⚠️ This support document is intended for users with an active VMware vSphere license. If you do not have a VMware vSphere license, you will need to purchase one to operate NETLAB+ until our team releases a version utilizing Proxmox.

.ıllNDG

NETLAB+®

Remote PC Guide Series - Volume 1

Introduction and Planning for Remote PC Implementation with NETLAB+

Document Version: 2020-04-24

What is a remote PC and how does it work with NETLAB+? This educational guide will introduce the concepts and terminology needed to begin planning Remote PC Implementation on your NETLAB+ system.

This guide is part of a multi-volume series, designed to provide you with the guidance needed to implement remote PCs on your NETLAB+ system. Learn more about the Remote PC Guide Series.

This guide is not an installation guide. This is an educational guide that explains what a Remote PC is and how it works in the NETLAB+ Environment.

1 Background

NETLAB+ remote PCs and servers in a pod can be implemented using virtual machines running on VMware vSphere. The flexibility and broad selection of operating systems and configurations that may be provisioned on a virtual machine offer great potential to support IT training in a wide range of disciplines using NETLAB+.

In the subsections below, we will begin by bringing to your attention the prerequisite knowledge recommended, along with building a fundamental understanding of how remote PCs, virtualization, and NETLAB+ work together.

Objectives

- What should I know before proceeding?
- What is a remote PC?
- What can users do with a remote PC?
- What is a virtual machine?
- How do NETLAB+, VMware vCenter, and VMware ESXi work together?

1.1 What should I know before proceeding?

NETLAB+ communicates with VMware vSphere to perform automated tasks and virtual machine management. Users of this guide should have a working knowledge of VMware vCenter, the vSphere Client, and VMware ESXi.

NETLAB+ administrators using this guide should be comfortable with the process of creating and configuring a virtual machine "from scratch" (using the vSphere Client).

The *VMware vSphere Virtual Machine Administration Guide* provides detailed guidance on provisioning virtual machines.

1.2   What is a Remote PC?

A *remote PC* is a personal computer or server that can be remotely accessed from another desktop. *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.
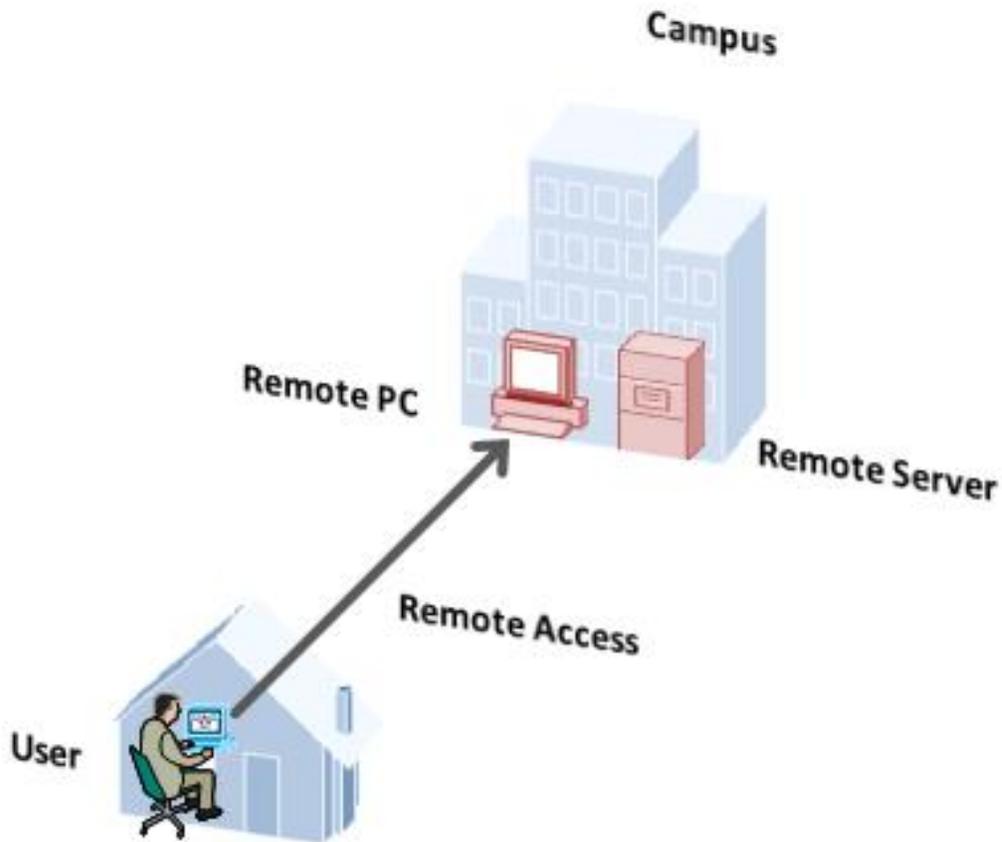
1.3   What can users do with a remote PC?

Users can remotely access the keyboard, video, and mouse of a remote PC. 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.

- **Online Lab Delivery.** Provide students with self-paced, scheduled access to real operating systems and application software, without distributing software or licenses.

- **Distance Learning.** Provide 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.** Provide scheduled usage to limited physical lab equipment and virtual machine host servers. Proactive Resource Awareness allows you to timeshare virtualization servers using the NETLAB+ scheduler.

- **Online Network Training.** Provides online delivery of network training. Remote PCs can interface with real lab equipment, such as routers, switches, and firewalls, all of which can be accessed remotely using NETLAB+.

- **Online General IT Training**. Provide 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. NETLAB+ includes 25 virtual topologies that can be used to teach a variety of courses, including Linux, Microsoft, or Cybersecurity. Pods using these topologies can be created very quickly using NETLAB+'s pod cloning and automated network features.

- **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, dealing with live viruses and malware, and scanning networks. At the end of the lab reservation, NETLAB+ will undo any changes.

- **NETLAB+ Supported Content** NETLAB+ is an excellent versatile solution for facilitating IT training in a variety of disciplines, including networking, virtualization, storage, and cybersecurity. NDG collaborates with leading industry training programs, including:

  - Cisco Networking Academy®
  - VMware IT Academy Program®
  - Linux Professional Institute
  - Palo Alto Networks Academy
  - Redhat® Academy

1.4   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 (VMs) to ensure that each application has time to execute.
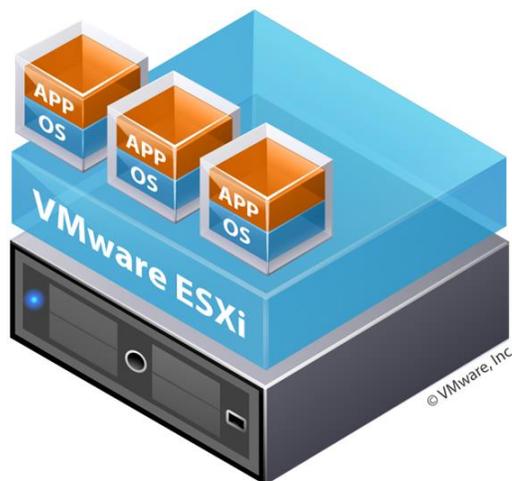

Virtualization allows you to host real operating systems and real application software with fewer hardware resources. To implement VMs, the NETLAB+ software interfaces with third-party virtualization products that run on separate servers (not on the NETLAB+ server).

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

1.5   How do NETLAB+, VMware vCenter, and VMware ESXi work together?

The following diagram depicts four major components that make up a typical NETLAB+ system setup using VMware vCenter and VMware ESXi 6.0.
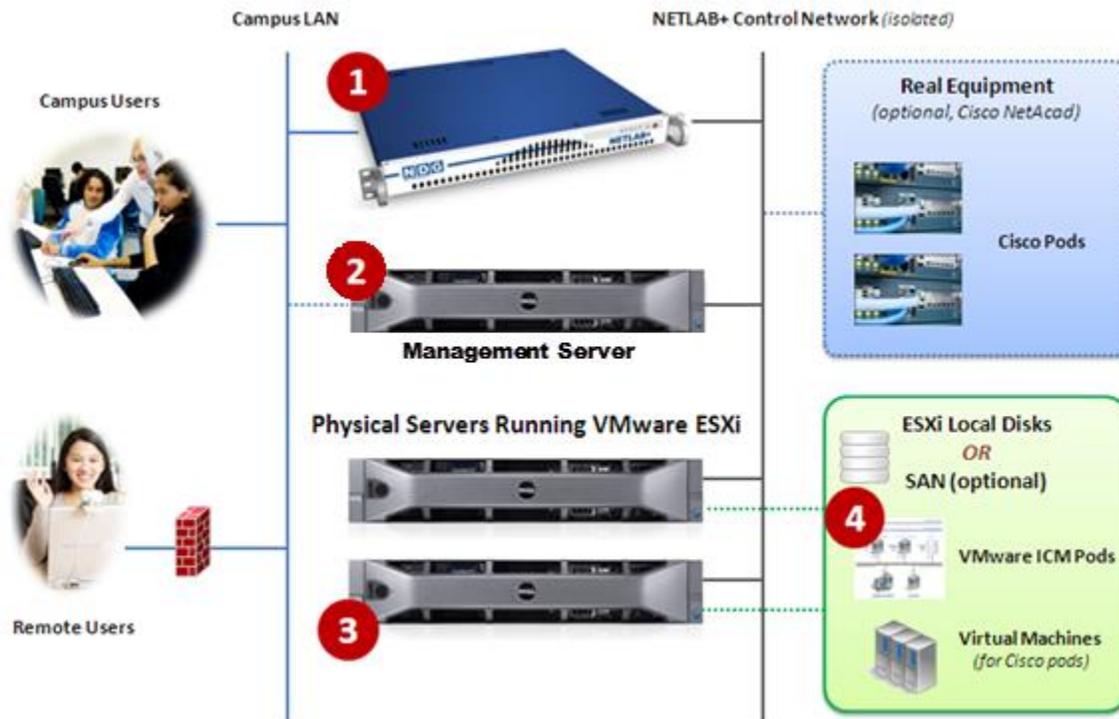

1. The NETLAB+ server provides the user interface for student and instructor access, an interface to manage VMs, and software features to automate virtual machine pod creation. This document assumes you have already set up your NETLAB+ server.

2. Management server running VMware vCenter Appliance is used to manage your physical VMware ESXi servers, to create VMs, and to take snapshots of virtual machines. NETLAB+ communicates with vCenter to perform automated tasks and virtual machine management.

3. Physical VMware ESXi servers host the virtual machines in your virtual machine pods. In the example environment shown here, there are two host servers. Each NETLAB+ remote PC or remote server runs inside of a virtual machine

4. Pods consisting of virtual machines reside on your physical ESXi host server disks. Optionally, these VMs can reside on a Storage Area Network (SAN).

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

Warning: NDG performance testing does not account for SAN latencies. Slides depicting a SAN do not advocate the purchase or use of a SAN.

Storage Area Network
(optional, purchased separately)
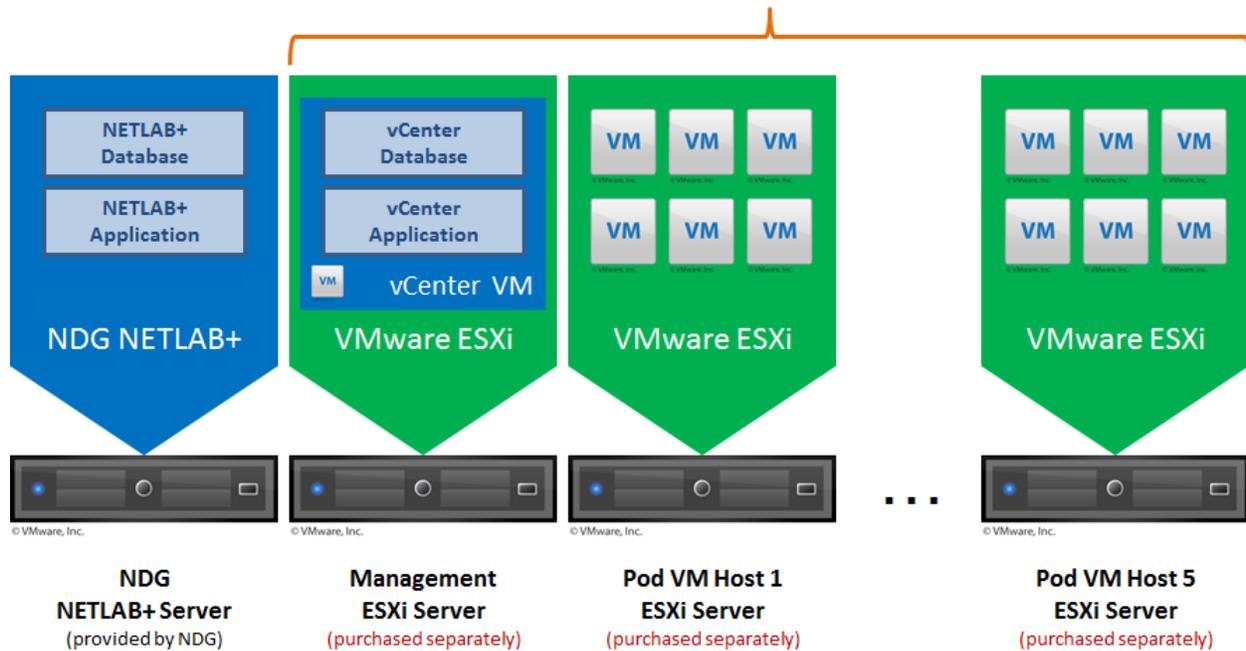
Here is a list of features and benefits provided by NETLAB+, working in conjunction with VMware vCenter and VMware ESXi.

- **Remote Access.** 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.

- **Sharing.** Multiple users can share access to a virtual machine simultaneously.

- **Connection Proxy.** 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 VMs 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.

- **Automated Operations.** Users may power on, power off, and revert to a clean state (scrub) from the NETLAB+ web interface.

- **Snapshots.** 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.

- **Progressive Labs.** Using NETLAB+ Pod Assigner, students may be assigned their own pod and personal VMs for an entire course. These VMs will retain their state between lab reservations.

- **Linked Virtual Machines.** NETLAB+ cloning operations support linked virtual machines. A linked virtual machine shares virtual disks with a master virtual machine in an ongoing manner. This conserves disk space and allows multiple virtual machines to use the same software installation. Linked virtual machines can be created very quickly because most of the disk is shared with the master VM.

- **Pod Cloning.** Pods containing only virtual machines can be cloned in a single operation. This is called pod cloning. The NETLAB+ administrator can clone a master pod very quickly. Using linked virtual machines, a typical pod can be cloned in one minute or less.

- **Automatic Networking.** Many NDG provided pod templates support automatic networking. When a pod starts, NETLAB+ will create all the necessary virtual switches and/or port groups on the VM's host server, and bind each virtual machine network adapter to the correct port group. At the end of the lab reservation, NETLAB+ will delete the virtual switches and port groups used by the pod to free networking resources.

- **Automatic Remote Display Setup.** NETLAB+ now supports the automatic setup of remote display parameters on virtual machines. This feature, combined with pod cloning and automatic networking, allows pods to be deployed very quickly from a set of master VMs without any manual setup.

- **Proactive Resource Awareness.** Proactive Resource Awareness allows you to time-share virtualization servers using the NETLAB+ scheduler. If scheduling a particular pod would exceed the virtualization host server limits in a 30-minute time slot, the pod cannot be scheduled at that time, which will be clearly indicated on the scheduler. This feature allows you to increase trainees with fewer servers while providing a good lab experience.

- **VM Deletion.** Virtual machines can be removed from the inventory and/or completely from the disk directly from NETLAB+. When deleting a pod, NETLAB+ provides the option to delete all virtual machines in one operation.

2   Planning

2.1   VMware Product Comparison

The following table compares NETLAB+ support for selected VMware hosting products.

> ⚠️ **Please use VMware ESXi 6.0 or 6.7.**
>
> **Do not update your virtual infrastructure to VMware vSphere 7.0.**
> vSphere 7.0 is currently not compatible with NETLAB+ since it cannot be used to connect to virtual machines and support the virtual infrastructure. The ESXi built-in VNC server has been removed from vSphere 7.0; therefore, it no longer supports connections to a virtual machine using NETLAB+'s built-in VNC web client.
>
> Please also note that **VMware vSphere 6.5 is not supported**.

VMware Product	VMware ESXi vCenter	VMware ESXi vCenter	VMware ESXi vCenter
VMware Major Version(s)	**6.7**	**6.0**	**5.1 U3**
NETLAB+ Support	**Supported, not documented***	**Recommended**	Deprecated
Minimum NETLAB+ Version		2015.R1.Final	2011.R2
Architecture		Bare Metal Hypervisor	Bare Metal Hypervisor
VMware Versions Tested by NDG		6.0	5.1
Host Operating System Required		No	No
vCenter Required		**Yes**	**Yes**

***Specifications and configuration guidance are not currently available for VMware vSphere 6.7.**

- VMware ESXi 6.0 is currently supported for **physical** host servers.
- VMware vCenter 6.0 appliance is currently supported for NETLAB+ VM management.

> ⚠️ If your system is currently using 5.1 U3, upgrading to ESXi 6.0 is advised.

2.2 NETLAB+ Feature Support

The following table compares NETLAB+ features that are supported with VMware virtualization.

NETLAB+ Features	VMware ESXi vCenter
VMware Major Version(s)	6.0
Remote PC Viewer	Yes
Power On / Off VM	Yes
Revert to Snapshot	Yes
Integration with VMware vCenter	Yes
VM Inventory	Yes
Linked Clones	Yes
Clone VM Pods and Individual VMs	Yes
Automatic Networking[1]	Yes
Automatic Remote Display Setup[2]	Yes
Delete Pod VMs and Individual VMs	Yes

[1] NETLAB+ will automatically setup networking on NDG standard pods.

[2] NETLAB+ will automatically program Remote Display parameters.

2.3   Virtual Machine Software Licenses

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

2.4   Obtaining VMware vSphere Software and Licenses for the NETLAB+ Infrastructure

Licensing considerations will vary, depending on your school's participation in the VMware IT Academy Program (VITA) program and/or the VMware Academic Subscription (VMAS) .

> Guidance on navigating licensing is available on the *VMware Product Licensing Through VMware Academic Subscription (VMAS)* chart.

Renewable licenses for your physical ESXi Host servers and vCenter Server are available from the VMware e-academy. Details on accessing the e-academy website can be found here: https://kivuto.com/solutions/institutions/vmware-academic-program-vmap/

Server	Software	Source
ESXi Hosts	VMware vSphere ESXi Server	VMware e-academy website
vCenter Server	VMware vCenter Appliance	VMware e-academy website

2.5   Networking Models

The NETLAB+ server, vCenter Server, and ESXi hosts may be *single-homed* or *dual-homed* depending on your requirements. This guide documents both common networking configurations:

- Single-Homed Networking
- Dual-Homed Networking

Please review each configuration to determine which one best suits your needs.

> The NETLAB+ server, the Management Server running vCenter server, and the ESXi hosts should be geographically co-located. If Single-Homed (outside) networking is used, all components should be connected by 1000Mb/s or higher speed LAN. NDG does not support split server configurations that traverse a WAN and/or configurations that place firewalls between these servers.

The following table describes the symbols and connection types denoted in the networking diagrams throughout this section.

Symbol	Connection Type
HTTP	HTTP Connection
PC	Remote PC Display User Connection
PCB	Remote PC Display Back Connection
MGT	VMware vSphere Management Connection
REQ	Real Equipment Traffic on VLANs
RDP	Remote Desktop Protocol

2.5.1 Single-Homed Networking

Single-homed networking (SH) connects one NIC from each server to a routable network on your campus. SH can be used if your pods contain only virtual machines (i.e., you are not hosting only real lab equipment). All traffic flows across the campus LAN.
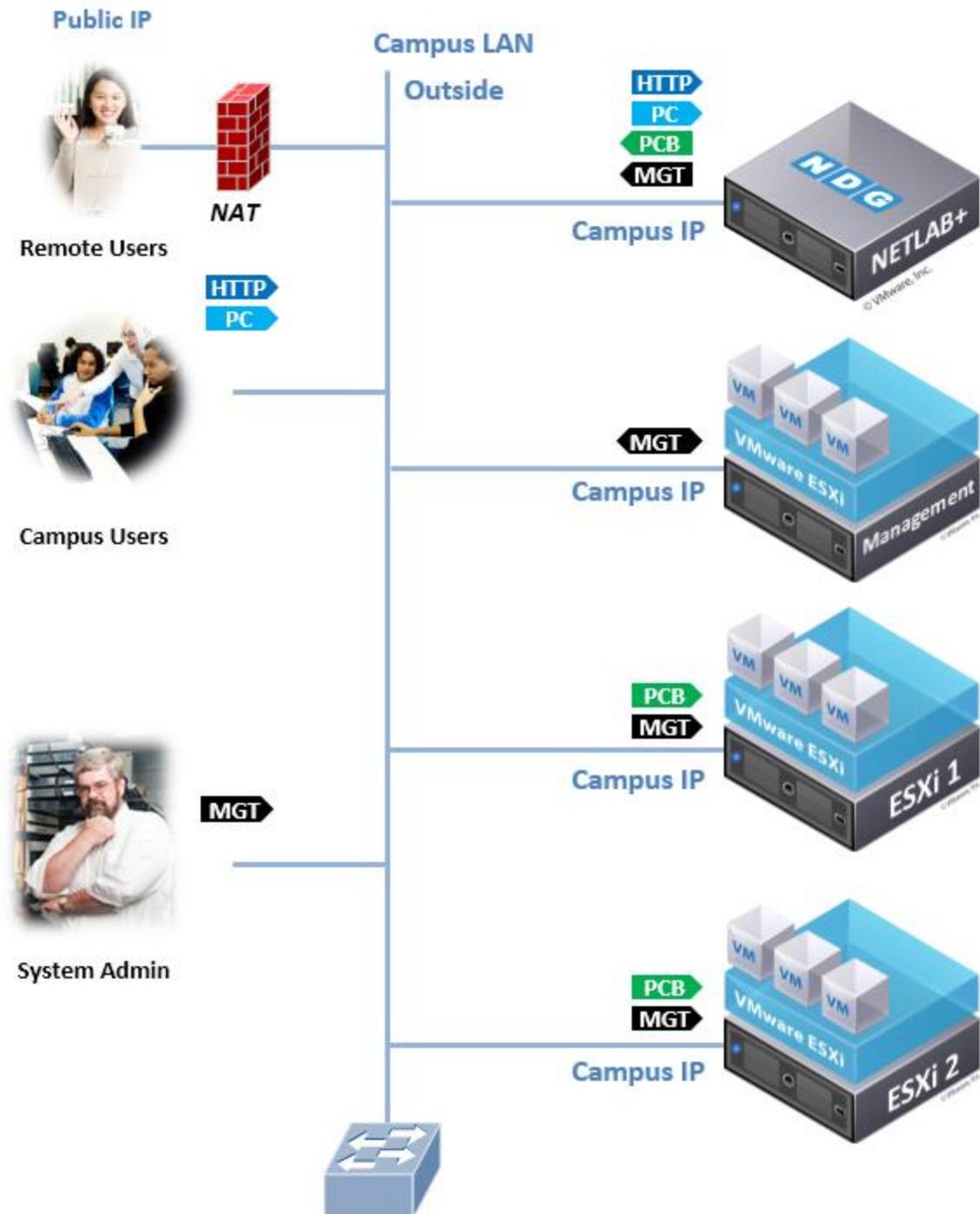
Single-Homed Networking does not require NETLAB+ control switches. A 1Gb/second switch port is highly recommended for each server connection. This will provide optimal bandwidth for remote display connections and virtual machine cloning operations between hosts.

If you have chosen single-homed networking, the following setup tasks can be performed now.

1. Obtain an IP address, subnet mask, and default gateway for each outside server interface connected to your campus LAN.
2. Connect the first Ethernet port of the Management Server to a Gigabit Ethernet port on your campus LAN.
3. Connect the first Ethernet port of each ESXi Host Server to a Gigabit Ethernet port on your campus LAN.

> ⚠ Remember, dual-homed is only necessary and required if you plan to use real physical lab devices, such as pods for the Cisco Networking Academy.

The IP addressing and DNS servers will be dictated by the model you select. The tables in this section are specific to Single-Homed Networking. Please fill out the table below to help assist you with configuration.

> 📝 It is strongly recommended that you print out your table in order to have it available for easy reference throughout the installation and configuration of your Virtual Machine Infrastructure as described in *Remote PC Guide Series - Volume 2, Installation*.

Single-Homed Model	
vCenter Outside IP Address	
ESXi Management Server Outside IP Address	
ESXi Host Server 1 Outside IP Address	
ESXi Host Server 2 Outside IP Address	
ESXi Host Server 3 Outside IP Address	
ESXi Host Server 4 Outside IP Address	
Subnet Mask	
Default Gateway	
Primary DNS Server	
Secondary DNS Server	

Later in the setup process, you will configure IP parameters for these interfaces. The following table shows key configurations parameters that will be implemented for this networking model.

	NETLAB+		vCenter Appliance		ESXi Management Server		ESXi Host 1 Server	
	Outside	Inside	Outside	Inside	Outside	Inside	Outside	Inside
IP Address	Campus		Campus		Campus		Campus	
Subnet Mask	Campus		Campus		Campus		Campus	
Gateway	Campus		Campus		Campus		Campus	
vSwitch			vSwitch0		vSwitch0		vSwitch0	
Management Path			*		*		*	

2.5.2   Dual-Homed Networking

Dual-homed networking (DH) can be used if you are hosting both virtual machines and real lab equipment in your NETLAB+ pods. In this environment, VLANs on NETLAB+ control switches serve as an "inside" communication path for virtual machine traffic between your ESXi host servers and real lab equipment.
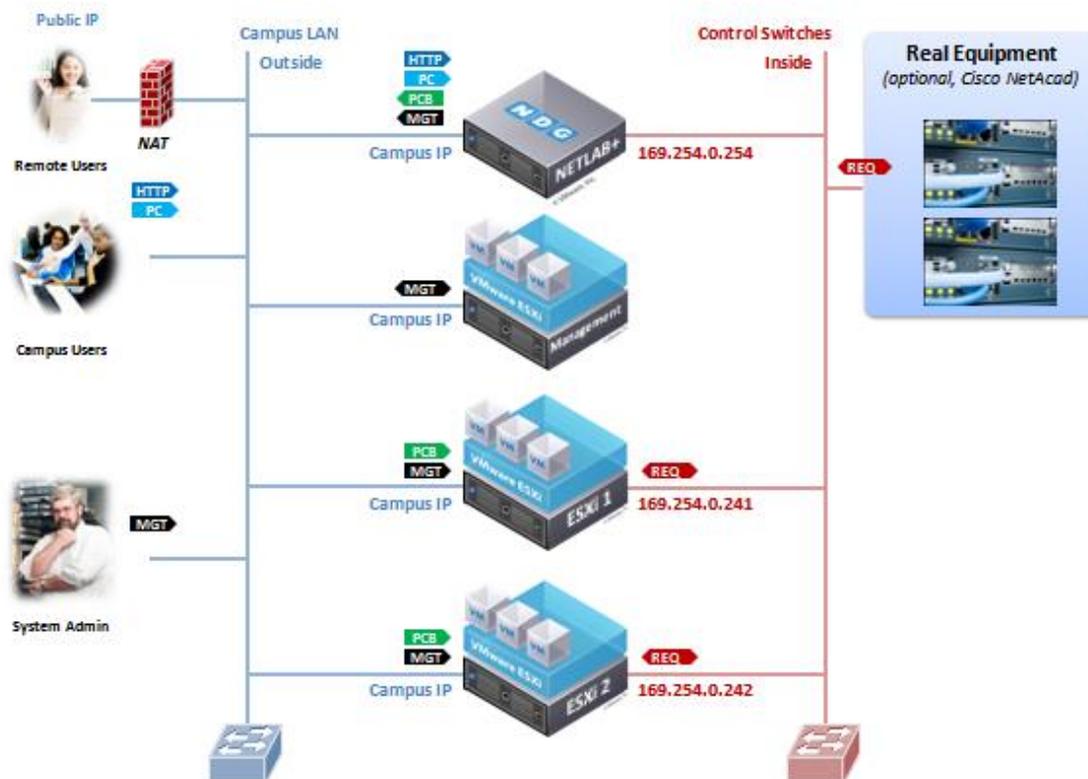
If you have chosen dual-homed as your networking model, the following setup tasks can be performed now.

1. Obtain an IP address, subnet mask, and default gateway for each outside server interface connected to your campus LAN.
4. Connect the first Ethernet port of the Management Server to a Gigabit Ethernet port on your campus LAN.
2. Connect each of your ESXi host servers:
   a. Connect the first Ethernet port of each ESXi host to a Gigabit Ethernet port on our campus LAN.
   b. Connect the second Ethernet port on your ESXi to a designated reserved port on a control switch, or a Gigabit Ethernet uplink port (if one is available). A Gigabit port will provide the highest bandwidth.

3. Console into the control switch and configure each inside ESXi host switchport as a trunk (NETLAB+ does not do this automatically).

```
interface FastEthernet0/n
  description inside connection to ESXi host #
  switchport mode trunk
  switchport mode nonegotiate
```

The IP addressing and DNS servers will be dictated by the model you select. The tables in this section are specific to Dual-Homed Networking. Please fill out the table below to help assist you with configuration.

> It is strongly recommended that you print out your table in order to have it available for easy reference throughout the installation and configuration of your Virtual Machine Infrastructure as described in *Remote PC Guide Series - Volume 2, Installation*.

Dual-Homed Model – Real Equipment Pods	
vCenter Outside IP Address	
ESXi Management Server Outside IP Address	
ESXi Host Server 1 Outside IP Address	
ESXi Host Server 1 Inside IP Address	169.254.0.241
ESXi Host Server 2 Outside IP Address	
ESXi Host Server 2 Inside IP Address	169.254.0.242
ESXi Host Server 3 Outside IP Address	
ESXi Host Server 3 Inside IP Address	169.254.0.243
ESXi Host Server 4 Outside IP Address	
ESXi Host Server 4 Inside IP Address	169.254.0.244
Outside Subnet Mask	
Inside Subnet Mask	255.255.255.0
Outside Default Gateway	
Inside Default Gateway	None
Primary DNS Server	
Secondary DNS Server	

Later in the setup process, you will configure virtual switches, VM kernel ports, and IP addresses for interfaces. The following table shows the key configuration parameters that will be implemented for this networking model.

	NETLAB+		vCenter Appliance		ESXi Host 1		ESXi Host 2	
	Outside	**Inside**	**Outside**	**Inside**	**Outside**	**Inside**	**Outside**	**Inside**
IP Address	Campus	169.254.0.254	Campus		Campus	169.254.0.241	Campus	169.254.0.242
Subnet Mask	Campus	255.255.255.0	Campus		Campus	255.255.255.0	Campus	255.255.255.0
Gateway	Campus	not set	Campus		Campus	not set	Campus	not set
vSwitch			vSwitch0		vSwitch0	vSwitch1	vSwitch0	vSwitch1
Management Path			*		*		*	

2.5.3   Outside vs. Inside Connection

Outside ESXi Connection. Your ESXi host connects to the outside campus LAN. Enter the IP address, subnet mask, and default gateway assigned by the campus LAN administrator.

Single-Homed Networking
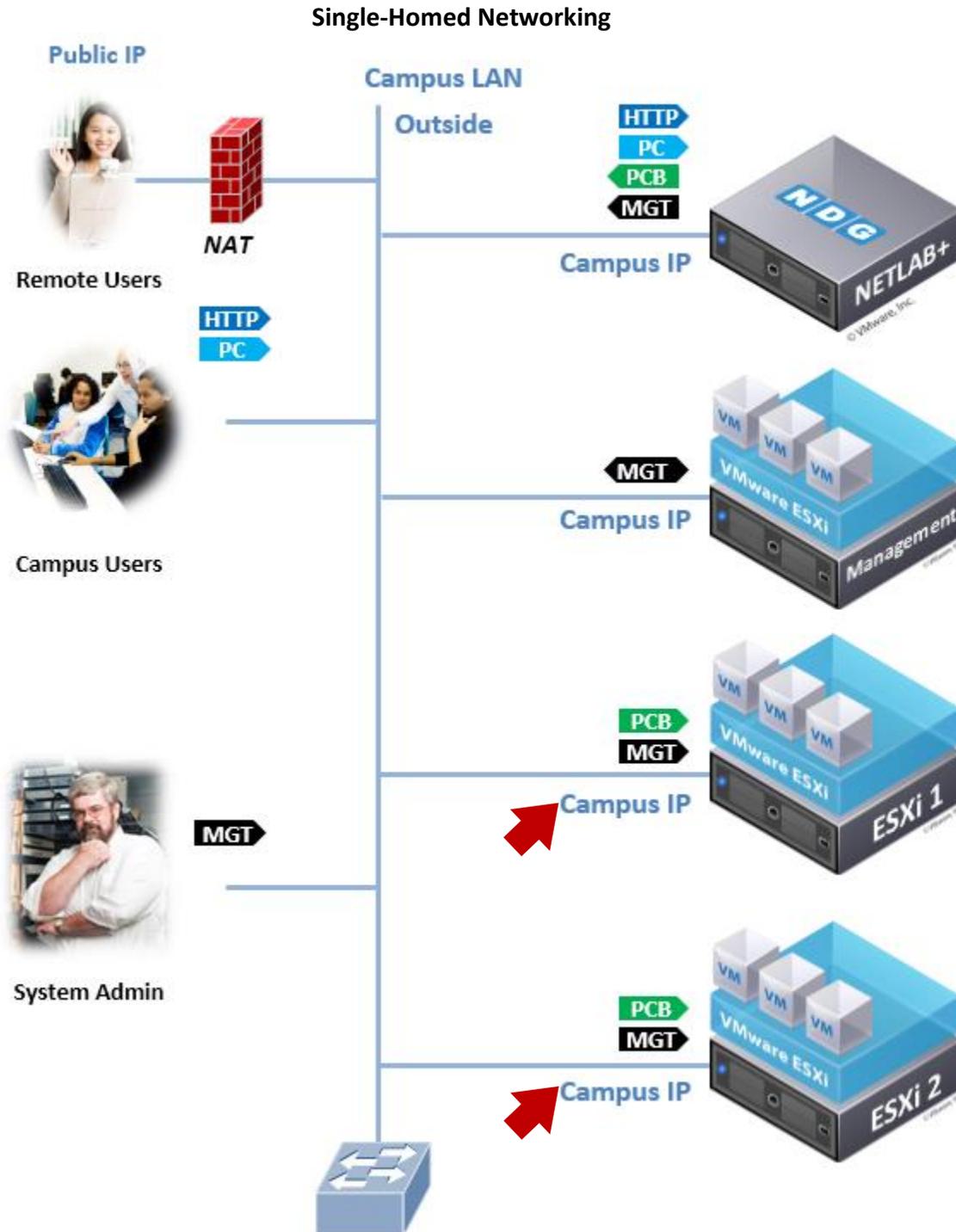
Dual-Homed Networking
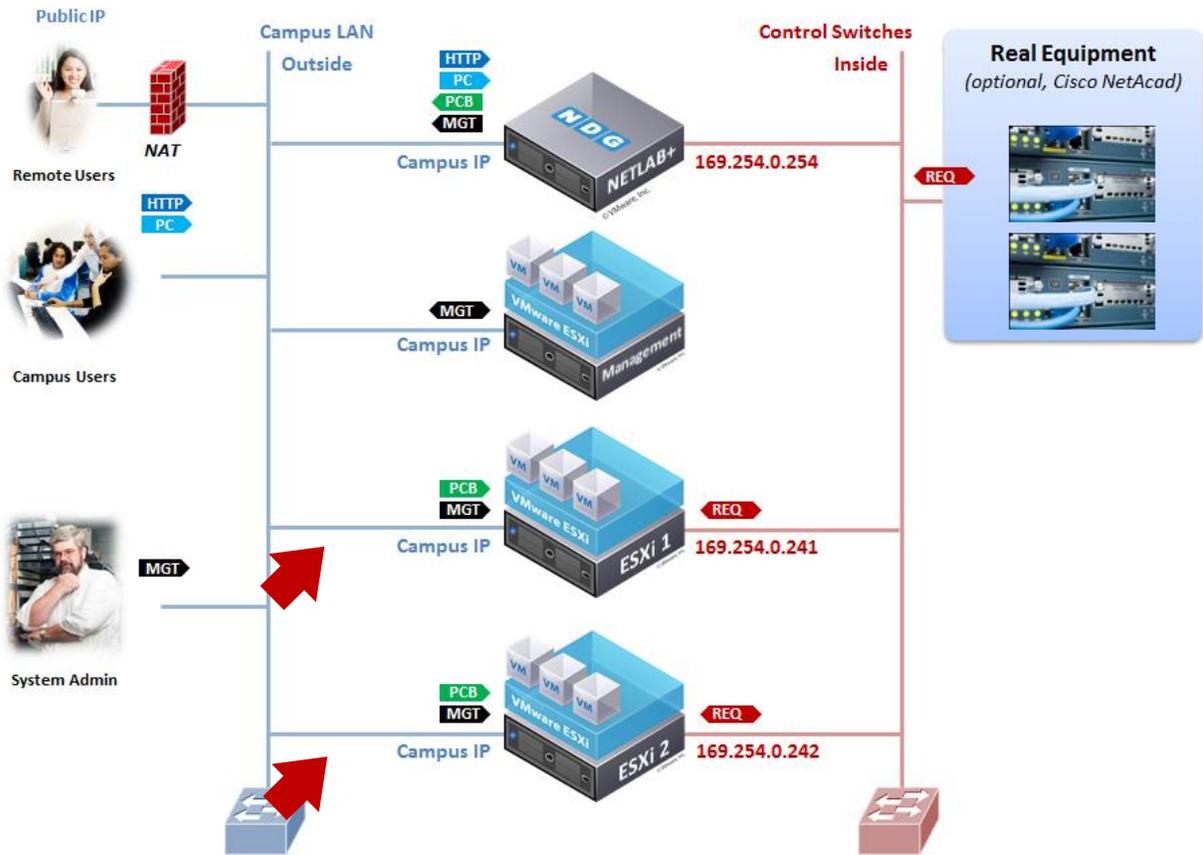
Inside ESXi Connection ONLY. Use one of the following IP configurations for each ESXi server that will have connectivity to real equipment.

Inside Interface	IP Address	Subnet Mask	Default Gateway
ESXi Server 1 Inside	169.254.0.241	255.255.255.0	not set
ESXi Server 2 Inside	169.254.0.242	255.255.255.0	not set
ESXi Server 3 Inside	169.254.0.243	255.255.255.0	not set
ESXi Server 4 Inside	169.254.0.244	255.255.255.0	not set
ESXi Server 5 Inside	169.254.0.245	255.255.255.0	not set
ESXi Server 6 Inside	169.254.0.246	255.255.255.0	not set
ESXi Server 7 Inside	169.254.0.247	255.255.255.0	not set
ESXi Server 8 Inside	169.254.0.248	255.255.255.0	not set
ESXi Server 9 Inside	169.254.0.249	255.255.255.0	not set

Dual-Homed Networking
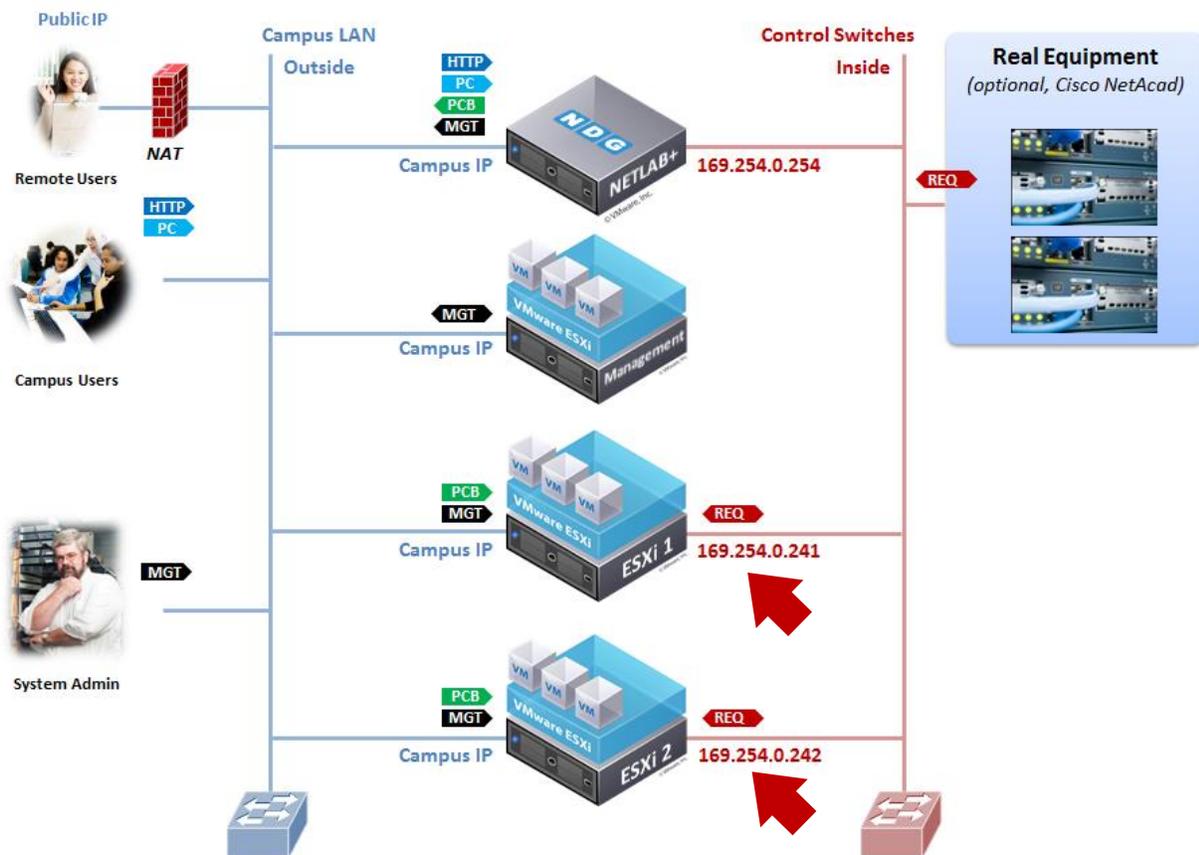
3   Storage Area Networks

A storage area network (SAN) provides centralized shared storage for virtual machines and data. Sharing storage usually simplifies storage administration and adds flexibility since virtual machines can be migrated from one ESXi host to another without copying large files.

NDG performs all testing on servers with Internal Direct Attached Storage (i.e., RAID arrays and RAID controllers directly attached to each). This is the configuration that most academic institutions are likely to find affordable and adopt.

A Storage Area Network (SAN) is a dedicated network that provides access to consolidated, block-level data storage that can be used for disk storage in a VMware vSphere environment.

Currently, NDG does not provide benchmarks, guidance, or troubleshooting for SAN configurations. Our documentation may show an optional SAN in the environment; however, this is not a recommendation or requirement to deploy a SAN.

NDG benchmarks and capacity planning guidance do not account for the additional latencies introduced by SAN.

- When compared to Direct Attached Storage, a SAN may introduce additional I/O latency between ESXi server and disk. Therefore, a SAN may reduce the number of active VMs you can run on an ESXi host.
- If you deploy a SAN, you should perform your own benchmarks and determine the number of active VMs you can host on your ESXi server. Your mileage may vary.
- Always configure NETLAB+ Proactive Resource Awareness to ensure that the number of VMs that can be activated will remain within your predetermined performance limits.

Deployment of a SAN requires skill and planning. Performance of SAN solutions can vary greatly. NDG performance benchmarks are based on Direct Attached Storage (local disks connected to each ESXi hosts). Free SAN solutions may be attractive, but test results show I/O rates that are half or less than directly attached SATA or SAS drives attached to the ESXi hosts.