
# Security Router Pod

## Planning and Installation Guide

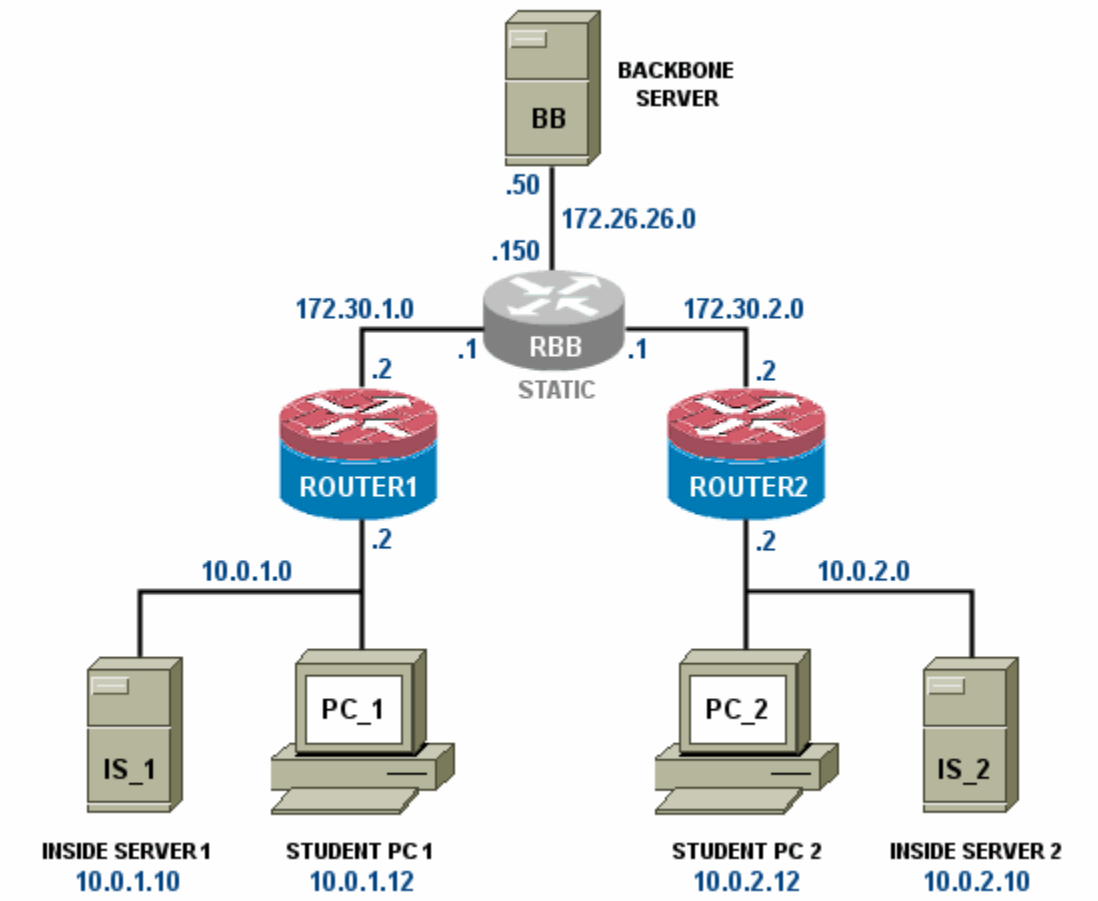
**For Cisco Networking Academy® FNSR Curriculum**

**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 Router Pod, used with *FNS: Router* (FNSR) labs.




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

The NETLAB$_{AE}$ Security Router Pod features direct access the console of ROUTER1 and ROUTER2. 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 FNSR 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 the 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 (ROUTER1, PC_1, and IS_1) to accomplish the lesson objective while using the right side of pod only for verification (i.e. pings, traces, VPN client, etc).

⇒ 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$_{AE}$.

## 1.4 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 are 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 Router Pod includes placeholders for 5 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.

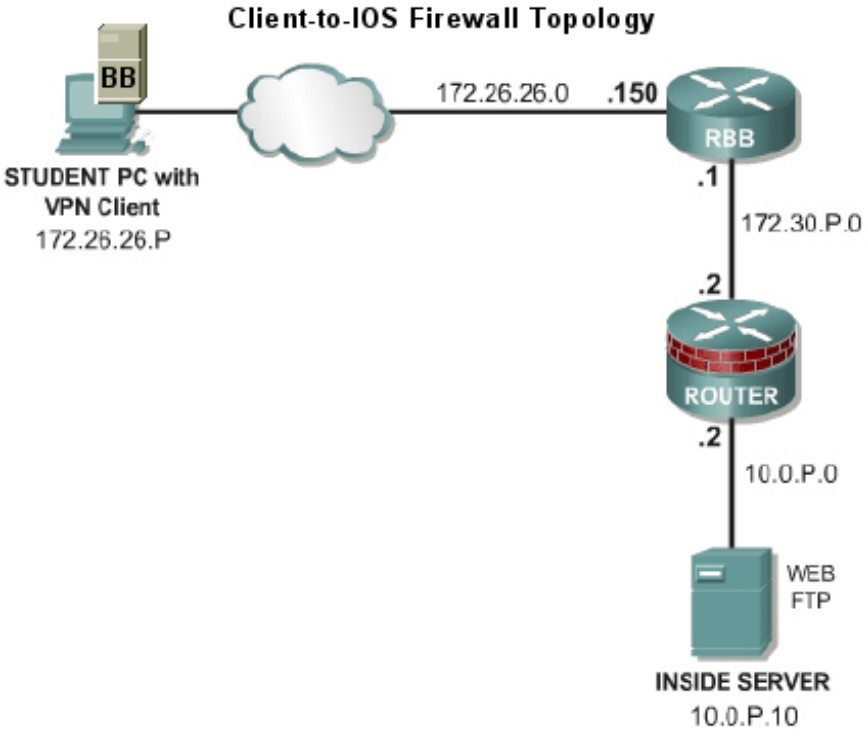
These options are fully explained in the *NETLAB+ Remote PC Guide*.

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

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

## 1.6 Client-to-IOS-Firewall Topology

The FNSR 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 ROUTER1 and ROUTER2

Both routers in the Security Router Pod have the same requirements.

| NETLAB$_{AE}$ Supported Devices | Ethernet Ports Required | IOS Release | Images (in order of preference) |
|---|---|---|---|
| 2611XM<br>2621XM<br>2651XM<br>2621[1] | 2 | 12.3(4)T Advanced IP Services<br><br>12.3(4)T Advanced Security | C266-advipservicesk9-mz.123.3-4.T6 (128/32)<br><br>C2600-advsecurityk9-mz.12.3-4.T6 (96/32) |

⇒ VPN Router bundles ship by default with 12.3(4)T or later. Do not go above the 12.3(7)T image, as the IOS Intrusion Detection commands have changed significantly in version 12.3(8)T. If the router has 12.3(8)T or later, the image must be downgraded.

⇒ Security Device Manager (SDM) version 1.2 or later will be required for labs in Modules 2 through 7. VPN router bundles ship by default with SDM.

[1] The 2621 model router will work for all labs excluding SDM labs once they have been upgraded from 16F/32DRAM to 16F/64DRAM.

## 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) A separate standalone RBB router for each Security Router Pod
- (2) Simulating 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 two 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.

FNSR 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 Router 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 Router Pod includes placeholders for 5 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.

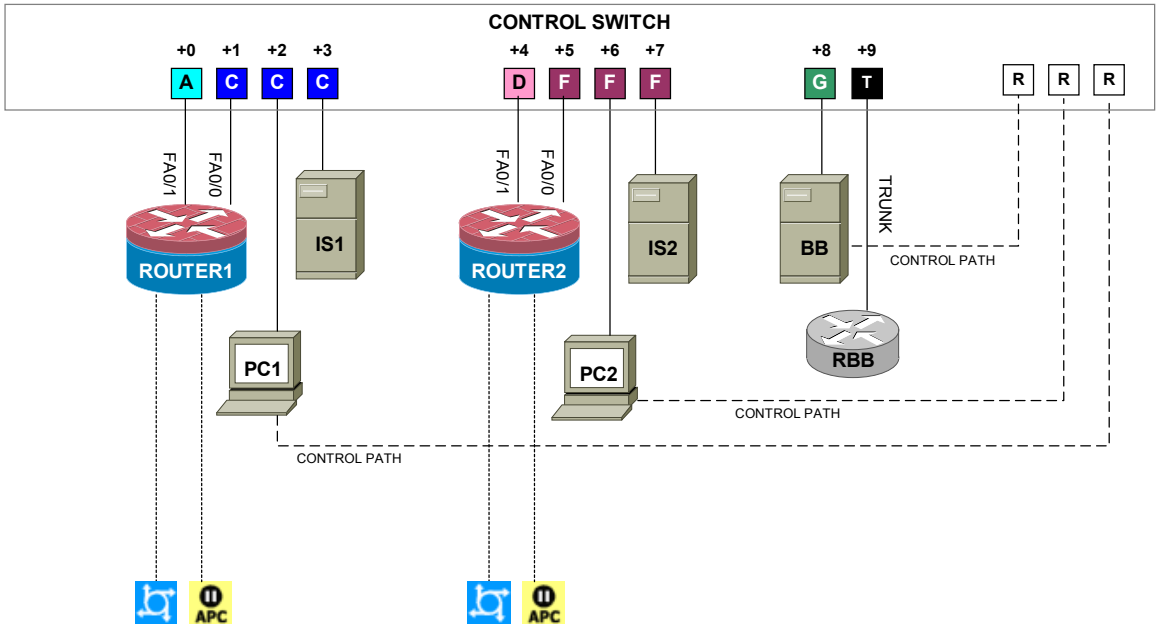
⇒ Management of control devices is covered in the *NETLAB+ Administrator Guide*.

The Security Router Pod requires the following control device resources:

| Control Device Resource | Quantity Required |
|---|---|
| Control Switch | 10 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 Router Pod.




⇒ The actual 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 Router Pod requires 10 consecutive ports on a supported control switch (other than a Catalyst 1900 series).

⇒ You cannot use a Catalyst 1900 series control switch because 802.lq trunking is not supported.

Ports are labeled +0 to +9 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 Router 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 +8. These VLANs are depicted as letters A, C, D, F, and G and represent a subnet in the topology (B and E are reserved for future DMZ segments and compatibility with the Security PIX Pod). 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 +9 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 PCs 2$^{nd}$ 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 Router Pod requires two access server ports. These ports provide console access to ROUTER1 and ROUTER2.

## 3.3 Switched Outlets


Switched outlets provide managed electrical power, allowing NETLAB$_{AE}$ and users to turn lab equipment on and off. The Security Router Pod requires a switched outlet for ROUTER1 and ROUTER2.

# PART 2 - IMPLEMENTATION

## 4 Pre-requisites

This section covers tasks that should be executed prior to adding a Security Router 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 Router Pod. Add control devices if necessary. Control device configuration is documented in the *NETLAB+ Administrator Guide.*

### 4.2 Upload IOS Images


Upload the IOS images for ROUTER1 and ROUTER2. NETLAB$_{AE}$ will recover these images on the router if they are erased from flash.

### 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 Router 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.

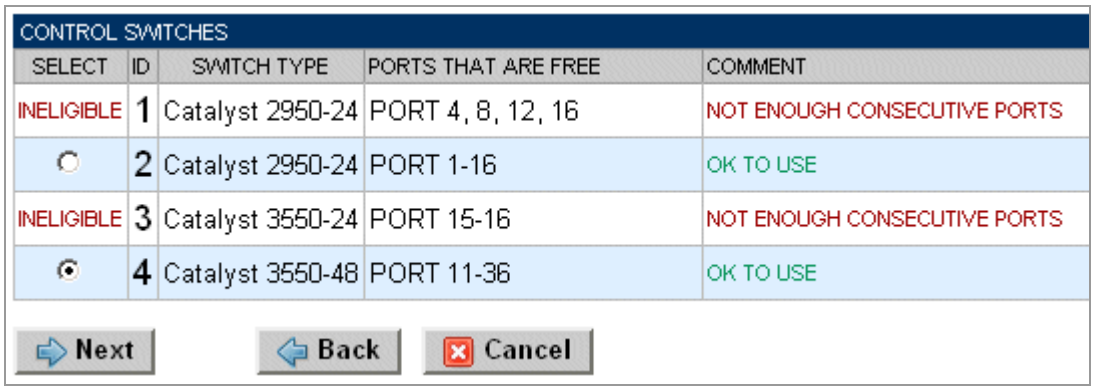
The New Pod Wizard will now help you add an equipment pod to your system.

## 5.2 Add a Security Router Pod

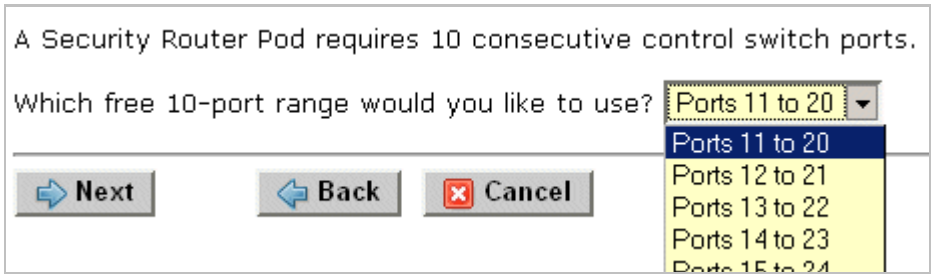

When prompted, select Security Router Pod.

## 5.3 Select Control Switch and Ports

A Security Router Pod requires 10 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.




Next, select the ports you want to use.



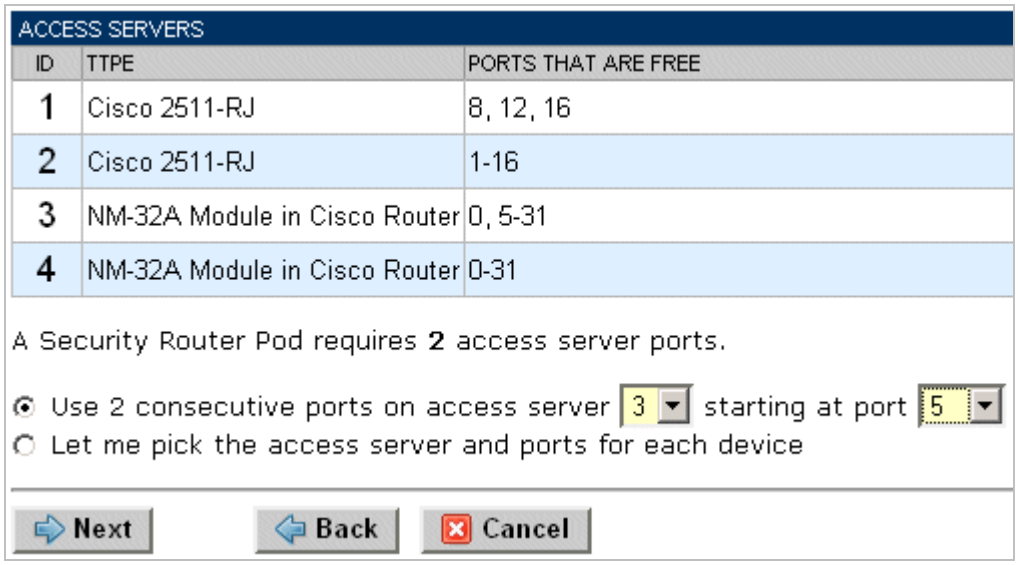

## 5.4 Select Access Server(s) and Ports

A Security Router Pod requires 2 access server ports.

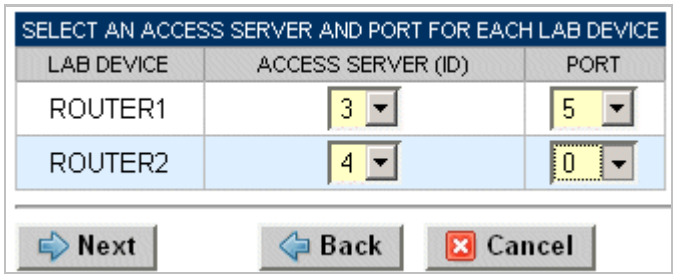
It is a good idea to use consecutive ports on one access server if possible. This practice will make it easier to cable and troubleshoot. If consecutive ports are not available, you can use non-consecutive ports, on different access servers if necessary.

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 router.



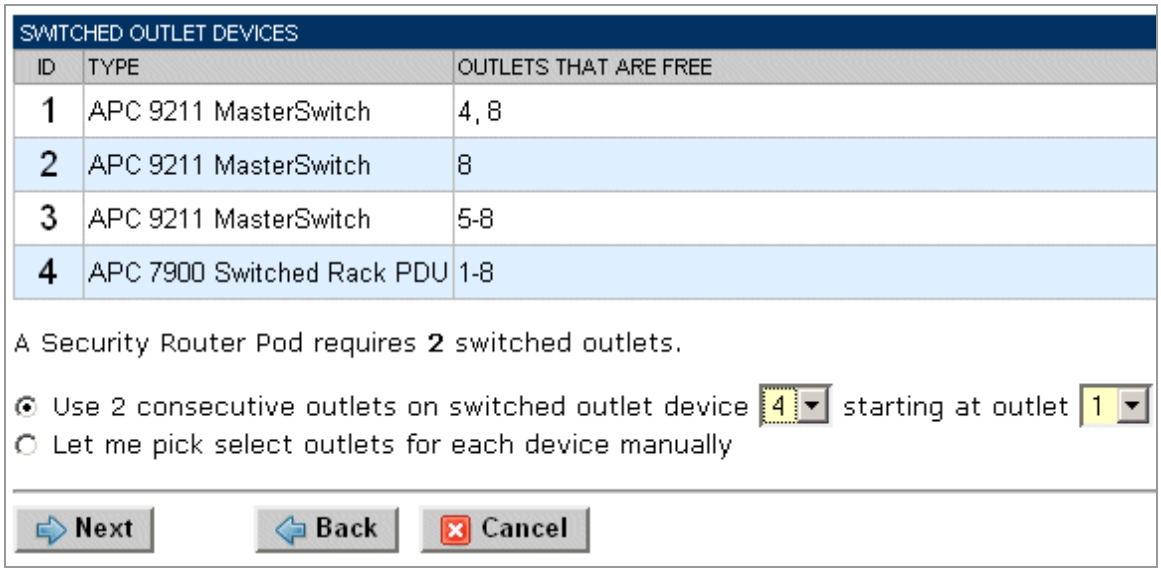

"Let me pick", allows you to make granular selections.



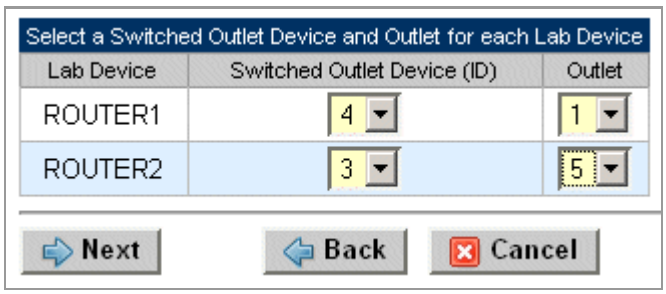

## 5.5 Select Switched Outlets

A Security Router 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.




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



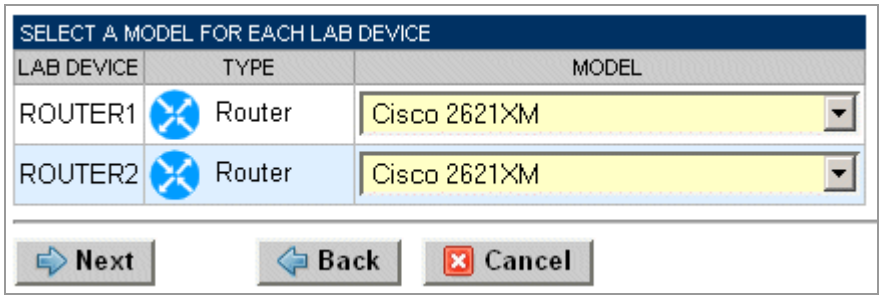
## 5.6 Select Router Types

Please specify a router model for ROUTER1 and ROUTER2. 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.

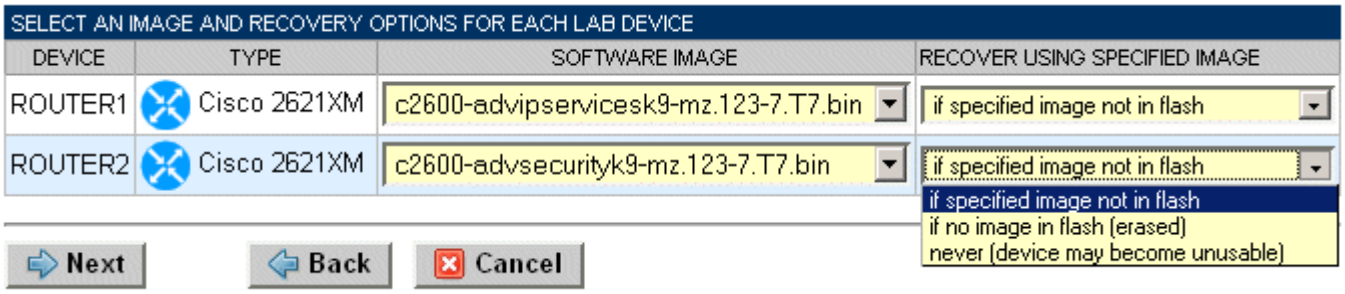
⇒ Improper selections may cause errors.

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



## 5.7 Select Software Images and Recovery Options

NETLAB$_{AE}$ scrubs ROUTER1 and ROUTER2 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.




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)

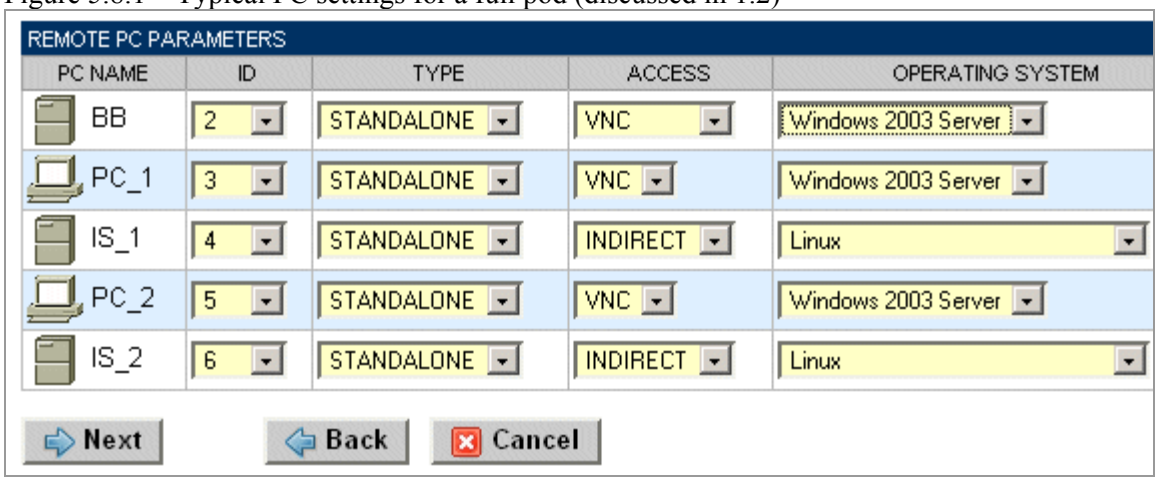
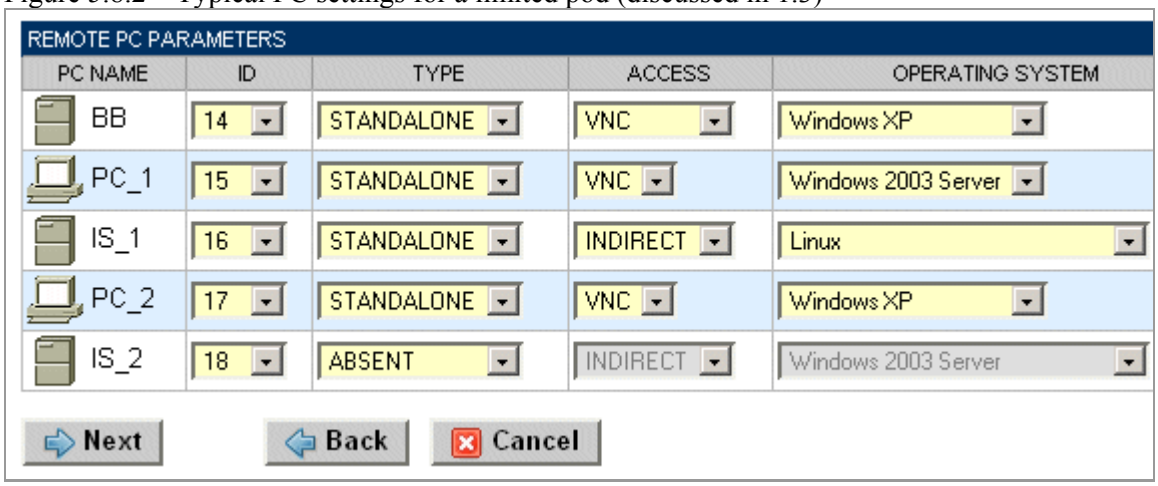



Figure 5.8.2 – Typical PC settings for a limited pod (discussed in 1.3)

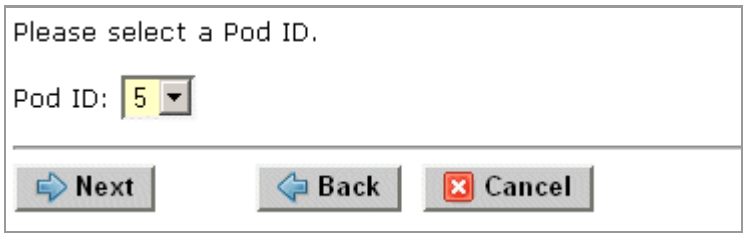



The following table describes the four most common settings as described in section 1.5:

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

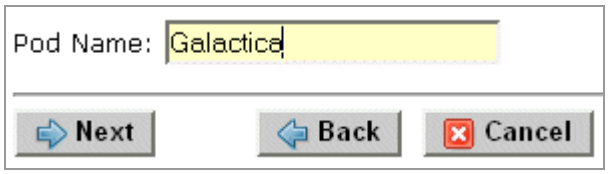
## 5.9 Select a Pod ID

Each pod is assigned a unique numeric ID.



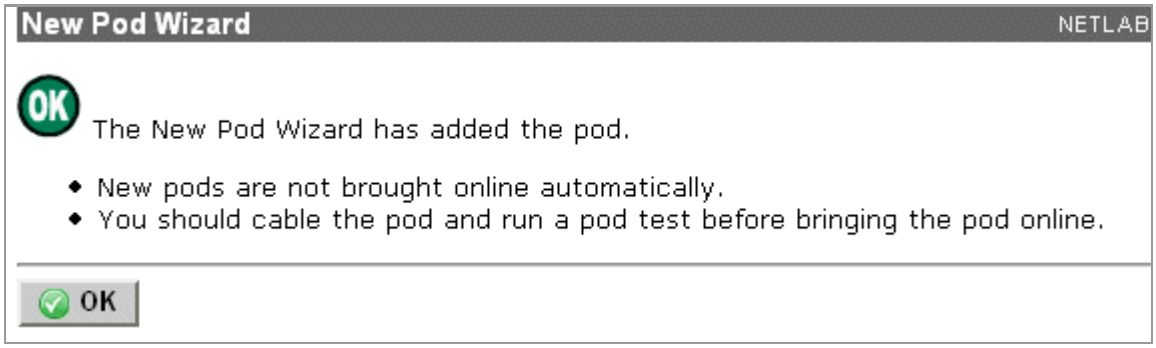

## 5.10 Select a Pod Name

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




## 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.




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.

| | | | | | |
|---|---|---|---|---|---|
|  | 5 | SECURITY ROUTER POD  2 Firewall Routers PCs & Servers | Galactica | OFFLINE | IDLE |

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

**Pod Management** NETLAB 3.6.0
**Admin** administrator

POD 5 - STATUS

| POD ID | POD NAME | STATUS | ACTIVITY | POD TYPE |
|---|---|---|---|---|
| 5 | Galactica | OFFLINE | IDLE | SECURITY ROUTER POD<br>2 Firewall Routers<br>PCs & Servers |

POD 5 - 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 2 PORT 1 | SOD 3 OUTLET 1 | c2600-advipservicesk9-mz.123-7.T7.bin |
| | ROUTER2 | Cisco 2621XM | AS 2 PORT 2 | SOD 3 OUTLET 2 | c2600-advipservicesk9-mz.123-7.T7.bin |

POD 5 - PCs AND SERVERS (click the GO buttons to reconfigure)

| GO | NAME | PC ID | TYPE | ACCESS | CONTROL IP | OPERATING SYSTEM |
|---|---|---|---|---|---|---|
| | BB | 2 | STANDALONE | VNC | 169.254.0.2 | Windows XP |
| | PC_1 | 3 | STANDALONE | VNC | 169.254.0.3 | Windows 2003 Server |
| | IS_1 | 4 | STANDALONE | INDIRECT | | Linux |
| | PC_2 | 5 | STANDALONE | VNC | 169.254.0.5 | Windows 2003 Server |
| | IS_2 | 6 | STANDALONE | INDIRECT | | Linux |

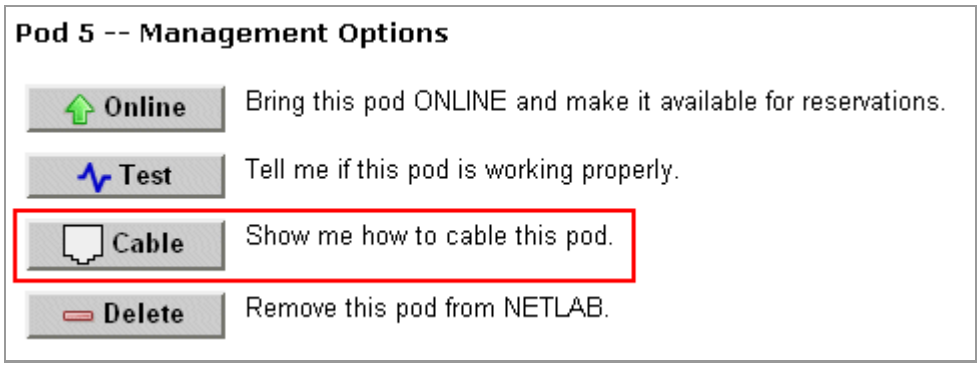
POD 5 - CONTROL SWITCH (click on the GO button to reconfigure control switch parameters)

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

# 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.




**Cable Chart** NETLAB 3.6.0
**Admin** administrator

The cable chart describes the connections for each lab device in the pod. Connections between control devices are not depicted - please refer to the Administrator Guide for guidance.

CABLE CHART FOR POD 5

**ROUTER1** (Cisco 2621XM)

| CONNECT FROM | USING CABLE | CONNECT TO | |
|---|---|---|---|
| FastEthernet0/0<br>10.0.1.2 (inside interface) | Ethernet CAT-5 Straight Through | C/S 3 | Port 2 |
| FastEthernet0/1<br>172.30.1.2 (outside interface) | Ethernet CAT-5 Straight Through | C/S 3 | Port 1 |
| Console | Console Cable | A/S 2 | Port 1 |
| Power | Power Cord | SOD 3 | Outlet 1 |

**ROUTER2** (Cisco 2621XM)

| CONNECT FROM | USING CABLE | CONNECT TO | |
|---|---|---|---|
| FastEthernet0/0<br>10.0.2.2 (inside interface) | Ethernet CAT-5 Straight Through | C/S 3 | Port 6 |

# 7 Configuring PCs

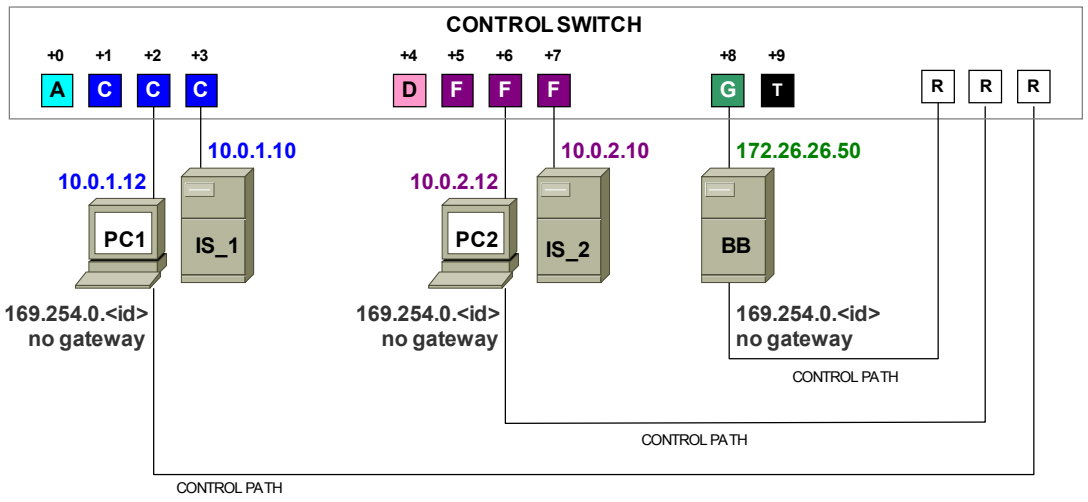
This section describes the basic tasks required to setup your PCs. Detailed guidance, such as securing the operating system and restoring the PC to a clean state is covered in the *NETLAB+ Remote PC Guide*.

**Caution: Connect your PCs and servers to 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

**Standalone/Direct** 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 |

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

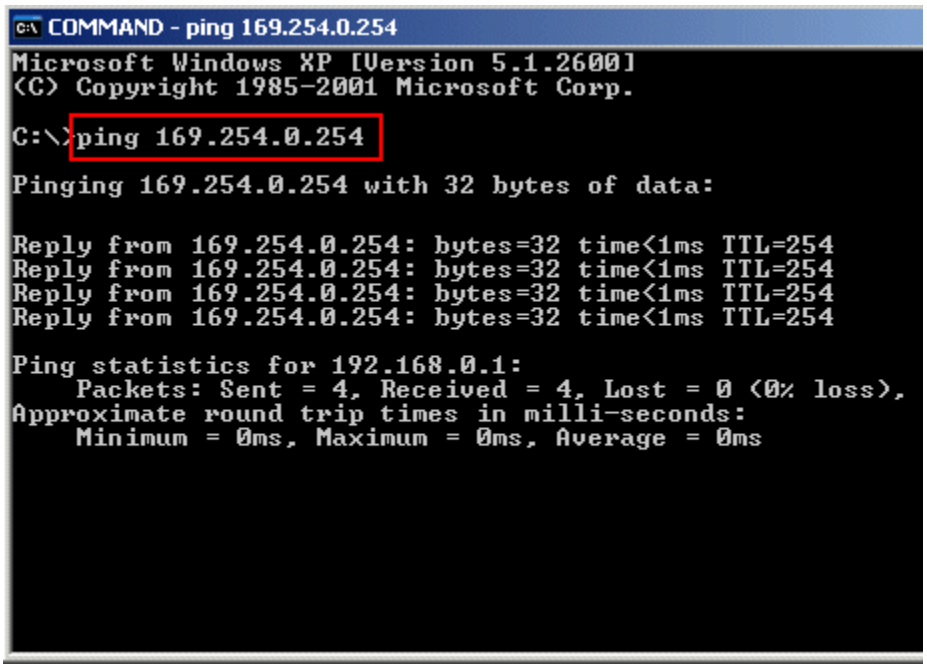
| GO | NAME | PC ID | STATUS | TYPE | ACCESS | CONTROL IP | OPERATING SYSTEM |
|---|---|---|---|---|---|---|---|
| | BB | 2 | ONLINE | STANDALONE | VNC | 169.254.0.2 | Windows XP |
| | PC_1 | 3 | ONLINE | STANDALONE | VNC | 169.254.0.3 | Windows XP |
| | IS_1 | 4 | n/a | STANDALONE | INDIRECT | | Linux |
| | PC_2 | 5 | ONLINE | STANDALONE | VNC | 169.254.0.5 | Windows XP |
| | IS_2 | 6 | OFFLINE | ABSENT | | | |

## 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.




## 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.

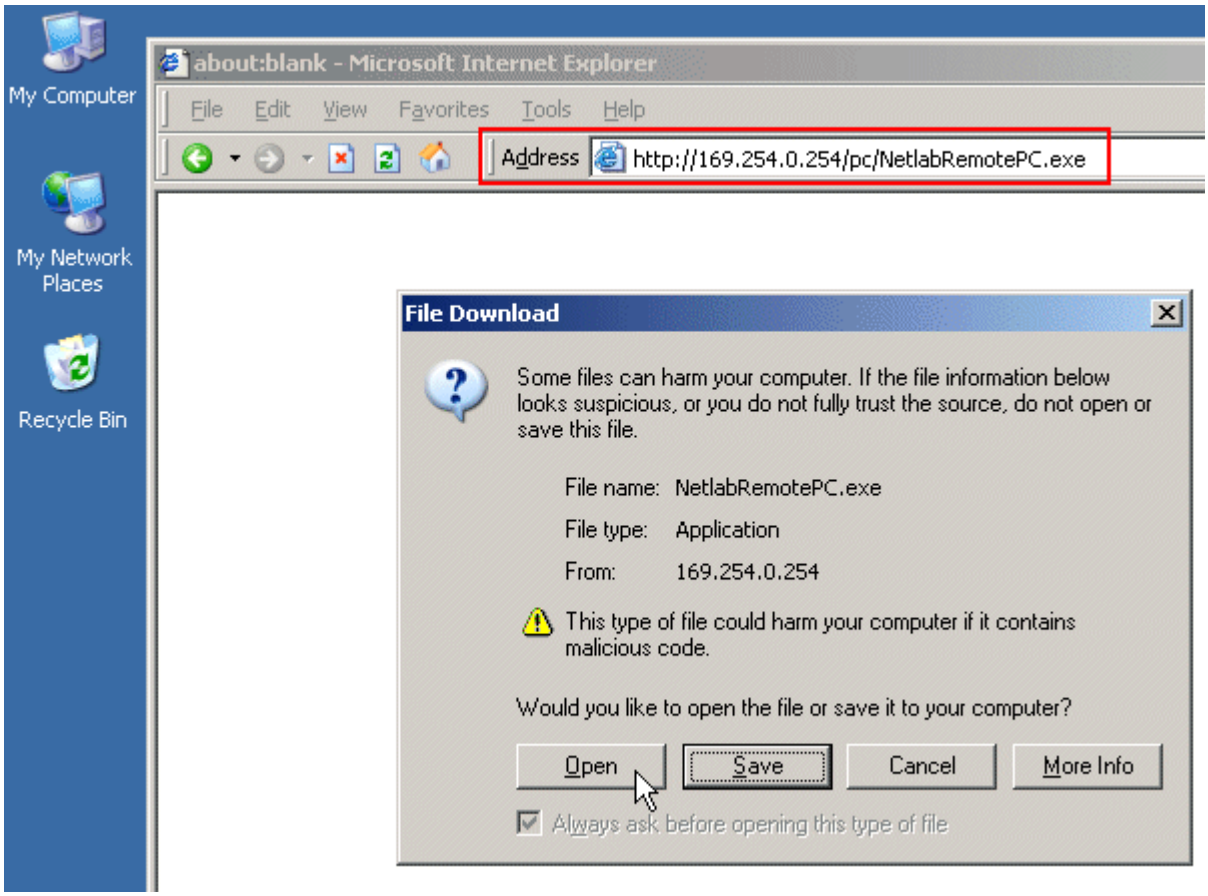
⇒ This software is only installed on direct access PCs (PC_1, PC_2 and BB). It should not be installed on IS_1, IS_2 or the users' PCs.

1) Open a web browser on the remote PC.

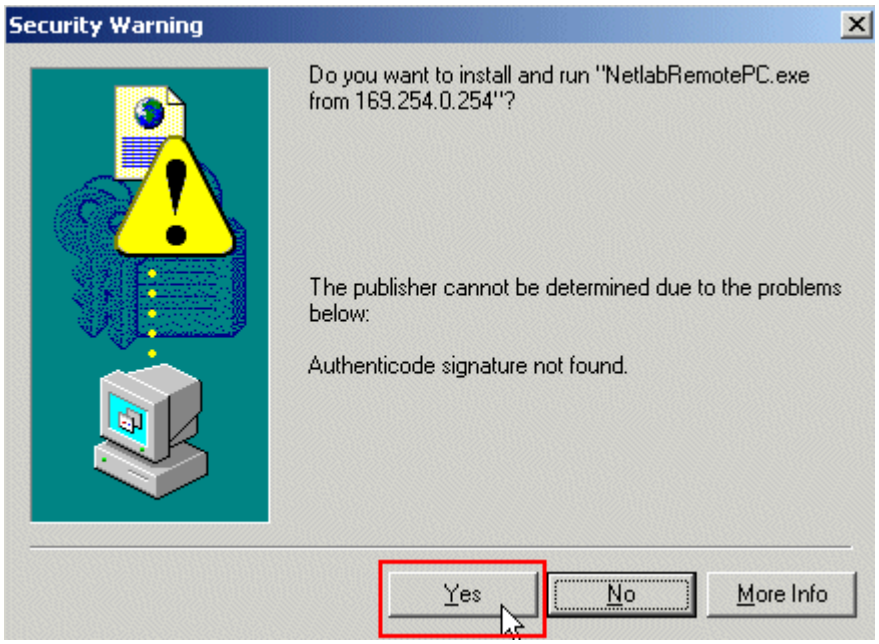
2) Enter the case-sensitive URL exactly as shown:

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

3) Click Open to install the package.




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



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 FNSR 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.

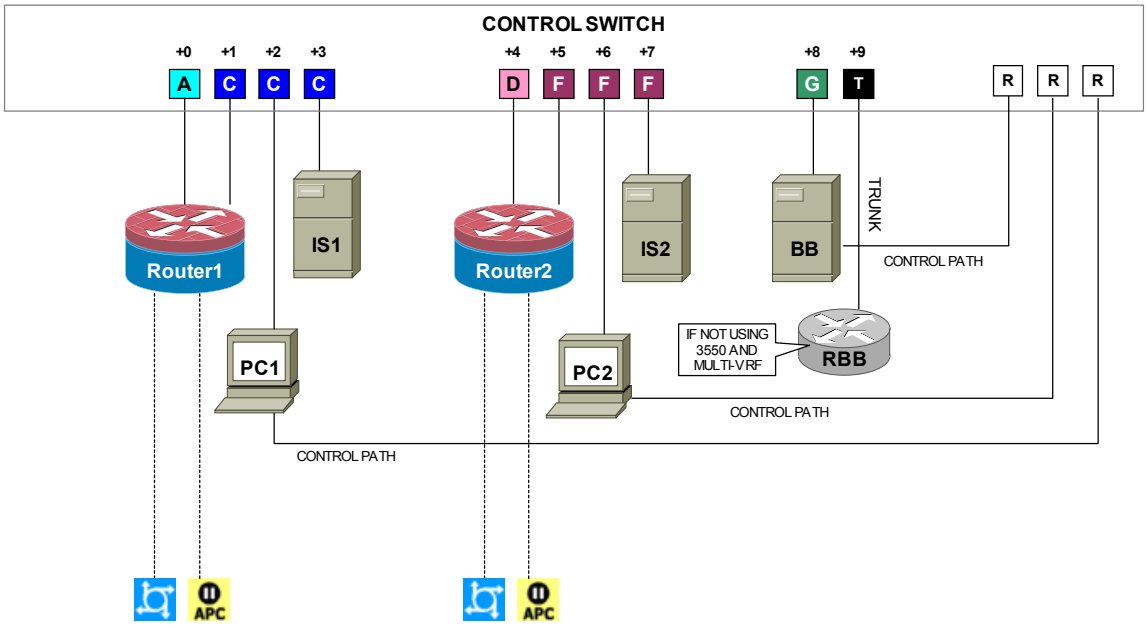
# 8 Configuring RBB


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.).

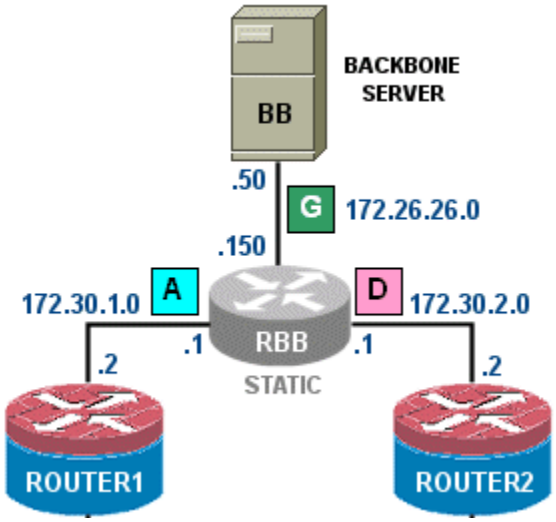
1
You can implement RBB in one of two ways:

- (1) Deploy a separate standalone RBB router for each Security Router 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 Router 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 Router Pod, RBB performs routing between network A, D, and G. RBB advertises routes to its peers using both EIGRP and RIP version 2. EIGRP is used in most of the FNSR labs. RIPv2 is used in the Route Authentication and Filtering lab.




## 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 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 | |

In this example, pod 5 uses VLANs 140-146. The base VLAN is 140.

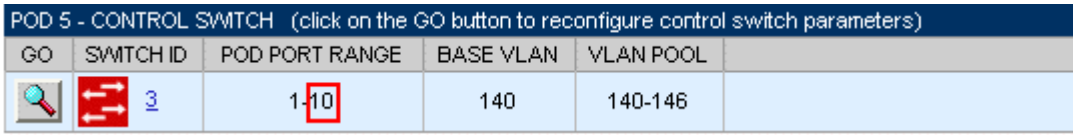
Now compute the actual VLANs by adding the base VLAN to the offset values listed below for each network. Record your results for future reference.

| Network | Offset (add to base VLAN) | Actual VLAN | Example |
|---|---|---|---|
| A | **+ 0** | = _____ | 140 + 0 = 140 |
| D | **+ 3** | = _____ | 140 + 3 = 143 |
| G | **+ 6** | = _____ | 140 + 6 = 146 |

## 8.2 Option 1 - Separate RBB for Each Security Router Pod

The most basic way to provide RBB routing is to 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 pod (base port + 9).



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 | |

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 140,143,146
 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 FastEthernet0/0.140
 description to ROUTER1 segment
 encapsulation dot1q 140
 ip address 172.30.1.1 255.255.255.0
 ip rip authentication mode md5
 ip rip authentication key-chain RTRAUTH
 no shutdown

interface FastEthernet0/0.143
 description to ROUTER2 segment
 encapsulation dot1q 143
 ip address 172.30.2.1 255.255.255.0
 ip rip authentication mode md5
 ip rip authentication key-chain RTRAUTH
 no shutdown

interface FastEthernet0/0.146
 description to BB segment
 encapsulation dot1q 146
 ip address 172.26.26.150 255.255.255.0
 no shutdown

! routing protocol for most labs
router eigrp 1
 network 172.26.0.0
 network 172.30.0.0
 no auto-summary

! routing protocol for rip / authentication lab
router rip
 version 2
 network 172.26.0.0
 network 172.30.0.0
```

## 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.

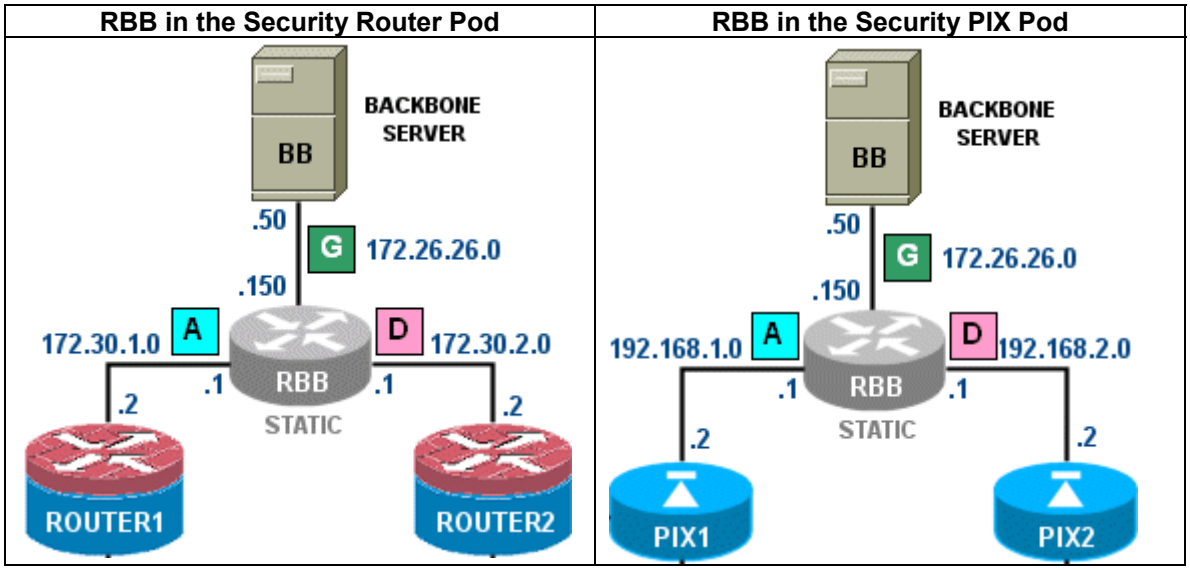
The router and IOS must support both 802.1q trunking and Mutli-VRF CE. Cisco's Feature Navigator can help with this task. FNSR labs use EIGRP. EIGRP support for Multi-VRF CE is very recent and can be found in some IOS 12.3 releases.

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.

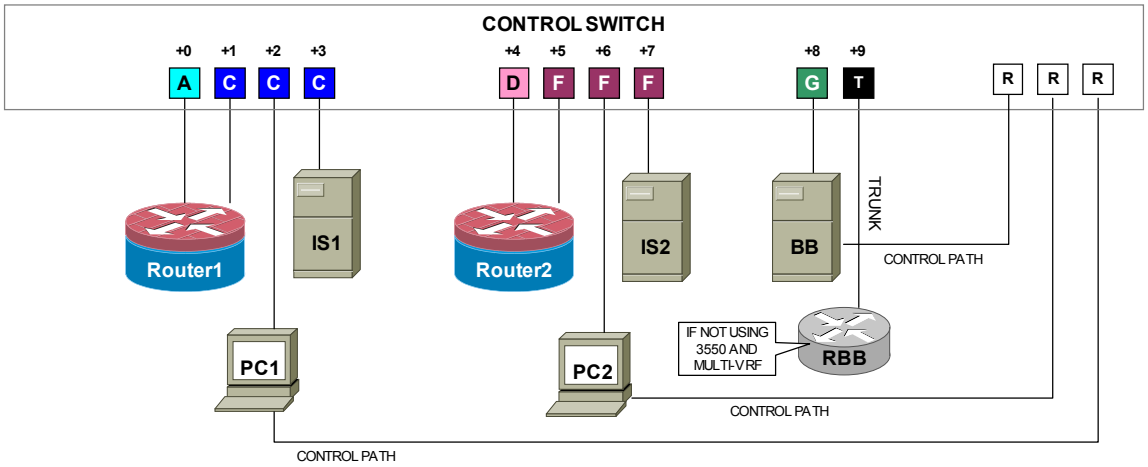



Similar to section 8.2, we determine that the BASE VLAN for POD_5 and POD_6 is 140 and 150 respectively. We compute the VLANs for network A, D, and G by adding the base VLAN for each pod to the offsets shown below.

***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)

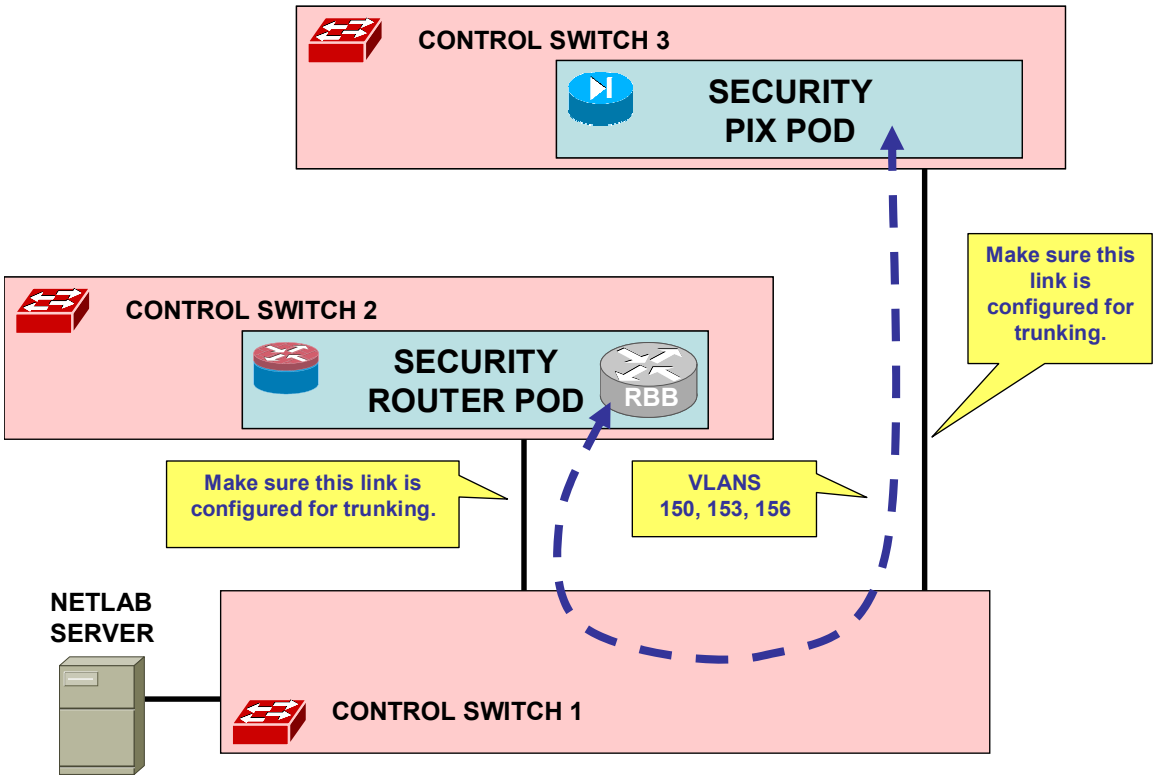
| GO | SWITCH ID | POD PORT RANGE | BASE VLAN | VLAN POOL | |
|---|---|---|---|---|---|
| | 3 | 1-10 | 140 | 140-146 | |

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.




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.**

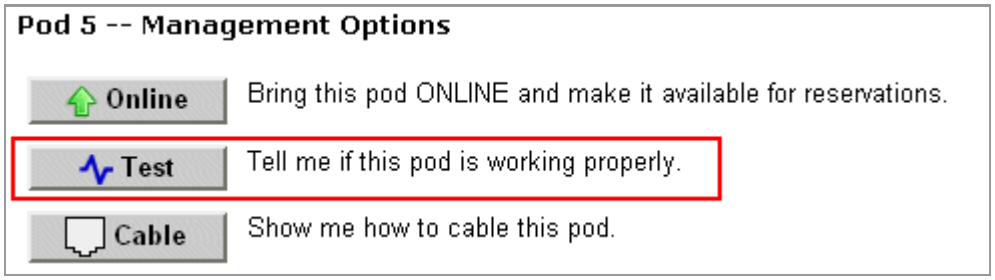
Exit configuration mode and **save** the configuration.

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
```

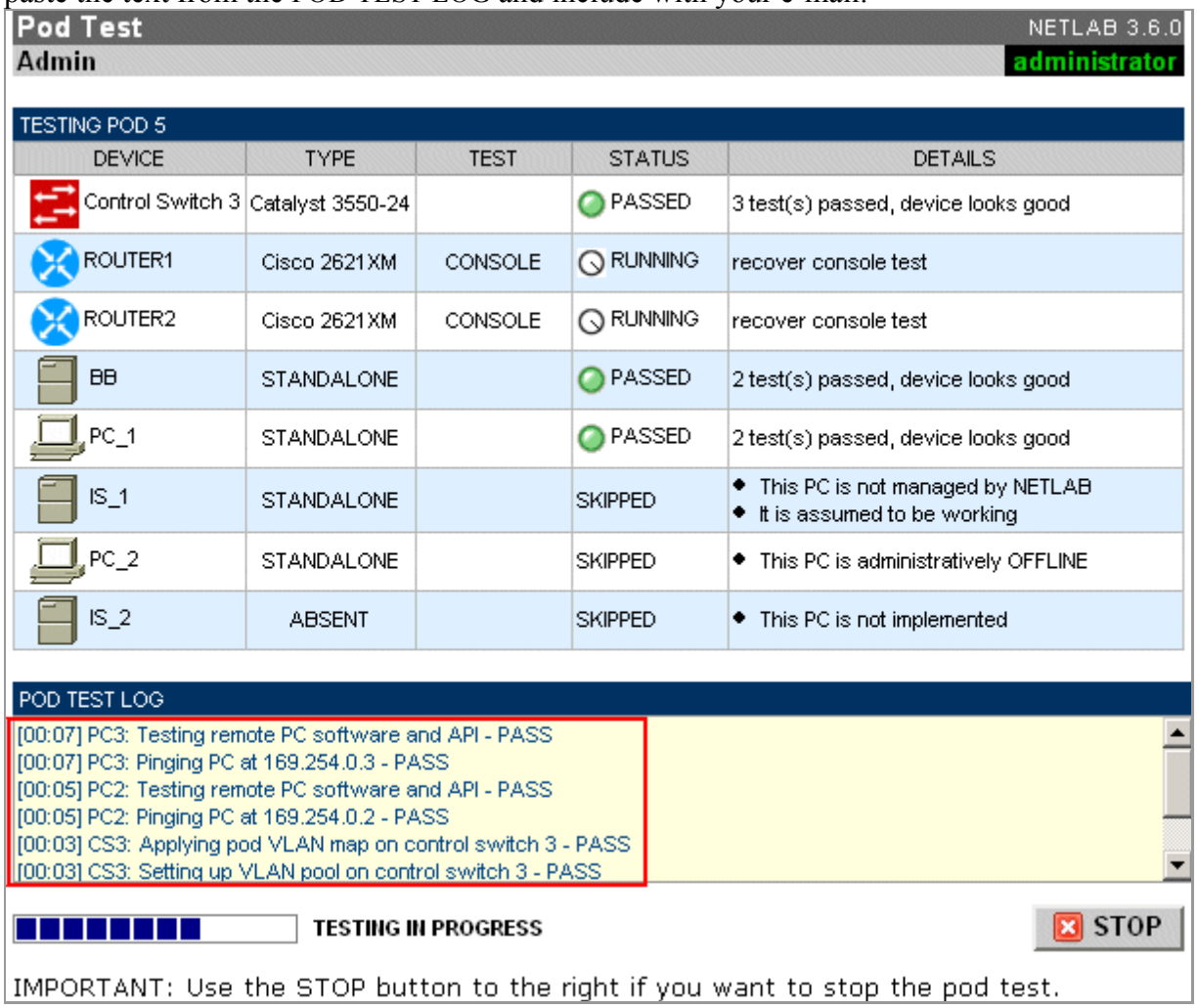
# 9 Testing the Pod

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.




⇒ 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.

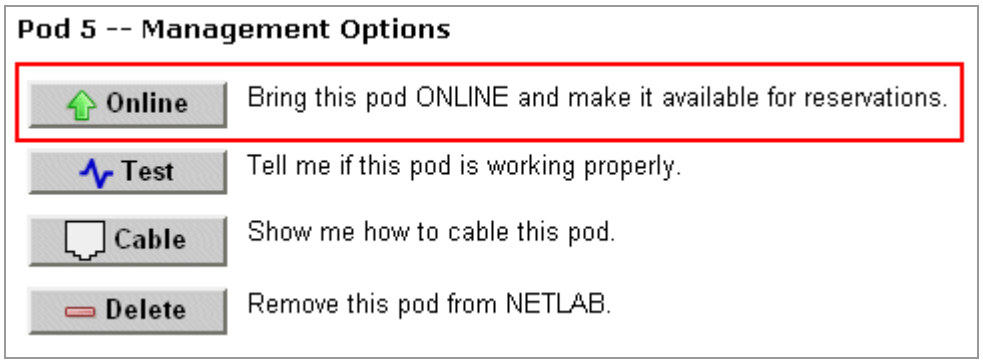
If you cannot resolve an issue and decide to contact technical support, please cut and paste the text from the POD TEST LOG and include with your e-mail.



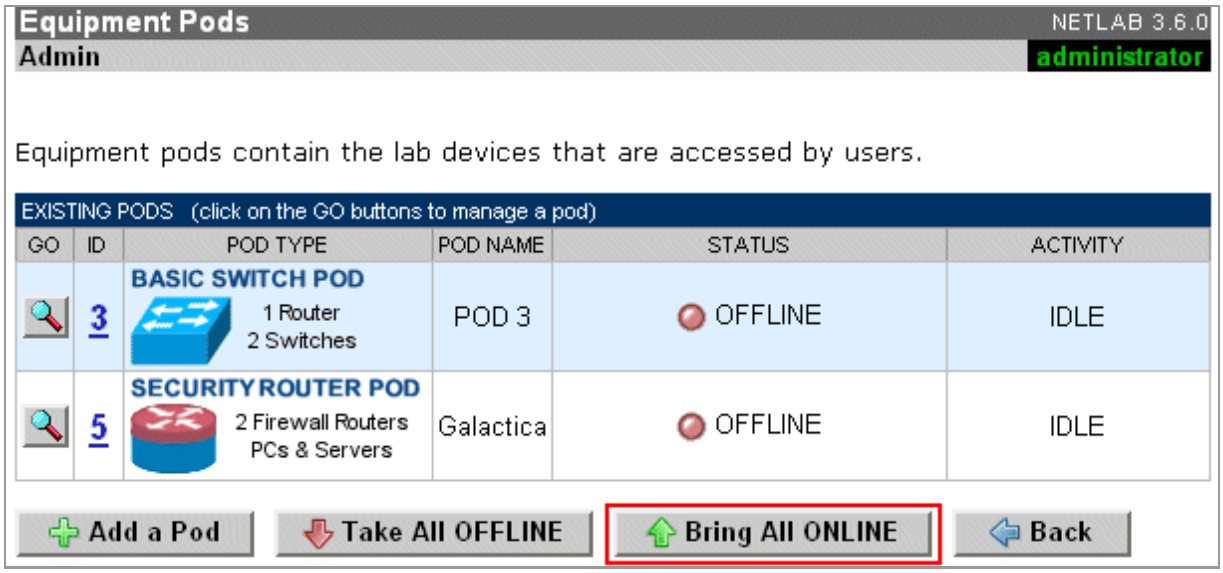
# 10 Finishing Up

## 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.



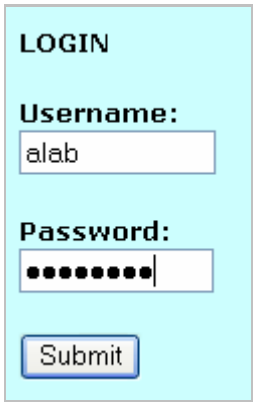

Alternatively, you can click Bring All ONLINE on the Equipment Pods page. Choose this option when you have no more additions or modifications to pods or control devices and you wish to put all pods into service.



## 10.2 Enable Security Router Pod and FNSR Exercises

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

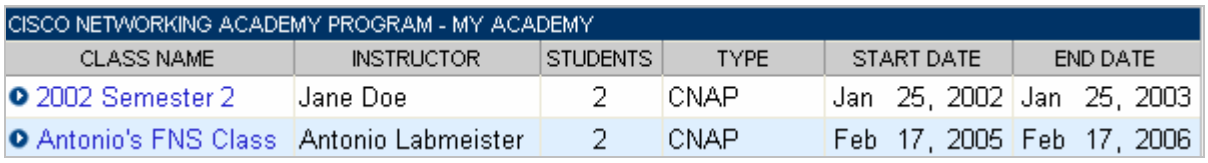
To add or edit class information, log into NETLAB$_{AE}$ using your instructor account. See the Instructor Accounts section of the *NETLAB+ Administrator Guide* for details.




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.

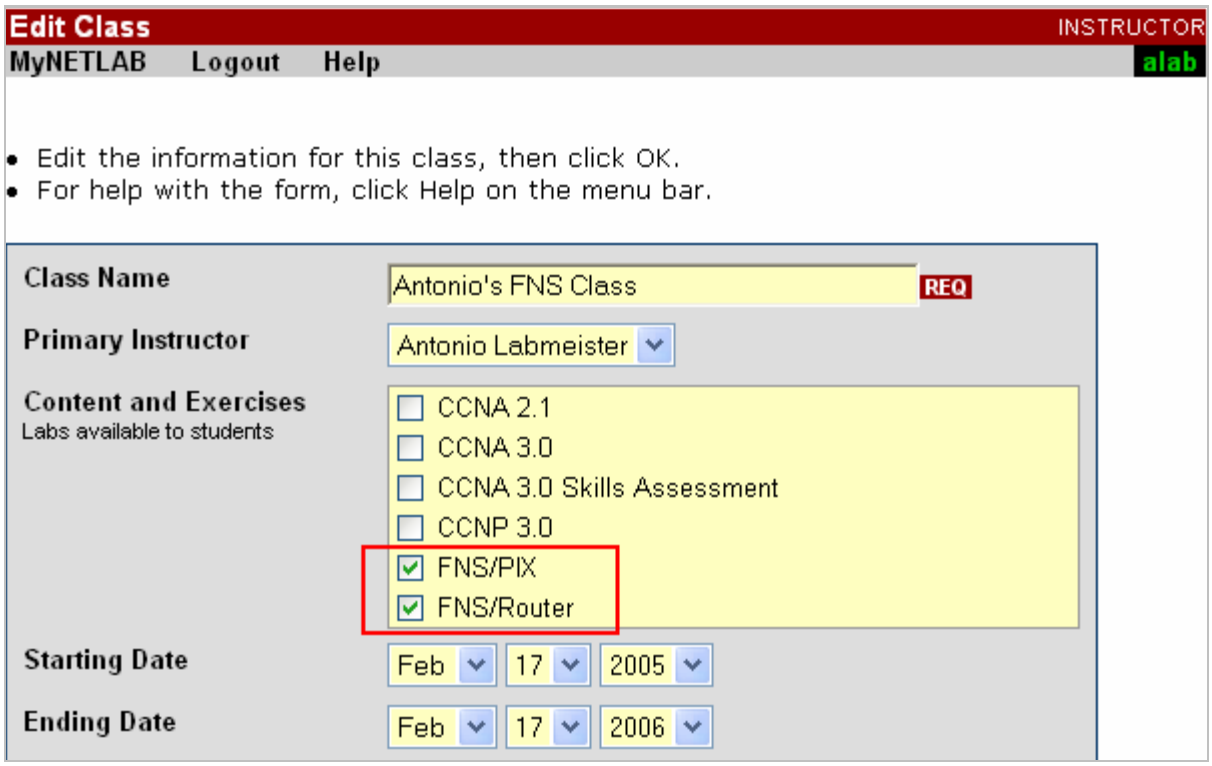

Select to add a new class or select an existing class from the class list by clicking on a class name.



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 |

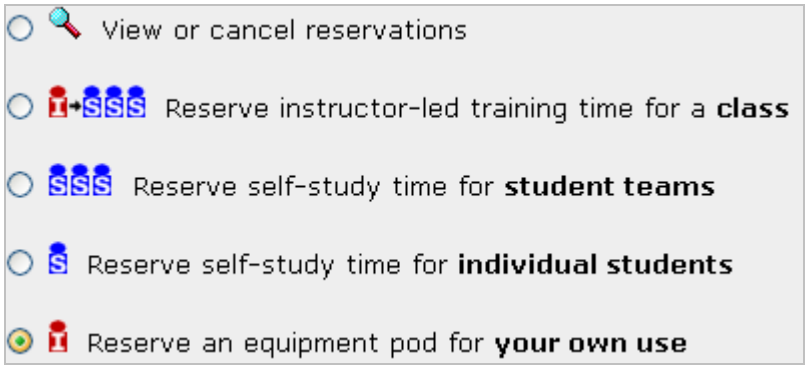
⇒ You may now enable more than one set of content. Previous NETLAB$_{AE}$ versions only allowed one content selection.



## 10.3 Schedule a Lab Reservation for Your New Pod.

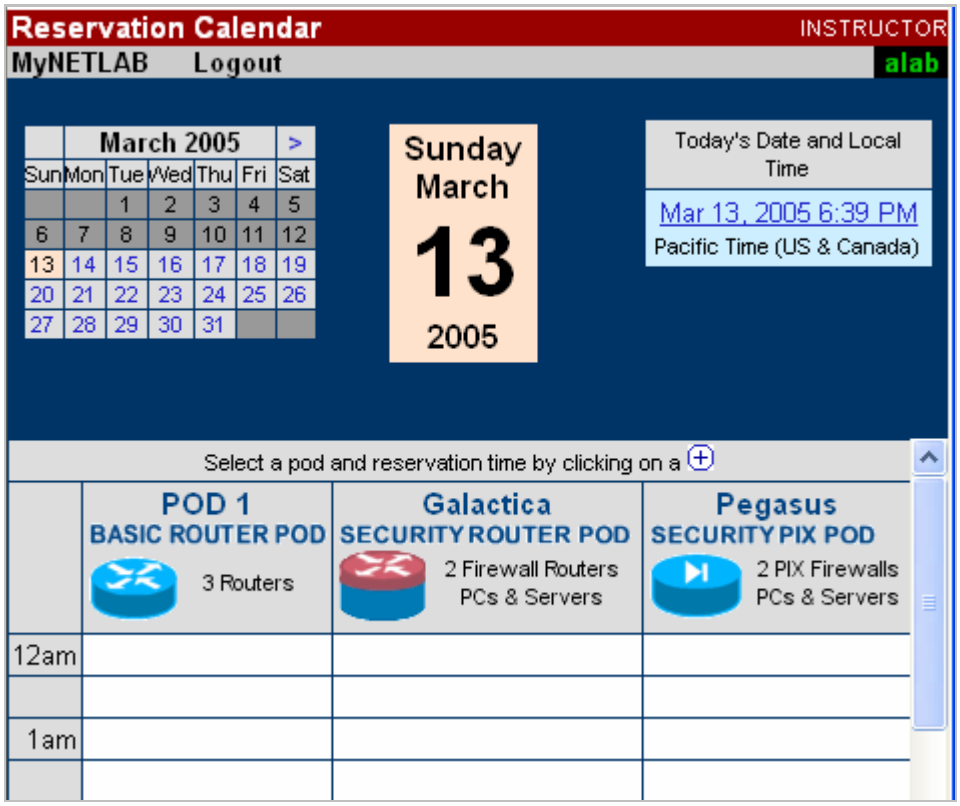
To schedule a lab reservation, select **Scheduler** from the menu bar or the link on the body of the MyNETLAB page.


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.

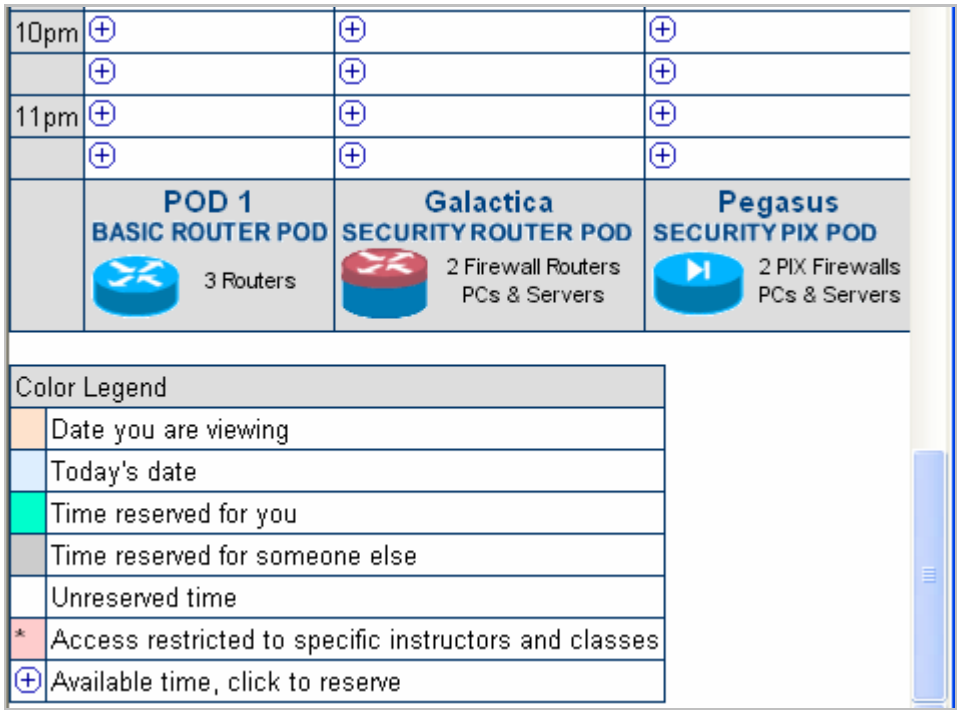



Select **OK** to proceed to the reservation calendar.

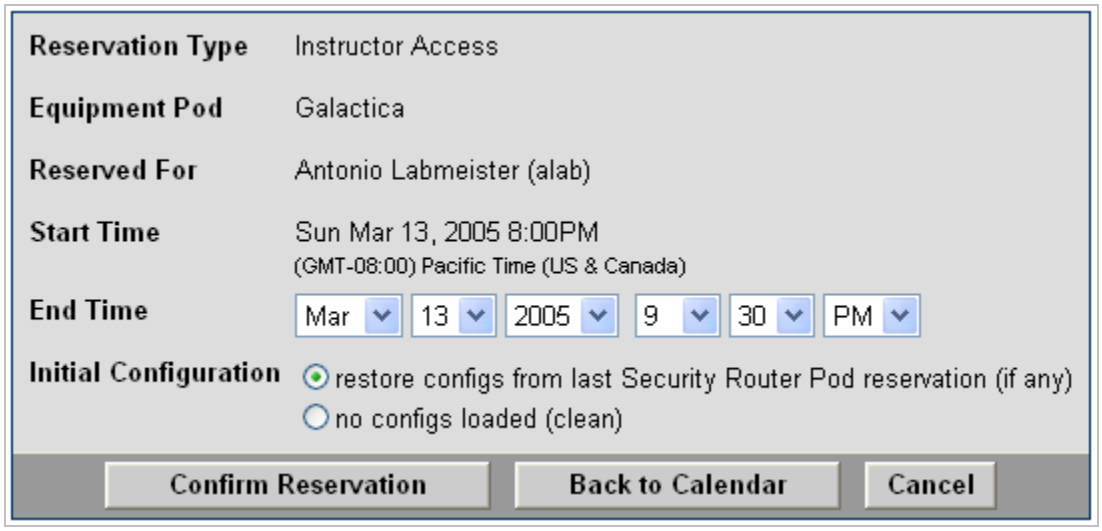
**Please Note: The selection of pods depicted may be different from the pods available at your site**.




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




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




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.


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

# 11 Appendix A - FNSR 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.. |
| 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 | Caution* | Install CSACS on Windows. *Requires Window's administrator access and overwrite of CSACS. Only recommended for Direct/VMware PCs. |
| 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 | Caution* | Configure SNMP. *We recommend that you preload Trap Watcher to avoid administrative access by users. |
| 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. Depending on the CA product used, you might have to run Windows 2000 or Windows 2003 server to support this exercise. |
| 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. *BB must be configured for direct access to support this lab. |
| 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. |