# RV345/RV345P 管理指南

首次发布日期: 2016 年 6 月 9 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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

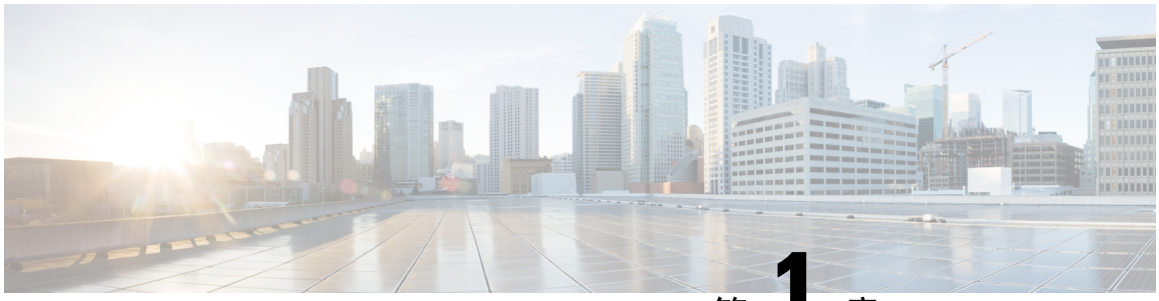
NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com go trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

# 目录



第 1 章

# 使用入门

感谢您选择思科 RV345/RV345P。本指南介绍如何安装和管理此设备。思科 RV345/Rv345P 自带默认设置，但互联网运营商 (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：



## 设置您的设备

本节将帮助您完成设备的初始设置，具体步骤如下：

**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。

系统启动时间通常不到 3 分钟。如果设备完全配置，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: LED 说明***

| | |
|---|---|
| **PWR（电源）** | 熄灭表示设备电源关闭。<br>绿色常亮表示设备电源开启且设备已启动。<br>绿色闪烁表示设备正在启动。 |

使用入门

| | |
|---|---|
| **DIAG（诊断）** | 熄灭表示系统正在启动。<br>红色慢闪 (1Hz) 表示系统正在进行固件升级。<br>红色快闪 (3Hz) 表示系统固件升级失败。<br>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。 |
| **LINK/ACT（链路/活动）（WAN1、WAN2 和 LAN 1-16）** | 熄灭表示端口未建立以太网连接。<br>绿色常亮表示端口已建立千兆以太网链路。<br>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。 |
| **GIGABIT（千兆）（WAN1、WAN2 和 LAN 1-16）** | 绿色常亮表示数据传输速度为 1000M。<br>熄灭表示数据传输速度不是 1000M。 |
| **DMZ（隔离区）** | 绿色常亮表示已启用 DMZ。<br>熄灭表示已禁用 DMZ。 |
| **VPN** | 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。<br>绿色常亮表示至少有一条 VPN 隧道处于活动状态。<br>绿色闪烁表示正在通过 VPN 隧道发送和接收数据。<br>琥珀色常亮表示已启用的 VPN 隧道处于非活动状态。 |
| **USB1 和 USB2** | 熄灭表示端口未连接 USB 设备或无法识别已插入的 USB 设备。<br>USB 装置成功连接到互联网运营商 (ISP)且 USB 存储装置已被识别。<br>绿色闪烁表示端口正在发送和接收数据。<br>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。 |
| **RESET（重置）** | 要重新启动设备，请使用曲别针或笔尖按住 RESET（重置）按钮不超过 10 秒。<br>要将设备重置为出厂默认设置，请按住 RESET（重置）按钮 10 秒。 |

# 使用入门

您可以使用此页面中提供的各种链接，按照屏幕上的指示快速配置您的网络设备。

**配置向导**

| | |
|---|---|
| **初始设置向导** | 将您定向至**初始设置向导**。 |
| **应用程序控制向导** | 将您定向至**应用程序控制向导**。 |

| | |
|---|---|
| **VPN 设置向导** | 将您定向至 **VPN 状态向导**。 |

初始配置

| | |
|---|---|
| **更改管理员密码** | 将您定向至**用户账户**页面，您可以在其中更改管理员密码和设置访客账户。 |
| **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 VLAN 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，您可以在其中管理设备配置。 |

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。

### 注销

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。

用户界面的设计便于进行设备设置和管理。下表介绍标题工具栏的图标。

**表 *2:*** 标题工具栏选项

| 图标 | 说明 |
|---|---|
|  | **切换按钮** – 位于标题栏的左上方，此切换按钮用于展开或折叠导航窗格。 |
|  | **语言选择** – 通过此下拉列表可选择用户界面的语言。 |
|  | **帮助** – 设备的在线帮助文档。 |
|  | **关于** – 设备的固件版本信息。 |
|  | **注销** – 单击可注销设备。 |

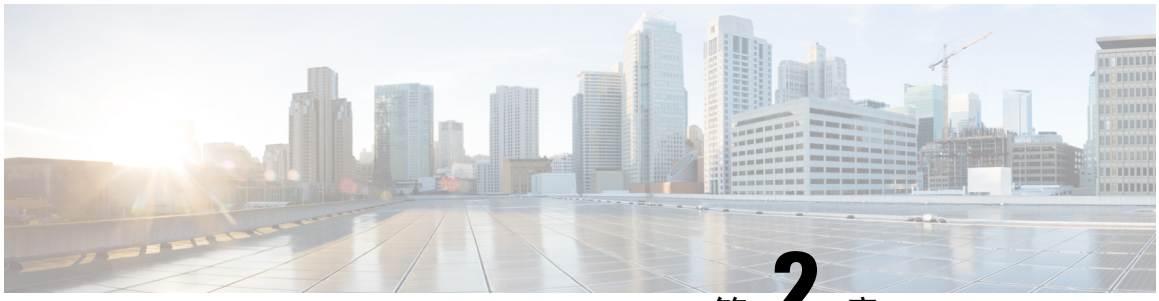
### 图标图例

此表列出图形界面中最常见的图标及相应的含义。

| | |
|---|---|
|  | **添加** - 单击此图标可添加一个条目。 |
|  | **编辑** - 单击此图标可编辑条目。 |
|  | **删除** - 单击此图标可删除一个条目。 |
|  | **刷新** - 单击此图标可刷新数据。 |
|  | **重置计数器** - 单击此图标可重置计数器。 |
|  | **复制** - 单击此图标可复制设置。 |
|  | **导出** - 单击此图标可导出配置。 |
|  | **导入** - 单击此图标可导入配置。 |
|  | **保存** - 单击此图标可保存配置。 |
|  | **连接** - 单击此图标可进行连接。 |
|  | **断开** - 单击此图标可断开连接。 |

### 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。



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

“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。
- **WAN1 MAC 地址** – WAN1 的 MAC 地址。
- **WAN2 MAC 地址** – WAN2 的 MAC 地址。
- **LAN MAC Address** – LAN 的 MAC 地址。

### 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。
- **链路状态** – 链路的状态。
- **速度状态** – 自动协商后设备的速度（以 Mbps 为单位）。

### 无线射频状态

**频段 1 (2.4GHz) 和频段 2 (5GHz)**

- **无线频段** – 显示无线频段是处于启用状态还是禁用状态。
- **MAC 地址** – 无线连接的 MAC 地址。
- **模式** – 支持的无线网络：2.4 GHz 频段为 802.11b/g/n；5 GHz 频段为 802.11a/n/ac。
- **通道** – 无线连接的带宽通道：2.4 GHz 频段为通道 11；5 GHz 频段为通道 42。
- – 无线频段的运行带宽：2.4 GHz 频段为 20/40MHz；5 GHz 频段为 80MHz。

### 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”。
- **多 WAN 状态** – 显示多 WAN 状态：“脱机”或“联机”。
- **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。

- **已启用** – **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。
- **已连接会话数** – 隧道的当前状态。

### 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 地址的状态。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** – 连接的设备的 IP 地址。
- **外部端口** – 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。
- **端口标签** – 端口的名称。
- **链路状态** – 链路的状态。
- **接收的数据包数** – 端口上接收的数据包数量。
- **接收的字节数** – 接收的数据包数量（以字节为单位）。
- **发送的数据包数** – 端口上发送的数据包数量。
- **发送的字节数** – 发送的数据包数量（以字节为单位）。
- **错误数据包数** – 设备未成功接收的数据包数量。

### 无线流量 (RV340W)

- **SSID 名称** – SSID 的名称。
- **VLAN** – VLAN ID。
- **频段名称** – 无线电频段的名称。
- **状态** – 无线状态。
- **接收的数据包数** – 端口上接收的数据包数量。
- **接收的字节数** – 接收的数据包数量（以字节为单位）。
- **发送的数据包数** – 端口上发送的数据包数量。
- **发送的字节数** – 发送的数据包数量（以字节为单位）。
- **组播数据包数** – 设备传输的组播数据包数量。
- **错误数据包数** – 设备未成功接收的数据包数量。
- **丢弃的数据包数** – 设备丢弃的数据包数量。

- **冲突包数** – 设备上发生冲突的数据包数量。
- **客户端数** – 连接到无线网络的客户端（设备）数量。

端口状态

- **端口 ID** – 定义的端口名称和编号。
- **端口标签** – 端口的名称。
- **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（具有正反接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。
- **发送的数据包数** – 已发送的流量类的出站数据包的数量。
- **丢弃的数据包数** – 已丢弃的出站数据包的数量。

入站 **QoS** 统计信息

- **队列** – 入站队列的数量。
- **流量类** – 分配给队列的流量类的名称。

- **发送的数据包数** – 已发送的流量类的入站数据包的数量。
- **丢弃的数据包数** – 已丢弃的入站数据包的数量。

# ARP 表

ARP 表会列出当前已连接的所有设备及其统计信息。

要打开“已连接的设备”页面，请单击**状态和统计信息 > ARP 表**。

- **主机名** – 连接的设备的名称。
- **IPv4** – 连接的设备的 IPv4 地址。
- **MAC 地址** – 连接的设备的 MAC 地址。
- **类型** – 显示设备 IP 地址的类型。
- **接口** – 显示连接所使用的接口。

### IPv6

- **IPv6 地址** – 显示连接的设备的 IPv6 地址。
- **MAC 地址** – 连接的设备的 MAC 地址。

# 路由表

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。路由表包含有关其直接关联的网络的拓扑信息。要查看 IPv4 和 IPv6 路由，请单击**状态和统计信息 > 路由表**。

### 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（已连接、动态）。

# DHCP 绑定

“DHCP 绑定”表会显示 IPv4/IPv6 地址、MAC 地址、租用到期时间和绑定类型（静态或动态）等 DHCP 客户端信息的状态。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/IPv6 地址** – 为客户端分配的 IP 地址。
- **MAC 地址** – 客户端已分配的 IP 地址的 MAC 地址。
- **租用到期时间** – 客户端系统的租用时间。
- **类型** – 显示连接状态（**静态**或**动态**）。
- **操作** – 允许您从绑定表中删除一个连接。

# 移动网络

移动网络可为设备及其子网提供移动性支持，同时确保 IP 连接对通过该移动设备连接到网络的 IP 主机仍然透明要查看设备的移动网络，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** – 运营商提供的 IP 地址。
- **子网掩码** – 运营商提供的掩码。
- **默认网关** – 运营商提供的默认网关。
- **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”）。

# 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：<br>• **全部** – 显示所有日志。<br>• **类别** – 显示所选类别的日志。 |
| **严重性** | 选择显示的某个选项，以查看根据严重程度显示的日志。 |
| **搜索关键字** | 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 26 页。

**步骤 4** 单击以下任意选项：

- **刷新** – 单击此项可刷新日志。
- **清除日志** – 单击此项可清除日志。
- **将日志导出到 PC** – 单击此项可将日志导出到 PC。
- **将日志导出到 USB** – 单击此项可将日志导出到 USB 存储设备。

# 网页认证状态

网页认证可利用多种权限和角色实现高度安全的自定义访客接入。此功能可为来访的顾客提供高度安全的无线互联网接入，并为使用个人移动设备的员工提供快速验证和连接。

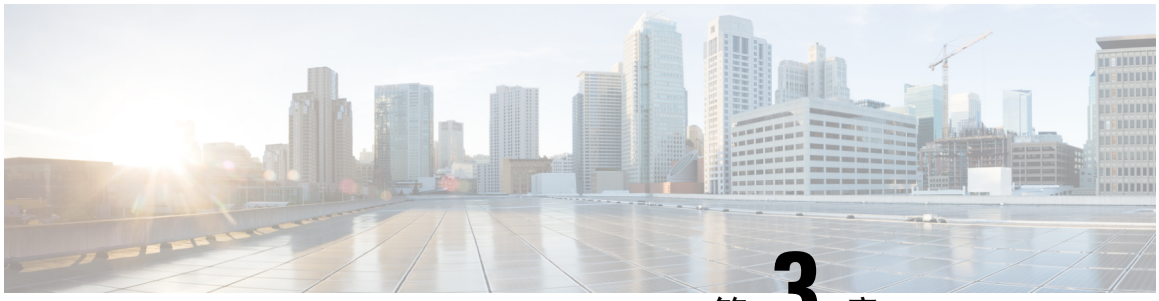
要打开并查看网页认证状态，请单击**状态和统计信息 > 网页认证状态**。

从下拉列表选择所需的 SSID，以显示下列详细信息。

**步骤 1** 从下拉列表选择所需的 SSID，以显示下列详细信息：

- **用户名** – 已连接的用户的名称。
- **SSID** – 网络的名称。
- **IP 地址** – 运营商提供的 IP 地址。
- **MAC 地址** – 运营商提供的掩码。
- **验证** – 运营商提供的默认网关。
- **发送的字节数** – 发送的数据包数量（以字节为单位）。
- **接收的字节数** – 接收的数据包数量（以字节为单位）。
- **连接时间** – 连接设备的持续时间。

**步骤 2** 选择所需的用户，然后单击**断开**可断开设备的连接。单击**刷新**可刷新页面上的数据。



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

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**可查看以下信息：

系统信息

- **设备型号** – 设备的型号。
- **PID VID** – 设备的 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。

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，并导致设备无法使用。

**步骤 2** 如果选择从 USB 驱动器升级，设备将搜索 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，设备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

要使用较新版本的固件更新设备，请执行以下操作：

**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，设备将支持从 USB 闪存驱动器中加载固件。设备会搜索 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，设备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。

设备还支持在系统启动期间，从 USB 闪存驱动器中加载配置文件。

- 此行为仅在设备处于出厂默认设置状态，且在接通电源前连接了 USB 闪存时发生。
- 设备会搜索 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，设备将检查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。

### 固件自动回退机制

设备的闪存中包含两个固件映像，用于提供自动回退机制，如果主用固件损坏或者在五次尝试后未能成功引导，设备会自动切换至辅助固件。

自动回退机制按以下方式工作：

1. 设备首先使用主用固件引导。
2. 如果固件损坏，当使用主用固件引导失败达 5 次后，设备会自动切换至辅助固件。如果设备宕机，无法自动重新引导，您可以关闭电源，打开电源，等待 30 秒后再次关闭电源，重复此过程 5 次，以便手动切换至辅助固件或备用固件。
3. 在使用辅助固件或备用固件完成引导后，请检查主用固件是否出现问题。
4. 如果需要，请再次重新加载新固件。

# 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

您可以使用 Ping 或 Trace 实用程序测试此设备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**。

# 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”中显示与设备相关联的证书。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**。

# 内置第三方 CA 证书

**步骤 1** 单击**显示内置第三方 CA 证书**。

**步骤 2** 从证书表中选择一项证书，然后单击**导出**。

**步骤 3** 请选择以下选项之一：

- 导出为 PKCS#12 格式 – 选择此选项可将相应的证书以 PKCS#12 格式导出。
- 导出为 PEM 格式 – 选择此选项可导出 PEM 类型的证书。
- 选择导出目标 – 使用此选项可选择导出至 PC 或 USB。

# 选择作为主证书

**步骤 1** 单击**选择作为主证书**。

**步骤 2** 在证书表中，选中与所需证书对应的复选框，然后单击**选择作为主证书**。

# 配置管理

“配置管理”页面提供有关设备文件配置的详细信息。

### 配置文件名称

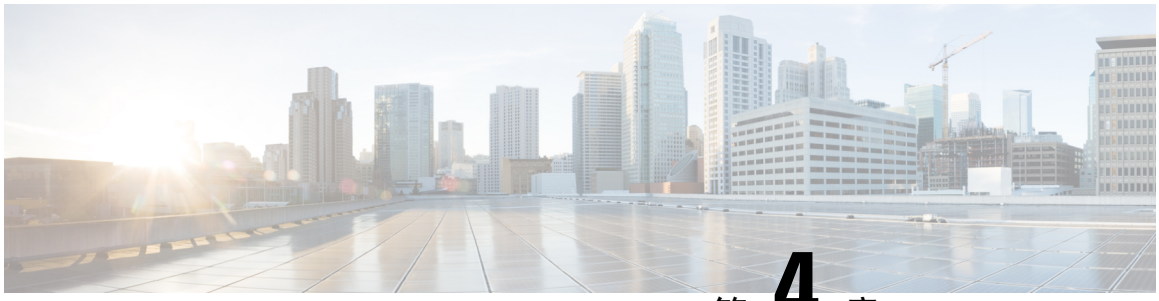
“配置文件名称”显示以下内容的最后更改时间详细信息：

- **正在运行的配置** – 设备当前使用的所有配置均包含在“正在运行的配置”文件中，该文件为易失性文件，每次重启后均会丢失。
- **启动配置** – 包含最后保存的所有配置，设备重新引导后会加载到“正在运行的配置”文件中。
- **镜像配置** – 设备在稳定状态下运行 24 小时（即 24 小时内未重新启动且配置未更改）后，会自动将启动配置复制到镜像配置。
- **备份配置** – 这是配置文件的额外副本，作为备份保存。除非被覆盖，否则将保留不变。

### 复制/保存配置

“复制/保存配置”部分会显示使用“正在运行的配置”文件的设备的默认配置，该文件并不稳定，而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** – 从下拉列表选择源文件名。
- **目标名** – 从下拉列表选择目标文件名。
- **保存图标闪烁** – 表明当存在未保存的数据时，保存图标是否会闪烁。要禁用/启用此功能，可单击**保存图标闪烁已启用**或**保存图标闪烁已禁用**。



第 4 章

# 系统配置

本节提供有关设备安装和配置的指导，其中包含以下主题：



## 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** - 选择以格林威治标准时间 (GMT) 为基准的时区。

**步骤 3** **设置日期和时间** - 选择**自动**或**手动**。

a) **自动** - 对于 NTP 服务器，选中**默认**，或选择**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）。这是一个内存区域，用于临时存储可撤销的操作，直到这些操作被写入磁盘。可接受的大小范围为 1 至 4096 KB，默认大小值为 1024 KB。

**步骤 4** 从“严重性”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** 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** | 与用户空间应用程序（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。 |
| **应用程序控制** | 与应用程序控制相关的日志。 |
| **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** | 来自于设备上连接的 3G/4G 装置的日志。 |
| **SSLVPN** | 与 SSLVPN 相关的日志。 |
| **PnP** | 与思科即插即用功能相关的日志。 |

**步骤 6** 要将日志保存到 USB 驱动器，请选中**自动保存到 USB**，然后选择用于保存日志的 USB。

# 电子邮件服务器

电子邮件服务器可以配置为电子邮件账户。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。设备支持 SMTP 邮件账户配置。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**，使设备在记录事件时发送电子邮件警报。

**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 范围之内的长度。默认为 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”字段中，输入以下信息：

| | |
|---|---|
| **系统日志服务器 1** | 输入除本地目标以外，日志消息所要发送到的系统日志服务器的 IP 地址。 |
| **传输** | 选择 UDP 或 TCP。 |
| **端口** | 输入系统日志服务器的端口值。 |
| **系统日志服务器 2** | 输入除本地目标以外，日志消息所要发送到的系统日志服务器的 IP 地址。 |
| **传输** | 选择 UDP 或 TCP。 |
| **端口** | 输入系统日志服务器的端口值。 |

**步骤 3** 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** | 对于电子邮件加密方法，您可以选择**无**或 **TLS/SSL**。 |

| | |
|---|---|
| **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** | 输入发件人的电子邮件地址。 |

**步骤 3** 单击**应用并测试与电子邮件服务器的连接**以测试连接。如果您想清除设置，请单击**清除**。

**步骤 4** 单击**应用**。

# 用户账户

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 > 用户账户**。

**步骤 2** 在“Web 登录会话超时”下，输入以下信息。

| | |
|---|---|
| **管理员空闲超时** | 输入所需的管理员空闲超时时间值。默认值为30分钟。 |
| **访客空闲超时** | 输入所需的访客空闲超时时间值。默认值为 30 分钟。 |

**步骤 3** 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 4** 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。 |
| **密码过期时间** | 输入密码过期天数值。(范围：0-365，0 表示从不过期）。 |

**步骤 5** 在“本地用户成员列表”部分，单击**添加**来添加用户，然后输入以下信息：

| | |
|---|---|
| **用户名** | 输入用户名。 |
| **新密码** | 输入密码。 |
| **新密码确认** | 确认密码。 |

| | |
|---|---|
| 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**导入**以导入用户账户。您也可以使用“下载”按钮下载用户模板。

**步骤 8** 要使用 RADIUS、LDAP 和 AD 进行外部用户验证，可使用远程验证服务。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。 |
| 新密码 | 输入要对用户账户使用的密码。 |
| 验证类型 | 选择验证类型：RADIUS（远程验证拨入用户服务）、Active Directory (AD) 或 LDAP。 |
| 主服务器 | 输入 RADIUS/Active Directory/LDAP 服务器的主 IP 地址。<br>端口：输入服务器的备用端口。 |
| 备份服务器 | 如果验证类型已选为 RADIUS，请输入服务器的备用 IP 地址。<br>端口：输入服务器的备用端口。 |
| 用户容器路径 | 如果验证类型已选为 Active Directory，请输入用户容器的完整路径信息。这也是用于验证的用户登录信息。 |
| 基本 DN | 如果验证类型已选为 LDAP，请输入 LDAP 服务器的基本可分辨名称 (DN)。基本 DN 是 LDAP 服务器在收到验证请求后搜索用户的位置。此字段应与 LDAP 服务器上配置的基本 DN 完全相同。 |
| 预共享密钥 | 如果验证类型已选为 RADIUS，则输入 RADIUS 服务器的预共享密钥。 |
| 确认预共享密钥 | 重新输入 RADIUS 服务器的预共享密钥以进行确认。 |

**步骤 9** 单击**应用**。

**步骤 10** 要启用服务验证顺序，请输入以下信息：

| | |
|---|---|
| 服务 | 您可以自定义以下服务的配置：<br>• Web 登录<br>• 站点到站点/Ez VPN 和第三方客户端到站点 VPN<br>• AnyConnect SSL VPN<br>• PPTP 服务器<br>• L2TP 服务器<br>• 802.1x<br>**注释** 对于 PPTP 服务器、L2TP 服务器和 802.1x，系统仅支持“本地数据库”和“RADIUS”验证类型。 |

| | |
|---|---|
| **使用默认设置** | 您可以根据所需的服务配置选择启用或禁用此项。对于“Web 登录”、“站点到站点/Ez VPN”、“第三方客户端到站点 VPN”，以及“AnyConnect SSL VPN”服务，系统会默认启用“使用默认设置”。<br>**注释** 如果启用此选项，“自定义 - 主要”和“自定义 - 辅助”选项将被禁用。 |
| **自定义：主要** | 您可以选择所需的主验证类型：无、本地数据库、RADIUS（远程验证拨入用户服务）、LDAP 或 Active Directory。 |
| **自定义：辅助** | 您可以选择所需的辅助验证类型：无、本地数据库、RADIUS（远程验证拨入用户服务）、LDAP 或 Active Directory。 |

**步骤 11** 单击**应用**。

# 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** | 从下拉列表中选择验证类型：<br>• **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。<br>• **Active Directory** – 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。<br>• **LDAP** – 轻型目录访问协议。 |
| **主服务器** | 输入主服务器的 IP 地址。<br>**端口** – 输入服务器的主端口。 |
| **备份服务器** | 输入备份服务器的 IP 地址。<br>**端口** – 输入服务器的备用端口。 |
| **预共享密钥** | 如果验证类型已选为 RADIUS，则输入 RADIUS 服务器的预共享密钥。 |
| **确认预共享密钥** | 重新输入 RADIUS 服务器的预共享密钥以进行确认。 |

**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。如果您在设备上添加 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。在设备上创建并启用 RADIUS 后，设备将使用 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/NETCONF/RESTCONF** | 指定向添加到组的用户授予的 Web 登录权限：<br>• **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。<br>• **只读** – 用户组成员在登录后只能读取系统状态，而无法编辑任何设置。<br>• **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。<br>• 单击**添加**打开**添加功能列表**弹出窗口。<br>• 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。<br>• 单击**添加**打开**添加功能列表**弹出窗口。<br>• 从下拉列表中选择配置文件，然后单击**添加**。 |
| **SSL VPN** | 要允许此组访问特定策略，请从“配置文件”下拉列表中选择一个配置文件。 |
| **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。 |

| | |
|---|---|
| 网页认证 | 对此群组选中“允许”复选框可对此组启用网页认证。单击**添加**可打开“添加功能列表”弹出窗口。从下拉列表中选择一个配置文件，然后单击**添加**。 |

**步骤 6** 单击**应用**。

# IP 地址组

为了配置和管理应用程序控制策略与 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 | 从下拉列表中选择组类型，并输入地址详细信息：<br>• **IP 地址** – 在“IP 地址”字段中输入 IP 地址。<br>• **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。<br>• **IP 地址范围** – 输入“起始 IP 地址”和“结束 IP 地址”。 |
| 地址详细信息 | 输入要添加到该 IP 组的设备的 MAC 地址。 |
| 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类型。 |

**步骤 4** 要添加设备，请单击**添加**，然后配置以下设置：

| 选项 | 描述 |
|---|---|
| MAC 地址 | 输入要添加到该 IP 组的设备的 MAC 地址。 |
| 设备和操作系统类型 | 从下拉列表中选择适当的设备类型和操作系统。 |

**步骤 5** 单击**应用**。

# SNMP

简单网络管理协议 (SNMP) 是一种互联网标准协议，它用于收集和组织有关 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。

利用简单网络管理协议(SNMP)，网络管理员可以在网络上发生关键事件时对这些事件进行管理和监控，并接收通知。设备支持 SNMP 版本 v1、v2c 和 v3。设备将充当 SNMP 代理，对来自 SNMP 网络管理系统的 SNMP 命令进行响应。它所支持的命令是标准 SNMP 命令：get、next 和 set。此外，它还会生成陷阱消息，从而在达到警报条件时通知 SNMP 管理器。相关示例包括重新引导、重新启动以及 WAN 链路事件。

**步骤 1** 要配置设备的 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。 |

**步骤 2** 在“陷阱配置”部分，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** 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设备上的故障和其他偶发性问题。为此，您可以对设备进行配置，以便在设备有重要固件更新时接收电子邮件通知。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**。

# 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**。

# 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**应用程序名称**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：（**全部**、**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**。

# PnP（即插即用）

思科 Open Plug-n-Play 代理是一种在思科 SMB 设备上运行的软件应用程序。当设备开启后，设备中内嵌的 Plug-n-Play 代理发现进程会尝试发现 Open Plug-n-Play 服务器的地址。Open Plug-n-Play 代理会使用 DHCP、域名系统 (DNS) 和思科云服务发现等方法获取所需的 Open Plug-n-Play 服务器 IP 地址。简化的 SMB 设备部署流程会自动完成以下与部署相关的操作任务：

要访问 PnP 页面，请选择**系统配置 > PnP**。要配置 PnP，请完成以下各步操作：

**步骤 1** 单击**启用**，然后输入以下信息。

| | |
|---|---|
| **PnP 传输模式** | • **自动**：选择此模式后，设备会自动从 PnP 服务器下载映像。<br>• **静态**：选择此模式后，您需要输入 IP/FQDN 和端口号，并从 CA 证书下拉列表中选择所要导入的证书。 |

**步骤 2** 单击**应用**。

# 即插即用连接服务

即插即用连接是 Cisco-provided 提供的服务, 是支持网络即插即用的设备发现服务器的最后手段。若要使用即插即用连接进行服务器发现, 必须首先创建一个表示管理器的控制器配置文件, 然后使用即插即用连接服务注册每个设备。

要访问即插即用连接服务, 请按照下列步骤操作:

**步骤 1** 在 web 浏览器中, 导航到 https://software.cisco.com。

**步骤 2** 单击屏幕右上角的 "登录" 按钮。使用与您的思科智能帐户关联的 cisco. com id 登录。

**步骤 3** 在 "网络即插即用" 标题下选择 "即插即用连接" 链接。此时将显示即插即用连接服务的主页。

## 创建控制器配置文件

若要创建控制器配置文件, 请按照下列步骤操作:

**步骤 1** 在浏览器中打开即插即用连接网页 https://software.cisco.com/#module/pnp 如有必要, 请选择要使用的正确虚拟帐户

**步骤 2** 选择 "控制器配置文件" 链接, 然后单击 "添加配置文件"。

**步骤 3** 从下拉列表中选择控制器 pnp server 的类型。然后单击 "下一步"。

**步骤 4** 指定配置文件的名称和说明 (可选)

**步骤 5** 在主控制器标题下, 使用提供的下拉列表选择是按名称还是按 ip 地址指定服务器。在提供的字段中填写服务器的一个或多个地址。

**步骤 6** 选择与服务器通信时要使用的协议。强烈建议使用 https 来确保设置过程的完整性。

**步骤 7** 如果选择的协议是 https, 并且服务器配置了自签名证书 (默认值) 或未由已知证书颁发机构签名的证书, 则应使用提供的控件上载服务器使用的证书。

**步骤 8** 单击 "下一步", 然后单击 "提交" 之前查看设置。

## 注册设备

从思科直接购买的某些产品可能会在购买时与您的思科智能帐户相关联, 这些产品将自动添加到即插即用连接中。但是, 思科的100至500系列即插即用产品中的大多数都需要手动注册。要使用即插即用连接注册设备, 请按照下列步骤操作:

**步骤 1** 在浏览器中打开即插即用连接网页 https://software.cisco.com/#module/pnp 如有必要, 请选择要使用的正确虚拟帐户。

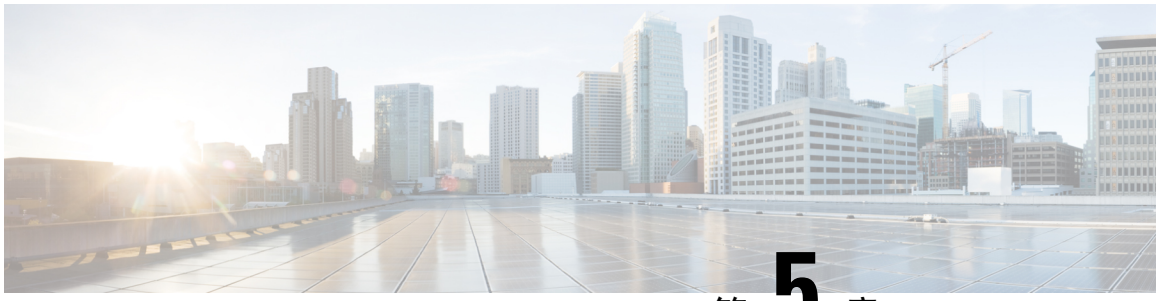
**步骤 2** 选择 "设备" 链接, 然后单击 "添加设备"。您可能需要获得批准才能手动将设备添加到您的帐户。这是一个一次性的过程, 如果需要, 一旦获得批准, 您将收到电子邮件通知。

**步骤 3** 选择是手动添加设备, 还是通过上传 csv 格式的详细信息来添加多个设备。单击提供的链接下载示例 csv 文件。如果选择上载 csv 文件, 请单击 "浏览" 按钮以选择该文件。然后单击 "下一步" 。

**步骤 4** 如果选择手动添加设备, 请单击 "识别设备"。指定要添加的设备的序列号和产品 id。从下拉列表中选择控制器配置文件。(可选) 输入此设备的说明。

**步骤 5** 重复步骤 4, 直到添加了所有设备, 然后单击 "下一步" 。

**步骤 6** 查看已添加的设备, 然后单击 "提交" 。



第 5 章

# WAN

本节介绍广域网 (WAN)，包含以下主题：



## WAN 设置

广域网 (WAN) 是分散在不同地理位置的电信或计算机网络的集合。此术语并不是指比局域网 (LAN) 更广阔的电信结构。广域网可以由私人拥有或租用，可使企业不受位置限制，有效履行日常职能。

设备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** 选择 **WAN > WAN 设置**。

**步骤 2** 在 WAN 表中，单击**添加或编辑**，然后对“IPv4”、“IPv6”或“高级”进行设置。

**步骤 3** 选择子接口名称并输入 VLAN ID。

**IPv4 和 IPv6 连接**

**步骤 4** 对于 IPv4 连接，请单击 **IPv4** 选项卡。

**步骤 5** 从列表中选择连接类型：

**当 IPv4 或 IPv6 连接使用 DHCP 时**

在“DCHP 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。 |

**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：

| | |
|---|---|
| **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）。 |
| **DNS 服务器** | 选择**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 PPPoE 时**

在“PPPoE 设置”部分输入以下信息：

| | |
|---|---|
| **与 IPv4 共享会话** | 选择**与 IPv4 共享会话**可重复使用 IPv4 PPPoE 设置中配置的相同用户名/密码，并从同一个 PPPoE 会话中获取 IPv4 和 IPv6 地址。 |
| **分离 IPv4 和 IPv6 会话** | 要将用户名/密码设置仅用于 IPv6 PPPoE 会话，请选择**分离 IPv4 和 IPv6 会话**。 |
| **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。 |
| **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。<br>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** 某些运营商不允许 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DCHP，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。 |
| **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。<br>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DCHP，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。<br>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 IPv4 连接使用网桥时**

| | |
|---|---|
| **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：

| | |
|---|---|
| **DNS 服务器** | 从下拉列表中选择**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。 |

**步骤 6** 要禁用 IPv6，请选中**禁用**。

**步骤 7** 单击**应用**。

**对于高级协议**

**步骤 8** 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 9** 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 连接的通道捆合。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 设置**。

**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** 选择一个接口，单击**编辑**并按照下面的说明配置以下各项：

- **重试次数** – 对设备执行 Ping 命令的次数。范围为 1 至 10，默认值为 3。

- **重试超时时间** – 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**，然后输入用于对设备执行 Ping 命令以进行网络服务检测的主机名。

**步骤 4** 单击**应用**返回“多 WAN”菜单。

**步骤 5** 然后，选中**启用基于策略的路由**，以启用基于策略的路由。

**步骤 6** 在策略绑定表中，单击**添加**、**编辑**或**删除**。策略绑定功能会规定将接口用于特定服务。利用此功能，管理员可以将特定的传出流量绑定到某一 WAN 接口。接下来，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**。<br>**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** 某些运营商不允许 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设备使用移动宽带连接（而不是电话或数据电缆）进行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，选择要应用设置的接口（USB1 或 USB2）。

**步骤 3** 在“卡状态”部分，单击连接图标建立连接。

**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** – 输入移动网络运营商提供的接入点名称。
- **拨号号码** – 输入移动网络运营商提供的用于连接互联网的号码。
- **用户名和密码** – 输入移动网络运营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** – 选择验证选项。

**步骤 4** 您可以从以下连接模式中选择一种。

- **按需连接** – 指定连接计时器，如果计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** – 定期检查与设备的连接，以便在连接断开时重新建立连接。在“重拨周期”中，输入设备自动检查连接的时间间隔（以秒为单位）。默认周期为 30 秒。

**步骤 5** **HiLink 模式** – 某些装置（例如华为 E8372）支持 HiLink 模式。您可以打开装置的配置页面来配置详细设置。要配置 HiLink 模式，请按照以下步骤操作：

a) 在“配置模式”中，选择 **HiLink** 连接到装置。
b) 输入装置关联的卡型号。
c) 单击**打开 HiLink 页面**，为装置配置相关设置。
d) **用户名和密码** – 输入用户名和密码。

# 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** 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“运营商”下拉列表中选择运营商的名称。
**步骤 6** 输入 DDNS 账户的**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** 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。

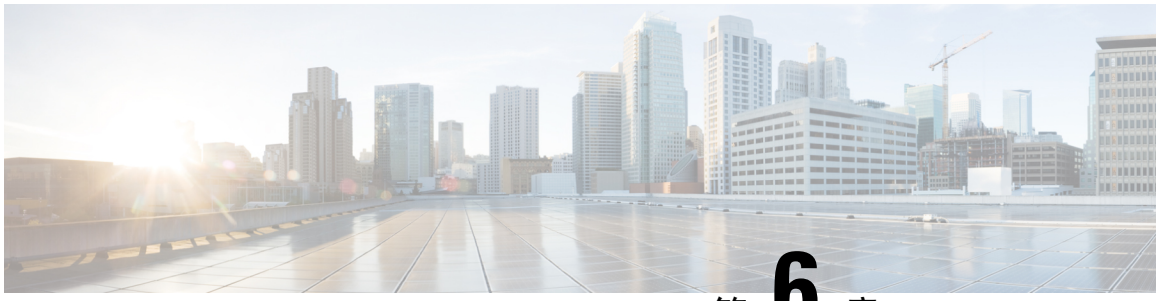
**步骤 3** 或者，选择**手动**并设置以下 6rd 参数。

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

# LAN

局域网 (LAN) 是一种覆盖面积相对较小且相互临近的区域（例如办公大楼、学校或家庭）的计算机网络。LAN 的特性因所使用的拓扑、协议和介质而异。

LAN 非常适合用于共享资源，例如文件、打印机、游戏或其他应用程序。LAN 通常会连接到其他 LAN、互联网或其他 WAN。本节包含以下主题：



## 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：

| | |
|---|---|
| **端口标签** | 输入端口的名称。 |
| **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 LAN16)**。 |
| 受监控端口 | 对发送用于映射的流量进行监控所用的端口。<br>从下拉列表中选择任一 LAN **(LAN1 到 LAN16)**。 |

**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。<br>从下拉列表中选择任一 LAN **(LAN1 到 LAN16)**。 |
| **LAG1** | 选择在适当的端口上对流量应用链路聚合。<br>从下拉列表中选择任一 LAN **(LAN1 到 LAN16)**。 |

**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**。

# PoE 设置 (RV345P)

以太网供电 (PoE) 是一项适用于 LAN（局域网）的技术，可以通过数据电缆而不是电线为设备供电。

为了让 PoE 正常运作，电流必须在电源端输入数据电缆并在设备端输出，电流始终与数据信号隔离，从而避免彼此干扰。电流通过馈电器输入数据电缆。如果数据电缆另一端的设备兼容 PoE，设备将正常工作而无需改装。如果设备不兼容 PoE，则必须安装选择器，以去掉数据电缆上的电流。

RV345P 有内置的 16 端口和 8 端口全双工 10/100/1000 千兆交换机，可以提供 PoE 功能。要配置 PoE 设置，请按照以下步骤操作：

**步骤 1** 选择 **LAN > PoE 设置**。

**步骤 2** 在“供电模式”部分，选择**端口限制**或**类别限制**。

**端口限制模式**

- 将功率限制为指定的瓦特数。要使这些设置生效，系统必须处于 PoE 端口限制模式。

**类别限制模式**

- 根据连接的设备的类别限制功率。要使这些设置生效，系统必须处于 PoE 类别限制模式。

**步骤 3** 单击**编辑**以编辑“端口限制”或“类别限制”设置。

**步骤 4** 对于“端口限制”，配置以下设置：

- **PoE 启用** – 选中以启用该功能。
- **电源优先级** – 选择优先级（严重、高或低）。
- **管理功率分配** – 输入毫瓦 (mW) 值（范围：0-30000，默认值：30000）。

**步骤 5** 对于“类别限制”，配置以下设置：

- **PoE 启用** – 选中以启用该功能。
- **电源优先级** – 选择优先级（严重、高或低）。

**步骤 6** 单击**应用**。

**步骤 7** 要启用“传统 PoE”，选中**启用**。

**步骤 8** 利用简单网络管理协议(SNMP)陷阱，代理可以通过未经请求的SNMP消息将重要事件通知管理站。要启用“SNMP陷阱”，选中**启用**。

**步骤 9** 在“电源陷阱阈值”中，输入以 % 表示的阈值。（范围：1-99，默认值：95）。

**注释** “PoE 属性表”显示 PoE 的运行状态和使用的电源等级。

# 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。

**步骤 4** 选中相应的复选框，以启用 VLAN 间路由和设备管理功能。

**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“分配 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** 选择**接口**，然后单击**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 地址连接到设备的时间（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** | • **选项 66** – 输入单个 TFTP 服务器的 IP 地址或主机名。<br>• **选项 150** – 输入一系列 TFTP 服务器的 IP 地址。<br>• **选项 67** – 输入启动文件名。<br>• **选项 43** – 输入供应商特定信息。 |

**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 地址连接到设备的时间。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，如果设备使用默认的 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/ASCII** | 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，并从下拉列表中选择一种格式。 |
| **位掩码** | 如果选择 HEX 作为电路 ID/ASCII 的格式，请输入位掩码。 |

**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 地址连接到设备的时间。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，如果设备使用默认的 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** | • **选项 66** – 输入单个 TFTP 服务器的 IP 地址或主机名。<br>• **选项 150** – 输入一系列 TFTP 服务器的 IP 地址。<br>• **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。确保在用户账户，第 29 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。

如果启用此功能，请在客户端设备上将设备配置为 DNS 服务器。默认情况下，Windows 计算机会设置为自动从默认网关中获取 DNS 服务器地址。

以运行 Windows 的 PC 为例，要更改 TCP/IP 连接设置，请按照以下步骤操作：

1. 转至“本地连接属性”>“Internet 协议”>“TCP/IP 属性”。
2. 选择“使用下列 DNS 服务器地址”。
3. 在“首选 DNS 服务器”栏中输入设备的 LAN IP 地址。

要添加新主机，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设备来实现与其他所有主机（本地网络中的主机除外）的通信。设备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。

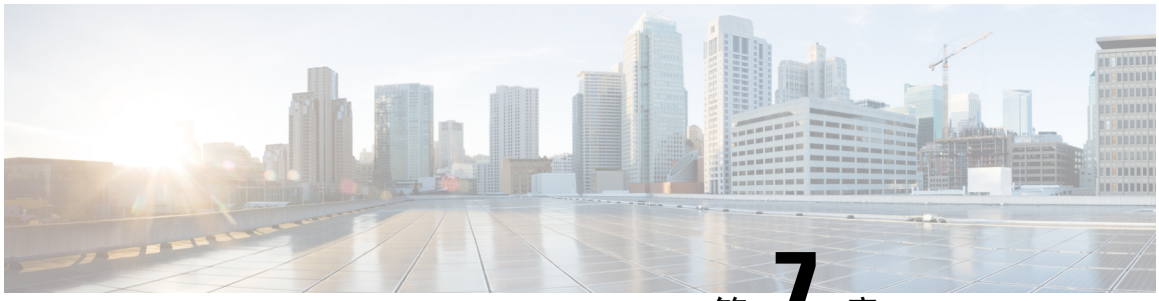
**步骤 3** 选中**启用**以启用路由器通告，然后配置以下设置：

| | |
|---|---|
| **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** | 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：<br>• **管理型** – 主机使用管理型的有状态配置协议 (DHCPv6)，通过 DHCPv6 获取有状态的地址和其他信息。<br>• **其他** – 使用管理型的有状态配置协议 (DHCPv6) 获取其他非地址信息，例如 DNS 服务器地址。 |
| **路由器偏好** | 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设备。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。 |
| **最大传输单位 (MTU)** | 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。 |
| **路由器有效期限** | 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。 |

**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 7 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，设备可以根据逻辑网络布局的实时变化选择路径。设备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

互联网组管理协议 (IGMP) 供 IP 网络上的主机和设备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程序提供支持。利用 IGMP 代理，设备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**，以允许设备与节点彼此通信。

**步骤 3** 从下拉列表中选择**上游接口**。

- **WAN 自动** – 设备可以支持多 WAN。如果选择 WAN 自动模式，设备将选择活动的 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。<br>**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。<br>• 选中**启用**可在 RIP 第 1 版上启用发送和接收路由信息。<br>• 选中**被动**可在 RIP 第 1 版上禁用发送路由信息。<br>**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。<br>• 选中**启用**可在 RIP 第 2 版上启用发送和接收路由信息。<br>• 选中**被动**可在 RIP 第 2 版上禁用发送路由信息。<br>**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。<br>• 选中**启用**可启用 RIP IPv6 路由。<br>• 选中**被动**可禁用发送 RIPng 版本。<br>**注释** 仅当选中**启用**时才可激活被动配置。 |
| **验证** | 此安全功能在与其他设备交换路由之前强制验证 RIP 数据包。此功能不可用于 RIPv1。<br>• 选中**启用**可启用验证，从而仅与网络中受信任的设备交换路由。<br>• **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设备之间没有进行通信，那么静态路由可以配置为在设备之间进行通信。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：

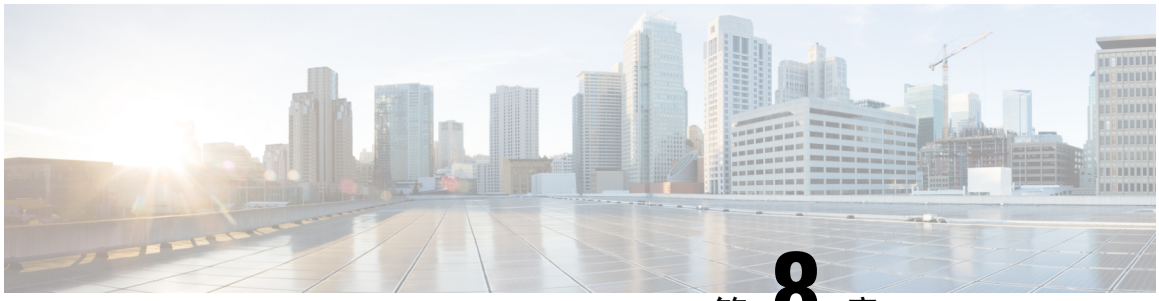
| | |
|---|---|
| **网络** | 输入您要向其分配静态路由的目标子网 IP 地址。 |
| **掩码** | 输入目标地址的子网掩码。 |
| **下一步跳** | 输入最后选择的设备的 IP 地址。 |
| **步跳计数** | 输入数据包在被丢弃之前可以通过的节点或步跳的最大次数。节点可以是网络上的任何设备，例如交换机或路由器。 |
| **度量标准** | 输入确定发送网络流量的最佳路由时使用的路由算法数量。 |
| **接口** | 从下拉列表中选择要用于此静态路由的接口。 |

**步骤 3** 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。 |
| **时长** | 输入 IP 地址的前缀位数。 |
| **下一步跳** | 输入最后选择的设备的 IP 地址。 |
| **度量标准** | 输入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** | 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 8 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

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**，然后输入以下信息：

| | |
|---|---|
| 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。<br>**注释** SYN泛洪、回音风暴和ICMP泛洪的流量速率均可配置，默认值分别为：128、15 和 100。 |
| **阻止 WAN 请求** | 选中**启用**可阻止对 WAN 的 ICMP 回音请求。 |
| **RESTCONF** | 默认情况下，此项在 LAN 接口上处于启用状态。您可以对 LAN 和 WAN 接口均启用此配置。 |
| **RESTCONF 端口** | 默认情况下，使用的端口为 443；您可以根据需要进行配置。 |

| | |
|---|---|
| **NETCONF** | 默认情况下，此项在 LAN 接口上处于启用状态。您可以对 LAN 和 WAN 接口均启用此配置。 |
| **NETCONF 端口** | 默认情况下，使用的端口为 830；您可以根据需要进行配置。 |
| **LAN/VPN Web 管理** | 允许 LAN 接口的成员通过 HTTP 或 HTTPS 连接到设备。选择 **HTTP** 或 **HTTPS**。 |
| **远程 Web 管理** | 允许远程登录系统或设备，并允许远程访问 Web 界面。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**）。<br>• 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程序层网关）** | 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。该应用程序层网关 (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）** | 网络协议的集合，可允许网络设备无缝发现彼此的存在，并为数据共享和通信建立功能正常的网络服务。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：<br>• **Java**：阻止 Web Java 功能。<br>• **Cookies**：阻止 Cookies。<br>• **ActiveX**：阻止 ActiveX。<br>• **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

您可以配置规则来根据特定参数（例如 IP 地址或端口）过滤数据包。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 | • **IPv4** – 选择要应用 IPv4 规则的服务。<br>• **IPv6** – 选择要应用 IPv6 规则的服务。<br>• **服务** – 从下拉列表中选择服务。 |
| 日志 | 从下拉列表中选择**真**或**从不**。<br>• **真** – 匹配规则。<br>• **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 | 选择要应用规则的源 IP 地址并输入以下信息：<br>• **任意**<br>• **单一 IP** – 输入一个 IP 地址。<br>• **IP 范围** – 输入 IP 地址范围。<br>• **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 | 选择要应用规则的源 IP 地址并输入以下信息：<br>• **任意**<br>• **单一 IP** – 输入一个 IP 地址。<br>• **IP 范围** – 输入 IP 地址范围。<br>• **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。<br>**注释** 请勿在此范围中包含设备的 WAN IP 地址。 |
| **范围长度** | 输入此范围中 IP 地址的数量。<br>**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。 |

**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** – 输入为此服务预留的端口号范围。
- **结束端口** – 输入为此服务预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，通过打开某个服务（例如FTP）的特定端口或端口范围，可以公共访问LAN网络设备上的服务。端口转发功能会为使用替换端口在服务器和LAN主机之间进行通信的服务（例如互联网游戏）打开端口范围。

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：

| | |
|---|---|
| **启用** | 选中此复选框可启用端口转发功能。 |
| **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。 |

**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 应用程序动态添加 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入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：

| | |
|---|---|
| **启用** | 启用或禁用端口触发规则。 |
| **应用程序名称** | 输入应用程序的名称。 |
| **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。 |

**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。

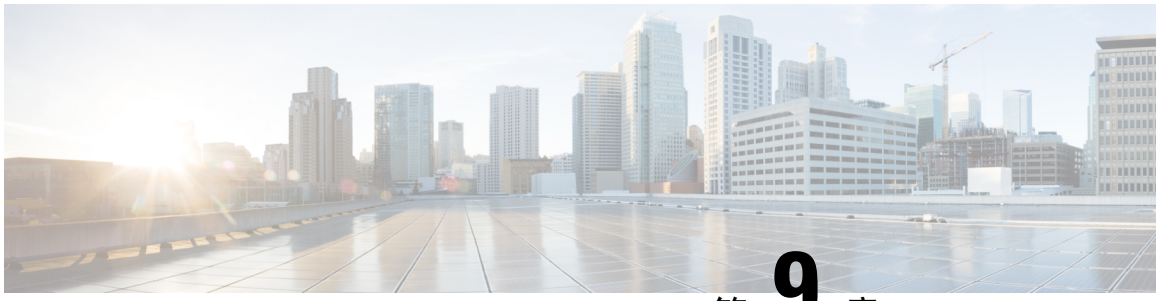
要配置 DMZ，请按照以下步骤操作：

**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 9 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 状态

虚拟专用网络 (VPN) 用于在安全性较低的网络中建立加密连接。当仅靠底层网络基础设施无法保护连接的系统时，VPN 可确保为连接的系统提供适当的保护。VPN 将作为隧道建立起一个专用网络，使用行业标准加密和验证技术安全地发送数据，从而保护发送数据的安全。

远程访问 VPN 通常依靠 IPSec 或 SSL 来保护连接。VPN 可为目标网络提供第 2 层接入，这需要使用 PPTP 或 L2TP 等在基本 IPSec 连接之上运行的隧道协议。IPSec VPN 支持适用于网关到网关隧道的站点到站点 VPN 以及适用于主机到网关隧道的客户端到服务器 VPN。例如，用户可以在分支机构配置一条 VPN 隧道，用于连接总部的设备，以确保分支机构可以安全地访问总部网络。如果用户需要从家里使用笔记本电脑或 PC 通过 VPN 服务器连接到公司网络，则可以使用客户端到服务器 VPN。

“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 > 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** – 已定义的 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 76 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 77 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 的应用程序。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。
- **会话数** – 会话的数量。

您还可以添加、编辑或删除 SSL VPN。（请参阅SSL VPN，第 83 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** – 连接的用户的名称。
- **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** – 建立或断开隧道连接。

### 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** – 连接的用户的名称。
- **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** – 建立或断开隧道连接。

### 远程工作人员 VPN 客户端

您可以在此页面中查看远程工作人员 VPN 客户端的状态。在“VPN - 远程工作人员 VPN 客户端”页面中，您只需进行最低限度的配置，即可创建一条 VPN 连接。当远程工作人员 VPN 客户端发起 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 VPN 隧道。

- **名称** – 隧道的名称。
- **状态** – 隧道的当前状态（“连接”或“中断”）。
- **主 DNS** – 主 DNS 服务器的 IP 地址。

- **辅助 DNS** – 辅助 DNS 服务器的 IP 地址。
- **主 WINS** – 主 Windows 互联网名称服务 (WINS) 服务器的 IP 地址。
- **辅助 WINS** – 辅助 WINS 服务器的 IP 地址。
- **默认域** – 默认域的名称。
- **拆分隧道** – 允许移动用户在启用 VPN 隧道的情况下同时访问不同的安全域（例如公共网络和本地 LAN 或 WAN）的隧道的名称。
- **拆分 DNS** – 拆分 DNS 可将内部主机定向至内部域名服务器进行名称解析，并将外部主机定向至外部域名服务器进行名称解析。拆分 DNS 的名称。
- **备用服务器 1、2 和 3** – 当与主 IPSec VPN 服务器的连接失败时，安全设备可发起与备用服务器的 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。定义为备用服务器的服务器名称。

# 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。如果秘钥模式为手动，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** 选择秘钥模式。

**步骤 5** 对于**自动秘钥模式**，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。<br>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。 |

**第 2 阶段选项**

| | |
|---|---|
| 协议选项 | 从下拉列表中选择协议。<br>• **ESP**：选择 ESP 进行数据加密，并输入加密选项。<br>• **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。 |
| 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。<br>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。 |
| 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。<br>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）。<br>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**）。 |

| | |
|---|---|
| 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，一个位置的本地设备可以通过 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设备可通过静态 IP 地址或动态 DNS 主机名标识。如果某个设备仅有一个动态 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，请在配置这两个设备时输入相应的设置（将本地和远程反向）。假设此设备的标识为设备 A。请在“本地组设置”部分输入其设置；在“远程组设置”部分输入另一设备（设备 B）的设置。配置另一个设备（设备 B）时，请在“本地组设置”部分输入其设置，并在“远程组设置”部分输入设备 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 | • **编辑** – 单击此项可编辑连接，系统会导航至“站点到站点 - 添加或编辑新连接”页面。<br>• **删除** – 单击此项可删除连接。<br>• **连接** – 单击此项可连接并建立隧道。<br>• **断开连接** – 单击此项可断开连接。 |

# 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。

要打开“客户端到站点”页面，请单击 **VPN > 客户端到站点**，系统将显示以下选项：

| | |
|---|---|
| **隧道名称** | 已连接的隧道的名称。 |
| **WAN 接口** | 用户组连接的接口的名称。 |
| **验证方法** | 连接所使用的验证方法的名称。 |

**添加客户端到站点连接**

**步骤 1** 单击**添加**，然后选择一个选项（**思科 VPN 客户端或第三方客户端**）。

**步骤 2** 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。 |
| **隧道名称** | 输入隧道的名称。 |
| **接口** | 从下拉列表中选择接口（**WAN1**、**WAN2**、**USB1 或 USB2**）。 |
| **IKE 验证方法** | 在基于 IKE 的隧道中用于 IKE 协商的验证方法。<br>• **预共享密钥**：IKE 对端彼此进行验证的方式是，计算并发送含预共享密钥的秘钥数据散列。如果接收端能够使用预共享密钥独立创建相同散列，表明两个对端必定共享相同秘钥，以此验证另一个对端。预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共享密钥。输入预共享密钥，单击**启用**以启用“预共享密钥最小复杂度”。要显示预共享密钥选项，请在“显示预共享密钥”部分选中**启用**复选框。<br>• **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**添加**可添加用户组。单击**删除**可删除用户组。 |
| 模式 | 选择模式选项。<br>• **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。<br>• **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**启用**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 3** 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** | 在基于 IKE 的隧道中用于 IKE 协商的验证方法。<br>• **预共享密钥**：IKE 对端彼此进行验证的方式是，计算并发送含预共享密钥的秘钥数据散列。如果接收端能够使用预共享密钥独立创建相同散列，表明两个对端必定共享相同秘钥，以此验证另一个对端。预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共享密钥。输入预共享密钥，单击“启用”以启用“预共享密钥最小复杂度”。<br>• **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 4** 在“高级设置”选项卡中，配置以下设置：

| | |
|---|---|
| **IPSec 配置文件** | 所要用于 VPN 隧道的 IPSec 配置文件的名称。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**）。 |

**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。 |
| **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。<br>“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**可使设备在开始连接时提议压缩。如果应答器拒绝此提议，则设备不会实施压缩。当设备本身用作应答器时，它将接受压缩（即使未启用压缩）。如果在设备上启用此功能，则在隧道另一端的设备上也应该启用此功能。 |

**步骤 5** 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**，检查以下内容：

| | |
|---|---|
| 远程工作人员 VPN 客户端 | 选择**开启**或**关闭**，以打开或关闭远程工作人员 VPN 客户端。 |
| 自动启动重试 | 选择**开启**或**关闭**，以重新尝试通过自动启动来建立连接。 |
| 重试间隔 | 失败后重新建立隧道的间隔时间。输入时间值（以秒为单位）。最大时间为 1800 秒。 |

**步骤 2** 在“远程工作人员 VPN 客户端”表中，单击**添加**并提供以下信息：

**基本设置**

| | |
|---|---|
| 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** | 在基于 IKE 的隧道中用于 IKE 协商的验证方法。<br>• **预共享密钥**：IKE 对端彼此进行验证的方式是，计算并发送含预共享密钥的秘钥数据散列。如果接收端能够使用预共享密钥独立创建相同散列，表明两个对端必定共享相同秘钥，以此验证另一个对端。预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共享密钥。选中**预共享密钥**，并在指定的字段中输入组名称和密码。<br>• **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** | • **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。<br>• **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。 |

高级设置

| | |
|---|---|
| **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。<br>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。 |
| **对端超时** | 输入以秒为单位的时间（范围：30 到 480）。 |

**步骤 3** 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**。

**注释** PPTP 服务器当前仅支持使用 PAP 作为本地数据库验证方法。要支持基于 MS-CHAPv2 的 Microsoft 点对点 (MPPE) 加密方法，则必须使用外部验证服务器。

# L2TP 服务器

第 2 层隧道协议 (L2TP) 是 PPTP 的延伸，互联网运营商 (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** | • **起始 IP 地址** – 输入起始 IP 地址。<br>• **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 |
| **预共享密钥** | 输入用于验证远程 IKE 对端的预共享密钥。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共享密钥。建议定期更改预共享密钥，以便最大限度地提高 VPN 的安全性。 |

| | |
|---|---|
| 确认预共享密钥 | 重新输入预共享密钥进行确认。 |

**步骤 3** 单击应用。

# 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“VPN”>“GRE 隧道”，然后提供以下信息：

| | |
|---|---|
| **GRE 隧道名称** | 输入 GRE 隧道的名称。 |
| **GRE 隧道描述** | 输入 GRE 隧道的描述。 |
| **启用** | 选中可启用 GRE 隧道。 |
| **来源** | 从下拉列表中选择隧道源。 |
| **目标** | 从下拉列表中选择隧道目标。 |
| **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。 |
| **MTU** | 最大传输单位 (MTU) 是可在网络中发送的最大数据包的大小。默认设置为 1400 字节，这是以太网的标准值。 |

**步骤 2** 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。设备支持思科 AnyConnect VPN 客户端（可在 [http://www.cisco.com/go/anyconnect/] 下载）。默认情况下，设备支持 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：

强制网关设置

| | |
|---|---|
| 思科 SSL VPN 服务器 | 选择**打开**或**关闭**以启用或禁用服务器。 |
| 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 | 确保设备始终连接到互联网。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**）。 |
| 密钥更新间隔 | 以秒为单位，输入密钥更新间隔时间值（**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，以配置 SSLVPN 组策略。

**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 SSLVPN 策略的描述。 |

**IE 代理设置**

| | |
|---|---|
| **IE 代理策略** | 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**）。<br>如果您选择**自动**或**绕过本地**，请输入以下信息：<br>• **地址** – IP 地址或域名。<br>• **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 客户端可通过设备顺利连接至 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 层上的互联网来实现点对点会话的方法。

**步骤 3** 单击**应用**。

第 10 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

应用程序控制是路由器上的附加安全功能，可增强安全网络，提高工作场所的工作效率，并最大限度地提高带宽。应用程序控制可用于智能手机和其他基于浏览器的应用程序。

### 设置

要添加、配置或修改应用程序控制策略，请按照以下步骤操作：

**步骤 1** 单击**安全 > 设置**。

**步骤 2** 在“应用程序控制”页面上，选择**打开**，并单击**应用**。

**步骤 3** 要创建新的应用程序控制策略，请在“应用程序控制策略”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** | 输入策略配置文件的名称。 |
| **说明** | 输入关于策略的简要说明。 |
| **启用** | 选中可执行应用程序控制策略。 |

| | |
|---|---|
| 应用程序 | 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**。 |
| **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：<br>• **类型**（选择“Mac”或“IP 组”）<br>• **IP/MAC** – 输入 MAC 地址<br>• **设备类型** – 选择设备类型<br>• **操作系统类型** – 选择操作系统类型 |
| 计划表 | 此项用于指定应用程序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** 单击**应用**。

# 应用程序统计信息

要打开“应用程序统计信息”页面，请单击**安全 > 应用程序统计信息**。系统将显示以下选项：

| | |
|---|---|
| **当前 WAN 流量更新** | 选择以秒为单位的持续时间 (15/30/60) 来查看所选 WAN 接口的流量。<br>**注释** 此选项仅适用于 WAN 以太网接口。 |
| **WAN 接口** | 选择所需接口，查看以图形格式显示的接口统计信息。 |
| **重置状态** | 单击此选项可重置统计信息。 |
| **应用程序** | 显示应用程序的名称。单击链接可查看正在使用该应用程序的客户端列表。 |
| **协议** | 应用程序流量所使用的协议，例如 TCP 和 UDP 等等。 |
| **端口** | 应用程序流量所使用的端口（目标端口）。 |
| **使用百分比** | 所有应用程序的使用百分比。 |
| **使用情况** | 按大小列出的正在使用的应用程序。 |
| **发送的数据包数** | 已发送的数据包数。 |
| **接收的数据包数** | 已接收的数据包数。 |
| **客户端数** | 正在使用该应用程序的客户端数量。 |

# 客户端统计信息

客户端统计信息显示当前或曾经连接到设备的客户端的历史数据。要查看“客户端统计信息”页面，请单击**安全 > 客户端统计信息**。“客户端统计信息”页面上的“客户端组表”显示了与客户端关联的所有现有组。您可以单击**添加**并输入组名来添加新组，也可以选择一个组并单击**编辑**来编辑现有组。

要查看和编辑客户端详细信息，请提供以下信息。

| | |
|---|---|
| **MAC 地址** | 显示客户端的 MAC 地址。单击此项可查看所有关联的应用程序。 |
| **IPv4 或 IPv6 地址** | 显示客户端的 IP 地址。 |
| **状态** | 客户端的当前状态。 |
| **主机名** | 客户端的主机名。单击此项可编辑主机名。 |
| **设备类型** | 客户端的设备名称。单击此项可进行编辑。 |
| **操作系统类型** | 显示客户端的操作系统类型。单击此项可进行编辑。 |
| **使用百分比** | 所有客户端的使用百分比。 |
| **IP 组** | 显示关联的 IP 组。您可以选择适当的 IP 组。 |

# Web 过滤

Web 过滤功能可用于管理对不当网站的访问。它可以筛查客户端的 Web 访问请求，确定允许还是拒绝该网站。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 URL 查找框中输入 URL，可验证或查找该 URL。您可以查看该 URL 的类别、信誉得分和状态。如果您想修改 URL 类别/得分，请单击 URL 评分审查链接。

**步骤 4** 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 5** 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 | • 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。<br>• 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。<br>• 单击**恢复为默认类别**可恢复默认设置。 |
| 设备类型 | 从下拉列表中选择需要应用策略的设备类型。 |
| 操作系统类型 | 从下拉列表中选择需要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** | 从下拉列表中选择需要应用此策略的 IP 组。 |
| 例外情况列表 | 单击**编辑**，然后**添加**并定义以下设置：<br>• **白名单** – 单击**添加**可定义绕过此策略的域名或关键词。<br>• **黑名单** – 单击**添加**可定义应阻止的域名或关键词。<br>• **例外情况列表** – 单击**添加**可指定从此策略中排除的 IP 地址。<br>单击**应用**。 |
| 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 6** 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** 对 DHCP 租用表中的 IP 和 MAC 绑定表单击**添加**，将这些条目添加到 IP 和 MAC 绑定表。

**步骤 6** 在“名称”列下，为该绑定表条目指定一个名称。

**步骤 7** 单击**应用**、**编辑**或**删除**，可应用新地址、编辑现有地址或删除现有地址。

# 思科 Umbrella

思科 Umbrella 是一款云安全平台，可针对互联网上的威胁提供第一道防线。此功能通过检查发送至 DNS 服务器的 DNS 查询，提供基于云的安全服务。这项集成功能使用 Umbrella 账户透明地拦截 DNS 查询，并将其重定向到 Umbrella。此设备将在 Umbrella 控制面板上显示为一台网络设备，您可以执行应用策略和查看报告等操作。

要配置 Umbrella，请按照以下步骤操作：

**步骤 1** 单击**安全 > 思科 Umbrella**。

**步骤 2** 选中**启用**可启用 Umbrella 功能。

**步骤 3** 如果您选择使用网络设备作为设备的标识，请按照以下步骤操作：

| | |
|---|---|
| **开始** | 单击“开始”，然后输入下列凭证：<br>1. 输入“密钥和密码”（从 Umbrella 账户复制），然后单击**下一步**。<br>2. 选择您的组织，然后单击**下一步**。<br>3. 选择所要关联的策略，然后单击**下一步**。<br>4. 输入设备的名称。如果注册成功，系统会显示一条成功消息。单击**确定**进入下一步。 |

**步骤 4** 如果使用 "网络" 作为此路由器的标识, 请检查此选项。

**步骤 5** 接下来, 将路由器的公共 ip 地址添加到伞式仪表板。或者, 如果您有动态的公共 ip 地址, 则可以手动将其添加到伞式仪表板上或按照说明进行操作。

**步骤 6** 在思科 Umbrella 门户上配置适当的策略，允许或拒绝流向完全限定域名 (FQDN) 的流量。

| | |
|---|---|
| **要绕过的本地域** | 输入要从 OpenDNS 绕过的域名。<br>您可以添加多个域。 |
| **DNSCrypt** | • 选中**启用**可将加密 DNS 查询发送至 OpenDNS 解析器。<br>• 提供 OpenDNS 解析器的公钥，以更新解析器列表。 |

**步骤 7** 到此为止，设备已完成注册。接下来，您可以根据需要完成以下任务：

| | |
|---|---|
| **更改凭证** | 单击此项可更新新凭证。 |
| **更改设备信息** | 单击此项可更改设备名称。 |
| **解除注册** | 单击此项可将您的设备从 Umbrella 账户解除注册。 |
| **更改路径** | 单击此项可更改设备关联的策略。 |

**步骤 8** 接下来，您可以配置高级配置设置：

| | |
|---|---|
| **要绕过的本地域** | 输入要从 OpenDNS 解析器绕过的本地域名。 |
| **DNSCrypt** | • 在此网络设备配置选项下，DNSCrypt 将始终启用。<br>提供 OpenDNS 解析器的公钥，以更新解析器列表。 |

# 威胁

仪表板显示配置反威胁和ips功能时的威胁和攻击的详细信息。仪表板为您提供了整个事件摘要的视图, 以及根据所选内容检测到的威胁和攻击的详细信息, 如日、周和月。

## 地位

在配置了防威胁和 IPS 功能的情况下，控制面板可显示威胁和攻击的详细信息。控制面板在一个视图中显示完整的事件摘要，并按照选择的范围（天、周、月等）列出检测到的威胁与攻击的详细信息。

单击**安全 > 威胁/ips > 状态**。您可以在所选选项卡下查看系统日期和时间、已扫描的威胁和攻击，以及已检测的威胁和攻击。默认情况下，您会看到“总计”选项卡下的状态信息。

| | |
|---|---|
| **总计** | 您可以从列表中选择“过去24小时”、“过去一周”或“过去一个月”，以查看相应时间范围内的事件。 |
| **威胁** | 显示以下信息：<br>• 前10个客户端-受影响的 mac 地址列表。 – 受影响的 MAC 地址的列表。<br>• 十大威胁-检测到的威胁列表 |
| **IPS** | 显示以下信息：<br>• 十大攻击客户-十大受攻击客户名单<br>• 十大 ips 攻击-十大 ips 攻击列表 |

## 设置

防病毒软件可保护网络用户免受电子邮件或数据中接收到的受感染和恶意软件内容的影响。防病毒功能支持 smtp、http、ftp、pop3 和 imap 协议。

在 "防病毒" 页上配置适当的设置, 以防止恶意软件或受感染的电子邮件。

要配置防威胁功能，请按照以下步骤操作：

**步骤 1** 单击**安全 > threat/ips > 杀毒软件**。

**步骤 2** 如果您希望启用防威胁功能，请选中**启用**复选框。

**步骤 3** 在“要扫描的应用程序”框中配置下列选项。

| | |
|---|---|
| **HTTP/FTP/SMTP/POP3/IMAP** | • 选中**启用**以激活配置。<br>• 选择适当的操作。<br>• **记录日志** – 选择此选项后，系统会在发现威胁时仅生成日志（包含客户端信息、签名 ID 等等）。此选项不会影响连接。<br>• **记录破坏日志** – 选择此选项可在发现威胁时丢弃连接，并记录要删除的消息。<br>**注释** 如果是在电子邮件附件中发现威胁，系统会在下载过程中截断文件。 |
| **启用文件大小阈值** | 选中此复选框后可输入扫描所需的文件大小。 |

**病毒数据库**

| | |
|---|---|
| **最近更新时间** | 显示最近一次更新签名的日期和时间。 |
| **文件版本** | 显示当前使用的签名版本。 |

# 入侵防御系统

入侵防御系统 (IPS) 会检查网络中的流量异常。您可以配置 IPS 来按照所配置的安全级别执行阻止或日志记录操作。

要配置 IPS，请按照以下步骤操作：

**步骤 1** 单击**安全 > IPS**。

**步骤 2** 选择**开启**以启用入侵防御系统功能。

| | |
|---|---|
| **模式** | • **阻止攻击（防御）** – 选择此模式可阻止所有攻击。此模式也会记录异常。<br>• **仅记录日志** – 选择此选项后，系统会在发现异常时仅生成日志（包含客户端信息、签名ID等等）。此选项不会影响连接。 |

| | |
|---|---|
| **IPS 安全等级** | • **注重连接性** – 选择此项可将所选模式应用到流量，以检测最关键的攻击。这提供了最少的保护: 仅检测到 (高严重性) 风险攻击。<br>• **注重平衡性** – 选择此项可将所选模式应用到流量，以检测严重攻击和关键攻击。这提供了中等保护: (高 + 中等严重性) 将被检查, 绕过低风险签名。<br>• **注重安全性** – 选择此项可将所选模式应用到流量，以检测一般攻击、严重攻击和关键攻击。这提供了最大的保护: 检查所有规则 (高 + 中/低严重级别)。 |

**入侵防御系统签名**

| | |
|---|---|
| **最近更新** | 显示最近一次更新签名的日期和时间。 |
| **文件版本** | 显示当前使用的签名版本。 |
| **按 IPS 签名 ID 搜索** | 输入签名的 ID，然后单击按钮检查签名是否受支持。 |

**IPS 签名表**

| | |
|---|---|
| **名称、ID、严重性和类别** | • 签名的名称。<br>• 签名的唯一标识符。要查看所选签名的完整详细信息，请单击此列中的链接。<br>• 严重性级别表示安全影响。<br>• 签名所属的类别。 |
| **在表格中显示签名** | 使用**首页**、**上一页**、**下一页**和**尾页**按钮可显示指定页号的签名，并设置显示顺序。此外，您可以在**每页行数**下拉列表中选择要显示的签名的数量。 |

第 11 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

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 端口应用程序、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** - 输入已定义的类的名称。
- **说明** - 输入类的说明。
- **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/应用程序** | • **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。<br>• **应用程序**：选择要应用于流量记录的应用程序。选择应用程序行为和类别。<br>**注释** 用户在“安全/应用程序控制”页面中启用应用程序控制之前，无法配置应用程序规则。 |
| **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** | 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。<br>• **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。<br>• **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** | 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。<br>• 根据传入数据包的 DSCP 值，将流量映射至不同的队列。 |
| **基于 CoS** | 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。<br>• 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”表中，为每个队列输入适当的加权值。

**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 12 章

# 配置向导

本节介绍如何配置设备，具体包括以下主题：



## 初始设置向导

初始设置向导可指导您完成设备的互联网访问配置。

**步骤 1** 在设备的图形用户界面中，单击**配置向导**。

**步骤 2** 接下来，单击**启动向导**，按照屏幕上的指示设置设备。初始设置向导将尝试自动检测和配置您的连接。如果无法进行检测和配置，初始设置向导会要求您提供与您的互联网连接相关的信息。您可能需要联系您的 ISP 来获取该信息。

**步骤 3** 使用初始设置向导完成设备的配置后，系统将要求您更改默认密码。请更改默认密码，然后继续完成屏幕上的指示。

**步骤 4** 使用新用户名和密码登录到设备。设备将显示“使用入门”页面。该页面显示了最常见的配置任务。

**步骤 5** 单击导航栏中列出的一项任务，以完成配置。有关设备管理器显示的各个部分的详细说明，请参阅管理指南中的相应章节。

## 应用程序控制向导

应用程序控制是设备的一项附加安全功能，可用于加强已经受到保护的网络，提高工作场所的工作效率，并最大限度优化带宽。对于智能手机和其他基于浏览器的应用程序，应用程序控制功能十分有用。

应用程序控制为全局配置，但是只有在将操作应用到策略后，才能被策略使用。在应用程序控制配置中创建应用程序控制操作后，您可以更改该应用程序控制操作，将其用于每个策略。

要添加、配置或修改应用程序控制策略，请按照以下步骤操作：

步骤 1 单击**配置向导 > 应用程序控制向导**。

步骤 2 单击**启动向导**启动应用程序控制向导。

步骤 3 在“应用程序控制”页面上，选择**打开**，并输入策略名称。

步骤 4 单击**下一步**，并在“应用程序列表”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）的应用程序名称。选择需要过滤的内容后，单击**应用**。

步骤 5 单击**下一步**，并从下拉列表中选择计划表，以阻止应用程序。

步骤 6 单击**提交**。

# VPN 设置向导

借助 VPN，远程主机可以像位于同一局域网中一样工作。设备可支持 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**配置向导 > VPN 设置向导**。此向导可用于创建站点到站点 VPN 隧道。按照下述步骤创建创建 VPN 隧道。

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。<br>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。<br>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。 |
| 预共享密钥 | 用于验证远程 IKE 对端的预共享密钥。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共享密钥。<br>建议定期更改预共享密钥，以便最大限度地提高 VPN 的安全性。 |

**第 2 阶段选项**

| | |
|---|---|
| **Diffie-Hellman (DH) 组** | 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。<br>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。<br>**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。 |
| 协议选项 | 从下拉列表中选择协议。<br>• **ESP**：选择 ESP 进行数据加密，并输入加密选项。<br>• **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。 |

**步骤 12** 单击**下一步**查看所有配置的摘要。

**步骤 13** 单击**提交**。

第 13 章

# 许可证

本节介绍许可证，其中包含以下主题：



## 许可证

思科智能许可是一种基于云的许可方法。它简化了思科软件的购买、部署、跟踪和续约，为您提供简单轻松的许可体验。当您首次启动设备时，系统会进入评估模式。您必须通过思科智能许可来注册和管理新购买的思科产品。要注册和管理新购买的思科产品，请单击**智能许可管理器**。如果您还没有思科智能账户，请注册一个思科智能账户。

要访问“许可证”页面，请依次选择**许可证 > 许可证**。

系统将显示一个弹出窗口，告知您的URL未加入白名单，您尚未注册，无法进行访问。您必须使用思科智能软件许可注册您的思科产品。要进行注册，请按照以下步骤操作：

- 确保所要注册的产品能够访问互联网。
- 在智能许可管理器中，登录您的智能账户。
- 导航至您要对该产品实例使用的许可证所在的虚拟账户。
- 生成产品实例注册令牌（用于识别您的智能账户），复制或保存该令牌。
- 单击**注册**，然后将令牌粘贴到显示的窗口中。

在“许可证”部分，您可以配置许可证或注册设备。这有助于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。

# 申请智能账户

智能账户为支持智能许可证的思科设备提供存储库，并方便用户管理自己的思科许可证。利用智能账户，用户可以激活许可证，监控许可证使用情况，并跟踪后续思科产品/服务购买活动。您需要创建客户智能账户才能使用设备的所有许可证管理功能。

要申请客户智能账户，请登录思科软件中心 (CSC)。如果您没有 CCO ID，请访问 www.cisco.com，单击**立即注册**。

---

**步骤 1** 访问思科软件中心。

**步骤 2** 转至“管理”部分，然后单击**申请智能账户**。

**步骤 3** 选择“**是，我有权代表我的公司**”，您将负责授权智能账户的激活。如果您不具有相关权限，或者您不想授权智能账户，请选择“**否，请通知下面指定的人员授权激活**”。

**步骤 4** 然后输入指定人员的账户名称，并单击**继续**。

可选步骤 – 如果需要编辑账户域标识符，请按照以下步骤操作：

**步骤 5** 在“编辑账户标识符”部分，更改域标识符（编辑域或添加前缀）。

**步骤 6** 单击“确定”确认使用新的域 ID。

**步骤 7** 检查账户名称，根据需要进行编辑。

**步骤 8** 单击**继续**继续申请智能账户。

**注释** 如果您在申请智能账户期间对账户域标识符进行了编辑，思科会与您联系，以便完成审批流程。

**步骤 9** 可选步骤 – 输入公司信息。如果您在账户授权选项下选择“**否**”，则必须在必填字段中提供公司名称和地址。

**步骤 10** 可选步骤 – 输入您想为其授予管理员访问权限的用户的邮箱 ID，以指定具有管理员访问权限的用户。

**步骤 11** 检查智能账户信息，并对申请管理员访问权限的用户进行验证。接下来，单击**提交请求**。
提交智能账户请求后，您会收到一封确认账户申请已经完成的邮件。在指定人员完成授权之前，申请将处于待处理状态。

**注释** 申请提交后，即会创建相应的个人智能账户。您可以将订单分配至个人智能账户，但是该智能账户必须激活，才能使用所购买的产品/服务。

---

# 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

您可以选择要用于设备的智能许可证。请确保您用于设备的虚拟账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** 选中所需的许可证。

**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**。

第 14 章

# 快速索引

本节包含以下主题：



## 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<br>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。<br>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：7XEEX17D99-3X49X08 1），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 RV345/P 路由器 | http://www.cisco.com/en/US/products/ps9923/tsd_products_support_series_home.html |

快速索引