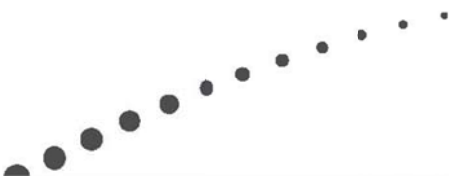




Citrix XenServer Design: Introduction to XenServer Networking

www.citrix.com





Contents

- About..... 4
 - Purpose of the Guide 4
 - Audience..... 5
 - Finding Configuration Instructions..... 5
 - Visual Legend 6
 - Additional Terminology 7
- Chapter 1: Introduction 8
- Chapter 2: Basic XenServer Networking Concepts..... 10
 - Introduction to XenServer Networking 10
 - Connecting Virtual Machines to Networks..... 11
 - Networking Configuration after Installation..... 13
 - Impact of Pools on XenServer Networking 14
 - Sequence of Networking Configuration Tasks..... 17
 - Cabling Configuration for XenServer 17
 - Connecting XenServer to Physical Switches 20
- Chapter 3: Sample Networking Scenario 22
 - Example: Adding Virtual Machines to a Network..... 22
 - Creating Network Resiliency through Bonds..... 23
 - Connecting a VM to a Network using Virtual Interfaces..... 25
 - Segregating VM Traffic from Management and Storage Traffic..... 27
 - Scenario 1: Segregating Traffic..... 28
 - Scenario 2: Using the Management Network for VM Traffic..... 29
 - Scenario 3: Isolating VM Traffic on a Private Network..... 30
 - Scenario 4: Connecting VMs to Multiple Linked VLANs 32



Version History.....38

About

This guide helps you understand XenServer networking and design a networking configuration for XenServer environments. It includes the following topics:

- The correct sequence in which to configure XenServer networking
- Guidance about cabling XenServer hosts and connecting them to physical switches
- How XenServer networking behaves in a pool
- An overview of basic networking concepts, including bonds and the primary management interface

Purpose of the Guide

This guide uses a scenario-based approach to explain basic XenServer networking concepts. Learning XenServer networking concepts provides the foundation for understanding networking design and best practices.

Since this guide is meant to help you achieve a high-level understanding of networking, it does not include in-depth information about networking features, such as quality of service or bonding. Likewise, this guide generally does not provide configuration instructions except as needed to clarify concepts.

This guide assumes the most common method of managing XenServer is through XenCenter, so it typically refers to XenCenter. However, it does provide CLI commands as well in some cases. However, because this is a concepts guide, it is assumed you will find instructions in the administrative documentation, as described in “Finding Configuration Instructions” on page 5.



Audience

Before reading this guide, you should have a basic knowledge of physical networking and, ideally, the physical network infrastructure in your environment. This guide has several audiences:

- **Application Administrators.** XenApp and XenDesktop administrators who are implementing a virtualization solution to virtualize Citrix products, IT infrastructure, or other applications they manage.
- **Systems Architects.** Systems architects who are designing a virtualized environment.
- **Infrastructure Engineers and Network Administrators.** Networking and storage professionals who configure storage or manage the Layer 2 network infrastructure in their organizations.

This guide assumes that you are familiar with basic XenServer concepts, including XenServer installation, XenCenter, resource pools, and the pool master.







Finding Configuration Instructions


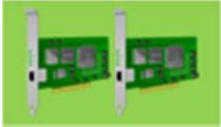
You can find networking configuration instructions in the following locations:

- **XenCenter Help.** The XenCenter help provides UI-based step-by-step instructions using XenCenter, the XenServer UI-based administration console. Users who are not comfortable with the XenServer `xe` CLI commands, may prefer this option.
- **XenServer Administrator's Guide.** The *XenServer Administrator's Guide* provides command-line based instructions for performing networking tasks. For integrators, it also provides information about XenServer networking from the object-model perspective.

Visual Legend

This guide relies heavily on diagrams to explain key concepts. These diagrams use the following icons:

Icon	Meaning
	<p>Virtual Machine (VM). A virtual computer that runs on the XenServer host.</p>
	<p>Virtual Interface. On VMs, the logical interface that appears and functions like a NIC is known as a virtual interface. A virtual interface lets VMs send and receive network traffic. Some product literature refers to virtual interfaces as VIFs and virtual NICs.</p>
	<p>Network. A network is the virtual network switching fabric built into XenServer that lets you connect your virtual machines. It links the physical NICs to the virtual interfaces and connects the virtual interfaces together.</p>
	<p>Host. A XenServer host is the physical computer on which XenServer runs.</p>
	<p>NIC. The physical network interface card (NIC) in a host.</p>
	<p>Pool. A XenServer resource pool is a connected group of up to 16 hosts which, combined with shared storage, provides a platform to run virtual machines.</p> <p>To join hosts to a pool, they require broadly compatible hardware and should be running the same XenServer version and patches.</p> <p>Pools comprise a pool master and subordinate servers known as pool members (sometimes also referred to as "slaves"). The pool master</p>

	<p>provides a single point of contact for all the servers in the pool and the master will forward commands to individual pool members as necessary.</p>
	<p>Physical Switch. The device on a physical network that connects network segments together.</p> <p>This guide presents physical switches either as a three-dimensional physical box or as a one-dimensional panel with ports.</p>
	<p>NIC Bond. In this guide, enclosing NICs in green represents a bond.</p> <p>A NIC bond is a pair of NICs configured so they logically function as one network card. NIC bonding is also known as <i>NIC teaming</i>.</p>

Additional Terminology

These terms appear in the sections that follow:

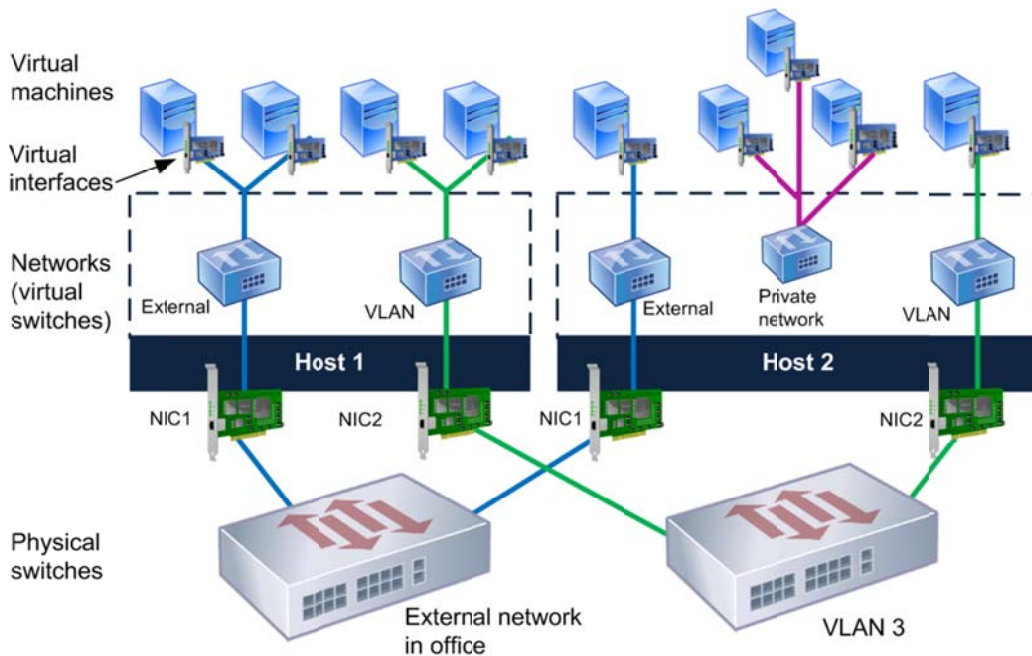
Primary Management Interface. The primary management interface is a NIC assigned an IP address that XenServer uses for its management network, including, but not limited to, traffic between hosts, between a host and Workload Balancing and for live migration.

VM traffic. The traffic going to or from a VM. This traffic may be from the VM's guest operating system or data users send to the application on the VM. VM traffic refers to the standard network traffic that was in your environment before you virtualized servers and their applications. This is sometimes referred to as guest traffic or VM/guest traffic.

Chapter 1: Introduction

This documentation explains basic networking concepts and their application by using a series of scenarios to illustrate the concepts. The scenarios begin immediately after installation and end with connecting a VM to a network.

These sample scenarios focus on three different types of networks: External Networks, VLANs, and single-server private networks. If you configured the scenarios demonstrated in this guide, by the time you finished, you would create a deployment that looked like the following illustration.



This illustration shows how virtual machines connect to three different types of networks: an external network, a VLAN network, and a single-server private network.



This guide explains these types of networks by providing the following information:

Chapter 2 introduces XenServer networking and explains how to prepare for XenServer networking configuration by configuring the physical infrastructure and hardware layers in your environment, including the correct sequence for physically configuring networking. The chapter also discusses the effect pooling XenServer hosts has on networking and describes the networking configuration after installation.

Chapter 3 provides several sample scenarios that illustrate how to add virtual machines to a network. The first scenario guides you through the process of segregating different types of traffic, including storage and management traffic. The second scenario gives you an alternative to dedicating NICs to specific types of traffic; it shows an example of using the management network for management and VM traffic. The third scenario shows an example of how to segregate traffic by creating a single-server private network on a host.

If you want to review XenServer networking concepts before reading this information, see the “Visual Legend” on page 6.

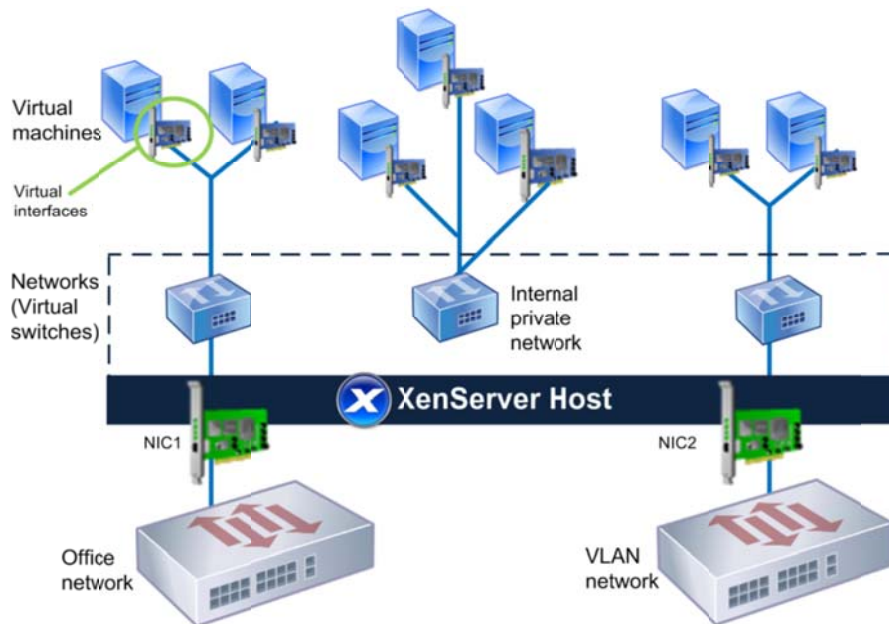
Chapter 2: Basic XenServer Networking Concepts

This chapter includes the following topics:

- An introduction to XenServer networking
- The network settings created during installation

Introduction to XenServer Networking

XenServer provides virtual networking features that let you build networks for your virtual machines the same way you build networks for physical machines.



The VMs connect to three different types of networks: an office network, an internal private network, and a VLAN.

You can connect virtual machines to your production network like you connect physical machines or build private networks within a host or pool for testing, development, or security purposes. You can connect virtual machines to your VLAN networks using standard VLAN configurations.

The most important networking components XenServer lets you configure are *virtual interfaces* and *networks*:

- **Virtual interfaces.** Virtual machines connect to networks using virtual NICs, known as virtual interfaces. Virtual interfaces let VMs send and receive network traffic. You can assign each virtual interface its own IP address and MAC address. Some product literature refers to virtual interfaces as *VIFs* and *virtual NICs*.
- **Networks.** XenServer has an internal virtual switch, known as a network, that lets virtual machines on a XenServer host communicate with each other using the same networking protocols that are used on physical networks.

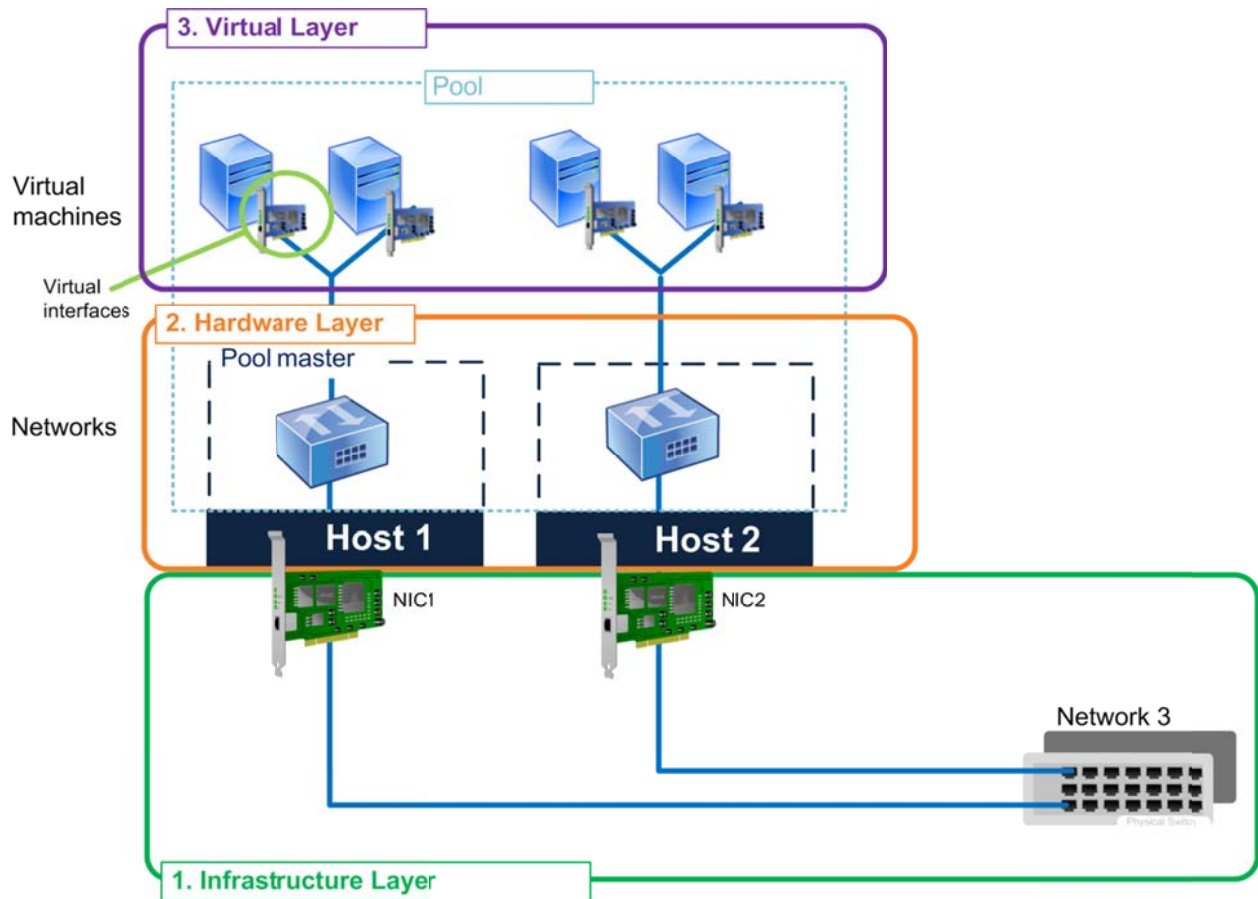
A network is the logical network switching fabric built into XenServer that lets you network your virtual machines. It links the physical NICs to the virtual interfaces and connects the virtual interfaces together. These networks are virtual switches that behave as regular L2 learning switches. Some vendors' virtualization products refer to networks as *virtual switches* or *bridges*.

Connecting Virtual Machines to Networks

When you are configuring network connectivity on XenServer hosts, your ultimate goal is to connect the VMs to a network. To do this:

1. Connect the host to a physical network. (For VMs without external network connectivity, you would configure a private network instead.)
2. Connect the VM by creating a Virtual Interface for it and connecting the Virtual Interface to a network. As shown in the illustration on page 10, the virtual interfaces on the VMs connect to networks in a host and then connect to a physical network through the host's NIC.

One way to think about these tasks is that you need to configure connectivity at both the hardware and virtual layers as shown in the illustration that follows.



This illustration shows the order in which you should configure networking in your virtual environment: (1) Start on the physical infrastructure layer, which means connecting NICs to switches; (2) configure the hardware layer, which means connecting hosts to networks and configuring these networks; (3) configure the virtual layer, which means attaching VMs to networks through virtual interfaces.

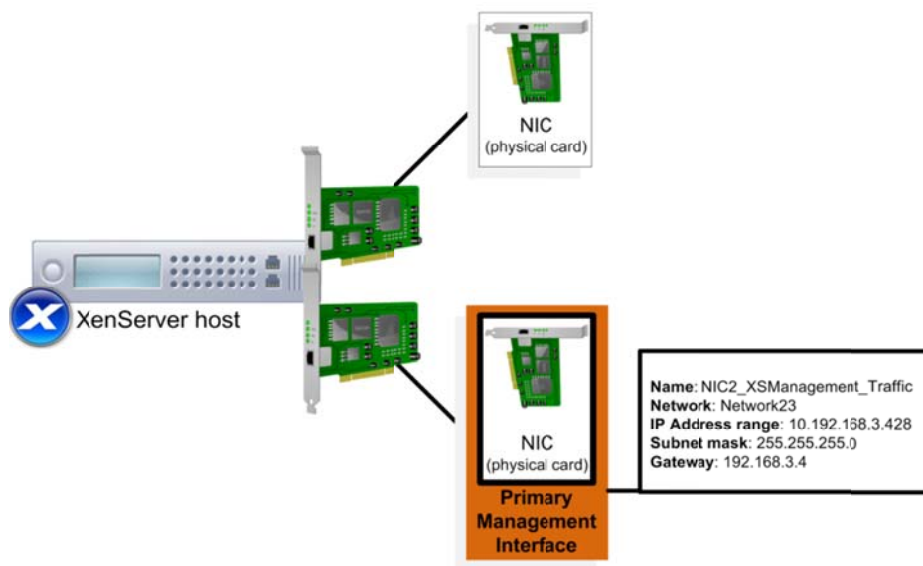
Important: Configuring networking in the order listed described in “Sequence of Networking Configuration Tasks” on page 17 is critical. If you vary from this sequence, the primary management interface may not be configured correctly on each host. If this occurs, all VMs in the pool may start on the pool master and not their home or optimal servers.

Networking Configuration after Installation

After installation, the XenServer *host* has all the information it needs to connect to at least one of your external networks. This is because you define the following networking options while installing XenServer:

- IP Address Configuration and Other Settings.** You set the host's initial XenServer networking configuration when you first install XenServer on the physical computer. XenServer Setup configures options, such as the IP address configuration (DHCP/static), based on the values you provide during installation.
- Network Connectivity.** XenServer installation prepares each NIC connected to a switch for network connectivity by creating one network for each NIC. This means that if the host has, for example, three NICs, XenServer creates three networks: Network 0, Network 1, Network 2. For a visual explanation, see page 14.
- Primary Management Interface and the Management Network.** During XenServer Setup, you specify an IP address for one NIC. XenServer uses that NIC to connect to your organization's network and to carry management traffic for functions like communicating with other hosts in a pool, XenCenter, Workload Balancing, and other components. This NIC is known as the *primary management interface*. This is the only NIC that Setup configures with an IP address.

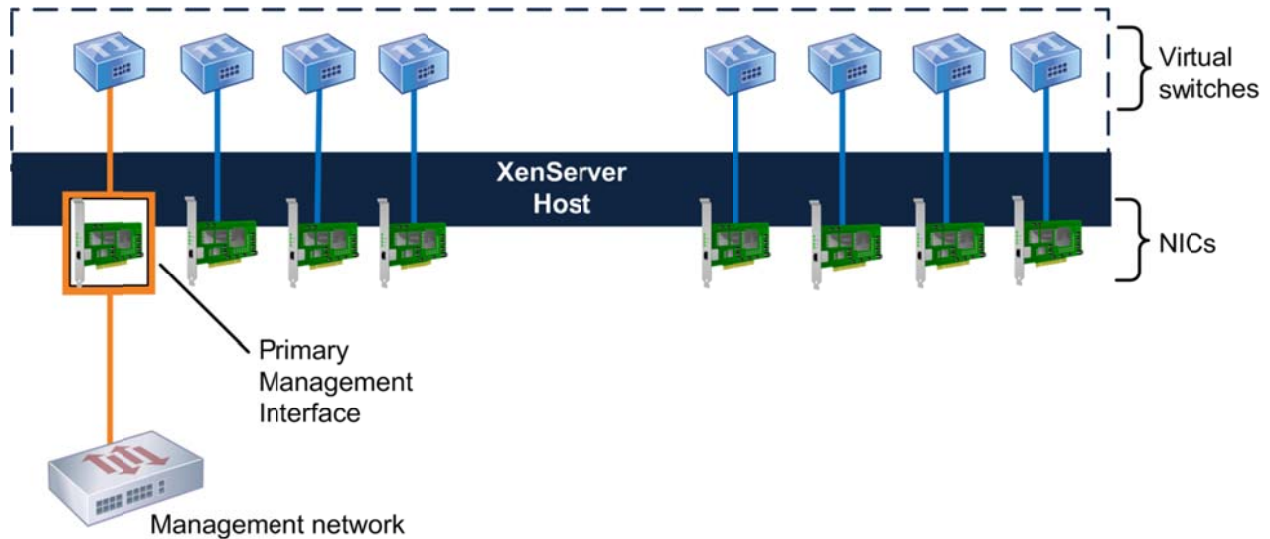
The illustration that follows shows a regular (unconfigured) NIC and a NIC configured as a primary management interface.



This illustration contrasts a regular NIC with one configured as the primary management interface. The primary management interface has an IP address, subnet mask, and gateway assigned to it.

During installation, XenServer also creates a separate network for each NIC it detects on the host. Unless you change this set up, XenServer uses the additional NICs on the host for VM traffic only.

The illustration that follows shows an example of XenServer’s initial network configuration following installation.



This illustration shows how, during installation, XenServer lets you choose a NIC as the primary management interface. In this case, the administrator selected NIC0. XenServer uses the other NICs for VM traffic.

Most environments require additional configurations to these basic network settings. These can range from creating pools to integrating additional networks, connecting your VMs to those networks, and configuring a separate storage network. The scenarios in the following chapter provide examples of these tasks.

Note: If you plug any NICs into switches after installing XenServer, if you cannot see the NICs in XenCenter or xsconsole, you might need to either a) run `xe pif-list` or `xe pif-plug` in the CLI or reboot the XenServer host.

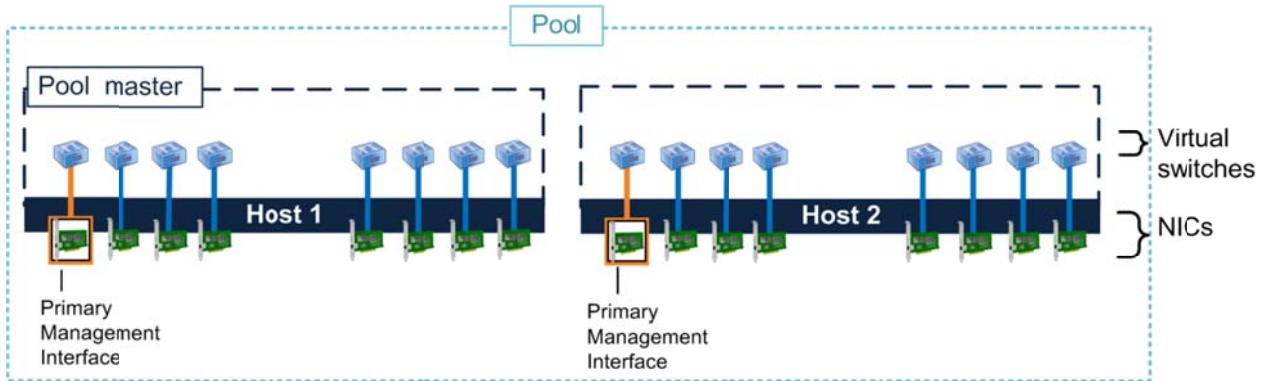
Impact of Pools on XenServer Networking

Networking is a pool-level feature in XenServer. When you change networking on the pool master, XenServer synchronizes all hosts in a pool to use the same network settings.

As a result, for XenServer to operate correctly, you must ensure that network settings match across all hosts in the pool, including:

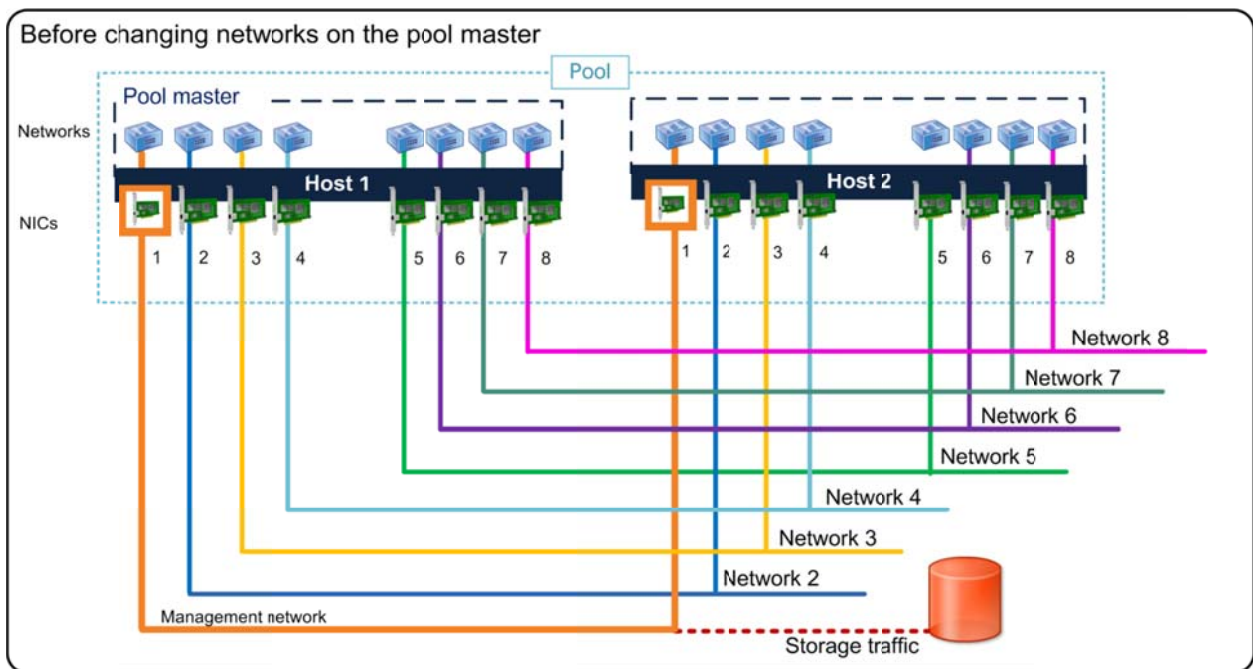
- Which NICs are bonded
- Which NICs are configured as the primary management interface
- Which NICs connect to storage

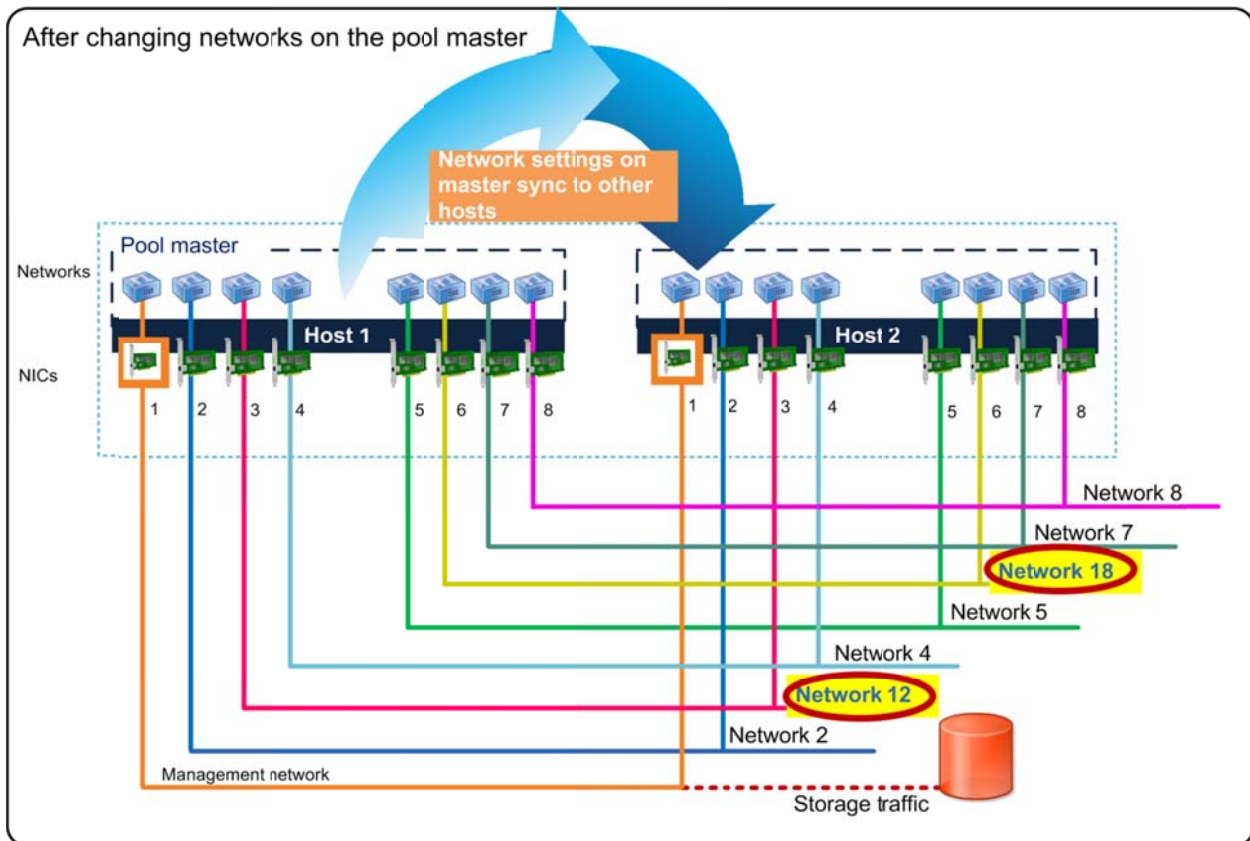
The networks to which NICs connect must be the same on the corresponding NICs on each host in the pool.



This illustration shows two hosts joined together in a pool before any networking configuration is performed on them.

Ideally, you should add all desired hosts to the pool before configuring any network settings. Pooling the hosts before configuring networking creates cleaner records in XenServer’s internal networking-configuration database.





These two illustrations show how XenServer replicates the network settings created on the pool master on all other hosts in the pool. In the top illustration, NICs 3 and 6 on both hosts use Networks 3 and 6. In the bottom illustration, after reconfiguring NIC 3 on the pool master to use Network 12 and NIC 6 to use Network 18, XenCenter automatically configures the other host in the pool to use those settings.

After creating a new pool or joining a host to an existing pool, XenServer automatically replicates the network settings on the master to the joining hosts.

When you use XenCenter to make networking changes, XenCenter changes the other hosts to match the newly modified host. When you use the CLI to change network settings, you must either:

- Change each host manually to match the modified host's settings
- Make the change on the pool master and restart all the member hosts in the pool

XenServer requires network settings to match across the pool because of features that use live migration, such as XenMotion, High Availability, and Workload Balancing. These features enable the physical server hosting a VM to change at any time, and possibly automatically without your intervention. Therefore, the VMs must be able to access all of their target networks regardless of which host XenServer moves them on to.



For this reason, it is critical to have *and maintain* an identical physical cabling, NIC, and switch configuration for each host across the pool. Likewise, Citrix strongly recommends changing the physical configuration on all hosts in a pool before changing network settings on each host.

Important: After joining the hosts to the pool, check the primary management interface on each member host to make sure that it has its own unique IP address and/or set the correct static IP address.

Sequence of Networking Configuration Tasks

Citrix recommends performing your initial networking configuration in the sequence that follows to help ensure XenServer stores your networking configuration correctly:

1. Cable the hosts by plugging all NICs into the appropriate switches, as described in “Cabling Configuration for XenServer” on page 17.
2. Configure the switches. See “Connecting XenServer to Physical Switches” on page 20.
3. Install XenServer on the hosts.
4. Create a pool of the hosts, if you want to pool them. See “Impact of Pools on XenServer Networking” on page 14.
5. Configure NIC bonds and networks. For more information, see the scenarios in “Chapter 3: Sample Networking Scenario.”

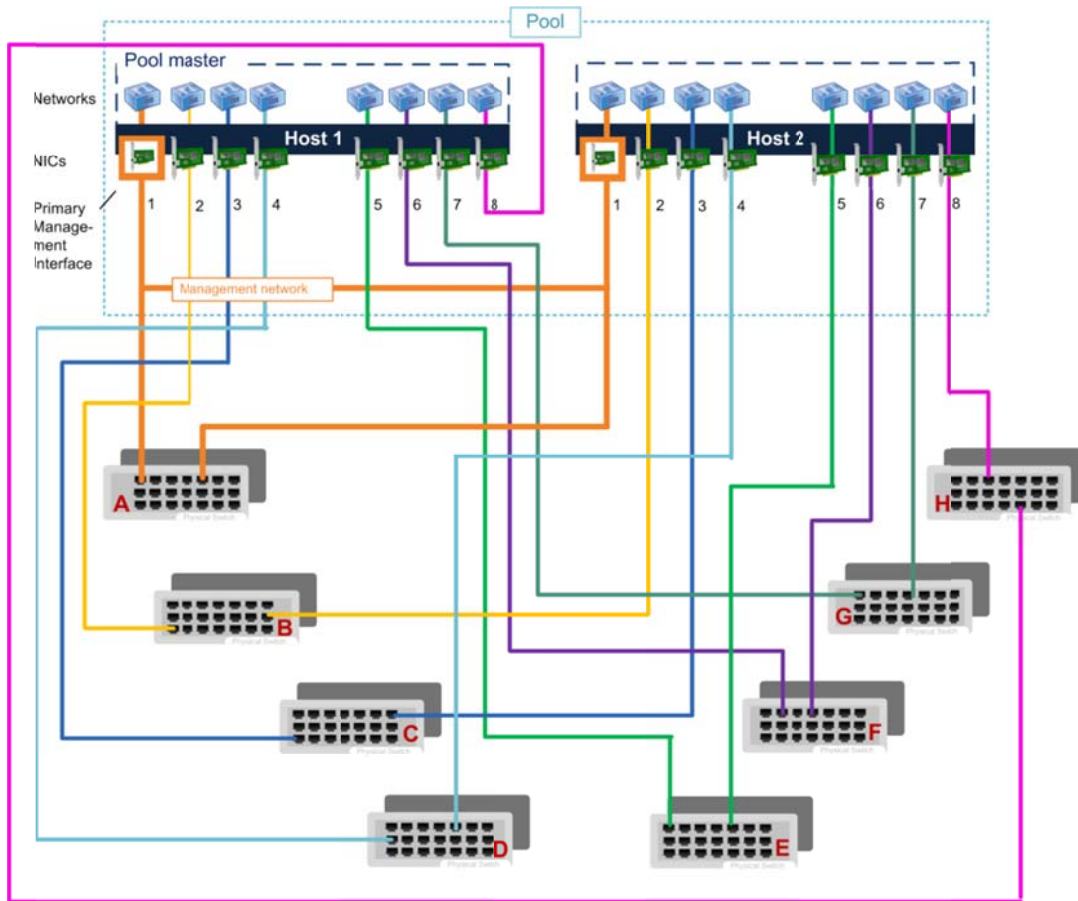
Cabling Configuration for XenServer

Citrix recommends plugging the physical Ethernet cables into all the NICs and the appropriate switches **before** installing XenServer. The ideal process is as follows:

1. If you did not cable your hosts before installation, plug all the NICs in each host in the pool into the appropriate switch ports.
2. Connect the corresponding NICs on each host in the pool to the same physical switch (that is, the same subnet).

The term *corresponding* refers to the NIC of the same number on another host. For example, NIC 3 on Host 1, NIC 3 on Host 2, NIC 3 on Host 3. This means that each individual NIC on every host must connect to the same physical network as the NIC in the same position on all other hosts in the pool.

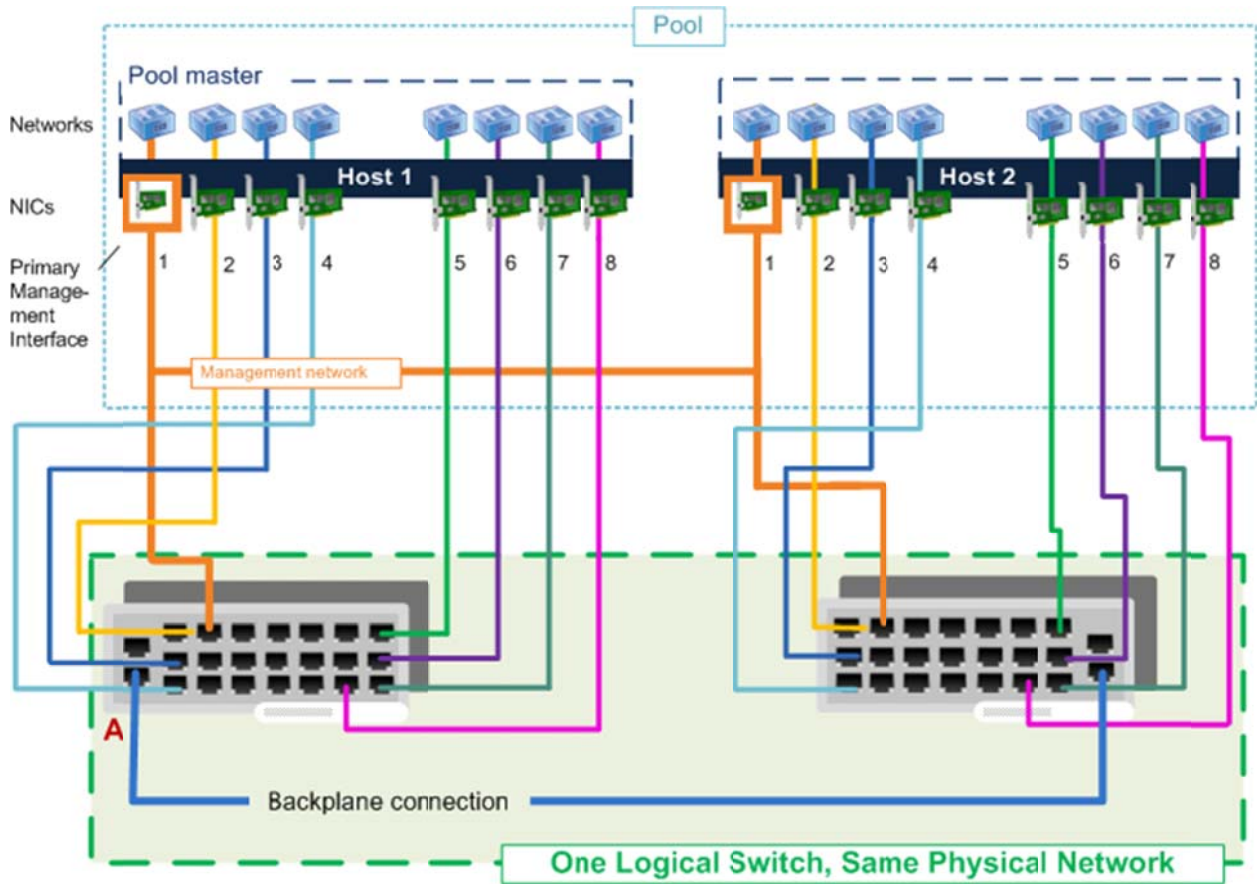
The following figure is a visual example of this configuration in an enterprise environment.



This illustration shows how each corresponding NIC on both hosts must physically connect to the same network. Each switch represents a separate physical network. Each member host's NICs must be connected to the same physical networks as the corresponding NICs on the pool master.

Ensuring the cabling on each host in the pool is correct is critical. As shown in the previous illustration, all NICs must connect to the same physical networks (shown as separate switches) as the NICs in the same position on all hosts across the pool.

In an environment with only one logical switch (for example, one that has a hierarchy of switches that form one large physical network), you only need to connect the NICs to switches on that network that have the same physical or logical (VLAN) connectivity. The example that follows shows how you might cable such an environment.



This illustration shows two switches that are connected across a backplane and are on the same physical network. These switches function logically as one unit. Because there are no VLANs configured on any of the ports and all ports have the same connectivity, the NICs can be plugged into any port on these two switches.

XenServer cannot detect if you make any errors while setting up the physical network. For example, if a XenServer host expects to be able to contact a specific gateway using a certain NIC, XenServer cannot indicate the cabling is incorrect. If you receive errors, they might not indicate network configuration as the cause.

Ensuring that the corresponding NIC on each host has the same network configuration is what ensures that a host's VM attached to, for example, Network 1, can communicate with a VM attached to Network 1 on another host. This ensures that if you migrate a VM to a new host, the VM retains the same physical connectivity after migration.

Note: When you configure networking, if you do not have all of your NICs plugged in to switches, you must have, at a minimum, the NIC(s) for the primary management interface on all hosts in your pool plugged into your network. Otherwise, the pool master cannot synchronize its network settings to the member hosts. Likewise, if you are using a dedicated NIC for storage, you must also connect the cables for that NIC on each host.

Connecting XenServer to Physical Switches

When connecting a XenServer host to a switch, you must configure the switch's ports differently than you would when connecting a workstation to a switch. There are specific, critical guidelines about the Spanning Tree Protocol (STP) and enabling PortFast. PortFast lets a switch port running Spanning Tree Protocol (STP) go directly from blocking to forwarding mode; skipping learning and listening.

To connect XenServer hosts to switch ports

When connecting XenServer hosts to switch ports, change the following:

1. Enable PortFast on the ports that you are plugging in XenServer hosts. However, note the following:
 - PortFast should only be enabled on ports connected to a single host.
 - The port you plugging XenServer into cannot be a trunk port and the port must be in access mode.
 - Ports used for storage should have PortFast enabled.
2. Disable port security on the ports that you are plugging in XenServer hosts.

Port security prevents multiple MACs from being presented to the same port. In a virtual environment, VMs present multiple MACs to the same port causing your port to shut down if you have port security enabled.

3. Disable the Spanning Tree Protocol on the ports that you are plugging in XenServer hosts.

If you are bonding NICs, you should disable the Spanning Tree Protocol to avoid failover delay issues.

4. If using a Cisco switch, disable the PortFast Bridge Protocol Data Unit (BPDU) guard feature on the ports that you are plugging in XenServer hosts.

The BPDU guard is a protection setting in the Spanning Tree Protocol that prevents you from attaching a network device to a switch port. When you attach a network device with the guard enabled, the port shuts down and an administrator must re-enable it.

Note: When PortFast port receives BPDUs, the reception indicates another bridge is somehow connected to the port, and it means that there is a possibility of a bridging loop forming during the Listening and Learning phases. In a valid PortFast configuration, configuration BPDUs should never be received. As a result, Cisco switches support a feature called PortFast BPDU guard, which is a feature that shuts down a PortFast-enabled port in the event a BPDU is received. This feature ensures that a bridging loop cannot form because the switch shuts down the port.



5. Change port speed settings to Static if using a 10/100 switch.

Connecting to a 100 MBP/s port set the PIF speeds to 100 MBPs static with full duplex.

Note: You do not need to change speed or duplex settings when connecting to 1GB switches.

Note: This topic was based on and enhanced from CTX123158 -- [Considerations for XenServer Switch Ports](#).

Chapter 3: Sample Networking Scenario

This chapter provides a scenario-based example of how to connect virtual machines to a physical network. This includes the following:

- Segregating traffic
- Using the management network for traffic in a very small environment

Example: Adding Virtual Machines to a Network

This section provides a sample scenario of a simple networking configuration that includes connecting VMs to networks, creating redundancy, and configuring NICs.

Designing a XenServer networking deployment may require several tasks, including, for example, configuring redundancy for network availability, configuring NICs, and, ultimately, connecting VMs to the desired networks. During this process, you might also separate different types of traffic for security or performance reasons (for example, separating traffic for managing the XenServer platform from VM traffic).

Before configuring networking on a pool, you should know to which networks your VMs will need to connect. A standard network configuration process might require:

1. Configuring redundancy for network availability.
2. Creating separate storage or management networks (used to separate management or storage traffic from VM traffic).
3. Creating VMs and connecting them to the desired XenServer network(s).

This section provides you with an example of that process. This section describes the different configuration options and steps required to put your virtual machines on the network by using a

sample scenario. While the scenario might not directly apply to your environment, it is designed to put XenServer’s networking features into context.

Creating Network Resiliency through Bonds

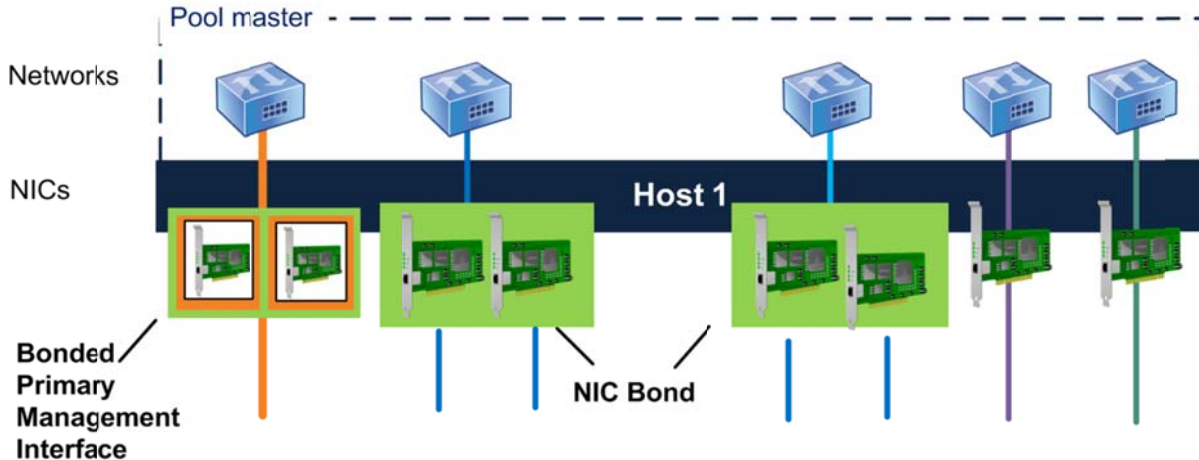
After joining all hosts to your pool, you may want to ensure that any critical servers have high availability access to the network. One way XenServer lets you achieve high network availability is to create redundancy through *NIC bonding*.

NIC bonding is a technique for increasing resiliency and/or bandwidth in which an administrator configures two NICs together so they logically function as one network card. Both NICs have the same MAC address and, in the case of management interfaces, have one IP address.

XenServer supports *bonding* two NICs together on a host. If one NIC in the bond fails, XenServer automatically redirects traffic to the second NIC. NIC bonding is also sometimes known as *NIC teaming*.

You can use XenCenter or the xe CLI to create NIC bonds. If XenCenter is managing a pool, XenServer automatically replicates the bonding configuration across all hosts in the pool.

In the illustration that follows, the primary management interface is bonded with a NIC so that it forms a bonded pair of NICs. XenServer will use this bond for management traffic.



This illustration shows three pairs of bonded NICs, including the primary management interface. Excluding the Primary Management Interface bond, XenServer uses the other two NIC bonds and the two un-bonded NICs for VM traffic.

Ensuring Resilience through Redundant Switches

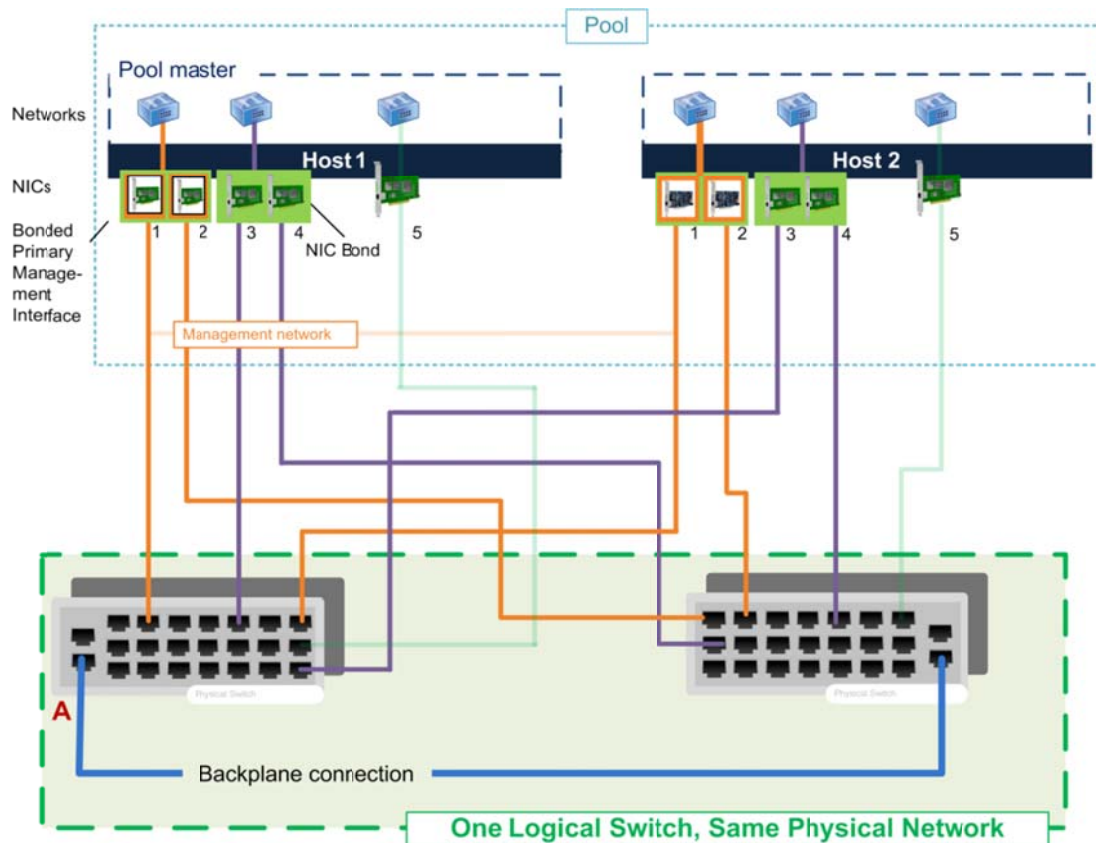
When VM networks use bonded NICs, traffic is sent over both NICs. If you connect one of the NICs in a bond to a second (redundant switch) and a single NIC or switch fails, the virtual machines remain on the network since their traffic fails over to the other NIC/switch.

Provided you enable bonding on NICs carrying only guest traffic, both links are active and NIC bonding can balance each VM's traffic between NICs. Likewise, bonding the primary management interface NIC to a second NIC also provides resilience. However, only one link (NIC) in the bond is active and the other remains unused unless traffic fails over to it.

If you bond a management interface, a single IP address is assigned to the bond. That is, each NIC does not have its own IP address; XenServer treats the two NICs as one logical connection.

Note: While NIC bonding can provide load balancing for traffic from multiple VMs, it cannot provide a single VM with the throughput of two NICs.

The illustration that follows shows how the cables and network configuration for the bonded NICs have to match.

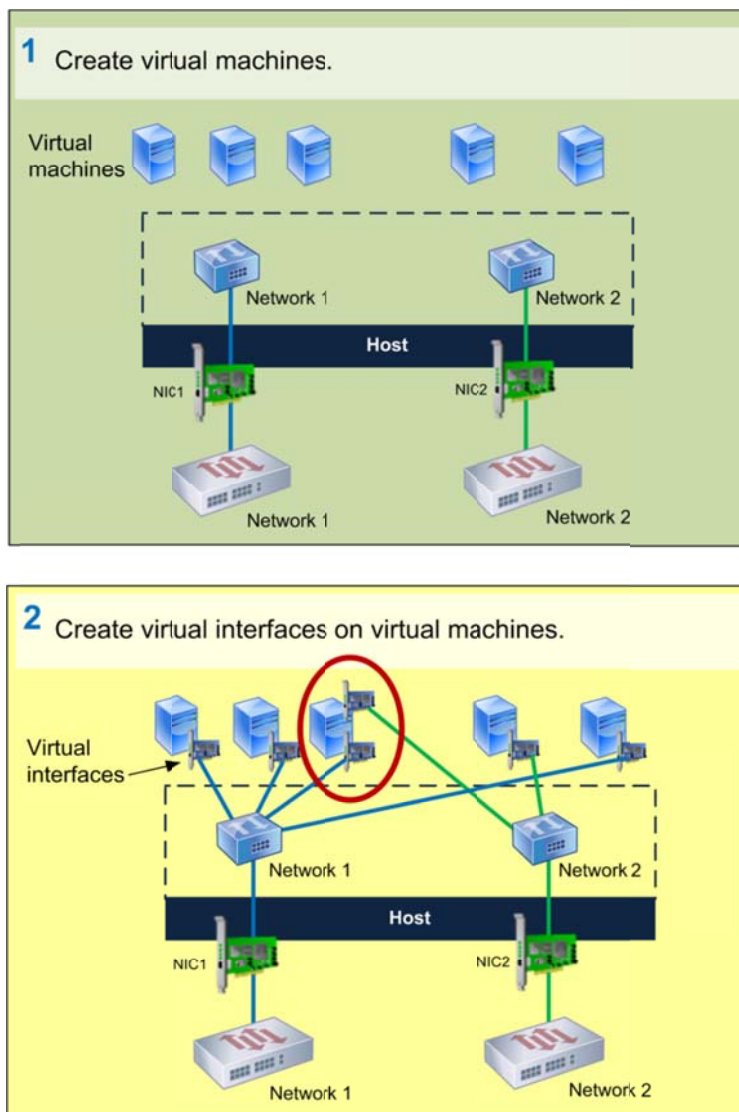


This illustration shows how two NICs in a bonded pair use the same network settings, as represented by the networks in each host. The NICs in the bonds connect to different switches for redundancy.

Connecting a VM to a Network using Virtual Interfaces

Virtual machines connect to a network through a virtual interface on that particular network. XenServer sends the VM's traffic through the target network's associated NIC. By default, when you create a VM in XenCenter, XenServer creates a virtual interface connecting the VM to Network 0. This configuration lets VMs connect to an external network through the NIC attached to Network 0.

You need a virtual interface on a VM for each separate physical network to which you want to connect it. In environments that connect to only one physical network, the virtual interface XenCenter creates by default when you create a VM may be sufficient for your needs. However, if you need a VM to connect to multiple physical networks, you must create a virtual interface for each one of those networks.



This illustration shows how VMs require a virtual interface for each physical network to which they need to connect.



Some additional points about virtual interfaces:

- Most, but not all, VMs have at least one virtual interface. (If an administrator accesses a VM only through XenCenter, the VM does not need a virtual interface.)
- Each virtual interface must have a “virtual” MAC address. You can configure XenServer to generate these automatically for you (recommended) or specify them manually.
- When you create a network in XenCenter, you can specify if you want XenCenter to create a new virtual interface for that network automatically, whenever you create a VM.
- Unlike for the physical and infrastructure layers, the networking configurations on VMs do not need to match other VMs in the pool.

Understanding Virtual MAC Addressing

Just like NICs in the physical world, each virtual interface must have its own (virtual) MAC address. When you create a virtual interface, you can either specify a MAC address manually or let XenServer generate one for you.

When XenServer generates MAC addresses automatically, it generates *locally administered addresses*. Locally administered addresses are addresses assigned to devices by a user, which typically lack manufacturer-specific encoding. As a result, they do not contain a manufacturer-specific *Organizationally Unique Identifier* (OUI). Typically, manufacturers “burn-in” MAC addresses in which the first three octets indicate which company manufactured the device.

This means that the MAC addresses XenServer generates will not clash with addresses from *hardware* devices on your network.

XenServer generates a MAC addresses at random based on the random seed in the *VM.other-config:mac-seed* parameter of the VM and the device number of the virtual interface (a sequence number for the VIF: 0...6).

A particular combination of a MAC seed and device number always results in the same MAC address. Consequently, if you remove a virtual interface from a VM and recreate it later, the new virtual interface typically gets the same MAC as before.

XenServer preserves MAC addresses when migrating VMs. However, when you copy or clone VMs, the VM receives a new random MAC address seed and the virtual interfaces get new MAC addresses based on that seed.

Tip: To obtain the MAC address of a XenServer VM in XenCenter, select the VM’s **Network** tab, select the virtual interface, and click **Properties**.

Segregating VM Traffic from Management and Storage Traffic

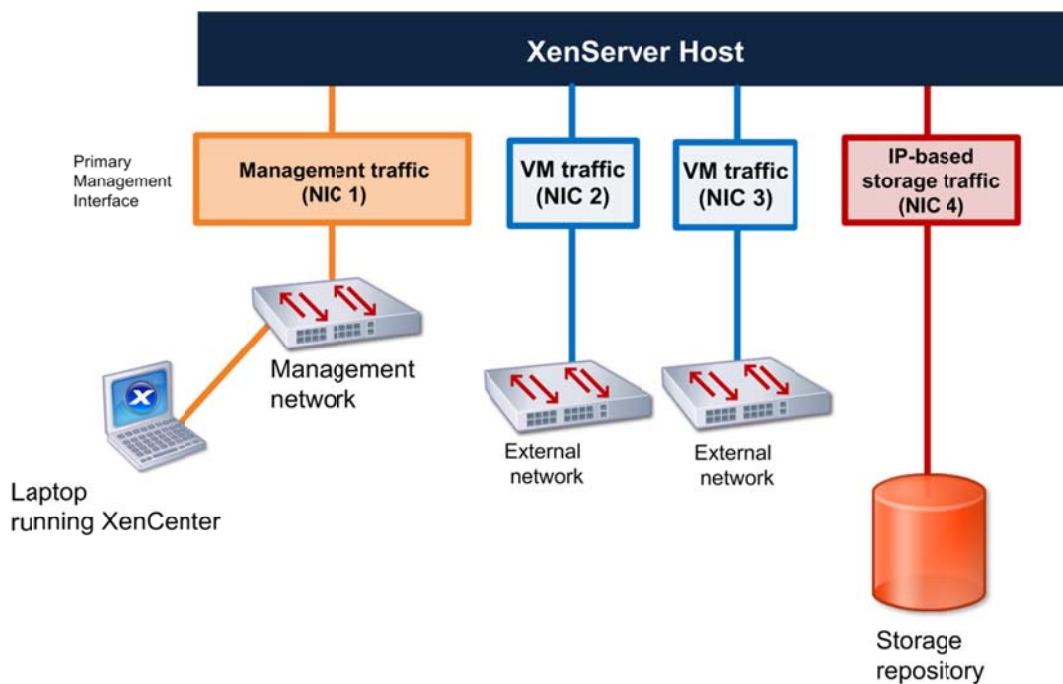
You can separate each type of traffic –VM, storage, and management traffic – onto its own network for either security or performance reasons.

For most environments, Citrix recommends segregating VM traffic from management traffic as the best practice. Not only does it increase the security of the management network, it can improve performance by reducing competition between traffic types for network resources, reducing potential collisions, and reducing the load on the primary management interface.

There are a variety of ways in which you can separate traffic, including:

- Separating all types of traffic from each other. For example, putting the virtual machines on a network not used for storage or management traffic.
- Separating the management traffic from the VM and storage traffic.

However, VMs will only use a NIC for VM traffic if they have a virtual interface on the same network as the NIC. The illustration that follows shows the best practice example of how you might separate traffic.



This illustration shows how NICs that are not designated for management or storage traffic only carry VM traffic.

While separating traffic is a best practice in larger environments, it is not an absolute requirement for all environments. In smaller environments, you may want to configure VMs to send their traffic on the management network. However, Citrix recommends evaluating the performance of this configuration regularly.

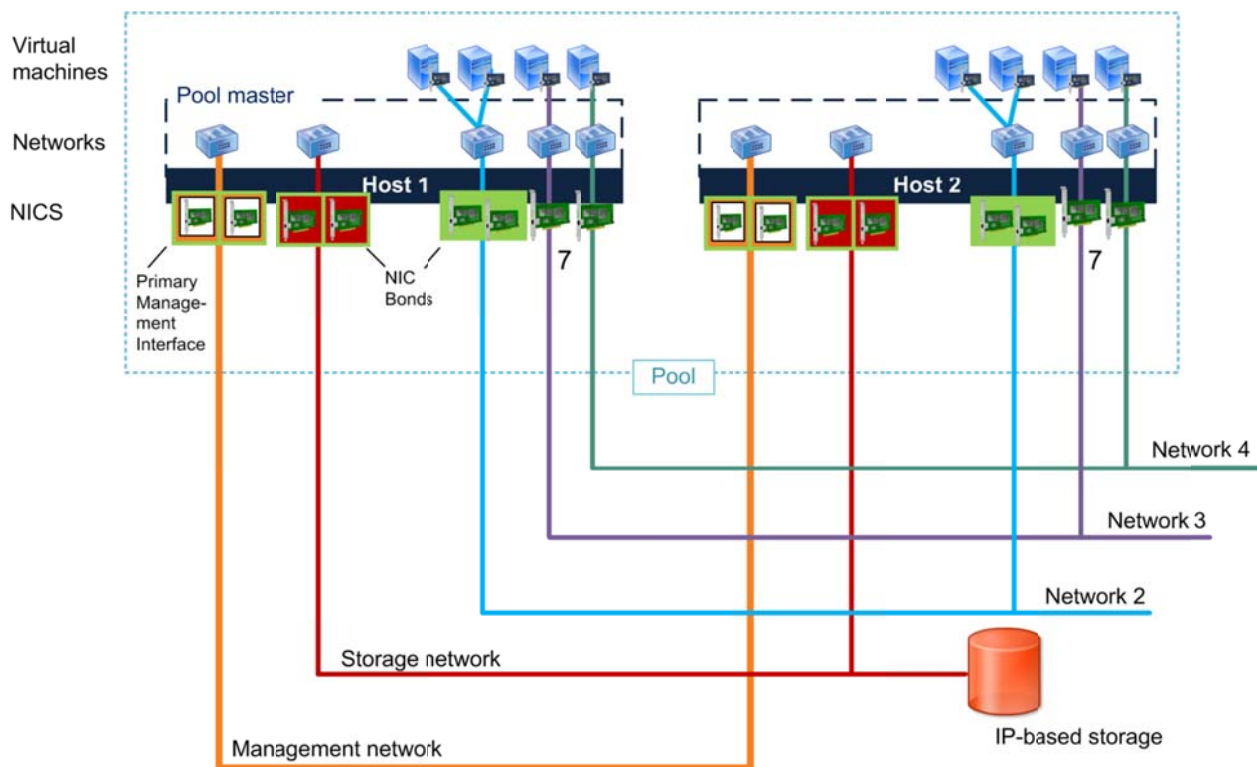
The scenarios that follow illustrate both of these concepts: separating traffic and sending traffic over NICs shared by multiple networks.

Scenario 1: Segregating Traffic

In this scenario, an administrator wants a dedicated network for management and storage traffic. To do this, the administrator:

- Attached the network cables coming from the NICs to a switch for a network to be used for VM traffic, which is physically isolated from the storage and management networks
- Created virtual interfaces on the same networks as the NICs

The illustration that follows shows these segregated networks.



This logical illustration shows segregated guest, storage, and management networks. In this scenario, all the VMs using network 2 can communicate with each other because they are configured to use the same (corresponding) NIC bond on their respective hosts and that bond connects to the same physical network. Likewise, the two VMs connected to network 3 can communicate with each since the corresponding NIC 7 on each host connects to the same physical switch.

As shown in previous illustration, not all NICs have virtual interfaces associated with them. If you do not configure a virtual interface connecting to the management network, the management NIC becomes dedicated for management traffic. For example, in the previous illustration there are NICs



connected to the management and storage networks that do not have corresponding virtual interfaces.

Note: Citrix does not recommend assigning IP addresses (that is, creating management interfaces) for each NIC on your host. Ideally, Citrix does not recommend using any NICs with IP addresses assigned to them for VM traffic.

Scenario 2: Using the Management Network for VM Traffic

In environments with minimal security requirements, you can configure VMs to share the management or storage networks.

In this example, the organization uses the management network for two purposes:

- XenCenter can connect to the management network through the primary management interface on the pool master. This is because of the IP address on that NIC. Likewise, hosts and other components, such as Workload Balancing, can use the connection to communicate with XenServer.

Note: XenCenter only communicates with the pool master and not any member servers. Specifically, XenCenter only connects to the IP address of the master's primary management interface.

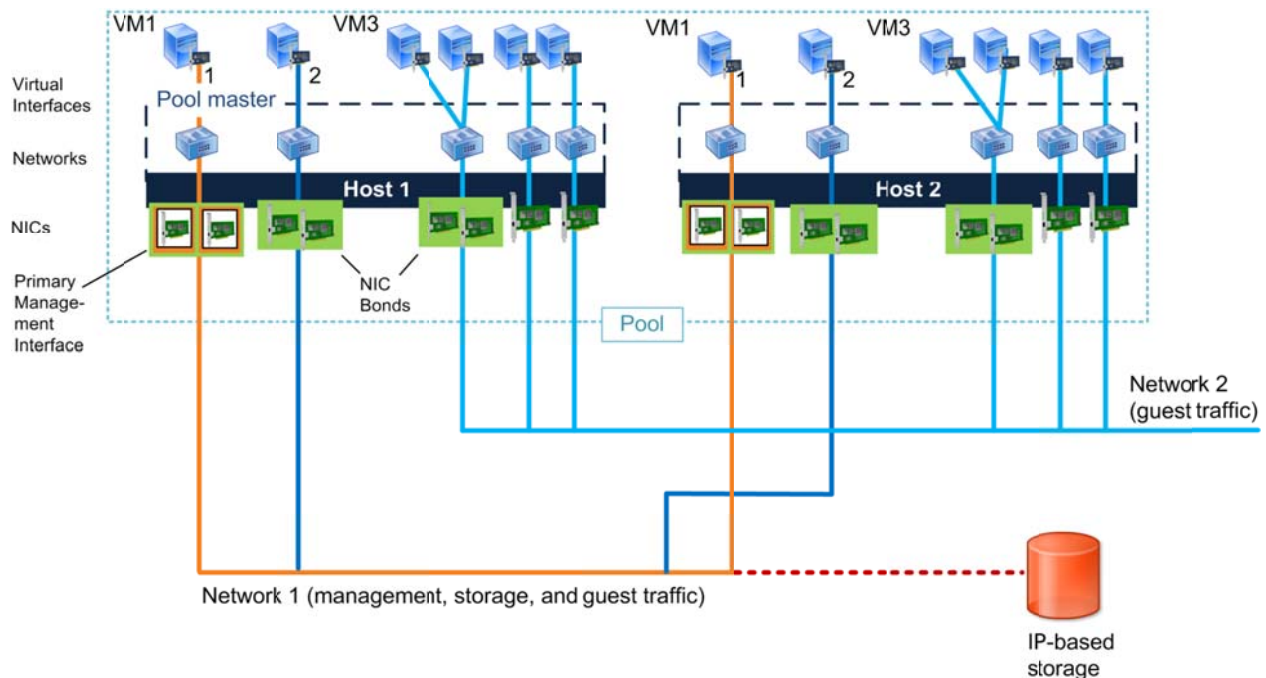
- VM traffic is also sent on this management network. This is the default configuration and requires no changes. To revert to this configuration, create a virtual interface on the VM and specify the VM network that is sharing the management network.

This configuration lets (1) XenServer use the NIC configured as the primary management interface to communicate with other hosts and (2) VMs transparently forward guest traffic onto that network and back.

However, this configuration has security implications. Workstations hosting XenCenter and XenServer hosts using this management network can communicate with each other because they are on the same network. This makes the management network, which ultimately manages the hardware layer and controls the hypervisors themselves, vulnerable to any attacks originating from the VMs. For example, if the VMs host Web servers, any successful attacks originating from outside the organization can potentially penetrate your entire virtual infrastructure – or all infrastructure on the targeted pool.

In contrast, scenario 1 on page 28 separates the VM traffic from the management network, which confines any successful external attacks to the guest network.

The following illustration shows some VMs sending their VM traffic over the management network.



This logical illustration shows how the administrator configured the virtual interfaces on VM 1 and VM 3 to send their traffic across the management network.

Note: Virtual interfaces appear differently in Linux and Windows VMs:

- In a Windows VM, the initial Windows installation has an emulated network device that uses a built-in driver.
- In a Linux VM, the NIC appears as a standard Linux network device and uses the high-speed Xen paravirtualized network driver.

After you install the XenServer Tools (for Windows guests), Windows also uses high-speed paravirtualized network drivers.

Scenario 3: Isolating VM Traffic on a Private Network

You might have specific types of workloads that require isolation. For example, in environments with technically savvy workers, you might not want servers with confidential employee data on the same network as regular VM traffic. XenServer lets you segregate traffic by creating two types of private networks: single-server private networks and cross-server private networks.

Private networks do not have an uplink or a physical NIC. Private networks connect VMs on the same XenServer host or the same resource pool. In a private network, VMs can only communicate with VMs on the same switch on the same host. In the case of cross-server private networks, VMs can only communicate with VMs on the same vSwitch.



Essentially, a private network functions like an isolated local area network that is local to either a host or a group of hosts (pool). This results in higher speed networks since responses between VMs are based on the storage speed and not limited by the network bandwidth or bottlenecks.

Due to the speed, lab machines and test environments are a good use case for private networks. Creating private networks might also be desirable for these reasons:

- **Security.** Single-server and cross-server private networks can let you isolate VMs from other network traffic (almost like creating a virtual “stove pipe”). Private networks and cross-server private networks are completely isolated from regular network traffic. VMs outside of the private network cannot sniff or inject traffic into the network, even if both sets of VMs are on the same physical server and the virtual interfaces on both sets of VMs transmit traffic across virtual interfaces connected to a network on the same underlying NIC.
- **Faster traffic for connections between VMs on the same host.** Because VMs do not need to interact with regular network and switches, they can transmit traffic faster to each other.

Private networks provide connectivity only between VMs on a given XenServer host and do not have a connection to the outside world. Networks with a NIC (PIF) association are considered external: they provide a bridge between virtual interfaces and the NIC connected to the network, enabling connectivity to resources available through the NIC.

Note: In previous XenServer releases, single-server private networks were known as internal networks.

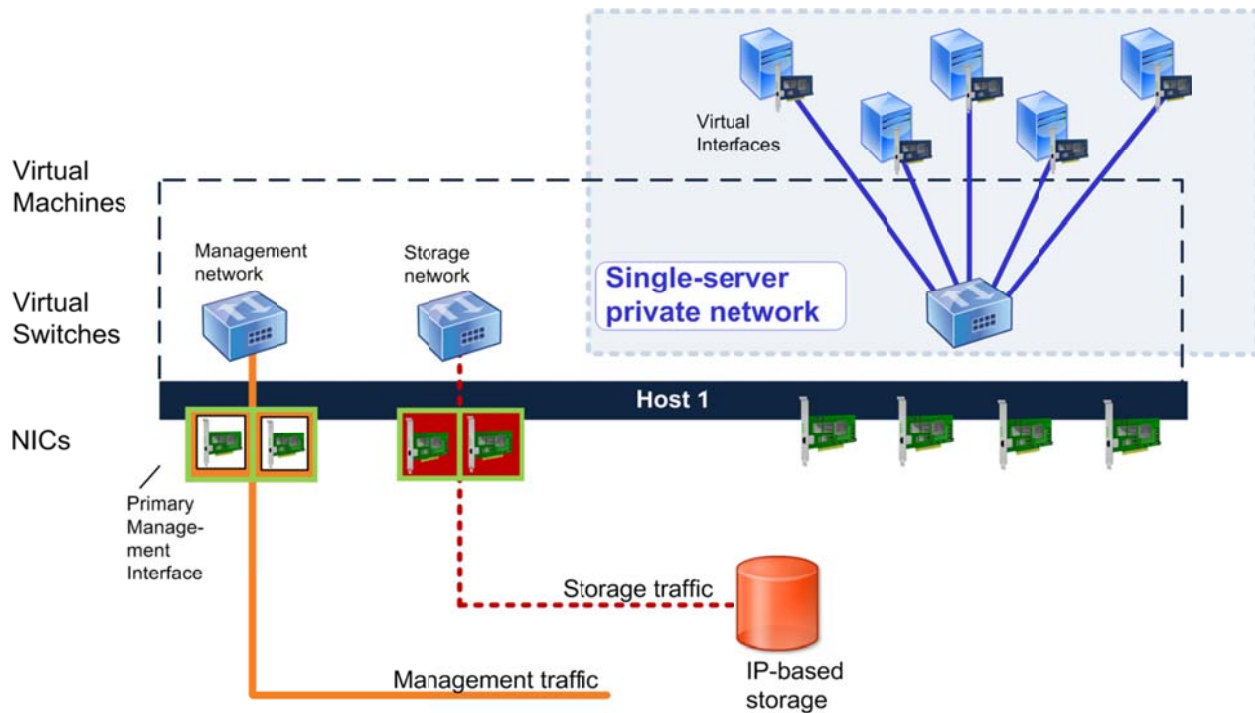
To create a cross-server private network, all pool servers must use the Open vSwitch for networking and the pool must have a vSwitch Controller configured. For information about configuring the vSwitches, see the *XenServer Administrator's Guide*. Configuring the vSwitch Controller is done outside of XenCenter and described in the *XenServer Distributed Virtual Switch Controller User Guide*.

Note: To use cross-server private networks, all the pool servers must be running XenServer 5.6 Feature Pack 1 or greater.

Isolating VM Traffic on One Host

If you have some VMs on one host that you do not want on your organization's network, you can create a *single-server private network*. This is an internal network that has no association with a physical network interface. It only connects the virtual machines on the host and has no connection to the outside world.

The illustration that follows shows a private network configured on one host.



This illustration shows how the virtual interfaces on the VMs are on the single-server private network. This network does not have any connect to any NICs since all traffic is sent inside the XenServer host.

To create a single-server private network that is isolated from the external network, you

1. Create a single-server private network in XenCenter.

In XenCenter, select the host in the Resource pane. Click the **Network** tab. Click **Add Network** and then select **Single-Server Private Network**.

Unlike when you create external networks, XenCenter does not prompt you to specify a NIC when you create private networks. This is because private networks do not require a NIC for connectivity.

2. Create a virtual interface on each VM that specifies the new private network.

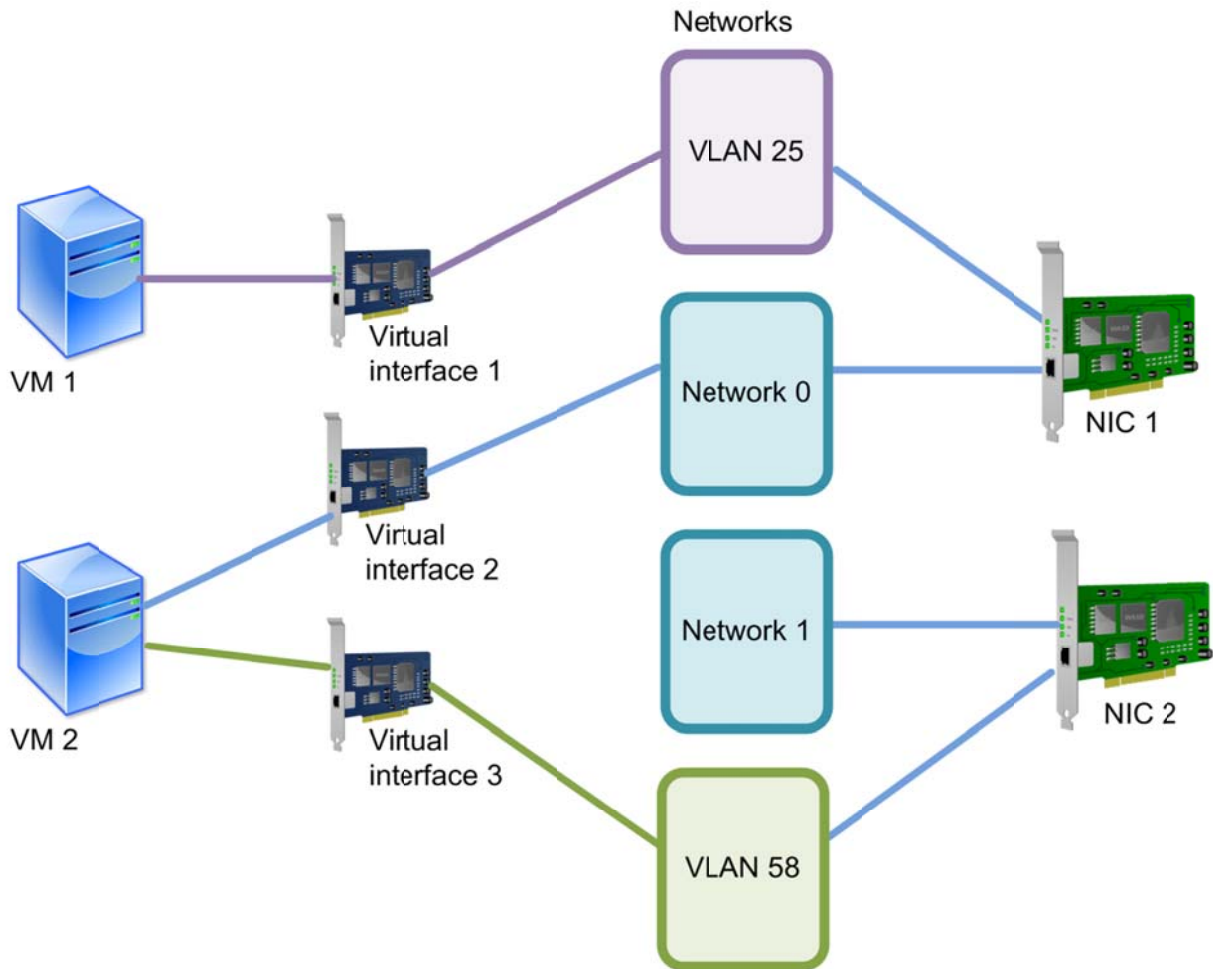
If you want to isolate the VMs' traffic completely, if necessary, remove any virtual interfaces on the VMs that are on an external network.

Note: To create cross-server private networks, see CTX127585 – [XenServer 5.6 Feature Pack 1 vSwitch Controller User Guide](#).

Scenario 4: Connecting VMs to Multiple Linked VLANs

Many organizations today configure VLANs to logically separate their physical networks for either performance or security reasons. If your organization has VLANs, you might want to connect your VMs to one or more VLANs on your network.

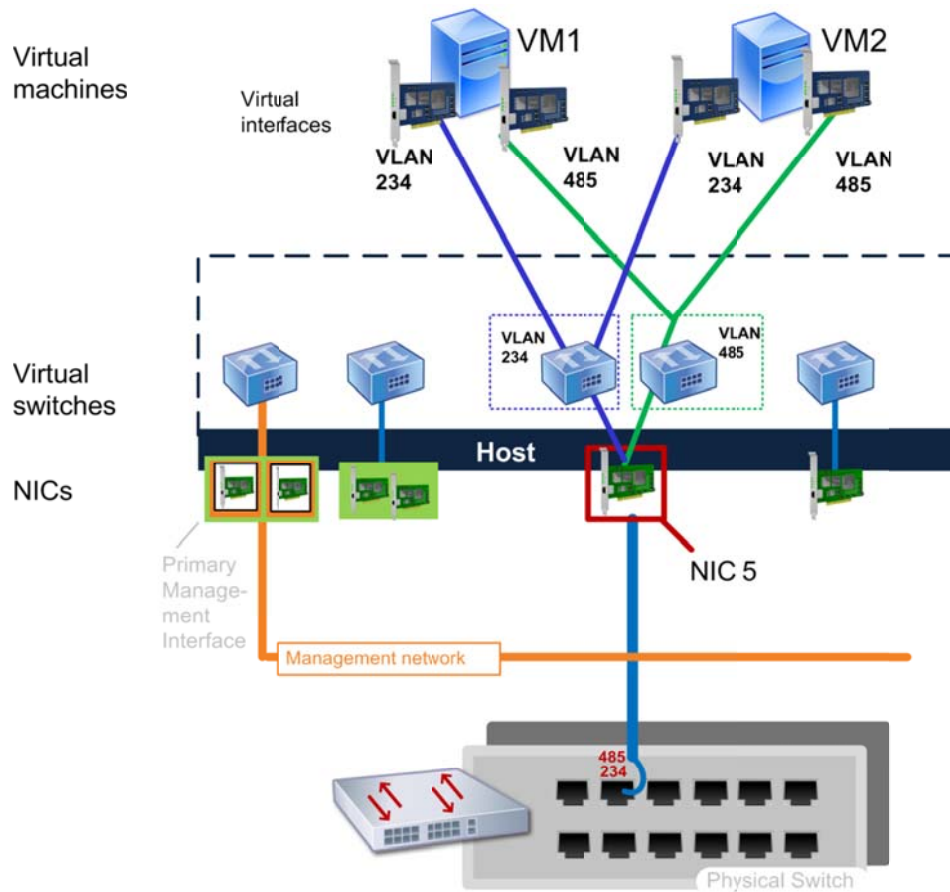
To connect a VM to a VLAN, you must create a network for the VLAN and then connect the VM to that network. To perform this configuration, you create a separate external network for each VLAN and then create a virtual interface on the VM for each of these networks.



This illustration shows how VMs require a separate virtual interface for each network to which you want to connect them, including VLANs. In this example, VM 2 connects to Network 0 through Virtual Interface 2 and to VLAN 58 through Virtual Interface 3. As shown by VM1 and NIC1, multiple networks can connect out through one NIC.

While trunk lines from the physical switch can contain multiple 802.1q VLANs, XenServer does not let you combine multiple VLANs in one XenServer network. This means that to let a VM connect to multiple VLANs you must either (a) create a separate network in XenServer for each VLAN or (b) create a XenServer network for a VLAN that can access all of the desired VLANs.

In the illustration that follows, the VMs connect to a VLAN through a trunked switch port.



This illustration shows how VMs on the host connect to an external network that the administrator configured to connect to VLAN 485 and VLAN 234. To achieve this, the administrator created an external network that uses NIC 5 to connect to a trunked switch port that includes VLAN 485 and a second external network that also uses NIC 5 to connect to VLAN 234. The administrator ran a cable from the VLAN trunk port to NIC 5.

Connecting a VM to a VLAN requires that you:

1. Create a physical connection between the corresponding NIC on each host and the VLAN trunk port for that VLAN on the switch.

For example, if you connect NIC 7 on the XenServer pool master to a VLAN trunk port on the switch with access to VLAN 485, you must run a cable from NIC 7 on all other hosts in the pool to a similarly configured VLAN trunk port on the same switch, which can access VLAN 485.

2. Enable XenServer to connect to a specific VLAN on the switch by creating an external network specifying that VLAN tag.

This means creating an external network on the XenServer pool master and specifying the VLAN tag when you create the network.

In XenCenter, select the pool (<*your-pool-name*>) in the **Resource** pane, click the **Network** tab, and click the **Add Network** button. In the New Network wizard, select **External Network**. On the **Location** page, specify the NIC you physically connected to the switch and enter the VLAN tag for the VLAN in the **VLAN** box.

In the XenServer CLI, you can use the **pool-vlan-create** xe command to create the VLAN on all hosts in a resource pool. For more information, see the *XenServer Administrator's Guide*.

After you create the network for the VLAN on the pool master, XenServer configures the NICs on all the other hosts so that the corresponding NIC on each host

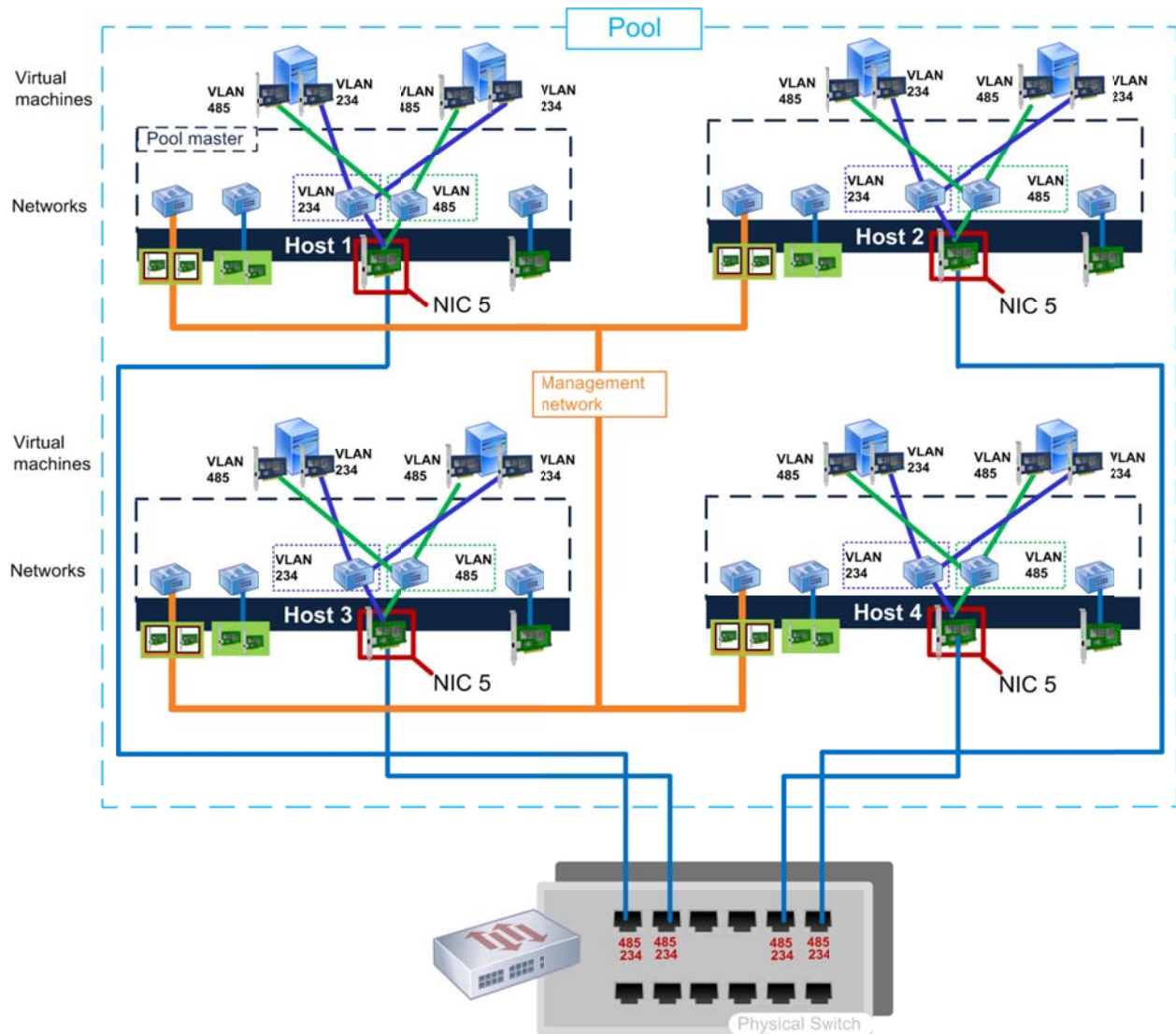
Note: The numbers of VLAN tags must be between 0 to 4094.

3. Connecting the appropriate VMs to the VLAN by configuring a virtual interface that points to that network on each VM you want to be able to connect to the VLAN.

In XenCenter, this is done by selecting the VM in the Resource pane, clicking the **Network** tab, and clicking **Add Interface** and then specifying the VLAN network when you create the interface.

Again, because networking is a pool-level feature, if you connect one host to a VLAN, you must connect all hosts in the pool to the VLAN. This means that you must physically connect the corresponding NIC on each host to the VLAN port on the switch.

In the illustration that follows the VMs on multiple hosts in a pool connect to a VLAN through a trunked switch port.



This illustration shows how, because XenServer automatically synchronizes the network settings in pools so that they match, NIC 7 on all hosts in the pool will be configured with the same network and VLAN settings as NIC 7 on the pool master. However, for the VMs on the member servers to be able to connect to the VLAN, the administrator must also physically connect NIC 7 on each host to a trunk port on the switch that can access VLAN 485.

Before configuring a VLAN, ensure the switch on your VLAN network is configured as follows:

- The port on the switch connected to each XenServer host must be configured as trunk port.
- The port on the switch must be configured for 802.1q encapsulation.
- Port security cannot be set on the trunk port.
- The port designated as trunk should be assigned a native VLAN; use 1 as default.

XenServer lets you create multiple networks and VLAN networks on the same NIC. XenServer does not limit the number of VLANs you can connect to VMs. Instead, the limit comes from the



802.1q standard is 4096. You add an external network for each VLAN to the host and then connect the VMs to the VLANs by specifying that network in the VM's virtual interface.

Note: If a Native VLAN is used on the switch trunk port, then you cannot assign that VLAN number to a VM on the XenServer.

For an example of a tested working model of a VLAN configuration, see CTX123489 -- [XenServer VLAN Networking](#). For more information about configuring VLANs on your switch and 802.1q support, see the documentation for your switches.

Tip: To verify that you have configured the XenServer host to communicate across the correct network, you can use the packet sniffing software included with your NICs to capture and display the VLAN tags that are transmitted across the switch to the XenServer.

Creating VLANs on Bonded Networks

XenServer supports connecting to VLANs from bonded NICs. To do so, do the following:

1. Bond the two NICs together. After you have done so, the NIC bond appears as a bonded network in XenCenter.
2. In XenCenter, for example, create an **External Network** specifying the following:
 - a) The VLAN's tag
 - b) The NIC bond as the NIC

You might want to name this external network the same name as the VLAN (for example, VLAN 25).

3. When you create the virtual interface for the VM, specify the external network with the VLAN tag as the network.

Creating VLANs on the Primary Management Interface

You can have a single VLAN on the primary management interface, and this VLAN can be on an access port. If you want to use a trunk, either you define a default VLAN on that trunk and the management interface can use that or you make the port a full access port.

XenServer 5.6 Feature Pack 1 does not support having a VLAN trunk port on the primary management interface.

Version History

Revision	Date	Comments
1	December 30, 2010	Initial release.
2	Feb 25, 2011	Added information about VLANs, MAC addresses, and single-server private networks. Added introductory chapter. Stylistic changes. Clarity improvements to illustrations. Fixed broken cross-reference.



About Citrix

Citrix Systems, Inc. (NASDAQ:CTXS) is the leading provider of virtualization, networking and software as a service technologies for more than 230,000 organizations worldwide. Its Citrix Delivery Center, Citrix Cloud Center (C3) and Citrix Online Services product families radically simplify computing for millions of users, delivering applications as an on-demand service to any user, in any location on any device. Citrix customers include the world's largest Internet companies, 99 percent of Fortune Global 500 enterprises, and hundreds of thousands of small businesses and prosumers worldwide. Citrix partners with over 10,000 companies worldwide in more than 100 countries. Founded in 1989, annual revenue in 2008 was \$1.6 billion.

©2010-2011 Citrix Systems, Inc. All rights reserved. Citrix®, Access Gateway™, Branch Repeater™, Citrix Repeater™, HDX™, XenServer™, XenApp™, XenDesktop™ and Citrix Delivery Center™ are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are property of their respective owners.