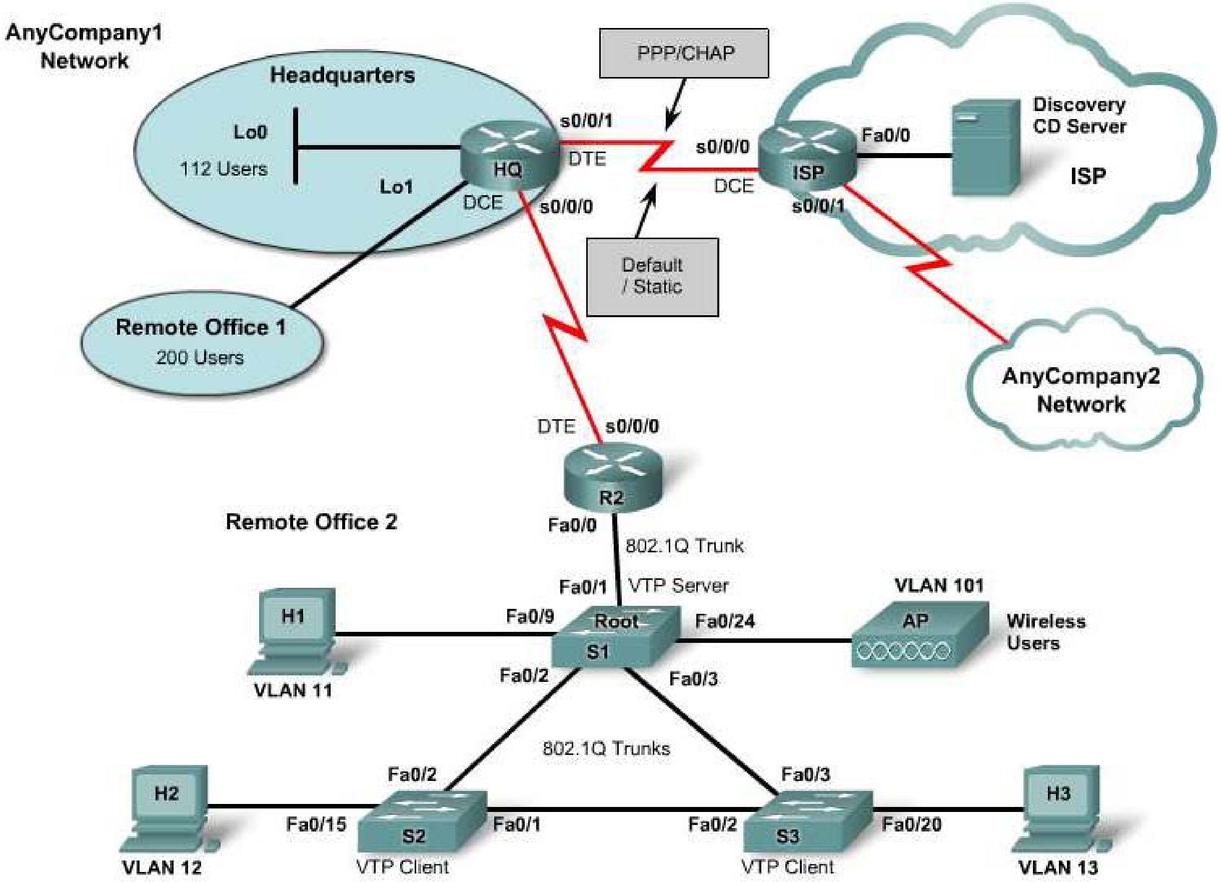
Summary Lab 10.0.1 Putting It All Together



Objectives

Part A

- Analyze the customer work order and proposed network design.
- Create a VLSM IP addressing scheme.

Part B

- Build a multilayer network and connect to a simulated ISP.
- Configure basic settings on switches with multiple VLANs and VTP.
- Configure the STP root bridge.
- Configure basic settings on routers and inter-VLAN routing.
- Verify basic connectivity, device configuration, and functionality.

Part C

- Configure multiple routers using OSPF, PAT and a default route.
- Configure WAN link using PPP and authentication.
- Configure multiple switches with port security.
- Configure ACLs to control network access and to secure routers.
- Verify connectivity, device configuration, and functionality.

Background / Preparation

AnyCompany is opening a new branch office (Remote Office 2) and has contracted you to extend the AnyCompany network into the new facilities. Corporate management has also decided that this would be a good time to restructure the existing network to provide increased levels of security and performance.

The existing network consists of a head office, which houses 112 employees, and a business office (remote office 1), which houses 200 employees. The new office space (Remote Office 2) will initially house four distinct groups of employees but will expand as the company grows. For this reason, implement VLANs to help manage the traffic. Also use VTP to simplify the task of managing the VLANs. One of the groups occupying the new office is the sales force. This group requires wireless access to the company network. Because security is of great concern, the wireless network must be on its own VLAN.

Initially the network in Remote Office 2 will consist of five VLANs.

This lab focuses on the configuration of the Cisco 1800 router and 2960 switch, or comparable equipment, using Cisco IOS commands. The information in this lab applies to other routers and switches; however, the command syntax may vary. Depending on the router model, the interfaces may differ. For example, on some routers Serial 0 may be Serial 0/0 or Serial 0/0/0 and Ethernet 0 may be FastEthernet 0/0.

It is recommenced to work in teams of three. Each person can be responsible for one of the three switches and its associated host PC. The team can work together to configure the two company routers.

The following resources are required:

- One ISP router with one serial and one FastEthernet interface (preconfigured by instructor)
- Three Ethernet 2960 switches (or comparable) for Remote Office 2 LAN
- Two 1841 routers (or other routers), one with a FastEthernet interface and one with two serial interfaces
- One Wireless Access Point (optional)
- One Ethernet 2960 switch to connect wired PCs
- Three Windows XP-based PCs to act as wired clients
- One Discovery CD Server, preconfigured by instructor (optional if a Loopback is on ISP router)
- Cat 5 cabling as necessary (straight-through and crossover)
- Two Serial DTE/DCE cables for WAN links
- ISP work order (included in this lab)

Part A – Review the work order and develop the VLSM subnet scheme

Task 1: Review the customer work order and proposed network.

You have received the following work order from your manager at the ISP. Review the work order to get a general understanding of what is to be done for the customer.

ABC-XYZ-ISP Inc.

Official Work Order

Customer: AnyCompany1 or AnyCompany2 **Date:** _____________

(Circle the customer name assigned by your instructor)

Address: 1234 Fifth Street, Anytown

Customer Contact: Fred Pennypincher, Chief Financial Officer

Phone number: 123-456-7890

Description of work to be performed

Review the proposed network topology at the beginning of the lab. The existing network includes Headquarters (HQ) and Remote Office 1 (RO1). You will need to configure the HQ router, build the network for Remote Office 2 (RO2) network and connect it to the HQ router. Equipment for the RO2 network consists of an additional 1841 router, 3 new 2960 switches, and a wireless Access Point (AP). RO2 will use VLANs to separate user departments, a server farm, and wireless users. The RO2 router will route between VLANs and pass traffic to the HQ router to be forwarded to the ISP. The HQ router must use a static address to communicate with the ISP router. The ISP serial interface IP address is:

____

If HQ is connected to the ISP as AnyCompany1, the IP address of the ISP Serial 0 interface is 209.165.201.1/30.

If HQ is connected to the ISP as AnyCompany2, the IP address of the ISP Serial 1 interface is 209.165.202.129/30.

The serial link to the new ISP uses PPP encapsulation with CHAP authentication and static routes. The OSPF routing protocol is to be used between the HQ and RO2 routers and the encapsulation on the WAN link between them is HDLC. Routes from the RO2 network must be summarized and advertised to the HQ router.

You will need to develop a VLSM addressing scheme that will accommodate the existing HQ and RO1 networks as well as the new RO2 network.

Assigned to: Approved by:

Guy Netwiz Bill Broadband, ISP Manager

Task 2: Develop the network scheme

NOTE: Be sure to have the instructor check your work for each step in this task before going on to Task 3.

Step 1: Determine the size of the CIDR address block assigned

a. The customer has been assigned CIDR network address: ______________________________

If network customer is AnyCompany1, use 172.20.0.0/22.

If network customer is AnyCompany2, use 172.20.4.0/22.

b. How many total host IP addresses does this CIDR address block represent?

____

Using this address block, you will develop a VLSM subnet scheme that will allow AnyCompanyX to support existing HQ and RO1 networks as well as the new RO2 network.

Step 2: Determine the size of each VLSM block to accommodate users

a. Based on the CIDR address assigned by the ISP and the number of users in each area or VLAN, optimally subnet this block of addresses to provide sufficient addresses for all offices (HQ, RO1, and RO2) and VLAN requirements.

b. To start, determine the size of the subnet address block required for a network area or group of users. Fill in the table with this information. Look at the number of users for each area or subnet and determine the smallest power of 2 that will cover the requirement. As an example, if 93 addresses were required, a VLSM block of 128 (2^7) would be needed. The next smallest power of 2 is 64 (2^6), which does not cover the requirement. A block of 128 results in some unused addresses but also allows for growth.

Network Area	No. Users / IPs	VLSM block size / No. of IPs (powers of 2)
HQ Network	112	
RO1 Network	200	
RO2 Network / VLANs		
VLAN 1 (Server Farm)	18 users	
VLAN 2 (Native/mgmt -IP)	9 users	
VLAN 11 (Dept 1)	75 users	
VLAN 12 (Dept 2)	112 users	
VLAN 13 (Dept 3)	38 users	
VLAN 101 (wireless)	52 users	
WAN link (RO2 to HQ)	2	
Total users and block sizes for RO2	306	
RO2 block size to subdivide	N/A	
Total users and all VLSM blocks	618	

c. To optimally allocate addresses from the /22 CIDR address, start by sorting the block sizes from largest to smallest. For this lab, add up the individual smaller blocks for each of the VLANs in the RO2 network and allocate a single larger block that will cover all the smaller block requirements. This keeps all of the subnets together for RO2 and aids in route summarization. Use the table below to order the network areas by the VLSM block size. List the large block for the entire RO2 network first, followed by the others. The larger RO2 block will be broken down into smaller subnets later.

Network Area / VLAN	VLSM block size starting with the largest first
RO2 total block size (will be subdivided into smaller blocks)	
RO1 Network	
HQ Network	
RO2 - VLAN 11 (Dept 1)	
RO2 - VLAN 12 (Dept 2)	
RO2 - VLAN 13 (Dept 3s)	
RO2 - VLAN 101 (wireless)	
RO2 - VLAN 1 (Server Farm)	
RO2 - VLAN 2 (Native/mgmt -IP)	
RO2 - HQ Wan link	

Step 3: Determine subnet addresses for the CIDR block

a. Determine which blocks of CIDR address to assign to each area of the network or VLAN. Use the VLSM subnet chart (Appendix A) to enter the subnet information for each of the CIDR blocks.

b. To determine the subnet addresses for the 172.20.0.0/22 or the 172.20.4.0/22 CIDR block, use the subnet calculator tool on the Cisco Network Academy website. With the subnet calculator tool, enter the Base Network Address (172.20.0.0 or 172.20.4.0) and the value of VLSM Mask 1 in dotted decimal, starting with 255.255.252.0 (/22). Click the **Actions** button **Calculate Subnetting using VLSM**. Use the same base address and increase the mask length by one each time to fill in the chart.

   NOTE: Entries for the subnet numbers for the /29 and /30 mask are not included in the table. Subdivide one of the /28s to a /30 for the WAN link.

Step 4: Allocate blocks of addresses to each area of the network

a. Fill in the following table based on the subnet information in the CIDR/VLSM Subnet Chart and the sorted table of address requirements. Draw lines around each of the blocks in the address table above, or color them in, and label each one according to the network area or VLAN to which it is assigned.

Network Area / VLAN	VLSM Block Size (# of addr)	Subnet Address and Prefix	Useable Address Range	Subnet Mask
RO2 total block size (will be subdivided into smaller blocks)				
RO2 – VLAN 11 (Dept 1)				
RO2 – VLAN 12 (Dept 2)				
RO2 – VLAN 13 (Dept 3)				
RO2 – VLAN 101 (wireless)				
RO2 – VLAN 1 (Server Farm)				
RO2 – VLAN 2 (Native/mgmt – IP)				
RO2 - WAN link				
RO1 Network				
HQ Network				

b. Have the instructor verify that your addressing scheme is accurate and assigns address space efficiently. You should not have any overlapping subnets and should have unused contiguous blocks of addresses that can used for future subnets as the company grows.

Task 3: Determine IP addresses to use for device interfaces

Step 1: Select IP addresses for use when configuring devices

Select addresses from the block assigned to an area of the network and fill in the IP address and subnet mask to be used for each device/interface in the topology. These IP addresses will be used later in Part C when configuring the network equipment.

NOTE: When finished with this Task, check with the instructor before proceeding.

Device Interface / IP Address Chart

Device	Interface	IP Address	Subnet Mask
HQ	Serial 0/0/0		
	Serial 0/0/1		
	Loopback0 (HQ)		
	Loopback1 (RO1)		
R2	Serial 0/0/0		
	FastEthernet 0/0	None	None
	Subint Fa0/0.1		
	Subint Fa0/0.2		
	Subint Fa0/0.11		
	Subint Fa0/0.12		
	Subint Fa0/0.13		
	Subint Fa0/0.101		
ISP	Serial 0/0/0	209.165.201.1 (AnyCompany1) or 209.165.202.129 (AnyCompany2)	255.255.255.252
S1 (RO2)	VLAN 2		
S2 (RO2)	VLAN 2		
S3 (RO2)	VLAN 2		
H1	NIC		
H2	NIC		
H3	NIC		

Step 2: Have the instructor check your work for this task before going on to Part B.

Part B – Physically construct the network and perform basic device configuration

Task 1: Build the network and connect cables to the interfaces and ports indicated

Connect your AnyCompanyX network router HQ to the ISP router. The ISP router and the Discovery CD Server should be preconfigured by the instructor. If ISP router is configured with a Loopback address in lieu of the Discovery CD Server, the HTTP server in the router must be enabled. If you are unsure, check with your instructor.

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

The IP addresses used to configure the devices in the following tasks should be based on your solution for the VLSM scheme.

NOTE: VLAN Mismatch Messages - You may want to wait until after the switches are configured to connect the trunk links. Otherwise, native VLAN mismatch messages come up until all switches are configured.

Task 2: Configure the HQ router

Step 1: Configure the HQ host name, passwords, no domain lookup, and message-of-the-day

Step 2: Configure the HQ serial and loopback interfaces

The WAN link from HQ to R2 uses default Cisco HDLC encapsulation.

The WAN link from HQ to ISP uses PPP with CHAP authentication.

Step 3: Create CHAP user ID and password

Configure a username for the ISP router on the HQ router with a password of **cisco** for use with CHAP authentication.

Step 4: Save the router running-config configuration to startup-config

Step 5: Copy the router running-config to a text editor and save it for later use, if needed

a. Open a text editor such as Windows Notepad.

b. Issue the **`show running-config`** command.

c. Copy the output and paste it into the text editor.

d. Save the file on the Windows Desktop as **HQ.txt**.

Task 3: Configure the Remote Office 2 router R2

Step 1: Configure the R2 host name, passwords, no domain lookup, and message-of-the-day

Step 2: Configure the RO2 FastEthernet subinterfaces and serial interfaces

a. It is easier to troubleshoot the FastEthernet subinterfaces if the numbers match the VLAN numbers they represent. They should also use 802.1Q encapsulation.

b. VLAN 2 is the native VLAN.

c. The WAN link from HQ to R2 uses default Cisco HDLC encapsulation.

Step 3: Save the router running-config configuration to startup-config

Step 4: Copy the router running-config to a text editor and save it for later use, if needed

a. Open a text editor such as Windows Notepad.

b. Issue the **`show running-config`** command.

c. Copy the output and paste it into the text editor.

d. Save the file on the Windows Desktop as **R2.txt**.

NOTE: If you need to use this file later, you will need to edit it to clean it up and make sure that the necessary interfaces have the **`no shutdown`** command applied to them.

Task 4: Configure the Remote Office 2 switch S1

NOTE: Be sure to erase the startup-config, delete the vlan.dat file, and reload the switch before beginning the configuration.

Step 1: Configure the S1 host name, passwords, no domain lookup, and message-of-the-day

Step 2: Configure the VLANs for Remote office 2 on S1 using the VLAN numbers and names shown in the chart below

Assign ports to each VLAN as indicated. Use the same chart to configure switches S2 and S3:

RO2 VLAN Number	VLAN Name	Ports assigned	Notes
VLAN 1 (default VLAN)	default	Ports 4-5	VLAN 1 cannot be renamed
VLAN 2 (Native/mgmt – IP)	Mgmnt	Port 23	
VLAN 11 (Dept 1 users)	Dept1	Ports 6 to 11	
VLAN 12 (Dept 2 users)	Dept2	Ports 12 to 17	
VLAN 13 (Dept 3 users)	Dept3	Ports 18 to 22	
VLAN 101 (wireless)	Wireless	Port 24	

Step 3: Assign an IP address to the Management VLAN 2 on S1

a. Assign the VLAN 2 address according to the Device Interface / IP Address Chart in Part A, Task 3, Step1.

b. Configure the switch with a default gateway to router R2 for VLAN 2.

Step 4: Configure S1 switch ports Fa0/1, Fa0/2 and Fa0/3 as 802.1Q trunks

The trunks carry VLAN information. Set each trunk to use VLAN 2 as the native VLAN.

Step 5: Configure S1 as the root switch for STP

Change the priority of native VLAN 2 from the default of 32769 to 4096.

Step 6: Configure a VTP domain

a. Configure the AnyCompanyX domain name (where X is 1 or 2) on S1 and a password of **cisco**.

b. Configure S1 as the VTP server.

Step 7: Save the switch running-config configuration to startup-config

Step 8: Copy the switch running-config to a text editor and save it for later use, if needed

Task 5: Configure the Remote Office 2 switch S2

Step 1: Configure the S2 host name, passwords, no domain lookup, and message-of-the-day

Step 2: Configure the VTP domain AnyCompanyX on S2 with S2 as a client using the password of cisco

It is not necessary to configure the VLANs on S2. As a VTP client, the information will be obtained from VTP server S1.

You will, however, need to assign ports to the VLANs according to the chart in Part B, Task 4, Step 2.

Step 3: Assign an IP address to the Management/Native VLAN 2 on S2

a. Use the IP address from the Device Interface / IP Address Chart in Part A, Task 3, Step 1.

b. Configure the switch with a default gateway to router R2 for VLAN 2.

Step 4: Configure Switch ports Fa0/1 and Fa0/2 as 802.1Q trunks to carry VLAN information

Step 5: Save the switch running-config configuration to startup-config and copy the switch running-config to a text editor for later use, if needed

Task 6: Configure the Remote Office 2 switch S3

Step 1: Configure the S3 host name, passwords, no domain lookup, and message-of-the-day

Step 2: Configure the VTP domain AnyCompanyX on S3 in client mode with a password of cisco

In client mode, it is not necessary to configure the VLANs on S3 because the information will be obtained from VTP server S1.

You will, however, need to assign ports to the VLANs according to the chart in Part B, Task 4, Step 2.

Step 3: Assign an IP address to the Management/Native VLAN 2 on S3

a. Use the IP address from the Device Interface / IP Address Chart in Part A, Task 3, Step1.

b. Configure the switch with a default gateway to router R2 for VLAN 2.

Step 4: Configure Switch ports Fa0/2 and Fa0/3 as 802.1Q trunks to carry VLAN information

Step 5: Save the switch running-config configuration to startup-config

Step 6: Copy the switch running-config to a text editor and save it for later use, if needed

Task 7: Configure host IP addresses

Step 1: Configure each host IP address and subnet mask

Use the information in the Device Interface / IP Address Chart in Part A, Task 3, Step 1.

Step 2: Configure the default gateway

Use the VLAN information to determine the default gateway for each host. This is the R2 subinterface address in the Device Interface / IP Address Chart in Part A, Task 3, Step 1.

Task 8: Verify device configurations and basic connectivity

Step 1: Before going on to Lab Part C, verify that the devices are correctly configured

Verify that there is basic connectivity as appropriate between devices for AnyCompanyX. Verify the following items and indicate which command you used:

Item to verify	Command used
Basic configuration of HQ (hostname, passwords, etc)	
Basic configuration of R2 (hostname, passwords, etc)	
Basic configuration of S1 (hostname, passwords, etc)	
Basic configuration of S2 (hostname, passwords, etc)	
Basic configuration of S3 (hostname, passwords, etc)	
Correct subinterfaces created on R2 Fa0/0	

Item to verify	Command used
Correct encapsulation on R2 subinterfaces	
Correct VLANs created on each switch	
Ports are in correct VLANs on each switch	
Native VLAN is VLAN 2	
Correct ports are 802.1Q trunks on each switch	
S1 is root switch	
S1 is VTP server	
S2 is VTP client	
S3 is VTP client	
Ping S1 from H1 H2, and H3	
Ping S2 from H1, H2, and H3	
Ping S3 from H1, H2, and H3	
Ping R2 default gateway from H1, H2, and H3	
Ping R2 default gateway from S1, S2, and S3	
Ping from H1 to H2 and H3 (between VLANs)	
Ping HQ from R2	

Part C – Routing, ACLs, and switch security configuration

Task 1: Configure routing for HQ and R2

Step 1: Configure OSPF process 1 for Area 0 on R2

Specify the subnet for each R2 interface using the appropriate wildcard mask.

Step 2: Configure OSPF process 1 for Area 0 on HQ

Step 3: Issue the `show ip route` command on HQ to see the routing table

How many OSPF routes have been learned from R2? __________

Step 4: Configure a default route to the ISP on HQ and propagate this route to R2 using OSPF

Step 5: Verify that R2 has learned about the default route configured on HQ

Use the **`show ip route`** command on R2.

`What is the gateway of last resort for R2?`

____

Step 6: Save the router running-config configuration to startup-config

Task 2: Configure overloaded NAT (PAT) on HQ

Step 1: Configure overloaded NAT (PAT) on HQ

a. Use the IP address on the serial port that connects to the ISP as the overloaded address.

b. Specify the inside and outside NAT interfaces.

Step 2: Ping the Serial 0/0/0 address of the ISP router (209.165.201.1 if AnyCompany1 or 209.165.201.129 if AnyCompany2) from the PC Host H1 command prompt

Was the ping successful? __________

Step 3: Open a browser on host H1 and enter the IP address of the ISP router Serial 0/0/0 interface (209.165.201.1)

Were you able to access the HTTP interface using the browser? __________

Step 4: On the HQ router issue the `show ip nat translations` command

```
HQ#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.201.2:512 172.20.0.2:512     209.165.201.1:512  209.165.201.1:512
tcp 209.165.201.2:1072 172.20.0.2:1072    209.165.201.1:80   209.165.201.1:80
```

For the ping (icmp) entry, what is the inside local address and port number?

____

For the ping (icmp) entry, what is the inside global address and port number?

____

For the browser connection (tcp) entry, what is the inside local address and port number?

____

For the browser connection (tcp), what is the outside global address and port number? _______________

Step 5: Save the router running configuration to NVRAM.

Task 3: Configure port security for the switches

Step 1: Display the MAC address table entry for Fa0/9

This is the port to which H1 is connected. Use the `show` **`mac-address-table int f0/9`** command. You may need to ping from the PC to the switch or other destination to refresh the MAC address table entry.

```
S1#show mac-address-table int f0/9
          Mac Address Table

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  11    000b.db04.a5cd    DYNAMIC     Fa0/9
Total Mac Addresses for this criterion: 1
```

Step 2: Before configuring port security, clear the dynamically learned MAC address entry using the `clear mac-address-table dynamic interface command`

Step 3: Before configuring port security, shut down the port and then issue the port security commands

a. The **`switchport port-security mac-address sticky`** command allows the switch to learn the MAC address currently associated with the port. This address will become part of the running comfiguration. If the running–config is saved to the startup-config, the MAC address will be retained when the switch is reloaded.

b. The **`switchport port-security`** command enables port security on the port using the defaults. The defaults are: 1 MAC address allowed and **`shutdown`** as the violation action to be taken. Enter **`no shutdown`** to bring the port back up so that it can learn the MAC address of the PC.

Step 4: Ping from H1 to the VLAN 11 default gateway

Allow some time to pass and then issue the **`show running-config`** command to see the MAC address that the switch learned.

Step 5: Display the port security for Fa0/9 using the show `port-security interface` command

What is the Port Status? ____________________________________

What is the Security Violation Count? ___________________________

What is the Source Address:Vlan? _____________________________

```
S1#show port-security int fa0/9
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
```

```
            Last Source Address:Vlan   : 000b.db04.a5cd:11
            Security Violation Count   : 0
```

Step 6: Remove the PC H1 cable from switch port Fa0/9 and connect the cable from PC H2

a. Ping from H2 to any IP address to cause a security violation on port Fa0/9. You should see security violation messages.

b. Issue the **`show port-security interface`** command again for Fa0/9.

What is the Port Status? ____

What is the Security Violation Count? ______________________________

What is the Source Address:Vlan? ________________________________)

Step 7: Move the cables for the PCs back to their original ports and restore port Fa0/9

a. Clear the sticky address entry for port Fa0/9.

b. To return the interface from `error disable` to `administratively up`, enter the **`shutdown`** command followed by the **`no shutdown`** command.

Step 8: Save the switch running-config configuration to startup-config

Step 9: Repeat Steps 1 through 6 to set port security for the other two switches, S2 and S3, and save the running config to startup-config

Task 4: Verify overall network connectivity before applying ACLs

Step 1: Before configuring ACLs, verify routing, NAT, and basic connectivity for AnyCompanyX and the ISP

Step 2: Verify the following items and indicate which command you used

Item to verify	Command used
Routing configuration of HQ (OSPF/Static)	
Routing configuration of R2 (OSPF/Static/Summary)	
NAT overload on HQ	
Port security on S1, S2, and S3	
Ping from H1, H2 ,and H3 to HQ S0/0/0	
Ping from H1, H2, and H3 to HQ Lo0 (HQ LAN)	
Ping from H1, H2, and H3 to HQ Lo1 (RO1 LAN)	
Ping from H1, H2, and H3 to ISP S0/0/0	
Ping from H1, H2, and H3 to ISP Discovery CD Server	
Web browser from H1, H2, and H3 to ISP router Loopback or Discovery CD Server address	
Telnet from H1, H2, and H3 to HQ and R2	

Task 5: Configure ACL Security on HQ and R2

NOTE: The following commands are based on IP address ranges for one possible solution to the VLSM scheme in part of the lab. Replace the address ranges with those that match the ones that you applied to the Remote Office 2 Hosts and VLANs.

Step 1: Create and apply an Extended Numbered ACL on the edge router (HQ)

a. The ACL allows replies to requests made by internal hosts to enter the network. Allow internal users to **`ping`** or **`trace`** any location on the Internet but do not allow any **`ping`** or **`trace`** access to people external to the enterprise.

b. Apply the ACL to the NAT outside interface of the HQ router to protect the AnyCompanyX network.

c. Test the ACL by pinging from H1, H2, and H3 to the ISP loopback address or the IP address of the Discovery CD Server.

Were the pings successful? __________

d. Using a browser from H1, H2, and H3, enter the ISP router Loopback0 address or the IP address of the Discovery CD Server.

Were you able to access the web interface of the router or the Web page from the server?

____

Step 2: Create and apply an Extended Named ACL on R2

a. The ACL allows web requests and pings to leave the Remote Office 2 network if they originated in VLANs 1, 11, 12, 13, or 101. Telnet traffic is permitted if it originated in VLAN 12, and FTP traffic is permitted if it originated in VLAN 13. All other traffic is denied.

b. On the R2 router, apply the ACL to each Fa0/0 subinterface except Fa0/0.2, the native VLAN.

c. Test the ACL by pinging from H1, H2, and H3 to the ISP loopback address or the IP address of the Discovery CD Server.

Were the pings successful? __________

d. Using a browser from H1, H2, and H3, enter the ISP router Loopback0 address or the IP address of the Discovery CD Server.

Were you able to access the web interface of the router or the Web page from the server?

____

e. Telnet from Host H1 in VLAN 11 to the HQ router using its S0/0/0 IP address.

Were you able to telnet to it? __________

f. Telnet from Host H2 in VLAN 12 to the HQ router using its S0/0/0 IP address.

Were you able to telnet to it? __________

g. Use the **`show access-lists`** command to verify that the ACL is working.

Step 3: Create and apply a standard ACL to control VTY access to the HQ router

a. The ACL should deny hosts from all VLANs on Remote Office 2 except for Host H2 on VLAN 12. This will still allow other hosts on VLAN 12 to access router R2 using telnet.

b. Apply the ACL to VTY lines 0 through 4 on the R2 router.

c. Telnet from Host H2 in VLAN 12 to the HQ router using its S0/0/0 IP address.

Were you able to telnet to it? ___

d. Change the IP address of H2 to another one that is on VLAN 12 and telnet again from Host H2 in VLAN 12 to the HQ router using its S0/0/0 IP address.

   Were you able to telnet to it? ___

e. Use the **`show access-lists`** command to verify that the ACLs are working.

Step 4: On R2 and HQ, save the router running configuration to NVRAM

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
800 (806)	Ethernet 0 (E0)	Ethernet 1 (E1)		
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
1700	FastEthernet 0 (Fa0)	FastEthernet 1 (Fa1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (Fa0/0)	Fast Ethernet 0/1 (Fa0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
2600	FastEthernet 0/0 (Fa0/0)	FastEthernet 0/1 (Fa0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
NOTE: To find out exactly how the router is configured, look at the interfaces. Doing this will identify the type of router as well as how many interfaces the router has. There is no way to effectively list all of the combinations of configurations for each router class. What is provided are the identifiers for the possible combinations of interfaces in the device. This interface chart does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in IOS command to represent the interface.				

APPENDIX A

CIDR / VLSM Subnet Chart

Base Address: 172.20.0.0		Subnet Mask: 255.255.252.0							
CIDR mask	/22	/23	/24	/25	/26	/27	/28	/29	/30
Dot mask (octets 3&4)	252.0	254.0	255.0	255.128	255.192	255.224	255.240	255.248	255.252
No hosts possible	1,024	512	256	128	64	32	16	8	4
Subnet # (octets 3&4)									

Base Address: 172.20.0.0		**Subnet Mask: 255.255.252.0**							