



Lab 1.1.1 Student Lab Orientation

Objective

In this lab, the students will complete the following tasks:

- Review the lab bundle equipment
- Understand the security pod topology
- Understand the pod naming and addressing scheme
- Load an IOS Firewall image
- Load the default lab configurations
- Cable the standard lab topology
- Test connectivity

Scenario

This lab describes the basics of cabling and configuring the standard lab topology for this course... Students will become familiar with the physical and logical topology that will be used throughout the course. To avoid problems with the lab exercises, proper lab setup and connectivity is required before configuring security. In real world scenarios, it is important to check the network for basic connectivity before proceeding with more advanced configurations.

Topology

Figure 1 illustrates the lab network environment used in the IOS Firewall router to IOS Firewall router lab activities. This topology will also be used in the labs that require configuration of the pod switches:

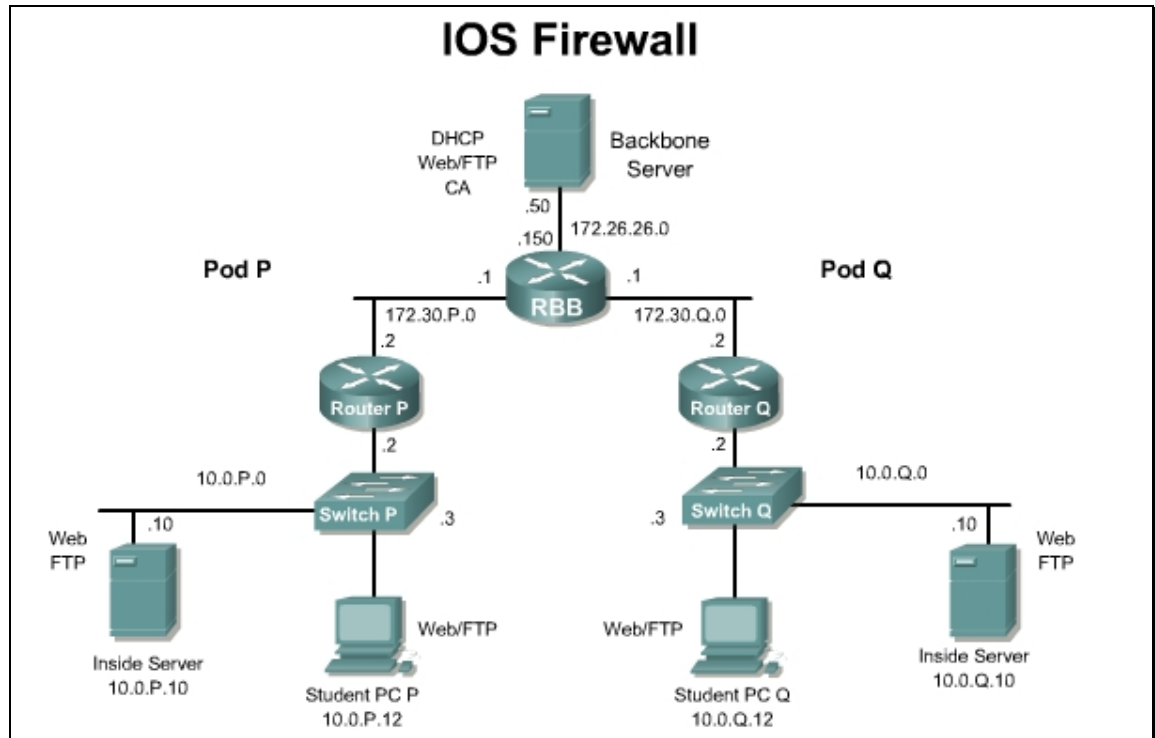


Figure 1

Figure 2 illustrates the lab network environment used in the VPN Client to IOS Firewall router lab activities:

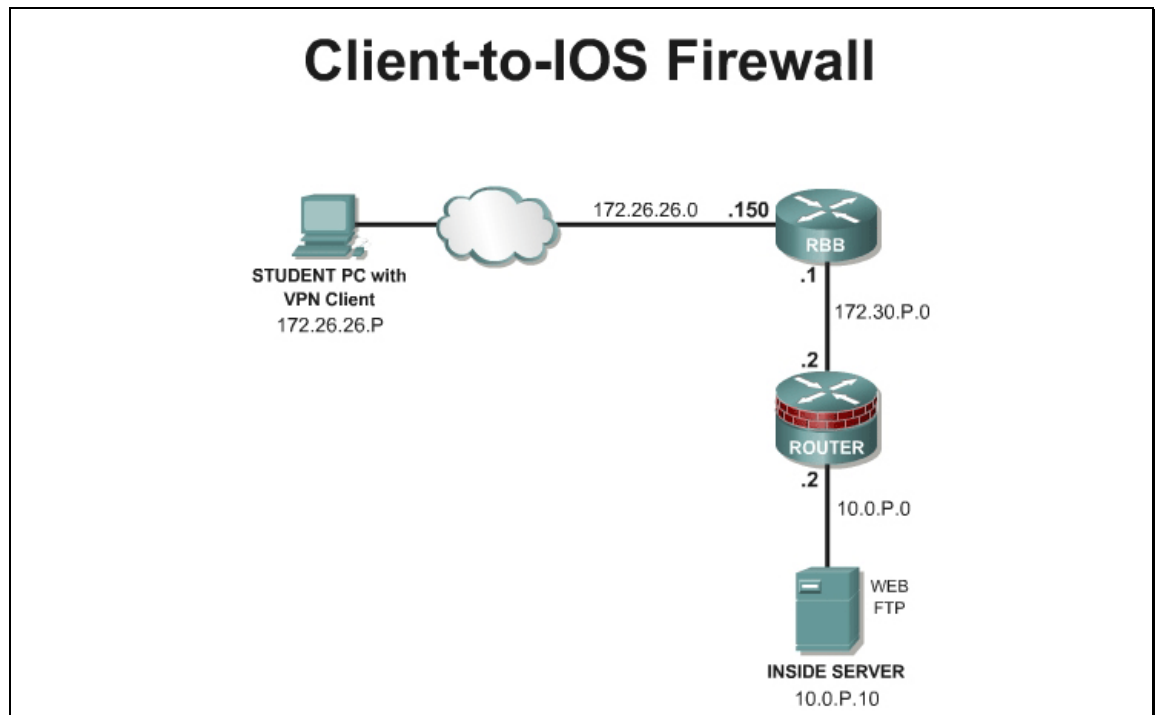


Figure 2

Figure 3 illustrates the lab network environment used in the PIX Security Appliance to PIX Security Appliance lab activities:

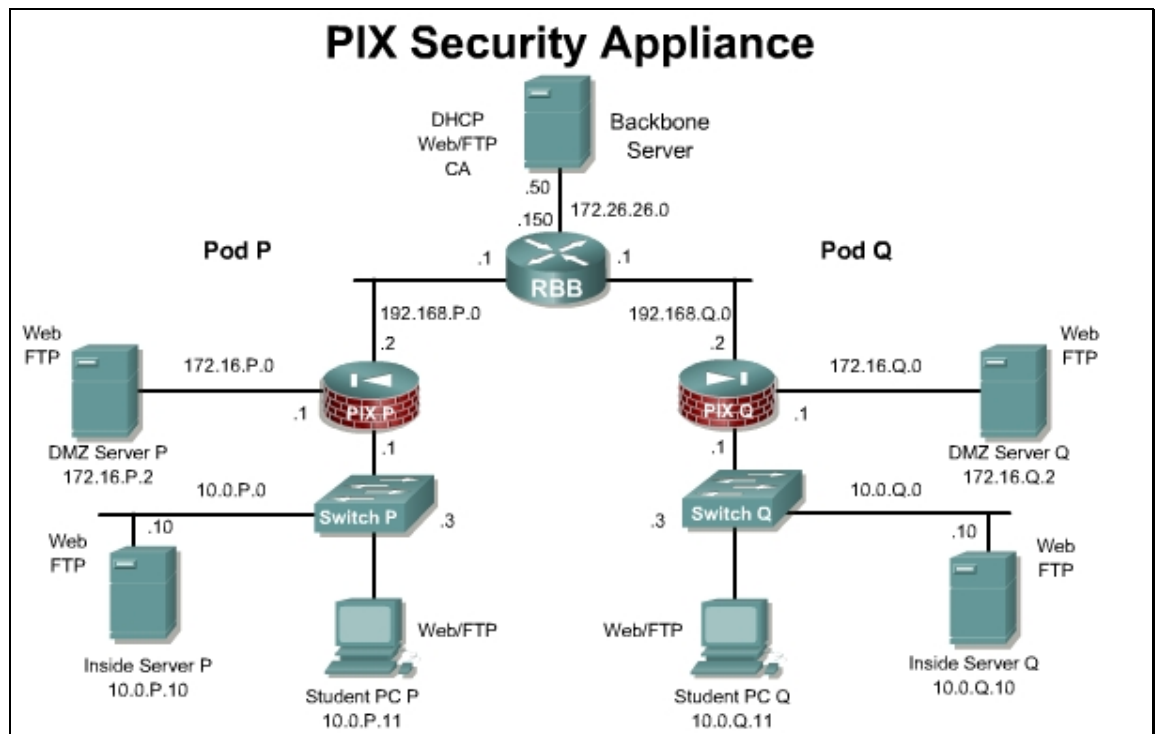


Figure 3

Figure 4 illustrates the lab network environment used in the VPN Client to PIX Security Appliance lab activities:

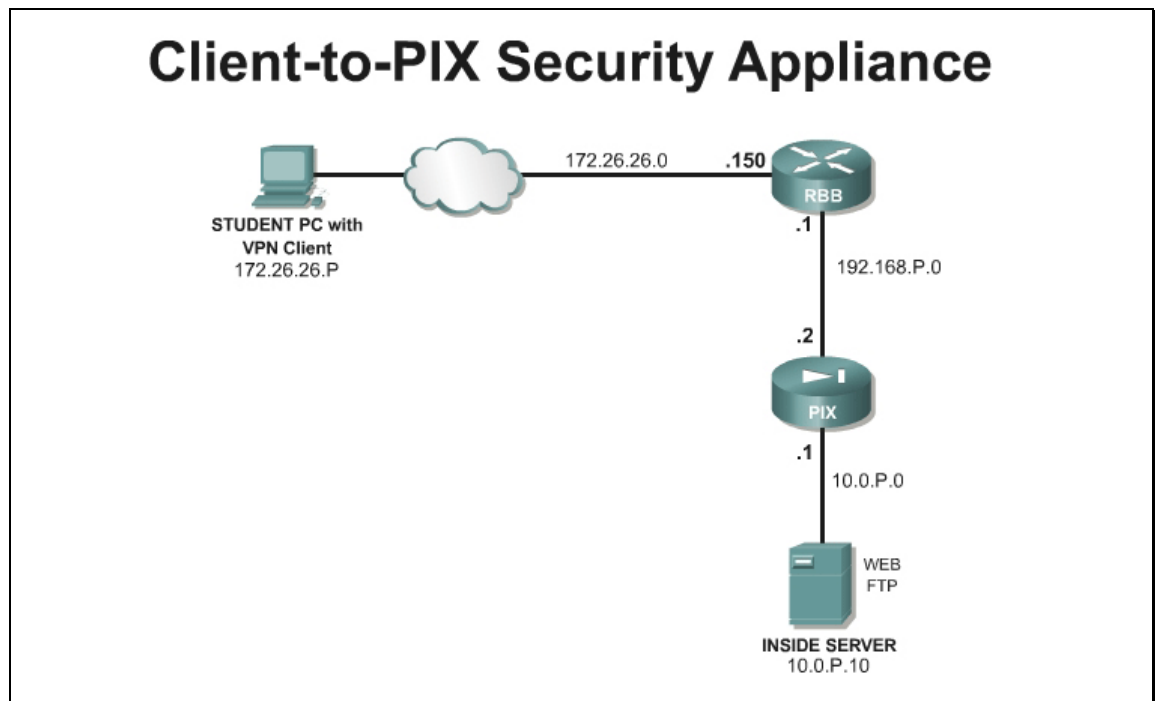


Figure 4

Figure 5 illustrates the logical topology with all of the devices connected.

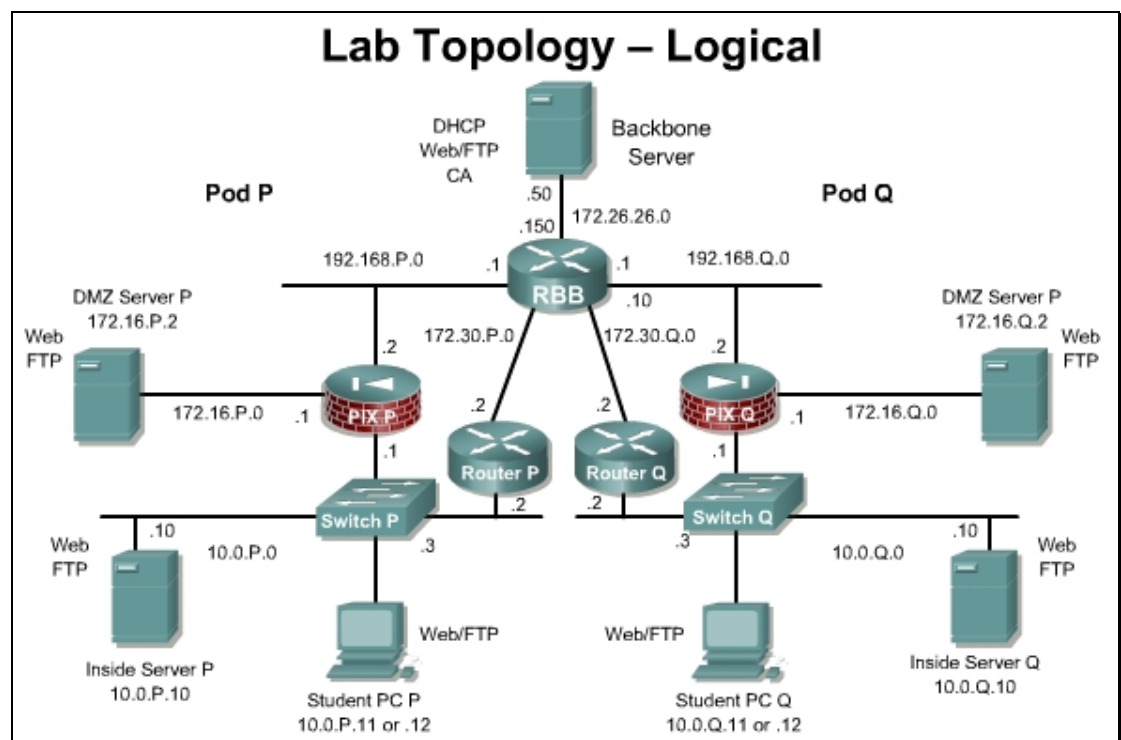


Figure 5

Preparation

There are two basic segments for the router topology:

<u>Name</u>	<u>Trust Level</u>	<u>Common</u>	<u>Network</u>	<u>Physical Port</u>
Inside	Trusted	Private-LAN	10.0.P.0/24	0/0
Outside	Untrusted	Public-WAN	172.30.P.0/24	0/1

There are three basic segments for the PIX Security Appliance topology:

<u>Name</u>	<u>Trust Level</u>	<u>Common</u>	<u>Network</u>	<u>Physical Port</u>
Inside	Trusted	Private - LAN	10.0.P.0/24	Ethernet0
Outside	Untrusted	Public-WAN	172.30.P.0/24	Ethernet1
Demilitarized Zone (DMZ)	Protected	Public Web Services	172.16.P.0/24	Ethernet2

In most of the labs, the physical interface will not be specific as Ethernet0, Fa0/0, E0/0 and so on. Instead, a lab will instruct students to configure the outside interface, the inside interface or the DMZ interface. Students will have to configure the interfaces based on the router or PIX Security Appliance model and interface characteristics.

Note that each topology figure indicates a specific numbering, naming and addressing scheme. The basic lab topology includes two pods. Each pod consists of a router, a PIX Security Appliance, a switch, a student PC, and an inside server. Some academies may have up to 10 pods. Therefore, the labs use **P** and **Q** values. The **P** value in the addressing and naming scheme refers to the assigned Pod router that will be assigned to a team consisting of one to four students. The **Q** value in the naming and addressing scheme is used when testing the security or connectivity with the peer team. For example, the team on Pod 1 router is asked to Ping the neighbor router at 172.30.Q.2. In this case the **Q** will be substituted with a 2.

The basic tasks in most labs are:

- Configure security on the pod device, such as router or PIX Security Appliance.
- Test the security and services through the pod device and through the peer device.

When testing connectivity and security configurations, be careful to observe the prompt. Below are some possible prompts:

- **C:**
- **Router>**
- **http://10.0.P.12**
- **ftp://172.26.26.50**

This is important since testing will be performed from the DOS prompt, a device prompt, or a Web browser.

Tools and Resources:

In order to complete this lab, the following is required:

- Two pod IOS Firewall routers (ROUTER)
- Two pod PIX Security Appliances (PIX)
- Two pod switches (SW)
- Two student PCs (PC) located at 10.0.P.12
- Servers
 - Setup Option 1-Dedicated Devices
 - One Backbone_Internet (BB) Server
 - Two Inside Servers (IS) located at 10.0.P.10
 - Two DMZ Servers (DMZ) located at 172.16.P.2 (Routers can be substituted)
 - Setup Option 2-SuperServer
 - One SuperServer (SS) with Intel Pro Server NIC with VLAN support. The VLAN NIC is only needed if using the SuperServer model.
- One Backbone switch
- One Backbone router
- Two console cables
- HyperTerminal
- Assorted Cat5 patch cables
- One Label machine (Optional)

Additional Materials

None

Command List

In this lab, the following commands will be used to configure the pod routers:

Command	Description
<code>copy run start</code>	Stores the current configuration in RAM into NVRAM.
<code>copy tftp flash</code>	Downloads a new image from the TFTP server to Flash memory.
<code>copy tftp start</code>	Downloads a configuration from the TFTP server into the

Command	Description
	NVRAM
enable	Turns on privileged commands.
show interface	Displays statistics for all interfaces configured on the router.
show ip interface	Displays the status and global parameters associated with an interface.
show ip route	Displays the contents of the IP routing table.
show running-config	Displays the current configuration in RAM
show startup-config	Displays the saved configuration that is stored in NVRAM
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

Step 1 Examine the Devices

- Physically examine each device. Notice the interfaces available on the IOS Router and PIX Security Appliance that are present in the lab environment.
- Notice the devices are labeled with an adhesive label. Below is a sample list of devices that should be labeled:

Router	PIX	Switch	Student PCs
Router1	Pix1	Switch1	Student PC 1
Router2	Pix2	Switch2	Student PC 2

Device	IP Address	Description
RBB	172.26.26.150	backbone router
SW0	172.26.26.200	backbone switch
BB	172.26.26.50	Backbone/Internet server
Inside Server 1	10.0.1.10	Inside Server – Pod 1
Inside Server 2	10.0.2.10	Inside Server – Pod 2
DMZ Server 1	172.16.1.2	DMZ Server – Pod 1
DMZ Server 2	172.16.2.2	DMZ Server – Pod 2

The standard FNS lab bundle equipment will create two standard pods. Each pod can accommodate one team consisting of one to four students. Two students per pod is recommended.

Step 2 Configure Student PCs (PC1, PC2)

- a. On the Student PCs, log in as administrator. Verify that the following list of installed software packages is located on the PC as directed by the instructor:
- Cisco Secure ACS v3.3 – It is recommended that the student PCs must be running Windows 2000 Server to install ACS. If the students PCs are not running Windows 2000 Server, ACS can be installed and run on the Inside servers or the Backbone server. This will require adjustments to the labs using ACS, when defining the AAA server address.
 - Syslog Server – Kiwi or equivalent
 - SSH Client – Putty.exe or equivalent
 - Reconnaissance Tools – such as NMapWin and SNMPWalk
 - VPN Client – Cisco VPN Client 4.6
 - TFTP Server – SolarWinds TFTP Server or equivalent
 - Other applications provided by the instructor
- b. Verify the i386 folder is located on the root drive C:\. This folder is used when adding any Windows components without the Windows Installation CD.

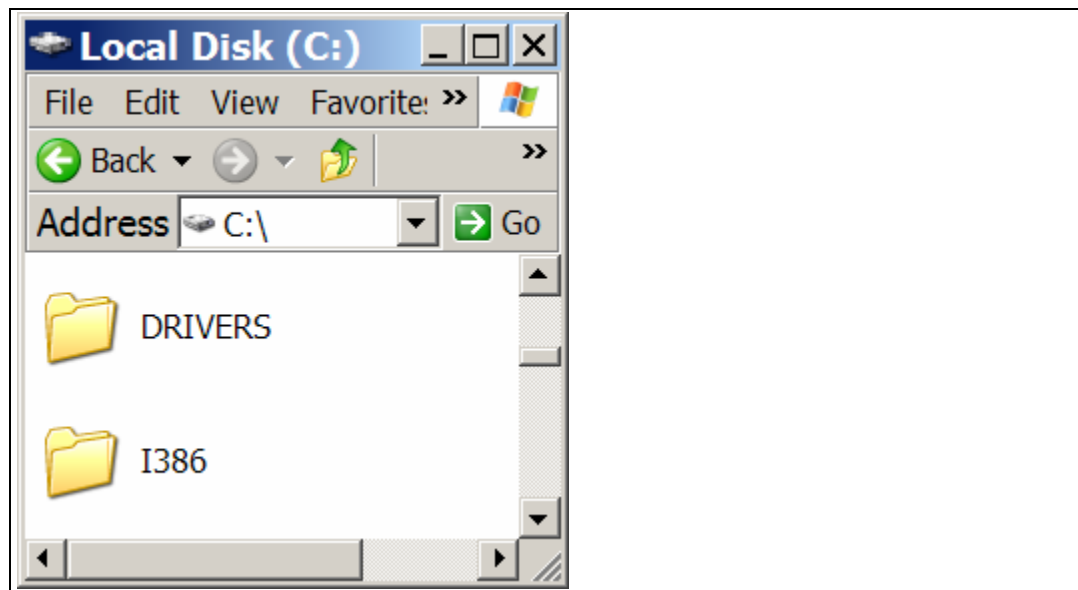


Figure 6

- c. Verify that HyperTerminal or equivalent terminal emulation software is installed.

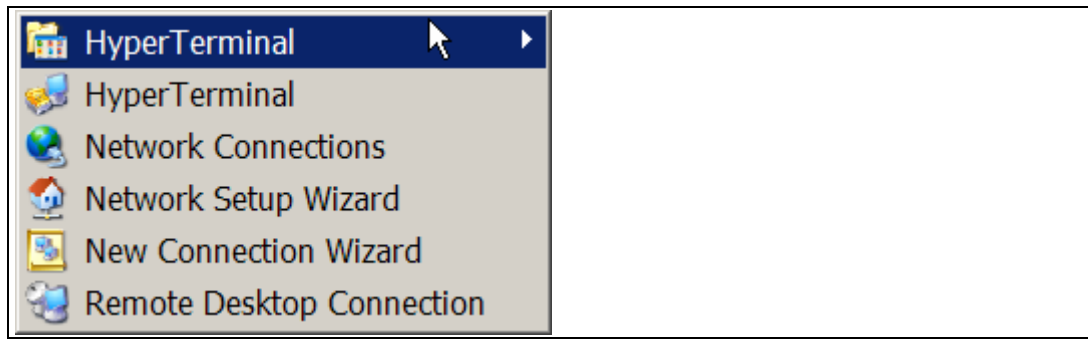


Figure 7

- d. Configure the Student PCs TCP/IP settings and services. For this lab activity, use the router to router settings shown below.

These settings will be used for the router to router labs:

<u>Label</u>	<u>Computer Name</u>	<u>Address</u>	<u>Gateway</u>
Student PC1	PC1	10.0.1.12/24	10.0.1.2
Student PC2	PC2	10.0.2.12/24	10.0.2.2

These settings will be used for the PIX Security Appliance to PIX Security Appliance labs:

<u>Label</u>	<u>Computer Name</u>	<u>Address</u>	<u>Gateway</u>
Student PC1	PC1	10.0.1.11/24	10.0.1.1
Student PC2	PC2	10.0.2.11/24	10.0.2.1

- e. Configure web and FTP services on the Student PCs. The instructor will provide default web pages to install in the wwwroot directory. Place the default configuration of all pod devices in the ftproot directory. The wwwroot and ftproot directories are located in C:\inetpub by default.
- f. Verify the web and FTP sites have been properly configured by opening Internet Services Manager (IIS) or equivalent web services if using another operating system or web server application. To verify that IIS is running, right click the My Computer icon and select **Manage** from the pop-up menu. Click the + icon next to **Services and Applications** to expand the menu and locate IIS.

Step 3 Verify the Lab Topology Cabling

Figure 8 illustrates a port mapping of SW0 in order to cable or verify the physical connections for the dedicated server setup option. Labeling the switch helps facilitate quick recabling when necessary.

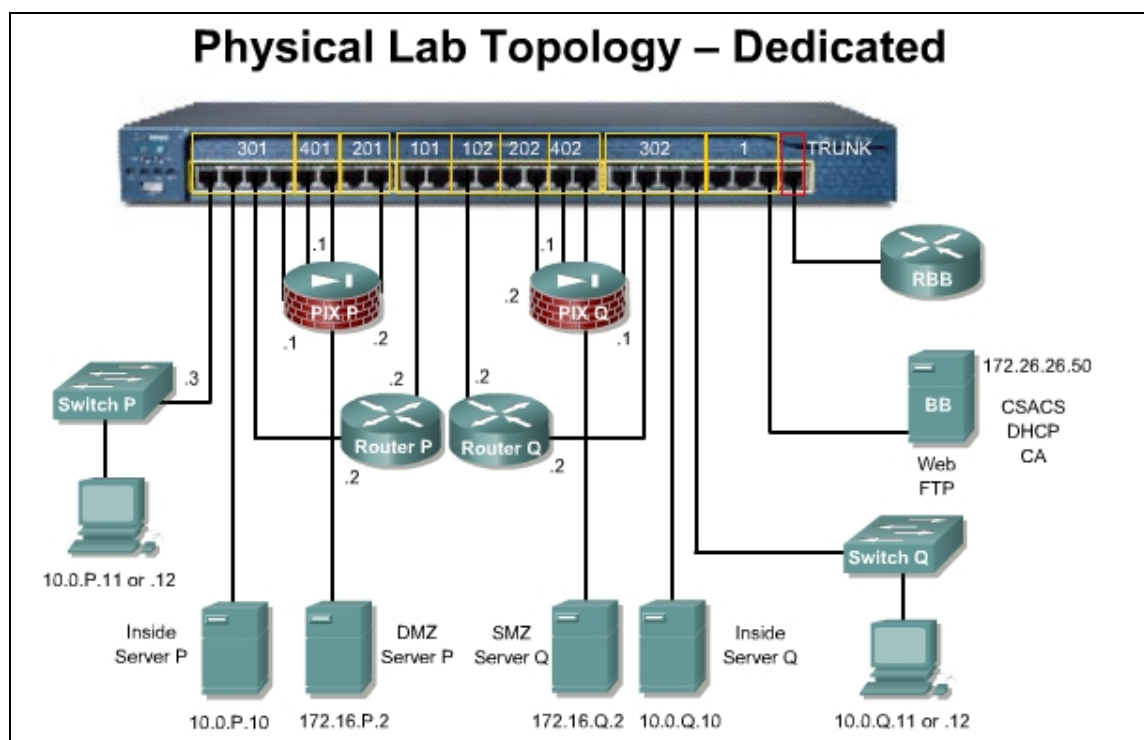
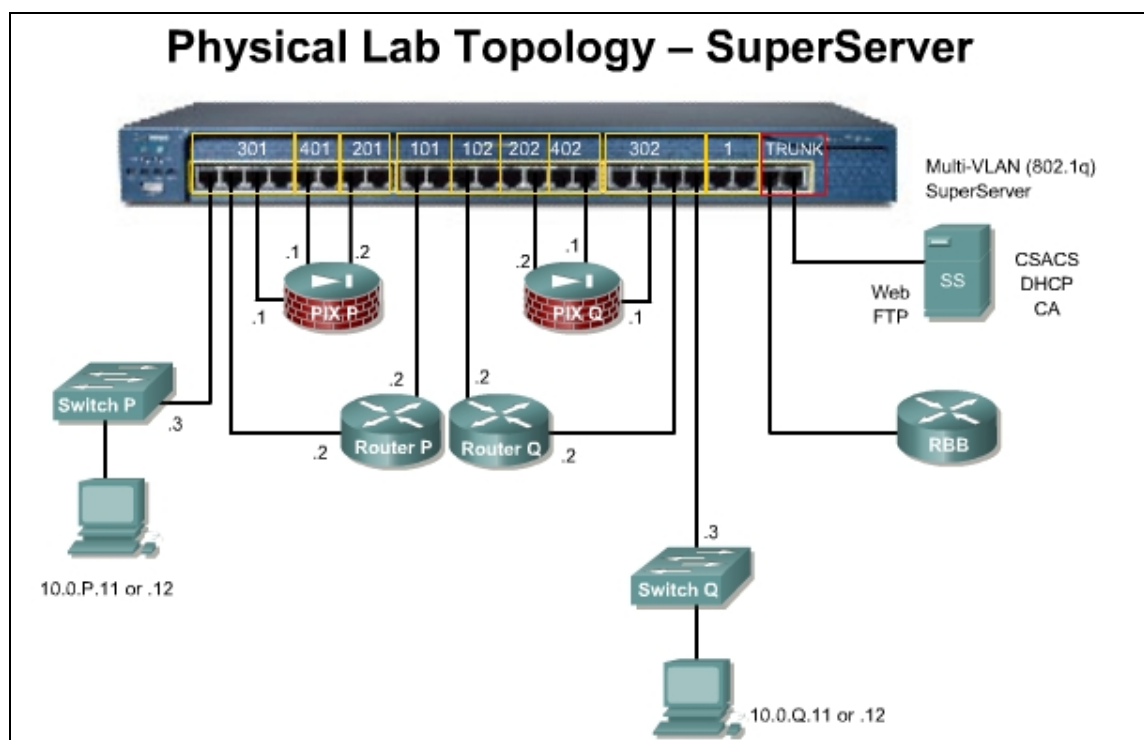


Figure 9 illustrates a sample port mapping of SW0 in order to cable or verify the physical connections for the SuperServer setup option. Labeling the switch helps facilitate quick recabling when necessary.



Step 4 Verify the Software Images on the Pod Devices

- a. Power and test the pod devices. If needed, refer to the appendices to upgrade the IOS image.

Platform	Release	Images
2610XM-2611XM	12.3(14)T Advanced Security	c2600-advsecurityk9-mz.123-14.T1.bin
PIX 515E	7.0(1)	pix701.bin
Catalyst 2950, 2950T	12.1(22)	c2950-i6k2l2q4-mz.121-22.EA4.bin

The router image must be 12.3(8)T or above, as the IOS Intrusion Detection commands are significantly different in earlier IOS versions. If the router has an image that is earlier than 12.3(8)T, the image must be upgraded.

Security Device Manager (SDM) version 2.0 or later will be required for some of the labs. The PIX pod devices should have version 7.0 or higher with Adaptive Security Device Manager (ASDM) version 5.0.

Step 5 Load Default Configurations on Pod Routers

- Reload, configure and verify Pod routers.
- On the respective router, load the following configuration. These text files are available from the instructor.

Pod Router 1	Pod Router 2
<pre> hostname Router1 ! logging console enable password cisco ! username sdm privilege 15 password 0 sdm ! no ip domain-lookup ! ip dhcp excluded-address 10.0.1.1 10.0.1.12 ! ip dhcp pool POD1_INSIDE network 10.0.1.0 255.255.255.0 default-router 10.0.1.2 ! interface FastEthernet0/0 description inside ip address 10.0.1.2 255.255.255.0 no shutdown ! interface FastEthernet 0/1 description outside ip address 172.30.1.2 255.255.255.0 no shutdown ! router eigrp 1 network 10.0.0.0 network 172.30.0.0 no auto-summary ! ip classless ip http server ip http authentication local ! line vty 0 4 password cisco privilege level 15 transport input telnet ssh login local ! end </pre>	<pre> hostname Router2 ! logging console enable password cisco ! username sdm privilege 15 password 0 sdm ! no ip domain-lookup ! ip dhcp excluded-address 10.0.2.1 10.0.2.12 ! ip dhcp pool POD2_INSIDE network 10.0.2.0 255.255.255.0 default-router 10.0.2.2 ! interface FastEthernet 0/0 description inside ip address 10.0.2.2 255.255.255.0 no shutdown ! interface FastEthernet0/1 description outside ip address 172.30.2.2 255.255.255.0 no shutdown ! router eigrp 1 network 10.0.0.0 network 172.30.0.0 no auto-summary ! ip classless ip http server ip http authentication local ! line vty 0 4 password cisco privilege level 15 transport input telnet ssh login local ! end </pre>

- Verify the router configuration and save it to flash.

```

RouterP#show run
RouterP#copy run start

```

The instructor will configure and verify RBB, SW0, and the basic configuration of the pod switches unless directed otherwise by the instructor.

Step 6 Test Connectivity

- a. Verify that the router interfaces are up.

```
RouterP> show ip interface brief
```

- b. Verify the routes.

```
RouterP> show ip route
```

- c. From the router, ping the outside interface of the peer router.

```
RouterP> ping 172.30.Q.2
```

- d. From the PC, ping RBB and the Backbone Server.

```
C:\ ping 172.26.26.150 and C:\ ping 172.26.26.50
```

- e. From the Student PC, ping the Inside Server.

```
C:\ ping 10.0.P.10
```

- f. From a browser on the Student PC, access the ftp/web page of the Inside Server

```
http://10.0.P.10 and ftp://10.0.P.10
```

- g. From the Student PC, ping the inside PC of the peer.

```
C:\ ping 10.0.Q.12
```

- h. From a browser on the Student PC, access the web/ftp page of the Backbone Server

```
http://172.26.26.50 and ftp://172.26.26.50
```

- i. From a browser on the Student PC, access the ftp page of the peer PC

```
http://10.0.Q.12 and ftp://10.0.Q.12
```