Network Fundamentals Pod

Planning and Installation Guide

For Cisco Networking Academy® CCNA Exploration Curriculum

Document Version: 2008-08-26

Contents

PART 1 – PLANNING

1   Introduction

The NETLAB$_{AE}$ Network Fundamentals Pod supports many CCNA 4.0 Exploration 1 lab exercises.
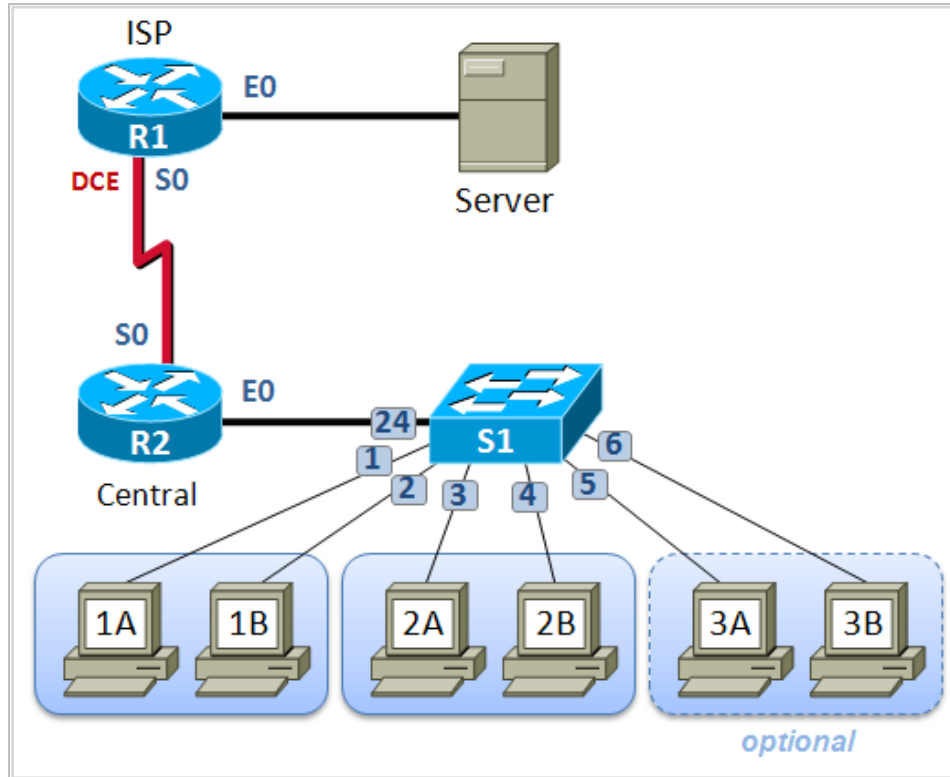
You may have up to eight (8) Network Fundamentals Pods per NETLAB$_{AE}$ system.

The Network Fundamentals Pod features direct access to router and switch consoles. Integration with a separate VMware Server supports up to seven (7) 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 Network Fundamentals Pod supports up to seven (7) remote PCs. NETLAB$_{AE}$ allows three alternative settings for each:

- **Direct/VMware**. The PC is implemented as a VMware virtual machine.
    - o   Users can control the keyboard, video, and mouse.
    - o   Users can power on, shutdown, reboot, and revert to a clean state.
    - o   Users can have administrator rights.

- **Indirect**. The PC is implemented, but not managed by NETLAB$_{AE}$.
    - o   Users may be able to interact with the PC, but cannot access the keyboard, video, or mouse through NETLAB$_{AE}$.

- **Absent**. The PC is not implemented.

These options are fully explained in the *NETLAB+ Remote PC Guide for VMware Server Implementation*. Direct/VMware offers complete administrative access on the remote PC. To learn more about VMware Server, please visit http://www.netdevgroup.com/ae/vmware.htm.

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

1.3   Dynamic Topologies

The Network Fundamentals 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.

In the CCNA Exploration 1 curriculum, the dynamic topologies feature is used in order to alter the NFP pod to support labs with the following logical topology.
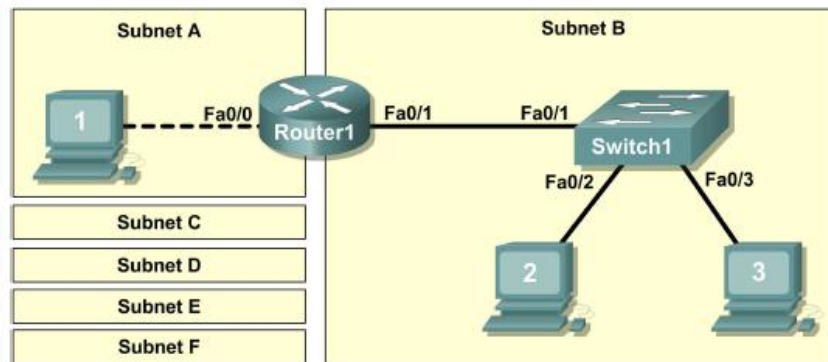
This topology requires two (2) FastEthernet interfaces. Physical router R2 in the NFP topology is used for the router activities in the diagram above, and therefore must have two FastEthernet interfaces. See section 2.1 for specific equipment requirements.

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   Routers R1, R2 and Switch S1

Router Name	Recommended Routers	Ethernet Ports Required	Serial Ports Required	Recommended Serial Modules
R1	Cisco 1841	1	1	1 x WIC-2A/S
R2	Cisco 1841	**2**	1	1 x WIC-2A/S
S1	Cisco 2960	7	N/A	N/A

Router R2 requires two FastEthernet interfaces to support several labs in CCNA Exploration 1. Please refer to section 1.3 for details.

Serial interfaces may be built-in, or provided by modular interface cards such as the WIC-2A/S. Serial connections between routers require the appropriate serial cables. You can use DTE and DCE cables back-to-back, or special cables that provide both DTE and DCE in one cable (available from SIGMAnet).

The control switch requires additional configuration commands to accommodate switch S1. Please refer to section 8.2.

The global command **boot enable-break** must be enabled on switch S1 for proper operation. Please see refer to section 8.3.

2.2   PCs and Servers

A Network Fundamentals Pod supports 7 VMware Server virtual machines, 4 are required, 2 are optional and 1plays a server role (Eagle Server). 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
PC1A	Windows XP	Student PC, client activities
PC1B	Windows XP	Student PC, client activities
PC2A	Windows XP	Student PC, client activities
PC2B	Windows XP	Student PC, client activities
PC3A	Windows XP	Student PC, client activities
PC3B	Windows XP	Student PC, client activities
Server	Eagle Server	The network services provided: Instant Messaging Wiki Server Domain Name Server Email Server Web Server FTP TFTP SSH

2.3   Eagle Server

Eagle Server is a pre-built application server that can be downloaded from the Tools section of Academy Connection. Appendix A of this document describes how to install and run Eagle Server as a VMware Server virtual machine.

The NDG implementation of Eagle Server allows direct access to the Eagle Server console. The KDE graphical user interface has been disabled to conserve server memory and bandwidth, and to improve remote access performance. KDE is not required.

Please refer to Appendix A for specific installation instructions for Eagle 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 Network Fundamentals Pod requires the following control device resources:

Control Device Resource	Quantity Required
Control Switch	10 consecutive ports 1 reserved port (VMware server)
Access Server	3 lines
Switched Outlet Devices	3 outlets

3.1   Control Switch Overview

NETLAB_{AE} uses a control switch to provide connectivity between devices in a Network Fundamentals Pod and VMware server(s). This pod requires **10 consecutive ports** on a supported control switch (other than a Catalyst 1900 series).
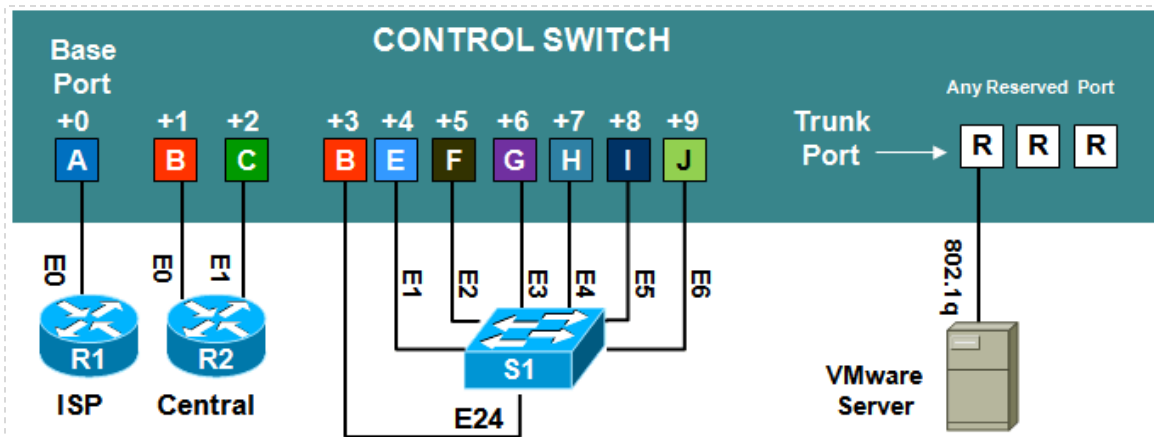
Ports are labeled **+0** to **+9** in the diagram and are relative to the *base port*. These ports must be consecutive on the same control switch.

> The FastEthernet connections between the lab switch and S1 and the control switch require crossover Ethernet cables (unless one or both switches support MDX).

> The control switch requires additional configuration commands to accommodate switch S1. Please refer to section 8.2.

> Ports +8 and +9 (S1 E5/E6) are allocated even if the PCs from group 3 are not implemented. Therefore, we recommend cabling these ports to avoid accidentally using them for something else.

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 14.

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

One "reserved" port on the control switch connects to an 802.1Q NIC card on the VMware Server. This allows devices in the pod to communicate with virtual machines.

The reserved port may be located on a different control switch, provided that all links between control switches are also configured as 802.1Q trunks and all VLANs are allowed. You may also have more than one VMware Server and virtual machines in the pod can be located on different VMware Servers. For more details, please see section 7.
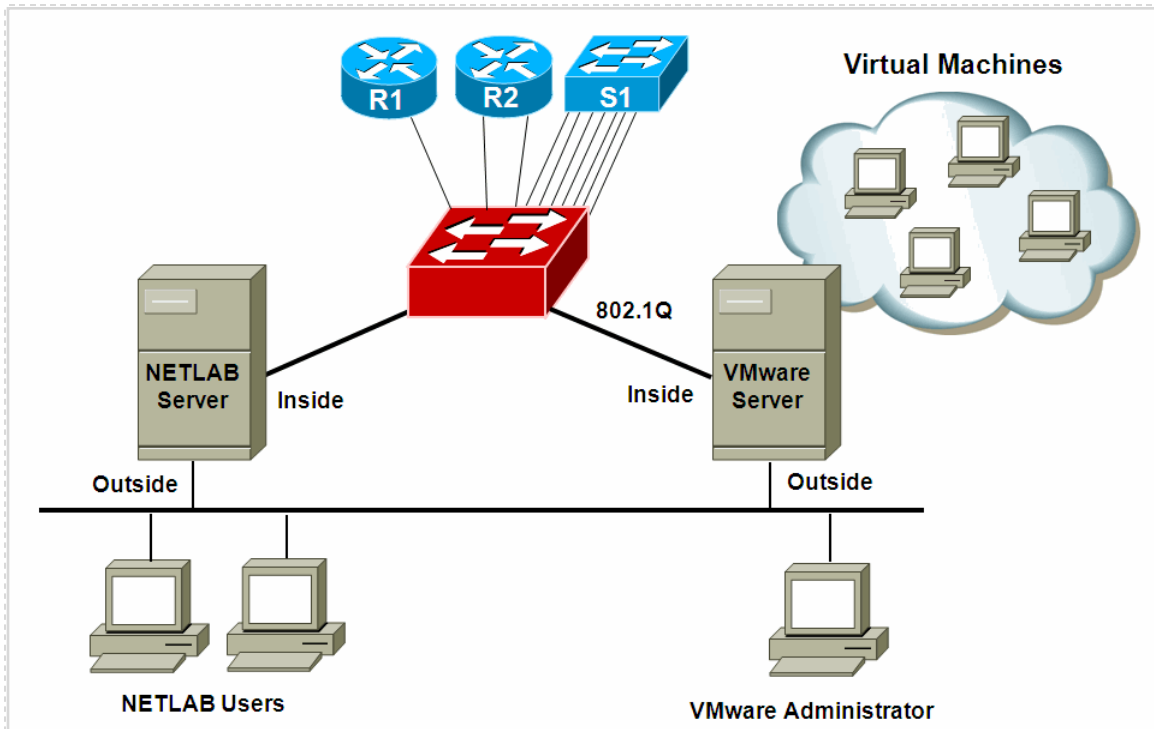
3.2   Access Server Ports

Access servers provide console connections to lab routers 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 Network Fundamental Pod requires **3 access server ports**.

Access server ports do not have to be consecutive, and can span multiple access servers.
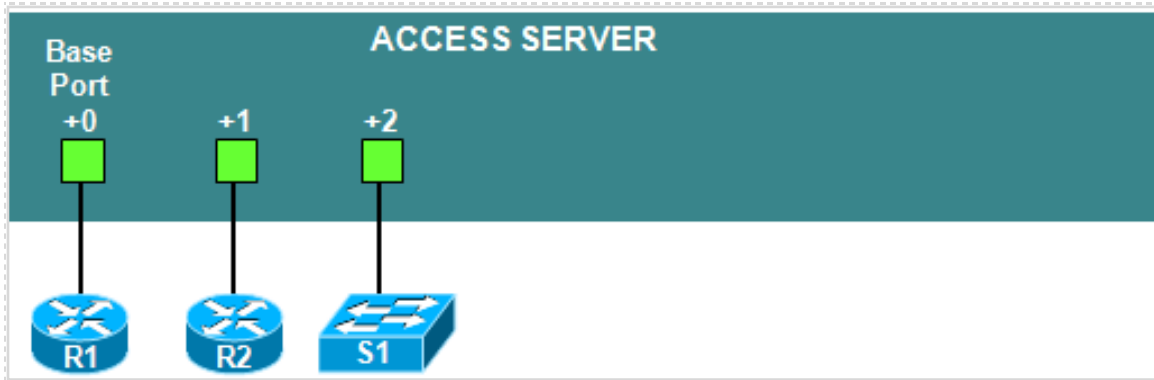
3.3   Switched Outlets

Switched outlets provide managed electrical power, allowing NETLAB$_{AE}$ and users to turn lab equipment on and off. A Network Fundamentals Pod requires **3 switched outlets**, one for each router.

Outlets do not have to be consecutive and may span multiple switched outlet devices (i.e. APC7900 or APC7920).
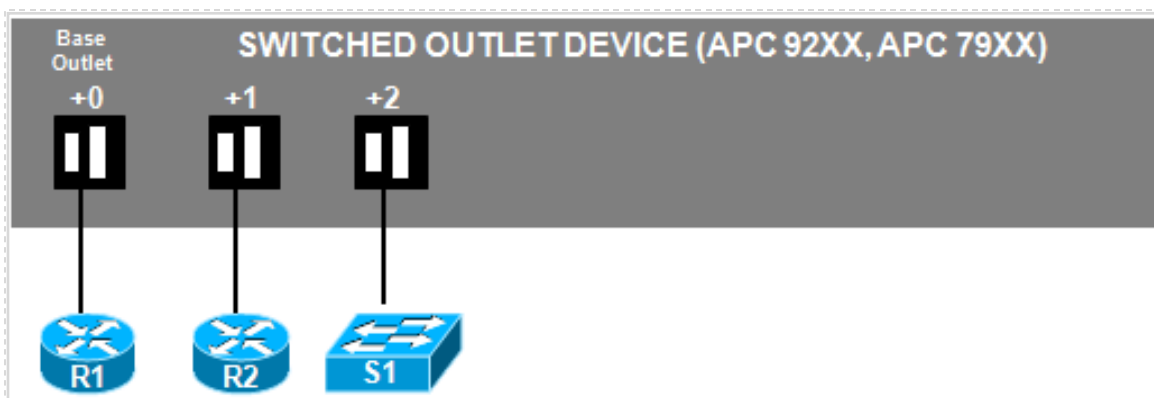
PART 2 – IMPLEMENTATION

4   Pre-requisites

This section covers tasks that should be executed prior to adding a Network Fundamentals 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 Network Fundamentals 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 Network Fundamentals Pod using the NETLAB$_{AE}$ New Pod Wizard.

5.1   Start the New Pod Wizard

Login to the administrator account.

Select Equipment Pods.

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

Select ➕ Add a Pod.

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

5.2   Add a Network Fundamentals Pod

When prompted, select the Network Fundamentals Pod.

5.3   Select Control Switch and Ports

A Network Fundamentals 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 Network Fundamentals Pod requires **3 access server ports**.

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

Use the physical port numbers shown on the access server. Some models start at port 1 (Cisco 2509 and 2511) and others start at port 0 (Cisco NM-16A and NM-32A modules).

NETLAB_{AE} allows you to choose consecutive ports on one access server, or you can choose "Let me pick" to select an access server and port for each router.

"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	1	0
R2	1	1
S1	1	2

Next   Back   Cancel

5.5   Select Switched Outlets

A Network Fundamentals Pod requires **3 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 7900 Switched Rack PDU	1-8
2	APC 9211 MasterSwitch	1-8
3	APC 7920 Switched Rack PDU	1-8

A AE Network Fundamentals Pod requires **3** switched outlets.

◉ Use 3 consecutive outlets on switched outlet device 1 starting at outlet 1
○ Let me pick select outlets for each device manually

Next   Back   Cancel

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

5.6   Select Device Types

Select the router models you are going to deploy.

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

$\Rightarrow$ Improper selections may cause errors.

$\Rightarrow$ NETLAB$_{AE}$ may offer selections that do not support the curriculum. See section 2.1 for a list of recommended devices for this pod.

R2 must have two FastEthernet interfaces, whereas R1 may have one.

5.7 Select Software Images and Recovery Options

NETLAB$_{AE}$ scrubs each router at the end of lab reservation or upon request. During a scrub, NETLAB$_{AE}$ can recover an IOS image if it is 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.

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. We have chosen not to implement PC 3A and 3B in this example, so the type is set to ABSENT.

> The Network Fundamentals Pod is especially suitable for teaching CCNA 4.0 Exploration 1. This course uses pairs of virtual machines at the same time in order to complete certain labs. Therefore, it is required to implement at least Group 1 (PC1A-PC1B) and Group 2 (PC2A-PC2B). The Group number 3 (PC3A-PC3B) is optional and may be installed if the POD will be used for team or classroom activities.

Typical remote PC settings

REMOTE PC SETTINGS				
PC NAME	ID	TYPE	ACCESS	OPERATING SYSTEM
Server	1	VMWARE	VNC	Linux
1A	2	VMWARE	VNC	Windows XP
1B	3	VMWARE	VNC	Windows XP
2A	4	VMWARE	VNC	Windows XP
2B	8	VMWARE	VNC	Windows XP
3A	9	ABSENT	VNC	Windows XP
3B	10	ABSENT	VNC	Windows XP

Next   Back   Cancel

The following TYPE and ACCESS combinations correspond to the documentation.

> The default TYPE setting is STANDALONE. This setting is not supported in the Network Fundamentals 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

5.10 Select a Pod ID

Each pod is assigned a unique numeric ID.

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.

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.
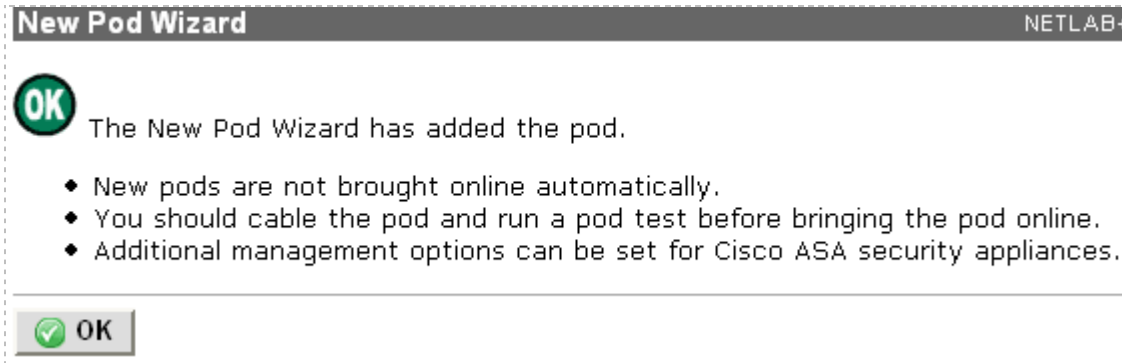
After you click OK, the new pod will appear in the list of equipment pods. Click on the magnifier button or pod ID to manage you new pod.

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

POD 2 - STATUS

POD ID	POD NAME	STATUS	ACTIVITY	POD TYPE
2	Galactica	⬤ OFFLINE	IDLE	NETWORK FUNDAMENTALS POD

POD 2 - 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 1 PORT 0	SOD 1 OUTLET 1	c1841-ipbase-mz.124-10.bin
🔍	✕ R2	Cisco 1841 (S0/1/x)	AS 1 PORT 1	SOD 1 OUTLET 2	c1841-ipbase-mz.124-10.bin
🔍	⇄ S1	Cisco 2960	AS 1 PORT 2	SOD 1 OUTLET 3	n/a

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

GO	NAME	PC ID	STATUS	TYPE	ACCESS	CONTROL IP	OPERATING SYSTEM
🔍	Server	1	ONLINE	VMWARE	VNC	10.0.0.25	Linux
🔍	1A	2	ONLINE	VMWARE	VNC	10.0.0.25	Windows XP
🔍	1B	3	ONLINE	VMWARE	VNC	10.0.0.25	Windows XP
🔍	2A	4	ONLINE	VMWARE	VNC	10.0.0.25	Windows XP
🔍	2B	8	ONLINE	VMWARE	VNC	10.0.0.25	Windows XP
🔍	3A	9	ONLINE	ABSENT	NULL		
🔍	3B	10	ONLINE	ABSENT	NULL		
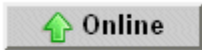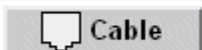
POD 2 - CONTROL SWITCH

SWITCH ID	POD PORT RANGE	BASE VLAN	VLAN POOL
⇄ 2	1-10	110	110-119

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.

The cable chart is continued on the next page.

S1 (Cisco 2960)

CONNECT FROM	USING CABLE	CONNECT TO	
Fastethernet 0/24	CAT-5 Crossover	C/S 2	Port 4
Fastethernet 0/1	CAT-5 Crossover	C/S 2	Port 5
Fastethernet 0/2	CAT-5 Crossover	C/S 2	Port 6
Fastethernet 0/3	CAT-5 Crossover	C/S 2	Port 7
Fastethernet 0/4	CAT-5 Crossover	C/S 2	Port 8
Fastethernet 0/5	CAT-5 Crossover	C/S 2	Port 9
Fastethernet 0/6	CAT-5 Crossover	C/S 2	Port 10
Console	Console Cable	A/S 1	Port 2
Power	Power Cord	SOD 1 APC	Outlet 3

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

The Ethernet interface names show in the cable guidance will be the actual interface names based on your selected hardware. However, the interface names shown for serial ports are relative, not actual. Please consider this when cabling the pod.

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 guide.

Refer to Appendix A of this document for special Eagle Server installation instructions.

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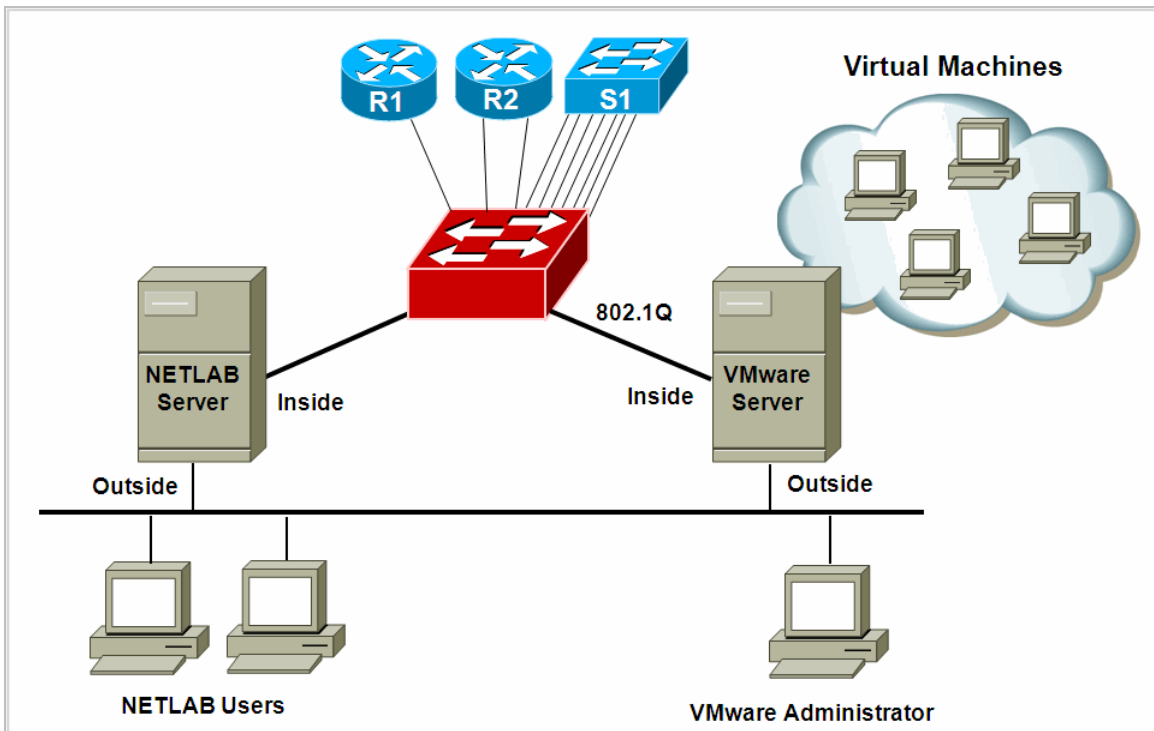
7.2   VMware Virtual Switches and VLANs

VMware Server virtual network adapters and virtual LAN switches (VMnets) are used to connect virtual machines to the pod. Network Fundamentals Pod uses up to **7 VMnets**, 5 are required and would be used for the Server, PC1A, PC1B, PC2A and PC2B. Two are optional and would be used for PC3A and PC3B. Since VMware Server (for Windows) supports 10 virtual switches, it is possible to host up to one complete Network Fundamental Pods on a single VMware Server or two if not installing the optional group 3 (PC3A and PC3B).

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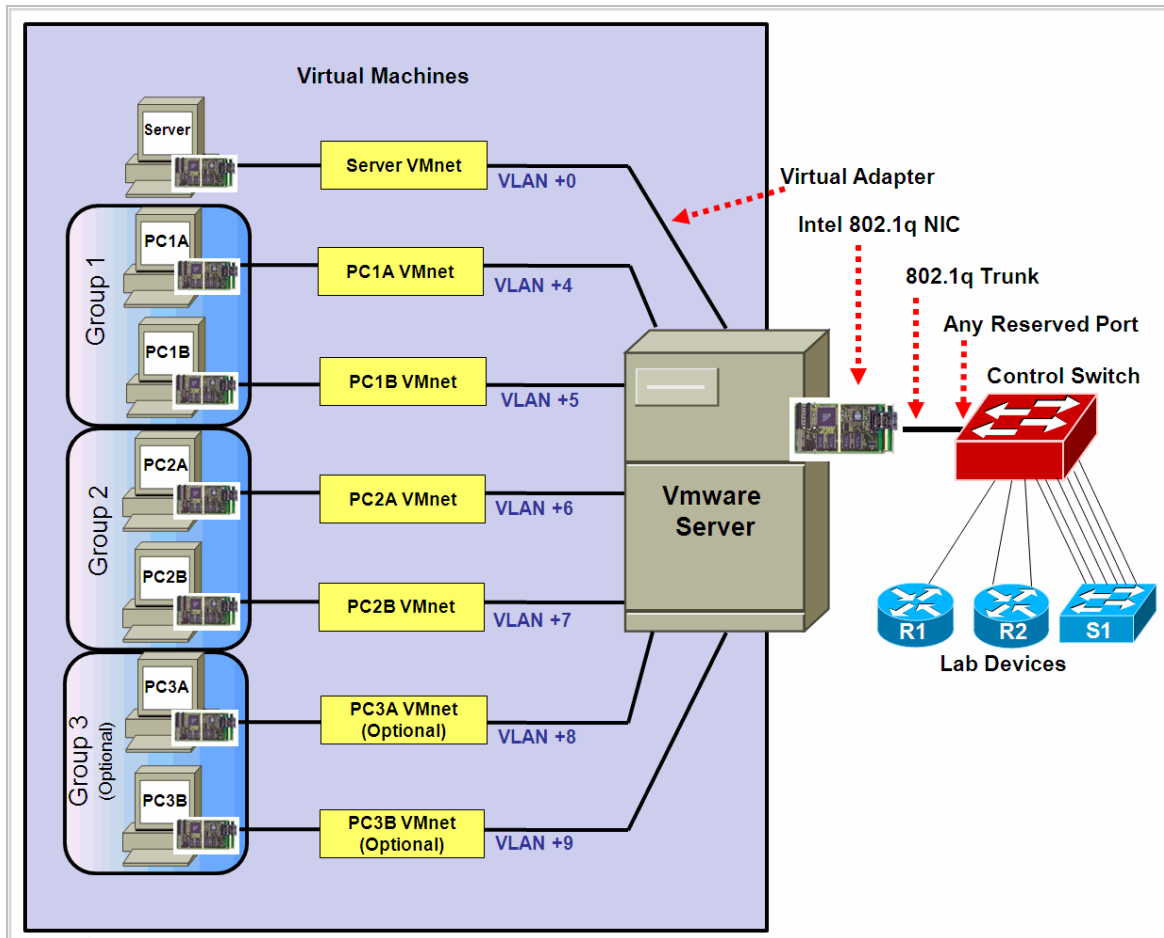
Each NETLAB$_{AE}$ pod is automatically assigned a pool of unique VLAN numbers. You must determine which VLAN numbers correspond to each virtual switch on the VMware server.

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.

In this example, pod 2 uses VLANs 110-119. The base VLAN is 110.

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	Server VMnet	+ 0	= _____	110 + 0 = 110
PC1A	PC1A VMnet	+ 4	= _____	110 + 4 = 114
PC1B	PC1B VMnet	+ 5	= _____	110 + 5 = 115
PC2A	PC2A VMnet	+6	= _____	110 + 6 = 116
PC2B	PC2B VMnet	+7	= _____	110 + 7 = 117
PC3A Optional	PC3A VMnet	+8	= _____	110 + 8 = 118
PC3B Optional	PC3B VMnet	+9	= _____	110 + 9 = 119

7.3   Configure VMware Server Inside Port

Refer to section 6 of the *NETLAB+ Remote PC Guide for VMware Server 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
subinterface. Only the VMware bridge protocol should be checked.
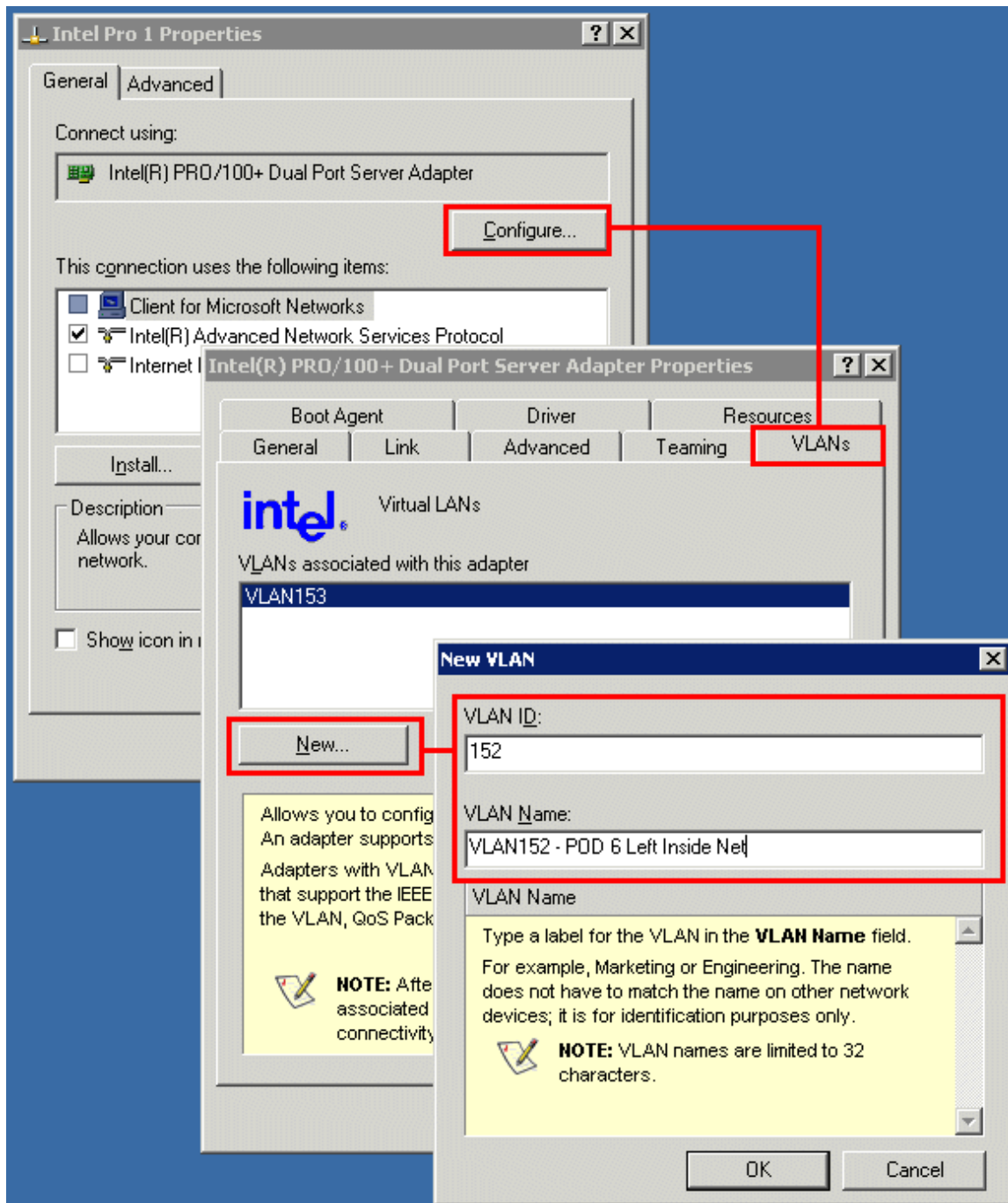
7.4   Create Virtual Switches (VMnet)

Refer to section 6 of the *NETLAB+ Remote PC Guide for VMware Server 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 Server Implementation*.
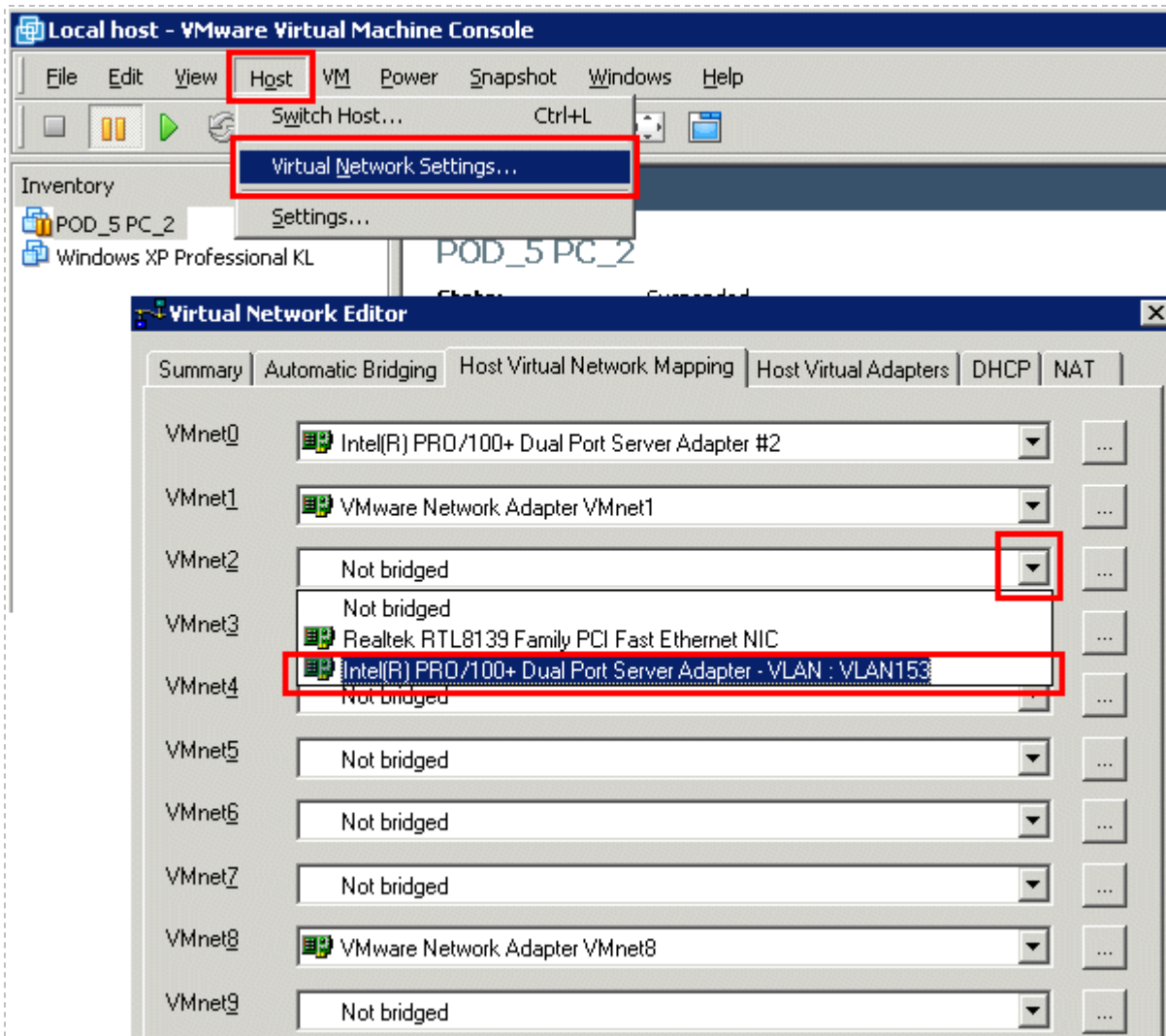
7.5 Binding Virtual Machines to Virtual Switches (VMnet)

Refer to section 7 of the *NETLAB+ Remote PC Guide for VMware Server 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	Server VMnet	+ 0	= _____	110 + 0 = 110
PC1A	PC1A VMnet	+ 4	= _____	110 + 4 = 114
PC1B	PC1B VMnet	+ 5	= _____	110 + 5 = 115
PC2A	PC2A VMnet	+6	= _____	110 + 6 = 116
PC2B	PC2B VMnet	+7	= _____	110 + 7 = 117
PC3A Optional	PC3A VMnet	+8	= _____	110 + 8 = 118
PC3B Optional	PC3B VMnet	+9	= _____	110 + 9 = 119

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.
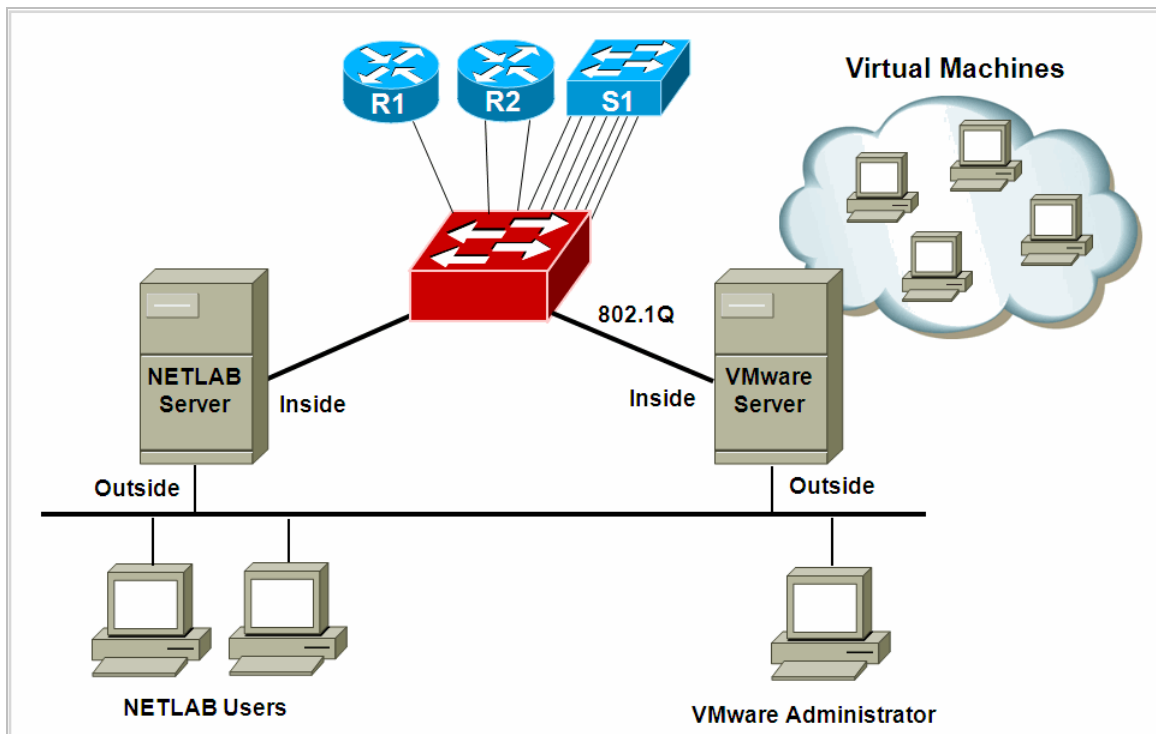
Once you have allocated a reserved port on the control switch, connect the VMware Server inside NIC using a straight through CAT5 cable. Configure the switch port as a trunk and allow only the VLANs that were bound to the VMnets. If your VMware server hosts virtual machines for more than one pod, allow 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 110,114,115,116,117,118,119
 switchport nonegotiate
 no switchport access vlan
 no shutdown
```

7.7   VMware Server(s) on Different Control Switch

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

Alternate Configuration
VMware Server(s) on Different Control Switches

CONTROL SWITCH 2

Network Fundamentals Pod
(10 Ports)

R

VMware GSX Server(s)

802.1Q TRUNK

ALLOW
ALL VLANS

802.1Q TRUNK

ALLOW
RELEVANT
VLANS

R = "Reserved Port"

NETLAB
SERVER

R   R

R

CONTROL SWITCH 1
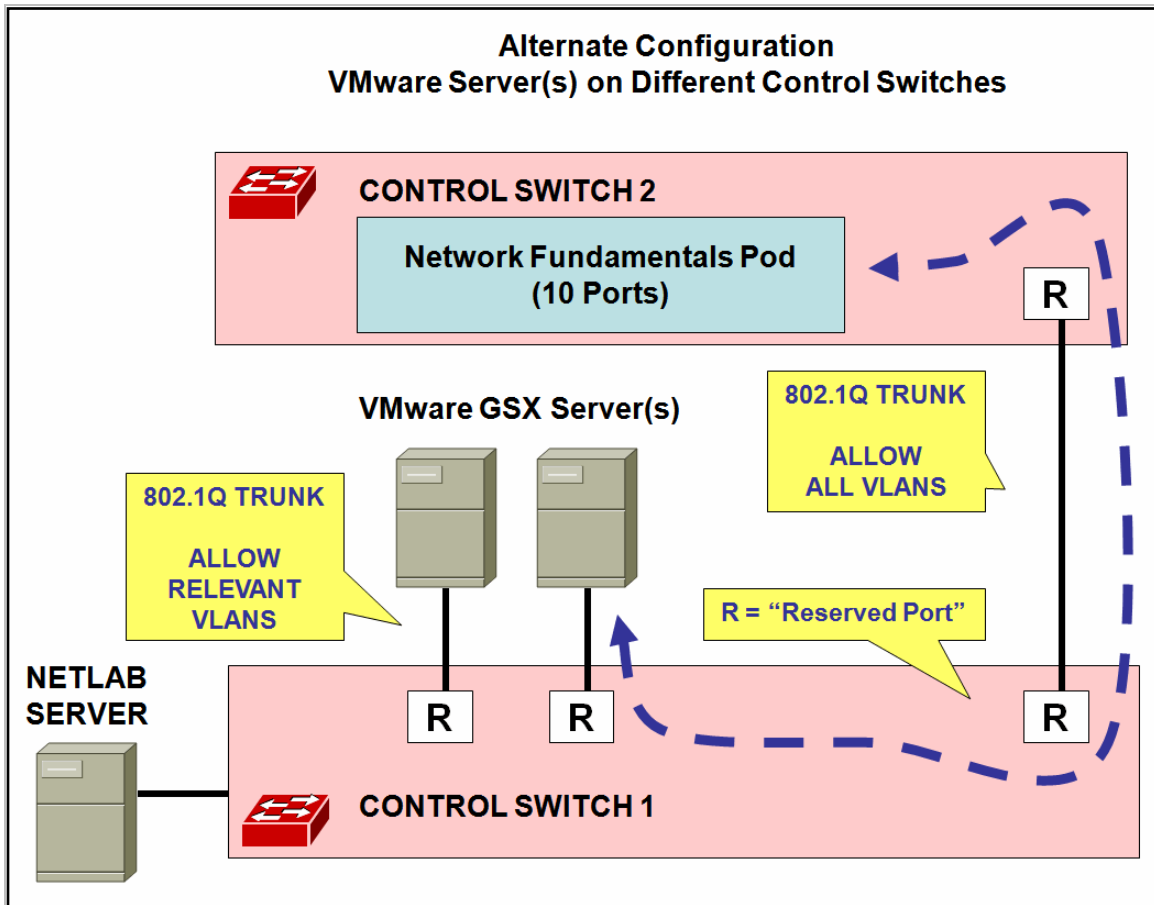
Ports connecting to VMware servers should only allow the VLANs associated with the pods being served. In addition, **switchport nonegotiate** should be used to suppress Dynamic Trunk Protocol (DTP):

```
interface FastEthernet0/23
 switchport mode trunk
 switchport trunk allowed vlan 110,114,115,116,117,118,119
 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 Network Fundamentals Pod requires additional switch configution tasks for successful operation. Using Hyperterm or other terminal, connect to the console port of the control switch in which the Network Fundamentals 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 in this case).

- **spanning-tree bpdufilter enable**
    - Instructs the control switch port not to send and receive spanning tree BPDU frames to and from the lab switch.
    - The spanning tree in the lab must not mingle with the 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 the control switch and the lab switch is trunking.
    - Trunking on ports that should be access ports, combined with BPDU filtering, creates loops that are not prevented by the 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's MAC address from lab switches when users are 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' s MAC address from lab switches when users are 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 7 control switch ports connecting to S1. 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 FastEthernet0/4
 description port to S1 port 24
 switchport mode access
 spanning-tree bpdufilter enable
 switchport nonegotiate
 no keepalive
 no cdp enable

interface FastEthernet0/5
 description port to S1 port 1 (Host PC1A - Group 1)
 switchport mode access
 spanning-tree bpdufilter enable
 switchport nonegotiate
 no keepalive
 no cdp enable
```

```
interface FastEthernet0/6
 description port to S1 port 2 (Host PC1B - Group 1)
 switchport mode access
 spanning-tree bpdufilter enable
 switchport nonegotiate
 no keepalive
 no cdp enable

interface FastEthernet0/7
 description port to S1 port 3(Host PC2A - Group 2)
 switchport mode access
 spanning-tree bpdufilter enable
 switchport nonegotiate
 no keepalive
 no cdp enable

interface FastEthernet0/8
 description port to S1 port 4(Host PC2B - Group 2)
 switchport mode access
 spanning-tree bpdufilter enable
 switchport nonegotiate
 no keepalive
 no cdp enable
```

```
interface FastEthernet0/9
 description port to S1 port 5 (Host PC3A – Group 3 Optional)
 switchport mode access
 spanning-tree bpdufilter enable
 switchport nonegotiate
 no keepalive
 no cdp enable

interface FastEthernet0/10
 description port to S1 port 6 (Host PC3B – Group 3 Optional)
 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

The following discussion applies to NFP switch S1.

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.

```
S1# show boot

BOOT path-list:        flash:c2950-i6q4l2-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 routers and virtual machines have been installed, you should run a pod test to verify that your pod is working. The pod test will detect common configuration and cabling problems.
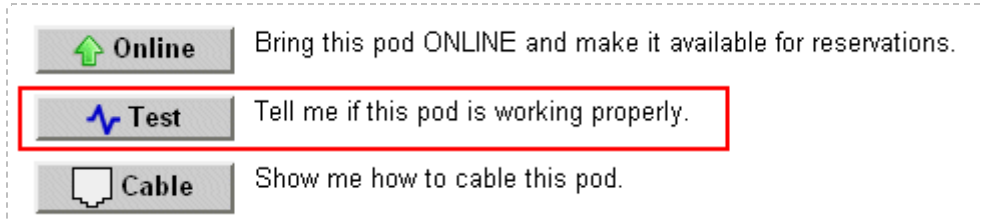
Some tests may take a long time. During the BOOTIOS test, NETLAB_{AE} may have to load the specified IOS image if it is not in flash. Some images are very large and can take up to 30 minutes to program into flash memory.

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

Pod Test   NETLAB+ 4.0.23
Admin   administrator

TESTING POD 2

DEVICE	TYPE	TEST	STATUS	DETAILS
Control Switch 2	Catalyst 2950-24	PING	◔ RUNNING	Pinging control switch at 169.254.1.12
R1	Cisco 1841 (S0/0/x)			
R2	Cisco 1841 (S0/1/x)			
S1	Cisco 2960			
Server	VMWARE			
1A	VMWARE			
1B	VMWARE			
2A	VMWARE			
2B	VMWARE			
3A	ABSENT		SKIPPED	◆ This PC is not implemented
3B	ABSENT		SKIPPED	◆ This PC is not implemented

POD TEST LOG

TESTING POD 2, AE Network Fundamentals Pod, 2 Routers, 1 Switch, 1 Server and 6 PC Clients...

■■ _____ **TESTING IN PROGRESS**   ⊠ STOP

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

10   Finishing Up

10.1   Bring the Pod(s) Back Online

Now you can bring the pod online and make it available for lab reservations. You can bring just this pod online by clicking the ⬆ Online button under Management Options.
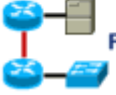
Alternatively, you can click ⬆ Bring All ONLINE on the Equipment Pods page. Choose this option when you have no more additions or modifications to pods or control devices and you wish to put all pods into service.

10.2   Enable Network Fundamentals Pod Exercises

To make the Network Fundamentals 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.

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
◉ CCNA 4.0 Exploration 1	Jane Doe	0	None	None	0	0.0
◉ CCNP 5.0 ISCW	Jane Doe	0	None	None	0	0.0
				Total	0	0.0

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 Network Fundamentals Pod is made available for student, team, or ILT reservations for this class.

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.

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.

9pm	⊕		⊕		⊕	
	⊕		⊕		⊕	
10pm	⊕		⊕		⊕	
	⊕		⊕		⊕	
11pm	⊕		⊕		⊕	
	⊕		⊕		⊕	
	Galactica NETWORK FUNDAMENTALS POD		**POD 2 BASIC ROUTER POD v2** 3 Routers PC Support		**CUATRO ROUTER POD** 4 routers, PCs	

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

Reservation Type	Instructor Access
Equipment Pod	Galactica
Reserve Pod For	Jane Doe
Time Zone	Eastern Time (US & Canada)
Start Time	Thursday January 11, 2007 6:00AM
End Time	Jan ▼ 11 ▼ 2007 ▼ 7 ▼ 30 ▼ AM ▼
Initial Configuration	⦿ restore configs from last AE Cuatro Router Pod reservation (if any) ○ load default configs for exercise ○ no configs loaded (clean)

✓ Confirm Reservation	⬅ Back to Calendar	❌ Cancel

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. Creating a VMware Server VM for Eagle Server

Eagle Server is a pre-built application server that can be downloaded from the Tools section of Academy Connection. This appendix describes how to install and run Eagle Server as a VMware Server virtual machine.

The NDG implementation of Eagle Server allows direct access to the Eagle Server console. The KDE graphical user interface has been disabled to conserve server memory and bandwidth, and to improve remote access performance. KDE is not required.

1. Download the VMware image rar package for the Eagle Server from Academy Connection (viewable from Resources → Tools). Unpackage the file locally on your VMware Server.

2. You may use a utility such as Winrar (http://www.rarlab.com/download.htm) to uncompress the contents of the Eagle Server rar package.

3. Create a new virtual machine using the following settings:

    a. Virtual machine configuration → Custom

    b. Guest O/S → Linux → Other Linux

    c. Virtual machine name → EAGLE_NFPx (where x = pod number)

    d. Access Rights → uncheck the box (or do not make private)

    e. Virtual machine account → Local system account

    f. Processors → One

    g. Memory → 512MB (only initially; after Eagle is installed on HDD, memory requirement is lowered to 256MB)

    h. Network connection → Use bridged networking (will be changed later to use a specific VMnet bound to the VLAN ID corresponding to R1 eth0)

    i. I/O adapter types → use default selection

    j. Disk → Create a new virtual disk

    k. Virtual Disk Type → IDE

    l. Disk capacity → 5GB (uncheck the box for "Allocate all disk space now")

    m. Disk file → use default selection

4. Edit virtual machine settings for the new VM

    a. Select the CD-ROM device from the Hardware tab. Set up the Eagle
        Server VM, so that it will boot the ISO image from the Eagle Server rar
        package downloaded in step 1. Browse to this ISO file and select it.
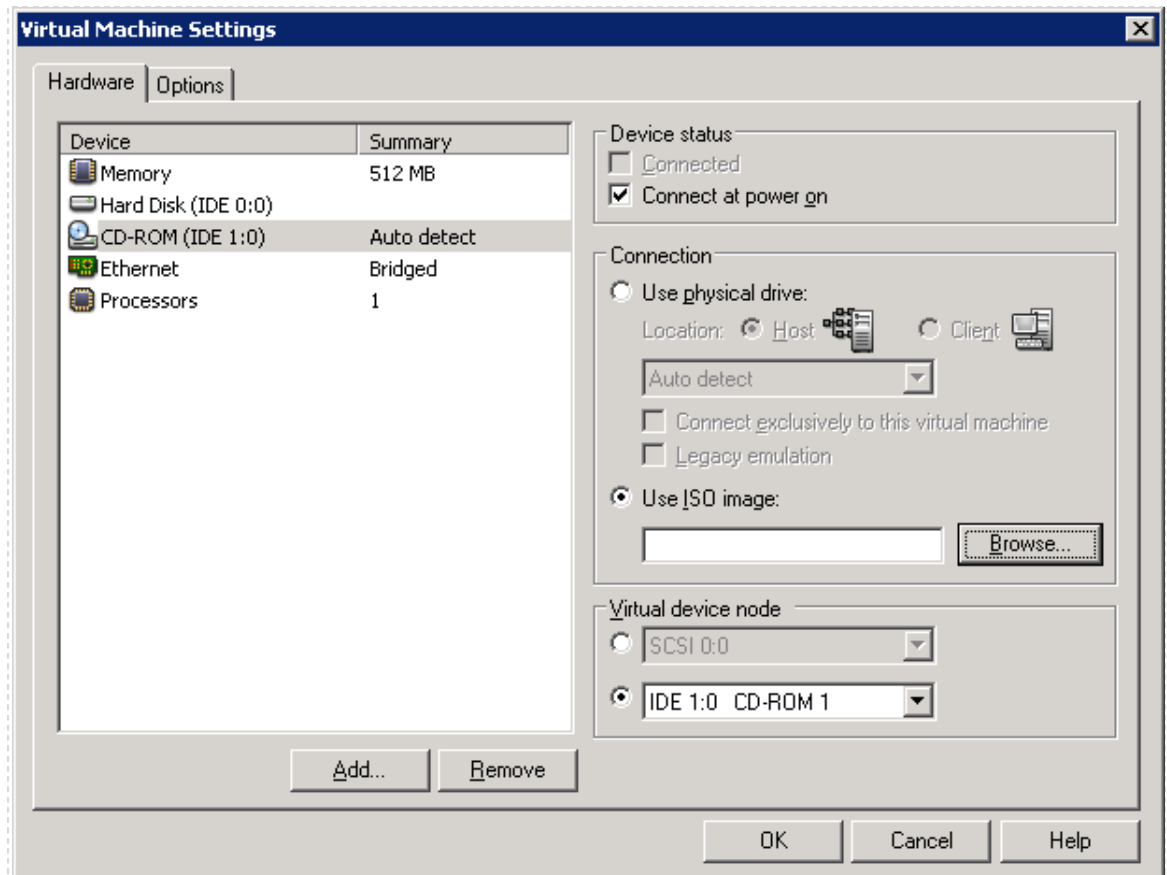
    b. Click on the Options tab and then select Snapshots.
    c. Change "When powering off" to "Ask me"

5. Take an initial snapshot to save your work up until this point.

6. Start this virtual machine.

7. Enter VM BIOS by quickly pressing the F2 button. You will have to do this very
    quickly. Make sure you have clicked inside the console window for the virtual
    machine, as it boots. The mouse will be trapped in the VM console.

8. Change the Boot order of devices. During the installation period, you want the
    CD-ROM to load first. After the installation is complete (step 20 below), you will
    change the BIOS to load the Hard Drive as the first device. Make sure to "Exit
    Saving Changes".

```
                    PhoenixBIOS Setup Utility
   Main      Advanced      Security     Power     Boot     Exit
 ┌────────────────────────────────────────────┬─────────────────────────┐
 │                                             │   Item Specific Help    │
 │    CD-ROM Drive                             ├─────────────────────────┤
 │   +Hard Drive                               │                         │
 │   +Removable Devices                        │ Keys used to view or    │
 │    Network boot from AMD Am79C970A          │ configure devices:      │
 │                                             │ <Enter> expands or      │
 │                                             │ collapses devices with  │
 │                                             │ a + or -                │
 │                                             │ <Ctrl+Enter> expands    │
 │                                             │ all                     │
 │                                             │ <Shift + 1> enables or  │
 │                                             │ disables a device.      │
 │                                             │ <+> and <-> moves the   │
 │                                             │ device up or down.      │
 │                                             │ <n> May move removable  │
 │                                             │ device between Hard     │
 │                                             │ Disk or Removable Disk  │
 │                                             │ <d> Remove a device     │
 │                                             │ that is not installed.  │
 └────────────────────────────────────────────┴─────────────────────────┘
  F1   Help   ↑↓  Select Item    -/+   Change Values     F9   Setup Defaults
  Esc  Exit   ↔   Select Menu   Enter  Select ▶ Sub-Menu  F10  Save and Exit
```

9. Boot into the Eagle Server CD options by pressing <ENTER> at the "boot:" prompt.

10. Before you install the Eagle Server onto the virtual hard disk, you must partition the hard disk into a Linux EXT partition using fdisk. To do this, you will need to Run Linux from CD (option 1).

11. After Eagle Server O/S boots, use the Shell/Konsole to access fdisk.

    a. Login as root by typing "su" and then the password for root, which is "cisco".

    b. Run the fdisk command (should be located at "/adios/sbin/fdisk") for the virtual drive (should be /dev/hda).

```
cisco@Eagle-Server:/var/home/cisco - Shell - Konsole
Session  Edit  View  Bookmarks  Settings  Help
[cisco@Eagle-Server cisco]$ su
Password:
[root@Eagle-Server cisco]# /adios/sbin/fdisk /dev/hda
Device contains neither a valid DOS partition table, nor Sun, SGI or OSF disklabel
Building a new DOS disklabel. Changes will remain in memory only,
until you decide to write them. After that, of course, the previous
content won't be recoverable.


The number of cylinders for this disk is set to 10402.
There is nothing wrong with that, but this is larger than 1024,
and could in certain setups cause problems with:
1) software that runs at boot time (e.g., old versions of LILO)
2) booting and partitioning software from other OSs
   (e.g., DOS FDISK, OS/2 FDISK)
Warning: invalid flag 0x0000 of partition table 4 will be corrected by w(rite)

Command (m for help):
```

c. Type m for help. Then type p to print the partition table. There will be no partition table yet, however you should see a 5GB drive available for partitioning (/dev/hda).

```
cisco@Eagle-Server:/var/home/cisco - Shell - Konsole
Session  Edit  View  Bookmarks  Settings  Help
Command (m for help): m
Command action
   a   toggle a bootable flag
   b   edit bsd disklabel
   c   toggle the dos compatibility flag
   d   delete a partition
   l   list known partition types
   m   print this menu
   n   add a new partition
   o   create a new empty DOS partition table
   p   print the partition table
   q   quit without saving changes
   s   create a new empty Sun disklabel
   t   change a partition's system id
   u   change display/entry units
   v   verify the partition table
   w   write table to disk and exit
   x   extra functionality (experts only)

Command (m for help): p

Disk /dev/hda: 5368 MB, 5368709120 bytes
16 heads, 63 sectors/track, 10402 cylinders
Units = cylinders of 1008 * 512 = 516096 bytes

   Device Boot      Start         End      Blocks   Id  System

Command (m for help):
```

d. Type n to add a new partition. Select p for primary partition and use number 1. Allocate the 1st and last cylinder, or the whole virtual hard drive for the partition size. When done, type p to print the new partition table. You should see /dev/hda1 now. Write the partition table to disk and exit.

```
cisco@Eagle-Server:/var/home/cisco - Shell - Konsole                    _ 🗗 ✕
Session  Edit  View  Bookmarks  Settings  Help
Command (m for help):
Command (m for help):
Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-10402, default 1):
Using default value 1
Last cylinder or +size or +sizeM or +sizeK (1-10402, default 10402):
Using default value 10402

Command (m for help): p

Disk /dev/hda: 5368 MB, 5368709120 bytes
16 heads, 63 sectors/track, 10402 cylinders
Units = cylinders of 1008 * 512 = 516096 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/hda1              1       10402     5242576+   83  Linux

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
[root@Eagle-Server cisco]#
```

12. Logout and Restart the Eagle Server. Press <ENTER> at the "boot:" prompt to load CD options again.

13. Select "installEXT" to load Eagle Server on our newly created /dev/hda1 partition. Type "/dev/hda1" as the device name.

14. Proceed with installation on /dev/hda1? (y/n) y <ENTER>

15. When the installation is complete you will press <ENTER> to return to the CD options menu.

16. You may halt the VM and just Power Off.

17. Edit virtual machine settings after the VM is off and back at the main VMware Console menu.

   a. Change the Memory allocation to 256MB. Now that the VM is running from HDD, we can reduce from 512MB.

   b. Change the CD-ROM device to not Connect at power on (uncheck box). Then select the Connection to use the physical drive instead of the ISO image. Since we have installed Eagle Server to the VMDK (or virtual disk), we no longer need the Eagle Server ISO image.

18. Start this virtual machine.

19. Enter VM BIOS by quickly pressing the F2 button. You will have to do this very quickly. Make sure you have clicked inside the console window for the virtual machine, as it boots. The mouse will be trapped in the VM console.

20. Change the Boot order of devices. During the installation period, you needed the CD-ROM to load first. Now that the installation is complete, you will change the BIOS to load the Hard Drive as the first device (you can use CD-ROM as the second device). Make sure to "Exit Saving Changes".

21. Eagle Server O/S should boot from the hard drive. You are now ready to install VMware Tools to improve the quality of the graphics display, keyboard, video, and mouse.

22. Install VMware Tools.

   a. VMware Console → VM → Install VMware Tools...

   b. Mount the cdrom device and install the TAR file into the tmp directory with the following commands:

```
$ su
Password: cisco
# mount /dev/cdrom /media/cdrom
# cd /tmp
# tar zxf /media/cdrom/VMwareTools-1.0.3-44356.tar.gz
# umount /media/cdrom
```

   c. Run the VMware Tools installer.

```
# cd vmware-tools-distrib
# ./vmware-install.pl
```

   d. Answer the questions about default directories. The default settings should be OK.

   e. Run the configuration program. The VMware Tools installer should automatically try to invoke this command for you.

```
vmware-config-tools.pl
```

   f. Continue with the configuration by using the default settings until you are asked about the display resolution.

   g. Change your display size to "800x600".

   h. The VMware Tools installation should be complete. However, you will need to setup ethernet0 and restart X windows.

   i. Configure eth0 for Eagle Server:

```
# cd /etc/sysconfig/network-scripts
```

> # cp –p bak.ifcfg-eth0 ifcfg-eth0
>
> # mcedit ifcfg-eth0
>
> DEVICE=eth0
> BOOTPROTO=none
> ONBOOT=yes
> IPADDR=192.168.254.254
> IPMASK=255.255.255.0

j. Exit mcedit with F10, making sure to save your changes.

k. Bring up ifcfg-eth0.

> # ./ifup ifcfg-eth0

l. The Eagle Server should be ready for networking:

> # /sbin/ifconfig

m. Log off of the root account.

> # exit

n. Since VMware Tools was installed in an X window session, restart X windows (or just simply Logout and Restart Computer).

o. In a Shell/Konsole session, launch the VMware Tools background application.

> $ vmware-toolbox &

p. You can run VMware Tools as root or as a normal user. The VMware-toolbox ensures you have access to all VMware Tools features.

q. You can minimize the VMware Toolbox window.

r. You may reboot the Eagle server to verify that the VMware Toolbox will start up on next boot.

23. Although the Eagle Server normally boots into run level 5 (X windows), we recommend changing the default run level to 3.

a. The X Server, or GUI interface, of the Eagle Server may consume critical virtual resources. In addition, the Fedora Core 3 platform's X Server may not work well with VMware Tools. The performance drain may be noticed in a remote pod setting.

      b.   From the Terminal/Konsole window edit the /etc/inittab file and change the default runlevel to 3 from 5:

> $ su
> # mcedit /etc/inittab
> id:3:initdefault

      c.   Exit mcedit and save your changes.

      d.   Reboot the Eagle server to verify if it boots into run level 3 (command prompt only).

24. Some important services, such as named (DNS service), may not start automatically after Eagle Server boots. You can typically run the command 'chkconfig --list' to verify which services are running and at which run level.

Note, if the display is hard to view, run 'chkconfig --list | less'.

      a.   Login to Eagle Server as root (password cisco).

      b.   A simple way to edit running services is by running setup. From the command line type 'setup'. A graphical menu will open.

```
ADIOS version 4 (based on Fedora Core 3)
Kernel 2.6.12 on an i686

Eagle-Server login: root
Password:
Last login: Mon Sep 24 15:11:08 on tty1
[root@Eagle-Server ~]# setup_
```

c. From the 'Choose a Tool' menu select 'System Services' and press <ENTER>.

```
Text Mode Setup Utility 1.17                          (c) 1999-2004 Red Hat, Inc.

                          ┤ Choose a Tool ├

                    Authentication configuration
                    Firewall configuration
                    Keyboard configuration
                    Mouse configuration
                    Network configuration
                    Printer configuration
                    System services
                    Timezone configuration
                    X configuration


                         Run Tool        Quit




   <Tab>/<Alt-Tab> between elements  |   Use <Enter> to edit a selection
```
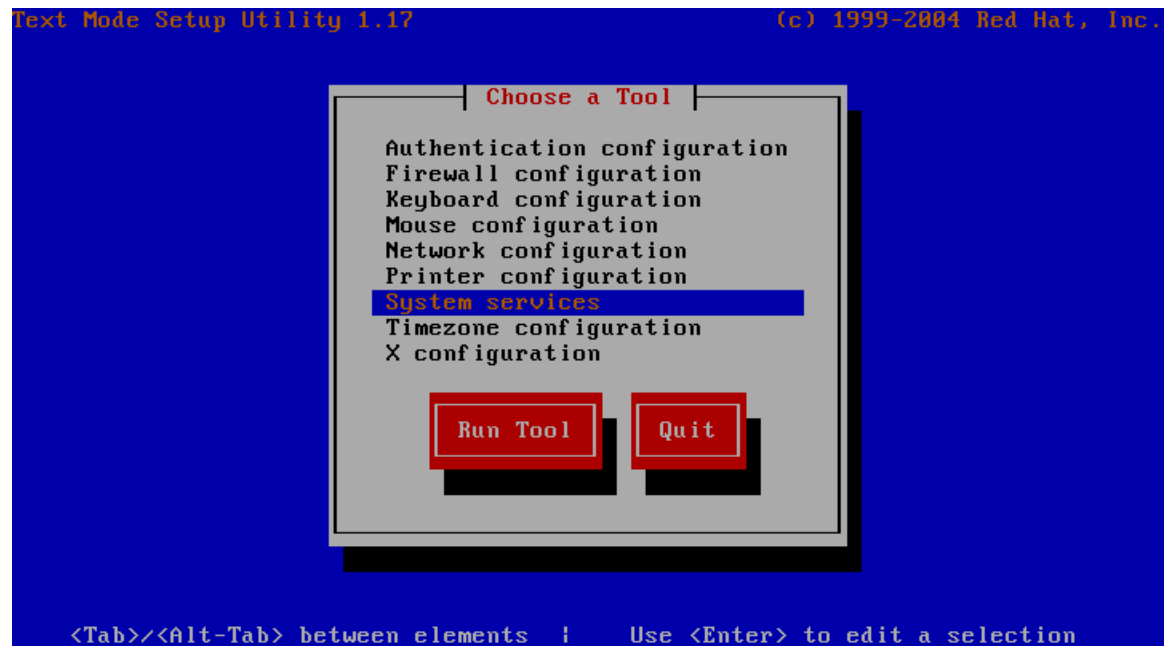
d. Scroll down through the listed services until you get to 'named'. Press <SPACEBAR> inside the selection box for the named service. You will notice an '*' in the box. Press <TAB> to select OK and exit the screen.

```
ntsysv 1.3.11.1 - (C) 2000-2001 Red Hat, Inc.


                          ┤ Services ├
          What services should be automatically started?

                    [ ] microcode_ctl
                    [ ] mysqld
                    [*] named
                    [ ] netdump                          #
                    [*] netfs
                    [ ] netplugd
                    [*] network
                    [ ] nfs


                      Ok                    Cancel




Press <F1> for more information on a service.
```
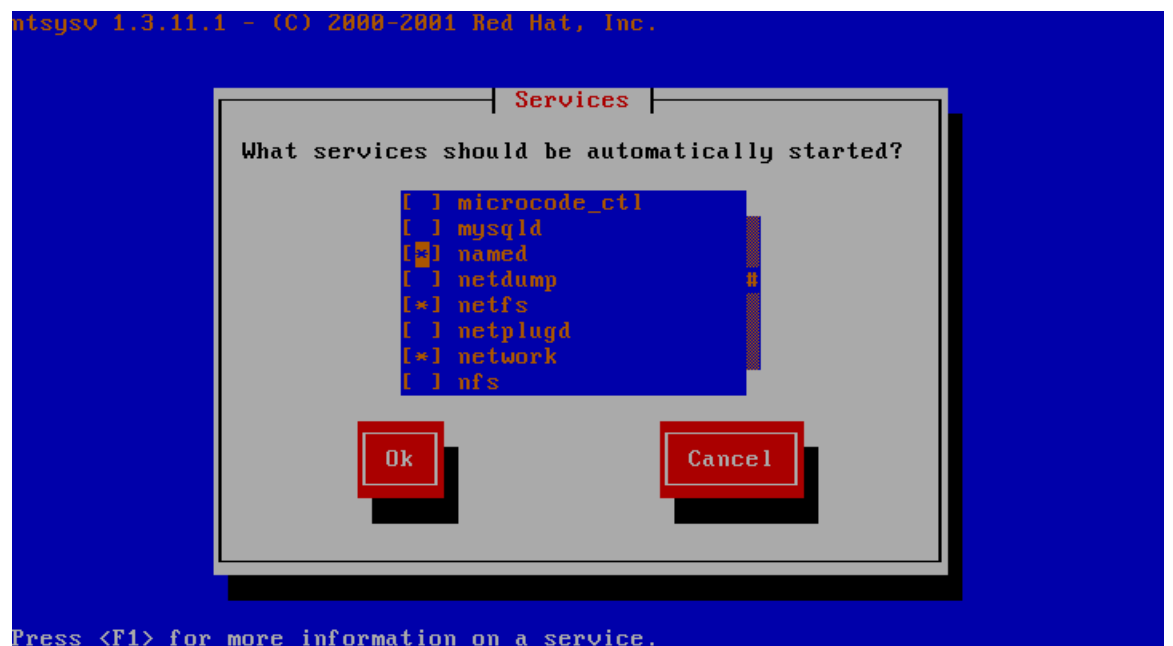
e. From the 'Choose a Tool' menu you may now Quit.

f. You should now notice that the named service will be 'on' for runlevels 3 and 5 (using the 'chkconfig --list' command).

g. Reboot Eagle Server to see if the named process will appear in the process list (you can view the running process list by typing 'ps aux'). The command for restart is 'shutdown -r now'.

h. After Eagle Server boots, login as root and view the running process list. You should see a process belonging to the named user.

25. You are now ready to power down the Eagle Server and change the VMX file to add the VNC settings so you may have remote access from a NETLAB+ pod.

a. Logout and Turn Off Computer.

b. Open the VMX file for the Eagle Server with notepad.

c. Add the 3 lines of VNC settings from the NETLAB+ equipment pod settings for the Eagle Server VM. Make sure to exit and save changes.

26. Take a final snapshot of the Eagle Server VM.