Installing Cisco Video Communications Server Expressway on a Business Edition 6000 Server

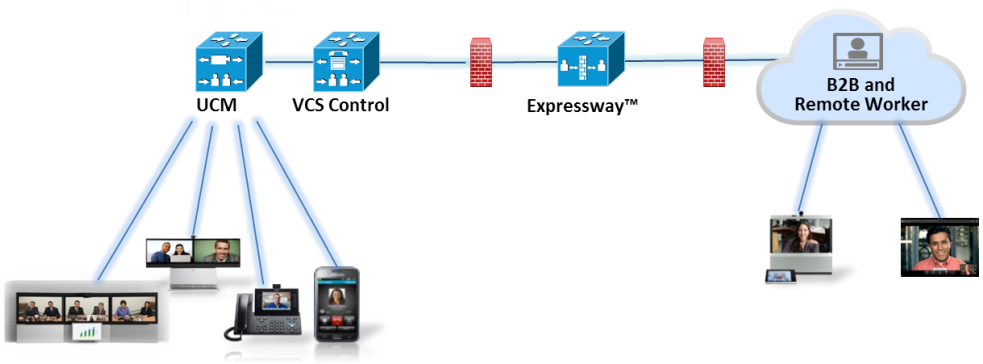
Introduction

A wide selection of applications can be installed on a Cisco Business Edition 6000 (BE 6000) server. Because of this functionality, you can consider a fully virtualized Video Communications Server Expressway (VCS-E) deployment using a common server platform.

VCS-E, when used with the Video Communications Server Control (VCS-C) application, allows you to make video calls between internal and external parties without the need for virtual private networks. To achieve this function, the VCS-E server is typically installed in a firewall demilitarized zone (DMZ) where the server may be reached from the public Internet and can communicate securely with the VCS-C server in the private domain (see Figure 1). When installed on a common virtualized host like the BE 6000, this secure network topology must be maintained.

This document illustrates a number of approaches to achieve these goals.

Figure 1 Target VCS Topology



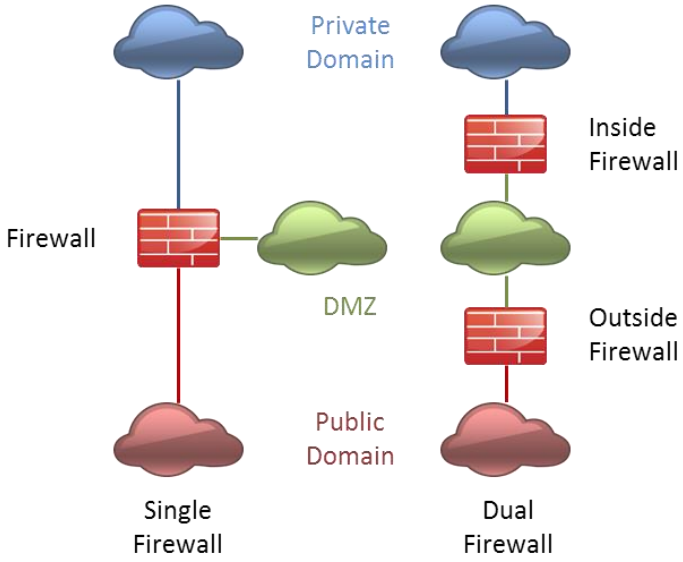
Deployment Options

For a co-resident deployment of VCS-E, the BE 6000 server has the flexibility to accommodate a number of different network design requirements.

Firewall Topology

The strategy that a business uses to implement a firewall DMZ and to protect the private domain will determine the connectivity requirements for the virtualised VCS-E. Figure 2 illustrates two of the most common approaches to firewall design. In the case of the single firewall design, VCS-E uses a single network connection to the firewall which is responsible for controlling the flow of traffic between the three security domains. In the dual firewall design, VCS-E requires separate network connections to access the public and private domains through the outside and inside firewalls. Licensing for Virtualized VCS-E includes the right to use a second network interface, allowing deployment with either architecture.

Figure 2 Firewall Designs



Layer Two Network Connectivity

When implementing the security domains that are shown in Figure 2, a business may choose to ensure the separation of network segments physically or logically. This separation might mean that dedicated Ethernet switches are used for each network segment, or that virtual LAN (VLAN) features are used to maintain separation within a common device. When using VLANs, connections to servers may use dedicated ports to ensure that the volume of traffic in one domain is not allowed to impact that in another. Alternatively, VLAN trunks may be used to optimise port usage.

The BE 6000 server, together with the bundled Virtualization Hypervisor, provide network connectivity and configuration options to accommodate any of these connectivity scenarios.

Connection Resiliency

The LAN architectures described above may also be made more resilient through the use of secondary network connections. The BE 6000 server offers support for interface teaming allowing both improved performance and protection against the loss of an individual link. Further information on interface teaming is provided in Appendix A.

System Capacity

The BE 6000 solution ships with a reduced footprint version of VCS which requires 4GB vRAM and permits up to 100 traversal and 100 non-traversal sessions. While this version is provided principally to build a VCS-C instance to use with the included promotional licenses, it may also be used to build VCS-E instances if required. Virtualized VCS-E licenses must be purchased separately. The BE 6000 part numbers may not be used to purchase VCS-E licensing. Should additional capacity be required, the standard VCS application package available from www.cisco.com/go/software may be used to build VCS-C or VCS-E instances, subject to the terms of the BE 6000 co-residency policy. This version requires 6GB vRAM and permits up to 100 traversal and 500 non-traversal sessions.

Introduction to VMware Hypervisor Networking

The Cisco Virtualization Hypervisor (VMware ESXi Hypervisor) includes the following networking concepts that you can use to implement the firewall designs discussed in the previous section.

vSwitch: A virtual implementation of a VLAN capable layer 2 switch within a host server. A vSwitch may or may not be connected to an external network.

Virtual Machine Port Group: Defines a template of port configuration options that may be assigned to and therefore group, vSwitch "ports." For the purposes of this document, each port group will essentially define a VLAN and its port membership.

Virtual Machine Network Adaptor: A virtual machine Ethernet interface. Each Network Adaptor may be associated with one Virtual Machine Port Group (and therefore one VLAN). Each Cisco application includes one or more Network Adapters.

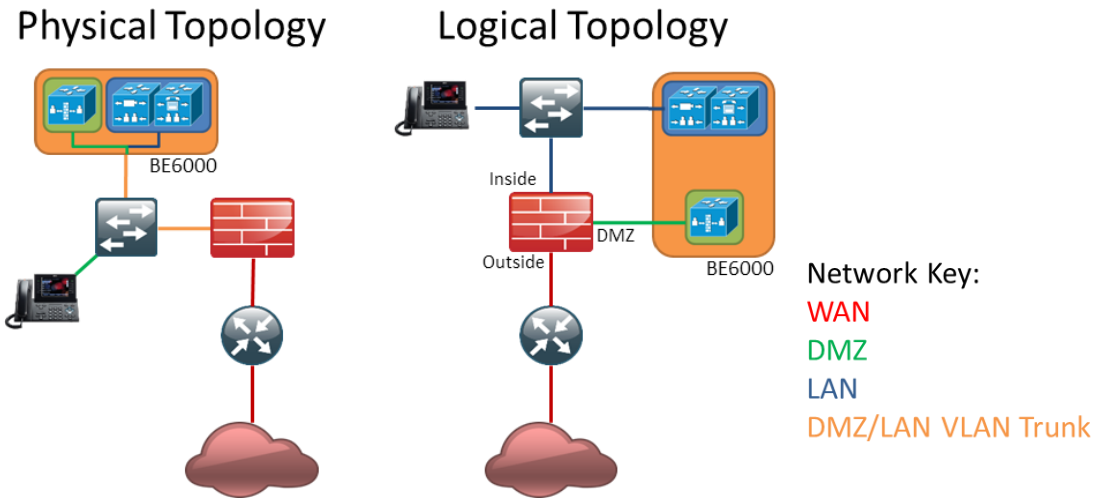
Physical Adapter: A physical host network interface which may be associated with a vSwitch to connect it with an external network. The physical adapter will automatically be configured as an 802.1q VLAN trunk (VLAN Switch Tagging mode) when multiple VLANs are created for its associated vSwitch.

Network Interface Card Teaming: Multiple physical adaptors may be associated with a vSwitch to increase connection bandwidth and protect against link loss. When teaming interfaces for improved throughput, all connections must be with the same switch. Further information on interface teaming is provided in Appendix A.

Configuration Procedure using Virtualized Networking

The following steps detail how to configure the Virtualization Hypervisor and the switched network to meet the needs of a single firewall solution with VLAN trunking as illustrated in Figure 3. See Appendix A for steps to add multiple physical connections to the server.

Figure 3: Example solution



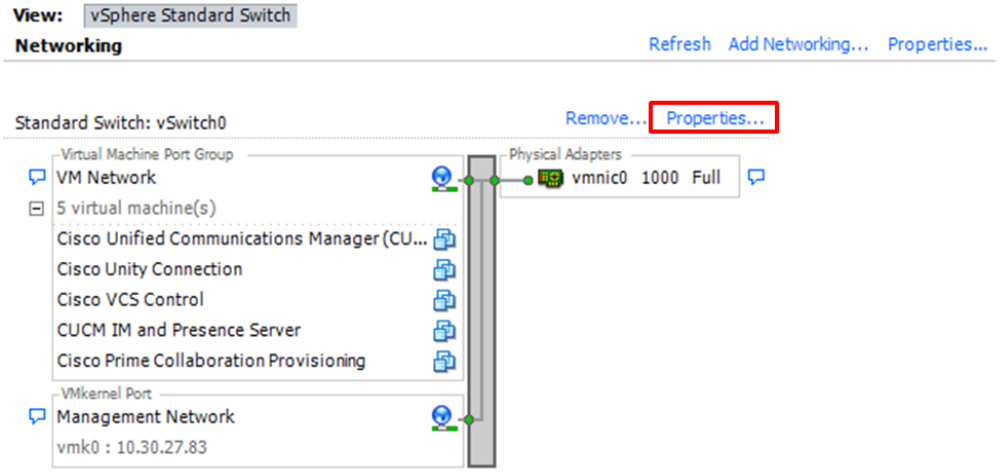
1. Configure the firewall to include a DMZ context or sub-network. Ensure that traffic policy rules are created to permit VCS-E communication with both internal and external networks. Full details of VCS-E IP Port use across public/DMZ and Private/DMZ boundaries are included in the following guide: http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/Cisco_VCS_IP_Port_Usage_for_Firewall_Traversal_Deployment_Guide_X7-2.pdf

2. Configure the layer 2 switch network to include a VLAN for DMZ traffic and ensure that this is mapped appropriately to the firewall DMZ port.
3. Configure the switch port assigned to the BE 6000 host as a VLAN trunk, ensuring that internal and DMZ networks only are allowed and connect it to the BE 6000 network interface 1. The following example illustrates how this can be configured using a Cisco Catalyst switch:

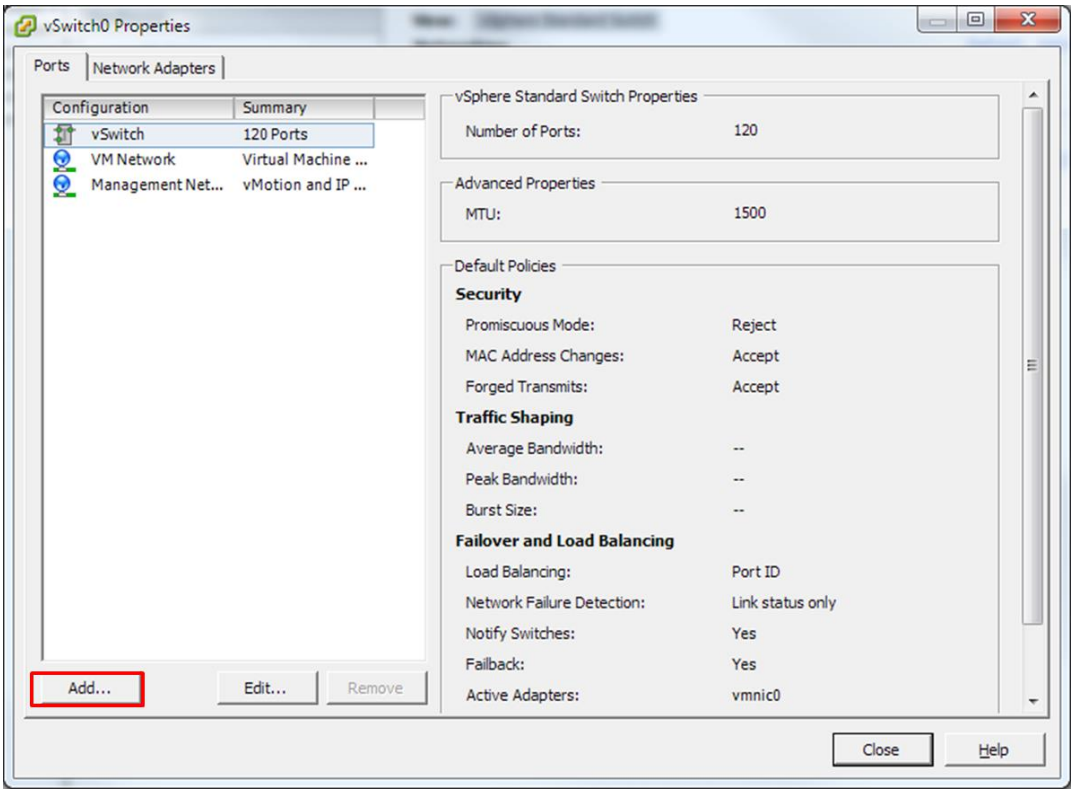
```
vlan 1
 name default
!
vlan 30
 name DMZ
!
interface GigabitEthernet1/1
 description BE 6000 Server Network Interface 1 (Internal/DMZ trunk)
 switchport trunk allowed vlan 1,30
 switchport mode trunk
 spanning-tree portfast trunk
!
```

Note: This example assumes that the native (untagged) VLAN is used for the internal network to correspond with the default hypervisor configuration. The use of VLAN 30 for the DMZ is for illustration purposes only. Any VLAN ID may be used for this purpose.

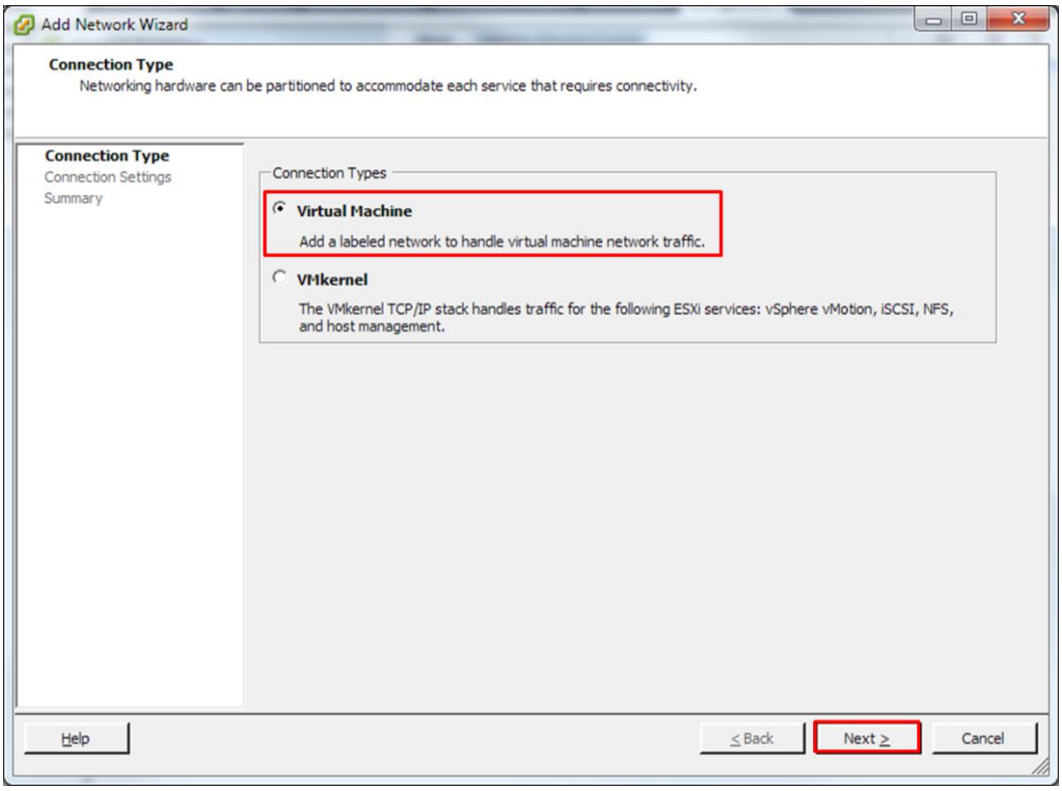
4. Use the vSphere client to configure the hypervisor networking features as follows:
    a. Access the network configuration screen by clicking the host icon in the left hand inventory panel, then selecting the **Networking** option from the **Configuration** tab. Note that core BE 6000 applications have been configured to use the default virtual machine port group. Click on **properties** for vSwitch0 to access the switch configuration screen.



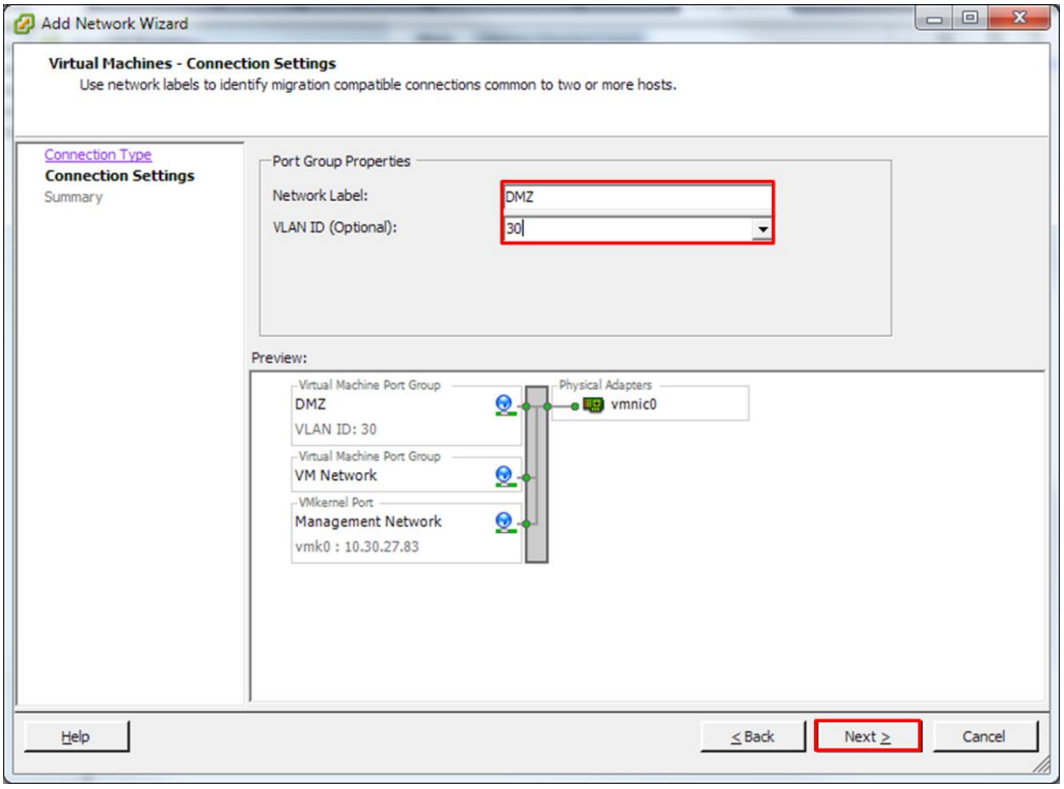
    b. Click **Add...** to start the Add Network Wizard.



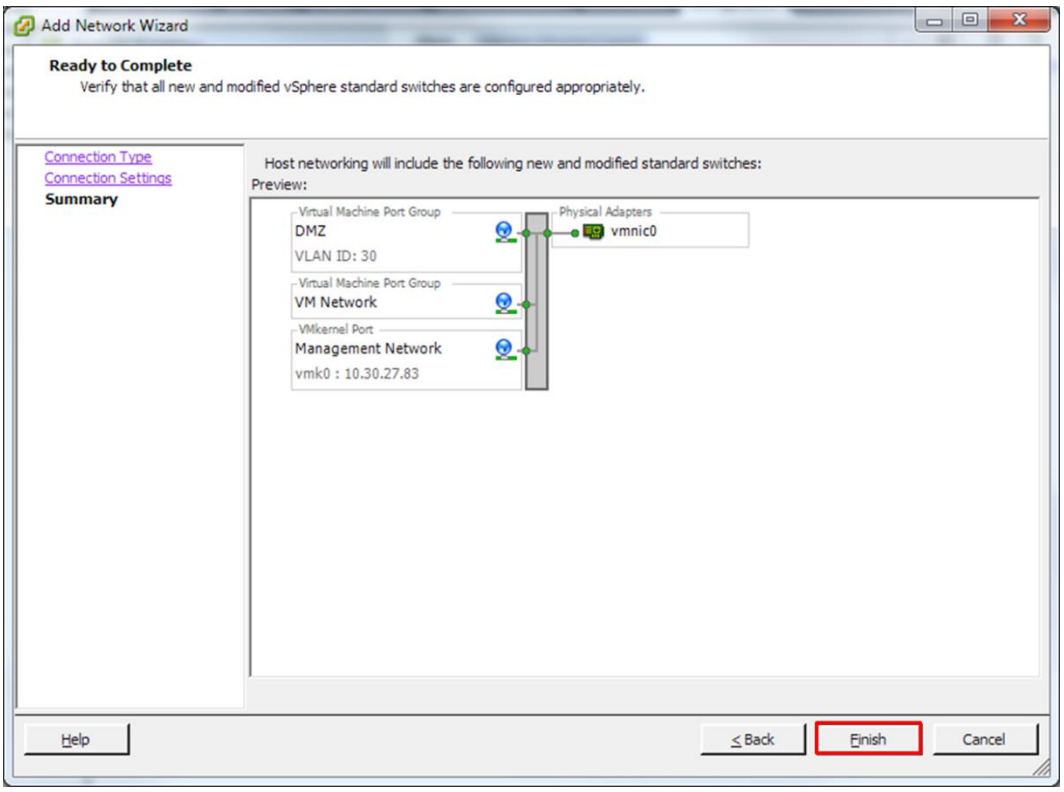
c. Accept the default setting to add a virtual machine network and click **Next**.



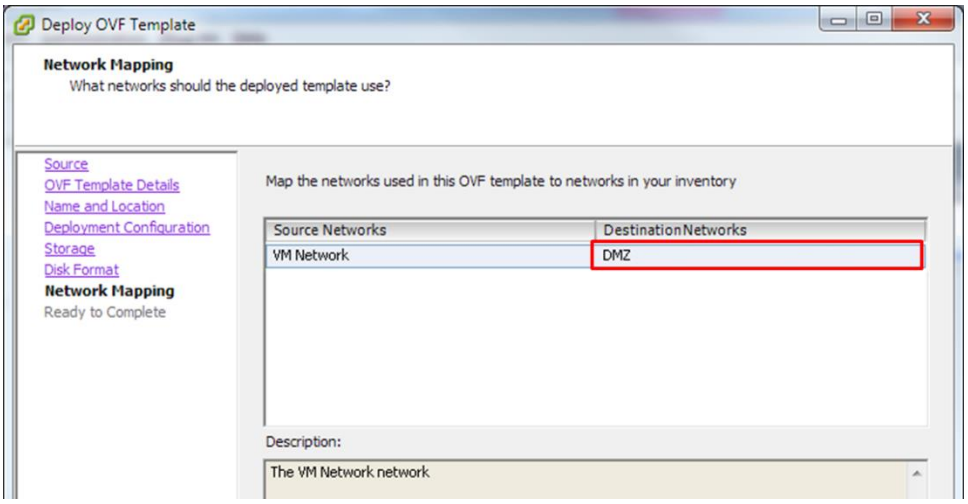
d. Add a **Network Label** and **VLAN ID** to suit your network design and click **Next**. Note that the VLAN ID should be typed in directly instead of using the dropdown box.



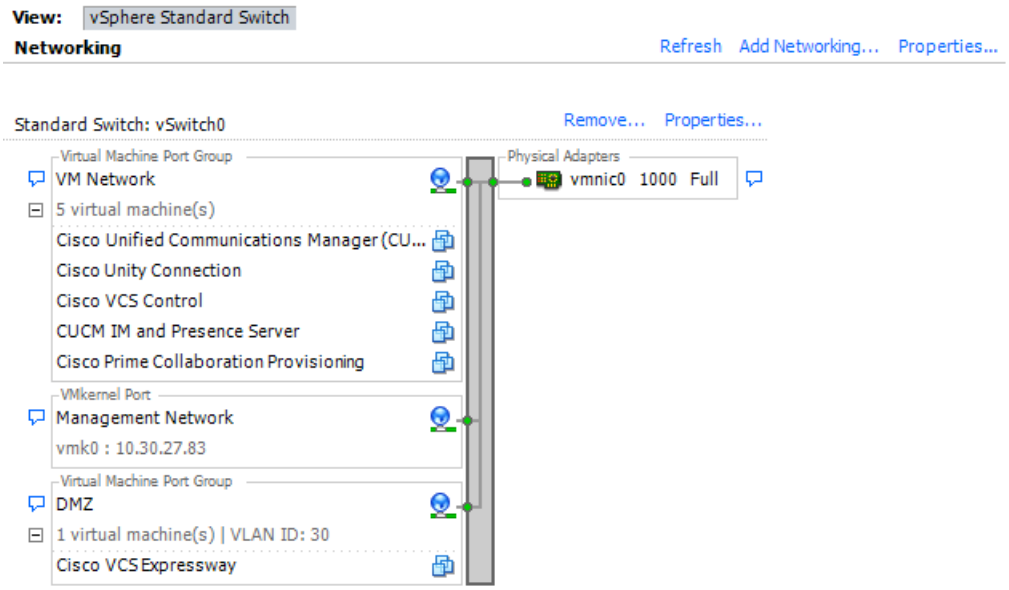
e. Check your settings for the new virtual machine port group and click **Finish**.



f. Deploy the VCS OVA for the VCS-E application, ensuring that the new DMZ port group is selected for the primary virtual machine network adaptor.



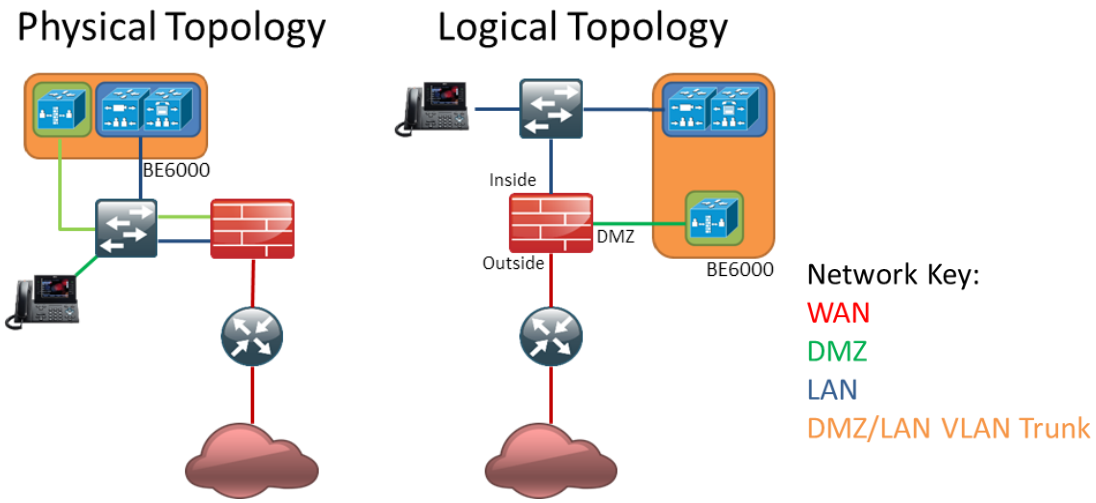
g. After deploying the VCS-E application, it will be associated with the new DMZ VLAN port group.



Configuration Procedure using Dedicated Network Connections

The following steps detail how to configure the Virtualization Hypervisor and the switched network to meet the needs of a single firewall solution with dedicated network connections for each security domain as illustrated in Figure 4.

Figure 4: Example solution

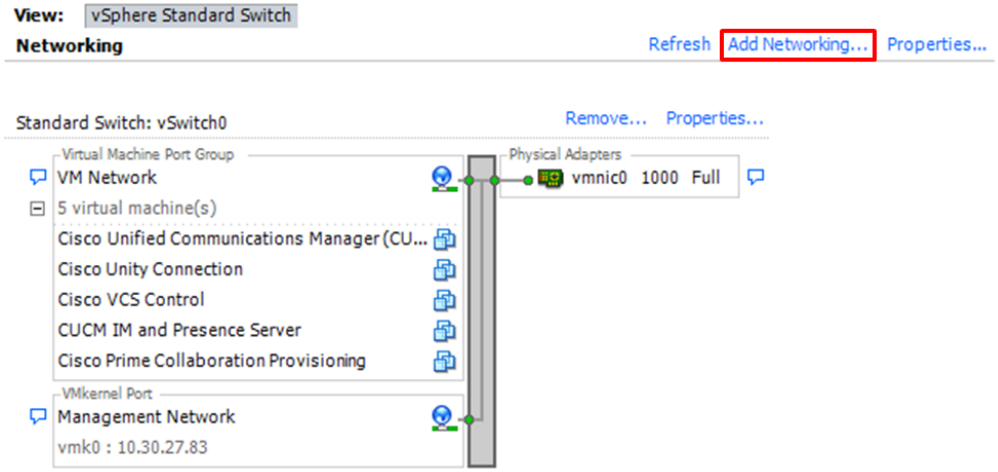


1. Configure the firewall to include a DMZ context or sub-network. Ensure that traffic policy rules are created to permit VCS-E communication with both internal and external networks. Full details of VCS-E IP Port use between public/DMZ and Private/DMZ boundaries are included in the following guide: http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/Cisco_VCS_IP_Port_Usage_for_Firewall_Traversal_Deployment_Guide_X7-2.pdf
2. Configure the layer 2 switch network to include a VLAN for DMZ traffic and ensure that this is mapped appropriately to the firewall DMZ port. Alternatively, you can use separate physical switches to achieve this separation.
3. Configure the switch ports that are assigned to the BE 6000 host for access to the internal and DMZ networks and connect them to the separate BE 6000 server network interfaces. The following example illustrates how this can be configured using a Cisco Catalyst switch when separating traffic using VLANs (default port configurations would typically be sufficient when using separate switches for each security domain):

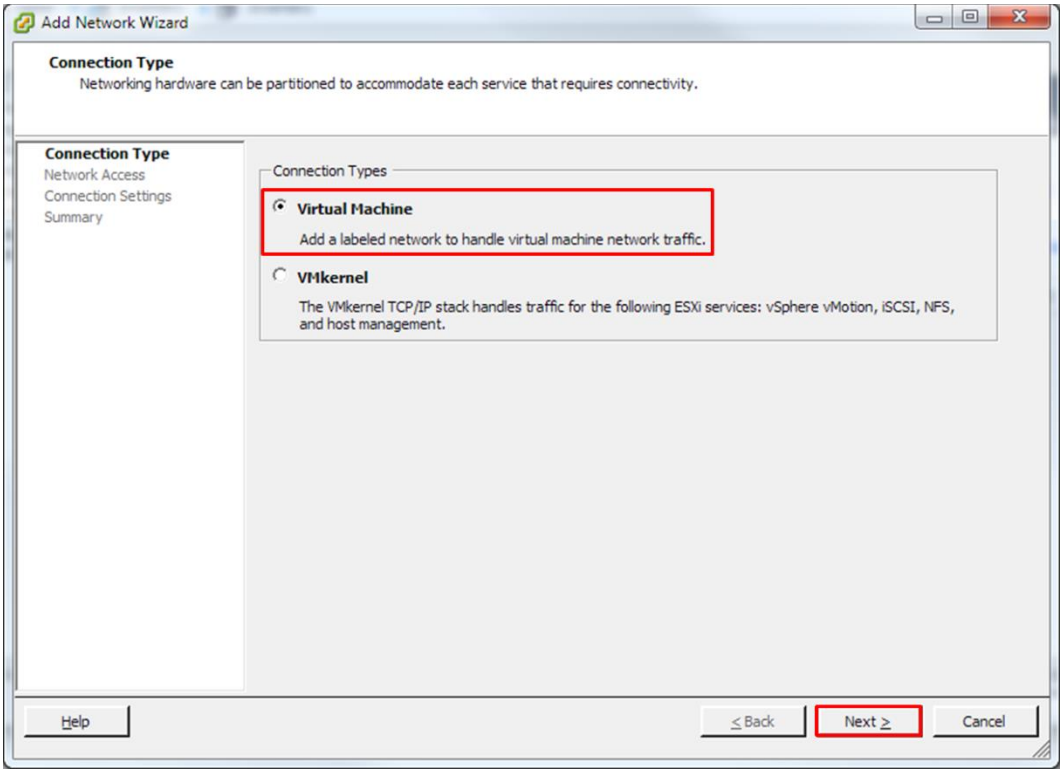
```
vlan 1
 name default
!
vlan 30
 name DMZ
!
interface GigabitEthernet1/1
 description BE 6000 Server Network Interface 1 (Internal Network)
 spanning-tree portfast
!
interface GigabitEthernet1/2
 description BE 6000 Server Network Interface 2 (DMZ Network)
 switchport access vlan 30
 spanning-tree portfast
!
```

   Note: This example assumes that the native (untagged) VLAN is used for the internal network to correspond with the default hypervisor configuration. The use of VLAN 30 for the DMZ is for illustration purposes only. Any VLAN ID may be used for this purpose.
4. Use the vSphere client to configure the hypervisor networking features as follows:

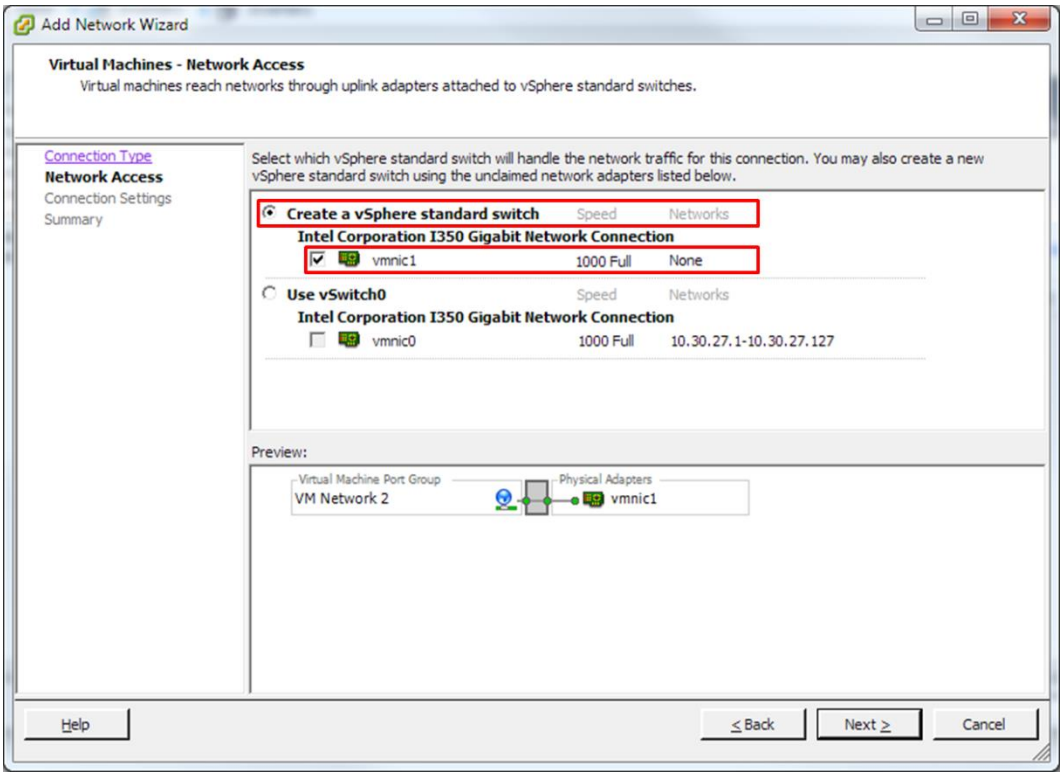
a. Access the network configuration screen by clicking the host icon in the left hand panel, then selecting the **Networking** option from the **Configuration** tab. Note that core BE 6000 applications have been configured to use the default virtual machine port group. Click **Add Networking…** to start the Add Network Wizard.



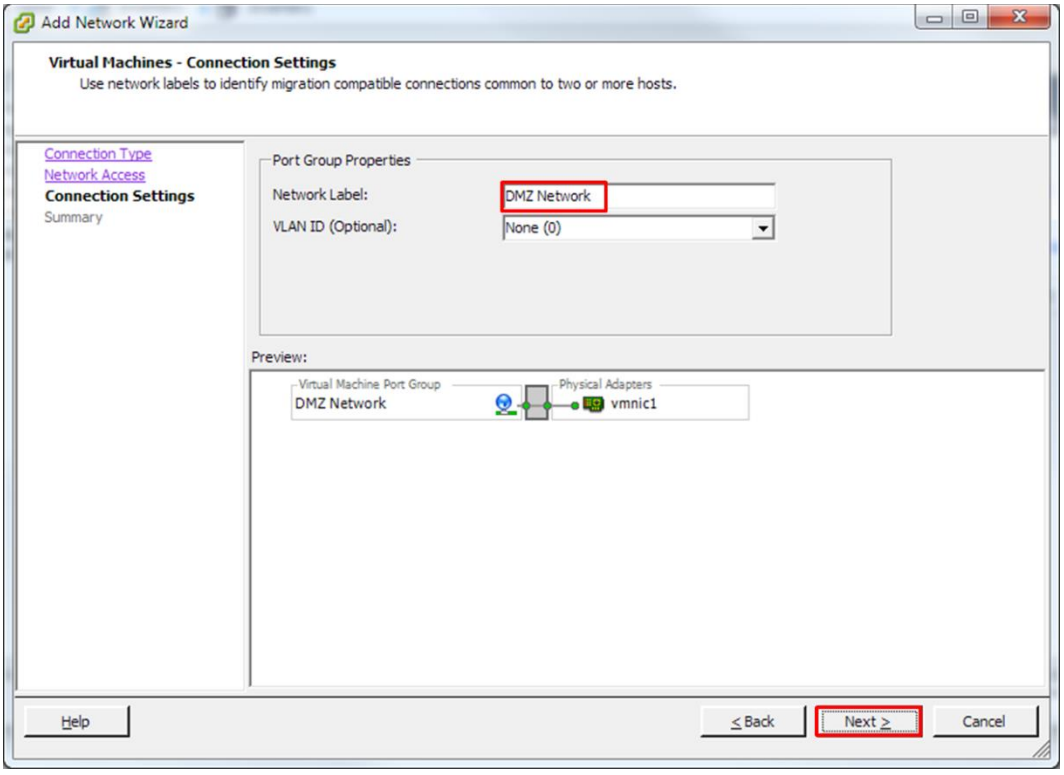
b. Accept the default setting to add a virtual machine network and click **Next**.



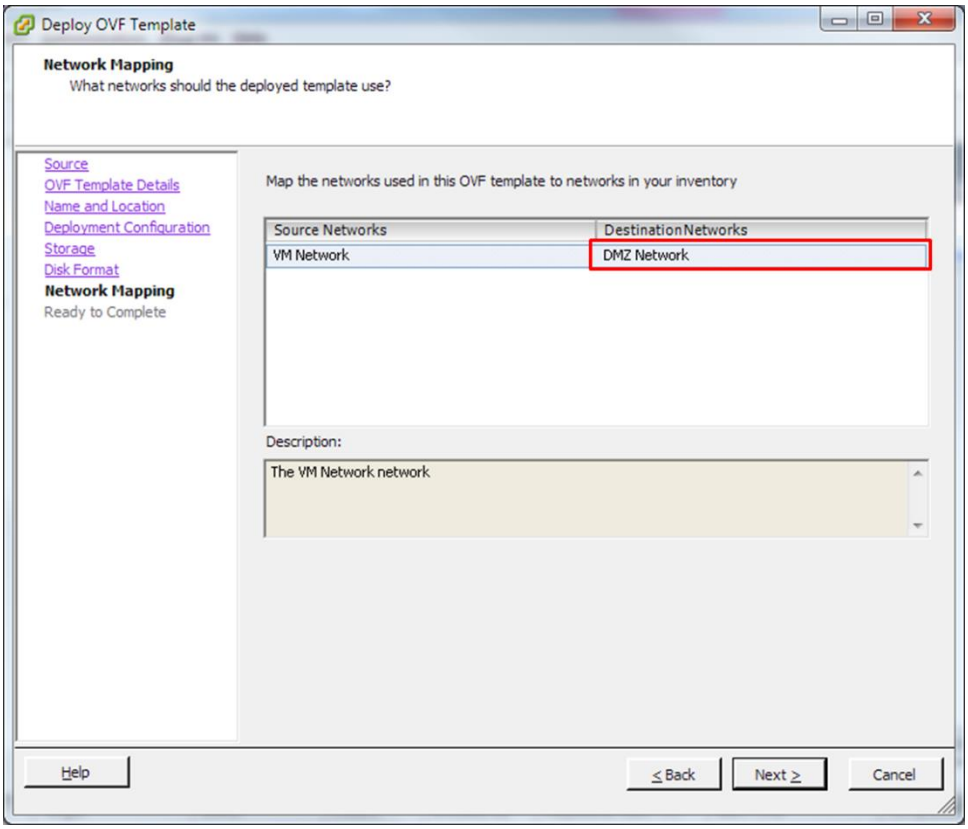
c. Select the option to create a new vSphere standard switch with an unused physical network interface (vmnic1 in this case) and click **Next**.



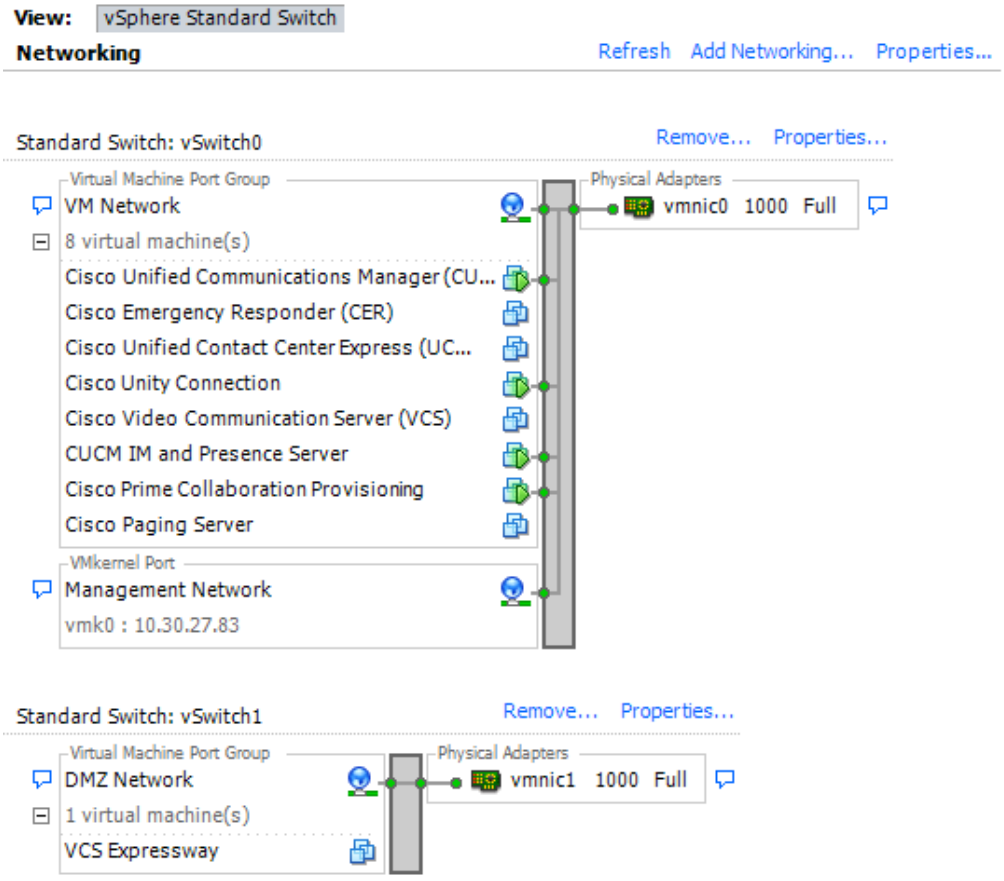
d. Add a label for the new switch, but leave the **VLAN ID** as zero. Click **Next** to review your changes, then click **Finish**.



e. Deploy the VCS OVA for the VCS-E application, ensuring that the new DMZ switch is selected for the primary virtual machine network adaptor.



f. Having deployed the VCS-E application, you will see it as connected to the new vSwitch.



Configuration for Dual Firewall Solutions

When deploying a dual firewall solution, your configuration largely follows the steps details in the previous sections, in this case assuming that the first DMZ connection is to the external firewall. Repeat the steps to create a new virtual machine port group (VLAN) or vSwitch for connection to the internal firewall, then edit the VCS-E virtual machine to assign its second network adapter to this new network. Finally, add a new VLAN or physical switch to the external network for the internal firewall sub-network.

Appendix A – Network Interface Card Teaming

Introduction

The solutions presented in the main body of this document focus on maintaining an appropriate separation of DMZ and internal networks within a virtualized BE 6000 server. In addition to this separation, the hypervisor NIC teaming feature allows multiple physical adapters to be associated with a vSwitch to provide load sharing and failover connectivity to the external network.

Failover and Load Balancing

When additional physical adapters are assigned to a vSwitch, they may be assigned as either active or standby. Depending on the way in which the server is connected to the physical network, traffic from virtual machines may be load balanced across active connections and in the event of a link failure a standby adapter will be made active to take over.

Switched Network Topologies

To maximise resiliency to failure, teamed interfaces are typically connected to different switching equipment. This might involve connecting to separate line cards in a chassis, switches in a stack, or to completely independent devices.

Where independent physical switches are used, teamed interfaces should be set to active, allowing the Ethernet Spanning Tree protocol to block connections that create a loop. In the event of a link or switch failure, the Spanning Tree protocol will reconverge to use a serviceable connection to the server. Where VLAN trunking is used, the Spanning Tree protocol can typically be configured per VLAN to prefer different connections for DMZ and internal network traffic under normal operation.

If connections are made to a common logical switch (i.e. chassis or cluster) that supports IEEE 802.3ad link aggregation, it is possible to load balance traffic across all active members of the link group under normal operation. Link aggregation can accommodate link failures more quickly than Spanning Tree and is transparent to VLANs, so may be used with either dedicated network, or VLAN trunk connections.

The following table illustrates how BE 6000 servers may accommodate network separation and NIC teaming. Note specifically that the Medium Density server only has sufficient interfaces to use NIC teaming when links are configured to use VLAN trunking.

Server Link Type	Medium Density 2 NICs	High Density 6 NICs
VLAN Trunk	✓	✓
Dedicated Links	✗	✓

Configuration

The following steps describe how to extend the configurations from this document to include NIC teaming.

Switch Configuration

When aggregating server interfaces, you must configure the switch ports to which they are connected to use 802.3ad link aggregation. The following example illustrates how this can be configured using VLAN trunking to a Cisco Catalyst switch:

```
vlan 1
 name default
!
vlan 30
 name DMZ
!
interface GigabitEthernet1/1
 description BE 6000 Server Network Interface 1 (Internal/DMZ trunk group)
 switchport trunk allowed vlan 1,30
 switchport mode trunk
 spanning-tree portfast trunk
 channel-group 1 mode passive
!
interface GigabitEthernet1/5
 description BE 6000 Server Network Interface 2 (Internal/DMZ trunk group)
 switchport trunk allowed vlan 1,30
 switchport mode trunk
 spanning-tree portfast trunk
 channel-group 1 mode passive
!
```

When connecting server interfaces to separate switches, remember that the switch port configuration is the same as the single link examples earlier in this document (the exception being that you must not enable the Spanning Tree Portfast feature).

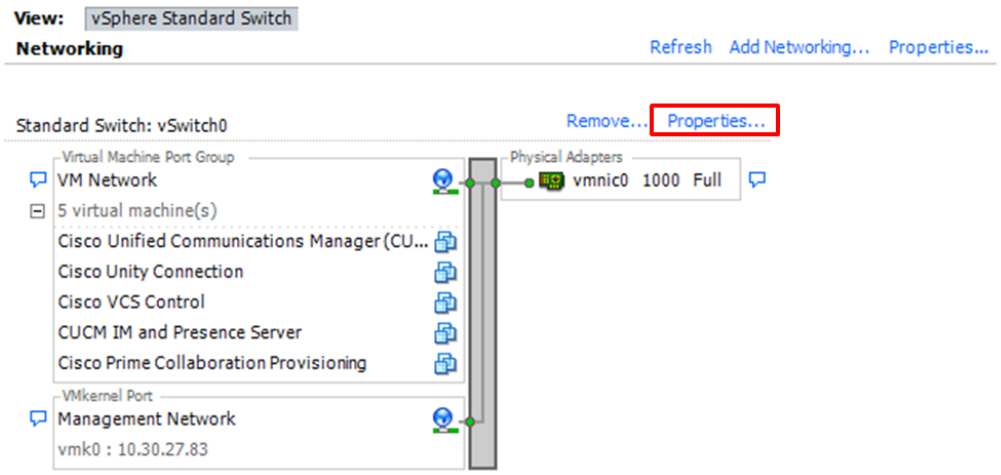
```
vlan 1
 name default
!
vlan 30
 name DMZ
!
interface GigabitEthernet1/1
 description BE 6000 Server Network Interface 1 (Internal/DMZ trunk)
 switchport trunk allowed vlan 1,30
 switchport mode trunk
!
```

The Spanning Tree VLAN cost command may be used balance traffic between links if required. See references for more details.

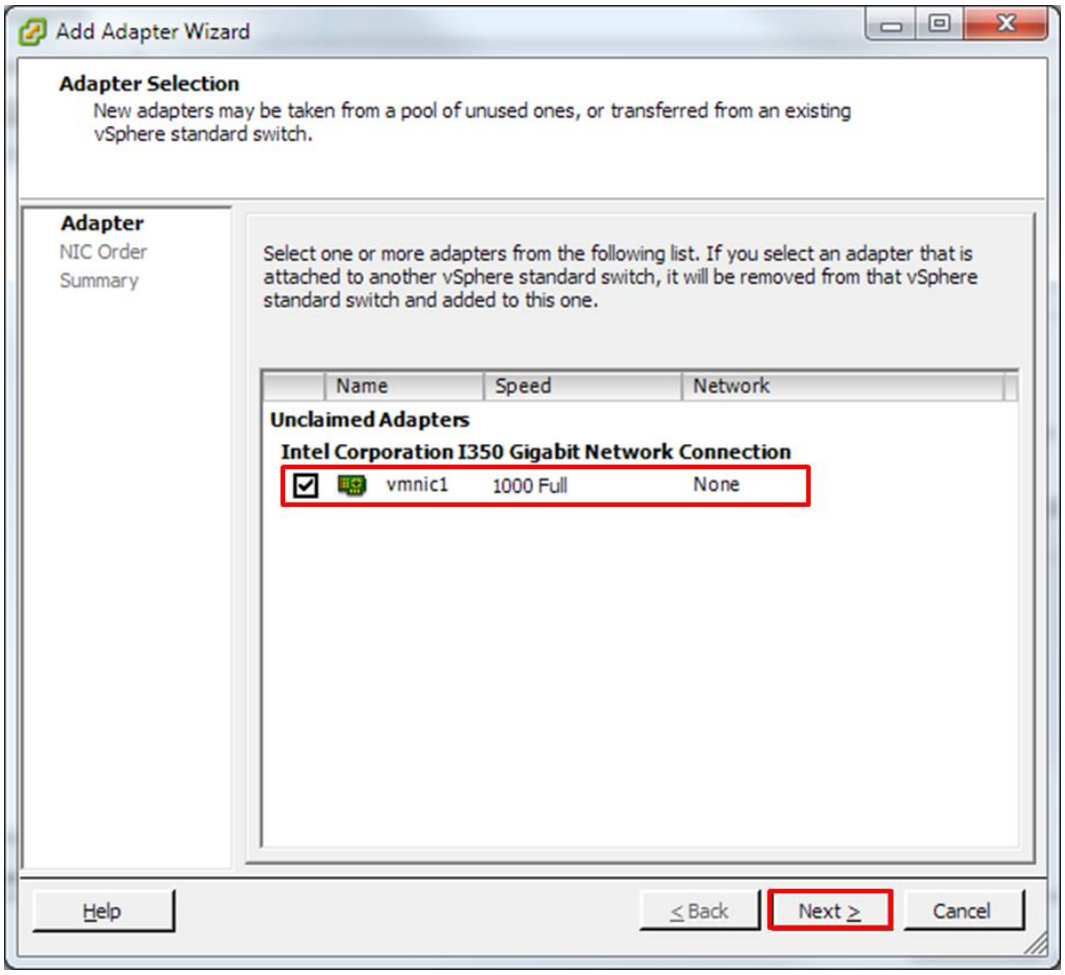
Hypervisor Configuration

Use the vSphere client to configure hypervisor networking features as follows:

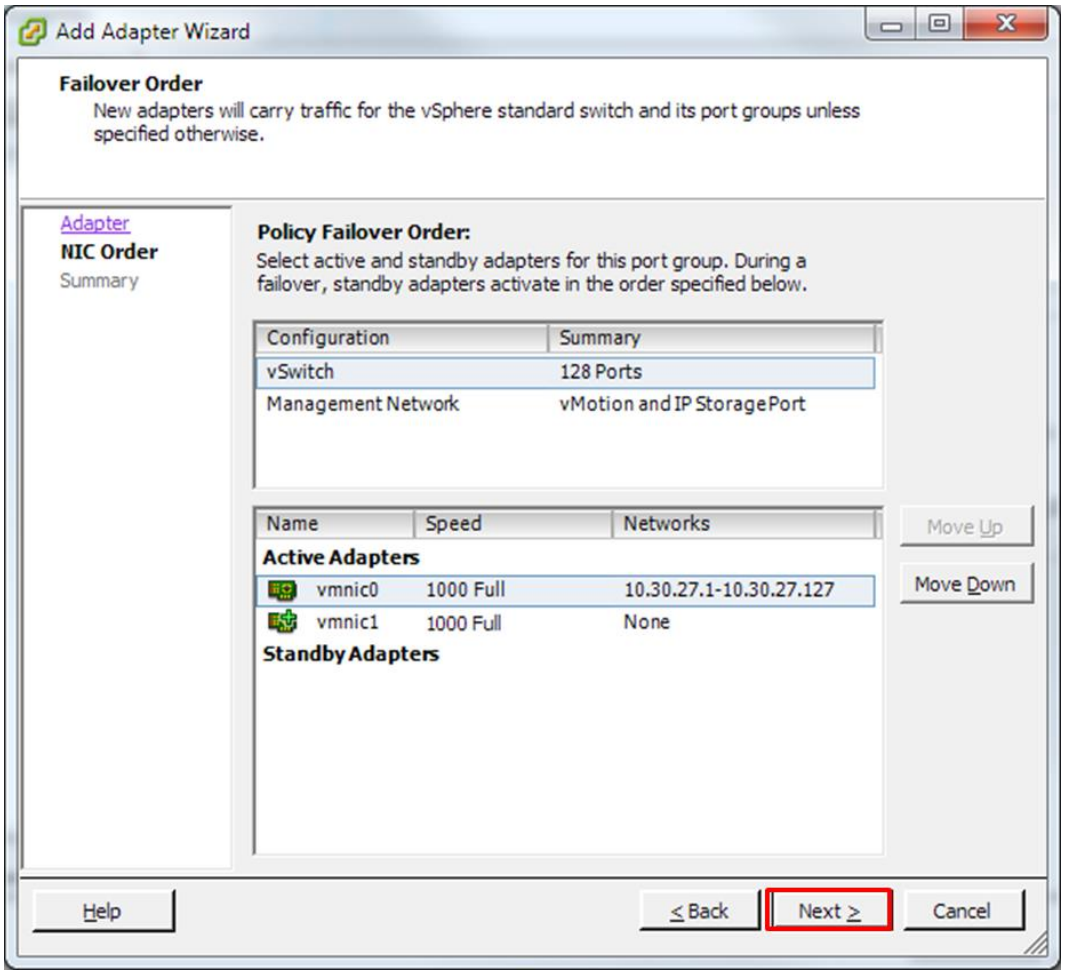
1. Access the network configuration screen by clicking the host icon in the left hand inventory panel, then selecting the **Networking** option from the **Configuration** tab. Click **Properties** for vSwitch0 to access the switch configuration screen.



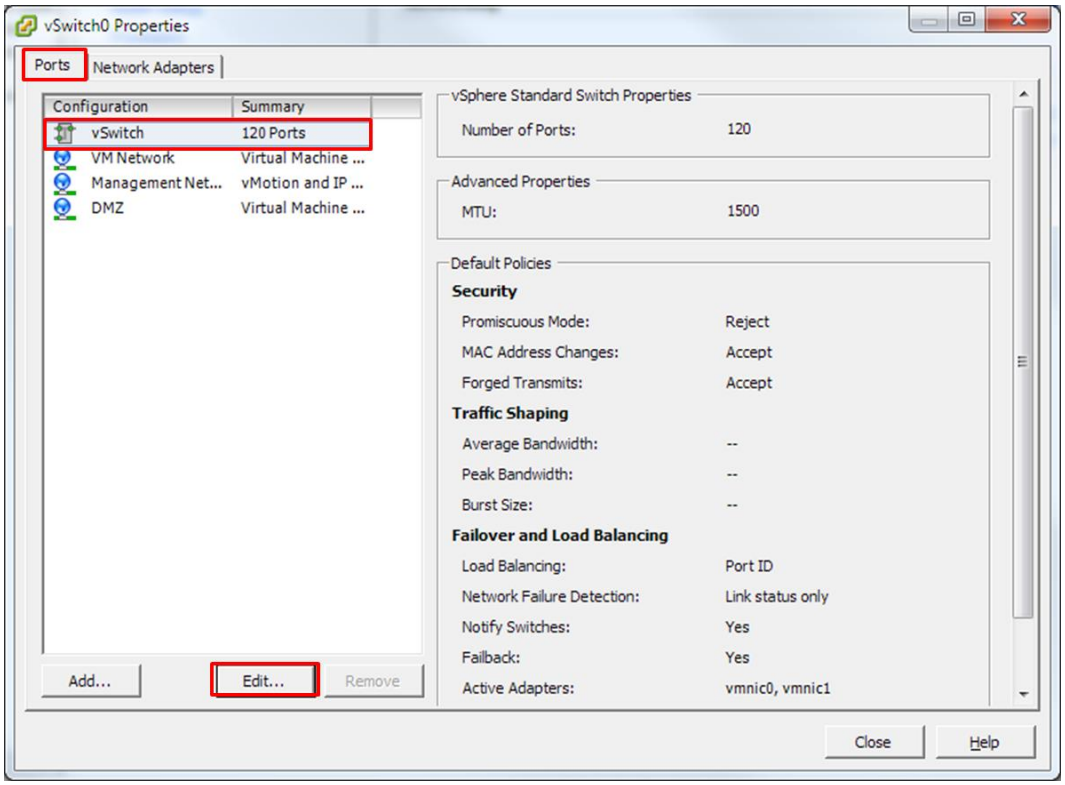
2. Select the **Physical Adapters** that should be added to the switch. When configuring a High Density server, it is recommended that a mix of motherboard and PCI card adapters are teamed. Click **Next**.



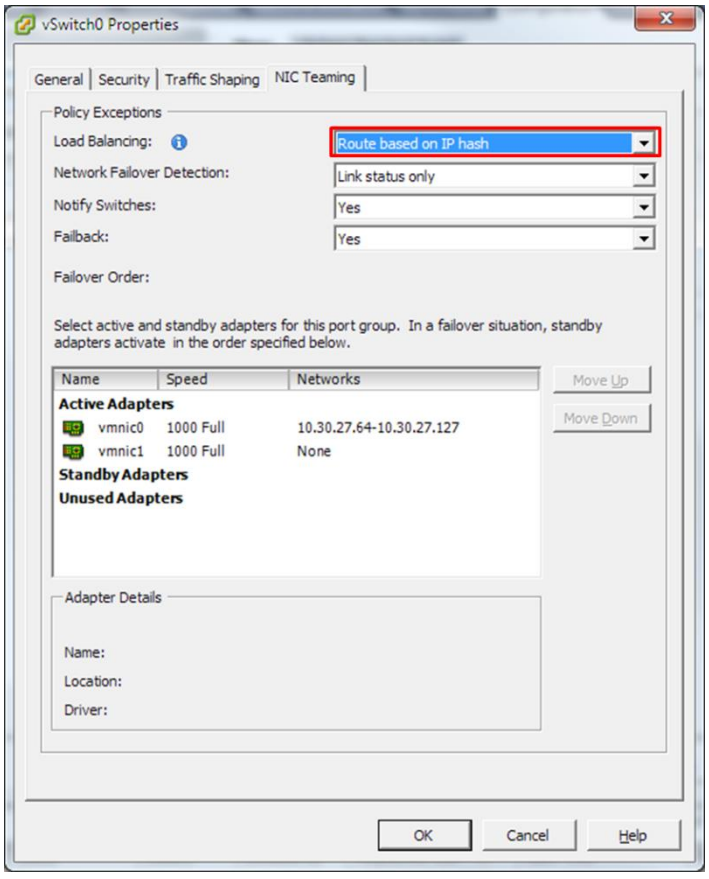
3. Adjust the failover policy for the added ports. **Move Down** the newly added adapter to standby if vSphere should manage link failover. Otherwise leave adapters active and click **Next**. Review the addition and click **Finish**.



4. If IEEE 802.3ad link aggregation is not required, close the vSwitch properties page to complete the process. To configure the vSwitch for link aggregation, select the **Ports** tab, from the **vSwitch0 Properties** page, then **Edit** the vSwitch object.



5. From the vSwitch Properties dialogue, select the **NIC Teaming** tab, then select **Route based on IP hash** for the load balancing policy. Click **OK** to close the dialogue and close the vSwitch0 properties screen to complete the configuration.



References:

VMware ESXi5.0 Networking Documentation: http://pubs.vmware.com/vsphere-50/index.jsp#com.vmware.vsphere.networking.doc_50/GUID-35B40B0B-0C13-43B2-BC85-18C9C91BE2D4.html

VLAN Load Balancing Between Trunks Using the Spanning-Tree Protocol Port Priority
http://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a00800ae96a.shtml

VCS Virtual Machine Deployment Guide:
http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/Cisco_VCS_Virtual_Machine_Deployment_Guide_X7-2.pdf

VCS Port Use:
http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/Cisco_VCS_IP_Port_Usage_for_Firewall_Traversal_Deployment_Guide_X7-2.pdf

Connecting Cisco UCM and VCS Deployment Guide:
http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/Cisco_VCS_Cisco_Unified_Communications_Manager_Deployment_Guide_CUCM_8_9_and_X7-2.pdf

VCS Control with Expressway Deployment Guide:
http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/Cisco_VCS_Basic_Configuration_Control_with_Expressway_Deployment_Guide_X7-2.pdf