



LAN Switching Pod

Planning and Installation Guide

For Cisco Networking Academy® CCNA Exploration and Discovery Curriculum

Document Version: **2008-10-29**

Copyright © 2008, Network Development Group, Inc.

www.netdevgroup.com

Network Development Group grants permission for Cisco Networking Academies to make copies and distribute this document to Academy students and instructors, provided that the document content is not modified.

NETLAB Academy Edition and NETLAB+ are registered trademarks of Network Development Group, Inc.

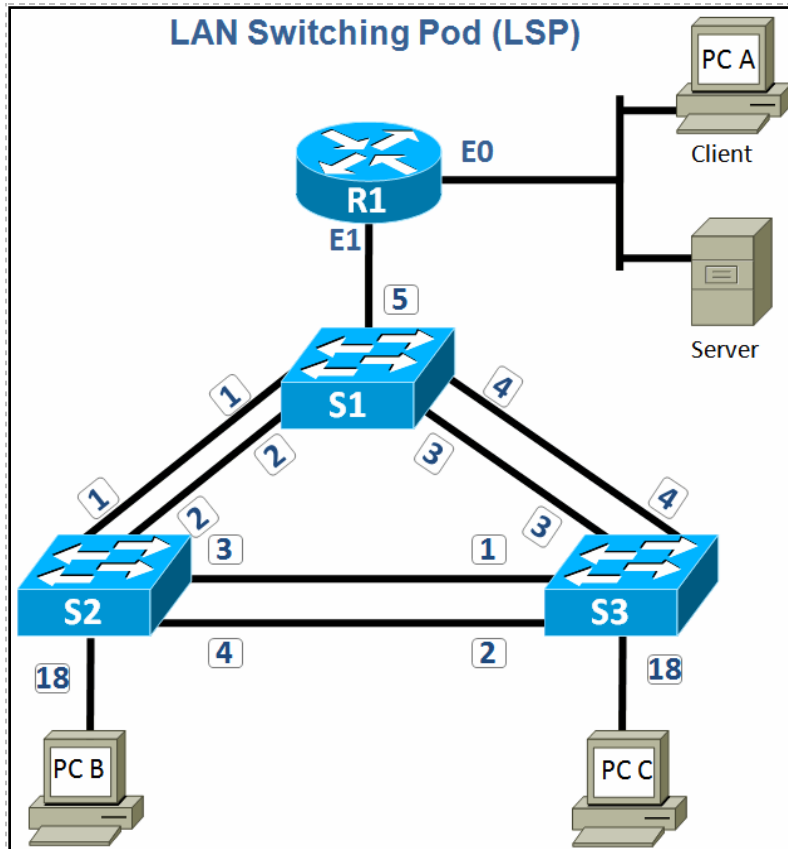
Cisco, IOS, Cisco IOS, Networking Academy, CCNA, CCNP, and PIX are registered trademarks of Cisco Systems, Inc.

1	Introduction.....	3
1.1	Deviations.....	4
1.2	Remote PC Support.....	4
1.3	Dynamic Topologies	4
2	Lab Device Requirements.....	5
2.1	Switches S1, S2 and S3.....	5
2.2	Router R1	5
2.3	PCs and Servers.....	6
3	Control Device Requirements.....	7
3.1	Control Switch Overview.....	7
3.2	Access Server Ports	9
3.3	Switched Outlets	9
4	Pre-requisites.....	10
4.1	Understanding VMware Server and Virtual Machines	10
4.2	Setup Control Devices.....	10
4.3	Upload IOS Images	10
4.4	Disable User Logins (optional)	10
5	Adding the Pod	11
5.1	Start the New Pod Wizard.....	11
5.2	Add a LAN Switching Pod.....	11
5.3	Select Control Switch and Ports.....	11
5.4	Select Access Server(s) and Ports	12
5.5	Select Switched Outlets.....	13
5.6	Select Device Types	14
5.7	Select Software Images and Recovery Options	15
5.8	Select PC Options.....	16
5.9	VMware Settings.....	17
5.10	Select a Pod ID	17
5.11	Select a Pod Name.....	17
5.12	Verify Your Settings.....	18
6	Cable the Pod	20
7	Configuring VMware and Virtual Machines	22
7.1	Connecting Virtual Machines to the Pod	22
7.2	VMware Virtual Switches and VLANs	23
7.3	Configure VMware Server Inside Port.....	25
7.4	Create Virtual Switches (VMnet).....	26
7.5	Binding Virtual Machines to Virtual Switches (VMnet)	27
7.6	Configuring the Control Switch for VMware	28
7.7	VMware Server(s) on Different Control Switch.....	29
8	Switch Configuration Tasks.....	31
8.1	Verify Control Switch IOS Version.....	31
8.2	Configure Control Switch Ports	31
8.3	Initial Lab Switch Setup.....	33
9	Testing the Pod	35
10	Finishing Up.....	36
10.1	Bring the Pod(s) Back Online.....	36
10.2	Enable LAN Switching Pod Exercises	37
10.3	Schedule a Lab Reservation for Your New Pod.....	38
Appendix A	Installing Discovery Server on a VMware Server	41

PART 1 – PLANNING

1 Introduction

The NETLAB_{AE} LAN Switching Pod is a versatile 3-switch, 1-router pod that supports many CCNA Exploration and Discovery lab exercises.



You may have up to eight (8) LAN Switching Pods per NETLAB_{AE} system.

The LAN Switching Pod features direct access to switch and router consoles. Integration with a separate VMware Server supports up to four (4) virtual PCs. NETLAB_{AE} can provide remote access to the keyboard, video, and mouse of the 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.

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

A LAN Switching Pod supports up to 4 remote PCs. NETLAB_{AE} allows 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 explained in the *NETLAB+ Remote PC Guide for VMware Server Implementation*. Direct/VMware offers complete administrative access on the remote PC. To learn more about VMware Server, please visit <http://www.netdevgroup.com/ae/vmware.htm>.

Direct/Standalone mode, as described in the *NETLAB+ Remote PC Guide for Standalone Implementation*, is not supported on this pod.

1.3 Dynamic Topologies

The LAN Switching Pod features dynamic topologies. NETLAB_{AE} can alter the topology and reposition PCs by manipulating VLANs on the control switch. This is done automatically based on the selected lab exercise. Instructors can change exercises and topologies during instructor led class reservations.

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 **CCNAExplorationEquipmentList.xls** (June 2007).

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 Switches S1, S2 and S3

Switch Name	Recommended Switch	
S1, S2 and S3	Cisco 2960	Catalyst 2960 24 10/100 + 2 1000BT LAN Base Image

Other devices options maybe can be used:

Switch Name	Switch	
S1, S2 and S3	Cisco 2950	24 10/100 ports w/ 2 10/100/1000BASE-T ports, Enhanced Image

The global command **boot enable-break** must be enabled on all switches for proper operation. Please see refer to section 8.

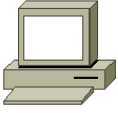


2.2 Router R1

Router Name	Recommended Router	
R1	Cisco 1841	Modular Router w/2xFE, 2 WAN slots, 32 FL/128 DR – IOS IP Base
	Cisco 2801	Modular Router w/2xFE, 2 WAN slots, 64 FL/128 DR – IOS IP Base

Other devices options maybe can be used:

Router Name	Router	
R1	Cisco 2621XM	w/2xFE, 2 WAN slots, 32 FL/128 DR – IOS IP Base
	Cisco 17xx	Router not supported



2.3 PCs and Servers

A LAN Switching Pod supports 4 VMware Server virtual machines. VMware Server is installed on a separate server.

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

- (1) VMware Server supports the operating system (as a “guest”).
- (2) Your choices are compatible with the curriculum.

Virtual Machine	Recommended O/S	Functions	Comment
Server	CCNA Discovery Server	Server	Recommended for CCNA Discovery*
A	Windows XP	Student PC, client activities	Recommended for CCNA Exploration*
B	Windows XP	Student PC, client activities	Recommended for CCNA Exploration and Discovery
C	Windows XP	Student PC, client activities	Recommended for CCNA Exploration and Discovery

* The LSP can be used for CCNA Exploration *and/or* CCNA Discovery, the following table depicts which VMs should be installed for each curriculum:

Course(s)	Server	PC A	PC B	PC C
CCNA Exploration	Not needed	Recommended	Recommended	Recommended
CCNA Discovery	Recommended	Not needed	Recommended	Recommended
CCNA Exploration and Discovery	Recommended	Recommended	Recommended	Recommended

The LAN Switching Pod includes the Discovery Server. The Discovery Server may be hosted as a virtual machine using VMware Server. Please refer to [Appendix A](#) for details on installing Discovery Server, as a Linux virtual machine, on a VMware server.

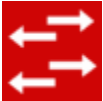
3 Control Device Requirements

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.

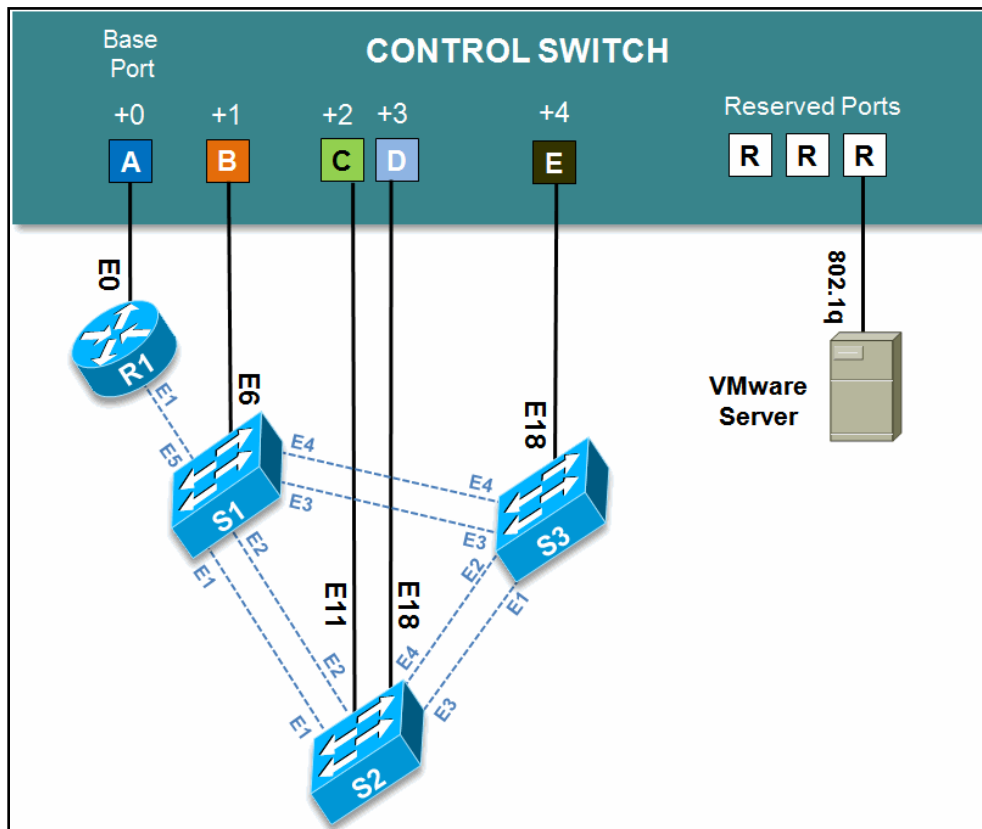
A LAN Switching Pod requires the following control device resources:

Control Device Resource	Quantity Required
Control Switch	5 consecutive ports 1 reserved port (VMware server)
Access Server	4 lines
Switched Outlet Devices	4 outlets



3.1 Control Switch Overview

NETLAB_{AE} uses a control switch to provide connectivity between devices in a LAN Switching Pod and VMware server(s). This pod requires **5 consecutive ports** on a supported control switch (other than a Catalyst 1900 series).

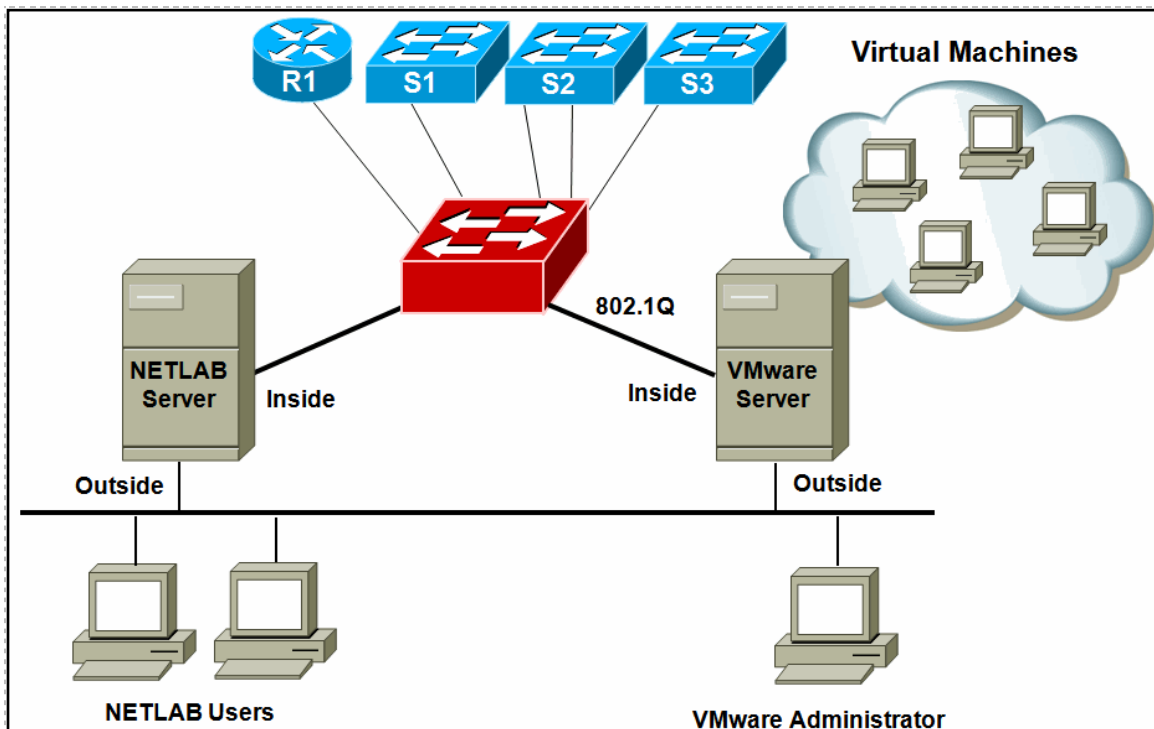


Ports are labeled +0 to +4 in the diagram and are relative to the *base port*. These ports must be consecutive on the same control switch. As with all pods, you choose a base port for the pod during pod installation (section 5). A control switch can support multiple pods. To determine the actual port 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 9.

Using SNMP, NETLAB_{AE} will automatically setup VLANs and configure ports on the control switch. These VLANs are depicted as letters “A” through “E” 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, which can be located on different VMware Servers. For more details, please see section 7.



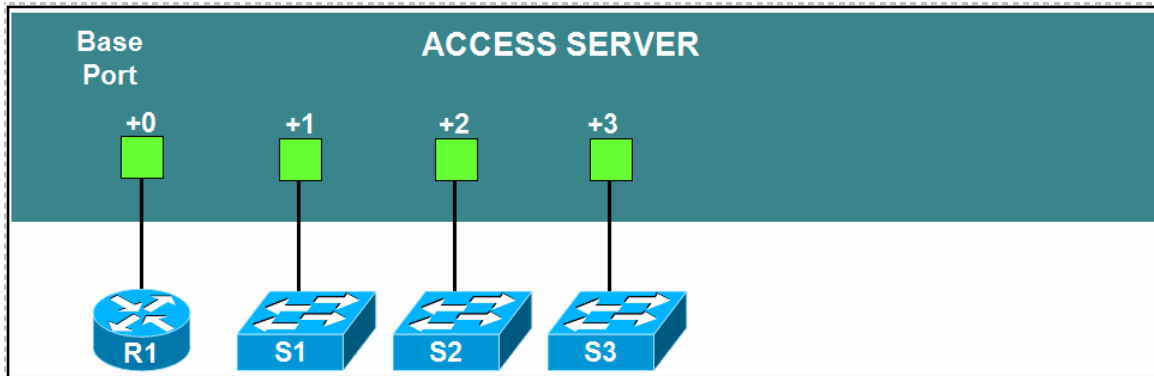


3.2 Access Server Ports

Access servers provide console connections to lab switches so that users can access them from NETLAB_{AE}. Users do not communicate directly with the access server. Rather, all connections are proxied through NETLAB_{AE}.

A LAN Switching Pod requires **4** access server ports.

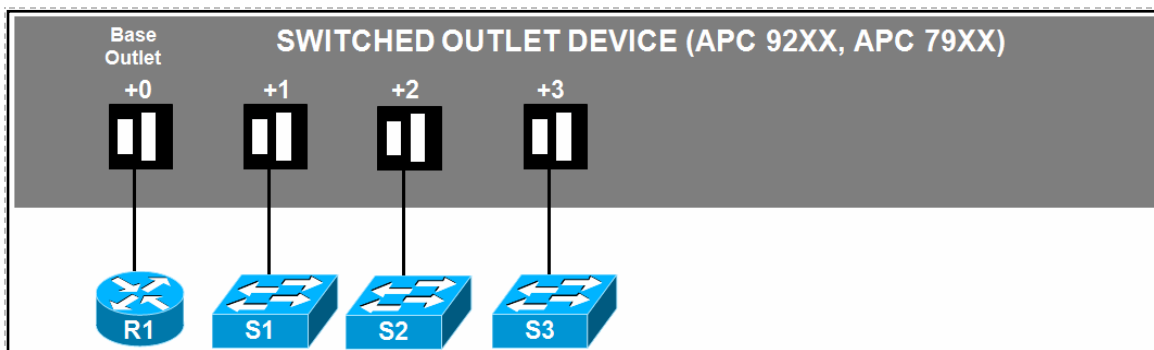
These ports do not have to be consecutive, and can span multiple access servers.



3.3 Switched Outlets

Switched outlets provide managed electrical power, allowing NETLAB_{AE} and users to turn lab equipment on and off. A LAN Switching Pod requires **4** switched outlets, one for each switch.

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 LAN Switching Pod.

4.1 Understanding VMware Server and Virtual Machines

The *NETLAB+ Remote PC Guide for VMware Server 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 LAN Switching 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. 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 LAN Switching 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 LAN Switching Pod

When prompted, select the LAN Switching Pod.




5.3 Select Control Switch and Ports

A LAN Switching Pod requires 5 **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
<input type="radio"/>	1	Catalyst 2950-24	PORT 9-16	OK TO USE
<input type="radio"/>	2	Catalyst 2950-24	PORT 11-16	OK TO USE
<input type="radio"/>	3	Catalyst 2950-24	PORT 6-16	OK TO USE

Next, select the ports you want to use.

 You have chosen control switch 1.

A AE LAN Switching Pod requires 5 consecutive control switch ports.

Which free 5-port range would you like to use?




Ports 9 to 13

Ports 9 to 13

Ports 10 to 14

Ports 11 to 15

Ports 12 to 16

5.4 Select Access Server(s) and Ports

A LAN Switching 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 switch.

ACCESS SERVERS		
ID	TYPE	PORTS THAT ARE FREE
1	Cisco 2511-RJ	8-16
2	NM-32A Module in Cisco 26xx (Lines 33-64)	0-3, 8-31

A AE LAN Switching Pod requires **4** access server ports.

Use 4 consecutive ports on access server starting at port

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
R1	2	0
S1	2	1
S2	1	8
S3	1	9

5.5 Select Switched Outlets

A LAN Switching 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	8
2	APC 9211 MasterSwitch	1-4

A AE LAN Switching Pod requires **4** switched outlets.

Use 4 consecutive outlets on switched outlet device sta 1 at outlet 8
 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
R1	1	8
S1	2	1
S2	2	2
S3	2	3





5.6 Select Device Types

Select the switch models you are going to deploy.

⇒ 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
R1	 Router	Cisco 1841 (S0/0/x)
S1	 Switch	Cisco 2960
S2	 Switch	Cisco 2960
S3	 Switch	Cisco 2960

5.7 Select Software Images and Recovery Options

Cisco switches do not provide a way for recovering IOS by using a LAN interface. Therefore, due to that limitation NETLAB+ does not offer the option for recovering IOS images on a switch at this time.

SELECT AN IMAGE AND RECOVERY OPTIONS FOR EACH LAB DEVICE			
DEVICE	TYPE	SOFTWARE IMAGE	RECOVER USING SPECIFIED IMAGE
R1	 Cisco 1841 (S0/0/x)	c1841-ipbase-mz.124-10.bin	if specified image not in flash
S1	 Cisco 2960	N/A	N/A
S2	 Cisco 2960	N/A	N/A
S3	 Cisco 2960	N/A	N/A

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 section 2.2).

5.8 Select PC Options

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 Server setup.

REMOTE PC SETTINGS				
PC NAME	ID	TYPE	ACCESS	OPERATING SYSTEM
 Server	5	VMWARE	VNC	Linux
 PC A	6	VMWARE	VNC	Windows XP
 PC B	7	VMWARE	VNC	Windows XP
 PC C	8	VMWARE	VNC	Windows XP

The following TYPE and ACCESS combinations correspond to the documentation.

The default TYPE setting is STANDALONE. This setting is not supported in the LAN Switching Pod. You must change the default setting.

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
5	Server	10.0.0.25	NETLAB	NETLAB	C:\POD_LSP_Server\DISCOVERY.vmx
6	PC A	10.0.0.25	NETLAB	NETLAB	C:\POD_LSP_PCa\WinXP.vmx
7	PC B	10.0.0.25	NETLAB	NETLAB	C:\POD_LSP_PCb\WinXP.vmx
8	PC C	10.0.0.25	NETLAB	NETLAB	C:\POD_LSP_PCa\WinXP.vmx

Next

Back

Cancel

5.10 Select a Pod ID

Each pod is assigned a unique numeric ID.

Each equipment pod is assigned a unique numeric ID.

Please select a Pod ID.

Pod ID:

Next

Back

Cancel

5.11 Select a Pod Name

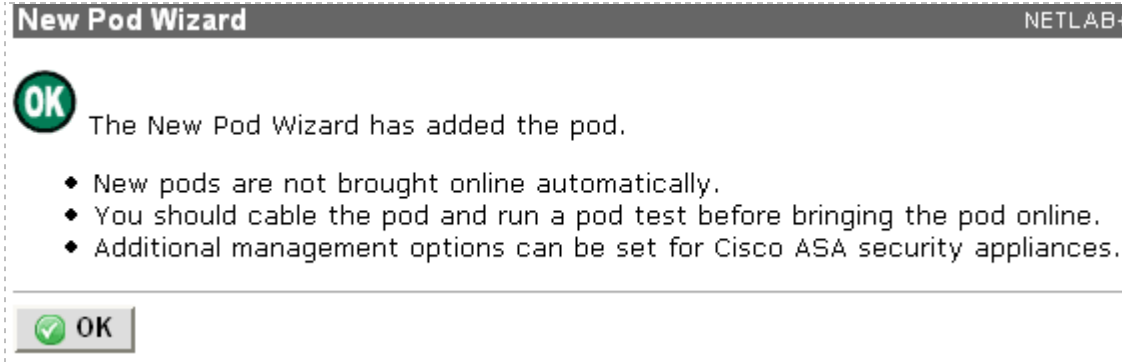
Each pod can have a unique name. This name will appear in the scheduler, along with the pod type.

Pod Name:

Next Back Cancel

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, 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 your new pod.


	4	LAN SWITCHING POD  3 Switches 1 Router PC Support	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 4 - STATUS				
POD ID	POD NAME	STATUS	ACTIVITY	POD TYPE
4	Galactica	 OFFLINE	IDLE	 LAN SWITCHING POD 3 Switches 1 Router PC Support

POD 4 - ROUTERS, SWITCHES, AND FIREWALLS (click on the GO buttons to reconfigure devices)					
GO	NAME	TYPE	 ACCESS PORTS	 SWITCHED OUTLETS	SOFTWARE IMAGE
	 R1	Cisco 1841 (S0/0/x)	AS 2 PORT 0	SOD 1 OUTLET 8	c1841-ipbase-mz.124-10.bin
	 S1	Cisco 2960	AS 2 PORT 1	SOD 2 OUTLET 1	n/a
	 S2	Cisco 2960	AS 1 PORT 8	SOD 2 OUTLET 2	n/a
	 S3	Cisco 2960	AS 1 PORT 9	SOD 2 OUTLET 3	n/a



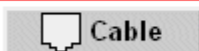

POD 4 - PCs AND SERVERS (click the GO buttons to reconfigure)							
GO	NAME	PC ID	STATUS	TYPE	ACCESS	CONTROL IP	OPERATING SYSTEM
	 Server	5	ONLINE	VMWARE	VNC	10.0.0.25	Linux
	 PC A	6	ONLINE	VMWARE	VNC	10.0.0.25	Windows XP
	 PC B	7	ONLINE	VMWARE	VNC	10.0.0.25	Windows XP
	 PC C	8	ONLINE	VMWARE	VNC	10.0.0.25	Windows XP

POD 4 - CONTROL SWITCH				
SWITCH ID	POD PORT RANGE	BASE VLAN	VLAN POOL	
 1	9-13	130	130-134	

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 4






R1 (Cisco 1841 (S0/0/x))

CONNECT FROM	USING CABLE	CONNECT TO	
FastEthernet 0/0	CAT-5 Straight Through	 C/S 1	Port 9
FastEthernet 0/1	CAT-5 Straight Through	SW1	FastEthernet0/5
Console	Console Cable	 A/S 2	Port 0
Power	Power Cord	 SOD 1 APC	Outlet 8

S1 (Cisco 2960)

CONNECT FROM	USING CABLE	CONNECT TO	
FastEthernet 0/1	CAT-5 Crossover	SW2	FastEthernet 0/1
FastEthernet 0/2	CAT-5 Crossover	SW2	FastEthernet 0/2
FastEthernet 0/3	CAT-5 Crossover	SW3	FastEthernet 0/3
FastEthernet 0/4	CAT-5 Crossover	SW3	FastEthernet 0/4
FastEthernet 0/5	CAT-5 Straight Through	R1	FastEthernet 0/1
FastEthernet 0/6	CAT-5 Crossover	 C/S 1	Port 10
Console	Console Cable	 A/S 2	Port 1
Power	Power Cord	 SOD 2 APC	Outlet 1

The cable chart is continued on the next page.

S2 (Cisco 2960)			
CONNECT FROM	USING CABLE	CONNECT TO	
FastEthernet 0/1	CAT-5 Crossover	SW1	FastEthernet 0/1
FastEthernet 0/2	CAT-5 Crossover	SW1	FastEthernet 0/2
FastEthernet 0/3	CAT-5 Crossover	SW3	FastEthernet 0/1
FastEthernet 0/4	CAT-5 Crossover	SW3	FastEthernet 0/2
FastEthernet 0/11	CAT-5 Crossover	 C/S 1	Port 11
FastEthernet 0/18	CAT-5 Crossover	 C/S 1	Port 12
Console	Console Cable	 A/S 1	Port 8
Power	Power Cord	 SOD 2	Outlet 2
S3 (Cisco 2960)			
CONNECT FROM	USING CABLE	CONNECT TO	
FastEthernet 0/1	CAT-5 Crossover	SW2	FastEthernet 0/3
FastEthernet 0/2	CAT-5 Crossover	SW2	FastEthernet 0/4
FastEthernet 0/3	CAT-5 Crossover	SW1	FastEthernet 0/3
FastEthernet 0/4	CAT-5 Crossover	SW1	FastEthernet 0/4
FastEthernet 0/18	CAT-5 Crossover	 C/S 1	Port 13
Console	Console Cable	 A/S 1	Port 9
Power	Power Cord	 SOD 2	Outlet 3

Virtual machine information will not appear on the cable chart. Refer to section 7 for configuration instructions.

The switch ports shown in the cable guidance are based on Cisco Catalyst 2960 switches.

7 Configuring VMware and Virtual Machines

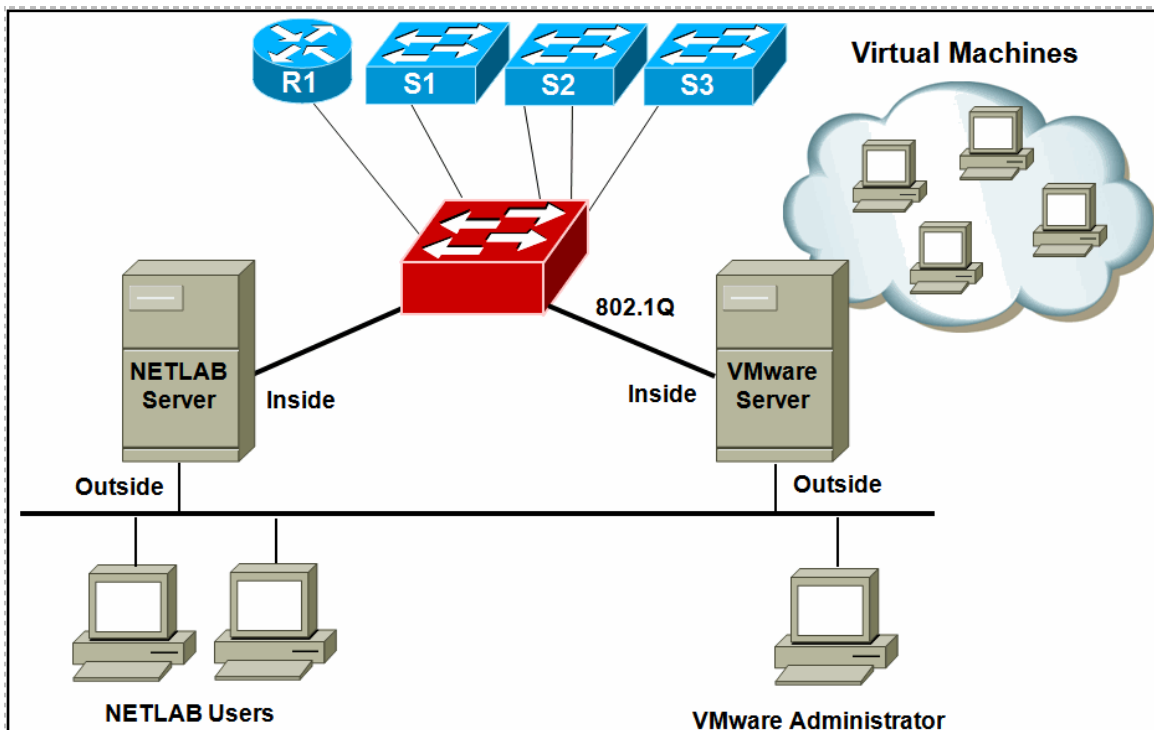
The *NETLAB+ Remote PC Guide for VMware Server Implementation* explains how to set up VMware Server and virtual machines. Please review the pod-specific information in this section and apply it to the general information in the *NETLAB+ Remote PC Guide for VMware Server Implementation*. Please note, only the sections referring to VMware are relevant; a LAN Switching 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.

The IP addresses and/or default gateways of each PC 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 the switches 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 and connected 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.

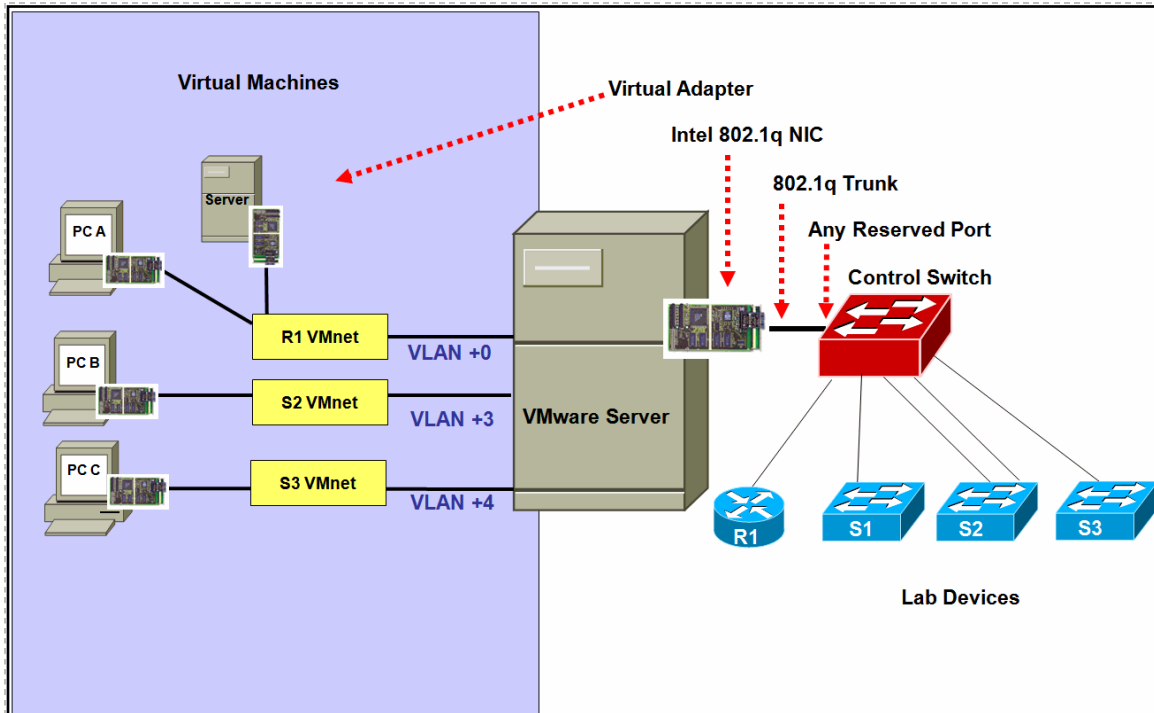


7.2 VMware Virtual Switches and VLANs

VMware Server virtual network adapters and virtual LAN switches (VMnets) are used to connect virtual machines to the pod. A LAN Switching Pod uses **3 VMnets** in the required configuration. Since VMware Server supports 10 virtual switches, it is possible to host up to 3 complete LAN Switching 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.

PC A and the Server 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 4 - CONTROL SWITCH			
SWITCH ID	POD PORT RANGE	BASE VLAN	VLAN POOL
 1	9-13	130	130-134

In this example, pod 10 uses VLANs 130-134. The base VLAN is 130.

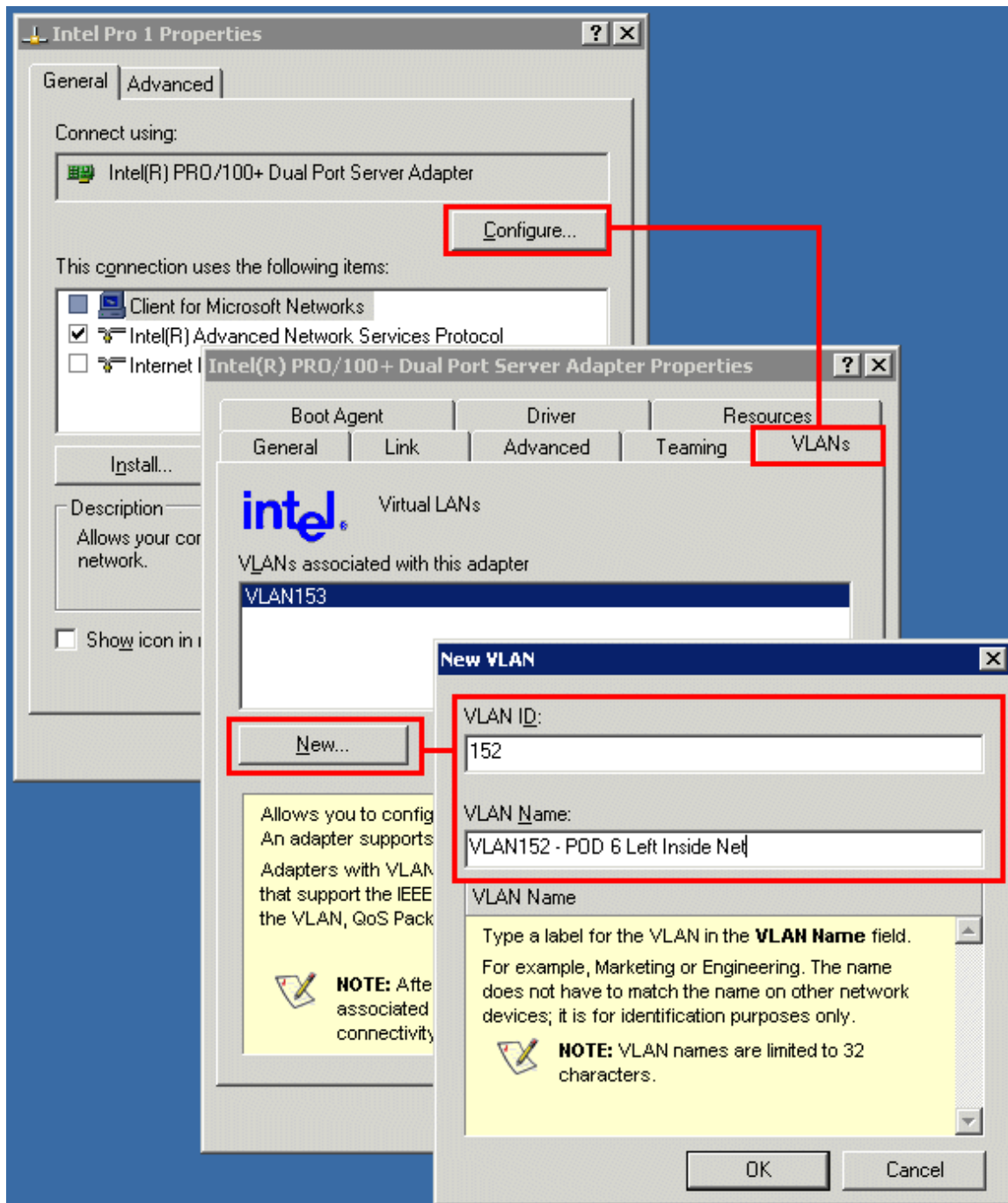
Next, determine the actual VLAN number for each virtual network by adding the base VLAN to the offsets in the table below.

Virtual Machines	Virtual Switch (VMnet)	Offset (add to base VLAN)	Actual VLAN	Example
Server	R1 VMnet	+ 0	= _____	$130 + 0 = 130$
PC A	R1 VMnet	+ 0	= _____	$130 + 0 = 130$
PC B	S2 VMnet	+ 3	= _____	$130 + 3 = 133$
PC C	S3 VMnet	+ 4	= _____	$130 + 4 = 134$

7.3 Configure VMware Server Inside Port

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

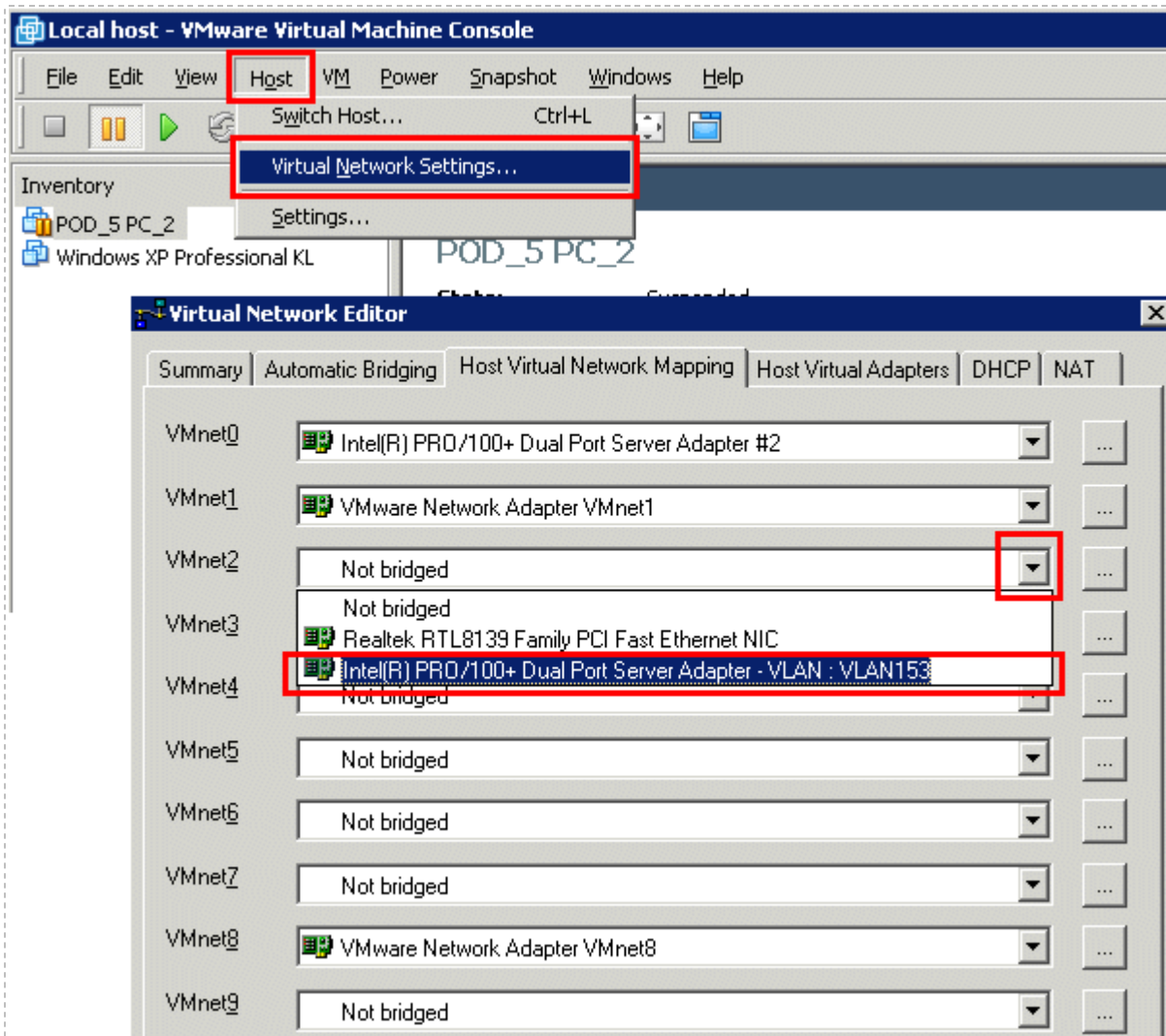
Be sure to **uncheck** TCP/IP and Client for Microsoft Networks from each VLAN sub-interface. Only the VMware bridge protocol should be checked.



7.4 Create Virtual Switches (VMnet)

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

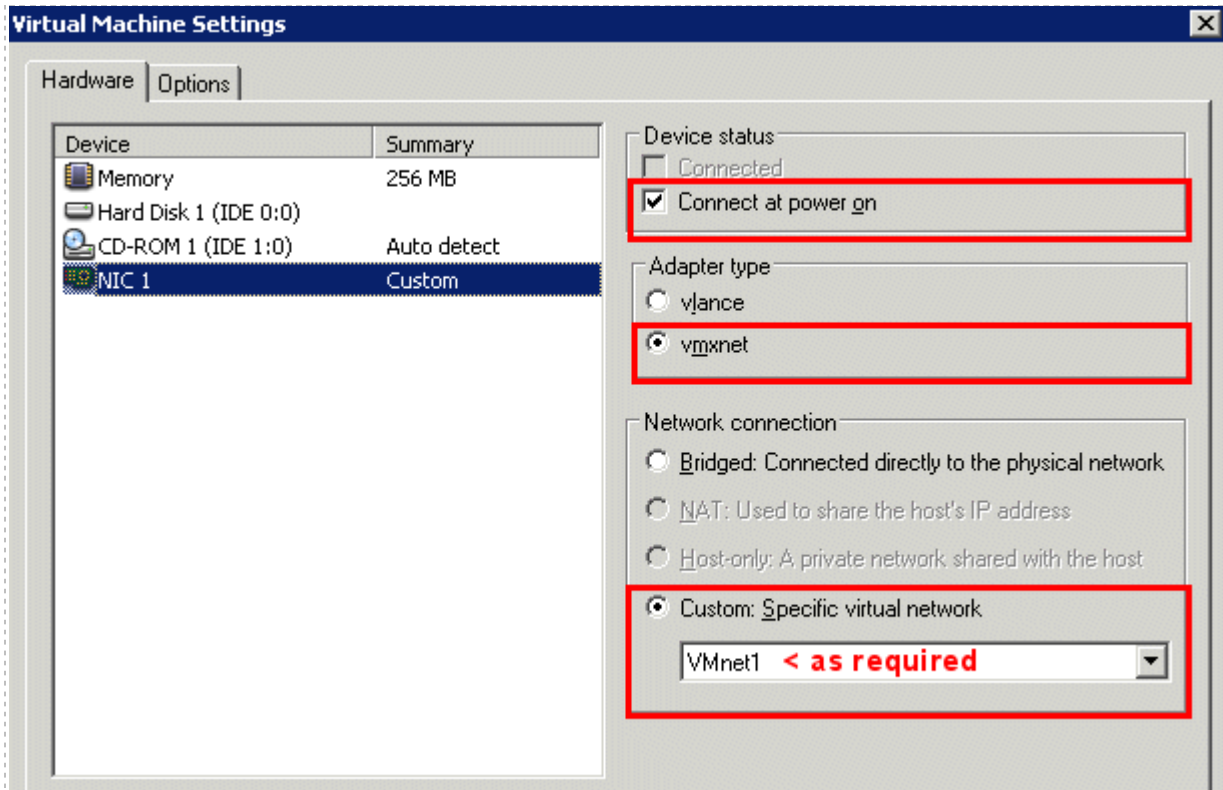
It does not matter which VMnet number you use. By default, VMnet0, VMnet1, and VMnet8 are reserved for special functions in VMware. However, you can convert these into ordinary VMnets to use with pods. This is explained in Appendix A of the *NETLAB+ Remote PC Guide for VMware Implementation*.



7.5 Binding Virtual Machines to Virtual Switches (VMnet)

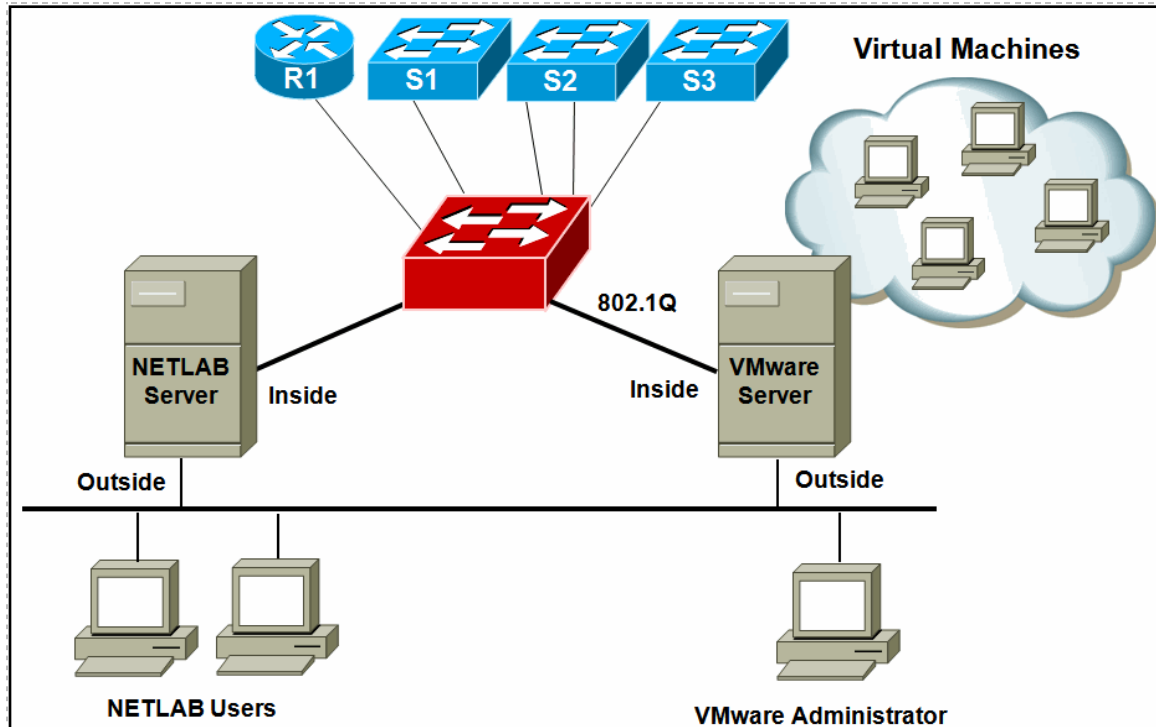
Refer to section 7 of the *NETLAB+ Remote PC Guide for VMware Implementation*. In the last section, you associated a specific VLAN with a virtual switch (VMnet). When you create a virtual machine, you must bind it to the correct virtual switch (and by association, VLAN).

Virtual Machines	Virtual Switch (VMnet)	Offset (add to base VLAN)	Actual VLAN	Example
Server	R1 VMnet	+ 0	= _____	130 + 0 = 130
PC A	R1 VMnet	+ 0	= _____	130 + 0 = 130
PC B	S2 VMnet	+ 3	= _____	130 + 3 = 133
PC C	S3 VMnet	+ 4	= _____	130 + 4 = 134



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.

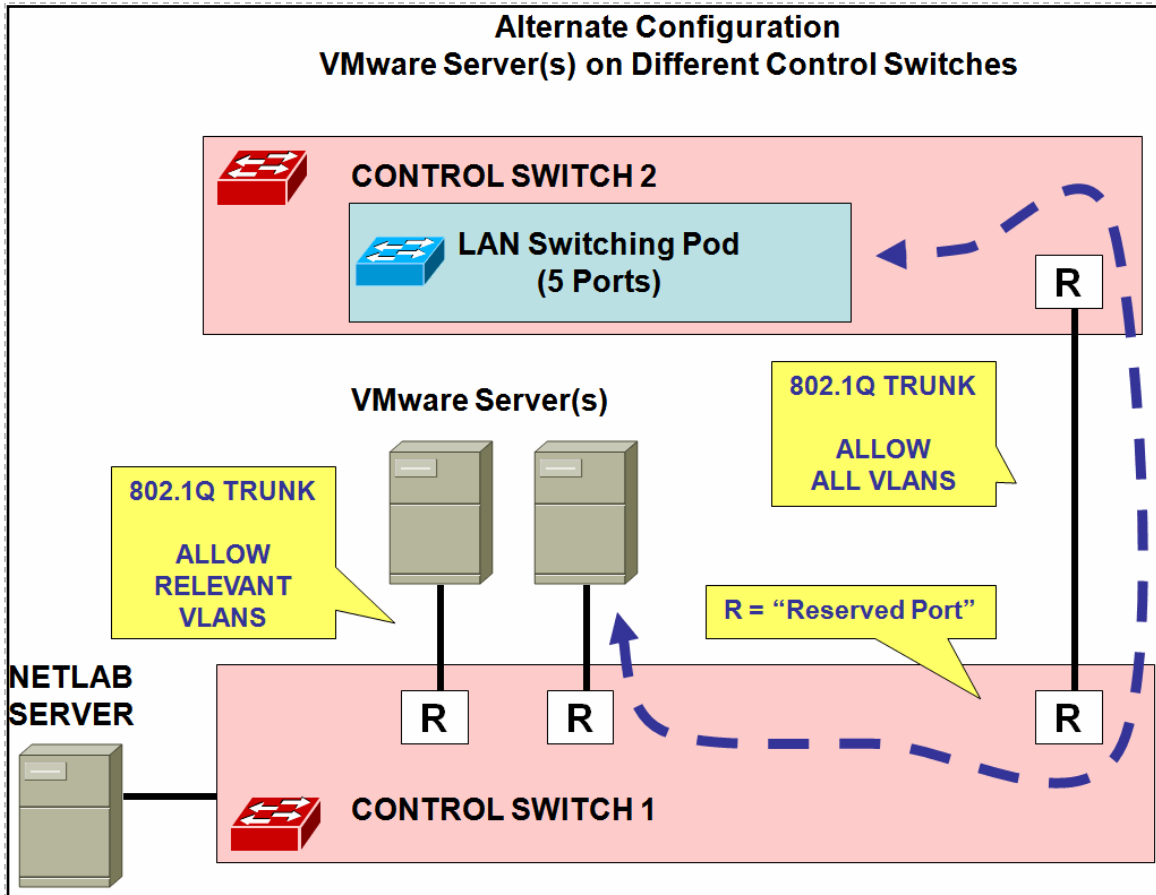
The control switch console password is **router**. The enable secret password is **cisco**. These passwords are used by NETLAB+ automation and technical support - please do not change them.

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

```
interface FastEthernet0/23
  switchport mode trunk
  switchport trunk allowed vlan 130,133,134
  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, if 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 130,133,134
  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 Switch Configuration Tasks

The LAN Switching Pod requires additional switch configuration tasks for successful operation. Using Hyperterm or other terminal emulator, connect to the console port of the control switch in which the Lan Switching Pod is connected. The following passwords are used on the control switch.

Console login password	router
Enable secret password	cisco

Please do not change the passwords – they are used NETLAB+ automation and technical support.

8.1 Verify Control Switch IOS Version

Each control switch should be running **IOS 12.1(22)EA2 or later**. Earlier versions may have defects that affect NETLAB_{AE}.

8.2 Configure Control Switch Ports

There are three essential commands that must be manually configured on each control switch port that connects to a lab switch (S1, S2, and S3 in this case).

- **spanning-tree bpdupfilter enable**
 - Instructs control switch port not to send and receive spanning tree BPDU frames to and from the lab switch.
 - Spanning tree in the lab must not mingle with spanning tree on the control switch. This would cause several undesirable effects in both the lab and on the control switches.
- **switchport mode access**
 - Prevents the link from becoming a trunk port.
 - The labs will not work as designed if the link between control switch and lab switch is trunking.
 - Trunking on ports that should be access ports, combined with BPDU filtering, creates loops that are not prevented by spanning-tree.
- **no cdp enable**
 - Disabling CDP is not critical, but will hide the control switch from lab switch users performing CDP commands.
- **switchport nonegotiate**
 - Prevents the interface from sending DTP messages.
 - Disabling DTP messages is not critical, but will hide the control switch' MAC address from lab switches when users performing commands to see the CAM table.

- **no keepalive**
 - Prevents the interface from sending L2 keepalive messages.
 - Disabling L2 keepalive messages is not critical, but will hide the control switch' MAC address from lab switches when users performing commands to see the CAM table.

Do not omit these commands! Without them, loops will form causing high CPU utilization, error-disabled ports, and connectivity loss. These commands are specific to switch pods and are not automatically configured.

Locate the 4 control switch ports connecting to S1,S2 and S3. Refer to the cabling diagram if necessary (section 6). The following commands must be manually added to each switch port.

Example switch port configuration. Interface numbers will vary.

```
interface FastEthernet0/10
  description port to S1 port 6
  switchport mode access
  spanning-tree bpdufilter enable
  switchport nonegotiate
  no keepalive
  no cdp enable

interface FastEthernet0/11
  description port to S2 port 11
  switchport mode access
  spanning-tree bpdufilter enable
  switchport nonegotiate
  no keepalive
  no cdp enable

interface FastEthernet0/12
  description port to S2 port 18(Host B)
  switchport mode access
  spanning-tree bpdufilter enable
  switchport nonegotiate
  no keepalive
  no cdp enable

interface FastEthernet0/13
  description port to S3 port 18 (Host C)
  switchport mode access
  spanning-tree bpdufilter enable
  switchport nonegotiate
  no keepalive
  no cdp enable
```

Note: If the control switch does not recognize the **spanning-tree bpdufilter** command, make sure the switch is running at least 12.1(22)EA2.

8.3 Initial Lab Switch Setup

Several switch models are subject to a common problem when used as a **lab switch**. These include (but not limited to):

- Cisco Catalyst 2900 XL Series
- Cisco Catalyst 2950 Series
- Cisco Catalyst 2960 Series
- Cisco Catalyst 3550 Series
- Cisco Catalyst 3560 Series

By default, these switches will not respond to a console break signal the same way routers do. There are two *environment variables* that affect this: **Enable Break** and **BOOT path-list**.

The following procedure explains how to check these variables and set them so that the console port will respond to a break signal.

When to Use

You must initialize the environment variables when:

- Installing a lab switch for the first time .
- The Enable Break environment variable is set to "no".
- The BOOT path-list environment variable is set.

This procedure does not apply to control switches.

Determining the Boot Status

From the enable mode, issue the following IOS command.

```
Lab_Sw# show boot

BOOT path-list:      flash:c2950-i6q412-mz.121-22.EA4.bin
Config file:         flash:config.text
Private Config file: flash:private-config.text
Enable Break:        no
Manual Boot:         no
```

Setting Up the Environment

Follow this procedure if Enable Break is set to “no” and/or the boot path-list is set to an image.

```
Lab_Sw# configure terminal
Lab_Sw(config)# boot enable-break
Lab_Sw(config)# no boot system
Lab_Sw(config)# end
Lab_Sw# copy run start
Lab_Sw# show boot

BOOT path-list:

Config file:          flash:config.text
Private Config file:  flash:private-config.text
Enable Break:        yes
Manual Boot:         no
```

Verification

With Enable Break set to "yes" and removal of a BOOT path-list, a pod test should pass.

If the environment variables are not set correctly, you may experience one of the following symptoms:

1. Pod test fails with a message such as "unable to put the switch into monitor mode"
2. Lab automation such as scrub fails
3. Users cannot perform password recovery (automated or manual)

9 Testing the Pod

After all switches 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

Bring this pod ONLINE and make it available for reservations.
 Tell me if this pod is working properly.
 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.


TESTING POD 3				
DEVICE	TYPE	TEST	STATUS	DETAILS
Control Switch 3	Catalyst 2950-24		PASSED	3 test(s) passed, device looks good
R1	Cisco 2611XM	BOOTIOS	RUNNING	boot IOS image test
S1	Cisco 2950T-24 (E)		WAITING	<ul style="list-style-type: none"> 2 test(s) passed 1 test(s) remaining
S2	Cisco 2950T-24 (E)	BOOTIOS	RUNNING	boot IOS image test
S3	Cisco 2950T-24 (E)		WAITING	<ul style="list-style-type: none"> 2 test(s) passed 1 test(s) remaining
Server	VMWARE		PASSED	1 test(s) passed, device looks good
PC A	VMWARE		PASSED	1 test(s) passed, device looks good
PC B	VMWARE		PASSED	1 test(s) passed, device looks good
PC C	VMWARE		PASSED	1 test(s) passed, device looks good

POD TEST LOG	
[01:49] S1: boot IOS image test - PASS	
[01:49] S3: boot IOS image test - PASS	
[00:57] S2: recover console test - PASS	
[00:39] S1: recover console test - PASS	
[00:39] S3: recover console test - PASS	


TESTING IN PROGRESS STOP


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.







NETWORKING ACADEMY[®]




 NETLAB+ 4.0.23
administrator


Equipment Pods


Admin


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
	<u>1</u>	CUATRO ROUTER POD 4 routers, PCs 	POD 1	 OFFLINE	IDLE
	<u>4</u>	LAN SWITCHING POD 3 Switches 1 Router PC Support 	Galactica	 OFFLINE	IDLE

 **Add a Pod**

 **Take All OFFLINE**

 **Bring All ONLINE**

 **Back**

10.2 Enable LAN Switching Pod Exercises

To make LAN Switching Pod available to classes and students, you must enable the corresponding lab exercise content in each new or existing class.

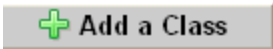
To add or edit class information, log into NETLAB_{AE} using your instructor account. See the Instructor Accounts section of the *NETLAB+ Administrator Guide* for details.

A login form with a light blue background and a dashed border. It contains two input fields: 'Username' with the text 'janedoe' and 'Password' with ten black dots. Below the fields is a 'Login' button.



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.

CLASS LIST COMMUNITY: ABC Technical School							
CLASS NAME	LEAD INSTRUCTOR(S)	# ENROLLED	START DATE	END DATE	LABS	LAB HOURS	
CCNP Fall Class	Jane Doe	4	Jan 4, 2007	Mar 4, 2007	2	1.5	
Janes Test Class	Jane Doe	0	None	None	0	0.0	
CCNx 3.x	Jane Doe	3	None	None	0	0.0	
					Total	2	1.5

In the global labs section of the class settings, check the labs that you wish to make available to your class.

These selections determine whether the LAN Switching Pod is made available for student, team, or ILT reservations for this class.

Class Name CCNP Fall Class **REQ**

Lead Instructor(s) Teacher One

Global Labs

- AE CCNA 1 English V3.1
- AE CCNA 2 English V3.1
- AE CCNA 3 English V3.1
- AE CCNA 4 English V3.1
- AE CCNA Bridge Exams 3.0
- AE CCNA English V2.1 (retired)
- AE CCNP BCMSN V5.0 English
- AE CCNP BSCI V5.0 English
- AE CCNP Pod Reservations (no labs)
- AE FNS Combined V1.2 English
- AE FNS PIX V1.2 English
- AE FNS Router V1.2 English

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.

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

Scheduler INSTRUCTOR
MyNETLAB Logout **janedoe**

<< January 2007 >>

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			

Now Showing **Wednesday**
January
24
2007

Today's Date and Local Time
January 24, 2007
4:40 PM
Eastern Time (US & Canada)

Select a pod and reservation by clicking on a

	Galactica LAN SWITCHING POD 3 Switches 1 Router PC Support	CSP #5 CUATRO SWITCH POD 4 switches 4 PCs
12am	(+)	(+)
	(+)	(+)
1am	(+)	(+)
	(+)	(+)

The reservation time area may be scrolled up and down.

- ⊕ Select an available time, and the confirmation page will be displayed.

Reservation Type Instructor Access

Equipment Pod POD 3

Reserve Pod For Geovany González

Time Zone Central Time (US & Canada)

Start Time Monday January 7, 2008 10:00AM

End Time Jan 7, 2008 11:00 AM

Initial Configuration

- restore configs from last AE LAN Switching Pod reservation (if any)
- load default configs for exercise
- 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.

6am	+	+	191 Jane Doe
	+	+	
7am	+	+	

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

Appendix A Installing Discovery Server on a VMware Server

You may install Discovery Server on a VMware server by following this procedure.

1. Download Discovery-Server-v2.0.iso from the [Cisco Academy Connection](#) website.
2. Use VMware Server 1.0.x to create a new virtual machine for Discovery Server:
<http://www.vmware.com/download/server/>
3. For general VMware guidance, please refer to the [VMware Server Administration Guide](#).
4. For a quick reference on how to create a VM for remote access (via a NETLAB+ server) refer to pages 32-46 of the [NETLAB+ Remote PC Guide for VMware Server Implementation](#)
5. Create a new Virtual Machine (using VMware Server Console).
 - a. Choose “Custom” configuration
 - b. O/S is Linux and specifically “Other Linux”
 - c. Name your VM
 - d. Uncheck “make this VM private”
 - e. select “Local System Account”
 - f. One processor is fine
 - g. 128MB RAM is fine for running Linux in text mode
 - h. Select the “Network connection” type that best fits your needs
 - i. Go with the default selected I/O adapter type
 - j. Create new virtual disk
 - k. Select IDE drive
 - l. 1.0 – 2.0 GB for Linux “var” partition is more than enough (only about 400mb will be used up)
 - m. Make sure to uncheck “Allocate all disk space now”
 - n. Finish VM
6. Drop the ISO file you downloaded in #1 into the VM directory (should be on your local disk’s root level as “\Virtual Machines\<<Name_of_VM>”).
7. From the VMware Server Console click on “Edit virtual machine settings” for the newly created VM.
 - a. Select the CD-ROM Hardware device and select the radio option to “Use ISO image”
 - b. Browse and select the ISO
 - c. From the Options tab select Snapshots and set “When powering off” to “Ask me”
8. Start the Discovery Server VM and press F2 in boot window very quickly.
 - a. From BIOS Boot tab, make sure the CD-ROM Drive boots first and the Hard Drive second
 - b. Exit saving changes

9. As soon as you see the main boot prompt type “m” and press <ENTER>.
 - a. Press “m” to access run option menu (to configure Adios)

10. You should see the “ADIOS-7.2 Live DVD Menu” in yellow with several run options.
 - a. At the “Option:” prompt type “r” to change starting run level from 5 to 3
 - b. At the “Option:” prompt type “fdisk” to partition the virtual IDE disk
 - i. You should see /dev/hda (this is the device that needs to be partitioned)
 - ii. Type “m” for help
 - iii. Type “n” to add a new partition
 - iv. Type “p” for primary and “1” partition number
 - v. Select the First cylinder and Last cylinder by default
 - vi. Type “m” for list of commands
 - vii. Type “p” to print the partition table
 - viii. Type “w” to write table to disk and exit
 - ix. Press <ENTER>
 - c. At the “Option:” prompt type “22” to run from DVD with var on virtual disk.
 - i. 22) Option 1 (run from DVD) + /var in its own disk partition)
 - ii. Enter device name: /dev/hda1
 - iii. Proceed with format of /dev/hda1? (y/n) y
 - iv. Press <enter>

11. Discovery server should boot into run level 3. You may notice some services did not start.
 - a. Eth0 may not start up because it is set to obtain DHCP address.
 - b. ipsec service did not start up
 - c. dhcpd service did not start up

12. Add the IP settings by editing the following files using mcedit:
 - a. /etc/sysconfig/network (add the gateway setting):
GATEWAY=172.17.0.1
 - b. /etc/sysconfig/network-scripts/ifcfg-eth0 (change or add the following settings)
BOOTPROTO=static
BROADCAST=172.17.255.255
IPADDR=172.17.1.1
NETMASK=255.255.0.0
NETWORK=172.17.0.0

13. Edit the named.conf file to allow any client PC to resolve Discovery server domains.
 - a. Edit the named.conf file located at /var/named/chroot/etc/named.conf.
 - b. Apply the following change:
From:
match-clients { localnets; localhost; };
match-destinations { localnets; localhost; };

To:
match-clients { any; };
match-destinations { any; };

14. Edit `/etc/rc.local` to restart `eth0` when the Discovery server boots up.
 - a. Edit the `/etc/rc.local` file (add the following to the end of the file):

```
# Restart Discovery server eth0
/sbin/ifdown /etc/sysconfig/network-scripts/ifcfg-eth0
/sbin/ifup /etc/sysconfig/network-scripts/ifcfg-eth0
```
15. Reboot the Discovery server to confirm all services start properly and `eth0` is assigned the proper IP address (172.17.1.1).
16. Gracefully shutdown (`/sbin/shutdown -h now`) the Discovery Server and take a VMware console snapshot to save your work.