

SeaChange Multicast Forward

Installation and User Guide



Seachange International (China) Inc.
Revision 1.0

Revision History

Revision	Author	Date	Description of Changes
0.1	Ashley Dong	8/27/2004	Initial Draft
0.2	Ashley Dong	9/20/2004	Supply product features and Update configuration, installation and so on
0.3	Ashley Dong	9/22/2004	Supply troubleshooting and example for reference
0.4	Ashley Dong	10/12/2004	Supply SE for reference
0.5	Ashley Dong	10/13/2004	Modification and add this table
1.0	Ashley Dong	11/19/2004	Configuration file modified

Notice

While SeaChange believes the information included in this publication is correct as of the publication date, information in this document is subject to change without notice.

UNLESS EXPRESSLY SET FORTH IN A WRITTEN AGREEMENT SIGNED BY AN AUTHORIZED REPRESENTATIVE OF SEACHANGE INTERNATIONAL INC., SEACHANGE MAKES NO WARRANTY OR REPRESENTATION OF ANY KIND WITH RESPECT TO THE INFORMATION CONTAINED HEREIN, INCLUDING WARRANTY OF MERCHANTABILITY AND FITNESS FOR A PURPOSE. SeaChange International Inc. assumes no responsibility or obligation of any kind for any errors contained herein or in connection with the furnishing, performance, or use of this document.

Software described in this document (a) is the property of Marquis Broadcast Ltd., (b) is furnished only under license, and (c) may be copied or used only as expressly permitted under the terms of the license.

©2003 SeaChange International Inc. All rights reserved.

Portions ©2003 Marquis Broadcast Ltd. All rights reserved.

SeaChange, MediaCluster, and GuestServe are registered trademarks of SeaChange International Inc.; SeaChange International, RAID2, GuestServe Networks, and MeTIL are trademarks of SeaChange International Inc.

Microsoft, MS, MS-DOS, Windows, Windows NT, and SQL Server are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe, the Adobe logo, Acrobat, and the Acrobat logo are trademarks of Adobe Systems Incorporated.

All other trademarks and registered trademarks are the property of their respective holders.

Manual Title: ***SeaChange Multicast Forward Installation and User Guide***
Revision: 01

Creation Date: August 27, 2004

Published by SeaChange International Inc.

Suite 502, Building 2 WITHUB Science Park
641 Tianshan Rd Chang Ning District, Shanghai, China

Contents

About This Manual.....	6
Product Overview.....	6
Introduction.....	6
Product Features.....	6
SeaChange Style Windows Service	7
Powerful Network Support.....	7
Multi-rail support for the tunnel connections without loop and duplicate.....	8
Deny List Support.....	8
SeaChange ManUtil/SNMP support.....	8
Site Requirements.....	9
McastFwd Server Requirements	9
Network Requirements	9
SeaChange ITV SDK Requirements.....	10
Installation.....	11
Before You Begin	11
Step 1. Install Released SeaChange Multicast Forward Services.....	13
Step 2. Verify SeaChange Multicast Forward Services	16
Uninstall SeaChange Multicast Forward Services.....	19
Upgrade SeaChange Multicast Forward Services.....	20
Configuration.....	22
“Step 1. Configure the <TunnelListener>”	22
“Step 2. Configure the <MulticastListener>”	22
“Step 3. Configure the <MulticastSender>”	22
“Step 4. Configure the <DenyList>”	23
“Step 5. Configure the <Tunnels> connection”	23
“Step 6. Configure the <Conversation>”	23
Configuration program	23
Operations	27
How to Start/Stop McastFwd service	27
How to Establish Tunnel Connections	28
How to Deny Multicast Forwarding against a specific source IP and Port.....	29
How to Use manUil to Monitor McastFwd runtime status.....	30
1. Tunnel status	31
2. Conversations status	32
3. DenyList status.....	32
4. Resenders status	32
How to verify Forwarding Multicast messages	33
Troubleshooting	35
Service installation fails	35
Can't monitor service runtime status with manUil.....	35
Can't establish tunnel connections.....	36

How to Contact Technical Support.....	36
Example for Reference.....	37
Topology Diagram	37
Configuration.....	38
Special Example.....	40

About This Manual

This manual tells how to set up, configure, use, and troubleshoot the SeaChange MCastFwd software. It has been created for the MCastFwd 0.1 release. If there is any problem and you cannot find solution in this manual, please email to: support@i-zq.com.

Product Overview

This section provides an overview of the SeaChange Multicast Forward Service product, including:

- [“Introduction”](#)
- [“Product Features”](#)

Introduction

The product is Multicast Forward that is the application software may need to have a multicast conversation that spans 2 or more subnets, since the multicast will never be allowed past the router serving the subnet when an application use multicast in a subnet. Broadly speaking, it is the rough equivalent of a V-LAN for multicast support.

It provides a service or daemon that will

- aggregate multicast traffic,
- forward it via a connection-oriented protocol to a receiving service or daemon
- re-multicast the traffic at the receiving service or daemon

Broadly speaking, it is the rough equivalent of a V-LAN for multicast support.

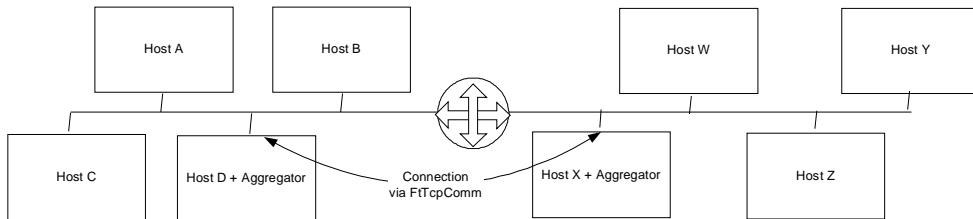


Figure 1 Small 2 Network System

In the small 2 network system above, a collection of nodes in both networks may want to participate in 1 single multicast conversation. The aggregators in each network would be configured to listen for that conversation and forward it to the other side.

Product Features

The main features of Multicast Forward Service are described below. It includes five parts:

[“SeaChange Style SeaChange Style Windows ServiceWindows Service”](#)

[“Powerful Network Support”](#)

[“Multi-rail support for the tunnel connections without loop and duplicate”](#)

[“Deny List Support”](#)

[“SeaChange ManUtil/SNMP support”](#)

SeaChange Style Windows Service

The McastFwd service is SeaChange Style Windows Service which runs as a Windows service using the SeaChange Service Shell and App Shell. User can start or stop the service in windows service list as below that is opened by the path: Control Panel => Administrative Tools => Services.

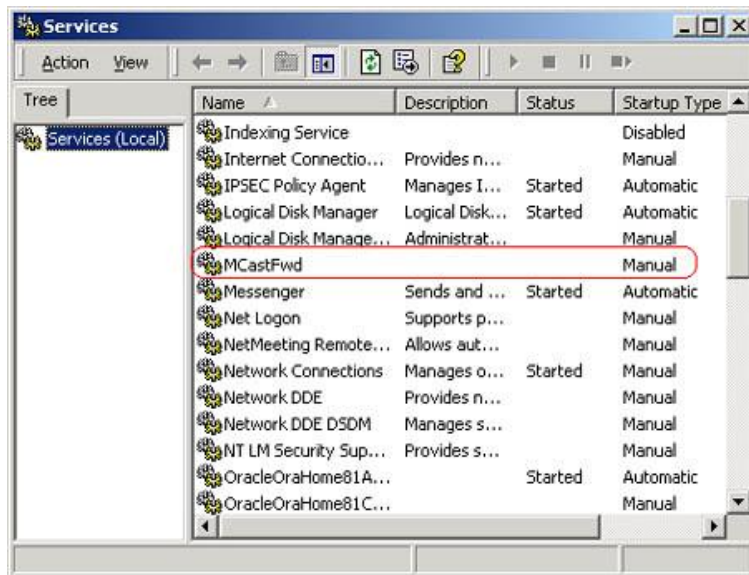


Figure 2 McastFwd in Service List

Powerful Network Support

The Multicast service and inter-service connections support both IPV4 and IPV6 conversations. The service can run on Windows 2003 for it supplies IPV6 environments. The solution supports both explicit IP addresses and resolvable host and group names for both IPv4 and IPv6 addresses in all network combinations. Further, to support all these network function, the service doesn't require any additional hardware and not need a separate machine to install.

Multi-rail support for the tunnel connections without loop and duplicate

The Multicast service supports multi-rail for the connection between different servers in which Multicast runs. That's to say a multicast conversation can be traversed multi-subnets. One Mcastfwd server forwards multicast messages on its local subnet to the other Mcastfwd server and the destined Mcastfwd server would subsequently re-multicast the received messages on its local subnet.

And the server is avoided to establish such rail to connect itself and the service can't forward any messages that were sourced from itself. And between two Mcastfwd installations there is only single TCP connection to forward multicast conversations.

Deny List Support

The Mcastfwd service support a deny list, containing both source addresses as well as source ports. Any messages sent from an IP/Port in this list should not be forwarded. This list can be added in configuration file (McastFwd.xml) and the format is as shown below.

```
<DenyList>
  <Source address="10.3.2.26" port="6000"/>
</DenyList>
```

Additionally, the deny items can be wildcast-ed (IPv4 address only), for example, the following definition is also acceptable:

```
<DenyList>
  < Source address="10.3.2.*" />
</DenyList>
```

Or

```
<DenyList>
  < Source address="192.168.0.0/24" />
</DenyList>
```

SeaChange ManUtil/SNMP support

The Mcastfwd service works equally well with SeaChange Manutil/SNMP for it always installs on SeaChange CC server. By ManUtil user can monitor the Mcastfwd run status including tunnel, conversation, denylist and resender interface.

Site Requirements

To deploy the SeaChange McastFwd service, your site must meet the following requirements:

- [“McastFwd Server Requirements”](#)
- [“Network Requirements”](#)
- [“SeaChange ITV SDK Requirements”](#)

McastFwd Server Requirements

Operation System Requirement

- | winNT4 or higher
- | Windows 2003 or higher (ipv6 support)

SeaChange CC (Command Center) server minimal requirement:

- | Intel SR1200 - 1 Rack Unit chassis
- | Processor: Intel Pentium III 1.0 GHz
- | Memory: 1,024 MB
- | Hard drives: 20GB, 30MB free disk space
- | NIC: 10/100M × 2

SeaChange MC (Media Cluster) Node group server minimal requirement:

- | Processor: Intel PIII 1.4 GHz
- | Memory: 256 MB
- | Hard drives: 40GB, 30MB free disk space
- | NIC: 10/100M × 2

Stand-alone PC server minimal requirement:

- | Intel x86 family Processor: PIII 1.0GHz
- | Memory: 256MB
- | Hard drivers: 20G
- | NIC: 100M × 2

Network Requirements

The network segments can be reached by ping operation but can't multicast each other.

- | ITV command center
- | ITV media cluster node

The later two are used to verify that the multicast forwarding service can be installed and work friendly with existing ITV components.

SeaChange ITV SDK Requirements

The SeaChange ITV SDK including ManUil should be installed which version is 2.0.2 if the Mcastfwd installation is not SeaChange CC server.

Installation

To install the SeaChange Multicast Forward Service, complete the following tasks:

[“Before You Begin”](#)

[“Step 1. Install Released SeaChange Multicast Forward Services”](#)

[“Step 2. Verify SeaChange Multicast Forward Services”](#)

[“Uninstall SeaChange Multicast Forward Services”](#)

[“Upgrade SeaChange Multicast Forward Services”](#)

If you encounter problems while completing these tasks, see [“Troubleshooting”](#)

Before You Begin

- q Decide which machines will serve as SeaChange McastFwd server to deal with Multicast traffic.
- q Decide which is picked as local machine and which as the remote one.

Table 1. Picked machine as servers

No	Servers		IP address
1	Remote		
2	*Local	Primary	
3		Backup	

* Local: When service deployed in SeaChange ITV CC, there would be two machines can be used as local server, generally CM1 as primary one and CM2 as backup one, for MDS1/2 having installed database software of SQL not to fit Mcastfwd service. When deployed in stand-alone machine, the local server is just only one machine that the primary one and the backup one is the same machine.

- q Prepare for installation of service to verify all target server OS is winNT4 or higher, ipv6 support only Win2003 or higher.
- q Verify the user login account is authorized as Administrator.
- q Remove the old SeaChange Multicast Forward Service and reboot the machine to guarantee a new state for installation.
- q List all the local IP addresses in the following table:

Table 2. Local IP addresse

No	IP address	NetInterfaceCard (name or MAC)	OtherEndOftheCable
1			
2			
3			
4			
5			

6			
7			
8			

Is there any two NICs connected to the same network segment physically? (Yes/No)

Leave one NIC connected to each network segment. _____

- q Pick the IP addresses from the above *Table 1 local IP addresses Table* to accept incoming tunnel connections:

IP address No. _____ as the primary address

IP address No. _____ as the backup address

Make sure these two addresses are not bound on the same NIC (Yes/No) _____

- q Pick the IP addresses from the above *Table 1 local IP addresses Table* to work as the default multicast traffic capture address:

IP address No. _____

IP address No. _____

IP address No. _____

IP address No. _____

IP address No. _____

IP address No. _____

IP address No. _____

IP address No. _____

....

Make sure no two IP addresses are on the same NIC, (Yes/No) _____

- q Determine the default re-sender interface. Select IP address from the *Table 1 local IP addresses Table*, and determine the send port:

Table 3 local resenders

ResenderNo	IP	Port	NIC
1			
2			
3			
4			
5			
6			

Make sure no two resenders are on the same NIC, (Yes/No) _____

- q If there is no other McastFwd services installed on the network segments that this machine belong to, simply skip this step. Otherwise, list their resender interface in the following table:

Table 4 Other resenders on the local network segments

ResenderNo	IP	Port
1		

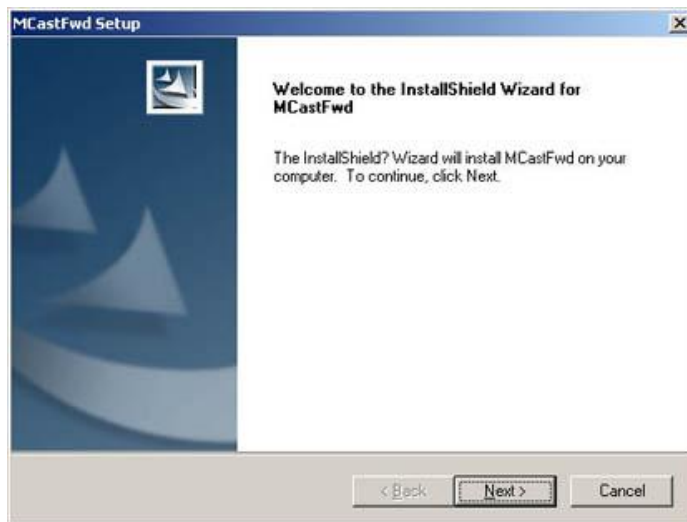
2		
3		
4		
5		
6		
7		
8		
9		
...		

**Note: Generally it's recommended that two services are all installed on ITV BMS in same one network segment in order to backup service.*

Step 1. Install Released SeaChange Multicast Forward Services

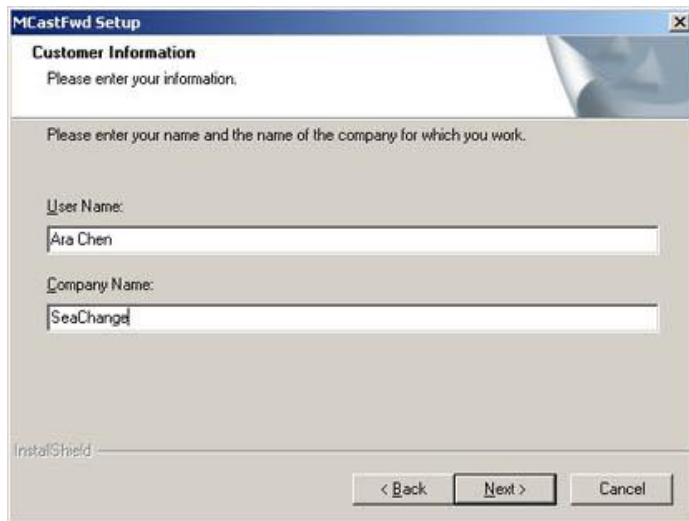
Have verified all 'Before You Begin' steps and then start to install Mcastfwd service.

1. Insert the SeaChange McastFwd software CD and locate and run Setup.exe
2. Double click setup icon to start up the installation process.



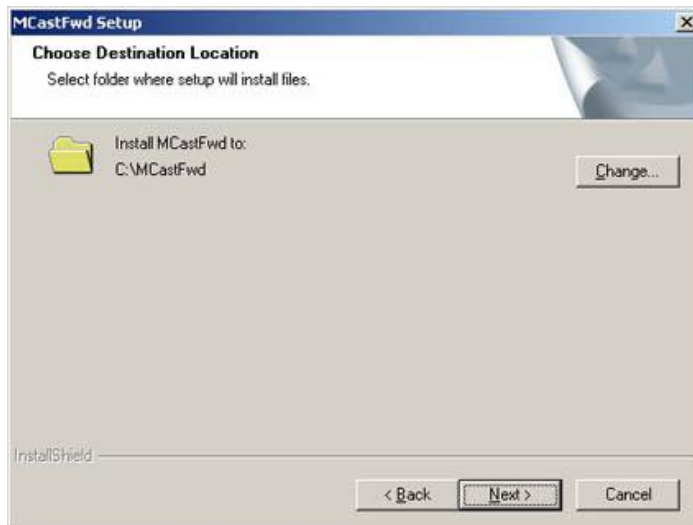
Interface 1 Welcome Interface

3. Click "Next".



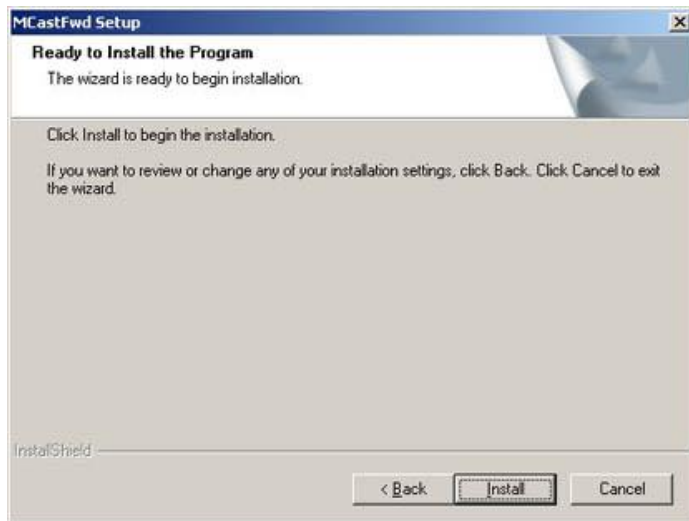
Interface 2 Customer Information

4. Input relevant customer information then click “Next”.



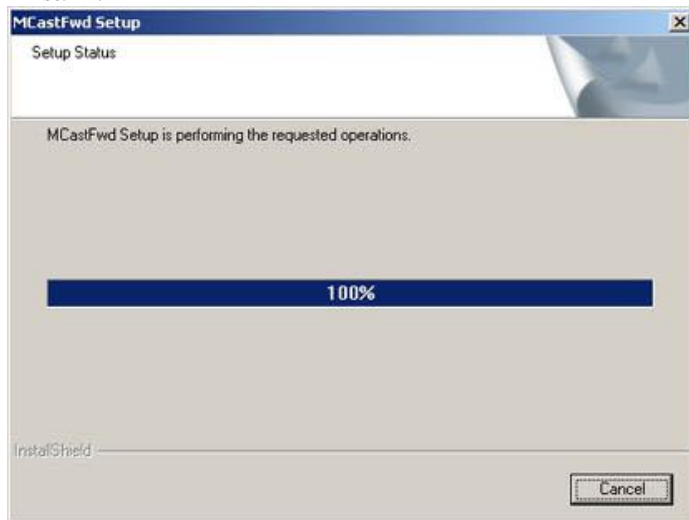
Interface 3 Installation Location

5. It appears the installing destination. The default directory is: C:\MCastFwd. If it's not your desired location, click “Change” to specify the installation location. Then, click “Next”.



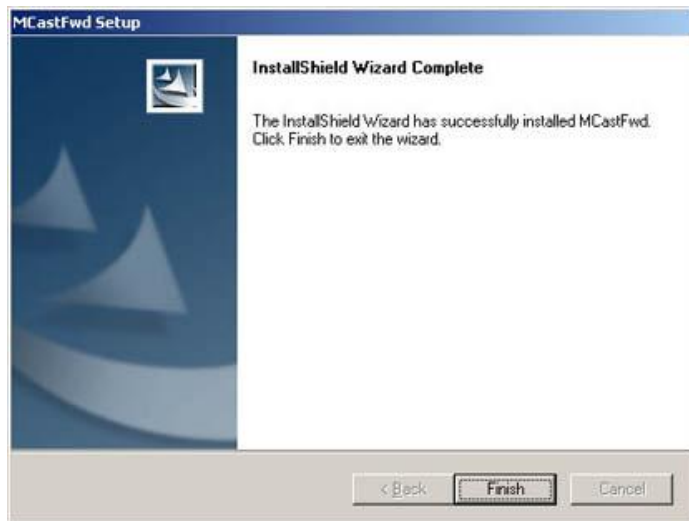
Interface 4 Confirmation Interface

6. Click "Install".



Interface 5 Setup Status

7. It pops up the setup status.



Interface 6 Installation Completed

8. Click "Finish". The installation of MCastFwd is completed.

Step 2. Verify SeaChange Multicast Forward Services

To check if the McastFwd Services installed to run normally, see steps as below:

1. An expected installation tree can be showed below:

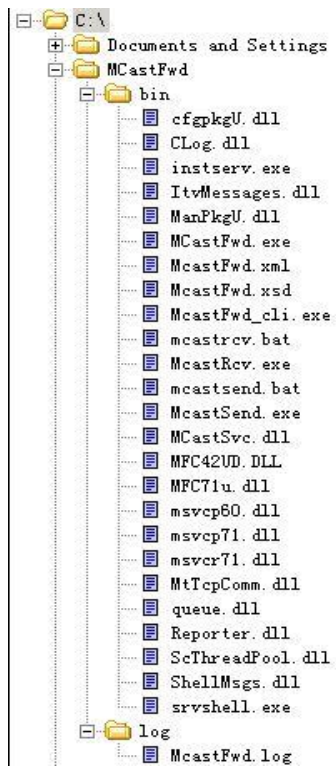


Figure 3 the Installation Tree

2. A 'McastFwd' service is listed in Services:

Open Control Panel => Administrative Tools => Services

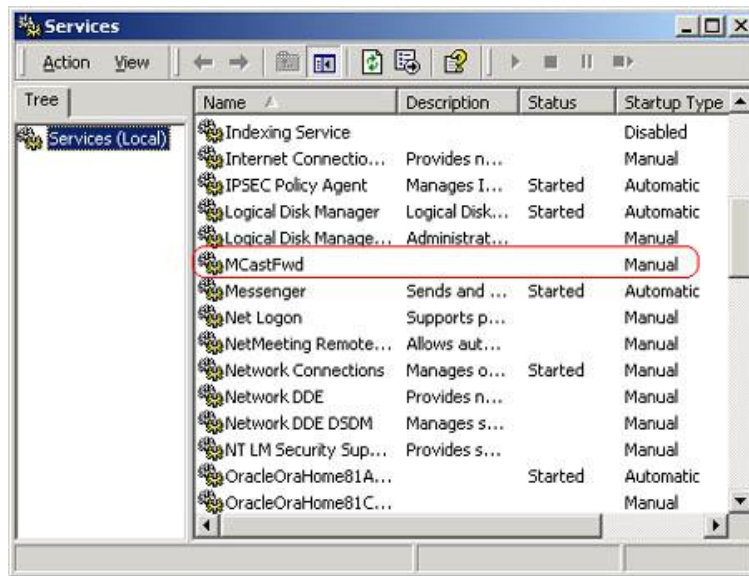


Figure 4 McastFwd in Service List

3. 'McastFwd' service registry keys

Open 'Run' => input 'regedit' => Open 'HKEY_LOCAL_MACHINE' => Open 'SOFTWARE'
=> Open 'SeaChange' => Open 'ITV' => Open 'CurrentVersion' => Open 'Services' => See the
'McastFwd' folder and Open it to see strings on the right table.

Verify paths of the 'ExtConfiguration' and the 'LogFileName' and log it.

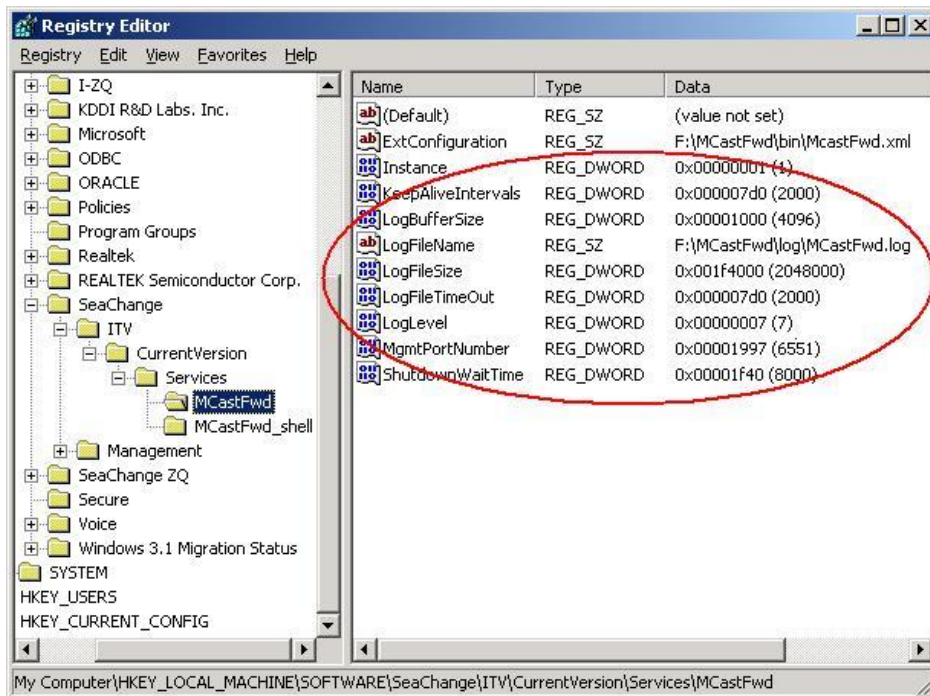


Figure 5 McastFwd in Regedit

Some registry keys in the Figure 6 will be specified as below:

ExtConfiguration	to set the path of the McastFwd configuration file McastFwd.xml.
LogBufferSize	to set the buffer size reserving for McastFwd log
LogfileName	to set the path of the McastFwd log file McastFwd.log under installation folder.
LogLevel	to set the path of the McastFwd log file McastFwd.log under installation folder.

Uninstall SeaChange Multicast Forward Services

Open control panel => Add/Remove program

Select the Mcastfwd program and press 'Delete' button to implement the uninstallation.

According to the prompt message to operate by default, press 'Finish' to complete the uninstallation process.

Enter the Regedit to verify the corresponding registry keys have been removed completely.

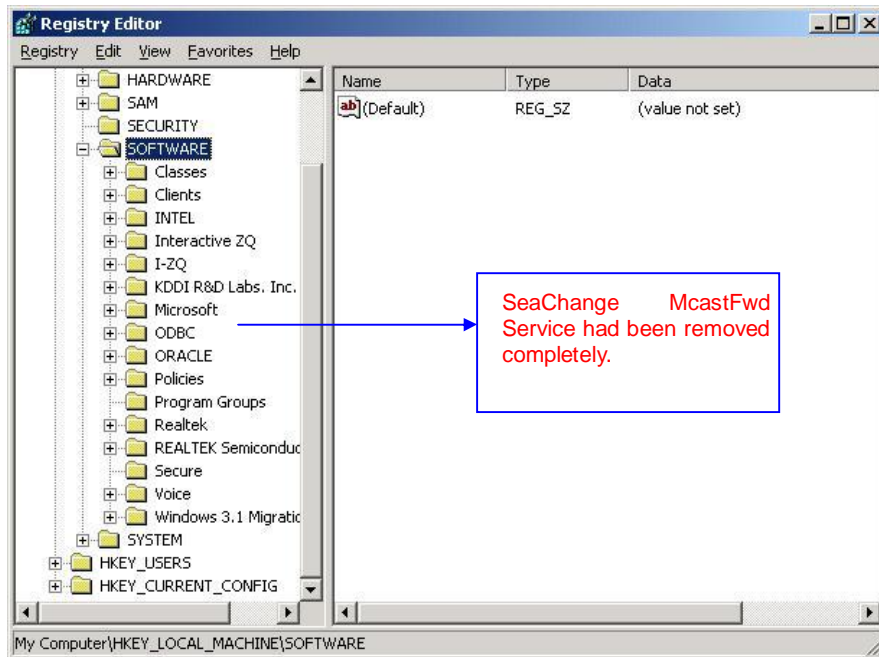


Figure 6 Regedit after uninstallation

Upgrade SeaChange Multicast Forward Services

Double click the installation exe file of new version on Mcastfwd server having old version installed.

The upgrade screen is as below shown:

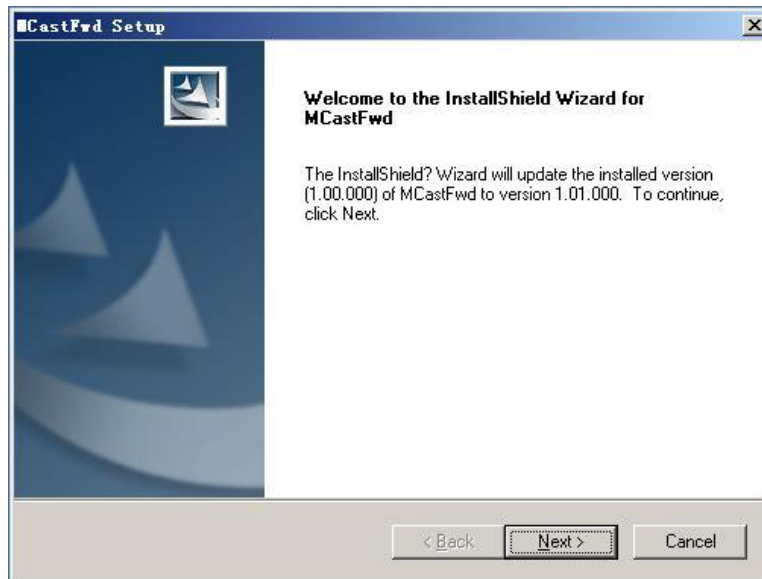


Figure 7 Upgrade interface

Then click 'Next' button to continue the process. When upgrade program is completed the below screen will pop up in which the upgraded version will also be displayed.

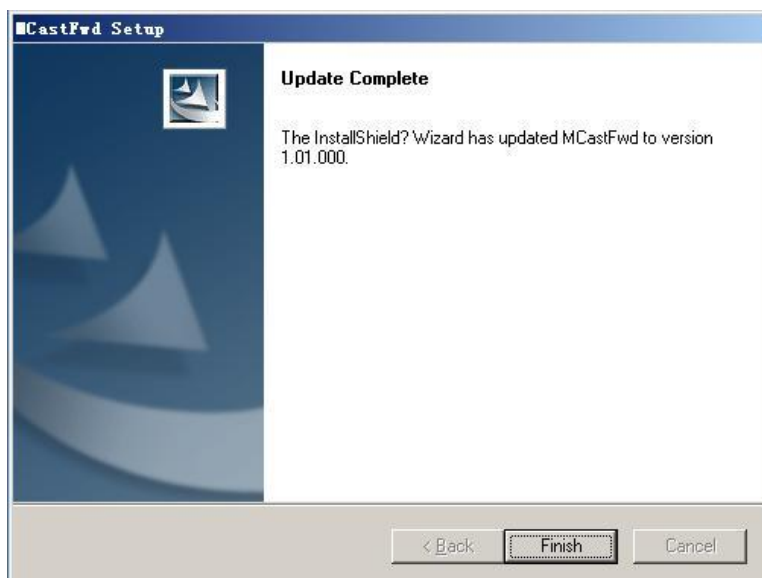


Figure 8 Upgrade finished interface

Configuration

Besides installing the service program, you must complete the following configuration tasks which the configuration file consists of before SeaChange Multicast Forward Services will work:

[“Step 1. Configure the <TunnelListener>”](#)

[“Step 2. Configure the <MulticastListener>”](#)

[“Step 3. Configure the <MulticastSender>”](#)

[“Step 4. Configure the <DenyList>”](#)

[“Step 5. Configure the <Tunnels> connection”](#)

[“Step 6. Configure the <Conversation> ”](#)

[“Configuration program”](#)

The configuration File name is McastFwd.xml and lies on the path of C:\McastFwd\bin which can be got in regedit (see before section [‘Figure 5 McastFwd in Regedit’](#)). The xml file is formatted as what McastFwd.xsd defined and starts with a root as following:

```
<Config xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="McastFwd.xsd">
```

To verify the McastFwd.xml you can keep the McastFwd.xsd in the installation folder and open the file with Microsoft Internet Explorer (ver 5.0+). If there is solecism in the xml file IE will display mistake information about the file.

“Step 1. Configure the <TunnelListener>”

<TunnelListener>: Local Addresses need to set for accepting incoming tunnel connections It includes at least 1 address of local host for socket element.

Note: The IP address should be two of those listed in [table 1](#).

“Step 2. Configure the <MulticastListener>”

<MulticastListener>: Default Local Addresses on which to listen for multicast It includes 0-n local IP address for socket element which can be omitted to correspond to the practical situation.

Note: The IP address should be two of those listed in [table 1](#).

“Step 3. Configure the <MulticastSender>”

<MulticastSender>: Default Local Addresses on which to send multicast It includes 0-n local IP address and port for socket element which can be omitted to correspond to the practical situation.

Note: The IP address should be two of those listed in [table 1](#).

“Step 4. Configure the <DenyList>”

<DenyList>: Default list of addresses from which messages should be ignored
It includes 0-n local address or wild cast address to be denied for denylist element. It also can be omitted by practical situation.

In general situation, the MulticastSender will be automatically added into the denylist by the service when there is one McastFwd server in one subnet.
But when there is several McastFwd services installed on the network segments that this machine belong to, you must add all other re-mcast forward interface into denylist here to avoid loop traffic. (The IP address is listed in [table 3](#).)

“Step 5. Configure the <Tunnels> connection”

<remotePort> is the port of Remote host.
<RemoteAddress>: Default list of remote servers that this service should connect and forward messages. The section of configuration includes two types of IP addresses in one conversation:
<LocalAddress> is IP address and port of Local host,
**Note: The IP address should be at lease one of those listed in [table 1](#).*

There is at least one section including RemoteAddress address and LocalAddress address for one connection. If it needs to establish several tunnels to connect and forward multicast message, you should add several <Tunnels> section in the same configuration file.

“Step 6. Configure the <Conversation>”

<groupAddr>, <groupPort>: Multicast IP address and port.
It includes at least one multicast address and port as socket element. When there are some conversations you should add some <conversation> sentence including different groupAddr and groupPort.
Meanwhile, user can add denylist and private re-mcast content into the conversation section as the private denylist address or the private tunnel connection for situation requirement.

**Note: Port mentioned in above content should not be conflicted by other services on the same machine.*

***Note: It is recommended that setting up directly the configuration file according to the above configuration steps.*

Configuration program

We also provide a configuration program to simplify the configuration work which can generate configuration file MCastfwd.xml automatically. What you just need to do is to answer its questions or to select its options along with it.
Open a Command Prompt; implement McastFwdConf.exe in the installation directory.

See the following sample, the red word is what user should input to follow the configuration guide.

```
C:\McastFwd\bin>McastFwdConf.exe -f mcastfwd.xml
The XML-formatted extension configuration for McastFwd is built with a
default setting and multiple conversation settings. The filename can be
specified in registry:
HKEY_LOCAL_MACHINE\SOFTWARE\SeaChange\ITV\CurrentVersion\McastFwd\ExtConfiguration

This program will guide you start with the default setting and then the
conversations.

#####
## default settings ##
#####
McastFwd can accept incoming tunnel connections from other McastFwd.
To make this feature enabled, McastFwd must open a tunnel server
listener which requires a port number and local IP addresses to bind.
Enter the TunnelListener port number: 1000
local address:
1) 192.168.10.5
2) 192.168.9.5
Select a local address for TunnelListener: 1
More address to bind TunnelListener [Y/N]: y
local address:
1) 192.168.10.5
2) 192.168.9.5
Select a local address for TunnelListener: 2
More address to bind TunnelListener [Y/N]: n
Configure default bind address to sniff mcast traffic [Y/N]: y
local address:
1) 192.168.10.5
2) 192.168.9.5
Select a local address for sniffing: 1
More bind address to sniff [Y/N]: n
Configure default bind address to re-mcast forwarded traffic [Y/N]: y
Enter the default send port number: 6000
local address:
1) 192.168.10.5
2) 192.168.9.5
Select a local address for re-mcasting: 2
More bind address to re-mcast [Y/N]: n
Configure default deny list to filter mcast traffic [Y/N]: y
Enter the source address: 192.168.9.5
```

```

Enter the source port number, 0 if any: 0
More source to deny [Y/N]: n
Configure default tunnel connections [Y/N]: y
Enter the remote tunnel server port number: 1000
Enter the remote address: 192.168.19.5
More backup remote address for the connection [Y/N]: y
Enter the remote address: 192.168.20.5
[Warning] you must be sure both remote addresses are on the same machine
local address:
1) 192.168.10.5
2) 192.168.9.5
Select a local address : 1
More backup local address for the connection [Y/N]: y
local address:
1) 192.168.10.5
2) 192.168.9.5
Select a local address : 2
More default tunnel connection [Y/N]: n
---- Default setting completed ----

#####
##  Conversations  ##
#####

A conversation is a combination of the destination multicast IP address
and port number, you must provide the information to specify.
Additionally, one conversation can has its own bind IP address to listener
and its own sender address. It can also have its own tunnel connections to
forward the message to the specified destination McastFwd instance. The
conversation will use the default listener and sender interface if the
private settings are not provided.
Enter the multicast group address: 225.25.15.35
Enter the multicast port number: 5000
Do you have any private setting for this conversation [Y/N]: n
---- conversation [225.25.15.35]:5000 setting completed ----

Configure more conversation [Y/N]: n
You must be sure the registry:
HKEY_LOCAL_MACHINE\SOFTWARE\SeaChange\ITV\CurrentVersion\McastFwd\ExtConfiguration

is point to the configuration file, then restart the McastFwd service to make the
configuration active. Turn the loglevel as DEBUG and check the log messages to verify if
the configuration is valid

```

The generated xml file is described as below:


```

: <Config>
: <Default>
: <TunnelListener localPort="1000">
  <LocalAddress address="192.168.10.5" />
  <LocalAddress address="192.168.9.5" />
</TunnelListener>
: <MulticastListener>
  <LocalAddress address="192.168.10.5" />
</MulticastListener>
: <MulticastSender localPort="6000">
  <LocalAddress address="192.168.9.5" />
</MulticastSender>
: <DenyList>
  <Source address="192.168.9.5" />
</DenyList>
: <Tunnels>
: <Connection remotePort="192.168.19.5">
  <RemoteAddress address="192.168.19.5" />
  <RemoteAddress address="192.168.20.5" />
  <LocalAddress address="192.168.10.5" />
  <LocalAddress address="192.168.9.5" />
</Connection>
</Tunnels>
</Default>
<Conversation groupAddr="225.25.15.35" groupPort="5000" />
</Config>

```

Operations

Once the installation and configuration tasks covered in the previous sections have been completed, you can perform the following SeaChange Multicast Forward Services operations:

[How to Start/Stop McastFwd service](#)

[How to Establish Tunnel Traffic](#)

[How to Deny Multicast Forwarding from a designated IP address and Port](#)

[How to Use manUil to Monitor McastFwd runtime status](#)

[How to Verify Forwarding Multicast message](#)

How to Start/Stop McastFwd service

After installing the McastFwd service we can start the service to use. There are two ways to use the service.

Ø **From the Windows Service Manager UI**

1. Open Control Panel => Administrative Tools => Services

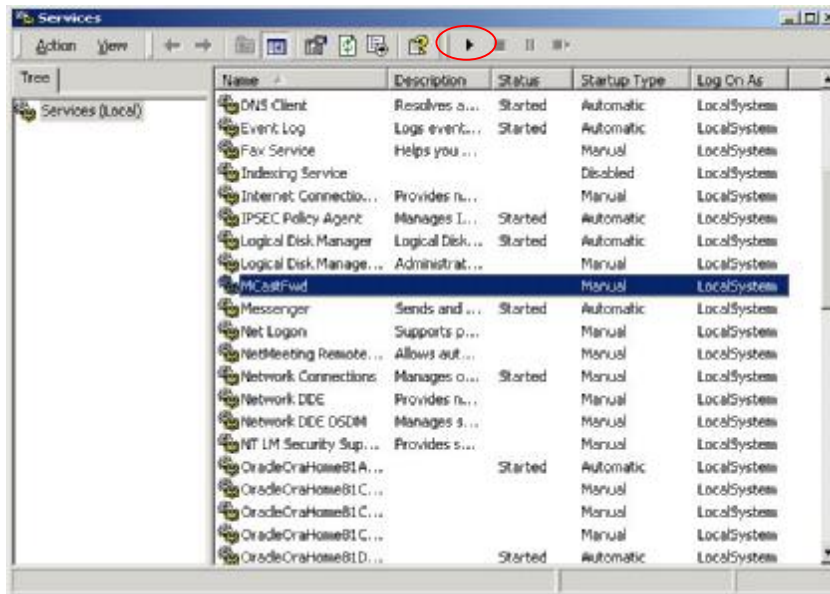


Figure 9 Start McastFwd in Services

2. Find and focus MCastFwd service, then press the „ / ■ button in the upper tool bar to start or stop it.

Ø From Command Prompt

1. Press 'Start' and input 'cmd' in 'Run' to open a cmd window.
2. Make sure the path in the front of cursor is McasFwd installation directory
C:\MCastFwd\bin.
3. Input the command sentence 'instserv.exe mcastfwd start' to start Mcastfwd service shown as below; similarly to stop the service with the 'instserv.exe mcastfwd stop' command.

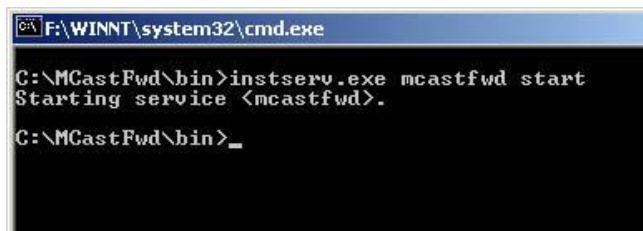


Figure 10 Start McastFwd in Command Prompt

How to Establish Tunnel Connections

1. Configure respectively the Mcastfwd.xml on the two servers which have been installed Mcastfwd service and will be established a tunnel to traffic, in their installation directory: 'C:\MCastFwd\bin'.

The parameters being configured are described below for details:

<TunnelListener>: Local host IP address (see "[Step 1. Configure the <TunnelListener>](#)" in [Configuration](#) section)

<RemoteServer>: IP address and port of Local and Remote hosts (see "[Step 5. Configure the <Tunnels> connection](#)" in [Configuration](#) section)

The following will illustrate with 2 servers' configurations. Assuming two servers IP addresses as below:

Server1 IP address: 192.168.9.5
192.168.10.5

Server2 IP address: 192.168.19.5
192.168.20.5

(1) on the Server 1

```
<Tunnels>
  <Connection remotePort="1000">
    <RemoteAddress address="192.168.19.5" />
    <RemoteAddress address="192.168.20.5" />
    <LocalAddress address="192.168.9.5" />
    <LocalAddress address="192.168.10.5" />
  </Connection>
</Tunnels>
```

带格式的: 缩进: 左 5.99 字符

带格式的: 缩进: 左 4.71 字符

带格式的: 缩进: 左 7 字符

带格式的: 缩进: 左 4.71 字符

带格式的: 缩进: 左 4.86 字符

(2) on the Server 2

```
<Tunnels>
  <Connection remotePort="1000">
    <RemoteAddress address="192.168.9.5" />
    <RemoteAddress address="192.168.10.5" />
    <LocalAddress address="192.168.19.5" />
    <LocalAddress address="192.168.20.5" />
  </Connection>
</Tunnels>
```

带格式的: 缩进: 左 5.99 字符

带格式的: 缩进: 左 4.71 字符

带格式的: 缩进: 左 7 字符

带格式的: 缩进: 左 4.71 字符

带格式的: 缩进: 左 4.86 字符

2. Start the Mcastfwd service on the two servers. Please see '[How to Start/Stop McastFwd service](#)' to operate.
3. Use manUi to check the unique tunnel has been established between two servers. Please see '[How to use manUi to monitor Mcastfwd runtime status](#)' for reference.

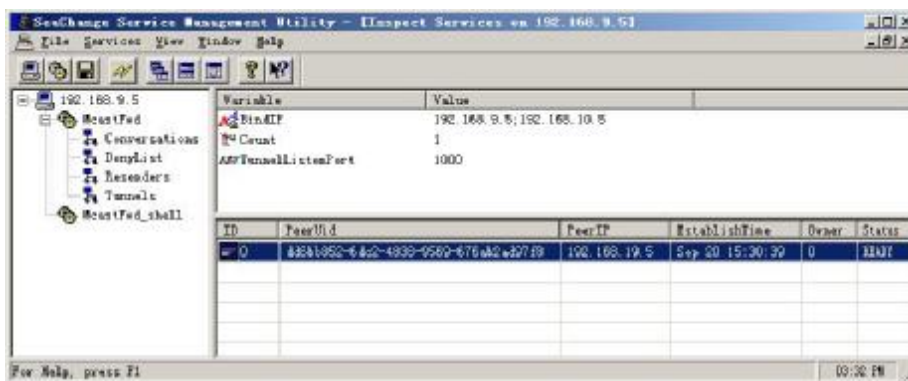


Figure 11 Established tunnel in manUi

How to Deny Multicast Forwarding against a specific source IP and Port

1. Determine a designated IP address and Port which should be deterred to forward multicast message. This IP address belongs to one host of the local area network including Mcastfwd server. For example the IP addresses 192.168.10.5 and the port 1000 need to deny which owned by a host named by 'A' lying on a subnet. Then this IP address and port "192.168.10.5: 1000" of host 'A' is designated and will be added into deny list in the configuration of server in the subnet.
2. Add the designated IP address and Port in <DenyList> which follows the <LocalSendAddress> content in the Mcastfwd server's configuration. (see "[Step 4. Configure the <DenyList>](#)" in [Configuration](#) section)

```
<DenyList>
  <Source address="192.168.10.5" port="1000" />
  <Source address="192.168.10.*" port="1111" />
  <Source address="192.168.10.0/24" port="2222" />
</DenyList>
```

删除的内容: .

4. Start the Mcastfwd service on the subnet's server. Please see '[How to Start/Stop McastFwd service](#)' to operate.
5. Use manUtil to check the denied IP address and port listed in the DenyList column. Please see '[How to use manUtil to monitor Mcastfwd runtime status](#)' for reference.

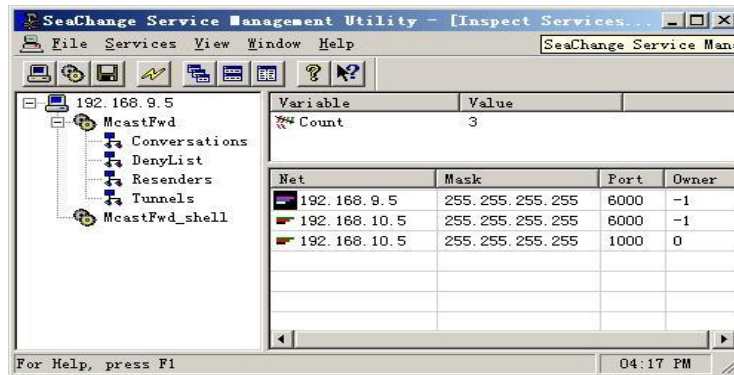



Figure 12 DenyList in manUtil

Note: The two IP addresses and ports listed in the DenyList column are the server's local addresses that are the default denied IP address and ports to avoid loop.

How to Use manUtil to Monitor McastFwd runtime status

1. Enter the SeaChange ITV SDK installation directory and double click the manUtil.exe Icon to open the management panel. Or open it by inputting 'manUtil' in Run window on the SeaChange CC server.
2. Click  the first icon in the tool bar and input the IP address of the computer need to monitor. Press Enter to open the monitor window. It includes two parts: McastFwd and McastFwd_shell.
3. To see McastFwd variables double click 'McastFwd' Icon on the left panel. (Figure as below)

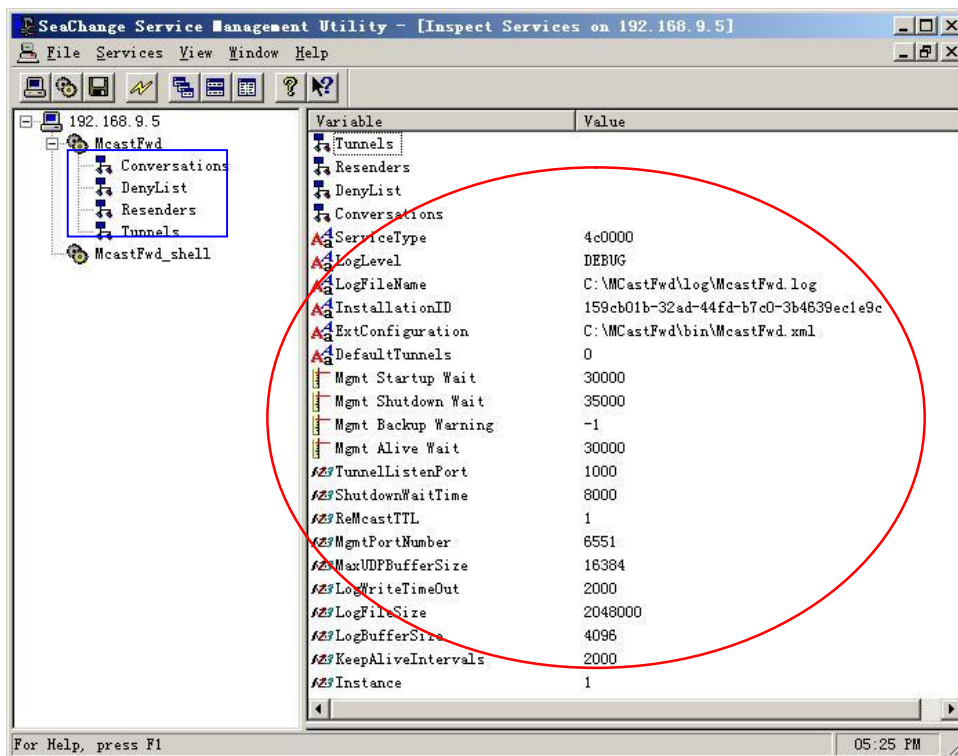


Figure 13 McastFwd variables in manUi

4. To see the McastFwd runtime status double click the corresponding Icon on the left panel. (See the blue box in above figure)

1. Tunnel status

Double click the 'Tunnels' icon to open the corresponding status window as below shown:

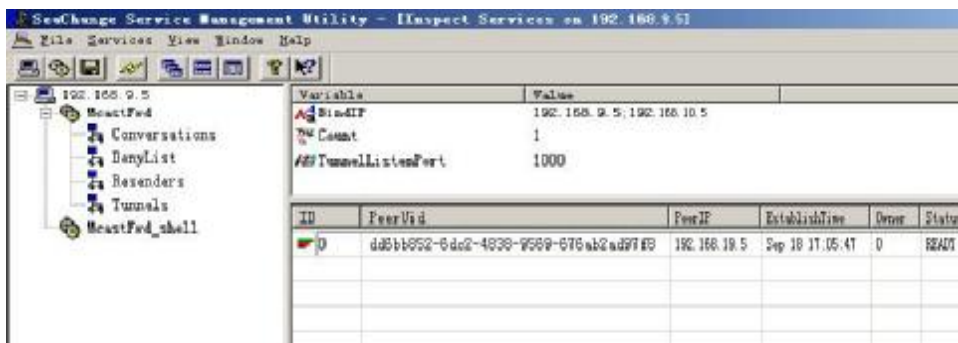


Figure 14 Tunnels status in manUil

Here list the parameters such as the PeerUid, the PeerIP, EsablishTime, Owner and Status.

PeerUid: the object server installation ID which lists in the McastFwd variables table in manUil. (see '[Figure 11 McastFwd variables in manUil](#)'))

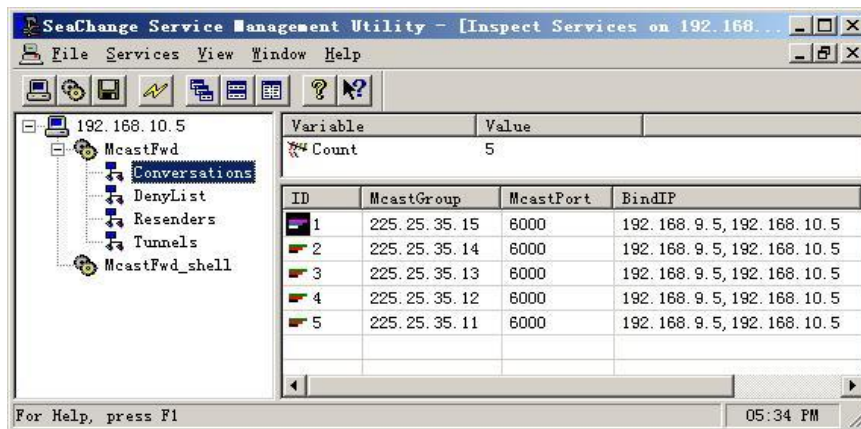
PeeIP: the object server IP address to connect via this tunnel.

EstablishTime: the time when the tunnel established.

Status: the tunnel current status.

2. Conversations status

Double click the 'Conversation' icon to list all current conversations shown as below:



SeaChange Service Management Utility - [Inspect Services on 192.168.10.5]

File Services View Window Help

192.168.10.5

- McastFwd
- Conversations
- DenyList
- Resenders
- Tunnels
- McastFwd_shell

Variable	Value
Count	5

ID	McastGroup	McastPort	BindIP
1	225.25.35.15	6000	192.168.9.5, 192.168.10.5
2	225.25.35.14	6000	192.168.9.5, 192.168.10.5
3	225.25.35.13	6000	192.168.9.5, 192.168.10.5
4	225.25.35.12	6000	192.168.9.5, 192.168.10.5
5	225.25.35.11	6000	192.168.9.5, 192.168.10.5

For Help, press F1

05:34 PM

Figure 15 Conversations in manUil

3. DenyList status

To see the denied IP address and port double click the 'DenyList' icon. (see '[Figure 10 DenyList in manUil](#)' to check the DenyList window)

4. Resenders status

Double click the 'Resenders' icon to list the resender interface IP address of the monitored computer which is configured in <LocalSendAddress> of Mcastfwd.xml. (see "[Step 3 Configure the <MulticastSend>](#)" in [Configuration](#) section)

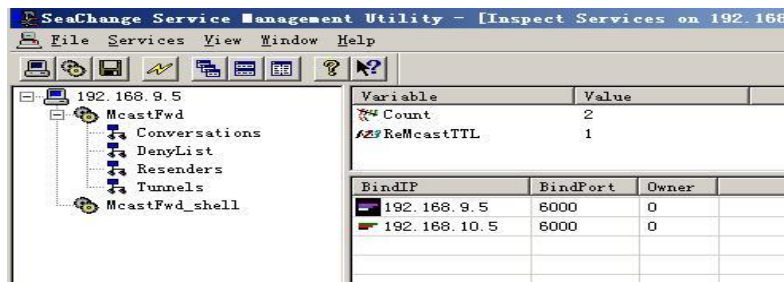


Figure 16 Resenders in manUiI

How to verify Forwarding Multicast messages

1. Open Command Prompt by inputting cmd in Run window on the two servers which the tunnel connects.
2. Make sure the path in the front of cursor is McasFwd installation directory C:\MCastFwd\bin.
3. On a machine on the same network segment of server 1, open a listener to implement 'mcastsnfr -g 225.25.35.15 -p 6000 -t 100' in commend window. Here 225.25.35.15 and 6000 are the specified multicast group and port which can be forwarded and lists into the server 2's conversations. (See '[Conversation status](#)' for reference.) And 100 follows '-t' is the listen time.
4. On a machine on the same network segment of server 2, open a sender by inputting 'mcastsend -g 225.25.35.15 -p 6000 -m TEST' in commend window. And then the program sends the multicast message 'TEST' to see if the above mcastsnfr program of 3) can receive the message. Here 'TEST' is multicast message which can be replaced by whatever you want to send.
5. Server 1 receive the inputted message 'TEST' from Resender IP address and port configured in the before section. (see '[Step 3 Configure the <MulticastSend>](#)' section for reference) If set 192.168.10.5: 5000 as the resenders address and port for an instance, what we can see from the receiver in server 1 is '**received from 192.168.10.5: 5000 TEST**'.

The Usage of Mcastsend & McastSnfr

Mcastsend Usage: McastSend [-b <bindIP>] [-r <bindport>] [-t <TTL>] [-i <n>] [-c <n>]
 -g <mcastIP> -p <port> {[-s] | [-m <message>] [-l <n>] }

Options:

- b: the local IP address to bind
- r: the local port to send message thru. default 1000
- t: package TTL (time to live). default 128

- i: repeat interval. default 500 msec
- c: repeat times. default 1
- g: the mulitcast group IP address
- p: the mulitcast port. default 1000
- s: send sequence number as message body, -m and -l will be ignored
- m: the message to send
- l: the length of message to send
- h: display this help

McastSnfrUsage: McastSnfr [-b <bindIP>] [-s] -g <mcastIP> -p <port>

Options:

- b: the local IP address to bind
- g: the mulitcast group IP address
- p: the mulitcast port. default 1000
- t: listen time, in sec. default 20
- s: with timestamps
- h: display this help

Troubleshooting

This section suggests ways to deal with problems that you might encounter while setting up or performing SeaChange MCastFwd service, including:

[‘Service installation fails’](#)

[‘Can’t monitor service runtime status with manUil’](#)

[‘Can’t establish tunnel’](#)

[‘How to Contact Technical Support’](#)

Service installation fails

You cannot find “MCastFwd” under “Services” of “Administrative Tool” in “Control Panel”, or under the installation directory, or in REGEDIT.

Possible Cause	Recommended Action
You have no administrator access to the computer.	Login your computer with administrator access. Delete the string “MCastFwd” in “REGEDIT”, if any. Reinstall MCastFwd in the system.

Can’t monitor service runtime status with manUil

When you open SeaChange manUil to be ready to monitor service runtime status you find the MCastFwd can’t be opened with double click.

Possible Cause	Recommended Action
Service doesn’t start.	Start the McastFwd service (see ‘How to Start/Stop McastFwd service’ section for operation.)
Incorrect settings in configuration file.	Stop the McastFwd service (see ‘How to Start/Stop McastFwd service’ section for operation.) Open the configuration file McastFwd.xml in installation directory C:\Mcastfwd\bin. Check the settings in this file all configured as instructed in Configuration section, especially the TunnelListener and LocalListenAddress settings.

Can't establish tunnel connections

The traffic tunnel can't be established between two servers McastFwd service runs. See the '[Tunnel status](#)' section to check the tunnel status with SeaChange manUil.

Possible Cause	Recommended Action
Incorrect settings in configuration file.	Stop the McastFwd service (see ' How to Start/Stop McastFwd service ' section for operation.) Open the configuration file McastFwd.xml in installation directory C:\Mcastfwd\bin. Check the settings in this file all configured as instructed in Configuration section, especially the TunnelListener and RemoteServer settings. (see ' Step 5. Configure the <Tunnels> connections ' and ' How to establish Tunnel Traffic ' section)
Bad IP network connection	Issue "ping" requests between the two servers. And if any fails reset router print on the two servers to make sure the network expedite.

How to Contact Technical Support

During your warranty period, or as part of your Full Service Maintenance contract, SeaChange provides technical support 24 hours per day, 7 days per week. You can send email to support@i-zq.com at any time or call the following telephone number directly: +12-021-52065233 Press 0 Extend to the operator.

If a support engineer can't take your call immediately, either hold the line or leave a phone number they can call back. We guarantee a response within **two hours**, regardless of time of day. Please have the following information available:

- 1 The case number, if you are calling about a previous problem
- 1 Your name, company name, and location (city, state or province, and country)
- 1 Telephone number at which you can be reached for the next **two hours**
- 1 Detailed problem description, including the symptoms, the activities that preceded the problem, and your troubleshooting steps and observations.

Example for Reference

Assuming the Mcastfwd on-site environment for an example:

There is a SeaChange Command Center server deployed in Shanghai. And the Mcastfwd service has been installed in the MDS1 server belonging to part of CC. The MDS1 has two IP addresses: 10.0.1.1 and 10.0.1.2 via which the multicast message can be routed respectively to Media Clusters in Guangzhou and Beijing.

Let it be supposed that the IP address in node 1 of Guangzhou's Media Cluster is 10.0.2.2, and another IP address in Beijing's is 10.0.3.3. All mask addresses is 225.25.25.25.

The following sections will instruct the topology diagram and configuration in each site.

Topology Diagram

The example's topology diagram is shown as below:

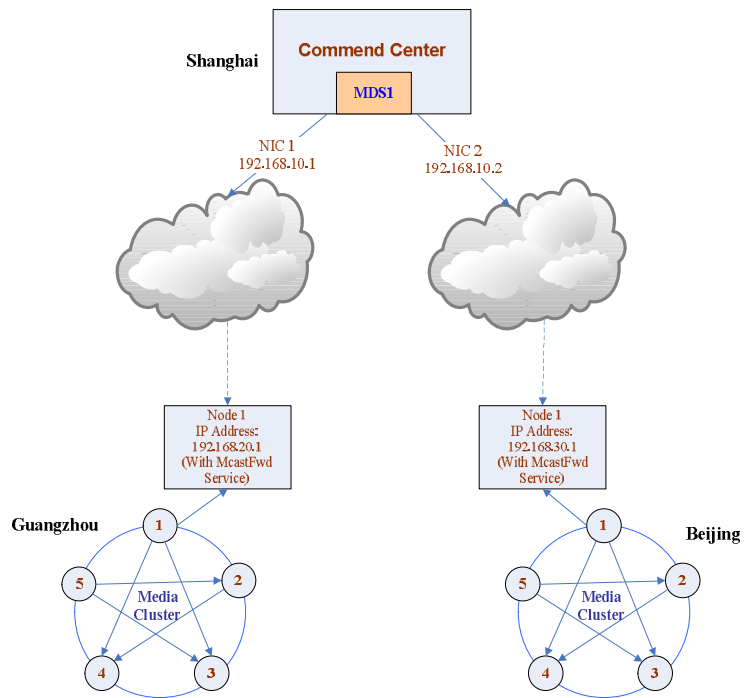


Figure 17 Topology Diagram for assumption

Configuration

The three sites IP addresses are described as the above diagram shown.

And the re-send interface IP address and port is determined as following:

ResenderNo	IP	Port	NIC/Site
1	192.168.10.1	5000	NIC 1
2	192.168.10.2	5000	NIC 2
3	192.168.20.1	5000	Guangzhou
4	192.168.30.1	5000	Beijing

The Mcastfwd service in MDS1 of Shanghai's CC should be configured in Mcastfwd.xml as the following:

```
<Config>
<Default>
<TunnelListener localPort="1000">
<LocalAddress address="192.168.10.1" />
<LocalAddress address="192.168.10.2" />
</TunnelListener>
<MulticastListener>
<LocalAddress address="192.168.10.1" />
<LocalAddress address="192.168.10.2" />
</MulticastListener>
<MulticastSender localPort="5000">
<LocalAddress address="192.168.10.1" />
<LocalAddress address="192.168.10.2" />
</MulticastSender>
<Tunnels>
<Connection remotePort="1000">
<RemoteAddress address="192.168.20.1" />
<LocalAddress address="192.168.10.1" />
</Connection>
<Connection remotePort="1000">
<RemoteAddress address="192.168.30.1" />
<LocalAddress address="192.168.10.2" />
</Connection>
</Tunnels>
</Default>
<Conversation groupAddr="225.25.15.35" groupPort="6000" />
</Config>
```

The Mcastfwd service in Guangzhou's Media Cluster should be configured in Mcastfwd.xml as the following:

```
<Config>
```

```

<Default>
<TunnelListener localPort="1000">
  <LocalAddress address="192.168.20.1" />
</TunnelListener>
<MulticastListener>
  <LocalAddress address="192.168.20.1" />
</MulticastListener>
<MulticastSender localPort="5000">
  <LocalAddress address="192.168.20.1" />
</MulticastSender>
<Tunnels>
<Connection remotePort="1000">
  <RemoteAddress address="192.168.10.1" />
  <LocalAddress address="192.168.20.1" />
</Connection>
</Tunnels>
</Default>
<Conversation groupAddr="225.25.15.35" groupPort="6000" />
</Config>

```

The Mcastfwd service in Beijing's Media Cluster should be configured in Mcastfwd.xml as the following:

```

<Config>
<Default>
<TunnelListener localPort="1000">
  <LocalAddress address="192.168.30.1" />
</TunnelListener>
<MulticastListener>
  <LocalAddress address="192.168.30.1" />
</MulticastListener>
<MulticastSender localPort="5000">
  <LocalAddress address="192.168.30.1" />
</MulticastSender>
<Tunnels>
<Connection remotePort="1000">
  <RemoteAddress address="192.168.10.2" />
  <LocalAddress address="192.168.30.1" />
</Connection>
</Tunnels>
</Default>
<Conversation groupAddr="225.25.15.35" groupPort="6000" />
</Config>

```

Special Example

Here will list the configuration for special example which is two servers in a same subnet and can multicast conversation each other without Mcastfwd.

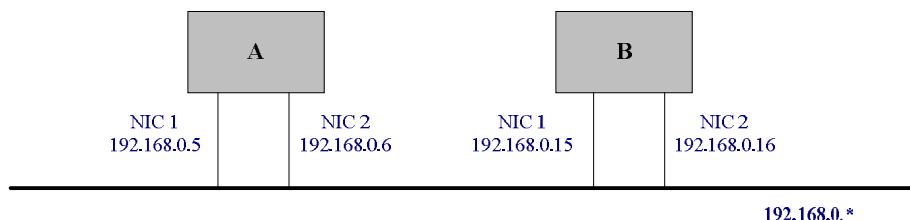


Figure 18 the Diagram for Special Example

The two server's IP addresses are collected in the below table.

No	IP address	NIC	Server
1	192.168.0.5	NIC 1	A
2	192.168.0.6	NIC 2	A
3	192.168.0.15	NIC 1	B
4	192.168.0.16	NIC 2	B

And the re-send interface IP address and port is determined as following:

ResenderNo	IP	Port	NIC/Server
1	192.168.0.5	5000	NIC 1/A
2	192.168.0.6	5000	NIC 2/A
3	192.168.0.15	5000	NIC 1/B
4	192.168.0.16	5000	NIC 2/B

Especially to notice that the servers in a same local area network should be added the IP address of the other machine into denylist in the configuration file to prevent loop. And so please refer to the section of "[Before you begin](#)", see "[Table 4](#)". The corresponding resender interface is described as below table:

ResenderNo	IP	Port	NIC/Server
1	192.168.0.5	5000	NIC 1/A
2	192.168.0.6	5000	NIC 2/A
3	192.168.0.15	5000	NIC 1/B
4	192.168.0.16	5000	NIC 2/B

The Mcastfwd server of A should be configured in Mcastfwd.xml as this:

<Config>

```

<Default>
<TunnelListener localPort="1000">
  <LocalAddress address="192.168.0.5" />
  <LocalAddress address="192.168.0.6" />
</TunnelListener>
<MulticastListener>
  <LocalAddress address="192.168.0.5" />
  <LocalAddress address="192.168.0.6" />
</MulticastListener>
<MulticastSender localPort="5000">
  <LocalAddress address="192.168.0.5" />
  <LocalAddress address="192.168.0.6" />
</MulticastSender>
<DenyList>
  <Socket address="192.168.0.15" port="5000" />
  <Socket address="192.168.0.16" port="5000" />
</DenyList>
<Tunnels>
<Connection remotePort="1000">
  <RemoteAddress address="192.168.0.15" />
  <RemoteAddress address="192.168.0.16" />
  <LocalAddress address="192.168. 0.5" />
  <LocalAddress address="192.168. 0.6"/>
</Connection>
</Tunnels>
</Default>
<Conversation groupAddr="225.25.15.35" groupPort="6000" />
</Config>

```

The configuration in Mcastfwd server of B should be described as following:

```

<Config>
<Default>
<TunnelListener localPort="1000">
  <LocalAddress address="192.168.0.15" />
  <LocalAddress address="192.168.0.16" />
</TunnelListener>
<MulticastListener>
  <LocalAddress address="192.168.0.15" />
  <LocalAddress address="192.168.0.16" />
</MulticastListener>
<MulticastSender localPort="5000">
  <LocalAddress address="192.168.0.15" />
  <LocalAddress address="192.168.0.16" />
</MulticastSender>
<DenyList>

```



```
<Socket address="192.168.0.5" port="5000" />
  <Socket address="192.168.0.6" port="5000" />
</DenyList>
<Tunnels>
<Connection remotePort="1000">
  <RemoteAddress address="192.168.0.5" />
  <RemoteAddress address="192.168.0.6" />
  <LocalAddress address="192.168. 0.15" />
  <LocalAddress address="192.168. 0.16"/>
</Connection>
</Tunnels>
</Default>
<Conversation groupAddr="225.25.15.35" groupPort="6000" />
</Config>
```