管理指南

思科 **RV130/RV130W** 边缘路由器

目录

目录

1

简介

本章提供的信息用于指导您完成安装过程并开始使用基于浏览器的设备管理器。

验证硬件安装

按照 《思科 RV130/130W 边缘路由器快速入门指南》配置设备，使其连接至您的有线和无线网络。

注意 请使用设备附带的 12 伏、 2 安电源。使用其他电源可能会降低性能或损坏设备。

要对硬件安装和互联网连接进行验证，请完成以下任务：

- 检查 LED 的状态。有关详情，请参阅设备附带的 《思科 RV130/130W 边缘路由器快速入门指南》。
- 将计算机连接至可用的 LAN 端口并确认您可以连接至互联网上的网站，如 www.cisco.com。
- 使用具有无线功能的 PC 连接至互联网上的网站，如 www.cisco.com。要配置无线功能，请参阅连接到您的无线网络。

使用设置向导

设置向导和设备管理器受以下浏览器支持：Microsoft Internet Explorer 6.0 或更高版本、 Mozilla Firefox 3.0 或更高版本，以及 Apple Safari 3.0 或更高版本。

要使用设置向导，请执行以下操作：

步骤 1 启动连接至 LAN 端口的计算机。

该计算机将成为设备的 DHCP 客户端，并将获得 192.168.1.xxx 范围内的 IP 地址。

步骤 2 启动 Web 浏览器，然后在地址栏中输入 **192.168.1.1**。此地址为设备的默认 IP 地址。

系统将显示一条关于站点安全证书的消息。设备使用自签名安全证书，系统显示该消息是由于设备对计算机来说是未知设备。

步骤 3 单击继续浏览此网站 （在您的特定 Web 浏览器上可能显示为其他选项）来继续访问网站。此时将显示登录页面。

步骤 4 输入用户名和密码。

默认用户名为 **cisco**。默认密码为 **cisco**。密码区分大小写。

步骤 5 单击 **Log In**。系统将启动设置向导。

步骤 6 按照屏幕上所显示的说明来设置设备。

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，设置向导会要求您提供有关您互联网连接的信息。您可能需要联系您的 ISP 来获取该信息。

设置向导完成设备的配置后，系统将要求您更改默认密码。按照屏幕上的说明进行操作。更改默认密码之后，系统将显示 **Getting Started** 页面。

配置后续步骤

虽然设置向导会自动配置设备，不过我们建议对一些设置进行自定义，以便提供更好的安全性和性能：

- 如果您已在网络上使用了 DHCP 服务器，而又不希望设备充当网络 DHCP 服务器，请禁用该服务器。请参阅配置 **LAN** 设置。
- 要配置虚拟专用网络 (VPN)，请参阅配置 **VPN**。
- 设备最多可支持四个无线网络。使用设置向导只能设置一个无线网络 （或 SSID）。要配置其他无线网络，请使用基于 Web 的设备管理器。请参阅配置无线网络。

使用 **Getting Started** 页面

Getting Started 页面显示设备上一些最常见的配置任务。单击网页上的链接可访问相关配置页面。

此页面在每次启动设备管理器时都会出现。要更改此行为，请选中 **Don't show on start up**。

Initial Settings

Change Default Administrator Password	显示 **Users** 页面，用于更改管理员密码以及设置访客帐户。请参阅配置用户帐户。
Launch Setup Wizard	启动设置向导。按照屏幕上的说明进行操作。
Configure WAN Settings	打开 **Internet Setup** 页面以更改参数。例如，设备主机名。请参阅配置 **WAN** 设置。
Configure LAN Settings	打开 **LAN Configuration** 页面以修改 LAN 参数。例如，管理 IP 地址。请参阅配置 **LAN** 设置。
Configure Wireless Settings	打开 **Basic Settings** 页面以管理无线功能。请参阅配置无线网络。

Quick Access

Upgrade Router Firmware	打开 **Firmware/Language Upgrade** 页面以升级设备固件或语言包。请参阅升级固件或更改语言。
Add VPN Clients	打开 **PPTP Server** 页面以设置和管理 VPN 隧道。请参阅配置 **PPTP**。
Configure Remote Management Access	打开 **Basic Settings** 页面以启用设备的基本功能。请参阅配置基本防火墙设置。

Device Status

System Summary	显示 **System Summary** 页面，其中显示设备的固件状态、 IPv4 和 IPv6 配置状态以及无线功能和防火墙的状态。请参阅查看系统摘要。
Wireless Status	显示 **Wireless Statistics** 页面，其中显示无线功能的状态。请参阅查看无线统计信息。
VPN Status	显示 **IPsec VPN Server** 页面，其中列出此设备所管理的 VPN。请参阅查看站点到站点 **IPsec VPN** 连接状态。

Other Resources

Support	单击可打开思科支持页面。
Forums	单击可访问思科在线支持论坛。

连接到您的无线网络

要将某个客户端设备 （例如计算机）连接到您的无线网络，请使用通过设置向导配置路由器时使用的无线安全性信息，在该客户端设备上配置无线连接。

以下步骤仅作举例之用；您配置设备时的操作可能与这些步骤有所出入。有关具体说明，请查看相应客户端设备的相关文档。

步骤 **1** 打开设备的无线连接设置窗口或程序。

您的计算机可能已安装了用于管理无线连接的专门软件；您也可以在 “ 控制面板 ” 下的网络连接或网络和 **Internet** 窗口中找到无线连接。（具体位置视您的操作系统而定。）

步骤 **2** 输入您在设置向导中为网络选择的网络名称 (SSID)。

步骤 **3** 选择加密类型，然后输入在设置向导中指定的安全密钥。

如果没有启用安全性功能 （不推荐），请将使用安全类型和密码短语配置的无线加密字段留空。

步骤 **4** 验证您的无线连接并保存您的设置。

2

查看设备状态

使用 **Status** 菜单中的页面可查看设备上 VPN、无线、活动的 TCP/IP 服务、强制网络门户设置以及事件日志的实时统计信息和配置设置。

要确保数据和统计信息在 Status 页面上经常更新，请从 **Refresh Rate** 下拉列表中选择刷新速率。

查看控制面板

选择 **Status** > **Dashboard** 可查看设备配置的静态视图。 Dashboard 页面显示有关设备固件版本、 CPU 和内存利用率、错误记录设置、 LAN、 WAN、无线、站点到站点 IPsec VPN 以及 PPTP VPN 服务器设置的信息。

要修改显示的信息，请单击 **details** 链接以访问相应部分的配置页面。有关管理 **Dashboard** 页面上显示的设置的详情，请参阅：

- 配置日志设置
- 配置基本站点到站点 **IPsec VPN**
- 配置 **LAN** 设置
- 配置有线 **WAN** 连接
- 配置基本无线设置

在 **Refresh Rate** 下拉列表中，选择用于在控制面板上刷新最新统计信息和参数值的速率。

当您单击 **Show Panel View** 时， Dashboard 页面还显示设备后面板的交互式视图。将鼠标悬停在每个端口上方可查看端口连接信息。

查看系统摘要

选择 **Status** > **System Summary** 可显示设备属性、IP 地址模式间的网络设置、防火墙、无线和 VPN 设置的详情。单击 **Refresh** 可查看最新信息。

单击带下划线的链接可访问相关配置窗口。例如，要修改 LAN IP 地址，请单击 **LAN IP**。此时将显示 LAN Configuration 窗口。

System Summary 页面分为以下部分显示信息：

System Information

- **Firmware Version** - 设备运行的当前软件版本。
- **Firmware MD5 Checksum** - 用于验证文件完整性的消息摘要算法。
- **Locale** - 路由器上安装的语言。
- **Language Version** - 安装的语言包版本。语言包版本应与当前安装的固件兼容。在某些情况下，较旧的语言包可以用于较新的固件映像。路由器会检查语言包版本是否与当前固件版本兼容。
- **Language MD5 Checksum** - 语言包的 MD5 校验和。
- **CPU Model** - 当前使用的 CPU 芯片集。
- **Serial Number** - 设备的序列号。
- **System Up Time** - 系统已经运行的时间长度。
- **Current Time** - 当天时间。
- **PID VID** - 设备的产品 ID 和版本 ID。

IPv4 Configuration

- **LAN IP** - 设备的 LAN IP 地址。
- **WAN IP** - 设备的 WAN IP 地址。要释放当前 IP 地址并获取新地址，请单击 **Release** 或 **Renew**。
- **Gateway** - 设备所连接的网关 （例如有线调制解调器）的 IP 地址。
- **Mode** - 如果启用了 NAT，则显示 **Gateway**，否则显示 **Router**。
- **DNS 1** - WAN 端口的主 DNS 服务器 IP 地址。
- **DNS 2** - WAN 端口的辅助 DNS 服务器 IP 地址。
- **DDNS** - 表示是启用还是禁用了 Dynamic DNS （动态 DNS）。

IPv6 Configuration

- **LAN IP** - 设备的 LAN IP 地址。
- **WAN IP** - 设备的 WAN IP 地址。
- **Gateway** - 设备所连接的网关 （例如有线调制解调器）的 IP 地址。
- **NTP** - 网络时间协议服务器 （主机名或 IPv6 地址）。
- **Prefix Delegation** - 从 ISP 处的设备返回的前缀，该前缀提供给设备上的 IPv6 地址。
- **DNS 1** - 主 DNS 服务器的 IP 地址。
- **DNS 2** - 辅助 DNS 服务器的 IP 地址。

Wireless Summary

显示在 **Wireless > Basic Settings** 页面上配置的无线网络的公用名称和安全设置。有关详情，请参阅配置基本无线设置。

Firewall Setting Status

显示 **Firewall > Basic Settings** 页面上配置的 DoS、 WAN 请求和远程管理设置。有关详情，请参阅配置基本防火墙设置。

VPN Setting Status

显示可用 IPsec 和 PPTP VPN 连接，以及每种 VPN 类型的已连接用户。

- **IPSec VPN Connections Available** - 可用 IPsec VPN 连接数。
- **PPTP VPN Connections Available** - 可用 PPTP VPN 连接数。
- **Connected IPSec VPN Users** - 已连接的 IPSec VPN 用户数。
- **Connected PPTP VPN Users** - 已连接的 PPTP VPN 用户数。

有关配置 VPN 服务器连接和用户帐户的详情，请参阅配置基本站点到站点 **IPsec VPN** 和配置 **PPTP**。

查看活动 **TCP/IP** 服务

选择 **Status > Active TCP/IP Services** 可查看设备上处于活动状态的 IPv4 和 IPv6 TCP/IP 连接。IPv4 和 IPv6 的 **Active Service List** 部分显示设备上处于活动状态的协议和服务。

查看无线统计信息

选择 **Status > Wireless Statistics** 可查看设备无线功能的无线统计信息数据。在 **Refresh Rate** 字段中，选择希望用于显示最新统计信息的速率。

要以千字节 (KB) 为单位显示四舍五入后的字节数，请选中 **Show Simplified Statistic Data** 复选框并单击 **Save**。默认情况下，字节数据以字节为单位显示，其他数字数据以长整型显示。

要重置无线统计信息计数器，请单击 **Clear Count**。计数器会在设备重启时重置。

查看强制网络门户状态

选择 **Status > Captive Portal** 可查看有关连接的强制网络门户用户的信息。有关在设备上配置强制网络门户的详情，请参阅配置强制网络门户。

查看站点到站点 IPsec VPN 连接状态

选择 **Status > Site-to-Site IPsec VPN** 可查看设备上活动站点到站点 IPsec VPN 策略的连接状态。有关配置 VPN 策略的信息，请参阅配置基本站点到站点 **IPsec VPN**。

要更改最新和实时连接状态的显示速率，请从 **Refresh Rate** 下拉列表中选择刷新速率。

默认情况下，字节数据以字节为单位显示，其他数字数据以长整型显示。要以千字节 (KB) 为单位显示四舍五入后的字节数，请选中 **Show Simplified Statistic Data** 框并单击 **Save**。

要终止活动 VPN 连接，请单击 **Disconnect**。

查看 IPsec VPN 服务器状态

选择 **Status > IPsec VPN Server** 可查看各 IPsec VPN 连接及连接持续时间的列表。有关配置 IPsec VPN 连接的详情，请参阅配置 **IPsec VPN** 服务器。

查看 PPTP 服务器

选择 **Status > PPTP Server** 可查看各 PPTP VPN 连接、连接持续时间以及可以对此连接执行的操作的列表。有关配置 PPTP VPN 连接的详情，请参阅配置 **PPTP**。

查看日志

选择 **Status > View Logs**。单击 **Refresh Logs** 可显示最新日志条目。

要过滤日志或指定要显示的日志的严重性，请选中日志类型旁的框，然后单击 **Go**。请注意，将自动包含所选日志类型之上的所有日志类型，并且不能取消选择这些类型。例如，选中 **Error** 复选框可自动包含紧急、警报和严重日志以及错误日志。

下面按照从高到低的顺序列出了事件的严重性级别：

- **Emergency** - 系统无法使用。
- **Alert** - 需要采取措施。
- **Critical** - 系统处于高危状态。
- **Error** - 系统出错。
- **Warning** - 系统已发出警告。
- **Notification** - 系统能够正常工作，但系统已发出通知。
- **Informational** - 设备信息。
- **Debugging** - 提供关于事件的详情。

要删除日志窗口中的所有条目，请单击 **Clear Logs**。

要将所有日志消息从设备保存到本地硬盘驱动器，请单击 **Save Logs**。

要指定每页显示的条目数，请从下拉菜单中选择数字。

要在日志页面之间移动，请使用页面导航按钮。

查看连接的设备

Connected Devices 页面显示有关连接到您路由器的活动客户端设备的信息。要查看连接的设备，请选择 **Status > Connected Devices**。

要指定要显示的接口类型，请从 **Filter** 下拉菜单中选择值：

- **All** - 连接到路由器的所有设备。
- **Wireless** - 通过无线接口连接的所有设备。
- **Wired** - 通过路由器上的以太网端口连接的所有设备。
- **WDS** - 连接到路由器的无线分布式系统 (WDS) 设备。

IPv4 ARP Table 显示来自响应设备地址解析协议 (ARP) 请求的其他路由器的信息。如果某个设备未响应请求，则该设备将从列表中移除。

IPv6 NDP Table 显示连接到设备本地链路的所有 IPv6 邻居发现协议 (NDP) 设备。

查看端口统计信息

Port Statistics 页面显示详细端口活动。

要查看端口统计信息，请选择 **Status > Port Statistics**。

要定期刷新页面，请从 **Refresh Rate** 下拉列表中选择刷新速率。

要以千字节 (KB) 为单位显示四舍五入后的字节数，请选中 **Show Simplified Statistic Data** 框并单击 **Save**。默认情况下，字节数据以字节为单位显示，其他数字数据以长整型显示。

要重置端口统计信息计数器，请单击 **Clear Count**。

Port Statistics 页面显示以下信息：

Interface	网络接口的名称。
Packet	已接收 / 发送的数据包数。
Byte	每秒接收 / 发送的信息字节数。
Error	已接收 / 发送的数据包错误数。

Dropped	已接收 / 发送但丢弃的数据包数。
Multicast	通过此无线功能发送的组播数据包数。
Collisions	此端口上发生的信号冲突数。如果端口与连接至此端口的另一个路由器或计算机上的端口同时尝试发送数据，则会发生冲突。

查看移动网络状态

有关设备上配置的移动 3G/4G 网络和通信设备 （装置）的移动网络统计信息。

要查看移动网络状态，请选择 **Status > Mobile Network**。系统将显示以下信息：

- **Connection** - 连接至访客网络的设备。
- **Internet IP Address** - 分配给 USB 设备的 IP 地址。
- **Subnet Mask** - USB 设备的子网掩码。
- **Default Gateway** - 默认网关的 IP 地址。
- **Connection Up Time** - 链路已运行的时间长度。
- **Current Session Usage** - 移动链路上所接收 (Rx) 和发射 (Tx) 的数据量。
- **Monthly Usage** - 每月下载的数据和带宽使用情况。
- **Manufacturer** - 卡制造商名称。
- **Card Model** - 卡型号。
- **Card Firmware** - 卡固件版本。
- **SIM Status** - 用户标识模块 (SIM) 状态。
- **IMS** - 与 GSM、 UMTS 或 LTE 网络移动电话用户关联的唯一标识。
- **Carrier** - 移动网络运营商。
- **Service Type** - 访问的服务类型。
- **Signal Strength** - 无线移动网络信号的强度。
- **Card Status** - 数据卡的状态。

3

配置网络

本章介绍如何在设备上配置网络设置。

配置 **WAN** 设置

可以通过 WAN 端口或 USB 端口上安装的无线调制解调器来建立互联网连接。本节介绍如何配置 WAN、移动网络以及故障切换和恢复。

配置有线 **WAN** 连接

根据您所拥有的互联网连接类型， IPv4 网络 WAN 属性的配置会有所不同。

配置 **DHCP**

如果您的互联网服务提供商 (ISP) 使用动态主机控制协议 (DHCP) 为您分配 IP 地址，您会在每次登录时收到动态生成的 IP 地址。

配置 DHCP WAN 设置的步骤：

步骤 **1** 选择 **Networking** > **WAN**。

步骤 2 从 **Internet Connection Type** 下拉列表中，选择 **Automatic Configuration - DHCP**。

步骤 3 从 **DNS Server Source** 下拉列表中，选择以下方式之一设置 DNS 服务器地址：

- 如果已拥有 ISP 提供的 DNS 服务器地址，请选择 **Use these DNS Servers**，然后输入主地址和辅助地址。
- 如果没有 ISP 提供的 DNS 服务器地址，请选择 **Get Dynamically from ISP**。
- 要使用 OpenDNS 提供的 DNS 服务器 （208.67.222.222、 208.67.220.220）解析 Web 地址，请选择 **Use OpenDNS**。

步骤 4 单击 **Save**。

配置静态 IP

如果 ISP 分配给您的是永久 IP 地址，请执行以下步骤来配置 WAN 设置：

步骤 1 选择 **Networking** > **WAN**。

步骤 2 从 **Internet Connection Type** 下拉菜单中，选择 **Static IP**。

步骤 3 输入以下信息：

Internet IP Address	WAN 端口的 IP 地址。
Subnet mask	WAN 端口的子网掩码。
DNS Server Source	DNS 服务器地址。如果已拥有 ISP 提供的 DNS 服务器地址，请选择 **Use these DNS Servers**，然后在 **Static DNS 1** 和 **Static DNS 2** 字段中输入主地址和辅助地址。 要使用 OpenDNS 提供的 DNS 服务器（208.67.222.222、 208.67.220.220）解析 Web 地址，请选择 **Use OpenDNS**。
Default Gateway	默认网关的 IP 地址。

步骤 4 单击 **Save**。

配置 PPPoE

配置基于以太网的点对点协议 (PPPoE) 设置的步骤：

步骤 1 选择 **Networking** > **WAN**。

步骤 2 从 **Internet Connection Type** 下拉菜单中，选择 **PPPoE**。

步骤 3 选择 PPPoE 简档，或单击 **Configure Profile** 创建新的简档。

步骤 4 在 PPPoE Profiles 页面上，输入以下信息 （可能需要联系 ISP，以获取 PPPoE 登录信息）：

Profile Name	PPPoE 简档的唯一名称。
Username	ISP 分配的用户名。
Password	ISP 分配的密码。
DNS Server Source	DNS 服务器地址。如果已拥有 ISP 提供的 DNS 服务器地址，请选择 **Use these DNS Servers**，然后输入主地址和辅助地址。如果没有，请选择 **Get Dynamically from ISP**。 要使用 OpenDNS 提供的 DNS 服务器（208.67.222.222、 208.67.220.220）解析 Web 地址，请选择 **Use OpenDNS**。

Connect on Demand	如果 ISP 根据您连接的时长收费，请选择此选项。选择此选项时，只有存在流量时，才打开互联网连接。如果连接处于空闲状态（即没有流量），则关闭连接。如果单击 **Connect on Demand**，请在 **Max Idle Time** 字段中输入关闭连接之前等待的分钟数。
Keep Alive	选择此选项时，互联网连接始终打开。在 redial period 字段中，输入设备在断开连接后尝试重新连接之前等待的秒数。
Authentication Type	**Auto-negotiation** - 服务器发送指明其安全算法设置的配置请求。设备随后发送回与服务器所发送的安全类型一致的鉴权凭证。 **PAP** - 点对点协议用于连接至 ISP 的密码鉴别协议 (PAP)。 **CHAP** - 询问握手鉴权协议 (CHAP) 要求客户端和服务器都知道安全密钥明文才能使用 ISP 服务。 **MS-CHAP** 或 **MS-CHAPv2** - 用于访问 ISP 服务的 Microsoft 版本的 CHAP。

步骤 **5** 单击 **Save**。

配置 PPTP

配置 PPTP 设置的步骤：

步骤 **1** 选择 **Networking** > **WAN**。

步骤 **2** 从 **Internet Connection Type** 下拉菜单中，选择 **PPTP**。

步骤 **3** 输入以下信息：

Internet IP Address	WAN 端口的 IP 地址。
Subnet mask	WAN 端口的子网掩码。
Default Gateway	默认网关的 IP 地址。
PPTP Server	点对点隧道协议服务器的 IP 地址。

Username	ISP 分配给您的用户名。
Password	ISP 分配给您的密码。
Connect on Demand	如果 ISP 根据您连接的时长收费，请选择此选项。选择此选项时，只有存在流量时，才打开互联网连接。如果连接处于空闲状态（即没有流量），则关闭连接。如果单击 **Connect on Demand**，请在 **Max Idle Time** 字段中输入关闭连接之前等待的分钟数。
Keep Alive	选择此选项时，互联网连接始终打开。在 **Redial period** 字段中，输入设备在断开连接后尝试重新连接之前等待的秒数。
Authentication Type	选择鉴权类型： **Auto-negotiation** - 服务器发送指明其安全算法设置的配置请求。设备随后发送回服务器之前所发送的安全类型的鉴权凭证。 **PAP** - 设备使用密码鉴别协议 (PAP) 连接至 ISP。 **CHAP** - 设备在连接至 ISP 时使用询问握手鉴权协议 (PAP)。 **MS-CHAP** 或 **MS-CHAPv2** - 设备在连接至 ISP 时使用 Microsoft 询问握手鉴权协议。
Service Name	输入新 PPTP 服务的名称。
MPPE Encryption	选中 **Enable** 复选框可为 PPTP 连接启用 Microsoft 点对点加密。
DNS Server Source	DNS 服务器地址。如果已拥有 ISP 提供的 DNS 服务器地址，请选择 **Use these DNS Servers**，然后在 **Static DNS 1** 和 **Static DNS 2** 字段中输入主地址和辅助地址。 要从 ISP 获取 DNS 服务器地址，请选择 **Get Dynamically from ISP**。 要使用 OpenDNS 提供的 DNS 服务器（208.67.222.222、 208.67.220.220）解析 Web 地址，请选择 **Use OpenDNS**。

步骤 **4** （可选）要配置可选设置，请参阅配置可选设置。

步骤 5 单击 **Save**。

配置 L2TP

配置 L2TP 设置的步骤：

步骤 1 选择 **Networking** > **WAN**。

步骤 2 从 **Internet Connection Type** 下拉菜单中，选择 **L2TP**。

步骤 3 输入以下信息：

Internet IP Address	WAN 端口的 IP 地址。
Subnet mask	WAN 端口的子网掩码。
Default Gateway	默认网关的 IP 地址。
L2TP Server	L2TP 服务器的 IP 地址。
Version	要使用的 L2TP 版本。如果选择版本 3，请输入供应商 ID 和虚拟电路 ID。
Cookie Length	L2TP v3 数据包中用于识别 L2TP 会话的 Cookie 的大小。
Vendor ID	L2TP 的 AVP 编码格式中包含的供应商 ID。 要在 AVP 中使用接受 IETF 属性值，请选择 Standard。 要实施思科的 L2TP 扩展和专用属性值，请选择 Cisco。
Virtual Circuit ID	用于传输 L2TP 数据包的第 2 层电路的标识符。如果选择 Cisco 作为 L2TP v3 的 **Vendor ID**，则需要此信息。
Username	输入 ISP 分配给您的用户名。
Password	输入 ISP 分配给您的密码。
Connect on Demand	如果 ISP 根据您连接的时长收费，请选择此选项。选择此选项时，只有存在流量时，才打开互联网连接。如果连接处于空闲状态（即没有流量），则关闭连接。如果单击 **Connect on Demand**，请在 **Max Idle Time** 字段中输入关闭连接之前等待的分钟数。

Keep Alive	选择此选项时，互联网连接始终打开。在 redial period 字段中，输入设备在断开连接后尝试重新连接之前等待的秒数。
Authentication Type	**Auto-negotiation** - 服务器发送指明其安全算法设置的配置请求。设备随后发送回与服务器所发送的安全类型一致的鉴权凭证。 **PAP** - 使用密码鉴别协议 (PAP) 连接至 ISP。 **CHAP** - 使用询问握手鉴权协议 (PAP) 连接至 ISP。 **MS-CHAP** 或 **MS-CHAPv2** - 使用 Microsoft 询问握手鉴权协议连接至 ISP。
Service Name	输入新 L2TP 服务的名称。
MPPE Encryption	选中 **Enable** 可为 L2TP 连接启用 Microsoft 点对点加密。
DNS Server Source	DNS 服务器地址。 如果已拥有 ISP 提供的 DNS 服务器地址，请选择 **Use these DNS Servers**，然后在 **Primary DNS Server** 和 **Secondary DNS Server** 字段中输入主地址和辅助地址。 要从 ISP 获取 DNS 服务器地址，请选择 **Get Dynamically from ISP**。 要使用 OpenDNS 提供的 DNS 服务器（208.67.222.222、 208.67.220.220）解析 Web 地址，请选择 **Use OpenDNS**。

步骤 **4** 单击 **Save**。

配置可选设置

配置可选设置的步骤：

步骤 **1** 在 **Optional Settings** 部分中，配置以下设置：

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。 除非 ISP 要求更改，否则建议选择 **Auto**。默认 MTU 大小为 1500 字节。 如果 ISP 要求自定义 MTU 设置，请选择 **Manual** 并输入 MTU 大小。
Size	自定义 MTU 大小。以太网网络的 MTU 标准值通常为 1500 字节。对于 PPPoE 连接，该值为 1492 字节。
Untagged VLAN	选中此框可启用 VLAN 标记功能。启用 （默认设置）时，所有流量都使用 VLAN ID 进行标记。 默认情况下，设备上的所有流量都使用 VLAN 1 （默认的非标记 VLAN）。所有流量都是不加标记的，直至您禁用非标记 VLAN、更改非标记流量 VLAN ID 或更改 VLAN ID。
Untagged VLAN ID	非标记 VLAN 的 ID 为介于 1 与 4094 之间的数字。默认值为 1。在此字段中指定的 VLAN 上的流量在转发到网络时，不使用 VLAN ID 进行标记。 VLAN 1 是默认的非标记 VLAN。
AP Management VLAN	与用于访问配置为接入点的设备的 IP 地址关联的 VLAN。 如果创建其他 VLAN，为了安全起见，请选择与在网络中其他交换机上配置的 VLAN 对应的值。可能需要更改管理 VLAN 以限制对设备管理器的访问。

步骤 **2** 单击 **Save**。

配置移动网络

选择 **Networking > WAN > Mobile Network** 可将设备配置为连接至移动宽带 USB 调制解调器 （连接至其 USB 接口）。

配置全局移动网络设置

为受支持的 USB 设备配置全局设置的步骤：

步骤 **1** 连接 USB 调制解调器。如果支持调制解调器，则系统会自动检测它并将其显示在 Mobile Network 页面上。

步骤 **2** 选择 **Auto** 或 **Manual** 连接模式。仅当连接模式设置为 Auto 时，以太网连接恢复才起作用。

- 要使调制解调器能够自动建立连接，请选择 **Auto** 模式。如果选择 Auto，请设置 **Connect on Demand** 时间或选择 **Keep Alive**。在互联网连接非活动时间达到 **Max Idle Time** 字段中指定的时间段之后， Connect on Demand 会终止连接。

  如果互联网连接由于非活动而被终止，则调制解调器会在用户尝试访问互联网时自动重新建立连接。在 **Max Idle Time** 字段中，输入互联网连接终止前空闲的分钟数。选择 **Keep Alive** 可使连接始终保持活动状态。

- 要手动连接或断开调制解调器连接，请选择 **Manual** 模式。

设备显示当前调制解调器连接状态，包括正在初始化、正在连接、正在断开连接或已断开连接。

步骤 **3** 确认 **Card Status** 字段显示您的移动卡为 **Connected**。

手动配置移动网络设置

要在 **Mobile Network Setup** 区域中更改移动网络参数，请单击 **Manual** 单选按钮。设备会自动检测支持的调制解调器并列出相应的配置参数。要覆盖全局参数，请选择 **Manual**。

步骤 **1** 在以下字段中输入信息：

字段	说明
Access Point Name (APN)	移动设备连接至的互联网网络。输入移动网络服务提供商提供的接入点名称。如果不知道接入点的名称，请与服务提供商联系。
Dial Number	移动网络服务提供商提供的用于连接互联网的拨号号码。

字段	说明
User Name Password	移动网络服务提供商提供的用户名和密码。
SIM Check	启用或禁用 SIM 卡检查。
SIM PIN	与 SIM 卡关联的 PIN 码。只有 GSM SIM 卡才显示此字段。 可以在 Auto 或 Manual 模式下修改 SIM PIN。
Server Name	用于互联网连接的服务器的名称 （如果服务器提供商提供）。
Authentication	服务提供商使用的鉴权。可以通过从下拉列表中选择鉴权类型来更改该值。默认为 Auto。如果不知道要使用的鉴权类型，请选择 Auto。
Service Type	最常用的移动数据服务连接类型 （基于区域服务信号）。如果您的位置仅支持一种移动数据服务，则可以限制首选选项，从而减少连接设置时间。第一选择始终搜索 HSPDA/3G/UMTS 服务，并在 GPRS 可用时自动切换为 GPRS。
LTE Service	长期演进 (LTE) 服务设置。 **Auto** 基于区域服务信号选择信号。 **4G only** 仅搜索 4G 信号。 **3G only** 仅搜索 3G 信号。

步骤 2 单击 **Save** 保存设置。

带宽上限设置

设备会监控移动网络链路上的数据活动，并在达到给定阈值时发出通知。

启用或禁用 Bandwidth Cap Tracking 并设置上限的步骤：

步骤 1 单击 **Enabled** 或 **Disabled**。

步骤 2 从下拉列表中选择 Monthly Renewal Date 以指示每月重置带宽上限的日期。

步骤 3 在 **Monthly Bandwidth Cap** 字段中，以兆字节为单位输入在设备执行操作 （如向管理员发送电子邮件）之前允许通过的最大数据量。

电子邮件设置

当达到带宽数据上限时，可以向管理员发送电子邮件消息。要设置目标电子邮件地址，请参阅配置日志电子邮件。

通过选中框来启用之后，将在以下时间发送电子邮件：

- 移动网络使用率超过给定百分比。
- 设备故障切换到备份路径并恢复。
- 移动网络链路处于活动状态期间，每经过指定间隔时。

设置故障切换和恢复

虽然以太网和移动网络链路都可用，但是一次只能使用一个连接建立 WAN 链路。当某个 WAN 连接中断时，设备会尝试在其他接口上建立连接。此功能称为*故障切换*。当主 WAN 连接恢复后，连接将恢复至原始路径并结束备份连接。此功能称为*恢复*。

步骤 1 选择 **Networking > WAN > Failover & Recovery** 以显示 Failover & Recovery 窗口。

步骤 2 选择 **Enable Failover to 3G WAN** 以启用移动网络链路并将其设置为从以太网链路进行故障切换。当以太网 WAN 链路处于不活动状态时，设备尝试在 USB 接口上启用移动网络链路。（如果故障切换未启用，则移动网络链路始终禁用。）

步骤 3 选择 **Enable Recovery back to Ethernet WAN** 以使链路可以返回为以太网链路，从而中断移动网络链路。**WAN > Mobile Network** 连接模式必须设置为 Auto 才能使用以太网 WAN 连接恢复。

步骤 4 在 **Failover Check Interval** 字段中，输入设备必须尝试检测移动网络链路上的物理连接或是否存在流量的频率 （以秒为单位）。如果链路处于空闲状态，则设备按此间隔尝试对目标执行 Ping 命令。如果没有回复 Ping 数据包，则设备认为链路中断并重试以太网 WAN 接口。

步骤 5 在 **Recovery Check Interval** 字段中，输入设备必须尝试检测以太网 WAN 链路上的物理连接或是否存在流量的频率 （以秒为单位）。如果链路处于空闲状态，则设备按此间隔尝试对目标执行 Ping 命令。如果回复了 Ping 数据包，则设备认为链路处于连接状态，然后尝试禁用移动网络链路并启用以太网 WAN 接口。

步骤 6 单击 ***Switch back to Ethernet immediately when Ethernet is available***，或单击 ***Switch back to Ethernet in a specific time range***，然后输入范围的开始和结束时间。

步骤 7 在 **Connection Validation Site** 字段中，选择要从中执行故障切换验证的站点。使用下一个步跳网关 （默认情况下设备会对默认网关执行 Ping 命令），或选择自定义站点并输入站点 IPv4 或 IPv6 地址。

步骤 8 单击 **Save** 保存设置。

WAN 接口表显示与互联网连接的以太网 WAN 和移动网络链路的状态。单击 **Status** 超链接以查看端口详情。

配置 LAN 设置

默认的 DHCP 和 TCP/IP 设置适用于大多数应用。如果希望网络上的另一个 PC 作为 DHCP 服务器，或如果要手动配置所有设备的网络设置，请禁用 DHCP。

您还可以使用 Windows 互联网命名服务 (WINS) 服务器，而不是使用将互联网域名（例如 www.cisco.com）映射到 IP 地址的 DNS 服务器。 WINS 服务器与 DNS 服务器等效，只是使用 NetBIOS 协议解析主机名。设备在其发送给 DHCP 客户端的 DHCP 配置中包含 WINS 服务器的 IP 地址。

如果您的设备连接至调制解调器，或连接至在相同子网 (192.168.1.x) 上配置了网络的另一个设备，它会自动将 LAN 子网更改为基于 10.x.x.x 的随机子网，避免与路由器 WAN 端的子网冲突。

更改设备管理 IP 地址

设备的本地设备管理 IP 地址是静态地址，默认为 192.168.1.1。

更改本地设备管理 IP 地址的步骤：

步骤 1 选择 **Networking** > **LAN** > **LAN Configuration**。

步骤 2 在 **IPv4** 部分中，输入以下信息：

VLAN	VLAN 编号。
Local IP Address	设备的本地 LAN IP 地址。确保此 IP 地址未被其他设备使用。
Subnet mask	本地 IP 地址的子网掩码。默认子网掩码为 255.255.255.0。

步骤 3 单击 **Save**。

更改设备的 IP 地址之后，您的 PC 将无法再显示设备管理器。

要显示设备管理器，请执行以下操作之一：

- 如果在设备上配置 DHCP，请释放并更新 PC IP 地址。
- 手动给 PC 分配 IP 地址。分配的地址必须与设备位于同一子网。例如，如果将设备 IP 地址更改为 10.0.0.1，分配的 PC IP 地址必须在 10.0.0.2 到 10.0.0.255 范围内。

打开新浏览器窗口，然后输入要重新连接的设备的新 IP 地址。

配置 DHCP 服务器

默认情况下，本设备用作无线 LAN (WLAN) 或有线 LAN 上的主机的 DHCP 服务器。它分配 IP 地址，并提供 DNS 服务器地址。

启用 DHCP 时，设备从 IPv4 地址池中为 LAN 上的其他网络设备分配 IP 地址。分配之前，设备会先对每个地址进行测试，以避免 LAN 上出现重复地址。

默认 IP 地址池为 192.168.1.100 到 192.168.1.149。要在网络设备上设置静态 IP 地址，请使用该池之外的 IP 地址。例如，假设 DHCP 池设置为默认参数， IP 地址池中从 192.168.1.2 到 192.168.1.99 的静态 IP 地址可以用于避免与 DHCP IP 地址池冲突。

配置 DHCP 设置的步骤：

步骤 1 选择 **Networking** > **LAN** > **LAN Configuration**。

步骤 2 （可选）从下拉列表中选择要编辑的 VLAN。

步骤 3 在 **DHCP Server** 字段中，选择以下选项之一：

Enable	允许设备充当网络中的 DHCP 服务器。
Disable	如果您想要手动配置所有网络设备的 IP 地址，请在设备上禁用 DHCP。
DHCP Relay	将另一个 DHCP 服务器分配的 IP 地址中继到网络设备。

如果启用了设备 DHCP 服务器，请输入以下信息：

Starting IP Address	IP 地址池中的第一个地址。加入 LAN 的任何 DHCP 客户端都将分配到一个此范围内的 IP 地址。
Maximum Number of DHCP Users	最大 DHCP 客户端数。
IP Address Range	（只读）对 DHCP 客户端可用的 IP 地址范围。
Client Lease time	IP 地址租用给客户端的持续时间 （以小时为单位）。
Static DNS 1	主 DNS 服务器的 IP 地址。
Static DNS 2	辅助 DNS 服务器的 IP 地址。
Static DNS 3	三级 DNS 服务器的 IP 地址。
WINS	主 WINS 服务器的 IP 地址。

步骤 4 如果选择了 **DHCP Relay**，请在 **Remote DHCP Server** 字段中输入中继网关的地址。中继网关会将 DHCP 消息传输给网络设备，包括其他子网上的设备。

步骤 5 单击 **Save**。

配置 VLAN

虚拟 LAN (VLAN) 是网络中按功能或其他共享特性联合起来的一组端点。与通常基于地理特性的 LAN 不同， VLAN 可以不按设备或用户的物理位置对端点进行分组。

设备有一个不能删除的默认 VLAN (VLAN 1)。您最多可在设备上另外创建 4 个 VLAN。

创建 VLAN 的步骤：

步骤 1 选择 **Networking** > **LAN** > **VLAN Membership**。

步骤 2 单击 **Add Row**。

步骤 3 输入以下信息：

VLAN ID	要分配给 VLAN 成员关系中的端点的数字形式的 VLAN ID。输入的数字必须在 3 到 4094 之间。 VLAN ID 1 保留为默认 VLAN，用于接口上接收到的非标记帧。
Description	标识 VLAN 的说明。
Port 1 **Port 2** **Port 3** **Port 4**	可以将设备上的 VLAN 关联到设备上的 LAN 端口。默认情况下，所有 LAN 端口都属于 VLAN1。您可以编辑这些端口，以将它们与其他 VLAN 关联。为每个端口选择传出帧类型： **Untagged** - 接口为 VLAN 的非标记成员。 VLAN 帧以不带标记的方式发送到端口 VLAN。 **Tagged** - 端口是 VLAN 的标记成员。 VLAN 帧以带标记的方式发送到端口 VLAN。 **Excluded** - 端口当前不是 VLAN 的成员。这是首次创建 VLAN 时所有端口的默认选项。

步骤 4 单击 **Save**。

要编辑 VLAN 的设置，请选择 VLAN 并单击 **Edit**。要删除所选 VLAN，请单击 **Delete**。单击 **Save** 应用更改。

配置静态 DHCP

可以配置路由器，以将特定的 IP 地址分配给具有特定 MAC 地址的客户端设备。

配置静态 DHCP 的步骤：

步骤 1 选择 **Networking** > **LAN** > **Static DHCP**。

步骤 2 从 **VLAN** 下拉菜单中选择 VLAN 编号。

步骤 3 单击 **Add Row**。

步骤 4 输入以下信息：

Description	客户端说明。
IP Address	要分配给客户端设备的 IP 地址。分配的 IP 地址应在 DHCP 地址池之外。 静态 DHCP 分配意味着每当客户端设备连接至网络时，DHCP 服务器都会为一个已定义的 MAC 地址分配同一个 IP 地址。 当使用相应 MAC 地址的客户端设备请求 IP 地址时， DHCP 服务器会为其分配保留的 IP 地址。
MAC Address	客户端设备的 MAC 地址。 MAC 地址的格式是 XX:XX:XX:XX:XX:XX，其中 X 是从 0 到 9（包含 0 和 9）的数字或介于 A 与 F （包含 A 和 F）的字母。

要编辑静态 DHCP 客户端的设置，请选择客户端并单击 **Edit**。要删除所选 DHCP 客户端，请单击 **Delete**。单击 **Save** 应用更改。

查看租用 DHCP 的客户端

可以查看网路上的端点 （通过主机名、 IP 地址或 MAC 地址进行标识）列表，并查看由 DHCP 服务器分配给这些端点的 IP 地址。还会显示端点的 VLAN。

要查看 DHCP 客户端，请选择 **Networking** > **LAN** > **DHCP Leased Client**。

对于设备上定义的每个 VLAN，会以表格的形式显示与相应 VLAN 关联的客户端列表。

将静态 IP 地址分配给连接的设备之一的步骤：

步骤 1 在连接的设备对应行中，选中 **Add to Static DHCP**。

步骤 2 单击 **Save**。

设备上的 DHCP 服务器会始终分配设备请求 IP 地址时显示的 IP 地址。

配置 DMZ 主机

设备支持非军事区 (DMZ)。 DMZ 是一个子网，向公众开放但位于防火墙后面。可以使用 DMZ 将传输到 WAN 端口 IP 地址的数据包重定向到 LAN 中特定 IP 地址。

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。您可以将防火墙规则配置为允许从 LAN 或 WAN 访问 DMZ 中的特定服务和端口。倘若 DMZ 节点遭到攻击， LAN 不一定会受到攻击。

必须为指定为 DMZ 主机的端点配置一个固定 （静态） IP 地址。向 DMZ 主机分配的 IP 地址应处于与设备 LAN IP 地址相同的子网中，但是该地址不能与分配给此网关 LAN 接口的 IP 地址相同。

配置 DMZ 的步骤：

步骤 1 选择 **Networking** > **LAN** > **DMZ Host**。

步骤 2 选中 **Enable** 以在网络上启用 DMZ。

步骤 3 从 **VLAN** 下拉菜单中选择启用了 DMZ 的 VLAN 的 ID。

步骤 4 在 **Host IP Address** 字段中，输入 DMZ 主机的 IP 地址。 DMZ 主机是接收重定向的数据包的端点。

步骤 5 单击 **Save**。

配置 RSTP

快速生成树协议 (RSTP) 是一种网络协议，可避免网络中的循环并动态重新配置应转发帧的物理链路。配置快速生成树协议 (RTSP) 的步骤：

步骤 1 选择 **Networking** > **LAN** > **RSTP**。

步骤 2 输入以下信息：

System Priority	从下拉菜单中选择系统优先级。系统优先级可选范围为 0 至 61440 （增量为 4096）。有效值有 0、4096、 8192、 12288、 16384、 20480、 24576、28672、 32768、 40960、 45056、 49152、53248、 57344 和 61440。 系统优先级越低，设备便更可能成为生成树中的根。默认值为 **327688**。
Hello Time	问候时间是生成树的根在发送问候消息之前等待的时间段。输入 1 到 10 之间的数字。默认值为 **2**。
Max Age	最长时间是路由器等待接收问候消息的时间段。如果达到最大时间，路由器会尝试更改生成树。输入 6 到 40 之间的数字。默认值为 **20**。
Forward Delay	转发延迟是接口从阻塞变为转发状态之间的间隔。输入 4 到 30 之间的数字。默认值为 **15**。
Force Version	选择要使用的默认协议版本。选择 **Normal** （使用 RSTP）或 **Compatible** （与旧 STP 兼容）。默认值为 **Normal**。

步骤 3 在 **Setting Table** 中，配置以下设置：

Protocol Enable	选中可在关联端口上启用 RSTP。 RSTP 在默认情况下为禁用状态。
Edge	选中可指定关联端口为边缘端口 （终端站）。取消选中可指定关联端口为指向其他 STP 设备的链路 （网桥）。边缘端口在默认情况下为启用状态。
Path Cost	为指定端口输入 RSTP 路径成本。默认值为 0 （设备自动确定路径值）。也可以输入 2 到 200000000 之间的数字。

步骤 4 单击 **Save**。

端口管理

可以配置设备 LAN 端口的速度和流量控制设置。

配置端口速度和流量控制的步骤：

步骤 1 选择 **Networking** > **Port Management**。

步骤 2 配置以下信息：

Port	端口号。
Link	端口速度。如果没有设备连接至端口，则此字段显示 **Down**。
Mode	从下拉菜单中选择以下端口速度之一： • **Auto Negotiation** - 设备和连接的设备选择公用速度。 • **10Mbps Half** - 两个方向都为 10 Mbps，但一次只能在一个方向上传输。 • **10Mbps Full** - 两个方向上同时为 10 Mbps。 • **100Mbps Half** - 个方向都为 100 Mbps，但一次只能在一个方向上传输。 • **100Mbps Full** - 两个方向上同时为 100Mbps。
Jumbo Frame	选中可在设备上启用巨型帧并在 LAN 上发送帧（每帧最多包含 9,000 字节数据）。标准以太网帧包含 1,500 字节数据。
Flow Control	选中可启用此端口的流量控制。 流量控制是管理两个节点之间数据传输速率，以防止较快发送者速度超过较慢接收者的过程。它为接收者提供了一种控制传输速度的机制，避免接收节点从传输节点接收到过量数据。

步骤 3 单击 **Save**。

配置链路聚合

使用 Link Aggregation 页面可将多个以太网链路分组为单个逻辑信道。链路聚合组可增加累积带宽而无需硬件升级，从而提高了设备的成本效益，并可在出现单个端口或电缆故障时促进实现简单重新路由。

向链路聚合组分配端口的步骤：

步骤 1 选择 **Networking > LAN > Link Aggregation**。 **Port Status** 部分显示与设备上每个端口关联的模式以及状态。

步骤 2 在 **Link Aggregation Setting Table** 部分中，选中各个端口对应的复选框以将其包含在组中。

步骤 3 单击 **Save**。

复制 MAC 地址

有时，可能需要将设备 WAN 端口的 MAC 地址设置为与您的 PC 或其他 MAC 地址相同的 MAC 地址。这称为 MAC 地址复制。

例如，一些 ISP 会在首次安装服务时注册您的计算机卡的 MAC 地址。将路由器置于有线调制解调器或 DSL 调制解调器之后时，ISP 无法识别来自设备 WAN 端口的 MAC 地址。

在这种情况下，要将设备配置为可被 ISP 识别，需要将 WAN 端口的 MAC 地址复制为与计算机 MAC 地址相同。

配置 MAC 地址复制的步骤：

步骤 1 选择 **Networking** > **MAC Address Clone**。

步骤 2 在 **MAC Address Clone** 字段中，选中 **Enable**。

步骤 3 要设置设备 WAN 端口的 MAC 地址，请执行以下操作之一：

- 要将 WAN 端口的 MAC 地址设置为 PC MAC 地址，请单击 **Clone My PC's MAC**。
- 要指定另一个 MAC 地址，请在 **MAC Address** 字段中输入。

步骤 4 单击 **Save**。

配置路由

使用 Routing 页面可为设备配置操作模式和其他路由选项。

配置操作模式

配置操作模式的步骤：

步骤 1 选择 **Networking** > **Routing**。

步骤 2 在 **Operating Mode** 字段中，选择以下选项之一：

Gateway	用于将设备作为网关使用。（推荐） 如果设备要同时用于承载互联网网络连接并执行路由功能，请保留此默认设置。
Router	（仅限高级用户）用于将设备作为路由器使用。 如果设备所在的网络中存在其他路由器，请选择此选项。 启用 Router 模式会在设备上禁用 NAT （网络地址转换）。

步骤 3 单击 **Save**。

配置动态路由

路由信息协议 (RIP) 是内部网络中常用的内部网关协议 (IGP)。路由器通过此协议可彼此自动交换路由信息，并动态调整路由表以适应网络中的变化。

设备通过动态路由 (RIP) 可以自动调整，以适应网络布局的物理更改，并与其他路由器交换路由表。

路由器会以源与目标之间的步跳数最少为原则，确定网络数据包的路由。

注 默认情况下， RIP 在设备上为禁用状态。

配置动态路由的步骤：

步骤 1 选择 **Networking** > **Routing**。

步骤 2 配置以下设置：

RIP	选中 **Enable** 可启用 RIP。设备将可以使用 RIP 来路由流量。
RIP Send Packet Version	选择 RIP 发送数据包版本 （**RIPv1** 或 **RIPv2**）。 用于向网络中其他路由器发送路由更新的 RIP 的版本会取决于其他路由器的配置设置。 RIPv2 向后兼容 RIPv1。
RIP Recv Packet Version	选择 RIP 接收数据包版本。

步骤 3 单击 **Save**。

配置 VLAN 间路由

要允许一个 VLAN 的终端站与另一个 VLAN 的终端站通信，请选中 **Inter VLAN Routing Enable** 复选框。

配置静态路由

您可以配置静态路由，以将数据包定向到目标网络。静态路由是数据包为到达特定主机或网络而必须经过的预定路径。

一些 ISP 会要求使用静态路由而非动态路由协议来构建您的路由表。静态路由与对等路由器交换路由信息时，不占用 CPU 资源。

您也可以使用静态路由来访问不支持动态路由协议的对等路由器。静态路由可同动态路由一起使用。本设备最多可支持 30 个静态路由。

请注意，不要在您的网络中引入路由环路。

配置静态路由的步骤：

步骤 1 选择 **Networking** > **Routing**。

步骤 2 从 **Route Entries** 下拉菜单中选择路由条目。

要删除路由条目，请单击 **Delete This Entry**。

步骤 3 为所选路由条目配置以下设置：

Enter Route Name	输入路由的名称。
Destination LAN IP	输入目标 LAN 的 IP 地址。
Subnet Mask	输入目标网络的子网掩码。
Gateway	输入用于此路由的网关的 IP 地址。
Interface	选择此路由将数据包发送到的接口： • **LAN & Wireless** - 单击此按钮可将数据包定向到 LAN 和无线网络。 • **Internet (WAN)** - 单击此按钮可将数据包定向到互联网 (WAN)。

步骤 4 单击 **Save**。

查看路由表

路由表包含有关其直接关联网络的拓扑的信息。

要查看网络上的路由信息，请选择 **Networking** > **Routing Table** 并选择以下选项之一：

- **Show IPv4 Routing Table** - 路由表显示时包含在 **Networking** > **Routing** 页面上配置的字段。
- **Show IPv6 Routing Table** - 路由表显示时包含在 **Networking** > **IPv6** 页面上配置的字段。

配置动态 DNS

动态 DNS (DDNS) 是一种互联网服务，可支持使用互联网域名来定位具有不同公共 IP 地址的路由器。要使用 DDNS，必须通过 DDNS 提供商 （如 DynDNS.com、TZO.com、 3322.org 或 noip.com）设置帐户。

路由器将 WAN IP 地址的变化通知给动态 DNS 服务器，从而可以使用域名访问网络上的任何公共服务。

配置 DDNS 的步骤：

步骤 1 选择 **Networking** > **Dynamic DNS**。

步骤 2 从下拉菜单中选择 **Update Interval**。

步骤 3 **DDNS Service Table** 部分列出可在设备上启用的 DDNS 服务。

步骤 4 选中要启用的服务的复选框，然后单击 **Edit**。

步骤 5 选中服务的 **Enable** 复选框。

步骤 6 配置以下信息：

Username/E-mail Address	DDNS 帐户的用户名或用于创建 DDNS 帐户的电子邮件地址。
Password	DDNS 帐户的密码。
Host / Domain Name	DDNS 服务器的主机名或用于访问网络的域的名称
Internet IP Address	（只读）设备的互联网 IP 地址。
Status	（只读）指示 DDNS 更新已成功完成或发送到 DDNS 服务器的帐户更新信息失败。

步骤 7 单击 **Test Configuration** 以测试 DDNS 配置。

步骤 8 单击 **Save**。

配置 IP 模式

针对 IPv4 和 IPv6 网络，可以配置广域网配置属性。您可以在这些页面中输入有关互联网连接类型的信息以及其他参数。

选择 IP 模式的步骤：

步骤 1 选择 **Networking** > **IP Mode**。

步骤 2 从 **IP Mode** 下拉菜单中选择以下选项之一：

LAN:IPv4, WAN:IPv4	用于在 LAN 和 WAN 端口上使用 IPv4。
LAN:IPv6, WAN:IPv4	用于在 LAN 端口上使用 IPv6，并在 WAN 端口上使用 IPv4。
LAN:IPv6, WAN:IPv6	用于在 LAN 和 WAN 端口上使用 IPv6。
LAN:IPv4+IPv6, WAN:IPv4	用于在 LAN 端口上使用 IPv4 和 IPv6，在 WAN 端口上使用 IPv4。
LAN:IPv4+IPV6, WAN:IPv4+IPv6	用于在 LAN 和 WAN 端口上使用 IPv4 和 IPv6。
LAN:IPv4, WAN:IPv6	用于在 LAN 端口上使用 IPv4，在 WAN 端口上使用 IPv6。

步骤 3 （可选）如果使用了 6to4 隧道 （可支持在 IPv4 网络上传输 IPv6 数据包），请执行以下操作：

a. 单击 **Show Static 6to4 DNS Entry**。

b. 在 **Domain** 和 **IP** 字段中，输入最多五个域到 IP 的映射。

当站点或最终用户要使用现有 IPv4 网络连接至 IPv6 互联网时，通常会使用 6to4 隧道功能。

步骤 4 单击 **Save**。

配置 IPv6

互联网协议版本 6 (IPv6) 是用于接替互联网协议版本 4 (IPv4) 的互联网协议 (IP) 版本。请根据您所拥有的互联网连接类型来配置 IPv6 网络的 WAN 属性。

配置 IPV6 WAN 连接

您可以对配置进行配置，使其作为此 WAN 的 ISP 的 DHCPv6 客户端或使用 ISP 提供的静态 IPv6 地址。

要在设备上配置 IPv6 WAN 设置，必须先将 IP 模式设置为以下模式之一：

- LAN:IPv6, WAN:IPv6
- LAN:IPv4+IPv6, WAN:IPv4
- LAN:IPv4+IPv6, WAN:IPv4+IPv6

有关如何设置 IP 模式的说明，请参阅配置 **IP** 模式。

配置 **SLAAC**

请将设备配置为使用无状态地址自动配置 (SLAAC) 进行 IPv6 客户端地址分配。

使用 SLAAC 的步骤：

步骤 **1** 选择 **Networking** > **IPv6** > **IPv6 WAN Configuration**。

步骤 **2** 在 **WAN Connection Type** 字段中，选择 SLAAC。对于无状态 DHCP， ISP 无需提供 DHCPv6 服务器。取而代之的是，源自设备的 ICMPv6 发现消息将被用于执行自动配置。

步骤 **3** 单击 **Save**。

配置 **DHCPv6**

如果 ISP 为您提供动态分配的地址，请将设备配置为 DHCPv6 客户端。

将设备配置为 DHCPv6 客户端的步骤：

步骤 **1** 选择 **Networking** > **IPv6** > **IPv6 WAN Configuration**。

步骤 **2** 在 **WAN Connection Type** 字段中，选择 **Automatic Configuration-DHCPv6**。网关连接至 ISP 的 DHCPv6 服务器以获取租用地址。

步骤 3 要自动将前缀分配给设备 （DHCP 客户端），请选择 **Prefix Delegation Enable** 单选按钮。

步骤 4 单击 **Save**。

配置静态 IPv6 WAN 地址

如果 ISP 为您分配固定地址用于访问 WAN，请将设备配置为使用静态 IPv6 地址。

配置静态 IPv6 WAN 地址的步骤：

步骤 1 选择 **Networking** > **IPv6** > **IPv6 WAN Configuration**。

步骤 2 在 **WAN Connection Type** 菜单，选择 **Static IPv6**。

步骤 3 输入以下信息：

IPv6 Address	WAN 端口的 IPv6 地址。
IPv6 Prefix Length	IPv6 前缀长度 （通常由 ISP 定义）。 IPv6 网络 （子网）由地址的初始位 （称为前缀）标识。子网中的所有主机都具有相同前缀。 例如，在 IPv6 地址 `2001:0DB8:AC10:FE01::` 中，前缀为 `2001`。
Default IPv6 Gateway	默认网关的 IPv6 地址。此地址通常是 ISP 端服务器的 IP 地址。
Static DNS 1	主 IPv6 DNS 服务器的 IP 地址。
Static DNS 2	辅助 IPv6 DNS 服务器的 IP 地址。

步骤 4 单击 **Save**。

配置 PPPoE IPv6 设置

您可以分别或同时运行 IPv4 PPPoE、 IPv6 PPPoE。如果同时运行，则 IPv6 WAN PPPoE 设置必须与 IPv4 WAN PPPoE 设置匹配。如果不匹配，则会显示一条消息，询问您是否要将 IPv6 协议设置为与 IPv4 协议匹配。请参阅配置 **PPPoE**。

配置 PPPoE IPv6 设置的步骤：

步骤 1 选择 **Networking** > **IPv6** > **IPv6 WAN Configuration**。

步骤 2 在 **WAN Connection Type** 字段中，选择 **PPPoE IPv6**。

步骤 3 输入以下信息 （可能需要联系 ISP 以获取 PPPoE 登录信息）：

Username	ISP 分配给您的用户名。
Password	ISP 分配给您的密码。
Connect on Demand	如果 ISP 根据您连接的时长收费，请选择此单选按钮。如果选择，仅当存在流量时，互联网连接才处于活动状态。如果连接处于空闲状态 （即没有流量），则关闭连接。在 **Max Idle Time** 字段中，输入从在链路上检测不到流量到关闭链路所需经过的分钟数。
Keep Alive	通过端口发送 “ 保持活动 ” 消息，使 WAN 链路保持连接。在 redial period 字段中，输入设备在断开连接后尝试重新连接之前等待的秒数。
Authentication Type	鉴权类型： **Auto-negotiation** - 服务器发送指明其安全算法设置的配置请求。设备使用鉴权凭证进行回复，其中包含服务器所发送的安全类型。 **PAP** - 使用密码鉴别协议 (PAP) 连接至 ISP。 **CHAP** - 使用询问握手鉴权协议 (PAP) 连接至 ISP。 **MS-CHAP** 或 **MS-CHAPv2** - 使用 Microsoft 询问握手鉴权协议连接至 ISP。
Service Name	登录 PPPoE 服务器时， ISP 可能要求提供的名称。
MTU	最大传输单位是可在网络中发送的最大数据包的大小。 除非 ISP 要求更改，否则建议选择 **Auto**。以太网网络的标准 MTU 值为 1500 字节。对于 PPPoE 连接，该值为 1492 字节。如果 ISP 要求自定义 MTU 设置，请选择 **Manual**。
Size	MTU 大小。如果 ISP 要求自定义 MTU 设置，请输入 MTU 大小。

Address Mode	动态或静态地址模式。如果选择静态模式，请在下一个字段中输入 IPv6 地址。
IPv6 Prefix Length	IPv6 前缀长度。
Default IPv6 Gateway	默认 IPv6 网关的 IP 地址。
Static DNS 1	主 DNS 服务器的 IP 地址。
Static DNS 2	辅助 DNS 服务器的 IP 地址。

步骤 **4** 单击 **Save**。

配置 IPv6 LAN 连接

在 IPv6 模式下， LAN DHCP 服务器默认情况下为启用状态 （与 IPv4 模式类似）。DHCPv6 服务器分配来自配置的地址池中的 IPv6 地址，这些地址使用分配给 LAN 的 IPv6 前缀长度。

要在设备上配置 IPv6 LAN 设置，必须先将 IP 模式设置为以下模式之一：

- LAN:IPv6, WAN:IPv4
- LAN:IPv6, WAN:IPv6
- LAN:IPv4+IPv6, WAN:IPv4
- LAN:IPv4+IPv6, WAN:IPv4+IPv6

有关如何设置 IP 模式的详情，请参阅配置 **IP** 模式。

配置 IPv6 LAN 设置的步骤：

步骤 **1** 选择 **Networking** > **IPv6** > **IPv6 LAN Configuration**。

步骤 **2** 输入以下信息以配置 IPv6 LAN 地址：

IPv6 Address	输入设备的 IPv6 地址。 网关的默认 IPv6 地址为 fec0::1 （或 FEC0:0000:0000:0000:0000:0000:0000:0001）。可以基于网络要求更改此 128 位 IPv6 地址。
IPv6 Prefix Length	输入 IPv6 前缀长度。 IPv6 网络 （子网）由地址的初始位 （称为前缀）标识。默认情况下，前缀长度为 64 位。 对于 IPv6 地址，网络中的所有主机都具有相同的初始位；在此字段中输入网络地址中公共初始位的位数。

步骤 3 单击 **Save** 或继续配置 IPv6 DHCP LAN 设置。

步骤 4 输入以下信息以配置 DHCPv6 设置：

DHCP Status	选中可启用 DHCPv6 服务器。 启用时，设备分配指定范围内的 IP 地址，并向请求 DHCP 地址的任何 LAN 端点提供其他信息。
Domain Name	（可选） DHCPv6 服务器的域名。
Server Preference	此 DHCP 服务器的服务器偏好级别。发送到 LAN 主机的具有最高服务器偏好值的 DHCP 通告消息优先于其他 DHCP 服务器通告消息。 默认值为 255。
Static DNS 1	ISP IPv6 网络上主 DNS 服务器的 IPv6 地址。
Static DNS 2	ISP IPv6 网络上辅助 DNS 服务器的 IPv6 地址。
Client Lease Time	向 LAN 上的端点租用 IPv6 的客户端租用持续时间（以秒为单位）。

步骤 5 选择 **Networking** > **IPv6** > **IPv6 LAN Configuration**。

步骤 6 在 **IPv6 Address Pools Table** 中，单击 **Add Row**。

步骤 7 输入以下信息：

Start Address	池的起始 IPv6 地址。
End Address	池的结束 IPv6 地址。
IPv6 Prefix Length	确定网络地址中公共初始位的位数的前缀长度。

步骤 8 单击 **Save**。

要编辑池的设置，请选择池并单击 **Edit**。要删除所选池，请单击 **Delete**。单击 **Save** 应用更改。

配置 IPv6 静态路由

可以配置静态路由以将数据包定向到目标网络。静态路由是数据包为到达特定主机或网络而必须经过的预定路径。

一些 ISP 需要静态路由而非使用动态路由协议来构建您的路由表。静态路由与对等路由器交换路由信息时，不占用 CPU 资源。

您也可以使用静态路由来访问不支持动态路由协议的对等路由器。静态路由可同动态路由一起使用。请注意，不要在您的网络中引入路由环路。

创建静态路由的步骤：

步骤 1 选择 **Networking** > **IPv6** > **IPv6 Static Routing**。

步骤 2 在静态路由列表中，单击 **Add Row**。

步骤 3 输入以下信息：

Name	路由名称。
Destination	此路由的目标主机或网络的 IPv6 地址。
Prefix Length	IPv6 地址中定义目标子网的前缀位的位数。
Gateway	用于访问目标主机或网络网关的 IPv6 地址。

Interface	路由的接口：**LAN**、 **WAN** 或 **6to4**。
Metric	路由的优先级。选择介于 2 与 15 之间的值。如果存在指向相同目标的多个路由，则使用具有最低度量标准的路由。
Active	选中可使路由处于活动状态。添加非活动状态路由时，该路由会在路由表中列出，但是不被设备使用。 如果添加路由时路由不可用，则输入非活动路由十分有用。当网络变为可用时，您可以启用路由。

步骤 4 单击 **Save**。

要编辑路由的设置，请选择路由并单击 **Edit**。要删除所选路由，请单击 **Delete**。单击 **Save** 应用更改。

配置路由 (RIPng)

下一代 RIP (RIPng) 是基于距离矢量 (D-V) 算法的路由协议。RIPng 使用 UDP 数据包，通过端口 521 交换路由信息。

RIPng 使用步跳数测量与目标之间的距离。步跳数称为度量标准 （或成本）。从路由器到直接连接网络的步跳数为 0。两个直接连接路由器之间的步跳数为 1。当步跳数大于或等于 16 时，不可抵达目标网络或主机。

默认情况下，每 30 秒发送一次路由更新。如果路由器在 180 秒后还未从相邻路由器收到任何路由更新，则会将从相邻路由器获知的路由视为不可达。再经过 240 秒之后，如果还未收到任何路由更新，则路由器将从路由表中移除这些路由。

在设备上， RIPng 在默认情况下为禁用状态。

配置 RIPng 的步骤：

步骤 1 选择 **Networking** > **IPv6** > **Routing (RIPng)**）。

步骤 2 选中 **Enable**。

步骤 3 单击 **Save**。

配置隧道

通过 IPv6 到 IPv4 隧道 （6-to-4 隧道）可以在 IPv4 网络上传输 IPv6 数据包。通过 IPv4 到 IPv6 隧道 （4-to-6 隧道）可以在 IPv6 网络上传输 IPv4 数据包。

6-to-4 隧道

6 当站点或最终用户要使用现有 IPv4 网络连接至 IPv6 互联网时，通常会使用 6-to-4 隧道。

配置 6-to-4 隧道的步骤：

步骤 1 选择 **Networking** > **IPv6** > **Tunneling**。

步骤 2 在 **6 to 4 Tunneling** 字段中，选中 **Enable**。

步骤 3 选择隧道类型：

- **6to4**
- **6RD** （快速部署）
- **ISATAP** （站内自动隧道寻址协议） - 选择 **Auto** 或 **Manual**。

步骤 4 对于 6RD 隧道，选择 **Auto** 或 **Manual**。如果选择 **Manual**，请输入以下信息：

- **IPv6 Prefix**
- **IPv6 Prefix Length**
- **Border Relay**
- **IPv4 Mask Length**

步骤 5 对于 ISATAP 隧道，选择 **Auto** 或 **Manual**。如果选择 **Manual**，请输入以下信息：

- **IPv6 Prefix**
- **IPv6 Prefix Length**

步骤 6 单击 **Save**。

4-to-6 隧道

配置 4-to-6 隧道的步骤：

步骤 1 选择 **Networking** > **IPv6** > **Tunneling**。

步骤 2 在 **4 to 6 Tunneling** 字段中，选中 **Enable** 框。

步骤 3 输入设备的本地 WAN IPv6 地址。

步骤 4 输入远程 IPv6 地址，或远程端点的 IP 地址。

步骤 5 单击 **Save**。

查看 IPv6 隧道状态

查看 IPv6 隧道状态的步骤：

步骤 1 选择 **Networking** > **IPv6** > **IPv6 Tunnels Status**。

步骤 2 单击 **Refresh** 可更新最新信息。

此页面显示有关通过专用 WAN 接口设置的自动隧道的信息。该表显示在设备上创建的隧道名称和 IPv6 地址。

配置路由器通告

设备上的路由器通告常驻程序 (RADVD) 会侦听 IPv6 LAN 上的路由器请求，并根据需要使用路由器通告进行回复。这属于无状态 IPv6 自动配置，设备将 IPv6 前缀分发给网络上的所有节点

配置 RADVD 的步骤：

步骤 1 选择 **Networking** > **IPv6** > **Router Advertisement**。

步骤 2 输入以下信息：

RADVD Status	选中 **Enable** 可启用 RADVD。
Advertise Mode	选择以下模式之一： **Unsolicited Multicast** - 将路由器通告 (RA) 发送至属于组播组的所有接口。 **Unicast only** - 将通告仅限为已知 IPv6 地址 （RA 仅发送至属于已知地址的接口）。
Advertise Interval	**Unsolicited Multicast** 的通告间隔 (4–1800)。默认值为 30。通告间隔为介于最短路由器通告间隔 (MinRtrAdvInterval) 与最长路由器通告间隔 (MaxRtrAdvInterval) 之间的随机值。 MinRtrAdvInterval = 0.33 * MaxRtrAdvInterval
RA Flags	选中 **Managed** 可将管理 / 有状态协议用于地址自动配置。 选中 **Other** 可将管理 / 有状态协议用于其他的非地址自动配置。

Router Preference	从下拉菜单中选择 **low**、**medium** 或 **high**。默认值为 medium。 路由器偏好为默认路由器提供偏好度量标准。 low、medium 和 high 值在 RA 消息中的未使用位中形成信号。此扩展对于路由器 （设置路由器偏好值）和主机（解释路由器偏好版本）可向后兼容。对于未实施路由器偏好的主机，可以忽略这些值。如果 LAN 上存在其他支持 RADVD 的设备，则此功能将十分有用。
MTU	MTU 大小 （0 或 1280 到 1500）。默认值为 1500 字节。 最大传输单位 (MTU) 是可在网络中发送的最大数据包的大小。 MTU 在 RA 中用于确保在 LAN MTU 未众所周知时网络上的所有节点都使用相同的 MTU 值。
Router Life Time	路由器有效寿命或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 **3** 单击 **Save**。

配置通告前缀

配置 RADVD 可用前缀的步骤：

步骤 **1** 选择 **Networking** > **IPv6** > **Advertisement Prefixes**。

步骤 **2** 单击 **Add Row**。

步骤 3 输入以下信息：

IPv6 Prefix Type	选择以下类型之一： **6to4** - 可用于在 IPv4 网络上传输 IPv6 数据包。当最终用户要使用现有 IPv4 连接来连接至 IPv6 互联网时，该会类型十分有用。 **Global/Local** - 可以在专用 IPv6 网络中使用的本地唯一的 IPv6 地址，或全局唯一的 IPv6 互联网地址。
SLA ID	如果选择 **6to4** 作为 IPv6 前缀类型，请输入站点级别聚合标识符 (SLA ID)。 6to4 地址前缀中的 SLA ID 设置为用于发送通告的接口 ID。
IPv6 Prefix	如果选择 **Global/Local** 作为 IPv6 前缀类型，请输入 IPv6 前缀。 IPv6 前缀指定 IPv6 网络地址。
IPv6 Prefix Length	如果选择 **Global/Local** 作为 IPv6 前缀类型，请输入前缀长度。前缀长度变量是一个十进制值，指示组成地址网络部分的地址连续高位的位数。
Prefix Lifetime	前缀有效期限，或允许请求路由器使用前缀的时间长度。

步骤 4 单击 **Save**。

4

配置无线网络

本章介绍如何在设备上配置无线网络。

无线安全性

无线网络使用方便、易于安装。因为无线网络的工作方式是通过无线电波发送信息，所以和传统有线网络相比更容易遭受入侵程序的危害。

无线安全性提示

虽然无法在物理上阻止某人连接至您的无线网络，但是可以采取以下措施来保证网络安全：

- 更改默认无线网络名称或 SSID。

  无线设备有默认的无线网络名称或 SSID。这是无线网络的名称，长度最多为 32 个字符。

要保护您的网络，请将默认无线网络名称更改为唯一名称以将您的无线网络与您周围可能存在的其他无线网络区分开来。

更改名称时，请勿使用个人信息，因为任何人在浏览无线网络时都可查看此信息。

- 更改默认密码。

  对于无线产品 （如接入点、路由器和网关），在您更改其设置时会要求输入密码。这些设备有一个默认密码。默认密码通常为 **cisco**。

  黑客知道这些默认值，就可能尝试利用它们访问您的无线设备并更改网络设置。要阻止未授权访问，请自定义设备密码，以便难以猜到。

- 启用 MAC 地址过滤。

  使用思科路由器和网关时可以启用 MAC 地址过滤。 MAC 地址是分配给每个联网设备的唯一的数字和字母序列。

  启用 MAC 地址过滤之后，只有特定 MAC 地址的无线设备才能访问无线网络。例如，可以指定网络中每个计算机的 MAC 地址，以便只有这些计算机才能访问您的无线网络。

- 启用加密。

  加密可保护在无线网络中传输的数据。 Wi-Fi 保护访问 (WPA/WPA2) 和有线等效加密 (WEP) 可为无线通信提供不同级别的安全性。当前，经过 Wi-Fi 认证的设备需要支持 WPA2，但是无需支持 WEP。

  使用 WPA/WPA2 加密的网络比使用 WEP 加密的网络更加安全，因为 WPA/WPA2 使用动态密钥加密。

  要在信息通过电波传输时被保护，请启用网络设备支持的最高级别加密。

  WEP 是一种比较老的加密标准，可能是一些不支持 WPA 的较旧设备上的唯一选项。

- 使无线路由器、接入点或网关远离外墙和窗户。
- 不使用无线路由器、接入点或网关时 （夜间、休假期间），请将它们关闭。
- 使用长度不少于八个字符的安全性较强的密码。混合使用字母和数字，避免使用可在字典中找到的标准单词。

一般网络与安全性准则

如果基础网络不安全，则无线网络再安全也无济于事。建议采取以下预防措施：

- 对网络上的所有计算机进行密码保护，并单独对敏感文件进行密码保护。
- 定期更改密码。
- 安装防病毒软件和个人防火墙软件。
- 禁用文件共享 （对等）以防应用程序在未经您同意的情况下使用文件共享。

设备上的无线网络

设备可提供四个虚拟无线网络或四个 SSID （服务集标识符）：ciscosb1、 ciscosb2、ciscosb3 和 ciscosb4。这些是这些网络的默认名称或 SSID，不过可以将这些名称更改为更有意义的名称。下表介绍这些网络的默认设置：

SSID 名称	ciscosb1	ciscosb2	ciscosb3	ciscosb4
Enabled	是	否	否	否
SSID Broadcast	已启用	已禁用	已禁用	已禁用
Security Mode	已禁用[1]	已禁用	已禁用	已禁用
MAC Filter	已禁用	已禁用	已禁用	已禁用
VLAN	1	1	1	1
Wireless Isolation with SSID	已禁用	已禁用	已禁用	已禁用
WMM	已启用	已启用	已启用	已启用
WPS Hardware Button	已启用	已禁用	已禁用	已禁用

1. 使用设置向导时，选择 Best Security 或 Better Security 可防止对设备进行未授权访问。

配置基本无线设置

选择 **Wireless** > **Basic Settings** 可配置基本无线设置。

配置基本无线设置的步骤：

步骤 1 选择 **Wireless** > **Basic Settings**。

步骤 2 在 **Radio** 字段中，选中 **Enable** 框以打开无线功能。默认情况下仅启用 **ciscosb1** 这一个无线网络。

步骤 3 在 **Wireless Network Mode** 字段中，从下拉菜单中选择以下选项之一：

B/G/N-Mixed	如果网络中有 Wireless-N、 Wireless-B 和 Wireless-G 设备。这是默认设置 （推荐）。
B Only	如果网络中只有 Wireless-B 设备，请选择此选项。
G Only	如果网络中只有 Wireless-G 设备，请选择此选项。
N Only	如果网络中只有 Wireless-N 设备，请选择此选项。
B/G-Mixed	如果网络中有 Wireless-B 和 Wireless-G 设备，请选择此选项。
G/N-Mixed	如果网络中有 Wireless-G 和 Wireless-N 设备，请选择此选项。

步骤 4 如果在 **Wireless Band Selection** 字段中选择了 **B/G/N-Mixed**、 **N-Only** 或 **G/N Mixed**，请选择网络中的无线带宽 （**20MHz** 或 **20/40MHz**）。如果选择 N-Only，则必须在网络中应用 WPA2 安全性。请参阅配置安全模式。

步骤 5 在 **Wireless Channel** 字段中，从下拉菜单中选择无线信道。

步骤 6 在 **AP Management VLAN** 字段中，如果使用默认设置，请选择 **VLAN 1**。

如果创建其他 VLAN，请选择与在网络中其他交换机上配置的 VLAN 对应的值。这样做是为了安全起见。可能需要更改管理 VLAN 以限制对设备管理器的访问。

步骤 7 （可选）在 **U-APSD (WMM Power Save)** 字段中，选择 **Enable** 以启用计划外自动节能 (U-APSD) 功能 （也称为 WMM 节能），无线功能可使用该功能节省电能。

U-APSD 是针对实时应用 （如 VoIP、在 WLAN 上传输全双工数据）而优化的节能方案。通过将传出 IP 流量分类为*语音*数据，这些类型的应用可以将电池使用寿命延长约 25% 并最大程度减小传输延迟。

步骤 8 （可选）配置四个无线网络的设置 （请参阅编辑无线网络设置）。

步骤 9 单击 **Save**。

编辑无线网络设置

Basic Settings 页面上的 **Wireless Table** 会列出设备上支持的四个无线网络的设置。

配置无线网络设置的步骤：

步骤 **1** 选中要配置的网络的对应框。

步骤 **2** 单击 **Edit**。

步骤 **3** 配置以下设置：

Enable SSID	单击 **On** 可启用该网络。
SSID Name	输入网络的名称。
SSID Broadcast	选中此框可启用 SSID 广播。如果启用了 SSID 广播，则无线路由器会将其可用性通告给路由器范围内配有无线功能的设备。
Security Mode	请参阅配置安全模式。
MAC Filter	请参阅配置 **MAC** 过滤。
VLAN	选择与网络关联的 VLAN。
Wireless Isolation with SSID	选中此框可启用 SSID 中的无线隔离。
WMM (Wi-Fi Multimedia)	选中此框可启用 WMM。
Max Associated Clients	可以连接至所选无线网络的最大客户端数。输入介于 1 与 64 之间的数字。
WPS	选中此框可将设备前面板上的 WPS 按钮映射到此网络。
Portal Profile	请参阅配置强制网络门户。

步骤 **4** 单击 **Save**。

配置安全模式

可以为无线网络配置以下安全模式之一：

- 配置 **WEP**
- 配置 **WPA-Personal**、 **WPA2-Personal** 和 **WPA2-Personal Mixed**
- 配置 **WPA-Enterprise**、 **WPA2-Enterprise** 和 **WPA2-Enterprise Mixed**

配置 **WEP**

WEP 安全模式的安全性较弱，使用的是基本的加密方式，没有 WPA 安全。当网络设备不支持 WPA 时，需要使用 WEP。

NOTE如果不必使用 WEP，我们建议您使用 WPA2。如果正在使用的只有 Wireless-N 模式，则必须使用 WPA2。

配置 WEP 安全模式的步骤：

步骤 **1** 选择 **Wireless** > **Basic Settings**。在 **Wireless Table** 中，选中要配置的网络的对应框。

步骤 **2** 单击 **Edit Security Mode**。系统将显示 **Security Settings** 页面。

步骤 **3** 在 **Select SSID** 字段中，选择要为其配置安全设置的 SSID。

步骤 **4** 在 **Security Mode** 菜单中，选择 **WEP**。

步骤 **5** 在 **Authentication Type** 字段中，选择以下选项之一：

- **Open System** - 这是默认选项。
- **Shared Key** - 如果网络管理员建议使用此设置，请选择此选项。如果您不确定，请选择默认选项。

在这两种情况下，无线客户端都必须提供正确的共享密钥 （密码）才能访问无线网络。

步骤 **6** 在 **Encryption** 字段中，选择加密类型：

- **10/64-bit(10 hex digits) -** 提供 40 位密钥。
- **26/128-bit(26 hex digits)** - 提供 104 位密钥，可实现更强的加密，使密钥更难解密。建议使用 128 位加密。

步骤 **7** （可选）在 **Passphrase** 字段中，输入字母数字短语 （长于八个字符，以实现最佳安全性），然后单击 **Generate Key** 以在 **WEP Key** 字段中生成四个唯一的 WEP 密钥。

如果要提供自己的密钥，请直接在 **Key 1** 字段中输入 （推荐）。密钥长度对于 64 位 WEP 应为 5 个 ASCII 字符 （或 10 个十六进制字符），对于 128 位 WEP 应为 13 个 ASCII 字符 （或 26 个十六进制字符）。有效的十六进制字符为 0 到 9 和 A 到 F。

步骤 8 在 **TX Key** 字段中，选择将哪个密钥用作设备访问无线网络时必须使用的共享密钥。

步骤 9 单击 **Save** 保存设置。

步骤 10 单击 **Back** 返回 **Basic Settings** 页面。

配置 WPA-Personal、 WPA2-Personal 和 WPA2-Personal Mixed

WPA Personal、 WPA2 Personal 和 WPA2 Personal Mixed 安全模式可提供可替代 WEP 的强安全性。

- **WPA-Personal** - WPA 属于由 Wi-Fi 联盟标准化的无线安全标准 (802.11i) 的一部分，用于在准备 802.11i 标准期间代替 WEP。 WPA-Personal 支持临时密钥完整性协议 (TKIP) 和高级加密标准 (AES) 加密。
- **WPA2-Personal** -（推荐） WPA2 是在最终 802.11i 标准中指定的实施的安全标准。 WPA2 支持 AES 加密，此选项使用预先共享密钥 (PSK) 进行鉴权。
- **WPA2-Personal Mixed** - 允许 WPA 和 WPA2 客户端同时使用 PSK 鉴权进行连接。

个人鉴权是 PSK，这是与无线对等方共享的字母数字密码短语。

配置 WPA Personal 安全模式的步骤：

步骤 1 在 **Wireless Table** (**Wireless** > **Basic Settings**) 中，选中要配置的网络的对应框。

步骤 2 单击 **Edit Security Mode**。系统将显示 **Security Settings** 页面。

步骤 3 在 **Select SSID** 字段中，选择要为其配置安全设置的 SSID。

步骤 4 在 **Security Mode** 菜单中，选择三个 WPA Personal 选项之一。

步骤 5 （仅限 WPA-Personal）在 **Encryption** 字段中，选择以下选项之一：

- **TKIP/AES** - 选择 **TKIP/AES** 可确保与可能不支持 AES 的较旧无线设备兼容。
- **AES** - 此选项更安全。

步骤 6 在 **Security Key** 字段中，输入字母数字短语 （8–63 个 ASCII 字符或 64 个十六进制数字）。密码强度计显示密钥的安全程度：below minimum、 weak、 strong、 very strong 或 secure。建议使用强度计指示为安全的安全密钥。

步骤 7 要在输入时显示安全密钥，请选中 **Unmask Password** 框。

步骤 8 在 **Key Renewal** 字段中，输入密钥更新之间的持续时间 （600–7200 秒）。默认值为 3600。

步骤 9 单击 **Save** 保存设置。单击 **Back** 返回 **Basic Settings** 页面。

配置 WPA-Enterprise、 WPA2-Enterprise 和 WPA2-Enterprise Mixed

WPA Enterprise、 WPA2 Enterprise 和 WPA2 Enterprise Mixed 安全模式允许使用 RADUIS 服务器鉴权。

- **WPA-Enterprise** - 允许将 WPA 与 RADIUS 服务器鉴权一起使用。
- **WPA2-Enterprise** - 允许将 WPA2 与 RADIUS 服务器鉴权一起使用。
- **WPA2-Enterprise Mixed** - 允许 WPA 和 WPA2 客户端同时使用 RADIUS 鉴权进行连接。

配置 WPA Enterprise 安全模式的步骤：

步骤 1 在 **Wireless Table** (**Wireless** > **Basic Settings**) 中，选中要配置的网络的对应框。

步骤 2 单击 **Edit Security Mode**。

步骤 3 在 **Select SSID** 字段中，选择要为其配置安全设置的 SSID。

步骤 4 在 **Security Mode** 菜单中，选择三个 WPA Enterprise 选项之一。

步骤 5 （仅限 WPA-Enterprise）在 **Encryption** 字段中，选择以下选项之一：

- **TKIP/AES** - 选择 **TKIP/AES** 可确保与可能不支持 AES 的较旧无线设备兼容。
- **AES** - 此选项更安全。

步骤 6 在 **RADIUS Server** 字段中，输入 RADIUS 服务器的 IP 地址。

步骤 7 在 **RADIUS Port** 字段中，输入用于访问 RADIUS 服务器的端口。

步骤 8 在 **Shared Key** 字段中，输入字母数字短语。

步骤 9 在 **Key Renewal** 字段中，输入密钥更新之间的持续时间 （600–7200 秒）。默认值为 3600。

步骤 10 单击 **Save** 保存设置。

步骤 11 单击 **Back** 返回 **Basic Settings** 页面。

配置 MAC 过滤

可以使用 MAC 过滤，根据请求设备的 MAC （硬件）地址来允许或拒绝访问无线网络。例如，可以输入一组计算机的 MAC 地址，仅允许这些计算机访问网络。可以为每个网络或 SSID 配置 MAC 过滤。

配置 MAC 过滤的步骤：

步骤 1 在 **Wireless Table** (**Wireless** > **Basic Settings**) 中，选中要配置的网络的对应框。

步骤 2 单击 **Edit MAC Filtering**。系统将显示 **Wireless MAC Filter** 页面。

步骤 3 在 **Edit MAC Filtering** 字段中，选中 **Enable** 框为此 SSID 启用 MAC 过滤。

步骤 4 在 **Connection Control** 字段中，选择对无线网络的访问类型：

- **Prevent** - 选择此选项可阻止具有 **MAC Address Table** 中列出的 MAC 地址的设备访问无线网络。此选项为默认选项。
- **Permit** - 选择此选项可允许具有 **MAC Address Table** 中列出的 MAC 地址的设备访问无线网络。

步骤 5 要显示无线网络中的计算机和其他设备，请单击 **Show Client List**。

步骤 6 在 **Save to MAC Address Filter List** 字段中，选中对应框以将设备添加到将被添加到 **MAC Address Table** 的设备的列表中。

步骤 7 单击 **Add to MAC** 以将 **Client List Table** 中所选设备添加到 **MAC Address Table**。

步骤 8 单击 **Save** 保存设置。

步骤 9 单击 **Back** 返回 **Basic Settings** 页面。

配置每天固定时间访问

要进一步保护您的网络，可以通过指定用户访问网络的时间来限制对网络的访问。

配置每天固定时间访问的步骤：

步骤 1 在 **Wireless Table** (**Wireless** > **Basic Settings**) 中，选中要配置的网络的对应框。

步骤 2 单击 **Time of Day Access**。系统将显示 **Time of Day Access** 页面。

步骤 3 在 **Active Time** 字段中，选中 **Enable** 启用每天固定时间访问。

步骤 4 在 **Start Time** 和 **Stop Time** 字段中，指定每天允许访问网络的时间。

步骤 5 单击 **Save**。

配置高级无线设置

高级无线设置只应由经验丰富的管理员进行调整；不正确的设置可能会降低无线性能。

配置高级无线设置的步骤：

步骤 1 选择 **Wireless** > **Advanced Settings**。系统将显示 Advanced Settings 页面。

步骤 2 配置以下设置：

Frame Burst	启用此选项可为无线网络提供更高性能，具体取决于无线产品的制造商。如果不确定如何使用此选项，请保留默认值 （启用）。
WMM No Acknowledgement	启用 WMM No Acknowledgement 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。默认情况下，此设置为禁用状态。
Basic Rate	Basic Rate 设置不是传输速率，而是服务准备平台可以用于传输的一系列速率。设备会将其基本速率通告给网络中的其他无线设备，让它们知道将使用的速率。服务准备平台也会通告它将自动选择传输的最佳速率。 当设备可以按所有标准无线速率（1 Mbps、2 Mbps、5.5 Mbps、11 Mbps、18 Mbps、24 Mbps、36 Mbps、48 Mbps 和 54 Mbps）传输时，默认设置为 Default。除了 B 和 G 速度之外，设备还支持 N 速度。其他选项有 1-2 Mbps （用于较旧无线技术）和 All （设备可以按所有无线速率传输）。 Basic Rate 不是数据传输的实际速率。如果要指定设备数据传输速率，请配置 Transmission Rate 设置。

Transmission Rate	应根据无线网络速度设置数据传输速率。可以从一系列传输速度中选择，也可以选择 **Auto** 让设备自动使用可能最快的数据速率并启用自动回退功能。自动回退会在设备与无线客户端之间协商最佳可能连接速度。默认为 Auto。
N Transmission Rate	应根据 Wireless-N 网络速度设置数据传输速率。可以从一系列传输速度中选择，也可以选择 **Auto** 让设备自动使用可能最快的数据速率并启用自动回退功能。自动回退会在设备与无线客户端之间协商最佳可能连接速度。默认为 Auto。
CTS Protection Mode	当 Wireless-N 和 Wireless-G 设备遇到严重问题，在具有大量 802.11b 流量的环境中无法传输到设备时，设备自动使用 CTS （清除发送）保护模式。 此功能提升了设备捕获所有 Wireless-N 和 Wireless-G 传输的能力，但是会严重降低性能。默认为 Auto。
Beacon Interval	Beacon Interval 值指示信标的频率间隔。信标是设备为同步无线网络而广播的数据包。 输入介于 40 与 3,500 毫秒之间的值。默认值为 100。

DTIM Interval	此值（介于 1 与 255 之间）指示发送流量指示消息 (DTIM) 的间隔。 DTIM 字段是倒计时字段，用于向客户端告知下一个窗口以便侦听广播和组播消息。 当设备缓冲了关联客户端的广播或组播消息时，它会发送包含 DTIM Interval 值的下一个 DTIM。其客户端会收到信标并被唤醒，以接收广播和组播消息。默认值为 1。
Fragmentation Threshold	此值指定在数据分为多个数据包之前的最大数据包大小。如果遇到较高数据包错误率，则可以稍微增大 Fragmentation Threshold。 将 Fragmentation Threshold 设置得太低可能会导致网络性能变差。建议仅稍微减小默认值。在大多数情况下，应保留其默认值 2346。
RTS Threshold	如果遇到了不一致的数据流，请仅稍微减小一点。建议使用的默认值为 2347。 如果网络数据包小于预设的请求发送 (RTS) 阈值大小，则不会启用 RTS/ 允许发送 (CTS) 机制。服务准备平台会将 RTS 帧发送给特定接收站并协商数据帧的发送。 接收 RTS 之后，无线站使用 CTS 帧进行响应以认可开始传输的权限。

步骤 **3** 单击 **Save**。

检测恶意接入点

恶意接入点是未经系统管理员授权的、安装在安全网络上的接入点 (AP)。恶意 AP 会形成安全威胁，因为可以访问内部部署的任何人都可以安装能够在未授权的情况下访问网络的无线 AP。

使用 Rogue AP Detection 页面能够使设备显示其在网络附近检测到的所有 AP 的信息。如果被列为恶意接入点的接入点实际上是合法接入点，则可以将其添加到 **Authorized AP Table**。选择刷新速率以确保 Rogue AP Detection 页面始终显示最新信息。

启用恶意 AP 检测的步骤：

步骤 1 选择 **Wireless > Rogue AP**。

步骤 2 单击 **Rogue AP Detection On** 单选按钮。

步骤 3 单击 **Save**。

向检测到的接入点授权的步骤：

步骤 1 在 **Rogue AP Detected Table** 中，选中要授权的接入点的对应框。

步骤 2 单击 **Authorize**。

将接入点添加到 Authorized AP Table 的步骤：

步骤 1 单击 **Add Row**。

步骤 2 输入要授权的接入点的 MAC 地址。

步骤 3 输入标识无线网络的 SSID 或名称。

步骤 4 选择与接入点关联的安全模式。

步骤 5 选择 TKIP （临时密钥完整性协议）或 CCMP （计数器密码模式协议）作为与接入点关联的加密算法。

步骤 6 选择 RADIUS 服务器或 PSK （预先共享密钥）以对接入点进行鉴权。

步骤 7 选择接入点使用的无线网络模式。

步骤 8 选择接入点使用的无线电频率。

步骤 9 单击 **Save**。

导入授权 **AP** 列表

可以使用 CSV 文件导入授权接入点的列表。创建 CSV 文件时，可使用以下值作为参考。

字段	值
Security	• 0 - 打开 • 1 - WEP • 2 - WPA-Personal • 3 - WPA-Enterprise • 4 - WPA2-Personal • 5 - WPA2-Enterprise
Network Mode	• 0 - B Only • 1 - G Only • 2 - N Only • 3 - BG-Mixed • 4 - GN-Mixed • 5 - BGN-Mixed

字段	值
Channel	• 0 - Auto • 1 - 2.412 • 2 - 2.417 • 3 - 2.422 • 4 - 2.427 • 5 - 2.432 • 6 - 2.437 • 7 - 2.442 • 8 - 2.447 • 9 - 2.452 • 10 - 2.457 • 11 - 2.462
Encryption	• 2 - TKIP • 4 - CCMP
Authentication	• 2 - PSK • 1 - RADIUS

确保 CSV 文件内容的组织方式如下所示：

BSSID	Security	Encryption	Authentication	Wireless Network	Channel	SSID
00:1C:10:CE:44:48	4	2	2	3	1	Auth_Guest

导入授权 AP 列表的步骤：

步骤 1 单击 **Merge** 可将要导入的接入点列表添加到 **Authorized AP Table** 中显示的接入点中。单击 **Replace** 可将表中的 AP 替换为要导入的列表中的 AP。

步骤 2 单击 **Browse** 以查找要导入的文件。

步骤 3 单击 **Save**。

配置 WDS

无线分布式系统 (WDS) 是在网络中实现接入点无线互连的系统。通过该系统可以使用多个接入点扩展无线网络，而无需使用有线骨干网来链接它们。

要建立 WDS 链路，本设备和其他远程 WDS 对等方必须设置相同的无线网络模式、无线信道、无线频段选择和加密类型 （None 或 WEP）。

可以在网桥模式 （其中一个 AP 充当多个 AP 之间的通用链路）或中继模式 （其中一个 AP 使用无线连接重复信号来连接两个 AP，无需使用有线连接到 LAN）下配置 WDS。

WDS 仅支持一个 SSID。

在网桥模式下配置 WDS 的步骤：

步骤 1 选择 **Wireless** > **WDS**。

步骤 2 要启用 WDS，请选中 **Enable** 复选框。

步骤 3 选择 **WDS Bridge** 单选按钮。

步骤 4 在 **Remote Wireless Bridge's MAC Address** 部分中，在 **MAC 1**、 **MAC 2**、 **MAC 3** 和 **MAC 4** 字段中输入要用作网桥的最多四个接入点的 MAC 地址。

步骤 5 单击 **Save**。

在中继模式下配置 WDS 的步骤：

步骤 1 选择 **Wireless** > **WDS**。

步骤 2 选中 **WDS** 复选框。

步骤 3 选择中继模式。如果选择 **Allow wireless signal to be repeated by a repeater**，请在 **MAC 1**、 **MAC 2** 和 **MAC 3** 字段中输入用作中继的最多三个接入点的 MAC 地址。

步骤 4 如果选择 **Repeat wireless signal of a remote access point**：

- 在 **MAC** 字段中输入无线接入点的 MAC 地址。
- 单击 **Show Available Networks** 以显示 **Available Networks Table**。单击 **Connect** 以将所选接入点的 MAC 地址添加到 **MAC** 字段。

步骤 5 单击 **Save**。

配置 WPS

配置 WPS 可允许启用 WPS 的设备方便且安全地连接至无线网络。有关在客户端设备上设置 WPS 的其他说明，请参阅客户端设备文档。

配置 WPS 的步骤：

步骤 1 选择 **Wireless** > **WPS**。系统将显示 Wi-Fi Protected Setup 页面。

步骤 2 从下拉菜单中选择 SSID 选项。

步骤 3 采用以下三种方式之一在客户端设备上配置 WPS：

a. 单击或按客户端设备上的 WPS 按钮，然后单击此页面上的 WPS 图标。

b. 输入客户端的 WPS PIN 号码，然后单击 **Register**。

c. 客户端设备需要来自此路由器的 PIN 号码，使用指示的路由器 PIN 号码。

Device PIN Status - WPA 设备个人标识号 (PIN) 状态。

Device PIN - 标识尝试连接的设备的 PIN。

PIN Lifetime - 密钥的有效期限。如果有效期限到期，系统将协商新的密钥。

配置 WPS 之后，以下信息会出现在 **WPS** 页面底部：Wi-Fi Protected Setup Status、 Network Name (SSID) 和 Security。

配置强制网络门户

使用强制网络门户可提供对互联网和网络资源的受控、经鉴权访问，对安全性无任何影响。强制网络门户显示一个特殊网页，用于对客户端进行鉴权，然后客户端才能使用互联网。可以配置强制网络门户验证以便允许访客和经鉴权的网络用户访问。

通过将设备上的每个虚拟无线网络与门户简档关联，来为这些网络配置强制网络门户实例。

创建强制网络门户简档

创建强制网络门户简档的步骤：

步骤 1 选择 **Wireless > Captive Portal > Portal Profile**。在 **Portal Profile Table** 部分中，单击 **Add Row**。要修改设备上提供的门户简档，请选中 **Default_Portal_Profile** 框并单击 **Edit**。

步骤 2 输入强制网络门户简档的名称。

步骤 3 选择是否使用该简档对网络上的访客用户或用户进行鉴权。

步骤 4 要在鉴权之后将用户重定向到某个 URL，请启用 **Auto Redirect URL**，然后在 **Redirect URL** 字段中输入完全合格域名或 IP 地址。例如，在 URL 中包含 http://。

步骤 5 在 **Session Timeout** 字段中，指定设备保持打开与关联的无线客户端鉴权会话的分钟数。默认超时为 60 分钟。

步骤 6 为要在页面上显示的文本选择字体颜色。

步骤 7 指定要显示的文本，如组织名称、用户名和密码字段的标签文本以及登录按钮上的标签。

步骤 8 输入与公司关联的标准版权文本。

步骤 9 在 **Error 1** 和 **Error 2** 字段中，输入在登录失败时和超过最大连接数时要向客户端显示的错误消息。

步骤 10 要使用复选框允许用户接受使用条款之后才继续，请启用 **Agreement**。 **Agreement Text** 字段中的文本将显示为复选框的标签。

步骤 11 在 **Acceptance Use Policy** 字段中输入要显示给用户的接受条款。

步骤 12 在 **Upload Files** 部分中，选择文件以上传符合公司品牌准则的公司徽标和背景文件。保存简档。

要预览此简档，请选择 **Captive Portal > Portal Page Preview**，然后从 **Portal Profile** 下拉列表中选择简档。

配置强制网络门户实例

为设备配置强制网络门户实例的步骤：

步骤 1 选择 **Wireless > Basic Settings**。

步骤 2 在 **Wireless Table** 部分中，对要为其配置强制网络门户的 SSID 选中 **Enable** 框。单击 **Edit**。

步骤 3 为该 SSID 选择门户简档。

可以使用 SSID 为设备创建最多四个强制网络门户。要创建新门户简档，请从下拉列表中选择 **Create a new Portal Profile**。选择 Default_Portal_Profile 可使用设备上提供的门户简档。

步骤 4 选中 **Enable** 框为 SSID 启用强制网络门户。

步骤 5 保存强制网络门户实例。

创建强制网络门户用户帐户

创建强制网络门户用户帐户的步骤：

步骤 1 选择 **Wireless > Captive Portal > User Accounts**。

步骤 2 单击 **Add Row**。

步骤 3 输入用户名和密码。重新输入密码进行验证。

建议密码不包含任何语言中的字典单词，应由字母 （包含大写和小写字母）、数字和符号组成。密码长度最多为 64 个字符。

步骤 4 在 **Access Time (Minutes)** 字段中，指定鉴权会话超时之前的持续时间。

步骤 5 要从 CSV 文件导入文件名和密码，请单击 **Import**。系统将显示 **Administration > Users** 页面。在 **Import Username and Password** 部分中，单击 **Browse** 找到文件，然后单击 **Import**。有关详情，请参阅导入用户帐户。

步骤 6 保存用户帐户。

配置设备模式

可以将本设备配置为以下工作模式：

- **Router -** 用于充当无线路由器。
- **AP**（接入点）**-** 用于向客户端提供无线连接并将 Wi-Fi 功能扩展到现有有线网络。当本设备用作接入点时，所有 LAN 端口都为禁用状态。

  确保在 **Networking > WAN > WAN Configuration** 页面上配置 AP 管理 VLAN 信息。有关详情，请参阅配置可选设置。

配置设备模式的步骤：

步骤 1 选择 **Wireless > Device Mode**，然后选择设备的工作模式。

步骤 2 单击 **Save**。

5

配置防火墙

本章介绍如何配置本设备的防火墙属性。

防火墙功能

可以通过创建并应用规则，使设备有选择性地阻止和允许入站和出站互联网流量，从而保护您的网络。随后指定如何以及在哪些设备上应用这些规则。为此，必须指定以下设置：

- 路由器应允许或阻止的服务或流量类型。例如， Web 浏览、 VoIP、其他标准服务和您定义的自定义服务。
- 流量方向 （通过指定流量的源和目标）；流量方向的指定需通过指定源区域 (LAN/WAN/DMZ) 和目标区域 (LAN/WAN/DMZ) 来完成。
- 关于路由器应在何时应用规则的时间表。
- 路由器应允许或阻止的关键字 （域名中或网页的 URL 中）。
- 用于按指定时间表对指定服务允许或阻止入站和出站互联网流量的规则。
- 路由器应阻止入站访问网络的设备的 MAC 地址。

- 发信号给路由器以允许或阻止访问按端口号定义的指定服务的端口触发器。
- 希望路由器发送给您的报告和警报。

例如，可以基于每天固定时间、 Web 地址和 Web 地址关键字建立受限访问策略。可以阻止 LAN 上的应用程序和服务 （如聊天室或游戏）访问互联网。可以阻止 WAN 或公共 DMZ 网络访问您网络上的特定 PC 组。

入站 （WAN 到 LAN/DMZ）规则限制对进入网络的流量的访问，可有选择性地仅允许特定外部用户访问特定本地资源。默认情况下，会阻止来自不安全 WAN 端所有的对安全 LAN（除了响应来自 LAN 或 DMZ 的请求）的访问。要允许外部设备访问安全 LAN 上的服务，必须为每个服务创建防火墙规则。

如果要允许传入流量，必须向公开路由器 WAN 端口的 IP 地址。这称为 “ 公开主机 ”。如何公开地址取决于 WAN 端口配置；如果设备的 WAN 端口分配的是静态地址，则可以使用 IP 地址，如果 WAN 地址是动态地址，则可以使用 DDNS （动态 DNS）名称。

出站 （LAN/DMZ 到 WAN）规则限制离开您网络的流量的访问，可有选择性地仅允许特定本地用户访问特定外部资源。默认出站规则是允许安全区域 (LAN) 访问公共 DMZ 或不安全 WAN。要阻止安全 LAN 上的主机访问外部 （不安全 WAN）服务，必须为每个服务创建防火墙规则。

配置基本防火墙设置

配置基本防火墙设置的步骤：

步骤 1 选择 **Firewall** > **Basic Settings**。

步骤 2 配置以下防火墙设置：

IP Address Spoofing Protection	要防止网络受到 IP 地址欺骗，请选中 **Enable** 复选框。
DoS Protection	选中 **Enable** 可启用拒绝服务防护。
Block WAN Request	阻止从 WAN 对设备进行的 Ping 请求。
LAN/VPN Web Access	选择可用于连接至防火墙的 Web 访问类型：HTTP 或 HTTPS （安全 HTTP）。

Remote Management **Remote Access** **Remote Upgrade** **Allowed Remote IP Address** **Remote Management Port**	请参阅配置远程管理。
IPv4 Multicast Passthrough (IGMP Proxy)	选中 **Enable** 可为 IPv4 启用组播通道。
IPv6 Multicast Passthrough (IGMP Proxy)	选中 **Enable** 可为 IPv6 启用组播通道。
SIP ALG	要允许会话启动协议 (SIP) 流量穿过防火墙，请选中 **SIP ALG** 复选框。设备最多支持 256 个会话。
UPnP **Allow Users to Configure** **Allow Users to Disable Internet Access**	请参阅配置通用即插即用。
Block Java	选中可阻止 Java 程序。 Java 程序是嵌入在网页中的小程序，可实现网页的动态功能。可能会有恶意程序用于损害或感染计算机。 启用此设置可阻止下载 Java 程序。单击 **Auto** 以自动阻止 Java，或单击 **Manual** 并输入在其上阻止 Java 的特定端口。
Block Cookies	选中可阻止 Cookie。 Cookie 由经常要求登录的网站用于存储会话信息。但是，有些网站使用 Cookie 存储跟踪信息和浏览习惯。启用此选项可过滤掉网站创建的 Cookie。 许多网站要求接受 Cookie 才能正常访问站点。阻止 Cookie 可能会导致许多网站不能正常工作。 单击 **Auto** 以自动阻止 Cookie，或单击 **Manual** 并输入在其上阻止 Cookie 的特定端口。

Block ActiveX	选中可阻止 ActiveX 内容。与 Java 程序类似，ActiveX 控件安装在运行 Internet Explorer 的 Windows 计算机上。可能会有恶意 ActiveX 控件被用来损害或感染计算机。 启用此设置可阻止下载 ActiveX 程序。 单击 **Auto** 以自动阻止 ActiveX，或单击 **Manual** 并输入在其上阻止 ActiveX 的特定端口。
Block Proxy	选中可阻止代理服务器。代理服务器 （或代理）允许计算机通过代理将连接路由到其他计算机，从而绕过某些防火墙规则。 例如，如果某个防火墙规则阻止指向特定 IP 地址的连接，则请求可以通过该规则不阻止的代理进行路由，使限制鞭长莫及。启用此功能可阻止代理服务器。 单击 **Auto** 以自动阻止代理服务器，或单击 **Manual** 并输入在其上阻止代理服务器的特定端口。

步骤 **3** 单击 **Save**。

配置远程管理

可以启用远程管理，以便可以从远程 WAN 网络访问本设备。

要配置远程管理，请在 **Basic Settings** 页面上配置以下设置：

Remote Management	选中 **Enable** 可启用远程管理。
Remote Access	选择可用于连接至防火墙的 Web 访问类型：HTTP 或 HTTPS （安全 HTTP）。
Remote Upgrade	要允许进行设备的远程升级，请选中 **Enable**。
Allowed Remote IP Address	单击 **Any IP Address** 按钮可允许从任何 IP 地址进行远程管理，或在地址字段中输入特定 IP 地址。

Remote Management Port	输入允许进行远程访问的端口。默认端口为 443。远程访问路由器时，必须在 IP 地址中输入远程管理端口。例如： **https://< 远程 ip>:< 远程端口 >**，或 ***https://168.10.1.11:443***

注意 启用远程管理之后，知道路由器 IP 地址的任何人都可访问路由器。因为恶意 WAN 用户可能重新配置设备并用于不正当的用途，所以强烈建议在继续操作之前更改管理员和所有访客密码。

配置通用即插即用

通用即插即用 (UPnP) 允许自动发现可以与本设备通信的设备。

要配置 UPnP，请在 **Basic Settings** 页面上配置以下设置：

UPnP	选中 **Enable** 可启用 UPnP。
Allow Users to Configure	选中此框可允许在其计算机或其他支持 UPnP 的设备上启用了 UPnP 支持的用户设置 UPnP 端口映射规则。如果禁用，则设备不允许应用程序添加转发规则。
Allow Users to Disable Internet Access	选中此框可允许用户禁用互联网访问。

管理防火墙时间表

可以创建防火墙时间表，以在特定日期或每天的特定时间应用防火墙规则。

添加或编辑防火墙时间表

添加或编辑防火墙时间表的步骤：

步骤 **1** 选择 **Firewall** > **Schedule Management**。

步骤 **2** 单击 **Add Row**。

步骤 3 在 **Name** 字段中输入用于标识时间表的唯一名称。此名称显示在 **Select Schedule** 列表中的 Firewall Rule Configuration 页面上。（请参阅配置访问规则。）

步骤 4 在 **Scheduled Days** 部分中，选择要将计划表应用于 All days 还是 Specific Days。如果选择 **Specific Days**，请选中要包含在时间表中的日期旁的框。

步骤 5 在 **Scheduled Time of Day** 部分中，选择要应用计划表的时间。如果选择 **Specific Time**，请输入开始和结束时间。

步骤 6 单击 **Save**。

配置服务管理

创建防火墙规则时，可以指定受规则控制的服务。可以选择常用类型的服务，也可以创建自定义服务。

通过 **Services Management** 页面可以创建应用防火墙规则的自定义服务。定义之后，新服务将出现在 **Available Custom Services** 表的列表中。

创建自定义服务的步骤：

步骤 1 选择 **Firewall** > **Service Management**。

步骤 2 单击 **Add Row**。

步骤 3 在 **Service Name** 字段中，输入服务名称以用于标识和管理。

步骤 4 在 **Protocol** 字段中，从下拉菜单中选择服务使用的第 4 层协议：

- **TCP**
- **UDP**
- **TCP & UDP**
- **ICMP**

步骤 5 在 **Start Port** 字段中，输入服务使用的 TCP 或 UDP 端口范围中的第一个端口。

步骤 6 在 **End Port** 字段中，输入服务使用的 TCP 或 UDP 端口范围中的最后一个 端口。

步骤 7 单击 **Save**。

要编辑条目，请选择该条目，然后单击 **Edit**。进行更改，然后单击 **Save**。

配置访问规则

配置默认出站策略

通过 **Access Rules** 页面可以针对从安全网络 (LAN) 定向到不安全网络 （专用 WAN/可选）的流量配置默认出站策略。

针对从不安全区域到安全区域的流量的默认入站策略是始终阻止，且不能更改。

NOTE 互联网访问策略可覆盖访问规则 （在设备上都已配置时）。

配置默认出站策略的步骤：

步骤 1 选择 **Firewall** > **Access Rules**。

步骤 2 选择 **Allow** 或 **Deny**。

注：确保在设备上启用 IPv6 支持以配置 IPv6 防火墙。请参阅配置 **IPv6**。

步骤 3 单击 **Save**。

重新排序访问规则

访问规则表中规则的显示顺序即为规则的应用顺序。您可能希望对该表进行重新排序，以便能够在其他规则之前优先应用某些规则。例如，您可能希望先应用允许某些类型流量的规则，然后阻止其他类型的流量。

重新排序访问规则的步骤：

步骤 1 选择 **Firewall** > **Access Rules**。

步骤 2 单击 **Reorder**。

步骤 3 选中要上移或下移的规则所在行中的框，然后单击向上或向下箭头以将规则上移或下移一行，或在下拉列表中选择规则的所需位置，然后单击 **Move to**。

步骤 4 单击 **Save**。

添加访问规则

设备上配置的所有防火墙规则都显示在 **Access Rules Table** 中。此列表还指示规则是否启用 （活动）并提供源 / 目标区域的摘要以及受规则影响的服务和用户。

创建访问规则的步骤：

步骤 1 选择 **Firewall** > **Access Rules**。

步骤 2 单击 **Add Row**。

步骤 3 在 **Connection Type** 字段中，选择流量的源：

- **Outbound (LAN > WAN) -** 选择此选项可创建出站规则。
- **Inbound (WAN > LAN) -** 选择此选项可创建入站规则。
- **Inbound (WAN > DMZ) -** 选择此选项可创建入站规则。

步骤 4 从 **Action** 下拉菜单中选择操作：

- **Always Block** - 始终阻止所选类型的流量。
- **Always Allow** - 从不阻止所选类型的流量。
- **Block by schedule** - 根据时间表阻止所选类型的流量。
- **Allow by schedule** - 根据时间表允许所选类型的流量。

步骤 5 从 **Services** 下拉菜单中，选择此规则允许或阻止的服务。选择 **All Traffic** 以允许将规则应用于所有应用程序和服务，或选择要阻止的单个应用程序：

- 域名系统 (DNS)、 UDP 或 TCP
- 文件传输协议 (FTP)
- 超文本传输协议 (HTTP)
- 安全超文本传输协议 (HTTPS)
- 简易文件传输协议 (TFTP)
- 互联网消息访问协议 (IMAP)
- 网络新闻传输协议 (NNTP)
- 邮局协议 (POP3)
- 简单网络管理协议 (SNMP)
- 简单邮件传输协议 (SMTP)

- Telnet
- STRMWORKS
- 终端接入控制器接入控制系统 (TACACS)
- Telnet （命令）
- 辅助 Telnet
- Telnet SSL
- 语音 (SIP)

步骤 6 在 **Source IP** 字段中，选择对其应用防火墙规则的用户：

- **Any** - 规则应用于源自本地网络中任何主机的流量。
- **Single Address** - 规则应用于源自本地网络中单个 IP 地址的流量。在 **Start** 字段中输入地址。
- **Address Range** - 规则应用于源自位于地址范围中的 IP 地址的流量。在 **Start** 字段输入起始 IP 地址，在 **Finish** 字段输入结束 IP 地址。

步骤 7 在 **Log** 字段中，指定是否应记录此规则的数据包。

要记录与此规则匹配的所有数据包的详情，请从下拉菜单中选择 **Always**。例如，如果某个时间表的出站规则选择为 **Block Always**，则对于尝试针对该服务建立出站连接的每个数据包，会在日志中记录包含数据包源地址和目标地址 （以及其他信息）的消息。

启用记录会生成大量日志消息，建议仅用于调试。

选择 **Never** 可禁用记录。

注：当流量从 LAN 或 DMZ 发送到 WAN 时，系统要求在传入 IP 数据包通过防火墙时重写这些数据包的源或目标 IP 地址。

步骤 8 选中 **Rule Status Enable** 复选框以启用新访问规则。

步骤 9 单击 **Save**。

创建互联网访问策略

设备支持多个用于阻止互联网访问的选项。可以阻止所有互联网流量、阻止发送到特定 PC 或端点的互联网流量，或是通过指定要阻止的关键字来阻止对互联网站点的访问。如果在站点名称 （例如网站 URL 或新闻组名称）中找到这些关键字，则站点将被阻止。

添加或编辑互联网访问策略

创建互联网访问策略的步骤：

步骤 1 选择 **Firewall** > **Internet Access Policy**。

步骤 2 单击 **Add Row**。

步骤 3 选中 **Status Enable** 复选框。

步骤 4 输入策略名称以用于标识和管理。

步骤 5 从 **Action** 下拉菜单中选择所需访问限制类型：

- **Always block** - 始终阻止互联网流量。这会阻止与所有端点之间的互联网流量。如果要阻止所有流量，但是允许特定端点接收互联网流量，请参阅步骤 7。
- **Always allow** - 始终允许互联网流量。可以细化此选项以阻止与指定端点之间的互联网流量；请参阅步骤 7。还可以允许除特定网站之外的所有互联网流量；请参阅步骤 8。
- **Block by schedule** - 根据时间表阻止互联网流量 （例如，如果要在工作日办公时间内阻止互联网流量，但是在办公时间之后和周末时允许互联网流量）。
- **Allow by schedule** - 根据时间表允许互联网流量。

如果选择 **Block by schedule** 或 **Allow by schedule**，请单击 **Configure Schedules** 以创建时间表。请参阅管理防火墙时间表。

步骤 6 从下拉菜单中选择时间表。

步骤 7 （可选）将访问策略应用于特定 PC 以允许或阻止来自特定设备的流量：

a. 在 **Apply Access Policy to the Following PCs** 表中，单击 **Add Row**。

b. 从 **Type** 下拉菜单中，选择如何标识 PC（按 MAC 地址、按 IP 地址或通过提供 IP 地址范围）。

c. 在 **Value** 字段中，根据上一步中的选择，输入以下内容之一：

- 对其应用策略的 PC 的 MAC 地址 (xx:xx:xx:xx:xx:xx)。
- 对其应用策略的 PC 的 IP 地址。
- 要阻止的地址范围的起始和结束 IP 地址 （例如， 192.168.1.2-192.168.1.253）。

步骤 **8** 阻止来自特定网站的流量的步骤：

a. 在 **Website Domain Name & Keyword** 表中，单击 **Add Row**。

b. 从 **Type** 下拉菜单中，选择如何阻止网站 （通过指定域名或通过指定 URL 中出现的关键字）。

c. 在 **Value** 字段中，输入用于阻止网站的 URL 或关键字。

例如，要阻止 example.com URL，请从下拉菜单中选择 **URL Address**，然后在 **Value** 字段中输入 **example.com**。例如，要阻止 URL 中包含关键字 “example” 的 URL，请从下拉菜单中选择 **Keyword**，然后在 **Value** 字段中输入 **example**。

步骤 **9** 单击 **Save**。

配置一对一网络地址转换 (NAT)

使用 One-to-one NAT 页面可将位于防火墙之后的本地 IP 地址映射到全局 IP 地址。一对一 NAT 是使配置有专用 IP 地址 （位于防火墙之后）的系统表现为具有公共 IP 地址。

设置一对一 NAT 规则的步骤：

步骤 **1** 选择 **Firewall > One-to-One NAT**。

步骤 **2** 单击 **Add Row**。

步骤 **3** 在 **Private Range Begin** 字段中，输入专用 (LAN) IP 地址范围的起始 IP 地址。

步骤 **4** 在 **Public Range Begin** 字段中，输入公共 (WAN) IP 地址范围的起始 IP 地址。

步骤 **5** 在 **Range Length** 中，输入应映射到专用地址的公共 IP 地址数。

步骤 6 在 **Service** 字段中，选择对其应用规则的服务。通过用于一对一 NAT 的服务可以配置服务，使其在流量发送到对应公共 IP 地址时由专用 IP (LAN) 地址接受。当对应公共 IP 地址上存在流量时，会接受范围内专用 IP 地址上配置的服务。

步骤 7 单击 **Save**。

配置端口转发

端口转发用于将来自互联网的流量从 WAN 上的一个端口重定向到 LAN 上的另一个端口。可使用常用服务，也可以定义自定义服务及关联端口进行转发。

Single Port Forwarding Rules 和 **Port Range Forwarding Rules** 页面列出此设备的所有可用端口转发规则，用于配置端口转发规则。

NOTE 端口转发不适用于 LAN 上的服务器，因为需根据建立传出连接的 LAN 设备来打开传入端口。

某些应用要求在外部设备连接至它们时，在特定端口或端口范围上接收数据才能正常运行。路由器必须仅在所需端口或端口范围上发送这类应用的所有传入数据。

网关具有要打开对应出站和入站端口的常用应用程序和游戏的列表。也可以通过定义流量类型 （TCP 或 UDP）以及要在启用时打开的传入和传出端口范围，来指定端口转发规则。

配置单端口转发

添加单端口转发规则的步骤：

步骤 1 选择 **Firewall** > **Single Port Forwarding**。系统将显示预先存在的应用程序列表。

步骤 2 在 **Application** 字段中，输入要为其配置端口转发的应用程序的名称。

步骤 3 在 **External Port** 字段中，输入在从传出流量进行连接请求时触发此规则的端口号。

步骤 4 在 **Internal Port** 字段中，输入远程系统用于响应所接收的请求的端口号。

步骤 5 在 **Interface** 下拉菜单中，选择 **Both (Ethernet & 3G)**、 **Ethernet** 或 **3G**。

步骤 6 在 **Protocol** 下拉菜单中选择协议 （**TCP**、 **UDP** 或 **TCP** & **UDP**）。

步骤 7 在 **IP Address** 字段中，输入特定 IP 流量将转发到的 LAN 端主机的 IP 地址。例如，可以将 HTTP 流量转发到 LAN 端 Web 服务器的 IP 地址的端口 80。

步骤 8 在 **Enable** 字段中，选中 **Enable** 框以启用规则。

步骤 9 单击 **Save**。

配置端口范围转发

添加端口范围转发规则的步骤：

步骤 1 选择 **Firewall** > **Port Range Forwarding**。

步骤 2 在 **Application** 字段中，输入要为其配置端口转发的应用程序的名称。

步骤 3 在 **External Port** 字段中，指定当传出流量发出连接请求时将触发此规则的端口号。

步骤 4 在 **Start** 字段中，指定进行转发的端口范围的起始端口号。

步骤 5 在 **End** 字段中，指定进行转发的端口范围的结束端口号。

步骤 6 在 **Interface** 下拉菜单中，选择 **Both (Ethernet & 3G)**、 **Ethernet** 或 **3G**。

步骤 7 在 **Protocol** 下拉菜单中选择协议 （**TCP**、 **UDP** 或 **TCP** & **UDP**）。

步骤 8 在 **IP Address** 字段中，输入特定 IP 流量将转发到的 LAN 端主机的 IP 地址。

步骤 9 在 **Enable** 字段中，选中 **Enable** 框以启用规则。

步骤 10 单击 **Save**。

配置端口范围触发

LAN 或 DMZ 上的设备通过端口触发可以请求一个或多个端口转发给他们。端口触发等待来自某一指定端口上 LAN/DMZ 的出站请求，然后为该指定类型的流量打开传入端口。

端口触发是一种动态端口转发形式，而应用程序通过打开的传出或传入端口传输数据。端口触发为指定的传出端口上的指定类型流量打开传入端口。端口触发比静态端口转发 （配置防火墙规则时可用）更灵活，因为规则不必引用特定 LAN IP 或 IP 范围。此外，端口在未使用时不会保留为打开状态，这样可提供端口转发所不具备的安全级别。

NOTE 端口触发不适用于 LAN 上的服务器，因为需根据建立传出连接的 LAN 设备来打开传入端口。

某些应用要求在外部设备连接至它们时，在特定端口或端口范围上接收数据才能正常运行。路由器必须仅在所需端口或端口范围上发送这类应用的所有传入数据。网关具有要打开对应出站和入站端口的常用应用程序和游戏的列表。也可以通过定义流量类型（TCP 或 UDP）以及要在启用时打开的传入和传出端口范围，来指定端口触发规则。

添加端口触发规则的步骤：

步骤 1 选择 **Firewall** > **Port Range Triggering**。

步骤 2 在 **Application** 字段中，输入要为其配置端口转发的应用程序的名称。

步骤 3 在 **Triggered Range** 字段中，输入当传出流量发出连接请求时将触发此规则的端口号或端口号范围。如果传出连接仅使用一个端口，请在两个字段中输入相同端口号。

步骤 4 在 **Forwarded Range** 字段中，输入远程系统用于响应所接收的请求的端口号或端口号范围。如果传入连接仅使用一个端口，请在两个字段中指定相同端口号。

步骤 5 在 **Interface** 下拉菜单中，选择 **Both (Ethernet & 3G)**、 **Ethernet** 或 **3G**。

步骤 6 在 **Enable** 字段中，选中 **Enable** 框以启用规则。

步骤 7 单击 **Save**。

6

配置 VPN

本章介绍如何配置设备的 VPN 和安全性。

VPN 隧道类型

可以在设备上配置 VPN 以提供以下两者之间的安全通信信道或隧道：

- 两个网关路由器
- 一个远程客户端设备和一个网关路由器

配置基本站点到站点 IPsec VPN

设备对单个网关到网关 VPN 隧道支持站点到站点 IPsec VPN。配置这些基本 VPN 设置之后，您就能够安全地连接至另一个支持 VPN 的路由器。例如，可以将分支站点处的设备配置为连接至连接企业站点处站点到站点 VPN 隧道的路由器，以便分支站点具有针对企业网络的安全访问。

为站点到站点 IPsec 连接配置基本 VPN 设置的步骤：

步骤 **1** 选择 **VPN > Site-to-Site IPsec VPN > Basic VPN Setup**。

步骤 **2** 在 **New *Connection Name*** 字段中，输入 VPN 隧道的名称。

步骤 **3** 在 ***Pre-Shared Key*** 字段中，输入预先共享密钥，或将在两个路由器之间交换的密码。必须是 8 至 49 个字符。

步骤 **4** 在 ***Endpoint Information*** 字段中输入以下信息：

- **Remote Endpoint** - 选择对设备将连接的路由器的标识是通过其 IP 地址还是通过完全合格域名。例如， IP 地址如 192.168.1.1，完全合格域名如 cisco.com。
- **Remote WAN (Internet) IP Address** - 输入远程端点的公共 IP 地址或域名。
- **Local WAN (Internet) IP Address** - 输入您的设备的公共 IP 地址或域名。

步骤 **5** 在 ***Secure Connection Remote Accessibility*** 字段中输入以下信息：

- **Remote LAN (Local Network) IP Address** - 远程端点的专用网络 (LAN) 地址。这是远程站点处的内部网络 IP 地址。
- **Remote LAN Subnet Mask** - 远程端点的专用网络 (LAN) 子网掩码。
- **Local LAN (Local Network) IP Address** - 本地网络的专用网络 (LAN) 地址。这是设备上的内部网络 IP 地址。
- **Local LAN (Local Network) Subnet Mask** - 本地网络的专用网络 (LAN) 子网掩码。

注：远程 WAN 和远程 LAN IP 地址不能共存于同一子网中。例如，当流量通过 VPN 路由时，远程 LAN IP 地址 192.168.1.100 和本地 LAN IP 地址 192.168.1.115 会导致冲突。第三个八位字节必须不同，从而使 IP 地址位于不同子网上。例如，远程 LAN IP 地址 192.168.1.100 和本地 LAN IP 地址 192.168.2.100 即可接受。

步骤 **6** 单击 **Save**。

查看默认值

单击 **View Default Settings** 可查看基本 VPN 设置中使用的默认值。这些值由 VPN Consortium 推荐，假设您使用预先共享密钥或设备和远程端点都知道的密码。

配置站点到站点 **IPsec VPN** 高级参数

高级 VPN 参数 （如 IKE 和其他 VPN 策略）控制设备如何启动和接收 VPN 连接。

要配置高级 VPN 参数，请选择 **VPN > Site-to-Site IPsec VPN > Advanced VPN Setup**。

管理 **IKE** 策略

互联网密钥交换 (IKE) 协议在两个 IPsec 主机之间动态地交换密钥。可以创建 IKE 策略以定义在通过 IPsec VPN 连接与远程路由器交换数据时要使用的安全参数。例如，可以创建 IKE 策略以便为对等鉴权和加密算法定义参数。确保 VPN 策略中的加密、鉴权和密钥组参数与远程路由器上的设置兼容。

添加 IKE 策略的步骤：

步骤 **1** 在 **Advanced VPN Setup** 页面上，单击 **Add Row**。

步骤 **2** 为 IKE 策略输入唯一名称以便能够方便地识别和管理策略。

步骤 **3** 在 **Exchange Mode** 字段中，为策略选择以下模式之一：

- **Main** - 协商安全性较高但较慢的隧道。
- **Aggressive** - 建立较快但安全性较低的连接。

步骤 **4** 在 **Local Identifier** 和 **Remote Identifier** 字段中，指明是要按其真实 IP 地址还是公共 IP 地址来标识设备和远程路由器。如果选择 IP 地址，请输入设备和远程路由器的真实 IP 地址。

步骤 **5** 在 ***IKE SA Parameters*** 部分中，配置各个参数，以便定义设备与远程路由器之间协商安全关联 (SA) 的强度和模式。

a. 在 **Encryption Algorithm** 字段中，选择用于加密数据的算法。

b. 在 **Authentication Algorithm** 字段中，为 VPN 报头指定鉴权算法。确保在 VPN 隧道两端配置相同的鉴权算法。

c. 在 **Pre-Shared Key** 字段中，输入密钥或密码。确保密码不包含双引号 (")。

d. 在 **Diffie-Hellman (DH) Group** 字段中，指定交换预先共享密钥时使用的 DH 组算法。 DH 组按位设置算法强度。确保在 IKE 策略两端配置相同的 DH 组。

e. 在 **SA-Lifetime** 字段中，输入安全关联变为无效之前的时间间隔 （以秒为单位）。

f. 要启用 **Dead Peer Detection** 功能，请选中 **Enable** 框。失效对等体检测 (DPD) 用于检测对等体是否为活动状态。如果检测到对等体已失效，则设备会删除 IPsec 和 IKE 安全关联。如果启用此功能，请同时输入以下设置：

- **DPD Delay -** 连续 DPD R-U-THERE 消息之间的间隔（以秒为单位）。DPD R-U-THERE 消息仅当 IPsec 流量空闲时才发送。
- **DPD Timeout -** 设备在将对等体视为失效之前应等待接收 DPD 消息回复的最长时间。

步骤 **6** 单击 **Save**。

NOTE如果已配置了 VPN 连接，则必须删除现有 VPN 连接才能添加另一个连接。

管理 **VPN** 策略

NOTE创建自动 VPN 策略之前，请确保创建作为自动 VPN 策略创建基础的 IKE 策略。

管理 VPN 策略的步骤：

步骤 **1** 选择 **VPN > Site-to-Site IPsec VPN > Advanced VPN Setup**。单击 **Add Row**。

步骤 **2** 在 **Add / Edit VPN Policy Configuration** 部分中：

a. 在 **Policy Name** 字段中，输入用于标识策略的唯一名称。

b. 在 **Policy Type** 字段中，选择以下选项之一：

- **Auto Policy** - 自动生成 VPN 隧道的一些参数。这要求将互联网密钥交换 (IKE) 协议用于两个 VPN 端点之间的协商。
- **Manual Policy** - 为每个终端点手动输入 VPN 隧道的所有参数 （包括密钥）。不涉及第三方服务器或组织。

c. **Remote Endpoint** - 选择要在远程端点处为网关提供的标识符类型：**IP Address** 或 **FQDN** （完全合格域名）。输入 IP 地址或 FQDN。

步骤 **3** 在 ***Local Traffic Selection*** 和 ***Remote Traffic Selection*** 部分中：

- 在 **Local IP** 和 **Remote IP** 字段中，指出 VPN 策略将包含的端点数：
  - **Single** - 将策略限制到一个主机上。在 **IP Address** 字段中输入属于 VPN 的主机的 IP 地址。

- **Subnet** - 允许整个子网连接至 VPN。在 **IP Address** 字段中输入网络地址，并在 **Subnet Mask** 字段中输入子网掩码。在 **IP Address** 字段中输入子网的网络 IP 地址。在 **Subnet Mask** 字段中输入子网掩码，如 255.255.255.0。该字段基于 IP 地址自动显示默认子网地址。

NOTE 请勿将重叠子网用于远程或本地流量选择器。使用这些子网需要在路由器和要使用的主机上添加静态路由。例如，请避免以下情况：

本地流量选择器：192.168.1.0/24

远程流量选择器：192.168.0.0/16

步骤 **4** 对于 **Manual** 策略类型，在 **Manual Policy Parameters** 部分中输入设置：

- **SPI-Incoming**、 **SPI-Outgoing** - 输入介于 3 与 8 个字符之间的十六进制值；例如， 0x1234。安全参数索引 (SPI) 标识传入和传出流量流的安全关联。
- **Manual Encryption Algorithm** - 选择用于加密数据的算法。
- **Key-In**、 **Key-Out** - 输入入站和出站策略的加密密钥。密钥长度取决于所选加密算法：
  - DES - 8 个字符
  - 3DES - 24 个字符
  - AES-128 - 16 个字符
  - AES-192 - 24 个字符
  - AES-256 - 32 个字符
- **Manual Integrity Algorithm** - 选择用于验证数据完整性的算法。
- **Key-In**、 **Key Out** - 输入入站和出站策略的完整性密钥 （用于具有完整性模式的 ESP）。密钥长度取决于所选算法：
  - MD5 - 16 个字符
  - SHA-1 - 20 个字符
  - SHA2-256 - 32 个字符

步骤 **5** 对于 **Auto** 策略类型，在 **Auto Policy Parameters** 部分中输入设置。

- **SA-Lifetime** - 输入安全关联的持续时间 （以秒为单位）。指定秒数过后，重新协商安全关联。默认值为 3600 秒。最小值为 300 秒。
- **Encryption Algorithm -** 选择用于加密数据的算法。
- **Integrity Algorithm -** 选择用于验证数据完整性的算法。

- **PFS Key Group -** 选中 **Enable** 框可启用完全向前保密 (PFS) 以提高安全性。速度较慢时，此协议可通过确保对每个第 2 阶段协商执行 Diffie-Hellman 交换，帮助防止窃听。
- **DH Group -** 指定交换预先共享密钥时使用的 DH 组算法。 DH 组按位设置算法强度。确保在 IKE 策略两端配置相同的 DH 组。
- **Select IKE Policy -** 选择定义 SA 协商特性的 IKE 策略。

步骤 **6** 单击 **Save**。

配置 **IPsec VPN** 服务器

使用 IPsec VPN 可建立跨互联网的加密隧道，实现对企业资源的安全远程访问。设备支持以下 IPsec VPN 客户端：

- TheGreenBow
- ShrewSoft

配置 **IPsec VPN** 服务器

配置 IPsec VPN 服务器的步骤：

步骤 **1** 选择 **VPN > IPsec VPN Server> Setup**。

步骤 **2** 选中 **Server Enable** 复选框。

步骤 **3** 在 **Phase 1** 部分中，配置设置以使两个 VPN 端点相互鉴权并协商 IKE 安全关联 (SA)，从而使安全信道在第 2 阶段协商 SA。

a. 在 ***Pre-Shared Key*** 字段中，输入预先共享密钥，或将在设备与远程端点之间交换的密码。该密码必须是 8 至 49 个字符。

b. 在 **Exchange Mode** 字段中，为 IPsec VPN 连接选择以下模式之一：

- **Main** - 协商隧道时的安全性较高，但速度较慢。
- **Aggressive** - 建立连接较快，但安全性较低。

c. 选择 **Encryption Algorithm** 以加密数据并为 VPN 报头选择 **Authentication Algorithm**。确保在设备和远程端点上配置相同的鉴权算法。

d. 在 **Diffie-Hellman (DH) Group** 字段中，指定交换预先共享密钥以按位设置算法强度时使用的 Diffie-Hellman 组算法。确保在设备和远程端点上配置相同的 DH 组。

e. 在 **IKE SA-Lifetime** 字段中，输入重新协商 VPN 连接的安全关联之前的持续时间（以秒为单位）。

步骤 **4** 在 **Phase 2 Configuration** 部分中，配置参数以协商 IPsec 隧道的 IPsec 安全关联 (SA)：

a. 在 **Local IP** 字段中，指示 VPN 策略将包含的端点数：

- **Single** - 将策略限制到一个主机上。在 **IP Address** 字段中输入属于 VPN 的主机的 IP 地址。
- **Subnet** - 允许整个子网连接至 VPN。在 **IP Address** 字段中输入网络地址，并在 **Subnet Mask** 字段中输入子网掩码。在 **IP Address** 字段中输入子网的网络 IP 地址。在 **Subnet Mask** 字段中输入子网掩码，如 255.255.255.0。该字段基于 IP 地址自动显示默认子网地址。

b. 在 **IPsec SA Lifetime** 字段中，输入重新协商 VPN 连接的安全关联之前的持续时间 （以秒为单位）。

c. 选择 **Encryption Algorithm** 以加密数据并为 VPN 报头选择 **Authentication Algorithm**。确保在设备和远程端点上配置相同的鉴权算法。

d. 要创建更安全的 IPsec VPN 连接，请选中 **PFS Key Group Enable** 复选框，从而确保在第 2 阶段进行新的 Diffie-Hellman 密钥交换。完全向前保密 (PFS) 可在第 1 阶段中生成的 DH 密钥在传输中受损时使用新密钥保护数据，从而提供额外的一层保护。确保两个 IPsec 端点都启用了 PFS。

步骤 **5** 单击 **Save**。

配置 **IPsec VPN** 用户帐户

步骤 **1** 选择 **VPN > IPsec VPN Server> User**。

步骤 **2** 单击 **Add Row**。

步骤 **3** 输入用户名和密码。

建议密码不包含任何语言中的字典单词，应由字母 （包含大写和小写字母）、数字和符号组成。密码长度最多为 64 个字符。

步骤 **4** 要从 .CSV 文件导入文件名和密码，请单击 **Import**。系统将显示 **Administration > Users** 页面。在 **Import Username and Password** 部分中，单击 **Browse** 找到文件，然后单击 **Import**。

步骤 **5** 保存用户帐户。

配置 **PPTP**

点对点隧道协议 (PPTP) 是一种网络协议，可跨公共网络 （如互联网）创建安全 VPN 连接，实现从远程客户端到企业网络的安全数据传输。

配置 **PPTP** 服务器

配置 PPTP VPN 服务器的步骤：

步骤 **1** 选择 **VPN** > **PPTP Server**。

步骤 **2** 在 **PPTP Server Configuration** 部分中，配置 PPTP VPN 设置：

a. 选中 **PPTP Server Enable** 复选框。

b. 输入 PPTP 服务器的 IP 地址。

c. 输入 PPTP 客户端的 IP 地址范围。

d. 要对通过 PPTP VPN 连接的数据进行加密，请选中 **MPPE Encryption Enable** 复选框。

步骤 **3** 单击 **Save**。

创建和管理 **PPTP** 用户

创建和启用 PPTP 用户的步骤：

步骤 **1** 选择 **VPN > PPTP Server**。在 **PPTP User Account Table** 中，单击 **Add Row**。

步骤 **2** 输入用于对 PPTP 用户进行鉴权的用户名和密码。输入长度为 4 到 32 个字符的值。

步骤 **3** 选中用户的 **Enable** 复选框。

步骤 **4** 要从 .CSV 文件导入文件名和密码，请单击 **Import**。系统将显示 **Administration > Users** 页面。在 **Import Username and Password** 部分中，单击 **Browse** 找到文件，然后单击 **Import**。

步骤 **5** 保存用户帐户。

配置 **VPN** 通道

源自 VPN 客户端的 VPN 流量使用 VPN 通道可以通过设备。

配置 VPN 通道的步骤：

步骤 **1** 选择 **VPN** > **VPN Passthrough**。

步骤 **2** 选中 **Enable** 复选框以选择允许通过设备的流量类型。

步骤 **3** 单击 **Save**。

SSL 证书

思科 RV130/RV130W 支持适用于 IPsec VPN 的证书身份验证。安全套接字层 (SSL) 证书可提供数据加密，并在 SSL 会话建立之前对服务器进行身份验证。

要管理 SSL 证书，请单击 **VPN > SSL Certificate**。

- 受信任证书 （**CA** 证书）表
  - 单击 **Upload** 转到 **Certificates** 页面。单击 **Browse**，从您的本地驱动器上选择一个受信任证书，然后单击 **Import**。
- 活动自签证书
  - 单击 **Upload** 转到 **Certificates** 页面。单击 **Browse**，从您的本地驱动器上选择一个活动自签证书，然后单击 **Import**。
- 自签证书请求

  自签证书是由标识您设备的 CA 签发的证书 （或者如果您不需要 CA 的身份保护，也可以进行自签名）。要请求由 CA 签署的自签证书，您可以通过输入身份识别参数从网关生成证书签名请求，并将其发送给相关 CA 签署。完成签署后，上传 CA 的受信任证书和 CA 签署的证书，以激活此网关的自签证书身份验证。这样一来，自签证书便可用于与对等点的 IPsec 连接，从而使网关的验证生效。

- **Generate Certificate -** 要生成 SSL 证书请求，请单击 **Generate Certificate**，系统将显示新的证书信息请求页面。

  Name - 输入新证书的名称。

  Subject - 请使用以下格式：“ CN=xxx ”（“ CN ”必须大写）。

  Hash Algorithm - 从下拉列表中选择所需的哈希算法。

  Signature Algorithm - 从下拉列表中选择所需的签名算法。

  Signature Key Length - 从下拉列表中选择所需的签名密钥长度。

  （可选） **IP Address -** 输入路由器的 IP 地址。

  （可选） **Domain Name -** 输入路由器的域名。

  （可选） **Email Address -** 输入请求者的电子邮件地址。

- **Export for Admin -** 要将证书请求导出到本地驱动器，请选择此项。

• **Export Certificate -** 要下载路由器证书，请单击 **Export for Client** 按钮。

单击 **Save** 可保存配置，单击 **Cancel** 可撤销设置。

VPN 设置向导

要使用 VPN 设置向导，请执行以下操作：

步骤 **1** 单击 **VPN > VPN Setup Wizard**。

步骤 **2** 屏幕上将弹出向导窗口。按照屏幕上所显示的说明来设置设备。

7

配置服务质量 (QoS)

本章介绍如何配置以下服务质量 (QoS) 功能：

服务质量 (QoS) 向各个应用程序、用户或数据流分配优先权，或保证数据流达到某个性能级别。当网络容量不足时，这些保证十分重要。例如，对于实时流多媒体应用程序 （如 IP 网络语音、在线游戏和 IP-TV，因为它们需要固定比特率并且对延迟十分敏感），以及容量受限的网络。

配置带宽管理

可以使用设备带宽管理功能管理从安全网络 (LAN) 流向不安全网络 (WAN) 的流量的带宽。

配置带宽

可以限制带宽以降低设备传输数据的速率。还可以使用带宽简档限制出站流量，这样可防止 LAN 用户占用所有互联网链路带宽。

设置上游和下游带宽的步骤：

步骤 **1** 选择 **QoS** > **Bandwidth Management**。

步骤 **2** 在 **Bandwidth Management** 字段中，选中 **Enable**。 ISP 提供的最大带宽显示在 **Bandwidth** 部分中。

步骤 3 在 **Bandwidth Table** 中，输入 WAN 接口的以下信息：

Upstream	用于向互联网发送数据的带宽 (kb/s)。
Downstream	用于从互联网接收数据的带宽 (kb/s)。（仅适用于默认 VLAN）

步骤 4 单击 **Save**。

配置带宽优先权

在 **Bandwidth Priority Table** 中，可以向服务分配优先权以管理带宽使用情况。

配置带宽优先权的步骤：

步骤 1 在 **Bandwidth Priority Table** 中，单击 **Add Row**。

步骤 2 在以下字段中输入信息：

Enable	选中可启用此服务的带宽管理。
Direction	选择要为入站还是出站流量设置优先权。
Category	选择是为服务、 VLAN/SSID、源 IP （入站流量）还是目标 IP （出站流量）设置带宽优先权。
Service	选择要为其设置优先权的服务。
VLAN/SSID	选择要为其设置优先权的 VLAN 或 SSID。
IP Address	如果在 **Category** 字段中选择 Source IP 或 Destination IP，请输入源或目标的 IP 地址和子网掩码。
Subnet Mask	
Priority	为所选类别设置优先权 （**low**、 **medium** 或 **high**）。
Remarking	选中可对差分服务代码点 (DSCP) 启用重新标记。启用此功能可基于 **DSCP Settings** 页面上的 DSCP 队列映射，对 LAN 上的网络流量设置优先权。
DSCP	为此网络上的数据包输入重新标记值。

步骤 3 单击 **Save**。

要编辑表中条目的设置，请选中相关框并单击 **Edit**。完成更改之后，单击 **Save**。

要从表中删除条目，请选中相关框并单击 **Delete**。单击 **Save**。

要添加新服务定义，请单击 **Service Management** 按钮。可以定义新服务以用于所有防火墙和 QoS 定义。请参阅配置服务管理。

配置基于端口的 QoS 设置

可以为设备上的每个端口配置 QoS 设置。设备支持四个优先权队列，用于对每个端口进行流量优先权设置。

为设备上的端口配置 QoS 设置的步骤：

步骤 1 选择 **QoS** > **QoS Port-Based Settings**。

步骤 2 对于 **QoS Port-Based Settings** 表中的每个端口，输入以下信息：

Trust Mode	从下拉菜单中选择以下选项之一： • **Port** - 启用基于端口的 QoS 设置。随后可以为特定端口设置流量优先权。流量队列优先权从最低优先权 1 开始，到最高优先权 3 结束。 • **DSCP** - 差分服务代码点 (DSCP)。启用此功能可基于 **DSCP Settings** 页面上的 DSCP 队列映射，对 LAN 上的网络流量设置优先权。 • **CoS** - 服务等级 (CoS)。
Default Traffic Forwarding Queue for Untrusted Devices	为出站流量选择优先权级别 （1 至 3）。

步骤 3 单击 **Save**。

要恢复默认基于端口的 QoS 设置，请单击 **Restore Default** 并保存更改。

配置 **CoS** 设置

使用 QoS Port-Based Settings 页面的链接可将 CoS 优先权设置映射到 QoS 队列。

将 CoS 优先权设置映射到流量转发队列的步骤：

步骤 **1** 选择 **QoS** > **CoS Settings**。

步骤 **2** 对于 **CoS Settings Table** 中的每个 CoS 优先权级别，请从 **Traffic Forwarding Queue** 下拉菜单中选择优先权值。

这些值根据流量类型，使用较高或较低流量优先权值进行标记。

步骤 **3** 单击 **Save**。

要恢复默认基于端口的 QoS 设置，请单击 **Restore Default** 然后单击 **Save**。

配置 **DSCP** 设置

可以使用 **DSCP Settings** 页面配置 DSCP 到 QoS 队列映射。

配置 DSCP 到 QoS 队列映射的步骤：

步骤 **1** 选择 **QoS** > **DSCP Settings**。

步骤 **2** 通过单击相关按钮，选择在 **DSCP Settings Table** 中是仅列出 RFC 值还是列出所有 DSCP 值。

步骤 **3** 对于 **DSCP Settings Table** 中的每个 DSCP 值，请从 **Queue** 下拉菜单中选择优先权级别。

这会将 DSCP 值映射到所选 QoS 队列。

步骤 **4** 单击 **Save**。

要恢复默认 DSCP 设置，请依次单击 **Restore Default** 和 **Save**。

8

Cisco Small BusinessCisco Small Business 管理设备

本章介绍设备的管理功能，包括用户创建、网络管理、系统诊断和日志、日期和时间以及其他设置。

设置设备属性

向设备分配名称和域名可确保其他设备可方便地识别它。

设置设备属性的步骤：

步骤 **1** 选择 **Administration > Device Properties**。

步骤 2 在 **Hostname** 字段中输入用于在网络上唯一标识设备的名称。例如 RTR141。

步骤 3 在 **Domain Name** 字段中，输入设备所在的域。例如 abcbusiness.com。如果不知道组织的域名，请联系网络管理员。

步骤 4 保存更改。

设置密码复杂性

对于密码更改，可强制实施密码复杂性最低要求。

配置密码复杂性设置的步骤：

步骤 1 选择 **Administration > Password Strength**。

步骤 2 在 ***Password Complexity Settings*** 字段中，选中 **Enable**。

步骤 3 配置密码复杂性设置：

Minimum Password Length	输入最小密码长度 （0-64 个字符）。
Minimum number of character classes	输入表示以下字符类别之一的数字： • 大写字母。 • 小写字母。 • 数字。 • 标准键盘上有的特殊字符。 默认情况下，密码必须包含以上至少三种类别的字符。
The new password must be different than the current one	选中 **Enable** 可要求新密码与当前密码不同。
Password Aging	选中 **Enable** 可使密码在指定时间之后过期。
Password aging time	输入密码过期之前的天数 (1-365)。默认值为 180 天。

步骤 4 单击 **Save**。

配置用户帐户

设备支持两个用于管理和查看设置的用户帐户：管理用户 （默认用户名和密码：cisco）和访客用户 （默认用户名：guest）。

访客帐户拥有只读访问权限。可以为管理员和访客帐户设置和管理用户名和密码。

配置用户帐户的步骤：

步骤 1 选择 **Administration** > **Users**。

步骤 2 在 ***Account Activation*** 字段中，选中要激活的帐户的框。（admin 帐户必须为活动状态。）

步骤 3 （可选）要编辑管理员帐户，请在 ***Administrator Account Setting*** 下选中 **Edit Administrator Settings**。要编辑访客帐户，请在 *Guest Settings* 下选中 **Edit Guest Settings**。输入以下信息：

New Username	输入新用户名。
Old Password	输入当前密码。
New Password	输入新密码。 建议密码不包含任何语言中的字典单词，应由字母（包含大写和小写字母）、数字和符号组成。密码长度最多为 64 个字符。
Retype New Password	重新输入新密码。

步骤 4 单击 **Save**。

导入用户帐户

可以使用 CSV 文件同时导入多个用户。

确保 CSV 文件中的数据的组织方式如下所示：

TYPE	USERNAME	PASSWORD
Admin	Admin123	Admin123
Guest	Guest123	Guest123

TYPE	USERNAME	PASSWORD	ENABLE
PPTP	PPTP-user-1	12345678	enable
PPTP	PPTP-user-2	345123678	disable

TYPE	USERNAME	PASSWORD
VPNServer	vpn-user-1	12345678
VPNServer	vpn-user-2	33245678

TYPE	USERNAME	PASSWORD	ACCESS_TIME
guestnet	guestnet-user-1	12345678	1440
guestnet	guestnet-user-2	33245678	60

NOTE 各列的名称区分大小写。请勿更改各列的顺序或名称。

从 CSV 文件导入用户帐户的步骤：

步骤 1 在 **Import User Name & Password** 字段中，单击 **Browse**。

步骤 2 找到文件，然后单击 **Open**。

步骤 3 单击 **Import**。

设置会话超时值

超时值是设备管理器会话结束之前允许处于不活动状态的分钟数。可以为 Admin 和 Guest 帐户配置超时。

配置会话超时的步骤：

步骤 1 选择 **Administration** > **Session Timeout**。

步骤 2 在 **Administrator Inactivity Timeout** 字段中，输入会话由于处于不活动状态而超时之前的分钟数。选择 **Never** 可允许管理员永久保持登录状态。

步骤 3 在 **Guest Inactivity Timeout** 字段中，输入会话由于处于不活动状态而超时之前的分钟数。选择 **Never** 可允许管理员永久保持登录状态。

步骤 4 单击 **Save**。

配置简单网络管理 (SNMP)

通过简单网络管理协议 (SNMP) 可以从 SNMP 管理器监控和管理路由器。SNMP 提供了一种远程方法，用于监控和控制网络设备，并用于管理配置、统计信息收集、性能和安全性。

配置 SNMP 系统信息

NOTE 需要先在计算机上安装 SNMP 软件，然后才能使用 SNMP。设备仅支持用于 SNMP 管理的 SNMPv3 以及用于 SNMP 陷阱消息的 SNMPv1/2/3。

启用 SNMP 的步骤：

步骤 1 选择 **Administration** > **SNMP**。

步骤 2 选中 **Enable** 可启用 SNMP。

步骤 3 对于 **Allow user access via Internet** 或 **Allow user access via VPN**，选中相应的 **Enable** 复选框可允许用户通过互联网访问或允许用户通过 VPN 访问。

步骤 4 在 **Mode** 字段中选择 SNMP 版本。

步骤 5 输入以下信息：

SysContact	输入此设备的联系人姓名。例如，网络管理员。
SysLocation	输入设备的物理位置。例如， Rack #2, 4th Floor。
SysName	输入用于方便标识设备的名称。例如 RTR 141。

步骤 6 单击 **Save**。

编辑 SNMPv3 用户

可以为设备的两个默认用户帐户 （Admin 和 Guest）配置 SNMPv3 参数。

配置 SNMPv3 设置的步骤：

步骤 1 选择 **Administration** > **SNMP**。

步骤 2 在 **SNMPv3 User Configuration** 下配置以下设置：

UserName	选择要配置的帐户 （**admin** 或 **guest**）。
Access Privilege	显示所选用户帐户的访问权限。
Security Level	选择 SNMPv3 安全级别： **No Authentication and No Privilege** - 不需要任何鉴权和私密性。 **Authentication and No Privilege** - 仅提交鉴权算法和密码。 **Authentication and Privilege** - 提交鉴权和私密性算法以及密码。
Authentication Algorithm Server	选择鉴权算法类型 （**MD5** 或 **SHA**）。
Authentication Password	输入鉴权密码。

Privacy Algorithm	选择私密性算法类型 （**DES** 或 **AES**）。
Privacy Password	输入私密性密码。

步骤 **3** 单击 **Save**。

配置 SNMP 陷阱

通过 **SNMP Trap Configuration** 部分中的字段可以配置设备将陷阱消息 （通知）发送到的 SNMP 代理。

配置陷阱的步骤：

步骤 1 选择 **Administration** > **SNMP**。

步骤 2 在 **Trap Configuration** 下配置以下设置：

IP Address	输入 SNMP 管理器或陷阱代理的 IP 地址。
Port	输入将陷阱消息发送到的 IP 地址的 SNMP 陷阱端口。
Community	输入代理所属的社区字符串。 大多数代理配置为监听公共社区中的陷阱。
SNMP Version	选择 SNMP 版本：**v1**、 **v2c** 或 **v3**。
SNMP Trap Severity Level	选择设备必须发送陷阱消息时的严重性级别。

步骤 3 单击 **Save**。

使用诊断工具

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。

- 网络工具
- 配置端口镜像

网络工具

使用网络工具可对网络进行故障排除。

使用 **PING**

可以使用 PING 实用程序测试此路由器与网络中其他设备之间的连接。还可以使用 Ping 工具测试互联网连接，方法是对完全合格域名 （例如 www.cisco.com）执行 Ping 命令。

使用 PING 的步骤：

步骤 1 选择 **Administration** > **Diagnostics** > **Network Tools**。

步骤 2 在 **IP Address / Domain Name** 字段中，输入要对其执行 Ping 命令的设备 IP 地址或完全合格域名，如 www.cisco.com。

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。

使用 **Traceroute**

Traceroute 实用程序显示目标 IP 地址与此路由器之间存在的所有路由器。路由器显示此路由器与目标之间的最多 30 个步跳 （中间路由器）。

使用 Traceroute 的步骤：

步骤 1 选择 **Administration** > **Diagnostics** > **Network Tools**。

步骤 2 在 **IP Address / Domain Name** 字段中，输入要追踪的 IP 地址。

步骤 3 单击 **Traceroute**。系统将显示 Traceroute 结果。

执行 **DNS** 查找

可以使用查找工具查找互联网上的主机（例如， Web、 FTP 或邮件服务器）的 IP 地址。

要检索互联网上的 Web、 FTP、邮件或任何其他服务器的 IP 地址，请在文本框中键入互联网名称并单击 **Lookup**。如果主机或域条目存在，则您会看到包含 IP 地址的响应。未知主机消息指示指定互联网名称不存在。

使用查找工具的步骤：

步骤 1 选择 **Administration** > **Diagnostics** > **Network Tools**。

步骤 2 在 **Internet Name** 字段中，输入主机的互联网名称。

步骤 3 单击 **Lookup**。系统将显示 nslookup 结果。

配置端口镜像

端口镜像通过从一个端口向监控端口发送所有传入和传出数据包的副本来监控网络流量。可以使用端口镜像作为诊断或调试工具，尤其是在躲避攻击或查看从 LAN 到 WAN 的用户流量以了解用户是否在访问不应访问的信息或网站时。

LAN 主机 (PC) 应使用静态 IP 地址避免与端口镜像有关的任何问题。如果没有为 LAN 主机配置静态 IP 地址，则 DHCP 租用可能会对 LAN 主机过期，可能会导致端口镜像失败。

配置端口镜像的步骤：

步骤 1 选择 **Administration** > **Diagnostics** > **Port Mirroring**。

步骤 2 在 **Mirror Source** 字段中，选择要镜像的端口。

步骤 3 从 **Mirror Port** 下拉菜单中选择镜像端口。如果使用某个端口进行镜像，请勿将该端口用于任何其他流量。

步骤 4 单击 **Save**。

配置日志和电子邮件设置

配置日志可监控指示设备状况和性能的活动。

配置日志设置

配置记录的步骤：

步骤 1 选择 **Administration** > **Logging** > **Log Settings**。

步骤 2 在 **Log Mode** 字段中，选中 **Enable**。

步骤 3 选中 **Email Alert Enable** 复选框可将设备配置为针对可能影响设备的性能、操作和安全性的事件或行为，或是为了进行调试，向特定电子邮件地址发送警报电子邮件。选中相应框可针对以下事件启用电子邮件警报：

WAN 连接 **/** 中断	当 WAN 链路中断时发送一封电子邮件，当链路再次连接时发送另一封电子邮件。
站点到站点 **IPsec VPN** 隧道连接 **/** 中断	当站点到站点 IPsec VPN 隧道中断时发送一封电子邮件，当隧道再次连接时发送另一封电子邮件。
CPU 过载	当 CPU 利用率高于阈值时发送一封警报电子邮件，当 CPU 利用率回落到正常值时发送另一封警报电子邮件。
系统启动	当设备正在启动时发送电子邮件警报。
新固件可用	当有新固件可供设备使用时发送电子邮件警报。

步骤 **4** 单击 **Add Row**。

步骤 5 配置以下设置：

Remote Log Server	输入将维护日志的日志服务器的 IP 地址。
Log Severity for Local Log and Email	选择要对其维护日志并将这些日志发送到特定电子邮件地址的事件的严重性。严重性高于所选日志类型的所有日志类型将自动包含在内，您不能排除这些类型。例如，如果选择 Error 日志，则也会选择 Emergency、 Alert 和 Critical。 下面按照从高到低的顺序列出了事件的严重性级别： • **Emergency** - 系统无法使用。 • **Alert** - 需要采取措施。 • **Critical** - 系统处于高危状态。 • **Error** - 系统出错。 • **Warning** - 系统已发出警告。 • **Notification** - 系统能够正常工作，但系统已发出通知。 • **Information** - 设备信息。 • **Debugging** - 详细事件信息。选择此日志严重性可生成较长的日志列表，不建议在正常路由器操作过程中使用。
Enable	要启用这些记录设置，请选中此框。

步骤 6 单击 **Save**。

步骤 7 单击 **View Logs** 查看系统日志表。

要编辑 **Logging Setting Table** 中的条目，请选择条目并单击 **Edit**。进行更改，然后单击 **Save**。

配置日志电子邮件

可以将设备配置为通过电子邮件发送日志。建议为发送和接收日志而设置单独的电子邮件帐户。

必须先设置要捕获的日志的严重性；请参阅配置日志设置。

配置日志电子邮件的步骤：

步骤 1 选择 **Administration** > **Logging** > **E-mail Settings**。

步骤 2 要启用日志事件的电子邮件，请选中 **Enable**。

系统将显示要捕获的日志的最低电子邮件日志严重性。要更改此设置，请单击 **Configure Severity**。

步骤 3 配置以下设置：

E-mail Server Address	输入 SMTP 服务器的地址。这是与设置的电子邮件帐户关联的邮件服务器 （例如, mail.companyname.com）。
E-mail Server Port	输入 SMTP 服务器端口。如果电子邮件提供商要求将专用端口用于电子邮件，请在此处输入。否则，请使用默认设置 (25)。
Return E-mail Address	输入在从路由器到发送目标电子邮件地址的日志无法送达时设备将消息发送到的返回电子邮件地址。
Send to E-mail Address (1)	输入将日志发送到的电子邮件地址 （例如, logging@companyname.com）。
Send to E-mail Address (2) (Optional)	
Send to E-mail Address (3) (Optional)	
E-mail Encryption	选择 SSL 或 TSL 作为电子邮件加密方法。 如果不想使用电子邮件加密方法，请选择 Disable。
Authentication with SMTP Server	如果 SMTP （邮件）服务器要求进行鉴权之后才接受连接，请从下拉菜单中选择鉴权类型：**None**、**LOGIN**、 **PLAIN** 和 **CRAM-MD5**。

E-mail Authentication Username	输入电子邮件鉴权用户名（例如，*logging@companyname.com*）。
E-mail Authentication Password	输入电子邮件鉴权密码（例如，用于访问将日志发送到的已设置电子邮件帐户的密码）。
E-mail Authentication Test	单击 **Test** 可测试电子邮件鉴权。

步骤 4 在 **Send E-Mail Logs by Schedule** 部分中，配置以下设置：

Unit	选择日志的时间单位（**Never**、 **Hourly**、 **Daily** 或 **Weekly**）。如果选择 **Never**，则不发送日志。
Day	如果选择每周时间表来发送日志，请选择在星期几发送日志。
Time	如果选择每天或每周时间表来发送日志，请选择一天中发送日志的时间。

步骤 5 单击 **Save**。

配置 Bonjour

Bonjour 是一种服务通告和发现协议。在设备上， Bonjour 仅通告启用 Bonjour 时在设备上配置的默认服务。

启用 Bonjour 的步骤：

步骤 1 选择 **Administration** > **Bonjour**。

步骤 2 选中 **Enable** 可启用 Bonjour。

步骤 3 要为 **Bonjour Interface Control Table** 中列出的 VLAN 启用 Bonjour，请选中对应的 **Enable Bonjour** 框。

可以为特定 VLAN 启用 Bonjour。通过在 VLAN 上启用 Bonjour，VLAN 上存在的设备可以发现路由器上可用的 Bonjour 服务 （如 HTTP/HTTPS）。

例如，如果 VLAN 配置的 ID 为 2，则除非为 VLAN 2 启用 Bonjour，否则 VLAN 2 上存在的设备和主机无法发现在路由器上运行的 Bonjour 服务。

步骤 4 单击 **Save**。

配置日期和时间设置

您可以配置时区、是否针对夏令时进行调整，以及使用哪个网络定时协议 (NTP) 服务器同步日期和时间。然后路由器从 NTP 服务器获取日期和时间信息。

配置 NTP 和时间设置的步骤：

步骤 1 选择 **Administration** > **Time Settings**。系统将显示当前时间。

步骤 2 在以下字段中输入信息：

Time Zone	选择与格林威治标准时间 (GMT) 相关的时区。
Adjust for Daylight Savings Time	如果您所在区域支持，请选中 **Adjust for Daylight Savings Time** 框。 如果在 **Set Date and Time** 字段中单击 **Manual**，则此复选框为灰色。
Daylight Saving Mode	如果选择 **By date**，请输入夏令时模式开始时的指定日期。 如果选择 **Recurring**，请输入夏令时开始时的月份、周、星期几和时间。 在 **From** 和 **To** 字段中输入相应信息。

Daylight Saving Offset	从下拉菜单中选择与协调世界时 (UTC) 之间的偏移。
Set Date and Time	选择要手动还是自动设置设备上的日期和时间。 如果选择 **Manual**，请在 **Enter Date and Time** 字段中输入日期和时间。
NTP Server	要使用默认 NTP 服务器，请单击 **Use Default** 按钮。 要使用特定 NTP 服务器，请单击 **User Defined NTP Server**，然后在两个可用字段中输入 NTP 服务器的完全合格域名或 IP 地址。

步骤 3 单击 **Save**。

备份和恢复系统

可以通过 **Administration > Backup / Restore Settings** 页面，备份自定义配置设置以供将来恢复或从以前的备份进行恢复。

当防火墙按配置方式工作时，可以备份配置以供将来恢复。在备份过程中，设置会保存为 PC 上的文件。可以从此文件恢复防火墙设置。

注意 在恢复操作过程中，请勿在操作完成之前尝试上线、关闭防火墙、关闭 PC 或使用防火墙。这大约需要一分钟。当测试指示灯熄灭时，多等待几秒，然后再使用防火墙。

备份配置设置

备份或恢复配置的步骤：

步骤 1 选择 **Administration > Backup/Restore Settings**。

步骤 2 选择要备份或清除的配置：

Startup configuration	选择此选项可下载启动配置。启动配置是设备使用的最新运行配置。 如果路由器启动配置丢失，请使用此页面将备份配置复制到启动配置，使以前的所有配置信息保持完整。 可以将启动配置下载到其他 RV130/RV130W 设备以进行方便部署。
Mirror configuration	如果设备在启动配置未进行更改的情况下运行 24 小时之后必须备份启动配置，请选择此选项。
Backup configuration	选择此选项可备份当前配置设置。

步骤 3 要基于所选配置选项下载备份文件，请单击 **Download**。

默认情况下，文件 （startup.cfg、 mirror.cfg 或 backup.cfg）会下载到默认 Downloads 文件夹中；例如， *C:\Documents and Settings\admin\My Documents\Downloads*。

步骤 4 要清除所选配置，请单击 **Clear**。

恢复配置设置

恢复以前保存的简档的步骤：

步骤 1 选择 **Administration** > **Backup/Restore Settings**。

步骤 2 在 Configuration Upload 字段中，选择要上传的配置 （**Startup Configuration** 或 **Backup Configuration**）。

步骤 3 单击 **Browse** 以查找文件。

步骤 4 选择文件，然后单击 **Open**。

步骤 5 单击 **Start to Upload**。

设备上传简档并使用其中包含的设置更新启动配置。设备随后重新启动并使用新配置。

复制配置设置

将启动配置复制到备份配置可确保具有备份副本，以防您忘记用户名和密码，被锁定在设备管理器外部。要返回设备管理器，请将设备重置为出厂默认设置。

备份简档保留在内存中，可用于将备份的配置信息复制到启动配置，这会恢复所有设置。

复制配置 （例如，将启动配置复制到备份配置）的步骤：

步骤 1 选择 **Administration** > **Backup/Restore Settings**。

步骤 2 在 **Copy** 字段中，从下拉菜单中选择源和目标配置。

步骤 3 单击 **Start to Copy**。

生成加密密钥

路由器允许生成加密密钥来保护备份文件。

生成加密密钥的步骤：

步骤 1 选择 **Administration** > **Backup/Restore Settings**。

步骤 2 单击 **Show Advanced Settings**。

步骤 3 在框中，输入用于生成密钥的种子短语。

步骤 4 单击 **Save**。

升级固件或更改语言

可以使用 **Administration** > **Firmware/Language Upgrade** 页面升级到较新版本的固件或更改路由器的语言。

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。

升级固件

使用较新版本的固件升级路由器的步骤：

步骤 1 选择 **Administration** > **Firmware/Language Upgrade**。

步骤 2 （可选）单击 **Download** 以下载最新版本的固件。

步骤 3 在 **File Type** 字段中，单击 **Firmware Image** 按钮。

步骤 4 单击 **Browse** 以查找并选择下载的固件。

步骤 5 （可选）要在固件升级之后将设备重置为默认出厂设置，请选中 **Reset all configurations/settings to factory defaults**。

注意 将设备重置为默认出厂设置可擦除所有配置设置。

步骤 6 单击 **Start Upgrade**。

验证了新固件映像之后，新映像会写入闪存，路由器会使用新固件自动重新启动。

步骤 7 选择 **Status** > **System Summary** 以确保路由器安装了新固件版本。

更改语言

在设备上更改语言的步骤：

步骤 1 选择 **Administration** > **Firmware/Language Upgrade**。

步骤 2 在 **File Type** 字段中，单击 **Language File** 按钮。

步骤 3 单击 **Browse** 以查找并选择语言文件。

步骤 4 （可选）要将设备配置参数重置为出厂默认值，请选中 **Reset all configuration/settings to factory defaults**。

步骤 5 单击 **Start Upgrade**。

重新启动设备

重新启动路由器的步骤：

步骤 1 选择 **Administration** > **Reboot**。

步骤 2 单击 **Reboot**。

恢复出厂默认设置

注意 在恢复操作过程中，请勿在操作完成之前尝试上线、关闭路由器、关闭 PC 或使用路由器。这大约需要一分钟。当测试指示灯熄灭时，多等待几秒，然后再使用路由器。

将出厂默认设置恢复到路由器的步骤：

步骤 1 选择 **Administration** > **Restore Factory Defaults**。

步骤 2 单击 **Default**。

9

Web 过滤

Web 过滤是路由器的一项功能，可用于管理对不当网站的访问。此功能可以筛选客户端的 Web 访问请求，决定是允许还是拒绝访问该网站，确保已经受到安全保护的网络更加安全，并提高工作场所的工作效率。

对于一般网络安全、物联网，以及/或者需要在特定部门的定制网络中实施的规则，管理员可能有一套指导原则。管理员可以创建自定义的计划规则，并将这些规则绑定到例外列表，从而在特定时间允许特定用户访问特定网站，或实现类似目的。

配置 Web 过滤

本节介绍如何在路由器中配置 Web 过滤功能，并着重说明此功能的重要性。要在路由器上启用并配置 Web 过滤功能，请按照以下步骤操作：

步骤 1 单击 **Web 过滤**。

步骤 2 在 “ Web 过滤 ” 部分，从下列选项中选择一项：

- **始终开启** - 始终启用 Web 过滤功能
- **计划** - 制定计划来决定何时启用 Web 过滤功能
- **始终关闭** - 禁用 Web 过滤功能

注 默认情况下，Web 过滤功能设置为 “ 始终关闭 ” 。

步骤 3 在 “ Web 信誉 ” 部分，选中**启用**可根据所选的过滤类别来启用过滤功能。

步骤 4 单击各个类别，然后从下列选项中选择一项，以管理和应用过滤器。

- **低** - 可从 “ 成人内容 ” 和 “ 安全 ” 类别中进行选择。选择和选取可用选项，对您的过滤器进行自定义。
- **中** - 可从 “ 成人内容 ” 、 “ 非法/可疑 ” 和 “ 安全 ” 类别中进行选择。选择和选取可用选项，对您的过滤器进行自定义。

- **高** - 可从“成人内容”、“商业/投资”、“娱乐”、“非法/可疑”、“IT 资源”、“时尚/文化”和“安全”类别中进行选择。选择和选取可用选项，对您的过滤器进行自定义。
- **自定义** - 无默认设置，允许自定义 Web 过滤。

步骤 5 单击**保存**和**后退**，返回“过滤”页面继续进行设置。

步骤 6 选中**启用 HTTPS 过滤**可根据网站的 IP 地址（而非 URL）过滤内容。采用安全 HTTP (HTTPS) 的网站将可以访问。如果需要将使用安全 URL 的网站作为拦截对象，请勿选中**启用 HTTPS 过滤**。

注 HTTPS 过滤的依据是 Web 服务器的 IP 地址，而非 URL，因为 URL 是加密的。多个网站使用同一个 Web 服务器 IP 地址的情形十分常见。在这种情况下，如果某个 IP 地址有多个关联的网站类别，路由器不会对相关页面进行拦截。但是，如果该 IP 地址托管了成人内容，或者该 IP 地址与已知的恶意软件托管或分发网站相关联，路由器会拦截相关页面。

步骤 7 如果在设置 Web 过滤选项时选择**计划**，屏幕将显示“计划表”。在“计划表”下，单击**添加行**创建一项计划规则或计划策略。

步骤 8 在“计划表”的“名称和描述”字段中，输入名称和描述。

步骤 9 然后选择每周在哪天或哪几天启用该规则或策略，以便在指定日期启用过滤功能。

步骤 10 接下来，使用 24 小时格式输入规则生效的时间。

步骤 11 最后，单击**激活**启用计划规则。

注 系统对所要执行的规则没有数量上的限制。

步骤 12 单击**保存**。

步骤 13 （可选）创建过滤过程中使用的允许、拒绝或排除网站/内容列表。从下列选项中选择一种类型：

- **白名单** - 单击**添加行**，然后从下拉列表中选择**域名**或**关键字**。根据所选内容，输入用于识别此策略的值。
- **黑名单** - 单击**添加行**，然后从下拉列表中选择**域名**或**关键字**。根据所选内容，输入用于识别此策略的值。
- **排除列表** - 单击**添加行**，然后从下拉列表中选择**域名**或**关键字**。根据所选内容，输入用于识别此策略的值。

步骤 14 如需编辑或删除 Web 过滤策略，请从列表中选择相关策略，然后单击**编辑**或**删除**。

步骤 15 单击**保存**。

A

快速索引

支持	
思科支持社区	www.cisco.com/go/smallbizsupport
思科支持和资源	www.cisco.com/go/smallbizhelp
电话支持联系人名单	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
思科固件下载	www.cisco.com/cisco/software/navigator.html?i=!ch 选择一个链接，以下载所需固件。无需登录。
思科开源请求	www.cisco.com/go/smallbiz_opensource_request
思科合作伙伴中心 （需要合作伙伴登录）	www.cisco.com/web/partners/sell/smb
产品文档	
思科 RV130/RV130W 边缘路由器	www.cisco.com/en/US/products/ps9923/tsd_products_support_series_home.html

有关欧洲批次 26 的相关测试结果，请查看此网页：www.cisco.com/go/eu-lot26-results。