

云计算与虚拟化技术



第6讲：vSphere Network and NSX

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

2021.10

讨论提纲

□ vSphere Network

- Virtual Network: OSI、Encapsulation、MAC、MTU、VLAN、TCP vs UDP、IPv6
- vSphere Virtual Network Components

□ vSphere Standard Switch

- vSphere Standard Switch (vSwitch)
- vSphere Distributed Switch (VDS)
- 使用vSphere Standard Switches *
- 使用Port Groups *
- 配置Virtual Switch Security

□ 案例:

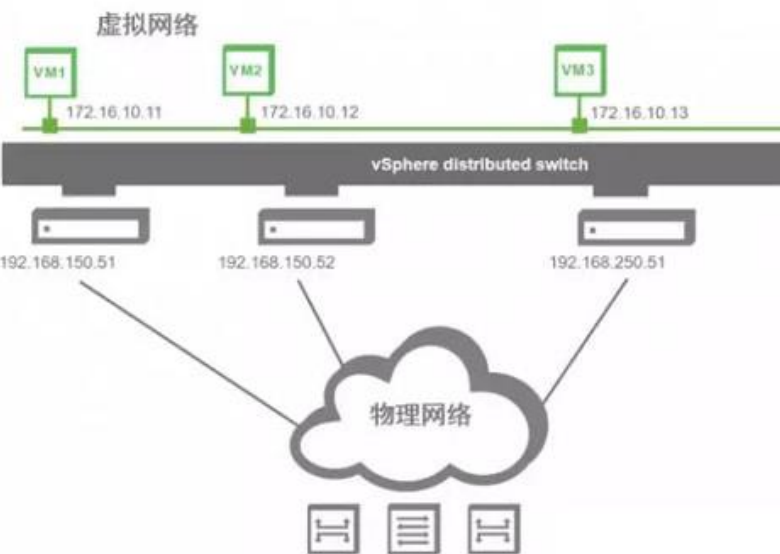
- 支持多VLAN的vSwitch实现方案
- 支持多网卡的VM实现方案

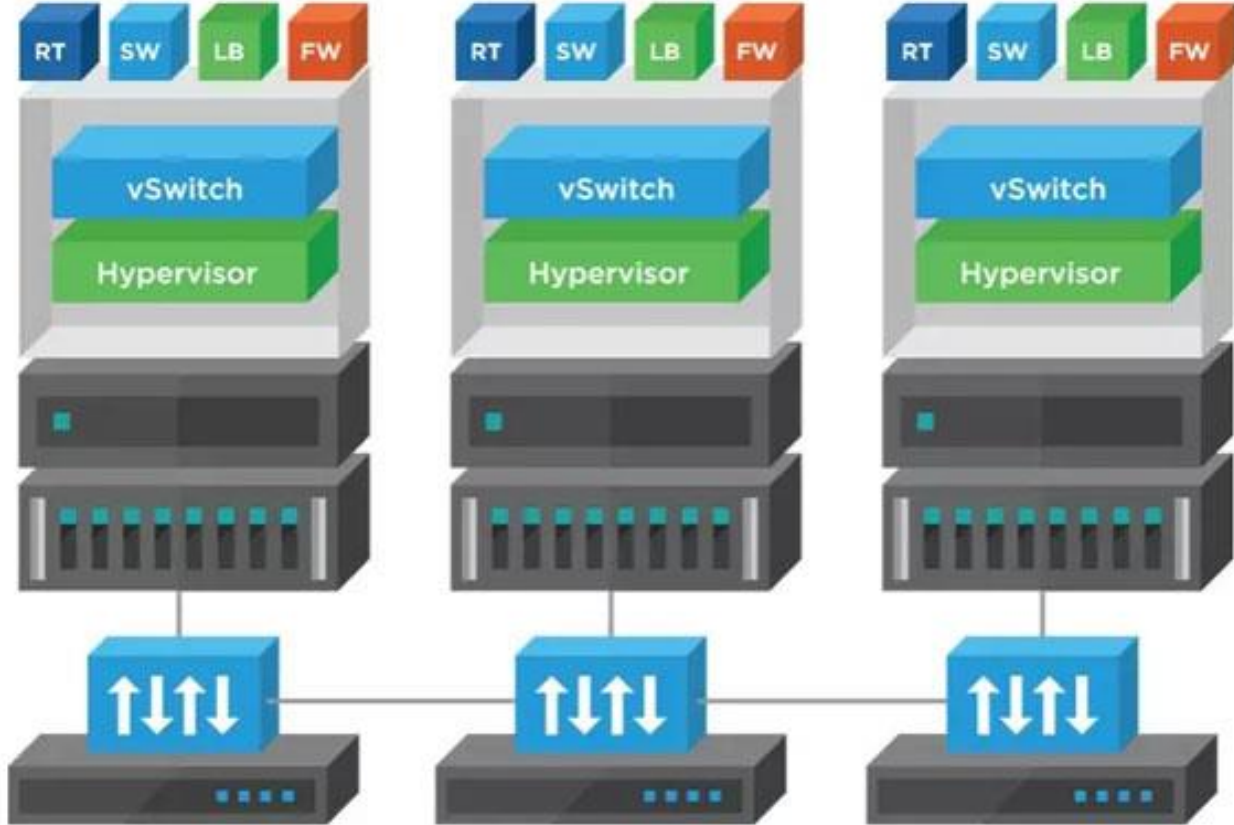


1.vSphere Network

- 网络是VMware基础设施的重要组成部分。
 - 传统数据中心使用物理网络。
 - 建设数据中心之前，就根据业务需求提前规划网络，完成网络设计。
 - 服务器接入不同设备，或使用VLAN接入交换机不同端口，区分不同业务系统。
 - 在基于 vSphere 的软件定义的数据中心中，VM都连接在 Hypervisor 所提供的的一个虚拟交换机上。交换机横跨 vSphere 集群的ESXi服务器的，称之为分布式交换机 (Distributed Switch)。
 - 所有VM的网络通讯都通过虚拟交换机来实现的，也可以通过软件来实现更多网络功能，这个软件就是VMware NSX。
 - VMware NSX来自于VMware在2012年收购的Nicia。



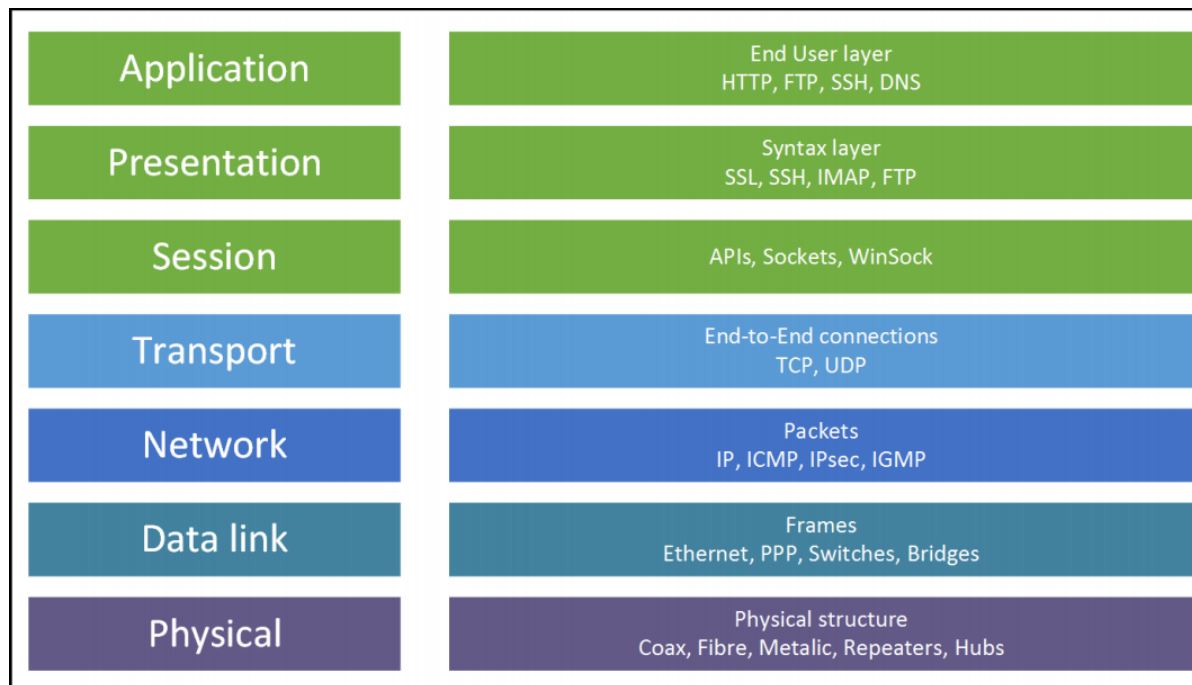




1.vSphere Network

1.1 Virtual Network

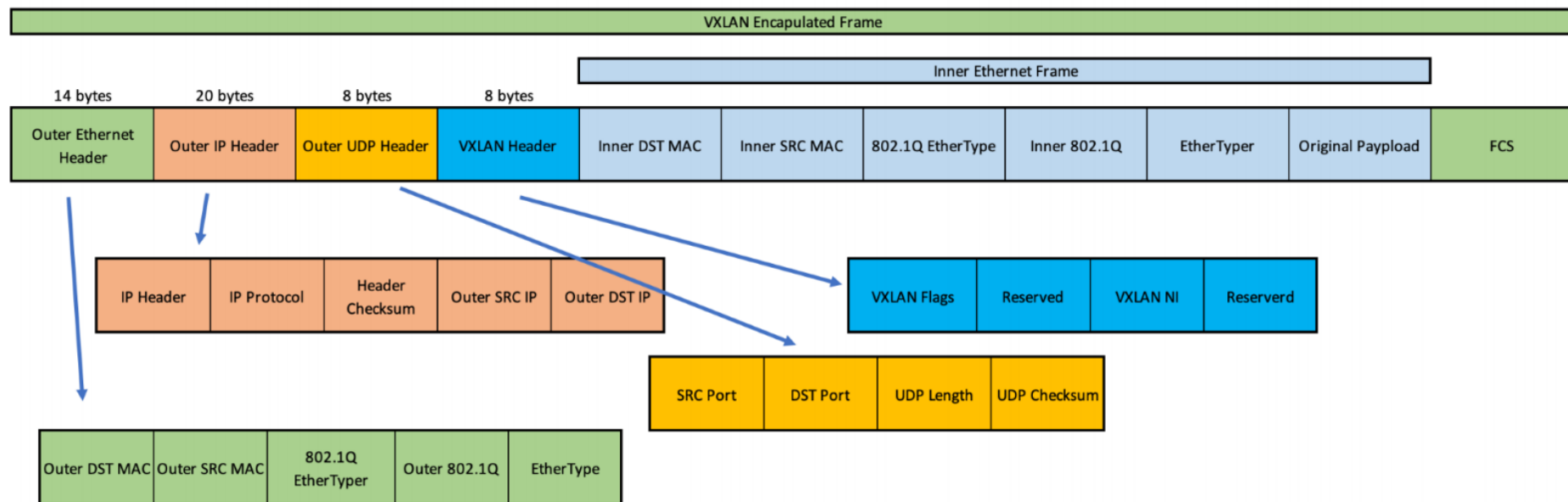
- OSI model
 - NSX支持L2 - L7



1.vSphere Network

1.1 Virtual Network

- 封装与解封装 (Encapsulation and de-encapsulation)
 - 通过网络传输的信息必须在通信的发送和接收端进行转换过程。
 - 转换过程是封装和接封装。这一点在《计算机网络原理》课程中已经充分介绍。
 - 在软件定义的网络中，使用vxlan。



1.vSphere Network

1.1 Virtual Network

- MAC转发表与自学习协议 (MAC tables and MAC learning process)
 - 物理交换机使用MAC转发表来执行帧转发。
 - 物理交换机通过自学习协议来构建MAC转发表。
 - 地址解析协议(ARP)可以发现与已知IP地址相对应的MAC地址，以便允许构建第2层数据包。
 - 在VMware ESXi中，查看ARP的命令是：`tcpdump-uw arp`



BBT-Cloud-node-1 - VMware - X

https://10.10.1.15/ui/#/host

vmware ESXi

root@10.10.1.15 | 帮助 | 搜索

主机

管理

监控

虚拟机

存储

网络

BBT-Cloud-node-1

使用 vCenter Server 管理 | 创建/注册虚拟机 | 关机 | 重新引导 | 刷新 | 操作

BBT-Cloud-node-1

版本: 6.7.0 Update 2 (Build 13009603)
状态: 正常 (已连接到 vCenter Server, 位于 10.10.1.250)
正常运行时间: 56.82 天

此主机由 vCenter Server 管理。vCenter Server 可以自动执行这些操作。无需干预。操作

ESXi shell 已在此主机上启用。只有出于管理目的需要时才应禁用 shell。操作

SSH 已在此主机上启用。只有出于管理目的需要时才应禁用 SSH。操作

硬件

制造商: Sugon

型号: 2400063524000741

CPU: 16 CPUs x AMD Opteron(TM) Processor 6320

内存: 127.98 GB

永久内存: 0 B

虚拟闪存: 0 B 已用, 0 B 容量

网络

主机名: BBT-Cloud-node-1

IP 地址: 1 vmk0: 10.10.1.15

DNS 服务器: 1.10.10.3.70

默认网关: 10.10.1.1

IPv6 已启用: 否

主机适配器: 2

网络

名称: VM Network-102

存储

物理适配器: 5

数据存储

名称: StudioCloud-SAN-1-SYSTEM-1, StudioCloud-SAN-1-SYSTEM-2, StudioCloud-SAN-2-SYSTEM-1, StudioCloud-SAN-2-SYSTEM-2

近期任务

任务: 目标

Hosts

Port Forwarding

History

see www.vmware.com/go/sysadmintools for details.

The ESXi Shell can be disabled by an administrative user. See the vSphere Security documentation for more information.

[root@BBT-Cloud-node-1:~] tcpdump -uw arp

```

tcpdump -uw: verbose output suppressed, use -v or -vv for full protocol decode
listening on vmk0, link-type ETHERNET, capture size 262144 bytes
08:17:48.899271 ARP, Request who-has 10.10.1.25 tell 10.10.1.24, length 46
08:17:52.001429 ARP, Request who-has 10.10.1.1 tell 10.10.1.24, length 46
08:17:52.729108 ARP, Request who-has 10.10.1.252 tell 10.10.1.253, length 46
08:18:24.159892 ARP, Request who-has 10.0.0.1 tell 10.0.0.89, length 46
08:18:36.000674 ARP, Request who-has 10.10.1.10 tell 10.10.1.24, length 46
08:18:40.728720 ARP, Request who-has 10.10.1.1 tell 10.10.1.117, length 46
08:19:03.904246 ARP, Request who-has 10.10.1.254 tell 10.10.1.12, length 46
08:19:07.723357 ARP, Request who-has 10.10.1.140 tell 10.10.1.1, length 46
08:19:07.724282 ARP, Request who-has 10.10.1.140 tell 10.10.1.1, length 46
08:19:07.724293 ARP, Request who-has 10.10.1.140 tell 10.10.1.1, length 46
08:19:07.724302 ARP, Request who-has 10.10.1.140 tell 10.10.1.1, length 46
08:19:11.184199 ARP, Request who-has 10.10.1.140 tell 10.10.1.1, length 46
08:19:11.184285 ARP, Request who-has 10.10.1.140 tell 10.10.1.1, length 46
08:19:11.184298 ARP, Request who-has 10.10.1.140 tell 10.10.1.1, length 46
08:19:11.184358 ARP, Request who-has 10.10.1.140 tell 10.10.1.1, length 46
08:19:13.286837 ARP, Request who-has 10.10.1.254 tell 10.10.1.13, length 46
08:19:14.207614 ARP, Request who-has 10.10.1.140 tell 10.10.1.1, length 46
08:19:14.207668 ARP, Request who-has 10.10.1.140 tell 10.10.1.1, length 46
08:19:14.207696 ARP, Request who-has 10.10.1.140 tell 10.10.1.1, length 46
08:19:14.207781 ARP, Request who-has 10.10.1.140 tell 10.10.1.1, length 46
08:19:15.549458 ARP, Request who-has 10.10.1.1 tell 10.10.1.27, length 46
08:19:22.108606 ARP, Request who-has 10.10.1.250 tell BBT-Cloud-node-1, length 28
08:19:22.109723 ARP, Reply 10.10.1.250 is-at 00:8c:29:b9:ff:9d (oui Unknown), length 46
08:19:22.246459 ARP, Request who-has 10.10.1.250 tell 10.10.1.16, length 46
08:19:22.247505 ARP, Request who-has 10.10.1.250 tell 10.10.1.17, length 46
08:19:38.432158 ARP, Request who-has 10.10.1.254 tell 10.10.1.14, length 46
08:19:40.132704 ARP, Request who-has 10.10.1.254 tell 10.10.1.11, length 46

27 packets captured
27 packets received by filter
0 packets dropped by kernel
[root@BBT-Cloud-node-1:~] esxcli network ip neighbor list
Neighbor      Mac Address      vmknic  Expiry  State  Type
-----
10.10.1.1     00:22:93:5b:14:b1 vmk0    1117 sec Unknown
10.10.1.5     e8:61:1f:12:95:58 vmk0    1004 sec Unknown
10.10.1.17    bc:ee:7b:11:99:ff vmk0    1125 sec Unknown
10.10.1.16    bc:ee:7b:1c:c6:fe vmk0    1125 sec Unknown
10.10.1.18    bc:ee:7b:1c:c5:fe vmk0    39 sec  Unknown
10.10.1.250   00:8c:29:b9:ff:9d vmk0    1125 sec Unknown
[root@BBT-Cloud-node-1:~]

```

INVITE TEAMMATES

CPU: 44.1 GHz, 2% 可用, 44.8 GHz 容量

内存: 109.17 GB, 15% 可用, 127.98 GB 容量

存储: 30.82 TB, 2% 可用, 31.61 TB 容量

的虚拟机内存(占满)

120
100
80
60
40
20
0

16:19

时间

1.vSphere Network

1.1 Virtual Network

□ MTU (Maximum Transmission Unit)

- 根据IEEE802.3规范，有效的以太网帧大小为64到1518字节，有效载荷从46到1500字节。
- 目前已经基于标准开发了不同的IEEE标准，支持扩展以太网帧。
 - VLAN tagging (802.1Q)
 - This is with an additional four bytes in the Ethernet header.
 - Provider Bridge (PB) 802.1ad:
 - This is with an additional eight bytes to the original frame to support service and customer tagging.
 - FCoE frames:
 - These have an MTU of 2,500 bytes.
 - Multiprotocol Label Switching (MPLS):
 - This increases the maximum Ethernet frame size to 1,518 bytes + (n * 4 bytes), where n is the number of stacked labels.
 - VXLAN:
 - This adds another 50 bytes.
 - Jumbo frames:
 - These are Ethernet frames with more than 1,500 bytes of payload, typically around 9,000 bytes. They are mostly used for IP-based storage traffic.



1.vSphere Network

1.1 Virtual Network

- MTU (Maximum Transmission Unit)
 - 作为最佳实践，应该对iSCSI或NFS流量使用大型帧(MTU 9000)。
 - 如果不使用大型帧，将大数据报文切到小帧的开销可能会影响IP存储的性能。
 - MTU单元的详细信息推荐阅读：
 - RFC 781: <https://tools.ietf.org/html/rfc791>
 - RFC 1191: <https://tools.ietf.org/html/rfc1191>
 - https://en.wikipedia.org/wiki/Maximum_transmission_unit
 - 在VMware ESXi上为iSCSI或NFS流量使用巨型帧，推荐官方文档KBKB1007654
 - <https://kb.vmware.com/s/article/1007654>



1.vSphere Network

1.1 Virtual Network

- VLAN (Virtual LAN)
 - VLAN是一个广播域。
 - 可以用VLAN分割以太网广播域。
 - 端口可配一个(访问模式或未标记模式)或多个VLAN(中继模式或标记模式)
 - VMware vSphere支持：
 - External VLAN Tagging: 外部VLAN标记, 仅在物理交换机
 - Virtual Switch VLAN Tagging: 虚拟交换机VLAN标记
 - VM VLAN Tagging: 虚拟机VLAN标记





4 bytes



2 bytes



2 bytes



3 bits

1 bit

12 bits



1.vSphere Network

1.1 Virtual Network

□ IPv6

- VMware vSphere同时支持IPv4和IPv6。
 - 从vSphere 4.1 开始，同时支持IPv4和IPv6，但默认禁用了IPv6支持。
 - 从vSphere 5.1 开始，默认启用IPv6。
 - 建议不要关闭IPv6支持。
 - 因为Linux和Windows操作系统都默认启用IPv6，虚拟化层面关闭IPv6可能产生错误
 - 如果不使用IPv6，则保持缺省即可。



1.vSphere Network

1.2 vSphere Virtual Network Components

- 使用VMware ESXi 和 vCSA构建Virtual Network，与构建物理网络逻辑上是相似的，但在操作和术语上有一定的差别。
- vSphere Virtual Network包含的术语和组件如下。
 - vSphere Standard Switch
 - 在VMKernel中由软件实现的基本交换机，为VM提供流量管理。
 - 必须通过ESXi进行管理，在每一台ESXi主机上配置。
 - 本课程使用此类型交换机，简称为vSwitch。
 - vSphere Distributed Switch
 - 在VMKernel中由软件实现的基本交换机，为VM和VMKernel提供流量管理。
 - 可以在vSphere创建的数据中心内，被ESXi主机和集群共享和管理。
 - 本课程不使用此类型交换机，简称为VDS。



1.vSphere Network

1.2 vSphere Virtual Network Components

- vSphere Virtual Network包含的术语和组件如下。
 - Port/Port Group
 - VMKernel Port
 - 专用虚拟交换机端口类型，配置IP地址，用于对Traffic、vMotion、vSAN、iSCSI storage、Network File System(NFS)、vSphere Replication、FT的管理。
 - Virtual Machine Port Group
 - 提供给VM使用的虚拟交换机端口，对应于物理交换机的接入端口。
 - Virtual LAN (VLAN)
 - Trunk Port (Trunking)
 - Access Port
 - Network Interface Card Team
 - 物理端口聚合，将多个端口聚合为一个逻辑端口实现负载均衡和容错。



1.vSphere Network

1.2 vSphere Virtual Network Components

- vSphere Virtual Network为VM提供的网络适配器(网卡)类型。
 - VMXNET Adapter
 - VMware提供的虚拟网络适配器，没有相对应的硬件网卡设备型号。
 - VMware对VM使用此网络适配器有针对性的进行了性能优化。
 - 通常操作系统是不会内置该适配器类型的驱动程序。
 - VM需要安装VMware Tools，即可获得VMXNET的驱动程序。
 - VMXNET 2 Adapter
 - 基于VMXNET实现，针对大型帧、硬件热插拔等网络高性能特性进行优化。
 - VMXNET 3 Adapter
 - 与VMXNET和VMXNET 2无关，不是升级版本。
 - 包含VMXNET 2所有功能，添加许多新功能。例如：多队列支持、IPv6卸载、MSI/MSI-X interrupt delivery。
 - 需要安装VMware Tool，以获得驱动程序。
 - E1000 Adapter
 - 模拟Intel 82545EM Gigabit network adapter的虚拟网卡。
 - E1000e Adapter
 - 模拟Intel 82574 Gigabit network adapter的虚拟网卡。
 - 需要VM硬件版本为8及以上版本支持。



- 其他虚拟机设备配置
- 从 ESXi 主机到虚拟机的 USB 配置
- 从客户端计算机到虚拟机的 USB 配置
- 将共享智能读卡器添加到虚拟机
- 使用虚拟机可信平台模块保护虚拟机
- 配置虚拟机选项
- 使用 vSphere vApp 管理多层应用程序
- 使用 vCenter Solutions Manager 监控解决方案
- 管理虚拟机
- 升级虚拟机
- 常见任务的所需特权
- 故障排除概览
- 虚拟机故障排除

虚拟机兼容性所支持的功能

功能	ESXi 6.7 Update 2 及更高版本	ESXi 6.7 或更高版本	ESXi 6.5 及更高版本	ESXi 6.0 及更高版本	ESXi 5.5 及更高版本	ESXi 5.1 及更高版本	ESXi 5.0 及更高版本	ESX/ESXi 4.x 及更高版本	ESX/ESXi 3.5 及更高版本
硬件版本	15	14	13	11	10	9	8	7	4
内存最大值 (GB)	6128	6128	6128	4080	1011	1011	1011	255	64
最大逻辑处理器数目	256	128	128	128	64	64	32	8	4
每个插槽的最大内核数 (虚拟 CPU)	64	64	64	64	64	64	32	8	1
最大 SCSI 适配器数	4	4	4	4	4	4	4	4	4
Bus Logic 适配器	Y	Y	Y	Y	Y	Y	Y	Y	Y
LSI Logic 适配器	Y	Y	Y	Y	Y	Y	Y	Y	Y
LSI Logic SAS 适配器	Y	Y	Y	Y	Y	Y	Y	Y	N
VMware 虚拟控制器	Y	Y	Y	Y	Y	Y	Y	Y	N
SATA 控制器	4	4	4	4	4	N	N	N	N
NVMe 控制器	4	4	4	N	N	N	N	N	N
虚拟 SCSI 磁盘	Y	Y	Y	Y	Y	Y	Y	Y	Y
SCSI 直通	Y	Y	Y	Y	Y	Y	Y	Y	Y
SCSI 热添加支持	Y	Y	Y	Y	Y	Y	Y	Y	Y
IDE 节点	Y	Y	Y	Y	Y	Y	Y	Y	Y
虚拟 IDE 磁盘	Y	Y	Y	Y	Y	Y	Y	Y	N
虚拟 IDE CD-ROM	Y	Y	Y	Y	Y	Y	Y	Y	Y
IDE 热添加支持	N	N	N	N	N	N	N	N	N
最大网卡数	10	10	10	10	10	10	10	10	4
PCNet32	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMXNet	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMXNet2	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMXNet3	Y	Y	Y	Y	Y	Y	Y	Y	N
E1000	Y	Y	Y	Y	Y	Y	Y	Y	Y
E1000e	Y	Y	Y	Y	Y	Y	Y	N	N
USB 1x 和	Y	Y	Y	Y	Y	Y	Y	Y	N

1.vSphere Network

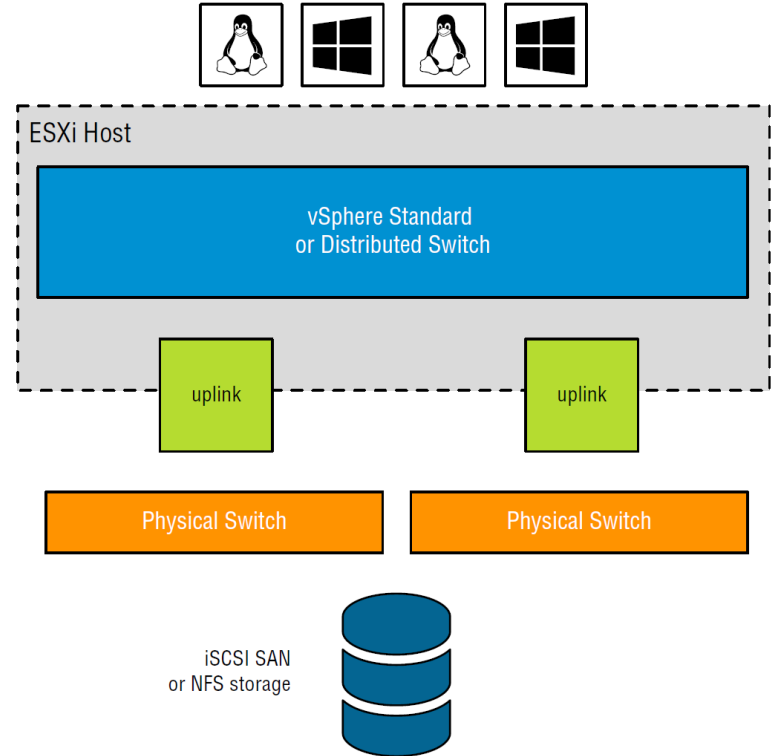
1.2 vSphere Virtual Network Components

□ vSphere Virtual Network

- 不是简单的虚拟网络。
- 必须和物理网络、网络接口卡、虚拟交换机结合起来。
- 虚拟网络设计，必须综合考虑通信的整体需求，充分结合物理环境、现有网络管理方案、网络设备型号后，进行整体设计。

FIGURE 5.1

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



2.vSphere Standard Switch

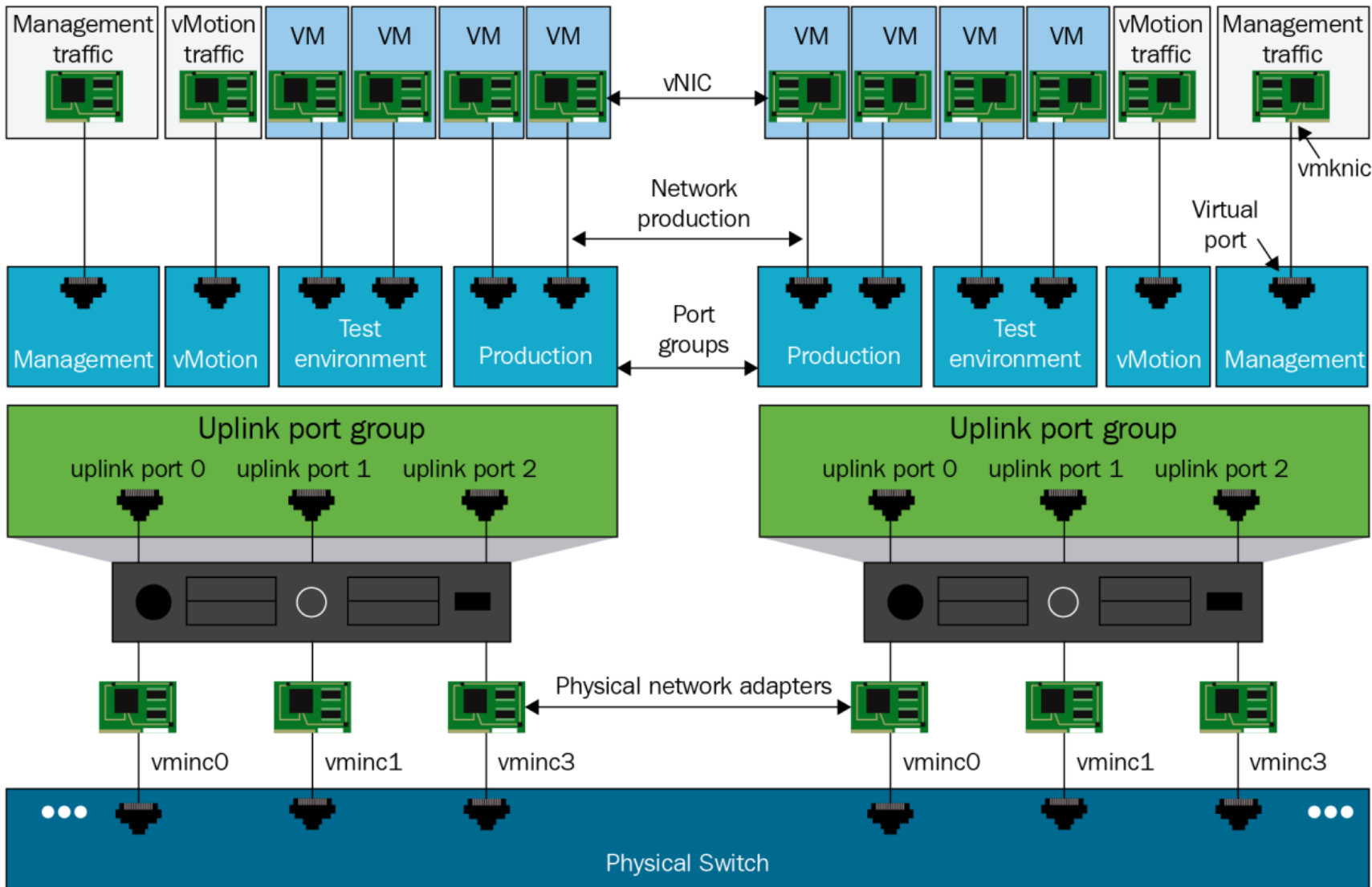
2.1 vSwitch

- vSphere Standard Switch (vSwitch) 用于将虚拟机和VMKernel Port与物理上行网络接口卡互连。
 - vSwitch的创建和管理方式：
 - vSphere Web Client
 - vSphere Cli using the esxcli command
 - vSwitch能够支持的通信：
 - 同一ESXi主机内的VM与VM之间通信
 - 不同ESXi主机上的VM与VM之间通信
 - VM与物理网络上主机或者其他VM通信
 - VMKernel进行网络管理、vMonitor、VMware vSAN、iSCSI、NFS、vSphere Replication、FT日志等



ESXi host 1

ESXi host 2

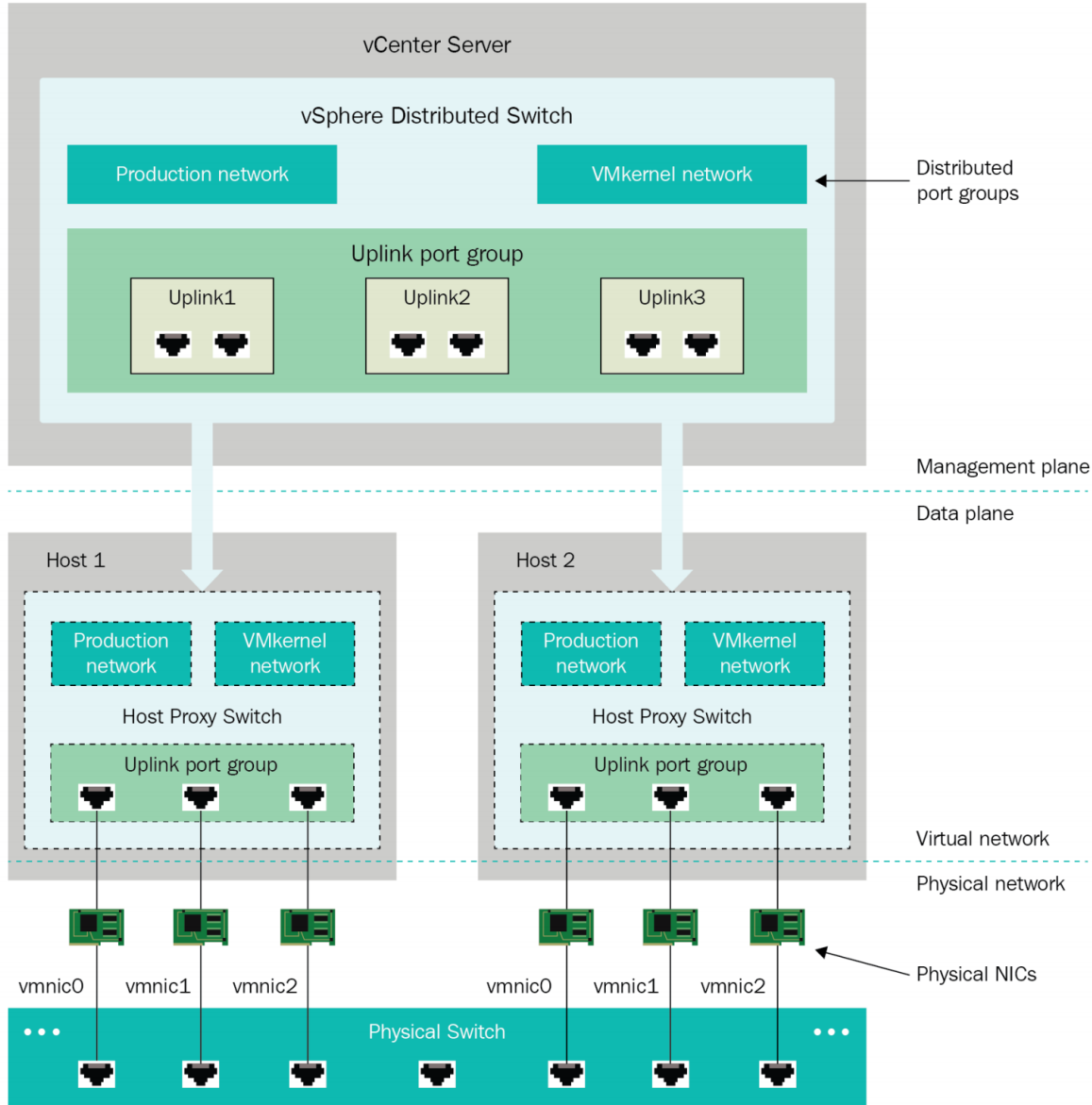


2.vSphere Standard Switch

2.2 VDS

- vSphere Distributed Switch (VDS)是数据中心所有关联ESXi主机的单一虚拟交换机。
 - VDS的创建和管理方式：
 - 在vCSA上进行配置，然后同步到ESXi主机
 - ESXi主机上无法自行配置
 - 使用vSphere Web Client进行
 - VDS能够支持的通信：
 - VMKernel和VM之间通信
 - 通过物理接口与外部网络通信
 - 通过VLAN实现网络分割
 - 支持Load Balancing、Failback、Security、Traffic shaping policies
 - 支持vSwitch的所有功能





Feature	Standard vSwitch	Distributed vSwitch
L2 forwarding	Yes	Yes
VLAN support	Yes	Yes
NIC teaming	Yes	Yes
Outbound traffic shaping	Yes	Yes
Inbound traffic shaping	No	Yes
Centralized management	No	Yes
PVLAN support	No	Yes
Netflow export support	No	Yes
Port mirroring	No	Yes
Multicast support	No	Yes
Traffic filtering	No	Yes
Network IO control	No	Yes



2.vSphere Standard Switch

2.3 使用vSphere Standard Switches

□ 使用vSwitch

■ 创建方法

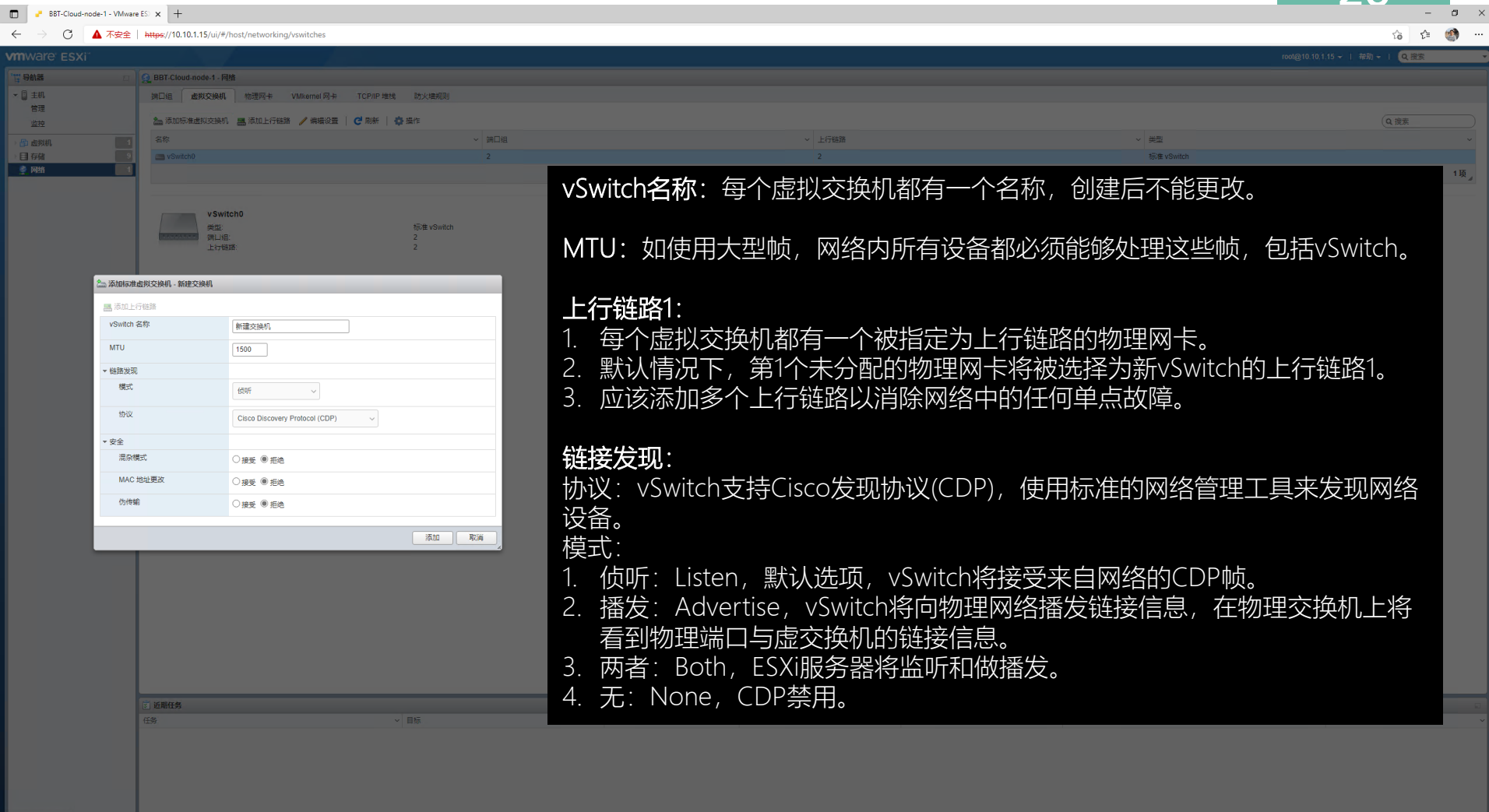
□ 使用vSphere Host Client (建议)

□ 通过vCSA创建

□ 通过ESXi CLI创建

- `esxcli network vswitch standard add --vswitch-name=newvswitch`
- `esxcli network vswitch standard set --cdp-status=listen --vswitch-name=newvswitch`
- `esxcli network vswitch standard set --mtu=9000 --vswitch-name=newvswitch`
- `esxcli network vswitch standard uplink add --uplink-name=vmnic --vswitch-name=newvswitch`
- `esxcli network vswitch standard policy failover set --vswitch-name=newvswitch`
- `esxcli network vswitch standard policy security set --vswitch-name=newvswitch`
- `esxcli network vswitch standard policy shaping set --vswitch-name=newvswitch`





vSwitch名称：每个虚拟交换机都有一个名称，创建后不能更改。

MTU：如使用大型帧，网络内所有设备都必须能够处理这些帧，包括vSwitch。

上行链路1：

1. 每个虚拟交换机都有一个被指定为上行链路的物理网卡。
2. 默认情况下，第1个未分配的物理网卡将被选择为新vSwitch的上行链路1。
3. 应该添加多个上行链路以消除网络中的任何单点故障。

链接发现：

协议：vSwitch支持Cisco发现协议(CDP)，使用标准的网络管理工具来发现网络设备。

模式：

1. 侦听：Listen，默认选项，vSwitch将接受来自网络的CDP帧。
2. 播发：Advertise，vSwitch将向物理网络播发链接信息，在物理交换机上将看到物理端口与虚交换机的链接信息。
3. 两者：Both，ESXi服务器将监听和做播发。
4. 无：None，CDP禁用。

名称	端口组	上行链路	类型
vSwitch0	2	2	标准 vSwitch

添加标准虚拟交换机 - 新建交换机

添加上行链路

vSwitch 名称: 新建交换机

MTU: 1500

链路发现

模式: 侦听

协议: Cisco Discovery Protocol (CDP)

安全

混杂模式: 接受 拒绝

MAC 地址更改: 接受 拒绝

伪传输: 接受 拒绝

添加 取消

安全性:

混杂模式:

- 拒绝: 默认选项。VM不接收其他VM的帧。
- 接受: 通过虚拟交换机的所有帧都被转发到连接到虚拟交换机（或端口组）的所有虚拟机。这对于检测和监控流量或当使用流量嗅探器分析器时有用。

MAC地址更改:

- 拒绝: VM不可以自行修改网络适配器的MAC地址。
- 接受: 默认选项。VM可以更改网络适配器的MAC地址。

伪传输:

- 拒绝: vSwitch将丢弃任何来源MAC地址不是VM定义的数据帧。
- 接受: vSwitch不执行数据帧过滤功能，允许所有数据帧出站。

The screenshot displays the VMware ESXi Host Client interface. The left sidebar shows navigation options: 主机 (Host), 管理 (Manage), 监控 (Monitor), 虚拟机 (Virtual Machines), 存储 (Storage), 网络 (Network), and vSwitch0. The main content area is titled 'vSwitch0' and provides configuration details and a topology diagram.

vSwitch0 Configuration:

- 添加上行链路: 编辑设置 | 刷新 | 操作
- vSwitch0: 标准 vSwitch, 端口组: 2, 上行链路: 2

vSwitch 详细配置:

属性	值
MTU	1500
端口	6556 (6648 可用)
链路发现	侦听 / Cisco Discovery Protocol (CDP)
附加的虚拟机	1 (1 活动)
信标时间间隔	1

网卡绑定策略:

策略	值
通知交换机	是
策略	基于源端口 ID 的路由
反向策略	是
故障恢复	是

安全策略:

策略	值
允许混杂模式	否
允许伪传输	是
允许 MAC 更改	是


网桥策略:

策略	值
已启用	否

vSwitch 拓扑:

- VM Network-102: VLAN ID: 102, 虚拟机 (1): VM-10.10.2.180-VMware vRealize Operation Manager-Photon, MAC 地址: 00:50:56:ac:61:97
- Management Network: VLAN ID: 101, VMkernel 端口 (1): vmk0: 10.10.1.15
- 物理适配器: vmnic1, 1000 Mbps, 全双工; vmnic0, 1000 Mbps, 全双工

使用vSphere Host Client
查看vSwitch的拓扑信息



网卡绑定

负载均衡：
决定网络通信如何在网络适配器之间分配，根据四种算法之一：
(1) 基于源端口ID的路由：默认选项。
vSwitch基于VSS或VDS上VM端口ID选择上行链路。
该方法需要在物理交换机进行配置，并且计算开销较低。
(2) 基于源MAC哈希的路由：
vSwitch基于VM MAC地址选择一个上行链路。
vSwitch使用虚拟机MAC地址和上行链路数量计算VM上行链路。
该方法支持所有的物理交换机，而且开销较低。
(3) 基于IP哈希的路由：
vSwitch基于VMs数据包源IP地址和目的IP地址为每个数据报文选择上行链路。
该方法需要上行链路支持并开启802.3ad。
(4) 使用明确故障切换顺序：
此策略没有实现负载均衡。
vSwitch使用适配器列表中的第一个可用的上行链路。
如果第一个上行链路故障，将按照列表顺序使用下一个可用的上行链路。

名称	速度	状态
vmnic0	1000 Mbps, 全双工	活动
vmnic1	1000 Mbps, 全双工	待机

修改vSwitch配置信息

The screenshot shows the VMware ESXi vSphere Client interface for configuring vSwitch0. The 'Network' tab is active, and the 'Add Upstream Network' configuration window is open. The configuration includes:

- MTU:** 1500
- 上行链路 1:** vmnic0 - 启动, 1000 mbps
- 上行链路 2:** vmnic1 - 启动, 1000 mbps
- 链路发现:** 模式: 侦听, 协议: Cisco Discovery Protocol (CDP)
- 安全:** 混杂模式: 拒绝, MAC 地址更改: 接受, 伪传输: 接受
- 网卡绑定:** 负载平衡: 基于源端口 ID 的路由, 网络故障切换检测: 仅链路状态
- 通知交换机:** 启用
- 故障恢复:** 启用
- 故障切换顺序:**

名称	速度	状态
vmnic0	1000 Mbps, 全双工	活动
vmnic1	1000 Mbps, 全双工	待机
- 流量调整:** 状态: 禁用, 平均带宽: 100000 kbps, 峰值带宽: 100000 kbps, 突发大小: 102400 KB

网卡绑定

网络故障切换检测:

此选项定义如何判断一个上行链接为不可用。

判断链路不可用的方法有两种:

(1) 仅链路状态: 默认选项。

仅检测链路故障, 例如拔掉电缆或物理连通性故障。

(2) 仅信标:

使用此检测模式须至少有3个网卡来进行信标探测。

发送并侦听物理NIC发送的以太网广播帧, 检测所有物理NIC中的链路故障。

ESXi主机每秒钟发送一次信标数据包。

通知交换机:

此选项是单一选项, 默认启用, 用于加快物理交换机能够快速改变网络拓扑。

当vSwitch链接的物理交换机端口发生变化时, vSwitch通过网络发送通知, 以通知物理交换机更新MAC查找表。

使用的协议是反向地址解析协议(RARP)。

修改vSwitch配置信息

The screenshot shows the VMware ESXi vSwitch configuration page for vSwitch0. The configuration includes:

- 添加上行链路:** MTU set to 1500. Two uplinks are configured: 上行链路 1 (vmnic0 - 启动, 1000 mbps) and 上行链路 2 (vmnic1 - 启动, 1000 mbps).
- 链路发现:** 模式 set to 侦听, 协议 set to Cisco Discovery Protocol (CDP).
- 安全:** 混杂模式 (disabled), MAC 地址更改 (accept), 伪传输 (accept).
- 网卡绑定:** 负载平衡 set to 基于源端口 ID 的路由, 网络故障切换检测 set to 仅链路状态.
- 通知交换机:** 启用.
- 故障恢复:** 启用.
- 故障切换顺序:** A table showing the order of network adapters:

名称	速度	状态
vmnic0	1000 Mbps, 全双工	活动
vmnic1	1000 Mbps, 全双工	待机
- 流量调整:** 状态 set to 禁用. Average bandwidth, peak bandwidth, and burst size are all set to 1000000.

网卡绑定

故障恢复:

此选项是单一选项，默认启用，决定物理适配器从故障恢复后如何处理。默认启用时，物理适配器恢复正常后，将立即处于可用状态。

故障切换顺序:

此选项对所有物理适配器进行列表排序。

可以通过“上移”、“下移”进行排序。

可以通过“标记为活动”、“标记为待机”改变物理适配器的工作状态。

修改vSwitch配置信息

The screenshot shows the VMware ESXi vSwitch configuration page for vSwitch0. The '流量调整' (Traffic Control) section is expanded, showing the following settings:

- 状态: 已启用 禁用
- 平均带宽: 1000000 kb/s
- 峰值带宽: 1000000 kb/s
- 突发大小: 1024000 KB

Below the traffic control settings, there is a table showing the status of network adapters:

名称	速度	状态
vmnic0	1000 Mbps, 全双工	活动
vmnic1	1000 Mbps, 全双工	待机

流量调整

状态:

启用流量调整或者禁用。默认情况下将禁用此选项。

平均带宽 (kbit/s) : 定义平均负载的上限。

峰值带宽 (kbit/s) : 定义突发流量时的上限。

突发大小(KB): 定义达到峰值时能够发送的最大字节总数。

修改vSwitch配置信息

The screenshot shows the vSphere Client interface for a virtual switch named '10.10.116'. The '配置' (Configuration) tab is active, showing the '虚拟交换机' (Virtual Switch) configuration. A modal dialog titled '10.10.116 - 添加网络' (10.10.116 - Add Network) is open, guiding the user through the process of adding a network. The dialog has four steps: 1. 选择连接类型 (Select connection type), 2. 选择目标设备 (Select target device), 3. 添加物理网络适配器 (Add physical network adapter), and 4. 即将完成 (Almost done). Under '选择连接类型', three options are listed: 'VMkernel 网络适配器' (VMkernel network adapter), '标准交换机的虚拟端口组' (Standard switch virtual port group), and '物理网络适配器' (Physical network adapter). The '物理网络适配器' option is selected and highlighted with a red box. A red arrow points from the '添加网络...' button in the background to this option. Another red arrow points from the '虚拟交换机' menu item in the left sidebar to the modal dialog. The background interface shows a list of virtual machines on the left and a 'Management Network' configuration in the main area.

10.10.116 - 添加网络

- 1 选择连接类型
- 2 选择目标设备
- 3 添加物理网络适配器
- 4 即将完成

选择连接类型
选择要创建的连接类型。

VMkernel 网络适配器
VMkernel TCP/IP 堆栈可处理以下 ESXi 服务的流量: vSphere vMotion、iSCSI、NFS、FCoE、Fault Tolerance、vSAN 和主机管理。

标准交换机的虚拟端口组
端口组将处理标准交换机上的虚拟机流量。

物理网络适配器
物理网络适配器处理网络中其他主机的网络流量。

CANCEL BACK NEXT

通过vCSA, 使用vSphere Client管理vSwitch

任务名称	开始时间	完成时间	服务器
检查新通知	2021/10/05 上午11:36:02	2021/10/05 上午11:38:02	10.101.250

全部 vSphere - 10.10.1... 12:17 21/10/05

2.vSphere Standard Switch

2.4 使用Port Groups

- 端口组： Port Groups
 - 端口组用于将VM和VMKernel接入到vSwitch。
 - ESXi安装后会默认创建两个端口组。
 - VM network：
 - 此端口组不包含任何虚拟机。
 - 在安装ESXi期间创建的默认使用vSwitch0的VM将使用此端口组。
 - Management network：
 - 用于ESXi的管理。



2.vSphere Standard Switch

2.4 使用Port Groups

□ 端口组：Port Groups

■ 创建方法

□ 使用vSphere Host Client (建议)

□ 通过vCSA创建

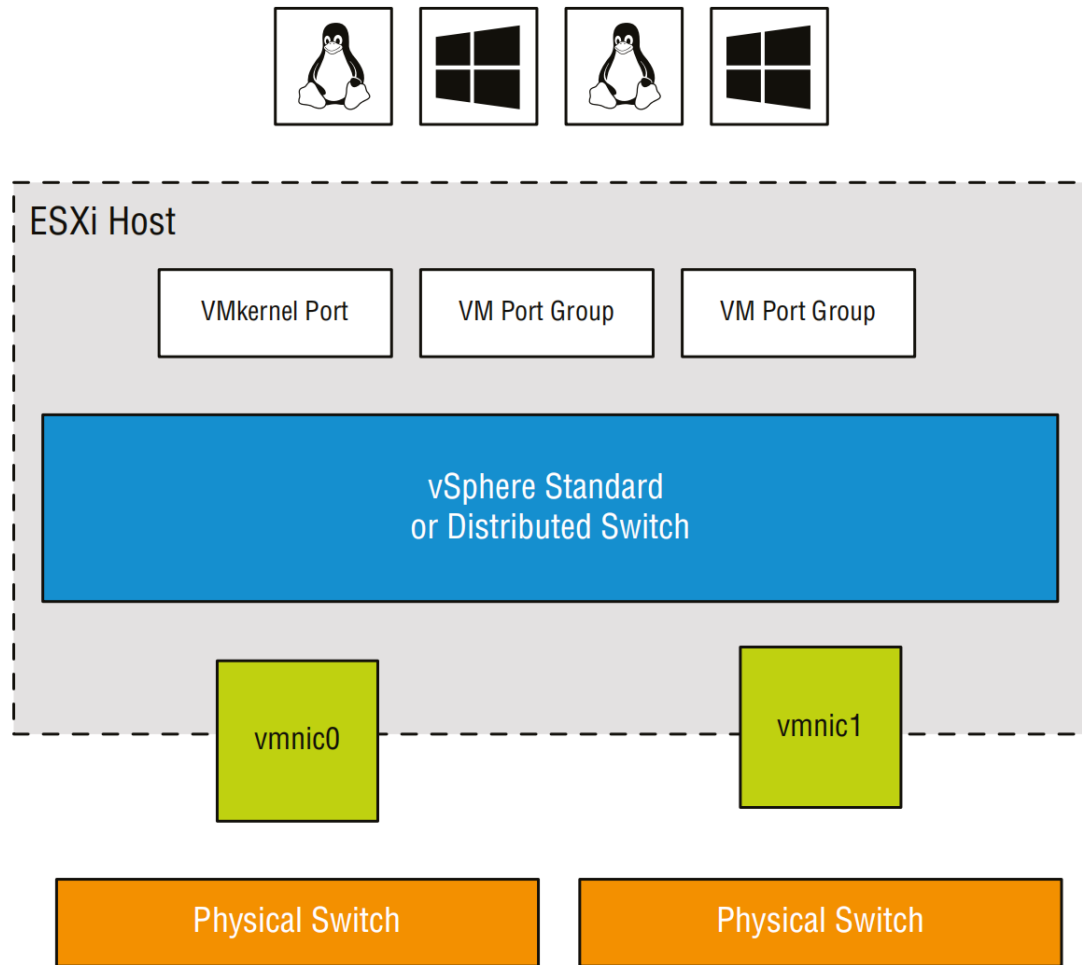
□ 通过ESXi CLI创建

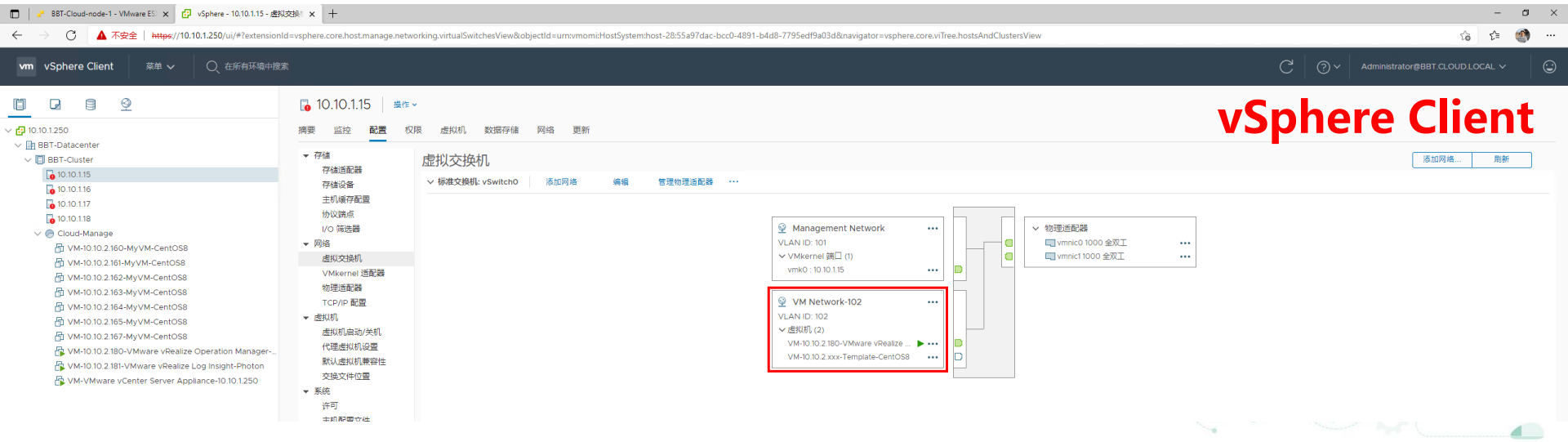
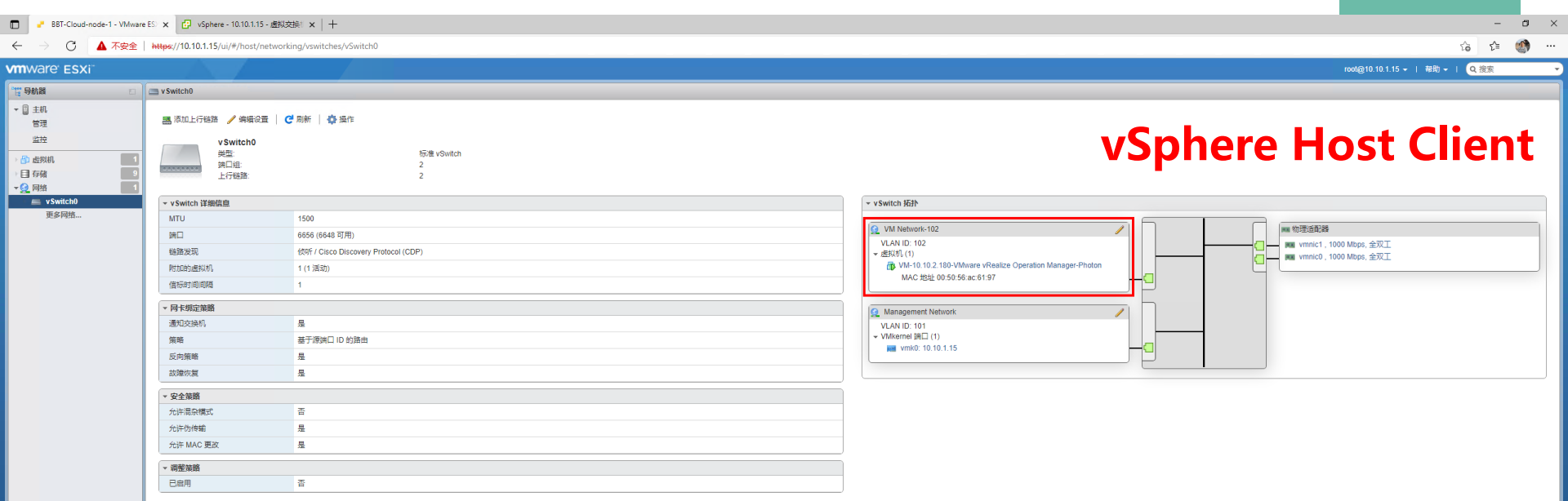
- `esxcli network vswitch standard portgroup add --portgroup-name=PGname --vswitch-name=vSwitch1`
- `esxcli network vswitch standard portgroup set -p PGname --vlan-id 1234`
- `esxcli network vswitch standard port group policy set`



FIGURE 5.3

Virtual switches can contain two connection types, a VMkernel port and a virtual machine port group.





vmware ESXi

BBT-Cloud-node-1 - 网络

名称	活动端口	VLAN ID	类型	vSwitch	虚拟机
VM Network-102	1	102	标准端口组	vSwitch0	1
Management Network	1	101	标准端口组	vSwitch0	不可用

添加端口组 - 新建端口组

名称: 新建端口组

VLAN ID: 0

虚拟交换机: vSwitch0

安全

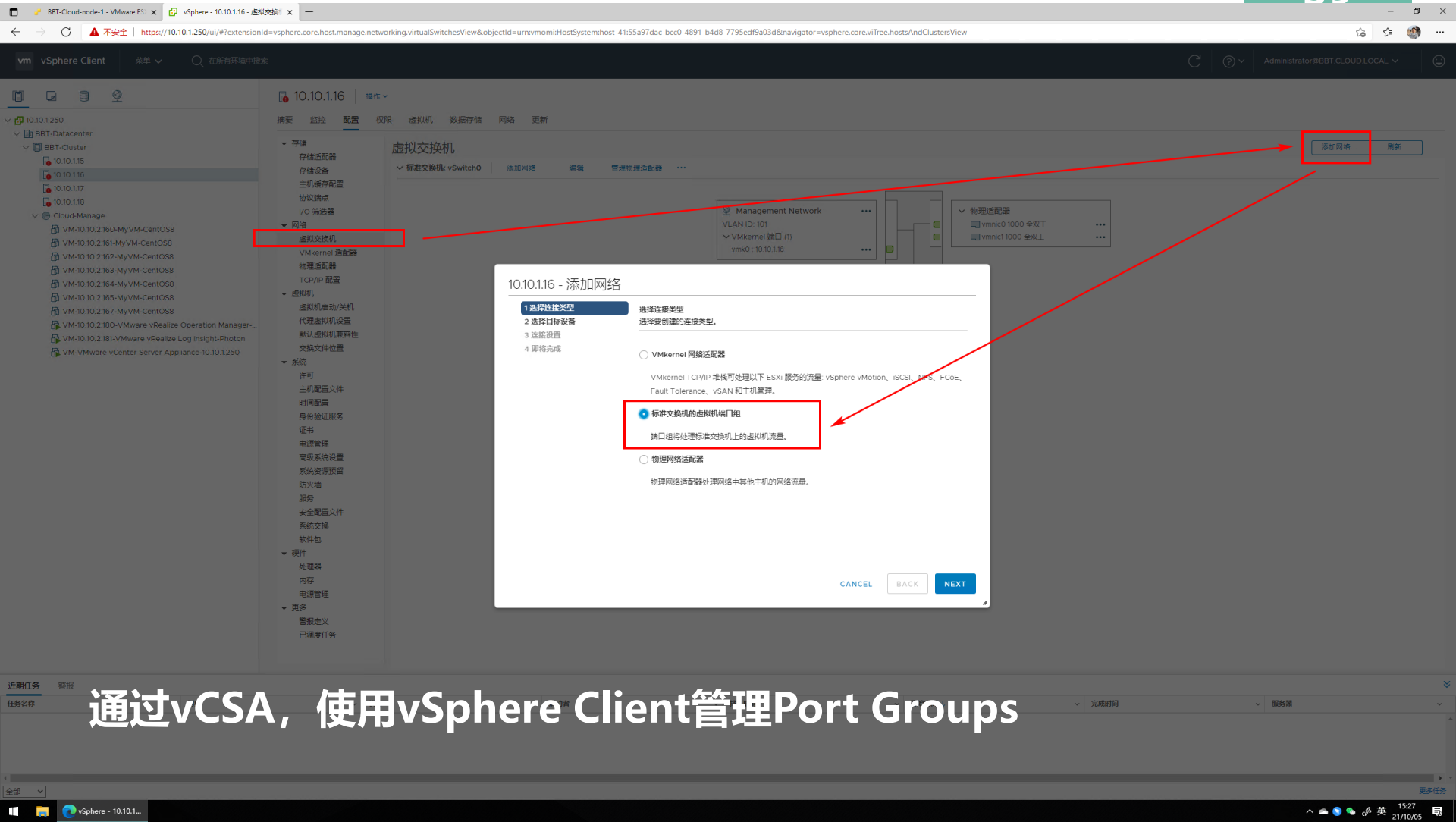
混杂模式: 接受 拒绝 从 vSwitch 继承

MAC 地址更改: 接受 拒绝 从 vSwitch 继承

伪传输: 接受 拒绝 从 vSwitch 继承

添加 取消

通过ESXi, 使用vSphere Host Client管理Port Groups



通过vCSA, 使用vSphere Client管理Port Groups

2.vSphere Standard Switch

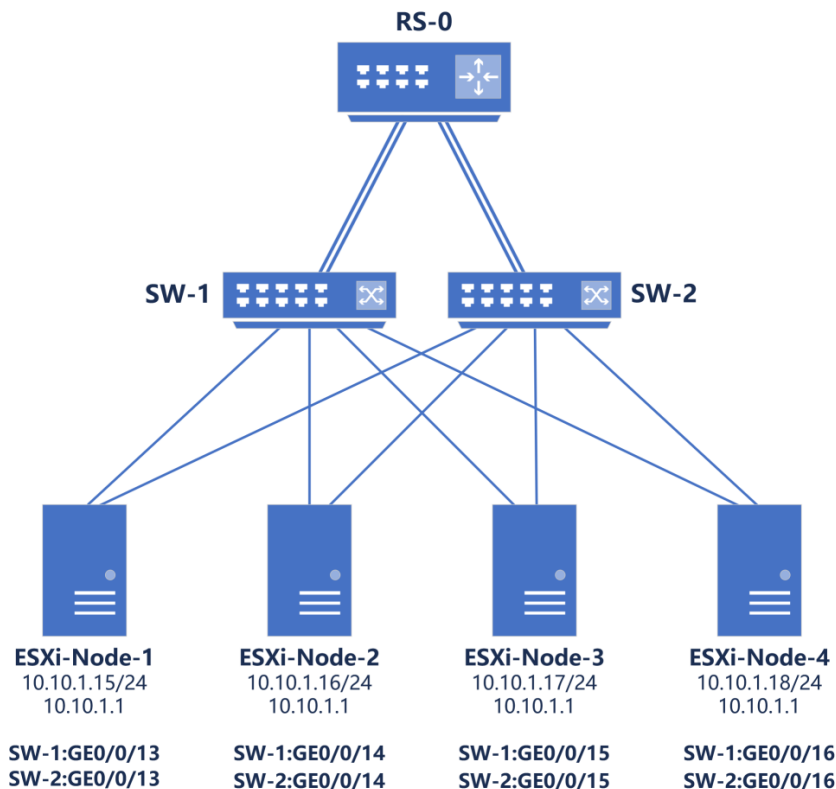
2.5 配置Virtual Switch Security

- vSwitch进行安全配置，可增强Layer 2的安全性。
 - 可以为vSwitch配置安全策略或端口组应用安全策略。
 - vSwitch的安全设置包括3个选项：
 - 混杂模式：Promiscuous mode
 - MAC地址更改：MAC address changes
 - 伪传输：Forged transmits
 - 通常建议在vSwitch上进行安全配置，端口组会自动集成。如果同时配置vSwitch和端口组，则端口组配置的优先级更高。



3.案例

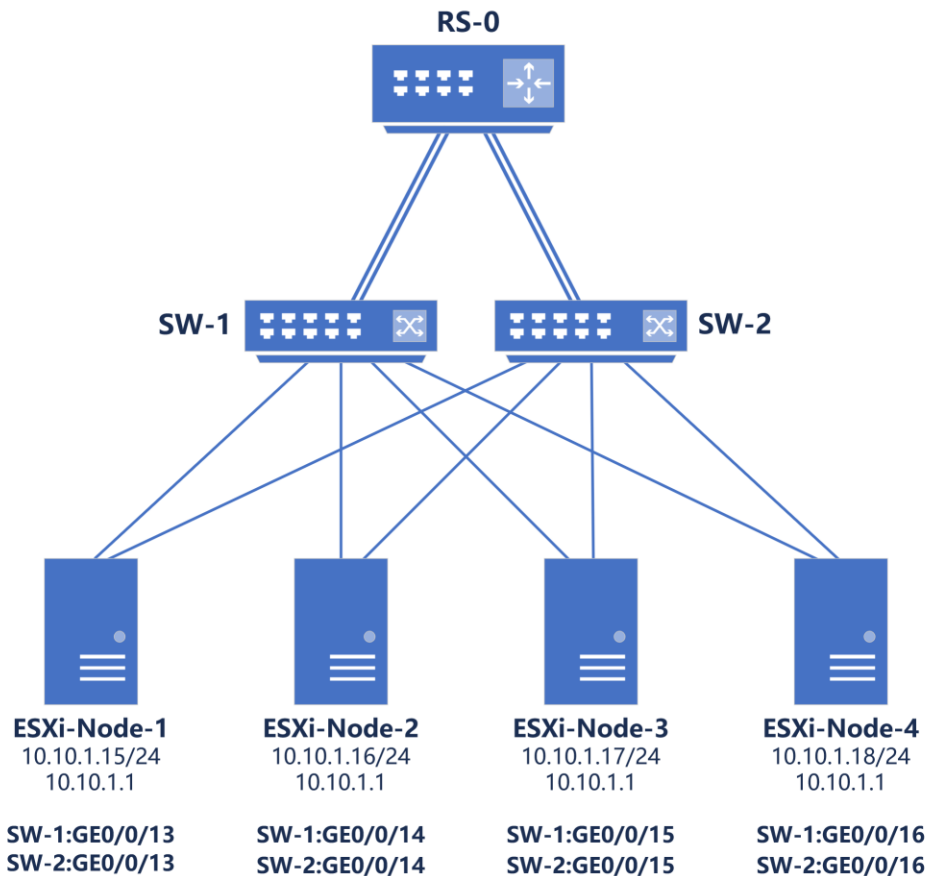
3.1 支持多VLAN的vSwitch实现方案



需求:

1. ESXi Host使用10.10.1.0/24
2. VM-A-Group使用10.10.2.0/24
3. VM-B-Group使用10.10.3.0/24
4. SW-1、SW-2使用VLAN区分
 - 10.10.1.0 vlan 101
 - 10.10.2.0 vlan 102
 - 10.10.3.0 vlan 103





```
[Network-Access-SW1]dis vlan
The total number of vlans is : 5
```

U: Up; D: Down; TG: Tagged; UT: Untagged;
 MP: Vlan-mapping; ST: Vlan-stacking;
 #: ProtocolTransparent-vlan; *: Management-vlan;

VID	Type	Ports
1	common	UT:GE0/0/1(U) GE0/0/2(U) GE0/0/3(U) GE0/0/4(U) GE0/0/5(U) GE0/0/6(U) GE0/0/7(U) GE0/0/8(U) GE0/0/9(U) GE0/0/10(U) GE0/0/11(U) GE0/0/12(U) GE0/0/13(U) GE0/0/14(U) GE0/0/15(U) GE0/0/16(U) GE0/0/17(U) GE0/0/18(U) Eth-Trunk0(U)
101	common	UT:GE0/0/19(D) GE0/0/20(U) TG:GE0/0/1(U) GE0/0/2(U) GE0/0/3(U) GE0/0/4(U) GE0/0/5(U) GE0/0/6(U) GE0/0/7(U) GE0/0/8(U) GE0/0/9(U) GE0/0/10(U) GE0/0/11(U) GE0/0/12(U) GE0/0/13(U) GE0/0/14(U) GE0/0/15(U) GE0/0/16(U) GE0/0/17(U) GE0/0/18(U) Eth-Trunk0(U)
102	common	TG:GE0/0/1(U) GE0/0/2(U) GE0/0/3(U) GE0/0/4(U) GE0/0/5(U) GE0/0/6(U) GE0/0/7(U) GE0/0/8(U) GE0/0/9(U) GE0/0/10(U) GE0/0/11(U) GE0/0/12(U) GE0/0/13(U) GE0/0/14(U) GE0/0/15(U) GE0/0/16(U) GE0/0/17(U) GE0/0/18(U) Eth-Trunk0(U)
103	common	TG:GE0/0/1(U) GE0/0/2(U) GE0/0/3(U) GE0/0/4(U) GE0/0/5(U) GE0/0/6(U) GE0/0/7(U) GE0/0/8(U) GE0/0/9(U) GE0/0/10(U) GE0/0/11(U) GE0/0/12(U) GE0/0/13(U) GE0/0/14(U) GE0/0/15(U) GE0/0/16(U) GE0/0/17(U) GE0/0/18(U) Eth-Trunk0(U)
104	common	TG:GE0/0/1(U) GE0/0/2(U) GE0/0/3(U) GE0/0/4(U) GE0/0/5(U) GE0/0/6(U) GE0/0/7(U) GE0/0/8(U) GE0/0/9(U) GE0/0/10(U) GE0/0/11(U) GE0/0/12(U) GE0/0/13(U) GE0/0/14(U) GE0/0/15(U) GE0/0/16(U) GE0/0/17(U) GE0/0/18(U) Eth-Trunk0(U)

VID	Status	Property	MAC-LRN	Statistics	Description
1	enable	default	enable	disable	VLAN 0001
101	enable	default	enable	disable	VLAN 0101
102	enable	default	enable	disable	VLAN 0102
103	enable	default	enable	disable	VLAN 0103
104	enable	default	enable	disable	VLAN 0104



