管理指南

思科精睿 (Cisco Small Business)

RV0xx 系列 10/100 VPN 路由器
型号 RV042、 RV082 和 RV016

78-20140-01

目录

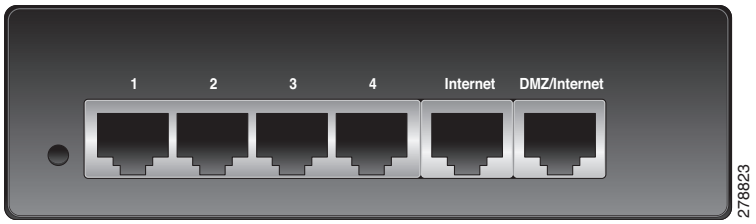
1

简介

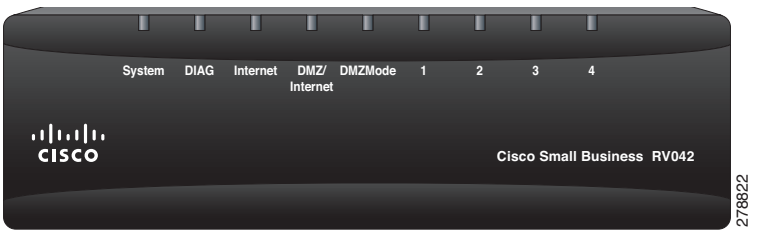
感谢您选择 RV0xx 系列 VPN 路由器。本指南提供了配置和管理路由器所需的完整信息。本章包括的信息可以帮助您开始使用路由器。请参阅以下主题：

RV0xx 系列路由器特征

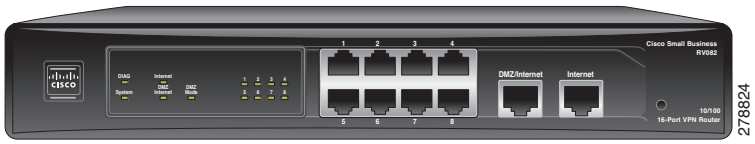
RV042 端口



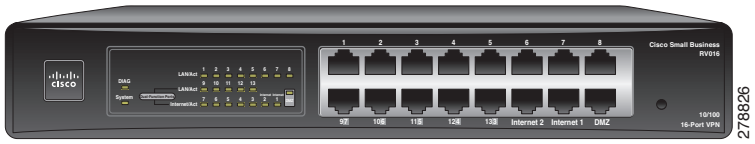
RV042 LED



RV082 端口和 LED



RV016 端口和 LED



端口

Internet （RV042 和 RV082）或 Internet 1-2 (RV016)：使用该端口可将路由器连接到宽带网络设备。

DMZ/Internet （RV042 和 RV082）：使用该端口可将路由器连接到另一宽带网络设备或 DMZ 主机 （例如 Web 服务器或 FTP 服务器）。 DMZ 允许公共 Internet 数据流访问您的网络上的指定计算机，而不会暴露您的 LAN。

DMZ (RV016)：使用该端口可将路由器连接到 DMZ 主机 （例如 Web 服务器或 FTP 服务器）。 DMZ 允许公共 Internet 数据流访问您的网络上的指定计算机，而不会暴露您的 LAN。

1-4 (RV042) 或 1-8 （RV082 和 RV016）：使用这些编号端口可连接计算机和其他本地网络设备。

Dual Function Ports （双功能端口） (RV016)：将这些端口用作 LAN 端口 （编号为 9-13），或将其配置为用作 Internet 端口 （编号为 3-7）。状态显示在相应的 LED 上：LAN/Act 9-13 或 Internet/Act 3-7。

LED

DIAG：当按下重置按钮超过 10 秒时，会触发系统重新引导，此时 LED 会缓慢闪烁。当按下重置按钮超过 20 秒时，系统会恢复出厂默认设置，此时 LED 会快速闪烁。如果固件升级失败，路由器将处于引导加载程序模式，且在路由器等待从 TFTP 服务器接收固件时， DIAG LED 将缓慢闪烁。当路由器完成工作前的准备后，该 LED 将熄灭。

System：当路由器接通电源后，该 LED 将呈绿色稳定亮起。当路由器运行诊断测试时，该 LED 会闪烁。

Internet （所有型号）、 DMZ/Internet （RV042 和 RV082）或 Internet/ACT (RV016)：当有设备连接到端口时，该端口对应的 LED 将呈绿色稳定亮起。该 LED 闪烁表示该端口上有网络活动。

DMZ Mode（RV042 和 RV082）：如果将 DMZ/Internet 端口配置为 DMZ，该 LED 将呈绿色稳定亮起。如果将端口配置为辅助 Internet 连接，该 LED 将熄灭。

DMZ (RV016)：如果路由器通过 DMZ 端口连接到 DMZ 主机，该 LED 将呈橙色稳定亮起。该 LED 闪烁表示该端口上有网络活动。

1-4 (RV042)、 1-8 (RV082) 或 LAN/Act 1-8 (RV016）：当有设备连接到端口时，该端口对应的 LED 将呈绿色稳定亮起。该 LED 闪烁表示该端口上有网络活动。

Dual Function Ports （双功能端口） LAN/Act 9-13 和 Internet/Act 3-7 (RV016)：对于每个双功能端口，这两个 LED 只会亮起一个，用以指示当前的端口功能 （LAN 或 Internet）。当有设备连接到端口时，该端口对应的 LED 将呈绿色稳定亮起。该 LED 闪烁表示该端口上有网络活动。

其他硬件特征

重置：重置按钮是一个凹陷的黑色按钮， RV042 的重置按钮在后面板上， RV082 和 RV016 的重置按钮在前面板上。

- **重新启动路由器或恢复连接的步骤**：如果路由器与 Internet 的连接出现问题，请使用笔尖按住 “Reset” 按钮一秒钟。
- **还原出厂默认设置的步骤**：如果路由器出现严重的问题，您尝试了所有其他的故障排除方法都未能解决，请按住 “Reset” 按钮 30 秒，还原出厂默认设置。之前输入的所有设置都将被丢弃。

安全槽：使用侧面板上的安全槽可以为路由器上锁，以防被盗。

电源：

- **RV042**：将提供的电源适配器连接到侧面板上的电源端口。
- **RV082 和 RV016**：将提供的交流电源电缆连接到后面板上的电源端口。

默认设置

参数	默认值
用户名	admin
密码	admin
LAN IP	192.168.1.1
DHCP 范围	192.168.1.100 到 149
子网掩码	255.255.255.0

安装选项

安放提示

- **环境温度** - 为防止路由器过热，请勿在环境温度超过 104° F (40° C) 的区域中使用。
- **空气流通** - 确保路由器周围通风顺畅。
- **机械装载** - 确保将路由器保持水平且安放平稳，以避免任何危险情况。

桌面安放

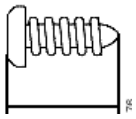
将路由器放在桌面上之前，请在底部面板上安装四个黏着垫。将路由器放在靠近电源插座的平坦表面上。

警告 请勿在路由器上放置任何物品；过度的重量会损坏路由器。

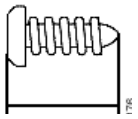
壁挂

路由器的底部面板上有两个壁式安装插槽。要将路由器安装在墙上，需使用安装硬件（未提供）。建议使用下图中所示的硬件 （非真实比例）。

针对 RV042 的建议硬件

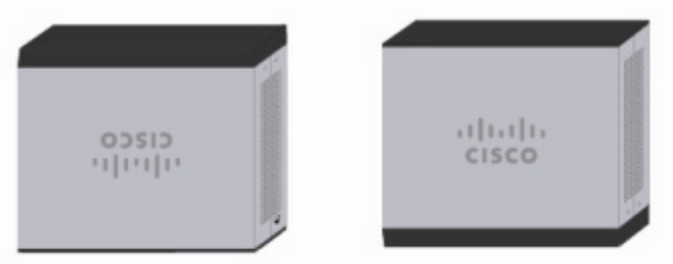
	
5-5.5 毫米	20-22 毫米

针对 RV082 和 RV016 的建议硬件

	
6.5-7 毫米	16.5-18.5 毫米

警告 安装不牢固可能会损坏路由器或造成人身伤害。对于因壁式安装不牢靠而造成的损失，思科概不负责。

警告 为安全起见，请确保将散热孔朝向一边。



步骤 1 在表面上钻两个装配孔。

- **RV042**：彼此相距 58 毫米
- **RV082 和 RV016**：彼此相距 94 毫米

步骤 2 在每个孔内插入一颗螺钉，在表面和螺钉头底座之间至少留出 1 毫米到 1.2 毫米的空隙。

步骤 3 将路由器壁式安装插槽套在螺钉上，然后向下滑动路由器，直至螺钉稳固卡入壁式安装插槽。

机架安装 RV082 或 RV016

您可以将 RV082 或 RV016 安装在标准大小的 19 英寸 （约 48 厘米）宽的机架中。路由器需要 1 个机架单元 (RU) 的空间，即 1.75 英寸 （44.45 毫米）高。产品附带安装支架。

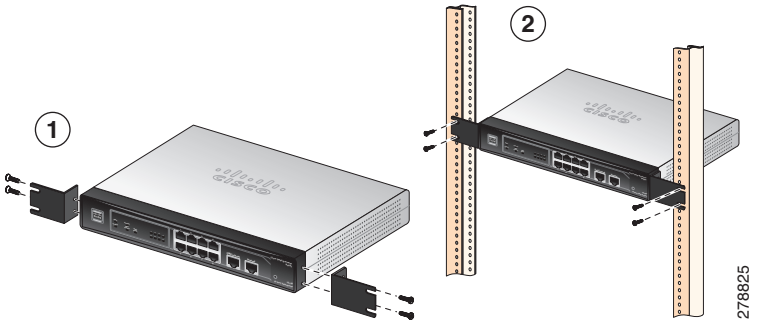
警告 在一个机架中安装多个设备时，请勿使电源插座或电路过载。

步骤 1 将路由器放置在坚固平坦的表面上。

步骤 2 使用附带的螺钉将其中一个附带的机架安装支架安装到路由器的一端。牢牢固定住支架。

步骤 3 按照相同的步骤将另一个支架安装到路由器的另一端。

步骤 4 使用合适的螺钉将支架牢牢固定到任意标准的 19 英寸机架。



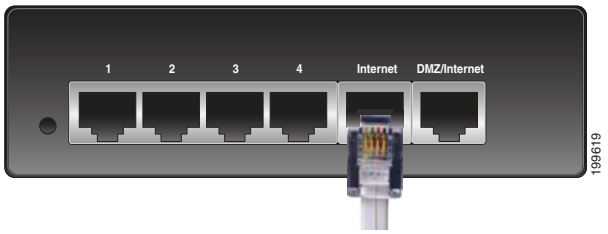
连接设备

步骤 1 确保关闭所有网络设备的电源，包括路由器、 PC、以太网交换机和宽带网络设备（DSL 或电缆调制解调器）。

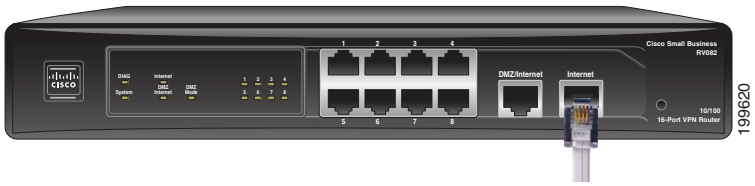
步骤 2 连接到 Internet 服务的步骤：

- **RV042 或 RV082**：将以太网电缆从宽带网络设备连接到路由器的 **Internet** 端口。

RV042 Internet 端口



RV082 Internet 端口



- **RV016**：将以太网电缆从宽带网络设备连接到路由器的 **Internet 1** 端口。

RV016 Internet 1 端口

步骤 3 连接辅助 Internet 服务的步骤：

- **RV042 和 RV082**：将以太网电缆从 **DMZ/Internet** 端口连接到另一宽带网络设备。
- **RV016**：将以太网电缆从 **Internet 2** 端口连接到另一宽带网络设备。

步骤 4 连接将作为 DMZ 主机的计算机或服务器的步骤：

- **RV042 和 RV082**：将以太网电缆从 **DMZ/Internet** 端口连接到 DMZ 主机。
- **RV016**：将以太网电缆从 **DMZ** 端口连接到 DMZ 主机。

步骤 5 要连接其他网络设备 （如计算机、打印服务器或以太网交换机），请将以太网电缆从某个编号 LAN 端口连接到该网络设备。

步骤 6 接通宽带网络设备的电源。

步骤 7 使用电源适配器 (RV042) 或电源电缆 （RV082 和 RV016）将路由器连接到电源插座。 System LED 将亮起。

步骤 8 接通其他网络设备的电源。

配置入门

步骤 1 将计算机连接到路由器上带编号的 LAN 端口。您的 PC 将成为路由器的 DHCP 客户端，并将接收 192.168.1.x 范围内的 IP 地址。

步骤 2 启动 Web 浏览器。要使用配置实用程序，您的 PC 上需安装 Internet Explorer（版本 6 及更高版本）、 Firefox 或 Safari （针对 Mac）。

步骤 3 在地址栏中输入路由器的默认 IP 地址：**192.168.1.1**

步骤 4 当显示登录页面时，输入默认用户名 **admin** 和默认密码 **admin** （小写）。

步骤 5 单击 “**Login**”。此时将显示 “*System Summary*”页面。

对于许多小型企业而言，路由器的默认设置已足以满足其需求。您的 Internet 服务提供商 (ISP) 可能需要其他设置。在 “*System Summary*”页面上，检查 WAN 状态，以查看路由器是否能够接收 IP 地址。如果无法接收，请继续下一个步骤。

步骤 6 要使用设置向导配置 Internet 连接，请单击 “*System Summary*”页面上的 “**Setup Wizard**”，或单击导航树中的 “**Wizard**”。在 “*Basic Setup*”部分中，单击 “**Launch Now**”。按照屏幕上的说明进行操作。

如果您的 Web 浏览器显示关于弹出窗口警告，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接。

思科强烈建立设置高安全性的管理员密码，以防路由器受到未经授权的访问。有关所有设置的详细信息，请参阅在线帮助和 《思科精睿 (Cisco Small Business) RV0xx 系列 VPN 路由器管理指南》。

故障排除提示

如果连接到 Internet 或基于 Web 的配置实用程序时出现问题，请执行以下操作：

- 确保 Web 浏览器未设置为脱机工作。
- 检查以太网适配器的本地连接设置。 PC 需要通过 DHCP 获得 IP 地址。或者，PC 也可拥有 192.168.1.x 范围内的静态 IP 地址，其中 x 代表 2 到 254 之间的任意数字。（192.168.1.1 为路由器的默认 LAN IP 地址， 192.168.1.255 为广播地址。）
- 确保在 Wizard 中输入设置 Internet 连接所需的正确设置，包括用户名和密码（如果需要）。

- 通过关闭调制解调器和路由器的电源，尝试重置这两个设备。随后，接通调制解调器的电源，使其闲置约 2 分钟。然后，接通路由器的电源。现在，您应该能够接收 WAN IP 地址。
- 检查调制解调器的 DHCP IP 地址范围。如果调制解调器使用 192.168.1.x 范围，请拔下连接调制解调器和路由器的电缆，然后启动路由器配置实用程序。在导航树中，选择 “**Setup**” > “**Network**”。输入新的设备 IP 地址，例如 10.1.1.1 或 192.168.0.1。或者，如果您有 DSL 调制解调器，请保持所有设置不变，而要求您的 ISP 将 DSL 调制解调器设置为桥接模式。

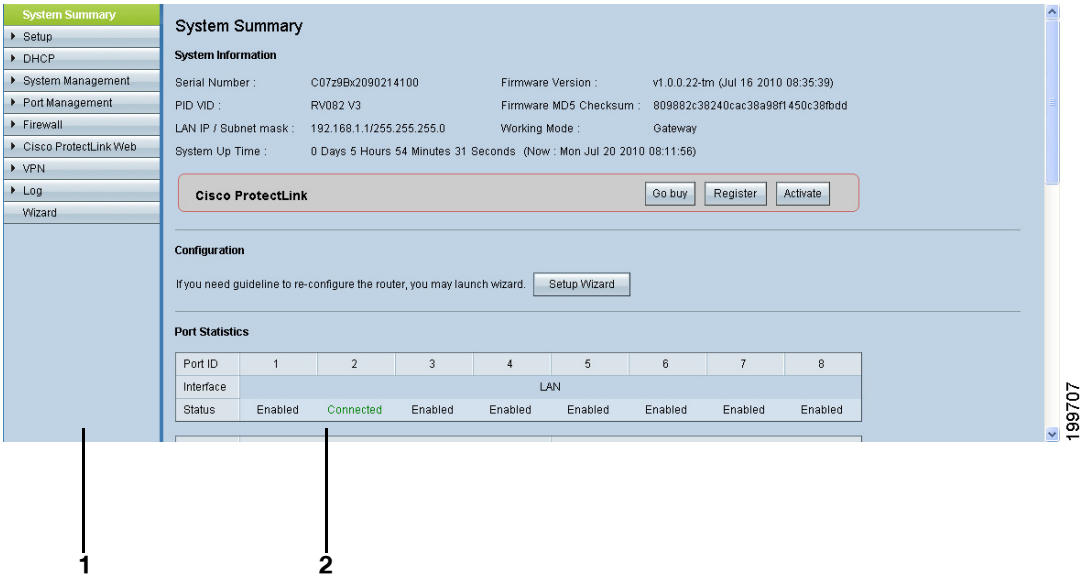
用户界面特征

用户界面旨在便于您设置和管理路由器。请参阅以下主题：

- **导航，页码 16**
- **弹出窗口，页码 16**
- **设置向导，页码 16**
- **保存设置，页码 17**
- **帮助，页码 17**
- **注销，页码 17**

导航

配置实用程序的主要模块以左侧导航窗格中的按钮形式表示。单击按钮可查看更多选项。单击选项可打开配置页面。选中的页面将显示在配置实用程序的主窗口中。



1. 导航树
2. 配置页面

弹出窗口

单击某些链接和按钮时会启动弹出窗口，其中显示详细信息或相关配置页面。如果您的 Web 浏览器显示关于弹出窗口警告，请允许显示被阻止的内容。

设置向导

产品配备了两种设置向导，可便于您设置 Internet 连接和 / 或 DMZ，以及为 WAN、LAN 和 DMZ 配置访问规则。您可以使用这些向导或使用配置实用程序的其他页面。

打开 Wizard 页面的步骤：单击 “*System Summary*” 页面上 “*Configuration*” 部分中的 “**Setup Wizard**” 按钮。或者，单击导航树中的 “**Wizard**”。有以下两种向导：

- **Basic Setup**：单击 “**Launch Now**” 配置 Internet 连接和 DMZ 的基本设置。按照屏幕上的说明进行操作。
- **Access Rule Setup**：单击 “**Launch Now**” 为 WAN、 LAN 和 DMZ 配置访问规则。按照屏幕上的说明进行操作。

保存设置

只有单击 “**Save**”按钮后，配置页面上的设置才会保存。导航到其他页面时，所有未保存的设置都将被丢弃。

要清除设置而不保存，您可以单击 “**Cancel**”按钮。

帮助

要查看有关所选配置页面的详细信息，请单击配置实用程序右上角附近的 “**Help**”链接。如果您的 Web 浏览器显示关于弹出窗口警告，请允许显示被阻止的内容。

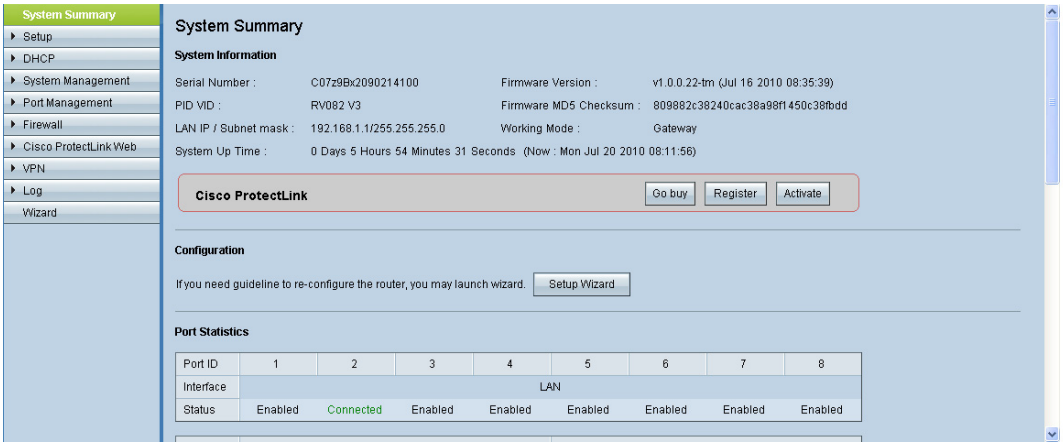
注销

要退出配置实用程序，请单击配置实用程序右上角附近的 “**Logout**”链接。此时将显示 “*Login*”页面。您可以关闭浏览器窗口。

2

查看系统摘要信息

登录配置实用程序后，将显示 “*System Summary*”页面。您也可以通过在导航树中单击 “**System Summary**”来查看此页面。使用此页面查看有关路由器和相关设置的当前状态信息。请参阅以下主题：



系统信息

本部分包括以下信息：

- **Serial Number**：路由器的序列号。
- **Firmware version**：路由器上安装的固件的当前版本号。
- **PID VID**：硬件的当前版本号。
- **MD5 Checksum**：用于文件验证的值。
- **LAN IP/Subnet mask**：本地网络上路由器的当前 IP 地址。
- **Working Mode**：工作模式 （“Gateway”或 “Router”）。
- **System Up time**：路由器处于活动状态的时间长度，以天数、小时数和分钟数表示。

Cisco ProtectLink Web

本节介绍可选 Cisco ProtectLink Web 服务的按钮。 ProtectLink Web 为您的网络提供安全保护。该服务可过滤网站地址 (URL) 并拦截潜在的恶意网站。（另请参阅**第 8 章，“Cisco ProtectLink Web 入门”**。）

您可以使用以下按钮：

- **Go buy**：单击此按钮可购买许可证以使用此服务。您将被重定向至 Cisco 网站上的 Cisco 经销商列表。然后按照屏幕上所显示的相关说明进行操作。
- **Register**：如果您有许可证但尚未注册，请单击此按钮。您将被重定向至 Cisco ProtectLink Web 网站。然后按照屏幕上所显示的相关说明进行操作。
- **Activate**：如果您已注册 Cisco ProtectLink Web 服务并希望激活此服务，请单击此按钮。您将被重定向至 Cisco ProtectLink Web 网站。按照屏幕上的说明进行操作。

注意 如果 “*System Summary*”页面上未显示 Cisco ProtectLink Web 选项，您可以升级路由器的固件以启用此功能。

配置

如果您需要路由器配置方面的帮助，请单击 “**Setup Wizard**”。随后，您可以使用以下向导：

- **基本设置向导**：使用此向导可设置您的 Internet 连接。
- **访问规则设置向导**：使用此向导可为您的 VPN 设置安全策略。

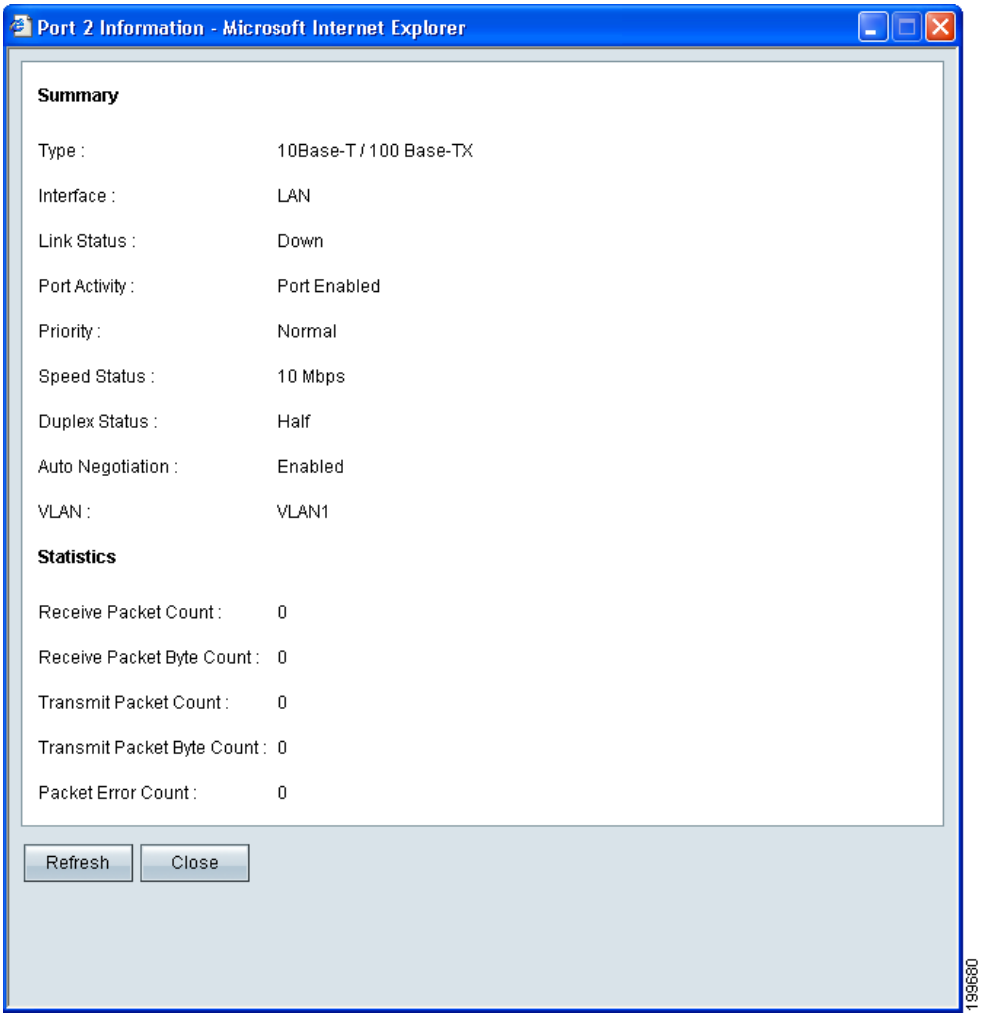
端口统计信息

此表显示了每个端口的状态和可用统计信息。它还提供了有关当前链路活动的详细信息。

- **Port ID**：端口标签。
- **Interface**：接口类型，例如 LAN、 WAN 或 DMZ。多个 WAN 接口由数字表示，例如 WAN1 或 WAN2。
- **Status**：端口的状态：“*Disabled*”（红色）、“*Enabled*”（黑色）或“*Connected*”（绿色）。状态显示为超链接形式，您可以单击它以打开“*Port Information*”窗口。

  端口信息窗口

  如果单击“*Port Statistics*”表中的某个状态，则会显示“*Port Information*”窗口。此窗口显示了有关接口和当前活动的最新信息。要更新显示的信息，请单击“**Refresh**”按钮。要关闭此窗口，请单击“**Close**”按钮。



此窗口显示了以下信息：

- **Type**：端口的类型， 10Base-T/100 Base-TX。
- **Interface**：接口的类型，例如 LAN、 DMZ 或 WAN。
- **Link Status**：链路的当前状态：“*Up*”或“*Down*”。
- **Port Activity**：端口上的当前活动，可以是“Port Enabled”、“Port Disabled”或“Port Connected”。
- **Priority**：优先级设置，“High”或“Normal”。
- **Speed Status**：速度， 10Mbps 或 100Mbps。
- **Duplex Status**：双工模式，“Half”或“Full”。

- **Auto negotiation**：自动协商设置，“On”或“Off”。
- **VLAN**：VLAN ID。
- **Receive Packet Count**：通过此端口接收的数据包数量。
- **Receive Packet Byte Count**：通过此端口接收的字节数。
- **Transmit Packet Count**：通过此端口传输的数据包数量。
- **Transmit Packet Byte Count**：通过此端口传输的字节数。
- **Packet Error Count**：数据包错误的数量。

WAN 状态

本节介绍每个 WAN 接口 （例如 WAN1、 WAN2 和 DMZ）的信息。

- **WAN 信息**：
  - **IP Address**：此接口的当前公共 IP 地址。
  - **Default Gateway**：此接口的默认网关 （仅限 WAN）。
  - **DNS**：此接口的 DNS 服务器的 IP 地址 （仅限 WAN）。
  - **Dynamic DNS**：此接口的 DDNS 设置，“Disabled”或“Enabled”（仅限 WAN）。
  - **DMZ Host**：它显示了 DMZ 主机的 DMZ 专用 IP 地址。默认为“**Disabled**”。
  - **Release** 和 **Renew**：如果端口设置为自动获取 IP 地址，则将显示这些按钮。单击“**Release**”可释放 IP 地址，而单击“**Renew**”可更新 DHCP 租用时间或获取新的 IP 地址。
  - **Connect** 和 **Disconnect**：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 Internet 服务的连接。单击“**Connect**”可重新建立连接。
- **DMZ 信息**：
  - **IP Address**：此接口的当前公共 IP 地址。

防火墙设置状态

本部分显示以下信息：

- **SPI (Stateful Packet Inspection)**：此功能的状态：“*On*”（绿色）或“*Off*”（红色）。

- **DoS (Denial of Service)**：此功能的状态，“*On*”（绿色）或“*Off*”（红色）。
- **Block WAN Request**：此功能的状态，“*On*”（绿色）或“*Off*”（红色）。
- **Remote Management**：此功能的状态，“*On*”（绿色）或“*Off*”（红色）。
- **Access Rule**：已设置的访问规则的数量。

VPN 设置状态

本部分显示以下信息：

- **Tunnel(s) Used**：使用中的 VPN 隧道数。
- **Tunnel(s) Available**：可用 VPN 隧道的数量。

日志设置状态

本部分显示以下信息：

- **Syslog Server**：Syslog 服务器的状态，“*On*”（绿色）或“*Off*”（红色）。
- **Email Log**：电子邮件日志的状态，“*On*”（绿色）或“*Off*”（红色）。

3

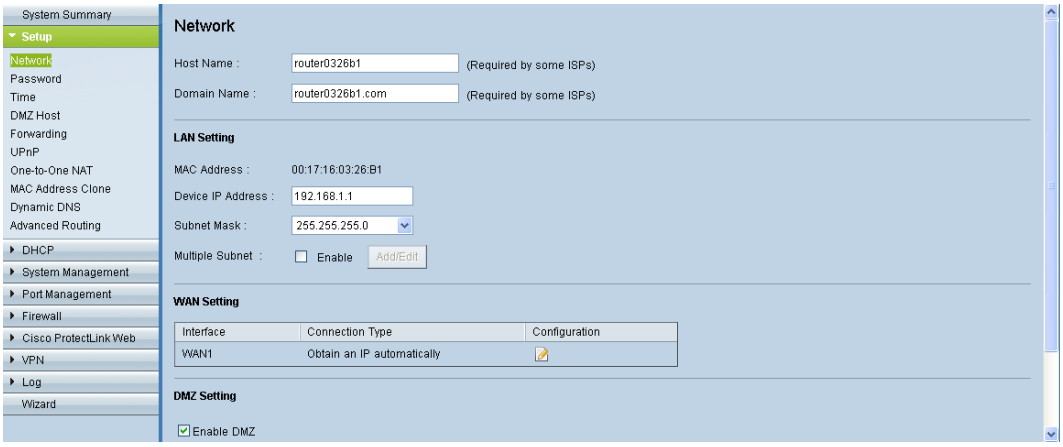
设置

使用 “*Setup*” 模块设置路由器的基本功能。请参阅以下主题：

设置网络

使用 “*Setup*” > “*Network*”页面设置 LAN、 WAN （Internet 连接）和 DMZ 接口。

打开此页面的步骤：在导航树中单击 “**Setup**” > “**Network**”。



注意 离开此页面前，请单击 “**Save**”保存设置，或单击 “**Cancel**”撤消设置。所有未保存的更改都将被丢弃。

该页面包括以下部分：

- **主机名和域名，页码 25**
- **LAN 设置 （设备 IP 地址和子网），页码 26**
- **WAN 设置 （Internet 连接），页码 28**
- **DMZ 设置，页码 28**

主机名和域名

部分 ISP 要求您指定主机名和域名，以便在 ISP 网络上标识您的路由器。默认值已提供，如有需要可进行更改。

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

LAN 设置（设备 IP 地址和子网）

默认的 LAN 设置应足以满足大多数小型企业的需求，但如有需要，您可以更改路由器的 LAN IP 地址并启用多个子网。

- **更改设备 IP 地址，页码 26**
- **启用多个子网，页码 26**

更改设备 IP 地址

步骤 1 输入新的“**Device IP Address**”和“**Subnet Mask**”。默认的 IP 地址是 192.168.1.1，默认的子网掩码是 255.255.255.0。

注意：路由器的 MAC 地址也在此部分显示。此值不可更改。

步骤 2 单击“**Save**”保存更改，或单击“**Cancel**”撤消更改。

应用设置时，会显示弹出窗口，提醒您需要使用新的设备 IP 地址登录到配置实用程序。单击“**OK**”关闭消息并继续更改 IP 地址，或单击“**Cancel**”关闭消息而不应用更改。

步骤 3 释放并更新 PC 的 IP 地址。然后您会收到路由器的新 IP 地址，该地址在新的 DHCP 范围内。

注意：默认情况下，路由器是可动态分配 IP 地址的 DHCP 服务器。同样在默认情况下， Windows PC 会动态接收 IP 地址。如果先前禁用了路由器的 DHCP 服务器或在 PC 上设置了静态 IP 地址，您将需要在正确的范围内配置新的静态 IP 地址。

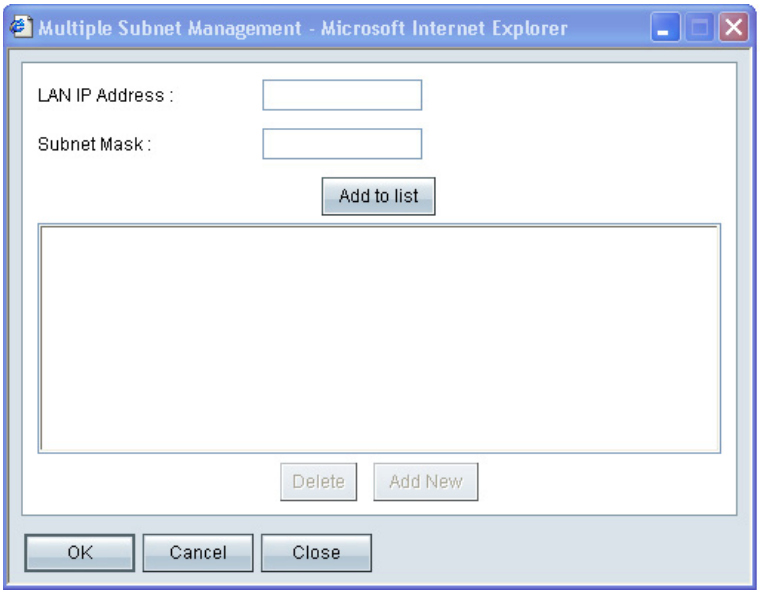
步骤 4 要重新连接到配置实用程序，请在浏览器的地址栏中输入新的设备 IP 地址。

启用多个子网

通常， Cisco RV0xx 系列路由器用作访问路由器，在一个单独的 LAN 子网内。默认情况下，防火墙经过预配置，如果源 IP 地址与路由器 LAN IP 地址位于不同的子网，防火墙将拒绝 LAN 访问。但您可启用多个子网，使得此路由器作为边缘设备工作并为 LAN 中的不同子网提供 Internet 连接。

步骤 1 单击“**Enable Multiple Subnet**”复选框以启用此功能。取消选中此框可禁用此功能。

步骤 2 单击“**Add/Edit**”创建或修改子网。单击此按钮后，将显示“*Multiple Subnet Management*”窗口。



步骤 3 在弹出窗口中，根据需要添加或编辑条目。

- **添加新子网的步骤**：输入 “LAN IP Address”和 “Subnet Mask”。单击 “**Add to List**”。 IP 地址和子网掩码将显示在列表中。根据需要重复此步骤，以添加其他子网。

  示例：

  - 两个子网：如果路由器的 LAN IP 地址为 192.168.1.1，子网掩码为 255.255.255.0，您可以用 LAN IP 地址 192.168.2.1、子网掩码 255.255.255.0 设置另一个子网。
  - 四个子网：如果路由器的 LAN IP 地址为 192.168.1.1，子网掩码为 255.255.255.192，您可以用三个 LAN IP 地址 192.168.2.65、192.168.2.129、192.168.2.193 和同一个子网掩码 255.255.255.192 创建三个子网。

- **添加其他子网的步骤**：输入信息，然后单击 “**Add to list**”。
- **修改子网的步骤**：单击列表中的子网。现有值将显示在文本字段中。输入新信息，然后单击 “**Update**”。如果不想修改所选子网，则可单击 “**Add New**”清空文本字段。
- **删除子网的步骤**：单击列表中的子网，然后单击 “**Delete**”。

步骤 4 在 “*Multiple Subnet*”窗口中输入设置后，请单击 “**OK**”保存更改，或单击 “**Cancel**”撤销更改。

WAN 设置 （Internet 连接）

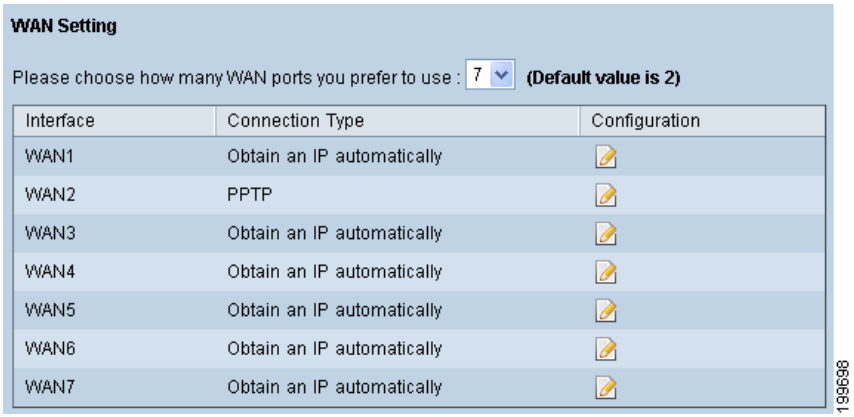
路由器预配置的默认设置足以满足许多网络的需要。然而，您的 ISP （网络服务提供商）或宽带 （DSL、电缆）承载器可能需要特殊的设置。请参考您的 ISP 提供的设置信息。

注意 您也可以使用基础设置向导设置 Internet 连接。在导航树中单击 “**Wizard**”。在 “*Basic Setup*”部分中单击 “**Launch Now**”。

“*WAN Setting*”表格列出了每个接口 （例如 DMZ、 WAN1 或 WAN2）的现有设置。列出的接口取决于路由器型号以及您为端口输入的设置，例如 DMZ/Internet （所有型号）和双功能端口 (Cisco RV016)。

根据需要执行以下操作。

- **更改 WAN 端口数 （仅限 Cisco RV016）的步骤：**使用下拉列表选择要启用的 WAN 端口数。默认选项为 2。如果您配置了其他 WAN 端口，则可使用双功能端口。



- **修改 WAN 设置的步骤：**如果在 “*Network*”页面上有未保存的更改，请在继续操作前单击 “**Save**”保存设置。对于要修改的接口，单击 “**Edit**”图标打开 “*Edit WAN Connection*”页面。有关详细信息，请参阅**编辑 WAN 连接，页码 30**。

DMZ 设置

在 Cisco RV042 和 Cisco RV082 上，您可以配置 Internet/DMZ 端口以用作 DMZ （De-Militarized Zone 或 De-Marcation Zone，停火区或分界区）。 Cisco RV016 有专用的 DMZ 端口。DMZ 允许 Internet 数据流访问网络上的指定主机，例如 FTP 服务器和 Web 服务器。其他网络资源则为专用资源。

此功能要求在 DMZ 上的每台主机上都有可公共路由的 IP 地址。您可联系您的 ISP，了解如何为此获得额外的 IP 地址。

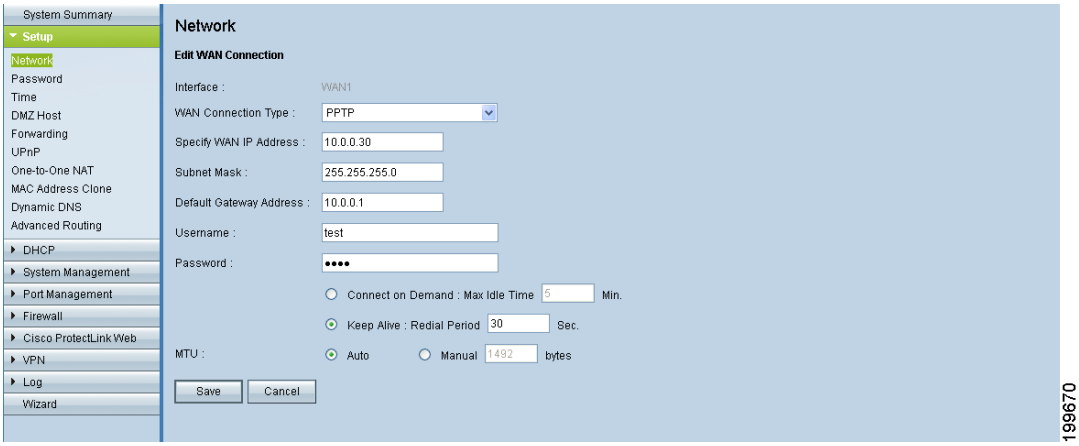
注意

- 应优先使用 DMZ，如果可行，强烈建议使用 DMZ 而非使用公共的 LAN 服务器或将这些服务器置于 WAN 端口，否则无法保护服务器并且 LAN 用户无法访问服务器。
- DMZ 上的每个服务器都需要唯一的公共 Internet IP 地址。您的 ISP 应能提供这些地址以及关于设置公共 Internet 服务器的信息。如果计划使用 DMZ 设置，请联系您的 ISP 获取静态 IP 信息。如果您的 ISP 仅提供一个静态 IP 地址或提供多个动态 IP 地址，请考虑使用 DMZ 主机功能。请参阅**设置 DMZ 主机，页码 36**。

根据需要执行以下操作。

- **在 DMZ/Internet 端口上启用 DMZ 的步骤**（**仅限 Cisco RV042 和 Cisco RV082**）：选中“**Enable DMZ**”复选框以启用此功能。然后按照以下说明编辑 DMZ 设置。如果希望将此端口用作 WAN 端口，取消选中该复选框，并确保在“*Dual WAN*”页面配置 WAN 设置。（请参阅**设置双 WAN 和多 WAN 连接，页码 60**。）
- **编辑 DMZ 设置的步骤**：单击“**Edit**”图标打开“*Edit DMZ Connection*”页面。有关详细信息，请参阅**编辑 DMZ 连接，页码 33**。如果您未保存设置，系统将显示警告消息。单击“**OK**”保存设置，或单击“**Cancel**”关闭窗口而不保存设置。

编辑 WAN 连接



单击 “*Network*” 页面的 “*WAN Settings*” 部分中的 “**Edit**” 图标后，将显示 “*Edit WAN Connection*” 页面。输入您的 ISP 提供的信息。

注意 离开此页面前，请单击 “**Save**” 保存设置，或单击 “**Cancel**” 撤消设置。所有未保存的更改都将被丢弃。

- **Interface**：显示所选 WAN 端口。此 ID 无法更改。
- **WAN Connection Type**：选择连接类型，如下所述。
  - **Obtain an IP Automatically**：如果 ISP 动态分配 IP 地址，则选择此选项。大多数电缆调制解调器用户都使用此连接类型。您的 ISP 将分配 DNS 服务器 IP 地址等设置。如果要指定 DNS 服务器，请选中 “**Use the Following DNS Server Addresses**” 框。然后，在 “**DNS Server (Required) 1**” 框中输入 IP 地址。作为可选操作，您可以输入第二个 DNS 服务器。系统将使用第一个可用 DNS 条目。
  - **Static IP**：如果 ISP 为您的帐户分配了永久 IP 地址，则选择此选项。然后，输入 ISP 提供的设置：

    Specify WAN IP Address：ISP 为您的帐户分配的外部 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 (Required) 1：指定的 DNS 服务器的 IP 地址。作为可选操作，输入第二个 DNS 服务器。系统将使用第一个可用 DNS 条目。

- **PPPoE (Point-to-Point Protocol over Ethernet)**：如果您的 ISP 使用 PPPoE （基于以太网的点对点协议）建立 Internet 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 和 **Password**：输入 ISP 帐户的用户名和密码。最多可包含 60 个字符。

  Connect on Demand：如果计费依据是连接到 Internet 的时间，则此功能可能十分有用。启用此功能后，如果连接在指定的时间段 （最长空闲时间）内处于不活动状态，则系统将断开连接。当您再次尝试访问 Internet 时，路由器将自动重新建立连接。如果启用此功能，请同时在 “**Max Idle Time**” 中输入值，以设置连接可以保持不活动状态的分钟数；当达到这一限值时，系统将终止连接。“Max Idle Time”的默认值为 5 分钟。

  Keep Alive：此功能可确保路由器始终连接到 Internet。启用此功能后，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。此选项可使连接无限期保持活动状态，即使在连接闲置时也是如此。如果启用此功能，请同时在 “**Redial Period**”中输入值，以指定路由器验证 Internet 连接的频率。默认周期为 30 秒。

- **PPTP (Point-to-Point Tunneling Protocol)**：如果您的 ISP 有要求，则选择此选项。 PPTP 是一种用于欧洲、以色列和其他国家 / 地区的服务。

  Specify WAN IP Address：ISP 为您的帐户分配的外部 IP 地址。

  Subnet Mask：ISP 指定的子网掩码。

  Default Gateway Address：默认网关的 IP 地址。

  Username 和 **Password**：输入 ISP 帐户的用户名和密码。最多可包含 60 个字符。

  Connect on Demand：如果计费依据是连接到 Internet 的时间，则此功能可能十分有用。启用此功能后，如果连接在指定的时间段 （最长空闲时间）内处于不活动状态，则系统将断开连接。当您再次尝试访问 Internet 时，路由器将自动重新建立连接。如果启用此功能，请同时在 “**Max Idle Time**” 中输入值，以设置连接可以保持不活动状态的分钟数；当达到这一限值时，系统将终止连接。“Max Idle Time”的默认值为 5 分钟。

  Keep Alive：此功能可确保路由器始终连接到 Internet。启用此功能后，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。此选项可使连接无限期保持活动状态，即使在连接闲置时也是如此。如果启用此功能，请同时在 “**Redial Period**”中输入值，以指定路由器验证 Internet 连接的频率。默认周期为 30 秒。

- **Transparent Bridge**：如果您在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 为您的帐户分配的外部 IP 地址。

  Subnet Mask：ISP 指定的子网掩码。

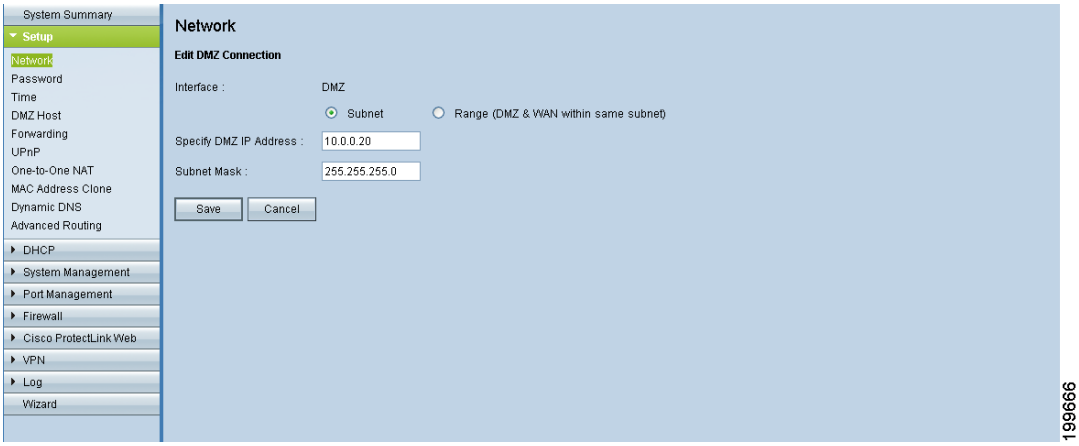
  Default Gateway Address：默认网关的 IP 地址。

  DNS Server (Required) 1：指定的 DNS 服务器的 IP 地址。作为可选操作，输入第二个 DNS 服务器。系统将使用第一个可用 DNS 条目。

  Internal LAN IP Range：将进行桥接的内部 LAN IP 范围。透明网桥的 WAN 和 LAN 将在同一子网中。

- **MTU**：最大传输单元 (MTU) 设置指定了允许进行网络传输的数据包大小上限。在大多数情况下，请保留默认值 “**Auto**”。要指定 MTU，请选择 “**Manual**”，然后输入最大 MTU 大小。

编辑 *DMZ* 连接



单击“*Network*”页面的“*DMZ Setting*”部分中的“**Edit**”图标后，将显示“*Edit DMZ Connection*”页面。

注意 离开此页面前，请单击“**Save**”保存设置，或单击“**Cancel**”撤消设置。所有未保存的更改都将被丢弃。

输入以下信息：

- **Subnet**：要将 DMZ 放置在与 WAN （默认设置）不同的子网中，请选择此选项。输入 DMZ IP 地址和子网掩码。
- **Range**：要将 DMZ 放置在与 WAN 相同的子网中，请选择此选项。输入要为 DMZ 端口预留的 IP 地址的范围。

更改管理员用户名和密码

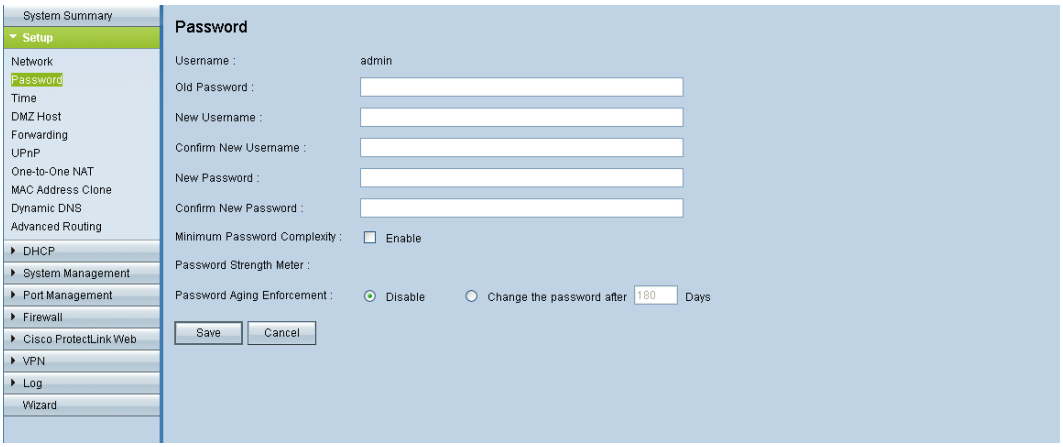
使用 “*Setup*” > “*Password*” 页面更新管理员用户名和密码。如果您愿意，也可以保留默认用户名 (admin)。但是，思科强烈建议将默认密码 (admin) 更改为不易猜测的高安全性密码。

警告 密码一旦丢失或遗忘，则无法恢复。若密码丢失或遗忘，您必须将路由器重置为出厂默认设置。重置后，所有配置更改都将被删除。

注意

- 如果在 “*Firewall*” > “*General*” 页面上启用远程访问，您必须更改管理员密码。
- 离开此页面前，请单击 “**Save**” 保存设置，或单击 “**Cancel**” 撤消设置。更改用户名或密码后，当您在导航树中选择任一选项时，系统会要求您使用新凭证登录。

打开此页面的步骤：在导航树中单击 “**Setup**” > “**Password**”。



- **Old Password**：输入旧密码。默认的密码为 **admin**。
- **New Username**：输入新的用户名 （如有需要）。要保留现有用户名，请将此字段留空。
- **Confirm New Username**：要进行确认，请完全按照上一个字段中显示的内容再次输入新的用户名。

- **New Password**：输入路由器的新密码。密码中可以包含字母数字字符和符号，但不能包含空格。
- **Confirm New Password**：要进行确认，请完全按照上一个字段中显示的内容再次输入新密码。如果两次输入的密码不一致，系统会显示错误消息。
- **Minimum Password Complexity**：如果您希望增强密码的复杂性并启用“Password Strength Meter”，请选中 “**Enable**”框。默认情况下，此选项为启用状态，而且我们也建议启用此选项。

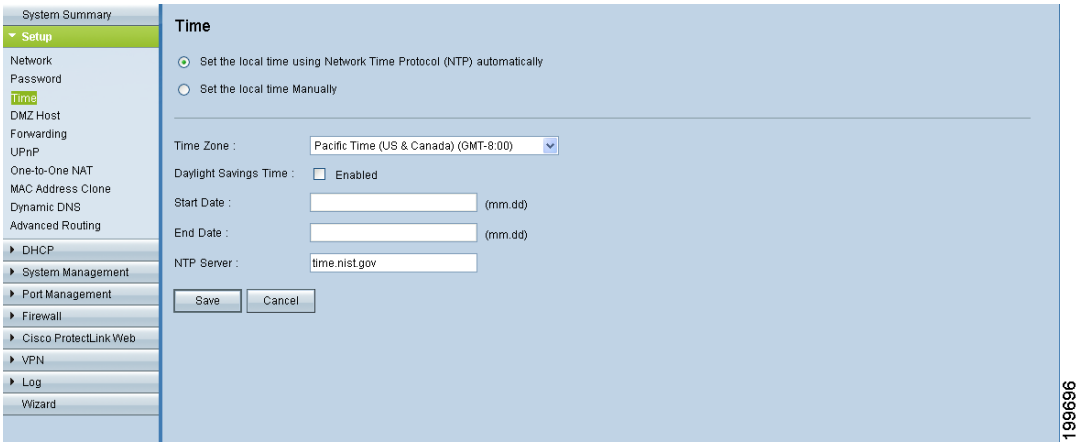
  启用 “Minimum Password Complexity”后，密码必须满足下列要求。单击“Save”按钮后，条目生效。

  - 至少包含 8 个字符。
  - 与用户名不同。
  - 与当前密码不同。
  - 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。
- **Password Strength Meter**：如果启用 “Minimum Password Complexity”，则 “Password Strength Meter”会根据复杂性规则指示密码强度。当您输入密码时，会出现彩色条。该彩色条包括红色 （不可接受）、黄色 （可接受）和绿色 （高安全性）三个等级。
- **Password Aging Enforcement**：如果您不希望密码过期，请选择 “**Disable**”。如果您希望密码在 “**Days**”中指定的天数 （默认为 180 天）后过期，请选择 “**Change the password after**”。

设置系统时间

通过 “*Setup*” > “*Time*”页面指定网络的系统时间。路由器使用时间设置标记日志事件的时间、自动应用访问规则和内容过滤器，以及为实现其他内部目的而执行其他活动。您可以允许路由器自动从服务器接收本地时间设置，或者您也可以手动输入本地时间。

打开此页面的步骤：在导航树中单击 “**Setup**” > “**Time**”。



注意 离开此页面前，请单击 “**Save**”保存设置，或单击 “**Cancel**”撤消设置。所有未保存的更改都将被丢弃。

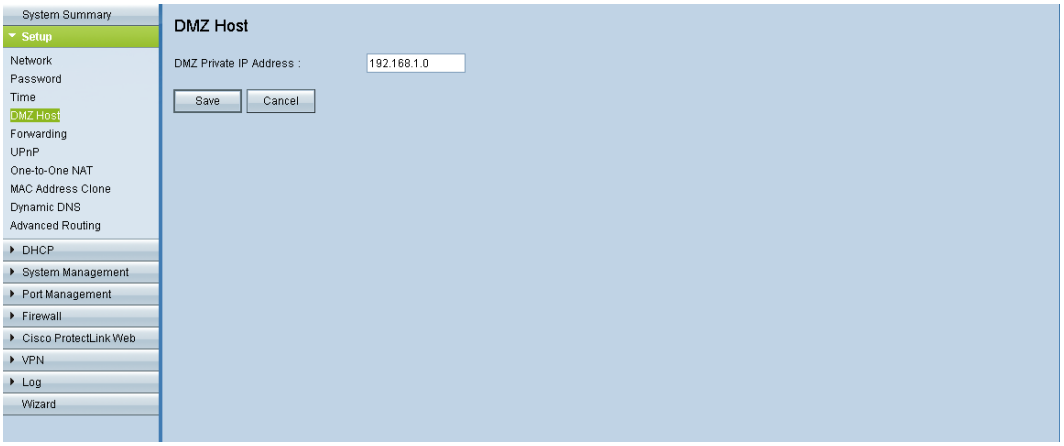
请选择以下选项之一来设置时间，然后输入所需信息。

- **Set the local time using Network Time Protocol (NTP) automatically**：要允许路由器自动从 NTP 服务器接收时间设置，请选择此选项。然后输入以下设置：
  - **Time Zone**：选择时区。默认为 **(GMT-08:00) Pacific Time (US & Canada); Tijuana**。
  - **Daylight Saving**：要自动调整夏令时，请选择 “**Enabled**”。在 “**Start Date**”字段中输入夏令时开始的月和日。请使用 mm.dd 格式，例如 6 月 25 日为 6.25。另外，请以相同的格式输入 “**End Date**”。
  - **NTP Server**：输入 NTP 服务器的 URL 或 IP 地址。默认为 *time.nist.gov*。
- **Set the local time Manually**：如果您希望自己设置本地时间，请选择此选项。然后输入以下信息：
  - **Date**：以 yyyy.mm.dd 格式输入当前日期，例如 2010 年 6 月 25 日为 2010.06.25。
  - **Hours, Minutes, Seconds**：以 hh:mm:ss 格式输入当前时间，例如下午 3:17:00 为 15:17:00。

设置 DMZ 主机

使用 “*Setup*” > “*DMZ Host*”页面允许网络上的某一设备作为 DMZ （非军事区）主机运行。此功能允许公共访问专用服务，例如 Internet 游戏和视频会议。

打开此页面的步骤：在导航树中单击 “**Setup**” > “**DMZ Host**”。



输入要用作 DMZ 主机的网络设备的 IP 地址。

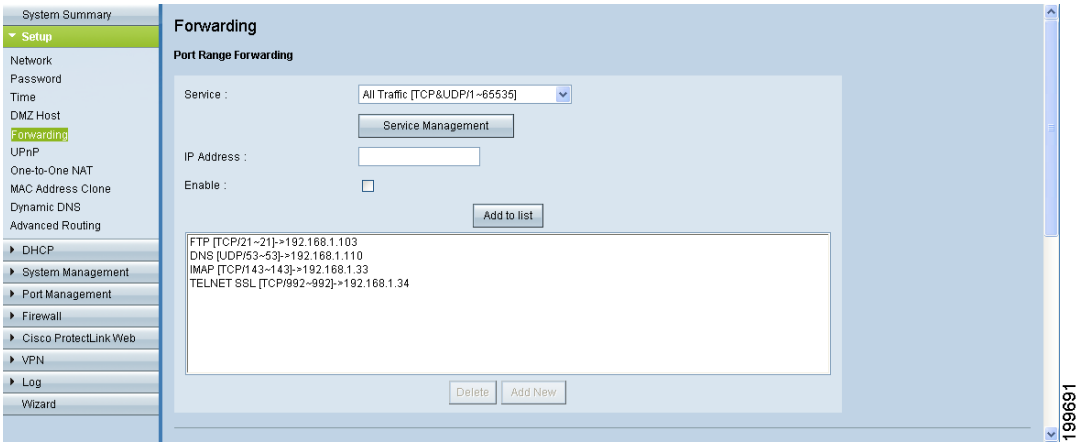
注意 离开此页面前，请单击 “**Save**”保存设置，或单击 “**Cancel**”撤消设置。所有未保存的更改都将被丢弃。

设置端口转发和端口触发

如果您需要允许公共访问连接至 LAN 端口的计算机上的服务，请使用 “*Setup*” > “*Forwarding*”页面。端口转发功能会为服务 （例如 FTP）打开指定端口或端口范围。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 Internet 游戏）打开端口范围。该页面包括以下部分：

- **端口范围转发，页码 38**
- **端口触发，页码 40**

打开此页面的步骤：在导航树中单击 “**Setup**” > “**Forwarding**”。



注意 离开此页面前，请单击 “**Save**”保存设置，或单击 “**Cancel**”撤消设置。所有未保存的更改都将被丢弃。

端口范围转发

端口转发可用于设置网络上的公共服务。当 Internet 用户向您的网络发出特定请求时，路由器可将这些请求转发给能够处理请求的计算机。例如，如果您设置将端口号 80 (HTTP) 转发到 IP 地址 192.168.1.2，则来自外部用户的所有 HTTP 请求都将转发到 192.168.1.2。

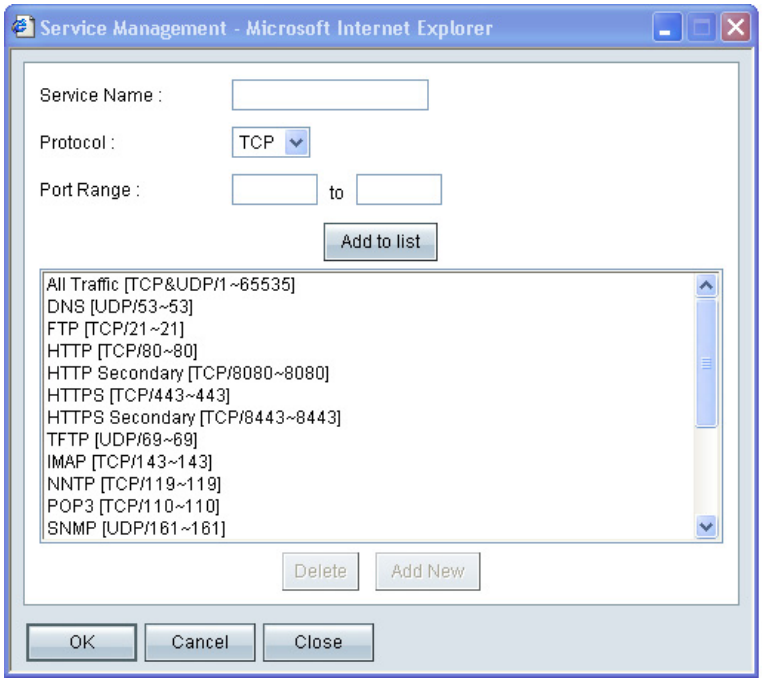
您可使用此功能通过 IP 网关建立 Web 服务器或 FTP 服务器。请确保您输入的 IP 地址是有效的。（要使 Internet 服务器正常运行，您可能需要建立静态 IP 地址。）为了提高安全性， Internet 用户将能够与服务器进行通信，但他们将无法实际建立连接。数据包只是通过路由器进行转发。

- **在列表中添加条目的步骤**：输入以下信息，然后单击 “**Add to list**”。
  - **Service**：选择服务。如果某个服务未列出，您可以添加服务。有关详细信息，请参阅**添加服务，页码 39**。
  - **IP Address**：输入您希望 Internet 用户访问的服务器的 LAN IP 地址。
  - **Enable**：选中此框可启用此端口范围转发条目。
- **添加另一新条目的步骤**：输入信息，然后单击 “**Add to list**”。
- **修改列表中条目的步骤**：单击要修改的条目。相关信息将显示在文本字段中。进行更改，然后单击 “**Update**”。如果无需进行更改，则可以单击 “**Add New**”，以取消选中该条目并清空文本字段。

- **从列表中删除条目的步骤**：单击要删除的条目，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。要选择多个单一条目，请按住 Ctrl 键然后单击每个条目。要取消选中某个条目，请按住 Ctrl 键的同时单击该条目。
- **查看端口范围表的步骤**：单击页面底部附近的 “**View**”。选择 “**Port Range Forwarding**” 或 “**Port Triggering**”。要更新显示内容，请单击 “**Refresh**”。要返回 “*Forwarding*” 页面，请单击 “**Close**”。

添加服务

要在 “*Service*” 列表中添加新条目或者更改之前创建的条目，请单击 “**Service Management**”。如果 Web 浏览器显示关于弹出窗口警告，请允许显示被阻止的内容。



在 “*Service Management*” 窗口中，根据需要添加或更新条目。关闭此窗口前，请单击 “**OK**” 保存设置，或单击 “**Cancel**” 撤消设置。所有未保存的更改都将被丢弃。

- **在列表中添加服务的步骤**：输入以下信息，然后单击 “**Add to List**”。列表中最多可包含 30 个服务。
  - **Service Name**：输入简短说明。
  - **Protocol**：选择所需协议。请参阅您托管的服务的相关文档。

- **Port Range**：输入所需的端口范围。

- **添加另一新服务的步骤**：输入信息，然后单击 “**Add to list**”。
- **修改已创建的服务的步骤**：单击列表中的服务。相关信息将显示在文本字段中。进行更改，然后单击 “**Update**”。如果无需进行更改，则可以单击 “**Add New**”，以取消选中该服务并清空文本字段。
- **从列表中删除服务的步骤**：单击要删除的条目。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。要选择多个单一条目，请按住 Ctrl 键然后单击相应条目。单击 “**Delete**”。

端口触发

端口触发允许路由器监视指定端口号的传出数据。路由器会记住发送匹配数据的计算机的 IP 地址，以便当请求的数据通过路由器返回时，路由器将使用 IP 地址和端口映射规则将数据传输到正确的计算机。

某些 Internet 应用程序或游戏使用替换端口在服务器和 LAN 主机之间进行通信。当您想要使用这些应用程序时，请在 “*Port Triggering*” 表中输入触发 （传出）端口和备用传入端口。随后，路由器会将传入数据包转发至指定的 LAN 主机。

根据需要添加或编辑条目。请记住，只有单击 “Save” 按钮后，设置才会保存。

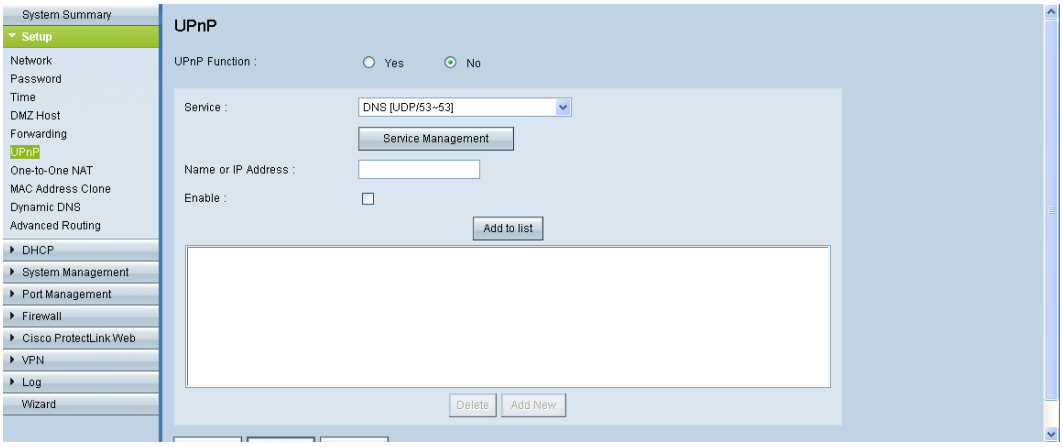
- **在列表中添加条目的步骤**：输入以下信息，然后单击 “**Add to List**”。列表中最多可包含 30 个应用程序。
  - **Application Name**：输入应用程序的名称。
  - **Trigger Port Range**：输入触发端口范围的起始和终止端口号。请参阅应用程序的文档。
  - **Incoming Port Range**：输入传入端口范围的起始和终止端口号。请参阅应用程序的文档。
  - **Enable**：选中此框可启用应用程序的端口触发。取消选中此框可禁用应用程序。
- **添加另一新条目的步骤**：输入信息，然后单击 “**Add to list**”。
- **修改列表中条目的步骤**：单击要修改的条目。相关信息将显示在文本字段中。进行更改，然后单击 “**Update**”。如果无需进行更改，则可以单击 “**Add New**”，以取消选中该条目并清空文本字段。
- **从列表中删除条目的步骤**：单击要删除的条目，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。要选择多个单一条目，请按住 Ctrl 键然后单击每个条目。要取消选中某个条目，请按住 Ctrl 键的同时单击该条目。

- **查看端口范围表的步骤**：单击页面底部附近的 “**View**”。选择 “**Port Range Forwarding**”或 “**Port Triggering**”。要更新显示内容，请单击 “**Refresh**”。要返回 “*Forwarding* ”页面，请单击 “**Close**”。

设置通用即插即用 (UPnP)

使用 “*Setup*” > “*UPnP*” 页面可启用通用即插即用 (UPnP)。此功能允许 Windows 自动配置路由器，为游戏和视频会议等 Internet 应用程序打开和关闭端口。

打开此页面的步骤：在导航树中单击 “**Setup**” > “**UPnP**”。



注意

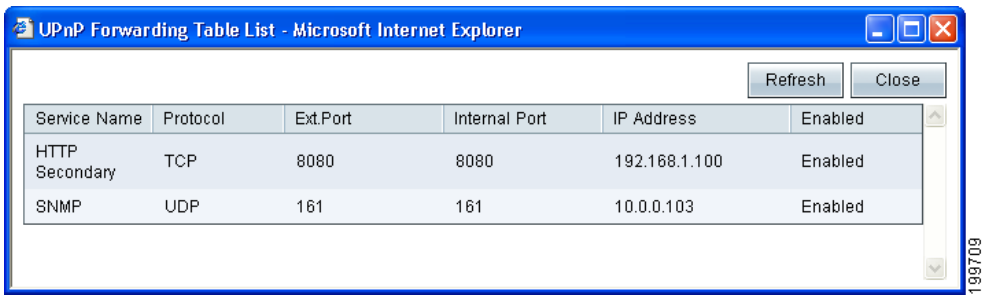
- 除非应用程序需要使用 UPnP，否则为安全起见，请将其禁用。
- 离开此页面前，请单击 “**Save**”保存设置，或单击 “**Cancel**”撤消设置。所有未保存的更改都将被丢弃。

要启用 UPnP，请单击 “**Yes**”。要禁用此功能，请单击 “**No**”。根据需要添加或编辑条目。

- **在列表中添加条目的步骤**：输入以下信息，然后单击 “**Add to List**”。列表中最多可包含 30 个服务。
  - **Service**：选择服务。如果某个服务未列出，您可以添加服务。请参阅**添加服务，页码 42**。
  - **Name or IP Address**：输入 UPnP 设备的名称或 IP 地址。
  - **Enable**：选择 “**Enable**”可启用此 UPnP 条目。

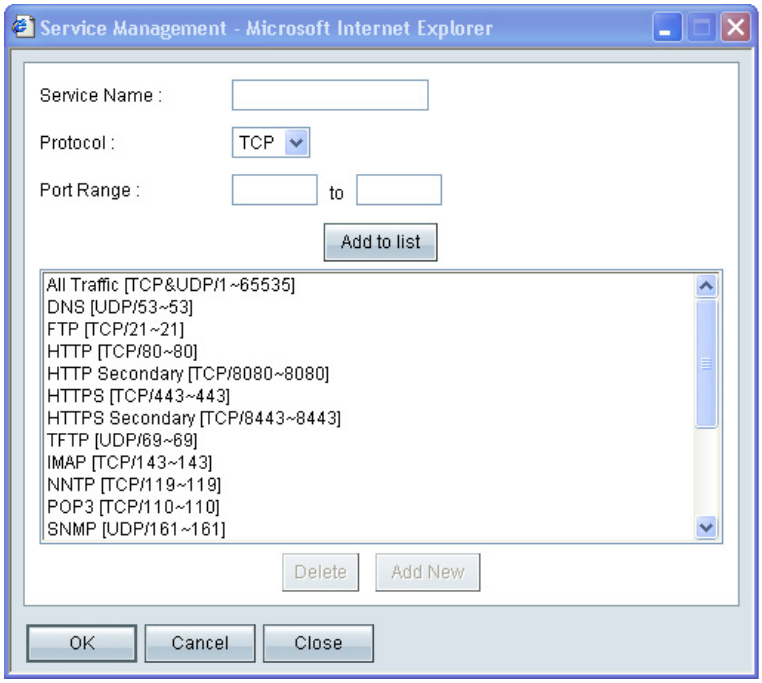
- **添加另一新条目的步骤**：输入信息，然后单击 “**Add to list**”。
- **修改列表中条目的步骤**：单击要修改的条目。相关信息将显示在文本字段中。进行更改，然后单击 “**Update**”。如果无需进行更改，则可以单击 “**Add New**”，以取消选中该条目并清空文本字段。
- **从列表中删除条目的步骤**：单击要删除的条目，然后单击 “**Delete**”。要选择某个区域内的所有条目，请单击第一个条目，按住 Shift 键，然后单击该区域中的最后一个条目。要选择多个单一条目，请按住 Ctrl 键然后单击每个条目。要取消选中某个条目，请按住 Ctrl 键的同时单击该条目。

  “*UPnP Forwarding Table List*”将显示当前数据。您可以单击 “**Refresh**”更新数据，或单击 “**Close**”关闭弹出窗口。
- **查看 UPnP 转发表的步骤**：单击页面底部附近的 “**View**”。要更新显示内容，请单击 “**Refresh**”。要返回 “*UPnP* ”页面，请单击 “**Close**”。



添加服务

要在 “*Service*”列表中添加新条目或者更改之前创建的条目，请单击 “**Service Management**”。如果 Web 浏览器显示关于弹出窗口警告，请允许显示被阻止的内容。



在“*Service Management*”窗口中，根据需要添加或更新条目。关闭此窗口前，请单击“**OK**”保存设置，或单击“**Cancel**”撤消设置。所有未保存的更改都将被丢弃。

- **在列表中添加服务的步骤**：输入以下信息，然后单击“**Add to List**”。列表中最多可包含 30 个服务。
  - **Service Name**：输入简短说明。
  - **Protocol**：选择所需协议。请参阅您托管的服务的相关文档。
  - **Port Range**：输入所需的端口范围。
- **添加另一新服务的步骤**：输入信息，然后单击“**Add to list**”。
- **修改已创建的服务的步骤**：单击列表中的服务。相关信息将显示在文本字段中。进行更改，然后单击“**Update**”。如果无需进行更改，则可以单击“**Add New**”，以取消选中该服务并清空文本字段。
- **从列表中删除服务的步骤**：单击要删除的条目。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。要选择多个单一条目，请按住 Ctrl 键然后单击相应条目。单击“**Delete**”。

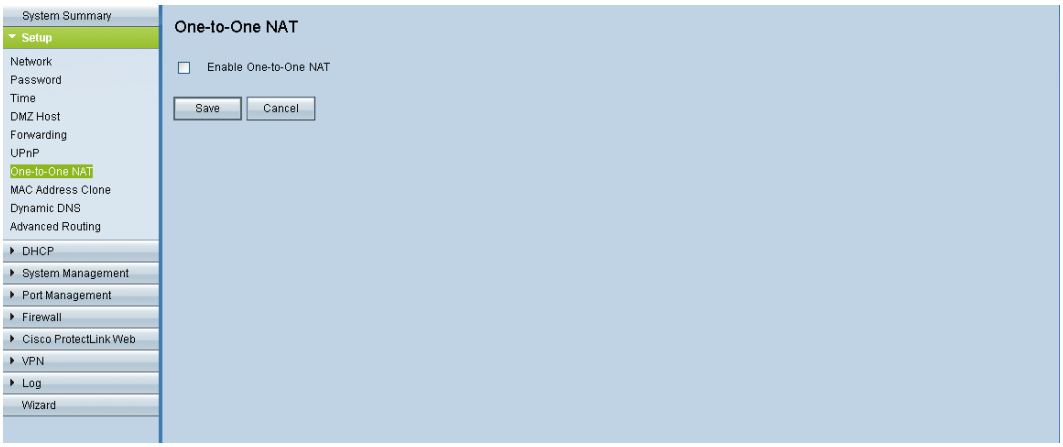
设置一对一 NAT

使用 “*Setup*” > “*One-to-One NAT*”页面启用一对一 NAT （网络地址转换）。在此过程中，系统会创建一种将有效的外部 IP 地址映射到 NAT 隐藏的内部 IP 地址的关系。随后，流量便可从 Internet 路由到指定的内部资源。

注意 为了获得最佳结果，请为您希望通过一对一 NAT 访问的内部资源预留 IP 地址。请参阅 **静态 IP 地址，页码 55**。

您可以映射单个关系，也可以将内部 IP 地址范围映射到长度相等的外部范围 （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。

打开此页面的步骤：在导航窗格中单击 “**Setup**” > “**One-to-One NAT**”。



注意 离开此页面前，请单击 “**Save**”保存设置，或单击 “**Cancel**”撤消设置。所有未保存的更改都将被丢弃。

要启用此功能，请选中 “**Enable One-to-One NAT**”框。根据需要添加或编辑条目。

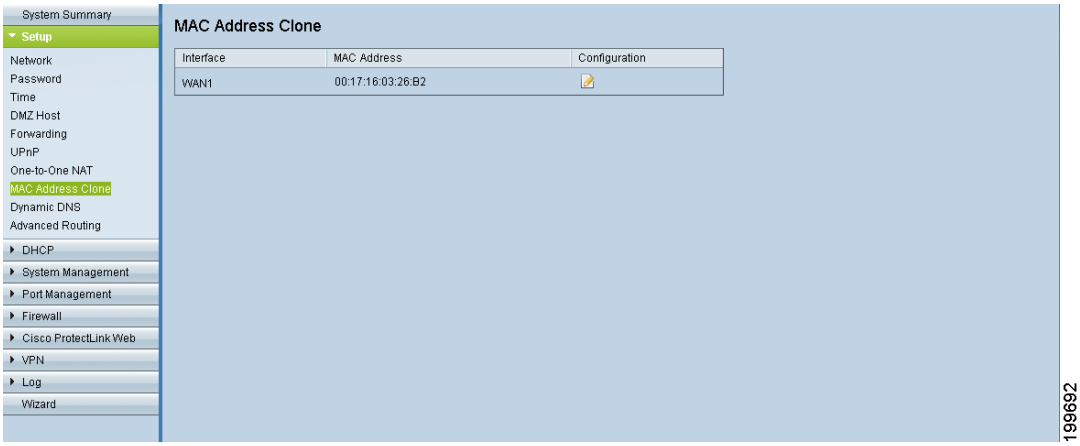
- **在列表中添加条目的步骤**：输入以下信息，然后单击 “**Add to List**”。
  - **Private Range Begin**：输入要映射到公共范围的内部 IP 地址范围的起始 IP 地址。请勿在此范围中包含路由器的 LAN IP 地址。
  - **Public Range Begin**：输入 ISP 提供的公共 IP 地址范围的起始 IP 地址。请勿在此范围中包含路由器的 WAN IP 地址。
  - **Range Length**：输入此范围中 IP 地址的数量。范围长度不能超过有效 IP 地址的数量。要映射单个地址，请输入 1。
- **添加另一新条目的步骤**：输入信息，然后单击 “**Add to list**”。

- **修改列表中条目的步骤**：单击要修改的条目。相关信息将显示在文本字段中。进行更改，然后单击“**Update**”。如果无需进行更改，则可以单击“**Add New**”，以取消选中该条目并清空文本字段。
- **从列表中删除条目的步骤**：单击要删除的条目，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。要选择多个单一条目，请按住 Ctrl 键然后单击每个条目。要取消选中某个条目，请按住 Ctrl 键的同时单击该条目。

复制路由器的 MAC 地址

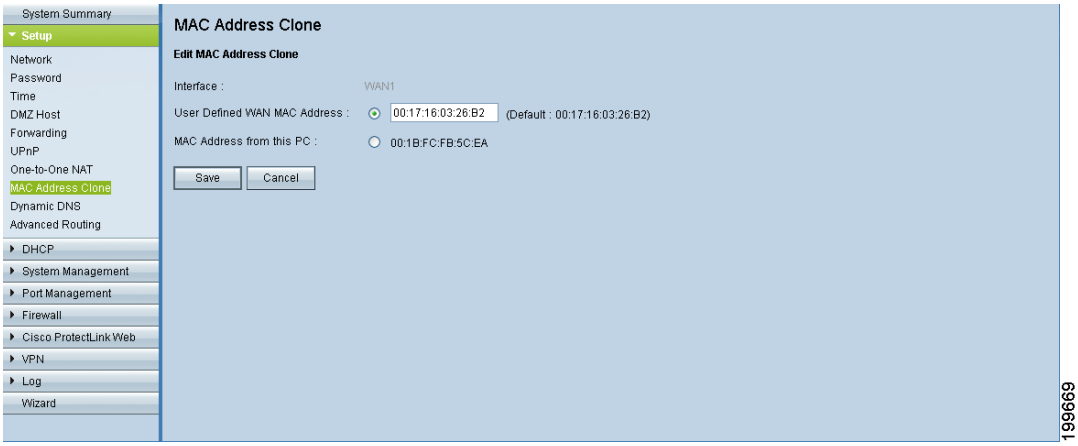
某些 ISP 会要求您注册 MAC 地址，该地址是一个 12 位的代码，被分配给相应的唯一硬件以用于进行身份识别。如果您之前已通过 ISP 注册了另一 MAC 地址，则可以使用“*Setup*”>“*MAC Address Clone*”页面将该地址“复制”到您的 Cisco RV0xx 系列路由器。通过使用此过程，您不必联系 ISP 更改已注册的 MAC 地址。

打开此页面的步骤：在导航树中单击“**Setup**”>“**MAC Address Clone**”。



此页面将显示当前设置。单击“**Edit**”图标以显示“*Edit MAC Address Clone*”页面。有关详细信息，请参阅**编辑 MAC 地址复制设置，页码 46**。

编辑 *MAC* 地址复制设置



单击“*MAC Address Clone*”页面上的“**Edit**”图标后，将显示“*Edit MAC Address Clone*”页面。

注意 离开此页面前，请单击“**Save**”保存设置，或单击“**Cancel**”撤消设置。所有未保存的更改都将被丢弃。

要复制 MAC 地址，请输入以下设置。

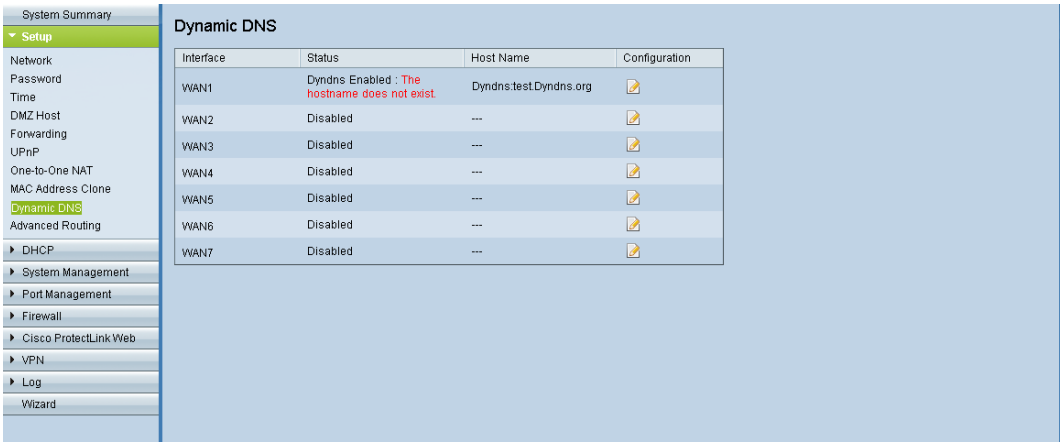
- **User Defined WAN MAC Address**：要手动复制 MAC 地址，请单击此单选按钮，然后输入通过您的 ISP 注册的 12 位 MAC 地址。
- **MAC Address from this PC**：要复制您当前用于配置路由器的计算机的 MAC 地址，请单击此单选按钮。此时将自动显示您的 PC 的 MAC 地址。

为 WAN 接口分配动态 DNS 主机名

通过动态域名系统 (DDNS) 服务，您可以为动态 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。使用“*Setup*”>“*Dynamic DNS*”页面，根据您的动态 DNS 信息配置 WAN 接口。

在路由器上配置动态 DNS 之前，您需要访问 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。

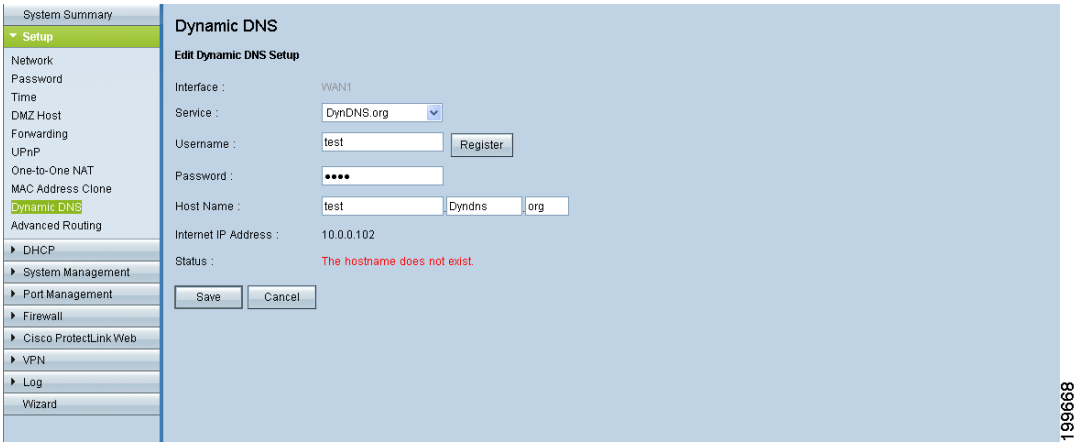
打开此页面的步骤：在导航树中单击“**Setup**”>“**Dynamic DNS**”。



注意 离开此页面前，请单击“**Save**”保存设置，或单击“**Cancel**”撤消设置。所有未保存的更改都将被丢弃。

此页面将显示当前设置。单击 WAN 接口的“**Edit**”图标，以显示“*Edit Dynamic DNS Setup*”页面。有关详细信息，请参阅**编辑动态 DNS 设置，页码 48**。

编辑动态 *DNS* 设置



单击 “*Dynamic DNS*” 页面上的 “**Edit**” 图标后，将显示 “*Edit Dynamic DNS Setup*” 页面。

注意 离开此页面前，请单击 “**Save**” 保存设置，或单击 “**Cancel**” 撤消设置。所有未保存的更改都将被丢弃。

从 “**DDNS Service**” 列表中，选择您的服务。然后，输入下述帐户信息。要禁用此功能，请选择 “**Disable**”。

- **Username**：输入您的 DDNS 帐户的用户名。

  如果您之前未注册任何主机名，则可以单击 “**Register**” 转至 DynDNS.com 网站并在其中免费注册动态 DNS 服务。单击 “**Sign up FREE**” 链接，然后继续完成所有步骤。

- **Password**：输入您的 DDNS 帐户的密码。

- **Host Name**：在这三个字段中输入您向 DDNS 提供商注册的主机名。例如，如果您的主机名是 *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**：接口的当前 WAN IP 地址。由于该地址是动态的，所以此项设置将会更改。

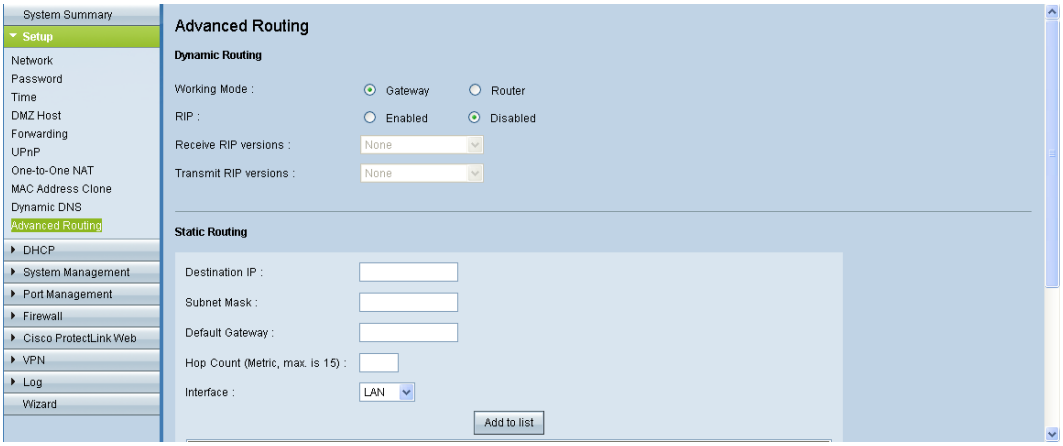
- **Status**：DDNS 功能的状态。如果状态信息指示发生错误，请确保您输入的 DDNS 服务帐户信息是正确的。

设置高级路由

使用 “*Setup*” > “*Advanced Routing*”页面配置动态和静态路由设置。请参阅以下部分：

- **配置动态路由，页码 49**
- **配置静态路由，页码 50**

打开此页面的步骤：在导航树中单击 “**Setup**” > “**Advanced Routing**”。



注意 离开此页面前，请单击 “**Save**”保存设置，或单击 “**Cancel**”撤消设置。所有未保存的更改都将被丢弃。

配置动态路由

动态路由使路由器能够自动调整以适应网络布局的物理更改。通过使用动态 RIP 协议，路由器可以计算网络数据包在源和目标之间传输的最有效路由方式。 RIP 协议会定期向网络中的其他路由器广播路由信息。它会以源和目标之间的跃点数最少为基础，决定最佳路由方式。

输入下述设置。

- **Working Mode**：请选择以下选项之一。
  - **Gateway**：如果路由器正在托管您的 Internet 网络连接，请选择此模式。此选项为系统默认的设置。
  - **Router**：如果有其他路由器和此路由器一起存在于网络上，并且另一个路由器充当连接 Internet 的网络网关，请选择此模式。在 Router 模式中，仅当您有另一个路由器充当网关时， Internet 连接才可用。由于网关路由器提供了防火墙保护，因此请禁用此路由器的防火墙。请参阅**配置常规防火墙设置，页码 81**。

- **RIP**：路由信息协议 (RIP) 允许路由器之间自动交换路由信息，并在网络发生变化时动态调整自己的路由表。 RIP 使用跃点限制来预防路由环路。要启用此选项，请选择 “**Enabled**”。否则，请选择 “**Disabled**”，保留默认设置。如果启用此功能，请同时配置以下设置：
- **Receive RIP versions**：选择用于接收网络数据的 RIP 协议：“**None**”、“**RIPv1**”、“**RIPv2**”或 “**Both RIP v1 and v2**”。

  RIPv1 是一种基于类的路由版本。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验证安全。
- **Transmit RIP versions**：选择用于传输网络数据的 RIP 协议：“**None**”、“**RIPv1**”、“**RIPv2 - Broadcast**”或 “**RIPv2 - Multicast**”。

  “**RIPv2 - Broadcast**”（建议设置）会在整个子网中广播数据。“**RIPv2 - Multicast**”会将数据发送到多播地址。“RIPv2 - Multicast”会将路由表多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。
- **查看当前数据的步骤**：单击页面底部附近的 “**View**”。此时将显示 “*Routing Table Entry List*”。您可以单击 “**Refresh**”更新数据，或单击 “**Close**”关闭弹出窗口。

配置静态路由

如果路由器连接到多个网络或网络中安装有多个路由器，则可能有必要在路由器之间设置静态路由。静态路由功能决定了数据在通过此路由器之前和之后通过网络的路径。您可以使用静态路由来允许不同的 IP 域用户通过路由器访问 Internet。

静态路由功能十分强大，应仅由高级用户使用。在许多情况下，最好使用动态路由，因为动态路由使路由器能够自动调整以适应网络布局的物理更改。

警告 静态路由是一种高级功能。请谨慎创建此类路由。

根据需要添加或编辑条目。请记住，只有单击 “Save”按钮后，设置才会保存。

- **添加新的静态路由的步骤**：输入以下设置，然后单击 “**Add to List**”。您最多可输入 30 个路由。
  - **Destination IP**：输入远程 LAN 区段的网络地址。对于标准 C 类 IP 域，该网络地址为目标 LAN IP 地址的前三个字段，而最后一个字段应为 0。
  - **Subnet Mask**：输入目标 LAN IP 域上所用的子网掩码。对于 C 类 IP 域，相应的子网掩码为 255.255.255.0。

- **Default Gateway**：输入网络路由器的 IP 地址，即为其创建此静态路由的地址。例如，如果此网络通过另一路由器连接到本地路由器的 LAN 端口，则请使用该路由器的 WAN IP 地址。
- **Hop Count**：输入适当的值 （最大为 15）。该值表示数据包在到达其目的地前所通过的节点数。节点可以是网络上的任何设备，例如计算机或路由器。
- **Interface**：选择要用于此路由的接口。如果此路由器为您的网络提供 Internet 连接，请选择 WAN 接口。如果此路由器通过 LAN 上的网关路由器获得 Internet 连接，请选择 “**LAN**”。

- **添加另一新静态路由的步骤**：输入信息，然后单击 “**Add to list**”。
- **修改列表中静态路由的步骤**：单击要修改的条目。相关信息将显示在文本字段中。进行更改，然后单击 “**Update**”。如果无需进行更改，则可以单击 “**Add New**”，以取消选中该条目并清空文本字段。
- **从列表中删除条目的步骤**：单击要删除的条目，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。
- **查看当前数据的步骤**：单击页面底部附近的 “**View**”。此时将显示 “*Routing Table Entry List*”。您可以单击 “**Refresh**” 更新数据，或单击 “**Close**” 关闭弹出窗口。

4

DHCP

使用 *DHCP* 模块配置 DHCP 服务器或 DHCP 中继代理的设置，并查看 DHCP 概要信息。请参阅以下主题：

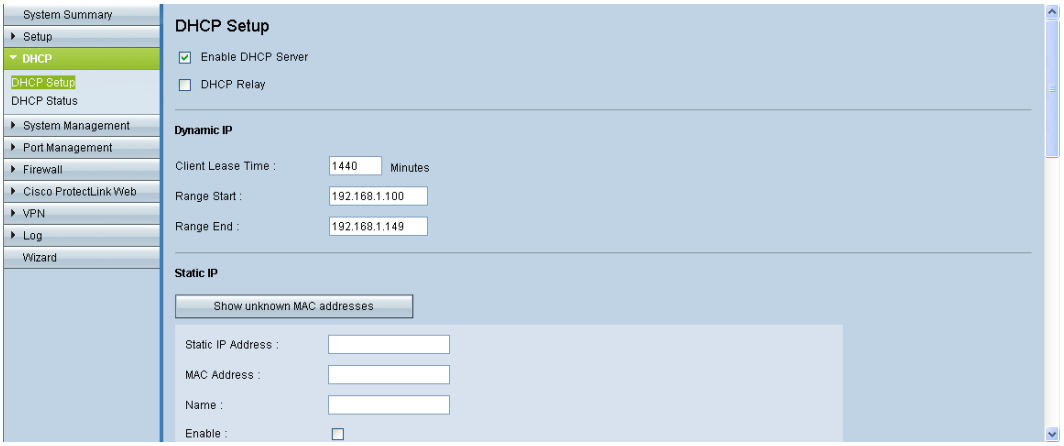
- **设置 DHCP 服务器或 DHCP 中继，页码 52**
- **查看 DHCP 状态信息，页码 58**

设置 DHCP 服务器或 DHCP 中继

使用 *“DHCP”* > *“DHCP Setup”* 页面将此路由器配置为 DHCP （动态主机配置协议）服务器或配置为 DHCP 中继代理。 DHCP 服务器会自动向网络上的计算机分配可用 IP 地址。客户端在指定时间内 “租用” 某个地址，过期后，该地址可以分配给其他设备。如果设备需要拥有不发生变化的 IP 地址，则可以将此设备添加到 Static IP 列表中。作为可选操作，您可以使用 Static IP 列表来阻止列表中未列出的设备或没有正确 IP 地址的设备进行访问。

如果网络中有另一 DHCP 服务器，或者如果您想要手动分配 IP 地址，则可以禁用 DHCP 功能并启用 DHCP 中继。有关详细信息，请参阅**启用 DHCP 服务器或 DHCP 中继，页码 53**。

打开此页面的步骤：在导航树中单击 “**DHCP**” > “**DHCP Setup**”。



注意 离开此页面前，请单击 “**Save**”保存设置，或单击 “**Cancel**”撤消设置。所有未保存的更改都将被丢弃。

启用 DHCP 服务器或 DHCP 中继

请选择以下选项之一：

- **Enable DHCP server**：如果启用此功能，则路由器最多可以将 IP 地址动态分配给 50 台连接的设备。

  *必需：*在此页面的 “**Dynamic IP**”部分中输入设置，如下所述。此页面的其他部分都是可选的。

- **Enable DHCP Relay**：如果您有另一 DHCP 服务器，则启用 DHCP 中继可以允许此路由器将客户端的 DHCP 请求传递给 DHCP 服务器。DHCP 中继机制允许 DHCP 客户端和 DHCP 服务器位于不同的网络。DHCP 客户端将发送 DHCP 发现广播数据包，以便从 DHCP 服务器处获取 IP 地址。此路由器将充当 DHCP 中继代理，向 DHCP 服务器发送 DHCP 单播。

  *必需：*在 “**DHCP Server IP Address**”中输入内容。此页面的其他部分都是可选的。

注意 如果 DHCP 服务器和 DHCP 中继都已禁用，请为网络中的每个设备都配置静态 IP 地址、子网掩码和 DNS 设置。确保您不会将同一 IP 地址分配给不同的计算机。

动态 IP（仅限 DHCP 服务器）

- **Client Lease Time**：即客户端租用时间，是指允许网络用户使用当前动态 IP 地址连接到路由器的时间量。输入时间量（单位：分钟）。范围为 5-43,200 分钟。默认为 1440 分钟（24 小时）。

  请注意：要从 DHCP 服务器接收 IP 地址，必须将客户端设备配置为自动从 DHCP 服务器获取 IP 地址。默认情况下， Windows 计算机设置为自动获取 IP。

- **Range Start** 和 **Range End**：输入起始 IP 地址和结束 IP 地址，以创建可动态分配的 IP 地址的范围。此范围最多可以包含 50 个 IP 地址，这也是服务器可以分配的最大数量。默认范围为 100-149。请确保路由器的 LAN IP 地址不在此动态 IP 范围之内。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（仅限 DHCP 服务器）

作为可选操作，输入 **DNS 服务器**的 IP 地址。您也可以输入辅助 DNS 服务器。相比于使用经由 WAN 设置动态分配的 DNS 服务器，指定 DNS 服务器可以提供更快的访问速度。您可以保留默认设置 0.0.0.0，以使用动态分配的 DNS 服务器。

WINS（仅限 DHCP 服务器）

作为可选操作，输入 **WINS 服务器**的 IP 地址。 Windows Internet 命名服务会将 NetBIOS 名称解析为 IP 地址。如果您不知道 WINS 服务器的 IP 地址，请保留默认值 0.0.0.0。

注意 为了对 DHCP 客户端支持 NetBIOS，路由器使用两种方法：

- 当 DHCP 客户端从路由器接收动态 IP 地址时，它会自动包含 WINS 服务器的信息，以支持 NetBIOS。
- 如果客户端拥有静态 IP 地址，则必须在 Windows 操作系统的 Internet 协议 (TCP/IP) 页面上配置 IP 地址、子网掩码、默认网关地址和 DNS 服务器设置。然后，必须在高级 TCP/IP 页面上配置 WINS IP 地址。（有关详细信息，请参阅 Windows 帮助。）

静态 IP 地址

启用 DHCP 后，您可能希望将静态 IP 地址分配给某些设备，例如 Web 服务器或 FTP 服务器。您最多可以将 100 个设备添加到 “*Static IP*” 列表中。

TIP 请确保所有这些设备都已配置为使用此静态 IP 地址。例如，在 Windows 计算机中，打开 “本地连接属性”，选择 “**Internet 协议 (TCP/IP)**”，然后单击 “**属性**” 按钮。选择 “**使用下面的 IP 地址**”，然后输入 IP 地址、子网掩码和默认网关 （路由器 IP 地址）。作为可选操作，输入首选 DNS 服务器。

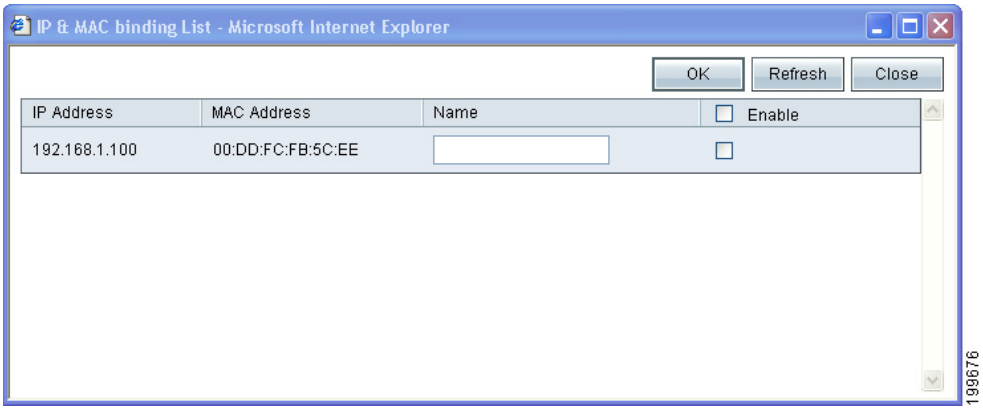
从列表中选择设备，或手动输入设备 IP 地址和 MAC 地址。

- **通过从列表中添加设备来分配静态 IP 地址，页码 55**
- **通过手动输入设备来分配静态 IP 地址，页码 56**
- **使用静态 IP 列表阻止设备，页码 57**

注意 即使路由器不是 DHCP 服务器，您仍可以使用此功能。

通过从列表中添加设备来分配静态 IP 地址

步骤 1 单击 “**Show unknown MAC addresses**”。此时将显示 “*IP & MAC binding list*”。如果 Web 浏览器显示弹出窗口消息，请允许显示被阻止的内容。



设备按 IP 地址和 MAC 地址列出。（MAC 地址通常显示在设备底部面板或后面板的标签上。）如有需要，您可以单击 “**Refresh**” 更新数据。

步骤 2 要选择设备，请首先在 “**Name**” 中输入描述性名称。然后选中 “**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 3 单击 “**OK**” 将设备添加到 “*Static IP*” 列表中，或者单击 “**Close**” 关闭弹出窗口而不添加所选设备。单击 “**OK**” 后，系统将显示一条消息。此消息包含重要信息。

阅读此消息，然后单击 “**OK**”。保持浏览器为打开状态，一直等到所选 MAC 地址出现在 “*Static IP*”列表中。

步骤 4 根据需要修改或删除列表条目：

- **修改设置的步骤**：单击列表中的设备。相关信息将显示在文本字段中。进行更改，然后单击 “**Update**”。如果无需进行更改，则可以单击 “**Add New**”，以取消选中该条目并清空文本字段。
- **从列表中删除条目的步骤**：单击要删除的条目，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。

通过手动输入设备来分配静态 IP 地址

在 “*Static IP Address*”部分中，根据需要添加或编辑条目。请记住，只有单击 “Save”按钮后，设置才会保存。

- **在列表中添加新设备的步骤**：输入以下信息，然后单击 “**Add to list**”。
  - **Static IP Address**：输入静态 IP 地址。如果希望路由器将静态 IP 地址分配给设备，您可以输入 0.0.0.0。
  - **MAC Address**：输入设备的 MAC 地址。（MAC 地址通常显示在设备底部面板或后面板的标签上。）输入地址时不得包含任何标点符号。
  - **Name**：输入设备的描述性名称。
  - **Enable**：选中此框可将静态 IP 地址分配给此设备。
- **添加另一新条目的步骤**：输入信息，然后单击 “**Add to list**”。
- **修改设置的步骤**：单击列表中的设备。相关信息将显示在文本字段中。进行更改，然后单击 “**Update**”。如果无需进行更改，则可以单击 “**Add New**”，以取消选中该条目并清空文本字段。
- **从列表中删除条目的步骤**：单击要删除的条目，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

您可以使用 “*Static IP list*” 控制对您网络的访问。您可以阻止列表中未列出的设备或没有正确 IP 地址的设备进行访问。

步骤 1 将设备添加到 “*Static IP list*”，如**静态 IP 地址，页码 55** 中所述。

步骤 2 启用或禁用以下功能：

- **Block MAC address on the list with wrong IP address**：如果计算机的 IP 地址已更改，则选中此框可阻止此计算机访问您的网络。例如，如果您之前已分配静态 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您的网络。此功能可以阻止用户在未经您允许的情况下更改他们的设备 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**：选中此框可阻止 “*Static IP list*” 中未列出的设备进行访问。此功能可以阻止未知设备访问您的网络。取消选中此框将允许所有配置有正确范围内 IP 地址的已连接设备进行访问。

DNS 本地数据库

域名服务 (DNS) 是一种将域名与其可路由 IP 地址相匹配的服务。您可以设置 DNS 本地数据库，以使路由器充当常用域名的本地 DNS 服务器。相比于使用外部 DNS 服务器，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 “*Setup*” > “*Network*” 页面的 “*WAN Setting*” 部分中指定的 DNS 服务器。

如果启用此功能，您还必须将客户端设备配置为使用路由器作为 DNS 服务器。默认情况下， Windows 计算机设置为自动从 WAN 设置中获取 DNS 服务器地址。您需要更改 TCP/IP 连接设置。例如，在运行 Windows 的 PC 上，转到 “*本地连接属性*” > “*Internet 协议*” > “*TCP/IP 属性*” 窗口。选择 “*使用下面的 DNS 服务器地址*”，然后输入路由器的 LAN IP 地址作为 “首选 DNS 服务器”。有关详细信息，请参阅您正配置的客户端的文档。

根据需要添加或更新条目。请记住，只有单击 “Save” 按钮后，设置才会保存。

- **添加新条目的步骤**：输入以下信息。然后单击 “**Add to list**”。
  - **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。
- **添加另一新条目的步骤**：输入信息，然后单击 “**Add to list**”。

- **修改设备设置的步骤**：单击列表中的设备。相关信息将显示在文本字段中。进行更改，然后单击 “**Update**”。如果无需进行更改，则可以单击 “**Add New**”，以取消选中该条目并清空文本字段。
- **从列表中删除条目的步骤**：单击要删除的条目，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。

查看 DHCP 状态信息

使用 “*DHCP*” > “*Status*” 页面查看 DHCP 服务器及其客户端的状态。您可以单击 “**Refresh**” 刷新数据。要释放客户端的 IP 地址，您可以单击 “**Delete**” 图标。

打开此页面的步骤：在导航树中单击 “**DHCP**” > “**DHCP Status**”。

DHCP 服务器

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 地址的数量。
- **Static IP Used**：使用的静态 IP 地址的数量。
- **DHCP Available**：可用动态 IP 地址的数量
- **Total**：DHCP 服务器可分配的动态 IP 地址的总数。

客户端表

对于所有使用 DHCP 服务器的网络客户端，客户端表显示当前的 DHCP 客户端信息：

- **Client Host Name**：这是分配给客户端主机的名称。
- **IP Address**：这是分配给客户端的动态 IP 地址。
- **MAC Address**：这表示客户端的 MAC 地址。
- **Client Lease Time**：这显示允许网络用户使用其当前动态 IP 地址连接到路由器的时间量。

5

系统管理

使用系统管理模块管理高级设置、配置诊断工具，以及执行固件升级、备份和重新启动等任务。请参阅以下主题：

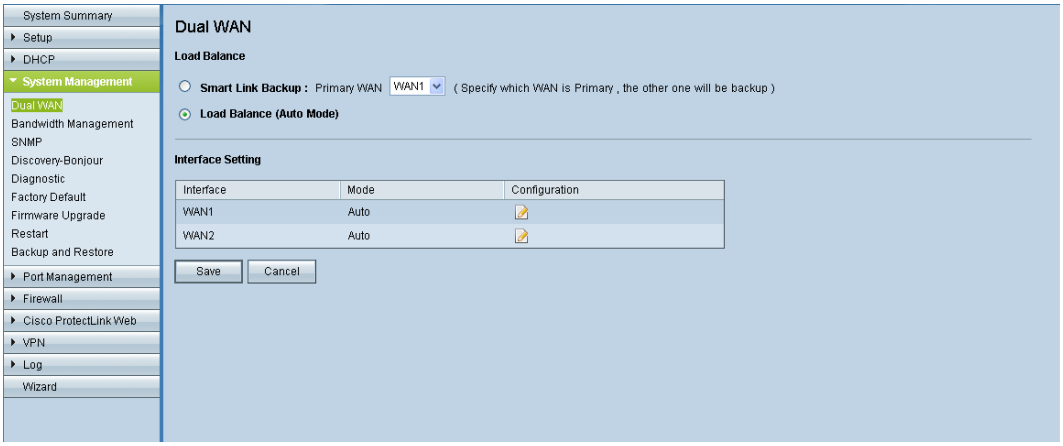
设置双 WAN 和多 WAN 连接

如果使用多个 WAN 接口，您可以使用“*System Management*”>“*Dual WAN*”页面（对于 RV016，则为“*Multi-WAN*”页面）配置 Internet 连接的设置。

打开此页面的步骤：在导航树中单击“**System Management**”>“**Dual WAN（对于 RV016，则为 Multi-WAN）**”。

注意 离开此页面前，请单击“**Save**”保存设置，或单击“**Cancel**”撤消设置。所有未保存的更改都将被丢弃。

模式 - Cisco RV042 和 Cisco RV082



通过使用 Internet 端口和 DMZ/Internet 端口，您最多可以配置两个 Internet 连接。您可以选择以下模式之一来管理 WAN 连接：

- **Smart Link Backup**：要确保连接不中断，请选择此模式。如果主 WAN 连接不可用，则系统会使用备份 WAN 连接。
- **Load Balance**：要同时使用两种 Internet 连接以增加可用带宽，请选择此模式。路由器会以加权轮循方式均衡两个接口之间的流量。

  注意：DNS 查询不受负载平衡的影响。

模式 - Cisco RV016

通过使用两个 Internet 端口和五个双功能端口，您最多可以配置七个 Internet 连接。您可以选择以下模式之一来管理 WAN 连接：

- **Intelligent Balancer (Auto Mode)**：要均衡所有接口之间的流量以增加可用带宽，请选择此选项。路由器会以加权轮循方式均衡接口间的流量。
- **IP Group (By Users)**：要根据优先级水平或服务等级 (CoS) 对每个 WAN 接口上的流量进行分组，请选择此选项。使用此功能，您可以为指定的服务和用户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 模式。要指定服务和用户，请单击 WAN 接口的 “**Edit**” 图标，然后为每个服务、 IP 地址或 IP 地址范围添加协议绑定条目。

  注意：路由器会为非 IP 组用户至少预留一个 WAN 端口，因此 WAN1 将始终设置为 Intelligent Balancer (Auto Mode)。协议绑定对 WAN1 不可用。

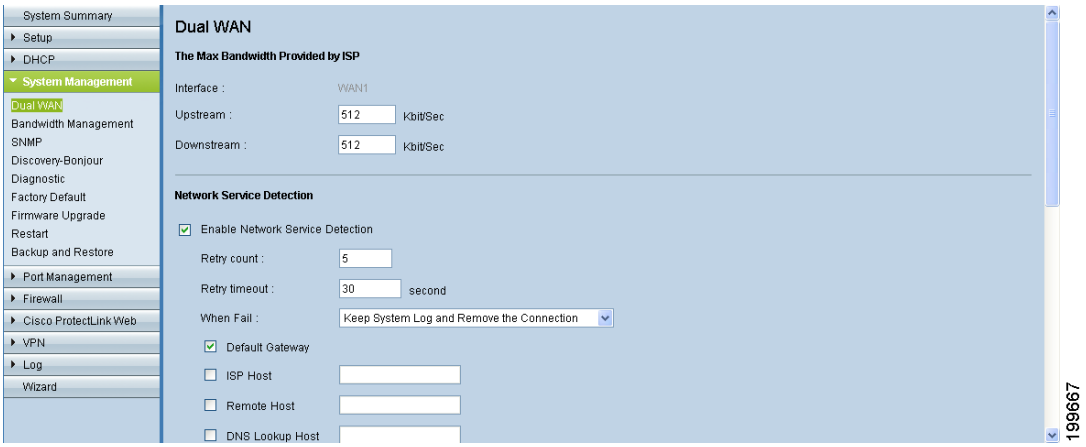
接口设置

单击要设置的接口的 “**Edit**” 图标。然后，在 “*Edit Dual WAN*” 设置页面上输入设置。有关详细信息，请参阅**编辑双 WAN 和多 WAN 设置，页码 63**。

注意 如果 “*Dual WAN*” 页面上有未保存的更改，此时会出现警告。您可以单击 “**OK**” 关闭消息。然后单击 “**Save**” 保存更改。保存更改后，单击 “**Edit**” 图标。或者在显示警告时，单击 “**Cancel**” 继续留在编辑页面而不保存更改。

编辑双 WAN 和多 WAN 设置

单击 “*Dual WAN*”（或 “*Multi-WAN*”）页面上 WAN 接口的 “**Edit**”图标后，将显示 “*Dual WAN Settings*”页面 （对于 RV016，则显示 “*Multi-WAN Settings*”页面）。根据需要输入接口设置。



注意 离开此页面前，请单击 “**Save**”保存设置，或单击 “**Cancel**”撤消设置。所有未保存的更改都将被丢弃。

Max Bandwidth Provided by ISP：

在此部分中，请输入您的 Internet 服务提供商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，路由器将使用另一 WAN 接口。

- **Upstream**：输入您的 ISP 提供的最大上行带宽。默认为 512 Kbit/sec。
- **Downstream**：输入您的 ISP 提供的最大下行带宽。默认为 512 Kbit/sec。

Network Service Detection：

作为可选操作，选中此框，以允许路由器通过 ping 指定设备来检测网络连接情况。然后，输入以下设置。取消选中此框可禁用此功能。

- **Retry count**：输入对设备执行 ping 命令的次数。默认为 5 次。
- **Retry timeout**：输入两次 ping 操作之间等待的秒数。默认为 30 秒。
- **When Fail**：选择 ping 测试失败时进行的操作。如果选择 “**Generate the Error Condition in the System Log**”，则路由器将在系统日志中记录失败。不会故障切换到其他接口。如果选择 “**Remove the Connection**”，则将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**、**Remote Host** 和 **DNS Lookup Host**：选中每个要执行 ping 命令以确定网络连接情况的设备所对应的框。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。如果您不想为了进行网络服务检测而 ping 此设备，请取消选中此框。

Protocol Binding (for Cisco RV016 only, when Load Balancer is selected)：

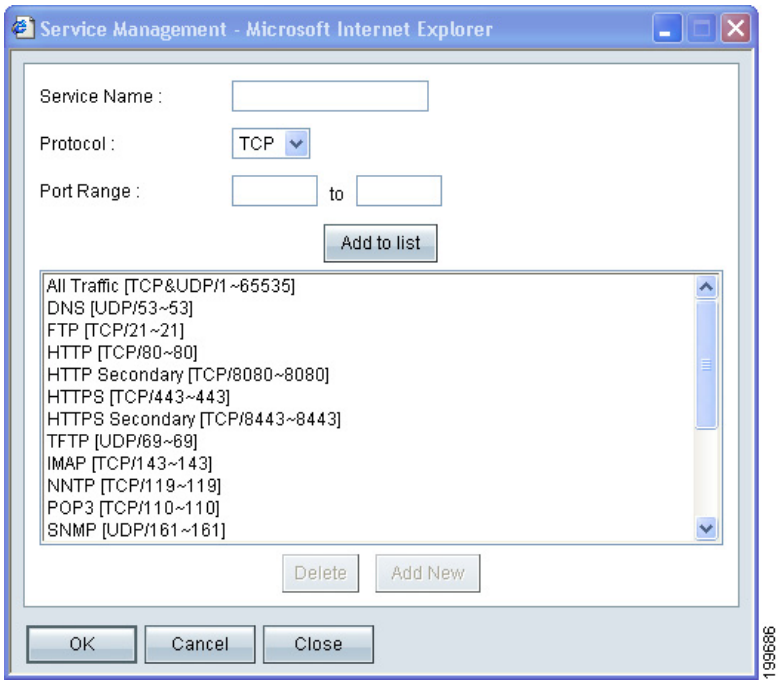
使用此功能可将此接口应用于指定的协议以及指定的源和目标地址。如果已启用 IP 组模式，则此功能不可用。

根据需要添加或更新条目。请记住，只有单击 Save 按钮后，条目才会保存。

- **在列表中添加新条目的步骤**：输入下述设置，然后单击 “**Add to list**”。
  - **Service**：选择要与此 WAN 接口绑定的服务 （或选择 “All Traffic”）。如果某服务未列出，您可以单击 “**Service Management**”添加此服务。有关详细信息，请参阅**添加服务，页码 65**。
  - **Source IP** 和 **Destination IP**：为通过此 WAN 端口的流量指定内部源和外部目标。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*”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。
  - **Enable**：选中此框以启用此规则，或取消选中此框以禁用此规则。
- **在列表中添加另一条目的步骤**：输入信息，然后单击 “**Add to list**”。
- **修改列表中条目的步骤**：单击要修改的条目。相关信息将显示在文本字段中。进行更改，然后单击 “**Update**”。如果无需进行更改，则可以单击 “**Add New**”，以取消选中该条目并清空文本字段。
- **从列表中删除条目的步骤**：单击要删除的条目，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。

添加服务

要在 “*Service*”列表中添加新条目或者更改之前创建的条目，请单击 “**Service Management**”。如果 Web 浏览器显示弹出窗口警告，请允许显示被阻止的内容。



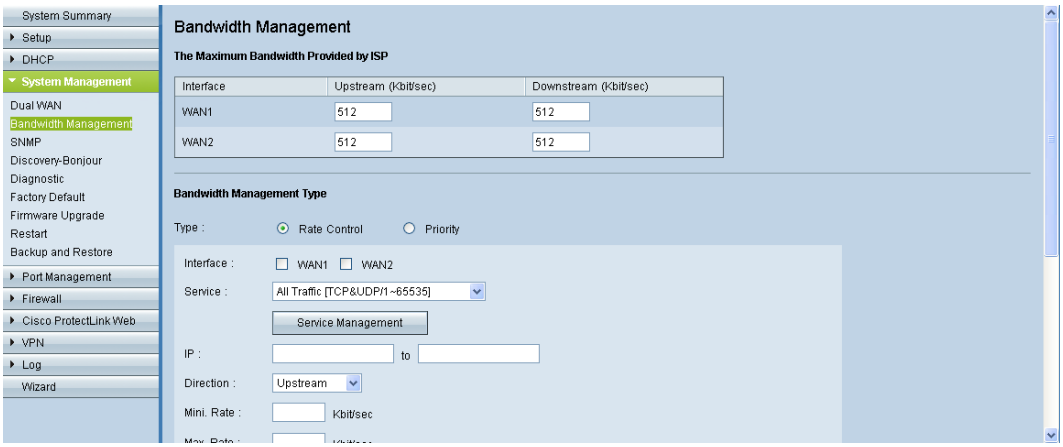
在 “*Service Management*”窗口中，根据需要添加或更新条目。关闭此窗口前，请单击 “**OK**”保存设置，或单击 “**Cancel**”撤消设置。所有未保存的更改都将被丢弃。

- **在列表中添加服务的步骤**：输入以下信息，然后单击 “**Add to List**”。列表中最多可包含 30 个服务。
  - **Service Name**：输入简短说明。
  - **Protocol**：选择所需协议。请参阅您正托管的服务的文档。
  - **Port Range**：输入所需的端口范围。
  - **添加另一新服务的步骤**：输入信息，然后单击 “**Add to list**”。
  - **修改已创建服务的步骤**：单击列表中的服务。相关信息将显示在文本字段中。进行更改，然后单击 “**Update**”。如果无需进行更改，则可以单击 “**Add New**”，以取消选中该服务并清空文本字段。
  - **从列表中删除服务的步骤**：单击要删除的条目。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 键的同时单击相应条目。单击 “**Delete**”。

管理带宽设置

使用“*System Management*”>“*Bandwidth Management*”页面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配置服务质量 (QoS) 设置。例如，您可以输入带宽规则以确保语音服务质量。有关详细示例，请参阅**附录 E，“带宽管理”**。

打开此页面的步骤：在导航树中单击 “**System Management**” > “**Bandwidth Management**”。



注意 离开此页面前，请单击 “**Save**”保存设置，或单击 “**Cancel**”撤消设置。所有未保存的更改都将被丢弃。

ISP 提供的最大带宽

输入您的 Internet 服务提供商 (ISP) 指定的最大带宽设置。

- **Upstream**：输入您的 ISP 提供的最大上行带宽。默认为 **512** kbit/sec。
- **Downstream**：输入您的 ISP 提供的最大下行带宽。默认为 **12** kbit/sec。

带宽管理类型

请选择以下管理选项之一：

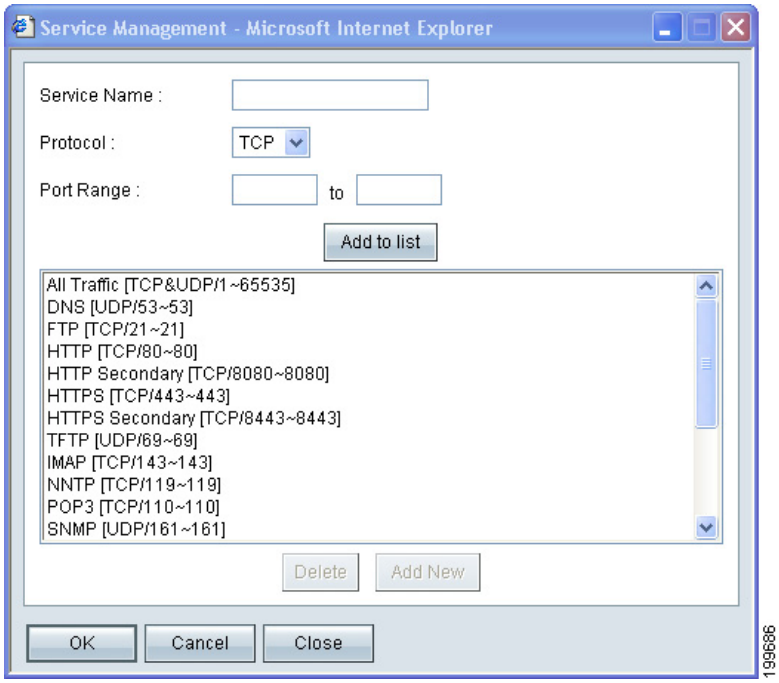
- **Rate Control**：选择此选项可指定每个服务或 IP 地址的最小 （保证）带宽和最大 （限制）带宽。
- **Priority**：选择此选项可通过确定高优先级和低优先级服务来管理带宽。

从 “**Interface**”中选择一项。添加受带宽管理影响的服务。

- **在列表中添加新服务的步骤**：输入下述设置，然后单击 “**Add to List**”。您最多可添加 100 个服务。
  - **Service**：选择要管理的服务。如果有服务未列出，您可以单击 “**Service Management**” 添加服务。有关详细信息，请参阅**添加服务，页码 68**。
  - **IP (for Rate Control only)**：输入您需要控制的 IP 地址或范围。要包括所有的内部 IP 地址，请保留默认设置。
  - **Direction**：请为出站流量选择 “**Upstream**”，或为入站流量选择 “**Downstream**”。
  - **Min. Rate (for Rate Control only)**：输入所保证的带宽的最低速率 (Kbit/sec)。
  - **Max. Rate (for Rate Control only)**：输入所保证的带宽的最高速率 (Kbit/sec)。
  - **Priority (for Priority management only)**：选择此服务的优先级：“**High**” 或 “**Low**”。
  - **Enable**：选中此框以启用此功能，或取消选中此框以禁用此功能。
- **在列表中添加另一服务的步骤**：输入信息，然后单击 “**Add to list**”。
- **修改列表中服务的步骤**：单击要修改的条目。相关信息将显示在文本字段中。进行更改，然后单击 “**Update**”。如果无需进行更改，则可以单击 “**Add New**”，以取消选中该条目并清空文本字段。
- **从列表中删除条目的步骤**：单击要删除的条目，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。

添加服务

要在 “*Service*”列表中添加新条目或者更改之前创建的条目，请单击 “**Service Management**”。如果 Web 浏览器显示关于弹出窗口警告，请允许显示被阻止的内容。



在 “*Service Management*”窗口中，根据需要添加或更新条目。关闭此窗口前，请单击 “**OK**”保存设置，或单击 “**Cancel**”撤消设置。所有未保存的更改都将被丢弃。

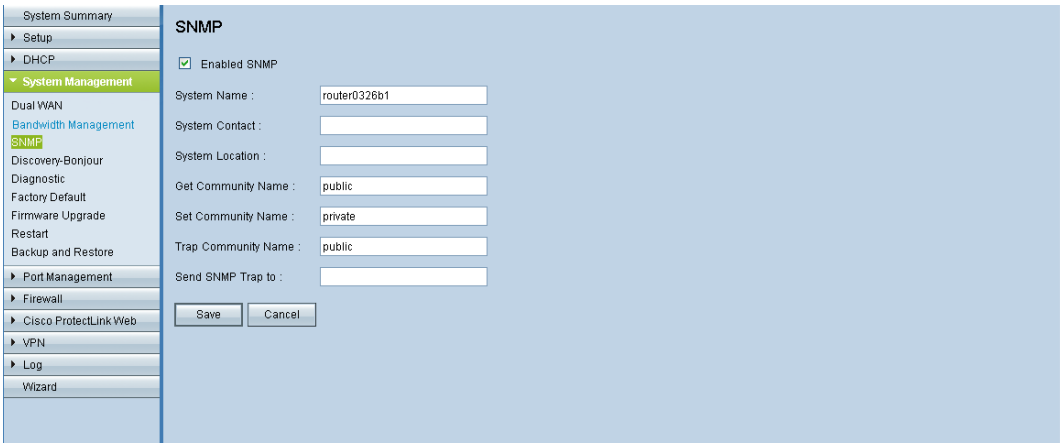
- **在列表中添加服务的步骤**：输入以下信息，然后单击 “**Add to List**”。列表中最多可包含 30 个服务。
  - **Service Name**：输入简短说明。
  - **Protocol**：选择所需协议。请参阅您托管的服务的相关文档。
  - **Port Range**：输入所需的端口范围。
- **添加另一新服务的步骤**：输入信息，然后单击 “**Add to list**”。
- **修改已创建服务的步骤**：单击列表中的服务。相关信息将显示在文本字段中。进行更改，然后单击 “**Update**”。如果无需进行更改，则可以单击 “**Add New**”，以取消选中该服务并清空文本字段。

- **从列表中删除服务的步骤**：单击要删除的条目。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 键的同时单击相应条目。单击 “**Delete**”。

设置 SNMP

使用 “*System Management*” > “*SNMP*” 页面为此路由器设置 SNMP。 SNMP（简单网络管理协议）是一种网络协议，允许网络管理员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。路由器支持 SNMP v1/v2c。路由器支持 MIBII 等标准 MIB （管理信息库）以及专用 MIB。路由器充当 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 链接事件。

打开此页面的步骤：在导航树中单击 “**System Management**” > “**SNMP**”。



注意 离开此页面前，请单击 “**Save**”保存设置，或单击 “**Cancel**”撤消设置。所有未保存的更改都将被丢弃。

- **Enabled SNMP**：选中此框可启用 SNMP。取消选中此框可禁用此功能。默认情况下，此功能为启用状态。
- **System Name**：设置路由器的主机名。
- **System Contact**：输入作为路由器更新事宜联系人的网络管理员的姓名。
- **System Location**：输入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。

- **Get Community Name**：输入社区字符串，用于对 SNMP GET 命令进行验证。输入的名称最多可以包含 64 个字母数字字符。默认为 **public**。
- **Set Community Name**：输入社区字符串，用于对 SNMP SET 命令进行验证。输入的名称最多可以包含 64 个字母数字字符。默认为 **private**。
- **Trap Community Name**：创建将随每个陷阱发送到 SNMP 管理器的密码。输入的名称最多可以包含 64 个字母数字字符。默认为 **public**。
- **Send SNMP Trap to**：输入运行 SNMP 管理软件的服务器的 IP 地址或域名。

使用 Bonjour 启用设备发现

使用 “*System Management*” > “*Discovery-Bonjour*” 页面启用或禁用服务发现协议 Bonjour。 Bonjour 可找到 LAN 上的计算机和服务器等网络设备。您使用的网络管理系统可能需要此功能。启用此功能之后，路由器会定期向其整个本地网络多播 Bonjour 服务记录，以通告此服务的存在。

注意 为了发现思科精睿 (Cisco 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。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，以便在配置和部署过程中提供帮助。有关详细信息以及要下载此实用程序，请访问 www.cisco.com/go/findit。

打开此页面的步骤：在导航树中单击 “**System Management**” > “**Discovery-Bonjour**”。

选中 “**Enable**” 框可启用 Bonjour。取消选中此框可禁用此功能。默认情况下，此功能处于启用状态。

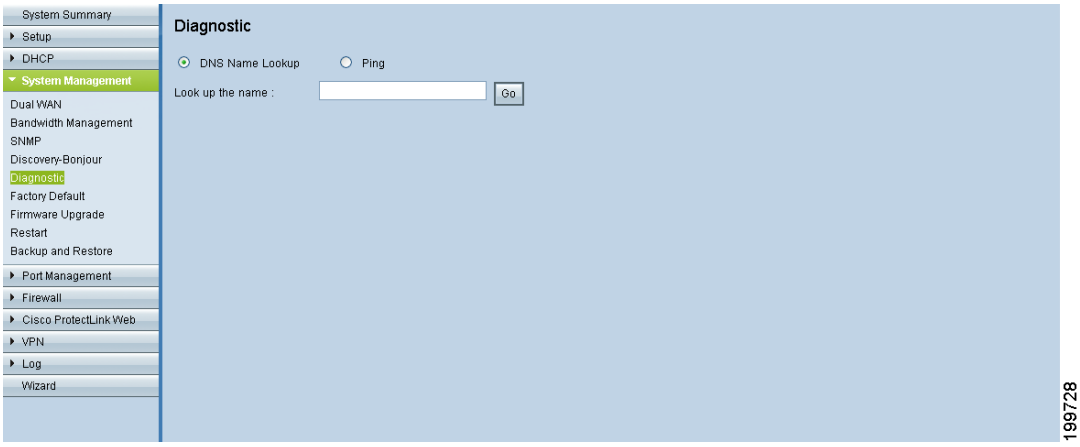
使用内置诊断工具

使用 “*System Management*” > “*Diagnostic*”页面访问 DNS Name Lookup 和 Ping 这两个内置工具。如果您怀疑存在连接问题，可使用这些工具进行检查。

打开此页面的步骤：单击 “**System Management**” > “**Diagnostic**”。

如果您知道 DNS 名称并希望获取 IP 地址，请选择 “**DNS Name Lookup**”。选择 “**Ping**”可对指向 Internet 上特定 IP 地址的连接进行测试。

DNS Name Lookup



选择此选项可对指向您在 “*Setup*” > “*Network*”页面上指定的 DNS 服务器的连接进行测试，或者查找您希望在 Ping 测试中使用的 IP 地址。

在 “**Look up the name**”字段中输入主机名，例如 www.cisco.com。该名称中不要包括前缀 （例如 *http://*）。然后单击 “**Go**”。如果测试成功，则系统会显示主机的 IP 地址。

注意 此工具要求路由器可以连接到 WAN 接口设置 （“*Setup*” > “*Network*”页面）中指定的有效 DNS 服务器。

Ping

选择此选项可通过输入 IP 地址来对指向指定主机的连接进行测试。如果您不知道 IP 地址，请使用 DNS 查找工具获取。 ping 测试可显示路由器是否能够向远程主机发送数据包并接收响应。如果 LAN 上的用户在访问 Internet 上的服务时遇到问题，首先应尝试对 DNS 服务器或 ISP 的其他服务器执行 ping 操作。如果此测试成功，请尝试对 ISP 外部的设备执行 ping 操作。这将显示问题是否与 ISP 的连接有关。

输入 IP 地址，然后单击 “**Go**”。如果测试成功，则系统会显示以下信息：

- **Status**：ping 测试的状态：“*Testing*”、“*Test Succeeded*”或 “*Test Failed*”
- **Packets**：ping 测试过程中传输的数据包数、接收的数据包数以及数据包丢失率
- **Round Trip Time**：ping 测试的最短、最长和平均往返时间

恢复出厂默认设置

使用 “*System Management*” > “*Factory Default*”页面清除所有配置信息并将路由器恢复为出厂默认设置。仅当您希望放弃所有已配置的设置和首选项时，才可使用此功能。

打开此页面的步骤：在导航树中单击 “**System Management**” > “**Factory Default**”。

步骤 1 如果您希望将路由器恢复为出厂默认设置，请单击 “**Return to Factory Default Setting**”。

步骤 2 当显示确认消息时，请单击 “**OK**”继续操作。如果您不希望恢复出厂默认设置，请单击 “**Cancel**”。

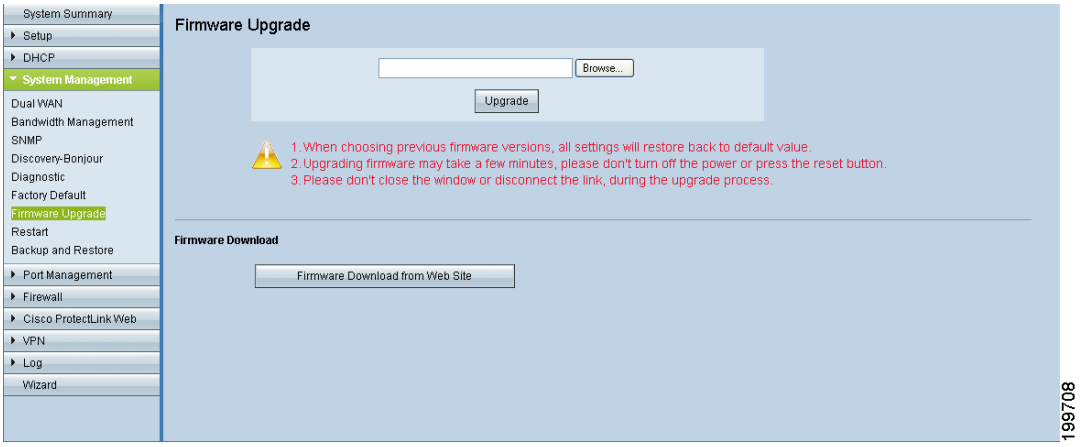
升级固件

使用 “*System Management*” > “*Firmware Upgrade*”页面下载适用于您的路由器的最新固件并进行安装。

警告 如果您选择较早版本的固件，则系统将使用出厂默认设置。所有自定义设置。

警告 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、按下重置按钮、关闭浏览器或断开链接。

打开此页面的步骤：在导航树中单击 “**System Management**” > “**Firmware Upgrade**”。



根据需要继续执行操作：

- **从计算机上的固件文件进行升级的步骤**：单击“**Browse**”按钮，然后选择已提取的文件。单击“**Firmware Upgrade Right Now**”。几分钟后，系统将显示“Rebooting”消息。在浏览器完成刷新之前，您需要等待大约一分钟时间。如果浏览器未自动显示登录页面，您可能需要在浏览器地址栏中重新输入 IP 地址。如果 PC 无法重新连接到配置实用程序，您可能需要释放并恢复 IP 地址。
- **从思科下载最新固件的步骤**：单击“**Firmware Download from Web Site**”。Web 浏览器将会打开 Cisco.com 上的路由器信息页面。单击“**Download Firmware**”按钮。继续浏览屏幕，选择最新的路由器固件并下载文件。在您的计算机中提取文件。然后，按上述操作执行固件升级。

重新启动路由器

如果您需要重新启动路由器，思科建议您使用此页面上的重新启动工具。当您从“*System Management*”>“*Restart*”页面重新启动时，路由器将在重置之前发送日志文件（如果日志记录已启用）。

打开此页面的步骤：在导航树中单击“**System Management**”>“**Restart**”。

步骤 1 单击“**Restart Router**”以重新启动路由器。

步骤 2 当显示确认消息时，请单击“**OK**”继续操作。如果您不希望重新启动路由器，请单击“**Cancel**”。

备份和恢复设置

使用“*System Management*”>“*Backup and Restore*”页面导入、导出和复制配置文件。路由器有两个配置文件：启动配置文件和镜像配置文件。启动文件是路由器引导时加载的配置文件。路由器会自动将启动文件复制到镜像文件。因此，镜像文件包含最新的有效配置。如果以后启动配置文件由于某种原因而失败，则系统将使用镜像配置文件。

注意 稳定运行 24 小时（在 24 小时内没有重新引导且没有配置更改）后，路由器会自动将启动配置复制到镜像配置。

打开此页面的步骤：在导航树中单击“**System Management**”>“**Backup and Restore**”。

您可以进行以下操作：

- **从配置文件恢复设置，页码 76**
- **备份配置文件和镜像文件，页码 76**
- **复制启动文件或镜像文件，页码 77**

从配置文件恢复设置

如果您希望恢复到之前保存的设置，则可以导入配置文件。

步骤 1 在“*Restore Startup Configuration File*”部分中，单击“**Browse**”。

步骤 2 选择配置文件 (.config)。

步骤 3 单击“**Restore**”。此过程最多可能需要 1 分钟时间。

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

步骤 5 当显示确认消息时，请单击“**OK**”。如果您不希望重新启动路由器，请单击“**Cancel**”。只有重新启动路由器之后，系统才会应用导入的设置。

注意：或者，您也可以使用 “Restart”按钮。按住 “**Restart**”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

您可以将启动和镜像配置文件保存在计算机上。如有需要，您可以使用这些文件恢复设置。

步骤 1 单击 “**Backup Startup Configuration**”或 “**Backup Mirror Configuration**”。

步骤 2 当显示 “*File Download*”窗口时，请单击 “**Save**”，然后选择文件位置。作为可选操作，您可以输入描述性的文件名。然后单击 “**Save**”。

提示：默认的文件名是 *Startup.config* 和 *Mirror.config*。如果您需要以后导入某个文件，则输入包括当前日期和时间的文件名可以简化识别，可能十分有帮助。

步骤 3 关闭 “*Download Complete*”窗口。

复制启动文件或镜像文件

如有需要，您可以手动将启动配置文件复制到镜像配置文件，或者也可以将镜像配置文件复制到启动配置文件。

TIP 您可以在进行更改之前使用此过程对已知配置进行备份。在进行更改之前，将启动文件复制到镜像文件。如果您对更改不满意，可以将镜像文件复制到启动文件，以恢复设置。

注意

- 每隔 24 小时，启动配置文件都会自动复制到镜像配置文件。
- 如果设置发生更改，则时间计数器将重置，且启动配置文件将在 24 小时后进行下一次自动复制。
- 如果镜像配置文件仍然处于出厂默认状态，则将镜像文件复制到启动文件时会立即将路由器重置为出厂默认设置。

要复制文件，请单击以下任一按钮：

- **Copy Startup to Mirror**：单击此按钮可将镜像文件替换为启动文件。复制操作会立即执行，且没有取消选项。操作完成后，浏览器页面将刷新。
- **Copy Mirror to Startup**：单击此按钮可将启动文件替换为镜像文件。复制操作会立即执行，且没有取消选项。很快，路由器将重新启动。如果 PC 无法立即重新加载登录页面，请在地址栏中重新输入配置实用程序的 IP 地址，然后登录。

6

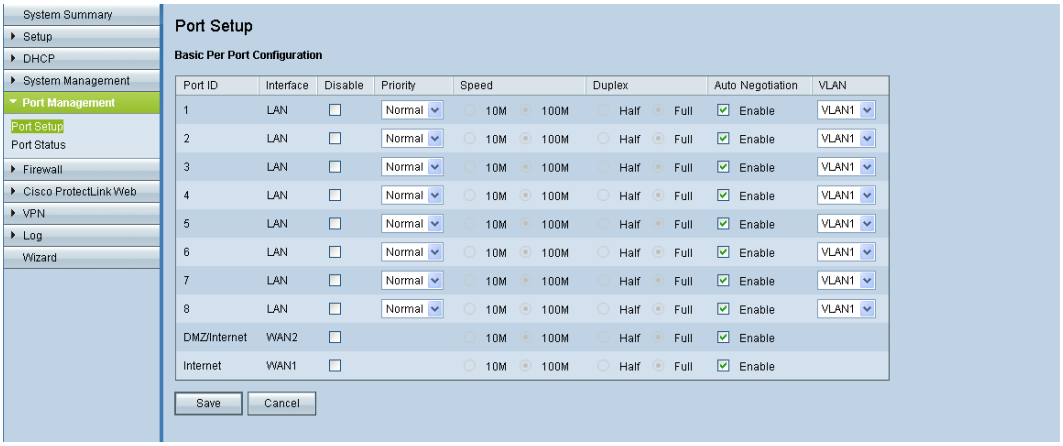
端口管理

使用端口管理模块配置端口设置并查看端口状态。

配置端口设置

对于大多数小型企业而言，默认的端口设置应该足以满足其需求，但您可以根据需要使用“*Port Management*”>“*Port Setup*”页面来自定义这些设置。您可以禁用某个端口或自定义其优先级、速度、双工模式和自动协商设置。您也可以启用基于端口的 VLAN 以控制网络中设备之间的流量。

打开此页面的步骤：在导航树中单击“**Port Management**”>“**Port Setup**”。



注意 离开此页面前，请单击“**Save**”保存设置，或单击“**Cancel**”撤消设置。所有未保存的更改都将被丢弃。

以下内容仅适用于 Cisco RV016：从下拉列表中选择 WAN 端口的数量，或保留默认数量 2。如果更改该数值，请保存设置。（您也可以使用“*Setup*”>“*Network*”页面来更改 WAN 端口的数量。）

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

根据需要输入以下设置：

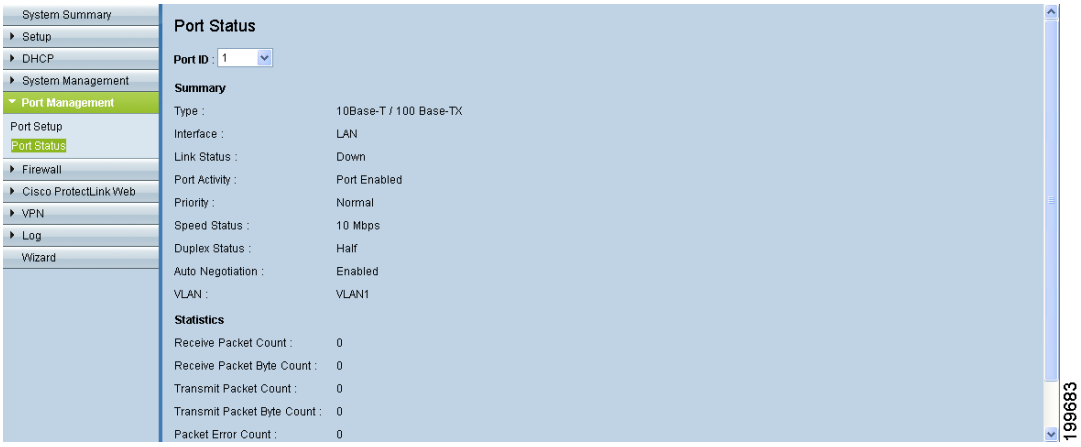
- **Disable**：选中此框可禁用某个端口。默认情况下，所有端口都为启用状态。
- **Priority** （仅限 LAN 端口）：使用此设置可为特定端口上的设备设置流量优先级，从而确保服务质量。例如，您可能会为用于游戏或视频会议的端口分配高优先级。对于每个端口，请选择合适的优先级水平，“**High**”或 “**Normal**”。默认的设置为 “Normal”。
- **Speed**：如果要调整此设置，请首先取消选中 “*Auto Neg*”列中的 “**Enable**”框，以禁用自动协商。然后选择端口速度：**10M** 或 **100M**。
- **Duplex**：如果要设置双工模式，请首先取消选中 “*Auto Neg*”列中的 “**Enable**”框，以禁用自动协商。选择双工模式，“**Half**”或 “**Full**”。
- **Auto Neg.**：选中 “**Enable**”框，以允许路由器自动协商连接速度和双工模式。默认情况下，此功能为启用状态。
- **VLAN** （仅限 LAN 端口）：默认情况下，所有 LAN 端口都在 VLAN 1 上。要将端口置于单独的 VLAN 上，请从下拉列表中选择一个 VLAN。

  可用 VLAN 的数量等于 LAN 端口的数量：Cisco RV042 上为 4 个， Cisco RV082 为 8 个，而 Cisco RV016 上最多为 13 个 （具体取决于双功能端口的使用情况）。例如，在端口 4 上可能有以太网交换机，用于为会议室中的来宾用户提供 Internet 连接。为了防止来宾访问您的 LAN 上的文件服务器和打印机，您可以将端口 4 置于 VLAN 2 上，而将其他端口保留在 VLAN 1 上。单独的 VLAN 上的设备之间没有通信。

查看端口的状态信息

使用 “*Port Management*” > “*Port Status*”页面查看所选端口的信息和统计信息。

打开此页面的步骤：在导航树中单击 “**Port Management**” > “**Port Status**”。



从“**Port ID**”列表中，选择一个端口。您可以单击“**Refresh**”更新数据。

概要

对于所选端口，“Summary”表中显示以下内容：

- **Type**：端口类型
- **Interface**：接口类型， LAN 或 WAN。
- **Link Status**：连接的状态
- **Port Activity**：端口的状态
- **Speed Status**：端口的速度， 10 Mbps 或 100 Mbps
- **Duplex Status**：双工模式：“*Half*”或“*Full*”。
- **Auto negotiation**：此功能的状态
- **VLAN**：端口的 VLAN

统计信息

对于所选端口，“Statistics”表中显示以下内容：

- **Port Receive Packet Count**：已接收的数据包的数量
- **Port Receive Packet Byte Count**：已接收的数据包字节数
- **Port Transmit Packet Count**：已传输的数据包的数量
- **Port Transmit Packet Byte Count**：已传输的数据包字节数
- **Port Packet Error Count**：数据包错误的数量

7

防火墙

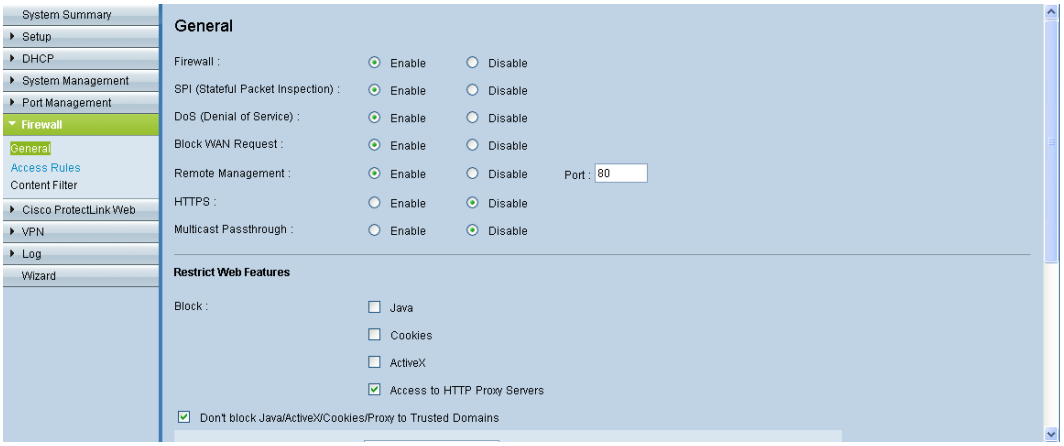
使用防火墙模块配置防火墙功能、创建访问规则，并设置内容过滤器以控制用户的 Internet 活动。请参阅以下主题：

- **配置常规防火墙设置，页码 81**
- **配置访问规则，页码 85**
- **配置防火墙访问规则，页码 84**
- **使用内容过滤器控制 Internet 访问，页码 90**

配置常规防火墙设置

对于大多数小型企业而言，默认的防火墙设置应该足以满足其需求。但是，您可以使用 “*Firewall*” > “*General*” 页面来禁用防火墙或指定要阻止的攻击类型。您还可以限制 Java 和 Cookies 等可能存在风险的网站功能。

打开此页面的步骤：在导航树中单击 “**Firewall**” > “**General**”。



注意

- 如果希望禁用防火墙 （不推荐），您必须先配置了管理员密码才能执行此操作。如果您仍在使用默认密码，则必须更改密码。有关详细信息，请参阅**更改管理员用户名和密码，页码 34**。
- 离开此页面前，请单击 “**Save**”保存设置，或单击 “**Cancel**”撤消设置。所有未保存的更改都将被丢弃。

启用或禁用防火墙及其相关功能：

- **Firewall**：选择启用或禁用防火墙。此功能默认为启用状态，且强烈建议保持启用状态，以便保护您的网络。启用或禁用防火墙还会对多个相关功能产生影响，如下所述。禁用防火墙的同时还会禁用访问规则和内容过滤器。

  如果选择 “**Disable**”且您仍在使用默认的管理员密码，则系统将显示一条消息。为了阻止对路由器的未授权访问，在禁用防火墙之前，必须更改密码。单击 “**OK**”转到 “*Password*”页面，或者单击 “**Cancel**”停留在当前页面。更改密码后，您可以返回此页面继续该流程。

- **SPI (Stateful Packet Inspection)**：启用此功能后，路由器将可以查看通过防火墙的信息。在传递数据包以通过更高的协议层进行处理之前，它会基于已建立的连接检测所有数据包。只有启用防火墙后，才能启用此功能。
- **DoS (Denial of Service)**：启用此功能后，可保护内部网络免受 Internet 攻击，例如 SYN Flooding、 Smurf、 LAND、 Ping of Death、 IP Spoofing 和重组攻击。只有启用防火墙后，才能启用此功能。
- **Block WAN Request**：启用此功能后，路由器将可以丢弃未接受的 TCP 请求和来自 WAN 侧的 ICMP 数据包。黑客将无法通过对 WAN IP 地址执行 ping 命令来找到路由器。只有启用防火墙后，才能启用此功能。
- **Remote Management**：启用此功能后，您可以通过 WAN 连接到路由器的基于 Web 的配置实用程序。默认情况下，此功能为禁用状态。只有启用防火墙后，才能启用此功能。如果希望启用远程管理，您应首先在 “*Setup*” > “*Password*”页面上配置高安全性的管理员密码。这种预防措施可以阻止未经授权的用户使用默认密码访问路由器。如果启用此功能，您可以保留 “**Port**”中的默认设置 80，或输入其他端口号 （通常会使用 8080）。

  请注意：启用远程管理功能后，您可以使用 Web 浏览器从 Internet 的任意位置访问配置实用程序。在 Web 浏览器中，输入 **http://< 路由器的 WAN IP 地址 >:port** ；如果已启用 HTTPS 功能，也可输入 **https://< 路由器的 WAN IP 地址 >:port**。

- **HTTPS**：启用此功能后，可允许受保护的 HTTP 会话。默认情况下，此功能为启用状态。

  请注意：如果禁用 HTTPS 功能，则用户将无法使用 QuickVPN 进行连接。

- **Multicast Pass Through**：启用此功能后， IP 多播数据包可以转发到合适的 LAN 设备中。 Multicast Pass Through 用于 Internet 游戏、视频会议和多媒体应用程序。默认情况下，此选项为禁用状态。

  重要事项：此路由器不支持通过 IPSec 隧道传输多播流量。 Multicast Pass Through 选项决定了路由器是否允许源自 Internet 的多播流量通过防火墙传输到 LAN。

限制 Web 功能

- **Java**：如果希望防火墙阻止 Java 程序，请选中此框。 Java 是一种常见的网站编程语言。如果拒绝 Java 程序，您可能无法访问使用此编程语言创建的 Internet 站点。折衷的办法是，您可以选中此框以阻止不受信任站点或未知站点上的 Java 程序，但同时允许受信任站点上的 Java 程序 （请参阅下文的 *Don 懿 block Java/Java/ActiveX/Cookies/Proxy to Trusted Domains [不要阻止到受信任域的 Java/Java/ActiveX/Cookies/Proxy]*）。默认情况下，系统不会阻止 Java 程序。

- **Cookies**：如果希望防火墙阻止所有的 Cookies，请选中此框。 Cookie 是网站存储在用户 PC 上的数据。如果阻止 Cookies，网站可能无法正常运行。折衷的办法是，您可以选中此框以阻止不受信任站点或未知站点上的 Cookies，但同时允许受信任站点上的 Cookies （请参阅下文的 *Don 懿 block Java/Java/ActiveX/Cookies/Proxy to Trusted Domains [不要阻止到受信任域的 Java/Java/ActiveX/Cookies/Proxy]*）。默认情况下，系统不会阻止 Cookies。

- **ActiveX**：如果希望防火墙阻止 ActiveX 控件，请选中此框。 ActiveX 是一种网站编程语言。如果拒绝 ActiveX，您可能无法访问使用此编程语言创建的 Internet 站点。折衷的办法是，您可以选中此框以阻止不受信任站点或未知站点上的 ActiveX，但同时允许受信任站点上的 ActiveX 程序 （请参阅下文的 *Don 懿 block Java/Java/ActiveX/Cookies/Proxy to Trusted Domains [不要阻止到受信任域的 Java/Java/ActiveX/Cookies/Proxy]*）。默认情况下，系统不会阻止 ActiveX。

- **Access to HTTP Proxy Servers**：如果希望阻止访问 HTTP 代理服务器，请选中此框。使用 WAN 代理服务器可能会降低路由器的安全性。如果启用此功能，系统将阻止访问使用端口 80 或 8080 的代理服务器。折衷的办法是，您可以选中此框以阻止访问不受信任的服务器或未知服务器，但同时允许访问受信任的服务器 （请参阅下文的 *Don 懿 block Java/Java/ActiveX/Cookies/Proxy to Trusted Domains [不要阻止到受信任域的 Java/Java/ActiveX/Cookies/Proxy]*）。默认情况下，系统不会阻止访问 HTTP 代理服务器。

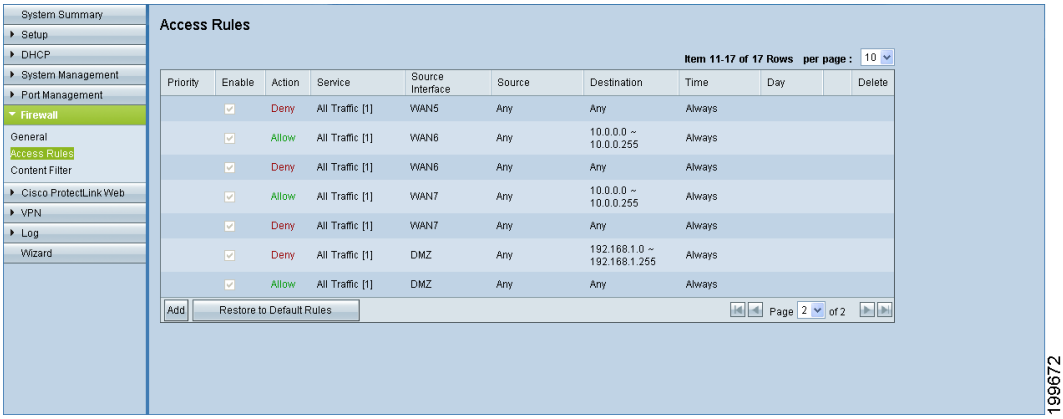
- **Don't block Java/ActiveX/Cookies/Proxy to Trusted Domains**：如果您已阻止任一 Web 功能，则选中此框可以对您在受信任列表中输入的域允许这些功能。（仅当选中其他任一复选框以禁用某一 Web 功能时，页面的此区域才可用。）如果不选中此框，则所选的 Web 功能将在所有网站上都受到阻止。

- **在受信任列表中添加域的步骤**：输入要添加到受信任列表中的域。然后单击“**Add to list**”。
- **在受信任列表中添加另一域的步骤**：输入该域，然后单击“**Add to list**”。
- **修改受信任列表中域的步骤**：单击该域。相关信息将显示在文本字段中。进行更改，然后单击“**Update**”。
- **从受信任列表中删除域的步骤**：单击该域，然后单击“**Delete**”。

配置防火墙访问规则

对于大多数小型企业而言，默认的访问规则应该足以满足其需求。但是，您可以使用“*Firewall*”>“*Access Rules*”页面来为您的网络修改或添加新的访问规则。访问规则决定了哪些流量允许通过路由器的防火墙。作为可选操作，您可以设置一个计划表，以使每个访问规则在指定的天数和时间内保持活动或不活动状态。

打开此页面的步骤：在导航树中单击“**Firewall**”>“**Access Rules**”。



注意 离开此页面前，请单击“**Save**”保存设置，或单击“**Cancel**”撤消设置。所有未保存的更改都将被丢弃。

请参阅以下主题：

- 关于访问规则，页码 85
- 配置访问规则，页码 85
- 设置访问规则，页码 87

关于访问规则

路由器有以下默认规则：

- 允许所有流量从 LAN 传输到 WAN。
- 拒绝所有流量从 WAN 传输到 LAN。
- 允许所有流量从 LAN 传输到 DMZ。
- 拒绝所有流量从 DMZ 传输到 LAN。
- 允许所有流量从 WAN 传输到 DMZ。
- 允许所有流量从 DMZ 传输到 WAN。

警告 使用自定义规则可以禁用所有的防火墙保护或阻止所有对 Internet 的访问，所以在创建或删除访问规则时，要极其谨慎。

以下四种其他默认规则将始终处于活动状态且无法被任何自定义规则覆盖：

- 始终允许从 LAN 到路由器的 HTTP 服务。
- 始终允许来自 LAN 的 DHCP 服务。
- 始终允许来自 LAN 的 DNS 服务。
- 始终允许从 LAN 到路由器的 Ping 服务。

配置访问规则

除默认规则之外，所有已配置的访问规则都列在 “Access Rules” 表中，您可以为每个自定义规则设置优先级。

注意 除此流程以外，您还可以使用访问规则向导。有关详细信息，请参阅**第 11 章，“向导”**。

如果您有多种规则，则可以调整显示方式。使用表格右上角的 “*Rows per page list*” 来选择每页显示的规则数。使用表格下方的 “*Page*” 列表来选择特定页面。使用导航按钮查看第一页、上一页、下一页和最后一页。某些按钮可能不可用，具体取决于页面数和当前选择。

- **Priority**：访问规则的优先级， 1 代表最高优先级。要更改规则的优先级，请从下拉列表中选择某个选项。如果两个访问规则之间存在冲突，则优先满足优先级较高的规则。默认访问规则的优先级最低。

创建访问规则时，路由器会自动分配优先级，但您可以在规则创建完成后更改优先级。

- **Enable**：要启用某个规则，请选中 “**Enable**” 框。要禁用某个规则，请取消选中该框。无法更改默认规则。

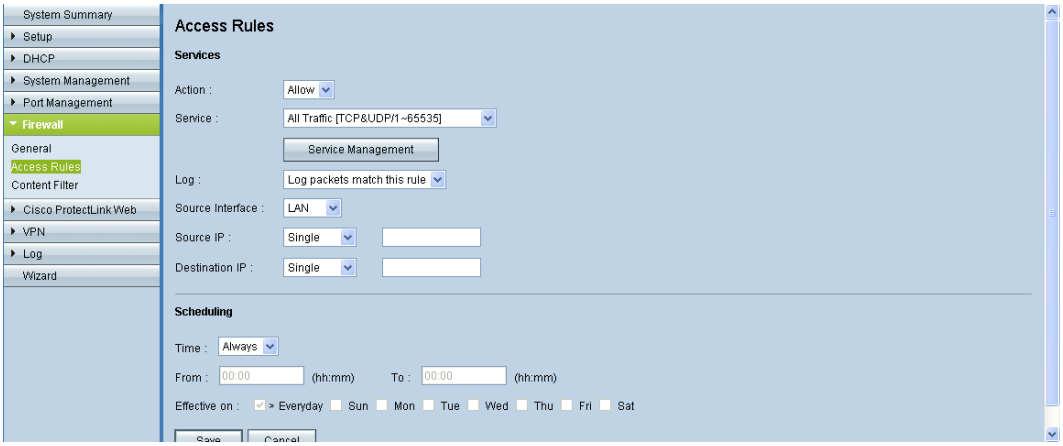
此页面显示的其他无法更改的信息如下：

- **Action**：规则执行的操作，可选择 Allow 或 Deny 以允许或拒绝访问
- **Service**：受此规则影响的服务
- **Source Interface**：受此规则影响的源接口
- **Source**：流量源的 IP 地址，也可选择 “Any”
- **Destination**：流量目标的 IP 地址，也可选择 “Any”
- **Time**：访问规则处于活动状态的特定时间间隔，也可选择 “Always”
- **Day**：访问规则处于活动状态的特定几天，也可选择 “Always”

根据需要添加或编辑规则。

- **添加规则的步骤**：单击 “**Add New Rule**”。输入设置，如**设置访问规则，页码 87** 中所述。
- **修改自定义规则的步骤**：单击 “**Edit**” 图标。输入设置，如**设置访问规则，页码 87** 中所述。
- **删除访问规则的步骤**：单击 “**Delete**” 图标。当屏幕上显示确认消息时，请单击 “**OK**” 继续操作，或单击 “**Cancel**” 关闭消息且不删除规则。
- **删除所有自定义规则的步骤**：单击 “**Restore to Default Rules**”。

设置访问规则



单击 “*Access Rules*”表中的 “**Add New Rule**”或 “**Edit**”图标后，在添加 / 编辑页面上输入以下信息。

注意 离开此页面前，请单击 “**Save**”保存设置。当出现 “Success”消息时，请单击 “**OK**”停留在当前页面以添加另一访问规则，或单击 “**Cancel**”返回 “*Access Rules*”表。要撤消此页面上的更改，请单击 “**Cancel**”。所有未保存的更改都将被丢弃。

服务

- **Action**：选择规则执行的操作，可选择 Allow 或 Deny 以允许或拒绝访问。
- **Service**：选择受此规则影响的服务。如果您需要添加服务，请单击 “**Service Management**”。有关详细信息，请参阅**添加服务，页码 88**。
- **Source Interface**：选择受此规则影响的源接口。
- **Source**：标识受此规则影响的流量源。对于单个 IP 地址，请从下拉列表中选择 “Single”；对于 IP 地址范围，请选择 “Range”；或者对于任意 IP 地址，请选择 “Any”。然后，输入一个或多个 IP 地址。
- **Destination**：标识受此规则影响的流量目标。对于单个 IP 地址，请从下拉列表中选择 “Single”；对于 IP 地址范围，请选择 “Range”；或者对于任意 IP 地址，请选择 “Any”。然后，输入一个或多个 IP 地址。

计划表

当此规则处于活动状态时，请保持默认设置或指定一个计划表：

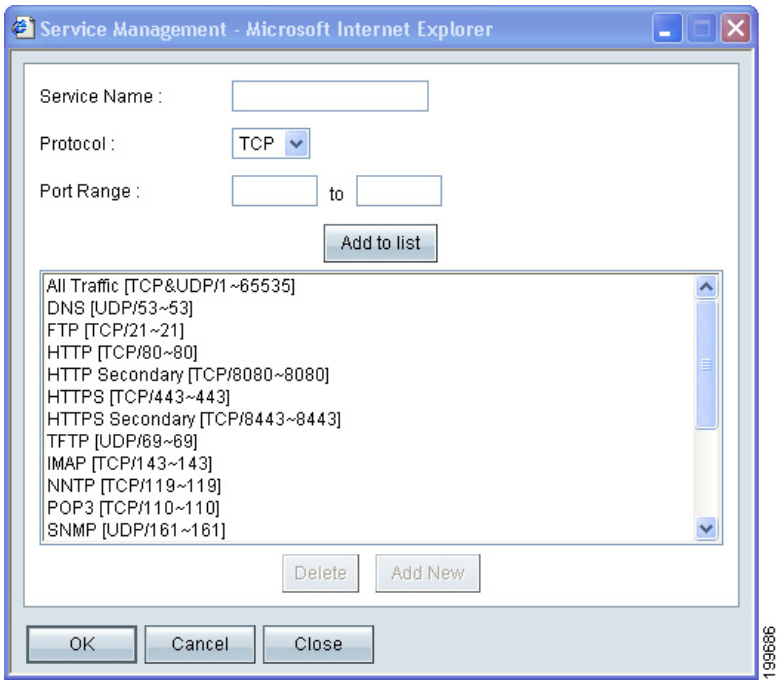
- **Time**：请选择以下选项之一：

- **Always**：如果要在一周中的每一天都始终应用此规则，请选择此选项。作为可选操作，您可以在“*From*”和“*To*”字段中输入一个时间段。
- **Interval**：如果要指定此规则处于活动状态的时间段，请选择此选项。如果选择此选项，您必须在“*From*”和“*To*”字段中输入一个时间段。作为可选操作，您可以指定一周中的某几天。

- **From** 和 **To**：如果选择“Interval”，请使用这些字段来指定此规则在哪些时间和哪几天处于活动状态。在“*From*”字段中输入开始时间，并在“*To*”字段中输入结束时间。使用 hh:mm 格式，例如下午 3:30 为 15:30。如果要在一天中始终应用此规则，请输入 00:00 到 00:00。
- **Effective on**：如果选择“Interval”，请使用这些复选框来指定此规则在哪几天处于活动状态。如果要此规则每天都处于活动状态，请选中“**Everyday**”框。要选择特定几天，请取消选中“**Everyday**”框，然后选中此规则处于活动状态的每一天所对应的框。

添加服务

要在“*Service*”列表中添加新条目或者更改之前创建的条目，请单击“**Service Management**”。如果 Web 浏览器显示弹出窗口警告，请允许显示被阻止的内容。



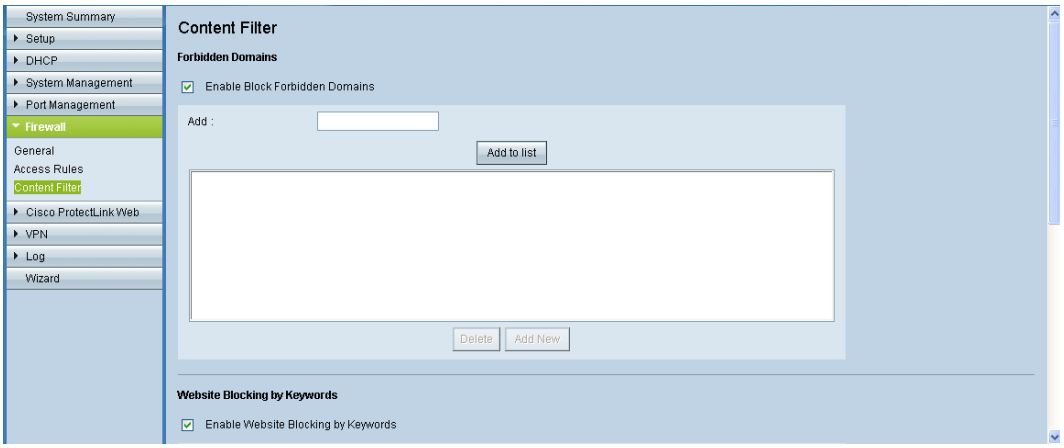
在“*Service Management*”窗口中，根据需要添加或更新条目。关闭此窗口前，请单击“**OK**”保存设置，或单击“**Cancel**”撤消设置。所有未保存的更改都将被丢弃。

- **在列表中添加服务的步骤**：输入以下信息，然后单击 “**Add to List**”。列表中最多可包含 30 个服务。
  - **Service Name**：输入简短说明。
  - **Protocol**：选择所需协议。请参阅您正托管的服务的文档。
  - **Port Range**：输入所需的端口范围。
- **添加另一新服务的步骤**：输入信息，然后单击 “**Add to list**”。
- **修改已创建服务的步骤**：单击列表中的服务。相关信息将显示在文本字段中。进行更改，然后单击 “**Update**”。如果无需进行更改，则可以单击 “**Add New**”，以取消选中该服务并清空文本字段。
- **从列表中删除服务的步骤**：单击要删除的条目。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 键的同时单击相应条目。单击 “**Delete**”。

使用内容过滤器控制 Internet 访问

使用 “*Firewall*” > “*Content Filter*”页面阻止您的用户访问不当网站。您可以通过指定域和关键字来阻止访问。

打开此页面的步骤：在导航树中单击 “**Firewall**” > “**Content Filter**”。



注意 离开此页面前，请单击 “**Save**”保存设置，或单击 “**Cancel**”撤消设置。所有未保存的更改都将被丢弃。

您可以阻止访问指定的域，或者阻止更大范围的站点、阻止访问包含指定关键字的 URL。此外，您还可以指定这些过滤器处于活动状态的日期和时间。该页面包括以下几个部分：

- **已禁止的域，页码 90**
- **按关键字阻止网站，页码 91**
- **计划表，页码 91**

注意 如果路由器上已激活 Cisco ProtectLink 服务，则内容过滤器规则将自动禁用。此时，应配置 ProtectLink 功能来控制 Internet 访问。有关详细信息，请参阅**第 8 章，“Cisco ProtectLink Web”**。

已禁止的域

选中 “**Enable Block Forbidden Domains**”框，以允许路由器阻止访问指定的域。取消选中此框可禁用此功能。

根据需要添加或编辑规则。请记住，只有单击 “Save”按钮后，条目才会保存。

- **在列表中添加条目的步骤**：在 “**Add**”框中键入域名。然后单击 “**Add to list**”。根据需要，重复此任务以添加其他域。

如果用户在浏览器地址栏中输入指定域名或导航到指定域内的网页，则系统将阻止访问。例如，假设系统已阻止 *yahoo.com*，则用户将无法成功输入任何以 *yahoo.com* 开头的 URL。另外，如果用户执行 Web 搜索并单击指定域（例如 *yahoo.com/news*）内的页面链接，系统同样也会阻止访问。但是，用户可以连接到 *mail.yahoo.com*，因为这是另一个不同的域。

- **修改列表中条目的步骤**：单击要修改的条目。进行更改，然后单击“**Update**”。如果无需进行更改，则可以单击“**Add New**”，以取消选中该条目并清空文本字段。
- **从列表中删除条目的步骤**：单击要删除的条目。然后单击“**Delete**”。

按关键字阻止网站

选中“**Enable Website Blocking By Keywords**”框，以允许路由器阻止访问包括指定字符的 URL。取消选中此框可禁用此功能。

根据需要添加或编辑规则。请记住，只有单击“Save”按钮后，条目才会保存。

- **在列表中添加条目的步骤**：在“**Add**”框中键入关键字。然后单击“**Add to list**”。关键字可以是一个完整的单词（例如 *government*），也可以是几个字符（例如 *gov*）。根据需要，重复此任务以添加其他关键字。

  如果用户输入或导航到包含指定字符的 URL，则系统将阻止访问。例如，假设系统已阻止 *yahoo*，则用户将无法访问 *www.yahoo.com*、*finance.yahoo.com* 或 *mydomain.com/news/yahoo*。
- **修改列表中条目的步骤**：单击要修改的条目。进行更改，然后单击“**Update**”。如果无需进行更改，则可以单击“**Add New**”，以取消选中该条目并清空文本字段。
- **从列表中删除条目的步骤**：单击要删除的条目。然后单击“**Delete**”。

计划表

当内容过滤处于活动状态时，请保留默认设置或指定一个计划表：

- **Time**：请选择以下选项之一：
  - **Always**：如果要在一周中的每一天都始终应用此规则，请选择此选项。作为可选操作，您可以在“*From*”和“*To*”字段中输入一个时间段。
  - **Interval**：如果要指定此规则处于活动状态的时间段，请选择此选项。如果选择此选项，您必须在“*From*”和“*To*”字段中输入一个时间段。作为可选操作，您可以指定一周中的某几天。
- **From** 和 **To**：如果选择“Interval”，请使用这些字段来指定此规则在哪些时间和哪几天处于活动状态。在“From”字段中输入开始时间，并在“To”字段

中输入结束时间。使用 hh:mm 格式，例如下午 3:30 为 15:30。如果要在一天中始终应用此规则，请输入 00:00 到 00:00。

- **Effective on**：如果选择 “Interval”，请使用这些复选框来指定此规则在哪几天处于活动状态。如果要此规则每天都处于活动状态，请选中 “**Everyday**” 框。要选择特定几天，请取消选中 “**Everyday**” 框，然后选中此规则处于活动状态的每一天所对应的框。

8

Cisco ProtectLink Web

您可选择 Cisco ProtectLink Web 服务来为您的网络提供安全保护。该服务可过滤网站地址 (URL) 并拦截潜在的恶意网站。请参阅以下主题：

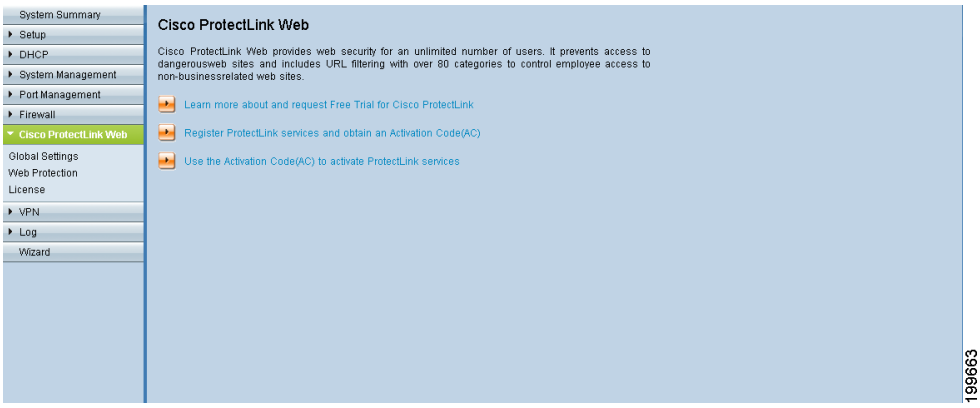
- **Cisco ProtectLink Web 入门，页码 93**
- **为许可 URL 和客户端指定全局设置，页码 94**
- **更新 ProtectLink 许可证，页码 98**

注意 有关此思科产品的详细信息，请访问 Cisco ProtectLink Web 信息页面，网址为 www.cisco.com/en/US/products/ps9953/index.html

Cisco ProtectLink Web 入门

使用 “*Cisco ProtectLink Web*”页面上的链接，您可以购买、注册和激活该服务。

打开此页面的步骤：在导航树中单击 “**Cisco ProtectLink Web**”。



选择相应的选项：

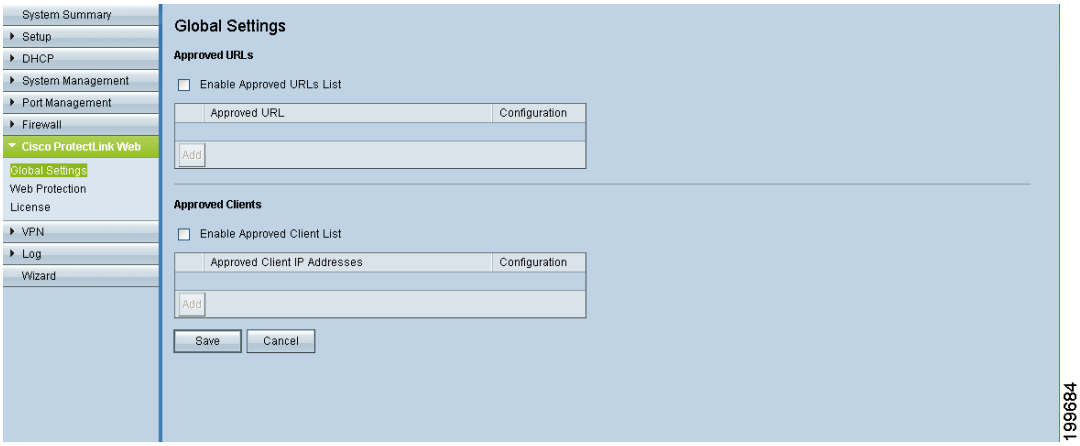
- **Learn more about and request Free Trial for Cisco ProtectLink**：单击此链接可打开 Cisco.com 上的 “Cisco ProtectLink Security Solutions” 页面。您可以阅读产品信息并为您的 RV 路由器获取 30 天的试用服务。
- **Register ProtectLink services and obtain an Activation Code (AC)**：如果您已购买该产品并准备注册，请单击此链接。当显示注册页面时，请按照屏幕上的说明输入您的注册密钥并提供所需信息。完成此流程后，请关闭 Web 页面。此时，屏幕上将显示激活码，且系统会将其发送到您提供的电子邮件地址。
- **Use the Activation Code (AC) to activate ProtectLink services**：如果您已完成产品注册并收到激活码，请单击此链接。当显示激活页面时，请输入您的激活码并按照屏幕上的说明继续操作。完成此流程后，请关闭 Web 页面。刷新 Web 浏览器，现在您的路由器已具有 ProtectLink Web 功能。此时将显示 “*Global Settings*” 页面。

注意 如果您将其中一个路由器替换为另一个支持此服务的路由器，则可以使用 “**Use the Activation Code**” 链接将 ProtectLink 服务的许可证传输至新路由器。

为许可 URL 和客户端指定全局设置

激活服务后，您可以使用 “*Cisco ProtectLink Web*” > “*Global Settings*” 页面在路由器上配置服务。

打开此页面的步骤：在导航树中单击 “**ProtectLink**” > “**Global Settings**”。



注意 仅当 Cisco ProtectLink Web 服务激活后，此页面才可用。请参阅 **Cisco ProtectLink Web 入门，页码 93**。

您可以指定用户始终能够访问的许可 URL。您也可以指定许可客户端，这些客户端不受您在 “Web Protection” 中配置的限制影响。

要在 “*Approved URLs*” 表或 “*Approved Clients*” 表中添加条目，请单击 “**Add**”。要删除条目，请单击 “Delete” 图标。

注意 离开此页面前，请单击 “**Save**” 保存设置，或单击 “**Cancel**” 撤消设置。所有未保存的更改都将被丢弃。

许可 URL 和许可客户端

单击 “*Cisco ProtectLink Web*” > “*Global Settings*” 页面上的 “Add” 按钮后，将显示 “Configuration” 页面。

注意 离开此页面前，请单击 “**Save**” 保存设置，或单击 “**Cancel**” 撤消设置。所有未保存的更改都将被丢弃。

许可 URL 配置

无论 “Web Protection” 设置如何，此列表上的域都始终可访问。

选中 “**Enable Approved URL list**” 框，以启用此功能。然后，添加始终可访问的受信任 URL （最多 20 个）。

- **添加条目的步骤**：单击 “**Add New**” 以打开 “*Approved URL Configuration*” 页面。在框中输入受信任 URL。要输入多个 URL，请在条目之间键入分号，例如 *www.cisco.com;www.google.com;www.mycompany.com*。指定域中的所有页面都将能够进行访问。单击 “**Save**” 保存更改，或单击 “**Cancel**” 撤消更改。

  如果您输入了任何无效字符，系统将显示一条消息。单击 “**OK**” 关闭该消息并编辑条目。不允许输入空格、逗号和符号。

- **删除条目的步骤**：单击 “**Delete**” 图标。

许可客户端配置

此列表中的客户端始终能够连接到所有网站。Web Protection 功能不会限制来自这些 IP 地址的 URL 请求。

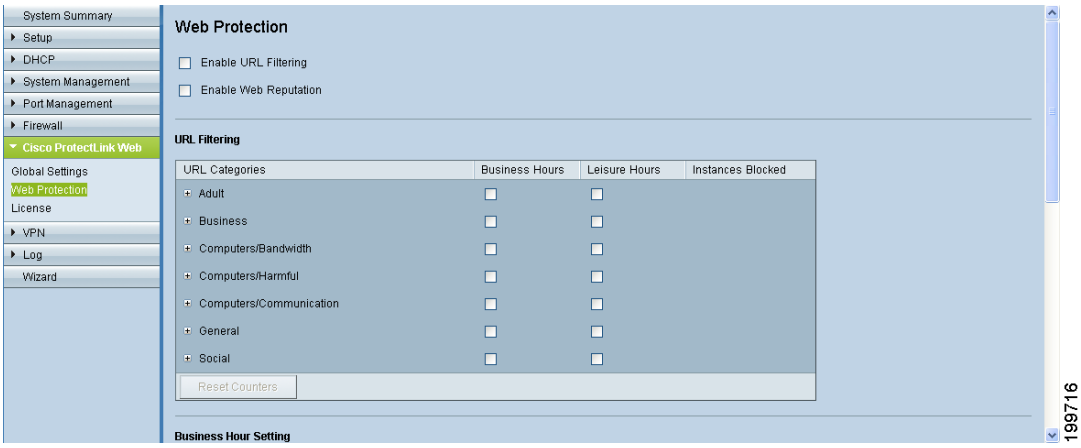
选中 “**Enable Approved Client list**” 框，以启用此功能。然后，最多添加 20 个始终能够访问已过滤 URL 的受信任客户端 （本地 IP 地址）。

- **添加条目的步骤**：输入 IP 地址或范围。要输入非连续的 IP 地址，请在条目之间键入分号，例如 *10.1.1.1;10.1.1.5*。要输入 IP 地址范围，请在范围内的第一个和最后一个地址之间键入连字符，例如 *10.1.1.0-10.1.1.10*。
- **删除条目的步骤**：单击 “**Delete**”图标。

为 URL 过滤启用 Web Protection

使用 “*Cisco ProtectLink Web*” > “*Web Protection*”页面配置 URL 过滤和 “Web Reputation”设置。

打开此页面的步骤：在导航树中单击 “**ProtectLink**” > “**Web Protection**”。



注意

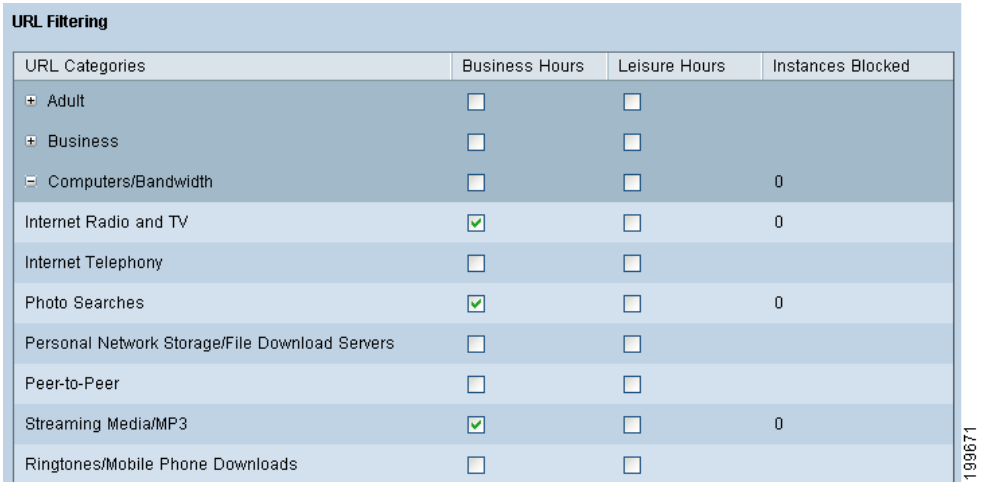
- 仅当 Cisco ProtectLink Web 服务激活后，此页面才可用。请参阅 **Cisco ProtectLink Web 入门，页码 93**。
- 离开此页面前，请单击 “**Save**”保存设置，或单击 “**Cancel**”撤消设置。所有未保存的更改都将被丢弃。

Web Protection

- **Enable URL Filtering**：选中此框可阻止访问基于预定义类别的网站。取消选中此框可禁用此服务。
- **Enable Web Reputation**：选中此框可根据 Cisco ProtectLink Web 安全数据库验证 URL 请求。建议使用此服务来拦截潜在的恶意网站。取消选中此框可禁用此服务。

URL 过滤

选择您希望在办公时间和休息时间拦截的网站类别和子类别。



注意 要定义办公时间和休息时间，请参阅“*办公时间设置*”部分。如果保留默认的办公时间设置，则每天所有时间都将归类为办公时间。您可以忽略休息时间对应的复选框。

- 要查看某个类别下的子类别，请单击加号 (+)。
- 要阻止对某个类别下所有子类别的访问，请选中此类别所对应的复选框。要禁用对某个类别的过滤，请取消选中该类别所对应的复选框。
- 要阻止对个别子类别的访问，请分别选中各复选框。要禁用对某个子类别的过滤，请取消选中每个复选框。
- **Instances Blocked**：对于每个已启用的过滤器，此列都会显示某人尝试访问某个已拦截站点的次数。
- **Reset Counters**：路由器会计算尝试访问某个受限 URL 的次数。要将计数器重置为零，请单击此按钮。

办公时间设置

使用此部分中的设置为 URL 过滤定义办公时间和休息时间。

注意 如果保留默认的办公时间设置，则每天所有时间都将归类为办公时间。如果选择特定的日期和时间，则选定的时段为办公时间，而未选定的时段为休息时间。

- **Business Days**：选中每个办公日期所对应的复选框。取消选中每个非办公日期所对应的复选框。在选中的日期将应用办公时间过滤器。在未选中的日期将应用休息时间过滤器。

- **Business Times**：要全天使用相同的设置，请保留默认设置 “**All day (24 hours)**”。要指定办公时间，请单击 “**Specify business hours**”。选中 “**Morning**” 框并选择 “*From*” 和 “*To*” 时间。然后，选中 “**Afternoon**” 框并选择 “*From*” 和 “*To*” 时间。在选中的时期将应用办公时间过滤器。在其他所有时期将应用休息时间过滤器。

Web Reputation

请选择相应的安全级别：

- **High**：选择此选项可拦截较多的潜在恶意网站，但同时也可能出现较多的拦截错误 （合法站点被归类为恶意网站）。
- **Medium**：选择此选项可拦截大多数潜在恶意网站，且出现较少的拦截错误（合法站点被归类为恶意网站）。“**Medium**”为建议设置。
- **Low**：选择此选项可拦截较少的潜在恶意网站，因此可降低出现拦截错误的风险。

URL 溢出控制

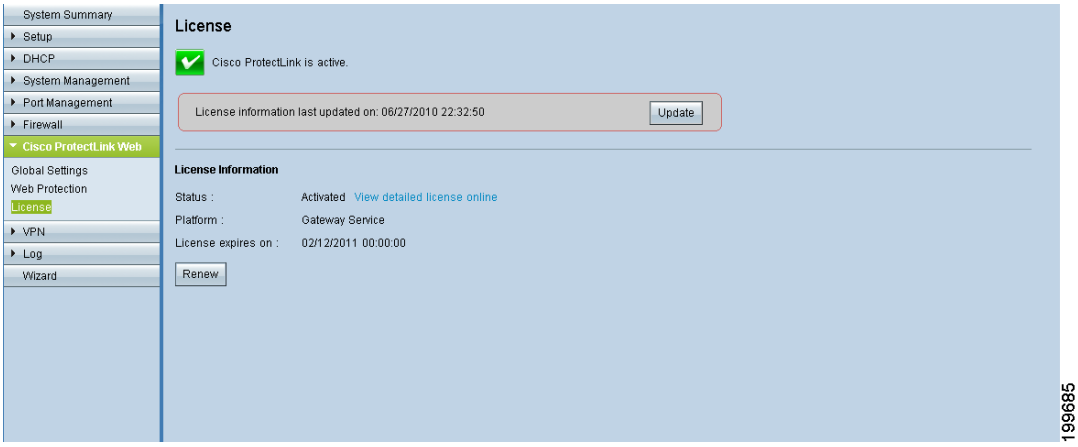
指定在 URL 请求的数量超出服务所能处理的数量时，此服务的行为。

- **Temporarily block URL requests**：建议使用此设置。选择此选项可在服务能够处理请求之前抑制溢出。此选项为系统默认的设置。
- **Temporarily bypass URL verification for requested URLs**：选择此选项可允许所有的溢出请求不经过验证而直接通过。不建议使用此设置。

更新 ProtectLink 许可证

使用 “*Cisco ProtectLink Web*” > “*License*” 页面查看许可证信息或更新许可证。

打开此页面的步骤：在导航树中单击 “**ProtectLink**” > “**License**”。



注意 仅当 Cisco ProtectLink Web 服务激活后，此页面才可用。请参阅 **Cisco ProtectLink Web 入门，页码 93**。

许可证

- **Update Information**：要刷新屏幕上显示的许可证信息，请单击 “**Update Information**”。

许可证信息

- **View detailed license online**：要在线查看许可证信息，请单击此链接。Web 浏览器将打开 “*ProtectLink Product Detail*” 页面。阅读完信息后，可以关闭该页面。
- **Status**：许可证的状态：“*Activated*” 或 “*Expired*”
- **Platform**：平台类型，“Gateway Service”。
- **License expires on**：许可证到期的日期和时间 （服务激活后一年）
- **Renew**：有关更新许可证的信息，请单击 “**Renew**”。购买延期密钥后，您可以注册该密钥并激活服务。

9

VPN

使用 VPN 模块配置虚拟专用网络 (VPN)，以允许从其他位置安全访问您的网站。请参阅以下主题：

VPN 简介

VPN 是在不同网络中的两个端点 （例如 VPN 路由器）之间建立起来的连接，它使用户能够在共享网络或公共网络 （例如 Internet）上安全地发送私人数据。这就建立起了一种专用网络，用户可在这两个位置或网络之间安全地发送数据。

通过创建 “隧道”可建立专用网络。 VPN 隧道可连接两台计算机或两个网络，并且能够使数据如同还在这些网络中一般地在 Internet 上进行传输。 VPN 隧道使用业内标准的加密和验证技术保护在两个网络之间发送的数据。

虚拟专用网络是一种可节省成本的选择，无需将专用、专有、租用的线路用于专用网络。它可用来创建连接总公司与分公司、远程工作者和 / 或移动办公的专业人员的安全的网络。

有两种基本的方法可用于创建 VPN 连接：

- **站点到站点**：某个办公室内的 VPN 路由器连接到位于远程办公室的 VPN 路由器。
- **远程访问**：安装有 VPN 客户端软件的计算机连接到 VPN 路由器。

VPN 路由器在两个端点之间创建了一条 “隧道”或通道，因此，两个端点之间的数据传输是安全的。安装有 VPN 客户端软件的计算机可以是其中一个端点。

对于 IPSec VPN 隧道， VPN 路由器和任何安装有内置 IPSec Security Manager（Windows 2000、 Windows XP 和 Windows 7）的计算机均可创建 VPN 隧道。如果计算机未安装内置客户端，则需要安装其他第三方 VPN 客户端软件。

注意 Cisco RV0xx 系列 VPN 路由器支持 IPSec VPN 客户端软件，包括 Cisco QuickVPN 软件。（有关详细信息，请参阅**附录 B，“用于 Windows 的 Cisco QuickVPN”**。）

RV0xx 系列路由器和任何运行 Windows 2000 或 XP 的计算机均可使用 PPTP 创建 VPN 隧道。

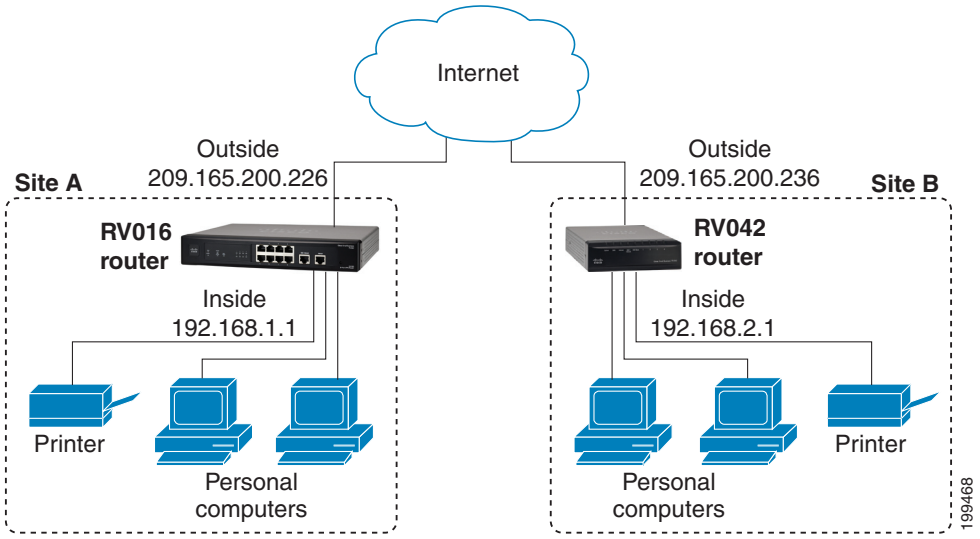
VPN 示例

以下示例分别列举了两个 VPN 路由器之间的 VPN 隧道以及使用 VPN 客户端软件的计算机和 VPN 路由器之间的 VPN 隧道。

VPN 路由器至 VPN 路由器

例如，一位远程工作者在家中使用他的 VPN 路由器来实现 Internet 连接永不间断。他按照自己在办公室中对 VPN 所进行的设置配置了路由器。当他连接至自己办公室里的路由器时，两个路由器便创建了一条 VPN 隧道对数据进行加密和解密。由于 VPN 使用的是 Internet，因此距离不是问题。现在，通过使用 VPN，这位远程工作者可安全地连接至总公司的网络，就像进行了物理连接一样。

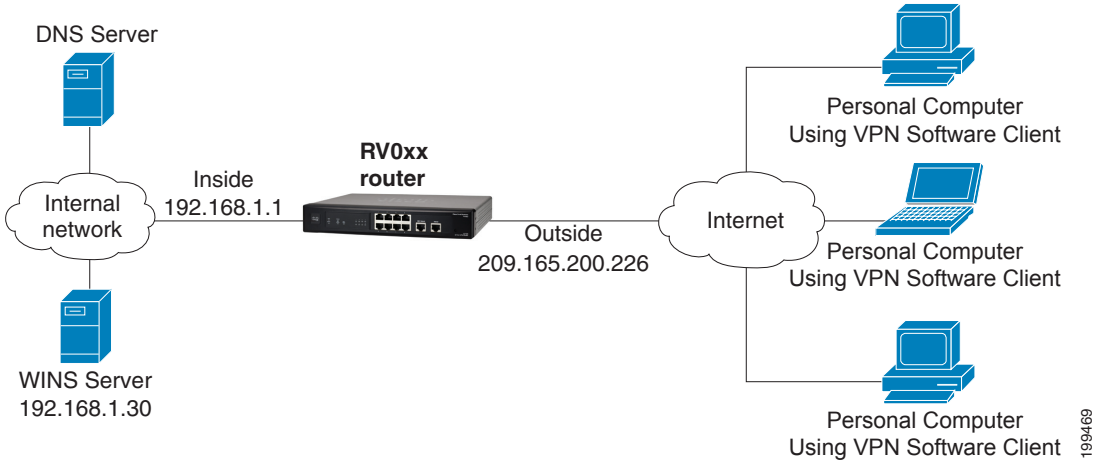
图 1 VPN 路由器至 VPN 路由器



计算机 （使用 VPN 客户端软件）至 VPN 路由器

下面列举了计算机至 VPN 路由器 VPN 的一个示例。一位出差在外的女商人在酒店房间内连接到自己的 Internet 服务提供商 (ISP)。她的笔记本电脑中安装了 VPN 客户端软件，且已使用自己办公室的 VPN 设置对软件进行了配置。她可访问 VPN 客户端软件，并可连接至总公司的 VPN 路由器。由于 VPN 使用的是 Internet，因此距离不是问题。现在，通过使用 VPN，这位女商人可安全地连接至总公司的网络，就像进行了物理连接一样。

图 2 计算机至 VPN 路由器

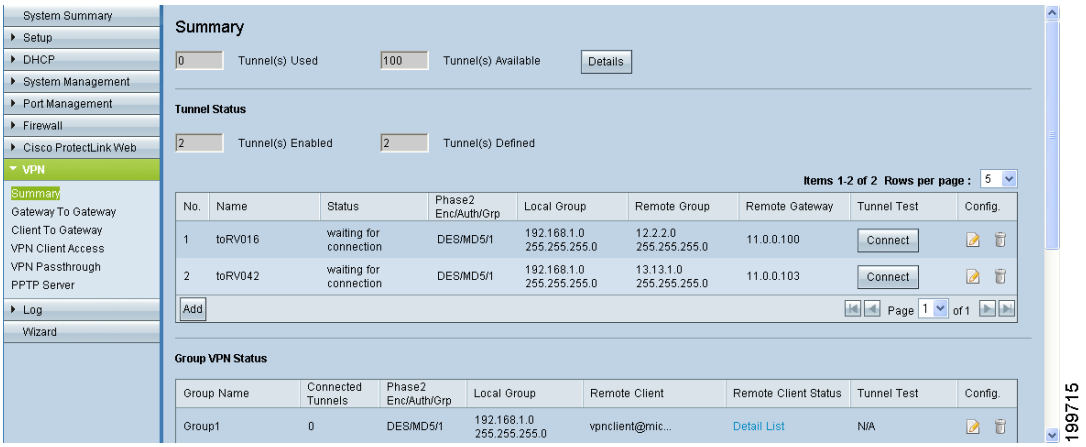


查看 VPN 概要信息

“*VPN*”>“*Summary*”页面显示了有关路由器 VPN 隧道设置的一般信息。路由器最多可支持 100 个隧道。

注意 如果 PPTP Server 已启用，则“*VPN*”>“*PPTP Server*”页面上将会显示有关 PPTP 客户端的概要信息。有关详细信息，请参阅**设置 PPTP 服务器，页码 123**。

打开此页面的步骤：在导航树中单击“**VPN**”>“**Summary**”。



概要

- **Tunnel(s) Used**：已使用的 VPN 隧道数
- **Tunnels Available**：可用的 VPN 隧道数
- **Detail**：请单击“**Detail**”获取详细信息。单击“**Refresh**”更新数据，或者单击“**Close**”返回到“*VPN Summary*”页面。对于每个 VPN 隧道，系统都会显示对应的“No.”、“Name”、“Status”、“Phase 2 Enc/Auth/Grp”、“Local Group”、“Remote Group”和“Remote Gateway”。

隧道状态

表格上方将会显示以下信息：

- **Tunnel(s) Enabled**：已启用的隧道数
- **Tunnel(s) Defined**：已定义的隧道数，包括启用和禁用的隧道

表中将会显示有关每个隧道的以下信息：

- **No.**：VPN 隧道的标识号

- **Name**：VPN 隧道的描述性名称
- **Status**：VPN 隧道的状态：“*Connected*”或“*Waiting for Connection*”
- **Phase2 Enc/Auth/Grp**：您在 “IPSec Setup”部分中选择的第 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)。

  如果您在 IPSec 部分中为 “Keying Mode”选择了 “Manual”，则仅显示加密类型和验证方法。
- **Local Group**：本地组的 IP 地址和子网掩码
- **Remote Group**：远程组的 IP 地址和子网掩码
- **Remote Gateway**：远程网关的 IP 地址
- **Tunnel Test**：单击 “**Connect**”验证 VPN 隧道的状态。测试结果将在“*Status*”列中更新。如果隧道已连接，可使用 “Disconnect”按钮结束连接。
- **Configure**：单击 “**Edit**”图标打开新页面，您可在该页面中更改隧道设置。要删除隧道设置，请选择隧道，然后单击 “**Delete**”图标
- **Tunnel Enabled**：已启用的 VPN 隧道数。
- **Tunnel Defined**：已定义的 VPN 隧道数。
- **Add**：单击此按钮可添加隧道。然后选择以下选项之一：
  - 要为使用 VPN 路由器的远程站点创建隧道，请选择 “**Gateway to Gateway**”。此时将会显示 “*Gateway to Gateway*”页面。请参阅**设置网关对网关 （站点到站点） VPN，页码 107**。
  - 要为使用 VPN 客户端软件的远程工作人员创建隧道，请选择 “**Client to Gateway**”。此时将会显示 “*Client to Gateway*”页面。请参阅**为 VPN 客户端设置远程访问隧道，页码 113**。
- **Navigation controls**：如果您有多种规则，则可以调整显示方式。使用表格右上角的 “*Rows per page list*”来选择每页显示的规则数。使用表格下方的“*Page*”列表来选择特定页面。使用导航按钮查看第一页、上一页、下一页和最后一页。某些按钮可能不可用，具体取决于页面数和当前选择。

GroupVPN 状态

如果您为任何客户端对网关隧道启用了 GroupVPN 设置，则此表中将会显示状态信息。

- **Group Name**：组 VPN 的描述性名称

- **Connected Tunnels**：登录到组 VPN 的用户数
- **Phase2 Enc/Auth/Grp**：在 “*IPSec Setup*” 部分中配置的第 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**：本地组的 IP 地址和子网掩码
- **Remote Client**：组 VPN 中的远程客户端
- **Remote Clients Status**：远程客户端的状态：“*Online*” 或 “*Offline*”。单击 “**Detail List**” 打开 “*Group List*” 窗口。此窗口将显示组名、 IP 地址和连接时间。您可单击 “**Refresh**” 更新数据，或单击 “**Close**” 关闭弹出窗口并返回到 “*VPN*” > “*Summary*” 页面。
- **Tunnel Test**：单击 “**Connect**” 验证组 VPN 的状态。测试结果将在 “*Status*” 列中更新。如果组 VPN 已连接，可使用 “Disconnect” 按钮结束连接。
- **Configure**：单击 “**Edit**” 图标打开新页面，您可在该页面中更改隧道设置。要删除隧道设置，请选择隧道，然后单击 “**Delete**” 图标
- **Navigation controls**：如果您有多种规则，则可以调整显示方式。使用表格右上角的 “*Rows per page list*” 来选择每页显示的规则数。使用表格下方的 “*Page*” 列表来选择特定页面。使用导航按钮查看第一页、上一页、下一页和最后一页。某些按钮可能不可用，具体取决于页面数和当前选择。

VPN Clients 状态

此部分将标识当前连接到路由器的 VPN 客户端。

- **No.**：VPN 客户端的 ID 号
- **Username**：VPN 客户端名称
- **Status**：VPN 客户端连接状态
- **Start Time**：VPN 客户端与路由器建立起 VPN 连接的时间
- **End Time**：VPN 客户端结束其到路由器的 VPN 连接的时间
- **Duration**：VPN 连接处于活动状态的时间段
- **Disconnect**：单击此按钮可断开任何 VPN 客户端连接。
- **Navigation controls**：如果您有多种规则，则可以调整显示方式。使用表格右上角的 “*Rows per page list*” 来选择每页显示的规则数。使用表格下方的 “*Page*” 列表来选择特定页面。使用导航按钮查看第一页、上一页、下一页和最后一页。某些按钮可能不可用，具体取决于页面数和当前选择。

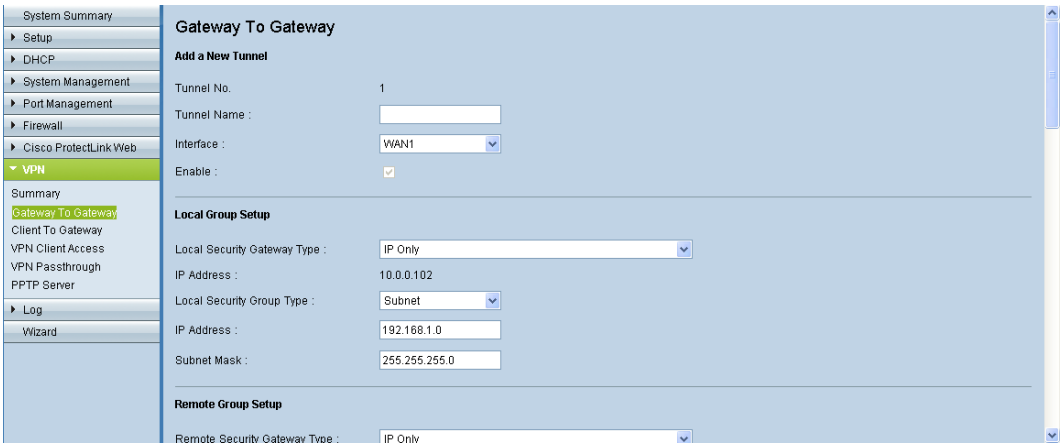
设置网关对网关 （站点到站点） VPN

使用 “*VPN*” > “*Gateway to Gateway*”页面在两个 VPN 设备 （例如办公室内的 Cisco RV082 路由器和远程工作人员家中的 Cisco RV042 路由器）之间创建新的隧道。

您将需要输入本地组和远程组的设置，并且在配置另一个路由器时映射这些设置。要想成功连接，则要求至少一个路由器可通过静态 IP 地址或动态 DNS 主机名标识。如果某个路由器仅有一个动态 IP 地址，您可使用任何电子邮件地址来验证是否已建立连接。隧道两端不能在相同的子网上。

“Local Group”和 “Remote Group”设置必须在两个路由器上进行映射。配置此路由器 （路由器 A）时，请在 “*Local Group Setup*”部分中输入其设置，并在 “*Remote Group Setup*”部分输入另一个路由器 （路由器 B）的设置。配置另一个路由器 （路由器 B）时，请在 “*Local Group Setup*”部分中输入其设置，并在 “*Remote Group Setup*”部分输入路由器 A 的设置。

打开此页面的步骤：在导航树中单击 “**VPN**” > “**Gateway to Gateway**”。或者，您也可以单击 “*VPN*” > “*Summary*”页面 “*Tunnel Status*”部分中的 “**Add Tunnel**”按钮。然后选择 “**Gateway to Gateway**”。



注意 离开此页面前，请单击 “**Save**”保存设置，或单击 “**Cancel**”撤消设置。所有未保存的更改都将被丢弃。

添加新隧道

- **Tunnel No**：自动生成的 ID 号
- **Tunnel Name**：在该字段中输入此 VPN 隧道的名称，例如 Los Angeles Office、 Chicago Branch 或 New York Division。此描述仅供您参考。无需与隧道另一端所使用的名称相匹配。

- **Interface**：选择此隧道使用的 WAN 端口。
- **Enable**：选中此框可启用 VPN 隧道。（创建 VPN 隧道时，系统会禁用此复选框。)

本地组设置和远程组设置

按照以下说明输入设置。本地设置用于此路由器，而远程设置则用于隧道另一端的路由器。配置另一个路由器上的 VPN 隧道时，请确保映射这些配置。

- **Local/Remote Security Gateway Type**：指定标识路由器的方法，以创建 VPN 隧道。本地安全网关在此路由器上，而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 地址或动态 DNS 主机名才可建立连接。
  - **IP Only**：如果此路由器拥有静态 WAN IP 地址，则选择此选项。 WAN IP 地址将会自动显示。

    对于 “*Remote Security Gateway Type*”，将会显示一个另外的字段。如果您知道远程 VPN 路由器的 IP 地址，请选择 “**IP Address**”，然后输入地址。如果您不知道远程 VPN 路由器的 IP 地址，请选择 “**IP by DNS Resolved**”，然后输入路由器在 Internet 上的真实域名。 Cisco RV082 将获取通过 DNS 解析的远程 VPN 设备 IP 地址，远程 VPN 设备的 IP 地址将显示在 “Summary”页面的 “VPN Status”部分中。
  - **IP + Domain Name (FQDN) Authentication**：如果此路由器拥有静态 IP 地址和注册域名，则选择此选项。此外，还需输入 “**Domain Name**”进行验证。该域名仅可用于一个隧道连接。

    对于 “*Remote Security Gateway Type*”，将会显示一个另外的字段。如果您知道远程 VPN 路由器的 IP 地址，请选择 “**IP Address**”，然后输入地址。如果您不知道远程 VPN 路由器的 IP 地址，请选择 “**IP by DNS Resolved**”，然后输入路由器在 Internet 上的真实域名。 Cisco RV082 将获取通过 DNS 解析的远程 VPN 设备 IP 地址，远程 VPN 设备的 IP 地址将显示在 “Summary”页面的 “VPN Status”部分中。
  - **IP + E-mail Addr.(USER FQDN) Authentication**：如果此路由器拥有静态 IP 地址并且您希望使用电子邮件地址进行验证，则选择此选项。当前的 WAN IP 地址将会自动显示。输入任意 “**Email Address**”进行验证。

    对于 “*Remote Security Gateway Type*”，将会显示一个另外的字段。如果您知道远程 VPN 路由器的 IP 地址，请选择 “**IP Address**”，然后输入地址。如果您不知道远程 VPN 路由器的 IP 地址，请选择 “**IP by DNS Resolved**”，然后输入路由器在 Internet 上的真实域名。 Cisco RV082 将获取通过 DNS 解析的远程 VPN 设备 IP 地址，远程 VPN 设备的 IP 地址将显示在 “Summary”页面的 “VPN Status”部分中。

- **Dynamic IP + Domain Name (FQDN) Authentication**：如果此路由器拥有动态 IP 地址和注册动态 DNS 主机名 （可从 DynDNS.com 等供应商处获得），则选择此选项。输入 “**Domain Name**”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**：如果此路由器拥有动态 IP 地址但没有动态 DNS 主机名，则选择此选项。输入任意 “**Email Address**”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.”。对于远程网关，请选择 “**IP Address**”和 “**IP Address by DNS Resolved**”。

- **Local/Remote Security Group Type**：指定可从此隧道访问的 LAN 资源。本地安全组对应于此路由器的 LAN 资源，而远程安全组对应于另一个路由器的 LAN 资源。
  - **IP Address**：选择此选项，指定一个设备。然后输入设备的 IP 地址。从该隧道仅可访问此设备。
  - **Subnet**：选择此选项 （默认选项）以允许从 VPN 隧道访问子网上的所有设备。然后输入子网 IP 地址和掩码。
  - **IP Range**：选择此选项以允许从 VPN 隧道访问一系列设备。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。

IPSec 设置

输入此隧道的 “Internet Protocol Security”设置。

重要事项：要进行任何加密， 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。

- **Keying Mode**：请选择以下密钥管理方法中的一种：
  - **Manual**：如果您想自行生成密钥而不希望启用密钥协商，请选择此选项。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。有关信息，请参阅 **Manual 模式必填字段，页码 110**。
  - **IKE with Preshared Key**：选择此选项，以使用 Internet 密钥交换协议为隧道设置安全关联 (SA)。 IKE 将使用预先共享密钥验证远程 IKE 对端。此设置是推荐设置，默认情况下为选中状态。输入所需设置。有关详细信息，请参阅 **“IKE with Preshared Key”模式必填字段，页码 110** 和 **“IKE with Preshared Key”模式高级设置，页码 111**。

- **Manual 模式必填字段**

  输入手动模式的设置。配置此隧道的另一个路由器时，请确保输入相同的设置。“Incoming / Outgoing SPI”设置必须在另一个路由器上进行映射。

  - **Incoming / Outgoing SPI**：安全性参数索引包含在 ESP （封装安全载荷协议）报头中进行传输，接收方和发送方将根据它选择用于处理数据包的安全关联。您可输入 100~ffffffff 范围内的十六进制值。每条隧道必须具有唯一的传入 SPI 和传出 SPI。任何两条隧道不得共享相同的 SPI。此处的传入 SPI 必须与隧道另一端的传出 SPI 值相匹配，反之亦然。

  - **Encryption**：选择加密方法：DES 或 3DES。此设置决定了用于对 ESP 数据包进行加密或解密的密钥的长度。DES 为 56 位加密，而 3DES 为 168 位加密。推荐使用 3DES，因为这种方法更加安全。

  - **Authentication**：选择验证方法：MD5 或 SHA1。验证方法决定了 ESP 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。SHA 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。

  - **Encryption Key**：输入用于加密和解密 IP 流量的密钥。如果已选择 DES 加密，则输入 16 位十六进制值。如果已选择 3DES 加密，则输入 40 位十六进制值。如果未输入足够位数的十六进制值，则需在密钥后追加零，以达到所需的长度。

  - **Authentication Key**：输入用于验证 IP 流量的密钥。如果已选择 MD5 验证，则输入 32 位十六进制值。如果已选择 SHA，则输入 40 位十六进制值。如果未输入足够位数的十六进制值，则需在密钥后追加零，以达到所需的长度。

- **“IKE with Preshared Key”模式必填字段**

  输入第 1 阶段和第 2 阶段的设置。在第 1 阶段将创建预先共享密钥以建立安全验证通信通道。在第 2 阶段， IKE 对端将使用安全通道代表 IPsec 等其他设备协商安全关联。配置此隧道的另一个路由器时，请确保输入相同的设置。

  - **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 - 1,024 位、Group 5 - 1,536 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**：选择此阶段的加密方法：DES、 3DES、AES-128、 AES-192 或 AES-256。加密方法决定了用于对 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**：选择此阶段的验证方法：MD5 或 SHA。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。 SHA 是一种可生成 160 位摘要的单向散列算法。推荐使用 SHA，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**：配置 VPN 隧道在此阶段处于活动状态的时间长度。第 1 阶段的默认值为 28800 秒。第 2 阶段的默认值为 3600 秒。
- **Perfect Forward Secrecy**：如果启用了完全向前保密 (PFS) 功能，则 IKE 第 2 阶段的协商将为 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。选中此框以启用此功能，或取消选中此框以禁用此功能。建议使用此功能。
- **Preshared Key**：输入用于验证远程 IKE 对端的预先共享密钥。您最多可以输入 30 位键盘字符和十六进制值，例如 My_@123 或 4d795f40313233。确保 VPN 隧道两端使用相同的预先共享密钥。强烈建议您定期更改预先共享密钥，以便将 VPN 安全性提到最高。
- **Minimum Preshared Key Complexity**：如果您希望启用 “Preshared Key Strength Meter”，请选中 “**Enable**”框。
- **Preshared Key Strength Meter**：如果您启用了 “Minimum Preshared Key Complexity”，该测量工具将会指示预先共享密钥的强度。输入预先共享密钥时，会出现彩色条。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先共享密钥，其中应包括八个以上字符、大写和小写字母、数字和符号，例如 -*^+=。

- **“IKE with Preshared Key”模式高级设置**

当 “Keying Mode”设置为 “IKE with Preshared Key”模式时，系统将提供高级设置。对于大多数用户，基本设置应足以满足其要求。高级用户可单击 “**Advanced +**”查看高级设置。要隐藏这些设置，请单击 “**Advanced -**”

- **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”。如果 “Remote Security Gateway Type”是 “*IP Only*”或者其中一种 “*IP +*” 类型，则可对此设置进行调整。选中此框将启用 “Aggressive Mode”，取消选中此框将禁用 “Aggressive Mode”并使用 “Main Mode”。

  注意：如果 “Remote Security Gateway Type”是其中一种 “*Dynamic IP*”类型，则必须使用 “Aggressive”模式。此框将自动选中，且无法更改此设置。

- **Compress (Support IP Payload Compression Protocol (IP Comp))**：IP Comp 是一种可减小 IP 数据报大小的协议。选中此框时，路由器将在启动连接时提出压缩。如果应答器拒绝此提议，则路由器将不会实施压缩。将路由器用作应答器时，它将始终接受压缩，即使是在压缩未启用的情况下。如果您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**：此功能将使路由器在 VPN 连接断开时尝试自动重新建立 VPN 连接。选中此框以启用此功能，或取消选中此框以禁用此功能。

- **AH Hash Algorithm**：AH （验证报头）协议描述了数据包格式和数据包结构的默认标准。使用 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。选中此框以使用此功能。然后选择验证方法：MD5 或 SHA1。 MD5 将生成 128 位摘要以验证数据包。 SHA 将生成 160 位摘要以验证数据包。隧道两端应使用相同的算法。

- **NetBIOS Broadcast**：NetBIOS 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，您可以通过选中此框允许 NetBIOS 广播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 Internet 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。这一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。取消选中此框可禁用此功能。隧道两端必须使用相同的设置。

- **Dead Peer Detection (DPD)**：选中此框时，路由器将定期发送 HELLO/ACK 消息以检查 VPN 隧道的状态。要使用该功能，必须在 VPN 隧道两端同时启用该功能。指定 HELLO/ACK 消息之间的时间间隔 （发送消息的频率）。

  Tunnel Backup：当 DPD 确定远程对端不可用时，有了该功能，路由器便可使用远程对端的备用 IP 地址或者备用的本地 WAN 接口重新建立 VPN 隧道。选中此框以启用此功能。然后输入以下所述设置。仅当 “Dead Peer Detection” 启用时，此功能才可用。

  Remote Backup IP Address：指定远程对端的备用 IP 地址，或者重新输入已为远程网关设置的 WAN IP 地址。

  Local Interface：选择要用来重新建立连接的 WAN 接口。

  VPN Tunnel Backup Idle Time：路由器启动时将使用此设置。如果主隧道未在指定时间内连接，则使用备用隧道。默认空闲时间为 30 秒。

- **Split DNS （仅限 RV082）**：使用拆分 DNS，路由器可以根据指定的域名，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。收到来自客户端的地址解析请求时，路由器将检查域名。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。选中此框以启用此功能，或取消选中此框以禁用此功能。

  DNS1：指定用于指定域的 DNS 服务器 IP 地址。作为可选操作，您也可以在 “**DNS2**” 字段中指定辅助 DNS 服务器。

  Domain Name 1 - Domain Name 4：为这些 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。

为 VPN 客户端设置远程访问隧道

使用 “*VPN*” > “*Client To Gateway*” 页面创建新的 VPN 隧道，以允许远程用户通过使用 TheGreenBow 等第三方 VPN 客户端软件访问您的网络。

注意 RV0xx 系列路由器支持 IPSec VPN 客户端软件，包括 Cisco QuickVPN 软件。要管理访问权限并为 Cisco QuickVPN 客户端生成证书，请单击 “**VPN Client Access**” 选项卡。（有关 QuickVPN 的详细信息，请参阅**附录 B，“用于 Windows 的 Cisco QuickVPN”**。）

打开此页面的步骤：在导航树中单击 “**VPN**” > “**Client to Gateway**”。或者，您也可以单击 “*VPN*” > “*Summary*” 页面 “*Tunnel Status*” 部分中的 “**Add Tunnel**” 按钮。然后选择 “**Client to Gateway**”。

您可以为一位远程用户配置一个 VPN 隧道或者为多位远程用户配置一个组 VPN。请参阅以下主题：

添加新隧道

请选择以下选项之一：

- **Tunnel**：选择此选项可为单个远程用户创建隧道。隧道编号将自动生成并显示在 “*Tunnel No*” 字段中。输入以下信息：
- **Group VPN**：选择此选项可为一组用户创建隧道。路由器最多可支持两个组 VPN。组号将自动生成并显示在 “*Group No*” 字段中。

输入以下信息：

- **Tunnel Name**：输入描述隧道的名称。对于单个用户，您可以输入用户名或位置。对于组 VPN，您可以标识组的业务角色或位置。此描述仅供您参考，无需与隧道另一端所使用的名称相匹配。
- **Interface**：选择相应的 WAN 端口。
- **Enable**：选中此框可启用组 VPN。

本地组设置

- **Local Security Gateway Type**：指定标识此路由器的方法，以创建 VPN 隧道。
  - **IP Only**：如果此路由器拥有静态 WAN IP 地址，则选择此选项。 WAN IP 地址将会自动显示。
  - **IP + Domain Name (FQDN) Authentication**：如果此路由器拥有静态 IP 地址和注册域名，则选择此选项。此外，输入任意 “**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**：如果此路由器拥有静态 IP 地址并且您希望使用电子邮件地址进行验证，则选择此选项。当前的 WAN IP 地址将会自动显示。输入任意 “**Email Address**” 进行验证。
  - **Dynamic IP + Domain Name (FQDN) Authentication**：如果此路由器拥有动态 IP 地址和注册动态 DNS 主机名 （可从 DynDNS.com 等供应商处获得），则选择此选项。输入 “**Domain Name**” 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**：如果此路由器拥有动态 IP 地址但没有动态 DNS 主机名，则选择此选项。输入任意 “**Email Address**” 进行验证。

- **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**：如果您选择使用域名验证，请输入域名。
- **Email**：如果您选择使用电子邮件验证，请输入电子邮件地址。

远程客户端设置

指定标识客户端的方法，以创建 VPN 隧道。

- **IP Only**：如果远程 VPN 客户端拥有静态 WAN IP 地址，则选择此选项。如果您知道客户端的 IP 地址，请选择 “**IP Address**”，然后输入地址。如果您不知道客户端的 IP 地址，请选择 “**IP by DNS Resolved**”，然后输入客户端在 Internet 上的真实域名。路由器将获取通过 DNS 解析的远程 VPN 客户端 IP 地址，远程 VPN 客户端的 IP 地址将显示在 “*Summary*” 页面的 “VPN Status” 部分中。
- **IP + Domain Name (FQDN) Authentication**：如果此客户端拥有静态 IP 地址和注册域名，则选择此选项。此外，还需输入 “**Domain Name**” 进行验证。该域名仅可用于一个隧道连接。

  如果您知道远程 VPN 客户端的 IP 地址，请选择 “**IP Address**”，然后输入地址。如果您不知道远程 VPN 客户端的 IP 地址，请选择 “**IP by DNS Resolved**”，然后输入客户端在 Internet 上的真实域名。路由器将获取通过 DNS 解析的远程 VPN 客户端 IP 地址，远程 VPN 客户端的 IP 地址将显示在 “*Summary*” 页面的 “VPN Status” 部分中。
- **IP + E-mail Addr.(USER FQDN) Authentication**：如果此客户端拥有静态 IP 地址并且您希望使用任意电子邮件地址进行验证，则选择此选项。当前的 WAN IP 地址将会自动显示。输入任意 “**Email Address**” 进行验证。

  如果您知道远程 VPN 客户端的 IP 地址，请选择 “**IP Address**”，然后输入地址。如果您不知道远程 VPN 客户端的 IP 地址，请选择 “**IP by DNS Resolved**”，然后输入客户端在 Internet 上的真实域名。 Cisco RV082 将获取通过 DNS 解析的远程 VPN 客户端 IP 地址，远程 VPN 设备的 IP 地址将显示在 “Summary” 页面的 “VPN Status” 部分中。

- **Dynamic IP + Domain Name (FQDN) Authentication**：如果此客户端拥有动态 IP 地址和注册动态 DNS 主机名 （可从 DynDNS.com 等供应商处获得），则选择此选项。输入 “**Domain Name**”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**：如果此客户端拥有动态 IP 地址但没有动态 DNS 主机名，则选择此选项。输入任意 “**Email Address**”进行验证。

IPSec 设置

输入此隧道的 “Internet Protocol Security”设置。

重要事项：要进行任何加密， VPN 隧道的两端必须就加密、解密和验证方法达成一致。

- **Keying Mode**：请选择以下密钥管理方法中的一种：
  - **Manual**：如果您想自行生成密钥而不希望启用密钥协商，请选择此选项。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。有关信息，请参阅 **Manual 模式必填字段，页码 116**。
  - **IKE with Preshared Key**：选择此选项，以使用 Internet 密钥交换协议为隧道设置安全关联 (SA)。 IKE 将使用预先共享密钥验证远程 IKE 对端。此设置是推荐设置，默认情况下为选中状态。输入所需设置。有关详细信息，请参阅 **“IKE with Preshared Key”模式必填字段，页码 117** 和 **“IKE with Preshared Key”模式高级设置，页码 118**。
- **Manual 模式必填字段**

  输入手动模式的设置。
  - **Incoming / Outgoing SPI**：安全性参数索引包含在 ESP （封装安全载荷协议）报头中进行传输，接收方和发送方将根据它选择用于处理数据包的安全关联。您可输入 100~ffffffff 范围内的十六进制值。每条隧道必须具有唯一的传入 SPI 和传出 SPI。任何两条隧道不得共享相同的 SPI。此处的传入 SPI 必须与隧道另一端的传出 SPI 值相匹配，反之亦然。
  - **Encryption**：选择加密方法：DES 或 3DES。此设置决定了用于对 ESP 数据包进行加密或解密的密钥的长度。DES 为 56 位加密，而 3DES 为 168 位加密。推荐使用 3DES，因为这种方法更加安全。
  - **Authentication**：选择验证方法：MD5 或 SHA1。验证方法决定了 ESP 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。SHA 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。

- **Encryption Key**：输入用于加密和解密 IP 流量的密钥。如果已选择 DES 加密，则输入 16 位十六进制值。如果已选择 3DES 加密，则输入 40 位十六进制值。如果未输入足够位数的十六进制值，则需在密钥后追加零，以达到所需的长度。
- **Authentication Key**：输入用于验证 IP 流量的密钥。如果已选择 MD5 验证，则输入 32 位十六进制值。如果已选择 SHA，则输入 40 位十六进制值。如果未输入足够位数的十六进制值，则需在密钥后追加零，以达到所需的长度。

- **“IKE with Preshared Key”模式必填字段**

输入第 1 阶段和第 2 阶段的设置。在第 1 阶段将创建预先共享密钥以建立安全验证通信通道。在第 2 阶段， IKE 对端将使用安全通道代表 IPsec 等其他设备协商安全关联。

- **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 - 1,024 位、Group 5 - 1,536 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**：选择此阶段的加密方法：DES、 3DES、AES-128、 AES-192 或 AES-256。加密方法决定了用于对 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**：选择此阶段的验证方法：MD5 或 SHA。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。 SHA 是一种可生成 160 位摘要的单向散列算法。推荐使用 SHA，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**：配置 VPN 隧道在此阶段处于活动状态的时间长度。第 1 阶段的默认值为 28800 秒。第 2 阶段的默认值为 3600 秒。
- **Perfect Forward Secrecy**：如果启用了完全向前保密 (PFS) 功能，则 IKE 第 2 阶段的协商将为 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。选中此框以启用此功能，或取消选中此框以禁用此功能。建议使用此功能。
- **Preshared Key**：输入用于验证远程 IKE 对端的预先共享密钥。您最多可以输入 30 位键盘字符和十六进制值，例如 My_@123 或 4d795f40313233。确保 VPN 隧道两端使用相同的预先共享密钥。强烈建议您定期更改预先共享密钥，以便将 VPN 安全性提到最高。

- **Minimum Preshared Key Complexity**：如果您希望启用 “Preshared Key Strength Meter”，请选中 “**Enable**”框。
- **Preshared Key Strength Meter**：如果您启用了 “Minimum Preshared Key Complexity”，该测量工具将会指示预先共享密钥的强度。输入预先共享密钥时，会出现彩色条。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先共享密钥，其中应包括八个以上字符、大写和小写字母、数字和符号，例如 -*^+=。

- **“IKE with Preshared Key”模式高级设置**

当 “Keying Mode”设置为 “IKE with Preshared Key”模式时，系统将提供高级设置。对于大多数用户，基本设置应足以满足其要求。高级用户可单击 “**Advanced +**”查看高级设置。要隐藏这些设置，请单击 “**Advanced -**”

- **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”。如果 “Remote Security Gateway Type”是 “*IP Only*”或者其中一种 “*IP +*”类型，则可对此设置进行调整。选中此框将启用 “Aggressive Mode”，取消选中此框将禁用 “Aggressive Mode”并使用 “Main Mode”。

  注意：如果 “Remote Security Gateway Type”是其中一种 “*Dynamic IP*”类型，则必须使用 “Aggressive”模式。此框将自动选中，且无法更改此设置。

- **Compress (Support IP Payload Compression Protocol (IP Comp))**：IP Comp 是一种可减小 IP 数据报大小的协议。选中此框时，路由器将在启动连接时提出压缩。如果应答器拒绝此提议，则路由器将不会实施压缩。将设备用作应答器时，它将始终接受压缩，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，则在客户端上也应该启用此功能。
- **Keep-Alive**：此功能将使路由器在 VPN 连接断开时尝试自动重新建立 VPN 连接。选中此框以启用此功能，或取消选中此框以禁用此功能。
- **AH Hash Algorithm**：AH （验证报头）协议描述了数据包格式和数据包结构的默认标准。使用 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。选中此框以使用此功能。然后选择验证方法：MD5 或 SHA1。 MD5 将生成 128 位摘要以验证数据包。 SHA 将生成 160 位摘要以验证数据包。隧道两端应使用相同的算法。
- **NetBIOS Broadcast**：NetBIOS 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 功能需要这些消息。LAN 广播流量通常不会通过

VPN 隧道进行转发。但是，您可以通过选中此框允许 NetBIOS 广播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 Internet 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。这一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。取消选中此框可禁用此功能。隧道两端必须使用相同的设置。

- **Dead Peer Detection (DPD)**：选中此框时，路由器将定期发送 HELLO/ACK 消息以检查 VPN 隧道的状态。要使用该功能，必须在 VPN 隧道两端同时启用该功能。指定 HELLO/ACK 消息之间的时间间隔 （发送消息的频率）。

  Remote Backup IP Address：指定远程对端的备用 IP 地址，或者重新输入已为远程网关设置的 WAN IP 地址。

  Local Interface：选择要用来重新建立连接的 WAN 接口。

- **Split DNS**：使用拆分 DNS，路由器可以根据指定的域名，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。如果隧道的一端有用于其内部域的本地 DNS 服务器，此功能将非常有用。收到来自客户端的地址解析请求时，路由器将检查域名。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。选中此框以启用此功能，或取消选中此框以禁用此功能。

  DNS1：指定用于指定域的 DNS 服务器 IP 地址。作为可选操作，您也可以在 “**DNS2**”字段中指定辅助 DNS 服务器。

  Domain Name 1 - Domain Name 4：为这些 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。

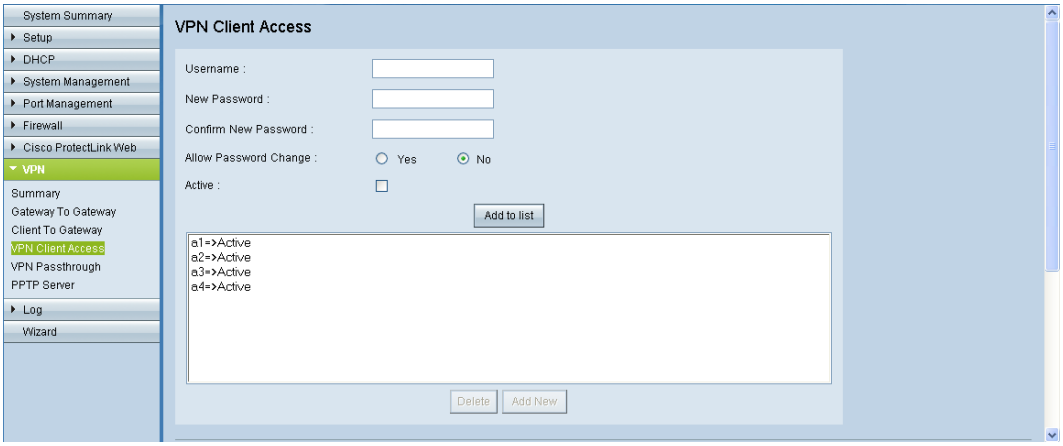
管理 VPN 用户和证书

使用 “*VPN*” > “*Client Access*”页面配置 VPN 用户名和密码并生成要在客户机上安装的 SSL 证书。最多可添加 50 个用户。首先，导出证书，将导出的证书用于 Cisco QuickVPN Client。然后在屏幕顶部输入相应信息，您输入的用户将显示在底部的列表中，其中还显示了用户的状态。路由器最多支持 50 个 Cisco QuickVPN Client。

注意

- QuickVPN Client 1.4.0.5 或更高版本支持 Windows 7/XP/Vista。必须在 Vista 和 Windows 7 中启用防火墙。 QuickVPN 用户必须拥有 PC 的管理员权限。
- 对于第三方 VPN 客户端，如 TheGreenbow，请配置客户端对网关隧道。
- 即使 PC 上没有安装证书，用户也可以进行连接。在连接至 VPN 隧道时用户将看到安全警告，但仍可在不使用该额外安全保护功能的情况下继续。

打开此页面的步骤：在导航树中单击 “**VPN**” > “**VPN Client Access**”。



按照需要添加或更新用户。对于每位新用户，请导出客户端证书，安装在该用户的 PC 上以获得更为安全的连接。

- **用户，页码 121**
- **证书管理，页码 121**

注意 离开此页面前，请单击 “**Save**”保存设置，或单击 “**Cancel**”撤消设置。所有未保存的更改都将被丢弃。初次保存这些设置时，系统将显示消息，询问您是否要路由器自动更改 LAN IP 地址以防止 IP 地址冲突。要更改 LAN IP 地址，请单击 “**Yes**”。如果出现 IP 冲突， QuickVPN 客户端将无法连接到路由器。

用户

- **在列表中添加 VPN 用户的步骤**：输入以下信息，然后单击 “**Add to list**”。添加用户之后，您可以生成要在用户计算机上安装的证书 （有关详细信息，请参阅**证书管理，页码 121**）。
  - **Username**：为此用户输入用户名。
  - **New Password**：输入密码。
  - **Confirm New Password**：重新输入密码以进行确认。
  - **Allow Password Change**：选中 “**Yes**” 允许用户更改密码，或者单击 “**No**” 阻止用户更改分配的密码。
  - **Active**：选中此复选框将激活新用户。
- **添加其他新用户的步骤**：输入信息，然后单击 “**Add to list**”。
- **修改列表中用户的步骤**：单击要修改的条目。相关信息将显示在文本字段中。进行更改，然后单击 “**Update**”。如果无需进行更改，则可以单击 “**Add New**”，以取消选中该条目并清空文本字段。
- **从列表中删除用户的步骤**：单击要删除的条目。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。要选择多个单一条目，请按住 Ctrl 键然后单击相应条目。单击 “**Delete**”。

证书管理

- **Generate New Certificate**：要生成新证书替换路由器上的现有证书，请单击 “**Generate**”。单击此按钮后，将显示确认页面。单击 “**OK**” 继续进行操作。
- **Export Certificate for Administrator**：路由器上的管理员证书包含专用密钥。您可以导出此证书的副本，将其保存为备份文件。例如，如果您要将路由器重置为出厂默认设置，则应首先导出此证书。重启路由器后，可将此文件导入以恢复证书。要导出管理员证书，请单击 “**Export for Admin**”。出现 “*File Download*” 窗口时，单击 “**Save**”。选择一个安全位置保存此证书，输入描述性文件名，然后单击 “**Save**”。出现 “*Download complete*” 窗口时，单击 “**Close**”。
- **Export Certificate for Client**：您可以在用户 PC 上安装客户端证书，以防中间人攻击。要导出客户端证书，请单击 “**Export for Client**”。出现 “*File Download*” 窗口时，单击 “**Save**”。找到客户端软件的安装目录 （通常为 C:\Program Files\Cisco Small Business\QuickVPN client），输入描述性文件名，然后单击 “**Save**”。出现 “*Download complete*” 窗口时，单击 “**Close**”。

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

- **Import Certificate**：要恢复先前保存的管理员证书，请单击 “**Browse**”，找到文件，然后单击 “**Open**”。然后单击 “**Import**”。出现确认消息时，单击 “**OK**”用指定的文件替换现有证书。单击 “**Cancel**”将关闭此消息并取消导入该证书。
- **Existing Certificate**：存储在路由器上的当前证书的文件名。

设置 VPN 通道

使用 “*VPN*” > “*VPN Passthrough*”页面启用或禁用多种 VPN 方法的通道。默认情况下， VPN 通道为启用状态，以便允许路由器 LAN 上的 VPN 客户端连接至 Internet 上的 VPN 服务器。

思科建议启用 VPN Passthrough，以允许 VPN 客户端通过路由器顺利连接至 VPN 端点。管理员可以禁用 “VPN Passthrough”，以阻止 VPN 客户端连接至 Internet 上的 VPN 端点。

打开此页面的步骤：在导航树中单击 “**VPN**” > “**VPN Passthrough**”。

注意 离开此页面前，请单击 “**Save**”保存设置，或单击 “**Cancel**”撤消设置。所有未保存的更改都将被丢弃。

根据需要启用或禁用以下设置：

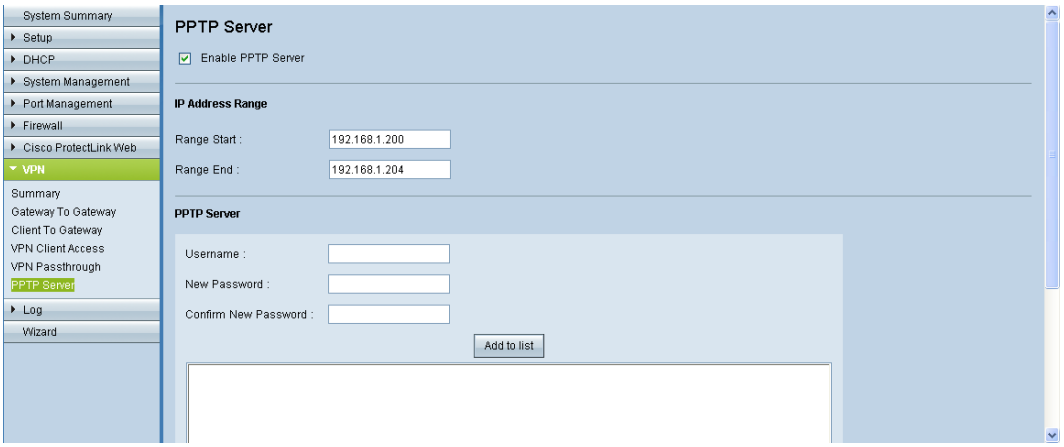
- **IPSec Passthrough**：Internet 协议安全 (IPSec) 是一套用于在 IP 层实现数据包安全交换的协议。默认情况下，系统将启用 IPSec Passthrough 来允许 IPSec 隧道通过路由器。

- **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)。默认情况下，系统将启用 “PPTP Passthrough”。
- **L2TP Passthrough**：第 2 层隧道协议是一种用于通过第 2 层上的 Internet 来启用点对点会话的方法。默认情况下，系统将启用 “L2TP Passthrough”。

设置 PPTP 服务器

使用 “*VPN*” > “*PPTP Server*”页面可为在 Windows XP 或 2000 上运行 PPTP 客户端软件的用户最多启用五个 PPTP （点对点隧道协议） VPN 隧道。 PPTP 客户端默认包含在 Microsoft Windows 中。

打开此页面的步骤：在导航树中单击 “**VPN**” > “**PPTP Server**”。



注意 离开此页面前，请单击 “**Save**”保存设置，或单击 “**Cancel**”撤消设置。所有未保存的更改都将被丢弃。

选中 “**Enable PPTP Server**”复选框将启用 PPTP VPN 隧道。取消选中此框可禁用此功能。默认情况下此功能为禁用状态。选中此复选框后，系统将显示其他字段。

IP 地址范围

输入要分配给 PPTP VPN 客户端的 LAN 地址范围。在 “**Range Start**”字段输入开始地址，在 “**Range End**”字段输入结束地址。默认范围为 192.168.1.200 至 92.168.1.204。

注意 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。

PPTP 服务器

添加或编辑 PPTP VPN 用户列表。

- **在列表中添加用户的步骤**：输入以下信息，然后单击 “**Add to list**”。
  - **Username**：为此用户输入用户名。
  - **New Password**：输入密码。
  - **Confirm New Password**：重新输入密码以进行确认。
- **添加其他新用户的步骤**：输入信息，然后单击 “**Add to list**”。
- **修改列表中用户的步骤**：单击要修改的条目。相关信息将显示在文本字段中。进行更改，然后单击 “**Update**”。如果无需进行更改，则可以单击 “**Add New**”，以取消选中该条目并清空文本字段。
- **从列表中删除用户的步骤**：单击要删除的条目。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。要选择多个单一条目，请按住 Ctrl 键然后单击相应条目。单击 “**Delete**”。

连接列表

此时将显示以下只读信息。您可以单击 “**Refresh**”更新数据。

- **Username**：PPTP VPN 客户端的名称。
- **Remote Address**：PPTP VPN 客户端的 WAN IP 地址。
- **PPTP IP Address**：PPTP 服务器在连接时分配给客户端的 LAN IP 地址。

10

记录系统统计信息

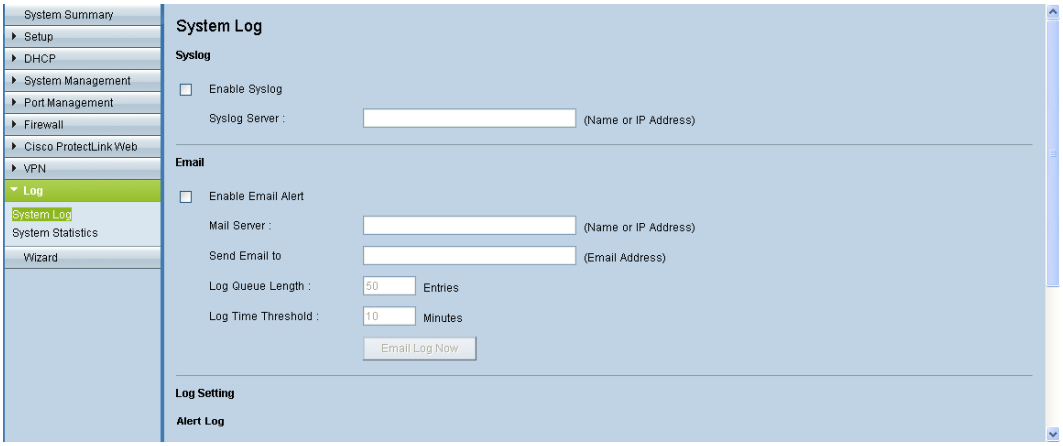
使用日志模块设置系统日志、配置警报以及查看系统统计信息。请参阅以下主题：

- **设置系统日志和警报，页码 125**
- **查看系统日志，页码 128**

设置系统日志和警报

使用 “*Log*” > “*System Log*” 页面配置日志和警报并查看日志表。

打开此页面的步骤：在导航树中单击 “**Log**” > “**System Log**”。



注意 离开此页面前，请单击 “**Save**” 保存设置，或单击 “**Cancel**” 撤消设置。所有未保存的更改都将被丢弃。

该页面包括以下部分：

- **Syslog 部分，页码 126**
- **电子邮件部分，页码 126**
- **日志设置，页码 126**

- **按钮，页码 127**

Syslog 部分

您可以启用路由器在记录事件时向 syslog 服务器发送详细的日志文件。

- **Enable Syslog**：Syslog 是用于捕获网络活动信息的行业标准协议。启用此功能后，路由器 syslog 可以捕获所有日志活动，并包括每个连接源和目标 IP 地址、 IP 服务和传输字节数。选中此框可启用 syslog。取消选中此框可禁用此功能。
- **Syslog Server**：输入 Syslog 服务器名称或 IP 地址。需重新启动 Cisco RV082 才能使更改生效。

电子邮件部分

您可以启用路由器在记录事件时发送电子邮件警报。

- **Enable E-Mail Alert**：选中此框可启用路由器，以向指定的电子邮件地址发送电子邮件警报。取消选中此框可禁用此功能。
- **Mail Server**：输入 ISP 提供的 SMTP 服务器的 IP 地址或名称。

  注意：您的 ISP 可能会要求您在 *“Setup”* > *“Network”* 页面中输入主机名，以标识您的路由器。
- **Send Email to**：输入您希望向其发送警报的电子邮件地址。
- **Log Queue Length**：指定电子邮件中包含的日志条目数。默认值为 50。
- **Log Time Threshold**：即日志时间阈值，是指发送电子邮件日志消息之前的最长等待时间。当等待时间超过 “Log Time Threshold” 中设置的值时，无论电子邮件日志缓存是否已满，系统都将发送电子邮件。指定在发送日志之前收集数据的分钟数。默认值为 10。
- **Email Log Now**：单击此按钮可立即向指定的电子邮件地址发送消息，以测试您的设置。

日志设置

选择要在日志中报告的事件：

- **警报日志**：这些事件包括常见的攻击类型以及未经授权的登录尝试。选中每种攻击类型，以将其包括在警告日志中。取消选中每个事件，以将其从警告日志中删除。
  - **Syn Flooding**：攻击者发送一系列 SYN 数据包，导致路由器打开过多无法处理的会话，并拒绝使流量合法的服务。

- **IP Spoofing**：攻击者发送带有伪造源 IP 地址的数据包，从而将攻击伪装成合法流量。
- **Win Nuke**：攻击者为使目标计算机崩溃而向 Windows 计算机发送带外消息。
- **Ping of Death**：攻击者为使目标计算机崩溃而发送非常大的 IP 数据包。
- **Unauthorized Login Attempt**：某人尝试在不提供正确的用户名和密码的情况下登录路由器配置实用程序。
- **Output Blocking Event**：ProtectLink Web 信誉或 URL 过滤中存在事件。

▪ **常规日志**：这些事件包括强制执行配置策略所采取的操作以及授权登录和配置更改等常规事件。选中每种事件类型，以将其包括在常规日志中。取消选中每个事件，以将其从常规日志中删除。

- **System Error Messages**：所有系统错误消息。
- **Deny Policies**：路由器根据您的访问规则拒绝访问的实例。
- **Allow Policies**：路由器根据您的访问规则允许访问的实例。
- **Configuration Changes**：某人保存配置中更改的实例。
- **Authorized Login**：某人在输入正确的用户名和密码之后成功登录路由器配置实用程序的实例。

按钮

使用以下按钮查看其他信息：

▪ **View System Log**：单击此按钮可查看系统日志。相关信息将显示在新窗口中。如果 Web 浏览器显示弹出窗口警告，请允许显示被阻止的内容。

在 “*System Log*”窗口中，您可以从下拉列表中选择特定的日志进行显示。单击 “**Refresh**”更新数据，或者单击 “**Clear**”擦除显示的所有信息。完成查看日志之后，请单击 “**Close**”关闭弹出窗口。

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**：单击此按钮可查看传出数据包信息。相关信息将显示在新窗口中。

在 “*Outgoing Log Table*”窗口中，您可以单击 “**Refresh**”更新数据。完成查看日志之后，请单击 “**Close**”关闭弹出窗口。

▪ **Incoming Log Table**：单击此按钮可显示传入数据包信息。相关信息将显示在新窗口中。如果 Web 浏览器显示弹出窗口警告，请允许显示被阻止的内容。

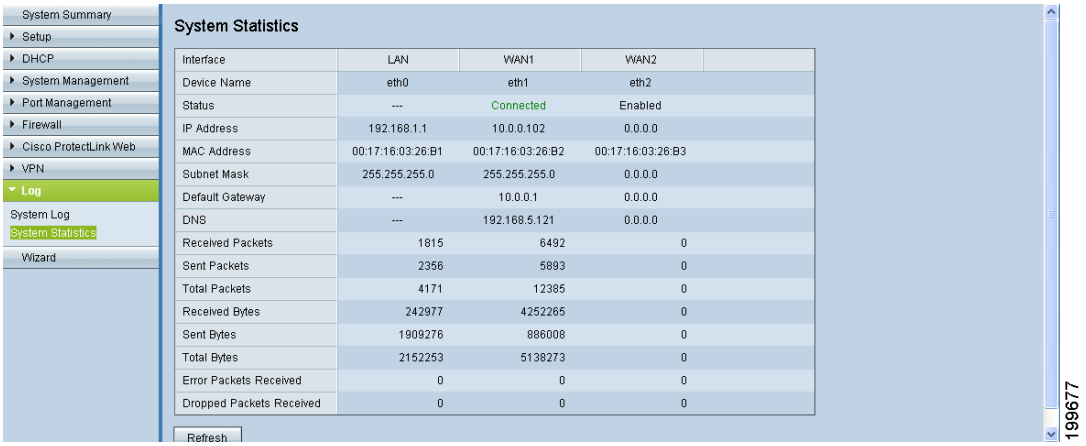
在 “*Incoming Log Table*”窗口中，您可以单击 “**Refresh**”更新数据。完成查看日志之后，请单击 “**Close**”关闭弹出窗口。

- **Clear Log Now**：单击此按钮可清除日志而不通过电子邮件发送。仅当您希望以后不再查看信息时，才可使用此按钮。

查看系统日志

使用 “*Log*” > “*System Log*”页面显示有关所有路由器端口 （LAN 和 WAN 端口）的统计信息。

打开此页面的步骤：在导航树中单击 “**Log**” > “**System Statistics**”。



Interface	LAN	WAN1	WAN2
Device Name	eth0	eth1	eth2
Status	---	Connected	Enabled
IP Address	192.168.1.1	10.0.0.102	0.0.0.0
MAC Address	00:17:16:03:26:B1	00:17:16:03:26:B2	00:17:16:03:26:B3
Subnet Mask	255.255.255.0	255.255.255.0	0.0.0.0
Default Gateway	---	10.0.0.1	0.0.0.0
DNS	---	192.168.5.121	0.0.0.0
Received Packets	1815	6492	0
Sent Packets	2356	5893	0
Total Packets	4171	12385	0
Received Bytes	242977	4252265	0
Sent Bytes	1909276	886008	0
Total Bytes	2152253	5138273	0
Error Packets Received	0	0	0
Dropped Packets Received	0	0	0

此时将显示每个接口 （例如， LAN、 WAN1、 WAN2 或 DMZ）的统计信息。您可以单击 “**Refresh**”更新数据。

对于每个端口，系统将会列出以下统计信息：

- **Device Name**：端口 ID，例如 eth0、 eth1、 eth2 等
- **Status**：端口状态。根据接口类型，状态可能为 “Connected、Disconnected”、“Enabled”或 “Disabled”。
- **IP Address**：接口的 IP 地址
- **MAC Address**：已连接设备的 MAC
- **Subnet Mask**：子网掩码
- **Default Gateway**：默认网关

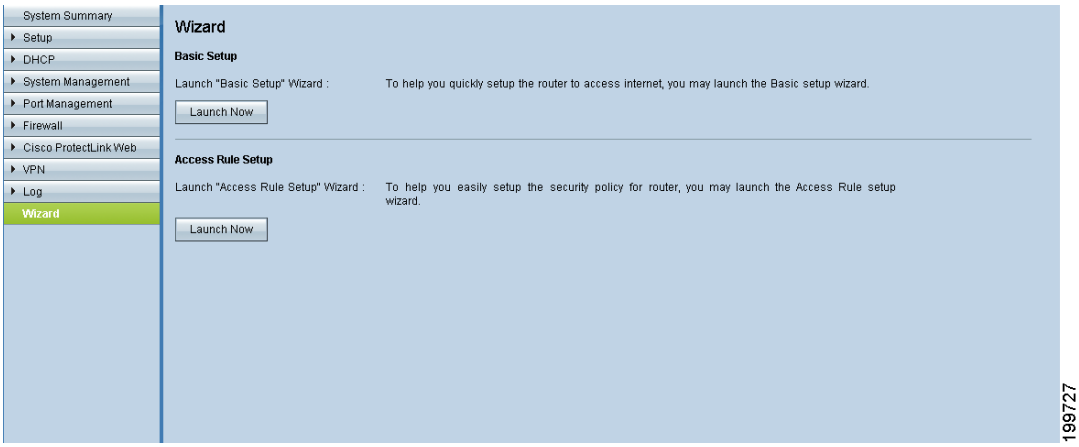
- **DNS**：用于 DNS 名称解析的 DNS 服务器
- **Received Packets**：通过此接口接收的数据包数量
- **Sent Packets**：通过此接口发送的数据包数量
- **Total Packets**：通过此接口发送和接收的数据包总数
- **Received Bytes**：通过此接口接收的字节数
- **Sent Bytes**：通过此接口发送的字节数
- **Total Bytes**：通过此接口发送和接收的总字节数
- **Error Packets Received**：通过此接口接收的错误数据包的数量
- **Dropped Packets Received**：已接收的由于错误校验和等问题而丢弃的数据包的数量。

11

向导

使用此选项卡访问基本设置向导和访问规则设置向导这两种设置向导。运行基本设置向导可更改 WAN 端口的数量或针对您的 Internet 连接设置路由器。运行访问规则设置向导可设置路由器的安全策略。

打开此页面的步骤：在导航树中单击 “**Wizard**”。或者，单击 “*System Summary*”页面上的 “**Setup Wizard**”。



该页面包括以下部分：

- **基本设置，页码 131**
- **访问规则设置，页码 131**

基本设置

使用基本设置向导更改 WAN 端口的数量或配置 Internet 连接。

单击 “**Launch Now**” 运行基本设置向导。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

使用访问规则设置向导创建防火墙访问规则。单击 “**Launch Now**” 运行访问规则设置向导。此向导提供了有关路由器默认规则的信息，可帮助您快速入门。按照屏幕上的说明继续操作。

A

故障排除

固件升级失败。

固件升级大约需要十分钟时间。如果您在固件升级过程中断开路由器的电源、按下 Reset 按钮、关闭“*System Management*”>“*Firmware Upgrade*”页面或断开计算机与路由器的连接，可能会出现错误。

如果固件升级失败，请使用配置实用程序的“*System Management*”>“*Firmware Upgrade*”页面重复固件升级流程。有关详细信息，请参阅**升级固件，页码 73**。

如果 Diag LED 继续闪烁，则代表固件映像已损坏。请使用 TFTP 实用程序升级固件。您可以从 www.cisco.com 下载 TFTP 实用程序。

您的计算机无法连接到 Internet。

请按照以下说明进行操作，直到您的计算机能够连接到 Internet：

- 确保路由器已接通电源。 System LED 应为绿色且不闪烁。
- 如果 System LED 闪烁，请断开所有网络设备 （包括调制解调器、路由器和计算机）的电源。然后按照**以下顺序**接通各设备的电源：
  - 电缆或 DSL 调制解调器
  - 路由器
  - 计算机
- 检查电缆连接情况。计算机应连接到路由器上编号为 1-4 的端口之一，而调制解调器必须连接到路由器上的 Internet 端口。

DSL 电话线无法接入路由器的 Internet 端口。

路由器不能代替调制解调器。要使用路由器，您仍然需要使用 DSL 调制解调器。将电话线连接到 DSL 调制解调器，再将安装 CD 插入计算机，然后按照屏幕上的说明进行操作。

路由器没有同轴端口用于电缆连接。

路由器不能代替调制解调器。要使用路由器，您仍然需要使用电缆调制解调器。将电缆连接到电缆调制解调器，再将安装 CD 插入计算机，然后按照屏幕上的说明进行操作。

B

用于 Windows 的 Cisco QuickVPN

客户端可使用 Cisco QuickVPN 访问您在此路由器上配置的客户端到网关隧道。请参阅以下主题：

- **简介，页码 134**
- **Cisco QuickVPN Client 安装和配置，页码 135**
- **使用 Cisco QuickVPN 软件，页码 135**

注意 有关配置流程的详细信息，请参阅**管理 VPN 用户和证书，页码 120**。

简介

Cisco RV0xx 系列 VPN 路由器支持 IPSec VPN 客户端软件，包括 Cisco QuickVPN 软件。要获取最新功能，请安装支持 Windows 7 的 QuickVPN Client 1.4.0.5 或更高版本。

此路由器最多可免费支持 50 个 Cisco QuickVPN 客户端。如果您的路由器最多仅支持十个客户端，请对其固件进行升级。

您可以在使用 VPN 客户端软件的计算机和 VPN 路由器之间创建 VPN 隧道。下面列举了计算机至 VPN 路由器 VPN 的一个示例。一位出差在外的女商人在酒店房间内连接到自己的 Internet 服务提供商 (ISP)。她的笔记本电脑中安装了 VPN 客户端软件，且已使用自己办公室的 VPN 设置对软件进行了配置。她可访问 VPN 客户端软件，并可连接至总公司的 VPN 路由器。由于 VPN 使用的是 Internet，因此距离不是问题。现在，通过使用 VPN，这位女商人可安全地连接至总公司的网络，就像进行了物理连接一样。

Cisco QuickVPN Client 安装和配置

对于每个 QuickVPN 客户端，请完成以下任务：

步骤 1 要下载 QuickVPN，请完成以下任务：

a. 启动 Web 浏览器，然后输入以下地址：www.cisco.com/go/software

b. 在 “Software Download Search”框中，输入：**QuickVPN**

c. 单击 “**Go**”。

d. 在搜索结果中，单击您的路由器所对应的链接。

e. 按照屏幕上的说明下载 QuickVPN 客户端。

步骤 2 要安装客户端证书，请将客户端证书保存至 QuickVPN 程序的安装目录中。
示例：C:\Program Files\Cisco Small Business\QuickVPN Client

注意：即使 PC 上没有安装证书， QuickVPN 也可以正常使用。用户将看到安全警告，但仍可以使用 QuickVPN，只是安全性不强。

使用 Cisco QuickVPN 软件

注意：作为可选操作，您可以在 PC 上安装 SSL 证书以提高安全性；如果未安装此证书，您仍可以使用 QuickVPN，但在此过程中将出现弹出警告。

对于每个 QuickVPN 客户端，请按照以下说明进行操作：

步骤 1 双击桌面上或系统托盘中的 Cisco QuickVPN 软件图标。

步骤 2 当显示 “*QuickVPN Login*”页面时，输入以下信息：

- **Profile Name**：输入配置文件的名称。
- **Username**：输入分配给您的用户名。
- **Password**：输入分配给您的密码。
- **Server Address**：输入远程路由器的 WAN IP 地址或域名。
- **Port for QuickVPN**：输入 QuickVPN 客户端将用于与远程 VPN 路由器进行通信的端口号，或者保留默认值 “**Auto**”。

- **Use Remote DNS Server**：如果启用此功能，则 QuickVPN 用户将使用远程 DNS 服务器 （由 QuickVPN 服务器提供），通过 QuickVPN 隧道解析远程子网中计算机的主机名。

步骤 3 要保存此配置文件，请单击 “**Save**”。

如果需要为多个站点创建通往这些站点的隧道，您可以创建多个配置文件，但请注意，一次只能有一条隧道处于活动状态。要删除此配置文件，请单击 “**Delete**”。要获取相关信息，请单击 “**Help**”。

步骤 4 要启动您的 QuickVPN 连接，请单击 “**Connect**”。系统显示连接进度的**顺序**如下：“*Connecting*”、“*Provisioning*”、“*Activating Policy*”以及 “*Verifying Network*”。

步骤 5 QuickVPN 连接建立后， QuickVPN 托盘图标将变为绿色，且系统将显示 “*QuickVPN Status*”页面。此页面将显示 VPN 隧道远程端的 IP 地址、 VPN 隧道启动的时间和日期以及 VPN 隧道处于活动状态的总持续时间。

步骤 6 要终止 VPN 隧道，请单击 “**Disconnect**”。

如果您单击 “Change Password”且有权更改自己的密码，系统将显示 “*Connect Virtual Private Connection*”页面。

- **Old Password**：输入您的密码。
- **New Password**：输入您的新密码。
- **Confirm New Password**：再次输入您的新密码。

步骤 7 单击 “**OK**”保存您的新密码。单击 “**Cancel**”取消更改。要获取相关信息，请单击 “**Help**”。

注意 只有在您的系统管理员授予您相应的权限后，您才能更改自己的密码。

C

网关到网关 VPN 隧道

综述

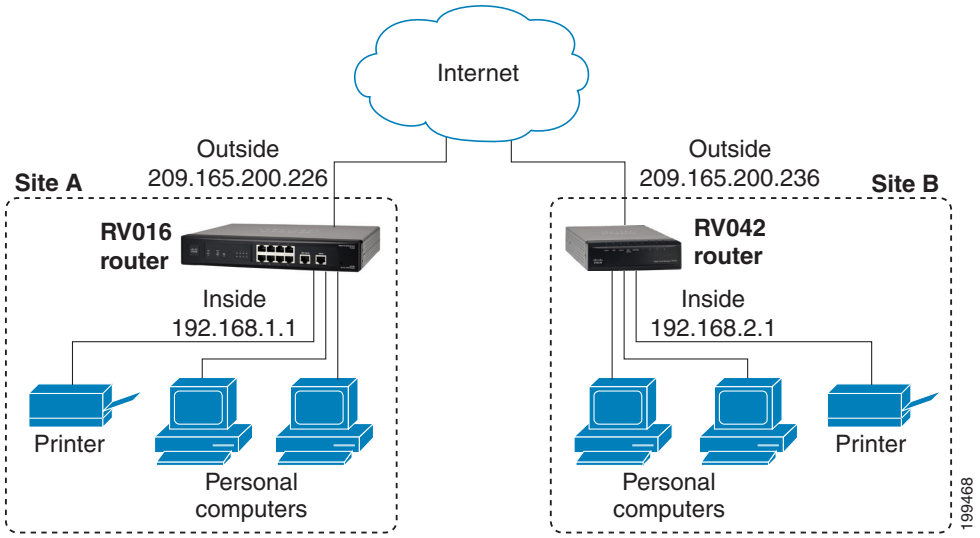
以下方案显示了如何在两个 VPN 路由器之间配置 IPSec VPN 隧道。我们使用两台计算机来测试隧道的活跃性。请参阅以下主题：

- 使用静态 IP 地址为远程网关进行配置，页码 137
- 使用动态 IP 地址为远程网关进行配置，页码 139

使用静态 IP 地址为远程网关进行配置

在此示例中，我们假设远程网关正使用某一静态 IP 地址。如果远程网关使用的是动态 IP 地址，则请参阅使用动态 IP 地址为远程网关进行配置，页码 139。

图 1 网关到网关 IPSec VPN 隧道 - 远程网关使用静态 IP



步骤 1 将 PC 连接到路由器 （站点 A），然后启动基于 Web 的配置实用程序。

步骤 2 在导航树中单击 “**VPN**” > “**Gateway to Gateway**”。

步骤 3 在 “*Tunnel Name*”字段中输入相应的名称。

步骤 4 选择相应的接口， **WAN1** 或 **WAN2**。

步骤 5 选中 “**Enable**”框。

步骤 6 在 “Local Security Gateway Type”字段中，请选择 “**IP Only**”。系统将自动检测站点 A 路由器的 WAN IP 地址。

在 “Local Security Group Type”字段中，请选择 “**Subnet**”。分别在 “*IP Address*”和 “*Subnet Mask*”字段中输入站点 A 路由器的本地网络设置。

步骤 7 在 “Remote Security Gateway Type”字段中，请选择 “**IP Only**”。在 “*IP Address*”字段中输入站点 B 路由器的 WAN IP 地址。

步骤 8 在 “Remote Security Group Type”字段中，请选择 “**Subnet**”。分别在 “*IP Address*”和 “*Subnet Mask*”字段中输入站点 B 路由器的本地网络设置。

步骤 9 在 “IPSec 设置”部分中，选择适当的加密、验证以及其他密钥管理设置。（这些设置应与站点 B 路由器的设置相匹配。）

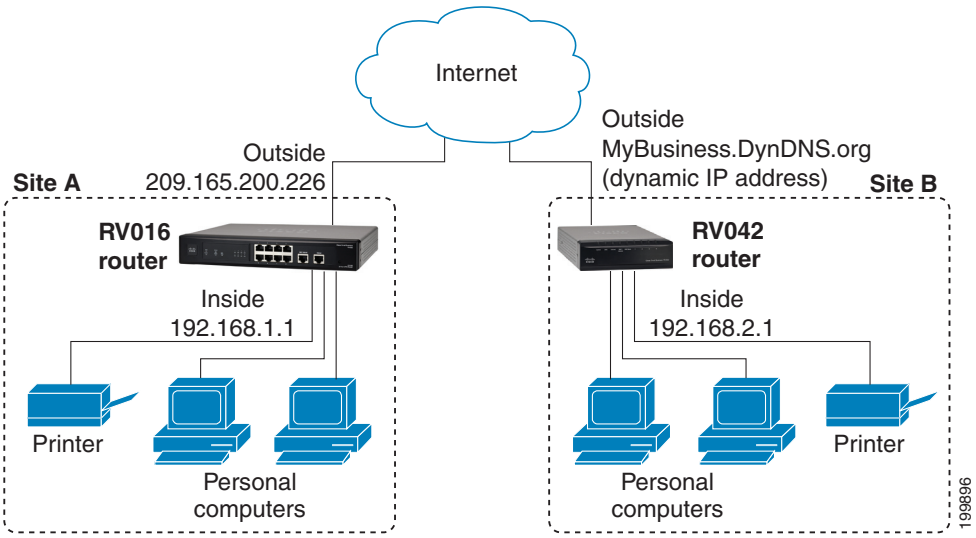
步骤 10 在 “*Preshared Key*”字段中，输入此密钥的字符串，例如 13572468。

步骤 11 如果您需要进行更为详细的设置，请单击 “**Advanced**”。否则，请单击 “**Save**”。

步骤 12 验证站点 A 和站点 B 的计算机是否能够相互连接 （有关详细信息，请参阅 Windows 帮助）。如果两台计算机能够相互连接，则表示 VPN 隧道的配置正确。

使用动态 IP 地址为远程网关进行配置

在此示例中，我们假设远程网关正使用某一动态 IP 地址，例如 MyBusiness.DynDNS.org。如果远程网关使用的是静态 IP 地址，则请参阅**使用静态 IP 地址为远程网关进行配置，页码 137**。



注意 每台计算机都必须安装网络适配器。在导航树中单击 “**VPN**” > “**Gateway to Gateway**”。

步骤 1 将 PC 连接到路由器 （站点 A），然后启动基于 Web 的配置实用程序。

步骤 2 在 “*Tunnel Name*” 字段中输入相应的名称。

步骤 3 选择相应的接口， **WAN1** 或 **WAN2**。

步骤 4 选中 “**Enable**”。

步骤 5 在 “Local Security Gateway Type” 字段中，请选择 “**IP Only**”。系统将自动检测站点 A 路由器的 WAN IP 地址。

步骤 6 在 “Local Security Group Type” 字段中，请选择 “**Subnet**”。分别在 “*IP Address*” 和 “*Subnet Mask*” 字段中输入站点 A 路由器的本地网络设置。

步骤 7 在 “Remote Security Gateway Type” 字段中，请选择 “**Dynamic IP + Domain Name (FQDN) Authentication**”，然后输入站点 B 路由器的域名。在此示例中，我们输入 MyBusiness.DynDNS.org。您也可以选择 “**Dynamic IP+ Email Address (User FQDN) Authentication**”，然后输入任意电子邮件地址。

步骤 8 在 “Remote Security Group Type” 字段中，请选择 “**Subnet**”。分别在 “*IP Address*” 和 “*Subnet Mask*” 字段中输入站点 B 路由器的本地网络设置。

步骤 9 在 “IPSec 设置” 部分中，选择适当的加密、验证以及其他密钥管理设置。（这些设置应与站点 B 路由器的设置相匹配。）

步骤 10 在 “*Preshared Key*” 字段中，输入此密钥的字符串，例如 13572468。

步骤 11 如果您需要进行更为详细的设置，请单击 “**Advanced**”。否则，请单击 “**Save**”。

步骤 12 验证站点 A 和站点 B 的计算机是否能够相互连接 （有关详细信息，请参阅 Windows 帮助）。如果两台计算机能够相互连接，则表示 VPN 隧道的配置正确。

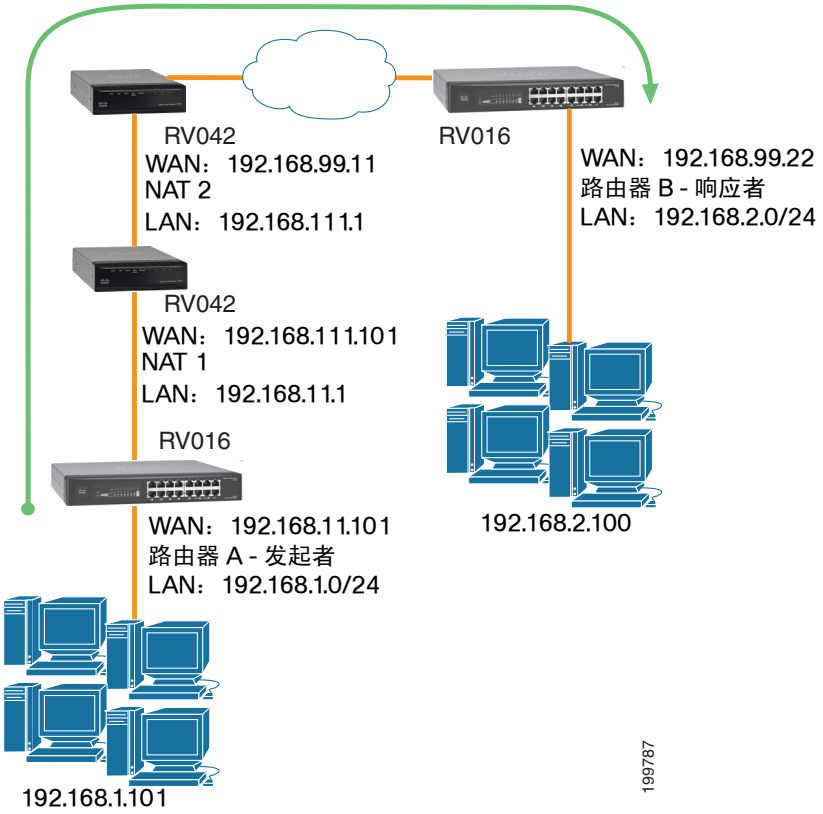
D

IPSec NAT 遍历

综述

网络地址转换 (NAT) 遍历技术可使受 IPSec 保护的数据通过 NAT。由于 IPSec 提供整个 IP 数据报的完整性，所以任何 IP 寻址更改都会使数据失效。为解决此问题， NAT 遍历会对入站数据报追加新的 IP 和 UDP 标头，以确保不对入站数据报流进行任何更改。

在以下方案中，路由器 A 会发出 IKE 协商，而路由器 B 为响应者。



注意 IPSec 发起者和响应者都必须支持检测路径中的 NAT 路由器并转到新端口的机制，如 RFC 3947 中所定义。

配置路由器 A

请按照以下说明配置路由器 A。

步骤 1 在已联网的计算机 （已指定为 PC 1）中启动 Web 浏览器。

步骤 2 访问路由器 A 的配置实用程序。

步骤 3 在导航树中单击 “**VPN**” > “**Gateway to Gateway**”。

步骤 4 在 “*Tunnel Name*”字段中输入相应的名称。

步骤 5 对于 “VPN Tunnel”设置，请选择 “**Enable**”。

步骤 6 在 “Local Security Gateway Type”字段中，请选择 “**IP Only**”。系统将自动检测路由器 A 的 WAN IP 地址。

在 “Local Security Group Type”字段中，请选择 “**Subnet**”。分别在 “*IP Address*”和 “*Subnet Mask*”字段中输入路由器 A 相应的本地网络设置。

步骤 7 在 “Remote Security Gateway Type”字段中，请选择 “**IP Only**”。在 “*IP Address*”字段中输入路由器 B 的 WAN IP 地址。

步骤 8 在 “Remote Security Group Type”字段中，请选择 “**Subnet**”。分别在 “*IP Address*”和 “*Subnet Mask*”字段中输入路由器 B 相应的本地网络设置。

步骤 9 在 “IPSec 设置”部分中，选择适当的加密、验证以及其他密钥管理设置。

步骤 10 在 “*Preshared Key*”字段中，输入此密钥的字符串，例如 13572468。

步骤 11 单击 “**Advanced Settings**”。

步骤 12 选中 “**NAT Traversal**”框以启用此功能。

步骤 13 单击 “**Save**”。

步骤 14 继续阅读下一部分内容：**配置路由器 B，页码 142**。

配置路由器 B

请按照以下说明配置路由器 B。

步骤 1 在已联网的计算机 （已指定为 PC 2）中启动 Web 浏览器。

步骤 2 访问路由器 B 的配置实用程序。

步骤 3 在导航树中单击 “**VPN**” > “**Gateway to Gateway**”。

步骤 4 在 “*Tunnel Name*”字段中输入相应的名称。

步骤 5 对于 “VPN Tunnel” 设置，请选择 “**Enable**”。

步骤 6 在 “Local Security Gateway Type” 字段中，请选择 “**IP Only**”。系统将自动检测路由器 B 的 WAN IP 地址。

在 “Local Security Group Type” 字段中，请选择 “**Subnet**”。分别在 “*IP Address*” 和 “*Subnet Mask*” 字段中输入路由器 B 相应的本地网络设置。

步骤 7 在 “Remote Security Gateway Type” 字段中，请选择 “**IP Only**”。在 “*IP Address*” 字段中输入 NAT 2 路由器的 WAN IP 地址。

步骤 8 在 “Remote Security Group Type” 字段中，请选择 “**Subnet**”。分别在 “*IP Address*” 和 “*Subnet Mask*” 字段中输入路由器 A 相应的本地网络设置。

步骤 9 在 “IPSec 设置” 部分中，选择适当的加密、验证以及其他密钥管理设置。

步骤 10 在 “*Preshared Key*” 字段中，输入此密钥的字符串，例如 13572468。

步骤 11 单击 “**Advanced Settings**”。

步骤 12 选中 “**NAT Traversal**” 框以启用此功能。

步骤 13 单击 “**Save**”。

E

带宽管理

本方案介绍了如何确保 Vonage IP 电话 (VoIP) 的服务质量 (QoS)。本示例使用的是 Vonage ；但类似说明同样适用于其他 VoIP 服务。请参阅以下主题：

- **创建新服务，页码 144**
- **创建新带宽管理规则，页码 145**

创建新服务

创建两个新服务，分别是 Vonage VoIP 和 Vonage 2。

步骤 1 访问 Vonage 网站 http://www.vonage.com。找到 Vonage VoIP 服务所使用的端口。

步骤 2 访问路由器的配置实用程序。

步骤 3 单击 “**System Management**” 选项卡。

步骤 4 在 “*Bandwidth Management*” 页面上，单击 “**Service Management**”。

步骤 5 在 “*Service Management*” 页面上的 “*Service Name*” 字段中，输入名称 （例如 Vonage VoIP）。

步骤 6 从 “*Protocol*” 下拉菜单中，选择 VoIP 服务所使用的协议。例如，某些 VoIP 设备使用的是 UDP。

步骤 7 在 “*Port Range*” 字段中输入其 SIP 端口范围。例如，您可以将 “Port Range” 设置为 5060 到 5070，以确保覆盖所有的活动端口。

步骤 8 单击 “**Add to List**”。

步骤 9 添加第二个服务。在 “*Service Name*” 字段中输入名称 （例如 Vonage 2）。

步骤 10 从 “*Protocol*” 下拉菜单中选择 **UDP**。

步骤 11 在 “*Port Range*” 字段中输入 RTP 端口范围。传入流量和传出流量都需要进行这些设置。例如，您可以将 “Port Range” 设置为 10000 到 25000，以确保覆盖所有的活动端口。

步骤 12 单击 “**Add to List**”。

步骤 13 单击 “**Save**”保存更改。

创建新带宽管理规则

创建以下四个新规则：Vonage VoIP （上行）、 Vonage VoIP （下行）、 Vonage 2 （上行）和 Vonage 2 （下行）。

步骤 1 为 Vonage 1 设置上行带宽规则的步骤：

a. 在 “*Bandwidth Management*”页面上，从 “*Service*”下拉菜单中选择 “**Vonage VoIP**”。

b. 输入您需要控制的 IP 地址或范围。要包括所有的内部 IP 地址，请保留默认值。

c. 从 “*Direction*”下拉菜单中，为出站流量选择 “**Upstream**”。

d. 在 “*Min. Rate*”字段中，输入所保证的带宽的最低速率。例如，您可以设置最低速率为 40 kbit/sec。

e. 在 “*Max. Rate*”字段中，输入所保证的带宽的最高速率。例如，您可以设置最高速率为 80 kbit/sec。

f. 选择 “**Enable**”以启用此规则。

g. 规则设置完成后，请单击 “**Add to list**”。

步骤 2 为 Vonage 1 设置下行带宽规则的步骤：

a. 从 “*Service*”下拉菜单中选择 “**Vonage VoIP**”。

b. 输入您需要控制的 IP 地址或范围。要包括所有的内部 IP 地址，请保留默认值。

c. 从 “*Direction*”下拉菜单中，为入站流量选择 “**Downstream**”。

d. 在 “*Min. Rate*”字段中，输入所保证的带宽的最低速率。例如，您可以设置最低速率为 40 kbit/sec。

e. 在 “*Max. Rate*”字段中，输入所保证的带宽的最高速率。例如，您可以设置最高速率为 80 kbit/sec。

f. 选择 “**Enable**”以启用此规则。

g. 规则设置完成后，请单击 “**Add to list**”。

步骤 3 为 Vonage 2 设置上行规则。

a. 从 “*Service*”下拉菜单中选择 “**Vonage 2**”。

b. 输入您需要控制的 IP 地址或范围。要包括所有的内部 IP 地址，请保留默认值 **0**。

c. 从 “*Direction*”下拉菜单中，为出站流量选择 “**Upstream**”。

d. 在 “*Min. Rate*”字段中，输入所保证的带宽的最低速率。例如，您可以设置最低速率为 40 kbit/sec。

e. 在 “*Max. Rate*”字段中，输入所保证的带宽的最高速率。例如，您可以设置最高速率为 80 kbit/sec。

f. 选择 “**Enable**”以启用此规则。

g. 规则设置完成后，请单击 “**Add to list**”。

步骤 4 为 Vonage 2 设置下行规则。

a. 从 “*Service*”下拉菜单中选择 “**Vonage 2**”。

b. 输入您需要控制的 IP 地址或范围。要包括所有的内部 IP 地址，请保留默认值 **0**。

c. 从 “*Direction*”下拉菜单中，为入站流量选择 “**Downstream**”。

d. 在 “*Min. Rate*”字段中，输入所保证的带宽的最低速率。例如，您可以设置最低速率为 40 kbit/sec。

e. 在 “*Max. Rate*”字段中，输入所保证的带宽的最高速率。例如，您可以设置最高速率为 80 kbit/sec。

f. 选择 “**Enable**”以启用此规则。

g. 规则设置完成后，请单击 “**Add to list**”。

步骤 5 单击 “**Save**”。

F

规格

注意 各种规格如有更改恕不另行通知。

RV042

规格	
型号	Cisco RV042
标准	IEEE 802.3、 802.3u
端口	4 个 10/100 RJ-45 端口， 1 个 10/100 RJ-45 Internet 端口， 1 个 10/100 RJ-45 DMZ/Internet 端口
按钮	Reset
电缆类型	5 类以太网
LED	System、Internet、DMZ/Internet、DMZ Mode、Diag 和 1-4
操作系统	Linux
性能	
NAT 吞吐量	100 Mbps
IPSec 吞吐量	59 Mbps
安全性	
防火墙	SPI 防火墙
访问规则	最多 50 个条目
端口转发	最多 30 个条目

端口触发	最多 30 个条目
URL 过滤	按域或关键字排列的静态列表 （已附带），通过 Cisco ProtectLink Web 服务进行动态过滤 （可选）

网络

双 WAN	可配置用于 Smartlink 备份或负载平衡
协议绑定	协议可以绑定到负载平衡条件下的特定 WAN 端口
DHCP	DHCP 服务器， DHCP 客户端
DNS	DNS 代理，动态 DNS （DynDNS、 3322）
NAT	多对一，一对一
DMZ	DMZ 端口， DMZ 主机
路由	静态和 RIP v1、 v2

QoS

基于端口的 QoS	可为每个 LAN 端口配置
基于服务的 QoS	支持速率控制或优先级
速率控制	每个服务都可配置上行 / 下行带宽
优先级	每个服务可映射至 3 种优先级之一

VPN

IPSec 用于连接分公司的 50 条 IPSec 隧道

QuickVPN	用于进行远程客户端访问的 50 位 QuickVPN 用户
PPTP	支持 5 个 PPTP 客户端的内置 PPTP 服务器
加密	DES、 3DES、 AES-128、 AES-192 和 AES-256
验证	MD5、 SHA1
IPSec NAT-T	支持网关到网关和客户端到网关隧道
VPN 通道	PPTP、 L2TP、 IPSec

管理

基于 Web	HTTPS
SNMP	支持 SNMP v1 和 v2c

日志	Syslog，电子邮件警报
环境	
尺寸	5.12" x 1.52" x 7.87" 宽 x 高 x 深 （130 x 38.5 x 200 毫米）
单位重量	1.27 磅 （0.576 千克）
电源	12V， 1A
认证	FCC B 类， CE B 类
操作温度	0oC 至 40oC （32oF 至 104oF）
存储温度	0oC 至 70oC （32oF 至 158oF）
操作湿度	10% 至 85%，无冷凝
存储湿度	5% 至 90%，无冷凝

Cisco RV082

规格	
型号	Cisco RV082 10/100 8 端口 VPN 路由器
标准	IEEE 802.3、 802.3u
端口	8 个 10/100 RJ-45 端口， 1 个 10/100 RJ-45 Internet 端口， 1 个 10/100 RJ-45 DMZ/Internet 端口
按钮	Reset
电缆类型	5 类以太网
LED	System、Internet、DMZ/Internet、DMZ Mode、Diag 和 1-8
安全功能	SPI 防火墙、 DES、 3DES 和 IPSec VPN 隧道 AES 加密
操作系统	Linux
性能	
NAT 吞吐量	200 Mbps
IPSec 吞吐量	97 Mbps

安全性	
防火墙	SPI 防火墙
DoS 预防	阻止多种拒绝服务攻击
访问规则	最多 50 个条目
端口转发	最多 30 个条目
端口触发	最多 30 个条目
阻止	Java、 Cookies、 ActiveX 和 HTTP 代理
URL 过滤	按域或关键字排列的静态列表 （已附带），通过 Cisco ProtectLink Web 服务进行动态过滤 （可选）
网络	
双 WAN	可配置用于 Smartlink 备份或负载平衡
WAN 类型	DHCP、静态 IP、 PPPoE、 PPTP、动态 DNS
协议绑定	协议可以绑定到负载平衡条件下的特定 WAN 端口
DHCP	DHCP 服务器、 DHCP 客户端、 DHCP 中继
DNS	DNS 代理，动态 DNS （DynDNS、 3322）
NAT	多对一，一对一
DMZ	DMZ 端口， DMZ 主机
路由	静态和 RIP v1、 v2
QoS	
基于端口的 QoS	可为每个 LAN 端口配置
基于服务的 QoS	支持速率控制或优先级
速率控制	每个服务都可配置上行 / 下行带宽
优先级	每个服务可映射至 3 种优先级之一
VPN	
IPSec	用于连接分公司的 100 条 IPSec 隧道
QuickVPN	用于进行远程客户端访问的 50 位 QuickVPN 用户
PPTP	支持 5 个 PPTP 客户端的内置 PPTP 服务器

加密	DES、 3DES、 AES-128、 AES-192 和 AES-256
验证	MD5、 SHA1
IKE	支持 Internet 密钥交换
IPSec NAT-T	支持网关到网关和客户端到网关隧道
高级选项	DPD、 Split DNS 和 VPN Backup
VPN 通道	PPTP、 L2TP、 IPSec
管理	
基于 Web	HTTPS
SNMP	支持 SNMP v1 和 v2c
日志	Syslog、电子邮件警报、 VPN 隧道、状态监控
环境	
尺寸	11.00" x 1.75" x 9.50" 宽 x 高 x 深 （279.4 x 44.45 x 241.3 毫米）
单位重量	3.25 磅 （1.475 千克）
电源	交流 100~240 V， 50~60 Hz
认证	FCC B 类， CE A 类
操作温度	0 °C 至 40 °C （32 °F 至 104 °F）
存储温度	0 °C 至 70 °C （32 °F 至 158 °F）
操作湿度	10% 至 85%，无冷凝
存储湿度	5% 至 90%，无冷凝

Cisco RV016

规格	
型号	Cisco RV016 10/100 16 端口 VPN 路由器
标准	IEEE 802.3、 802.3u
端口	16 个 10/100 RJ-45 端口，包括 2 个 Internet 端口，1 个 DMZ 端口，8 个 LAN 端口，以及 5 个可配置的 Internet/LAN 端口

按钮	Reset
电缆类型	5 类以太网
LED	Diag、 System、 LAN/Act 1-13、 Internet/Act 1-7 和 DMZ
操作系统	Linux
性能	
NAT 吞吐量	200 Mbps
IPSec 吞吐量	97 Mbps
安全性	
防火墙	SPI 防火墙
DoS 预防	阻止多种拒绝服务攻击
访问规则	最多 50 个条目
端口转发	最多 30 个条目
端口触发	最多 30 个条目
URL 过滤	按域或关键字排列的静态列表 （已附带），通过 Cisco ProtectLink Web 服务进行动态过滤 （可选）
网络	
多 WAN	最多支持 7 个具有负载平衡的 WAN 端口，其中某些 WAN 端口可以专用于指定的 IP 范围和服务
WAN 类型	DHCP、静态 IP、 PPPoE、 PPTP、动态 DNS
协议绑定	协议可以绑定到特定 WAN 端口
DHCP	DHCP 服务器， DHCP 客户端
DNS	DNS 代理，动态 DNS （DynDNS、 3322）
NAT	多对一，一对一
DMZ	DMZ 端口， DMZ 主机
路由	静态和 RIP v1、 v2
QoS	
基于端口的 QoS	可为每个 LAN 端口配置

基于服务的 QoS	支持速率控制或优先级
速率控制	每个服务都可配置上行 / 下行带宽
优先级	每个服务可映射至 3 种优先级之一
VPN	
IPSec	用于连接分公司的 100 条 IPSec 隧道
QuickVPN	用于进行远程客户端访问的 50 位 QuickVPN 用户
PPTP	支持 10 个 PPTP 客户端的内置 PPTP 服务器
加密	DES、 3DES、 AES-128、 AES-192 和 AES-256
验证	MD5、 SHA1
IKE	支持 Internet 密钥交换
IPSec NAT-T	支持网关到网关和客户端到网关隧道
失效对等体检测	支持 DPD
VPN 通道	PPTP、 L2TP、 IPSec
管理	
基于 Web	HTTPS
SNMP	支持 SNMP v1 和 v2c
日志	Syslog、电子邮件警报、 VPN 隧道、状态监控
环境	
尺寸	11.00" x 1.75" x 9.50" 宽 x 高 x 深（279.4 x 44.45 x 241.3 毫米）
单位重量	3.25 磅 （1.475 千克）
电源	交流 100~240 V， 50-60 Hz
认证	FCC B 类， CE A 类
操作温度	0 °C 至 40 °C （32 °F 至 104 °F）
存储温度	0 °C 至 70 °C （32 °F 至 158 °F）
操作湿度	10% 至 85%，无冷凝
存储湿度	5% 至 90%，无冷凝

G

快速索引

思科提供了大量的资源来帮助您和您的客户尽享思科精睿 (Cisco Small Business) 路由器所带来的所有优势。

支持	
思科精睿 (Cisco Small Business) 支持社区	www.cisco.com/go/smallbizsupport
思科精睿 (Cisco Small Business) 支持和资源	www.cisco.com/go/smallbizhelp
电话支持联系人	www.cisco.com/go/sbsc
思科精睿 (Cisco Small Business) 固件下载	www.cisco.com/go/software
产品文档	
思科精睿 (Cisco Small Business) 路由器	www.cisco.com/go/smallbizrouters
思科精睿 (Cisco Small Business)	
思科精睿产品渠道合作伙伴中心 （需要合作伙伴登录）	www.cisco.com/web/partners/sell/smb
思科精睿 (Cisco Small Business) 首页	www.cisco.com/smb