



Remote PC Guide for VMware Implementation Using VMware Server 2.x

Document Version: **2010-08-12**



This guide is a primer for adding remotely accessible PC or servers into your NETLAB Academy Edition® or NETLAB Professional Edition® equipment pods using the [VMware Inc.](#) virtualization product VMware Server 2.x.

This guide covers features available in NETLAB+ version **2009.R1** and later. The details of this guide are specific to **VMware Server version 2.x**.

Documentation for interfacing with other versions of VMware virtualization products can be found in their respective *Remote PC Guide for VMware Implementation* guides.

Copyright © 2010, Network Development Group, Inc.
www.netdevgroup.com

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

VMware is a registered trademark of VMware, Inc. Cisco, IOS, Cisco IOS, Networking Academy, CCNA, and CCNP are registered trademarks of Cisco Systems, Inc.

Part 1	Background	6
1.1	What is a Remote PC?	6
1.2	What Can Users Do With a Remote PC?	7
1.3	What is a Virtual Machine?	8
1.4	What Does VMware Provide?	9
1.5	How Do NETLAB+ and VMware Servers Work Together?.....	11
Part 2	Planning	13
2.1	What Software Is Required?.....	13
2.1.1	Product Licensing.....	14
2.1.2	VMware Hosting Product Comparison	15
2.1.3	NETLAB+ Support Summary for VMware Server 2.x	16
2.1.4	NETLAB+ Known Issues for VMware Server 2.x.....	17
2.1.4.1	10 Virtual Switch Limit.....	17
2.1.4.2	Continuous High CPU Utilization Causes Timeouts.....	18
2.1.4.3	NETLAB+ Not Tested With All Guest Operating Systems.....	18
2.1.4.4	NETLAB+ Does Not Support Novell Netware	18
2.1.4.5	NETLAB+ Does not Support DLink Network Cards	18
2.1.4.6	NETLAB+ Does not Support Broadcom Networking Adapters.....	19
2.1.4.7	Intel PROSet Device Manager Tabs Not Visible Through Terminal Svcs.	19
2.1.5	Upgrading From VMware Server 1.x to 2.x	20
2.2	VMware Host Hardware Requirements	21
2.3	How Many VMware Server Host Systems Do I Need?	23
Part 3	VMware Host System Setup	28
3.1	Install and Configure Microsoft Windows Server Operating System.....	28
3.1.1	Install Chipset Drivers	28
3.1.2	Configure RAID.....	29
3.1.3	Disable IIS (Recommended)	29
3.2	Install Advanced Networking Drivers and Utilities.....	30
3.3	Networking Models	32
3.3.1	VMware Host Connectivity Using ISEC	34
3.3.2	VMware Host Connectivity Using IMAN	36
3.3.3	VMware Host Connectivity Using OMAN	38
3.4	Inside Interface Tasks	40
3.4.1	Open Network Connections Window	40
3.4.2	Select and Rename Inside Interface	41
3.4.3	Unbind Protocols from Inside Physical Interface.....	42
3.4.4	Understanding VLAN 1 and Bridged VLANs.....	43
3.4.5	Creating VLAN 1 using an Intel Networking Adapter.....	44
3.4.6	Configure VLAN 1 Protocols and TCP/IP Settings	49
3.4.7	Establishing the Inside Connection	52
3.4.7.1	Allocated Reserved Port on Control Switch for Inside Connection	52
3.4.7.2	Configure Reserved Control Switch Port for Inside Connection	53
3.4.7.3	Configure Trunking Between Multiple Control Switches.....	53
3.4.7.4	Connect Inside Interface and Verify Link	54
3.4.7.5	Verify VLAN 1 Connectivity	54

3.5	Outside Interface Tasks	56
3.5.1	Open Network Connections Window	56
3.5.2	Select and Rename Outside Interface	57
3.5.3	Configure Outside Interface Protocols	57
3.5.4	Configure Outside Interface TCP/IP Settings	59
3.5.5	Connect and Verify Connectivity	60
3.6	Disable Windows Firewall.....	62
3.7	Enable Remote Desktop (Recommended)	63
3.8	Installing VMware Server Software.....	64
3.9	Creating a NETLAB+ Management Account	70
3.10	Granting Permissions.....	71
3.11	Maximizing Available Virtual Switches	73
Part 4	Adding Virtual Machines	75
4.1	Creating a New Virtual Machine (VM).....	75
4.1.1	Selecting the Guest Operating system.....	77
4.1.2	Selecting Memory and Processors.....	78
4.1.3	Creating a Virtual Hard Disk.....	79
4.1.4	Adding a Network Adapter	80
4.1.5	Selecting CD/DVD Properties.....	82
4.1.6	Selecting Floppy Drive Options.....	84
4.1.7	Selecting USB Controller Options	85
4.1.8	Verifying the Virtual Machine Configuration Settings.....	86
4.2	Setting Snapshot Options	87
4.3	Installing a Guest Operating System	89
4.4	Editing the Virtual CD/DVD Device	89
4.5	Installing the VMware Tools.....	92
4.6	Setting the Virtual Machine Display Properties for Remote Access	94
4.7	Adjusting Visual Effects	96
4.8	Disabling the Desktop Background.....	97
4.9	Adding Software Applications	98
4.10	Taking a Snapshot of Your Virtual Machine	98
4.11	Remote PC Settings (for New Pods)	99
4.12	Modifying PC Settings.....	102
4.13	Configuring Remote Display Options	103
4.14	Taking a New Snapshot of the Virtual Machine	105
4.15	Verify the Virtual Machine	106
Part 5	Connecting Virtual Machines to Real Lab Devices	110
5.1	Determining Which VLAN Numbers Are Used by Your Pod	111
5.1.1	Determining VLANs Example 1 – Cuatro Router Pod	112
5.1.2	Determining VLANs Example 2 – Cuatro Switch Pod.....	114
5.2	Creating VLAN Adapters	116
5.2.1	Create a Proper VLAN Adapter using an Intel Adapter	116
5.2.2	Uncheck the Unused Protocols from Network Properties	118
5.3	Mapping VLAN interfaces to available Virtual Networks (VMnets).....	120
5.4	Configure a VM to use the correct VMnet (using VI Web Access).....	121

5.5	Deleting the Placeholder VLAN 3	123
Part 6	Verifying Connectivity and Troubleshooting	125
6.1	Verifying Connectivity Between Virtual Machines and Lab Gear	125
6.2	Review and Modify VM Settings For an Existing Virtual Machine	131
6.3	The Most Frequently Encountered VMware Issues	137
Appendix A	Using Reserved Virtual Networks for External Connectivity.....	142
Appendix B	Copying VMDK File to Clone Virtual Machines	145
Appendix C	Contacting NDG for Technical Support	147
Appendix D	Upgrading from VMware Server 1.0 and GSX to VMware Server 2.x...	148
Appendix E	Experimental Use of a Broadcom Networking Adapter	150
Appendix E.1	VLAN Support for Broadcom Networking Adapters.....	150
Appendix E.2	Creating VLAN 1 – Broadcom Adapters.....	151
Appendix E.3	VLAN Support for Broadcom Networking Adapters.....	156
Appendix F	Resolving Errors to the Configuration File	158

OBJECTIVES

PART 1 - Background

- What is a remote PC?
- What can users do with a remote PC?
- What is a virtual machine?
- What does VMware Server 2.x provide?
- How does NETLAB+ integrate with VMware Server?

PART 2 – Planning

- What software is needed?
- What hardware is needed?
- How many VMware host servers do I need?

PART 3 – VMware Server Setup

- Install Microsoft Windows Server operating system
- Create NETLAB+ management account
- Configure physical networks
- Install VMware Server software
- Prepare for virtual networking

PART 4 – Adding Virtual Machines

- How do I add a virtual machine to my VMware Server?
- How do I make a virtual machine accessible to NETLAB+ users?

PART 5 – Connecting Virtual Machines to Real Lab Devices

- Connecting to an External Network
- Creating VLAN interfaces
- Configuring VMnets

PART 6 – Verifying Connectivity and Troubleshooting

- Verifying Connectivity Between Virtual Machines and Lab Gear
- Identify and resolve the most frequently encountered VMware issues.

Part 1 Background

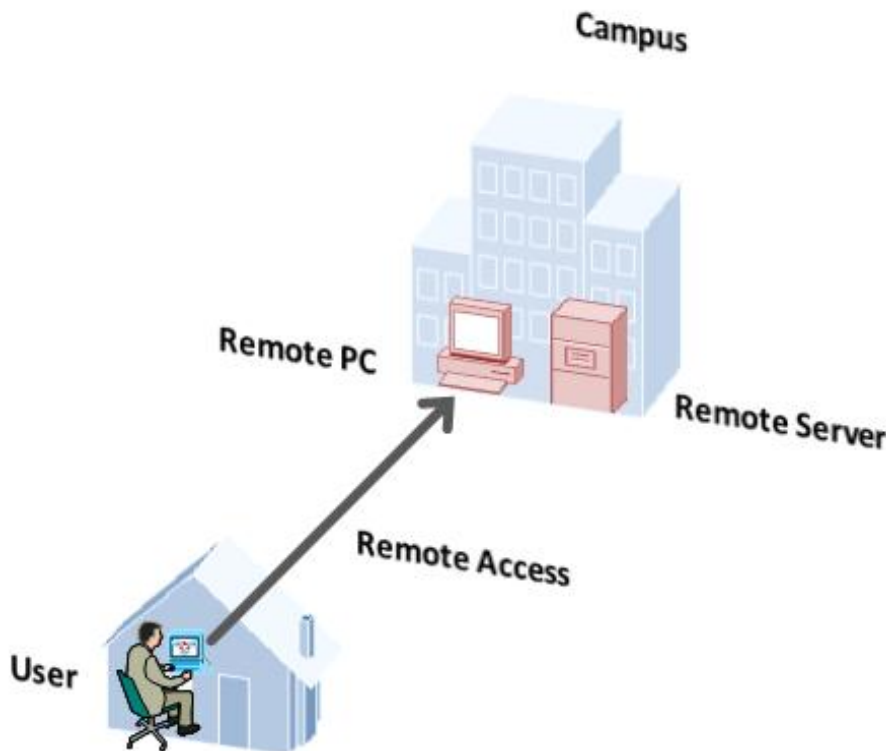
This section builds a fundamental understanding of how remote PCs, virtualization and NETLAB+ work together.

Objectives

- What is a remote PC?
- What can users do with a remote PC?
- What is a virtual machine?
- What does VMware Server 2.x provide?
- How does NETLAB+ integrate with VMware Server?

1.1 What is a Remote PC?

A *remote PC* is a personal computer or server that can be remotely accessed from another PC. *Remote access* allows a user to have full access to the keyboard, video, and mouse of the remote PC. NETLAB+ provides built-in client software for remote access, which is loaded automatically via the user's web browser.



1.2 What Can Users Do With a Remote PC?

Users can remotely access the keyboard, video, and mouse of a virtual machine. NETLAB+ also provides special features such as shared simultaneous access, interfacing with real lab equipment (routers, switches, and firewalls), remotely powering a PC on or off, and restoring the PC to a clean state. This offers a wide range of possibilities. Here are a few scenarios that are being used today.

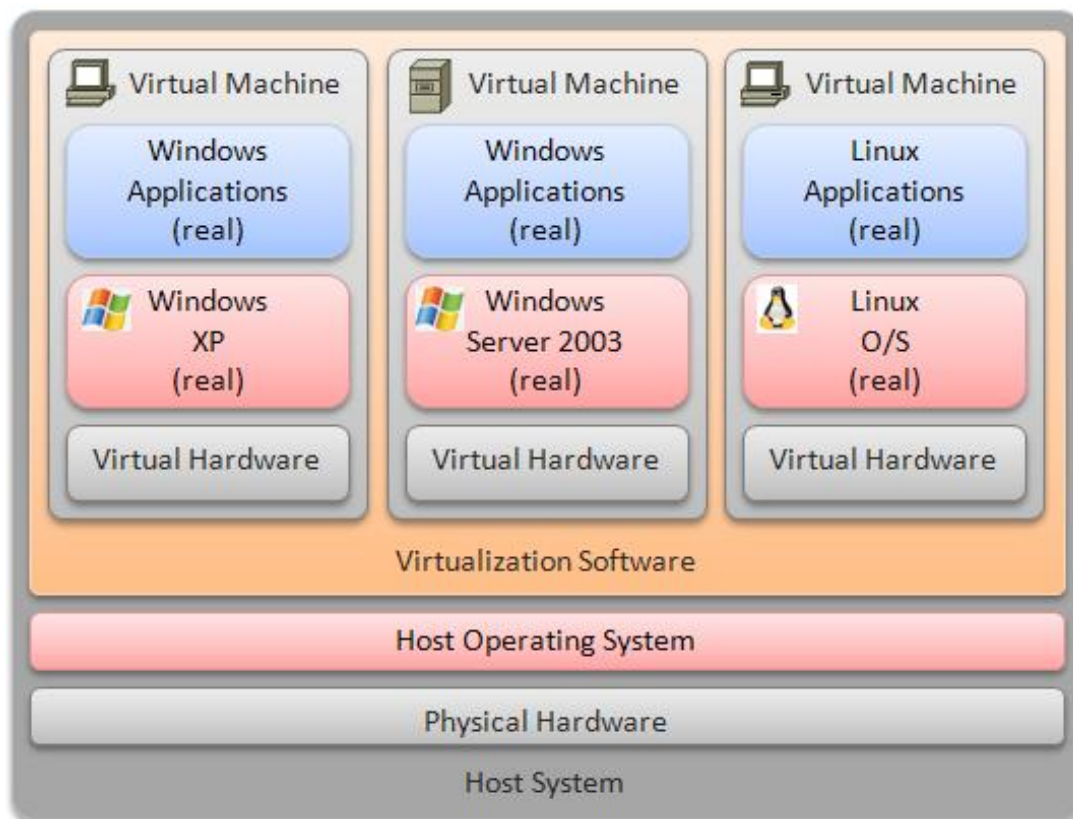
- **Application Service.** Provides students with access to real operating systems and application software, without distributing software or licenses.
- **Distance Learning.** Provides remote instructor-led training by allowing simultaneous shared access to remote PCs and remote servers. Several users can connect to and share the remote PC's graphical user interface at the same time. Using NETLAB+, students can observe what the instructor is doing on the remote PC, and vice-versa.
- **Resource Scheduling.** Provides controlled, scheduled usage to limited hardware resources.
- **License Management.** Limits the number of licensed operating systems or software applications that can be used at the same time.
- **Online General IT Training.** Provides on-line access to real operating systems and real application software. Using NETLAB+, remote PCs can be completely isolated from production networks, providing a safe environment for instructors and students to do things that are not typically allowed on production networks. Students can safely experience administrative privileges in complex computing environments. You can now provide labs that are not practical for students to set up at home, or scenarios that would be too difficult to set up by new IT students.
- **Online Lab Delivery.** Provides remote delivery of student assignments and lab work.
- **Online Network Training.** Provides online delivery of network training. Remote PCs can be interface with real lab equipment, such as routers, switches, and firewalls, all of which can be accessed remotely using NETLAB+.
- **Online Security Training.** Provides online delivery of security training. Using NETLAB+, remote PCs can be completely isolated from production networks, providing a safe environment for instructors and students to do things that are not typically allowed on production networks. This might include configuring PCs and lab devices using administrator privileges, installing new software, capturing network traffic, experimenting with firewalls and VPNs, running malicious

software, and scanning networks. At the end of the lab reservation, NETLAB+ will undo any changes.

1.3 What is a Virtual Machine?

In NETLAB+, a *virtual machine* is a remote PC or remote server that runs on virtualized hardware. Although the hardware is virtualized, real operating systems and real application software can still be used; virtual hardware appears to be real as far as the software is concerned. In fact, the software running on a virtual machine is allowed to execute instructions directly on the real CPU. This provides relatively good performance, comparable to actual hardware in most cases. A special process known as the *hypervisor* manages workload among virtual machines to ensure that each application has time to execute.

The result is that virtualization allows you to host real operating systems and real application software with fewer hardware resources.



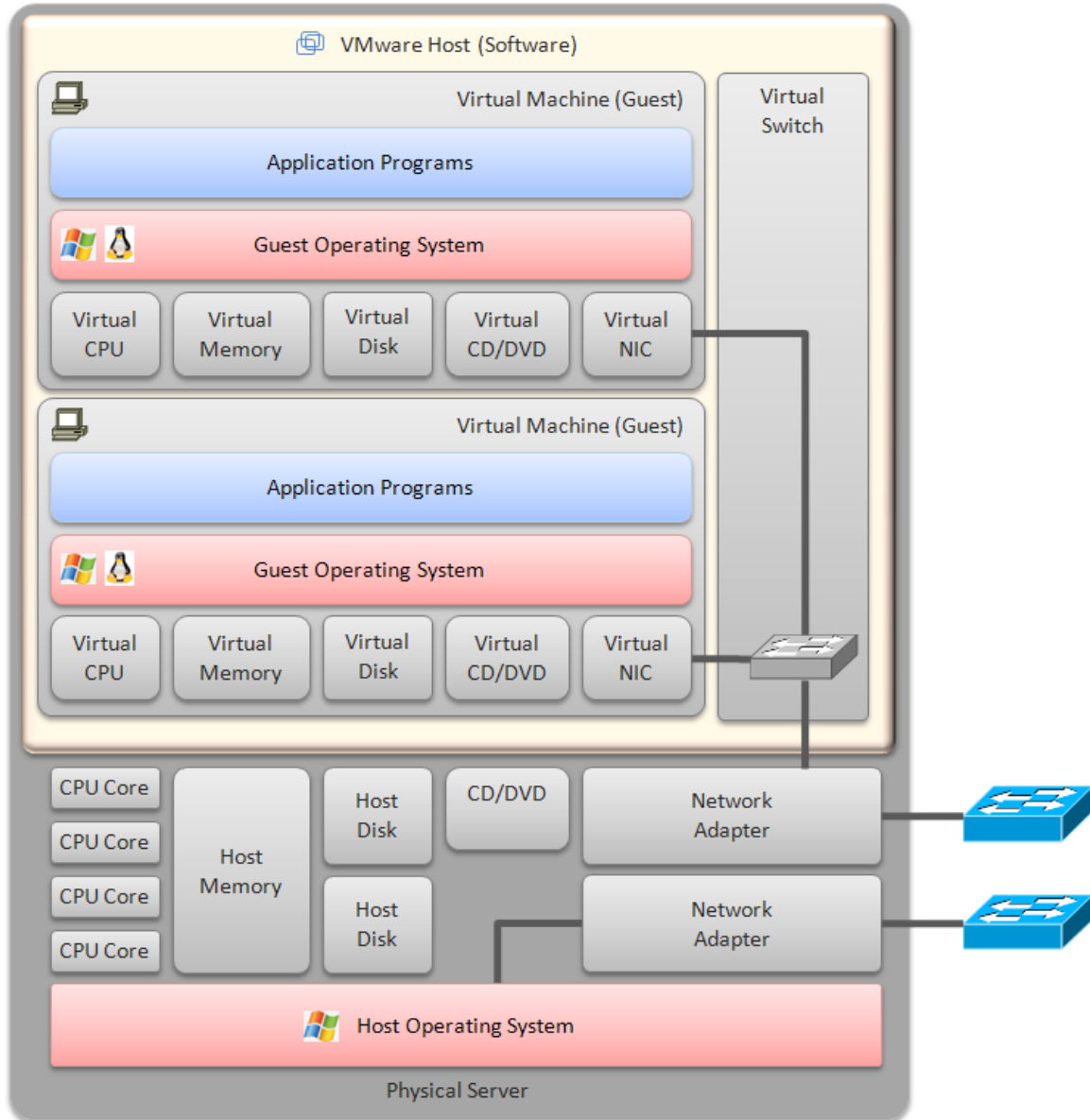
To implement virtual machines, the NETLAB+ software interfaces with third party virtualization products that run on separate servers (not on the NETLAB+ server). This guide is specific to VMware Server 2.x, from VMware Inc.

NETLAB+ provides remote PC access solutions for both virtual machines and real *standalone* PCs. However, due to the rapid progress of virtualization technology and the numerous benefits it provides, NDG recommends that all new remote PCs be implemented using virtual machines. New development and support for standalone PC interfacing is no longer provided by NDG.

1.4 What Does VMware Provide?

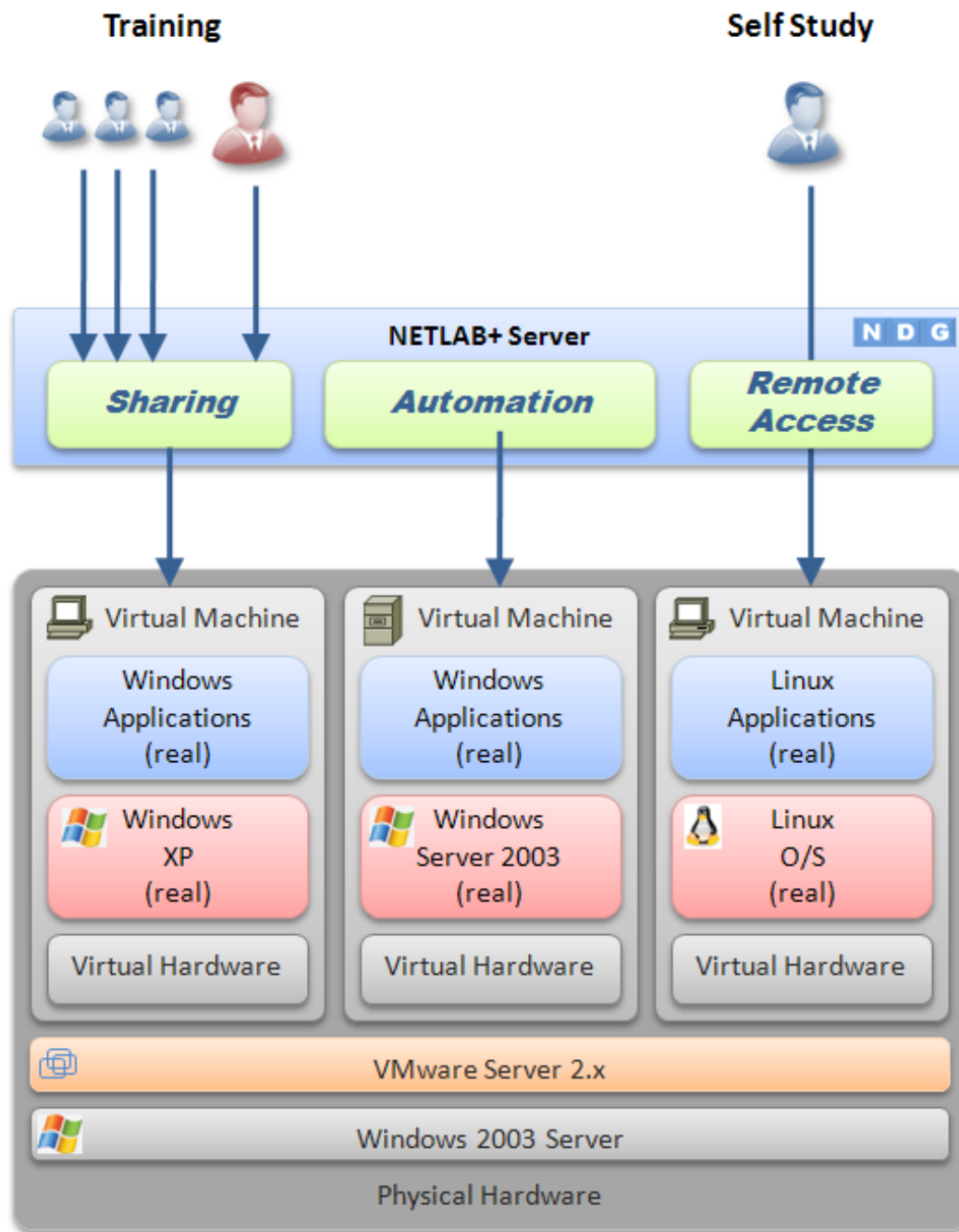
VMware provides *virtualization server* software. The software abstracts computing resources so that several PCs or servers can run on the same physical server.

Each NETLAB+ remote PC or remote server runs inside of a virtual machine. VMware provides virtual CPU, virtual memory, virtual disk drives, virtual networking interface cards, and other virtual hardware for each virtual machine. VMware also provides the concept of a virtual networking switch. Virtual switches can be connected to real networks via host network adapters, allowing virtual machines to connect to real networks.



1.5 How Do NETLAB+ and VMware Servers Work Together?

NETLAB+ interfaces with VMware virtualization servers using protocols and application programming interfaces (API) to incorporate virtual machines (PCs and servers) into the lab environment, and make them remotely accessible in an easy-to-use, intuitive way. It also facilitates sharing so that multiple users can access the keyboard, video and mouse of a virtual machine simultaneously.



Here is list of features and benefits provided by NETLAB+, working in conjunction with VMware virtualization servers.

- The keyboard, video and mouse of each virtual machine can be accessed without a “backdoor” network or interface on the virtual machine. Access to a virtual machine is proxied through NETLAB+ and the virtualization host system, similar to KVM-over-IP hardware solutions.
- No special client software (other than Java) is required on the user’s computer. NETLAB+ will download its remote PC access application to the client whenever the user clicks on a PC.
- Multiple users can share access to a virtual machine simultaneously.
- NETLAB+ *multiplexes* virtual machine traffic using a single IP address and two TCP ports. It also provides a front-end to the virtual machine environment, so that virtualization servers and virtual machines do not have to be placed on production networks. This significantly increases security and eases firewall administration.
- If the user has a valid lab reservation, NETLAB+ will proxy client access to the keyboard, video and mouse of the virtual machine. This access is terminated when the lab reservation completes, ensuring that users of different reservations do not interfere with each other.
- NETLAB+ supports *revert to snapshot*. Changes to a virtual machine can be discarded at the end of a lab reservation, returning the PC to a clean state.
- Users can have administrative privileges on a virtual machine without risk.
- Users may power on, power off, and revert to clean state (scrub) from the NETLAB+ web interface.
- Users can shutdown and reboot a virtual machine during the lab, without losing changes.
- Virtual network interfaces on a virtual machine can be tied to real networks in the lab. NETLAB+ provides the framework to separate lab networks from real networks in a secure manner.

Virtualization using VMware is performed on separate physical servers, not included with NETLAB+. You can interface with multiple VMware virtualization servers if necessary.

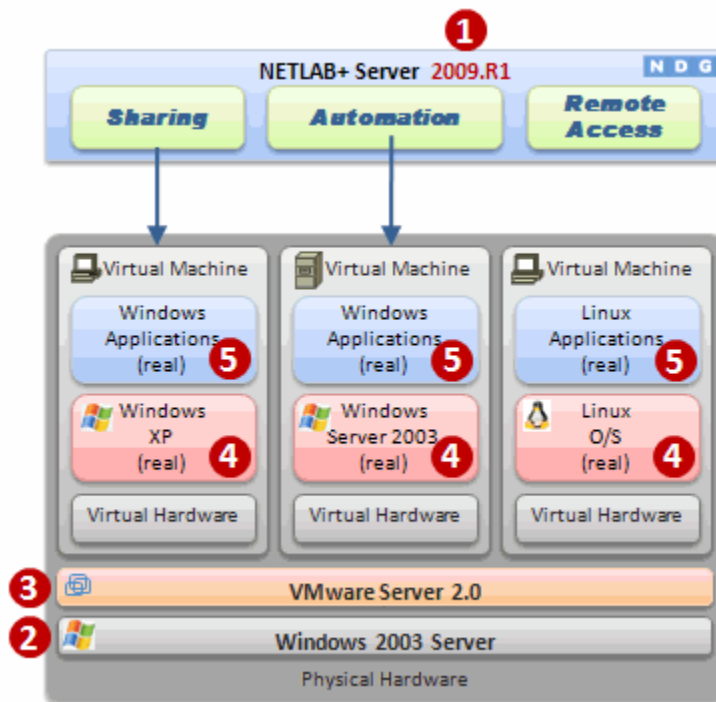
Part 2 Planning

This section discusses the software and hardware requirements for planning a remote PC deployment using VMware Server 2.x.

Objectives

- What software is required?
- What hardware is required?
- How many VMware host servers do I need?

2.1 What Software Is Required?



Refer to the numbered diagram above.

- (1)** Your NETLAB+ server must be running version **2009.R1** or later to interface with VMware Server 2.x.
- (2)** Each virtualization server requires a copy of Microsoft Windows 2003 Server. In VMware and NETLAB+ terms, this is called the *host operating system*. Other Windows host operating systems are supported by VMware. This guide will provide guidance for Windows 2003 Server, which is the recommended host operating system at this time.

- (3)** Each VMware virtualization server requires a copy of VMware Server, available from <http://www.vmware.com>. Other VMware products are supported (see the table below). All examples and procedures in this guide are specific to VMware Server 2.x.
- (4)** Each virtual machine requires a copy of a supported operating system. In VMware and NETLAB+ terms, this is called a *guest operating system*. Please refer to the VMware Server documentation to determine which operating systems versions are currently supported. NETLAB+ has been tested with Microsoft Windows and Linux operating systems.

Novell Netware is known to have problems with cursor updates, and is therefore not supported at this time.

- (5)** Each virtual machine can run application programs. These are installed on each virtual machine the same way you install software on a real PC.

2.1.1 Product Licensing

For the purpose of software licenses, each virtual machine and VMware server system is treated as an independent real PC or server. Please refer to the specific vendor license agreements (and educational discount programs, if applicable) to determine licensing requirements for your virtual machine's software, server software, operating systems, and application programs.

2.1.2 VMware Hosting Product Comparison

The following table compares NETLAB+ support and features for selected VMware hosting products. This guide is specific to **VMware Server 2.x**. Should you decide to use one of the other listed products with NETLAB+, please switch to the respective NETLAB+ guide that matches the specific VMware product.

Product	VMware Server	VMware ESXi	VMware ESX	VMware GSX	
VMware Version	2.x	1.x	3.5 U3	3.5 U3	3.x
NETLAB+ Support	BETA	Supported	PLANNED	Planned	Deprecated (2)
Minimum NETLAB+ Version	2009.R1	4.0.11	2009.R1	TBD	3.7.0
Architecture	Hosted	Hosted	Hypervisor		Hosted
Minimum VMware Version Required	2.0	1.0.3	3.5 U3		3.1
VMware Versions Tested by NDG	2.0	1.0.3 1.0.6 1.0.7	3.5 U3		3.1 3.2
Host Operating System Required	Windows	Windows	No		Windows
Windows Server O/S Versions Tested	2003	2003 2000	n/a		2003 2000
Linux Server O/S Versions Tested	n/a (1)	n/a (1)	n/a		n/a (1)
NETLAB+ Feature Support:					
• Remote PC Viewer	Yes	Yes	Yes		Yes
• Power On / Off	Yes	Yes	Yes		Yes
• Revert to Snapshot (scrub)	Yes	Yes	Yes		Yes

(1) VMware Server for Linux or VMware GSX for Linux is not currently supported or documented by NDG. However, you may run Linux as a *guest operating system* on virtual machines.

(2) VMware GSX has been replaced by VMware Server 1.x and VMware Server 2.x.

2.1.3 NETLAB+ Support Summary for VMware Server 2.x

NETLAB+ Support Status	BETA	
Minimum NETLAB+ Version Required	NETLAB+ 2009.R1	
VMware Server Minimum Version Required	VMware Server 2.0	
VMware Server Versions Tested	VMware Server 2.0 (Build 116503)	
Windows Host Operating Systems Tested	Windows Server 2003	
Linux Host Operating Systems Tested	NDG does not currently support Linux as a host operating system for VMware Server.	
Guest Operating Systems Tested ^(1, 2)	Windows XP (x86, 32-bit)	
Minimum Number of Virtual Machines (on each VMware server host)	10 *	* With adequately sized hardware.
Maximum Number of Virtual Machines (on each VMware server host)	10 **	** The maximum is determined by hardware and the number of virtual switches required. See known issue in section 2.1.4.1.
Number of Virtual Switches Supported	10 max	See known issue in section 2.1.4.1.
NETLAB+ Supported Features	Remote PC Viewer Power On Power Off Revert to Snapshot (scrub)	

(1) Please refer to the VMware Guest Operating System Installation Guide for specific product support, installation instructions and known issues.

(2) Older 32-bit processors will only support 32-bit guest operating systems. A 64-bit processor is required for 64-bit guest operating systems.

2.1.4 NETLAB+ Known Issues for VMware Server 2.x

In this section, we will discuss several known issues encountered when using VMware Server 2.x with NETLAB+.

2.1.4.1 10 Virtual Switch Limit

VMware Server 2.x for Windows supports 10 virtual switches per server. This is a hard limit.

Count the number virtual switches that are required by each pod. This number cannot exceed 10 per VMware Server. This limit may affect the number of virtual machines that can be run on one VMware server and the number of servers required. If you are using one of the standard NETLAB_{AE} pods, section 2.3 of this guide provides the virtual machine count and virtual switch count for each pod type.

A high-end system capable of hosting 20 or more virtual machines may be wasted if the virtual switch count limit of 10 effectively limits you to a much smaller number of virtual machines.

The following table discusses three common scenarios and the possible impact of the 10 virtual switch limit.

Scenario	Impact
No Networking. Your virtual machines do not utilize virtual networking or virtual switches.	Virtual switches will not be a limiting factor in the number of hosted virtual machines.
1:1 Ratio. The pod design(s) requires that each virtual machine have its own dedicated virtual switch.	The number of possible virtual machines on one server is exactly 10 (with adequate hardware).
Shared Virtual Switches. The pod design(s) has virtual machines that share a virtual switch.	If your pod designs (topologies) have virtual machines that share a virtual switch, then 10 or more virtual machines per server are possible, provided no more than 10 virtual switches are used and the hardware can support the total number of virtual machines on the server.

Workaround. Consider using one of the supported VMware ESX/ESXi products listed in section 2.1.2. These products support more virtual switches per server, allowing you to place and run more virtual machines and virtual switches on fewer high-end servers.

2.1.4.2 Continuous High CPU Utilization Causes Timeouts

Continuous high CPU utilization at or near capacity on all processor cores cause API connection timeouts. This in turn may cause automated operations performed in NETLAB+ to fail.

Causes. Running too many active virtual machines on one server, and/or using a server with inadequate hardware resources.

Workaround #1. Add additional VMware servers and divide the workload.

Workaround #2. Upgrade server CPU and memory. Additional CPU speed, processor cores and memory are usually helpful. See the hardware discussion in the later section for additional guidance.

Workaround #3. Consider using one of the supported VMware ESX/ESXi products listed in section 2.1.2. These products provide more control over CPU resource allocation and can be configured to dedicate processing cycles to system tasks.

2.1.4.3 NETLAB+ Not Tested With All Guest Operating Systems

VMware provides a *Guest Operating System Installation Guide* that contains a list of supported guest operating systems and the known issues for each. Not all operating systems in this document have been tested with NETLAB+.

We recommend that you thoroughly test each unique guest operating system in the NETLAB+ environment prior to production deployment. In particular, you should install the VMware Tools on the guest operating system, and then use the NETLAB+ Remote PC Viewer to test for proper functioning of the keyboard, mouse, mouse cursor, and screen updates.

2.1.4.4 NETLAB+ Does Not Support Novell Netware

Novell Netware as a guest operating system is not supported by NETLAB+ at this time. There are known issues with cursor updates, making remote access unusable.

2.1.4.5 NETLAB+ Does not Support DLink Network Cards

DLink network cards and/or chipsets are not supported. NDG has verified that the DLink driver has an MTU problem when used with VMware virtual switches. This problem will break almost all labs.

2.1.4.6 NETLAB+ Does not Support Broadcom Networking Adapters

We strongly discourage the use of Broadcom networking adapters due to a problem with the configuration utility and the use of VLANs. **We recommend upgrading to an Intel Networking Adapter for the inside interface** (see section [2.1.3](#)).

BACS configuration requires teaming. Certain teaming modes will absolutely not work since they can result in these undesirable conditions:

- Duplicate IP addresses on control devices.
- Duplicate MAC addresses on virtual machines in the lab.

Generic trunking mode is the only known mode that appears to work. If you already have Broadcom Adapters and wish to pursue experimental use of them, refer to [Appendix E](#). Broadcom Adapters may be used for the outside interface (section [3.5](#)).

2.1.4.7 Intel PROSet Device Manager Tabs Not Visible Through Terminal Svcs.

Intel PROSet for Device Manager tabs are not visible through Terminal Services when viewed through Microsoft Internet Explorer. The tabs are visible when a user is logged on locally to the Server. Access to the Device Manager tabs is necessary to create VLANs from Remote Desktop (see section [3.2](#)).

This issue can be resolved by changing the default user account from "**interactive user**" to a user with administrative rights (solution for Windows XP and Windows 2003 server):

- On the target system, select **Start** → **Run**.
- Type "**dcomcnfg**" in the text field and click **OK**. The Component Services Console Root window will open.
- In the left pane, double-click **Component Services** → **Computers** → **My Computer** → **DCOM Config**.
- In either pane, **Right-click** **NCS2Prov** → **Properties**. The DCOM configuration properties window will open.
- In the NCS2Prov Properties window, click the **Identify** tab. Change the user account to "**the launching user**".
- Click **OK** to exit the NCS2Prov Properties window. Close the Component Services window.

Please refer to this [Intel support page](#) for more information.

2.1.5 Upgrading From VMware Server 1.x to 2.x

The management interfaces, APIs, and virtual machine settings for VMware Server 2.x have changed significantly from version 1.x, which has required NDG to develop this separate guide.

Configuration changes to both NETLAB+ and virtual machine settings are required when upgrading a virtual machine from 1.x to 2.x. [Appendix D](#) documents the necessary changes.

2.2 VMware Host Hardware Requirements

At this point, you have decided that VMware Server 2.x is the appropriate product to host your virtual machines. (If not, please switch to the respective NETLAB+ guide that matches the specific VMware product.)

Henceforth, references to “**VMware**”, “**VMware host system**” and “**VMware server**” in this document refers to a server running VMware Server version 2.x virtualization software.

Next, we will explore hardware requirements.

Remote PCs are implemented on one or more VMware host systems (separate from the NETLAB+ server). The following table is a list of recommended hardware for VMware Server.

Servers that do not meet the minimum requirements listed may work, but may encounter performance issues and/or lack support for certain guest operating systems. Please consult the [VMware Server User's Guide](#) for details, particularly if you wish to run 64-bit guest operating systems.

	Recommended Minimum / Features	Notes
Processor(s)	x86-64 compatible (Intel, AMD) <ul style="list-style-type: none"> • 4 or more cores • 2.33Ghz per core Intel -specific features: <ul style="list-style-type: none"> • Intel 64 (formerly EM64T) ^{1,2} • Intel-VT (Vanderpool) AMD-specific features: <ul style="list-style-type: none"> • AMD64 revision D or later ^{1,2} • AMD-V (virtualization) 	Examples that meet minimum: <ul style="list-style-type: none"> • Intel Xeon E5410 (Quad core)⁴ • Intel Core i7 940 • Intel Core i7 920 • Intel Xeon X3350 • Intel Xeon X3330 • Intel Core 2 Quad Q9650 • Intel Core 2 Quad Q9550 • Intel Core 2 Quad Q9450 • Intel Core 2 Quad Q6700 • AMD Phenom II X4 940
Memory	4 GB (minimum) ^{***}	*** 4GB is the maximum supported by the 32-bit version of Windows Server 2003/2008 Standard Edition. The 64-bit version of Windows Server 2003/2008 Standard Edition will support up to 32GB of ram.
Disk ³	320GB – 1 TB, RAID 1 or RAID 5	See note 3 below concerning RAID.

Network Interfaces	<p>Dual (2) 100/1000 Ethernet with 802.1q</p> <p>Supported Interfaces:</p> <ul style="list-style-type: none"> • Intel server adapter (825XX chipset) with Advanced Network Support (ANS) features <p>Unsupported:</p> <ul style="list-style-type: none"> • All DLink cards (see 2.1.4.5) • Broadcom adapters/chipsets (see 2.1.4.6) 	<p>Examples in this document are based on the Intel PROSet configuration tools.</p> <p>DLink cards are not supported. (see section 2.1.4.5).</p>
Host Operating System	Microsoft Windows Server 2003 ***	<p>*** The 32-bit version supports a maximum of 4GB of RAM.</p> <p>For more than 4GB (up to 32GB), consider using the 64-bit version.</p>

(1) x86-64 should not be confused with the Intel [Itanium](#) (formerly *IA-64*) architecture, which is not compatible on the native instruction set level with the x86 or x86-64 architecture.

(2) VMware provides a standalone utility that you can use without VMware Server to perform the same check and determine whether your CPU is supported for VMware Server virtual machines with 64-bit guest operating systems. You can download the 64-bit processor check utility from <http://www.vmware.com/download>.

(3) VMware ESX/ESXi only supports hardware RAID. If you plan to upgrade from VMware Server to VMware ESX/ESXi in the future, be sure the RAID controller is supported by ESX/ESXi. Please note that the “on-board” RAID in many motherboards is actually software RAID (or “fake” RAID), because the actual RAID functions are performed by device drivers running on the host operating system.

(4) This hardware was used by NDG as the 2009 test platform.


2.3 How Many VMware Server Host Systems Do I Need?

The number of VMware host systems and memory requirements vary based on the lab topologies and number of pods you want to implement.


NDG recommends no more than 10 to 12 virtual machines per server with hardware meeting the requirements in section 2.2. Each virtual machine uses CPU cycles and memory on the server. VMware Server supports up to 4 virtual machines per CPU core. The table below shows a hypothetical allocation of processor cores for virtual machines and other system tasks. You do not actually configure this; the operating system will do this dynamically based on workload.

CPU Core #1	VM1 VM2 VM3 VM4
CPU Core #2	VM5 VM6 VM7 VM8
CPU Core #3	VM9 VM10 VM11* VM12*
CPU Core #4	Host Operating System, VMware, and API processes

* VM11 and VM12, assuming the virtual switch limitation of 10 was not exceeded by topology requirements.

 If you have more than one ESXi host server, consider spreading the VMs from each pod across all of host servers. This will evenly spread the load on critical system resources for each ESXi host (processing and memory).

Running too many virtual machines may starve the host operating system and/or VMware Server APIs. This may lead to timeouts and task automation failures in NETLAB+.

 If a single VMware host is shared among multiple pods and the VMware host does not meet the requirements from section 2.2, users from one pod may notice a substantial delay when the reservation begins/ends from another shared pod. When a reservation begins, NETLAB+ instructs the VMware host server to power on or resume all Virtual Machines represented in that lab topology. When this occurs, the VMware host may experience a high CPU load for several minutes. This can result in sub-optimal and even unresponsive communications for those NETLAB+ users logged in from a different pod, accessing Virtual Machines hosted by the same VMware server.

Step-By-Step Guidance

Step 1. Carefully study your lab topologies and determine the number of virtual switches and virtual machines required by each pod. The requirements for several NETLAB_{AE} pods shown below assume that you are implementing all PCs supported by the pod.

The following table shows some of the pods that support virtual machines in NETLAB_{AE}. For an updated list of NETLAB_{AE} topologies, please view the [lab topologies page](#).

	Maximum Virtual Switches (VMnet)	Maximum Virtual Machines
Basic Router Pod v2 (BRPv2)	3	4
Basic Switch Pod v2 (BSPv2)	3	3
Cuatro Router Pod (CRP)	4	5
Cuatro Switch Pod (CSP)	4	4
LAN Switching Pod (LSP)	3	4
Network Fundamentals Pod (NFP)	5 required 2 optional	5 required 2 optional
Network Security Pod 2.0 (NSP)	5	7

Step 2. Add up the number of virtual switches and virtual machines used by each pod you are implementing. For example:

Pod Name	Type	Virtual Switches	Virtual Machines
POD 1	Basic Router Pod Version 2	3	4
POD 2	Basic Router Pod Version 2	3	4
POD 3	Basic Router Pod Version 2	3	4
POD 4	Basic Router Pod Version 1	0 (n/a)	0 (n/a)
POD 5	Basic Switch Pod Version 2	3	3
POD 6	Network Security Pod (2.0)	5	7
Total		17	22

Step 3. Assign each pod that supports PCs to a VMware host server.

Remember, VMware Server 2.x for Windows supports 10 virtual switches per server on Windows Server host platforms. This is a hard limit.

In the example from step 2, 17 virtual switches are required. Since you can have up to 10 virtual switches per server, you would need at least two VMware host servers for this implementation. Server 1 could accommodate POD1, POD2, and POD3. Server 2 could accommodate POD5 and POD6. Note, POD4 does not support PCs and uses no VMware host resources.

VMware Host #1 – Example			
Pod	Type	Virtual Switches	Virtual Machines
POD 1	Basic Router Pod Version 2	3	4
POD 2	Basic Router Pod Version 2	3	4
POD 3	Basic Router Pod Version 2	3	4
Total		9	12

VMware Host #2 - Example			
Pod	Type	Virtual Switches	Virtual Machines
POD 5	Basic Switch Pod Version 2	3	3
POD 6	Network Security Pod (2.0)	5	7
Total		8	10

Step 4. Based on the pod type and curriculum requirements, determine which guest operating system you will use on each virtual machine. Tabulate the operating system and memory requirements for the host operating system and virtual machines. You should allocate the same amount of memory as you would if standing up a real PC. The following would represent typical choices for VMware Host 1 in the previous example.

VMware Host System #1 - Example			
Pod	PC Name	Operating System	Memory (MB)
n/a	VMware Host O/S	Windows Server 2003	512
POD 1	PC1a	Windows XP	128
POD 1	PC1b	Windows XP	128
POD 1	PC2	Windows XP	128
POD 1	PC3	Windows XP	128
POD 2	PC1a	Windows XP	128
POD 2	PC1b	Windows XP	128
POD 2	PC2	Windows XP	128
POD 2	PC3	Windows XP	128
POD 3	PC1a	Windows XP	128
POD 3	PC1b	Windows XP	128
POD 3	PC2	Windows XP	128
POD 3	PC3	Windows XP	128
Total			2048 (2GB) *

* At least 4GB per server is now recommended to support recent mainstream operating system requirements with greater memory requirements.

To utilize all available virtual switches on a VMware host system, it is possible to split virtual switches and machines in a single pod across two different VMware hosts. However, you should be familiar with the remote PC and virtual switch layout for each pod before attempting this.

Step 5. Translate the requirements from steps 1 through 4 into an itemized list for each server. The two VMware host systems in the previous examples would require the following items.

VMware Host System #1 - Example		
Quantity	Item	Role
1	Server <ul style="list-style-type: none"> • Intel Core i7 920 (2.93 GHz X 4 cores) • 2GB RAM Minimum (4GB recommended) • 2 x 640GB Hard Disks with RAID1 support • Dual (2) Intel Network Interfaces with 802.1q VLAN tag support 	server hardware
1	VMware Server for Windows, Version 2.x	virtual machine software
1	Windows 2003 Server - Standard Edition	host operating system
12	Windows XP (Home or Pro)	guest operating systems

VMware Host System #2 - Example		
Quantity	Item	Role
1	Server <ul style="list-style-type: none"> • Intel Core i7 920 (2.93 GHz X 4 cores) • 2GB RAM Minimum (4GB recommended) • 2 x 640GB Hard Disks with RAID1 support • Dual (2) Intel Network Interfaces with 802.1q VLAN tag support 	server hardware
1	VMware Server for Windows, Version 2.x	virtual machine software
1	Windows 2003 Server - Standard Edition	host operating system
5	Windows XP (Home or Pro)	guest operating systems
3	Windows 2000 Server	guest operating systems
2	Linux	guest operating systems

Part 3 VMware Host System Setup

This section describes the initial preparation of a VMware host system running VMware Server 2.x software and Microsoft Windows 2003 Server as the host operating system. After preparation of each host server is complete, virtual machines can be added (as *guests*) and integrated into the overall NETLAB+ system.

Objectives

- Install and configure Microsoft Windows Server operating system.
- Create a NETLAB+ management account.
- Install VLAN drivers and utilities.
- Configure and connect networking adapters.
- Install VMware Server software.
- Prepare system for virtual networking.

All tasks in this section are performed on **separate dedicated servers** that you provide. Do not perform any of the tasks in this section on the NETLAB+ server appliance, as this will delete the NETLAB+ software, requiring you to return it to the factory for re-installation.

3.1 Install and Configure Microsoft Windows Server Operating System

If your system was not preloaded with the Microsoft Windows Server operating system, you should do that now. This guide provides examples based on Microsoft Windows Server 2003. Other versions may differ slightly.

Install the operating system on the physical server per Microsoft installation instruction guides (if not pre-installed).

3.1.1 Install Chipset Drivers

If you installed the operating system, you may need to install the chipset drivers supplied with the computer and/or motherboard, usually on a CD or DVD. Running Windows without the proper chipset drivers installed may result in poor performance, and/or hardware not being recognized.

3.1.2 Configure RAID

Configure your RAID drivers (if necessary) and create your RAID arrays. Software RAID solutions (on board “fake” RAID) may require that you configure your RAID arrays prior to installing Windows Server and/or require a driver disk during the installation. Ignore this step if your system does not support RAID, or you do not wish to configure RAID.

3.1.3 Disable IIS (Recommended)

If the Microsoft IIS web server is running, you can disable or uninstall it to free up memory and other resources. This component is not required.

3.2 Install Advanced Networking Drivers and Utilities

Virtual LAN (VLAN) support is required if you want to bridge your virtual machines to real networks and real lab equipment (such as routers, switches, and firewalls). This section describes the VLAN drivers and management utilities for Intel networking adapters. You can skip this section if your virtual machines do not need to communicate with lab equipment and/or external networks on separate VLANs.

VLAN support for Intel networking adapters is provided by the ANS driver (which may be different than the driver provided). VLANs are managed using the Intel PROset software utility. These are packaged together and available for download on the Intel.com website.

Network Connectivity

Drivers and software for Intel® Gigabit and PRO/1000 Network Adapters

Solution:

Top Downloads

[Network drivers for Windows* 2000, XP, & Server* 2003 \(32-bit\)](#)

[Network drivers for Windows Vista* & Server* 2008 \(32-bit\)](#)

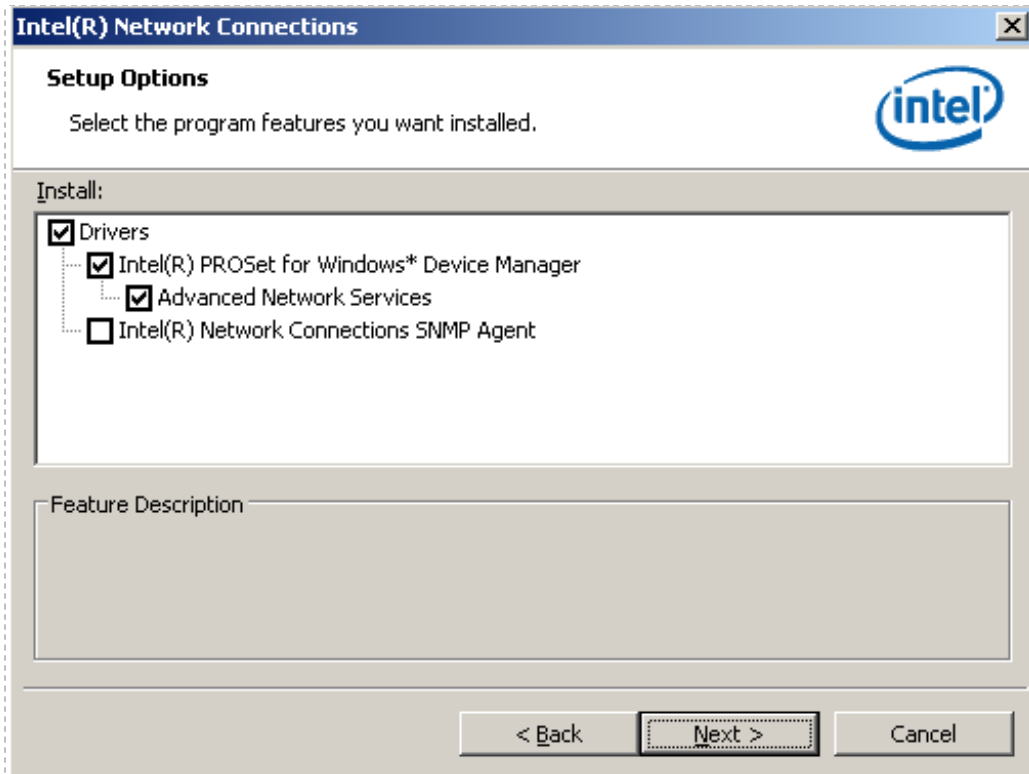
Intel® PRO/1000 and Gigabit Network Adapters

You do not need to download a separate file for each Intel network adapter. Each file includes drivers for multiple adapters including 10/100, gigabit, and 10 Gigabit adapters.

Note: Additional information about using driver downloads is available at [Install, extract files without installing, and using DxSetup utility](#).

Operating System (OS)	Download Type	File Name
Windows Vista* & Server* 2008 (32-bit)	Driver, Intel® PROSet, ANS, and SNMP	PROVISTA32.EXE
Windows Vista & Server 2008, x64	Driver, Intel PROSet, ANS, and SNMP	PROVISTAX64.EXE
Windows Server 2008 for Intel® Itanium®-based systems	Driver, Intel PROSet, ANS, and SNMP	PROWS0864.EXE
Windows* 2000, XP, and Server 2003	Driver, Intel PROSet, ANS, and SNMP	PRO2KXP.EXE
Windows Server* 2003 x64 Windows* XP x64	Base, Intel PROSet, ANS, etc.	PROEM64T.EXE
Windows Server 2003 for Intel® Itanium®-based systems	Driver, Intel PROSet, ANS, and SNMP	PROWS64.EXE

For Windows Server 2003 (32-bit), the file name is PRO2KXP.EXE (version 13.5 at the time of this writing). Download and run the installer. Select the **PROSet** and **ANS drivers** options as shown below.



3.3 Networking Models

Several types of network communication occur to and from the VMware host system.

- **KVM.** Provides remote Keyboard/Video/Mouse access to virtual machines, via the NETLAB+ server.
- **API.** Provides an interface for NETLAB+ to query and control virtual machines (status, power on, power off, and revert to snapshot).
- **Bridging (optional).** Allows virtual machines to connect to real lab devices such as routers, switches, and firewalls. This is accomplished by connecting VMware virtual machines to virtual switches, then connecting virtual switches to Virtual LANs (VLAN) behind NETLAB+ control switches. Although not documented in this guide, physical network adapters (NICs) on the VMware host system may be directly connected to lab devices as an alternative to VLANs, for special applications that require direct unobstructed connectivity between a virtual machine and external lab device.
- **Remote Management (optional).** System administrators may wish to manage VMware host servers and virtual machines using Remote Desktop and other remote management protocols.

NDG has developed three networking models to facilitate this communication.

- Inside Networking with High Security (ISEC)
- Inside Networking with External Management (IMAN)
- Outside Networking with External Management (OMAN)

Please evaluate the three models and choose the one that best fits your situation. Other undocumented models are also possible.

NDG recommends:

- **IMAN** for most environments.
- **ISEC** for high security environments.
- **OMAN** for older networking interfaces and drivers that will not support the inside models; otherwise, do not implement this model.

Networking Model	ISEC	IMAN	OMAN
Security	Excellent	Very Good	Good, with proper diligence in firewall configuration
Manage VMware hosts and virtual machines from remote consoles	No	Yes	Yes
Required number of Ethernet ports in each VMware server	1	2	2
Requires 802.1q VLAN support on inside interface	Yes	Yes	Yes
Requires 802.1q support on outside interface	n/a	No	No
Requires native (untagged) VLAN 1 support on inside interface	Yes	Yes	No
KVM and API traffic flow	Inside network (control switches)	Inside network (control switches)	Outside network (user LAN)
Documented in section	3.3.1	3.3.2	3.3.3

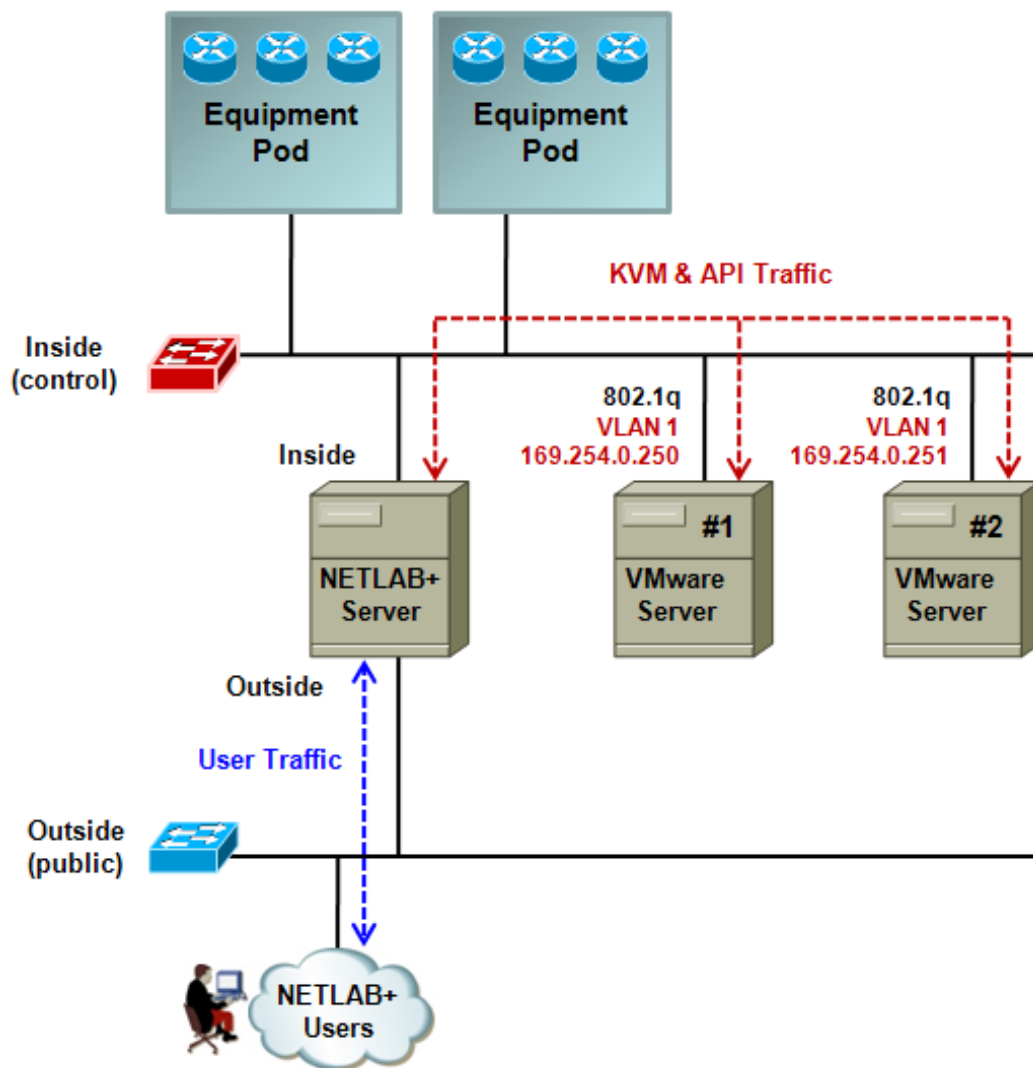
The following three sections describe each model in detail. Choose one of the three models and perform the network setup tasks outlined in the corresponding section for each VMware host server.

3.3.1 VMware Host Connectivity Using ISEC

This section examines the Inside Networking with High Security (ISEC).

ISEC is the most secure of the three models, because all VMware host and virtual machine communication occurs completely behind the NETLAB+ inside interface. Traffic is **not routed** between the outside and inside. Rather, users communicate with virtual machines using a transparent proxy service running on the NETLAB+ server.

This high level of security comes with sacrifice. Server management and virtual machine installations must be done at the system console via CD/DVD. If you would like the ability to manage VMware servers from Remote Desktop and/or load software and files from the campus LAN or Internet, then skip ahead to the IMAN model (section 3.3.2).



Reasons to Choose ISEC (one or more may apply)

- The highest possible security is required.
- The outside network is not strongly protected by a firewall, and/or is directly exposed on all ports to campus users.
- The server only supports one Ethernet port.
- Remote management is not required.
- Internet or campus LAN access is not required from the host operating system console.

ISEC Limitations

- ISEC provides no network connectivity to the campus LAN or Internet for remote management, software downloads, or virtual machine installation.
- VMware servers must be managed from directly connected consoles.
- Virtual machines must be installed from the host console. Software must be installed from CD/DVD.

ISEC Requirements

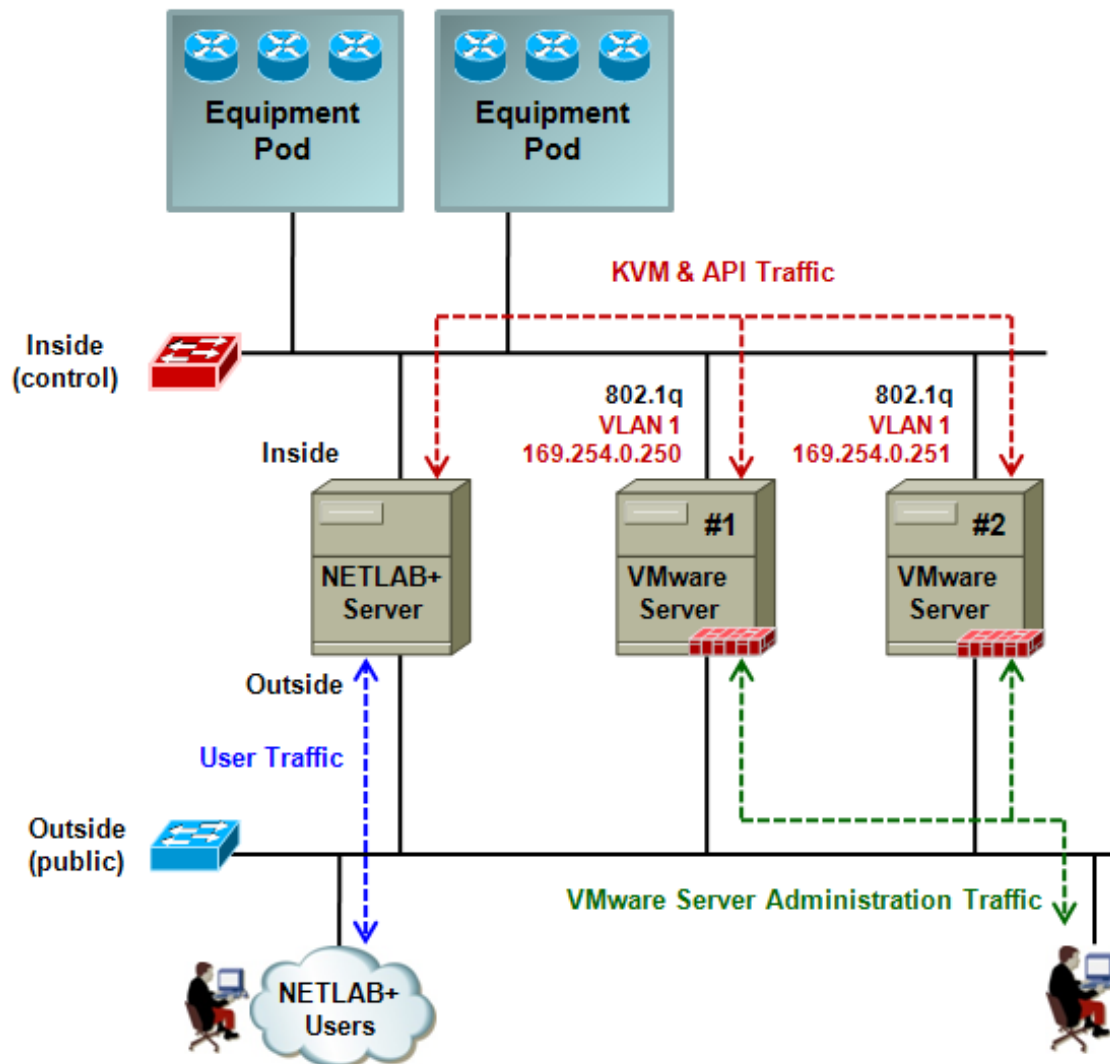
- Each VMware Server requires one Ethernet interface. This interface must support 802.1q*, with no VLAN tagging on VLAN 1 (this is called the *native* or *untagged* VLAN).

* Technically, 802.1q is not needed if you are not interfacing to external networks and real lab devices (i.e. a 100% remote-PC-only configuration). To simplify the documentation and provide consistency, we configure 802.1q in all cases, resulting in a “VLAN-ready” configuration.

3.3.2 VMware Host Connectivity Using IMAN

This section documents the Inside Networking model with External Management (IMAN).

IMAN provides a balance between security and manageability. All virtual machine traffic (Bridging), KVM, and automation traffic (API) remain behind the NETLAB+ inside interface (i.e. the control switches). The outside interface on each VMware server provides a path for remote management of the VMware host system and virtual machines.



Reason to Choose IMAN

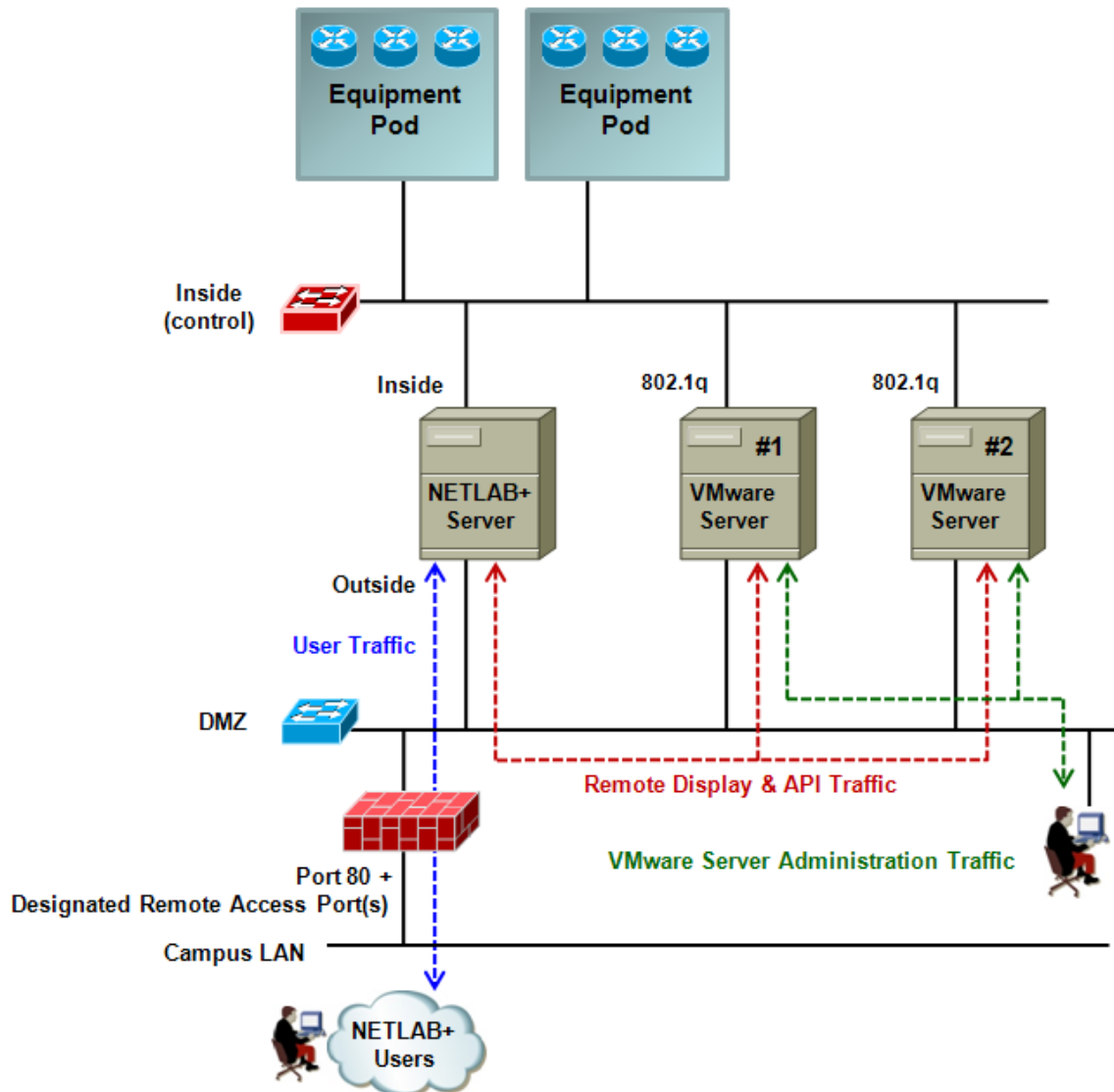
- Provides a practical method for managing VMware host systems and virtual machines, while keeping most NETLAB+ and lab communication safely on a private network.

IMAN Requirements (all apply)

- Each VMware Server requires two Ethernet interfaces. The inside interface must support 802.1q with no VLAN tagging on VLAN 1 (this is called the *native* or *untagged* VLAN). The outside interface has no special requirements.
- To provide maximum security, inbound connections to the outside interface on each VMware server should be limited to the IP addresses of trusted management workstations.

3.3.3 VMware Host Connectivity Using OMAN

This section documents the Outside Networking model with External Management (OMAN). This method can be used if your VMware Server inside interface is not capable of untagged VLAN frames for VLAN 1. This is usually only an issue with older network drivers.



OMAN provides minimal security, unless sufficiently firewalled per the diagram above. If your network interface drivers support a native/untagged VLAN, you are encouraged to use the ISEC or IMAN methods.

Reason to Choose the OMAN

- The network driver for the inside interface on your VMware server is not capable of removing VLAN tags from VLAN 1, the VLAN used by NETLAB+ for several functions.

Limitations Imposed

- To provide adequate security using this method, the outside network should be a DMZ protected by a firewall or router ACLs. Only the ports designated in the [CSS, Connectivity and Firewall Considerations](#) whitepaper should be permitted to ingress this LAN segment (labeled DMZ in the drawing).

Requirements

- Each VMware Server requires two Ethernet interfaces. The inside interface must support 802.1q. The outside interface has no special requirements.

3.4 Inside Interface Tasks

In this section we will configure the inside interface on the VMware host system. The tasks in the following sub-sections apply to all networking models (ISEC, IMAN, and OMAN), unless otherwise noted.

Objectives

- Rename the inside interface for easy identification.
- Unbind protocols from the inside physical interface.
- Understand the role of VLAN 1 and other bridged VLANs.
- Use Intel utilities to enable and manage 802.1q VLANs.
- Create VLAN 1 (IMAN, ISEC)
- Assign IP address to VLAN 1 (IMAN, ISEC)
- Connect the inside interface to the control switch.
- Bring up the inside connection.
- Verify the link and IP connectivity.

3.4.1 Open Network Connections Window

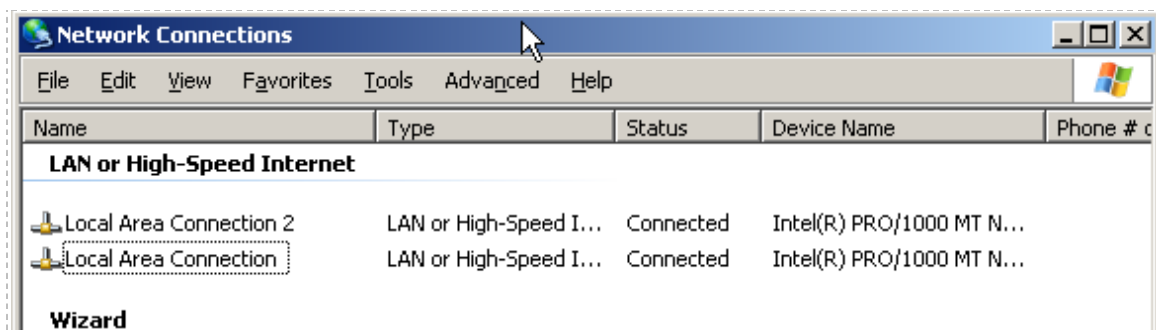
Navigate to the Network Connections panel:

- **Start** → **Control Panel** → *right click* on **Network Connections** → **Open**

Select the detail view:

- **View** (menu item) → **Details**

The Network Connections Panel should now look like this:

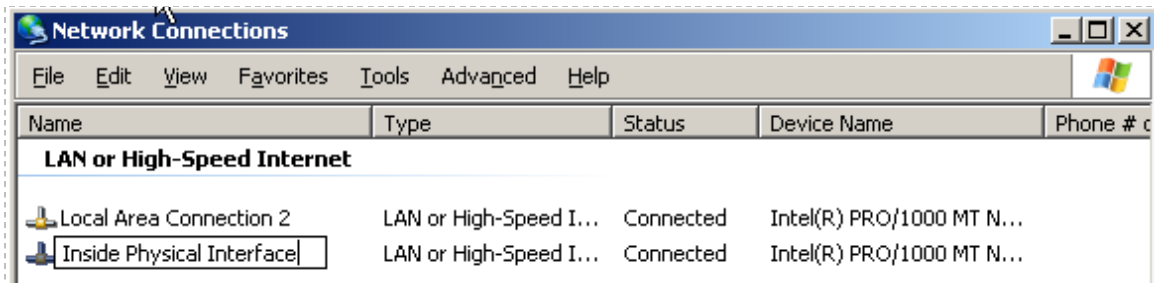


3.4.2 Select and Rename Inside Interface

Select an unused physical Ethernet network interface on the VMware host server.
Identify the corresponding LAN adapter in Windows Server.

Rename this interface to “Inside Physical Interface”:

- **Right click** on the interface and select **Rename**.
- Change the name to **“Inside Physical Interface”** and press **Enter**.



+

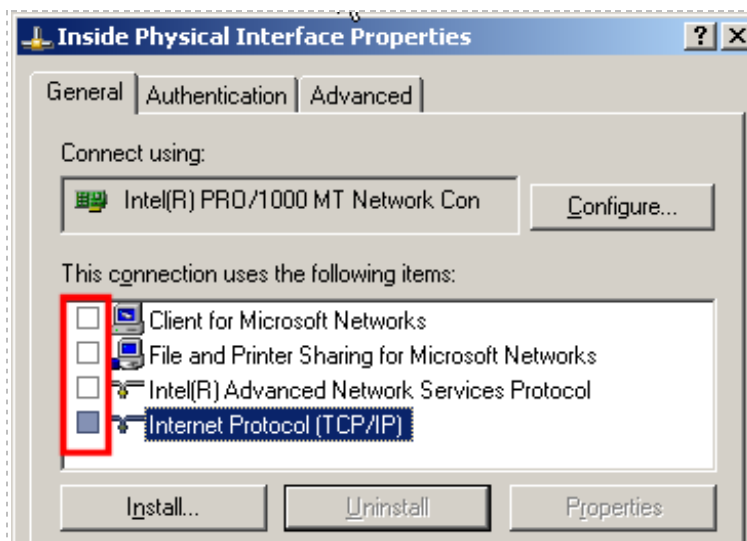
3.4.3 Unbind Protocols from Inside Physical Interface

The Inside Physical Interface is only used as container for VLAN *sub-interfaces*. Since protocols will be defined at the sub-interface level, we unbind all protocols (including TCP/IP) from the container interface.

From the Network Connection window, open the properties window for the Inside Physical Interface (renamed in previous task):

- **Right click** on **Inside Physical Interface** → **Properties**.

The property window should appear:



Unbind the protocols from the interface by un-checking them. In particular, ensure the following protocols are unchecked.

UNCHECK	Client for Microsoft Networks
UNCHECK	File and Printer Sharing for Microsoft Networks
UNCHECK	Internet Protocol (TCP/IP)
UNCHECK	VMware Bridge Protocol (this item should not be listed unless VMware Server was installed before this stepped)

When finished, click OK. This applies the changes. You must do this before continuing to the next step.

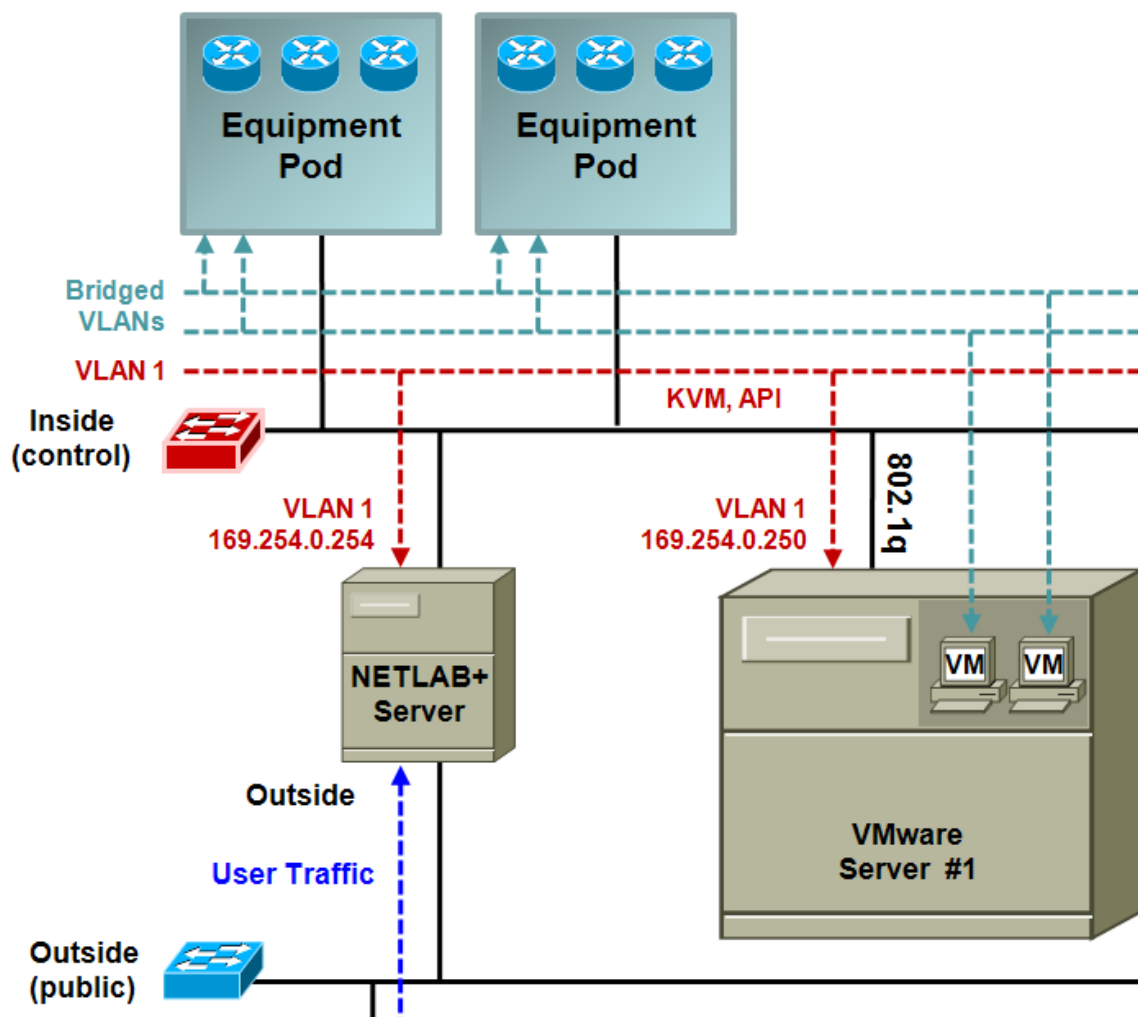
3.4.4 Understanding VLAN 1 and Bridged VLANs

The number of physical adapters required is greatly reduced by using VLANs.

In the ISEC and IMAN models, *VLAN 1* is used to transport KVM and API traffic between NETLAB+ and the VMware host operating system. In the OMAN model, KVM and API traffic is transported on the outside interface; *VLAN 1* is not used.

Bridged VLANs are used to transport network data between virtual machines and real lab equipment.

The Inside Physical Interface runs 802.1q and acts as container for VLANs. *VLAN 1* corresponds to the native (untagged) VLAN on the control switch. In the next step, you will enable 802.1q and create a *VLAN 1* sub-interface (ISEC, IMAN). Later in the document, you will learn how to bridge virtual machines to real equipment using bridged VLANs.



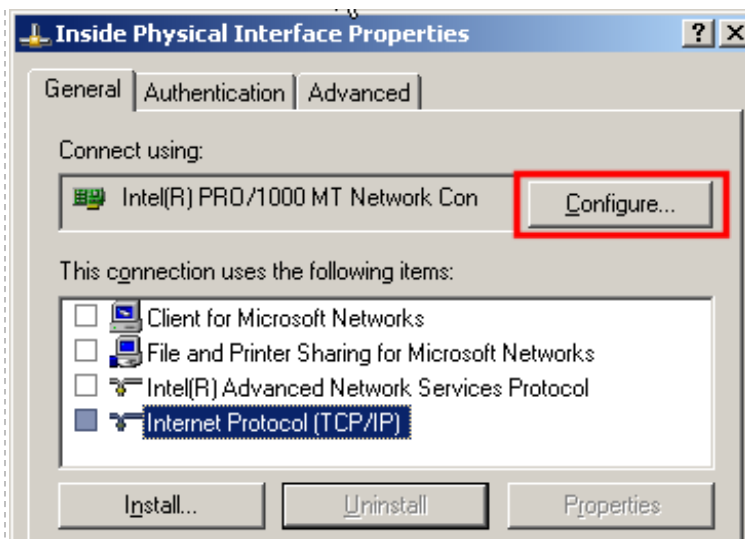
3.4.5 Creating VLAN 1 using an Intel Networking Adapter

This section applies to ISEC and IMAN. Skip ahead to section 3.4.7 if you are implementing OMAN.

In this step, we will create a VLAN 1 sub-interface on the **Inside Physical Interface** (container interface). The VLAN 1 sub-interface has two unique properties:

- VLAN 1 is the only sub-interface that will be *untagged*. All other sub-interfaces (if interfacing to real equipment) will use 802.1q VLAN tagging.
- VLAN 1 is the only sub-interface that binds the TCP/IP protocol. All other inside sub-interfaces will be bridged using the VMware Bridge Protocol.

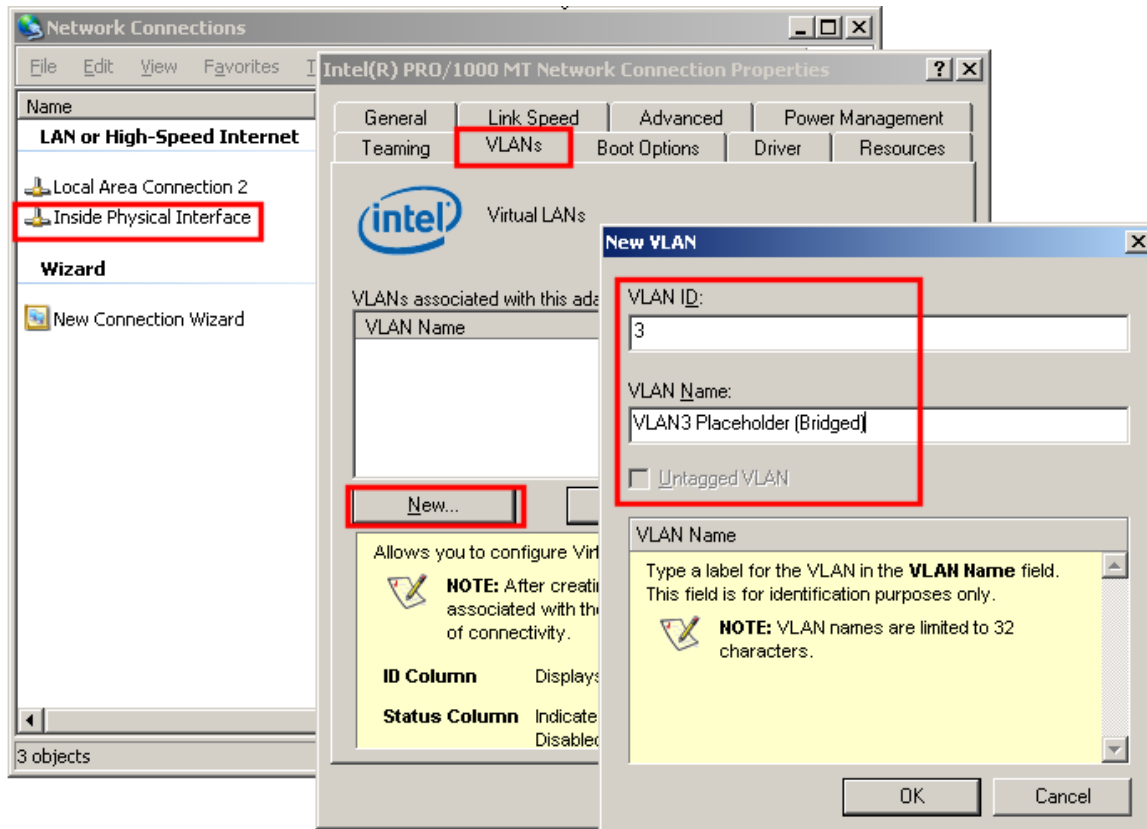
Return to the Network Properties window for the **Inside Physical Interface**. Verify that the protocols from step 3 are still unbound (unchecked). Next, click the **Configure** button.



At least two VLANs must exist before VLAN 1 can become untagged. Therefore, we will create VLAN 3 as a temporary *placeholder* VLAN **prior** to creating VLAN 1.

To create the placeholder VLAN:

- Click the **VLANs** tab.
- Click the **New** button.
- Enter “**3**” in the VLAN ID field.
- Enter “**VLAN3 Placeholder (Bridged)**” in the VLAN Name field.
- Click **OK**.

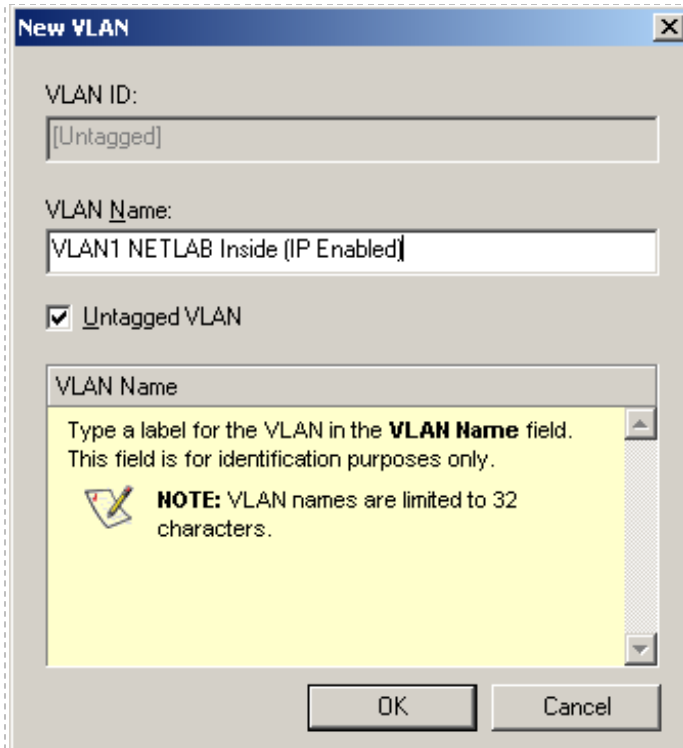


💡 Notice that the Untagged VLAN checkbox is inaccessible. This is the reason we could not create VLAN 1 first. This behavior is specific to Intel.

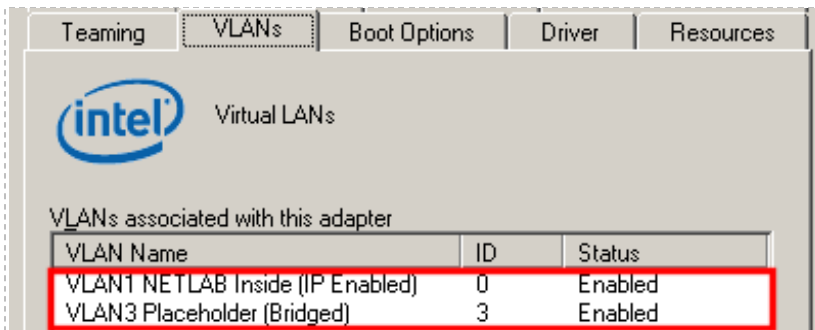
With a placeholder VLAN in place, we can now create an untagged VLAN 1.

Begin creating another new VLAN using the same procedure:

- For this VLAN, **uncheck** the **Untagged VLAN** option.
- Enter **“VLAN1 NETLAB Inside (IP Enabled)”** in the VLAN Name field.
- Click **OK**.

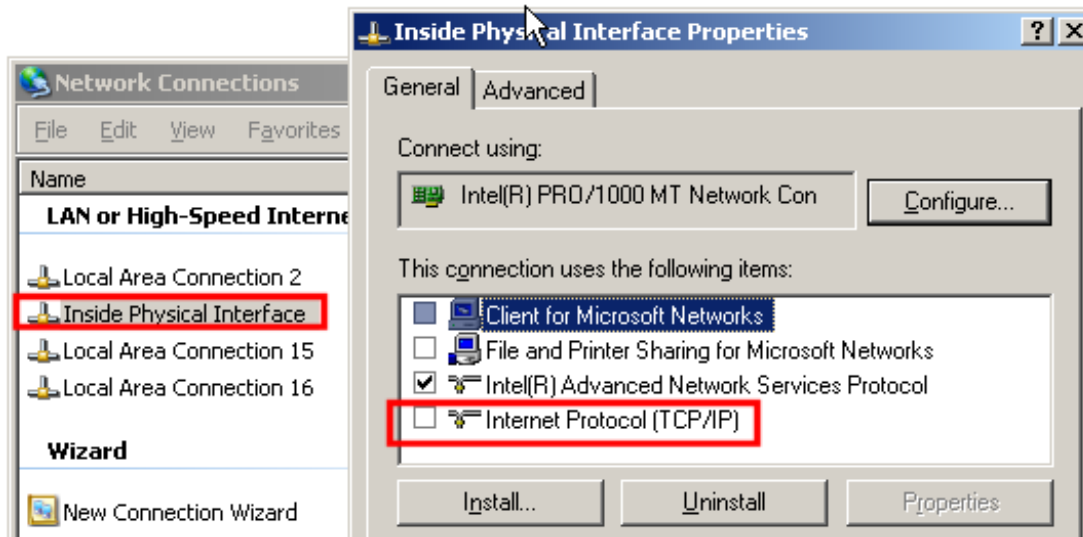


You should now have two VLANs associated with the inside adapter, as shown below. If so, click OK to save changes and exit from the Connection Properties window.

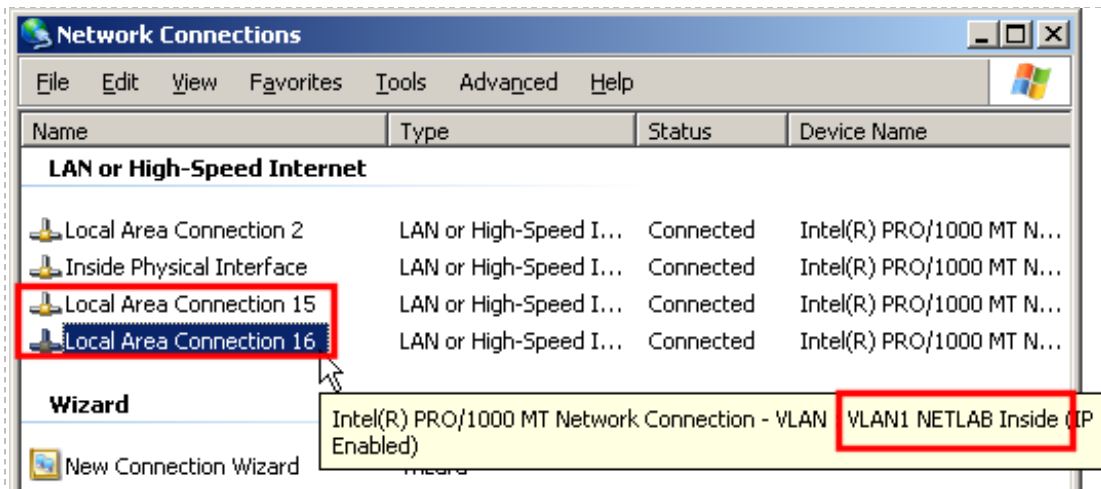


💡 The VLAN ID untagged VLAN reports an ID of 0 on the Intel adapter. This is actually VLAN 1 on the control switch.

Return to the **Inside Physical Interface** properties window and verify that Internet Protocol (TCP/IP) is still **unchecked** (if not, uncheck it again). The Intel Advanced Network Services Protocol may have been automatically checked as a result of VLAN creation, and this is OK.



As the result of creating VLAN 1 and VLAN 3, you should see two new networking adapters in the Network Connections window. However, the VLAN names you have assigned do not automatically transfer to the windows adapters; they must be renamed manually.

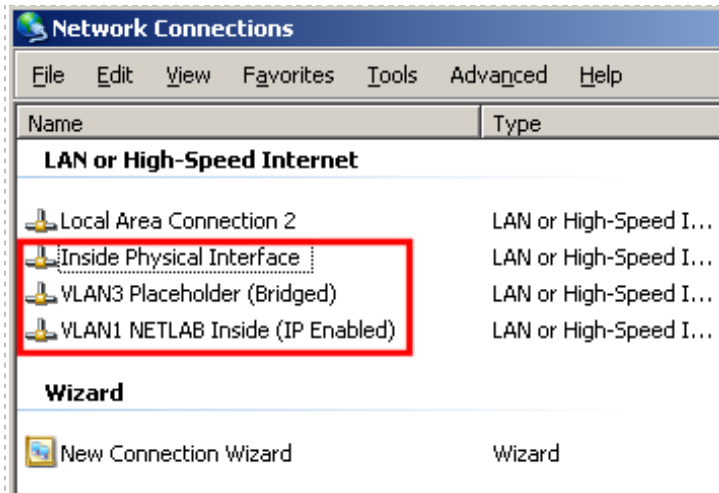


Hover the mouse over each adapter until Windows displays a yellow *tool tip* for the interface. Use the tool tip to identify the VLAN.

Once you have identified the Windows adapters associated with VLAN 1 and VLAN 3, rename the corresponding Windows' adapter.) using the same names you assigned during VLAN creation.

Network Connections → *right click* the interface name → **Rename**

The Network Connections window should now look like this:



💡 VLAN 1 and VLAN 3 interfaces are logical sub-interfaces of the Inside Physical Interface. However, this hierarchy is not reflected in the Windows Network Connections. Windows treats VLAN interfaces as ordinary network adapters.

💡 VLAN 3 can be deleted after creating other bridged VLANs for virtual machines. This will be discussed in later sections.

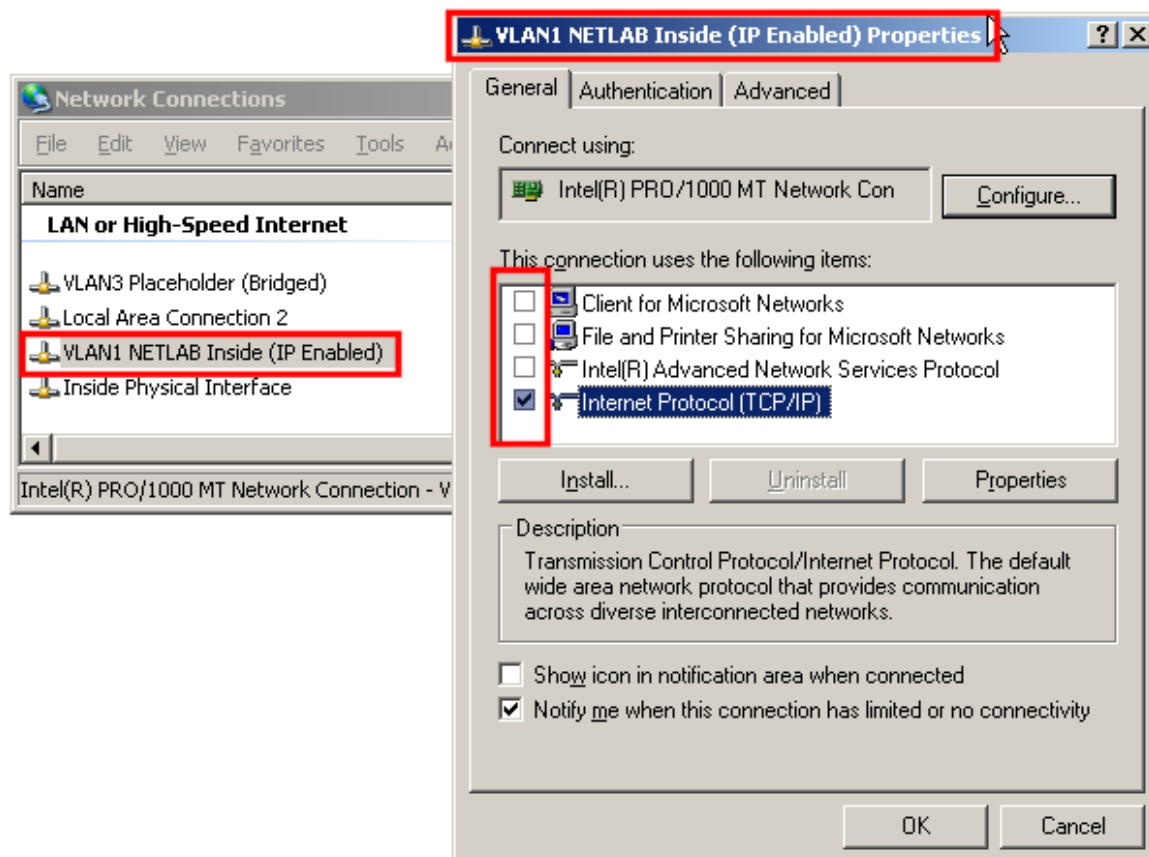
3.4.6 Configure VLAN 1 Protocols and TCP/IP Settings

This section applies to ISEC and IMAN. Skip ahead to section 3.4.7 if you are implementing OMAN.

In this section, we configure the network protocols and TCP/IP settings for VLAN 1:

- Return to the **Network Connections** window.
- **Right click** on the **VLAN1 NETLAB Inside** interface to invoke the context menu.
- Select **Properties** from the context menu.
- **Uncheck** **Client for Microsoft Networks**.
- **Uncheck** **File and Printer Sharing for Microsoft Networks**.
- **Check** **Internet Protocol (TCP/IP)**.

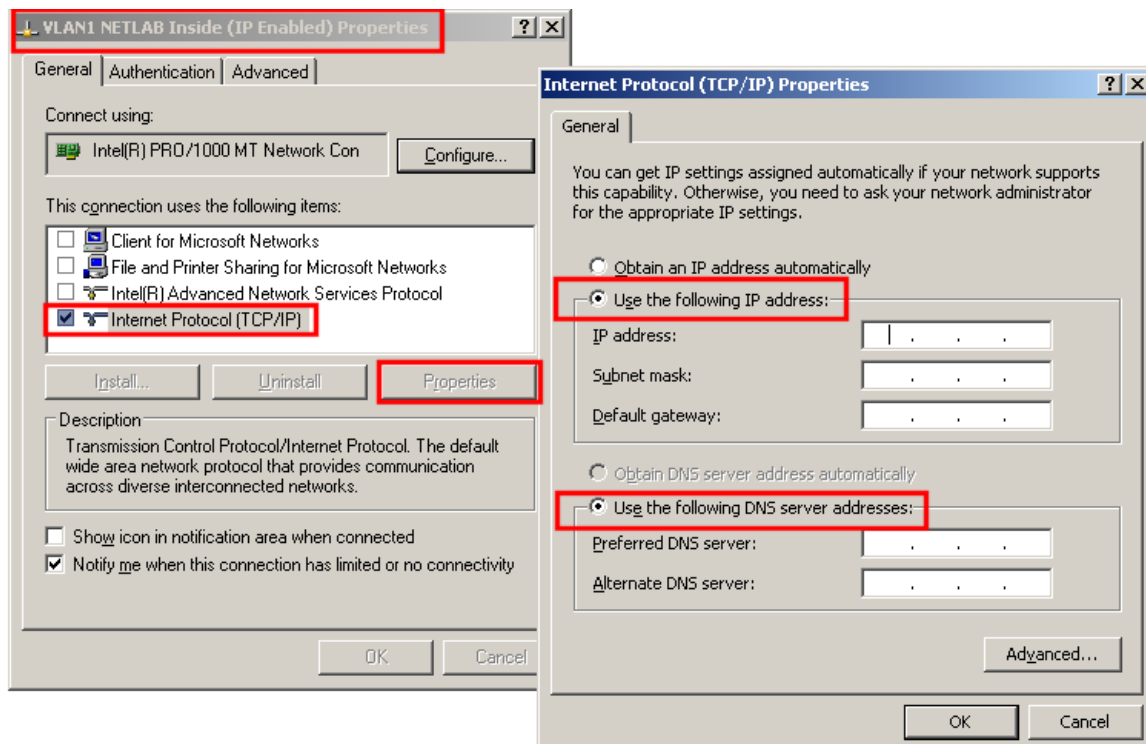
Your properties for the VLAN interface should now look like this:



Next, initiate manual IP address and setting assignment for the VLAN 1 interface.

- From the interface Properties window, select **Internet Protocol (TCP/IP)** by clicking on the words (not the checkbox). You should now see the **Internet Protocol (TCP/IP) Properties** window.
- Click on the radio button choice, **Use the following IP address:** to assign an IP address manually.
- Click on the radio button choice, **Use the following DNS server addresses:** to assign DNS servers manually.

You are here:



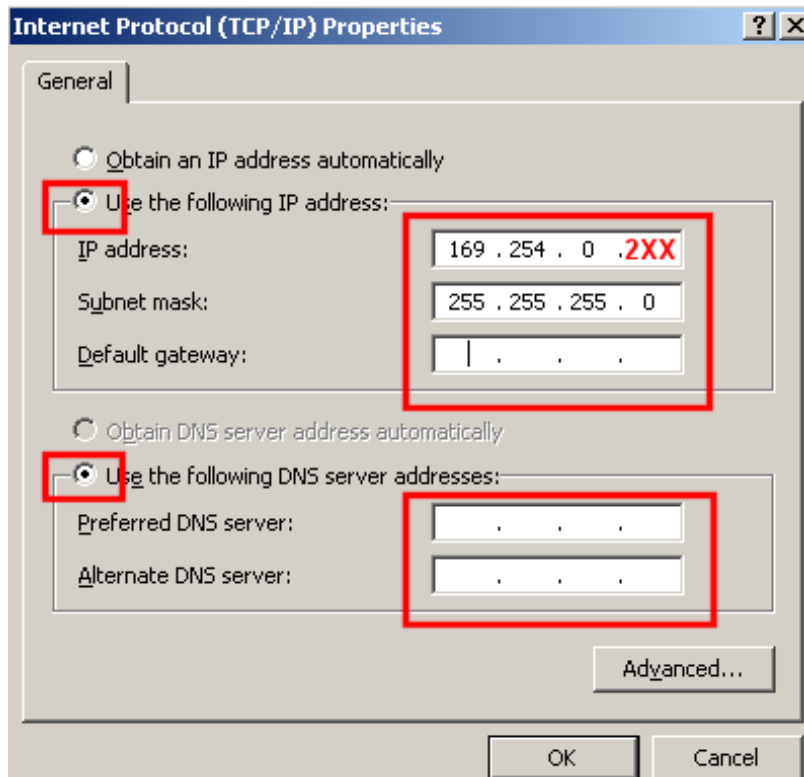
Configure the TCP/IP settings for VLAN 1 using the table on the next page.

- Do not use the same IP address on more than one server.
- Do not use 169.254.0.254 (this is assigned to the NETLAB+ server)

VMware Host Server > VLAN1 NETLAB Inside Interface > TCP/IP Properties		
IP Configuration Interface	VLAN 1 (untagged VLAN sub-interface)	
IP Address	169.254.0.250	1 st server
	169.254.0.251	2 nd server
	169.254.0.252	3 rd server
	169.254.0.253	4 th server
	169.254.0.254	NETLAB+ ... DO NOT USE
	169.254.0.240	5 th server

	169.254.0.249	14 th server
Subnet Mask	255.255.255.0	
Default Gateway	None (leave blank)	
Preferred DNS Server	None (leave blank)	
Alternate DNS Server	None (leave blank)	

You are here:



Click **OK** to save your changes.

3.4.7 Establishing the Inside Connection

In this section, you will establish a connection between the VMware host inside port and NETLAB+ server.

Objectives

- Select a reserved control switch and port.
- Configure the control switch port.
- Bring up the link.
- Verify VMware host system can connect to NETLAB+ using VLAN 1.
- Troubleshoot the connection if necessary.

3.4.7.1 Allocated Reserved Port on Control Switch for Inside Connection

There are several issues to keep in mind when selecting a reserved port. Remember that reserved ports operate in VLAN 1, so there are no consecutive port requirements. Typically, when installing control devices, it is desirable to connect NETLAB+, access servers, switched outlet devices, and all other control switches to Control Switch 1, in a hub and spoke fashion. Please refer to the *Installing the Control Plane* section of the [NETLAB+ Installation Guide](#) for detailed discussion of reserved ports and control devices.

For each VMware server you install, the inside connection may be located on any reserved port that is available on a control switch. In most cases, you may have more than one control switch and VMware server. If this is the case, you should try to select a reserved port from the same control switch where the pods associated with the VMware server reside. In some circumstances, your VMware server may be hosting several pods. Consequently, 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. The most important factor would be keeping the pod gear communication and VMware server communication located on one or two control switches.

3.4.7.2 Configure Reserved Control Switch Port for Inside Connection

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.

Example switch port configuration. Interface number will vary.

```
interface FastEthernet0/23
description inside connection for VMware Server #1
switchport mode trunk

switchport nonegotiate
no switchport access vlan
no shutdown
```

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.

3.4.7.3 Configure Trunking Between Multiple Control Switches

If the reserved port selected for your VMware server is on a different control switch than the lab equipment pods it is serving, you must ensure that inter-switch links between control switches are configured in trunking mode. Some switches models will automatically form trunks. However, it is recommended that both sides be manually configured as trunk ports per the configuration commands below.

Example switch port configuration. Interface number will vary.

```
interface FastEthernet0/24
description Trunk to control switch #2
switchport mode trunk

switchport nonegotiate
no switchport access vlan
no shutdown
```

3.4.7.4 Connect Inside Interface and Verify Link

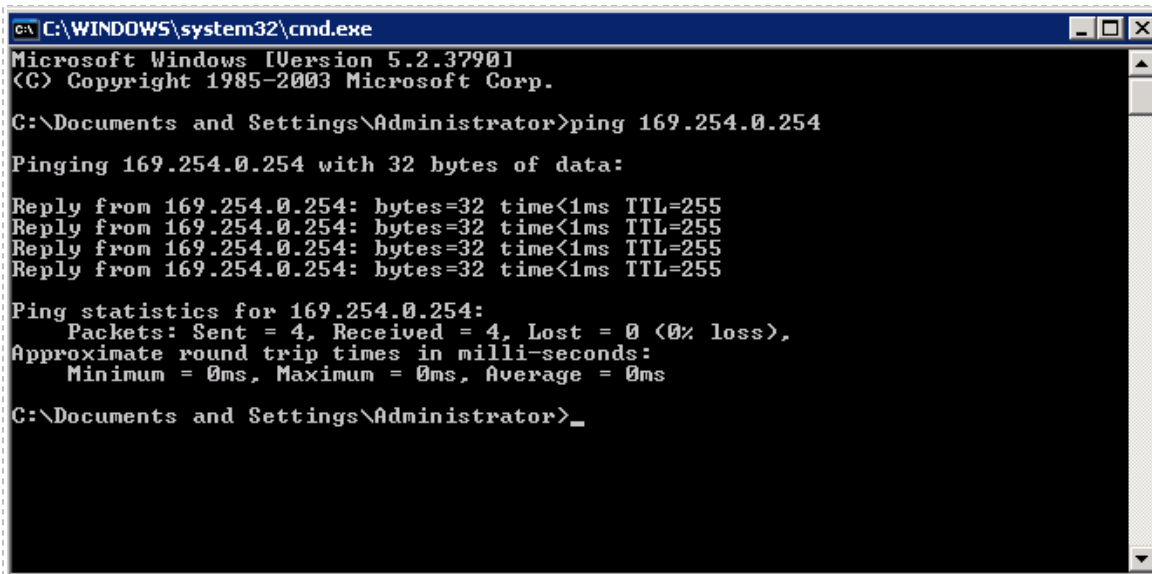
After you have configured the reserved the port as described in the previous section, verify your cabling between the reserved port and the VMware Server inside NIC. Check the interface status of the reserved port:

```
netlab-cs1#show interfaces FastEthernet 0/23
FastEthernet0/23 is up, line protocol is up (connected)
```

3.4.7.5 Verify VLAN 1 Connectivity

This section applies to ISEC and IMAN. Skip ahead to section 3.5 if you are implementing OMAN

Ping from the server to 169.254.0.254. On the VMware host, open a window for the Command Prompt and ping the inside IP address of the NETLAB+ server (169.254.0.254).



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 169.254.0.254

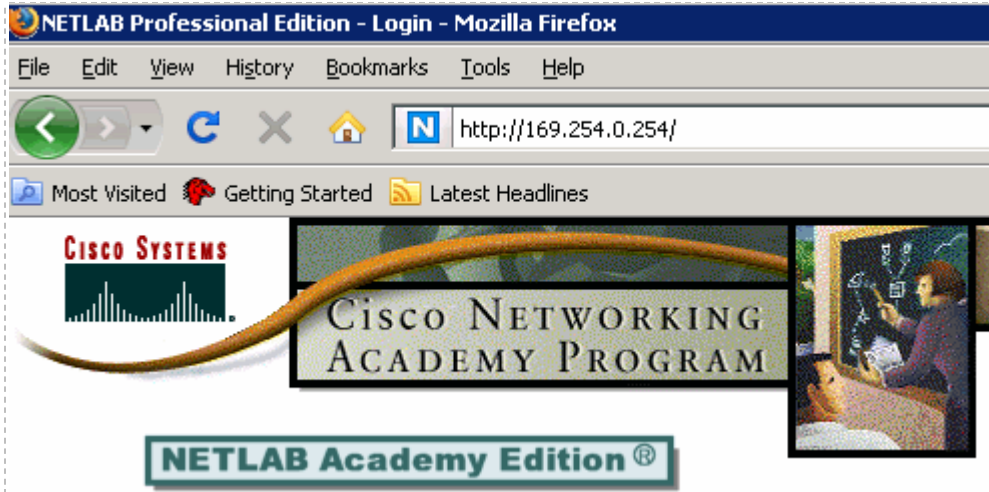
Pinging 169.254.0.254 with 32 bytes of data:

Reply from 169.254.0.254: bytes=32 time<1ms TTL=255
Reply from 169.254.0.254: bytes=32 time<1ms TTL=255
Reply from 169.254.0.254: bytes=32 time<1ms TTL=255
Reply from 169.254.0.254: bytes=32 time<1ms TTL=255

Ping statistics for 169.254.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>_
```

You may also verify the connection by opening a Web browser and accessing the NETLAB+ login page by entering the inside IP address.



The web browser should open to the NETLAB+ login page, allowing you to login using the administrator account.

3.5 Outside Interface Tasks

In this section, we will configure the outside interface on the VMware host system.

The tasks in the following sub-sections apply only to IMAN and OMAN. ISEC does not use an outside interface, so please skip ahead to the next section if you are implementing ISEC.

Objectives

- Rename the outside interface for easy identification.
- Unbind protocols that are not needed.
- Bind the TCP/IP protocol to the outside interface.
- Assign IP address to the outside interface.
- Bring up the outside interface.
- Verify IP connectivity.

3.5.1 Open Network Connections Window

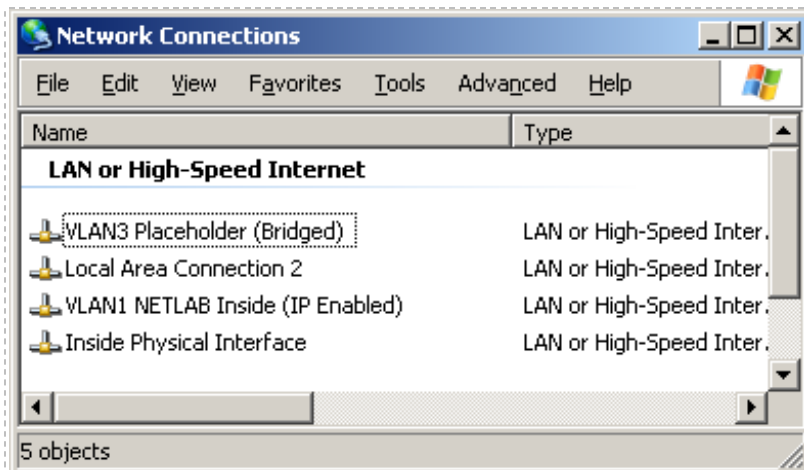
Navigate to the Network Connections panel:

Start → **Control Panel** → *right click* on **Network Connections** → **Open**

Select the detail view:


View (menu item) → **Details**

The Network Connections Panel should now look like this:



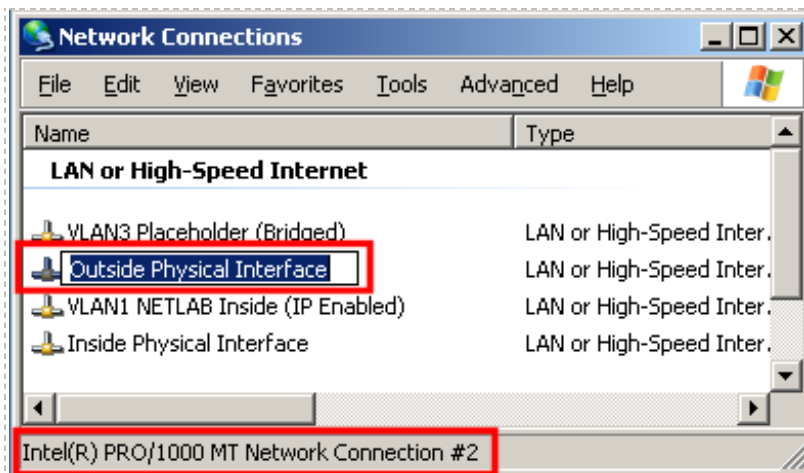
3.5.2 Select and Rename Outside Interface

Select an **unused** physical Ethernet network interface on the VMware host server that will be used for the outside interface. Identify the corresponding LAN adapter in Windows Server.

 By clicking on the interface, Windows will provide additional identifying information in the status bar.

Rename this interface to “**Outside Physical Interface**”:

- **Right click** on the interface and select **Rename**.
- Change the name to “**Outside Physical Interface**” and press **Enter**.



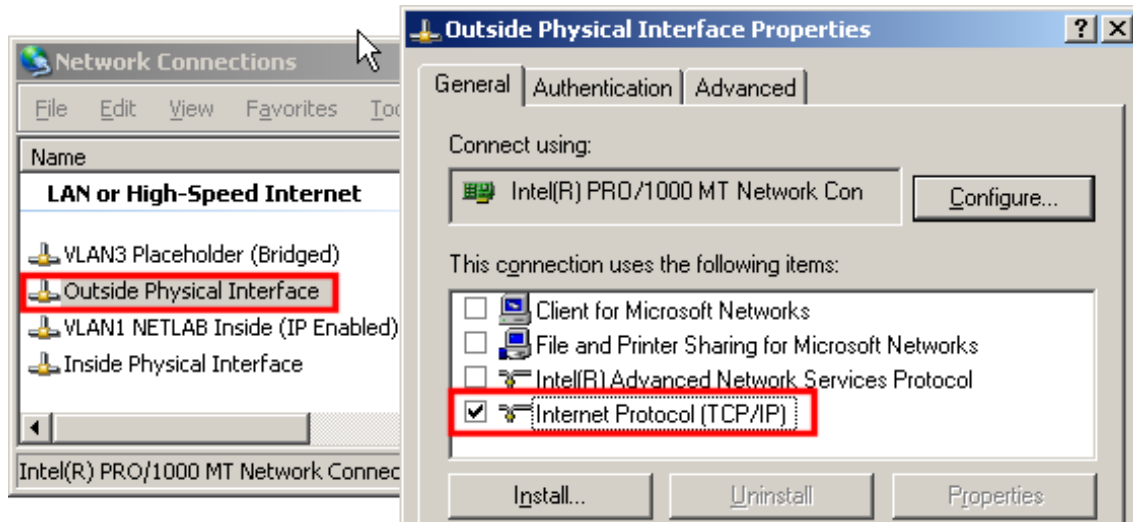
3.5.3 Configure Outside Interface Protocols

The Outside Physical Interface only runs TCP/IP, unlike the inside physical interface. There is no need to configure VLANs or 802.1q support.

From the Network Connection window, open the properties window for the Outside Physical Interface (renamed in previous task):

Right click on **Outside Physical Interface** → **Properties**.

The property window should appear:



Bind the protocols you require for outside management of your VMware server. TCP/IP should be checked.

AS NEEDED	Client for Microsoft Networks. Not recommended on a dedicated VMware host system.
AS NEEDED	File and Printer Sharing for Microsoft Networks. Not recommended for a VMware hosts system.
CHECK	Internet Protocol (TCP/IP)
UNCHECK	VMware Bridge Protocol (this item should not be listed unless VMware Server was installed before this stepped)

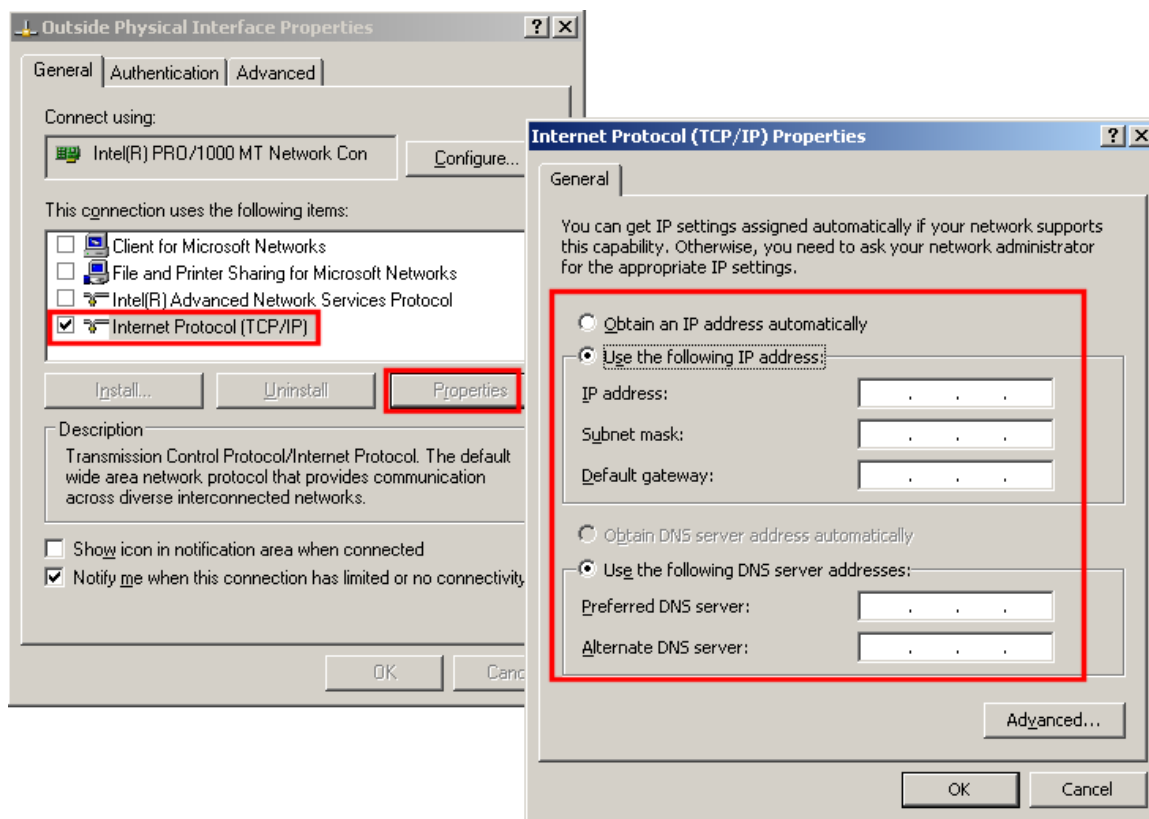
When finished, click OK. This applies the changes. You must do this before continuing to the next step.

3.5.4 Configure Outside Interface TCP/IP Settings

In this section, we configure the network protocols and TCP/IP settings for the outside interface.

ISEC does not use an outside interface. This section does not apply to ISEC.

- Return to the **Network Connections** window.
- **Right click** on the **Outside Physical Interface** to invoke the context menu.
- Select **Properties** from the context menu.
- Click on **Internet Protocol (TCP/IP)** to select it.
- Click the **Properties** button.



Assign TCP/IP parameters for the outside interface as assigned. This interface is connected to a local campus LAN, so be sure to obtain a valid unique IP address from your network administrator.

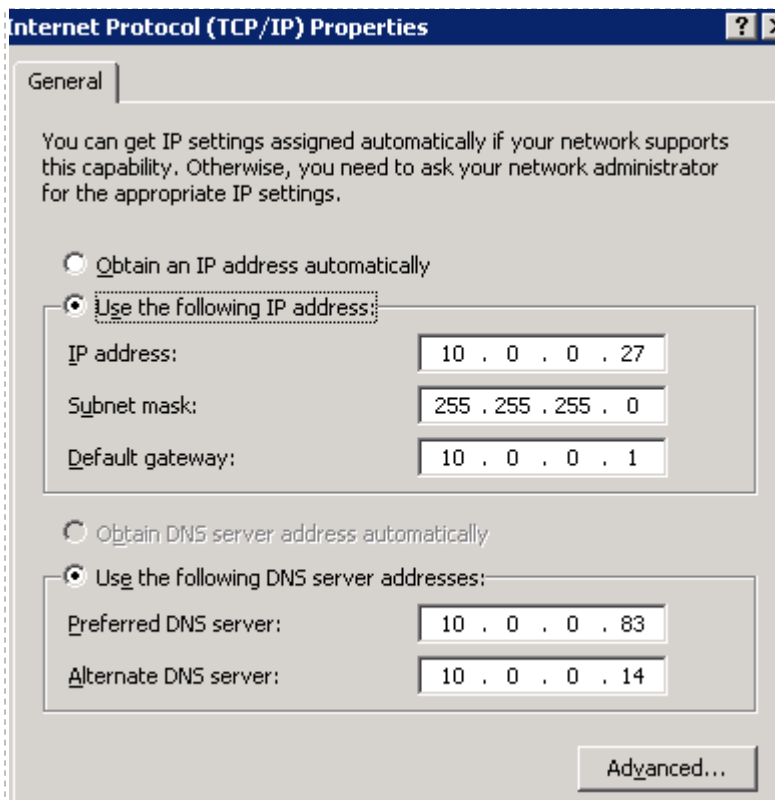
If you are using the OMAN networking model, a **static IP address** must be assigned because NETLAB+ must connect to this server using the IP address. If you are using IMAN, it is possible to use DHCP, as NETLAB+ does not need to reach the outside interface of your VMware server.

3.5.5 Connect and Verify Connectivity

After you have assigned an IP address to the **Outside Physical Interface**, you should verify connectivity to the NETLAB+ server.

Verifying connectivity is especially recommended if you use OMAN.

The IP address shown here, 10.0.0.27 is an example; your LAN may have a different address.



Ping the outside IP address of the NETLAB+ server.

The IP Address shown here is for example purposes only, your IP address will vary.

```
Command Prompt
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 10.0.0.85

Pinging 10.0.0.85 with 32 bytes of data:

Reply from 10.0.0.85: bytes=32 time<1ms TTL=255
Reply from 10.0.0.85: bytes=32 time<1ms TTL=255
Reply from 10.0.0.85: bytes=32 time<1ms TTL=255
Reply from 10.0.0.85: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.0.85:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>_
```

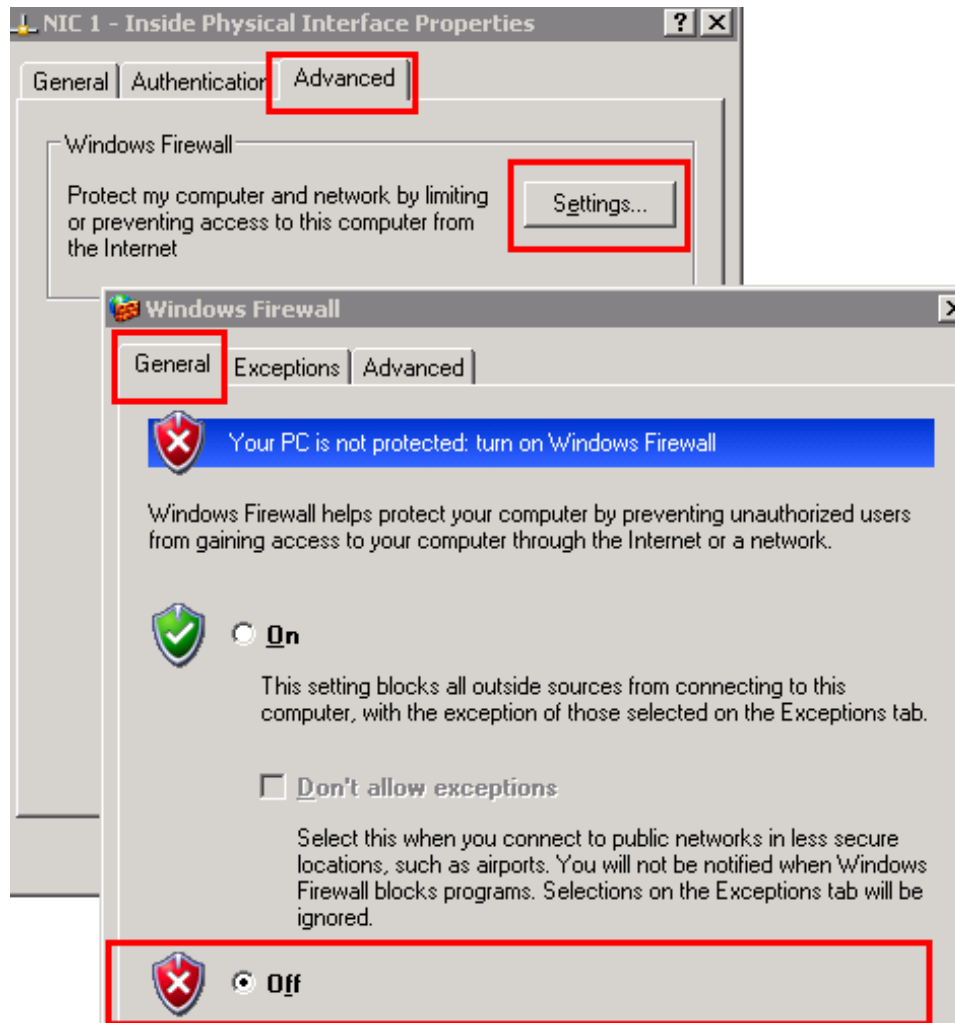
You may also open a browser and access the NETLAB+ login web page:



3.6 Disable Windows Firewall


The following guidance applies only to ISEC.

Disable the Windows Firewall function as shown so that KVM and API connections can reach the VMware host server.



Windows Firewall is not required for ISEC, and enabling it may cause connections problems that might be difficult to troubleshoot.

If you want to run the firewall anyway, ensure that the NETLAB+ inside interface (169.254.0.254) can make connections to the VMware server inside interface using the following ports: TCP 80, 443, 8222, 8333, 902, 903, 3389, 5900 through 6150, ICMP echo request/reply (ping). This list may be revised in future versions.

 Disable the firewall until everything is working.

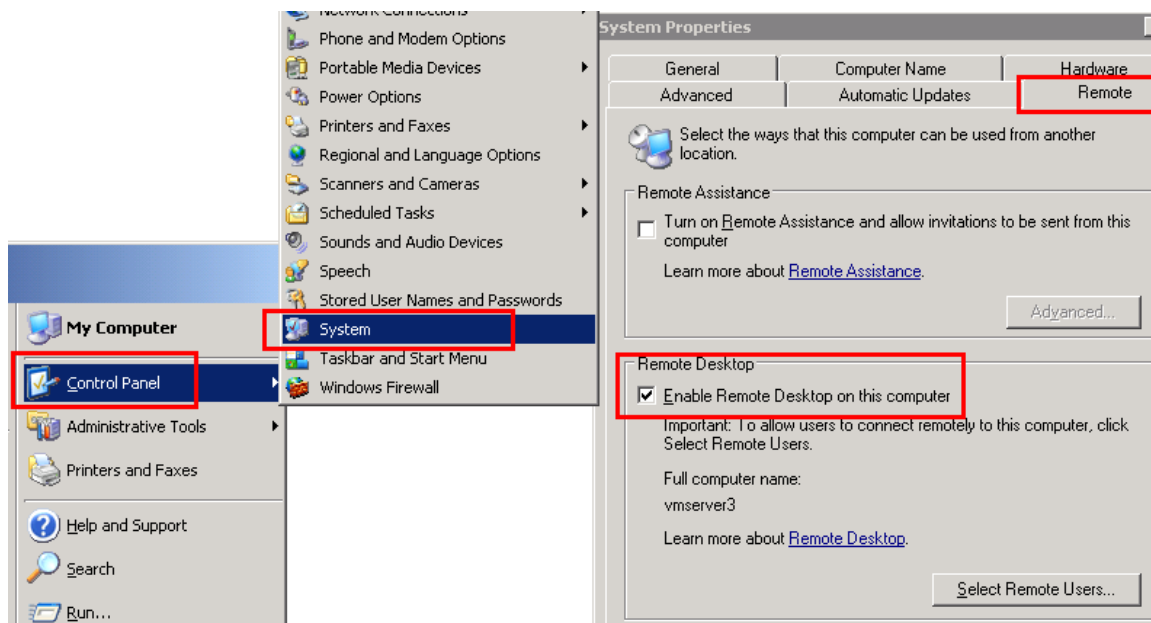
3.7 Enable Remote Desktop (Recommended)

Should you require assistance with your server or virtual machine setup, NDG can securely connect to your VMware host, using NETLAB+ as a proxy server. This access is enabled only as needed for each troubleshooting session, and then disabled at the end of the session.


Remote Desktop significantly expedites the troubleshooting process, since it allows us to review your host and virtual machine settings very quickly.

Enable Remote Desktop on the VMware server host operating system.

- **Start → Control Panel → System → Remote tab → Remote Desktop > Enable Remote Desktop** on this computer (see illustration below).



Ensure that Windows Firewall (if enabled) is not blocking TCP port 3389 on the inside interface if using IMAN or ISEC, or the outside interface if using OMAN.

 Remote Desktop requires valid credentials. NDG will require the Windows Server administrator account and password to access your host system. NDG may also provide additional configuration instructions, depending on your IP settings and firewall configuration.

3.8 Installing VMware Server Software

This section describes the tasks involved in setting up a VMware host system.

You may obtain a free download of VMware Server 2.x from VMware, Inc. Go to www.vmware.com and complete the registration process to obtain your free copy of the latest version VMware Server 2.x. During registration, you will receive a serial number, which you will later enter during installation.

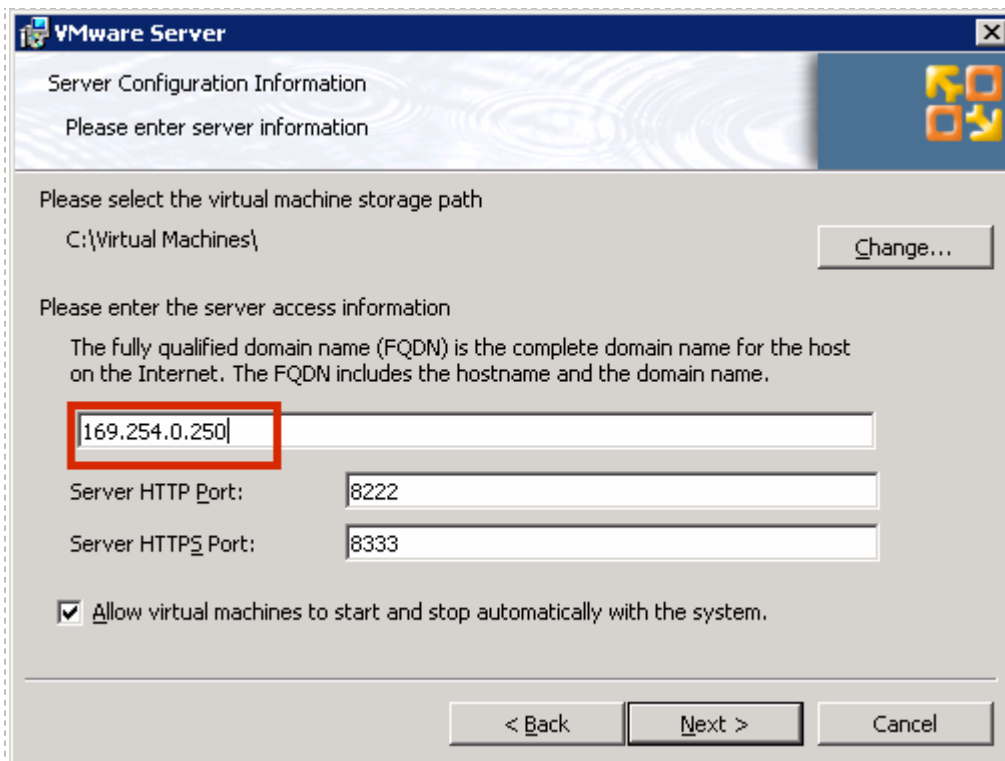
An installation wizard will guide you through the VMware product installation.



You will be required to enter the IP address for KVM and API traffic flow. If you are implementing ISEC or IMAN, use the inside network address of the VMware server. If you are implementing OMAN, use the outside network address of the VMware server. Do not enter a FQDN or host name here (use a static IP address).

Do not change the default settings for Server HTTP Port (8222) and Server HTTPS Port (8333).

The IP addresses displayed in screenshots serve as examples, your IP address may differ.

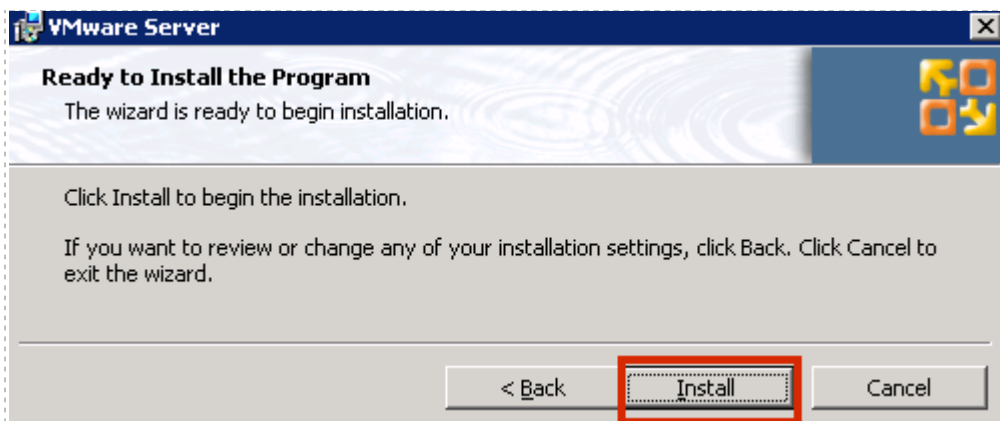


The screenshot shows the 'VMware Server' configuration window. The title bar reads 'VMware Server'. The main content area is titled 'Server Configuration Information' and contains the instruction 'Please enter server information'. Below this, there are three sections:

- 'Please select the virtual machine storage path' with a text box containing 'C:\Virtual Machines\'. To the right is a 'Change...' button.
- 'Please enter the server access information'. Below this is a paragraph explaining FQDN: 'The fully qualified domain name (FQDN) is the complete domain name for the host on the Internet. The FQDN includes the hostname and the domain name.' Below this paragraph is a text box containing '169.254.0.250', which is highlighted with a red rectangle.
- 'Server HTTP Port:' with a text box containing '8222'.
- 'Server HTTPS Port:' with a text box containing '8333'.

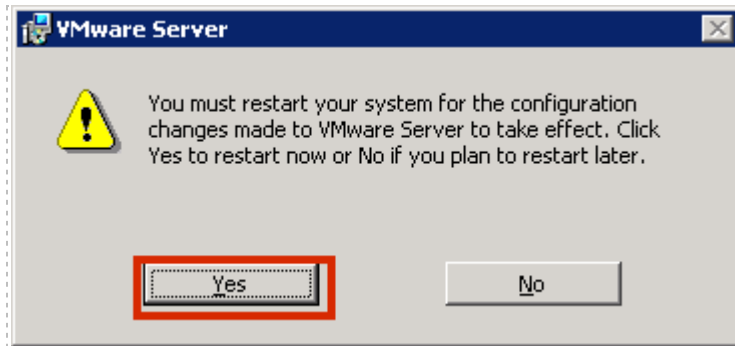
At the bottom, there is a checked checkbox labeled 'Allow virtual machines to start and stop automatically with the system.' Below the checkbox are three buttons: '< Back', 'Next >', and 'Cancel'.

Click **Install** to begin the installation process.



The screenshot shows the 'VMware Server' window at the 'Ready to Install the Program' step. The title bar reads 'VMware Server'. The main content area is titled 'Ready to Install the Program' and contains the instruction 'The wizard is ready to begin installation.' Below this, there are two paragraphs: 'Click Install to begin the installation.' and 'If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.' At the bottom, there are three buttons: '< Back', 'Install', and 'Cancel'. The 'Install' button is highlighted with a red rectangle.

When prompted, select **Yes** to restart your system to allow the configuration changes to take effect.

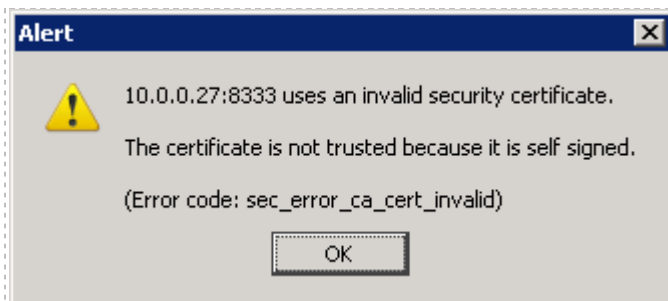


After the system has restarted, click on the VMware server desktop icon.




Click **OK** to acknowledge the security alert.

Please be aware that the pages displaying this security alert information on your system may differ slightly, depending on your browser selection.



Select the option to add an exception.



Secure Connection Failed

10.0.0.27:8333 uses an invalid security certificate.


The certificate is not trusted because it is self signed.

(Error code: sec_error_ca_cert_invalid)

- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

[Or you can add an exception...](#)

Add the exception.



Secure Connection Failed

10.0.0.27:8333 uses an invalid security certificate.

The certificate is not trusted because it is self signed.

(Error code: sec_error_ca_cert_invalid)

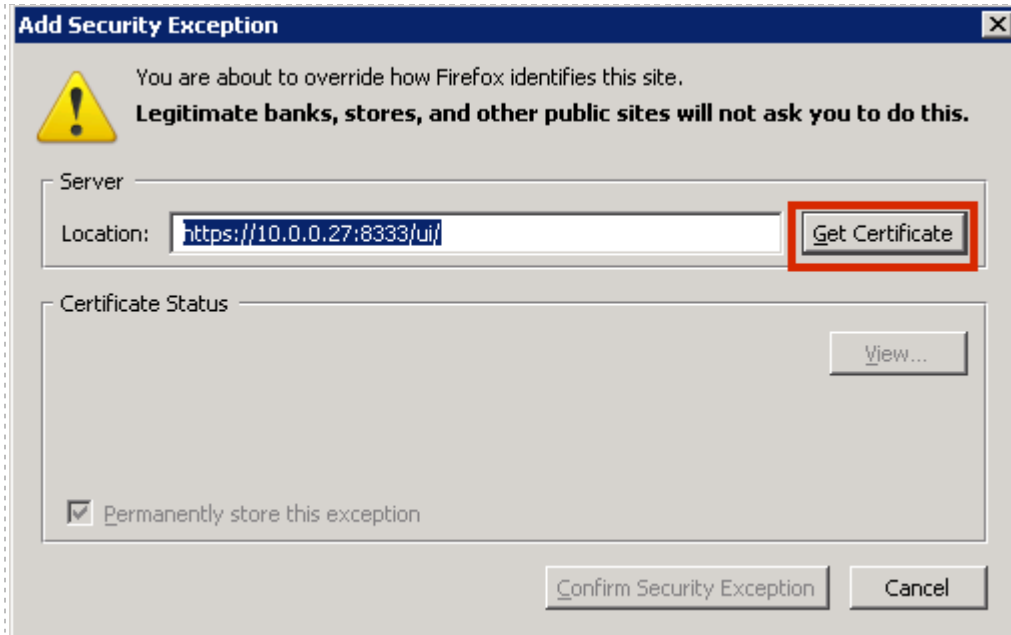
- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

You should not add an exception if you are using an internet connection that you do not trust completely or if you are not used to seeing a warning for this server.

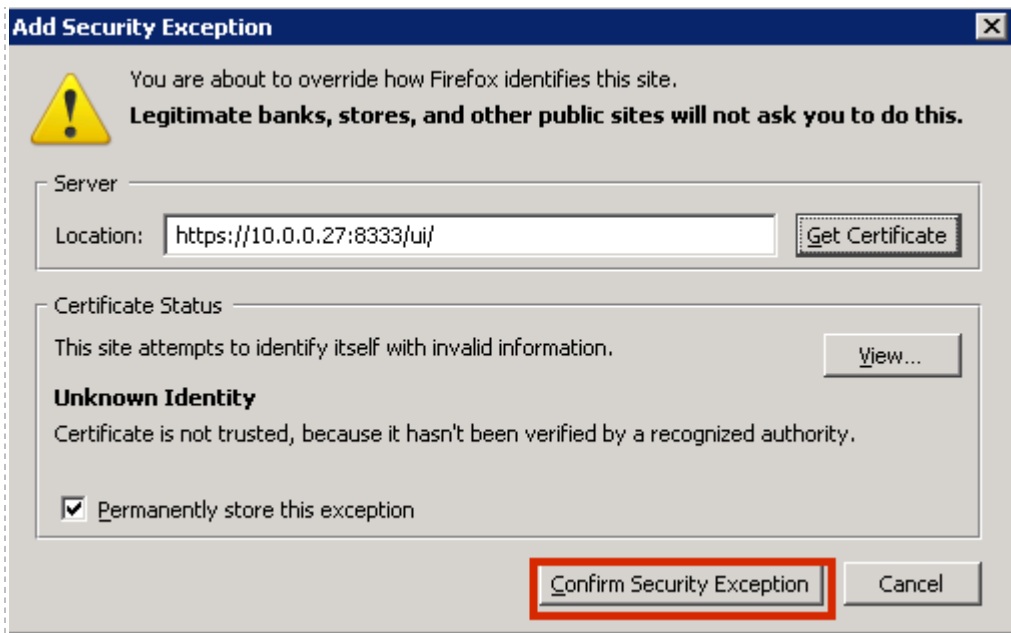
Get me out of here!

Add Exception...

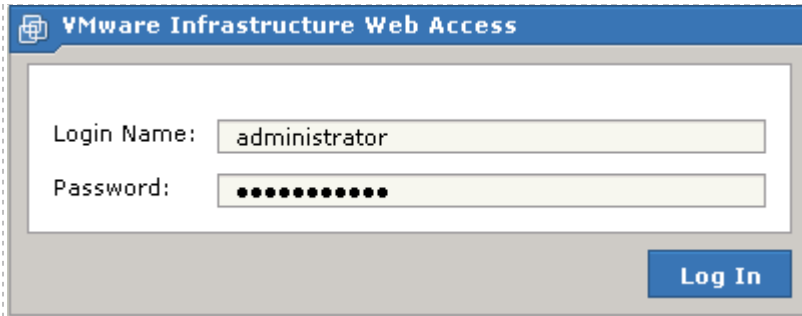
Choose the **Get Certificate** Option



Continue by confirming the security exception.



Once you have confirmed the security exception, the VMware Server login prompt will appear. You may login using your Windows Server Administrator account.



The screenshot shows a web browser window titled "VMware Infrastructure Web Access". The page contains a login form with two input fields: "Login Name:" with the text "administrator" and "Password:" with a masked password of ten dots. A blue "Log In" button is located at the bottom right of the form area.

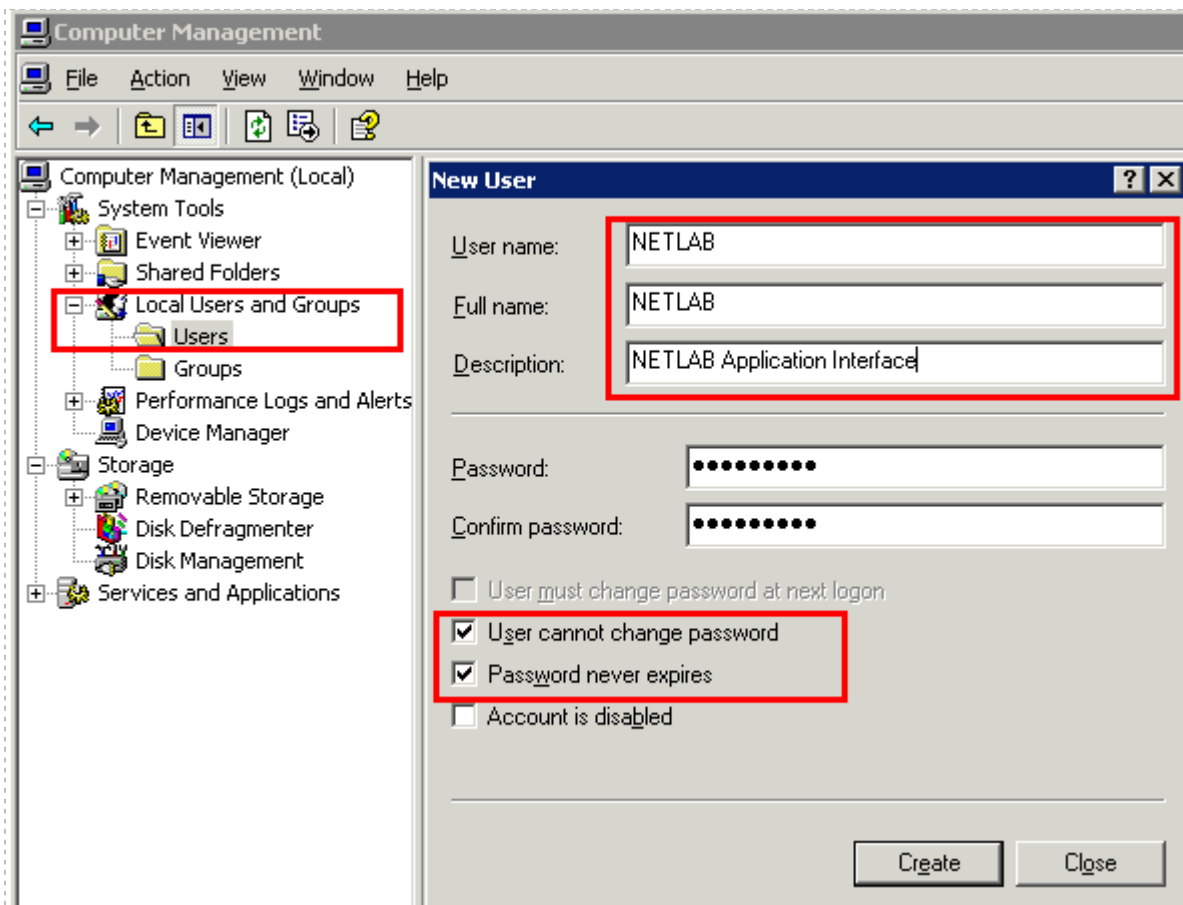
3.9 Creating a NETLAB+ Management Account

To use a VMware virtual machine with NETLAB+, a dedicated NETLAB+ management account on the host operating system is required. NETLAB+ will use this account to control virtual machines through the VMware API.

You must perform the following task from the **administrator** account.

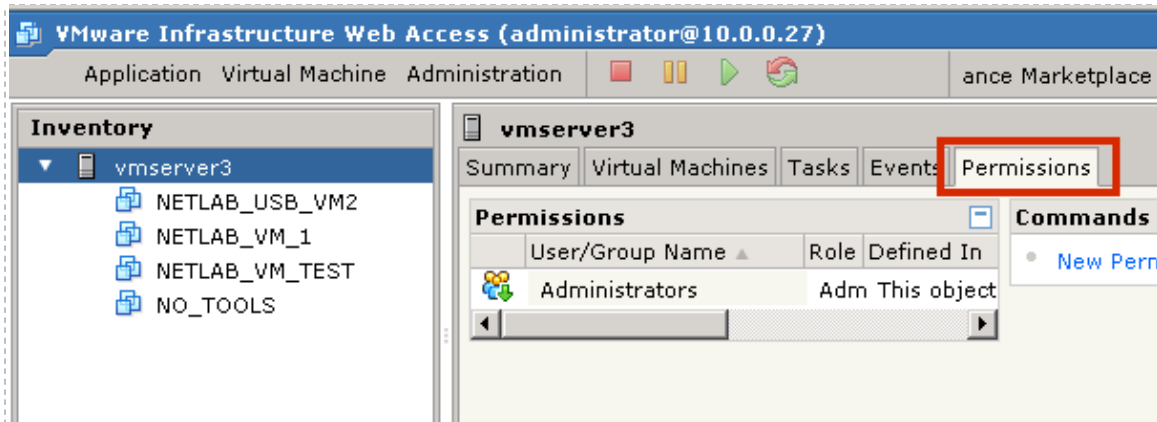
Using the Windows Computer Management interface, create a dedicated account for NETLAB+ and assign a password. The recommended user name and full name is **NETLAB** (but this is not required). Check the boxes for **Password never expires** and **User cannot change password**.

- Users → New User “NETLAB” → Password never expires is *checked*, User cannot change password is *checked*.



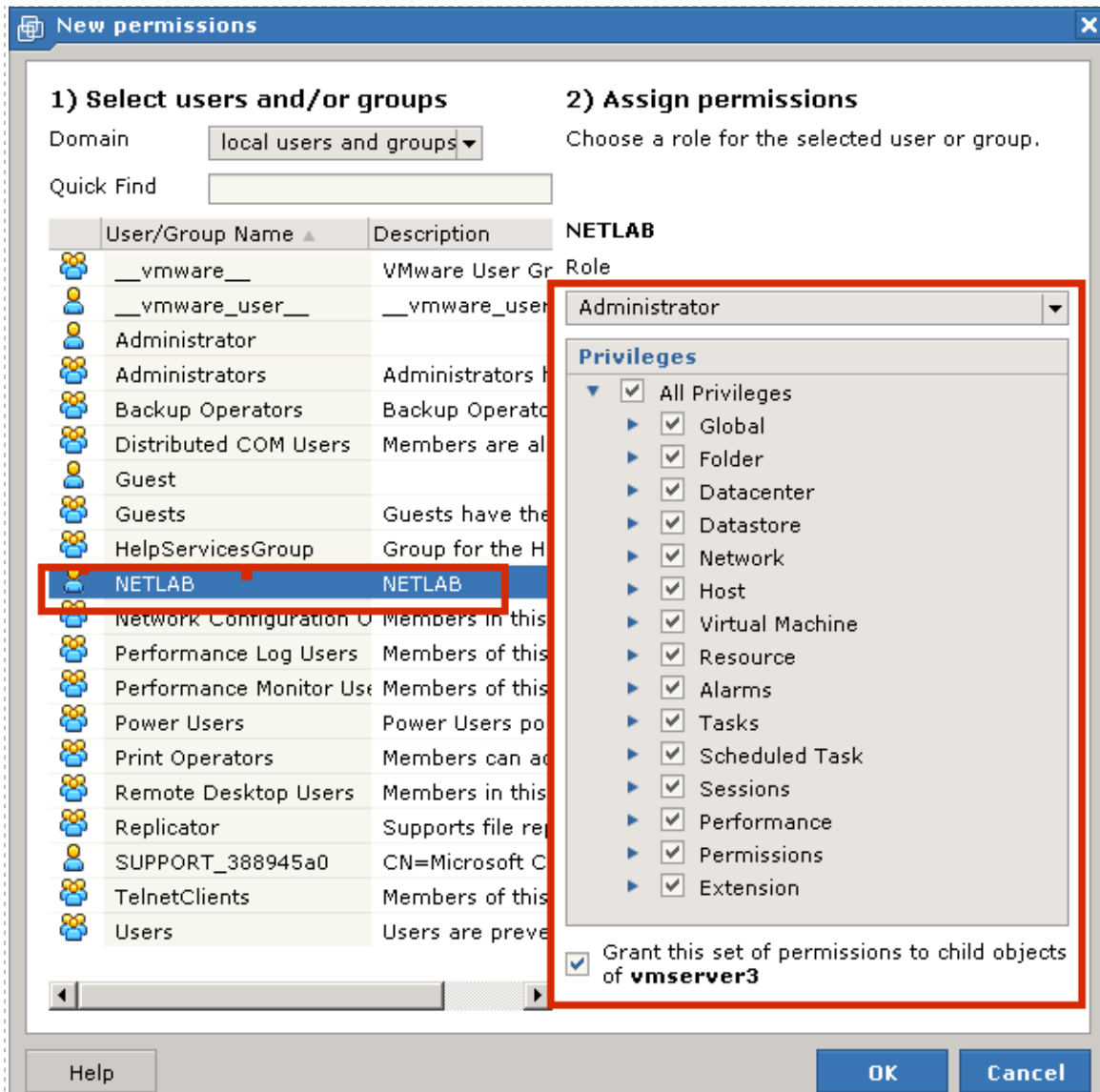
3.10 Granting Permissions

NETLAB+ must have full access to the VMware Virtual Machines. This will require modifying the permissions settings for the NETLAB+ management account (see section 3.9). Permissions are modified from the **Permissions** tab of the **VMware Infrastructure Web Access** page (referred to hereafter as the **VI Web Access** page), which is displayed after login, (see section 3.8).



Select the **NETLAB** account and assign **All Privileges**, as shown.

- **Permissions** > User/Group name **NETLAB** > **All Privileges** is *checked*

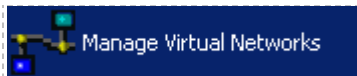
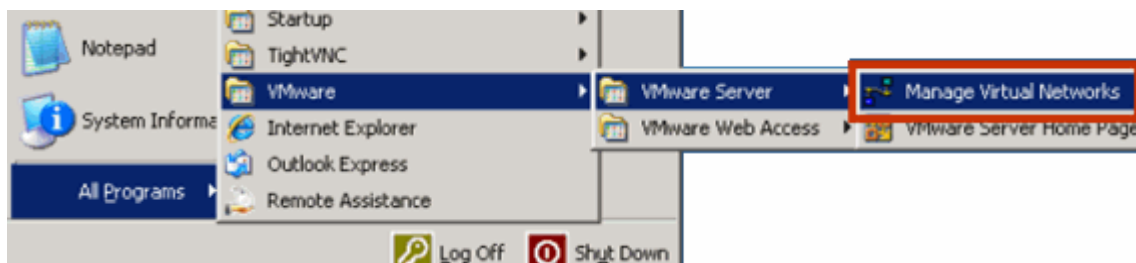


3.11 Maximizing Available Virtual Switches

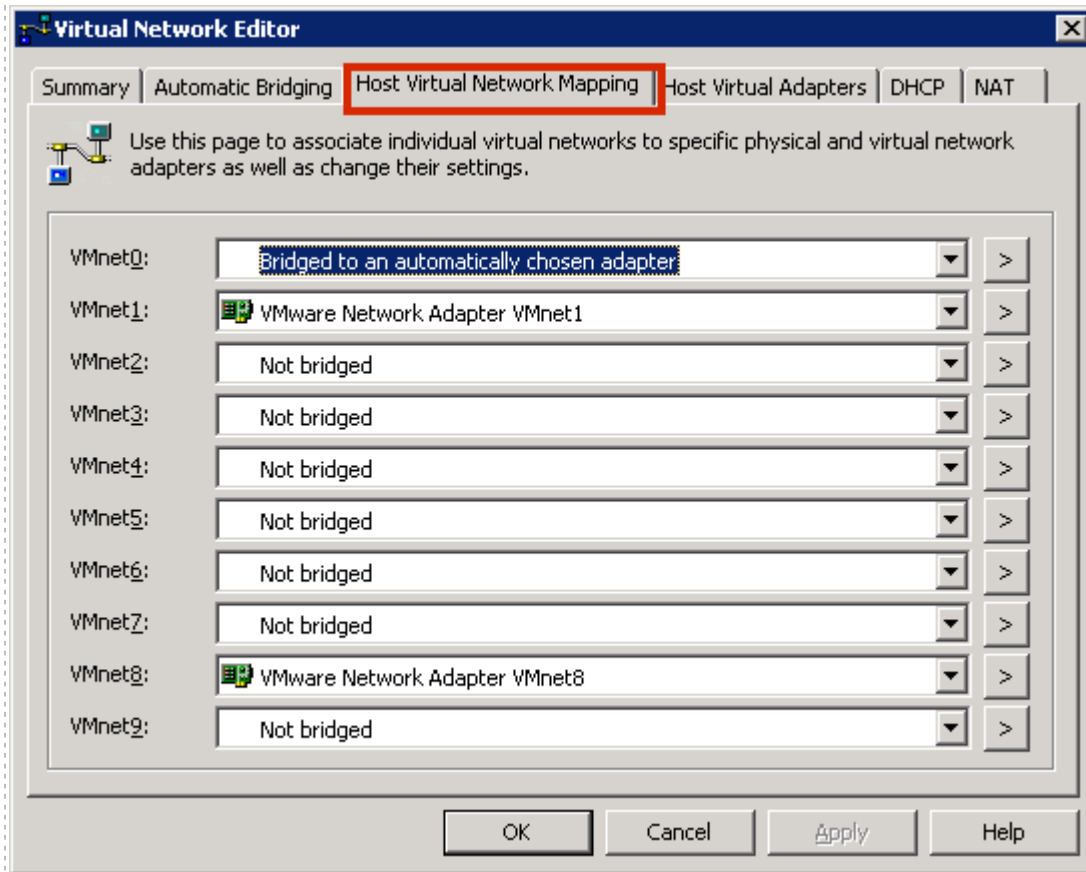
VMware uses three of its virtual networks (VMnet) to provide special guest services such as NAT and DHCP. By default, virtual networks VMnet0, VMnet1, and VMnet8 are unavailable for external connectivity to lab networks behind NETLAB+. However, if the built-in services are not needed, you can reconfigure and reclaim these virtual networks for external connectivity.

From the Start menu of your host machine, select the **Manage Virtual Networks** option to view the current VMnet settings.

Start → **All Programs** → **VMware** → **VMware Server** → **Manage Virtual Networks**



The VMnets are shown on the **Host Virtual Network Mapping** section of the Virtual Network Editor.



NETLAB Academy Edition[®] pods do not utilize the built-in VMware networking services. Therefore, the steps outlined in 0 will maximize the number of available virtual switches that can interface with lab pods.

Part 4 Adding Virtual Machines

This section explains how to configure a new VMware Server 2.x virtual machine and the proper settings required for NETLAB+. Repeat this process for each new virtual machine.

After completing preparation of each host server as described in [Part 3](#), virtual machines can be added (as *guests*) and integrated into the overall NETLAB+ system.

Objectives

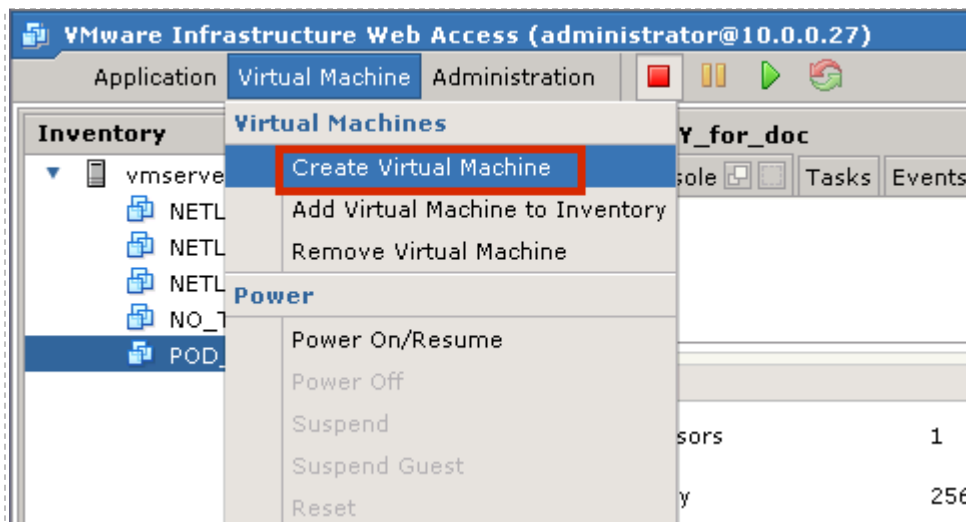
- Add virtual machines to the VMware server host system.
- Make virtual machines accessible to NETLAB+ users.

The process outlined in this section must be followed for each virtual machine added to the system.

4.1 Creating a New Virtual Machine (VM)

Working again from the, **VI Web Access**:

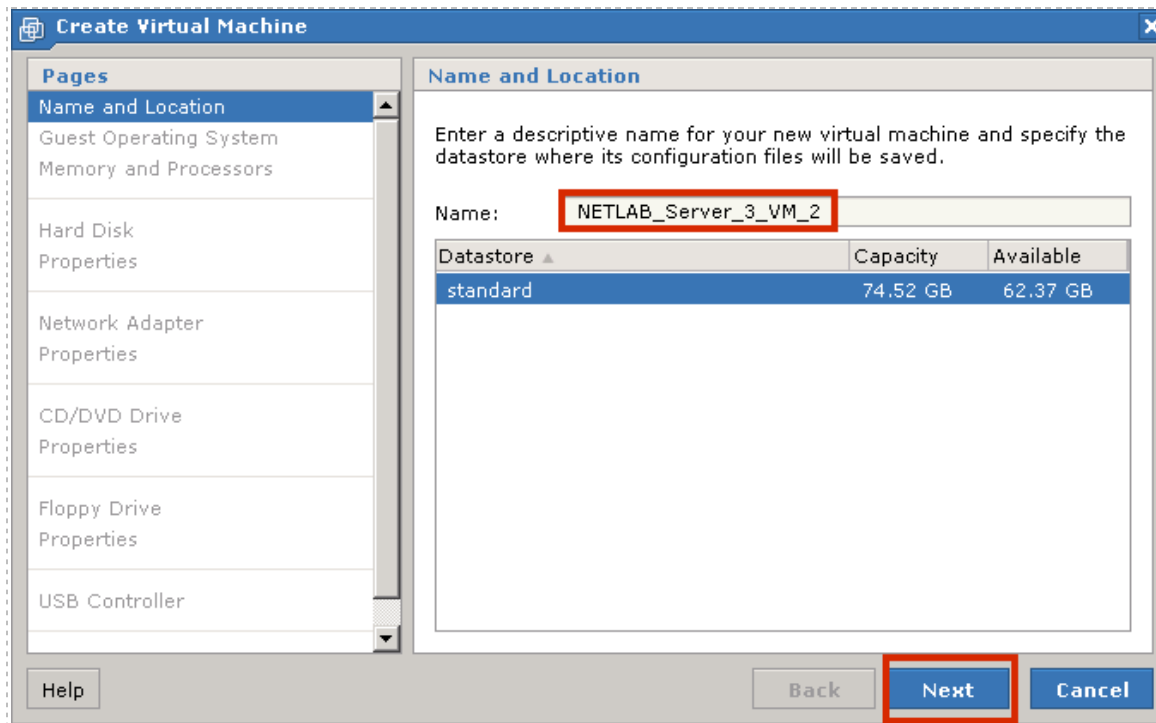
Select the **Create Virtual Machine** option on the Virtual Machine tab.



You will be prompted to enter a name for your new virtual machine.

Choose a name for your virtual machine very carefully. Here are two recommended naming conventions to consider:

- [VM NAME] = [POD_X_PC_Y]: If you do not plan on moving virtual machines from one pod to another, we recommend that you include the NETLAB+ pod number and/or PC ID in the name.
- [VM NAME] = [SERVER_X_VM_Y]: Another, more flexible naming convention would include the VMware server number and virtual machine number. This method would be useful if you are going to be moving virtual machines from one pod type to another.

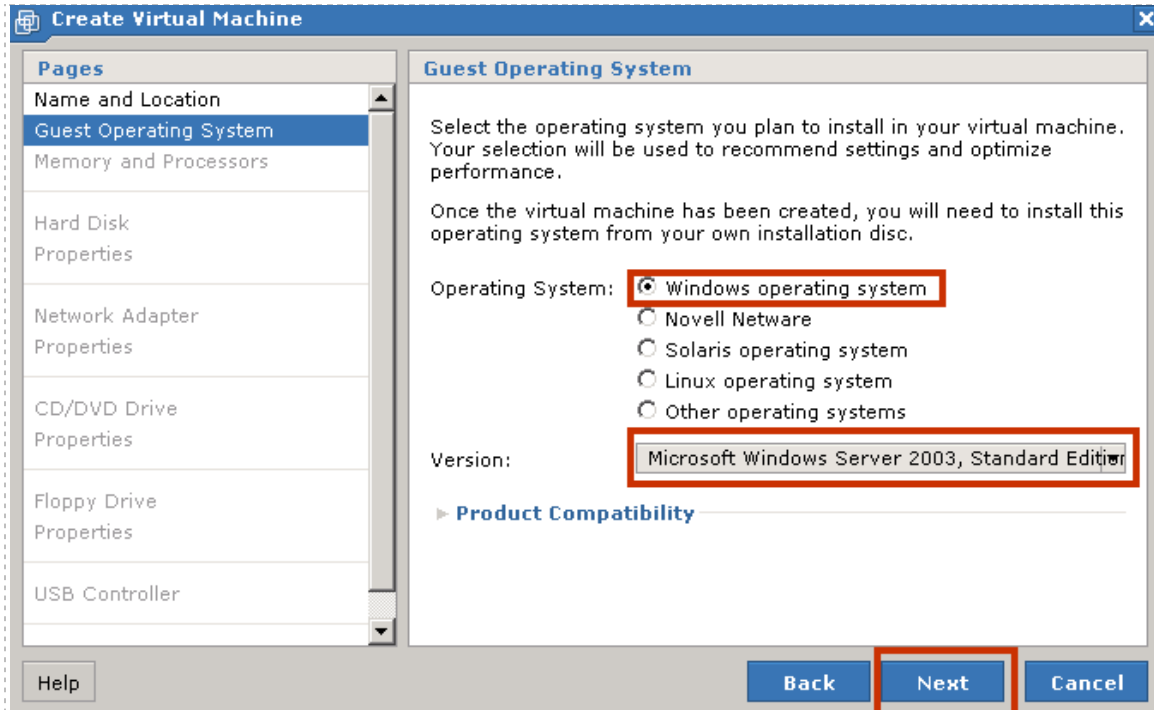


Select **Next** to continue.

4.1.1 Selecting the Guest Operating system

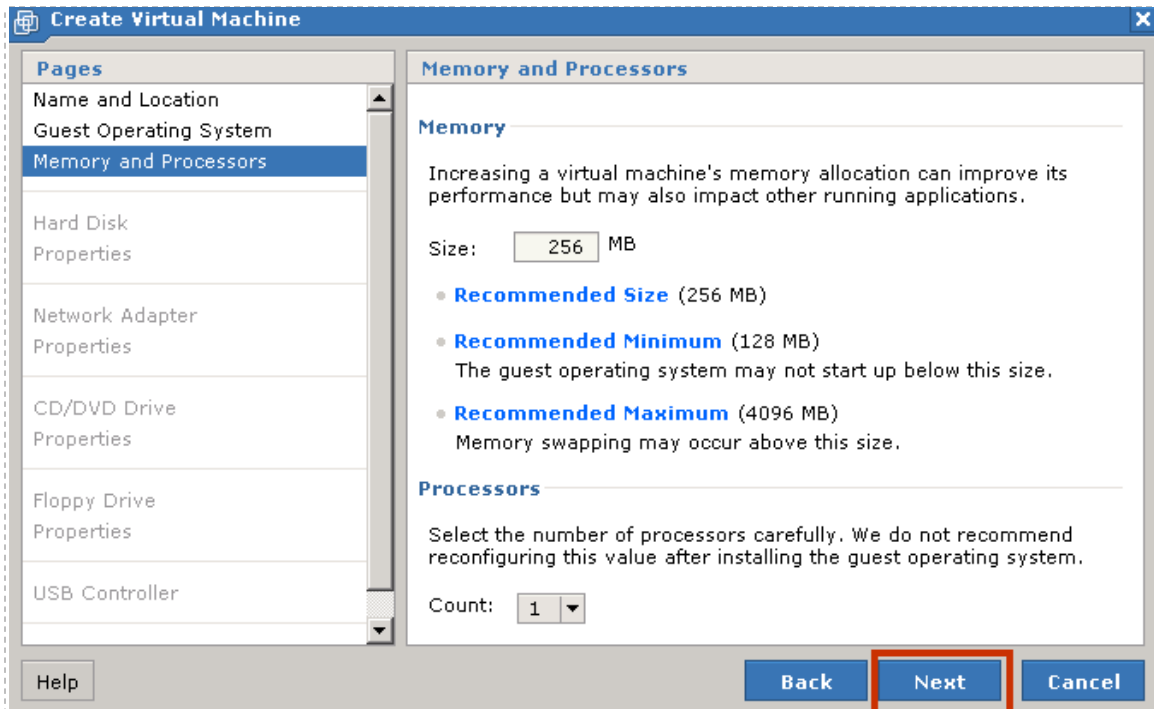
The Guest Operating system and version of your choice that you will install on your virtual machine must be selected.

In this example, Microsoft Windows Server 2003 is selected as the Guest Operating System.



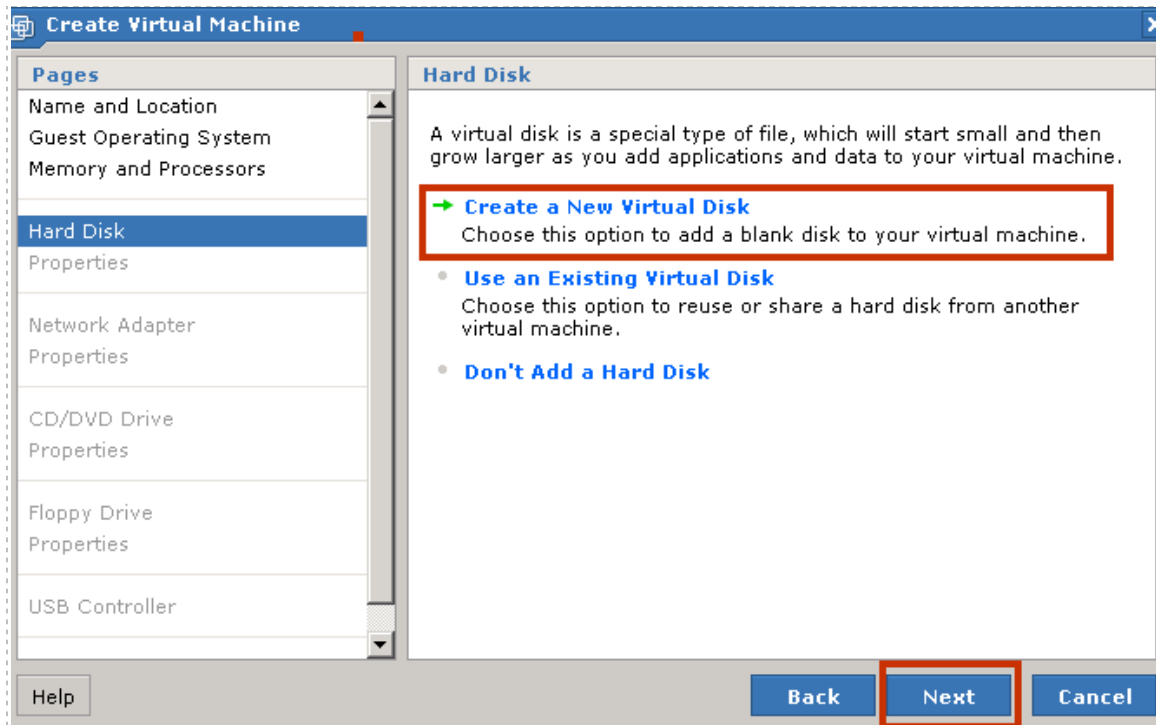
4.1.2 Selecting Memory and Processors

Choose the amount of physical memory that will be allocated to the virtual machine. In most cases, you may use the default settings for memory and processors. If memory space is a concern, you may need to select a value closer to the recommended minimum. Please make sure you do not oversubscribe system resources (see section 2.1.4.2).




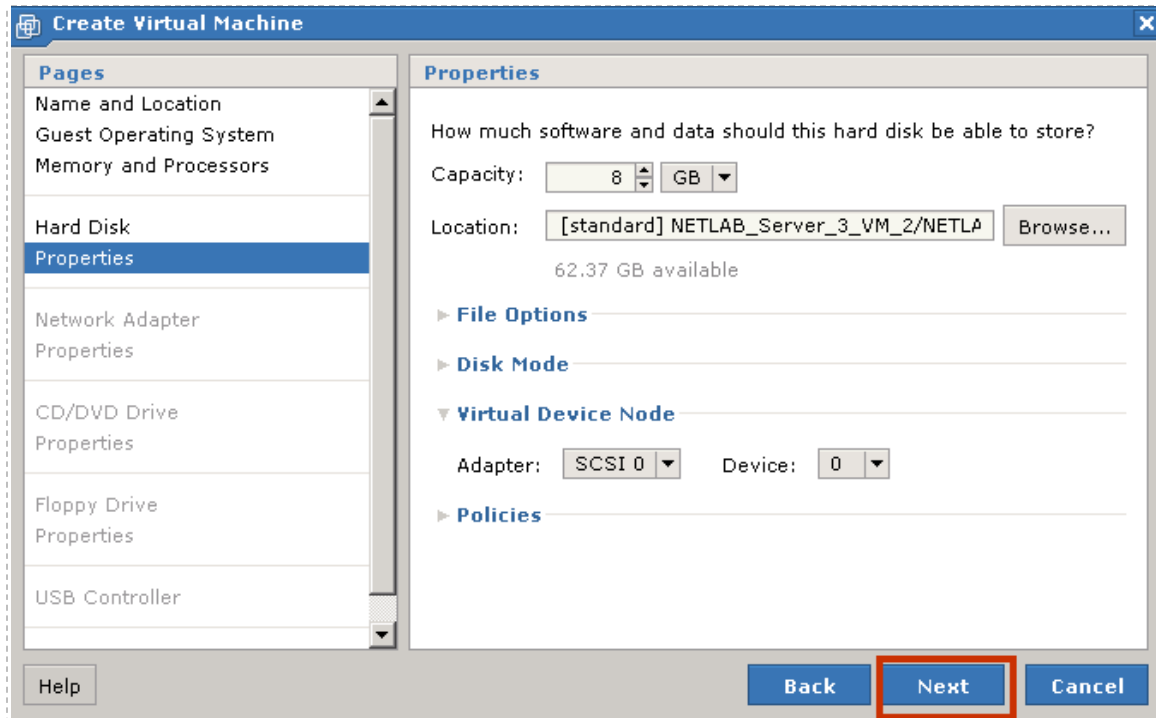
4.1.3 Creating a Virtual Hard Disk

Use the default settings to **Create a New Virtual Disk** for your virtual machine.



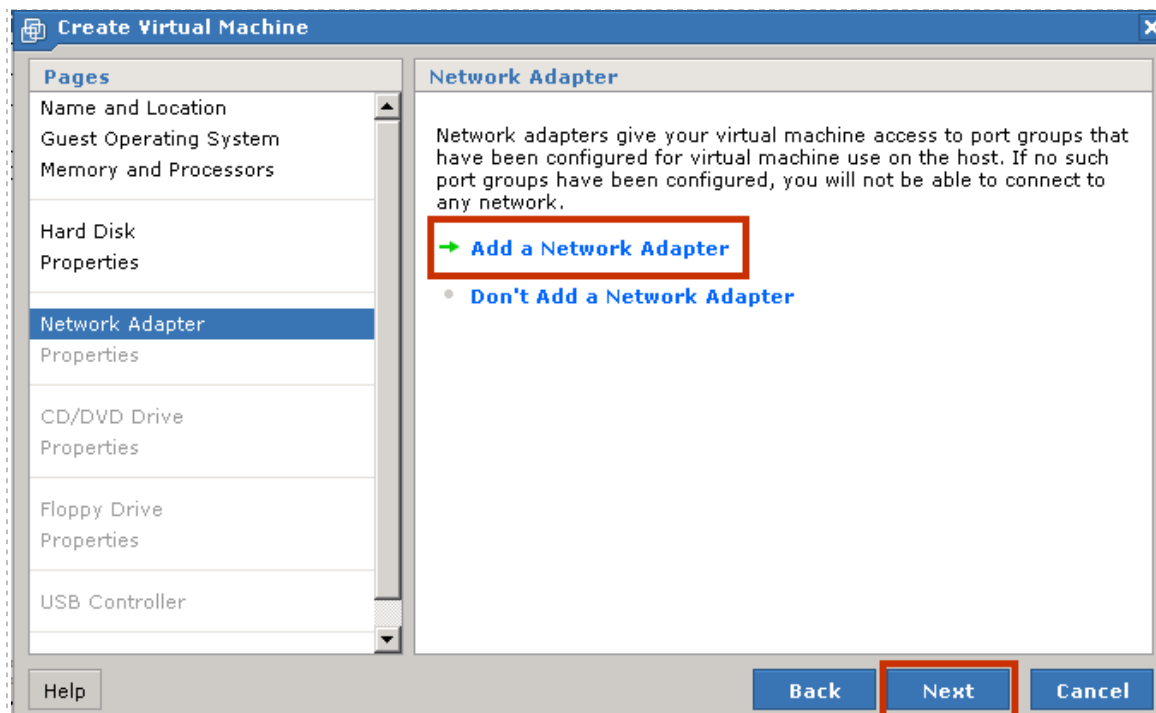
Specify the disk capacity for this virtual machine. Select a disk size that will be adequate to store the guest operating system and all of its software applications for pod labs. The example below shows a selection of 8GB; your requirements may vary.

 The use of SCSI drivers in a Windows XP or Windows Server 2003 virtual machine requires a special SCSI driver. You may [download the driver from the VMware website](#).

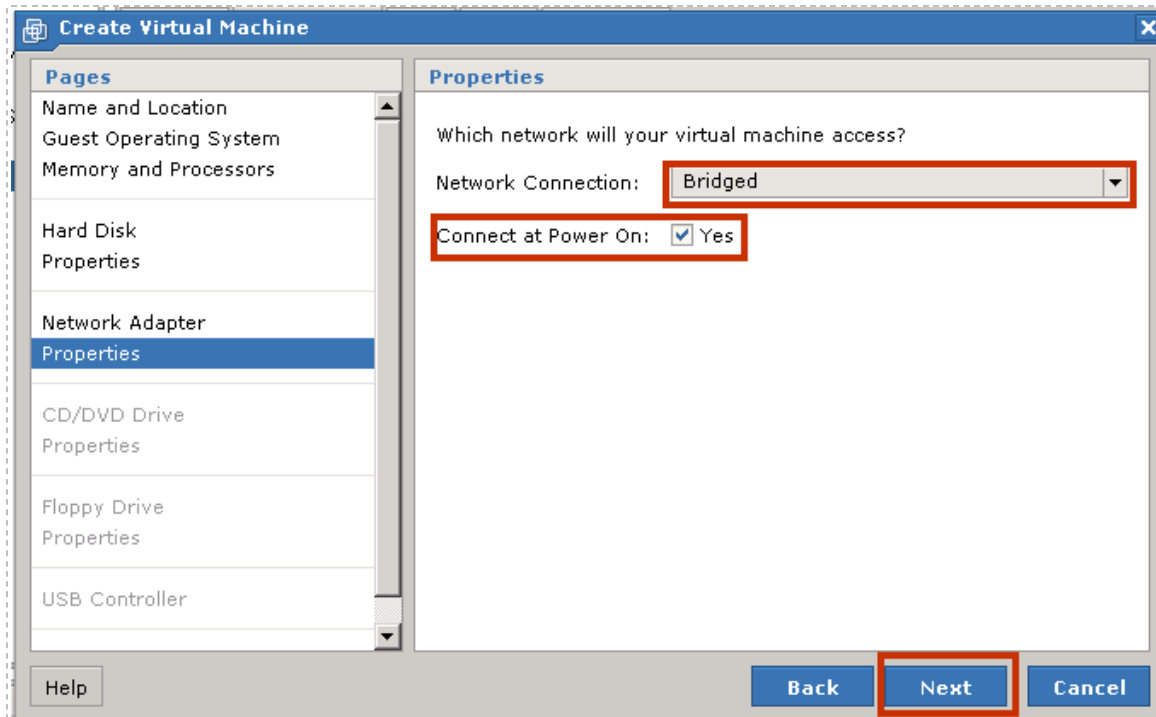


4.1.4 Adding a Network Adapter

In most cases, it will be necessary to **Add a Network Adaptor** to the virtual machine. If your equipment pod will consist of only one individual PC, a Network Adapter is not necessary.



Select a **Network Connection** type for this virtual machine. Select **Bridged**, as shown below, if this virtual machine will connect externally to a NETLAB+ VLAN. Keep the **Connect at Power On** option set to **Yes**.

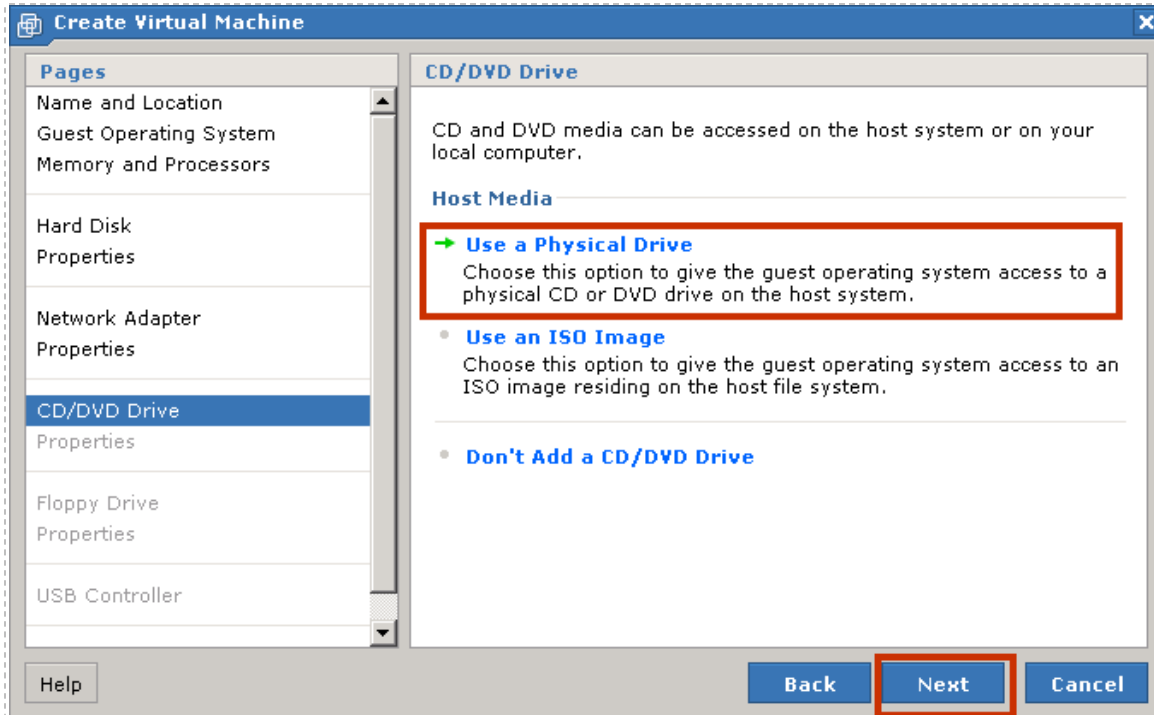


If your virtual machine will be connected to an external network, it will be necessary to edit the virtual NIC, after the virtual machine is created (see section 5.3).

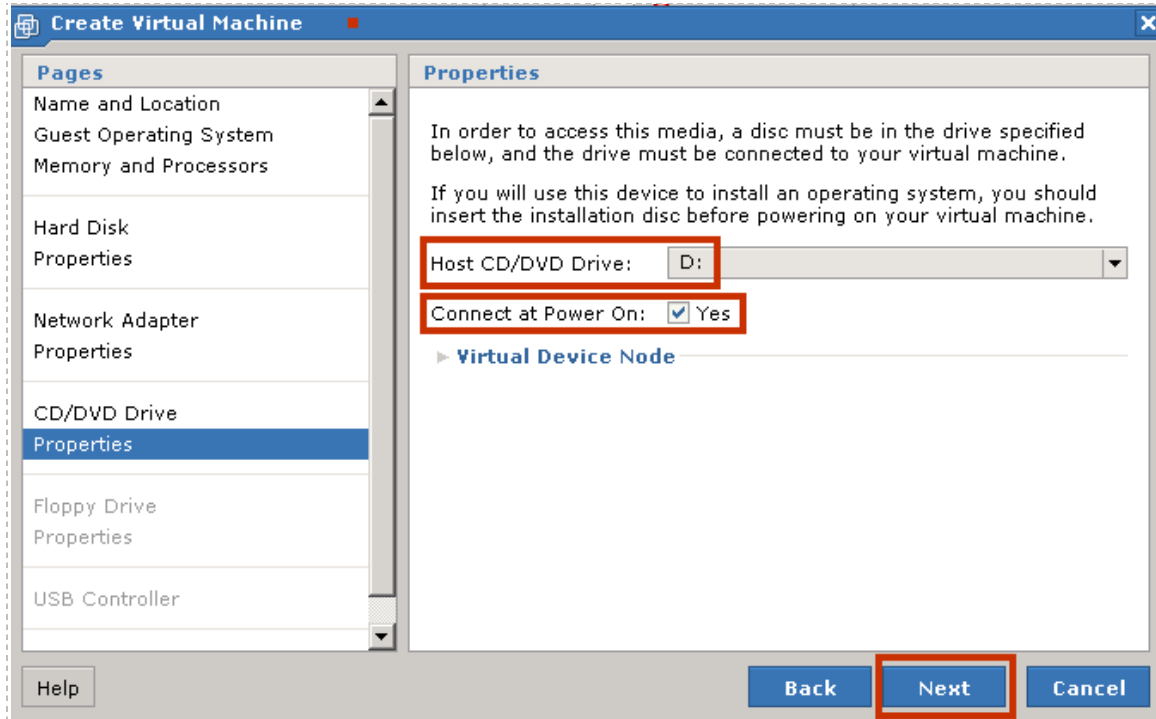
4.1.5 Selecting CD/DVD Properties

Next, you may use the default option, **Use a Physical Drive** in order to give the guest operating system access to the CD/DVD drive on the host system which will allow you to install the guest operation system. If you prefer, you may select the option to **Use an ISO Image** to give the guest operating system access to an ISO image residing on the host file system in order to install the guest operating system.

In this example, the option to Use a Physical drive was selected.

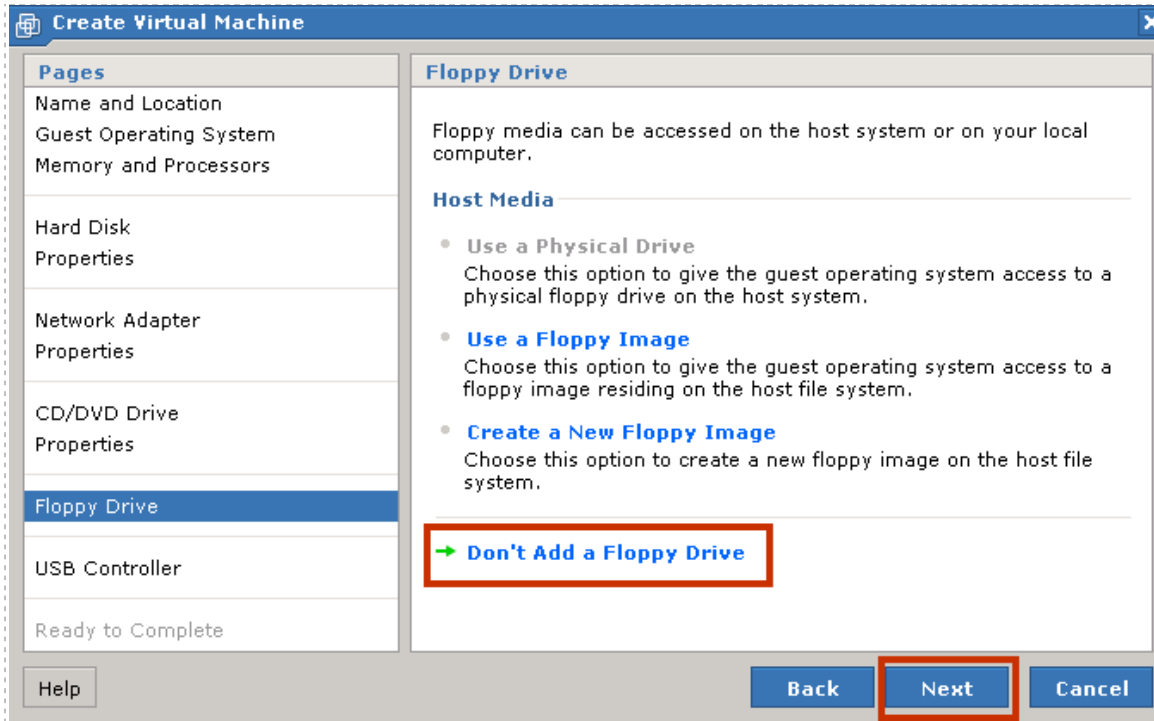


If you have selected the option to use a physical drive, you will be prompted to select the CD/DVD drive on your host system that you will use to install the guest operating system. This setting will be edited after the guest operating is installed, as described in section 4.4. The **Connect at Power on** check box must be *checked*.



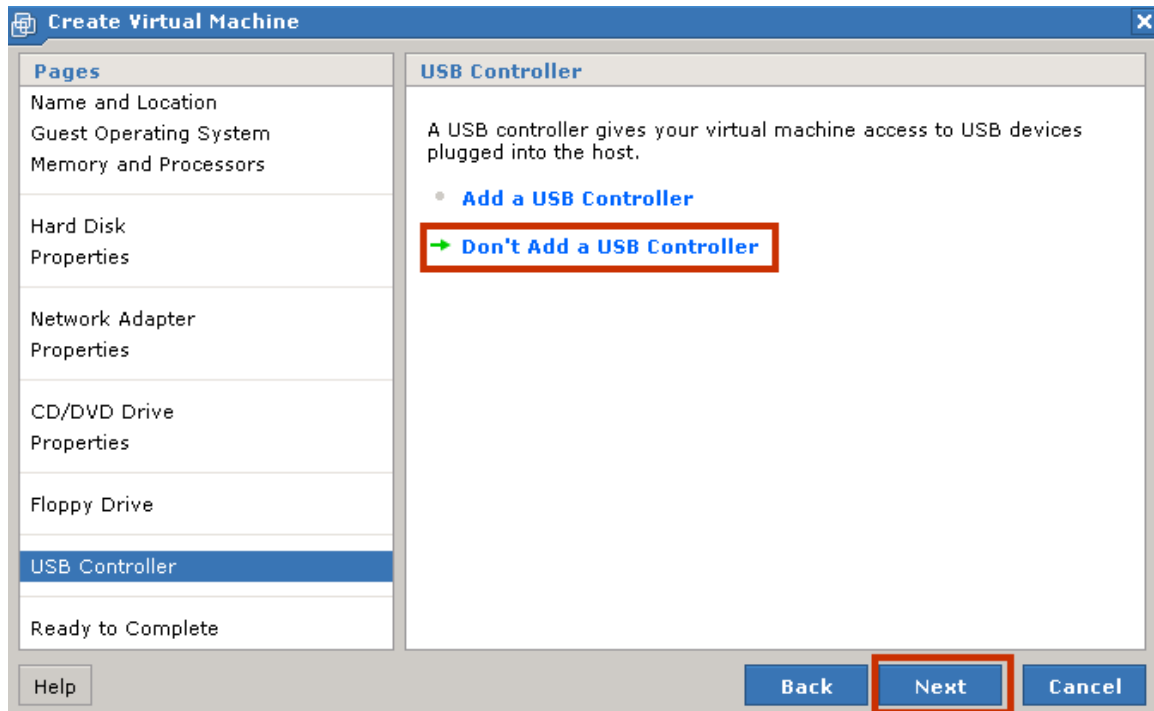
4.1.6 Selecting Floppy Drive Options

A floppy drive is not necessary. Select the **Don't add a Floppy Drive** option.



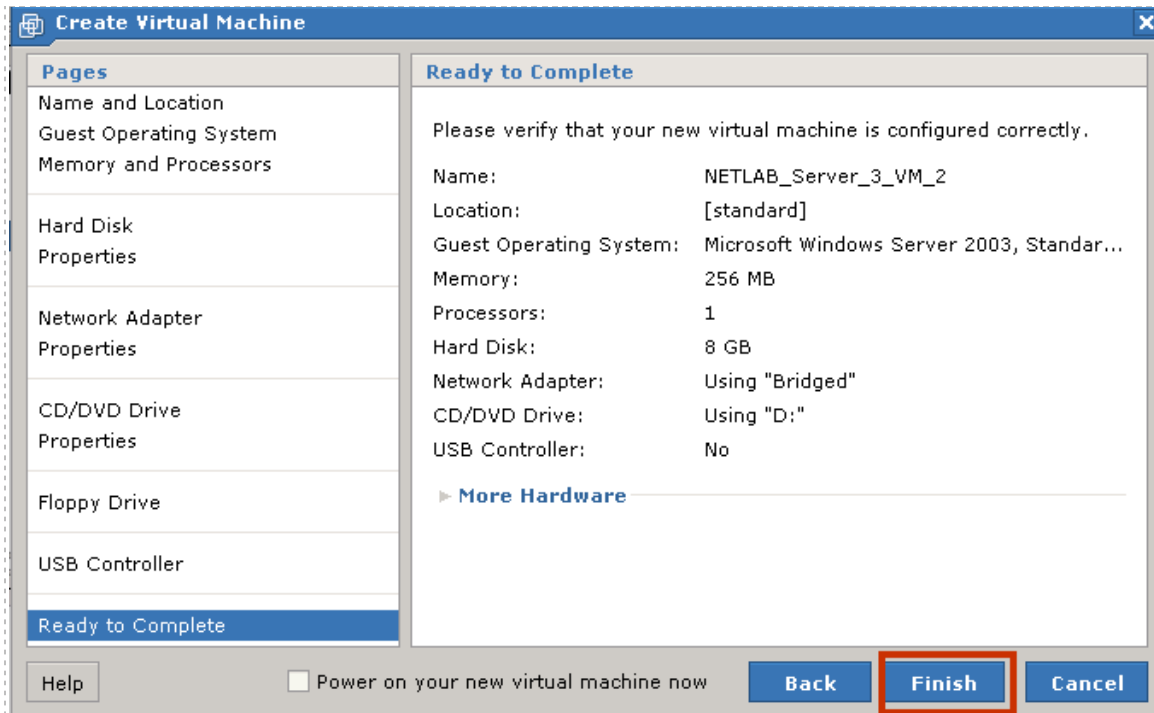
4.1.7 Selecting USB Controller Options

A USB controller is not necessary. Select the **Don't Add a USB Controller** option.

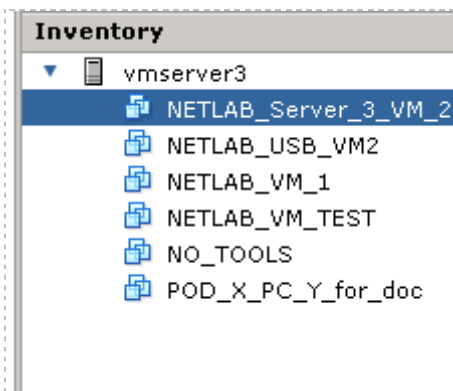


4.1.8 Verifying the Virtual Machine Configuration Settings

Select **Finish** after verifying the configuration settings displayed on the page.



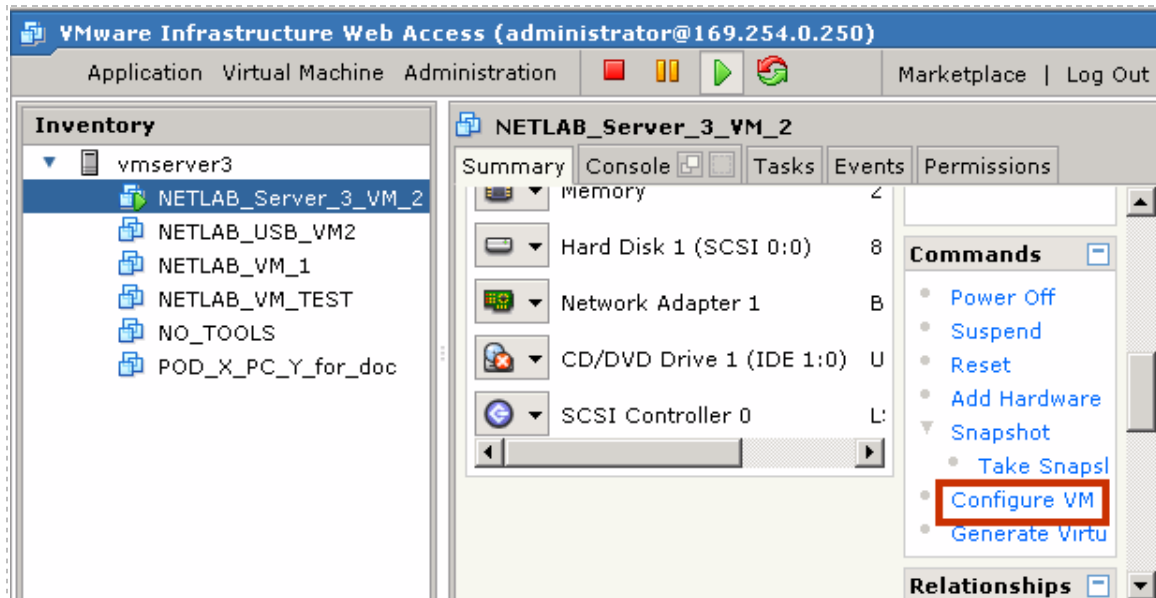
Your virtual machine will now be listed in the virtual machine inventory.



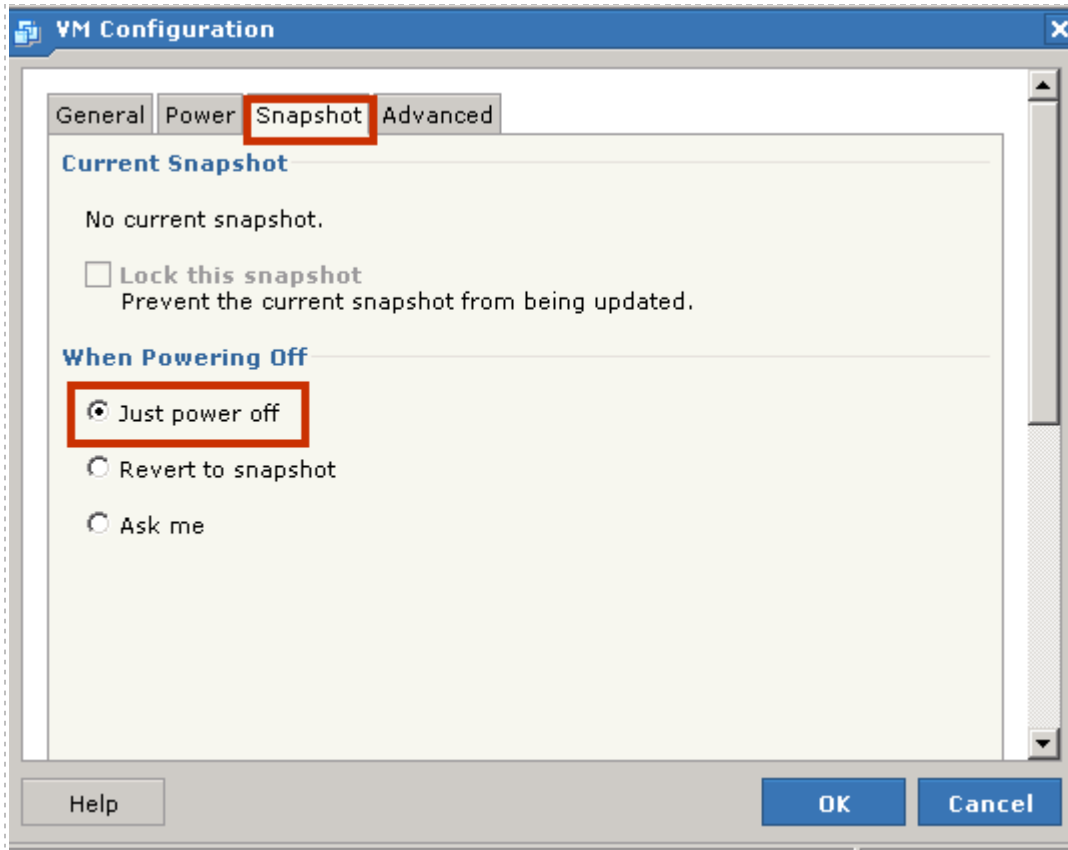
4.2 Setting Snapshot Options

NETLAB+ works in conjunction with VMware snapshots to restore a virtual machine to a clean state. This can occur automatically at the end of a lab reservation, or when a user selects the scrub command from the NETLAB+ action tab (see the *Action Tab* section of the [NETLAB+ Instructor Guide](#)).

Verify that the snapshot setting for your virtual machine is set to **Just Power Off**. This setting is accessed in the Commands section by selecting **Configure VM**.



Select the **Snapshot** tab and make certain the **Just Power Off** setting is selected.



For scrub operations, NETLAB+ will Revert to Snapshot by using internal calls through the VMware API. This will allow NETLAB+ to restore the PC to a clean state.

Use of the **Just Power Off** setting is specific to VMware Server version 2.x.

If you are upgrading to VMware Server 2.x, from VMware server 1.x or GSX, it is necessary to change the power-off option from "Ask me" to **Just Power Off**. Please see [Appendix D](#) for details.

4.3 Installing a Guest Operating System

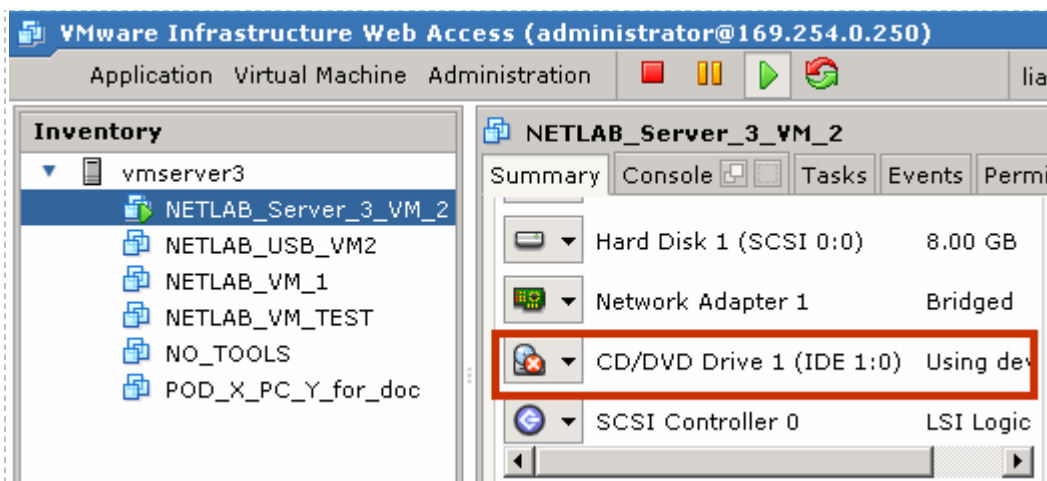
After you have configured the virtual machine settings, you must install an operating system on the virtual machine. During the virtual machine installation process, you configured to have access to the physical CD/DVD drive on your host system, or to have access to an ISO image.

Depending on your selection, insert the operating system CD in the server's CD/DVD drive or access the location of the ISO image. Follow the installation procedure as prompted. Please refer to section 2.1 for information on software requirements and product licensing.

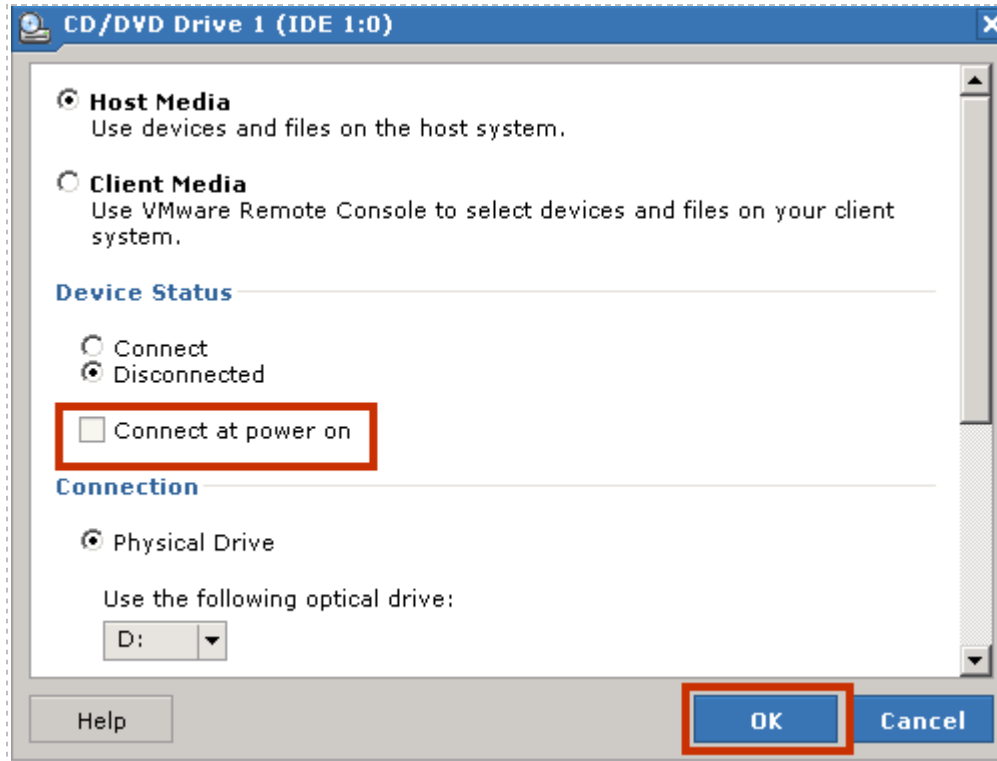
4.4 Editing the Virtual CD/DVD Device

If you have configured your virtual machine to access the physical CD/DVD drive on your host machine, make sure to edit the CD/DVD device with the recommended settings.

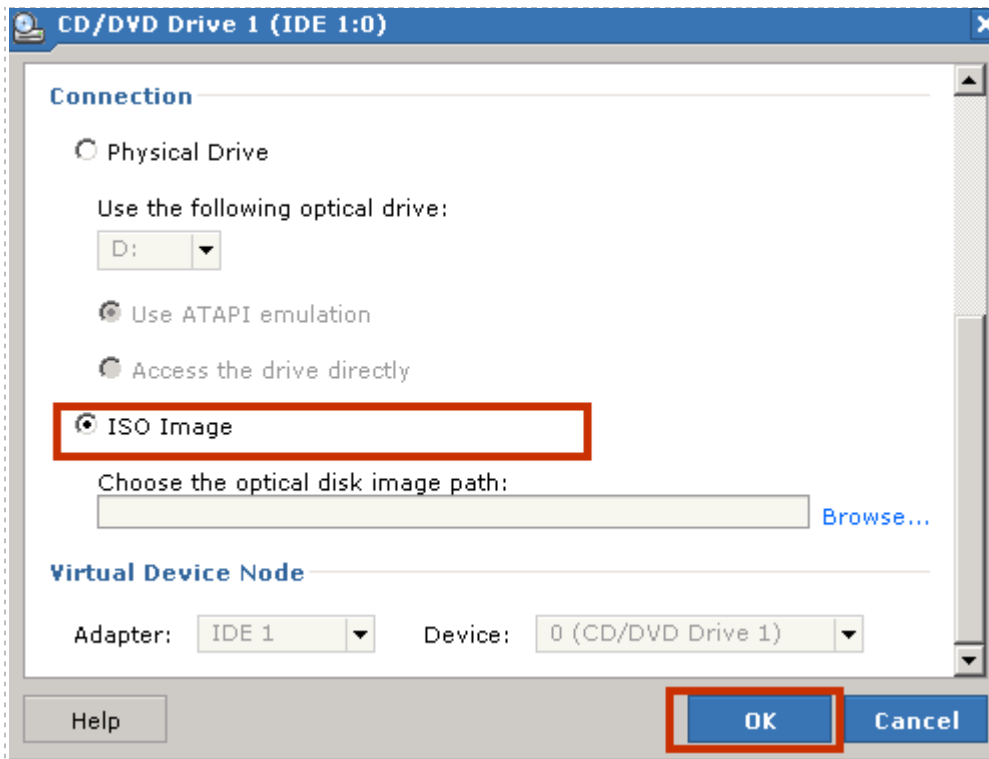
These CD/DVD settings must be edited **after** installing the guest operating system (see section 4.3).



Uncheck the **Connect at power on** box. This is necessary to prevent the virtual machine from attempting to connect to the VMware host's CD/DVD device, which could result in undesired properties or boot errors.



You may point the CD/DVD device connection to a unique ISO image on the local VMware host. If you choose this option, make sure each virtual machine you create does not point to the same ISO file. Otherwise, you may see some undesired properties or boot errors.



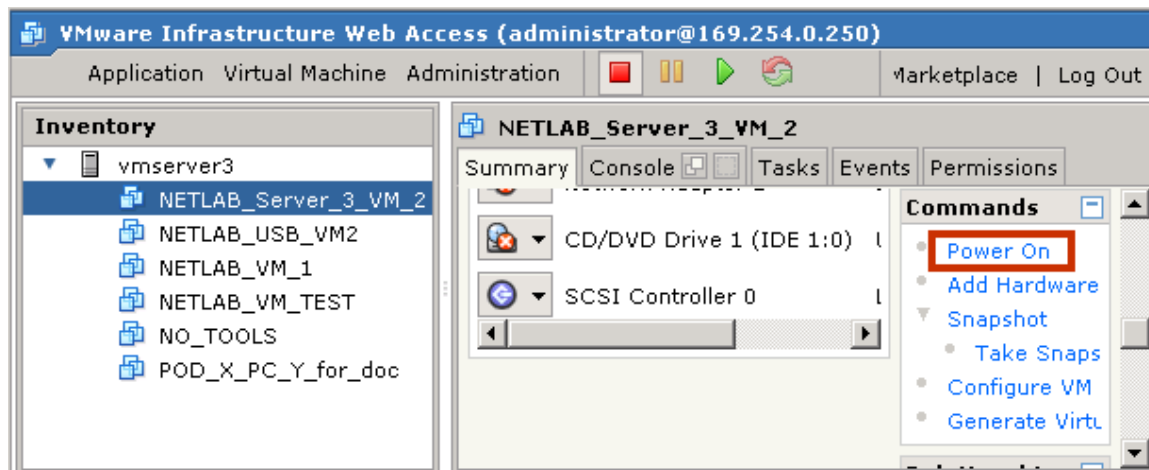
4.5 Installing the VMware Tools

Installation of VMware Tools is required to ensure optimal performance and proper NETLAB+ operation.

VMware Tools must be installed **after** installing the guest operating system (see section 4.3).

Your virtual machine must be powered on to install VMware Tools.

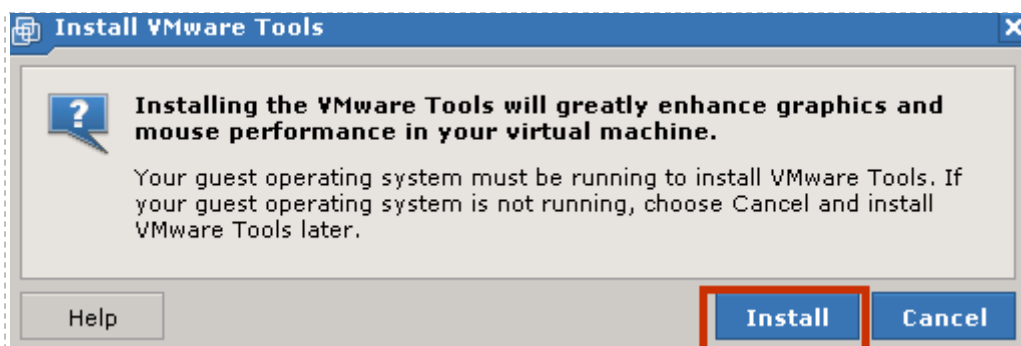
Select **Power On** in the **Commands** section to power on your virtual machine.



Select the **Install VMware Tools** option in the status section.



Assuming you have completed the installation of the guest operating system as described in section 4.3, you may proceed with the install of VMware Tools.



4.6 Setting the Virtual Machine Display Properties for Remote Access

For optimal performance and minimal bandwidth consumption, we recommend using the lowest possible resolution setting. The use of **800 x 600** provides a good fit on a typical laptop screen without the need to scroll the display.

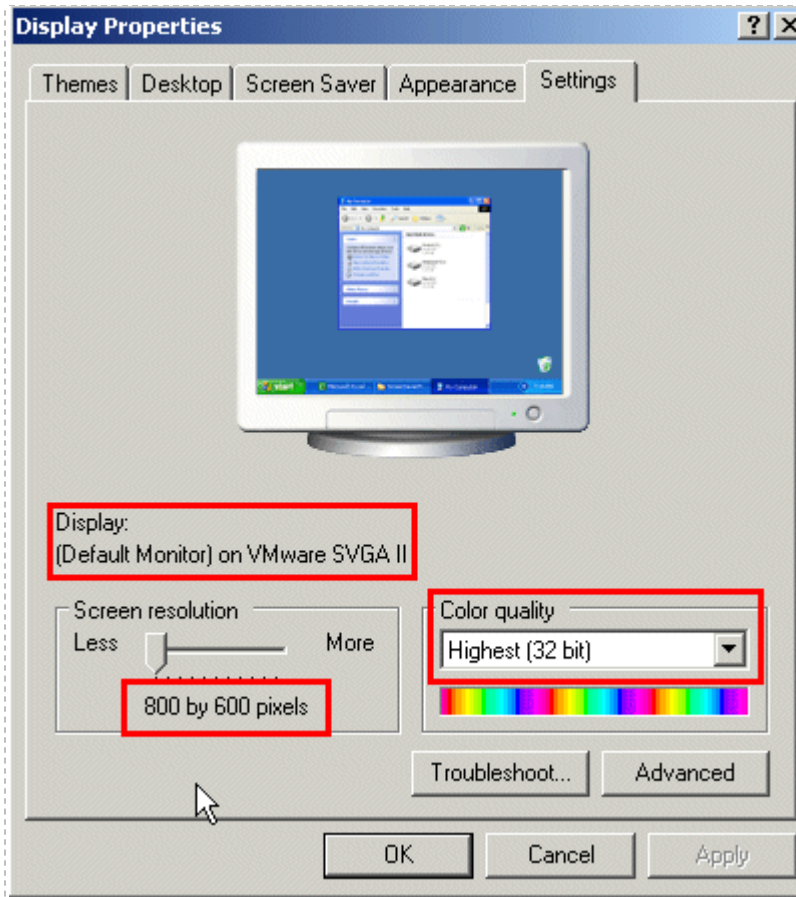
It is possible, however, that your applications may require a higher resolution, such as 1024 x 768.

32-bit color is required. Display update problems have been observed with the 16-bit setting.

The following task assumes a virtual machine running a Windows XP operating system. Adjust accordingly for other operating systems.

To set the screen resolution and color quality:

- Boot the virtual machine.
- **Right click** on the display and select **Properties**.
- Click on the Desktop tab.
- Click on the **Settings** tab.
- Set screen resolution to your desired resolution (800 x 600 is used in this example).
- Set color quality to **32-bit** (required).



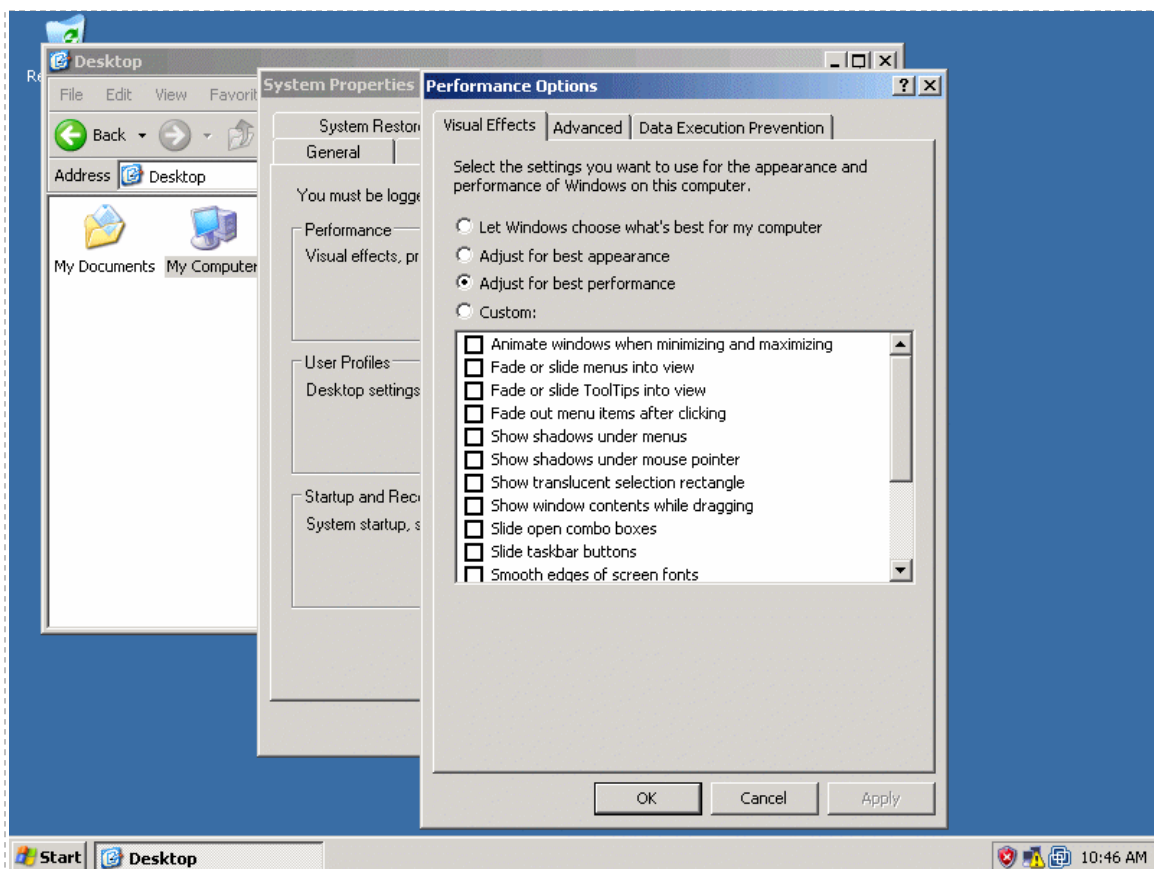
4.7 Adjusting Visual Effects

Visual effects must be adjusted to provide minimal bandwidth utilization and to ensure the responsiveness of the remote experience.

The following task assumes a virtual machine running a Windows XP operating system. Adjust accordingly for other operating systems.

Adjust the visual effects:

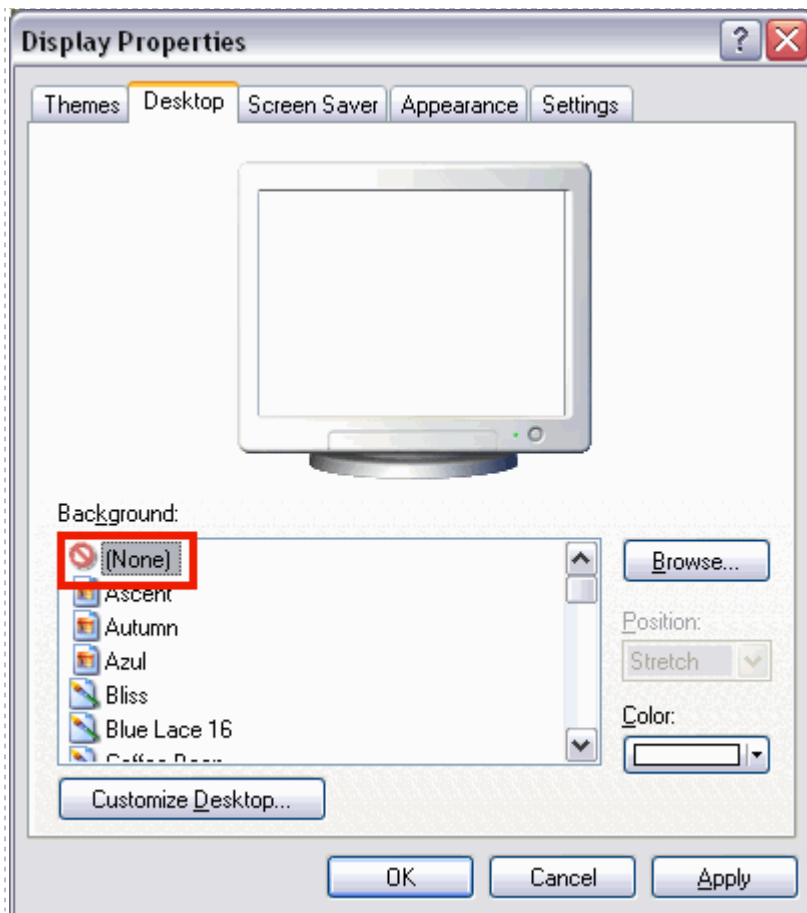
- **Right click** on **My Computer** and select **Properties**.
- Click on the **Advanced** tab.
- Click the **Settings** button for **Performance**.
- Click the **Visual Effects** tab.
- Select the radio button to **Adjust for best performance**.
- Click **Ok** to accept changes.



4.8 Disabling the Desktop Background

The desktop background must be set to **None** to provide minimal bandwidth utilization and to ensure the responsiveness of the remote experience.

- Boot the virtual machine.
- **Right click** on the display and select **Properties**.
- Click on the **Desktop** tab.
- Select **None** for the Background.



4.9 Adding Software Applications

You may now add new software to your virtual machine as required by the lab exercises you plan to use on your pods.

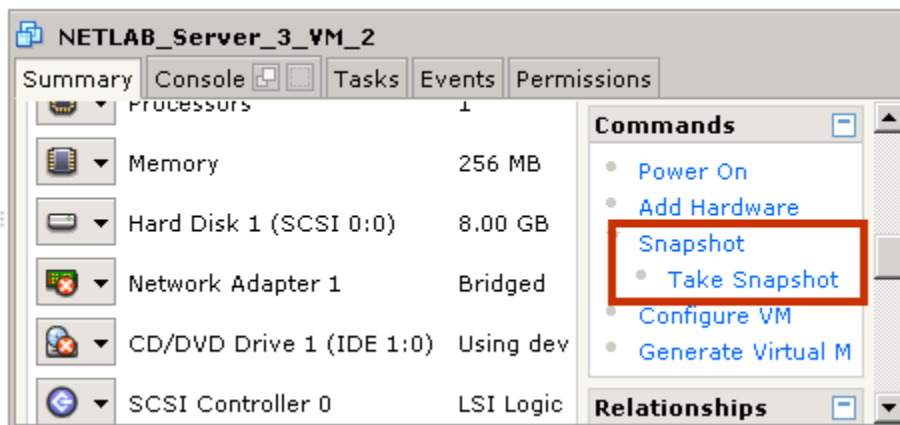
Please refer to the *Installing New Software in a Virtual Machine* section of the [VMware Server User's Guide](#) for details.

4.10 Taking a Snapshot of Your Virtual Machine

Each time you make changes or install new applications on a virtual machine, be sure to take a new *Snapshot*. Any changes made to the virtual machine by lab users will be lost when the virtual machine guest operating system reverts to the snapshot:

- At the end of a lab reservation.
- When a user selects Scrub from the NETLAB+ Action tab.

Take a snapshot by selecting the **Take Snapshot** option in the **Commands** section.







If you do not take a new snapshot after modifying the configuration file, your changes will be lost the next time the snapshot reverts. Your changes will also be lost if the virtual machine is not powered off when the configuration file is edited.

DO NOT take a Snapshot of a Virtual Machine when it is either turned on or suspended. Make sure VM is powered off each time you take a new Snapshot.

4.11 Remote PC Settings (for New Pods)

Remote PCs are part of a lab topology, so they must be configured in NETLAB+ when a new equipment pod is added. All settings (except ID) can be modified later. Remote PCs are only available in pods where the network topology indicates the existence of lab PCs.

Remote PC settings will appear in the New Pod Wizard when you add an equipment pod that supports remote PCs. Each PC has an ID, type, access method, and operating system setting. All settings (except ID) can be modified later. To modify existing PCs, skip ahead to section 4.12.





REMOTE PC SETTINGS				
PC NAME	ID	PC / VIRTUAL MACHINE TYPE	ACCESS	OPERATING SYSTEM
 Host A	18	VMWARE Server 2.0	VNC	Windows XP
 Host B	19	VMWARE Server 2.0	VNC	Windows Server 2003
 Host C	20	VMWARE Server 1.0/GSX	VNC	Linux
 Host D	21	VMWARE Server 2.0	VNC	Windows XP

For **PC/Virtual Machine Type**, use the **VMWARE Server 2.0** setting for VMware virtual machine implementations using VMware Server version 2.x. This is the correct setting if you are following the procedures outlined in this guide.

The **Access** setting, **VNC**, allows direct access to the PC's keyboard, video and mouse using the VNC protocol. This setting cannot be altered when VMware Server 2.0 has been selected as the PC/Virtual Machine Type.

The **Operating System** setting specifies an OS for this PC. The availability of a selection does not guarantee compatibility with all labs.

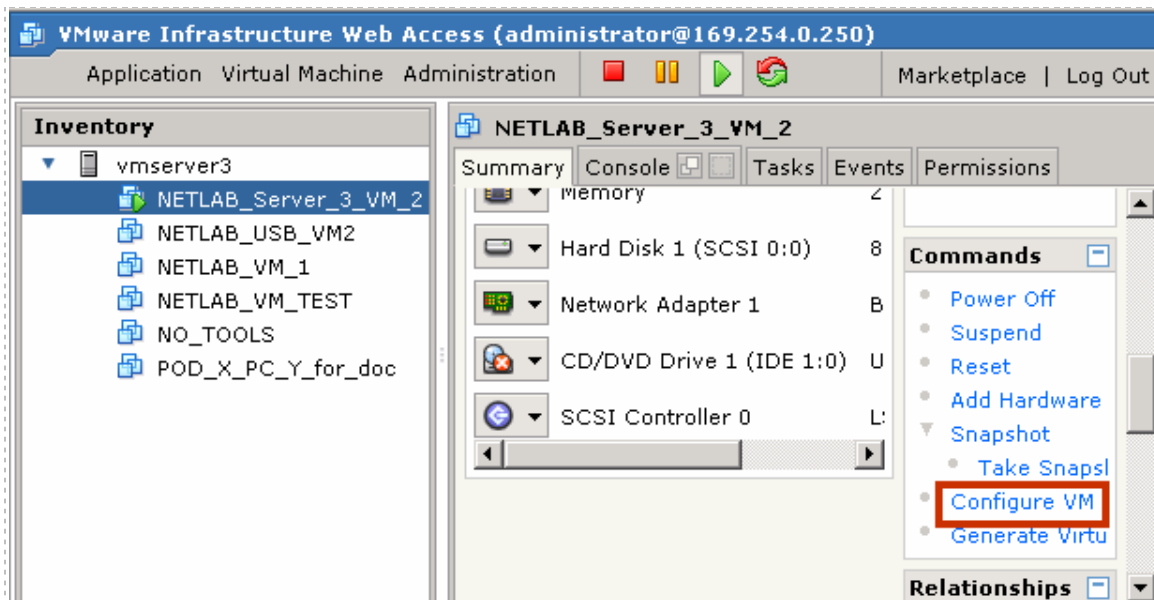
NETLAB+ will prompt for additional settings on the next page.

VMWARE VIRTUAL MACHINE SETTINGS					
PC ID	PC NAME	IP ADDRESS	USERNAME	PASSWORD	CONFIGURATION FILE
18	 Host A	169.254.1.253	NETLAB	myvmhost	[datastore1] XP Pro Template VM/XF
19	 Host B	169.254.1.253	NETLAB	myvmhost	[datastore1] XP Pro Template VM/XF
20	 Host C	169.254.1.253	NETLAB	myvmhost	[datastore1] XP Pro Template VM/XF
21	 Host D	169.254.1.253	NETLAB	myvmhost	[datastore1] XP Pro Template VM/XF

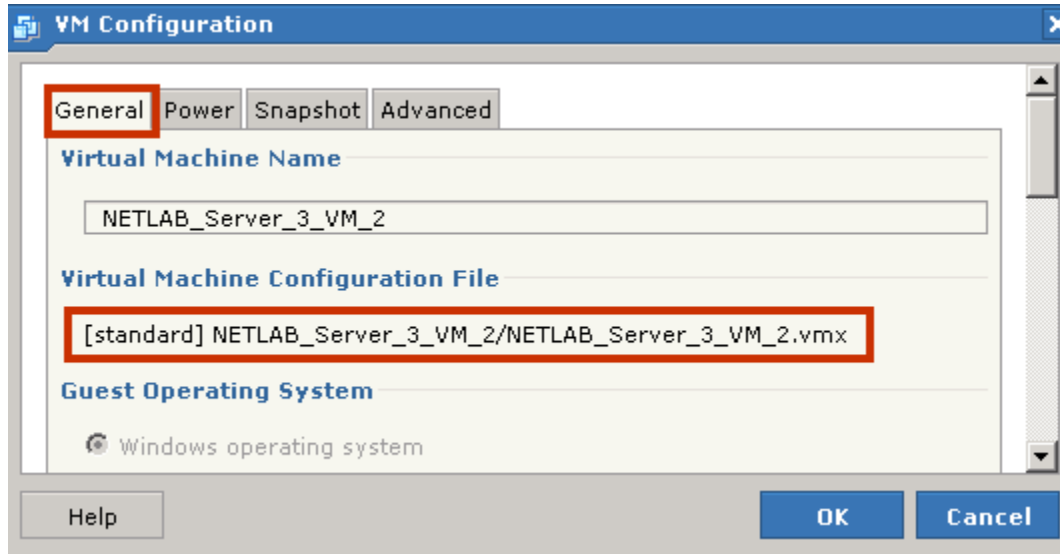
Each virtual machine requires four VMware-specific settings.


- The **IP Address** setting is used to connect to the VMware host system. This is the IP address used for KVM and API traffic flow. If you are implementing ISEC or IMAN, use the inside network address of the VMware server. If you are implementing OMAN, use the outside network address of the VMware server.
- **Username** specifies an operating system account on the VMware host system. NETLAB+ will use this account to login to the VMware host and control virtual machines through the VMware API (see section 3.9).
- **Password** specifies the password associated with the host account (see section 3.9).
- **Configuration File** Enter the relative path of the virtual machine configuration file on the VMware host, including datastore. This file name is typically in the form of [datastore] <pc name>/<operating system>.vmx.

The name of the configuration file of your virtual machine can be found by selecting the **Configure VM** section.



The configuration file name is displayed on the **General** tab.











 You can copy and paste the full pathname of a VM Configuration file from the VM configuration screen into the NETLAB+ VMware virtual machine settings **Configuration File Name** field.

The use of relative path names is specific to VMware Server 2.x. VMware server 1.0 and GSX require absolute path names. If you are upgrading from VMware Server 1.0 and GSX, you must change your configuration file path names to use relative path names, as shown in the example above. Please refer to [Appendix D](#) for details on upgrading to VMware Server 2.x from VMware Server 1.0 and GSX.


4.12 Modifying PC Settings

To modify PC settings, or convert an existing PC to use VMware Server 2.x:

1. Take the pod offline.
2. Select the PC from the Pod Management page.

POD 6 - PCs AND SERVERS (click the GO buttons to reconfigure)								
GO	NAME	PC ID	STATUS	TYPE	ACCESS	CONTROL IP	OPERATING SYSTEM	
	 Host A	18	ONLINE	VMWARE Server 1.0/GSX	VNC	169.254.1.253	Windows XP	
	 Host B	19	ONLINE	VMWARE Server 2.0	VNC	169.254.1.253	Windows Server 2003	
	 Host C	20	ONLINE	VMWARE Server 2.0	VNC	169.254.1.253	Linux	
	 Host D	21	ONLINE	VMWARE Server 2.0	VNC	169.254.1.253	Windows XP	

3. Change Type to **VMWARE Server 2.0** (if it is not the current setting).
4. Specify the VMware settings (described in section 4.11).


POD 5 - PC 17	
PC ID	17
PC Name	 Standalone PC
Type	VMWARE Server 2.0 ▼
VMware Host IP Address	10.0.0.27
VMware Host Username	NETLAB
VMware Host Password	NETLAB
VMware Guest Configuration File	[standard] NETLAB_VM_1\NETLAB_VM_1.vmx
VMware Guest Operating System	Windows XP ▼
VMware Guest VNC Settings	RemoteDisplay.vnc.enabled = "true" RemoteDisplay.vnc.password = "NETLAB" RemoteDisplay.vnc.port = "5917"
Access Method	VNC ▼
Admin Status	ONLINE ▼
Options	<input checked="" type="checkbox"/> revert to snapshot during scrub operation

If you want NETLAB+ to return the PC to a clean state after a lab reservation, make sure "revert to snapshot" is checked. Recall from section 4.2 that the virtual machine snapshot power-off option must also be set to **Just Power Off**.

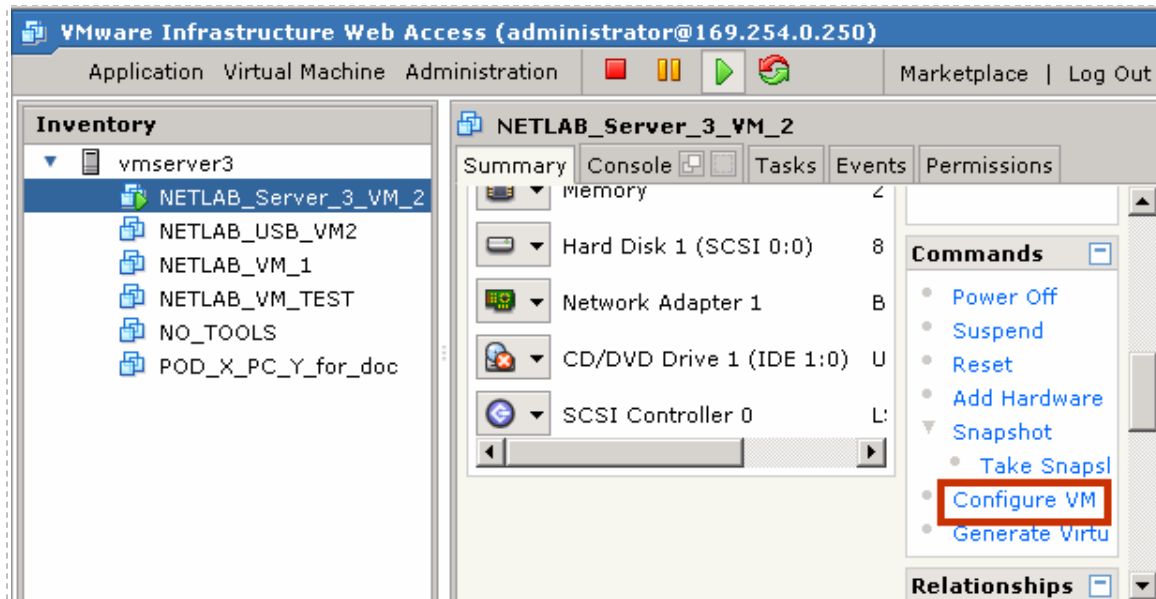
4.13 Configuring Remote Display Options

To allow NETLAB+ users to access the keyboard, video, and mouse of a virtual machine, you must add three **RemoteDisplay** statements to the virtual machine's configuration file.

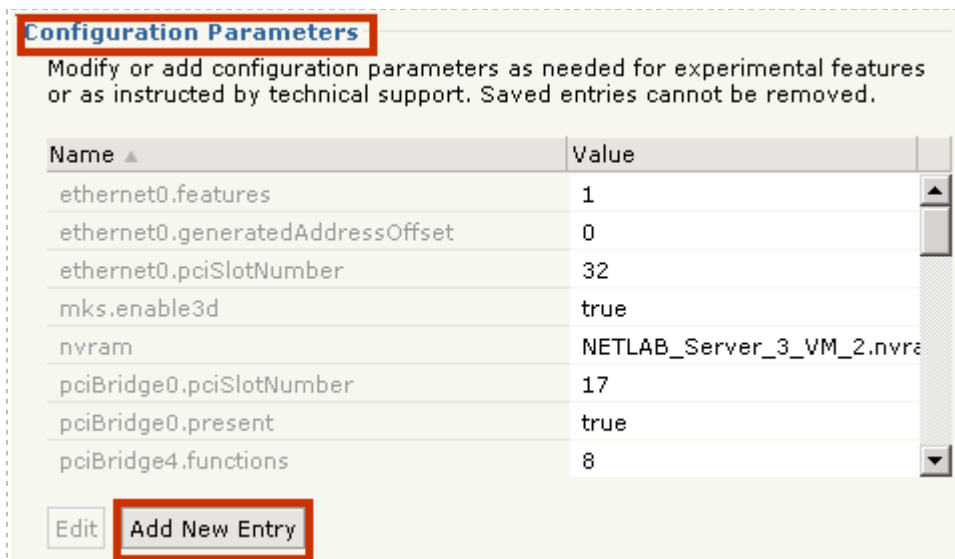
1. Access the detailed remote PC settings from the NETLAB+ Pod Management page (as described in section 4.11).
2. Obtain the **VMware Guest VNC Settings** (automatically computed by NETLAB+). The settings for this example are highlighted in the picture below (your settings will vary).

POD 6 - PC 18	
PC ID	18
PC Name	 Host A
Type	VMWARE Server 2.0 <input type="button" value="v"/>
VMware Host IP Address	169.254.1.253
VMware Host Username	NETLAB
VMware Host Password	myvmhost
VMware Guest Configuration File	C:\Virtual Machines\POD_1PC_3\winXpro
VMware Guest Operating System	Windows XP <input type="button" value="v"/>
VMware Guest VNC Settings	RemoteDisplay.vnc.enabled = "true" RemoteDisplay.vnc.password = "NETLAB" RemoteDisplay.vnc.port = "5918"
Access Method	VNC <input type="button" value="v"/>
Admin Status	ONLINE <input type="button" value="v"/>
Options	<input checked="" type="checkbox"/> revert to snapshot during scrub operation

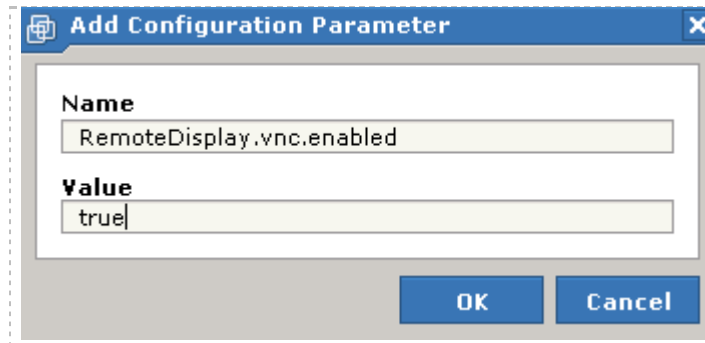
3. From the VMware management console, make sure the PC is powered **OFF or suspended**.
4. Working from the **VI Web Access** page, select your virtual machine in the Inventory list and the click on **Configure VM** in the **Commands** section.



5. Select the **Advanced** tab and scroll down to the **Add New Entry** function located in the **Configuration Parameters** section.



6. Add each of the three VMware guest VNC settings as configuration parameters.

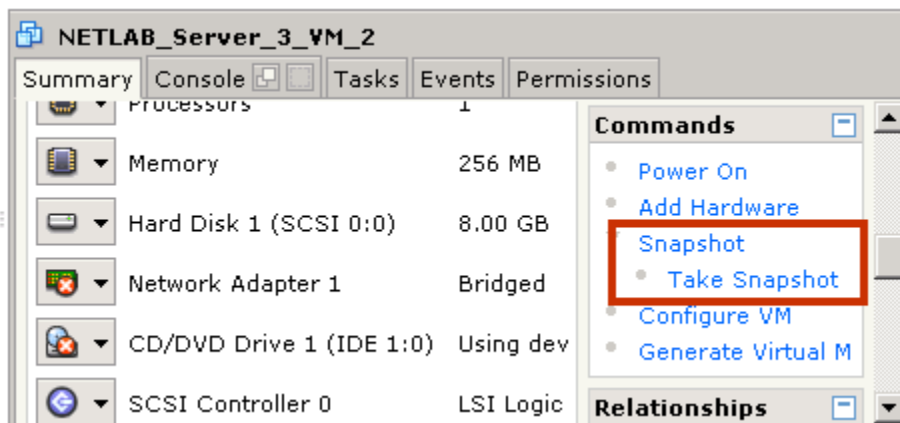


If you make an error while keying in a configuration parameter, you may need to remove the virtual machine from the inventory (without deleting it from the disk), edit the VMX file and re-add, or restart the VMware Server services, by following the procedure described in [Appendix F](#).

4.14 Taking a New Snapshot of the Virtual Machine

After completing the task of adding the configuration statements to the configuration file you must take a new snapshot of your virtual machine.

Select the **Take Snapshot** option in the **Commands** section.

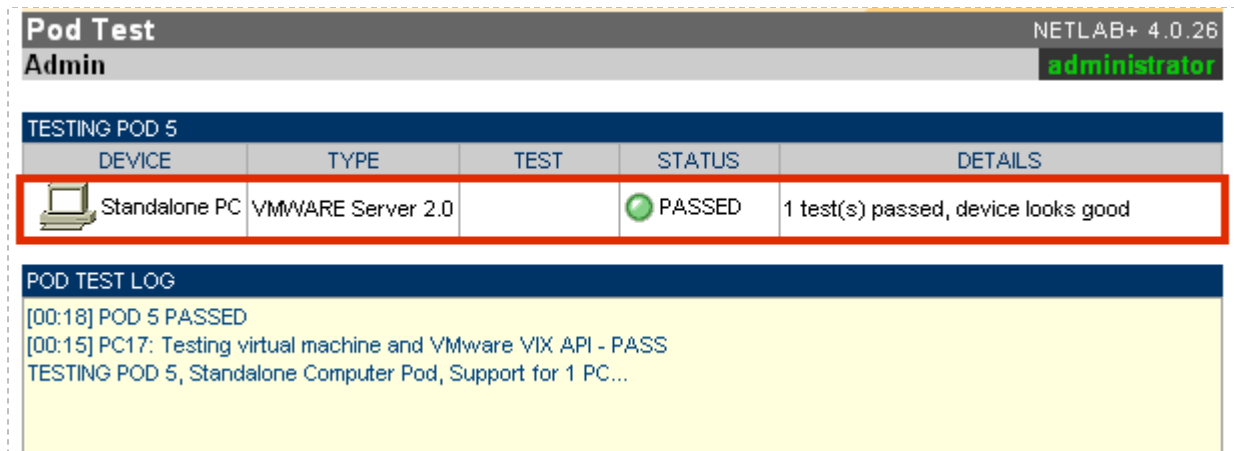


If you do not take a new snapshot after modifying the configuration file, your changes will be lost the next time the snapshot reverts. Your changes will also be lost if the virtual machine is not powered off when the configuration file is edited.



4.15 Verify the Virtual Machine

After your virtual machine is configured, perform the following tasks to verify the API is functioning.

The Pod Test only verifies the remote display parameters and the function of the VMware API. The Pod Test does not test network connectivity to networking gear such as routers, switches and firewalls. The process required to bridge your virtual machines to real networks and real lab equipment (such as routers, switches, and firewalls) is described in detail in [Part 5](#).



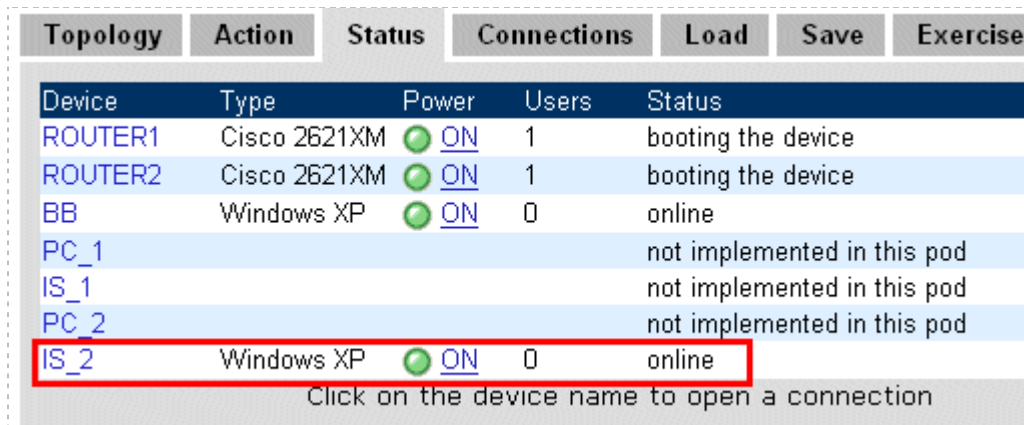
Pod Test NETLAB+ 4.0.26
 Admin administrator





TESTING POD 5				
DEVICE	TYPE	TEST	STATUS	DETAILS
 Standalone PC	VMWARE Server 2.0		 PASSED	1 test(s) passed, device looks good

POD TEST LOG

```
[00:18] POD 5 PASSED
[00:15] PC17: Testing virtual machine and VMware VIX API - PASS
TESTING POD 5, Standalone Computer Pod, Support for 1 PC...
```

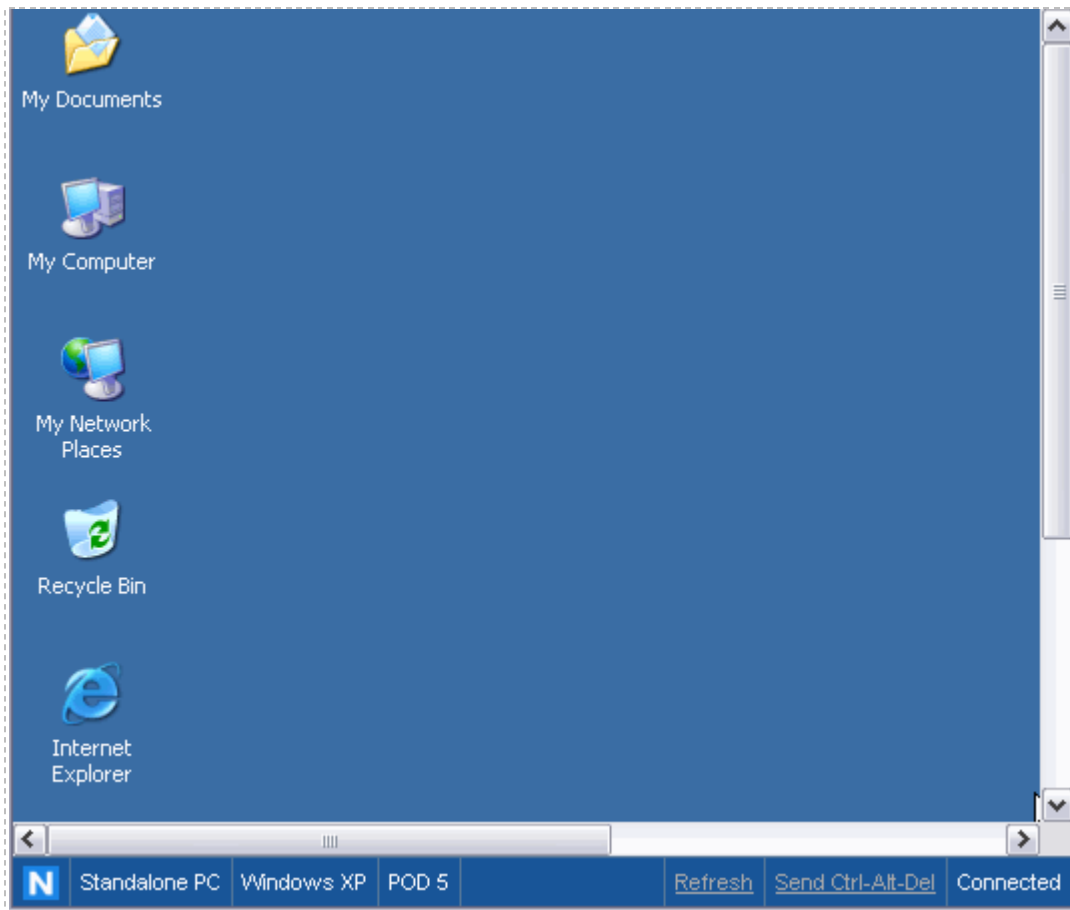
1. Run a pod test. NETLAB+ will check your settings and verify that the API is working.
2. Bring the pod back online.
3. Login to an instructor account and create a lab reservation to test your virtual machine(s).
4. On the **Status** tab, your virtual machines should be online.



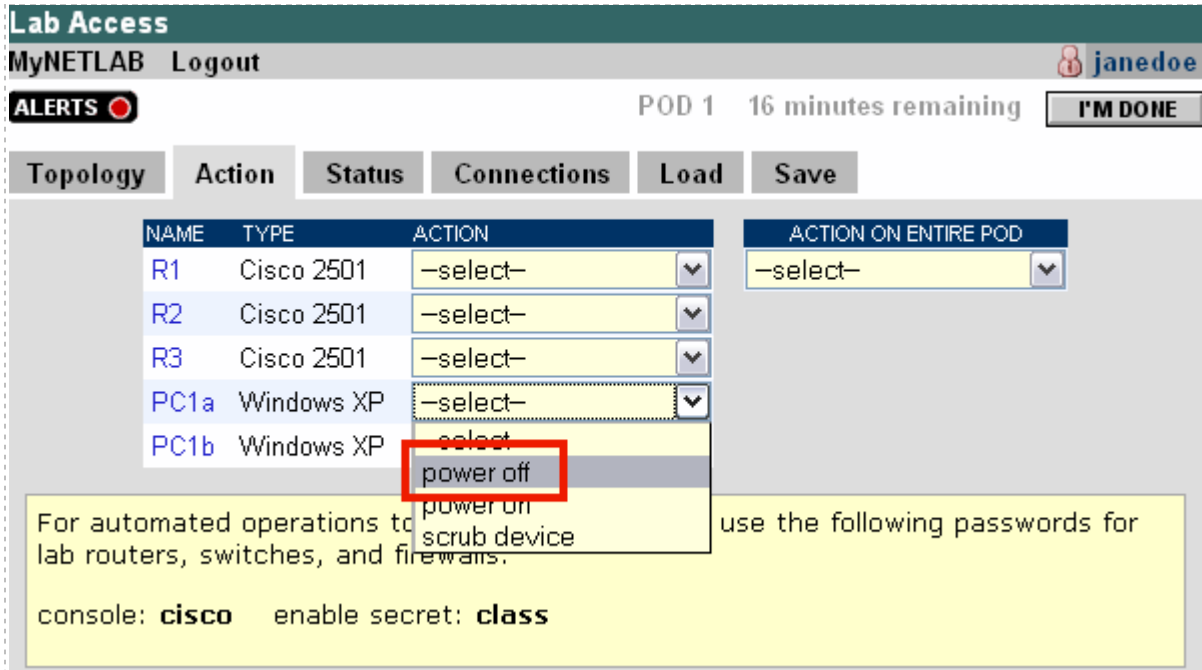
Topology	Action	Status	Connections	Load	Save	Exercise
Device	Type	Power	Users	Status		
ROUTER1	Cisco 2621XM	 ON	1	booting the device		
ROUTER2	Cisco 2621XM	 ON	1	booting the device		
BB	Windows XP	 ON	0	online		
PC_1				not implemented in this pod		
IS_1				not implemented in this pod		
PC_2				not implemented in this pod		
IS_2	Windows XP	 ON	0	online		

Click on the device name to open a connection

5. Open a connection to the PC by clicking on the device in the topology, the status tab, or connections tab. This will bring up the NETLAB+ Java viewer (assuming you have Java installed).



- Test the VMware API. **Power off** the machine from the **Action** tab.



Lab Access
MyNETLAB Logout janedoe

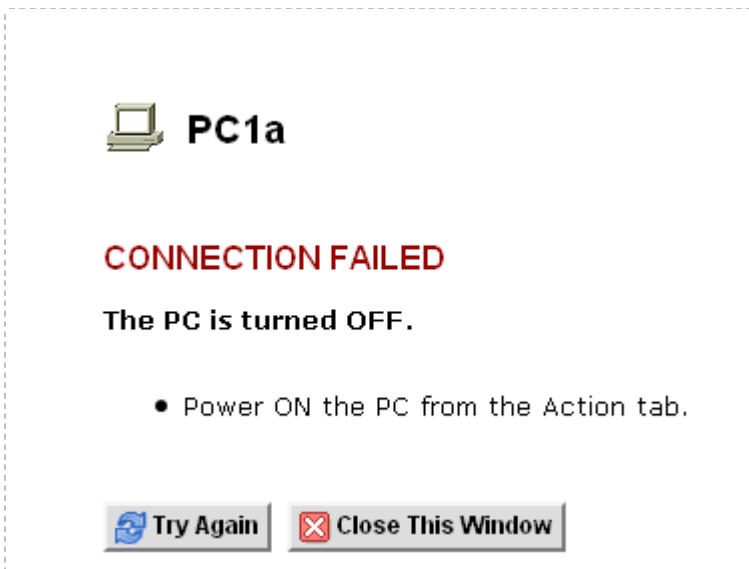
ALERTS POD 1 16 minutes remaining I'M DONE


Topology Action Status Connections Load Save

NAME	TYPE	ACTION	ACTION ON ENTIRE POD
R1	Cisco 2501	-select-	-select-
R2	Cisco 2501	-select-	-select-
R3	Cisco 2501	-select-	-select-
PC1a	Windows XP	-select-	-select-
PC1b	Windows XP	-select-	-select-

For automated operations to use the following passwords for lab routers, switches, and firewalls:
console: **cisco** enable secret: **class**

If you had a connection open, it should drop. If you reconnect, NETLAB+ should know the PC is powered off (by obtaining the status of the virtual machine via the VMware API).

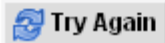



 **PC1a**

CONNECTION FAILED

The PC is turned OFF.

- Power ON the PC from the Action tab.

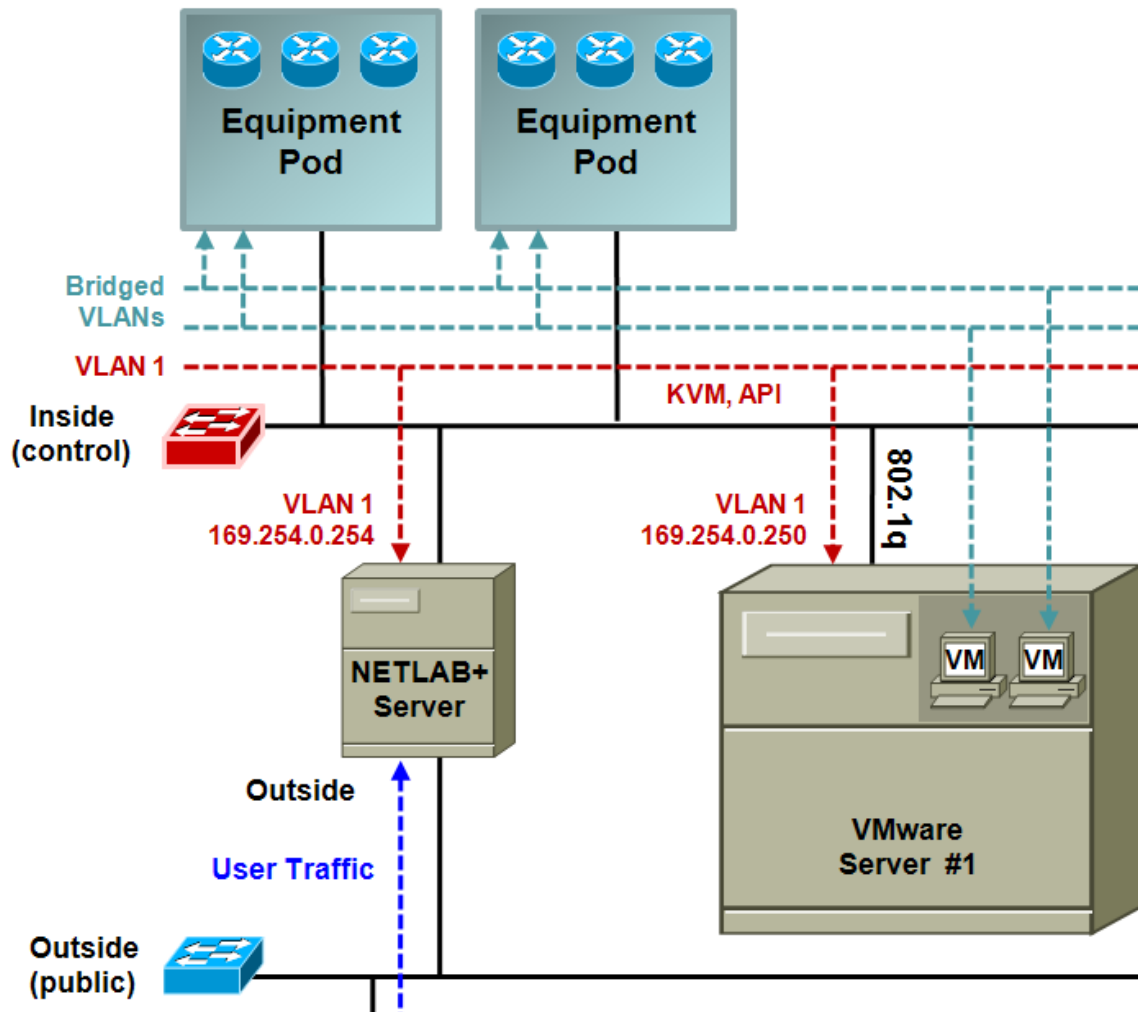
- From the **Action tab**, power the virtual machine back **ON**. Wait a minute for the machine to startup. You should now be able to reconnect.

8. Test the scrub device/ snapshot feature. Make some changes to the PC (i.e. move some icons around and create some files). Select **Scrub Device** on the Action tab. The PC will reboot and your connection will drop (this is normal). Wait a minute for the machine to restart. You should now be able to reconnect, and your previous changes should be gone.

Part 5 Connecting Virtual Machines to Real Lab Devices

This section focuses on the establishing communication between virtual machines and lab devices in the topology. You can skip this section if your virtual machines do not need to communicate with lab equipment and/or external networks on separate VLANs.

Virtual LANs (VLANs) are used to bridge your virtual machines to real lab equipment (such as routers, switches, and firewalls). These VLANs are implemented on control switches and managed by the NETLAB+ software.



The following objectives will make more sense after you have added a new equipment pod.

Objectives

- Determine which VLAN numbers are used by your pod.
- Create the proper VLAN adapter using an Intel networking adapter.
- Uncheck the unused Protocols from Network Properties.
- Bind each VLAN adapter to an available VMware virtual switch (VMnet).
- Configure a Virtual Switch to use correct VMnet (using VI Web Access).
- Take a final snapshot to save changes made to the VM configuration.

5.1 Determining Which VLAN Numbers Are Used by Your Pod

The VLAN adapters you must create for your virtual machines will vary based on which pods you have added to your NETLAB+ server.

A *VLAN Pool* is the consecutive range of VLANs used by NETLAB+. Each pod has a unique *VLAN pool* and the actual VLAN numbers will be unique for each pod. **You must determine which VLAN numbers used by NETLAB+ must be trunked to the VMware host.**

There are resources available to assist you in determining which VLAN numbers are used:

- If you are implementing a standard NETLAB+ Academy Edition[®] pod, you may refer to the *Configuring VMware and Virtual Machines* section of the appropriate [pod-specific guide](#) to obtain this information, including the VLAN Offset Reference Table specific to your pod. The examples in the subsections below provide more detail regarding this process.
- If you are implementing a custom pod design, consult with the individual who created the pod design and refer to the *Pod Design Theory* section of the [NETLAB+ Pod Design Guide](#) for additional information.

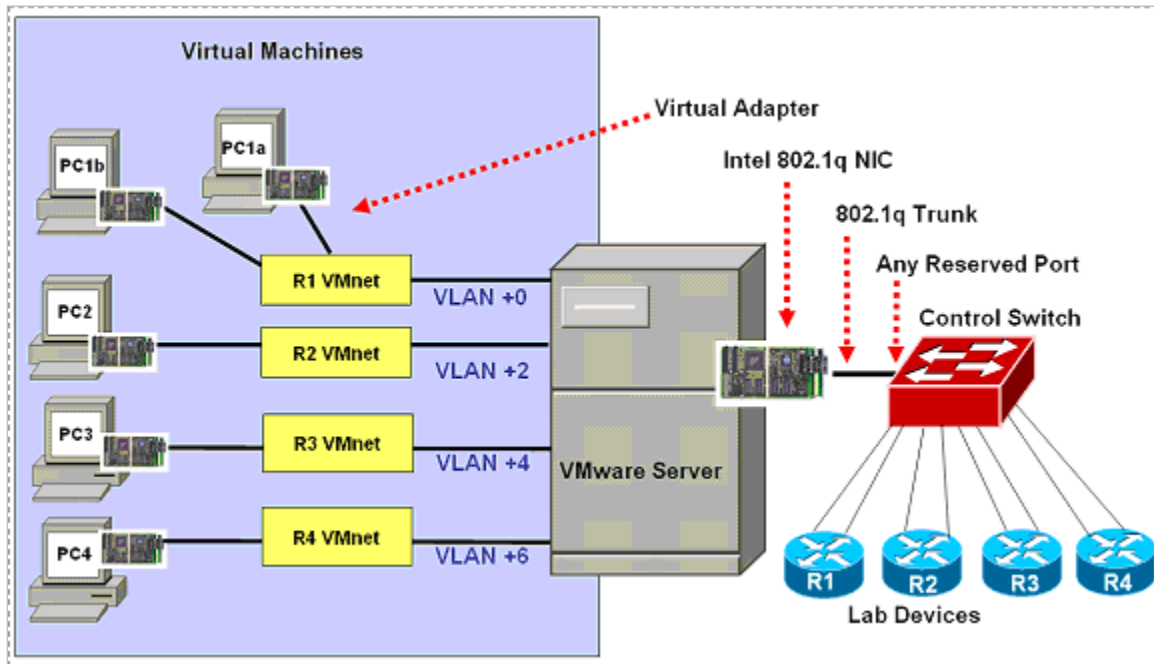
VMware Server virtual network adapters and virtual LAN switches (VMnets) are used to connect virtual machines to the pod. Depending on the pod design, some virtual machines may share the same VLAN. Without the proper VLAN adapter mapped to an available VMnet, the connections between pod devices and/or virtual machines will not function properly.

5.1.1 Determining VLANs Example 1 – Cuatro Router Pod

In this example, we see that a Cuatro Router Pod uses **4 VMnets** in the required configuration. Since VMware Server supports 10 virtual switches, it is possible to host up to 2 complete Cuatro Router 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.

PC1a and PC1b 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.

Step 1. Determine the Base VLAN for the pod.

The base VLAN and VLAN pool numbers are displayed on the Pod Management page in the Control Switch table. Please see the *Verifying Your Settings* section of the [NETLAB+ Administrator Guide](#) for details on accessing the Pod Management page to find the base VLAN number for your pod.

An example of the VLAN pool information available on the Pod Management page. In this example, pod 7 uses VLANs 160-167. The base VLAN is 160. Your VLAN numbers will vary.

POD 7 - CONTROL SWITCH			
SWITCH ID	POD PORT RANGE	BASE VLAN	VLAN POOL
 2	1-8	160	160-167

Step 2. Determine the actual VLAN number for each virtual network.

Add the base VLAN to the offsets in the table below. In this example, the **VLAN Offset Reference Table** from the [NETLAB_{AE} Cuatro Router Pod Guide](#) is used. Consult the appropriate [pod-specific guide](#) to obtain the information for your pod.

The base VLAN value used below (160) is an example, the base VLAN of your pod will vary.

VLAN Offset Reference Table – Cuatro Router Pod

Virtual Machines	Virtual Switch (VMnet)	Offset (add to base VLAN)	Actual VLAN	Example
PC1a PC1b	R1 VMnet	+ 0	= _____	160 + 0 = 160
PC2	R2 VMnet	+ 2	= _____	160 + 2 = 162
PC3	R3 VMnet	+ 4	= _____	160 + 4 = 164
PC4	R4 VMnet	+6	= _____	160 + 6 = 166

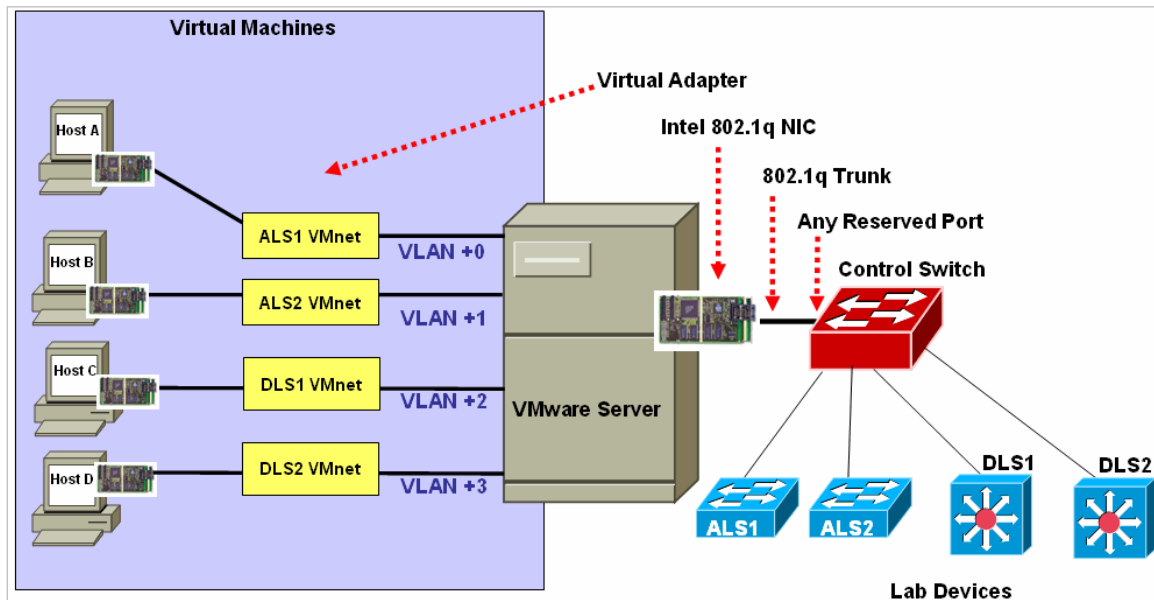
In this example, we have determined that we must create VLAN adapters for VLANs 160, 162, 164, and 166.

5.1.2 Determining VLANs Example 2 – Cuatro Switch Pod

In this example, we observe that the Cuatro Switch Pod uses **4 VMnets** in the required configuration. Since VMware Server supports 10 virtual switches, it is possible to host up to 2 complete Cuatro Switch 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.

PC1a and PC1b 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.

Step 1. Determine the Base VLAN for the pod.

The base VLAN and VLAN pool numbers are displayed on the Pod Management page in the Control Switch table. Please see the *Verifying Your Settings* section of the [NETLAB+ Administrator Guide](#) for details on accessing the Pod Management page.

An example of the VLAN pool information available on the Pod Management page, your VLAN numbers will vary.

POD 10 - CONTROL SWITCH			
SWITCH ID	POD PORT RANGE	BASE VLAN	VLAN POOL
 2	9-12	190	190-193

In this example, Pod 10 uses VLANs 190-193. The base VLAN is 190.

Step 2. Determine the actual VLAN number for each virtual network.

Add the base VLAN to the offsets in the table below. In this example, the **VLAN Offset Reference Table** from the [NETLAB_{AF} Cuatro Switch Pod Guide](#) is used. (Consult the appropriate [pod-specific guide](#) to obtain the information for your pod)

The base VLAN value used below (190) is an example, the base VLAN of your pod will vary.

VLAN Offset Reference Table – Cuatro Switch Pod

Virtual Machines	Virtual Switch (VMnet)	Offset (add to base VLAN)	Actual VLAN	Example
Host A	ALS1 VMnet	+ 0	= _____	190 + 0 = 190
Host B	ALS 2 VMnet	+ 1	= _____	190 + 1 = 191
Host C	DLS 1 VMnet	+ 2	= _____	190 + 2 = 192
Host D	DLS 2 VMnet	+ 3	= _____	190 + 3 = 193

In this example, we have determined that we must create VLAN adapters for VLANs 190, 191, 192, and 193.

5.2 Creating VLAN Adapters

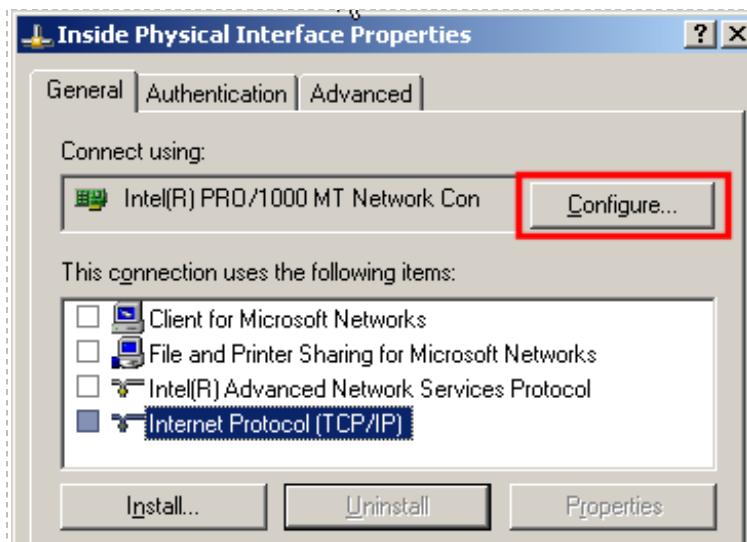
Based on the VLAN numbers you identified in the previous section, follow the steps described in the subsections below to create each of the VLAN adapters required.

5.2.1 Create a Proper VLAN Adapter using an Intel Adapter

Navigate to the Network Connections panel:

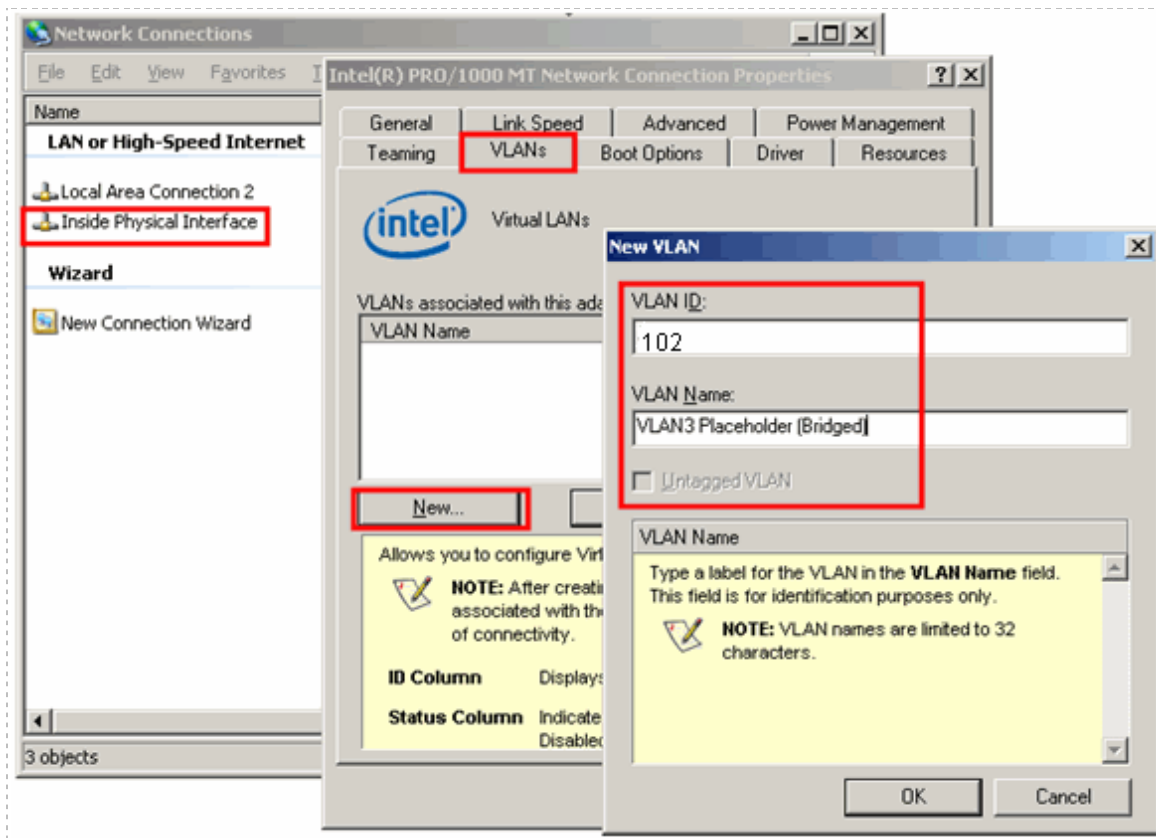
- **Start** → **Control Panel** → *right click* on **Network Connections** → **Open**

You will create a VLAN sub-interface on the **Inside Physical Interface** (container interface). Open the Network Properties window for the **Inside Physical Interface**. Next, click the **Configure** button.



To create a VLAN:

- Click the **VLANs** tab.
- Click the **New** button.
- Enter the appropriate **VLAN ID** as per section 5.1.
- Enter a descriptive name(i.e. pod number and remote pc number) for the **VLAN Name** field.
- Click **OK**.

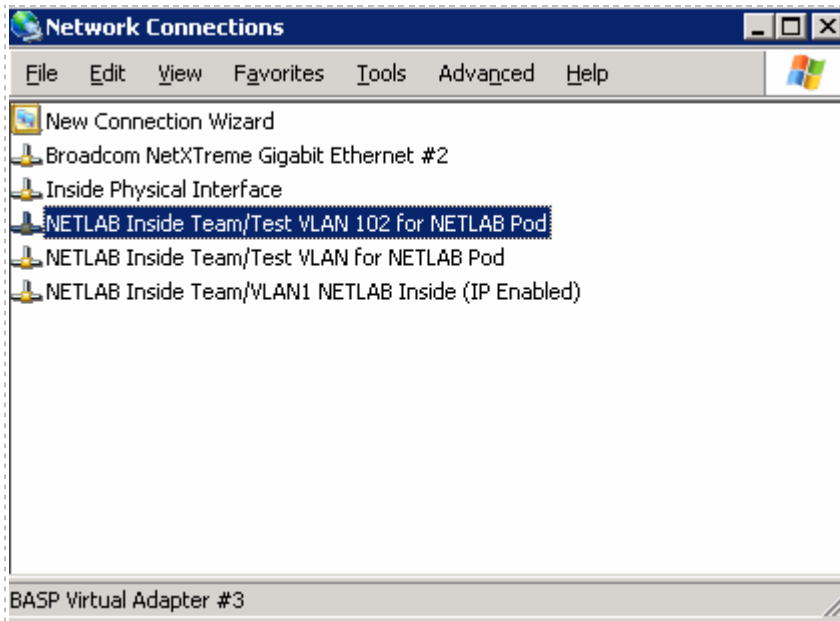


5.2.2 Uncheck the Unused Protocols from Network Properties

After you add your pod VLANs, make sure **VMware Bridge Protocol** is the only selected protocol.

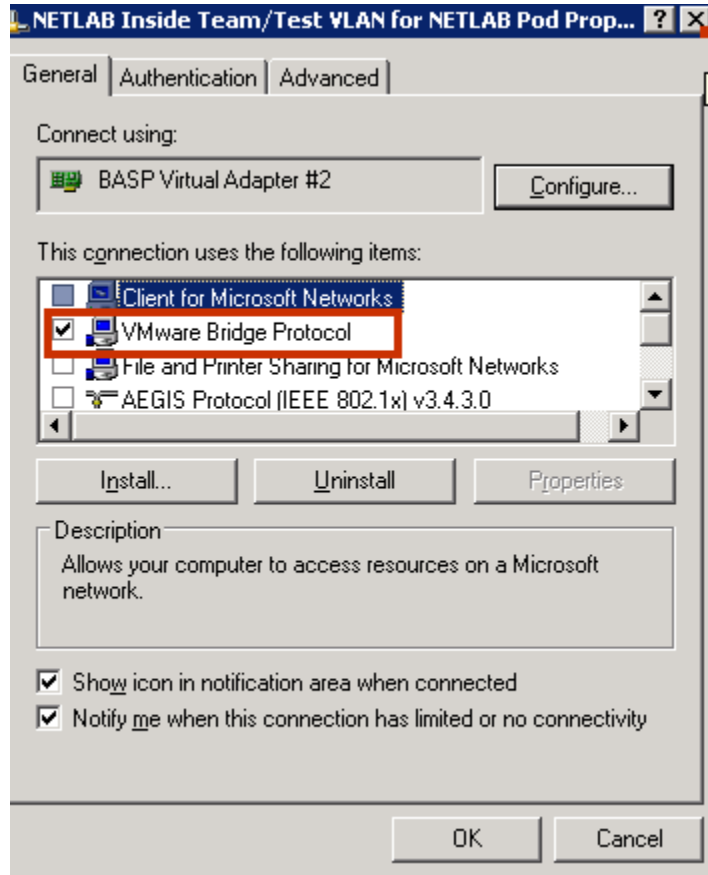
Start → **Control Panel** → *right click* on **Network Connections** → **Open**

Select the detail view. **View** (menu item) → **Details**



Right Click your VLAN name → **Properties**.

VMware Bridge Protocol must be **checked**. All others that you are able to uncheck should be **unchecked**. There may be checked items that are required by the driver that you do not have the option of un-checking (this is ok).



Traffic should be **bridged**, not routed, between equipment pods and VMware virtual machines. Therefore, it is important to **unbind TCP/IP** and Microsoft client protocols from each of the 802.1q sub-interfaces on the VMware host adapter that are associated with lab VLANs.

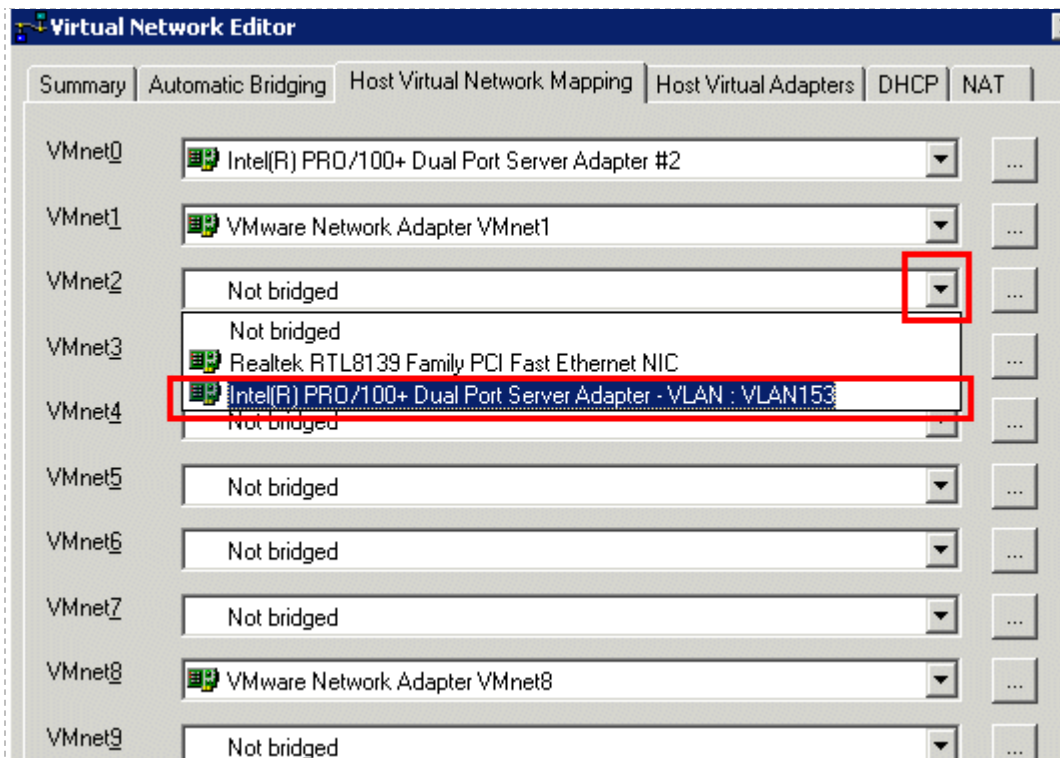
5.3 Mapping VLAN interfaces to available Virtual Networks (VMnets)

The VMware Virtual Network Editor is used to bridge virtual networks in VMware to real networks in NETLAB+ (review section 5.2). On a Windows VMware Server host, you may create up to 10 virtual networks (VMnet) that can connect one or more virtual machines to a VLAN in NETLAB+. By default VMnet0, VMnet1, and VMnet8 provide special functions. See [Appendix A](#) for a description of how to reclaim them for external connectivity to NETLAB+.

To allocate a virtual switch and connect to a VLAN in NETLAB+:

- Access the **Virtual Network Editor** (see 3.11) and select the **Host Virtual Network Mapping** tab.
- Assign an available **VMnet** to a VLAN interface. Each VLAN created, as per section 5.2, should be available in the drop down lists.

This image uses VLAN 153 as an example; your selections will vary.

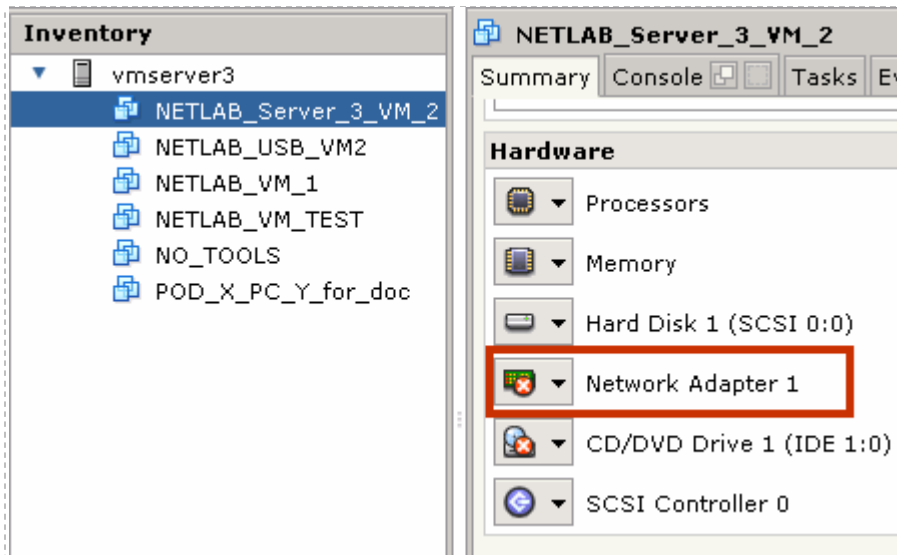


If the VLAN interfaces do not appear from the drop down list, the system will require a reboot to initialize the newly created adapters. Any VLAN interfaces created during the process described in section 5.2 only show up in the VMware Virtual Network Editor after the server (or VMware host) has been rebooted.

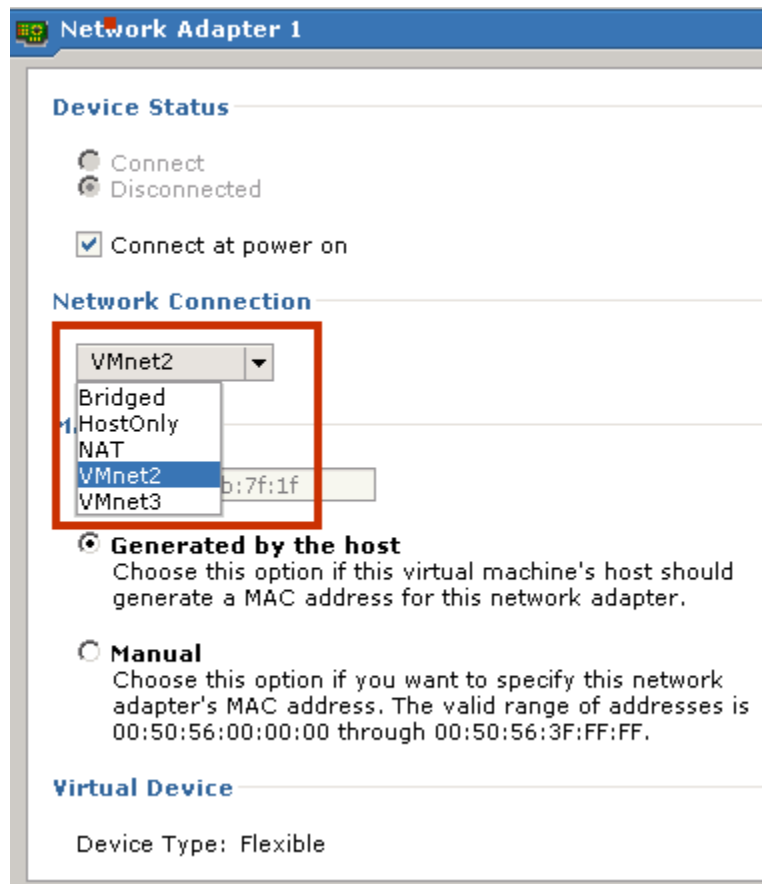
5.4 Configure a VM to use the correct VMnet (using VI Web Access)

Once you have added the proper VLANs and mapped them to an available VMnet, you are ready to configure each virtual machine to use the appropriate VMnet.

1. From the **VI Web Access** page, select the virtual machine from the inventory list and locate **Network Adapter 1** in the **Hardware** Section of the **Summary** tab.



2. Click on **Network Adapter 1** and select **Edit**.
3. Review the available VMnet selections in the **Network Connections** section. Your VMnets mapped as per section 5.3, should appear as pulldown selections.



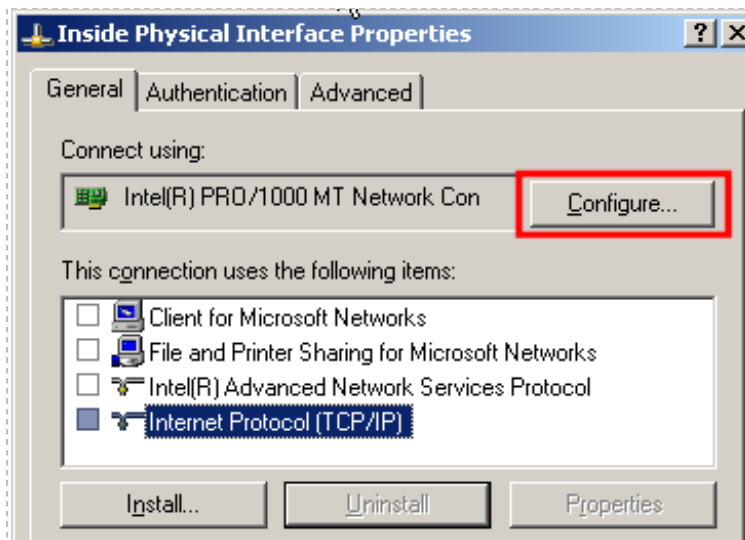
VMnet selections will not appear until you have mapped a VLAN interface to a VMnet (using Virtual Network Editor). **If you have mapped your VLANs using the Virtual Network Editor and the VMnets do not appear from the drop down list, the system will require a reboot to update the VMware Server services.**

4. Select the proper VMnet for this VM. If you do not select the correct VMnet, your virtual machine will not use the proper VLAN adapter and cannot communicate with lab gear during a lab reservation. The proper VMnet to choose for the virtual machine is the VMnet that was mapped to the VLAN of the virtual machine (see section 5.3).
5. Take a final snapshot of your virtual machine (see section 4.14).

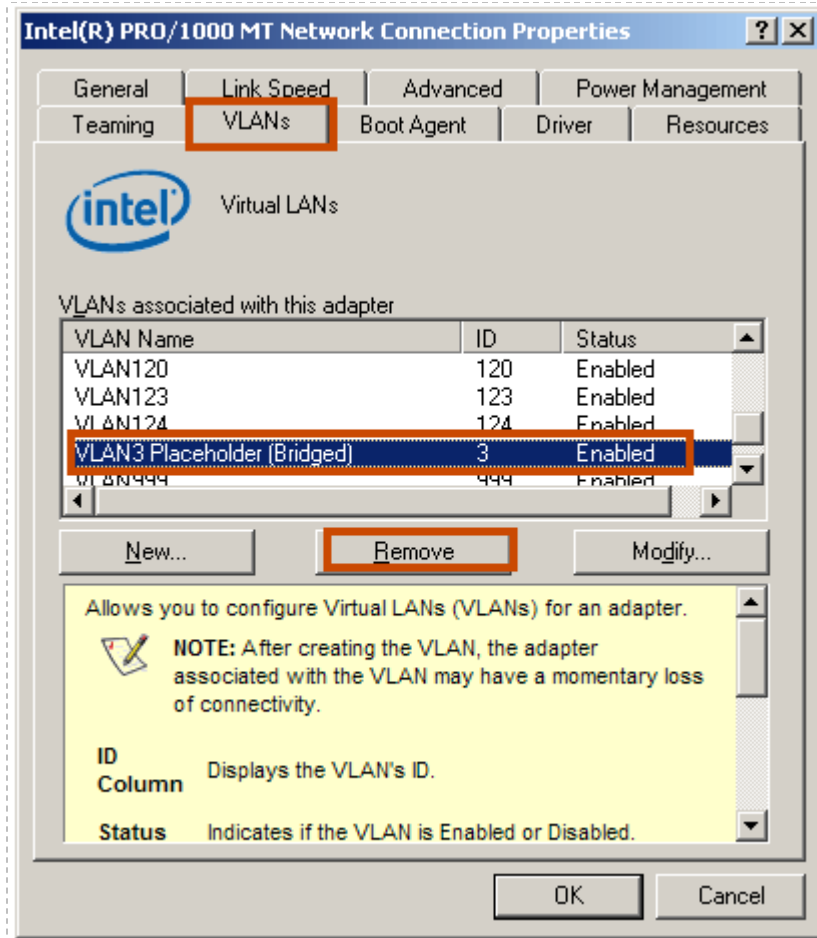
5.5 Deleting the Placeholder VLAN 3

Recall from section 3.4.5 that VLAN 3 was created as a temporary placeholder. This was necessary in order to create untagged VLAN 1, since 2 VLANs must exist before VLAN 1 can become untagged. VLAN 3 may now be deleted.

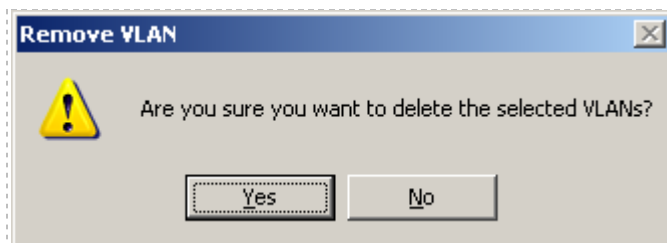
Return to the Network Properties window for the **Inside Physical Interface** (see section 3.4.5). Next, click the **Configure** button.



- Click the **VLANs** tab.
- Select **VLAN3 Placeholder (Bridged)**
- Click **Remove** to delete the VLAN.



Select **Yes** to confirm the delete of VLAN 3.



Part 6 Verifying Connectivity and Troubleshooting

This section provides guidance on common troubleshooting issues associated with the implementation of VMware Server with NETLAB+ and guidance on verifying connectivity after installation. Please review the material in this section prior to contacting NDG for customer support (see [Appendix C](#)).

Objectives

- Verifying connectivity between virtual machines and lab gear.
- Reviewing and/or modifying virtual machine settings for existing virtual machines.
- Identify and resolve the most frequently encountered VMware issues.

6.1 Verifying Connectivity Between Virtual Machines and Lab Gear

We strongly encourage verifying the connectivity between your virtual machines and lab gear after completing the processes outlined in [Part 5](#), using the method described in this section.

The troubleshooting methods shown here can also aid you in determining why a remote PC in a NETLAB+ pod is having network connectivity problems.

Verify that your pod is online (see the *Equipment Pods* section of the [NETLAB+ Administrator Guide](#)) and that the pod passes the pod test (see section [4.15](#)).

The example below illustrates a NETLAB_{AE} BRPv2 topology installed as Pod #5 on Control Switch #4:

BRPv2 Lab Device	Device Port	Control Switch #4 Port	NETLAB+ Pod VLAN
Router 1	fa 0/0	fa 0/1	140
	fa 0/1	fa 0/2	141
PC1a	virtual NIC	fa 0/23	140
PC1b	virtual NIC	fa 0/23	140
Router 2	fa 0/0	fa 0/3	142
	fa 0/1	fa 0/4	143
PC2	virtual NIC	fa 0/23	142
Router 3	fa 0/0	fa 0/5	144
	fa 0/1	fa 0/6	145
PC3	virtual NIC	fa 0/23	144

In order to test the connectivity between remote PCs and neighboring lab devices, using the above example, you may follow these steps, using an Instructor Account (see the *Manage Accounts* section of the [NETLAB+ Administrator Guide](#)).

1. Make a lab reservation.
2. Configure IP addresses on the remote PCs and neighboring lab devices you will be testing.
3. In the example above, PC1a and PC1b should share the same VMnet, so they should be able to ping each other. If they cannot ping each other, then you should review the following:
 - What VMnet is PC1a and PC1b using? (refer to [5.3](#))
 - Is there a firewall installed or enabled on the virtual machine?
4. To verify the connectivity between remote PCs and neighboring lab devices, you should test the following:
 - Ping from PC1a to R1 and vice versa.
 - Ping from PC1b to R1 and vice versa.
 - Ping from PC2 to R2 and vice versa.
 - Ping from PC3 to R3 and vice versa.
5. If you can ping from a remote PC to a neighboring lab device, but cannot ping from the lab device to the remote PC, then you may want to determine if there is a firewall installed or enabled on the virtual machine.
6. If any of the tests from step 4 completely fail (you cannot ping from remote PC to neighboring lab device and vice versa), then you will need to analyze the network traffic on the control switch. Using the above example, perform the following steps:
 - Connect a PC or terminal to the console port of the control switch.
 - Type “**show vlan**” or “**show vlan brief**” to view the VLAN status on the control switch.

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.

```
Connected to 169.254.1.14.
Escape character is '^]'.

User Access Verification

Password:
netlab-cs4>en
Password:
netlab-cs4#show vlan

VLAN Name                Status    Ports
-----
1    default                active    Fa0/14, Fa0/15, Fa0/16,
                                           Fa0/18, Fa0/19, Fa0/20,
                                           Fa0/22, Fa0/24, Gi0/1
3    NETLAB_3               active
11   NETLAB_11              active
12   NETLAB_12              active
13   NETLAB_13              active
140  NETLAB_140             active    Fa0/1
141  NETLAB_141             active    Fa0/2
142  NETLAB_142             active    Fa0/3
143  NETLAB_143             active    Fa0/4
144  NETLAB_144             active    Fa0/5
145  NETLAB_145             active    Fa0/6
```

During a lab reservation, you will notice the active lab ports and their VLAN assignments. From the example above, Pod #5 is a BRPv2 installed on ports fa0/1 through fa0/6 on Control Switch #4. The base VLAN for this pod is 140.

- On the control switch, type “**show interfaces trunk**” to view the trunk information.

```
netlab-cs4#show interfaces trunk

Port      Mode      Encapsulation  Status      Native vlan
Fa0/23    on        802.1q         trunking    1

Port      Vlans allowed on trunk
Fa0/23    140,142,144

Port      Vlans allowed and active in management domain
Fa0/23    140,142,144

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/23    140,142,144
```

This command will reveal whether or not you have properly configured the control switch port that connects to the VMware trunking port. The following shows the proper configuration for the example above on port 23 of Control Switch #4.

```
netlab-cs4#show running-config interface fastEthernet 0/23
Building configuration...

Current configuration : 252 bytes
!
interface FastEthernet0/23
 description trunk to VMware 10.0.0.25
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 140,142,144
 switchport trunk pruning vlan none
 switchport mode trunk
 switchport nonegotiate
 no ip address
end
```


- Obtain the MAC address of a virtual machine by using the “**ipconfig /all**” command at the command prompt of the virtual machine.

```

C:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Pod_5 PC_2>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : UM-51B
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Unknown
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . :
    Description . . . . . : VMware PCI Ethernet Adapter
    Physical Address. . . . . : 00-0C-29-2F-57-F2
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . : Yes
    Autoconfiguration IP Address. . : 169.254.123.104
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . :

C:\Documents and Settings\Pod_5 PC_2>

```

- On the control switch, type “**show mac-address-table dynamic**”. Use the MAC address table to verify: 1) whether the MAC addresses of the remote PCs are in the table and 2) if these MAC addresses are in the correct VLANs.

```

netlab-cs4#show mac-address-table dynamic
      Mac Address Table
-----
Vlan    Mac Address      Type        Ports
----    -
140     0000.0c5d.150e   DYNAMIC     Fa0/1
140     000c.291d.6ee8   DYNAMIC     Fa0/23
140     000c.292f.57f2   DYNAMIC     Fa0/23
142     000c.291f.6542   DYNAMIC     Fa0/23
142     0010.7b81.aae0   DYNAMIC     Fa0/3
144     0000.0c76.bd12   DYNAMIC     Fa0/5
144     000c.29c1.1bc7   DYNAMIC     Fa0/23
1       000d.60f3.1757   DYNAMIC     Fa0/24
1       0050.5000.1109   DYNAMIC     Fa0/24
1       00c0.b763.c4ce   DYNAMIC     Fa0/24
1       00c0.b7a3.1def   DYNAMIC     Fa0/24
Total Mac Addresses for this criterion: 11

```

7. If any of the tests from step 4 completely fail (you cannot ping from the remote PC to a neighboring lab device and vice versa), and the MAC address of a remote PC is either:
 - a. Not in the correct VLAN or
 - b. Does not show up in the control switch MAC address table, please review the VLAN and VMnet settings for your NETLAB+ pod very carefully. Refer to [Part 5](#) for complete details.

Possible error conditions include:

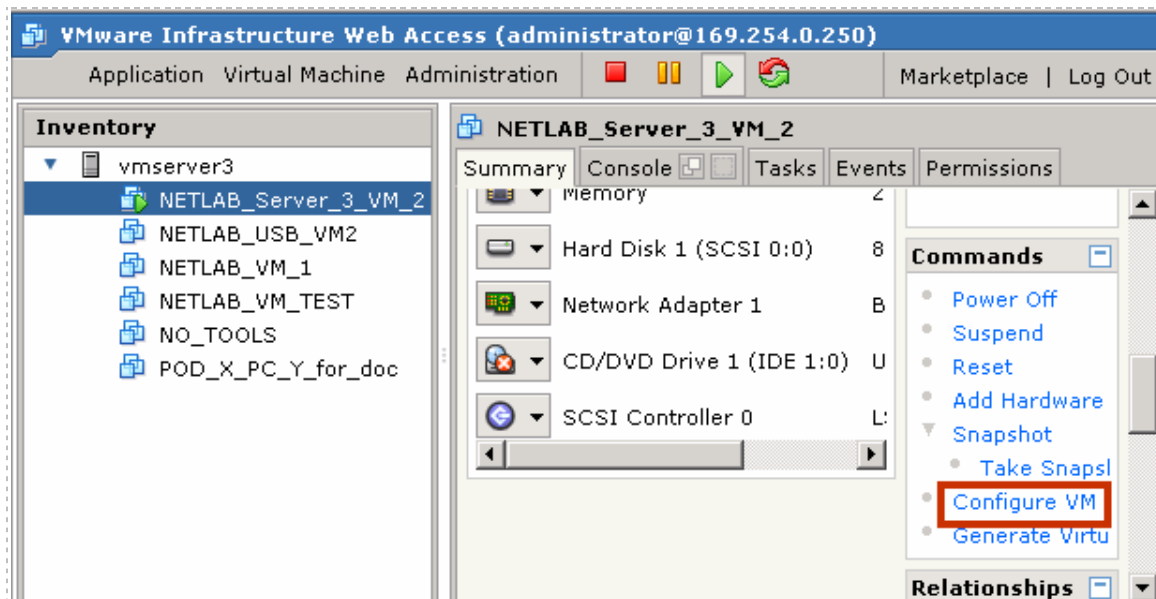
- An incorrect VLAN ID was entered when creating a VLAN interface.
- No VLAN or an incorrect VLAN was mapped to a VMnet using the Virtual Network Editor
- The wrong VMnet was configured for the Virtual Machine's configuration (using the VI Web Access page). In this case you would have to take a new snapshot (after correction is applied).
- The control switch port (for the Inside Connection) is not trunking or not allowing the correct VLANs.

If you are in the process of installing a new NETLAB_{AE} pod on your NETLAB+ system, please return now to the respective [pod-specific guide](#) for your pod. The final chapters, *Testing the Pod*, and *Finishing Up* provide details that will allow you ensure your pod is installed properly and ready for use.

6.2 Review and Modify VM Settings For an Existing Virtual Machine

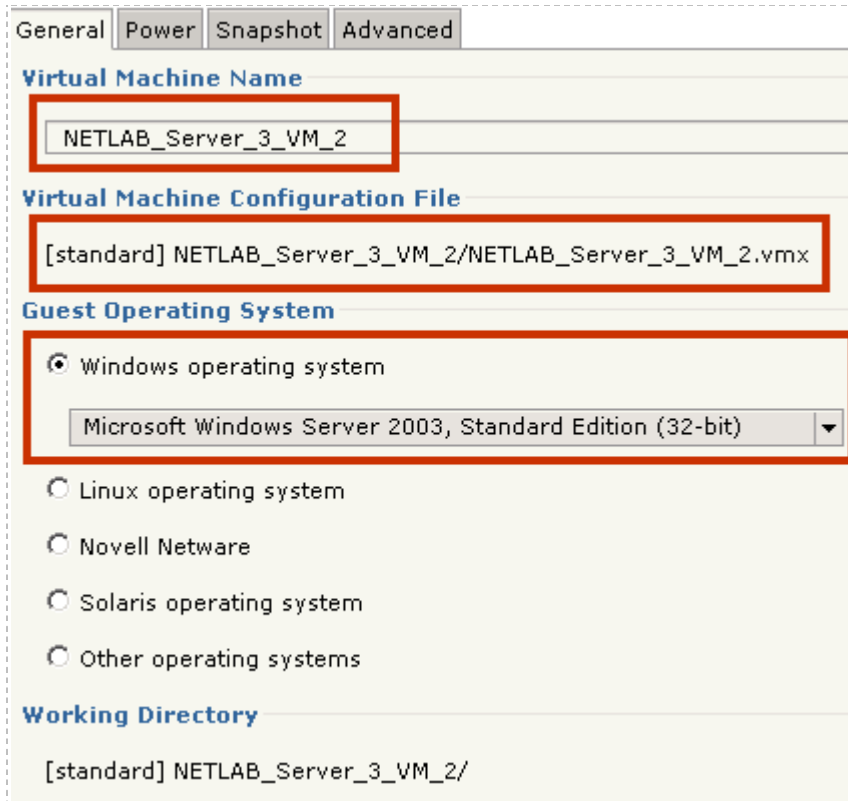
Section 4.1 outlined the creation of new virtual machines using the New Virtual Machine Wizard. This section describes how to verify and/or modify the VM settings of an existing virtual machine for integration with NETLAB+.

Using the **VI Web Access** page, select your virtual machine from the Inventory and click **Configure VM** in the **Commands** section.



The settings on the general tab include the Virtual Machine Name, Configuration File, and your selection of guest operating system.

The machine and file names shown here are for example purposes, your selections may vary.



General | Power | Snapshot | Advanced

Virtual Machine Name
NETLAB_Server_3_VM_2

Virtual Machine Configuration File
[standard] NETLAB_Server_3_VM_2/NETLAB_Server_3_VM_2.vmx

Guest Operating System

Windows operating system
Microsoft Windows Server 2003, Standard Edition (32-bit)

Linux operating system

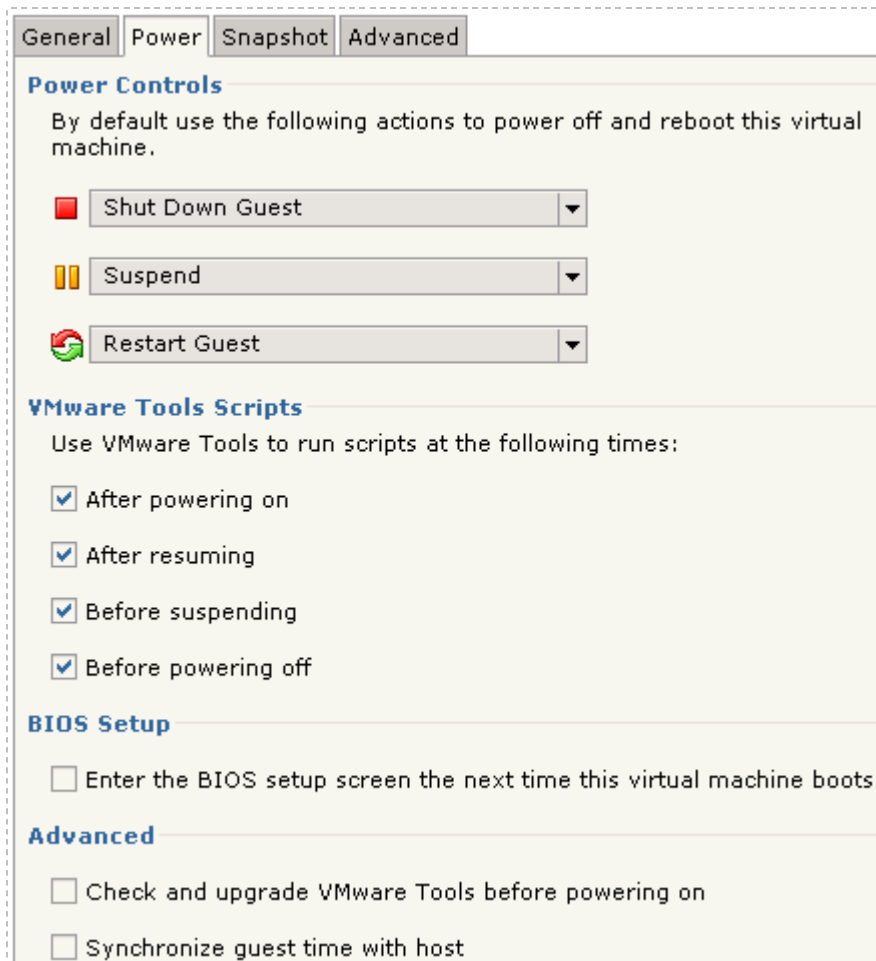
Novell Netware

Solaris operating system

Other operating systems

Working Directory
[standard] NETLAB_Server_3_VM_2/

Select the **Power** tab to display the Power settings. Use the default selections for Power settings, as shown in the screenshot below.





The screenshot shows the VMware configuration interface with the 'Power' tab selected. The 'Power Controls' section includes three dropdown menus: 'Shut Down Guest' (with a red square icon), 'Suspend' (with a yellow vertical bar icon), and 'Restart Guest' (with a green circular arrow icon). The 'VMware Tools Scripts' section has four checked checkboxes: 'After powering on', 'After resuming', 'Before suspending', and 'Before powering off'. The 'BIOS Setup' section has one unchecked checkbox: 'Enter the BIOS setup screen the next time this virtual machine boots'. The 'Advanced' section has two unchecked checkboxes: 'Check and upgrade VMware Tools before powering on' and 'Synchronize guest time with host'.


General Power Snapshot Advanced

Power Controls

By default use the following actions to power off and reboot this virtual machine.

 Shut Down Guest

 Suspend

 Restart Guest

VMware Tools Scripts

Use VMware Tools to run scripts at the following times:

- After powering on
- After resuming
- Before suspending
- Before powering off

BIOS Setup

- Enter the BIOS setup screen the next time this virtual machine boots

Advanced

- Check and upgrade VMware Tools before powering on
- Synchronize guest time with host

Select the **Snapshot** tab. The **When Powering Off** option must be set to **Just Power Off**. If these options are unavailable, check to make sure the Virtual Machine is neither running nor suspended.



General Power Snapshot Advanced

Current Snapshot

No current snapshot.

Lock this snapshot
Prevent the current snapshot from being updated.

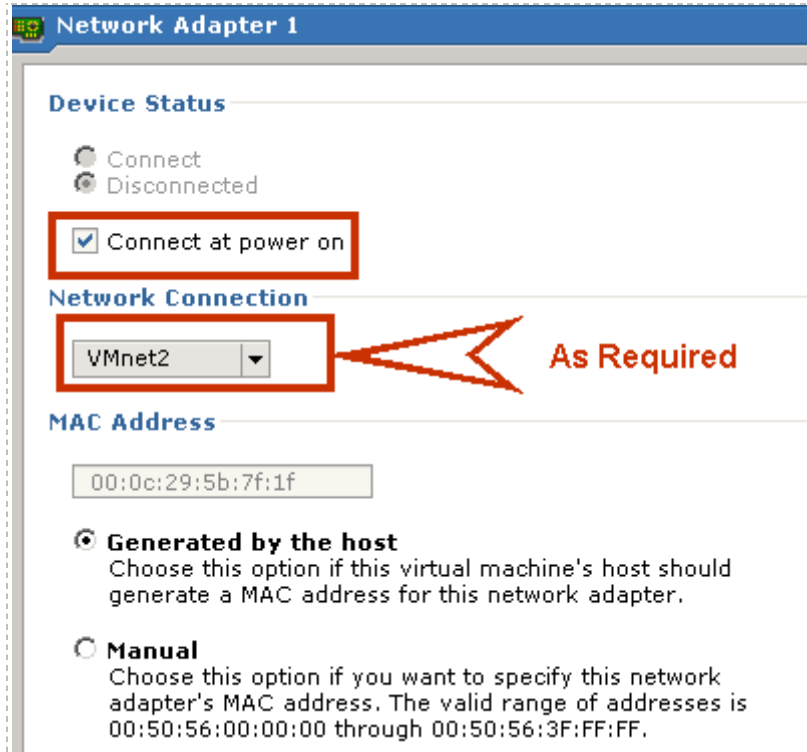
When Powering Off

Just power off

Revert to snapshot

Ask me

If this virtual machine must connect to an external network, such as a VLAN behind NETLAB+, you must connect a virtual network interfaces to the desired VMnet (see section 5.4 for details on accessing these settings).



Network Adapter 1

Device Status

Connect

Disconnected

Connect at power on

Network Connection

VMnet2

MAC Address

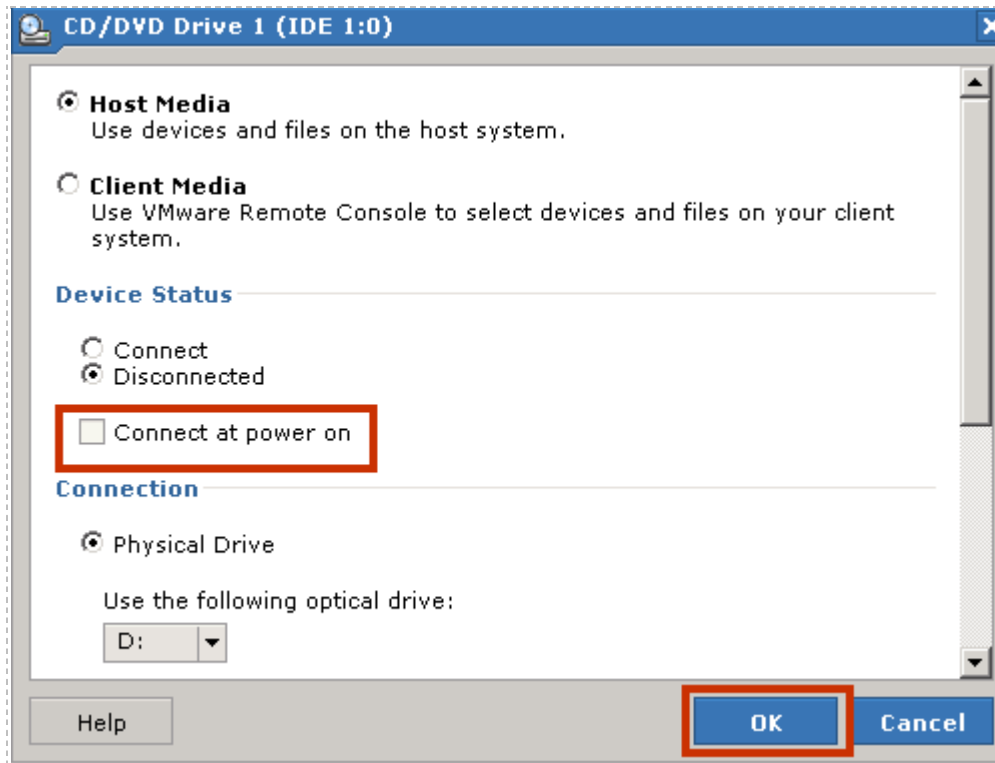
00:0c:29:5b:7f:1f

Generated by the host
Choose this option if this virtual machine's host should generate a MAC address for this network adapter.

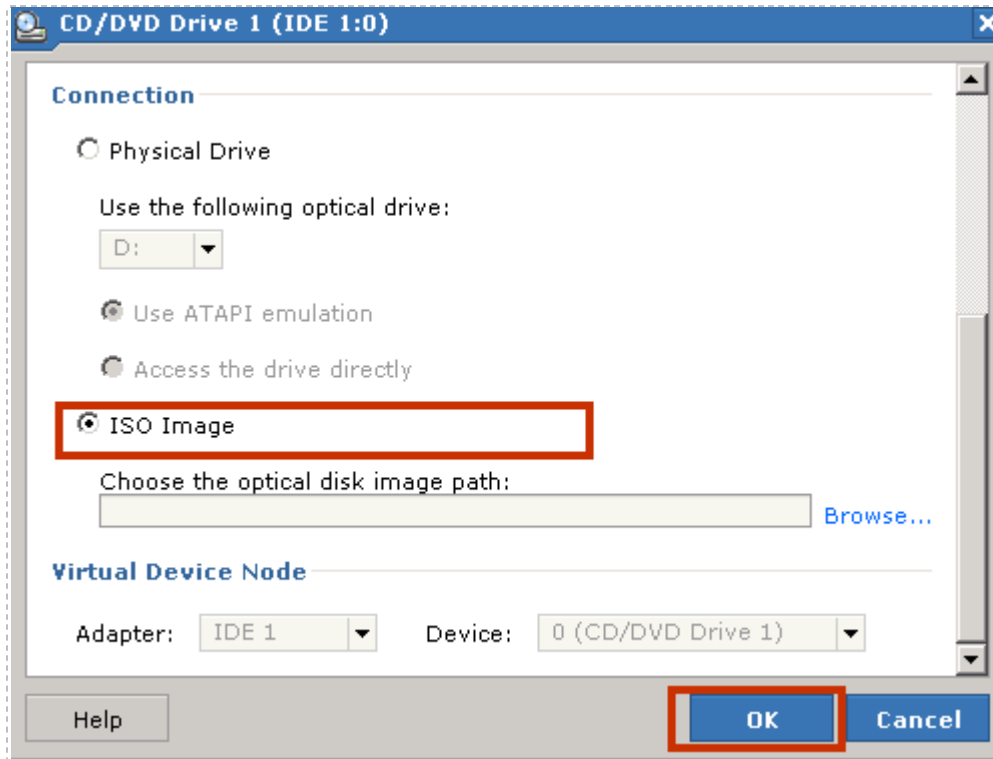
Manual
Choose this option if you want to specify this network adapter's MAC address. The valid range of addresses is 00:50:56:00:00:00 through 00:50:56:3F:FF:FF.

As Required

Verify the settings for the CD/DVD drive (see section 4.4 for details on accessing these settings). **Uncheck** the **Connect at power on** box. This is necessary to prevent the virtual machine from attempting to connect to the VMware host's CD/DVD device, which could result in undesired properties or boot errors.



You may also point the CD/DVD device connection to a unique ISO image on the local VMware host. If you choose this option, make sure each virtual machine you create does not point to the same ISO file. Otherwise, you may see some undesired properties or boot errors.

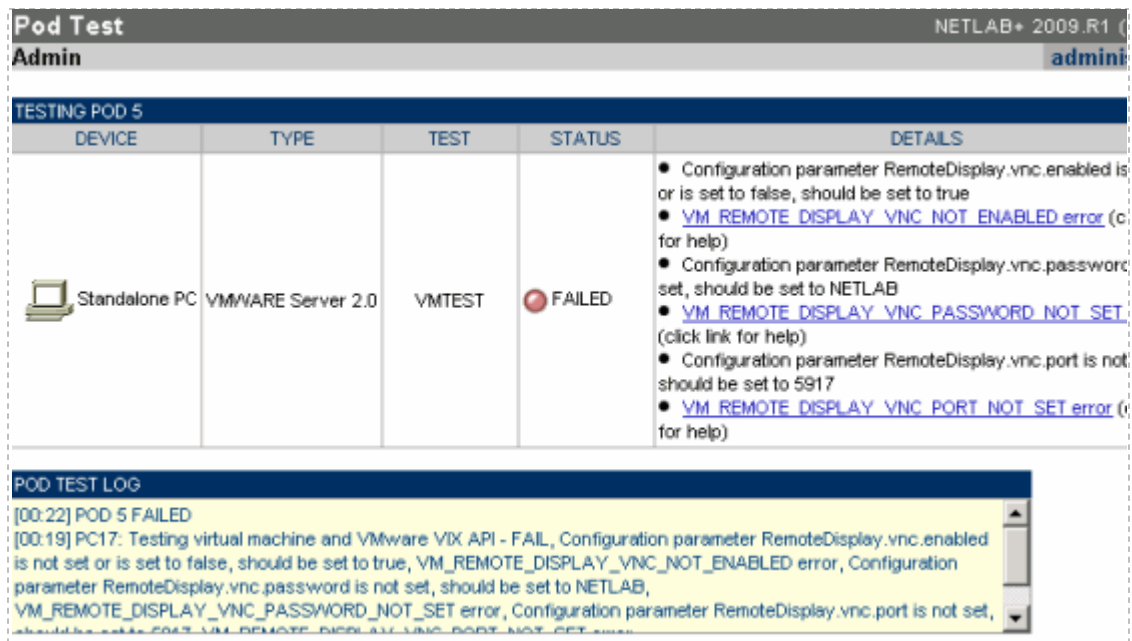


6.3 The Most Frequently Encountered VMware Issues



If you are experiencing problems with your virtual machines or they are not passing the pod test, please review the following symptoms and resolutions carefully:

1. **Symptom:** The user runs a pod test and the results indicate that the remote display settings are missing or misconfigured.

Additional information regarding error conditions is available by selecting the hyperlinked text within the details section of the pod test results.



The screenshot shows the 'Pod Test Admin' interface. At the top, it says 'Pod Test Admin' and 'NETLAB+ 2009.R1'. Below that, there's a section for 'TESTING POD 5'. A table lists the test results:

DEVICE	TYPE	TEST	STATUS	DETAILS
 Standalone PC	VMWARE Server 2.0	VMTEST	 FAILED	<ul style="list-style-type: none"> ● Configuration parameter RemoteDisplay.vnc.enabled is not set or is set to false, should be set to true ● VM_REMOTE_DISPLAY_VNC_NOT_ENABLED error (click link for help) ● Configuration parameter RemoteDisplay.vnc.password is not set, should be set to NETLAB ● VM_REMOTE_DISPLAY_VNC_PASSWORD_NOT_SET error (click link for help) ● Configuration parameter RemoteDisplay.vnc.port is not set, should be set to 5917 ● VM_REMOTE_DISPLAY_VNC_PORT_NOT_SET error (click link for help)


Below the table is a 'POD TEST LOG' section with the following text:

```
[00:22] POD 5 FAILED
[00:19] PC17: Testing virtual machine and VMware VIX API - FAIL, Configuration parameter RemoteDisplay.vnc.enabled is not set or is set to false, should be set to true, VM_REMOTE_DISPLAY_VNC_NOT_ENABLED error, Configuration parameter RemoteDisplay.vnc.password is not set, should be set to NETLAB, VM_REMOTE_DISPLAY_VNC_PASSWORD_NOT_SET error, Configuration parameter RemoteDisplay.vnc.port is not set, should be set to 5917, VM_REMOTE_DISPLAY_VNC_PORT_NOT_SET error
```

Resolution: Each virtual machine allocated for a NETLAB+ pod for remote PC access should have the VNC settings saved into the VMX file. This procedure is described in section 4.13.

2. Symptoms:

- a. The pod test is taking an unusually long time, fails to complete or
- b. You see the following error in the pod test:

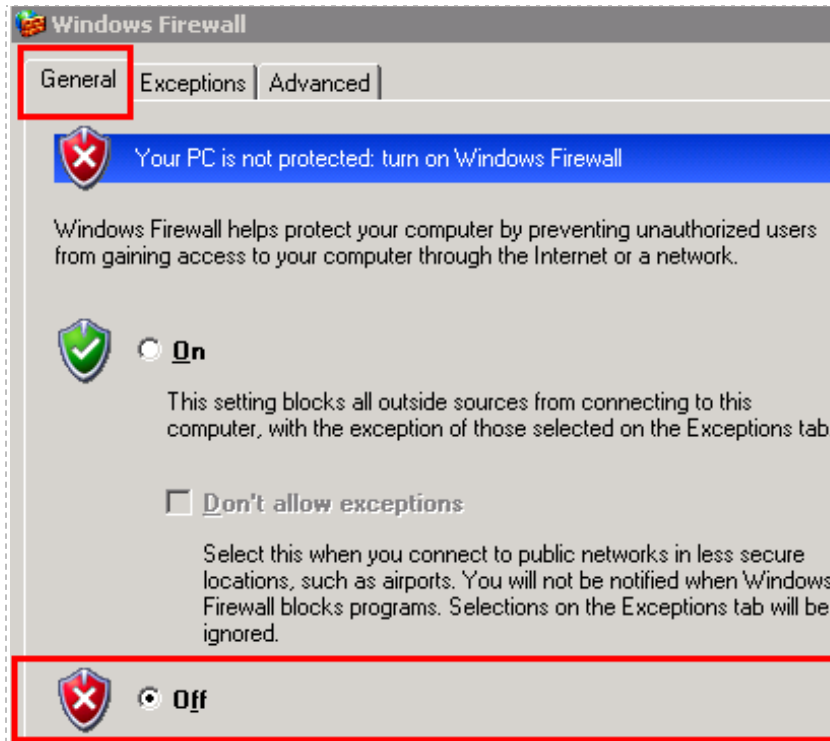
Pod Test				
Admin				admin
TESTING POD 5				
DEVICE	TYPE	TEST	STATUS	DETAILS
 Standalone PC	VMWARE Server 2.0	VMTEST	FAILED	<ul style="list-style-type: none"> • VIX could not get VNC settings • status=fail error="could not read variable RemoteDisplay.vnc.enabled" vix_error="virtual machine needs to be powered on" vix_errcode="VIX_E_VM_NOT_RUNNING (3006)" host="169.254.0.250" port="8333"
POD TEST LOG				
<pre>[00:12] POD 5 FAILED [00:09] PC17: Testing virtual machine and VMware VIX API - FAIL, VIX could not get VNC settings, status=fail error="not read variable RemoteDisplay.vnc.enabled" vix_error="The virtual machine needs to be powered on" vix_errcode="VIX_E_VM_NOT_RUNNING (3006)" host="169.254.0.250" port="8333" TESTING POD 5, Standalone Computer Pod, Support for 1 PC...</pre>				

Resolution: These symptoms are related to incorrect snapshot settings. The Virtual Machine should have the snapshot setting of **Just Power Off** (see section 4.2).

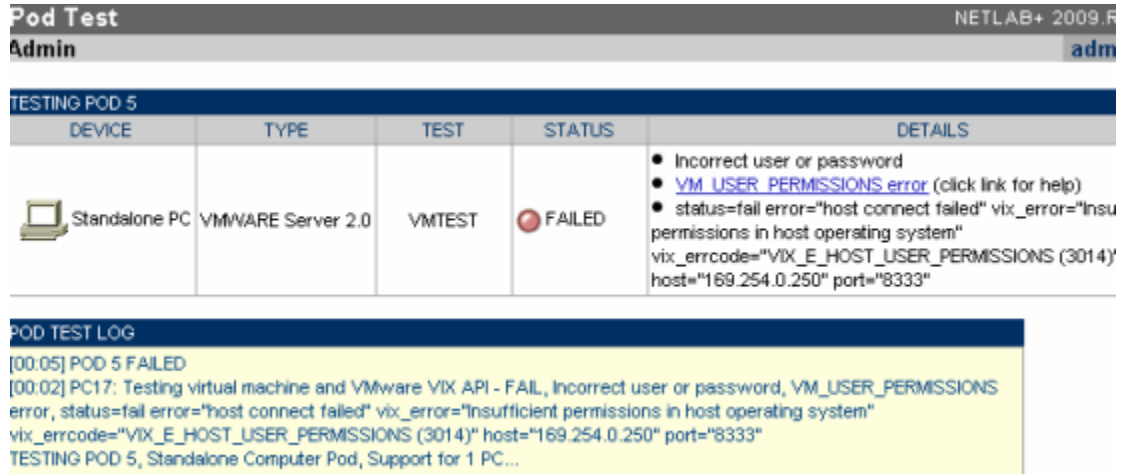
3. **Symptom:** You are unable to ping lab gear from the virtual machine.

Resolutions: See section 6.1 for an example of a troubleshooting scenario.



- a. Network traffic should be **bridged**, not routed, between equipment pods and VMware virtual machines. Therefore, it is important to **unbind TCP/IP** and Microsoft client protocols from each of the 802.1q sub-interfaces on the VMware host adapter that are associated with lab VLANs. Reference section 5.2.2 for full details.
- b. Each virtual machine should have the proper custom VMnet selected and that VMnet should be mapped to the proper VLAN adapter. Reference section 5.3 for full details.
- c. Disable built-in firewalls on the virtual machine (Windows firewall, for example).



4. **Symptom:** A Pod test failure indicates API-Fail incorrect user or password.



The screenshot shows the 'Pod Test' interface. At the top, it says 'Pod Test Admin' and 'NETLAB+ 2009.F' with a user 'adm'. Below is a table titled 'TESTING POD 5' with the following data:

DEVICE	TYPE	TEST	STATUS	DETAILS
 Standalone PC	VMWARE Server 2.0	VMTEST	 FAILED	<ul style="list-style-type: none"> Incorrect user or password VM_USER_PERMISSIONS error (click link for help) status=fail error="host connect failed" vix_error="Insufficient permissions in host operating system" vix_errcode="VIX_E_HOST_USER_PERMISSIONS (3014)" host="169.254.0.250" port="8333"

Below the table is a 'POD TEST LOG' section with the following text:

```
[00:05] POD 5 FAILED
[00:02] PC17: Testing virtual machine and VMware VIX API - FAIL, Incorrect user or password, VM_USER_PERMISSIONS error, status=fail error="host connect failed" vix_error="Insufficient permissions in host operating system" vix_errcode="VIX_E_HOST_USER_PERMISSIONS (3014)" host="169.254.0.250" port="8333"
TESTING POD 5, Standalone Computer Pod, Support for 1 PC...
```

Resolution: Make certain you have created the management account (section 3.9) and you added to proper permissions (section 3.10).

5. **Symptom:** My keyboard and/or mouse are behaving very erratically (sub as, double letters, or the mouse is very jumpy) when using the NETLAB+ Remote PC viewer.

Resolution: Each virtual machine should have **VMware Tools** installed. Refer to section 4.5 for full details.

6. **Symptom:** I am using a non-Windows guest operating system, and I cannot get the mouse to behave properly.

Resolution: Some guest operating systems, such as Linux, require very specific steps to install VMware Tools properly. For example, most Linux VMs require you to run a configuration script to complete the VMware Tools installation. Do not assume that VMware Tools is properly installed without reviewing the guidelines as per the VMware documentation:

<http://kb.vmware.com/selfservice/dynamic/kc.do?externalId=340&sliceId=2&command=show&forward=nonthreadedKC&kcId=340>.

7. **Symptom:** You are in a NETLAB+ reservation and the Remote PC viewer is slightly sluggish in performance.

Resolution: Each virtual machine should be adjusted for optimum remote display access (see section 4.6):

- a. Minimal screen resolution with 32-bit color quality (see sections 4.6).
 - b. Do not use a graphical background. The desktop background should be plain or none (see section 4.8).
 - c. Adjust the visual effects for best performance (each O/S may have different settings, see section 4.7).
8. **Symptom:** Your virtual machines are giving an “UNKNOWN” status from the Status tab of a lab reservation in NETLAB+.

Resolution: Review the following potential causes:

- a. We recommend no more than 10 to 12 virtual machines, **MAXIMUM**, per server that meets the **MINIMUM** requirements in section 2.2. Each virtual machine uses CPU cycles and memory on the server. As a simple rule of thumb, divide the processor clock speed by the number of virtual machines to determine the speed of each virtual machine in a heavily loaded environment (i.e. all pods are running at the same time and users are working on the PCs). For example, a 3GHz processor could run 10 virtual machines at 300MHz each. This does not account for overhead on the host operating system.

If your VMs are running in a heavily loaded environment, the VMware daemon process may stall, hang, or become unresponsive. This could cause requests from the NETLAB+ server to be ignored. This would give an “UNKNOWN” status for your remote PCs from the Status tab of a lab reservation in NETLAB+.

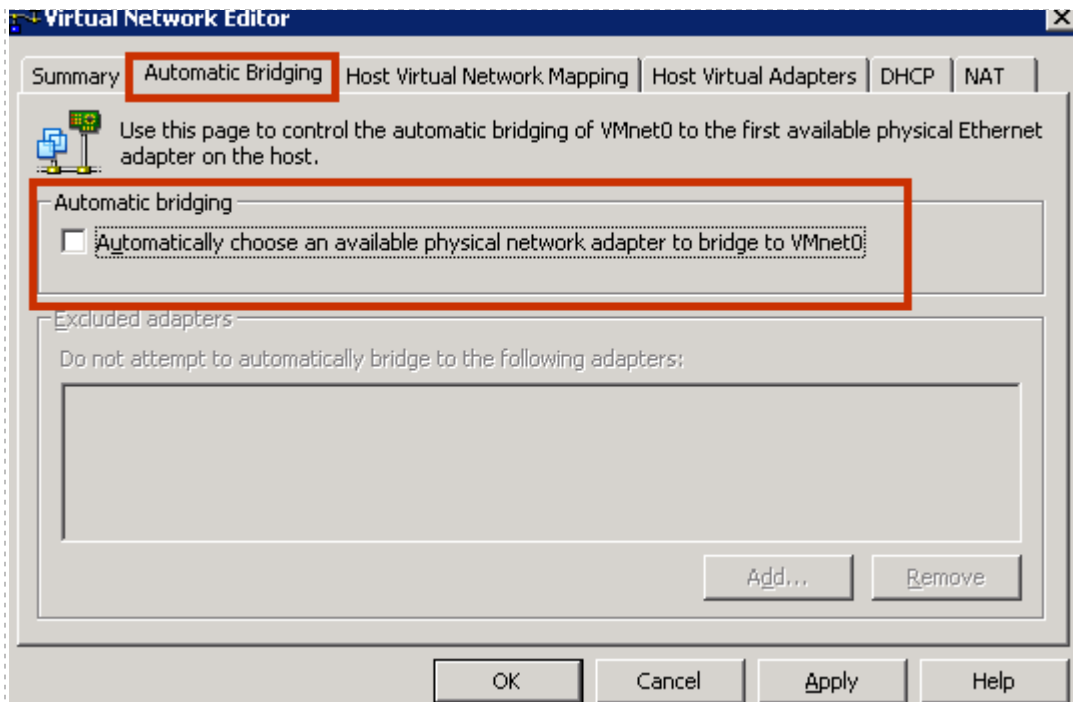
- b. Each virtual machine should have their virtual CD/DVD device disabled, (section 4.4).
- c. Verify each VM setting from section 6.2.

Appendix A Using Reserved Virtual Networks for External Connectivity

VMware uses three of its virtual networks (VMnet) to provide special guest services such as NAT and DHCP. By default, virtual networks VMnet0, VMnet1, and VMnet8 are unavailable for external connectivity to lab networks behind NETLAB+. However, if the built-in services are not needed, you can reconfigure and reclaim these virtual networks for external connectivity.

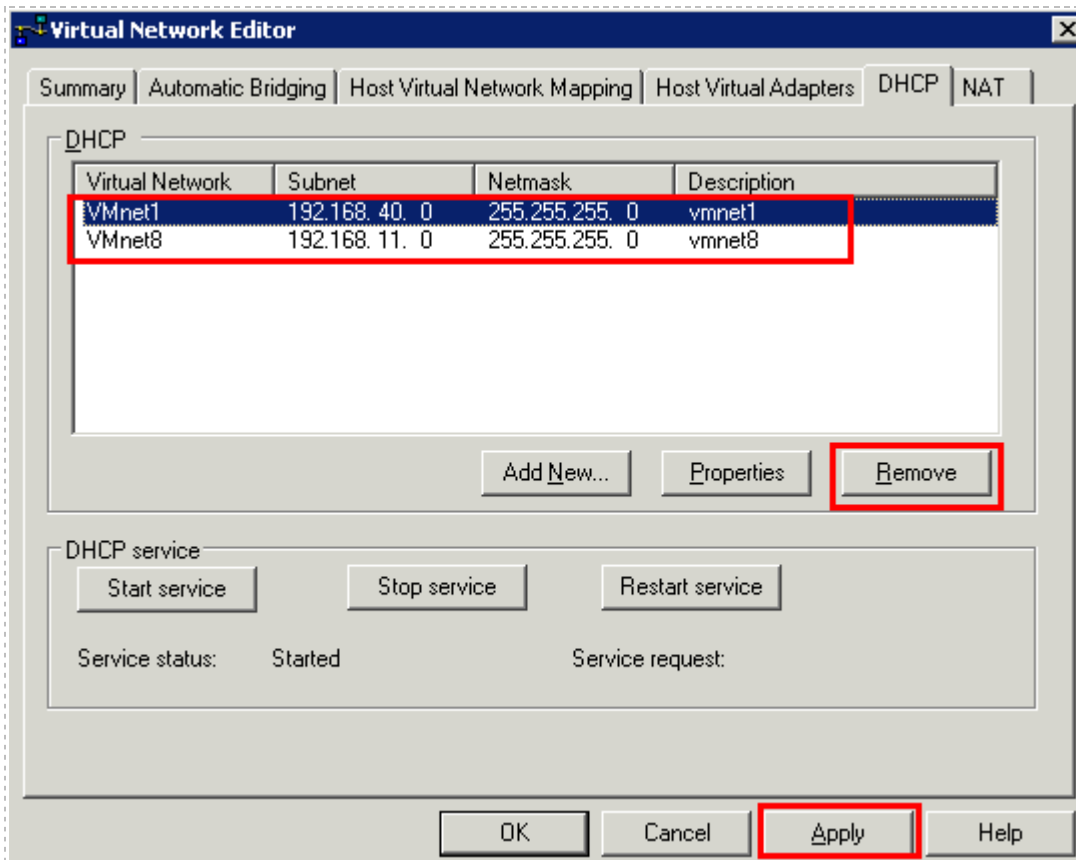
NETLAB Academy Edition[®] pods do not utilize the built-in VMware networking services. Therefore, the steps outlined below will maximize the number of available virtual switches that can interface with lab pods.

Open the Virtual Network Editor (see section 3.11) and select the **Automatic Bridging** Tab.



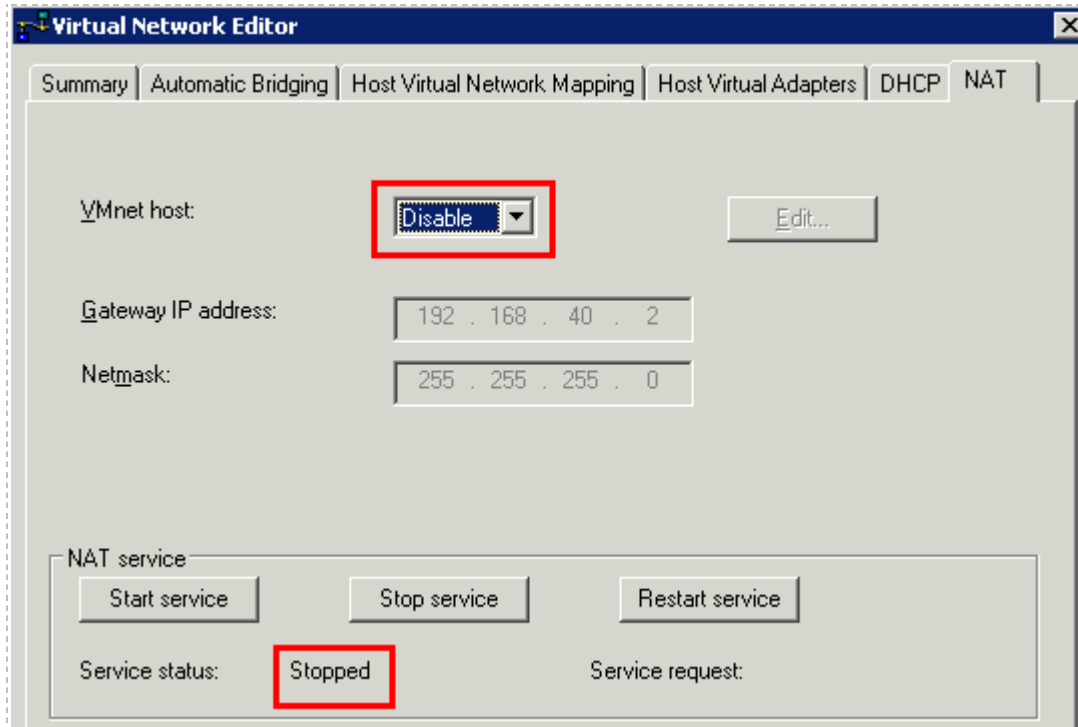
1. Click on the DHCP tab.
2. Remove VMnet1 and click **Apply**.
3. Remove VMnet8 and click **Apply**.

The service status should change to **Stopped**.



4. Click on the NAT tab.
5. Change VMnet host to **Disable** and click **Apply**.

The service status should change to **Stopped**.



All ten VMnet virtual networks can now be used to provide connectivity to external VLANs. This process is described in section 5.3.

Appendix B Copying VMDK File to Clone Virtual Machines

Once you have successfully created a single virtual machine, you may clone this VM to create new VMs as a short cut. This would essentially save the time it takes to install a new guest operating system and VMware Tools.

Each guest operating system is fully functional and must meet the vendor's licensing requirements.

This short cut is useful only if your NETLAB+ pod VMs are going to have similar virtual machine settings:

- VM memory size (can be adjusted easily after new copy is created)
- VM hard disk size (**cannot** be adjusted easily)
- VM Operating System (this must be the same if you are cloning)

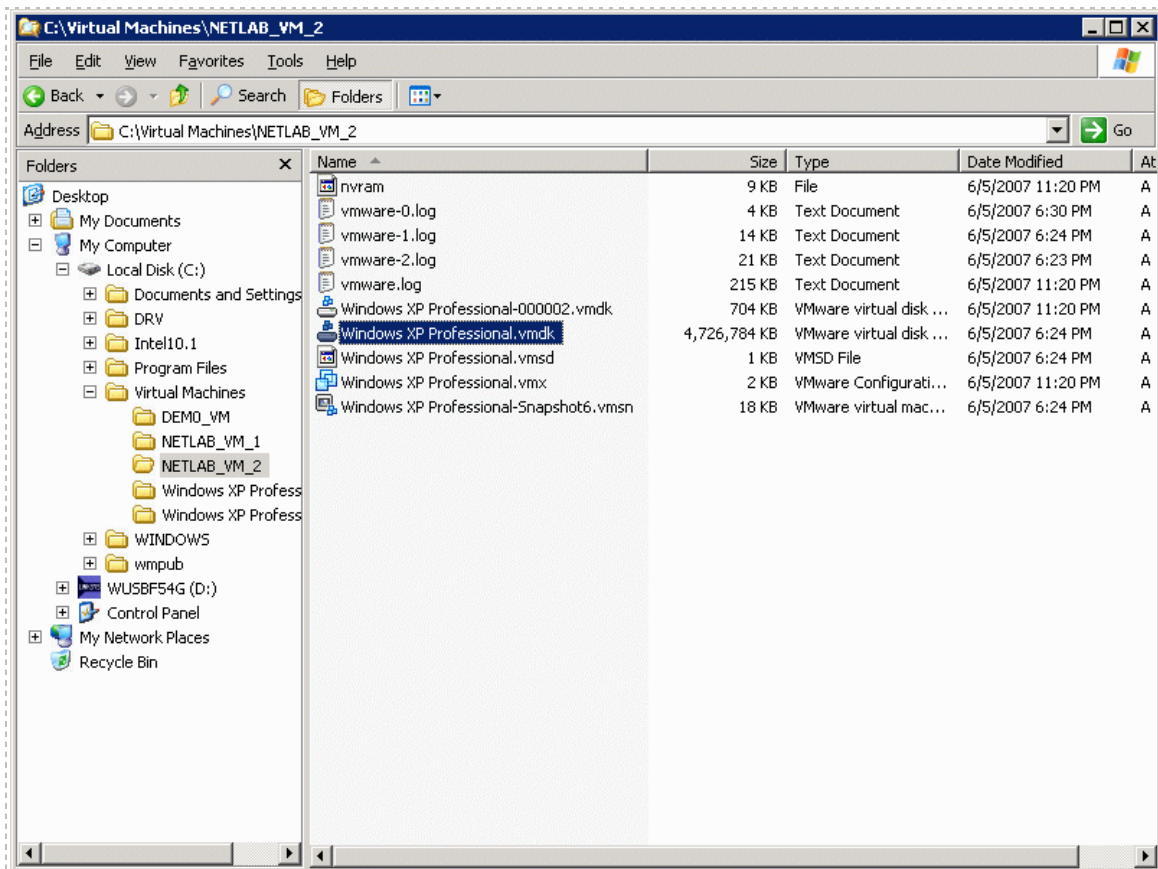
The following steps highlight procedure for cloning your virtual machine to create new VMs. It is assumed you have successfully created a single VM as per [Part 4](#).

1. Create a new Virtual Machine by following the exact steps from sections [4.1](#) through [4.2](#). Make sure your new VM has the same hard disk size and VMDK file name as the VM you are copying.

Always create a new virtual disk for your VMs; do not use an existing virtual disk (each VM, whether copied or not, should have its own unique virtual hard disk).

- Copy and Paste the VMDK (VMware virtual disk) file from the directory of the virtual machine you are copying to the directory of the VM you just created (the VM directories should be located in the Virtual Machines directory on your host server).

Do not cut, move, or rename the VMDK file. The new VM's virtual disk file (VMDK) will be overwritten by the VMDK file you are copying. If you have not renamed the VMDK files, then the VMDK file names should be the same in both directories.



- Start the new virtual machine you have just cloned. It should be an exact copy of the VM you copied. Make any necessary changes to the copied VM, to separate it from the copied VM (i.e. if these VMs will be networked on the same subnet, you may want to change the Computer Name or IP settings).
- Power down the cloned VM and take a snapshot to save your work.
- Repeat steps 1 through 4 above to clone any further required VMs for your NETLAB+ pods.
- Perform a pod test (see section 4.15) to verify connectivity.

Appendix C Contacting NDG for Technical Support


If you need to contact NDG for support, please be aware that VMware Server is a third party product. NDG cannot transfer a customer to the VMware help desk, but we will do our best to help you setup and operate a remotely accessible PC or server using supported VMware virtualization products on your NETLAB+ system under the following guidelines:

1. The NETLAB+ administrator has thoroughly studied the NDG documentation including this guide, and attempted to install Virtual Machines (VMs) based on NDG recommendations.
2. Remote access to both the VMware Server and NETLAB+ server provides the most effective way for NDG to assist customers.
 - a. NDG provides up to 2 hours of support assistance for customers with current NETLAB+ support agreements if remote access is enabled.
 - b. NDG can remotely troubleshoot a VMware server from the NETLAB+ server. Please contact NDG for specific instructions.
 - c. Remote access to the NETLAB+ server is provided via SSH (preferred) or Telnet. Please reference the NDG [CSS whitepaper](#) for port details.
 - d. We request that the NETLAB+ administrator be present while NDG is providing assistance.

Appendix D Upgrading from VMware Server 1.0 and GSX to VMware Server 2.x

There are several modifications required in order to update an existing virtual machine running VMware server 1.x or GSX to VMware server 2.x.

1. Modify the power-off option to **Just Power Off**. The VMware API in VMware Server versions 1.x does not currently provide a mechanism to manage snapshots. NETLAB+ works around this limitation by utilizing a dialog. If you are upgrading to VMware Server 2.x, it is necessary to change the power-off option from **Ask Me** to **Just Power Off**. Please refer to section [4.2](#) for details.
2. Modify the **PC Type** setting to **VMware Server 2.0**. This value is must be set for each virtual machine that you are upgrading to VMware Server 2.x. Please refer to [4.12](#) for details.

POD 5 - PC 17	
PC ID	17
PC Name	 Standalone PC
Type	VMWARE Server 2.0 ▼
VMware Host IP Address	10.0.0.27
VMware Host Username	NETLAB
VMware Host Password	NETLAB
VMware Guest Configuration File	[standard] NETLAB_VM_1\NETLAB_VM_1.vmx
VMware Guest Operating System	Windows XP ▼
VMware Guest VNC Settings	RemoteDisplay.vnc.enabled = "true" RemoteDisplay.vnc.password = "NETLAB" RemoteDisplay.vnc.port = "5917"
Access Method	VNC ▼
Admin Status	ONLINE ▼
Options	<input checked="" type="checkbox"/> revert to snapshot during scrub operation

3. Modify the value of the VMware Guest Configuration file to the format of a relative path name. This value must be set for each virtual machine that you are upgrading to VMware Server 2.x. This file name is typically in the form of [datastore]<pc name>/<operating system>.vmx. Example: [standard] POD_1 PC_3/winXPpro.vmx. Please refer to [4.12](#) for details.

The use of relative path names is specific to VMware Server 2.x. VMware server 1.0 and GSX require absolute path names. If you are upgrading from VMware Server 1.0 and GSX, you must change your configuration file path names to use relative path names, as shown in the example above.

4. If you are converting a VMware 1.0 Virtual Machine to a VMware 2.x Virtual Machine, please reference the appropriate procedure from the official VMware documentation: [VMware Server User's Guide](#).
5. Run at pod test to verify the function of the API, see section [4.15](#).

Appendix E Experimental Use of a Broadcom Networking Adapter

We strongly discourage the use of NetXTreme™ Broadcom networking adapters due to a problem with the configuration utility and the use of VLANs. **We recommend upgrading to an Intel Networking Adapter for the inside interface.**

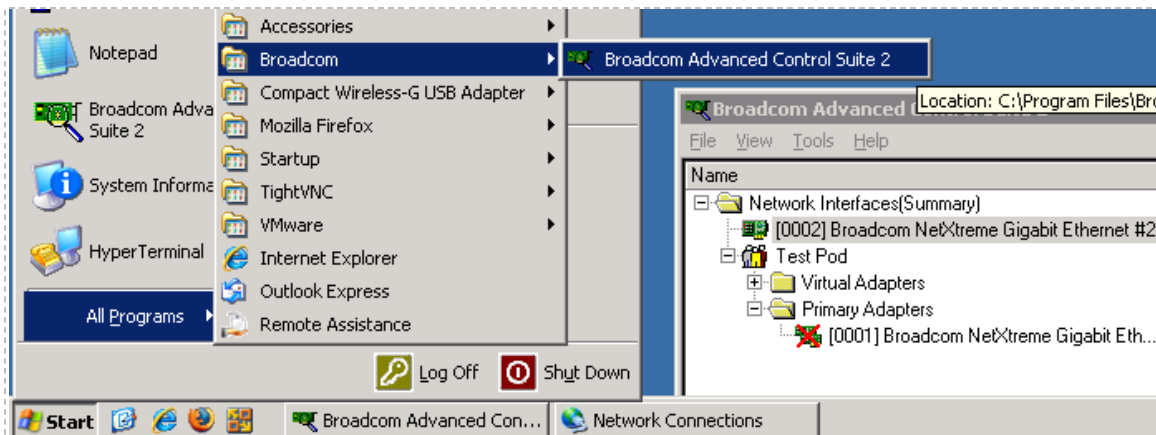
Please refer to section [2.1.4.6](#) for details on this known issue.

This section below provides guidance for those who have already purchased Broadcom adapters and wish to pursue experimental use.

Appendix E.1 VLAN Support for Broadcom Networking Adapters

VLAN support for Broadcom NetXTreme™ adapters is provided by the driver and the Broadcom Advanced Control Suite (BACS) software. This software is often included on a CD-ROM that ships with your server. You can also obtain an updated copy of this software by downloading the driver for your specific adapter from the Broadcom website. After successfully installing BACS, you can access the configuration tool from the Windows Start menu.

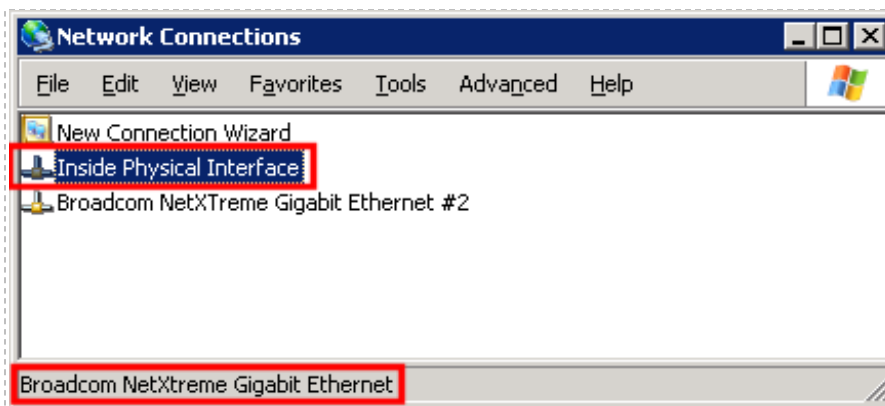
➤ **Start → All Programs → Broadcom → Broadcom Advanced Control Suite**



Appendix E.2 Creating VLAN 1 – Broadcom Adapters

This section is an alternative to the procedure described in section 3.4.5. The use of an Intel Networking Adapter is strongly recommended.

From the Network Connections window, identify the Broadcom-assigned name for the Inside Physical Interface. The easiest way to do this is to click on the interface to highlight it; the Broadcom name will be displayed in the status bar. Alternatively, the Broadcom name is displayed as a tooltip when you hover the mouse over the Windows interface name.

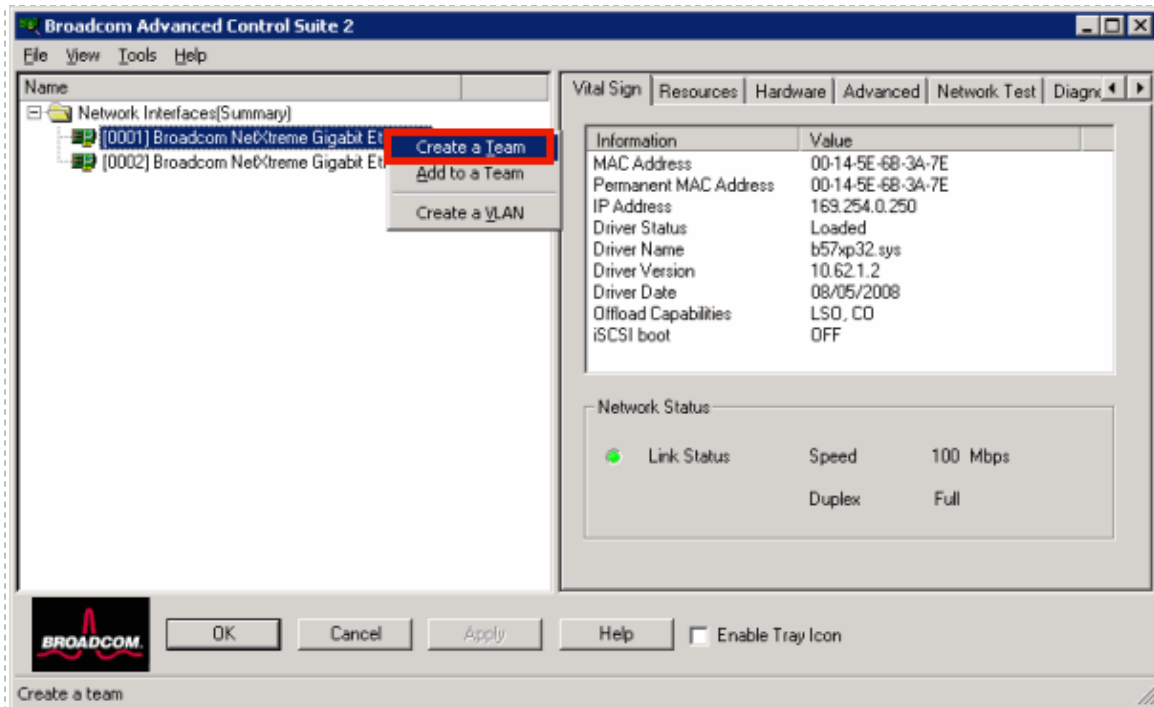


On a Broadcom networking adapter, VLANs are created using the BACS application:

Start → All Programs → Broadcom → Broadcom Advanced Control Suite

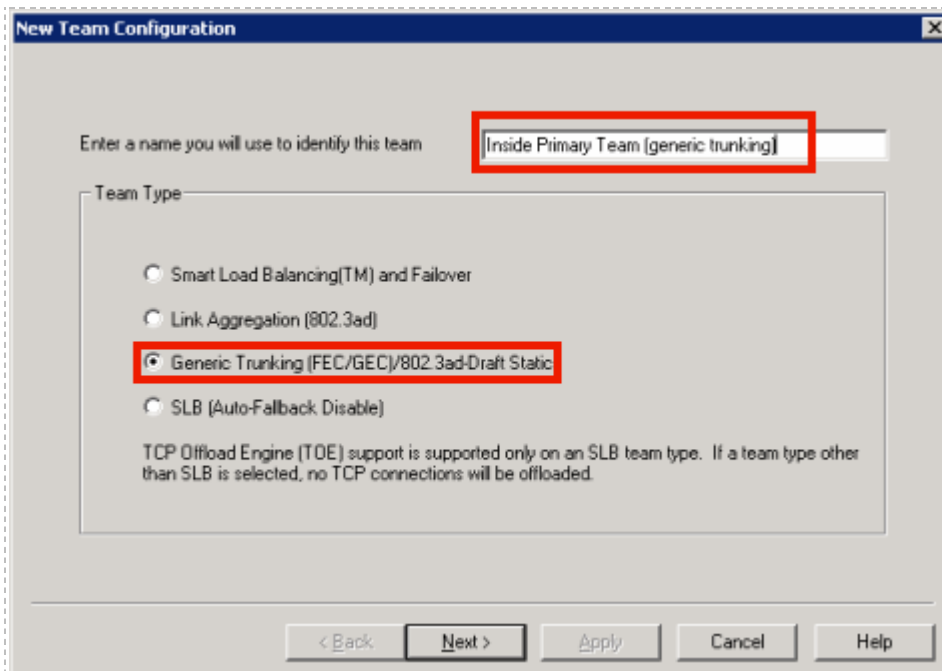
Select the **Broadcom name** for the **Inside Physical Interface** (identified in the previous step).

- **Right click** on the Broadcom interface name.
- Select **Create a Team**

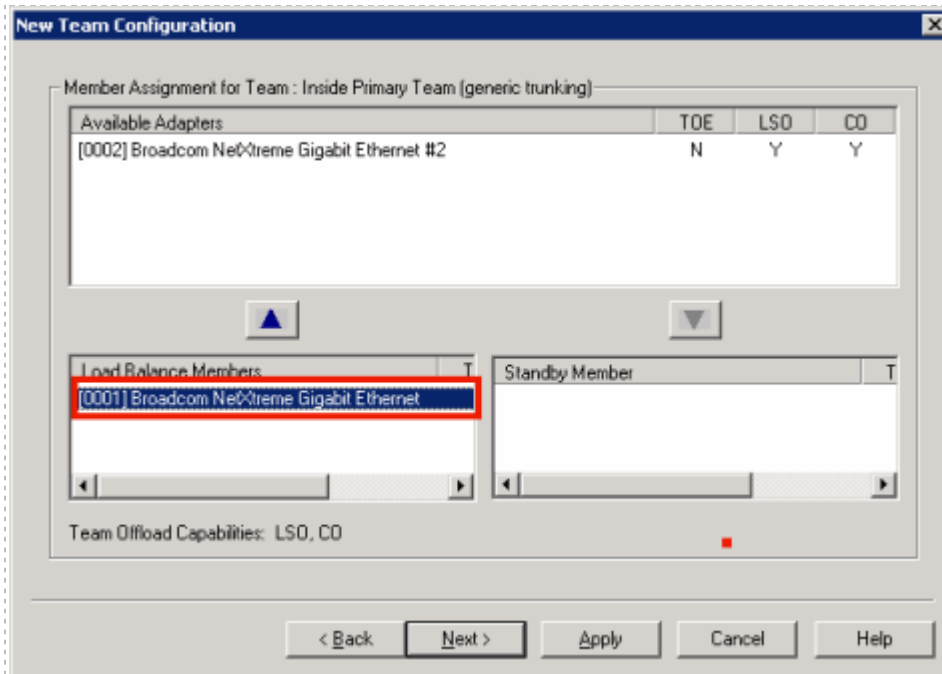


- Enter a descriptive name to identify the team.
- Select **Generic Trunking** for **Team Type**

The team must be set to Generic Trunking mode. This is required due to known issues as described in section [2.1.4.6](#).

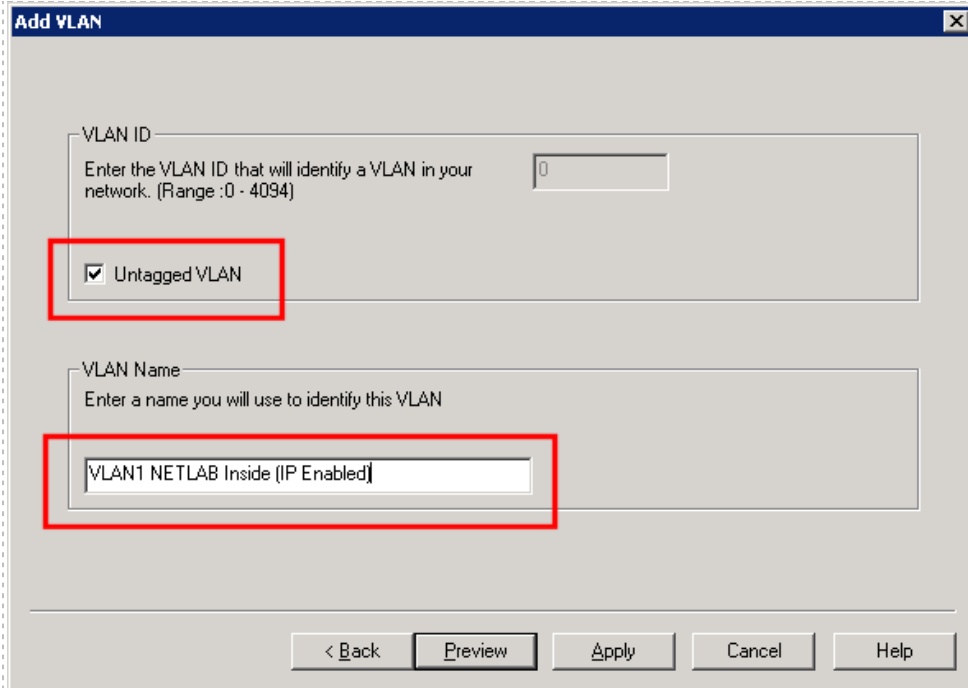


- You must assign the trunking interface to a load balance membership to continue.
- Click **Apply**.



Create an Untagged VLAN.

- Check the **Untagged VLAN** checkbox.
- Name the VLAN, **“VLAN1 NETLAB Inside (IP Enabled)”**.
- Click **Apply**.



Add VLAN

VLAN ID
Enter the VLAN ID that will identify a VLAN in your network. (Range :0 - 4094)

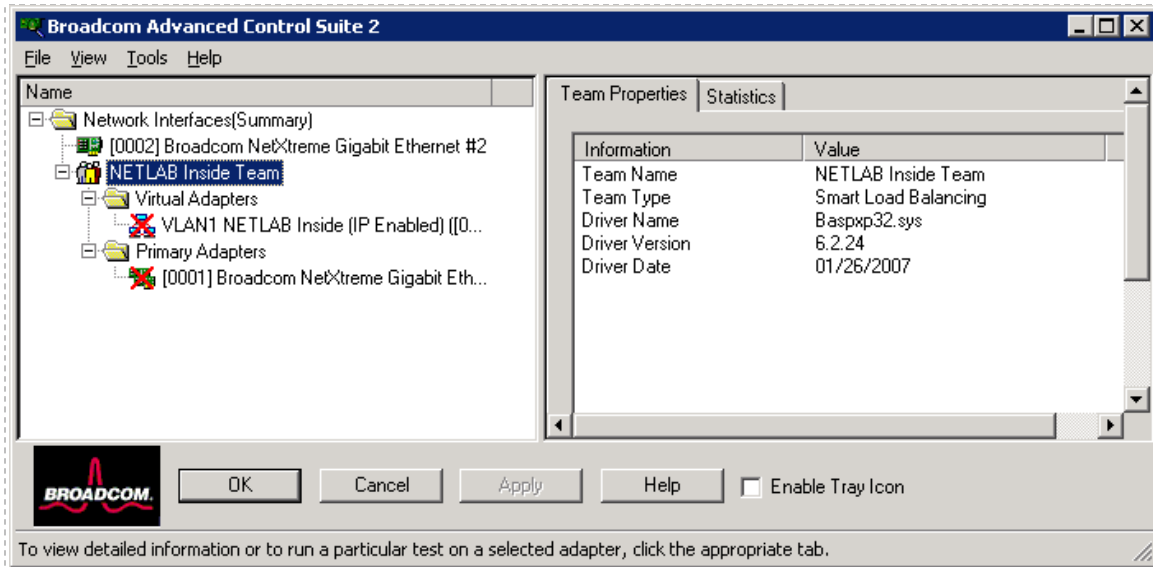
Untagged VLAN

VLAN Name
Enter a name you will use to identify this VLAN

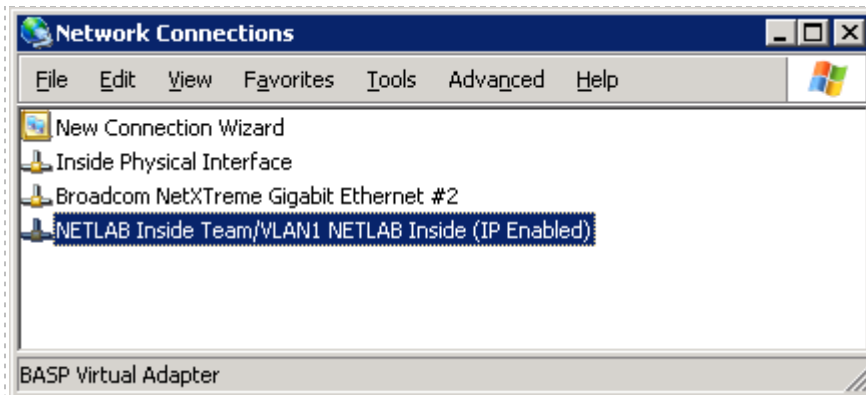
VLAN1 NETLAB Inside (IP Enabled)

< Back Preview Apply Cancel Help

If you expand the tree nodes, the Broadcom Inside Interface should now have a structure that looks like this:



BACS will also create a new Windows networking adapter for VLAN 1. If the Windows name is not the same name you provided in the BACS utility, rename the interface in Windows so they match.



The VLAN 1 adapter is a logical sub-interface of the Inside Physical Interface. However, this hierarchy is not reflected in the Windows Network Connections. Windows treats VLAN interfaces as ordinary network adapters.

Appendix E.3 VLAN Support for Broadcom Networking Adapters

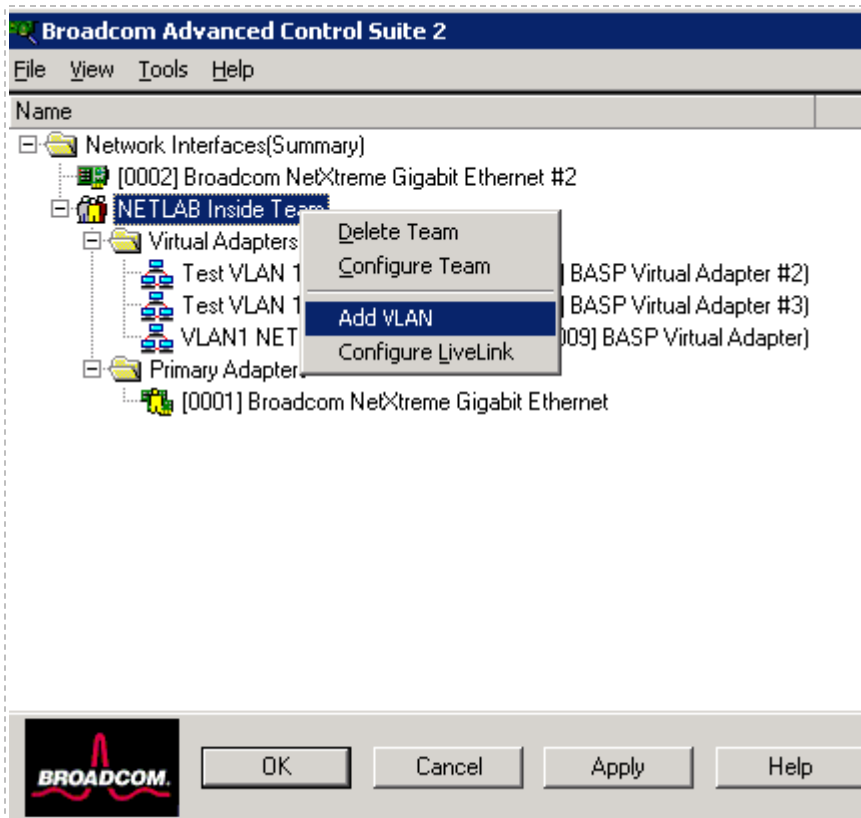
This section is an alternative to the procedure described in section 5.2. The use of an Intel Networking Adapter is strongly recommended.

On a Broadcom networking adapter, VLANs are created using the BACS application:

Start → All Programs → Broadcom → Broadcom Advanced Control Suite

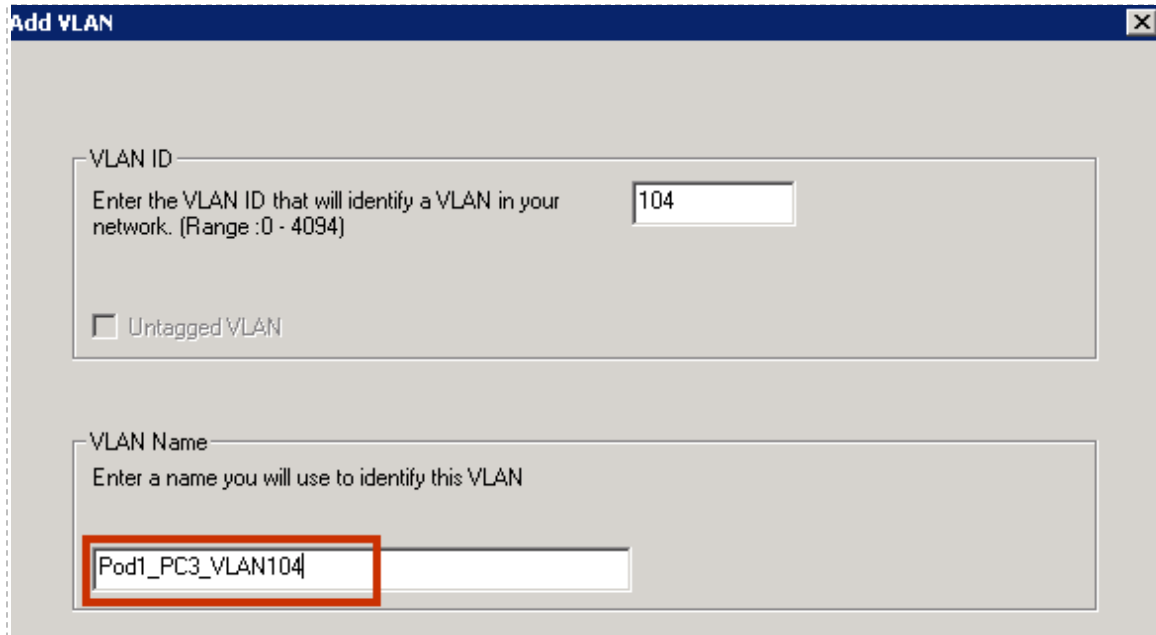
Locate the **Broadcom name** for the **Inside Physical Interface** (as described in [Appendix E.2](#)).

- **Right click** on the **NETLAB Inside Team**.
- Select **Add VLAN**.

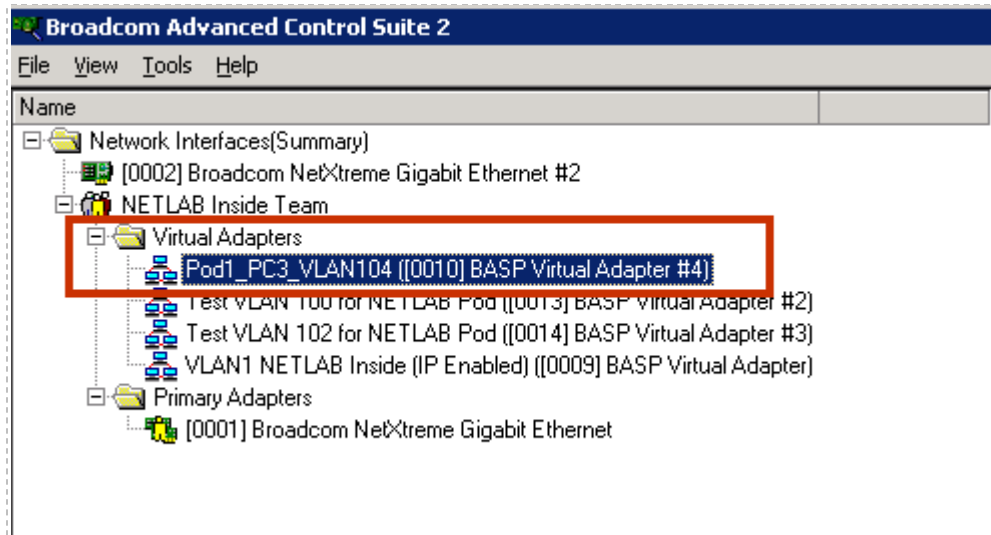


To create a VLAN:

- Enter the appropriate **VLAN ID** as per section 5.1.
- Enter a descriptive name(i.e. pod number and remote pc number) for the **VLAN Name** field.
- Click **Apply**.

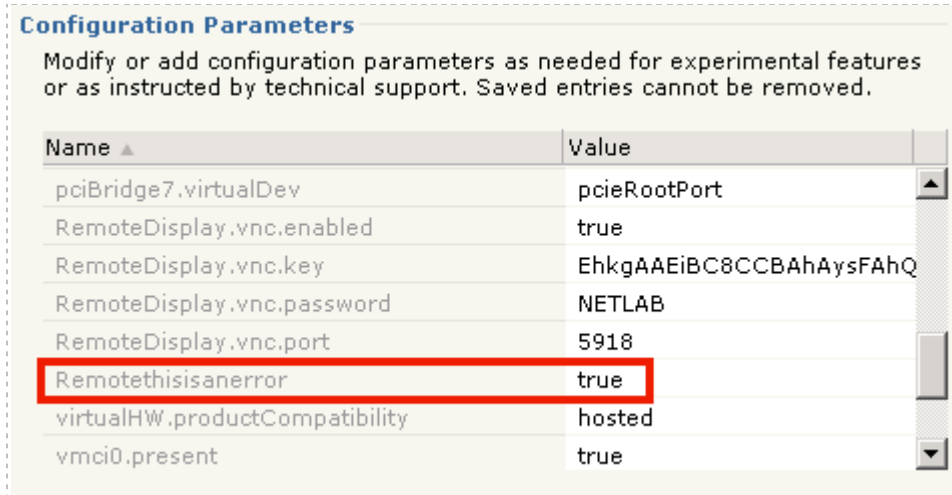


The VLAN you have added will now appear in the list of virtual adapters.



Appendix F Resolving Errors to the Configuration File

If you make an error while keying in a configuration parameter, it will result in an erroneous entry in the configuration parameters of the virtual machine. Here, we show an example of an incorrect entry in the configuration parameters (section 4.13).

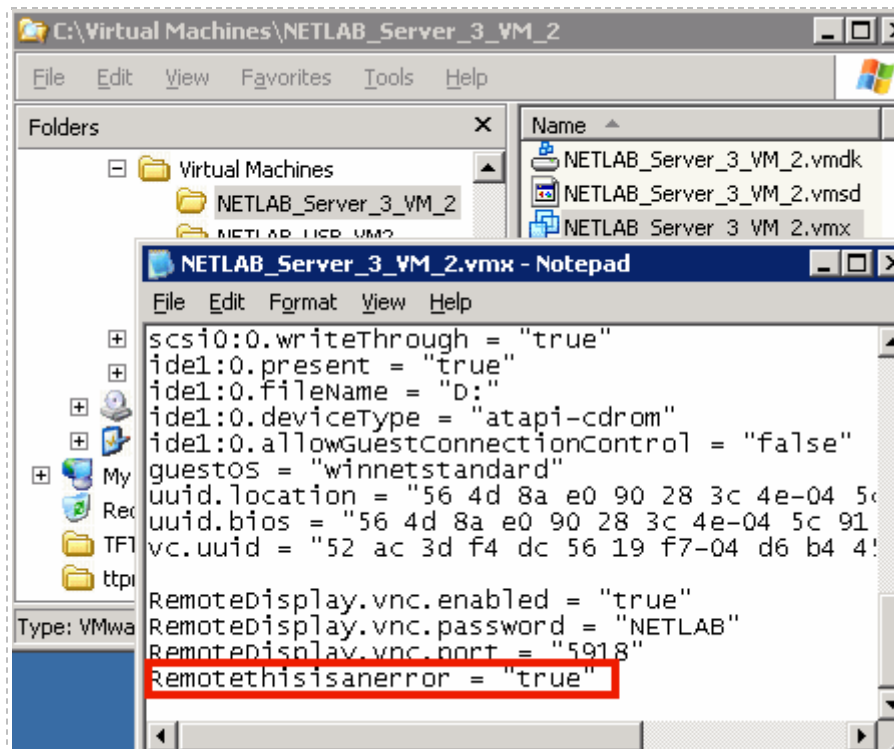


Configuration Parameters
Modify or add configuration parameters as needed for experimental features or as instructed by technical support. Saved entries cannot be removed.

Name ▲	Value
pciBridge7.virtualDev	pcieRootPort
RemoteDisplay.vnc.enabled	true
RemoteDisplay.vnc.key	EhkgAAEiBC8CCBAhAysFAhQ
RemoteDisplay.vnc.password	NETLAB
RemoteDisplay.vnc.port	5918
Remotethisisanerror	true
virtualHW.productCompatibility	hosted
vmci0.present	true

Use the following procedure to remove incorrect entries from the configuration file. It may be necessary to remove the virtual machine from the inventory (without deleting it from the disk), edit the VMX file and re-add, or restart the VMware Server services:

- Power down the VM.
- Remove the virtual machine from the inventory. **Virtual Machine** → **Remove Virtual Machine**. **DO NOT CHECK the Delete this virtual machine's files from the disk Option.**
- Edit the VMX file as desired.
 - a. Open the VMware configuration file for the virtual machine in Notepad.
 - b. Delete the incorrect entry from the file.



- c. Save and close the configuration file.
- Re-add the VM. **Virtual Machine** → **Add Virtual Machine to Inventory**
 - Verify the changes took place **Configure VM** → **Advanced Tab** → **Configuration Parameters**. Look through the list of configuration parameters and verify the three **RemoteDisplay** configuration parameters are present and that the erroneous entry has been removed.

Configuration Parameters

Modify or add configuration parameters as needed for experimental features or as instructed by technical support. Saved entries cannot be removed.

Name ▲	Value
pciBridge7.virtualDev	pcieRootPort
RemoteDisplay.vnc.enabled	true
RemoteDisplay.vnc.key	EhkgAAEiBC8CCBAhAysFAhQ
RemoteDisplay.vnc.password	NETLAB
RemoteDisplay.vnc.port	5918
virtualHW.productCompatibility	hosted
vmci0.present	true
vmware.tools.installstate	none

When you are finished editing the file, take a new snapshot of your virtual machine (see section 4.10).