Considerations for Deploying Cisco Expressway™ Solutions on a Business Edition Server

December 17 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-0883

Contents

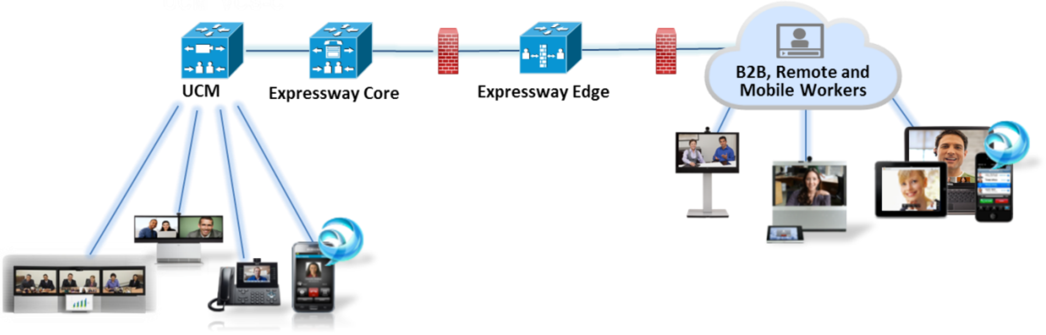
http://www.cisco.com/go/trademarks

Introduction

It is possible to consider a fully virtualized Cisco Expressway remote and mobile access collaboration solution using a common Cisco Business Edition server.

The Cisco Expressway solution comprises of Core and Edge components that allow remote video and mobile clients to communicate with a private communications platform without the need for virtual private networks. To achieve this, an Expressway Edge server is typically installed in a firewall DMZ where it may be reached from the public Internet and can communicate securely with an Expressway Core server in the private domain (Figure 1). When installed on a common Business Edition virtualized host, it is imperative that this secure network topology is maintained. This document illustrates a number of approaches that could be considered to achieve these goals.

Figure 1 Target Expressway Topology



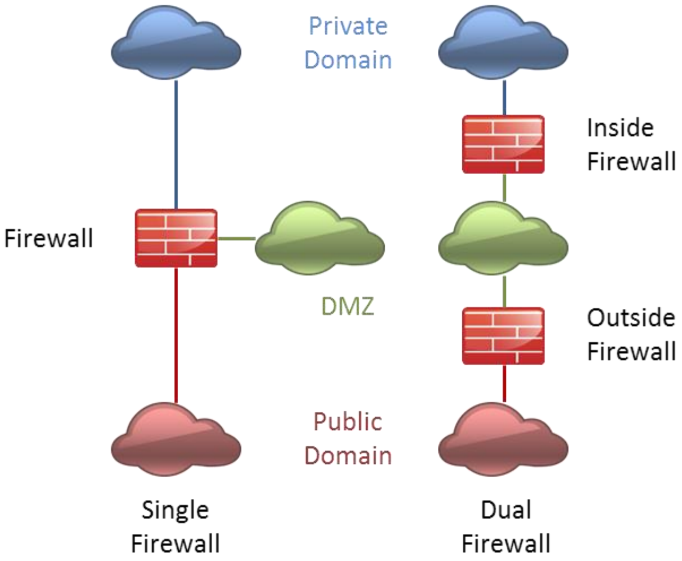
Deployment Options

When planning a co-resident deployment of Expressway Core and Edge, the Business Edition server has the flexibility to accommodate a number of different network design requirements.

Firewall Topology

The strategy used by a business to implement a firewall demilitarized zone (DMZ) and to protect the private domain will determine the connectivity requirements for the virtualised Expressway Edge. Two of the most common approaches to firewall design are illustrated in figure 2. In the case of the single firewall design, Expressway Edge 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, Expressway Edge requires separate network connections to access the public and private domains via the outside and inside firewalls respectively. Licensing for Virtualized Expressway Edge 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 shown in Figure 2, a business may choose to ensure the separation of network segments either physically or logically. This 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 Business Edition 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 Business Edition 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.

Introduction to VMware Hypervisor Networking

The Cisco Virtualization Hypervisor (VMware vSphere Hypervisor) includes the following networking concepts that may be used 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.

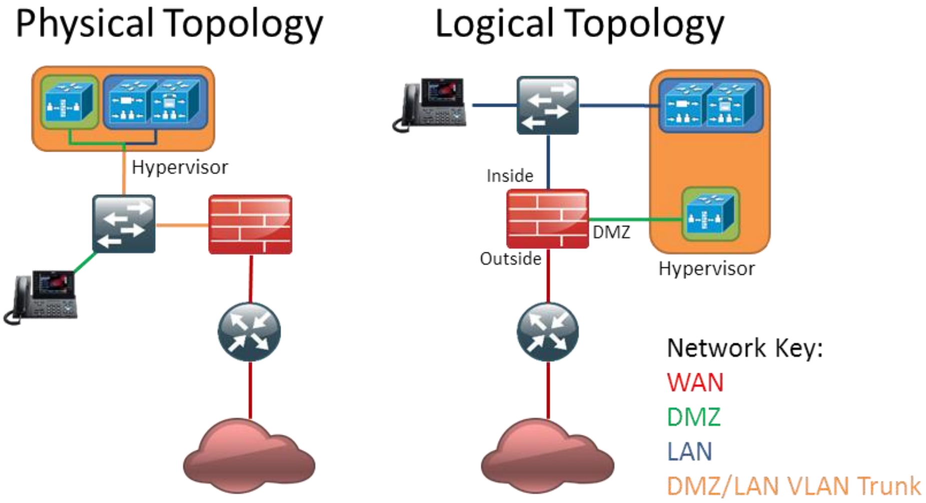
Physical Adapter: A physical host network interface which may be associated with a vSwitch to connect it with an external network. The physical adapter will automatically be configured as an 802.1q VLAN trunk (VLAN Switch Tagging mode) when multiple VLANs are created for its associated vSwitch.

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. Refer to Appendix A for steps to add multiple physical connections to the server.

Figure 3: Example solution

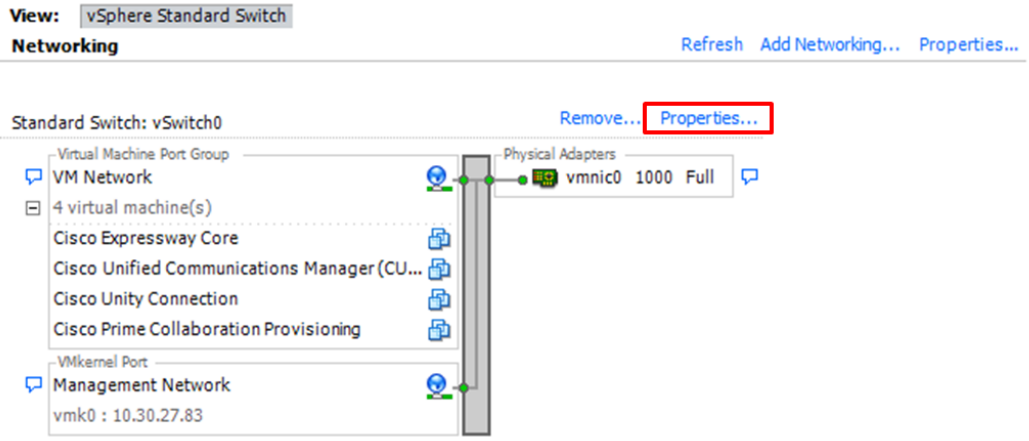


1. Configure the firewall to include a DMZ context or sub-network. Ensure that traffic policy rules are created to permit Expressway Edge communication with both inside and outside networks. Full details of Expressway Edge IP Port use across Inside/DMZ and Outside/DMZ boundaries are included in the following guide:
   http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/X8-1/Cisco-VCS-IP-Port-Usage-for-Firewall-Traversal-Deployment-Guide-X8-1.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 Business Edition server as a VLAN trunk, ensuring that internal and DMZ networks only are allowed and connect it to the Business Edition server network interface 1. The following example illustrates how this may be configured using a Cisco Catalyst switch:

```
vlan 1
 name default
!
vlan 30
 name DMZ
!
interface GigabitEthernet1/1
 description BE 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 inside 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 applications have been configured to use the default virtual machine port group. Click on **properties** for vSwitch0 to access the switch configuration screen.



View: vSphere Standard Switch

Networking

Standard Switch: vSwitch0

Virtual Machine Port Group

VM Network

4 virtual machine(s)

Cisco Expressway Core

Cisco Unified Communications Manager (CU...

Cisco Unity Connection

Cisco Prime Collaboration Provisioning

VMkernel Port

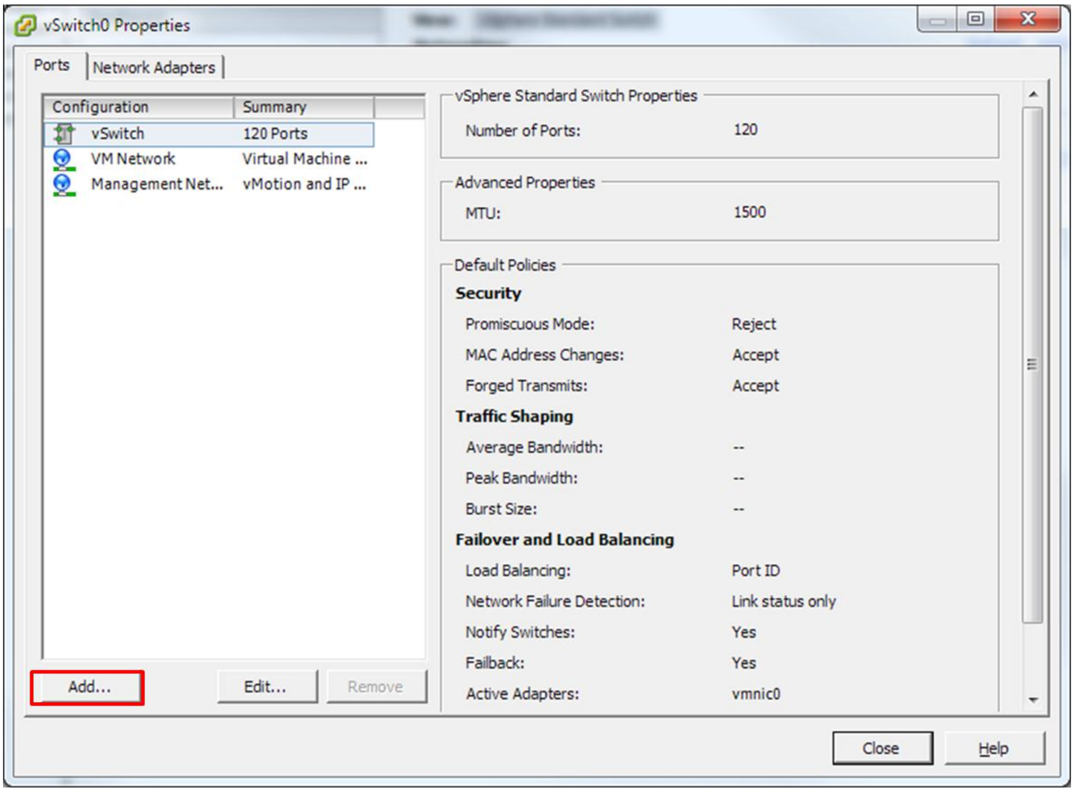
Management Network

vmk0 : 10.30.27.83

Physical Adapters

vmnic0 1000 Full

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



vSwitch0 Properties

Configuration	Summary
vSwitch	120 Ports
VM Network	Virtual Machine ...
Management Net...	vMotion and IP ...

vSphere Standard Switch Properties

Number of Ports: 120

Advanced Properties

MTU: 1500

Default Policies

Security

Promiscuous Mode: Reject

MAC Address Changes: Accept

Forged Transmits: Accept

Traffic Shaping

Average Bandwidth: --

Peak Bandwidth: --

Burst Size: --

Failover and Load Balancing

Load Balancing: Port ID

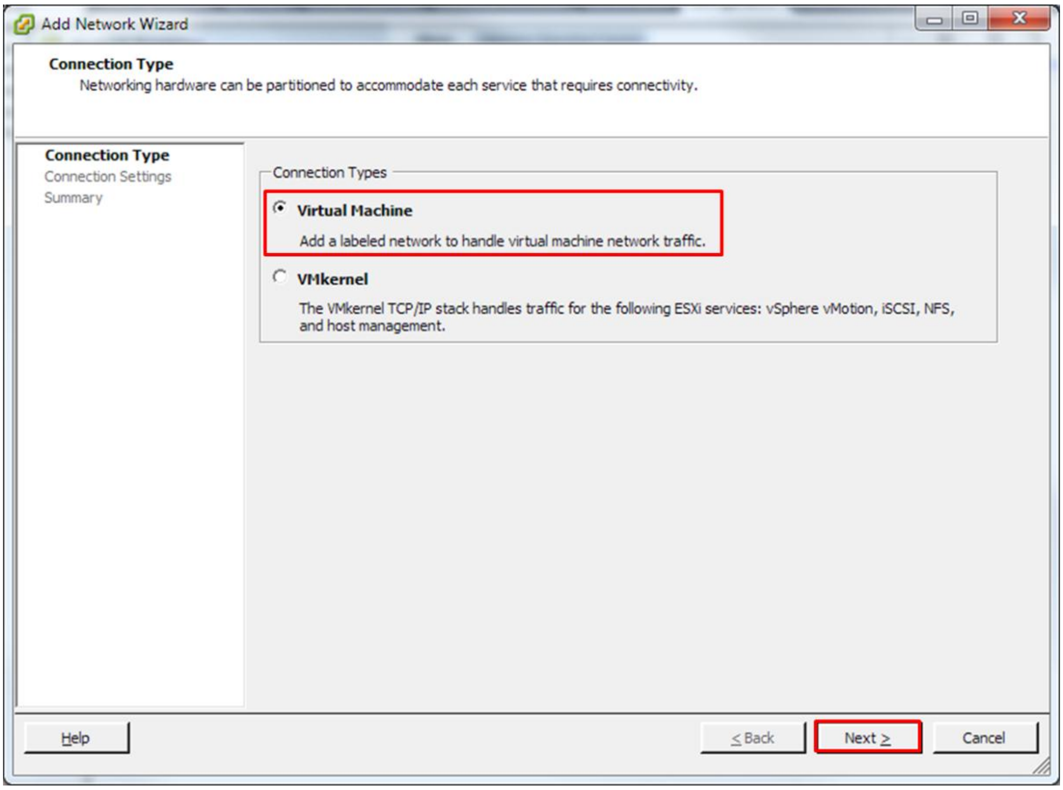
Network Failure Detection: Link status only

Notify Switches: Yes

Failback: Yes

Active Adapters: vmnic0

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



Add Network Wizard

Connection Type

Networking hardware can be partitioned to accommodate each service that requires connectivity.

Connection Types

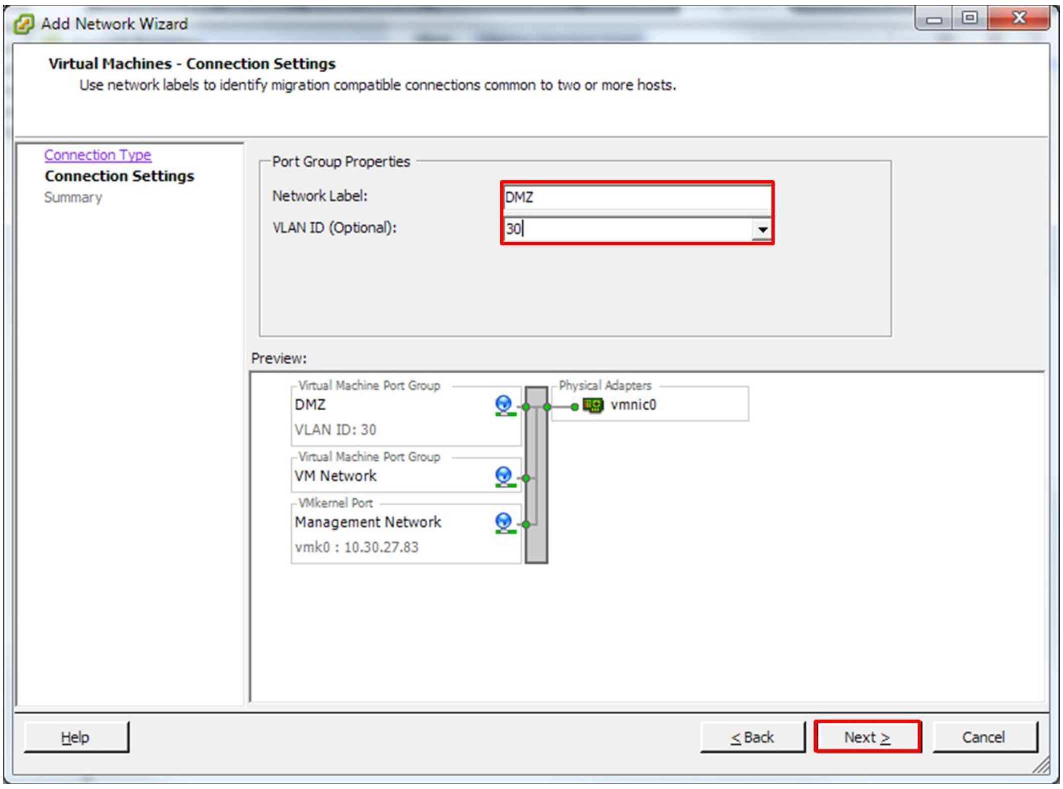
● **Virtual Machine**

Add a labeled network to handle virtual machine network traffic.

○ **VMkernel**

The VMkernel TCP/IP stack handles traffic for the following ESXi services: vSphere vMotion, iSCSI, NFS, and host management.

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.



Add Network Wizard

Virtual Machines - Connection Settings

Use network labels to identify migration compatible connections common to two or more hosts.

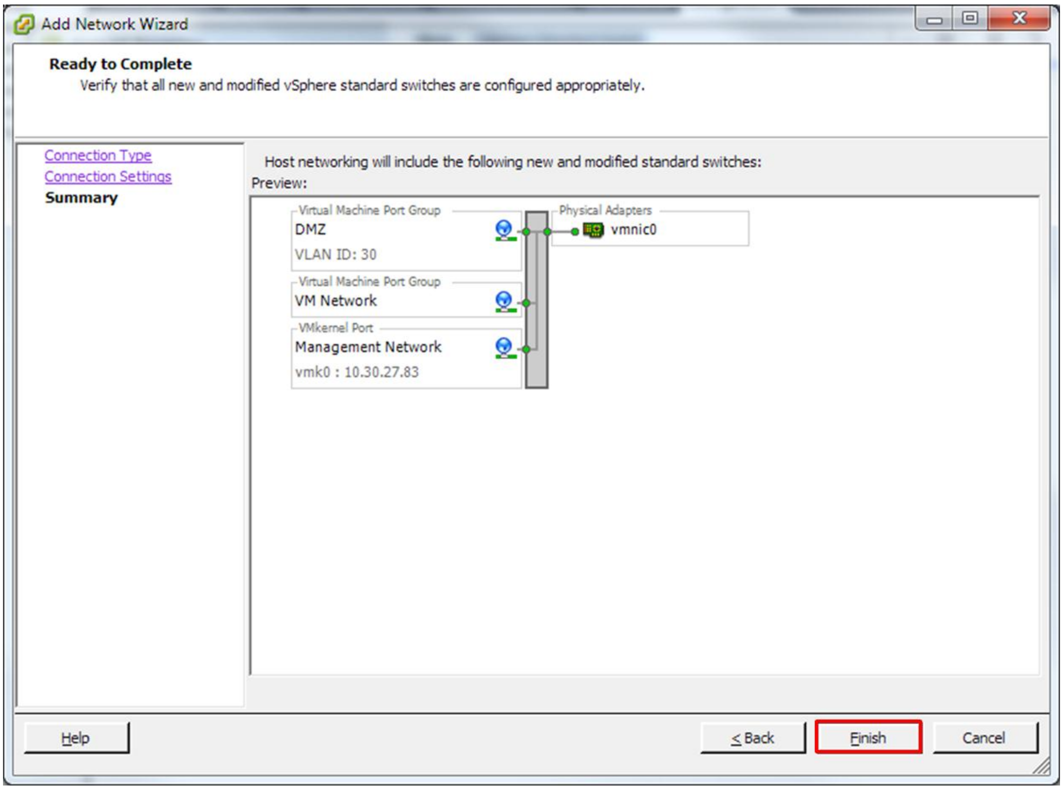
Port Group Properties

Network Label: DMZ

VLAN ID (Optional): 30

Preview:

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



Add Network Wizard

Ready to Complete

Verify that all new and modified vSphere standard switches are configured appropriately.

Host networking will include the following new and modified standard switches:

Preview:

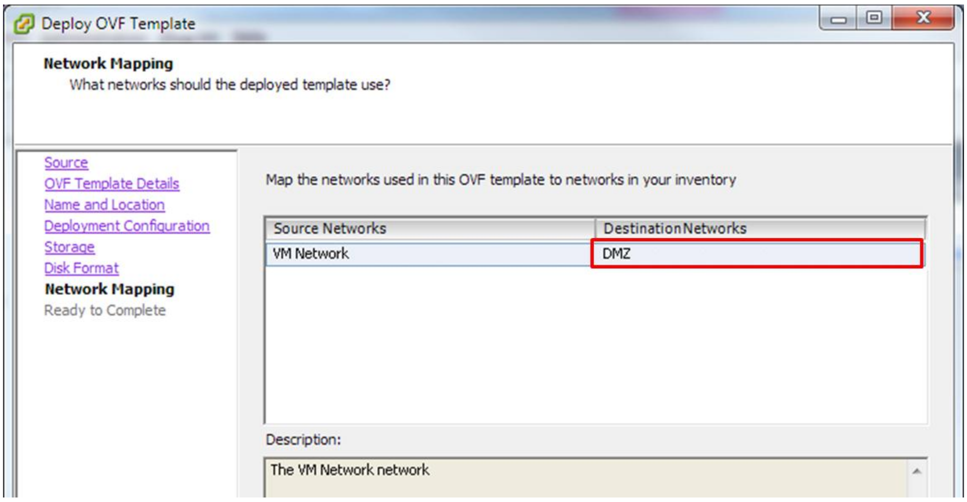
Virtual Machine Port Group: DMZ, VLAN ID: 30

Virtual Machine Port Group: VM Network

VMkernel Port: Management Network, vmk0 : 10.30.27.83

Physical Adapters: vmnic0

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



Deploy OVF Template

Network Mapping

What networks should the deployed template use?

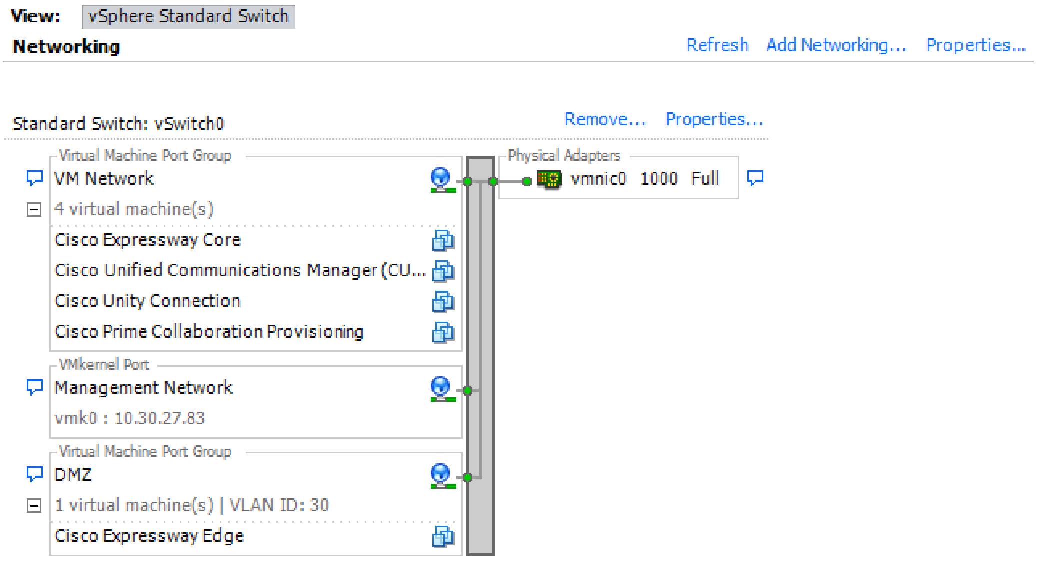
Map the networks used in this OVF template to networks in your inventory

Source Networks	Destination Networks
VM Network	DMZ

Description:

The VM Network network

g. Having deployed the Expressway Edge application, it will be seen using the DMZ VLAN in the new port group.



View: vSphere Standard Switch

Networking

Standard Switch: vSwitch0

Virtual Machine Port Group
VM Network
4 virtual machine(s)
Cisco Expressway Core
Cisco Unified Communications Manager (CU...
Cisco Unity Connection
Cisco Prime Collaboration Provisioning

VMkernel Port
Management Network
vmk0 : 10.30.27.83

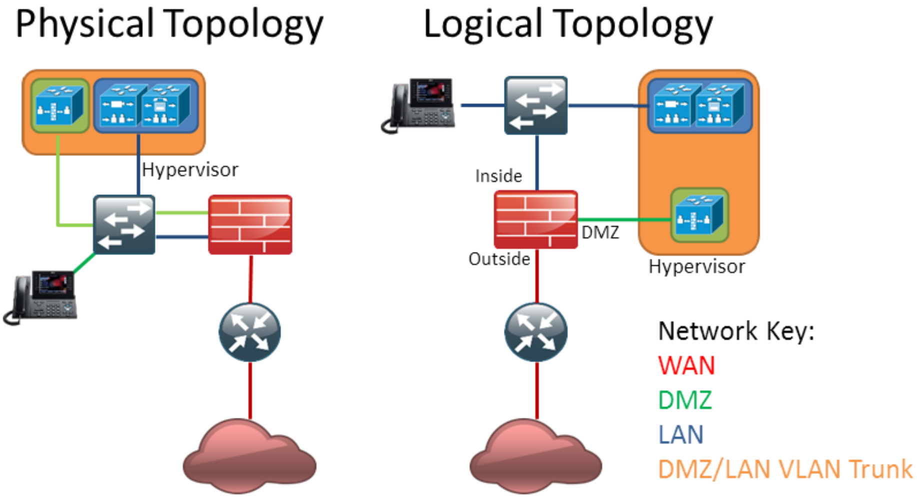
Virtual Machine Port Group
DMZ
1 virtual machine(s) | VLAN ID: 30
Cisco Expressway Edge

Physical Adapters
vmnic0 1000 Full

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 Expressway Edge communication with both inside and outside networks. Full details of Expressway Edge IP Port use between Inside/DMZ and Outside/DMZ boundaries are included in the following guide: http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/X8-1/Cisco-VCS-IP-Port-Usage-for-Firewall-Traversal-Deployment-Guide-X8-1.pdf

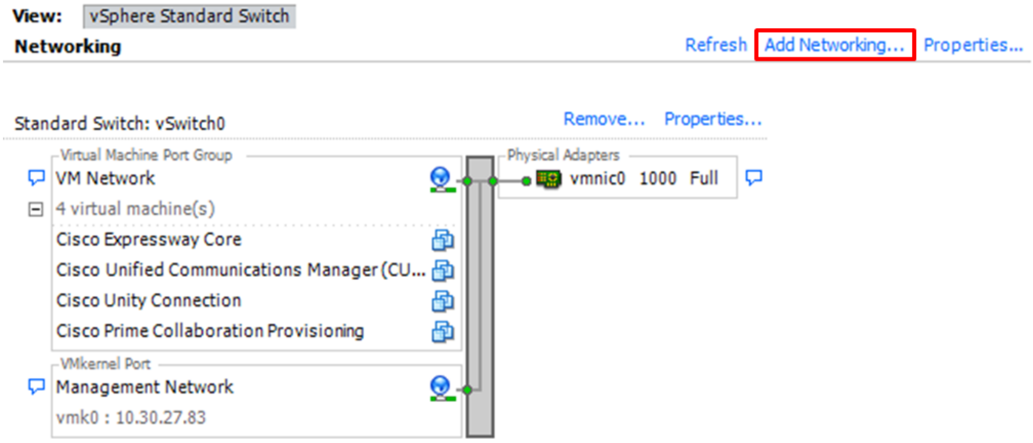
2. Configure the layer 2 switch network to include a VLAN for DMZ traffic and ensure that this is mapped appropriately to the firewall DMZ port. Alternatively, separate physical switches may be used to achieve this separation.

3. Configure the switch ports assigned to the Business Edition server for access to the internal and DMZ networks and connect them to the separate Business Edition server network interfaces. The following example illustrates how this may 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):

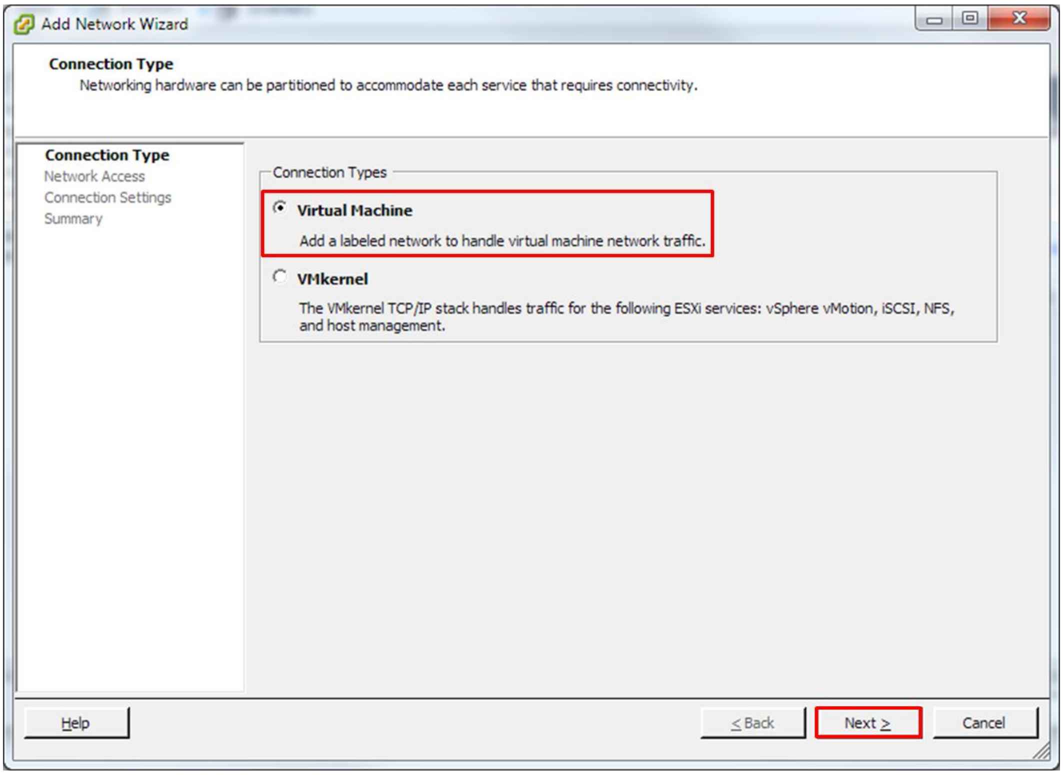
```
vlan 1
 name default
!
vlan 30
 name DMZ
!
interface GigabitEthernet1/1
 description BE Server Network Interface 1 (Internal Network)
 spanning-tree portfast
!
interface GigabitEthernet1/2
 description BE Server Network Interface 2 (DMZ Network)
 switchport access vlan 30
 spanning-tree portfast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

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 collaboration applications have been configured to use the default virtual machine port group. Click on **Add Networking…** to start the Add Network Wizard.



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



Connection Type

Networking hardware can be partitioned to accommodate each service that requires connectivity.

Connection Types

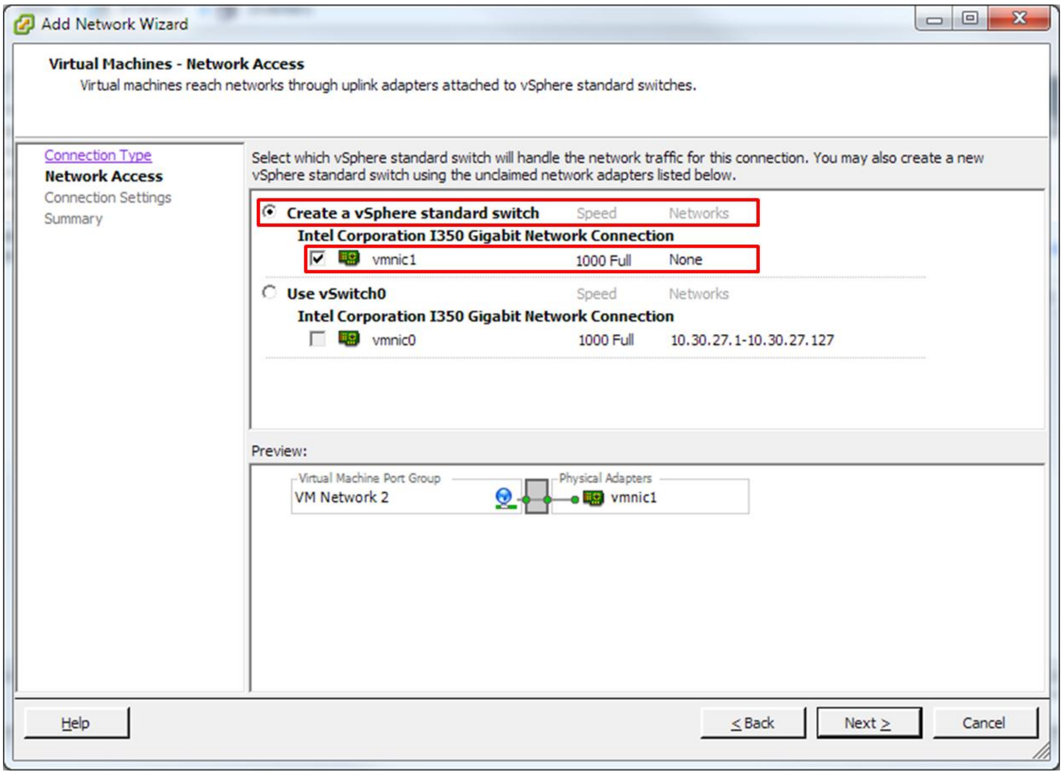
● **Virtual Machine**

Add a labeled network to handle virtual machine network traffic.

○ **VMkernel**

The VMkernel TCP/IP stack handles traffic for the following ESXi services: vSphere vMotion, iSCSI, NFS, and host management.

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



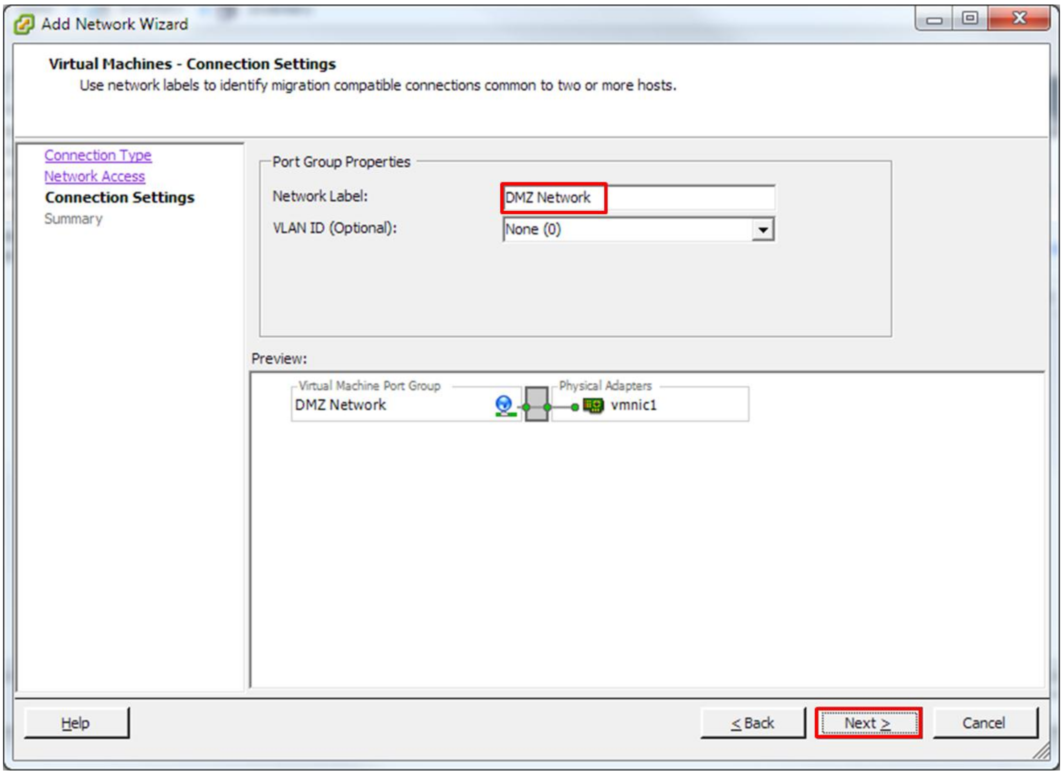
Virtual Machines - Network Access

Virtual machines reach networks through uplink adapters attached to vSphere standard switches.

Select which vSphere standard switch will handle the network traffic for this connection. You may also create a new vSphere standard switch using the unclaimed network adapters listed below.

	Speed	Networks
● **Create a vSphere standard switch**		
Intel Corporation I350 Gigabit Network Connection		
☑ vmnic1	1000 Full	None
○ **Use vSwitch0**		
Intel Corporation I350 Gigabit Network Connection		
□ vmnic0	1000 Full	10.30.27.1-10.30.27.127

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



Add Network Wizard

Virtual Machines - Connection Settings

Use network labels to identify migration compatible connections common to two or more hosts.

Port Group Properties

Network Label: DMZ Network

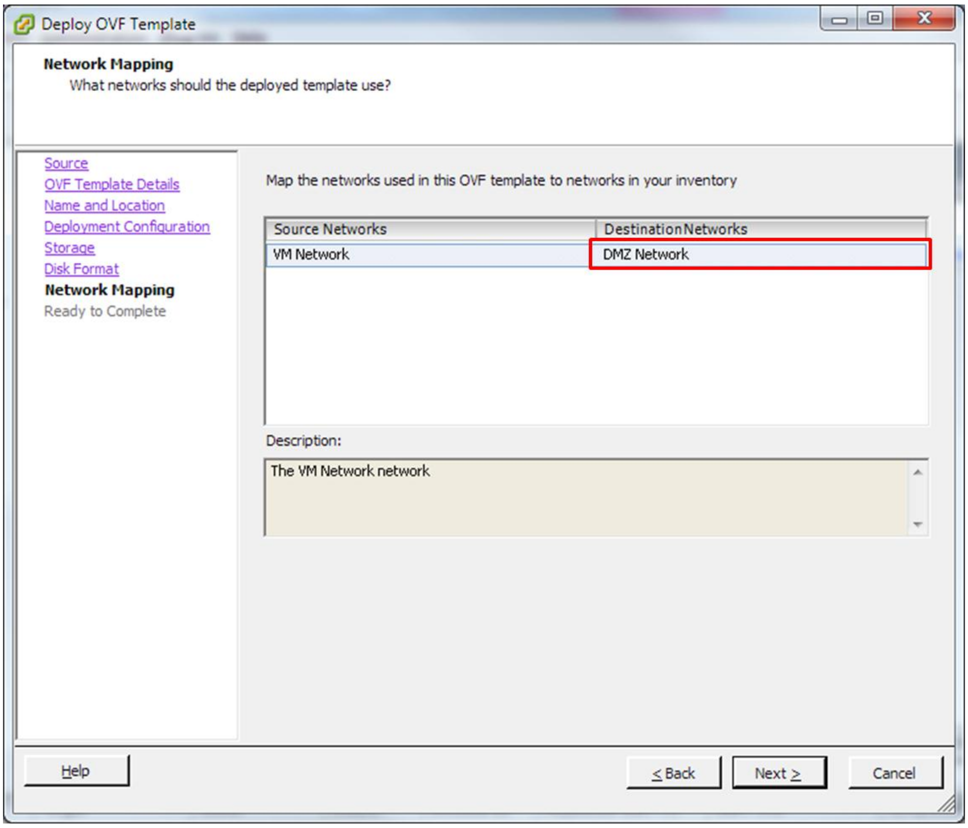
VLAN ID (Optional): None (0)

Preview:

Virtual Machine Port Group: DMZ Network

Physical Adapters: vmnic1

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



Deploy OVF Template

Network Mapping

What networks should the deployed template use?

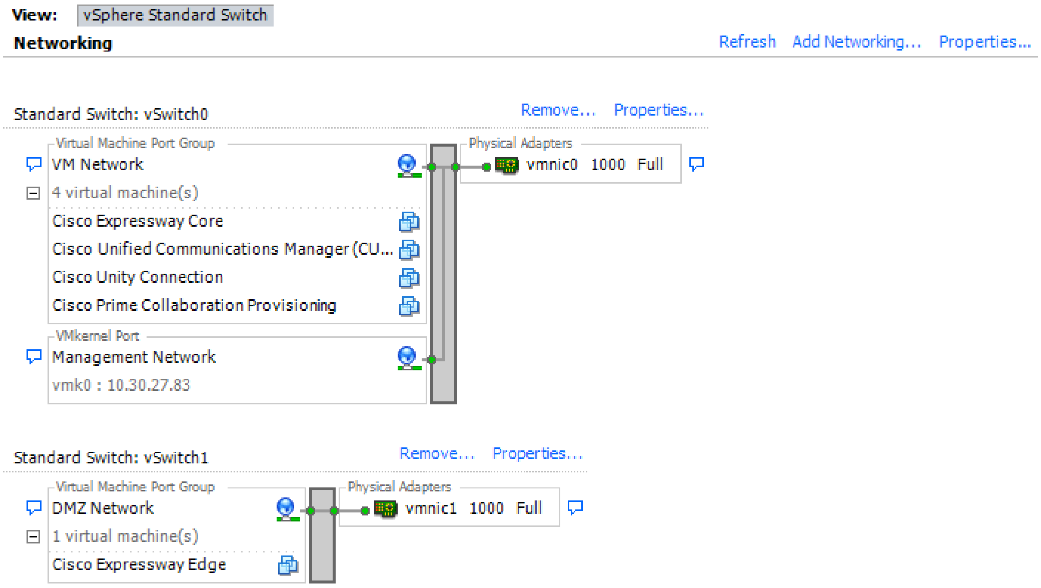
Map the networks used in this OVF template to networks in your inventory

Source Networks	Destination Networks
VM Network	DMZ Network

Description:

The VM Network network

f. Having deployed the Expressway Edge application, it will be seen connected to the new vSwitch.



Configuration for Dual Firewall Solutions

When deploying a dual firewall solution, configuration largely follows the steps detailed 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 inside firewall, then edit the Expressway Edge 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 inside 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 inside networks within a virtualized Business Edition 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 Business Edition 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	BE6000 MD	BE6000 HD	BE7000
Link Type	2 NICs	6 NICs	12 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, the switch ports to which they are connected must be configured to use 802.3ad link aggregation. The following example illustrates how this may be configured using VLAN trunking to a Cisco Catalyst switch:

```
vlan 1
 name default
!
vlan 30
 name DMZ
!
interface GigabitEthernet1/1
 description BE 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 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, switch port configuration is the same as the single link examples earlier in this document. The exception being that Spanning Tree Portfast **must not** be used.

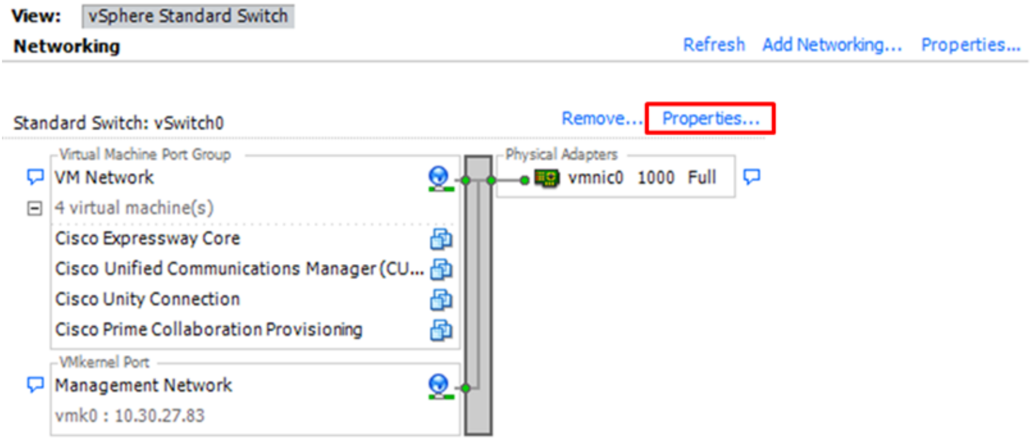
```
vlan 1
 name default
!
vlan 30
 name DMZ
!
interface GigabitEthernet1/1
 description BE Server Network Interface 1 (Internal/DMZ trunk)
 switchport trunk allowed vlan 1,30
 switchport mode trunk
!
```

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

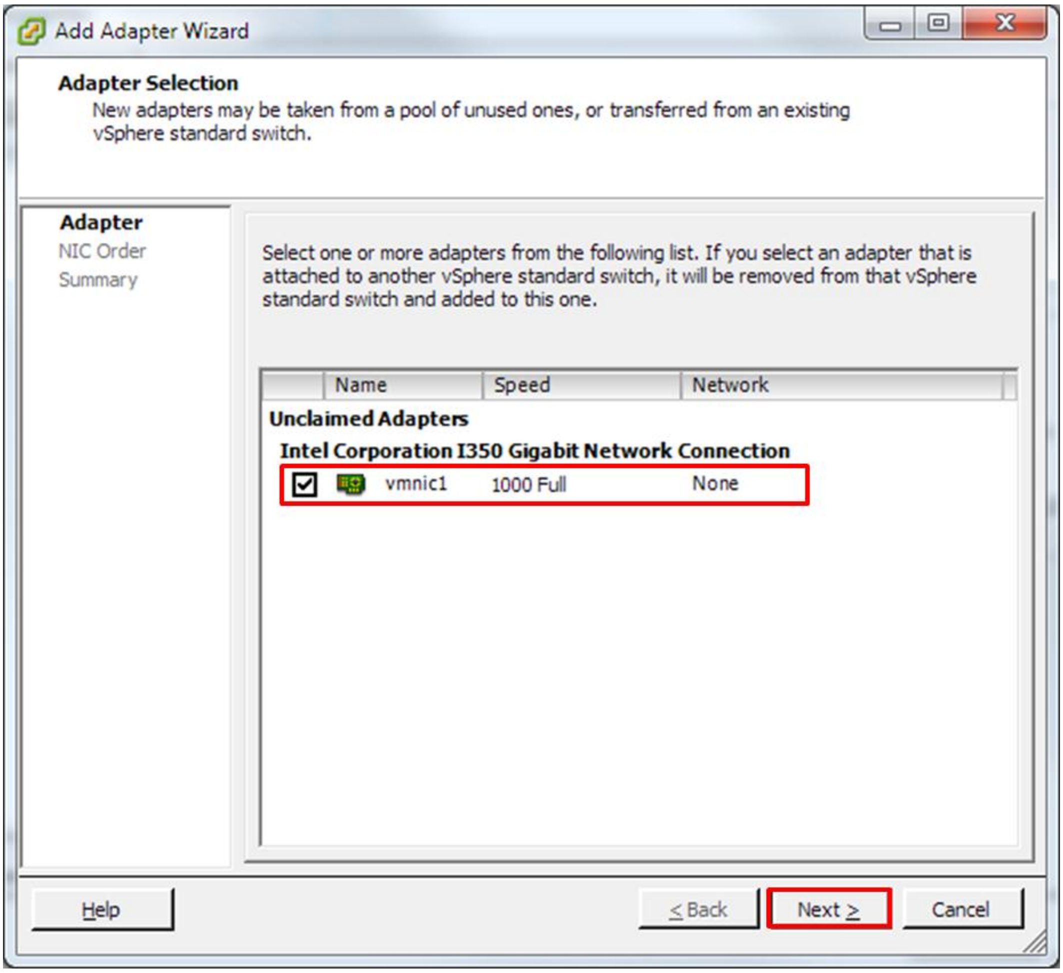
Hypervisor Configuration

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 on **properties** for vSwitch0 to access the switch configuration screen.



2. Select the **Physical Adapters** that should be added to the switch. It is recommended that a mix of motherboard and PCI card network adapters are teamed. Click **Next**.



Add Adapter Wizard

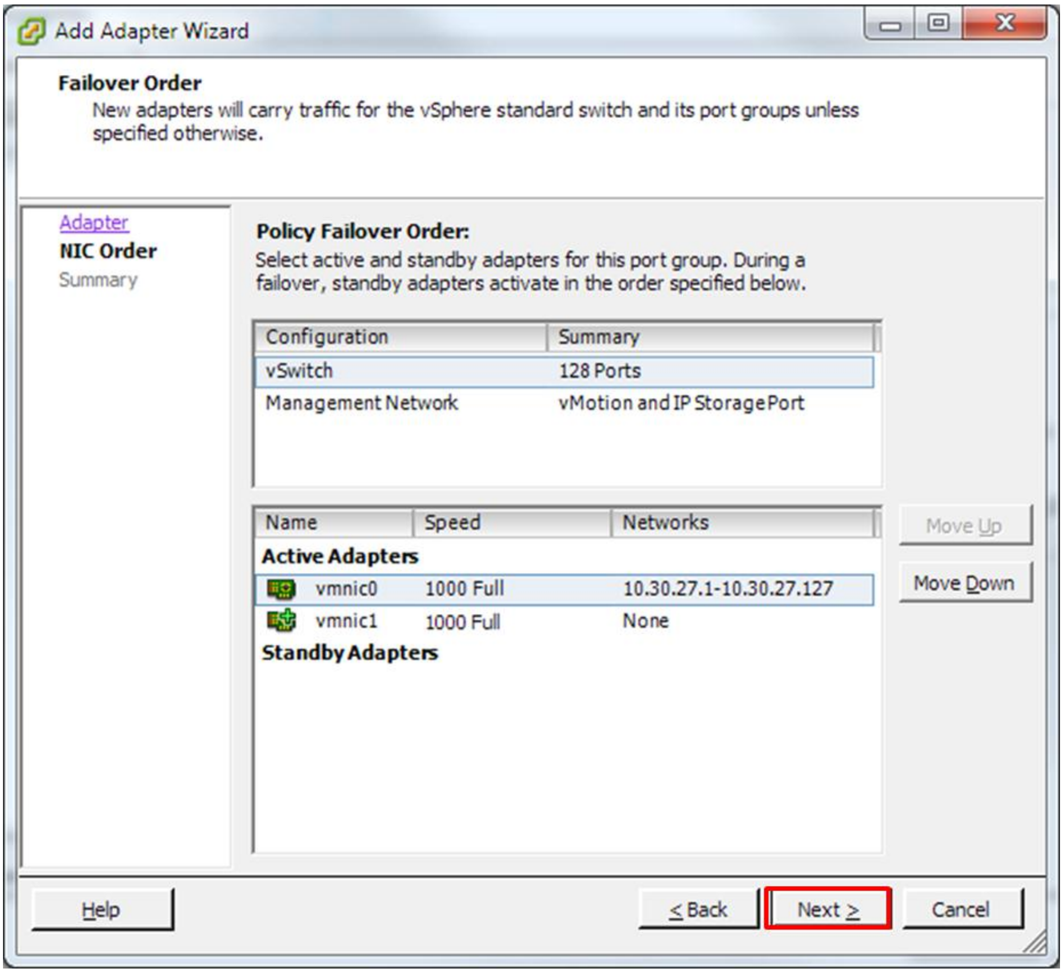
Adapter Selection

New adapters may be taken from a pool of unused ones, or transferred from an existing vSphere standard switch.

Select one or more adapters from the following list. If you select an adapter that is attached to another vSphere standard switch, it will be removed from that vSphere standard switch and added to this one.

	Name	Speed	Network
Unclaimed Adapters			
Intel Corporation I350 Gigabit Network Connection			
☑	vmnic1	1000 Full	None

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**.



Add Adapter Wizard

Failover Order

New adapters will carry traffic for the vSphere standard switch and its port groups unless specified otherwise.

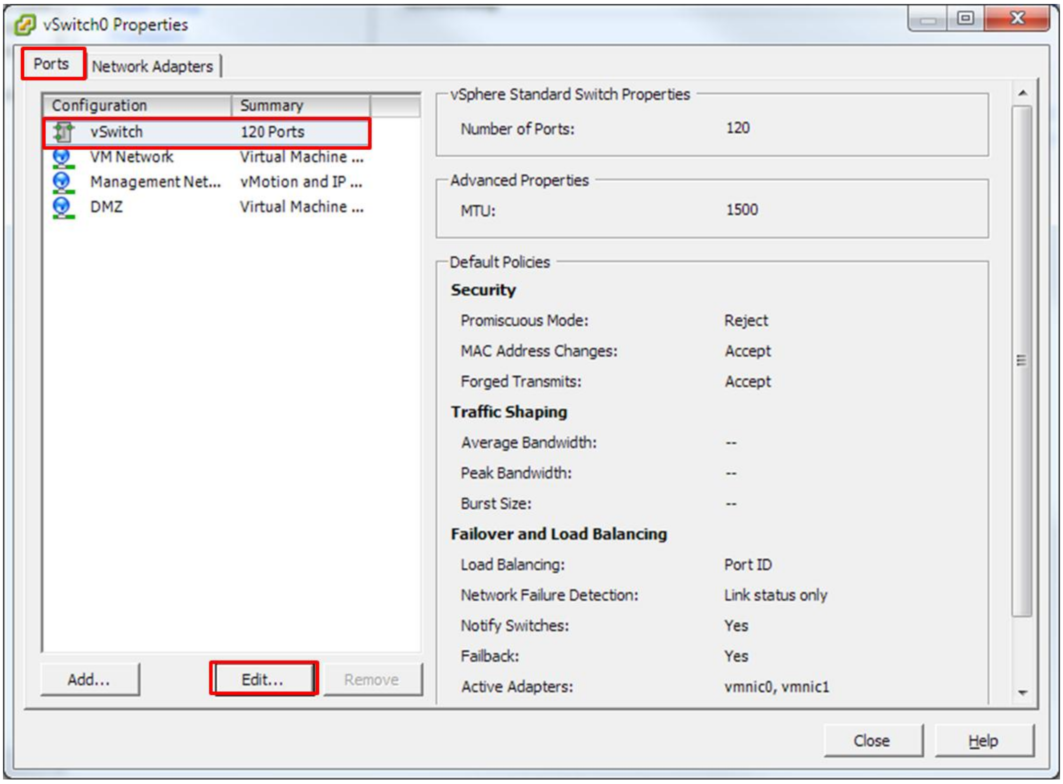
Policy Failover Order:

Select active and standby adapters for this port group. During a failover, standby adapters activate in the order specified below.

Configuration	Summary
vSwitch	128 Ports
Management Network	vMotion and IP Storage Port

Name	Speed	Networks
Active Adapters		
vmnic0	1000 Full	10.30.27.1-10.30.27.127
vmnic1	1000 Full	None
Standby Adapters		

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.



vSwitch0 Properties

Configuration	Summary
vSwitch	120 Ports
VM Network	Virtual Machine ...
Management Net...	vMotion and IP ...
DMZ	Virtual Machine ...

vSphere Standard Switch Properties

Number of Ports: 120

Advanced Properties

MTU: 1500

Default Policies

Security

Promiscuous Mode: Reject

MAC Address Changes: Accept

Forged Transmits: Accept

Traffic Shaping

Average Bandwidth: --

Peak Bandwidth: --

Burst Size: --

Failover and Load Balancing

Load Balancing: Port ID

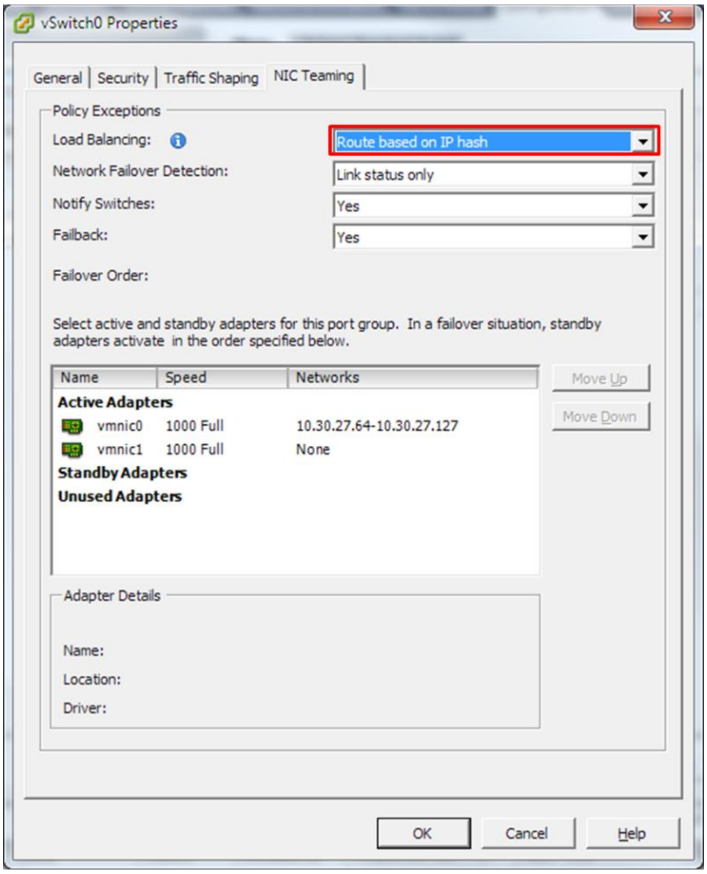
Network Failure Detection: Link status only

Notify Switches: Yes

Failback: Yes

Active Adapters: vmnic0, vmnic1

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.



Policy Exceptions

Load Balancing: Route based on IP hash

Network Failover Detection: Link status only

Notify Switches: Yes

Failback: Yes

Failover Order:

Select active and standby adapters for this port group. In a failover situation, standby adapters activate in the order specified below.

Name	Speed	Networks
Active Adapters		
vmnic0	1000 Full	10.30.27.64-10.30.27.127
vmnic1	1000 Full	None
Standby Adapters		
Unused Adapters		

Adapter Details

Name:

Location:

Driver:

References:

VMware ESXi5.0 Networking Documentation:
http://pubs.vmware.com/vsphere-51/index.jsp#com.vmware.vsphere.networking.doc/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/X8-1/Cisco-VCS-Virtual-Machine-Install-Guide-X8-1.pdf

VCS Port Use:
http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/X8-1/Cisco-VCS-IP-Port-Usage-for-Firewall-Traversal-Deployment-Guide-X8-1.pdf

Connecting Cisco UCM and VCS Deployment Guide:
http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/X8-1/Cisco-VCS-SIP-Trunk-to-Unified-CM-Deployment-Guide-CUCM-8-9-and-X8-1.pdf

VCS Control with Expressway Deployment Guide:
http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/X8-1/Cisco-VCS-Basic-Configuration-Control-with-Expressway-Deployment-Guide-X8-1.pdf

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.
The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS.CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnershiprelationship between Cisco and any other company. (1110R)

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain versionof the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional
and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership
relationship between Cisco and any other company. (1110R)