Application Notes for Configuring Sagem-Interstar XMediusFAX SP Edition with Avaya Aura™ Communication Manager and Avaya Aura™ SIP Enablement Services via SIP Trunking Interface - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring the Sagem-Interstar XMediusFAX SP Edition with Avaya Aura™ Communication Manager and Avaya Aura™ SIP Enablement Services (SES) using a SIP trunk.

XMediusFAX is a software based fax server that sends and receives fax calls over an IP network. In the tested configuration, XMediusFAX interoperates with the Avaya Aura™ Communication Manager and the Avaya Aura™ SIP Enablement Services to send/receive faxes using SIP trunks and T.38 fax protocol between XMediusFAX and the Avaya SIP infrastructure.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the procedures for configuring the Sagem-Interstar XMediusFAX Service Provider (SP) Edition with Avaya Aura™ Communication Manager and Avaya Aura™ SIP Enablement Services (SES) using SIP trunks.

XMediusFAX is a software based fax server that sends and receives fax calls over an IP network. In the tested configuration, XMediusFAX interoperates with the Communication Manager and the SIP Enablement Services to send/receive faxes using SIP trunks and T.38 protocol between XMediusFAX and the Avaya SIP infrastructure.

1.1. Interoperability Compliance Testing

The compliance test tested interoperability between XMediusFAX and the Communication Manager and the SIP Enablement Services by making intra-site and inter-site fax calls to and from XMediusFAX. The XMediusFAX server connects (at each of the two sites in the test configuration) to the Communication Manager and the SIP Enablement Services via SIP trunks (see **Section 2** for detailed configuration). Specifically, the following fax operations were tested in the setup for the compliance test:

- Fax from/to XMediusFAX to/from fax machine at local site
- Fax from/to XMediusFAX to/from fax machine at remote site
- Fax from/to XMediusFAX to/from XMediusFAX server at remote site

In the compliance test, Site A and Site B were connected by both ISDN-PRI trunks and SIP trunks. The inter-site calls were tested by using either of these 2 types of trunks between sites.

Faxes were sent with various page lengths, resolutions and at various fax data speeds. For capacity, a large number of 2-page faxes were continuously sent between the two XMediusFAX servers across sites. Serviceability testing included verifying proper operation/recovery from failed cables, unavailable resources, restarts of the Communication Manager and the SIP Enablement Services as well as XMediusFAX reboots. Fax calls were also tested with different Avaya Media Gateway media resources to process the fax data. This included the TN2302AP IP Media Processor (MedPro) circuit pack and the TN2602AP IP Media Processor circuit pack in the Avaya G650 Media Gateway, as well as the integrated Voice over Internet Protocol (VoIP) engine of the Avaya G350 Media Gateway.

1.2. Support

For technical support on XMediusFAX, contact Sagem-Interstar at:

- Phone: (888) 766-1668
- Email: support@sagem-interstar.com

2. Configuration

Figure 1 illustrates the configuration used in these Application Notes. In the sample configuration, two sites are connected via direct SIP trunks and ISDN-PRI trunks. Faxes can be sent between the two sites using either of these two trunk groups.

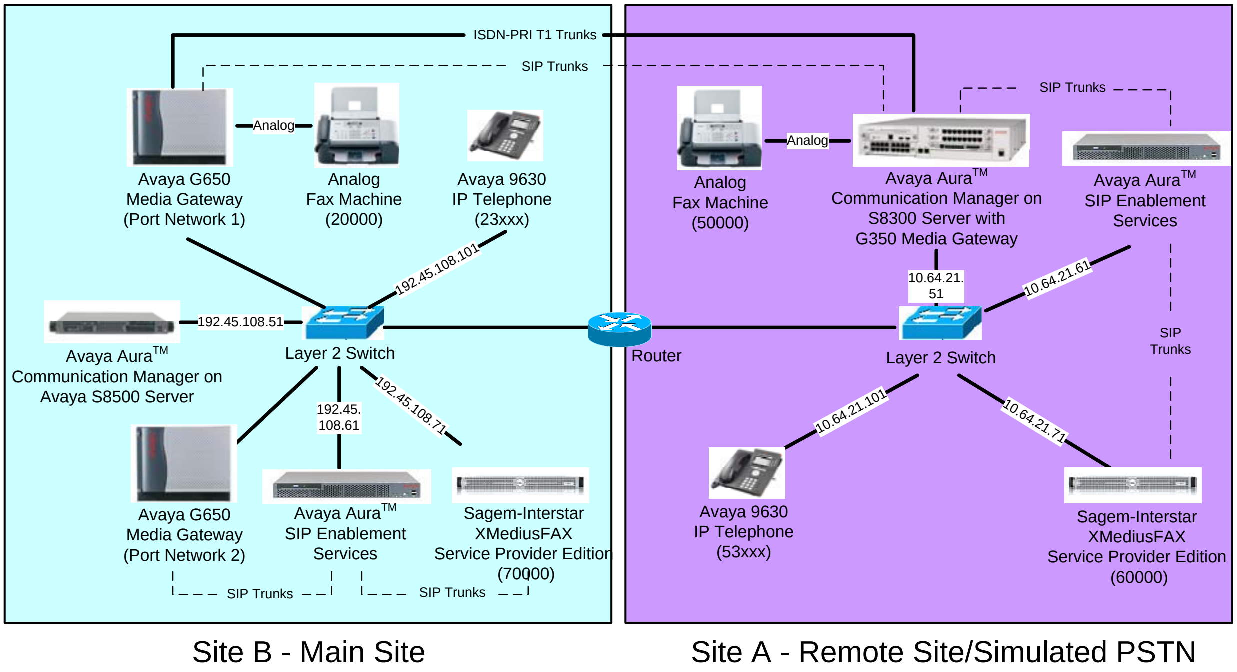


Figure 1: XMediusFAX interoperating with Communication Manager and SIP Enablement Services

Located at Site B is a SIP Enablement Services server and an Avaya S8500 Server running Communication Manager with two Avaya G650 Media Gateways. Each media gateway is configured as a separate port network in separate IP network regions. XMediusFAX at this site is running on a Windows 2003 Server and communicates to the Avaya SIP infrastructure (Communication Manager and SIP Enablement Services) via SIP trunks whose signaling is terminated on a CLAN circuit pack in port network 2. The media resources required by the trunk are provided by the IP Media Processor (MedPro) circuit pack. Two versions of the IP MedPro circuit pack were tested in this configuration: TN2302AP and TN2602AP. Endpoints at this site include Avaya 9600 Series IP Telephones (with SIP and H.323 firmware) and an analog fax machine.

Located at Site A is an SIP Enablement Services server and an Avaya S8300 Server running Communication Manager in an Avaya G350 Media Gateway. XMediusFAX at this site is also running on a Windows 2003 Server and communicates to the Avaya SIP infrastructure (Communication Manager and SIP Enablement Services) via SIP trunks. On the Avaya G350 Media Gateway, the signaling and media resources needed to support SIP trunks are integrated directly on the media gateway processor. Endpoints at this site include an Avaya 1600 Series IP Telephone (with H.323 firmware), Avaya 9600 Series IP Telephones (with H.323 firmware and SIP firmware), and an analog fax machine.

Although the IP telephones are not involved in the faxing operations, they are present in the configuration to verify that VoIP telephone calls are not affected by the FoIP faxing operations and vice versa.

Outbound fax calls originating from XMediusFAX are sent to the SIP Enablement Services server first, then from the SIP Enablement Services to the Communication Manager, via the configured SIP trunks. Based on the dialed digits, the Communication Manager will direct the calls to the local fax machine, or the inter-site trunks (ISDN-PRI or SIP) to reach the remote site. Inbound fax calls terminating to XMediusFAX from the local fax machine or from the remote site are first received by the Communication Manager. The Communication Manager then directs the calls to XMediusFAX via the configured SIP trunks.

3. Equipment and Software Validated

The following equipment and software/firmware were used for the sample configuration provided:

Equipment	Software/Firmware
Avaya S8500 Server running Avaya Aura™ Communication Manager (Site B)	R5.2.1 SP1 (R015x.02.1.016.4-17959)
Avaya G650 Media Gateway (Site B) - 2 CLANs - 2 IP MedPros – TN2302AP - 2 IP MedPros – TN2602AP	TN799DP - HW01 FW24 TN2302AP - HW20 FW120 TN2602AP - HW02 FW051
Avaya Aura™ SIP Enablement Services (Site B)	5.2.1.016.4
Avaya S8300 Server running Avaya Aura™ Communication Manager (Site A)	R5.2.1 SP1 (R015x.02.1.016.4-17959)
Avaya G350 Media Gateway (Site A)	30.10.4
Avaya Aura™ SIP Enablement Services (Site A)	5.2.1.016.4
Avaya 1608 IP Telephone (H.323)	1.100
Avaya 9620 IP Telephone (SIP) Avaya 9630 IP Telephone (SIP) Avaya 9630 IP Telephone (H.323)	2.2 2.2 & 2.0 3.0
Analog Fax Machines	-
Sagem-Interstar XMediusFAX SP Edition Fax Server running on Windows 2003 Server	6.5 with patch XMFSP_6.5.0.127

4. Configure Avaya Aura™ Communication Manager

This section describes the Communication Manager configuration necessary to interoperate with XMediusFAX. It focuses on the configuration of the SIP trunks connecting XMediusFAX to the Avaya SIP infrastructure with the following assumptions:

- Procedures necessary to support SIP and connectivity to Avaya SES have been performed as described in [3], including all SIP phones at each site.
- All other components are assumed to be in place and previously configured, including the SIP and ISDN-PRI trunk groups that connect both sites.

The procedures for configuring Communication Manager include the following areas:

- Verify Communication Manager license (Step 1)
- Identify IP Interfaces (Step 2)
- Administer IP network regions (Steps 3 – 6)
- Administer IP codec set (Steps 7 – 8)
- Administer SIP signaling group (Step 9)
- Administer SIP trunk group (Steps 10 – 11)
- Administer public unknown numbering (Step 12)
- Administer route pattern (Step 13)
- Administer AAR analysis (Steps 14 – 15)
- Turn on Media Shuffling on cross-site SIP trunks (Step 16)

The configuration of the Communication Manager was performed using the System Access Terminal (SAT). After the completion of the configuration, perform a **save translation** command to make the changes permanent.

The examples shown in this section refer to Site B. Unless specified otherwise, these same steps also apply to Site A using values appropriate for Site A from **Figure 1**.

Step	Description
1.	**Communication Manager License** Use the **display system-parameters customer-options** command to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Navigate to **Page 2**, and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column. The license file installed on the system controls the maximum permitted. If there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.

```
change system-parameters customer-options                       Page   2 of  11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                             USED
                     Maximum Administered H.323 Trunks: 800   100
           Maximum Concurrently Registered IP Stations: 18000 1
             Maximum Administered Remote Office Trunks: 0     0
Maximum Concurrently Registered Remote Office Stations: 0     0
              Maximum Concurrently Registered IP eCons: 0     0
  Max Concur Registered Unauthenticated H.323 Stations: 0     0
                Maximum Video Capable H.323 Stations: 0     0
                 Maximum Video Capable IP Softphones: 0     0
                       Maximum Administered SIP Trunks: 800   232
  Maximum Administered Ad-hoc Video Conferencing Ports: 0     0
   Maximum Number of DS1 Boards with Echo Cancellation: 0     0
                             Maximum TN2501 VAL Boards: 10    1
                     Maximum Media Gateway VAL Sources: 0     0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   2
   Maximum Number of Expanded Meet-me Conference Ports: 0     0
```

Step	Description
2.	**IP Interfaces**

- Use the **list ip-interface all** command to identify which IP interfaces are located in which network region. The example below shows the IP interfaces used in the compliance test. All interfaces in cabinet 01 (port network 1) as indicated in the **Slot** field are in IP network region 1 as indicated in the **Net Rgn** field. These interfaces are highlighted below. Testing with the TN2302AP and TN2602AP circuit packs were done separately. When testing with the TN2302AP, the TN2602AP was disabled (turned off) and vice versa as indicated in the **ON** field. Node Names are defined using the **change node-names ip** command.

```
list ip-interface all                                               Page   1
                                IP INTERFACES

                                                                   Net
ON Type   Slot  Code/Sfx      Node Name/       Mask  Gateway Node     Rgn  VLAN
                              IP-Address
-- ------ ----- --------      ---------------  ----  ---------------  ---  ----
 y MEDPRO 01A02 TN2302        MEDPRO1A         /24   Gateway001       1    n
                              192.45.108.54
 y C-LAN  01A03 TN799  D      CLAN1A           /24   Gateway001       1    n
                              192.45.108.55
 y MEDPRO 02A02 TN2302        MEDPRO2A         /24   Gateway001       2    n
                              192.45.108.56
 y C-LAN  02A03 TN799  D      CLAN2A           /24   Gateway001       2    n
                              192.45.108.57
 n MEDPRO 01A04 TN2602        MEDPRO1A-2       /24   Gateway001       1    n
                              192.45.108.58
 n MEDPRO 02A04 TN2602        MEDPRO2A-2       /24   Gateway001       2    n
                              192.45.108.59
```

- Node Names in the above screen are defined using the **change node-names ip** command.

```
change node-names ip                                         Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
CLAN1A              192.45.108.55
CLAN2A              192.45.108.57
CM-A                10.64.21.41
MEDPRO1A            192.45.108.54
MEDPRO1A-2          192.45.108.58
MEDPRO2A            192.45.108.56
MEDPRO2A-2          192.45.108.59
SES-B               192.45.108.61
```

Step	Description
3.	**IP Network Region – Region 1** The configuration of the IP network regions (**Steps 3 – 6**) is assumed to be already in place and is included here for clarity. At Site B, the Avaya S8500 Server, the Avaya G650 Media Gateway comprising port network 1, and all IP endpoints were located in IP network region 1 using the parameters described below. Use the **display ip-network-region** command to view these settings. The example below shows the values used for the compliance test. ▪ The **Authoritative Domain** field was configured to match the domain name configured on Avaya SES. In this configuration, the domain name is ***business.com***. This name appears in the “From” header of SIP messages originating from this IP region. ▪ A descriptive name was entered for the **Name** field. ▪ **IP-IP Direct Audio** (Media Shuffling) was enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. This was done for both intra-region and inter-region IP-IP Direct Audio. This is the default setting. Media Shuffling can be further restricted at the trunk level on the **Signaling Group** form. ▪ The **Codec Set** field was set to the IP codec set to be used for calls within this IP network region. In this case, IP codec set ***1*** was selected. ▪ The default values were used for all other fields. At Site A, all IP components were located in IP network region 1 and the IP network region was configured in the same manner as shown below.

```
display ip-network-region 1                                     Page   1 of
                               IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: business.com
    Name: PN1
MEDIA PARAMETERS              Intra-region IP-IP Direct Audio: yes
      Codec Set: 1            Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                    IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                   RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

Step **Description**

4.

IP Network Region 1 – Continued

On **Page 3**, codec sets are defined for inter-region calls. In the case of the compliance test at Site B, calls from IP network region 1, **Source Region 1**, to IP network region 2, **dst rgn 2**, used **codec set 1.** The default values were used for all other fields. At Site A, only one IP network region exists so no inter-region settings were required.

```
display ip-network-region 1                                     Page   3 of  19

 Source Region: 1     Inter Network Region Connection Management     I       M
                                                                     G  A    e
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    a
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    s
 1    1                                                                 all
 2    1     y    NoLimit                                             n
```

5.

IP Network Region – Region 2

At Site B, IP network region 2 was created for port network 2 in a similar manner as IP network region 1 shown in **Step 3** but with a different name.

```
display ip-network-region 2                                     Page   1 of  19
                               IP NETWORK REGION
  Region: 2
Location:         Authoritative Domain: business.com
    Name: PN2
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

6.

IP Network Region 2 – Continued

The inter-region codec setting was created similarly to **Step 4**.

```
display ip-network-region 2                                     Page   3 of  19

 Source Region: 2     Inter Network Region Connection Management     I       M
                                                                     G  A    e
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    a
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    s
 1    1     y    NoLimit                                             n all
 2    1                                                                 all
```

Step	Description
7.	**Codecs** Use the **change ip-codec-set** command to verify the codec used for the testing. The example below shows that ***G.711MU*** is used in the compliance test.

```
display ip-codec-set 1                                          Page   1 of   2

                          IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n         2        20
```

Step	Description
8.	**Codecs - Continued** On **Page 2**, set the **FAX Mode** field to ***t.38-standard*.** This is necessary to support the XMediusFAX server assigned to IP network region 2. The **Modem Mode** field should be set to ***off***. Leave the **FAX Redundancy** setting at its default value of ***0*.** A packet redundancy level can be assigned to improve packet delivery and robustness of FAX transport over the network (with increased bandwidth as trade-off). Avaya uses IETF RFC-2198 and ITU-T T.38 specifications as redundancy standard. With this standard, each Fax over IP packet is sent with additional (redundant) 0 to 3 previous fax packets based on the redundancy setting. A setting of 0 (no redundancy) is suited for networks where packet loss is not a problem.

```
display ip-codec-set 1                                          Page   2 of   2

                          IP Codec Set

                              Allow Direct-IP Multimedia? n



                    Mode                Redundancy
    FAX             t.38-standard        0
    Modem           off                  0
    TDD/TTY         US                   3
    Clear-channel   n                    0
```

Step	Description
9.	**Signaling Group for Fax Calls** For the compliance test, this signaling group and the associated SIP trunk group are used for routing fax calls to/from the XMediusFAX server. For the compliance test at Site B, signaling group 7 was configured using the parameters highlighted below. All other fields were set as described in [3]. ▪ The **Group Type** was set to ***sip***. ▪ The **Transport Method** was set to ***tcp***. As a result, the **Near-end Listen Port** and **Far-end Listen Port** are automatically set to ***5060.*** ▪ The **Near-end Node Name** was set to ***CLAN2A***, the node name that maps to the IP address of the CLAN circuit pack used to connect to XMediusFAX. Node names are defined using the **change node-names ip** command (see **Step 2** above). ▪ The **Far-end Node Name** was set to ***SES-B***. This node name maps to the IP address of the SIP Enablement Services server as defined using the **change node-names ip** command. ▪ The **Far-end Network Region** was set to ***2***. This is the IP network region which contains XMediusFAX. ▪ The **Far-end Domain** was set to the IP address assigned to XMediusFAX. This domain is sent in the headers of SIP INVITE messages for calls originating from and terminating to the fax server using this signaling group. ▪ **Direct IP-IP Audio Connections** was set to ***y***. This field must be set to ***y*** to enable Media Shuffling on the trunk level (see **Step 3** on **IP-IP Direct Audio**). ▪ The default values were used for all other fields.

```
display signaling-group 7
                                SIGNALING GROUP

 Group Number: 7              Group Type: sip
                        Transport Method: tcp
  IMS Enabled? n





   Near-end Node Name: CLAN2A                Far-end Node Name: SES-B
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 2
Far-end Domain: 192.45.108.100

                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? n                     Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

Step	Description
10.	**Trunk Group for Fax Calls** For the compliance test, trunk group 7 was used for the SIP trunk group for routing fax calls to/from XMediusFAX. Trunk group 7 was configured using the parameters highlighted below. All other fields were set as described in [3]. On **Page 1**: ▪ The **Group Type** field was set to ***sip***. ▪ A descriptive name was entered for the **Group Name**. ▪ An available trunk access code (TAC) that was consistent with the existing dial plan was entered in the **TAC** field. ▪ The **Service Type** field was set to ***tie***. ▪ The **Signaling Group** was set to the signaling group shown in the previous step. ▪ The **Number of Members** field contained the number of trunks in the SIP trunk group. It determines how many simultaneous SIP calls can be supported by the configuration. ▪ The default values were used for all other fields.

```
display trunk-group 7                                           Page   1 of  21
                                TRUNK GROUP

Group Number: 7                    Group Type: sip           CDR Reports: y
  Group Name: FaxServer-SIP               COR: 1        TN: 1        TAC: *007
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                       Signaling Group: 7
                                                     Number of Members: 24
```

Step	Description
11.	**Trunk Group for Fax Calls – continued** On **Page 3**: ▪ Set the **Numbering Format** field to ***public***. This field specifies the format of the calling party number sent to the far-end. ▪ Default values may be used for all other fields.

```
display trunk-group 7                                           Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



                     Numbering Format: public
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n
```

Step	Description
12.	**Public Unknown Numbering** Public unknown numbering defines the calling party number to be sent to the far-end. Use the **change public-unknown-numbering** command to create an entry that will be used by the trunk groups defined in **Steps 10-11**. In the example shown below, all calls originating from a 5-digit extension beginning with 2, 6, or 7 and routed across any trunk group (**Trk Grp** column is blank) will be sent as a 5-digit calling number.

```
display public-unknown-numbering 0                              Page   1 of
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext           Trk       CPN             CPN
Len Code          Grp(s)    Prefix          Len
                                                     Total Administered: 3
 5  2                                      5            Maximum Entries: 9999
 5  6                                      5
 5  7                                      5
```

Step	Description
13.	**Route Pattern** Use the **change route-pattern** command to create a route pattern that will route fax calls to the SIP trunk that connects to the XMediusFAX server. The example below shows the route pattern used for the compliance test at Site B. A descriptive name was entered for the **Pattern Name** field. The **Grp No** field was set to the trunk group created in **Steps 10–11**. The Facility Restriction Level (**FRL**) field was set to a level that allows access to this trunk for all users that require it. The value of ***0*** is the least restrictive level. The default values were used for all other fields.

```
display route-pattern 7                                         Page   1 of   3
                    Pattern Number: 7   Pattern Name: ToFaxServer
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 7    0                                                              n   user
 2:                                                                     n   user
 3:                                                                     n   user
 4:                                                                     n   user
 5:                                                                     n   user
 6:                                                                     n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                                         none
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
```

Step	Description
14.	**Routing Calls to XMediusFAX** Automatic Alternate Routing (AAR) was used to route calls to XMediusFAX. Two places need to be changed to support this routing. At first use the **change dialplan analysis** command to create an entry in the dial plan. The example below shows entries previously created for Site B using the **display dialplan analysis** command. The 5th highlighted entry specifies that numbers that begin with ***7*** are of Call Type ***aar***. Second use the **change aar analysis** command to create an entry in the AAR Digit Analysis Table. The example below shows entries previously created for Site B using the **display aar analysis 0** command. The 4th highlighted entry specifies that numbers that begin with ***7*** and are ***5*** digits long use route pattern ***7.*** Route pattern ***7*** routes calls to the XMediusFAX fax server at Site B.

```
display dialplan analysis                                       Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location:  all          Percent Full:    1

       Dialed   Total  Call    Dialed   Total  Call     Dialed   Total  Call
       String   Length Type    String   Length Type     String   Length Type
     0            3    fac
     2            5    ext
     5            5    ext
     6            5    aar
     7            5    aar
     8            1    fac
     9            1    fac
     *            4    dac
```

```
display aar analysis 0                                          Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location:  all          Percent Full:    1

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    50                    5    5     4        aar          n
    53                    5    5     4        aar          n
    6                     5    5     4        aar          n
    7                     5    5     7        aar          n
```

Step	Description
15.	**Routing Calls From Site B to Site A** The AAR Digit Analysis Table in **Step 14** also shows that a 5-digit dialed number starting with 50 or 6 will use route pattern 4 by AAR. The previously created route pattern ***4*** as displayed below specifies that a call from Site B to the fax machine 50000 or the XMediusFAX server 60000 at Site A will be routed to trunk group 4 which is an administered ISDN-PRI trunk. In the same way, this trunk group can be changed to a SIP trunk group for fax calls from Site B to Site A to go over a SIP trunk.

```
display route-pattern 4                                         Page   1 of   3
                    Pattern Number: 4   Pattern Name: CMnorth RP
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 4    0                                                              n   user
 2:                                                                     n   user
 3:                                                                     n   user
 4:                                                                     n   user
 5:                                                                     n   user
 6:                                                                     n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                                         none
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
 4: y y y y y n  n            rest                                         none
 5: y y y y y n  n            rest                                         none
 6: y y y y y n  n            rest                                         none
```

Step	Description
16.	**Turn On Media Shuffling on SIP Trunk between Sites** Use the **change signaling-group** command to turn on Media Shuffling on the previously administered SIP trunks between Site B and Site A (in this compliance test, trunk group 1 was used at Site B). Note that the **Far-end Node Name** is ***CM-A*** which indicates that the trunk is set up between two Communication Managers directly without going through an SES.

```
change signaling-group 1                                        Page   1 of   1
                                SIGNALING GROUP

 Group Number: 1              Group Type: sip
                        Transport Method: tcp
  IMS Enabled? n





   Near-end Node Name: CLAN1A                Far-end Node Name: CM-A
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 2
Far-end Domain:

                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? n                     Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

5. Configure Avaya Aura™ SIP Enablement Services

This section covers the configuration of the SIP Enablement Services at Site B. The SIP Enablement Services are configured via an Internet browser using the administration web interface. It is assumed that the SIP Enablement Services software and the license file have already been installed on the server. During the software installation, an installation script is run from the Linux shell of the server to specify the IP network properties of the server along with other parameters. In addition, it is assumed that the setup screens of the administration web interface have been used for initial configurations. For additional information on these installation tasks, refer to [4].

Each SIP endpoint used in the compliance test that registers with the SIP Enablement Services requires that a user and media server extension be created in the SIP Enablement Services. This configuration is not directly related to the interoperability between XMediusFAX and the Avaya SIP infrastructure (Communication Manager and SIP Enablement Services), so it is not included here. These procedures are covered in [4].

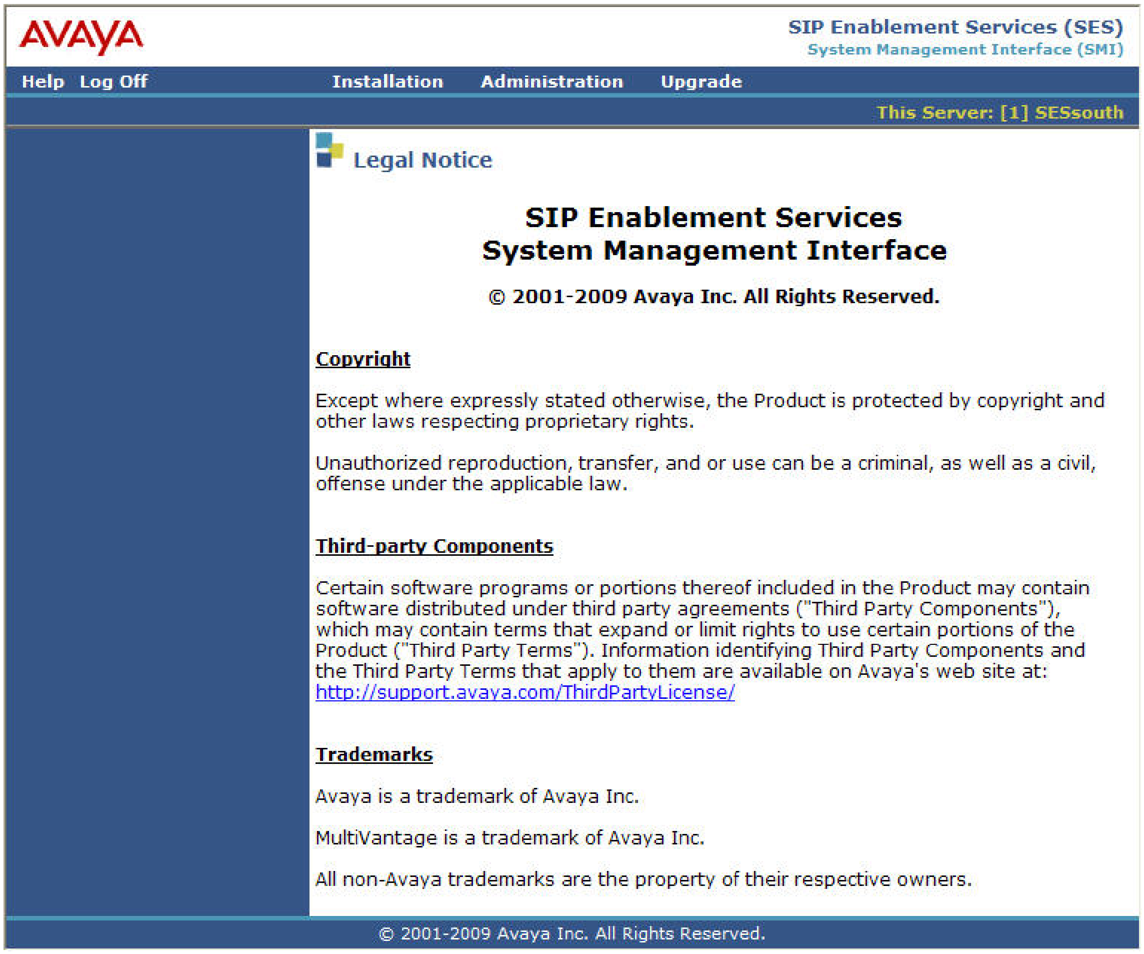
This section is divided into two parts. **Section 5.1** summarizes the user-defined parameters used in the SIP Enablement Services installation procedures that are important for the understanding of the solution as a whole. It does not attempt to show the installation procedures in their entirety. It also describes any deviations from the standard procedures, if any.

Section 5.2 describes configurations beyond those covered in **Section 5.1** that are necessary for interoperating with XMediusFAX.

The documented configurations must be repeated for the SIP Enablement Services at Site A using values appropriate for Site A from **Figure 1**. This includes but is not limited to the IP addresses, SIP domain and user extensions.

5.1. Summarize Initial Configuration Parameters

This section summarizes the applicable user-defined parameters used during the SIP installation procedures.

Step	Description
1.	**Login** Access the Avaya SES administration web interface by entering http://<*ip-addr*>/admin as the URL in an Internet browser, where <*ip-addr*> is the IP address of the Avaya SES server. Log in with the appropriate credentials and the page below will be displayed. 

Legal Notice

SIP Enablement Services
System Management Interface

© 2001-2009 Avaya Inc. All Rights Reserved.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights.

Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them are available on Avaya's web site at: http://support.avaya.com/ThirdPartyLicense/

Trademarks

Avaya is a trademark of Avaya Inc.

MultiVantage is a trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

© 2001-2009 Avaya Inc. All Rights Reserved.

Step	Description
2.	**Top Page** Select **Administration → SIP Enablement Services** from the top menu (not shown). The Avaya SES **Top** page will be displayed as shown below. 

Top

Manage Users	Add and delete Users.
Manage Address Map Priorities	Adjust Address Map Priorities.
Manage Adjunct Systems	Add and delete Adjunct Systems.
Manage Event Aggregators	Add/Delete Event Aggregators.
Certificate Management	Manage Certificates.
Manage Conferencing	Add and delete Conference Extensions.
Manage Emergency Contacts	Add and delete Emergency Contacts.
Export Import to ProVision	Export and import data using ProVision on this host.
Manage Hosts	Add and delete Hosts.
IM logs	Download IM Logs.
Manage Communication Manager Servers	Add and delete Communication Manager Servers.

Step	Description
3.	**Initial Configuration Parameters** As part of the Avaya SES installation and initial configuration procedures, the following parameters were defined. Although these procedures are out of the scope of these Application Notes, the values used in the compliance test are shown below for reference. After each group of parameters is a brief description of the required steps to view the values for that group from the Avaya SES administration home page shown in the previous step. Note that for Site A, the **SIP Trunk IP Address** should be set to the IP assigned to the Avaya Communication Manager (***procr***) since there is no separate CLAN circuit pack in the Avaya G350 Media Gateway. • **SIP Domain**: ***business.com*** (To view, navigate to **Server Configuration→System Properties**) • **Host IP Address** (SES IP address): ***192.45.108.61*** • **Host Type**: ***SES combined home-edge*** (To view, navigate to **Hosts→List**; click **Edit**) • **Communication Manager Interface Name**: ***CM-B*** • **SIP Trunk Link Type**: ***TCP*** • **SIP Trunk IP Address** (CLAN2A IP address): ***192.45.108.57*** (To view, navigate to **Communication Manger Servers→List**; click **Edit**)

5.2. XMediusFAX Specific Configuration

This section describes additional SIP Enablement Services configurations necessary for interoperating with XMediusFAX. These specific configurations include the following:

- Administer Communication Manager Server Address Map (Steps 1 – 4)
- Administer trusted host (Step 5)

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>

Communication Manager Server Address Map

A Communication Manager Server Address Map is needed to route calls to the fax machines (local or remote) or the XMediusFAX fax server at the remote site. This is because neither the caller nor the called party is a registered user on the local Avaya SES with a media server extension assigned to it. Thus, Avaya SES does not know how to route this call to Avaya Communication Manager. To accomplish this task, a Communication Manager Server Address Map is needed.

To view the Communication Manager Server Address Maps, navigate to **Communication Manager Servers → List** in the left pane.

List Communication Manager Servers

<table>
<tr><th colspan="5">Commands</th><th>Interface</th><th>Host</th></tr>
<tr><td>Edit</td><td>Extensions</td><td>Map</td><td>Test-Link</td><td>Delete</td><td>CM-B</td><td>192.45.108.61</td></tr>
</table>

Add Another Communication Manager Server Interface

</td></tr>
</table>

Step	Description
2.	**Communication Manager Servers Address Map – Continued**

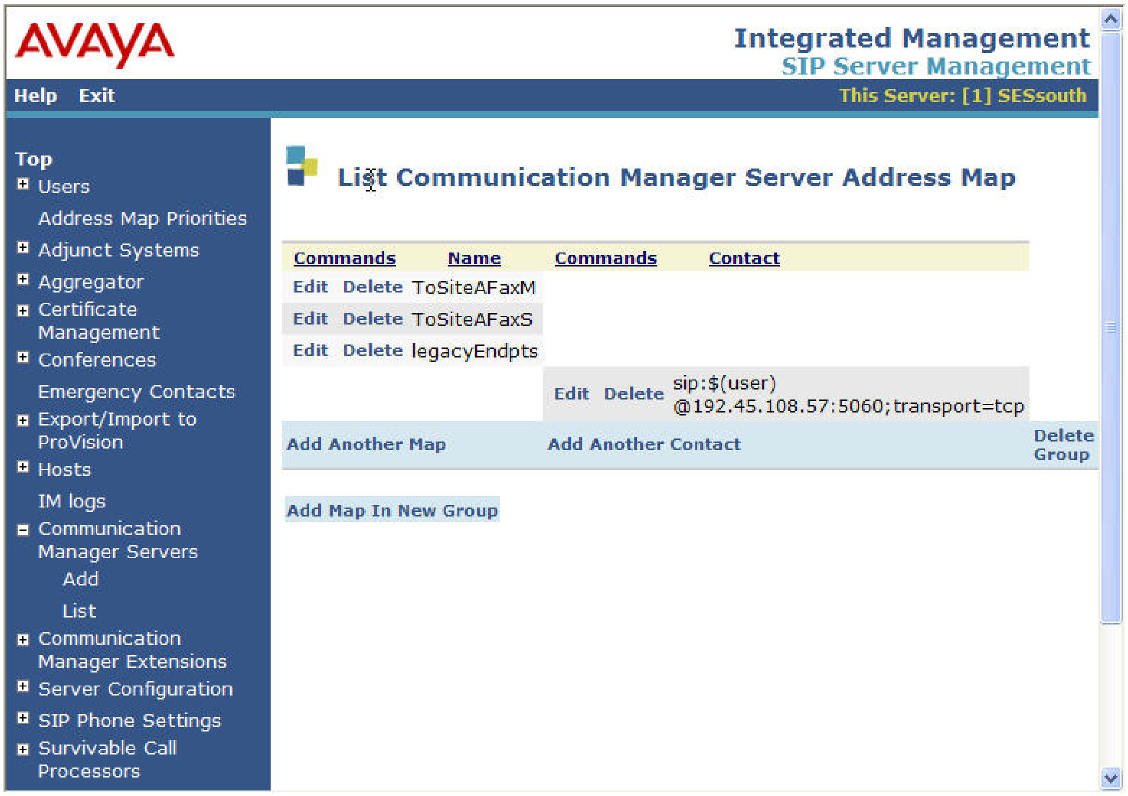
In the displayed window above, click the **Map** link in the **CM-B** interface entry. The list of Communication Manager Server Address Maps will appear as shown below. Each map defines criteria for matching calls to the Avaya SES based on the contents of the SIP Request-URI of the call

In the example below, three configured maps are shown for the compliance test:

- ***legacyEndpts*** was used for mapping calls to the fax machine at local site
- ***ToSiteAFaxM*** was used for mapping calls to the fax machine at remote site
- ***ToSiteAFaxS*** was used for mapping calls to the XMediusFAX fax server at remote site

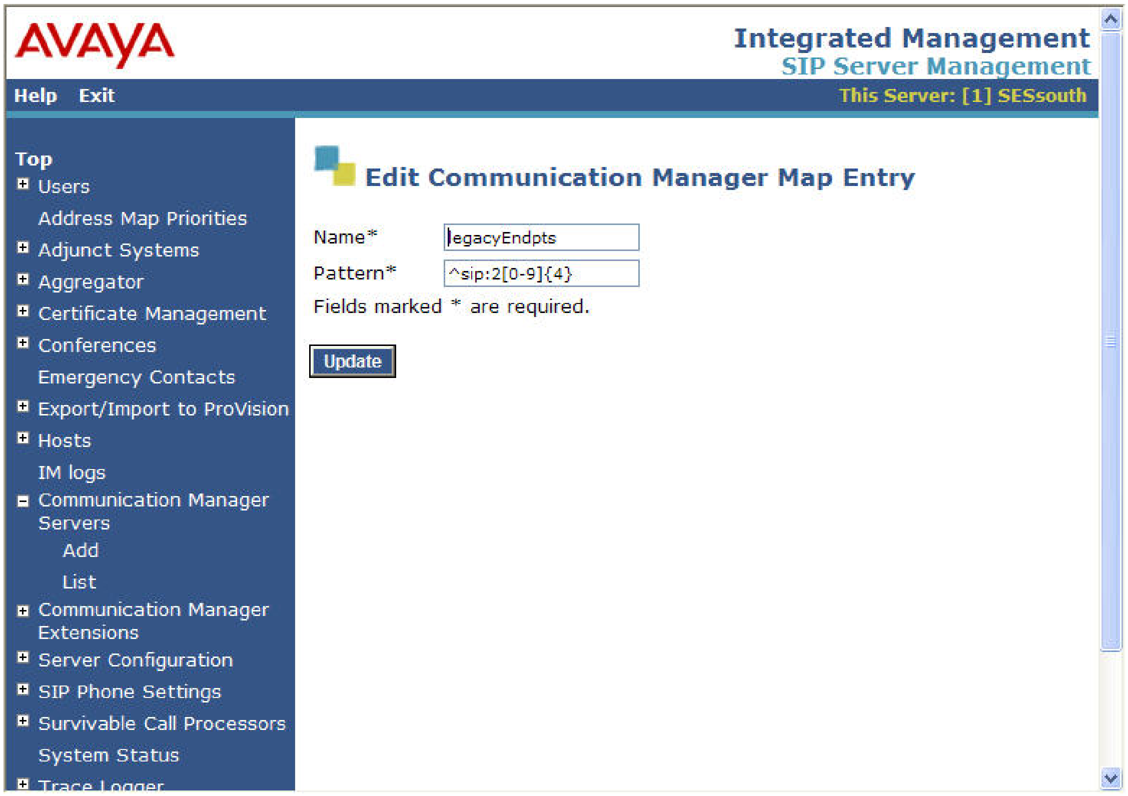
All 3 maps were associated to a **Contact** that directs the calls to the IP address of the **CLAN2A** interface, ***192.45.108.57***, using port ***5060*** and ***TCP*** as the transport protocol. The user portion in the original request URI is substituted for ***$(user)*** in the **Contact** expression shown below and in the screenshot:

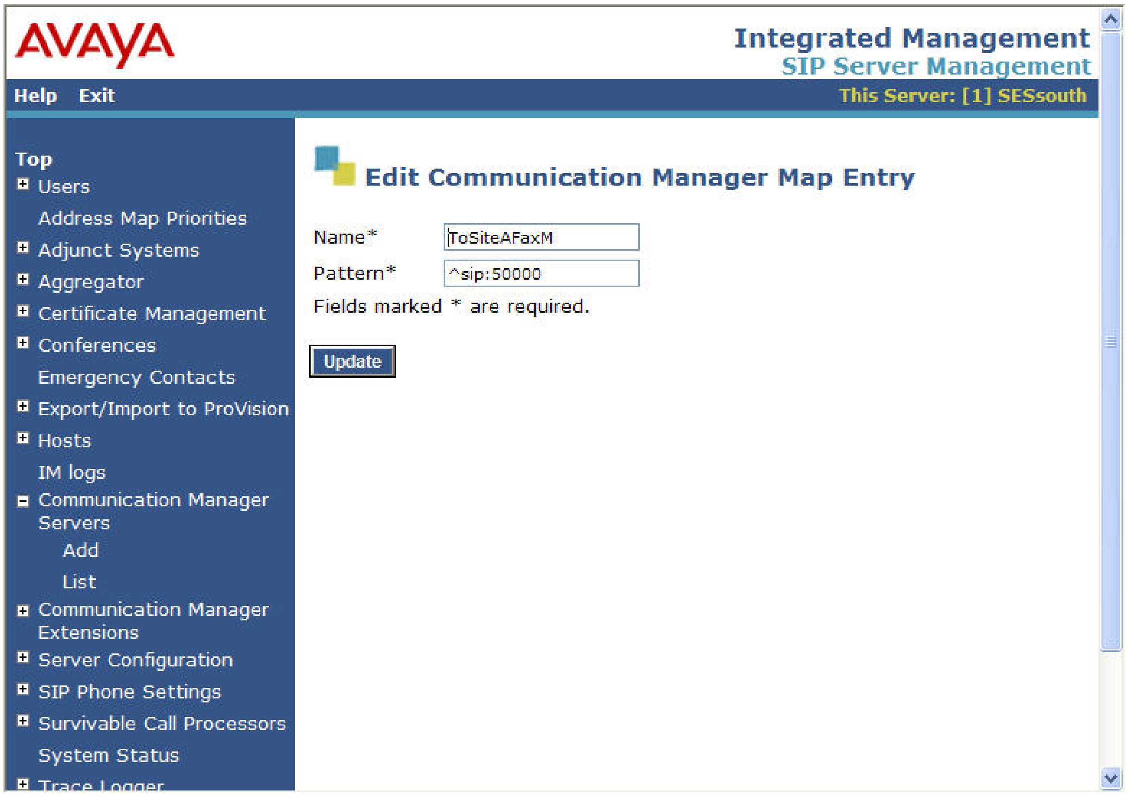
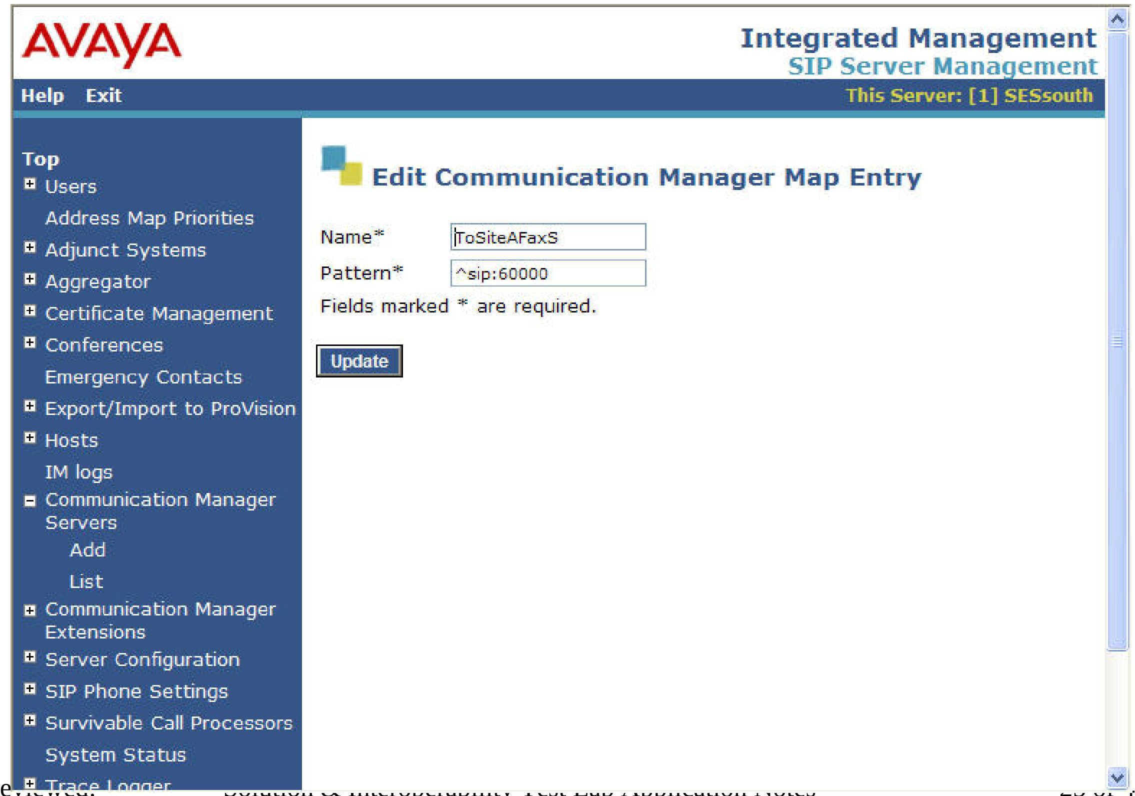
```
sip:$(user)@192.45.108.57:5060;transport=tcp
```

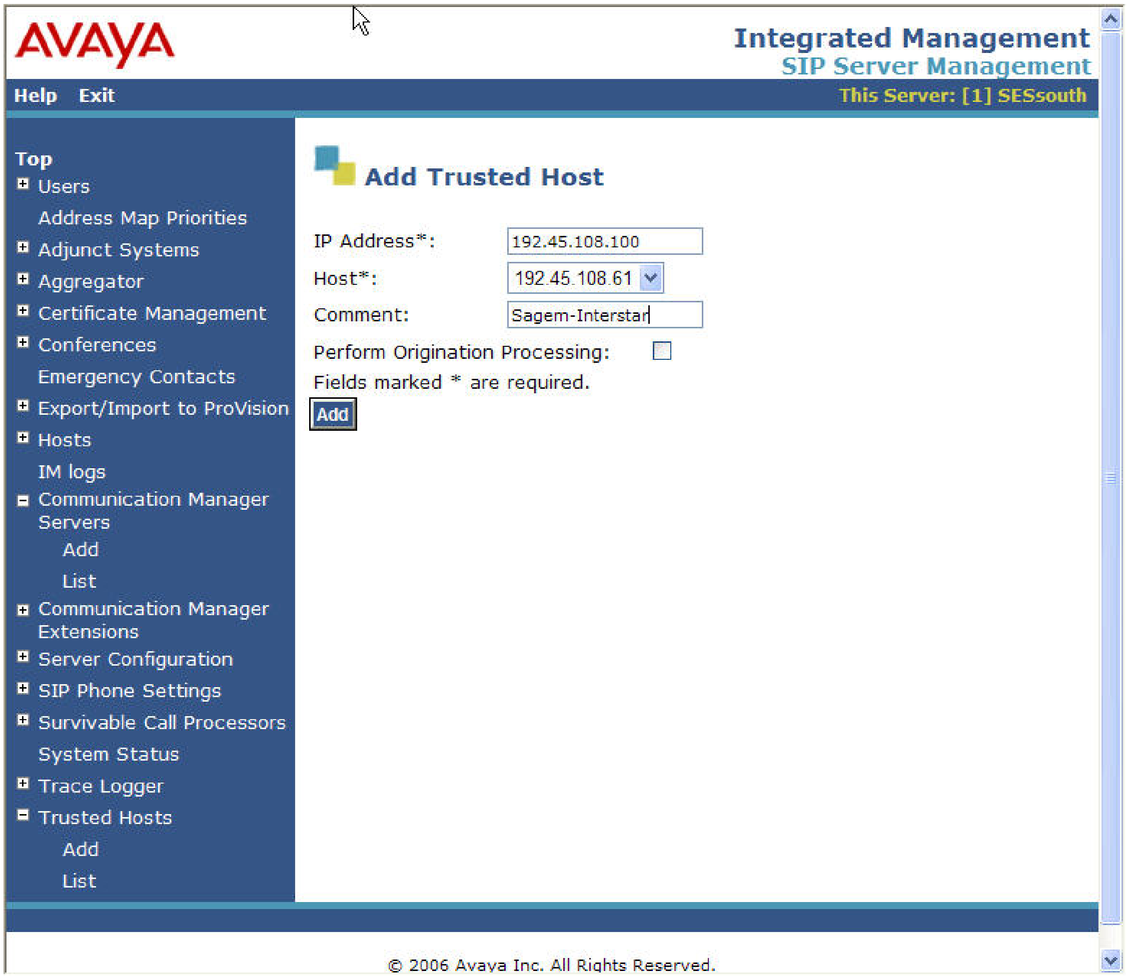


List Communication Manager Server Address Map

Commands	Name	Commands	Contact
Edit Delete	ToSiteAFaxM		
Edit Delete	ToSiteAFaxS		
Edit Delete	legacyEndpts		
		Edit Delete	sip:$(user) @192.45.108.57:5060;transport=tcp

Step	Description
3.	**Communication Server Address Map – Continued** To view or edit the call matching criteria of the map, click the **Edit** link next to the map name. The content of the Communication Server Address Map is described below. ▪ **Name**: Contains any descriptive name ▪ **Pattern**: Contains an expression to define the matching criteria for calls to be routed to this Avaya Communication Manager. For the address map named ***legacyEndpts***, the expression will match any URI that begins with ***sip:2*** followed by any digit between ***0-9*** for the next ***4*** digits. Additional information on the syntax used for address map patterns can be found in [4]. If any changes are made, click **Update**.  Edit Communication Manager Map Entry Name* legacyEndpts Pattern* ^sip:2[0-9]{4} Fields marked * are required.

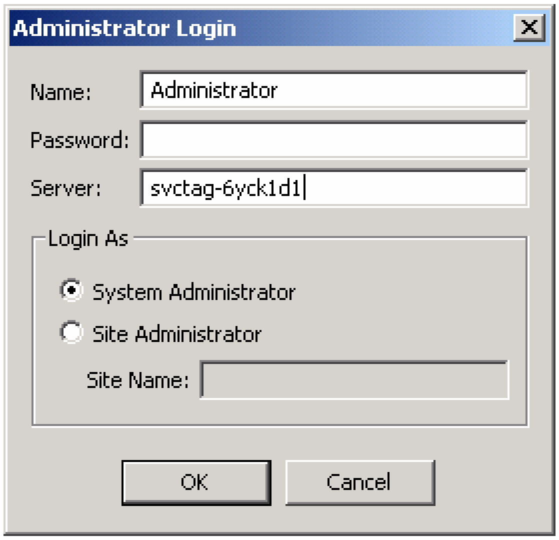
Step	Description
4.	**Communication Server Address Map – Continued** Displayed below are the address maps configured in the compliance test for routing calls to the fax machine and fax server at remote site.  Edit Communication Manager Map Entry Name* ToSiteAFaxM Pattern* ^sip:50000 Fields marked * are required.  Edit Communication Manager Map Entry Name* ToSiteAFaxS Pattern* ^sip:60000 Fields marked * are required.

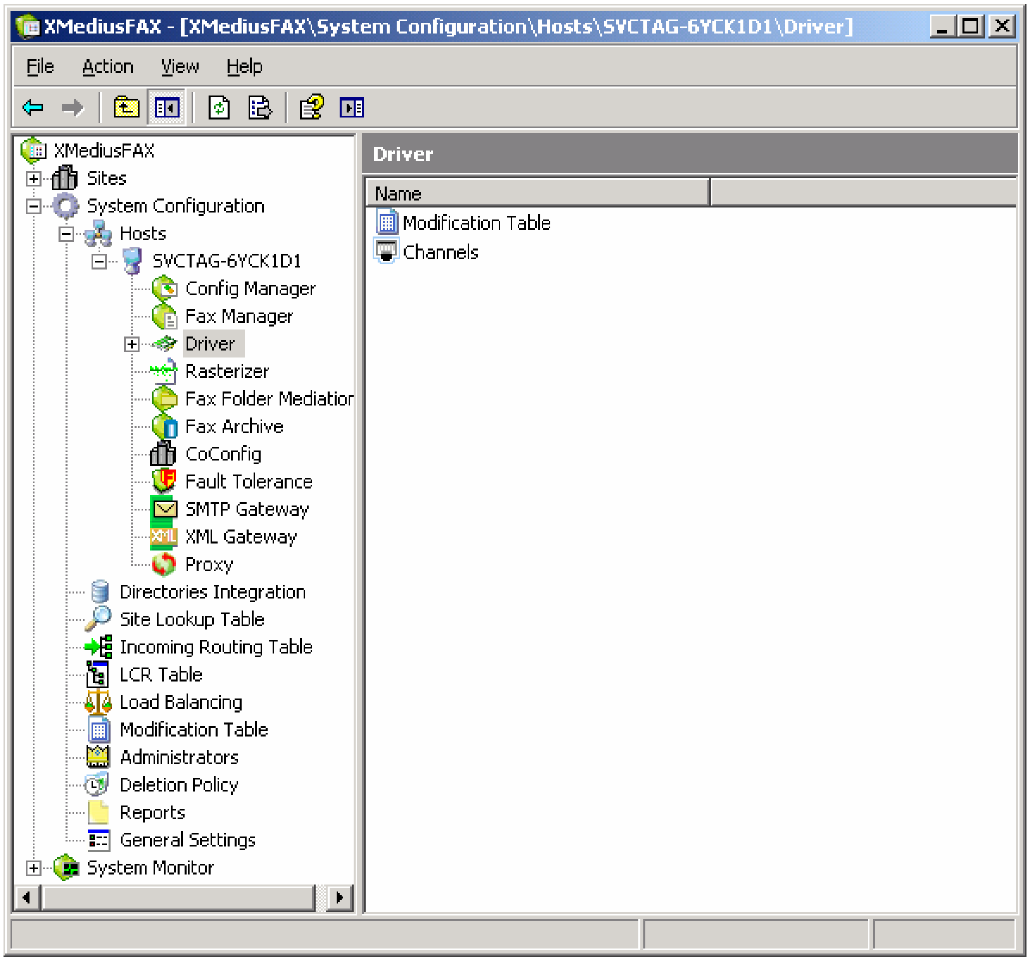
Step	Description
5.	**Trusted Host** XMediusFAX fax server must be added as a Trusted Host (to the SIP Enablement Services). To add a new Trusted Host, navigate to **Trusted Hosts → Add Trusted Host** in the left pane. In the displayed window, configure the following fields: ▪ **IP Address**: Enter IP address assigned to the XMediusFAX server ▪ **Host**: Select the IP address for the Avaya SES ▪ **Comments**: Enter a descriptive text After the fields are properly set, click **Add**.  Add Trusted Host IP Address*: 192.45.108.100 Host*: 192.45.108.61 Comment: Sagem-Interstar Perform Origination Processing: ☐ Fields marked * are required. Add

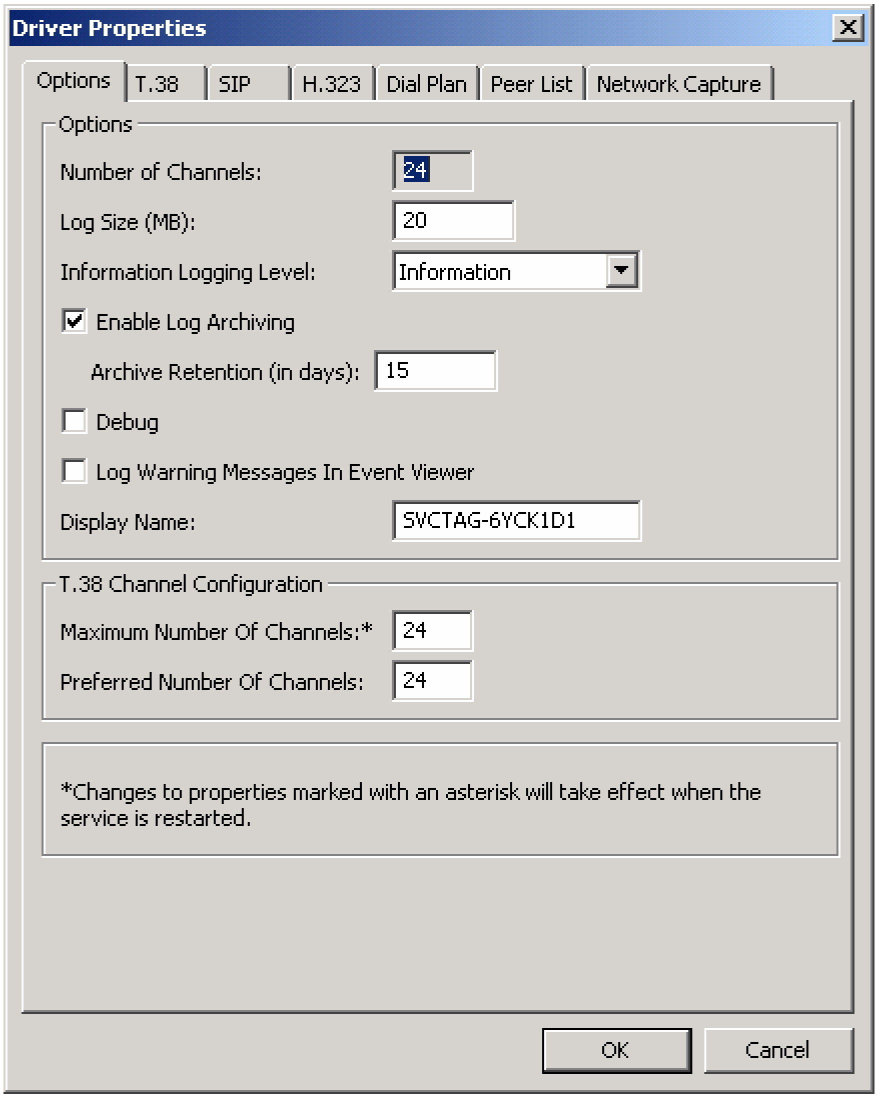
6. Configure Sagem-Interstar XMediusFAX

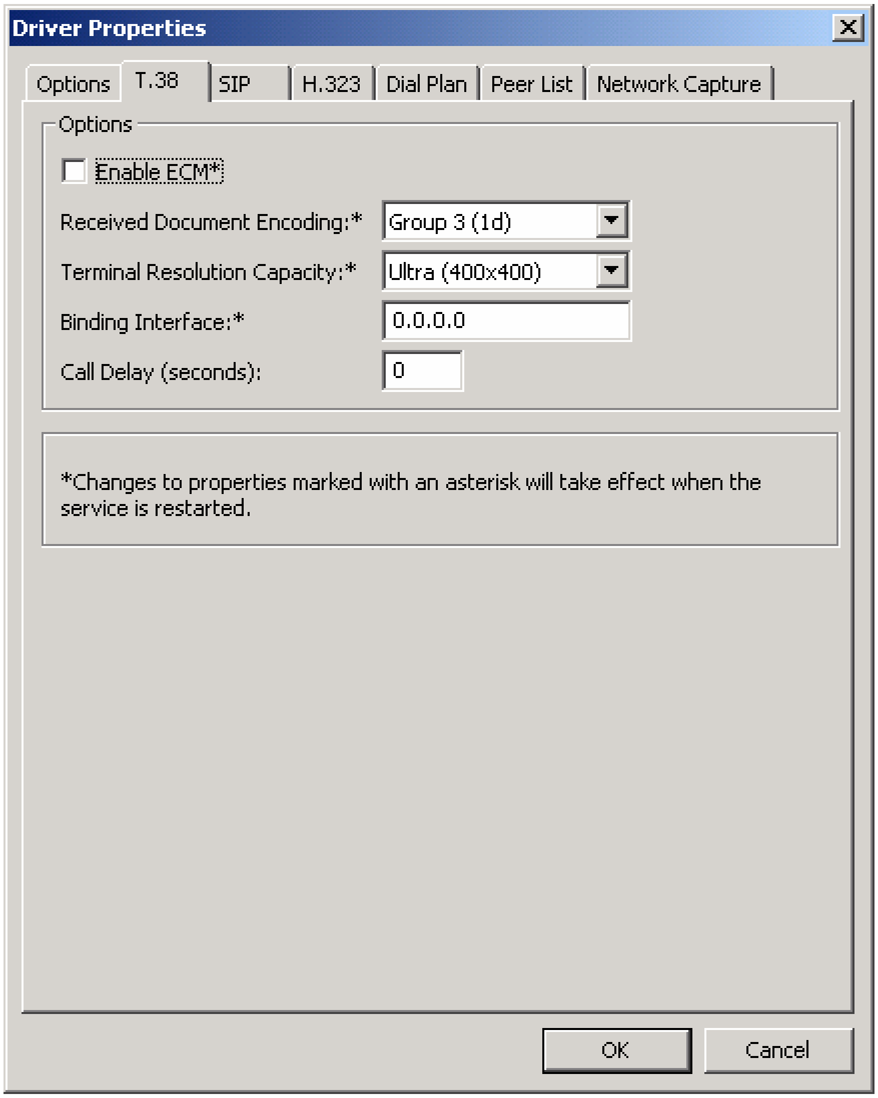
This section describes the configuration of XMediusFAX. It assumes that the application and all required software components have been installed and properly licensed. The number of channels supported by the XMediusFAX server is controlled via an XMediusFAX server license file. For instructions on sending and receiving faxes, consult the XMediusFAX Administrator Guide [5] and User Guide [7].

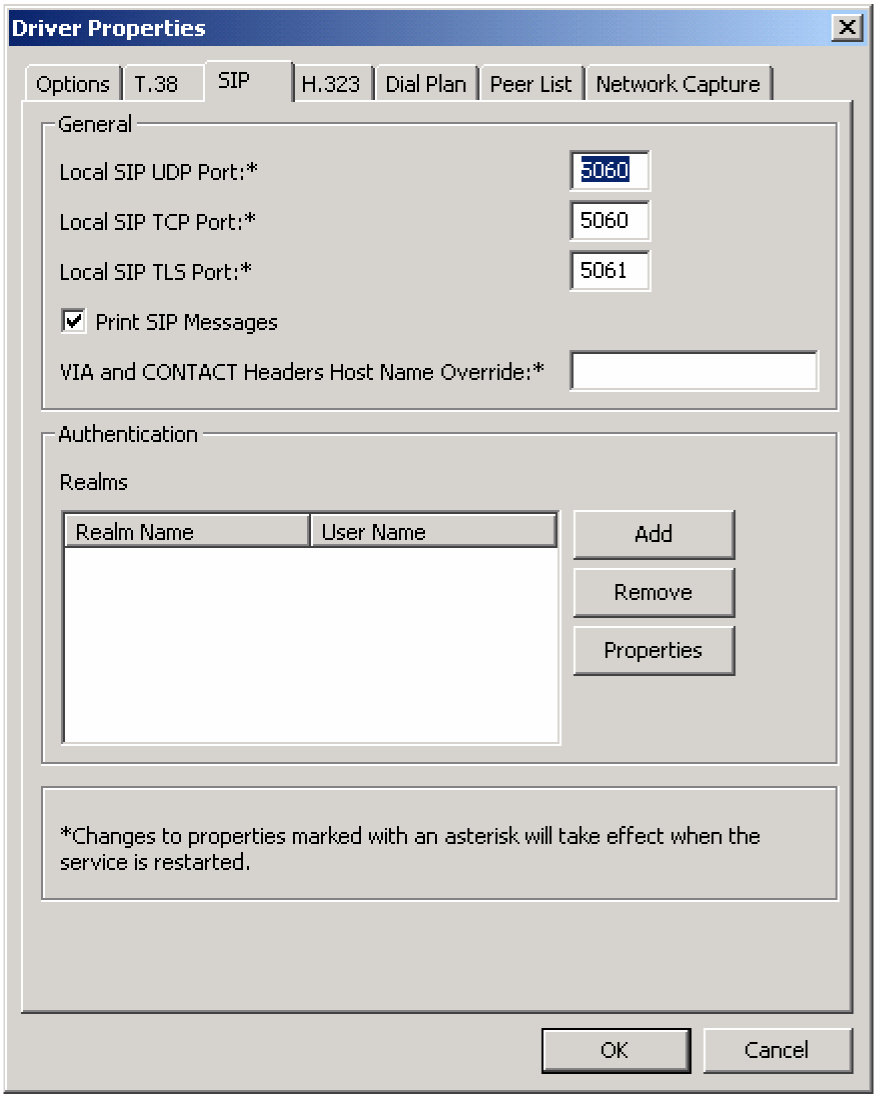
The examples shown in this section refer to Site B. Unless specified otherwise, the same steps also apply to Site A using values appropriate for Site A from **Figure 1**.

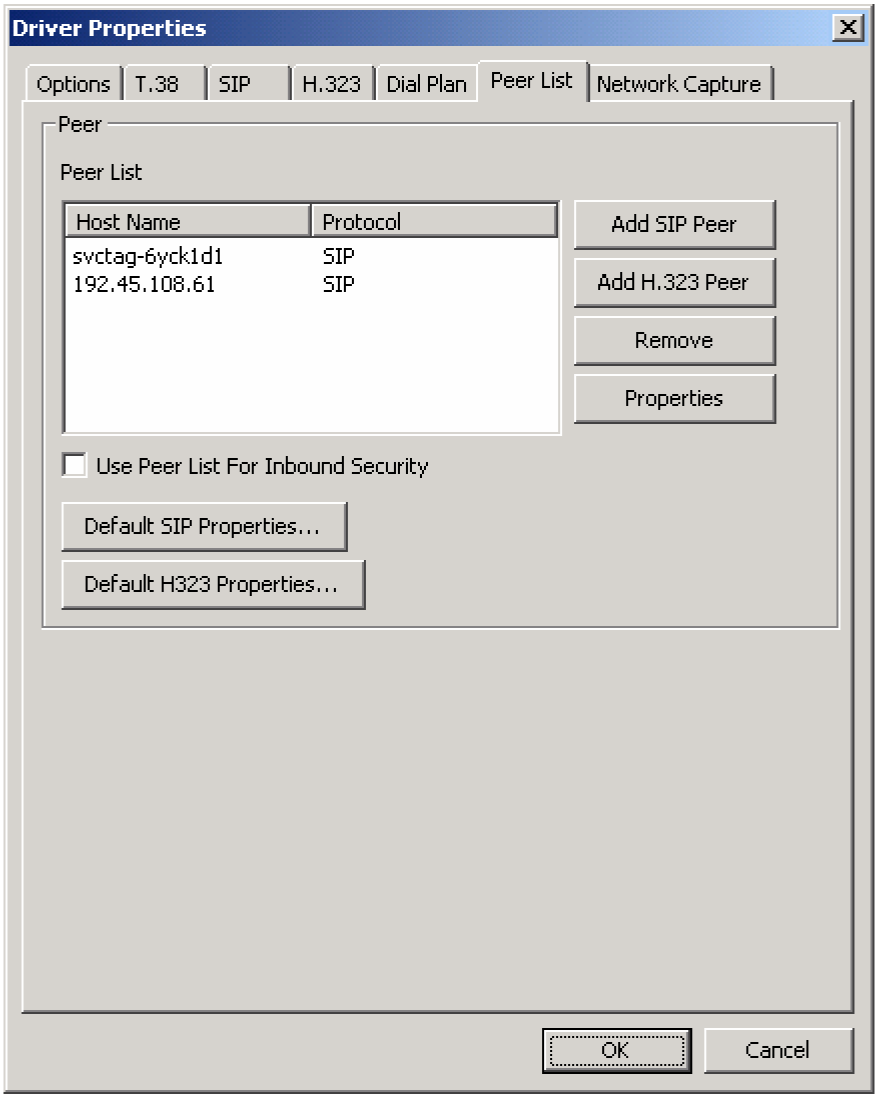
Step	Description
1.	**Prepare Windows 2003 Server for XMediusFAX launch** To function properly XMediusFAX needs to have read/write privileges to the C:\Windows\temp folder. If McAfee VirusScan Enterprise is running on the Windows 2003 server, the C:\Windows\temp folder needs to be excluded from the scan list. Consult Sagem-Interstar for instructions.
2.	**Launch the Application** On the XMediusFAX server, launch the XMediusFAX application from the Windows Start Menu. Navigate to **Start → All Programs → XMediusFAX → XMediusFAX**. A login screen appears. Log in with proper credentials. Click the **OK** button.  Administrator Login Name: Administrator Password: Server: svctag-6yck1d1 Login As ● System Administrator ○ Site Administrator Site Name:

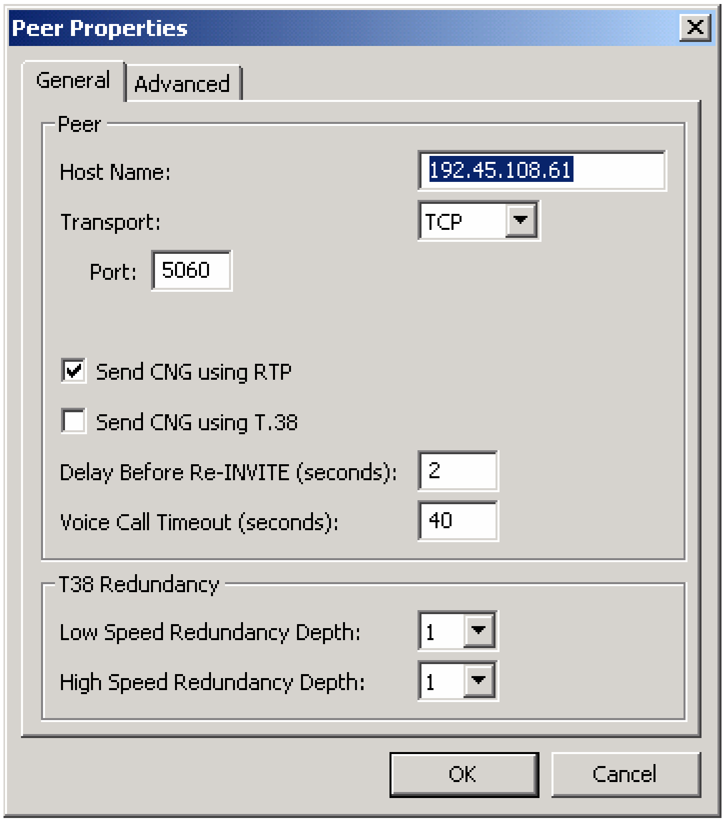
Step	Description
3.	**Configure Driver Properties** On the main screen, navigate to **XMediusFAX → System Configuration → Hosts → SVCTAG-6YCK1D1 → Driver** in the left hand tree menu. Right-click on **Driver** and select **Properties** (not shown). 

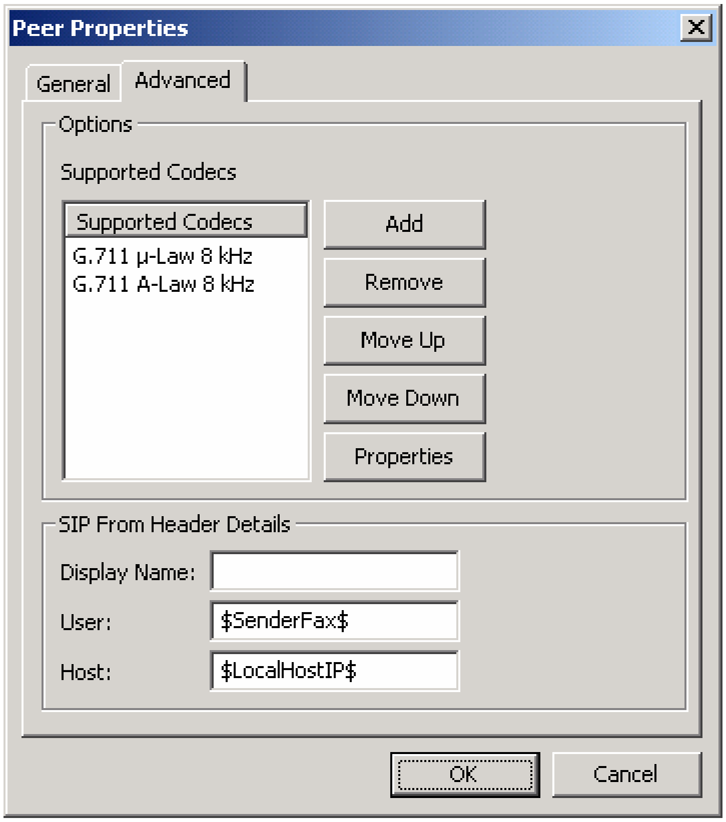
Step	Description
4.	**General Options** On the **Driver Properties** screen, select the **Options** tab. Set the **Maximum Number Of Channels** and **Preferred Number Of Channels** fields under **T.38 Channel Configuration** to the number of simultaneous faxes to be processed. This number should be consistent with the **Number of Members** field specified in **Section 4, Step 10**.  Options Number of Channels: 24 Log Size (MB): 20 Information Logging Level: Information ☑ Enable Log Archiving Archive Retention (in days): 15 ☐ Debug ☐ Log Warning Messages In Event Viewer Display Name: SVCTAG-6YCK1D1 T.38 Channel Configuration Maximum Number Of Channels:* 24 Preferred Number Of Channels: 24 *Changes to properties marked with an asterisk will take effect when the service is restarted.

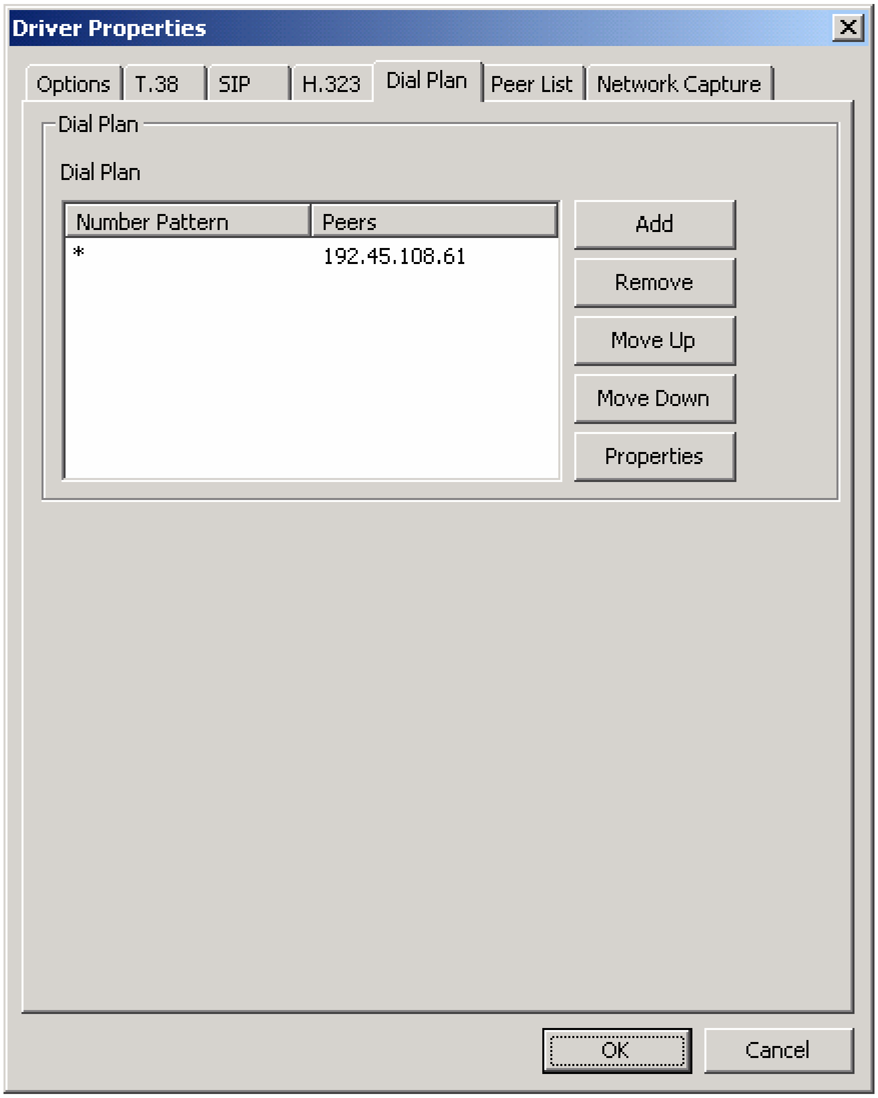
Step	Description
5.	**T.38 Parameters** On the **Driver Properties** screen, select the **T.38** tab. Configure the fields as follows: • **Received Document Encoding –** Set this field to the highest encoding allowed. For the compliance test, this value was set to ***Group 3 (1d)***. • **Terminal Resolution Capacity –** Set this field to the highest resolution allowed. For the compliance test, this value was set to ***Ultra (400x400)***.  ☐ Enable ECM* Received Document Encoding:* Group 3 (1d) Terminal Resolution Capacity:* Ultra (400x400) Binding Interface:* 0.0.0.0 Call Delay (seconds): 0 *Changes to properties marked with an asterisk will take effect when the service is restarted.

Step	Description
6.	**SIP Parameters** On the **Driver Properties** screen, select the **SIP** tab. Configure the fields as follows: - **Local SIP TCP port –** Set this field to match the **Far-end Listen Port** field in **Section 4**, **Step 9**. For the compliance test, TCP was used as the transport layer protocol by the XMediusFAX.  Local SIP UDP Port:* 5060 Local SIP TCP Port:* 5060 Local SIP TLS Port:* 5061 ☑ Print SIP Messages VIA and CONTACT Headers Host Name Override:* *Changes to properties marked with an asterisk will take effect when the service is restarted.

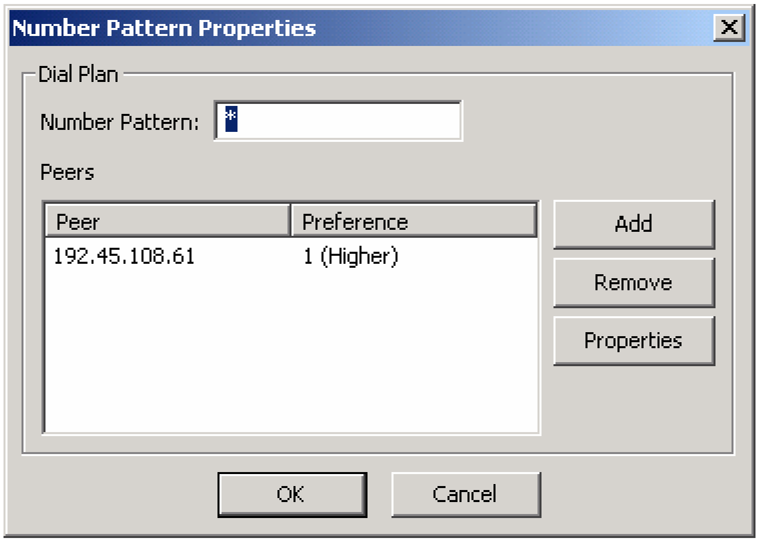
Step	Description
7.	**Peer List** On the **Driver Properties** screen, select the **Peer List** tab. To add a new SIP peer, select the **Add SIP Peer** button and enter the values shown in **Step 8**. To view an existing peer, highlight the peer in the list and click **Properties**. The example below shows the peer list after the Avaya SIP Enablement Services interface, ***192.45.108.61***, has been added to the list.  Peer List Host Name / Protocol svctag-6yck1d1 SIP 192.45.108.61 SIP ☐ Use Peer List For Inbound Security

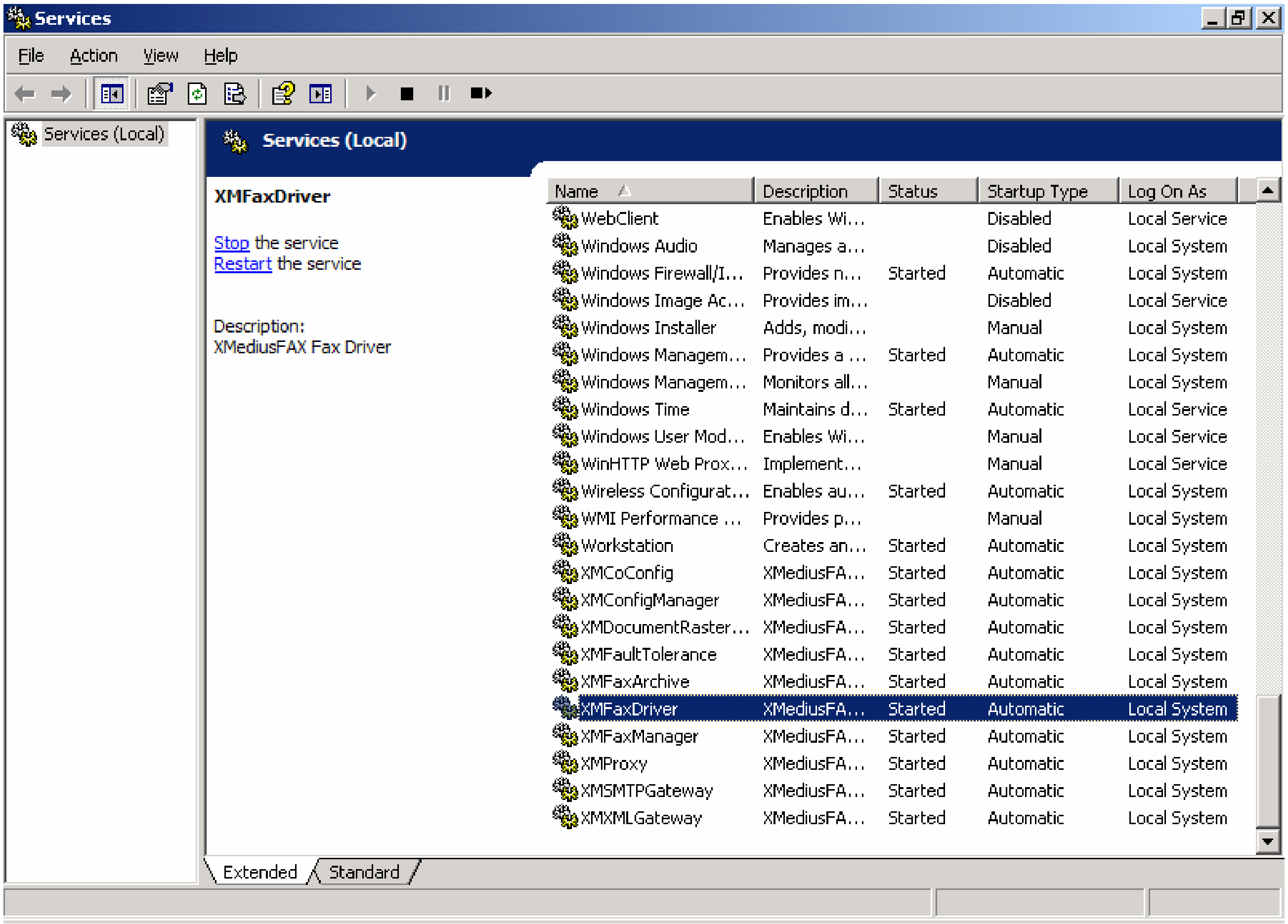
Step	Description
8.	**Peer Properties** On the **Peer Properties** screen, configure as follows: - **Host Name** – Set this field to the IP address of the Avaya SIP Enablement Services server in **Section 5.1, Step 3**. - **Transport:** Set this field to ***TCP***. For the compliance test, TCP was used as the transport layer protocol by the XMediusFAX. - **Port** - Set this field to ***5060***. - Check the **Send CNG using RTP** field.  Host Name: 192.45.108.61 Transport: TCP Port: 5060 ☑ Send CNG using RTP ☐ Send CNG using T.38 Delay Before Re-INVITE (seconds): 2 Voice Call Timeout (seconds): 40 Low Speed Redundancy Depth: 1 High Speed Redundancy Depth: 1

Step	Description
9.	**Codec** On the **Peer Properties** screen, select the **Advanced** tab. To add a codec for the SIP peer, select the **Add** button and select the values from the drop-down menu. To view an existing codec, highlight the codec in the list and click **Properties**. The example below shows the codec list supported by the newly added SIP peer.  Supported Codecs G.711 µ-Law 8 kHz G.711 A-Law 8 kHz Display Name: User: $SenderFax$ Host: $LocalHostIP$

Step	Description
10.	**Dial Plan** On the **Driver Properties** screen, select the **Dial Plan** tab. To add a new entry to the dial plan, select the **Add** button and enter the values shown in **Step 11**. To view an existing entry, highlight the entry in the list and click **Properties** to get the **Number Pattern Properties** screen. The example below shows the dial plan after the entry for ***** (any value) has been added to the list. 

Number Pattern	Peers
*	192.45.108.61

Step	Description
11.	**Number Pattern Properties** On the **Number Pattern Properties** screen, configure as follows: • **Number Pattern** – Set this field to the pattern to match. In this example, the value of ***** indicates any dialed number is acceptable. • **Peer –** Click the **Add** button. In the **Peer Properties** window that appears (not shown), enter the **Peer** IP Address and **Preference** value of ***1*** and click **OK**. In this example, only one peer is configured.  Number Pattern: * Peer: 192.45.108.61 Preference: 1 (Higher) Lastly, click OK on the **Driver Properties** screen shown in **Step 10**, to accept the Driver Configuration.

Step	Description
12.	Once all the driver properties have been configured, go to **Start → Control Panel → Administrative Tools → Services** to stop and start the **XMFaxDriver** service to effect the changes. 

XMFaxDriver

Stop the service
Restart the service

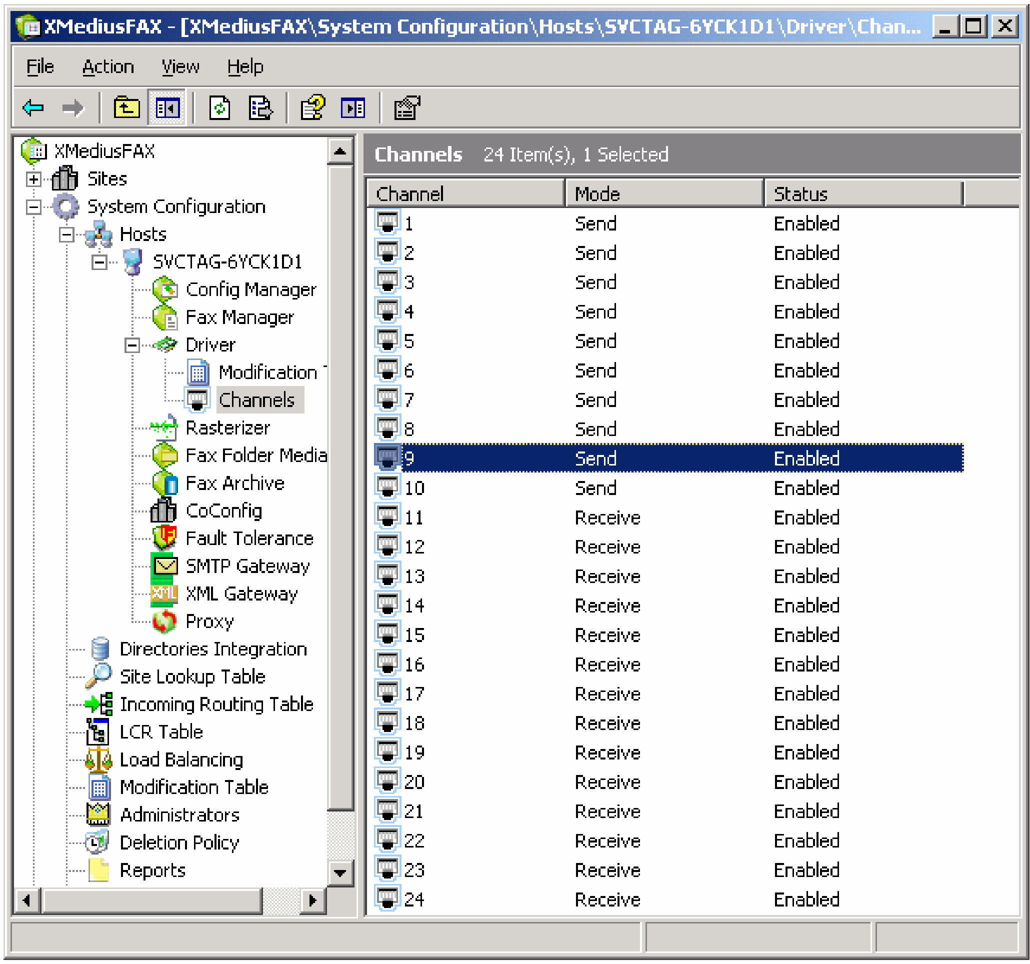
Description:
XMediusFAX Fax Driver

Name	Description	Status	Startup Type	Log On As
WebClient	Enables Wi...		Disabled	Local Service
Windows Audio	Manages a...		Disabled	Local System
Windows Firewall/I...	Provides n...	Started	Automatic	Local System
Windows Image Ac...	Provides im...		Disabled	Local Service
Windows Installer	Adds, modi...		Manual	Local System
Windows Managem...	Provides a ...	Started	Automatic	Local System
Windows Managem...	Monitors all...		Manual	Local System
Windows Time	Maintains d...	Started	Automatic	Local Service
Windows User Mod...	Enables Wi...		Manual	Local Service
WinHTTP Web Prox...	Implement...		Manual	Local Service
Wireless Configurat...	Enables au...	Started	Automatic	Local System
WMI Performance ...	Provides p...		Manual	Local System
Workstation	Creates an...	Started	Automatic	Local System
XMCoConfig	XMediusFA...	Started	Automatic	Local System
XMConfigManager	XMediusFA...	Started	Automatic	Local System
XMDocumentRaster...	XMediusFA...	Started	Automatic	Local System
XMFaultTolerance	XMediusFA...	Started	Automatic	Local System
XMFaxArchive	XMediusFA...	Started	Automatic	Local System
XMFaxDriver	XMediusFA...	Started	Automatic	Local System
XMFaxManager	XMediusFA...	Started	Automatic	Local System
XMProxy	XMediusFA...	Started	Automatic	Local System
XMSMTPGateway	XMediusFA...	Started	Automatic	Local System
XMXMLGateway	XMediusFA...	Started	Automatic	Local System

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>13.</td><td>

Configure Channels

On the main screen, navigate to **XMediusFAX → System Configuration → Hosts → SVCTAG-6YCK1D1 → Driver → Channels** in the left hand tree menu. Right-click on each channel in the right pane to set the **Mode** to ***Send***, ***Receive*** or ***Both***. In the compliance test, 10 channels were set to ***Send*** and 14 channels were set to ***Receive***.



Channels 24 Item(s), 1 Selected

Channel	Mode	Status
1	Send	Enabled
2	Send	Enabled
3	Send	Enabled
4	Send	Enabled
5	Send	Enabled
6	Send	Enabled
7	Send	Enabled
8	Send	Enabled
9	Send	Enabled
10	Send	Enabled
11	Receive	Enabled
12	Receive	Enabled
13	Receive	Enabled
14	Receive	Enabled
15	Receive	Enabled
16	Receive	Enabled
17	Receive	Enabled
18	Receive	Enabled
19	Receive	Enabled
20	Receive	Enabled
21	Receive	Enabled
22	Receive	Enabled
23	Receive	Enabled
24	Receive	Enabled

s

</td></tr>
</table>

7. General Test Approach and Test Results

This section describes the compliance testing used to verify the interoperability of Sagem-Interstar XMediusFAX SP Edition with the Avaya SIP infrastructure (Communication Manager and SIP Enablement Services). This section covers the general test approach and the test results.

7.1. General Test Approach

The general test approach was to make intra-site and inter-site fax calls to and from XMediusFAX. In the compliance test configuration Site B served as the main enterprise site and Site A served as a simulated PSTN or a remote enterprise site. Inter-site calls and simulated PSTN calls were made using SIP trunks or ISDN-PRI trunks between the sites. By using two Communication Managers and two port networks with one of the Communication Managers, fax calls across multiple TDM/IP hops were able to be tested. Faxes were sent with various page lengths, resolutions, and at various fax data speeds. For capacity testing, a 100 2-page faxes were continuously sent between the two XMediusFAX servers. Because the G350 has a limited DSP capacity, a G450 with the same configuration was used for the capacity testing. Serviceability testing included verifying proper operation/recovery from failed cables, unavailable resources, and Communication Manager and XMediusFAX restarts. Fax calls were also tested with different Avaya Media Gateway media resources to process the fax data. This included the TN2302 MedPro circuit pack, the TN2602 MedPro circuit pack in the Avaya G650 Media Gateway; and the integrated VoIP engine of the Avaya G350 Media Gateway.

7.2. Test Results

XMediusFAX successfully passed compliance testing. The following observations were made during the compliance test:

- All the fax calls were established successfully with or without shuffling on. However, for those inter-site calls that have shuffling on and SIP trunks used between the two sites, the audio was not shuffled from end-to-end. Instead, Port Network 1 Medpro media resources were used in the audio path for those calls.
- To function properly XMediusFAX needs to have read/write privileges to the C:\Windows\temp folder. If McAfee VirusScan Enterprise is running on the Windows 2003 server, the C:\Windows\temp folder needs to be excluded from the scan list to make the folder readable and writeable by XMediusFAX.
- During the serviceability testing, the cable between the router and the Layer 2 switch that connected the XMediusFAX server was unplugged to simulate a network disruption. When the cable was plugged back in, inbound calls to the XMediusFAX were working. But outbound calls from the XMediusFAX server did not work any more. This was because the Windows 2003 server, the XMediusFAX server ran on, still kept the old TCP socket. The XMediusFAX server can go back to normal by stopping and starting the XMediusFAX Driver service manually.

8. Verification Steps

The following steps may be used to verify the configuration:

- From the Avaya Communication Manager SAT, use the **status signaling-group** command to verify that the SIP signaling groups configured in **Step 9** of **Section 4** are in-service.
- From the Avaya Communication Manager SAT, use the **status trunk-group** command to verify that the SIP trunk group configured in **Section 4**, **Steps 10 - 11** is in-service.
- Verify that fax calls can be placed to/from XMediusFAX server at each site.
- From the Avaya Communication Manager SAT, use the **list trace tac** command to verify that fax calls are routed to the expected trunks.
- From the Avaya Communication Manager SAT, use the **status trunk group** command to identify the trunk used for a particular call and then use the **status trunk group/member** command to verify the audio path of the call.

9. Conclusion

These Application Notes describe the procedures required to configure the Sagem-Interstar XMediusFAX Service Provider (SP) Edition to interoperate with Avaya SIP infrastructure (Communication Manager and SIP Enablement Services). The Sagem-Interstar XMediusFAX SP Edition successfully passed compliance testing with the observations documented in **Section 7.2**.

10. Additional References

[1] *Avaya Aura™ Communication Manager Feature Description and Implementation*, Doc # 555-245-205, May 2009.
[2] *Administering Avaya Aura™ Communication Manager*, Doc # 03-300509, May 2009.
[3] *SIP support in Avaya Aura™ Communication Manager Running on the Avaya S8xxx Servers*, Doc # 555-245-206, May 2009.
[4] *Administering Avaya Aura™ SIP Enablement Services on the Avaya S8300 Server*, Doc # 03-602508, May 2009.
[5] *Sagem-Interstar XMediusFAX Administrator Guide*, November 2009
[6] *Sagem-Interstar XMediusFAX Installation and Maintenance Guide*, November 2009
[7] *Sagem-Interstar XMediusFAX User Guide*, November 2009

Product documentation for Avaya products may be found at http://support.avaya.com.

Documentation for XMediusFAX version 6.5 may be found at www.sagem-interstar.com.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.