Appendix D

Troubleshooting External Audio/Video Call Failures

Problem Description

This document provides a step-by-step approach to troubleshooting the following issues:

- Calls between external and internal users, who are using products such as Microsoft® Office Communicator and Microsoft Office Communicator Phone Edition, that fail to connect.
- External users, who are using products such as Office Communicator, Office Communicator Phone Edition, and, Microsoft Office Live Meeting, cannot join a conference.

The troubleshooting methods in this document assume that audio/video calls between internal users can be made successfully. It is also assumed that the A/V Edge and A/V Authentication services on the Audio/Video Edge Server are running. To verify this you can do the following:

1. Ensure that the Office Communications Server 2007 R2 Admin Tools are installed on the server.
2. Open the **Computer Management Console**.
3. Expand the **Services and Applications** node.
4. Click **Office Communications Server 2007 R2** and verify in the right pane that the A/V Edge and A/V Authentication services are running.

If either of the services is not running, start the service by doing the following:

- Right-click **Office Communications Server 2007 R2**, click **Start**, and then select the service that you want to start.

If either of the services cannot be started, do the following:

1. Open Event Viewer Management Console.
2. Click the **Office Communications Server** node, and then check for errors.

If errors are found, mitigate the problems listed in Event Viewer and start the service or services again.

Troubleshooting

To troubleshoot external audio/video call failures the Office Communicator log file is needed. To enable logging for your Office Communicator application running outside your enterprise firewall, do the following:

1. Click **Tools**, and then click **Options**.
2. Click the **General** tab.
3. Select the **Turn on logging in Communicator** check box (Figure D-1).

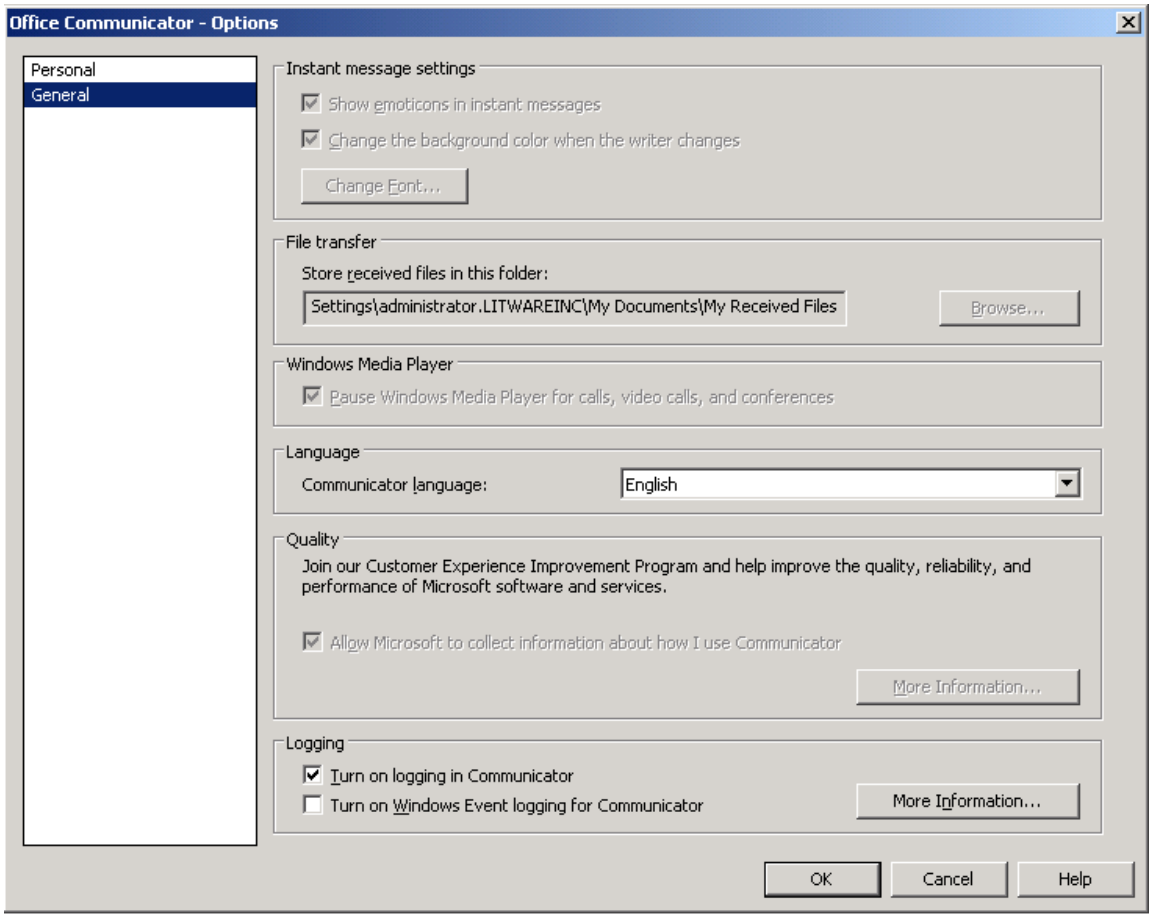

Figure D-1 Turning on logging in Communicator

Restart Office Communicator to create a fresh log and attempt to make a call to an internal user, which should fail. The log files are stored in the Tracing subfolder of your Windows user profile folder (this folder is the Documents and Settings folder on Windows Server® 2003). To locate the information you need from the log file, do the following (Most tags and messages of interest are highlighted for you, but will not be in the logfiles created):

1. Open the Communicator-uccapi-0.uccapilog file (or the Communicator-uccapi-1.uccapilog file if the data described in the following log file sample is not found the first file).

2. In the log file, locate the *SUBSCRIBE SIP* message by searching for the tag *Sending Packet* repeatedly until *SUBSCRIBE* is found on the next line and an XML string with the root node *provisioningGroupList* follows shortly.

3. Record the *CALL-ID* string found a few lines after *SUBSCRIBE*:

```
11/21/2008|23:31:10.381 190:4FC INFO  :: Sending Packet - 192.168.1.5:5061 (From
Local Address: 192.168.1.10:1259) 1288 bytes:


11/21/2008|23:31:10.381 190:4FC INFO  :: SUBSCRIBE sip:bart@litwareinc.com SIP/2.0
Via: SIP/2.0/TLS 192.168.1.10:1259
Max-Forwards: 70
From: <sip:bart@litwareinc.com>;tag=a8a3ea681b;epid=3c465b617a
To: <sip:bart@litwareinc.com>
Call-ID: 8a9fb943e213456482dbede7bc8ea467
CSeq: 1 SUBSCRIBE
Contact: <sip:bart@litwareinc.com;opaque=user:epid:cYUGvoWWcl6mKX37xhEMuAAA;gruu>
User-Agent: UCCAPI/3.5.6874.0 OC/3.5.6874.0 (Microsoft Office Communicator 2007 R2
(RC))
Event: vnd-microsoft-provisioning-v2
Accept: application/vnd-microsoft-roaming-provisioning-v2+xml
Supported: com.microsoft.autoextend
Supported: ms-benotify
Proxy-Require: ms-benotify
Supported: ms-piggyback-first-notify
Expires: 0
Proxy-Authorization: NTLM qop="auth", realm="SIP Communications Service",
opaque="EB6E1210", targetname="OCS-FE.litwareinc.com", crand="faeb2ac9", cnum="4",
response="01000000000000000bfb8bea5f1377568"
Content-Type: application/vnd-microsoft-roaming-provisioning-v2+xml
Content-Length: 327
<provisioningGroupList
xmlns="http://schemas.microsoft.com/2006/09/sip/provisioninggrouplist"><provisioning
Group name="ServerConfiguration"/><provisioningGroup
name="meetingPolicy"/><provisioningGroup name="ucPolicy"/><provisioningGroup
name="publicationGrammar"/><provisioningGroup
name="userSetting"/></provisioningGroupList>


11/21/2008|23:31:10.381 190:4FC INFO  :: End of Sending Packet - 192.168.1.5:5061
(From Local Address: 192.168.1.10:1259) 1288 bytes
```

4. Next, search for the tag *Data Received* and stop when on the next line the SIP message displays as *SIP/2.0 200 OK* and the *CALL-ID* string that follows is the same as the one recorded at step 3. This is the response to the *SUBSCRIBE SIP* message above.

```
11/21/2008|23:31:10.396 190:4FC INFO  :: Data Received - 192.168.1.5:5061 (To Local
Address: 192.168.1.10:1259) 37770 bytes:


11/21/2008|23:31:10.396 190:4FC INFO  :: SIP/2.0 200 OK
ms-user-logon-data: RemoteUser
Contact: <sip:pool01.litwareinc.com:5061;transport=tls;ms-fe=OCS-
FE.litwareinc.com;received=192.168.100.5;ms-received-cid=602>
Authentication-Info: NTLM rspauth="0100000000000000F0006AACF1377568",
srand="DE6811F2", snum="4", opaque="EB6E1210", qop="auth", targetname="OCS-
FE.litwareinc.com", realm="SIP Communications Service"
Content-Length: 36747
From: "Bart Duncan"<sip:bart@litwareinc.com>;tag=a8a3ea681b;epid=3c465b617a
To: <sip:bart@litwareinc.com>;tag=AB7E8D4E
Call-ID: 8a9fb943e213456482dbede7bc8ea467
CSeq: 1 SUBSCRIBE
Via: SIP/2.0/TLS 192.168.1.10:1259;ms-received-port=1259;ms-received-cid=C00
Expires: 0
Content-Type: application/vnd-microsoft-roaming-provisioning-v2+xml
Event: vnd-microsoft-provisioning-v2
subscription-state: terminated;expires=0
ms-piggyback-cseq: 1
Supported: ms-piggyback-first-notify
Record-Route: <sip:sip.litwareinc.com:5061;transport=tls;opaque=state:Ci.Rc00;lr;ms-
route-sig=aa_Jh7C4Dqf13k-Iw196o5m5xoObxFTUCeRI7rlwAA>
<provisionGroupList
xmlns="http://schemas.microsoft.com/2006/09/sip/provisiongrouplist-notification">
<provisionGroup name="ServerConfiguration" >
<ucMaxVideoRateAllowed>VGA-600K</ucMaxVideoRateAllowed>
<absInternalServerUrl>https://pool01.litwareinc.com/Abs/Int/Handler</absInternalServ
erUrl>
<absWebServiceEnabled>true</absWebServiceEnabled>
<ucPC2PCAVEncryption>RequireEncryption</ucPC2PCAVEncryption>
<organization>Corporation</organization>
<consoleDownloadInternalUrl>http://r.office.microsoft.com/r/rlidOCS?clid=1033&amp;p1
=livemeeting</consoleDownloadInternalUrl>
<consoleDownloadExternalUrl>http://r.office.microsoft.com/r/rlidOCS?clid=1033&amp;p1
=livemeeting</consoleDownloadExternalUrl>
<helpdeskInternalUrl>http://r.office.microsoft.com/r/rlidLiveMeeting?p1=12&amp;p2=en
_us&amp;p3=LMInfo&amp;p4=supportserver</helpdeskInternalUrl>
<helpdeskExternalUrl>http://r.office.microsoft.com/r/rlidLiveMeeting?p1=12&amp;p2=en
_us&amp;p3=LMInfo&amp;p4=supportserver</helpdeskExternalUrl>
<dlxInternalUrl>https://pool01.litwareinc.com/GroupExpansion/Int/service.asmx</dlxIn
ternalUrl>
<dlxEnabled>true</dlxEnabled>
<ucDiffServVoice>40</ucDiffServVoice>
<ucVoice802_1p>0</ucVoice802_1p>
<ucEnforcePinLock>true</ucEnforcePinLock>
<ucMinPinLength>6</ucMinPinLength>
<ucPhoneTimeOut>10</ucPhoneTimeOut>
<ucExchangeMWIPoll>3</ucExchangeMWIPoll>
<ucEnableSIPSecurityMode>High</ucEnableSIPSecurityMode>
<ucEnableUserLogging>false</ucEnableUserLogging>
<updatesServerInternalUrl>https://pool01.litwareinc.com/RequestHandler/ucdevice.upx<
/updatesServerInternalUrl>
```

```
<updatesServerEnabled>true</updatesServerEnabled>
<ucPortRangeEnabled>false</ucPortRangeEnabled>
<ucMinMediaPort>5350</ucMinMediaPort>
<ucMaxMediaPort>5353</ucMaxMediaPort>
<ucMinSipDynamicPort>7100</ucMinSipDynamicPort>
<ucMaxSipDynamicPort>7103</ucMaxSipDynamicPort>
<qosEnabled>false</qosEnabled>
<ucLocationProfile >
LOCPROF</ucLocationProfile>
<mrasUri >
sip:edgesrv.litwareinc.com@litwareinc.com;gruu;opaque=srvr:MRAS:P2nY_WtqnEGPHhBbcYD8
VQAA</mrasUri>
```

5. Locate the body of the *200 OK* SIP message, which is an XML string with the root node called *provisionGroupList*.
6. Next, find the node *mrasUri* in this XML string.

If *mrasUri* is not found, there might be a problem with the global or pool settings, and these settings will have to be verified before you continue troubleshooting *mrasUri*.

Verify Global and Pool Settings

To verify global settings, do the following:

1. Open Office Communications Server 2007 R2 Management Console.
2. Right-click the forest node, and then select **Global Properties**.
3. Click the **Edge Servers** tab (Figure D-2).

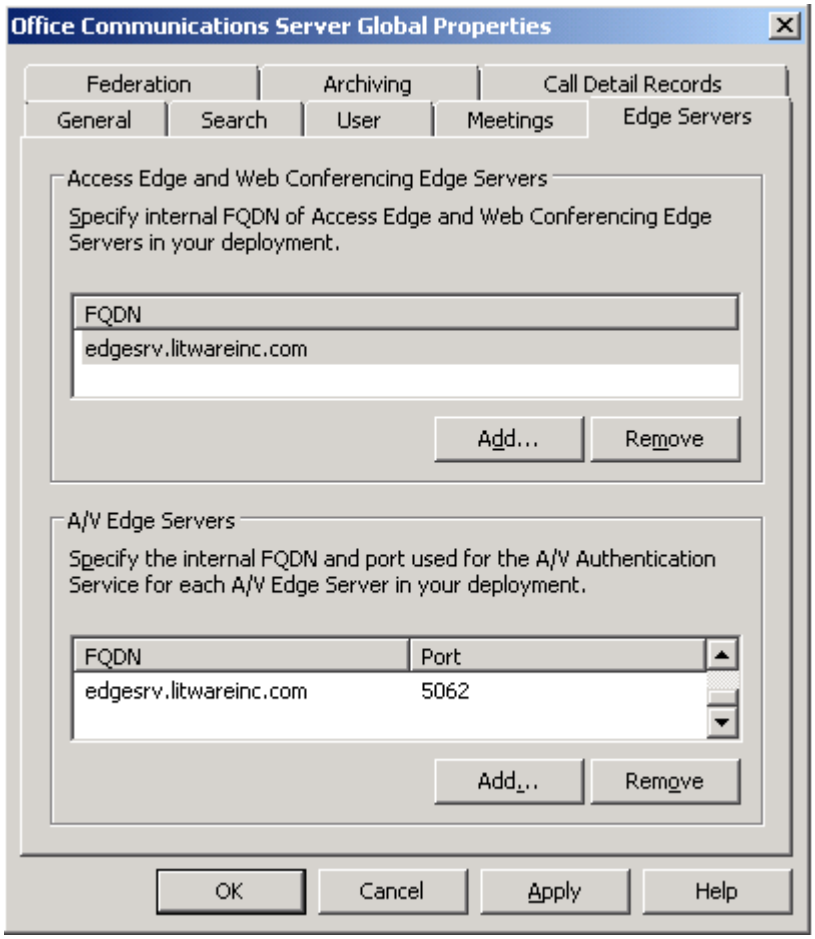

Figure D-2 Global properties

4. Verify that the Audio/Video Edge Server is in the **A/V Edge Servers** list. If it is not in the list, click **Add** and it to the list.

To verify pool settings, do the following:

1. For every Enterprise pool and Standard Edition Server, right-click the pool node, and then select **Pool Properties** (Figure D-3).

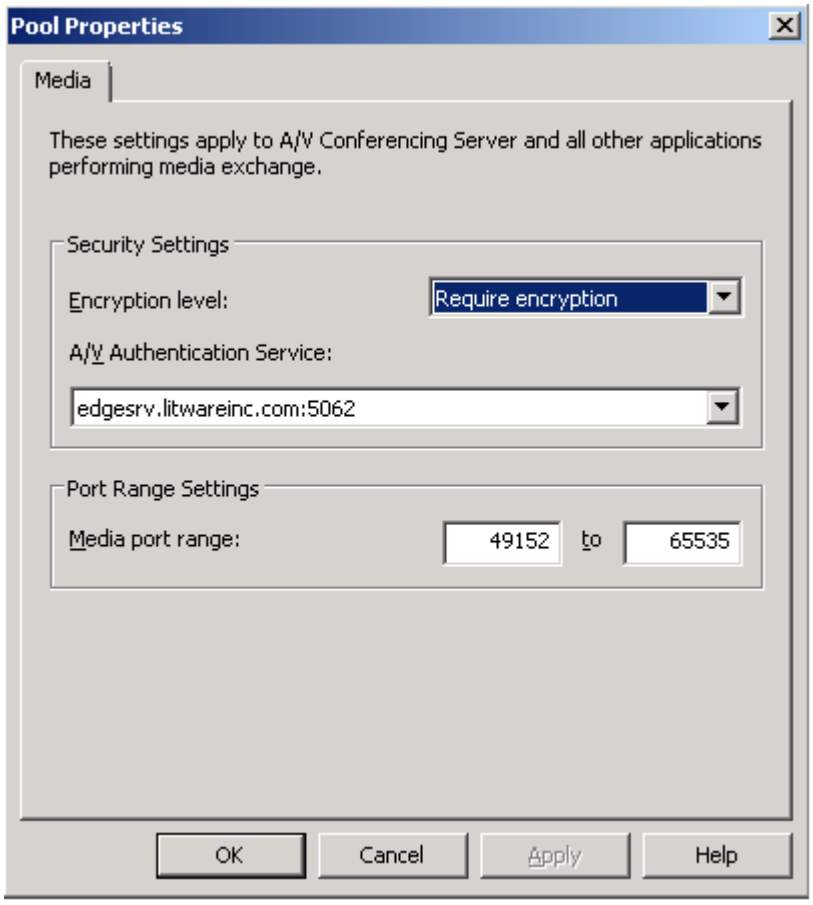

Figure D-3 Pool properties

2. Verify that the Audio/Video Edge Server is selected in the **A/V Authentication Service** list. Select the Audio/Video Edge Server in the A/V Authentication Service list.

If *mrasUri* is found, you can continue troubleshooting by doing the following:

1. Locate the MRAS request by searching for the tag *Sending Packet* followed by the SERVICE SIP message. This also contains an XML body with a root node called, *request*, and the sub-node called, *credentialsRequest*, which is important to record.

```
11/21/2008|23:31:11.162 190:4FC INFO  :: Sending Packet - 192.168.1.5:5061 (From
Local Address: 192.168.1.10:1259) 1292 bytes:


11/21/2008|23:31:11.162 190:4FC INFO  :: SERVICE
sip:edgesrv.litwareinc.com@litwareinc.com;gruu;opaque=srvr:MRAS:P2nY_WtqnEGPHhBbcYD8
VQAA SIP/2.0
```

```
Via: SIP/2.0/TLS 192.168.1.10:1259
Max-Forwards: 70
From: <sip:bart@litwareinc.com>;tag=a12b482214;epid=3c465b617a
To:
<sip:edgesrv.litwareinc.com@litwareinc.com;gruu;opaque=srvr:MRAS:P2nY_WtqnEGPHhBbcYD
8VQAA>
Call-ID: 54b45caa1e33428abe89238d8b8ddd80
CSeq: 1 SERVICE
Contact: <sip:bart@litwareinc.com;opaque=user:epid:cYUGvoWWcl6mKX37xhEMuAAA;gruu>
User-Agent: UCCAPI/3.5.6874.0 OC/3.5.6874.0 (Microsoft Office Communicator 2007 R2
(RC))
Proxy-Authorization: NTLM qop="auth", realm="SIP Communications Service",
opaque="EB6E1210", targetname="OCS-FE.litwareinc.com", crand="0674576e", cnum="7",
response="010000000000000015bb4719f1377568"
Content-Type: application/msrtc-media-relay-auth+xml
Content-Length: 460
<request requestID="31344152" version="2.0"
to="sip:edgesrv.litwareinc.com@litwareinc.com;gruu;opaque=srvr:MRAS:P2nY_WtqnEGPHhBb
cYD8VQAA" from="sip:bart@litwareinc.com"
xmlns="http://schemas.microsoft.com/2006/09/sip/mrasp"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><credentialsRequest
credentialsRequestID="31344152"><identity>sip:bart@litwareinc.com</identity><locatio
n>internet</location><duration>480</duration></credentialsRequest></request>
11/21/2008|23:31:11.162 190:4FC INFO  :: End of Sending Packet - 192.168.1.5:5061
(From Local Address: 192.168.1.10:1259) 1292 bytes
```

2. As you did earlier in this procedure, record the *Call-ID* string that is a few lines below the *SERVICE SIP* message.
3. Use the *Call-ID* to search the corresponding *200 OK* SIP message, if any.

If the *200 OK* SIP message is not found, it means the A/V Authentication Service could not be reached and the configuration of the internal interface of Audio/Video Edge Server should be checked.

Verify Audio/Video Edge Server Internal Interface Configuration

To verify the internal interface configuration for the Audio/Video Edge Servers, you will have to do the following on every Audio/Video Edge Server in your environment:

1. Ensure that the Office Communications Server 2007 R2 Admin Tools are installed on the server.
2. Open Computer Management Console.
3. Expand the **Services and Applications** node.
4. Right-click **Office Communications Server 2007 R2**, and then click **Properties**.

5. Click the **Internal** tab (Figure D-4).

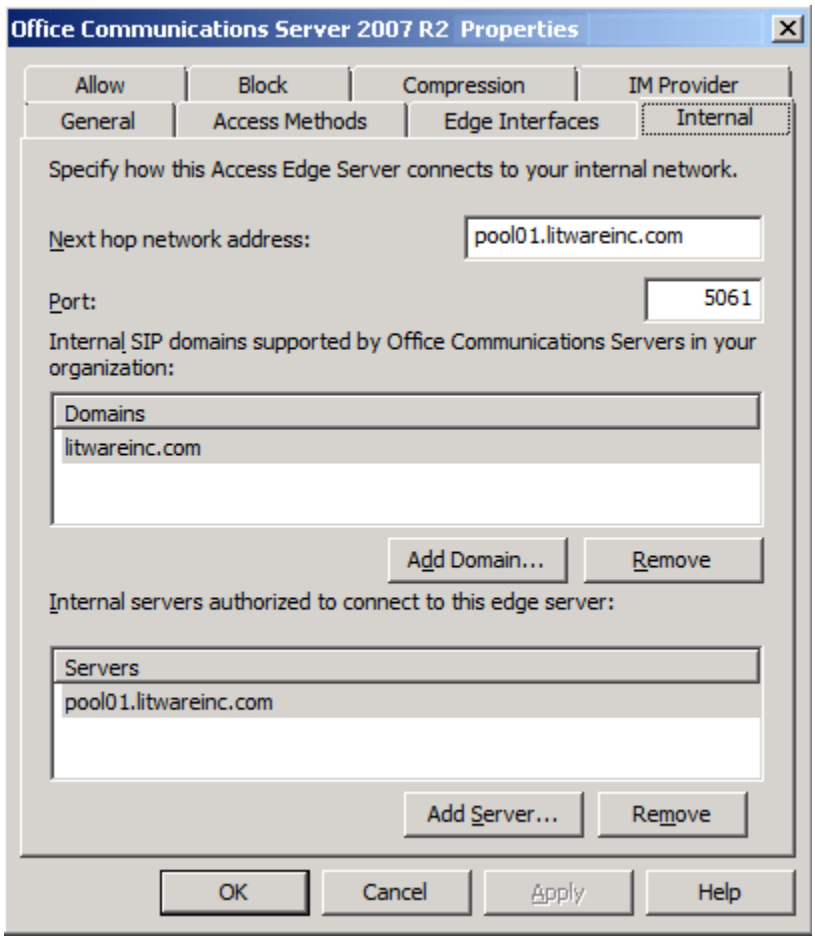

Figure D-4 Internal tab on the Office Communications Server 2007 R2 Properties dialog box

6. Verify the following:

- Each SIP domain that is in your Office Communications Server environment appears in the **Internal SIP domains supported by Office Communications Server in your organization** list. If there are any domains missing, click **Add Domain** to add them.
- Each Enterprise pool and Standard edition server that is part of your Office Communications Server environment appears in the **Internal servers authorized to connect to this edge server** list. If there are any servers missing, click **Add**

Server. If using a Director, add the FQDN of the Director; otherwise, type the FQDN of each Enterprise pool and Standard Edition server in your organization.

7. Click the **Edge Interfaces** tab (Figure D-5).

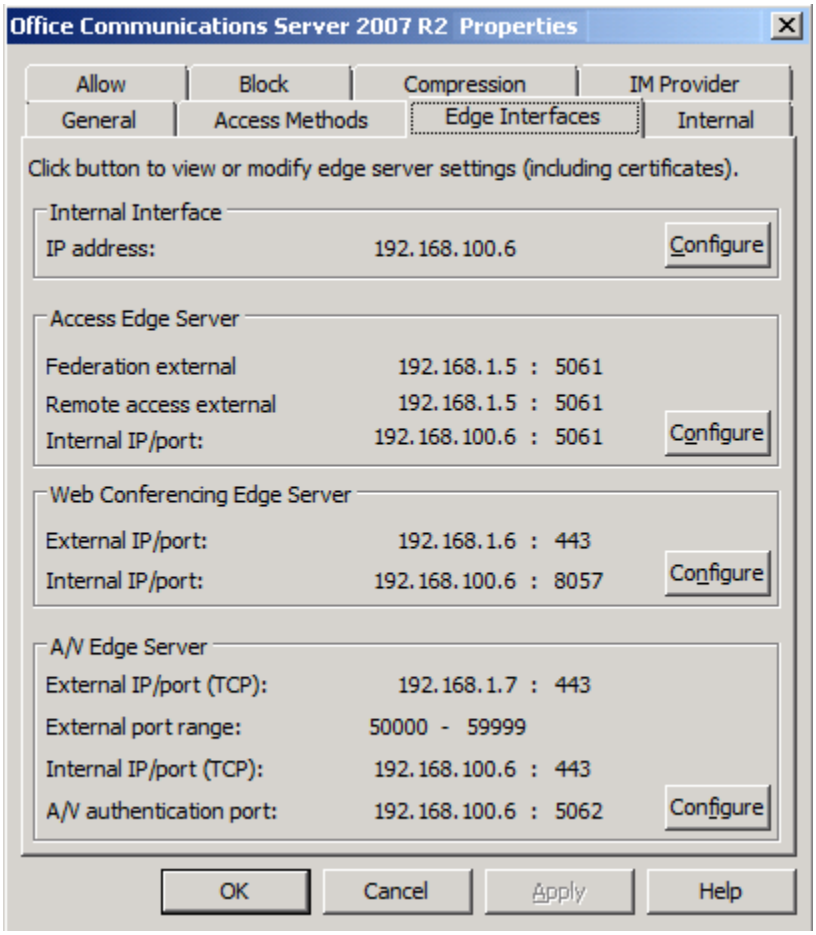

Figure D-5 Edge Interfaces tab on the Office Communications Server 2007 R2 Properties dialog box

8. In the **Internal Interface** section, click **Configure**.

9. Verify the following settings:

- The proper certificate is selected. The subject name (SN) of the certificate must match the FQDN of the internal interface. If a hardware load balancer is used, the SN must match the FQDN corresponding to the virtual IP (VIP) of the hardware load balancer.

- Ensure the Enhanced Key Usage (EKU) for the certificate is present and the intended purpose is Server Authentication.
- The certificate chain of the CA that issued the certificate for the internal interface is installed on your Audio/Video Edge Server. If necessary, download and install the CA certificate chain for the internal interface.
- The root certificate of the CA that issued the certificate for the internal interface is on the list of trusted root CAs. If necessary, add the root certificate to the list of trusted root CAs.

Note For more information about certificates, see Chapter 4.

If the *200 OK* SIP message is found it should contain in its body an XML string that has the root node called, *response,* and a sub-node called, *credentialsResponse,* as shown in the following log file sample.

```
11/21/2008|23:31:11.428 190:4FC INFO  :: Data Received - 192.168.1.5:5061 (To Local
Address: 192.168.1.10:1259) 1769 bytes:


11/21/2008|23:31:11.428 190:4FC INFO  :: SIP/2.0 200 OK
ms-user-logon-data: RemoteUser
Via: SIP/2.0/TLS 192.168.1.10:1259;ms-received-port=1259;ms-received-cid=C00
Authentication-Info: NTLM rspauth="01000000636F6D0027C74476F1377568",
srand="807B1E03", snum="8", opaque="EB6E1210", qop="auth", targetname="OCS-
FE.litwareinc.com", realm="SIP Communications Service"
FROM: "Bart Duncan"<sip:bart@litwareinc.com>;tag=a12b482214;epid=3c465b617a
TO:
<sip:edgesrv.litwareinc.com@litwareinc.com;gruu;opaque=srvr:MRAS:P2nY_WtqnEGPHhBbcYD
8VQAA>;tag=e1fef8fa0
CSEQ: 1 SERVICE
CALL-ID: 54b45caa1e33428abe89238d8b8ddd80
CONTENT-LENGTH: 956
CONTENT-TYPE: application/msrtc-media-relay-auth+xml
SERVER: RTCC/3.5.0.0 MRAS/2.0
ms-edge-proxy-message-trust: ms-source-type=EdgeProxyGenerated;ms-ep-
fqdn=edgesrv.litwareinc.com;ms-source-verified-user=verified
<?xml version="1.0"?>
<response xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" requestID="31344152" version="2.0"
serverVersion="2.0"
to="sip:edgesrv.litwareinc.com@litwareinc.com;gruu;opaque=srvr:MRAS:P2nY_WtqnEGPHhBb
cYD8VQAA" from="sip:bart@litwareinc.com" reasonPhrase="OK"
xmlns="http://schemas.microsoft.com/2006/09/sip/mrasp">
  <credentialsResponse credentialsRequestID="31344152">
    <credentials>

<username>AgAAJPctcgsByUyufn7q4YrV9tVY9EdbrUyIexcz3eMAAAAASV+M/CxEBxJ/lw9WZiktcVEUa/
E=</username>
```

```
      <password>/VA3PEf0jF+Bz9QbU0EwrJWGTOI=</password>
      <duration>480</duration>
    </credentials>
    <mediaRelayList>
      <mediaRelay>
        <location>internet</location>
        <hostName>avedge.litwareinc.com</hostName>
        <udpPort>3478</udpPort>
        <tcpPort>443</tcpPort>
      </mediaRelay>
    </mediaRelayList>
  </credentialsResponse>
</response>


11/21/2008|23:31:11.428 190:4FC INFO  :: End of Data Received - 192.168.1.5:5061 (To
Local Address: 192.168.1.10:1259) 1769 bytes
```

Next, search for the actual call, which is initiated by the SIP message *INVITE*. Again, look for the tag *Sending Packet* and *INVITE* on the next line, but make sure the content that follows several lines below contains a line *m=audio*. This is the SDP offer, which also contains the candidates (*a=candidate* lines).

```
11/21/2008|23:35:11.691 2808:36EC INFO  :: Sending Packet - 192.168.1.5:5061 (From
Local Address: 192.168.1.10:44511) 5168 bytes:


11/21/2008|23:35:11.691 2808:36EC INFO  :: INVITE sip:jeremy@litwareinc.com SIP/2.0
Via: SIP/2.0/TLS 192.168.1.10:44511
Max-Forwards: 70
From: <sip:bart@litwareinc.com>;tag=2038f73c52;epid=b9ca774f83
To: <sip:jeremy@litwareinc.com>
Call-ID: e41f3fa11696494d90130b78761b202c
CSeq: 1 INVITE
Contact: <sip:bart@litwareinc.com;opaque=user:epid:cYUGvoWWcl6mKX37xhEMuAAA;gruu>
User-Agent: UCCAPI/3.5.6874.0 OC/3.5.6874.0 (Microsoft Office Communicator 2007 R2
(RC))
Ms-Conversation-ID: AclM+ZBufwp5XteZTK+XrhF5f/WE8A==
Supported: timer
Supported: histinfo
Supported: ms-safe-transfer
Supported: ms-sender
Supported: ms-early-media
Supported: Replaces
Supported: 100rel
ms-keep-alive: UAC;hop-hop=yes
Allow: INVITE, BYE, ACK, CANCEL, INFO, UPDATE, REFER, NOTIFY, BENOTIFY, OPTIONS
P-Preferred-Identity: <sip:bart@litwareinc.com>
Supported: ms-conf-invite
Proxy-Authorization: NTLM qop="auth", realm="SIP Communications Service",
opaque="9A2F8732", targetname="OCS-FE.litwareinc.com", crand="9eb79f5f", cnum="14",
response="010000006500670040072c8ab197eec75"
Content-Type: multipart/alternative;boundary="----
```

```
=_NextPart_000_0003_01C94CB6.82AAA4B0"
Content-Length: 4028
------=_NextPart_000_0003_01C94CB6.82AAA4B0
Content-Type: application/sdp
Content-Transfer-Encoding: 7bit
Content-Disposition: session; handling=optional; ms-proxy-2007fallback



v=0
o=- 0 0 IN IP4 192.168.1.7
s=session
c=IN IP4 192.168.1.7
b=CT:99980
t=0 0
m=audio 52545 RTP/AVP 114 111 112 115 116 4 8 0 97 13 118 101
k=base64:lZB99ZQKU8xXLim+eEyrypB8wyr9BfnRErbcExJ8cc9grfIzrr6cUOJor2Zr
a=candidate:UOBdojwDkC1fPKrOEjaKI+g2VKcU8xLZDCOYmZdrsNk 1 1aZ9EbjsP8LMhi6fxLVJVQ UDP
0.830 192.168.1.10 50000
a=candidate:UOBdojwDkC1fPKrOEjaKI+g2VKcU8xLZDCOYmZdrsNk 2 1aZ9EbjsP8LMhi6fxLVJVQ UDP
0.830 192.168.1.10 50014
a=candidate:JQc3UONarZ7lwyGXr//s7EmOnl6F6Z8OuMeNZ4qDU5E 1 F/UCIT9x+77pF8zQ8mtg5g TCP
0.190 192.168.1.7 50746
a=candidate:JQc3UONarZ7lwyGXr//s7EmOnl6F6Z8OuMeNZ4qDU5E 2 F/UCIT9x+77pF8zQ8mtg5g TCP
0.190 192.168.1.7 50746
a=candidate:elRO2SdL1Y2t63HSfeFuulLk6WjcDzcz4aV8VWg2Hlw 1 OVOOAdm3Py63sPHZvIzrBQ UDP
0.490 192.168.1.7 52545
a=candidate:elRO2SdL1Y2t63HSfeFuulLk6WjcDzcz4aV8VWg2Hlw 2 OVOOAdm3Py63sPHZvIzrBQ UDP
0.490 192.168.1.7 53966
a=candidate:xpXdFAepostqQMh2UnShBb+FbkbOREQaSuCLinwQYfc 1 Qspv7+/H8O6wVmZj26rRNQ TCP
0.250 192.168.1.10 50010
a=candidate:xpXdFAepostqQMh2UnShBb+FbkbOREQaSuCLinwQYfc 2 Qspv7+/H8O6wVmZj26rRNQ TCP
0.250 192.168.1.10 50010
```

If none of the *a=candidate* lines contain the IP address of the external interface of the Audio/Video Edge Server, it means a media session could not be established with the Audio/Video Edge Server and the configuration of the external interface of the Audio/Video Edge Server should be checked along with the NAT and firewall configuration.

Verify Audio/Video Edge Server External Interface Configuration

To verify the external interface configuration on every Audio/Video Edge Server in your environment, do the following:

1. Ensure that the Office Communications Server 2007 R2 Admin Tools are installed on the server.
2. Open Computer Management Console.

3. Expand the **Services and Applications** node.
4. Right-click **Office Communications Server 2007 R2**, and then click **Properties**.
5. Click the **Edge Interfaces** tab.
6. In the **A/V Edge Server** section, click **Configure** to open the A/V Edge Server dialog box (Figure D-6).

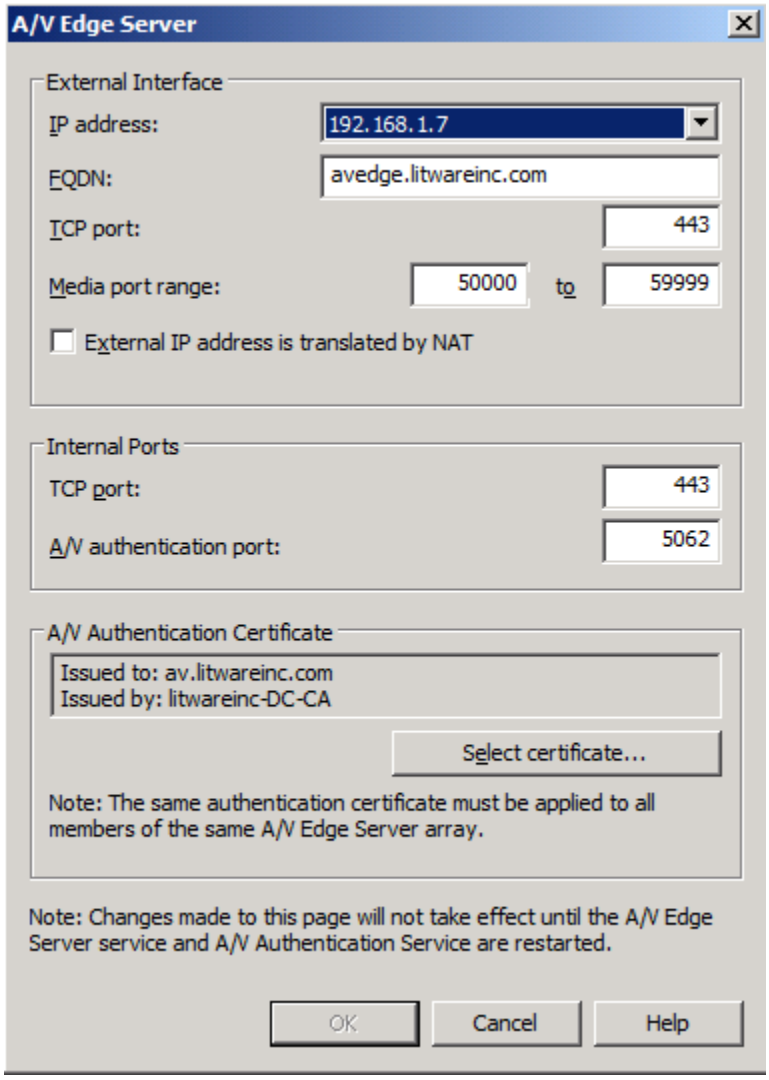

Figure D-6 A/V Edge Server dialog box

7. Verify the following settings:

- Check the A/V Authentication Certificate has a private key. If not, use a certificate that has a private key.
- If hardware load balancers are used on the external and internal edges, ensure that all the Audio/Video Edge Servers use the same TCP and UDP port values for the external interface. This also applies to the internal edge. Also, the same A/V Authentication Certificate must be used on all Audio/Video Edge Servers.
- Check the TCP and UDP port values for the external interface are configured with the default values. If not, change the TCP port to 443 and the UDP port to 3478 (the UDP port can be changed by using WMI). To allow federated calls between users in different organizations, keep the TCP port as 443 and UDP port as 3478 for the external interface.
- If the external IP address is translated by NAT, verify that the **External IP address is translated by NAT** check box is selected.
- Check the IP address for the external interface is publicly routable. If the **External IP address is translated by NAT** check box is not selected, the IP address for the external interface must be publicly routable. If the check box is selected, the NAT-ed IP address must be publicly routable.
- If the external IP address is translated by NAT, ensure that the external FQDN can be resolved from the Audio/Video Edge Server. Use the *ping* or *nslookup* commands to verify this. You can either add a DNS entry or modify the local hosts file to map the FQDN to the NAT-ed address.

Verify Network Address Translation (NAT) Settings

To ensure that your NAT settings are configured correctly, verify the following:

- You are not using a hardware load balancer with NAT. NAT in conjunction with a load balancer is not a supported deployment.
- The internal IP address of the Audio/Video Edge Server is not translated by NAT. NAT on the internal edge is not a supported deployment.
- Ports are mapped straight through by the NAT. Ensure there is a one-to-one port mapping with the Audio/Video Edge Server ports.

Verify Firewall Settings

Verify the following settings on your firewalls:

- The internal firewall allows the necessary inbound and outbound traffic. The internal firewall must allow the following Audio/Video Edge Server traffic:
    - Outbound on UDP port 3478 for TURN/STUN/UDP
    - Outbound only on TCP port 443 for TURN/STUN/TCP
    - Outbound only on TCP port 5062 for SIP/TLS
- The external firewall allows the necessary inbound/outbound traffic. The external firewall must allow the following Audio/Video Edge Server traffic:
    - Inbound/outbound on UDP port 3478 for TURN/STUN/UDP
    - Inbound only on TCP port 443 for TURN/STUN/TCP
- If federated calls are made to users who belong to different organizations and there are Audio/Video Edge Servers in the communication path that are not running Office Communications Server 2007 R2, verify the following:
    - UDP media ports must be open in the external firewall for inbound and outbound traffic. The external firewall must allow inbound and outbound traffic on UDP media ports range 50000-59999 for STUN/RTP. To configure a different range, follow the steps outlined in *Verify Audio/Video Edge Server External Interface Configuration* section earlier in this document to display the A/V Edge Server dialog.
    - TCP media ports must be open in the external firewall for outbound traffic. The external firewall must allow outbound traffic on UDP media ports range 50000-59999 for STUN/RTP. To configure a different range, follow the steps outlined in *Verify Audio/Video Edge Server External Interface Configuration* section earlier in this document to display the A/V Edge Server dialog.
- If federated Desktop Sharing is used with users who belong to different organizations and all Audio/Video Edge Servers in the communication path are running Office Communications Server 2007 R2, verify the following:
    - TCP media ports must be open in the external firewall for outbound traffic. The external firewall must allow outbound traffic on TCP media ports range 50000-59999 for STUN/RTP. To configure a different range, follow the steps outlined in the "Verify Audio/Video Edge Server External Interface Configuration" section earlier in this document to display the A/V Edge Server dialog.
- If you are using Windows Server 2008 Firewall, ensure that the firewall exception rules described earlier in this section are defined for the program *System* by doing the following:

1. Open the **Properties** dialog box for the exception rule that you want to change.
2. Click the **Programs and Services** tab.
3. Select the **This program** option, and then type *System* in the box underneath (Figure D-7).

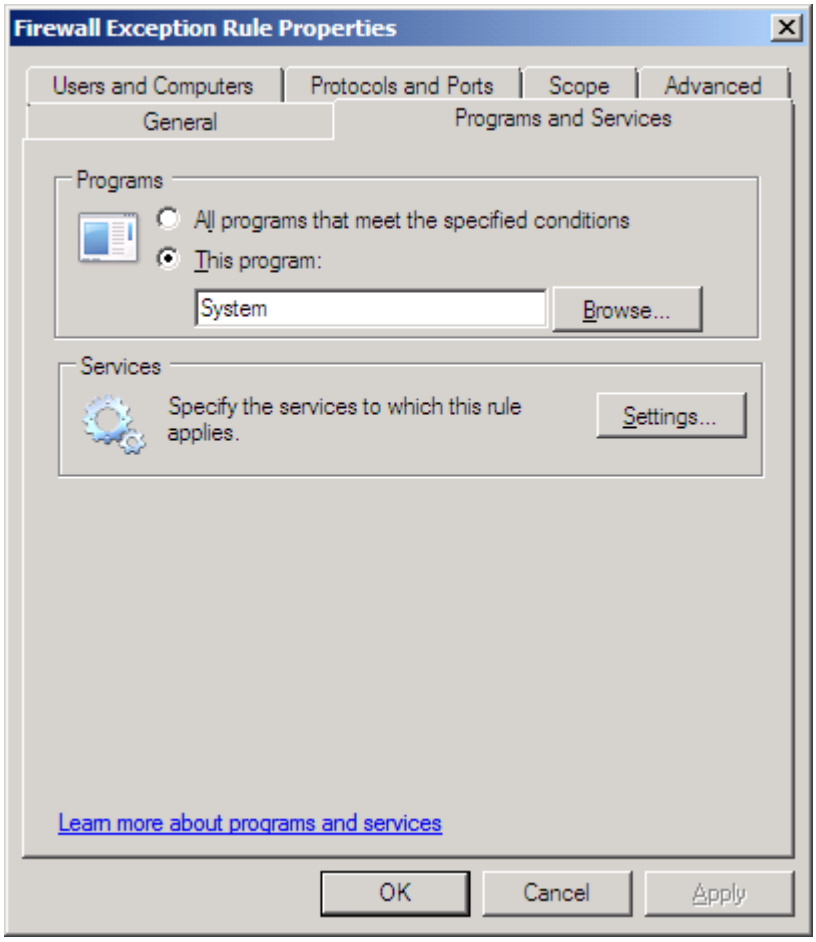

Figure D-7 Firewall Exception Rule Properties

Note For more information about firewall rules, see Chapter 4.

If the Audio Edge Server is behind a NAT and there are candidates in the *a=candidate* lines that contain the private IP address of the external interface instead of the NAT-ed IP address, it is because the **External IP address is translated by NAT** checkbox is not selected in the **A/V Edge Server** dialog box (Figure D-6).

Next Steps

If none of the troubleshooting steps explained so far in this document have solved the issue, more advanced debugging is needed. First, start a debugging session on the Audio/Video Edge Server to collect logs by doing the following:

1. Ensure that the Office Communications Server 2007 R2 Admin Tools are installed on the server.
2. Open Computer Management Console.
3. Expand the **Services and Applications** node.
4. Right-click **Office Communications Server 2007 R2**, select **Logging Tool**, and then click **New Debugging Session**.
5. In the Office Communications Server 2007 R2 Logging Tool, select the checkboxes for **MRAS**, **S4**, and **SIPStack**.
6. Ensure that for each component the **All** option is selected under **Level** and the **All Flags** check box is selected under **Flags** (Figure D-8).
7. Click **Start Logging**.
8. Restart external Office Communicator, and then stop the logging in the Office Communications Server 2007 R2 Logging Tool. View the logs by clicking **View Log Files** and look for errors that will help you further troubleshoot the issue.

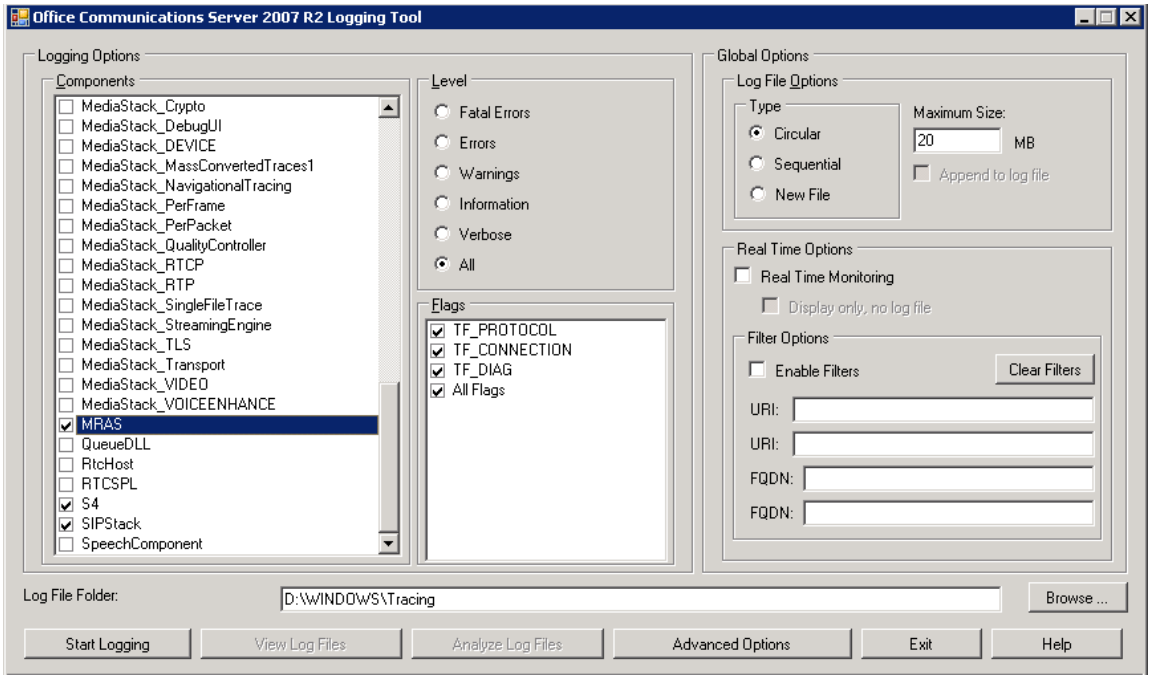

Figure D-8 Office Communications Server 2007 R2 Logging Tool

Another debugging method is to collect Netmon captures on all hops between the external user and Audio/Video Edge Server and make sure that the packets reach the Audio/Video Edge Server. STUN and RTP traffic should be monitored.

—Radu Constantinescu
Senior Lead Software Development Engineer in Test, Office Communications Server