

实验 - 使用 SSH 访问网络设备

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	未提供
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	网卡	192.168.1.3	255.255.255.0	192.168.1.1

目标

- 第 1 部分：配置基本设备设置
- 第 2 部分：配置路由器用于 SSH 访问
- 第 3 部分：通过 Wireshark 检查 Telnet 会话
- 第 4 部分：通过 Wireshark 检查 SSH 会话
- 第 5 部分：配置交换机用于 SSH 访问
- 第 6 部分：从交换机上的 CLI 执行 SSH

背景/场景

在过去，人们在远程配置网络设备时采用的网络协议一般都是 Telnet。但是，Telnet 这样的协议不会验证或加密客户端与服务器间发送的信息。这就让网络嗅探器有机可乘，能够截取口令和配置信息。

Secure Shell (SSH) 网络协议可以建立与路由器或其他网络设备的安全终端仿真连接。SSH 会对经过网络链路的所有信息进行加密，并验证远程计算机的身份。作为远程登录工具，越来越多的网络专家采用 SSH 来取代 Telnet。SSH 最常用于登录远程设备并执行命令；不过，它也可通过关联的 Secure FTP (SFTP) 或 Secure Copy (SCP) 协议传输文件。

要使用 SSH，相互通信的网络设备必须配置为支持该协议。在本实验中，您将在路由器上启用 SSH 服务器，然后使用装有 SSH 客户端的 PC 连接到该路由器。在本地网络上，该连接一般通过以太网和 IP 建立。

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。您还将面对自行配置交换机来接受 SSH 连接。

注意：CCNA 动手实验所用的路由器是采用 Cisco IOS Release 15.2(4)M3 (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 Cisco IOS 版本。根据型号以及 Cisco IOS 版本不同，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：确保所使用的路由器和交换机的启动配置都已擦除。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 台交换机（支持 Cisco IOS 15.0(2) lanbasek9 版映像的 Cisco 2960 或同类交换机）
- 1 台 PC（采用 Windows 7、Vista 或 XP 且支持终端仿真程序，比如安装有 Tera Term 和 Wireshark）
- 用于通过控制台电缆配置 Cisco IOS 设备的控制台端口
- 如拓扑图所示的以太网电缆

第 1 部分：配置设备的基本设置

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和交换机。

第 3 步：配置路由器。

- 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. 禁用 DNS 查找，以防路由器尝试将输入有误的命令视为主机名进行转换。
- d. 指定 **class** 作为特权 EXEC 加密密码。
- e. 指定 **cisco** 作为控制台密码并启用登录。
- f. 指定 **cisco** 作为 vty 密码并启用登录。
- g. 加密明文密码。
- h. 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。
- i. 使用地址分配表中包含的信息配置并激活路由器上的 G0/1 接口。
- j. 将运行配置保存到启动配置文件中。

第 4 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 5 步：检验网络连通性。

从 PC-A Ping R1。如果 ping 失败，请排除连接故障。

第 2 部分：配置路由器用于 SSH 访问

使用 Telnet 连接到网络设备具有很大的安全风险，因为所有信息都以明文格式发送。SSH 会加密会话数据并提供设备验证，这是推荐使用 SSH 进行远程连接的原因。在第 2 部分中，您将配置路由器通过 VTY 线路接受 SSH 连接。

第 1 步：配置设备身份验证。

生成加密密钥时，设备名称和域会用作加密密钥的一部分。因此，必须在发出 **crypto key** 命令之前输入这些名称。

- a. 配置设备名称。

```
Router(config)# hostname R1
```

- b. 配置设备的域。

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

第 2 步：配置加密密钥方法。

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

```
The name for the keys will be: R1.ccna-lab.com
```

```
% The key modulus size is 1024 bits
```

```
% Generating 1024 bit RSA keys, keys will be non-exportable...
```

```
[OK] (elapsed time was 1 seconds)
```

```
R1(config)#
```

```
*Jan 28 21:09:29.867: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

第 3 步：配置本地数据库用户名。

```
R1(config)# username adminprivilege 15 secret adminpass
```

```
R1(config)#
```

```
*Feb 6 23:24:43.971: End->Password:QHjxdsVkjtoP7VxKIcPsLdTiMIvyLkyjT1HbmYxZigc
```

```
R1(config)#
```

注意：权限级别 15 会授予用户管理员权限。

第 4 步：在 VTY 线路上启用 SSH。

- a. 使用 **transport input** 命令，在入站 VTY 线路上启用 Telnet 和 SSH。

```
R1(config)# line vty 0 4
```

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

- b. 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
```

```
R1#
```

第 5 步：将运行配置保存到启动配置文件中。

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

第 3 部分：通过 Wireshark 检查 Telnet 会话

在第 3 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)。

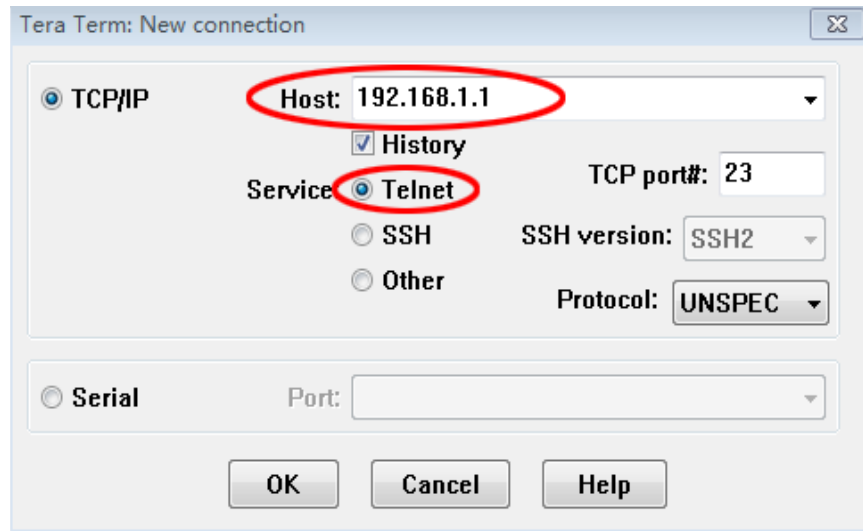
注意：默认情况下，Windows 7 中的命令提示符不提供 Telnet。要在命令提示符窗口中启用 Telnet，请单击开始>控制面板>程序>程序和功能>打开或关闭 Windows 功能。单击“Telnet 客户端”复选框，然后单击“确定”。

第 1 步：打开 Wireshark 并开始在 LAN 接口捕获数据。

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。

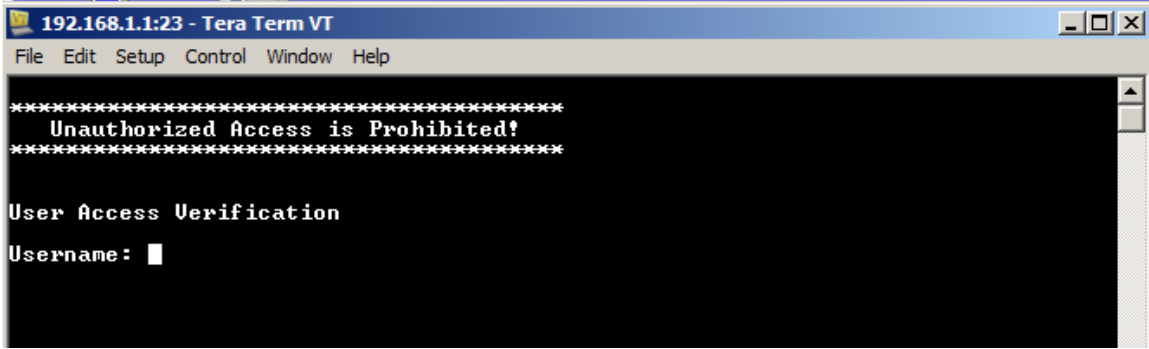
第 2 步：开始通过 Telnet 会话访问路由器。

- 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？ _____

- 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。



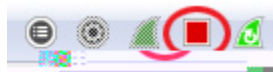
c. 发出 **show run** 命令。

```
R1# show run
```

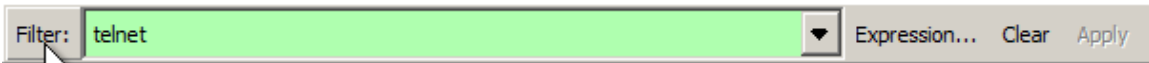
d. 输入 **exit** 退出 Telnet 会话并退出 Tera Term。

```
R1# exit
```

第 3 步：停止 Wireshark 捕获。

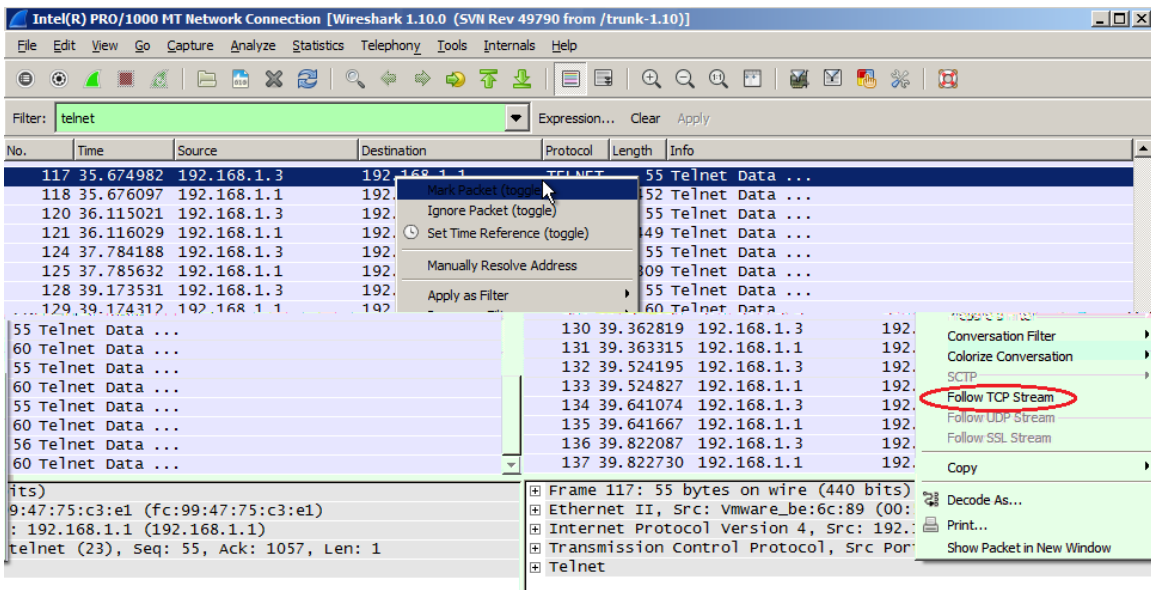


第 4 步：在 Wireshark 捕获数据上应用 Telnet 过滤器。

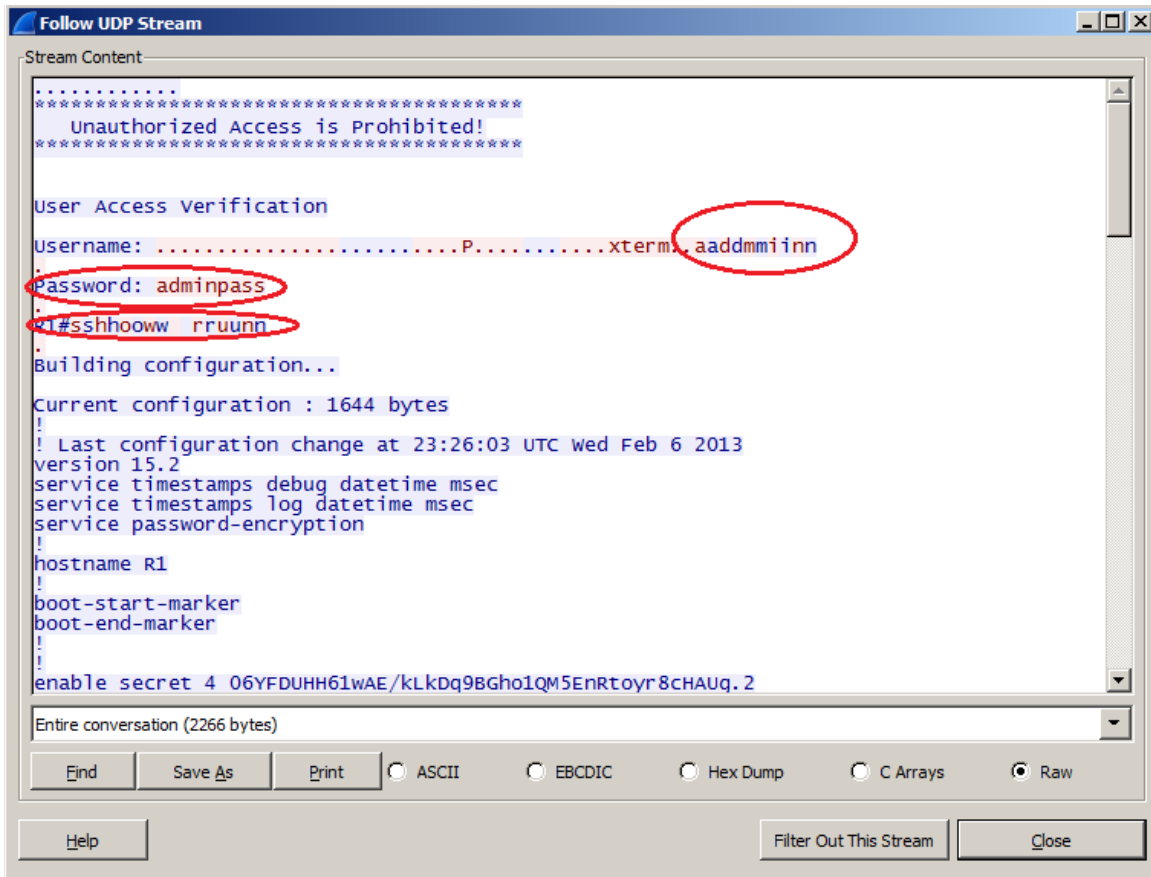


第 5 步：使用 Wireshark 中的 Follow TCP Stream 功能查看 Telnet 会话。

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)。

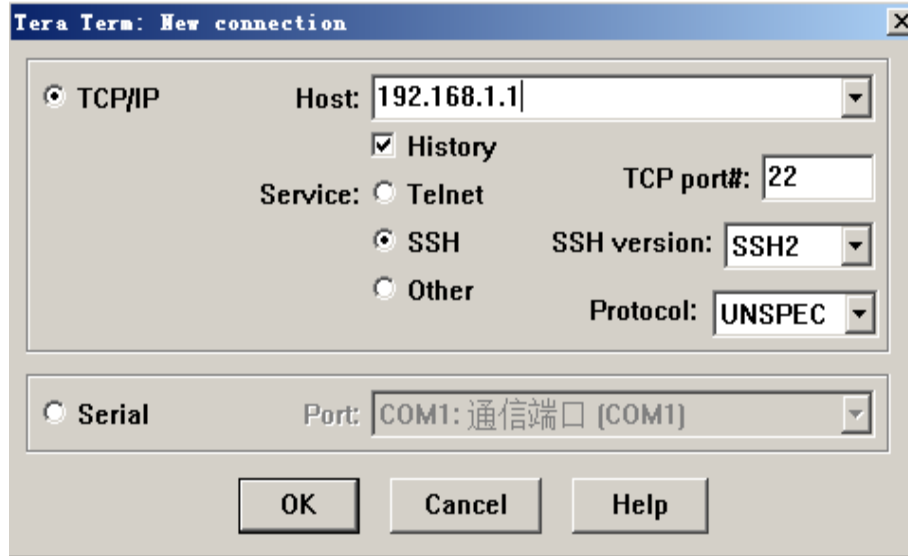
第 4 部分: 通过 Wireshark 检查 SSH 会话

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 并开始 LAN 接口捕获数据。

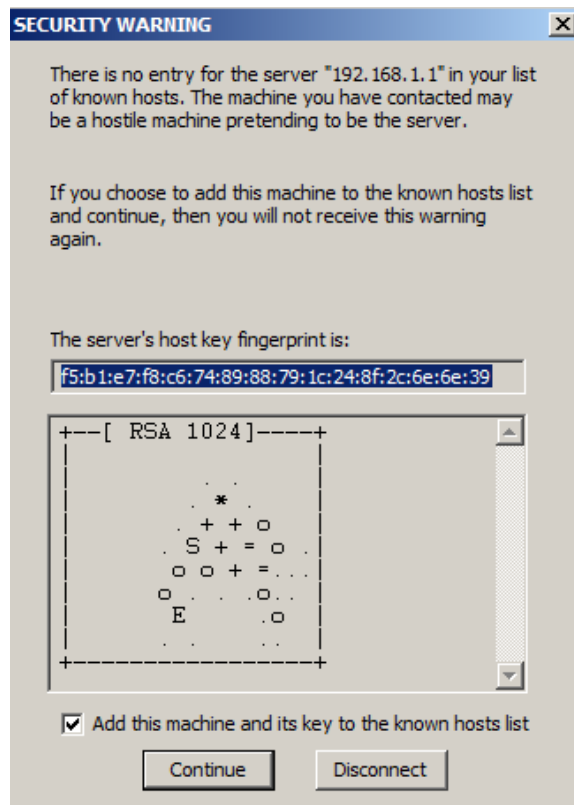
第 2 步: 在路由器上启动 SSH 会话。

- 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。确保选中 **SSH** 单选按钮, 然后单击 **OK** (确定) 连接到路由器。

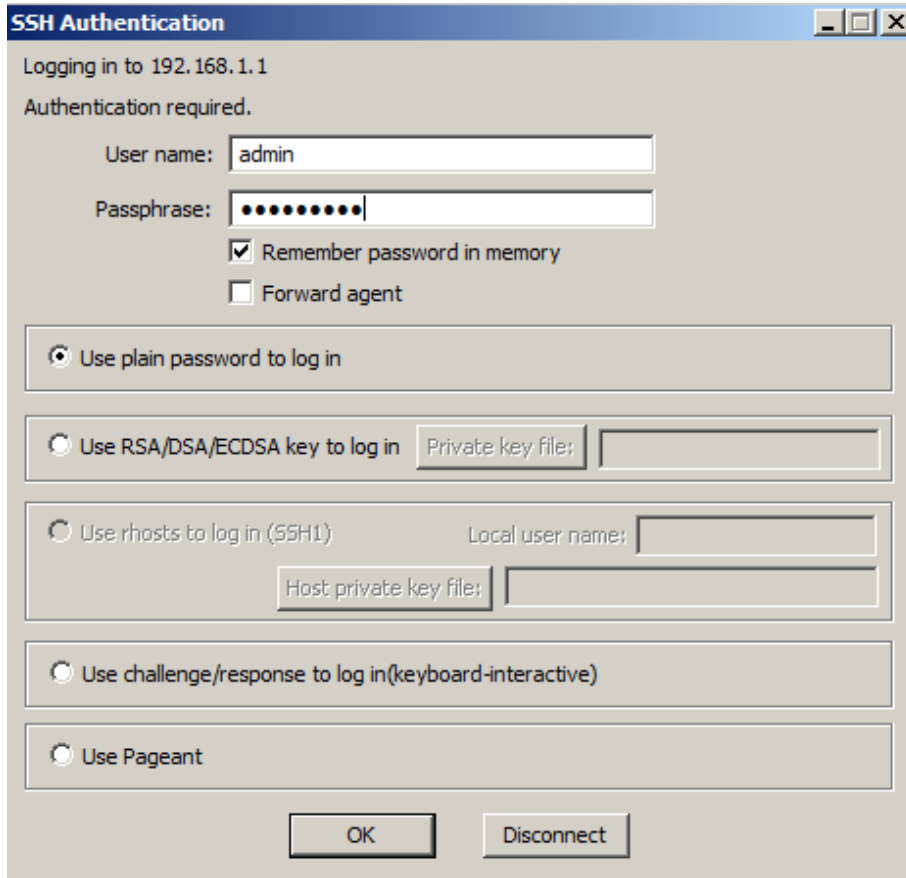


什么是 SSH 会话的默认 TCP 端口? _____

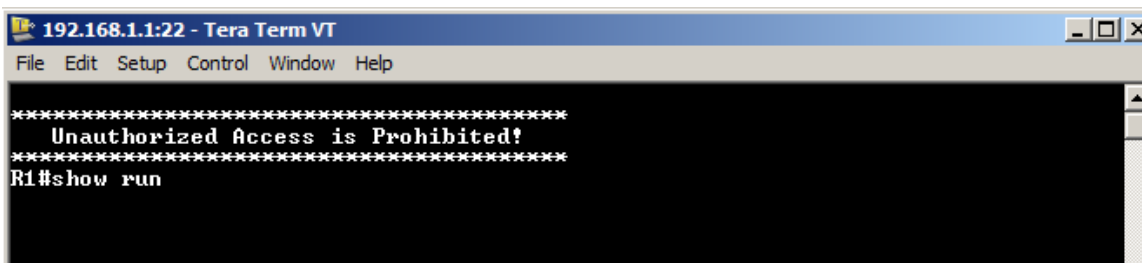
- b. 首次建立到设备的 SSH 会话时, 会生成**安全警告**, 通知您之前未连接到此设备。此消息是身份验证过程的一部分。阅读安全警告消息并单击 **Continue** (继续)。



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



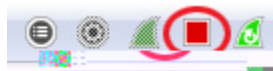
- d. 您已在路由器上建立了 SSH 会话。Tera Term 软件看起来很像命令窗口。在命令提示符下, 发出 **show run** 命令。



- e. 发出 **exit** 命令退出 SSH 会话和 Tera Term。

R1# **exit**

第 3 步: 停止 Wireshark 捕获。

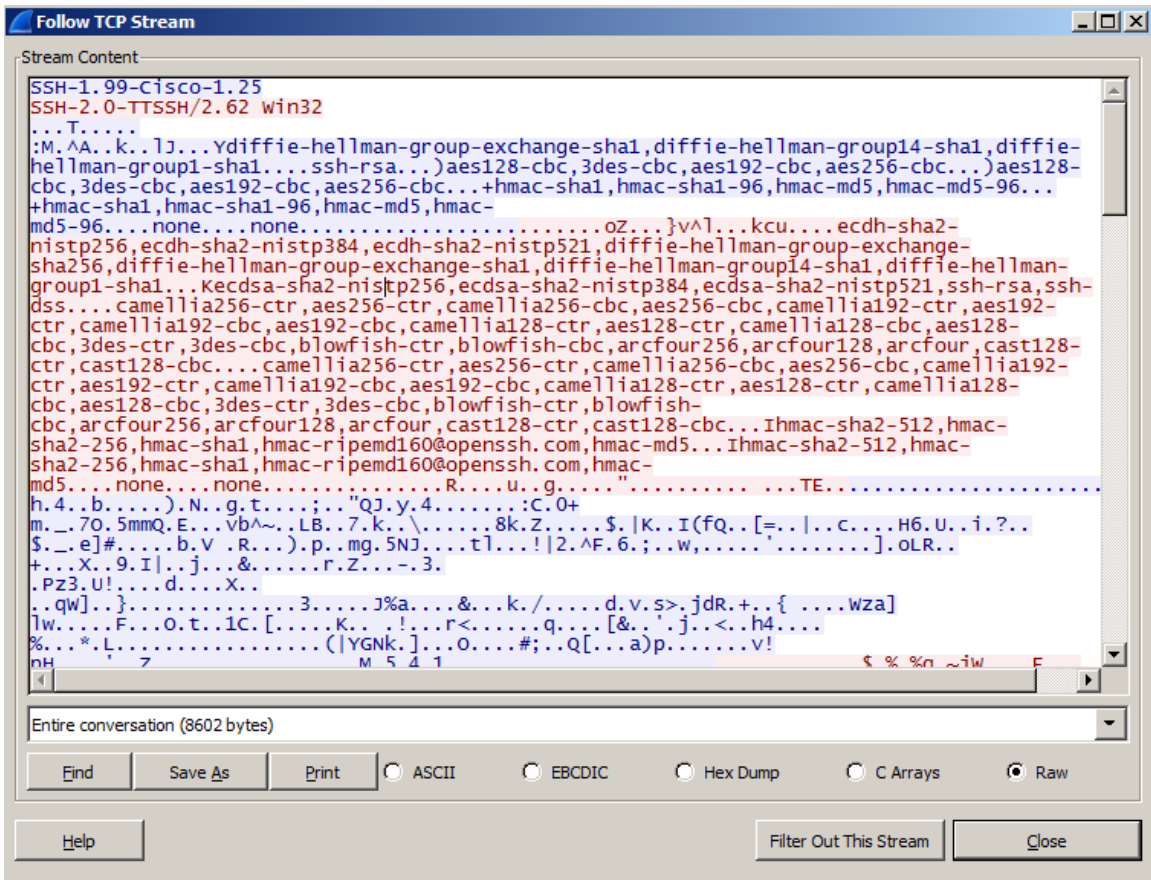


第 4 步：对 Wireshark 捕获数据应用 SSH 过滤器。



第 5 步：使用 Wireshark 中的 Follow TCP Stream 功能查看 Telnet 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。数据已加密和，无法读取。将 SSH 会话中的数据与 Telnet 会话中数据进行比较。



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，点击 **Close**（关闭）。
- d. 关闭 Wireshark。

第 5 部分：配置交换机用于 SSH 访问

在第 5 部分中，您将配置拓扑中的交换机以接受 SSH 连接。交换机配置完成后，您就可以使用 Tera Term 建立 SSH 会话。

第 1 步：在交换机上配置基本设置。

第 2 步：配置交换机接受 SSH 连接。

请使用第 2 部分中为路由器配置 SSH 时使用的命令来为交换机配置 SSH。

第 3 步：建立到交换机的 SSH 连接。

从 PC-A 启动 Tera，然后建立到 S1 上 SVI 接口的 SSH 连接。

第 4 步：根据情况进行故障排除。

您是否能建立与交换机的 SSH 会话？

第 6 部分：从交换机上的 CLI 建立 SSH 连接

Cisco IOS 内置有 SSH 客户端，可以从 CLI 运行。在第 6 部分中，您将从交换机的 CLI 建立到路由器的 SSH。

第 1 步：查看 Cisco IOS SSH 客户端可用的参数。

使用问号 (?) 可显示可供 **ssh** 命令使用的参数选项。

```
S1# ssh ?
  -c      Select encryption algorithm
  -l      Log in using this user name
  -m      Select HMAC algorithm
  -o      Specify options
  -p      Connect to this port
  -v      Specify SSH Protocol Version
  -vrf    Specify vrf name
  WORD    IP address or hostname of a remote system
```

第 2 步：从 S1 建立到路由器 R1 的 SSH。

- a. 在建立到 R1 的 SSH 时，您必须使用 **-l admin** 选项。这样您就可以作为用户 **admin** 登录。出现提示时，输入密码 **adminpass**。

```
S1# ssh -l admin 192.168.1.1
Password:
*****
Warning: Unauthorized Access is Prohibited!
*****

R1#
```

实验 - 使用 SSH 访问网络设备

- b. 您可以通过按下 **Ctrl+ Shift+ 6** 组合键返回到 S1，而无需关闭您与 R1 的 SSH 会话。按下 **Ctrl+Shift+6** 组合键并按下 **x**。您应该看到显示交换机特权 EXEC 提示符。

```
R1#  
S1#
```

- c. 要在 R1 上返回到 SSH 会话，请在空白 CLI 行按下 Enter 键。您可能需要再次按 Enter 键才能看见路由器 CLI 提示符。

```
S1#  
[Resuming connection 1 to 192.168.1.1 ... ]
```

```
R1#
```

- d. 要在 R1 上关闭 SSH 会话，请在路由器提示符下键入 **exit**。

```
R1# exit  
  
[Connection to 192.168.1.1 closed by foreign host]  
S1#
```

CLI 支持哪些版本的 SSH?

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	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #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。