Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Acme Packet Net-Net Session Director with Avaya SIP Enablement Services and Avaya Communication Manager to Support SIP Remote Users with NAT Traversal – Issue 1.0

Abstract

These Application Notes describes the procedures for configuring Acme Packet Net-Net Session Director with Avaya SIP Enablement Services (SES) and Avaya Communication Manager.

Acme Packet Net-Net Session Director is a SIP security appliance that manages and protects the flow of SIP signaling and related media across an untrusted network. The compliance testing focused on telephony scenarios between remote SIP endpoints and the SIP infrastructure at a main site across an untrusted network with far-end network address translation (NAT) traversal.

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

1. Introduction

These Application Notes describes the procedures for configuring Acme Packet Net-Net Session Director with Avaya SIP Enablement Services (SES) and Avaya Communication Manager.

Acme Packet Net-Net Session Director is a SIP security appliance that manages and protects the flow of SIP signaling and related media across an untrusted network. The compliance testing focused on telephony scenarios between remote SIP endpoints and the SIP infrastructure at a main site across an untrusted network with far-end network address translation (NAT) traversal.

1.1. Configuration

Figure 1 illustrates the test configuration. The test configuration shows several remote users connected by different means to an untrusted IP network to access the SIP infrastructure at a main enterprise site. Session Director resides at the edge of the enterprise network and acts as a back-to-back user agent (B2BUA). One port of Session Director is connected to the untrusted public network and another port is connected to the private enterprise LAN. The remote SIP endpoints will direct SIP and RTP traffic to the public IP address of Session Director. Session Director will proxy user registrations and other SIP signaling messages to Avaya SES on behalf of the remote endpoints. In this manner, Session Director can protect the main site infrastructure from any SIP-based attacks. The voice communication across the untrusted network uses SIP over UDP and RTP for the media streams. In addition, other data traffic related to the voice communication is also routed through Session Director. This includes the TFTP traffic used to access the configuration file for the Avaya 4600 Series SIP Telephones and the HTTP traffic used to access the license server for the Avaya one-X Desktop Edition. Any remaining data traffic flowing in or out of the enterprise would not pass through Session Director but instead would typically pass through a traditional data firewall at the edge of the enterprise. This connection is not shown in **Figure 1** since **Figure 1** focuses only on the connections necessary to support the remote SIP endpoints.

Located at the main site on the private LAN side of Session Director is an Avaya SES and an Avaya S8300 Server running Avaya Communication Manager in an Avaya G700 Media Gateway. Avaya SES is configured as a combined home/edge server. Session Director also has a port dedicated to a separate subnet for management. Endpoints include two Avaya 4600 Series IP Telephones (with SIP firmware), an Avaya 6408D Digital Telephone, and an Avaya 6210 Analog Telephone. An ISDN-PRI trunk connects the media gateway to the PSTN. One PSTN number assigned to the ISDN-PRI trunk at the main site is mapped to a telephone extension at the main site. The other is mapped to the telephone extension of one of the remote users.

The Avaya 4600 Series IP Telephones (with SIP firmware) located at the main site are registered directly to Avaya SES. All calls originating from Avaya Communication Manager at the main office and destined for the remote users will be routed through the on-site Avaya SES, Session Director and across the untrusted IP network.

The remote users are comprised of the following:

- An Avaya 4600 Series IP Telephone (with SIP firmware) and an Avaya one-X Desktop Edition connected directly to the untrusted network.
- Two Avaya 4600 Series IP Telephones (with SIP firmware) and an Avaya one-X Desktop Edition connected behind a consumer broadband router/firewall. This router was configured to perform NAT. More specifically, it performed both network address and port translation (NAPT).
- An Avaya 4600 Series IP Telephone (with SIP firmware) connected behind a second consumer broadband router/firewall. This router was also configured to perform NAPT.

The remote users register with Avaya SES via Session Director. All calls originating from the remote users are routed across the untrusted IP network, Session Director, and Avaya SES to Avaya Communication Manager at the main site.

All Avaya 4600 Series SIP Telephones, both local and remote, use the TFTP server at the main site to obtain their configuration files. The Avaya one-X Desktop Editions use Avaya SES as the license server.

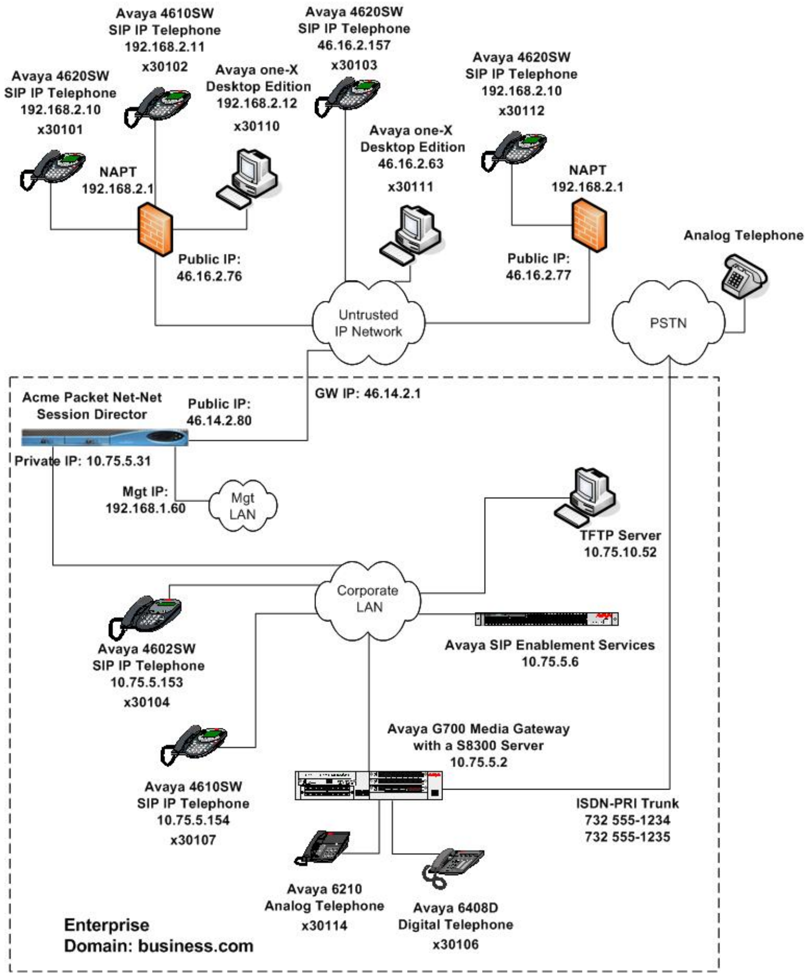


Figure 1: Session Director Test Configuration

2. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8300 Server with Avaya G700 Media Gateway Avaya IA 770 Intuity Audix	Avaya Communication Manager 4.0 Service Pack (R014x.00.0.730.5-13566)
Avaya SIP Enablement Services (SES)	3.1.2
Avaya 4602SW IP Telephone Avaya 4610SW IP Telephones Avaya 4620SW IP Telephones	SIP version 2.2.2
Avaya one-X Desktop Edition	2.1 SP1 (Build 70) (Windows XP Professional)
Avaya 6408D Digital Telephone	-
Avaya 6210 Analog Telephone	-
Analog Telephone	-
Windows PC (TFTP Server)	Windows XP Professional
Acme Packet Net-Net Session Director	4.1.4 Patch 4

Table 1: Equipment Used

3. Configure Avaya Communication Manager

This section describes the Avaya Communication Manager configuration. It assumes the procedures necessary to support SIP have been performed as described in [3]. It also assumes that an off-PBX station (OPS) has been configured on Avaya Communication Manager for each SIP endpoint in the configuration as described in [3] and [4]. This section will summarize the critical user-defined parameters used in the compliance test as part of the procedures referenced above. It will also describe any deviations from the standard procedures.

The configuration of Avaya 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.

Step	Description
1.	**IP network region** The Avaya Media Server, Avaya SES and SIP endpoints were located in a single IP network region (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.

- **Authoritative Domain**: ***business.com*** This field was configured to match the domain name configured on Avaya SES. This name will appear in the "From" header of SIP messages originating from this IP region.
- **Name**: ***default*** Any descriptive name may be used.
- **Intra-region IP-IP Direct Audio**: ***yes***
  Inter-region IP-IP Direct Audio: ***yes***
  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. Shuffling can be further restricted at the trunk level on the **Signaling Group** form.
- **Codec Set**: ***1*** The codec set contains the set of codecs available for calls within this IP network region. This includes SIP calls since all necessary components are within the same region.

```
display ip-network-region 1                                     Page   1 of  19
                               IP NETWORK REGION
Region: 1
Location:         Authoritative Domain: business.com
    Name: default
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
2.	**Codecs** IP codec set 1 was used for the compliance test. Multiple codecs were listed in priority order to allow the codec used by a specific call to be negotiated during call establishment. The list includes the codecs the enterprise wishes to support within the normal trade-off of bandwidth versus voice quality. The example below shows the values 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
 2: G.729AB           n         2        20
 3:
```

Step	Description
3.	**Signaling Group** For the compliance test, signaling group 1 was used for the signaling group associated with the SIP trunk group between the Avaya S8300 Server and Avaya SES. Signaling group 1 was configured using the parameters highlighted below. All other fields were set as described in [3]. ▪ **Near-end Node Name**: ***procr*** This node name maps to the IP address of the Avaya S8300 Server. Node names are defined using the **change node-names ip** command. ▪ **Far-end Node Name**: ***SES*** This node name maps to the IP address of Avaya SES. ▪ **Far-end Network Region**: ***1*** This defines the IP network region which contains Avaya SES. ▪ **Far-end Domain**: ***business.com*** This domain is sent in the "To" header of SIP messages of calls using this signaling group.

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

 Group Number: 1              Group Type: sip
                         Transport Method: tls



   Near-end Node Name: procr                Far-end Node Name: SES
 Near-end Listen Port: 5061               Far-end Listen Port: 5061
                                       Far-end Network Region: 1
       Far-end Domain: business.com

                                               Bypass If IP Threshold Exceeded? n

         DTMF over IP: rtp-payload              Direct IP-IP Audio Connections? y
                                                          IP Audio Hairpinning? n
Enable Layer 3 Test? n
 Session Establishment Timer(min): 120
```

Step	Description
4.	**Trunk Group** For the compliance test, trunk group 1 was used for the SIP trunk group between the Avaya S8300 Server and Avaya SES. Trunk group 1 was configured using the parameters highlighted below. All other fields were set as described in [3]. ▪ **Signaling Group**: ***1*** This field is set to the signaling group shown in the previous step. ▪ **Number of Members: *24*** This field represents the number of trunks in the SIP trunk group. It determines how many simultaneous SIP calls can be supported by the configuration. Each SIP call between two SIP endpoints (whether internal or external) requires two SIP trunks for the duration of the call. Thus, a call from a SIP telephone to another SIP telephone will use two SIP trunks. A call between a non-SIP telephone and a SIP telephone will only use one trunk.

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

Group Number: 1                   Group Type: sip          CDR Reports: y
  Group Name: SES Trk Grp                COR: 1        TN: 1        TAC: 101
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                         Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                      Signaling Group: 1
                                                   Number of Members: 24
```

Step	Description
5.	On **Page 3**: ▪ Verify the **Numbering Format** field is set to ***public***. This field specifies the format of the calling party number sent to the far-end. ▪ The default values may be retained for the other fields.

```
add trunk-group 1                                                 Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                       Maintenance Tests? y

                     Numbering Format: public
                                                UUI Treatment: service-provider


                                                Replace Unavailable Numbers? n


 Show ANSWERED BY on Display? y
```

Step	Description
6.	Use the **change public-unknown-numbering 0** command to define the full calling party number to be sent to the far-end. Add an entry for the trunk group defined in **Step 7**. In the example shown below, all calls originating from a 5-digit extension beginning with 3 and routed across trunk group 1 will be sent as a 5 digit calling number. This calling party number will be sent to the far-end in the SIP "From" header.

```
change public-unknown-numbering 0                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext           Trk       CPN             CPN
Len Code          Grp(s)    Prefix          Len
                                                     Total Administered: 4
 5  3             1                         5           Maximum Entries: 240
 5  3             99                        5
```

7.	Automatic Route Selection (ARS) was used to route calls to the PSTN. In the compliance test, PSTN numbers that begin with 1732 were used for testing. The **change ars analysis *n*** command was used to add an entry in the ARS Digit Analysis Table for the dialed string beginning with ***n***. In the example shown, PSTN numbers that begin with 1732 and 11 digits long use route pattern 2. Route pattern 2 routes calls to the ISDN-PRI trunk between the main site and the PSTN shown in **Figure 1**. The configuration of the ISDN-PRI trunk is beyond the scope of these Application Notes.

```
change ars analysis 1732                                        Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location:  all           Percent Full:    3

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    1732                  11   11    2        fnpa         n
    174                   11   11    deny     fnpa         n
    175                   11   11    deny     fnpa         n
    176                   11   11    deny     fnpa         n
    177                   11   11    deny     fnpa         n
```

8.	The **change inc-call-handling-trmt trunk-group *n*** command was used to map a PSTN number to a station, where ***n*** is the trunk group number connected to the PSTN. The compliance test used trunk group 2 to connect to the PSTN. This trunk group configuration is not shown in these Application Notes. The example below shows two incoming 11-digit numbers being deleted and replaced with the extension number of the desired station.

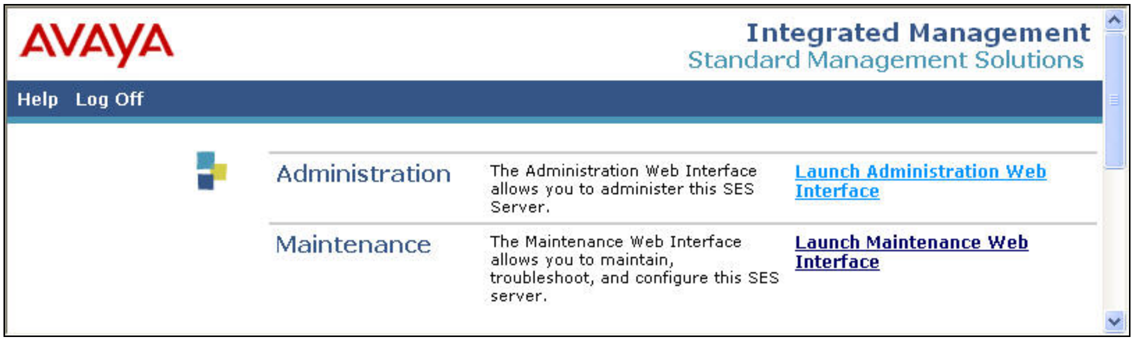
```
change inc-call-handling-trmt trunk-group 2                     Page   1 of   3
                       INCOMING CALL HANDLING TREATMENT
 Service/      Called    Called      Del Insert           Per Call Night
 Feature        Len      Number                           CPN/BN   Serv
 tie             11 17325551234      11  30104
 tie             11 17325551235      11  30101
```

4. Configure Avaya SES

This section covers the configuration of Avaya SES. Avaya SES is configured via an Internet browser using the administration web interface. It is assumed that the Avaya SES 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 to initially configure Avaya SES. For additional information on these installation tasks, refer to [5].

Each SIP endpoint used in the compliance test requires that a user and media server extension be created on Avaya SES. This configuration is not directly related to the interoperability of Session Director so it is not included here. These procedures are covered in [5].

Session Director acts as a back-to-back user agent (B2BUA). As such, Session Director will proxy user registrations and other SIP signaling messages to Avaya SES on behalf of the remote endpoints. Thus, Session Director appears as a set of endpoints to Avaya SES. As a result, no outbound proxy settings, address maps or trusted host settings are required on Avaya SES to support the remote users. Avaya SES is configured as a combined home/edge server.

Step	Description
1.	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 then select the **Launch Administration Web Interface** link from the main page as shown below.  The Administration Web Interface allows you to administer this SES Server. The Maintenance Web Interface allows you to maintain, troubleshoot, and configure this SES server.

Step	Description
2.	The Avaya SES **Top** page will be displayed as shown below. If any changes are made within Avaya SES, an **Update** link appears in the bottom of the blue navigation bar on the left side of the Avaya SES administration pages. It is necessary to click this link to commit the pending changes to the database.  **Manage Users** Add and delete Users. **Manage Conferencing** Add and delete Conference Extensions. **Manage Media Server Extensions** Add and delete Media Server Extensions. **Manage Emergency Contacts** Add and delete Emergency Contacts. **Manage Hosts** Add and delete Hosts. **Manage Media Servers** Add and delete Media Servers. **Manage Adjunct Systems** Add and delete Adjunct Systems. **Manage Services** Start and stop server processes on this host.
3.	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 parameter is a brief description of how to view the value from the Avaya SES administration home page shown in the previous step. • SIP Domain: ***business.com*** (To view, navigate to **Server Configuration→System Parameters**) • Host (SES IP address): ***10.75.5.6*** (To view, navigate to **Host→List**; Click **Edit**) • Media Server (Avaya Communication Manager) Interface Name: ***CMeast*** (To view, navigate to **Media Server→List**; Click **Edit**) • SIP Trunk IP Address (Avaya S8300 Server IP address): ***10.75.5.2*** (To view, navigate to **Media Server→List**; Click **Edit**)

5. Configure the Avaya SIP Telephones

The SIP telephones at the main office will use Avaya SES as the registrar and SIP proxy. The SIP telephones of the remote users will use the public IP address of Session Director as the registrar and SIP proxy.

The table below shows an example of the SIP telephone networking settings for both the main site and remote users.

	Main Site	**Remote User w/o NAT**	**Remote User w/ NAT**
Extension	30104	30103	30101
IP Address	10.75.5.153	46.16.2.157	192.168.2.10
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
Call Server (Registrar/Proxy)	10.75.5.6	46.14.2.80	46.14.2.80
Router	10.75.5.1	46.16.2.1	192.168.2.1
File Server	10.75.10.52	46.14.2.80	46.14.2.80

Table 2: Telephone Network Settings

6. Configure Acme Packet Net-Net Session Director

This section describes the configuration of Session Director. Session Director was configured via the administrative command line interface. This section assumes the reader is familiar with accessing and configuring Session Director.

Session Director was configured as a policy based bridge in a hosted NAT traversal environment. This is one of the base configurations described in [7]. A graphical representation of this configuration is shown in **Figure 2**. It shows the internal components needed for this configuration. Each of these components is defined in the Session Director configuration file which is included in **Appendix A**. This is the configuration used for the compliance test.

This section will not attempt to describe each component in its entirety but instead will highlight critical fields in each component which relates directly to the connection to Avaya SES or the Avaya SIP endpoints. These same fields are highlighted in Appendix A. The remaining fields are generally the default/standard value used by Session Director for that field. For additional details on the administration of Session Director, refer to [7]. The configuration described in this section was performed from the Session Director command line interface.

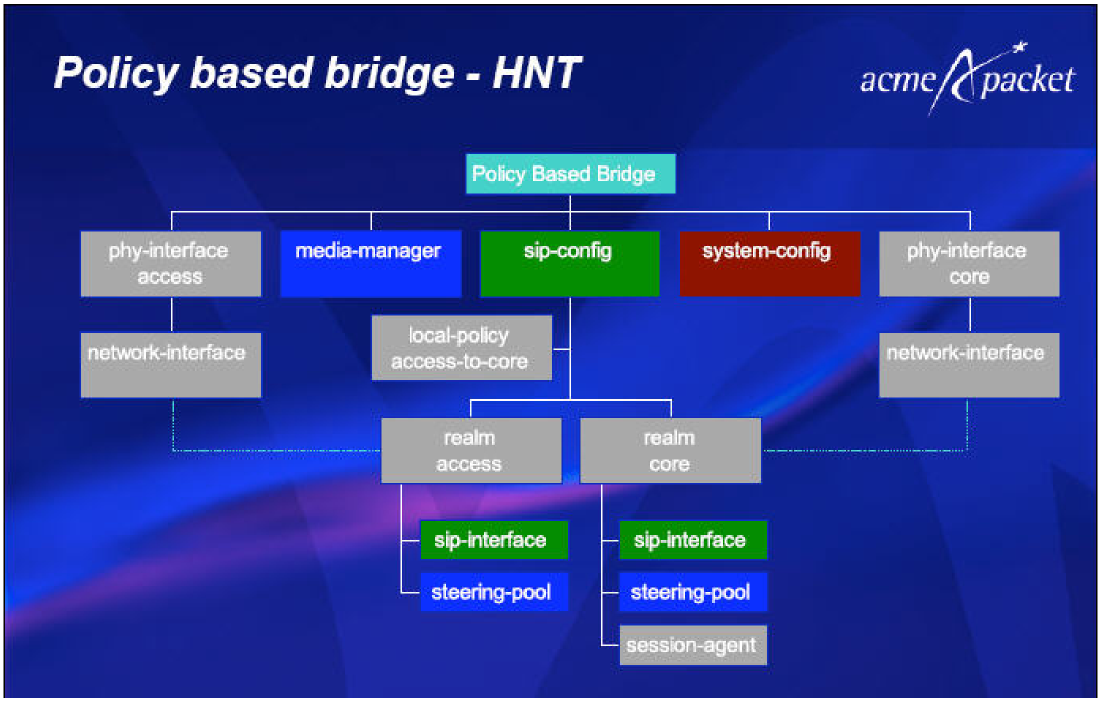


Figure 2: Graphical Representation of the Session Director Configuration

6.1. System Configuration

The system configuration defines system-wide parameters for Session Director.

The key system configuration (***system-config***) fields are:

- **hostname**: The name assigned to the Session Director.
- **description**: A short description of the configuration.
- **default-gateway**: The IP address of the default gateway. In this case, the default gateway is the next hop IP address for traffic leaving the enterprise.

```
system-config
        hostname                      DevConnect
        description                   Avaya DevConnect Station Feature Test
        location
        mib-system-contact
        mib-system-name
        mib-system-location
        snmp-enabled                  enabled
        enable-snmp-auth-traps        disabled
        enable-snmp-syslog-notify     disabled
        enable-snmp-monitor-traps     disabled
        enable-env-monitor-traps      disabled
        snmp-syslog-his-table-length  1
        snmp-syslog-level             WARNING
        system-log-level              WARNING
        process-log-level             NOTICE
        process-log-ip-address        0.0.0.0
        process-log-port              0
        call-trace                    disabled
        internal-trace                disabled
        log-filter                    all
        default-gateway               46.14.2.1
        restart                       enabled
        exceptions
        telnet-timeout                300
        console-timeout               300
        remote-control                enabled
        link-redundancy-state         disabled
        last-modified-date            2007-06-12 09:34:46
```

6.2. Physical and Network Interfaces

As part of the compliance test, the Ethernet interface slot 0 / port 0 of Session Director was connected to the external untrusted network. Ethernet slot 1 / port 0 was connected to the internal corporate LAN. A network interface was defined for each physical interface to assign it a routable IP address.

The key physical interface (***phy-interface***) fields are:

- **name**: A descriptive string used to reference the Ethernet interface.
- **operation-type**: ***Media*** This setting indicates both signaling and rtp packets use this interface.
- **slot / port**: The identifier of the specific front panel Ethernet interface used.

```
phy-interface
        name                           M00
        operation-type                 Media
        port                           0
        slot                           0
        virtual-mac
        admin-state                    enabled
        auto-negotiation               enabled
        duplex-mode                    FULL
        speed                          100
        last-modified-date             2006-12-20 10:15:46
phy-interface
        name                           M10
        operation-type                 Media
        port                           0
        slot                           1
        virtual-mac
        admin-state                    enabled
        auto-negotiation               enabled
        duplex-mode                    FULL
        speed                          100
        last-modified-date             2006-12-20 10:15:56
```

The key network interface (***network-interface***) fields are:

- **name**: The name of the physical interface (defined above) that is associated with this network interface.
- **ip-address**: The IP address assigned to this interface.
- **netmask**: Subnet mask for the IP subnet.
- **gateway**: The subnet gateway address.
- **hip-ip-list**: The allowed ip address list to accept administrative traffic (such as icmp ping).
- **icmp-address**: The ip address used to pass icmp pings.

```
network-interface
        name                           M00
        sub-port-id                    0
        hostname
        ip-address                     46.14.2.80
        pri-utility-addr
        sec-utility-addr
        netmask                        255.255.255.0
        gateway                        46.14.2.1
        sec-gateway
        gw-heartbeat
                state                          disabled
                heartbeat                      0
                retry-count                    0
                retry-timeout                  1
                health-score                   0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                    11
        hip-ip-list                    46.14.2.80
        ftp-address
        icmp-address                   46.14.2.80
        snmp-address
        telnet-address
        last-modified-date             2007-06-12 09:08:22
network-interface
        name                           M10
        sub-port-id                    0
        hostname
        ip-address                     10.75.5.31
        pri-utility-addr
        sec-utility-addr
        netmask                        255.255.255.0
        gateway                        10.75.5.1
        sec-gateway
        gw-heartbeat
                state                          disabled
                heartbeat                      0
                retry-count                    0
                retry-timeout                  1
                health-score                   0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                    11
        hip-ip-list                    10.75.5.31
        ftp-address
        icmp-address                   10.75.5.31
        snmp-address
        telnet-address
        last-modified-date             2007-06-12 09:30:37
```

6.3. Realm

The realm assigns common logical characteristics to be used by one or more interfaces, address spaces, etc. Two realms were defined for the compliance test. The ***access*** realm was defined for the external network and the ***core*** realm was defined for the internal network.

The key realm (***realm-config***) fields are:

- **identifier**: A string used as a realm reference. This will be used by the configuration of other components.
- **network interfaces**: The network interfaces located in this realm.

```
realm-config
        identifier                     access
        addr-prefix                    0.0.0.0
        network-interfaces
                                       M00:0
        mm-in-realm                    enabled
        mm-in-network                  enabled
        mm-same-ip                     enabled
        mm-in-system                   enabled
        …
        < text removed for brevity >
        …
realm-config
        identifier                     core
        addr-prefix                    0.0.0.0
        network-interfaces
                                       M10:0
        mm-in-realm                    enabled
        mm-in-network                  enabled
        mm-same-ip                     enabled
        mm-in-system                   enabled

        < text removed for brevity >
```

6.4. SIP Interface

The SIP interface (***sip-interface***) defines the receiving characteristics of the SIP interfaces on Session Director. Two SIP interfaces were defined; one for each realm. Each SIP interface contained two sip ports entries so that Session Director could use UDP or TCP for SIP signaling.

The key SIP interface (***sip-interface***) fields are:

- **realm-id**: The name of the realm to which this interface is assigned.
- **sip port**
    - **address**: The ip address assigned to this sip-interface.
    - **port**: The port assigned to this sip-interface. Port 5060 is used for both UDP and TCP.
    - **transport-protocol**: The transport method used for this interface. One sip port used UDP and the other used TCP.

```
sip-interface
        state                          enabled
        realm-id                       access
        sip-port
                address                        46.14.2.80
                port                           5060
                transport-protocol             UDP
                tls-profile
                allow-anonymous                registered
        sip-port
                address                        46.14.2.80
                port                           5060
                transport-protocol             TCP
                tls-profile
                allow-anonymous                registered
        carriers
        trans-expire                   0
        invite-expire                  0

       < text removed for brevity >

sip-interface
        state                          enabled
        realm-id                       core
        sip-port
                address                        10.75.5.31
                port                           5060
                transport-protocol             UDP
                tls-profile
                allow-anonymous                all
        sip-port
                address                        10.75.5.31
                port                           5060
                transport-protocol             TCP
                tls-profile
                allow-anonymous                all
        carriers
        trans-expire                   0
        invite-expire                  0

       < text removed for brevity >
```

6.5. Steering Pools

Steering pools define the range of UDP ports to be used for the RTP voice stream. Two steering pools were defined; one for each realm.

The key steering pool (***steering-pool***) fields are:

- **ip-address:** The address of the interface on Session Director.
- **start-port:** An even number of the port that begins the range.
- **end-port:** An odd number of the port that ends the range.
- **realm-id:** The realm to which this steering pool is assigned.

```
steering-pool
        ip-address                     46.14.2.80
        start-port                     49152
        end-port                       65535
        realm-id                       access
        network-interface
        last-modified-date             2007-06-12 09:09:46
steering-pool
        ip-address                     10.75.5.31
        start-port                     49152
        end-port                       65535
        realm-id                       core
        network-interface
        last-modified-date             2006-12-20 10:16:56
```

6.6. Local Policy

Local policy controls the routing of SIP calls from one realm to another.

The key local policy (***local-policy***) fields are:

- **from-address**: A policy filter indicating the originating IP address to which this policy applies. An asterisk ("*") indicates any IP address.
- **to-address**: A policy filter indicating the terminating IP address to which this policy applies. An asterisk ("*") indicates any IP address.
- **source-realm**: A policy filter indicating the matching realm in order for the policy rules to be applied.
- **state**: The activation state of the policy. Set to ***enabled***.
- **policy-attribute**
  - **next-hop**: The IP address where the message should be sent when the policy rules match.
  - **realm**: The realm associated with the next-hop IP address.

In this case, the policy provides a simple routing rule indicating that messages originating from the ***access*** realm are to be sent to the ***core*** realm via IP address 10.75.5.6 (Avaya SES).

```
local-policy
        from-address                   *
        to-address                     *
        source-realm                   access
        activate-time                  N/A
        deactivate-time                N/A
        state                          enabled
        policy-priority                none
        last-modified-date             2006-12-20 10:14:50
        policy-attribute
                next-hop                       10.75.5.6
                realm                          core
                action                         none
                terminate-recursion            disabled
                carrier
                start-time                     0000
                end-time                       2400
                days-of-week                   U-S
                cost                           0
                app-protocol                   SIP
                state                          enabled
                media-profiles
```

6.7. Static Flow

A static flow creates a path for data other than SIP traffic to pass through Session Director. Acme Packet recommends that any data required to support the SIP communication pass through Session Director. Thus, two static flows were defined for the compliance test. One static flow allowed the Avaya 4600 Series SIP Telephones to access their configuration files using TFTP via Session Director. The other static flow allowed the Avaya one-X Desktop Editions to access their license server using HTTP via Session Director.

The key static flow (***static flow***) fields are:

- **in-realm-id**: The realm where the flow originates.
- **in-source**: This field was left blank. Thus, the incoming source IP address can be any value.
- **in-destination**: The incoming destination IP address and port number of the flow. In the case of the compliance test, Session Director appears as the destination server to the endpoints. Thus, the incoming destination IP address is the external IP address of Session Director.
- **out-realm-id**: The realm where the flow will terminate.
- **out-source**: The outgoing source IP address and port number. Session Director appears as the originator of this traffic on the outbound side. Thus, the outgoing source IP address is the internal IP address of Session Director.
- **out-destination**: The destination IP address and port number of the flow. In the case of the TFTP traffic, the destination is the TFTP server (10.75.10.52:69). In the case of the HTTP traffic, the destination is the license server which is Avaya SES (10.75.5.6:80).
- **protocol**: The layer 3 protocol. The protocol is ***UDP*** for TFTP or ***TCP*** for HTTP.
- **alg-type**: Some data traffic requires application layer gateway (ALG) processing of the IP payload. TFTP requires this processing, so the field was set to ***TFTP*** for the TFTP traffic. HTTP does not require an ALG so this field was set to ***NAPT***, which indicates typical network address and port translation (NAPT).
- **start-port**: The starting port of the port range to use for this flow.
- **end-port**: The last port of the port range to use for this flow.

Static flow configuration for TFTP:

```
static-flow
        in-realm-id                    access
        in-source                      0.0.0.0
        in-destination                 46.14.2.80:69
        out-realm-id                   core
        out-source                     10.75.5.31
        out-destination                10.75.10.52:69
        protocol                       UDP
        alg-type                       TFTP
        start-port                     40000
        end-port                       40999
        flow-time-limit                0
        initial-guard-timer            60
        subsq-guard-timer              60
        average-rate-limit             0
        last-modified-date             2007-06-12 11:03:07
```

Static flow configuration for HTTP:

```
static-flow
        in-realm-id                    access
        in-source                      0.0.0.0
        in-destination                 46.14.2.80:80
        out-realm-id                   core
        out-source                     10.75.5.31
        out-destination                10.75.5.6:80
        protocol                       TCP
        alg-type                       NAPT
        start-port                     41000
        end-port                       41999
        flow-time-limit                0
        initial-guard-timer            60
        subsq-guard-timer              60
        average-rate-limit             0
            last-modified-date             2007-06-12 11:06:21
```

6.8. Host Routes

A host route was required to properly route traffic to the TFTP server since it was connected to a subnet which was not directly connected to either port of Session Director.

The key host route (***host-routes***) fields are:

- **dest-network**: The network address where the TFTP server was connected.
- **netmask**: The network mask for the **dest-network**.
- **gateway**: The default gateway Session Director should use to reach the **dest-network**.

```
host-routes
        dest-network                   10.75.10.0
        netmask                        255.255.255.0
        gateway                        10.75.5.1
        last-modified-date             2007-06-12 09:34:24
```

7. Interoperability Compliance Testing

This section describes the compliance testing used to verify the interoperability of Acme Packet Net-Net Session Director with Avaya SIP Enablement Services and Avaya Communication Manager. This section covers the general test approach and the test results.

7.1. General Test Approach

The general test approach was to make calls through Session Director using various codec settings and exercising common PBX features. Calls were made between the remote users and the main site, between the remote users and the PSTN, and between the remote users.

7.2. Test Results

Session Director passed compliance testing. The following features and functionality were verified. Any observations related to these tests are listed at the end of this section.

- Successful registrations of the remote endpoints at the main site.
- Calls between a remote user without NAT and both SIP and non-SIP endpoints at the main site.

- Calls between a remote user with NAT and both SIP and non-SIP endpoints at the main site.
- Calls between a remote user with and without NAT and the PSTN.
- Calls between a remote user without NAT and a remote user with NAT.
- Calls between remote users behind the same NAT.
- Calls between remote users behind different NATs.
- Calls using various SIP telephone types including the Avaya 4600 Series IP Telephones (with SIP firmware), and the Avaya one-X Desktop Edition (SIP Softphone). The Avaya one-X Desktop Edition was tested using TCP instead of the default TLS. This was because the particular Session Director unit used for the testing did not have the hardware installed necessary to support TLS.
- G.711u and G.729AB codec support
- Proper recognition of DTMF transmissions by navigating voicemail menus.
- Proper operation of voicemail with message waiting indicators (MWI).
- PBX features including Hold, Transfer, Call Waiting, Call Forwarding and Conference.
- Extended telephony features using Avaya Communication Manager Feature Name Extensions (FNE) such as Conference On Answer, Call Park, Call Pickup, Automatic Redial and Send All Calls. For more information on FNEs, please refer to [4].
- Proper system recovery after a Session Director restart and loss of IP connection.

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 group is in-service.
- From the Avaya Communication Manager SAT, use the **status trunk-group** command to verify that the SIP trunk group is in-service.
- From the Avaya SES web administration interface, verify that all remote endpoints are registered with Avaya SES using the private IP address of Session Director. To view, navigate to **Users→Registered Users**.
- Verify that calls can be placed between a remote user without NAT and SIP and non-SIP endpoints at the main site.
- Verify that calls can be placed between a remote user with NAT and SIP and non-SIP endpoints at the main site.
- Verify that calls can be placed between remote users with and without NAT.

9. Support

For technical support on Session Director, contact Acme Packet via the support link at www.acmepacket.com or send email to support@acmepacket.com.

10. Conclusion

Acme Packet Net-Net Session Director passed compliance testing. These Application Notes describe the procedures required to configure Acme Packet Net-Net Session Director to interoperate with Avaya SIP Enablement Services and Avaya Communication Manager to support remote users with NAT traversal as shown in **Figure 1**.

11. Additional References

[1] *Feature Description and Implementation For Avaya Communication Manager*, Doc # 555-245-205, Issue 5.0, February 2007.

[2] *Administrator Guide for Avaya Communication Manager*, Doc # 03-300509, Issue 3.1, February 2007.

[3] *SIP support in Avaya Communication Manager Running on the Avaya S8300, S8400, S8500 Series and S8700 Series Media Server*, Doc # 555-245-206, Issue 6.1, March 2007.

[4] *Avaya Extension to Cellular and Off-PBX Station (OPS) Installation and Administration Guide Release 3.0*, version 6.0, Doc # 210-100-500, Issue 9, June 2005

[5] *Installing and Administering SIP Enablement Services*, Doc# 03-600768, Issue 4, May 2007.

[6] *Avaya IA 770 INTUITY AUDIX Messaging Application*, Doc # 11-300532, May 2005.

[7] *Session Director Installation Guide*.

[8] *Session Director Administration Guide*.

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

Product documentation for Session Director can be obtained from Acme Packet.

Appendix A: Session Director Configuration File

Included below is the Session Director configuration file used during the compliance testing.

```
host-routes
        dest-network                   10.75.10.0
        netmask                        255.255.255.0
        gateway                        10.75.5.1
        last-modified-date             2007-06-12 09:34:24
local-policy
        from-address                   *
        to-address                     *
        source-realm                   access
        activate-time                  N/A
        deactivate-time                N/A
        state                          enabled
        policy-priority                none
        last-modified-date             2006-12-20 10:14:50
        policy-attribute
                next-hop                       10.75.5.6
                realm                          core
                action                         none
                terminate-recursion            disabled
                carrier
                start-time                     0000
                end-time                       2400
                days-of-week                   U-S
                cost                           0
                app-protocol                   SIP
                state                          enabled
                media-profiles
media-manager
        state                          enabled
        latching                       enabled
        flow-time-limit                86400
        initial-guard-timer            300
        subsq-guard-timer              300
        tcp-flow-time-limit            86400
        tcp-initial-guard-timer        300
        tcp-subsq-guard-timer          300
        tcp-number-of-ports-per-flow   2
        hnt-rtcp                       disabled
        algd-log-level                 NOTICE
        mbcd-log-level                 NOTICE
        home-realm-id                  access
        red-flow-port                  1985
        red-mgcp-port                  1986
        red-max-trans                  10000
        red-sync-start-time            5000
        red-sync-comp-time             1000
        max-signaling-bandwidth        10000000
        max-untrusted-signaling        100
        min-untrusted-signaling        30
        app-signaling-bandwidth        0
        tolerance-window               30
        rtcp-rate-limit                0
        min-media-allocation           32000
```

```
        min-trusted-allocation         1000
        deny-allocation                1000
        anonymous-sdp                  disabled
        arp-msg-bandwidth              32000
        fragment-msg-bandwidth         0
        last-modified-date             2007-06-12 09:33:00
network-interface
        name                           M00
        sub-port-id                    0
        hostname
        ip-address                     46.14.2.80
        pri-utility-addr
        sec-utility-addr
        netmask                        255.255.255.0
        gateway                        46.14.2.1
        sec-gateway
        gw-heartbeat
                state                          disabled
                heartbeat                      0
                retry-count                    0
                retry-timeout                  1
                health-score                   0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                    11
        hip-ip-list                    46.14.2.80
        ftp-address
        icmp-address                   46.14.2.80
        snmp-address
        telnet-address
        last-modified-date             2007-06-12 09:08:22
network-interface
        name                           M10
        sub-port-id                    0
        hostname
        ip-address                     10.75.5.31
        pri-utility-addr
        sec-utility-addr
        netmask                        255.255.255.0
        gateway                        10.75.5.1
        sec-gateway
        gw-heartbeat
                state                          disabled
                heartbeat                      0
                retry-count                    0
                retry-timeout                  1
                health-score                   0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                    11
        hip-ip-list                    10.75.5.31
        ftp-address
        icmp-address                   10.75.5.31
```

```
        snmp-address
        telnet-address
        last-modified-date             2007-06-12 09:30:37
phy-interface
        name                           M00
        operation-type                 Media
        port                           0
        slot                           0
        virtual-mac
        admin-state                    enabled
        auto-negotiation               enabled
        duplex-mode                    FULL
        speed                          100
        last-modified-date             2006-12-20 10:15:46
phy-interface
        name                           M10
        operation-type                 Media
        port                           0
        slot                           1
        virtual-mac
        admin-state                    enabled
        auto-negotiation               enabled
        duplex-mode                    FULL
        speed                          100
        last-modified-date             2006-12-20 10:15:56
realm-config
        identifier                     access
        addr-prefix                    0.0.0.0
        network-interfaces
                                       M00:0
        mm-in-realm                    enabled
        mm-in-network                  enabled
        mm-same-ip                     enabled
        mm-in-system                   enabled
        bw-cac-non-mm                  disabled
        msm-release                    disabled
        qos-enable                     disabled
        generate-UDP-checksum          disabled
        max-bandwidth                  0
        ext-policy-svr
        max-latency                    0
        max-jitter                     0
        max-packet-loss                0
        observ-window-size             0
        parent-realm
        dns-realm
        media-policy
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid
        class-profile
        average-rate-limit             0
        access-control-trust-level     none
        invalid-signal-threshold       0
        maximum-signal-threshold       0
        untrusted-signal-threshold     0
```

```
        deny-period                    30
        symmetric-latching             disabled
        pai-strip                      disabled
        trunk-context
        early-media-allow
        additional-prefixes
        restricted-latching            none
        restriction-mask               32
        accounting-enable              enabled
        user-cac-mode                  none
        user-cac-bandwidth             0
        user-cac-sessions              0
        net-management-control         disabled
        delay-media-update             disabled
        codec-policy
        codec-manip-in-realm           disabled
        last-modified-date             2007-06-12 13:24:08
realm-config
        identifier                     core
        addr-prefix                    0.0.0.0
        network-interfaces
                                       M10:0
        mm-in-realm                    enabled
        mm-in-network                  enabled
        mm-same-ip                     enabled
        mm-in-system                   enabled
        bw-cac-non-mm                  disabled
        msm-release                    disabled
        qos-enable                     disabled
        generate-UDP-checksum          disabled
        max-bandwidth                  0
        ext-policy-svr
        max-latency                    0
        max-jitter                     0
        max-packet-loss                0
        observ-window-size             0
        parent-realm
        dns-realm
        media-policy
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid
        class-profile
        average-rate-limit             0
        access-control-trust-level     none
        invalid-signal-threshold       0
        maximum-signal-threshold       0
        untrusted-signal-threshold     0
        deny-period                    30
        symmetric-latching             disabled
        pai-strip                      disabled
        trunk-context
        early-media-allow
        additional-prefixes
        restricted-latching            none
        restriction-mask               32
```

```
        accounting-enable              enabled
        user-cac-mode                  none
        user-cac-bandwidth             0
        user-cac-sessions              0
        net-management-control         disabled
        delay-media-update             disabled
        codec-policy
        codec-manip-in-realm           disabled
        last-modified-date             2006-12-20 10:16:14
sip-config
        state                          enabled
        operation-mode                 dialog
        dialog-transparency            enabled
        home-realm-id                  access
        egress-realm-id
        nat-mode                       None
        registrar-domain               *
        registrar-host                 *
        registrar-port                 5060
        init-timer                     500
        max-timer                      4000
        trans-expire                   32
        invite-expire                  180
        inactive-dynamic-conn          32
        pac-method
        pac-interval                   10
        pac-strategy                   PropDist
        pac-load-weight                1
        pac-session-weight             1
        pac-route-weight               1
        pac-callid-lifetime            600
        pac-user-lifetime              3600
        red-sip-port                   1988
        red-max-trans                  10000
        red-sync-start-time            5000
        red-sync-comp-time             1000
        add-reason-header              disabled
        sip-message-len                4096
        enum-sag-match                 disabled
        extra-method-stats             disabled
        options                        max-udp-length=0
        last-modified-date             2007-06-13 09:45:51
sip-interface
        state                          enabled
        realm-id                       access
        sip-port
                address                        46.14.2.80
                port                           5060
                transport-protocol             UDP
                tls-profile
                allow-anonymous                registered
        sip-port
                address                        46.14.2.80
                port                           5060
                transport-protocol             TCP
                tls-profile
                allow-anonymous                registered
```

```
        carriers
        trans-expire                   0
        invite-expire                  0
        max-redirect-contacts          0
        proxy-mode
        redirect-action
        contact-mode                   none
        nat-traversal                  always
        nat-interval                   180
        tcp-nat-interval               90
        registration-caching           enabled
        min-reg-expire                 300
        registration-interval          1800
        route-to-registrar             enabled
        secured-network                disabled
        teluri-scheme                  disabled
        uri-fqdn-domain
        trust-mode                     all
        max-nat-interval               3600
        nat-int-increment              10
        nat-test-increment             30
        sip-dynamic-hnt                disabled
        stop-recurse                   401,407
        port-map-start                 0
        port-map-end                   0
        in-manipulationid
        out-manipulationid
        sip-ims-feature                disabled
        operator-identifier
        anonymous-priority             none
        max-incoming-conns             0
        per-src-ip-max-incoming-conns  0
        inactive-conn-timeout          0
        network-id
        ext-policy-server
        default-location-string
        charging-vector-mode           pass
        charging-function-address-mode pass
        ccf-address
        ecf-address
        term-tgrp-mode                 none
        implicit-service-route         disabled
        rfc2833-payload                101
        rfc2833-mode                   transparent
        constraint-name
        response-map
        local-response-map
        tcp-keepalive                  none
        last-modified-date             2007-06-13 10:27:37
sip-interface
        state                          enabled
        realm-id                       core
        sip-port
                address                        10.75.5.31
                port                           5060
                transport-protocol             UDP
                tls-profile
```

```
                allow-anonymous                all
        sip-port
                address                        10.75.5.31
                port                           5060
                transport-protocol             TCP
                tls-profile
                allow-anonymous                all
        carriers
        trans-expire                   0
        invite-expire                  0
        max-redirect-contacts          0
        proxy-mode
        redirect-action
        contact-mode                   none
        nat-traversal                  none
        nat-interval                   30
        tcp-nat-interval               90
        registration-caching           disabled
        min-reg-expire                 300
        registration-interval          3600
        route-to-registrar             disabled
        secured-network                disabled
        teluri-scheme                  disabled
        uri-fqdn-domain
        trust-mode                     all
        max-nat-interval               3600
        nat-int-increment              10
        nat-test-increment             30
        sip-dynamic-hnt                disabled
        stop-recurse                   401,407
        port-map-start                 0
        port-map-end                   0
        in-manipulationid
        out-manipulationid
        sip-ims-feature                disabled
        operator-identifier
        anonymous-priority             none
        max-incoming-conns             0
        per-src-ip-max-incoming-conns  0
        inactive-conn-timeout          0
        network-id
        ext-policy-server
        default-location-string
        charging-vector-mode           pass
        charging-function-address-mode pass
        ccf-address
        ecf-address
        term-tgrp-mode                 none
        implicit-service-route         disabled
        rfc2833-payload                101
        rfc2833-mode                   transparent
        constraint-name
        response-map
        local-response-map
        tcp-keepalive                  none
        last-modified-date             2007-06-13 10:28:15
static-flow
```

```
        in-realm-id                    access
        in-source                      0.0.0.0
        in-destination                 46.14.2.80:69
        out-realm-id                   core
        out-source                     10.75.5.31
        out-destination                10.75.10.52:69
        protocol                       UDP
        alg-type                       TFTP
        start-port                     40000
        end-port                       40999
        flow-time-limit                0
        initial-guard-timer            60
        subsq-guard-timer              60
        average-rate-limit             0
        last-modified-date             2007-06-12 11:03:07
static-flow
        in-realm-id                    access
        in-source                      0.0.0.0
        in-destination                 46.14.2.80:80
        out-realm-id                   core
        out-source                     10.75.5.31
        out-destination                10.75.5.6:80
        protocol                       TCP
        alg-type                       NAPT
        start-port                     41000
        end-port                       41999
        flow-time-limit                0
        initial-guard-timer            60
        subsq-guard-timer              60
        average-rate-limit             0
        last-modified-date             2007-06-12 11:06:21
steering-pool
        ip-address                     46.14.2.80
        start-port                     49152
        end-port                       65535
        realm-id                       access
        network-interface
        last-modified-date             2007-06-12 09:09:46
steering-pool
        ip-address                     10.75.5.31
        start-port                     49152
        end-port                       65535
        realm-id                       core
        network-interface
        last-modified-date             2006-12-20 10:16:56
system-config
        hostname                       DevConnect
        description                    Avaya DevConnect Station Feature Test
        location
        mib-system-contact
        mib-system-name
        mib-system-location
        snmp-enabled                   enabled
        enable-snmp-auth-traps         disabled
        enable-snmp-syslog-notify      disabled
        enable-snmp-monitor-traps      disabled
        enable-env-monitor-traps       disabled
```

```
        snmp-syslog-his-table-length   1
        snmp-syslog-level              WARNING
        system-log-level               WARNING
        process-log-level              NOTICE
        process-log-ip-address         0.0.0.0
        process-log-port               0
        call-trace                     disabled
        internal-trace                 disabled
        log-filter                     all
        default-gateway                46.14.2.1
        restart                        enabled
        exceptions
        telnet-timeout                 300
        console-timeout                300
        remote-control                 enabled
        link-redundancy-state          disabled
        last-modified-date             2007-06-12 09:34:46
task done
```

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 Developer*Connection* Program at devconnect@avaya.com.