志信息
VPN	路由器IPSec VPN相关的日志信息

15.3 流量监控

路由器为您提供了端口流量和 IP 流量的监控功能，您可以根据路由器所获取的统计数据，更好地了解网络运行状况，便于管理与控制。

- 监控端口流量：统计每个物理端口的流量。
- 监控 IP 流量：统计局域网内各在线主机通过 WAN 口的流量。

说明

路由器支持以下两种查看模式供您对端口流量和 IP 流量进行监控：

- 比特模式：以每秒传输的比特数为单位来显示流量和速率信息。
- 包模式：以每秒传输的报文个数为单位来显示流量和速率信息。

15.3.1 监控端口流量

页面向导：系统监控→流量监控→端口流量

本页面为您提供如下主要功能：

在比特模式下查看路由器各端口的发送/接收流量、发送/接收速率及链路状态


端口流量统计

查看方式: 列表模式 图形化模式

查看模式: 比特模式 包模式

端口镜像信息: LAN3 >>> LAN1

端口	发送流量(bit)	接收流量(bit)	发送速率(Kbps)	接收速率(Kbps)	链路状态
WAN1	0	0	0	0	未连接
WAN2	0	0	0	0	未连接
LAN1	0	0	0	0	未连接
LAN2	89.6527M	14.5409M	26.368	3.471	1000M全双工
LAN3	0	0	0	0	未连接
LAN4	0	0	0	0	未连接

清零 刷新 10 秒

在包模式下查看路由器各端口的发送/接收流量、发送/接收速率及链路状态


端口流量统计

查看方式: 列表模式 图形化模式

查看模式: 比特模式 包模式

端口镜像信息: LAN3 >>> LAN1

端口	发送流量(pkt)	接收流量(pkt)	错误包数(pkt)	丢包数(pkt)	发送包速率(pps)	接收包速率(pps)	链路状态
WAN1	0	0	0	0	0	0	未连接
WAN2	0	0	0	0	0	0	未连接
LAN1	0	0	0	0	0	0	未连接
LAN2	13.1630K	13.0150K	0	0	3	3	1000M全双工
LAN3	0	0	0	0	0	0	未连接
LAN4	0	0	0	0	0	0	未连接

清零 刷新 10 秒

页面中关键项的含义如下表所示。

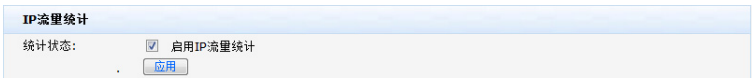
表15-4 页面关键项描述

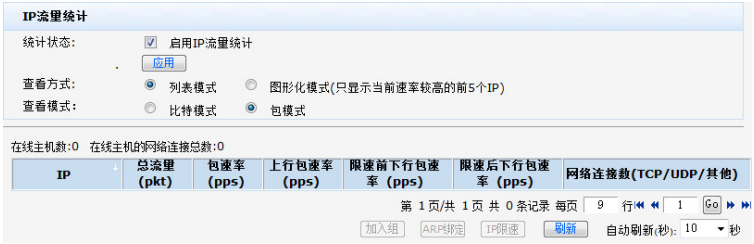
页面关键项	描述
统计周期	选择页面统计数据刷新的时间间隔，缺省为10秒
自动刷新	选中该复选框，页面的统计数据会根据统计周期自动刷新
查看方式	选择端口流量统计的显示方式 缺省情况下，路由器使用列表模式
查看模式	选择端口流量统计的显示模式 缺省情况下，路由器使用比特模式
端口镜像信息	显示路由器各物理端口之间的端口镜像状态
发送流量/接收流量	显示路由器相应端口发送/接收的总流量
发送速率/接收速率 发送包速率/接收包速率	显示路由器相应端口发送/接收报文的速率
错误包数	显示路由器相应端口发送/接收的错误包总数
丢包数	显示路由器相应端口丢包的总数
链路状态	显示对应端口的链路状态 说明 如果该端口未有物理连接或出现链路故障，则显示“未连接”

15.3.2 监控IP流量

页面向导：系统监控→流量监控→IP 流量

本页面为您提供如下主要功能：

启用局域网IP流量统计功能（选中“启用内网IP流量统计”复选框，单击<应用>按钮生效。缺省情况下，IP流量统计功能处于关闭状态）	
在比特模式下查看局域网内各在线主机通过WAN口的总流量、总速率、上行/下行速率及网络连接数	

在包模式下查看局域网内各在线主机通过WAN口的总流量、总速率、上行/下行速率及网络连接数	

页面中关键项的含义如下表所示。

表15-5 页面关键项描述

页面关键项	描述
统计周期	选择页面统计数据刷新的时间间隔，缺省为10秒
自动刷新	选中该复选框，页面的统计数据会根据统计周期自动刷新
查看方式	选择IP流量统计的显示方式 缺省情况下，路由器使用列表模式
查看模式	选择IP流量统计的显示模式 缺省情况下，路由器使用比特模式
总流量	显示相应主机通过WAN口的总流量
速率 包速率	显示相应主机通过WAN口的总速率
上行速率/限速前下行速率/限速后下行速率 上行包速率/限速前下行包速率/限速后下行包速率	显示相应主机通过WAN口的上行速率和限速前后下行速率 **说明** 您可以通过路由器的 IP流量限制功能来限制对应主机的上行速率/下行速率
网络连接数	显示对应的主机所尝试的网络连接总数 **说明** 您可以通过路由器的 网络连接限数功能来限制对应主机的网络连接总数

15.3.3 安全统计

当您开启了路由器防攻击相应的功能后，路由器的安全统计模块会对攻击报文的个数和可疑的一些报文进行统计。您可以通过查看和分析统计数据的变化，来判断网络环境是否存在欺骗和攻击行为。

页面向导：系统监控→流量监控→安全统计

本页面为您提供如下主要功能：

- 开启路由器的报文统计功能（选中“开启数据包统计功能”复选框，单击<应用>按钮生效）
- 对源认证失败的和可疑的报文进行统计（具体报文的描述请参见“表 15-6”）

页面中关键项的含义如下表所示。

表15-6 页面关键项描述

页面关键项	描述
报文源认证失败	源认证失败的判断依赖于路由器的报文源认证设置。对于源认证失败的报文，路由器会直接将其丢弃。如果您在统计数据中发现此类报文的个数不断增加，可能您的网络环境中存在IP欺骗或MAC欺骗攻击行为
LAN侧可疑	当来自LAN侧的报文未与路由器表项冲突（比如：ARP表项），但又不能确认该报文是否来源于合法的主机时，则认为是可疑报文。缺省情况下，路由器允许其通过。但如果您在统计数据中发现此类报文的个数不断增加，可能您的组网环境出现了问题或存在攻击行为
WAN侧非法	由因特网侧主动向路由器发送的报文，比如：因特网侧主机主动尝试与路由器建立Telnet连接，则认为是非法报文。如果在特定时间段内，您在统计数据中发现此类报文的个数不断增加，并造成网络稳定性下降，则可能遭受到了来自因特网侧的攻击，建议您更改WAN口的IP地址，或者联系运营商进行处理

15.4 网络维护

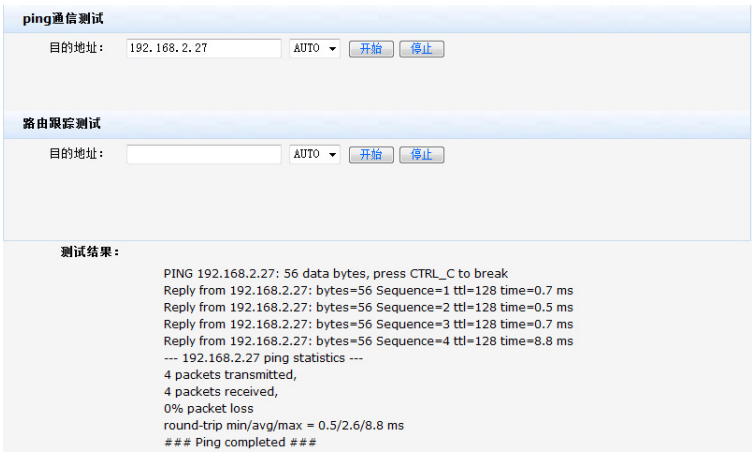
15.4.1 网络诊断

路由器为您提供两种网络诊断工具：

- ping 测试：检测路由器与目标主机或另一台设备是否连通。
- 路由跟踪测试：检查从路由器到达目标主机所经过的路由情况。

页面向导：系统监控→网络维护→网络诊断

本页面为您提供如下主要功能：

选择ping测试进行网络诊断（输入“目的地址”，选择测试的端口，单击<开始>按钮执行诊断）	
选择路由跟踪测试进行网络诊断（输入“目的地址”，选择测试的端口，单击<开始>按钮执行诊断）	

说明

- ping 测试结果

当路由器可以接收到从目标主机侧返回的应答时，表示路由器与目标主机连通（如上图所示）；否则表示两者之间不连通，可能网络存在问题。

- 路由跟踪测试结果

如上图所示，只存在一跳，表示路由器和目标主机之间属于直连路由。

15.4.2 抓包工具

通过设置抓包工具的相关参数，直接抓取经过路由器接口的数据包，便于维护人员更有效地分析及定位问题，降低维护成本。

页面向导：系统监控→网络维护→抓包工具

本页面为您提供如下主要功能：

在对话框中设置匹配规则来控制抓包的数据报文 单击<开始>按钮，系统开始抓包，抓包过程中，当前抓取的分组数会显示在页面上	
单击<停止>按钮即可停止数据包的抓取，此时系统会自动提示您导出抓包文件“tcpdump.pcap”到本地，该文件可使用wireshark（ethereal）等软件打开	

页面中关键项的含义如下表所示。

表15-7 页面关键项描述

页面关键项	描述
接口	选择抓取报文的来源接口 说明 支持当前路由器的所有 WAN、VLAN 等接口
协议	选择需要抓取的报文的协议类型 说明 • 缺省协议为 ALL，即抓取所有类型的数据包 • 如您手动修改协议为 ARP、RARP、ICMP 时，源端口号和目的端口号将无法设置

页面关键项	描述
源/目的主机	设置抓取报文的源/目的主机过滤条件，以抓取符合条件的数据包： • 所有主机：抓取所有源/目的主机的数据包 • IP 地址过滤：仅允许抓取源/目的主机为所设置 IP 地址的数据包 • MAC 地址过滤：仅允许抓取源/目的主机为所设置 MAC 地址的数据包
IP地址	设置抓取报文的源/目的IP地址，点分十进制类型，取值范围：0.0.0.0～255.255.255.255
MAC地址	设置抓取报文的MAC地址，输入格式为xx:xx:xx:xx:xx:xx （或xx-xx-xx-xx-xx-xx、或xxxx-xxxx-xxxx），且不区分大小写
源/目的端口	输入抓取报文的源/目的端口号，需要配置正确的端口号才能抓到相应端口的报文。 取值范围：1～65535，最多可设置10个单一端口，端口间用英文逗号“,”隔开，比如：100,200,300 说明 如果要抓取所有端口的报文，您可以将其设置为 0
主机关系	设置源主机与目的主机之间的逻辑关系： • 或：设置抓取报文为源主机与目的主机之间所有报文的并集 • 与：设置抓取报文为源主机与目的主机之间所有报文的交集
双向抓取	选中该项，则系统会抓取源主机与目的主机之间的双向报文 说明 只有在主机关系设置为“与”时，该选项方可勾选
抓取包长度	设置抓包的最大报文长度，当tcpdump的数据包长度超过所设数值时，数据包将会被截断。取值范围：1～2000 说明 如果您设置的抓取包长度过大，会增加包的处理时间，并减少可缓存数据包的数量，从而可能导致部分数据包的丢失。故而，在保证数据包长度足够的前提下，建议您设置尽可能小的抓包长度
内存使用阈值	设置抓包过程中所允许的系统内存最大使用率，当内存使用率达到所设阈值时，系统会主动停止抓包，并提示用户导出抓包文件。取值范围为70～90，缺省值为80

15.4.3 系统自检

页面向导：系统监控→网络维护→系统自检

路由器为您提供简便的系统自检功能，您可以随时单击页面中的<开始>按钮，在弹出的页面中将会分类显示检测结果及一些注意事项。通过该检测信息，您可以判断路由器当前的设置是否合理、运行是否正常等。

15.4.4 导出故障定位信息

页面向导：系统监控→网络维护→一键导出

当路由器运行出现异常时，您可以单击页面中的<导出>按钮，确认后，路由器可以自动把当前的运行状态、故障定位所需的各种信息压缩成一个定位信息文件下载到本地。H3C 技术支持人员可以根据该文件快速、准确地定位问题，从而可以更好地为您解决路由器的使用问题。

16 典型组网配置举例

16.1 企业典型组网配置举例

16.1.1 组网需求

- 某企业使用电信线路接入，对应的带宽为 30M，带机量为 100 台；
- 提供内部网络 SSID 为 H3C、访客网络 SSID 为 H3C_GUEST，加密方式为 WPA-PSK/WPA2-PSK 加密的无线接入服务，以确保内网和外网的无线网络安全；
- 防止局域网内的 ARP 攻击；
- 防止局域网内某些主机使用 P2P 软件（比如：BT、迅雷等）过度占用网络资源；
- 禁止局域网内某些主机（比如：192.168.1.2～192.168.1.10）在某个时间段（比如：每天的 08:00～18:00）访问外网；
- 禁止局域网内除某些主机（比如：192.168.1.50～192.168.1.55）外，其他主机在某个时间段（比如：每天的 08:30～18:00）访问某些网站（比如：www.xxx.com 等）；
- 禁止局域网内某些主机（比如：192.168.1.15～192.168.1.20）使用 QQ 上线。

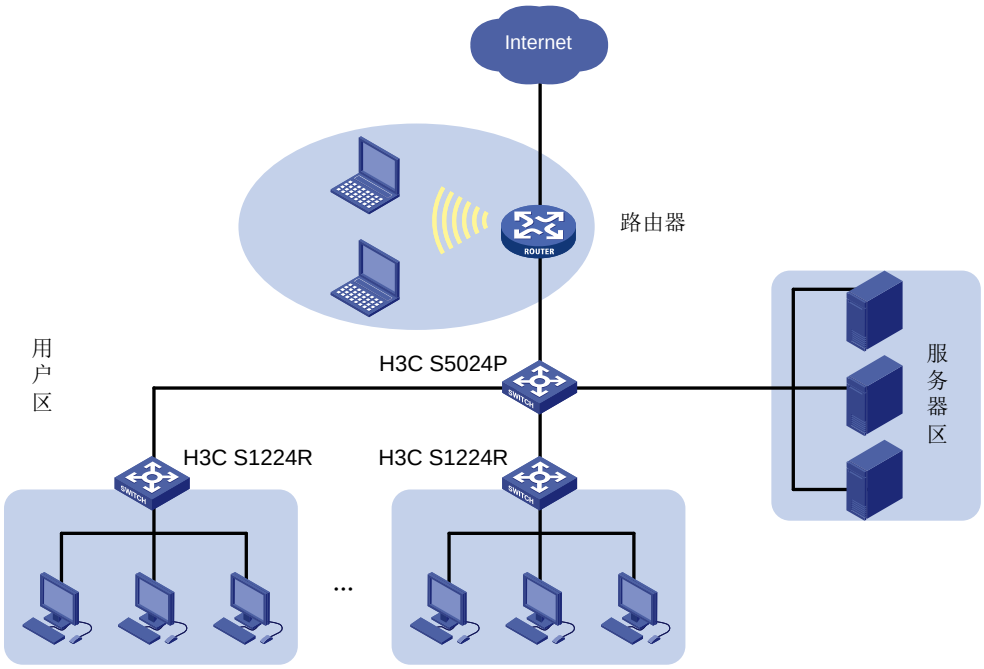
16.1.2 组网配置方案

下面以具体的组网配置方案为例进行说明：

- 网关使用 H3C NR-1200W、汇聚交换机采用 H3C S5024P、接入交换机采用 H3C S1224R；
- 设置 WAN 口通过静态方式连接到因特网；
- 使用 DHCP 服务器功能给局域网内各主机动态分配 IP 地址；
- 开启 ARP 绑定功能来防止 ARP 表项受到攻击；
- 设置 IP 流量限制和网络连接数限制，防止 P2P 软件过度占用网络资源；
- 设置防火墙的出站通信策略功能来禁止特定主机在某个时间段访问外网；
- 设置网站过滤功能来禁止局域网内某些主机访问指定网站；
- 设置业务控制功能来禁止某些主机使用 QQ 上线。

16.1.3 组网图

图16-1 典型应用组网图



16.1.4 设置步骤

说明

此典型配置举例仅体现 NR-1200W 上的设置，且所涉及的设置均在 NR-1200W 缺省配置的基础上进行。如果您之前已经对 NR-1200W 做过相应的设置，为了保证效果，请确保当前设置和以下设置不冲突。

1. 在管理计算机的 Web 浏览器地址栏中输入 http://192.168.1.1，回车。输入用户名和密码（缺省均为 admin，区分大小写），单击<登录>按钮后便可进入 Web 设置页面

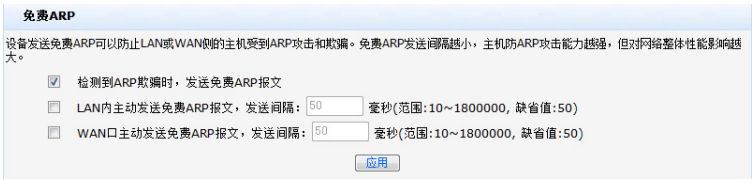
2. 选择“无线管理→基本设置→内部网络”，设置内部网络 SSID 名称、加密方式和密钥，供公司员工办公时使用，单击<应用>按钮生效

3. 选择“无线管理→基本设置→访客网络”，设置访客网络 SSID 名称、加密方式和密钥，供访客使用，单击<应用>按钮生效

4. 选择“接口管理→WAN 设置→连接到因特网”，在“WAN 网口”下拉框中选择“静态地址（手工配置地址）”选项。用电信提供的参数填写 WAN 口的上网参数，单击<应用>按钮生效

5. 选择“安全专区→ARP 安全→ARP 检测”，设置 IP 地址搜索范围，单击<扫描>按钮开始搜索。待搜索完毕后，请确认搜索是否有遗漏（比如：查看搜索到的条目数是否与客户端的开机数一致）。如果没有遗漏，单击<全选>按钮选中所有的表项，再单击<静态绑定>按钮，将所有客户端主机的 IP/MAC 进行绑定即可；如果存在遗漏，您还可以选择“安全专区→ARP 安全→ARP 绑定”，手工添加 ARP 绑定项

6. 选择“安全专区→ARP 安全→ARP 防护”，选中“检测到 ARP 欺骗时，发送免费 ARP 报文”复选框，单击<应用>按钮生效

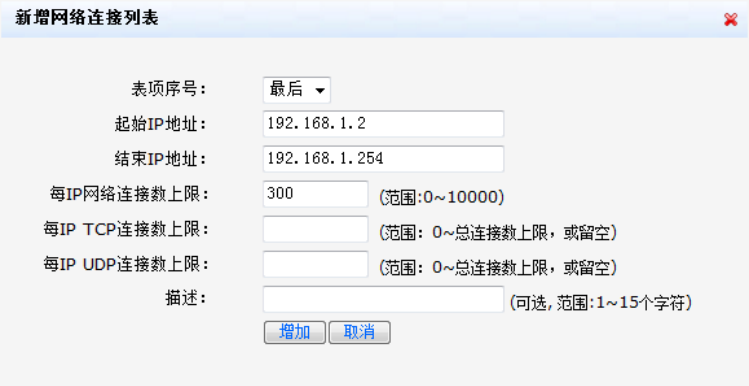


7. 选择“QoS 设置→流量管理→IP 流量限制”。选中“启用 IP 流量限制”复选框和“允许每 IP 通道借用空闲的带宽”单选框，单击<应用>按钮生效

8. 单击<新增>按钮，在弹出的对话框中设置 IP 流量限制规则：建议上行和下行流量的上限值均设置为 300Kbps。同时，您也可以根据实际的网络情况对其进行适当地调整

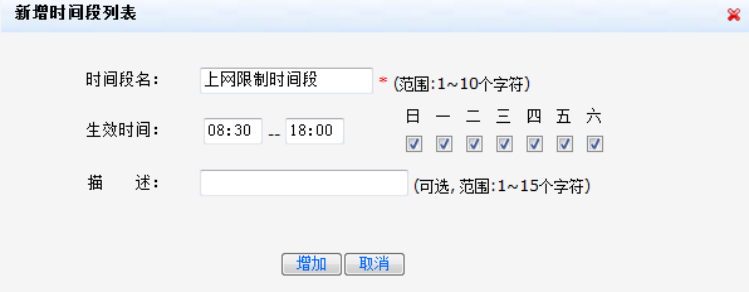
9. 选择“QoS 设置→连接限制→网络连接限数”，选中“启用网络连接限数”复选框，单击<应用>按钮生效

10. 单击<新增>按钮，在弹出的对话框中设置对每台客户端主机进行网络连接数限制（建议网络连接数设置在 300～500 之间），单击<增加>按钮完成操作



11. 选择“安全专区→防火墙→出站通信策略”，单击<新增>按钮，在弹出的对话框中设置相应的策略，如右图所示。单击<增加>按钮完成操作

12. 选择“上网管理→组管理→时间段管理”，单击<新增>按钮，在弹出的对话框中设置相应的时间段列表，如右图所示。单击<增加>按钮完成操作

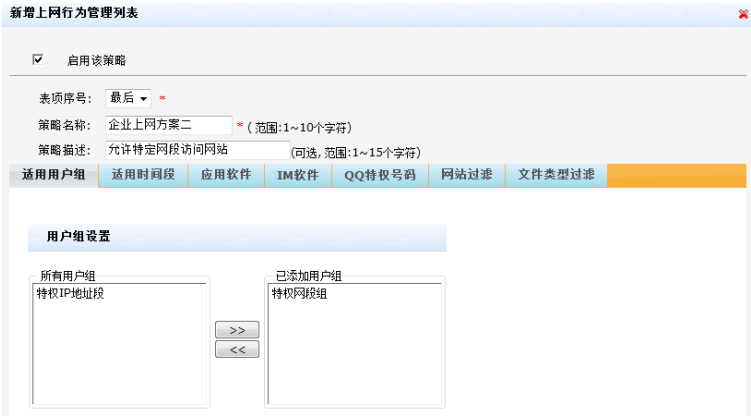


13. 选择“上网管理→策略管理→行为策略管理”，单击<新增>按钮，在弹出的对话框中设置相应的上网行为管理策略，如右图所示，设置策略名称和策略描述，选择适用时间段列表，并添加相应时间段

14. 选择网站过滤，并进行相应设置，如右图所示。选中“启用网站过滤功能”复选框，再选中“仅禁止访问列表中的网站地址”单选框，单击<新增>按钮，设置精确匹配的网站地址为“www.xxx.com”，并单击<保存>按钮生效，单击<完成策略配置>按钮完成操作

15. 选择“上网管理→组管理→用户组管理”，单击<新增>按钮，在弹出的对话框中设置“特权网段组”用户组列表，如右图所示。单击<增加>按钮完成操作

16. 选择“上网管理→策略管理→行为策略管理”，单击<新增>按钮，在弹出的对话框中设置相应的上网行为管理策略，如右图所示，设置策略名称和策略描述，选择适用用户组列表，并添加相应用户组



17. 选择网站过滤，并进行相应设置，如右图所示。不选中“启用网站过滤功能”复选框，单击<完成策略配置>按钮完成操作

18. 选择“上网管理→组管理→用户组管理”，单击<新增>按钮，在弹出的对话框中设置“特权 IP 地址段”用户组列表，如右图所示。单击<增加>按钮完成操作

19. 选择“上网管理→策略管理→行为策略管理”，单击<新增>按钮，在弹出的对话框中设置相应的上网行为管理策略，如右图所示，设置策略名称和策略描述，选择适用用户组列表，并添加相应用户组

20. 选择 IM 软件，并进行相应设置，如右图所示。选中“启用 IM 软件控制功能”复选框，再选中“禁止 QQ 上线”复选框，单击<完成策略配置>按钮完成操作

16.2 上网管理典型配置举例

16.2.1 组网需求

企业某部门通过 NR-1200W 连接网络，对该区域用户群进行上网行为管理，具体需求如下：

(1) 设置区域内用户群的 IP 地址范围为 192.168.1.0～192.168.1.100；

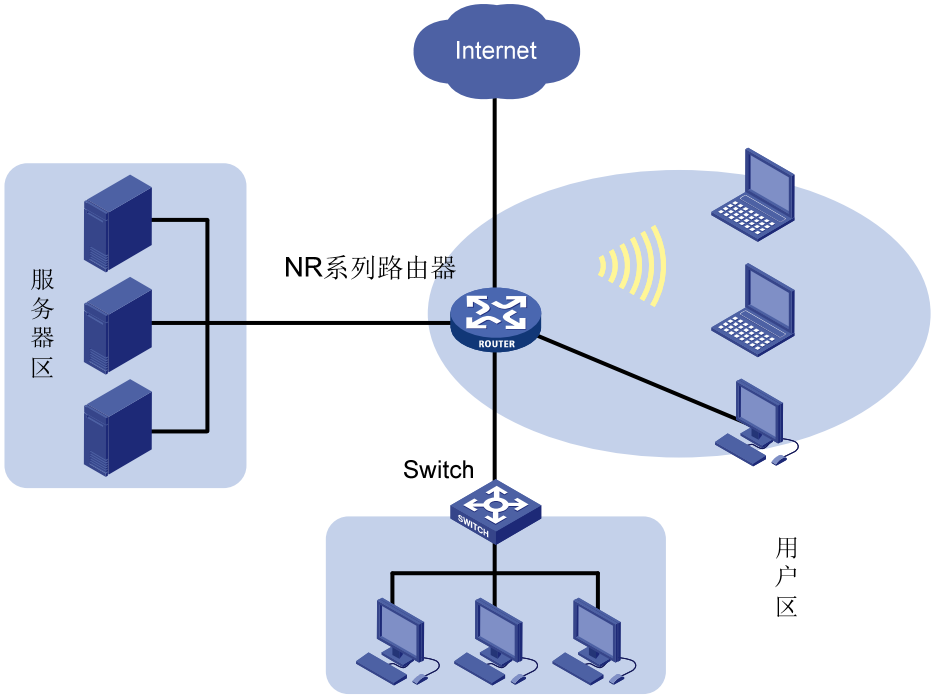
(2) 限制该区域内时间为工作日，即周一到周五、每天 8:00～18:00；

(3) 限制该区域内的用户以下具体的上网行为：

- 禁止工作日内使用同花顺软件，但是允许使用广发至强与国元证券软件、大智慧与分析家软件、光大证券软件；
- 禁止工作日内使用 QQ 软件；
- 工作日内允许 QQ 号码为 81293624、12936245、22936335 等用户上线；
- 禁止工作日内浏览淘宝（www.taobao.com）、新浪（www.sina.com）等网站地址；
- 禁止工作日内下载后缀名为 cfg 和 jpg 文件。

16.2.2 组网图

图16-2 组网示意图



16.2.3 配置步骤

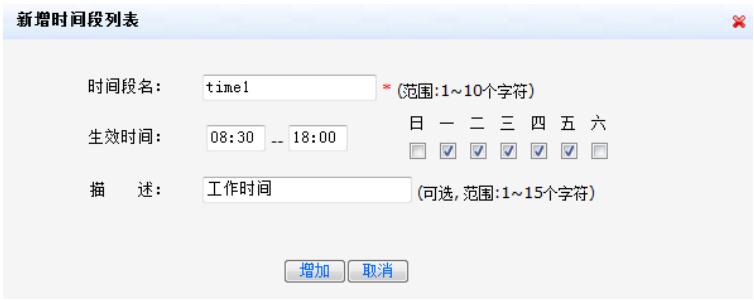
说明

此典型配置案例中所涉及的设置均在 NR-1200W 缺省配置的基础上进行。本案例为配置一条组网需求的行为策略规则，如果需要配置其他类型规则，通过编辑或者新增行为策略表项即可。

1. 在管理计算机的 Web 浏览器地址栏中输入 http://192.168.1.1，回车。输入用户名和密码（缺省均为 admin，区分大小写）。单击<登录>按钮后便可进入 Web 设置页面

2. 选择“上网管理→组管理→用户组管理”，单击<新增>按钮，在弹出的对话框中设置用户组列表，用户组名为 group1，在 IP 地址段输入 192.168.1.0 到 192.168.1.100，单击<添加>按钮，并添加相应的描述信息，单击<增加>按钮完成操作

3. 选择“上网管理→组管理→时间段管理”，单击<新增>按钮，在弹出的对话框中设置时间段列表，时间段名为 time1，设置生效时间为 08:30～18:00，勾选一、二、三、四、五，并添加相应的描述信息，单击<增加>按钮完成操作



4. 选择“上网管理→行为策略管理→行为策略管理”，单击<新增>按钮，在弹出的对话框中，勾选“启用该策略”，设置策略名称和策略描述信息；在适用用户组页签中，添加 group1 到“已添加用户组”中

5. 在适用时间段页签中，添加 time1 到“已添加时间段”中

6. 在应用软件页签中，选中“启用应用软件控制功能”复选框，并在金融软件列表中选中“禁止同花顺”复选框（如果您想限制其他金融软件，在需要禁止的软件前勾选即可）

7. 在 IM 软件页签中，选中“启用 IM 软件控制功能”复选框，并选中“禁止 QQ 上线”复选框（如果您仍允许访问 RTX 服务器，可以输入最多三个 RTX 服务器地址）

8. 在 QQ 特权号码页签中，选中“启用 QQ 特权号码”复选框，并设置 QQ 特权号码。在下面列表中，单击<新增>按钮，逐次添加 81293624、12936245、22936335 等您想要添加的特权 QQ 号码，并添加描述信息，单击<保存>按钮保存该列表

9. 在网站过滤页签中，选中“启用网站过滤功能”复选框和“仅禁止访问列表中的网站地址”，并设置访问列表中的网站地址。在下面的列表中，单击<新增>按钮，逐次添加模糊匹配的网站地址（taobao，sina 或者其他您想要添加的网址）以及添加描述信息，单击<保存>按钮保存该列表

10. 在文件类型过滤页签中，选中“启用文件类型过滤”复选框，单击<新增>按钮，在文件过滤列表中添加文件类型为 cfg、jpg 等您想要添加的文件后缀名，并添加相应的描述信息，单击<保存>按钮保存该列表

11. 最后单击<完成策略配置>按钮完成操作

17 附录 - 命令行设置

本章节主要包含以下内容：

您可以在局域网内通过 Telnet 本地登录路由器进行命令行设置。

请先确保管理计算机与路由器之间网络连通。然后在管理计算机上单击屏幕左下角<开始>按钮进入“开始”菜单。选择[运行]，在弹出的“运行”对话框中输入“telnet xxx.xxx.xxx.xxx”（xxx.xxx.xxx.xxx为路由器LAN口的IP地址）。回车后按界面提示输入用户名和密码（缺省情况下，两者均为admin）即可登录路由器进行设置，具体命令行介绍请参见“17.1 命令行在线帮助”。

路由器为您提供以下简单的命令行维护。

表17-1 命令行索引

命令行	请参见
ip address	17.2.1
restore default	17.2.2
reboot	17.2.3
display sysinfo	17.2.4
display device manuinfo	17.2.5
display version	17.2.6
admin acl info	17.2.7
admin acl default	17.2.8
ping	17.2.9

17.1 命令行在线帮助

(1) 在任一视图下，键入<?>获取该视图下所有的命令及其简单描述。

```
<H3C>?
    reboot          Reboot device
    restore         Restore configuration
    ip              Display the IP configuration
    display         Display current information
    ping            Ping function
    quit            Exit from the device
    admin           Admin the LAN interface
```

(2) 键入一命令，后接以空格分隔的“?”，如果该命令行位置有关键字，则列出全部关键字及其简单描述。

```
<H3C>ip ?
    address         Display IP addresses
```

(3) 键入一字符串，其后紧接<?>，列出以该字符串开头的所有命令。

```
<H3C>di?
    display
```

(4) 键入命令的某个关键字的前几个字母，按下<Tab>键，如果以输入字母开头的关键字唯一，则可以显示出完整的关键字。

```
<H3C>di  ←按下<Tab>键
<H3C>display
```

17.2 命令行操作

17.2.1 查看路由器LAN口的IP地址

输入 **ip address** 命令并回车，即可显示路由器 LAN 口的 IP 地址信息。

17.2.2 恢复路由器到出厂设置

输入 **restore default** 命令并回车，确认后，路由器将恢复到出厂设置并重新启动。

说明

恢复出厂设置后，路由器的用户名、密码以及IP地址等所有设置都会被恢复到缺省设置。路由器的缺省信息请参见“19 附录 - 缺省设置”。

17.2.3 重新启动路由器

输入 **reboot** 命令并回车，确认后，路由器将重新启动。

17.2.4 显示路由器系统资源使用情况

输入 **display sysinfo** 命令并回车，显示路由器的 CPU 和内存使用情况。

17.2.5 显示路由器硬件信息

输入 **display device manuinfo** 命令并回车，显示路由器基本的硬件信息，比如：设备型号、设备序列号、设备 MAC 地址等。

17.2.6 显示路由器软件/硬件版本信息

输入 **display version** 命令并回车。

17.2.7 显示局域网内允许访问路由器的用户IP地址信息

输入 **admin acl info** 命令并回车。

17.2.8 恢复局域网内允许所有用户访问路由器

输入 **admin acl default** 命令并回车。

17.2.9 网络连通性测试

输入 **ping** [**-a** *source-ip* | **-c** *count* | **-i** *interface-name* | **-s** *packet-size*] * *host*

表17-2 Ping 命令参数项描述

参数	描述
-a *source-ip*	指定ICMP回显请求（ECHO-REQUEST）报文的源IP地址。该地址必须是路由器接口的IP地址
-c *count*	指定ICMP回显请求报文的发送次数，取值范围为1～4294967295，缺省值为4
-i *interface-name*	指定发送ICMP回显请求报文的路由器接口名称。不指定该参数时，将根据目的IP查找路由表或者转发表来确定发送ICMP回显请求报文的接口
-s *packet-size*	指定发送的ICMP回显请求报文的长度（不包括IP和ICMP报文头），取值范围为20～8100，单位为字节，缺省值为56字节
host	目的端的IP地址或主机名，主机名为1～31个字符的字符串

18 附录 - 故障排除

本手册仅介绍简单的路由器故障处理方法，如仍不能排除，可通过 表 18-2 获取售后服务。

表18-1 故障排除

常见问题	故障排除
Power灯不亮	1. 请检查电源线是否连接正确 2. 请检查电源线插头是否插紧，无松动现象
端口指示灯不亮	1. 请检查网线与路由器的以太网端口是否卡紧，无松动现象 2. 将网线的两端分别插到路由器的两个以太网端口上，如果该两个端口对应的指示灯都亮，表示网线正常；否则该网线可能存在问题，请更换网线重新尝试
不能通过Web设置页面本地登录路由器	1. 使用 MS-DOS 方式的 **Ping** 命令检查网络连接 • Ping 127.0.0.1 用来检查管理计算机的 TCP/IP 协议是否安装 • Ping 路由器 LAN 口的 IP 地址来检查管理计算机与路由器是否连通 2. 通过 **ip address** 命令来查看当前路由器 LAN 口的地址，核对您输入的 IP 地址是否正确 3. 如果管理计算机使用静态 IP 地址，请确认其 IP 地址是否与路由器 LAN 口的 IP 地址处于同一网段 4. 路由器允许管理的用户数已经达到最大值（最多支持 5 个用户同时登录），请稍后再试 5. 请检查 Web 浏览器是否设置代理服务器或拨号连接，若有，请取消设置
局域网内用户出现掉线，无法访问因特网	1. 检查与路由器级连的交换机的网线和路由器 WAN 口的网线是否存在松动现象 2. 检查路由器是否已经对局域网内所有主机进行了 ARP绑定 3. 登录路由器的 Web 设置页面，选择“安全专区→防火墙→出站通信策略”，查看是否配置了某 IP 地址段在某段时间内无法访问因特网
局域网内用户出现玩游戏时比较卡（可能某些用户正在使用P2P软件下载）	1. 登录路由器的 Web 设置页面，选择“系统监控→流量监控→IP 流量”，单击列表上的标题栏利用排序功能找出当前占用带宽最大的主机，并对该主机进行限速设置 2. 检查路由器是否设置了 IP流量限制和 网络连接数限制
忘记设备Web管理登录密码	• 单击 Web 登录界面的“忘记密码？”链接进入页面后下载文件“XXXX_restore.txt”（点击右键，选择“目标另存为”保存该文件到本地，IE8及以下版本先直接点击文件，再点击右键保存文件，XXXX 为产品名称，比如 NR-1200W），将该文件放入 U 盘（FAT32 格式）根目录，将 U 盘插入 USB 接口，设备可恢复缺省登录密码。如果不能正常下载该文件，可手动创建同名文件，在文件第一行顶格输入 **restore password** 保存即可（注意：恢复缺省登录密码后会在 U 盘中将该文件删除） • 通过 Reset 键进行恢复（在设备通电情况下，用针状物按住 Reset 键 5 秒钟左右，直至诊断指示灯慢速闪烁，可恢复设备的缺省登录密码，连接到 Web 界面，输入缺省用户名和密码进行登录）

表18-2 获取售后服务

故障类型	描述	如何获取售后服务
硬件类故障	比如：出现设备不能正常通电、未插网线但以太网端口指示灯却常亮等问题	请联系当地授权服务中心予以确认后更换（各地区的H3C授权服务中心的联系方式可在H3C官方网站找到）
软件类问题	比如：出现设备功能不可用、异常等问题或配置咨询	请联系H3C技术支持服务热线：400－810－0504

19 附录 - 缺省设置

表 19-1 列出了路由器的一些重要的缺省设置信息，供您参考。

表19-1 路由器缺省设置

选项		缺省设置
接口管理	LAN口IP地址	IP地址：192.168.1.1 子网掩码：255.255.255.0
	LAN口基本属性	端口模式：Auto 广播风暴抑制：不抑制 流控：关闭
	多WAN工作模式	均衡模式
	连接因特网方式	DHCP自动获取方式
	WAN网口线路检测	关闭
	端口镜像	无
无线管理	内部网络SSID名称	H3C和H3C_5G
	访客网络SSID名称	H3C_GUEST和H3C_5G_GUEST
	SSID加密	不加密
	接入控制	关闭
	二层漫游	禁用
	禁止弱信号客户端接入	禁用
	广播探测	禁用
	AP管理设置	禁用
	AP配置模板	默认为当前无线配置
安全专区	ARP防护	采用路由器检测到ARP攻击时，LAN口或WAN口会主动发送免费ARP
	网站过滤	关闭
	防火墙	出站通信缺省策略：允许 入站通信缺省策略：禁止
	IDS防范	开启各攻击类型防护
	报文源认证	开启基于静态路由、静态ARP表、动态ARP表的报文源认证
	异常流量防护	开启，且防护等级为高

选项		缺省设置
QoS管理	IP流量限制	关闭
	绿色通道管理	关闭
	限制通道管理	关闭
	网络连接限数	关闭
高级设置	NAT	开启
	ALG应用	开启
	DDNS	关闭
	UPnP	关闭
设备管理	系统时间	通过缺省的NTP服务器获取
	远程管理	远程Web管理：关闭 远程Telnet管理：关闭
	用户管理	用户：admin 密码：admin
	超时时间	5分钟

20 附录 - 术语表

表20-1 术语表

术语缩写	英文全称	中文名称	含义
1000Base-T	1000Base-T	1000Base-T	1000Mbit/s基带以太网规范，使用两对5类双绞线连接，可提供最大1000Mbit/s的传输速率
100Base-TX	100Base-TX	100Base-TX	100Mbit/s基带以太网规范，使用两对5类双绞线连接，可提供最大100Mbit/s的传输速率
10Base-T	10Base-T	10Base-T	10Mbit/s基带以太网规范，使用两对双绞线（3/4/5类双绞线）连接，其中一对用于发送数据，另一对用于接收数据，提供最大10Mbit/s传输速率
DDNS	Dynamic Domain Name Service	动态域名服务	动态域名服务（Dynamic Domain Name Service），能实现固定域名到动态IP地址之间的解析
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议	动态主机配置协议（Dynamic Host Configuration Protocol）为网络中的主机动态分配IP地址、子网掩码、网关等信息
DHCP Server	Dynamic Host Configuration Protocol Server	DHCP 服务器	动态主机配置协议服务器（Dynamic Host Configuration Protocol Server）是一台运行了DHCP动态主机配置协议的设备，主要用于给DHCP客户端分配IP地址
DNS	Domain Name Service	域名服务	域名服务（Domain Name Service）将域名解析成IP地址。DNS信息按等级分布在整个因特网上的DNS服务器间，当我们访问一个网址时，DNS服务器查看发出请求的域名并搜寻它所对应的IP地址。如果该DNS服务器无法找到这个IP地址，就将请求传送给上级DNS服务器，继续搜寻IP地址。例如，www.yahoo.com 这个域名所对应的IP地址为 216.115.108.243
DoS	Denial of Service	拒绝服务	拒绝服务（Denial of Service）是一种利用合法的方式请求占用过多的服务资源，从而使其他用户无法得到服务响应的网络攻击行为
DSL	Digital Subscriber Line	数字用户线路	数字用户线（Digital Subscriber Line）这种技术使得数字数据和仿真语音信号都可以在现有的电话线路上进行传输。目前比较受家庭用户青睐的是ADSL接入方式
Firewall	Firewall	防火墙	防火墙（Firewall）技术保护您的计算机或局域网免受来自外网的恶意攻击或访问
FTP	File Transfer Protocol	文件传输协议	文件传输协议（File Transfer Protocol）是一种描述网络上的计算机之间如何传输文件的协议
HTTP	Hypertext Transfer Protocol	超文本传送协议	超文本传送协议（Hypertext Transfer Protocol）是一种主要用于传输网页的标准协议
Hub	Hub	集线器	共享式网络连接设备，工作在物理层，主要用于扩展局域网规模
ISP	Internet Service Provider	因特网服务提供商	因特网服务提供商（Internet Service Provider），提供因特网接入服务的提供商

术语缩写	英文全称	中文名称	含义
LAN	Local Area Network	局域网	局域网（Local Area Network）一般指内部网，例如家庭网络，中小型企业的内部网络等
MAC address	Media Access Control address	介质访问控制地址	介质访问控制地址（Media Access Control address），MAC地址是由厂商指定给设备的永久物理地址，它由6对十六进制数字所构成。例如：00-0F-E2-80-65-25。每一个网络设备都拥有一个全球唯一的MAC地址
NAT	Network Address Translation	网络地址转换	网络地址转换（Network Address Translation），可以把局域网内的多台计算机通过NAT转换后共享一个或多个公网IP地址，接入Internet，这种方式同时也可以屏蔽局域网用户，起到网络安全的作用。通常共享上网的宽带路由器都使用这个技术
NMS	Network Management Station	网络管理站	NMS运行SNMP客户端程序的工作站，能够提供非常友好的人机交互界面，方便网络管理员完成绝大多数的网络管理工作
Ping	Packet Internet Grope	因特网包探测器	Ping 命令是用来测试本机与网络上的其它计算机能否进行通信的诊断工具。Ping命令将报文发送给指定的计算机，如果该计算机收到报文则会返回响应报文
PPP	Point-to-Point Protocol	点对点协议	点对点协议（Point-to-Point Protocol）是一种链路层通信协议
PPPoE	PPP over Ethernet	点对点以太网承载协议	点对点以太网承载协议（PPP over Ethernet）在以太网上承载PPP协议封装的报文，它是目前使用较多的业务形式
QoS	Quality of Service	服务质量	服务质量（Quality of Service）是用来解决网络延迟和阻塞等问题的一种技术。当网络过载或拥塞时，QoS 能确保重要业务量不受延迟或丢弃，同时保证网络的高效运行
RJ-45	RJ-45	RJ-45	用于连接以太网交换机、集线器、路由器等设备的标准插头。直连网线和交叉网线通常使用这种接头
Route	Route	路由	基于数据的目的地址和当前的网络条件，通过有效的路由选择能够到达目的网络或地址的出接口或网关，进行数据转发。具有路由功能的设备称作路由器（router）
SNMP	Simple Network Management Protocol	简单网络管理协议	SNMP是网络中管理设备和被管理设备之间的通信规则，它定义了一系列消息、方法和语法，用于实现管理设备对被管理设备的访问和管理
TCP	Transfer Control Protocol	传输控制协议	传输控制协议（Transfer Control Protocol）是一种面向连接的、可靠的传输层协议
TCP/IP	Transmission Control Protocol/Internet Protocol	传输控制协议/网际协议	传输控制协议/网际协议（Transmission Control Protocol/Internet Protocol），网络通信的基本通信协议簇。TCP/IP定义了一组协议，不仅仅是TCP和IP
Telnet	Telnet	Telnet	一种用来访问远程主机的基于字符的交互程序。Telnet允许用户远程登录并对设备进行管理
UDP	User Datagram Protocol	用户数据报协议	用户数据报协议（User Datagram Protocol）是一种面向非连接的传输层协议

术语缩写	英文全称	中文名称	含义
UPnP	Universal Plug and Play	通用即插即用	通用即插即用（Universal Plug and Play），支持UPnP的设备彼此可自动连接和协同工作
WAN	Wide Area Network	广域网	广域网（Wide Area Network）是覆盖地理范围相对较广的数据通信网络，如因特网