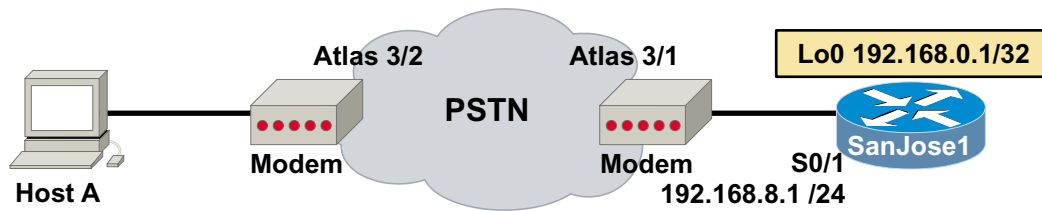


Lab 3.7.2: Configuring PPP Options: Authentication and Compression



Objective

In this lab, you will configure a Cisco router to accept PPP dial-up connections from a workstation using key PPP options: authentication and compression.

Scenario

The International Travel Agency wants you to configure dial-up access to the central router SanJose1 using PPP. In order to secure dial-up access, you are to configure authentication. Also, you have been asked to configure compression in order to maximize the amount of data that can be transferred across the link.

Step 1

Before beginning this lab, it is recommended that you reload the router after erasing its startup configuration. This will prevent you from having problems caused by residual configurations. Build and configure the network according to the above diagram, but do not configure SanJose1's serial interface yet. Configure SanJose1 with the appropriate hostname and IP addresses. Use the Adtran Atlas 550, or similar device, to simulate the PSTN. If you are using the Atlas 550, be sure the line cables from both modems are plugged into the respective octal FXS voice module ports of the Atlas 550 as labeled in the diagram.

Step 2

Configure SanJose1's serial interface for an asynchronous connection.

```
SanJose1(config)#interface s0/1
SanJose1(config-if)#physical-layer async
SanJose1(config-if)#async mode dedicated
SanJose1(config-if)#ip address 192.168.8.1 255.255.255.0
SanJose1(config-if)#peer default ip address 192.168.8.5
```

Remember, the **peer default ip address** command is used to automatically assign the dial-up host an IP address. Next, configure the line as shown:

```
SanJose1(config)#line 2
SanJose1(config-line)#login
SanJose1(config-line)#password cisco
SanJose1(config-line)#speed 115200
SanJose1(config-line)#flowcontrol hardware
SanJose1(config-line)#modem inout
```

```
SanJose1(config-line)#transport input all
SanJose1(config-line)#stopbits 1
```

Since you will be using Telnet and reverse Telnet during this exercise, configure the virtual terminals:

```
SanJose1(config-line)#line vty 0 4
SanJose1(config-line)#login
SanJose1(config-line)#password cisco
```

Step 3

Configure PPP to use PAP authentication using the following commands:

```
SanJose1(config-line)#interface s0/1
SanJose1(config-if)#encapsulation ppp
SanJose1(config-if)#ppp authentication pap
SanJose1(config-if)#exit
SanJose1(config)#username hosta password itsasecret
```

Recall that PPP supports two different authentication protocols, PAP and CHAP.

1. Which protocol, PAP or CHAP, is considered the most secure? Why?

When using PPP authentication, the router checks received username and password combinations against a database. In this exercise, the username and password database is stored locally on the router. The `username name password password` command is used to enter this local authentication information. In Lab 3.7.3, you will configure the router to use a non-local password/username database stored on a security server.

Step 4

Configure PPP to use compression, using the following commands:

```
SanJose1(config)#interface s0/1
SanJose1(config-if)#ppp compression stacker
```

The `ppp compression` command specifies the compression algorithm to use with PPP. Both link partners must be configured to use the same compression algorithm. In this case, you will configure PPP to use the stacker algorithm (sometimes called the Lempel-Ziv algorithm, or LZS). Stacker is CPU-intensive.

1. What other method of PPP compression is available?

You can also compress the headers of your TCP/IP packets in order to reduce their size, thereby increasing performance. Header compression is particularly useful on networks with a large percentage of small packets, such as those supporting many Telnet connections. This feature only compresses the TCP header, so it has no effect on UDP packets or other protocol headers. Enable TCP header compression with the following command:

```
SanJose1(config-if)#ip tcp header-compression
```

Note that TCP header compression is often referred to as Van Jacobsen (VJ) compression, after its inventor's name.

This completes the PPP configuration.

Step 5

Reverse Telnet to the modem, restore the modem's factory default settings (AT&F), configure the modem to answer on the second ring (ATS0=2), then disconnect the session. (Refer to Lab 3.7.1 for the procedure if necessary.)

At this point, you may want to reboot all of the lab equipment in order to prevent potential problems with residual configurations. Write SanJose1's configuration to NVRAM and reload the router, power cycle the modem, and power cycle the Adtran Atlas 550.

Step 6

Before configuring Host A's Dial-Up Networking, enable PPP debug on SanJose1's console using the following command:

```
SanJose1#debug ppp negotiation
```

After enabling debug, configure Dial-Up Networking on Host A to dial SanJose1. If you are using the standard Adtran Atlas 550 configuration, configure Dial-Up Networking to dial 555-6001, with the username hosta, and password itsasecret.

Be sure this connection is not configured to bring up a terminal window. From Host A, dial SanJose1. If the connection attempt fails, troubleshoot as necessary (you may have to repeat Step 5). Once you have connection successfully examine the debug output. SanJose1's output should include the following:

```
Se0/1 LCP: State is Open
Se0/1 PPP: Phase is AUTHENTICATING, by this end
Se0/1 PAP: I AUTH-REQ id 1 len 16 from "hosta"
Se0/1 PAP: Authenticating peer hosta
Se0/1 PAP: O AUTH-ACK id 1 len 5
Se0/1 PPP: Phase is UP
Se0/1 IPCP: O CONFREQ [Closed] id 8 len 16
Se0/1 IPCP: CompressType VJ 15 slots (0x0206002D0F00)
Se0/1 IPCP: Address 192.168.8.1 (0x03060A010101)
Se0/1 CCP: O CONFREQ [Closed] id 4 len 10
Se0/1 CCP: LZSDCP history 1 check mode SEQ process UNCOMPRESSED
(0x170600010201)
```

1. According to the debug output, who is the authenticating peer?

2. During the AUTHENTICATING phase, does the debug indicate the authentication protocol used?

3. What does CompressType VJ refer to?

4. What does LZSDCP refer to?

5. According to the debug output on SanJose1, during which PPP phase(s) are LCP frames exchanged?

6. According to the debug output on SanJose1, which kinds of NCPs were exchanged between Host A and SanJose1?

While Host A is still connected to SanJose1 (reconnect if necessary), issue the **show compress** command. A sample output is shown below.

```
SanJose1#show compress
Serial0/1
  Software compression enabled
  uncompressed bytes xmt/rcv 0/2357
  1 min avg ratio xmt/rcv 0.000/0.000
  5 min avg ratio xmt/rcv 0.000/0.000
  10 min avg ratio xmt/rcv 0.000/2.419
  no bufs xmt 0 no bufs rcv 0
  resyncs 0
Additional Stacker Stats:
Transmit bytes:  Uncompressed = 0 Compressed = 0
Received bytes:  Compressed = 564 Uncompressed = 0
```

7. According to the output of this command, is the compression method hardware or software-based?

Disconnect your dial-up session and redial using the wrong password. Leave the PPP debug running on SanJose1. The connection should fail.

8. What indications as to why the connection failed are included in the debug output's AUTHENTICATING PHASE?

