

# Protocol Analysis: Telnet and SSH

## Objective:

Use protocol analyzer software to compare and contrast remote connections made to a computer using Telnet and Secure Shell (SSH).

## Background:

Protocol analysis software has a feature called capture. This feature allows all frames *through an interface* to be captured for analysis. In other words, if your software has an interface to an Ethernet LAN, your protocol analysis will involve only those frames seen on that LAN segment.

Protocol analyzers, such as Fluke's Protocol Expert and Ethereal, typically break down each frame into its component OSI layers. With this feature, one can actually examine the exchange of frames on the local network and the exchange of packets between networks. This ability aids in troubleshooting, development and education.

## Telnet Overview:

Telnet is an application layer protocol in the TCP/IP suite that supports remote terminal connections. It passes keystrokes from the local computer to the remote computer and displays output from the remote computer on the local computer. Traffic is relayed across the network in **plaintext**.

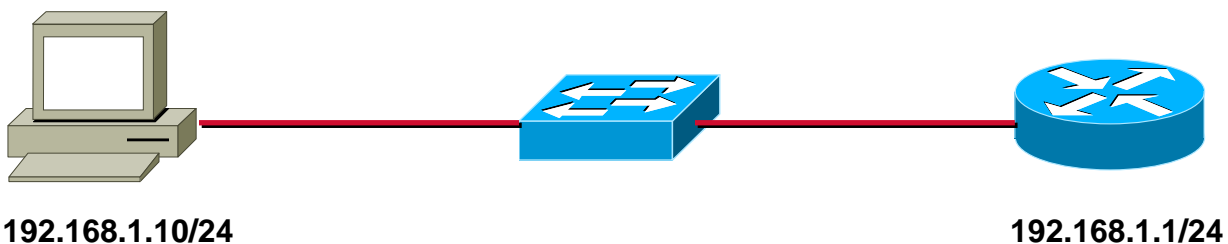
## Secure Shell (SSH) Overview:

SSH is a set of protocols that support **secure** remote terminal connections. It passes keystrokes from the local computer to the remote computer and displays output from the remote computer on the local computer. This protocol uses encryption such that traffic is relayed across the network in **ciphertext**.

## Tools / Preparation:

Assemble a small LAN that includes a computer workstation and a Cisco 2600 series router with an IOS that supports the SSH protocol. The LAN may be created using a crossover cable, a Layer 1 Ethernet hub, or a Layer 2 Ethernet switch. If using a switch, ensure that Spanning Tree Protocol (IEEE 802.1D) is disabled so as to reduce background traffic generated by the switch. This will simplify an analysis of this lab's traffic.

The workstation should include an O/S such as Windows 2000 with the Microsoft TCP/IP stack, a network protocol analysis tool such as the Fluke Protocol Expert or Ethereal, and an SSH client such as PuTTY. PuTTY is a free Telnet/SSH Client; documentation and download links may be found at <http://www.chiark.greenend.org.uk/~sgtatham/putty/>. Ethereal is open source; documentation and download links may be found at <http://www.ethereal.com/>.



## Procedure:

1. Configure the router.
  - a. Set up the router's name and domain. These will be used to name the encryption keys in a later step.
    - i. hostname **RemoteRTR**
    - ii. ip domain-name **analyze.net**
  - b. Set up the router's LAN interface.
    - i. interface fastethernet 0/0
    - ii. ip address **192.168.1.1 255.255.255.0**
    - iii. no shutdown
  - c. Set up the router's remote access ports to allow 'local authentication' using the Telnet and SSH protocols.
    - i. line vty 0 4
    - ii. login **local**
    - iii. transport input **telnet ssh**
  - d. Set up the router's local login ID's.
    - i. username **telnet** password **remote**
    - ii. username **ssh** password **remote**
  - e. Set up the router's encryption module to generate Rivest, Shamir, and Adleman (RSA) key pairs. This is a public (asymmetric) key cryptosystem that allows for the creation of a shared secret (symmetric) key without ever exposing the shared key over the network.
    - i. crypto key generate **rsa**
    - ii. When prompted, choose the default key modulus size: **512**
2. Configure the workstation's TCP/IP settings from:

**Start => Settings => Control Panel => Network and Dial-up Connections**

- a. Right click: **Local Area Connection**
- b. Select: **Properties**
- c. Select: **Internet Protocol (TCP/IP)**
- d. Select: **Properties**
- e. Set IP address to: **192.168.1.10**
- f. Set Subnet mask to: **255.255.255.0**
- g. Set Default gateway to: **192.168.1.1**
- h. Click: **OK**

3. Start the workstation's protocol analysis software. If using Fluke's Protocol Expert,
  - a. Start the data capture by clicking the **green triangular flag** located on the leftmost portion of the Protocol Expert's third toolbar.
  - b. Notice that the Protocol Expert's Monitor screen shows network utilization. This is the traffic being seen on the workstation's Ethernet NIC.
4. Establish a Telnet connection to the router by opening a command prompt on the workstation from:

**Start => Run**

- a. Type: **Command**
  - b. Click: **OK**
  - c. At the command prompt, enter **telnet 192.168.1.1**
  - d. At the 'username:' prompt, enter **telnet**
  - e. At the 'password:' prompt, enter **remote**
  - f. You should now see the router's command line interface (**RemoteRTR>**)
  - g. Enter the router command: **show users**
  - h. Note the **Line, User, and Location** information (*display may take a couple seconds*)
- 
5. Establish an SSH connection to the router from the workstation.
    - a. Start the workstation's PuTTY application.
    - b. On the PuTTY configuration window, select the **Session** category and enter the following under **Basic options for your PuTTY session**.
      - i. Host Name (or IP address): **192.168.1.1**
      - ii. Port: **22**
      - iii. Protocol: **SSH**
    - c. Select the **Open** button at the bottom of the PuTTY Configuration window.
      - i. If the router is set to use single-DES symmetric encryption (DES is relatively easy to break with today's computing power), the PuTTY console will issue a warning and ask if you want to proceed with the connection. Select: **Yes**
      - ii. When prompted with 'login as:' enter **ssh**
      - iii. When prompted for 'ssh@192.168.1.1's password:' enter **remote**
      - iv. You should now see the router's command line interface (**RemoteRTR>**)
    - d. Enter the router command: **show users**
    - e. Note the **Line, User, and Location** information (*display may take a couple seconds*)
-

6. Stop the workstation's data capture by clicking the **red square** on the Protocol Expert's third toolbar.
7. Prepare to examine the captured data by pressing the "**F9**" key twice. The Ethernet frames will be listed in the order seen on the workstation's NIC. You may look at each frame by clicking on its line in the upper part of the data capture screen. The selected frame will then be decoded into its respective Open Systems Interconnect (OSI) model layers under the **Detail View** section below.
8. Select the first frame in which the **Summary** identifies it as carrying **TCP DP=23**.
9. From the **Data Link Control** decode section, record the Destination and Source **MAC addresses**. Destination: \_\_\_\_\_ Source: \_\_\_\_\_
10. MAC addresses are used to communicate on a Local Area Network (LAN). Identify who is talking to whom. (Hint: Open a new command prompt and enter **ipconfig /all** to see the workstation's MAC address. Enter **show interface fastethernet 0/0** from either the Telnet or SSH connections to see the router's MAC address).  
\_\_\_\_\_
11. From the **Ethernet Data Link Layer** decode, note the **Packet Type** being carried in this Ethernet Frame. \_\_\_\_\_
12. Internet Protocol (IP) is the Network Layer protocol used on the Internet. It provides the logical addressing scheme that allows for communication across networks.
13. From the **Internet Protocol** decode, record the Source and Destination addresses.  
Source: \_\_\_\_\_ Destination: \_\_\_\_\_  
Identify who is talking to whom. \_\_\_\_\_
14. Also from the Internet Protocol decode, identify the Transport Layer protocol being carried in this packet. (Hint: Its **ID type is 6**). \_\_\_\_\_
15. Transmission Control Protocol (TCP) is the reliable connection-oriented protocol used to transport data segments across the Internet.
16. From the **Transmission Control Protocol** decode, note the **Source** and **Destination Ports**. Source: \_\_\_\_\_ Destination: \_\_\_\_\_
17. The conversations of network applications are maintained and managed via port designations. Well-known applications have designated ports. What port is used to identify **Telnet traffic**? \_\_\_\_\_
18. As an aside, you may wish to examine the different **Flags** from the TCP decode. Along with the **Sequence** and **Acknowledgement Numbers**, these are used to establish and manage the reliable flow of data segments.
19. The **Data/FCS** decode provides a frame-level check, validating it against errors.

20. Now move to the frames in which the **Summary** identifies them as carrying **Telnet Data**. While selecting each in turn, examine the **TELNET** decode. What do you see?

---

---

---

---

---

---

21. Given the data stream you have just recorded, how secure do you feel about your **login ID, password** and the results of your **show users** command?

---

22. Now select the first frame in which the **Summary** identifies it as carrying **TCP DP=22**.

Record the following:

- a. Destination MAC \_\_\_\_\_
- b. Source MAC \_\_\_\_\_
- c. Packet Type \_\_\_\_\_
- d. Source IP \_\_\_\_\_
- e. Destination IP \_\_\_\_\_
- f. Protocol Type \_\_\_\_\_
- g. Source Port \_\_\_\_\_
- h. Destination Port \_\_\_\_\_

23. Given the forgoing information, identify who is talking to whom and what application data is being transported.

---

---

24. Knowing that you logged into the router using SSH after Telnet, you may surmise that **port 22 is SSH**. You may also recall that port 22 was set on your PuTTY console.

25. Now scroll through all the frames with port 22 identified as either the Destination (DP) or Source (SP). Do you ever find a SSH decode? \_\_\_\_\_

26. Please take some time to record your reflections from this lab.

---

---

---

---

---

---