370111

管理指南

思科 **Small Business**
RV320/RV325 千兆双 WAN 口 VPN 路由器

目录

目录

目录

1

使用入门

感谢您选择思科 RV320/RV325 千兆双 WAN 口 VPN 路由器。本章内容有助于您开始使用设备。

使用 **Getting Started** （使用入门）窗口

对于许多小型企业而言，默认设置已足够使用。根据网络需求，可能需要修改设置；互联网服务提供商 (ISP) 也可能要求修改设置。要使用网页界面，您的 PC 上需安装 Internet Explorer （版本 6 及更高版本）、 Firefox 或 Safari （针对 Mac）。

启动网页界面的步骤：

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**。浏览器可能会发出该网站不信任的警告。继续访问此网站。

步骤 4 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 **Login** （登录）。此时将显示 **System Summary** （系统摘要）页面。查看 **Port Activity** （端口活动）来了解是否启用了 WAN 连接。如果未启用，请继续执行下一个步骤。

步骤 6 要使用设置向导配置互联网连接，请单击 System Summary 页面上的 **Setup Wizard** （设置向导）。或者，单击导航树中的 **Wizard** （向导），然后单击 Basic Setup （基本设置）部分中的 **Launch Now** （现在启动）。按照屏幕上的说明进行操作。

如果 Web 浏览器显示关于弹出窗口的警告，请允许显示被阻止的内容。

步骤 7 要配置其他设置，请使用导航树中的链路。

故障排除提示

如果连接到互联网或基于 Web 的网页界面时出现问题，请执行以下操作：

- 确保 Web 浏览器未设置为 Work Offline （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，PC 也可以为其指定 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 Wizard 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。随后，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 调制解调器设置为桥接模式。

用户界面功能特性

用户界面旨在方便您设置和管理设备。

导航

网页界面的主要模块在左侧导航窗格中以按钮形式表示。单击按钮可查看更多选项。单击选项可打开页面。

弹出窗口

单击某些链路和按钮会启动弹出窗口，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，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，请单击网页界面右上角附近的 **Help** （帮助）。如果 Web 浏览器显示关于弹出窗口的警告，请允许显示被阻止的内容。

退出

要退出网页界面，请单击网页界面右上角附近的 **Logout** （退出）。系统将显示 **Login** 页面。

2

系统摘要

System Summary 页面上显示有关设备的连接、状态、设置和日志的当前信息。

系统信息

系统信息描述：

- **Serial Number** （序列号） - 设备的序列号。
- **Firmware version** （固件版本） - 所安装固件的版本号。
- **PID VID** - 硬件的版本号。
- **MD5 Checksum** （MD5 校验和） - 用于文件验证的值。
- **LAN IPv4/ Subnet Mask** （LAN IPv4/ 子网掩码） - 设备的 IPv4 管理 IP 地址和子网掩码。
- **LAN IPv6/ Prefix** （LAN IPv6/ 前缀） - IPv6 管理 IP 地址和前缀。
- **Working Mode** （工作模式） - 控制设备与 WAN 连接有关的行为。当设备承载互联网 WAN 连接时，选择 Gateway Mode （网关模式）。当设备位于没有 WAN 连接的网络上或使用其他设备建立 WAN 连接时，选择 Router Mode （路由器模式）。要更改此参数，请单击 **Working Mode** 以显示 Advanced Routing （高级路由）窗口。
- **LAN** - IPv4 管理 IP 地址。如果已在设置网络页面上启用了 Dual-Stack IP （双堆叠 IP），则 IPv6 地址和前缀长度也会显示。
- **System Up time** （系统运行时间） - 设备处于活动状态的时间，以天数、小时数和分钟数表示。

配置 （向导）

若要使用互联网连接设置向导并在设置流程中获得提示，请单击 **Setup Wizard** 以启动向导。

端口活动

Port Activity 部分显示端口接口并指示每个端口的状态：

- **Port ID** （端口 ID） - 端口标签。
- **Interface** （接口） - 接口类型：LAN、 WAN 或 DMZ。多个 WAN 接口由数字表示，例如 WAN1 或 WAN2。
- **Status** （状态） - 端口的状态：Disabled （已禁用）（红色）、 Enabled （已启用）（黑色）或 Connected （已连接）（绿色）。状态值为超链路形式。单击该链路可打开 **Port Information** （端口信息）窗口。

要显示有关当前链路活动的详情，请单击该端口的 **Status** 条目。

端口信息 （详细信息）

Port Information 窗口显示有关端口上的接口和当前活动的详情：

- **Type** （类型） - 端口类型：10BASE-T 或 100BASE-TX 或 1000BASE-T。
- **Interface** - 接口类型：LAN、 DMZ 或 WAN。
- **Link Status** （链路状态） - 链路的状态：Up （连接）或 Down （中断）。
- **Port Activity** - 端口上的当前活动：Port Enabled （端口已启用）、 Port Disabled （端口已禁用）或 Port Connected （端口已连接）。
- **Priority** （优先级） - 端口数据优先级：High （高）或 Normal （普通）。
- **Speed Status** （速度状态） - 端口速度：10 Mbps 至 1000 Mbps。
- **Duplex Status** （双工状态） - 双工模式：Half （半）或 Full （全）。
- **Auto negotiation** （自动协商） - 启用自动协商后，即自动协商参数的状态为 On （打开）时，系统会检测双工模式。如果连接需要交叉，则系统会自动选择 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。

- **VLAN** - 此端口的 VLAN ID。有两个预定义的 VLAN：25 和 100。 VLAN 25 可用于访客进行 VLAN 访问， VLAN 100 可用于语音流量。默认情况下，不启用 VLAN 25 和 VLAN 100。
- **Receive Packet Count** （接收数据包计数） - 在此端口上接收的数据包数量。
- **Receive Packet Byte Count** （接收数据包字节计数） - 在此端口上接收的字节数。
- **Transmit Packet Count** （传输数据包计数） - 由此端口传输的数据包数量。
- **Transmit Packet Byte Count** （传输数据包字节计数） - 由此端口传输的字节数。
- **Packet Error Count** （数据包错误计数） - 数据包错误总数。

IPv4 和 IPv6

IPv4 或 IPv6 部分显示每个 WAN 端口的统计信息。（在设置网络页面上启用 Dual-Stack IP 后，即可使用 IPv6 选项卡。）

WAN 信息

此部分提供了以下 WAN 信息：

- **IP Address** （IP 地址） - 此接口的公共 IP 地址。
- **Default Gateway** （默认网关） - 此接口的默认网关。
- **DNS** - 此接口的 DNS 服务器的 IP 地址。
- **Dynamic DNS** （动态 DNS） - 此端口的 DDNS 设置：Disabled 或 Enabled。
- **Release** （释放）和 **Renew** （更新） - 如果该端口设置为从服务器获取 IP 地址，则会显示这些按钮。单击 **Release** 可释放 IP 地址。单击 **Renew** 可更新租用时间或获取一个新的 IP 地址。
- **Connect** （连接）和 **Disconnect** （断开连接） - 如果端口设置为 PPPoE 或 PPTP，则将显示这些按钮。单击 **Disconnect** 可断开与互联网服务的连接。单击 **Connect** 可建立连接。

DMZ 信息

此部分提供了以下 DMZ 信息：

- **IP Address** - 此接口的当前公共 IP 地址。
- **DMZ Host** （DMZ 主机） - DMZ 主机的专用 IP 地址。默认为 **Disabled**。

安全状态

此部分显示安全功能的状态：

- **SPI**（数据包状态检测）- 防火墙的状态：On（打开）（绿色）或 Off（关闭）（红色）。跟踪数据包在网络上进行传输时网络连接（例如 TCP 流和 UDP 通信）的状态。防火墙区分不同连接类型的合法数据包。只有符合已知活动连接的数据包才允许通过防火墙；其他数据包则被拒绝。
- **DoS**（拒绝服务）- DoS 筛选器的状态：On（绿色）或 Off（红色）。DoS 攻击是指企图使目标用户无法使用机器或网络资源。
- **Block WAN Request**（阻止 WAN 请求）- 通过*隐藏*互联网设备中的网络端口并阻止其他互联网用户对网络执行 Ping 操作或检测网络，使得外部用户难以顺利进入网络。状态为 On（绿色）或 Off（红色）。
- **Remote Management**（远程管理）- 表示是否允许通过远程连接管理设备。On（绿色）表示允许远程管理。Off（红色）表示不允许远程管理。
- **Access Rule**（访问规则）- 已设置的访问规则的数量。

要显示有关安全功能的详情，请单击该功能的标签。

VPN 设置状态

此部分显示 VPN 隧道的状态：

- **VPN Tunnel(s) Used**（使用的 VPN 隧道）- 使用中的 VPN 隧道。
- **VPN Tunnel(s) Available**（可用的 VPN 隧道）- 可用的 VPN 隧道。
- **Easy VPN Tunnel(s) Used**（使用的简单 VPN 隧道）- 使用中的简单 VPN 隧道。
- **Easy VPN Tunnel(s) Available**（可用的简单 VPN 隧道）- 可用的简单 VPN 隧道。
- **PPTP Tunnel(s) Used**（使用的 PPTP 隧道）- 使用中的点对点隧道协议 (PPTP) 隧道。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) 隧道封装 PPP 数据包。
- **PPTP Tunnel(s) Available**（可用的 PPTP 隧道）- 可用的 PPTP 隧道。

SSL VPN 状态

SSL VPN 可以从 IPsec 与网络地址转换 (NAT) 和防火墙规则冲突的位置进行连接：

- **SSL VPN Tunnel(s) Used**（使用的 SSL VPN 隧道）- 使用中的 SSL VPN 隧道。
- **SSL VPN Tunnel(s) Available**（可用的 SSL VPN 隧道）- 剩余的可用的 SSL VPN 隧道。

日志设置状态

此部分显示日志的状态：

- **Syslog Server** （系统日志服务器） - 系统日志的状态：On （绿色）或 Off （红色）。
- **E-mail Log** （电子邮件日志） - 电子邮件日志的状态：On （绿色）或 Off （红色）。

3

设置

使用 Setup（设置）> Network（网络）页面设置 LAN、WAN（互联网）、DMZ 等。

设置网络

要打开 Network 页面，请单击 Setup > Network。

某些 ISP 要求您指定主机名和域名来标识设备。默认值已提供，但是可根据需要进行更改。

- **Host Name** （主机名） - 保留默认设置或输入 ISP 指定的主机名。
- **Domain Name** （域名） - 保留默认设置或输入 ISP 指定的域名。

IP 模式

选择要在网络上使用的寻址类型：

- **IPv4 Only** （仅 IPv4） - 仅支持 IPv4 寻址。
- **Dual-Stack IP** - 支持 IPv4 和 IPv6 寻址。保存参数后，可以为 LAN、WAN 和 DMZ 网络配置 IPv4 和 IPv6 地址。

添加或编辑 **IPv4** 网络

默认情况下，配置一个 IPv4 LAN 子网，即 192.168.1.1。对于大多数小型企业而言，一个子网通常足以满足其需求。如果 LAN 设备源 IP 地址位于未获得特别许可的子网上，则防火墙会拒绝访问。您可以允许来自其他子网的流量并将此设备用作为网络提供互联网连接的边缘路由器。

步骤 1 单击 **IPv4** 选项卡可显示 Multiple Subnet （多个子网）表。

步骤 2 要添加子网，请单击 **Add** （添加）。 IP Address 和 Subnet Mask （子网掩码）字段会显示在列中。单击 **Save** （保存）后，可以将子网编辑为 VLAN 的一部分、通过 DHCP 服务器管理 IP 地址，或设置 TFTP 服务器参数。

步骤 3 在设备的 **IP Address** 和 **Subnet Mask** 中输入相应的值。

步骤 4 单击 **Save** 保存更改，或单击 **Cancel** （取消）撤消更改。

要编辑子网，请选择要修改的 IPv4 子网并单击 **Edit** （编辑）。修改子网参数的流程将在 **DHCP** 设置一节中予以介绍。

编辑 **IPv6** 地址前缀

如果 IP Mode （IP 模式）启用了 Dual-Stack IP，则可以配置 IPv6 前缀。

要配置 IPv6 前缀，请单击 **IPv6** 选项卡，选择 IPv6 前缀，然后单击 **Edit**。默认 IP 地址为 fc00::1，默认前缀长度为 7。仅当在 **IP** 模式表中启用了 **Dual-Stack IP** 后才能使用 IPv6 选项卡。系统将显示 **DHCP** 设置窗口。

WAN1 或 WAN2 端口设置

WAN Setting （WAN 设置）表中显示了接口 （例如 USB1、 WAN1 或 WAN2）和连接类型。可以修改接口的设置。

注 如果运行的是 IPv6，请选择 **IPv6** 选项卡，然后选择要配置的 WAN 接口。否则，IPv6 参数不会显示在 **WAN Connections Settings** （WAN 连接设置）窗口中。

要配置 **WAN Connection Settings**，请选择一个 WAN 接口并单击 **Edit**。系统将显示 **WAN Connection Settings**。

从菜单中选择 **WAN Connection Type** （WAN 连接类型）并修改以下内容中所述的相关参数：

Obtain an IP Automatically （自动获取 **IP**）选项

如果 ISP 为设备动态分配了一个 IP 地址，请选择此选项。（大多数电缆调制解调器用户都使用此连接类型。）ISP 为设备分配此端口的 IP 地址，包括 DNS 服务器 IP 地址。

要指定一个 DNS 服务器，请选中 **Use the Following DNS Server Addresses** （使用下面的 DNS 服务器地址）并输入 **DNS Server 1** （DNS 服务器 1）的 IP 地址。作为可选操作，可以输入第二个 DNS 服务器。系统将使用第一个可用的 DNS 服务器。

要自动设置最大传输单位 (**MTU**) 大小，请选择 **Auto** （自动）。否则，要手动设置 **MTU** 大小，请选择 **Manual** （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。）

要配置 IPv6 参数，请选中 **Enable**。选中该选项后，将可以通过选定接口处理 DHCPv6 客户端流程和前缀授权请求。当 ISP 能够使用 DHCPv6 发送 LAN 前缀时，请使用此选项。如果 ISP 不支持此选项，请手动配置 LAN 前缀：

注 启用 DHCP-PD 后，系统会禁用手动 LAN IPv6 寻址。禁用 DHCP-PD 后，系统会启用手动 LAN IPv6 寻址。

- **LAN IPv6 Address** （LAN IPv6 地址） - ISP 为 LAN 设备分配的全局 IPv6 前缀 （如适用）。（有关详情，请与 ISP 联系。）
- **Prefix Length** （前缀长度） - IPv6 前缀的长度：IPv6 网络 （子网）由地址的初始位 （称为前缀）标识。对于 IPv6 地址，网络中的所有主机都具有相同的初始位。输入网络地址中常见初始位的位数。默认前缀长度为 64。
- **LAN Prefix Assignment** （LAN 前缀分配）：
  - **Without any action** （不执行任何操作） - 不为 LAN 端 PC 提供无状态或有状态的 IPv6 地址。
  - **Configure to RA automatically** （自动配置到 RA） - 为 LAN 端 PC 提供*无状态*的 IPv6 地址。
  - **Configure to DHCPv6 automatically** （自动配置到 DHCPv6） - 为 LAN 端 PC 提供*有状态*的 IPv6 地址。
  - **Configure to RA and DHCPv6 automatically** （自动配置到 RA 和 DHCPv6） - 为 LAN 端 PC 提供无状态和有状态的 IPv6 地址。

Static IP （静态 **IP**）选项

如果 ISP 为帐户分配了永久 IP 地址，则选择此选项。输入 ISP 提供的设置：

- **Specify WAN IP Address**（指定 WAN IP 地址）- ISP 为帐户分配的 IP 地址。
- **Subnet Mask (IPv4)** （子网掩码 (IPv4)） - 子网掩码。
- **Default Gateway Address** （默认网关地址） - 默认网关的 IP 地址。

要指定一个 DNS 服务器，请输入 **DNS Server 1** 的 IP 地址。作为可选操作，可以输入第二个 DNS 服务器。系统将使用第一个可用的 DNS 服务器。

要自动设置最大传输单位 (**MTU**) 大小，请选择 **Auto**。否则，要手动设置 **MTU** 大小，请选择 **Manual** 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。）

配置 IPv6 参数的步骤：

- **LAN IPv6 Address -** ISP 为 LAN 设备分配的全局 IPv6 前缀 （如适用）。（有关详情，请与 ISP 联系。）
- **Prefix Length -** IPv6 前缀的长度：IPv6 网络 （子网）由地址的初始位 （称为前缀）标识。对于 IPv6 地址，网络中的所有主机都具有相同的初始位。输入网络地址中常见初始位的位数。默认前缀长度为 64。
- **LAN Prefix Assignment**
  - **Without any action -** 不为 LAN 端 PC 提供无状态或有状态的 IPv6 地址。
  - **Configure to RA automatically -** 为 LAN 端 PC 提供*无状态*的 IPv6 地址。
  - **Configure to DHCPv6 automatically -** 为 LAN 端 PC 提供*有状态*的 IPv6 地址。
  - **Configure to RA and DHCPv6 automatically -** 为 LAN 端 PC 提供无状态和有状态的 IPv6 地址。

PPPoE 选项

如果 ISP 使用 PPPoE （基于以太网的点对点协议）建立互联网连接 （DSL 线路的典型连接方式），则选择此选项。然后，输入 ISP 提供的设置：

- **Username** （用户名）和 **Password** （密码） **-** ISP 帐户的用户名和密码。每个条目最多可包含 255 个字符。
- **Service Name** （服务名称） **-** ISP 提供的一组服务，用服务名称标识。
- **Connection Timers** （连接定时器） **-** 连续一段时间处于非活动状态后，断开连接。
  - **Connect on Demand** （按需连接） **-** 启用此功能后，设备会自动建立连接。如果启用了此功能，请输入 **Max Idle Time** （最长空闲时间），即连接断开前，连接可以保持非活动状态的分钟数。默认最长空闲时间为 5 分钟。
  - **Keep Alive** （保持活动） **-** 确保路由器始终连接到互联网。选择此功能后，路由器将通过定期发送一些数据包来保持连接处于活动状态。即使链路长时间处于闲置状态，此选项也可使连接无限期处于活动状态。如果启用了此功能，请同时在 **Redial Period** （重拨周期）中输入值，以指定路由器验证互联网连接的频率。默认周期为 30 秒。
- **Use the Following DNS Server Addresses -** 允许从 DNS 服务器中获取连接信息。

- **DNS Server 1** 和 **DNS Server 2** （DNS 服务器 2） - DNS 服务器的 IP 地址。作为可选操作，可以输入第二个 DNS 服务器。系统将使用第一个可用的 DNS 服务器。
- **MTU** - 最大传输单位 (**MTU**) 大小。选择 **Auto** 可自动设置大小。否则，要手动设置 **MTU** 大小，请选择 **Manual** 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。）

要配置 IPv6 参数，请选中 **Enable**。选中该选项后，将可以通过选定接口处理 DHCPv6 客户端流程和前缀授权请求。当 ISP 能够使用 DHCPv6 发送 LAN 前缀时，请使用此选项。如果 ISP 不支持此选项，请手动配置 LAN 前缀：

注 启用 DHCP-PD 后，系统会禁用手动 LAN IPv6 寻址。禁用 DHCP-PD 后，系统会启用手动 LAN IPv6 寻址。

- **LAN IPv6 Address** - ISP 为 LAN 设备分配的全局 IPv6 前缀 （如适用）。（有关详情，请与 ISP 联系。）
- **Prefix Length** - IPv6 前缀的长度。 IPv6 网络 （子网）由地址的初始位 （称为前缀）标识。对于 IPv6 地址，网络中的所有主机都具有相同的初始位。输入网络地址中常见初始位的位数。默认前缀长度为 64。
- **LAN Prefix Assignment**：
  - **Without any action** - 不为 LAN 端 PC 提供无状态或有状态的 IPv6 地址。
  - **Configure to RA automatically** - 为 LAN 端 PC 提供*无状态*的 IPv6 地址。
  - **Configure to DHCPv6 automatically** - 为 LAN 端 PC 提供*有状态*的 IPv6 地址。
  - **Configure to RA and DHCPv6 automatically** - 为 LAN 端 PC 提供无状态和有状态的 IPv6 地址。

PPTP (IPv4) 选项

如果 ISP 有要求，则选择此选项。点对点隧道协议 (PPTP) 是一种用于欧洲和以色列的服务。

- **Specify WAN IP Address** - ISP 为帐户分配的 IP 地址。
- **Subnet Mask (IPv4)** - 为帐户分配的子网掩码。
- **Default Gateway Address** - 默认网关的 IP 地址。
- **Username** 和 **Password** - ISP 帐户的用户名和密码。最多可包含 60 个字符。

- **Connection Timers -** 连续一段时间处于非活动状态后，断开连接。
  - **Connect on Demand -** 启用此功能后，设备会自动建立连接。如果启用了此功能，请输入 **Max Idle Time**，即连接断开前，连接可以保持非活动状态的分钟数。默认最长空闲时间为 5 分钟。
  - **Keep Alive -** 确保路由器始终连接到互联网。选择此功能后，路由器将通过定期发送一些数据包来保持连接处于活动状态。即使链路长时间处于闲置状态，此选项也可使连接无限期处于活动状态。如果启用了此功能，请同时在 **Redial Period** 中输入值，以指定路由器验证互联网连接的频率。默认周期为 30 秒。
- **MTU -** 最大传输单位 (**MTU**) 大小。选择 **Auto** 可自动设置大小。否则，要手动设置 **MTU** 大小，请选择 **Manual** 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。）

Transparent Bridge (IPv4) （透明网桥 **(IPv4)**）选项

如果希望使用此路由器连接两个网络区段，则选择此选项。只有一个 WAN 接口可以设置为透明网桥。

- **Specify WAN IP Address -** ISP 为帐户分配的外部 IP 地址。
- **Subnet Mask -** ISP 指定的子网掩码。
- **Default Gateway Address -** 默认网关的 IP 地址。
- **DNS Server 1** 和 **DNS Server 2 -** DNS 服务器的 IP 地址。作为可选操作，可以输入第二个 DNS 服务器。系统将使用第一个可用的 DNS 服务器。
- **Internal LAN IP Range**（内部 LAN IP 范围）**-** 桥接的内部 LAN IP 范围。透明网桥的 WAN 和 LAN 必须在同一子网中。
- **MTU -** 最大传输单位 (**MTU**) 大小。选择 **Auto** 可自动设置大小。否则，要手动设置 **MTU** 大小，请选择 **Manual** 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。）

Stateless Address Autoconfiguration (IPv6) （无状态地址自动配置 **(IPv6)**）选项

如果 ISP 使用 IPv6 Router Solicitations （路由器请求）和 Router Advertisements （路由器通告），则选择此选项，网络上的主机可以了解它们所连接到的网络。之后，它们可以在该网络上自动配置主机 ID。

要指定一个 DNS 服务器，请输入 **DNS Server 1** 的 IP 地址。作为可选操作，可以输入第二个 DNS 服务器。系统将使用第一个可用的 DNS 服务器。

要自动设置最大传输单位 (**MTU**) 大小，请选择 **Auto**。否则，要手动设置 **MTU** 大小，请选择 **Manual** 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。）

配置 IPv6 参数的步骤：

- **LAN IPv6 Address** - ISP 为 LAN 设备分配的全局 IPv6 前缀 （如适用）。（有关详情，请与 ISP 联系。）
- **Prefix Length** - IPv6 前缀的长度：IPv6 网络 （子网）由地址的初始位 （称为前缀）标识。对于 IPv6 地址，网络中的所有主机都具有相同的初始位。输入网络地址中常见初始位的位数。默认前缀长度为 64。
- **LAN Prefix Assignment**：
  - **Without any action** - 不为 LAN 端 PC 提供无状态或有状态的 IPv6 地址。
  - **Configure to RA automatically** - 为 LAN 端 PC 提供*无状态*的 IPv6 地址。
  - **Configure to DHCPv6 automatically** - 为 LAN 端 PC 提供*有状态*的 IPv6 地址。
  - **Configure to RA and DHCPv6 automatically** - 为 LAN 端 PC 提供无状态和有状态的 IPv6 地址。

IPv6 in IPv4 Tunnel (IPv6) （**IPv4** 隧道中的 **IPv6 (IPv6)**）选项

如果 ISP 使用 IPv6 in IPv4 Tunnel 建立互联网连接，则选择此选项。

必须输入 IPv4 **Static IP** （静态 **IP**）选项地址。然后，输入 ISP 提供的设置：

- **Local IPv6 Address** （本地 IPv6 地址） - ISP 帐户的本地 IPv6 地址。
- **Remote IPv4 Address** （远程 IPv4 地址） - ISP 帐户的远程 IPv4 地址。
- **Remote IPv6 Address** （远程 IPv6 地址） - ISP 帐户的远程 IPv6 地址。
- **DNS Server 1** 和 **DNS Server 2** - DNS 服务器的 IP 地址。作为可选操作，可以输入第二个 DNS 服务器。系统将使用第一个可用的 DNS 服务器。
- **LAN IPv6 Address** - ISP 为 LAN 设备分配的全局 IPv6 前缀 （如适用）。（有关详情，请与 ISP 联系。）
- **Prefix Length** - IPv6 前缀的长度：IPv6 网络 （子网）由地址的初始位 （称为前缀）标识。对于 IPv6 地址，网络中的所有主机都具有相同的初始位。输入网络地址中常见初始位的位数。默认前缀长度为 64。
- **LAN Prefix Assignment**
  - **Without any action** - 不为 LAN 端 PC 提供无状态或有状态的 IPv6 地址。
  - **Configure to RA automatically** - 为 LAN 端 PC 提供*无状态*的 IPv6 地址。
  - **Configure to DHCPv6 automatically** - 为 LAN 端 PC 提供*有状态*的 IPv6 地址。
  - **Configure to RA and DHCPv6 automatically** - 为 LAN 端 PC 提供无状态和有状态的 IPv6 地址。

6to4 Tunnel (IPv6) （**6to4** 隧道 **(IPv6)**）选项

选择此选项可跨两个独立的 IPv6 网络在 IPv4 网络 （或真实 IPv4 互联网连接）中建立自动隧道。输入以下参数：

Relay IPv4 Address （中继 IPv4 地址） - 允许 6to4 主机与本征 IPv6 互联网进行通信。必须有一个 IPv6 默认网关设置为 6to4 地址，该地址包含 6to4 中继路由器的 IPv4 地址。为了避免需要用户手动设置此地址，系统已分配了 **192.88.99.1** 的任播地址，可将数据包发送至 6to4 中继路由器。

- **DNS Server 1** 和 **DNS Server 2** - DNS 服务器的 IP 地址。作为可选操作，可以输入第二个 DNS 服务器。系统将使用第一个可用的 DNS 服务器。
- **LAN IPv6 Address** - ISP 为 LAN 设备分配的全局 IPv6 前缀 （如适用）。（有关详情，请与 ISP 联系。）
- **Prefix Length** - IPv6 前缀的长度。 IPv6 网络 （子网）由地址的初始位 （称为前缀）标识。对于 IPv6 地址，网络中的所有主机都具有相同的初始位。输入网络地址中常见初始位的位数。默认前缀长度为 64。
- **LAN Prefix Assignment**
  - **Without any action** - 不为 LAN 端 PC 提供无状态或有状态的 IPv6 地址。
  - **Configure to RA automatically** - 为 LAN 端 PC 提供*无状态*的 IPv6 地址。
  - **Configure to DHCPv6 automatically** - 为 LAN 端 PC 提供*有状态*的 IPv6 地址。
  - **Configure to RA and DHCPv6 automatically** - 为 LAN 端 PC 提供无状态和有状态的 IPv6 地址。

IPv6 Rapid Deployment (6rd) Tunnel (IPv6) （**IPv6** 快速部署 **(6rd)** 隧道 **(IPv6)**）选项

如果 ISP 使用 6rd Tunnel (IPv6 Rapid Deployment) 建立互联网连接，则选择此选项。输入 ISP 提供的设置。

- **6rd Configuration Mode** （6rd 配置模式）：
  - **Manual** - 根据 ISP 提供的信息，手动设置 6rd Prefix （6rd 前缀）、 Relay IPv4 Address 和 IPv4 Mask Length （IPv4 掩码长度）。
  - **Auto (DHCP)** - 使用 DHCP （选项 212）获取 6rd Prefix、 Relay IPv4 Address 和 IPv4 Mask Length。
- **6rd Prefix** - ISP 帐户的 6rd 前缀。
- **Relay IPv4 Address** - ISP 帐户的中继 IPv4 地址。
- **IPv4 Mask Length** - ISP 帐户的 6rd IPv4 子网掩码长度。（通常此值为 0。）

- **DNS Server 1** 和 **DNS Server 2** - DNS 服务器的 IP 地址。作为可选操作，可以输入第二个 DNS 服务器。系统将使用第一个可用的 DNS 服务器。
- **LAN IPv6 Address** - ISP 为 LAN 设备分配的全局 IPv6 前缀 （如适用）。（有关详情，请与 ISP 联系。）
- **Prefix Length** - IPv6 前缀的长度。 IPv6 网络 （子网）由地址的初始位 （称为前缀）标识。对于 IPv6 地址，网络中的所有主机都具有相同的初始位。输入网络地址中常见初始位的位数。默认前缀长度为 64。
- **LAN Prefix Assignment**
  - **Without any action** - 不为 LAN 端 PC 提供无状态或有状态的 IPv6 地址。
  - **Configure to RA automatically** - 为 LAN 端 PC 提供*无状态*的 IPv6 地址。
  - **Configure to DHCPv6 automatically** - 为 LAN 端 PC 提供*有状态*的 IPv6 地址。
  - **Configure to RA and DHCPv6 automatically** - 为 LAN 端 PC 提供无状态和有状态的 IPv6 地址。

USB1 或 USB2 端口设置

USB 端口配置管理此设备和 USB 装置之间的连接。它还管理 WAN 端口故障切换（冗余）。某些 USB 装置自动配置凭证。其他装置 （例如 Verizon UML290VW 4G 装置）需要手动配置。有关详情，请参阅有关装置的制造商文档。

3G/4G 连接

要建立 3G 或 4G 连接，请输入下列信息：

- **Pin Code** （Pin 码）和 **Confirm Pin Code** （确认 Pin 码） - 与 SIM 卡相关联的 PIN 码。只有 GSM SIM 卡才显示此字段。
- **Access Point Name** （接入点名称） - 移动设备连接到的互联网网络。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** （拨号） - 移动网络服务提供商提供的用于连接互联网的号码。
- **Username** 和 **Password** - 移动网络服务提供商提供的用户名和密码。
- **Enable DNS** （启用 DNS） - 选中该框以启用 DNS。
- **DNS Server (Required)** （DNS 服务器 （必填））和 **DNS Server (Optional)** （DNS 服务器 （可选）） - DNS 服务器的 IP 地址。作为可选操作，可以输入第二个 DNS 服务器。系统将使用第一个可用的 DNS 服务器。

- **MTU** - 最大传输单位 (**MTU**) 大小。选择 **Auto** 可自动设置大小。否则，要手动设置 **MTU** 大小，请选择 **Manual** 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。）

设置故障切换和恢复

虽然以太网和移动网络链路都可能可用，但是一次只能使用一个连接建立 WAN 链路。无论何时某个 WAN 连接中断，设备都会尝试在其他接口上建立另一个连接。此功能称为 *Failover （故障切换）*。当主要的 WAN 连接恢复后，连接将恢复至该路径并放弃备份连接。此功能称为 *Recovery （恢复）*。

步骤 1 要显示 Failover & Recovery 窗口，请单击 **Setup** > **Network**。

步骤 2 选择一个 USB 端口，然后单击 **Edit**。系统将显示 Network 窗口。

步骤 3 单击 **USB Failover** （USB 故障切换）选项卡，输入以下信息：

- **Operational Mode** （运行模式)- 当以太网 WAN 链路关闭时，设备会尝试在 USB 接口上建立移动网络链路。配置故障切换行为：
  - (3G/4G) Failover Hot Standby（故障切换热备份）- 丢失的以太网 WAN 端口连接通过 3G/4G USB 链路重定向 WAN 流量。处于备用状态时，接通 USB 装置的电源。
  - (3G/4G) Failover Cold Standby （故障切换冷备份） - 丢失的以太网 WAN 端口连接通过 3G/4G USB 链路重定向 WAN 流量。处于备用状态时，断开 USB 装置的电源。
  - Primary Mode （主要模式） - 3G/4G 链路用作主要的 WAN 连接。
- **Signal Quality** （信号质量） - 表示 3G/4G USB 装置和接入点之间的信号强度。单击 **Refresh** （刷新）可更新读数。

步骤 4 为了防止数据过多，请选择 **Charge Count** （费用计数）。 **Traffic (KB)** （流量 (KB)）跟踪通过 USB 链路发送或接收的数据量 （以千字节为单位）。 **Time (min)** （时间（分钟））计算 3G/4G 连接处于活动状态的分钟数。

- 如果选择 Traffic (KB)，请输入下列信息：
  - **Premium** （费用） - 指定数据量的费用 （以美元为单位）。
  - **Extra Charge** （额外费用） - 超出指定量时，每千字节数据要收取的费用（以美元为单位）。
  - **Stop connection** （停止连接） - 选中此项可启用在数据量超出指定量时断开连接。

- 如果选择 Time (min)，请输入下列信息：
  - **Premium -** 指定时间段的费用 （以美元为单位）。
  - **Extra Charge -** 超出指定时间段时的费用 （以美元为单位）。
  - **Stop connection -** 选中此项可启用在超出指定时间时断开连接。

系统将显示窗口：

- **Previous Cumulative Time**（以前累积的时间）- 自重置后，3G/4G 连接接通的时间。
- **Current Cumulative Time**（当前累积的时间）- 自设备建立 3G/4G 连接之后经过的时间。
- **Charge** （费用） - 自重置计数器之后，连接的估计成本。

步骤 5 设置 **Diagnostic** （诊断）行为：

- **Restart count**（重新启动计数） - 选中并输入每月重新启动计数器的日期。如果数值大于当月天数 （例如， 30 天月份中出现数值 31），则计数器会在当月最后一天重新启动。
- **Self-test daily** （每天自检） - 选中并输入每天自检的时间 （24 小时制）以测试连接。如果设备可以从服务提供商获取 IP 地址，则自检被视为成功。否则，系统会将故障发送到日志。
- **Log self-test** （日志自检） - 选中以记录所有自检活动。（所有测试结果都会发送到日志中。）

步骤 6 单击 **Save** 保存设置。

DMZ 启用

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 端口的数据包重定向到 LAN 中特定的 IP 地址。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。建议将必须连接至 WAN （例如 Web 或电子邮件服务器）的主机置于 DMZ 网络中。

必须为指定为 DMZ 主机的端点配置一个固定的 （静态） IP 地址。应该在同一子网中为 DMZ 主机分配一个 IP 地址作为此设备的 LAN IP 地址，但是该地址不能与分配给此网关接口的 IP 地址相同。

配置 DMZ 的步骤：

步骤 1 选择 **Setup** > **Network**，然后选中 **Enable DMZ**（启用 DMZ）。系统将显示一条消息。

步骤 2 单击 **Yes**（是）接受更改。

步骤 3 在 **DMZ Settings**（DMZ 设置）表中选择 DMZ 接口，然后单击 **Edit**。系统将显示 **Edit DMZ Connection**（编辑 DMZ 连接）窗口。

步骤 4 选择 **Subnet**（子网）可显示 DMZ 服务的子网，然后输入 **DMZ IP Address**（DMZ IP 地址）和 **Subnet Mask**。或者选择 **Range**（范围）可在同一子网上为 DMZ 服务预留一组 IP 地址，然后输入 IP 地址范围。

步骤 5 单击 **Save**。

密码

用户名和密码允许对设备的管理访问。默认的用户名为 **cisco**。默认密码是 **cisco**。用户名和密码可以更改。我们强烈建议将默认密码更改为较强的密码。

要打开 Password 页面，请单击 **Setup > Password**。

如果在 （防火墙）通用 页面上启用了远程管理，则*必须*更改密码。

注意 密码一旦丢失或遗忘，则无法恢复。如果丢失或遗忘，则必须将设备重置为出厂默认设置，从而移除所有配置更改。如果远程访问设备并将设备重置为出厂默认设置，则在同一子网上建立本地有线链路之前，无法登录设备。

更改用户名和密码之后，您就会退出，需要使用新凭证重新登录到设备。

修改用户名和密码

请按照以下步骤改用户名和密码：

步骤 1 选择 **Setup>Password**。

步骤 2 设定以下参数：

- **Username -** 新用户名。要保留当前用户名，请将此字段留空。

- **Old Password** （旧密码） - 当前密码。如果您仅仅是修改用户名不修改用户密码，此字段为必填项。

  注　如果您仅仅是修改用户名不修改用户密码，请保持 **New Password** 和 **Confirm New Password** 字段为空。

- **New Password** （新密码） - 设备的新密码，使用字母数字字符和符号。不允许使用空格。
- **Confirm New Password** （确认新密码） - 新密码。如果两次输入的密码不一致，系统会显示错误消息。
- **Session Timeout** （会话超时） - 空闲会话超时。

步骤　3　单击 **Save**，保存您的设置。

设置密码复杂性

设置密码复杂性的步骤：

步骤　1　在 **Password Complexity Settings** （密码复杂性设置）区域，请选中 **Enable**。推荐启用此选项。

步骤　2　设定以下密码复杂性设置，包括：

Minimal password length	设定密码的最小字符长度 （0-64 个字符）。默认为最少 8 个字符长度。
Minimal number of character classes	设定密码应包含的最少字符类型。默认至少包含以下四种字符类别中的三种： ▪ 大写字母 ▪ 小写字母 ▪ 数字 ▪ 特殊字符 （支持标准键盘上的所有字符，除了单引号、双引号和反斜线 (' " \) 以外）
The new password must be different than the current one	勾选此选项，新密码不能与当前密码相同。默认为启用。

Password Aging （密码老化）	勾选此选项，一段时间后密码将过期。当密码过期后，必须重新设置新密码。默认为启用。如果不希望密码过期，请禁用此选项。
Password aging time （密码老化时间）	如启用密码过期，请输入密码到期之前要经过的天数。默认为 180 天。

步骤 3 单击 **Save**，保存您的设置。

时间

时间对网络设备至关重要，因此它可以正确获取系统日志和错误消息的时间戳，并与其他网络设备同步数据传输。

您可以配置时区 （无论是否调整夏令时，以及使用哪个网络时间协议 (NTP) 服务器）以同步日期和时间。然后路由器从 NTP 服务器获取日期和时间信息。

要打开 Time （时间）页面，请单击 **Setup > Time**。

要配置 NTP 和时间设置，请选择 **System** （系统） > **Time**。

- **Time Zone** （时区） - 与格林威治标准时间 (GMT) 相关的时区。
- **Daylight Savings Time** （夏令时） - 启用或禁用夏令时调整。在 **From** （开始时间）字段中输入开始日期，在 **To** （结束时间）字段中输入结束日期。
- **Set Date and Time** （设置日期和时间） - **Auto** 启用 NTP 服务器。如果选择 Auto，请输入完全合格的 **NTP Server** （NTP 服务器）名称或 IP 地址。**Manual** 启用设置本地日期和时间，并使用设备时钟维持时间。如果选择 **Manual**，请输入 **Date and Time** （日期和时间）。

DMZ 主机

DMZ Host 允许 LAN 中的一个主机连接到互联网以使用服务，例如互联网游戏和视频会议。通过使用防火墙访问规则可能会限制从互联网访问 DMZ Host。

要打开 DMZ Host 页面，请单击 **Setup > DMZ Host**。

要配置 DMZ 主机，请输入 **DMZ Private IP Address** （DMZ 专用 IP 地址）并单击 **Save**。

（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。端口触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。

要打开端口转发页面，请单击 **Setup > Forwarding** （转发）。

配置端口转发

当用户在网络上请求服务时，设备会根据端口转发参数将这些请求转发至服务器。系统会拒绝访问任何未指定的服务。例如，当端口号 80 (HTTP) 转发到 IP 地址 192.168.1.2 时，接口上所有的 HTTP 请求都会转发到 192.168.1.2。系统会拒绝任何其他流量，除非其他条目特别允许。

使用此功能建立 Web 服务器或 FTP 服务器。请确保输入的 IP 地址有效。（要运行互联网服务器，可能有必要使用静态 IP 地址。）为了提高安全性，外部用户能够与服务器进行通信，但是不允许连接到网络设备。

将服务添加到表或编辑服务的步骤：

步骤 1 要添加服务，请在 Port Range Forwarding （端口范围转发）表中单击 **Add**。

要编辑服务，请选择相应行并单击 **Edit**。

字段打开可以修改。

步骤 2 配置以下设置：

- 从下拉菜单中选择 **Service** （服务）。（如果服务未列出，可以按照添加或编辑服务名称部分中的说明修改列表。）
- 输入服务器的 **IP Address**。
- 选择 **Interface**。
- 选择 **Status**。选中此框可启用此服务。取消选中此框可禁用此服务。

步骤 3 单击 **Save**。

添加或编辑服务名称

添加或编辑 Service 列表上的条目的步骤：

步骤 1 单击 **Service Management** （服务管理）。如果 Web 浏览器显示弹出窗口的警告，请允许显示被阻止的内容。

步骤 2 要添加服务，请在 Service Management 表中单击 **Add**。

要编辑服务，请选择相应行并单击 **Edit**。

字段打开可以修改。如果 Web 浏览器显示弹出窗口的警告，请允许显示被阻止的内容。

步骤 3 列表中最多可包含 30 个服务：

- **Service Name** - 简短说明。
- **Protocol** （协议） - 所需协议。请参阅您托管的服务的相关文档。
- **Port Range** （端口范围） - 为此服务预留的端口号范围。

步骤 4 单击 **Save**。

配置端口触发

利用端口触发功能，设备可以监视特定端口号的传出数据。设备会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传输到正确的客户端。

某些互联网应用程序或游戏使用非典型端口在服务器和 LAN 主机之间进行通信。要使用这些应用程序，请在 Port Triggering （端口触发）表中输入触发 （传出）端口和备用传入端口。

将应用程序名称添加到表或编辑应用程序名称的步骤：

步骤 1 单击 **Setup** > **Forwarding**。

步骤 2 要添加应用程序名称，请在 Port Range Forwarding 表中单击 **Add**。

要编辑应用程序名称，请选择相应行并单击 **Edit**。字段打开可以修改。

如果 Web 浏览器显示弹出窗口的警告，请允许显示被阻止的内容。

步骤 3 配置以下设置：

- **Application Name** （应用程序名称） - 应用程序的名称。

- **Trigger Port Range** （触发端口范围） - 触发端口范围的起始和终止端口号。有关其他信息，请参阅应用程序的文档。
- **Incoming Port Range** （传入端口范围） - 传入端口范围的起始和终止端口号。有关其他信息，请参阅应用程序的文档。

步骤 4 单击 **Save**。

删除表格条目

要从表中删除条目，请单击要删除的条目，然后单击 **Delete** （删除）。要选择某个区域内的所有条目，请单击第一个条目，按住 **Shift** 键，然后单击该区域中的最后一个条目。要选择单个条目，请按住 **Ctrl** 键的同时单击每个条目。要取消选中某个条目，请按住 **Ctrl** 键的同时单击该条目。

端口地址转换

端口地址转换 (PAT) 是网络地址转换 (NAT) 的扩展，允许 LAN 上的多个设备映射至单个公共 IP 地址以保存 IP 地址。

除带有目标端口 （外部端口）的传入数据包被转换为具有其他目标端口 （内部端口）的数据包之外， PAT 与端口转发在其他方面均相似。互联网服务提供商 (ISP) 将单个 IP 地址分配到边缘设备。当计算机登录互联网时，此设备会为客户端分配一个端口号，追加至内部 IP 地址，从而为计算机指定一个唯一 IP 地址。

如果其他计算机登录互联网，则此设备会为其分配相同的公共 IP 地址，但是端口号不同。虽然两台计算机共用相同的公共 IP 地址，但是此设备知道哪台计算机发送了数据包，因为设备使用端口号为数据包分配计算机的唯一内部 IP 地址。

要打开此页，请选择 **Setup** > **Port Address Translation** （端口地址转换）。

添加或编辑 PAT 的步骤：

步骤 1 要添加服务，请在 Port Address Translation 表中单击 **Add**。

要编辑服务，请选择相应行并单击 **Edit**。字段打开可以修改。

如果 Web 浏览器显示弹出窗口的警告，请允许显示被阻止的内容。

步骤 2 从下拉菜单中选择 **Service**。最多可包含 30 个服务。（如果服务未列出，可以按照添加或编辑服务名称部分中的说明修改列表。）

步骤 3 请输入服务所在网络设备的 IP 地址或名称。

步骤 4 单击 **Save**。

添加或编辑服务名称

添加或编辑 Service 列表上的条目的步骤：

步骤 1 单击 **Service Management**。如果 Web 浏览器显示弹出窗口的警告，请允许显示被阻止的内容。

步骤 2 要添加服务，请在 Service Management 表中单击 **Add**。

要编辑服务，请选择相应行并单击 **Edit**。字段打开可以修改。

如果 Web 浏览器显示弹出窗口的警告，请允许显示被阻止的内容。

步骤 3 列表中最多可包含 30 个服务：

- **Service Name** - 简短说明。
- **Protocol** - 所需协议。请参阅您托管的服务的相关文档。
- **External Port** （外部端口） - 外部端口号。
- **Internal Port** （内部端口） - 内部端口号。

步骤 4 单击 **Save**。

设置一对一 NAT

一对一 NAT 创建了一种关系，将有效的 WAN IP 地址映射到 NAT 隐藏的 WAN （互联网）看不到的 LAN IP 地址。这可以保护 LAN 设备被发现和受攻击。

为了获得最佳结果，请为希望通过一对一 NAT 访问的内部资源预留 IP 地址。

可以映射单个 LAN IP 地址，也可以将 IP 地址范围映射到长度相等的外部 WAN IP 地址范围 （例如，三个内部地址和三个外部地址）。第一个内部地址将映射到第一个外部地址，第二个内部 IP 地址将映射到第二个外部 IP 地址，依此类推。

要打开此页，请在导航窗格中选择 **Setup** > **One-to-One NAT** （一对一 NAT）。

要启用此功能，请选中 **Enable**。

要在列表中添加条目，请单击 **Add** 并输入以下信息：

- **Private Range Begin** （专用范围起始值） - 要映射到公共范围的内部 IP 地址范围的起始 IP 地址。请勿在此范围中包含路由器的管理 IP 地址。
- **Public Range Begin**（公共范围起始值）- ISP 提供的公共 IP 地址范围的起始 IP 地址。请勿在此范围中包含路由器的 WAN IP 地址。
- **Range Length** （范围长度） - 此范围中 IP 地址的数量。范围长度不能超过有效 IP 地址的数量。要映射单个地址，请输入 1。

要修改条目，请选中要修改的条目并单击 **Edit**。相关信息将显示在文本字段中。进行更改，然后单击 **Save**。

MAC 地址克隆

某些 ISP 会要求注册 MAC 地址 （分配给每个网络设备的唯一 12 位身份识别代码）。如果以前通过 ISP 为设备注册过其他 MAC 地址，则可以选择此功能将该地址克隆至设备。否则，您必须联系 ISP 更改注册的 MAC 地址。

注 启用 MAC Address Clone （MAC 地址克隆）后，端口镜像无法工作。

要打开此页，请在导航窗格中选择 **Setup** > **MAC Address Clone**。

克隆 MAC 地址的步骤：

步骤 1 单击 **Interface** 单选按钮。

步骤 2 单击 **Edit** 可显示 Edit MAC Address Clone （编辑 MAC 地址克隆）页面。

- **User Defined WAN MAC Address** （用户定义的 WAN MAC 地址） - 单击该单选按钮并输入您通过 ISP 注册的 12 位 MAC 地址。
- **MAC Address from this PC**（此 PC 的 MAC 地址）- 单击可将计算机的 MAC 地址用作设备的克隆 MAC 地址。

步骤 3 单击 **Save**。

将动态 DNS 分配到 WAN 接口

通过动态域名系统 (DDNS) 服务，可以为动态 WAN IP 地址分配固定域名，从而可以在 LAN 中托管自己的 Web、 FTP 或其他类型的 TCP/IP 服务器。选择此功能可使用 DDNS 信息配置 WAN 接口。

在路由器上配置 Dynamic DNS 之前，建议您访问 www.dyndns.org 并注册一个域名。（该服务由 DynDNS.org 提供）。中国用户请访问 www.3322.org 进行注册。

要打开此页，请在导航窗格中选择 **Setup > Dynamic DNS** 。

选择接口并单击 **Edit** 后，系统将显示 Edit Dynamic DNS Setup （编辑动态 DNS 设置）页面。

编辑 DDNS 服务的步骤：

步骤 1 从 **DDNS Service** （DDNS 服务）列表中，选择服务。

步骤 2 输入帐户信息：

- **Username -** DDNS 帐户的用户名。如果未注册任何主机名，请单击 **Register**（注册）转至 DynDNS.com 网站，在该网站免费注册 Dynamic DNS 服务。
- **Password -** DDNS 帐户的密码。
- **Host Name -** 通过 DDNS 提供商注册的主机名。例如，如果主机名是 *myhouse.dyndns.org*，则在第一个字段中输入 *myhouse*，在第二个字段中输入 *dyndns*，在最后一个字段中输入 *org*。

此时将显示以下只读信息：

- **Internet IP Address** （互联网 IP 地址） **-** 接口的 WAN IP 地址。
- **Status-** DDNS 的状态。如果状态信息指示发生错误，请确保输入的 DDNS 服务帐户信息正确。

步骤 3 单击 **Save**。

高级路由

此功能支持动态路由，并可将静态路由添加至 IPv4 和 IPv6 的路由表中。

要查看路由表，请单击 **View Routing Table** （查看路由表）。单击 **Refresh** 更新数据。单击 **Close** （关闭）关闭弹出窗口。

配置动态路由

根据路由协议携带的信息，动态路由自动构建路由表，且网络几乎可自主调整，以避免网络故障和堵塞。

要使用路由信息协议 (RIP) 配置 IPv4 动态路由，请单击 **IPv4** 选项卡。

要使用路由信息协议下一代 (RIPng) 配置 IPv6 动态路由，请单击 **IPv6** 选项卡。

配置 **IPv4** 动态路由

步骤 1 选择 Working Mode：

- **Gateway** （网关） - 如果此设备托管互联网网络连接，请选择此模式。此选项为系统默认的设置。
- **Router** （路由器） - 如果设备位于连接有其他路由器的网络上并且另一台设备是连接互联网的网络网关或者此网络未连接到互联网，请选择此模式。在 Router 模式中，仅当有另一个路由器充当网关时，网络设备才可以使用互联网连接。由于网关提供了防火墙保护，因此请禁用此设备的防火墙。

步骤 2 启用 **RIP**，可让此设备与其他路由器自动交换路由信息，并在网络发生变化时动态调整自己的路由表。默认设置为 Disabled。如果启用此功能，请同时配置以下设置：

- **Receive RIP versions**（接收 RIP 版本）- 选择用于接收网络数据的 RIP 协议：**None** （无）、 **RIPv1**、 **RIPv2** 或 **Both RIP v1 and v2** （RIP v1 和 v2）。

  RIPv1 是一种基于类别的路由版本。它不包括子网信息，因此不支持变长子网掩码 (VLSM)。RIPv1 同样不支持路由器验证，因此容易受到攻击。**RIPv2** 携带子网掩码且支持密码安全验证。

- **Transmit RIP versions** （传输 RIP 版本） - 选择用于传输网络数据的 RIP 协议：**None**、 **RIPv1**、 **RIPv2 - Broadcast** （RIPv2 - 广播）或 **RIPv2 - Multicast** （RIPv2 - 组播）。

  RIPv2 - Broadcast （推荐设置）会在整个子网中广播数据。 **RIPv2 - Multicast** 会将数据发送到组播地址。RIPv2 - Multicast 会将路由表组播到毗邻的路由器而非广播到整个网络，同样有助于避免不必要的负载。

步骤 3 单击 **Save**。

配置 **IPv6** 动态路由

如果在 Setup > Network 页面上启用了 Dual-Stack IP，则可以使用 IPv6 选项卡。

要启用 RIPng，请选中 **RIPng** 框。

配置静态路由

可以为 IPv4 或 IPv6 配置静态路由。这些是路由表中未过期的路由。您最多可输入 30 个路由。

要配置静态路由，请单击 **Add** 或选择一个条目，然后单击 **Edit**：

- **Destination IP** （目标 IP） - 远程 LAN 区段的子网地址。对于 C 类 IP 域，该网络地址为目标 LAN IP 地址的前三个字段；最后一个字段应为 0。
- **Subnet Mask (IPv4 only)** （子网掩码 （仅 IPv4）） - 目标 LAN IP 域中使用的子网掩码。对于 C 类 IP 域，子网掩码通常为 255.255.255.0。
- **Prefix Length (IPv6 only)** （前缀长度 （仅 IPv6）） - IPv6 前缀的长度。
- **Default Gateway** - 最后选择的路由器的 IP 地址。
- **Hop Count** （跳跃计数） - 在被丢弃之前数据包通过的节点或跳跃的最多次数（最多为 15 次跳跃）。节点可以是网络上的任何设备，例如交换机或路由器。
- **Interface** - 要用于此路由的接口。

要从列表中删除条目，请单击要删除的条目，然后单击 **Delete**。

要查看当前数据，请单击 **View Routing Table**。此时将显示 Routing Table Entry List（路由表条目列表）。可以单击 **Refresh** 更新数据，或单击 **Close** 关闭弹出窗口。

入站负载平衡

入站负载平衡将入站流量平均分配到每个 WAN 端口以充分利用带宽。还可以防止流量分配不均和拥塞。

启用和配置入站负载平衡的步骤：

步骤 1 单击 **Enable Inbound Load Balance** （启用入站负载平衡）。

步骤 2 输入 **Domain Name** 信息：

- **Domain Name** - DNS 服务提供商分配的域名。
- **TTL**（存活时间） - DNS 查询的时间间隔（秒， 0~65535）。较长的时间间隔会影响刷新时间。较短的时间间隔会增加系统负载，但是 Inbound Load Balance（入站负载平衡）的准确率更高。您可以调整此参数，实现网络的最佳性能。
- **Admin** （管理员） - 管理员电子邮件地址。

步骤 3 输入 **DNS Server** （DNS 服务器）参数：

- **Name Server** （名称服务器） - 转换域名的 DNS 服务器。
- **Interface** - 与名称服务器相对应的 WAN 接口。系统显示获取的、启用的 WAN IP 地址。

步骤 4 在 **Host** （记录） **Name** 字段中输入提供服务的主机名 （例如邮件服务器或 FTP 服务器），并为分配入站流量选择 **WAN IP** 接口。

步骤 5 输入 **Alias** （别名）（为可能提供多项服务的一台计算机主机分配多个名称），和 **Target** （目标）（现有的 A Record （A 记录）域名）。

步骤 6 单击 **SPF Settings** （SPF 设置）以添加 SPF 文本。 SPF （发件人策略框架）是一个电子邮件验证系统，通过验证发件人 IP 地址检测电子邮件仿冒 （一种常见的漏洞）来阻止垃圾邮件。（无需配置此字段。详情请访问 http://www.openspf.org/Tools#wizard?mydomain=&x=35&y=6。）

步骤 7 输入 **Mail Server** （邮件服务器）参数：

- **Host Name** - 邮件主机的名称 （不含域名）。
- **Weight** （权重） - 邮件主机的顺序。较低的数字具有最高优先级。
- **Mail Server** - 保存在 A Record 中的服务器名称或外部邮件服务器的名称。

步骤 8 单击 **Save**。

USB 设备升级

使用此网络设备可以升级 USB 设备固件。

要升级连接到 USB 端口的 USB 设备，请浏览要从 PC 上传到 USB 设备的文件并单击 **Upgrade** （升级）。

4

DHCP

动态主机配置协议 (DHCP) 是用于配置网络设备的网络协议，以便设备在 IP 网络上进行通信。DHCP 客户端使用 DHCP 协议从 DHCP 服务器获取配置信息，例如 IP 地址、默认路由及一个或多个 DNS 服务器地址。然后 DHCP 客户端使用此信息对主机进行配置。配置流程完成后，主机就能够通过互联网进行通信了。

DHCP 服务器可维护含有可用 IP 地址和配置信息的数据库。从客户端收到请求后，DHCP 服务器会确定 DHCP 客户端连接到的网络，并为客户端分配适用的 IP 地址或前缀，同时为该客户端发送相应的配置信息。

DHCP 服务器和 DHCP 客户端必须连接到同一网络链路。在较大的网络中，每个网络链路都包含一个或多个 DHCP 中继代理。这些 DHCP 中继代理从 DHCP 客户端接收消息并将其转发至 DHCP 服务器。 DHCP 服务器将响应发送回中继代理，然后中继代理将这些响应发送至本地网络链路上的 DHCP 客户端。

DHCP 服务器分配给客户端的 IP 地址通常会有一定的有效期 （称为*租用*）。DHCP 客户端应在该期限过期之前更新 IP 地址。如果没有更新，则过期之后必须停止使用该地址。

DHCP 用于 IPv4 和 IPv6。虽然两个版本的用途是相同的，但是 IPv4 和 IPv6 协议的内容大不相同，应该被视为两个单独的协议。

DHCP 设置

DHCP Setup （DHCP 设置）选项用于为 IPv4 或 IPv6 配置 DHCP。利用它，某些设备可以从 TFTP 服务器下载配置。如果没有预先配置 IP 地址和 TFTP 服务器 IP 地址，设备启动后，将会使用 Option 66 （选项 66）、 Option 67 （选项 67）和 Option 150 （选项 150）将请求发送至 DHCP 服务器以获取此信息。

DHCP Option 150 是思科专有的。与此要求类似的 IEEE 标准为 Option 66。与 Option 150 一样， Option 66 用于指定 TFTP 服务器的名称。 Option 67 可以提供启动文件名称。

利用 Option 82 （选项 82）（DHCP 中继代理信息选项）， DHCP 中继代理将客户端发起的 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。

要打开此页，请选择 **DHCP > DHCP Setup**。

要设置 DHCP IPv4，请单击 **IPv4** 选项卡。要设置 DHCP IPv6，请单击 **IPv6** 选项卡。

为 **IPv4** 配置 **DHCP**

为 IPv4 配置 DHCP 的步骤：

步骤 1 选择 **VLAN** 或 **Option 82**。

步骤 2 如果选择 **Option 82**，请使用 DHCP > 选项 **82** 添加电路 ID。添加之后，这些电路 ID 会列在 **Circuit ID** （电路 ID）下拉菜单中。

如果选择 **VLAN**，请从 **VLAN ID** 菜单中选择 VLAN 并输入以下信息：

- **Device IP Address** （设备 IP 地址） - 管理 IP 地址。
- **Subnet Mask** - 管理 IP 子网掩码。

步骤 3 选择 **DHCP Mode** （DHCP 模式）：

- **Disable** - 在此设备上禁用 DHCP。不需要填写其他参数。
- **DHCP Server**（DHCP 服务器）- 将客户端 DHCP 请求传输至设备的 DHCP 服务器。
- **DHCP Relay** （DHCP 中继） - 通过设备传递其他 DHCP 服务器中的 DHCP 请求和回复。如果选择 DHCP Relay，请输入 **Remote DHCP Server** （远程 DHCP 服务器）的 IP 地址。
- **Client Lease Time** （客户端租用时间） - 网络用户可以使用当前 IP 地址连接到路由器的时间 （以分钟为单位）。有效值为 5 至 43200 分钟。默认为 1440 分钟（即 24 小时）。
- **Range Start** （范围起始值）和 **Range End** （范围结束值） - 构成可动态分配的 IP 地址范围的起始和结束 IP 地址。该范围内的 IP 地址数可以达到服务器在不引起功能重叠 （例如 PPTP 和 SSL VPN）时能够分配的最大数目。请勿在此动态 IP 范围中包含此设备的 LAN IP 地址。例如，如果路由器使用默认的 LAN IP 地址 **192.168.1.1**，则起始值必须为 192.168.1.2 或更大值。
- **DNS Server** - DNS 服务类型；在此可获取 DNS 服务器 IP 地址。
- **Static DNS 1** （静态 DNS 1）和 **Static DNS 2** （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，则设备将使用第一个 DNS 服务器响应请求。
- **WINS** - Windows 互联网命名服务 (WINS) 服务器的可选 IP 地址，用于将 NetBIOS 名称解析到 IP 地址。如果不知道 WINS 服务器的 IP 地址，请使用默认值 0.0.0.0。

步骤 4 请输入 TFTP 服务器参数：

- **TFTP Server Host Name** （TFTP 服务器主机名） - TFTP 服务器的主机名。
- **TFTP Server IP** （TFTP 服务器 IP） - TFTP 服务器的 IP 地址。
- **Configuration Filename** （配置文件名） - 用于升级设备的文件的配置文件名。

为 **IPv6** 配置 **DHCP**

为 IPv6 配置 DHCP 的步骤：

步骤 1 输入 **IPv6 Address** （IPv6 地址）。

步骤 2 输入 **Prefix Length**。

步骤 3 选择 **DHCP Mode**：

- **Disable** - 在此设备上禁用 DHCP。不需要填写其他参数。
- **DHCP Server** - 将客户端 DHCP 请求传输至设备的 DHCP 服务器。
- **DHCP Relay** - 通过设备传递其他 DHCP 服务器中的 DHCP 请求和回复。
- **Client Lease Time** - 网络用户可以使用当前 IP 地址连接到路由器的时间。输入时间 （以分钟为单位）。有效值为 5 至 43200 分钟。默认为 1440 分钟 （即 24 小时）。
- **DNS Server 1** 和 **DNS Server 2** - （可选） DNS 服务器的 IP 地址。如果输入第二个 DNS 服务器，则设备将使用第一个 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。使用默认设置 0.0.0.0 可使用动态分配的 DNS 服务器。

步骤 4 输入 IPv6 地址池：

- **Start Address** （起始地址） - IPv6 地址池的起始地址。
- **End Address** （结束地址） - IPv6 地址池的结束地址。
- **Prefix Length** - IPv6 IP 地址前缀的长度。

查看 DHCP 状态

DHCP Status （DHCP 状态）显示 DHCP 服务器的状态及其客户端。

要打开此页，请在导航树中选择 **DHCP** > **DHCP Status**。

仅在设置网络页面上启用 Dual-Stack IP 之后，方可使用 IPv6 选项卡。

要查看 DHCP 状态和客户端，请单击 **IPv4** 选项卡或 **IPv6** 选项卡。对于 IPv4，请选择 **VLAN** 或 **Option 82**。对于 IPv6，请选择 **Prefix** （前缀）。

对于 DHCP 服务器，系统将显示以下信息：

- **DHCP Server -** DHCP 服务器的 IP 地址。
- **Dynamic IP Used** （使用的动态 IP） **-** 使用的动态 IP 地址的数量。
- **Static IP Used (IPv4 only)** （使用的静态 IP （仅 IPv4）） **-** 使用的静态 IP 地址的数量。
- **DHCP Available** （可用的 DHCP） **-** 可用动态 IP 地址的数量。
- **Total** （总数） **-** DHCP 服务器管理的动态 IP 地址的总数。

Client Table （客户端表）显示 DHCP 客户端信息：

- **Client Host Name** （客户端主机名） **-** 分配给客户端主机的名称。
- **IP Address -** 分配给客户端的动态 IP 地址。
- **MAC Address (IPv4 only)** （MAC 地址 （仅 IPv4）） **-** 客户端的 MAC 地址。
- **Client Lease Time -** 网络用户可以使用动态 IP 地址连接到路由器的时间。

要释放 IPv4 客户端 IP 地址，请选择 **Client Host Name**，然后单击 **Delete**。

单击 **Refresh** 更新数据。

选项 82

利用 Option 82 （DHCP 中继代理信息选项）， DHCP 中继代理将客户端发起的 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。

利用 DHCP Option 82 Configurable Circuit ID （DHCP 选项 82 可配置电路 ID），您可以决定在 Option 82 Circuit ID （选项 82 电路 ID）描述中提供的信息，从而增强了验证安全性。

要打开此页，请在导航树中选择 **DHCP > Option 82** 。

要添加 **Circuit ID**，请单击 **Add**。系统会向表中新添加一行，电路 ID 会列在 **DHCP** 设置窗口的 Circuit ID 下拉菜单中。

要编辑 **Circuit ID**，请选择相应行并单击 **Edit**。即可修改该行。

IP 和 MAC 绑定

当设备配置为 DHCP 服务器或 DHCP 中继时，可以将静态 IP 地址绑定到最多 100 个网络设备，例如 Web 服务器或 FTP 服务器。绑定不会向设备分配 IP 地址。应确保在 IP & MAC 绑定表中绑定到静态 IP 地址的每台设备都配置为使用静态 IP 地址。

通常设备的 MAC 地址实际显示在设备底部面板或后面板的标签上。

要打开此页，请在导航树中选择 **DHCP > IP & MAC Binding** （IP & MAC 绑定）。

通过发现绑定 **IP** 地址

将已知 IP 地址绑定到 MAC 地址并命名该绑定，具体步骤为：

步骤 **1** 单击 **Show Unknown MAC Addresses** （显示未知 MAC 地址）。系统将显示 IP & MAC Binding Table （IP & MAC 绑定表）。如果 Web 浏览器显示弹出窗口的消息，请允许显示被阻止的内容。

设备按 IP 地址和 MAC 地址列出。如有需要，请单击 **Refresh** 更新数据。

步骤 **2** 输入描述性 **Name**。

步骤 **3** 选中 **Enable** 框。或者，通过单击 Enable 列顶部的复选框来选择列表中的所有设备。

步骤 **4** 单击 **Save** 将设备添加到 Static IP 列表中，或者单击 **Close** 关闭弹出窗口不添加所选设备。

手动绑定 **IP** 地址

要在列表中添加新的绑定，请单击 **Add** 并输入以下信息：

- **Static IP Address**（静态 IP 地址） **-** 静态 IP 地址。如果希望路由器将静态 IP 地址分配给此设备，则输入 0.0.0.0。
- **MAC Address**（MAC 地址） **-** 设备的 MAC 地址。输入地址时不得包含任何标点符号。
- **Name -** 设备的描述性名称。
- **Enable -** 选中此框可将静态 IP 地址绑定到此设备。

编辑或删除绑定的条目

要 **Edit** 设置，请选择列表中的条目并单击 **Edit**。相关信息将显示在文本字段中。进行更改，然后单击 **Save**。

要从列表中 **Delete** 条目，请选择要删除的条目，然后单击 **Delete**。要选择某个区域内的所有条目，请单击第一个条目，按住 **Shift** 键，然后单击该区域中的最后一个条目。要选择单个条目，请按住 **Ctrl** 键的同时单击每个条目。要取消选中某个条目，请按住 **Ctrl** 键的同时单击该条目。

使用静态 **IP** 列表阻止设备

Static IP 列表可用于控制网络的访问权限。

阻止列表中未列出的设备或无正确 IP 地址的设备进行访问，具体步骤为：

- **Block MAC address on the list with wrong IP address**（阻止列表上 IP 地址错误的 MAC 地址） **-** 选中此框可阻止设备的 IP 地址更改时访问网络。例如，如果已分配静态 IP 地址 192.168.1.100，而其他人将此设备配置为使用 192.168.149，则此设备将无法连接到网络。此功能可以阻止用户在未经允许的情况下更改设备 IP 地址。取消选中此框将允许访问，而不考虑当前的 IP 地址分配情况。
- **Block MAC address not on the list**（阻止列表上没有的 MAC 地址） **-** 选中此框可阻止 Static IP 列表中未列出的设备进行访问。此功能可以阻止未知设备访问网络。取消选中此框将允许所有配置有正确范围内 IP 地址的设备进行访问。

DNS 本地数据库

域名服务 (DNS) 可将域名与其可路由 IP 地址相匹配。您可以设置 DNS Local Database （DNS 本地数据库），以使设备充当常用域名的本地 DNS 服务器。与使用外部 DNS 服务器相比，使用本地数据库的速度可能更快。如果请求的域名不在本地数据库中，则该请求将转发至设置网络 > WAN Setting 页面中指定的 DNS 服务器。

如果启用此功能，还必须将客户端设备配置为使用该设备作为 DNS 服务器。默认情况下， Windows 计算机设置为自动从默认网关中获取 DNS 服务器地址。

要更改 TCP/IP 连接设置，例如，在运行 Windows 的 PC 上，转到 *Local Area Connection Properties* （本地连接属性） > *Internet Protocol* （互联网协议） > *TCP/IP Properties* （*TCP/IP* 属性）窗口。选择 **Use the following DNS server address**，然后输入路由器的 LAN IP 地址作为 Preferred DNS Server （首选 DNS 服务器）。有关详情，请参阅正在配置的客户端文档。

添加、编辑或删除本地 **DNS** 条目

要添加新条目，请单击 **Add** 并输入以下信息：

- **Host Name -** 输入域名，如 *example.com* 或 *example.org*。如果未包含域名的最后一级，则 Microsoft Windows® 将自动在条目末尾附加 *.com*。
- **IP Address -** 输入资源的 IP 地址。

要 **Edit** 设置，请选择列表中的条目。相关信息将显示在文本字段中。进行更改，然后单击 **Save**。

要从列表中 **Delete** 条目，请选择要删除的条目，然后单击 **Delete**。要选择某个区域内的所有条目，请单击第一个条目，按住 **Shift** 键，然后单击该区域中的最后一个条目。要选择单个条目，请按住 **Ctrl** 键的同时单击每个条目。要取消选中某个条目，请按住 **Ctrl** 键的同时单击该条目。

路由器通告 (IPv6)

RADVD （路由器通告常驻程序）用于 IPv6 自动配置和路由。启用后，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。

如果在设置网络页面上启用了 Dual-Stack IP，则可以使用此页面。如果未启用，则当您尝试打开此页时将显示一则消息。

要打开此页，请在导航树中选择 **DHCP** > **Router Advertisement**。

要 **Enable Router Advertisement** （启用路由器通告），请选中此框并填写其他字段：

- **Advertise Mode** （通告模式） - 请选择以下选项之一：
  - **Unsolicited Multicast** （未经请求的组播） - 将 Router Advertisement 消息发送至组播组中的所有接口。此选项为系统默认的设置。同时还需输入 **Advertisement Interval** （通告间隔）；发送 Router Advertisement 消息的间隔。输入 10 至 1800 秒之间的任意值。默认为 30 秒。
  - **Unicast only** （仅单播） - 仅将 Router Advertisement 消息发送至众所周知的 IPv6 地址。
- **RA Flags**（RA 标签） - 确定主机是否可以使用 DHCPv6 获取 IP 地址和相关信息。选项如下：
  - **Managed** （管理型） - 主机使用管理型、有状态的配置协议 (DHCPv6) 通过 DHCPv6 获取有状态的地址和其他信息。
  - **Other** （其他） - 使用管理型、有状态的配置协议 (DHCPv6) 获取其他非地址信息，例如 DNS 服务器地址。
- **Router Preference** （路由器偏好）—**High** （高）、 **Medium** （中）或 **Low**（低）偏好度量标准用于多宿主主机有权访问多个路由器的网络拓扑中。此度量标准有助于主机选择合适的路由器。如果有两个路由器可以访问，则选择具有较高偏好的路由器。对于未实施路由器偏好的主机，可以忽略这些值。默认设置为 High。
- **MTU** - 可在网络中发送的最大数据包的大小。 MTU （最大传输单位）用于 Router Advertisement 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。
- **Router Lifetime** （路由器有效期限） - Router Advertisement 消息在路由上存在的时间 （以秒为单位）。默认值为 3600 秒。

要添加新子网，请单击 **Add**，然后输入 **IPv6 Address**、 **Prefix Length** 和 **Lifetime**（有效期限）。

5

系统管理

System Management （系统管理）配置高级设置 （例如诊断工具）并执行固件升级、备份和设备重新启动等任务。

双 WAN 连接

如果使用了多个 WAN 接口，则使用此功能可配置互联网连接的设置。

要配置 WAN 端口，请在导航树中选择 **System Management** > **Dual WAN** （双 WAN）。

要配置负载平衡，请选择以下模式之一来管理 WAN 连接：

- **Smart Link Backup** （智能链路备份） - 确保连接不中断。如果主 WAN 连接不可用，则系统会使用备份 WAN 连接。从下拉菜单中选择主 WAN 接口。
- **Load Balance** （负载平衡） - 同时使用两种 WAN 连接以增加可用带宽。路由器会以加权轮循方式均衡两个接口之间的流量。

注 DNS 查询不受负载平衡的影响。

要配置 Interface Settings （接口设置），请选择 **WAN Interface** （WAN 接口），然后单击 **Edit**。系统将显示接口的设置窗口。输入以下参数：

ISP 提供的最大带宽

输入 ISP 指定的最大带宽设置。如果带宽超出指定值，则在下次连接时，路由器将使用其他 WAN 接口。

- **Upstream** （上行） - ISP 提供的最大上行带宽。默认值为 10000 kbs。最大值为 1000000 kbs。
- **Downstream** （下行） - ISP 提供的最大下行带宽。默认值为 10000 kbs。

网络服务检测

作为可选操作，选中此框可允许设备通过 Ping 特定的设备来检测网络连接，然后输入以下所述设置：

- **Retry count** （重试计数） - 对设备执行 Ping 命令的次数。范围为 1 到 99999，默认值为 3。
- **Retry timeout** （重试超时） - 两次 Ping 操作之间等待的秒数。范围为 1 到 9999999，默认值为 10 秒。
- **When Fail** （失败时） - Ping 测试失败时执行的操作。
  - **Generate the Error Condition in the System Log** （在系统日志中生成错误情况） - 在系统日志中记录失败状况。不会故障切换到其他接口。
  - **Keep System Log and Remove the Connection** （保留系统日志并删除连接） - 进行故障切换并使用备用接口。 WAN 端口的连接恢复后，其流量也随之恢复。
- **Default Gateway**、 **ISP Host** （ISP 主机）、 **Remote Host** （远程主机）和 **DNS Lookup Host** （DNS 查找主机） - 选择要 Ping 的设备以确定网络连接。对于 ISP 主机或远程主机，请输入 IP 地址。对于 DNS 查找主机，请输入主机名或域名。如果不想为了进行网络服务检测而 Ping 此设备，请取消选中此框。

协议绑定

Protocol Binding （协议绑定）要求将此接口应用于指定的协议、源和目标地址。它允许管理员将特定的出站流量绑定到 WAN 接口。当两个 WAN 接口具有不同的特征，或者从 LAN 到 WAN 的某些流量必须通过同一 WAN 接口时，此功能很有用。

要添加或编辑表格条目，请单击 **Add** 或 **Edit** 并输入以下信息：

- **Service** - 要与此 WAN 接口绑定的服务 （或 All Traffic （所有流量））。如果某服务未列出，可以单击 **Service Management** 添加此服务。有关详情，请参阅添加或编辑服务。
- **Source IP** （源 IP）和 **Destination IP** - 通过此 WAN 端口的流量的内部源和外部目标。对于 IP 地址范围，请在第一个字段中输入第一个地址，并在 *To （到）* 字段中输入最后一个地址。对于单个 IP 地址，请在两个字段中输入同一地址。

要启用协议绑定，请选中此框以启用该规则，或取消选中此框以禁用该规则。

要 **Edit** 设置，请选择列表中的条目。相关信息将显示在文本字段中。进行更改，然后单击 **Save**。

要从列表中 **Delete** 条目，请选择要删除的条目，然后单击 **Delete**。要选择某个区域内的所有条目，请单击第一个条目，按住 **Shift** 键，然后单击该区域中的最后一个条目。要选择单个条目，请按住 **Ctrl** 键的同时单击每个条目。要取消选中某个条目，请按住 **Ctrl** 键的同时单击该条目。

添加或编辑服务

要向 Service 列表中添加新条目或更改条目，请单击 **Service Management**。列表中最多可包含 30 个服务。如果 Web 浏览器显示弹出窗口的警告，请允许显示被阻止的内容。

要在列表中添加服务，请单击 **Add** 并输入以下信息：

- **Service Name -** 简短说明。
- **Protocol -** 所需协议。请参阅您托管的服务的相关文档。
- **Port Range -** 所需的端口范围。

要 **Edit** 设置，请在列表中选择条目并单击 **Edit**。相关信息将显示在文本字段中。进行更改，然后单击 **Save**。

要从列表中 **Delete** 条目，请选择要删除的条目，然后单击 **Delete**。要选择某个区域内的所有条目，请单击第一个条目，按住 **Shift** 键，然后单击该区域中的最后一个条目。要选择单个条目，请按住 **Ctrl** 键的同时单击每个条目。要取消选中某个条目，请按住 **Ctrl** 键的同时单击该条目。

带宽管理

Bandwidth Management （带宽管理）调整上行流量和下行流量的带宽设置，并为不同类型的流量 （例如语音服务）配置服务质量 (QoS) 设置。

要打开带宽管理，请在导航树中选择 **System Management** > **Bandwidth Management**。

ISP 提供的最大带宽

输入 ISP 指定的最大带宽设置：

- **Upstream -** ISP 提供的最大上行带宽。
- **Downstream -** ISP 提供的最大下行带宽。

带宽管理类型

请选择以下管理选项之一：

- **Rate Control** （速率控制） - 每个服务或 IP 地址的最小 （保证）带宽和最大（限制）带宽。最多可添加 100 个服务。
- **Priority** （优先级） - 通过确定高优先级和低优先级服务来管理带宽。

速率控制

要添加受带宽管理限制的接口，请单击 **Add** 并输入以下设置：

- **Interface** - 支持该服务的接口。
- **Service** - 要管理的服务。如果有服务未列出，请单击 **Service Management** 添加服务。
- **IP** - 要控制的 IP 地址或范围。
- **Direction** （方向） - 为出站流量选择 **Upstream**。为入站流量选择 **Downstream**。
- **Min. Rate** （最低速率） - 所保证的带宽的最低速率 （以 kbs 为单位）。
- **Max. Rate** （最高速率） - 所保证的带宽的最高速率 （以 kbs 为单位）。

选中此框可启用此服务。

配置优先级

要添加受带宽管理限制的接口，请单击 **Add** 并输入以下设置：

- **Interface** - 支持该服务的接口。
- **Service** - 要管理的服务。如果有服务未列出，请单击 **Service Management** 添加服务。
- **Direction** - 为出站流量选择 **Upstream**。为入站流量选择 **Downstream**。
- **Priority** - 选择此服务的优先级：**High** （高）或 **Low** （低）。默认优先级级别为 Medium （中），这是隐含的，未显示在网页界面中。

选中此框可启用此服务。

要 **Edit** 设置，请在列表中选择条目并单击 **Edit**。相关信息将显示在文本字段中。进行更改，然后单击 **Save**。

要从列表中 **Delete** 条目，请选择要删除的条目，然后单击 **Delete**。要选择某个区域内的所有条目，请单击第一个条目，按住 **Shift** 键，然后单击该区域中的最后一个条目。要选择单个条目，请按住 **Ctrl** 键的同时单击每个条目。要取消选中某个条目，请按住 **Ctrl** 键的同时单击该条目。

SNMP

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、监控并接收通知。设备支持 SNMP v1/v2c 和 SNMP v3。设备支持 MIBII 等标准管理信息库 (MIB) 以及专用 MIB。

设备充当 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/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。

要打开此页，请在导航树中选择 **System Management > SNMP**。

配置 SNMP

- **System Name** （系统名称） - 设备的主机名。
- **System Contact** （系统联系人） - 作为设备更新事宜联系人的网络管理员的姓名。
- **System Location** （系统位置） - 网络管理员的联系信息：电子邮件地址、电话号码或寻呼机号码。
- **Trap Community Name** （陷阱社区名称） - 随每个陷阱发送到 SNMP 管理器的密码。字符串中最多可以包含 64 个字母数字字符。默认为 **public**。
- **Enable SNMPv1/v2c** （启用 SNMPv1/v2c） - 启用 SNMP v1/v2c。
  - **Get Community Name** （获取社区名称） - 验证 SNMP GET 命令的社区字符串。输入的名称长度最多可以包含 64 个字母数字字符。默认为 *public*。
  - **Set Community Name** （设置社区名称） - 验证 SNMP SET 命令的社区字符串。输入的名称长度最多可以包含 64 个字母数字字符。默认为 *private*。
  - **SNMPv1/v2c Trap Receiver IP Address** （SNMPv1/v2c 陷阱接收器 IP 地址） - 运行 SNMP 管理软件的服务器的 IP 地址或域名。

- **Enable SNMPv3** （启用 **SNMPv3**） - 启用 SNMPv3。（在创建 SNMP 组和用户之前，请选中此框并单击 **Save**。）请按照配置 **SNMPv3** 中的相关说明来操作。
  - **SNMPv3 Trap Receiver IP Address** （SNMPv3 陷阱接收器 IP 地址） - 运行 SNMP 管理软件的服务器的 IP 地址或域名。
  - **SNMPv3 Trap Receiver User** （SNMPv3 陷阱接收器用户） - 运行 SNMP 管理软件的服务器的用户名。

配置 **SNMPv3**

可以创建 SNMPv3 组来管理 SNMP MIB 访问权限并识别对每个组有访问权限的用户。

添加或编辑组的步骤：

步骤 1 在 Group Table （组表）中单击 **Add**，或选择一个组后单击 **Edit**。

步骤 2 输入 **Group Name** （组名称）。

步骤 3 从下拉菜单中选择 **Security Level** （安全等级）。选择 **Authentication** （验证）或 **Privacy** （隐私）强制用户使用密码进行验证。选择 **No Authentication** （不验证）、**No Privacy** （无隐私）后，该组中的所有用户都无需设置验证密码或隐私密码。默认为 **No Authentication, No Privacy**。 Authentication 和 Privacy 密码至少需要 8 个字符。

步骤 4 选择组成员可以访问的 **MIBs**。

步骤 5 单击 **Save**。

添加或编辑用户的步骤：

步骤 1 在 User Table （用户表）中单击 **Add** 或选择一个用户后单击 **Edit**。

步骤 2 输入 **User Name** （用户名）。

步骤 3 从下拉菜单中选择 **Group** （组）。

步骤 4 选择 **Authentication Method** （验证方法）并输入 **Authentication Password** （验证密码）。

步骤 5 选择 **Privacy Method**（隐私方法）并输入 **Privacy Password** （隐私密码）。

步骤 6 单击 **Save**。

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 多播 Bonjour 服务记录，以通告此服务的存在。

注 为了发现思科 Small Business 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。有关详情以及要下载此实用程序，请访问 www.cisco.com/go/findit。

要打开此页，请在导航树中选择 **System Management > Discovery-Bonjour** （发现 - Bonjour）。

要全局启用 Bonjour，请选中 **Discovery Enable** （发现启用）框。默认情况下，此功能处于启用状态。

要为 VLAN 启用 Bonjour，请在 **Enable Bonjour** （启用 Bonjour）列中选中此框。默认情况下，此功能处于启用状态。

LLDP 属性

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、主要有线以太网上通告其身份、功能和邻居。 LLDP 信息由设备每隔一段固定时间，从每个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) 序列构成。

要打开此页，请在导航树中选择 **System Management > LLDP Properties** （LLDP 属性）。

要启用 LLDP Properties，请选中 **Enable** 框。（默认情况下，此功能处于启用状态。）

要在接口上启用 LLDP Properties，请选中 **Enable**、 **WAN1** 或 **WAN2** 框。（默认情况下，这些功能处于启用状态。）

LLDP Neighbor （LLDP 邻居）表显示以下信息：

- **Local Port** （本地端口） - 端口标识符。
- **ChassisID Subtype** （机箱 ID 子类型） - 机箱 ID 的类型 （例如， MAC 地址）。
- **ChassisID** （机箱 ID） - 机箱的标识符。如果机箱 ID 子类型为 MAC 地址，则会显示设备的 MAC 地址。
- **Port ID Subtype** （端口 ID 子类型） - 端口标识符的类型。

- **Port ID** - 端口标识符。
- **System Name** - 设备的名称。
- **Time to Live** （存活时间） - 发送 LLDP 通告更新的速率 （以秒为单位）。

使用诊断

Diagnostic 页面可访问 DNS Name Lookup （DNS 名称查询）和 Ping 这两个内置工具。如果怀疑存在连接问题，可使用这些工具检查原因。

要打开此页，请选择 **System Management > Diagnostic**。

要使用 DNS 获取 IP 地址，请选择 **DNS Lookup** （DNS 查询），输入 **Lookup Domain Name** （查询域名），例如 www.cisco.com，然后单击 **Go** （转至）。系统将显示 IP 地址。

对指向指定主机的连接进行测试，请选择 **Ping**，输入 IP 地址或主机名，然后单击 **Go**。如果不知道 IP 地址，请使用 DNS Lookup 工具获取。 Ping 可显示设备是否能够向远程主机发送数据包并接收响应。

如果测试成功，则系统会显示以下信息：

- **Status** - 测试的状态：Testing （正在测试）、 Test Succeeded （测试成功）或 Test Failed （测试失败）
- **Packets** （数据包） - Ping 测试过程中传输的数据包数量、接收的数据包数量以及数据包丢失率
- **Round Trip Time** （往返时间） - Ping 测试的最短、最长和平均往返时间

出厂默认设置

要打开此页，请选择 **System Management > Factory Default** （出厂默认设置）。

要重新启动设备并将所有参数还原为出厂默认值，请单击 **Factory Default**。

要将设备恢复为出厂默认设置 （包括默认证书），请单击 **Factory Default Including Certificates** （包含证书的出厂默认设置）。

固件升级

利用此功能，可从 PC 或 USB 闪存驱动器中下载设备固件并进行安装。此窗口显示当前正在设备上运行的 **Firmware Version**。

注 如果选择较早版本的固件，则设备可能重置为出厂默认值。建议在升级固件之前，先操作备份和恢复步骤备份配置。

升级固件的过程可能需要数分钟时间。

在此过程中，请勿关闭电源、按重置按钮、关闭浏览器或断开链路。

要打开此页，请选择 **System Management > Firmware Upgrade** （固件升级）。

要从 PC 上传固件，请选择 **Firmware Upgrade from PC** （从 PC 升级固件）并浏览文件。

要从 USB 闪存驱动器中上传固件，请选择 **Firmware Upgrade from USB** （从 USB 中升级固件）并选择文件。

语言设置

语言包可以上传至设备。该窗口显示语言环境、语言版本和 Language MD5 Checksum （语言 MD5 校验和）。

要打开此页，请选择 **System Management > Language Setup** （语言设置）。

添加或更新语言的步骤：

步骤 1 从 **Mode** （模式）菜单中选择 **Add**、 **Update** （更新）或 **Delete**。

步骤 2 输入 **New Language Name** （新语言名称）。

步骤 3 浏览 **Language File Name** （语言文件名称）。

步骤 4 单击 **Save**。

重新启动

从 Restart （重新启动）页面重新启动时，路由器会在设备重置之前发送日志文件（如果日志记录已启用）。系统会保留设备的参数。

要打开此页，请在导航树中选择 **System Management > Restart**。

要重新启动设备，请单击 **Restart Router** （重新启动路由器）。

备份和恢复

可以导入、导出和复制配置文件。路由器有两个管理型配置文件，即启动和镜像。当设备启动运行配置并将启动文件复制到镜像文件时，会从存储器中加载启动文件。因此，镜像文件包含最新的有效配置。

如果由于某种原因启动配置文件已被破坏或失败，则使用镜像配置文件。稳定运行 24 小时 （在 24 小时内未重新启动且配置未更改）后，路由器会自动将启动配置复制到镜像配置。

从配置文件恢复设置

从以前保存到 PC 或 USB 闪存驱动器的文件中恢复启动配置的步骤：

步骤 1 在 Restore Startup Configuration File （恢复启动配置文件）部分，选择 **Restore Startup Configuration File from PC** （从 PC 恢复启动配置文件），然后单击 **Browse** （浏览）。或者选择 **Restore Startup Configuration File from USB** （从 USB 中恢复启动配置文件），然后单击 **Refresh**。

步骤 2 选择配置文件 (.config)。

步骤 3 单击 **Restore** （恢复）。此过程最多可能需要 1 分钟时间。如果配置文件包含的密码不同于当前设备的管理密码，则恢复配置文件之前，系统会要求您输入此密码。

步骤 4 在导航树中单击 **System Management > Restart**。

使用 **System Management > Restart** 重新启动设备后，系统才会应用导入的设置。

或者，也可以按住设备上的 **Reset** 按钮一秒钟后再松开，即可重新启动路由器。

备份配置文件和镜像文件

将启动和镜像配置文件保存到计算机或 USB 闪存驱动器，具体步骤：

步骤 1 选择 **Backup Configuration File to PC** （将配置文件备份到 PC）或 **Backup Configuration File to USB** （将配置文件备份到 USB）。

步骤 2 单击 **Backup Startup Configuration** （备份启动配置）或 **Backup Mirror Configuration** （备份镜像配置）。系统将显示 File Download （文件下载）窗口。

步骤 3 单击 **Save** 并选择保存文件的位置。也可以输入文件名后单击 **Save**。

提示 默认的文件名是 *Startup.config* 和 *Mirror.config*。需要 *.config* 扩展名。为方便识别，输入包括当前日期和时间的文件名可能十分有用。

将镜像文件复制到启动文件

可以手动将设备的启动配置文件复制到镜像配置文件。

可以在更改启动配置之前使用此过程对已知的良好配置进行备份。

- 每隔 24 小时，启动配置文件都会自动复制到镜像配置文件。
- 当您保存对设备参数的更改时，时间计数器将重置，启动配置文件将在 24 小时后进行下一次自动复制，除非您手动强制将启动文件另存为镜像文件。

要将启动文件复制到镜像文件，请单击 **Copy Mirror to Startup** （将镜像文件复制到启动文件）。复制操作会立即执行，且无法取消。操作完成后，页面将刷新。

清理配置

清理配置功能会删除镜像文件和启动文件。

要删除镜像文件和启动文件，请单击 **Sanitize Configuration** （清理配置）。

注意 删除镜像文件操作会立即执行，且无法取消，设备会重新启动并恢复到出厂默认设置。

将固件备份到 **USB** 闪存驱动器

要将固件备份到 USB 端口上的闪存驱动器，请从下拉菜单中选择端口，然后单击 **Backup** （备份）。设备会将固件图像另存为 **`image.bin`**。

6

端口管理

使用 Port Management （端口管理）配置端口设置并查看端口状态。

可以启用端口镜像，禁用端口或设置优先级、速度、双工模式和自动协商。也可以启用基于端口的 VLAN 来控制网络中设备之间的流量。

配置端口

可以设置端口镜像并管理端口，包括优先级和模式。端口镜像用于将一个端口上看到的网络数据包的副本发送到另一端口上的网络镜像连接。它经常用于需要进行网络流量监控的网络应用 （例如入侵检测系统）。思科系统交换机上的端口镜像通常也称为交换端口分析器 (SPAN)。

网络工程师或管理员使用端口镜像分析并调试数据或诊断网络上的错误。此功能有助于您监控网络性能并在出现问题时向您发送警报。

注 启用 **MAC** 地址克隆后，端口镜像将无法工作。

要打开此页，请在导航树中选择 **Port Management > Port Setup** （端口设置）。

RV320：要启用端口镜像，请选中 **Enable Mirror Port** （启用镜像端口）。 WAN 和 LAN 2-4 上的传入和传出数据包将复制到 LAN1。

RV325：要启用端口镜像，请选中 **Enable Mirror Port** （启用镜像端口）。 LAN 2-14 上的传入和传出数据包将复制到 LAN1。

每个端口都会显示以下只读信息：

- **Port ID -** 端口号或名称，与设备标签上的内容相同
- **Interface -** 接口类型：LAN、 WAN 或 DMZ

输入以下设置：

- **Disable -** 选中此框可禁用端口。默认情况下，所有端口都为启用状态。
- **Priority -** 对于每个端口，请选择合适的优先级级别， **High** 或 **Normal**。这可为特定端口上的设备设置流量优先级，从而确保服务质量 (QoS)。例如，您可能会为用于游戏或视频会议的端口分配 High 优先级。默认的设置为 Normal。

- **Mode -** 端口速度与双工模式。选择 **Auto Negotiation** 后，设备会与连接的设备自动协商连接速度和双工模式。

端口状态

端口状态显示端口状态的概要。单击 **Refresh** 可更新数据。

要打开此页，请在导航树中选择 **Port Management > Port Status** （端口状态）。

以太网表显示以下信息：

- **Port ID -** 端口的位置。
- **Type -** 端口类型。
- **Link Status -** 连接的状态。
- **Port Activity -** 端口的状态。
- **Priority -** 在 Port Setup 窗口中设置的端口优先级。
- **Speed Status -** 端口的速度， 10 Mbps 或 100 Mbps 或 1000 Mbps。
- **Duplex Status -** 双工模式， *Half* 或 *Full*。
- **Auto negotiation -** 双工模式的状态。

流量统计信息

要打开此页，请在导航树中选择 **Port Management > Traffic Statistics** （流量统计信息）。

对于所选端口， Statistics （统计信息）表中显示以下内容：

- **Port ID -** 端口的位置。
- **Link Status -** 连接的状态。
- **Rx Packets** （接收的数据包） **-** 端口上接收的数据包数量。
- **Rx Packets -** 接收的数据包数量 （以字节为单位）。
- **Tx Packets** （发送的数据包） **-** 端口上发送的数据包数量。

- **Tx Packets** - 发送的数据包数量 （以字节为单位）。
- **Packet Error** （数据包错误） - 数据包错误的数量。

VLAN 成员关系

默认情况下，所有 LAN 端口都在 VLAN 1 上。

要打开此页，请在导航树中选择 **Port Management > VLAN Membership** （VLAN 成员关系）。

要启用 VLAN，请选中 **VLAN Enable** （VLAN 启用）。

添加或编辑 VLAN 的步骤：

- **VLAN ID** - VLAN 的标示符。
- **Description** - 此 VLAN 的说明。
- **Inter VLAN Routing** （VLAN 间路由） - 允许在 VLAN 之间传输数据包。禁用了 VLAN 间路由的 VLAN 会与其他 VLAN 隔离。可以配置防火墙访问规则，以进一步控制 （允许或拒绝） VLAN 间流量。
- （**RV320**）**LAN 1** 到 **LAN 4** - 可以对端口进行标记、取消标记或从 VLAN 中排除。
- （**RV325**） **LAN 1** 到 **LAN 14** - 可以对端口进行标记、取消标记或从 VLAN 中排除。

Qos：CoS/DSCP 设置

此选项通过服务等级 (CoS) 对流量进行分组，为指定的服务确保带宽和较高的优先级。所有未添加至 IP 组的流量都使用 Intelligent Balancer （智能平衡器）模式。

要打开此页，请在导航树中选择 **Port Management > Qos:CoS/DSCP Setting** （Qos：CoS/DSCP 设置）。

要配置服务队列，请从下拉菜单中选择 **Queue** （队列）优先级 （4 是最高级别， 1 是最低级别）。

要设置差分服务代码点 (DSCP)，请从下拉菜单中选择 **Queue**。

DSCP 标记

差分服务代码点或 DiffServ 指定了一种简单、可扩展的方法，用于分类和管理网络流量并提供服务质量 (QoS)。 DiffServ 可用于向关键网络流量 （例如语音或流媒体）提供低延迟，同时向非关键服务 （例如 Web 流量或文件传输）提供简单的尽力服务。

要打开此页，请在导航树中选择 **Port Management > DSCP Marking** （DSCP 标记）。

要配置服务队列，请单击 **Add** 或 **Edit**，然后设置 Cos/802.1p Values （值）、 Action （操作）并输入 Priority。

802.1X 配置

基于端口的网络访问控制使用 IEEE 802 LAN 基础设施的物理访问权限特性提供了一种有效的方法，对连接到具有点对点连接特性的 LAN 端口的设备进行验证和授权，以及在验证和授权失败的情况下阻止访问该端口。此环境中的一个端口是连接到 LAN 基础设施的一个单独的点。

要打开此页，请在导航树中选择 **Port Management > 802.1X Configuration** （802.1X 配置）。

配置基于端口的验证的步骤：

步骤 1 选中 **Port-based Authentication** （基于端口的验证）以启用该功能。

步骤 2 输入 RADIUS 服务器的 IP 地址。

步骤 3 输入 **RADIUS UDP Port** （RADIUS UDP 端口）号。

步骤 4 输入 **RADIUS Secret** （RADIUS 安全密钥）。

步骤 5 从下拉菜单的 Port （端口）表中选择 **Administration State** （管理状态）：

- **ForceAuthorized** （强制授权） - 无需授权。强制授权 LAN 端口后，连接到该 LAN 端口的 PC 必须具有静态 IP 地址。*必须* 强制授权*至少一个 LAN 端口*。
- **Force Unauthorized** （强制未授权） - 受控的端口状态设置为丢弃流量；数据包无法传输。
- **Auto** - 启用基于端口的验证。根据设备与客户端之间的验证交换，接口在授权状态和未授权状态之间转换。

步骤 6 单击 **Save**。

7

防火墙

防火墙的主要目的是根据预定规则集，分析数据包并确定是否允许其通过，从而控制传入和传出网络流量。网络防火墙在内部网络和另一网络之间构建了一个桥梁，前者通常认为是安全可信的，后者通常认为是不安全且不受信任的外部 （间）网络 （例如互联网）。

通用

通用防火墙控件管理通常由互联网浏览器和应用程序使用的功能。

要打开此页，请在导航树中选择 **Firewall > General** （通用）。

启用防火墙功能

要启用 **Firewall**，请选中 **Enable**。可根据需要启用或禁用以下防火墙功能：

- **SPI** （数据包状态检测） **-** 监控数据包在网络上进行传输时网络连接 （例如 TCP 流和 UDP 通信）的状态。防火墙区分不同连接类型的合法数据包。只有符合已知活动连接的数据包才允许通过防火墙；其他数据包则被拒绝。
- **DoS** （拒绝服务） **-** 检测导致服务器过载的尝试次数。总体而言， DoS 攻击通过以下三种方式实现：强制重置目标计算机、消耗资源使其无法再提供目标服务，以及阻碍目标用户和受害者之间的通信媒体使他们无法再充分通信。
- **Block WAN Request -** 丢弃 TCP 请求和 ICMP 数据包。
- **Remote Management -** 启用后允许远程管理设备。默认情况下，端口为 443。它可以更改为任何用户定义的端口。字符串将为 https://<wan-ip>:<remote-management-port>
- **Multicast Pass Through** （组播通过） **-** 允许组播消息通过设备。
- **HTTPS -** 超文本传输协议安全是一种通信协议，用于在计算机网络上实现安全通信，尤其广泛部署于互联网上。
- **SSL VPN -** 允许 SSL VPN 连接。

- **SIP ALG -** 增强防火墙或 NAT 的应用层网关。利用它，可以将自定义 NAT 遍历过滤器插入网关支持地址和端口转换，从而执行 SIP *控制／数据*协议。
- **UPnP -** 通用即插即用是一套网络协议，可实现各种网络设备 （例如个人电脑、打印机、互联网网关、 Wi-Fi 接入点和移动设备）在网络上的相互无缝连接，并为数据共享和通信建立功能正常的网络服务。

限制 **Web** 功能

要限制 Web **Java**、**Cookies**、**ActiveX** 或 **Access to HTTP Proxy Servers**（访问 HTTP 代理服务器）功能，请选中该复选框。

要*仅*允许选定的功能 （Java、 Cookies、 ActiveX 或 Access to HTTP Proxy Servers）并限制所有其他功能，请启用 **Exception** （例外情况）。

配置受信任的域名

要添加受信任的域，请单击 **Add** 并输入 **Domain Name**。

要编辑受信任的域，请单击 **Edit**，然后修改 **Domain Name**。

访问规则

访问规则通过允许或拒绝由 IP 地址标识的特定服务或设备的访问，来限制对子网的访问权限。

要打开此页，请在导航树中选择 **Firewall > Access Rules** （访问规则）。

要添加或编辑服务，请单击 **Service Management**。此功能在添加或编辑服务名称中有介绍。

将访问规则添加到 **IPv4** 访问规则表

添加 （或编辑） IPv4 访问规则的步骤：

步骤 1 单击 **IPv4** 选项卡。

步骤 2 单击 **Add** （或选择相应行，然后单击 **Edit**）。

步骤 3 从下拉菜单中为此规则选择 Action、 **Allow** （允许）或 **Deny** （拒绝）。

步骤 4 请从下拉菜单中选择 **Service**。

步骤 5 选择 **Log packets matching this rule** （记录与此规则相匹配的数据包）或 **No Log**（无日志）。

步骤 6 从下拉菜单中选择 **Source Interface** （源接口）。

步骤 7 从下拉菜单中选择 **Source IP** 地址。如果选择了 **Single** （单个），请输入源 IP 地址。如果选择了 **Range**，请输入源 IP 地址的范围。

步骤 8 从下拉菜单中选择 **Destination IP** 地址。如果选择了 **Single**，请输入目标 IP 地址。如果选择了 **Range**，请输入目标 IP 地址的范围。

步骤 9 选择时间，为此访问规则配置 **Scheduling** （调度）。选择 **Always** （始终），则该访问规则全天 24 小时都有效。选择 **Interval** （时间间隔）可设置时间，并在 **From** （起始时间）和 **To** （终止时间）字段中输入访问规则生效的小时、分钟数。例如，*07:00* 至 *20:00*。访问规则不允许设置两个时间间隔。

步骤 10 选择一周中的 **Effective On** （生效天数）。

步骤 11 单击 **Save**。

将访问规则添加到 **IPv6** 访问规则表

添加 （或编辑） IPv6 访问规则的步骤：

步骤 1 单击 **IPv6** 选项卡。

步骤 2 单击 **Add** （或选择相应行，然后单击 **Edit**）。

步骤 3 从下拉菜单中为此规则选择 Action、 **Allow** 或 **Deny**。

步骤 4 从下拉菜单中选择 **Service**。

步骤 5 从下拉菜单中选择 **Log** （日志）。

步骤 6 从下拉菜单中选择 **Source Interface**。

步骤 7 从下拉菜单中选择 **Source IP Prefix Length** （源 IP 前缀长度）。如果选择了 **Single**，请输入源 IP 前缀。如果选择了 **Range**，请输入起始 IP 前缀和前缀长度。

步骤 8 从下拉菜单中选择 **Destination Prefix Length** （目标前缀长度）。如果选择了 **Single**，请输入目标 IP 前缀。如果选择了 **Range**，请输入起始 IP 前缀和前缀长度。

步骤 9 单击 **Save**。

内容过滤器

内容过滤器用于拒绝指定的包含特定关键字的域和网站。内容过滤器允许或拒绝指定的包含特定关键字的域和网站。

要打开此页，请在导航树中选择 **Firewall > Content Filter** （内容过滤器）。

阻止已禁止的域

阻止域的步骤：

步骤 1 选择 **Block Forbidden Domains** （阻止已禁止的域）。

步骤 2 在 **Forbidden Domains** （已禁止的域）表格中添加 （或编辑）域。

步骤 3 在 **From** 和 **To** 字段中输入访问规则生效的小时、分钟数来设置时间。

步骤 4 选择一周中的 **Effective On** 天数。

步骤 5 单击 **Save**。

阻止网站关键字

阻止网站关键字的步骤：

步骤 1 选择 **Block Forbidden Domains**。

步骤 2 在 **Website Blocking by Keywords** （按关键字阻止网站）表中单击 **Add** （或 **Edit**）。

步骤 3 在 **Keyword** （关键字）列中输入文字。

步骤 4 单击 **Save**。

接受允许的域

接受指定域的步骤：

步骤 1 选择 **Accept Allowed Domains** （接受允许的域)。

步骤 2 在 **Allowed Domains** （允许的域）表中单击 **Add** （或 **Edit**）。

步骤 3 在 **Domain Name** 列中输入名称。

步骤 4 单击 **Save**。

调度

在选定天数的特定时间内可以调度限制。

调度时间和天数的步骤：

步骤 1 从下拉菜单中选择 **Time**。选择 **Always**，则该规则全天 24 小时都有效。选择 **Interval** 可设置时间。

步骤 2 如果在步骤 1 中选择了 Always，请跳至 步骤 4。如果选择了 Interval，请在 **From** 和 **To** 字段中输入访问规则生效的小时、分钟数来设置时间。例如， *07:00* 至 *20:00*。内容过滤器不允许设置两个时间间隔。

步骤 3 选中一周中的 **Effective On** 天数。

步骤 4 单击 **Save**。

8

VPN

VPN 是在不同网络的两个端点之间建立的连接，它可以确保用户在共享网络或公共网络（例如互联网）上安全地发送私人数据。该隧道建立起了一种专用网络，能够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。

摘要

此功能显示了有关 VPN 隧道设置的一般信息。设备最多可支持 100 个隧道。为 EasyVPN 用户或与启用了 Mode Configuration （模式配置）选项 （如带预共享密钥的 **IKE** 和带证书的 **IKE** 的高级设置中所述）的设备相连接的 VPN 客户端保留 Virtual IP Range （虚拟 IP 范围）。

要打开此页，请在导航树中选择 **VPN > Summary** （摘要）。

要设置用于 VPN 隧道的 IP 地址范围，请单击 **Edit** 并输入以下参数：

- **Range Start** 和 **Range End** - 用于 VPN 隧道的 IP 地址范围的起始和结束地址。
- **DNS Server 1** 和 **DNS Server 2** - DNS 服务器的可选 IP 地址。如果输入第二个 DNS 服务器，则设备将使用第一个 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。使用默认设置 0.0.0.0 可使用动态分配的 DNS 服务器。
- **WINS Server1** （WINS 服务器 1）和 **WINS Server 2** （WINS 服务器 2） - WINS 服务器的可选 IP 地址。 Windows 互联网命名服务会将 NetBIOS 名称解析为 IP 地址。如果不知道 WINS 服务器的 IP 地址，请使用默认值 0.0.0.0。
- **Domain Name 1** （域名 1）到 **4** - 如果此路由器具有静态 IP 地址和注册域名，例如 *MyServer.MyDomain.com*，请输入 **Domain Name** 进行验证。该域名仅可用于一个隧道连接。

VPN Tunnel Status （VPN 隧道状态）显示 **Tunnels Used** （使用的隧道）、 **Tunnels Available** （可用的隧道）、 **Tunnels Enabled** （启用的隧道）和 **Tunnels Defined** （定义的隧道）的数量。

隧道状态连接表

该 Connection Table （连接表）显示在 **VPN** > 网关对网关 和 **VPN** > 客户端到网关中创建的条目：

- （隧道）**No** （号） - 自动生成的隧道 ID 号。
- （隧道） **Name** - 此 VPN 隧道的名称，例如 Los Angeles Office、 Chicago Branch 或 New York Division。此描述仅供参考；无需与隧道另一端使用的名称相匹配。
- **Status** - VPN 隧道的状态， *Connected* 或 *Waiting for Connection （等待连接）*。
- **Phase2 Enc/Auth/Grp** （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)。
- **Local Group** （本地组） - Local Group 的 IP 地址和子网掩码。
- **Remote Group** （远程组） - Remote Group 的 IP 地址和子网掩码。
- **Remote Gateway** （远程网关） - Remote Gateway 的 IP 地址。
- **Tunnel Test** （隧道测试） - VPN 隧道的状态。

组 **VPN** 状态连接表

该连接表显示在 **VPN** > 客户端到网关中创建的条目：

- **Group Name** - 此 VPN 隧道的名称。此描述仅供参考；无需与隧道另一端使用的名称相匹配。
- **Tunnels** （隧道数） - 登录到组 VPN 的用户数。
- **Phase2 Enc/Auth/Grp** - 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)。
- **Local Group** - Local Group 的 IP 地址和子网掩码。
- **Remote Client** （远程客户端） - Remote Client 的 IP 地址和子网掩码。
- **Details** （详情） - Remote Gateway 的 IP 地址。
- **Tunnel Test** - VPN 隧道的状态。

网关对网关

在站点到站点或网关对网关 VPN 中，一个办公室的本地路由器可以通过 VPN 隧道连接到远程路由器。客户端设备可以访问网络资源，如同它们都在同一个站点一样。此模式可用于远程办公室中的多个用户。

要打开此页，请在导航树中选择 **VPN > Gateway to Gateway** （网关对网关）。

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

隧道两端不能在相同的子网上。例如，如果站点 A LAN 使用 192.168.1.x/24 子网，则站点 B 可以使用 192.168.2.x/24。

要配置隧道，请在配置这两个路由器时输入相应的设置 （将*本地*和*远程*反向）。假设此路由器标识为 Router A。请在 *Local Group Setup （本地组设置）*部分输入其设置；在 *Remote Group Setup （远程组设置）*部分输入另一路由器 （Router B）的设置。配置另一个路由器 （Router B）时，请在 *Local Group Setup* 部分输入其设置，并在 *Remote Group Setup* 部分输入 Router A 的设置。

添加新隧道

输入隧道的以下设置：

- **Tunnel No** （隧道号） - 隧道的 ID 号。
- **Tunnel Name** （隧道名称） - 此 VPN 隧道的名称，例如 Los Angeles Office、Chicago Branch 或 New York Division。此描述仅供参考。无需与隧道另一端使用的名称相匹配。
- **Interface** - 此隧道使用的 WAN 端口。
- **Keying Mode** （密钥模式） - 标识隧道安全性：Manual、IKE with Preshared Key （带预共享密钥的 IKE）、 IKE with Certificate （带证书的 IKE）。
- **Enable** - 选中此框可启用 VPN 隧道，或取消选中此框可禁用该隧道。默认情况下，启用该隧道。

本地组设置

为此路由器输入 Local Group Setup 的设置。（配置另一个路由器上的 VPN 隧道时，请镜像这些配置。)

注 所有选项都会记录下来，但是只有那些与选定的参数相关的选项才会显示。

密钥模式 = 手动或带预共享密钥的 **IKE** 选项

- **Local Security Gateway Type** （本地安全网关类型） - 标识路由器以建立 VPN 隧道的方法。 Local Security Gateway （本地安全网关）在此路由器上，而 Remote Security Gateway （远程安全网关）则在另一个路由器上。其中至少有一个路由器必须拥有静态 IP 地址或 DNS 主机名才可建立连接。
  - **IP Only**（仅 IP）- 此路由器具有静态 WAN IP 地址。WAN IP 地址会自动显示。
  - **IP + Certificate**（IP + 证书）- 此路由器具有会自动显示的静态 WAN IP 地址。仅当选择 IKE with Certificate 时，此选项才可用。
  - **IP + Domain Name (FQDN) Authentication** （IP + 域名 (FQDN) 验证） - 此设备具有静态 IP 地址和注册域名，例如 *MyServer.MyDomain.com*。此外，也可输入 **Domain Name** 进行验证。该域名仅可用于一个隧道连接。
  - **IP + E-mail Addr.(USER FQDN) Authentication** （IP + 电子邮件地址 (用户 FQDN) 验证） - 此设备具有静态 IP 地址，且使用电子邮件地址进行验证。 WAN IP 地址会自动显示。输入 **Email Address** （电子邮件地址）可进行验证。
  - **Dynamic IP + Domain Name (FQDN) Authentication** （动态 IP + 域名 (FQDN) 验证） - 此路由器拥有动态 IP 地址和注册的动态 DNS 主机名（DynDNS.com 等供应商处有提供）。输入 **Domain Name** 可进行验证。该域名仅可用于一个隧道连接。
  - **Dynamic IP + E-mail Addr.(USER FQDN) Authentication** （动态 IP + 电子邮件地址 (用户 FQDN) 验证） - 此路由器拥有动态 IP 地址但没有动态 DNS 主机名。输入 **Email Address** 可进行验证。

    如果两个路由器都拥有动态 IP 地址 （如 PPPoE 连接），请勿同时为两个网关选择 **Dynamic IP + Email Addr.** （动态 IP + 电子邮件地址）。对于远程网关，请选择 **IP Address** 和 **IP Address by DNS Resolved** （DNS 解析的 IP 地址）。

密钥模式 = 带证书的 **IKE** 选项

- **Local Security Gateway Type -** 可以使用此隧道的 LAN 资源。唯一选项是 **IP + Certificate** （IP + 证书）。
  - **IP Address -** 显示设备的 WAN IP 地址。
- **Local Certificate** （本地证书） **-** 可以在 Certificate Management （证书管理） > 我的证书窗口中使用的证书。请从下拉菜单中选择相应的证书。

  Self-Generator （自生成器）显示证书生成器窗口。

  Import Certificate （导入证书）显示我的证书窗口。
- **Local Security Group Type** （本地安全组类型） **-** 允许选择单个 **IP** 地址、**Subnet** （子网）或子网内的 **IP** （地址） **Range**。
  - **IP Address -** 指定可以使用此隧道的一个设备。输入设备的 **IP Address**。
  - **Subnet -** 允许子网上的所有设备使用 VPN 隧道。输入子网的 **IP Address** 和 **Subnet Mask**。
  - **Begin IP** （起始 IP）和 **End IP** （结束 IP）（IP 范围） **-** 可以使用 VPN 隧道的设备范围。在 **Begin IP** 中输入第一个 IP 地址并在 **End IP** 中输入最后一个 IP 地址。

远程组设置选项

输入此路由器的 Remote Group Setup 的设置：

- **Remote Security Gateway Type**（远程安全网关类型） **-** 标识路由器以建立 VPN 隧道的方法。Remote Security Gateway 是另一个路由器。其中至少有一个路由器必须拥有静态 IP 地址或动态 DNS 主机名才可建立连接。
  - **IP Only -** 静态 WAN IP 地址。如果知道远程 VPN 路由器的 IP 地址，请选择 **IP Address**，然后输入地址。如果不知道远程 VPN 路由器的 IP 地址，请选择 **IP by DNS Resolved** （DNS 解析的 IP），然后输入路由器的域名。思科路由器可以获取 DNS 解析的远程 VPN 设备的 IP 地址。
  - **IP + Domain Name (FQDN) Authentication -** 此路由器具有静态 IP 地址和注册域名，例如 *MyServer.MyDomain.com*。如果知道远程 VPN 路由器的 IP 地址，请选择 **IP Address**，然后输入地址。如果不知道远程 VPN 路由器的 IP 地址，请选择 **IP by DNS Resolved**，然后输入路由器的域名。思科路由器可以获取 DNS 解析的远程 VPN 设备的 IP 地址。

- **IP + E-mail Address (USER FQDN) Authentication**（IP + 电子邮件地址 (用户 FQDN) 验证）- 此路由器具有静态 IP 地址，且可使用电子邮件地址进行验证。如果知道远程 VPN 路由器的 IP 地址，请选择 **IP Address**，然后输入 IP 地址。如果不知道远程 VPN 路由器的 IP 地址，请选择 **IP by DNS Resolved**，然后输入路由器的真实域名。思科路由器可以获取 DNS 解析的远程 VPN 设备的 IP 地址。
- **Dynamic IP + Domain Name (FQDN) Authentication** - 此路由器拥有动态 IP 地址和注册的动态 DNS 主机名 （DynDNS.com 等供应商处有提供）。输入 **Domain Name** 可进行验证。该域名仅可用于一个隧道连接。
- **Dynamic IP + E-mail Address (USER FQDN) Authentication** - 此路由器拥有动态 IP 地址但没有动态 DNS 主机名。输入 **Email Address** 可进行验证。如果两个路由器都拥有动态 IP 地址 （如 PPPoE 连接），请勿同时为两个网关选择 **Dynamic IP + Email Address**。对于远程网关，请选择 **IP Address** 或 **IP Address by DNS Resolved**。

- **Local Security Group Type** - 可以使用此隧道的 LAN 资源。 Local Security Group （本地安全组）对应于此路由器的 LAN 资源，而 Remote Security Group （远程安全组）对应于另一个路由器的 LAN 资源。
  - **IP Address** - 指定可以使用此隧道的一个设备。输入设备的 **IP Address**。
  - **Subnet** - 允许子网上的所有设备使用 VPN 隧道。输入子网的 **IP Address** 和 **Subnet Mask**。
  - **IP Range** - 可以使用 VPN 隧道的设备范围。在 **Begin IP** 中输入第一个 IP 地址并在 **End IP** 中输入最后一个 IP 地址。

IPSec 设置选项

要成功进行加密， VPN 隧道的两端必须就加密、解密和验证方法达成一致。在两个路由器上输入完全相同的设置。

输入 Phase 1 （第 1 阶段）和 Phase 2 （第 2 阶段）的设置。在 Phase 1 创建预共享密钥以建立安全验证通信通道。在 Phase 2，IKE 对端将使用安全通道代表 IPsec 等其他服务协商安全关联。为此隧道配置其他路由器时，请确保输入相同设置。

- **Phase 1 / Phase 2 DH Group** （第 1 阶段 / 第 2 阶段 DH 组） - DH (Diffie-Hellman) 是一个密钥交换协议。有三个主密钥长度不同的组：Group 1 （组 1） - 768 位、Group 2（组 2） - 1024 位，以及 Group 5（组 5） - 1536 位。若要较快的速度和较低的安全性，请选择 **Group 1**。若要较慢的速度和较高的安全性，请选择 **Group 5**。默认情况下选择 Group 1。

- **Phase 1 / Phase 2 Encryption**（第 1 阶段 / 第 2 阶段加密）- 此阶段的加密方法有：DES、 3DES、 AES-128、 AES-192 或 AES-256。加密方法决定了对 ESP 数据包进行加密或解密的密钥的长度。推荐使用 AES-256，因为这种方法更加安全。
- **Phase 1 / Phase 2 Authentication**（第 1 阶段 / 第 2 阶段验证）- 此阶段的验证方法为：MD5 或 SHA1。验证方法决定了 ESP （封装安全载荷协议）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。
- **Phase 1 / Phase 2 SA Life Time**（第 1 阶段 / 第 2 阶段 SA 有效期限）- VPN 隧道在此阶段处于活动状态的时间。 Phase 1 的默认值为 28800 秒。 Phase 2 的默认值为 3600 秒。
- **Perfect Forward Secrecy** （完全向前保密） - 如果启用了完全向前保密 (PFS)，则 IKE Phase 2 的协商将为 IP 流量加密和验证生成新的密钥资料。因此，试图强行破坏加密密钥的黑客将无法获取将来的 IPsec 密钥。选中此框可启用此功能，或取消选中此框可禁用此功能。建议使用此功能。
- **Preshared Key** （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（不支持 ' ' " \）。确保 VPN 隧道两端使用相同的 Preshared Key。强烈建议定期更改 Preshared Key，以便最大限度地提高 VPN 的安全性。
- **Minimum Preshared Key Complexity** （最低预共享密钥复杂性） - 选中 **Enable** 框可启用 Preshared Key Strength Meter （预共享密钥强度计）。
- **Preshared Key Strength Meter** - 启用 Minimum Preshared Key Complexity 后，该测量工具将会指示预共享密钥的强度。输入预共享密钥时，会出现彩色条。彩色条变化范围从红色 （弱）到黄色 （可接受），再到绿色 （强）。

提示 请输入一个复杂的预共享密钥，包括八个以上字符、大写和小写字母、数字和符号，例如 -*^+=。

带预共享密钥的 IKE 和带证书的 IKE 的高级设置

对于大多数用户，基本设置应足以满足其需求；高级用户可单击 **Advanced** （高级）显示高级设置。如果在某个路由器上更改了 Advanced 设置，则在另一个路由器上也要输入该设置。

- **Aggressive Mode** （Aggressive 模式） - IKE SA 协商包括以下两种模式：Main Mode （Main 模式）和 Aggressive Mode。如果网络安全是首选因素，建议选择 Main Mode。如果网络速度是首选因素，建议选择 Aggressive Mode。选中此框将启用 Aggressive Mode，取消选中此框将使用 Main Mode。

  如果 Remote Security Gateway Type 是 *Dynamic IP* 类型的一种，则必须使用 Aggressive Mode。此框将自动选中，且无法更改此设置。

- **Compress (Support IP Payload Compression Protocol (IP Comp))** （压缩（支持 IP 载荷压缩协议） (IP Comp)） - 可减小 IP 数据报大小的协议。选中此框，路由器将在启动连接时提议压缩。如果应答器拒绝此提议，则路由器不会实施压缩。将路由器用作应答器时，它将接受压缩，即使是在压缩未启用的情况下。如果在该路由器上启用此功能，则在隧道另一端的路由器上也应该启用此功能。

- **Keep-Alive** （持久连接） - 如果连接断开，则尝试重新建立 VPN 连接。

- **AH Hash Algorithm** （AH 散列算法） - 验证报头 (AH) 协议描述了数据包格式和数据包结构的默认标准。当 AH 作为安全协议时，保护作用将扩展到 IP 报头，以验证整个数据包的完整性。选中此框可使用此功能并可选择验证方法：MD5 或 SHA1。 MD5 生成 128 位摘要来验证数据包。 SHA1 生成 160 位摘要来验证数据包。隧道两端应使用相同的算法。

- **NetBIOS Broadcast** （NetBIOS 广播） - 广播消息用于 Windows 网络中的名称解析，以标识计算机、打印机和文件服务器等资源。某些软件应用程序和 “网上邻居” 等 Windows 功能将使用这些消息。 LAN 广播流量通常不会通过 VPN 隧道进行转发。但是，选中此框后， NetBIOS 广播就可从隧道的一端转播到另一端。

- **NAT Traversal** （NAT 遍历） - 使用网络地址转换 (NAT)，拥有专用 LAN 地址的用户可以通过将可公共路由的 IP 地址用作源地址来访问互联网资源。但是，对于入站流量， NAT 网关无法自动将公共 IP 地址转换为专用 LAN 上的特定目标。此问题将导致无法成功实现 IPsec 交换。如果 VPN 路由器在 NAT 网关之后，请选中此框以启用 NAT 遍历。隧道两端必须使用相同的设置。

- 失效对等体检测 **(DPD)**- 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 **Interval** 字段中指定 HELLO/ACK 消息之间的时间间隔。

- **Extended Authentication** （扩展验证） - 使用 IPsec 主机的用户名和密码验证 VPN 客户端或使用在 User Management （用户管理）中找到的用户数据库。 IPSec 主机和边缘设备都必须启用 Extended Authentication。要使用 **IPsec Host** （IPsec 主机），请单击该单选按钮并输入 **User Name** 和 **Password**。要使用 **Edge Device** （边缘设备），请单击该单选按钮并从下拉菜单中选择数据库。要添加或编辑数据库，请单击 **Add/Edit** （添加 / 编辑）以显示 User Management 窗口。

- **Tunnel Backup** （隧道备份） - 当 DPD 确定远程对端不可用时，利用该功能，路由器便可使用远程对端的备用 IP 地址或者备用本地 WAN 接口重新建立 VPN 隧道。选中此框可启用此功能并可输入以下设置。仅当 Dead Peer Detection 启用时，此功能才可用。

  - **Remote Backup IP Address**（远程备份 IP 地址） - 远程对端的备用 IP 地址，或者重新输入已为远程网关设置的 WAN IP 地址。

  - **Local Interface** （本地接口） - 用来重新建立连接的 WAN 接口。

  - **VPN Tunnel Backup Idle Time** （VPN 隧道备用空闲时间） - 当路由器启动并且主隧道未在指定时间内连接时，将使用备用隧道。默认空闲时间为 30 秒。

- **Split DNS** （拆分 DNS） - 根据指定的域名，将一些 DNS 请求发送至一个 DNS 服务器，将其他 DNS 请求发送至另一个 DNS 服务器。路由器收到来自客户端的地址解析请求时，将检查域名。如果该域名与 Split DNS 设置中的其中一个域名相匹配，则路由器会将此请求传递至指定的 DNS 服务器。否则，路由器会将此请求传递至 WAN 接口设置中指定的 DNS 服务器。

  DNS Server 1 和 **DNS Server 2** - 用于指定域的 DNS 服务器的 IP 地址。作为可选操作，也可以在 **DNS Server 2** 字段中指定辅助 DNS 服务器。

  Domain Name 1 （域名 1）至 **Domain Name 4** （域名 4） - 为 DNS 服务器指定域名。这些域的请求将被传递至指定的 DNS 服务器。

客户端到网关

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 TheGreenBow 等第三方 VPN 客户端软件访问网络。

要打开此页，请在导航树中选择 **VPN > Client to Gateway** （客户端到网关）。

为一个远程用户配置 VPN 隧道、为多个远程用户配置组 VPN 或配置 Easy VPN （简单 VPN）：

- **Tunnel** - 为单个远程用户创建隧道。隧道编号将自动生成。
- **Group VPN** （组 VPN） - 为一组用户创建隧道，从而避免了为单个用户配置的需要。所有的远程用户都可以使用相同的 Preshared Key 连接设备，数量高达所支持隧道的最大数量。路由器最多可支持两个 VPN 组。组编号将自动生成。
- **Easy VPN** - 允许远程用户通过使用思科 VPN 客户端（也称为 *Cisco Easy VPN Client （思科简单 VPN 客户端）*）实用程序 （产品 CD 上提供）连接此设备：
  - 版本 5.0.07 支持 Windows 7 （32 位和 64 位）、 Windows Vista （32 位和 64 位）和 Windows XP （32 位）
  - 版本 4.9 支持 Mac OS X 10.4 和 10.5
  - 版本 4.8 支持基于 Linux 的因特尔

  要将其设置为 Easy VPN，请在此页上配置组密码，并在用户管理部分的 User Management Table （用户管理表）中为每个思科 VPN 客户端用户添加用户名和密码。添加用户时，应该选择 Unassigned （未分配）组。其他组用于 SSL VPN。

配置隧道或组 **VPN**

输入以下信息：

- **Tunnel Name** - 描述隧道的名称。对于单个用户，可以输入用户名或位置。对于组 VPN，可以标识组的业务角色或位置。此描述仅供参考，无需与隧道另一端使用的名称相匹配。
- **Interface** - WAN 端口。

- **Keying Mode -** 选择关键管理方法：
  - **Manual -** 自己生成密钥，但不启用密钥协商。手动密钥管理用于小型静态环境或用于进行故障排除。输入所需设置。
  - **IKE** （互联网密钥交换）**with Preshared Key -** 使用此协议为隧道设置安全关联 (SA)。（建议使用此设置。）如果选择了 **Group VPN** （组 VPN），则这是唯一可用的选项。
  - **IKE with Certificate -** 使用证书验证远程 IKE 对端。
- **Enable -** 选中此框可启用此 VPN。

配置简单 **VPN**

输入以下信息：

- **Name -** 描述隧道的名称。对于单个用户，可以输入用户名或位置。此描述仅供参考，无需与隧道另一端使用的名称相匹配。
- **Minimum Password Complexity -** 启用该选项后，密码的最低要求如下：
  - 长度为八个字符。
  - 不能与用户名相同。
  - 不能与当前密码相同。
  - 至少包含以下 4 种字符类别中的 3 种：大写字母、小写字母、数字和可使用标准键盘输入的特殊字符 （不支持 ' ' " \）。
- **Password -** Easy VPN 密码。
- **Password Strength Meter -** 启用 Minimum Password Complexity 后，Password Strength Meter 会根据复杂性规则指示密码强度。彩色条变化范围从红色 （不可接受）到黄色 （可接受），再到绿色 （强）。
- **Interface -** 此隧道使用的 WAN 端口。
- **Enable -** 选中此框可启用 VPN 隧道，或取消选中此框可禁用该隧道。默认情况下，启用该隧道。
- **Tunnel Mode** （隧道模式） **- Split Tunnel** （拆分隧道）允许互联网预定的流量未经加密直接发送至互联网。 **Full Tunnel** （全隧道）将所有流量发送至头端设备，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）。
- **IP Address -** 分配给 VPN 接口的 IP 地址。
- **Subnet Mask -** 子网掩码。

- **Extended Authentication -** 使用 IPsec 主机的用户名和密码验证 VPN 客户端或使用在 User Management 中找到的用户数据库。要使用 **IPsec Host**，请单击该单选按钮并输入 **User Name** 和 **Password**。要使用 **Edge Device**，请单击该单选按钮并从下拉菜单中选择数据库。要添加或编辑数据库，请单击 **Add/Edit** 以显示 User Management 窗口。

本地组设置

输入以下信息：

- **Local Security Gateway Type -** 标识路由器以建立 VPN 隧道的方法。Remote Security Gateway 是另一个路由器。其中至少有一个路由器必须拥有静态 IP 地址或动态 DNS 主机名才可建立连接。
  - **IP Only -** 静态 WAN IP 地址。如果知道远程 VPN 路由器的 IP 地址，请选择 **IP Address**，然后输入地址。如果不知道远程 VPN 路由器的 IP 地址，请选择 **IP by DNS Resolved**，然后输入路由器的域名。思科路由器可以获取 DNS 解析的远程 VPN 设备的 IP 地址。
  - **IP + Domain Name (FQDN) Authentication -** 此设备具有静态 IP 地址和注册域名，例如 *MyServer.MyDomain.com*。如果知道远程 VPN 路由器的 IP 地址，请选择 **IP Address**，然后输入地址。如果不知道远程 VPN 路由器的 IP 地址，请选择 **IP by DNS Resolved**，然后输入路由器的域名。思科路由器可以获取 DNS 解析的远程 VPN 设备的 IP 地址。
  - **IP + E-mail Address (USER FQDN) Authentication -** 此设备具有静态 IP 地址，且使用电子邮件地址进行验证。如果知道远程 VPN 路由器的 IP 地址，请选择 **IP Address**，然后输入 IP 地址。如果不知道远程 VPN 路由器的 IP 地址，请选择 **IP by DNS Resolved**，然后输入路由器的真实域名。思科路由器可以获取 DNS 解析的远程 VPN 设备的 IP 地址。
  - **Dynamic IP + Domain Name (FQDN) Authentication -** 此路由器拥有动态 IP 地址和注册的动态 DNS 主机名 （DynDNS.com 等供应商处有提供）。输入 **Domain Name** 可进行验证。该域名仅可用于一个隧道连接。
  - **Dynamic IP + E-mail Address (USER FQDN) Authentication -** 此路由器拥有动态 IP 地址但没有动态 DNS 主机名。输入 **Email Address** 可进行验证。

    如果两个路由器都拥有动态 IP 地址 （如 PPPoE 连接），请勿同时为两个网关选择 Dynamic IP + Email Address。对于远程网关，请选择 **IP Address** 和 **IP Address by DNS Resolved**。

- **Local Security Group Type -** 指定可以访问此隧道的 LAN 资源。
  - **IP Address -** 选择此选项可仅允许一个 LAN 设备访问 VPN 隧道。然后输入计算机的 IP 地址。仅该设备可以使用此 VPN 隧道。
  - **Subnet -** 选择此选项 （默认选项）可允许子网上的所有设备访问 VPN 隧道。然后输入子网 IP 地址和掩码。
  - **IP Range -** 选择此选项可允许一系列设备访问 VPN 隧道。然后在 **Begin IP** 字段中输入第一个地址，并在 **End IP** 字段中输入最后一个地址，以确定 IP 地址范围。
- **Domain Name -** 如果选择使用域名验证，请输入域名。
- **Email** （电子邮件） **-** 如果选择使用电子邮件验证，请输入电子邮件地址。

单个用户的远程客户端设置

指定标识客户端的方法，以创建 VPN 隧道。 Single User （单个用户）或 *Tunnel* 类型、VPN 提供以下选项：

- **IP Only -** 远程 VPN 客户端具有静态 WAN IP 地址。如果知道客户端的 IP 地址，请选择 **IP Address**，然后输入地址。如果不知道客户端的 IP 地址，请选择 **IP by DNS Resolved**，然后输入客户端在互联网上的域名。路由器将获取使用 DNS 解析的远程 VPN 客户端的 IP 地址，远程 VPN 客户端的 IP 地址将显示在 Summary 页面的 VPN Status 部分。
- **IP + Domain Name (FQDN) Authentication -** 客户端具有静态 IP 地址和注册域名。此外，也可输入 **Domain Name** 进行验证。该域名仅可用于一个隧道连接。

  如果知道远程 VPN 客户端的 IP 地址，请选择 **IP Address**，然后输入地址。如果不知道远程 VPN 客户端的 IP 地址，请选择 **IP by DNS Resolved**，然后输入客户端在互联网上的真实域名。路由器将获取通过 DNS 解析的远程 VPN 客户端的 IP 地址，远程 VPN 客户端的 IP 地址将显示在 Summary 页面的 VPN Status 部分。
- **IP + Email Address (USER FQDN) Authentication -** 客户端具有静态 IP 地址，且可使用电子邮件地址进行验证。当前的 WAN IP 地址将会自动显示。输入任一 **Email Address** 可进行验证。

  如果知道远程 VPN 客户端的 IP 地址，请选择 **IP Address**，然后输入地址。如果不知道远程 VPN 客户端的 IP 地址，请选择 **IP by DNS Resolved**，然后输入客户端在互联网上的真实域名。设备将获取通过 DNS 解析的远程 VPN 客户端的 IP 地址，远程 VPN 客户端的 IP 地址将显示在 Summary 页面的 VPN Status 部分。
- **Dynamic IP + Domain Name (FQDN) Authentication -** 客户端拥有动态 IP 地址和注册的动态 DNS 主机名 （DynDNS.com 等供应商处有提供）。输入 **Domain Name** 可进行验证。该域名仅可用于一个隧道连接。
- **Dynamic IP + E-mail Addr.(USER FQDN) Authentication -** 客户端拥有动态 IP 地址但没有动态 DNS 主机名。输入任一 **Email Address** 可进行验证。

组的远程客户端设置

指定标识客户端的方法，以创建 VPN 隧道。 Group VPN 提供以下选项：

- **Domain Name (FQDN) Authentication** （域名 (FQDN) 验证） - 通过注册的域名标识客户端。输入 **Domain Name** 可进行验证。该域名仅可用于一个隧道连接。
- **Email Address (USER FQDN) Authentication** - 通过电子邮件地址标识客户端进行验证。在提供的字段中输入地址。
- **Microsoft XP/2000 VPN Client** （Microsoft XP/2000 VPN 客户端） - 客户端软件是内置的 Microsoft XP/2000 VPN Client。

IPSec 设置

要成功进行加密， VPN 隧道的两端必须就加密、解密和验证方法达成一致。在两个路由器上输入完全相同的设置。

输入 Phase 1 和 Phase 2 的设置。在 Phase 1 创建预共享密钥以建立安全验证通信通道。在 Phase 2，IKE 对端将使用安全通道为 IPsec 等其他服务协商安全关联。为此隧道配置其他路由器时，请确保输入相同设置。

- **Phase 1 / Phase 2 DH Group** - DH (Diffie-Hellman) 是一个密钥交换协议。有三个主密钥长度不同的组：Group 1 - 768 位、 Group 2 - 1024 位，以及 Group 5 - 1536 位。若要较快的速度和较低的安全性，请选择 **Group 1**。若要较慢的速度和较高的安全性，请选择 **Group 5**。默认情况下选择 Group 1。
- **Phase 1 / Phase 2 Encryption** - 此阶段的加密方法有：DES、 3DES、 AES-128、 AES-192 或 AES-256。加密方法决定了对 ESP 数据包进行加密或解密的密钥的长度。推荐使用 AES-256，因为这种方法更加安全。
- **Phase 1 / Phase 2 Authentication** - 此阶段的验证方法为：MD5 或 SHA1。验证方法决定了 ESP （封装安全载荷协议）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。
- **Phase 1 / Phase 2 SA Life Time** - VPN 隧道在此阶段处于活动状态的时间。Phase 1 的默认值为 28800 秒。 Phase 2 的默认值为 3600 秒。
- **Perfect Forward Secrecy** - 如果启用了完全向前保密 (PFS)，则 IKE Phase 2 的协商将为 IP 流量加密和验证生成新的密钥资料。因此，试图强行破坏加密密钥的黑客将无法获取将来的 IPsec 密钥。选中此框可启用此功能，或取消选中此框可禁用此功能。建议使用此功能。
- **Minimum Preshared Key Complexity** - 选中 **Enable** 框可启用 Preshared Key Strength Meter。

- **Preshared Key -** 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。确保 VPN 隧道两端使用相同的 Preshared Key。建议定期更改 Preshared Key，以便最大限度地提高 VPN 的安全性。
- **Preshared Key Strength Meter -** 启用 Minimum Preshared Key Complexity 后，该测量工具将会指示预共享密钥的强度。输入预共享密钥时，会出现彩色条。彩色条变化范围从红色 （弱）到黄色 （可接受），再到绿色 （强）。

提示 请输入一个复杂的预共享密钥，包括八个以上字符、大写和小写字母、数字和符号，例如 -*^+= （不支持 ' ' " \）。

带预共享密钥的 IKE 和带证书的 IKE 的高级设置

对于大多数用户，基本设置应足以满足其需求；高级用户可单击 **Advanced** 显示高级设置。如果在某个路由器上更改了 Advanced 设置，则在另一个路由器上也要输入该设置。

- **Aggressive Mode -** IKE SA 协商包括以下两种模式：Main Mode 和 Aggressive Mode。如果网络安全是首选因素，建议选择 Main Mode。如果网络速度是首选因素，建议选择 Aggressive Mode。选中此框将启用 Aggressive Mode，取消选中此框将使用 Main Mode。
  如果 **Remote Security Gateway Type** 是其中一种 *Dynamic IP* 类型，则必须使用 Aggressive Mode。此框将自动选中，且无法更改此设置。
- **Compress (Support IP Payload Compression Protocol (IP Comp)) -** 可减小 IP 数据报大小的协议。选中此框，路由器将在启动连接时提议压缩。如果应答器拒绝此提议，则路由器不会实施压缩。将路由器用作应答器时，它将接受压缩，即使是在压缩未启用的情况下。如果在该路由器上启用此功能，则在隧道另一端的路由器上也应该启用此功能。
- **Keep-Alive -** 如果连接断开，则尝试重新建立 VPN 连接。
- **AH Hash Algorithm -** 验证报头 (AH) 协议描述了数据包格式和数据包结构的默认标准。当 AH 作为安全协议时，保护作用将扩展到 IP 报头，以验证整个数据包的完整性。选中此框可使用此功能并可选择验证方法：MD5 或 SHA1。 MD5 生成 128 位摘要来验证数据包。 SHA1 生成 160 位摘要来验证数据包。隧道两端应使用相同的算法。
- **NetBIOS Broadcast -** 广播消息用于 Windows 网络中的名称解析，以标识计算机、打印机和文件服务器等资源。某些软件应用程序和 “网上邻居” 等 Windows 功能将使用这些消息。 LAN 广播流量通常不会通过 VPN 隧道进行转发。但是，选中此框后， NetBIOS 广播就可从隧道的一端转播到另一端。

- **NAT Traversal -** 使用网络地址转换 (NAT)，拥有专用 LAN 地址的用户可以通过将可公共路由的 IP 地址用作源地址来访问互联网资源。但是，对于入站流量， NAT 网关无法自动将公共 IP 地址转换为专用 LAN 上的特定目标。此问题将导致无法成功实现 IPsec 交换。如果 VPN 路由器在 NAT 网关之后，请选中此框以启用 NAT 遍历。隧道两端必须使用相同的设置。
- **Extended Authentication -** 用户在使用预共享密钥或证书进行验证的基础上，还可通过指定用户名和密码进一步验证传入的 IPSec 隧道请求。
  - **IPsec Host -** 表示使用 **IPsec Host** 进行扩展验证。
    User Name - 验证用户名。
    Password - 验证密码。
  - **Edge Device -** 从系统摘要窗口中配置的虚拟 IP 范围中，为传入隧道请求者提供一个 IP 地址 （进行验证之后）。请从下拉菜单中选择设备。要添加或编辑设备域，请单击 **Add/Edit** 以显示用户管理窗口。
- **Mode Configuration -** 从 VPN > 摘要窗口中配置的虚拟 IP 范围中，为传入隧道请求者提供一个 IP 地址 （进行验证之后）。

VPN 通道

借助 VPN Passthrough （VPN 通道）， VPN 客户端可通过路由器顺利连接至 VPN 端点。默认情况下，此选项为启用状态。

要打开此页，请在导航树中选择 **VPN > VPN Passthrough**。

要启用 VPN Passthrough，请为允许的协议选中 **Enable**：

- **IPSec Passthrough -** 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 Passthrough -** 点对点隧道协议 (PPTP) 允许通过 IP 网络传输点对点协议 (PPP)。
- **L2TP Passthrough -** 第 2 层隧道协议是一种通过第 2 层上的互联网来启用点对点会话的方法。

PPTP 服务器

最多可为运行 PPTP 客户端软件的用户启用 10 个 PPTP （点对点隧道协议） VPN 隧道。例如，在 Windows XP 或 2000 中，用户打开 Network Connections （网络连接）面板并创建一个新的连接。在向导中，用户选择该选项可使用 Virtual Private Network （虚拟专用网络）连接创建指向工作场所的连接。用户必须知道此设备的 WAN IP 地址。有关详情，请参阅有关操作系统的相关文档或帮助文件。

要打开此页，请在导航树中选择 **VPN > PPTP Server** （PPTP 服务器）。

要启用 PPTP 服务器并允许 PPTP VPN 隧道，请选中 **Enable** 框并输入地址范围：

Range Start 和 **Range End** - 分配给 PPTP VPN 客户端的 LAN 地址范围。用于 PPTP VPN 客户端的 LAN IP 地址范围应在路由器正常 DHCP 范围之外。

Connection Table 显示正在使用的隧道。 PPTP 用户帐户添加在用户管理窗口中（在 Group 列中选择 **Unassigned**。）

9

证书管理

数字证书通过指定的证书主体认证公共密钥的所有权。这允许其他方 （依赖方）依赖专用密钥 （其与经过认证的公共密钥相对应）所做的签名或断言。在这种信任关系模式中， CA 为证书的主体（所有者）和证书依赖方同时信任的可靠第三方。 CA 是许多公共密钥基础架构 (PKI) 机制的特性。

使用 Certificate Management （证书管理）可以生成并安装 SSL 证书。

我的证书

通过自签名或第三方授权最多可添加 50 个证书。还可以使用证书生成器创建证书，也可以从 PC 或 USB 设备中导入证书。

自签名 SSL 证书本身并不被浏览器所信任，虽然它们可用于加密，但确实可能导致浏览器显示警报消息，通知用户证书尚未由用户所选择信任的实体颁发。

即使 PC 上没有安装证书，用户也可以进行连接。在连接至 VPN 隧道时用户会看到安全警报，但仍可在不使用该额外安全保护功能的情况下继续连接。

要打开此页，请在导航树中选择 **Certificate Management > My Certificate**。

要将证书标识为主证书，请单击所需证书的单选按钮，然后单击 **Select as Primary Certificate** （选择为主证书）。

要显示证书信息，请单击 **Details** 图标。

导出或显示证书或专用密钥

客户端证书允许客户端连接到 VPN。导出或显示证书或专用密钥的步骤：

步骤 1 单击相关图标 **Export Certificate for Client** （导出客户端证书）或 **Export Certificate for Administrator** （导出管理员证书）或 **Export Private Key** （导出专用密钥）。系统将显示 File Download 窗口。

Export Certificate for Client - 允许客户端连接到 VPN 的客户端证书。

Export Certificate for Administrator - 包含专用密钥，可以导出副本作为备份文件。例如，在将设备重置为出厂默认设置之前，可以先导出此证书。在重新启动设备之后，再将此文件导入以恢复证书。

Export Private Key - 某些 VPN 客户端软件需要单独具有专用密钥、 CA 证书和证书的凭证。

步骤 2 单击 **Open** （打开）可显示该密钥。单击 **Save** 可保存该密钥。

导入第三方或自签名证书

无法授权或签名外部生成的证书签名请求 (CSR)；必须使用 **CSR** 授权添加外部 CSR。

导入证书的步骤：

步骤 1 单击 **Add**。

步骤 2 选择 **3rd-party Authorized** （第三方已授权）或 **Self Signed** （自签名）。

步骤 3 选择 **Import from PC** （从 PC 中导入）或 **Import from USB Device** （从 USB 设备中导入）。

步骤 4 浏览 **CA Certificate** （CA 证书）。（仅第三方。）

步骤 5 浏览 **Certificate and Private Key** （证书和专用密钥）（第三方或自签名）。

步骤 6 单击 **Save**。

受信任的 SSL 证书

安全套接字层 (SSL) 是一项标准安全技术，用于在 Web 服务器和浏览器之间创建加密的链路。此链路确保在 Web 服务器和浏览器之间传递的所有数据保持隐秘且完整。SSL 是一项行业标准，数以百万的网站用它来保护与客户的在线交易。Web 服务器需要 SSL 证书才能生成 SSL 链路。

SSL 证书由受信任的证书颁发机构颁发，不会显示警告并可在网站和浏览器之间以透明的方式建立安全链路。挂锁表明用户拥有某个企业的加密链路，该企业获得了受信任的证书颁发机构颁发的受信任的 SSL 证书。

要打开此页，请在导航树中选择 **Certificate Management > Trusted SSL Certificate** （受信任的 SSL 证书）。

Certificate Table （证书表）可用于认证并显示证书信息。

要查看有关证书的其他信息，请单击 **Details**。

要导入第三方证书，请单击 **Add**，然后导入证书：

步骤 1 选择 **Import from PC** 或 **Import from USB Device**。

步骤 2 浏览 **CA Certificate**。

步骤 3 单击 **Save**。

受信任的 IPsec 证书

IPsec 用于交换密钥生成和验证数据、密钥建立协议、加密算法或安全验证的验证机制以及验证与 SSL 证书的在线交易。

要打开此页，请在导航树中选择 **Certificate Management > Trusted IPsec Certificate** （受信任的 IPsec 证书）。

要显示证书信息，请单击 **Details** 图标。

要导出或显示证书，请单击 **Export Certificate** （导出证书）图标。出现一个弹出窗口，在此您可以 **Open** 此证书进行检测或将证书 **Save** 到 PC。

要导入第三方证书，请单击 **Add**，然后导入证书：

步骤 1 选择 **CA Certificate**。

步骤 2 选择 **Import from PC** 或 **Import from USB Device**。

步骤 3 浏览 **Certificate** （证书）。（第三方或自签名。）

步骤 4 单击 **Save**。

证书生成器

Certificate Request Generator （证书请求生成器）收集信息并生成专用密钥文件和证书请求。可以选择生成自签名证书或证书签名请求 (CSR) 便于外部证书颁发机构进行签名。保存配置后，生成的 CSR 或自签名证书会显示在我的证书下面。

要打开此页，请在导航树中选择 **Certificate Management > Certificate Generator**（证书生成器）。

生成证书的步骤：

步骤 1 输入以下参数：

- **Type** - 证书请求类型。
- **Country Name** （国家 / 地区名称） - 原产国 / 地区。
- **State or Province Name**（州或省 / 直辖市 / 自治区名称）- 州或省 / 直辖市 / 自治区 （可选）。
- **Locality Name** （城市名称） - 城市 （可选）。
- **Organization Name** （组织名称） - 组织 （可选）。
- **Organizational Unit Name** （组织单位名称） - 组织的子集。
- **Common Name** （通用名称） - 组织的通用名称。
- **Email Address** - 联系人的电子邮件地址 （可选）。
- **Key Encryption Length** （密钥加密长度） - 密钥的长度。
- **Valid Duration** （有效期） - 证书有效的天数。

步骤 2 单击 **Save**。系统将显示我的证书窗口。

CSR 授权

CSR （证书签名请求）是证书生成器生成的数字身份证书。在证书颁发机构 (CA) 签名之前，它不是一个完整的证书。此设备能作为 CA 在 Certificate Management>CSR Authorization 中签名 / 授权外部生成的 CSR。一旦此设备将外部生成的 CSR 签名之后，已签名的 CSR 就成为了受信任的证书，并移到了**受信任的 IPsec 证书**窗口。（要将设备配置恢复为出厂默认值，包括默认证书，请使用**出厂默认设置**窗口。）

对证书进行签名的步骤：

步骤 1 单击 **Browse** 显示 **Certificate Signing Request** （证书签名请求）。

步骤 2 要选择相应的专用密钥对 CSR 进行授权和签名，请选择该证书以便与 **My Certificate** 下拉菜单中的请求相关联。

步骤 3 单击 **Save**。

10

日志

日志使用陷阱或定期记录的方式记录系统的状态。

系统日志

配置短消息服务 (SMS) 日志和警报。

要打开此页，请在导航树中选择 **Log** > **System Log** （系统日志）。

配置系统日志发送 **SMS**

要为日志配置链路，请进行以下操作：

步骤 1 单击 **Enable**。

步骤 2 选择 **USB1** 或 **USB2**，通过 USB 端口发送日志。

步骤 3 选中 **Dial Number1** （拨号数字 1）和 / 或 **Dial Number2** （拨号数字 2）并输入要拨打的电话号码。

步骤 4 单击 **Test** （测试）可测试链路。

步骤 5 选择发送日志的时间：

- 链路建立时。
- 链路断开时。
- 验证失败时。
- 系统启动时。

步骤 6 单击 **Save**。

配置系统日志服务器

要启用服务器，请单击 **Enable** 并输入 **Syslog Server** 的名称。

配置电子邮件通知

要配置电子邮件通知，请选中 **Enable** 并完成以下设置：

- **Mail Server** - 邮件服务器的名称或 IP 地址。
- **Authentication** - 邮件服务器登录验证类型。
  - **None** - 无需任何验证信息。
  - **Login Plain** （登录明文） - 以明文格式验证。
  - **TLS** - 安全连接的验证协议（例如，Gmail 使用端口 587 上的 TLS 验证选项）。
  - **SSL** - 安全连接的验证协议 （例如， Gmail 使用端口 465 上的 SSL 验证选项）。
- **SMTP Port** （SMTP 端口） - 简单邮件传输协议端口号。
- **Username** - 电子邮件用户名。例如：
  Mail Server：smtp.gmail.com
  Authentication：SSL
  SMTP PORT：465
  Username：xxxxx@gmail.com
  Password：yyyyyy
- **Password** - 电子邮件密码。
- **Send Email to 1** （发送邮件至 1）和 （可选） **2** - 电子邮件地址。例如，发送电子邮件至：zzz@company.com。
- **Log Queue Length** （日志队列长度） - 发送通知之前的日志条目数。例如，*10* 个条目。
- **Log Time Threshold** （日志时间阈值） - 日志通知之间的时间。例如， *10* 分钟。
- **Real Time Alert** （实时警报） - 触发即时通知的事件。
- **Email Alert when block/filter contents accessed** （阻止 / 过滤访问的内容时发送电子邮件警报） - 当设备尝试访问被阻止或过滤的内容时，会发送电子邮件警报。
- **Email Alert for hacker attack**（黑客攻击时发送电子邮件警报）- 当尝试使用拒绝服务 (DOS) 攻击的黑客尝试访问时，会发送电子邮件警报。

要立即通过电子邮件发送日志，请单击 **Email Log Now** （现在通过电子邮件发送日志）。

配置日志

要触发日志条目，请选择事件：

- **Syn Flooding** （SYN 泛洪） - 接收 TCP 连接请求的速度要比设备可以处理的请求快。
- **IP Spoofing** （IP 欺骗） - 发送了明显伪造源 IP 地址的 IP 数据包，旨在隐瞒发送方身份或假冒其他计算系统。
- **Unauthorized Login Attempt** （未授权的登录尝试） - 已拒绝的网络登陆尝试。
- **Ping of Death** （Ping 炸弹） - 检测到恶意或其他恶意 Ping 已发送至计算机。通常 Ping 大小为 32 字节 （如果考虑互联网协议 [IP] 报头，则为 84 字节）；以往，许多计算机系统都无法处理大于 65535 字节 （最大 IPv4 数据包大小）的 Ping 数据包。发送过大的 Ping 可能使目标计算机崩溃。
- **Win Nuke** - 影响 Microsoft Windows 95、 Microsoft Windows NT 和 Microsoft Windows 3.1x 计算机操作系统的远程拒绝服务攻击 (DoS)。
- **Deny Policies** （拒绝策略） - 根据配置的策略，拒绝访问。
- **Authorized Login** （已授权登录） - 授权的用户已登录到网络。
- **System Error Messages** （系统错误消息） - 系统错误消息已记录。
- **Allow Policies** （允许策略） - 授权的用户已通过配置的策略登录到网络。
- **Kernel** （内核） - 所有系统内核消息。
- **Configuration Changes** （配置更改） - 修改设备配置时的实例。
- **IPsec and PPTP VPN** （IPsec 和 PPTP VPN） - VPN 隧道协商、连接和断开连接状态。
- **SSL VPN** - SSL VPN 隧道协商、连接和断开连接状态。
- **Network** - WAN/DMZ 接口已连接或断开连接。

其他信息 （日志按钮）

如果 Web 浏览器显示弹出窗口的警告，请允许显示被阻止的内容。单击 **Refresh** 可更新数据。

单击以下按钮查看其他信息：

- **View System Log** （查看系统日志） - 查看 **System Log**。要指定日志，请从下拉菜单中选择过滤器。

  日志条目包括事件的日期和时间、事件类型以及消息。消息指定了策略类型（例如 Access Rule）、源 (SRC) 的 LAN IP 地址，以及 MAC 地址。

- **Outgoing Log Table** （传出日志表） - 传出数据包信息。
- **Incoming Log Table** （传入日志表） - 传入数据包信息。
- **Clear Log Now** （现在清除日志） - 单击可清除日志，不通过电子邮件发送日志 （仅当您不希望以后查看信息时）。

系统统计信息

要打开此页，请在导航树中选择 **Log** > **System Statistic** （系统统计信息）。

系统将显示有关端口和连接到该端口的设备的详情。

流程

要打开此页，请在导航树中选择 **Log** > **Processes** （流程）。

系统将显示有关正在运行的流程的详情。

11

SSL VPN

通过 SSL VPN （安全套接字层虚拟专用网络），用户可以使用 Web 浏览器建立指向此设备的安全、远程访问 VPN 隧道。用户无需在计算机上预先安装软件或硬件客户端。使用 SSL VPN 可以从互联网上几乎任何计算机中安全、轻松地访问广泛的 Web 资源和启用了 Web 的应用程序。具体包括：

- 内部网站
- 启用了 Web 的应用程序
- NT/Active Directory （活动目录）文件共享 （即 My Network Place （我的网络位置））
- MS Outlook Web Access
- 应用程序访问 （对其他基于 TCP 的应用程序的端口转发访问）

SSL VPN 使用安全套接字层协议及其接替物传输层安全协议在远程用户和中央站点中配置的特定受支持内部资源之间建立安全连接。此设备识别必须使用代理的连接，并且 SSL VPN Web 门户与验证子系统进行交互以验证用户身份。

基于组向 SSL VPN 会话用户提供对资源的访问权限。业务合作伙伴等用户可以归到对内部网络上的资源没有直接访问权限的组中。或者，对于需要内部网络上所有资源的访问权限的用户，此设备支持 Virtual Passage（虚拟通道）， Virtual Passage 允许授权用户通过 SSL VPN 隧道从此设备中获取 IP 地址，然后成为内部网络的一部分。

状态

提供 SSL VPN 隧道的状态。用户可以从此窗口中注销。

要打开此页，请在导航树中选择 **SSL VPN** > **Status**。

系统将显示 SSL Status Table （SSL 状态表）：

- **User** （用户） - 用户的名字。
- **Group** - 相关组。

- **IP** - IP 地址。
- **Login Time** （登录时间） - 用户登录到隧道的时间。

要注销用户，请在 **Logout** 列中单击该图标。

组管理

组管理控制用户组，包括对资源的访问权限。管理员可以创建多个用户组，其中每个组具有 LAN 中不同组资源的访问权限。典型方案有两个用户组，其中一个组包含员工，另一个组包含业务合作伙伴。虽然此设备支持多个域，但是经常可以看到一个小型企业具有一个绑定到特殊验证数据库 （例如本地数据库、 RADIUS 或 LDAP）的单个域。

要打开此页，请在导航树中选择 **SSL VPN** > **Group Management**。

SSL Status Table 包含以下信息：

- **Group** - 组的名称。
- **Domain** （域） - 对用户进行授权的数据库。
- **User** （用户） - 用户名和类型。单击 **Details** 可显示。
- **Resource** （资源） - 允许组访问的系统资源。单击 **Details** 可显示。
- **Status** - 组状态。

删除组

要删除组，请在 **SSL Status** （SSL 状态）表中单击要删除的组的名称，然后单击 **Delete**。如果用户仅属于一个组，当管理员删除该组时，会自动删除相应的用户。

要为验证域删除属于默认组的组，请删除相应的域 （无法在 Edit Group Settings （编辑组设置）窗口中删除该组）。

如果该组不是验证域的默认组，请删除该组中的所有用户，然后删除该组。

添加或编辑组

要添加 （或修改）组，请单击 **Add** （或选择一个条目，然后单击 **Edit**），然后输入以下参数：

- **Group Name** - 组的名称。如果正在编辑现有组，则无法修改此参数。
- **Domain** - 组域。单击 **Add** 或 **Edit** 可显示 **Group Management** 窗口。
- **Enabled** - 选中可启用此组。
- **Service Idle Time** （服务空闲时间） - 在结束会话之前，连接可以处于空闲状态的时间。

选择要为此组启用的资源：

- **Service -** 此组可用的服务。
- **Customized Service Bookmark** （自定义服务书签） **-** 服务 （Telnet、 SSH、 FTP）和远程桌面服务 （RDP5、 VNC）可以使用组建立的书签。通过这种方式，用户无需记住或设置服务器名称或 IP 地址；他们单击即可使用管理员预先配置的资源。

  管理员可以查看用户 Web 门户上显示的所有已配置书签。
- **My Desktop** （我的桌面） **-** 启用 RDP5 和 VNC。远程桌面协议客户端增强功能 (**RDP5**) ActiveX 书签目前支持用于资源映射的高级 Windows 选项，具有重定向驱动器、重定向打印机、重定向端口和重定向智能卡的选项。虚拟网络计算 (**VNC**) 是一个图形桌面共享系统，它使用远程帧缓存 (RFB) 协议远程控制另一台计算机。它通过网络将键盘和鼠标事件从一台计算机传输到另一台计算机，并将图形屏幕更新中继回传。
- **Terminal Service** （终端服务） **-** 允许应用程序，例如 Word、 Excel 和 PowerPoint。
- **Other** （其他） **-** 允许访问 My Network Place 和 Virtual Passage。 Virtual Passage 可以是分割隧道 （未为隧道进行特殊标记的流量通过其他虚拟连接发送），也可以是 Full Tunnel （全隧道）（通过隧道发送所有流量）。

每个默认用户组的资源将显示在表中。

资源名称 / 组名称	所有用户	监督者	移动用户	分公司员工
互联网服务				
Telnet	v			
SSH	v			
FTP	v	v	v	v
微软终端				
Services	v	v	v	
Word	v	v	v	
Excel	v	v	v	
Power Point	v	v	v	
Access	v	v	v	

资源名称 / 组名称	所有用户	监督者	移动用户	分公司员工
Outlook	v	v	v	
Internet Explorer	v			
FrontPage	v			
ERP	v	v	v	v
远程桌面				
RDP5	v		v	
VNC	v			
My Network Place	v	v		
Virtual Passage	v	v		

资源管理

SSL VPN 支持微软终端服务，包括 Word、 Excel、 PowerPoint、 Access、 Outlook、 Internet Explorer、 FrontPage 和 ERP。对于可供用户使用的每个终端服务，配置资源并指定应用程序服务器的 IP 地址和指向应用程序的路径。

要打开此页，请在导航树中选择 **SSL VPN** > **Resource Management** （资源管理）。

要添加 （或修改）资源，请单击 **Add** （或选择一个条目，然后单击 **Edit**），然后输入以下参数：

- **Application Description** （应用程序描述） - 应用程序的描述。
- **Application and Path** （应用程序和路径） - 路径和可执行文件名。
- **Working Directory** （工作目录） - 应用程序目录。
- **Host Address** （主机地址） - 托管服务的计算机的 IP 地址。
- **Application Icon** （应用程序图标） - 要显示的图标。
- **Enable** - 启用资源。

高级设置

高级 SSL VPN 设置限制可以访问服务、更改服务端口或修改横幅的 IP 地址范围。

要打开此页，请在导航树中选择 **SSL VPN** > **Advanced Setting** （高级设置）。

要修改高级设置，请输入以下参数：

- **Client Address Range Starts**（客户端地址范围起始值）- 允许地址范围的起始 IP 地址。
- **Client Address Range Ends** （客户端地址范围结束值） - 允许地址范围的结束 IP 地址。
- **Service Port** （服务端口） - SSL VPN 的端口号。
- **Business Name** （业务名称） - 显示为业务名称横幅的字符串。
- **Resource Name** （资源名称） - 显示为资源名称横幅的字符串。

11

SSL VPN
高级设置

12

用户管理

用户管理控制域和用户访问，主要用于 PPTP、思科 VPN 客户端 （也称为 EasyVPN）和 SSL VPN。

要打开此页，请在导航树中选择 **User Management**。

添加 （或修改）域的步骤：

步骤 1 单击 **Add** （或选择一个条目，然后单击 **Edit**）。

步骤 2 选择 **Authentication Type** （验证类型）并输入所需信息：

- **Local Data Base** （本地数据库） - 对本地数据库进行验证。
  - **Domain** - 域名用户选择登录到 SSL VPN 门户。
- **Radius** （**PAP**、 **CHAP**、 **MSCHAP**、 **MSCHAPv2**） - 使用密码鉴别协议 (PAP)、询问握手鉴权协议 (CHAP)、 Microsoft 询问握手鉴权协议 (MSCHAP) 或 Microsoft 询问握手鉴权协议版本 2 (MSCHAPv2) 对 RADIUS 服务器进行验证。
  - **Domain** - 域名用户选择登录到 SSL VPN 门户。
  - **Radius Server** （Radius 服务器） - RADIUS 服务器的 IP 地址。
  - **Radius Password** （Radius 密码） - 验证 *密钥*。
- Active Directory - Windows Active Directory 验证。注意 Active Directory 验证是最容易出错的。如果无法使用 Active Directory 进行验证，请阅读本节末尾的故障排除步骤。
  - **Domain** - 域名用户选择登录到 SSL VPN 门户。
  - **AD Server Address** （AD 服务器地址） - Active Directory 服务器的 IPv4 地址。
  - **AD Domain Name** （AD 域名） - Active Directory 服务器的域名。

- **LDAP -** 轻型目录访问协议。
  - **Domain -** 域名用户选择登录到 SSL VPN 门户。
  - **LDAP Server Address** （LDAP 服务器地址） **-** LDAP 服务器的 IPv4 地址。
  - **LDAP Base DN** （LDAP 库 DN） **-** LDAP 查询的搜索库。搜索库字符串的一个示例是 `CN=Users,DC=yourdomain,DC=com`。

步骤 **3** 单击 **OK** （确定）。

要添加 （或修改）用户，请单击 **Add** （或选择一个条目，然后单击 **Edit**），然后输入以下信息：

- **Username -** 用户输入的用于登录到 SSL VPN 门户的名字。可以使用密码窗口对用户的用户名和密码进行更改。
- **Password -** 用于验证的密码。
- **Group -** 源自组管理中 SSL Status Table 的组。默认情况下， Group 下拉菜单有 5 个选项； 4 个默认的 SSLVPN 组和 Unassigned。 Unassigned 组包含 PPTP VPN 用户和 EasyVPN 用户。管理员组只有一个用户，管理员组的默认用户名为 **Cisco**。
- **Domain -** 列在 Domain Management （域管理）表中的域的名称。

13

向导

从 Wizard 页面，可以启动 Basic Setup （基本设置）向导，指导用户完成设备的初始配置过程。 Access Rule 向导指导用户完成为网络配置安全策略的过程。

要打开此页，请在导航树中选择 **Wizard**。

基本设置

基本设置

使用 Basic Setup Wizard （基本设置向导）更改 WAN 端口的数量或配置互联网连接。

单击 **Launch Now** 可运行 Basic Setup Wizard。按照屏幕上的说明继续操作。请参阅 ISP 提供的信息输入所需的连接设置。

访问规则设置

访问规则设置

使用 Access Rule Setup Wizard （访问规则设置向导）创建防火墙访问规则。单击 **Launch Now** 可运行 Access Rule Setup Wizard。该向导将提供有关此设备的默认规则的信息。按照屏幕上的说明继续操作。

14

快速索引

支持	
思科 Small Business 支持社区	www.cisco.com/go/smallbizsupport
在线技术支持和文档（需要登录）	www.cisco.com/support
电话支持联系人名单	www.cisco.com/en/US/support/tsd_cisco_small_ business_support_ center_contacts.html
软件下载 （需要登录）	请转至 tools.cisco.com/support/downloads，然后在 Software Search （软件搜索）框中输入相应的型号。

产品文档	
思科 RV320/RV325 千兆双 WAN 口 VPN 路由器	www.cisco.com/en/US/products/ps9923/tsd_products_support_series_home.html
思科 Small Business	
思科 Small Business 合作伙伴中心 （需要合作伙伴登录）	www.cisco.com/web/partners/sell/smb
思科 Small Business 主页	www.cisco.com/smb
市场	www.cisco.com/go/marketplace

2013 年 7 月 16 日修订　　78-20928-01