A P P E N D I X B

Configuring Dual-NIC Cisco Unified Videoconferencing Solution Deployments

About the Functionality of Dual-NIC Deployments

This chapter provides general information about the dual-NIC deployment of the Desktop Server component of the Cisco Unified Videoconferencing Manager and its configuration.

Dual-NIC deployments provide a simpler network configuration as well as better security. Dual-NIC deployments are more secure, because ports between a DMZ and a private network do not need to be opened for Desktop Server. Dual-NIC deployments allow you to bridge the internal firewall. External client access is only granted to the external NIC. The internal NIC communicates with the internal network components (, Cisco Unified Videoconferencing 3500 Series MCU, and Cisco Unified Videoconferencing Manager) and internal clients.

Each of the two NICs is assigned to a separate IP address according to its IP network range. You must use a FQDN with DNS resolution on the private network for the internal IP and external IP on the extranet.
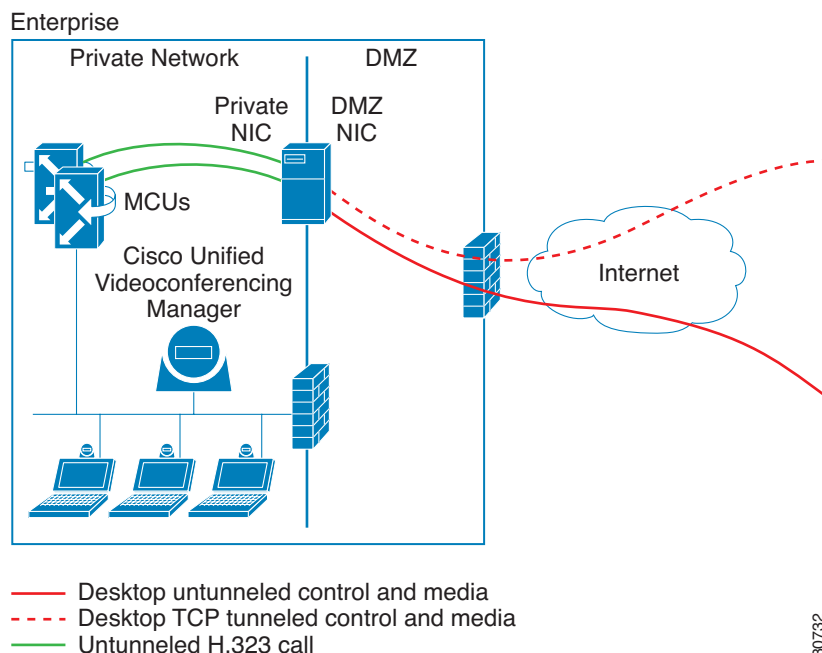
Note In large centralized deployments which use a load balancer, we recommend that you use the dual-NIC deployment.

If your Desktop Server has dual-NIC cards, one of the NICs resides in the enterprise network and the other NIC resides in the DMZ, as shown in Figure B-1.

Figure B-1   Small Deployment—Dual NICs

Installing a Desktop Server in Dual-NIC Deployment

Procedure

Step 1   Perform the installation as described in the "Installing a Desktop Server" section on page 2-5.

Step 2   During the installation, enter the private NIC address in the Desktop Server network interface address field.
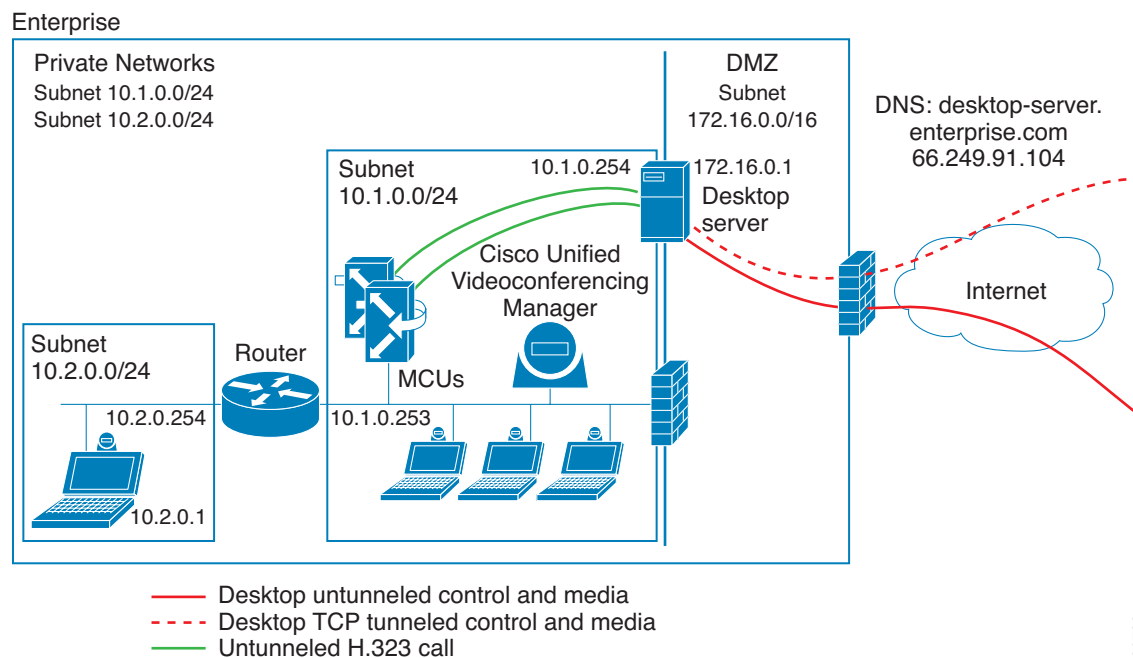
How to Configure Settings for Single/Dual-NIC Deployments

Deployment Examples

Typically a corporate private network is comprised of several IP subnets, each having its own IP range as shown in Figure B-2. Routers provide an access to the subnets; in the presented example subnets have the following ranges: 10.1.0.0/24 and 10.2.0.0/24.

Figure B-2   Dual-NIC Deployment Example

The Desktop Server can have multiple Network Interface Cards (NICs). Depending on the deployment and network configuration, you might want to control which NIC is used for various server communications.

In secure multiple NIC deployments you can use a NIC configured behind the firewall to communicate with various servers, while using another NIC to which the external Desktop Clients connect. You must configure the Desktop Server network interface address to represent the NIC behind the firewall. Then in the Public Address (FQDN) field on the Servers tab, enter a DNS name which resolves to the NIC outside the firewall and is accessible both inside and outside the corporate network. In the example presented in Figure B-2, the NIC for external Desktop Clients connection is 172.16.0.1, the NIC behind the firewall is 10.1.0.254, FQDN is desktop-server.enterprise.com, and the address 66.249.91.104 is statically mapped to 172.16.0.1

FQDN represents the Desktop Server IP address which both internal and external clients use for connection.

Desktop Clients can connect to the Desktop Server either by an IP or a DNS name. If a DNS name is not specified in the Public Address field, the Desktop Server network interface address is used. However, in many deployments the Desktop Server network interface address is not accessible to clients outside the intranet, due to NAT or firewall restrictions. Therefore, we recommend that you specify the Public Address, which must be a DNS name resolving to the correct Desktop Server IP address both inside and outside the corporate network. In the example presented in Figure B-2, the FQDN: sd.enterprise.com is resolved to 64.233.187.99 for external clients and to 10.1.0.254 for internal clients.

Configuring Desktop Server Network Interface

This section describes how to configure a network interface address for the Desktop Server. The Desktop Server communicates with these types of servers in the deployment:

- Cisco Unified Videoconferencing 3500 Series MCU and —For media and call setup.
- Cisco Unified Videoconferencing Manager or Cisco Unified Videoconferencing 3500 Series MCU—For moderation and meeting control.
- Cisco Unified Videoconferencing Streaming Server—For media and control.

Procedure

Step 1   Click **Status** in the sidebar of the Desktop Server Administration web user interface, and then click the link showing the Desktop Server IP address.

Step 2   Enter the IP address that the Desktop Server must use to communicate with various servers.

> **Note**   The light next to the **Address** field indicates whether connection to the Desktop Server is successful or not. When the light is red, a tooltip containing error details is displayed.

Step 3   For secure multiple NIC deployments, enter a DNS name in the **Public Address** field.

Step 4   Select the maximum call rate from the list.

Step 5   Click **OK** or **Apply**.

Modifying Static Routing Configuration

You must perform the procedure described in this section must be performed only for IP subnets located behind routers in a private network. Do not modify the static routing configuration for a private network subnet used by the Desktop Server. For example, for a deployment illustrated in Figure B-2 on page B-3, do not modify the static routing configuration for subnet 10.1.0.0/24.

Procedure

Step 1   Open the Windows command line window.

Step 2   Enter:

route add <IP subnet> mask <subnet mask> <router IP address> -p

For example,

route add 10.2.0.0 mask 255.255.255.0 10.1.0.253 -p

Step 3   Perform Step 2 for all IP subnets located behind routers.