Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Direct SIP Trunking from Avaya Communication Manager using an Acme Packet Net-Net Session Director and a SIP PSTN Gateway – Issue 1.0

Abstract

These Application Notes describe the configuration of Direct SIP Trunking from Avaya Communication Manager to an Acme Packet Net-Net Session Director and a SIP PSTN gateway. The SIP PSTN gateway provided ISDN PRI trunks to a telecommunications service provider network for PSTN interoperability. In this configuration, an Avaya Session Enablement Services (SES) edge server is not used as part of the SIP trunking solution.

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 describe the configuration of Direct SIP Trunking from Avaya Communication Manager to an Acme Packet Net-Net Session Director and a SIP PSTN gateway. The SIP PSTN gateway provided ISDN PRI trunks to a telecommunications service provider network for PSTN interoperability. In this configuration, an Avaya Session Enablement Services (SES) edge server is not used as part of the SIP trunking solution. This configuration (not involving the SES) will be referred to in these Application Notes as "Direct SIP Trunking".

Direct SIP Trunking uses the Acme Packet Net-Net Session Director (SD) features to distribute SIP signaling for incoming calls to multiple Avaya Communication Manger C-LAN interfaces. This provides for additional capacity, load balancing and survivability options (upon a C-LAN failure or isolation event). In addition, the Acme Packet SD performs conversion between the TCP transport for SIP messages used by the Avaya Communication Manager and the UDP transport commonly used by other communication elements and service provider networks.

The configuration tested is shown in **Figure 1**. The Acme Packet SD is a session border controller that acts as an intermediary to manage the SIP signaling and RTP media packets between Avaya Communication Manager and other SIP terminations (such as the SIP PSTN gateway or a SIP trunk directly to a telecommunication service provider.) The session border controller often resides at the boundary of the enterprise customer's IP network and serves as a security device to isolate the customer's internal network from the public domain. Within these Application Notes, the networking was configured in a similar manner; the subnet used by Avaya Communication Manager was not directly connected to the subnet used by the SIP PSTN gateway and all SIP and RTP packets were routed through the Acme Packet SD. Other configurations are possible, but not addressed herein.

These Application Notes specifically address the following capabilities that were verified within the Avaya Solution and Interoperability Test Lab in Lincroft, NJ:

- Incoming PSTN calls to Avaya Communication Manager IP and Digital telephones.
- Outbound PSTN calls from Avaya (H.323) IP and Digital telephones.
- Trunk to trunk forwarding (tandem routing) of an inbound PSTN call to another PSTN telephone via Avaya Communication Manager.
- G.711mu and G.729a codecs.
- Direct IP-IP media between (H.323) IP telephones and SIP trunks.
- Direct IP-IP media for SIP trunk to SIP trunk forwarded calls.
- Use of hunt groups, ACD splits, announcements, vectors and auto-attendant applications.
- Load balancing of incoming calls across multiple C-LAN SIP interfaces.
- Alternate routing upon failure of C-LAN SIP interface for incoming and outgoing calls.

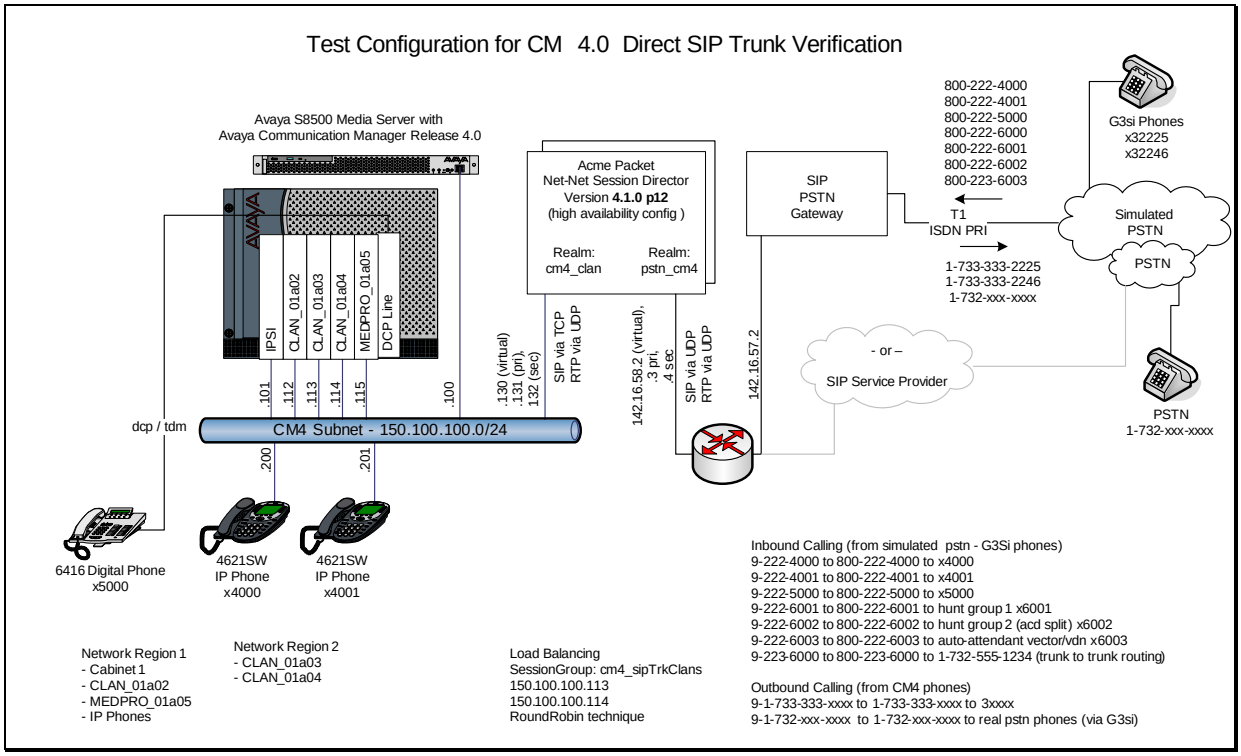

Figure 1 – Direct SIP Trunking Test Configuration

2. Equipment and Software Validated

The following products and software were used for the configuration in **Figure 1**.

Component	Version
Avaya	
Avaya S8500B Media Server	Communication Manager 4.0 (R014x.00.0.730.5)
Avaya G650 Media Gateway	
TN2312BP IP Server Interface (IPSI) TN799DP Control-LAN (C-LAN)	HW12 FW036 HW01 FW017
TN2602AP IP Media Processor (Medpro)	HW02 FW025
TN2224CP Digital Line	HW08 FW015
Avaya 4621SW IP (H.323) Telephones	Release 2.2 (a20d01b2_2.bin)
Avaya 6416D+M Digital Telephone	n/a
Acme Packet	
Net-Net 4000 Session Director (2 units in a high availability configuration)	4.1.0 P12 Licensed Features: SIP, Routing, Load Balancing, High Availability, PAC

Table 1 – Equipment and Version

3. Configure Avaya Communication Manager

The Avaya Communication Manager was installed and configured for basic station to station calling prior to beginning the configuration shown in these Application Notes. These basic configuration details are outside the scope of the SIP trunking application and not included here.

3.1. SIP Trunk Configuration

3.1.1. Verify System Capacity and Required Features

The Avaya Communication Manager license controls the customer options. Contact an authorized Avaya sales representative for assistance if insufficient capacity exists or a required feature is not enabled.

Verify that there is sufficient remaining SIP trunk capacity available for the SIP PSTN gateway as well as any other SIP trunking applications in use.

This is done by displaying Page 2 of the **System-Parameters Customer-Options** form. The number of SIP trunks available to assign to new or existing trunk groups is the difference between the **Maximum Administered SIP Trunks** and the **USED** value.

```
display system-parameters customer-options                    Page   2 of  10
                               OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 0     0
           Maximum Concurrently Registered IP Stations: 5     2
             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: 100   20

   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   2
         Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 0     0

        (NOTE: You must logoff & login to effect the permission changes.)
```

Figure 2: System-Parameters Customer-Options Form – Page 2

Verify that the Automatic Route Selection (ARS) feature is enabled on Page 3 of the **System-Parameters Customer-Options** form.

```
display system-parameters customer-options                    Page   3 of  10
                              OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? n          Audible Message Waiting? n
        Access Security Gateway (ASG)? n              Authorization Codes? n
        Analog Trunk Incoming Call ID? n                      CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? n                        CAS Main? n
Answer Supervision by Call Classifier? n                Change COR by FAC? n
                                 ARS? y  Computer Telephony Adjunct Links? n
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? n
          ARS/AAR Dialing without FAC? n                      DCS (Basic)? n
          ASAI Link Core Capabilities? n                DCS Call Coverage? n
          ASAI Link Plus Capabilities? n               DCS with Rerouting? n
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? n
              ATM WAN Spare Processor? n                          DS1 MSP? n
                                 ATMS? n             DS1 Echo Cancellation? n
                  Attendant Vectoring? n



        (NOTE: You must logoff & login to effect the permission changes.)
```

Figure 3: System-Parameters Customer-Options Form – Page 3

3.1.2. Determine Node Names

Use the "change node-names ip" command to view (or assign) the node names to be used in this configuration.

- "acme_cm4-side" and "150.100.100.130" are the **Name** and **IP Address** of the Acme Packet SD interface where Avaya Communication Manager SIP trunk messages are sent.

- "clan_01a03" and "150.100.100.113" are the **Name** and **IP Address** of the TN799DP C-LAN interface used for the first SIP signaling group (with the Acme Packet SD).

- "clan_01a04" and "150.100.100.114" is the **Name** and **IP Address** of the C-LAN interface used for the second SIP trunk group (with the Acme Packet SD).

```
change node-names ip                                          Page   1 of   2
                                  IP NODE NAMES
    Name                 IP Address
acme_cm4-side          150.100.100.130
clan_01a02             150.100.100.112
clan_01a03             150.100.100.113
clan_01a04             150.100.100.114
default                0.0.0.0
medpro_01a05           150.100.100.115
procr                  150.100.100.100
val_01a08              150.100.100.118
```

Figure 4: IP Node Names

3.1.3. Define IP Codec Sets

This configuration uses two IP codec sets.

- G.711mu codec is used for local voice calls between Avaya telephones. This is IP codec set 1.
- G.729a and G.711mu codecs (in that priority) are used for voice calls via the SIP trunks to the SIP PSTN gateway. This is IP codec set 2.

Using "change ip-codec-set 1" command, enter "**G.711MU**" as the only **Audio Codec**. Retain the defaults for the remaining fields.

```
change 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:
 3:
```

Figure 5: IP Codec Set 1

Using "change ip-codec-set 2" command, enter "**G.729A**" and "**G.711MU**" as the first and second **Audio Codec** values on the form. Again, retain the defaults for the remaining fields.

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

                         IP Codec Set

   Codec Set: 2

   Audio        Silence      Frames   Packet
   Codec        Suppression  Per Pkt  Size(ms)
 1: G.729A           n         2        20
 2: G.711MU          n         2        20
 3:
```

Figure 6: IP Codec Set 2

3.1.4. Verify Near End IP Network Region

These Application Notes use IP network region 1 (the normal default) for the G650 Media Gateway, the IP telephones and the C-LAN (in slot 1a02) used for IP telephone registration. This will be the near-end network region for calls to the SIP PSTN gateway.

Use the "display cabinet n" command (when "n" is "1" in this case) to verify the **IP Network Region** assignment of the G650-port carrier.

```
display cabinet 1
                                    CABINET
 CABINET DESCRIPTION
                  Cabinet: 1
           Cabinet Layout: G650-rack-mount-stack
             Cabinet Type: expansion-portnetwork


                Location: 1         IP Network Region: 1

 Rack: row6          Room: sitl         Floor:             Building:

 CARRIER DESCRIPTION
   Carrier       Carrier Type        Number

      E        not-used             PN  01
      D        not-used             PN  01
      C        not-used             PN  01
      B        not-used             PN  01
      A        G650-port            PN  01
```

Use the "change ip-network-map" command to assign the IP telephones to **Region 1**. In these Application Notes, the IP telephone addresses are with the range specified by the **From IP Address** and **To IP Address** fields (as shown in **Figure 1**.)

```
change ip-network-map                                          Page   1 of  32
                         IP ADDRESS MAPPING

                                                                 Emergency
                                       Subnet                    Location
 From IP Address  (To IP Address   or Mask)  Region    VLAN   Extension
 150.100.100.200  150.100.100.210             1        n
    .   .   .        .   .   .                          n
    .   .   .        .   .   .                          n
    .   .   .        .   .   .                          n
```

Figure 7: IP Network Map for IP Telephones

3.1.5. Configure the C-LAN IP Network Region Assignment

In these Application Notes, three C-LAN's are assumed to been previously installed as part of the initial Avaya Communication Manager basic installation (using the procedures as described in [2]) and assigned the Node Names shown in **Figure 4**. The configuration in this section will assign them to the Network Regions appropriate for Direct SIP Trunking application.

Using the "change ip-interface uucss" command (where uu is the cabinet, c is carrier, and ss is the slot of the respective C-LAN), assign the **Network Region** value as follows:

- C-LAN "1a02" to Network Region 1
- C-LAN "1a03" to Network Region 2
- C-LAN "1a04" to Network Region 2

Note: In order to change an existing ip-interface, the **Enable Ethernet Port** must first be set to "n", the form saved and then the "change ip-interface uucss" done again. The **Enable Ethernet Port** must then be re-enabled with "y" when the **Network Region** value is set.

The resulting ip-interface of the C-LAN used for IP (H.323) telephone registration is:

```
change ip-interface 1a02                                      Page   1 of   1
                                 IP INTERFACES


                  Type: C-LAN
                  Slot: 01A02
             Code/Suffix: TN799  D
               Node Name: clan_01a02
              IP Address: 150.100.100.112
             Subnet Mask: 255.255.255.0                        Link: 12
          Gateway Address:    .   .   .
  Enable Ethernet Port? y                       Allow H.323 Endpoints? y
         Network Region: 1                       Allow H.248 Gateways? y
                  VLAN: n                         Gatekeeper Priority: 5

 Target socket load and Warning level: 400
       Receive Buffer TCP Window Size: 8320
                               ETHERNET OPTIONS
                  Auto? n
                 Speed: 100Mbps
                Duplex: Full
```

Figure 8: IP Interface of C-LAN 1a02 used for IP Telephones

The resulting ip-interface if the C-LAN to be used for SIP signaling group 3 is:

```
change ip-interface 01a03                                     Page   1 of   1
                                 IP INTERFACES


                  Type: C-LAN
                  Slot: 01A03
             Code/Suffix: TN799  D
               Node Name: clan_01a03
              IP Address: 150.100.100.113
             Subnet Mask: 255.255.255.0                        Link: 13
          Gateway Address:    .   .   .
  Enable Ethernet Port? y                       Allow H.323 Endpoints? y
         Network Region: 2                       Allow H.248 Gateways? y
                  VLAN: n                         Gatekeeper Priority: 5

 Target socket load and Warning level: 400
       Receive Buffer TCP Window Size: 8320
                               ETHERNET OPTIONS
                  Auto? n
                 Speed: 100Mbps
                Duplex: Full
```

Figure 9: IP Interface of C-LAN 1a03 used for SIP Signaling Group 3

The resulting ip-interface if the C-LAN to be used for SIP signaling group 4 is:

```
change ip-interface 01a04                                     Page   1 of   1
                                 IP INTERFACES


                  Type: C-LAN
                  Slot: 01A04
           Code/Suffix: TN799  D
             Node Name: clan_01a04
            IP Address: 150.100.100.114
           Subnet Mask: 255.255.255.0                      Link: 14
        Gateway Address:    .   .   .
  Enable Ethernet Port? y                       Allow H.323 Endpoints? y
         Network Region: 2                       Allow H.248 Gateways? y
                  VLAN: n                         Gatekeeper Priority: 5

 Target socket load and Warning level: 400
       Receive Buffer TCP Window Size: 8320
                               ETHERNET OPTIONS
                  Auto? n
                 Speed: 100Mbps
                Duplex: Full
```

Figure 10: IP Interface of C-LAN 1a04 used for SIP Signaling Group 4

3.1.6. Define IP Network Regions

IP network regions set various IP network properties for SIP trunk groups and other IP elements (such as IP telephones, media processor cards, etc.) assigned to the region.

In these Application Notes, two distinct IP network regions are defined.

- "IP Network Region 1" serves as the default region for Avaya Communication Manager and defines properties for local extension to extension calling.
- "IP Network Region 2" defines the properties for calls routed via SIP trunks to the SIP PSTN gateway via the Acme Packet SD.

Using the "change ip-network-region 1" command, enter on Page 1:

- **Name:** a descriptive string such as "Avaya CM Main Location".
- **Authoritative Domain:** leave blank (for ip-network-region 1).
- **Codec Set:** the value "1" corresponding to the ip-codec-set defined in Section 3.1.3 for local calls between telephones on Avaya Communication Manager.
- **Intra-region IP-IP Direct Audio**: the value "yes" (the default).
- **Inter-region IP-IP Direct Audio:** the value "yes" (the default).

The IP-IP Direct Audio settings ensure the most efficient use of TN2602AP Media Processor resources.

Defaults for the remaining values are also used.

```
change ip-network-region 1                                    Page   1 of  19
                             IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain:
    Name: Avaya CM Main Location
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
```

Figure 11: IP Network Region 1 – Page 1

Page 3 of the IP network region form is used to define the codec set and connectivity characteristics between IP network regions.

In these Application Notes, region 1 and 2 are directly connected (using the local LAN) without bandwidth restrictions. Calls between these regions are to use codec set 2 (as defined within Section 3.1.3).

On Page 3, configure the "**src rgn 1 dst rgn 2**" row as follows:

- **codec set**: enter "**2**", to use the codec choices defined in Section 3.1.3 for calls with the SIP PSTN gateway.
- **direct WAN**: enter "**y**" to indicate that regions 1 and 2 are directly connected.
- **Total WAN-BW-limits**: enter "**:NoLimit**" to indicate that there is no explicit limit on the bandwidth or number of simultaneous calls between the regions.

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

                   Inter Network Region Connection Management

 src dst codec direct   Total           Video                          Dyn
 rgn rgn  set   WAN  WAN-BW-limits  Norm Prio  Shr Intervening-regions  CAC IGAR
 1   1    1
 1   2    2     y        :NoLimit              n                            n
 1   3
 1   4
```

Figure 12: IP Network Region 1 – Page 3

Configure IP Network Region 2, using the "change ip-network-region 2" command.
Enter:

- **Name:** a descriptive string such as "AcmePacket SIP Trks"

- **Authoritative Domain:** enter an IP address (or domain name) used to reach this network region. In this case the IP address of the Acme Packet SIP interface (e.g., "150.100.100.130") is used.
- **Codec Set:** the value "2" corresponding to the ip-codec-set defined in Section 3.1.3 for calls using the SIP PSTN gateway.
- **Intra-region IP-IP Direct Audio**: the value "yes" (the default).
- **Inter-region IP-IP Direct Audio:** the value "yes" (the default).

```
change ip-network-region 2                                    Page   1 of  19
                             IP NETWORK REGION
  Region: 2
Location:         Authoritative Domain: 150.100.100.130
    Name: AcmePacket SIP Trks
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 2              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 20000                     IP Audio Hairpinning? n
   UDP Port Max: 20999
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
```

Figure 13: IP Network Region 2 – Page 1

Verify that Page 3 of the "change ip-network-region 2" command appears as shown below without any additional entries. The codec set and inter-region connectivity characteristics for the **src rgn 2 dst rgn 1** row were established during the configuration of IP network region 1.

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

                   Inter Network Region Connection Management

 src dst codec direct   Total           Video                          Dyn
 rgn rgn  set   WAN  WAN-BW-limits  Norm Prio  Shr Intervening-regions  CAC IGAR
 2   1    2     y        :NoLimit              n                           n
 2   2    2
 2   3
 2   4
```

Figure 14: IP Network Region 2 – Page 3

3.1.7. Define SIP Trunk Groups

Two SIP trunk groups are defined for calls with the SIP PSTN gateway (routed via the Acme Packet SD). Each SIP trunk group requires a corresponding SIP signaling group to define the characteristics of the signaling relationship with the Acme Packet SD. Each signaling group uses a separate C-LAN card for redundancy and capacity purposes.

All incoming calls use the round robin load balancing feature of the Acme Packet SD to uniformly distribute calls across both C-LANs (and thus both SIP trunk groups). If the Acme Packet SD detects a failure of SIP signaling to one C-LAN, it automatically routes all calls to the remaining C-LAN interface until the failed signaling is restored.

All outbound calls are routed to the SIP trunk groups using Automatic Route Selection. The route patterns selected by ARS overflow from the first choice SIP trunk group to the second when a signaling failure or all trunks busy occurs.

3.1.7.1 Obtain "init" login ID for Avaya Communication Manager

The SIP signaling groups in these Application Notes require "tcp" as the transport method, instead of the default "tls". The use of "tcp" is administratively restricted and not an available choice when using the "craft" or customer administrative login ids.

In order to complete the administration below, the "init" login id must be used to initially create the signaling group. "Init" login privileges must be obtained from Avaya technical support. After the signaling group is created the additional "init" privileges are no longer required (as long as the transport method is not modified.

3.1.7.2 Establish the SIP Signaling Groups

Log into the Avaya Communcation Manager SAT using the "init" login ID.

Using the "add signaling-group n" command (where "n" is the number of the signaling group), configure the signaling groups 3 and 4 as follows:

- **Group Type**: set to "sip".
- **Transport Method**: set to "tcp". (As discussed above, the "init" login id privileges are required to perform this step. The **Transport Method** field will not be editable otherwise.)
- **Near-end Node Name**: set to the C-LAN node name (defined in Section 3.1.2) used for the respective signaling group. In these Application Notes, "clan_01a03" and "clan_01a04" are used for signaling group 3 and 4, respectively.
- **Far-end Node Name**: set to the interface on the Acme Packet SD that will receive the SIP signaling messages. In these Application Notes, "acme_cm4-side" will be used for both signaling group 3 and 4. The IP address associated with this **Far-end Node Name** will be the destination IP address where SIP messages are sent.
- **Near-end Listen Port**: set to "5060", the default port of SIP signaling using tcp transport.
- **Far-end Listen Port**: set to "5060".
- **Far-end Network Region**: set to "2", the network region defined for SIP PSTN gateway calls defined in Section 3.1.6.
- **Far-end Domain**: set to IP address or domain name of the Acme Packet SD interface used by Avaya Communication Manager. In these Application Notes the IP address of "150.100.100.130" is used.

- **Direct IP-IP Audio Connections**: set to "y", indicating the RTP paths should be optimized to reduce the use of media processing resources when possible.
- **DTMF over IP:** set to "rtp-payload". This value enables Avaya Communication Manager to send DTMF transmissions using RFC 2833 [9].

The default values for the other fields may be used.

The resulting form for signaling group 3 is shown below.

```
add signaling-group 3                                          Page   1 of   1
                              SIGNALING GROUP

Group Number: 3              Group Type: sip
                       Transport Method: tcp




  Near-end Node Name: clan_01a03            Far-end Node Name: acme_cm4-side
Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                       Far-end Network Region: 2
      Far-end Domain: 150.100.100.130

                                            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): 3
```

Figure 15: Signaling Group 3

The resulting form for signaling group 4 is shown below.

```
add signaling-group 4                                          Page   1 of   1
                              SIGNALING GROUP

Group Number: 4              Group Type: sip
                       Transport Method: tcp




  Near-end Node Name: clan_01a04            Far-end Node Name: acme_cm4-side
Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                       Far-end Network Region: 2
      Far-end Domain: 150.100.100.130

                                            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): 3
```

Figure 16: Signaling Group 4

3.1.7.3 Establish SIP Trunk Groups

Using the "add trunk-group n" command (where "n" is the number of the trunk group), configure trunk groups 3 and 4.

On Page 1 of the Trunk Group form:

- **Group Type**: set to "sip".
- **Group Name**: enter a descriptive string such as "SIP-AcmeTG3" and "SIP-AcmeTG4" for trunk groups 3 and 4, respectively.
- **TAC**: enter a trunk access code such as "#003" and "#004" for trunk groups 3 and 4, respectively.
- **Service Type**: set to "public-ntwrk" for trunks to the PSTN.
- **Signaling Group**: set to "3" and "4" (for trunk groups 3 and 4, respectively) as defined within Section 3.1.7.2.
- **Number of Members**: set to the maximum number of simultaneous calls permitted for each trunk group. Within these Application Notes, "10" was used for each trunk group.

The default values may be used on the remaining pages of the trunk-group form.

The resulting form for trunk-group 3 is shown below.

```
add trunk-group 3                                          Page   1 of  21
                              TRUNK GROUP

Group Number: 3                    Group Type: sip           CDR Reports: y
  Group Name: SIP-AcmeTG3                  COR: 1        TN: 1        TAC: #003
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n

                                                    Signaling Group: 3
                                                  Number of Members: 10
```

Figure 17: Trunk Group 3

The resulting form for trunk-group 4 is shown below.

```
add trunk-group 4                                          Page   1 of  21
                              TRUNK GROUP

Group Number: 4                    Group Type: sip           CDR Reports: y
  Group Name: SIP-AcmeTG4                  COR: 1        TN: 1        TAC: #004
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n

                                                    Signaling Group: 4
                                                  Number of Members: 10
```

Figure 18: Trunk Group 4

3.1.8. Configure Calling Party Number Information

The calling party number (e.g., "18002224001") is sent in the userinfo portion of the SIP "From" header as shown below.

```
From: "Jane Smith" <sip:18002224001@150.100.100.130>;tag=80f839da25c3db
```

The "public-unknown-numbering" command controls the calling party number sent in the SIP "From" field for calls originating from Avaya Communication Manager. The public-unknown-numbering is configured to send an 11 digit number consisting of "1800222" plus the 4 digit extension number. In these Application Notes, extensions use numbers between "4000" and "6999".

Using the "change public-unknown-numbering n" command (where "n" is the leading digit of the extension range), specify the calling party number information as follows:

- **Ext Len**: set to "4", the length of the extensions used.
- **Ext Code**: set to the leading digit of the extension used. In these note, "4", "5", and "6" are entered to cover all possible extensions between 4000 and 6999.
- **Trk Grp(s):** by default, leave blank to perform the same conversion across all SIP (and ISDN) trunk groups.
- **CPN Prefix**: set to the leading digits (e.g., "1800222") that are to be sent as the calling party number.
- **Total CPN Len**: set to the total length (e.g., "11") of the calling party number to be sent. The extension number will be appended to the **CPN Prefix** to form complete calling party number of **Total CPN Len** digits.

The completed public-unknown-numbering form is shown below.

```
change public-unknown-numbering 4                              Page   1 of   2
                     NUMBERING - PUBLIC/UNKNOWN FORMAT
                                          Total
Ext Ext           Trk       CPN            CPN
Len Code          Grp(s)    Prefix         Len
                                                    Total Administered: 3
 4  4                       1800222        11          Maximum Entries: 9999
 4  5                       1800222        11
 4  6                       1800222        11
```

Figure 19: Public Unknown Numbering

3.1.9. Configure Call Routing

3.1.9.1 Outbound Calls

In these Application Notes, Automatic Route Selection is used to route outbound calls via the SIP trunk groups to the Acme Packet SD (that in turn routes the calls to the PTSN gateway). In addition the ARS route patterns support alternate routing (via the second SIP trunk group) should the primary trunk group be unavailable.

Here, the configuration of one outbound calling pattern supporting calls to 1-733-xxx-xxx is shown. Routing will select SIP trunk group 3 as the first choice, with overflow to SIP trunk group 4 as required.

A typical installation will generally require additional dial string and route pattern entries but that is beyond the scope of these Application Notes. Further information on ARS administration is discussed in References [1] and [3].

ARS administration begins by verifying the availability of the feature as shown in Section 3.1.1.

Following the verification, use the "change dialplan analysis" command to create a feature access code (fac) for ARS use.

- **Dialed String**: enter "9" that will become the user dialed prefix for outbound calls.
- **Total Length**: enter "1" as the length of the prefix.
- **Call Type**: enter "fac" as the type of prefix.

```
change dialplan analysis                                        Page   1 of  12
                            DIAL PLAN ANALYSIS TABLE
                                                          Percent Full:    1

      Dialed   Total  Call    Dialed   Total  Call     Dialed   Total  Call
      String   Length Type    String   Length Type     String   Length Type
       0          1   attd
       4          4   ext
       5          4   ext
       6          4   ext
       9          1   fac
       *          3   dac
       #          4   dac
```

Figure 20: Dial Plan Analysis

Use the "change feature-access-codes" command to assign the feature access code "9" to **Auto Route Selection (ARS) - Access Code 1** as shown below.

```
change feature-access-codes                                     Page   1 of   7
                            FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code: *71
                       Answer Back Access Code:

      Auto Alternate Routing (AAR) Access Code:
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA: *61    All: *62    Deactivation: *60
   Call Forwarding Enhanced Status:        Act:        Deactivation:
                         Call Park Access Code:
                       Call Pickup Access Code:
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code:
                        Change COR Access Code:
                   Change Coverage Access Code:
                   Contact Closure   Open Code:          Close Code:
```

Figure 21: ARS Feature Access Code

Use the "change ars analysis nn" command to configure the ARS route pattern selection rules as follows. Here "nn" is "17", the first two digits of the dialed number after the ARS access code.

- **Dialed String**: enter the leading digits (e.g., "1733") necessary to uniquely select the desired route pattern.
- **Total Min**: enter the minimum number of digits (e.g., "11") expected for this PSTN number.
- **Total Max**: enter the maximum number of digits (e.g., "11") expected for this PSTN number.
- **Route Pattern**: enter the route pattern number (e.g., "3") to be used. The route pattern (to be defined next) will specify the trunk group(s) to be used calls matching the dialed number.
- **Call Type**: enter "fnpa", the call type for North American 1+10 digit calls.

```
change ars analysis 17                                      Page   1 of   2
                           ARS DIGIT ANALYSIS TABLE
                                 Location:  all           Percent Full:    1

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    1733                  11   11    3        fnpa         n
```

Figure 22: ARS Digit Analysis Entries

Use the "change route-pattern n" command (where "n" is the **Route Pattern** number used above) to specify the SIP trunk groups selected for the outbound call.

In the form:

- **Pattern Name**: enter a descriptive string such as "SIP-AcmeSD-3,4" to describe the routing pattern.
- **Secure SIP?**: leave as "n", the default.
- **Grp No**: enter the trunk groups to be used in priority order. Trunk group 3 is the first choice route followed by trunk group 4 in this configuration.
- **FRL**: enter the minimum facility restriction level (e.g., 1) necessary to use this trunk group, with 0 being the least restrictive. The FRL within the Class of Restriction (COR) assigned to the station must be greater than or equal to 1 in this case to use these trunk groups.
- **Pfx Mrk**: enter "1", to always send the prefix 1 on 10 digit calls.
- **LAR**: enter the routing behavior to be followed if the call is not successfully completed using the trunk group. "Next" will cause the call to attempt to use the next choice in the routing pattern. "None" indicates that no further attempts will be made to complete the call. In the example below, a call that fails when attempting to use trunk group 3, will automatically attempt to use trunk group 4 before being abandoned.

The defaults values for the remaining fields may be used.

The completed route pattern form is shown below.

```
change route-pattern 3                                        Page   1 of   3
                  Pattern Number: 3   Pattern Name: SIP-AcmeSD-3,4
                                        Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                              DCS/ IXC
    No          Mrk Lmt List Del  Digits                                QSIG
                                  Dgts                                  Intw
 1: 3    1       1                                                       n   user
 2: 4    1       1                                                       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                                       next
 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
```

Figure 23: Route Pattern 3

3.1.9.2 Incoming Calls

This step configures the routing of incoming DID numbers to the proper extensions.

In these Application Notes, the following incoming toll-free 800 numbers are used.

Digits Received (within SIP INVITE message)	Extension (or Hunt Group) Answering
800 222 4000	4000
800 222 4001	4001
800 222 5000	5000
800 222 41xx	60xx
800 223 0000	Forwarded to PSTN @ 1 732 555 1234 via SIP trunk

Use the "change inc-call-handling-trmt trunk-group n" command (where "n" is the SIP trunk group number) to administer the incoming number routing. This administration must be done for each incoming trunk group.

- **Called Len**: enter the total number of incoming digits received (e.g., "10").
- **Called Number**: enter the specific digit pattern to be matched.
- **Del**: enter the number of leading digits that should be deleted
- **Insert**: enter the specific digits to be inserted at the beginning of the adjusted incoming digit string (to form what should be complete number).

The completed inc-call-handling-trmt form for trunk group 3 is shown below.

```
change inc-call-handling-trmt trunk-group 3                    Page   1 of  30
                      INCOMING CALL HANDLING TREATMENT
 Service/      Called    Called      Del Insert
 Feature        Len      Number
 public-ntwrk    10 80022240         6
 public-ntwrk    10 80022241         8   60
 public-ntwrk    10 8002225000       10  5000
 public-ntwrk    10 8002230000       10  917325551234
```

The form for trunk group 4 is shown below.

```
change inc-call-handling-trmt trunk-group 4                    Page   1 of  30
                      INCOMING CALL HANDLING TREATMENT
 Service/      Called    Called      Del Insert
 Feature        Len      Number
 public-ntwrk    10 80022240         6
 public-ntwrk    10 80022241         8   60
 public-ntwrk    10 8002230000       10  917325551234
```

3.1.10. Save Avaya Communication Manager Changes

This completes the configuration of the Avaya Communication Manager.

Use the “save translation” command to make the changes permanent.

4. Configure the Acme Packet Net-Net Session Director

This section describes the configuration of the Acme Packet Net-Net Session Director. The Net-Net Session Director acts as an intermediary between the Avaya Communication Manager CLAN interfaces and the SIP PSTN gateway.

These Application Notes assume the Acme Packet SD has been previously installed according Acme Packet guidelines. The basic installation and configuration is beyond the scope of this SIP trunking application.

The Acme Packet Net-Net Session Director was configured using a telnet command line session using its administrative interface. The following sections contain output (text outlined within boxes) from the **show running-config** command that was used to display the configuration of the SD. The general configuration information shown in Section 4.1 is not specific to the SIP trunking in the Application Notes. It is included for reference purposes but without further explanation. Section 4.2 through Section 4.4 contain the specific configuration details (highlighted by bold text) important to the Direct SIP Trunking configuration within these Application Notes. The remaining fields are generally the default value used by the Acme Packet SD. For additional details on the administration of the Acme Packet SD, refer to [5].

4.1. General Configuration

The general configuration elements of the Acme Packet SD configuration used are shown below without further elaboration.

```
system-config
        hostname                        acmesystem
        description
        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                 100.3.3.1
        restart                         enabled
        exceptions
        telnet-timeout                  600
        console-timeout                 600
        remote-control                  enabled
        last-modified-date              2007-01-30 11:27:07
```

```
host-routes
        dest-network                    101.0.0.0
        netmask                         255.0.0.0
        gateway                         200.2.2.2
        last-modified-date              2006-08-17 15:35:15
```

```
redundancy-config
        state                           enabled
        log-level                       INFO
        health-threshold                75
        emergency-threshold             50
        port                            9090
        advertisement-time              500
        percent-drift                   210
        initial-time                    1250
```

```
        becoming-standby-time          180000
        becoming-active-time           100
        cfg-port                       1987
        cfg-max-trans                  10000
        cfg-sync-start-time            5000
        cfg-sync-comp-time             1000
        gateway-heartbeat-interval     0
        gateway-heartbeat-retry        0
        gateway-heartbeat-timeout      1
        gateway-heartbeat-health       0
        peer
                name                           sbcsec
                state                          enabled
                type                           Secondary
                destination
                        address                        169.254.1.2:9090
                        network-interface              wancom1:0
                destination
                        address                        169.254.2.2:9090
                        network-interface              wancom2:0
        peer
                name                           sbcpri
                state                          enabled
                type                           Primary
                destination
                        address                        169.254.1.1:9090
                        network-interface              wancom1:0
                destination
                        address                        169.254.2.1:9090
                        network-interface              wancom2:0
        last-modified-date             2007-01-31 12:33:01
```

```
sip-config
        state                          enabled
        operation-mode                 dialog
        dialog-transparency            enabled
        home-realm-id                  acme
        egress-realm-id
        nat-mode                       Public
        registrar-domain
        registrar-host
        registrar-port                 0
        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                 0
        last-modified-date              2007-01-29 17:11:48
```

```
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
        options                         active-arp
        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
        last-modified-date              2007-01-31 14:49:17
```

4.2. SIP Trunks to Avaya Communication Manager

4.2.1. Physical and Network Interfaces

In this configuration, a dedicated LAN subnet (150.100.100.0/24) was used for all communication between the Acme Packet SD and the Avaya Communication Manager CLAN and Medpro IP interfaces. This subnet does not have IP routing connectivity with any other IP subnet. All SIP signaling and RTP media packets using this subnet are routed via Acme Packet SD to reach the SIP PSTN gateway.

Ethernet interface slot 0 / port 2 (on each Acme Packet SD server in the redundant configuration) is dedicated for the Avaya Communication Manager connectivity and connected to the Ethernet switch providing the 150.100.100.0/24 LAN subnet.

The tables below show the details of the "phy-interface" and "network-interface" commands.

The key physical interface fields are:

- **name:** a descriptive string used to reference the Ethernet interface.
- **operation-type:** "Media" indicating both signaling and rtp packets use this interface.
- **slot / port**: the identifier of the specific front panel Ethernet interface used.
- **virtual-mac**: the mac address that will be dynamically assigned to the interface on the active SD server (in the redundant pair). This address must be determined using the guidelines provided in the Acme Packet SD documentation [6].

```
phy-interface
        name                            cm4_clan
        operation-type                  Media
        port                            2
        slot                            0
        virtual-mac                     00:08:25:01:b5:6e
        admin-state                     enabled
        auto-negotiation                enabled
        duplex-mode                     FULL
        speed                           100
        last-modified-date              2007-01-30 11:50:06
```

The key network-interface fields are:

- **name:** a reference of the phy-interface (defined above).
- **ip-address**: the virtual IP address of the active "cm4_clan" interface
- **pri-utility-addr**: the fixed IP address assigned to this interface on the primary SD server
- **sec-utility-addr**: the fixed IP address assigned to this interface on the secondary SD server
- **netmask**: subnet mask for the IP subnet
- **gateway**: the subnet gateway address. In this case, gateway is null since all routing via this interface remained within the 150.100.100.0/24 subnet.
- **hip-ip-list**: allowed ip address to accept administrative traffic (such as icmp ping)
- **icmp-address**: ip address used to pass icmp pings

```
network-interface
        name                            cm4_clan
        sub-port-id                     0
        hostname
        ip-address                      150.100.100.130
        pri-utility-addr                150.100.100.131
        sec-utility-addr                150.100.100.132
        netmask                         255.255.255.0
        gateway
        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                     150.100.100.130
        ftp-address
        icmp-address                    150.100.100.130
        snmp-address
        telnet-address
        last-modified-date              2007-01-31 18:36:18
```

4.2.2. SIP Interface

The "sip-interface" configuration defines the receiving characteristics of the SIP interfaces on the Acme Packet SD. The Avaya Communication Manager SIP signaling groups will send SIP messages to the sip-interface defined below.

The key sip-interface fields are:

- **realm-id**: the name (defined within Section 4.2.4) of the realm that this interface is assigned.
- **address**: the ip address assigned to this sip-interface. This must match the **IP Address** associated with the **Name** "acme_cm4_side" as defined in the IP Node Names form shown in **Figure 4**. (Note this corresponds to the **Far-end Node Name** used in the SIP signaling groups defined in Section 3.1.7.2.)
- **port**: the tcp port assigned to this sip-interface. This must match the **Far-end Listen Port** assigned for the SIP signaling groups in Section 3.1.7.2.
- **transport-protocol**: the transport method used for this interface. This must match the "tcp" **Transport Method** assigned for the signaling groups in Section 3.1.7.2.

```
sip-interface
        state                           enabled
        realm-id                        cm4_clan
        sip-port
                address                         150.100.100.130
```

```
                port                            5060
                transport-protocol              TCP
                tls-profile
                allow-anonymous                 all
        carriers
        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
        last-modified-date              2007-01-30 11:21:53
```

Steering pools define the range of UDP ports to be used for the RTP voice stream.

The key "steering-pool" parameters are:

- **ip-address:** the address of the interface on the Acme SD.
- **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 that that the steering pool is assigned to.

```
steering-pool
        ip-address                      150.100.100.130
        start-port                      20000
        end-port                        20999
        realm-id                        cm4_clan
        network-interface
        last-modified-date              2007-01-29 15:42:17
```

4.2.3. SIP Session Agent and Session Groups

The "session-agent" configuration defines specific interfaces where the Acme Packet SD will send SIP signaling messages.

In this case, a "session-agent" is defined for each Avaya Communication Manager SIP signaling group defined within Section 3.1.7.2. The field names below refer to fields in the signaling group forms shown in **Figure 15** and **Figure 16** unless stated otherwise. Recall that these signaling groups were defined use different C-LANs for reliability and load balancing purposes.

The key session-agent fields are:

- **hostname:** the IP address of the respective **Near-end Node Name** (e.g., respective C-LANs). (This IP address is found on the IP Node Names form shown in **Figure 4** in Section 3.1.2.)
- **port:** the **Near-end Listen Port** specified for the respective signaling groups.
- **app-protocol:** enter "SIP"
- **transport-method:** "DynamicTCP" corresponding to the "TCP" **Transport Method** specified in the signaling group forms.
- **realm-id:** the realm (e.g., "cm4_clan") that these session agents belong to.
- **description:** a descriptive string to identify the far end interface
- **max-sessions:** a call admission control value that matches the **Number of Members** value assigned in the trunk groups form shown in **Figure 17** and **Figure 18** in Section 3.1.7.3.
- **ping-method:** the specific SIP message sent to verify the sip trunk group is active. Note this is a case-sensitive and must be entered exactly as "OPTIONS;hops=0".
- **ping-interval:** the number of seconds between issuing the OPTIONS ping.

This is the session-agent configuration associated with the signaling group 3 (using C-LAN 1a03.)

```
session-agent
        hostname                        150.100.100.113
        ip-address
        port                            5060
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                DynamicTCP
        realm-id                        cm4_clan
        description                     clan_1a03
        carriers
        allow-next-hop-lp               enabled
        constraints                     enabled
        max-sessions                    10
        max-outbound-sessions           0
        max-burst-rate                  0
        max-sustain-rate                0
        min-seizures                    5
        min-asr                         0
        time-to-resume                  0
        ttr-no-response                 0
        in-service-period               0
        burst-rate-window               0
        sustain-rate-window             0
        req-uri-carrier-mode            None
        proxy-mode
        redirect-action
        loose-routing                   enabled
        send-media-session              enabled
        response-map
        ping-method                     OPTIONS;hops=0
        ping-interval                   60
        media-profiles
        in-translationid
        out-translationid
        trust-me                        disabled
        request-uri-headers
        stop-recurse
        local-response-map
        ping-to-user-part
        ping-from-user-part
        li-trust-me                     disabled
        in-manipulationid
        out-manipulationid
        p-asserted-id
        trunk-group
        max-register-sustain-rate       0
        early-media-allow
        invalidate-registrations        disabled
        rfc2833-mode                    none
        rfc2833-payload                 0
        last-modified-date              2007-01-31 15:47:22
```

This is the session-agent configuration associated with the signaling group 4 (using C-LAN 1a04.)

```
session-agent
        hostname                        150.100.100.114
        ip-address
        port                            5060
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                DynamicTCP
        realm-id                        cm4_clan
        description                     clan_01a04
        carriers
        allow-next-hop-lp               enabled
        constraints                     enabled
        max-sessions                    10
        max-outbound-sessions           0
        max-burst-rate                  0
        max-sustain-rate                0
        min-seizures                    5
        min-asr                         0
        time-to-resume                  0
        ttr-no-response                 0
        in-service-period               0
        burst-rate-window               0
        sustain-rate-window             0
        req-uri-carrier-mode            None
        proxy-mode
        redirect-action
        loose-routing                   enabled
        send-media-session              enabled
        response-map
        ping-method                     OPTIONS;hops=0
        ping-interval                   60
        media-profiles
        in-translationid
        out-translationid
        trust-me                        disabled
        request-uri-headers
        stop-recurse
        local-response-map
        ping-to-user-part
        ping-from-user-part
        li-trust-me                     disabled
        in-manipulationid
        out-manipulationid
        p-asserted-id
        trunk-group
        max-register-sustain-rate       0
        early-media-allow
        invalidate-registrations        disabled
        rfc2833-mode                    none
        rfc2833-payload                 0
        last-modified-date              2007-01-31 15:47:30
```

The session-group configuration defines a logical group of session agents used to send SIP messages to Avaya Communication Manager. Included in the session group configuration is the strategy used to distribute calls across the multiple session agents. In this case a round-robin strategy was chosen.

The key session-group fields are:

- **group-name**: a string used to reference this session group
- **description**: a description of the session group
- **app-protocol**: the signaling protocol used
- **strategy**: the load balancing strategy used
- **dest**: the hostname of the multiple session agents forming the session group

```
session-group
        group-name                      cm4_sipTrkClans
        description                     all sip trunk clans
        state                           enabled
        app-protocol                    SIP
        strategy                        RoundRobin
        dest
                                        150.100.100.113
                                        150.100.100.114
        trunk-group
        last-modified-date              2007-01-26 17:29:06
```

4.2.4. Realm Configuration

The realm-config assigns common logical characteristics to be used by one or more interfaces, address spaces, etc.

In this section the "cm4_clan" realm is defined. The primary function of this realm definition is to uniformly apply rules to modify specific addresses within all outgoing SIP messages from the interface associated with the realm. The sip message modification rules are defined within the sip-manipulation configuration (named "NAT_IP") shown in Section 4.4

The key realm-config fields in this configuration are:

- **identifier**: a string used as realm reference
- **addr-prefix**: the IP address subnet (e.g., "150.100.100.0/24") that this realm applies to.
- **network-interfaces**: the **name** and **sub-port-id** (separated by a colon) of the network interface(s) defined to be within this realm. These fields were specified in Section 4.2.1.
- **out-manipulationid**: enter the **name** of the "sip-manipulation" rule (defined in Section 4.4) that should be applied on messages sent by the realm.

The realm-config for "cm4_clan" (the subnet used for Avaya Communication Manager) is shown below.

```
realm-config
        identifier                      cm4_clan
        addr-prefix                     150.100.100.0/24
        network-interfaces
                                        cm4_clan:0
        mm-in-realm                     disabled
        mm-in-network                   enabled
        mm-same-ip                      enabled
        mm-in-system                    enabled
        msm-release                     disabled
        qos-enable                      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              NAT_IP
        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
        last-modified-date              2007-01-29 16:08:11
```

4.2.5. Local Policy

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

The key local-policy fields in this configuration are:

- **From-address**: a policy filter indicating that the originating IP addresses that this policy applies to. An asterisk ("*") indicates any IP address.
- **To-address**: a policy filter indicating that the terminating IP addresses that this policy applies to. An asterisk ("*") indicates any IP address.
- **Source-realm**: a policy filter indicating the matching realm in order for the policy rules to be applied.
- **policy-attribute next-hop**: the IP address where the message should be sent when the policy rules match.
- **policy-attribute 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 "cm4_clan" realm are to be sent to the realm "pstn_cm4" via IP address 147.16.57.2 (the SIP PSTN gateway).

This local-policy indicates that the Acme Packet SD should route calls originating from the Avaya Communication Manager ("cm4_clan" realm) to the SIP PSTN gateway ("pstn_cm4" realm) at IP address 142.16.57.2.

```
local-policy
```

```
        from-address
                                        *
        to-address
                                        *
        source-realm
                                        cm4_clan
        activate-time                   N/A
        deactivate-time                 N/A
        state                           enabled
        policy-priority                 none
        last-modified-date              2007-01-29 15:46:50
        policy-attribute
                next-hop                        142.16.57.2
                realm                           pstn_cm4
                action                          none
                terminate-recursion             disabled
                carrier
                start-time                      0000
                end-time                        2400
                days-of-week                    U-S
                cost                            0
                app-protocol
                state                           enabled
                media-profiles
```

4.3. SIP Trunks to SIP PSTN Gateway

The configuration necessary for the Acme Packet SD to communicate with the SIP PSTN gateway using SIP is shown below. Note that load balancing (using session agent groups) and SIP failure detection (using SIP OPTION pings) were not defined for this gateway. The description of the key fields was previously discussed in Section 4.2.1.

4.3.1. Physical and Network Interfaces

Here, Acme Packet SD interfaces at slot 0 / port 0 on each server are assigned addresses from the LAN subnet (142.16.58.0/24) to communication with the SIP PSTN gateway at IP address 142.16.57.2.

The table below show the details of the “phy-interface”.

```
phy-interface
        name                            pstn
        operation-type                  Media
        port                            0
        slot                            0
        virtual-mac                     00:08:25:01:be:e8
        admin-state                     enabled
        auto-negotiation                enabled
        duplex-mode                     FULL
        speed                           100
        last-modified-date              2006-03-08 17:40:04
```

The table below shows the details of the “network-interface”.

```
network-interface
        name                            pstn
        sub-port-id                     0
        hostname
        ip-address                      142.16.58.2
        pri-utility-addr                142.16.58.3
        sec-utility-addr                142.16.58.4
        netmask                         255.255.255.0
        gateway                         142.16.58.1
        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                     142.16.58.2
        ftp-address
        icmp-address                    142.16.58.2
        snmp-address
        telnet-address
        last-modified-date              2006-10-10 08:44:01
```

4.3.2. SIP Interface

The “sip-interface” configuration defines the receiving characteristics of the SIP interface on the Acme Packet SD for messages received from the SIP PSTN gateway. The description of the key fields was previously discussed in Section 4.2.2.

This SIP interface uses the “UDP” **transport-protocol** and listens on the **port** “5060”. These characteristics are matched to interface used on the SIP PSTN gateway in these Application Notes.

Below is the complete sip-interface configuration.

```
sip-interface
        state                           enabled
        realm-id                        pstn_cm4
        sip-port
                address                         142.16.58.2
                port                            5060
                transport-protocol              UDP
                tls-profile
                allow-anonymous                 all
        carriers
        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
        last-modified-date              2007-01-26 12:20:45
```

Steering pools define the range of UDP ports to be used for the RTP voice stream to the SIP PSTN gateway.

```
steering-pool
        ip-address                      142.16.58.2
        start-port                      20000
        end-port                        20999
        realm-id                        pstn_cm4
        network-interface
        last-modified-date              2007-01-29 15:42:26
```

4.3.3. SIP Session Agent and Session Groups

The "session-agent" configuration defines where SIP signaling messages will be sent. The description of the key fields was previously discussed in Section 4.2.3

In this case, the "session-agent" defines the information used to send SIP messages to the SIP PSTN gateway. Max sessions and ping-methods were not used for this SIP PSTN gateway.

```
session-agent
        hostname                        142.16.57.2
        ip-address
        port                            5060
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                UDP
        realm-id                        *
        description                     pstn_gateway
        carriers
        allow-next-hop-lp               enabled
        constraints                     disabled
        max-sessions                    0
        max-outbound-sessions           0
        max-burst-rate                  0
        max-sustain-rate                0
        min-seizures                    5
        min-asr                         0
        time-to-resume                  0
        ttr-no-response                 0
        in-service-period               0
        burst-rate-window               0
        sustain-rate-window             0
        req-uri-carrier-mode            None
        proxy-mode
        redirect-action
        loose-routing                   enabled
        send-media-session              enabled
        response-map
        ping-method
        ping-interval                   0
        media-profiles
        in-translationid
```

```
        out-translationid
        trust-me                        disabled
        request-uri-headers
        stop-recurse
        local-response-map
        ping-to-user-part
        ping-from-user-part
        li-trust-me                     disabled
        in-manipulationid
        out-manipulationid
        p-asserted-id
        trunk-group
        max-register-sustain-rate       0
        early-media-allow
        invalidate-registrations        disabled
        rfc2833-mode                    none
        rfc2833-payload                 0
        last-modified-date              2007-01-29 15:47:12
```

A session-group is not defined for the SIP PSTN gateway since load balancing was not part of this configuration.

4.3.4. Realm Configuration

The realm-config assigns common logical characteristics to be used by one or more interfaces, address spaces, etc. The description of the key fields was previously discussed in Section 4.2.4.

Below, the "pstn_cm4" realm is defined for communications with the SIP PSTN gateway. The primary function of this realm definition is to apply the sip message modification rules are defined within the sip-manipulation configuration (named "NAT_IP") shown in Section 4.4. The **addr-prefix** equal "0.0.0.0" means that the realm-config rules will be applied to messages from any address received on the **network-interfaces** "pstn:0".

```
realm-config
        identifier                      pstn_cm4
        addr-prefix                     0.0.0.0
        network-interfaces
                                        pstn:0
        mm-in-realm                     disabled
        mm-in-network                   enabled
        mm-same-ip                      enabled
        mm-in-system                    enabled
        msm-release                     disabled
        qos-enable                      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              NAT_IP
        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
        last-modified-date              2007-01-29 16:08:27
```

4.3.5. Local Policy

Local policy controls the routing of SIP calls from one realm to another. The description of the key fields was previously discussed in Section 4.2.5.

The local-policy indicates that the Acme Packet SD should route calls originating from the "pstn_cm4" realm (that the SIP PSTN gateway is assigned to) using the Session Agent Group (SAG) "cm4_sipTrkClans" defined within Section 4.2.3. Note the use of the Session Agent Group indicator "SAG:" in the **next-hop** field. This indicates that messages use the logical session group to perform the round robin load balancing rather than routing directly to a specific C-LAN address. (The "SAG:" tag was not clearly documented in the Acme Packet documentation in [6].)

```
local-policy
        from-address
```

```
                                *
        to-address
                                *
        source-realm
                                pstn_cm4
        activate-time           N/A
        deactivate-time         N/A
        state                   enabled
        policy-priority         none
        last-modified-date      2007-01-29 15:52:32
        policy-attribute
                next-hop                    SAG:cm4_sipTrkClans
                realm                       cm4_clan
                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
```

4.4. SIP Header Manipulation

Sip-manipulation uses Header Manipulation Rules (HMR) to modify SIP messages according to specific predefined rules.

In this application, the purpose is to convert addresses within SIP messages from the 150.100.100.0/24 subnet (used by Avaya Communication Manager) to the 142.16.57.0/24 subnet (used by the SIP PSTN gateway.) when routing between the respective realms. This avoids the alternative approach using the SIP NAT functions that can negatively impact performance and capacity of the Acme Packet SD.

Further information can be found in the Acme Packet Best Current Practice Document 520-0014-00 [6] that describe the use of HMR to improve performance.

The key sip-manipulation fields in this configuration are:

- **name:** a string used to reference the sip-manipulation rules (as used in the realm-config in Sections 4.2.4 and 4.3.4).
- **header-rule name**: a descriptive string used to describe the header rule.
- **header-rule msg-type**: the type of SIP message that the rule is applied to.
- **header-rule element-rule name:** the specific SIP header the rule is applied to.
- **header-rule element-rule new-value:** "$LOCAL_IP" and "$REMOTE_IP" are variable substitutions to be performed. "$LOCAL_IP" is the IP address of Acme Packet SD interface sending the message. "$REMOTE_IP" is the address that the Acme Packet SD is sending the message to.

The sip-manipulation rules used in these Application Notes is shown below.

```
sip-manipulation
        name                            NAT_IP
        header-rule
                name                            From
                action                          manipulate
                match-value
                msg-type                        request
                methods
                element-rule
                        name                            FROM
                        type                            uri-host
                        action                          replace
                        match-val-type                  ip
                        match-value
                        new-value                       $LOCAL_IP
        header-rule
                name                            To
                action                          manipulate
                match-value
                msg-type                        request
                methods
                element-rule
                        name                            TO
                        type                            uri-host
                        action                          replace
                        match-val-type                  ip
                        match-value
                        new-value                       $REMOTE_IP
        header-rule
                name                            Remote-Party-ID
                action                          manipulate
                match-value
                msg-type                        request
                methods
                element-rule
                        name                            RPID
                        type                            uri-host
                        action                          replace
                        match-val-type                  ip
                        match-value
                        new-value                       $LOCAL_IP
```

5. Verification Steps

This section provides steps that may be performed to verify the operation of the Direct SIP trunking configuration described in the Application Notes.

The Avaya Communication Manager “list trace station”, “list trace tac”, “status station” and/or “status trunk-group” commands are helpful diagnostic tools to verify correct operation and to troubleshoot problems. Also using a SIP protocol analyzer such as WireShark (a.k.a, Ethereal)

to monitor the SIP messaging at the various interfaces (C-LAN, Acme Packet and/or SIP PSTN gateway) is often very helpful in troubleshooting issues.

- Incoming Calls – Verify that calls placed from a PSTN telephone to the DID number assigned are properly routed via the SIP trunk group(s) to the expected telephone, hunt group, ACD split, etc. Verify the talk-path exists in both directions, that calls remain stable for several minutes and disconnect properly.

- Outbound Calls – Verify that calls placed to a PSTN telephone are properly routed via the SIP trunk group(s) defined in the ARS route patterns. Verify that the talk-path exists in both directions and that calls remain stable and disconnect properly.

- Direct IP-IP Connections – This applies if IP telephones and Direct IP-IP are used. Verify that stable calls are using Direct IP-IP talk paths using the "status station" or "status trunk-group" commands. When Direct IP-IP is used, the Audio Connection field will indicate "ip-direct" instead of "ip-tdm".

- Load Balancing of Incoming Calls – This applies if multiple SIP trunk groups (using multiple C-LANs and Acme Packet Load Balancing) are used. Verify that incoming calls are distributed across the trunk groups defined with the session-agent-group of the Acme Packet SD.

- Alternate Routing of Inbound Calls on C-LAN failure – This applies if multiple SIP trunk groups (using multiple C-LANs) are used. Maintenance busy the C-LAN associated with an incoming SIP trunk group and verify using the "list trace station" or "list trace trunk" commands that inbound calls are routed to the active SIP trunk group (using a separate C-LAN). Verify that the original trunk group is used once the C-LAN is returned to service. Repeat for other incoming SIP trunk groups. **Note: This may be service affecting!**

- Alternate Routing of Outbound Calls on C-LAN failure – This applies if multiple SIP trunk groups (using multiple C-LANs) are used. Maintenance busy the C-LAN associated with the first-choice trunk group and verify using the "list trace station" or "list trace trunk" commands that outbound calls overflow to the next SIP trunk group (using a separate C-LAN). Verify that the original trunk group is used once the C-LAN is returned to service. Repeat for other route-patterns using these trunk groups. **Note: This may be service affecting!**

6. Support

For technical support on the Acme Packet Net-Net Session Director, visit www.acmepacketcom.

7. Conclusion

These Application Notes describe the configuration steps required to establish sip trunking directly with Avaya Communication Manager to an Acme Packet Net-Net Session Director and a

SIP PSTN gateway for the purpose of PSTN interconnection. This configuration was successfully compliance tested with the demonstration of calls in both directions with the PSTN. The ability to use incoming load balancing across multiple Avaya Communication Manger C-LAN interfaces and endure a C-LAN interface isolation or failure was shown.

8. References

The Avaya product documentation is available at http://support.avaya.com.

[1] *Administrator Guide for Avaya Communication Manager*, February 2007, Issue 3, Document Number 03-300509.
[2] *Adding New Hardware for Avaya Media Servers and Gateways*, February 2007, Issue 2, Release 4.0, Document Number 03-300684
[3] *Feature Description and Implementation for Avaya Communication Manager,* Issue 5, Document Number 555-245-205
[4] *SIP Support in Avaya Communication Manager Running on the Avaya S8300, S8400, S8500 series and S8700 series Media Server*, March 2007, Issue 6.1, Document Number 555-245-206.
[5] *4600 Series IP Telephone Release 2.6 LAN Administrator Guide*, August 2006, Issue 4, Document Number 555-233-507

The following documentation is provided with the Acme Packet Net-Net Session Director or is available from Acme Packet Technical Support. See www.acmepacket.com for further information.

[6] *Net-Net Session Director Configuration Guide*, Acme Packet, Inc., Release Version 4.1, Document Number 400-0061-41A, August 8, 2006.
[7] *SIP Peering Configuration on the Net-Net Session Director - Software Versions 4.0.0 and Newer*, Acme Packet Best Current Practice, Document # 520-0014-00, March 16, 2006

Several Internet Engineering Task Force (IETF) standards track RFC documents were referenced within these Application Notes. The RFC documents may be obtained at: http://www.rfc-editor.org/rfcsearch.html.

[8] RFC 3261 - *SIP (Session Initiation Protocol)*, June 2002, Proposed Standard
[9] RFC 2833 - *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, May 2000, Proposed Standard

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.