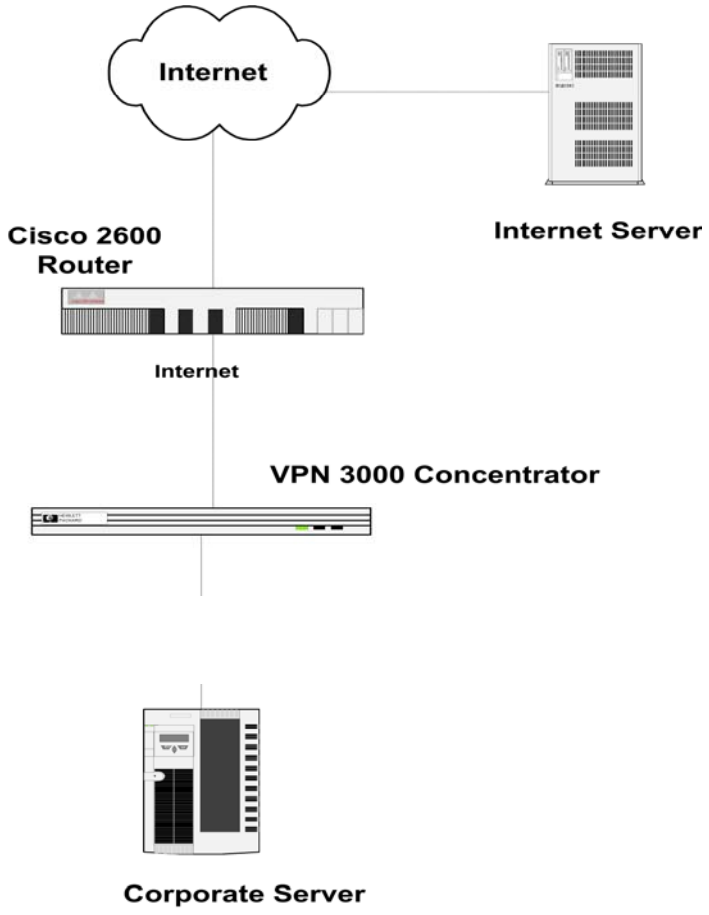
Lab Exercise – Configure Cisco VPN 3000 Concentrator

Objectives

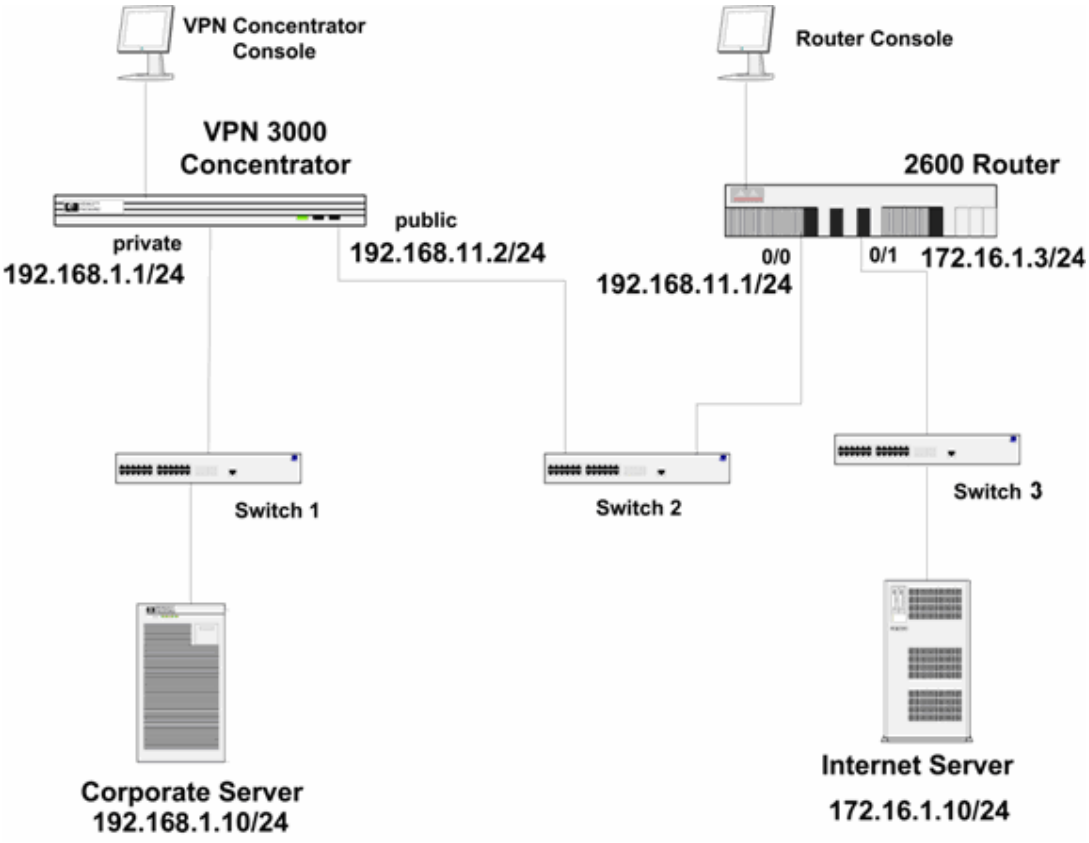
In this lab exercise you will complete the following three tasks:

- Task 1:
  - Configure the 2600 Router for Internet Access
  - Install and configure the Cisco VPN Client on Windows Client PC
  - Configure the Cisco VPN 3000 Concentrator using console and VPN manager

Visual Objective



Lab Setup Diagram



Scenario

Your company wants you and your team to provide a VPN solution using remotely located Cisco VPN Clients terminating at a centrally located Cisco VPN 3000 Concentrator. This will allow remote connection to the Corporate Server.

Note: Install Cisco VPN Client before starting this lab. The Cisco VPN Client (IPSec client) is typically installed from the Cisco VPN 3000 Concentrator series CDROM, using the instructions supplied with the CDROM. In this lab exercise, the source files for the Cisco VPN Client already reside on the hard disk drive of the "**Internet Server**" PC. Perform the common windows setup procedure to install the Cisco VPN Client.

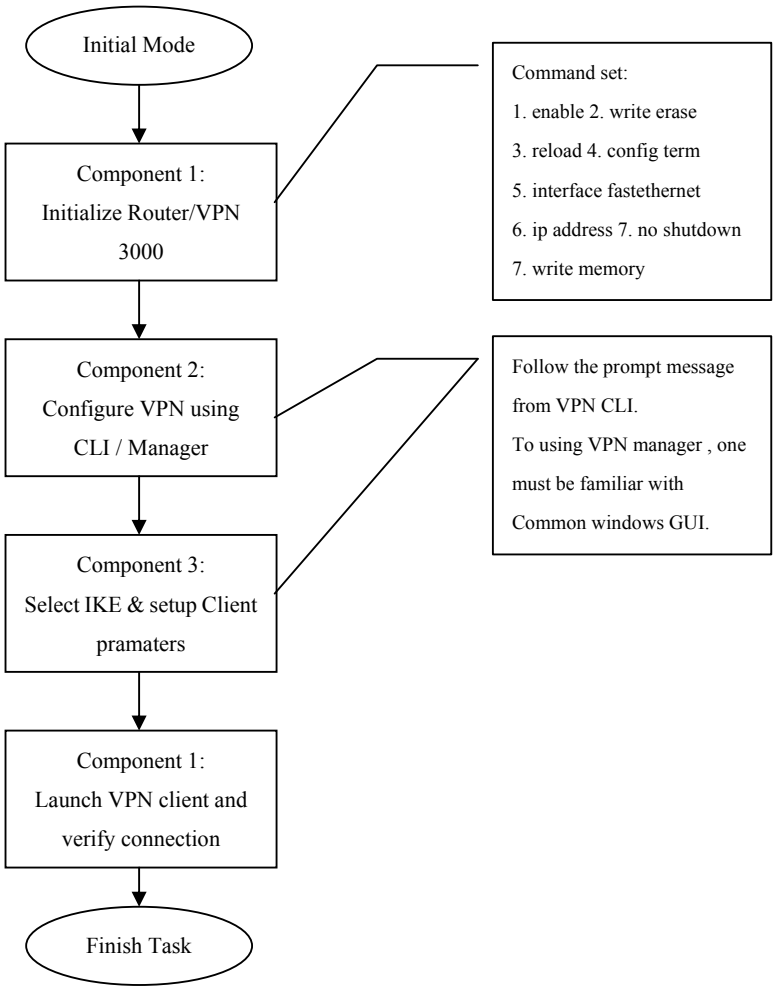
Network Parameters used in this Lab

	contents	***comments***
Internet Server	172.16.1.10	Subnet mask 255.255.255.0
2600 Router outside interface [fastethernet0/0]	192.168.11.1	Subnet mask 255.255.255.0
2600 Router inside interface [fastethernet0/1]	172.16.1.3	Subnet mask 255.255.255.0
VPN 3000 public interface	192.168.11.2	Subnet mask 255.255.255.0
VPN 3000 private interface	192.168.1.1	Subnet mask 255.255.255.0
Corporate Server	192.168.1.10	Subnet mask 255.255.255.0
Console prompt	router> OR router# OR router(config)#	router> initial mode router# enable mode router(config)# configuration mode
Ctrl+Z	backward to previous mode	
3000 Concentrator user_id/passwd	Admin/admin	
2600 Router passwd	None/none	

Task 1 – Configure the Cisco VPN 3000 Concentrator and a Cisco Router

Your task in this lab exercise is to install and configure the Cisco VPN Client and configure the Cisco VPN 3000 Concentrator to enable IPSec encrypted tunnels using pre-shared keys. To achieve the above goal, you need to go through several important components. First, you start configuring the HQ Router for basic connectivity and reload the Cisco VPN 3000 Concentrator to Factory Settings. Second, you need to configure the Cisco VPN 3000 Concentrator Private Interface using CLI (command line interface) and configure the VPN 3000 Concentrator using the VPN 3000 Concentrator Series Manager. Then, you should select the Cisco VPN 3000 Concentrator IKE Proposal and set up Client Parameters in the 3000 VPN Concentrator. Finally, you configure the Cisco VPN Client and launch the Cisco VPN Client and Verify Connection.

Task overview



Task 1.1: Reload router and VPN to manufactory settings.

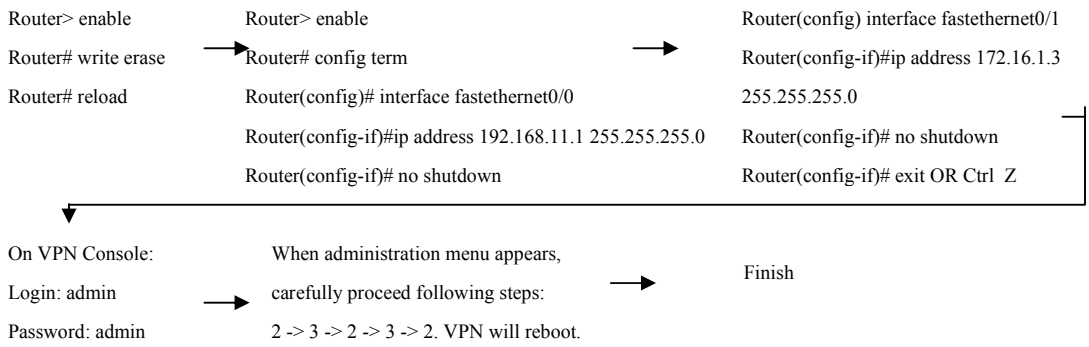
Configure the HQ Router for basic connectivity and reload the Cisco VPN 3000 Concentrator to Factory Setting.

Command description

	command	*command usage*	*comments*
Initialize Router/VPN	**enable**	VPN>enable	Switch pix to enable mode (VPN#)
	write	VPN# write erase	Erase previous configuration to default
	reload	VPN# reload	Reload basic manufacture setup routine.

	command	*command usage*	*comments*
	configure	VPN# configure term	Switch pix to configurable status.
	hostname	VPN# hostname *name*	Change the hostname to *name*

Configure Router & VPN step by step

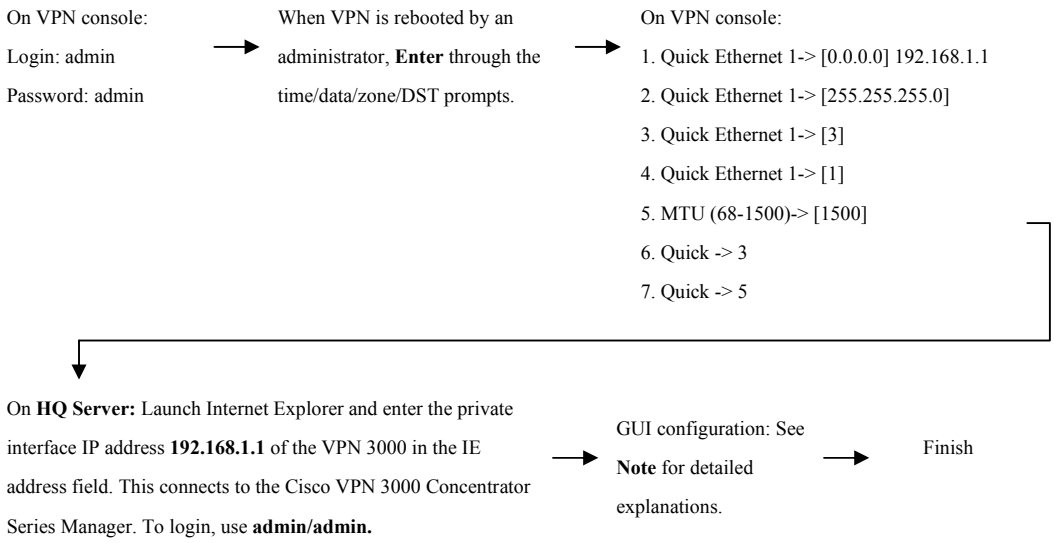


Note:

1. If you are prompted to enter the initial configuration dialog when configuring cisco router, enter NO.
2. To test the outside connectivity, using following command:
   a) Router# ping 172.16.1.10.
   b) You should be able to see the message like:

      "Success rate is 80 percent (4/5), round trip min/avg/max = 1/1/1 ms"

3. The Reboot scheduled immediately message appears followed by the Rebooting VPN 3000 Concentrator Series now message. Do not attempt to log into the first login prompt you see as it takes several moments for the Cisco VPN 3000 Concentrator to complete the reboot function. A login prompt appears when the reboot is complete.



Note:

1. The username (login) and password are always case sensitive.
2. In the main window, click "**click here to start Quick Configuration".**
3. From the Configuration-Quick-IP Interfaces window, complete the following sub-steps:
   a) Verify the IP addresses of Ethernet 1 (**192.168.1.1**)
   b) Click on the **Ethernet Interface 2 (Public),** Click on the **Static IP Addressing**, and then enter the IP address and mask to the boxes provided: 192.168.11.2|255.255.255.0
   c) Click the **Apply** button at the bottom of the page. Verify the IP addresses and click **Continue** if they are correct.
4. From the Configuration-Quick-System Info window, complete the following sub-steps:
   a) Enter **HQ** in the System Name field.
   b) Enter the correct time, date and time zone.
   c) Select or deselect the **Enable DST** Support check box.
   d) Leave the DNS Server IP Address field set to 0.0.0.0
   e) Enter **cisco.com** in the Domain field.
   f) Enter the perimeter router IP address of **192.168.11.1** in the Default Gateway field.
   g) Click **Continue**.
5. From the Configuration-Quick-Protocols window, complete the following sub-steps:
   a) De-Select the **PPTP** check box.
   b) De-Select the **L2TP** check box.
   c) Select the **IPSec** check box.
   d) Click Continue.
6. From the Configuration-Quick-Address Assignment window, complete the following sub-steps:
   a) Select **Configured Pool.**

b) Enter an IP address of **192.168.1.100** in the Range Start field.
c) Enter an IP address of **192.168.1.200** in the Range End field.
d) Click Continue.

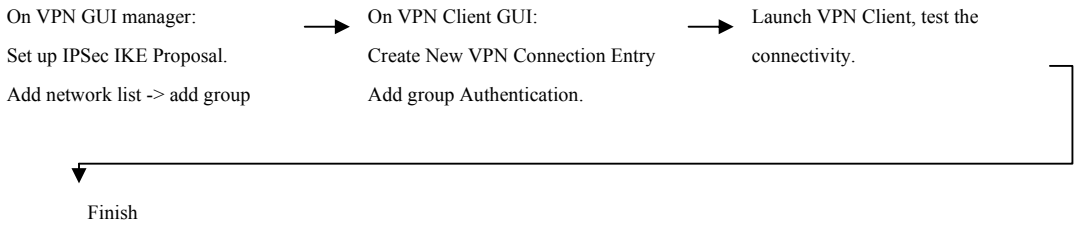
7. From the Configuration-Quick-Authentication window, complete the following:
   a) Choose **Internal Server** from the Server Type drop-down menu. Click Continue.

> **Note** You are setting up a pool of addresses to hand out to clients as they connect to the concentrator. You could also set up a DHCP Server to hand out the addresses, have the users specify their own address, or use an authentication server (like Cisco ACS) to hand out addresses

8. From the Configuration-Quick-User Database window, complete the following sub-steps:
   a) Enter **johnq** in the User Name field.
   b) Enter **johnq123** in the Password field.
   c) Enter **johnq123** in the Verify field.
   d) Click **Add** to add new user to the database. The new username should appear in the Current Users window. Click Continue.
9. From the Configuration-Quick-IPSec Group Window, complete the following sub-steps:
   a) Enter **hqclient** in the Group Name field.
   b) Enter **hqclient** in the password field.
   c) Enter **hqclient** in the Verify field. Click Continue.

> **Note** By choosing Internal, we can put username and passwords into the 3000 concentrator. This works great for small deployments, but in large deployments, you should use an external TACACS or RADIUS server like Cisco ACS. This sets up one group called hqclient. You can set up more groups later, and have different rights and parameters based on those groups.

Complete the following steps to setup the Cisco VPN 3000 Concentrator group parameters you set earlier. These settings will affect all clients that connect to this group:



Note:

1. To set the IPSec IKE Proposal:
   a) From the Configuration menu tree, drill down to **Configuration > System > Tunneling Protocols > IPSec > IKE Proposals**.

b) Ensure that the **CiscoVPNClient-3DES-MD5** proposal appears first under the Active Proposals list.
c) Always select the **CiscoVPNClient-3DES-MD5** when using the Cisco 3.x or 4.x VPN Client. Do not close IE.

2. Complete the following steps to setup the Cisco VPN 3000 Concentrator group parameters you set earlier. These settings will affect all clients that connect to this group:
   a) From the Configuration menu tree, drill down to the **Configuration>Policy Management>Traffic Management>Network Lists**. Click **Add** and type Tunnel in the List Name box. Then, type 192.168.1.0/0.0.0.255 in Network List box. At last, click **Add.**
   b) From the Configuration menu tree, drill down to **Configuration>User Management>BaseGroups.**
   c) Choose **hqclient** from the Current Groups list.
   d) Click **Modify Group**.
   e) Choose **Identity** tab. Verify that the Group Name is set to *hqclient*
   f) Choose the **General** tab. Verify that the Access Hours is set to No *Restrictions*.
   g) Choose the **IPSec** tab. Verify that the **Authentication** is set to *Internal*.
   h) Choose the **Client Config** tab. Scroll down and change **Split Tunneling Policy** to *Only tunnel networks in thelist*.
   i) Change **Split Tunneling Network List** to *Tunnel*.
   j) Choose the **Client FW** tab. Click **Apply**.
   k) Configure the user we created before by drilling down into the **Configuration>User Management>Users**.
   l) Highlight user **johnq**, and click **Modify**.
   m) Under **Group**, select the **hqclient** in the drop down box. Click **Apply.**
   n) Click on the **save needed** icon. Click **OK**.
3. Complete the following steps to configure the networking parameters if the new Cisco VPN Client:
   a) Choose Start**>Programs>Cisco Systems VPN Client>VPN Client**. The VPN Client window opens up.
   b) If there are any entries in the Connection Entry windows, select **Connection Entries>Delete**. Once the Connection box is empty, go to the next step.
   c) Click **New**. The Create New VPN Connection Entry window opens.
   d) Enter the following information at the top of the screen:
      i. Connection Entry: **HQ Connection**
      ii. Description: **Corporate Access**
      iii. Host: **192.168.11.2**
      iv. Click on the **Authentication** tab. Enter the following information under group Authentication: Name: **hqclient /** Password: **hqclient /** Confirm Password: **hqclient**
   e) Click on the **Transport** tab. Add a checkmark to the box next to **Allow Local LAN access**.
   f) Click **Save**. HQ Connection shows up in the Connection Entry Window.
4. Complete the following steps to launch the Cisco VPN client on the Internet Server.

a) If the Cisco VPN Client window is not already open, choose **Start>Programs>Cisco Systems VPN Client>VPN Client.**
b) Verify that the connection entry is the HQ Connection.
c) Highlight the HQ connection entry and click **Connect**. At the bottom of the VPN Client Window, several messages flash by quickly. Complete the following sub-steps:
   i. When prompted for a username, enter **johnq**.
   ii. When prompted for a password, enter **johnq123**.
   iii. Click **OK**. The following messages flash by quicky:

   You will see message like this:

```
Initializing the connection
Contacting the security gateway
Authenticating user
```

At this moment, you have successfully launched the Cisco VPN Client!

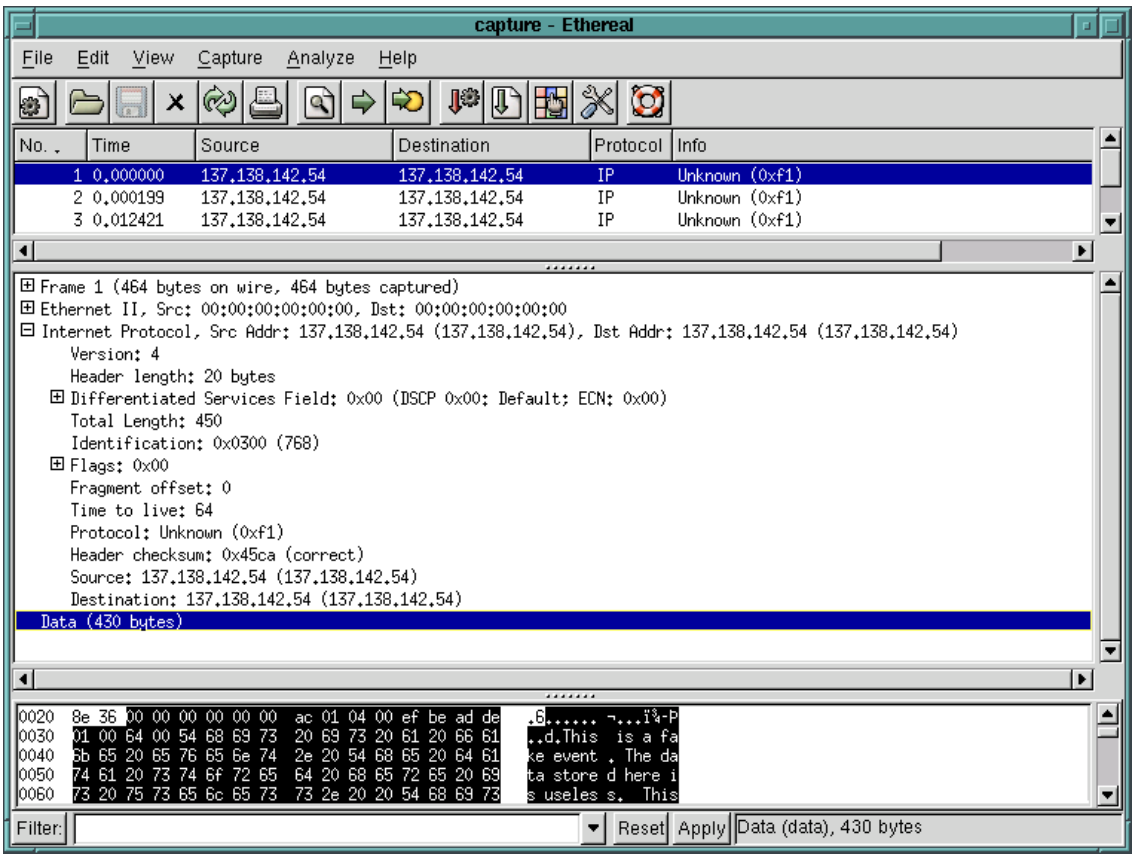
Extra Credit

If you wish, these steps will further your understanding of Virtual Private Networks. We are going to show how a VPN encrypts network traffic by running a telnet connection and sniffing the password. Telnet is a popular remote management program used to control a computer. **This extra credit starts after the router setup and before the VPN setup.**

Step 1 – After configuring the router, connect the **blue** cable from the switch to the corporate server.

Step 2 – Go to "SecurityOne"and on the desktop is the lab 4 folder. If you are not logged in, login using username: lab4 and the password: lab4. Double click on the Ethereal link. Ethereal is a program which scans all network traffic coming through it. It is connected to the monitor port on the switch, which copies all traffic and sends it to SecurityOne.

Step 3 – Ethereal should open up and display the main screen.



Step 4 – Go to Capture -> Start and press ok. Ethereal will begin capturing traffic running throughout the network.

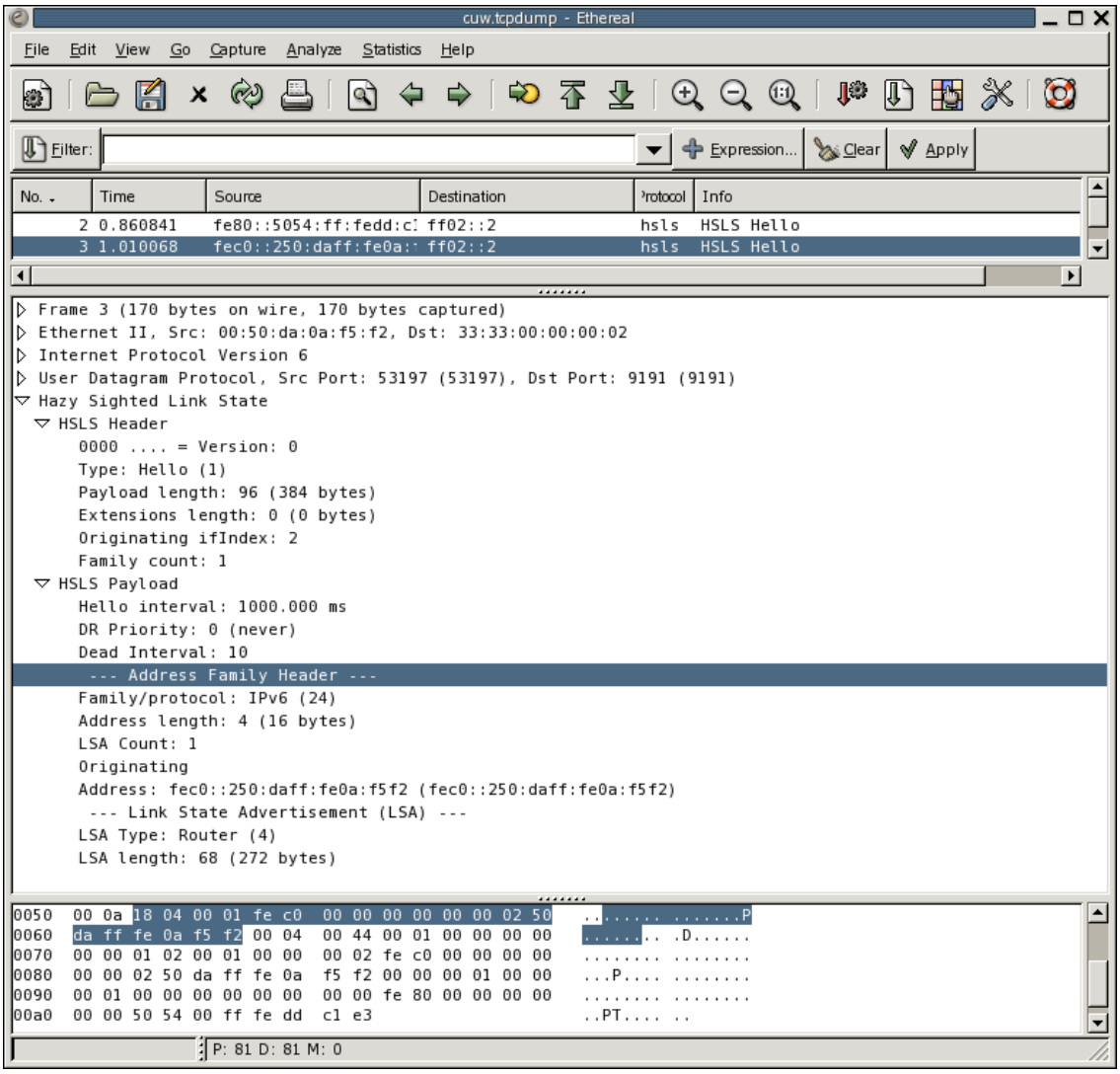
Step 5 – Now go back to your Internet Server machine and click Start -> Run -> and type "CMD". A command prompt window will open.

Step 6 – Type "Telnet 192.168.1.10"and press "y" when the screen asks you. Type the username "ISTStudent" and the password "DeanThomas." Don't worry if it tells you the password failed, this is just an example. Telnet is a utility that allows remote control of a computer.

Step 7 – Go back to SecurityOne and click "Stop Capture."

Step 8 – After stopping capture, under the protocol column should be different types of protocols listed, such as "ICMP," "TCP," etc. Look for "TELNET" protocol. You can sort the column by clicking on it.

Step 9 – Click on the line that mentions "TELNET" until it is highlighted. Then right click on the line, and select "Follow TCP Stream." What this does is it pieces together the packets sent back and force into a coherent conversation. You should see the password you typed in the following window. Take a screenshot of this by going to the top of the screen and selecting System -> Capture. An attacker could use this program to sniff your network and see all the traffic flowing through your network. We will see how a VPN will help in the following steps.



Step 10 – Connect the blue cable back to the VPN private port and continue the rest of the lab. Return here when you have set up the VPN and completed the lab.

Step 11 – Now run steps 2-9 again, but this time with the cable remaining connected to the VPN. When you check Ethereal, notice no Telnet packets have been detected. A VPN

encrypts the connection from end to end, so it keeps communication secure from anyone who is sniffing your traffic. The packets are actually encapsulated into the Cisco secure packet, which is why you can only see Cisco packets now. This completes the Extra Credit.

Report to deliver:

The group report is to show what you did in the project. Please clearly state your results of this project. You need to hand in a report in the following formats:

- A cover page (including project title) with group name and group members
- A table of contents with page numbers
- Using double-spaced typing for convenient grading
- Hard copies only, Font size 12, Single column
- A bound or stapled document, with numbered pages

The report should have the following sections. Each section has multiple items. You need to write a report section by section that covers all required items. However, you do not have to write the report item by item. Take screenshots if it is necessary.

Section I: Introduction:

You should have the following parts:

- Describe the goal and motivation of this project. In addition to what has been stated in the project instruction, please tell your own expectation in this project.
- Give an outline of this report, in which the content of each section needs to be briefly described.

Section II: VPN

You should have the following parts:

- Briefly describe the concept of VPN.
- Briefly describe the features that Cisco VPN has.

Section III: Task 1

You should have the following parts:

- Please describe how you construct the Network step by step in detail and in order. In order to show the detail of each step, for example, you need to describe which port of the switch you used, which interface in the router/pix you used, etc. You can take some snapshots of the screen to facilitate your description.
- After the Network is constructed, show the results you get from configuring the network. For example, what command you used, and what response you got? This may not be the same as you see in the lab document.

Section IV: Questions

1. What is the split tunneling policy?
   a. Traffic will not leave the network.
   b. Traffic will go directly to the Internet bypassing the VPN tunnel.
   c. Traffic will go through the VPN.
   d. All of the above is possible.
2. Which of the following configuration is possible using the Configuration menu tree?
   a. Users by using the User Management menu
   b. Groups by using the User Management menu

c. Network Lists by using the Traffic Management menu
d. All of the above

. 3. Why do we need different user groups for users of the VPN?
a. We like to give different names
b. We need different policies for different users
c. Users like to be part of the group
a. All of the above.

4. Which of the following about network lists is true.
b. The network lists menu may be reached using the Configuration menu tree.
c. A List name has to be provided
d. A range of IP addresses has to be provided
e. All of the above.

5. To access the PDM console, what type of communication is needed?
a. http
b. ftp
c. https
d. None of the above

Section V: Experiment Log

This part should describe your activities in this project.

- Clearly state the responsibility of each group member. If possible, give a table to tell who did which task, who collected information of which device, who wrote which part of the report, who coordinated the group work activities, etc.
- Give a log of your group activity, such as what you did on which day, and how many people attend.

Grading Rubric

This project has a number of specific requirements. The requirement for each section is documented in the above project instruction "Report to deliver". Whether you will get credits depends on the following situations:

- You will get full credits on one item, if it is correctly reported as required and well written.
- You will get half credits on one item, if it is reported as required but there is something definitely wrong.
- You will not get any credit for one item, if it is not reported.

The credits for each section are in the following. Each item in one section has equal credits.

1. Section I: Introduction (10%):

Each item has 5 credits.

2. Section II: VPN (25%):

First two items have 10 credits each; the third item has five credits.

3. Section III: Task 1(30%):

Each item has 15credits.

4. Section IV: Questions (25%)

Each question has 5 credits.

5. Section IV: Experiment log (10%)

- If you are responsible for some parts of your group work, you get 10 credits. If you do nothing for your group work, you get 0.
- If you attend more than 90% of your group activities, you get 10 credits. If you attend between 70% and 90%, you get 7 credits. If you attend between 50% and 70%, you get 5. Otherwise, you get 0.

Note

This is a group project. Only hard copies of the report will be accepted. Be sure to include the names of all the teammates and email addresses in the report. The report should be turned in before class on the specified due date. Late grade will be deducted in case the submission is not made on time and prior permission is not obtained from the Dr Liu for submitting later than the specified due date.