



Innovative
Solutions

Omnicast Directory Failover System

Installation & Configuration Procedure for Omnicast 4.x

Genetec Technical Support

4/30/2010

© 2009 Genetec Inc. All rights reserved.

Genetec Inc. distributes this document with software that includes an end–user license agreement and is furnished under license and may be used only in accordance with the terms of the license agreement. The contents of this document are protected under copyright law.

The contents of this guide are furnished for informational use only and are subject to change without notice. Genetec Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this guide.

This publication may not be copied, modified, or reproduced in any form or for any purpose, nor can any derivative works be created there from without Genetec Inc.'s prior written consent.

Genetec Inc. reserves the right to revise and improve its products as it sees fit. This document describes the state of a product at the time of document's last revision, and may not reflect the product at all times in the future.

In no event shall Genetec Inc. be liable to any person or entity with respect to any loss or damage that is incidental to or consequential upon the instructions found in this document or the computer software and hardware products described herein. The use of this document is subject to the disclaimer of liability found in the end–user license agreement.

"Genetec", "Omnicast", "Synergis", "AutoVu", "Federation", the Genetec stylized "G" and the Omnicast, Synergis and AutoVu logos are trademarks of Genetec Inc., either registered or pending registration in several jurisdictions.

"Security Center" and the Security Center logo are trademarks of Genetec Inc.

Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.

All specifications are subject to change without notice.

Document Title: Omnicast Directory Failover System

Documentation Number:

Date: April 30, 2010

Table of Contents

1.	General Information	4
1.1.	Document Revision.....	4
1.2.	Contacting Technical Assistance.....	5
2.	Basics of Directory Failover	6
3.	Preparation	6
3.1.	License Verification.....	6
3.2.	Time Synchronization	7
3.3.	Network Connectivity.....	7
4.	Server Installation on the Primary and Failover Servers	7
5.	Scenario #1: Simple Scenario	10
5.1.	Configuration on the Primary Server.....	10
5.2.	Configuration on the Failover Server	13
5.3.	Verifying the Omnicast services in the Config Tool.....	17
5.4.	Running the DFC Wizard.....	18
6.	Scenario #2: Local Directories	23
6.1.	Configuration on the Primary Server.....	24
6.2.	Configuration on the Failover Global Directory Server	24
6.3.	Configuration on the Failover Local Directory Server	24
6.4.	Verifying the Omnicast services in the Config Tool.....	29
6.5.	Running the DFC Wizard.....	30
7.	Failover synchronization process	35
8.	Troubleshooting Directory Failover Issues.....	38
8.1.	Clients do not connect to failover Directory	38
8.2.	Directory on failover server is always started.....	41
8.3.	Status shows “Software Broken”	44
9.	Appendix A: Scenario #3: Global Directories With No Multicast	45
9.1.	Configuration on the Primary Server.....	45
9.2.	Configuration on the Failover Local Directory Server	45
9.3.	Verifying the Omnicast services in the Config Tool.....	45
9.4.	Running the DFC Wizard.....	46
9.5.	Modifying the Gateway on Failover Server	48

Omnicast Directory Failover System

Installation & Configuration Procedure for Omnicast 4.x

1. General Information

The purpose of this document is to guide integrators and Omnicast system administrators on how to install and configure an Omnicast Directory Failover system (FOS).

This article applies only to Omnicast 4.x versions. The screenshots were taken from an Omnicast 4.5 system so there may be minor differences if your system is another version. This should not have an effect on the procedure unless specified.

1.1. Document Revision

Date	Description
2007-10-05	Initial version for Omnicast 4.1 (by Ismael Picot).
2010-01-01	Updated document.
2010-02-12	Update local Directories diagram.
2010-04-30	Added public address config; Added Appendix A.

1.2. Contacting Technical Assistance

Customers can reach Genetec's Technical Assistance Center (GTAC) using any one of the following methods:

Log in to Genetec's Technical Assistance Portal (GTAP)

<https://GTAP.genetec.com/>

Send questions, via e-mail, to:

support@genetec.com

Telephone questions to the GTAC at:

1-514-856-7100

or

1-866-338-2988 (Canada and US only)

FAX questions to the GTAC at: 1-514-332-1692

From Monday to Friday, 8:00 AM to 8:00 PM (Eastern time, GMT -5h)

No matter which method is used to reach the GTAC, customers should be ready to provide all relevant information describing the problem or question, including System ID and version information.

2. Basics of Directory Failover

In Omnicast, the Directory is responsible for the system configuration and user authentication. In the event that the Directory server fails or becomes unavailable, no client applications will be able to login. For the system to be more fault-tolerant, Omnicast has a feature called the Directory Failover Coordinator which stops or starts the backup or failover Directory, depending on the state of the primary Directory.

The Directory Failover Coordinator (DFC) is responsible for the following functions:

- Keeps the Failover Directory databases (containing configurations and alarms) up to date while on standby.
- Starts and stops the local Directory services when appropriate, based on the failover list and the polling of Directories
- Upon primary Directory failure, the next available Directory in the failover list takes over as the main Directory

When the primary Directory is restored and functional:

- The primary Directory pushes its configurations to all failover Directories (from Omnicast 4.1 and on).
- Changes made to the failover Directories during failover are lost (unless a shared SQL server architecture is used) (from Omnicast 4.1 and on).
- Alarms are not lost after failback, as the Alarm DB synchronization is bidirectional.

3. Preparation

This section details steps that should be performed prior to installing or configuring the Directory FOS.

3.1. License Verification

The Directory Failover is a license option as it is with many other Omnicast features. Please verify that the failover server has one **Failover directory server** option.

License Contents

Part Number	Description	Qty
Om-E-1FOD-41*	1 Failover directory server	1

This license option should create the same Directory options on the failover Directory as on the primary Directory.

3.2. Time Synchronization

Prior to installing the Failover Directory server, the time synchronization between the two servers must be checked. Please ensure that your Directory servers are synchronized on the same time source.

If you do not have a time source on your network, please refer to the Knowledge Base article **KB0000022** in the Genetec Technical Assistance Portal (GTAP).

Failure to synchronize the time between your servers could result in registry and database corruption and unexpected behaviour.

The time synchronization is CRITICAL. Please do not proceed any further unless you are sure your two servers are time synchronized.

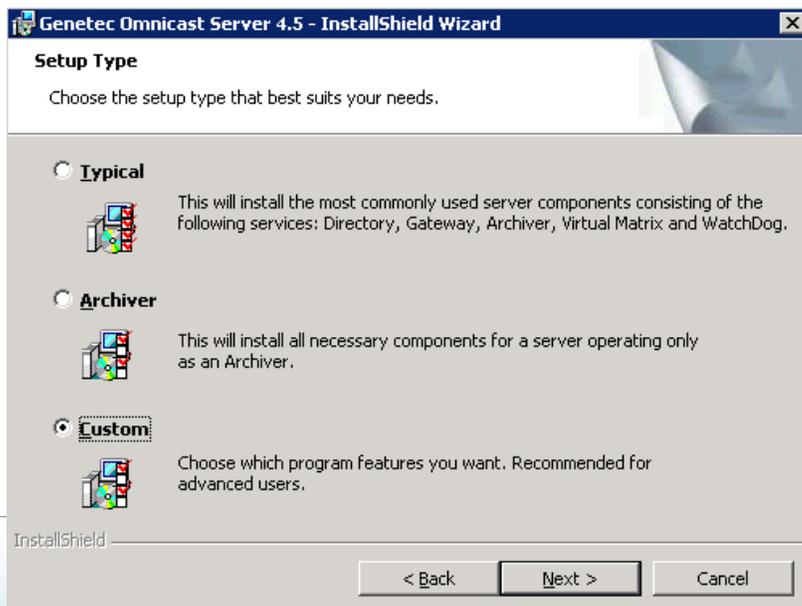
3.3. Network Connectivity

Verify that the Omnicast servers have network connectivity between them (i.e. “ping” successfully).

4. Server Installation on the Primary and Failover Servers

Please perform the following steps to install the necessary Omnicast services on the primary and failover services:

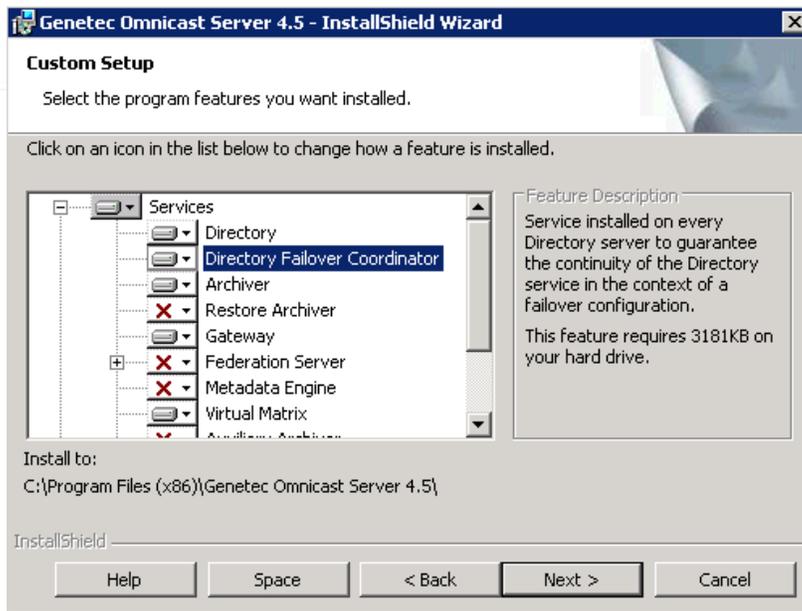
- 1) Run the setup.exe (Server option) from the Omnicast install package.
- 2) When you reach the Setup Type screen, choose **Custom**.



3) The following services are **MANDATORY** for the FOS:

- **Directory**
- **Directory Failover Coordinator**
- **Gateway**

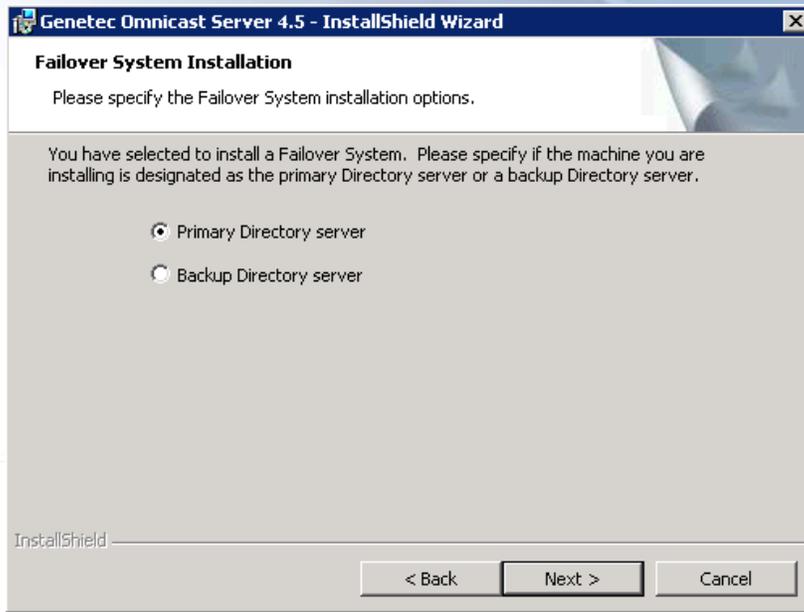
These three services **MUST** be installed on **BOTH** servers (the primary server and the failover server). The other services, like Archiver or Virtual Matrix, are optional.



Once finished, click **Next**.

4) When you reach the Failover System Installation screen:

- On the **primary server**, choose "Primary Directory server".
- On the **failover server(s)**, choose "Backup Directory server".



Once finished, click **Next**.

- 5) On the failover server, since you chose “Backup Directory server”, you will have to enter the IP address of the primary Directory server in the next screen.



In Omnicast versions 4.2 and higher, the connection type Directory or Gateway can be selected here. If multicast is supported on the network, select Directory. If multicast is not supported, select Gateway. This option can be changed later using the Directory Failover Coordinator (DFC) wizard in the Config Tool.

Once finished, click **Next**.

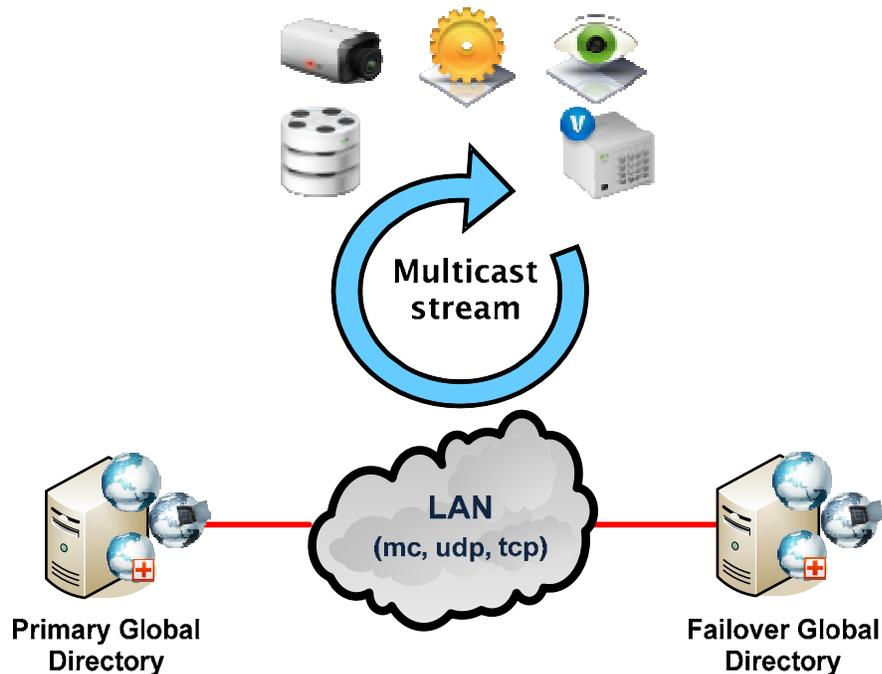
- 6) Click **Next** until the installation finishes.

5. Scenario #1: Simple Scenario

The configuration of the servers for a Directory FOS can be different depending on many different factors. The following sections describe different scenarios which should depict most of the FOS possibilities. Please choose the scenario that best matches your setup.

The “simple” scenario typically applies on most systems. This scenario has the following requirements:

- 1) Only two servers are involved in the Directory FOS: Primary server and failover server
- 2) Multicast must be supported on the network
- 3) Both servers are on a LAN with good network bandwidth (100 Mbps or higher)



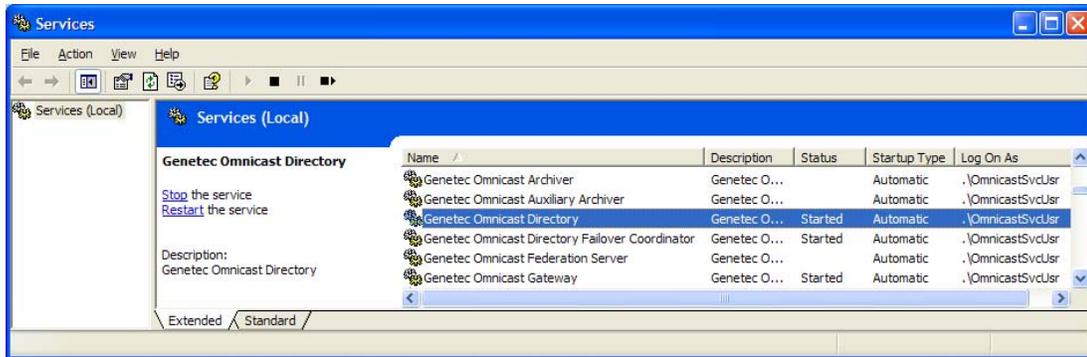
5.1. Configuration on the Primary Server

Please perform the following steps on the primary server:

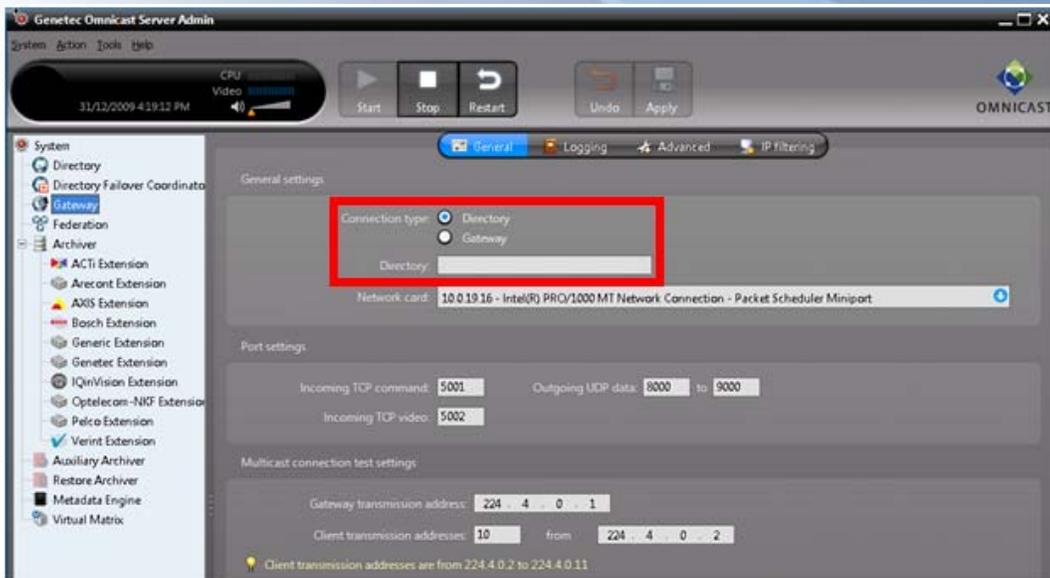
- 1) Verify that the **Directory**, **Directory Failover Coordinator** and **Gateway** services are started, as seen in the Omnicast Server Admin:



- 2) Verify that the startup type for these three services is set to **Automatic**. You can access the Windows services by going to Control Panel / Administrative Tools / Services



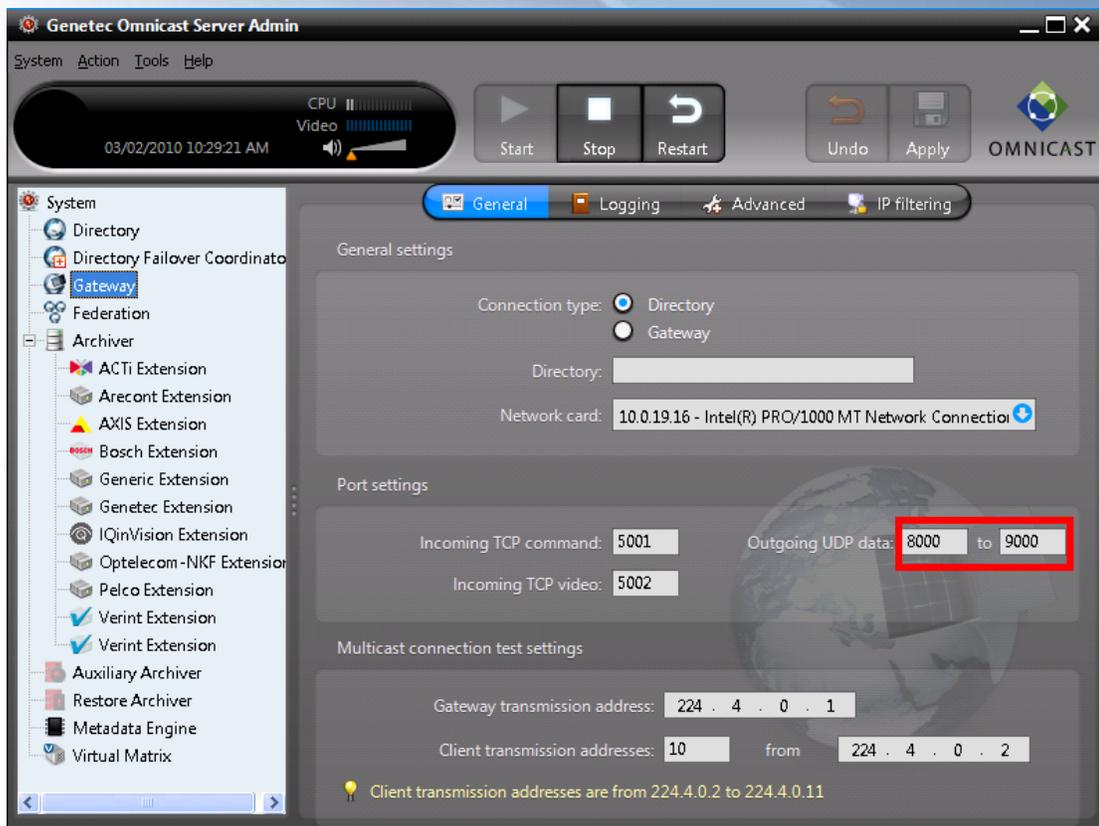
- 3) The Gateway must have a "Directory" as the Connection Type. In the Directory field, leave it blank or put the local IP address:



- 4) All the other services (like Directory Failover Coordinator, Archiver, Virtual Matrix, etc.) must point to the local Gateway using the local IP address or leaving it blank.



- 5) Verify that the Gateway is configured with the following **Outgoing UDP data** port range: 8000-9000. If not, please change it.



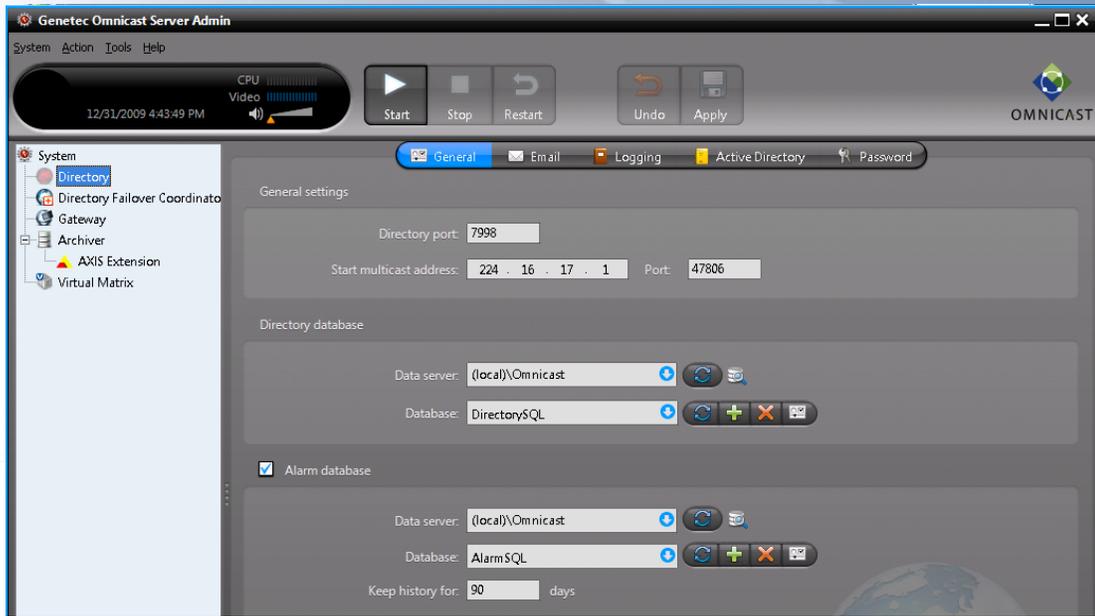
6) Go to System > Network and set the public IP address.



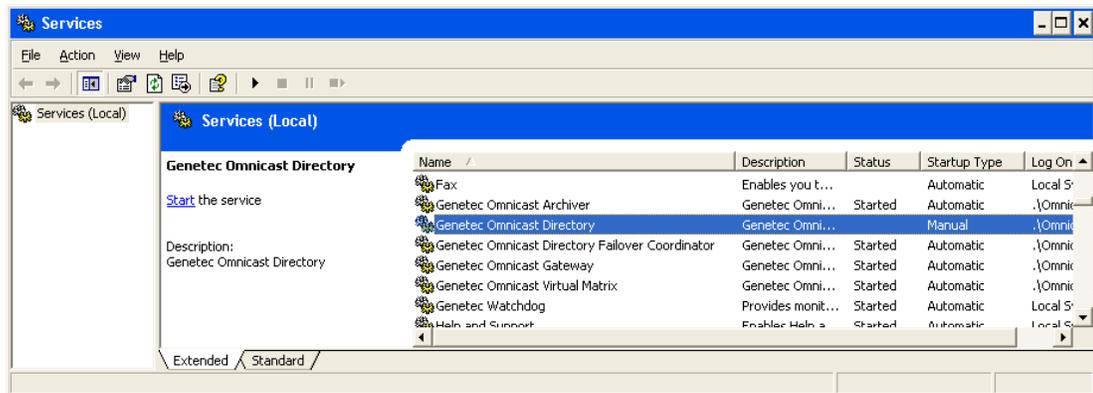
5.2. Configuration on the Failover Server

Please perform the following steps on the Failover Server:

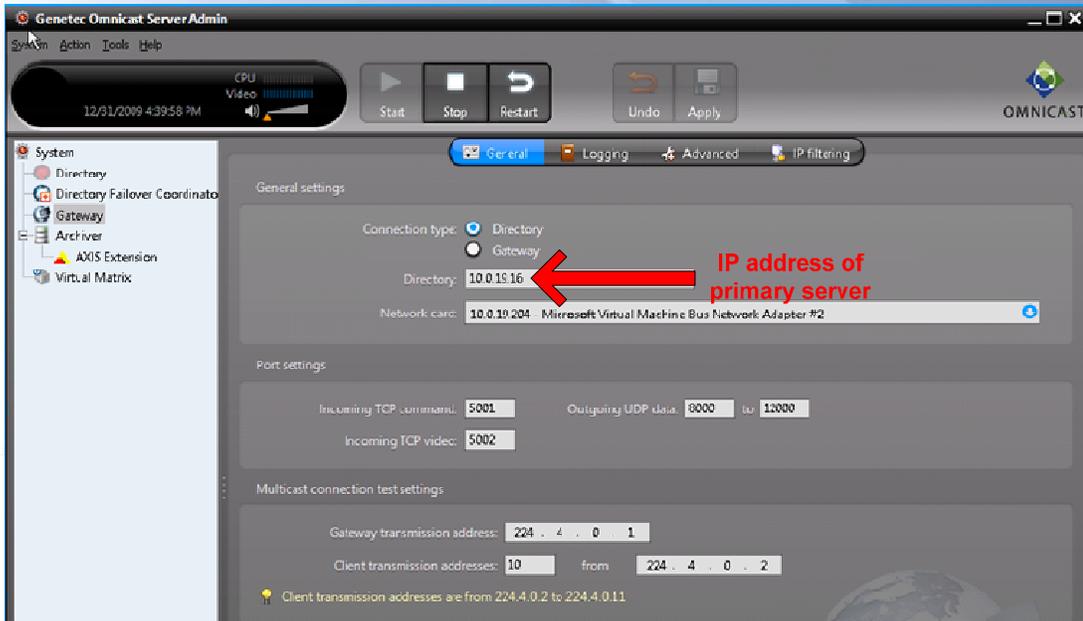
- 1) Verify that the Directory service is stopped and its startup type is set to "Manual". The Directory Failover Coordinator and Gateway services should be started.



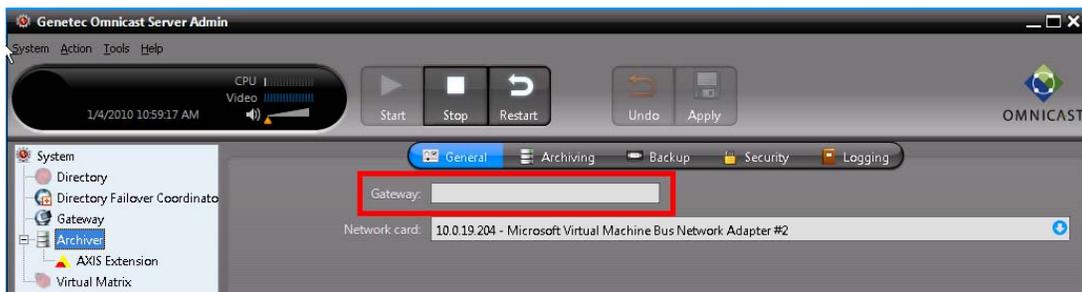
You can access the Windows services by going to Control Panel / Administrative Tools / Services:



- 2) The Gateway must have "Directory" as the Connection Type. In the Directory field, put the IP address of the primary server.



- 3) All the other services (like Directory Failover Coordinator, Archiver, Virtual Matrix, etc.) must point to the local Gateway using the local IP address or leaving it blank.



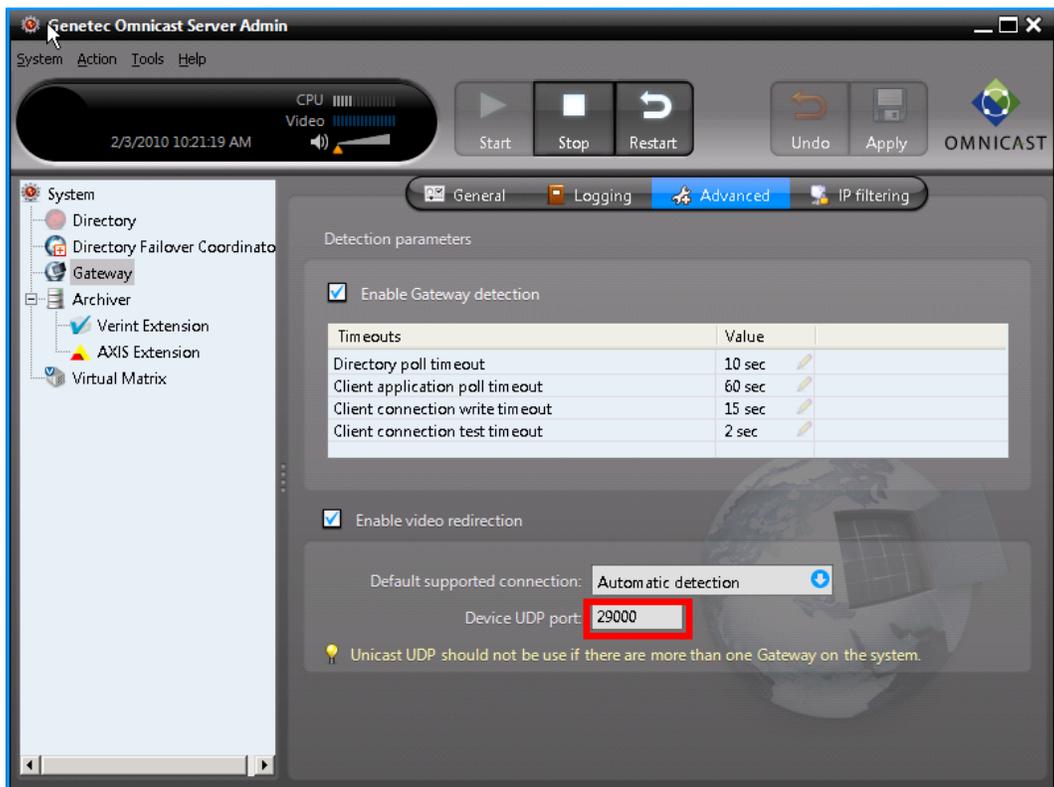
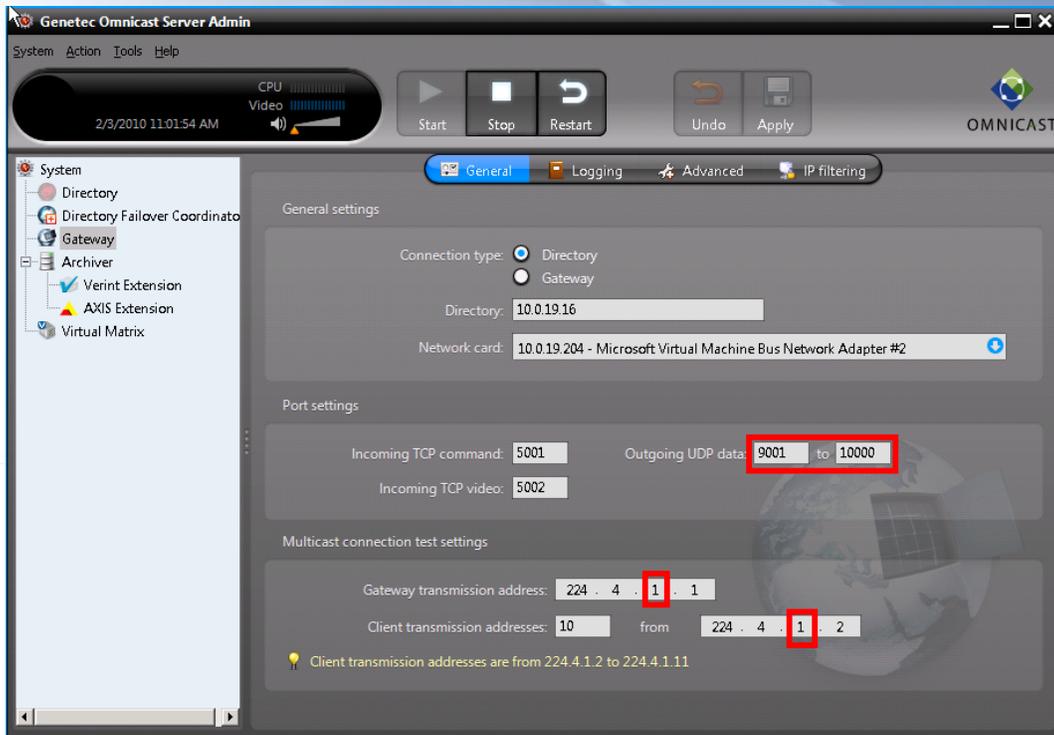
- 4) Since there are multiple Gateways in this scenario, it is better to allocate different test addresses and UDP ports to avoid any conflicts. The following settings need to be changed. The values indicated are suggested (they can be different depending on your system):

Gateway > General

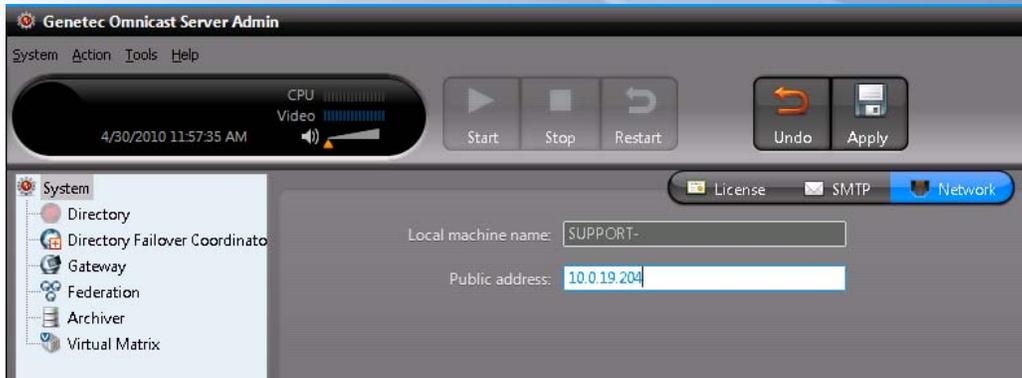
- a. Outgoing UDP data: 9001-10000
- b. Gateway transmission address: 224.4.1.1
- c. Client transmission addresses from: 224.4.1.2

Gateway > Advanced

- a. Device UDP port: 29000



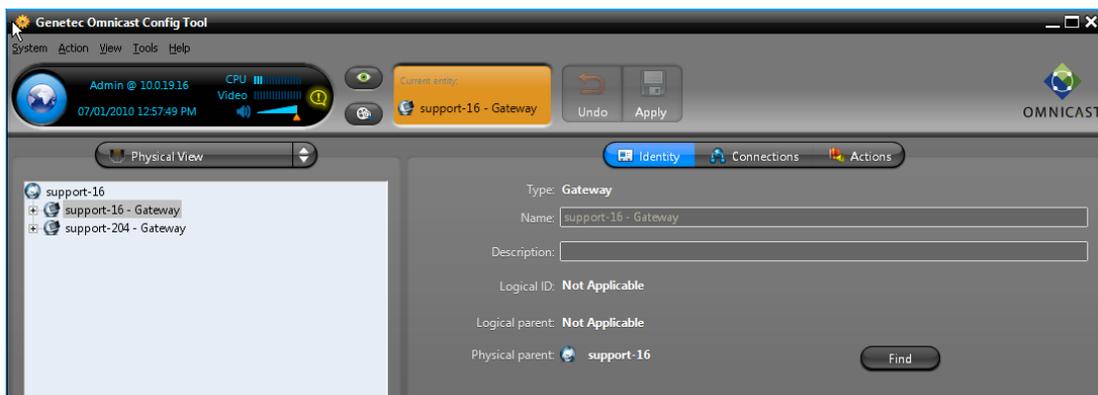
5) Go to System > Network and set the **Public address** with its local IP address.



5.3. Verifying the Omnicast services in the Config Tool

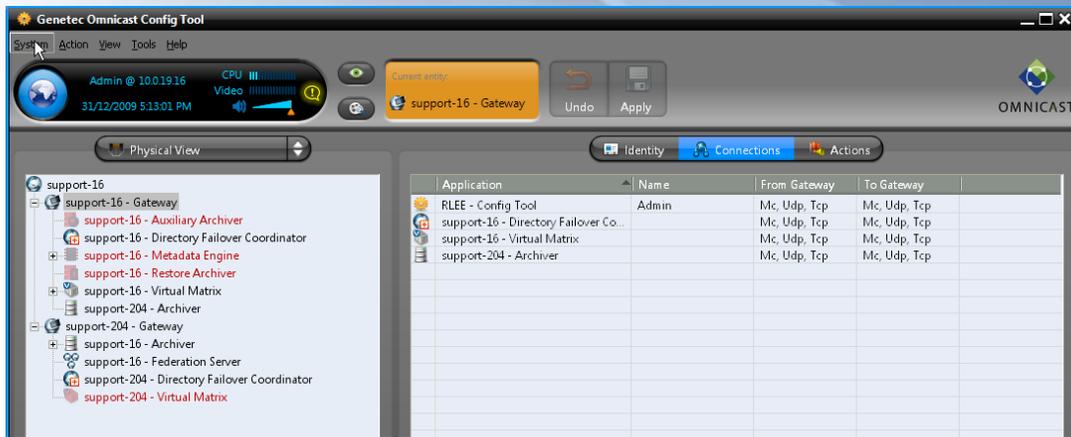
Please perform the following to verify that the Omnicast services on both servers have been properly configured and detected by the main Directory:

- 1) Open the Config Tool / Physical View.
- 2) Verify that both the primary and failover servers have the following services:
 - a. Directory Failover Coordinator
 - b. Gateway
- 3) Verify that both Gateways appear in the same level under the Directory.

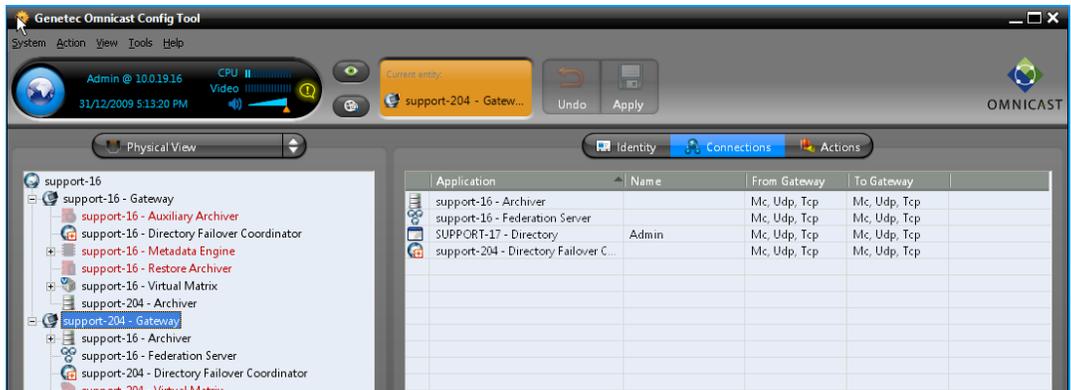


- 4) Go to the Physical View / Gateway / Connections.
- 5) In BOTH Gateways, all the services under both the "From Gateway" and "To Gateway" columns should have **Mc, Udp, Tcp**. Do not continue if you do not see Mc, Udp, Tcp in both columns as this scenario does not apply to your system.

Primary Gateway:



Failover Gateway:

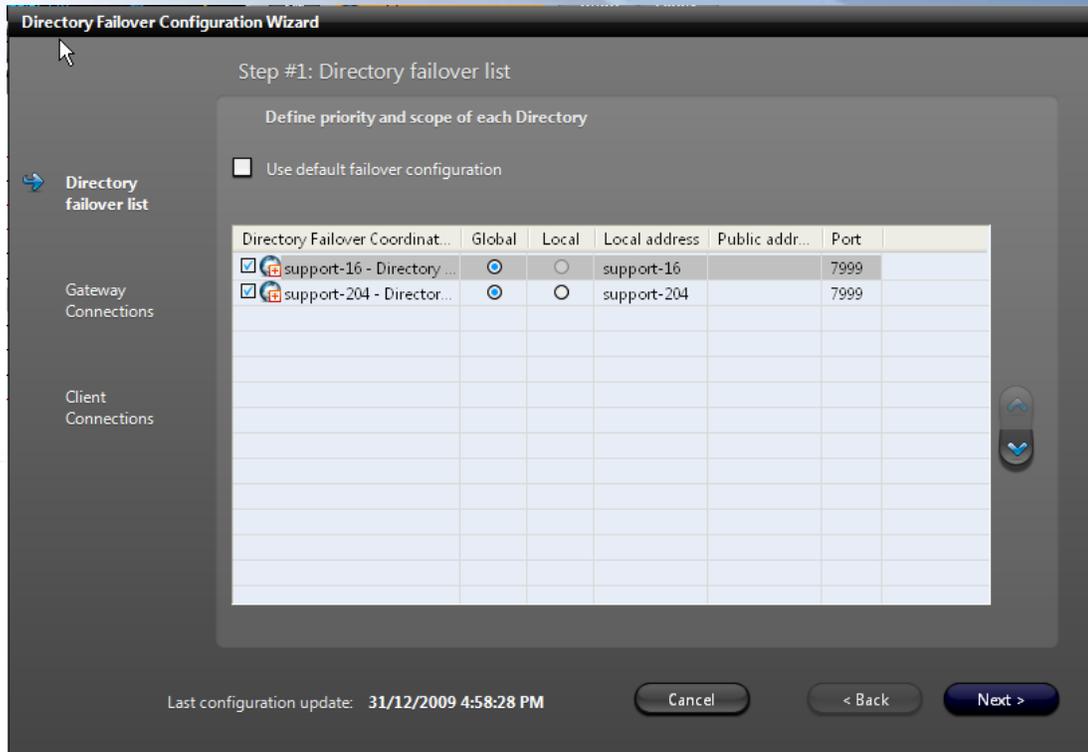


Note: It is possible that some services will not connect to its local Gateway and appear under the other Gateway (like support-204 Archiver shown in the above screenshots). Since multicast is supported on the network, it does not matter which Gateway the services actually connect to.

5.4. Running the DFC Wizard

The next step is to run the Directory Failover Configuration (DFC) Wizard to configure the failover list. Please perform the following steps:

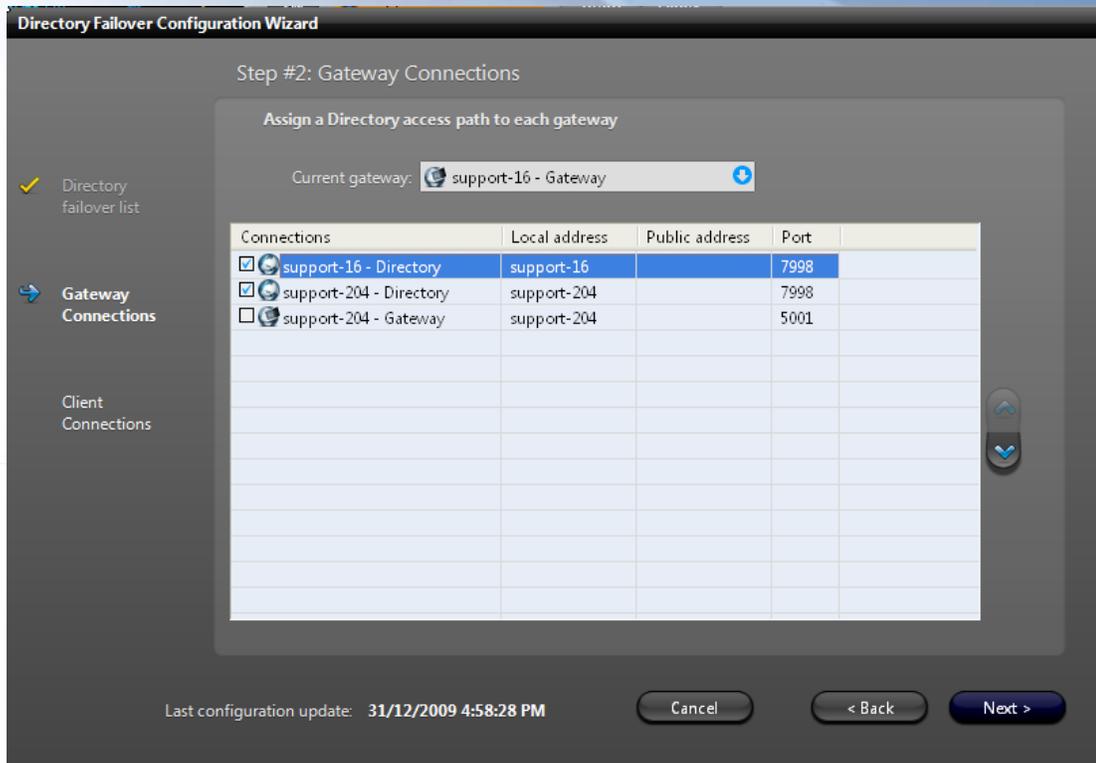
- 1) In the Config Tool, go to Tools / **Configure Directory Failover**. The Directory Failover Configuration Wizard will pop open.
- 2) **Uncheck** the box "Use default failover configuration".
- 3) Check both servers and make them **Global**. The order of the list is important: the first server in the list is the primary; the second server in the list is the failover or backup.



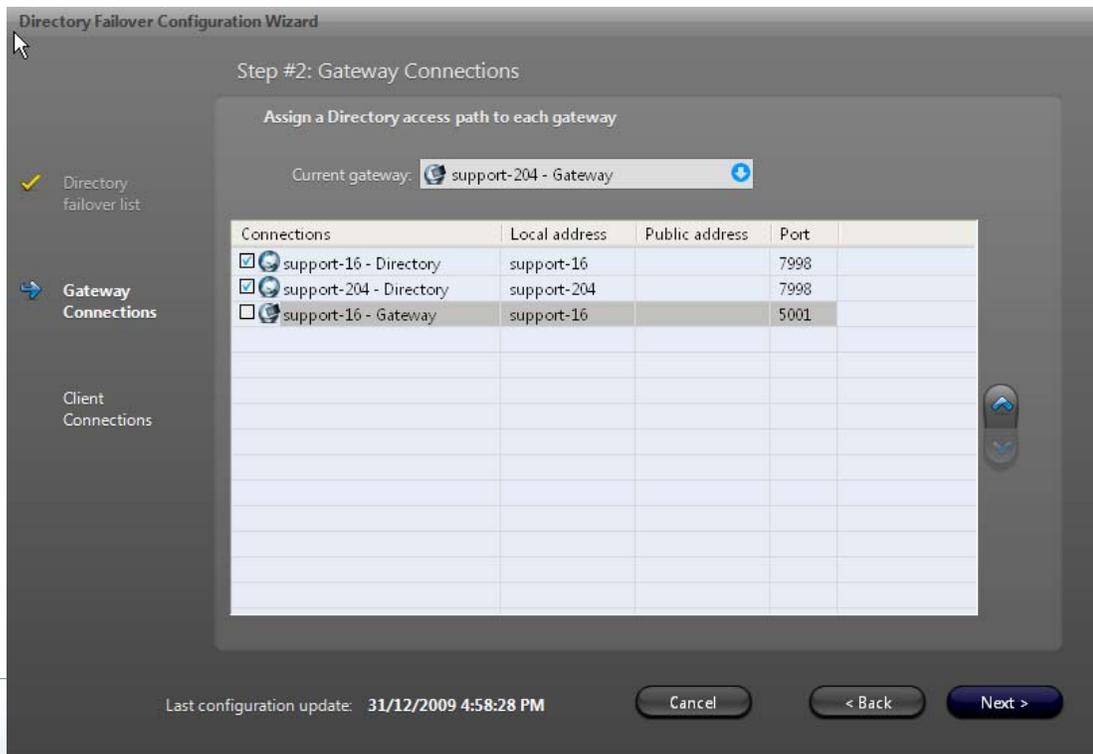
4) Click **Next**.

5) Step #2 in the DFC Wizard is to configure the Gateway connections. This step will define the order each Gateway will try to connect to the Directory.

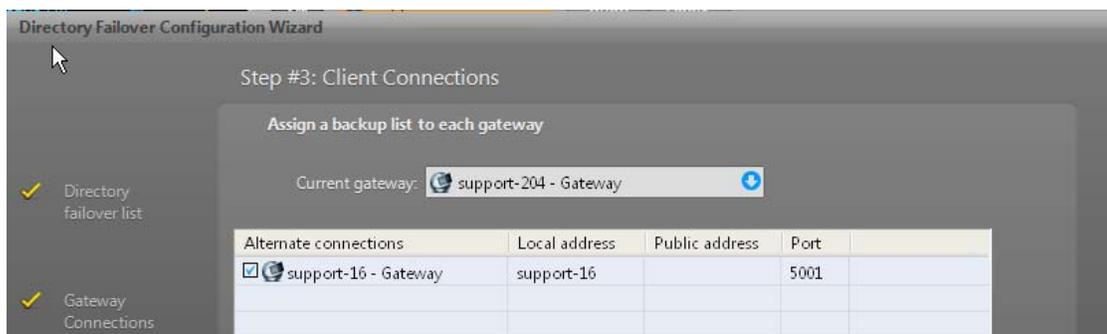
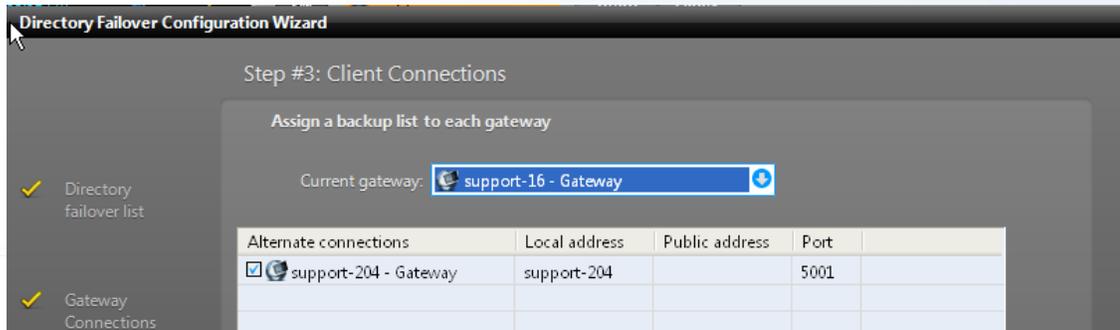
From the drop down list, select the **primary Gateway**. Using the up and down arrows, change the order of the list to have the primary Directory first and the backup Directory second. The Gateway machine should NOT be checked in this scenario. Check the two Directories as follows:



- 6) From the drop down list, select the Gateway on the failover server. The list should be configured the same as the primary Gateway as in the previous step.



- 7) Click **Next**.
- 8) Step #3 in the DFC Wizard is to configure the client connection list. Since there are only two Gateways, the alternate connection is always the other Gateway. Just ensure the connection list is similar to the following:



- 9) Click **Finish**. After clicking this button, the DFC services will restart and the synchronization process will begin. Please refer to the next section for a description of the synchronization process.
- 10) In the Physical View, the primary DFC should appear under the same level as the Gateways and the failover DFC should appear under its local Gateway.

Genetec Omnicast Config Tool

System Action View Tools Help

Admin @ 10.0.19.16 CPU Video
31/12/2009 5:43:44 PM

Current entity: support-204 - Gatew... Undo Apply

OMNICAST

Physical View

Identity Connections Actions

support-16

- support-16 - Gateway
 - support-16 - Auxiliary Archiver
 - support-16 - Metadata Engine
 - support-16 - Restore Archiver
 - support-16 - Virtual Matrix
 - support-204 - Archiver
- support-204 - Gateway
 - support-16 - Archiver
 - support-16 - Federation Server
 - support-204 - Directory Failover Coordinator
 - support-204 - Virtual Matrix
 - support-16 - Directory Failover Coordinator

Application	Name	From Gateway	To Gateway
support-16 - Archiver		Mc, Udp, Tcp	Mc, Udp, Tcp
support-16 - Federation Server		Mc, Udp, Tcp	Mc, Udp, Tcp
SUPPORT-17 - Directory	Admin	Mc, Udp, Tcp	Mc, Udp, Tcp
support-204 - Directory Failover C...		Mc, Udp, Tcp	Mc, Udp, Tcp

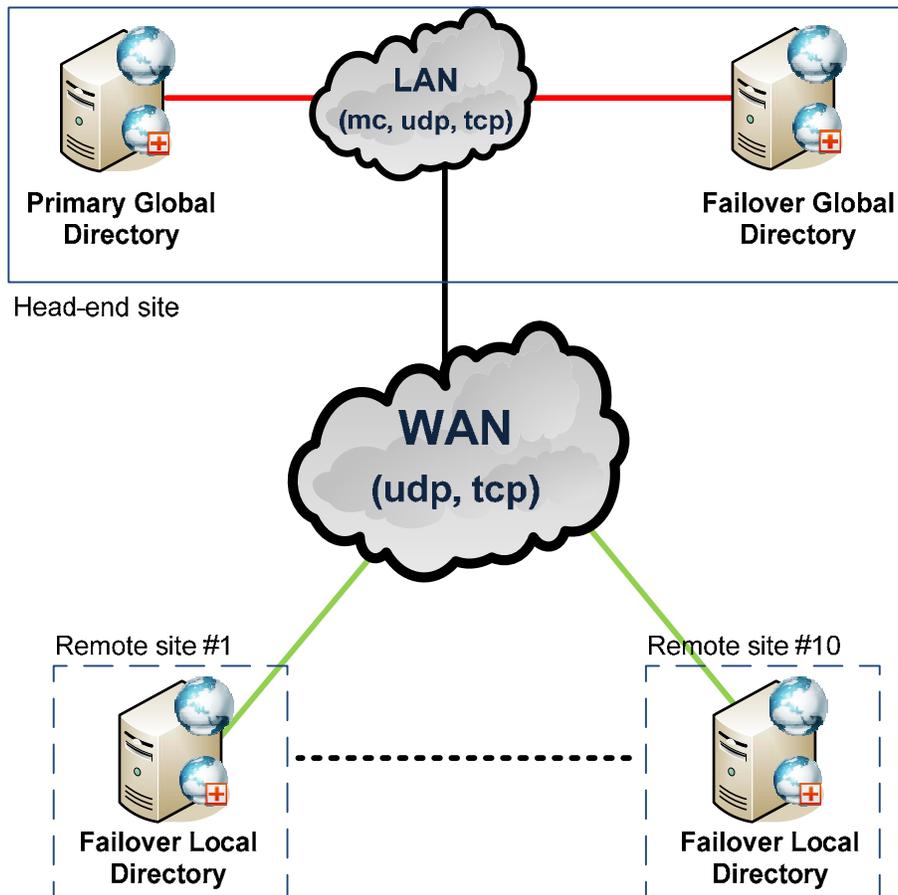
4 items

6. Scenario #2: Local Directories

In this scenario, there are more than 2 servers involved in the FOS. Since only 2 global Directories are recommended, the remaining Directories will have to be configured as local. In most cases, the local Directory server is at a remote location where the network bandwidth to the global Directory servers is limited. The two global Directory servers are at the “head end” location where multicast is supported and network bandwidth is not a problem.

This scenario has the following requirements:

- 1) Two servers acting as global Directories; remaining servers acting as local Directories
- 2) Multicast is only supported on the network with the global Directories
- 3) Good network bandwidth between the global Directories (100 Mbps or more)
- 4) Bandwidth is limited to the local Directory server (minimum 1.5 Mbps or higher to each local Directory)



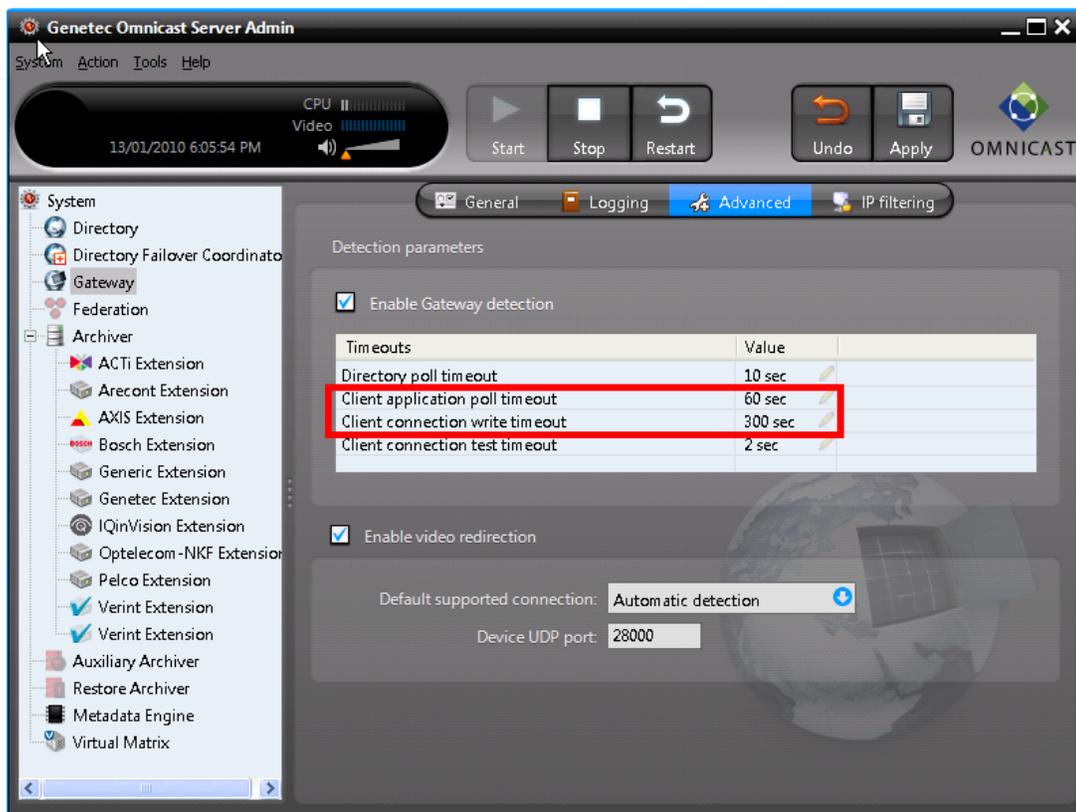
Note that using Federation may be a better option for you if you are considering using Local Directories. Please contact us or one of our Sales Engineers to discuss this option.

6.1. Configuration on the Primary Server

The configuration on the primary server is the same as in the Simple scenario (refer to section 5.1).

Please perform these additional steps:

- 1) Since the bandwidth on the WAN is limited, it may be necessary to increase the **Client connection timeout** to a maximum of 300 sec and the **Client application poll timeout** to 60 sec. If the failover Gateway often loses connection to the primary server, then it is necessary to increase this timeout.



6.2. Configuration on the Failover Global Directory Server

Since the Failover Global Directory server meets the requirements of Scenario #1 (Simple), it should be configured the same way. Please perform the steps described in section 5.2.

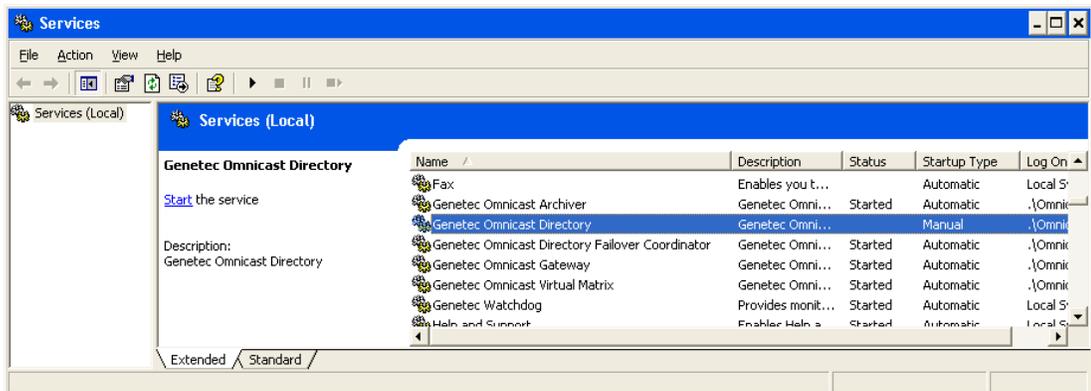
6.3. Configuration on the Failover Local Directory Server

Please perform the following steps on the Failover Local Directory Server:

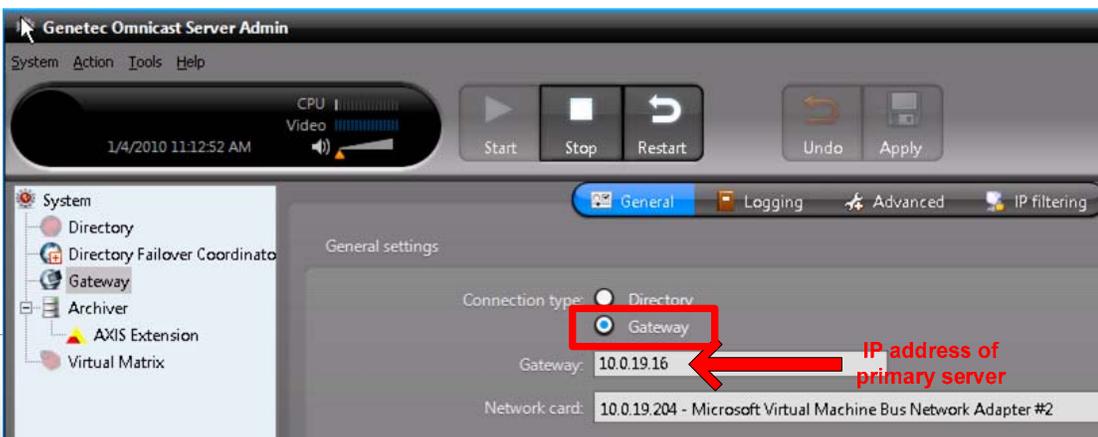
- 1) Verify that the Directory service is stopped and its startup type is set to "Manual". The Directory Failover Coordinator and Gateway services should be started.



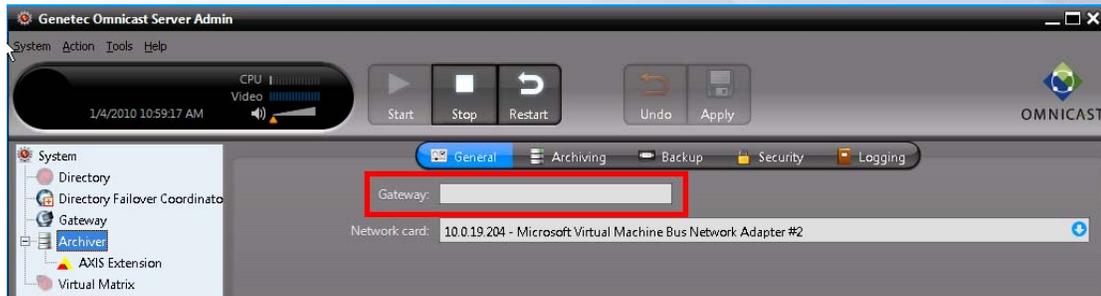
You can access the Windows services by going to Control Panel / Administrative Tools / Services:



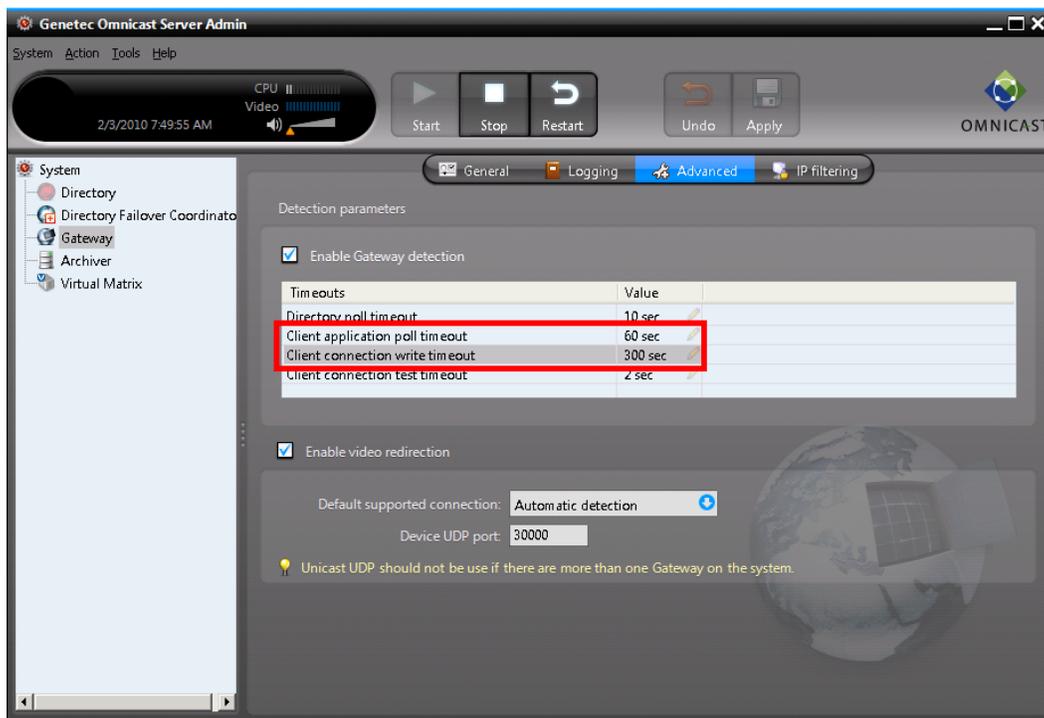
- In a Reverse Gateway configuration, the Gateway must have "Gateway" as the Connection Type. In the Gateway field, put the IP address of the primary server.



- 3) All the other services (like Directory Failover Coordinator, Archiver, Virtual Matrix, etc.) must point to the local Gateway using the local IP address or leaving it blank.



- 4) Since the bandwidth on the WAN is limited, it may be necessary to increase the **Client connection timeout** to a maximum of 300 sec and the **Client application poll timeout** to 60 sec. If the failover Gateway often loses connection to the primary server, then it is necessary to increase this timeout.



- 5) Since there are multiple Gateways in this scenario, it is better to allocate different test addresses and UDP ports to avoid any conflicts. The following settings need to be changed. The values indicated are suggested (they can be different depending on your system):

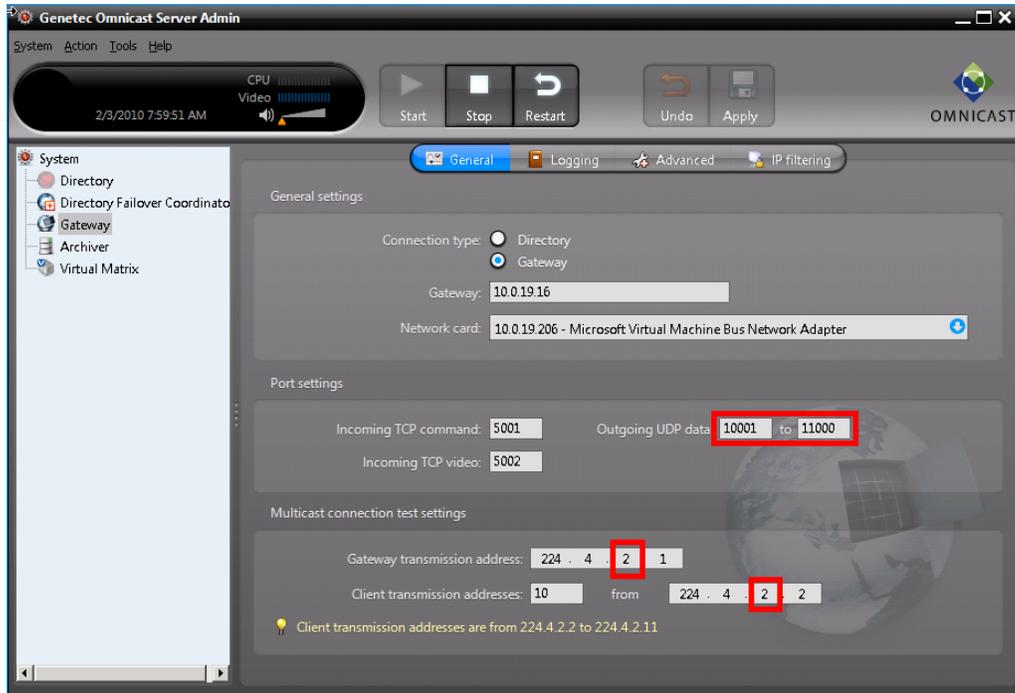
Gateway > General

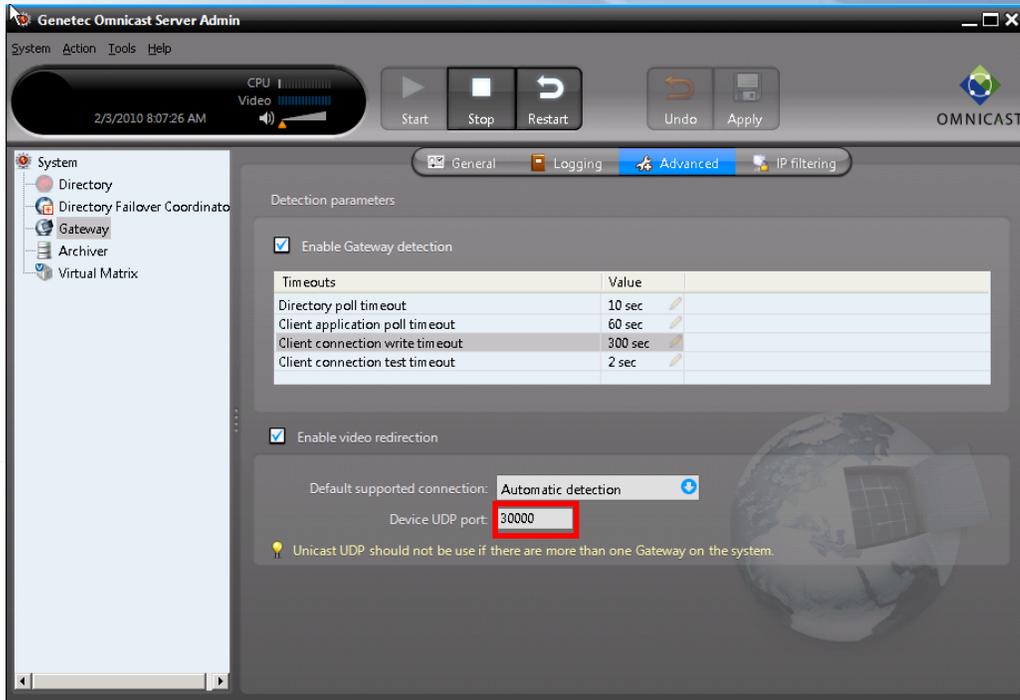
- a. Outgoing UDP data: 10001-11000 (increments of 1000 for each additional Gateway)

- b. Gateway transmission address: 224.4.2.1 (increments of 1 in the 3rd octet for each additional Gateway)
- c. Client transmission addresses from: 224.4.2.2 (increments of 1 in the 3rd octet for each additional Gateway)

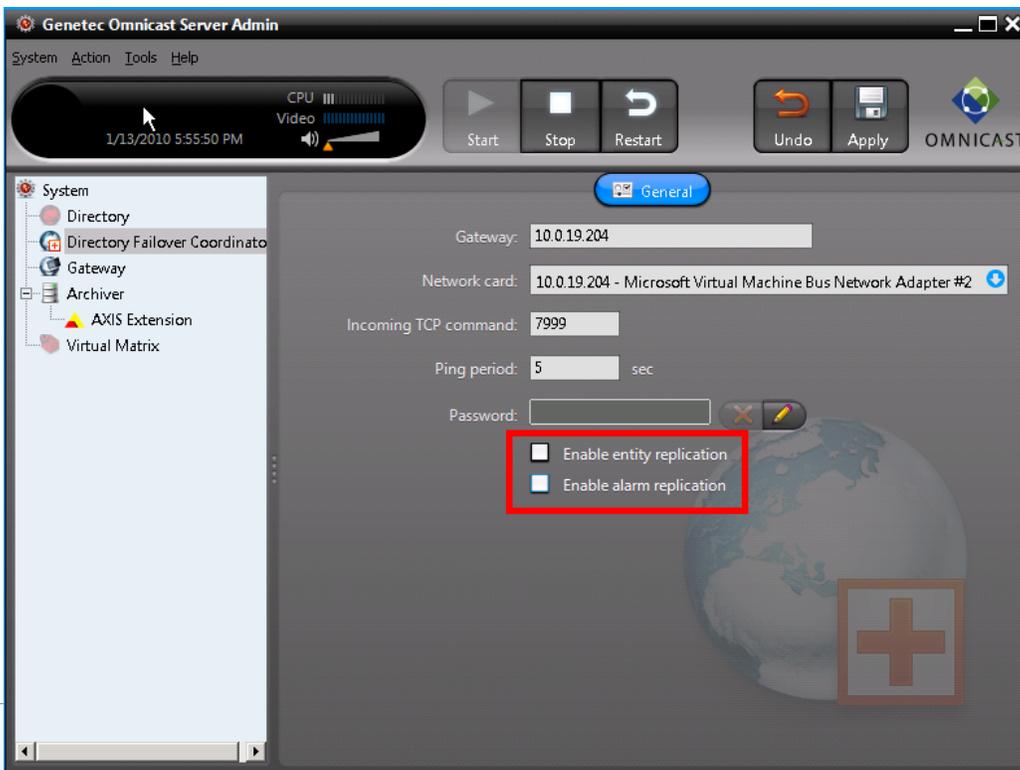
Gateway > Advanced

- d. Device UDP port: 30000 (increments of 1000 for each additional Gateway)





- 6) Since the bandwidth is usually limited and latency is higher on the WAN, it is better to disable the **Entity and Alarm Replication** on the DFC. Whenever there are changes to the configuration, you will need to perform a manual synchronization whenever a configuration is changed.



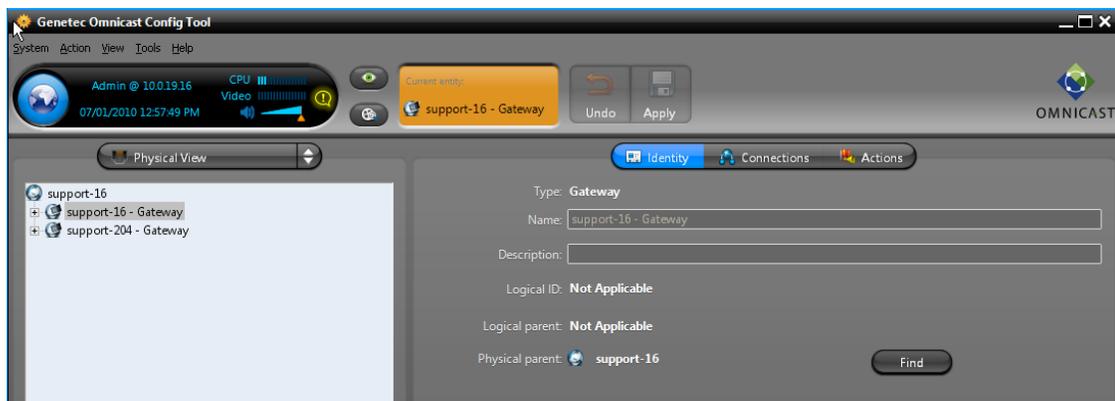
- 7) Go to System > Network and set the **Public address** with its local IP address.



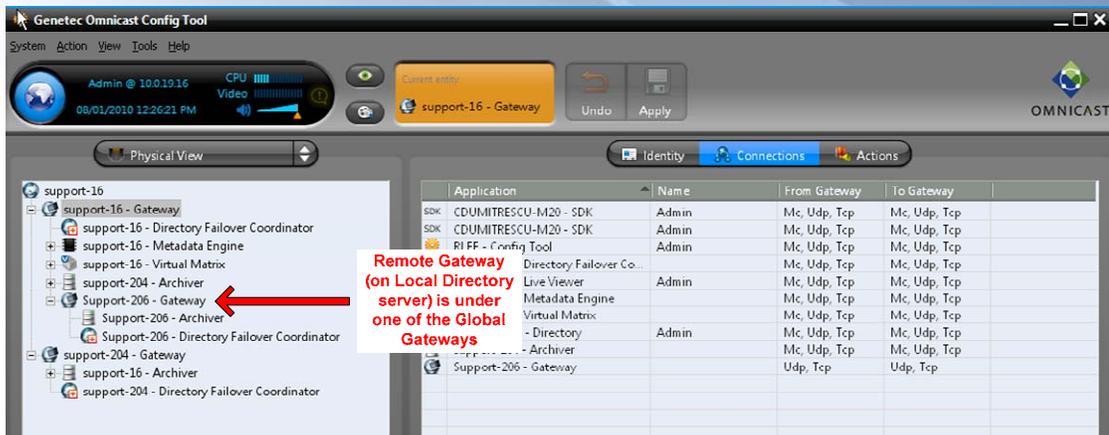
6.4. Verifying the Omnicast services in the Config Tool

Please perform the following to verify that the Omnicast services on both servers have been properly configured and detected by the main Directory:

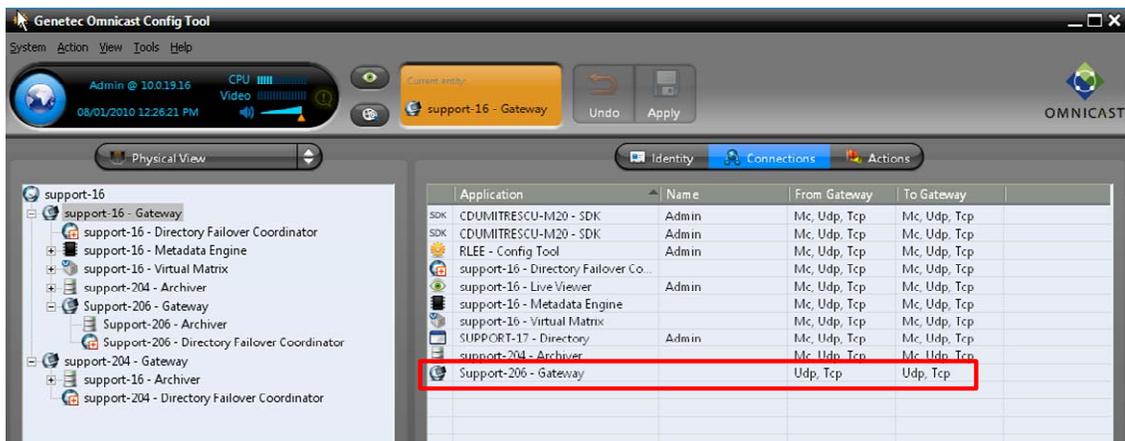
- 1) Open the Config Tool / Physical View.
- 2) Verify that ALL the Directory servers have the following services:
 - a. Directory Failover Coordinator
 - b. Gateway
- 3) Verify that both Global Gateways appear at the same level under the Directory.



- 4) Verify that the remote Gateway is detected under one of the Gateways on the LAN.



- 5) In the Physical View / Gateway / Connections, the remote Gateway should be detected by the primary Gateway as **Udp, Tcp**.



6.5. Running the DFC Wizard

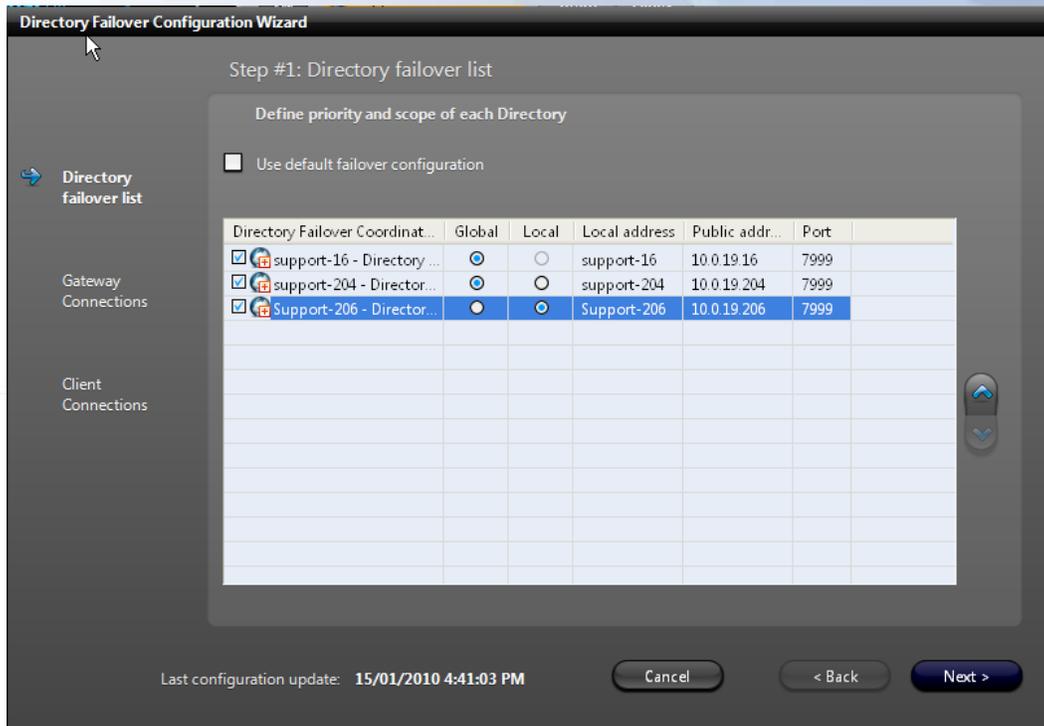
The next step is to run the Directory Failover Configuration (DFC) Wizard to configure the failover list. Please perform the following steps:

- 1) In the Config Tool, go to Tools / **Configure Directory Failover**. The Directory Failover Configuration Wizard will pop open.
- 2) On Step #1, uncheck the box "Use default failover configuration".
- 3) Check both servers that are on the LAN and make them **Global**. Check the remote servers that are on the WAN and make them **Local**.

The order of the list is important:

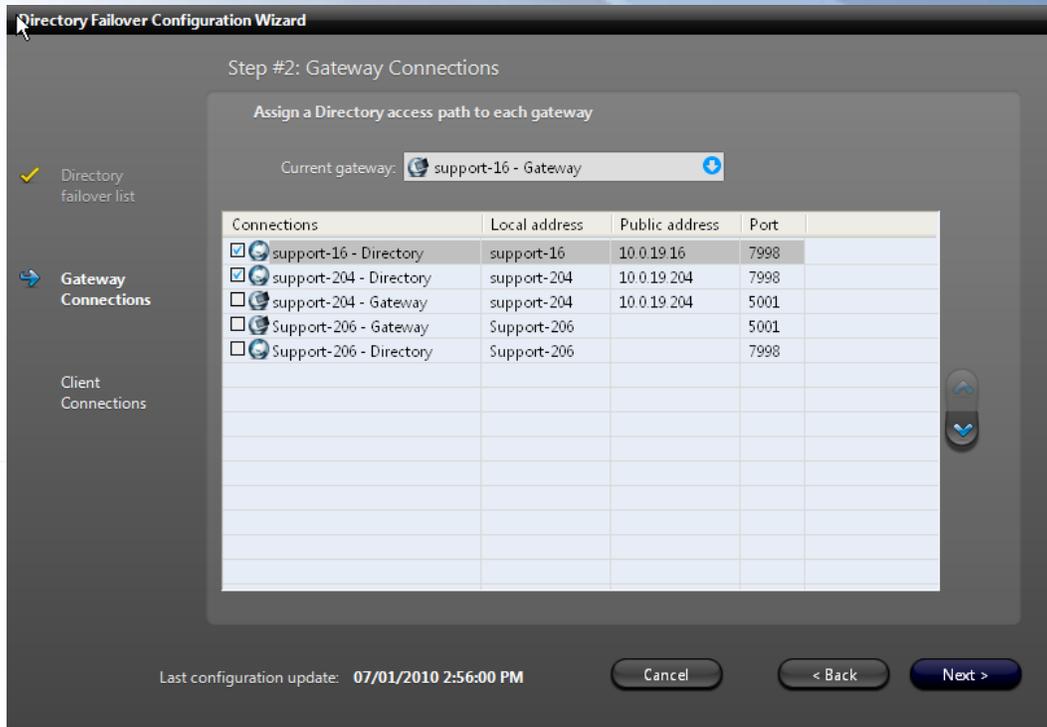
- First server in the list is the primary Global Directory
- Second server in the list is the failover Global Directory

- The remaining servers can be in any order since they are the Local Directories

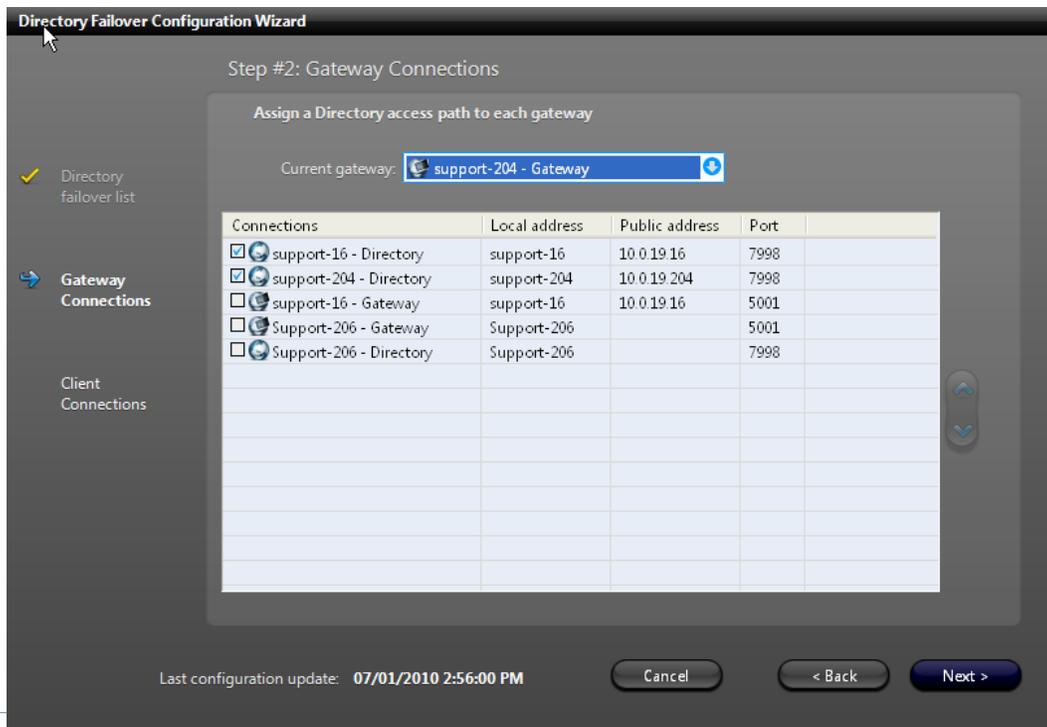


- 4) Click **Next**.
- 5) Step #2 in the DFC Wizard is to configure the Gateway connections. This step will define the order each Gateway will try to connect to the Directory.

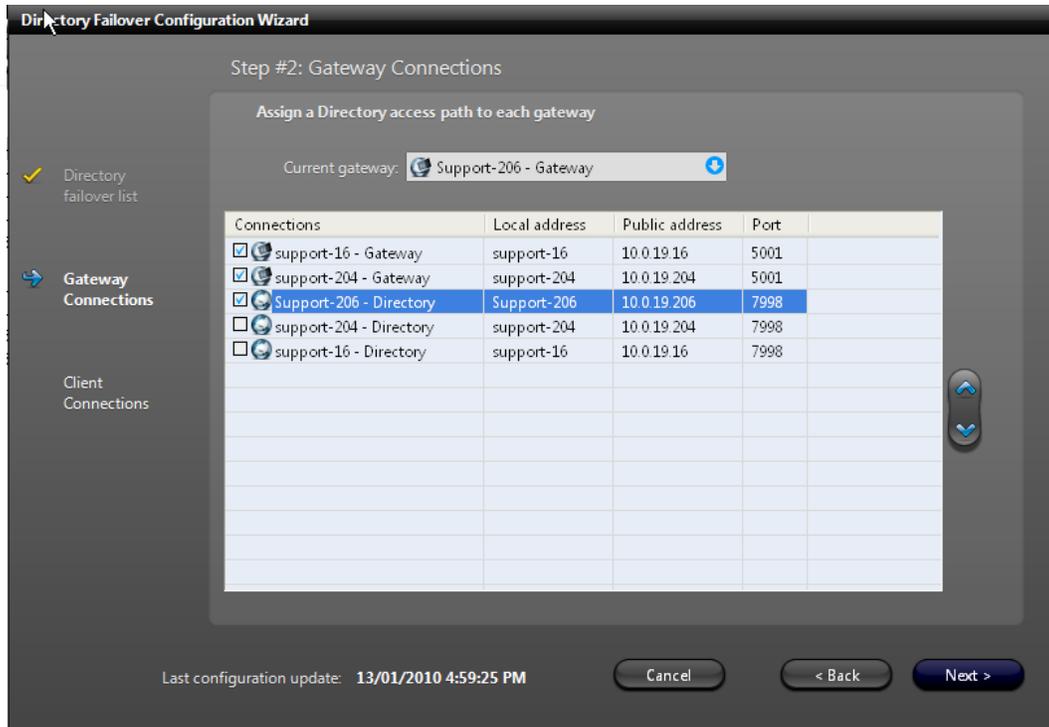
From the drop down list, select the Gateway that is on the primary Global Directory. Using the up and down arrows, change the order of the list to have the primary Global Directory first and the failover Global Directory second. The remote Directories and Gateways should NOT be checked since the Gateways on the LAN should never try to connect to the remote Gateways on the WAN to reach a Directory.



- 6) From the drop down list, select the Gateway that is on the **failover Global Directory server**. The list should be configured the same as the primary Gateway in the previous step.

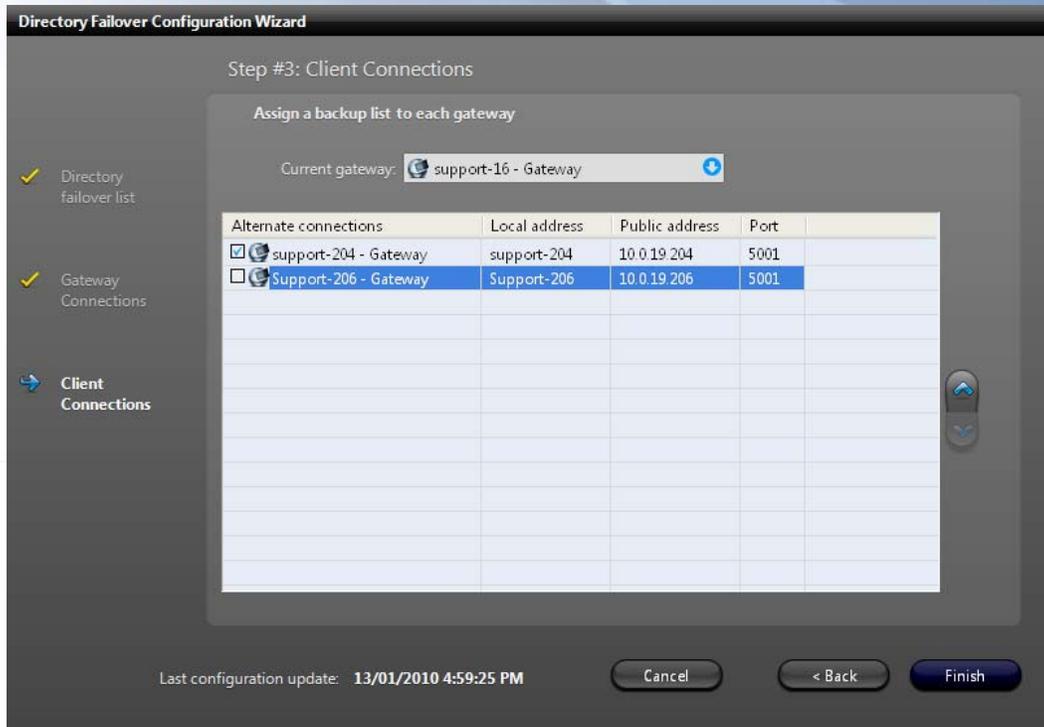


- 7) From the drop down list, select the remote Gateway that is on the **failover Local Directory server**. This Gateway should try to connect to the Global Directories first via their Gateways (i.e. Reverse Gateway) and then try to connect to its local Directory. Therefore, it should be configured as follows:
- First server in the list is the Gateway on the primary server at the head-end
 - Second server in the list is the Gateway on the failover server at the head-end
 - The last server in the list should be its own local Directory

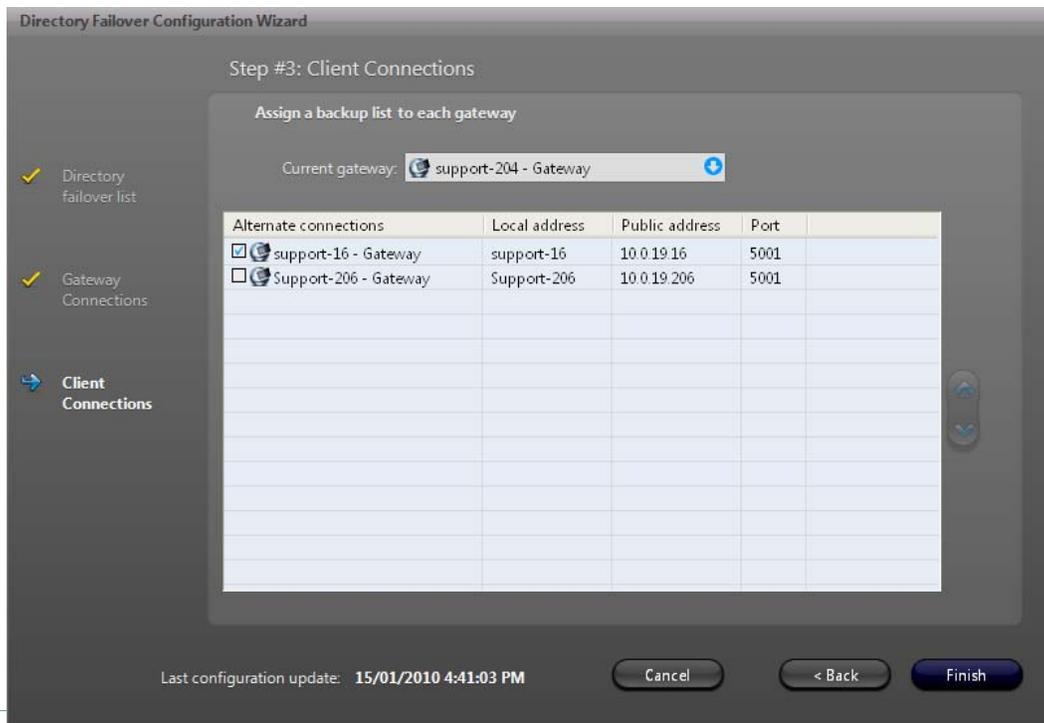


- 8) Step #3 in the DFC Wizard is to configure the client connection list. This section configures the alternative choices for the Gateway to which the client applications should connect.

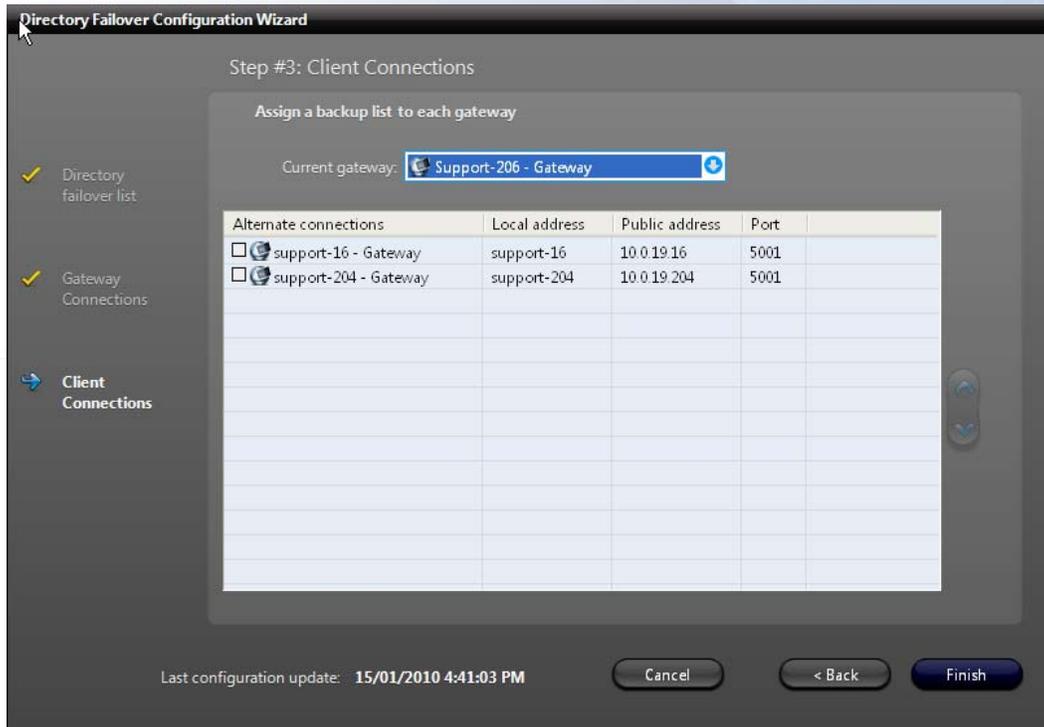
Select the Gateway on the Primary Global Directory server. The only alternative is to connect to the Gateway on the Failover Directory server on the LAN. It should NOT connect to the remote Gateways.



- 9) Select the Gateway on the Failover Global Directory. It should be configured similarly as the Gateway on the Primary Global Directory server.



- 10) Select the remote Gateway. None of the Gateways should be selected. We do not want the client applications at the remote sites to ever connect to the Gateway at the head-end.



- 11) Click **Finish**. After clicking this button, the DFC services will restart and the synchronization process will begin. Please refer to the next section for a description of the synchronization process.

7. Failover synchronization process

If the Directory Failover has been configured properly, synchronization of the Directory databases should occur. Depending on the size of your system, this can take up to 15 minutes (even more for very large systems). The Replication Status can be checked by clicking the failover Directory Failover Coordinator in the Config Tool:

The screenshot shows the Genetec Omnicast Config Tool interface. The top bar includes the title 'Genetec Omnicast Config Tool' and a menu with 'System', 'Action', 'View', 'Tools', and 'Help'. Below the menu, there are system status indicators for 'Admin @ 100.19.16' and '15/01/2010 4:41:09 PM', along with CPU and Video usage bars. A 'Current entity' dropdown is set to 'support-204 - Direct...'. The main interface is divided into a left sidebar with a tree view of entities and a main content area. The tree view shows a hierarchy starting with 'support-16', including 'Gateway', 'Archiver', 'Metadata Engine', 'Virtual Matrix', and 'Directory Failover Coordinator'. The main content area has tabs for 'Identity' and 'Statistics'. The 'Identity' tab is active, displaying a 'Directory failover list' table and a 'Status' section.

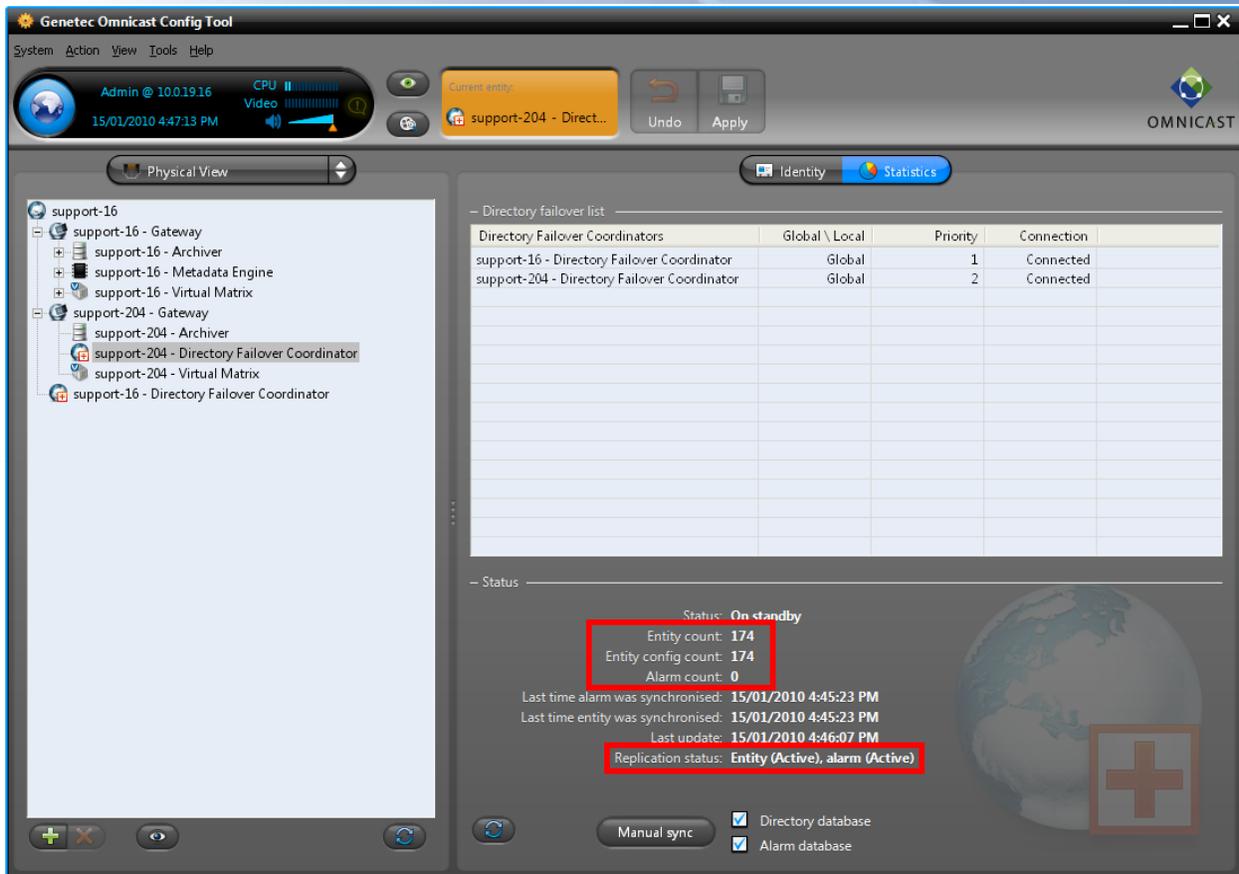
Directory Failover Coordinators	Global \ Local	Priority	Connection
support-16 - Directory Failover Coordinator	Global	1	Connected
support-204 - Directory Failover Coordinator	Global	2	Connected

The 'Status' section shows the following information:

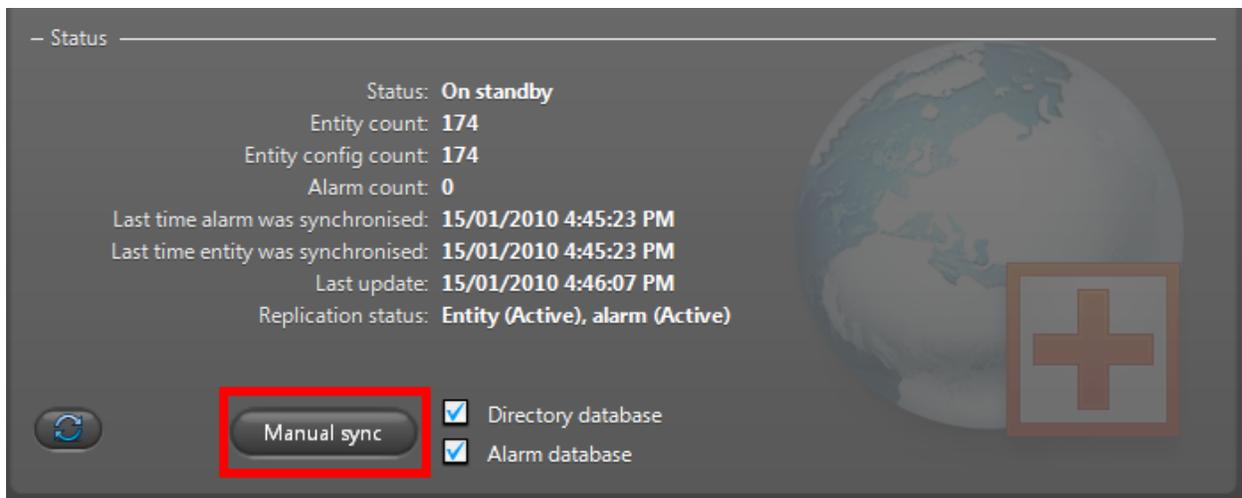
- Status: **On standby**
- Entity count: 0
- Entity config count: 0
- Alarm count: 0
- Last time alarm was synchronised: 15/01/2010 4:40:38 PM
- Last time entity was synchronised: 15/01/2010 4:40:38 PM
- Last update: 15/01/2010 4:41:06 PM
- Replication status: Entity **Synchronizing (63%)** alarm (Active)

At the bottom, there is a 'Manual sync' button and two checked checkboxes: 'Directory database' and 'Alarm database'. A globe icon and a red cross icon are also visible in the status area.

Once the synchronization has completed successfully, the Status will change to **On Standby** and the Replication Status will change to **Active** and the different counts should have a value.



For remote Directories where the entity replication has been disabled, you can perform a manual synchronization when needed by clicking on the **Manual Sync** button on the remote Directory Failover Coordinator.

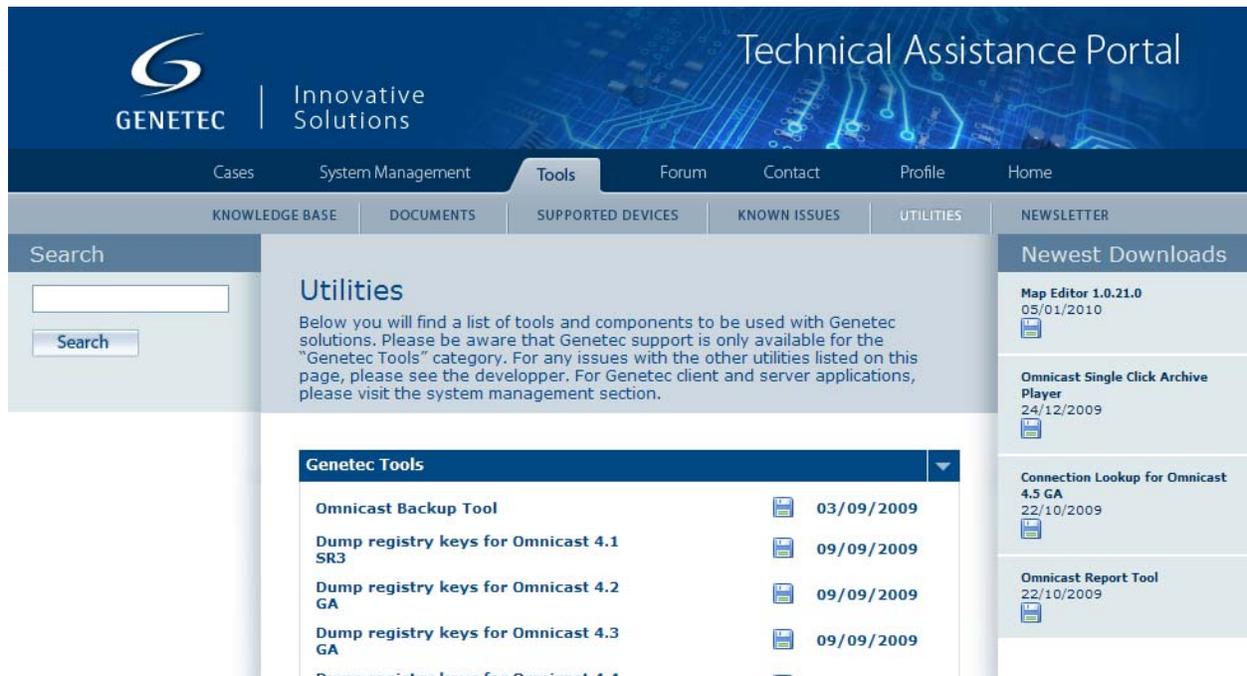


8. Troubleshooting Directory Failover Issues

The following are some of the common issues that we encounter with Directory Failover and some troubleshooting steps you can perform.

ALWAYS BACKUP THE DIRECTORY DATABASE AND REGISTRY ON ALL SERVERS BEFORE MAKING CHANGES DURING THE TROUBLESHOOTING.

You can use the Omnicast Backup Tool to perform the backup. You can download the Backup Tool at our GTAP (<http://gtap.genetec.com/>):



The screenshot shows the Genetec Technical Assistance Portal. The header includes the Genetec logo and 'Innovative Solutions'. The main navigation bar has tabs for Cases, System Management, Tools, Forum, Contact, Profile, and Home. Below this is a secondary navigation bar with links for KNOWLEDGE BASE, DOCUMENTS, SUPPORTED DEVICES, KNOWN ISSUES, UTILITIES, and NEWSLETTER. The 'Utilities' section is active, displaying a search box and a list of tools. The 'Genetec Tools' list includes:

Tool Name	Date
Omicast Backup Tool	03/09/2009
Dump registry keys for Omnicast 4.1 SR3	09/09/2009
Dump registry keys for Omnicast 4.2 GA	09/09/2009
Dump registry keys for Omnicast 4.3 GA	09/09/2009
Dump registry keys for Omnicast 4.4	

On the right side, there is a 'Newest Downloads' section with items like 'Map Editor 1.0.21.0', 'Omicast Single Click Archive Player', 'Connection Lookup for Omnicast 4.5 GA', and 'Omicast Report Tool'.

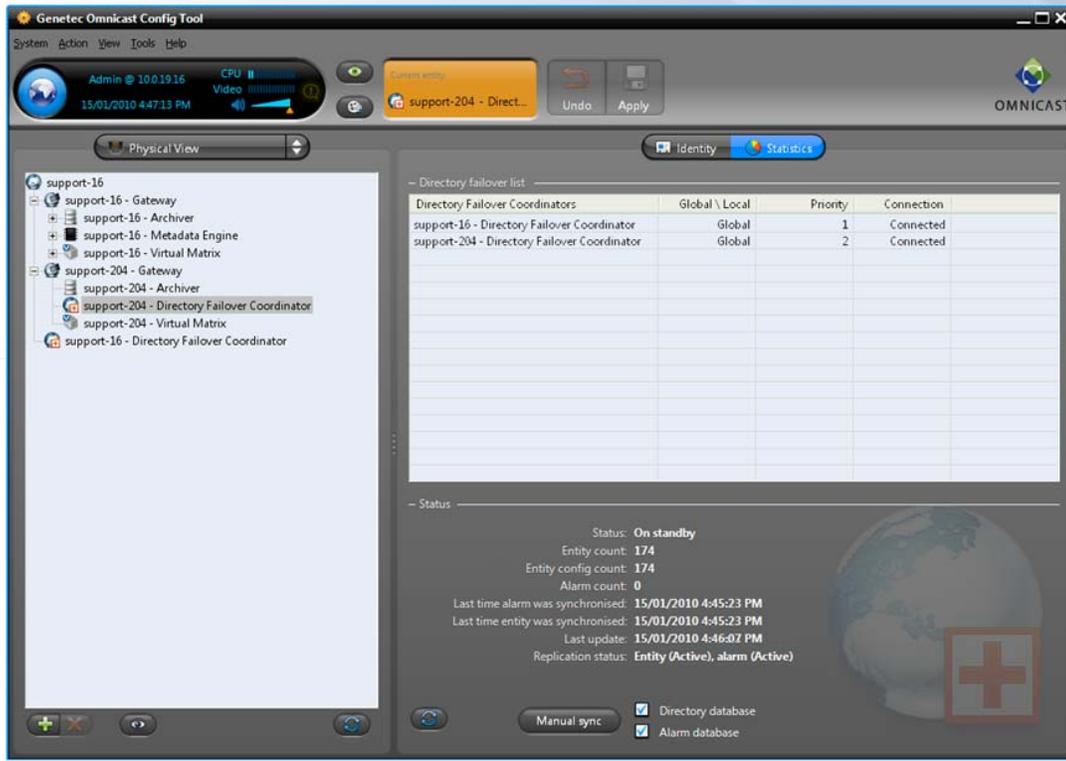
8.1. Clients do not connect to failover Directory

A failover condition has started so the client applications have disconnected. They do not reconnect to the failover Directory as it is expected. Please do the following to troubleshoot the problem:

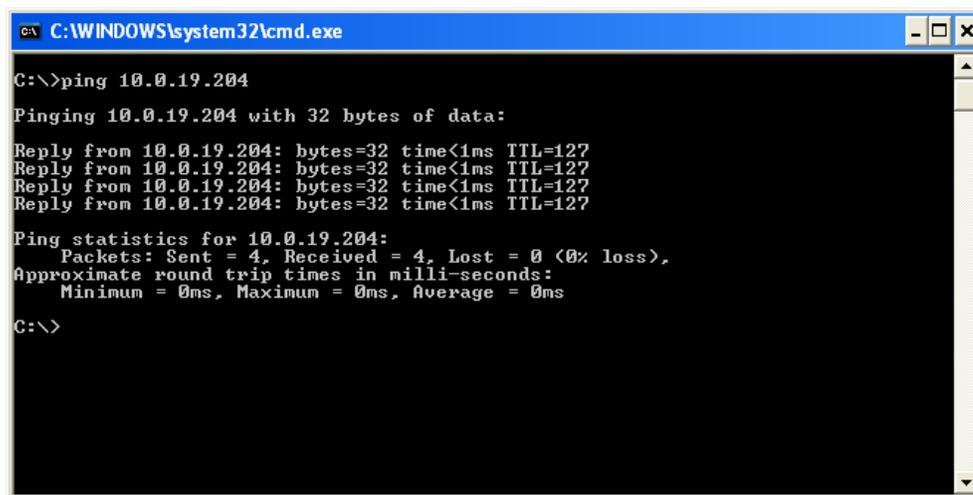
- 1) Verify that after the Directory on the failover server has started, usually in about 2 minutes after the failover condition started.

Name	Description	Status	Startup Type	Log On As
Genetec Omnicast Archiver	This service is r...	Started	Automatic	.\OmicastSvcUsr
Genetec Omnicast Directory	This service is t...	Started	Manual	.\OmicastSvcUsr
Genetec Omnicast Directory Failover ...	Service installe...	Started	Automatic	.\OmicastSvcUsr
Genetec Omnicast Gateway	Service allowin...	Started	Automatic	.\OmicastSvcUsr
Genetec Omnicast Virtual Matrix	This service pr...	Started	Automatic	.\OmicastSvcUsr
Genetec Watchdog	Provides monit...	Started	Automatic	.\OmicastSvcUsr

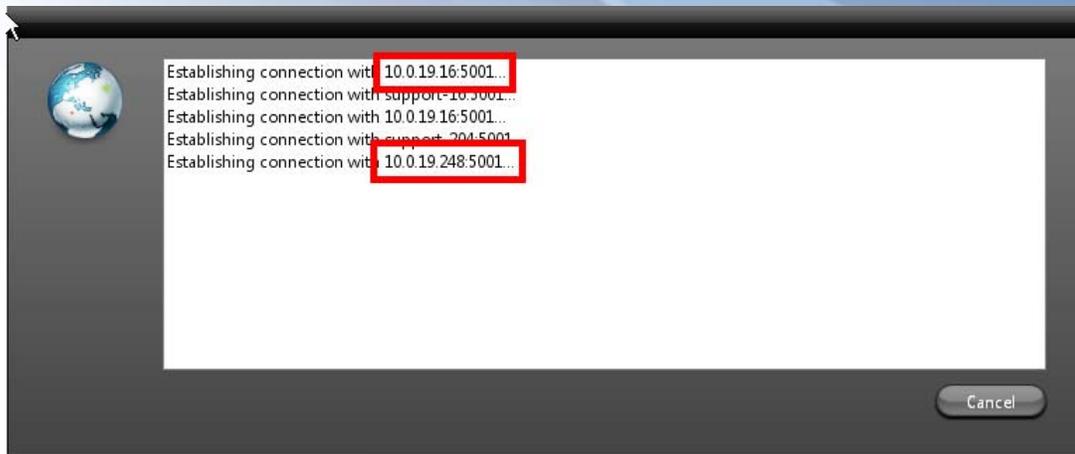
- Verify that the synchronization process has completed successfully on the DFC of the Failover Directory server.



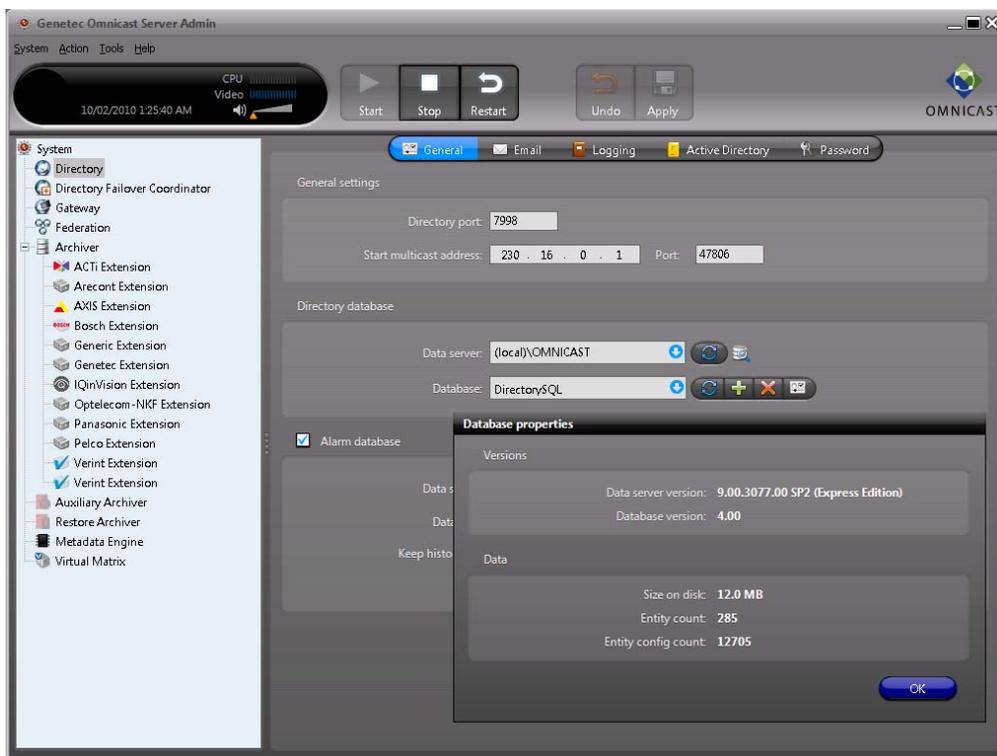
- Verify that the client workstation has connectivity to the failover server (i.e. can ping the failover server).



- As the client application is trying to establish connection, verify that you see it try to connect to the failover server.



- 5) Install the client application (ex: Config Tool) on the failover server and see if it can connect to the failover Directory.
- 6) Verify that the database on the failover Directory is valid. This can be done by checking the database properties in the Server Admin > Directory > Database > Properties.



- 7) Verify that the windows firewall is stopped and disabled in services.msc.

Windows Event Log	This service man...	Started	Automatic	Local Service
Windows Firewall	Windows Firewal...		Disabled	Local Service
Windows Font Cache Service	Optimizes perfor...		Manual	Local Service
Windows Installer	Adds, modifies, ...		Manual	Local System
Windows Management Instrumen	Provides a comm...	Started	Automatic	Local System

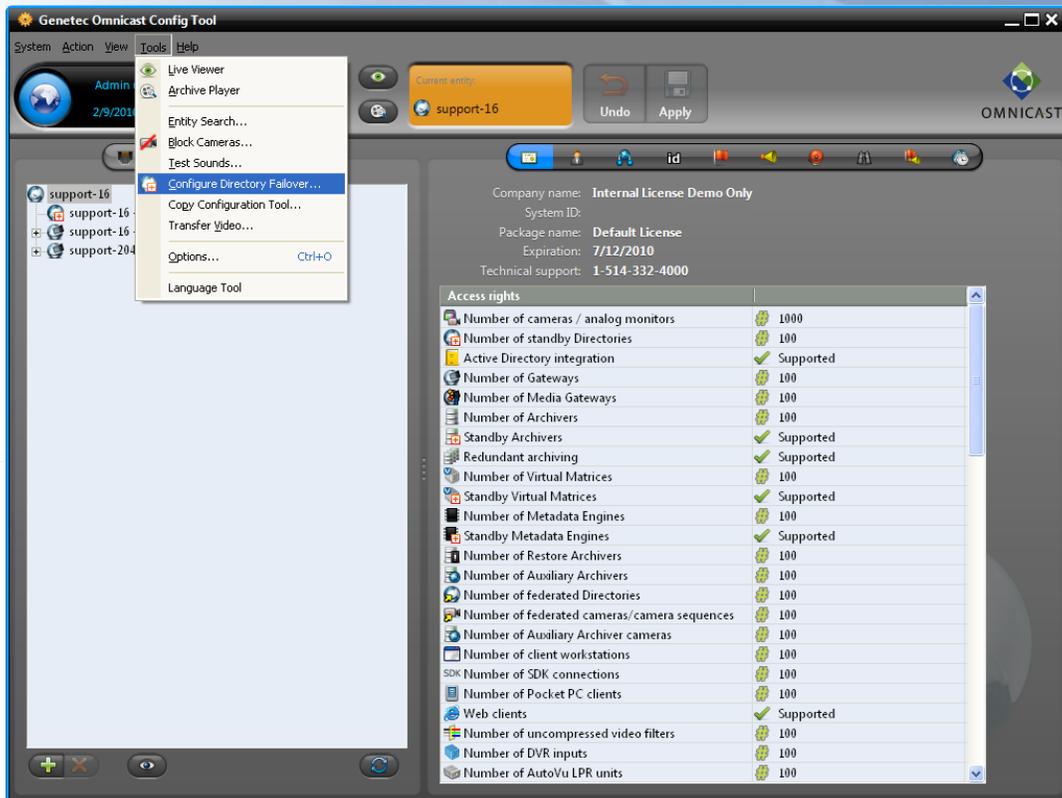
8.2. Directory on failover server is always started

You notice that the Directory service on the failover server is always started:

Name ^	Description	Status	Startup Type	Log On As
Genetec Omnicast Archiver	This service is r...	Started	Automatic	.\OmnicastSvcUsr
Genetec Omnicast Directory	This service is t...	Started	Manual	.\OmnicastSvcUsr
Genetec Omnicast Directory Failover ...	Service installe...	Started	Automatic	.\OmnicastSvcUsr
Genetec Omnicast Gateway	Service allowin...	Started	Automatic	.\OmnicastSvcUsr
Genetec Omnicast Virtual Matrix	This service pr...	Started	Automatic	.\OmnicastSvcUsr
Genetec Watchdog	Provides monit...	Started	Automatic	.\OmnicastSvcUsr

This is not normal because the failover Directory service should only be started when there is a failover condition. Please do the following to troubleshoot the problem:

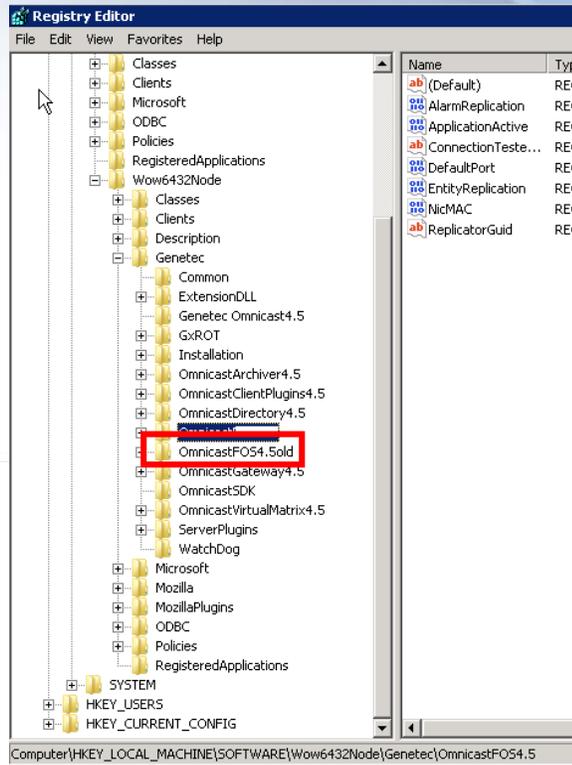
- 1) Verify that the DFC service has been set to Manual in services.msc.
- 2) Run the DFC Wizard again.



- 3) It is possible the DFC is detecting a problem on the primary server. Stop and disable the Directory on the failover server and ensure the clients can login to the primary Directory. If you cannot login to the primary Directory, you will need to resolve this problem first.

Genetec Omnicast Archiver	This service is re...	Started	Automatic	.\OmnicastSvcUsr
Genetec Omnicast Directory	This service is th...	Disabled	Disabled	.\OmnicastSvcUsr
Genetec Omnicast Directory Failover Coordinator	Service installed ...	Started	Automatic	.\OmnicastSvcUsr
Genetec Omnicast Gateway	Service allowing ...	Started	Automatic	.\OmnicastSvcUsr
Genetec Omnicast Virtual Matrix	This service prov...	Started	Automatic	.\OmnicastSvcUsr
Genetec Watchdog	Provides monitor...	Started	Automatic	.\OmnicastSvcUsr

- 4) It is possible that the failover server thinks it is the primary. To completely clear the FOS configuration on the failover, do the following:
- Make a backup of both the primary and failover servers using the Omnicast backup tool.
 - On the failover server, stop the DFC service.
 - Open regedit.
 - Export HKEY_LOCAL_MACHINE\SOFTWARE\Genetec to make a backup.
 - Rename HKEY_LOCAL_MACHINE\SOFTWARE\Genetec\OmnicastFOS4.x to OmnicastFOS4.xold. Ex: OmnicastFOS4.5old.

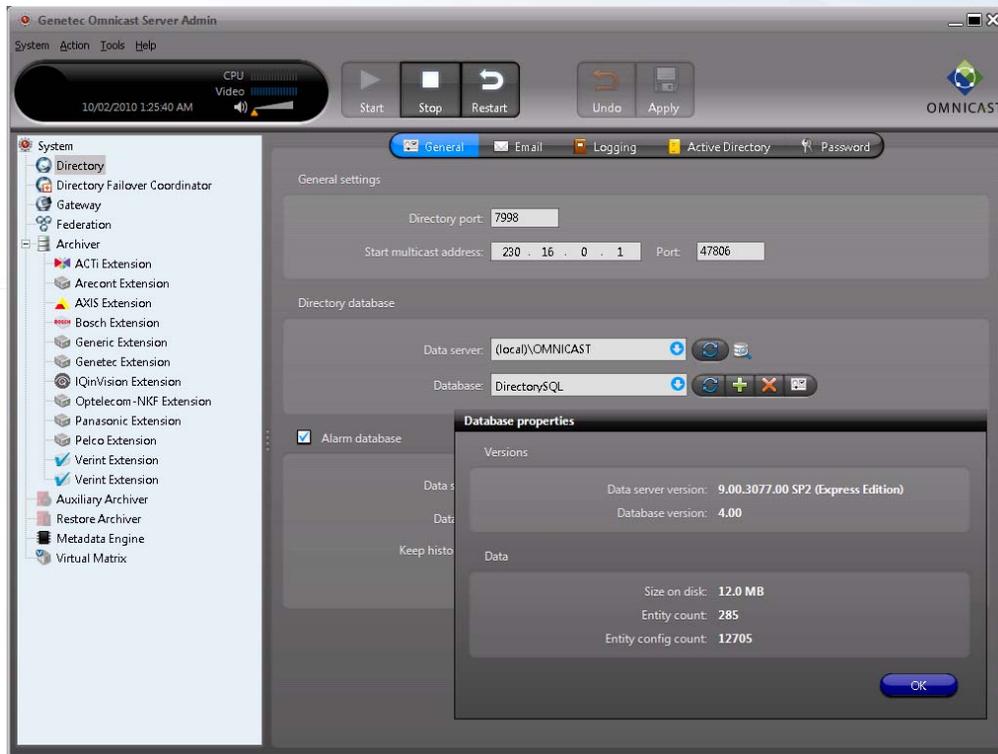


- f. Start the DFC service.
- g. Open the Watchdog Tray. You should now see 2 DFC services, one in red (stopped) and another in green (running). Right-click on the one in red and select “Remove application” to delete it.



- h. Reconfigure the failover server as described in this document and run the DFC Wizard again.

- 5) Verify that the database on the primary Directory is valid. This can be done by checking the database properties in the Server Admin > Directory > Database > Properties. If it appears that the database on the primary Directory is corrupted, you can restore a backup from the failover Directory.



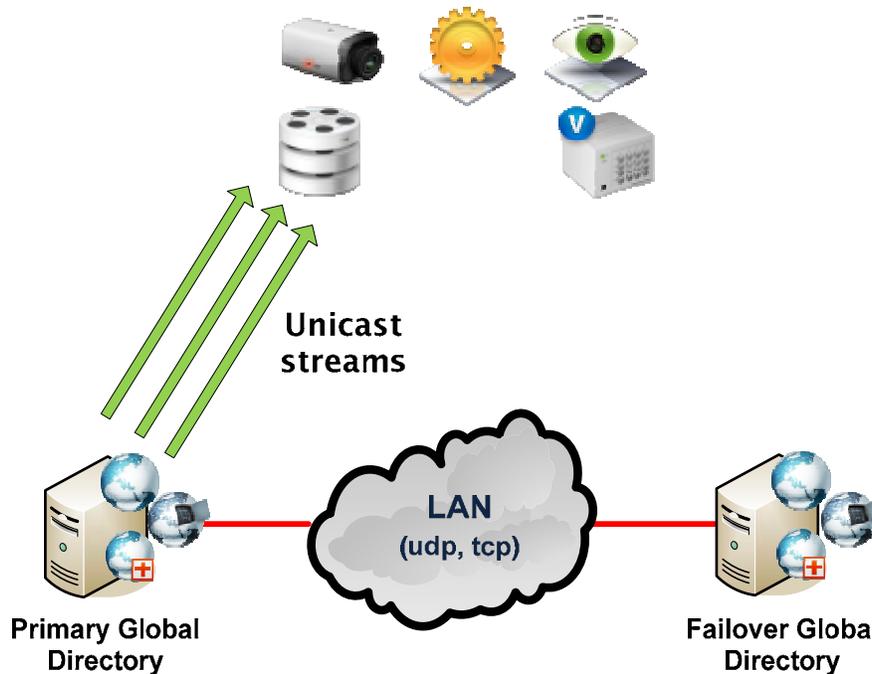
8.3. Status shows “Software Broken”

In the Statistics of the DFC on the Failover Directory server, the Status indicates “Software Broken”. This error means that the primary DFC cannot connect to the failover DFC. Verify that failover server is reachable and there is sufficient bandwidth between the servers. Ensure that port 7999 is open.

9. Appendix A: Scenario #3: Global Directories With No Multicast

This scenario is not common but worth mentioning. This scenario has the following requirements:

- 1) Only two servers are involved in the Directory FOS: Primary server and failover server
- 2) Multicast is NOT supported on the network
- 3) Both servers are on a LAN with good network bandwidth (100 Mbps or higher)



Please note that this configuration should NOT be used on large systems where there is a high amount of live viewing. If you are unsure, please contact us or one of our Sales Engineers to discuss this option.

9.1. Configuration on the Primary Server

The configuration on the primary server is the same as in the Simple scenario (refer to section 5.1).

9.2. Configuration on the Failover Local Directory Server

The configuration on the primary server is the same as in the Simple scenario (refer to section 5.2).

9.3. Verifying the Omnicast services in the Config Tool

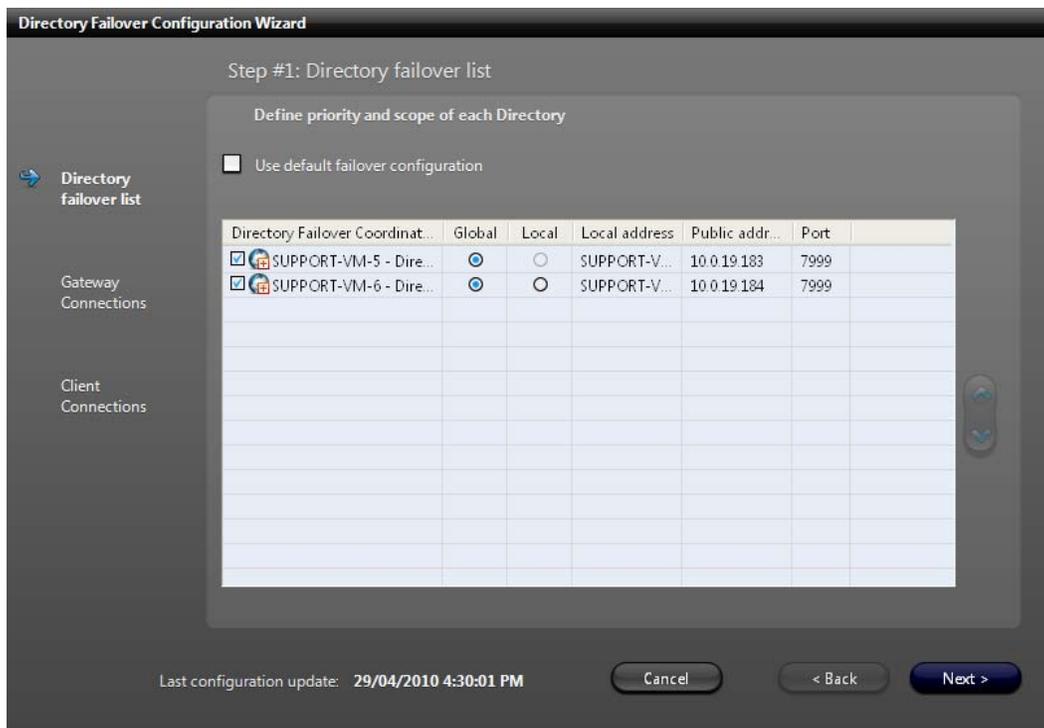
Please follow the procedure described in section 5.3. However, only the services on the same server as the Gateway will be detected in **Mc, Udp, Tcp** since multicast should be detected locally on the

server. Services on another server will be detected in **Udp, Tcp** since multicast is not available on the network.

9.4. Running the DFC Wizard

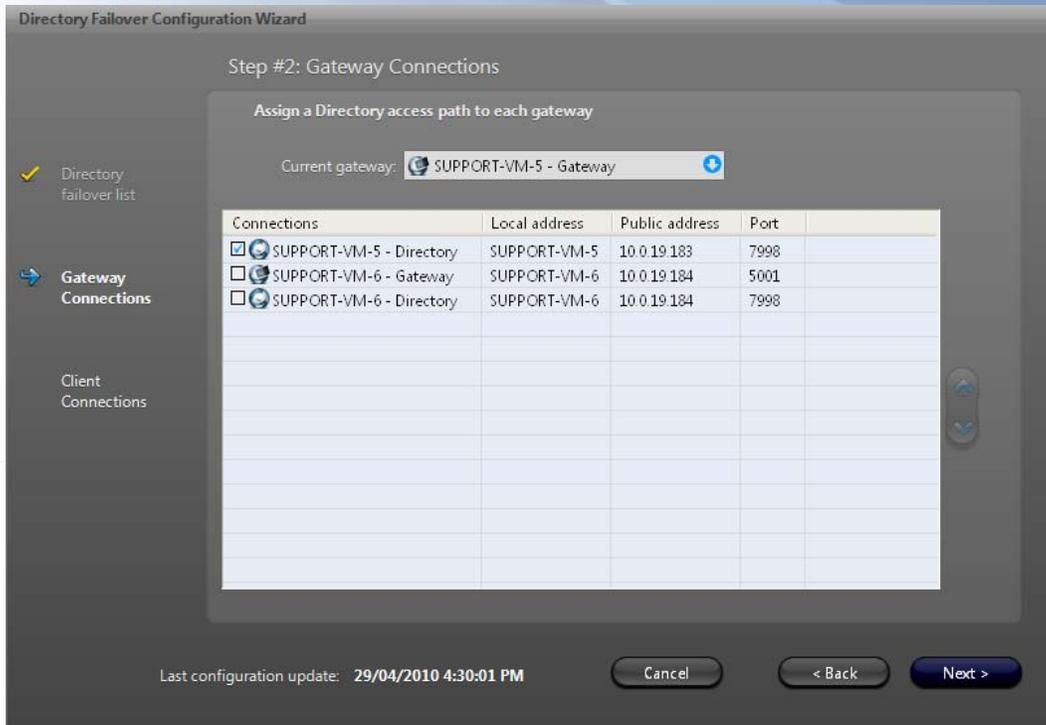
The next step is to run the Directory Failover Configuration (DFC) Wizard to configure the failover list. Please perform the following steps:

- 1) In the Config Tool, go to Tools / **Configure Directory Failover**. The Directory Failover Configuration Wizard will pop open.
- 2) **Uncheck** the box “Use default failover configuration”.
- 3) Check both servers and make them **Global**. The order of the list is important: the first server in the list is the primary; the second server in the list is the failover or backup.

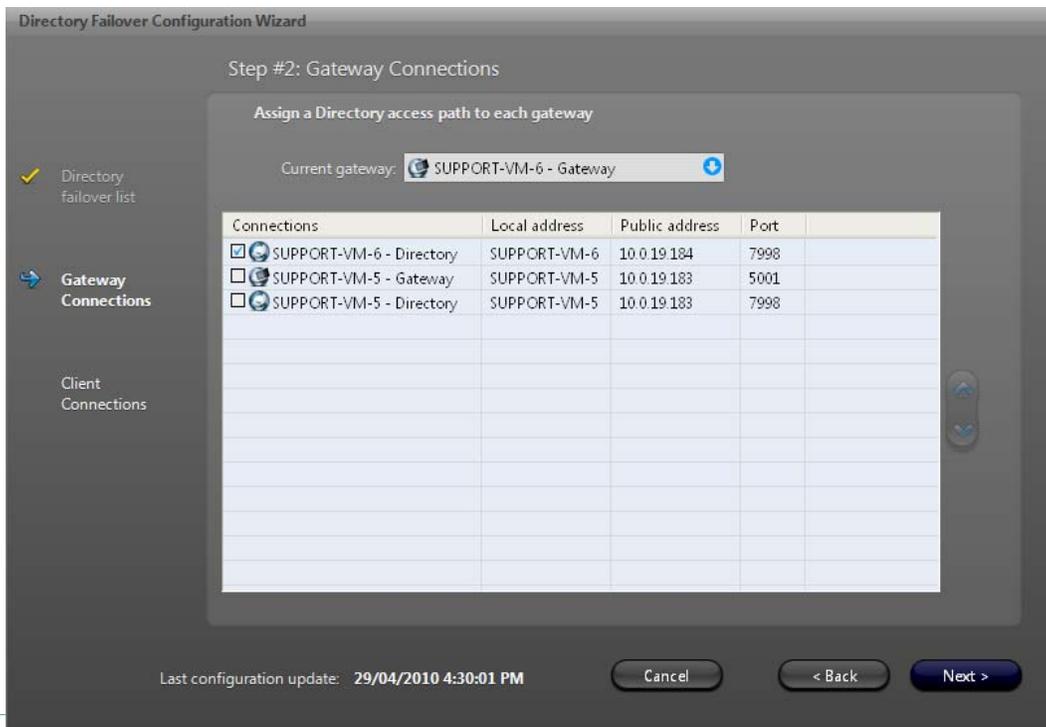


- 4) Click **Next**.
- 5) Step #2 in the DFC Wizard is to configure the Gateway connections. This step will define the order each Gateway will try to connect to the Directory.

From the drop down list, select the **primary Gateway**. Check only its own Directory as follows:

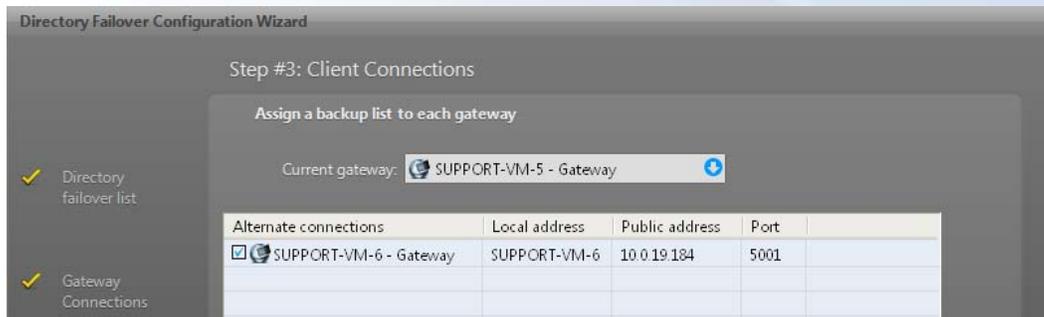


- 6) From the drop down list, select the Gateway on the failover server. Check only its own Directory as follows:



- 7) Click **Next**.

- 8) Step #3 in the DFC Wizard is to configure the client connection list. Since there are only two Gateways, the alternate connection is always the other Gateway. Just ensure the connection list is similar to the following:

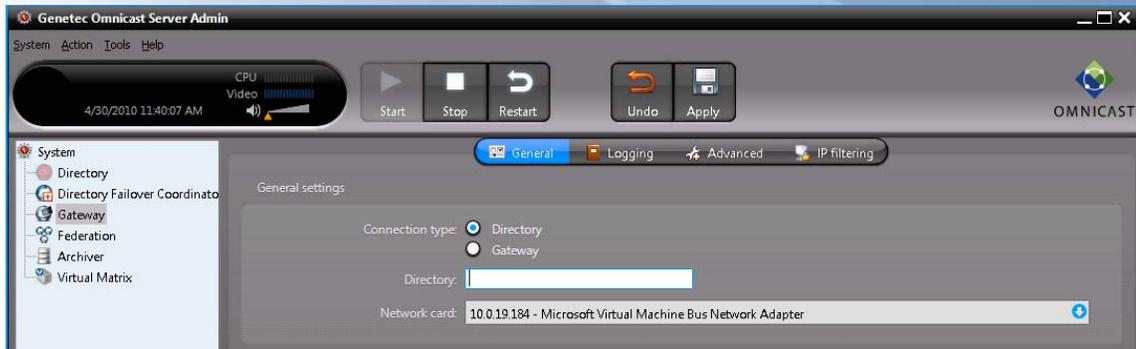


- 9) Click **Finish**. After clicking this button, the DFC services will restart and the synchronization process will begin.

9.5. Modifying the Gateway on Failover Server

To avoid redirections passing through both Gateways, the Gateway on the failover server needs to be modified so that it only connects to its local Directory. As such, only one Gateway will be online at any one time. The Gateway on the primary server will be online and the Gateway on the failover server will be in red (or offline) most of the time. Only when the failover Directory is started then the Gateway on the failover server will be online.

- 1) On the failover server, open the Server Admin.
- 2) On the Gateway > General, change the Connection Type to "Directory". In the Directory field, leave it blank or put the local IP address:



- 3) Once the Gateway is restarted, in the Config Tool, the Gateway on the failover server will be in red which is normal. The Gateway will only be online when in failover mode (i.e. when the failover Directory has started).

