Trademarks

Any brand names and product names included in this manual are trademarks, registered
trademarks, or trade names of their respective holders.

To the Holder of the Manual

The contents of this manual are current as of the date of publication. ADTRAN reserves the
right to change the contents without prior notice.

In no event will ADTRAN be liable for any special, incidental, or consequential damages or for
commercial losses even if ADTRAN has been advised thereof as a result of issue of this
publication.
Customer Service, Product Support Information, and Training

ADTRAN will replace or repair this product within five years from the date of shipment if the product does not meet its published specification, or if it fails while in service.

A return material authorization (RMA) is required prior to returning equipment to ADTRAN. For service, RMA requests, training, or more information, see the toll-free contact numbers given below.

Presales Inquiries and Applications Support

Please contact your local distributor, ADTRAN Applications Engineering, or ADTRAN Sales:

- Applications Engineering  (800) 615-1176
- Sales  (800) 827-0807

Post-Sale Support

Please contact your local distributor first. If your local distributor cannot help, please contact ADTRAN Technical Support and have the unit serial number available.

- Technical Support  (888) 4ADTRAN

The Custom Extended Services (ACES) program offers multiple types and levels of service plans which allow you to choose the kind of assistance you need. For questions, call the ACES Help Desk.

- ACES Help Desk  (888) 874-2237

Training

The Enterprise Network (EN) Technical Training offers training on our most popular products. These courses include overviews on product features and functions while covering applications of ADTRAN’s product lines. ADTRAN provides a variety of training options, including customized training and courses taught at our facilities or at your site. For more information about training, please contact your Territory Manager or the Enterprise Training Coordinator.

- Training Phone  (800) 615-1176, ext. 7500
- Training Fax  (256) 963-6700
- Training Email  training@adtran.com
- Web Site  www.adtran.com/training
- Online Training  www.adranuniversity.com
NetVanta PowerPak Lab Guide Contents

NetVanta PowerPak Self Study Equipment List ......................................................... L-i
Lab 1: Configuring VLANs ..................................................................................... L1-1
Lab 2: IP Routing over Frame Relay ..................................................................... L2-1
Lab 3: IP Routing over PPP .................................................................................. L3-1
Lab 4: Internet Access ......................................................................................... L4-1
Lab 5: InterVLAN Routing .................................................................................. L5-1
Lab 6: IKE with Pre-shared Keys ......................................................................... L6-1
NetVanta PowerPak Lab #1

Exploring ADTRAN OS and Configuring VLANs

SETUP

- Connect the COM port on your PC to the CONSOLE port on the rear panel of the NetVanta 3448. Use a DB-9 (female) to DB-9 (male) straight-through serial cable.

- Open a VT-100 session with the NetVanta 3448. Use the HyperTerminal icon on your desktop with the following settings:
  - Baud Rate = 9600
  - Parity = None
  - Data Bits = 8
  - Stop Bits = 1
  - Flow Control = None

- Press <Enter> on the keyboard and the access prompt should appear. Enter into Enable Mode by typing 'enable' and factory default the NetVanta 3448 using the following commands:

  ```
  Router# erase startup-config // Erase start-up configuration file
  Router# reload // Reload/reboot the Switch
  
  Enter <n> for 'no' when asked if wanting to save system configuration.
  Enter <y> for 'yes' when asked if wanting to reboot system.
  ```

- Re-establish the connection and log back in to the Enable Mode.

- Locate the 8 switchports. Connect your PC to port 1.

- Disable routing for this lab. We will not be using the routing features in the 3448 in this lab. We will explore the routing features in future labs.

  ```
  Router#configure terminal
  Router(config)#no ip routing
  Router(config)#end
  Router#copy running-config startup-config
  ```
PART 1: EXPLORE THE ADTRAN OPERATING SYSTEM
The objective of this section of the Lab is to explore and become more comfortable with the ADTRAN OS Command Line Interface. Feel free to explore, experiment, and ask questions.

1. After connecting, press <Enter> on the keyboard to display the Router> prompt.

2. Type a “?” to display commands available in the current mode.
   
   `Router> ?`

3. Type `show ?` to display options available to the “show” command.
   
   `Router> show ?`

4. What firmware version is the NetVanta 3448 running?

5. Type `enable` to enter the Enable Mode.
   
   `Router> enable`

6. Type a “?” to display commands available in the Enable Mode.
   
   `Router# ?`

7. Type `configure terminal` to enter the Global Configuration Mode.
   
   `Router# configure terminal`

8. Type “?” to display commands available in this mode.
   
   `Router(config)# ?`

9. Change the hostname of the router to NetVanta 3448.
   
   `Router(config)# hostname NetVanta3448`
10. Change the enable password to adtran.

   NetVanta3448(config)# enable password adtran

11. Exit completely out of the NetVanta 3448 and then log back in to the Enable Mode.

   At what level are you prompted to enter a password?

12. Display the running-configuration that is stored in RAM. You should see the changes made to the hostname and enable password.

   NetVanta3448# show running-config

13. Save the current configuration.

   NetVanta3448# copy running-config startup-config
**Configuring VLANs**

In this lab, you will explore ADTRAN OS and configure the NetVanta 3448 for VLAN membership. You will configure the parameters of your management VLAN. You will segment your network traffic through VLANs. Using the VLAN troubleshooting tools, you will verify that your network is properly segmented.

**CONFIGURATION SUMMARY – Step by step instructions begin on next page**

- The IP address of your laptop should be 192.168.99.1XX where XX is your bench number (e.g. 101, 102, ..., 110, 111, etc.). The PC Subnet Mask will be 255.255.255.0

- Create a VLAN Database
  - VLAN 100 – Name, Sales
  - VLAN 200 – Name, Engineering

- Use VLAN 1 as the Management VLAN with an IP Address of 192.168.99.X /24, where X is your bench number (e.g. 1, 2, ... 10, 11, etc.).

- Assign VLANs to appropriate Ethernet Interfaces
  - VLAN 100 – Ethernet Ports 4-6
  - VLAN 200 – Ethernet Ports 7-8

- Verify Network Segmentation through VLANs.
CREATING THE VLAN DATABASE

14. Type `show run verbose` at the enable prompt to view the default Ethernet Port Configuration.

   NetVanta3448# show run verbose

15. Notice the default settings for interface switchports 0/1 through 0/8. What is the current mode: access or trunk? What VLAN is active on all ports?

16. There is more than one way to create VLANs. Create VLAN 100 and VLAN 200 to demonstrate two of the methods.

   Create VLAN 100 and name it Sales. Use the “?” to view other commands within the database.

   NetVanta3448#vlan database
   NetVanta3448(vlan)#vlan 100 name Sales
   NetVanta3448(vlan)#exit

   Create VLAN 200 and name it Engineering using a second method.

   NetVanta3448#configure terminal
   NetVanta3448(config)#vlan 200
   NetVanta3448(config-vlan 200)#name Engineering
   NetVanta3448(config-vlan 200)#end

   Do you remember another way to add VLANs? The commands in step 18 will create a vlan as well, if it doesn’t already exist.

17. View the newly created VLANs

   NetVanta3448#show vlan brief
18. Assign the appropriate VLANs to the correct switch ports as noted below in the chart.

   **Note:** Use the “range” keyword below to easily configure multiple interfaces simultaneously.

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Ethernet Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1-3</td>
</tr>
<tr>
<td>100</td>
<td>Ports: 4-6</td>
</tr>
<tr>
<td>200</td>
<td>Ports: 7-8</td>
</tr>
</tbody>
</table>

NetVanta3448# `configure terminal`
NetVanta3448(config)# `interface switchport 0/1`
NetVanta3448 (config-swx 0/1)# `switchport access vlan <vlan id>`
NetVanta3448 (config-swx 0/1)# `switchport mode access`

19. Type `show vlan` at the enable prompt to verify the changes you have made.

20. Configure the following IP Address scheme on your switch and PC.
    (interface VLAN 1 will be the management VLAN)

   - PC IP Address: 192.168.99.1XX
   - PC Subnet Mask: 255.255.255.0
   - Switch IP Address: 192.168.99.XX
   - Switch Subnet Mask: 255.255.255.0

   **Note:** When assigning a layer 3 address to one of the 8 switchports the IP address must be assigned to a vlan interface as shown below.

NetVanta3448(config)# `interface vlan 1`
NetVanta3448(config-intf-vlan 1)# `ip address 192.168.99.XX 255.255.255.0`
NetVanta3448(config-intf-vlan 1)# `no shut`
NetVanta3448(config-intf-vlan 1)# `end`

21. Verify that you can Ping your NetVanta 3448 from the PC command prompt.
22. Set-up Telnet Access to the NetVanta 3448. What parameters must be configured in order to telnet to the device? (See Module 3)

_____________________________________________________

_____________________________________________________

23. Verify that you are able to Telnet to the NetVanta 3448.

24. Move your PC to Switchport #4. Are you able to ping the PC from your switch? __________

25. Which port(s) must your PC be connected to on the switch to Telnet to the Switch? Why? ________________________________

26. Use the following command from the enable prompt to determine the VLAN settings for port #4:

   NetVanta3448#show interface switchport 0/4 switchport

27. What is the current output of this command?

   Name: _______________________________________________
   Switchport: ____________________________________________
   Administrative Mode: _________________________________
   Access Mode VLAN: ________________________________

28. Save your current settings to a file called VLANconfig.

   NetVanta3448#copy running-config VLANconfig
CONFIGURING TRUNKING

NOTE: You will need a partner for this part of the lab.

In this part of the lab, you will connect to your partner’s switch. By configuring a trunk between the switches, you will be able to extend the VLANs that you both have created.

29. Connect port 8 on your switch to port 8 on your partner’s switch.

30. From the switch command prompt, ping your partner’s switch. Were you successful? _______________________

31. From the PC’s command prompt, attempt to ping your partner’s PC. Were you successful? _______________________

32. Now, configure port 8 as a trunk port on BOTH switches.

   NetVanta3448#configure terminal
   NetVanta3448(config)#interface switchport 0/8
   NetVanta3448(config-swx 0/8)#switchport mode trunk

33. Now, attempt to ping from your PC to your partner’s PC. Were you successful? _______________________

L1-8   NetVanta PowerPak Course Guide
The following commands are used in this lab. Refer to them as needed.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>erase startup-config</td>
<td>Factory Defaults the Unit</td>
</tr>
<tr>
<td>show run verbose</td>
<td>Displays the current operating configuration and default settings. This file is stored in RAM</td>
</tr>
<tr>
<td>vlan database</td>
<td>Configure the VLAN Database Settings</td>
</tr>
<tr>
<td>vlan XXX name _______</td>
<td>Set the VLAN name field</td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters the Global Configuration mode.</td>
</tr>
<tr>
<td>show vlan</td>
<td>Displays all options available to the spanning-tree command</td>
</tr>
<tr>
<td>switchport access VLAN X</td>
<td>Sets the VLAN on an interface</td>
</tr>
<tr>
<td>Switchport mode access</td>
<td>Configures the Switchport Mode for VLAN Access vs. Trunking</td>
</tr>
<tr>
<td>interface vlan 1</td>
<td>Enters the VLAN Management Configuration Settings</td>
</tr>
<tr>
<td>ip address X.X.X.X X.X.X.X</td>
<td>Configures the IP Address for the Switch</td>
</tr>
<tr>
<td>no shut</td>
<td>Enables a particular interface</td>
</tr>
<tr>
<td>enable password adtran</td>
<td>Configures the password adtran for the enable prompt.</td>
</tr>
<tr>
<td>Line telnet 0 4</td>
<td>Configure Password settings for Line Telnet 0.</td>
</tr>
<tr>
<td>ping X.X.X.X</td>
<td>Allows you to ping a remote device</td>
</tr>
</tbody>
</table>
In this exercise you will configure the branch office NetVanta 3448 with a default route to the host site.

**CONFIGURATION SUMMARY** – Step by step instructions begin on next page

- T1: ESF/B8ZS
- Timing provided on the T1 circuit
- Data channels are DS0s 1-24
- Layer 2 Encapsulation: Frame Relay
- Frame Relay interface type is DTE
- Frame Relay LMI type is ANSI
- DLCI: 1XX (XX is your bench number / bench 1 = 101, bench 5 = 105, bench 12 = 112, etc.)
- IP address of your PC is 192.168.X.99 /24 (X is your bench number)
- The default gateway for the PC is 192.168.X.1 (X is your bench number)
- The VLAN IP address is 192.168.X.1 /24 (X is your bench number)
- The WAN IP address is 10.10.X.1 with a 30 bit mask. (X is your bench number)
- Default route to the host site
SETUP

- Disconnect the connection between your switch and your partner's switch. This lab does not require a partner.

- Connect your PC into switchport 1 on the back of the NetVanta 3448.

- Verify or change the IP address and default gateway of your PC.
  - IP address = 192.168.X.99 (X is the bench number).
  - Default gateway = 192.168.X.1 (X is the bench number).

Note: This is different from the previous lab. In the previous lab, partner benches needed to be on the same network. In this lab, each bench will be its own network.

- Factory default the NetVanta 3448 using the following commands:

  Router# erase startup-config // Erase start-up configuration file
  Router# reload // Reload/reboot the Switch

  Enter <n> for 'no' when asked if wanting to save system configuration.
  Enter <y> for 'yes' when asked if wanting to reboot system.

- Re-establish the connection and log back in to the Enable Mode.

- Connect the T1 circuit specified by the instructor to the 'WAN-T1' port of the NetVanta 3448. Use the cable specified by the instructor. In most cases, this will be your gray network T1 cable connecting to the bench jack labeled 'T1'.
CONFIGURE THE VLAN INTERFACE

1. Enter the Global Configuration mode.
   
   NetVanta3448# configure terminal

2. Type `interface vlan 1` to access the configuration parameters for the VLAN interface.
   
   NetVanta3448(config)# interface vlan 1

3. Display commands available in this mode.
   
   NetVanta3448(config-intf-vlan 1)# ?

4. Assign an IP address of `192.168.X.1` and a 24-bit subnet mask to the VLAN Interface.  
   (X is your unit number)
   
   NetVanta3448(config-intf-vlan 1)# ip address 192.168.X.1 255.255.255.0

5. Activate the VLAN interface.
   
   NetVanta3448(config-intf-vlan 1)# no shutdown

6. Return to the Global Configuration Mode.
   
   NetVanta3448(config-intf-vlan 1)# exit

7. Type `exit` again to exit the Global Configuration Mode.
   
   NetVanta3448(config)# exit

8. Verify that the Ethernet interface is up.
   
   NetVanta3448# show interface switchport 0/1

9. Using `ping`, test the connectivity from the switch/router to your PC.
   
   NetVanta3448# ping 192.168.X.99 (X is your unit #)
   
   Were you successful? (Y/N) ________  If not, verify cabling and steps above.
CONFIGURE THE T1 INTERFACE

10. Configure and enable the T1 (DS1) interface using default T1 configuration parameters, timing from the circuit, and channels 1 through 24.

   NetVanta3448# configure terminal
   NetVanta3448(config)# interface t1 1/1
   NetVanta3448(config-t1 1/1)# tdm-group 1 timeslots 1-24
   NetVanta3448(config-t1 1 1/1)# no shutdown

11. From the current interface mode, verify that the T1 circuit is up and not in alarm.

   NetVanta3448(config-t1 1/1)# do show int t1 1/1

CONFIGURE THE FRAME RELAY INTERFACE

12. Configure and enable frame relay virtual interface 1 with an interface type of DTE and LMI-type of ANSI.

   NetVanta3448(config-t1 1/1)# interface fr 1
   NetVanta3448(config-fr 1)# frame-relay intf-type dte
   NetVanta3448(config-fr 1)# frame-relay lmi-type ansi

13. Create a frame relay sub-interface and assign your DLCI to this interface.

   DLCI #: 1XX (XX is your unit number / unit 1=101, unit 5=105, unit 12=112)

   NetVanta3448(config-fr 1)# interface fr 1.1XX
   NetVanta3448(config-fr 1)# frame-relay interface-dlci 1XX

14. Assign an IP address of 10.10.X.1 and a 30-bit subnet mask to the frame relay sub-interface. (X is your unit number)

   NetVanta3448(config-fr 1.1XX)# ip address 10.10.X.1 255.255.255.252

15. Cross-connect the T1 interface to the frame relay virtual interface.

   NetVanta3448(config-fr 1.1XX)# cross-connect 1 t1 1/1 1 fr 1

NOTE: You will not have context sensitive help for this command, unless you exit from interface configuration to global configuration mode.
16. From the Privileged mode, display the PVC statistics.

   NetVanta3448# **show frame-relay pvc**

CREATE A DEFAULT ROUTE

17. Enter the Global Configuration Mode.

18. Create a default route to the host router's WAN interface, which is connected via the frame relay link.

   NetVanta3448(config)# **ip route 0.0.0.0 0.0.0.0 frame-relay 1.1XX**
   
   (X is your unit number)
TEST THE CONNECTION

19. From the enable mode, display the contents of the IP routing table.

   NetVanta3448# **show ip route**

20. Ping a PC or router on one of the other networks.

   Router IP address: 192.168.X.1  (X is the unit number)
   PC IP address: 192.168.X.99

   Were you successful? (Y/N) __________  If not, verify cabling and steps above. Also verify that the bench you are trying to ping has completed these steps.

SAVE CONFIGURATION

21. Save the running configuration to the startup configuration.

   NetVanta3448# **copy running-config startup-config**

22. Type the following to create a backup copy of the running configuration to a file called baseline stored in FLASH.

   NetVanta3448# **copy running-config baseline**

   **The Configuration File ‘baseline’ Will Be Used in Future Labs.**

   **Note:** Type **show flash** to display the files in flash.
## COMMAND REFERENCE

The following commands are used in this lab. Refer to them as needed.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>Displays available commands</td>
</tr>
<tr>
<td>exit or logout</td>
<td>Exit from the basic or enable mode</td>
</tr>
<tr>
<td>show ?</td>
<td>Displays all options available to the show command</td>
</tr>
<tr>
<td>show version</td>
<td>Displays hardware and software status</td>
</tr>
<tr>
<td>enable</td>
<td>Turns on privileged commands</td>
</tr>
<tr>
<td>disable</td>
<td>Turns off privileged commands</td>
</tr>
<tr>
<td>con&lt;Tab&gt;</td>
<td>The &lt;Tab&gt; key will auto-complete the partially typed command</td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters the Global Configuration mode</td>
</tr>
<tr>
<td>hostname &lt;name&gt;</td>
<td>Defines the name of this router</td>
</tr>
<tr>
<td>enable password &lt;password&gt;</td>
<td>Assigns the privilege level password</td>
</tr>
<tr>
<td>show startup-config</td>
<td>Displays contents of the startup configuration. This file is stored in NVRAM</td>
</tr>
<tr>
<td>show running-config</td>
<td>Displays the current operating configuration. This file is stored in RAM</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>Saves the current configuration to the startup configuration (NVRAM)</td>
</tr>
<tr>
<td>reload</td>
<td>Halts and performs a cold restart</td>
</tr>
<tr>
<td>interface sw 0/1</td>
<td>Enters into the switchport slot 0, port 1 interface for further configuration</td>
</tr>
<tr>
<td>interface vlan 1</td>
<td>Enters into the interface for vlan 1 for further configuration</td>
</tr>
<tr>
<td>ip address A.B.C.D A.B.C.D</td>
<td>Sets IP address of this interface</td>
</tr>
<tr>
<td>no shutdown</td>
<td>Used to restore (turn on) the interface</td>
</tr>
<tr>
<td>exit</td>
<td>Exit from the EXEC mode</td>
</tr>
<tr>
<td>show interfaces switchport 0/1</td>
<td>Shows status and configuration of a specific interface</td>
</tr>
<tr>
<td>&lt;ctrl&gt; z</td>
<td>Exits completely out of the Configuration mode</td>
</tr>
<tr>
<td>ping A.B.C.D</td>
<td>Sends echo messages</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>interface t1 1/1</td>
<td>Enters T1 Interface Configuration Mode</td>
</tr>
<tr>
<td>tdm-group 1 timeslots 1-4</td>
<td>Defines a group of configured DS0s on this T1</td>
</tr>
<tr>
<td>clock source line</td>
<td>Recovers clock from the network</td>
</tr>
<tr>
<td>no shutdown</td>
<td>Turns on t1 interface slot 1 port 1</td>
</tr>
<tr>
<td>interface fr 1</td>
<td>Creates a FR virtual interface</td>
</tr>
<tr>
<td>frame-relay intf-type dte</td>
<td>Configures FR interface as user role</td>
</tr>
<tr>
<td>frame-relay lmi-type ansi</td>
<td>Defines signal type of this interface</td>
</tr>
<tr>
<td>no shutdown</td>
<td>Turns on the FR interface</td>
</tr>
<tr>
<td>interface fr 1.#</td>
<td>Creates a FR sub-interface</td>
</tr>
<tr>
<td>frame-relay interface-dlci #</td>
<td>Defines the DLCI # for this sub-interface</td>
</tr>
<tr>
<td>ip address A.B.C.D A.B.C.D</td>
<td>Sets IP address of this interface</td>
</tr>
<tr>
<td>cross-connect 1 t1 1/1 1 fr 1</td>
<td>Cross-connects TDM groups with other TDM groups or virtual interfaces</td>
</tr>
<tr>
<td>&lt;ctrl&gt; z</td>
<td>Exits completely out of the Configuration Mode</td>
</tr>
<tr>
<td>show frame-relay pvc</td>
<td>FR PVC statistics</td>
</tr>
<tr>
<td>ip route 0.0.0.0.0.0.0.0 X.X.X.X</td>
<td>Sets a default route to X.X.X.X</td>
</tr>
<tr>
<td>show ip route</td>
<td>Displays entries in the route table</td>
</tr>
<tr>
<td>copy running-config “filename”</td>
<td>Saves the current configuration to a file in flash</td>
</tr>
</tbody>
</table>
NetVanta PowerPak Lab #3  
*IP Routing over PPP*

**DESCRIPTION**  
In this lab, you will configure a point to point connection. This lab requires a partner. Unit 1 will connect to Unit 2. Unit 3 will connect to Unit 4. Unit 5 will connect to Unit 6. Unit 7 will connect to Unit 8. Also, we will create a static route to the LAN at the remote UNIT.

**Note:** This lab assumes that you have successfully completed Labs 1 and 2.

**CONFIGURATION SUMMARY – Step by step instructions begin on next page**

- T1: ESF/B8ZS
- Data channels are DS0s 1-24
- Layer 2 Encapsulation: PPP
- IP information for your PC will be 192.168.X.99 /24 with a default gateway of 192.168.X.1 (X is your Unit number). This should already be done.
- The VLAN Interface or Ethernet Interface IP address is 192.168.X.1 /24 (X is your Unit number). This should already be done.
- The WAN IP address is 10.10.10X.1 or 10.10.10X.2 with a 30 bit mask. (If your Unit number is odd, use 10.10.10X.1. If it is even, use 10.10.10X.2. X is the Odd Unit number. For example, Unit 3 and Unit 4 will connect. The WAN IP for Unit 3 will be 10.10.103.1. The WAN IP for Unit 4 will be 10.10.103.2.)
- Static route to the remote UNIT LAN.
SETUP

☐ Connect your PC into switchport 1 on the NetVanta 3448.

☐ Connect the T1 circuit specified by the instructor to the ‘WAN-T1/1’ port of the NetVanta 3448.

☐ Remove the Frame Relay interface and tdm-group statements from previous lab.

```
Router(config)# no interface frame-relay 1
Router(config)# int t1 1/1
Router(config-t1 1/1)# no tdm-group 1
Router(config-t1 1/1)# end
```

CONFIGURE THE T1 INTERFACE

1. Configure and enable the T1 (DS1) interface using default T1 configuration parameters and channels 1 through 24.

```
UnitX# configure terminal
UnitX(config)# interface t1 1/1
UnitX(config-t1 1/1)# tdm-group 1 timeslots 1-12
UnitX(config-t1 1/1)# no shutdown
```

2. From the current interface mode, verify that the T1 circuit is up and not in alarm.

```
UnitX(config-t1 1/1)# do show int t1 1/1
```

CONFIGURE THE PPP INTERFACE

3. Assign an IP address of 10.10.10X.1 or 10.10.10X.2 and a 30-bit subnet mask to the ppp interface. (Use 10.10.10X.1 if your Unit number is odd. Use 10.10.10X.2 if your Unit number is even.)

```
UnitX(config-ppp 1)# ip address 10.10.10X.1 255.255.255.252
(UnitX is the ODD Unit number)

UnitY(config-ppp 1)# ip address 10.10.10X.2 255.255.255.252
(UnitY is the EVEN Unit number)
```
4. Cross-connect the T1 interface to the frame relay virtual interface.

   UnitX(config-ppp 1)# cross-connect 1 t1 1/1 1 ppp 1
   UnitX(config-ppp 1)# end

NOTE: You will not have context sensitive help for the cross-connect command, unless you exit from interface configuration to global configuration mode.

5. From the Privileged mode, display the status of the PPP interface.

   UnitX# show interface ppp 1

CREATE A STATIC ROUTE

6. Enter the Global Configuration Mode.

7. Create a static route to the remote Unit router’s LAN through the PPP interface.

   For odd numbered Units:
   
   UnitX(config)# ip route 192.168.Y.0 255.255.255.0  ppp 1

   For even numbered Units:
   
   UnitY(config)# ip route 192.168.X.0 255.255.255.0  ppp 1

   (UnitX is the odd Unit number and UnitY is the even Unit number)

Y is the even Unit #
TEST THE CONNECTION

8. From the enable mode, display the contents of the IP routing table.

   UnitX# show ip route

   Do you have any entries for networks besides your own? (Y/N)__________

9. Ping the PC or router on the other network.

   Router IP address: 192.168.X.1  (X is the Unit number)
   PC IP address: 192.168.X.99

   _____________________________

   Were you successful? (Y/N)__________ If not, verify cabling and steps above. Also verify that the other Unit has completed these steps.

SAVE CONFIGURATION

10. Save the running configuration to the startup configuration.

   UnitX# copy running-config startup-config

   Do **Not** Copy This Configuration To ‘baseline.’
In this exercise you will configure the NetVanta 3448 to perform NAT on traffic originating on the internal network and destined for the Internet.

**CONFIGURATION SUMMARY – Step by step instructions begin on next page**

- This lab builds on the baseline configuration file that was saved in lab #2.
- The Ethernet IP address is 192.168.X.1 /24 (X is your unit number)
- IP address of your PC is 192.168.X.99 /24, or is obtained via DHCP if you configured the DHCP server on your NetVanta.
- The WAN IP address is 10.10.X.1 /30
SETUP

☐ Verify or change the IP address and default gateway of your PC.
  o IP address = 192.168.X.99 (X is the bench number).
  o Default gateway = 192.168.X.1 (X is the bench number).

☐ Connect the T1 circuit specified by the instructor to the 'WAN-T1' port of the NetVanta 3448. Use the cable specified by the instructor. In most cases, this will be your gray network T1 cable connecting to the bench jack labeled 'T1'.

☐ Connect one end of an Ethernet cable to port 1 of the NetVanta 3448 and the other end to your PC.

☐ Connect the COM port on your PC to the CONSOLE port on the rear panel of the NetVanta 3448. Use a DB-9 (female) to DB-9 (male) straight-through serial cable.

☐ Open a VT-100 session with the NetVanta 3448. Use the HyperTerminal icon on your desktop with the following settings:
  − Baud Rate = 9600
  − Parity = None
  − Data Bits = 8
  − Stop Bits = 1
  − Flow Control = None

☐ Re-establish the connection and log back in to the Enable Mode.
RESTORE SAVED CONFIGURATION

1. Display the contents of flash.
   
   Switch# show flash
   
   Do you see the configuration file named “baseline” that you saved in the first lab?

2. Copy this file to startup-config and then reload the router.
   
   Switch# copy baseline startup-config

3. After the reload, verify that you can ping the following:
   
   Host router (192.168.200.1) (Y/N) __________
   Other routers (10.10.X.1) (Y/N) __________
   You may have to wait for others to restart their routers.

4. From the Global Configuration mode, turn on the NetVanta 3448 firewall.
   
   NetVanta3448(config)# ip firewall

5. Set the firewall policy logging threshold to one.
   
   NetVanta3448(config)# ip firewall policy-log threshold 1

6. Save the running configuration.
CONFIGURE ACCESS POLICIES

In this part of the lab you will create an Access Control List (ACL) called MatchALL; you will create two Access Control Policies (ACP); and then you will apply an ACP to both the LAN and WAN interfaces. The ACL and ACP’s created will allow all traffic out but no traffic in. To verify your configuration, you will ping other routers in the classroom, including the host router.

7. From the Global Config mode, display options available to the ip access-list command.

   NetVanta3448(config)# ip access-list ?

   What are the two types of access-lists that can be created?

   __________________________________________________________

8. Create a standard access control list called MatchAll.

   NetVanta3448(config)# ip access-list standard MatchAll

9. Type “?” to display commands available in this mode.

   NetVanta3448(config-std-nacl)# ?

10. Execute the command that will match packets from any source host?

    NetVanta3448(config-std-nacl)# permit any

11. Exit to the Global Configuration mode.

    _______________________________________________________

12. Create a policy-class called Inside.

    NetVanta3448(config)# ip policy-class Inside

13. Type “?” to display commands available in this mode.

    NetVanta3448(config-policy-class)# ?

    Which command is used to allow traffic?  ___________________

    _______________________________________________________
14. Specify that the Inside ACP allow all packets that match the list MatchAll.
   NetVanta3448(config-policy-class)# allow list MatchAll

15. Create a second ACP called Outside.
   NetVanta3448(config-policy-class)# ip policy-class Outside

16. From this prompt, show the running configuration for the policy classes.
   NetVanta3448(config-policy-class)# do show run policy-class
   What does the configuration say about the policy-class Outside?
   __________________________________________________________
   There is an implicit discard. We want to discard all traffic, so there is no need to define any rules in this policy-class.
   Which command would you use to explicitly block traffic?
   __________________________________________________________
APPLY THE ACCESS CONTROL POLICY TO AN INTERFACE

So far, you have turned on the firewall, created an ACL called MatchAll and two ACP’s called Inside and Outside. The final step in this configuration is to apply the ACP to an interface.

17. Enter the interface configuration mode for VLAN 1.

   NetVanta3448(config-policy-class)# interface vlan 1

18. Apply the Inside ACP to interface VLAN 1.

   NetVanta3448(config-intf-vlan 1)# access-policy Inside

19. Enter the interface configuration mode for your frame relay sub-interface.

   NetVanta3448(config-eth 0/1)# interface fr 1.1XX  (XX is your unit #)

20. Apply the Outside ACP to your frame relay subinterface.

   NetVanta3448(config-fr 1.101)# access-policy Outside

21. Save the running configuration.

______________________________________________________________

TEST THE ACCESSIBILITY OF YOUR ROUTER

22. Can you ping the host router (192.168.200.1)?    Y/N __________

23. Have someone ping you. Could they?    Y/N __________

24. Can you ping the WAN interface of another router that has been configured up to this point?    Y/N __________
This lab will configure NAT to translate each of the inside IP addresses to the same Global IP address that is assigned to the WAN interface.

25. Edit the ip policy-class Inside.

   NetVanta3448(config)# ip policy-class Inside

26. Remove the existing “allow list MatchAll” statement.

   NetVanta3448(config-policy-class)# no allow list MatchAll

   Why this step is required? (Hint: ACP’s and ACL’s are order dependent.)

27. Display the commands available to the NAT command.

   NetVanta3448(config-policy-class)# nat ?

   The SOURCE option is used to perform network address translation on traffic leaving the inside network going out to the Internet. i.e. the source address will be translated.

28. Type the following to configure NAT to translate each of the local devices to the same Global IP address that is assigned to the WAN interface.

   NetVanta3448(config-policy-class)# nat source list MatchAll interface fr 1.1XX overload
Pair up with another site to complete this section.

29. Allow incoming ping to verify that NAT is configured properly.

NetVanta3448(config)# ip access-list extended MatchPing
NetVanta3448(config-ext-nacl)# permit icmp any any
NetVanta3448(config-ext-nacl)# ip policy-class Outside
NetVanta3448(config-policy-class)# allow list MatchPing self

30. From your PC, ping the other network’s router. (10.10.X.1)

31. Execute the “show event-history” command. What firewall message displayed at your partner’s router?

______________________________________________________________________________________

32. What was the source address of the ICMP packets displayed at your partner’s router?

______________________________________________________________________________________

Did NAT function properly? (Y/N)__________

If answer is yes, save the configuration.

Do Not Save This Configuration To baseline.

This Configuration Will Be Used In The Next Lab.
# COMMAND REFERENCE

The following commands are used in this lab. Refer to them as needed.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Turns on Privileged commands</td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters the Global Configuration Mode</td>
</tr>
<tr>
<td>hostname &lt;name&gt;</td>
<td>Defines the name of this router</td>
</tr>
<tr>
<td>interface vlan 1</td>
<td>Enters into the ethernet slot 0, port 1 interface for further configuration</td>
</tr>
<tr>
<td>ip address A.B.C.D A.B.C.D</td>
<td>Sets IP address of this interface</td>
</tr>
<tr>
<td>no shutdown</td>
<td>Turns on an interface</td>
</tr>
<tr>
<td>interface fr 1</td>
<td>Creates a frame-relay virtual interface</td>
</tr>
<tr>
<td>interface fr 1.10X</td>
<td>Creates a frame-relay sub-interface</td>
</tr>
<tr>
<td>show interfaces</td>
<td>Shows status and configuration of all interfaces</td>
</tr>
<tr>
<td>ip firewall</td>
<td>Enables firewall security features</td>
</tr>
<tr>
<td>ping A.B.C.D</td>
<td>Sends echo messages</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>Saves the current configuration to the startup configuration (NVRAM)</td>
</tr>
<tr>
<td>copy running-config “word”</td>
<td>Saves the current configuration to a named file in NVRAM</td>
</tr>
<tr>
<td>ip access-list standard “word”</td>
<td>Creates a standard access list</td>
</tr>
<tr>
<td>permit any</td>
<td>Permits all packets</td>
</tr>
<tr>
<td>ip policy-class “word”</td>
<td>Creates of configure a policy class</td>
</tr>
<tr>
<td>allow list “word”</td>
<td>Allows packets matching ACL</td>
</tr>
<tr>
<td>discard list “word”</td>
<td>Discards packets matching ACL</td>
</tr>
<tr>
<td>access-policy “word”</td>
<td>Assigns access control policy to this interface</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>permit “subnet” “wildcard bits”</code></td>
<td>Permits packets matching subnet and wildcard bits</td>
</tr>
<tr>
<td><code>do “root command”</code></td>
<td>Does a root command from the current mode</td>
</tr>
<tr>
<td><code>no discard list “word”</code></td>
<td>Removes this discard line</td>
</tr>
<tr>
<td><code>no allow list &lt;name&gt;</code></td>
<td>Removes the allow line</td>
</tr>
<tr>
<td><code>nat source list &lt;name&gt; interface fr 1.101 overload</code></td>
<td>NAT each of the inside devices that match the list with the same Global IP address that is assigned to interface fr 1.101</td>
</tr>
<tr>
<td><code>permit “subnet” “wildcard bits”</code></td>
<td>Permits packets matching the subnet and wildcard bits specified</td>
</tr>
<tr>
<td><code>nat source list &lt;name&gt; address A.B.C.D overload</code></td>
<td>NAT each of the inside devices that match the list with the same specified Global IP address</td>
</tr>
</tbody>
</table>
This lab builds on the configuration that was saved in the previous lab #4.

When the firewall is enabled routing between VLANs must be configured. This lab will setup a VLAN for the Sales Dept and one for the Engineering Dept. The PCs in each VLAN will be able to pass traffic to/from each other.

In this exercise you will pair up with another student. Each lab partner will use his/her own PC. One will be designated as Sales Dept (S) while the other is designated as Engineering Dept (E). Both will connect into a single NetVanta 3448.

**CONFIGURATION SUMMARY** – Step by step instructions begin on next page

- The Ethernet IP addresses for Sales (S) and Engineering (E) is 192.168.X.1 /24 (X is your unit number).

- IP addresses of the PCs are 192.168.X.99 /24 for each lab partner.

For example, if unit #2 and unit #3 have paired up as Sales and Engineering respectively, the table below should be followed.

<table>
<thead>
<tr>
<th></th>
<th>Sales</th>
<th>Engineering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet</td>
<td>192.168.2.1</td>
<td>192.168.3.1</td>
</tr>
<tr>
<td>PC</td>
<td>192.168.2.99</td>
<td>192.168.3.99</td>
</tr>
</tbody>
</table>

- The WAN IP address remains the same, 10.10.X.1 /30. X is the unit # to whom the 3448 belongs.
SETUP

☐ Instructions for Sales Dept.
   - Connect an ethernet cable from the PC to switchport 0/1.
   - Confirm PC IP address is 192.168.X.99 /24 with default gateway set to 192.168.X.1 (X is the Sales Dept Unit #)

☐ Instructions for Engineering Dept.
   - Connect an ethernet cable from the PC to switchport 0/8.
   - Confirm PC IP address is 192.168.X.99 /24 with default gateway set to 192.168.X.1 (X is the Engineering Dept Unit #)

☐ Confirm the T1 circuit remains connected.

☐ Re-establish the connection and log back in to the Enable Mode.
Create two VLANs, one for Sales and another for Engineering.

1. Create VLANs.
   For Sales Dept
   ```
   NetVanta3448#configure terminal
   NetVanta3448(config)#interface switchport 0/1
   NetVanta3448(config-swx 0/1)#switchport access vlan 1
   ```
   For Engineering Dept
   ```
   NetVanta3448#configure terminal
   NetVanta3448(config)#interface switchport 0/8
   NetVanta3448(config-swx 0/8)#switchport access vlan 2
   ```

2. Assign IP addresses to both VLANs.
   For Sales Dept – (Use the Sales PC unit # for X)
   ```
   NetVanta3448(config)#interface vlan 1
   NetVanta3448(config-intf-vlan 1)#ip address 192.168.X.1 /24
   NetVanta3448(config-intf-vlan 1)#no shut
   ```
   For Engineering Dept – (Use the Engineering PC unit # for X)
   ```
   NetVanta3448(config)#interface vlan 2
   NetVanta3448(config-intf-vlan 10X)#ip address 192.168.X.1 /24
   NetVanta3448(config-intf-vlan 10X)#no shut
   ```

Observe that there is already a policy called INSIDE applied to VLAN 1. The INSIDE policy is currently performing NAT on all traffic that originates from the private network. The traffic flow between Sales and Engineering should be allowed without being processed through NAT.

Create an extended access-list to match the type of traffic that will pass between the Sales and Engineering VLANs

3. Create an extended access-list called VLANtoVLAN
NetVanta3448#configure terminal
NetVanta3448(config)#ip access-list extended VLANtoVLAN
NetVanta3448(config-ext-nacl)#permit icmp any any

Reference the VLANtoVLAN access-list in the INSIDE policy. Note that this new statement needs to be processed before the existing NAT statement.

4. Edit the INSIDE policy

   NetVanta3448(config)#ip policy-class Inside
   NetVanta3448(config-policy-class)#allow list VLANtoVLAN

5. Show the policy-class INSIDE and notice the order.

   NetVanta3448(config-policy-class)#do show run policy-class

   The allow statement (VLANtoVLAN) was added to the bottom of the policy. In this order, all traffic will match the NAT statement. The VLANtoVLAN statement must appear above the NAT statement in order to be effective.

6. Remove the NAT statement to reorder the list. HINT: Using the mouse highlight the entire NAT statement, right-click and copy it. Type no (and a space), then right-click and paste the statement. Hit enter to execute.

   NetVanta3448(config-policy-class)#no nat source list MatchAll interface fr 1.102 overload

   Execute the do show run policy-class again to confirm it has been removed.

   NetVanta3448(config-policy-class)#do show run policy-class

   Add the NAT statement back again and it will be added to the bottom of the policy. Simply paste it and hit enter.

   NetVanta3448(config-policy-class)#nat source list MatchAll interface fr 1.102 overload

   Execute the do show run policy-class one final time to confirm it has been added and is now at the bottom of the policy Inside.

   NetVanta3448(config-policy-class)#do show run policy-class
Finally, the Inside policy is already applied to VLAN 1, however, it has not been applied to VLAN 2. Apply it now.

7. Apply the policy to VLAN 2.

   NetVanta(config)#interface vlan 2
   NetVanta(config-intf-vlan 2)#access-policy Inside
   NetVanta(config-intf-vlan 2)#end

8. Test the InterVLAN routing by clearing the event-history and ping to/from the Sales and Engineering PCs.

   NetVanta#clear event-history
   NetVanta#show event-history

9. Test the InterVLAN routing by pinging to/from the Sales/Engineering VLANs (ie PCs).

   PC IP address: 192.168.X.99 (X is the unit number)

   Were you successful? (Y/N) __________  If not, verify steps above.

10. Save the configuration. Do not copy configuration to baseline.
The following commands are used in this lab. Refer to them as needed.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Turns on Privileged commands</td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters the Global Configuration Mode</td>
</tr>
<tr>
<td>hostname &lt;name&gt;</td>
<td>Defines the name of this router</td>
</tr>
<tr>
<td>interface vlan 1</td>
<td>Enters into the ethernet slot 0, port 1 interface for further configuration</td>
</tr>
<tr>
<td>ip address A.B.C.D A.B.C.D</td>
<td>Sets IP address of this interface</td>
</tr>
<tr>
<td>no shutdown</td>
<td>Turns on an interface</td>
</tr>
<tr>
<td>interface fr 1</td>
<td>Creates a frame-relay virtual interface</td>
</tr>
<tr>
<td>interface fr 1.10X</td>
<td>Creates a frame-relay sub-interface</td>
</tr>
<tr>
<td>show interfaces</td>
<td>Shows status and configuration of all interfaces</td>
</tr>
<tr>
<td>ip firewall</td>
<td>Enables firewall security features</td>
</tr>
<tr>
<td>ping A.B.C.D</td>
<td>Sends echo messages</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>Saves the current configuration to the startup configuration (NVRAM)</td>
</tr>
<tr>
<td>copy running-config “word”</td>
<td>Saves the current configuration to a named file in NVRAM</td>
</tr>
<tr>
<td>ip access-list standard “word”</td>
<td>Creates a standard access list</td>
</tr>
<tr>
<td>permit any</td>
<td>Permits all packets</td>
</tr>
<tr>
<td>ip policy-class “word”</td>
<td>Creates of configure a policy class</td>
</tr>
<tr>
<td>allow list “word”</td>
<td>Allows packets matching ACL</td>
</tr>
<tr>
<td>discard list “word”</td>
<td>Discards packets matching ACL</td>
</tr>
<tr>
<td>access-policy “word”</td>
<td>Assigns access control policy to this interface</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>permit “subnet” “wildcard bits”</code></td>
<td>Permits packets matching subnet and wildcard bits</td>
</tr>
<tr>
<td><code>do “root command”</code></td>
<td>Does a root command from the current mode</td>
</tr>
<tr>
<td><code>no discard list “word”</code></td>
<td>Removes this discard line</td>
</tr>
<tr>
<td><code>no allow list &lt;name&gt;</code></td>
<td>Removes the allow line</td>
</tr>
<tr>
<td><code>nat source list &lt;name&gt; interface fr 1.101 overload</code></td>
<td>NAT each of the inside devices that match the list with the same Global IP address that is assigned to interface fr 1.101</td>
</tr>
<tr>
<td><code>permit “subnet” “wildcard bits”</code></td>
<td>Permits packets matching the subnet and wildcard bits specified</td>
</tr>
<tr>
<td><code>nat source list &lt;name&gt; address A.B.C.D overload</code></td>
<td>NAT each of the inside devices that match the list with the same specified Global IP address</td>
</tr>
</tbody>
</table>
In this exercise you will configure the remote office NetVanta 3448 to protect all traffic leaving your remote office LAN destined for the corporate HQ LAN.

VPN CONFIGURATION

- Protect traffic leaving Remote office LAN destined for Corporate HQ LAN
- IKE SA parameters
  - Initiate and respond in Main mode
  - Peer = 172.16.100.1 (Corporate Headquarters public IP address)
  - IKE Attributes = 3DES, SHA, Diffie Hellman Group 2, Lifetime – 3600 seconds
- IKE remote-id = 172.16.100.1 with pre-shared key of YourInternetSecurity
- IPSec SA parameters
  - Transform-set using 3DES and SHA
  - Lifetime of 1200 seconds
  - PFS = Group 2
SETUP

☐ Ensure that your PC is configured to obtain an IP address automatically and that the NetVanta is configured to be a DHCP Server.

☐ Ensure that your PC Ethernet port is securely connected with an Ethernet cable to port 1 on the NetVanta 3448.

☐ Ensure that your WAN T1 port is securely connected with a T1 cable to the WAN jack specified by your instructor.

☐ Connect the COM port on your PC to the CONSOLE port on the rear panel of the NetVanta 3448. Use a DB-9 (female) to DB-9 (male) straight-through serial cable.

☐ Open a VT-100 session with the NetVanta 3448. Use the HyperTerminal icon on your desktop with the following settings:
  – Baud Rate = 9600
  – Parity = None
  – Data Bits = 8
  – Stop Bits = 1
  – Flow Control = None

☐ Optional: Press <Enter> on the keyboard and the access prompt should appear. Enter into Enable Mode by typing ‘enable’ and factory default the NetVanta 3448 using the following commands:

  Router# erase startup-config // Erase start-up configuration file
  Router# reload // Reload/reboot the router

  Enter <n> for ‘no’ when asked if wanting to save system configuration.
  Enter <y> for ‘yes’ when asked if wanting to reboot system.

  Router# copy baseline startup-config
  Router# reload

  Enter <n> for ‘no’ when asked if wanting to save system configuration.
  Enter <y> for ‘yes’ when asked if wanting to reboot system.

☐ Re-establish the connection and log back in to the Enable Mode

* When you need to dynamically obtain an IP address on your PC, perform the following from the PC command prompt.

  Windows 2000 or XP: ipconfig /release and ipconfig /renew
VERIFY BASIC ROUTER CONFIGURATION

In the initial configuration of this lab, you will verify the setup of basic routing and verify connectivity. Your router will also be set up as a DHCP server providing IP addresses to your LAN.

1. Using the diagram above, ensure that the Remote Office NetVanta 3448 is configured correctly. Use the following commands as a guide. You may also see firewall configuration commands.

```
! Configure Public Interface
interface fr 1.10X
   ip address 10.10.X.1 255.255.255.252
   no shutdown

! Configure Private Interface
interface vlan 1
   ip address 192.168.X.1 255.255.255.0
   no shutdown
   ip route 0.0.0.0 0.0.0.0 10.10.X.2
   ip dhcp-server pool dhcpPool
      network 192.168.X.0 255.255.255.0
      default-router 192.168.X.1
```

2. Verify that your PC obtained an IP address and that you can ping your router's PRIVATE Ethernet interface FROM YOUR PC. ping 192.168.X.1

3. FROM YOUR ROUTER, verify that you can ping 172.16.100.1.

4. Note that the baseline configuration DOES NOT have the firewall enabled. We will complete the initial VPN configuration and testing WITHOUT the firewall.
VPN CONFIGURATION

In the following steps, you will configure the remote office NetVanta 3448 to protect all traffic from the remote office to corporate network.

NetVanta 3448 VPN Configuration Settings

<table>
<thead>
<tr>
<th>IKE SA (phase 1) policy parameters</th>
<th>IPSec SA (phase 2) policy parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Respond: Main Mode</td>
<td>Protect traffic from the remote office network to the corporate network</td>
</tr>
<tr>
<td>Initiate: Main Mode</td>
<td>Peer: 172.16.100.1</td>
</tr>
<tr>
<td>Encryption Algorithm: 3DES</td>
<td>Encryption Algorithm: 3DES</td>
</tr>
<tr>
<td>Hash Algorithm: SHA</td>
<td>Hash Algorithm: SHA</td>
</tr>
<tr>
<td>Diffie Hellman Group: 2</td>
<td>Lifetime: 1200 seconds</td>
</tr>
<tr>
<td>Lifetime: 3600 seconds</td>
<td>PFS: Group 2</td>
</tr>
<tr>
<td>Local ID: WAN IP address</td>
<td></td>
</tr>
<tr>
<td>Remote ID: Peer Public IP Address</td>
<td></td>
</tr>
<tr>
<td>172.16.100.1</td>
<td></td>
</tr>
<tr>
<td>Pre-shared key: YourInternetSecurity</td>
<td></td>
</tr>
</tbody>
</table>

5. Enable VPN functionality in the NetVanta 3448.

    Router(config)# ip crypto

6. Display options available to the crypto command.

    Router(config)# crypto ?

Which option is used to configure IKE policy parameters?

7. Define the remote id for the corporate site.

    Router(config)# crypto ike remote-id address 172.16.100.1
                  preshared-key YourInternetSecurity
CREATE AND CONFIGURE THE IKE POLICY

8. Create an IKE policy with a priority of 1

   Router(config)# crypto ike policy 1

9. Type “?” to display commands available in this mode.

   Router(config-ike)# ?

10. Set this IKE policy up to initiate and respond to IKE negotiations in Main mode only.

11. Define the peer for this IKE policy as 172.16.100.1. (The corporate public IP address)

   Router(config-ike)# peer 172.16.100.1

12. Create an IKE attribute policy with a priority of 1.

   Router(config-ike)# attribute 1

13. Type the following to view the default attributes for your IKE policy.

   Router(config-ike-attribute)# do show running-config verbose

   List the default IKE attributes?

   Authentication: __________          Encryption: __________
   Hash: __________          Group: __________          Lifetime: __________

14. Set the following IKE attribute policy parameters:

   Encryption:  3DES
   Hash:   SHA
   Group:   2
   Lifetime:  3600 seconds
CREATE THE IPSEC TRANSFORM SET

15. Display authentication and encryption options available to a transform set.

   Router(config)# crypto ipsec transform-set Secure ?

16. Create a transform set named “Secure” specifying the 3DES encryption algorithm and SHA authentication algorithm.

   Router(config)# crypto ipsec transform-set Secure esp-3des esp-sha-hmac

DEFINE TRAFFIC THAT WILL BE PROTECTED

Remote Office       Corporate HQ

NetVanta 3448

Source Network 192.168.X.0 /24

Destination Network 192.168.100.0 /24

17. Create an extended access list named CorpVPNTraffic that will protect all traffic from the remote office network to the corporate network.

   Router(config)# ip access-list extended CorpVPNTraffic
   Router(config-ext-nacl)# permit ip 192.168.X.0 0.0.0.255 192.168.100.0 0.0.0.255
   
   \(X\) is your unit number

Remember with VPN ACLs, the entries in the list are defined with respect to the local system. In the example above, the source is the remote office private network and the destination is the corporate private network.
CREATE AND CONFIGURE THE CRYPTO MAP

18. Type the following to create an IPSec/IKE Crypto map that will be used for the VPN traffic back to the corporate network.

   Router(config)# crypto map CorpVPNMap 1 ipsec-ike

19. Type “?” to display commands available in this mode.

   Router(config-crypto-map)# ?

20. Specify the access control list that will determine the traffic to be encrypted.

   Router(config-crypto-map)# match address CorpVPNTraffic

21. Define the peer for this crypto map as 172.16.100.1. (The corporate public IP address)

   Router(config-crypto-map)# set peer 172.16.100.1

22. Set the Perfect Forward Secrecy to Diffie-Hellman group 2.

   Router(config-crypto-map)# set pfs group2

23. Specify the transform set that this crypto map will use.

   Router(config-crypto-map)# set transform-set Secure

24. Set the IPSec security association lifetime to 1200 seconds.

   Router(config-crypto-map)# set security-association lifetime seconds 1200

APPLY THE CRYPTO MAP TO THE TRANSMITTING INTERFACE

25. From the Frame Relay sub-interface configuration mode, assign the crypto map named CorpVPNMap.

   Router(config-fr1.1XX)# crypto map CorpVPNMap

26. Save your configuration.
VERIFY YOUR CONFIGURATION

NetVanta 3448 VPN Configuration Settings

<table>
<thead>
<tr>
<th>IKE SA (phase 1) policy parameters</th>
<th>IPSec SA (phase 2) policy parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Respond: Main Mode</td>
<td>Protect traffic from the remote office network to the corporate network</td>
</tr>
<tr>
<td>Inititate: Main Mode</td>
<td>Peer: 172.16.100.1</td>
</tr>
<tr>
<td>Encryption Algorithm: 3DES</td>
<td>Encryption Algorithm: 3DES</td>
</tr>
<tr>
<td>Hash Algorithm: SHA</td>
<td>Hash Algorithm: SHA</td>
</tr>
<tr>
<td>Diffie Hellman Group: 2</td>
<td>Lifetime: 1200 seconds</td>
</tr>
<tr>
<td>Lifetime: 3600 seconds</td>
<td>PFS: Group 2</td>
</tr>
<tr>
<td>Local ID: WAN IP address</td>
<td></td>
</tr>
<tr>
<td>Remote ID: Peer Public IP Address</td>
<td></td>
</tr>
<tr>
<td>172.16.100.1</td>
<td></td>
</tr>
<tr>
<td>Pre-shared key: YourInternetSecurity</td>
<td></td>
</tr>
</tbody>
</table>

Using the following commands, verify that you have configured the NetVanta 3448 to match the above parameters.

27. Display your router’s running configuration.

    Router# show running-config

    Verify that there are no error messages in the VPN configuration. If there are error messages, correct them before continuing.

28. Display the remote id and pre-shared key.

    Router# show crypto ike remote-id

29. Display the IKE policy that you created.

    Router# show crypto ike policy

30. What currently displays with the following commands?

    Router# show crypto ike sa ______________________________

    Router# show crypto ipsec sa ______________________________

NOTE: The output should be blank because you haven’t generated any interesting traffic.
TEST YOUR CONFIGURATION

31. Type the following to display IKE messages as they happen.

   Router# debug crypto ike

32. FROM YOUR PC, ping the corporate router’s Ethernet IP address. 192.168.100.1

   The first few packets may not go through due to tunnel negotiation.

33. View the beginning of IKE debug output and answer the following question.

   What IKE negotiation mode was used in the first message?

   ____________________________________________________________

34. Display the IKE security association.

   Router# show crypto ike sa

   What is the remaining lifetime of the IKE security association?

   ____________________________________________________________

35. Display the IPSec security association.

   Router# show crypto ipsec sa

   How many IPSec security associations are currently active?

   ____________________________________________________________

36. FROM YOUR PC, ping the corporate router’s Ethernet IP address. 192.168.100.1

   Did any new VPN negotiation take place? __________________________

37. Clear only the IPSec security association and then verify that only the IPSec SA has been cleared.

   Router# clear crypto ipsec sa

   Router# show crypto ipsec sa Did the IPSec SA clear? _____________

   Router# show crypto ike sa Did the IKE SA clear? ________________

38. FROM YOUR PC, ping the corporate router’s Ethernet IP address. 192.168.100.1

39. View the beginning of IKE debug output and answer the following question.
What IKE negotiation **mode** was used in the first message?

40. Display the IKE security association.

   Router# **show crypto ike sa**

   What is the remaining lifetime of the IKE security association?

41. Display the IPSec security association.

   Router# **show crypto ipsec sa**

   How many IPSec security associations are currently active?
CONFIGURE THE FIREWALL TO ALLOW VPN TRAFFIC

In the previous lab, you configured the Firewall to NAT all traffic outbound from your LAN. Because we restored the baseline configuration, that firewall configuration is no longer in the router. In this portion of the lab, we will re-do the Internet access Firewall configuration. This exercise will help you to see how the firewall and VPN work together.

In order for traffic from your PC to the corporate network to be encapsulated in the VPN tunnel, we must first "allow" this traffic through the firewall.

42. First, enable the firewall.

   Router(config)# ip firewall

43. Now, create an access control list that matches all traffic.

   Router(config)# ip access-list standard MatchAll
   Router(config-std-nacl)# permit any

44. In order for traffic from your PC to the corporate network to be encapsulated in the VPN tunnel, we must first "allow" this traffic through the firewall. Create a policy-class "Inside" and allow the corporate VPN traffic. Recall that you created an access-list to match corporate VPN traffic when you configured the VPN selectors in step 17.

   Router(config)# ip policy-class Inside
   Router(config-policy-class)# allow list CorpVPNTraffic

45. Add a NAT statement to the ACP.

   Router(config-policy-class)# nat source list MatchAll interface fr 1.1XX overload

46. In order for traffic from the Corporate network to have access into your LAN, you must allow the traffic through the firewall. Create a policy-class “Outside” and allow VPN traffic from Corporate into your LAN.

   Router(config-policy-class)# ip policy-class Outside
   Router(config-policy-class)# allow reverse list CorpVPNTraffic

   NOTE: The "reverse" keyword simply reverses the source and destination of an extended ACL.

47. Finally, apply the access control policies to the appropriate interfaces.

   Router(config)# interface vlan 1
   Router(config-intf-vlan 1)# access-policy Inside
   Router(config-intf-vlan 1)# interface fr 1.1XX
   Router(config-fr 1.1XX)# access-policy Outside
TEST YOUR CONFIGURATION

48. Clear only the IPSec security association and then verify that only the IPSec SA has been cleared.

   Router# clear crypto ipsec sa
   Router# show crypto ipsec sa
   Router# show crypto ike sa

   Did the IPSec SA clear? ________________
   Did the IKE SA clear? ________________

49. Type the following to clear any sessions that may be active in the firewall.

   Router# clear ip policy-sessions

50. Type the following to display IKE messages as they happen.

   Router# debug crypto ike

51. FROM YOUR PC, ping the corporate router’s Ethernet IP address. 192.168.100.1

   The first few packets may not go through due to tunnel negotiation.

52. Did you see any new ike negotiations?

53. Show the running configuration for the policy classes

   Router# show running-config policy-class

   Notice the order of the entries in the “Inside” policy-class. What would happen if the order of the entries in that policy-class were reversed?

Time Permitting

Have your instructor insert errors for troubleshooting. Use the show and debug commands to solve the problem.
## COMMAND REFERENCE

The following commands are used in this lab. Refer to them as needed.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip crypto</td>
<td>Enable VPN functionality</td>
</tr>
<tr>
<td>crypto ike remote-id address A.B.C.D</td>
<td>Define the remote id</td>
</tr>
<tr>
<td>crypto ike policy 1</td>
<td>Create IKE policy with priority of 1</td>
</tr>
<tr>
<td>initiate main</td>
<td>Initiate IKE negotiation in Main mode</td>
</tr>
<tr>
<td>respond main</td>
<td>Can only respond to IKE negotiation using main mode</td>
</tr>
<tr>
<td>peer A.B.C.D</td>
<td>Define IKE peer for this policy</td>
</tr>
<tr>
<td>client configuration pool vpnPool</td>
<td>Specify the client configuration pool that this IKE policy will use</td>
</tr>
<tr>
<td>attribute 1</td>
<td>Create IKE policy attribute set 1</td>
</tr>
<tr>
<td>encryption 3des</td>
<td>Set IKE encryption algorithm</td>
</tr>
<tr>
<td>hash sha</td>
<td>Set IKE hash algorithm</td>
</tr>
<tr>
<td>group 2</td>
<td>Set IKE Diffie-Hellman to group 2</td>
</tr>
<tr>
<td>lifetime 3600</td>
<td>Set IKE lifetime to 3600 seconds</td>
</tr>
<tr>
<td>crypto ipsec transform-set Secure</td>
<td>Create a transform set named Secure</td>
</tr>
<tr>
<td>esp-3des esp-sha-hmac</td>
<td></td>
</tr>
<tr>
<td>ip access-list extended CorpVPNTraffic</td>
<td>Create an extended access list named CorpVPNTraffic</td>
</tr>
<tr>
<td>permit ip 192.168.1.0 0.0.0.255 192.168.100.0</td>
<td>Permit all traffic from the 192.168.1.0 network to the 192.168.100.0 network</td>
</tr>
<tr>
<td>match address CorpVPNTraffic</td>
<td>Specify the ACL that will determine the traffic to be encrypted</td>
</tr>
<tr>
<td>set peer A.B.C.D</td>
<td>Define IPSec peer</td>
</tr>
<tr>
<td>set pfs group2</td>
<td>Enable Perfect Forward Secrecy using Diffie-Hellman Group 2</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>set transform-set Secure</td>
<td>Specify the transform set that this crypto map will use</td>
</tr>
<tr>
<td>set security-association lifetime</td>
<td>IPSec SA lifetime 1200 seconds</td>
</tr>
<tr>
<td>seconds 1200</td>
<td></td>
</tr>
<tr>
<td>crypto map CorpVPNMap</td>
<td>Apply crypto map to an interface</td>
</tr>
<tr>
<td>show crypto ike remote-id</td>
<td>Display the remote id and pre-shared key</td>
</tr>
<tr>
<td>show crypto ike policy</td>
<td>Display IKE policy(s)</td>
</tr>
<tr>
<td>show crypto ike sa</td>
<td>Display IKE security associations</td>
</tr>
<tr>
<td>show crypto ipsec sa</td>
<td>Display IPSec security associations</td>
</tr>
<tr>
<td>debug crypto ike</td>
<td>Display IKE messages real-time</td>
</tr>
<tr>
<td>clear crypto ipsec sa</td>
<td>Tear down IPSec SA</td>
</tr>
</tbody>
</table>