Networking Topology For Your System

This chapter describes the different networking topologies supported for this product, including the advantages and disadvantages of each. Select the one that best meets your needs and your network deployment.

☞

Important   If you want mobile users to attend meetings, then select a network topology that includes the Internet Reverse Proxy virtual machine. You must deploy the Internet Reverse Proxy regardless of how the mobile user attends a meeting.

When using a cellular data network, mobile users join the meeting through the Internet to the Internet Reverse Proxy. When using a local Wi-Fi connection, mobile users join the meeting through the Internet Reverse Proxy (non-split-horizon network topology) or directly to the internal virtual machines (split-horizon network topology).

Virtual Machine Layout in Your Network

Cisco WebEx Meetings Server comprises two groups of virtual machines: the internal virtual machines and the Internet Reverse Proxy virtual machines. All systems must comprise one or more internal virtual machines. The Internet Reverse Proxy is required only for systems where external users can host or attend meetings

from the Internet and mobile devices. Without an Internet Reverse Proxy, only internal and VPN users can host or join meetings.

☞

Important If you want mobile users to attend meetings, then select a network topology that includes the Internet Reverse Proxy virtual machine. You must deploy the Internet Reverse Proxy regardless of how the mobile user attends a meeting.

For more information about using an Internet Reverse Proxy, see Network Considerations for the Internet Reverse Proxy, on page 8.

Internal Virtual Machines

Internal virtual machines refer to the Admin virtual machine, and if applicable, the Media and Web virtual machines.

- The internal virtual machines *must* be on a single, common VLAN or subnet. During the system deployment, you will see error messages if your IP address assignments violate this rule. The system design assumes that all the internal virtual machines, including any HA virtual machines, are connected together on a local LAN, offering high bandwidth, negligible packet loss, and latency under 4 ms, between these virtual machines. The Cisco WebEx Meetings Server system is not designed to be split between multiple data centers.

- Cisco recommends placing all the internal virtual machines on the same Ethernet switch. However, when provisioning highly available systems you should deploy two Ethernet switches to ensure network level redundancy.

  Voice, data, video and the SAN all rely on the network bandwidth. It is critical to deploy a network that is capable of handling the required load.

- If you decide instead to place the virtual machines on different Ethernet switches within the same datacenter, then your network *must meet* the specific bandwidth and network latency requirements as described in Network Bandwidth Requirements, on page 9. In this situation, the switch-to-switch trunk must meet the same networking characteristics as the L3 latency and throughput for a single physical switch.

For additional information on systems with HA, see Redundant Network in HA Deployments, on page 7.

Different Types of Network Topology For Your System

This product supports the following network topologies:

Note   If your network topology includes forward proxies, they must meet specific requirements for the Internet Reverse Proxy to work properly. See the *Cisco WebEx Meetings Server Troubleshooting Guide* for complete details.

Internal Internet Reverse Proxy Network Topology

This section describes the network topology when all the virtual machines in your system, including the Internet Reverse Proxy, are in the same internal network.

Note   This configuration permits users to sign in and join meetings securely from the Internet without a VPN connection.

Note   If you are using automatic deployment, then the ESXi hosts for all your virtual machines (including the Internet Reverse Proxy) must be managed from the same VMware vCenter. This vCenter information is required during an automatic system deployment.

You will define the Administration URL, the WebEx Site URL, the private VIP address, and the public VIP address during the deployment of your system. For more information about these terms, and when you provide them, see the Installation section of the *Cisco WebEx Meetings Server Administration Guide*.

This is a schematic diagram of an all internal Internet Reverse Proxy network topology.
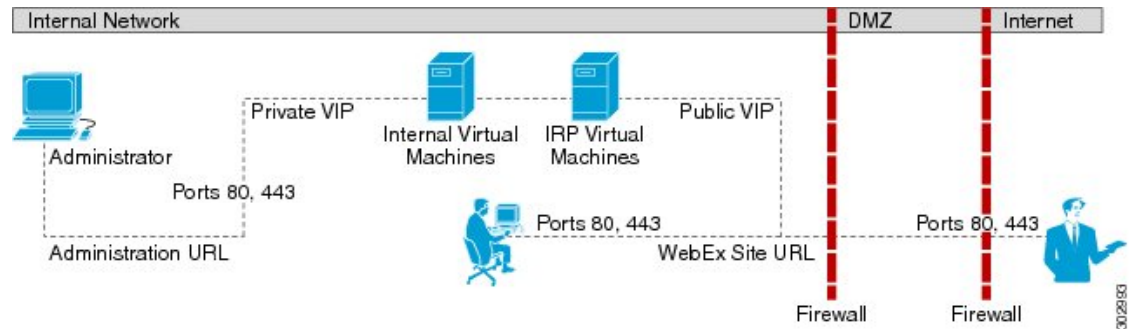
Note   For a complete list of the port access required for this deployment, see Port Access When All the Virtual Machines Are in the Internal Network.

Advantages of an All Internal Internet Reverse Proxy Network Topology

- Compared with the non-split-horizon network topology, there are no virtual machines in the DMZ.

- Compared with the non-split-horizon network topology, the network traffic for internal users will not connect through the DMZ to host or attend meetings.

Disadvantages of an All Internal Internet Reverse Proxy Network Topology

- Public access (allowing external users to access the system) requires opening inbound ports (80 and 443) directly from the Internet to the internal network.

For more information about Internet Reverse Proxies, see Network Considerations for the Internet Reverse Proxy, on page 8.

Non-Split-Horizon Network Topology

This section describes the network topology when you have a non-split-horizon DNS. The internal virtual machines (Admin, and if applicable, Media and Web) are in the internal network, and the Internet Reverse Proxy is in the DMZ network.

Note This configuration permits users to sign in and join meetings securely from the Internet without a VPN connection.

For this product, the primary difference between a split-horizon and a non-split-horizon network topology is that for a split-horizon system, internal users access the WebEx site URL using the private VIP address. External users (outside the firewall) access the WebEx site URL using the public VIP address. For a non-split-horizon network, all users (internal and external) access the WebEx site URL using the public VIP address.

You will define the Administration URL, the WebEx Site URL, the private VIP address, and the public VIP address during the deployment of your system. For more information about these terms, and when you provide them, see the Installation section of the *Cisco WebEx Meetings Server Administration Guide*.

This is a schematic diagram of a non-split-horizon network topology.
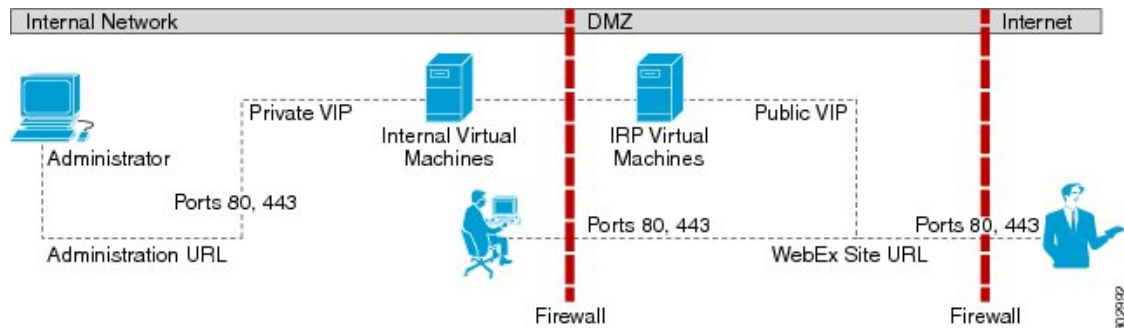
Note For a complete list of the port access required for this deployment, see Port Access With an Internet Reverse Proxy in the DMZ Network.

Advantages of a Non-Split-Horizon Network Topology

- Tight control on the traffic that comes in and goes out of a network.

- Addresses more common, simple DNS network requirements.

Disadvantages of a Non-Split-Horizon Topology

- Complex setup, but not as complex as the split-horizon network topology.

- Internal traffic is directed to the DMZ network. All network traffic from the Internet as well as from the internal (private network) goes to the Internet Reverse Proxy in the DMZ network, then comes back to the internal virtual machines.

- Requires more ports to be opened in the firewall between the DMZ and internal network than the all internal network topology.

- Automatic system deployment (for 50, 250, or 800 concurrent user systems only) requires a more detailed setup in vCenter.

- Of the three network topologies, this configuration most affects network performance, since all of the meetings load is through the Internet Reverse Proxy. Because there are multiple hops, network latency is affected as well.

Note Refer to Network Bandwidth Requirements, on page 9 for details about NIC speed requirements for non-split-horizon DNS deployments.

All Internal Network Topology

This section describes the network topology when all the virtual machines in your system are in the same internal network. There is no public access; only internal and VPN users can host or join meetings.

Note If you are using automatic deployment, then the ESXi hosts for all your virtual machines must be managed from the same VMware vCenter. This vCenter information is required during an automatic system deployment.

You will define the Administration URL, the WebEx Site URL and the private VIP address during the deployment of your system. For more information about these terms, and when you provide them, see the Installation section of the *Cisco WebEx Meetings Server Administration Guide*.

This is a schematic diagram of an all internal network topology.
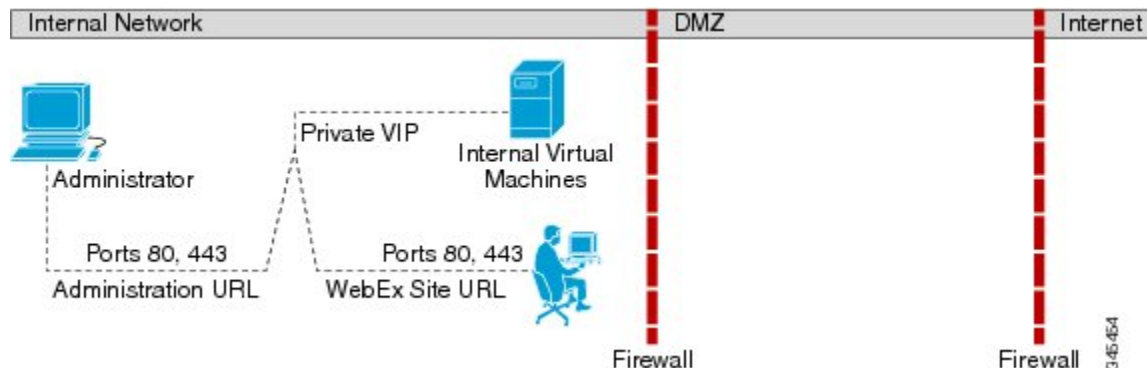
Advantages of an All Internal Network Topology

- Provides lower latency as there are fewer network hops between the virtual machines.

Disadvantages of an All Internal Network Topology

- There is no public access (allowing external users to access the system) and no access for mobile users.

Split-Horizon Network Topology

This section describes the network topology when you have a split-horizon DNS. The internal virtual machines (Admin, and if applicable, Media and Web) are in the internal network, and the Internet Reverse Proxy is in the DMZ network.
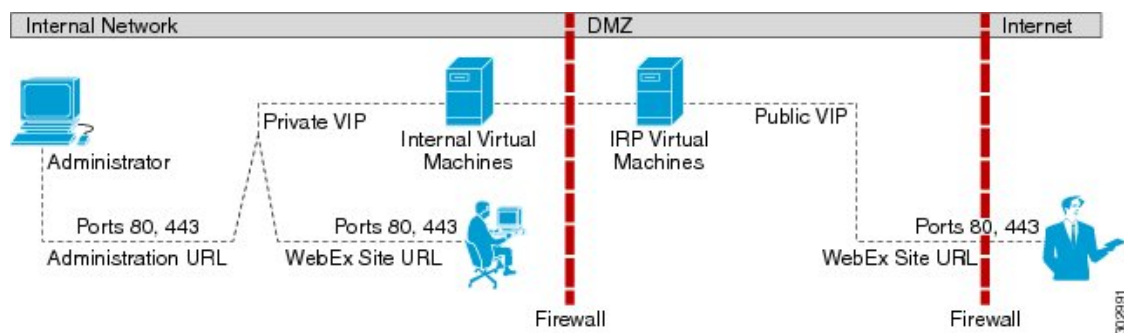
Note
This configuration permits users to sign in and join meetings securely from the Internet without a VPN connection.

In a split-horizon deployment, Internet-origin traffic (including mobile users employing a cellular data network) goes to the Internet Reverse Proxy. Internal-origin traffic (including mobile users employing local Wi-Fi) goes directly to the internal virtual machines.

For this product, the primary difference between a split-horizon and a non-split-horizon network topology is that for a split-horizon system, internal users access the WebEx site URL using the private VIP address. External users (outside the firewall) access the WebEx site URL using the public VIP address. For a non-split-horizon network, all users (internal and external) access the WebEx site URL using the public VIP address.

You will define the Administration URL, the WebEx Site URL, the private VIP address, and the public VIP address during the deployment of your system. For more information about these terms, and when you provide them, see the Installation section of the *Cisco WebEx Meetings Server Administration Guide*.

This is a schematic diagram of a split-horizon network topology.

Note
For a complete list of the port access required for this deployment, see Port Access With an Internet Reverse Proxy in the DMZ Network.

Advantages of a Split-Horizon Network Topology

• Tight control on the traffic that comes in and goes out of a network.

• There is a separation of network traffic hitting the system, enabling a more distributed spread of the load.

  The traffic coming in from the Internet will go to the Internet Reverse Proxy. The traffic coming from the internal (private network) will go directly to the internal virtual machines (Admin, and if applicable, Media and Web).

• Performance and network latency is better than a non-split-horizon DNS, but worse than an all internal network topology.

Disadvantages of a Split-Horizon Topology

• Of the three different network topologies, this is the most complex setup.

• Requires sophisticated DNS mapping.

• Requires more ports to be opened in the firewall between the DMZ and internal network than the all internal network topology.

• Automatic system deployment (for 50, 250, or 800 concurrent user systems only) requires a more detailed setup in vCenter.

• Because of web redirection, for internal users, the WebEx site URL is replaced with the URL exposing the hostname of the virtual machine containing the web services as well as the Media virtual machines.

Refer to Network Bandwidth Requirements, on page 9 for details about NIC speed requirements for split-horizon DNS deployments.

Redundant Network in HA Deployments

Cisco WebEx Meetings Server does not implement High Availability (HA) in the traditional sense where you deploy a primary system, then deploy a second HA system, and then join both into a HA pair. Instead, Cisco WebEx Meetings Server combines the primary system and the HA system into one single system. For details on each system size, see Deploying Your System in a Single Datacenter.

• The redundant (HA) virtual machines must be co-located in the same data center with the primary virtual machines. All these virtual machines must be on the same VLAN or subnet. The speed and latency requirements for connectivity between the primary and HA components are the same as defined previously for the primary virtual machines.

> ☞
>
> **Important** Cisco does not support splitting the primary and redundant (HA) components of the system between data centers.

• Connectivity between all the internal virtual machines, both primary and HA, must be fully redundant, so that the failure of a switch or network link will not sever the connectivity between the primary and HA components. To achieve this redundancy, each host server should have dual redundant connections to a pair of Ethernet switches (that is, a connection to switch A plus a connection to switch B).

- The primary and redundant (HA) Internet Reverse Proxy virtual machines must be on a common VLAN or subnet (typically not the same subnet as the internal virtual machines). Connectivity between these two Internet Reverse Proxy virtual machines should be fully redundant, in the same manner as the internal virtual machines.

Network Considerations for the Internet Reverse Proxy

The Internet Reverse Proxy virtual machines share the same general networking requirements as the internal virtual machines. For the non-split-horizon and split-horizon DNS configuration, the Internet Reverse Proxy virtual machines are deployed in your DMZ network and not the internal network.

Restriction Even if the Cisco UCS Servers are configured with two NICs, Cisco WebEx Meetings Server does not support pointing one NIC to the Internet and the other NIC to the Intranet. This restriction applies regardless of the mappings between the physical NICs and virtual NICs used by vSphere (and the Internet Reverse Proxy).

The Internet Reverse Proxy virtual machine always connects to a single external VLAN regardless of the number or NICs you use. If you use multiple physical NICs, and they are connected to different switches or routers, the NICs must still be connected to the same VLAN.

Therefore, you cannot use the Internet Reverse Proxy to bridge traffic between two separate network segments (with one pointing to the Internet and the other pointing to the Intranet). The next section describes how you can accomplish this goal.

Latency Between Internal Virtual Machines and the Internet Reverse Proxy

The maximum acceptable round-trip latency on the path between the NIC on the Internet Reverse Proxy and the NIC on any of the internal virtual machines is 4 ms. Latency reduces the usable bandwidth on TCP connections, possibly resulting in a degraded user experience.

Note The 4 ms latency limit does not apply to the path between any of Cisco WebEx Meetings Server components and end users endpoints.

Network Traffic Isolation

You may set up network traffic isolation between the Internet and your internal network by using a DMZ Ethernet switch. The following procedure and diagram illustrate one example:

1 Connect the Internet Reverse Proxy to a head-end switch or router and use that switch or router to split the Internet and Intranet traffic.

2 Once the switch or router splits the traffic, then you can pipe those two traffic patterns to two separate physical ports on the switch or router. One port points to the Internet and other port points to the Intranet.

Here is a diagram of a sample network topology:
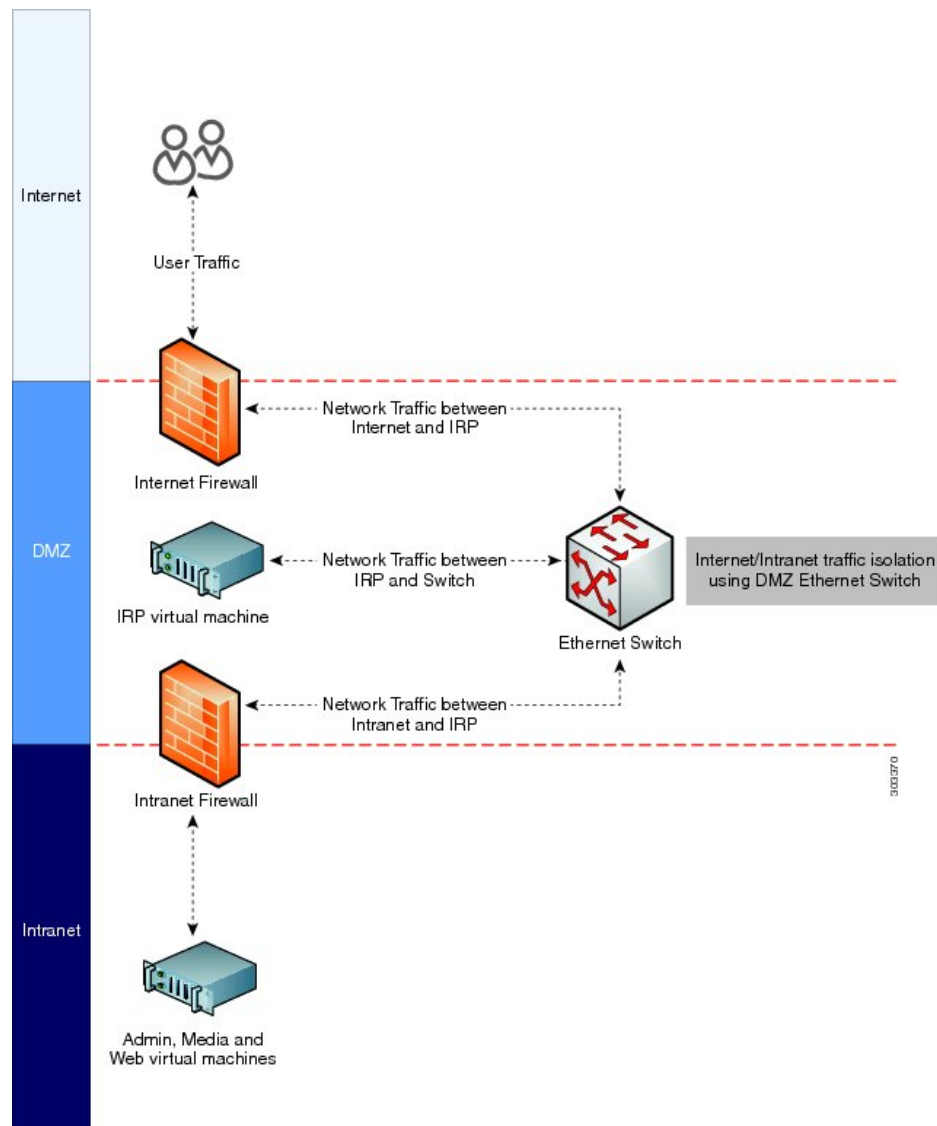
For information about network bandwidth requirements, see Network Bandwidth Requirements, .

Network Bandwidth Requirements

This section describes the bandwidth requirements for 50, 250, 800 and 2000 user systems. Meeting the bandwidth requirements outlined in the section will provide a quality end user experience for your users who host and attend WebEx meetings, and helps ensure that your network can support the traffic demands from the web sharing, audio, and video.

Estimating Bandwidth for End User Sessions

It is important to estimate the network bandwidth to support the traffic demands of video, audio, and web sharing for the size of your user system. The bandwidth requirements for this product are fundamentally the

same as for Cisco WebEx cloud services. If you wish to optimize your network provisioning, Cisco WebEx cloud services bandwidth usage is presented in the WebEx Network Bandwidth White Paper.

The information in the following table shows the expected bandwidth for video, audio and web sharing.

WebEx Meeting Component	Aggregate End User Session Bandwidth
Video (360p + 6 thumbnails)	1.5 Mb/s
Audio	0.1 Mb/s
Web sharing (This value assumes you flip a slide every 30 seconds.)	0.6 Mb/s
Total maximum bandwidth	2.2 Mb/s

Although 2.2 Mb/s is the maximum expected bandwidth for a single user connection, Cisco recommends using the maximum expected bandwidth of 1.5 Mb/s when calculating bandwidth requirements. Because only one-half of the maximum number of users can employ video, audio, and web sharing while the remaining users should use only audio and web sharing, this yields an average bandwidth of approximately 1.5 Mb/s per user connection.

If you refer to the *WebEx Network Bandwidth White Paper*, you will notice that the bandwidth values in the preceding table are based on worst-case traffic conditions. Average bandwidth utilization is *much* smaller, but Cisco recommends using worst case numbers for the following reasons:

- Using the worst case numbers for your calculation should help you provide the needed bandwidth to prevent a degraded user experience as a result of heavy usage.

- The Cisco WebEx Meetings Server sends the same data simultaneously to all the participants in a meeting. When a WebEx host flips a page on a presentation, an image of that page (possibly comprising several megabytes) is sent separately to each endpoint, simultaneously, and as quickly as possible.

Bandwidth on Network Paths

Use the following process to determine the necessary bandwidth on various network paths.

1 Determine the averaged bandwidth for a user session using the table provided in the preceding section.
2 Determine the maximum number of users you expect to connect simultaneously over that link.

3 Multiply the total bandwidth by the maximum number of users.

Scenario examples:

- If you expect a maximum of 100 users to connect concurrently from the Internet, you will probably need 1.5 Mb/s x 100 = 150 Mb/s of available bandwidth on your ISP connection and through your external firewall to the Internet Reverse Proxy. For mor details about Internet Reverse Proxy, see Network Considerations for the Internet Reverse Proxy, on page 8

- Assume you have a 2000 user system with all connections going through the Internet Reverse Proxy. In this scenario, you need to assume traffic for all 2000 users will connect to the Internet Reverse Proxy, and then from the Internet Reverse Proxy to the internal virtual machines. The aggregate bandwidth

coming into the Internet Reverse Proxy from other parts of the network will be 2000 x 1.5 Mb/s = 3 Gb/s. For more details about non-split-horizon, see Non-Split-Horizon Network Topology, on page 4.

Note The same 3 Gb/s of traffic passes inbound and outbound through the Internet Reverse Proxy, requiring the NIC on the Internet Reverse Proxy to handle 6 Gb/s of user traffic. See the next section for more information about bandwidth requirements for the NIC on the Internet Reverse Proxy.

- Assume you have 2000 user system in a split-horizon DNS deployment. In this scenario, your Internet users will connect to the Internet Reverse Proxy while intranet users connect directly to the internal virtual machines. Assume ten percent of your users connect to a meeting using the Internet versus 90 percent of users connect to their meetings through the Intranet. The result is the aggregate bandwidth coming into the Internet Reverse Proxy will now be approximately 300 Mb/s (10 percent of 2000 users times 1.5 Mb/s equals 300 Mb/s). If that same 300 Mb/s of traffic passes from the Internet Reverse Proxy, the NIC on the Internet Reverse Proxy may be required to handle 600 Mb/s of user traffic. This is a dramatically lower bandwidth requirement than with a non-split-horizon DNS deployment described in the previous scenario. The reduction in network traffic has direct bearing on the recommendations for NIC or switch interface speed (see next section) which can result in you being able to deploy less expensive 1 Gb/s NICs on the Cisco UCS Server for the Internet Reverse Proxy or 1 Gigabit Ethernet Switch Infrastructure in DMZ network. For more details about split-horizon, see Split-Horizon Network Topology, on page 6.

Note You may be required to deploy 1 Gigabit Ethernet NICs configured for NIC Teaming if the Internet Reverse Proxy usage is marginally close to the 1000 Mb/s threshold.

See NIC Teaming for Bandwidth Aggregation, on page 13 for more details.

Bandwidth on Cisco WebEx Meetings Server Network Interfaces

For direct interfaces between your switching architecture and your system, we recommend provisioning your interface NICs to the maximum speeds shown in the following table. These speeds apply to the connectivity between the Cisco UCS Servers and ports on head-end switches in your local switching infrastructure only. These are the recommended speeds needed to support worst-case traffic requirements.

System Capacity	NIC or Switch Interface Speed
50 user system	1 Gb/s
250 user system	1 Gb/s
800 user system	10 Gb/s [1]
2000 user system	10 Gb/s [2]

[1] You may optionally choose to reduce network infrastructure costs by deploying NIC Teaming using two or more Gigabit Ethernet NICs on the UCS Server and NIC Teaming on the head-end switch.

[2] If you have a non-split-horizon DNS deployment, the 10 Gb/s requirement pertains to the IRP and internal virtual machines. If you have a split-horizon DNS deployment, you may be able to reduce the network infrastructure demands on your IRP (and DMZ network), which can result in you being able to deploy less

expensive 1 Gb/s NICs on the Cisco UCS Server for the Internet Reverse Proxy or 1 Gigabit Ethernet Switch Infrastructure in DMZ network, as described in the "Bandwidth on Network Paths" section. However the 10 Gb/s speed requirement holds true for the internal virtual machines (and internal network).

See the following section "Bandwidth Considerations for Split-Horizon DNS Deployments" for more information about using 1 Gb/s NICSs and Ethernet switches for a split-horizon DNS deployment.

Assumptions for NIC Speed Calculations:

- The aggregate end-user session bandwidth (1.5 Mb/s) was used to calculate the NIC speeds shown in the preceding table.

- The inter-virtual machine control traffic must be free of congestion. This especially applies to 2000 user systems and any system provisioned for high availability. Severe congestion on virtual machine links can result in system instability and consequent interruption of service.

- The connections to NAS storage, used for recording and database backup, must not be congested.

- Protocol overhead and implementation inefficiencies will result in usable link bandwidth that is significantly less than the 1 Gb/s or 10 Gb/s speed labels.

- If a large percentage of your traffic will hit the Internet Reverse Proxy when users log in to meetings, you need to remember that every user connection passes twice through the NIC on the Internet Reverse Proxy (inbound and outbound). Using the 2000 user system as an example, this means the NIC on the Internet Reverse Proxy may be required to handle 6 Gb/s of user traffic (2000 users times 1.5 Mb/s equals 3 Mb/s, times two for inbound and outbound traffic equals 6 Mb/s).

Conservatively, we ask that the local connections be no more than 60 percent used for end user media traffic, allowing the remaining 40 percent to be available for other traffic, unusual traffic bursts, and network overhead. Using the 800 user system as an example, we estimate the end user traffic at 1.2 Gb/s for the Admin and Media virtual machines and 2.4 Gb/s for the Internet Reverse Proxy virtual machine. Applying the 60 percent rule, we want the NIC to be capable of handling 2 Gb/s for the Admin and Media virtual machines (1.2 estimated user traffic for the Admin and Media virtual machines divided by 60 percent estimated normal bandwidth consumption equals 2.0 Gb/s) and 4 Gb/s for the Internet Reverse Proxy virtual machine.

Note The NIC speeds shown in the preceding table do not account for bandwidth used for accessing SAN storage. If Fibre Channel over Ethernet (FCoE) is used for a SAN connection, it should be provisioned to use an independent network interface.

Bandwidth Considerations for Split-Horizon DNS Deployments

With a split-horizon DNS deployment, some of your users will be logging in to meetings from the Internet and that traffic will hit the Internet Reverse Proxy, while the majority of users who are on the internal network will be logging into meetings without hitting the Internet Reverse Proxy. With a split-horizon DNS deployment, if you speed up your network and segment your traffic so that most of your traffic stays within the internal network (as opposed to hitting the Internet Reverse Proxy), you can potentially use NIC Teaming and provision a lower-end NIC (1 Gb/s NIC) on the Internet Reverse Proxy and provision the switching infrastructure between the Internet Reverse Proxy and the Internet to be 1 Gb/s, or at least lower than the recommended 10 Gb/s, for a 2000 user system.

For example, if a company has 100 users who want to access a 2000 port user system from the Internet concurrently, you would need a bandwidth of 150 Mb/s (1.5 Mb/s aggregate user session bandwidth * 100 users = 150 Mb/s). This implies that a network infrastructure from the DMZ network to the Internet Reverse Proxy can be 1 Gb/s Ethernet switches, and the Ethernet NIC interface on the Internet Reverse Proxy can be

1 Gb/s, as opposed to the stated 10 Gb/s interface requirement. Even when you factor in that the Internet Reverse Proxy sees double the traffic (meaning its NIC would have to handle 300 Mb/s of user traffic), applying the 60 percent rule (explained in the "Bandwidth on Cisco WebEx Meetings Server Network Interfaces" section) translates to 500 Mb/s. A 1 Gb/s link is still sufficient, but it would not be sufficient if we assumed 250 users instead of 100 users.

Note The optimization of bandwidth is only applicable for the NIC on the Internet Reverse Proxy in a split-horizon DNS deployments.

For non-split-horizon DNS deployments, you must deploy 10 Gb/s Ethernet switches and Ethernet NIC interfaces on the Internet Reverse Proxy.

NIC Teaming for Bandwidth Aggregation

Configuring NIC Teaming on your UCS Servers that contain the ESXi host with the internal virtual machines provides two advantages: NIC Teaming load balances the network traffic between physical and virtual networks, and provides failover in the event of a hardware failure or a network outage. In addition, for deployments where 10 Gb/s infrastructure is not available, it may be possible for you to team multiple 1 Gb/s NICs to achieve an equivalent result.

Note For more information about NIC speeds required for different size user systems, see the section "Bandwidth on Cisco WebEx Meetings Server Network Interfaces" in this chapter.

Cisco supports NIC Teaming for bandwidth load balancing for all user system sizes--50, 250, 800, and 2000 user systems--but it is most useful for customers who are trying to optimize networking costs for an 800 user system. The aggregate bandwidth requirements to and from Cisco UCS Servers and the head-end switches for an 800 user system are projected to be similar to using Dual 1 Gigabit Ethernet NICs (or Quad 1 Gigabit Ethernet NICs on a system with HA) to support worst-case traffic requirements, thereby alleviating the need to provision the UCS Servers with 10 Gigabit Ethernet NICs (or to purchase 10 Gigabit Ethernet head-end switches).

Note For information about provisioning NIC teaming in VMware, refer to the VMware documentation at http://kb.vmware.com and search for "NIC teaming in ESXi/ESX".

Assuming the use of traditional network interfaces and Ethernet switches, you can provide redundancy by using NIC teaming and duplicate switches, as outlined in the following process:

- Set up an Ethernet switch which supports IEEE 802.3ad/IEEE 802.1ax Link Aggregation Control Protocol (LACP).

- Using vCenter, connect the virtual machine port group associated with the Cisco WebEx Meetings Server virtual machines to both physical adapters.

- Connect both physical adapters to the switch.

- Provision the switch to statically provision the two ports as a team.

- Using VMware vSphere, set NIC Teaming to Active/Active to allow throughput on both NIC interfaces.

For example, for an 800 user deployment, two 1 Gb/s links may be substituted for each 10 Gb/s link on the ESXi host with the internal virtual machines, and four 1 Gb/s links may be substituted for each 10 Gb/s link on the Internet Reverse Proxy. (To get fault tolerance on a system with HA, as described in the section "Redundant Network Connections for HA Deployments", it is necessary to double the number of links.) With the ESXi host with the internal virtual machines, connect two 1 Gb/s links to the first Ethernet switch *plus* two 1 Gb/s links to the second Ethernet switch.

Note   The example server configurations shown in the *Cisco WebEx Meetings Server System Requirements* do not include sufficient network interfaces to support NIC Teaming for this purpose.