NDG
NETLAB Academy Edition®

Network Security Pod – Version 2.0

Planning and Installation Guide

For Cisco Networking Academy® Network Security 2.0 Curriculum

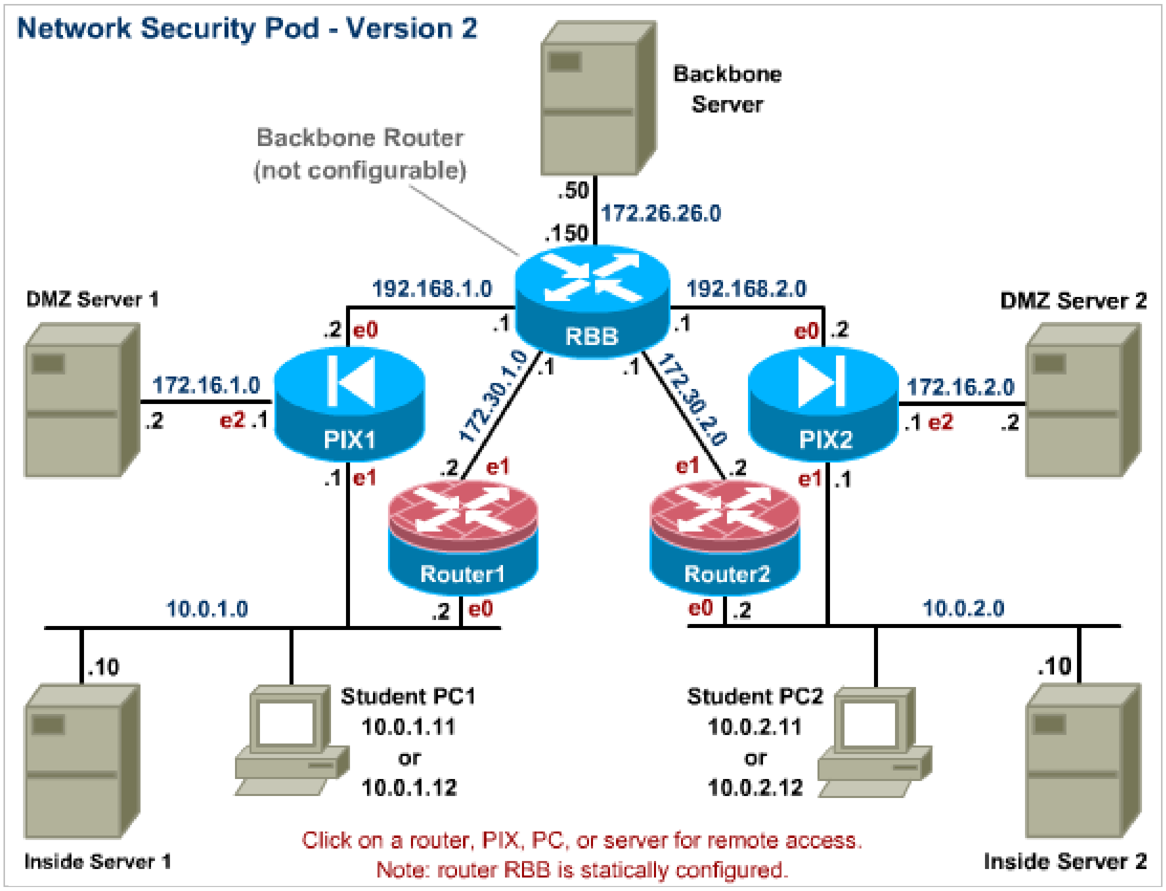
Document Version: 2008-03-10

PART 1 – PLANNING

1 Introduction

The NETLAB$_{AE}$ -Network Security Pod (version 2.0) corresponds to the Academy Network Security 2.0 curriculum.

This document assumes that you have reviewed Academy Network Security 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.



Click on a router, PIX, PC, or server for remote access.
Note: router RBB is statically configured.

You may have up to four (4) Network Security pods per NETLAB$_{AE}$ system.

The Network Security pod features direct access to router and PIX consoles.
This pod also supports integration with a separate VMware server to provide PC and server support. NETLAB$_{AE}$ can provide remote access to the keyboard, video, and mouse of VMware virtual machines in the pod.

NETLAB$_{AE}$ users in a team or instructor-led class can share access to a device console or PC.

The security labs are designed around a two-team model. One team of students configures the left (or P) side, while another team configures the right (or Q) side.

⇒ 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$_{AE}$ provides this flexibility, certain choices may be required by the curriculum and by NETLAB$_{AE}$.

1.1 Deviations

Remote users may get confused by local deviations from the standard curriculum and labs. The 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.

1.2 Remote PC Support

The Network Security Pod supports 7 remote PCs. NETLAB$_{AE}$ supports three alternative settings for each:

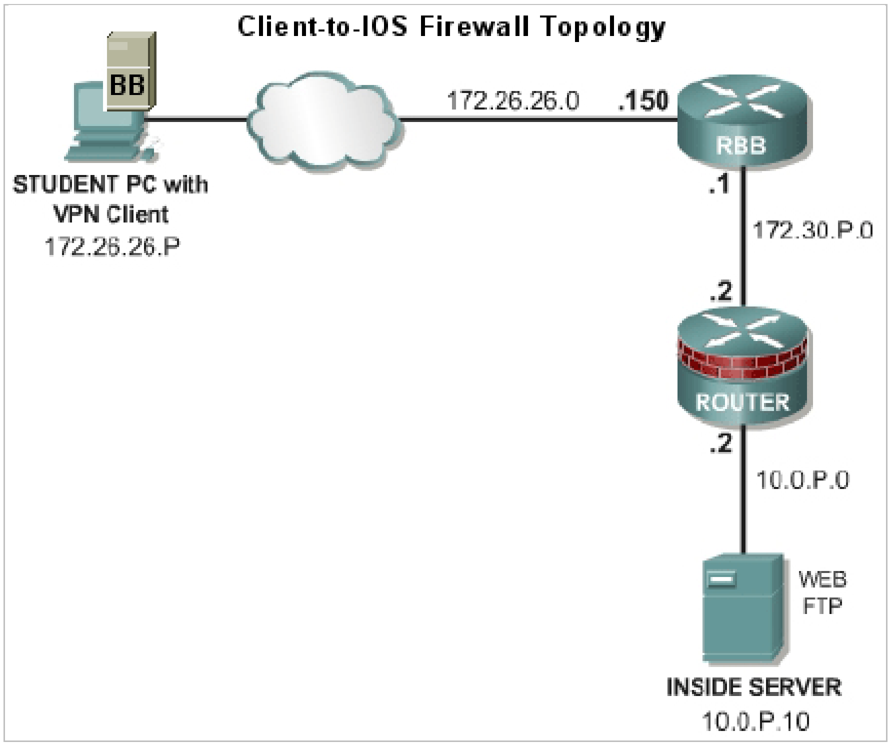
- **Direct/VMware**. The PC is implemented as a VMware virtual machine.
  - Users can control the keyboard, video, and mouse.
  - Users can power on, shutdown, reboot, and revert to a clean state.
  - Users can have administrator rights.
- **Indirect**. The PC is implemented, but not managed by NETLAB$_{AE}$.
  - 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 fully explained in the *NETLAB+ Remote PC Guide for VMware Server Implementation*. Direct/VMware offers complete administrative access on the remote PC and offers the greatest support for labs. To learn more about VMware virtualization products, please visit the company's web site at http://www.vmware.com.

Please Note: Direct/Standalone (as described in the *NETLAB+ Remote PC Guide for Standalone Implementation*) is not supported on this pod.

1.3 Client-to-IOS-Firewall Topology

The 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

Lab devices are part of the topology and users can interact with them either directly or indirectly.

The equipment listed in subsequent sections is derived from the official Academy spreadsheet **`NSv2.0_Configuration_and_Pricing_Guide_03OCT05.xls`.**

Other equipment may work if it is supported by NETLAB$_{AE}$ and can meet the minimum requirements for feature sets, interfaces, IOS, RAM, and Flash. A list of NETLAB$_{AE}$ supported lab equipment can be found on the NDG website. Please note, compatibility with NETLAB$_{AE}$ does not guarantee compatibility with the Academy labs.

2.1 ROUTER1 and ROUTER2

Recommended Devices	Ethernet Ports Required	IOS Releases
Cisco 831 (Economy)	2	S831CHK9-12402T Cisco 831 Series IOS IP/FW 3DES
Cisco 1841 (Standard)	2	IP Advanced Security Minimum of 12.3.(8)T IOS IP/FW/IDS Plus IPSec56 or 3DES image
Cisco 2811 (Premium)	2	IP Advanced Security Minimum of 12.3.(8)T IOS IP/FW/IDS Plus IPSec56 or 3DES image

2.2 PIX1 and PIX2

Devices	Ethernet Ports Required	IOS Features
ASA 5510* ***RECOMMENDED***	3	IOS 7.0(6) or higher.
PIX 515E	3	PIX-515E-DMZ Bundle (Chassis, Restricted SW, 64MB SDRAM, 3 FE ports. Includes PIX-1FE PIX 10/100 Fast Ethernet card) Select SF-PIX-515-7.0 [PIX OS 7.0- or later] for the PIX 515E Chassis for Software Option. Select PIX-515-VPN-3DES for PIX-VPN Options (or select PIX-VPN-DES in encryption restricted countries)
PIX 501 PIX 506E	2 **	** **501s and 506s do not have a DMZ interface and cannot be upgraded to OS v 7.0 or later.** These models are options in NETLAB, but they are limited in functionality. At least one PIX in the pod should be a PIX 515E.

*Even though the ASA 5510 is not included in the recommended academy equipment list for the Network Security courses, this is the best option because PIX5xx are mostly EOS (End Of Sale).

2.3 Router Backbone (RBB)

RBB is a backbone router with a static configuration. At least one Fast Ethernet port supporting 802.1q is required.

NETLAB$_{AE}$ Recommended Devices	Ethernet Ports Required	IOS Features
Cisco 1841	1	12.2, IP, 802.1q, RIP
Cisco 2801		
Cisco 2620/21		

NETLAB$_{AE}$ does not allocate an access server connection for RBB, so users cannot directly access the console port. However, it is part of the topology so users can indirectly interact with it (i.e. ping, trace, RIP, etc.).

⇒ You may allow student Telnet access to RBB from BB, PC1, or PC2. Since RBB is part of the pod infrastructure, we do not recommend privileged (enable) access.

2.4 PCs and Servers

The Network Security pod supports 7 VMware virtual machines. VMware virtualization is installed on a separate server. The *NETLAB+ Remote PC Guide for VMware Implementation* contains general information for setting up a VMware server.

Please Note: The Academy labs refer to a “SuperServer” option. This is not supported by VMware or NETLAB$_{AE}$. Multiple servers in the pod are implemented as virtual machines on the VMware server.

The following operating system choices are typical based on the curriculum. These choices are not mandatory; you can make substitutions provided:

(1) VMware virtualization products support the operating system (as a “guest”).
(2) Your choices are compatible with the curriculum.

Virtual Machine	O/S	Functions
PC1 PC2	Windows XP	Student PC, client activities, VPN
IS1 IS2	Windows 2000 or 2003 Server	CSACS, Web, FTP, DHCP
DMZ1 DMZ2	Linux or Windows	Web, FTP
BB	Windows 2000 or 2003 Server	Backbone Server

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 lab users.

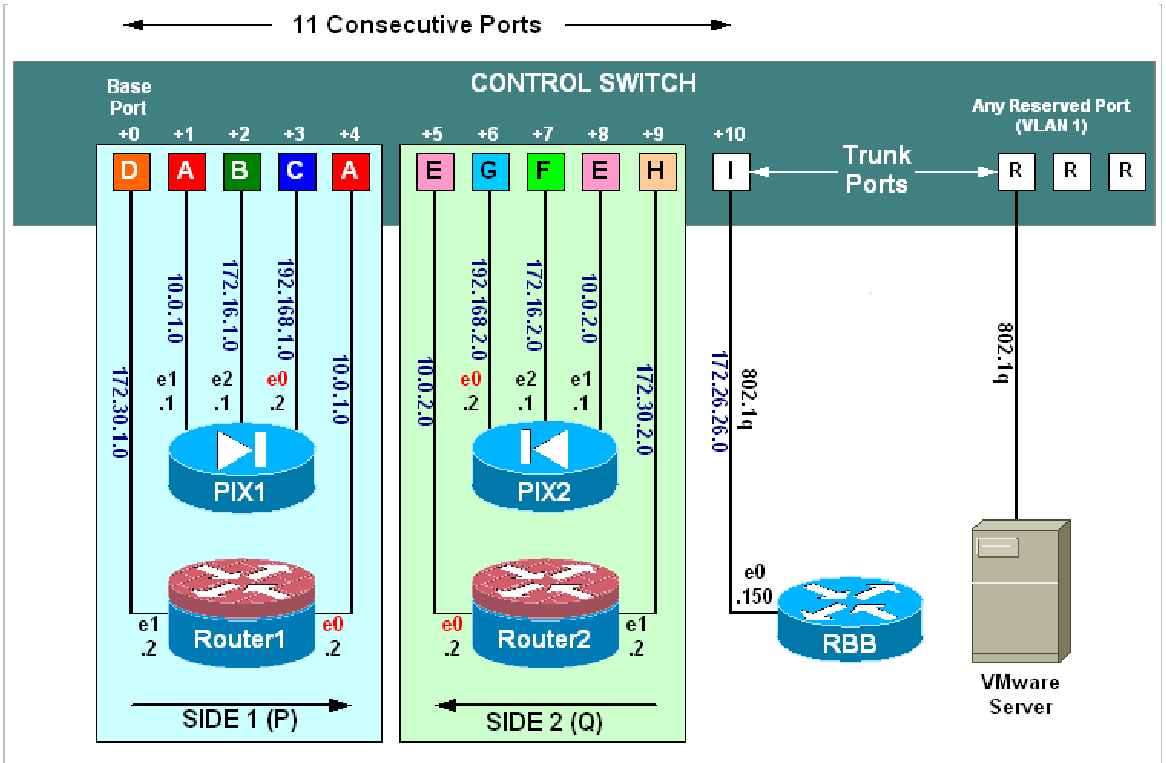
⇒ The *NETLAB+ Administrator Guide* explains how to add, change, or delete control devices.

The Network Security Pod requires the following control device resources:

Control Device Resource	Quantity Required
Control Switch	**11** consecutive ports **1** reserved port (VMware server)
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 Network Security Pod and VMware server(s). This pod requires **11** consecutive ports on a supported control switch (other than a Catalyst 1900 series).



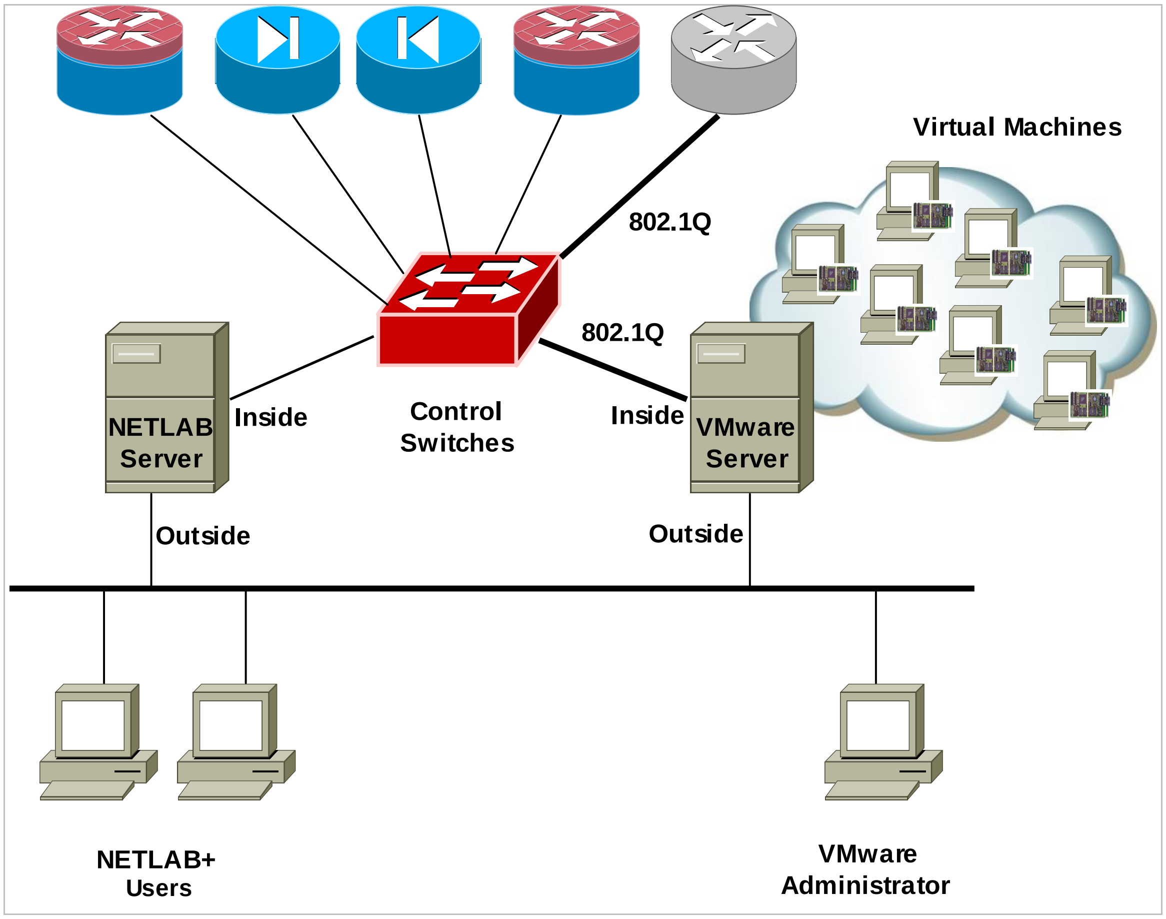
Caution: observe port symmetry between side 1 and side 2 !

⇒ The Academy labs refer to backbone switch “SW0”. This device is not implemented in NETLAB$_{AE}$. Rather, the functionality is implemented on a control switch. In addition, the NETLAB$_{AE}$ cable scheme (depicted above) is different from the SW0 cable scheme.

Ports are labeled **+0** to **+10** in the diagram and are relative to the *base port*. These ports must be consecutive on the same control switch. As with all pods, you choose a base port for the pod during pod installation (section 5). A control switch can support multiple pods. To determine the actual port numbers used for this pod, add the base port number to the relative port numbers shown in the diagram. For example, if the base port is 5, the actual port numbers will be 5 to 15.

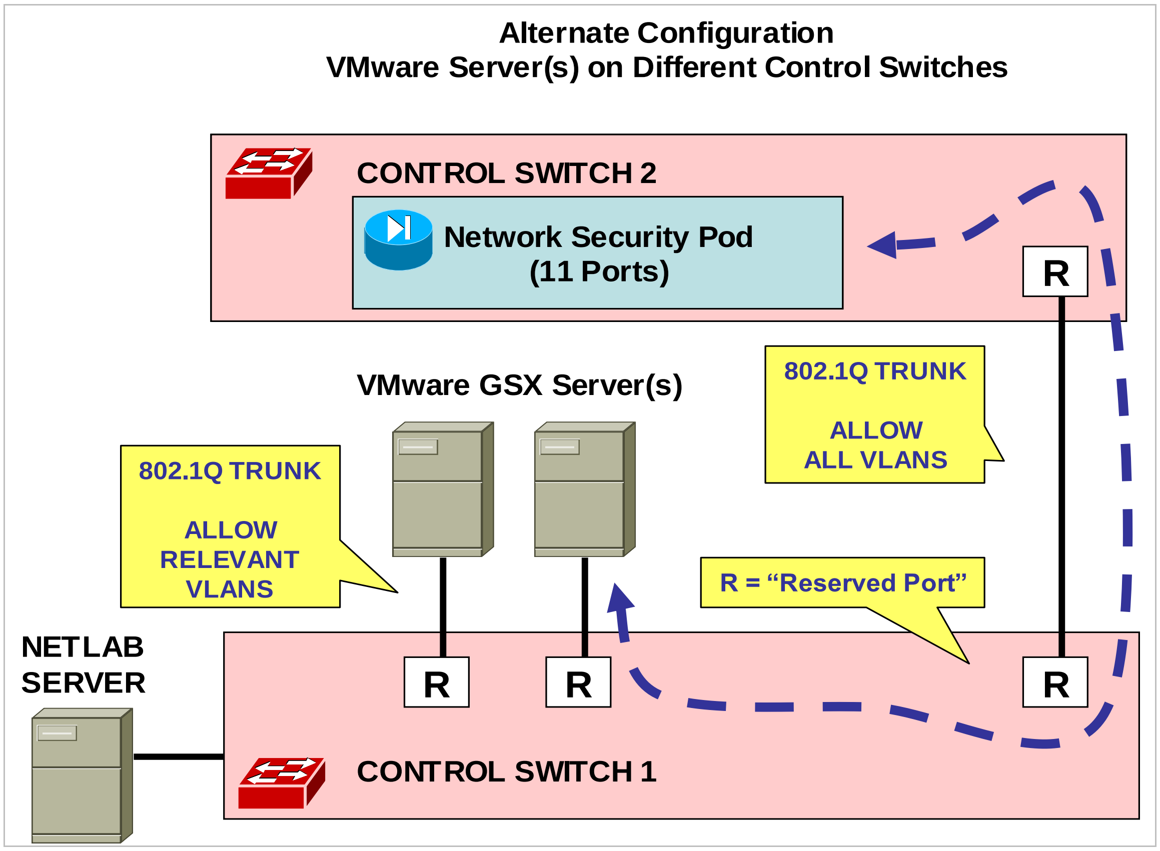
Using SNMP, NETLAB$_{AE}$ will automatically setup VLANs and configure ports on the control switch. These VLANs are depicted as letters “A” through “I” and represent one subnet in the topology. Each NETLAB$_{AE}$ pod has a unique *VLAN pool* and the actual VLAN numbers will be unique for each NETLAB$_{AE}$ pod. This is to avoid conflict between pods.

One “reserved” port on the control switch connects to an 802.1q NIC card on the VMware server. This allows devices in the pod to communicate with virtual machines.



The reserved port may be located on a different control switch, provided that all links between control switches are also configured as 802.1q trunks and all VLANs are allowed. You may also have more than one VMware server and virtual machines in the pod can be located on different VMware servers.

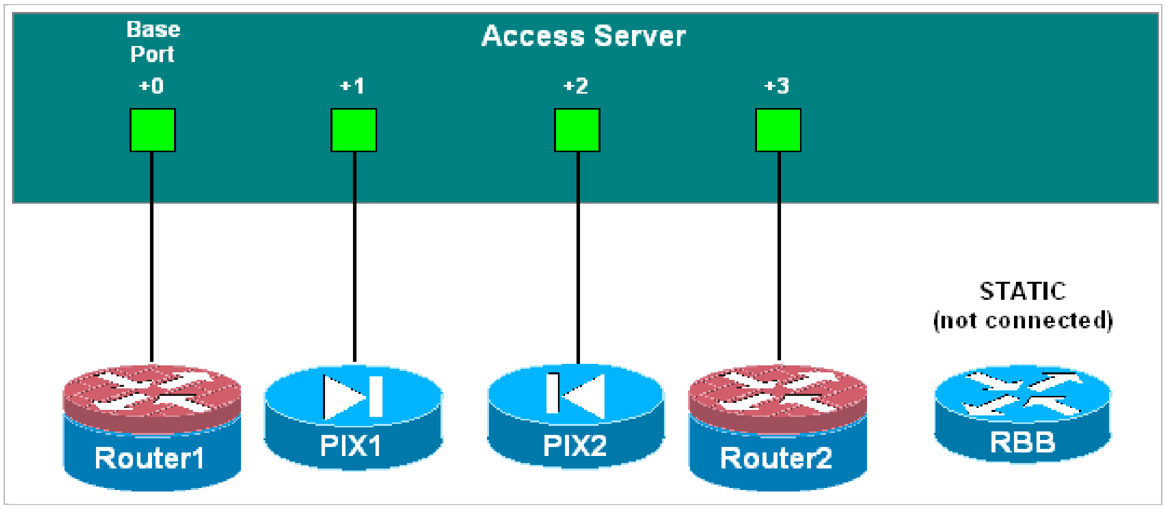
For more details, please see section 7.



3.2 Access Server

Access servers provide console connections to lab routers and PIX devices so that users can access these devices from NETLAB$_{AE}$. Users do not communicate directly with the access server. Rather, all connections are proxied through NETLAB$_{AE}$.

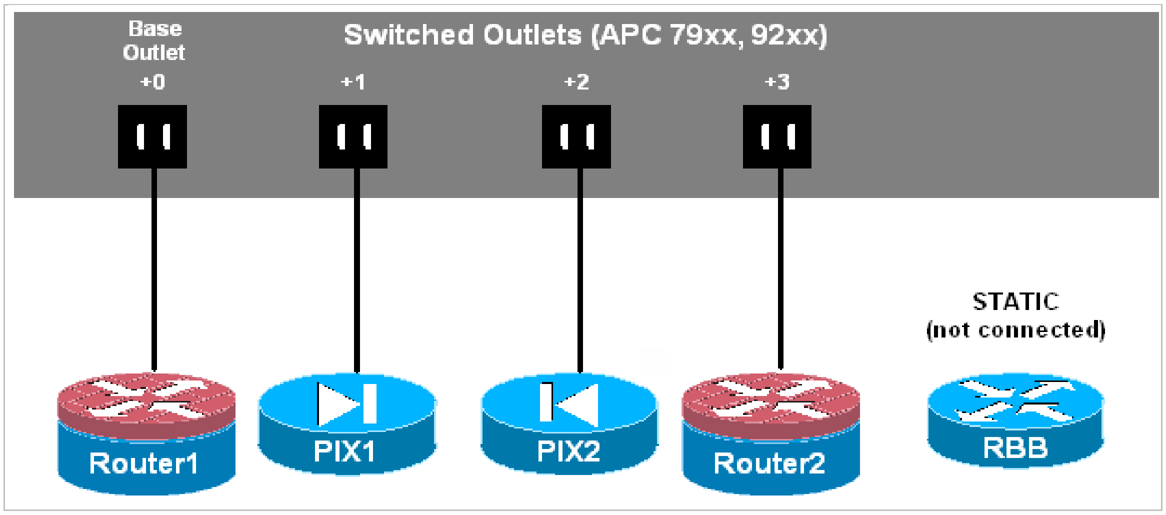
The Network Security pod requires **4** access server ports. **These ports do not have to be consecutive, and can span multiple access servers.**



3.3 Switched Outlets

Switched outlets provide managed electrical power, allowing NETLAB$_{AE}$ and users to turn lab equipment on and off. The Network Security pod requires **4** switched outlets, one for ROUTER1, ROUTER2, PIX1, and PIX2.

Outlets do not have to be consecutive and may span multiple switched outlet devices (i.e. APC7900 or APC7920).



PART 2 – IMPLEMENTATION

4 Pre-requisites

This section covers tasks that should be executed prior to adding a Network Security pod.

4.1 Understanding VMware Virtualization and Virtual Machines

The *NETLAB+ Remote PC Guide for VMware Implementation* contains essential information for setting up a VMware server and virtual machines. It should be used in conjunction with this guide.

4.2 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 Network Security pod. Add control devices if necessary. Control device configuration is documented in the *NETLAB+ Administrator Guide.*

4.3 Upload IOS Images

Upload the IOS images for the lab routers and PIX devices. NETLAB$_{AE}$ will recover these images on the devices if they are erased from flash.

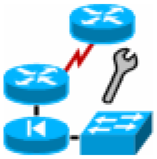
4.4 Disable User Logins (optional)

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 Network Security 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.

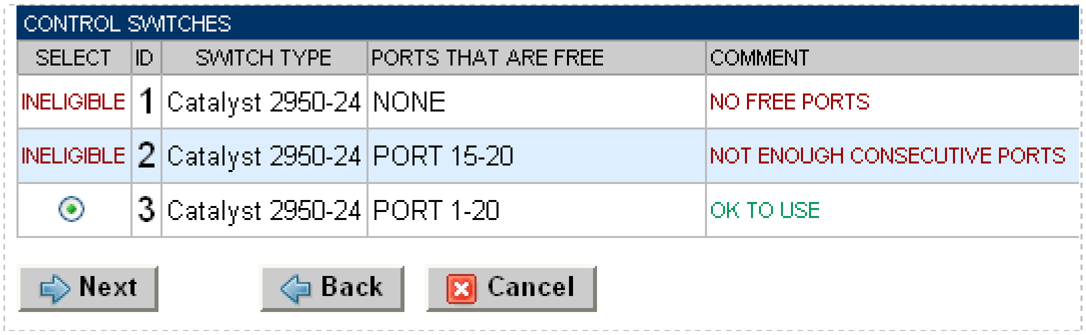
The New Pod Wizard will now help you add an equipment pod to your system.

5.2 Add a Network Security Pod

When prompted, select Network Security Pod 2.0.

5.3 Select Control Switch and Ports

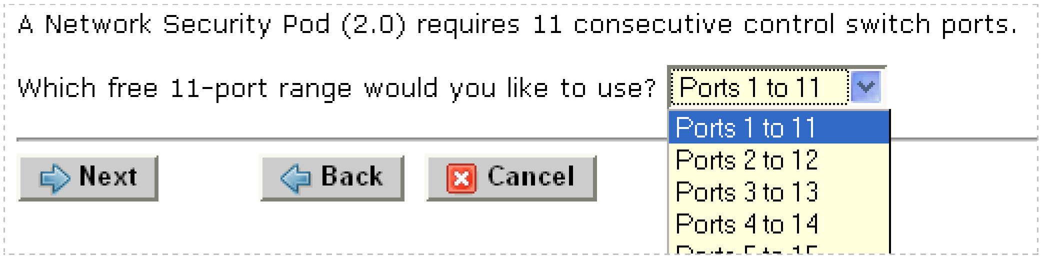
A Network Security pod requires 11 consecutive control switch ports. NETLAB$_{AE}$ will present a list of the control switches on your system. Switches that meet the port requirement can be selected. Choose one control switch for your new pod.



CONTROL SWITCHES

SELECT	ID	SWITCH TYPE	PORTS THAT ARE FREE	COMMENT
INELIGIBLE	1	Catalyst 2950-24	NONE	NO FREE PORTS
INELIGIBLE	2	Catalyst 2950-24	PORT 15-20	NOT ENOUGH CONSECUTIVE PORTS
◉	3	Catalyst 2950-24	PORT 1-20	OK TO USE

Next, select the ports you want to use.



A Network Security Pod (2.0) requires 11 consecutive control switch ports.

Which free 11-port range would you like to use? Ports 1 to 11

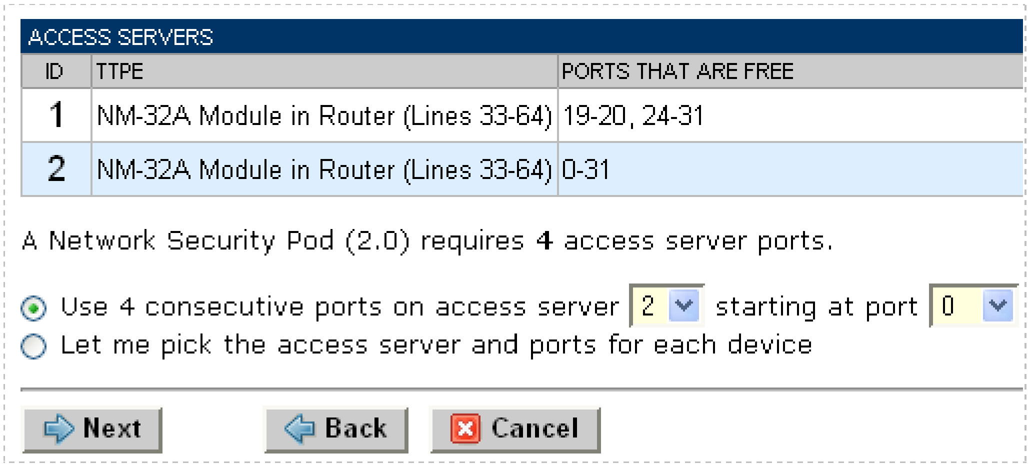
5.4 Select Access Server(s) and Ports

A Network Security pod requires 4 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.

Use the physical port numbers shown on the access server. 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 router.



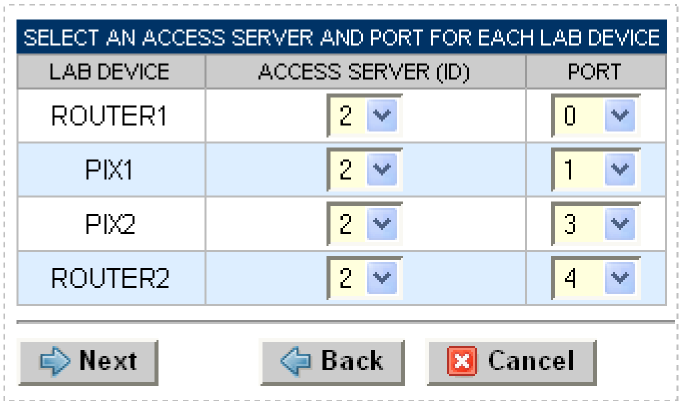
ACCESS SERVERS

ID	TTPE	PORTS THAT ARE FREE
1	NM-32A Module in Router (Lines 33-64)	19-20, 24-31
2	NM-32A Module in Router (Lines 33-64)	0-31

A Network Security Pod (2.0) requires **4** access server ports.

● Use 4 consecutive ports on access server 2 starting at port 0
○ Let me pick the access server and ports for each device

"Let me pick", allows you to make granular selections and split ports among several access servers.



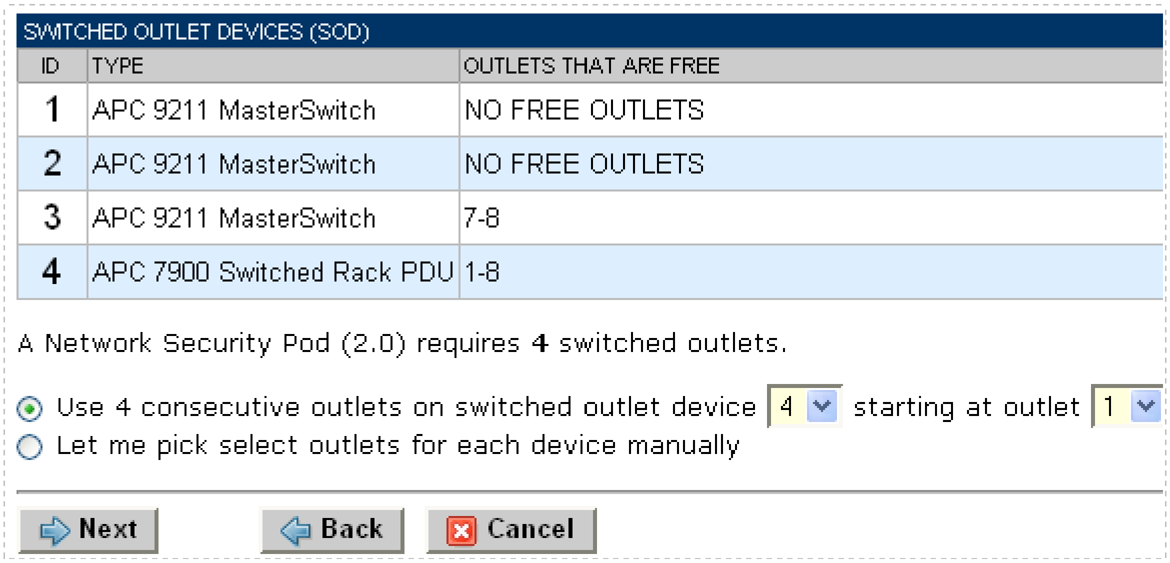
SELECT AN ACCESS SERVER AND PORT FOR EACH LAB DEVICE

LAB DEVICE	ACCESS SERVER (ID)	PORT
ROUTER1	2	0
PIX1	2	1
PIX2	2	3
ROUTER2	2	4

5.5 Select Switched Outlets

A Network Security Pod requires 4 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.



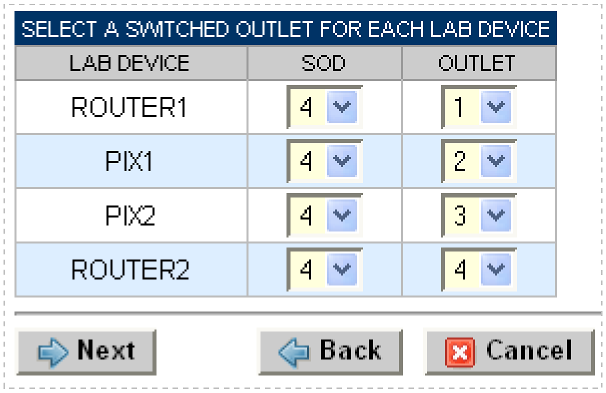
SWITCHED OUTLET DEVICES (SOD)

ID	TYPE	OUTLETS THAT ARE FREE
1	APC 9211 MasterSwitch	NO FREE OUTLETS
2	APC 9211 MasterSwitch	NO FREE OUTLETS
3	APC 9211 MasterSwitch	7-8
4	APC 7900 Switched Rack PDU	1-8

A Network Security Pod (2.0) requires **4** switched outlets.

● Use 4 consecutive outlets on switched outlet device 4 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
ROUTER1	4	1
PIX1	4	2
PIX2	4	3
ROUTER2	4	4

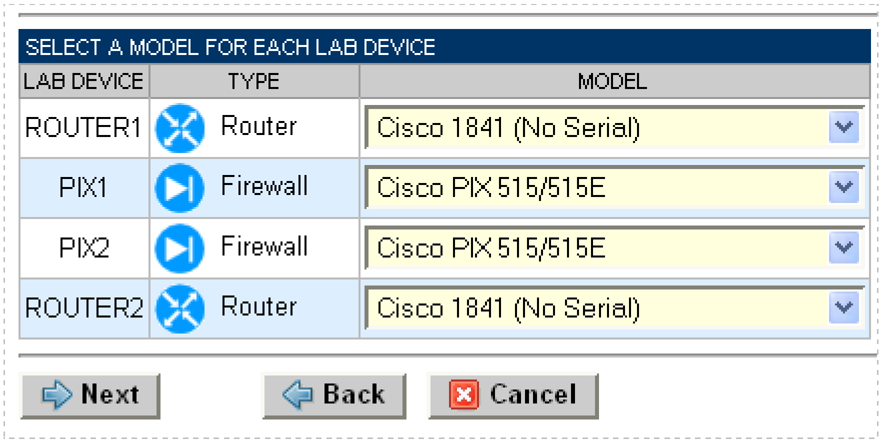
5.6 Select Device Types

Select the router and PIX models you are going to deploy. RBB is a statically configured router, so it does not appear in the router 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 do not support the curriculum. See section 2 for a list of recommended devices for this pod.

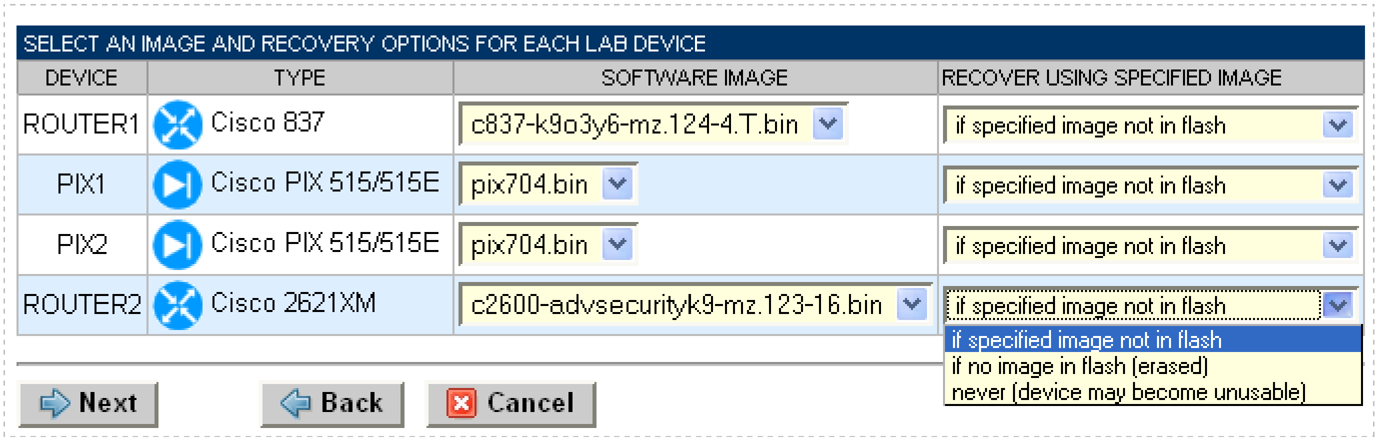


SELECT A MODEL FOR EACH LAB DEVICE

LAB DEVICE	TYPE	MODEL
ROUTER1	Router	Cisco 1841 (No Serial)
PIX1	Firewall	Cisco PIX 515/515E
PIX2	Firewall	Cisco PIX 515/515E
ROUTER2	Router	Cisco 1841 (No Serial)

5.7 Select Software Images and Recovery Options

NETLAB$_{AE}$ scrubs each router and PIX device at the end of lab reservation or upon request. During a scrub, NETLAB$_{AE}$ can recover an IOS 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
ROUTER1	Cisco 837	c837-k9o3y6-mz.124-4.T.bin	if specified image not in flash
PIX1	Cisco PIX 515/515E	pix704.bin	if specified image not in flash
PIX2	Cisco PIX 515/515E	pix704.bin	if specified image not in flash
ROUTER2	Cisco 2621XM	c2600-advsecurityk9-mz.123-16.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, NETLABAE automated boot process will fail and manual restoration of IOS will be required.

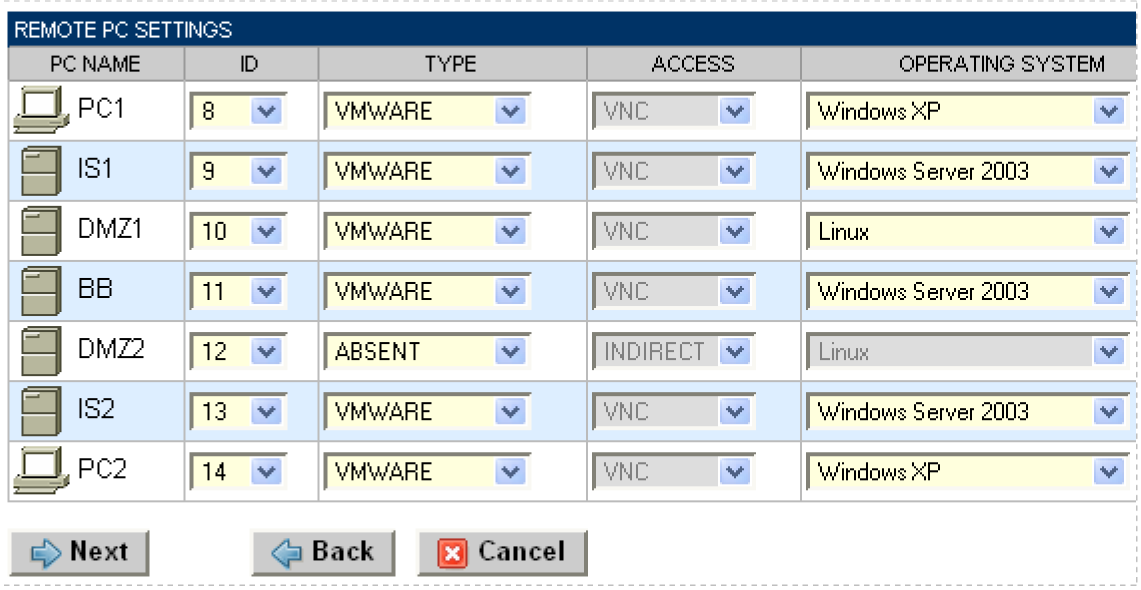
⇒ If you select an automatic recovery option, you must also select a software image supported by the curriculum (see section 2).

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.

The example below shows the typical settings for a VMware setup. We have chosen not to implement DMZ2 in this example, so the type is set to ABSENT.

Figure 5.8.1 – Typical remote PC settings



REMOTE PC SETTINGS

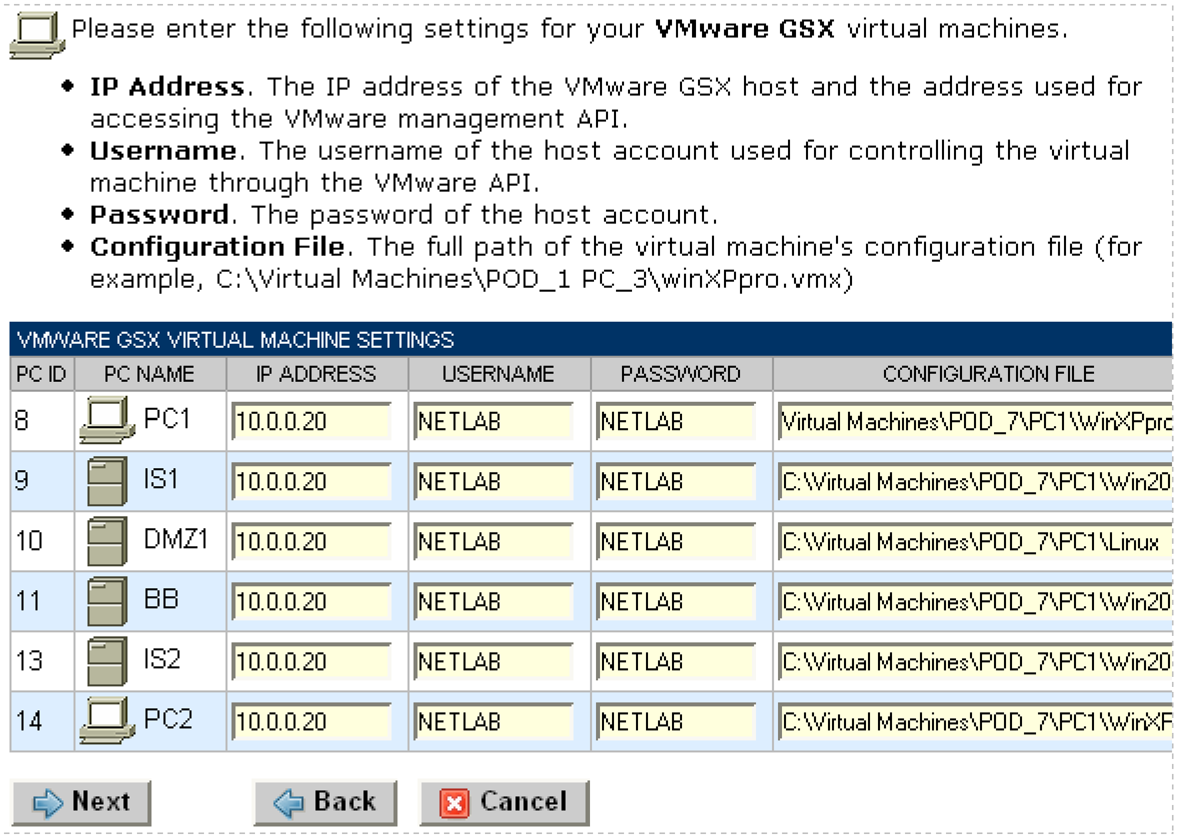
PC NAME	ID	TYPE	ACCESS	OPERATING SYSTEM
PC1	8	VMWARE	VNC	Windows XP
IS1	9	VMWARE	VNC	Windows Server 2003
DMZ1	10	VMWARE	VNC	Linux
BB	11	VMWARE	VNC	Windows Server 2003
DMZ2	12	ABSENT	INDIRECT	Linux
IS2	13	VMWARE	VNC	Windows Server 2003
PC2	14	VMWARE	VNC	Windows XP

The following TYPE and ACCESS combinations correspond to the documentation.

Please Note: Direct/Standalone is not supported in the Network Security Pod.

To implement…	Set TYPE to…	Set ACCESS to…
Direct/VMware	VMWARE	VNC
Direct/Standalone (not supported in this pod)	STANDALONE	VNC
Indirect	(any)	INDIRECT
Absent (no PC)	ABSENT	n/a

5.9 VMware Settings



Please enter the following settings for your **VMware GSX** virtual machines.

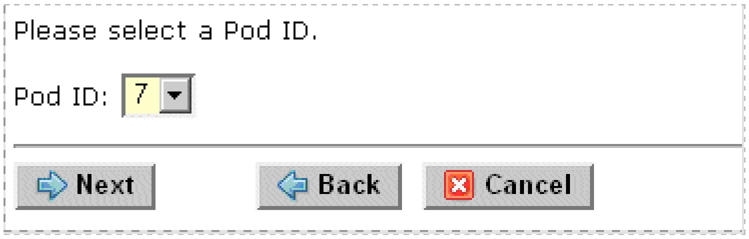
- **IP Address**. The IP address of the VMware GSX host and the address used for accessing the VMware management API.
- **Username**. The username of the host account used for controlling the virtual machine through the VMware API.
- **Password**. The password of the host account.
- **Configuration File**. The full path of the virtual machine's configuration file (for example, C:\Virtual Machines\POD_1 PC_3\winXPpro.vmx)

VMWARE GSX VIRTUAL MACHINE SETTINGS

PC ID	PC NAME	IP ADDRESS	USERNAME	PASSWORD	CONFIGURATION FILE
8	PC1	10.0.0.20	NETLAB	NETLAB	Virtual Machines\POD_7\PC1\WinXPpro
9	IS1	10.0.0.20	NETLAB	NETLAB	C:\Virtual Machines\POD_7\PC1\Win20
10	DMZ1	10.0.0.20	NETLAB	NETLAB	C:\Virtual Machines\POD_7\PC1\Linux
11	BB	10.0.0.20	NETLAB	NETLAB	C:\Virtual Machines\POD_7\PC1\Win20
13	IS2	10.0.0.20	NETLAB	NETLAB	C:\Virtual Machines\POD_7\PC1\Win20
14	PC2	10.0.0.20	NETLAB	NETLAB	C:\Virtual Machines\POD_7\PC1\WinXP

5.10 Select a Pod ID

Each pod is assigned a unique numeric ID.

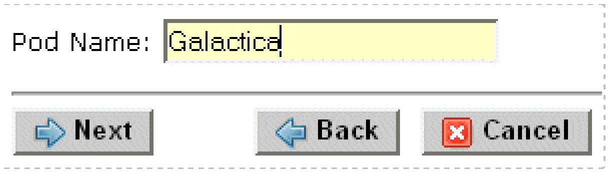


Please select a Pod ID.

Pod ID: 7

5.11 Select a Pod Name

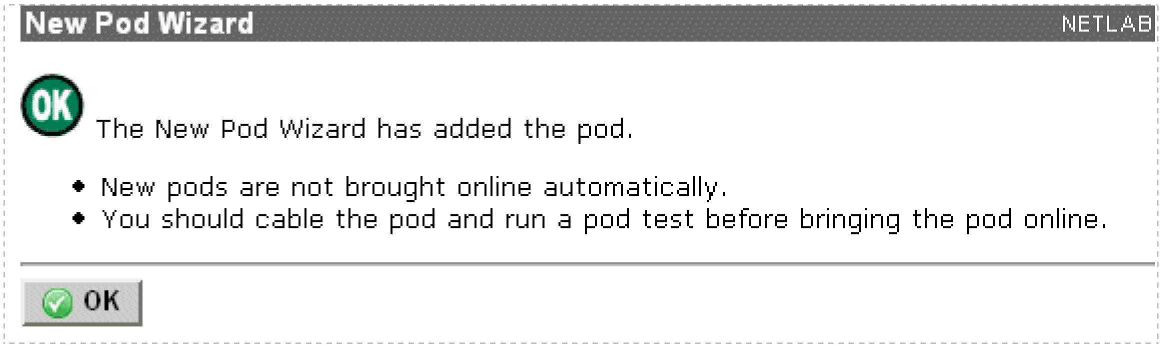
Each pod can have a unique name. This name will appear in the scheduler, along with the pod type.



Pod Name: Galactica

5.12 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.



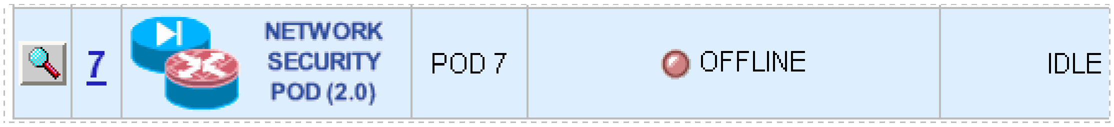
New Pod Wizard NETLAB

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.

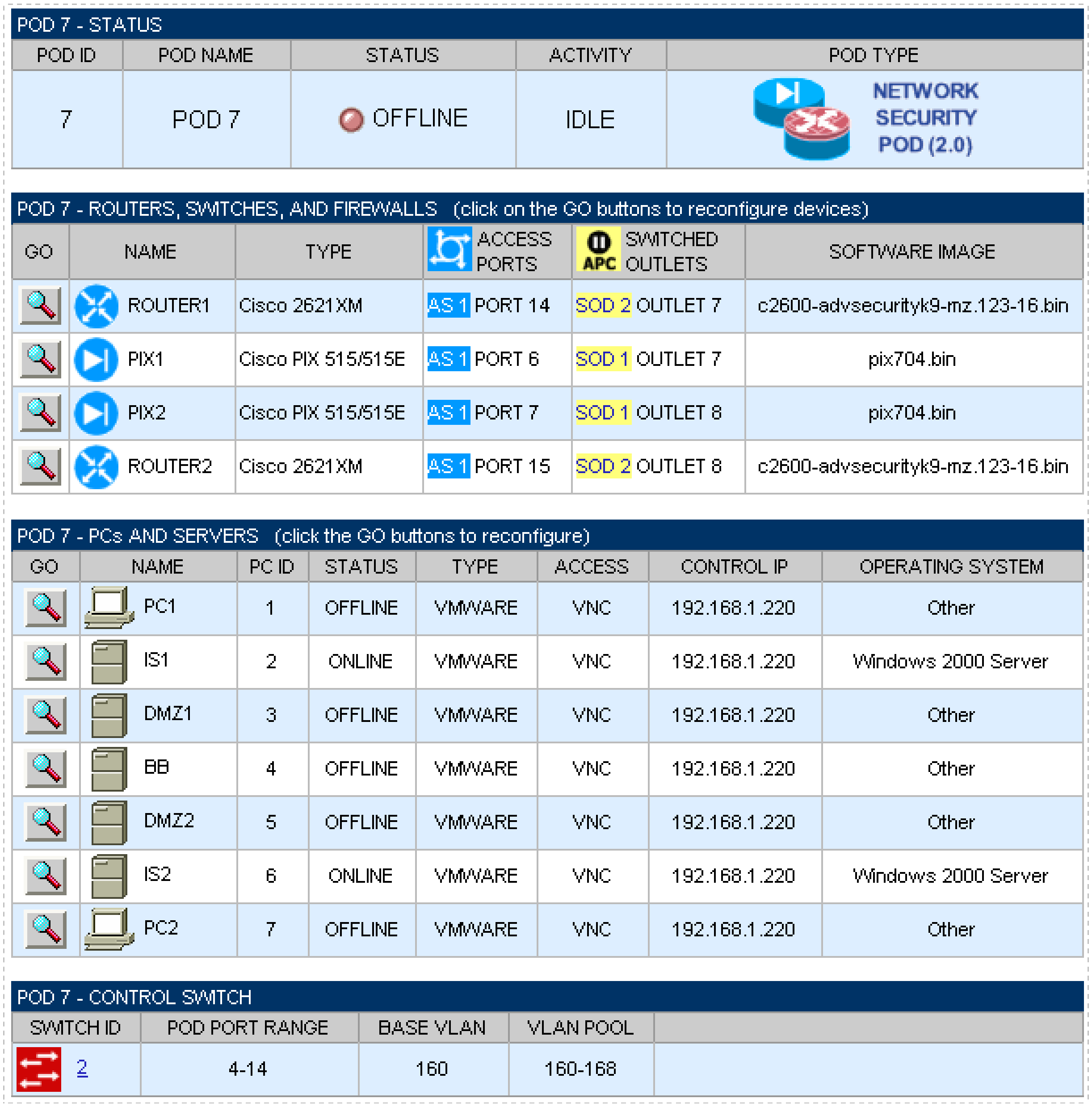
After you click OK, the new pod will appear in the list of equipment pods.

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



🔍	7	NETWORK SECURITY POD (2.0)	POD 7	● OFFLINE	IDLE

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



POD 7 - STATUS

POD ID	POD NAME	STATUS	ACTIVITY	POD TYPE
7	POD 7	● OFFLINE	IDLE	NETWORK SECURITY POD (2.0)

POD 7 - ROUTERS, SWITCHES, AND FIREWALLS (click on the GO buttons to reconfigure devices)

GO	NAME	TYPE	ACCESS PORTS	SWITCHED OUTLETS	SOFTWARE IMAGE
🔍	ROUTER1	Cisco 2621XM	AS 1 PORT 14	SOD 2 OUTLET 7	c2600-advsecurityk9-mz.123-16.bin
🔍	PIX1	Cisco PIX 515/515E	AS 1 PORT 6	SOD 1 OUTLET 7	pix704.bin
🔍	PIX2	Cisco PIX 515/515E	AS 1 PORT 7	SOD 1 OUTLET 8	pix704.bin
🔍	ROUTER2	Cisco 2621XM	AS 1 PORT 15	SOD 2 OUTLET 8	c2600-advsecurityk9-mz.123-16.bin

POD 7 - PCs AND SERVERS (click the GO buttons to reconfigure)

GO	NAME	PC ID	STATUS	TYPE	ACCESS	CONTROL IP	OPERATING SYSTEM
🔍	PC1	1	OFFLINE	VMWARE	VNC	192.168.1.220	Other
🔍	IS1	2	ONLINE	VMWARE	VNC	192.168.1.220	Windows 2000 Server
🔍	DMZ1	3	OFFLINE	VMWARE	VNC	192.168.1.220	Other
🔍	BB	4	OFFLINE	VMWARE	VNC	192.168.1.220	Other
🔍	DMZ2	5	OFFLINE	VMWARE	VNC	192.168.1.220	Other
🔍	IS2	6	ONLINE	VMWARE	VNC	192.168.1.220	Windows 2000 Server
🔍	PC2	7	OFFLINE	VMWARE	VNC	192.168.1.220	Other

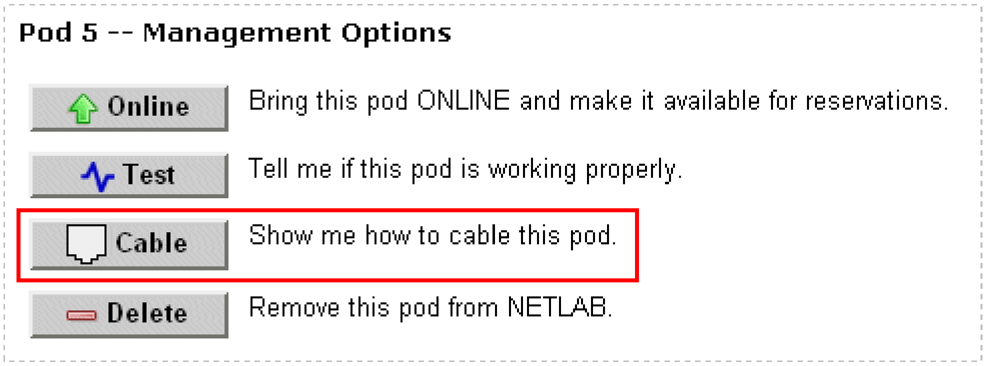
POD 7 - CONTROL SWITCH

SWITCH ID	POD PORT RANGE	BASE VLAN	VLAN POOL	
2	4-14	160	160-168	

6 Cable the Pod

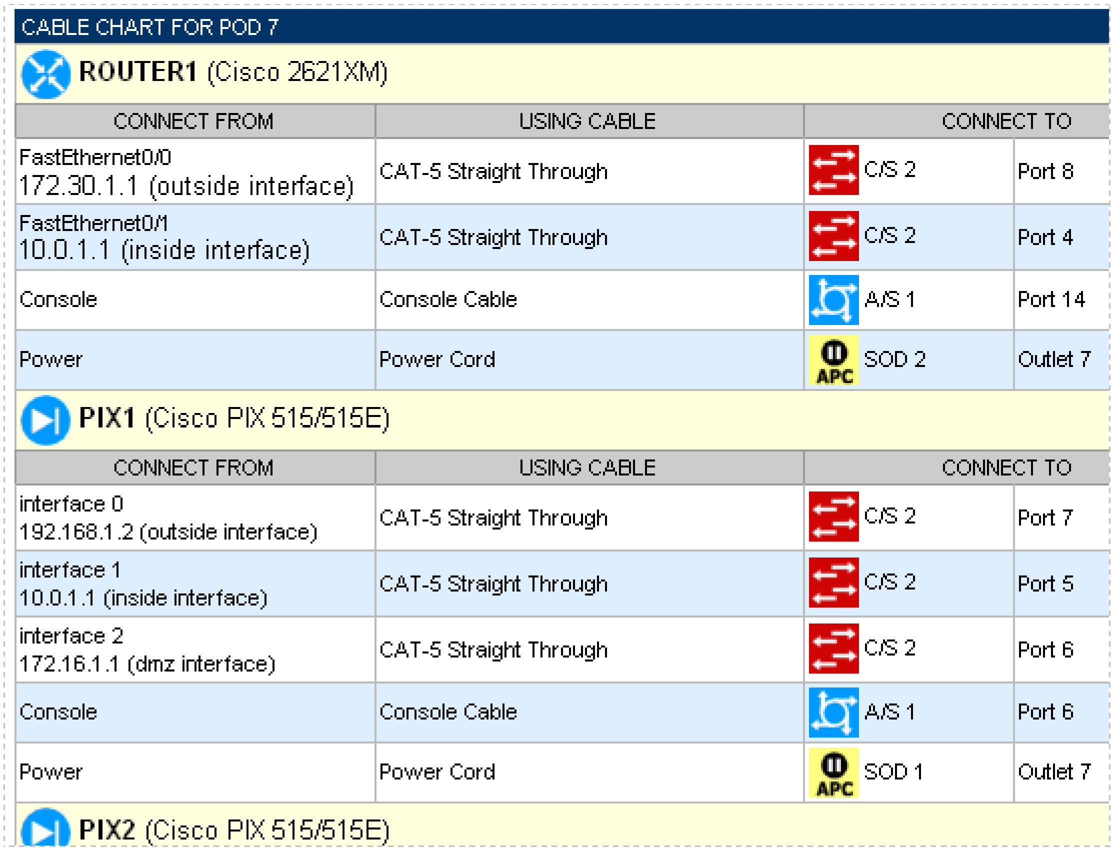
Use the NETLAB$_{AE}$ cable chart feature to help you connect the lab devices in your pod. The chart is generated in real-time and contains port-specific information based on your current lab device and control device settings.

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



Pod 5 -- 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 7

ROUTER1 (Cisco 2621XM)

CONNECT FROM	USING CABLE	CONNECT TO	
FastEthernet0/0 172.30.1.1 (outside interface)	CAT-5 Straight Through	C/S 2	Port 8
FastEthernet0/1 10.0.1.1 (inside interface)	CAT-5 Straight Through	C/S 2	Port 4
Console	Console Cable	A/S 1	Port 14
Power	Power Cord	SOD 2	Outlet 7

PIX1 (Cisco PIX 515/515E)

CONNECT FROM	USING CABLE	CONNECT TO	
interface 0 192.168.1.2 (outside interface)	CAT-5 Straight Through	C/S 2	Port 7
interface 1 10.0.1.1 (inside interface)	CAT-5 Straight Through	C/S 2	Port 5
interface 2 172.16.1.1 (dmz interface)	CAT-5 Straight Through	C/S 2	Port 6
Console	Console Cable	A/S 1	Port 6
Power	Power Cord	SOD 1	Outlet 7

PIX2 (Cisco PIX 515/515E)

Please Note: Router RBB and virtual machine information will not appear on the cable chart. Refer to section 6 and section 7 for cabling and configuration instructions.

7 Configuring VMware and Virtual Machines

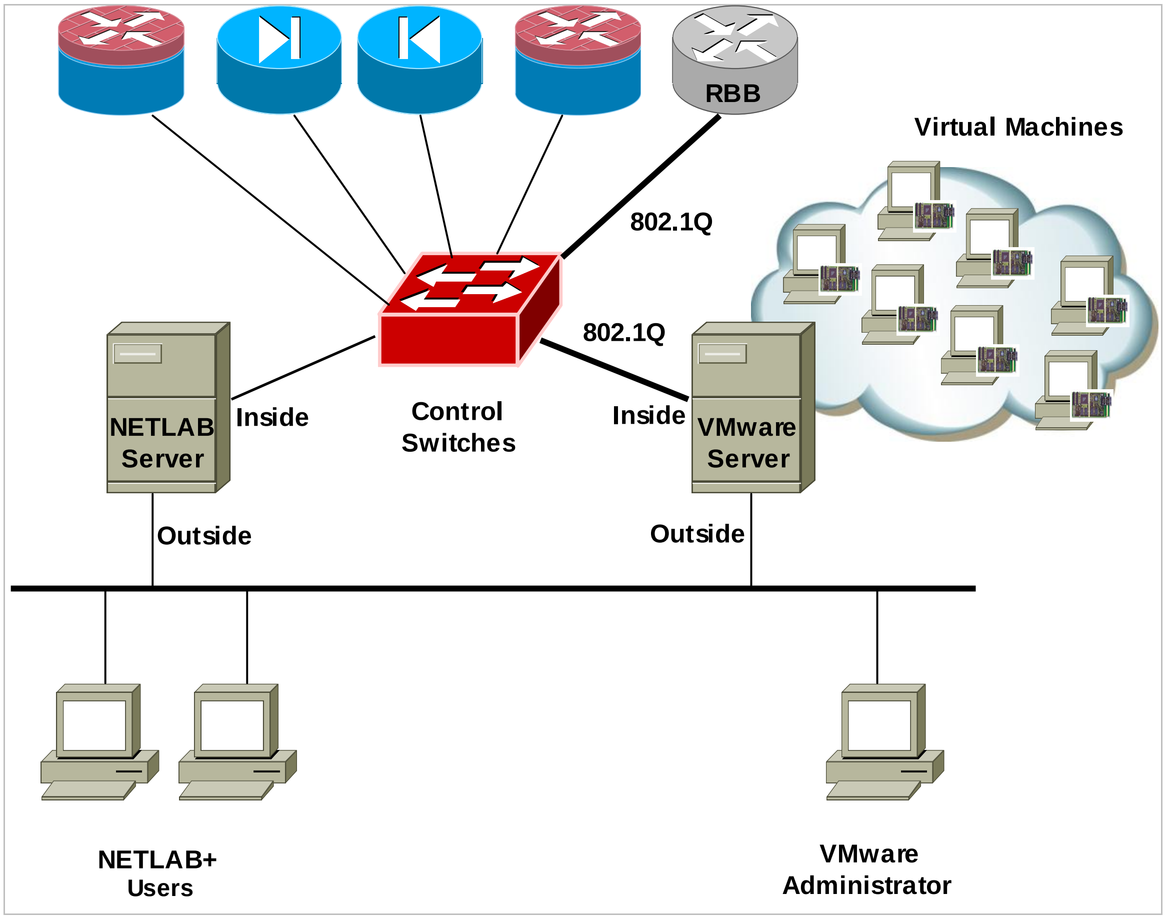
The *NETLAB+ Remote PC Guide for VMware implementation* explains how to set up VMware server and virtual machines. Please review the pod-specific information in this section and apply it to the general information in the *NETLAB+ Remote PC Guide for VMware Implementation*. Please note, only the sections referring to VMware are relevant; the Network Security pod does not support standalone PCs.

After you load applications or make changes to a PC, be sure to take a VMware snapshot. NETLAB$_{AE}$ instructs VMware to "revert" to the snapshot at the end of each lab reservation. Any changes made after a snapshot are lost.

Please Note: The IP addresses and/or default gateways of PC1, PC2, IS1, and IS2 may vary. Depending on your snapshots, the student may need to adjust IP settings to reflect the lab.

7.1 Connecting Virtual Machines to the Pod

Virtual Machines must communicate with routers and PIX devices in the pod. Control switches provide the connection point. In the recommended configuration (below), the VMware server is equipped with an inside and outside interface. The inside interface is configured for 802.1Q connects to a reserved port on a control switch. Traffic between virtual machines and devices in the pod traverse the VMware server inside interface. Preferably, the VMware server should connect to the same control switch as the pod.

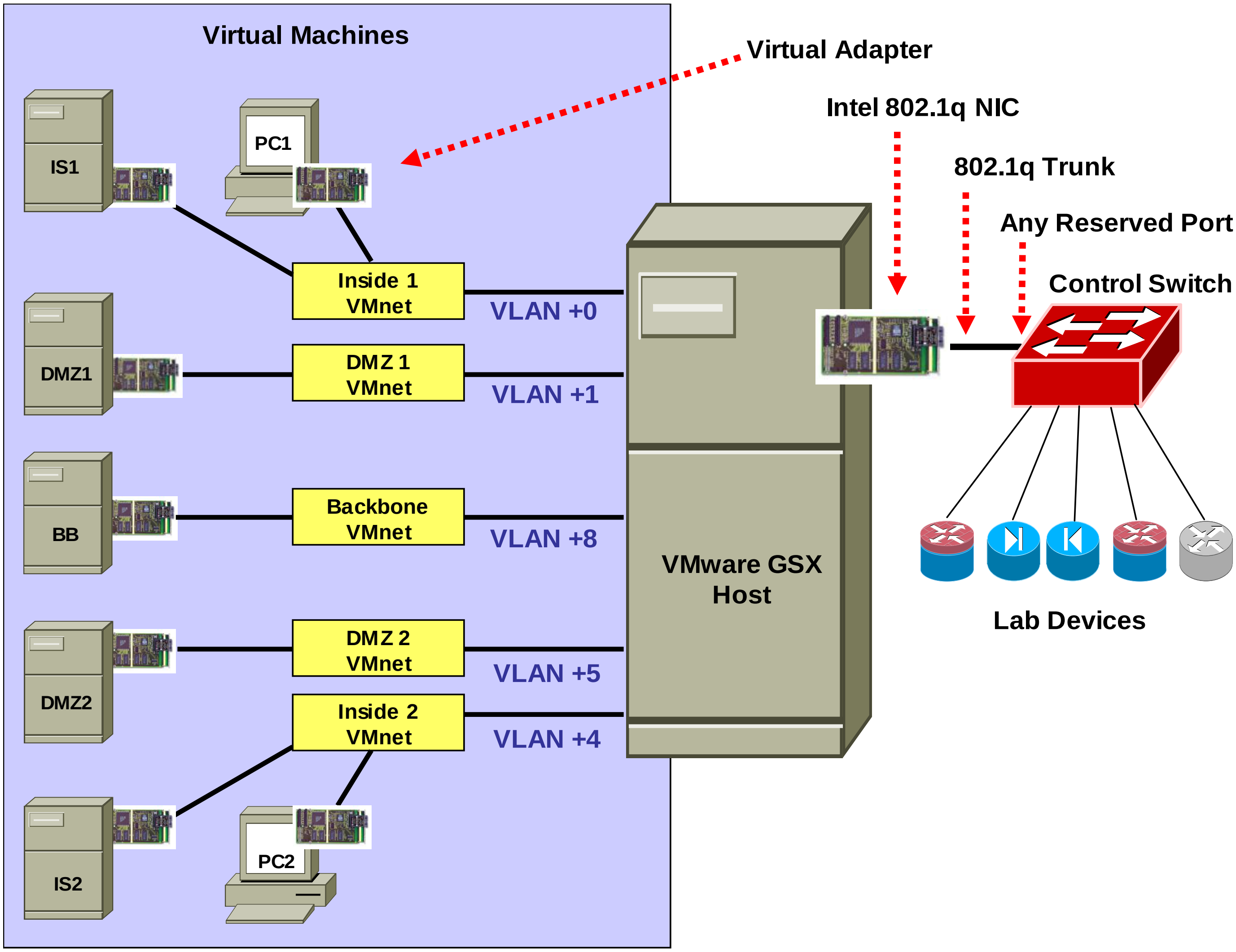


7.2 VMware Virtual Switches and VLANs

VMware virtual network adapters and virtual LAN switches (VMnets) are used to connect virtual machines to the pod. The Network Security pod uses **5 VMnets**. Since VMware virtualization supports 10 virtual switches, it is possible to host 2 complete Network Security pods on a single VMware server.

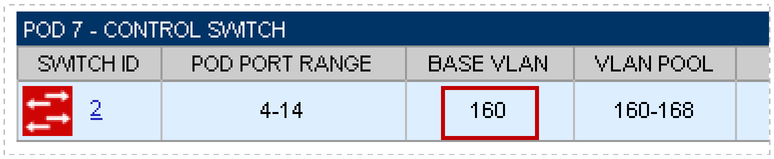
Each virtual switch is mapped to a specific VLAN and bound to the VMware inside 802.1Q NIC card. The actual VLAN numbers used are based on the pod's ID number.

IS1 and PC1 share a common VMnet and VLAN. IS2 and PC2 also share a common VMnet and VLAN.



Each NETLAB$_{AE}$ pod is automatically assigned a pool of unique VLAN numbers. You must determine which VLAN numbers correspond to each virtual switch on the VMware server.

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 7 - CONTROL SWITCH

SWITCH ID	POD PORT RANGE	BASE VLAN	VLAN POOL
2	4-14	160	160-168

In this example, pod 7 uses VLANs 160-168. The base VLAN is 160.

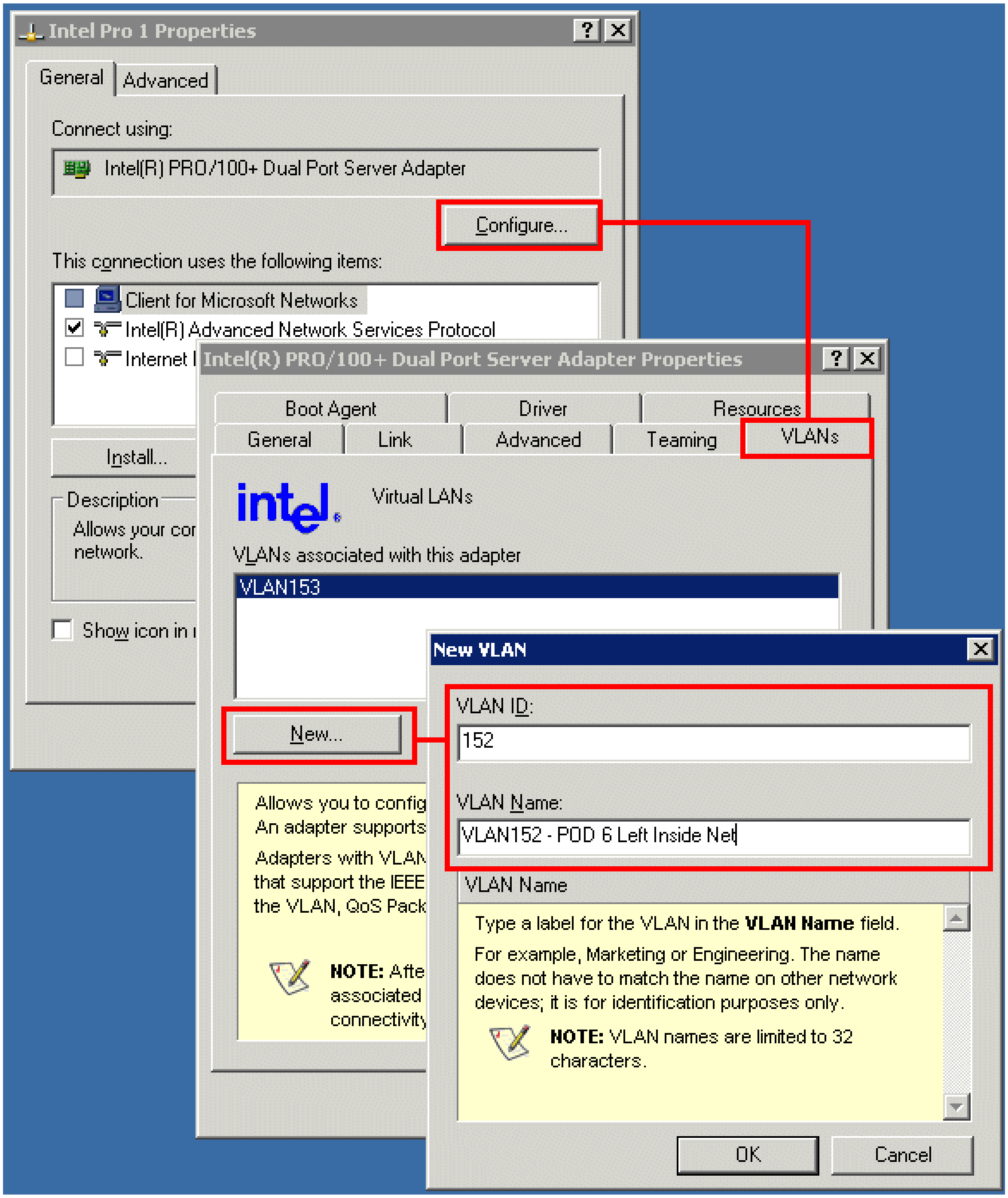
Next, determine the actual VLAN number for each virtual network by adding the base VLAN to the offsets in the table below.

Virtual Machines	Virtual Switch (VMnet)	Offset (add to base VLAN)	Actual VLAN	Example
PC1 IS1	Inside 1	+ 0	= _____	160 + 0 = 160
DMZ1	DMZ1	+ 1	= _____	160 + 1 = 161
BB	Backbone	+ 8	= _____	160 + 8 = 168
DMZ2	DMZ2	+ 5	= _____	160 + 5 = 165
PC2 IS2	Inside 2	+ 4	= _____	160 + 4 = 164

7.3 Configure VMware Server Inside Port

Refer to section 6 of the *NETLAB+ Remote PC Guide for VMware Implementation*. Create the 5 VLANs (calculated above) on the VMware server's inside 802.1Q NIC.

Although it is possible to bind an IP address, mask, and gateway to each VLAN on the server's inside NIC, you should not do so. The VLANs created on the server act as a layer 2 conduit between lab devices and virtual machines. Binding layer 3 information to the VLAN interfaces on the server adapter may cause unpredictable routing and/or leakage to outside networks.



Connect using: Intel(R) PRO/100+ Dual Port Server Adapter

This connection uses the following items:

- ☐ Client for Microsoft Networks
- ☑ Intel(R) Advanced Network Services Protocol
- ☐ Internet

Allows your co
network.

VLANs associated with this adapter: VLAN153

Allows you to config
An adapter supports
Adapters with VLAN
that support the IEEE
the VLAN, QoS Pack

NOTE: Afte
associated
connectivity

VLAN ID: 152

VLAN Name: VLAN152 - POD 6 Left Inside Net

VLAN Name

Type a label for the VLAN in the **VLAN Name** field.

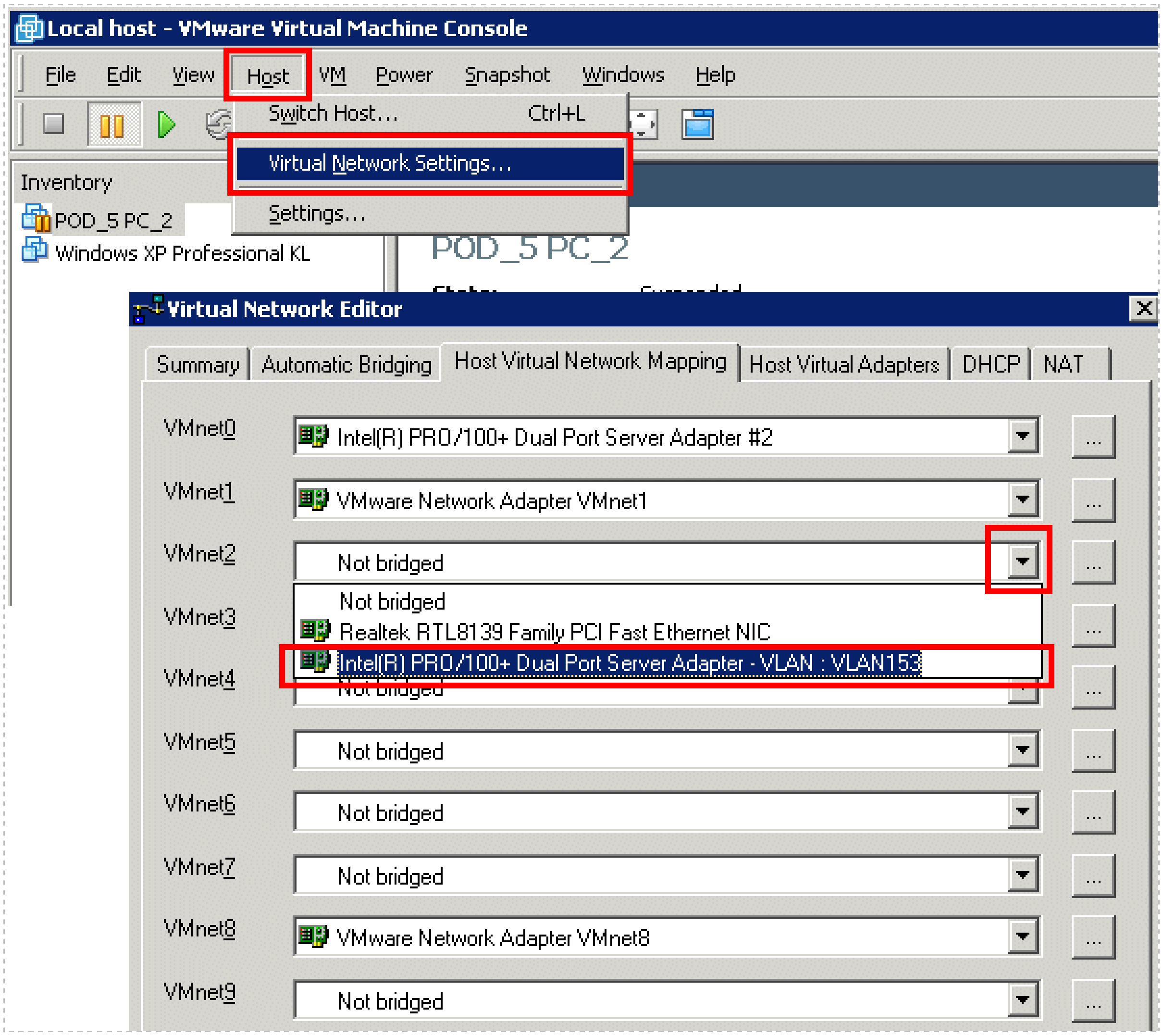
For example, Marketing or Engineering. The name does not have to match the name on other network devices; it is for identification purposes only.

NOTE: VLAN names are limited to 32 characters.

7.4 Create Virtual Switches (VMnet)

Refer to section 6 of the *NETLAB+ Remote PC Guide for VMware Implementation*. Create 5 virtual switches and bind them to the VLANs created in the previous section.

It does not matter which VMnet number you use. By default, VMnet0, VMnet1, and VMnet8 are reserved for special functions in VMware. However, you can convert these into ordinary VMnets to use with pods. This is explained in Appendix A of the *NETLAB+ Remote PC Guide for VMware implementation*.


Local host - VMware Virtual Machine Console
File
Edit
View
Host
VM
Power
Snapshot
Windows
Help
Switch Host... Ctrl+L
Virtual Network Settings...
Settings...
Inventory
POD_5 PC_2
Windows XP Professional KL
POD_5 PC_2
Virtual Network Editor
Summary
Automatic Bridging
Host Virtual Network Mapping
Host Virtual Adapters
DHCP
NAT
Not bridged
Realtek RTL8139 Family PCI Fast Ethernet NIC
Intel(R) PRO/100+ Dual Port Server Adapter - VLAN : VLAN153

VMnet0 Intel(R) PRO/100+ Dual Port Server Adapter #2

VMnet1 VMware Network Adapter VMnet1

VMnet2 Not bridged

VMnet3

VMnet4 Not bridged

VMnet5 Not bridged

VMnet6 Not bridged

VMnet7 Not bridged

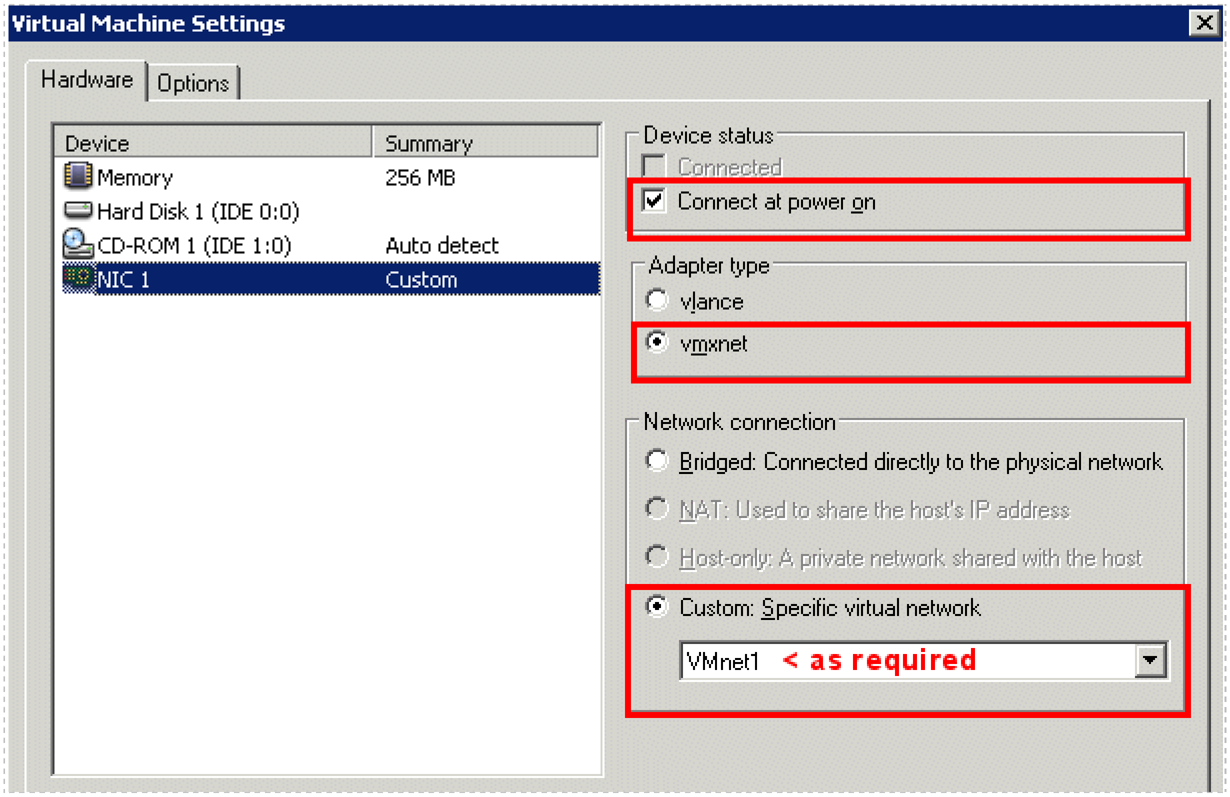
VMnet8 VMware Network Adapter VMnet8

VMnet9 Not bridged

7.5 Binding Virtual Machines to Virtual Switches (VMnet)

Refer to section 7 of the *NETLAB+ Remote PC Guide for VMware Implementation*. In the last section, you associated a specific VLAN with a virtual switch (VMnet). When you create a virtual machine, you must bind it to the correct virtual switch (and by association, VLAN).

Virtual Machines	Virtual Switch (VMnet)	Offset (add to base VLAN)	Actual VLAN	Example
PC1 IS1	Inside 1	+ 0	= _____	160 + 0 = 160
DMZ1	DMZ1	+ 1	= _____	160 + 1 = 161
BB	Backbone	+ 8	= _____	160 + 8 = 168
DMZ2	DMZ2	+ 5	= _____	160 + 5 = 165
PC2 IS2	Inside 2	+ 4	= _____	160 + 4 = 164



Virtual Machine Settings

Hardware | Options

Device	Summary
Memory	256 MB
Hard Disk 1 (IDE 0:0)	
CD-ROM 1 (IDE 1:0)	Auto detect
NIC 1	Custom

Device status
□ Connected
☑ Connect at power on

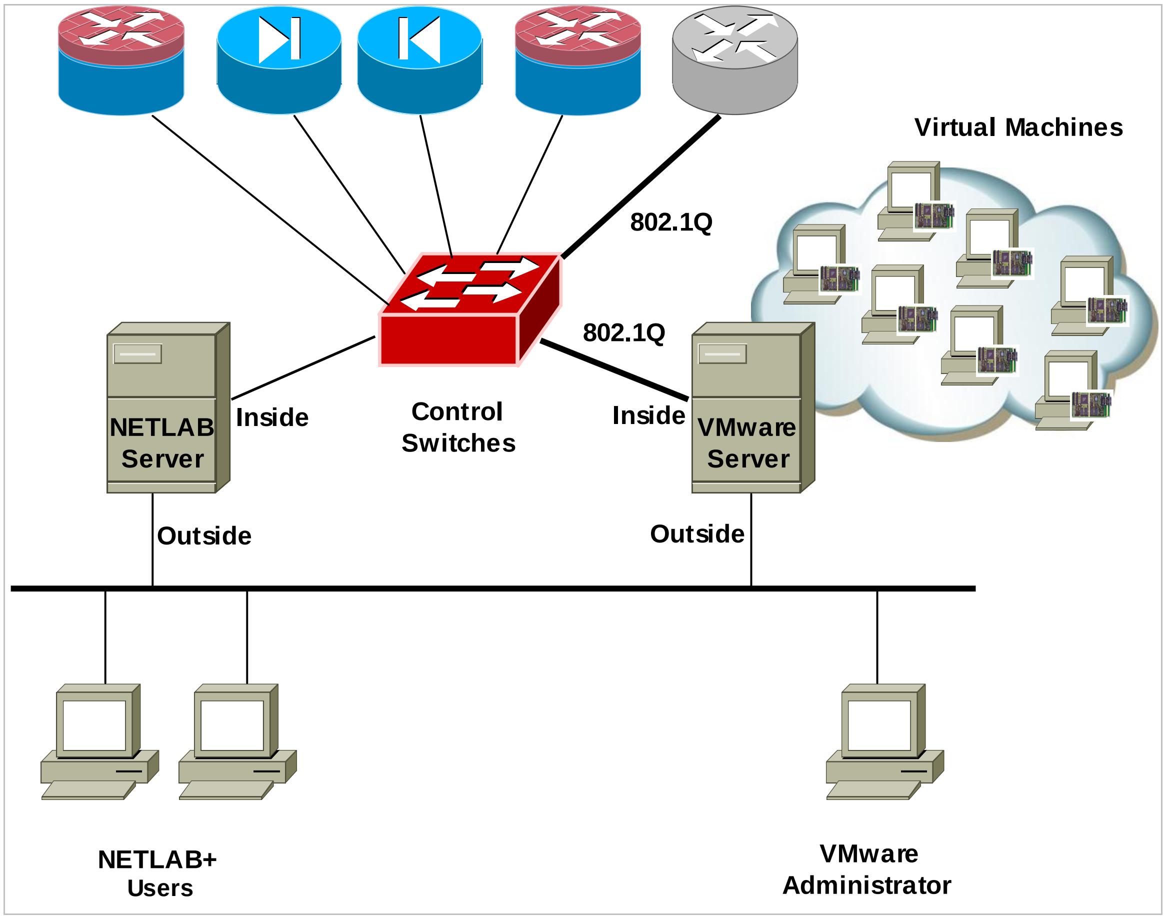
Adapter type
○ vlance
● vmxnet

Network connection
○ Bridged: Connected directly to the physical network
○ NAT: Used to share the host's IP address
○ Host-only: A private network shared with the host
● Custom: Specific virtual network

VMnet1 < as required

7.6 Configuring the Control Switch for VMware

One “reserved” port on the control switch connects to an 802.1q NIC card on the VMware server. This allows devices in the pod to communicate with virtual machines. The reserved port should be configured as an 802.1q trunk port.



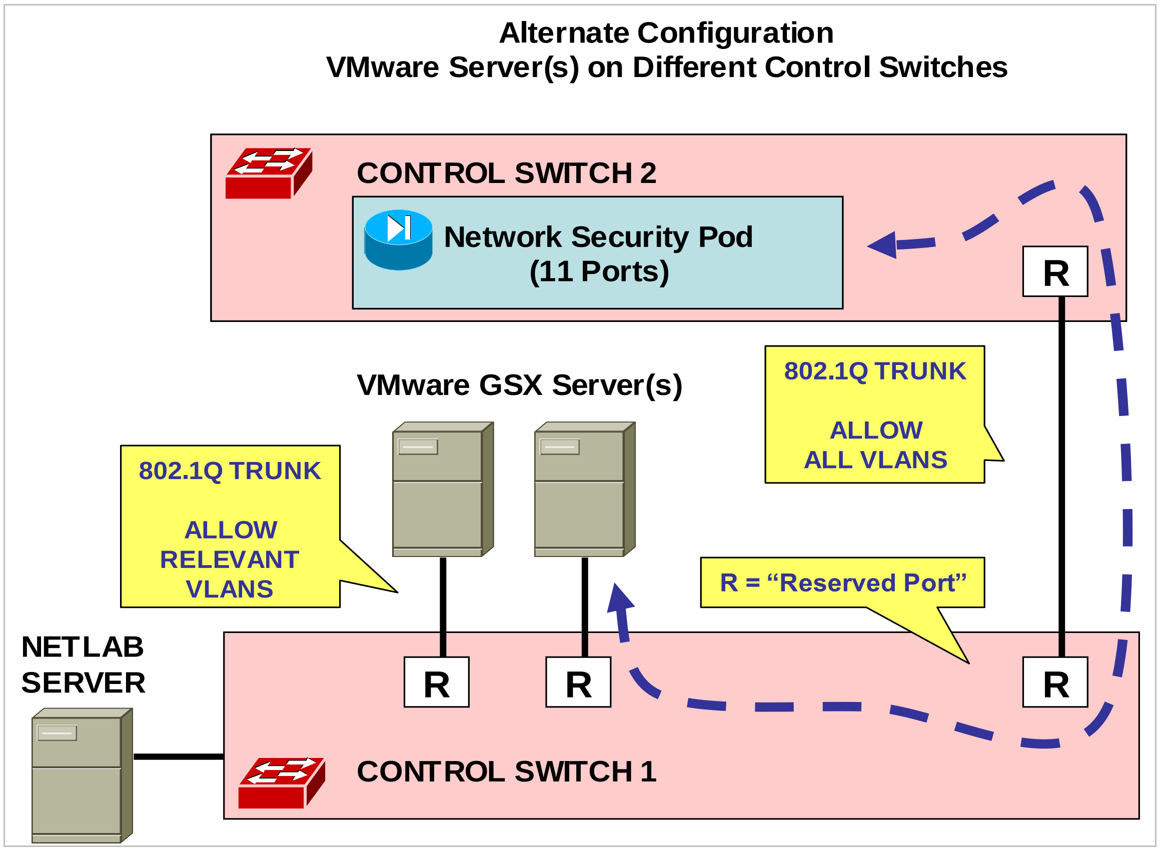
Once you have allocated a reserved port on the control switch, connect the VMware server inside NIC using a straight through CAT5 cable. Configure the switch port as a trunk and allow only the VLANs that were bound to the VMnets. If your VMware server hosts virtual machines for more than one pod, allow all the relevant VLANs for each pod.

Example switch port configuration. Interface number and VLANs will vary.

```
interface FastEthernet0/23
 switchport mode trunk
 switchport trunk allowed vlan 160,161,164,165,168
 switchport nonegotiate
 no switchport access vlan
 no shutdown
```

7.7 VMware Server(s) on Different Control Switch

The reserved port may be located on a different control switch, provided that all links between control switches are also configured as 802.1q trunks and all VLANs are allowed. You may also have more than one VMware server. Virtual machines in the pod can be located on different VMware servers.



Ports connecting to VMware servers should only allow the VLANs associated with the pods being served. In addition, "switchport nonegotiate" should be used to suppress Dynamic Trunk Protocol (DTP):

```
interface FastEthernet0/23
 switchport mode trunk
 switchport trunk allowed vlan 160,161,164,165,168
 switchport nonegotiate
 no switchport access vlan
 no shutdown
```

Ports connecting control switches together, allow all VLANs and DTP:

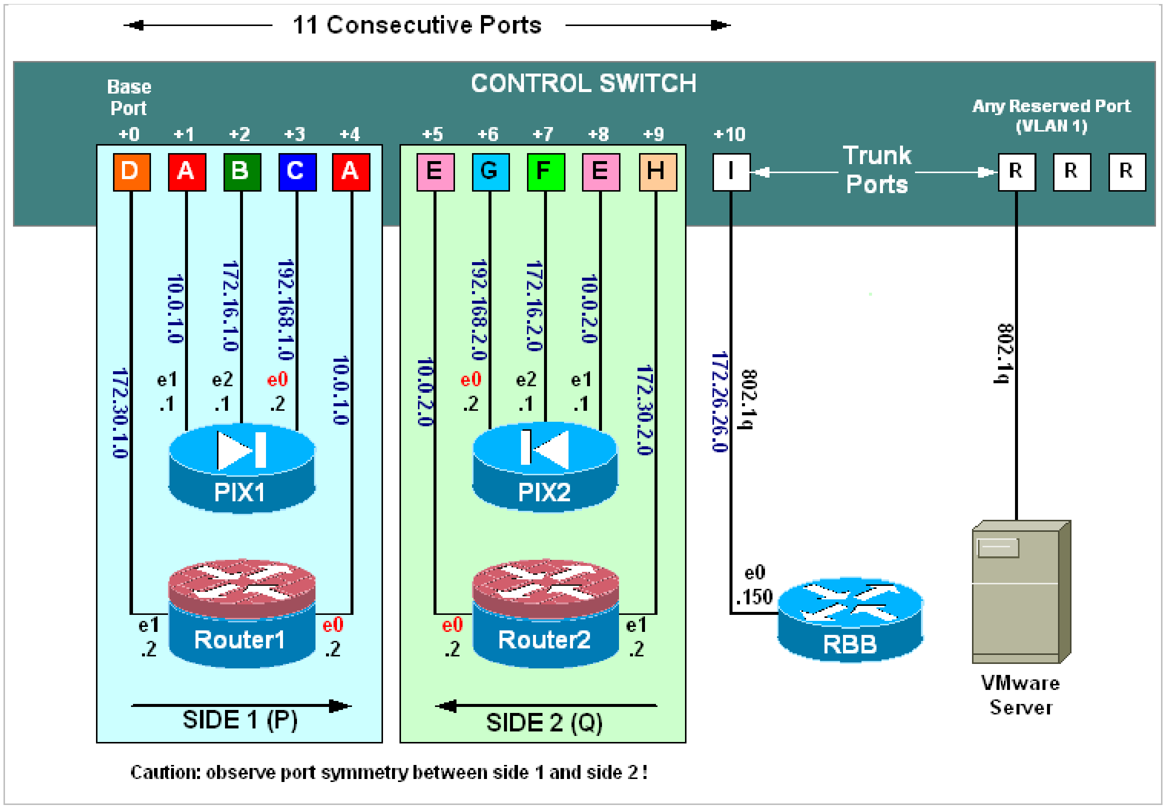
```
interface FastEthernet0/24
 switchport mode trunk
 no switchport access vlan
 switchport trunk allowed vlan all
 no shutdown
```

8 Backbone Router Configuration (RBB)

RBB is a backbone router with a static configuration. At least one Fast Ethernet port supporting 802.1q is required. NETLAB$_{AE}$ does not allocate an access server connection for RBB, so users cannot directly access the console port. However, it is part of the topology so users can indirectly interact with it (i.e. ping, trace, RIP, etc.).

⇒ You may allow student Telnet access to RBB from BB, PC1, or PC2. Since RBB is part of the pod infrastructure, we do not recommend privileged (enable) access.

The RBB router should be connected to control switch port +10 as depicted below. For example, if the base port for this pod is FastEthernet0/1, then connect RBB to FastEthernet0/11.

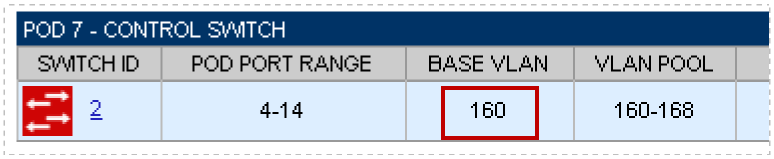


Caution: observe port symmetry between side 1 and side 2 !

8.1 Determine VLANs

Recall that each pod is automatically assigned a pool of unique VLAN numbers. Next, you must determine which VLAN numbers are actually used for the networks that attach to RBB.

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.

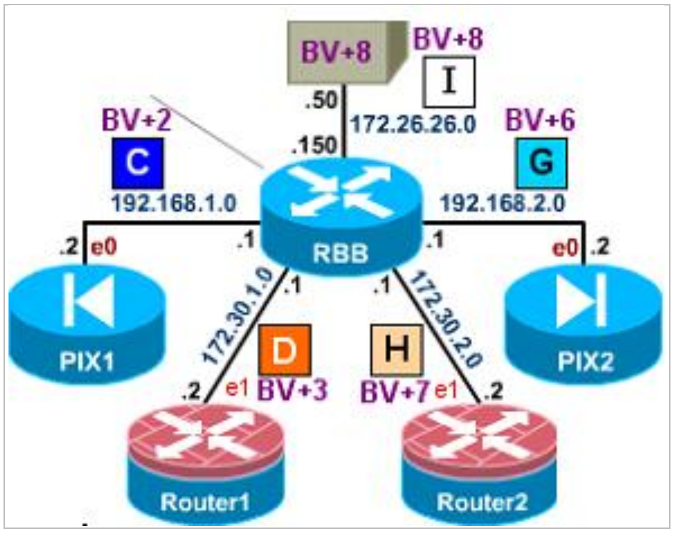


POD 7 - CONTROL SWITCH

SWITCH ID	POD PORT RANGE	BASE VLAN	VLAN POOL
2	4-14	160	160-168

In this example, pod 7 uses VLANs 160-168. The base VLAN is 160.

RBB connects to 5 of these VLANs, depicted as VLAN C, D, H, G, and I.



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 (shown above)	Subnet	Offset (add to base VLAN)	Actual VLAN	Example
C	192.168.1.0	+ 2	= _____	160 + 2 = 162
D	172.30.1.0	+ 3	= _____	160 + 3 = 163
G	192.168.2.0	+ 6	= _____	160 + 6 = 166
H	172.30.2.0	+ 7	= _____	160 + 7 = 167
I	172.26.26.0	+ 8	= _____	160 + 8 = 168

8.2 Configure RBB's Control Switch Port

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 FastEthernet0/11
 switchport mode trunk
 switchport trunk allowed vlan 162,163,166,167,168
 switchport nonegotiate
 no switchport access vlan
 no shutdown
```

8.3 Configure RBB

Connect and configure RBB via the console port.

Since RBB is static and not managed by NETLAB$_{AE}$, you should use a different enable password than the one used for hands on lab routers.

```
enable secret some-other-password
!(not class!, not router!, not cisco!)
```

To allow telnet access to RBB by users, configure a password on vty 0 through 5. The standard Academy password is "cisco".

```
line vty 0 5
 password cisco
 login
```

Alternatively, to prevent telnet access to RBB from users, disable login on vty lines 0 through 5.

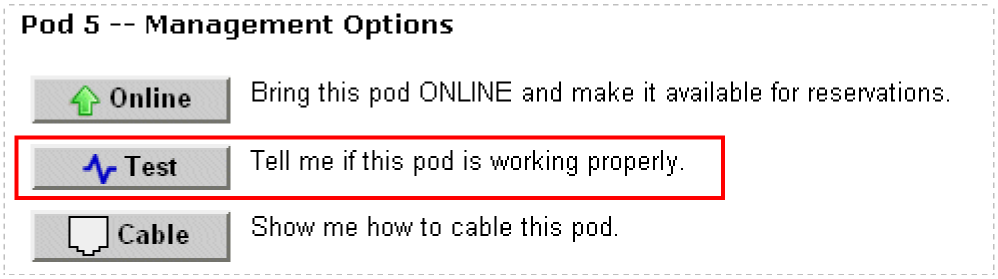
```
line vty 0 5
 no login
```

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

```
hostname RBB

key chain RTRAUTH
 key 1
  key-string 123456789

interface FastEthernet0/0.162
 description to PIX1 outside network
 encapsulation dot1q 162
 ip address 192.168.1.1 255.255.255.0
 no shutdown

interface FastEthernet0/0.163
 description to ROUTER1 outside network
 encapsulation dot1q 163
 ip address 172.30.1.1 255.255.255.0
 ip rip authentication mode md5
 ip rip authentication key-chain RTRAUTH
 no shutdown

interface FastEthernet0/0.166
 description to PIX2 outside network
 encapsulation dot1q 166
 ip address 192.168.2.1 255.255.255.0
 no shutdown

interface FastEthernet0/0.167
 description to ROUTER2 outside network
 encapsulation dot1q 167
 ip address 172.30.2.1 255.255.255.0
 ip rip authentication mode md5
 ip rip authentication key-chain RTRAUTH
 no shutdown

interface FastEthernet0/0.168
 description to BB backbone server
 encapsulation dot1q 168
 ip address 172.26.26.150 255.255.255.0
 no shutdown

router rip
 version 2
 network 172.30.0.0
 no auto-summary

router eigrp 1
 auto-summary
 network 172.30.0.0
 no auto-summary
```

9 Testing the Pod

After all routers and virtual machines 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.

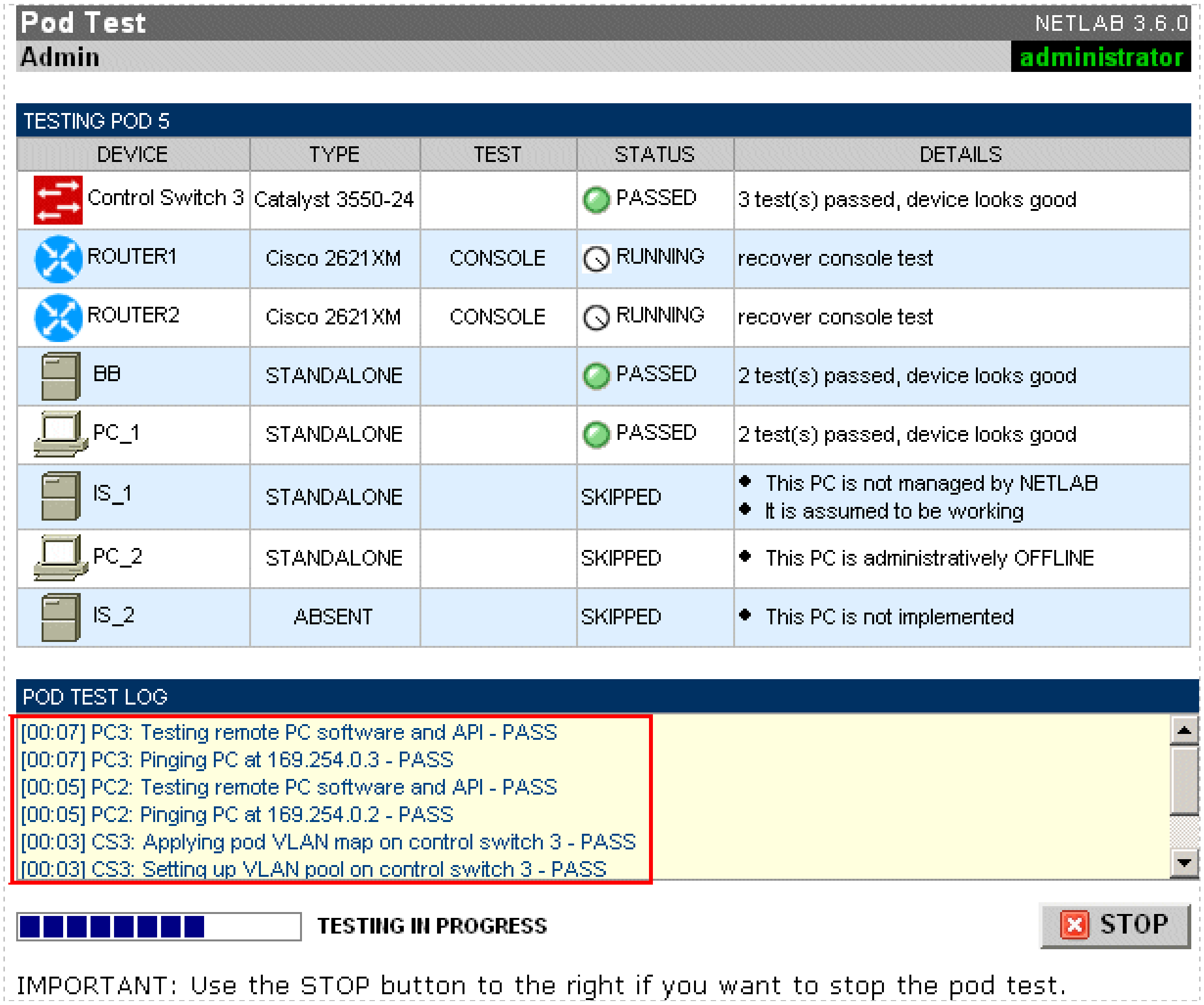


Pod 5 -- Management Options

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.

⇒ 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.



Pod Test NETLAB 3.6.0

Admin administrator

TESTING POD 5

DEVICE	TYPE	TEST	STATUS	DETAILS
Control Switch 3	Catalyst 3550-24		PASSED	3 test(s) passed, device looks good
ROUTER1	Cisco 2621XM	CONSOLE	RUNNING	recover console test
ROUTER2	Cisco 2621XM	CONSOLE	RUNNING	recover console test
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
PC_2	STANDALONE		SKIPPED	◆ This PC is administratively OFFLINE
IS_2	ABSENT		SKIPPED	◆ This PC is not implemented

POD TEST LOG

```
[00:07] PC3: Testing remote PC software and API - PASS
[00:07] PC3: Pinging PC at 169.254.0.3 - PASS
[00:05] PC2: Testing remote PC software and API - PASS
[00:05] PC2: Pinging PC at 169.254.0.2 - PASS
[00:03] CS3: Applying pod VLAN map on control switch 3 - PASS
[00:03] CS3: Setting up VLAN pool on control switch 3 - PASS
```

TESTING IN PROGRESS

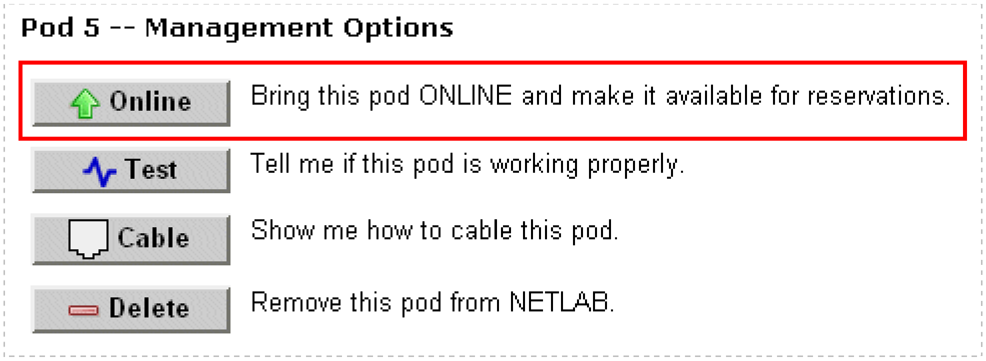
STOP

IMPORTANT: Use the STOP button to the right if you want to stop the pod test.

10 Finishing Up

10.1 Bring the Pod(s) Back Online

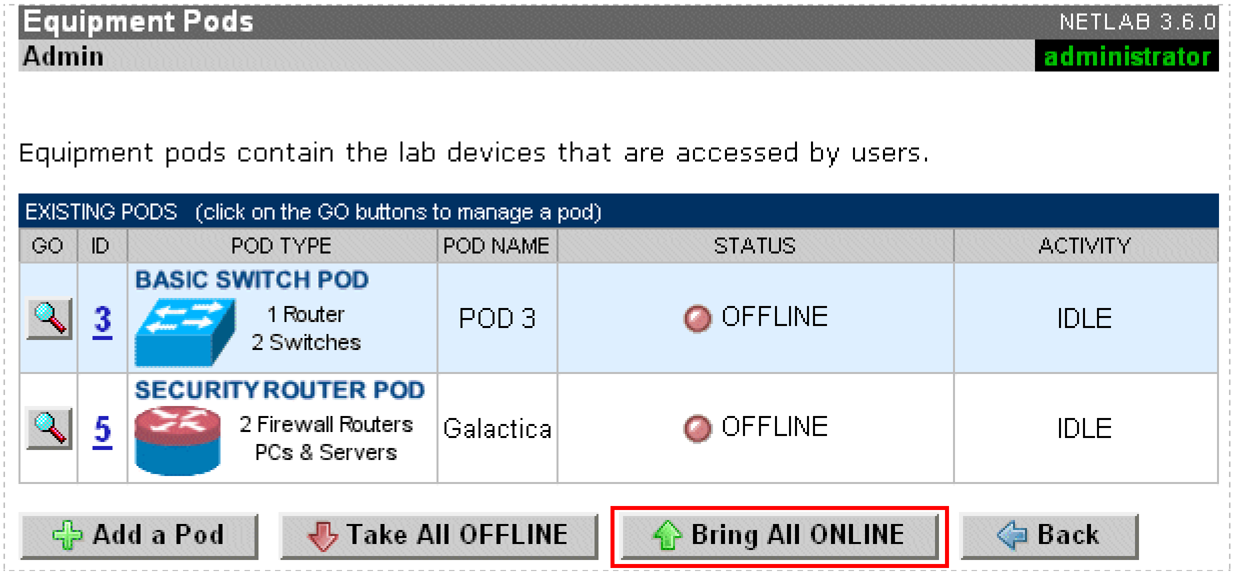
Now you can bring the pod online and make it available for lab reservations. You can bring just this pod online by clicking the Online button under Management Options.



Pod 5 -- 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.



Equipment Pods NETLAB 3.6.0

Admin administrator

Equipment pods contain the lab devices that are accessed by users.

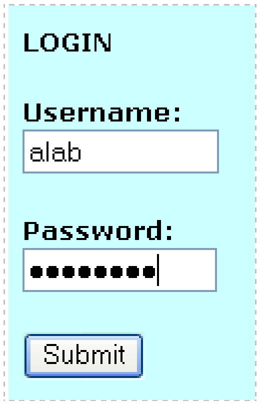
EXISTING PODS (click on the GO buttons to manage a pod)

GO	ID	POD TYPE	POD NAME	STATUS	ACTIVITY
	3	BASIC SWITCH POD 1 Router 2 Switches	POD 3	OFFLINE	IDLE
	5	SECURITY ROUTER POD 2 Firewall Routers PCs & Servers	Galactica	OFFLINE	IDLE

10.2 Enable Network Security Exercises

To make the Network Security pod and lab exercises available to classes and students, you must enable it in each 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.

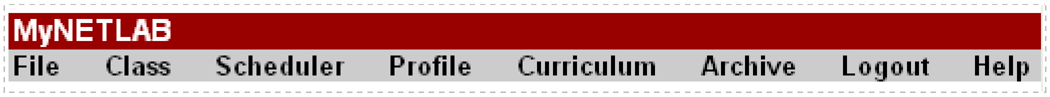


LOGIN

Username: alab

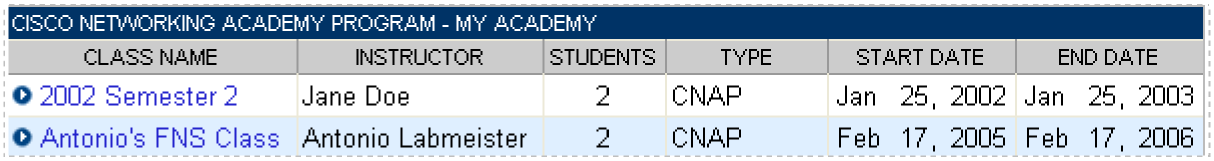
Password: ●●●●●●●●

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.

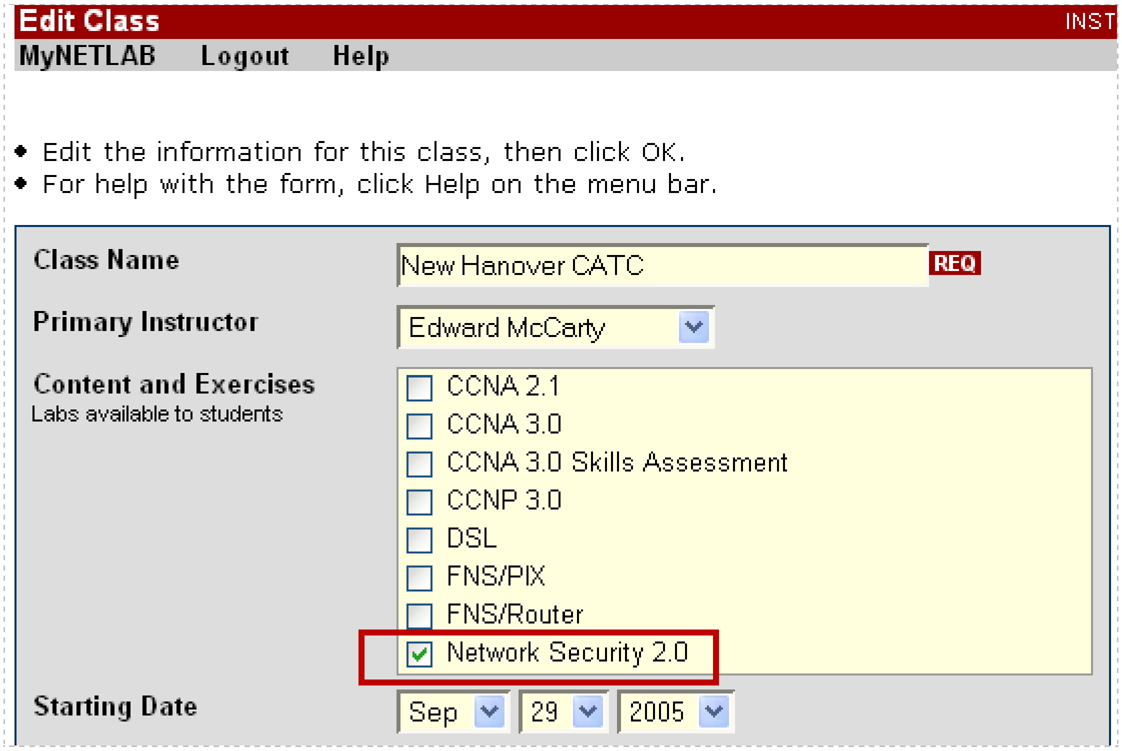
Select to add a new class or select an existing class from the class list by clicking on a class name.



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

Check the box for Network Security 2.0.



Edit Class INST

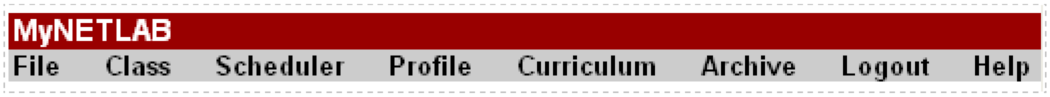
MyNETLAB Logout Help

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

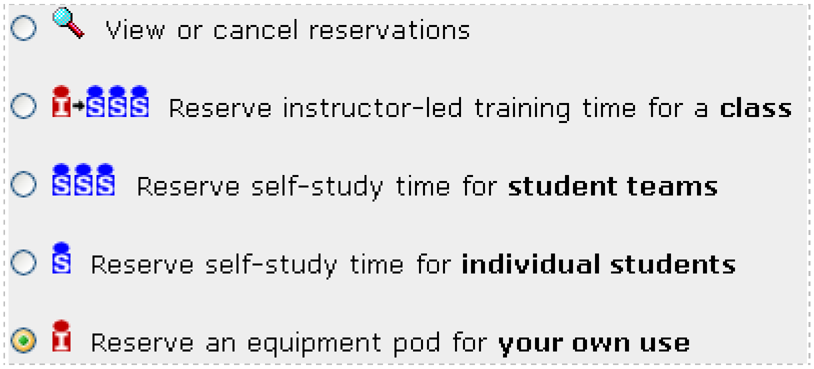
Class Name	New Hanover CATC REQ
Primary Instructor	Edward McCarty
Content and Exercises Labs available to students	□ CCNA 2.1 □ CCNA 3.0 □ CCNA 3.0 Skills Assessment □ CCNP 3.0 □ DSL □ FNS/PIX □ FNS/Router ☑ Network Security 2.0
Starting Date	Sep 29 2005

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**

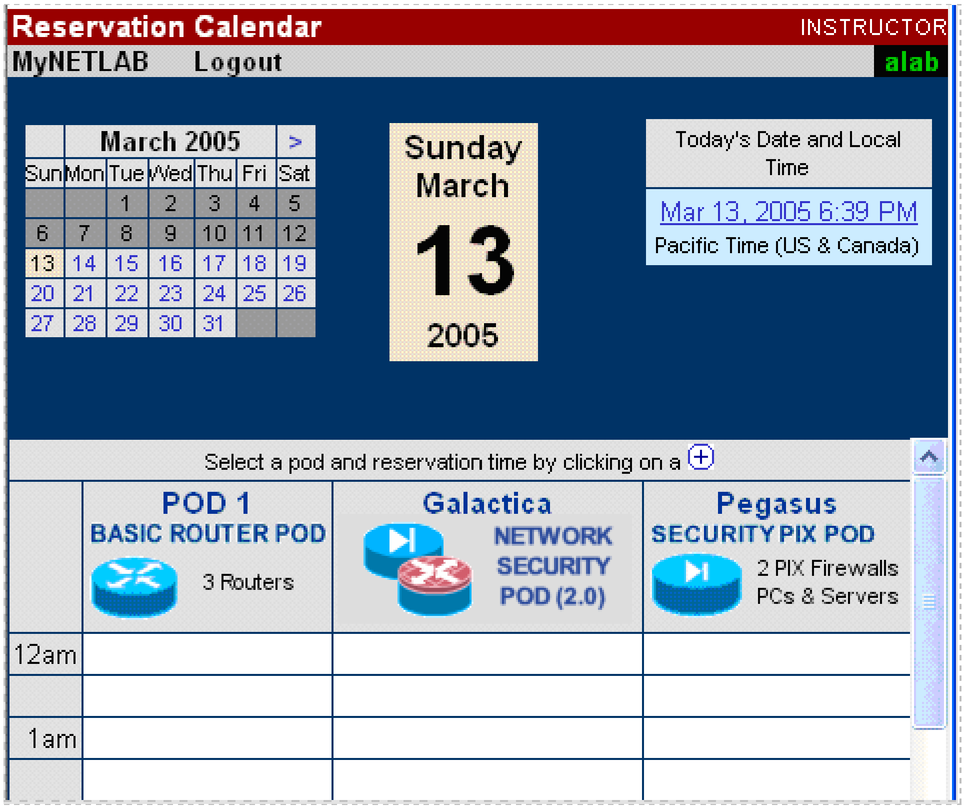
○ Reserve self-study time for **student teams**

○ 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		

Sunday March 13 2005

Today's Date and Local Time

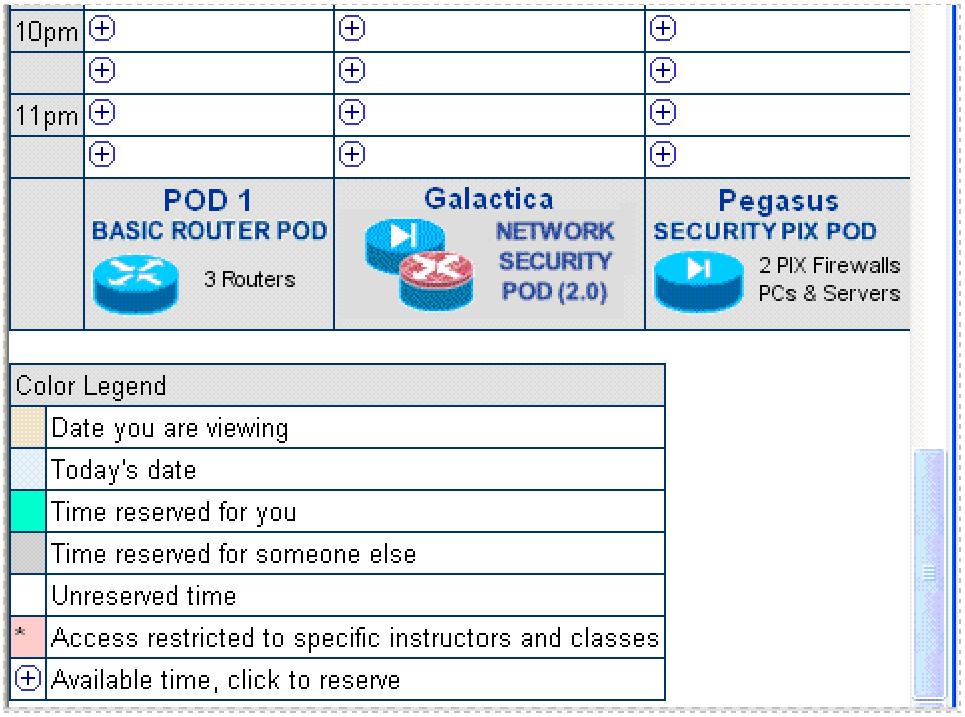
Mar 13, 2005 6:39 PM

Pacific Time (US & Canada)

Select a pod and reservation time by clicking on a ⊕

	POD 1 BASIC ROUTER POD 3 Routers	Galactica NETWORK SECURITY POD (2.0)	Pegasus SECURITY PIX POD 2 PIX Firewalls PCs & Servers
12am			
1am			

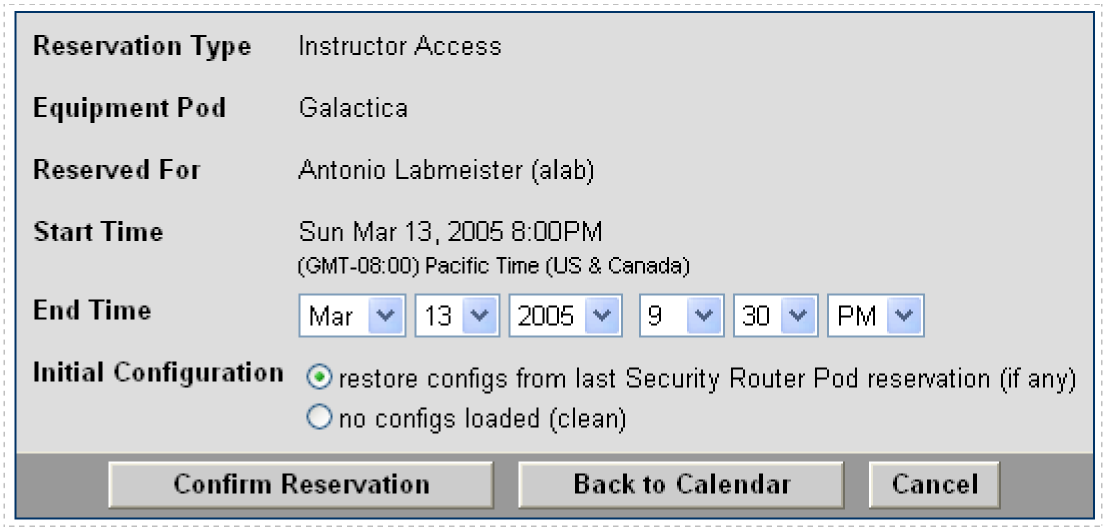
The reservation time area may be scrolled up and down. Scroll to the bottom to display the color legend.



10pm	⊕	⊕	⊕
	⊕	⊕	⊕
11pm	⊕	⊕	⊕
	⊕	⊕	⊕
	POD 1 BASIC ROUTER POD 3 Routers	Galactica NETWORK SECURITY POD (2.0)	Pegasus SECURITY PIX POD 2 PIX Firewalls PCs & Servers

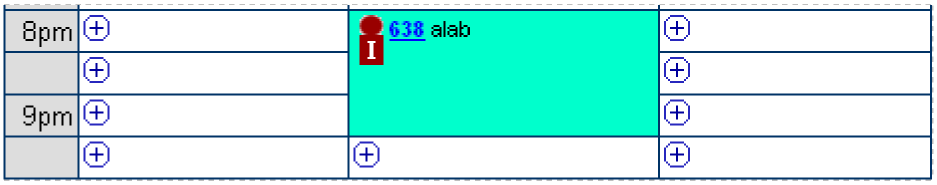
Color Legend	
▨	Date you are viewing
▨	Today's date
🟩	Time reserved for you
▨	Time reserved for someone else
□	Unreserved time
*	Access restricted to specific instructors and classes
⊕	Available time, click to reserve

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



Reservation Type	Instructor Access
Equipment Pod	Galactica
Reserved For	Antonio Labmeister (alab)
Start Time	Sun Mar 13, 2005 8:00PM (GMT-08:00) Pacific Time (US & Canada)
End Time	Mar 13 2005 9 30 PM
Initial Configuration	● restore configs from last Security Router 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 638 alab	⊕
	⊕		⊕
9pm	⊕		⊕
	⊕	⊕	⊕

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

11 Appendix A – Supported Network Security 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	Yes	The use of common network mapping tools, hacking programs, and scripts on a LAN and across a WAN.
Configure SSH	Yes	Configure SSH access.
Controlling TCP/IP Services	Yes	In this lab, students will complete the following objectives: • Begin the process of implementing a secure perimeter router • Explicitly deny common TCP/IP services • Verify TCP/IP services have been disabled
Configure Routing Authentication and Filtering	Yes	In this lab, students will demonstrate the use of authentication and filters to control route updates from peer routers.
General Router Security	Yes	Configure basic router security features.
Configure Basic Security using Security Device Manager	Caution*	Copy the SDM files to router Flash memory. *You must manually load SDM files in flash. NETLAB$_{AE}$ does not automatically manage SDM images.
Lock-and-Key ACLs	Yes	In this lab, students will configure a dynamic ACL for lock-and-key security.
Time-Based ACLs	Yes	Time-based ACLs allow administrators to control when users are permitted or denied access to network resources. Time-based ACLs can be applied to NAT, interfaces, lines, and virtually all other ACL scenarios. In this lab, students will control web access
Configure Cisco IOS Firewall CBAC on a Cisco Router	Yes	Context-based Access Control (CBAC).
Configure AAA on Cisco Router	Yes	In this exercise, students will protect the network access server (NAS), or pod router, by securing access using simple passwords without authentication, authorization, and accounting (AAA). Then students will configure the NAS to perform AAA authentication
Install and Configure CSACS 3.0 for Windows	Yes	Install CSACS on Windows.
Configure Authentication Proxy	Yes	In this lab, students will configure authentication proxy on a Cisco router.
Configure IOS Firewall IDS	Yes	The Intrusion Detection Systems provide a level of protection beyond the firewall by protecting the network from internal and external attacks and threats.
Configure Logging	Yes	In this lab, students will use logging to monitor network events.
Configure SNMP	Yes	Configure SNMP.

Setting Time and NTP	Yes	All Cisco routers provide an array of time-of-day services. These services allow the products to accurately keep track of the current time and date, to synchronize multiple products to the same time, and to provide time services to other systems.
Configuring Cisco IOS IPSec using Pre-Shared Keys	Yes	The XYZ Company has purchased Cisco routers and wants to create a secure VPN over the Internet between two sites. The company wants to configure a secure VPN gateway using IPSec between two Cisco routers to use pre-shared keys for authentication.
Configuring Cisco IOS IPSec with Pre-Shared Keys using SDM	Yes	In this lab, the student will learn the following objectives: Prepare to configure Virtual Private Network (VPN) Support, Configure VPN tunnel using SDM VPN Wizard, Modify IKE and IP Security (IPSec) configuration, Verify and test IPSec configuration
Configuring Cisco GRE IPSec Tunnel using SDM	Yes	In this lab, the student will learn the following objectives: Prepare to configure Virtual Private Network (VPN) Support, Configure GRE/IPSec tunnel using SDM VPN Wizard, Modify GRE/IPSec configuration, Verify and test GRE/IPSec configuration.
Configure IPSec using Digital Certificates	Yes*	The XYZ Company has purchased Cisco routers and wants to create a secure Virtual Private Network (VPN) over the Internet between two sites. The company wants to configure a secure VPN gateway using IPSec between two Cisco routers using a certificate authority. *A supported CA server must be loaded on Backbone Server or other PC.
Configure Remote Access Using Cisco Easy VPN	Yes	In this lab exercise, the team will configure a Cisco Easy VPN Server given a Cisco 2600 Series router, and a Cisco VPN Client 3.5 given a PC running Windows 2000. Upon completion of these configuration tasks, the group will test the connectivity between.
Configure Cisco Easy VPN Server with NAT	Yes	In this lab, students will use the Network Address Translation (NAT) and Port Address Translation (PAT) to hide internal addresses.