



RV340W 管理指南

首次发布日期: 年 月 日

上次修改日期: 年 月 日

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

<http://www.cisco.com>

Tel: 408 526-4000

800 553-NETS (6387)

Fax: 408 527-0883

本手册中有关产品的规格和信息如有更改，恕不另行通知。本手册中的所有声明、信息和建议均准确可靠，但我们不为其提供任何明示或暗示的担保。用户必须承担使用产品的全部责任。

随附产品的软件许可和有限担保在随产品一起提供的信息包中提供，且构成本文的一部分。如果您无法找到软件许可或有限保证，请向您的思科代表索取。

以下是符合 FCC 规则的 A 类设备的相关信息：经测试，本设备符合 FCC 规则第 15 部分对 A 类数字设备的限制规定。这些限制旨在提供合理的保护，防止设备在商业环境中运行时产生有害干扰。本设备可以产生、利用并发射无线射频能量。如果不按说明手册中的要求安装和使用本设备，有可能对无线电通信产生有害干扰。在居民区运行此设备可能会造成有害干扰，在这种情况下，用户需要自费消除干扰。

以下是符合 FCC 规则的 B 类设备的相关信息：经测试，本设备符合 FCC 规则第 15 部分对 B 类数字设备的限制规定。设置这些限制的目的在于设备安装于居所时，提供合理保护以避免干扰。本设备可以产生、利用并发射无线射频能量。如果不按说明中的要求安装和使用本设备，有可能对无线电通信产生有害干扰。不过，我们不能保证在任何安装中都不会产生干扰。如果本设备确实对无线电或电视接收造成干扰（可以通过打开和关闭设备来确定），建议用户采取以下一种或多种措施来消除干扰：

- 重新调整接收天线的方向或位置。
- 增大设备和接收器之间的距离。
- 将设备和接收器连接到不同的电路插座上。
- 咨询经销商或有经验的无线电/电视技术人员，以寻求帮助。

在未经思科授权的情况下修改本产品，可能使 FCC 的批准失效，并失去运行本产品的许可。

TCP 报头压缩的思科设计是美国加州大学伯克利分校 (UCB) 所开发计划的修订版 - 作为 UNIX 操作系统的 UCB 公共领域版本。保留所有权利。版权所有 © 1981, Regents of the University of California。

即使有任何其他担保，这些供应商的所有文档文件和软件均“按原样”提供，包含其原有的所有瑕疵。思科和上面所提及的提供商拒绝所有明示或暗示担保，包括（但不限于）适销性、特定用途适用性和无侵权担保，或者因买卖或使用以及商业惯例所引发的担保。

在任何情况下，对于任何间接、特殊、连带发生或偶发的损坏，包括（但不限于）因使用或无法使用本手册而导致的任何利润损失或数据损失或损坏，思科及其供应商概不负责，即使思科及其供应商已获知此类损坏的可能性也不例外。

本档中使用的任何 Internet 协议 (IP) 地址和电话号码并非实际地址和电话号码。此档中的所有示例、命令显示输出、网络拓扑图和其它图形仅供说明之用。说明性内容中用到的任何真实 IP 地址或电话号码纯属巧合，并非有意使用。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标列表，请访问此网址：<http://www.cisco.com/go/trademarks>。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。(1110R)



目录

简介 1

使用入门 1

启动设置向导 3

故障排除提示 4

用户界面 4

状态和统计信息 7

系统摘要 7

TCP/IP 服务 9

端口流量 9

WAN QoS 统计信息 10

应用统计信息 11

已连接的设备 12

路由状态 12

DHCP 绑定 13

移动网络 13

VPN 状态 14

查看日志 16

管理 17

重启 17

文件管理 18

手动升级 19

自动更新 19

诊断 20

许可证 21

智能许可证使用 21

证书 21

导入证书 22

生成 CSR/证书	22
配置管理	23
系统配置	25
初始设置向导	26
系统	27
时间	27
日志	28
电子邮件服务器	30
远程系统日志服务器	30
电子邮件	30
用户帐户	31
远程验证服务	32
用户组	33
IP 地址组	34
SNMP	35
发现 Bonjour	36
LLDP	36
自动更新	37
服务管理	38
计划表	38
WAN	39
WAN 设置	39
多 WAN	42
移动网络	44
移动网络设置	44
带宽上限设置	45
动态 DNS	45
硬件 DMZ	46
IPv6 转换	46
IPv6 的 IPv4 封装隧道 (6in4)	47
IPv6 快速部署 (6rd)	47
QoS	49
流量类	49

WAN 队列	50
WAN 监管	51
WAN 带宽管理	51
交换机分类	52
交换机队列	53
LAN	55
端口设置	55
VLAN 设置	56
LAN/DHCP 设置	57
静态 DHCP	60
802.1X 配置	60
DNS 本地数据库	61
路由器通告	61
无线	63
基本设置	63
配置 2.4 GHz 无线电	66
配置 5 GHz 无线电	67
高级设置	68
Captive Portal	69
WPS	71
路由	73
IGMP 代理	73
RIP	74
静态路由	75
防火墙	77
基本设置	77
访问规则	78
网络地址转换	80
静态 NAT	80
端口转发	81
端口触发	82
会话超时	83
DMZ 主机	84

VPN	85
VPN 设置向导（站点到站点）	85
IPSec 配置文件	87
站点到站点	89
创建站点到站点 VPN 连接	90
创建安全 GRE 隧道	93
客户端到站点	95
远程工作人员 VPN 客户端	98
PPTP 服务器	100
L2TP 服务器	100
SSL VPN	101
VPN 通道	103
安全	105
应用控制向导	105
应用控制	106
Web 过滤	107
内容过滤	108
IP 源防护	108
快速索引	111
快速索引	111



第 1 章

简介

感谢您选择思科 RV340W 路由器。本指南介绍如何安装和管理路由器。本章包括的信息可以帮助您开始使用您的设备。思科 RV340W 自带默认设置，但互联网服务提供商 (ISP) 可能要求您修改设置。您可以使用 Internet Explorer（版本 10 和更高版本）、Firefox 或 Chrome（PC 版）或 Safari（Mac 版）等 Web 浏览器修改设置。

本节包含以下主题：

- [使用入门，第 1 页](#)
- [启动设置向导，第 3 页](#)
- [用户界面，第 4 页](#)

使用入门

此页面显示设备上最常见的配置任务。要启动路由器，请按照以下步骤操作：

-
- 步骤 1** 将 PC 连接到设备上带编号的 LAN 端口。如果将 PC 配置为 DHCP 客户端，则系统会将 192.168.1.x 范围内的 IP 地址分配到该 PC。
 - 步骤 2** 启动 Web 浏览器。
 - 步骤 3** 在地址栏中输入设备的默认 IP 地址，即 **192.168.1.1**。浏览器可能会发出警告，指出这是不受信任的网站。继续访问此网站。
 - 步骤 4** 在系统显示登录页面时，输入默认用户名 **cisco** 和默认密码 **cisco**（小写）。
 - 步骤 5** 单击**登录**。

注释 在系统启动的过程中，会有越来越多的电源 LED 持续闪烁，直至系统启动完成。启动时，PWR、LINK/ACT 和 LAN 1 的 GIGIBIT LED 将闪烁。启动到 25% 时，PWR、LINK/ACT 和 LAN 1 与 2 的 GIGIBIT LED 将闪烁。启动到 50% 时，PWR、LINK/ACT 和 LAN 1、2 与 3 的 GIGIBIT LED 将闪烁。启动到 75% 时，PWR、LINK/ACT 和 LAN 1、2、3 与 4 的 GIGIBIT LED 将闪烁。

系统启动时间通常不到 3 分钟。如果路由器完全配置，且所有功能均配置为最高设置，可能需要 7 分钟才能完成系统启动。

表 1: 路由器的 LED 细节

PWR（电源）	<p>熄灭表示设备电源关闭。</p> <p>绿色常亮表示设备电源开启且设备已启动。</p> <p>绿色闪烁表示设备正在启动。</p>
DIAG（诊断）	<p>熄灭表示系统正在启动。</p> <p>红色慢闪 (1Hz) 表示系统正在进行固件升级。</p> <p>红色快闪 (3Hz) 表示系统固件升级失败。</p> <p>红色常亮表示系统在使用活动映像和非活动映像时或在救援模式下启动失败。</p>
LINK/ACT（链路/活动）（WAN1、WAN2 和 LAN1-4）	<p>熄灭表示端口未建立以太网连接。</p> <p>绿色常亮表示端口已建立千兆以太网链路。</p> <p>绿色闪烁表示端口的千兆以太网链路正在发送或接收数据。</p>
GIGABIT（千兆）（WAN1、WAN2 和 LAN1-4）	<p>绿色常亮表示数据传输速度为 1000M。</p> <p>熄灭表示数据传输速度不是 1000M。</p>
DMZ（隔离区）	<p>绿色常亮表示已启用 DMZ。</p> <p>熄灭表示已禁用 DMZ</p>
VPN（虚拟专用网络）	<p>熄灭表示设备没有定义 VPN 隧道，或者所有定义的 VPN 隧道都被禁用。</p> <p>绿色常亮表示至少有一条 VPN 隧道处于活动状态。</p> <p>绿色闪烁表示正在通过 VPN 隧道发送和接收数据。</p> <p>琥珀色常亮表示已启用的 VPN 隧道处于非活动状态。</p>

USB 1 和 USB 2	<p>熄灭表示端口未连接 USB 设备或无法识别已插入的 USB 设备。</p> <p>USB 装置成功连接到 Internet 服务提供商 (ISP) (已分配 IP 地址), 以及 USB 存储装置已被识别时, 指示灯呈绿色常亮状态。</p> <p>绿色闪烁表示端口正在发送和接收数据。</p> <p>琥珀色常亮表示 USB 装置已被识别, 但未能连接至 ISP (未分配 IP 地址)。USB 存储装置访问出现错误。</p>
Reset (重置)	<p>要重新启动路由器, 请使用曲别针或笔尖按住 Reset (重置) 按钮不超过 10 秒。</p> <p>要将路由器重置为出厂默认设置, 请按住 Reset (重置) 按钮 10 秒。</p>
Wireless (无线)	<p>LED 亮起表示已启用内部接入点。</p> <p>LED 熄灭表示已禁用内部接入点。</p>

启动设置向导

“启动设置向导”页面中的说明可以指引您完成设备配置过程。

要打开此页面, 请在导航树中选择“启动设置向导”, 然后按照屏幕上的说明继续操作。有关设置互联网连接所需的信息, 请咨询 ISP。

启动设置向导

初始设置向导	将您定向至初始设置向导。
VPN 设置向导	将您定向至 VPN 状态向导。
应用控制向导	将您定向至应用控制向导。

初始配置

更改管理员密码	将您定向至用户帐户页面, 您可以在其中更改管理员密码和设置访客帐户。
配置 WAN 设置	将您定向至 WAN 设置页面, 您可以在其中修改 WAN 参数。
配置 USB 设置	将您定向至移动网络页面, 您可以在其中修改 USB 配置。
配置 LAN 设置	将您定向至 VLAN 成员关系页面, 您可以在其中配置 VLAN。

快速访问

升级路由器固件	将您定向至 文件管理 页面，您可以在其中更新设备固件。
配置远程管理访问权限	将您定向至 防火墙>基本设置 页面，您可以在其中启用设备的基本功能。
备份设备配置	将您定向至 配置管理 页面，您可以在其中管理路由器配置。

设备状态

系统摘要	将您定向至 系统摘要 页面，其中显示设备的 IPv4 和 IPv6 配置以及防火墙状态。
VPN 状态	将您定向至 VPN 状态 页面，其中显示此设备管理的 VPN 的状态。
端口统计信息	将您定向至 端口流量 页面，其中显示设备的端口状态和端口流量。
流量统计信息	将您定向至 TCP/IP 服务 页面，其中显示设备的端口监听状态和已建立的连接的状态。
查看系统日志	将您定向至 查看日志 页面，其中显示设备的日志。

故障排除提示

如果连接到互联网或基于 Web 的 Web 界面时出现问题，请执行以下操作：

- 确保 Web 浏览器未设置为脱机工作。
- 检查以太网适配器的局域网连接设置。PC 应该通过 DHCP 获得 IP 地址。或者，也可以为 PC 指定 192.168.1.x 范围内的静态 IP 地址，并将默认网关设置为 192.168.1.1（设备的默认 IP 地址）。
- 确保在向导中输入正确设置互联网连接所需的设置。
- 通过关闭调制解调器和设备的电源，重置这两个设备。接下来，接通调制解调器的电源，使其闲置约 2 分钟。然后，接通设备的电源。现在，您应该能够接收 WAN IP 地址。
- 如果您有 DSL 调制解调器，请要求 ISP 将 DSL 调制解调器设置为网桥模式。

用户界面

用户界面旨在便于您设置和管理设备。

导航

Web 界面的主要模块以左侧导航窗格中的按钮形式表示。单击按钮可查看更多选项。单击选项可打开页面。

弹出窗口

单击某些链接和按钮会启动弹出窗口，这些窗口会显示详细信息或相关配置页面。如果 Web 浏览器显示关于弹出窗口的警告消息，请允许显示被阻止的内容。

帮助

要查看有关所选配置页面的信息，请单击 Web 界面右上角的**帮助**。如果 Web 浏览器显示关于弹出窗口的警告消息，请允许显示被阻止的内容。

退出

要退出 Web 界面，请单击 Web 界面右上角附近的**退出**。系统将显示**登录**页面。



第 2 章

状态和统计信息

本节提供有关设备的各种配置设置的信息，包含以下主题：

- [系统摘要](#)，第 7 页
- [TCP/IP 服务](#)，第 9 页
- [端口流量](#)，第 9 页
- [WAN QoS 统计信息](#)，第 10 页
- [应用统计信息](#)，第 11 页
- [已连接的设备](#)，第 12 页
- [路由状态](#)，第 12 页
- [DHCP 绑定](#)，第 13 页
- [移动网络](#)，第 13 页
- [VPN 状态](#)，第 14 页
- [查看日志](#)，第 16 页

系统摘要

“系统摘要”提供设备上设置的快照视图。它显示设备的固件、序列号、端口流量、路由状态、移动网络，以及 VPN 服务器设置。要查看此系统摘要，请单击[状态和统计信息 > 系统摘要](#)。

系统信息

- **主机名** — 主机的名称。
- **序列号** — 设备的序列号。
- **系统运行时间** — 设备处于活动状态的时间，以年-月-日、小时数和分钟数表示。
- **当前时间** — 当前的日期和时间。

- **PID VID** — 硬件的版本号。

固件信息

- **固件版本** — 所安装固件的版本号。
- **固件 MD5 校验和** — 用于文件验证的值。

端口状态

- **端口 ID** — 定义的端口名称和编号。
- **接口** — 用于连接的端口的名称。
- **已启用** — 端口的状态。
- **速度** — 自动协商后设备的速度（以 Mbps 为单位）。

IPv4 和 IPv6

- **接口** — 接口的名称。
- **IP 地址** — 分配给接口的 IP 地址。
- **默认网关** — 接口的默认网关。
- **DNS** — DNS 服务器的 IP 地址。
- **动态 DNS** — 接口 DDNS（动态 DNS）的 IP 地址：“已启用”或“已禁用”。
- **更新** — 单击可更新 IP 地址。
- **释放** — 单击可释放接口。

VPN 状态

- **类型** — VPN 隧道的类型。
- **活动** — 已启用或已禁用。
- **已配置** — VPN 隧道的状态（是否已配置）。
- **最大支持会话数** — 设备上支持的隧道的最大数量。
- **已连接会话** — 隧道的状态。

防火墙设置状态

- **状态数据包检测 (SPI)** — 又称为动态数据包过滤，能够监控活动连接的状态，并使用这些信息确定哪些网络数据包可通过防火墙。
- **拒绝服务 (Dos)** — Dos 过滤器服务的状态为已启用（打开）或已禁用（关闭）。DoS 攻击是指企图使目标用户无法使用机器或网络资源。

- **阻止 WAN 请求** — 通过向互联网设备隐藏网络端口并阻止其他互联网用户检测网络，使得外部用户难以顺利进入网络。
- **远程管理** — 表示是否允许通过远程连接管理设备。
- **访问规则** — 已设置的访问规则的数量。

日志设置状态

- **系统日志服务器** — 系统日志的状态。
- **电子邮件日志** — 要使用电子邮件发送的日志的状态。

TCP/IP 服务

“TCP/IP 服务”页面显示协议、端口和 IP 地址的统计信息。要查看 TCP/IP 服务，请单击**状态和统计信息 > TCP/IP 服务**。

端口监听状态

- **协议** — 用于通信的协议的类型。
- **监听 IP 地址** — 设备上的监听 IP 地址。
- **监听端口** — 设备上的监听端口。

已建立的连接的状态

- **协议** — 用于通信的协议的类型。
- **本地 IP 地址** — 系统的 IP 地址。
- **本地端口** — 不同服务的监听端口。
- **外部地址** — 已连接的设备的 IP 地址。
- **外部端口** — 已连接的设备的端口。
- **状态** — 会话的连接状态。

端口流量

“端口流量”页面显示设备接口的统计信息和状态。要查看设备的“端口流量”页面，请单击**状态和统计信息 > 端口流量**。

端口流量

- **端口 ID** — 定义的端口名称和编号。

- **链路状态** — 接口的状态。
- **接收的数据包** — 端口上接收的数据包数量。
- **接收的字节** — 接收的数据包数量（以字节为单位）。
- **发送的数据包** — 端口上发送的数据包数量。
- **发送的字节** — 发送的数据包数量（以字节为单位）。
- **数据包错误** — 有关错误数据包的详细信息。
- **刷新** — 刷新显示的统计信息。
- **重置计数器** — 将所有值重置为零。

端口状态

- **端口 ID** — 定义的端口名称和编号。
- **链路状态** — 接口的状态。
- **端口活动** — 端口的状态（例如：端口已启用、已禁用或已连接）。
- **速度状态** — 自动协商后设备的速度（以 Mbps 为单位）。
- **双工状态** — 双工模式：“半双工”或“全双工”。
- **自动协商** — 自动协商参数的状态。启用自动协商后，即自动协商参数的状态为打开时，它会检测双工模式。如果连接需要交叉，它会自动选择 MDI（介质相关接口）或 MDIX（具有正反转线自适应功能的介质相关接口）配置，以与链路另一端相匹配。

WAN QoS 统计信息

“WAN QoS 统计信息”页面显示出站和入站 WAN QoS 的统计信息。要查看设备的“WAN QoS 统计信息”页面，请单击**状态和统计信息 > WAN QoS 统计信息**。

- **接口** — 接口的名称。
- **策略名称** — 策略的名称。
- **说明** — WAN QoS 统计信息的说明。
- **清除计数器** — 单击可清除计数器。

出站 QoS 统计信息

- **队列** — 出站队列的数量。
- **流量类** — 分配给队列的流量类的名称。
- **已发送的数据包** — 已发送的流量类的出站数据包的数量。
- **已丢弃的数据包** — 已丢弃的出站数据包的数量。

进站 QoS 统计信息

- 队列 — 进站队列的数量。
- 流量类 — 分配给队列的流量类的名称。
- 已发送的数据包 — 已发送的流量类的进站数据包的数量。
- 已丢弃的数据包 — 已丢弃的进站数据包的数量。

应用统计信息

“应用统计信息”显示路由器的使用情况数据。要查看“应用统计信息”页面，请单击**状态和统计信息 > 应用统计信息**。

- 清除计数器 — 重置表中的所有统计信息。

最大流量生成应用（按类别）

- 类别 — 访问过的应用类别的列表。
- 流量 — 流量（以兆字节为单位）。

最大流量生成应用（按名称）

- 应用 — 访问过的应用的列表。
- 流量 — 流量（以兆字节为单位）。

最大流量生成者

- 流量生成者 — 访问过的 IP 地址的列表。
- 流量 — 流量（以兆字节为单位）。

最大流量生成者（按设备类型）

- 设备 — 访问过的设备的列表。
- 流量 — 流量（以兆字节为单位）。

最大流量生成者（按操作系统类型）

- 操作系统 — 使用过的操作系统的列表。
- 流量 — 流量（以兆字节为单位）。



注释

如果 AVC 被禁用或许可过期，系统可能会弹出一个窗口，说明 AVC 被禁用或许可过期。

已连接的设备

“已连接的设备”页面列出路由器上连接的所有设备。要查看此“已连接的设备”页面，请单击状态和统计信息 > 已连接设备。

IPv4

- **主机名** — 连接的设备的名称。
- **IPv4 地址** — 连接的设备的 IP 地址。
- **MAC 地址** — 连接的设备的 MAC 地址。
- **类型** — 设备 IP 地址的类型。
- **接口** — 连接设备的接口。

IPv6

- **IPv6 地址** — 连接的设备的 IPv6 地址。
- **MAC 地址** — 连接的设备的 MAC 地址。

路由状态

路由是在网络中将数据包从一台主机移动至另一台主机的过程。此过程的路由状态显示在路由表中。路由表包含有关其直接关联网络的拓扑的信息。要查看设备的 IPv4 和 IPv6 路由状态，请单击状态和统计信息 > 路由状态。

IPv4 和 IPv6 路由

- **目标** — 连接的 IP 地址和子网掩码。
- **下一步跳** — 下一步跳的 IP 地址。数据包经过的步跳的最大数量（最多为 15 步跳）。
- **度量标准** — 确定发送网络流量的最佳路由时使用的路由算法数量。
- **接口** — 路由连接的接口的名称。
- **源** — 路由的源。

DHCP 绑定

“DHCP 绑定”页面显示 IP 地址、MAC 地址、租用到期时间和绑定类型（静态或动态）等 DHCP 客户端信息的统计信息。要查看设备的“DHCP 绑定”页面，请单击[状态和统计信息 > DHCP 绑定](#)。

“DHCP 绑定表”显示以下内容：

- **IPv4 地址** — 分配的 IP 地址。
- **MAC 地址** — 客户端分配的 IP 地址的 MAC 地址。
- **租用到期** — 客户端系统的租用时间。
- **类型** — 连接状态（静态或动态）。

移动网络

移动网络可让路由器及其子网具备移动性，同时继续保持 IP 连接对通过该移动路由器连接到网络的 IP 主机的透明度。要查看路由器的移动网络，请单击[状态和统计信息 > 移动网络](#)。接下来，从下拉列表中选择接口（**USB1** 或 **USB2**）。单击**刷新**可刷新移动网络状态。

连接

- **互联网 IP 地址** — 服务提供商提供的 IP 地址。
- **子网掩码** — 服务提供商提供的掩码。
- **默认网关** — 服务提供商提供的默认网关。
- **连接运行时间** — 连接设备的持续时间。
- **当前拨号会话数据流量使用情况** — 每个会话的数据流量使用情况。
- **月度数据流量使用情况** — 月度数据流量使用情况。

数据卡状态

- **制造商** — 设备的制造商。
- **卡固件** — 制造商提供的固件版本。
- **SIM 状态** — SIM 的状态。
- **IMSI** — 设备的唯一编号。
- **运营商** — 数据网络运营商的名称或类型。
- **服务类型** — 数据服务类型。
- **信号强度** — 数据信号的强度。
- **卡状态** — 卡状态（“断开连接”或“已连接”）。

VPN 状态

“VPN 状态”显示站点到站点、客户端到站点、SSL VPN、PPTP、L2TP 和远程工作人员 VPN 客户端的隧道状态。要查看设备的 VPN 状态，请单击[状态和统计信息 > VPN 状态](#)。

站点到站点隧道状态

- **已使用的隧道** — 正在使用的 VPN 隧道。
- **可用隧道** — 可用的 VPN 隧道。
- **已启用的隧道** — 已启用的 VPN 隧道。
- **已定义的隧道** — 定义的 VPN 隧道。

在连接表中，您可以添加、编辑、删除或刷新隧道。（请参阅[站点到站点](#)，第 89 页）。您还可以单击**列显示选择**，以选择在连接表中显示的列标题。

客户端到站点隧道状态

在此模式下，互联网中的客户端连接到服务器，以访问服务器后的企业网络/LAN。为确保安全连接，您可以实施客户端到站点 VPN。您可以查看所有的客户端到隧道连接，并在连接表中添加、编辑或删除连接。（请参阅[客户端到站点](#)，第 95 页）。

连接表显示以下信息：

- **组或隧道名称** — VPN 隧道的名称。此名称仅供参考，不一定与隧道另一端使用的名称相匹配。
- **连接** — 连接的状态。
- **第 2 阶段加密/验证/组** — 第 2 阶段加密类型 (NULL/DES/3DES/AES-128/AES-192/AES-256)、验证方法 (NULL/MD5/SHA1) 和 DH 组号 (1/2/5)。
- **本地组** — 本地组的 IP 地址和子网掩码。

SSL VPN 状态

通过安全套接字层虚拟专用网络 (SSLVPN)，用户可以使用 Web 浏览器建立通向此设备的安全远程访问 VPN 隧道。使用 SSL VPN 可以从互联网上的几乎所有计算机安全、轻松地访问各类 Web 资源和支持 Web 的应用。您可以在此处查看 SSL VPN 隧道的状态。

- **已使用的隧道** — 用于连接的 SSL VPN 隧道。
- **可用隧道** — 可用于 SSL VPN 连接的隧道。

连接表显示已建立的隧道的状态。您还可以添加、编辑或删除连接。

- **策略名称** — 在隧道上应用的策略的名称。
- **会话** — 会话的数量。

您还可以添加、编辑或删除 SSL VPN。（请参阅[SSL VPN](#)，第 101 页）。

PPTP 隧道状态

点对点隧道协议可使用 128 位密钥加密数据。它用于确保将消息从一个 VPN 节点安全地发送到另一个节点。

- **已使用的隧道** — 用于 VPN 连接的 PPTP 隧道。
- **可用隧道** — 可用于 PPTP 连接的隧道。

连接表 — 显示已建立的隧道的状态。您还可以建立或断开以上连接。

- **会话 ID** — 建议的连接或当前连接的会话 ID。
- **用户名** — 已连接的用户名称。
- **远程访问** — 远程连接或建议连接的 IP 地址。
- **隧道 IP** — 隧道的 IP 地址。
- **连接时间** — 隧道连接的时间。
- **操作** — 连接隧道或断开隧道连接。

L2TP 隧道状态

第 2 层隧道协议是一种通过在第 2 层上使用互联网来启用点对点会话的方法。您可以查看 L2TP 隧道状态的状态。

- **已使用的隧道** — 用于 VPN 连接的 L2TP 隧道。
- **可用隧道** — 可用于 L2TP 连接的隧道。

连接表 — 显示已建立的隧道的状态。您还可以建立或断开以上连接。

- **会话 ID** — 建议的连接或当前连接的会话 ID。
- **用户名** — 已连接的用户名称。
- **远程访问** — 远程连接或建议连接的 IP 地址。
- **隧道 IP** — 隧道的 IP 地址。
- **连接时间** — 隧道连接的时间。
- **操作** — 连接隧道或断开隧道连接。

查看日志

“查看日志”页面显示设备的所有日志。您可以根据类别、严重程度或关键字过滤这些日志。您还可以刷新、清除这些日志，并将这些日志导出到 PC 或 USB 中。要查看设备日志，请按照以下步骤操作：

步骤 1 依次单击状态和统计信息 > 查看日志。

步骤 2 在“日志过滤条件”下选择相应的选项。

类别	单击以下任意选项即可查看日志： <ul style="list-style-type: none"> • 全部 — 显示所有日志。 • 类别 — 显示所选类别的日志。
严重程度	选择显示的某个选项，以查看根据严重程度显示的日志。
关键字	输入关键字，使系统根据关键字显示日志。

步骤 3 单击显示日志。

注释 要配置日志设置，请参阅[日志，第 28 页](#)。

步骤 4 单击以下任意选项：

- **刷新** — 单击可刷新日志。
- **清除日志** — 单击可清除日志。
- **日志导出到 PC** — 单击可将日志导出到 PC。
- **日志导出到 USB** — 单击可将日志导出到 USB 存储设备。



第 3 章

管理

本节介绍设备的管理功能，其中包含以下主题：

- [重启](#)，第 17 页
- [文件管理](#)，第 18 页
- [诊断](#)，第 20 页
- [许可证](#)，第 21 页
- [证书](#)，第 21 页
- [配置管理](#)，第 23 页

重启

借助重启功能，用户可使用活动映像或非活动映像重新启动设备。

要访问“重启”页面，请按照以下步骤操作：

-
- 步骤 1** 单击**管理 > 重启**。
 - 步骤 2** 在“重启后的活动映像”部分，从下拉列表中选择一个选项（**活动映像 x.x.xx.xx** 或**非活动映像 x.x.xx.xx**）
 - 步骤 3** 选择**首选重启选项**。
 - 重新启动设备。
 - 重启后还原为出厂默认设置。
 - 重启后还原为出厂默认设置（包括证书）。
 - 步骤 4** 单击**重启**以重新启动设备。
-

文件管理

“文件管理”提供设备的快照视图。要查看“文件管理”信息，请按照以下步骤操作：

步骤 1 单击**管理 > 文件管理**以查看以下信息：
系统信息

- **设备型号** — 设备的型号。
- **PID VID** — 路由器的 PID 和 VID 号。
- **当前固件版本** — 当前固件版本。
- **最近更新** — 最近一次固件更新的日期。
- **Cisco.com 上可用的最新版本** — 最新固件版本。
- **最近检查** — 最近一次检查的日期。

签名

- **当前签名版本** — 签名的版本。
- **最近更新** — 执行最近一次更新的日期。
- **Cisco.com 上可用的最新版本** — 最新签名版本。
- **最近检查** — 最近一次检查的日期。

USB 装置驱动程序

- **当前装置驱动程序版本** — 内置 USB 装置驱动程序的版本。
- **最近更新** — 执行最近一次更新的日期。
- **Cisco.com 上可用的最新版本** — 最新装置驱动程序版本。
- **最近检查** — 最近一次检查的日期。

语言包

- **当前语言包版本** — 语言包的版本。
- **最近更新** — 最近一次更新的日期。
- **Cisco.com 上可用的最新版本** — 最新语言包版本。
- **最近检查** — 最近一次检查的日期。

手动升级

在“手动升级”部分，可以将固件、签名文件、USB 装置驱动程序或语言文件上传和升级至更新版本。

注意 在固件升级过程中，请勿在操作完成之前尝试上线、关闭设备、关闭 PC 或以任何方式中断过程。此过程大约需要一分钟（包括重新启动过程）。在正向闪存写入的特定时间点中断升级过程可能会损坏闪存并使路由器无法使用。

步骤 2 如果选择从 USB 驱动器升级，路由器将搜索 USB 闪存驱动器以查找固件映像文件，这类文件的名称包含以下一项或多项内容：PID、MAC 地址和序列号。如果 USB 闪存驱动器中有多个固件文件，路由器将选择名称中包含最具体信息的文件，即根据具体程度，优先级从高到低。

手动升级

使用较新版本的固件更新路由器的步骤。

步骤 1 选择**管理 > 文件管理**。

步骤 2 在“手动升级”部分，选择文件类型（**固件映像、签名文件、USB 装置驱动程序或语言文件**）。

步骤 3 在“升级方式”部分，选择一个选项（**Cisco.com、PC 或 USB**）并单击**刷新**。

步骤 4 选中**将所有配置/设置重置为出厂默认设置**可重置所有配置并应用出厂默认设置。

步骤 5 单击**升级**可将选中的映像上传至设备。

自动更新

如果在系统启动期间使用了 U 盘，路由器将支持从 USB 闪存驱动器中加载固件。路由器将搜索 USB 闪存驱动器，查找名称中包含以下一种或多种信息的固件映像文件：PID、MAC 地址和序列号。如果 USB 闪存驱动器中有多个固件文件，路由器将选择名称中包含最具体信息的文件，即根据具体程度，优先级从高到低。

- PID-MAC-SN.IMG
- PID-SN.IMG
- PID-MAC.IMG
- PID.IMG

使用其他名称的文件将被忽略。如果固件映像版本高于固件当前版本，固件将升级至此映像，DUT 将会重启。然后，升级过程将重新开始。

如果路由器未在 USB1 中找到更新的映像，那么它将会使用同一逻辑查看 USB2。

路由器还支持在系统启动期间，从 USB 闪存驱动器中加载配置文件。

- 这种行为仅在路由器处于出厂默认设置状态，且在接通电源前连接了 USB 闪存驱动器时出现。

- 路由器将搜索 USB 闪存驱动器，查找名称中包含以下一种或多种信息的配置文件：PID、MAC 地址和序列号。如果 USB 闪存驱动器中有多个固件文件，路由器将选择名称中包含最具体信息的文件，即根据具体程度，优先级从高到低。

PID-MAC-SN.xml

PID-SN.xml

PID-MAC.xml

PID.xml

使用其他名称的文件将被忽略。

自动固件回退机制

路由器在闪存中包含两份固件文件并提供自动回退机制。当将要启动的固件有损坏或启动五次失败后，设备可以自动切换到备份的固件来启动。

自动回退机制的工作流程如下：

- 1 路由器首先尝试用当前的固件启动
- 2 如果当前的固件有损坏，自动启动五次均失败后会切换到备份固件启动。如果路由器卡在启动过程中，不能自动重启，可以手动断电再上电，等上电30秒后再次断电，这样操作5次后设备也会切到备份的固件。
- 3 当设备用备份的固件启动后，请检查原来的主固件是否有问题。
- 4 如果确认主固件有问题，请重新上传主固件。

诊断

设备提供了几个诊断工具来帮助对网络问题进行故障排除。使用下列诊断工具监视网络的整体状况。

使用 Ping 或 Trace

可以使用 Ping 或 Trace 实用程序测试此路由器与网络中其他设备之间的连接。要使用 Ping 或 Trace，请按照以下步骤操作：

-
- 步骤 1 选择**管理 > 诊断**。
 - 步骤 2 在“Ping 或 Trace 一个 IP 地址”部分的“IP 地址/域名”字段中输入 IP 地址或域名。
 - 步骤 3 单击 **Ping**。系统将显示 Ping 结果。这些结果可说明设备是否可访问。或单击**跟踪路由**。系统将显示追踪路由结果。
 - 步骤 4 要执行 DNS 查找，请在“执行 DNS 查找”>“IP 地址/域名”字段中输入 IP 地址或域名，并单击**查找**。
-

许可证

在“许可证”部分，您可以配置许可证或注册路由器。它可以简化思科软件体验，并帮助您了解思科软件的使用方式。

智能软件许可状态

“智能软件许可状态”部分显示设备的许可证信息。

注册状态 — “已注册”或“未注册”，以及注册日期。

许可证授权状态 — “已授权”、“评估模式”、“不合规”、“授权已到期”或“评估期已到期”，以及许可证授权日期。

受控导出功能 — 默认情况下不允许。

智能许可证使用

您可以选择要用于路由器的智能许可证。请确保您的路由器虚拟帐户中有足够的许可证，否则会产生不合规问题。

要配置智能许可证，请按照以下步骤操作：

-
- 步骤 1** 在“智能许可证使用”下，单击**选择许可证**。
 - 步骤 2** 选中适用的许可证并在**帐户**下输入许可证号。
 - 步骤 3** 单击**保存**。
 - 步骤 4** 此时会显示“许可证授权更新”弹出窗口，单击**确定**。
-

证书

证书在通信过程中具有重要作用。由受信任的证书颁发机构(CA)签名的证书可以确保证书持有者的真实身份。如果数据没有受信任的签名证书，则可能会被加密，但是与您通信的对方可能并非您预期的通信对象。

此页显示证书列表及证书详细信息。您可以导出自签名证书、本地证书和 CSR 证书，也可以导入 CA 证书、本地证书或 PKCS#12 证书。您还可以将 PC/USB 中的证书文件导入新证书。

如果导入了设备证书，它将会取代对应的 CSR 证书。

“证书表”中显示与路由器相关联的证书。对于“证书表”中所列的证书，您可以执行删除、导出、查看详细信息或证书导入操作。

导入证书

要导入证书，请按照以下步骤操作：

-
- 步骤 1** 单击**导入证书**。
- 步骤 2** 从下拉列表中选择要导入的证书类型：
- 本地证书
 - CA 证书
 - PKCS#12 编码文件。
- 步骤 3** 输入证书名称。（对于 PKCS#12，必须输入密码。）
- 步骤 4** 选中从 **PC 导入**，单击**选择文件**以从特定位置上传并导入证书。
- 步骤 5** 选中从 **USB 导入**，单击**刷新**以从 USB Key 上传并导入证书。
- 步骤 6** 单击**上传**。
-

生成 CSR/证书

-
- 步骤 1** 单击**生成 CSR/证书**。
- 步骤 2** 从下拉列表中选择要生成的证书类型。
- 步骤 3** 输入以下信息：

证书名称	输入证书名称。证书名称不能包含空格或特殊字符。
主题备选名称	输入名称，并选择以下选项之一： IP 地址 、 FQDN 或 电子邮件 。
国家/地区名称	从下拉列表中选择国家/地区。
省/直辖市/自治区名称	输入省/直辖市/自治区。
地区名称	输入地区名称。
组织名称	输入组织名称。
组织单元名称	输入组织单元名称。
通用名称	输入通用名称。
电子邮件地址	输入电子邮件地址。

密钥加密长度	从下拉菜单中选择密钥加密长度。应为 512 或 2048。
有效期	输入天数（范围 1-10950 ，默认值： 360 ）。

步骤 4 单击生成。

配置管理

“配置管理”页面提供路由器文件配置详细信息。

配置文件名称

“配置文件名称”显示以下内容的最后更改时间详细信息：

- 运行配置
- 启动配置
- 镜像配置
- 备份配置

复制/应用配置

“复制/应用配置”部分显示使用运行配置文件的设备的默认配置，该文件并不稳定，且重启后不会保留设置。您可以将此运行配置文件保存到启动配置文件。

- 源文件名 — 从下拉列表中选择源文件名。
- 目标文件名 — 从下拉列表中选择目标文件名。
- 保存图标闪烁 — 表明在有未保存的数据时，图标是否会闪烁。要禁用/启用该功能，可单击禁用保存图标闪烁。



第 4 章

系统配置

系统配置向导可在安装和配置路由器时提供指导。本节包含以下主题：

- [初始设置向导，第 26 页](#)
- [系统，第 27 页](#)
- [时间，第 27 页](#)
- [日志，第 28 页](#)
- [电子邮件，第 30 页](#)
- [用户帐户，第 31 页](#)
- [用户组，第 33 页](#)
- [IP 地址组，第 34 页](#)
- [SNMP，第 35 页](#)
- [发现 Bonjour，第 36 页](#)
- [LLDP，第 36 页](#)
- [自动更新，第 37 页](#)
- [服务管理，第 38 页](#)
- [计划表，第 38 页](#)

初始设置向导

在“初始设置向导”页面中，您可以检查连接并配置基本路由器设置。运行设置向导页面中的说明可以指引您完成设备配置过程。

步骤 1 单击系统配置 > 初始设置向导。

步骤 2 单击下一步进入“检查连接”页面。如果路由器检测到连接，此页面将显示连接详细信息。

步骤 3 从下拉列表中选择接口。

步骤 4 单击下一步。

步骤 5 在配置路由器选择连接类型下，选择互联网连接类型。

步骤 6 如果选择动态 IP 或 DHCP，单击下一步。

步骤 7 如果选择静态 IP 地址，单击下一步并配置以下设置。

静态 IP 地址	输入静态 IP 地址。
子网掩码	输入子网掩码。
网关 IP	输入网关 IP。
DNS	输入 DNS 的 IP 地址。

步骤 8 如果选择 PPPoE，单击下一步并配置以下设置。

帐户名称	输入帐户名称。
密码	输入密码。
确认密码	确认密码。

步骤 9 如果选择 PPTP 或 L2TP，单击下一步并配置以下设置。

帐户名称	输入帐户名称。
密码	输入密码。
确认密码	确认密码。
静态 IP 地址	输入静态 IP 地址。
子网掩码	输入子网掩码。
网关 IP	输入网关 IP。
远程服务器	输入远程服务器。
DNS	输入 DNS 的 IP 地址。

步骤 10 从“时区”下拉列表中选择路由器的时区。

步骤 11 选择以下选项之一：

- 启用网络时间协议同步，可自动设置日期和时间。
- 手动设置日期和时间，可手动设置日期和时间。输入日期和时间。

步骤 12 单击下一步。

步骤 13 在“选择 MAC 地址”部分，选择以下选项之一：

- 使用默认地址（推荐）。
- 使用本计算机的地址。
- 使用此地址 — 输入一个 MAC 地址。

步骤 14 单击下一步。

步骤 15 在“摘要”部分，检查设置并单击提交。

系统

您的 ISP 可能会分配一个主机名和一个域名以识别您的设备，或要求您指定同样的信息。如果是前一种情况，您可以根据需要更改默认值。按照下面这些步骤分配主机名和域名。

步骤 1 单击系统配置 > 系统。

步骤 2 在“主机名”字段中输入主机名。

步骤 3 在“域名”字段中输入域名。

步骤 4 单击应用。

时间

设置时间对网络设备至关重要，因为这样每个系统日志和错误消息可以获取时间戳，以便准确跟踪并与其他网络设备同步数据传输。

您可以配置时区（根据需要调整夏令时），并选择网络时间协议 (NTP) 服务器以同步日期和时间。

要配置时间和 NTP 服务器设置，请按照以下步骤操作：

-
- 步骤 1** 单击系统配置 > 时间。
- 步骤 2** 设置时区 — 选择与格林威治标准时间 (GMT) 相关的时区。
- 步骤 3** 设置日期和时间 — 选择自动或手动。
- a) 自动 — 选中默认或用户定义并输入符合条件的 NTP 服务器名称。
- b) 手动 — 输入日期和时间。
- 步骤 4** 设置夏令时 — 选中此项可启用夏令时时间。您可以选择夏令时模式 — 按日期或循环，然后输入开始日期和结束日期。您还可以指定夏令时偏移量（以分钟为单位）。
- 步骤 5** 单击应用。
-

日志

系统日志 (Syslog) 是网络设备的基本设置之一，它用于记录设备数据。您可以定义应生成日志的实例。只要发生此类定义的实例，系统都将生成包含时间和事件的日志。日志将被发送至系统日志服务器或以电子邮件的形式发送。然后，可以使用系统日志对网络进行分析和故障排除，以及提高网络的安全性。

配置日志设置

要配置日志设置，请按照以下步骤操作：

-
- 步骤 1** 单击系统配置 > 日志。
- 步骤 2** 在“日志”部分的日志设置下，选中启用。
- 步骤 3** 在日志缓存字段中，输入以 KB 为单位的值（范围：1 KB 至 4096 KB，默认值：1024 KB）。
- 步骤 4** 严重性 - 从下拉列表中选择相应的日志严重性级别。下面按照从高到低的顺序列出了严重性级别。

紧急	0 级，表示系统无法使用。
警报	1 级，表示需要立即采取措施。
严重	2 级，表示系统处于高危状态。
错误	3 级，表示设备中存在错误，例如单个端口离线。
警告	4 级，表示在记录警告消息时设备能够正常工作，但已经发生操作问题。
通知	5 级，表示发生了虽在正常范围之内，但却值得注意的情况。在记录通知时，设备能够正常工作，但系统已发出通知。
信息	6 级，表示算不上错误，但需要特殊处理的状态。

调试	7 级，表示调试消息包含通常只在调试问题时使用的信息。
----	-----------------------------

步骤 5 类别 — 选中全部或要在设备上记录的任意必需事件类别。

内核	涉及内核代码的日志。
许可证	涉及许可证违规的日志。
系统	与用户空间应用（例如，NTP、会话和 DHCP）相关的日志。
Web 过滤	与触发 Web 过滤的事件相关的日志。
防火墙	与防火墙规则、攻击和内容过滤相关的日志。
应用控制	与应用控制相关的日志。
网络	与路由、DHCP、WAN、LAN 和 QoS 相关的日志。
用户	与用户活动相关的日志。
VPN	与 VPN 相关的日志包含 VPN 隧道建立失败、VPN 网关故障等实例。
3G/4G	来自插入路由器的 3G/4G 装置的日志。
SSLVPN	与 SSLVPN 相关的日志。

步骤 6 在自动保存至 USB 中，选中启用以自动保存日志。

电子邮件服务器

电子邮件服务器可以配置为电子邮件帐户。电子邮件服务器日志会定期发送至特定电子邮件地址，因此管理员始终能够掌握网络的最新动态。路由器支持SMTP邮件帐户配置。例如：电子邮件地址、密码、报文摘要、可选参数、SMTP服务器端口号、SSL及TLS。

-
- 步骤 1 在电子邮件服务器部分，选中电子邮件系统日志，以启用在记录事件时，路由器发送电子邮件警报的功能。
 - 步骤 2 在电子邮件设置部分，单击链接到电子邮件设置页面，以配置电子邮件设置。
 - 步骤 3 在电子邮件主题部分输入主题。
 - 步骤 4 在严重性部分，从下拉列表中选择严重性级别。
 - 步骤 5 在日志队列长度部分，输入在 1 至 1000 范围内的长度。默认值为 50。
 - 步骤 6 在日志时间阈值部分，从下拉列表中选择时间阈值。
 - 步骤 7 在实时电子邮件警报部分，选中“全部”或您希望设备记录的任意电子邮件警报类别。
-

远程系统日志服务器

远程系统日志服务器用于将生成消息和事件的软件与存储和分析这些消息和事件的系统分隔开。启用远程系统日志服务器后，网络驱动程序会通过VPN隧道向本地内联网或互联网中的系统日志服务器发送消息。通过指定名称或IP地址，可对系统日志服务器进行配置。

-
- 步骤 1 在系统日志服务器部分中，选中启用以启用向远程服务器发送系统日志的功能。
 - 步骤 2 在系统日志服务器 1 字段中，输入日志消息应发送到的系统日志服务器的IP地址。
 - 步骤 3 在系统日志服务器 2 字段中，输入日志消息应发送到的系统日志服务器的IP地址。
 - 步骤 4 单击应用。
-

电子邮件

您可以按自己的规格要求配置设备的电子邮件服务器。

配置电子邮件

要配置电子邮件服务器，请按照以下步骤操作：

步骤 1 选择系统配置 > 电子邮件。

步骤 2 在电子邮件服务器下，输入以下信息：

SMTP 服务器	输入 SMTP 服务器的地址。
SMTP 端口	输入 SMTP 端口。
电子邮件加密	选择 无 或 TLS/SSL 作为电子邮件加密方法。
验证	从下拉列表中选择验证类型：无，登录，纯文本或 MD5。
电子邮件收件人 1	输入收件人的电子邮件地址。
电子邮件收件人 2	输入收件人的电子邮件地址（可选）。
电子邮件发件人地址	输入发件人的电子邮件地址。

步骤 3 单击测试与电子邮件服务器的连接以测试连接。

步骤 4 单击应用。

用户帐户

您可以创建、编辑和删除本地用户，并使用适用于各种服务（例如 PPTP、VPN 客户端、Web GUI 登录和 SSLVPN）的本地数据库验证这些用户的身份。如此一来，管理员能够进行控制，并仅允许本地用户访问网络。

要创建本地用户并确定密码复杂性，请按照以下步骤操作：

步骤 1 依次选择系统配置 > 用户帐户。

步骤 2 在本地用户密码复杂性下，选中启用以启用密码复杂性。

步骤 3 配置密码复杂性设置。

最短密码长度	输入最短密码长度以创建新密码（范围：0 到 64，默认为 8）。
最少字符类别数	输入应该用于新密码的最少字符类别数（范围：0 到 4，默认为 3）。使用以下四个类别中的三种构成密码：（大写字母、小写字母、数字或特殊字符）。
新密码不得与当前密码相同	如果启用此选项，在当前密码过期后，系统会要求用户输入与当前密码不同的密码。

步骤 4 在本地用户成员列表表中，单击“添加”以向路由器添加用户。

步骤 5 在添加用户帐户页面，输入以下信息：

用户名	输入用户名。
新密码	输入密码。
新密码确认	确认密码。
密码强度计	显示密码强度。
组	从下拉列表中选择组（管理员或访客）。

步骤 6 单击应用。

步骤 7 单击编辑或删除以编辑或删除现有的用户。

步骤 8 在编辑用户帐户页面，输入以下信息：

旧密码	输入旧密码。
新密码	输入新密码。
新密码确认	确认密码。
组	从下拉列表中选择组（管理员或访客）。

步骤 9 单击应用。

步骤 10 依次单击导入和选择文件，以导入用户名和密码 CSV 文件。

步骤 11 单击下载用户模板以下载用户模板。

远程验证服务

要使用 RADIUS 和 LDAP 启用外部用户验证，可使用远程验证服务。

步骤 1 在远程验证服务表中，单击添加并输入以下信息：

名称	指定域的名称。
----	---------

验证类型	<p>从下拉列表中选择验证类型：</p> <ul style="list-style-type: none"> • RADIUS — 为连接并使用网络服务的用户提供验证、授权和记帐 (AAA) 集中式管理的网络协议。 • 活动目录 — 有助于统一使用相互关联、复杂和不同的网络资源的 Windows OS 目录服务。 • LDAP — 轻型目录访问协议。
主服务器	<p>输入主服务器的 IP 地址。 端口 — 输入服务器的主端口。</p>
备份服务器	<p>输入备份服务器的 IP 地址。 端口 — 输入服务器的备份端口。</p>
预共享密钥	<p>如果验证类型已选为 RADIUS，则输入 RADIUS 服务器的预共享密钥。</p>
确认预共享密钥	<p>重新输入 RADIUS 服务器的预共享密钥以进行确认。</p>

步骤 2 单击应用保存设置。单击编辑或删除可编辑或删除现有的域。

注释 外部数据库优先级始终为 RADIUS/LDAP/AD/本地。如果您在路由器上添加 Radius 服务器，则 Web 登录服务和其他服务将使用 RADIUS 外部数据库对用户进行验证。不提供单独为 Web 登录服务启用外部数据库并为其他服务配置其他数据库的选项。在路由器上创建并启用 RADIUS 后，路由器将使用 RADIUS 服务作为 Web 登录、站点到站点 VPN、EzVPN/第三方 VPN、SSL VPN、PPTP/L2TP VPN、802.1x 的外部数据库。

用户组

管理员可以为共享同一组服务的一群用户创建用户组。此类用户组可被授权访问多项服务，例如 Web 登录、PPTP、L2TP 和 EzVPN。

要创建用户组，请按照以下步骤操作：

- 步骤 1** 依次选择系统配置 > 用户组。
- 步骤 2** 在“用户组表”下，单击添加创建新用户组。
- 步骤 3** 在“组名称”字段中，输入组的名称。
- 步骤 4** 在“本地用户成员关系列表”下，在“加入”列中选中所需的复选框，以将用户列表添加到组。
- 步骤 5** 在“服务”下，选择用户组有权访问的服务，并输入以下信息。

Web 登录	指定向添加到组的用户授予的 Web 登录权限： <ul style="list-style-type: none"> • 已禁用 — 用户组的任何成员都不能使用 Web 浏览器登录配置实用程序。 • 只读 — 用户组的成员登录后只能读取系统状态。他们无法编辑任何设置。 • 管理员 — 用户组的所有成员均拥有配置和读取系统状态的完整权限。
站点到站点 VPN	选中授予此组权限以便访问站点到站点 VPN 策略。 <ul style="list-style-type: none"> • 单击添加打开添加功能列表弹出窗口。 • 从下拉列表中选择配置文件，然后单击添加。
EzVPN/第三方	选中授予此组权限以便访问站点到站点 VPN 策略。 <ul style="list-style-type: none"> • 单击添加打开添加功能列表弹出窗口。 • 从下拉列表中选择配置文件，然后单击添加。
SSL VPN	从下拉列表中选择配置文件。
PPTP VPN	选中允许可启用 PPTP 验证。
L2TP	选中允许可启用 L2TP 验证。
802.1x	选中允许可启用 802.1x 验证。

步骤 6 单击应用。

注释 802.1x 仅支持 RADIUS 验证。PPTP/L2TP 支持 RADIUS 和本地数据库。如果您选择本地数据库，则只支持使用密码验证协议 (PAP) 进行本地验证。

IP 地址组

为了配置和管理应用控制策略与 Web 过滤，必须设置 IP 地址组。要配置 IP 地址组，请按照以下步骤操作：

步骤 1 单击系统配置 > IP 地址组。

步骤 2 在 IP 地址组表中单击添加，以添加组并输入名称。要删除组，请单击删除。

步骤 3 单击添加并输入以下信息。

协议	从下拉列表中选择 IPv4 或 IPv6。
----	-----------------------

类型和地址详细信息	<p>从下拉列表中选择组类型，并输入地址详细信息：</p> <ul style="list-style-type: none"> • IP 地址 — 在“IP 地址”字段中输入 IP 地址。 • IP 地址子网 — 在“IP 地址”字段中输入 IP 地址，在“掩码”字段中输入其子网掩码。 • IP 地址范围 — 输入“起始 IP 地址”和“结束 IP 地址”。
-----------	---

步骤 4 单击应用。

SNMP

简单网络管理协议 (SNMP) 是一种互联网标准协议，它用于收集和组织的 IP 网络中托管设备的信息，并修改这一信息以改变设备行为。

步骤 1 要配置路由器的 SNMP，请输入以下信息：

SNMP 启用	选中此选项可启用 SNMP。
允许来自互联网的用户访问	选中此选项可允许来自互联网的用户访问。
允许来自 VPN 的用户访问	选中此选项可允许来自 VPN 的用户访问。
版本	从下拉列表中选择版本。
系统名称	输入系统名称。
系统联系人	输入系统联系人。
系统位置	输入系统位置。
获取社区	输入社区的名称。
设置社区	输入社区的名称。

陷阱配置

使用陷阱配置，您可以设置路由器（无论从哪个传出接口）向单个地址发送的每个 SNMP 陷阱数据包的源地址。

步骤 2 要配置 SNMP 陷阱，请输入以下信息。

陷阱接收器 IP 地址	输入 IP 地址。
-------------	-----------

陷阱接收器端口	输入端口号。
---------	--------

步骤 3 完成设置后，单击应用。

发现 Bonjour

Bonjour 是一项服务发现协议，用于定位 LAN 上的计算机和服务器等网络设备。启用此功能之后，设备会定期向 LAN 组播 Bonjour 服务记录，以通告此服务的存在。



注释 为了发现思科 S 系列产品，思科提供了一种通过 Web 浏览器上的简单工具栏即可工作的实用程序，称为 FindIt。此实用程序可发现网络中的思科设备并显示序列号和 IP 地址等基本信息。如需了解更多信息并下载此实用程序，请访问 www.cisco.com/go/findit。

要启用“发现 Bonjour”，请按照以下步骤操作：

步骤 1 选择系统配置 > 发现 Bonjour。

步骤 2 选中启用以全局启用“发现 Bonjour”。（默认情况下，此功能处于启用状态。）

步骤 3 选中应用。

LLDP

链路层发现协议 (LLDP) 是网络设备使用的互联网协议套件中的供应商中立协议，用于在 IEEE 802 局域网通告其身份、功能和邻居。LLDP 信息由设备以固定时间间隔，从其接口以以太网帧的形式进行发送。每个帧包含一个 LLDP 数据单元 (LLDPDU)。每个 LLDPDU 都由类型-长度-值 (TLV) 结构序列构成。

要配置 LLDP，请按照以下步骤操作：

步骤 1 选择系统配置 > LLDP。

步骤 2 在 LLDP 部分，选中启用。（默认情况下，此功能处于启用状态。）

步骤 3 在 LLDP 端口设置表中，选中启用 LLDP 以在接口上启用 LLDP。

步骤 4 单击应用。

步骤 5 LLDP 邻居设置表中显示以下信息：

- **本地端口** — 端口标识符。
- **机箱 ID 子类型** — 机箱 ID 的类型（例如，MAC 地址）。
- **机箱 ID** — 机箱的标识符。如果机箱 ID 子类型为 MAC 地址，则屏幕上会显示设备的 MAC 地址。
- **端口 ID 子类型** — 端口标识符的类型。
- **端口 ID** — 端口标识符。
- **系统名称** — 设备的名称。
- **存活时间** — 发送 LLDP 通告更新的速率（以秒为单位）。

步骤 6 要查看关于 LLDP 端口的详细信息，请选择“本地端口”并单击**详细信息**。

步骤 7 要刷新“LLDP 邻居设置表”，请单击**刷新**。

自动更新

升级至最新固件版本有助于修复路由器上的故障和其他偶发性问题。为此，可以配置路由器，从而在您的设备有重要固件更新时，通过电子邮件向您发送通知。通过配置，可以针对特定类型的网络事件，以指定时间间隔发送信息。您需要先配置电子邮件服务器，然后才能配置这些通知。

要配置“自动更新”，请按照以下步骤操作：

步骤 1 选择**系统配置 > 自动更新**。

步骤 2 从**检查频率**下拉列表中，选择设备自动检查可能固件版本的频率（**从不**、**每周一次**或**每月一次**）。单击**立即检查**可立即执行检查。

步骤 3 在**通知方式**字段中，选中“电子邮件收件人”并输入电子邮件地址。通知将发送至配置的电子邮件地址。如果您尚未配置电子邮件服务器，应单击电子邮件字段旁边给出的说明中的链接，并配置电子邮件服务器。

步骤 4 在**自动更新**下，选择**通知**以接收更新通知。

步骤 5 从下拉列表中选择自动更新固件的时间。您可以选择接收通知，并为以下项目配置更新：

- 系统固件
- USB 调制解调器固件
- 安全签名

步骤 6 单击**应用**。

服务管理

“服务管理”部分显示有关系统配置的信息。您可以向“服务管理”列表添加新条目或更改条目。要配置服务管理，请按照以下步骤操作：

-
- 步骤 1 单击系统配置 > 服务管理。
 - 步骤 2 在“服务表”中，单击添加。
 - 步骤 3 在应用名称字段中，输入名称以用于标识和管理。
 - 步骤 4 在“协议”字段中，从下拉列表中选择该服务使用的第4层协议：（TCP和UDP、TCP、UDP、IP、ICMP）。
 - 步骤 5 在起始端口/ICMP 类型/IP 协议中，输入端口号、ICMP 类型或 IP 协议。
 - 步骤 6 在结束端口字段中，输入端口号。
 - 步骤 7 单击应用。
 - 步骤 8 要编辑条目，请选择该条目，然后单击编辑。进行更改，然后单击应用。
-

计划表

网络设备应得到保护，从而抵御可能损害机密性或导致数据损坏或拒绝服务的蓄意攻击和病毒。创建计划表可以在特定的日期或时间应用防火墙或端口转发规则。

要配置计划表，请按照以下步骤操作：

-
- 步骤 1 选择系统配置 > 计划表。
 - 步骤 2 在计划表中，单击添加创建新的计划表。选择计划表并单击编辑可编辑计划表。
 - 步骤 3 在名称列中输入名称以查找计划表。
 - 步骤 4 输入所需的计划表开始时间和结束时间。
 - 步骤 5 选中每天可将计划表应用到周内的每一天。如果您只需要在某几天应用计划表，则取消选中此选项。在这种情况下，请再选中您要在星期几应用计划表。您也可以选择工作日或周末。
 - 步骤 6 单击应用。
-



第 5 章

WAN

本节介绍广域网 (WAN)，包含以下主题：

- [WAN 设置](#)，第 39 页
- [多 WAN](#)，第 42 页
- [移动网络](#)，第 44 页
- [动态 DNS](#)，第 45 页
- [硬件 DMZ](#)，第 46 页
- [IPv6 转换](#)，第 46 页

WAN 设置

路由器上有两个可以配置的物理 WAN 和 VLAN 接口。要配置 WAN 设置，请按照以下步骤操作：

- 步骤 1** 依次选择 **WAN > WAN 设置**。
- 步骤 2** 在 **WAN 表** 中单击添加。
- 步骤 3** 选择接口 (**WAN1** 或 **WAN 2**)。选择接口后，相应的子接口名称将会显示在下方。将该子接口添加至“多 WAN”表，以转发默认的路由流量，否则它将根据路由表仅转发已连接的路由流量。
- 步骤 4** 输入 **VLAN ID**。
- 步骤 5** 配置 IPv4、IPv6 或高级协议设置。
- 步骤 6** 单击应用。
IPv4 和 IPv6 连接
- 步骤 7** 对于 IPv4 连接，请单击 **IPv4** 选项卡。
- 步骤 8** 从列表中选择连接类型：
当 **IPv4** 或 **IPv6** 连接使用 **DHCP** 时

在“DHCP 设置”部分输入以下信息：

DNS 服务器	选择使用 DHCP 提供的 DNS 服务器或使用如下 DNS。
静态 DNS 1 和静态 DNS 2	在字段中输入主要和/或辅助静态 DNS 的 IP 地址。
DHCP-PD（仅限 IPv6）	选中即可启用并输入前缀名称。

当 IPv4 或 IPv6 连接使用静态 IP 时

在静态 IP 设置部分输入以下信息：

WAN IP 地址	输入 IP 地址。
子网掩码	输入子网掩码。
默认网关	输入默认网关的 IP 地址。此接口上必须有默认网关，才能参与负载平衡和故障切换（多 WAN）。
静态 DNS 1 和静态 DNS 2	在字段中输入主要和/或辅助静态 DNS 的 IP 地址。
DHCP-PD（仅限 IPv6）	选中即可启用并输入前缀名称。

当 IPv4 或 IPv6 连接使用 PPPoE 时

在“PPPoE 设置”部分输入以下信息：

用户名	ISP 分配给您的用户名。
密码	ISP 分配给您的密码。
DNS 服务器	选择使用 PPPoE 提供的 DNS 服务器或使用 DNS。
静态 DNS 1 和静态 DNS 2	在字段中输入主要和/或辅助静态 DNS 的 IP 地址。
连接模式	如果 ISP 收取连接费用，请选择 按需连接 。输入由于处于不活动状态而终止连接之前，等待的最大空闲时间（以秒为单位）。默认值为 5 分钟。 选择 保持活动 以定期检查连接，并在连接断开后自动重新建立连接。
验证类型	从下拉列表中选择验证类型（自动、PAP、CHAP、MS-CHAP、MS-CHAPv2）。
服务名称	输入服务的名称。
DHCP-PD（仅限 IPv6）	选中即可启用并输入前缀名称。

注释 某些服务提供商不允许 ping 默认网关，特别是 PPPoE 连接的网关。请转至“多 WAN”页面禁用“网络服务检测”功能，或选择有效的主机进行检测。否则，设备不会转发流量。

当 IPv4 通过 PPTP 连接时

在“PPTP”部分输入以下信息：

IP 分配	对于 DHCP，请选择此选项以使 DHCP 提供 IP 地址。对于静态 IP，请选择此选项，并提供 IP 地址、子网掩码和默认网关的 IP 地址。
PPTP 服务器 IP/FQDN	输入服务器的名称。
用户名	ISP 分配给您的用户名。
密码	ISP 分配给您的密码。
DNS 服务器	选择使用 PPTP 提供的 DNS 服务器或使用 DNS。
静态 DNS 1 和静态 DNS 2	在字段中输入主要和/或辅助静态 DNS 的 IP 地址。
连接模式	如果 ISP 收取连接费用，请选择 按需连接 。输入由于处于不活动状态而终止连接之前，等待的最大空闲时间（以秒为单位）。默认值为 5 分钟。 选择 保持活动 以定期检查连接，并在连接断开后自动重新建立连接。。
验证类型	从下拉列表中选择验证类型（自动、PAP、CHAP、MS-CHAP、MS-CHAPv2）。
MPPE 加密	选中即可启用 MPPE 加密。

当 IPv4 连接使用 L2TP 时

在“L2TP 设置”部分输入以下信息。

IP 分配	对于 DHCP，请选择此选项以使 DHCP 提供 IP 地址。对于静态 IP，请选择此选项，并提供 IP 地址、子网掩码和默认网关的 IP 地址。
L2TP 服务器 IP/FQDN	输入服务器的名称。
用户名	ISP 分配给您的用户名。
密码	ISP 分配给您的密码。
DNS 服务器	选择使用 L2TP 提供的 DNS 服务器或使用 DNS。
静态 DNS 1 和静态 DNS 2	在字段中输入主要和/或辅助静态 DNS 的 IP 地址。
连接模式	如果 ISP 收取连接费用，请选择 按需连接 。输入由于处于不活动状态而终止连接之前，等待的最大空闲时间（以秒为单位）。默认值为 5 分钟。 选择 保持活动 以定期检查连接，并在连接断开后自动重新建立连接。
验证类型	从下拉列表中选择验证类型（自动、PAP、CHAP、MS-CHAP、MS-CHAPv2）。

当 IPv6 连接使用网桥时

网桥设置

桥接至	系统默认为 VLAN1。
IP 地址	输入 IP 地址。

子网掩码	输入子网掩码。
默认网关	输入默认网关。
静态 DNS 1 和静态 DNS 2	在字段中输入主要和/或辅助静态 DNS 的 IP 地址。

当 IPv6 连接使用 SLAAC 时

在“SLAAC 设置”部分输入以下信息：

静态 DNS 1 和静态 DNS 2	在字段中输入主要和/或辅助静态 DNS 的 IP 地址。
DHCP-PD（仅限 IPv6）	选中即可启用并输入前缀名称。

步骤 9 单击应用。

对于高级协议

步骤 10 单击“高级”选项卡，配置以下内容：

MTU（最大传输单位）	选择自动可自动设置大小。要手动设置 MTU 大小，请选择手动并输入 MTU 大小。（该层可以传递的最大协议数据单元的大小，以字节为单位。）
MAC 地址克隆	选中 MAC 地址克隆，然后输入 MAC 地址。单击克隆我的 PC 的 MAC 地址可将计算机的 MAC 地址用作设备的克隆 MAC 地址。

注释 启用“MAC 地址克隆”后，端口镜像无法工作。

步骤 11 单击应用。

注释 将这些子接口中的任意接口添加至“多 WAN”表，以转发默认路由流量。否则，它将根据路由表，仅转发已连接的路由流量。

多 WAN

WAN 故障切换和负载平衡功能可实现多个 WAN 接口的高效利用。根据配置，此功能可用于多个接口之间的流量分配。多 WAN 功能基于权值分配，提供多个 WAN 接口（WAN 和 USB）之间的出站 WAN 流量和负载平衡。它还使用重复的 Ping 测试监控每个 WAN 连接，并在连接断开时将出站流量自动路由至另一个 WAN 接口。由于采用 5 元组连接，还可以配置特定的出站流量规则。它对每个 IP 连接执行出站网络负载平衡，而不是单个连接同时使用多个 WAN 连接的通道捆绑。为实现负载平衡或故障切换，它还可以为 WAN 配置 VLAN 接口。

要配置多 WAN 设置，请按照以下步骤操作：

步骤 1 选择 **WAN > 多 WAN**。

步骤 2 在“接口设置表”中，配置以下设置：

- **接口** — 应用负载平衡和故障切换配置的 WAN 接口名称。选择并检查所需接口（**WAN1**、**WAN2**、**USB1** 或 **USB2**）。
- **优先级（用于故障切换）** — 为接口输入优先级值，用于在其他接口上建立另一个连接。
- **加权百分比或加权带宽（用于负载平衡）** — 输入每个连接的加权百分比或值。在尝试平衡带宽负载时，如果主连接过载，接口会将流量路由至辅助连接。为确保两个连接的充分利用，两个连接的负载平衡权值之比应反映连接的带宽之比。

步骤 3 单击**高级配置**，并配置以下设置：

a) **启用网络服务检测** — 选中此选项以允许设备通过 Ping 特定的设备检测网络连接，然后输入下述设置。

- **重试计数** — Ping 设备的次数。范围为 1 至 10，默认值为 3。
- **重试超时** — 两次 Ping 操作之间的等待时间（以秒为单位）。范围为 1 至 300，默认值为 5 秒。
- **检测目标** — 选择**默认网关**或**远程主机** — 如果选择远程主机，则输入主机。

步骤 4 单击**应用**。

步骤 5 **启用基于策略的路由** — 选中以启用该功能。

步骤 6 然后，单击**添加或编辑**，并配置以下设置：

优先级	输入优先级值。
源 IP	输入源 IP 地址。
目标 IP	输入目标 IP 地址。
服务	从下拉列表中选择服务。如果某服务未列出，可以单击 服务管理 添加服务。
传出接口	从下拉列表中选择传出接口（ WAN1 、 WAN2 、 USB1 或 USB2 ）。
故障切换至备份 WAN	从“故障切换至备份 WAN”下拉列表中选择 打开 或 关闭 。 注释 如果选择 关闭 ，当绑定接口离线或断开时，流量将被丢弃。
状态	选择 启用 或 禁用 以启用或禁用策略的状态。

步骤 7 还可通过单击**编辑**或**删除**以编辑或删除配置。

步骤 8 单击**应用**。

注释 某些服务提供商不允许 Ping 默认网关。请选择有效的远程主机以检测网络连接，或者直接禁用检测。否则，设备不会转发流量。

移动网络

移动宽带调制解调器是一种允许笔记本电脑、个人电脑或路由器使用移动宽带连接（而不是电话或数据电缆）获取互联网接入的调制解调器。

要配置移动网络，请按照以下步骤操作：

-
- 步骤 1 选择 **WAN > 移动网络**。
 - 步骤 2 在“全局设置”部分，选择接口（USB1 或 USB2）以应用设置。
 - 步骤 3 在“卡状态”部分，单击**连接**以建立连接。
 - 步骤 4 在“服务类型”部分，从下拉列表中选择服务类型。
-

移动网络设置

要配置移动网络设置，请按照以下步骤操作：

-
- 步骤 1 在“配置模式”中，选择**自动**以自动连接到网络。
 - 步骤 2 输入 **SIM PIN** - 与 SIM 卡关联的 PIN 码。
 - 步骤 3 或者，选择**手动**以手动连接到网络，并配置以下设置：
 - **接入点名称** — 输入移动网络服务提供商提供的接入点名称。
 - **拨号号码** — 输入移动网络服务提供商提供的用于连接互联网的号码。
 - **用户名和密码** — 输入移动网络服务提供商提供的用户名和密码。
 - **SIM PIN** — 输入与 SIM 卡关联的 PIN 码。
 - **服务器名称** — 输入服务器的名称。
 - **验证** — 选择要验证的选项。
 - 步骤 4 从以下连接模式中选择一种。
 - **按需连接** — 指定连接定时器，如果定时结束且这段时间内无活动，则终止连接。输入以秒为单位的“最长空闲时间”，即在因无活动而终止连接前的等待时间。默认值为 5 分钟。
 - **保持活动** — 定期检查与路由器的连接，以便在连接断开时重新建立连接。在“重拨周期”中，输入路由器自动检查连接的时间间隔（以秒为单位）。默认周期为 30 秒。

带宽上限设置

“带宽上限跟踪”将一段时间内传输的数据量限制在指定值。它又被称为带宽上限或数据上限。要配置带宽上限设置，请按照以下步骤操作：

步骤 1 选中**带宽上限跟踪**，输入以下信息：

- **每月更新日期** — 选择应用带宽上限设置的天数。
- **每月带宽上限** — 输入数据的大小。
- **当 3G/4G 流量达到每月带宽上限的某个百分比时向管理员发送电子邮件** — 选择每月带宽上限的数据百分比。当达到上限时，向管理员发送电子邮件警告。

步骤 2 完成设置后，单击**应用**。

动态 DNS

并非所有计算机都使用静态 IP 地址，而动态域名系统 (DDNS) 就是一种能确保域名链接到变化的 IP 地址的方法。DDNS 通过服务器主机名、地址或其他信息的主动配置自动更新 DNS 中的服务器。DDNS 将固定域名分配给动态的 WAN IP 地址。因此，您可以在 LAN 上托管自己的 Web FTP 或其他类型的 TCP/IP 服务器。有多种 DDNS 服务可供选择，其中大部分免费，或者以很低的价格提供。最受欢迎的是 DynDNS。

要配置动态 DNS 策略，请按照以下步骤操作：

-
- 步骤 1 选择 **WAN > 动态 DNS**。
 - 步骤 2 在“动态 DNS 表”中，选择要添加到动态 DNS 策略的接口（**WAN1**、**WAN2**、**USB1** 或 **USB2**）。
 - 步骤 3 单击**编辑**。
 - 步骤 4 选中**启用该动态 DNS 策略**以启用策略配置。
 - 步骤 5 从“提供商”下拉列表中选择服务提供商的名称。
 - 步骤 6 输入 DDNS 帐户的**用户名和密码**。
 - 步骤 7 在“完全限定域名”中输入设备全称，包括域名。
 - 步骤 8 选中**启用**以接收动态 DNS 提供商的更新，并选择周期。
 - 步骤 9 单击**应用**。
 - 步骤 10 单击**刷新**以刷新动态 DNS 表。
-

硬件 DMZ

隔离区 (DMZ) 接受所有传入流量并允许所有传出流量。DMZ 是一个子网，向公众开放但位于防火墙之后。可以使用 DMZ 将传输到 WAN 端口的数据包重定向到特定 IP 地址。您可以配置防火墙规则，从而允许从 LAN 和 WAN 访问 DMZ 中的特定服务和端口。倘若任意 DMZ 节点遭到攻击，LAN 不一定会受到攻击。建议将必须向 WAN 公开的主机（例如 Web 或电子邮件服务器）置于 DMZ 网络中。

要配置硬件 DMZ，请按照以下步骤操作：

-
- 步骤 1 选择 **WAN > 硬件 DMZ**。
 - 步骤 2 单击**启用**，将 LAN4 更改为 DMZ 端口。
 - 步骤 3 选择子网以确定 DMZ 服务的子网，然后输入 **DMZ IP 地址**和**子网掩码**。
 - 步骤 4 选择**范围**（DMZ 和 WAN 位于同一子网内），并输入 IP 范围。
 - 步骤 5 单击**应用**。
-

IPv6 转换

要从 IPv4 迁移至 IPv6，可以使用名为 6in4 的互联网转换机制。6in4 使用隧道，将 IPv6 流量封装进配置的 IPv4 链接。6in4 流量通过 IPv4 发送，使用 IPv4 数据包报头。其后为 IPv6 数据包，其 IP 报头的 IP 协议编号设置为 41。

要配置 IPv6 转换，请按照以下步骤操作：

-
- 步骤 1 选择 **WAN > IPv6 转换**。
 - 步骤 2 在“隧道表”中，选择要配置的接口，并单击**编辑**。
 - 步骤 3 选中**启用**。
 - 步骤 4 输入说明。
 - 步骤 5 从下拉列表中选择本地接口（**WAN1** 或 **WAN 2**）。
 - 步骤 6 “本地 IPv4 地址”显示选中接口的地址。
-

IPv6 的 IPv4 封装隧道 (6in4)

要添加 IPv4 隧道 (6in4)，请输入以下信息：

-
- 步骤 1 单击 **IPv6 的 IPv4 封装隧道 (6in4)** 选项卡。
 - 步骤 2 输入远程 **IPv4** 地址。
 - 步骤 3 输入本地 **IPv6** 地址。
 - 步骤 4 输入远程 **IPv6** 地址。
 - 步骤 5 完成设置后，单击**应用**。
-

IPv6 快速部署 (6rd)

在 IPv6 快速部署 (6rd) 中，每个 ISP 使用其自有的 IPv6 前缀之一，而不是 6to4 的标准化特殊 2002::/16 前缀。因此，对于可接入 IPv6 网络的所有本征 IPv6 主机，均可保证提供商 6rd 主机的可用性。

要添加 IPv6 快速部署 (6rd)，请输入以下信息：

-
- 步骤 1 单击“**IPv6 快速部署 (6rd)**”选项卡。
 - 步骤 2 单击从 **DHCP 自动获取**，以使用 DHCP（选项 212）获取 6rd 前缀、中继 IPv4 地址和 IPv4 掩码长度。
 - 步骤 3 或者，选择**手动**并设置以下 6rd 参数。
 - a) 输入中继的 **IPv4** 地址。
 - b) 输入 **IPv4** 通用前缀长度。
-

- c) 输入 **IPv6 前缀/长度**。IPv6 网络（子网）通过前缀进行标识。网络中所有主机的 IPv6 地址具有相同的初始位。输入网络地址中常见初始位的位数。默认值为 64。

步骤 4 单击应用。



第 6 章

QoS

本节介绍服务质量 (QoS)，此功能用于优化网络流量，从而提升用户体验。QoS 通过在网络中设置特定数据类型（视频、音频、文件）的优先级，来控制和管理网络资源。此功能专门应用于为视频点播、IPTV、IP 电话、流媒体、视频会议和在线游戏生成的网络流量。本节包含以下主题：

- [流量类，第 49 页](#)
- [WAN 队列，第 50 页](#)
- [WAN 监管，第 51 页](#)
- [WAN 带宽管理，第 51 页](#)
- [交换机分类，第 52 页](#)
- [交换机队列，第 53 页](#)

流量类

流量类根据服务将互联网流量引导至所需队列。服务可以是第 4 层 TCP 或 UDP 端口应用、源或目标 IP 地址、DSCP、接收接口、操作系统和设备类型。

要配置流量类，请按照以下步骤操作：

- 步骤 1** 依次单击 **QoS > 流量类**。
- 步骤 2** 在“流量表”中，单击**添加**（或选择相应行，然后单击**编辑**），并输入以下信息：
- **类名称** — 输入定义的类的名称。
 - **说明** — 输入类说明。
 - **使用中** — 队列策略正在使用的流量类记录。
- 步骤 3** 在“服务”表中，单击**添加**（或选择相应行，然后单击**编辑**），并输入以下信息：

服务名称	输入服务的名称。
接收接口	从下拉列表中选择接口（WAN1、WAN2、USB1、USB2、LAN1、LAN2、LAN3、LAN4 或 VLAN1）。
IP 版本	选择 IPv4、IPv6 或任意一个（如果您不清楚流量版本）。
源 IP	输入流量的源 IP 地址。
目标 IP	输入流量的目标 IP 地址。
服务/应用	<ul style="list-style-type: none"> • 服务：选择要应用于流量记录的服务的名称。提供源和目标端口。 • 应用：选择要应用于流量记录的应用。选择应用行为和类别。 <p>注释 用户在“安全/应用控制”页面中启用应用控制之前，无法配置应用规则。</p>
设备类型	从下拉列表中选择产生流量的设备所属的类型。
操作系统类型	从下拉列表中选择产生流量的设备运行的操作系统。
匹配 DSCP	DSCP 匹配 IPv6 流量的 IPv6 标头中的流量类值。流量类值是配置的值的 4 倍。例如，如果用户将匹配的 DSCP 配置为 10，然后将 DSCP 重写为 18。此规则会匹配流量类值为 40 的 IPv6 流，并将 DSCP 重写为 72。从下拉列表中选择与传入数据包中的 DSCP 值匹配的 DSCP 值。
重写 DSCP	从下拉列表中选择传入数据包中要替换成的 DSCP 值。

步骤 4 单击应用。

WAN 队列

可在三个相互排斥的模式（速率控制、优先级和低延迟）中对来自 LAN 到 WAN 的网络流量进行控制。

要配置 WAN 队列，请按照以下步骤操作：

-
- 步骤 1 单击 **QoS > WAN 队列**。
 - 步骤 2 在“WAN 队列表”中，选择所需的队列引擎（优先级、速率控制或低延迟）。
 - 步骤 3 在“WAN 队列表”中，单击**添加**，然后输入策略名称并提供说明。
 - 步骤 4 如果选择“优先级队列”，则在“排队优先级表”中从下拉列表中选择每个队列的流量类。
 - 步骤 5 如果选择“速率控制队列”，则在“队列速率控制表”中选择“流量类”，然后输入每个队列的最小和最大速率。
 - 步骤 6 如果选择“低延迟队列”，则在“队列低延迟表”中选择“流量类”，然后配置每个队列的带宽共享值。
 - 步骤 7 单击**应用**。
-

WAN 监管

在“WAN 监管”中，速率控制模式可支持八个队列。每个队列均可配置为使用最大速率。

要配置“WAN 监管”页面，请按照以下步骤操作：

-
- 步骤 1 单击 **QoS > WAN 监管**。
 - 步骤 2 选中在 **WAN 接口**上启用**流量监管**。
 - 步骤 3 在“策略类表”中，为每个队列配置以下设置：

流量类	选择未指定或默认。
最大速率	输入队列的最大带宽速率（以百分数表示）以限制从 WAN 到 LAN 的传入流量。

- 步骤 4 单击**应用**。
-

WAN 带宽管理

WAN 接口可以使用 ISP 提供的最大带宽进行配置。对此值（以 KBP/S 为单位的传输速率）进行配置后，可以定义的速率对进入端口的流量进行整形。

要配置 WAN 带宽管理，请按照以下步骤操作：

步骤 1 单击 **QoS > WAN 带宽管理**。

步骤 2 在“WAN 带宽管理表”中，选择接口，然后配置以下设置：

上游 (kb/s)	输入上游流量速率（以 kb/s 为单位）。
下游 (kb/s)	输入下游流量速率（以 kb/s 为单位）。*您将需要为下游带宽启用 WAN 监管功能，否则下游带宽不会生效。
出站排队策略	选择要向 WAN 接口应用的出站排队策略。

步骤 3 单击应用。

交换机分类

在基于端口、基于 DSCP 和基于 CoS 等 QoS 模式下，数据包是向外发送的。

要配置交换机分类，请单击 **QoS > 交换机分类**，并按照以下步骤操作：

步骤 1 选择所需的交换机 QoS 模式（基于端口、基于 DSCP 或基于 CoS）。

基于端口	<p>在每个 LAN 端口上，传入数据包基于映射关系映射到特定队列。</p> <ul style="list-style-type: none"> • LAN 端口队列 — 选择“LAN 端口队列”，以映射各个 LAN 端口上的传入流量。 • LAG 端口队列 — 启用 LAG 后，系统会使用配置的队列映射进入此 LAG 接口的所有流量。
基于 DSCP	<p>对于 IPv6 流量，DSCP 会匹配 IPv6 标头中的流量类值，并将其放置在不同的队列中。流量类值是 DSCP 值的 4 倍。例如，如果用户的配置是 DSCP 值 10 映射至队列 1，那么系统会将流量类值为 40 的 IPv6 流放入队列 1。交换机必须使用传入数据包的 DSCP 字段，并使用映射表优先安排数据包进入特定队列。</p> <ul style="list-style-type: none"> • 根据传入数据包的 DSCP 值，将流量映射至不同的队列。
基于 CoS	<p>交换机使用传入数据包优先级“CoS”位，并将数据包划分到用户配置的队列。</p> <ul style="list-style-type: none"> • 根据传入数据包的 CoS 值，通过从下拉列表中选择队列将流量映射至不同的队列。

步骤 2 单击应用。

交换机队列

在“交换机队列”中，可以通过为每个队列分配加权，配置每个端口上所有四个队列的队列加权。加权的范围是 1 到 100。启用 LAG 后，用户可以定义所有四个队列的队列加权。



注释 如果加权为 0，则意味着相应队列在优先级最高的队列中。

要配置 LAN 端口队列加权，请单击“QoS > 交换机队列”，并完成以下操作：

步骤 1 在“LAN 端口队列加权”中，为每个队列选择相应的加权。

步骤 2 单击应用。

步骤 3 单击恢复默认设置，恢复系统默认设置。

步骤 4 “LAG 端口队列加权”表会显示 LAG 端口及其队列加权。



第 7 章

LAN

本节介绍局域网 (LAN)，这是一种覆盖面积相对较小区域（例如办公大楼、学校或家庭）的计算机网络。本节包含以下主题：

- [端口设置，第 55 页](#)
- [VLAN 设置，第 56 页](#)
- [LAN/DHCP 设置，第 57 页](#)
- [静态 DHCP，第 60 页](#)
- [802.1X 配置，第 60 页](#)
- [DNS 本地数据库，第 61 页](#)
- [路由器通告，第 61 页](#)

端口设置

“端口设置”页面显示 EEE、流量控制、模式、端口镜像和链路聚合的端口。
要配置 LAN 的端口设置，请按照以下步骤操作：

步骤 1 选择 **LAN > 端口设置**。

步骤 2 在各基本端口配置表中，配置以下设置：

端口	列出路由器上当前可用的端口。
已启用	选中此选项可启用端口并对端口进行设置。禁用此复选框后，端口上的所有设置将全部丢失。
EEE（节能以太网）	选中此选项可降低端口在数据活动量较少时的功耗。

流量控制	选中此选项可启用对称流量控制。流量控制用于在连接到设备的 LAN PC 之间收发暂停帧和对应的暂停帧。
模式	从下拉列表中选择端口设置模式。

步骤 3 在“端口镜像配置”部分，输入以下信息：

启用	选中启用可启用端口镜像配置。
目标端口	从下拉列表中选择任一 LAN (LAN1 到 LAN4)。
受监控端口	对发送用于映射的流量进行监控所用的端口。 从下拉列表中选择任一 LAN (LAN1 到 LAN4)。

步骤 4 在链路聚合配置表中，输入以下信息：

组名称	列出链路组的名称。
未分配	选中此选项可将端口从 LAG 表中删除。 从下拉列表中选择任一 LAN (LAN1 到 LAN4)。
LAG1	选择在适当的端口上对流量应用链路聚合。 从下拉列表中选择任一 LAN (LAN1 到 LAN4)。

警告 端口（将成为 LAG 的一部分）上现有的配置会全部丢失。

步骤 5 单击应用。

VLAN 设置

通过应用指定的 VLAN，可以为端口上的流量加标记。这种标记有助于区分和转发流量。系统中仅有 32 个 VLAN。如果 WAN 使用了少数 VLAN，那么 LAN 可以使用剩余的 VLAN。

要配置 VLAN 设置，请输入以下信息：

-
- 步骤 1** 选择 **LAN > VLAN 设置**。
- 步骤 2** 在 VLAN 表中，单击**添加**。
- 步骤 3** 输入 VLAN ID。（范围为 1-4093）。
- 步骤 4** 选中可启用 **Inter-VLAN**。
- 步骤 5** 输入 IPv4 地址。
- 步骤 6** 输入前缀、前缀长度和接口标识符。
- 步骤 7** 单击**编辑**或**删除**可编辑或删除 VLAN 表配置。
- 步骤 8** 在“VLAN 到端口表”中，单击**编辑**可向 LAN 端口分配 VLAN。为表中所列的每个 VLAN 指定以下信息。
- **不标记** — 从下拉列表中选择**不标记**可取消端口标记。
 - **标记** — 从下拉列表中选择**标记**可将端口添加为所选 VLAN 的成员。从这一指向所选 VLAN 的端口发送的数据包将具备 VLAN ID 标记。如果端口上没有非标记的 VLAN，接口将自动加入 VLAN1。
 - **排除** — 从下拉列表中选择**排除**可将端口从所选 VLAN 中排除。从端口排除非标记 VLAN 后，端口会自动加入默认的 VLAN。
- 步骤 9** 单击**应用**。
-

LAN/DHCP 设置

DHCP 设置为中继配置 DHCP 服务器，或为 LAN 客户端配置选项 82（DHCP 中继代理信息选项），以获取 IP 地址。DHCP 服务器维持本地池和租用。它还允许 LAN 客户端连接到远程服务器以获取 IP 地址。

利用选项 82，DHCP 中继代理在将客户端发起的 DHCP 数据包转发至 DHCP 服务器时，可以包含有关自身的信息。DHCP 服务器可以使用此信息实施 IP 寻址或其他参数分配策略。

要配置 LAN/DHCP 设置，请按照以下步骤操作：

-
- 步骤 1** 选择 **LAN > LAN/DHCP 设置**。
- 步骤 2** 在“LAN/DHCP 设置表”中，单击**添加**。
- 步骤 3** 如果选择**接口**，请从下拉列表中选择一个 VLAN，并单击**下一步**。
- 步骤 4** 要为 IPv4 配置 DHCP，请为 IPv4 选择 DHCP 类型。

已禁用	在该设备上为 IPv4 禁用 DHCP 服务器。不需要填写其他参数。
服务器	DHCP 服务器将地址分配给对应池中的客户端。

中继	通过设备发送 DHCP 请求和其他 DHCP 服务器的回复。输入远程 DHCP 服务器 IPv4 地址以配置 DHCP 中继代理。
----	---

为 IPv4 配置 DHCP

步骤 5 单击下一步，并配置以下设置：

客户端租用时间	网络用户可以使用当前 IP 地址连接到路由器的时间（以分钟为单位）。有效值为 5 至 43,200 分钟。默认为 1440 分钟（即 24 小时）。
范围起始值和范围结束值	可以动态分配 IP 地址的范围起始值和结束值。该范围内的 IP 地址数可以达到服务器在不覆盖 PPTP 和 SSL VPN 时能够分配的最大数目。
DNS 服务器	DNS 服务类型；在此可获取 DNS 服务器 IP 地址。
静态 DNS 1 和静态 DNS 2	DNS 服务器的静态 IP 地址。（可选）如果输入第二个 DNS 服务器，设备将使用第一个 DNS 服务器响应请求。
WINS 服务器	Windows 互联网命名服务 (WINS) 服务器的可选 IP 地址，用于将 NetBIOS 名称解析为 IP 地址。默认为 0.0.0.0。
DHCP 选项	<ul style="list-style-type: none"> • 选项 66 — 输入单个 TFTP 服务器的 IP 地址或主机名。 • 选项 150 — 输入一系列 TFTP 服务器的 IP 地址。 • 选项 67 — 输入启动文件名。

为 IPv6 配置 DHCP 类型

步骤 6 要为 IPv6 配置 DHCP 模式，请输入以下信息：

禁用	在该设备上禁用 DHCP。不需要填写其他参数。
服务器	该 DHCP 服务器将地址分配给对应池中的客户端。

步骤 7 单击下一步，并配置以下设置：

客户端租用时间	网络用户可以使用当前 IP 地址连接到路由器的时间。输入时间（以分钟为单位）。有效值为 5 至 43,200 分钟。默认为 1460 分钟（24 小时）。例如，如果路由器使用默认的 LAN IP 地址 192.168.1.1，则起始值必须为 192.168.1.2 或更大。
范围起始值	IPv6 地址池的起始地址。
范围结束值	IPv6 地址池的结束地址。
DNS 服务器	ISP 提供的 DNS（服务器静态）、代理或 DNS 服务器的类型。

静态 DNS1 和 DNS2	(可选) DNS 服务器的 IP 地址。如果输入第二个 DNS 服务器, 设备将使用第一个 DNS 服务器进行响应。与使用动态分配的 DNS 服务器相比, 指定 DNS 服务器可以提供更快的访问速度。默认为 0.0.0.0。
-----------------------	--

配置选项 82 电路

步骤 8 若要配置选项 82 电路, 请输入以下信息。

说明	输入选项 82 客户端的说明。
电路 ID	加强验证安全, 以确定选项 82 电路 ID 中提供的信息。输入电路 ID 及其格式。

步骤 9 单击下一步, 并输入以下信息:

IP 地址和子网掩码	输入设备的 IP 地址和子网掩码。
-------------------	-------------------

步骤 10 单击下一步。

步骤 11 要添加新的 DHCP 配置, 请配置以下设置:

客户端租用时间	网络用户可以使用当前 IP 地址连接到路由器的时间。输入时间 (以分钟为单位)。有效值为 5 至 3200 分钟。默认为 1460 分钟 (24 小时)。
范围起始值和范围结束值	可以动态分配 IP 地址的范围起始值和结束值。该范围内的 IP 地址数可以达到服务器在不覆盖 PPTP 和 SSL VPN 时能够分配的最大数目。例如, 如果路由器使用默认的 LAN IP 地址 192.168.1.1, 则起始值必须为 192.168.1.2 或更大。
DNS 服务器	DNS 服务类型; 在此可获取 DNS 服务器 IP 地址。
静态 DNS 1 和静态 DNS 2	DNS 服务器的静态 IP 地址。(可选) 如果输入第二个 DNS 服务器, 设备将使用第一个 DNS 服务器响应请求。
WINS 服务器	Windows 互联网命名服务 (WINS) 服务器的可选 IP 地址, 用于将 NetBIOS 名称解析为 IP 地址。默认为 0.0.0.0。
DHCP 选项	<ul style="list-style-type: none"> • 选项 66 — 输入单个 TFTP 服务器的 IP 地址或主机名。 • 选项 150 — 输入一系列 TFTP 服务器的 IP 地址。 • 选项 67 — 输入启动文件名。

步骤 12 单击确定, 然后单击应用。

静态 DHCP

利用静态 DHCP，可使用指向定义的 MAC 的 IPv4 地址。

要配置静态 DHCP，请按照以下步骤操作：

-
- 步骤 1 选择 LAN > 静态 DHCP。
 - 步骤 2 单击添加。
 - 步骤 3 在“静态 DHCP 表”中，在“名称”字段中输入名称。
 - 步骤 4 在相应的字段中输入 IPv4 地址和 MAC 地址。
 - 步骤 5 选中启用。
 - 步骤 6 单击应用。
-

802.1X 配置

IEEE 802.1X 基于端口的验证可防止未经授权的设备（客户端）访问网络。该网络访问控制使用 IEEE 802 LAN 基础设施的物理访问特性，对连接到 LAN 端口（具有点对点连接特性）的设备进行验证和授权。在此环境中，一个端口是 LAN 基础设施的一个单独连接点。

设备支持多主机模式。在该模式下，在连接的主机中，只需一台主机成功获得授权，所有主机即可获得网络访问权限。如果端口未经授权（重新授权失败或收到了 EAPOL-logoff 消息），系统将拒绝所有连接的客户端访问网络。

配置基于端口的验证的步骤：

-
- 步骤 1 选择 LAN > 802.1X 配置。
 - 步骤 2 选中启用基于端口的验证以启用该功能。
注释 802.1X 要求使用 RADIUS 进行验证。确保在用户帐户，第 31 页中定义了 RADIUS 服务器。
 - 步骤 3 从“802.1X 配置表”的下拉列表中选择“管理状态”。
 - 强制授权 — 无需授权。必须强制为至少一个 LAN 端口授权。
 - 自动 — 启用基于端口的验证。接口根据设备与客户端之间的验证交换在授权状态和未经授权状态之间转换。
 - 步骤 4 单击应用。
注释 在启用基于端口的验证之前，确保相应的配置处于活动状态且正确无误。
-

DNS 本地数据库

一种本地域名服务 (DNS) 服务器，用于加速的 DNS 服务响应。DNS 将域名与其可路由 IP 地址进行匹配。对于常用域名，相比于使用外部 DNS 服务器，使用 DNS 本地数据库充当本地 DNS 服务器可以更快给出结果。如果请求的域名不在本地数据库中，则该请求将转发至在“设置”页面上指定的 DNS 服务器。

要配置 DNS 本地数据库，请按照以下步骤操作：

-
- 步骤 1 选择 LAN > DNS 本地数据库。
 - 步骤 2 单击添加，并输入主机名和 IPv4 或 IPv6 地址。您还可以编辑或删除 DNS。
 - 步骤 3 单击应用。
-

路由器通告

路由器通告常驻程序 (RADVD) 用于定义接口设置、前缀、路由和通知。主机依靠其本地网络中的路由器来实现与其他所有主机（本地网络中的主机除外）的通信。路由器定期发送并响应路由器通告消息。通过启用此功能，消息会由路由器定期发送并响应请求。主机使用该信息了解本地网络的前缀和参数。禁用此功能可以有效禁用自动配置，需要在每台设备上手动配置 IPv6 地址、子网前缀和默认网关。

要配置路由器通告，请按照以下步骤操作：

-
- 步骤 1 选择 LAN > 路由器通告。
 - 步骤 2 从下拉列表中选择 VLAN ID。
 - 步骤 3 选中启用以启用路由器通告，然后配置以下设置：

通告模式	从下拉列表中选择通告模式（单播或主动提供的组播）。
通告间隔	输入发送路由器通告消息的时间间隔（介于 10 至 1800 之间，默认为 30 秒）。

RA 标签	<p>确定主机是否可以使用 DHCPv6 获取 IP 地址和相关信息。选择并选中以下选项之一：</p> <ul style="list-style-type: none"> • 管理型 — 主机使用管理型、有状态的配置协议 (DHCPv6) 通过 DHCPv6 获取有状态的地址和其他信息。 • 其他 — 使用管理型、有状态的配置协议 (DHCPv6) 获取其他非地址信息，例如 DNS 服务器地址。
路由器偏好	<p>多宿主主机有权访问多个路由器的网络拓扑中使用的偏好度量标准。路由器偏好有助于主机选择合适的路由器。有三种偏好可供选择，即高、中或低。默认设置为“高”。从下拉列表中选择偏好。</p>
最大传输单位 (MTU)	<p>MTU 是可在网络中发送的最大数据包的大小。它用于路由器通告消息中以确保在 LAN MTU 未众所周知时网络上的所有节点都使用相同的 MTU 值。默认设置为 1500 字节，这是以太网的标准值。对于 PPPoE 连接，标准值为 1492 字节。除非 ISP 要求进行其他设置，否则不应更改此设置。输入介于 1280 与 1500 之间的值。</p>
路由器有效期限	<p>输入路由器通告消息在路由上存在的时间（以秒为单位）。默认值为 3600 秒。</p>

步骤 4 在“前缀表”中，单击添加并输入前缀的名称。

步骤 5 在“前缀长度和有效期限”字段中输入前缀长度和有效期限。

步骤 6 单击应用。



第 8 章

无线

无线局域网 (WLAN) 是一种无线分布技术，该技术以高频无线电波为媒介构建灵活的数据通信系统，通常会使用无线接入点来实现互联网连接。此技术通常用于扩展（而不是取代）建筑物或园区内的有线局域网。由于无线局域网使用射频技术发送和接受数据，所以此类网络无需使用有线连接。只要是在信号覆盖区域内，即使用户四处移动，也能始终保持网络连接。

本节介绍无线局域网，这是一种典型的本地局域网，通过高频无线电波（而非有线连接）在节点之间进行通信。本节包含以下主题：

- [基本设置](#)，第 63 页
- [高级设置](#)，第 68 页
- [Captive Portal](#)，第 69 页
- [WPS](#)，第 71 页

基本设置

RV340W 可提供无线局域网 (WLAN) 功能，所有端口（LAN 端口和 WLAN 端口）均在单一广播域中。此路由器支持 802.11ac 标准，可同时选择 2.4 GHz 和 5 GHz 两个频段。根据选择的无线电类型，您可以选择 WLAN 网络发送和接收数据的频率或通道。为每个无线电选择合适的通道宽度有助于提高 WLAN 的吞吐量。

在“基本设置”中，您可以添加、编辑或删除无线 SSID 设置，也可以选择并配置无线电通道。您最多可以为每个无线电添加 4 个独立的虚拟无线网络。也就是说，您最多只能添加 8 个 SSID（每个无线电 4 个 SSID）。达到此上限后，“添加”按钮将变成灰色。

要配置无线 SSID 设置，请按照以下步骤操作：

- 步骤 1** 选择无线 > 基本设置。
- 步骤 2** 在“无线表”中，单击添加或编辑。
- 步骤 3** 然后在“添加/编辑无线 SSID 设置”页面中配置以下设置：

SSID 名称	此项用于指定网络的名称。
启用	选中启用可启用对应的网络。
主动应用于无线电	选择 2.4G 或 5G 频段，可在网络设置和所选频段都满足条件的情况下，将网络连接到所选频段。系统将在所选的无线电频段中创建此 SSID。选择 两者 可将此 SSID 同时配置到两个无线电频段，并将此配置文件关联到具有相应网络设置的可用网络。
SSID 广播	如果您希望某个范围内的无线客户端在扫描可用网络时能够检测到此无线网络，可选中此项，以启用 SSID 广播。如果您不希望此 SSID 可被发现，请禁用此功能。如果禁用此项，无线客户端只有在提供 SSID 和所需安全凭证的情况下，才能连接到您的无线网络。
安全模式	<p>此项用于为网络选择安全模式，可用选项如下：</p> <ul style="list-style-type: none"> • WEP-64：如果您使用不支持 WPA 或 WPA2 安全模式的旧型设备，可选择 64 位 WEP 安全模式，然后输入 WEP 密钥。WEP 密钥应由 10 个十六进制字符组成。 • WEP-128：如果您使用不支持 WPA 或 WPA2 安全模式的旧型设备，可选择 128 位 WEP 安全模式，然后输入 WEP 密钥。WEP 密钥应由 26 个十六进制字符组成。 • WPA2-个人：选择 Wi-Fi 保护访问第 II 版 (WPA2) 安全协议可获得更强的安全保护。如果选择此项，您需要输入一个字母数字式密码。 • WPA-WPA2-个人：如果您同时允许 WPA 和 WPA2 客户端连接到您的无线网络，选择此协议可以获得更强的安全保护。如果选择此项，您需要输入一个字母数字式密码。 • WPA2-企业：选择此安全协议可使用 RADIUS 服务器身份验证。若选择此项，请指定以下值： <ul style="list-style-type: none"> RADIUS 服务器 IP 地址（用于处理客户端身份验证的 RADIUS 服务器的 IP 地址）。 RADIUS 服务器端口（用于访问 RADIUS 服务器的端口）。 RADIUS 密码（共享的 RADIUS 密码）。 • WPA-WPA2-企业：如果您同时允许 WPA 和 WPA2 客户端连接到您的无线网络，选择此协议可以使用 RADIUS 服务器进行身份验证。如果选择此项，您需要指定“RADIUS 服务器 IP 地址”、“RADIUS 服务器端口”和“RADIUS 密码”。

PMF	<p>1 如果“安全模式”设置为“无”，则“PMF”会自动设置为不需要，并会显示为灰色（不可编辑）。</p> <p>2 如果“安全模式”设置为“WPA2-XXX”，则“PMF”默认设置为能够。</p> <ul style="list-style-type: none"> • 此默认值可以编辑 — 用户可以将其设置为不需要或需要。 • 如果“安全模式”设置为“WPA-XXX”且“PMF”设置为能够，在进行保存时，系统可能会弹出警告，例如“PMF已启用。但是，一些无线客户端可能无法与PMF完全兼容，并存在不稳定的问题。” <p>注释 要设置PMF配置选项，请参阅下面的PMF表。</p>
使用 SSID 进行无线隔离	选中 启用 可在 SSID 中启用无线隔离。启用无线隔离后，连接到同一 SSID 的无线客户端将无法相互可见或相互通信。
WMM	要根据接入类别 (AC) 确定流量的优先级并对流量进行排队，请选中 启用 以启用无线多媒体扩展 (WME)。启用 WME 可以实现更高效的吞吐量，但是在杂乱的无线电频率 (RF) 环境下可能会出现较高的错误率。
WPS	选中“ 启用 ”可启用 Wi-Fi 保护设置 (WPS)。此项最多支持两种使用模式：“PIN”和“Push Button”。如果启用此项，请单击 配置 ，然后在弹出窗口中设置 WPS 参数。有关配置 WPS 的详细信息，请参阅 WPS，第 71 页 。
VLAN	此项用于指定 SSID 所需映射到的 VLAN ID。连接到此网络的设备将被分配此 VLAN 中的地址。默认 VLAN ID 为 1，如果所有设备都在同一个网络中，您可以无需更改此设置。
关联的最大客户端数	<p>此项用于指定可以同时关联的最大客户端数（对于 2.4G 频段，默认值为每个 SSID 50 个；对于 5G 频段，默认值为每个 SSID 124 个）。</p> <p>注释 所有启用的 SSID 所配置的“关联的最大客户端数”总数不应超过 50 个客户端 (2.4G) 或 124 个客户端 (5G)（如果启用 MU-MIMO，则不应超过 128）。</p>
访问时刻	此项用于指定 SSID 可用的时间段，如果要使 SSID 仅在每天的特定时刻或每周的特定日期可用，可以使用此设置。您还可以指定用户可以访问网络的时间，以限制对网络的访问，从而进一步保护您的网络。
MAC 过滤	通过使用 MAC 过滤，您可以根据请求设备的 MAC（硬件）地址来允许或拒绝访问无线网络。选中“ 启用 ”可以为相应的 SSID 启用 MAC 过滤。如果启用此项，请单击 配置 ，为无线网络指定 MAC 黑名单（禁止访问网络的设备）和白名单（允许访问网络的设备）。

Captive Portal	选中“启用”可以为 SSID 启用 Captive Portal 验证。如果启用此项，您需要从下拉列表中选择门户配置文件。您也可以单击 新建 ，自行配置一个新的配置文件。有关添加新的 Captive Portal 配置文件的详细信息，请参阅 Captive Portal ，第 69 页。
-----------------------	---

表 2: PMF 表

无线接入点设置	客户端设置	结果	是否安全
不需要	不需要	不使用 PMF 连接	
不需要	能够	不使用 PMF 连接	
不需要	Required	无连接	
能够	不需要	不使用 PMF 连接	
能够	能够	使用 PMF 连接	
能够	需要	使用 PMF 连接	
需要	不需要	无连接	
需要	能够	使用 PMF 连接	
需要	需要	使用 PMF 连接	

配置 2.4 GHz 无线电

路由器支持双频功能（2.4 GHz 和 5 GHz），您可以选择启用或禁用此功能。您还可以指定每个频段的通道数，或选择**自动通道选择**。这些设置将应用到所有虚拟无线网络。根据选择的无线电频段，

WLAN 网络会以特定频率（或所选通道）收发数据。为每个无线电选择合适的通道宽度有助于提高 WLAN 的吞吐量。

要配置并发通道选择参数，请按照以下步骤操作：

配置 2.4 GHz 无线电

-
- 步骤 1** 单击**无线 > 基本设置 > 2.4G**。
- 步骤 2** 单击**无线电**启用 2.4 GHz 频段。
- 步骤 3** 从“无线网络模式”下拉列表中，选择网络频段模式（“仅 B”、“仅 G”、“仅 N”、“B/G 混合”、“G/N 混合”或“B/G/N 混合”）。
- 步骤 4** 单击 **20 MHz** 或 **20/40 MHz**，选择通道宽度。
- 步骤 5** 单击“较低”或“较高”单选按钮，选择主通道。
注释 如果您在步骤 4 中选择了 **20 MHz 带宽**，或者从下拉列表中选择了**自动**，则无法选择主通道。
- 步骤 6** 从下拉列表中选择适当的无线通道。您可以选择**自动**，让系统来选择通道。
如果您选择**较低**作为主通道设置，则可以选择的通道范围为 1 至 7。如果您选择**较高**，则可以选择的通道范围为 5 至 11。
- 步骤 7** 要启用“非调度自动节能发送” (U-APSD) 模式，并允许连接的客户端使用 U-APSD 功能达到节能目的，请选中**U-APSD (WMM 节能)**。此设置可以使用 802.11e 和传统 802.11 提供的机制调整能耗，实现节能。
- 步骤 8** 单击**应用**。
-

配置 5 GHz 无线电

要配置 5 GHz 无线电，请按照以下步骤操作：

-
- 步骤 1** 单击**无线 > 基本设置 > 5G**。
- 步骤 2** 单击**无线电**启用 5 GHz 频段。
- 步骤 3** 从“无线网络模式”下拉列表中，选择网络频段模式（“仅 A”、“N/AC 混合”或“A/N/AC 混合”）。
- 步骤 4** 单击 **20 MHz**、**40 MHz** 或 **80 MHz**单选按钮，选择通道宽度。
- 步骤 5** 单击**较低**或**较高**，选择主通道。
注释 只有在选择 40 MHz 带宽的情况下，才能选择主通道。

- 步骤 6** 从下拉列表中选择适当的无线通道。您可以选择**自动**，让系统来选择通道。
- 步骤 7** 如果设备支持省电功能，而且您希望启用“非调度自动节能发送”(U-APSD)模式，请选中**U-APSD (WMM 节能)**。
- 步骤 8** 选中**多用户 MIMO**启用此功能。多用户多输入多输出(MIMO)功能可以在 5G 频段上同时支持最多 4 个平行组。
- 步骤 9** 单击**应用**。

高级设置

您可以为每个无线电设定高级设置，例如“帧突发”、“WMM 无确认”、“基本速率”、“传输速率”、“DTIM 间隔”、“RTS 阈值”等。

要配置“无线”选项下的高级设置，请按照以下步骤操作：

- 步骤 1** 依次单击**无线 > 高级设置 > 2.4G 或 5G 选项卡**。

- 步骤 2** 配置以下设置：

帧突发	选中 启用 可允许以最小帧间隔发送多个帧，从而提高网络效率并减少系统开销。
WMM 无确认	选中 启用 可实现较高的吞吐量。但是在干扰较多的射频 (RF) 环境下，启用此项会导致错误率上升。
数据速率	对于“数据速率”，单击 设置为默认值 为“基本速率”和“传输速率”选择默认值。
基本速率	选择“基本速率”设置 — 服务准备平台可以达到的传输速率。设备会向网络中的其他无线设备通告它的基本速率，以确保其他无线设备了解所要使用的速率。服务准备平台也会通告它将自动选择传输的最佳速率。
传输速率	选择“传输速率”设置 — 根据无线网络速度决定的数据传输速率。
CTS 保护模式	“允许发送”(CTS)保护模式是 802.11 无线网络协议使用的一种机制，可减少由于隐藏节点问题导致的帧冲突。默认情况下，此项设置为 自动 。要禁用此项，请单击 禁用 。
信标间隔	此项用于指定信标间隔（信标传输活动的时间间隔），单位为毫秒。信标是一种由设备广播的数据包，用于与无线网络同步节点（如无线接入点）必须发送信标的时间（也称为“目标信标传输时间”或“TBIT”）。信标间隔以“时间单位”(TU)表示，可设置的范围介于 40 至 3500 毫秒之间，默认值为 100。

DTIM 间隔	此项用于指定“发送流量指示图”(DTIM)间隔。此设置可通知客户端无线接入点中存在缓冲的组播/广播数据。这些数据包含在按 DTIM 间隔指定的频率定期生成的信标中。可设置的范围介于 1 至 255 之间，默认值为 1。
分片阈值	此项用于输入“分片阈值”，此值指定在数据分为多个数据包之前的最大数据包大小。在数据包错误率较高的情况下，可以稍微增大“分片阈值”。将“分片阈值”设置得过低可能会导致网络性能变差。可设置的范围介于 256 至 2346 之间，默认值为 2346。
RTS 阈值	“RTS 阈值”字段用于输入“请求发送”(RTS)的阈值大小。如果网络数据包小于指定的阈值大小，则 RTS/CTS 机制不会启用。可设置的范围介于 0 至 2347 之间，默认值为 2347。
发射功率	此项用于在“发射功率”下拉列表中选择所要发送(Tx)的数据量。

步骤 3 选择所需值后，单击应用。

Captive Portal

Captive Portal 功能为客户端提供经过验证且受控的网络资源访问权限，而且不会影响安全性。换言之，连接到 WLAN 接口的客户端在获得授权之前，会被限制在一个“围墙花园”内。Captive Portal 会显示一个特殊网页，用于对客户端进行身份验证，然后客户端才能使用互联网。不过，客户端可以解析 DNS，并通过 Web 浏览器访问专门添加到该“围墙花园”的网站。身份验证通过用于发起身份验证的 Captive Portal 进行。如果未经过身份验证的客户端试图连接到某个网页（在端口 80），守护进程会拦截该请求，并将其重定向到 Captive Portal（UI 端口）。

您可以在设备中针对每个虚拟无线网络配置 Captive Portal，只需将虚拟无线网络与门户配置文件关联即可。您还可以通过选择**状态和统计信息 > Captive Portal 状态**，来查看 Captive Portal 的状态。有关如何启用 Captive Portal 配置文件的说明，请参阅**基本设置，第 63 页**。

要创建 Captive Portal 配置文件，请按照以下步骤操作：

步骤 1 单击无线 > Captive Portal。

步骤 2 在“Captive Portal”页面中，单击“门户配置文件表”底部的添加。要修改现有门户配置文件，请选中相应的复选框，然后单击编辑。

步骤 3 在“添加 Captive Portal 配置文件”页面中，配置以下设置：

配置文件名称	输入新 Captive Portal 配置文件的名称。
身份验证	选择是启用（身份验证）或禁用（无身份验证）身份验证。

更改用户登录请求，重定向到	可以选择原始 URL，也可以选择新 URL 并在文本字段输入一个 URL，以便在完成身份验证后将用户重定向到该 URL。
空闲超时	设置身份验证的有效时间，单位为秒，范围介于 0-1440 之间。0 表示时间无限。

步骤 4 在“门户页面自定义”部分，配置以下设置：

字体颜色	从下拉列表中为页面上显示的文本选择一种字体颜色。
背景图片	单击 选择文件 ，然后选择一张图像作为门户页面显示的背景图片。
公司名称	指定所要显示的公司名称。
公司徽标图片	单击 选择文件 ，然后选择所要显示的公司徽标图像。
欢迎消息	输入登录时显示的欢迎消息。
用户名字段	输入用户名字段显示的文本。
密码字段	输入密码字段显示的文本。
登录按钮名称	输入登录按钮上显示的文本。
版权信息	输入与公司关联的标准版权文本。
身份验证失败时的错误消息	输入登录失败时显示的错误消息。
超过最大客户端数时的错误消息	输入在超过最大连接数量时显示的消息文本。
显示协议	选中 显示协议 可提示用户接受使用协议。
协议标题	输入协议文本的标题。
协议内容	输入所要显示的协议条款。

步骤 5 单击**应用**。

如需预览此配置文件，请单击**预览**。要针对特定用户帐户启用 Captive Portal，请选择**系统配置 > 用户帐户**以及**系统配置 > 用户组**。

WPS

Wi-Fi 保护设置 (WPS) 是一种网络安全功能，可使支持 WPS 的客户端轻松且安全地连接到无线网络。您可以通过 3 种方式连接到支持 WPS 的无线网络：WPS Push Button、客户端设备的 WPS PIN 号码，以及在 WPS 配置页面生成的设备 PIN 号码。

要配置 WPS，请执行以下操作：

-
- 步骤 1** 依次单击**无线 > WPS**。系统将显示“Wi-Fi 保护设置”页面。
- 步骤 2** 从 WPS 下拉列表中选择 SSID（需要配置 WPS 的网络对应的 SSID）。
- 步骤 3** 从“无线”下拉列表中选择无线电频段（“**2.4G**”、“**5G**”或“**两者**”）。
- 步骤 4** 采用以下三种方式中的一种，在客户端设备上配置 WPS：
- a) 在客户端上单击 **WPS**，然后在此 WPS 配置页面中单击 **WPS**。
 - b) 如果客户端设备具有 WPS PIN 号码，则在配置页面的文本字段中输入该号码，然后单击**注册**。
 - c) 如果客户端设备需要使用路由器提供的 PIN 号码，则单击**生成**，然后在客户端中输入生成的 PIN 号码。在“PIN 有效期限”字段中，选择所需的密钥有效期限。如果有效期限到期，系统将协商新的密钥。
- 完成上述步骤后，即可完成 WPS 配置。
-



第 9 章

路由

本节介绍路由，即在网络中选择最佳路径的过程。动态路由是一种提供最佳数据路由的联网技术。利用动态路由，路由器可以根据逻辑网络布局的实时变化选择路径。路由器的路由协议负责在动态路由过程中创建、维护和更新动态路由表。本节包含以下主题：

- [IGMP 代理，第 73 页](#)
- [RIP，第 74 页](#)
- [静态路由，第 75 页](#)

IGMP 代理

互联网组管理协议 (IGMP) 供 IP 网络上的主机和路由器用于创建组播组成员身份。IGMP 可用于 Web 资源，并为在线视频流和游戏流等应用提供支持。利用 IGMP 代理，路由器可以代表背后的客户端发出 IGMP 消息。

要启用 IGMP 代理，请按照以下步骤操作：

- 步骤 1** 选择常规 > IGMP 代理。
- 步骤 2** 选中启用 **IGMP 代理**，以允许路由器与节点彼此通信。
- 步骤 3** 从下拉列表中选择上游接口。

- **WAN 自动** — 路由器可以支持多 WAN。如果选择 WAN 自动模式，路由器将选择活动的 WAN 作为上游端口。如果多 WAN 已启用并以负载平衡模式工作，则端口号最小的 WAN 端口将是上游端口。例如，如果 WAN1 和 WAN2 处于负载平衡模式，那么 WAN1 将是上游端口。如果 WAN1 断开，WAN2 将成为上游端口。
- **固定接口** — 固定接口将始终使用选定端口作为上游端口（即使已经断开）。例如，如果 WAN1 和 WAN2 处于负载平衡模式，而您选择 WAN2 作为上游端口，那么 WAN1 将不接收组播流量，无论 WAN2 处于连接还是断开状态。如果选择**固定接口**，还请确保选择了 **WAN 1、WAN 2 或 VLAN1**。

步骤 4 选择“下游接口”WAN 或 VLAN1。

步骤 5 单击应用。

RIP

路由信息协议 (RIP) 是在局域网 (LAN) 中使用的标准 IGP（内部网关协议）。如果一个网络连接离线，RIP 可以迅速重新路由网络数据包，从而确保更高的网络稳定性。RIP 处于活动状态时，只要有足够的可用网络资源，用户就几乎或完全不会遇到因单个路由器、交换机或服务器故障导致的服务中断。

要配置 RIP，请按照以下步骤操作：

步骤 1 选择路由 > RIP。

步骤 2 要启用 RIP，请选中 **Ipv4** 或 **Ipv6** 或同时选中，然后配置以下设置：

接口	在相应的接口中选中 启用 以接收来自上游的路由。 注释 为接口选中 启用 会自动为该接口选中 RIP 第 1 版、RIP 第 2 版、RIPng (Ipv6) 和验证。反之，取消选中 启用 会取消选中全部设置。
RIP 第 1 版	此协议使用有类路由，不包含子网信息或验证。 <ul style="list-style-type: none">选中启用可在 RIP 第 1 版上启用发送和接收路由信息。选中被动可在 RIP 第 1 版上禁用发送路由信息。 注释 仅当选中 启用 时才可激活被动配置。
RIP 第 2 版	这是一种使用组播并具有密码验证的无类协议。 <ul style="list-style-type: none">选中启用可在 RIP 第 2 版上启用发送和接收路由信息。选中被动可在 RIP 第 2 版上禁用发送路由信息。 注释 仅当选中 启用 时才可激活被动配置。
RIPng (IPv6)	下一代路由信息协议 (RIPng) 使用用户数据报数据包 (UDP) 发送路由信息。它基于 RIP 第 2 版，但用于 IPv6 路由。 <ul style="list-style-type: none">选中启用可启用 RIP Ipv6 路由。选中被动可禁用发送 RIPng 版本。 注释 仅当选中 启用 时才可激活被动配置。

验证	<p>此安全功能在与其他路由器交换路由之前强制验证 RIP 数据包。此功能不可用于 RIPv1。</p> <ul style="list-style-type: none"> 选中启用可启用验证，从而仅与网络中受信任的路由器交换路由。 密码：选择验证类型 — 明文（常用的验证方法）或 Md5（质询-响应验证机制） — 并输入密码。
----	--

步骤 3 单击**应用**。

静态路由

静态路由是手动配置的固定路径，是数据包到达目标位置的必经之处。如果当前网络拓扑上的路由器之间没有进行通信，那么静态路由可以配置为在路由器之间进行通信。与动态路由相比，静态路由占用的网络资源较少，因为静态路由不会不断计算下一次要进行的路由。

要配置静态路由，请按照以下步骤操作：

步骤 1 依次选择**路由 > 静态路由**。

步骤 2 对于 IPv4 路由，请在“路由表”中单击**添加**或**编辑**，并配置以下内容：

网络	输入您要向其分配静态路由的目标子网 IP 地址。
掩码	输入目标地址的子网掩码。
下一步跳	输入最后选择的路由器的 IP 地址。
度量标准	“度量标准”字段中的值表示网络和目标设备之间的路由器数量。此为直接连接，因此可以将其设置为最小值：1。
接口	从下拉列表中选择要用于此静态路由的接口。

步骤 3 完成设置后，单击**应用**。

步骤 4 对于 IPv6 路由，请在“路由”表中单击**添加**或**编辑**，并配置以下内容：

前缀	输入 IPv6 前缀。
长度	输入 IP 地址的前缀位数。
下一步跳	输入最后选择的路由器的 IP 地址。

度量标准	“度量标准”字段中的值表示网络和目标设备之间的路由器数量。此为直接连接，因此可以将其设置为最小值：1。
接口	从下拉列表中选择要用于此静态路由的接口。

步骤 5 单击应用。



第 10 章

防火墙

本节介绍防火墙，这是一种旨在防御入侵者攻击，确保网络安全的方法。防火墙会检查流量，并过滤不符合指定安全条件的传输。防火墙能决定允许或拒绝哪些数据包进出网络。本节包含以下主题：

- [基本设置](#)，第 77 页
- [访问规则](#)，第 78 页
- [网络地址转换](#)，第 80 页
- [静态 NAT](#)，第 80 页
- [端口转发](#)，第 81 页
- [端口触发](#)，第 82 页
- [会话超时](#)，第 83 页
- [DMZ 主机](#)，第 84 页

基本设置

在“基本设置”页面上，您可以启用和配置基本设置。您还可以将受信任的域添加到该列表中。要配置基本设置，请按照以下步骤操作：

步骤 1 单击“防火墙”>“基本设置”，输入以下信息：

防火墙	选中“启用”可启用防火墙设置；取消选中启用可禁用。
DoS（拒绝服务）	选中启用可启用 DoS。DoS 可阻止 Ping 炸弹、SYN 泛洪检测率 [最大数/秒]、IP 欺骗、回音风暴、ICMP 泛洪、UDP 泛洪和 TCP 泛洪攻击。
阻止 WAN 请求	选中启用可阻止对 WAN 的 ICMP 回音请求。

LAN/VPN Web 管理	选择 HTTP 或 HTTPS。
远程 Web 管理	选中启用启用远程 Web 管理，并输入端口号（默认值为 443，范围为 1025-65535）。 • 选择 HTTP 或 HTTPS。
允许的远程 IP 地址	选中任意 IP 地址或输入远程访问的 IP 地址范围。
SIP ALG（会话初始化协议应用层网关）	选中启用以允许 SIP ALG。这会嵌入流经具有网络地址转换 (NAT) 功能的已配置设备，从而经过转换并编码为数据包的 SIP 消息。该应用层网关 (ALG) 与 NAT 一起，用于转换 SIP 或会话描述协议 (SDP) 消息。
FTP ALG 端口	输入端口号。默认值为 21。FTP ALG 端口转换 FTP 数据包。
UPnP（通用即插即用）	选中启用可启用通用即插即用。
限制 Web 功能	选中可限制下列 Web 功能： • Java: 阻止 Web Java 功能。 • Cookies: 阻止 Cookies。 • ActiveX: 阻止 ActiveX。 • 访问 HTTP 代理服务器: 阻止 HTTP 代理服务器。
例外情况	选中启用将只允许选定的 Web 功能（例如，Java、Cookies、ActiveX 或“访问 HTTP 代理服务器”）并限制所有其他功能。

步骤 2 在受信任的域表中，选中域名以编辑现有域设置。

步骤 3 单击添加、编辑或删除以添加、编辑或删除域。

步骤 4 单击应用。

访问规则

要配置访问规则，请按照以下步骤操作：

步骤 1 选择防火墙 > 访问规则。在访问规则表中，输入以下信息：

步骤 2 单击添加或选择相应行，然后单击编辑，并输入以下信息：

规则状态	选中启用可启用特定访问规则。取消选中可禁用。
------	------------------------

操作	从下拉列表中选择 允许或拒绝 。
服务	<ul style="list-style-type: none"> • IPv4 — 选择要应用 IPv4 规则的服务。 • IPv6 — 选择要应用 IPv6 规则的服务。 • 服务 — 从下拉列表中选择服务。
日志	<p>从下拉列表中选择真或从不。</p> <ul style="list-style-type: none"> • 真 — 符合规则。 • 从不 — 无需日志。
源接口	从下拉列表中选择源接口（ WAN1、WAN2、USB1、USB2、VLAN1 或“任意”）。
源地址	<p>选择要应用规则的源 IP 地址并输入以下信息：</p> <ul style="list-style-type: none"> • 任意 • 单一 IP — 输入一个 IP 地址。 • IP 范围 — 输入 IP 地址的范围。 • 子网 — 输入网络的子网。
目标接口	从下拉列表中选择源接口（ WAN1、WAN2、USB1、USB2、VLAN1 或“任意”）。
目的地址	<p>选择要应用规则的源 IP 地址并输入以下信息：</p> <ul style="list-style-type: none"> • 任意 • 单一 IP — 输入一个 IP 地址。 • IP 范围 — 输入 IP 地址的范围。 • 子网 — 输入网络的子网。
计划表名称	从下拉列表中选择 商务、夜间、营销或工作 ，以应用防火墙规则。然后，单击链接以配置计划表。

- 步骤 3** 单击**应用**。
- 步骤 4** 单击**恢复为默认规则**以恢复默认规则。
- 步骤 5** 单击**服务管理**以配置服务。
- 步骤 6** 要添加服务，请单击**添加**。要编辑或删除服务，请选择相应行并单击**编辑**或**删除**。
- 步骤 7** 配置以下设置：
- **应用名称** — 服务或应用的名称。
 - **协议** — 所需协议。请参阅您托管的服务的相关文档。
 - **起始端口/ICMP 类型/IP 协议** — 为此服务预留的端口号范围。
 - **结束端口** — 为此服务预留的最后一个端口号。
- 步骤 8** 单击**应用**。
-

网络地址转换

通过网络地址转换 (NAT)，使用未注册 IP 地址的专用 IP 网络可以连接网络。在数据包被转发至公共网络之前，NAT 会将内部网络的专用地址转换为公共地址。

要配置 NAT，请按照以下步骤操作：

- 步骤 1** 单击**防火墙 > 网络地址转换**。
- 步骤 2** 在 **NAT** 表中，为接口列表中的每个接口选中**启用 NAT** 以启用该功能。
- 步骤 3** 单击**应用**。
-

静态 NAT

静态 NAT 用于防止 LAN 设备被发现和遭受攻击。静态 NAT 创建了一种关系，将有效的 WAN IP 地址映射到由 NAT 在 WAN（互联网）上隐藏的 LAN IP 地址。

- 步骤 1** 单击**防火墙 > 静态 NAT**。
- 步骤 2** 单击**添加**（或选择相应行，然后单击**编辑**），并输入相关信息。

专用 IP 地址范围起始 IP 地址	输入要映射到公共范围的内部 IP 地址范围的起始 IP 地址。
---------------------------	---------------------------------

公共 IP 地址范围起始 IP 地址	输入 ISP 提供的公共 IP 地址范围的起始 IP 地址。 注释 请勿在此范围中包含路由器的 WAN IP 地址。
范围长度	输入此范围中 IP 地址的数量。 注释 范围长度不得超过有效 IP 地址的数量。要映射单个地址，请输入 1。
服务	从下拉列表中选择适用于静态 NAT 的服务的名称。
接口	从下拉列表中选择接口名称。
活动	选择活动以启用。

步骤 3 单击**服务管理**。

步骤 4 要添加服务，请单击“服务”表下的**添加**。要编辑或删除服务，请选择相应行并单击**编辑**或**删除**。字段打开可以修改。

步骤 5 配置以下服务：

- **应用名称** — 服务或应用的名称。
- **协议** — 输入协议。
- **起始端口/ICMP 类型/IP 协议** — 输入为此服务保留的端口号的范围。
- **结束端口** — 输入为此服务保留的最后一个端口号。

步骤 6 单击**应用**。

端口转发

利用端口转发功能，通过为某个服务打开特定端口或端口范围，可以公开访问 LAN 网络设备上的服务。

要配置端口转发，请按照以下步骤操作：

步骤 1 单击**防火墙 > 端口转发**。

步骤 2 在**端口转发表**中，单击**添加**（或选择某一行并单击**编辑**），并配置以下设置：

外部服务	从下拉列表中选择外部服务。（如果服务未列出，可以按照“服务管理”部分中的说明添加或修改列表。）
内部服务	从下拉列表中选择内部服务。（如果服务未列出，可以按照“服务管理”部分中的说明添加或修改列表。）

内部 IP 地址	输入服务器的内部 IP 地址。
接口	从下拉列表中选择要应用端口转发的接口。
状态	启用或禁用端口转发规则。

步骤 3 单击服务管理。

步骤 4 在服务表中，单击添加（或选择某一行并单击编辑），并配置以下设置：

- 应用名称 — 服务或应用的名称。
- 协议 — 所需协议。请参阅您托管的服务的相关文档。
- 起始端口/ICMP 类型/IP 协议 — 为此服务预留的端口号范围。
- 结束端口 — 为此服务预留的最后一个端口号。

步骤 5 单击应用。

注释 通过 UPnP 应用动态添加 UPnP 的端口转发规则。

步骤 6 在 UPnP 端口转发表中，单击刷新以刷新 UPnP 列表。

端口触发

端口触发可在用户通过触发端口发送出站流量后为进站流量打开指定端口或端口范围。利用端口触发功能，设备可以监视特定端口号的传出数据。设备能记住发送匹配数据的客户端的 IP 地址。当请求的数据通过设备返回时，设备将使用 IP 寻址和端口映射规则将数据发送到正确的客户端。

要向端口触发表添加服务或编辑服务，请配置以下设置：

步骤 1 单击添加（或选择相应行，然后单击编辑）并输入以下信息：

应用名称	输入应用的名称。
触发服务	从下拉列表中选择服务。（如果服务未列出，可以按照“服务管理”部分中的说明添加或修改列表。）
传入服务	从下拉列表中选择服务。（如果服务未列出，可以按照“服务管理”部分中的说明添加或修改列表。）
接口	从下拉列表中选择接口。
状态	启用或禁用端口触发规则。

步骤 2 单击**服务管理**，以添加或编辑服务列表上的条目。

步骤 3 在**服务表**中，单击**添加**或**编辑**，然后配置以下设置：

- **应用名称** — 服务或应用的名称。
- **协议** — 所需协议。请参阅您托管的服务的相关文档。
- **起始端口/ICMP 类型/IP 协议** — 为此服务预留的端口号范围。
- **结束端口** — 为此服务预留的最后一个端口号。

步骤 4 单击**应用**。

会话超时

借助会话超时功能，您可以为 TCP/UDP/ICMP 流量配置会话超时和最大并发连接设置。会话超时设置的是 TCP 或 UDP 会话闲置多长时间后会超时。

要配置会话超时，请按照以下步骤操作：

步骤 1 单击**防火墙 > 会话超时**。

步骤 2 输入以下信息：

TCP 会话超时	输入 TCP 会话的超时值（以秒为单位）。这段时间之后，系统将从会话表中删除不活动的 TCP 会话。
UDP 会话超时	输入 UDP 会话的超时值（以秒为单位）。这段时间之后，系统将从会话表中删除不活动的 UDP 会话。
ICMP 会话超时	输入 ICMP 会话的超时值（以秒为单位）。这段时间之后，系统将从会话表中删除不活动的 ICMP 会话。
最大并发连接数量	输入允许的最大并发连接数量。
当前连接	显示当前连接的数量。
清除连接	单击该按钮可清除当前连接。

步骤 3 单击**应用**。

DMZ 主机

DMZ 是一个子网，向公众开放但位于防火墙之后。使用 DMZ 可以将传输到 WAN 端口的数据包重新定向到 LAN 中特定的 IP 地址。

DMZ 主机允许 LAN 中的一个主机连接到互联网以使用服务，例如互联网游戏、视频会议、Web 或电子邮件服务器。可使用防火墙访问规则限制从互联网访问 DMZ 主机。建议将必须连接 WAN 以使用服务的主机置于 DMZ 网络中。

要配置 DMZ，请按照以下步骤操作：

-
- 步骤 1 选择防火墙 > DMZ。
 - 步骤 2 在 DMZ 主机中，选中启用。
 - 步骤 3 输入 DMZ 主机 IP 地址。
 - 步骤 4 单击应用。
-



第 11 章

VPN

本节介绍虚拟专用网络 (VPN)，它用于在安全性较低的网络中建立加密连接。虚拟专用网络确保安全连接到底层网络基础设施。隧道建立的专用网络可使用加密和验证安全地发送数据。本节包含以下主题：

- [VPN 设置向导（站点到站点），第 85 页](#)
- [IPSec 配置文件，第 87 页](#)
- [站点到站点，第 89 页](#)
- [客户端到站点，第 95 页](#)
- [远程工作人员 VPN 客户端，第 98 页](#)
- [PPTP 服务器，第 100 页](#)
- [L2TP 服务器，第 100 页](#)
- [SSL VPN，第 101 页](#)
- [VPN 通道，第 103 页](#)

VPN 设置向导（站点到站点）

借助 VPN，远程主机可以像位于同一局域网中一样工作。路由器可支持 50 个隧道。VPN 设置向导引导用户为站点到站点 IPSec 隧道设置安全的连接。这可以避免设置复杂和可选的参数，从而简化配置，让任何用户都可以快速、高效地设置 IPSec 隧道。

要启动 VPN 设置向导，请单击 **VPN > VPN 设置向导**。请按照以下步骤配置向导。

- 步骤 1** 在“开始使用”部分，在为此连接命名框中输入连接名称。
- 步骤 2** 从下拉列表中选择接口（**WAN1、WAN2、USB1 或 SB2**）。
- 步骤 3** 单击下一步。
- 步骤 4** 在“远程路由器设置”部分，从下拉列表中选择**远程连接类型**。如果选择**IP 地址**，则输入 IP 地址；如果选择**完全限定域名 (FQDN)**，则输入名称。
- 步骤 5** 单击下一步进入下一个屏幕。
- 步骤 6** 在“本地和远程网络”部分，在“本地流量选择”下，从下拉列表中选择本地 IP（**IP 地址或子网**）。如果选择**IP 地址**，则输入 IP 地址；如果选择**子网**，则输入 IP 地址和子网掩码。
- 步骤 7** 在“远程流量选择”下，从下拉列表中选择远程 IP（**IP 地址或子网**）。如果选择**IP 地址**，则输入 IP 地址；如果选择**子网**，则输入 IP 地址和子网掩码。
- 步骤 8** 单击下一步。
- 步骤 9** 在“IPSec 配置文件”中，从下拉列表中选择 IPsec 配置文件。
- 步骤 10** 如果选择默认，则单击下一步。
- 步骤 11** 如果选择新配置文件，则配置以下设置：
第 1 阶段选项

Diffie-Hellman (DH) 组	从下拉列表中选择 DH 组（ 第 2 组或第 5 组 ）。DH 是一种密钥交换协议，有两组不同的主密钥长度：第 2 组最长 1,024 位，第 5 组最长 1,536 位。若要较快的速度和较低的安全性，请选择第 2 组。若要较慢的速度和较高的安全性，请选择第 5 组。默认情况下选择第 2 组。
加密	从下拉列表中选择加密选项（ 3DES、AES-128、AES-192 或 AES-256 ）。加密方法决定了对 ESP/ISAKMP 数据包进行加密或解密的算法。
验证	验证方法决定了封装安全载荷协议 (ESP) 报头数据包生效的方法。MD5 是一种可生成 128 位摘要的单向散列算法。SHA1 是一种可生成 160 位摘要的单向散列算法。推荐使用 SHA1，因为这种方法更加安全。确保 VPN 隧道两端使用相同的验证方法。选择验证方法（ MD5、SHA1 或 SHA2-256 ）。
安全关联持续时间（秒）	IKE SA 在此阶段处于活动状态的时间。第 1 阶段的默认值为 28,800 秒。
完全向前保密 (PFS)	选中 启用 以启用 PFS，并输入持续时间（秒），或者取消选中 启用 以禁用。当 PFS 启用时，IKE 第 2 阶段协商将为 IPsec 流量加密和验证生成新密钥。建议启用此功能。
预先共享密钥	用于验证远程 IKE 对端的预先共享密钥。最多可以输入 30 位键盘字符或十六进制值，例如 My_@123 或 4d795f40313233。VPN 隧道两端必须使用相同的预先共享密钥。 建议定期更改预先共享密钥，以便最大限度地提高 VPN 的安全性。

第 2 阶段选项

Diffie-Hellman (DH) 组	<p>从下拉列表中选择 DH 组（第 2 组或第 5 组）。DH 是一种密钥交换协议，有两组不同的主密钥长度：第 2 组最长 1,024 位，第 5 组最长 1,536 位。</p> <p>若要较快的速度和较低的安全性，请选择第 2 组。若要较慢的速度和较高的安全性，请选择第 5 组。默认情况下选择第 2 组。</p> <p>注释 仅当在第 1 阶段选项下启用完全向前保密时才启用此功能。</p>
协议选项	<p>从下拉列表中选择协议。</p> <ul style="list-style-type: none"> • ESP: 选择 ESP 进行数据加密，并输入加密选项。 • AH: 在数据不需要保密但必须进行验证的情况下，选择此选项以确保数据完整性。
加密	<p>从下拉列表中选择加密选项（3DES、AES-128、AES-192 或 AES-256）。加密方法决定了对 ESP/ISAKMP 数据包进行加密或解密的算法。</p>
验证	<p>选择验证方法（MD5、SHA1 或 SHA2-256）。</p>
安全关联持续时间（秒）	<p>VPN 隧道 (IPSec SA) 在此阶段处于活动状态的时间。第 2 阶段的默认值为 3600 秒。</p>

步骤 12 单击下一步查看所有配置的摘要。

步骤 13 单击提交。

IPSec 配置文件

IPSec 配置文件包含与算法相关的信息，例如自动模式下第 I 和第 II 阶段协商的加密、验证和 DH 组。如果密钥模式为手动，这些配置文件还包含相应算法的密钥。任何 IPsec VPN 记录（例如，站点到站点、客户端到站点或远程工作人员 VPN 客户端）均引用 IPsec 配置文件。

要配置 IPSec 配置文件，请按照以下步骤操作：

步骤 1 选择 **VPN > IPsec 配置文件**。

步骤 2 在“IPSec 配置文件表”中，单击添加。

步骤 3 在“添加新 IPSec 配置文件”下的“配置文件名称”部分输入名称。

步骤 4 选择密钥模式。

步骤 5 对于自动密钥模式，配置以下设置：

第 1 阶段选项

Diffie-Hellman (DH) 组	从下拉列表中选择 DH 组（第 2 组或第 5 组）。DH 是一种密钥交换协议，有两组不同的主密钥长度：第 2 组最长 1,024 位，第 5 组最长 1,536 位。 若要较快的速度和较低的安全性，请选择第 2 组。若要较慢的速度和较高的安全性，请选择第 5 组。默认情况下选择第 2 组。
加密	从下拉列表中选择加密选项（3DES、AES-128、AES-192 或 AES-256）。加密方法决定了对 ESP/ISAKMP 数据包进行加密或解密的算法。
验证	验证方法决定了封装安全载荷协议 (ESP) 报头数据包生效的方法。MD5 是一种可生成 128 位摘要的单向散列算法。SHA1 是一种可生成 160 位摘要的单向散列算法。推荐使用 SHA1，因为这种方法更加安全。确保 VPN 隧道两端使用相同的验证方法。选择验证方法（MD5、SHA1 或 SHA2-256）。
安全关联持续时间（秒）	IKE SA 在此阶段处于活动状态的时间。第 1 阶段的默认值为 28,800 秒。
完全向前保密 (PFS)	选中启用以启用 PFS，并输入持续时间（秒），或者取消选中启用以禁用。当 PFS 启用时，IKE 第 2 阶段协商将为 IPSec 流量加密和验证生成新密钥。建议启用此功能。

第 2 阶段选项

协议选项	从下拉列表中选择协议。 <ul style="list-style-type: none"> • ESP: 选择 ESP 进行数据加密，并输入加密选项。 • AH: 在数据不需要保密但必须进行验证的情况下，选择此选项以确保数据完整性。
加密	从下拉列表中选择加密选项（3DES、AES-128、AES-192 或 AES-256）。加密方法决定了对 ESP/ISAKMP 数据包进行加密或解密的算法。
验证	选择验证方法（MD5、SHA1 或 SHA2-256）。
安全关联持续时间（秒）	VPN 隧道 (IPSec SA) 在此阶段处于活动状态的时间。第 2 阶段的默认值为 3600 秒。
Diffie-Hellman (DH) 组	从下拉列表中选择 DH 组（第 2 组或第 5 组）。DH 是一种密钥交换协议，有两组不同的主密钥长度：第 2 组最长 1,024 位，第 5 组最长 1,536 位。 若要较快的速度和较低的安全性，请选择第 2 组。若要较慢的速度和较高的安全性，请选择第 5 组。默认情况下选择第 2 组。

步骤 6 对于手动密钥模式，配置以下设置：

IPSec 配置

安全参数索引 (SPI) 传入	输入一个数字（范围：100 - FFFFFFFF，默认值：100）。 SPI 是一种在使用 IPsec 进行 IP 流量隧道传输时添加到报头的标识标记。此标记帮助内核识别两种流量流，这二者可能使用了不同的加密规则和算法。
SPI 传出	输入一个数字（范围：100 - FFFFFFFF，默认值：100）。
加密	从下拉列表中选择加密选项（ 3DES 、 AES-128 、 AES-192 或 AES-256 ）。加密方法决定了对 ESP/ISAKMP 数据包进行加密或解密的算法。
密钥输入	输入一个数字（十六进制，48 个字符）。十六进制格式的密钥，用于解密接收到的 ESP 数据包。
密钥输出	输入一个数字（十六进制，48 个字符）。十六进制格式的密钥，用于加密普通数据包。
验证	验证方法决定了封装安全载荷协议 (ESP) 报头数据包生效的方法。MD5 是一种可生成 128 位摘要的单向散列算法。SHA1 是一种可生成 160 位摘要的单向散列算法。推荐使用 SHA1，因为这种方法更加安全。确保 VPN 隧道两端使用相同的验证方法。选择验证方法（ MD5 、 SHA1 或 SHA2-256 ）。
安全关联持续时间（秒）	IKE SA 在此阶段处于活动状态的时间。第 1 阶段的默认值为 28,800 秒。
密钥输入	输入一个数字（十六进制，32 个字符）。十六进制格式的密钥，用于解密接收到的 ESP 数据包。
密钥输出	输入一个数字（十六进制，32 个字符）。十六进制格式的密钥，用于加密普通数据包。

- 步骤 7** 选择 IPsec 配置文件，并单击**编辑**或**删除**。
- 步骤 8** 要复制现有配置文件，请选择配置文件并单击**复制**。
- 步骤 9** 单击**应用**。

站点到站点

在站点到站点 VPN 中，一个位置的本地路由器可以通过 VPN 隧道连接到远程路由器。客户端设备可以访问网络资源，如同它们都在同一个站点一样。此模式可用于远程位置中的多个用户。

要想成功连接，则要求至少其中一个路由器可通过静态 IP 地址或动态 DNS 主机名标识。如果某个路由器仅有一个动态 IP 地址，您可使用任何电子邮件地址（用户 FQDN）或 FQDN 来确认是否已建立连接。

隧道两端的两个 LAN 子网不能在相同的网络中。例如，如果站点 A LAN 使用 192.168.1.x/24 子网，则站点 B 可以使用 192.168.2.x/24。

要配置隧道，请在配置这两个路由器时输入相应的设置（将本地和远程反向）。假设此路由器标识为路由器 A。请在“本地组设置”部分输入其设置；在“远程组设置”部分输入另一路由器（路由器 B）的设置。配置另一个路由器（路由器 B）时，请在“本地组设置”部分输入其设置，并在“远程组设置”部分输入路由器 A 的设置。

要配置站点到站点 VPN，请按照以下步骤操作：

步骤 1 单击 **VPN > 站点到站点**。

步骤 2 站点到站点表中将显示以下选项：

连接名称	使用 VPN 设置向导创建的 VPN 隧道连接的名称。无需与隧道另一端使用的名称相匹配。
远程端点	VPN 连接的目标远程端点的 IP 地址。可以是 FQDN 或 IP 地址。
接口	用于隧道的接口。
IPSec 配置文件	用于 VPN 隧道的 IPSec 配置文件。
本地流量选择	产生流量的流量选择器。
远程流量选择	流量去往的流量选择器。
状态	隧道的状态。
操作	<ul style="list-style-type: none"> • 编辑 — 单击可编辑连接，系统导航至“站点到站点 - 添加或编辑新连接”页面。 • 删除 — 单击可删除连接。 • 连接 — 单击可连接并建立隧道。 • 断开连接 — 单击可断开连接。
创建站点到站点 VPN	单击可创建新的站点到站点隧道。
创建安全的 GRE 隧道	单击可创建新的 GRE 隧道。

创建站点到站点 VPN 连接

步骤 1 在“基本设置”选项卡中，提供以下信息：

启用	单击 启用 以启用配置。
连接名称	输入 VPN 隧道的连接名称。此名称仅供参考；不一定与隧道另一端使用的名称相匹配。
IPSec 配置文件	默认 - 已选择“自动配置文件”。
接口	从下拉列表中选择用于该隧道的接口（ WAN1 、 WAN2 、 USB1 或 USB2 ）。
远程端点	从下拉列表中选择 静态 IP 或 FQDN 。

IKE 验证方法

预先共享密钥	IKE 对端彼此进行验证的方式是，计算并发送含预先共享密钥的密钥数据散列。如果接收端能够使用预先共享密钥独立创建相同散列，表明两个对端必定共享相同密钥，以此验证另一个对端。预先共享密钥不能很好地扩展，因为配置每个 IPSec 对端时，必须使用与其建立会话的其余每一个对端的预先共享密钥。输入预先共享密钥，单击 启用 以启用“预先共享密钥最小复杂度”。
证书	数字证书是一个数据包，包含证书持有人身份（姓名或 IP 地址、证书序列号、证书有效日期，以及证书持有人公共密钥的副本）等信息。X.509 标准定义了标准数字证书的格式。X.509 标准第 3 版定义了证书的数据结构。从下拉列表中选择证书。

适用于本地组设置

本地标识符类型	从下拉列表中选择“本地 WAN IP”、“本地 FQDN”或“本地用户 FQDN”
本地标识符	根据您的选择输入标识符名称或 IP 地址
本地 IP 类型	从下拉列表中选择 IP 地址 或 子网 。
IP 地址	输入可使用该隧道的设备的 IP 地址。
子网掩码	输入子网掩码。

远程组设置

远程标识符类型	从下拉列表中选择“本地 WAN IP”、“本地 FQDN”或“本地用户 FQDN”。
远程标识符	根据您的选择输入标识符名称或 IP 地址
远程 IP 类型	从下拉列表中选择 IP 地址 或 子网 。
IP 地址	输入可使用该隧道的设备的 IP 地址。
子网掩码	输入子网掩码。

步骤 2 在“高级设置”选项卡中，提供以下信息：

积极模式	<p>IKE SA 协商有两种模式——主模式和积极模式。如果注重网络安全，建议使用主模式。如果注重网络速度，建议使用积极模式。选中启用可启用积极模式，取消选中启用将使用主模式。</p> <p>如果“远程安全网关类型”是一种动态 IP 类型，则必须使用积极模式。系统将自动选中此复选框，并且此设置无法更改。</p>
压缩	<p>一种可减小 IP 数据报大小的协议。选中“压缩”后，路由器将在启动连接时提议压缩。如果应答器拒绝此提议，则路由器不会实施压缩。将路由器用作应答器时，它将接受压缩，即使是在压缩未启用的情况下。如果在该路由器上启用此功能，则在隧道另一端的路由器上也应该启用此功能。</p>
NetBIOS 广播	<p>广播消息用于 Windows 网络中的名称解析，以标识计算机、打印机和文件服务器等资源。某些软件应用程序和“网上邻居”等 Windows 功能将使用这些消息。LAN 广播流量通常不会通过 VPN 隧道进行转发。但是，选中此复选框后，NetBIOS 广播就可从隧道的一端转播到另一端。</p>
持久连接	<p>以固定时间间隔尝试重新建立 VPN 连接。</p>
对端无响应检测 (DPD) 启用	<p>单击 DPD 以启用 DPD。该功能定期发送 HELLO/ACK 消息以检查 VPN 隧道的状态。必须在 VPN 隧道两端同时启用 DPD 选项。在“间隔”字段中，输入以下信息以指定 HELLO/ACK 消息之间的时间间隔：</p> <ul style="list-style-type: none"> • 延时：输入每条 HELLO 消息之间的延时。 • 检测超时：输入宣布对端无响应前的超时时间。 • 延迟操作：DPD 超时后要采取的操作。从下拉列表中选择清除或重启。
扩展验证	<p>选中扩展验证以启用该功能。</p> <p>对于单个用户，选择用户并输入用户名和密码。</p> <p>对于组，选择组名称，并从下拉列表中选择管理员或访客。</p>
拆分 DNS	<p>选中拆分 DNS以启用该功能。</p> <p>根据指定的域名，将一些 DNS 请求发送至一个 DNS 服务器，将其他 DNS 请求发送至另一个 DNS 服务器。路由器收到地址解析请求时，将检查域名。如果该域名与“拆分 DNS”设置中的某个域名匹配，路由器会将此请求传递至指定的 DNS 服务器。否则，路由器会将此请求传递至 WAN 接口设置中指定的 DNS 服务器。</p> <p>DNS 服务器 1 和 DNS 服务器 2—输入用于指定域的 DNS 服务器的 IP 地址。作为可选操作，您也可以在“DNS 服务器 2”字段中指定辅助 DNS 服务器。</p> <p>域名 1 至 6—输入 DNS 服务器的域名。域的请求将被传递至指定的 DNS 服务器。</p>

步骤 3 要启用站点到站点故障切换，应在“高级设置”选项卡中启用“持久连接”。然后，在“故障切换”选项卡中提供以下信息：

隧道备份	选中 隧道备份 以启用该功能。当主隧道故障时，该功能使路由器能够使用远程对端的备用 IP 地址或者备用的本地 WAN 接口重新建立 VPN 隧道。仅当 DPD 启用时，此功能才可用。
远程备用 IP 地址	输入远程对端的 IP 地址，或者重新输入已为远程网关设置的 WAN IP 地址。
本地接口	从下拉列表中选择本地接口（ WAN1 、 WAN2 、 USB1 或 USB2 ）。

注释 要启用站点到站点故障切换，必须在“高级设置”选项卡中启用“持久连接”。

步骤 4 单击应用。

创建安全 GRE 隧道

通用路由封装 (GRE) 是一种可用的隧道机制，它使用 IP 作为传输协议，并承载许多不同的乘客协议。隧道相当于虚拟点对点链接，具有两个端点，这两个端点分别由隧道源地址和隧道目的地址标识。

步骤 1 单击创建安全 GRE 隧道。

步骤 2 单击启用以启用配置，并输入以下信息：

适用于 GRE 隧道信息

接口名称	输入用于连接隧道的接口的名称。
隧道源	从下拉列表中选择隧道源（ WAN1 、 WAN2 、 USB1 或 USB2 ）。
隧道目标	从下拉列表中选择隧道目标（ 静态 IP 或 FQDN ）。
GRE 隧道的 IP 地址	输入承载传输协议的隧道的 IP 地址。
子网掩码	输入 GRE 隧道的子网掩码。

适用于 IPSec 隧道

连接名称	连接的名称。
IPSec 配置文件	从下拉列表中选择 IPSec 配置文件（ 默认 、 IPSecProfileAuto 、 IPSecProfileManual 、 手动 1 或 自动 ）。
本地标识符类型	从下拉列表中选择“本地 WAN IP”、“本地 FQDN”或“本地用户 FQDN”。

本地标识符	根据选定项输入标识符名称或 IP 地址。
远程标识符类型	从下拉列表中选择本地 WAN IP、本地 FQDN 或本地用户 FQDN。
远程标识符	根据选定项输入标识符名称或 IP 地址。

适用于 IKE 验证方法

预先共享密钥	IKE 对端彼此进行验证的方式是，计算并发送含预先共享密钥的密钥数据散列。如果接收端能够使用预先共享密钥独立创建相同散列，表明两个对端必定共享相同密钥，以此验证另一个对端。预先共享密钥不能很好地扩展，因为配置每个 IPSec 对端时，必须使用与其建立会话的其余每一个对端的预先共享密钥。输入预先共享密钥，单击 启用 以启用“预先共享密钥最小复杂度”。
证书	数字证书是一个数据包，包含证书持有人身份（姓名或 IP 地址、证书序列号、证书有效日期，以及证书持有人公共密钥的副本）等信息。X.509 标准定义了标准数字证书的格式。X.509 标准第 3 版定义了证书的数据结构。从下拉列表中选择证书。

适用于路由协议

静态路由	选中“静态路由”以启用静态路由，并从下拉列表中选择以下选项。 <ul style="list-style-type: none"> • 拆分隧道 — 允许移动用户使用相同或不同网络连接同时访问不同的安全域，例如公共网络和 LAN 或 WAN。 • 隧道传输所有流量 — 允许通过隧道传输所有流量。
IP 地址	单击 添加 并输入 IP 地址。还可通过单击 编辑 或 删除 ，编辑或删除现有记录。
子网掩码	输入子网掩码。
组播转发	选择 组播转发 以允许路由器将组播流量转发至包含其他接收组播设备的网络。组播转发可防止向没有接收节点的网络转发组播流量。单击链接以配置 IGMP 代理接口。
积极模式	单击以启用积极模式。

步骤 3 单击应用。



客户端到站点

互联网上的客户端可以连接服务器，以访问服务器后的企业网络或 LAN。使用此功能可以创建新的 VPN 隧道，使远程工作人员和商务旅行人员可使用第三方 VPN 客户端软件访问网络。

要配置客户端到站点，请按照以下步骤操作：

- 步骤 1** 单击 **VPN > 客户端到站点**。
- 步骤 2** 单击**添加**。系统将显示“IPsec 客户端到站点组”表。
- 步骤 3** 要添加客户端到站点连接，请单击**添加**。
- 步骤 4** 在添加新组部分，选择一个选项（“思科 VPN 客户端”或“第三方客户端”）。
- 步骤 5** 对于“思科 VPN 客户端”，配置以下设置：

启用	单击 启用 以启用配置。
组名称	输入组名称。在 IKE 协商期间，该组名称用作该组所有成员的标识。
接口	从下拉列表中选择接口（ WAN1 、 WAN2 、 USB1 或 USB2 ）。
IKE 验证方法	<p>在基于 IKE 的隧道中用于 IKE 协商的验证方法。</p> <ul style="list-style-type: none"> • 预先共享密钥：IKE 对端彼此进行验证的方式是，计算并发送含预先共享密钥的密钥数据散列。如果接收端能够使用预先共享密钥独立创建相同散列，表明两个对端必定共享相同密钥，以此验证另一个对端。预先共享密钥不能很好地扩展，因为配置每个 IPsec 对端时，必须使用与其建立会话的其余每一个对端的预先共享密钥。输入预先共享密钥，单击启用以启用“预先共享密钥最小复杂度”。 • 证书：数字证书是一个数据包，包含证书持有人身份（姓名或 IP 地址、证书序列号、证书有效日期，以及证书持有人公共密钥的副本）等信息。X.509 标准定义了标准数字证书的格式。X.509 标准第 3 版定义了证书的数据结构。从下拉列表中选择证书。
用户组	单击 组名称 并选择用户组（“ 管理员 ”或“ 访客 ”）。单击 添加 或 删除 可修改用户组。
模式	<p>选择模式选项。</p> <ul style="list-style-type: none"> • 客户端—客户端请求 IP 地址，服务器提供配置的地址范围以内的 IP 地址。选择客户端，并输入客户端 LAN 的起始和结束 IP 地址。 • 网络扩展模式 (NEM)—客户端提出子网建议，对于这些子网，服务器后的 LAN 和客户端建议的子网之间的流量需应用 VPN 服务。
客户端 LAN 的池范围	起始 IP —输入池范围的起始 IP 地址。 结束 IP —输入池范围的结束 IP 地址。

适用于模式配置

主 DNS	输入主 DNS 服务器的 IP 地址。
辅助 DNS	输入辅助 DNS 服务器的 IP 地址。
主 Windows 互联网名称服务 (WINS) 服务器	输入主 WINS 的 IP 地址。
辅助 WINS 服务器	输入辅助 WINS 的 IP 地址。
默认域	输入要在远程网络中使用的默认域的名称。
备用服务器 1、2 和 3	输入备用服务器 1、2 和 3 的 IP 地址或域名。当与主 IPsec VPN 服务器的连接失败时，安全设备可启动与备用服务器的 VPN 连接。备用服务器 1 的优先级最高，备用服务器 3 的优先级最低。
拆分隧道	选中可启用拆分隧道。然后，单击添加，输入拆分隧道的 IP 地址和子网掩码。您可以添加、编辑或删除拆分隧道。
拆分 DNS	选中可启用拆分 DNS。然后，单击添加，输入拆分 DNS 的域名。您可以添加、编辑或删除拆分隧道。

适用于第三方客户端

步骤 6 在“基本设置”选项卡中，配置以下设置：

启用	单击启用以启用配置。
隧道名称	VPN 隧道的名称。此名称仅供参考，不一定与隧道另一端使用的名称相匹配。
接口	从下拉列表中选择接口（WAN1、WAN2、USB1 或 USB2）。
IKE 验证方法	<p>在基于 IKE 的隧道中用于 IKE 协商的验证方法。</p> <ul style="list-style-type: none"> • 预先共享密钥： IKE 对端彼此进行验证的方式是，计算并发送含预先共享密钥的密钥数据散列。如果接收端能够使用预先共享密钥独立创建相同散列，表明两个对端必定共享相同密钥，以此验证另一个对端。预先共享密钥不能很好地扩展，因为配置每个 IPsec 对端时，必须使用与其建立会话的其余每一个对端的预先共享密钥。输入预先共享密钥，单击“启用”以启用“预先共享密钥最小复杂度”。 • 证书： 数字证书是一个数据包，包含证书持有人身份（姓名或 IP 地址、证书序列号、证书有效日期，以及证书持有人公共密钥的副本）等信息。X.509 标准定义了标准数字证书的格式。X.509 标准第 3 版定义了证书的数据结构。从下拉列表中选择证书。

本地标识符	从下拉列表中选择本地标识符类型（ IP 地址 、 FQDN 或 用户 FQDN ），并输入标识符。
远程标识符	从下拉列表中选择远程标识符类型（ 远程 IP 或 用户 FQDN ），并输入标识符。
扩展验证	选中 扩展验证 以启用该功能。单击 添加 以添加扩展验证，并选择 管理员 或 访客 。
客户端 LAN 的池范围	起始 IP — 输入池范围的起始 IP 地址。 结束 IP — 输入池范围的结束 IP 地址。

步骤 7 在“高级设置”选项卡中，配置以下设置：

IPSec 配置文件	设为默认。
远程端点	从下拉列表中选择远程端点（ 静态 IP 、 FQDN 或 动态 IP ）。

适用于本地组设置

本地 IP 类型	从下拉列表中选择本地 IP 类型（ IP 地址 或 子网 ）。
IP 地址	输入设备的 IP 地址。
子网掩码	输入子网掩码。

适用于模式配置

主 DNS	输入主 DNS 服务器的 IP 地址。
辅助 DNS	输入辅助 DNS 服务器的 IP 地址。
主 Windows 互联网名称服务 (WINS) 服务器	输入主 WINS 的 IP 地址。
辅助 WINS 服务器	输入辅助 WINS 的 IP 地址。
默认域	输入要在远程网络中使用的默认域的名称。
备用服务器 1、2 和 3	输入备用服务器 1、2 和 3 的 IP 地址或域名。当与主 IPSec VPN 服务器的连接失败时，安全设备可启动与备用服务器的 VPN 连接。备用服务器 1 的优先级最高，备用服务器 3 的优先级最低。
拆分隧道	选中可启用拆分隧道。然后，单击 添加 ，输入拆分隧道的 IP 地址和子网掩码。您可以添加、编辑或删除拆分隧道。
拆分 DNS	选中可启用拆分 DNS。然后，单击 添加 ，输入拆分 DNS 的域名。您可以添加、编辑或删除拆分隧道。

更多设置

积极模式	选中积极模式以启用该功能。 “积极模式”功能用于为 IP 安全 (IPsec) 对端指定 RADIUS 隧道属性，并发起与隧道属性的互联网密钥交换 (IKE) 积极模式协商。
压缩（支持 IP 负载压缩协议 [IP Comp]）	选中压缩，可启用路由器在开始连接时提议压缩的功能。如果应答器拒绝此提议，则路由器不会实施压缩。将路由器用作应答器时，它将接受压缩，即使是在压缩未启用的情况下。如果在该路由器上启用此功能，则在隧道另一端的路由器上也应该启用此功能。

步骤 8 完成设置后，单击应用。

远程工作人员 VPN 客户端

远程工作人员 VPN 客户端功能可允许设备以思科 VPN 硬件客户端的形式运行，从而最大程度地降低远程位置的配置要求。当远程工作人员 VPN 客户端启动 VPN 连接后，IPSec VPN 服务器会将 IPSec 策略推送至远程工作人员 VPN 客户端，并创建相应的隧道。

要配置远程工作人员 VPN 客户端，请按照以下步骤操作：

步骤 1 单击 VPN > 远程工作人员 VPN 客户端，并配置以下内容：

远程工作人员 VPN 客户端	选中打开或关闭。启动时，只有一个远程工作人员 VPN 客户端的连接可以处于活动状态。如果您在启动时启用了—个远程工作人员 VPN 客户端，那么它会禁用与其他客户端规则有关的此选项。
自动启动重试	选中打开或关闭。
重试间隔	输入以秒为单位的时间（范围：120 到 1800）。
重试限制	输入重试次数上限（范围：0 到 16）。

步骤 2 单击应用。

步骤 3 在“远程工作人员 VPN 客户端”表中，单击添加。

步骤 4 在“基本设置”部分提供以下信息：

名称	输入配置文件的名称。
服务器（远程地址）	输入远程服务器的 IP 地址。
启动时的活动连接	在启动时启动连接。无论何时，都只能有一个配置文件处于“打开”状态，以便在启动时开始协商

IKE 验证方法	<p>在基于 IKE 的隧道中用于 IKE 协商的验证方法。</p> <ul style="list-style-type: none"> • 预先共享密钥: IKE 对端彼此进行验证的方式是, 计算并发送含预先共享密钥的密钥数据散列。如果接收端能够使用预先共享密钥独立创建相同散列, 表明两个对端必定共享相同密钥, 以此验证另一个对端。预先共享密钥不能很好地扩展, 因为配置每个 IPSec 对端时, 必须使用与其建立会话的其余每一个对端的预先共享密钥。选中预先共享密钥, 并在指定的字段中输入组名称和密码。 • 证书: 数字证书是一个数据包, 包含证书持有人身份 (姓名或 IP 地址、证书序列号、证书有效日期, 以及证书持有人公共密钥的副本) 等信息。X.509 标准定义了标准数字证书的格式。X.509 版本 3 定义了证书的数据结构。选中证书, 然后选择默认。
模式	<ul style="list-style-type: none"> • 客户端 — 客户端请求 IP 地址, 服务器提供配置的地址范围以内的 IP 地址。选择客户端, 并输入用户名和密码。 • 网络扩展模式 (NEM) — 客户端提出子网建议, 对于这些子网, 服务器后的 LAN 和客户端建议的子网之间的流量需应用 VPN 服务。ezvpn 客户端 NEM 模式仅支持 LAN IP 10.0.0.0/8、172.16.0.0/12 或 192.168.0.0/16。此外, 当处于 NEM 模式下时, 服务器后的 LAN 和客户端应位于不同的子网。选择NEM, 并从下拉列表中选择 VLAN, 然后输入用户名和密码。
VLAN	选择一个 VLAN。
用户名	输入用户名。
用户密码	输入密码。
确认用户密码	确认密码。

适用于高级设置

备用服务器 1、2 和 3	<p>输入备用服务器 1、2 和 3 的 IP 地址或域名。</p> <p>当与主 IPSec VPN 服务器的连接失败时, 安全设备可启动与备用服务器的 VPN 连接。备用服务器 1 的优先级最高, 备用服务器 3 的优先级最低。</p>
对端超时	输入以秒为单位的时间 (范围: 30 到 480)。

步骤 5 单击应用。

PPTP 服务器

点对点隧道协议 (PPTP) 是实施虚拟专用网络的一种方法。PPTP 使用 TCP 控制通道和通用路由封装 (GRE) 隧道操作封装 PPP 数据包。最多可为运行 PPTP 客户端软件的用户启用 25 个 PPTP (点对点隧道协议) VPN 隧道。在向导中, 用户选择该选项可使用 VPN 连接创建指向工作场所的连接。

要配置 PPTP 服务器, 请按照以下步骤操作:

步骤 1 单击 **VPN > PPTP 服务器**, 然后提供以下信息:

PPTP 服务器	选择打开或关闭可启用或禁用 PPTP 服务器。
起始和结束 IP 地址	如果已启用 PPTP, 可输入起始和结束 IP 地址。
DNS1 和 DNS2 IP 地址	输入主要和辅助 DNS 服务器的 IP 地址。
用户验证	选择用户验证 (Admin 或 默认)。
Microsoft 点对点加密 (MPPE)	MPPE 可对基于 PPP 的拨号连接或 PPTP VPN 连接中的数据进行加密。支持 128 位密钥 MPPE 加密方案。从下拉列表中选择 MPPE 加密 (无 或 128 位)。

步骤 2 单击**应用**。

L2TP 服务器

第 2 层隧道协议 (L2TP) 是 PPTP 的延伸, 互联网服务提供商 (ISP) 使用该协议实现互联网上的 VPN。L2TP 不会为它传输的数据提供加密。要对数据进行加密, 需要使用其他安全协议 (如 IPsec)。

L2TP 隧道建立在 L2TP 访问集中器 (LAC) 和 L2TP 网络服务器 (LNS) 之间。这些设备之间也建立了 IPsec 隧道, 并且所有 L2TP 隧道流量均使用 IPsec 加密。

要配置 L2TP 服务器, 请按照以下步骤操作:

步骤 1 单击 **VPN > L2TP 服务器**。

步骤 2 提供以下信息:

L2TP 服务器	选中打开或关闭以启用或禁用 L2TP 服务器。
最大传输单位	可通过 L2TP 隧道发送的最大数据包的大小。如果 L2TP 已启用, 输入数据包的大小 (范围: 128-1400, 默认值: 1400)。
用户验证	选择用户验证 (组名称 或 管理员)。

地址池	<ul style="list-style-type: none"> • 起始 IP 地址 — 输入起始 IP 地址。 • 结束 IP 地址 — 输入结束 IP 地址。
DNS1 和 DNS2 IP 地址	输入 DNS1 和 DNS2 服务器的主 IP 和辅助 IP 地址。
IPSec	选中打开为 L2TP 隧道启用 IPSec 安全。
IPSec 配置文件	默认
预先共享密钥	输入用于验证远程 IKE 对端的预先共享密钥。最多可以输入 30 位键盘字符或十六进制值，例如 My_@123 或 4d795f40313233。VPN 隧道两端必须使用相同的预先共享密钥。建议定期更改预先共享密钥，以便最大限度地提高 VPN 的安全性。
确认预先共享密钥	重新输入预先共享密钥进行确认。

步骤 3 单击应用。

SSL VPN

利用安全套接字层虚拟专用网络 (SSL VPN)，用户可以通过对网络流量进行加密，使用安全且经过验证的路径远程访问受限制的网络。路由器支持思科 AnyConnect VPN 客户端（可在 [<http://www.cisco.com/go/anyconnect/>] 下载）。默认情况下，路由器支持 2 个 SSL VPN 隧道，用户可通过注册许可证使路由器最多支持 50 个通道。完成安装和激活后，SSL VPN 将创建一个安全的远程访问 VPN 隧道。



注释 此外，如需在您的设备上安装和使用思科 AnyConnect 安全移动客户端，必须具有思科 AnyConnect 安全移动客户端许可证。有关如何订购思科 AnyConnect 安全移动客户端许可证的详情，请访问 <http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf>。我们推荐适合 25-99 名用户的 AnyConnect Plus 许可证。

要配置 SSL VPN，请按照以下步骤操作：

步骤 1 单击 **VPN>SSL VPN**。

步骤 2 在“常规配置服务器”选项卡中，提供以下信息：

思科 SSL VPN 服务器	选择打开或关闭以启用或禁用服务器。
----------------	-------------------

强制网关设置

网关接口	从下拉列表中选择网关接口（WAN1、WAN2、USB1 或 USB2）。
网关端口	输入网关端口号（范围：1 到 65535）。
证书文件	默认。
客户端地址池	输入客户端地址池的 IP 地址。
客户端子网掩码	输入客户端子网掩码。
客户端域	输入客户端域名。
登录横幅	输入要显示为登录横幅的文本。

可选网关设置

空闲超时	输入以秒为单位的空闲超时值（范围：60 到 86,400）。
会话超时	TCP 或 UDP 会话闲置多长时间后会超时。输入以秒为单位的会话超时值（范围：60 到 1,209,600）。
客户端 DPD 超时	定期发送 HELLO/ACK 消息以检查 VPN 隧道的状态。必须在 VPN 隧道两端同时启用此功能。在“间隔”字段中指定 HELLO/ACK 消息之间的时间间隔。输入以秒为单位的客户端 DPD 超时值（范围：0 到 3600）。
网关 DPD 超时	定期发送 HELLO/ACK 消息以检查 VPN 隧道的状态。必须在 VPN 隧道两端同时启用此功能。在“间隔”字段中指定 HELLO/ACK 消息之间的时间间隔。输入以秒为单位的网关 DPD 超时值（范围：0 到 3600）。
保持活动	确保路由器始终连接到互联网。如果连接断开，则尝试重新建立 VPN 连接。输入以秒为单位的保持活动状态值（范围：0 到 600）。
租用期限	输入以秒为单位的隧道连接时间值（范围：600 到 1,209,600）。
最大 MTU	以字节为单位，输入可以通过网络发送的数据包大小（范围：576 到 1406）。
中继间隔	以秒为单位，输入中继间隔时间值（范围：0 到 43,200）。

步骤 3 单击应用。

步骤 4 在“组策略服务器”标签中，单击添加并提供以下信息。

基本设置

策略名称	输入策略名称。将整组属性应用于一组用户，而不是分别为每个用户指定各个属性的组策略。
主 DNS	输入主 DNS 服务器的 IP 地址。

辅助 DNS	输入辅助 DNS 服务器的 IP 地址。
主 WINS	输入主 WINS 的 IP 地址。
辅助 WINS	输入辅助 WINS 的 IP 地址。
说明	输入说明。

IE 代理设置

IE 代理策略	<p>用于建立 VPN 隧道的 Internet Explorer 代理设置。从下拉列表中选择 IE 代理策略（无、自动、绕过本地或已禁用）。</p> <p>如果您选择自动或绕过本地，请输入以下信息：</p> <ul style="list-style-type: none"> • 地址 — IP 地址或域名。 • 端口 — 输入端口号（范围：1 到 65,535）。
---------	---

- 步骤 5** 在“IE 例外情况代理”表中，单击添加、编辑或删除，以添加、编辑或删除 IE 例外情况。
拆分隧道设置

启用拆分隧道	选中启用拆分隧道以允许互联网预定的流量未经加密直接发送至互联网。“全隧道”将所有流量发送至终端设备，然后在该处路由至目标资源（消除了通过 Web 访问企业网络路径）。
拆分选项	应用拆分隧道时，您可以选择包含流量以包含流量，也可以选择排除流量。

- 步骤 6** 在“拆分网络”表中，单击添加、编辑或删除，以添加、编辑或删除 DNS 例外情况。
步骤 7 配置 IP 和子网掩码。
步骤 8 单击应用。

VPN 通道

借助“VPN 通道”，VPN 客户端可通过路由器顺利连接至 VPN 端点。默认情况下，此功能处于启用状态。

要配置 VPN 通道，请按照以下步骤操作：

步骤 1 选择 **VPN > VPN 通道**。

步骤 2 要启用 VPN 通道，请为获得批准的各个协议选中**启用**：

- **IPSec 通道** — 互联网协议安全 (IPSec) 是一套用于在 IP 层实现数据包安全交换的协议。
- **PPTP 通道** — 点对点隧道协议 (PPTP) 允许通过 IP 网络传输点对点协议 (PPP)。
- **L2TP 通道** — 第 2 层隧道协议是一种通过第 2 层上的互联网来启用点对点会话的方法。

步骤 3 单击**应用**。



第 12 章

安全

本节介绍网络安全，其中涵盖用于防止和监控未授权访问、误用、修改或拒绝计算机网络的策略。本节包含以下主题：

- [应用控制向导](#)，第 105 页
- [应用控制](#)，第 106 页
- [Web 过滤](#)，第 107 页
- [内容过滤](#)，第 108 页
- [IP 源防护](#)，第 108 页

应用控制向导

要添加、配置或修改应用控制策略，请按照以下步骤操作：

-
- 步骤 1** 单击**安全 > 应用控制向导**。
 - 步骤 2** 在“应用控制”页面上，选择**打开**，并输入策略名称。
 - 步骤 3** 单击**下一步**，并在“应用列表”上方单击**编辑**，以配置需要过滤（或者需要阻止或记录到日志）的应用名称。选择需要过滤的内容后，单击**应用**。
 - 步骤 4** 单击**下一步**，并从下拉列表中选择计划表，以阻止应用。
 - 步骤 5** 单击**提交**。
-

应用控制

要添加、配置或修改应用控制策略，请按照以下步骤操作：

- 步骤 1** 单击安全 > 应用控制。
- 步骤 2** 在“应用控制”页面上，选择打开，并单击应用。
- 步骤 3** 要创建新的应用控制策略，请在“应用控制策略”表下单击添加。
- 步骤 4** 在“策略配置文件-添加/编辑”部分指定以下信息：

策略名称	输入名称。
说明	输入说明。
启用	选中可执行应用控制策略。
应用	单击编辑，从列表中选择需要过滤（或者需要阻止或记录到日志）的内容，然后单击应用。
应用列表	显示已配置的过滤器的“类别”、“应用”和“行为”的列表。
设备类型	从下拉列表中选择设备类型。
操作系统类型	从下拉列表中选择操作系统。
IP 组	从下拉列表中选择一个 IP 组以应用策略。
排除列表	在“排除列表”下，单击添加并配置以下设置： <ul style="list-style-type: none"> • 类型（选择“Mac”或“IP 组”） • IP/MAC — 输入 MAC 地址 • 设备类型 — 选择设备类型 • 操作系统类型 — 选择操作系统类型
计划表	此项用于指定应用控制策略何时处于活动状态，可从下拉列表中选择计划表，也可以单击始终开启应用 Web 过滤。

- 步骤 5** 完成设置后，单击应用。

Web 过滤

Web 过滤功能可防止您访问不当网站。它可以筛查客户端的 Web 访问请求，确定允许还是拒绝该网页。要启用并配置 Web 过滤，请按照以下步骤操作：

步骤 1 单击安全 > Web 过滤。

步骤 2 在“Web 过滤”部分，选择打开或关闭，然后单击应用。

步骤 3 在“Web 过滤策略”表中，单击添加。要编辑现有的策略，可单击编辑对其进行修改。

步骤 4 在“Web 过滤 - 添加/编辑策略”页面中，输入以下信息：

策略名称	为您正在创建的 Web 过滤策略指定名称。
说明	输入对策略的简要说明。
启用	选中启用以激活策略。
类别	<ul style="list-style-type: none"> 单击编辑并选择所需的过滤级别（选择要过滤的适当 Web 类别）。选择高、中、低或自定义，以定义过滤范围。还可以从成人内容、商业/投资、娱乐、非法/可疑、IT 资源、时尚/文化、其他和安全类别中选择项目。系统会阻止属于所选项目的传入 URL。 单击应用可回到 Web 过滤 - 添加/编辑策略页面。您可以看到所选 Web 内容已列在类别下的申请列表中。 单击恢复为默认类别可恢复默认设置。
设备类型	从下拉列表中选择应应用策略的设备类型。
操作系统类型	从下拉列表中选择应应用策略的操作系统。
Web 信誉	选中可启用 Web 信誉分析。
在 IP 组中应用	从下拉列表中选择应应用此策略的 IP 组。
例外情况列表	<p>单击编辑，然后添加并定义以下设置：</p> <ul style="list-style-type: none"> 白名单 — 单击添加可定义绕过此策略的域名或关键词。 黑名单 — 单击添加可定义应阻止的域名或关键词。 例外情况列表 — 单击添加可指定从此策略中排除的 IP 地址。 <p>单击应用。</p>
计划表	从下拉列表中选择所需的计划表。单击始终开启，应用 Web 过滤。

步骤 5 单击**确定**，保存相关配置。

内容过滤

内容过滤用于限制某些不希望的网站，阻止它们访问客户端。它可以根据域名和关键字阻止访问网站，还可以通过计划表设置内容过滤的生效时间。

要配置和启用内容过滤，请按照以下步骤操作：

步骤 1 单击**安全 > 内容过滤**。

步骤 2 选中**启用内容过滤**以启用该功能。

步骤 3 选择所需单选按钮。

阻止匹配的 URL	选中 阻止匹配的 URL 以阻止特定的域和关键字。
仅允许匹配的 URL	选中 仅允许匹配的 URL 以仅允许指定的域和关键字。

步骤 4 在“按域过滤”表下，单击**添加**。

步骤 5 在“域名”列中输入要过滤/允许的域。

步骤 6 要指定内容过滤规则的生效时间，请从“计划表”下拉列表中选择计划表。

步骤 7 在“按关键字过滤”下，单击**添加**。

步骤 8 在“关键字名称”列中输入要阻止/允许的关键字。

步骤 9 要指定内容过滤规则的生效时间，请从“计划表”下拉列表中选择计划表。通过选择名称并单击**编辑**，可修改现有域名或关键字名称。

步骤 10 单击**应用**。

IP 源防护

IP 源防护是一种安全功能，它根据配置的 IP MAC 绑定过滤流量，从而限制不受信任的 IP 和 MAC 地址上的 IP 流量。这是一种过滤器，仅当每个数据包的 IP 地址和 MAC 地址与 IP-MAC 绑定表中的条目匹配时，才允许 LAN 端口上的流量。当一台主机尝试仿冒和使用另一台主机的 IP 地址时，此功能可以帮助防止 IP 欺骗攻击。

要配置 IP 源防护，请按照以下步骤操作：

步骤 1 单击**安全 > IP 源防护**。

步骤 2 如果需要 IP 和 MAC 绑定，选中**启用 IP 源防护**。

步骤 3 如果只需要过滤 MAC 地址而不需要考虑 IP 地址，选中**阻止未知 MAC 地址**。

步骤 4 在“IP 和 MAC 绑定表”中，单击**添加**，并输入静态 IPv4 地址和 MAC 地址进行绑定。

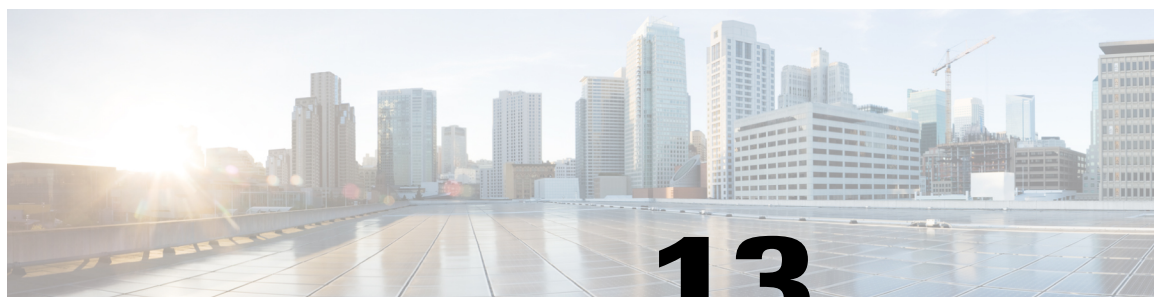
步骤 5 单击**应用**。

步骤 6 单击**编辑**或**删除**以编辑或删除现有地址。

注释 “DHCP 租用表”列出了 DHCP 服务器/中继的所有可用的静态 DHCP 和动态租用。单击**添加到 IP 和 MAC 绑定表**，以将可用租用添加到绑定表。

您必须手动将 DHCP 租借条目添加到 IP 和 MAC 绑定表。只有 IP 和 MAC 绑定表中的条目将工作。

注释 IP Source Guard 仅在 RV340W 的有线主机上工作，而不是无线



第 13 章

快速索引

本节包含以下主题：

- [快速索引](#)，第 111 页

快速索引

支持

思科支持社区	http://www.cisco.com/go/smallbizsupport
思科支持和资源	http://www.cisco.com/go/smallbizhelp
电话支持联系人名单	http://www.cisco.com/c/en/us/support/web/tsd-cisco-small-business-support-center-contacts.html
思科固件下载	http://www.cisco.com/go/smallbizfirmware 选择链接，可下载相应思科产品的固件。无需登录。
思科开源请求	如果希望接收在适用的免费/开源许可证（例如 GNU 宽松/通用公共许可证）下您有权获得的源代码副本，请将您的请求发送至： external-opensource-requests@cisco.com 。 请在您的请求中提供思科产品名称、版本和 18 位参考号（例如：7XEEX17D99-3X49X081），此参考号可以在产品的开源文档中找到。
思科合作伙伴中心（需要合作伙伴登录）	http://www.cisco.com/c/en/us/partners.html
思科 RV340W 路由器	http://www.cisco.com/en/US/products/ps9923/tsd_products_support_series_home.html

