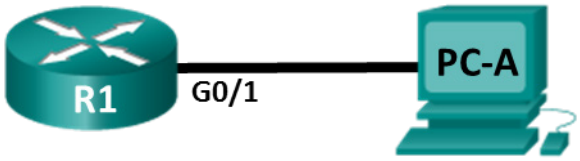
实验 - 在 Wireshark 中检查 Telnet 和 SSH

拓扑



地址分配表

设备	接口	IP 地址	子网掩码	默认网关
R1	G0/1	192.168.1.1	255.255.255.0	N/A
PC-A	网卡	192.168.1.3	255.255.255.0	192.168.1.1

目标

第 1 部分：配置设备用于 SSH 访问

第 2 部分：通过 Wireshark 检查 Telnet 会话

第 3 部分：通过 Wireshark 检查 SSH 会话

背景/场景

在本实验中，您将配置路由器接受 SSH 连接，并使用 Wireshark 捕获和查看 Telnet 和 SSH 会话。本练习将演示 SSH 中加密的重要性。

注意：CCNA 动手实验所用的路由器是采用 Cisco IOS 15.2(4)M3 版（universalk9 映像）的 Cisco 1941 集成多业务路由器 (ISR)。所用的交换机是采用 Cisco IOS Release 15.0(2)（lanbasek9 映像）的 Cisco Catalyst 2960 系列。也可使用其他路由器、交换机以及其他 Cisco IOS 版本。根据型号以及 Cisco IOS 版本的不同，可用命令和产生的输出可能与实验显示的不一样。请参考本实验末尾的“路由器接口摘要表”以了解正确的接口标识符。

注意：确保路由器和交换机的启动配置已经清除。如果不确定，请联系教师。

所需资源

- 1 台路由器（支持 Cisco IOS 15.2(4)M3 版通用映像的 Cisco 1941 或同类路由器）
- 1 台 PC（采用 Windows 7 或 8 且支持终端仿真程序，比如安装有 Tera Term 和 Wireshark）
- 用于通过控制台端口配置 Cisco IOS 设备的控制台电缆
- 如拓扑图所示的以太网电缆

© 2015 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

第 1 部分：配置设备用于 SSH 访问

在第 1 部分中，您将建立网络拓扑并配置基本设置，例如接口 IP 地址、设备访问和路由器密码。

第 1 步：建立如拓扑图所示的网络。

第 2 步：初始化并重新加载路由器。

第 3 步：在路由器上配置基本设置。

a. 通过控制台连接到路由器，并启用特权 EXEC 模式。

b. 进入配置模式。

c. 根据地址分配表配置设备名称。

d. 要防止路由器尝试将错误输入的命令视为主机名，则禁用 DNS 查找。

e. 指定 **class** 作为特权 EXEC 加密密码。

f. 指定 **cisco** 作为控制台密码并启用登录。

g. 指定 **cisco** 作为 VTY 密码并启用登录。

h. 加密明文密码。

i. 创建一个向访问设备者发出警告的标语：未经授权，禁止访问。

j. 使用地址分配表中包含的信息配置并激活 G0/1 接口。

第 4 步：配置 R1 以访问 SSH。

a. 配置设备的域。

```
R1(config)# ip domain-name ccna-lab.com
```

b. 配置加密密钥方法。

```
R1(config)# crypto key generate rsa modulus 1024
```

c. 配置本地数据库用户名。

```
R1(config)# username admin privilege 15 secret adminpass
```

d. 在 VTY 线路上启用 Telent 和 SSH。

```
R1(config)# line vty 0 4
R1(config-line)# transport input telnet ssh
```

e. 更改登录方法以便使用本地数据库验证用户。

```
R1(config-line)# login local
R1(config-line)# end
```

第 5 步：将运行配置保存到启动配置文件中。

© 2015 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

第 6 步：配置 PC-A。

a. 使用 IP 地址和子网掩码配置 PC-A。

b. 配置 PC-A 的默认网关。

第 7 步：检验网络连接。

从 PC-A 对 R1 执行 ping 操作。如果 ping 失败，请排除连接故障。

第 2 部分：通过 Wireshark 检查 Telnet 会话

在第 2 部分中，您将使用 Wireshark 捕获和查看 Telnet 会话在路由器上传输的数据。您将使用 Tera Term 通过 telnet 访问 R1 并登录，然后在路由器上发出 **show run** 命令。

注意：如果 Telnet/SSH 客户端软件包在 PC 上未安装，则您必须在继续之前安装它。这两个常用的免费 Telnet/SSH 软件包是 Tera Term (http://download.cnet.com/Tera-Term/3000-20432_4-75766675.html) 和 PuTTY (www.putty.org)。

注意：默认情况下，Windows 7 中的命令提示符不提供 Telnet。要在命令提示符窗口中启用 Telnet，请单击**开始 > 控制面板 > 程序 > 程序和功能 > 打开或关闭 Windows 功能**。单击“**Telnet 客户端**”复选框，然后单击“**确定**”。

第 1 步：捕获数据

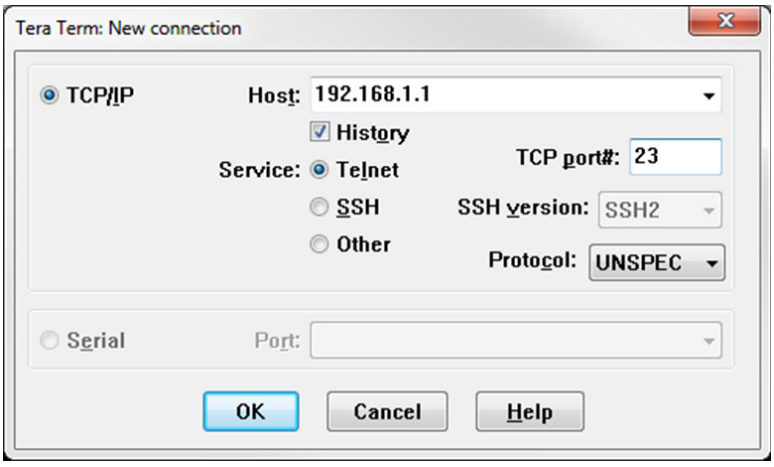
a. 启动 Wireshark。

b. 在 LAN 接口开始捕获数据。

注意：如果您无法在 LAN 接口上开始捕获，则可能需要使用 **Run as administrator**（以管理员身份运行）选项打开 Wireshark。

第 2 步：开始通过 Telnet 会话访问路由器。

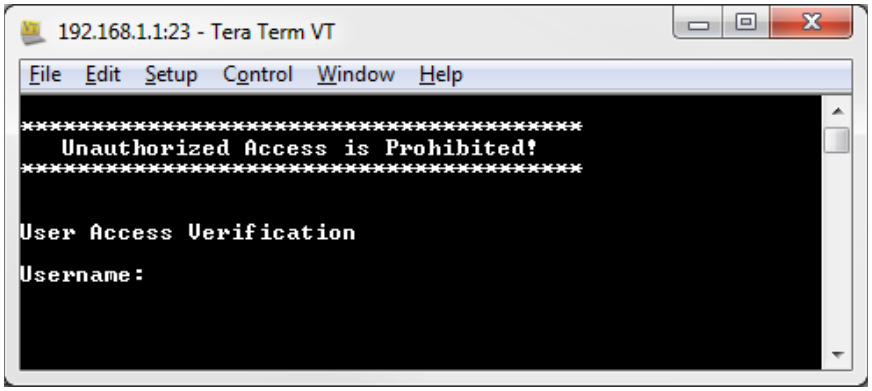
a. 打开 Tera Term 并选择 **Telnet** Service（Telnet 服务）单选按钮，然后在 Host（主机）字段中，输入 **192.168.1.1**。



什么是 Telnet 会话的默认 TCP 端口？

© 2015 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

b. 在 Username:（用户名：）提示符下，输入 **admin**，然后在 Password:（密码:）提示符下，输入 **adminpass**。之所以生成这些提示符是因为您使用 **login local** 命令将 VTY 线路配置为使用本地数据库。



c. 发出 **show run** 命令。

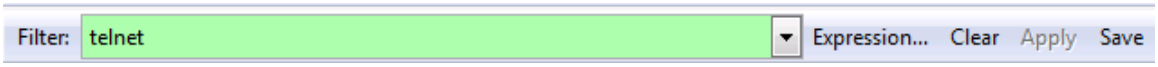
```
R1# show run
```

d. 输入 **exit** 退出 Telnet 会话并退出 Tera Term。

```
R1# exit
```

第 3 步：停止 Wireshark 捕获。

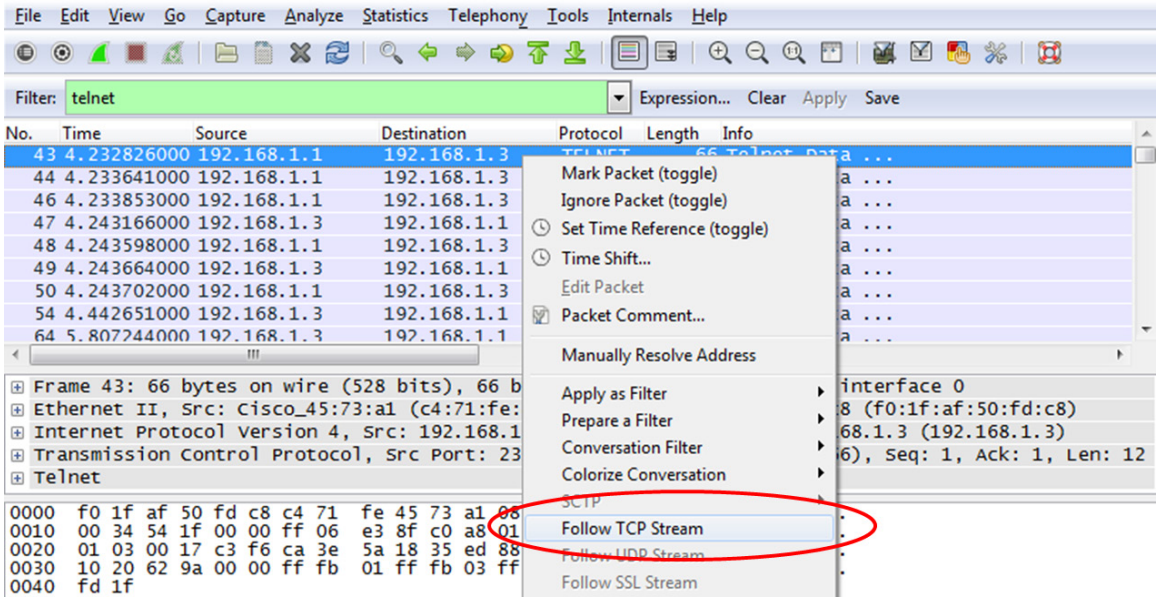
第 4 步：对 Wireshark 捕获数据应用 Telnet 过滤器。



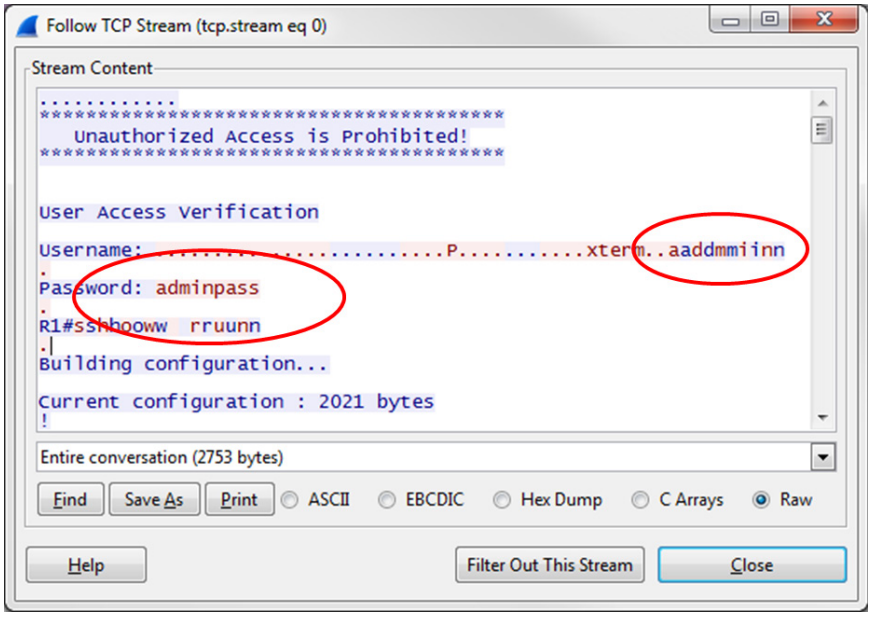
© 2015 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

第 5 步： 在 Wireshark 中使用 Follow TCP Stream（按照 TCP 数据流）特性查看 Telnet 会话。

a. 在 Wireshark 的 **Packet list**（数据包列表）部分，右键单击一个 **Telnet** 线路，然后在下拉列表中，选择 **Follow TCP Stream**（按照 TCP 数据流）。



b. Follow TCP Stream（按照 TCP 数据流）窗口显示路由器中 Telnet 会话的数据。整个会话以明文显示，包括密码。注意：您输入的用户名和 **show run** 命令显示为重复字符。这是由 Telnet 中响应设置（允许您查看屏幕上输入的字符）造成的。



c. 在 **Follow TCP Stream**（按照 TCP 数据流）窗口中检查完您的 Telnet 会话后，请单击 **Close**（关闭）。

© 2015 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

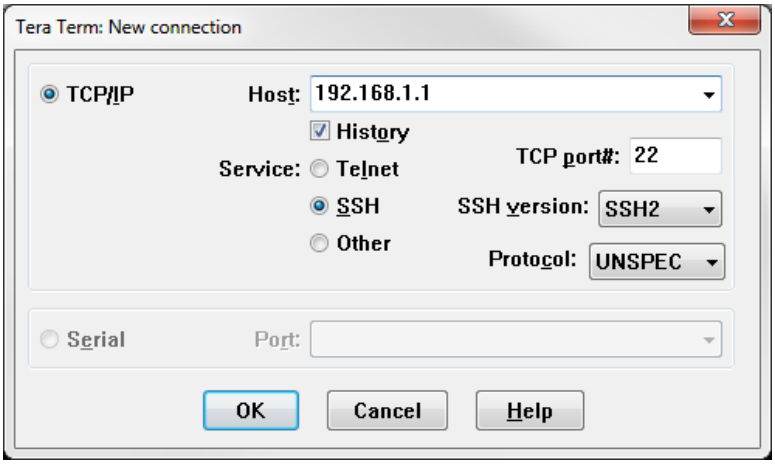
第 3 部分：通过 Wireshark 检查 SSH 会话

在第 4 部分中，您将使用 Tera Term 软件建立与路由器的 SSH 会话。我们将使用 Wireshark 来捕获和查看此 SSH 会话的数据。

第 1 步：打开 Wireshark 并在 LAN 接口开始捕获数据。

第 2 步：在路由器上启动 SSH 会话。

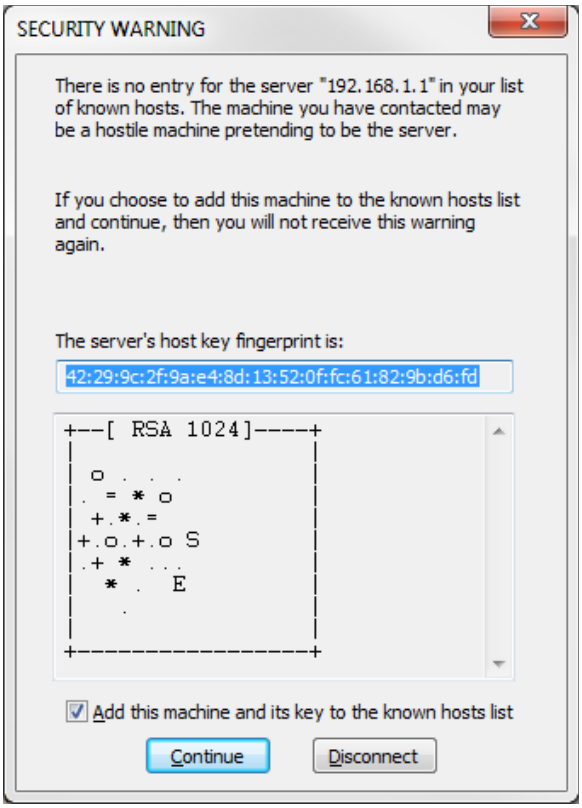
a. 打开 Tera Term 并在 Tera Term: New Connection（Tera Term: 新建连接）窗口的 Host:（主机:）字段中输入 R1 的 G0/1 接口 IP 地址。确保“**SSH**”单选按钮已选中，然后单击“**确定**”连接路由器。



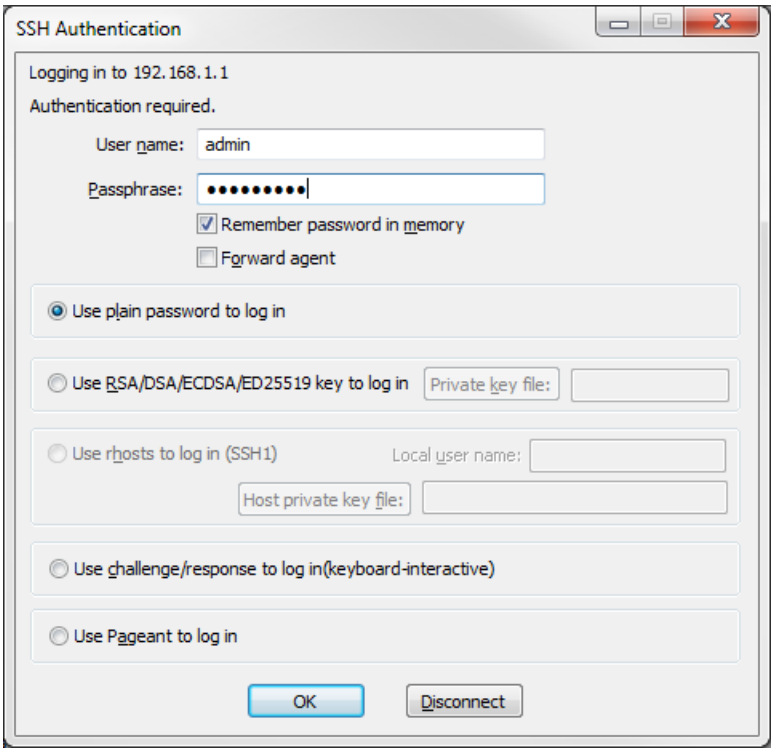
什么是 SSH 会话的默认 TCP 端口？

b. 首次建立到设备的 SSH 会话时，会生成**安全警告**，通知您之前未连接到此设备。此消息是身份验证过程的一部分。阅读安全警告消息并单击 **Continue**（继续）。

© 2015 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

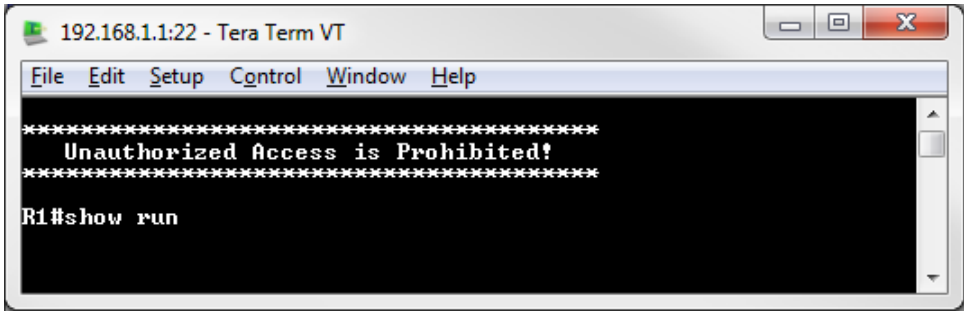


c. 在 SSH Authentication（SSH 身份验证）窗口中，输入用户名 **admin**，密码 **adminpass**。单击 **OK**（确定），登录路由器。



© 2015 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

d. 您已在路由器上建立了 SSH 会话。Tera Term 软件看起来很像命令窗口。在命令提示符下，发出 **show run** 命令。

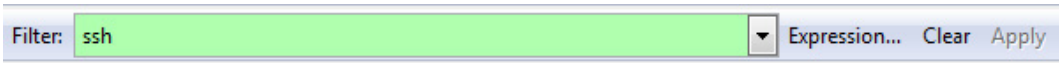


e. 发出 **exit** 命令退出 SSH 会话。

```
R1# exit
```

第 3 步： 停止 Wireshark 捕获。

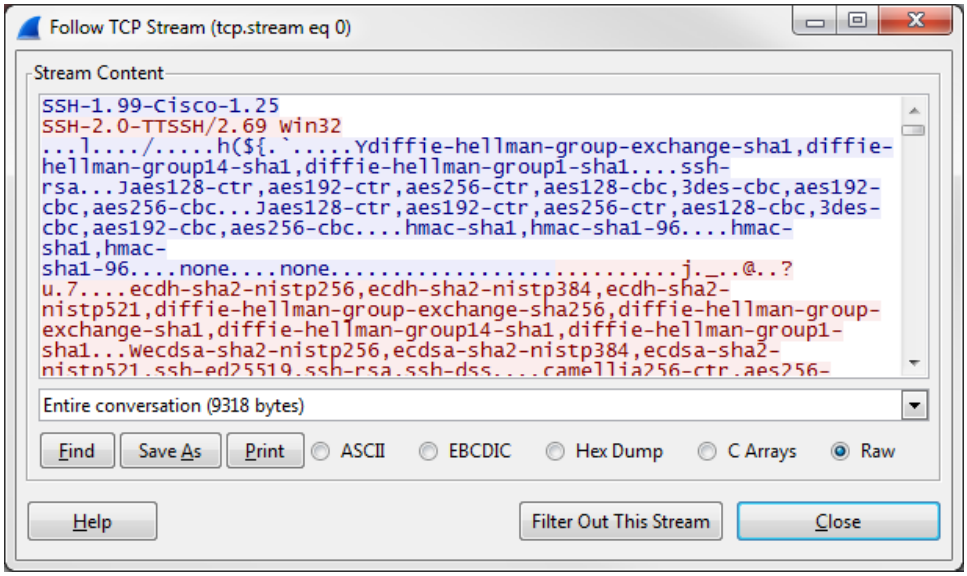
第 4 步： 对 Wireshark 捕获数据应用 SSH 过滤器。



第 5 步： 在 Wireshark 中使用 Follow TCP Stream（按照 TCP 数据流）特性查看 SSH 会话。

a. 在 Wireshark 的 **Packet list**（数据包列表）部分，右键单击一个 **SSHv2** 线路，然后在下拉列表中，选择 **Follow TCP Stream**（按照 TCP 数据流）选项。

b. 检查 SSH 会话的 **Follow TCP Stream**（按照 TCP 数据流）窗口。数据已加密，无法读取。将 SSH 会话中的数据与 Telnet 会话中的数据进行比较。



© 2015 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

进行远程连接时为什么首选 SSH，而不是 Telnet？

c. 检查您的 SSH 会话后，单击 **Close**（关闭）。

d. 关闭 Wireshark。

思考

您如何让多个用户（每个用户都有自己的用户名）来访问网络设备？

路由器接口摘要表

路由器接口摘要				
路由器型号	**以太网接口 1**	**以太网接口 2**	**串行接口 1**	**串行接口 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

注意：若要了解如何配置路由器，请查看接口来确定路由器类型以及路由器拥有的接口数量。我们无法为每类路由器列出所有的配置组合。下表列出了设备中以太网和串行接口组合的标识符。此表中未包含任何其他类型的接口，但实际的路由器可能会含有其他接口。例如 ISDN BRI 接口。括号中的字符串是约定缩写，可在 Cisco IOS 命令中用来代表接口。

© 2015 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。