Sample Configuration Illustrating Avaya Aura™ Communication Manager SIP Trunk Survivability with Enterprise Survivable Server and Acme Packet Net-Net 4500 Session Director – Issue 1.0

Abstract

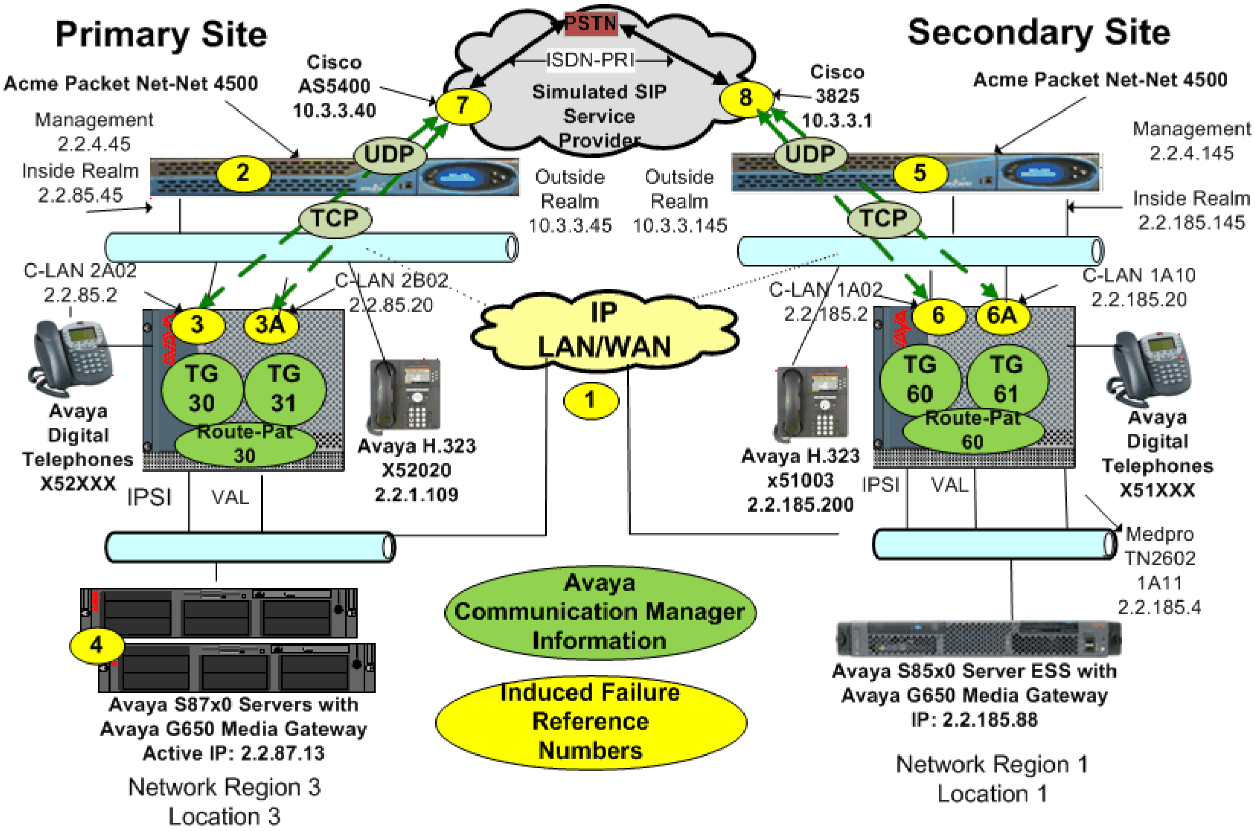
These Application Notes illustrate a sample configuration of Avaya Aura™ Communication Manager Release 5.2 with SIP Trunks to Acme Packet Net-Net 4500 Session Director at two sites. For business continuity, a primary site uses Avaya S8730 Servers, and a secondary site uses an Avaya S8500 Server as an Enterprise Survivable Server (ESS). At each site, two Avaya C-LAN cards are configured for SIP Trunking to the "inside" realm of an Acme Packet Net-Net 4500 Session Director. On the "outside" realm, each Acme Packet Net-Net 4500 Session Director is connected to a SIP network simulating a public SIP Service Provider. Within each site, the Acme Packet Net-Net 4500 Session Director is configured for load spreading and fast fail-over of inbound calls to the enterprise from the PSTN. For outbound calls to the PSTN, Communication Manager is configured for location-based routing for trunk selection and Look-Ahead Routing for trunk fail-over. Other Communication Manager multi-site features such as locally-sourced announcements via Audio Groups are also configured for efficiency and survivability.

When all elements are functioning, Communication Manager running on the active Avaya S8730 Server is processing all inbound and outbound SIP Trunk calls for both sites, efficiently allocating resources such as announcements, media processors, and trunks from the appropriate site's gateway. These Application Notes focus on considerations and expected behaviors when various failures are induced. For example, the verification of these Application Notes includes normal operation, failure of connectivity to C-LANs, failure of the enterprise data network activating the ESS, and failure of the Acme Packet Net-Net Session Directors.

1. Introduction

These Application Notes illustrate a sample configuration of Avaya Aura™ Communication Manager Release 5.2 with SIP Trunks to Acme Packet Net-Net 4500 Session Director at two sites. **Figure 1** illustrates relevant aspects of the sample configuration. A primary site uses Avaya S8730 Servers, and a secondary site uses an Avaya S8500 Server as an Enterprise Survivable Server (ESS). At each site, two Avaya C-LAN cards are configured for SIP Trunking to the Session Director using TCP for the SIP signaling connectivity. Each Session Director is also connected to a SIP network simulating a SIP Service Provider. Since most SIP Service Providers use UDP for SIP signaling, the SIP signaling connectivity from the Acme Packet Net-Net 4500 toward the "outside realm" uses UDP.

When all elements are functioning, the active Avaya S8730 Server at the primary site is processing all inbound and outbound SIP Trunk calls for both sites, efficiently allocating resources such as announcements, media processors, and trunks from the appropriate site's gateway. These Application Notes focus on considerations and expected behaviors when failures are induced, and induced failure points are numbered in **Figure 1** for later reference. The verification of these Application Notes includes normal operation, failure of connectivity to C-LANs, failure of the enterprise data network isolating the secondary site and activating the ESS, and failure of the Acme Packet Net-Net Session Director.



Primary Site
Secondary Site
PSTN
ISDN-PRI
Simulated SIP Service Provider
Cisco AS5400 10.3.3.40
Cisco 3825 10.3.3.1
Acme Packet Net-Net 4500
Management 2.2.4.45
Inside Realm 2.2.85.45
Management 2.2.4.145
Inside Realm 2.2.185.145
UDP
TCP
Outside Realm 10.3.3.45
Outside Realm 10.3.3.145
C-LAN 2A02 2.2.85.2
C-LAN 2B02 2.2.85.20
C-LAN 1A02 2.2.185.2
C-LAN 1A10 2.2.185.20
IP LAN/WAN
1
2
3
3A
4
5
6
6A
7
8
TG 30
TG 31
Route-Pat 30
TG 60
TG 61
Route-Pat 60
Avaya Digital Telephones X52XXX
Avaya H.323 X52020 2.2.1.109
Avaya H.323 x51003 2.2.185.200
Avaya Digital Telephones X51XXX
IPSI
VAL
Medpro TN2602 1A11 2.2.185.4
Avaya S87x0 Servers with Avaya G650 Media Gateway Active IP: 2.2.87.13
Network Region 3 Location 3
Avaya S85x0 Server ESS with Avaya G650 Media Gateway IP: 2.2.185.88
Network Region 1 Location 1
Avaya Communication Manager Information
Induced Failure Reference Numbers

Figure 1: Avaya Aura™ Communication Manager Survivable SIP Trunking

These Application Notes complement previously published documents with testing of the latest Communication Manager and Acme Packet Net-Net Session Director software. For example, reference [JSR] documents Communication Manager direct SIP Trunking to Acme Packet, based on prior versions of the products. Reference [JSR] does not include an ESS in the configuration, so a focus of these Application Notes is to cover survivability considerations in a multi-site SIP Trunking model. **Figure 1** shows the types of failures induced as part of the verification of these Application Notes, illustrated in Section 5.

As in reference [JSR], the Acme Packet Net-Net 4500 is used to distribute SIP signaling for incoming calls to multiple C-LAN interfaces, providing load spreading and fast automatic fail-over. The Acme Packet Net-Net 4500 performs conversion between TCP transport for SIP signaling used by Communication Manager to UDP transport commonly used by SIP Service Providers. The Acme Packet Net-Net 4500 also performs Session Border Controller (SBC) functions, providing security and topology-hiding at the enterprise edge. In the sample configuration, all SIP signaling and RTP media between the enterprise and the (simulated) SIP Service Provider flows through the Acme Packet Net-Net 4500.

A customer interested in SIP Trunk survivability may want a redundant pair of Acme Packet Net-Net 4500 Session Directors at each site. Although the sample configuration verified in these Application Notes used only a single Acme Packet Net-Net 4500 at each site, the Acme Packet configuration shown in Section 4 and **Appendix A** was prepared as if there were a high availability Acme Packet configuration at each site. Actual verification testing of the Acme Packet Net-Net 4500 High Availability configuration with Communication Manager was performed as part of Avaya DevConnect compliance testing, and the Application Notes in reference [AP-HA] documents the configuration and testing results.

1.1. Summary of Inbound Calls to the Enterprise

Figure 2 illustrates aspects of the sample configuration related to inbound calls to the enterprise from the PSTN. Although further elaboration of the simulation of the SIP Service Provider is out of scope, **Figure 2** may help with understanding assumptions and call flow verifications. For example, it is assumed that published PSTN telephone numbers such as Direct Inward Dial (DID), Listed Directory Numbers (LDN), or toll-free numbers that map to Avaya Vector Directory Numbers (VDNs) can arrive to the enterprise from the service provider via either the primary site or the secondary site SIP Trunks. A SIP service provider may load balance inbound calls to the enterprise between sites, or route particular numbers to a specific site preferentially, with fail-over to the other site as needed.

As shown in **Figure 2**, the DID number 732-852-1816 is preferentially routed to the primary site, but can fail-over to the secondary site. The DID number 732-852-2940 is preferentially routed to the secondary site, but can fail-over to the primary site. Communication Manager can map any received telephone number to any destination via the incoming call handling table of the trunk group. During testing, calls arriving via the primary site SIP trunks were directed to users at both the primary and the secondary sites, and vice-versa.

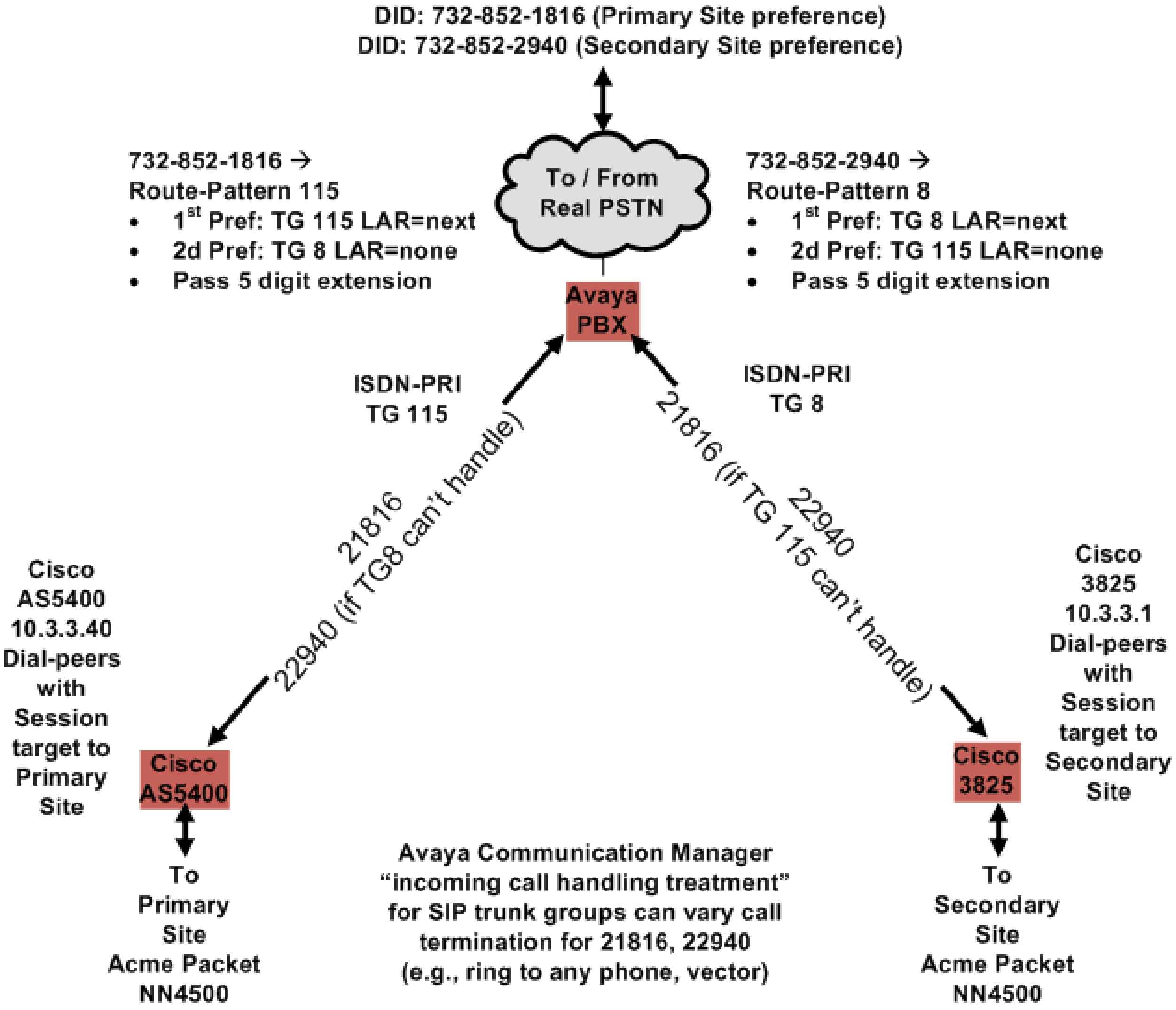

DID: 732-852-1816 (Primary Site preference)
DID: 732-852-2940 (Secondary Site preference)
To / From Real PSTN
732-852-1816 →
Route-Pattern 115
• 1st Pref: TG 115 LAR=next
• 2d Pref: TG 8 LAR=none
• Pass 5 digit extension
732-852-2940 →
Route-Pattern 8
• 1st Pref: TG 8 LAR=next
• 2d Pref: TG 115 LAR=none
• Pass 5 digit extension
Avaya PBX
ISDN-PRI TG 115
ISDN-PRI TG 8
21816
22940 (if TG8 can't handle)
22940
21816 (if TG 115 can't handle)
Cisco AS5400 10.3.3.40 Dial-peers with Session target to Primary Site
Cisco AS5400
Cisco 3825 10.3.3.1 Dial-peers with Session target to Secondary Site
Cisco 3825
To Primary Site Acme Packet NN4500
To Secondary Site Acme Packet NN4500
Avaya Communication Manager "incoming call handling treatment" for SIP trunk groups can vary call termination for 21816, 22940 (e.g., ring to any phone, vector)

Figure 2: Incoming Calls to the Enterprise from the PSTN

1.2. Session Director and Communication Manager Terminology

The table below provides a "translation" for key concepts and terminology that may be helpful to readers familiar with Acme Packet Session Director or Avaya Aura™ Communication Manager, but not both. Of course, these analogies are imperfect, so the table is intended only as a starting point in understanding.

Acme Packet Concept	**Avaya Aura™ Communication Manager Concept**	**Notes**
Session-agent (SIP)	SIP Signaling Group and SIP Trunk Group	The session-agent defines a SIP peer, similar to an Avaya SIP signaling group/trunk group.
Session-agent group (SAG)	Route-Pattern with multiple SIP Trunk Groups	Session agents can be configured in a SAG, so that routing to the SAG can use any session agent in the group. The analogy is imperfect in that the SAG can use strategies that select agents from the SAG based on real-time traffic conditions and defined constraints (i.e., more sophisticated load balancing options)
Sag-recursion	Look-Ahead Routing (LAR) for a route-pattern	If a session agent is selected, but a "downstream" failure results, sag-recursion can trigger Session Director to automatically use a different session agent in the SAG. This is similar to Communication Manager selection of a SIP trunk group, followed by a downstream signaling failure causing LAR (route-advance) to the next trunk in the route pattern.
Session-agent configuration for "ping-method OPTIONS"	"Enable Layer 3 Test" = "y" for the SIP Signaling Group	Both Communication Manager and Acme Packet can be configured to source OPTIONS messages to check the health of a peer. See Section 1.3 for more information.

To summarize the Acme Packet Net-Net 4500 configuration in Section 4, each C-LAN represents a "session agent". A "session agent group" (SAG) is configured to group the C-LANs, and a strategy for distribution of calls to the session agents that are members of the group is specified. In the sample configuration, once an inbound call reaches an enterprise site, the Session Director is configured for round-robin call distribution to the two C-LANs at the site that are members of the session agent group. If connectivity to a particular C-LAN fails, and the Acme Packet Net-Net 4500 has not yet detected the failure, an inbound call directed to the failed C-LAN will encounter a "transaction timeout". The transaction timeout will cause the call to be directed to the other C-LAN at the same site automatically. In addition, the session agent for the failed C-LAN will be marked out-of-service so that subsequent inbound calls will flow to an operational C-LAN without experiencing the timeout. If all C-LANs that are part of the session agent group experience a transaction timeout, then a SIP 408 message would be returned to the SIP Service Provider. If all C-LANs that are part of the session agent group are already marked out of service, then a SIP 503 Service Unavailable would be returned to the SIP Service Provider. Similarly, if the public side of the Session Director experienced failures for an outbound call from Communication Manager, Communication Manager would receive no SIP response after 100 TRYING, a 408 Transaction Timeout, or a 503 Service Unavailable, depending on the particular failure scenario. Note that all these conditions are triggers for Communication Manager Look-Ahead Routing. Reference [LAR] documents another sample configuration for Look-Ahead Routing, and includes a more complete list of SIP triggers.

In the sample configuration, the Acme Packet Net-Net 4500 at a given site does not have session agents to C-LANs at the other site. It is presumed that a production SIP Service Provider can redirect calls from one site to another based on failure conditions, such as a timeout, or the return of a 503 Service Unavailable. If this is not the case, or there are other reasons to avoid leveraging the service provider's failover capability for an internal enterprise failure, each Acme Packet Net-Net Session Director could be configured with session agents and session agent groups to reach C-LANs at both sites.

1.3. SIP OPTIONS Message, Service States, and Call Acceptance

Both Communication Manager and the Acme Packet Net-Net 4500 can use a SIP OPTIONS message to verify connectivity health. This section summarizes the use of the SIP OPTIONS message, the implications for in-service and out-of-service determinations, and the effect on new call attempts. See Section 5.7 for Wireshark traces related to the topics in this section.

In the sample configuration, the Acme Packet Net-Net 4500 is configured to periodically check the availability of a session agent (e.g., C-LAN) via a SIP OPTIONS message. The interval between SIP OPTIONS messages is configurable. By default, any SIP response would be considered an acceptable reply, including normal "200 OK" responses, but also other responses such as "503 Unavailable". The responses from Communication Manager deemed acceptable for marking the session agent in-service can be configured, if desired. Although a failed SIP OPTIONS exchange can result in a session agent being marked out-of-service, in a system with continuous call activity, it would be more likely that a transaction timeout for a SIP method such as INVITE would cause a recently failed session agent to be marked out-of-service. In this light, the SIP OPTIONS exchange is more likely to be the method of bringing a previously failed session-agent back in service. Therefore, if rapid recovery from prior failures is paramount, the time between SIP OPTIONS generated by the Acme Packet Net-Net 4500 can be reduced to a low value. In the sample configuration, testing was done with a 60 second interval, and later with a 16 second interval.

If the Acme Packet Net-Net 4500 has marked a session-agent out-of-service, the session agent will not be chosen for call activity. That is, if both an out-of-service session agent and an in-service session agent appear in the same session agent group, the in-service session agent will naturally be chosen for the next call. The out-of-service session agent can come back in-service either via a response from the Avaya C-LAN to an Acme Packet sourced SIP OPTIONS message, or due to a SIP message, such as an INVITE or OPTIONS received from the Avaya C-LAN. Indeed, if an INVITE message for a Communication Manager outbound call is received by the Acme Packet Net-Net 4500 from a session agent that had been marked out-of-service, the

INVITE is processed, the call can succeed, and the session agent is again marked in-service. For the reader familiar with Avaya trunk states, this is similar to the Communication Manager behavior for a trunk marked in the "Out-of-service/Far-end" state.

When an Avaya SIP signaling group is marked with "Enable Layer 3 Test" = "y", Communication Manager will periodically send a SIP OPTIONS method to the far-end of the signaling group. When the Acme Packet Net-Net 4500 receives such a SIP OPTIONS, it checks the logical "next-hop". In the sample configuration, the "next hop" is the SIP Service Provider. If there is no in-service next-hop, then the Acme Packet Net-Net 4500 returns a 503 Service Unavailable to Communication Manager. Communication Manager will then mark the SIP signaling group for "bypass", and the corresponding SIP trunk group will be marked "Out-of-service/Far-end". For example, if the Acme Packet Net-Net 4500 has detected that the SIP Service Provider network has failed, then a SIP OPTIONS from the Avaya C-LAN will receive a 503, and the Avaya trunks will be marked for bypass, which is appropriate. In this state, although outbound calls from the enterprise will not select the trunk, if an inbound call is received, the network has apparently recovered. The call will be accepted, and the Avaya SIP trunk group will be marked in-service.

1.4. Summary of Outbound Calls from the Enterprise to the PSTN

For outbound calls, Communication Manager location-based routing can direct outgoing calls from users at a given site to the SIP trunks in the same site, with fail-over to use SIP trunks at the other site as needed. The user dials the Automatic Route Selection (ARS) access code followed by the PSTN number. In the sample configuration, if a user at the primary site dials the number, the call will be directed to route-pattern 30, which lists the SIP trunks at the primary site first. If the trunks at the primary site are unable to take the call, either due to congestion or failure, the call will proceed out the trunks at the secondary site, which are also members of route-pattern 30. Outbound calls placed from users at the secondary site are directed to route-pattern 60, which lists the SIP trunks at the secondary site first, with overflow and fail-over to the SIP trunks at the primary site.

2. Equipment and Software Validated

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

Equipment	Software
Avaya S8730 Servers (Main)	Avaya Aura™ Communication Manager Release 5.2 (947.3)
Avaya S8500 Server (ESS)	Avaya Aura™ Communication Manager Release 5.2 (947.3)
Avaya 4600-Series Telephones (H.323)	Release 2.8.3 – H.323
Avaya 9600-Series Telephones (H.323)	Release 3.0 – H.323
Avaya 2400-Series Digital Telephones	N/A
Acme Packet Net-Net 4500 Session Directors	CX6.1.0 patch 3
Cisco AS5400 Universal Gateway	12.4(15)T7
Cisco 3825 Integrated Services Router	12.4(11)XW7

3. Avaya Aura™ Communication Manager Configuration

This section describes aspects of the Communication Manager configuration to support the network shown in **Figure 1**. Both references [JSR] and [AP-HA] give prescriptive instructions for configuring the connectivity between Communication Manager and Acme Packet Session Director. Product documentation can be found in references [CM1], [CM2], [CM3], and [ESS]. In these Application Notes, sufficient detail is shown to document the configuration, but the focus is not on step-by-step configuration, but rather on understanding the expected results. All configuration is illustrated via System Access Terminal (SAT) screens, and some screens may be abridged for brevity.

A license file controls availability of Communication Manager features and capacities. It is assumed that appropriate licensing is in place to support a multi-site configuration with ESS, SIP Trunking, announcements, and other illustrated features.

3.1. Node Names

Node names are mappings of names to IP Addresses that can be used in various screens. The following abridged list output shows the relevant node-names in the sample configuration. Shown in bold are the entries for the C-LAN interfaces that will be the near-end of Avaya SIP signaling groups, and the Acme Packet Net-Net 4500 entries that will be the far-end of Avaya SIP signaling groups.

```
list node-names all                                                  Page   1
                        NODE NAMES
Type     Name               IP Address
IP       ESSCid002Sid003    2.2.185.88
IP       Gateway001         2.2.185.1
IP       Gateway002         2.2.85.1
IP       Gateway003         2.2.26.1
IP       Gateway004         2.2.4.1
IP       S83LSP-in-G250     2.2.25.88
IP       S83LSP-in-G700     2.2.1.88
IP       ShdVirt02A07       2.2.26.4
IP       c-lan              2.2.185.2
IP       c-lan1A10          2.2.185.20
IP       c-lan2a02          2.2.85.2
IP       c-lan2b02          2.2.85.20
IP       nn4500-prisite     2.2.85.45
IP       nn4500-secsite     2.2.185.145
IP       tn2602-1a11        2.2.185.4
IP       tn2602-2a07        2.2.26.3
IP       tn2602-2b07        2.2.26.2
IP       val-1a07           2.2.185.25
IP       val-2a08           2.2.85.25
```

3.2. Network Regions

Network regions provide a means to logically group resources. As indicated in **Figure 1**, region 3 is used at the primary site, and region 1 is used at the secondary site, to logically group phones, media processors and other resources.

Non-IP telephones (e.g., analog, digital) derive network region and location configuration from the Avaya gateway to which the device is connected. The following display command shows that cabinet 1 is an Avaya G650 Media Gateway configured for network region 1 and location 1. In the sample configuration, cabinet number 1 is in the "secondary site".

```
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: right         Room: demo         Floor:             Building: Demo-Room

 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
```

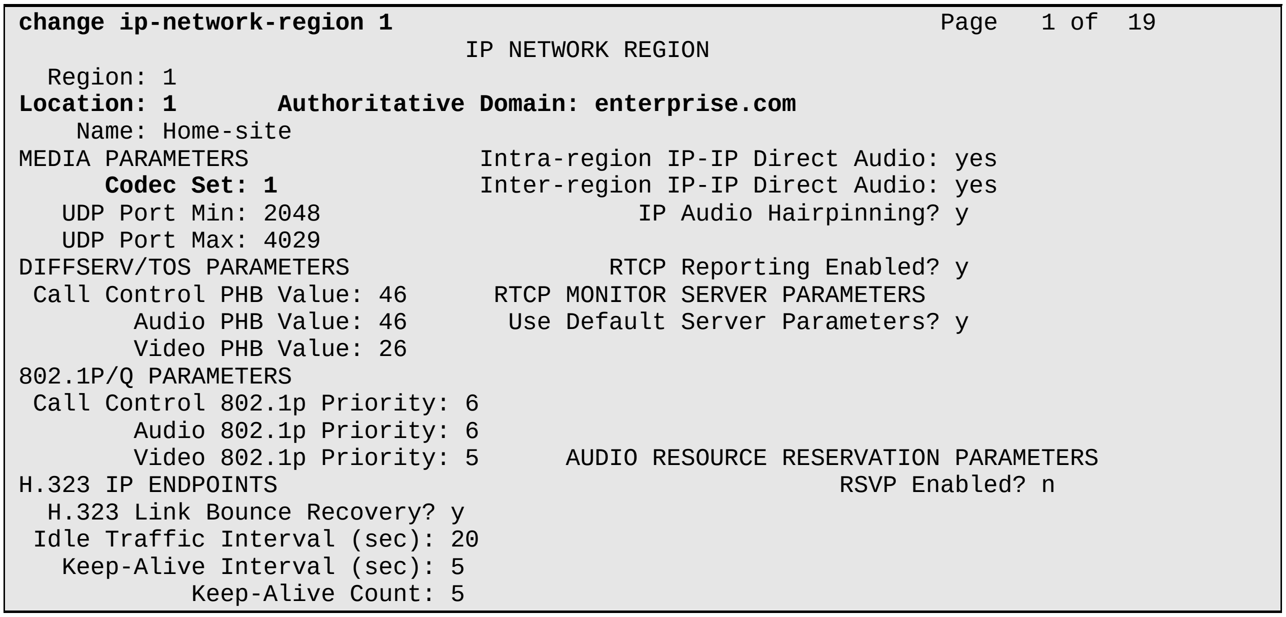
The following display command shows that cabinet 2 is an Avaya G650 Media Gateway stack configured for network region 3 and location 3. In the sample configuration, cabinet number 2 is in the “primary site”.

```
display cabinet 2
                                    CABINET
 CABINET DESCRIPTION
                  Cabinet: 2
           Cabinet Layout: G650-rack-mount-stack
             Cabinet Type: expansion-portnetwork

                 Location: 3         IP Network Region: 3

 Rack: center        Room: demo         Floor:             Building: Demo-Room

 CARRIER DESCRIPTION
   Carrier       Carrier Type        Number

      E        not-used            PN  02
      D        not-used            PN  02
      C        not-used            PN  02
      B        G650-port           PN  02
      A        G650-port           PN  02
```

IP telephones can be assigned a network region based on an IP address mapping. The network region can also associate the IP telephone to a location for location-based routing decisions. The following screen illustrates a subset of the IP network map configuration used to verify these Application Notes. If the IP address of a registering IP Telephone does not appear in the ip-network-map, the phone is assigned the network region of the C-LAN to which it registers. When the IP address of a registering IP telephone is in the ip-network-map, the phone is assigned the network region assigned by the form shown below. Avaya IP Telephones with IP Addresses in the primary site are mapped to network region 3. For example, the specific IP address 2.2.1.109 is mapped to network region 3. Avaya IP Telephones with IP Addresses in the secondary site are mapped to network region 1. For example, the range of IP addresses from 2.2.185.200 through 2.2.185.250 is mapped to network region 1.

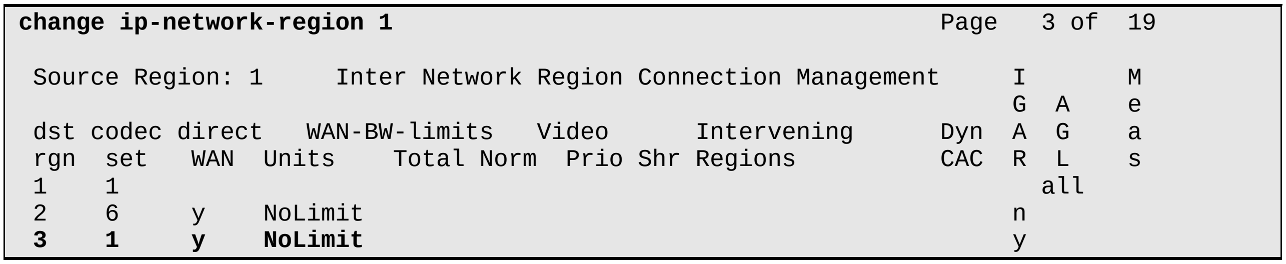
```
change ip-network-map                                           Page   1 of  63
                               IP ADDRESS MAPPING
                                              Subnet Network     Emergency
 IP Address                                   Bits   Region VLAN Location Ext
 --------------------------------------------- ------ ------ ---- -------------
  FROM: 2.2.1.109                               /      3      n
   TO: 2.2.1.109

  FROM: 2.2.185.200                            /       1      n
   TO: 2.2.185.250
```

The following screen shows IP Network Region 1 configuration. Note that location 1 has been assigned to region 1. IP Telephones in region 1 that make ARS calls can consult the ARS location-specific tables for location 1. Connections within network region 1 use codec set 1 by virtue of the “Codec Set” configuration shown on Page 1 below.



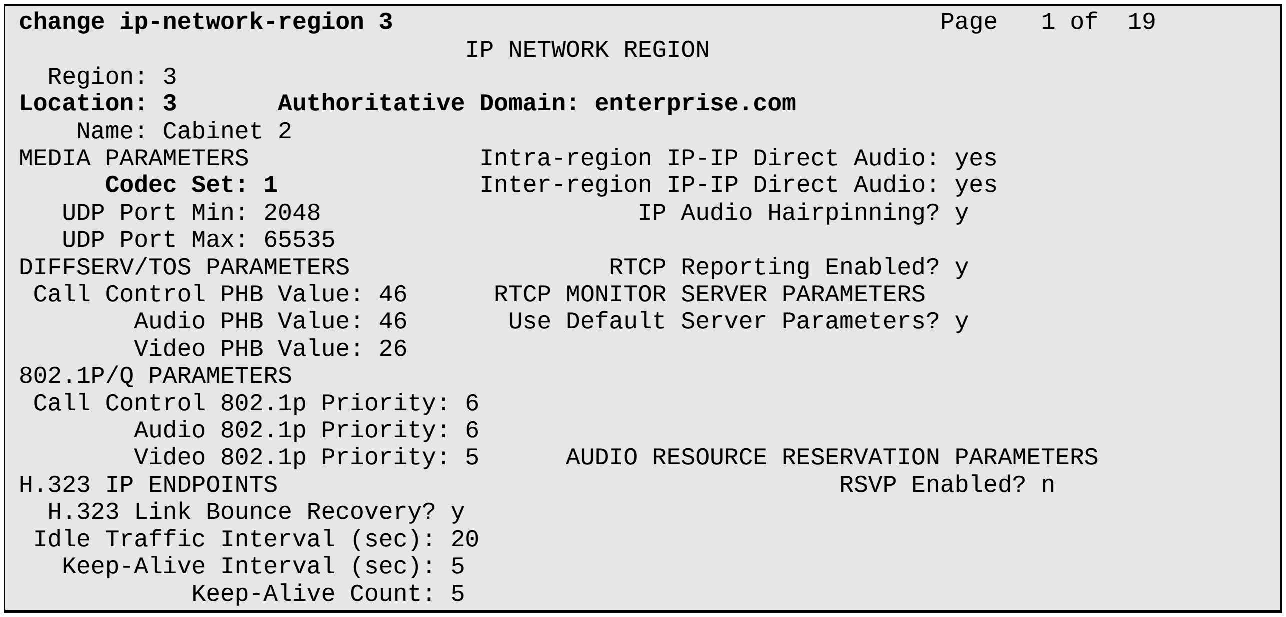
```
change ip-network-region 1                                      Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: enterprise.com
    Name: Home-site
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? y
   UDP Port Max: 4029
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
```

The following screen shows the inter-network region connection configuration for region 1. The bold row shows that network region 1 is directly connected to network region 3, and that codec set 1 will also be used for connections between region 1 and region 3. If a different codec should be used for inter-region connectivity than for intra-region connectivity (**Page 1**), a different codec set can be entered in the codec set field for the appropriate row in the screen shown below. Once submitted, the configuration becomes symmetric, meaning that network region 3, Page 3 will also show codec set 1 for region 3 – region 1 connectivity.



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

 Source Region: 1     Inter Network Region Connection Management     I       M
                                                                     G  A    e
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    a
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    s
 1    1                                                                 all
 2    6     y    NoLimit                                             n
 3    1     y    NoLimit                                             y
```

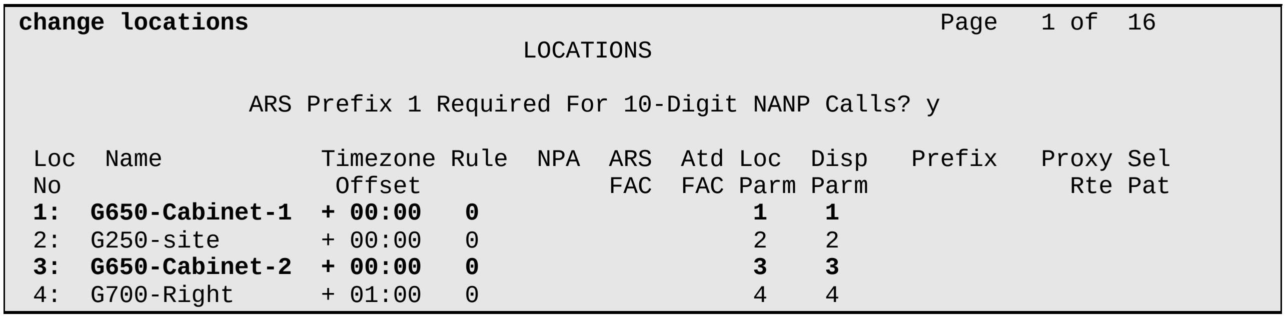
The following screen shows IP Network Region 3 configuration. Note that location 3 has been assigned to region 3. IP Telephones in region 3 that make ARS calls can consult the ARS location-specific tables for location 3. Other parameters are similar to region 1.



```
change ip-network-region 3                                      Page   1 of  19
                               IP NETWORK REGION
  Region: 3
Location: 3       Authoritative Domain: enterprise.com
    Name: Cabinet 2
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? y
   UDP Port Max: 65535
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
```

3.3. Locations

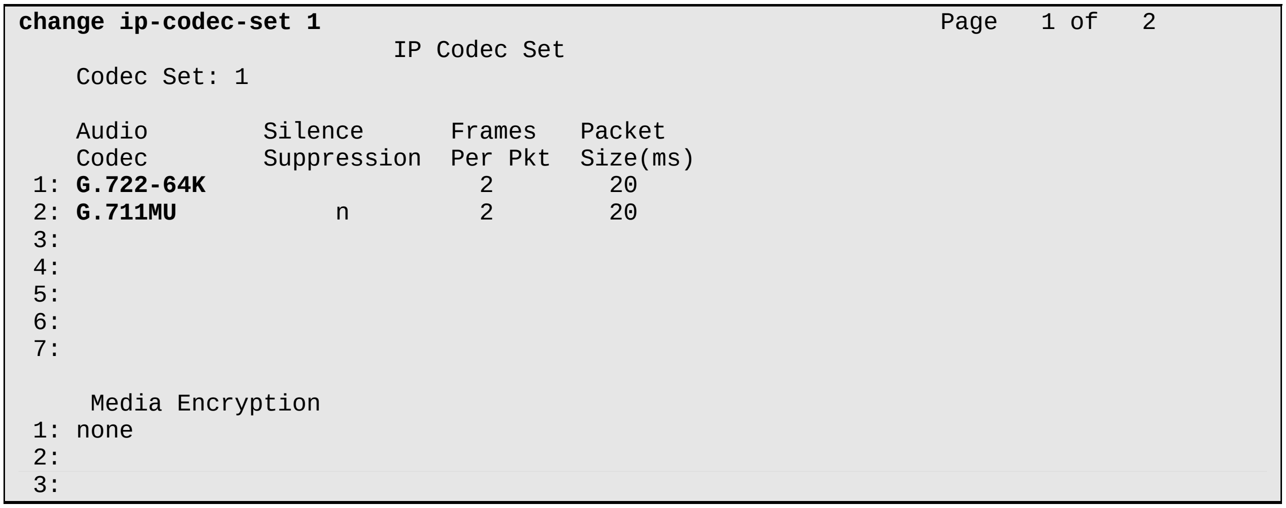
The “change locations” screen allows other location-specific parameters to be defined in a multi-location system, if needed.



```
change locations                                                Page   1 of  16
                                   LOCATIONS

                ARS Prefix 1 Required For 10-Digit NANP Calls? y

 Loc  Name           Timezone Rule  NPA  ARS  Atd Loc  Disp   Prefix   Proxy Sel
 No                   Offset             FAC  FAC Parm Parm              Rte Pat
 1:  G650-Cabinet-1  + 00:00   0                   1    1
 2:  G250-site       + 00:00   0                   2    2
 3:  G650-Cabinet-2  + 00:00   0                   3    3
 4:  G700-Right      + 01:00   0                   4    4
```

3.4. IP Codec Sets

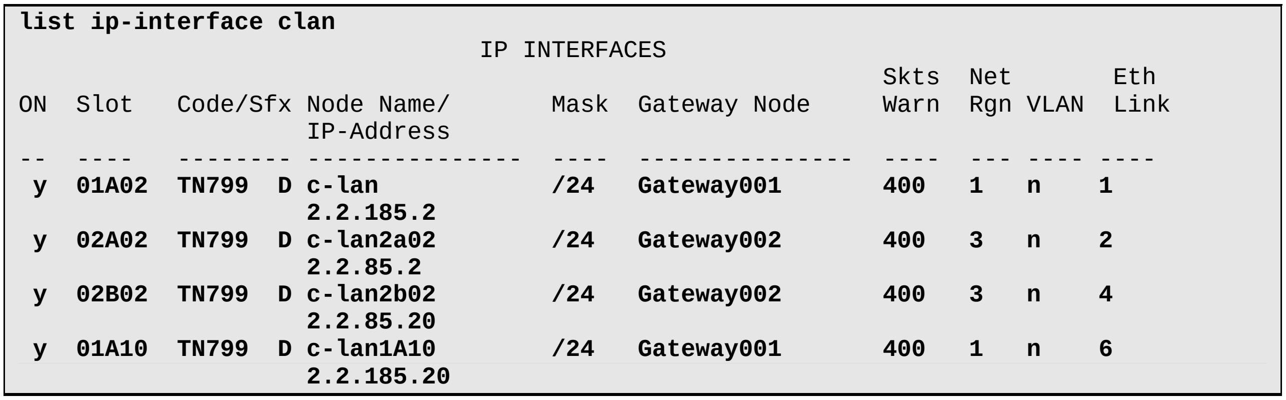
The following screen shows the configuration for codec set 1. In general, an IP codec set is a list of allowable codecs in priority order. In the sample configuration, all calls to and from the PSTN via the SIP trunks will use G.711MU. Other calls using this same codec set that are between devices capable of the G.722-64K codec (e.g., Avaya 9600-Series IP Telephone) can use G.722.



```
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.722-64K                   2        20
 2: G.711MU           n         2        20
 3:
 4:
 5:
 6:
 7:

     Media Encryption
 1: none
 2:
 3:
```

3.5. IP Interfaces

The following screen lists the C-LAN interfaces relevant to the sample configuration. Both the primary site and secondary site have a pair of TN799DP cards that interface to the Acme Packet Net-Net 4500 at that site. The primary site C-LANs are configured in network region 3, and the secondary site C-LANs are configured in network region 1.



```
list ip-interface clan
                                IP INTERFACES
                                                            Skts  Net       Eth
ON  Slot   Code/Sfx Node Name/       Mask  Gateway Node     Warn  Rgn VLAN  Link
                    IP-Address
--  ----   -------- ---------------  ----  ---------------  ----  --- ---- ----
 y  01A02  TN799  D c-lan            /24   Gateway001       400   1   n    1
                    2.2.185.2
 y  02A02  TN799  D c-lan2a02        /24   Gateway002       400   3   n    2
                    2.2.85.2
 y  02B02  TN799  D c-lan2b02        /24   Gateway002       400   3   n    4
                    2.2.85.20
 y  01A10  TN799  D c-lan1A10        /24   Gateway001       400   1   n    6
                    2.2.185.20
```

The following screen lists the media processor interfaces relevant to the sample configuration. The primary site has a pair of TN2602 in an active/standby configuration in network region 3. In such a configuration, it is the IP Address associated with the Virtual Node (i.e., ShdVirt2A07 = 2.2.26.4) that will be evident in the verifications in Section 5. The secondary site has a single TN2602 in network region 1.

```
list ip-interface medpro
                                IP INTERFACES
                                                       Net
ON Slot  Code/Sfx Node Name/      Mask Gateway Node    Rgn VLAN Virtual Node
                  IP-Address
-- ----- -------- --------------- ---- -------------- --- ---- ---------------
 y 02A07 TN2602   tn2602-2a07     /24  Gateway003      3   n    ShdVirt02A07
                  2.2.26.3
 y 02B07 TN2602   tn2602-2b07     /24  Gateway003      3   n    ShdVirt02A07
                  2.2.26.2
 y 01A11 TN2602   tn2602-1a11     /24  Gateway001      1   n
                  2.2.185.4
```

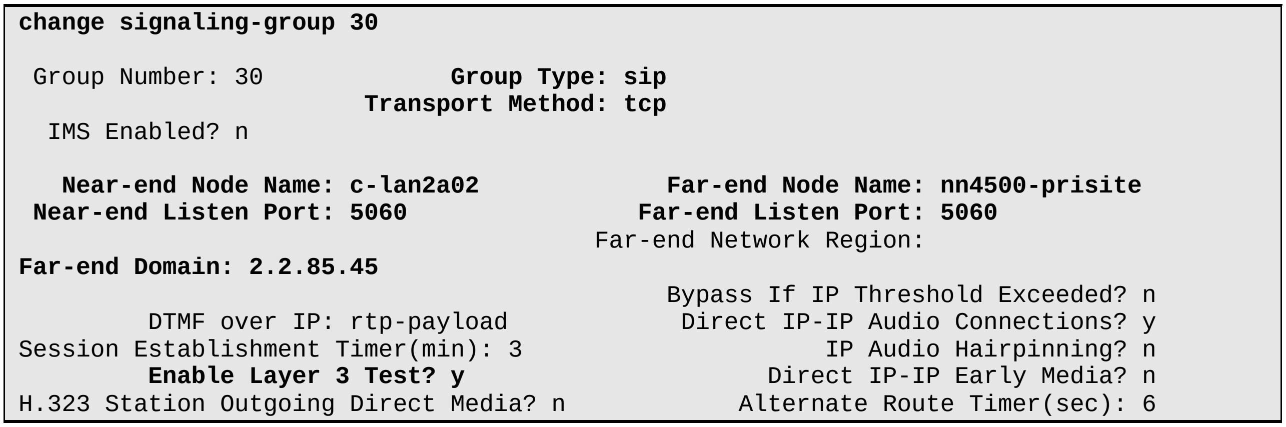
The following screen lists the TN2501 announcement interfaces in the system. There is one TN2501 configured at the primary site, and one TN2501 configured at the secondary site. Audio groups are used allowing either TN2501 to source the same announcement, for efficiency and redundancy benefits.

```
list ip-interface val
                                IP INTERFACES
ON Slot Code Sfx Node Name           IP Address  /Mask  Gateway Address  V-LAN
-- ---- ---- --- -----------------  ------------------  ---------------  -----
y 01A07 TN2501   val-1a07           2.2.185.25     /24  Gateway001       n
y 02A08 TN2501   val-2a08           2.2.85.25      /24  Gateway002       n
```

3.6. SIP Signaling Groups

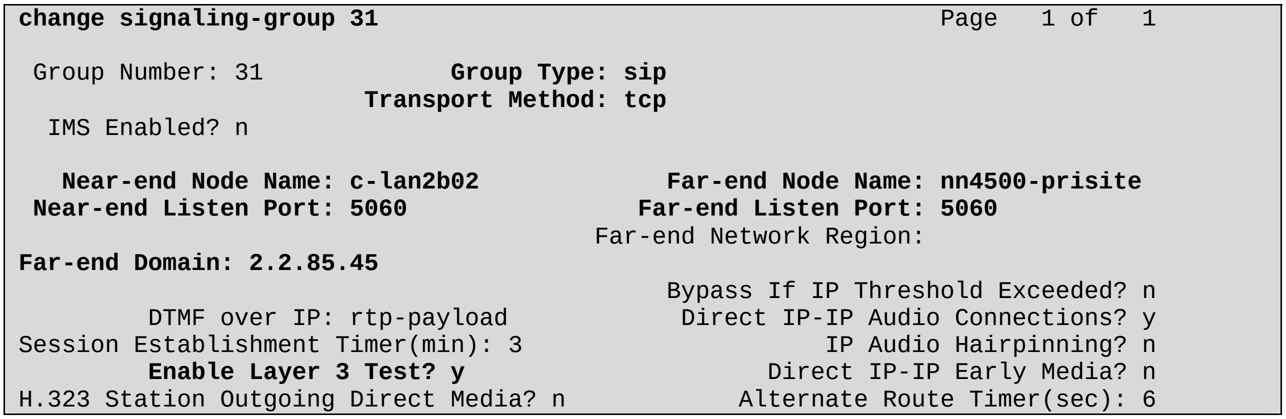
This section illustrates the configuration of the SIP Signaling Groups to the Acme Packet Net-Net 4500. Each signaling group has a "Group Type" of "sip", and a "Near-end Node Name" of a C-LAN interface. The "Far-end Node Name" is the node name of an Acme Packet Net-Net 4500. The "Transport Method" for all signaling groups is "tcp" using port 5060. The "Far-end Domain" for each signaling group is the "inside" IP Address of the appropriate Acme Packet Net-Net 4500. The "Enable Layer 3 Test" field is enabled to allow Communication Manager to maintain the signaling group using the SIP OPTIONS method, as described in Section 1.3. Other fields can be left at default values, including "DTMF over IP" set to "rtp-payload" which corresponds to RFC 2833. Note that the "Alternate Route Timer" that defaults to 6 seconds impacts fail-over timing for outbound calls. If Communication Manager does not get an expected response, Look-Ahead Routing can be triggered, after the expiration of the Alternate Route Timer. See the example verifications in Section 5.6.

The following screen shows signaling group 30. The near-end is the C-LAN labeled with "Induced Failure Reference Number 3" in **Figure 1**. The far-end is the Acme Packet Net-Net 4500 at the primary site. Optionally, the "Far-end Network Region" can be configured with a network region number, to logically associate the SIP Service Provider to a region, for codec-selection, call admission control, or other reasons.



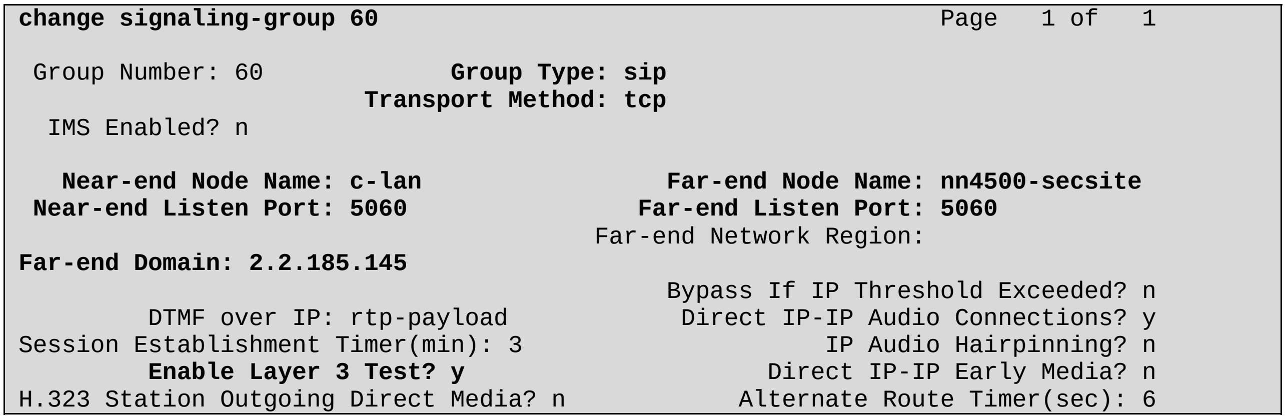
```
change signaling-group 30

 Group Number: 30             Group Type: sip
                        Transport Method: tcp
  IMS Enabled? n

   Near-end Node Name: c-lan2a02             Far-end Node Name: nn4500-prisite
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region:
Far-end Domain: 2.2.85.45
                                             Bypass If IP Threshold Exceeded? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                     Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

The following screen shows signaling group 31. The near-end is the C-LAN labeled with "Induced Failure Reference Number 3A" in **Figure 1**. The far-end is the Acme Packet Net-Net 4500 at the primary site.



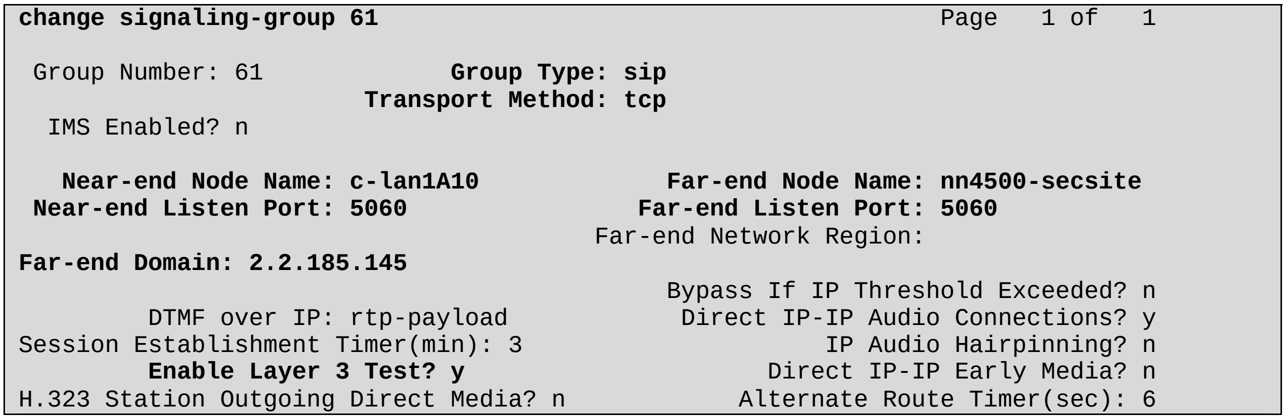
```
change signaling-group 31                                       Page   1 of   1

 Group Number: 31             Group Type: sip
                        Transport Method: tcp
  IMS Enabled? n

   Near-end Node Name: c-lan2b02             Far-end Node Name: nn4500-prisite
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region:
Far-end Domain: 2.2.85.45
                                             Bypass If IP Threshold Exceeded? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                     Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

The following screen shows signaling group 60. The near-end is the C-LAN labeled with “Induced Failure Reference Number 6” in **Figure 1**. The far-end is the Acme Packet Net-Net 4500 at the secondary site.



```
change signaling-group 60                                          Page   1 of   1

 Group Number: 60              Group Type: sip
                        Transport Method: tcp
  IMS Enabled? n

   Near-end Node Name: c-lan                  Far-end Node Name: nn4500-secsite
 Near-end Listen Port: 5060                 Far-end Listen Port: 5060
                                         Far-end Network Region:
Far-end Domain: 2.2.185.145
                                              Bypass If IP Threshold Exceeded? n
         DTMF over IP: rtp-payload             Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                      IP Audio Hairpinning? n
         Enable Layer 3 Test? y                     Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

The following screen shows signaling group 61. The near-end is the C-LAN labeled with “Induced Failure Reference Number 6A” in **Figure 1**. The far-end is the Acme Packet Net-Net 4500 at the secondary site.



```
change signaling-group 61                                          Page   1 of   1

 Group Number: 61              Group Type: sip
                        Transport Method: tcp
  IMS Enabled? n

   Near-end Node Name: c-lan1A10              Far-end Node Name: nn4500-secsite
 Near-end Listen Port: 5060                 Far-end Listen Port: 5060
                                         Far-end Network Region:
Far-end Domain: 2.2.185.145
                                              Bypass If IP Threshold Exceeded? n
         DTMF over IP: rtp-payload             Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                      IP Audio Hairpinning? n
         Enable Layer 3 Test? y                     Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

3.7. SIP Trunk Groups

This section illustrates the configuration of the SIP Trunks Groups to the Acme Packet Net-Net 4500. Four SIP trunk groups are configured, corresponding to the four signaling groups defined in the previous section. Each trunk group has a “Group Type” of “sip”.

The following shows page 1 for trunk group 30. The “Number of Members” field defines how many simultaneous calls are permitted for the trunk group, and can be coordinated with Acme Packet Net-Net 4500 call admission control features if desired.

```
change trunk-group 30                                           Page   1 of  21
                                TRUNK GROUP
Group Number: 30                   Group Type: sip           CDR Reports: y
  Group Name: SIP-PSTN-30                 COR: 1        TN: 1        TAC: 130
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                                       Signaling Group: 30
                                                     Number of Members: 10
```

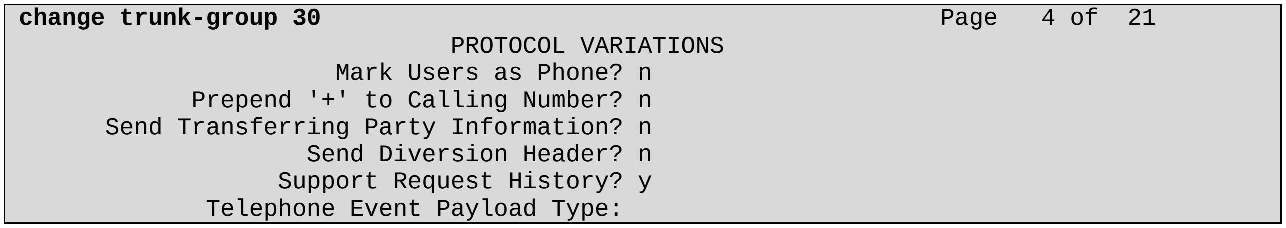
The following shows Page 2 for trunk group 30. All parameters shown are default values, except for the “Preferred Minimum Session Refresh Interval”, which has been changed from 600 to 900 to avoid unnecessary SIP messaging with the Cisco products used to simulate the SIP Service Provider. As such, this screen will not be repeated for the other trunk groups.

```
change trunk-group 30                                           Page   2 of  21
      Group Type: sip
TRUNK PARAMETERS
     Unicode Name: yes
                                            Redirect On OPTIM Failure: 5000
            SCCAN? n                               Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 900
```

The following shows Page 3 for trunk group 30. All parameters shown are at default values. As such, this screen will not be repeated for the other trunk groups.

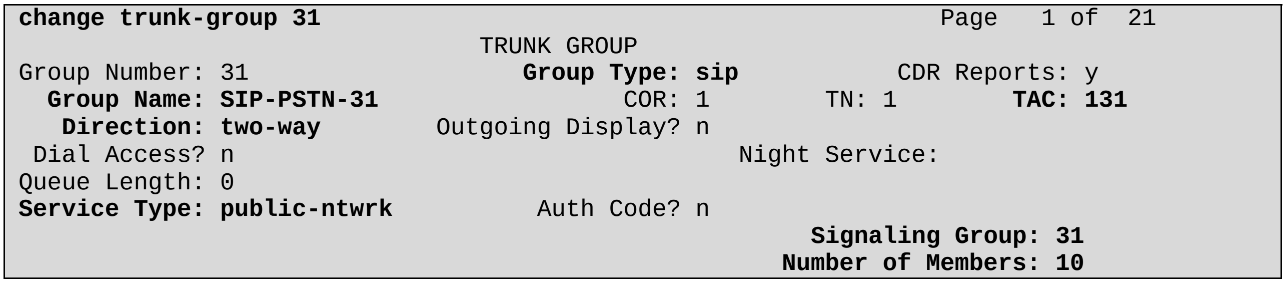
```
change trunk-group 30                                           Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y
                     Numbering Format: public
                                                UUI Treatment: service-provider

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

The following shows Page 4 for trunk group 30. All parameters shown are at default values. As such, this screen will not be repeated for the other trunk groups. Depending on the service provider, it may be necessary to enter a specific value, such as 101, in the “Telephone Event Payload Type” associated with DTMF signaling. Check with the specific service provider. Similarly, some service providers may require that the fields “Support Request History” and “Send Diversion Header” be changed from default values for proper support of redirection features such as Extension to Cellular or call forwarding off-net.



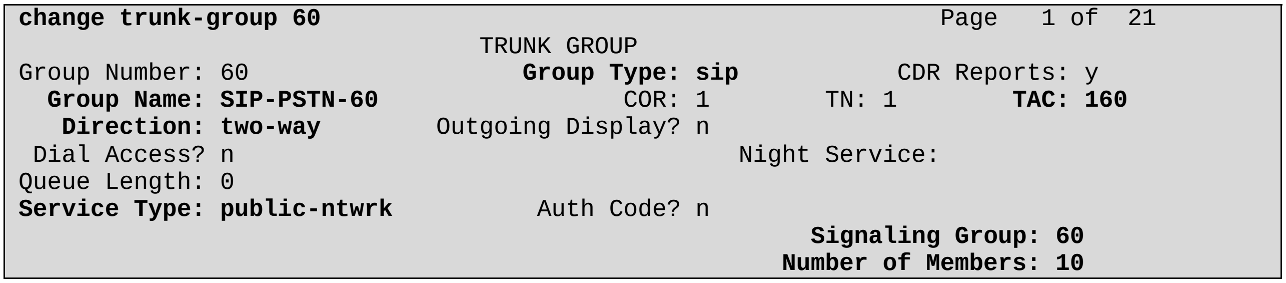
```
change trunk-group 30                                           Page   4 of  21
                              PROTOCOL VARIATIONS
                      Mark Users as Phone? n
            Prepend '+' to Calling Number? n
      Send Transferring Party Information? n
                    Send Diversion Header? n
                  Support Request History? y
             Telephone Event Payload Type:
```

The following shows Page 1 for trunk group 31.



```
change trunk-group 31                                           Page   1 of  21
                                TRUNK GROUP
Group Number: 31                   Group Type: sip           CDR Reports: y
  Group Name: SIP-PSTN-31                 COR: 1        TN: 1        TAC: 131
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                                       Signaling Group: 31
                                                     Number of Members: 10
```

The following shows Page 1 for trunk group 60.



```
change trunk-group 60                                           Page   1 of  21
                                TRUNK GROUP
Group Number: 60                   Group Type: sip           CDR Reports: y
  Group Name: SIP-PSTN-60                 COR: 1        TN: 1        TAC: 160
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                                       Signaling Group: 60
                                                     Number of Members: 10
```

The following shows Page 1 for trunk group 61.

```
change trunk-group 61                                           Page   1 of  21
                                TRUNK GROUP
Group Number: 61                   Group Type: sip          CDR Reports: y
  Group Name: SIP-PSTN-61                 COR: 1        TN: 1        TAC: 161
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                                       Signaling Group: 61
                                                     Number of Members: 10
```

3.8. Route Patterns

Route pattern 30 will be used for calls that prefer the SIP trunks at the primary site (trunk groups 31 and 30), but may use the SIP trunk at the secondary site (trunk groups 60 and 61) if the SIP trunks at the primary site are busy or failed. Note also that Look-Ahead Routing (LAR) is set to "next". As an example of LAR, assume the Acme Packet 4500 at the primary site has just failed, and Communication Manager has not yet marked trunks 31 and 30 out-of-service. Assume that an outbound call is made that chooses this route-pattern. The call can use "LAR" for automatic "route-advance" to complete successfully using the SIP trunks at the secondary site. Digit manipulation can be performed on the number, if needed. In the sample configuration, the leading digit (i.e., the 1) is deleted and a 10 digit number is sent. (This may not be representative of the numbering scheme expected by a production SIP Service Provider.)

```
change route-pattern 30                                        Page   1 of   3
                    Pattern Number: 30  Pattern Name: SIP-PSTN-P
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                               DCS/ IXC
    No          Mrk Lmt List Del  Digits                                 QSIG
                             Dgts                                        Intw
 1: 31   0                    1                                           n   user
 2: 30   0                    1                                           n   user
 3: 60   0                    1                                           n   user
 4: 61   0                    1                                           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                                            next
 3: y y y y y n  n            rest                                            next
 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
```

Route pattern 60 will be used for calls that prefer the SIP trunks at the secondary site (trunk groups 61 and 60), but may use the SIP trunk at the primary site (trunk groups 30 and 31) if the SIP trunks at the secondary site are busy or failed. As with route-pattern 30, LAR is configured to “next” to allow calls to complete automatically using the primary site trunks in failure scenarios.

```
change route-pattern 60                                        Page   1 of   3
                    Pattern Number: 60  Pattern Name: SIP-PSTN-S
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                            DCS/ IXC
    No          Mrk Lmt List Del  Digits                              QSIG
                             Dgts                                     Intw
 1: 61   0                    1                                        n   user
 2: 60   0                    1                                        n   user
 3: 30   0                    1                                        n   user
 4: 31   0                    1                                        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                                       next
 3: y y y y y n  n            rest                                       next
 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
```

3.9. Administer Public Numbering

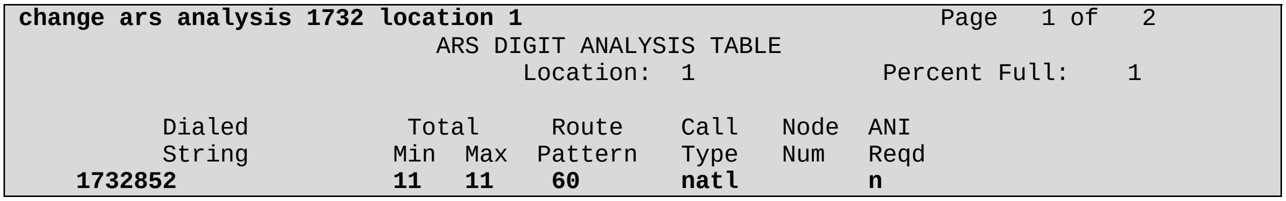
The “change public-unknown-numbering” command may be used to define the format of the calling party number to be sent. In the bolded rows shown in the abridged output below, all calls originating from a 5-digit extension beginning with 52 (i.e., 52XXX) will be prefixed with 732852, and a 10 digit calling party number of the form 7328522XXX will be sent, when the SIP trunk groups (30, 31, 60, 61) in the configuration are chosen for the call. Although not shown, similar configuration covered other telephone extension ranges, such as 51XXX.

```
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: 13
 5  5                                        5          Maximum Entries: 9999
 5  52              30        732852        10
 5  52              31        732852        10
 5  52              60        732852        10
 5  52              61        732852        10
```

3.10. Configure ARS Analysis For Outbound Call Routing

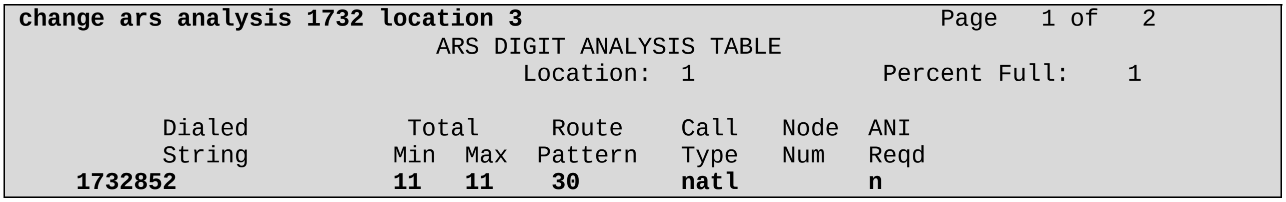
Location-based routing is configured so that users at different locations that dial the same telephone number can have calls choose different route-patterns and trunks. In the sample configuration, users at the primary site that dial PSTN telephone numbers will preferentially use trunks at the primary site. Similarly, users at the secondary site that dial PSTN telephone numbers will preferentially use trunks at the secondary site. Upon congestion or failure, calls can use the alternate site's trunks.

The following screen shows a sample ARS configuration for location 1. If a user at location 1, such as extension 51003, dials the ARS access code followed by 1-732-852-XXXX, the call will select route pattern 60.



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

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    1732852               11   11    60       natl         n
```

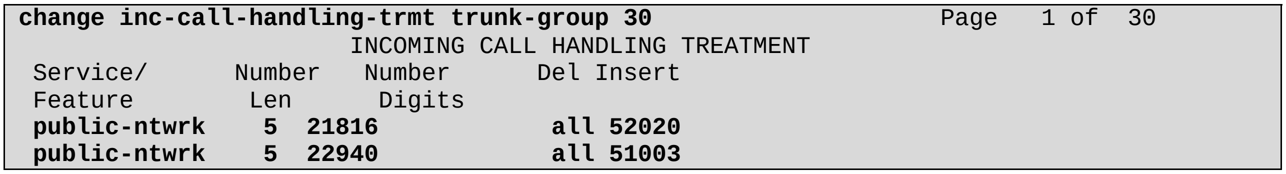
The following screen shows a sample ARS configuration for location 3. If a user at location 3, such as extension 52020, dials the ARS access code followed by 1-732-852-XXXX, the call will select route pattern 30.



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

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    1732852               11   11    30       natl         n
```

3.11. Configure Incoming Call Handling Treatment For Inbound Digit Manipulation

The "incoming call handling treatment" for a trunk group can be used to manipulate the digits received for an incoming call. In the sample configuration, the number sent from the (simulated) SIP Service Provider has no direct relationship to the corresponding extension in Communication Manager. Therefore, "all" digits are deleted, and the desired Communication Manager extension is inserted. In the sample configuration, if a PSTN user dials 732-852-1816, the number 21816 arrives via one of the SIP Trunks (as shown in **Figure 2**). The incoming call handling table maps 21816 to 52020, the local extension corresponding to the external PSTN number. During testing, the number to insert was varied, so that different types of telephones (e.g., IP, digital) and vector directory numbers (VDN) could be tested.



```
change inc-call-handling-trmt trunk-group 30                    Page   1 of  30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk   5   21816            all 52020
 public-ntwrk   5   22940            all 51003
```

The corresponding configuration for trunk group 31 is shown below.

```
change inc-call-handling-trmt trunk-group 31                    Page   1 of  30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    5  21816            all 52020
 public-ntwrk    5  22940            all 51003
```

The corresponding configuration for trunk group 60 is shown below.

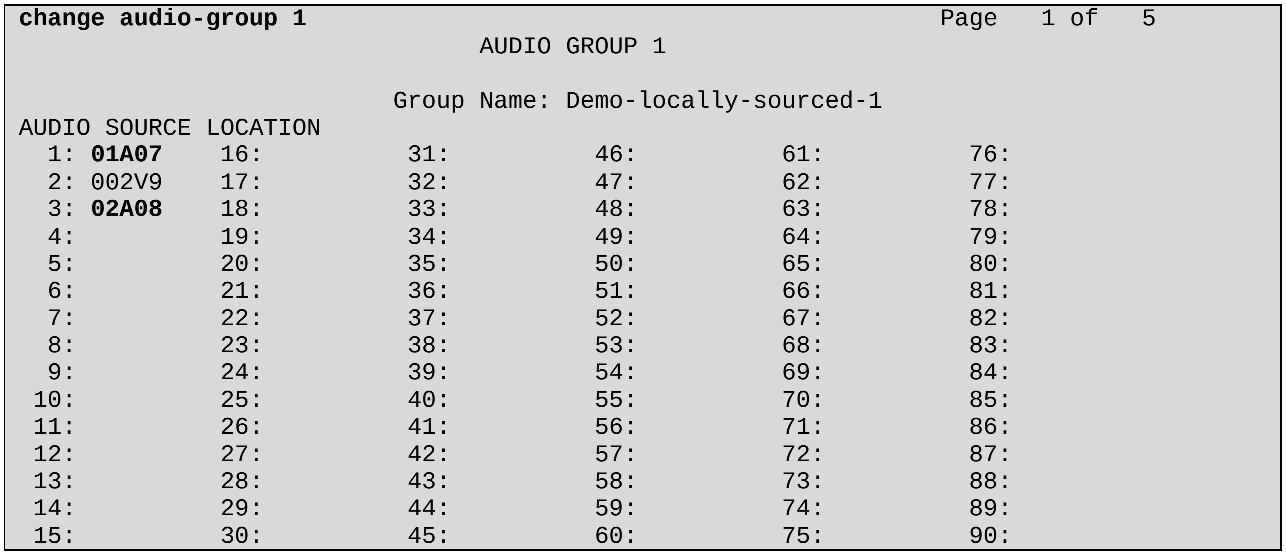
```
change inc-call-handling-trmt trunk-group 60                    Page   1 of  30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    5  21816            all 52020
 public-ntwrk    5  22940            all 51003
```

The corresponding configuration for trunk group 61 is shown below.

```
change inc-call-handling-trmt trunk-group 61                    Page   1 of  30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    5  21816            all 52020
 public-ntwrk    5  22940            all 51003
```

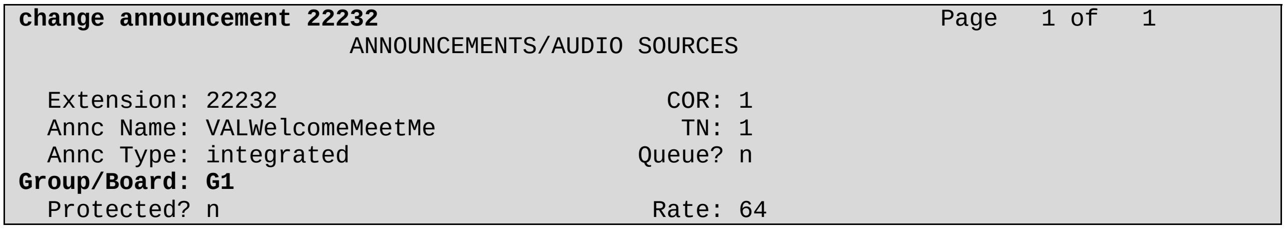
3.12. Summarizing Announcement-Related Configuration

Audio Group 1 contains announcement resources on the TN2501 card at the primary site as well as the TN2501 at the secondary site. The audio group concept allows Communication Manager to choose the most efficient announcement source for a call and also provides for redundancy. The following screen shows the configuration. Included in audio group 1 are the TN2501 card at the primary site (2A08), and the TN2501 card at the secondary site (1A07). (The other audio source at 2V9 is a gateway that is not relevant to the sample configuration).



```
change audio-group 1                                          Page   1 of   5
                                AUDIO GROUP 1

                          Group Name: Demo-locally-sourced-1
AUDIO SOURCE LOCATION
  1: 01A07    16:          31:          46:          61:          76:
  2: 002V9    17:          32:          47:          62:          77:
  3: 02A08    18:          33:          48:          63:          78:
  4:          19:          34:          49:          64:          79:
  5:          20:          35:          50:          65:          80:
  6:          21:          36:          51:          66:          81:
  7:          22:          37:          52:          67:          82:
  8:          23:          38:          53:          68:          83:
  9:          24:          39:          54:          69:          84:
 10:          25:          40:          55:          70:          85:
 11:          26:          41:          56:          71:          86:
 12:          27:          42:          57:          72:          87:
 13:          28:          43:          58:          73:          88:
 14:          29:          44:          59:          74:          89:
 15:          30:          45:          60:          75:          90:
```

The following screen shows an announcement being assigned to audio group 1. When this announcement is requested (e.g., by a vector), the announcement can be sourced by any member of the audio group containing the appropriate announcement file. All else equal, Communication Manager can select the most efficient member of the group (e.g., an announcement in the same gateway or region as the listener). If failures occur, the audio group provides redundancy benefits, allowing the same call logic to remain in place despite the failure.



```
change announcement 22232                                     Page   1 of   1
                       ANNOUNCEMENTS/AUDIO SOURCES

  Extension: 22232                        COR: 1
  Annc Name: VALWelcomeMeetMe              TN: 1
  Annc Type: integrated                Queue? n
Group/Board: G1
  Protected? n                           Rate: 64
```

The following portion of “list announcements” output shows other announcements that can be sourced by Audio Group 1.   Verification scenarios in Section 5 use these announcements.

```
list announcement
                           ANNOUNCEMENTS/AUDIO SOURCES
Announcement                                                  Source      Num of
Extension             Type       Name                        Pt/Bd/Grp    Files
22232                 integrated VALWelcomeMeetMe             G1          3
22233                 integrated VALDenyIncorrectCode         G1          3
22234                 integrated VALFirstPartyJoin            G1          3
22235                 integrated VALDenyConfFull              G1          3
22236                 integrated VALConfInProgJoin            G1          3
22555                 integrated Demo-locally-sourced-1       G1          3
```

3.13. Summarizing VDN and Vector-Related Configuration

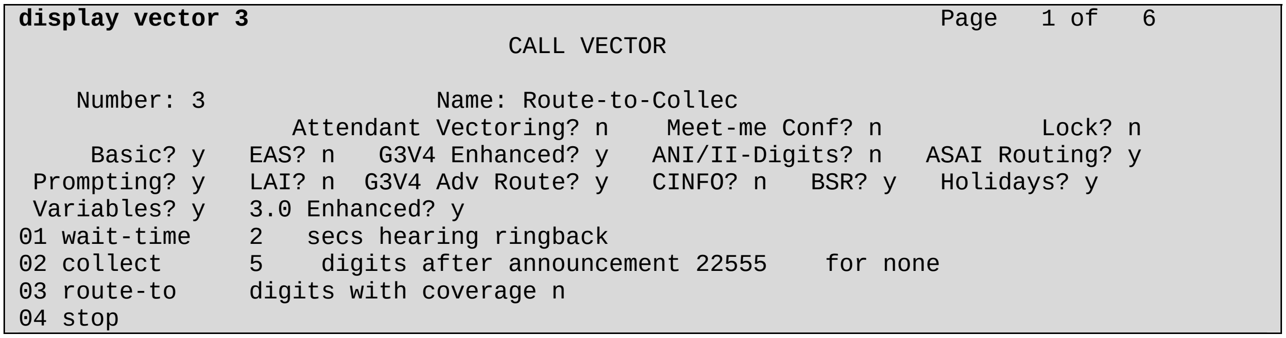
The following list command shows a mapping of vector directory numbers (VDN) to call vectors used in the verification of the configuration. For testing, the VDN was inserted via the incoming call handling table for the SIP trunk group, invoking the command logic in the corresponding vector.

```
list vdn
                          VECTOR DIRECTORY NUMBERS
                                                                        Evnt
                                      VDN         Vec           Orig    Noti
Name (22 characters)   Ext/Skills     Ovr COR TN  PRT Num  Meas Annc    Adj
Meet-me 51081          51081           n  1   1    V  1    none
Route-to-collected     51082           n  1   1    V  3    none
```

The following sample meet-me conference vector was used to verify proper collection of DTMF for the conference password, as well as proper announcement source selection for the various announcements requested by the vector. In the verifications, calls to VDN 51081 will be shown, arriving from both the primary and secondary sites.

```
display vector 1                                                Page   1 of   6
                                  CALL VECTOR

    Number: 1                Name: Meet-me 58081
                   Attendant Vectoring? n    Meet-me Conf? y           Lock? y
     Basic? y   EAS? n   G3V4 Enhanced? y   ANI/II-Digits? n   ASAI Routing? y
 Prompting? y   LAI? n  G3V4 Adv Route? y   CINFO? n   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    2   secs hearing ringback
02 collect      6    digits after announcement 22232
03 goto step    5             if digits           =      meet-me-access
04 disconnect   after announcement 22233
05 goto step    10            if meet-me-idle
06 goto step    13            if meet-me-full
07 announcement 22236
08 route-to     meetme
09 stop
10 announcement 22234
11 route-to     meetme
12 stop
```

The following simple vector was also used to allow calls to be directed to any five digit telephone extension in the configuration. The extension was collected from the caller after an announcement prompt.

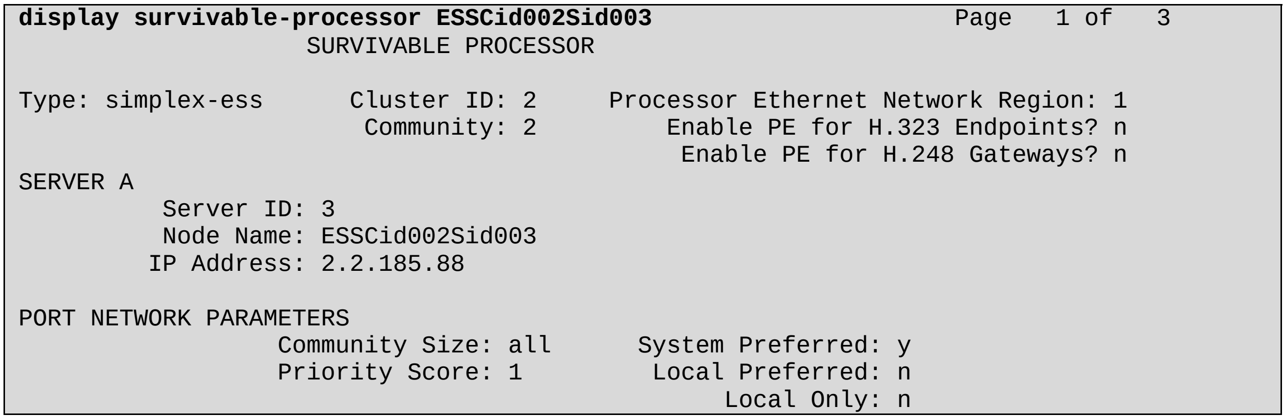


```
display vector 3                                                Page   1 of   6
                                  CALL VECTOR

    Number: 3                Name: Route-to-Collec
                   Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? n   G3V4 Enhanced? y   ANI/II-Digits? n   ASAI Routing? y
 Prompting? y   LAI? n  G3V4 Adv Route? y   CINFO? n   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    2   secs hearing ringback
02 collect      5    digits after announcement 22555    for none
03 route-to     digits with coverage n
04 stop
```

3.14. Summarizing ESS-Related Configuration

This section summarizes aspects of the Enterprise Survivable Server (ESS) configuration. Product documentation [ESS] should be consulted for more information on configuring ESS.

The S8500 Server at the secondary site corresponds with the survivable processor node name “ESSCid002Sid003”. The following screen shows the configuration. This ESS is cluster 2, server 3, with IP Address 2.2.185.88. It is capable of assuming control over the co-located Avaya G650 Media Gateway, should the secondary site be isolated from the primary site. It is also capable of assuming control over all sites, if both S8730 Servers fail or are rendered unreachable.



```
display survivable-processor ESSCid002Sid003                     Page   1 of   3
                    SURVIVABLE PROCESSOR

Type: simplex-ess      Cluster ID: 2     Processor Ethernet Network Region: 1
                        Community: 2         Enable PE for H.323 Endpoints? n
                                              Enable PE for H.248 Gateways? n
SERVER A
          Server ID: 3
          Node Name: ESSCid002Sid003
         IP Address: 2.2.185.88

PORT NETWORK PARAMETERS
                  Community Size: all      System Preferred: y
                  Priority Score: 1         Local Preferred: n
                                                 Local Only: n
```

Port networks can also be assigned a community, if desired. The following shows the relevant configuration screen.

```
display system-parameters port-networks                         Page   1 of   2

               COMMUNITY ASSIGNMENTS FOR PORT NETWORKS

 PN Community     PN Community     PN Community     PN Community    PN Community
 ------------     ------------     ------------     ------------    ------------
  1: 1            14: 1            27: 1            40: 1           53: 1
  2: 2            15: 1            28: 1            41: 1           54: 1
  3: 1            16: 1            29: 1            42: 1           55: 1
  4: 1            17: 1            30: 1            43: 1           56: 1
  5: 1            18: 1            31: 1            44: 1           57: 1
  6: 1            19: 1            32: 1            45: 1           58: 1
  7: 1            20: 1            33: 1            46: 1           59: 1
  8: 1            21: 1            34: 1            47: 1           60: 1
  9: 1            22: 1            35: 1            48: 1           61: 1
 10: 1            23: 1            36: 1            49: 1           62: 1
 11: 1            24: 1            37: 1            50: 1           63: 1
 12: 1            25: 1            38: 1            51: 1           64: 1
 13: 1            26: 1            39: 1            52: 1
```

On Page 2, other ESS-related parameters can be defined.

```
display system-parameters port-networks                         Page   2 of   2
                   PORT NETWORK RECOVERY RULES

 FAILOVER PARAMETERS                              FALLBACK PARAMETERS
 No Service Time Out Interval (min): 5                Auto Return: no

    PN Cold Reset Delay Timer (sec): 60
```

3.15. Saving Configuration Changes

The command “save translation all” can be used to save the configuration. In the sample configuration, translations were automatically saved and synchronized with each survivable processor, such as the ESS, on a nightly basis, as a result of the bold parameters in the screen shown below.

```
change system-parameters maintenance                           Page   1 of   3
                   MAINTENANCE-RELATED SYSTEM PARAMETERS

OPERATIONS SUPPORT PARAMETERS
     CPE Alarm Activation Level: minor
SCHEDULED MAINTENANCE
                                          Start Time: 22 : 00
                                           Stop Time: 06 : 00
                                    Save Translation: daily
 Update LSP and ESS Servers When Saving Translations: y
```

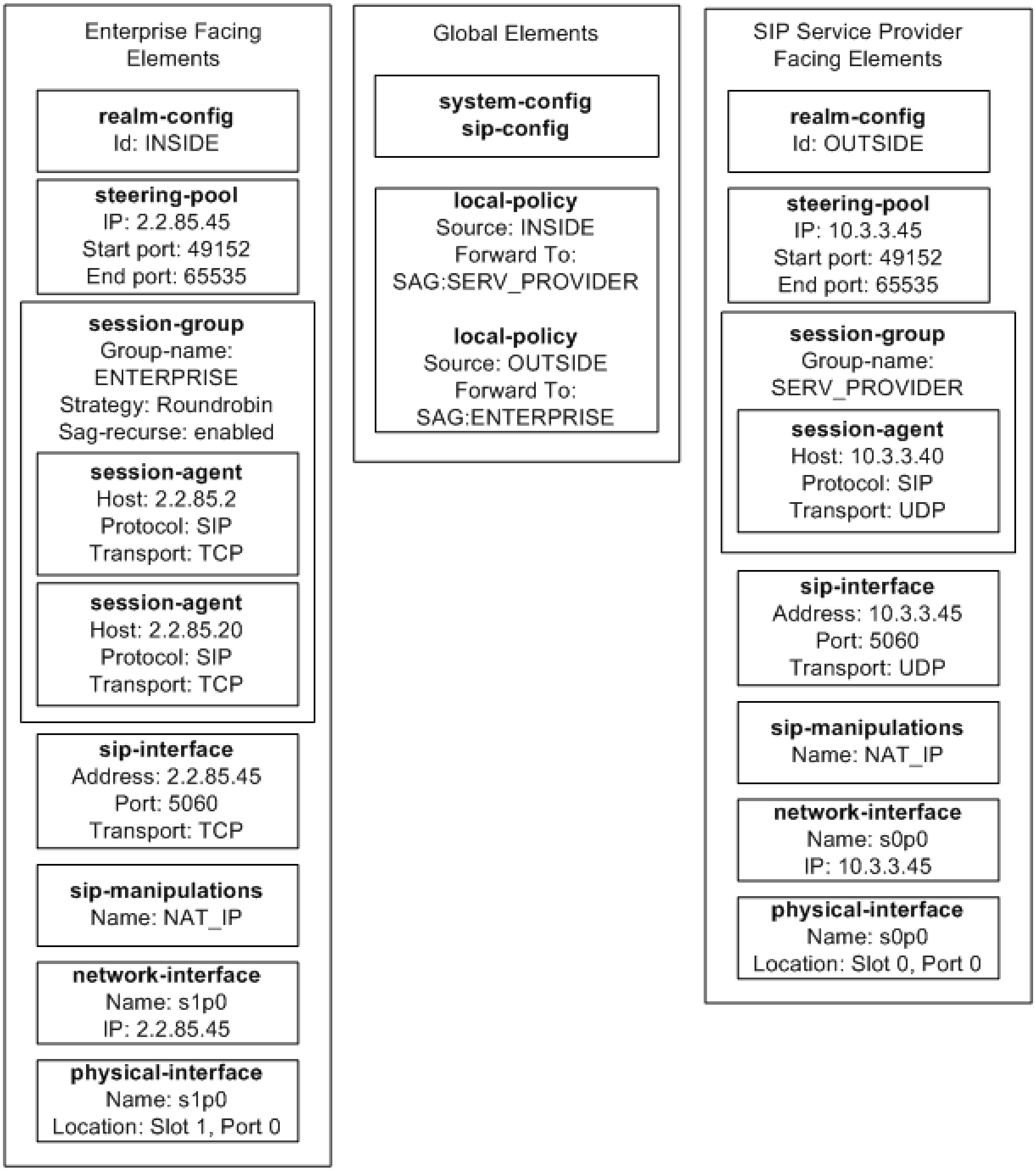
4. Configure Acme Packet Net-Net Session Directors

This section describes the configuration of the Session Directors for interoperability with Communication Manager. Although specifics such as IP addresses will vary, the configurations for the Acme Packet Net-Net 4500 at the primary and secondary sites are conceptually identical. Unless otherwise noted, the screens in this section will show the primary site configuration only, and the introductory text will note differences to be expected at the secondary site.

The Session Director can be configured via the Acme Packet Command Line Interface (ACLI). This section assumes the reader is familiar with accessing and configuring the Session Director.

The complete configuration file for the primary site is shown in **Appendix A**. The full configuration file includes standard configuration (e.g., redundancy-config, media-manager, etc.) that are not directly related to the interoperability test and not described in this section. This section will not attempt to describe each parameter but instead will highlight items relevant to the sample configuration. The remaining parameters are generally the default/standard value. For additional details on the administration of the Session Director, refer to [AP1].

Figure 3 illustrates a pictorial view of key aspects of the sample configuration for the Acme Packet Net-Net 4500 at the primary site. The configuration at the secondary site is conceptually identical, but of course the appropriate IP Addresses shown in **Figure 1** must be substituted.



Enterprise Facing Elements

realm-config
Id: INSIDE

steering-pool
IP: 2.2.85.45
Start port: 49152
End port: 65535

session-group
Group-name: ENTERPRISE
Strategy: Roundrobin
Sag-recurse: enabled

session-agent
Host: 2.2.85.2
Protocol: SIP
Transport: TCP

session-agent
Host: 2.2.85.20
Protocol: SIP
Transport: TCP

sip-interface
Address: 2.2.85.45
Port: 5060
Transport: TCP

sip-manipulations
Name: NAT_IP

network-interface
Name: s1p0
IP: 2.2.85.45

physical-interface
Name: s1p0
Location: Slot 1, Port 0

Global Elements

system-config
sip-config

local-policy
Source: INSIDE
Forward To: SAG:SERV_PROVIDER

local-policy
Source: OUTSIDE
Forward To: SAG:ENTERPRISE

SIP Service Provider Facing Elements

realm-config
Id: OUTSIDE

steering-pool
IP: 10.3.3.45
Start port: 49152
End port: 65535

session-group
Group-name: SERV_PROVIDER

session-agent
Host: 10.3.3.40
Protocol: SIP
Transport: UDP

sip-interface
Address: 10.3.3.45
Port: 5060
Transport: UDP

sip-manipulations
Name: NAT_IP

network-interface
Name: s0p0
IP: 10.3.3.45

physical-interface
Name: s0p0
Location: Slot 0, Port 0

Figure 3: Pictorial View of the Primary Site Session Director Configuration

4.1. Acme Packet Command Line Interface Summary

The Session Director is configured using the Acme Packet Command Line Interface (ACLI). The following are the generic ACLI steps for configuring various elements.

1. Access the console port of the Session Director using a PC and a terminal emulation program such as HyperTerminal. Use the following settings for the serial port on the PC.
   - Bits per second: 115200
   - Data bits: 8
   - Parity : None
   - Stop bits: 1
   - Flow control: None
2. Log in to the Session Director with the user password.
3. Enable the Superuser mode by entering the **enable** command and then the superuser password. The command prompt will change to include a "#" instead of a ">" while in Superuser mode. This level of system access (i.e., at the "acmesystem#" prompt) will be referred to as the ***main*** level of the ACLI. Specific sub-levels of the ACLI will then be accessed to configure specific ***elements*** and specific ***parameters*** of those elements.
4. In Superuser mode, enter the **configure terminal** command. The **configure terminal** command is used to access the system level where all operating and system elements may be configured. This level of system access will be referred to as the ***configuration*** level.
5. Enter the name of an element to be configured (e.g., **system**).
6. Enter the name of a sub-element, if any (e.g., **phy-interface).**
7. Enter the name of an element parameter followed by its value (e.g., **name s0p0**).
8. Enter **done** to save changes to the element. Use of the **done** command causes the system to save and display the settings for the current element.
9. Enter **exit** as many times as is necessary to return to the configuration level.
10. Repeat **Steps 4 - 8** to configure all the elements.
11. Enter **exit** to return to the main level.
12. Type **save-config** to save the entire configuration.
13. Type **activate-config** to activate the entire configuration.

After accessing different levels of the ALCI to configure elements and parameters, it is necessary to return to the main level to run certain tasks such as saving the configuration, activating the configuration, or rebooting the system.

4.2. System Configuration

The system configuration defines system-wide parameters for the Session Director. Key system configuration (***system-config***) fields include:

- **default-gateway**: The IP address of the default gateway for the *management network*. In the sample configuration, the default gateway for the management network at both sites is 2.2.4.1.
- **source-routing**: ***enabled*** By default, the Session Director's FTP, ICMP, telnet, and SNMP services cannot be accessed via the media interfaces. These services can be

administratively enabled, if desired, as described in reference [AP1] in the context of HIP or host-in-path functions. Although not strictly required, source-routing was enabled in the sample configuration to allow source routing of HIP packets based on source IP addresses (i.e., the Session Director will send replies out the same interface from which it received the request).

```
system-config
        hostname                       acmesbc
       < text removed for brevity >

        call-trace                    disabled
        internal-trace                disabled
        log-filter                    all
        default-gateway               2.2.4.1
        restart                       enabled
        exceptions
        telnet-timeout                0
        console-timeout               0
        remote-control                enabled
        cli-audit-trail               enabled
        link-redundancy-state         disabled
        source-routing                enabled
```

4.3. Physical and Network Interfaces

In the sample configuration, for each Session Director, the Ethernet interface slot 0 / port 0 was connected to the external untrusted network, and 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. Key physical interface (***phy-interface***) fields include:

- **name**: A descriptive string used to reference the Ethernet interface.
- **operation-type**: ***Media*** indicates both signaling and media packets are sent on this interface.
- **slot / port**: The identifier of the specific Ethernet interface used.

```
phy-interface
        name                          s0p0
        operation-type                Media
        port                          0
        slot                          0
        virtual-mac                   00:08:25:a0:e2:28
        admin-state                   enabled
        auto-negotiation              enabled
        duplex-mode                   FULL
        speed                         100
phy-interface
        name                          s1p0
        operation-type                Media
        port                          0
        slot                          1
        virtual-mac                   00:08:25:a0:e2:29
        admin-state                   enabled
        auto-negotiation              enabled
        duplex-mode                   FULL
        speed                         100
```

Key network interface (***network-interface***) fields include:

- **name**: The name of the physical interface (defined previously) that is associated with this network interface.
- **ip-address**: A virtual IP address assigned to a high availability pair of Session Directors. As mentioned in Section 1, although each site in the sample configuration had a single Acme Packet Net-Net 4500, the configuration was done as if each site had a pair. Verification of the Acme Packet Net-Net 4500 High Availability Configuration with Communication Manager is documented in reference [AC-HA].
- **pri-utility-addr**: The physical address of the primary Session Director in the high availability pair.
- **sec-utility-addr**: The physical address of the secondary Session Director in the high availability pair.
- **netmask**: Subnet mask for the IP subnet.
- **gateway**: The subnet gateway address.
- **icmp-address**: The list of IP addresses from which the Session Director will answer ICMP requests on this interface. This has been left blank for each network interface, since there is no need to respond to ICMP requests in the sample configuration on these interfaces. Recall that the SIP Signaling Groups on Communication Manager have been configured for “Enable Layer 3 Test” = “y”, which means that SIP OPTIONS messages rather than ICMP “pings” will be used to test connectivity.

The settings for the public side network interface of the primary site Session Director are shown below. (The settings for the secondary site Session Director used 10.3.3.145, 10.3.3.146, and 10.3.3.147.)

```
network-interface
        name                          s0p0
        sub-port-id                   0
        description
        hostname
        ip-address                    10.3.3.45
        pri-utility-addr              10.3.3.46
        sec-utility-addr              10.3.3.47
        netmask                       255.255.255.0
        gateway                       10.3.3.1

       < text removed for brevity >
         icmp-address
        last-modified-by              admin@console
        last-modified-date            2009-04-13 15:10:34
```

The settings for the private side network interface of the primary site Session Director are shown below. (The settings for the secondary site Session Director used 2.2.185.145, 2.2.185.146, and 2.2.185.147.)

```
network-interface
        name                           s1p0
        sub-port-id                    0
        description
        hostname
        ip-address                     2.2.85.45
        pri-utility-addr               2.2.85.46
        sec-utility-addr               2.2.85.47
        netmask                        255.255.255.0
        gateway                        2.2.85.1

       < text removed for brevity >
         icmp-address
        last-modified-by               admin@console
        last-modified-date             2009-04-13 15:11:38
```

4.4. Realm

A realm represents a group of related Session Director components. Defining realms allows flows to pass through a connection point between two networks. Two realms were defined for the compliance test. The ***OUTSIDE*** realm was defined for the external network and the ***INSIDE*** realm was defined for the internal network.

Key realm (***realm-config***) parameters include:

- **identifier**: A string used as a realm reference. This will be used in the configuration of other components.
- **network interfaces**: The network interfaces located in this realm.
- **mm-in-realm:** Although not required in a peering configuration, this parameter was enabled in the sample configuration. This parameter allows calls within the same realm to have media flow through the Acme Packet Net-Net 4500. See [AP1] for more details.
- **out-manipulationid**: ***NAT_IP*** This name refers to a set of sip-manipulations (defined in Section 4.9) that are performed on outbound traffic from the SBC. The "NAT_IP" set of sip-manipulations will be specified in each realm, and will be applied bi-directionally.

The realm-config settings for the primary site Session Director are shown below. (The settings for the secondary site Session Director are identical.)

```
realm-config
        identifier                     OUTSIDE
        description
        addr-prefix                    0.0.0.0
        network-interfaces
                                       s0p0:0
        mm-in-realm                    enabled
        mm-in-network                  enabled
        mm-same-ip                     enabled
        mm-in-system                   enabled
               < text removed for brevity >
         out-translationid
        in-manipulationid
        out-manipulationid             NAT_IP
        class-profile
        average-rate-limit             0

realm-config
        identifier                     INSIDE
        description
        addr-prefix                    0.0.0.0
        network-interfaces
                                       s1p0:0
        mm-in-realm                    enabled
        mm-in-network                  enabled
        mm-same-ip                     enabled
        mm-in-system                   enabled
       < text removed for brevity >
        out-translationid
        in-manipulationid
        out-manipulationid             NAT_IP
```

4.5. SIP Configuration

The SIP configuration (***sip-config***) defines global system-wide SIP parameters. Key SIP configuration (***sip-config***) parameters include:

- **home-realm-id**: The name of the realm on the private side of the Session Director.
- **nat-mode**: None. No SIP-NAT function is necessary
- **options max-udp-length=0** Enables UDP fragmented packets
- **options set-inv-exp-at-100-resp** Sets SIP Timer C when a 100 Trying is received in response to INVITE. See reference [AP1] for more details.

The sip-config settings for the primary site Session Director are shown below. (The settings for the secondary site Session Director are identical.)

```
sip-config
        state                          enabled
        operation-mode                 dialog
        dialog-transparency            enabled
        home-realm-id                  INSIDE
        egress-realm-id                INSIDE
        nat-mode                       None
      < text removed for brevity >
         options                      max-udp-length=0
                                      set-inv-exp-at-100-resp
```

4.6. SIP Interface

The SIP interface (***sip-interface***) defines the receiving characteristics of the SIP interfaces on the Session Director. Two SIP interfaces were defined, one for each realm. Key SIP interface (***sip-interface***) fields include:

- **realm-id**: The name of the realm assigned to this interface.
- **sip port**
  - **address**: The IP address assigned to this sip-interface.
  - **port**: The port assigned to this sip-interface. Port 5060 is used for UDP and TCP.
  - **transport-protocol**: UDP transport is used on the "outside" for simulating communication with a SIP Service Provider, and TCP transport is used on the "inside" to Communication Manager.
  - **allow-anonymous:** Defines from whom SIP requests will be allowed. The value of ***agents-only*** is used. Thus, SIP requests will only be accepted from configured session agents (as defined in Section 4.7).
- **trans-expire:** Sets the expiration timer in seconds for SIP transactions. As per reference [AP1], this parameter sets Timer B, Timer F, and Timer H defined by RFC 3261. In the sample configuration, trans-expire was changed from the default of 32 seconds in the global "sip-config" to 6 seconds in the "sip-interface". As an example implication, assume an incoming call arrives from the PSTN that the Acme Packet Session Director sends on to an Avaya C-LAN that appears to be an in-service session agent. However, there is no response. After 6 seconds (rather than 32), the transaction times out, and as a result of session agent group recursion specified in Section 4.8, an INVITE is sent to the other C-LAN in the session agent group. The six seconds was chosen for symmetry with the "Alternate Route Timer" default on the Avaya signaling group.
- **invite-expire:** Sets the expiration timer in seconds for SIP transactions after receiving a provisional response. In the sample configuration, this is set to 180 seconds, which is set artificially high to distinguish its behavior from the **trans-expire** parameter. For example, this allows ample time after receiving a 100 Trying for the network to route a call.
- **charging-vector-mode delete:** In the sample configuration, the Acme Packet Net-Net Session Director is configured to simply delete the P-Charging-vector header that is received by Communication Manager 5.2 for outbound calls from the enterprise. Communication Manager creates an "icid" value in the P-Charging-vector that contains a private network IP address (however, see Section 6). Since the sample configuration does not make use of the P-Charging-vector, the header is deleted so that private network addresses are not visible to the public SIP Service Provider network. Other P-Charging-vector treatment options (i.e., besides delete) are described in reference [AP1].

The sip-interface settings for the primary site Session Director are shown below. (The settings for the secondary site Session Director are identical, save for the IP Address differences shown in **Figure 3** and **Figure 1**)

```
sip-interface
        state                         enabled
        realm-id                      OUTSIDE
        description
        sip-port
                address                       10.3.3.45
                port                          5060
                transport-protocol            UDP
                tls-profile
                allow-anonymous               agents-only
       < text removed for brevity >

sip-interface
        state                         enabled
        realm-id                      INSIDE
        description
        sip-port
                address                       2.2.85.45
                port                          5060
                transport-protocol            TCP
                tls-profile
                allow-anonymous               agents-only
       < text removed for brevity >
       trans-expire                  6
       invite-expire                 180

       charging-vector-mode         delete
```

4.7. Session Agent

A session agent defines the characteristics of a signaling peer to the Session Director. Each Communication Manager C-LAN interface is defined as a session agent. Key session agent (***session-agent***) parameters include:

- **hostname**: Fully qualified domain name or IP address of this SIP peer.
- **ip-address:** The IP address of this SIP peer.
- **port**: The port used by the peer for SIP traffic.
- **app-protocol**: ***SIP***
- **transport-method**: ***StaticTCP.*** With static TCP, a TCP connection can be re-used for multiple sessions. With the alternative "DynamicTCP", a new connection must be established for each session. DynamicTCP also works with Communication Manager, but since DynamicTCP had already been documented in the compliance testing performed in reference [AC-HA], static TCP was used in this sample configuration to show that it is a viable option for interoperability with Communication Manager.
- **realm-id**: The realm id where this peer resides.
- **description**: A descriptive name for the peer.
- **max-sessions:** Although not used in the sample configuration, this parameter can allow call admission control to be applied for the session agent. For example, in reference [JSR], the max-sessions parameter is configured to match the number of members in the corresponding Avaya SIP trunk group. If this is not configured, and the Session Director sends an INVITE to an Avaya signaling group whose corresponding trunk group has no

available members, Communication Manager will respond with a SIP 503. The Session Director will redirect the call to another session agent in the SAG.

- **ping-method**: ***OPTIONS;hops=0*** The SIP OPTIONS message will be sent to the peer to verify that the SIP connection is functional. In addition, this parameter causes the Session Director to set the Max-Forward field to 0 in outbound OPTIONS pings generated by the Session Director to this session-agent.
- **ping-interval**: Specifies the interval between SIP OPTIONS "pings" in seconds. Since the intent is to monitor the health of the connection, "pings" may be suppressed if there is traffic to/from the session-agent that shows the connection is up.
- **ping-in-service-response-codes** Although not defined in the sample configuration, this parameter can be used to specify the list of response codes that keep a session agent in-service. By default, any response from the session agent is enough to keep the session agent in service. If it is desired that only a 200 OK response is a valid response to OPTIONS, then 200 can be entered. Note that Communication Manager will respond to OPTIONS with a 503 in various conditions where the SIP trunk group corresponding to the SIP signaling group has no available members to handle a call. This condition can occur when the SIP trunk group is administratively busied out, as well as any case where the trunk group is in-service, but there are no available members to handle a call (i.e., all trunk members in use for calls).
- **out-service-response-codes** Although not defined in the sample configuration, this parameter can be used to specify the list of "OPTIONS ping" response codes that take a session agent out-of-service.
- **options trans-timeouts=1** This parameter defines the number of consecutive non-ping transaction timeouts that will cause the session agent to be marked out-of-service. For example, with this option set to 1, if an INVITE is sent to an Avaya C-LAN that is currently marked in-service, but no response is received resulting in a transaction timeout, the session agent will be immediately marked out-of-service. In the sample configuration, where session agent groups are used, this allows future calls to flow to in-service session agents in the group without experiencing a delay due to a transaction timeout. Note that an explicit error response, such as a 503, is not considered a transaction timeout.
- **reuse-connections TCP** Enables TCP connection re-use.
- **tcp-keepalive enabled** Enables standard TCP Keep-Alives
- **tcp-reconn-interval 10** Specifies the idle time, in seconds, before TCP keep-alive messages are sent.

In the sample configuration shown in **Figure 1**, the settings for the four session agents representing the C-LAN interfaces labeled 3, 3A, 6, and 6A are the same, except of course for the appropriate hostname, ip-address, and description. The key settings for the session agent for the C-LAN labeled 3 in **Figure 1** are shown below.

```
session-agent
        hostname                       2.2.85.2
        ip-address                     2.2.85.2
        port                           5060
        state                          enabled
        app-protocol                   SIP
        app-type
        transport-method               StaticTCP
        realm-id                       INSIDE
        egress-realm-id
        description                    Primary Site C-LAN 2A02
        carriers
        allow-next-hop-lp              enabled
        constraints                    disabled
        max-sessions                   0
        < text removed for brevity >
        ping-method                    OPTIONS;hops=0
        ping-interval                  16
        ping-send-mode                 keep-alive
        ping-in-service-response-codes
        out-service-response-codes
        options                        trans-timeouts=1

        reuse-connections              TCP
        tcp-keepalive                  enabled
        tcp-reconn-interval            10
        < text removed for brevity >
```

The key settings for the session agent to the (simulated) SIP Service Provider at the primary site are shown below. For the secondary site Acme Packet Net-Net 4500, the session agent configuration to the (simulated) SIP Service Provider is similar, except of course the hostname and ip-address are different (10.3.3.1).

```
session-agent
        hostname                       10.3.3.40
        ip-address                     10.3.3.40
        port                           5060
        state                          enabled
        app-protocol                   SIP
        app-type
        transport-method               UDP
        realm-id                       OUTSIDE
        egress-realm-id
        description                    Service Provider Proxy
        carriers
        allow-next-hop-lp              enabled
        constraints                    disabled
        max-sessions                   0
        < text removed for brevity >

        ping-method                    OPTIONS;hops=0
        ping-interval                  16
        ping-send-mode                 keep-alive
        < text removed for brevity >
```

4.8. Session Agent Groups (SAG)

A session agent group is a logical collection of two or more session agents that behave as a single aggregate entity. In the sample configuration, the two C-LANs at each site are configured in a session agent group within the Acme Packet Net-Net 4500 at that site. Although not required, a session agent group is also created for connectivity to the (simulated) SIP PSTN, for easy adaptation to outside networks with multiple options for next hops.

Key session group (***session-group***) parameters include:

- **group-name**: a unique name for the session agent group.
- **app-protocol**: ***SIP***
- **strategy**: selects the algorithm to use for distribution of traffic among the session agents in the group. In the sample configuration, a simple **roundrobin** distribution is selected for alternating traffic among the C-LANs. More sophisticated alternatives are available including "leastbusy" and "propdist" (Proportional Distribution) based on configurable session constraints, and are described in reference [AP1].
- **dest**: Identifies the session agents that are members of the session agent group. For the session agent group "Enterprise", the appropriate C-LAN IP Addresses are entered.
- **sag-recursion** If enabled, allows re-trying another session agent in the session agent group after a failure for the previously selected session agent. For example, if an INVITE message is sent to a C-LAN and the C-LAN does not respond, SAG recursion allows an INVITE to be automatically directed to another C-LAN in the SAG. Those familiar with Communication Manager terminology may benefit from the following parallel. Conceptually, SAG recursion is similar to Avaya Look-Ahead Routing, where the SAG is the route-pattern, the session agents are the trunk groups in the route-pattern and SAG recursion allows "LAR" to the next trunk in the pattern upon a failure. Note that this analogy is imperfect in that the Acme Packet Net-Net Session Director can make decisions about which session-agent in the SAG to choose based on algorithms that would check usage and load before selecting the next session agent. In the sample configuration, SAG recursion is enabled for the session agent group containing the C-LAN interfaces to Communication Manager. Since there is really only one session agent on the outside for each Acme Packet Net-Net 4500 in the sample configuration, sag-recursion is moot and is shown in the default disabled state.

In the sample configuration shown in **Figure 1**, the C-LAN interfaces labeled 3 and 3A are defined in a SAG on the Acme Packet Net-Net 4500 at the primary site, and the C-LAN interfaces labeled 6 and 6A are defined in a SAG on the Acme Packet Net-Net 4500 at the secondary site. Although not configured, there is nothing that would preclude including C-LAN session agents from one site in the session agent group of the Acme Packet Net-Net 4500 at the other site.

The following shows the configuration of session agent groups on the Acme Packet Net-Net 4500 at the primary site. For the Acme Packet Net-Net 4500 at the secondary site, the configuration is similar, except that the destinations for the "ENTERPRISE" SAG are the C-LANs at the secondary site (2.2.185.2, 2.2.185.20), and the destination for the

“SERV_PROVIDER” SAG is the IP Address of the public network agent available to the secondary site (10.3.3.1).

```
session-group
        group-name                    ENTERPRISE
        description
        state                         enabled
        app-protocol                  SIP
        strategy                      RoundRobin
        dest
                                      2.2.85.2
                                      2.2.85.20
        trunk-group
        sag-recursion                 enabled
        stop-sag-recurse              401,407

session-group
        group-name                    SERV_PROVIDER
        description
        state                         enabled
        app-protocol                  SIP
        strategy                      Hunt
        dest
                                      10.3.3.40
        trunk-group
        sag-recursion                 disabled
        stop-sag-recurse              401,407
```

4.9. SIP Manipulation

SIP manipulations are rules used to modify the SIP messages. For example, SIP manipulations can be performed to ensure private network topology hiding and confidentiality. In Section 4.4, it was defined that the set of sip-manipulations named NAT_IP would be performed in each realm. Key SIP manipulation (***sip-manipulation***) parameters include:

- **name**: The name of this set of SIP header rules.
- **header-rule**:
  - **name**: The name of this individual header rule.
  - **header-name**: The SIP header to be modified.
  - **action**: The action to be performed on the header.
  - **comparison-type**: The type of comparison performed when determining a match.
  - **msg-type**: The type of message to which this rule applies.
  - **element-rule**:
    - **name:** The name of this individual element rule.
    - **type:** Defines the particular element in the header to be modified.
    - **action:** The action to be performed on the element.
    - **match-val-type**: Element matching criteria on the data type (if any) in order to perform the defined action.
    - **comparison-type**: The type of comparison performed when determining a match.
    - **match-value**: Element matching criteria on the data value (if any) in order to perform the defined action.
    - **new-value**: New value for the element (if any).

In the configuration file in **Appendix A**, six modifications (or **header-rules**) were defined. ***manipFrom***, ***manipTo***, ***manipRpid***, ***manipHistInfo, storeAlertInfo, and manipAlertInfo***. These header manipulations were added to hide the private IP address of the Session Director which can appear in the “To”, “History-Info” and “Alert-Info” SIP headers. This IP address appears in these fields because this IP address is configured as the **Far-end Domain** field on the Communication Manager signaling group form. For each of these fields, the intent of the header rule is to change the private IP address in this field to the actual destination IP address as the message is forwarded on. It is less important to hide the addresses coming from the public side. However, these same rules were applied uniformly to both sides, and the sip-manipulations were configured on each realm.

The example below shows the ***manipTo*** header-rule. It specifies that the “To” header in SIP request messages will be manipulated based on the element rule defined. The element rule specifies if the host part of the URI in this header is an IP address, than replace it with the value of $REMOTE_IP. The value of $REMOTE_IP is the IP address of the SIP peer.

```
sip-manipulation
        name                           NAT_IP
        description                    Topology hiding for SIP headers
        < text removed for brevity >
        header-rule
                name                           manipTo
                header-name                    To
                action                         manipulate
                comparison-type                case-sensitive
                match-value
                msg-type                       request
                new-value
                methods
                element-rule
                        name                           natToIp
                        parameter-name
                        type                           uri-host
                        action                         replace
                        match-val-type                 ip
                        comparison-type                case-sensitive
                        match-value
                        new-value                      $REMOTE_IP

        < text removed for brevity >
```

The ***manipHistInfo*** rule performs a similar operation for the “History-Info” SIP header. Due to the more complicated format of the “Alert-Info” SIP header, two rules ***storeAlertInfo***, and ***manipAlertInfo*** were defined to perform a translation for this SIP header. For the complete configuration of these rules, refer to **Appendix A**.

4.10. Steering Pools

Steering pools define sets of ports that are used for steering media flows (e.g., RTP) through the Acme Packet Net-Net 4500. The selected ports are used to modify the SDP to cause receiving session agents to direct media to the Acme Packet Net-Net 4500. Two steering pools were defined, one for each realm. Consult reference [AP1] for more information, including a means to use steering pool configuration for call admission control.

Key steering pool (***steering-pool***) parameters include:

- **ip-address:** The address of the interface on the 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.

The following shows the steering-pool configuration on the Acme Packet Net-Net 4500 at the primary site. For the Acme Packet Net-Net 4500 at the secondary site, the configuration is similar, except that the IP Addresses are different. **Figure 3** and **Figure 1** show the IP Addresses used at the secondary site.

```
steering-pool
        ip-address                     10.3.3.45
        start-port                     49152
        end-port                       65535
        realm-id                       OUTSIDE
        network-interface
        last-modified-by               admin@console
        last-modified-date             2009-04-13 15:11:26
steering-pool
        ip-address                     2.2.85.45
        start-port                     49152
        end-port                       65535
        realm-id                       INSIDE
        network-interface
        last-modified-by               admin@console
        last-modified-date             2009-04-13 15:12:25
```

4.11. Local Policy

Local policy controls the routing of SIP calls from one realm to another. Key local policy (***local-policy***) parameters include:

- **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.
- **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 first policy provides a simple routing rule indicating that messages originating from the ***OUTSIDE*** realm are to be sent to the ***INSIDE*** realm via the session agent group (SAG) named "ENTERPRISE". These local-policy settings are the same for the Acme Packet Net-Net 4500 at each site. The destination session agents defined within the SAG are site-specific.

```
local-policy
        from-address
                                       *
        to-address
                                       *
        source-realm
                                       OUTSIDE
        description
        activate-time                  N/A
        deactivate-time                N/A
        state                          enabled
        policy-priority                none
        last-modified-by               admin@console
        last-modified-date             2009-04-13 15:14:47
        policy-attribute
                next-hop                       SAG:ENTERPRISE
                realm                          INSIDE
                action                         none
                terminate-recursion            disabled
                carrier
                start-time                     0000
                end-time                       2400
                days-of-week                   U-S
                cost                           0
                app-protocol                   SIP
                state                          enabled
                methods
                media-profiles
```

The second policy indicates that messages originating from the ***INSIDE*** realm are to be sent to the ***OUTSIDE*** realm via session agent group “SERV_PROVIDER”.

```
local-policy
        from-address
                                       *
        to-address
                                       *
        source-realm
                                       INSIDE
        description
        activate-time                  N/A
        deactivate-time                N/A
        state                          enabled
        policy-priority                none
        last-modified-by               admin@console
        last-modified-date             2009-04-13 15:14:29
        policy-attribute
                next-hop                       SAG:SERV_PROVIDER
                realm                          OUTSIDE
                action                         none
                terminate-recursion            disabled
                carrier
                start-time                     0000
                end-time                       2400
                days-of-week                   U-S
                cost                           0
                app-protocol                   SIP
                state                          enabled
                methods
                media-profiles
```

5. Verifications

This section illustrates sample results obtained with the tested configuration. While it is not practical to illustrate all possible call scenarios, a representative sampling of calls is included as a reference. Section 6 documents test observations that resulted in product modification requests.

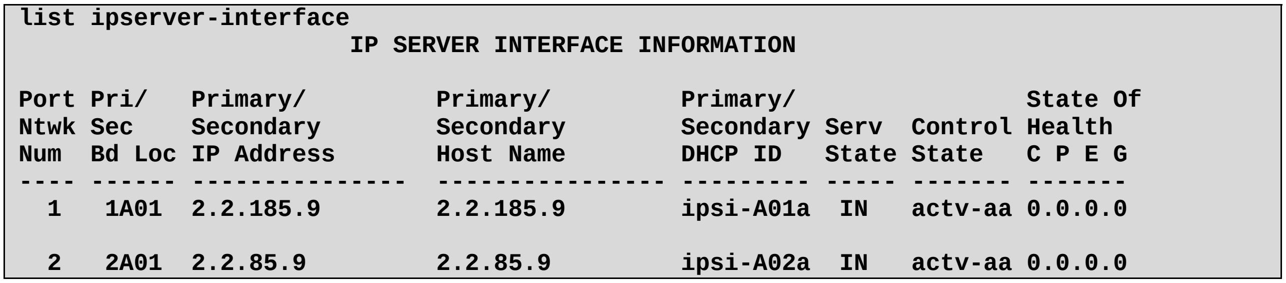
5.1. Normal Operation

This section shows various types of calls when all components are functioning normally. All calls are processed by the active S8730 Server at the primary site. Inbound and outbound calls can use the SIP Trunks at either site, subject to routing rules and efficient allocation of resources.

The following screen, taken from the active S8730 Server during normal operation, shows that cluster 1, the S8730 Server pair, controls both the primary and secondary site. The “Connected Clus(ter) IDs” shows that cluster 2, the S8500 ESS, can be reached by the IPSIs.

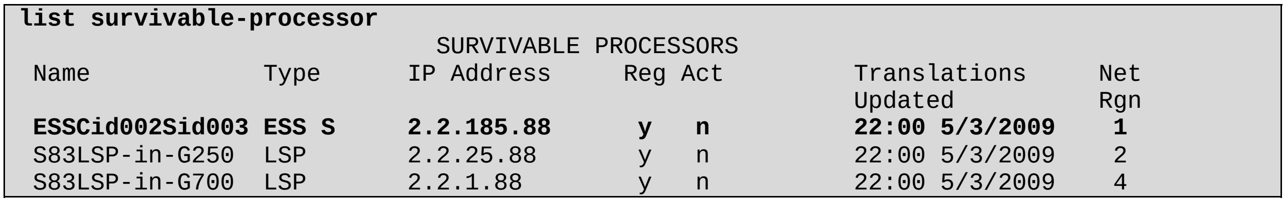
```
status ess port-networks
Cluster ID 1             ESS PORT NETWORK INFORMATION

                  Port IPSI   Pri/ Pri/    Cntl Connected
   Com  Intf Intf Ntwk Gtway  Sec  Sec     Clus Clus(ter)
PN Num  Loc  Type Ste  Loc    Loc  State     ID IDs
 1   1  1A01 IPSI up    1A01  1A01 actv-aa    1   1   2
 2   2  2A01 IPSI up    2A01  2A01 actv-aa    1   1   2
```

The following screen, taken from the active S8730 Server during normal operation, shows that the primary and secondary site IPSIs are controlled by the S8730 Server and “in-service”.



```
list ipserver-interface
                       IP SERVER INTERFACE INFORMATION

Port Pri/   Primary/         Primary/         Primary/                 State Of
Ntwk Sec    Secondary        Secondary        Secondary Serv  Control Health
Num  Bd Loc IP Address       Host Name        DHCP ID   State State   C P E G
---- ------ ---------------  ---------------- --------- ----- ------- -------
  1   1A01  2.2.185.9        2.2.185.9        ipsi-A01a  IN   actv-aa 0.0.0.0

  2   2A01  2.2.85.9         2.2.85.9         ipsi-A02a  IN   actv-aa 0.0.0.0
```

The following screen, taken during normal operation, shows that the ESS with IP Address 2.2.185.88 is registered with up-to-date translations.



```
list survivable-processor
                             SURVIVABLE PROCESSORS
 Name             Type      IP Address     Reg Act         Translations     Net
                                                           Updated          Rgn
 ESSCid002Sid003  ESS S     2.2.185.88      y   n          22:00 5/3/2009    1
 S83LSP-in-G250   LSP       2.2.25.88       y   n          22:00 5/3/2009    2
 S83LSP-in-G700   LSP       2.2.1.88        y   n          22:00 5/3/2009    4
```

5.1.1. Incoming Calls from PSTN Arriving via SIP Trunk to Primary Site

The following trace output shows a call incoming on signaling group 31 / trunk group 31 from PSTN telephone 732-852-2550. The incoming call handling table for trunk group 31 mapped the received number (21816) to extension 52020. Extension 52020 is an IP Telephone with IP Address 2.2.1.109 in Region 3. Initially, the IP Media Processor in region 3 (2.2.26.4) is used, but as can be seen in the final trace output, once the call is answered, the final RTP media path is “ip-direct” from the IP Telephone (2.2.1.109) to the “inside” of the Acme Packet Net-Net 4500 at the primary site (2.2.85.45).

```
list trace tac 131                                                     Page   1
                                LIST TRACE
time            data
14:16:11     Calling party trunk-group 31 member 1  cid 0x77
14:16:11     Calling Number & Name 7328522550 NO-CPName
14:16:11     active trunk-group 31 member 1  cid 0x77
14:16:11     dial 52020
14:16:11     ring station    52020 cid 0x77
14:16:11     G711MU ss:off ps:20
             rgn:3 [2.2.1.109]:15144
             rgn:3 [2.2.26.4]:3392
14:16:11     G711MU ss:off ps:20
             rgn:3 [2.2.85.45]:49206
             rgn:3 [2.2.26.4]:3384
14:16:15     active station    52020 cid 0x77
14:16:15     G711MU ss:off ps:20
             rgn:3 [2.2.85.45]:49206
             rgn:3 [2.2.1.109]:15144
14:16:15     G711MU ss:off ps:20
             rgn:3 [2.2.1.109]:15144
             rgn:3 [2.2.85.45]:49206
```

With this call up, the “show sipd agent” command was run on the primary Acme Packet Net-Net 4500, with the following output. Note that session agent 2.2.85.20 (C-LAN for signaling group 31) shows an Active Outbound session, and session agent 10.3.3.40 (the SIP Service Provider) shows an Active Inbound session.

```
acmesbc-pri# show sipd agent
                   ----- Inbound -----  ---- Outbound ----- -- Latency --   Max
Session Agent      Active  Rate  ConEx  Active  Rate  ConEx    Avg    Max Burst
10.3.3.40         I     1   0.0      0       0   0.0      0  0.000  0.000     1
2.2.85.2          I     0   0.0      0       0   0.0      0  0.000  0.000     1
2.2.85.20         I     0   0.0      0       1   0.0      0  0.118  0.118     1
```

The following output shows a “status trunk” command output illustrating status for a similar inbound call, this time using signaling group 30 and trunk group 30. Recall that the Session Director is configured for round-robin call distribution to these two session agents. For signaling purposes, the C-LAN at 2.2.85.2 is communicating with the Session Director at 2.2.85.45. The media path is directly from the IP Telephone (2.2.1.109) to the Session Director. For any of these traces, it can be observed that the far-end port for RTP (in this case 49204) is within the range specified by the Acme Packet “steering-pool”.

```
status trunk 30/1                                             Page   2 of   3
                                CALL CONTROL SIGNALING
Near-end Signaling Loc: 02A0217
  Signaling   IP Address                              Port
   Near-end:  2.2.85.2                              : 5060
    Far-end:  2.2.85.45                             : 5060
 H.245 Near:
  H.245 Far:
   H.245 Signaling Loc:           H.245 Tunneled in Q.931? no

 Audio Connection Type: ip-direct     Authentication Type: None
    Near-end Audio Loc:                        Codec Type: G.711MU
   Audio      IP Address                              Port
   Near-end:  2.2.1.109                             : 15144
    Far-end:  2.2.85.45                             : 49204
```

In the next example, a call arrives via SIP Trunk 30 at the primary site, but is directed to a station user (x51003) at the secondary site. The final connection is inter-region “ip-direct” between the IP Telephone (2.2.185.200) at the secondary site and the Session Director at the primary site (2.2.85.45).

```
list trace tac 130                                                   Page   1
                                LIST TRACE
time            data
14:41:58     Calling party trunk-group 30 member 1  cid 0x88
14:41:58     Calling Number & Name 7328522550 NO-CPName
14:41:58     active trunk-group 30 member 1  cid 0x88
14:41:58     dial 51003
14:41:58     ring station    51003 cid 0x88
14:41:58     G711MU ss:off ps:20
             rgn:1 [2.2.185.200]:2836
             rgn:3 [2.2.26.4]:3664
14:41:58     G711MU ss:off ps:20
             rgn:3 [2.2.85.45]:49212
             rgn:3 [2.2.26.4]:3656
14:41:58     xoip options: fax:Relay modem:off tty:US  uid:0x50050
             xoip ip: [2.2.26.4]:3656
14:42:07     active station    51003 cid 0x88
14:42:07     G711MU ss:off ps:20
             rgn:3 [2.2.85.45]:49212
             rgn:1 [2.2.185.200]:2836
14:42:07     G711MU ss:off ps:20
             rgn:1 [2.2.185.200]:2836
             rgn:3 [2.2.85.45]:49212
```

In the next example, a call arrives via the primary site SIP trunks, and the call is directed to call vector 1 via a VDN (x51081) that plays an announcement (x22232), and then collects and verifies password digits from a caller. This type of call verifies proper collection of DTMF via RFC 2833, and also illustrates the Communication Manager audio group concept that allows announcements to be sourced from the local Avaya gateway. Audio groups enable efficient utilization of resources, and also provide redundancy benefits.

From the bolded rows, note that the tone receiver as well as the announcements are sourced from a board in the 2A carrier at the primary site.

```
list trace tac 130                                                  Page   1
                                LIST TRACE
time            data
15:16:47     Calling party trunk-group 30 member 1  cid 0x96
15:16:47     Calling Number & Name 7328522550 NO-CPName
15:16:47     active trunk-group 30 member 1  cid 0x96
15:16:47     dial 51081
15:16:47     ring vector 1    cid 0x96
15:16:47     G711MU ss:off ps:20
             rgn:3 [2.2.85.45]:49216
             rgn:3 [2.2.26.4]:3856
15:16:47     xoip options: fax:Relay modem:off tty:US  uid:0x50050
             xoip ip: [2.2.26.4]:3856
15:16:49     tone-receiver     02AXX03 cid 0x96
15:16:49     active announcement    22232 cid 0x96
15:16:49     hear audio-group 1 board 02A08 ext 22232 cid 0x96
15:16:59     active announcement    22234 cid 0x96
15:16:59     hear audio-group 1 board 02A08 ext 22234 cid 0x96
```

In the next example, a call arrives via the primary site SIP trunks, and the call is directed to Avaya call vector 3 via a VDN (x51082) that plays an announcement (x22555) and collects digits for call routing. This also shows the locally-sourced announcements, and illustrates a call that arrives via the primary site SIP trunks, but connects with a user (x51003) at the secondary site.

```
list trace tac 131                                                 Page   1
                                LIST TRACE
time            data
15:44:31     Calling party trunk-group 31 member 1  cid 0xab
15:44:31     Calling Number & Name 7328522550 NO-CPName
15:44:31     active trunk-group 31 member 1  cid 0xab
15:44:31     dial 51082
15:44:31     ring vector 3    cid 0xab
15:44:31     G711MU ss:off ps:20
             rgn:3 [2.2.85.45]:49226
             rgn:3 [2.2.26.4]:4088
15:44:31     xoip options: fax:Relay modem:off tty:US  uid:0x5005a
             xoip ip: [2.2.26.4]:4088
15:44:33     tone-receiver     02AXX08 cid 0xab
15:44:33     active announcement    22555 cid 0xab
15:44:33     hear audio-group 1 board 02A08 ext 22555 cid 0xab
15:44:42     dial 51003
15:44:42     ring station    51003 cid 0xab
15:44:42     G711MU ss:off ps:20
             rgn:1 [2.2.185.200]:2836
             rgn:3 [2.2.26.4]:4096
             VOIP data from: [2.2.26.4]:4088
15:44:46     active station    51003 cid 0xab
15:44:46     G711MU ss:off ps:20
             rgn:3 [2.2.85.45]:49226
             rgn:1 [2.2.185.200]:2836
15:44:46     G711MU ss:off ps:20
             rgn:1 [2.2.185.200]:2836
             rgn:3 [2.2.85.45]:49226
```

The following shows the "status trunk" output for this same call, reinforcing the trace. The final connection is "ip-direct" from the IP Telephone (2.2.185.200) at the secondary site to the Acme Packet Net-Net 4500 (2.2.85.45) at the primary site. For Communication Manager, this is like any inter-region connection, subject to the typical rules of inter-region connection management (i.e., codec selection, call admission control, etc.).

```
status trunk 31/1                                           Page   2 of   3
                                CALL CONTROL SIGNALING
Near-end Signaling Loc: 02B0217
  Signaling   IP Address                             Port
   Near-end:  2.2.85.20                            : 5060
    Far-end:  2.2.85.45                            : 5060
 H.245 Near:
  H.245 Far:
   H.245 Signaling Loc:           H.245 Tunneled in Q.931? no

 Audio Connection Type: ip-direct     Authentication Type: None
    Near-end Audio Loc:                        Codec Type: G.711MU
   Audio      IP Address                             Port
   Near-end:  2.2.185.200                          : 2836
    Far-end:  2.2.85.45                            : 49226
```

5.1.2. Outgoing Call to PSTN from Primary Site

The following trace shows an outbound ARS call from IP Telephone x52020 to the PSTN number 17328522550. The call is routed based on the location of the originator to route pattern 30, which contains trunk group 31. The call initially uses a media processor in region 3 (2.2.26.4), but after the call is answered, the call is "shuffled" to become an "ip-direct" connection between the IP Telephone (2.2.1.109) and the Acme Packet Session Director at the primary site (2.2.85.45).

```
list trace station 52020                                           Page   1
                                LIST TRACE
time            data
16:01:11     active station    52020 cid 0xb4
16:01:11     G711MU ss:off ps:20
             rgn:3 [2.2.1.109]:15144
             rgn:3 [2.2.26.4]:4196
16:01:14     dial 991732852 route:ARS
16:01:14     term trunk-group 31    cid 0xb4
16:01:15     dial 9917328522550 route:ARS
16:01:15     route-pattern  30 preference 1  cid 0xb4
16:01:15     seize trunk-group 31 member 2  cid 0xb4
16:01:15     Setup digits 7328522550
16:01:15     Calling Number & Name 52020 John Public
16:01:15     Proceed trunk-group 31 member 2  cid 0xb4
16:01:15     G711MU ss:off ps:20
             rgn:3 [2.2.85.45]:49228
             rgn:3 [2.2.26.4]:4208
16:01:15     xoip options: fax:Relay modem:off tty:US  uid:0x5005b
             xoip ip: [2.2.26.4]:4208
16:01:22     active trunk-group 31 member 2  cid 0xb4
16:01:22     G711MU ss:off ps:20
             rgn:3 [2.2.1.109]:15144
             rgn:3 [2.2.85.45]:49228
16:01:22     G711MU ss:off ps:20
             rgn:3 [2.2.85.45]:49228
             rgn:3 [2.2.1.109]:15144
```

Outbound calls were also made to PSTN destinations requiring a log-in with password, such as a messaging system, to verify that DTMF was working properly in the outbound direction.

5.1.3. Incoming Calls from PSTN Arriving Via PSTN to Secondary Site

The following trace output shows a call incoming on signaling group 60 / trunk group 60 from PSTN telephone 732-852-2550. The incoming call handling table for trunk group 60 mapped the received number (22940) to extension 51003. Extension 51003 is an IP Telephone with IP Address 2.2.185.200 in Region 1. Initially, the IP Media Processor in region 1 (2.2.185.4) is used, but as can be seen in the final lines, once the call is answered, the final RTP media path is "ip-direct" from the IP Telephone (2.2.185.200) to the "inside" of the Acme Packet Net-Net 4500 at the secondary site (2.2.185.145).

```
list trace tac 160                                                    Page   1
                                LIST TRACE
time            data
14:20:28     Calling party trunk-group 60 member 1  cid 0x79
14:20:28     Calling Number & Name 7328522550 NO-CPName
14:20:28     active trunk-group 60 member 1  cid 0x79
14:20:28     dial 51003
14:20:28     ring station    51003 cid 0x79
14:20:28     G711MU ss:off ps:20
             rgn:1 [2.2.185.200]:2836
             rgn:1 [2.2.185.4]:2732
14:20:28     G711MU ss:off ps:20
             rgn:1 [2.2.185.145]:49290
             rgn:1 [2.2.185.4]:2724
14:20:28     xoip options: fax:Relay modem:off tty:US  uid:0x50064
             xoip ip: [2.2.185.4]:2724
14:20:32     active station    51003 cid 0x79
14:20:33     G711MU ss:off ps:20
             rgn:1 [2.2.185.145]:49290
             rgn:1 [2.2.185.200]:2836
14:20:33     G711MU ss:off ps:20
             rgn:1 [2.2.185.200]:2836
             rgn:1 [2.2.185.145]:49290
```

With this call up, the "show sipd agent" command was run on the Acme Packet Net-Net 4500 in the secondary site, with the following output. Note that session agent 2.2.185.2 (C-LAN for signaling group 60) shows an Active Outbound session, and session agent 10.3.3.1 (the SIP Service Provider) shows an Active Inbound session.

```
sbcsecsite-pri# show sipd agent
14:25:19-59 (recent)
                   ----- Inbound -----  ---- Outbound ----- -- Latency --   Max
Session Agent      Active  Rate  ConEx  Active  Rate  ConEx    Avg    Max Burst
10.3.3.1          I     1   0.0      0       0   0.0      0  0.004  0.004     2
2.2.185.2         I     0   0.0      0       1   0.0      0  0.118  0.118     2
2.2.185.20        I     0   0.0      0       0   0.0      0  0.117  0.117     2
```

The following output shows a "status trunk" command output illustrating status for a different inbound call, this time using signaling group 61 and trunk group 61. Recall that the Session Director is configured for round-robin call distribution to these two session agents. For signaling purposes, the C-LAN at 2.2.185.20 is communicating with the Session Director at 2.2.185.145. The media path is directly from the IP Telephone (2.2.185.200) to the Session Director. For any of these traces, it can be observed that the far-end port for RTP (in this case 49292) is within the range specified by the Acme Packet “steering-pool”.

```
status trunk 61/1                                               Page   2 of   3
                                CALL CONTROL SIGNALING
Near-end Signaling Loc: 01A1017
  Signaling   IP Address                               Port
   Near-end:  2.2.185.20                             : 5060
    Far-end:  2.2.185.145                            : 5060
 H.245 Near:
  H.245 Far:
   H.245 Signaling Loc:           H.245 Tunneled in Q.931? no

 Audio Connection Type: ip-direct     Authentication Type: None
    Near-end Audio Loc:                        Codec Type: G.711MU
   Audio      IP Address                               Port
   Near-end:  2.2.185.200                            : 2836
    Far-end:  2.2.185.145                            : 49292
```

With this call up, the “show sipd agent” command was run on the Acme Packet Net-Net 4500 in the secondary site, with the following output. Note that session agent 2.2.185.20 (C-LAN for signaling group 61) shows an Active Outbound session, and session agent 10.3.3.1 (the SIP Service Provider) shows an Active Inbound session.

```
sbcsecsite-pri# show sipd agent
14:29:05-45 (recent)
                   ----- Inbound -----  ---- Outbound ----- -- Latency --   Max
Session Agent      Active  Rate  ConEx  Active  Rate  ConEx    Avg    Max Burst
10.3.3.1          I     1   0.0      0       0   0.0      0  0.004  0.004     2
2.2.185.2         I     0   0.0      0       0   0.0      0  0.118  0.118     2
2.2.185.20        I     0   0.0      0       1   0.0      0  0.119  0.119     2
```

In the next example, a call arrives via the secondary site SIP trunks, and the call is directed to Avaya call vector 1 via a VDN (x51081) that plays an announcement (x22232), and then collects and verifies password digits from a caller. This type of call verifies proper collection of DTMF via RFC 2833, and also illustrates the Communication Manager audio group concept that allows announcements to be sourced from the local Avaya gateway.

From the bolded rows, note that the tone receiver as well as the announcements are sourced from a board in the 1A carrier at the secondary site.

```
list trace tac 161                                                  Page   1
                                LIST TRACE
time            data
15:23:49     Calling party trunk-group 61 member 1  cid 0x9d
15:23:49     Calling Number & Name 7328522550 NO-CPName
15:23:49     active trunk-group 61 member 1  cid 0x9d
15:23:49     dial 51081
15:23:49     ring vector 1    cid 0x9d
15:23:49     G711MU ss:off ps:20
             rgn:1 [2.2.185.145]:49300
             rgn:1 [2.2.185.4]:3028
15:23:49     xoip options: fax:Relay modem:off tty:US  uid:0x5006e
             xoip ip: [2.2.185.4]:3028
15:23:51     tone-receiver     01AXX07 cid 0x9d
15:23:51     active announcement    22232 cid 0x9d
15:23:51     hear audio-group 1 board 01A07 ext 22232 cid 0x9d
15:24:00     active announcement    22234 cid 0x9d
15:24:00     hear audio-group 1 board 01A07 ext 22234 cid 0x9d
```

In the next example, a call arrives via the secondary site SIP trunks, and the call is directed to Avaya call vector 3 via a VDN (x51082) that plays an announcement (x22555) and collects digits for call routing. While this also shows the locally-sourced announcements, this is included to show a call that arrives via the secondary site SIP trunks, but connects with a user (x52020) at the primary site.

```
list trace tac 160                                                  Page   1
                                LIST TRACE
time            data
15:50:14     Calling party trunk-group 60 member 1  cid 0xad
15:50:14     Calling Number & Name 7328522550 NO-CPName
15:50:14     active trunk-group 60 member 1  cid 0xad
15:50:14     dial 51082
15:50:14     ring vector 3    cid 0xad
15:50:14     G711MU ss:off ps:20
             rgn:1 [2.2.185.145]:49302
             rgn:1 [2.2.185.4]:3084
15:50:14     xoip options: fax:Relay modem:off tty:US  uid:0x50064
             xoip ip: [2.2.185.4]:3084
15:50:16     tone-receiver     01AXX03 cid 0xad
15:50:16     active announcement    22555 cid 0xad
15:50:16     hear audio-group 1 board 01A07 ext 22555 cid 0xad
             <text removed>
15:50:31     dial 52020
15:50:31     ring station    52020 cid 0xad
15:50:31     G711MU ss:off ps:20
             rgn:3 [2.2.1.109]:15144
             rgn:1 [2.2.185.4]:3092
15:50:34     active station    52020 cid 0xad
15:50:34     G711MU ss:off ps:20
             rgn:1 [2.2.185.145]:49302
             rgn:3 [2.2.1.109]:15144
15:50:34     G711MU ss:off ps:20
             rgn:3 [2.2.1.109]:15144
             rgn:1 [2.2.185.145]:49302
```

The following shows the “status trunk” output for this same call, reinforcing the trace. The final connection is ip-direct from the IP Telephone (2.2.1.109) at the primary site to the Acme Packet Net-Net 4500 (2.2.185.145) at the secondary site. For Communication Manager, this is like any inter-region connection, subject to the typical rules of inter-region connection management (i.e., codec selection, call admission control, etc.).

```
status trunk 60/1                                               Page   2 of   3
                                CALL CONTROL SIGNALING
Near-end Signaling Loc: 01A0217
  Signaling   IP Address                               Port
   Near-end:  2.2.185.2                              : 5060
    Far-end:  2.2.185.145                            : 5060
 H.245 Near:
  H.245 Far:
   H.245 Signaling Loc:           H.245 Tunneled in Q.931? no

 Audio Connection Type: ip-direct     Authentication Type: None
    Near-end Audio Loc:                        Codec Type: G.711MU
   Audio      IP Address                               Port
   Near-end:  2.2.1.109                              : 15144
    Far-end:  2.2.185.145                            : 49302
```

5.1.4. Outgoing Call to PSTN from Secondary Site

The following trace shows an outbound ARS call from IP Telephone x51003 to the PSTN number 17328522550. (Note that this is the same telephone number called in Section 5.1.2). The call is routed based on the location of the originator to route pattern 60, which contains trunk group 61. The call initially uses a media processor in region 1 (2.2.185.4), but after the call is answered, the call is “shuffled” to become an “ip-direct” connection between the IP Telephone (2.2.185.200) and the Acme Packet at the secondary site (2.2.185.145).

```
list trace station 51003                                            Page   1
                                LIST TRACE
time            data
16:08:09     active station    51003 cid 0xb9
16:08:09     G711MU ss:off ps:20
             rgn:1 [2.2.185.200]:2836
             rgn:1 [2.2.185.4]:3200
16:08:13     dial 991732852 route:ARS
16:08:13     term trunk-group 61    cid 0xb9
16:08:14     dial 9917328522550 route:ARS
16:08:14     route-pattern  60 preference 1  cid 0xb9
16:08:14     seize trunk-group 61 member 2  cid 0xb9
16:08:14     Setup digits 7328522550
16:08:14     Calling Number & Name 7328521003 Peter Parker
16:08:14     Proceed trunk-group 61 member 2  cid 0xb9
16:08:14     G711MU ss:off ps:20
             rgn:1 [2.2.185.145]:49308
             rgn:1 [2.2.185.4]:3212
16:08:14     xoip options: fax:Relay modem:off tty:US  uid:0x5006f
             xoip ip: [2.2.185.4]:3212
16:08:19     active trunk-group 61 member 2  cid 0xb9
16:08:19     G711MU ss:off ps:20
             rgn:1 [2.2.185.200]:2836
             rgn:1 [2.2.185.145]:49308
16:08:19     G711MU ss:off ps:20
             rgn:1 [2.2.185.145]:49308
             rgn:1 [2.2.185.200]:2836
```

Outbound calls were also made to PSTN destinations requiring a log-in with password, such as a messaging system, to verify that DTMF was working properly in the outbound direction.

5.2. Enterprise IP WAN Failure Isolating Secondary Site (ESS Controls Secondary Site Only)

This section shows example calls when the enterprise IP network that allows the secondary site to communicate with other sites is down. Refer to “Induced Failure Reference Number 1” in **Figure 1**. Since the secondary site is isolated from the primary site, the S8500 ESS in the secondary site controls the Avaya G650 Media Gateway in the secondary site. The primary site has not experienced a failure, and therefore the primary site active S8730 Server still controls the primary site Avaya G650 Media Gateway.

The following screen, taken from the ESS, shows that the ESS is controlling port network 1 only.

```
list ipserver-interface
                       IP SERVER INTERFACE INFORMATION

Port Pri/   Primary/         Primary/         Primary/                State Of
Ntwk Sec    Secondary        Secondary        Secondary Serv  Control Health
Num  Bd Loc IP Address       Host Name        DHCP ID   State State   C P E G
---- ------ ---------------  ---------------- --------- ----- ------- -------
  1   1A01  2.2.185.9        2.2.185.9        ipsi-A01a  IN   actv-aa 0.0.0.0
  2   2A01  2.2.85.9         2.2.85.9         ipsi-A02a  OUT  active  0.1.1.0
```

5.2.1. Incoming Call from PSTN to Primary Site

Since the primary site remains under the control of the Avaya S8730 Server, incoming calls from the SIP Trunks at the primary site to primary site users are identical to those illustrated in Section 5.1.1. These traces will not be repeated here.

If an incoming call arrives from the PSTN via the primary site SIP trunks, and needs to be directed to a user at the secondary site, then the call can complete using the Communication Manager Dial Plan Transparency feature. Reference [DPT] shows an example configuration for Dial-Plan Transparency using the same two sites configured in these Application Notes. In the sample configuration, the routing of the calls to the Listed Directory Numbers (LDN) used for Dial-Plan Transparency (DPT) used traditional ISDN-PRI trunks to the PSTN. Although not tested as part of these Application Notes, there is nothing that precludes use of SIP Trunks to route the inter-network region LDN calls for DPT.

The following trace gives an example of a call that arrives via the primary site SIP trunks controlled by the Avaya S8730 Server, but the call is meant for a secondary site user, while the secondary site is under the control of the ESS.

```
list trace tac 130                                                     Page   1
                                LIST TRACE
time            data
13:34:24     Calling party trunk-group 30 member 1  cid 0xd80
13:34:24     Calling Number & Name 7328522550 NO-CPName
13:34:24     active trunk-group 30 member 1  cid 0xd80
13:34:24     dial 51003
13:34:24     term station    51003 cid 0xd80
13:34:24     DPT starting to NR  1 station  51003 cid 0xd80
13:34:24     dial 7328511777 route:ARS
13:34:24     term trunk-group 11    cid 0xd80
13:34:24     dial 7328511777 route:ARS
13:34:24     route-pattern  11 preference 1  cid 0xd80
13:34:24     seize trunk-group 11 member 4  cid 0xd80
13:34:24     Calling Number & Name 7328522550 NO-CPName
13:34:25     Proceed trunk-group 11 member 4  cid 0xd80
13:34:25     tone-receiver     02B0108 cid 0xd80
13:34:25     Alert trunk-group 11 member 4  cid 0xd80
13:34:25     G711MU ss:off ps:20
             rgn:3 [2.2.85.45]:49166
             rgn:3 [2.2.26.4]:2112
13:34:25     xoip options: fax:Relay modem:off tty:US  uid:0x50050
             xoip ip: [2.2.26.4]:2112
13:34:25     active trunk-group 11 member 4  cid 0xd80
```

The following screen shows the "status trunk" output from the S8730 Server for this same call, after the call was answered by station 51003 at the secondary site. The primary site has a connection between the incoming SIP trunk and the outbound ISDN-PRI trunk used to route the DPT LDN call. The RTP media path connects the primary site Session Director to the active media processor (2.2.26.4) in the duplicated media processor configuration at the primary site, to convert to the TDM interface used by the ISDN-PRI card.

```
status trunk 30/1                                               Page   2 of   4
                                CALL CONTROL SIGNALING
Near-end Signaling Loc: 02A0217
  Signaling   IP Address                               Port
   Near-end:  2.2.85.2                               : 5060
    Far-end:  2.2.85.45                              : 5060
 H.245 Near:
  H.245 Far:
   H.245 Signaling Loc:           H.245 Tunneled in Q.931? no

 Audio Connection Type: ip-tdm        Authentication Type: None
    Near-end Audio Loc: 02A0701                Codec Type: G.711MU
   Audio      IP Address                               Port
   Near-end:  2.2.26.4                               : 2112
    Far-end:  2.2.85.45                              : 49166
```

The following trace, taken from the S8500 ESS, shows the trace of the incoming DPT LDN call from an ISDN-PRI interface for this same call. The number “51777” in the trace is the “Incoming LDN Extension” for network region 1, as documented in the sample configuration in reference [DPT]. The called user sees the display “CALL FROM 732-852-2550 SV”, which is typical of a call that uses DPT to complete in survivable mode. The number “732-852-2550” is the actual PSTN caller’s telephone number.

```
list trace tac 107                                                  Page   1
                                LIST TRACE
time            data
13:35:25     Calling party trunk-group 7 member 4  cid 0x1d
13:35:25     Calling Number & Name 7328522550 NO-CPName
13:35:25     active trunk-group 7 member 4  cid 0x1d
13:35:25     dial 51777
13:35:25     ring      cid 0x1d
13:35:25     active      cid 0x1d
13:35:25     tone-receiver     01AXX04 cid 0x1d
13:35:28     ring station    51003 cid 0x1d
13:35:28     G711MU ss:off ps:20
             rgn:1 [2.2.185.200]:2734
             rgn:1 [2.2.185.4]:2132
13:35:34     active station    51003 cid 0x1d
             VOIP data from: [2.2.185.4]:2132
```

5.2.2. Outgoing Call to PSTN from Primary Site

Since the primary site remains under the control of the Avaya S8730 Server, calls from primary site users are identical to those illustrated in Section 5.1.2. Traces will not be repeated here.

5.2.3. Incoming Call from PSTN to Secondary Site

An incoming call to the secondary site, under the control of the ESS, also appears the same as those shown in Section 5.1.3. The following trace is included for completeness, to reinforce the capability of the ESS in a fragmented system to handle calls using the same call flow logic, requesting the same vectors and audio-group announcements, as when the system is whole (i.e., all gateways controlled by the same server). The trace shows a call to a meet-me conference.

```
list trace tac 130                                                  Page   1
                                LIST TRACE
time            data
15:51:35     Calling party trunk-group 30 member 1  cid 0x2b9
15:51:35     Calling Number & Name 7328522550 NO-CPName
15:51:35     active trunk-group 30 member 1  cid 0x2b9
15:51:35     dial 51081
15:51:35     ring vector 1    cid 0x2b9
15:51:35     G711MU ss:off ps:20
             rgn:3 [2.2.85.45]:49244
             rgn:3 [2.2.26.4]:12148
15:51:35     xoip options: fax:Relay modem:off tty:US  uid:0x50050
             xoip ip: [2.2.26.4]:12148
15:51:37     tone-receiver     02B0108 cid 0x2b9
15:51:37     active announcement    22232 cid 0x2b9
15:51:37     hear audio-group 1 board 02A08 ext 22232 cid 0x2b9
15:51:42     active announcement    22234 cid 0x2b9
15:51:42     hear audio-group 1 board 02A08 ext 22234 cid 0x2b9
```

In a fragmented system, where one server controls one site, and another server controls another site, it should be understood that calls to meet-me conference vectors could result in some conferees joining one conference on one system, and some conferees joining a different physical conference on the other system, even though the users dialed the same conference number. Conditional logic can be used in the meet-me conference vector commands to distinguish behavior depending on whether a main or a survivable server is in control.

5.2.4. Outgoing Call to PSTN from Secondary Site

If an outbound PSTN call is made from a secondary site user that results in the call being routed to route pattern 60, using the configuration shown in these Application Notes, where secondary site trunks are listed before primary site trunks, the results are the same as those shown in Section 5.1.4 for normal operation.

The following trace, taken from the ESS, shows an outbound ARS call from IP Telephone x51003 to the PSTN number 17328522550. (Note that this is the same telephone number called in Section 5.1.2). The call is routed based on the location of the originator to route pattern 60, which contains trunk group 61. The call initially uses a media processor in region 1 (2.2.185.4), but after the call is answered, the call is “shuffled” to become an “ip-direct” connection between the IP Telephone (2.2.185.200) and the Acme Packet at the secondary site (2.2.185.145).

```
list trace station 51003                                           Page   1
                                LIST TRACE
time            data
13:48:48     active station    51003 cid 0x1e
13:48:48     G711MU ss:off ps:20
             rgn:1 [2.2.185.200]:2734
             rgn:1 [2.2.185.4]:2176
13:48:53     dial 991732852 route:ARS
13:48:53     term trunk-group 61    cid 0x1e
13:48:54     dial 9917328522550 route:ARS
13:48:54     route-pattern  60 preference 1  cid 0x1e
13:48:54     seize trunk-group 61 member 2  cid 0x1e
13:48:54     Setup digits 7328522550
13:48:54     Calling Number & Name 7328521003 Peter Parker
13:48:54     Proceed trunk-group 61 member 2  cid 0x1e
13:48:54     G711MU ss:off ps:20
             rgn:1 [2.2.185.145]:49162
             rgn:1 [2.2.185.4]:2188
13:48:54     xoip options: fax:Relay modem:off tty:US  uid:0x5006f
             xoip ip: [2.2.185.4]:2188
             VOIP data from: [2.2.185.4]:2188
13:49:02     active trunk-group 61 member 2  cid 0x1e
13:49:02     G711MU ss:off ps:20
             rgn:1 [2.2.185.200]:2734
             rgn:1 [2.2.185.145]:49162
13:49:02     G711MU ss:off ps:20
             rgn:1 [2.2.185.145]:49162
             rgn:1 [2.2.185.200]:2734
```

If the configuration were different, such that a call from the secondary site user was directed to a route pattern where the SIP trunks at the primary site were listed before the SIP trunks at the secondary site, see Section 6.

5.3. Avaya S8730 Servers Off-Line (ESS Controls Primary and Secondary Site)

This section pertains to cases where both Avaya S8730 Servers are off-line. Refer to induced failure reference number 4 in **Figure 1**.

Note that if only one S8730 Server is off-line, the system continues to operate using the operational server in the statefully redundant S8730 Server pair. Indeed, all components in the Avaya control network can be duplicated (i.e., duplicated servers, duplicated control network switch connectivity, duplicated IPSI cards in Avaya G650 Media Gateways) to mitigate the risk of the failure type noted in this section. To induce the failure resulting in the ESS controlling both sites during testing, the S8730 Servers were disabled such that IPSI cards at both the primary site and secondary site were unable to communicate with either Avaya S8730 Server.

From the time the failure is induced until the expiration of the "IPSI no-service timer" governing ESS fail-over, all inbound calls to the enterprise will fail. The Acme Packet Net-Net 4500 will get no response from Communication Manager. As described in Section 1, an inbound call can result in a SIP 408 back to the SIP Service Provider, due to a "transaction timeout", or a 503 back to the SIP Service Provider, once the session agents are marked out-of-service.

After the IPSI no-service timer expires, the ESS will take control over the Avaya G650 Media Gateways at both the primary and secondary sites. The Avaya interfaces will be reset and brought into service. After this, all incoming and outgoing calls will behave identically to those shown in Section 5.1. That is, Communication Manager running on the ESS can direct calls identically to Communication Manager running on the main S8730 cluster. This was tested successfully, but the redundant traces are not included here. (If desired, conditional operators in call vectors can distinguish behaviors when an ESS is controlling call processing.)

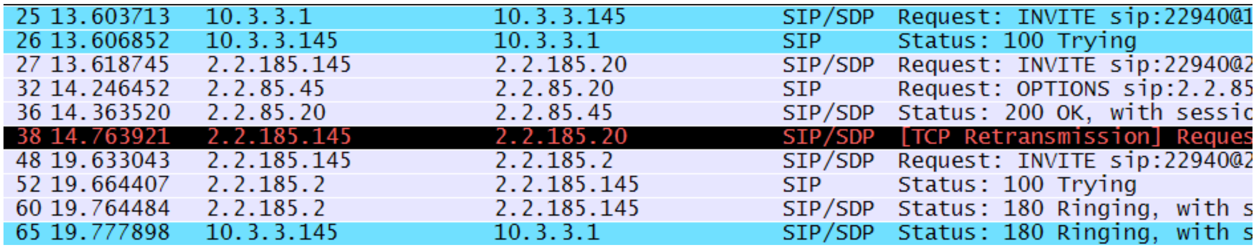
5.4. Avaya C-LAN(s) Off-line or Busy

This section pertains to cases where an Avaya C-LAN interface is not reachable by the Acme Packet Net-Net Session Director. Refer to induced failure reference numbers 3, 3A, 6, and 6A in **Figure 1**.

5.4.1. Incoming Call from PSTN to a SAG with One Failed or Busy C-LAN

If there is one failed C-LAN (session agent) at the time when an incoming call arrives, the behavior depends on whether the Acme Packet Net-Net 4500 has realized the C-LAN is no longer available. If the Session Director has not made the determination that the C-LAN is unreachable, the C-LAN could be tried, subject to the SAG group strategy. The session will experience a "transaction timeout", and the session agent will be marked out-of-service. The INVITE will be directed to the working session agent in the SAG, and the call will complete, albeit with a slight delay (i.e., the transaction timeout).

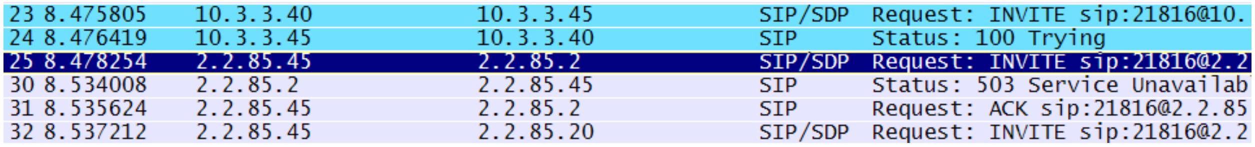
The following Wireshark trace illustrates such a condition. In frame 25, the service provider sends an INVITE to the Session Director at the secondary site. In frame 27, the Session Director sends the INVITE to session agent 2.2.185.20, corresponding to signaling group 61. However, just before this call, Ethernet connectivity to the C-LAN with IP Address 2.2.185.20 was removed. In frame 38, the TCP re-transmission can be seen. In frame 48, six seconds after the INVITE was initially sent in frame 27, the Session Director sends an INVITE to session agent 2.2.185.2 in the same SAG. The call succeeds using signaling group and trunk group 60.



```
25 13.603713  10.3.3.1       10.3.3.145     SIP/SDP  Request: INVITE sip:22940@1
26 13.606852  10.3.3.145     10.3.3.1       SIP      Status: 100 Trying
27 13.618745  2.2.185.145    2.2.185.20     SIP/SDP  Request: INVITE sip:22940@2
32 14.246452  2.2.85.45      2.2.85.20      SIP      Request: OPTIONS sip:2.2.85
36 14.363520  2.2.85.20      2.2.85.45      SIP/SDP  Status: 200 OK, with sessic
38 14.763921  2.2.185.145    2.2.185.20     SIP/SDP  [TCP Retransmission] Reques
48 19.633043  2.2.185.145    2.2.185.2      SIP/SDP  Request: INVITE sip:22940@2
52 19.664407  2.2.185.2      2.2.185.145    SIP      Status: 100 Trying
60 19.764484  2.2.185.2      2.2.185.145    SIP/SDP  Status: 180 Ringing, with s
65 19.777898  10.3.3.145     10.3.3.1       SIP/SDP  Status: 180 Ringing, with s
```

Once the failed C-LAN has been marked out-of-service due to the transaction timeout, new incoming calls will immediately be directed to the working session agent in the SAG, and the call will complete without the delay.

If an Avaya trunk group is busied out (maintenance busy) or simply has no available trunk members when an INVITE arrives for the corresponding signaling group, Communication Manager will respond with a 503. This response will immediately cause the Session Director to attempt to deliver the call to a different session agent in the SAG. The following Wireshark trace illustrates such a call. In frame 23, the SIP Service Provider sends the INVITE to the Session Director. In frame 25, the Session Director sends the INVITE to a Communication Manager session agent, in this case via 2.2.85.2, signaling group 30. At this moment, there are no trunk members in trunk group 30 available to take the call.   In frame 30, Communication Manager responds with a 503. In frame 32, the Session Director sends the INVITE to a different session agent in the SAG, in this case 2.2.85.20, signaling group 31. Although not shown, the call can complete using signaling group and trunk group 31.



```
23 8.475805   10.3.3.40      10.3.3.45      SIP/SDP  Request: INVITE sip:21816@10.
24 8.476419   10.3.3.45      10.3.3.40      SIP      Status: 100 Trying
25 8.478254   2.2.85.45      2.2.85.2       SIP/SDP  Request: INVITE sip:21816@2.2
30 8.534008   2.2.85.2       2.2.85.45      SIP      Status: 503 Service Unavailab
31 8.535624   2.2.85.45      2.2.85.2       SIP      Request: ACK sip:21816@2.2.85
32 8.537212   2.2.85.45      2.2.85.20      SIP/SDP  Request: INVITE sip:21816@2.2
```

Note that the 503 response is not considered a “transaction timeout” and therefore the session agent is not taken out-of-service by the Session Director. If it is intended that the Session Director should no longer try a C-LAN, the Avaya signaling group can be busied out rather than the trunk group. If the Avaya signaling group is busied out, the Session Director will mark the session agent out-of-service.

5.4.2. Incoming Call from PSTN to a SAG After Network Recovery

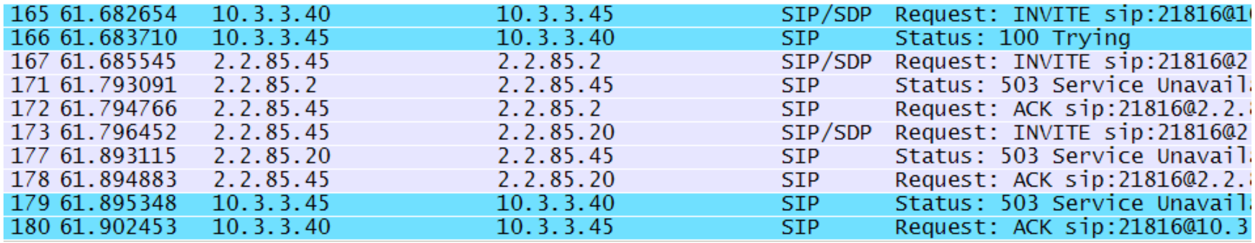
As described in Section 1.3, Communication Manager can mark a SIP Signaling Group for bypass and the corresponding SIP trunk members “Out-of-Service/Far-end” (OOS/FE) due to failure of the SIP OPTIONS exchange. If the network recovers, but a successful SIP OPTIONS exchange has not yet occurred, the Avaya trunk members may be “OOS/FE” when an incoming INVITE arrives.   Communication Manager will accept the incoming call. The following screen shows an example where an incoming call was received just after recovery. Note that Communication Manager 5.2 will quickly mark the trunks in-service.

```
status trunk 30
                             TRUNK GROUP STATUS
Member   Port     Service State      Mtce Connected Ports
                                     Busy
0030/001 T00080   OOS/FE-active      no   S00046
0030/002 T00081   OOS/FE-idle        no
0030/003 T00082   OOS/FE-idle        no
```

5.4.3. Incoming Call from PSTN when All Failed C-LANs / All Trunks Busy

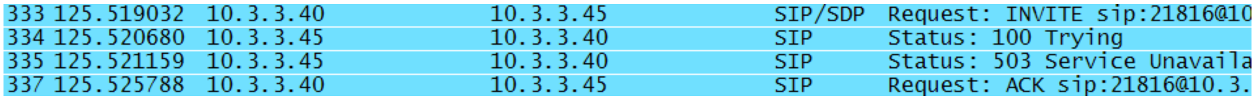
If all C-LAN session agents that are members of a SAG are not responding, or all trunks at a site are busy, then the Acme Packet Net-Net 4500 will in general return a SIP 503 to the network. Assuming the SIP Service Provider can redirect calls to the opposite site upon receiving a 503 from the initial site used for the call, then the call can complete successfully at the working site.

The following is a wireshark trace for an “all trunks busy” condition. In frame 165, the service provider sends an INVITE to the Session Director. In frame 167, the Session Director sends the INVITE to 2.2.85.2, the session agent corresponding to Avaya signaling group 30. In frame 171, Communication Manager sends a 503. In this case, there are no available trunk members in trunk group 30 to handle the call. In frame 173, the Session Director sends the INVITE to 2.2.85.20, another session agent in the same SAG. In frame 177, Communication Manager sends a 503 because there are no available trunk members in trunk group 31 either. In frame 179, the Session Director returns a 503 to the SIP Service Provider. For calls to fail-over to the alternate site, the SIP Service Provider must have the capability to redirect the call upon receipt of a 503 Service Unavailable from the enterprise site.



```
165 61.682654   10.3.3.40           10.3.3.45           SIP/SDP  Request: INVITE sip:21816@1
166 61.683710   10.3.3.45           10.3.3.40           SIP      Status: 100 Trying
167 61.685545   2.2.85.45           2.2.85.2            SIP/SDP  Request: INVITE sip:21816@2
171 61.793091   2.2.85.2            2.2.85.45           SIP      Status: 503 Service Unavail
172 61.794766   2.2.85.45           2.2.85.2            SIP      Request: ACK sip:21816@2.2.
173 61.796452   2.2.85.45           2.2.85.20           SIP/SDP  Request: INVITE sip:21816@2
177 61.893115   2.2.85.20           2.2.85.45           SIP      Status: 503 Service Unavail
178 61.894883   2.2.85.45           2.2.85.20           SIP      Request: ACK sip:21816@2.2.
179 61.895348   10.3.3.45           10.3.3.40           SIP      Status: 503 Service Unavail
180 61.902453   10.3.3.40           10.3.3.45           SIP      Request: ACK sip:21816@10.3
```

Had the Session Director already marked both session agents in the session agent group out-of-service (e.g., neither C-LAN has responded to previous SIP OPTIONS), the response back to the Service Provider would also be a 503 Service Unavailable. In this case, the 503 response is returned immediately. The following Wireshark trace illustrates this condition.



```
333 125.519032  10.3.3.40           10.3.3.45           SIP/SDP  Request: INVITE sip:21816@10
334 125.520680  10.3.3.45           10.3.3.40           SIP      Status: 100 Trying
335 125.521159  10.3.3.45           10.3.3.40           SIP      Status: 503 Service Unavaila
337 125.525788  10.3.3.40           10.3.3.45           SIP      Request: ACK sip:21816@10.3.
```

5.4.4. Outgoing Calls to PSTN with Signaling Failure

The following screen shows a trace of a call placed immediately after introducing a failure in the signaling path for signaling group 31. Trunk group 31 has not yet been marked out-of-service, so it is chosen. The resultant failure (“denial event 1192”) causes the call to route-advance via Look-Ahead Routing (LAR) to trunk group 30 and complete successfully.

```
list trace tac 131                                                   Page   1
                                LIST TRACE
time            data
14:57:59     dial 9917328522550 route:ARS
14:57:59     route-pattern  30 preference 1  cid 0x60
14:57:59     seize trunk-group 31 member 3  cid 0x60
14:57:59     Calling Number & Name 52020 John Public
14:58:00     denial event 1192: Temporary failure D1=0x8c51 D2=0x29
14:58:00     term trunk-group 31    cid 0x60
14:58:00     route-pattern  30 preference 1 unavailable cid 0x60
14:58:00     dial 9917328522550 route:ARS
14:58:00     term trunk-group 30    cid 0x60
14:58:00     dial 9917328522550 route:ARS
14:58:00     route-pattern  30 preference 2  cid 0x60
14:58:00     seize trunk-group 30 member 2  cid 0x60
14:58:00     Calling Number & Name 52020 John Public
14:58:00     Proceed trunk-group 30 member 2  cid 0x60
14:58:00     G711MU ss:off ps:20
             rgn:3 [2.2.85.45]:49190
             rgn:3 [2.2.26.4]:3352
14:58:04     active trunk-group 30 member 2  cid 0x60
14:58:05     G711MU ss:off ps:20
             rgn:3 [2.2.1.109]:46902
             rgn:3 [2.2.85.45]:49190
14:58:05     G711MU ss:off ps:20
             rgn:3 [2.2.85.45]:49190
             rgn:3 [2.2.1.109]:46902
```

The following shows output from the primary site Acme Packet Net-Net 4500, showing that the Session Director has detected that the session agent (2.2.85.20) is out-of-service.

```
acmesbc-pri# show sipd agent
13:59:42-37 (recent)
                   ----- Inbound -----  ---- Outbound ----- -- Latency --   Max
Session Agent      Active  Rate  ConEx  Active  Rate  ConEx    Avg    Max Burst
10.3.3.40         I      0   0.0      0       1   0.0      0  0.007  0.007     1
2.2.85.2          I      1   0.0      0       0   0.0      0  0.118  0.118     1
2.2.85.20         O      0   0.0      0       0   0.0      0  0.000  0.000     1
```

If Communication Manager has already marked the SIP trunks out-of-service, calls can complete successfully via an in-service trunk in the route-pattern, independent of LAR. For example, if trunks 30 and 31 are out-of-service, calls can complete using trunk group 60 or 61.

5.5. Acme Packet Net-Net Session Director Off-line

This section pertains to cases where an Acme Packet Net-Net Session Director is off-line. For example, during testing the Acme Packet Net-Net Session Director was powered down. Refer to induced failure reference numbers 2 and 5 in **Figure 1**. Again, note that either or both sites could use a pair of Acme Packet Net-Net Session Directors in a High Availability (HA) configuration. The Acme Packet HA configuration was documented and tested in reference [AC-HA].

5.5.1. Incoming Call from PSTN, Site’s Acme Packet Net-Net 4500 Off-line

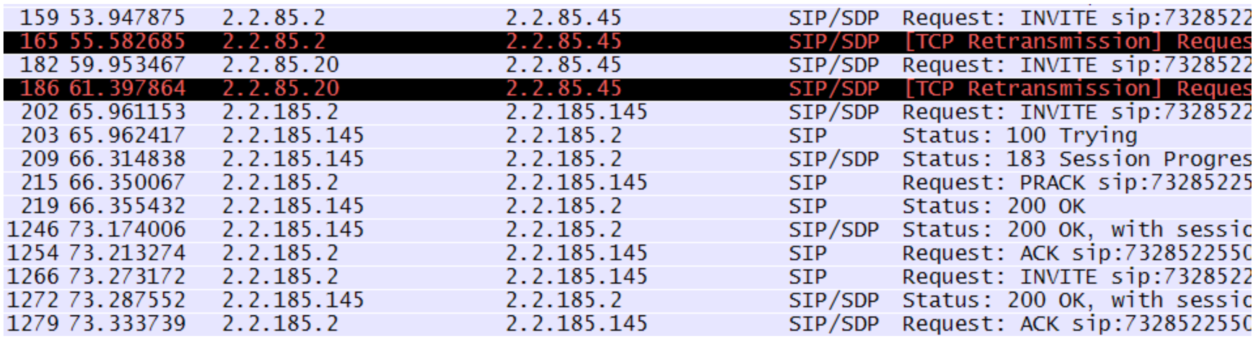
When the Acme Packet Net-Net 4500 is not responding at one site, it is expected that the SIP Service Provider would redirect the call to the other site. Therefore, incoming calls can still succeed, subject to the capabilities of the SIP Service Provider to provide fail-over. From a Communication Manager point of view, incoming calls can arrive from either the primary site or secondary site and reach any user. Therefore, inbound calls with an Acme Packet Net-Net 4500 offline look to Communication Manager like the call traces in Section 5.1, arriving from the working Acme Packet Net-Net 4500.

5.5.2. Outgoing Call to PSTN, Site’s Acme Packet Net-Net 4500 Off-line

The sample trace that follows was taken immediately after power is removed from the Acme Packet Net-Net 4500 at the primary site. Extension 52020 dials the ARS access code followed by 17328522550. The call is delivered to route pattern 30, which lists the two trunk groups at the primary site first followed by the two trunks at the secondary site. Six seconds after trying trunk group 30, the denial event marked in bold in the trace triggers LAR to the next choice in the pattern, trunk group 31. The bold denial event triggers LAR to the next choice, trunk group 60. Since trunk group 60 is operating normally, the call completes using trunk group 60. Note that the six seconds is governed by the timer named “Alternate Route Timer” on the Avaya signaling group. Six seconds is the default value. Ultimately, the final connection is an inter-region “ip-direct” connection between the IP Telephone (2.2.1.109) at the primary site and the Acme Packet Net-Net 4500 (2.2.185.145) at the secondary site.

```
list trace tac 130                                                   Page   1
                                LIST TRACE
time            data
16:42:37     dial 9917328522550 route:ARS
16:42:37     route-pattern  30 preference 1  cid 0x690
16:42:37     seize trunk-group 30 member 2  cid 0x690
16:42:37     Setup digits 7328522550
16:42:37     Calling Number & Name 7328522020 John Public
16:42:43     denial event 1191: Network failure D1=0x8c51 D2=0x26
16:42:43     term trunk-group 30    cid 0x690
16:42:43     route-pattern  30 preference 1 unavailable cid 0x690
16:42:43     dial 9917328522550 route:ARS
16:42:43     term trunk-group 31    cid 0x690
16:42:43     dial 9917328522550 route:ARS
16:42:43     route-pattern  30 preference 2  cid 0x690
16:42:43     seize trunk-group 31 member 2  cid 0x690
16:42:43     Calling Number & Name 7328522020 John Public
16:42:49     denial event 1191: Network failure D1=0x8c51 D2=0x26
16:42:49     term trunk-group 30    cid 0x690
16:42:49     route-pattern  30 preference 2 unavailable cid 0x690
16:42:49     dial 9917328522550 route:ARS
16:42:49     term trunk-group 60    cid 0x690
16:42:49     dial 9917328522550 route:ARS
16:42:49     route-pattern  30 preference 3  cid 0x690
16:42:49     seize trunk-group 60 member 3  cid 0x690
16:42:49     Calling Number & Name 52020 John Public
16:42:49     Proceed trunk-group 60 member 3  cid 0x690
16:42:49     G711MU ss:off ps:20
             rgn:1 [2.2.185.145]:49328
             rgn:3 [2.2.26.4]:28792
16:42:52     active trunk-group 60 member 3  cid 0x690
16:42:53     G711MU ss:off ps:20
             rgn:3 [2.2.1.109]:15144
             rgn:1 [2.2.185.145]:49328
16:42:53     G711MU ss:off ps:20
             rgn:1 [2.2.185.145]:49328
             rgn:3 [2.2.1.109]:15144
```

The following is a wireshark trace for a similar call. In frame 159, Communication Manager sends an INVITE to the Session Director via trunk group 30 (signaling group 30, 2.2.85.2), but receives no response. In frame 182, Communication Manager sends an INVITE to the Session Director via trunk group 31 (signaling group 31, 2.2.85.20), but again receives no response. In frame 202, Communication Manager sends an INVITE to the Session Director at the other site via trunk group 60 (signaling group 60, 2.2.185.2). This call completes successfully.



```
 159 53.947875   2.2.85.2        2.2.85.45       SIP/SDP  Request: INVITE sip:7328522
 165 55.582685   2.2.85.2        2.2.85.45       SIP/SDP  [TCP Retransmission] Reques
 182 59.953467   2.2.85.20       2.2.85.45       SIP/SDP  Request: INVITE sip:7328522
 186 61.397864   2.2.85.20       2.2.85.45       SIP/SDP  [TCP Retransmission] Reques
 202 65.961153   2.2.185.2       2.2.185.145     SIP/SDP  Request: INVITE sip:7328522
 203 65.962417   2.2.185.145     2.2.185.2       SIP      Status: 100 Trying
 209 66.314838   2.2.185.145     2.2.185.2       SIP/SDP  Status: 183 Session Progres
 215 66.350067   2.2.185.2       2.2.185.145     SIP      Request: PRACK sip:73285225
 219 66.355432   2.2.185.145     2.2.185.2       SIP      Status: 200 OK
1246 73.174006   2.2.185.145     2.2.185.2       SIP/SDP  Status: 200 OK, with sessic
1254 73.213274   2.2.185.2       2.2.185.145     SIP      Request: ACK sip:732852255C
1266 73.273172   2.2.185.2       2.2.185.145     SIP      Request: INVITE sip:7328522
1272 73.287552   2.2.185.145     2.2.185.2       SIP/SDP  Status: 200 OK, with sessic
1279 73.333739   2.2.185.2       2.2.185.145     SIP/SDP  Request: ACK sip:732852255C
```

If Ethernet connectivity for the Acme Packet Net-Net 4500 inside interface is removed, call trace results are similar.

If the failure persists, Communication Manager will mark the signaling group for bypass (and trunk groups OOS/FE). Therefore, outbound calls like the ones traced above would immediately proceed to the trunks connecting to the working Acme Packet Net-Net 4500, without the delay associated with the timeout of the outbound INVITEs. LAR is only required when the trunks are chosen because they appear to be in-service, and then a timeout or down-stream failure occurs requiring a route-advance.

The following screen shows an example of an Avaya SIP trunk group in the "Out-of-Service/Far-end" state (OOS/FE). In this state, Communication Manager will accept an incoming call (i.e., accept INVITE), but will not offer an outgoing call (i.e., send INVITE).

```
status trunk 30
                             TRUNK GROUP STATUS
Member   Port     Service State      Mtce Connected Ports
                                     Busy
0030/001 T00080   OOS/FE-idle        no
0030/002 T00081   OOS/FE-idle        no
0030/003 T00082   OOS/FE-idle        no
0030/004 T00083   OOS/FE-idle        no
0030/005 T00084   OOS/FE-idle        no
0030/006 T00085   OOS/FE-idle        no
0030/007 T00086   OOS/FE-idle        no
0030/008 T00087   OOS/FE-idle        no
0030/009 T00088   OOS/FE-idle        no
0030/010 T00089   OOS/FE-idle        no
```

The following screen shows an example of an Avaya SIP signaling group marked for "bypass". This is a signaling group state corresponding to the "OOS/FE" state shown in the prior screen. In general, an Avaya SIP signaling group will be in this state when the far-end has not replied with a 200 OK to previously sourced SIP OPTIONS messages. In the sample configuration, if the Acme Packet Net-Net 4500 at the "far-end" of the Avaya signaling group has failed, this state will be seen.

```
status signaling-group 30
                         STATUS SIGNALING GROUP
        Group ID: 30                            Active NCA-TSC Count: 0
      Group Type: sip                            Active CA-TSC Count: 0
  Signaling Type: facility associated signaling
     Group State: far-end bypass
```

This state will also be seen if the Acme Packet Net-Net 4500 is functioning properly, but the SIP Service Provider that is the "next hop" has failed. The Acme Packet Net-Net 4500 will respond with a 503 when the "next hop" is out of service.

The following command executed at the primary site Acme Packet Net-Net 4500 shows that the session agent to the SIP Service Provider (10.3.3.40) is “O” for out-of-service. This means that the Acme Packet will be unable to forward the SIP OPTIONS received from Communication Manager to the SIP Service Provider. Communication Manager will receive a 503 and mark the trunks for bypass, which is desirable.

```
acmesbc-pri# show sipd agent
12:32:38-41 (recent)
                      ----- Inbound -----   ---- Outbound ----- -- Latency --   Max
Session Agent        Active  Rate  ConEx  Active  Rate  ConEx    Avg    Max Burst
10.3.3.40           O     0   0.0      0       0   0.0      1  0.000  0.000     0
2.2.85.2            I     0   0.0      0       0   0.0      0  0.104  0.118     0
2.2.85.20           I     0   0.0      0       0   0.0      0  0.110  0.118     0
```

The following screen shows the Avaya demand test that can force the SIP OPTIONS to be sent. The failure of test number 1675 shown below corresponds to the failure of the SIP OPTIONS test.

```
test signaling-group 30
                                 TEST RESULTS
Port        Mtce Name   Alt. Name       Test No.  Result           Error Code
30          SIP-SGRP                    1386      PASS
30          SIP-SGRP                    1392      PASS
30          SIP-SGRP                    1387      ABORT            1005
30          SIP-SGRP                    1675      FAIL             3
```

Failure of the secondary site Acme Packet Net-Net 4500 produces similar results.

5.6. SIP Service Provider Network Off-line

This section pertains to cases where all enterprise components are functioning, but the SIP Service Provider network is not. Refer to induced failure reference numbers 7 and 8 in **Figure 1**.

5.6.1. Outbound Calls to PSTN

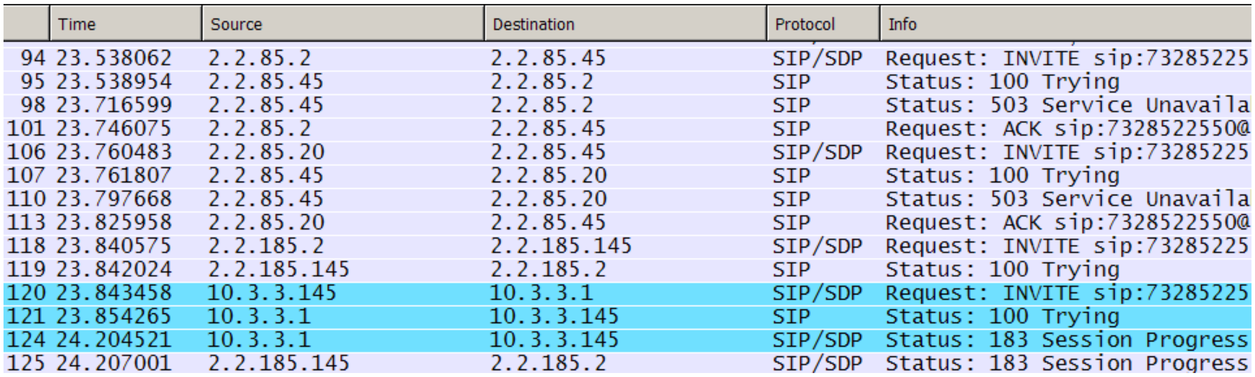
The Communication Manager route-pattern configuration can contain trunks of various kinds. In the sample configuration, only SIP trunk groups are shown in route pattern 30 and 60. In production environments, it will be common to have traditional trunks such as ISDN-PRI trunks available as an alternate to the SIP trunks   A call to a route pattern that preferentially uses SIP trunks can overflow or “look-ahead” and complete successfully to traditional trunks later in the pattern. The following screen shows an example call trace when a user at the primary site attempts an outbound PSTN call right after the failure of the primary site link to the service provider network. That is, Communication Manager can still communicate with the Acme Packet Net-Net 4500, but the Acme Packet Net-Net 4500 at the primary site is unable to communicate with the public network, and the Acme Packet Net-Net 4500 at the primary site has not yet marked the session agent to the public network out-of-service. Since Communication Manager has not yet marked the trunks OOS, the call is offered to the first choice in the route-pattern (a primary site trunk), then the second choice in the route-pattern (another primary site trunk), and then the call completes successfully using the third choice in the route-pattern (a secondary site trunk).

```
list trace station 52020                                           Page   1
                                LIST TRACE
time            data
10:16:40     active station    52020 cid 0xce2
10:16:40     G711MU ss:off ps:20
             rgn:3 [2.2.1.109]:15144
             rgn:3 [2.2.26.4]:2624
10:16:42     dial 991732852 route:ARS
10:16:42     term trunk-group 30    cid 0xce2
10:16:43     dial 9917328522550 route:ARS
10:16:43     route-pattern  30 preference 1  cid 0xce2
10:16:43     seize trunk-group 30 member 7  cid 0xce2
10:16:43     Setup digits 7328522550
10:16:43     Calling Number & Name 7328522020 John Public
10:16:43     Proceed trunk-group 30 member 7  cid 0xce2
10:16:49     denial event 1191: Network failure D1=0x8c51 D2=0x26
10:16:49     route-pattern  30 preference 1 unavailable cid 0xce2
10:16:49     dial 9917328522550 route:ARS
10:16:49     term trunk-group 31    cid 0xce2
10:16:49     dial 9917328522550 route:ARS
10:16:49     route-pattern  30 preference 2  cid 0xce2
10:16:49     seize trunk-group 31 member 5  cid 0xce2
10:16:49     Calling Number & Name 7328522020 John Public
10:16:49     Proceed trunk-group 31 member 5  cid 0xce2
10:16:53     dial 9917328522550 route:ARS
10:16:53     term station    52020 cid 0xce2
10:16:55     denial event 1191: Network failure D1=0x8c51 D2=0x26
10:16:55     term trunk-group 30    cid 0xce2
10:16:55     route-pattern  30 preference 2 unavailable cid 0xce2
10:16:55     dial 9917328522550 route:ARS
10:16:55     term trunk-group 60    cid 0xce2
10:16:55     dial 9917328522550 route:ARS
10:16:55     route-pattern  30 preference 3  cid 0xce2
10:16:55     seize trunk-group 60 member 6  cid 0xce2
10:16:55     Calling Number & Name 7328522020 John Public
10:16:56     Proceed trunk-group 60 member 6  cid 0xce2
10:16:56     G711MU ss:off ps:20
             rgn:1 [2.2.185.145]:49156
             rgn:3 [2.2.26.4]:2688
10:17:01     active trunk-group 60 member 6  cid 0xce2
10:17:01     G711MU ss:off ps:20
             rgn:3 [2.2.1.109]:15144
             rgn:1 [2.2.185.145]:49156
10:17:01     G711MU ss:off ps:20
             rgn:1 [2.2.185.145]:49156
             rgn:3 [2.2.1.109]:15144
```

In the case shown above, the Wireshark trace would show that the Acme Packet Net-Net 4500 at the primary site responds with 100 TRYING to both INVITE messages, but Communication Manager would receive nothing after 100 TRYING. Communication Manager does a “route-advance” due to “LAR = next” on the route-pattern.

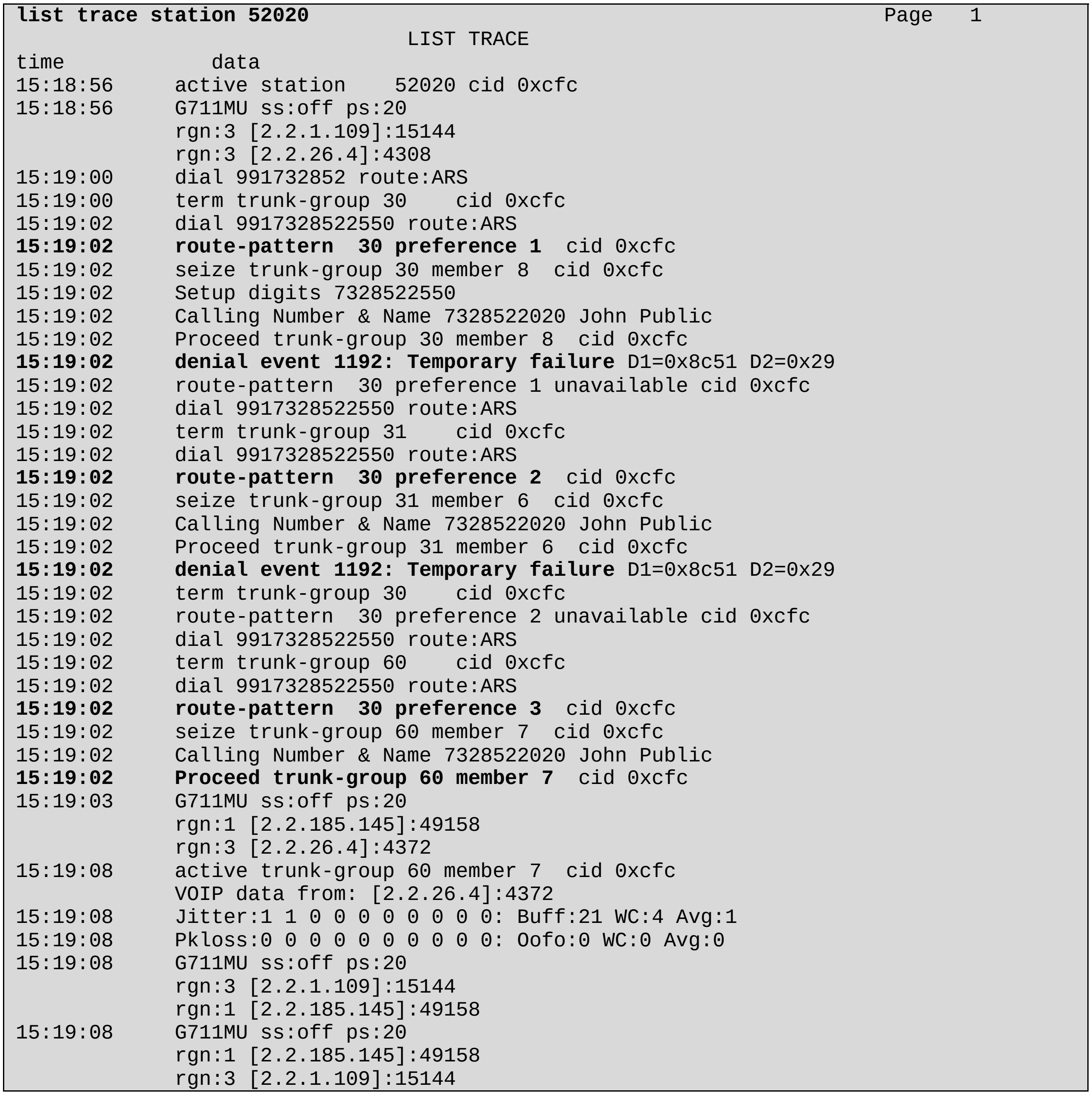
Now assume the network outage persists long enough for the Acme Packet Net-Net 4500 at the primary site to mark the session agent to the public network out-of-service. However, the outage has not persisted long enough for Communication Manager to have marked the trunks to the Session Director out-of-service. In the sample configuration, the Session Director sources SIP OPTIONS every 16 seconds, so the Session Director will generally discover that the session agent to the service provider is out before Communication Manager. The following screen shows an example call trace for a user at the primary site attempting an outbound PSTN call in this state Since Communication Manager has not yet marked the trunks OOS, the call is offered to the first choice in the route-pattern (a primary site trunk). Since the Session Director has already marked the "next-hop" out-of-service, the Session Director responds with a 503. Communication Manager can therefore immediately route-advance (no need to wait for timeout) to the second choice in the route-pattern (another primary site trunk), and again the Session Director responds with a 503. The call completes successfully (and quickly) using the third choice in the route-pattern (a secondary site trunk).

The following portion of a wireshark trace reinforces the description. Frames 94 and 106 show the INVITE sent to the primary site Session Director for trunk groups 30 and 31, respectively. Frames 98 and 110 show the Session Director 503 response, since the next-hop is out-of-service. Frame 118 shows the INVITE sent to the secondary site Session Director via trunk group 60, and the remaining frames show this call is being processed normally. The timestamps show that the route-advance is happening very quickly; the calling user is unlikely to perceive any additional delay due to the "Look-ahead Routing".



	Time	Source	Destination	Protocol	Info
94	23.538062	2.2.85.2	2.2.85.45	SIP/SDP	Request: INVITE sip:73285225
95	23.538954	2.2.85.45	2.2.85.2	SIP	Status: 100 Trying
98	23.716599	2.2.85.45	2.2.85.2	SIP	Status: 503 Service Unavaila
101	23.746075	2.2.85.2	2.2.85.45	SIP	Request: ACK sip:7328522550@
106	23.760483	2.2.85.20	2.2.85.45	SIP/SDP	Request: INVITE sip:73285225
107	23.761807	2.2.85.45	2.2.85.20	SIP	Status: 100 Trying
110	23.797668	2.2.85.45	2.2.85.20	SIP	Status: 503 Service Unavaila
113	23.825958	2.2.85.20	2.2.85.45	SIP	Request: ACK sip:7328522550@
118	23.840575	2.2.185.2	2.2.185.145	SIP/SDP	Request: INVITE sip:73285225
119	23.842024	2.2.185.145	2.2.185.2	SIP	Status: 100 Trying
120	23.843458	10.3.3.145	10.3.3.1	SIP/SDP	Request: INVITE sip:73285225
121	23.854265	10.3.3.1	10.3.3.145	SIP	Status: 100 Trying
124	24.204521	10.3.3.1	10.3.3.145	SIP/SDP	Status: 183 Session Progress
125	24.207001	2.2.185.145	2.2.185.2	SIP/SDP	Status: 183 Session Progress

The following screen shows the Communication Manager call trace for this same call.



```
list trace station 52020                                          Page   1
                                LIST TRACE
time            data
15:18:56     active station    52020 cid 0xcfc
15:18:56     G711MU ss:off ps:20
             rgn:3 [2.2.1.109]:15144
             rgn:3 [2.2.26.4]:4308
15:19:00     dial 991732852 route:ARS
15:19:00     term trunk-group 30    cid 0xcfc
15:19:02     dial 9917328522550 route:ARS
15:19:02     route-pattern  30 preference 1  cid 0xcfc
15:19:02     seize trunk-group 30 member 8  cid 0xcfc
15:19:02     Setup digits 7328522550
15:19:02     Calling Number & Name 7328522020 John Public
15:19:02     Proceed trunk-group 30 member 8  cid 0xcfc
15:19:02     denial event 1192: Temporary failure D1=0x8c51 D2=0x29
15:19:02     route-pattern  30 preference 1 unavailable cid 0xcfc
15:19:02     dial 9917328522550 route:ARS
15:19:02     term trunk-group 31    cid 0xcfc
15:19:02     dial 9917328522550 route:ARS
15:19:02     route-pattern  30 preference 2  cid 0xcfc
15:19:02     seize trunk-group 31 member 6  cid 0xcfc
15:19:02     Calling Number & Name 7328522020 John Public
15:19:02     Proceed trunk-group 31 member 6  cid 0xcfc
15:19:02     denial event 1192: Temporary failure D1=0x8c51 D2=0x29
15:19:02     term trunk-group 30    cid 0xcfc
15:19:02     route-pattern  30 preference 2 unavailable cid 0xcfc
15:19:02     dial 9917328522550 route:ARS
15:19:02     term trunk-group 60    cid 0xcfc
15:19:02     dial 9917328522550 route:ARS
15:19:02     route-pattern  30 preference 3  cid 0xcfc
15:19:02     seize trunk-group 60 member 7  cid 0xcfc
15:19:02     Calling Number & Name 7328522020 John Public
15:19:02     Proceed trunk-group 60 member 7  cid 0xcfc
15:19:03     G711MU ss:off ps:20
             rgn:1 [2.2.185.145]:49158
             rgn:3 [2.2.26.4]:4372
15:19:08     active trunk-group 60 member 7  cid 0xcfc
             VOIP data from: [2.2.26.4]:4372
15:19:08     Jitter:1 1 0 0 0 0 0 0 0 0: Buff:21 WC:4 Avg:1
15:19:08     Pkloss:0 0 0 0 0 0 0 0 0 0: Oofo:0 WC:0 Avg:0
15:19:08     G711MU ss:off ps:20
             rgn:3 [2.2.1.109]:15144
             rgn:1 [2.2.185.145]:49158
15:19:08     G711MU ss:off ps:20
             rgn:1 [2.2.185.145]:49158
             rgn:3 [2.2.1.109]:15144
```

Once Communication Manager detects via a SIP OPTIONS background test that the network is out (see Section 1.3 and Section 5.7 for details), a similar call would simply “bypass” the trunks that are marked out-of-service, and the call would immediately route to the secondary site Acme Packet Net-Net 4500.

The following screen shows a Communication Manager call trace after Communication Manager has marked trunk groups 30 and 31 out-of-service.

```
list trace station 52020                                            Page   1
                                LIST TRACE
time            data
15:25:53     active station    52020 cid 0xcfe
15:25:53     G711MU ss:off ps:20
             rgn:3 [2.2.1.109]:15144
             rgn:3 [2.2.26.4]:4472
15:25:57     dial 991732852 route:ARS
15:25:57     term trunk-group 30    cid 0xcfe
15:25:58     route-pattern  30 preference 1 unavailable cid 0xcfe
15:25:58     term trunk-group 31    cid 0xcfe
15:25:58     route-pattern  30 preference 2 unavailable cid 0xcfe
15:25:58     dial 9917328522550 route:ARS
15:25:58     route-pattern  30 preference 3  cid 0xcfe
15:25:58     seize trunk-group 60 member 8  cid 0xcfe
15:25:58     Setup digits 7328522550
15:25:58     Calling Number & Name 52020 John Public
15:25:58     Proceed trunk-group 60 member 8  cid 0xcfe
15:25:58     G711MU ss:off ps:20
             rgn:1 [2.2.185.145]:49160
             rgn:3 [2.2.26.4]:4480
15:25:58     xoip options: fax:Relay modem:off tty:US  uid:0x5006b
             xoip ip: [2.2.26.4]:4480
             VOIP data from: [2.2.26.4]:4480
15:26:06     active trunk-group 60 member 8  cid 0xcfe
15:26:06     G711MU ss:off ps:20
             rgn:3 [2.2.1.109]:15144
             rgn:1 [2.2.185.145]:49160
15:26:06     G711MU ss:off ps:20
             rgn:1 [2.2.185.145]:49160
             rgn:3 [2.2.1.109]:15144
```

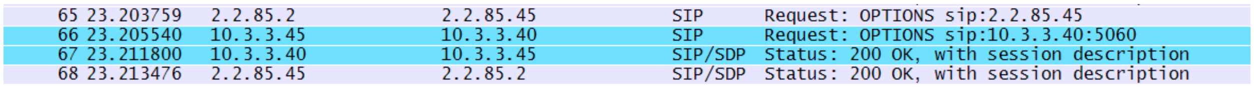
If there is a failure of the SIP Service Provider network at the secondary site, results for outbound calls made by secondary site users would be similar, except the calls would use route-pattern 60 and “route-advance” to the primary site trunks for call completion.

5.6.2. Inbound Calls from PSTN

Obviously, if the service provider is not delivering inbound calls via either site, then no inbound calls will be received. If the service provider experiences a failure at one site, but not at the other, than fail-over mechanisms internal to the SIP service provider may deliver all calls via the working site, even those that may typically arrive via the other site. The Communication Manager and Session Director configuration will allow a call to any user to arrive via either site.

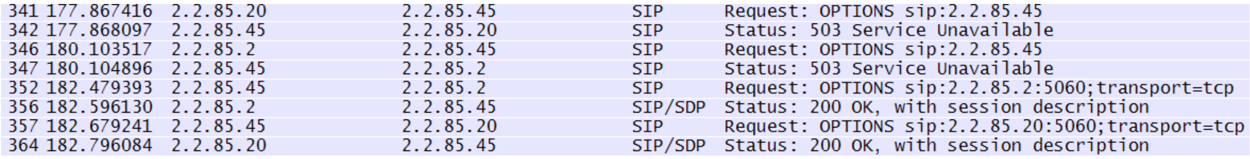
5.7. Wireshark Traces Illustrating SIP OPTIONS Behaviors

See Section 1.3 for additional information. The following portion of a wireshark trace illustrates a SIP OPTIONS exchange initiated by Communication Manager for signaling group 30, when the network is functioning normally. Signaling group 30 has near-end C-LAN IP 2.2.85.2, and the far-end is the inside address of the Acme Packet Net-Net 4500 at the primary site. In frame 65, Communication Manager sends the SIP OPTIONS to the Session Director. In frame 66, the Session Director forwards the SIP OPTIONS to the “outside” SIP Service Provider network, session agent 10.3.3.40. In frame 67, the network responds with 200 OK. In frame 68, the Session Director responds to Communication Manager with 200 OK. The Avaya signaling group is in-service. Note that Wireshark was configured such that TCP messages would appear in gray, and UDP messages in blue.



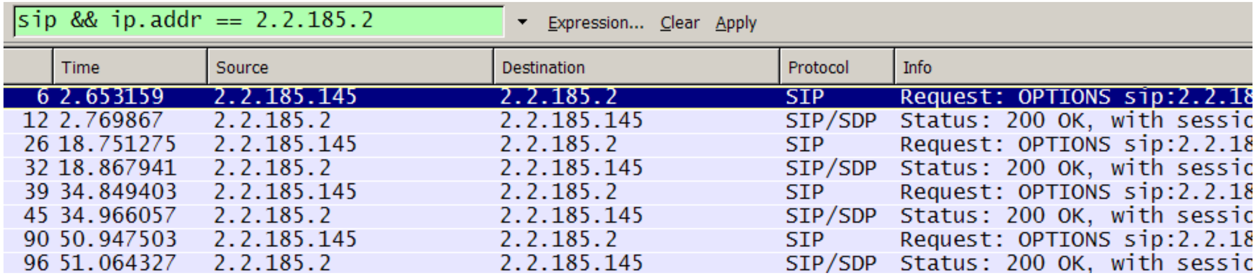
```
 65 23.203759   2.2.85.2          2.2.85.45         SIP      Request: OPTIONS sip:2.2.85.45
 66 23.205540   10.3.3.45         10.3.3.40         SIP      Request: OPTIONS sip:10.3.3.40:5060
 67 23.211800   10.3.3.40         10.3.3.45         SIP/SDP  Status: 200 OK, with session description
 68 23.213476   2.2.85.45         2.2.85.2          SIP/SDP  Status: 200 OK, with session description
```

The following portion of a Wireshark trace illustrates a SIP OPTIONS exchange initiated by Communication Manager for signaling group 30 and 31, when the enterprise network is functioning normally, but the link to the service provider is not. In frames 341 and 346, Communication Manager sends the SIP OPTIONS to the Session Director for signaling groups 31 and 30, respectively. In frames 342 and 347, the Session Director responds with 503 Service Unavailable. Under these conditions, Communication Manager marks signaling groups for "bypass" and the corresponding trunk groups "Out-of-Service/Far-end". In frames 352 and 357, the Session Director sources SIP OPTIONS toward Communication Manager session agents. In frames 356 and 364, Communication Manager responds with 200 OK. The Session Director considers the session agents in-service. If the service provider network recovers and sends an INVITE, the call will be processed by both the Session Director and Communication Manager.



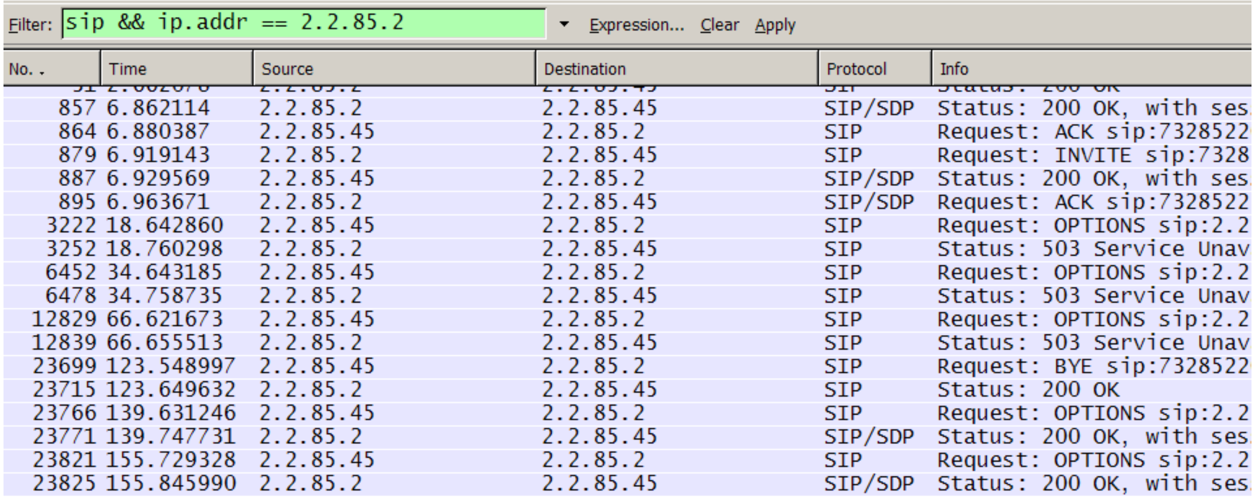
```
341 177.867416  2.2.85.20         2.2.85.45         SIP      Request: OPTIONS sip:2.2.85.45
342 177.868097  2.2.85.45         2.2.85.20         SIP      Status: 503 Service Unavailable
346 180.103517  2.2.85.2          2.2.85.45         SIP      Request: OPTIONS sip:2.2.85.45
347 180.104896  2.2.85.45         2.2.85.2          SIP      Status: 503 Service Unavailable
352 182.479393  2.2.85.45         2.2.85.2          SIP      Request: OPTIONS sip:2.2.85.2:5060;transport=tcp
356 182.596130  2.2.85.2          2.2.85.45         SIP/SDP  Status: 200 OK, with session description
357 182.679241  2.2.85.45         2.2.85.20         SIP      Request: OPTIONS sip:2.2.85.20:5060;transport=tcp
364 182.796084  2.2.85.20         2.2.85.45         SIP/SDP  Status: 200 OK, with session description
```

The following wireshark trace illustrates the periodicity of OPTIONS messages sourced by the Session Director for an otherwise idle session agent. The timing had been configured to 16 seconds, to speed recovery from prior failures.



```
sip && ip.addr == 2.2.185.2

     Time        Source          Destination     Protocol  Info
  6 2.653159    2.2.185.145     2.2.185.2       SIP       Request: OPTIONS sip:2.2.18
 12 2.769867    2.2.185.2       2.2.185.145     SIP/SDP   Status: 200 OK, with sessic
 26 18.751275   2.2.185.145     2.2.185.2       SIP       Request: OPTIONS sip:2.2.18
 32 18.867941   2.2.185.2       2.2.185.145     SIP/SDP   Status: 200 OK, with sessic
 39 34.849403   2.2.185.145     2.2.185.2       SIP       Request: OPTIONS sip:2.2.18
 45 34.966057   2.2.185.2       2.2.185.145     SIP/SDP   Status: 200 OK, with sessic
 90 50.947503   2.2.185.145     2.2.185.2       SIP       Request: OPTIONS sip:2.2.18
 96 51.064327   2.2.185.2       2.2.185.145     SIP/SDP   Status: 200 OK, with sessic
```

The following Wireshark trace illustrates the Communication Manager behavior when a SIP OPTIONS message is received on a signaling group for which there are no trunk members currently available from the corresponding trunk groups. This condition could exist when the trunk group is maintenance busy, or if all members of the trunk group are in-use for calls. In the trace below, the INVITE in trace 879 is for a call that uses the last available trunk member in trunk group 30. In frame 3222, the Session Director sends SIP OPTIONS to 2.2.85.2, corresponding to signaling group 30. In frame 3252, Communication Manager responds with a 503 Service Unavailable. The SIP OPTIONS and 503 Response are repeated several times. In frame 23699, a call is disconnected, freeing up a trunk group member. The next SIP OPTIONS from the Session Director, in frame 23766, receives a 200 OK response from Communication Manager.



```
Filter: sip && ip.addr == 2.2.85.2

No.   Time        Source       Destination  Protocol  Info
  857 6.862114    2.2.85.2     2.2.85.45    SIP/SDP   Status: 200 OK, with ses
  864 6.880387    2.2.85.45    2.2.85.2     SIP       Request: ACK sip:7328522
  879 6.919143    2.2.85.2     2.2.85.45    SIP       Request: INVITE sip:7328
  887 6.929569    2.2.85.45    2.2.85.2     SIP/SDP   Status: 200 OK, with ses
  895 6.963671    2.2.85.2     2.2.85.45    SIP/SDP   Request: ACK sip:7328522
 3222 18.642860   2.2.85.45    2.2.85.2     SIP       Request: OPTIONS sip:2.2
 3252 18.760298   2.2.85.2     2.2.85.45    SIP       Status: 503 Service Unav
 6452 34.643185   2.2.85.45    2.2.85.2     SIP       Request: OPTIONS sip:2.2
 6478 34.758735   2.2.85.2     2.2.85.45    SIP       Status: 503 Service Unav
12829 66.621673   2.2.85.45    2.2.85.2     SIP       Request: OPTIONS sip:2.2
12839 66.655513   2.2.85.2     2.2.85.45    SIP       Status: 503 Service Unav
23699 123.548997  2.2.85.45    2.2.85.2     SIP       Request: BYE sip:7328522
23715 123.649632  2.2.85.2     2.2.85.45    SIP       Status: 200 OK
23766 139.631246  2.2.85.45    2.2.85.2     SIP       Request: OPTIONS sip:2.2
23771 139.747731  2.2.85.2     2.2.85.45    SIP/SDP   Status: 200 OK, with ses
23821 155.729328  2.2.85.45    2.2.85.2     SIP       Request: OPTIONS sip:2.2
23825 155.845990  2.2.85.2     2.2.85.45    SIP/SDP   Status: 200 OK, with ses
```

Although it was tested to have the Session Director mark the session agent out-of-service upon receipt of a 503, it was deemed unnecessary and potentially sub-optimal to do so. If no Avaya SIP trunk members are available when the Session Director sends an INVITE, Communication Manager will send a 503 response that triggers the Session Director to try another session agent in the session agent group. The call will succeed. If session agents were marked out-of-service in response to the 503, the time to recover the session agent back to in-service could result in calls unnecessarily being redirected. Moreover, the “max-sessions” parameter for the session agent could be used to prevent the Session Director from sending calls when the maximum number of sessions (calls, trunk members) is reached.

6. Test Observations Leading to Product Modification Requests

This section documents observations made during testing that stimulated product modification requests.

Avaya Aura™ Communication Manager Release 5.2 is the first Communication Manager release to include the P-Charging-Vector for outbound SIP trunk calls. A modification request has been entered to change the way that the ICID in the P-Charging-Vector is encoded. Until the modification request is resolved, the Acme Packet Net-Net Session Director configuration can delete the P-Charging-Vector to avoid revealing private side IP Address information to the public network. Section 4.6 documents the relevant configuration. This modification request is targeted for inclusion in Service Pack 1 for Release 5.2.

Section 5.2.4 covers outbound calls made by users at the ESS site, when the system is fragmented, such that the ESS controls the secondary site, and the active S8730 Server controls the primary site. In the sample configuration, PSTN calls from secondary site users are directed to a route pattern that contains “local” secondary site SIP trunks before primary site SIP trunks. Therefore, outbound calls from users at the secondary site will succeed, using the SIP trunks at the secondary site. In an alternate configuration, where calls from secondary site users controlled by the ESS could be directed to route patterns that contain SIP trunks at the primary site before SIP trunks at the secondary site, outbound calls can potentially fail. A modification request was entered, and it is expected that a fix will be available in Service Pack 1 for Release 5.2.

With the generally available Acme Packet Session Director release used for the testing, the Session Director could respond with a SIP 503 to Communication Manager sourced OPTIONS messages after certain types of failures. For example, if the Ethernet connectivity to a C-LAN were removed for a minute, and then re-inserted, Communication Manager would send OPTIONS to the Acme Packet Net-Net 4500 as part of restoring the SIP signaling group. These initial SIP OPTIONS from Communication Manager resulted in a 503 response. Despite the 503, the Session Director did mark the session agent in-service, and could deliver calls to Communication Manager using the restored C-LAN session agent. However, in the absence of incoming call activity, Communication Manager would consider the corresponding trunks “Out-of-service/Far-end” until an OPTIONS exchange sourced by Communication Manager succeeds. This generally occurred in approximately 5-7 minutes. An Acme Packet ticket, 18281, was entered to document the problem. A “workspace” with a fix was also delivered to Avaya for testing, which was tested and did resolve the problem. It is expected that the fix will be delivered to a forthcoming generally available release of the Session Director.

7. Conclusion

As illustrated in these Application Notes, Communication Manager 5.2 can interoperate with Acme Packet Net-Net 4500 to achieve a survivable SIP Trunking solution.

8. Additional References

This section references the documentation relevant to these Application Notes. Avaya product documentation is available at http://support.avaya.com. Acme Packet product documentation is available at http://www.acmepacket.com. A support account may be required to access the Acme Packet documentation.

[JSR] Application Notes for Configuring Direct SIP Trunking from Communication Manager using an Acme Packet Net-Net Session Director and a SIP PSTN Gateway
http://www.avaya.com/master-usa/en-us/resource/assets/applicationnotes/cm4acmesippstn.pdf

The following Application Notes show two independent sites running Communication Manager networked via SIP Trunks to a pair of Acme Packet Net-Net 4500 configured in a High Availability Configuration:
[AC-HA] Application Notes for Configuring Acme Packet Net-Net 4500 Session Director with Direct SIP Trunking to Avaya Communication Manager, Issue 1.0
http://www.avaya.com/master-usa/en-us/resource/assets/applicationnotes/Acme4500CM5DTrk.pdf

[LAR] Sample Configuration for SIP Private Networking and SIP Look-Ahead Routing Using Avaya Communication Manager, Issue 1.0
http://www.avaya.com/master-usa/en-us/resource/assets/applicationnotes/sip-pvt-lar.pdf

[DPT] Configuring Avaya Communication Manager for Dial-Plan Transparency and Inter-Gateway Alternate Routing, Issue 1.1
http://www.avaya.com/master-usa/en-us/resource/assets/applicationnotes/dpt-igar.pdf

[CM1] *Administering Avaya Aura™ Communication Manager*, Document Number 03-300509, Release 5.2, May 2009.
http://support.avaya.com/elmodocs2/comm_mgr/r5.0/03-300509_4.pdf

[CM2] *Avaya Aura™ Communication Manager Feature Description and Implementation,* Document Number 555-245-205, Issue 7, May 2009
http://support.avaya.com/elmodocs2/comm_mgr/R5_2/555_245_205_7.pdf

[CM3] *SIP Support in Avaya Aura™ Communication Manager* Document Number 555-245-206, Issue 9, May 2009
http://support.avaya.com/elmodocs2/comm_mgr/R5_2/555_245_206_9.pdf

[ESS] *Using the Avaya Enterprise Survivable Servers,* Document Number 03-300428, Issue 5, May 2009
http://support.avaya.com/elmodocs2/comm_mgr/R5_2/03_300428_5.pdf

[AP1] *Net-Net 4000 ACLI Configuration Guide* Release S-C6.1.0 January 2009, Document Number 400-0061-61 Rev 1.01

Appendix A: Session Director Configuration File

This Appendix contains the Session Director configuration file for the primary site Acme Packet Net-Net 4500 as a reference. The contents of the configuration file can be shown by using the **show running-config** command.

```
acmesbc-pri# show running-config
access-control
            realm-id             OUTSIDE
            description
            source-address           10.3.3.40
            destination-address       0.0.0.0
            application-protocol      SIP
            transport-protocol        UDP
            access                   permit
            average-rate-limit        0
            trust-level              medium
            minimum-reserved-bandwidth     0
            invalid-signal-threshold  1
            maximum-signal-threshold     15000
            untrusted-signal-threshold  4
            nat-trust-threshold     0
            deny-period            30
            last-modified-by        admin@console
            last-modified-date       2009-04-13 15:13:04
local-policy
            from-address
                              *
            to-address
                              *
            source-realm
                              INSIDE
            description
            activate-time          N/A
            deactivate-time         N/A
            state               enabled
            policy-priority        none
            last-modified-by        admin@console
            last-modified-date       2009-04-13 15:14:29
            policy-attribute
                                     next-hop              SAG:SERV_PROVIDER
                                     realm               OUTSIDE
                                     action              none
                                     terminate-recursion      disabled
                                     carrier
                                     start-time           0000
                                     end-time              2400
                                     days-of-week            U-S
                                     cost               0
                                     app-protocol           SIP
                                     state              enabled
                                     methods
                                     media-profiles
local-policy
            from-address
```

```
                              *
          to-address
                              *
          source-realm
                              OUTSIDE
          description
          activate-time                N/A
          deactivate-time              N/A
          state                   enabled
          policy-priority              none
          last-modified-by             admin@console
          last-modified-date           2009-04-13 15:14:47
          policy-attribute
                                        next-hop                      SAG:ENTERPRISE
                                        realm                         INSIDE
                                        action                        none
                                        terminate-recursion           disabled
                                        carrier
                                        start-time                    0000
                                        end-time                      2400
                                        days-of-week                  U-S
                                        cost                          0
                                        app-protocol                  SIP
                                        state                         enabled
                                        methods
                                        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
          red-flow-port                1985
          red-mgcp-port                1986
          red-max-trans                10000
          red-sync-start-time          5000
          red-sync-comp-time           1000
          media-policing               enabled
          max-signaling-bandwidth      775880
          max-untrusted-signaling      5
          min-untrusted-signaling      4
          app-signaling-bandwidth      0
          tolerance-window             30
          rtcp-rate-limit              0
          min-media-allocation         32000
          min-trusted-allocation       60000
          deny-allocation              32000
          anonymous-sdp                disabled
```

```
             arp-msg-bandwidth              32000
             fragment-msg-bandwidth           0
             rfc2833-timestamp              disabled
             default-2833-duration          100
             rfc2833-end-pkts-only-for-non-sig enabled
             translate-non-rfc2833-event    disabled
             dnsalg-server-failover         disabled
             last-modified-by               admin@console
             last-modified-date             2009-04-13 15:09:35
network-interface
             name                         wancom1
             sub-port-id                    0
             description
             hostname
             ip-address
             pri-utility-addr               169.254.1.1
             sec-utility-addr               169.254.1.2
             netmask                      255.255.255.252
             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
             ftp-address
     icmp-address
             snmp-address
             telnet-address
             last-modified-by               admin@console
             last-modified-date             2009-04-13 15:08:33
network-interface
             name                         wancom2
             sub-port-id                    0
             description
             hostname
             ip-address
             pri-utility-addr               169.254.2.1
             sec-utility-addr               169.254.2.2
             netmask                      255.255.255.252
             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
            ftp-address
    icmp-address
            snmp-address
            telnet-address
            last-modified-by              admin@console
            last-modified-date            2009-04-13 15:08:50
network-interface
            name                      s0p0
            sub-port-id                 0
            description
            hostname
            ip-address                 10.3.3.45
            pri-utility-addr            10.3.3.46
            sec-utility-addr            10.3.3.47
            netmask                    255.255.255.0
            gateway                    10.3.3.1
            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
            ftp-address
    icmp-address
            snmp-address
            telnet-address
            last-modified-by              admin@console
            last-modified-date            2009-04-13 15:10:34
network-interface
            name                      s1p0
            sub-port-id                 0
            description
            hostname
            ip-address                 2.2.85.45
            pri-utility-addr            2.2.85.46
            sec-utility-addr            2.2.85.47
            netmask                    255.255.255.0
            gateway                    2.2.85.1
            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
            ftp-address
    icmp-address
            snmp-address
            telnet-address
            last-modified-by          admin@console
            last-modified-date        2009-04-13 15:11:38
phy-interface
            name                  s0p0
            operation-type            Media
            port                 0
            slot                 0
            virtual-mac             00:08:25:A0:E2:28
            admin-state             enabled
            auto-negotiation          enabled
            duplex-mode               FULL
            speed                 100
            last-modified-by          admin@console
            last-modified-date        2009-04-13 15:07:37
phy-interface
            name                  s0p1
            operation-type            Media
            port                 1
            slot                 0
            virtual-mac             00:08:25:A0:E2:29
            admin-state             disabled
            auto-negotiation          enabled
            duplex-mode               FULL
            speed                 100
            last-modified-by          admin@console
            last-modified-date        2009-04-13 15:07:54
phy-interface
            name                  s1p0
            operation-type            Media
            port                 0
            slot                 1
            virtual-mac             00:08:25:A0:E2:2e
            admin-state             enabled
            auto-negotiation          enabled
            duplex-mode               FULL
            speed                 100
            last-modified-by          admin@console
            last-modified-date        2009-04-13 15:08:05
phy-interface
            name                  s1p1
            operation-type            Media
            port                 1
```

```
                slot                    1
                virtual-mac                  00:08:25:A0:E2:2f
                admin-state                  disabled
                auto-negotiation               enabled
                duplex-mode                    FULL
                speed                      100
                last-modified-by               admin@console
                last-modified-date             2009-04-13 15:08:15
phy-interface
                name                       wancom1
                operation-type                 Control
                port                     1
                slot                    0
                virtual-mac
                wancom-health-score             8
                last-modified-by               admin@console
                last-modified-date             2009-04-13 15:08:23
phy-interface
                name                       wancom2
                operation-type                 Control
                port                     2
                slot                    0
                virtual-mac
                wancom-health-score             9
                last-modified-by               admin@console
                last-modified-date             2009-04-13 15:08:41
realm-config
                identifier                 OUTSIDE
                description
                addr-prefix                  0.0.0.0
                network-interfaces
                                      s0p0:0
                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
                fallback-bandwidth              0
                max-priority-bandwidth            0
                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
                manipulation-string
```

```
        class-profile
        average-rate-limit            0
        access-control-trust-level     medium
        invalid-signal-threshold       1
        maximum-signal-threshold       1
        untrusted-signal-threshold     1
        nat-trust-threshold           0
        deny-period                  60
        ext-policy-svr
        symmetric-latching            disabled
        pai-strip                    disabled
        trunk-context
        early-media-allow
        enforcement-profile
        additional-prefixes
        restricted-latching           none
        restriction-mask              32
        accounting-enable             enabled
        user-cac-mode                 none
        user-cac-bandwidth            0
        user-cac-sessions             0
        icmp-detect-multiplier        0
        icmp-advertisement-interval    0
        icmp-target-ip
        monthly-minutes               0
        net-management-control        disabled
        delay-media-update            disabled
        refer-call-transfer           disabled
        codec-policy
        codec-manip-in-realm          disabled
        constraint-name
        call-recording-server-id
        stun-enable                  disabled
        stun-server-ip               0.0.0.0
        stun-server-port              3478
        stun-changed-ip               0.0.0.0
        stun-changed-port             3479
        match-media-profiles
        qos-constraint
        last-modified-by              admin@console
        last-modified-date            2009-04-13 15:10:52
realm-config
        identifier                   INSIDE
        description
        addr-prefix                  0.0.0.0
        network-interfaces
                                    s1p0:0
        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
fallback-bandwidth             0
max-priority-bandwidth         0
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
manipulation-string
class-profile
average-rate-limit             0
access-control-trust-level     high
invalid-signal-threshold       0
maximum-signal-threshold       0
untrusted-signal-threshold     0
nat-trust-threshold            0
deny-period                    30
ext-policy-svr
symmetric-latching             disabled
pai-strip                      disabled
trunk-context
early-media-allow
enforcement-profile
additional-prefixes
restricted-latching            none
restriction-mask               32
accounting-enable              enabled
user-cac-mode                  none
user-cac-bandwidth             0
user-cac-sessions              0
icmp-detect-multiplier         0
icmp-advertisement-interval    0
icmp-target-ip
monthly-minutes                0
net-management-control         disabled
delay-media-update             disabled
refer-call-transfer            disabled
codec-policy
codec-manip-in-realm           disabled
constraint-name
call-recording-server-id
stun-enable                    disabled
stun-server-ip                 0.0.0.0
stun-server-port               3478
stun-changed-ip                0.0.0.0
stun-changed-port              3479
match-media-profiles
qos-constraint
last-modified-by               admin@console
```

```
        last-modified-date          2009-04-13 15:11:51
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
        media-if-peercheck-time     0
        peer
                        name                    acmesbc-pri
                        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
        peer
                        name                    acmesbc-sec
                        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
        last-modified-by            admin@console
        last-modified-date          2009-04-13 15:09:08
session-agent
        hostname                    10.3.3.40
        ip-address                  10.3.3.40
        port                        5060
        state                       enabled
        app-protocol                SIP
        app-type
        transport-method            UDP
        realm-id                    OUTSIDE
        egress-realm-id
        description                 Service Provider Proxy
        carriers
```

```
allow-next-hop-lp              enabled
constraints                    disabled
max-sessions                   0
max-inbound-sessions           0
max-outbound-sessions          0
max-burst-rate                 0
max-inbound-burst-rate         0
max-outbound-burst-rate        0
max-sustain-rate               0
max-inbound-sustain-rate       0
max-outbound-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                  16
ping-send-mode                 keep-alive
ping-in-service-response-codes
out-service-response-codes
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
manipulation-string
p-asserted-id
trunk-group
max-register-sustain-rate      0
early-media-allow
invalidate-registrations       disabled
rfc2833-mode                   none
rfc2833-payload                0
codec-policy
enforcement-profile
refer-call-transfer            disabled
reuse-connections              NONE
tcp-keepalive                  none
tcp-reconn-interval            0
```

```
        max-register-burst-rate     0
        register-burst-window        0
        last-modified-by          admin@2.2.4.150
        last-modified-date         2009-04-23 15:38:48
session-agent
        hostname                2.2.85.2
        ip-address             2.2.85.2
        port                 5060
        state                enabled
        app-protocol             SIP
        app-type
        transport-method           StaticTCP
        realm-id               INSIDE
        egress-realm-id
        description             Primary Site C-LAN 2A02
        carriers
        allow-next-hop-lp          enabled
        constraints            disabled
        max-sessions             0
        max-inbound-sessions         0
        max-outbound-sessions         0
        max-burst-rate           0
        max-inbound-burst-rate       0
        max-outbound-burst-rate       0
        max-sustain-rate          0
        max-inbound-sustain-rate      0
        max-outbound-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           16
        ping-send-mode             keep-alive
        ping-in-service-response-codes
        out-service-response-codes
        options               trans-timeouts=1
        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
        manipulation-string
        p-asserted-id
        trunk-group
        max-register-sustain-rate     0
        early-media-allow
        invalidate-registrations      disabled
        rfc2833-mode                  none
        rfc2833-payload               0
        codec-policy
        enforcement-profile
        refer-call-transfer           disabled
        reuse-connections             TCP
        tcp-keepalive                 enabled
        tcp-reconn-interval           10
        max-register-burst-rate       0
        register-burst-window         0
        last-modified-by              admin@2.2.4.150
        last-modified-date            2009-04-23 15:38:57
session-agent
        hostname                      2.2.85.20
        ip-address                    2.2.85.20
        port                          5060
        state                         enabled
        app-protocol                  SIP
        app-type
        transport-method              StaticTCP
        realm-id                      INSIDE
        egress-realm-id
        description                   Primary Site C-LAN 2B02
        carriers
        allow-next-hop-lp             enabled
        constraints                   disabled
        max-sessions                  0
        max-inbound-sessions          0
        max-outbound-sessions         0
        max-burst-rate                0
        max-inbound-burst-rate        0
        max-outbound-burst-rate       0
        max-sustain-rate              0
        max-inbound-sustain-rate      0
        max-outbound-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                 16
        ping-send-mode                keep-alive
        ping-in-service-response-codes
        out-service-response-codes
        options                       trans-timeouts=1
        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
        manipulation-string
        p-asserted-id
        trunk-group
        max-register-sustain-rate     0
        early-media-allow
        invalidate-registrations      disabled
        rfc2833-mode                  none
        rfc2833-payload               0
        codec-policy
        enforcement-profile
        refer-call-transfer           disabled
        reuse-connections             TCP
        tcp-keepalive                 enabled
        tcp-reconn-interval           10
        max-register-burst-rate       0
        register-burst-window         0
        last-modified-by              admin@2.2.4.150
        last-modified-date            2009-04-23 15:39:03
session-group
        group-name                    SERV_PROVIDER
        description
        state                         enabled
        app-protocol                  SIP
        strategy                      Hunt
        dest
                                      10.3.3.40
        trunk-group
        sag-recursion                 disabled
        stop-sag-recurse              401,407
        last-modified-by              admin@console
        last-modified-date            2009-04-13 15:13:19
session-group
        group-name                    ENTERPRISE
        description
        state                         enabled
        app-protocol                   SIP
        strategy                       RoundRobin
        dest
                                  2.2.85.2
                                  2.2.85.20
        trunk-group
        sag-recursion                  enabled
        stop-sag-recurse               401,407
        last-modified-by               admin@2.2.4.150
        last-modified-date             2009-04-14 12:58:18
sip-config
        state                          enabled
        operation-mode                 dialog
        dialog-transparency            enabled
        home-realm-id                  INSIDE
        egress-realm-id                INSIDE
        nat-mode                       None
        registrar-domain
        registrar-host
        registrar-port                 0
        register-service-route         always
        init-timer                     500
        max-timer                      4000
        trans-expire                   32
        invite-expire                  180
        inactive-dynamic-conn          32
        enforcement-profile
        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             enabled
        registration-cache-limit       0
        register-use-to-for-lp         disabled
        options                        max-udp-length=0
                   set-inv-exp-at-100-resp
        add-ucid-header                disabled
        last-modified-by               admin@console
        last-modified-date             2009-04-13 15:09:49
sip-interface
        state                          enabled
        realm-id                       OUTSIDE
        description
        sip-port
```

```
                        address                 10.3.3.45
                        port                    5060
                        transport-protocol      UDP
                        tls-profile
                        allow-anonymous         agents-only
                        ims-aka-profile
        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
        manipulation-string
        sip-ims-feature                 disabled
        operator-identifier
        anonymous-priority              none
        max-incoming-conns              0
        per-src-ip-max-incoming-conns  0
        inactive-conn-timeout           0
        untrusted-conn-timeout          0
        network-id
        ext-policy-server
        default-location-string
        charging-vector-mode            none
        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
```

```
            ims-aka-feature              disabled
            enforcement-profile
            refer-call-transfer          disabled
            route-unauthorized-calls
            tcp-keepalive                none
            add-sdp-invite               disabled
            add-sdp-profiles
            last-modified-by             admin@2.2.4.150
            last-modified-date           2009-04-22 14:51:13
sip-interface
            state                        enabled
            realm-id                     INSIDE
            description
            sip-port
                        address                        2.2.85.45
                        port                           5060
                        transport-protocol             TCP
                        tls-profile
                        allow-anonymous                agents-only
                        ims-aka-profile
            carriers
            trans-expire                 6
            invite-expire                180
            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
            manipulation-string
            sip-ims-feature              disabled
            operator-identifier
            anonymous-priority           none
            max-incoming-conns           0
            per-src-ip-max-incoming-conns  0
            inactive-conn-timeout        0
            untrusted-conn-timeout       0
            network-id
            ext-policy-server
            default-location-string
            charging-vector-mode          delete
            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
            ims-aka-feature              disabled
            enforcement-profile
            refer-call-transfer          disabled
            route-unauthorized-calls
            tcp-keepalive                none
            add-sdp-invite               disabled
            add-sdp-profiles
            last-modified-by             admin@2.2.1.10
            last-modified-date           2009-04-20 15:23:45
sip-manipulation
            name                         NAT_IP
            description                    Topology hiding for SIP headers
            header-rule
                                    name                        manipFrom
                                    header-name                    From
                                    action                      manipulate
                                    comparison-type                case-sensitive
                                    match-value
                                    msg-type                      request
                                    new-value
                                    methods
                                    element-rule
                                        name                        FROM
                                        parameter-name
                                        type                        uri-host
                                        action                       replace
                                        match-val-type                  ip
                                        comparison-type                 case-sensitive
                                        match-value
                                        new-value                      $LOCAL_IP
            header-rule
                                    name                        manipTo
                                    header-name                    To
                                    action                      manipulate
                                    comparison-type                case-sensitive
                                    match-value
                                    msg-type                      request
                                    new-value
                                    methods
                                    element-rule
                                        name                        TO
```

```
                           parameter-name
                           type              uri-host
                           action             replace
                           match-val-type         ip
                           comparison-type         case-sensitive
                           match-value
                           new-value            $REMOTE_IP
header-rule
                       name                manipRpid
                       header-name            Remote-Party-ID
                       action             manipulate
                       comparison-type         case-sensitive
                       match-value
                       msg-type              request
                       new-value
                       methods
                       element-rule
                           name              RPID
                           parameter-name
                           type              uri-host
                           action             replace
                           match-val-type         ip
                           comparison-type         case-sensitive
                           match-value
                           new-value            $LOCAL_IP
header-rule
                       name                manipHistInfo
                       header-name            History-Info
                       action             manipulate
                       comparison-type         case-sensitive
                       match-value
                       msg-type              request
                       new-value
                       methods
                       element-rule
                           name              HISTORYINFO
                           parameter-name
                           type              uri-host
                           action             replace
                           match-val-type         ip
                           comparison-type         case-sensitive
                           match-value
                           new-value            $REMOTE_IP
header-rule
                       name                storeAlertInfo
                       header-name            Alert-Info
                       action             store
                       comparison-type         pattern-rule
                       match-value            (.+@)([0-9.]+)(.+)
                       msg-type              request
                       new-value
                       methods
header-rule
                       name                manipAlertInfo
                       header-name            Alert-Info
```

```
                                        action                  manipulate
                                        comparison-type              boolean
                                        match-value                $storeAlertInfo
                                        msg-type                   request
                                        new-value
$storeAlertInfo.$1+$REMOTE_IP+$storeAlertInfo.$3
                                        methods
            last-modified-by            admin@2.2.4.150
            last-modified-date          2009-04-13 16:42:52
steering-pool
            ip-address                  10.3.3.45
            start-port                  49152
            end-port                    65535
            realm-id                    OUTSIDE
            network-interface
            last-modified-by            admin@console
            last-modified-date          2009-04-13 15:11:26
steering-pool
            ip-address                  2.2.85.45
            start-port                  49152
            end-port                    65535
            realm-id                    INSIDE
            network-interface
            last-modified-by            admin@console
            last-modified-date          2009-04-13 15:12:25
system-config
            hostname                    acmesbc
            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
            collect
                                        sample-interval            5
                                        push-interval              15
                                        boot-state                 disabled
                                        start-time                 now
                                        end-time                   never
                                        red-collect-state          disabled
                                        red-max-trans              1000
                                        red-sync-start-time        5000
                                        red-sync-comp-time         1000
                                        push-success-trap-state    disabled
            call-trace                  disabled
            internal-trace               disabled
            log-filter                   all
            default-gateway              2.2.4.1
            restart                      enabled
            exceptions
            telnet-timeout               0
            console-timeout              0
            remote-control               enabled
            cli-audit-trail              enabled
            link-redundancy-state        disabled
            source-routing               enabled
            cli-more                     disabled
            terminal-height              24
            debug-timeout                0
            trap-event-lifetime          0
            last-modified-by             admin@console
            last-modified-date           2009-04-13 15:06:34
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 Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com.