Security PIX Pod

Planning and Installation Guide

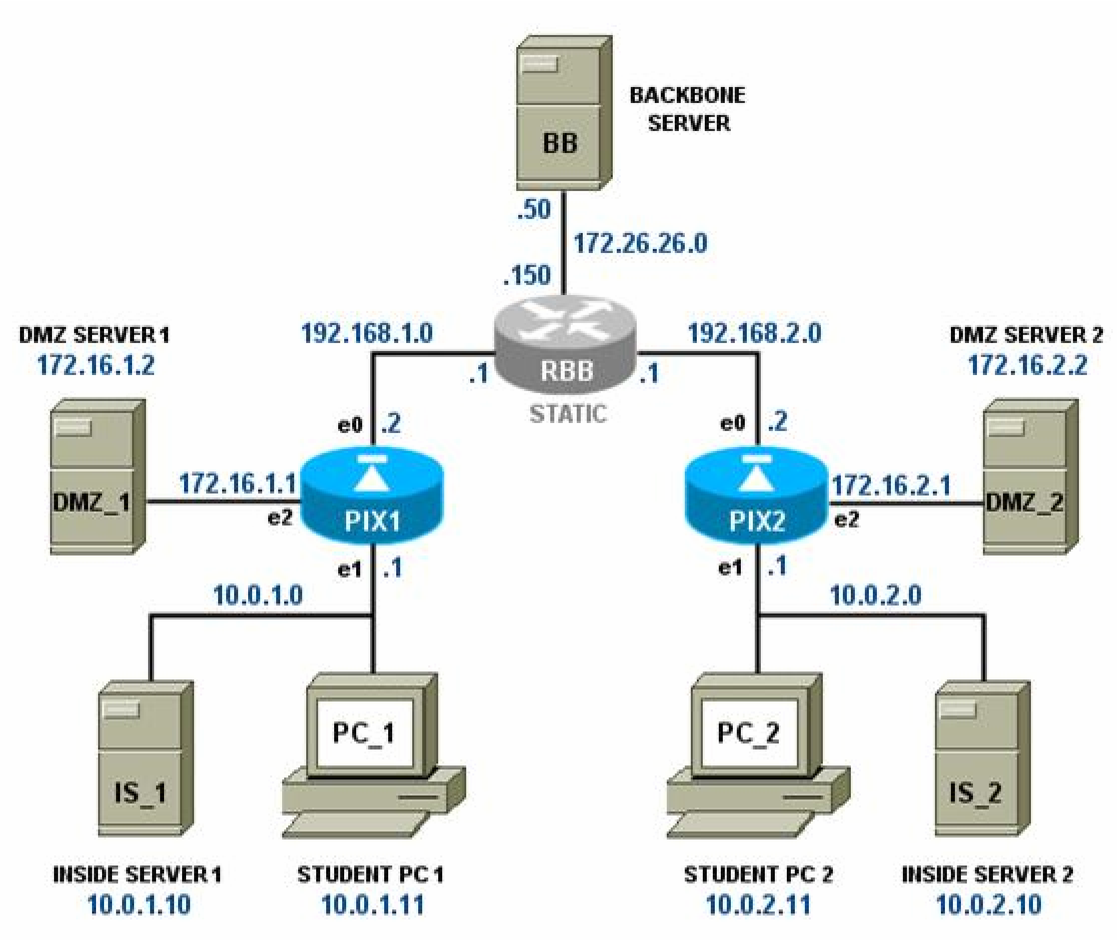
For Cisco Networking Academy® FNSP Curriculum

Document Version: 2005-04-29

PART 1 – PLANNING

1 Introduction

NETLAB Academy Edition® features two pods for use with the *Fundamentals of Network Security* (FNS) curriculum. This guide documents the NETLAB$_{AE}$ Security PIX Pod, used with *FNS: PIX* (FNSP) labs.



You may have up to two Security PIX Pods per NETLAB$_{AE}$ system.

The NETLAB$_{AE}$ Security PIX Pod features direct access to the console of PIX1 and PIX2. Depending on your settings, NETLAB$_{AE}$ can also provide remote access to the keyboard, video, and mouse of PCs and servers in the pod.

1.1 Lab Orientation

This document assumes that you are familiar with the FNS curriculum and labs. In particular, you should review the Student Lab Orientation exercise. This lab provides an overview of the pod, labs, objectives, and general requirements

1.2 Full Pod

The FNSP labs are designed around a two-team model. One team of students configures the left side of the pod, while another team configures the right side. In this scenario, all devices should be implemented. .

1.3 Limited Pod

In additional to supporting the "full pod" (see 1.2), NETLAB$_{AE}$ also offers support for a "limited pod". NETLAB$_{AE}$ users in a team or instructor-led class can share access to a router console or PC. Therefore, all users can work from the left side of the pod (PIX_1, PC_1, IS_1 and DMZ_1) to accomplish the lesson objective while using the right side of pod only for verification (i.e. pings, traces, VPN client, etc.

⇒ In order to reduce operating costs, NETLAB$_{AE}$ does not mandate that you implement every PC and server, nor does it require any particular operating system. You can easily reconfigure the pod settings at any time during the semester, making adjustments and repositioning PCs as needed. Although NETLAB$_{AE}$ gives you lots of flexibility, certain choices may be required by the curriculum and by NETLAB$_{AE}$

1.4 Deviations

Users often contact our technical support team for lab-related problems. Users are typically not aware that there are many NETLAB$_{AE}$ servers and may be easily confused by local deviations from the standard curriculum and labs.

The FNS curriculum is relatively complex and offers many opportunities to "make adjustments to the labs". If your NETLAB$_{AE}$ pods will be made accessible outside your local Academy, you should carefully consider the impact of deviations and substitutions.

Even if your user community is local or relatively small, we recommend that you (1) document the specifics of your pods and (2) use the NETLAB$_{AE}$ *News and Announcements* feature to point users to your documentation.

1.5 Remote PC Support

The Security Pix Pod includes placeholders for 7 remote PCs. You have several options for each PC.

- **Direct/VMware**. The PC is implemented as a VMware GSX virtual machine.
  - Users can control the keyboard, video, and mouse.
  - Users can power on, shutdown, reboot, and revert to a clean state.
  - Users can have administrator rights.
- **Direct/Standalone.** The PC is implemented on a standalone machine, or a virtual product emulating a standalone machine.
  - Users can control the keyboard, video, and mouse.
  - Users can revert to a clean state by rebooting.
  - Users have limited rights (administrative access not recommended).
- **Indirect**. The PC is implemented, but not managed by NETLAB$_{AE}$.
  - Users may be able to interact with the PC, but cannot access the keyboard, video, or mouse through NETLAB$_{AE}$.
- **Absent**. The PC is not implemented.

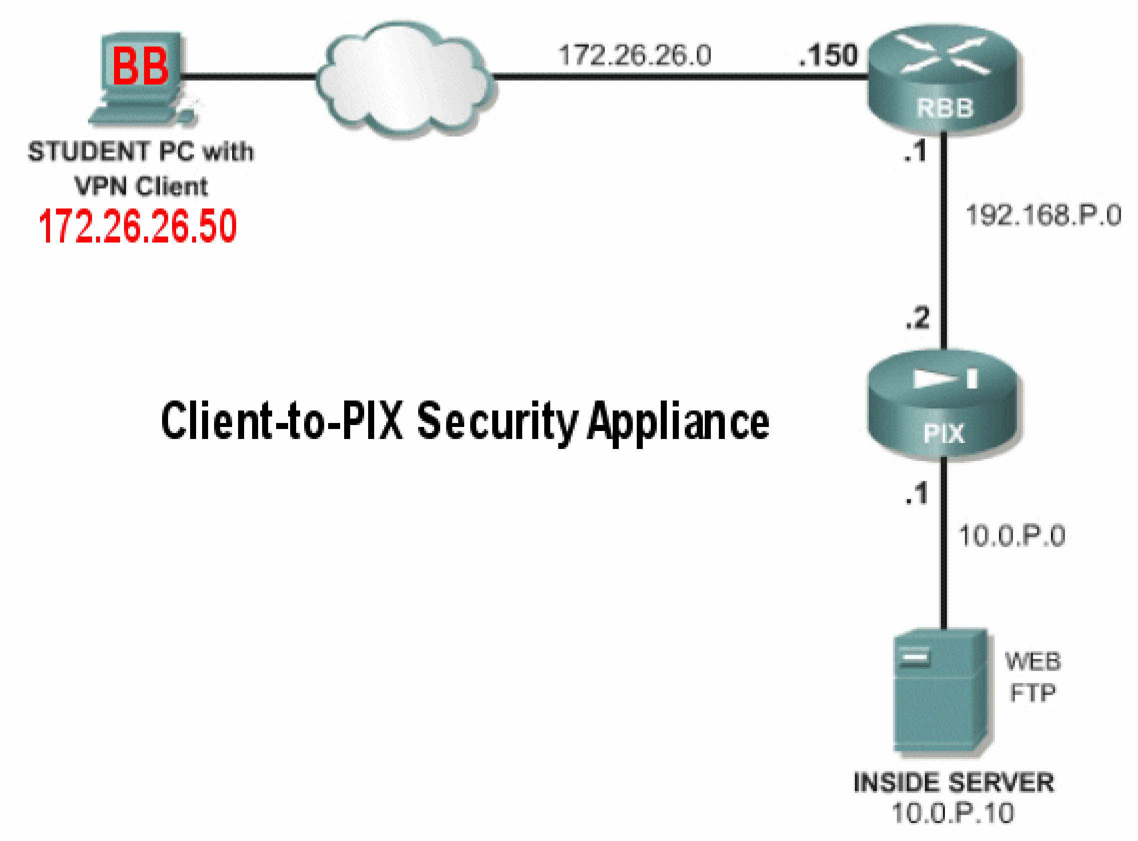
These options are explained in the *NETLAB+ Remote PC Guide*.

Most of the FNSP labs do not require administrative rights on the PC. Therefore, Direct/Standalone remote PCs can be used effectively with FNSP.

Direct/VMware offers complete administrative access on the remote PC and offers the greatest support for FNSP labs.

1.6 Client-to-IOS-Firewall Topology

The FNSP curriculum contains labs that use a *Client-to-IOS Firewall* topology. NETLAB$_{AE}$ does not implement a separate pod type for these labs. You may optionally configure the Backbone Server (BB) for *direct* access by users, and use BB for VPN client exercises. By enabling direct access, BB can also be used as an external PC for labs that require testing from an outside network (i.e. simulating a host on the Internet).



2 Lab Device Requirements

This section describes the requirements for each lab device. Lab devices are part of the topology and users can interact with them either directly or indirectly.

2.1 PIX1 and PIX2

Both PIX security appliances in the Security PIX Pod have the same requirements.

NETLAB$_{AE}$ Supported Devices	Ethernet Ports Required	IOS Release	Image Files
PIX515E PIX5XX[1]	3	6.3(4)	pix634.bin (IOS) pdm-302.bin (pix device manager[2]) np63.bin (password recovery image)

[1] The PIX 501 and PIX 506E but do not support a DMZ.

[2] NETLAB$_{AE}$ does not automatically manage the PDM image.

2.2 Router Backbone (RBB)

RBB is a static router. It is not accessible or configurable by users. However, it is part of the topology so users can indirectly interact with it (i.e. ping, trace, RIP, etc.).

You can implement RBB in one of two ways:

- (1) Use a separate standalone RBB router for each Security PIX Pod
- (2) Simulate RBB for two or more security pods by utilizing multi-VRF on one physical router.

Configuration of each option is covered in detail in section 8.

2.3 Backbone Server / VPN Client PC

The Backbone Server (BB) provides services that are typically provided by Internet servers.

The FNS curriculum provides three options for the backbone server (BB):

- Option 1 – a dedicated BB server.
- Option 2 - one SuperServer with Intel Pro Server NIC with VLAN support, serving as several PCs in the pod.

⇒ **NETLAB$_{AE}$ currently does not support the SuperServer (option 2).** You should use VMware GSX (or other virtualization) products to simulate several machines. Virtual machines have their own routing tables, which avoids asymmetric routing problems in the pod.

FNSP refers to a *Client-to-IOS Firewall* configuration. NETLAB$_{AE}$ does not have a pod type for this topology. However, you may also configure the Backbone Server (BB) for *direct* access, which means that users can login and interact with the Windows interface.

By loading the Cisco VPN client software on BB, users can use the NETLAB$_{AE}$ Security PIX Pod for client-to-IOS firewall labs. Direct access also allows BB to be used as an external PC for labs that require testing from an outside network (i.e. simulating the Internet).

2.4 PCs and Servers

The Security PIX Pod includes placeholders for 7 remote PCs. Please refer to section 1.5 and the *NETLAB+ Remote PC guide*.

3 Control Device Requirements

NETLAB$_{AE}$ *control devices* provide internal connectivity, console access, and managed power. Control devices are dynamically managed by NETLAB$_{AE}$ and are not accessible or configurable by end users.

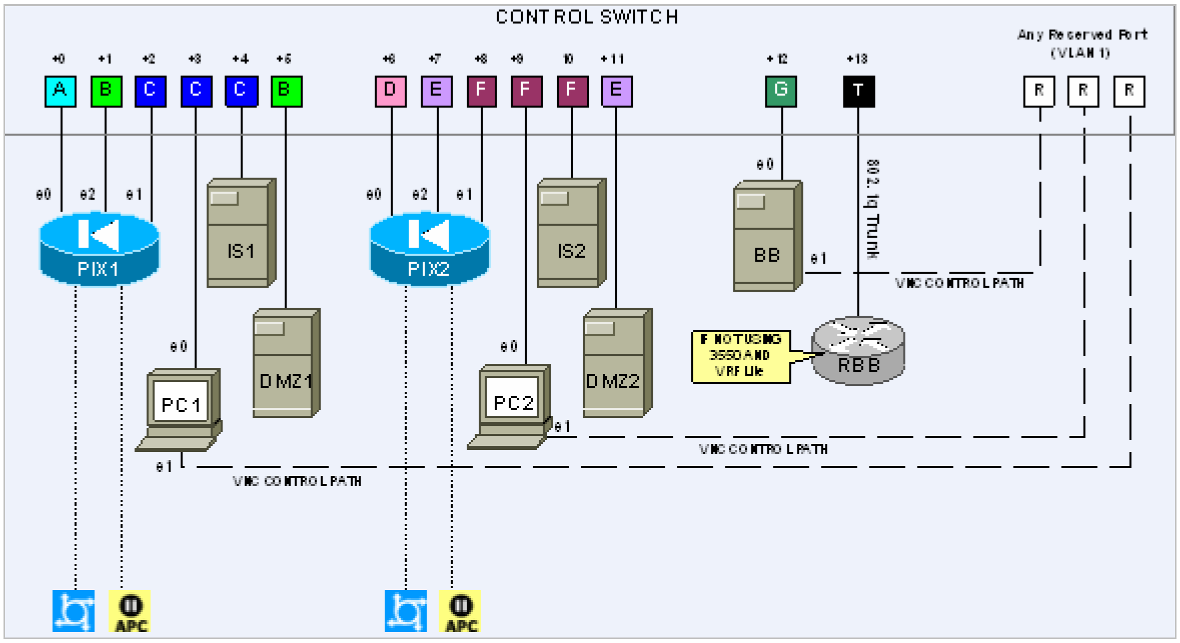
⇒ Management of control devices is covered in the *NETLAB+ Administrator Guide*.

The Security PIX Pod requires the following control device resources:

Control Device Resource	Quantity Required
Control Switch	14 consecutive ports + Up to 5 Reserved Ports
Access Server	2 lines
Switched Outlet Devices	2 outlets

3.1 Control Switch Overview

NETLAB$_{AE}$ uses a control switch to provide connectivity between devices in the Security PIX Pod.



⇒ Academy FNS labs refer to SW0. This device is not implemented in NETLAB$_{AE}$. In addition, the NETLAB$_{AE}$ cable scheme (depicted above) is different from SW0.

The Security PIX Pod requires 14 consecutive ports on a supported control switch (other than a Catalyst 1900 series).

⇒ A Catalyst 1900 series control switch cannot be used because 802.lq trunking is not supported.

Ports are labeled +0 to +13 in the diagram and are relative to the *base port* of your choice. As with all pods, you choose a base port for the Security PIX Pod. To determine the actual port numbers, simply add the base port number chosen for this pod to the depicted relative port numbers. For example, if the base port is 5, the actual port numbers will be 5 to 14.

Using SNMP, NETLAB$_{AE}$ will automatically assign and program VLANs on ports +0 to +12. These VLANs are depicted as letters A, B, C, D, E, F, and G. Each NETLAB$_{AE}$ pod has a unique *VLAN pool* and the actual VLAN numbers will be unique for each NETLAB$_{AE}$ pod. This is to avoid conflict between pods.

Port +13 provides a trunk port if you choose to implement RBB as a separate router (see 8.2). Alternatively, you can use this port to provide trunking for multiple security pods in conjunction with the multi-VRF approach outlined in section 8.3.

You also need a reserved control switch port for each **Direct/Standalone** remote PC. These ports (depicted as R) connect to the PC's 2nd interface and provide a control path for NETLAB$_{AE}$ Remote PC software functions. The control path (1) allows users to access the keyboard, video, and mouse and (2) allows NETLAB$_{AE}$ to communicate with the PC through an API.

3.2 Access Server

Access servers provide console connections to lab routers, lab switches, and lab firewall devices so that users can access these devices from NETLAB$_{AE}$. The Security PIX Pod requires two access server ports. These ports provide console access to PIX1 and PIX2.

3.3 Switched Outlets

Switched outlets provide managed electrical power, allowing NETLAB$_{AE}$ and users to turn lab equipment on and off. The Security PIX Pod requires a switched outlet for PIX1 and PIX2.

PART 2 - IMPLEMENTATION

4 Pre-requisites

This section covers tasks that should be executed prior to adding a Security PIX Pod.

4.1 Setup Control Devices

Using the guidelines in section 3, decide which control switch ports, access server ports, and switched outlets you will use for your Security PIX Pod. Add control devices if necessary. Control device configuration is documented in the *NETLAB+ Administrator Guide.*

4.2 Upload IOS Images

Upload the PIX software images and password recovery images (i.e. np63.bin) for PIX1 and PIX2. NETLAB$_{AE}$ will recover lost software images on the appliance if they are erased from flash. The password recovery image will be used to perform password recovery, and to scrub the PIX.

4.3 Disable User Logins (optional)

You must take all equipment pods offline to add pods or configure control devices. You may wish to disable user logins during this time.

5 Adding the Pod

This section walks you through the process of adding a Security PIX Pod using the NETLAB$_{AE}$ New Pod Wizard.

5.1 Start the New Pod Wizard

Login to the administrator account.

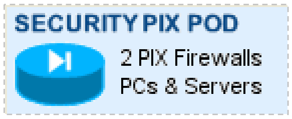
Select Equipment Pods.

Select Take All OFFLINE if any of the pods are online. Caution: this will cancel any reservations in progress.

Select Add a Pod.

The New Pod Wizard will now help you add an equipment pod to your system.

5.2 Add a Security PIX Pod



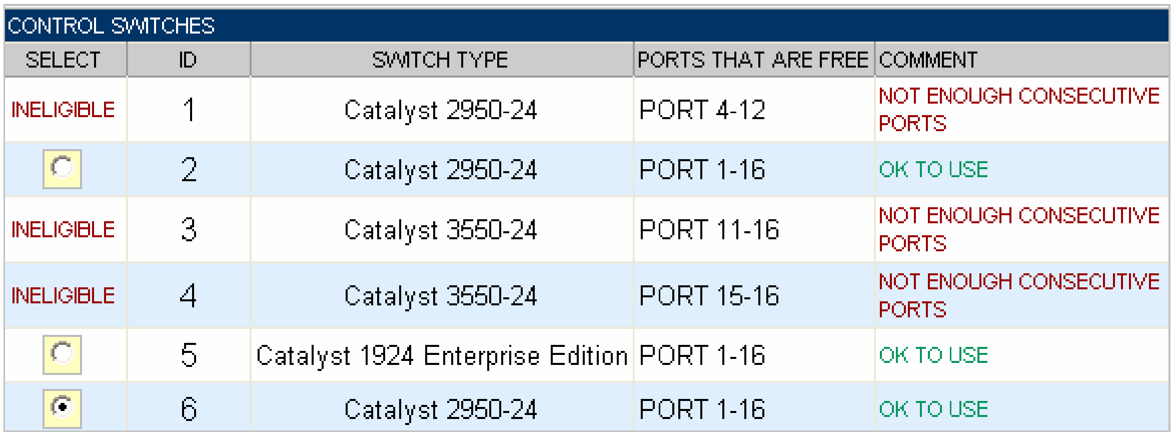
SECURITY PIX POD

2 PIX Firewalls
PCs & Servers

When prompted, select Security PIX Pod.

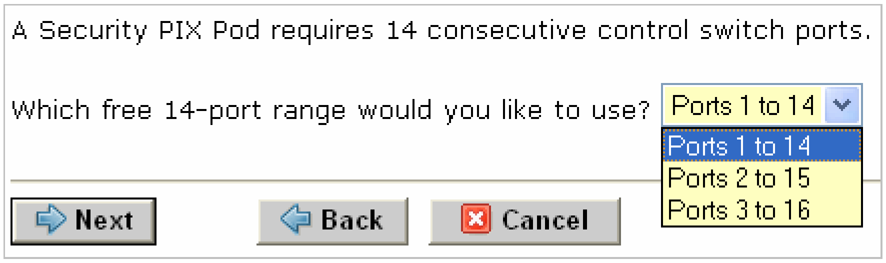
5.3 Select Control Switch and Ports

A Security PIX Pod requires 14 consecutive control switch ports. NETLAB$_{AE}$ will present a list of the control switches on your system. Switches that meet the port requirement can be selected. Choose one control switch for your new pod.



CONTROL SWITCHES				
SELECT	ID	SWITCH TYPE	PORTS THAT ARE FREE	COMMENT
INELIGIBLE	1	Catalyst 2950-24	PORT 4-12	NOT ENOUGH CONSECUTIVE PORTS
○	2	Catalyst 2950-24	PORT 1-16	OK TO USE
INELIGIBLE	3	Catalyst 3550-24	PORT 11-16	NOT ENOUGH CONSECUTIVE PORTS
INELIGIBLE	4	Catalyst 3550-24	PORT 15-16	NOT ENOUGH CONSECUTIVE PORTS
○	5	Catalyst 1924 Enterprise Edition	PORT 1-16	OK TO USE
●	6	Catalyst 2950-24	PORT 1-16	OK TO USE

Next, select the ports you want to use.



A Security PIX Pod requires 14 consecutive control switch ports.

Which free 14-port range would you like to use? Ports 1 to 14

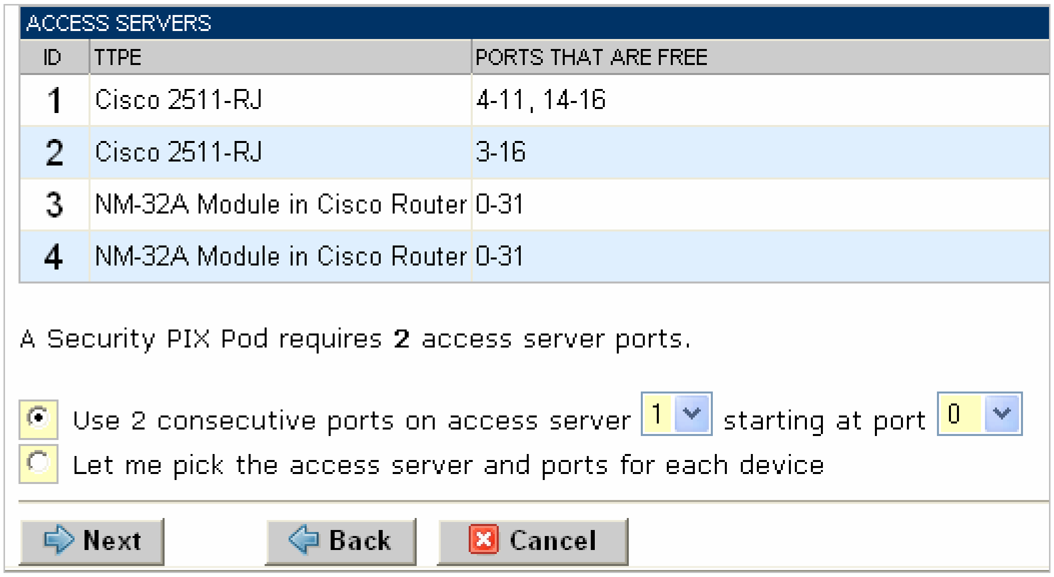
5.4 Select Access Server(s) and Ports

A Security PIX Pod requires 2 access server ports.

It is a good idea to use consecutive ports on one access server if possible. This practice will make it easier to cable and troubleshoot. If consecutive ports are not available, you can use non-consecutive ports, on different access servers if necessary.

When specifying ports, use the port numbers shown on the access server itself. Some models start at port 1 (Cisco 2509 and 2511) and others start at port 0 (Cisco NM-16A and NM-32A modules).

NETLAB$_{AE}$ allows you to choose consecutive ports on one access server, or you can choose “Let me pick” to select an access server and port for each device.



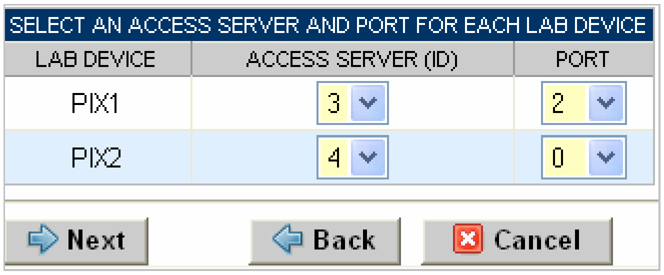
ACCESS SERVERS

ID	TTPE	PORTS THAT ARE FREE
1	Cisco 2511-RJ	4-11, 14-16
2	Cisco 2511-RJ	3-16
3	NM-32A Module in Cisco Router	0-31
4	NM-32A Module in Cisco Router	0-31

A Security PIX Pod requires **2** access server ports.

● Use 2 consecutive ports on access server 1 starting at port 0
○ Let me pick the access server and ports for each device

“Let me pick”, allows you to make granular selections.



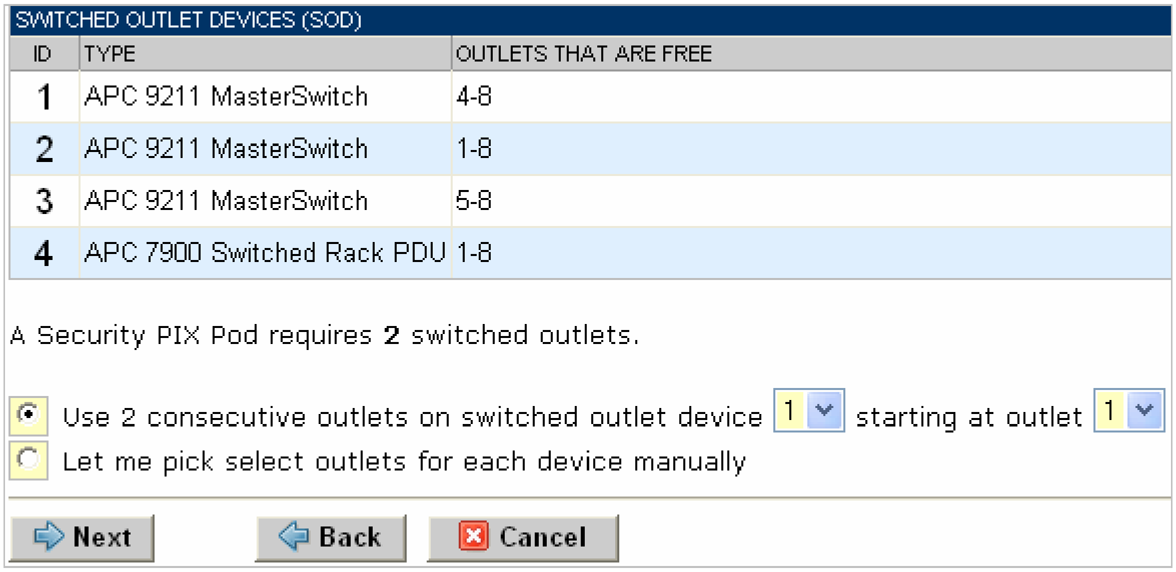
SELECT AN ACCESS SERVER AND PORT FOR EACH LAB DEVICE

LAB DEVICE	ACCESS SERVER (ID)	PORT
PIX1	3	2
PIX2	4	0

5.5 Select Switched Outlets

A Security PIX Pod requires 2 switched outlets.

It is a good idea to use consecutive outlets on one switched outlet device (SOD) if possible. This practice will make it easier to cable and troubleshoot. If consecutive outlets are not available, you may use non-consecutive outlets, spanning multiple SODs if necessary.



SWITCHED OUTLET DEVICES (SOD)

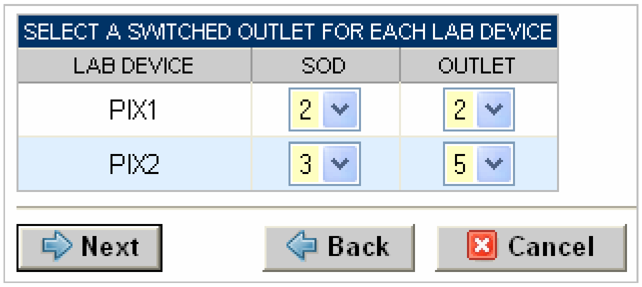
ID	TYPE	OUTLETS THAT ARE FREE
1	APC 9211 MasterSwitch	4-8
2	APC 9211 MasterSwitch	1-8
3	APC 9211 MasterSwitch	5-8
4	APC 7900 Switched Rack PDU	1-8

A Security PIX Pod requires **2** switched outlets.

● Use 2 consecutive outlets on switched outlet device 1 starting at outlet 1

○ Let me pick select outlets for each device manually

"Let me Pick", will allow you to make granular selections.



SELECT A SWITCHED OUTLET FOR EACH LAB DEVICE

LAB DEVICE	SOD	OUTLET
PIX1	2	2
PIX2	3	5

5.6 Select Models for Lab Devices

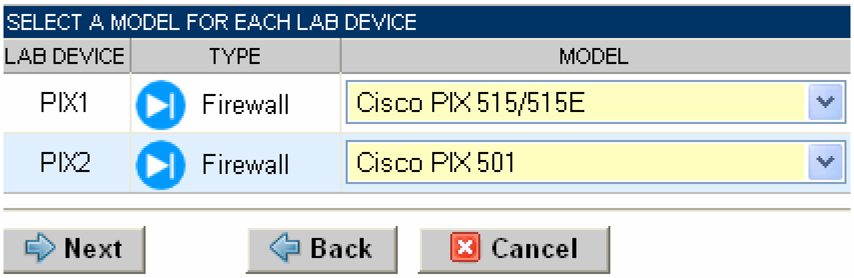
Please specify a model for PIX1 and PIX2. RBB is a statically configured router, so it does not appear in the device selection process

⇒ Your selections are used to assign the appropriate NETLAB$_{AE}$ device driver.

⇒ Improper selections may cause errors.

⇒ NETLAB$_{AE}$ may offer selections that meet the port requirements, but do not support the curriculum. See section 2.1 for a list of supported devices.

⇒ **The PIX 501 or PIX 506E does not support a DMZ segment.**

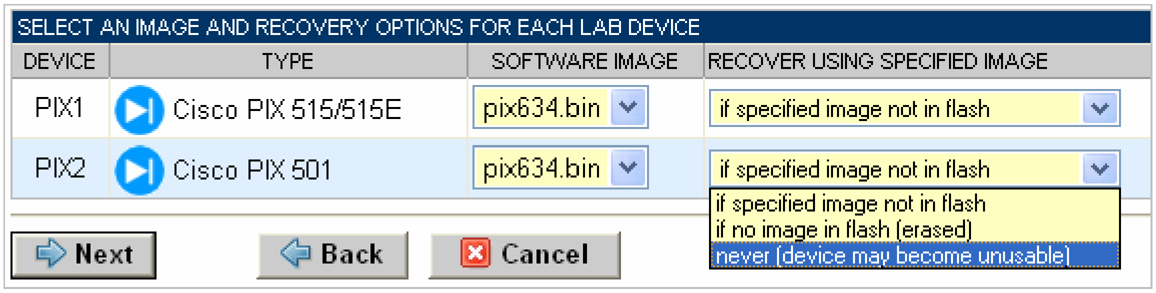


SELECT A MODEL FOR EACH LAB DEVICE

LAB DEVICE	TYPE	MODEL
PIX1	Firewall	Cisco PIX 515/515E
PIX2	Firewall	Cisco PIX 501

5.7 Select Software Images and Recovery Options

NETLAB$_{AE}$ scrubs PIX1 and PIX2 at the end of lab reservation or upon request. During a scrub, NETLAB$_{AE}$ can recover a PIX image if it has been erased from flash.



SELECT AN IMAGE AND RECOVERY OPTIONS FOR EACH LAB DEVICE

DEVICE	TYPE	SOFTWARE IMAGE	RECOVER USING SPECIFIED IMAGE
PIX1	Cisco PIX 515/515E	pix634.bin	if specified image not in flash
PIX2	Cisco PIX 501	pix634.bin	if specified image not in flash

if specified image not in flash
if no image in flash (erased)
never (device may become unusable)
Next
Back
Cancel

You have three choices for flash recovery:

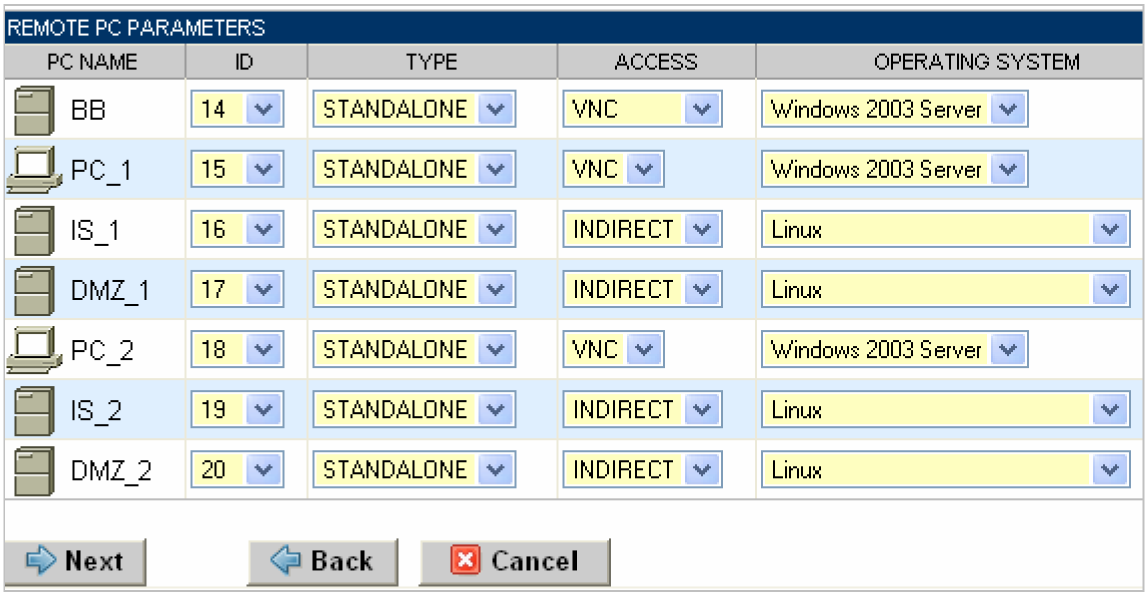
Recovery Using Specified Image	During A Scrub Operation…
If specified image not in flash	Restores the selected software image if that image is not in flash.
If no image in flash (erased)	Restores the selected software image if there are no .bin images in flash. No action is taken if flash contains a .bin image (even if it is not the specified one).
Never (device may become unusable)	NETLAB$_{AE}$ will take no action if the flash does not contain a bootable image. In this case, NETLAB$_{AE}$ automated boot process will fail and manual restoration of IOS will be required.

⇒ If you select an automatic recovery option, you must also select a software image supported by the curriculum (see 2.1).

5.8 Select PC Options

Section 2.4 discussed various options for your pod's PCs and servers. In this task, you will select an ID, type, access method, and operating system for your PCs and servers.

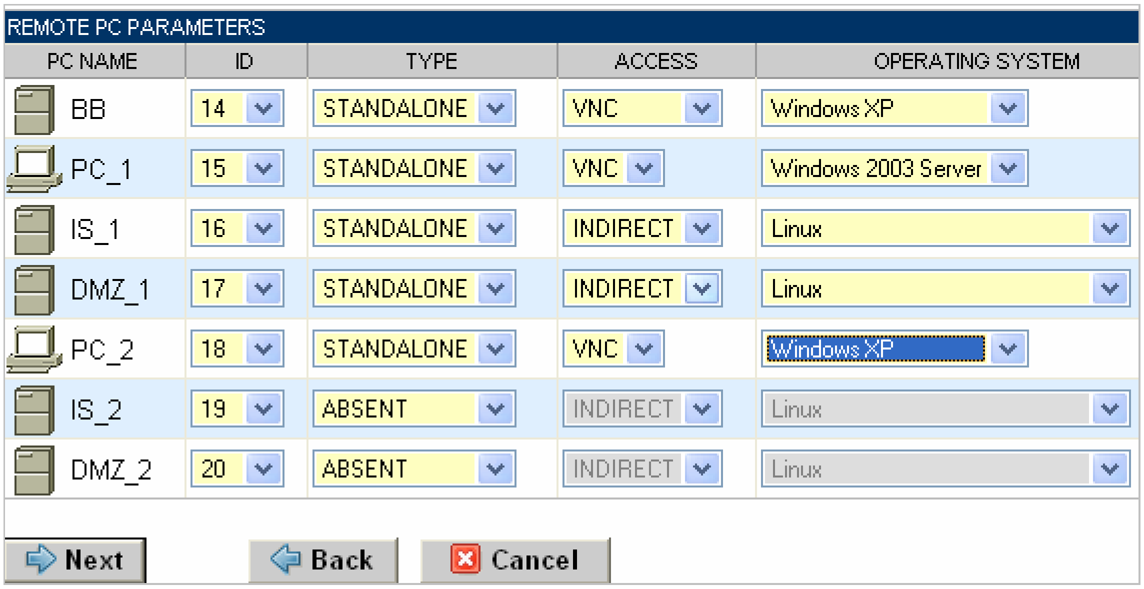
Figure 5.8.1 – Typical PC settings for a full pod (discussed in 1.2)



REMOTE PC PARAMETERS

PC NAME	ID	TYPE	ACCESS	OPERATING SYSTEM
BB	14	STANDALONE	VNC	Windows 2003 Server
PC_1	15	STANDALONE	VNC	Windows 2003 Server
IS_1	16	STANDALONE	INDIRECT	Linux
DMZ_1	17	STANDALONE	INDIRECT	Linux
PC_2	18	STANDALONE	VNC	Windows 2003 Server
IS_2	19	STANDALONE	INDIRECT	Linux
DMZ_2	20	STANDALONE	INDIRECT	Linux

Figure 5.8.2 – Typical PC settings for a limited pod (discussed in 1.3)



REMOTE PC PARAMETERS

PC NAME	ID	TYPE	ACCESS	OPERATING SYSTEM
BB	14	STANDALONE	VNC	Windows XP
PC_1	15	STANDALONE	VNC	Windows 2003 Server
IS_1	16	STANDALONE	INDIRECT	Linux
DMZ_1	17	STANDALONE	INDIRECT	Linux
PC_2	18	STANDALONE	VNC	Windows XP
IS_2	19	ABSENT	INDIRECT	Linux
DMZ_2	20	ABSENT	INDIRECT	Linux

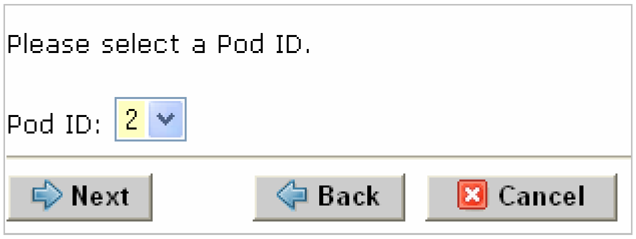
The following table describes the four most common settings as described in section 1.5:

To implement…	Set TYPE to…	Set ACCESS to…
Direct/VMware (available 2Q05)	**VMWARE**	**VNC**
Direct/Standalone	**STANDALONE**	**VNC**
Indirect	(any)	**INDIRECT**
Absent (no PC)	**ABSENT**	n/a

Detail descriptions of these settings are provided in the *NETLAB+ Remote PC Guide*.

5.9 Select a Pod ID

Each pod is assigned a unique numeric ID.

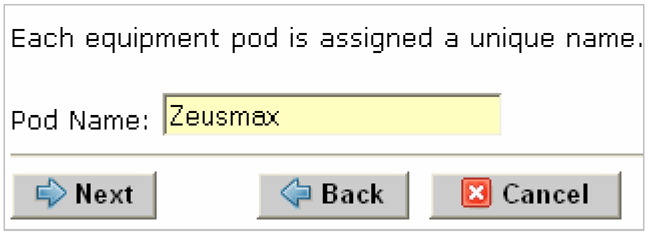


Please select a Pod ID.

Pod ID: 2

5.10 Select a Pod Name

Each pod can have a unique name. This name will appear in the scheduler, along with the pod type.

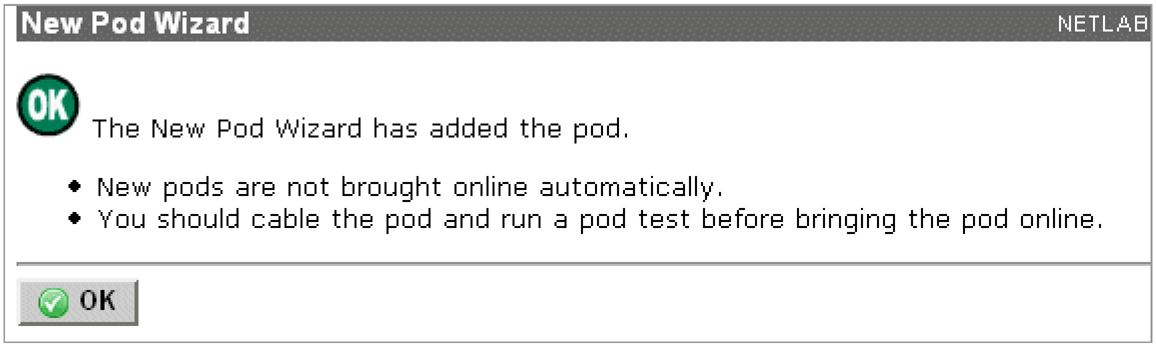


Each equipment pod is assigned a unique name.

Pod Name: Zeusmax

5.11 Verify Your Settings

At this point NETLAB$_{AE}$ has added the pod to its database. However, the pod has not been brought online yet. You will want to cable up the pod, configure PCs, configure router RBB, and run a pod test before bringing the pod online. These tasks are discussed in the remaining sections.



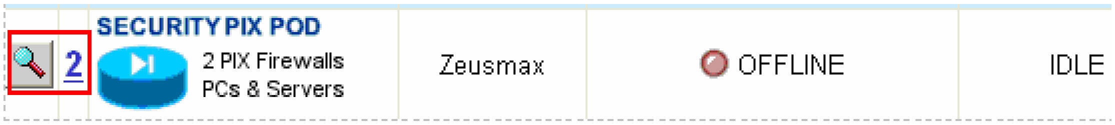
New Pod Wizard NETLAB

OK The New Pod Wizard has added the pod.

- New pods are not brought online automatically.
- You should cable the pod and run a pod test before bringing the pod online.

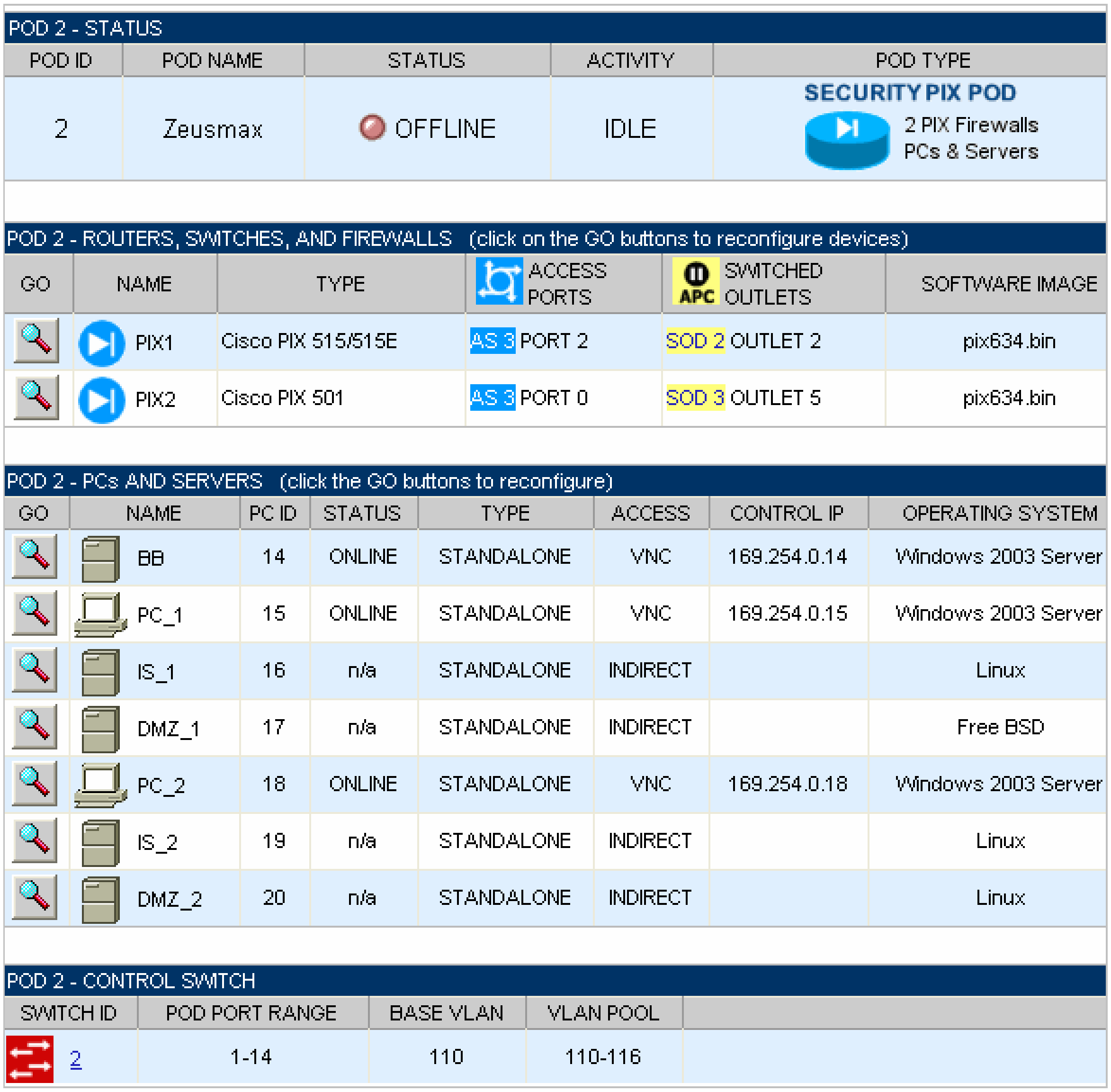
After you click OK, the new pod will appear in the list of equipment pods.

Click on the magnifier button or pod ID to manage you new pod.



🔍	2	SECURITY PIX POD 2 PIX Firewalls PCs & Servers	Zeusmax	● OFFLINE	IDLE

NETLAB$_{AE}$ will display the status of the pod and the high-level settings for each device, PC, and control switch.



POD 2 - STATUS

POD ID	POD NAME	STATUS	ACTIVITY	POD TYPE
2	Zeusmax	● OFFLINE	IDLE	SECURITY PIX POD 2 PIX Firewalls PCs & Servers

POD 2 - ROUTERS, SWITCHES, AND FIREWALLS (click on the GO buttons to reconfigure devices)

GO	NAME	TYPE	ACCESS PORTS	SWITCHED OUTLETS	SOFTWARE IMAGE
	PIX1	Cisco PIX 515/515E	AS 3 PORT 2	SOD 2 OUTLET 2	pix634.bin
	PIX2	Cisco PIX 501	AS 3 PORT 0	SOD 3 OUTLET 5	pix634.bin

POD 2 - PCs AND SERVERS (click the GO buttons to reconfigure)

GO	NAME	PC ID	STATUS	TYPE	ACCESS	CONTROL IP	OPERATING SYSTEM
	BB	14	ONLINE	STANDALONE	VNC	169.254.0.14	Windows 2003 Server
	PC_1	15	ONLINE	STANDALONE	VNC	169.254.0.15	Windows 2003 Server
	IS_1	16	n/a	STANDALONE	INDIRECT		Linux
	DMZ_1	17	n/a	STANDALONE	INDIRECT		Free BSD
	PC_2	18	ONLINE	STANDALONE	VNC	169.254.0.18	Windows 2003 Server
	IS_2	19	n/a	STANDALONE	INDIRECT		Linux
	DMZ_2	20	n/a	STANDALONE	INDIRECT		Linux

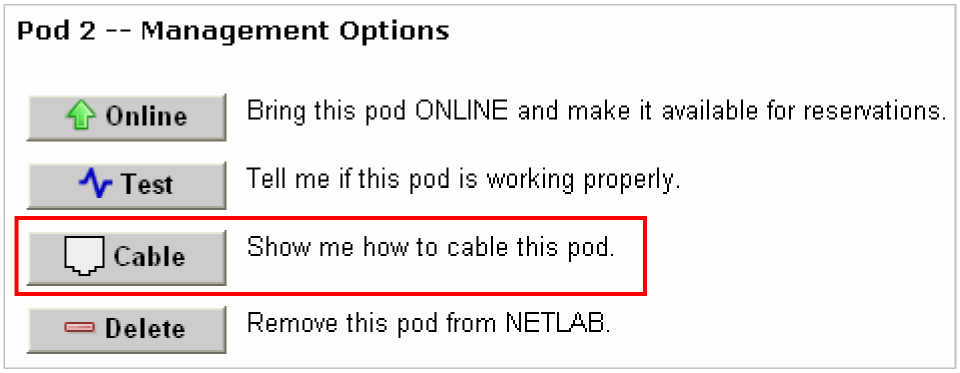
POD 2 - CONTROL SWITCH

SWITCH ID	POD PORT RANGE	BASE VLAN	VLAN POOL
2	1-14	110	110-116

6 Cable the Pod

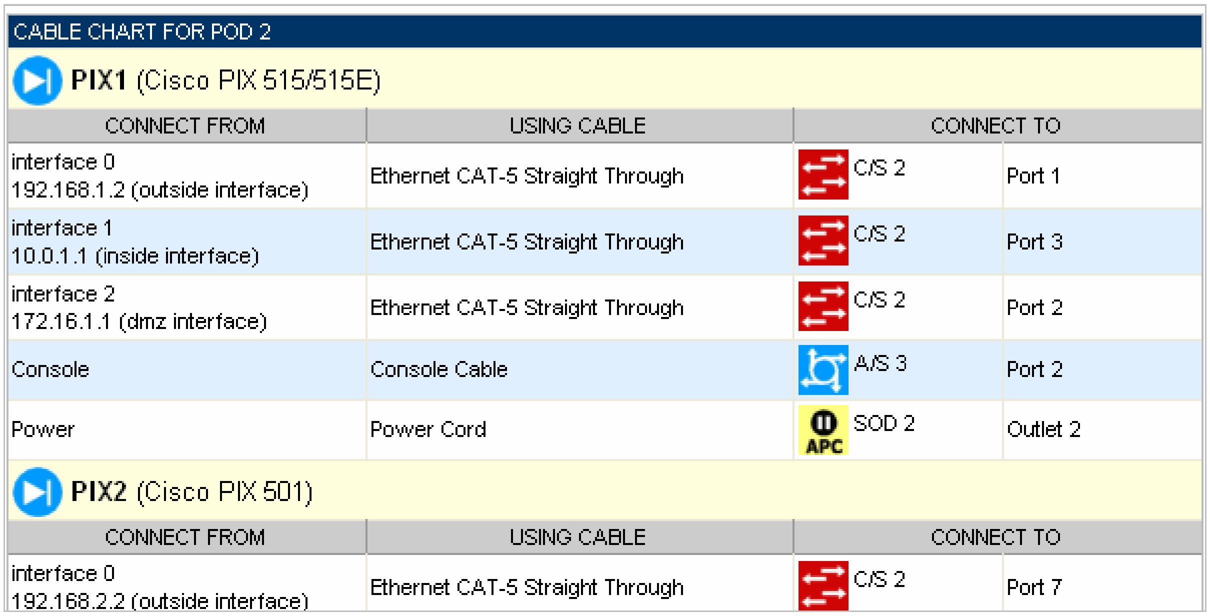
Use the NETLAB$_{AE}$ cable chart feature to help you connect the lab devices in your pod. The chart is generated in real-time and contains port-specific information based on your current lab device and control device settings.

The cable chart function is accessed from the pod management page.



Pod 2 -- Management Options

Online	Bring this pod ONLINE and make it available for reservations.
Test	Tell me if this pod is working properly.
Cable	Show me how to cable this pod.
Delete	Remove this pod from NETLAB.



CABLE CHART FOR POD 2

PIX1 (Cisco PIX 515/515E)

CONNECT FROM	USING CABLE	CONNECT TO	
interface 0 192.168.1.2 (outside interface)	Ethernet CAT-5 Straight Through	C/S 2	Port 1
interface 1 10.0.1.1 (inside interface)	Ethernet CAT-5 Straight Through	C/S 2	Port 3
interface 2 172.16.1.1 (dmz interface)	Ethernet CAT-5 Straight Through	C/S 2	Port 2
Console	Console Cable	A/S 3	Port 2
Power	Power Cord	APC SOD 2	Outlet 2

PIX2 (Cisco PIX 501)

CONNECT FROM	USING CABLE	CONNECT TO	
interface 0 192.168.2.2 (outside interface)	Ethernet CAT-5 Straight Through	C/S 2	Port 7

7 Configuring PCs

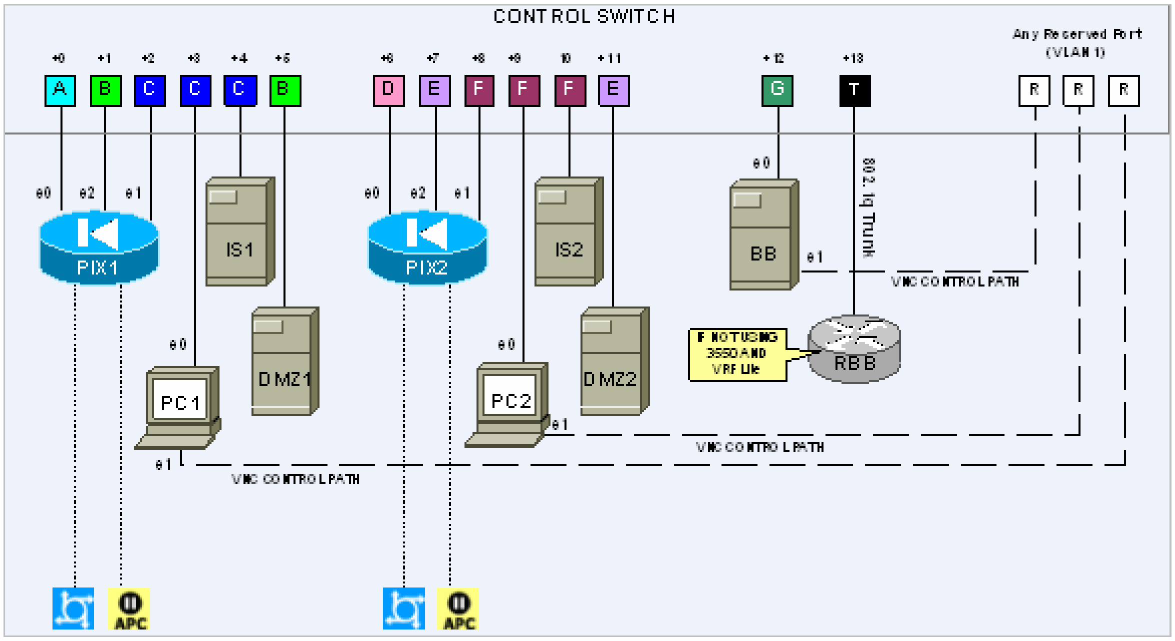
This section describes the basic tasks required to setup your PCs. Detailed guidance, such as securing the operating system and restoring the PC to a clean state is covered in the *NETLAB+ Remote PC Guide*.

Caution: Connect your PCs and servers to AC power via a surge protector, not a NETLAB$_{AE}$ switched outlet device (i.e. APC). Even though an unused outlet may currently be ON, NETLAB$_{AE}$ may turn the outlet OFF during certain tests.

7.1 Assign IP Addresses

Direct/Standalone remote PCs have two network interfaces and have two IP addresses. One interface faces the pod, and the other to any reserved control switch port. Reserved control switch ports reside in VLAN 1 and provide a path to the inside interface of the NETLAB$_{AE}$ server. The control path IP addresses will be based on the PC ID assigned in the new pod wizard (see below).

⇒ Do not set a default gateway on the control path interfaces.

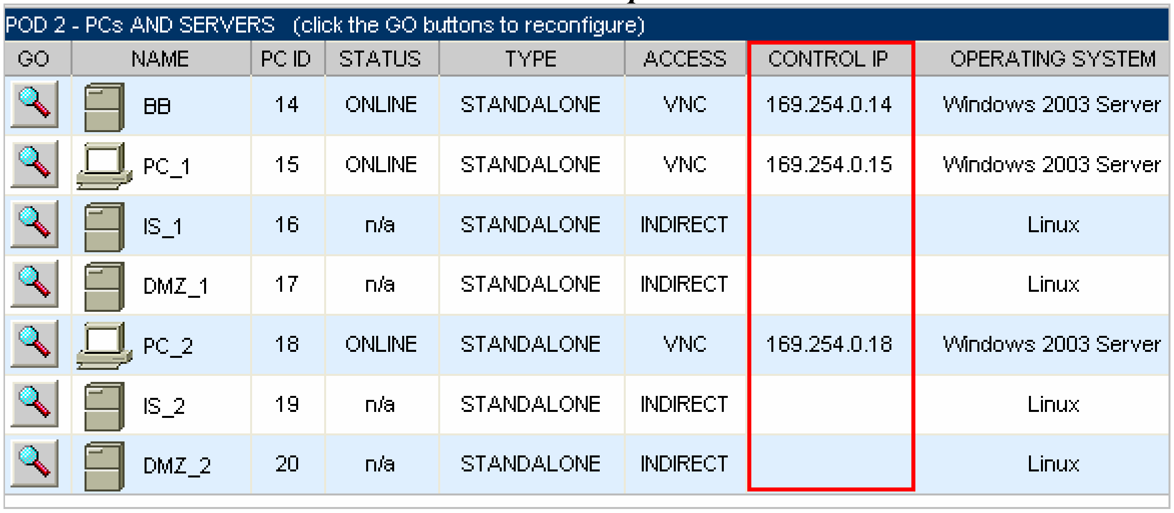


The following table shows the correct IP parameters for each PC and server.

	Primary Interface To Pod			Secondary Interface (Direct/Standalone PCs ONLY)		
	IP Address	**Mask**	**Gateway**	**IP Address**	**Mask**	**Gateway**
PC_1	10.0.1.12	/24	10.0.1.2	169.254.0.<pc_id>	/24	None
PC_2	10.0.2.12	/24	10.0.2.2	169.254.0.<pc_id>	/24	None
BB	172.26.26.50	/24	172.26.26.150	169.254.0.<pc_id>	/24	None
IS_1	10.0.1.10	/24	10.0.1.2	169.254.0.<pc_id>	/24	None
IS_2	10.0.2.10	/24	10.0.1.2	169.254.0.<pc_id>	/24	None
DMZ_1	172.16.1.2	/24	172.16.1.1	169.254.0.<pc_id>	/24	None
DMZ_2	172.16.2.2	/24	172.16.2.1	169.254.0.<pc_id>	/24	None

The secondary IP addresses for Direct/Standalone PCs are derived from the unique PC ID. The actual addresses are listed on the pod management page.

This is a sample…



POD 2 - PCs AND SERVERS (click the GO buttons to reconfigure)

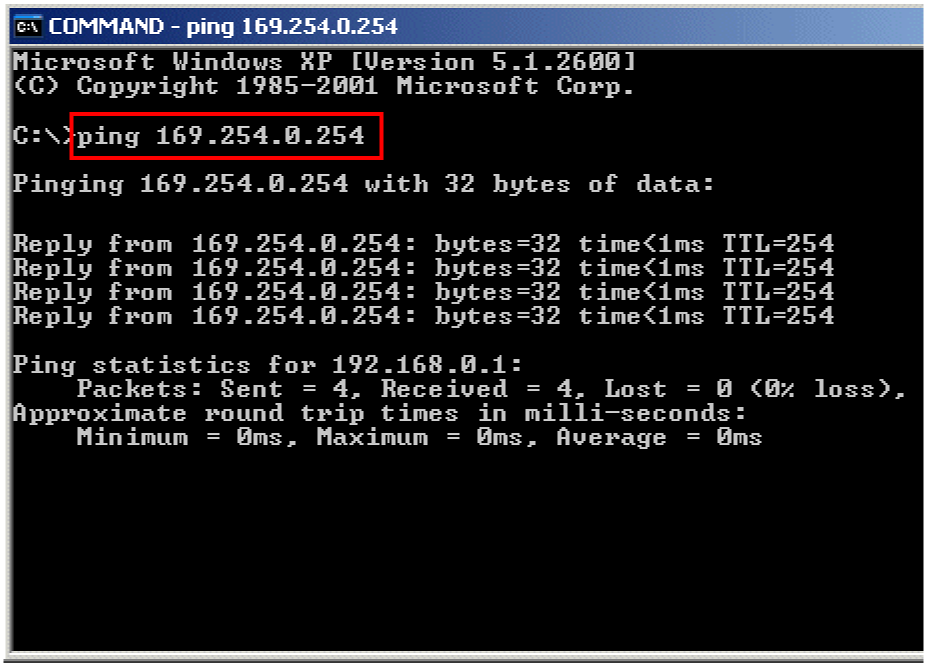
GO	NAME	PC ID	STATUS	TYPE	ACCESS	CONTROL IP	OPERATING SYSTEM
	BB	14	ONLINE	STANDALONE	VNC	169.254.0.14	Windows 2003 Server
	PC_1	15	ONLINE	STANDALONE	VNC	169.254.0.15	Windows 2003 Server
	IS_1	16	n/a	STANDALONE	INDIRECT		Linux
	DMZ_1	17	n/a	STANDALONE	INDIRECT		Linux
	PC_2	18	ONLINE	STANDALONE	VNC	169.254.0.18	Windows 2003 Server
	IS_2	19	n/a	STANDALONE	INDIRECT		Linux
	DMZ_2	20	n/a	STANDALONE	INDIRECT		Linux

7.2 Test the Control Path

For each **Direct/Standalone** remote PC, verify the control path between the PC secondary interface and the NETLAB$_{AE}$ server inside interface. All interfaces and switch ports in the control path should be administratively enabled and should have a green link light.

Open a command window and ping the NETLAB$_{AE}$ server inside address **169.254.0.254**.

⇒ NETLAB$_{AE}$ also binds 169.254.1.1 on its inside interface, but you will not be able to ping this address from a properly configured remote PC.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>ping 169.254.0.254

Pinging 169.254.0.254 with 32 bytes of data:

Reply from 169.254.0.254: bytes=32 time<1ms TTL=254
Reply from 169.254.0.254: bytes=32 time<1ms TTL=254
Reply from 169.254.0.254: bytes=32 time<1ms TTL=254
Reply from 169.254.0.254: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

7.3 Load Remote PC Software

You must load the NETLAB$_{AE}$ Remote PC software package on **Direct/Standalone** remote PCs. The installation package is stored on the NETLAB$_{AE}$ server and is downloaded using a web browser on the PC.

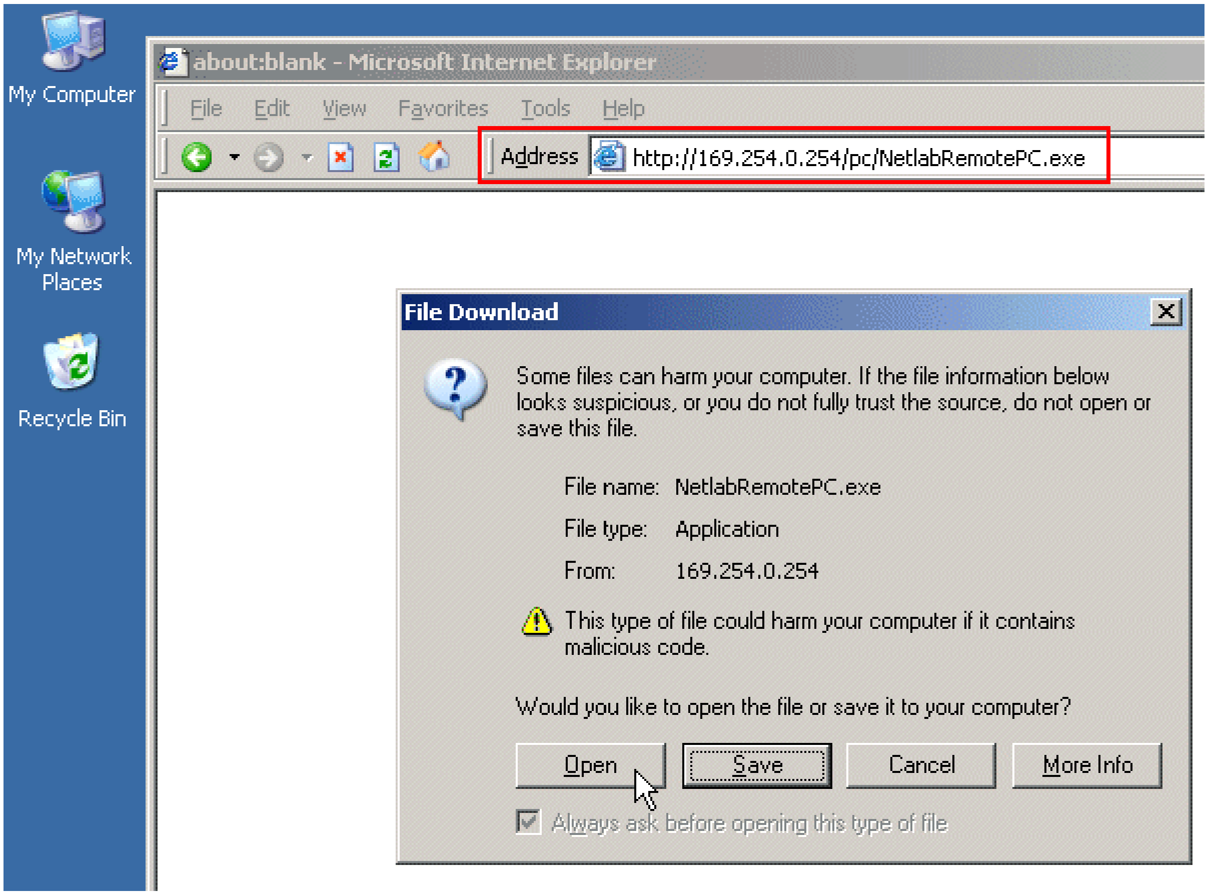
⇒ This software is only installed on direct access PCs (PC_1, PC_2 and BB). It should not be installed on IS_1, IS_2 or the users' PCs.

1) Open a web browser on the remote PC.

2) Enter the case-sensitive URL exactly as shown:

```
http://169.254.0.254/pc/NetlabRemotePC.exe
```

3) Click Open to install the package.


My Computer
My Network Places
Recycle Bin
about:blank - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address

http://169.254.0.254/pc/NetlabRemotePC.exe

File Download

Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: NetlabRemotePC.exe

File type: Application

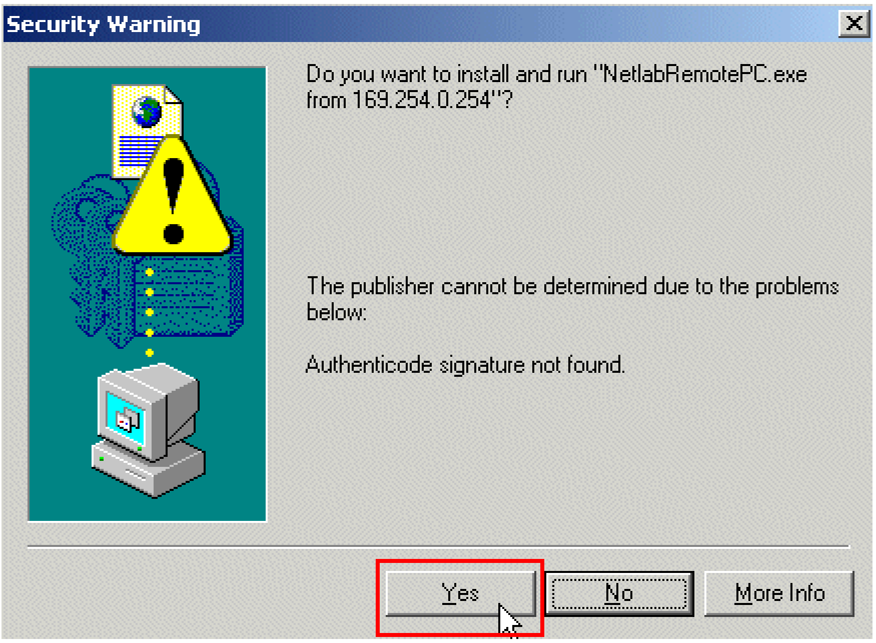
From: 169.254.0.254

This type of file could harm your computer if it contains malicious code.

Would you like to open the file or save it to your computer?

☑ Always ask before opening this type of file

4) Answer **Yes** at the Security Warning.


Security Warning

Do you want to install and run "NetlabRemotePC.exe from 169.254.0.254"?

The publisher cannot be determined due to the problems below:

Authenticode signature not found.

5) Agree to the license.
6) Read the README file.

7.4 Load Curriculum Specific Software

Install the software on the PC outlined in the FNSP curriculum and Student Orientation Lab.

7.5 Secure the PC

NETLAB$_{AE}$ does not prescribe any specific security policies for your PCs. However, you should implement a policy appropriate for your user community.

For Direct/Standalone PCs, we recommend that you:

1) Setup the guest account for casual user access. You should only allow very trusted users access to the administrator account (or equivalent), if you allow this at all. Appendix A highlights the few labs that may require admin privileges.

2) Use the policy editor to remove the system Shutdown option from the guest account. If a user shuts down a PC, that PC is unusable until someone physically powers it on.

3) Install and activate image restoration software such as *Horizon DataSys Drive Vaccine*. NETLAB$_{AE}$ will reboot the PC between lab reservations so that Drive Vaccine (or equivalent) can restore the PC to a clean state.

Please see the *NETLAB+ Remote PC Guide* for additional security tips.

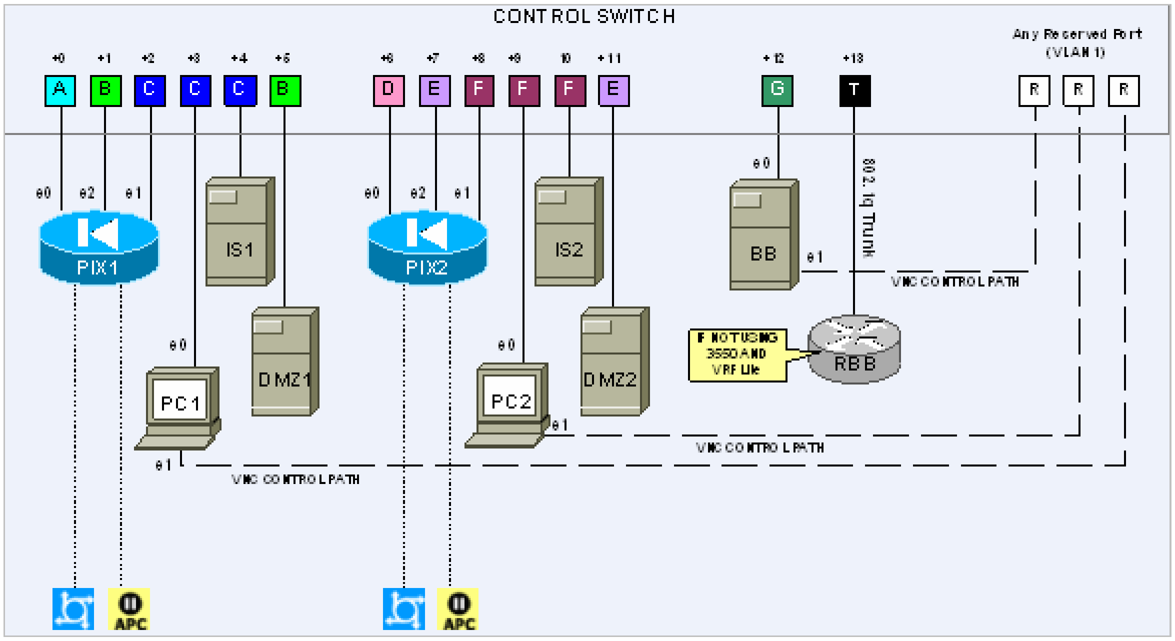
8 Configuring RBB

RBB is a statically configured router. It is not accessible or configurable by users. However, it is part of the topology so users can indirectly interact with it (i.e. ping, trace, RIP, etc.).

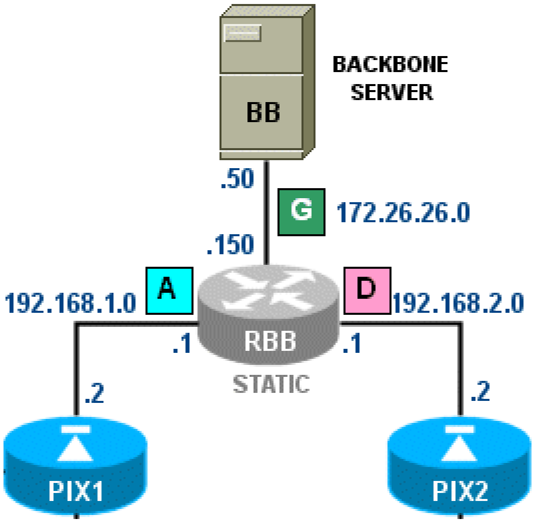
You can implement RBB in one of two ways:

- (1) Deploy a separate standalone RBB router for each Security PIX Pod.
- (2) Simulate RBB for two or more security pods by utilizing multi-VRF CE on one physical router

The following diagram shows how the networks in the Security PIX Pod are implemented as VLANs on the control switch. For illustration, each VLAN is given a letter and color. To avoid conflicts between pods, the actual pool of VLAN numbers selected for each pod is different.



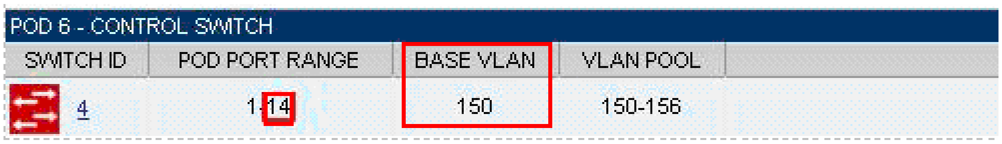
In the Security PIX Pod, RBB performs routing between network A, D, and G. .



8.1 Determine VLANs

Recall that each pod is automatically assigned a pool of unique VLAN numbers. Regardless of how you choose to implement RBB routing, you will need to determine what VLAN numbers are actually used for network A, D, and G.

First, determine the base VLAN for the pod you are setting up. This is shown on the pod management page. From the administrative account, go to Equipment Pods and select the pod from the list. Obtain the BASE VLAN from the CONTROL SWITCH table.



POD 6 - CONTROL SWITCH

SWITCH ID	POD PORT RANGE	BASE VLAN	VLAN POOL
4	1-14	150	150-156

In this example, pod 6 uses VLANs 150-156. The base VLAN is 150.

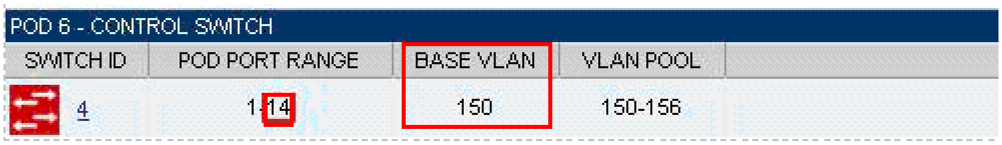
Now compute the actual VLANs by adding the base VLAN to the offset values listed below for each network. Record your results for future reference.

Network	Offset (add to base VLAN)	Actual VLAN	Example
A	**+ 0**	= ______	150 + 0 = 150
D	**+ 3**	= ______	150 + 3 = 153
G	**+ 6**	= ______	150 + 6 = 156

8.2 Option 1 – Separate RBB for Each Security PIX Pod

The most basic way to provide RBB routing is to stand up a separate RBB router for each Security Pod. RBB will need at least one 802.1q capable FastEthernet port.

Refer to the same CONTROL SWITCH table from section 8.1. Connect RBB to the last control switch port assigned to the Security PIX Pod (base port + 13)



POD 6 - CONTROL SWITCH			
SWITCH ID	POD PORT RANGE	BASE VLAN	VLAN POOL
4	1-14	150	150-156

Next, connect to the console of the control switch. Configure RBB's control switch port as a trunk. Limit allowed VLANs to those computed in the VLAN table (see 8.1).

Sample configuration for RBB control switch port – items in blue will vary.

```
interface FastEthernet0/10
 switchport mode trunk
 switchport trunk allowed vlan 150,153,156
 switchport nonegotiate
 no switchport access vlan
 no shutdown
```

Connect and configure RBB via the console port. Since RBB is static and not managed by NETLAB$_{AE}$, you may want to use a different enable password than the one used for hands-on lab routers. You may also wish to disable login on VTY lines.

Sample RBB configuration – items in blue will vary by pod and admin preference.

```
hostname RBB

! normal enable secret not recommended
enable secret different

key chain RTRAUTH
 key 1
  key-string 123456789

interface FastEthernet0/0.150
 description to PIX1 segment
 encapsulation dot1q 150
 ip address 172.30.1.1 255.255.255.0
 ip rip authentication mode md5
 ip rip authentication key-chain RTRAUTH
 no shutdown

interface FastEthernet0/0.153
 description to PIX segment
 encapsulation dot1q 153
 ip address 172.30.2.1 255.255.255.0
 ip rip authentication mode md5
 ip rip authentication key-chain RTRAUTH
 no shutdown
```

8.3 Option 2 – Using Multi-VRF CE on a Separate Physical Router to Simulate Several RBB Routers

You can leverage Cisco's Multi-VRF CE feature (also known as VRF Lite) to provide an RBB routing function for two or more NETLAB$_{AE}$ security pods (Router or PIX) using only one physical router. Multi-VRF stands for Multiple Virtual Routing and Forwarding. As the name implies, this feature allows you to have multiple routing tables in one router. Frame Relay or VLAN interfaces can be mapped to a specific routing table (VRF). In essence, you are simulating multiple virtual routers with one physical router.

The router and IOS must support both 802.1q trunking and Mutli-VRF CE. Cisco's Feature Navigator can help with this task. FNSP labs use EIGRP. EIGRP support for Multi-VRF CE is very recent and can be found in some IOS 12.3 releases.

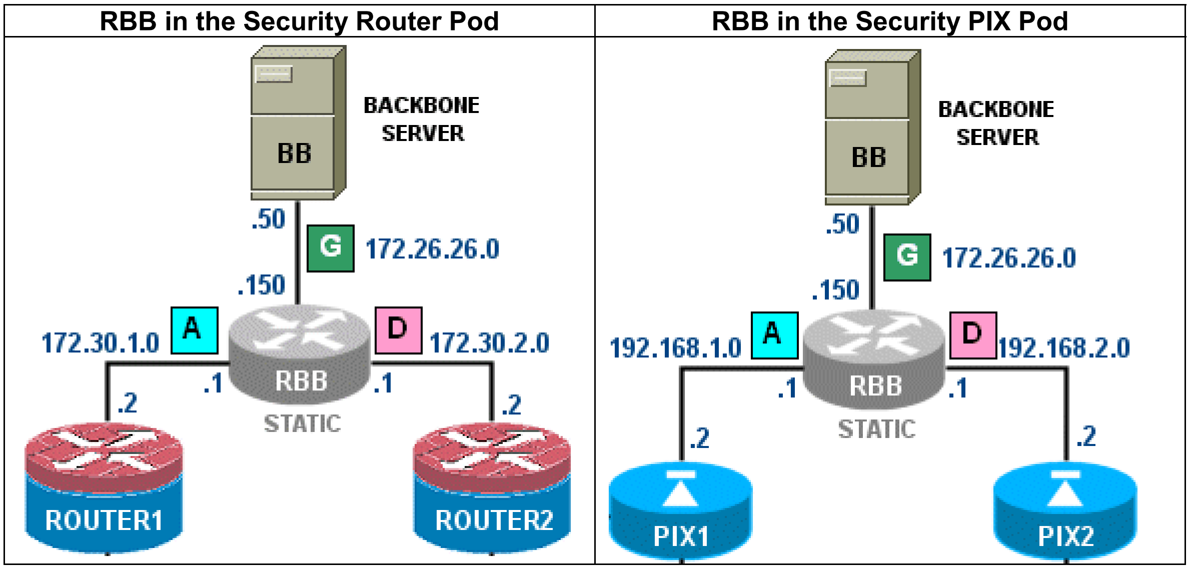
Building on option 1 (see 8.2), the physical router is connected to the "T" control switch port, designated for RBB on any one of the security pods The security pods do not need to be on the same control switch, as long as all control switches are interconnected on trunking ports and all VLANs are permitted between control switches.

⇒ NETLAB$_{AE}$ manages the VLAN database on each control switch using SNMP. During control switch configuration, NETLAB$_{AE}$ sets the control switch to VTP transparent mode. You should not change the control switches to VTP Server or VTP Client mode. In lieu of VTP, NETLAB$_{AE}$ will maintain an identical VLAN database on each control switch.

.

In the example to follow, we will use a Cisco 2621 running Multi-VRF CE to provide a virtual RBB for a Security Router Pod (POD_5) and a Security PIX Pod (POD_6). The physical router is a Cisco 2621 running 12.3(6c) Telco (c2600-telco-mz.123-6c.bin).

Both Security Router Pod and Security PIX Pod share a similar VLAN layout. This is by design. RBB provides routing between networks A, D, and G depicted below.

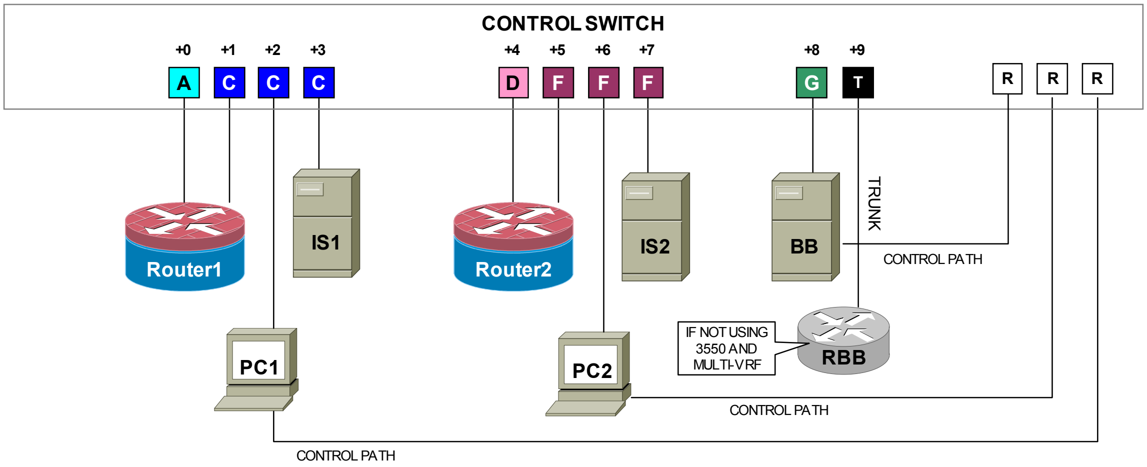


Similar to section 8.2, we determine that the BASE VLAN for POD_5 and POD_6 is 140 and 150 respectively. We compute the VLANs for network A, D, and G by adding the base VLAN for each pod to the offsets shown below.

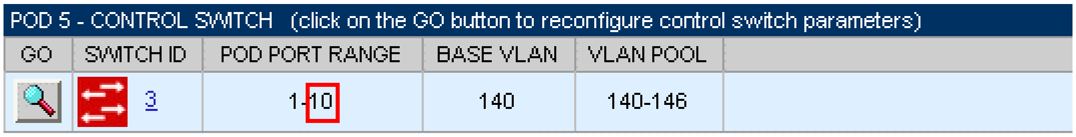
Figure 8.3.1 – RBB routed VLANS for POD_5 and POD_6

Network	Offset (add to base VLAN)	POD_5	POD_6
A	**+ 0**	140 + 0 = 140	150 + 0 = 150
D	**+ 3**	140 + 3 = 143	150 + 3 = 153
G	**+ 6**	140 + 6 = 146	150 + 6 = 156

You can connect the physical router to the designated “T” port on either security pod. In this case, we will use POD_5, a Security Router Pod.



POD_5 is using ports 1 to 10 on control switch 3. Therefore, the "T" port is FastEthernet0/10.



POD 5 - CONTROL SWITCH (click on the GO button to reconfigure control switch parameters)

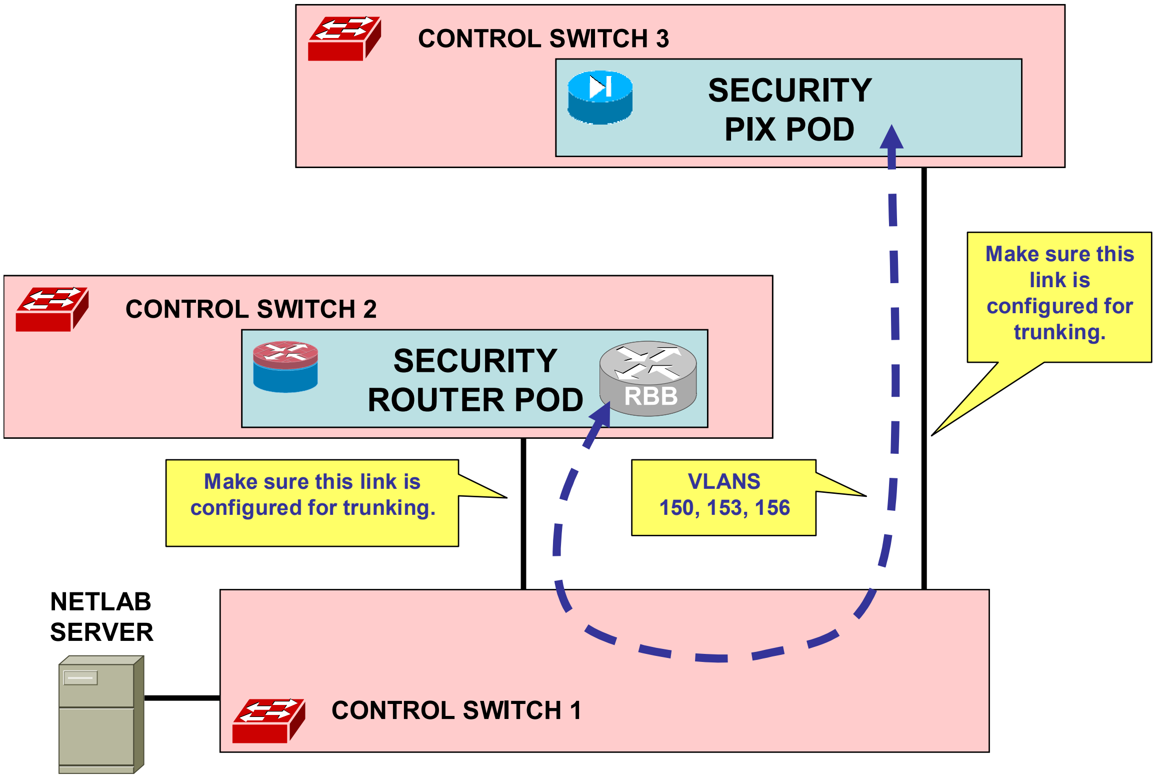
GO	SWITCH ID	POD PORT RANGE	BASE VLAN	VLAN POOL
🔍	3	1-10	140	140-146

We want to provide routing for all the VLANs computed in Figure 8.3.1 above. Therefore, we will configure FastEthernet0/10 for 802.1q and permit the VLANs for both pods.

Sample configuration for RBB control switch port – items in blue will vary.

```
interface FastEthernet0/10
 switchport mode trunk
 switchport trunk allowed vlan 140,143,146,150,153,156
 switchport nonegotiate
 no switchport access vlan
 no shutdown
```

Our two security pods will actually be connected to two different control switches. Recall that NETLAB$_{AE}$ maintains an identical VLAN database on each control switch (similar to VTP). As long as trunking is enabled between control switches, no additional switch setup is required.



Make sure this link is configured for trunking.

Make sure this link is configured for trunking.

VLANS 150, 153, 156

Next, we configure the physical RBB router. Begin by creating a virtual routing and forwarding instance for POD_5 and POD_6. Each VRF will represent a virtual RBB router. Each VRF requires a unique route descriptor in the form *rd:rd*. We will use the pod ID for the *rd* values.

```
hostname multi-RBB
!
ip vrf POD_5
 rd 5:5
!
ip vrf POD_6
 rd 6:6
```

Create a MD5 key chain for the RIPv2 lab. We will apply this to two networks in the Security Router Pod.

```
key chain RTRAUTH
 key 1
  key-string 123456789
```

Next, configure sub-interfaces for networks A, D, and G in POD_5. Apply the **ip vrf forwarding** command before assigning the IP address. This command assigns the VLAN sub-interface to a VRF. The two sub-interfaces facing network A and D will be configured for RIP MD5 authentication, in support of one of the lab exercises.

Now create sub-interfaces for POD_6.

```
interface FastEthernet0/0.150
 description POD_6 net A to PIX1
 encapsulation dot1Q 150
 ip vrf forwarding POD_6
 ip address 192.168.1.1 255.255.255.0
!
interface FastEthernet0/0.153
 description POD_5 net D to PIX2
 encapsulation dot1Q 153
 ip vrf forwarding POD_6
 ip address 192.168.2.1 255.255.255.0
!
interface FastEthernet0/0.156
 description POD_5 net G to BB
 encapsulation dot1Q 156
 ip vrf forwarding POD_6
 ip address 172.26.26.150 255.255.255.0
```

Next, we create an EIGRP and RIPv2 routing instance and assign them to the POD_5 VRF using the **address-family ipv4 vrf** command. EIGRP requires an **autonomous-system 1** command within the address family. POD_6 is the PIX pod and does not use EIGRP or RIP. If POD_6 was another Router pod, you would configure address families POD_6 for EIGRP and RIP similar to POD_5.

```
router eigrp 1
 auto-summary
 !
 address-family ipv4 vrf POD_5
 autonomous-system 1
 network 172.26.0.0
 network 172.30.0.0
 no auto-summary
!
router rip
 version 2
 !
 address-family ipv4 vrf POD_5
 network 172.26.0.0
 network 172.30.0.0
 no auto-summary
```

⇒ Because the PIX pod uses NAT on the outside interfaces, no routing protocols or static routes are required for the PIX pod's VRF.

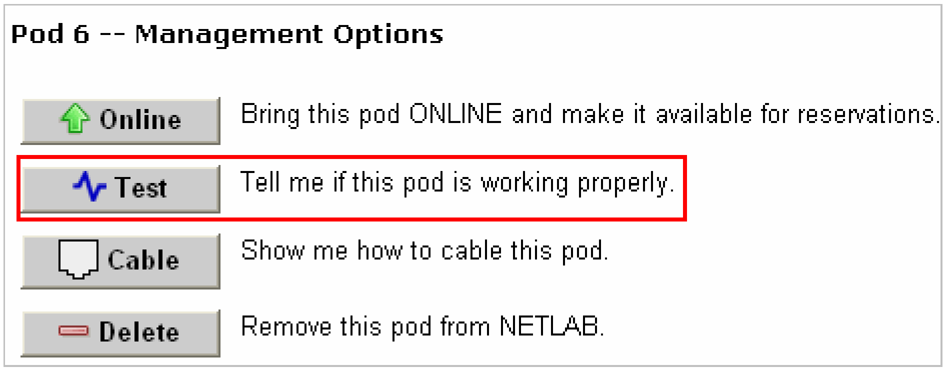
Exit configuration mode and **save** the configuration.

Once your pods are running and configs are loaded into ROUTER1 and ROUTER2, you can verify your VRF routing using the **show ip route vrf** command.

```
multi_RBB# show ip route vrf POD_5

Routing Table: POD_5

Gateway of last resort is not set

     172.26.0.0/24 is subnetted, 1 subnets
C       172.26.26.0 is directly connected, FastEthernet0/0.146
     172.30.0.0/24 is subnetted, 2 subnets
C       172.30.2.0 is directly connected, FastEthernet0/0.143
C       172.30.1.0 is directly connected, FastEthernet0/0.140
   10.0.0.0/24 is subnetted, 2 subnets
D       10.0.2.0 [90/30720] via 172.30.2.2, 00:00:27, FastEthernet0/0.143
D       10.0.1.0 [90/30720] via 172.30.1.2, 00:00:12, FastEthernet0/0.140
```

9 Testing the Pod

After all routers and PCs have been installed, you should run a pod test to verify that your pod is working. The pod test will detect common configuration and cabling problems.

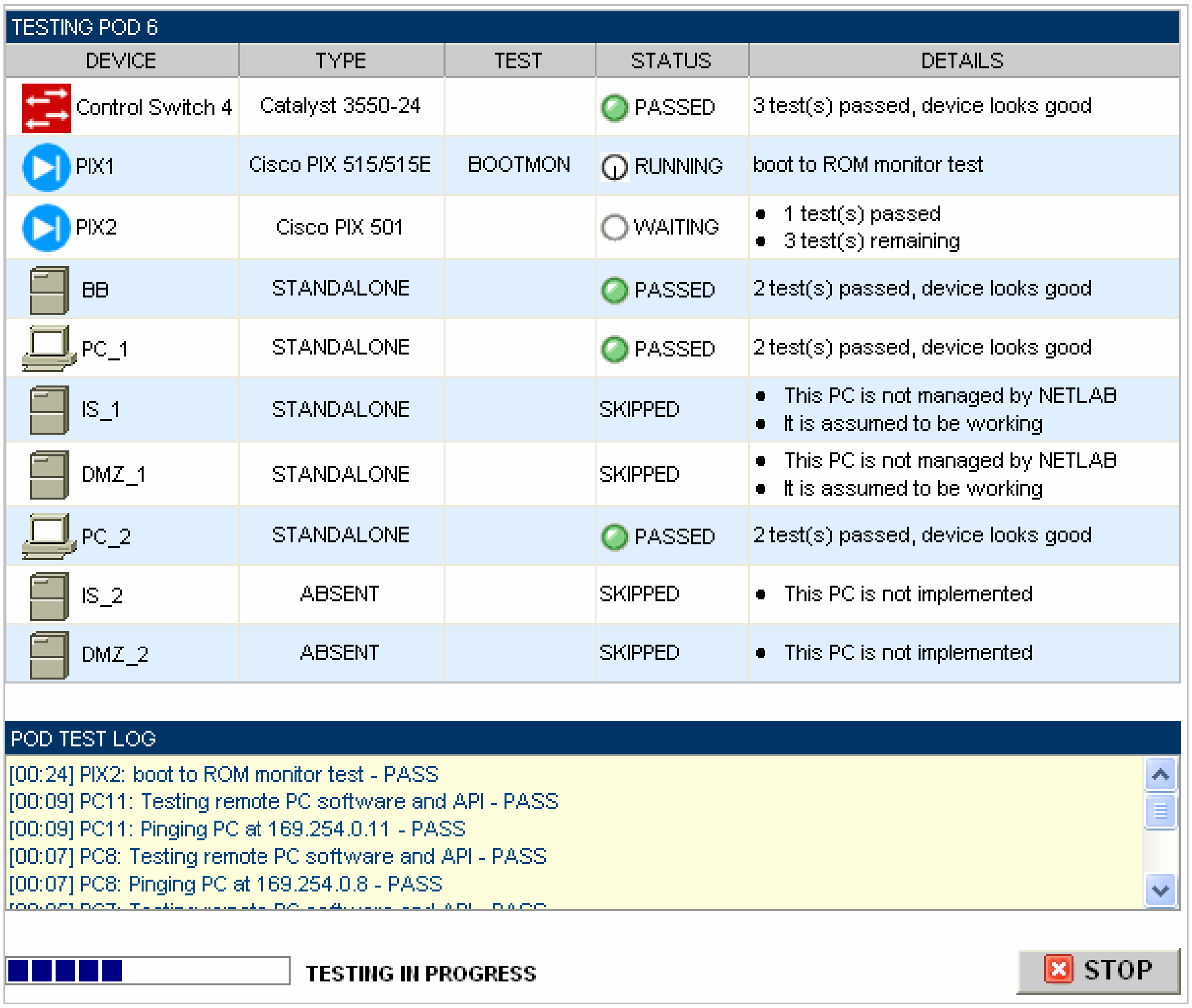


Pod 6 -- Management Options

Online	Bring this pod ONLINE and make it available for reservations.
Test	Tell me if this pod is working properly.
Cable	Show me how to cable this pod.
Delete	Remove this pod from NETLAB.

⇒ Some tests may take a long time. During the BOOTIOS test, NETLAB$_{AE}$ may have to load the specified IOS image if it is not in flash. Some images are very large and can take up to 30 minutes to program into flash memory.

If you cannot resolve an issue and decide to contact technical support, please cut and paste the text from the POD TEST LOG and include with your e-mail.



TESTING POD 6

DEVICE	TYPE	TEST	STATUS	DETAILS
Control Switch 4	Catalyst 3550-24		● PASSED	3 test(s) passed, device looks good
PIX1	Cisco PIX 515/515E	BOOTMON	◔ RUNNING	boot to ROM monitor test
PIX2	Cisco PIX 501		○ WAITING	• 1 test(s) passed • 3 test(s) remaining
BB	STANDALONE		● PASSED	2 test(s) passed, device looks good
PC_1	STANDALONE		● PASSED	2 test(s) passed, device looks good
IS_1	STANDALONE		SKIPPED	• This PC is not managed by NETLAB • It is assumed to be working
DMZ_1	STANDALONE		SKIPPED	• This PC is not managed by NETLAB • It is assumed to be working
PC_2	STANDALONE		● PASSED	2 test(s) passed, device looks good
IS_2	ABSENT		SKIPPED	• This PC is not implemented
DMZ_2	ABSENT		SKIPPED	• This PC is not implemented

POD TEST LOG

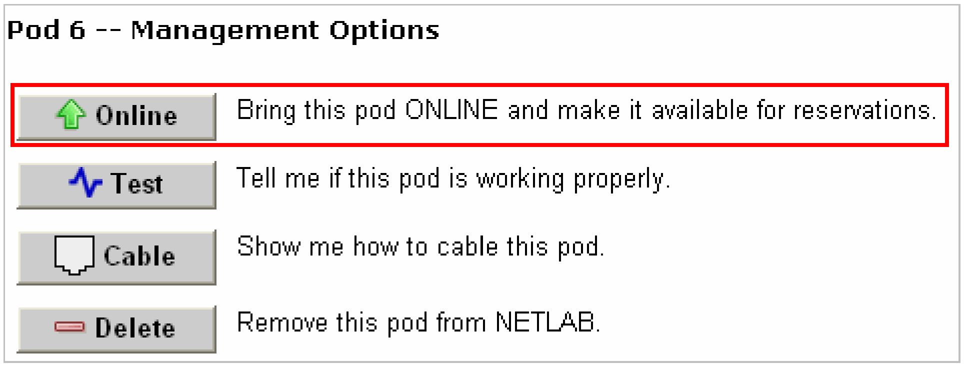
```
[00:24] PIX2: boot to ROM monitor test - PASS
[00:09] PC11: Testing remote PC software and API - PASS
[00:09] PC11: Pinging PC at 169.254.0.11 - PASS
[00:07] PC8: Testing remote PC software and API - PASS
[00:07] PC8: Pinging PC at 169.254.0.8 - PASS
[00:05] PC7: Testing remote PC software and API - PASS
```

TESTING IN PROGRESS

10 Finishing Up

10.1 Bring the Pod(s) Back Online

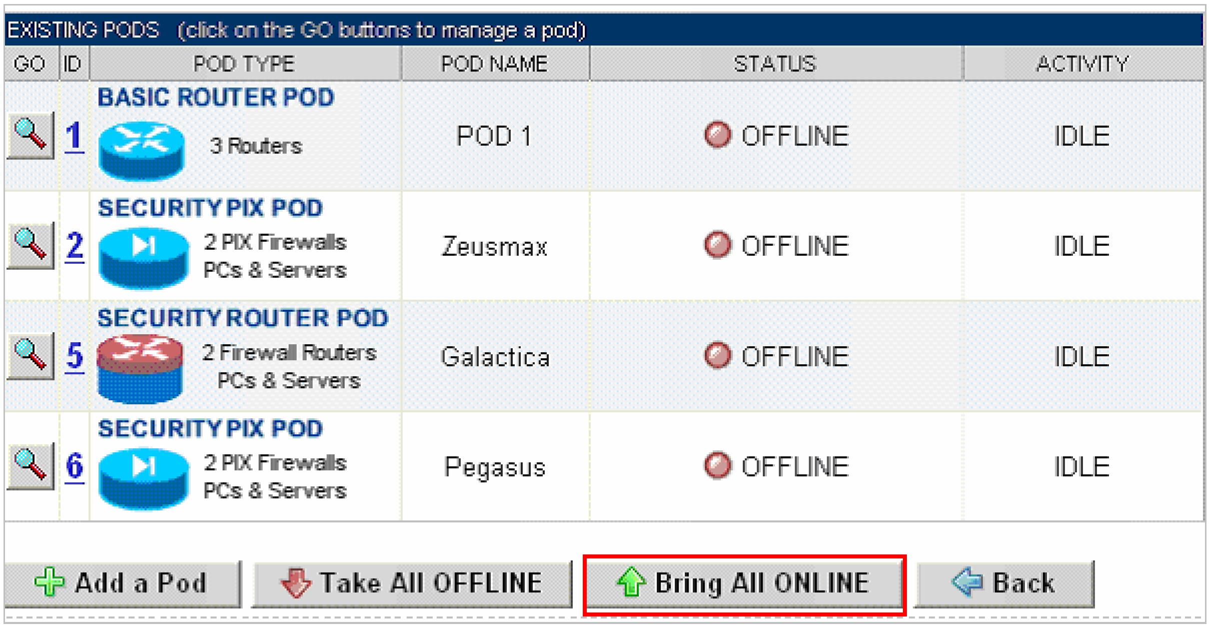
Now you can bring the pod online and make it available for lab reservations. You can bring just this pod online by clicking the Online button under Management Options.



Pod 6 -- Management Options

Online	Bring this pod ONLINE and make it available for reservations.
Test	Tell me if this pod is working properly.
Cable	Show me how to cable this pod.
Delete	Remove this pod from NETLAB.

Alternatively, you can click Bring All ONLINE on the Equipment Pods page. Choose this option when you have no more additions or modifications to pods or control devices and you wish to put all pods into service.



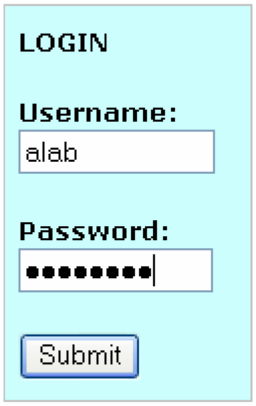
EXISTING PODS (click on the GO buttons to manage a pod)

GO	ID	POD TYPE	POD NAME	STATUS	ACTIVITY
	1	BASIC ROUTER POD 3 Routers	POD 1	OFFLINE	IDLE
	2	SECURITY PIX POD 2 PIX Firewalls PCs & Servers	Zeusmax	OFFLINE	IDLE
	5	SECURITY ROUTER POD 2 Firewall Routers PCs & Servers	Galactica	OFFLINE	IDLE
	6	SECURITY PIX POD 2 PIX Firewalls PCs & Servers	Pegasus	OFFLINE	IDLE

10.2 Enable Security PIX Pod and FNSP Exercises

To make the Security PIX Pod and FNSP lab exercises available to classes and students, you must first enable FNS/PIX in a new or existing class.

To add or edit class information, log into NETLAB$_{AE}$ using your instructor account. See the Instructor Accounts section of the *NETLAB+ Administrator Guide* for details.

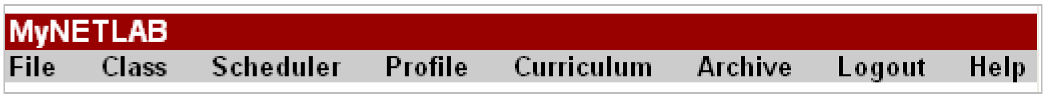


LOGIN

Username: alab

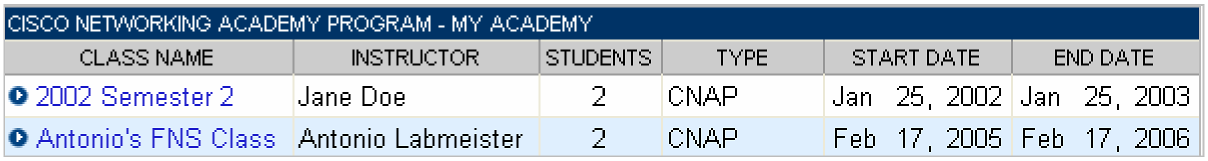
Password: ●●●●●●●●

Select **Class** from the menu bar at the top of the MyNETLAB page, or the link in the body of the page.



The Class Manager page will be displayed.

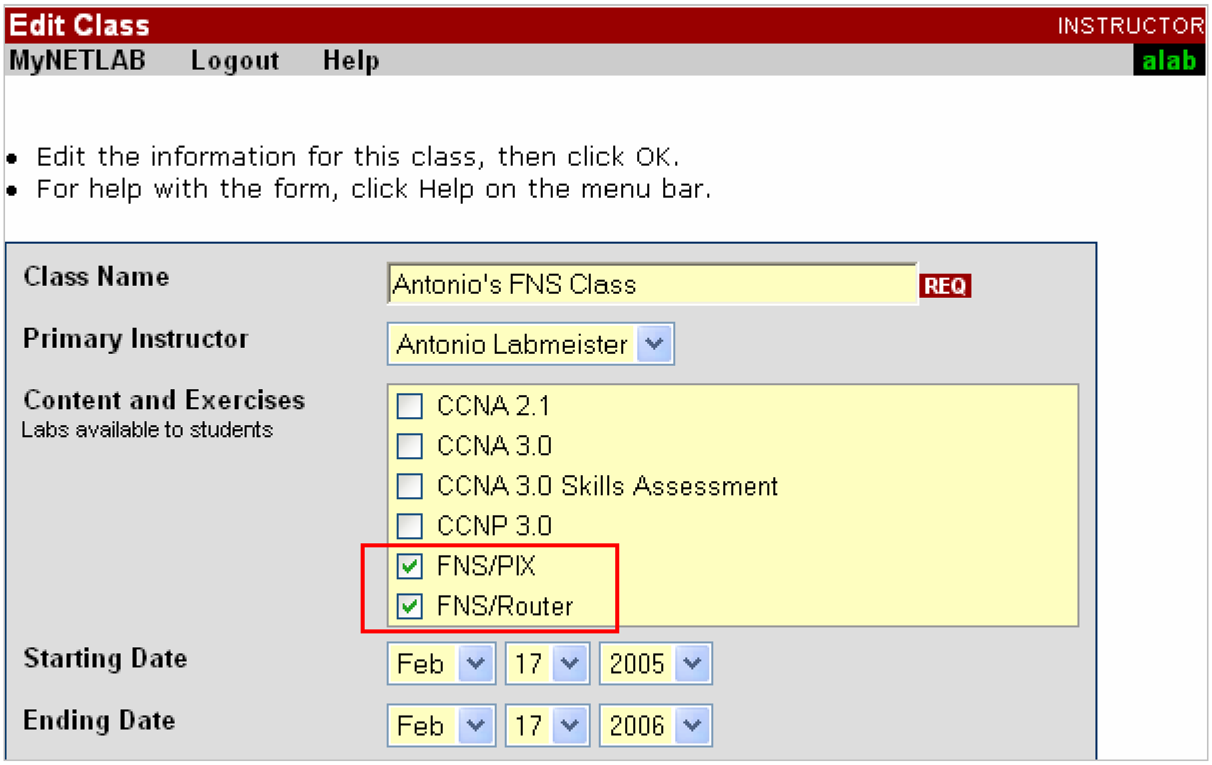
Select to add a new class or select an existing class from the class list by clicking on a class name.



CISCO NETWORKING ACADEMY PROGRAM - MY ACADEMY

CLASS NAME	INSTRUCTOR	STUDENTS	TYPE	START DATE	END DATE
2002 Semester 2	Jane Doe	2	CNAP	Jan 25, 2002	Jan 25, 2003
Antonio's FNS Class	Antonio Labmeister	2	CNAP	Feb 17, 2005	Feb 17, 2006

⇒ You may now enable more than one set of content. Previous NETLAB$_{AE}$ versions only allowed one content selection.

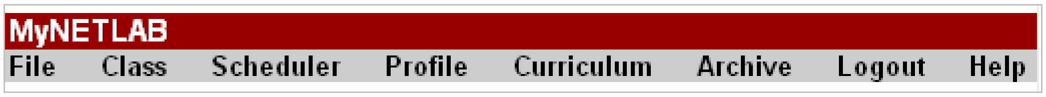


- Edit the information for this class, then click OK.
- For help with the form, click Help on the menu bar.

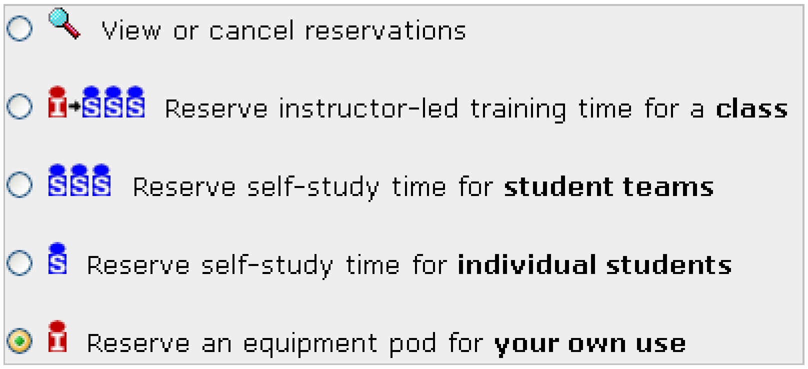
Class Name	Antonio's FNS Class
Primary Instructor	Antonio Labmeister
Content and Exercises Labs available to students	□ CCNA 2.1 □ CCNA 3.0 □ CCNA 3.0 Skills Assessment □ CCNP 3.0 ☑ FNS/PIX ☑ FNS/Router
Starting Date	Feb 17 2005
Ending Date	Feb 17 2006

10.3 Schedule a Lab Reservation for Your New Pod.

To schedule a lab reservation, select **Scheduler** from the menu bar or the link on the body of the MyNETLAB page.



The Scheduler Options screen will be displayed. Detailed descriptions of the scheduler options are available by selecting **Help** on the menu bar. In this example, we will reserve an equipment pod for your own use.



○ View or cancel reservations

○ Reserve instructor-led training time for a **class**

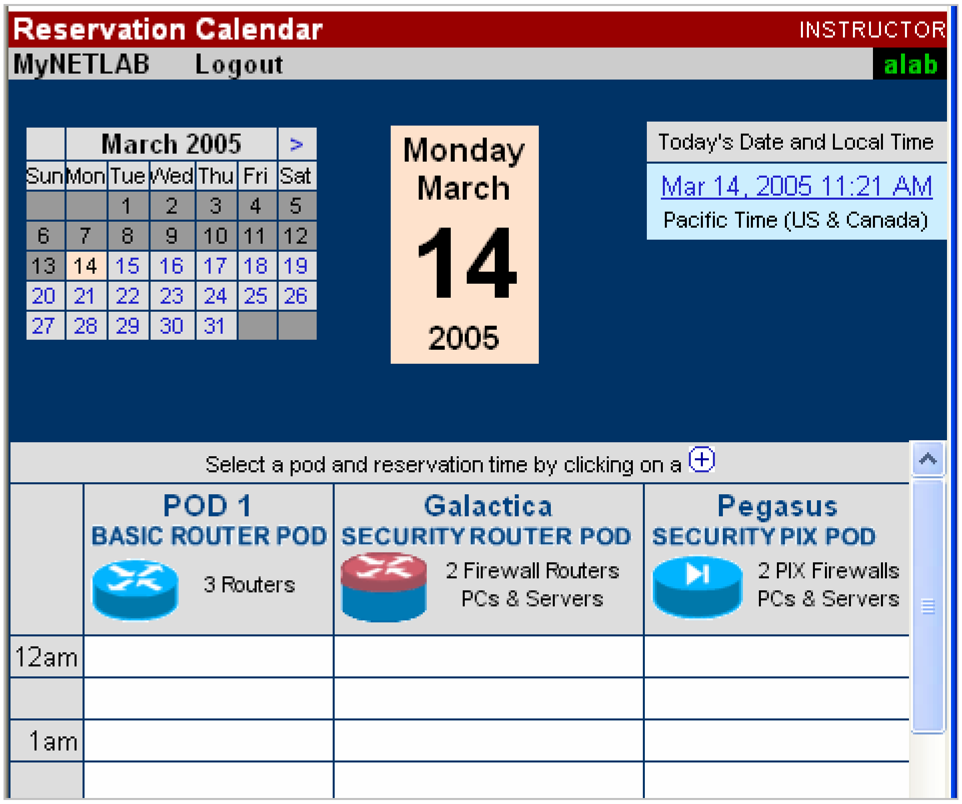
○ Reserve self-study time for **student teams**

○ Reserve self-study time for **individual students**

● Reserve an equipment pod for **your own use**

Select **OK** to proceed to the reservation calendar.

Please Note: The selection of pods depicted may be different from the pods available at your site.



Reservation Calendar INSTRUCTOR

MyNETLAB Logout alab

	March 2005					>
Sun	Mon	Tue	Wed	Thu	Fri	Sat
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

Monday March 14 2005

Today's Date and Local Time

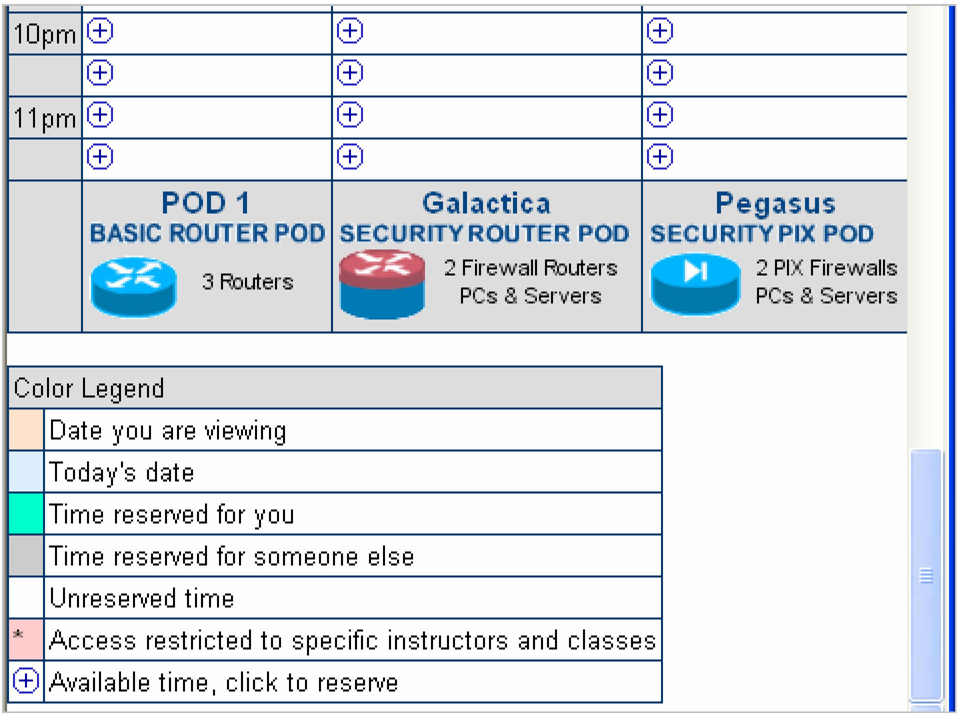
Mar 14, 2005 11:21 AM

Pacific Time (US & Canada)

Select a pod and reservation time by clicking on a ⊕

	POD 1 BASIC ROUTER POD 3 Routers	Galactica SECURITY ROUTER POD 2 Firewall Routers PCs & Servers	Pegasus SECURITY PIX POD 2 PIX Firewalls PCs & Servers
12am			
1am			

The reservation time area may be scrolled up and down. Scroll to the bottom to display the color legend.

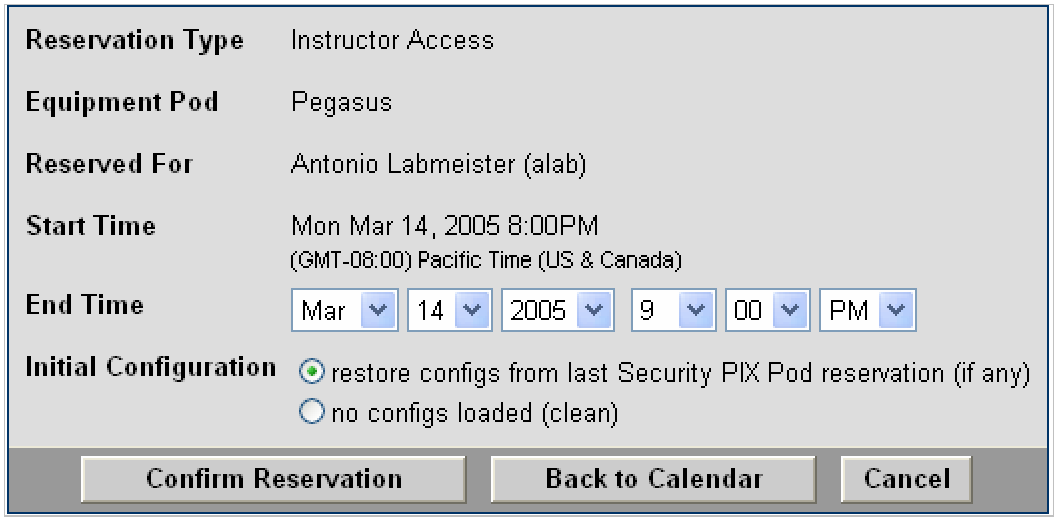


10pm	⊕	⊕	⊕
	⊕	⊕	⊕
11pm	⊕	⊕	⊕
	⊕	⊕	⊕
	POD 1 BASIC ROUTER POD 3 Routers	Galactica SECURITY ROUTER POD 2 Firewall Routers PCs & Servers	Pegasus SECURITY PIX POD 2 PIX Firewalls PCs & Servers

Color Legend	
🟧	Date you are viewing
🟦	Today's date
🟩	Time reserved for you
▨	Time reserved for someone else
□	Unreserved time
*	Access restricted to specific instructors and classes
⊕	Available time, click to reserve

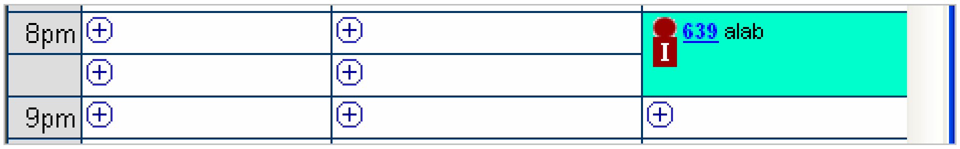
.

⊕ Select an available time, and the Reserve Instructor Access Time page will be displayed.



Reservation Type	Instructor Access
Equipment Pod	Pegasus
Reserved For	Antonio Labmeister (alab)
Start Time	Mon Mar 14, 2005 8:00PM (GMT-08:00) Pacific Time (US & Canada)
End Time	Mar 14 2005 9 00 PM
Initial Configuration	● restore configs from last Security PIX Pod reservation (if any) ○ no configs loaded (clean)

Review the details of the reservation and select **Confirm Reservation**. You can return to the reservation calendar to see your lab reservation on the time reservation portion. Remember, you may need to scroll the page to see your information.



8pm	⊕	⊕	I 639 alab
	⊕	⊕	
9pm	⊕	⊕	⊕

For more information on scheduling reservations, see the Scheduler section of the *NETLAB+ Instructor Guide*.

11 Appendix A - FNSP Supported Labs

LAB Name	NETLAB$_{AE}$ Support	Comments
Student Lab Orientation	Yes	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.
Vulnerabilities and Exploits	Caution*	The use of common network mapping tools, hacking programs, and scripts on a LAN and across a WAN. Requires administrator access on the PCs. Only recommended for Direct/VMware PCs..
Configuring the PIX Security Appliance using Setup Mode and PDM Startup Wizard	Yes	In this lab exercise, students will complete the following tasks: Verify the PIX and Student PC are properly cabled and installed, Erase the current configuration, Configure basic settings using the Interactive Setup mode, Configure basic settings using the PDM Startup Wizard.
Configuring the PIX Security Appliance with PDM	Yes	The Cisco PIX Device Manager (PDM) is a browser-based configuration tool that enables administrators to set up, configure, and monitor the PIX Security Appliance graphically, without requiring an extensive knowledge of the PIX Security Appliance command-l
Configure the PIX Security Appliance using CLI	Yes	In this lab exercise, students will complete the following tasks: Execute general maintenance commands, Configure the PIX Security Appliance inside and outside interfaces, Test and verify basic PIX Security Appliance operation
Configuring the PIX Security Appliance as a DHCP Server	Caution*	* This lab is not recommended for Direct/Standalone PCs. Requires administrator access on the PCs and changing of IP configuration on the correct interface. Modification of the wrong interface may break NETLAB$_{AE}$'s Remote PC control path and VNC access.
Configure Access Through the PIX Security Appliance using PDM	Yes	In this lab exercise, students will complete the following tasks: Use PDM to verify the starting configuration, Configure the PIX Security Appliance to allow inbound traffic to the bastion host using PDM, Configure the PIX Security Appliance to allow inbound traffic to the inside host using PDM, Test and verify correct PIX Security Appliance operation

		using PDM
Configure Access Through the PIX Security Appliance	Yes	In this lab exercise, students will complete the following tasks: • Configure a PIX Security Appliance to protect an enterprise network from Internet access. • Configure the PIX Security Appliance to allow inbound traffic to the inside host.
Configure Multiple Interfaces	Yes	In this lab, the student will complete the objective of configuring three PIX interfaces and configure access through the PIX Security Appliance.
Configure ACLs in the PIX Security Appliance	Yes	Configure ACLs in the PIX Security Appliance.
Configure Object Groups	Yes	PIX code version 6.2 introduced the feature called object grouping, which allows objects such as IP hosts or networks, protocols, ports, and Internet Control Message Protocol (ICMP) types to be grouped into objects.
Configure Object Groups and Nested Object Groups using CLI	Yes	In this lab, the student will complete the following objectives: Configure a service, ICMP-Type, and nested server object group, Configure an inbound access control list (ACL) with object groups, Configure web and ICMP access to the inside host, Test and verify the inbound ACL.
Configure Local AAA on the PIX Security Appliance	Yes	In this lab exercise, students will complete the following tasks: Configure a local user, Configure and test inbound and outbound authentication, Configure and test telnet and http console access, Configure and test Virtual Telnet authentication, Change and test authentication timeouts and prompts.
Configure AAA on the PIX Security Appliance Using Cisco Secure ACS for Windows 2000	Yes	In this lab exercise, students will complete the following tasks: • Install the Cisco Secure Access Control Server (ACS) for a Windows 2000 server. • Add a user to the Cisco Secure ACS database. • Identify the AAA server and protocol. • Configure and test.
Configure and Test Advanced Protocol Handling on the Cisco PIX Security Appliance	Yes	Some applications embed addressing information into the application data stream and negotiate randomly picked Transport Control Protocol (TCP) or User Datagram Protocol (UDP) port numbers or IP addresses. In these cases application aware inspection,

		fixup.
Configure Intrusion Detection		In this lab exercise, students will complete the following tasks: • Configure the use of Cisco Intrusion Detection System (IDS) information signatures and send Cisco IDS Syslog output to a Syslog server. • Configure the use of IDS attack signatures.
Configure LAN-Based Failover (OPTIONAL)	No	Requires additional PIX.
Configure User Authentication and Command Authorization using PDM	Yes	In this lab exercise, students will complete the following tasks: Configure command authorization, Configure Local User Authentication, Configure SSH
Configure SSH, Command Authorization, and Local User Authentication	Yes	In this lab exercise, students will complete the following tasks: • Configure SSH • Configure command authorization. • Configure Local User Authentication.
Configure a Site-to-Site IPSec VPN Tunnel Using PDM	Yes	In this lab exercise, students will complete the following tasks: Configure IKE and IPSec parameters using the PDM VPN Wizard, Test and verify IPSec configuration.
Configure a Site-to-Site IPSec VPN Tunnel Using CLI	Yes	In this lab exercise, students will complete the following tasks: Prepare to configure VPN support, Configure IKE and IPSec parameters, Test and verify IPSec configuration.
Configure a Secure VPN Using IPSec between a PIX and a VPN Client using PDM	Yes	In this lab exercise, students will complete the following tasks: Configure the PIX Easy VPN Server feature using the VPN Wizard, Install and configure the Cisco VPN Client on the Student PC, Verify and Test the Cisco VPN Client remote access connection
Configure a Secure VPN Using IPSec between a PIX and a VPN Client using CLI	Yes	In this lab exercise, students will complete the following tasks: Configure and Verify the PIX Easy VPN Server feature using CLI, Install and configure the Cisco VPN Client on a Microsoft Windows end-user PC, Verify and Test the Cisco VPN Client remote access connection

Configure IPSec between Two PIX Security Appliances with CA support	Yes*	In this lab exercise, the student will complete the following tasks: • Configure CA support on a PIX Security Appliance. • Configure IKE phase one and phase two using RSA signatures for authentication between two PIX Security Appliances. • Test and verify. *A supported CA server must be loaded on Backbone Server. Depending on the CA product used, you might have to run Windows 2000 or Windows 2003 server to support this exercise.
Configure SNMP using PDM	Yes	In this lab exercise, students will complete the following tasks: Enable SNMP community string, Establishing the Contact and location of the SNMP Agent, Limit SNMP to inside server, Testing the configuration.
Perform Password Recovery	Yes	In this lab exercise, students will complete the following tasks: • Upgrade the PIX image. • Perform password recovery procedures.