Cisco SDM Express 用户指南

公司总部
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
电话：408 526-4000
800 553-NETS (6387)
传真：408 526-4100

客户订单号：
文本部件号：OL-7141-04

本手册中与产品相关的规范和信息如有更改，恕不另行通知。本手册中的所有声明、信息和建议据信准确无误，但不含任何形式的明示或暗示担保。用户必须对任何产品的应用负全责。

产品随附的软件许可和有限担保在随产品装运的信息包中进行了阐述，并作为此参考的一部分。如果无法找到软件许可或有限担保，请与您的 CISCO 代表联系索要副本。

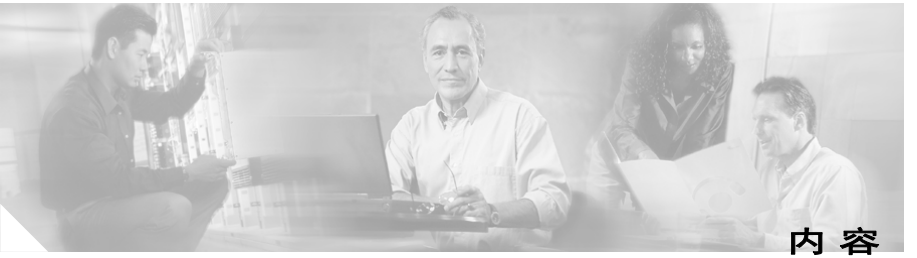
Cisco 实现的 TCP 报头压缩改编自 University of California, Berkeley (UCB) 开发的、作为 UNIX 操作系统的 UCB 公用域版本组成部分的程序。保留所有权利。版权所有 © 1981，University of California 董事。

尽管此处可能涉及任何其它担保，但这些供应商的所有文档文件和软件将按“原样”（不排除带有各种问题）提供。CISCO 及以上提及的供应商拒绝进行所有明示或暗示担保，包括但不限于适销性、特殊目的适用性及非侵权的担保，或因交易习惯或贸易惯例而引起的各种争端。

任何情况下，即便 CISCO 或其供应商已被告知以下损害的可能性，CISCO 或其供应商对任何直接、特殊、间接或意外损害也均不负责，包括但不限于因使用或不能使用本手册造成的利润损失或者数据的丢失或损毁。

本文档中使用的任何 Internet 协议 (IP) 地址并不表示实际地址。文档中包含的任何示例、命令显示输出以及图示仅用于演示目的。演示内容中用到的任何实际 IP 地址纯属无意和巧合。

Cisco SDM Express 用户指南



章 1

Cisco SDM Express

Cisco SDM Express 窗口将指导您对路由器进行基本配置。在完成基本配置之后，路由器将在 LAN 上可用，建立 WAN 连接，并具有防火墙功能。

欢迎

此向导引导您完成基本配置，帮助您执行下列操作：

- 命名路由器。
- 指定用户名和密码。
- 可使用 Cisco SDM Express 向导手动配置路由器，或者用从 USB 标记或 USB 闪存设备加载的配置文件、安全设备配置 (SDP) 或 Cisco 网络服务进行配置（如果您的 Cisco IOS 版本支持这些功能）。

  如果使用 Cisco 网络服务配置路由器，则可以提供 Cisco 网络服务参数使路由器与 Cisco 网络服务服务器进行通信并获取配置。
- 更改出厂默认的 LAN IP 地址。

  如果选择 SDP 或 Cisco 网络服务配置路由器，则可跳过此任务。
- 为 LAN 创建 DHCP 地址池。

  如果选择 SDP 或 Cisco 网络服务配置路由器，则可跳过此任务。
- 确定 DNS 服务器以及组织域名。请联系网络管理员或 Internet 服务提供商获取这些信息。

  如果选择 SDP 或 Cisco 网络服务配置路由器，则可跳过此任务。
- 创建 WAN 连接。

- 为 LAN 和 WAN 连接创建防火墙。
- 进行能够增强网络性能及安全的设置。

若要配置其它接口，以及进行更高级的配置设置，请使用 Cisco 路由器和安全设备管理器 (Cisco SDM)。有关详细信息，请参阅 Cisco 路由器和安全设备管理器。

基本配置

“基本配置”窗口可用于命名您正在配置的路由器、输入组织的域名，以及控制对 Cisco SDM Express、Cisco 路由器和安全设备管理器以及 CLI 的访问。

主机名字段

输入要赋予路由器的名称。

域名字段

输入您的组织的域名。*cisco.com* 是一个域名示例，但您的域名可能以其它后缀结束，如 *.org* 或 *.net*。

用户名和密码字段

必须为 Cisco SDM Express 用户和远程登录用户设置用户名和密码。

备注 在您下次及其后使用 Cisco SDM Express 时，您将使用在此窗口中设置的用户名和密码，除非您更改它们。使密码难以猜测但易于记忆。

用户名字段

在此字段中输入用户名。

输入新密码字段

在此字段中输入新密码。密码必须至少 6 个字符。

重新输入新密码字段

重新输入新密码以进行确认。

启用加密密码字段

启用加密密码可控制通过远程登录或控制台端口访问路由器的用户对特权 EXEC 模式的访问。在特权 EXEC 模式下，用户可进行配置更改，并且可访问此模式之外不可用的其它命令。必须在**输入密码**字段中输入启用加密密码，然后在**重新输入密码**字段中再次输入该密码以进行确认。密码必须为 6 个字符或更多。

备注 请选择您可以记住但其他人难以猜测的启用加密密码。不能通过查看配置文件来读取该密码，因为它是以加密形式进行存储的。

路由器配置

此窗口列出了可用于配置路由器的选项。其中的某些选项只有在您的 Cisco IOS 版本支持该选项的情况下才会出现。

SDM Express

选择此选项以使用 Cisco SDM Express 手动配置路由器。

USB 标记或 USB 闪存

如果有 USB 标记或 USB 闪存设备连接在路由器上，并且其中包含相应的配置文件，则选择此选项。

备注 如果 USB 标记和 USB 闪存设备同时连接到路由器上，则 Cisco SDM Express 将使用 USB 标记。如果要使用连接到路由器上的 USB 闪存设备，则在运行 Cisco SDM Express 之前，必须从路由器上卸下所有 USB 标记。

安全设备配置

如果网络管理员为您提供了通过 SDP 配置路由器的信息，则选择“安全设备配置 (SDP)”。

在选择 SDP 选项之前，请确保以下几点：

- 路由器和 SDP 服务器之间存在 IP 连接。
- 您的 Web 浏览器支持 JavaScript。

如果选择 SDP，则在您完成 Cisco SDM Express 向导之后，新的浏览器窗口将自动打开。新的浏览器窗口中包含一个向导，它将指导您通过 SDP 配置路由器。

有关 SDP 的更多信息，请访问

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008028afbd.html#wp1043332

CNS 服务器

如果您的服务提供商提供了 Cisco 网络服务服务器信息，则选择此选项。有关详细信息，请单击 Cisco 网络服务。

自 USB 标记提供

通过该窗口可以向路由器提供自连接至路由器的 USB 标记加载的 CCCD 配置文件。CCCD 文件是启动配置文件，可以使用 TMS 软件将其加载至 USB 标记上。

备注 仅当将 USB 标记连接至路由器时，该窗口才会显示。如果 USB 标记和 USB 闪存设备同时连接到路由器上，则 Cisco SDM Express 将使用 USB 标记。如果要使用连接到路由器上的 USB 闪存设备，则在运行 Cisco SDM Express 之前，必须从路由器上卸下所有 USB 标记。

向路由器提供 CCCD 配置文件时，该文件与正在运行的配置相融，同时也成为启动配置的一部分。

小心 Cisco SDM 不会检查用于配置路由器的配置文件的有效性。确保预计使用的配置文件的内容含有相应设置。

如要自 USB 标记向路由器提供文件，采取如下步骤：

步骤 1 从**标记名称**下拉菜单中选择 USB 标记名称。

步骤 2 如果*不*想使用默认 PIN 登录到 USB 标记，则选择**指定设备和 PIN**，并在“标记 PIN”字段中输入一个 PIN。

如果选择**指定设备和默认 PIN**，则默认 PIN 1234567890 将用于登录到 USB 标记。

步骤 3 单击**登录**登录到 USB 标记。

如果无法登录到 USB 标记，则路由器可能无法从 USB 标记进行配置。单击**返回**按钮并选择其它方法配置路由器。

步骤 4 单击**预览 CCCD** 以在下部窗格中显示文件内容。

自 USB 闪存供应

通过该窗口可以向路由器提供自连接至路由器的 USB 闪存设备加载的配置文件。仅当将 USB 闪存设备连接至路由器时，该窗口才会显示。

向路由器提供配置文件时，该文件与正在运行的配置相融，同时也成为启动配置的一部分。

小心 Cisco SDM 不会检查用于配置路由器的配置文件的有效性。确保预计使用的配置文件的内容含有相应数据。

如要自 USB 闪存设备向路由器提供文件，采取如下步骤：

步骤 1 在“文件名”字段中输入配置文件的名称（完整路径），或单击**浏览**打开文件选择窗口。

文件必须具备 .cfg 扩展名，或者文件名必须为 CCCD 文件。CCCD 文件是启动配置文件。

步骤 2 单击**预览文件**以在下部窗格中显示文件内容。

文件选择

通过此窗口可以自路由器加载文件。在此窗口中仅可以查看 DOSFS 文件系统。

窗口的左侧显示代表 Cisco 路由器闪存和连接至路由器上的 USB 设备的目录系统的可扩展树。

窗口右侧显示了一个文件和目录名称的列表，这些文件和目录是在窗口左侧中指定的目录下找到的。同样显示每个文件的大小，以字节为单位，以及最近一次修改每个文件和目录的日期和时间。

可以选择将某一文件加载至窗口右侧的列表中。文件列表下面是“文件名”字段，其中包含指定文件的完整路径。

备注 如果选择向路由器提供配置文件，文件必须为 CCCD 文件或者具备 .cfg 扩展名。

名称

单击**名称**以按名称字母顺序对文件和目录进行排序。再次单击**名称**将使排序顺序反向。

大小

单击**大小**以根据大小对文件和目录进行排序。目录大小总为零字节，即使它们并不是空的。再次单击**大小**将使排序顺序反向。

修改的时间

单击**修改的时间**以根据修改日期和时间对文件和目录进行排序。再次单击**修改的时间**将使排序顺序反向。

无线接口配置

若要配置路由器无线接口，则单击**是**。Cisco SDM Express 将配置路由器以将无线通信桥接到 LAN 接口。如果不想配置无线接口，则单击**否**。如果单击**否**，仍可以配置 LAN 接口设置。

Cisco SDM Express 可用于配置一个无线接口。如果路由器上还有其它无线接口，则使用无线应用程序配置它们。

LAN 接口配置

通过该窗口可以配置 LAN 以太网接口 IP 地址和子网信息。

如果在完成 Cisco SDM Express 向导后需要更改 LAN 以太网接口的 IP 地址和子网信息，则可以再次启动 Cisco SDM Express，单击 LAN 并根据需要编辑地址，如此即可。

接口 / 桥接接口列表

如果路由器有多个 LAN 接口，则接口会显示在该列表中。选择您要配置的 LAN 接口。

如果路由器有无线接口，并且您在“无线接口配置”窗口中单击**是**，则此列表将标为“桥接接口”。选择您要桥接无线通信的接口。

IP 地址字段

以点分十进制格式输入 LAN 接口的 IP 地址。如果要使用“网络地址转换”(NAT) 或“端口地址转换”(PAT)，则此项可以是一个专用 IP 地址。

备注 请记录此地址。完成 Cisco SDM Express 向导并重新启动路由器之后，应使用此地址运行 Cisco SDM Express。请不要使用在路由器的《快速入门指南》(Quick Start Guide) 中提供的地址。

子网掩码字段

请输入网络的子网掩码。请从网络管理员或服务提供商那里获取该值。子网掩码使路由器能够确定以上 IP 地址的多少位是用于定义该地址的网络和子网部分的。通过该子网掩码值还可确定此路由器连接到的 LAN 中可以拥有的主机数。

子网位数字段

或者，也可以输入用于定义 IP 地址的网络和子网部分的位数。您的网络管理员或服务提供商可能会以此形式提供子网掩码信息。

无线参数字段

在初始配置时，如果路由器具有无线接口，并且在**无线接口配置**窗口单击“是”，则会显示这些字段。如果您是在编辑配置，则在初始配置期间进行无线设置时，会显示这些字段。无线通信会桥接到该 LAN 接口。

请输入该无线通信的“服务集标识符”(SSID)。SSID 是无线网络设备用来建立并保持无线连接的唯一标识符。

备注 更改已配置的 SSID 值会断开无线连接。

如果您在完成 Cisco SDM Express 向导之后编辑 LAN 配置，并且想配置高级无线参数，则单击分类栏中的**无线**。

“刷新”、“应用更改”、“放弃更改”按钮

如果您正在编辑初始配置，则这些按钮将可见。有关详细信息，请单击 Cisco SDM Express 按钮。

DHCP 服务器配置

动态主机配置协议 (DHCP) 是一种简单的寻址形式，它在无需使用静态寻址以及无需使用特定服务的端口号的情况下使用。DHCP 在主机登录到网络上时动态为其分配一个 IP 地址，并且在其注销时收回该地址。这样，将能够重新使用主机不再使用的地址。使用 DHCP 可为您的内部网络上的资源（如 PC）分配地址。

“在 LAN 接口上启动 DHCP 服务器”复选框

选中此项以允许路由器为 LAN 上的设备分配专用 IP 地址。在此窗口中启用此选项后，DHCP 服务器会将 IP 地址租借给主机一天时间。如果选中了此复选框，则必须在“起始 IP 地址”和“结束 IP 地址”字段中输入值。

起始 IP 地址字段

根据您为 LAN 接口指定的 IP 地址和子网掩码，Cisco SDM Express 将在此字段中输入 IP 地址范围中的最小地址。如果想使 DHCP 地址池的范围更小，您可以将此值更改为较大的地址值，但是您必须输入与 LAN 接口地址处于同一子网中的地址，否则 Cisco SDM Express 显示一则消息通知您该地址无效。

结束 IP 地址字段

根据您为 LAN 接口指定的 IP 地址和子网掩码，Cisco SDM Express 将在此字段中输入 IP 地址范围的最高有效地址。如果想使 DHCP 地址池的范围更小，您可以将此值更改为更小的地址值，但是您必须输入与 LAN 接口地址处于同一子网中的地址，否则 Cisco SDM Express 显示一则消息通知您该地址无效。

域名字段

在完成初始配置之后可见。可以输入您的组织的域名。*cisco.com* 是一个域名示例，但您的域名可能以其它后缀结束，如 *.org* 或 *.net*。

“将所有 DHCP 选项参数导入 DHCP 服务器数据库”复选框

在完成初始配置之后可见。如果要将 DHCP 选项参数导入 DHCP 服务器数据库，并在 LAN 上的 DHCP 客户端请求 IP 地址时将这些信息发送给这些客户端，则选中此选项。

主域名服务器字段

输入路由器将使用的主 DNS 服务器的 IP 地址。您的网络管理员或服务提供商将为您提供该 IP 地址。

主 DNS 服务器是路由器尝试解析 IP 地址时首先连接的服务器。

辅助域名服务器字段

输入路由器将使用的辅助 DNS 服务器的 IP 地址（如果有）。您的网络管理员或服务提供商将为您提供该 IP 地址。

辅助 DNS 服务器是在主服务器不可用时路由器将连接的服务器。

“为 DHCP 客户端使用这些 DNS 值”复选框

在 LAN 接口上启用了 DHCP 服务器时可用。如果希望路由器 DHCP 客户端能够使用您在此窗口中输入其 IP 地址的 DNS 服务器，则选择此项。

“刷新”、“应用更改”、“放弃更改”按钮

如果您正在编辑初始配置，则这些按钮将可见。有关详细信息，请单击 Cisco SDM Express 按钮。

Internet (WAN)：以太网接口

使用此窗口配置以太网 WAN 接口。

“启用 PPPoE”复选框

如果您的服务提供商要求路由器使用 PPPoE，则选中此项以启用 PPPoE 封装。如果服务提供商不使用 PPPoE，则不选此选项。如果路由器运行的是不支持 PPPoE 封装的 Cisco IOS 版本，则此复选框将不可用。

地址类型列表

选择下列其中一项：

静态 IP 地址选项

如果选择静态 IP 地址，则在提供的字段中输入 IP 地址和子网掩码或子网位数。

动态（DHCP 客户端）选项

如果选择动态，则路由器将从远程 DHCP 服务器租用 IP 地址。输入将分配地址的 DHCP 服务器的名称。

未编号的 IP 选项

如果希望接口共享已经分配给其它接口的 IP 地址，请选择**未编号的 IP**。然后，选择希望当前配置的接口将使用其 IP 地址的接口。如果未选择“启用 PPPoE”，则此选项不可用。

Easy IP (经过协商的 IP)

如果路由器将通过 PPP/IPCP 地址协商获得 IP 地址，则选择 **Easy IP（经过协商的 IP）**。如果未选择“启用 PPPoE”，则此选项不可用。

“验证类型”复选框

选中服务提供商使用的验证类型所属框。如果不知道服务提供商使用哪种验证类型，可以选中这两个框：路由器将尝试上述两种验证类型，从而其中一次尝试将获得成功。

CHAP 验证比 PAP 验证更安全。

用户名字段

由 Internet 服务提供商或网络管理员提供，并用作 CHAP 和 / 或 PAP 验证的用户名。

密码字段

请输入由您的服务提供商提供的完全相同的密码。密码区分大小写。例如，密码“test”不同于“Test”。

确认密码字段

将您在前一框中输入的密码再重新输入一次。

“刷新”、“应用更改”、“放弃更改”按钮

如果您正在编辑初始配置，则这些按钮将可见。有关详细信息，请单击 Cisco SDM Express 按钮。

Internet (WAN)：自动检测封装

Cisco SDM Express 支持 SB 106、SB 107、Cisco 836 和 Cisco 837 路由器的自动检测。但是，如果您配置的是运行 Cisco IOS 12.3(8)T 或 12.3(8.3)T 版的 Cisco 837 路由器，则不支持自动检测功能。

单击**自动检测按钮**以使 Cisco SDM Express 发现封装类型。如果 Cisco SDM Express 查找成功，它将自动应用找到的封装类型和其它配置参数。

如果 Cisco SDM Express 无法检测封装类型，必须通过单击**用户指定**指定封装和验证类型。

状态图标和启用或禁用按钮

在您使用 Cisco SDM Express 编辑初始配置时，状态图标将显示。向上箭头图标表示接口已启动。向下箭头图标表示接口已停用。

在您使用 Cisco SDM Express 编辑初始配置时，**启用**或**禁用**按钮可用。如果选择的接口已启用，则可以使用**禁用**按钮关闭该接口。如果选择的接口已关闭，则可以使用**启用**按钮启用该接口。

Internet (WAN)：用户指定封装

在指定封装时，使用此窗口配置 WAN 接口。

状态图标和启用或禁用按钮

在您使用 Cisco SDM Express 编辑初始配置时，状态图标将显示。向上箭头图标表示接口已启动。向下箭头图标表示接口已停用。

在您使用 Cisco SDM Express 编辑初始配置时，**启用**或**禁用**按钮可用。如果选择的接口已启用，则可以使用**禁用**按钮关闭该接口。如果选择的接口已关闭，则可以使用**启用**按钮启用该接口。

封装列表

下表中说明了在您具有 ADSL、G.SHDSL 或“ISDN 上的 ADSL”接口时的可用封装。

封装	说明
PPPoE	提供“以太网上的点对点协议”封装。当您在 ATM 接口上配置 PPPoE 时，将创建 ATM 子接口以及拨号器接口。这些逻辑接口会显示在“摘要”窗口中。 如果路由器运行的是不支持 PPPoE 封装的 Cisco IOS 软件版本，则禁用 PPPoE 选项。
PPPoA	提供基于 ATM 的点对点协议封装（AAL5 SNAP 和 AAL5 MUX）。如果路由器运行的是不支持 PPPoA 封装的 Cisco IOS 软件版本，则禁用 PPPoA 选项。
RFC 1483 路由选择带 AAL5 SNAP	在选择 ATM 接口后，此选项可用。在您配置 RFC 1483 连接时，将会创建 ATM 子接口。此子接口将在“摘要”窗口中显示。
RFC 1483 路由带 AAL5 MUX	在选择 ATM 接口后，此选项可用。在您配置 RFC 1483 连接时，将会创建 ATM 子接口。此子接口将在“摘要”窗口中显示。

虚拟路径标识符字段

请输入通过您的服务提供商或系统管理员获得的“虚拟路径标识符”(VPI) 值。VPI 用于在 ATM 转换和路由选择中确定用于大量连接的路径。

虚拟电路标识符字段

请输入通过您的服务提供商或系统管理员获得的“虚拟电路标识符”(VCI) 值。VCI 用于在 ATM 转换和路由选择中确定可以和其它连接共享的某条路径中的具体连接。

地址类型列表

选择下列其中一项：

- **静态 IP 地址** - 如果选择静态 IP 地址，则在提供的字段中输入 IP 地址和子网掩码或子网位数。
- **动态（DHCP 客户端）** - 如果选择动态，则路由器将从远程 DHCP 服务器租用 IP 地址。输入将分配地址的 DHCP 服务器的名称。

- **未编号的 IP** - 如果希望接口共享已分配给另一个接口的 IP 地址，则选择**未编号的 IP**。然后，选择希望当前配置的接口将使用其 IP 地址的接口。
- **Easy IP（经过协商的 IP）** - 如果路由器将通过 PPP/IPCP 地址协商获得 IP 地址，则选择 **Easy IP（经过协商的 IP）**。

“用于中央办公室远程连接的 IP 地址”字段

如果要配置 G.SHDSL 连接，则输入此链路将连接的网关的 IP 地址。此 IP 地址由服务提供商或网络管理员提供。该网关是路由器必须连接的系统，以便访问 Internet 或贵组织的 WAN。

“验证类型”复选框

选中服务提供商使用的验证类型所属框。如果不知道服务提供商使用哪种验证类型，可以选中这两个框：路由器将尝试上述两种验证类型，从而其中一次尝试将获得成功。

CHAP 验证比 PAP 验证更安全。

用户名字段

输入由 Internet 服务提供商或网络管理员提供的用户名，该用户名将用作 CHAP 和 / 或 PAP 验证的用户名。

密码字段

请输入由您的服务提供商提供的完全相同的密码。密码区分大小写。例如，密码“test”不同于“Test”。

确认密码字段

将您在前一框中输入的密码再重新输入一次。

“刷新”、“应用更改”、“放弃更改”按钮

如果您正在编辑初始配置，则这些按钮将可见。有关详细信息，请单击 Cisco SDM Express 按钮。

WAN 接口选择

利用 Cisco SDM Express 可配置一个 WAN 连接。如果您的路由器有多个 WAN 接口，请在此窗口中选择要配置的接口。从列表中选择要配置的接口，单击**添加连接**，然后在所显示的对话框中配置连接。

备注 如果不配置 WAN 连接，则您将无法配置防火墙、路由、Cisco 网络服务或 SDP。

“添加连接”、“编辑”和“删除”按钮

如果尚未配置 WAN 连接，则会启用**添加连接**按钮。如果至少已经配置了一个 WAN 连接，则会启用**编辑**和**删除**按钮。

要配置接口，请选择接口并单击**添加连接**。如果此按钮禁用，则可以使用 Cisco SDM 配置其它 WAN 连接，或者删除已配置的连接并配置另一个连接。

要编辑现有配置，请选择接口并单击**编辑**。

要删除配置，请选择接口并单击**删除**。

启用或禁用按钮

在使用 Cisco SDM Express 编辑初始配置时可用。如果选择的接口已启用，则可以使用**禁用**按钮关闭该接口。如果选择的接口已关闭，则可以使用**启用**按钮启用该接口。

接口列表

显示所有 WAN 接口的接口名称、IP 地址和接口类型。如果没有为接口配置 IP 地址，则会显示文本“无 IP 地址”。

备注 如果没有在“LAN 接口配置”窗口中用新的 IP 地址配置默认 LAN 接口，则该接口将在此窗口中列出，并且可配置为 WAN 接口。

刷新按钮

如果您正在编辑初始配置，则该按钮可见。有关详细信息，请单击 Cisco SDM Express 按钮。

串行连接

在此窗口中创建或编辑串行连接。

封装列表

选择此连接的封装。如果是编辑连接，则不能在此窗口中更改封装类型。必须删除该连接，然后使用所需的封装类型创建一个新连接。

- **帧中继** - 一种交换数据链路层协议，它在相连的设备之间使用 HDLC 封装处理多条虚拟电路。
- **HDLC** - 高级数据链路控制。由“国际标准化组织”(ISO) 开发的面向比特位的同步数据链路层协议。HDLC 针对使用帧字符和校验和的同步串行链路规定了一种数据封装方法。
- **PPP** - 点对点协议。

验证详细信息

如果选择 PPP 封装，则可以提供您的 Internet 服务提供商可能需要的验证信息。

- **用户名** - 输入由 Internet 服务提供商或网络管理员提供的完全相同的用户名，该名称将用作 CHAP 和 / 或 PAP 验证的用户名。
- **密码** - 输入服务提供商所提供的完全相同的密码。密码区分大小写。例如，密码“test”不同于“Test”。
- **确认密码** - 再次输入在前面的框中输入的同一个密码。

地址类型列表

- **静态 IP 地址** - 对帧中继、PPP 和 HDLC 封装类型可用。如果选择静态 IP 地址，则在提供的字段中输入 IP 地址和子网掩码或子网位数。
- **未编号的 IP** - 对帧中继、PPP 或 HDLC 封装类型可用。如果希望接口共享已经分配给其它接口的 IP 地址，请选择**未编号的 IP**。然后，选择希望当前配置的接口将使用其 IP 地址的接口。
- **经过协商的 IP** - 仅对 PPP 封装类型可用。如果路由器将通过 PPP/IPCP 地址协商获得 IP 地址，则选择 **Easy IP（经过协商的 IP）**。

IP 地址和子网掩码字段

如果选择“静态 IP 地址”，在这些字段中提供 IP 地址和子网掩码。

帧中继配置设置链接

单击帧中继配置设置可获取 DLCI、LMI 和“使用帧中继 IETF 帧中继封装”字段的说明。

帧中继配置设置

DLCI 字段

请在此字段中输入“数据链路连接标识符”(DLCI)。相对此接口上使用的所有 DLCI，此号码必须唯一。DLCI 为此连接提供唯一的帧中继标识符。

如果您正在编辑现有连接，则禁用 DLCI 字段。如果需要更改该 DLCI，请删除相应的连接，然后再次创建。

LMI 类型字段

请询问您的服务提供商您应该使用下列哪一种“本地管理接口”(LMI) 类型。LMI 类型指定用于监控连接的协议：

ANSI 选项

由“美国国家标准协会”(ANSI) 标准 T1.617 定义的 Annex D。

Cisco 选项

由 Cisco 和其它三家公司联合定义的 LMI。

ITU-T Q.933 选项

ITU-T Q.933 Annex A。

自动感测选项

默认值。此设置允许路由器通过与交换机通信检测正在使用哪种 LMI 类型，并允许路由器然后使用该类型。如果自动感测失败，路由器将使用 Cisco LMI 类型。

“使用 IETF 帧中继封装”复选框

选择此项以使用 Internet 工程任务组 (IETF) 封装。此选项在连接非 Cisco 生产的路由器时使用。如果要使用此接口连接非 Cisco 生产的路由器，则选择此复选框。

Internet (WAN)：高级选项

利用此窗口可指定默认静态路由，并在路由器上启用 NAT。

“创建默认路由”复选框

当通信发往路由器未知的网络时，默认静态路由会指定路由器要将通信发送到的 IP 地址或接口。如果选择**使用此接口作为转发接口**，则路由器将把所有此类通信发送到您所配置的 WAN 接口。如果选择**下一跳 IP 地址**，请指定想要路由器转发此类通信的地址。

如果选择具有动态 IP 地址的 WAN 接口，则不会显示这些字段。

CNS 服务器信息

如果您已配置了 WAN 连接，并且选择使用 Cisco 网络服务选项配置路由器，则会出现此窗口。可在该窗口中输入服务提供商提供的 Cisco 网络服务服务器信息。输入 Cisco 网络服务服务器的 IP 地址和登录信息，以使 Cisco SDM Express 可检索路由器的配置信息。

“输入 CNS 服务器 IP 地址 / 主机名”字段

必须输入网络上的 Cisco 网络服务服务器的 IP 地址或主机名。如果输入主机名，必须提供能够将该主机名解析为一个 IP 地址的一个 DNS 服务器的 IP 地址。

“输入 CNS ID 字符串”字段

必须输入从 Cisco 网络服务服务器获取配置文件所需的设备 ID。

“输入 CNS 密码”字段

输入用于登录 Cisco 网络服务服务器的密码，该密码对应于上面输入的用户 ID。

主 DNS 字段

输入路由器将使用的主域名服务器 (DNS) 的 IP 地址。您的网络管理员或服务提供商将为您提供该 IP 地址。

主 DNS 服务器是路由器尝试解析 IP 地址时首先连接的服务器。

备注 如果在“输入 CNS 服务器 IP 地址 / 主机名”字段中输入了主机名来标识 Cisco 网络服务服务器，则必须在“主 DNS”字段中输入 DNS 服务器的 IP 地址。

辅助 DNS 字段

输入路由器将使用的辅助域名服务器（如果有）的 IP 地址。您的网络管理员或服务提供商将为您提供该 IP 地址。

辅助 DNS 服务器是在主服务器不可用时路由器将连接的服务器。

防火墙配置

“防火墙配置”窗口提供了让 Cisco SDM Express 在 WAN 和 LAN 接口上配置防火墙的选项。可以在初始设置期间应用防火墙选项，或者在完成路由器的初始配置后，使用 Cisco SDM Express 应用防火墙。

如果让 Cisco SDM Express 配置防火墙，则可以在以后使用 Cisco SDM 防火墙策略配置功能修改该防火墙配置。

备注
- 如果在您的路由器上运行的 Cisco IOS 版本支持防火墙功能集，则此功能可用。
- 如果未配置 WAN 接口，则“防火墙配置”窗口不会出现。

防火墙以下列方式保护您的网络：

- 将默认访问规则应用到内部接口和外部接口 - Cisco SDM Express 创建并应用一系列默认访问规则以及其它设置，以允许 DNS 和 HTTP 通信，但拒绝专用 IP 地址空间。
- 将默认检查规则应用到外部接口 - Cisco SDM Express 创建并应用一系列默认检查规则。
- 对外部接口启用 IP 单播反向路径转发 (RPF) -“IP 单播 RPF”是导致路由器用数据包进入该路由器时通过的接口来检查该数据包源地址的一种功能。如果根据路由表发现该输入接口不是到源地址的可行路径，则相应的数据包将被丢弃。这种源地址验证用于防范 IP 欺骗。

如果选择让 Cisco SDM Express 配置防火墙，则可在以后使用 Cisco SDM 来修改防火墙配置。如果选择不配置防火墙，则可以在以后使用 Cisco SDM Express 或 Cisco SDM 进行配置。有关详细信息，请单击 Cisco 路由器和安全设备管理器。

安全设置

此窗口允许您禁用 Cisco IOS 软件中默认启用的功能，以及那些可能造成安全性风险，或者可使路由器发送大量消息以至于用尽其可用内存的功能。除非您知道您的要求与此不同，否则应选中此复选框。此帮助主题链接到 Cisco SDM Express 每个安全设置的说明。

在已经完成初始配置后，可以使用 Cisco SDM Express 更改在此窗口所做的安全设置。如果要更改此帮助页中所述的设置组下面列出的任何单个设置，可以使用 Cisco SDM 进行更改。有关详细信息，请单击 Cisco 路由器和安全设备管理器。

“在路由器上禁用 SNMP 服务”复选框

选择此项以禁用路由器上的 SNMP 服务。有关为何应禁用 SNMP 的说明，请参阅帮助主题禁用 SNMP。

“禁用存在安全隐患的服务”复选框

选择此项以在路由器上禁用下列服务。有关为何要禁用这些服务的说明，请单击以下链接：

- 禁用指名服务
- 禁用 PAD 服务
- 禁用 TCP 小型服务器服务
- 禁用 UDP 小型服务器服务
- 禁用 IP BOOTP 服务器服务
- 禁用 IP 身份识别服务
- 禁用 CDP
- 禁用 IP 源路由
- 禁用 IP Gratuitous ARP
- 禁用 IP 重定向
- 禁用 IP Proxy ARP
- 禁用 IP 定向广播
- 禁用 MOP 服务
- 禁用 IP 未达
- 禁用 IP 掩码应答

“启用增强路由器 / 网络安全性的服务”复选框

选择此项以在路由器上启用下列安全性增强功能和服务。有关这些服务和功能的说明，请单击以下链接：

- 启用网络流交换
- 启用入站远程登录会话的 TCP 持久连接
- 启用出站远程登录会话的 TCP 持久连接
- 对调试程序启用序列号和时间戳
- 启用 IP CEF
- 设置调度程序时间间隔
- 设置调度程序分配

- 设置 TCP Synwait 时间
- 启用日志
- 在所有外部接口上启用“单点传送 RPF”

“增强路由器访问安全性”复选框

选择此项以在路由器上实现下列安全性增强配置。有关这些服务和功能的说明，请单击以下链接：

- 将最小密码长度设置为少于 6 个字符
- 将验证失效率设置为小于 3 次重试
- 设置标识
- 启用远程登录设置
- 对路由器访问启用 SSH

“加密密码”复选框

选择此项启用密码加密。有关详细信息，请参阅帮助主题启用密码加密服务。

“将路由器日期和时间与本地 PC 设置同步”复选框

默认选中。如果不想使用运行 Cisco SDM Express 的 PC 的当前设置来设置路由器日期和时间，则不选此复选框。

摘要

“摘要”窗口显示了您对路由器配置所做的更改。如果需要对配置进行更改，请单击**返回**，返回到您要在其中进行更改的窗口。

单击**完成**将输入的数据保存到路由器配置文件中。

备注 单击**完成**后，如果您按照我们的建议为 LAN 接口提供了新的 IP 地址，则您将丢失与路由器的连接。为了能够重新连接到路由器，必须确保 PC 与路由器保持位于同一子网中，然后输入您为 LAN 接口分配的新 IP 地址。有关详细信息，请单击初始配置后重新连接到路由器。

帮助补充

下列帮助主题提供其它信息。

Cisco 路由器和安全设备管理器

在使用 Cisco SDM Express 为路由器提供了基本配置之后，可使用 Cisco 路由器和安全设备管理器 (Cisco SDM) 配置其它连接、优化使用 Cisco SDM Express 完成的配置，以及配置虚拟专用网 (VPN) 和数字证书之类的高级功能。

Cisco SDM 可能已安装在路由器上，或者您可能收到了一张 CD，可用来在 PC 或路由器上安装 Cisco SDM。如果从 Cisco.com 下载了 Cisco SDM，则可以使用安装程序在 PC 或路由器上安装 Cisco SDM。

若要启动 Cisco SDM，单击“工具”菜单上的 **Cisco SDM**。

Cisco 网络服务

如果您的服务提供商提供了 Cisco 网络服务服务器信息，则选择此选项。如果选择此选项，则 Cisco SDM Express 向导将收集有关 Cisco 网络服务服务器的信息，然后显示 WAN 配置窗口，以便于您配置将连接到 Cisco 网络服务服务器并获取配置的 WAN 连接。如果服务提供商未提供 Cisco 网络服务服务器信息，或您想使用 Cisco SDM Express 配置路由器，则不选此选项。

如果属于以下情况，则您将无法使用 Cisco 网络服务：

- 路由器未安装 WAN 接口，或者 Cisco SDM Express 不支持路由器的 WAN 接口。为了使路由器能够获得 Cisco 网络服务配置文件，Cisco SDM Express 必须能够配置 WAN 接口。如果 Cisco SDM Express 确定它无法配置 WAN 接口，它就会显示一条错误消息，通知您无法使用 Cisco 网络服务。如果路由器上未安装 WAN 接口，并且您仍想使用 Cisco 网络服务，那么请单击“取消”离开启动向导并关闭 Cisco SDM Express。然后，安装 Cisco SDM Express 支持的 WAN 接口卡，重新启动 Cisco SDM Express, 然后在启动向导中选择 **CNS 服务器**（Cisco 网络服务服务器）。

  如需获得支持的接口卡的列表，请参阅位于以下地址的 Cisco SDM 发行说明：

  http://www.cisco.com/go/sdm

- 您未选择此选项，并且使用 Cisco SDM Express 配置了 LAN 和 WAN 接口，然后返回到“路由器配置”窗口并选择 **CNS 服务器**。如果要使用 Cisco 网络服务，请单击**取消**离开启动向导并关闭 Cisco SDM Express。然后，重新启动 Cisco SDM Express 并在“路由器配置”窗口中选择 **CNS 服务器**。

安全设置

下列主题说明了 Cisco SDM Express 可以进行的安全设置。

禁用 SNMP

Cisco SDM Express 将尽可能禁用简单网络管理协议 (SNMP)。SNMP 是一种网络协议，可为检索和发布与网络性能和进程有关的数据提供工具。它广泛用于路由监视，并经常用于路由器配置更改。但是出于以下原因，最常用的 SNMP V1 通常是一种安全性风险：

- 它使用被称为*公用字符串*的验证字符串（密码），这些字符串以纯文本储存并在网络中发送。
- 作为定期轮询的一部分，大多数 SNMP 实现会反复发送这些字符串。
- 它是一个很具有欺骗性且基于数据报的事务协议。

因为 SNMP 可用于检索网络路由表的副本以及敏感的网络信息，因此建议如果网络不需要 SNMP，则禁用 SNMP。Cisco SDM Express 最初将请求禁用 SNMP。

将传送给路由器以禁用 SNMP 的配置如下：

```
no snmp-server
```

禁用指名服务

Cisco SDM Express 会尽可能地禁用指名服务。“指名”用于了解哪些用户已登录到网络设备上。虽然此信息通常并非高度敏感，但是有时可能对攻击者有用。

此外，指名服务可用于一种被称为“死亡一指”的特定类型的“拒绝服务”(DoS) 攻击，这种攻击会每时每刻向指定计算机发送指名请求，且从不中断。

将传送给路由器以禁用指名服务的配置如下：

```
no service finger
```

可以使用 SDM 安全审计功能撤销该修复。要了解操作方法，有关详细信息，请单击 Cisco 路由器和安全设备管理器。

禁用 PAD 服务

Cisco SDM Express 将尽可能禁用所有数据包汇编器 / 反汇编器 (PAD) 命令以及 PAD 设备与访问服务器之间的连接。

将传送给路由器以禁用 PAD 的配置如下：

```
no service pad
```

可使用 Cisco SDM 安全审计功能撤销该修复。如需了解如何进行，请参阅 Cisco SDM 中的“安全审计”联机帮助。有关详细信息，请单击 Cisco 路由器和安全设备管理器。

禁用 TCP 小型服务器服务

Cisco SDM Express 会尽可能地禁用小型服务。默认情况下，运行 Cisco IOS 11.3 或更低版本的 Cisco 设备提供了“小型服务”：echo、chargen 和 discard。（Cisco IOS 软件版本 12.0 及更高版本默认情况下禁用小型服务。）这些服务，尤其是其“用户数据报协议”(UDP) 版本，很少用于正当用途，但它们可用于启动“拒绝服务”(DoS) 和其它攻击，这些攻击在其它情况下将通过数据包过滤来防止。

例如，攻击者可能发送一个“域名系统”(DNS) 数据包，用源地址假冒 DNS 服务器（这在其它情况下是无法做到的），用源端口假冒 DNS 服务端口（端口 53）。如果这样的数据包发送到路由器 UDP echo 端口，则后果将是路由器把 DNS 数据包发送到有问题的服务器。对于此数据包将不会应用外发访问列表检查，因为它可能被视为是由路由器本身在本地生成的。

虽然通过反欺骗访问列表可避免大部分滥用小型服务的情况，或者使其危险性降低，但是在作为防火墙的一部分的任何路由器上，或者位于网络安全性关键部分的任何路由器上，都应该几乎总是禁用这些服务。因为这些服务极少使用，因此最好的策略通常是在各种类型的所有路由器上都禁用它们。

将传送给 TCP 小型服务器以禁用指名服务的配置如下：

```
no service tcp-small-servers
```

可使用 Cisco SDM 安全审计功能撤销该修复。如需了解如何进行，请参阅 Cisco SDM 中的“安全审计”联机帮助。有关详细信息，请单击 Cisco 路由器和安全设备管理器。

禁用 UDP 小型服务器服务

Cisco SDM Express 会尽可能地禁用小型服务。默认情况下，运行 Cisco IOS 11.3 或更低版本的 Cisco 设备提供了“小型服务”：echo、chargen 和 discard。（Cisco IOS 软件版本 12.0 及更高版本默认情况下禁用小型服务。）这些服务，尤其是其 UDP 版本，很少用于正当用途，并且它们可用于启动 DoS 以及其它可通过数据包过滤来防止的攻击。

例如，攻击者可能发送一个 DNS 数据包，用源地址假冒 DNS 服务器（这在其它情况下是无法做到的），用源端口假冒 DNS 服务端口（端口 53）。如果这样的数据包发送到路由器 UDP echo 端口，则后果将是路由器把 DNS 数据包发送到有问题的服务器。对于此数据包将不会应用外发访问列表检查，因为它可能被视为是由路由器本身在本地生成的。

虽然通过反欺骗访问列表可避免大部分滥用小型服务的情况，或者使其危险性降低，但是在作为防火墙的一部分的任何路由器上，或者位于网络安全性关键部分的任何路由器上，都应该几乎总是禁用这些服务。因为这些服务极少使用，因此最好的策略通常是在各种类型的所有路由器上都禁用它们。

将传送给 UDP 小型服务器以禁用指名服务的配置如下：

```
no service udp-small-servers
```

可使用 Cisco SDM 安全审计功能撤销该修复。如需了解如何进行，请参阅 Cisco SDM 中的“安全审计”联机帮助。有关详细信息，请单击 Cisco 路由器和安全设备管理器。

禁用 IP BOOTP 服务器服务

Cisco SDM Express 将尽可能禁用自举协议 (BOOTP) 服务。BOOTP 允许路由器和计算机在启动时自动从集中维护的服务器配置所需的 Internet 信息，其中包括下载 Cisco IOS 软件。因此，攻击者有可能使用 BOOTP 下载路由器的 Cisco IOS 软件副本。

此外，BOOTP 服务易受 DoS 攻击；因此应将其禁用或由防火墙过滤。

将传送给路由器以禁用 BOOTP 的配置如下：

```
no ip bootp server
```

可使用 Cisco SDM 安全审计功能撤销该修复。如需了解如何进行，请参阅 Cisco SDM 中的“安全审计”联机帮助。有关详细信息，请单击 Cisco 路由器和安全设备管理器。

禁用 IP 身份识别服务

Cisco SDM Express 会尽可能地禁用身份识别支持。身份识别支持允许您查询 TCP 端口以进行身份确认。此功能可使不安全的协议报告启动 TCP 连接的客户机以及响应此连接的主机的身份。有了身份识别支持，您就可以连接主机上的 TCP 端口、发布用于请求信息的简单文本串，并接收简单的文本串答复。

允许直接相连的网段上的任何系统获知路由器为 Cisco 设备，并确定其型号以及所运行的 Cisco IOS 软件版本，这种做法将是非常危险的。此信息可用来设计针对路由器的攻击。

将传送给路由器以禁用 IP 身份识别服务的配置如下：

```
no ip identd
```

可使用 Cisco SDM 安全审计功能撤销该修复。如需了解如何进行，请参阅 Cisco SDM 中的“安全审计”联机帮助。有关详细信息，请单击 Cisco 路由器和安全设备管理器。

禁用 CDP

Cisco SDM Express 尽可能禁用 Cisco 发现协议。Cisco 发现协议是 Cisco 路由器用来在 LAN 网段上进行相互识别的专有协议。此协议很危险，因为它允许直接相连的网段上的任何系统获知路由器是 Cisco 设备，并确定其型号以及所运行的 Cisco IOS 软件版本。此信息可用来设计针对路由器的攻击。

将传送给路由器以禁用 Cisco 发现协议的配置如下：

```
no cdp run
```

可使用 Cisco SDM 安全审计功能撤销该修复。如需了解如何进行，请参阅 Cisco SDM 中的“安全审计”联机帮助。有关详细信息，请单击 Cisco 路由器和安全设备管理器。

禁用 IP 源路由

Cisco SDM Express 会尽可能禁用 IP 源路由。IP 协议支持源路由选项，这些选项允许 IP 数据报发送者控制数据报向其最终目的地传送时将要采用的路由，通常还会控制任何答复将采用的路由。这些选项在网络中很少用于正当用途。一些早期的 IP 实现不能正确处理源路由数据包，在向运行这些实现的机器发送带有源路由选项数据报时，可能会使机器崩溃。

禁用 IP 源路由将会导致 Cisco 路由器永不转发带源路由选项的 IP 数据包。

将传送给路由器以禁用 IP 源路由的配置如下：

```
no ip source-route
```

可使用 Cisco SDM 安全审计功能撤销该修复。如需了解如何进行，请参阅 Cisco SDM 中的“安全审计”联机帮助。有关详细信息，请单击 Cisco 路由器和安全设备管理器。

启用密码加密服务

Cisco SDM Express 会尽可能地启用密码加密。密码加密将指示 Cisco IOS 软件对密码、“盘问握手验证协议”(CHAP) 保密信息，以及保存在配置文件中的类似数据进行加密。这对于防止意外窥视者读取密码很有用，例如，他们碰巧从管理员肩膀上窥视密码。

将传送给路由器以启用密码加密的配置如下：

```
service password-encryption
```

可使用 Cisco SDM 安全审计功能撤销该修复。如需了解如何进行，请参阅 Cisco SDM 中的“安全审计”联机帮助。有关详细信息，请单击 Cisco 路由器和安全设备管理器。

启用网络流交换

Cisco SDM Express 将尽可能启用网络流交换。网络流交换是一项 Cisco IOS 功能，它在使用访问控制列表 (ACL) 以及其他建立和增强网络安全性的功能的同时提高路由性能。网络流根据源和目标 IP 地址以及 TCP 端口号识别网络数据包流。然后，网络流只使用流的初始数据包进行与 ACL 的比较以及其他安全性检查，而不是必须使用网络流中的每个数据包。这样可增强性能，使您能够利用所有的路由器安全功能。

将传送给路由器以启用网络流的配置如下：

```
ip route-cache flow
```

可使用 Cisco SDM 安全审计功能撤销该修复。如需了解如何进行，请参阅 Cisco SDM 中的“安全审计”联机帮助。有关详细信息，请单击 Cisco 路由器和安全设备管理器。

启用入站远程登录会话的 TCP 持久连接

Cisco SDM Express 将尽可能为入站和出站远程登录会话启用 TCP 持久连接信息。启用 TCP 持久连接将使路由器定期生成持久连接信息，以使其检测并丢弃已断开的远程登录连接。

将传送给路由器以便为入站远程登录会话启用 TCP 持久连接的配置如下：

```
service tcp-keepalives-in
```

可使用 Cisco SDM 安全审计功能撤销该修复。如需了解如何进行，请参阅 Cisco SDM 中的“安全审计”联机帮助。有关详细信息，请单击 Cisco 路由器和安全设备管理器。

启用出站远程登录会话的 TCP 持久连接

Cisco SDM Express 将尽可能为入站和出站远程登录会话启用 TCP 持久连接信息。启用 TCP 持久连接将使路由器定期生成持久连接信息，以使其检测并丢弃已断开的远程登录连接。

将传送给路由器以便为出站远程登录会话启用 TCP 持久连接的配置如下：

```
service tcp-keepalives-out
```

可使用 Cisco SDM 安全审计功能撤销该修复。如需了解如何进行，请参阅 Cisco SDM 中的“安全审计”联机帮助。有关详细信息，请单击 Cisco 路由器和安全设备管理器。

对调试程序启用序列号和时间戳

Cisco SDM Express 会尽可能对所有调试程序和日志消息启用序列号和时间戳。调试程序和日志消息中的时间戳指示消息生成的时间和日期。序列号指示具有相同时间戳的消息生成的顺序。了解消息生成的时间和顺序是诊断潜在攻击时使用的一项重要工具。

传送给路由器以启用时间戳和序列号的配置如下：

```
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timeout msec
service sequence-numbers
```

启用 IP CEF

Cisco SDM Express 尽可能启用 Cisco Express 转发或分布式 Cisco Express 转发。由于在通信开始到达新目标时不需要生成缓存条目，因此在大量通信要发送到很多目标的情况下，Cisco Express 转发的行为比其它模式更具有可预测性。在 SYN 攻击下，针对 Cisco Express 转发配置的路由其性能优于使用传统缓存的路由器。

将传送给路由器以启用 Cisco Express 转发的配置如下：

```
ip cef
```

设置调度程序时间间隔

Cisco SDM Express 会尽可能在路由器上配置调度程序时间间隔。当路由器快速交换大量数据包时，它可能会花许多时间响应来自网络接口的中断，致使其它任何工作无法完成。某些非常快速的数据包流可能造成此情况，这可能阻止对路由器进行管理访问，当设备遭受攻击时，这是极其危险的情况。调整调度程序时间间隔，使路由器在指定的时间间隔后运行系统进程，甚至当 CPU 使用率为 100% 时也不例外，从而确保可随时对路由器进行管理访问。

将传送给路由器以调整调度程序时间间隔的配置如下：

```
scheduler interval 500
```

设置调度程序分配

在不支持 **scheduler interval** 命令的路由器上，Cisco SDM Express 应尽可能配置 **scheduler allocate** 命令。当路由器快速交换大量数据包时，它可能会花许多时间响应来自网络接口的中断，致使其它任何工作无法完成。一些速度非常快的数据包流可能会导致这种情况出现。它会阻止对路由器的管理访问，这在设备受到攻击时是非常危险的。**调度程序分配**命令可保证留出一定百分比的路由器 CPU 进程用于处理除网络交换以外的活动，如管理进程。

将传送给路由器以设置调度程序分配百分比的配置如下：

```
scheduler allocate 4000 1000
```

设置 TCP Synwait 时间

Cisco SDM Express 尽可能将 TCP synwait 时间设置为 10 秒。“TCP synwait 时间”是一个值，它在抵御 SYN 满溢攻击（一种“拒绝服务”(DoS) 攻击形式）时很有用。TCP 连接需要经过三步“握手”后才能首次建立连接。由发起方发出连接请求，接收方发出确认函，然后再由发起方发出对此确认函的认可。在此三阶段握手完成后，连接随即完成，数据传输可以开始。SYN 满溢攻击向主机发送重复的连接请求，但从不发送用于完成连接的确认接受，从而造成主机上未完成的连接数不断增加。由于未完成连接的缓冲器通常小于已完成连接的缓冲器，所以这会导致主机不堪重负从而使其瘫痪。将 TCP synwait 时间设置为 10 秒，可使路由器在 10 秒钟后切断未完成连接，以防止未完成连接在主机上累积。

将传送给路由器以将 TCP synwait 时间设置为 10 秒的配置如下：

```
ip tcp synwait-time <10>
```

启用日志

Cisco SDM Express 会尽可能启用带时间戳和序列号的日志。由于“安全审计”会提供有关网络事件的详细信息，因此日志在识别和响应安全事件方面至关重要。时间戳和序列号提供了有关网络事件发生的日期、时间和顺序的信息。

将传送给路由器以启用和配置记录日志的配置如下（将 *<log buffer size>* 和 *<logging server ip address>* 替换为您输入 Cisco SDM Express 中的相应值）：

```
logging console critical
logging trap debugging
logging buffered <log buffer size>
logging <logging server ip address>
```

在所有外部接口上启用“单点传送 RPF”

Cisco SDM Express 会尽可能在连接到 Internet 的所有接口上启用单点传送“反向路径转发”(RPF)。RPF 作为一项功能，可使路由器根据数据包借以进入路由器的接口检查任何数据包的源地址。如果根据路由表发现该输入接口不是到源地址的可行路径，则相应的数据包将被丢弃。这种源地址验证用于防范 IP 欺骗。

仅当路由对称时，此功能才起作用。如果网络以如下方式设计，即从主机 A 到主机 B 的通信通常采用一条不同于从主机 B 到主机 A 的通信所采用的路径，则检查总会失败，并将无法在这两个主机之间进行通信。这种不对称路由在 Internet 核心中很常见。启用此功能前，请确保您的网络未使用不对称路由。

此外，单点传送 RPF 只能在 IP Cisco Express 转发已启用的情况下启用。Cisco SDM Express 将检查路由器配置以确定 IP Cisco Express 转发是否已启用。如果 IP Cisco Express 转发未启用，则 Cisco SDM Express 将建议启用 IP Cisco Express 转发，如果建议得到认可则进行启用。如果 Cisco SDM Express（或任何其他原因）未启用 IP Cisco Express 转发，则单点传送 RPF 也不会启用。

为启用单点传送 RPF，会将以下配置发送给连接至专用网络外部的每一接口的路由器，请用接口标识符替换 <*outside interface*>：

```
interface <outside interface>
ip verify unicast reverse-path
```

禁用 IP Gratuitous ARP

Cisco SDM Express 会尽可能禁用 IP 免费“地址解析协议”(ARP) 请求。免费 ARP 是一个 ARP 广播，其中源和目的地 MAC 地址相同。它主要由主机用来向网络通知其 IP 地址。假冒的免费 ARP 消息可能导致网络映射信息在存储时出错，从而造成网络故障。

为禁用免费 ARP，将向路由器发送以下配置：

```
no ip gratuitous-arps
```

可使用 Cisco SDM 安全审计功能撤销该修复。如需了解如何进行，请参阅 Cisco SDM 中的“安全审计”联机帮助。有关详细信息，请单击 Cisco 路由器和安全设备管理器。

禁用 IP 重定向

Cisco SDM Express 会尽可能禁用“Internet 消息控制协议”(ICMP) 重定向消息。ICMP 通过传送有关路径、路由和网络条件的信息支持 IP 通信。ICMP 重定向消息指令端节点使用某特定路由器作为其前往特定目的地的路径。在一个正常运转的 IP 网络中，路由器将仅把重定向消息发送给其本身局域子网上的主机，绝不会有端节点发送重定向消息，并且绝不会使重定向消息经历多于一次网络转发。但是，攻击者将会破坏这些规则；一些攻击也正是在此基础上发生的。禁用 ICMP 重定向消息将不会对网络运行产生影响，而且还可扼杀这种可能的攻击方法。

将传送给路由器以禁用 ICMP 重定向消息的配置如下：

```
no ip redirects
```

禁用 IP Proxy ARP

Cisco SDM Express 会尽可能禁用代理“地址解析协议”(ARP)。网络使用 ARP 将 IP 地址转换为 MAC 地址。通常 ARP 被限定在单个 LAN 范围，但是路由器可以充当 ARP 请求的代理，从而使 ARP 查询跨越多个 LAN 段可用。因为代理 ARP 打破了 LAN 安全性屏障，因此只能将其用在安全性级别相等的两个 LAN 之间，并且只能在必要时使用。

将传送给路由器以禁用代理 ARP 的配置如下：

```
no ip proxy-arp
```

可使用 Cisco SDM 安全审计功能撤销该修复。如需了解如何进行，请参阅 Cisco SDM 中的“安全审计”联机帮助。有关详细信息，请单击 Cisco 路由器和安全设备管理器。

禁用 IP 定向广播

Cisco SDM Express 会尽可能禁用 IP 定向广播。IP 定向广播是发送到子网的广播地址的数据报，发送数据报的机器不直接连接到子网上。定向广播将通过网络以单点数据包方式路由，直到其到达目标子网，然后被转换成一个链路层广播。由于 IP 寻址体系结构本身的性质，决定了只有链路内最后一台路由器（即直接连接目标子网的路由器）才能最后确定定向广播。定向广播偶尔用于一些正当用途，但在金融服务行业之外的使用较为少见。

IP 定向广播常被用于极为常见和流行的“smurf”拒绝服务攻击，并且还可用于某些相关的攻击。在“smurf”攻击中，攻击者通过一个假冒的源地址将 ICMP 回送请求发送到一个定向广播地址，导致目标子网上的所有主机将应答发送给被冒充的源。通过连续发送此类请求数据流，攻击者能够创生一个更大的应答数据流，此数据流将能够彻底淹没其地址被冒充的主机。

禁用 IP 定向广播会导致原本要在该接口“扩散”到联路层广播的定向广播被丢弃。

将传送给路由器以禁用 IP 定向广播的配置如下：

```
no ip directed-broadcast
```

可使用 Cisco SDM 安全审计功能撤销该修复。如需了解如何进行，请参阅 Cisco SDM 中的“安全审计”联机帮助。有关详细信息，请单击 Cisco 路由器和安全设备管理器。

禁用 MOP 服务

Cisco SDM Express 会尽可能在所有以太网接口上禁用“维护操作协议”(MOP)。在和 DECNet 网络进行通信时，可使用 MOP 向路由器提供配置信息。MOP 易受到各种攻击。

将传送给路由器用于在以太网接口上禁用 MOP 服务的配置如下：

```
no mop enabled
```

可使用 Cisco SDM 安全审计功能撤销该修复。如需了解如何进行，请参阅 Cisco SDM 中的“安全审计”联机帮助。有关详细信息，请单击 Cisco 路由器和安全设备管理器。

禁用 IP 未达

Cisco SDM Express 会尽可能禁用“Internet 消息控制协议”(ICMP) 主机未达消息。ICMP 通过传送有关路径、路由和网络条件的信息支持 IP 通信。如果路由器收到使用未知协议的非广播数据包，或者路由器收到无法传送至最终目的地的数据包（因为路由器不知道到达目的地地址的路由）时，将发送 ICMP 主机不可达消息。攻击者可以使用这些消息来获取网络映射信息。

将传送给路由器以禁用 ICMP 主机未达消息的配置如下：

```
int <all-interfaces>
no ip unreachables
```

可使用 Cisco SDM 安全审计功能撤销该修复。如需了解如何进行，请参阅 Cisco SDM 中的“安全审计”联机帮助。有关详细信息，请单击 Cisco 路由器和安全设备管理器。

禁用 IP 掩码应答

Cisco SDM Express 会尽可能禁用“Internet 消息控制协议”(ICMP) 掩码应答消息。ICMP 通过传送有关路径、路由和网络条件的信息支持 IP 通信。当网络设备必须知道网际网络中某个特定子网的子网掩码时，ICMP 掩码应答消息就会发送。ICMP 网络应答消息将由具有所请求信息的设备发送给请求相应信息的设备。攻击者可以使用这些消息来获取网络映射信息。

将传送给路由器以禁用 ICMP 掩码应答消息的配置如下：

```
no ip mask-reply
```

可使用 Cisco SDM 安全审计功能撤销该修复。如需了解如何进行，请参阅 Cisco SDM 中的“安全审计”联机帮助。有关详细信息，请单击 Cisco 路由器和安全设备管理器。

将最小密码长度设置为少于 6 个字符

Cisco SDM Express 尽可能将路由器配置为要求最少 6 个字符的密码长度。攻击者破解密码的一种方法便是尝试所有可能的字符组合，直到找出密码。对于较长的密码，其字符的组合方式会相当多，使得这种攻击方法变得更加困难。

此配置更改将要求路由器上每个密码的长度至少为 6 个字符，包括用户密码、启用密码、加密密码、控制台密码、AUX 密码、tty 密码以及 vty 密码。仅当路由器上运行的 Cisco IOS 版本支持最小密码长度功能时，才会进行此配置更改。

将传送给路由器的配置如下：

```
security passwords min-length <6>
```

将验证失效率设置为小于 3 次重试

Cisco SDM Express 尽可能将路由器配置为在 3 次登录尝试失败之后锁定访问。有一种破解密码的方法叫“字典”攻击，此方法所使用的软件会尝试使用字典中的每个字进行登录。此配置将在 3 次登录尝试失败之后将对路由器的访问锁定 15 秒，从而使字典攻击方法失效。除了锁定对路由器的访问之外，此配置还会在 3 次登录尝试失败之后生成日志消息，以便向管理员发出有关未成功登录尝试的警告。

将传送给路由器以在 3 次登录尝试失败之后锁定路由器访问的配置如下：

```
security authentication failure rate <3>
```

设置标识

Cisco SDM Express 会尽可能配置文本标识。在某些辖区内，如果您提供相应的警示标识，告诫未经授权的用户，他们实际上是在未获授权的情况下使用您的系统，那么对闯入您系统的用户提起民事和 / 或刑事诉讼将更容易进行。在其它辖区内，您有可能被禁止监控用户甚至是未授权用户的行为，除非您已采取措施通知他们您要这样做的意图。文本标识是执行此通知的一种方法。

将传送给路由器以创建文本标识的配置如下（将 *<company name>*、*<administrator email address>* 以及 *<administrator phone number>* 替换为您输入 Cisco SDM Express 中的相应值）：

```
banner ~
Authorized access only
This system is the property of <company name> Enterprise.
Disconnect IMMEDIATELY as you are not an authorized user!
Contact <administrator email address> <administrator phone number>.
~
```

启用远程登录设置

Cisco SDM Express 通过实现以下配置，可尽可能保证控制台、AUX、vty 和 tty 线路的安全：

- 配置**传输输入**和**传输输出**命令，以定义可用于连接以上各线路的协议。
- 在控制台和 AUX 线路中将 exec 超时值设置为 10 分钟，使管理用户在无活动状态持续 10 分钟后从这些线路中注销。

将发送给路由器以保证控制台、AUX、vty 和 tty 线路安全的配置如下：

```
!
line console 0
transport output telnet
exec-timeout 10
login local
!
line AUX 0
transport output telnet
exec-timeout 10
login local
!
line vty ….
transport input telnet
login local
```

对路由器访问启用 SSH

如果路由器上运行的 Cisco IOS 版本是加密映像（使用 56 位数据加密标准 (DES) 加密并受限于导出限制的映像），则 Cisco SDM Express 将尽可能实现以下配置以保护远程登录访问：

- 为远程登录访问启用 Secure Shell (SSH)。SSH 可使远程登录访问更为安全。
- 将 SSH 超时值设为 60 秒，会使未完成的 SSH 连接在 60 秒后关闭。
- 将锁定对路由器的访问前所允许的不成功 SSH 登录尝试最大次数设置为 2。

将传送给路由器用于保护访问和文件传输功能安全的配置如下：

```
ip ssh time-out 60
ip ssh authentication-retries 2
!
line vty 0 4
transport input ssh
!
```

Cisco SDM Express 按钮

帮助按钮

单击该项打开新的浏览器窗口，并显示有关所显示的 Cisco SDM Express 窗口的信息。

“关于”按钮

单击**关于**会显示包含 Cisco SDM Express 版本信息的窗口。单击此窗口中的**硬件和软件详细信息**可显示下列信息。

硬件详细信息：

- 路由器型号
- 路由器中的总内存量
- 路由器中总的闪存容量
- 路由器启动位置（例如：闪存）

还提供硬件配置图。

软件详细信息：

- 路由器运行的 Cisco IOS 软件的名称。
- Cisco IOS 软件的版本
- Cisco IOS 软件支持的功能集，如防火墙和 VPN
- Cisco SDM Express 的版本

“退出”按钮

完成初始配置后，单击**退出**以关闭 Cisco SDM Express。

刷新按钮

如果您正在编辑初始配置，则该按钮可见。单击**刷新**以刷新 Cisco SDM Express 中的路由器数据。

应用更改按钮

如果您正在编辑初始配置，则该按钮可见。单击**应用更改**可将已做出的更改传送到路由器。

放弃更改按钮

如果您正在编辑初始配置，则该按钮可见。单击**放弃更改**可清除所做更改的窗口。

初始配置后重新连接到路由器

如果您按照建议给路由器 LAN 接口分配了一个新 IP 地址，则在传送配置后会失去与路由器的连接。

在使用 Cisco SDM Express 执行初始配置后，请采用此步骤重新连接路由器。

步骤 1 将 PC 置于与路由器 LAN 接口所在的子网中。

- 如果将路由器配置为 DHCP 服务器，您必须将 PC 配置为自动获取 IP 地址，然后打开一个命令窗口并依次输入 **ipconfig /release** 命令及 **ipconfig /renew** 命令。
- 如果未将路由器配置为 DHCP 服务器，您必须为 PC 分配一个与路由器处于相同子网中的静态 IP 地址。例如，如果使用子网掩码 255.255.255.224 将 LAN IP 地址更改为 10.20.20.1，则会为您的 PC 分配一个介于 10.20.20.2 和 10.20.20.30 之间的 IP 地址并且使用相同的子网值

步骤 2 如果配置一个不同于默认接口的 LAN 接口，请确保将您的 PC 连接到已配置的 LAN 接口。例如，如果将 FE 0/1（而不是 FE 0/0）配置为 LAN 接口，请确保将您的 PC 连接到 FE 0/1。

步骤 3 PC 就绪之后，在浏览器中输入您提供给路由器 LAN 接口的新 IP 地址（http:// *新 IP 地址），以此将 PC 重新连接到路由器*。例如，如果您将 LAN IP 地址更改为 10.20.20.1，则要在 web 浏览器中输入 http://10.20.20.1 才能再次连接路由器。

步骤 4 重新连接之后，测试 WAN 连接以确保可以连接到 Internet。

有关详细信息，请单击测试您的 WAN (Internet) 连接。

测试您的 WAN (Internet) 连接

可将浏览器指向远程网站（如 www.cisco.com）以测试 Internet 连接。如果能够连接到您输入的远程网站，则 WAN 配置已正确生效。

如果无法连接到远程网站，则可以执行以下操作以使用 Cisco SDM 进行故障诊断：

步骤 1 单击“工具”菜单上的 **Cisco SDM** 以启动 Cisco SDM。

步骤 2 登录到 Cisco SDM 并单击**接口和连接**。

步骤 3 单击“编辑”选项卡并且选择要测试的 WAN 连接。

步骤 4 单击**测试 连接**并按照出现的指示进行操作。Cisco SDM 将报告可能的问题并提出建议操作。

SDP 故障诊断提示

在注册使用安全设备配置 (SDP) 以建立路由器和证书服务器之间的连接之前，请使用以下信息。如果在注册中遇到问题，可复检以下任务，以确定问题的根源。

当 SDP 启动时，必须最小化显示此帮助主题的浏览器窗口，以便可查看 SDP Web 应用程序。

故障诊断提示

以下建议涉及在本地路由器以及认证中心 (CA) 服务器上做好相应的准备工作。您需要将这些要求传达给 CA 服务器的管理员。请确保以下事项：

- 本地路由器与 CA 服务器彼此之间存在 IP 连接。本地路由器必须能够对证书服务器成功执行 ping 操作，证书服务器也必须能够对本地路由器成功执行 ping 操作。
- CA 服务器管理员使用的 web 浏览器要支持 JavaScript。
- CA 服务器管理员在本地路由器具备启用权限。

- 本地路由器上的防火墙允许通过证书服务器收到和发出通信。
- 如果申请方和 / 或接受登记方配置了防火墙，则必须确保该防火墙允许从调用 SDM /SDP 应用程序的 PC 发来的 HTTP 或 HTTPS 通信。

有关 SDP 的详细信息，请参阅以下网页：

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008028afbd.html#wp1043332

章 2

Cisco SDM Express 编辑模式

SDM Express 编辑屏幕允许您更改 LAN 和 WAN 配置，并可更改防火墙、NAT、PAT、路由和安全设置。

概述

“概述”窗口提供了有关路由器 LAN、WAN 和防火墙配置的基本信息。

图标

“开启”。开启接口。

“活动”。防火墙处于活动状态。

“关闭”。接口关闭。

“非活动”。防火墙处于非活动状态

LAN 字段

LAN 字段显示 LAN 连接的接口、IP 地址和 DHCP 服务器信息。

- **接口** - LAN 接口的名称。例如，Fast Ethernet 0。如果 SDM Express 无法识别路由器的 LAN 接口，则它将在此字段中显示已配置的 LAN 接口的数量。
- **IP/ 掩码** - 后跟子网位数（表示子网掩码）的 IP 地址。LAN IP 地址通常取自于专用 IP 地址范围。例如，使用子网掩码 255.255.255.0 的 IP 地址 10.10.10.1 将显示为 10.10.10.1/24。
- **DHCP 服务器** - **已配置**或**未配置**。
- **DHCP 池** - 如果配置了 DHCP 服务器，则此字段包含对 DHCP 客户端可用的 IP 地址范围。例如，如果在 10.10.10.0 网络中使用某一 IP 地址配置了 LAN 接口，则可使用从 10.10.10.1 至 10.10.10.254 的地址范围来配置 DHCP 地址池。

如果 SDM Express 无法识别路由器上的 LAN 接口，则它将显示所支持的 LAN 接口的总数以及所配置的 LAN 接口的总数。

Internet (WAN) 字段

Internet 字段显示 WAN 接口的名称、配置的 WAN 连接的类型以及 IP 地址子网掩码信息。

- **接口** - WAN 接口的名称，例如 ATM 0/1。如果 SDM Express 无法识别路由器的 WAN 接口，则它将在此字段中显示已配置的 WAN 连接的数量。
- **连接类型** - WAN 连接的类型，例如 ADSL 或 G.SHDSL
- **IP/ 掩码** - 后跟子网位数（表示子网掩码）的 IP 地址。例如，使用子网掩码 255.255.255.0 的 IP 地址 172.16.33.15 将显示为 172.16.33.15/24。

如果 SDM Express 无法识别路由器上的 WAN 接口，则它将显示所支持的 WAN 接口的总数以及所配置的 WAN 接口的总数。

防火墙字段

- **防火墙类型** - SDM Express“模认”、“自定义”或“无”。
- **内部** - 内部（即受信）接口的 IP 地址。
- **外部** - Internet 接口的连接类型。

基本配置

该窗口显示路由器上配置的用户帐户，并使您能够更改启用加密的密码。要进入“IOS CLI 启用”模式，必须使用启用加密的密码。

如果要添加或删除用户帐户，可使用 Cisco Router and Security Device Manager (SDM) 来实现。

编辑 / 删除按钮

使用这些按钮可管理路由器上的用户帐户。可编辑现有的用户帐户并删除现有的帐户。如果需要新建用户帐户，可使用 SDM 完成此操作。有关详细信息，请单击 Cisco 路由器和安全设备管理器。

备注 如选定了使用“视图”选项创建的用户帐户，将禁用“编辑”和“删除”按钮。

用户名 / 登录密码 / 密码已加密字段

该区域列出路由器上的用户帐户。

启用加密密码字段

在这些字段中输入新密码。确保记住该密码。该密码在路由器上以加密的形式存储，并且不能读取。

主机名字段

如需要，可编辑路由器的主机名。

域名字段

可编辑已为路由器配置的域名。

刷新 / 应用更改 / 放弃更改按钮

如果是编辑初始配置，则会显示这些按钮。有关详细信息，请单击 Cisco SDM Express 按钮。

编辑用户名

在该窗口中提供的字段中编辑用户帐户。

用户名字段

在此字段中编辑用户名。

密码字段

在此字段中输入或编辑密码。

在**确认密码**字段中重新输入密码。如果密码和确认密码不一致，则单击**确定**时会显示一个错误消息窗口。

当您单击**确定**时，新建或编辑过的帐户信息会显示在“为远程登录配置用户帐户”窗口中。

“使用 MD5 散列算法加密密码”复选框

这是显示当前密码 MD5 加密设置的只读字段。复选标记表示已使用单向 Message Digest 5 (MD5) 算法加密密码。

LAN

“桥接 / 不要将 LAN 接口与无线进行桥接”复选框

如果路由器具有无线接口，则可从无线网络将通信桥接到以太网 LAN。如果要在路由器上的以太网 LAN 和无线网络之间桥接通信和共享地址，请单击**桥接 LAN 接口与无线接口**。

LAN 接口配置字段

可在这些字段中编辑 LAN 接口的 IP 地址和子网掩码。如果需要有关 IP 地址和子网掩码字段的详细信息，请参见 IP 地址字段。

无线

如路由器有无线接口，则会显示“无线”窗口。如果需要配置高级的无线参数，请单击**启动无线应用程序**。

刷新按钮

如果是编辑初始配置，则会显示该按钮。有关详细信息，请单击 Cisco SDM Express 按钮。

WAN - 无法配置 WAN 接口

如 SDM Express 无法配置已选定为 WAN 接口的接口，会显示该窗口。如果 SDM Express 不支持选定的接口，或者如果接口存在使用 CLI 输入的部分配置，就可能发生这种情况。

选择配置另一接口，或登录路由器并删除要配置接口下的配置声明。从“工具”部分中选择**远程登录**，登录到路由器并进入配置模式。使用 CLI 删除配置声明。然后返回 SDM Express 并配置 WAN 接口。

没有可用的 WAN

如 SDM Express 未能在路由器上检测到 WAN 接口，则会显示该窗口。

删除连接

删除连接时可能涉及相关联的配置命令，这些命令可在配置中保留或与该连接一起删除。单击**查看详细信息**可显示这些关联。单击“隐藏详细信息”可隐藏关联详细信息。

如果希望 SDM Express 将连接与这些关联一并删除，请单击**自动删除所有关联**。

如果希望自己删除这些关联，请单击**我将在稍后删除这些关联**。

要自己删除这些关联，请在“工具”菜单中单击**远程登录**，登录路由器，然后输入 **enable** 命令进入“启用”模式。然后输入命令的 **no** 形式来删除所关联的配置。例如，如果命令 **ip tcp adjust mss** 与连接关联，则输入：

```
no ip tcp adjust mss
```

防火墙

如果在初始安装时没有启用防火墙，则使用此窗口可启用防火墙，如果已启用防火墙，可使用该窗口禁用防火墙。如果路由器运行的 Cisco IOS 映像不支持防火墙功能集，则不能在该路由器上启用基本防火墙。如果路由器是有多个 LAN 或 WAN 接口的模块路由器，则不能使用 SDM Express 启用基本防火墙。

有关基本防火墙功能的说明，请参见防火墙配置。

启用防火墙 / 禁用防火墙按钮

使用这些按钮可添加或删除基本防火墙配置。

无法配置防火墙窗口

如果 SDM Express 无法让您配置防火墙，将显示“无法配置防火墙”窗口。以下是防火墙无法配置的可能原因。

- 路由器为固定端口路由器，并且没有确切配置一个 LAN 和 WAN 接口。
- 路由器为模块路由器，或者有两个以上已配置的接口。
- 已使用其它工具将防火墙和 / 或访问控制列表应用到路由器。

刷新按钮

如果是编辑初始配置，则会显示该按钮。有关详细信息，请单击 Cisco SDM Express 按钮。

NAT

如果 LAN 中的设备有专用地址，可通过使用网络地址转换 (NAT) 允许它们共享一个公用 IP 地址。NAT 使用端口号识别主机以及您希望使用的主机服务。

单击**启用 NAT** 可使用路由器中的 NAT。

无法配置 NAT

如果处于 SDM Express 编辑模式，则此窗口将在 SDM Express 无法帮助您配置 NAT 时出现。SDM Express 可能出于以下原因而无法帮助您配置 NAT。

- 路由器为固定端口路由器，并且没有确切配置一个 LAN 和 WAN 接口。
- 路由器为模块路由器，或者有两个以上已配置的接口。
- NAT 已经配置在某个接口上。

添加按钮

单击该项添加新的 NAT 规则。

编辑按钮

单击该项编辑所选 NAT 规则。

刷新按钮

如果是编辑初始配置，则会显示该按钮。有关详细信息，请单击 Cisco SDM Express 按钮。

添加或编辑地址转换规则

通过此窗口可以输入或编辑服务器的 IP 地址转换信息。

专用 IP 地址

输入服务器在内部网络上使用的 IP 地址。此地址不能是 Internet 上外部使用的 IP 地址。

公用 IP 地址

选择**使用 WAN 接口 IP 地址**以使用路由器 WAN 接口的 IP 地址。已配置的 WAN 接口的 IP 地址出现在右侧。或者选择**新 IP 地址**并输入服务器 IP 地址。

服务器类型

自下拉菜单中选择如下服务器类型之一：

- 网络服务器

  服务于 HTML 和其他 WWW 网页的 HTTP 主机。
- 电子邮件服务器

  用于发送 Internet 邮件的 SMTP 服务器。
- 其他

  该服务器不是 Web 服务器或电子邮件服务器，但是需要端口转换以提供服务。此选项将激活“转换后的端口”字段以及“协议”下拉菜单。

如果不选服务器类型，则发往您为该服务器选择的公用 IP 地址的所有通信将路由到该服务器，并且不会进行端口转换。

原始端口

输入服务器使用的端口号，以接受来自内部网络的服务请求。

转换后的端口

输入服务器使用的端口号，以接受来自互联网的服务请求。

协议

选择 TCP 或 UDP 以表示服务器通过原始端口和转换后的端口所使用的协议。

路由

如配置更改指示宜于编辑默认路由，可使用该“路由”窗口编辑现有默认路由。例如，如果已更改了 WAN 接口的静态 IP 地址，则有可能也需要更改默认网关的 IP 地址。

启用复选框

如果要启用默认路由，请选中该复选框。如果已经定义了默认路由，则该框为选中状态。取消选中该复选框将禁用默认路由。

“转发（下一跳）”字段

可指定路由器上的某个接口为下一跳，或者可指定某个 IP 地址为下一跳。如果单击“接口”，则从下拉列表中选择接口。如果单击 **IP 地址**，请输入 IP 地址。

刷新 / 应用更改 / 放弃更改按钮

如果是编辑初始配置，则会显示这些按钮。有关详细信息，请单击 Cisco SDM Express 按钮。

安全设置

此窗口允许您禁用在 Cisco IOS 软件中默认启用的功能，但是这样做可能带来安全隐患，或者使路由器以很高的容量发送消息以至用尽其可用内存。应该使这些框保留选中状态，除非您确信自己有不同的要求。

如果允许 SDM Express 生成这些设置，并且您想在以后对这些设置组下所述的任何单个设置进行更改，则可以使用 SDM 进行。有关详细信息，请单击 Cisco 路由器和安全设备管理器。

“全选”（Cisco 推荐选项）复选框

单击**全选**可让您在该窗口中实现所有的安全设置。如果以后决定要更改该安全设置，可使用 Cisco SDM 完成此操作。

“禁用存在安全隐患的服务”复选框

单击此框可在路由器上禁用下列服务。有关为何要禁用这些服务的说明，请单击以下链接：

- 禁用指名服务
- 禁用 PAD 服务
- 禁用 TCP 小型服务器服务
- 禁用 UDP 小型服务器服务
- 禁用 IP BOOTP 服务器服务
- 禁用 IP 身份识别服务
- 禁用 CDP
- 禁用 IP 源路由
- 禁用 IP Gratuitous ARP
- 禁用 IP 重定向
- 禁用 IP Proxy ARP
- 禁用 IP 定向广播
- 禁用 MOP 服务
- 禁用 IP 未达禁用 IP 掩码应答

“启用增强路由器 / 网络安全性的服务”复选框

单击此框可在您的路由器上启用下列增强安全性的功能和服务。有关这些服务和功能的说明，请单击以下链接：

- 启用网络流交换
- 启用入站远程登录会话的 TCP 持久连接
- 启用出站远程登录会话的 TCP 持久连接
- 对调试程序启用序列号和时间戳
- 启用 IP CEF
- 设置调度程序时间间隔
- 设置调度程序分配
- 设置 TCP Synwait 时间
- 启用日志

“加密密码”复选框

选中此框可启用密码加密。有关详细信息，请参阅帮助主题启用密码加密服务。

“与本地 PC 时钟同步”复选框

单击该按钮可使路由器与本地 PC 上的时钟同步。

刷新 / 应用更改 / 放弃更改按钮

如果是编辑初始配置，则会显示这些按钮。有关详细信息，请单击 Cisco SDM Express 按钮。

工具

SDM Express 提供了多个可以使用的工具

Ping 选项

单击将打开一个窗口，可在其中指定 ping 的来源和目标。有关详细信息，请参阅 Ping。

远程登录选项

显示 Windows 的“远程登录”对话框，该对话框允许您连接到路由器并且使用远程登录协议访问 Cisco IOS 命令行 (CLI) 接口。

Cisco SDM 选项

单击可启动 Cisco Router and Security Device Manager (SDM)。SDM 允许您执行高级的配置。

软件更新选项

可让 SDM Express 帮助您更新路由器上的配置软件。可通过 Cisco.com 更新，如果已将 SDM.zip 文件下载到 PC 中，可使用该文件来进行更新。有关详细信息，请单击以下任一链接。

- 从 Cisco.com 更新 SDM
- 从本地 PC 更新 SDM
- 从 CD 更新 SDM

Ping

可以在此窗口为对等设备执行 ping 操作。可以选择 ping 操作的来源和目标。您可能希望在重新配置 WAN 连接后对远程对等项执行 ping 操作。

源字段

选择或输入要启动 ping 操作的 IP 地址。如果您要使用的地址不在列表中，则可以在字段中输入其它地址。可从路由器上的任意接口启动 ping 操作。默认情况下，会从与远程设备连接的外部接口启动 **ping** 命令。

目标字段

选择您要执行 ping 操作的 IP 地址。如果您要使用的地址不在列表中，则可以在字段中输入其它地址。

为远程对等项执行 ping：

指定来源和目标，并单击 **Ping**。可以读取 **ping** 命令的输出结果，以确定 ping 是否成功。

清除 ping 命令的输出：

单击**清除**。

从 Cisco.com 更新 SDM

可直接从 Cisco.com 更新 SDM Express 和 SDM。SDM 检查 Cisco.com 上的可用版本，如果有版本比路由器上当前运行的版本更高，则 SDM 将通知您。然后可以使用“更新”向导更新 SDM。

通过 Cisco.com 更新 SDM：

步骤 1 从“工具”菜单中选择“通过 Cisco.com 更新 SDM”。选择此选项可启动更新向导。

步骤 2 使用更新向导获取 SDM 文件，并将它们复制到路由器。

CCO 登录

必须提供 CCO 登录名和密码才能访问此网页。提供用户名和密码，然后单击“确定”。

如果没有 CCO 登录名和密码，则可以打开 Web 浏览器并转至位于以下链接的 Cisco 网站获取：

http://www.cisco.com

当网页打开时，单击“注册”并提供获取用户名和密码所必需的信息。然后，再次尝试此操作。

从本地 PC 更新 SDM

可使用从 Cisco.com 上下载的 SDM.zip 文件更新 SDM。SDM 提供了更新向导，该向导将把必要的文件复制到路由器上。

要通过运行 SDM 的 PC 上更新 SDM，请按以下步骤操作：

步骤 1 从下列 URL 下载 sdm-v*nn*.zip 文件：

http://www.cisco.com/cgi-bin/tablebuild.pl/sdm

如果有一个以上的 SDM.zip 文件，请使用版本最高的副本。

步骤 2 使用更新向导将 SDM 文件从 PC 复制到路由器。

从 CD 更新 SDM

如果您有 SDM CD，则可使用它更新路由器上的 SDM。要完成该操作，请执行下列步骤：

步骤 1 将 SDM CD 放入 PC 的 CD 驱动器中。

步骤 2 选择**从 CD 更新 SDM**，在读取文本后，在“一般说明”窗口中单击**更新软件**。

步骤 3 SDM 将使您能够在 CD 上查找文件 SDM-Updates.xml。找到文件后，单击**打开**。

步骤 4 按照安装指导中的说明进行。

日期和时间属性

使用此窗口进行路由器日期和时间设置。您可以使 SDM Express 将设置项与 PC 同步，或手动进行设置。

“与本地 PC 时钟同步”复选框

选中此选项可将 SDM Express 设置为使路由器的日期和时间设置与 PC 的日期和时间设置同步。

“同步”复选框

单击该项使 SDM Express 执行同步。SDM Express 仅在您单击**“同步”时才会以此方式调整日期和时间设置；它不会在后续会话期间自动与 PC 重新进行同步。如果未选中“与本地 PC 时钟同步”，则此按钮禁用。**

备注 启动 SDM Express 之前必须在 PC 上进行“时区”和“夏时制”设置，以便在您单击**同步**时 SDM Express 可以收到正确的设置。

编辑日期和时间字段

通过此区域手动设置日期和时间。可从下拉列表中选择月份和年份，然后在日历中选择当月的日期。“时间”区域中字段的值要求采用 24 小时格式。可按照“格林尼治标准时间”(GMT) 选择时区，也可浏览所在时区中主要城市的列表。

如果您想要路由器调整夏时制时间和“标准”时间的时间设置，请选中**自动按夏时制调整时间**。

应用按钮

单击此按钮可应用您在“日期”、“时间”和“时区”字段中进行的日期和时间设置。

重置为出厂默认设置

您可将路由器的配置重新设置为出厂默认值，并将当前配置保存到一个以后可以使用的文件中。如果您更改了路由器 LAN IP 地址的出厂值 10.10.10.1，则您将失去路由器与 PC 间的连接，因为在您重新设置时，该 IP 地址将会变回到 10.10.10.1。

备注 Cisco 3620、3640、3640A 和 7000 系列路由器上不支持“重置为出厂默认设置”功能。

步骤 1：将运行配置另存到 PC

在该步骤中，会将路由器的运行配置另存到 PC，以便在需要时可将其恢复到您的路由器。使用**浏览**按钮可选择存储配置的目录。

步骤 2：记录这些步骤，而后重新设置路由器。

因为在单击**重新设置**时，您会失去与路由器的联系，所以您必须知道在重新设置路由器后重新连接的方式。

a) 使用 10.10.10.0 网络上的 IP 地址配置 PC。

将 PC 配置到 10.10.10.0 子网中。根据路由器的情况，您必须配置 PC 自动获取 IP 地址，或使用 10.10.10.0 子网中的静态 IP 地址配置 PC。

如果您有在下表中列出的路由器，则可配置 PC 自动获取 IP 地址。请参考使用静态或动态 IP 地址重新配置您的 PC 了解具体操作。

如果您有这些路由器中的一个，则可配置 PC 自动获取 IP 地址。
SB10x、Cisco 83x、85x、87x、1701、1710、1711 和 1712、180x 和 181x。

如果下表中列出了您的路由器，请将 PC 的 IP 地址配置为 10.10.10.0 子网中介于 10.10.10.2 和 10.10.10.6 之间的某个 IP 地址，并使用子网掩码 255.255.255.248。请参考使用静态或动态 IP 地址重新配置您的 PC 以了解如何进行此操作。

如果您有这些路由器中的一个，则可使用 10.10.10.0 子网中的静态 IP 地址配置 PC。
Cisco 1721、1751、1760、1841、2600XM、2691、28xx、36xx、37xx 和 38xx。

b) 浏览到 http(s)://10.10.10.1。

在重置后，路由器恢复原始出厂默认 IP 地址 10.10.10.1，您必须使用该地址进行重新连接。

c) 请使用用户名 cisco 和密码 cisco 再次登录 SDM Express。

用户名和密码也已经被返回到其默认设置，必须使用这些原始值登录 SDM Express。

刷新按钮

如果是编辑初始配置，则会显示该按钮。有关详细信息，请单击 Cisco SDM Express 按钮。

使用静态或动态 IP 地址重新配置您的 PC

给 PC 分配静态 IP 地址或配置 PC 自动获取 IP 地址的各个过程略有不同，具体情况视 PC 正在运行的 Microsoft Windows 而定。

备注 请先重新设置路由器，然后再重新配置 PC。

Microsoft Windows NT

双击“控制面板”中的“网络”图标以显示**网络**窗口。单击**协议**，选择第一个“TCP/IP 协议”条目，然后单击**属性**。在“属性”窗口中，选择此连接所使用的以太网适配器。单击**自动获得 IP 地址**以获得一个动态 IP 地址。

要获得静态 IP 地址，请单击**指定 IP 地址**。输入 IP 地址 10.10.10.2 或 10.10.10.0 子网中大于 10.10.10.1 的任何其它地址。输入子网掩码 255.255.255.248。可将其它字段保留为空。单击**确定**。

Microsoft Windows ME

双击“控制面板”中的**网络**图标以显示“网络”窗口。在以太网适配器满足连接使用的情况下双击“TCP/IP 协议”条目以显示 TCP/IP **属性**。在 **IP 地址**选项卡中，单击**自动获得 IP 地址**以获得一个动态 IP 地址。

要获得静态 IP 地址，请单击**指定 IP 地址**。输入 IP 地址 10.10.10.2 或 10.10.10.0 子网中大于 10.10.10.1 的任何其它地址。输入子网掩码 255.255.255.248。可将其它字段保留为空。单击**确定**。

Microsoft Windows 2000

从“控制面板”中选择**网络和拨号连接 / 本地连接**。在“连接时使用”字段中选择以太网适配器。选择“Internet 协议”，并单击“属性”。单击**自动获得 IP 地址**以获得一个动态 IP 地址。

要获得静态 IP 地址，请单击**指定 IP 地址**。输入 IP 地址 10.10.10.2 或 10.10.10.0 子网中大于 10.10.10.1 的任何其它地址。输入子网掩码 255.255.255.248。可将其它字段保留为空。单击**确定**。

Microsoft Windows XP

单击**开始**，选择**设置**、**网络连接**，然后选择要使用的 LAN 连接。单击**属性**，选择 **Internet 协议 TCP/IP**，然后单击**属性**按钮。单击**自动获得 IP 地址**以获得一个动态 IP 地址。

要获得静态 IP 地址，请单击**指定 IP 地址**。输入 IP 地址 10.10.10.2 或 10.10.10.0 子网中大于 10.10.10.1 的任何其它地址。输入子网掩码 255.255.255.248。可将其它字段保留为空。单击**确定**。

功能不可用

如正尝试配置的功能不可用，则显示该窗口。当 ISO 映像或路由器硬件不支持某功能时，可能会出现这种情况。

索引

T

U

Z