云计算与虚拟化技术

第6讲：vSphere Network

阮晓龙

13938213680 / rxl@hactcm.edu.cn

http://cloud.xg.hactcm.edu.cn
http://www.51xueweb.cn

河南中医药大学信息管理与信息系统教研室
信息技术学院网络与信息系统科研工作室

2019.3

讨论提纲

- Introducing vSphere Network
- Working with vSphere Standard Switches
  - Configuring the Management Network
  - Configuring VMkernel Networking
  - Configuring Virtual Machine Networking
  - Configuring VLANs
  - Configuring NIC Teaming
- Configuring Virtual Switch Security
  - Promiscuous mode
  - MAC address changes
  - Forged transmits
- Case

1.Introducing vSphere Network

- Designing and building vSphere networks with ESXi and vCenter Server bears some similarities to designing and building physical networks, but there are enough significant differences that an overview of components and terminology is warranted.
- Before addressing some of the factors that affect network design in a virtual environment, let's define the components that may be used to build your virtual network.

1.Introducing vSphere Network

- vSphere Standard Switch
  - A software-based switch that resides in the VMkernel and provides traffic management for virtual machines.
  - Users must manage vSphere Standard Switches independently on each ESXi host.
  - the term vSwitch also refers to a vSphere Standard Switch.

1.Introducing vSphere Network

- vSphere Distributed Switch
  - A software-based switch that resides in the VMkernel and provides traffic management for virtual machines and the VMkernel.
  - vSphere Distributed Switches are shared by and managed across ESXi hosts and clusters within a vSphere datacenter.
  - You might see vSphere Distributed Switch abbreviated as VDS, or just distributed switch.

1.Introducing vSphere Network

- Port/Port Group
  - A logical object on a vSphere Standard or Distributed Switch that provides specialized services for the VMkernel or virtual machines.
  - A virtual switch can contain a VMkernel port or a Virtual Machine Port Group.
  - On a vSphere Distributed Switch, these are called distributed port groups.

1.Introducing vSphere Network

- VMkernel Port
  - A specialized virtual switch port type that is configured with an IP address to allow hypervisor management traffic, vMotion, VMware vSAN, iSCSI storage, Network File System (NFS) storage, vSphere Replication, and vSphere Fault Tolerance (FT) logging.
  - VMkernel ports are also created for VXLAN tunnel endpoints (VTEPs) as used by the VMware NSX network virtualization and security platform. These VMkernel ports are created with the VXLAN TCP/IP stack rather than using the default stack.
  - TCP/IP stacks are covered a bit later in the chapter.
  - A VMkernel port is also referred to as a vmknic.

1.Introducing vSphere Network

- Virtual Machine Port Group
  - A group of virtual switch ports that share a common configuration and allow virtual machines to access other virtual machines that are configured on the same port group or accessible PVLAN or on the physical network.
- Virtual LAN (VLAN)
  - A logical local area network configured on a virtual or physical switch that provides efficient traffic segmentation, broadcast control, security, and efficient bandwidth utilization by providing traffic only to the ports configured for that particular VLAN.

1.Introducing vSphere Network

- Trunk Port (Trunking)
  - A port on a physical switch that listens for and knows how to pass traffic for multiple VLANs. It does so by maintaining the 802.1q VLAN tags for traffic moving through the trunk port to the connected device(s).
  - Trunk ports are typically used for switchto-switch connections to allow VLANs to pass freely between switches. Virtual switches support VLANs, and using VLAN trunks enables the VLANs to pass freely into the virtual switches.
- Access Port
  - A port on a physical switch that passes traffic for only a single VLAN. Unlike a trunk port, which maintains the VLAN identification for traffic moving through the port, an access port strips away the VLAN information for traffic moving through the port.

1.Introducing vSphere Network

- Network Interface Card Team
  - The aggregation of physical network interface cards (NICs) to form a single logical communication channel.
  - Different types of NIC teams provide varying levels of traffic load balancing and fault tolerance.
- VMXNET Adapter
  - A virtualized network adapter operating inside a guest operating system (guest OS).
  - The VMXNET adapter is optimized for performance in a virtual machine. VMware Tools are required to be installed in the guest OS to provide the VMXNET driver.
  - The VMXNET adapter is sometimes referred to as a paravirtualized driver.

1.Introducing vSphere Network

- VMXNET 2 Adapter
  - The VMXNET 2 adapter is based on the VMXNET adapter but provides some high-performance features commonly used on modern networks, such as jumbo frames and hardware offloads.
  - VMware Tools are required to be installed in the guest OS to provide the VMXNET driver.

1.Introducing vSphere Network

- VMXNET 3 Adapter
  - The VMXNET 3 adapter is the next-generation paravirtualized NIC, designed for performance, and is not related to VMXNET or VMXNET 2.
  - It offers all the features available in VMXNET 2 and adds several new features like multiqueue support (also known as Receive Side Scaling in Windows), IPv6 offloads, and MSI/MSI-X interrupt delivery.
  - VMXNET 3 requires virtual machine hardware version 7 or later as well as VMware Tools installed in the guest OS to provide the VMXNET driver.

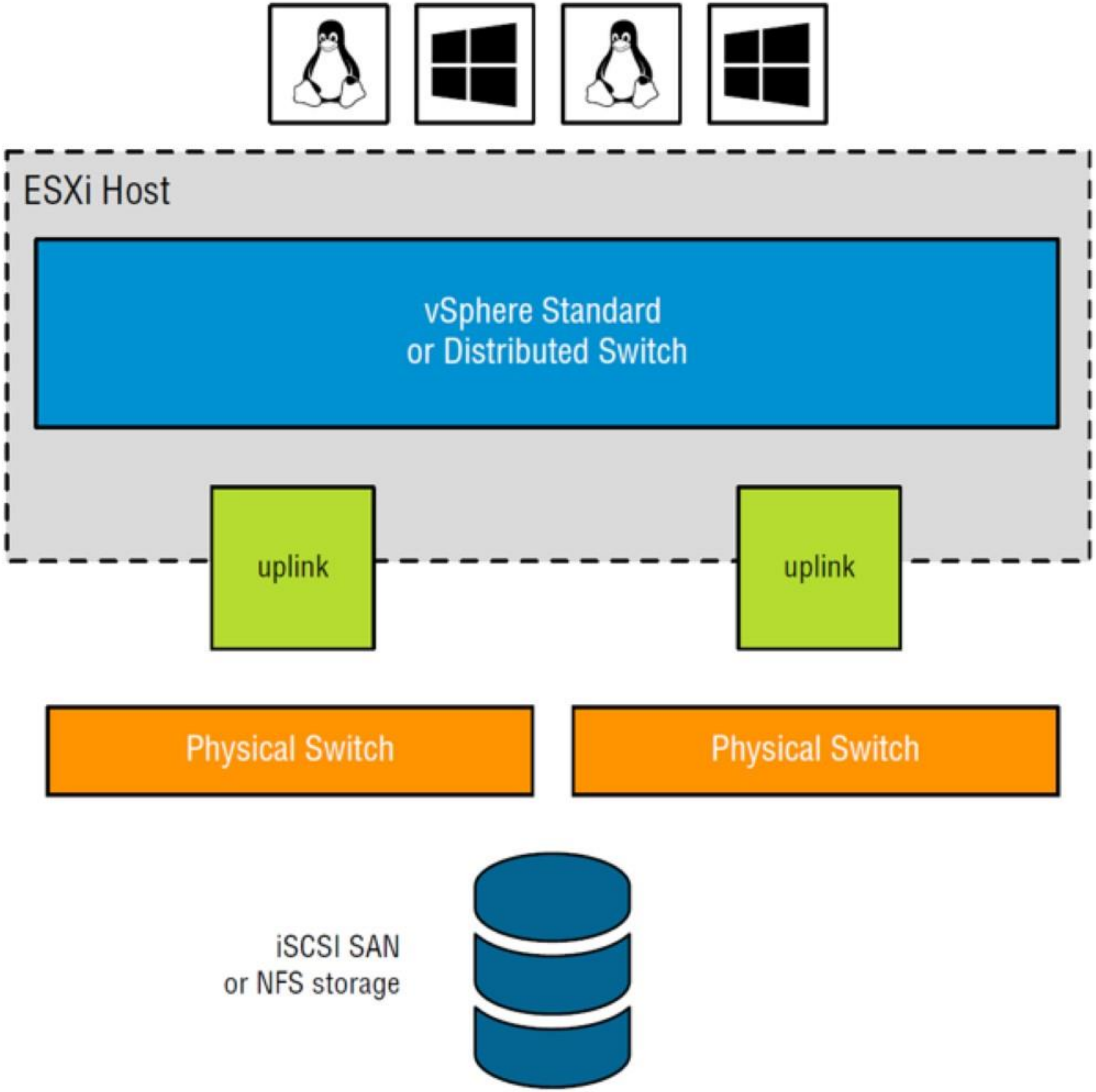
1.Introducing vSphere Network

- E1000 Adapter
  - A virtualized network adapter that emulates the Intel 82545EM Gigabit network adapter.
  - Typically, the guest OS provides a built-in driver.
- E1000e Adapter
  - A virtualized network adapter that emulates the Intel 82574 Gigabit network adapter.
  - The E1000e requires virtual machine hardware version 8 or later.
  - The E1000e adapter is available for Windows 8 and newer operating systems and is not available for Linux.

1.Introducing vSphere Network

- Following questions will determine the design of vSphere network:
  - Do you have or need a dedicated network for management traffic, such as for the management of physical switches?
  - Do you have or need a dedicated network for vMotion traffic?
  - Do you have an IP storage network? Is this IP storage network a dedicated network? Are you running iSCSI or NFS? Are you planning on implementing VMware vSAN?
  - How many NICs are standard in your ESXi host design?
  - Do the NICs in your hosts run 1 Gb Ethernet, 10 Gb Ethernet, 25 Gb Ethernet, or 40 Gb Ethernet?
  - Do you need extremely high levels of fault tolerance for virtual machines?
  - Is the existing physical network composed of VLANs?
  - Do you want to extend the use of VLANs into the virtual switches?
  - Will you be introducing an overlay, such as VXLAN or Geneve, into your network through the use of NSX?

FIGURE 5.1
Successful vSphere networking is a blend of virtual and physical network adapters and switches.



2.vSphere Standard Switch

2.1Configuring the Management Network

- Management traffic is a special type of network traffic that runs across a VMkernel port. VMkernel ports provide network access for the VMkernel's TCP/IP stack, which is separate and independent from the network traffic generated by virtual machines.
- The ESXi hosts management network, however, is treated a bit differently than other VMkernel ports in two ways:
  - the ESXi management VMkernel port is automatically created when you install ESXi. In order for the ESXi host to be reachable across the network, a management VMkernel port must be configured and working.

2.vSphere Standard Switch

2.1Configuring the Management Network

- The ESXi hosts management network, however, is treated a bit differently than other VMkernel ports in two ways:
  - the Direct Console User Interface (DCUI)—the user interface that exists when you're working at the physical console of a server running ESXi—provides a mechanism for configuring or reconfiguring the management network (Management VMKernel port) but not any other forms of networking on that host, apart from a few options for resetting network configuration.

- VMware ESXi DCUI
  - Network Adapters
  - VLAN
  - IPv4 Configration
  - IPv6 Configration

2.vSphere Standard Switch

- VMkernel networking carries management traffic, but it also carries all other forms of traffic that originate with the ESXi host itself.
- VMkernel ports are used for Management, vMotion, vSAN, iSCSI, NFS, vSphere Replication, and vSphere FT, basically, all types of traffic that are generated by the hypervisor itself.

2.vSphere Standard Switch

2.2Configuring VMkernel Networking

FIGURE 5.14
A VMkernel adapter is assigned an IP address for accessing iSCSI or NFS storage devices or for other management services.

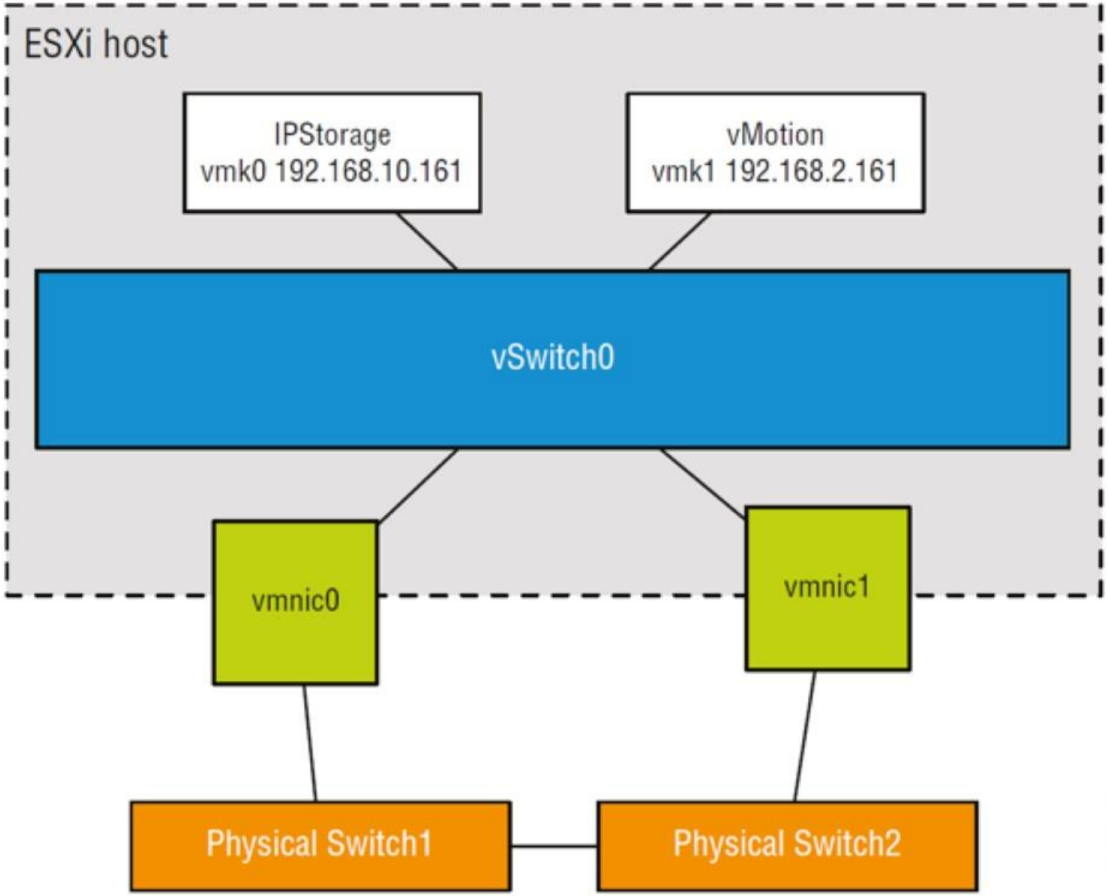
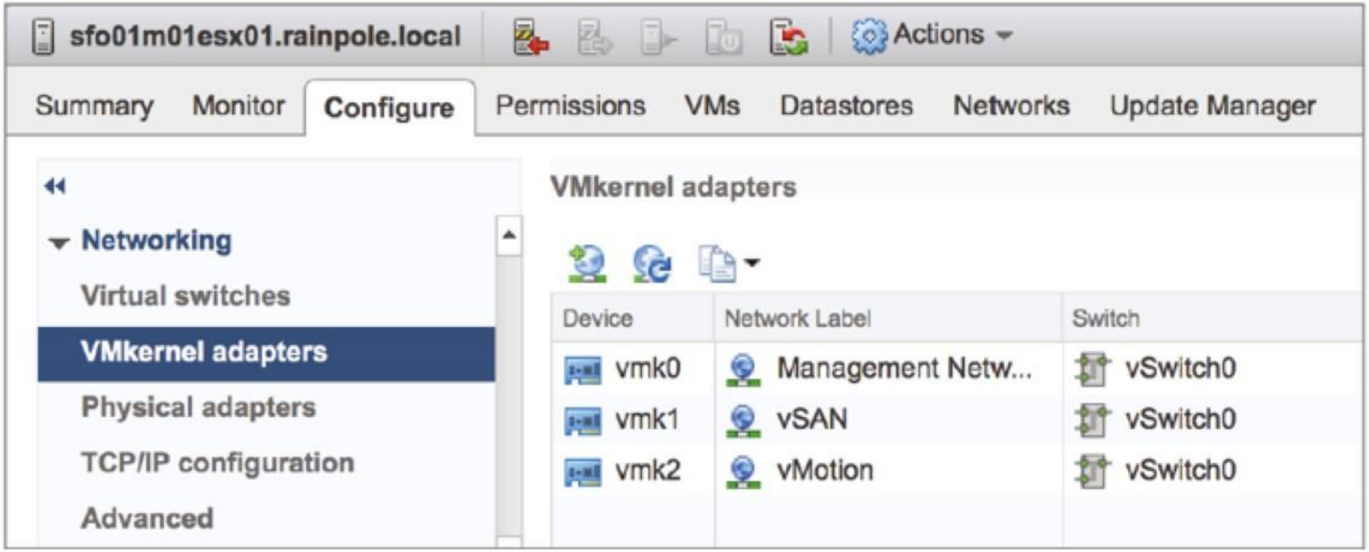


FIGURE 5.15
It is recommended to add only one type of traffic to a VMkernel interface.



sfo01m01esx01.rainpole.local

Actions

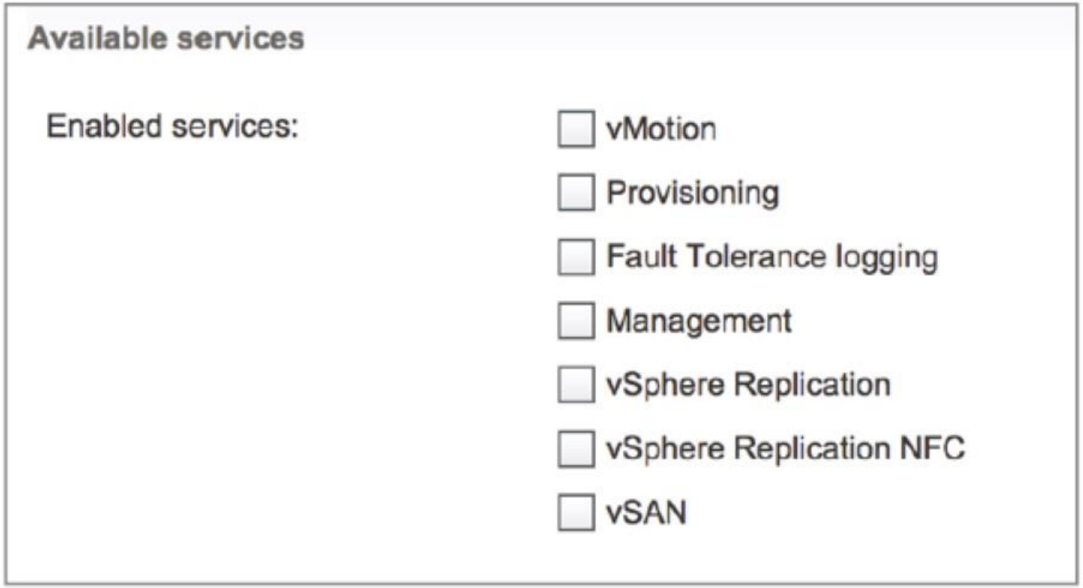
Summary | Monitor | **Configure** | Permissions | VMs | Datastores | Networks | Update Manager

- Networking
  - Virtual switches
  - **VMkernel adapters**
  - Physical adapters
  - TCP/IP configuration
  - Advanced

VMkernel adapters

Device	Network Label	Switch
vmk0	Management Netw...	vSwitch0
vmk1	vSAN	vSwitch0
vmk2	vMotion	vSwitch0

FIGURE 5.16
VMkernel traffic types in vSphere 6.7. Starting with vSphere 6.0, VMkernel ports can now also carry Provisioning traffic, vSphere Replication traffic, and vSphere Replication NFC traffic.



Available services

Enabled services:

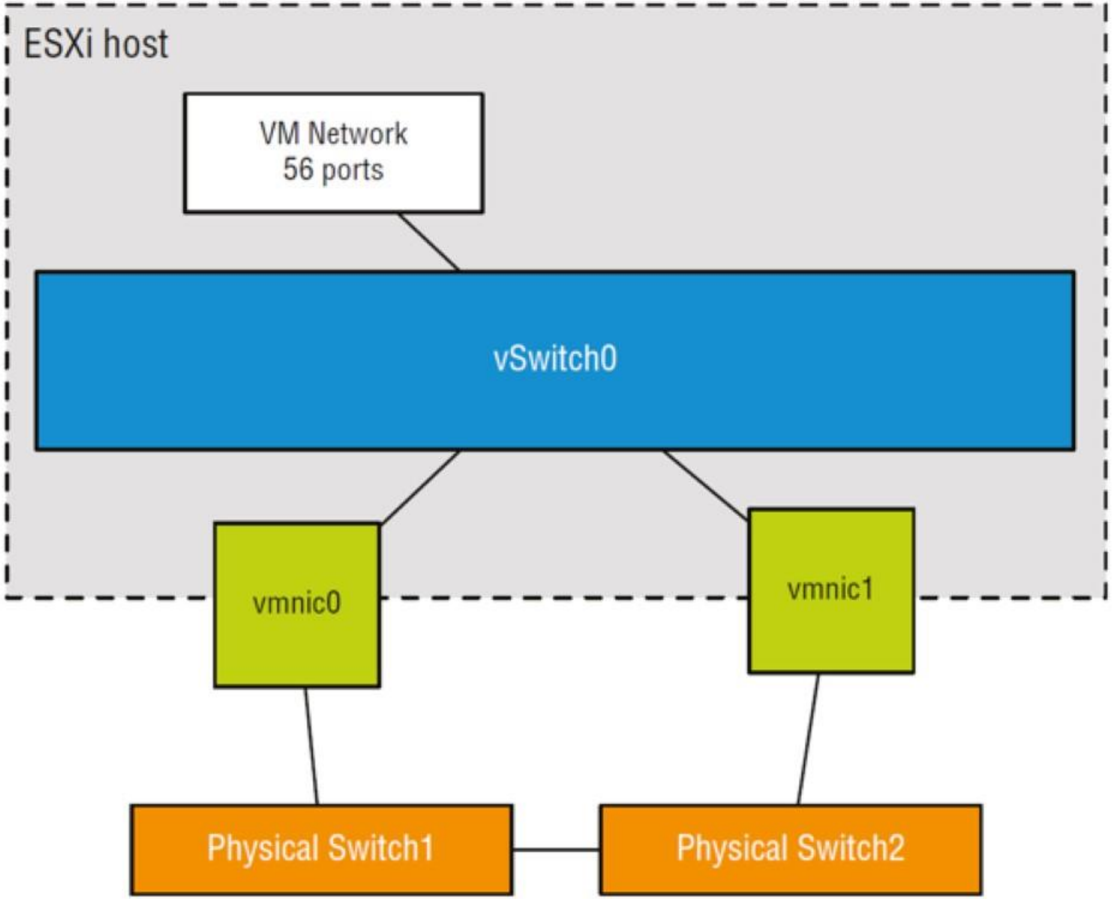
□ vMotion
□ Provisioning
□ Fault Tolerance logging
□ Management
□ vSphere Replication
□ vSphere Replication NFC
□ vSAN

- 基于vCSA进行演示VMKernel
  - Virtual switches
  - VMkernel adapters
  - Physical adapters
  - TCP/IP configuration
  - Advanced
  - VMkernel traffic types

2.vSphere Standard Switch

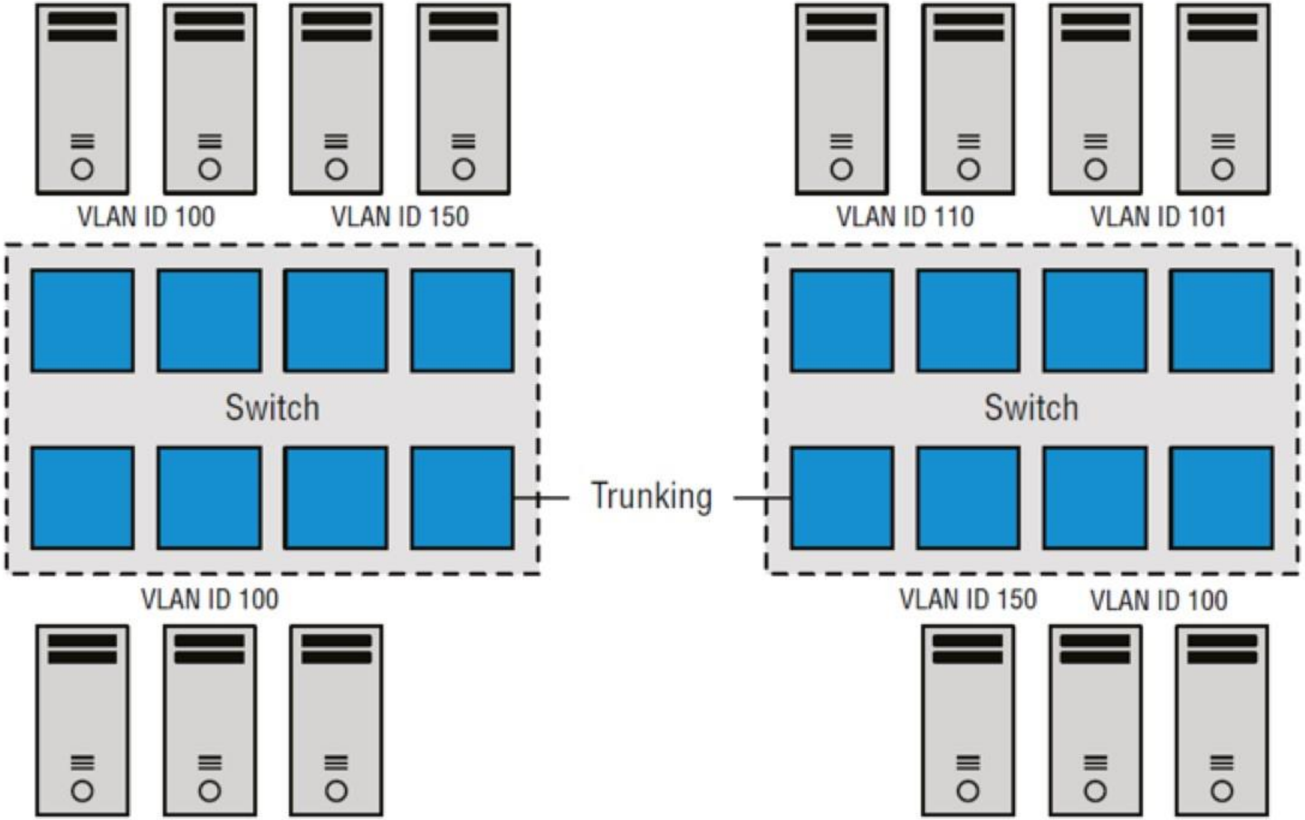
2.3Configuring Virtual Machine Networking

Figure 5.22
A vSwitch with a Virtual Machine Port Group uses associated physical network adapters to establish switch-to-switch connections with physical switches.

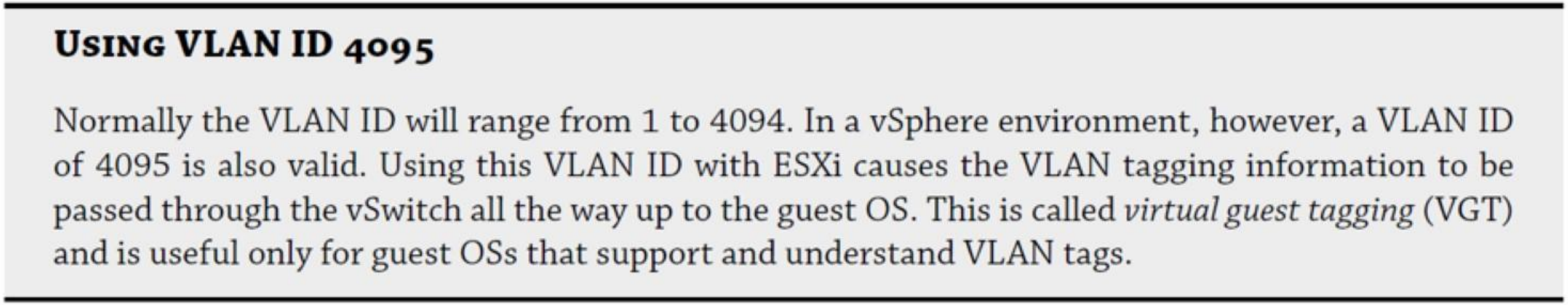


2.vSphere Standard Switch

Figure 5.23
Virtual LANs provide secure traffic segmentation without the cost of additional hardware.



2.vSphere Standard Switch



USING VLAN ID 4095

Normally the VLAN ID will range from 1 to 4094. In a vSphere environment, however, a VLAN ID of 4095 is also valid. Using this VLAN ID with ESXi causes the VLAN tagging information to be passed through the vSwitch all the way up to the guest OS. This is called *virtual guest tagging* (VGT) and is useful only for guest OSs that support and understand VLAN tags.

2.vSphere Standard Switch

- VLANs are an important part of ESXi networking because of the impact they have on the number of vSwitches and uplinks required.
- Consider this configuration:
  - The management network needs access to the network segment carrying management traffic.
  - Other VMkernel ports, depending on their purpose, may need access to an isolated vMotion segment or the network segment carrying iSCSI and NFS traffic.
  - Virtual Machine Port Groups need access to whatever network segments are applicable for the virtual machines running on the ESXi hosts.

FIGURE 5.24
Supporting multiple networks without VLANs can increase the number of vSwitches, uplinks, and cabling that is required.

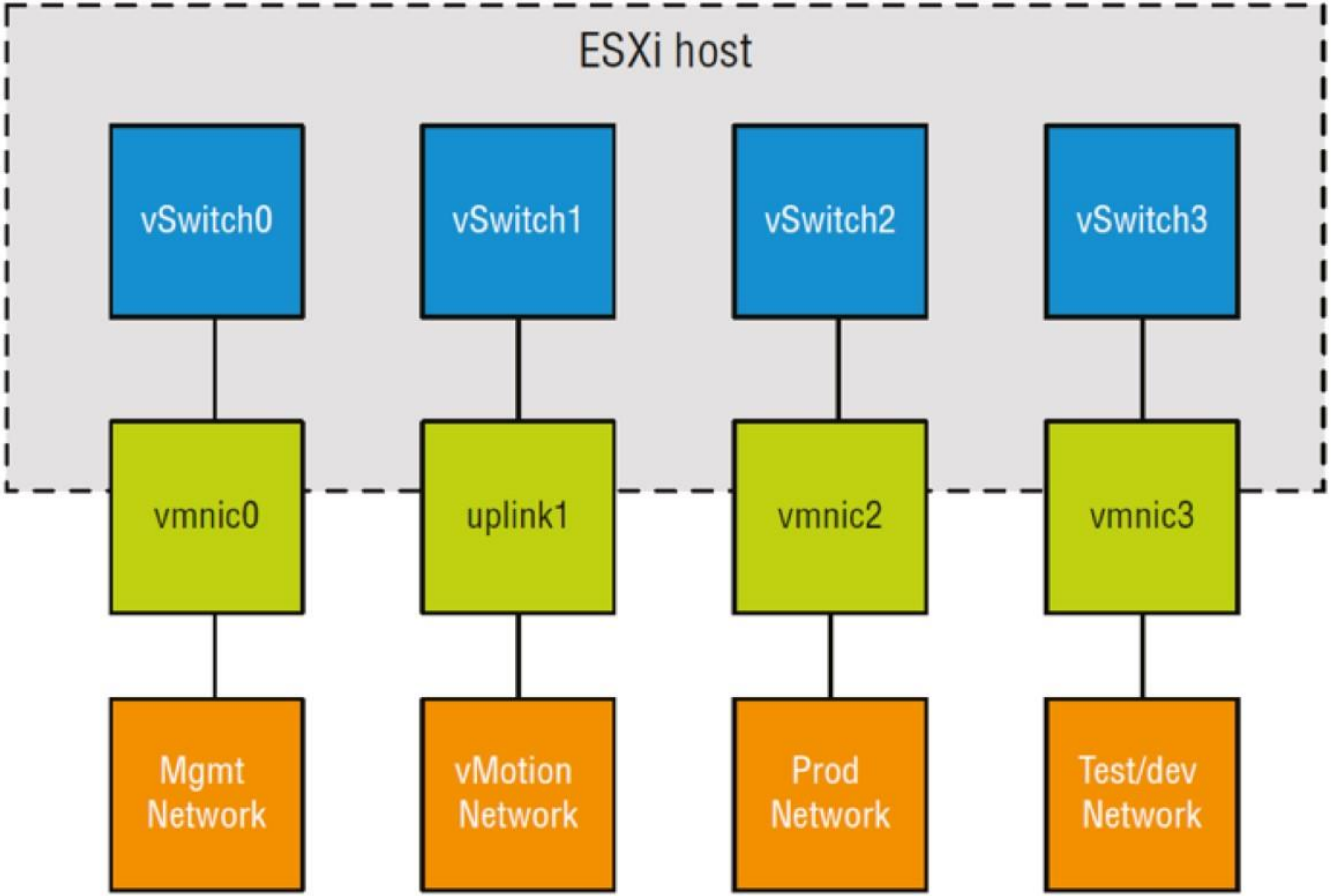
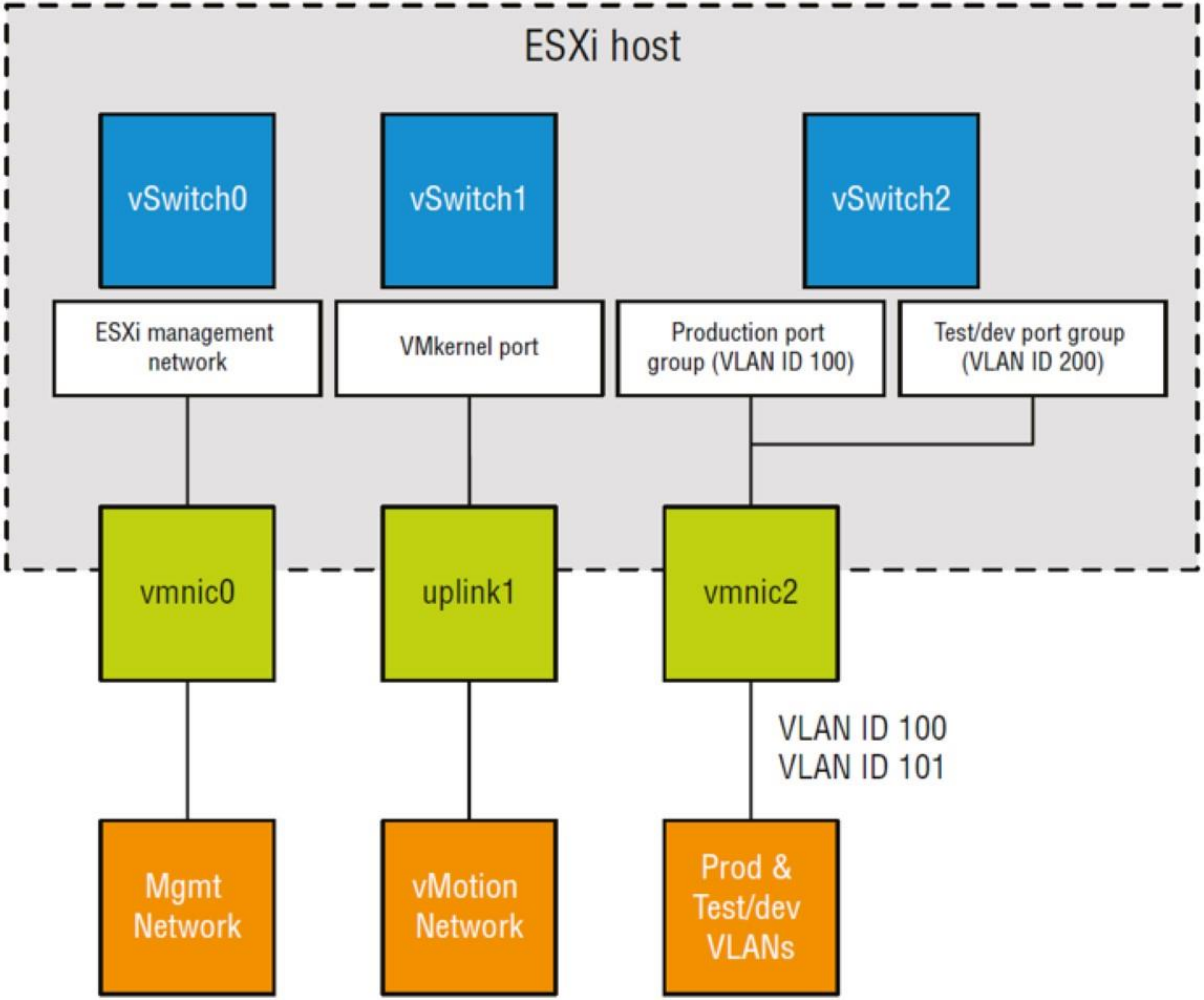


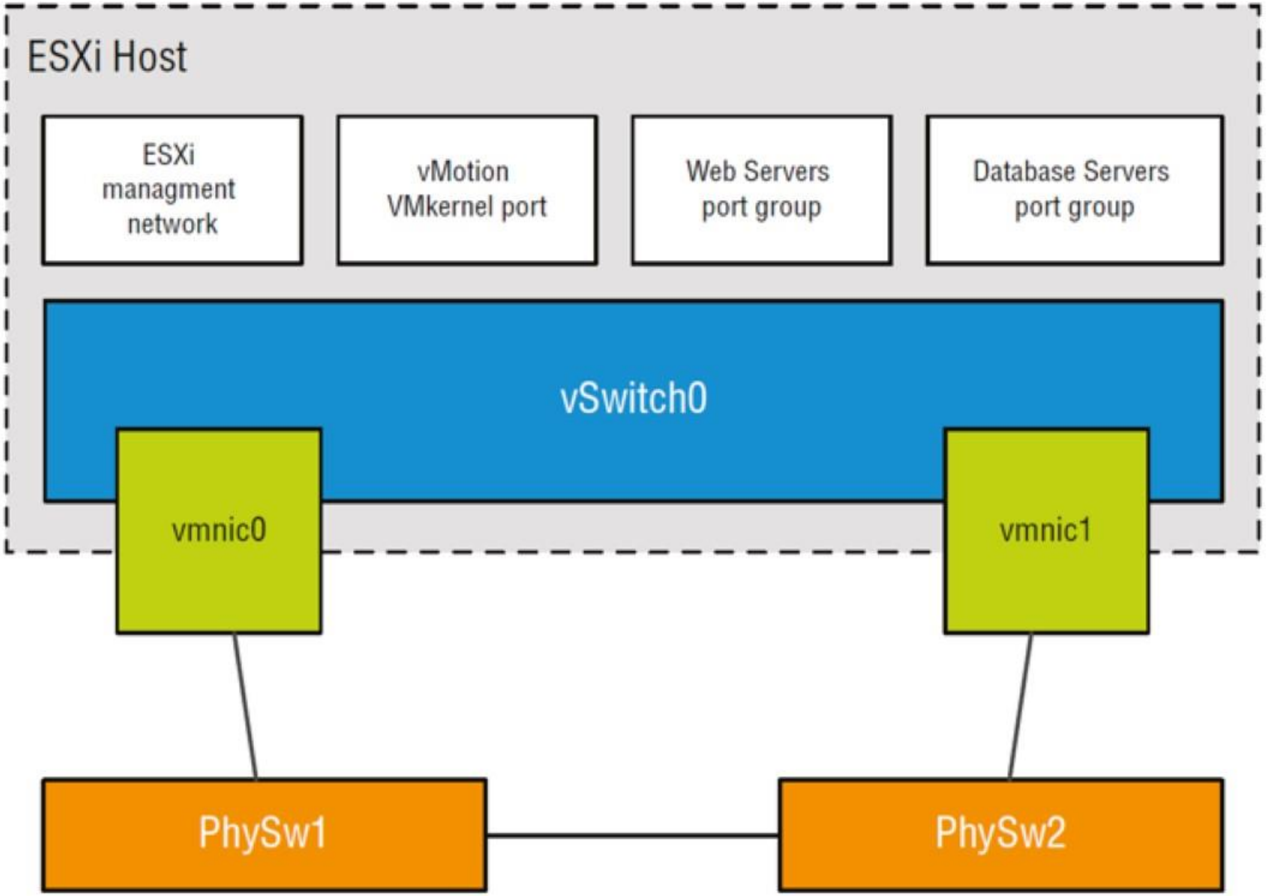
FIGURE 5.25
VLANs can reduce the number of vSwitches, uplinks, and cabling required.



2.vSphere Standard Switch

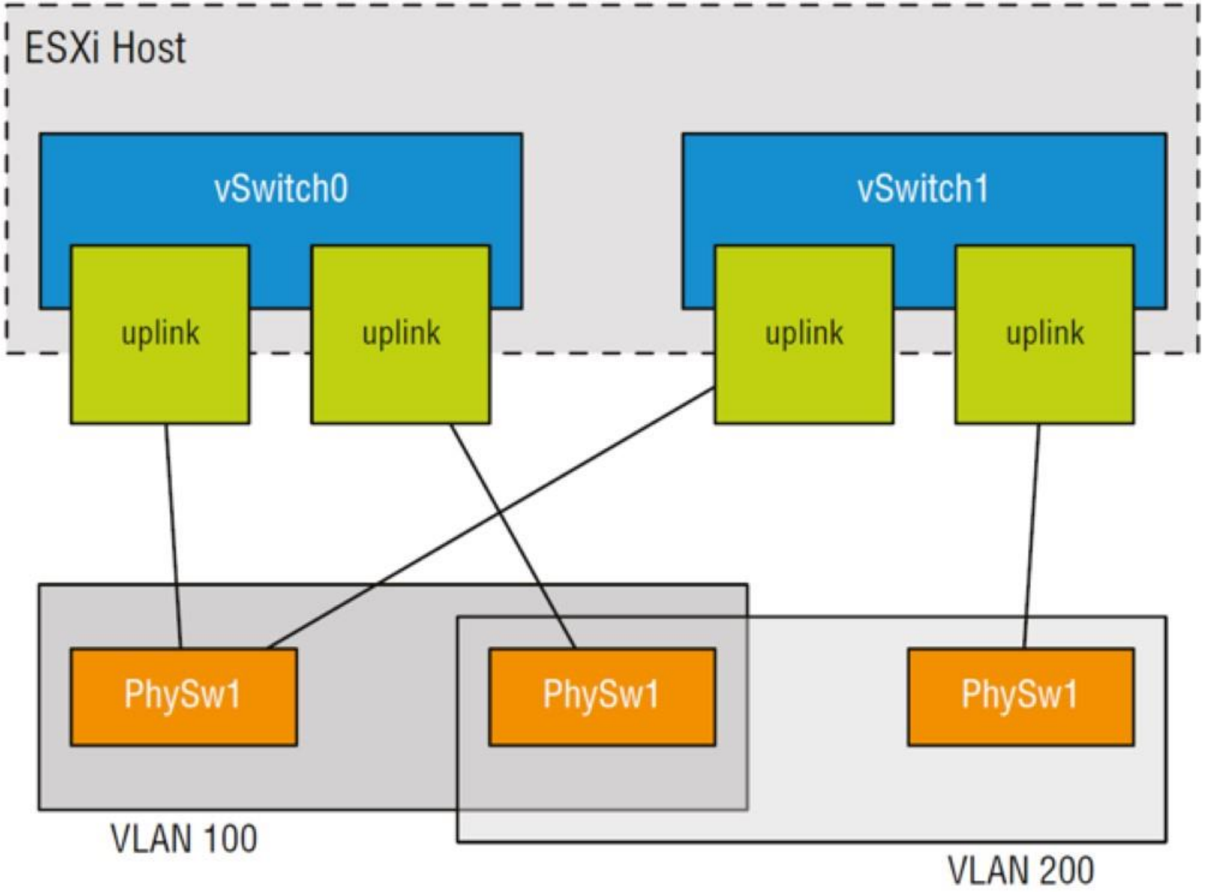
2.5Configuring NIC Teaming

FIGURE 5.28
Virtual switches with multiple uplinks offer redundancy and load balancing.



2.vSphere Standard Switch

FIGURE 5.30
All the physical network adapters in a NIC team must carry the same VLANs.



3.Case

- 基于VMware WorkStation Pro + GNS3实现VLAN
  - VMware ESXi：10.10.100.0/24
  - vSwitch 1：10.10.101.0/24 VLAN ID：1001
  - vSwitch 2：10.10.102.0/24 VLAN ID：1002
  - vSwitch 3：10.10.103.0/24 VLAN ID：1003
  - vSwitch 4：10.10.104.0/24 VLAN ID：1004

3.Case

- 基于Sugon A620 + Physical Switch实现vSwitch
  - 每台服务器两个网卡接口，实现负载均衡

  - VMware ESXi：10.10.100.0/24
  - vSwitch 1：10.10.101.0/24 VLAN ID：1001
  - vSwitch 2：10.10.102.0/24 VLAN ID：1002
  - vSwitch 3：10.10.103.0/24 VLAN ID：1003
  - vSwitch 4：10.10.104.0/24 VLAN ID：1004