Avaya Solution & Interoperability Test Lab

Configuring Avaya Communication Manager using Avaya G250 Media Gateway with Inter-Gateway Alternate Routing and Call Administration Control-Bandwidth Limit Features - Issue 1.0

Abstract

These Application Notes present a sample configuration of the Avaya Inter-Gateway Alternate Routing (IGAR) feature with Call Administration Control – Bandwidth Limit (CAC-BL) for Avaya S8500 Media Server and Avaya G650 Media Gateway in a main office controlling an Avaya G250-BRI Media Gateway in a small office. Under normal operation, a primary IP link is used for communication between two offices. If the primary link is out of service, a VPN tunnel across the Internet can be used as a backup. The number of supported VoIP calls is based on which IP connection is used. Detailed VPN configuration between the Avaya G250-BRI Media Gateway (with a dynamic IP address) and a Cisco PIX is covered. A Cisco 3745 Voice Gateway is used to simulate access to PSTN. Detailed ISDN BRI configuration between the Cisco 3745 Voice Gateway and the Avaya G250-BRI is also covered. Quality of Service (QoS) is not covered in these Application Notes, but standard QoS design practices should be applied.

1. Introduction

The network diagram in **Figure 1** shows two offices. The office labeled "Main Office" uses an Avaya S8500 Media Server and an Avaya G650 Media Gateway. The office labeled "Small Office" contains an Avaya G250-BRI Media Gateway .

Under normal operation, the Main and Small Offices communicate through a primary link between the Cisco 3745 access router and the Avaya G250-BRI Media Gateway. If the primary link is out of service, a VPN tunnel across the Internet between the Avaya G250-BRI Media Gateway and the Cisco PIX can be used as a backup. The access to the Internet from the Avaya G250-BRI is a Cable modem. This interface can be connected directly to the Cable modem or via a Cable Modem Router. The Cable Modem Router functions as a DHCP server and a Network Address Translation (NAT) device for the Avaya G250-BRI Media Gateway.

The Avaya Inter-Gateway Alternate Routing (IGAR) feature provides a means of alternately using PSTN facilities when the IP link is incapable of carrying the bearer connection. The number of calls allowed on the IP link is determined by the value of the Call Administration Control – Bandwidth Limit (CAC-BL) reported from the Avaya G250-BRI Media Gateway and the IP Codec used between the Main and the Small Offices. If the primary link is up, the Avaya G250-BRI Media Gateway will report the CAC-BL configured on the primary link. If the primary link is out of service, the Avaya G250-BRI Media Gateway will report the CAC-BL configured on the backup link. The maximum number of VoIP calls can be dynamically changed based on which IP connection is used.

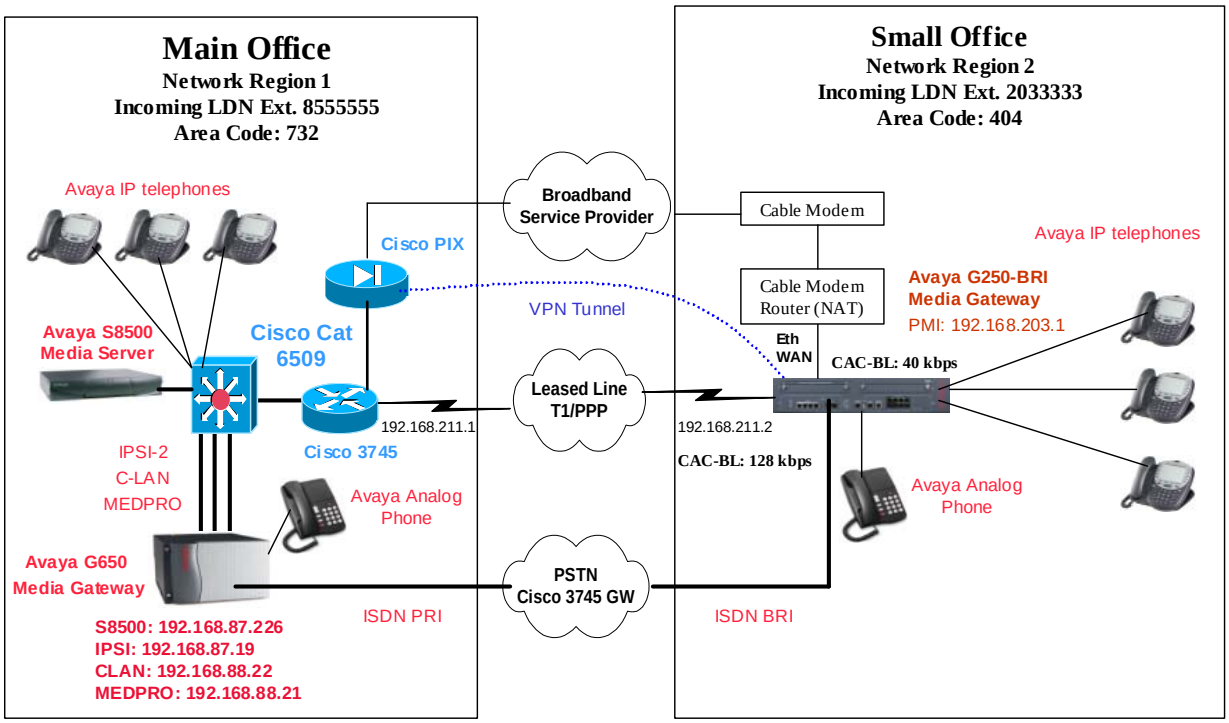

Figure 1: IGAR Configuration with Dynamic CAC-BL

2. Equipment and Software Validated

Table 1 below shows the versions verified in these Application Notes.

Equipment	Software
Avaya Communication Manager Avaya S8500 Media Server Avaya S8300 Media Server (LSP)	 3.0 (load 337.0) 3.0 (load 337.0)
Avaya G650 Media Gateway IPSI (TN2312AP) C-LAN (TN799DP) MEDPRO (TN2302AP)	 HW03 FW012 HW01 FW012 HW15 FW102
Avaya G250-BRI Media Gateway	24.11.1
Avaya 4600 Series IP Telephones	2.1.3
Cisco 3745 Access Router/Voice Gateway	12.3(11)T3
Cisco 3745 Voice Gateway	12.3(11)T3
Cisco Catalyst 6509 Switch Layer 2 Layer 3	 8.3(4) 12.1(13)E6
Cisco PIX 525	6.3(4)

Table 1: Software Versions

3. Configurations

Avaya IGAR is a single-server feature that provides an alternate bearer path between Port Networks (PNs) or Gateways (GWs). In order to keep a single-server system, the IP connection must exist between the Avaya Media Server and Avaya PNs/GWs. The Avaya G250-BRI Media Gateway will register with the Avaya S8300 LSP when there is no IP connection between the Main and Small Offices.

The Avaya IGAR feature preserves the internal makeup of a call between a pair of PNs or GWs in separate network regions even if the voice bearer portion of the call is rerouted over alternate PSTN facilities. One unique DID number (also known as an Listed Directory Number or LDN) per network region is all that is required to successfully terminate to the IGAR extension for that particular network region.

Section 3.2 only shows the Avaya G250-BRI Media Gateway and IGAR related configuration. Refer to reference [1] for details on how to configure Avaya S8500 Media Server to control the Avaya G650 Media Gateway and the Avaya S8300 LSP.

3.1. Configure Avaya G250-BRI Media Gateway

3.1.1. Configure Avaya G250-BRI Media Gateway – Data Switching

The following screen shows VLAN configurations of VLAN 202 and 203. VLAN 203 is configured as the Primary Management Interface (PMI). The G250-BRI Media Gateway will use the PMI to register to the Media Gateway Controllers (MGC).

```
interface Vlan 202
 ip address 192.168.202.1   255.255.255.0
 exit
!
interface Vlan 203
 icc-vlan
 ip address 192.168.203.1   255.255.255.0
 pmi
 exit
```

In the following screen, the Ethernet WAN (FastEthernet 10/2) port is connected to the Cable modem Router and is configured as a DHCP client. A MM340 T1/E1 data module is used on the G250-BRI Media Gateway as a primary link to the Main Office. The module is configured as T1 by default. Channel group 1 is configured with 24 channels. The corresponding serial interface 2/1:1 is configured to PPP encapsulation.

```
interface FastEthernet 10/2
 ip address dhcp
 exit

ds-mode t1

controller t1 2/1
 linecode b8zs
 framing esf
 channel-group 1 timeslots 1-24 speed 64
 exit
!
interface Serial 2/1:1
 encapsulation ppp
 ip address 192.168.211.2   255.255.255.0
 exit
```

The following shows the IP routing configuration. As shown, OSPF is used on the primary link and a default route can be obtained through the Ethernet WAN port (obtained from the DHCP server). If the primary link is out of service, the routing entries learned from OSPF will be gone and the default route will be used.

```
router ospf
 network 192.168.202.0   0.0.0.255       area 0.0.0.0
 network 192.168.203.0   0.0.0.255       area 0.0.0.0
 network 192.168.211.0   0.0.0.255       area 0.0.0.0
 exit
```

The Avaya G250-BRI Media Gateway can be configured to be a DHCP and TFTP server for Avaya IP telephones. Refer to reference [2] for detailed configuration.

3.1.2. Configure Avaya G250-BRI Media Gateway – Media Gateway

The CAC-BL can be statically configured on an interface with a priority. Based on the following configuration, the CAC-BL is configured to 128 kbps with priority 255 (the highest priority) on the primary link. The CAC-BL is configured to 40 kbps on the backup link with the default priority 128. If both links are up, the G250-BRI Media Gateway will report the CAC-BL with a higher priority, which is 128 kbps configured on the serial interface. If the primary link is out of service, the CAC-BL 40 kbps configured on FastEthernet 10/2 will be reported.

The number of VoIP calls supported is based on the reported CAC-BL and the Codec being used between a network region pair. Avaya Communication Manager will count 27 kbps for each G.729 call and 85 kbps for each G.711 call. In the sample configuration, the G.729 Codec is configured between the Main and Small Offices. Therefore, four calls will be supported on the primary link and one call on the backup link. If no VoIP calls are desired on the backup line.

```
interface FastEthernet 10/2
 dynamic-cac 40
 ip address dhcp
 exit

interface Serial 2/1:1
 encapsulation ppp
 dynamic-cac 128 255
 ip address 192.168.211.2   255.255.255.0
```

The following shows the MGC list configuration. The IP address 192.168.88.22 is the C-LAN IP address of the Avaya G650 Media Gateway, and 192.168.203.3 is the IP address of the Avaya S8300 Media Server LSP installed in the Avaya G250-BRI Media Gateway. If there is no IP connection between the Main and Small Offices, the Avaya G250-BRI Media Gateway will register with the S8300 Media Server LSP.

```
set mgc list 192.168.88.22,192.168.203.3
```

3.1.3. Configure Avaya G250-BRI Media Gateway – VPN

The Avaya G250-BRI Media Gateway is also a VPN appliance. The following shows the ISAKMP policy configuration. The configuration of the Cisco PIX and Avaya G250-BRI Media Gateway must match for the IKE phase 1 proposal.

```
crypto isakmp policy 1
 description "High Phase 1 Proposal"
 encryption aes
 hash sha
 group 1
 authentication pre-share
```

The following screen configures ISAKMP peer configuration with the Cisco PIX. The Avaya G250-BRI Media Gateway is configured with the IP address of the Cisco PIX. The Avaya G250 Media Gateway must be configured to initiate the IKE connection (aggressive mode) since the Cisco PIX does not know the dynamic IP address of the Avaya G250 Media Gateway. The Avaya G250-BRI Media Gateway supports standard VPN Dead Peer Detection (DPD) keepalives. The command **keepalive 10 retry 2 on-demand** is used to configure the DPD keepalives. With the **on-demand** approach, the G250-BRI Media Gateway never sends a DPD message if it has no traffic to send. If the Avaya G250-BRI Media Gateway has to send outbound traffic and the peer status is questionable, the G250-BRI Media Gateway will send a DPD message to query the status of the peer. In the example, the G250-BRI Media Gateway will send a DPD keep alive message every 10 seconds, and to retry every two seconds if the DPD messages fail.

```
crypto isakmp peer address 12.160.179.124
 pre-shared-key ****
 isakmp-policy 1
 initiate mode aggressive
 keepalive 10 retry 2 on-demand
```

The following screen creates an IPSec Phase 2 transform-set proposal. Perfect Forward Secrecy (PFS) is enabled to strengthen the tunnel against brute force attacks.

```
crypto ipsec transform-set H2 esp-aes esp-sha-hmac
 set pfs group2
```

The following screen assigns an IPSec phase 2 proposal to the Cisco PIX via crypto map:

```
crypto map 1
 description "Phase 2 Proposal"
 set peer 12.160.179.124
 set transform-set H2
```

The following screen configures a crypto-list 901 to define the VPN traffic between the Avaya G250-BRI Media Gateway and Cisco PIX. The source IP address 192.168.202.0 with a wild card 0.0.1.255 defines networks 192.168.202.0/24 and 192.168.203.0/24. The destination IP 192.168.80.0 with a wild card 0.0.15.255 defines networks 192.168.80.0/24 to 192.168.95.0/24. Several pairs of source and destination IP networks can be defined with the same or different remote VPN peers (protect crypto map).

```
ip crypto-list 901
 name "To-Cisco-PIX"
 local-address FastEthernet 10/2
!
 ip-rule 1
  protect crypto map 1
  source-ip 192.168.202.0 0.0.1.255
  destination-ip 192.168.80.0 0.0.15.255
```

Apply an IP crypto-list to the public facing interface, which is FastEthernet 10/2 in the sample:

```
interface FastEthernet 10/2
 dynamic-cac 40
 ip crypto-group 901
 ip address dhcp
```

In the sample configuration, the Avaya G250-BRI Media Gateway is connected to the Cable modem router. The Cable modem router functions as a port network address translation device. NAT causes compatibility problems for many types of applications including VPN. The NAT problem can be resolved by using the NAT-T feature. The NAT-T feature is used to detect the presence of a local NAT device. Once detected, the two peers tunnel IKE and IPSec through a UDP port, allowing the NAT device to work seamlessly with VPN. The standard UDP port is 4500. NAT-T and NAT-T keepalive are enabled by default on the Avaya G250.

Use the command **crypto ipsec nat-transparency udp-encapsulation** to enable the NAT-T. Use the command **crypto isakmp nat keepalive** to enable NAT-T keepalive and configure the keepalive interval.

```
G250-BRI-001(super)# crypto ipsec nat-transparency udp-encapsulation
Done!

G250-BRI-001(super)# crypto isakmp nat keepalive 20
Done!
```

3.2. Configure Avaya Communication Manager

3.2.1. Configure Avaya Communication Manager controlling G250-BRI Media Gateway

In order to add the Avaya G250-BRI Media Gateway to Avaya Communication Manager, the serial number of the Avaya G250-BRI Media Gateway must be known. Use **show system** on the Avaya G250-BRI Media Gateway to obtain the serial number.

```
G250-BRI-001(super)# show system
…
Serial No           : 04IS52658365
Model No            : G250-BRI
HW Vintage          : 3
HW Suffix           : A
FW Vintage          : 24.11.1
```

Use the command **add media-gateway** to add the Avaya G250-BRI Media Gateway with the following parameters (the G250-BRI Media Gateway is configured to Network Region 2):

Type: g250-bri
Serial No: 04IS52658365
Network Region: 2

Use the command **change media-gateway** to verify the registration status. The following output shows that the Avaya G250-BRI Media Gateway registers with the Avaya S8500 Media Server through the controller IP address 192.168.88.22, which is the C-LAN IP address of the Avaya G650 Media Gateway. As seen, the G250-BRI Media Gateway registers to the controller using its PMI IP address (192.168.203.1).

```
change media-gateway 1                                      Page   1 of   1
                            MEDIA GATEWAY
        Number: 1                                IP Address: 192.168.203.1
          Type: g250-bri           FW Version/HW Vintage: 24 .11 .1  /0
          Name: G250-BRI                      MAC Address: 00:04:0d:6d:33:21
     Serial No: 04IS52658365                 Encrypt Link? y
 Network Region: 2                              Location: 1
     Registered? y                  Controller IP Address: 192.168.88 .22
  Recovery Rule: 1                               Site Data:
      Slot   Module Type              Name
       V1:   S8300                   ICC MM
       V2:
       V3:   1T+2L Integ Analog      ANA IMM
       V4:   2 Port Integ BRI        BRI IMM

       V9:
 Max Survivable IP Ext: 8
```

3.2.2. Controlling Intra-Office and Inter-Office VoIP Behavior on Avaya Communication Manager

In this sample configuration, IP Network Region 1 is configured for the Main Office and IP Network Region 2 is configured for the Small Office. IP codec-set 1 is configured to G.711MU for intra-office calls in the LAN while IP codec-set 2 is configured G.729B for inter-office calls to conserve bandwidth over the WAN.

In the sample configuration, the C-LAN and the Media Processor of the Avaya G650 Media Gateway are configured to Network Region 1 by the command **change ip-interface <board#>**. The Avaya G250-BRI Media Gateway is configured to Network Region 2 in Section 3.2.1. The following screen configures the Avaya G650 to Network Region 1. By configuring the Avaya G650 Media Gateway to Network Region 1, all the non-IP boards (for example, trunk circuit packs) will belong to Network Region 1.

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


                 Location: 1         IP Network Region: 1

 Rack:               Room:              Floor:             Building:
```

Use the command **change ip-network-map** to configure the IP endpoints to a network region based on their source IP address. As shown, The IP endpoints in the Main Office are configured to Network Region 1 and the IP endpoints in the Small Office are configured to Network Region 2.

```
change ip-network-map                                          Page   1 of  3
                         IP ADDRESS MAPPING

                                                                Emergency
                                      Subnet                    Location
 From IP Address  (To IP Address   or Mask)  Region    VLAN    Extension
 192.168.88 .0    192.168.88 .255     24       1        88
 192.168.89 .0    192.168.89 .255     24       1        89
 192.168.202.0    192.168.202.255     24       2        202
 192.168.203.0    192.168.203.255     24       2        203
```

The following screen shows ip-codec-set 1 and 2 configurations:

```
change ip-codec-set 1                                          Page   1 of   2
                         IP Codec Set
    Codec Set: 1

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

     Media Encryption
 1: none
```

```
change ip-codec-set 2                                          Page   1 of   2
                         IP Codec Set
    Codec Set: 2

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.729B            n          2        20

     Media Encryption
 1: none
```

3.2.3. Configure PSTN Trunks for the Avaya G650 and G250-BRI Media Gateways

Refer to reference [3] on how to configure ISDN T1/PRI between Avaya Communication Manager and the Cisco Voice Gateways. The following screen shows the T1/PRI layer 1 configuration.

```
Display ds1 01A13                                              Page   1 of   2
                              DS1 CIRCUIT PACK

           Location: 01A13                          Name: To-cisco
           Bit Rate: 1.544                  Line Coding: b8zs
   Line Compensation: 1                    Framing Mode: esf
      Signaling Mode: isdn-pri
             Connect: pbx
   TN-C7 Long Timers? n                  Country Protocol: 1
Interworking Message: PROGress           Protocol Version: a
Interface Companding: mulaw                         CRC? n
          Idle Code: 11111111
                           DCP/Analog Bearer Capability: 3.1kHz

                                        T303 Timer(sec): 4

      Slip Detection? n                Near-end CSU Type: other
                         Alarm When PRI Endpoint Detached? y
```

The following shows **signaling-group** configuration:

```
display signaling-group 10                                    Page   1 of   5
                                SIGNALING GROUP
 Group Number: 10             Group Type: isdn-pri
                     Associated Signaling? y          Max number of NCA TSC: 0
                        Primary D-Channel: 01A1324     Max number of CA TSC: 0
                                                     Trunk Group for NCA TSC:
       Trunk Group for Channel Selection: 10
          Supplementary Service Protocol: a
```

Use the command **add bri-trunk-board <Board #>** to add the BRI board on the Avaya G250-BRI Media Gateway. Note that **TEI** must configured to **0** to work with the Cisco 3745 Voice Gateway. **Interface Companding** must be configured to **mu-law** to match the default Cisco Voice Gateway configuration.

```
add bri-trunk-board 01v4                                      Page   1 of   2
                          ISDN-BRI TRUNK CIRCUIT PACK

               Location: 001V4                              Name:
   Interface Companding: mu-law    DCP/Analog Bearer Capability: 3.1kHz
  T3 Timer Length (sec): 15

 Port  Interface   Side  Cntry/Peer  TEI                      Layer 1 Detect
                          Protocol                           Stable? Slips?
   1: peer-slave    b       QSIG     0                          y      n
   2:                                0                          y      n
```

Use the command **add trunk-group <group #>** to add a trunk group for the ISDN BRI. Use the command **display trunk-group <group#>** to verify the configuration. The following tables show the configuration. Trunk group 140 is configured with two ISDN BRI channels. Note that the second B channel must be configured to port 17 (001V4**17)**.

```
display trunk-group 140                                       Page   1 of  19
                                TRUNK GROUP

Group Number: 140                 Group Type: isdn          CDR Reports: y
  Group Name: OUTSIDE CALL               COR: 1        TN: 2        TAC: 140
   Direction: two-way        Outgoing Display? n         Carrier Medium: PRI/BRI
 Dial Access? y                Busy Threshold: 255       Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n            TestCall ITC: rest
                        Far End Test Line No:
TestCall BCC: 4
TRUNK PARAMETERS
         Codeset to Send Display: 6     Codeset to Send National IEs: 6
        Max Message Size to Send: 260   Charge Advice: none
  Supplementary Service Protocol: a     Digit Handling (in/out): enbloc/enbloc
```

```
display trunk-group 140                                    Page   3 of  19
                                TRUNK GROUP
                                     Administered Members (min/max):   1/2
GROUP MEMBER ASSIGNMENTS                 Total Administered Members:   2

       Port    Code Sfx Name        Night           Sig Grp
  1: 001V401  2BRIIM
  2: 001V417  2BRIIM
```

3.2.4. Configure IGAR Between Avaya G650 and G250-BRI Media Gateways

Use the command **change system-parameters features** to enable IGAR on a system-wide basis.

```
change system-parameters features                          Page   5 of  16
                        FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:               Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
                             Switch Name:

    Emergency Extension Forwarding (min): 10
  Enable Inter-Gateway Alternate Routing? y
```

The following screen shows the IGAR configuration for Network Region 1 (the Main Office). The IGAR extension for Network Region 1 is configured to 8555555. When this extension is used for the IGAR, it expands to 1-732-855-5555.

```
display ip-network-region 1                                Page   2 of  19
                                IP NETWORK REGION


INTER-GATEWAY ALTERNATE ROUTING
 Incoming LDN Extension: 8555555
 Conversion To Full Public Number - Delete: 0  Insert: 1732
 Maximum Number of Trunks to Use: 10
```

The following screen shows the IGAR configuration for Network Region 2 (the Small Office). The IGAR extension for Network Region 2 is configured to 2033333. When this extension is used for the IGAR, it expands to 1-404-203-3333. The S8300 LSP is configured in the **LSP NAMES IN PRIORITY ORDER** field so that the IP telephones in Network Region 2 can receive the LSP address upon registration.

```
display ip-network-region 2                                    Page   2 of  19
                              IP NETWORK REGION

INTER-GATEWAY ALTERNATE ROUTING
 Incoming LDN Extension: 2033333
 Conversion To Full Public Number - Delete: 0  Insert: 1404
 Maximum Number of Trunks to Use: 10

 LSP NAMES IN PRIORITY ORDER         SECURITY PROCEDURES
 1   S8300-LSP1                      1   challenge
```

The following screen shows how to enable Dynamic CAC and IGAR between a network region pair. The **WAN-BW-Limits** is configured to **Dynamic** and the **Dynamic CAC Gateway** is configured to Media Gateway 1 (G250-BRI). Configure **IGAR** to **y** to enable IGAR between Network Regions 1 and 2.

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

                  Inter Network Region Connection Management

 src dst  codec  direct                                    Dynamic CAC
 rgn rgn   set    WAN    WAN-BW-limits  Intervening-regions    Gateway    IGAR
 2   1     2       y           :Dynamic                         1         y
```

The IGAR uses ARS for call routing. The following screens show the ARS configuration. The local PSTN trunk is configured to reach the remote IGAR DID number.

```
change ars analysis 1404                                       Page   1 of   2
                            ARS DIGIT ANALYSIS TABLE
                                  Location:  all          Percent Full:    1

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    1404                  11   11    10       fnpa         n
```

```
display route-pattern 10                                       Page   1 of   3
                   Pattern Number: 10  Pattern Name:
                                         Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                          DCS/ IXC
    No          Mrk Lmt List Del  Digits                            QSIG
                              Dgts                                  Intw
 1: 10   0                     0                                     n   user
```

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

         Dialed           Total     Route    Call   Node  ANI
         String         Min  Max  Pattern   Type   Num   Reqd
   1732                 11   11    140      fnpa         n
```

```
display route-pattern 140                                   Page   1 of   3
                  Pattern Number: 140 Pattern Name:
                                       Secure SIP? n
   Grp FRL NPA Pfx Hop Toll No.  Inserted                        DCS/ IXC
   No          Mrk Lmt List Del  Digits                        QSIG
                             Dgts                              Intw
 1: 140  0                    0                                 n   user
```

In Section 3.3, the Cisco 3745 Voice Gateway is configured to forward the last 7 digits to the Avaya Media Gateway. Use the command **change inc-call-handling-trmt trunk-group** to delete the first two digits to match the local 5 digit extension for incoming PSTN calls. Since the IGAR extension is configured to 7 digits (8555555), this number must not be shortened

```
change inc-call-handling-trmt trunk-group 10                Page   1 of  30
                     INCOMING CALL HANDLING TREATMENT
 Service/       Called    Called        Del  Insert          Per Call  Night
 Feature         Len      Number                             CPN/BN    Serv
 tie              7   8555555           1    8
 tie              7   855               2
```

```
change inc-call-handling-trmt trunk-group 140               Page   1 of  30
                     INCOMING CALL HANDLING TREATMENT
 Service/       Called    Called        Del  Insert          Per Call  Night
 Feature         Len      Number                             CPN/BN    Serv
 tie              7   2033333           1    2
 tie              7   203               2
```

3.3. Configure Cisco 3745 Voice Gateway To Simulate PSTN

The controller T1 3/0 on the Cisco 3745 Voice Gateway is connected to the ISDN/PRI on the Avaya G650 Media Gateway. The following screen shows the configuration:

```
controller T1 3/0
 framing esf
 clock source internal
 linecode b8zs
 pri-group timeslots 1-24

interface Serial3/0:23
 no ip address
 no logging event link-status
 isdn switch-type primary-5ess
 isdn incoming-voice voice
 isdn outgoing display-ie
 no cdp enable
```

The interface BRI2/0 on the Cisco 3745 Voice Gateway is connected to the Avaya G250-BRI. The Cisco BRI must be configured to NT side in Layer 1 because the Avaya G250-BRI Media Gateway only supports the TE side. A BRI S/T cross over cable (cross-pairs 4-6 and 3-5) must be used between the Cisco and the Avaya G250-BRI Media Gateway.

The BRI interface on the Cisco is configured to network in layer 2 with isdn switch-type basic-qsig to match the Avaya G250-BRI Media Gateway configuration in Section 3.2.3. The following shows the Cisco BRI configuration:

```
interface BRI2/0
 no ip address
 isdn switch-type basic-qsig
 isdn protocol-emulate network
 isdn layer1-emulate network
 isdn incoming-voice voice
```

The following screen shows the dial plan configuration on the Cisco Voice Gateway. Note that the last 7 digits are forwarded to the Avaya Media Gateways.

```
dial-peer voice 1 pots
 destination-pattern 404.......
 port 2/0/0
 forward-digits 7
!
dial-peer voice 2 pots
 destination-pattern 732855....
 direct-inward-dial
 port 3/0:23
 forward-digits 7
```

3.4. Configure Cisco 6509

The Cisco Catalyst 6509 with a routing engine is used to connect the Avaya S8500 Media Server, G650 Media Gateway and other IP endpoints shown in **Figure 1**. The following screen shows the VLAN configuration. VLAN 87 is used for the Avaya S8500 Media Server and the IPSI of the Avaya G650 Media Gateway. VLAN 88 is used for the Avaya C-LAN, MEDPRO of the Avaya G650 Media Gateway and the IP telephones. VLAN 102 is used for the inter-connection between the Cisco 6509 and Cisco 3745 access router.

```
interface Vlan87
 ip address 192.168.87.1 255.255.255.0
 no ip route-cache
 no ip mroute-cache
!
interface Vlan88
 ip address 192.168.88.1 255.255.255.0
 ip helper-address 192.168.89.5
 no ip route-cache
 no ip mroute-cache
!
interface Vlan89
 ip address 192.168.89.1 255.255.255.0
 no ip route-cache
 no ip mroute-cache
!
interface Vlan102
 ip address 192.168.200.2 255.255.255.0
 no ip unreachables
 no ip route-cache
 no ip mroute-cache
```

```
router ospf 1
 log-adjacency-changes
 network 192.168.87.0 0.0.0.255 area 0
 network 192.168.88.0 0.0.0.255 area 0
 network 192.168.89.0 0.0.0.255 area 0
 network 192.168.200.0 0.0.0.255 area 0

ip route 0.0.0.0 0.0.0.0 192.168.200.1
```

3.5. Configure Cisco 3745 Access Router

The Cisco 3745 access router is connected to the Cisco 6509, Cisco PIX and the Avaya G250-BRI Media Gateway. The following screen shows the interface configuration. Interface FastEthernet 0/0 is connected to the Cisco 6509, interface Serial 0/0 to the Avaya G250-BRI Media Gateway via T1 and FastEthernet 1/1 to the private interface of the Cisco PIX.

```
interface FastEthernet0/0
 ip address 192.168.200.1 255.255.255.0
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 192.168.211.1 255.255.255.0
 encapsulation ppp
 service-module t1 clock source internal
!
interface FastEthernet1/1
 ip address 192.168.128.1 255.255.255.0
 duplex auto
 speed auto
```

The following screen shows IP routing configuration. The default route is configured to the Cisco PIX.

```
router ospf 1
 log-adjacency-changes
 network 192.168.128.0 0.0.0.255 area 0
 network 192.168.200.0 0.0.0.255 area 0
 network 192.168.211.0 0.0.0.255 area 0

ip route 0.0.0.0 0.0.0.0 192.168.128.2
```

3.6. Configure the Cisco PIX Firewall

The following configurations use CLI on the Cisco PIX.

3.6.1. Basic Configuration

The following shows the basic configurations for the interfaces, static routes and default route. Ethernet 0 is configured as a public interface with IP address 12.160.179.124 and Ethernet 1 is configured as a private interface with IP address 192.168.128.2. The default route is configured to the outside interface and a static route is configured to the inside interface.

```
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
ip address outside 12.160.179.124 255.255.255.224
ip address inside 192.168.128.2 255.255.255.0
route outside 0.0.0.0 0.0.0.0 12.160.179.97 1
route inside 192.168.80.0 255.255.240.0 192.168.128.1 1
```

3.6.2. Access List Configuration

By default, Network Address Translation (NAT) applies to all the outgoing traffic. Since a VPN tunnel is configured between the Main Office and the Small Office, NAT is not necessary. An access list **nonatvpn** is configured to match the VPN traffic.

```
access-list nonatvpn permit ip 192.168.80.0 255.255.240.0 192.168.202.0 255.255.254.0
```

Apply access list **nonatvpn** to the inside interface of the Cisco PIX:

```
nat (inside) 0 access-list nonatvpn
```

3.6.3. VPN Configuration

Refer to reference [4] for static-to-static IPSec VPN configuration. In the sample configuration, the IP address of the Avaya G250-BRI Media Gateway is dynamic. The Cisco PIX must be configured to dynamically accept connections. Since the G250-BRI Media Gateway is connected to a NAT device, NAT-T must be enabled on the Cisco PIX so that UDP encapsulation can be used for the IPSec traffic between the Cisco PIX and Avaya G250. The following screen shows the annotated configuration for the IKE phase 1 proposal.

```
!---enable isakmp on the outside interface.

isakmp enable outside

!--- match to any incoming isakmp connection.

isakmp key ******** address 0.0.0.0 netmask 0.0.0.0

!--- policy for accepting dynamic connections from Avaya G250 Media Gateway.
!----  NAT-T is enabled.
!---- match the G250 Phase I configuration.

isakmp identity address
isakmp nat-traversal 20
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption aes
isakmp policy 1 hash sha
isakmp policy 1 group 1
isakmp policy 1 lifetime 86400
```

The following screen shows the IPSec (IKE phase 2) configuration:

```
!--- IPSec configuration to match the G250 Phase II configuration.
!--- Dynamic-map is configured.

crypto ipsec transform-set H2 esp-aes esp-sha-hmac
crypto dynamic-map G250-Dynamic 2 set pfs group2
crypto dynamic-map G250-Dynamic 2 set transform-set H2
crypto map dyn-map 20 ipsec-isakmp dynamic G250-Dynamic
crypto map dyn-map interface outside
```

Enter the **sysopt connection permit-ipsec** command to implicitly permit IPSec packets to bypass PIX Firewall Access Lists, access groups, and conduits.

```
sysopt connection permit-ipsec
```

4. Verification Steps

4.1. Verify IP Connectivity and Dynamic CAC-BL

When the primary link is up, use the command **show ip route** to verify that the correct IP routing entries are learned by the OSPF routing protocol. Verify that FastEthernet 10/2 DHCP client gets its dynamic IP address and default route from the Cable modem router (configured as a DHCP server). Verify that the Avaya IP telephones, the Avaya G250-BRI Media Gateway and S8300 LSP are registered to the Avaya S8500 Media Server.

```
G250-BRI-001(super)# show ip route
Showing 12 rows
    Network     Mask      Interface            Next-Hop      Cost  TTL  Source
--------------- ---- ------------------ ------------------ ----- --- ---------
0.0.0.0            0 FastEth  10/2       192.168.1.1            1 n/a DHCP
192.168.1.0       24 FastEth  10/2       192.168.1.100          1 n/a LOCAL
192.168.87.0      24 Serial   2/1:1      192.168.211.1         67 n/a OSPF
192.168.88.0      24 Serial   2/1:1      192.168.211.1         67 n/a OSPF
192.168.89.0      24 Serial   2/1:1      192.168.211.1         67 n/a OSPF
192.168.200.0     24 Serial   2/1:1      192.168.211.1         66 n/a OSPF
192.168.202.0     24 Vlan     202        192.168.202.1          1 n/a LOCAL
192.168.203.0     24 Vlan     203        192.168.203.1          1 n/a LOCAL
192.168.211.0     24 Serial   2/1:1      192.168.211.2          1 n/a LOCAL
192.168.211.1     32 Serial   2/1:1      192.168.211.2          1 n/a LOCAL
```

Use the command **show dynamic-cac** on the G250-BRI Media Gateway to check the reported Region Bearer Bandwidth Limit (RBBL).

```
G250-BRI-001(super)# show dynamic-cac

Current RBBL  : 128 kbps
Last event    : 0 Days, 00:00:03
Last event BBL: 128 kbps
```

Use the command **status ip-network-region 2** to verify that the correct RBBL value is received.

```
status ip-network-region 2

                    Inter Network Region Bandwidth Status
                                                 Number of   # Times
Src Dst  Conn    Conn  BW-limit   BW-Used(Kbits) Connections BW-Limit  IGAR
Rgn Rgn  Type    Stat                 Tx    Rx     Tx     Rx Hit Today Now/Today

  2   1 direct   pass  128 Dynamic     0     0      0      0     28      0/  5
```

Shutdown the primary link on the G250-BRI Media Gateway or on the remote peer. Verify that the VPN backup is up and all the traffic can get through between the Main and Small Offices. Verify that the CAC-BL value configured on the backup link is reported.

```
status ip-network-region 2

                    Inter Network Region Bandwidth Status
                                                 Number of   # Times
Src Dst  Conn    Conn  BW-limit   BW-Used(Kbits) Connections BW-Limit  IGAR
Rgn Rgn  Type    Stat                Tx    Rx     Tx     Rx Hit Today Now/Today

  2   1 direct   pass   40 Dynamic     0     0      0      0     28      0/  5
```

4.2. Verify IGAR Feature

In the sample configuration, make two phone calls between the Main and Small Offices when the primary link is down and the backup link is up. Use the command **status ip-network-region** to verify that the first call uses VoIP and the second uses IGAR.

```
status ip-network-region 2

                    Inter Network Region Bandwidth Status
                                                 Number of   # Times
Src Dst  Conn    Conn  BW-limit   BW-Used(Kbits) Connections BW-Limit  IGAR
Rgn Rgn  Type    Stat                Tx    Rx     Tx     Rx Hit Today Now/Today

  2   1 direct   pass   40 Dynamic    27    27      1      1     32      1/  6
```

For testing purposes, all calls can be forced to use the IGAR feature by configuring the Codec between Network Regions 1 and 2 to **pstn**. Another way to force IGAR is to configure the CAC-BL to 0. Do not forget to restore the configuration after testing.

If necessary, use the command **list trace station <ext.>** to troubleshoot IGAR problems. The following screen shows a correct IGAR trace. As seen, IGAR is triggered since there is no bandwidth available for a VoIP call. Note that ARS access code 9 (configured by **change feature-access-codes**) is added to the dialing number for call routing.

```
list trace station 50001
                                LIST TRACE
time            data

12:56:10     tone-receiver     01AXX04 cid 0x78
12:56:10     active station    50001 cid 0x78
12:56:13     dial 30000
12:56:13     ring station    30000 cid 0x78
12:56:13     denial event 2332: No BW, prowler <--> MG D1=0x7f00001b D2=0x78
12:56:13     IGAR starting call app A station  30000 cid 0x78
12:56:13     dial 91404203 route:PREFIX|FNPA|ARS
12:56:13     term trunk-group 10    cid 0x79
12:56:13     dial 914042033333 route:PREFIX|FNPA|ARS
12:56:13     route-pattern  10 preference 1  cid 0x79
12:56:13     seize trunk-group 10 member 16  cid 0x79
12:56:13     Setup digits 4042033333
12:56:13     Calling Number & Name NO-CPNumber NO-CPName
12:56:13     Proceed trunk-group 10 member 16  cid 0x79
12:56:13     tone-receiver     01AXX08 cid 0x79
12:56:13     Alert trunk-group 10 member 16  cid 0x79
12:56:13     active trunk-group 10 member 16  cid 0x79
12:56:14     IGAR active call app A trunks 10/16 & 140/1 cids 0x79 & 0x7a
```

4.3. Verify VPN Status

When the primary link is out of service, the VPN tunnel should be brought up. Use the command **show crypto isakmp sa** on the Avaya G250-BRI Media Gateway to display the current IKE SA. As shown in the following table, DPD and NAT-T are enabled. Note that the local IP address 192.168.1.100 is obtained from the Cable modem router.

```
G250-BRI-001(super)# show crypto isakmp sa

C-id Local           Remote          State   Encr    Hash Aut DH TTL   DPD Nat-T
---- --------------- --------------- ------- ------- ---- --- -- ----- --- -----
  25 192.168.1.100   12.160.179.124  Ready   aes     sha  psk  1 86355 Yes Yes
```

Use the command **show crypto ipsec sa** on the Avaya G250-BRI Media Gateway to display the current IPSec status. The NAT-T feature works as expected since UDP encapsulation with UDP port 4500 is used for the VPN.

```
G250-BRI-001(super)# show crypto ipsec sa

Interface: FastEthernet 10/2
 Crypto list id: 901, Local address: FastEthernet 10/2.0

  Rule: 1, Crypto map: 1, "Phase 2 Proposal"
  Local address:   192.168.1.100:4500, Remote address: 12.160.179.124:4500
  Local identity:  192.168.202.0/255.255.254.0
  Remote identity: 192.168.80.0/255.255.240.0
  Remote identity: 192.168.80.0/255.255.240.0
  Current outbound spi: 0x90942e46

  Inbound packets                          Outbound packets
  ---------------------------------    ---------------------------------
  Total                        110363    Total                        191515
    Total OK                   110363      Total OK                   191504
      Decrypt                  110363        Encrypt                  191504
      Verify                   110363        Digest                   191504
      Decaps                   110363        Encaps                   191504
    Total discards                  0      Total discards                11

   SA Type         SPI        Transform     PFS Secs left  KB left    Mode
   --------------- ---------- ------------- --- ---------- ---------- ---------
   Inbound ESP     0x1000     esp-aes       #2        1973    4607910 Tunnel
                              esp-sha-hmac

   Outbound ESP    0x90942e46 esp-aes       #2        1973    4598290 Tunnel
                              esp-sha-hmac
```

Use the command **show crypto isakmp sa** on the Cisco PIX to display the current IKE SA. Note that the destination IP address of the SA is the public IP address on the Cable modem router.

```
Cisco-PIX# show crypto isakmp sa
Total     : 1
Embryonic : 0
        dst               src         state     pending     created
  12.160.179.124    68.38.206.155    QM_IDLE           0           1
```

Use the command **show crypto ipsec sa** on the Cisco PIX to display the current IPSec status. The Cisco PIX has learned the correct local and remote IP networks from the Avaya G250-BRI Media Gateway. The NAT-T feature works as expected since UDP encapsulation with UDP port 4500 is used for theVPN.

```
Cisco-PIX# show crypto ipsec sa

interface: outside
    Crypto map tag: dyn-map, local addr. 12.160.179.124

   local  ident (addr/mask/prot/port): (192.168.80.0/255.255.240.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.202.0/255.255.254.0/0/0)
   current_peer: 68.38.206.155:4500
     PERMIT, flags={transport_parent,}
    #pkts encaps: 20, #pkts encrypt: 20, #pkts digest 20
    #pkts decaps: 3572, #pkts decrypt: 3572, #pkts verify 3572
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 12.160.179.124, remote crypto endpt.: 68.38.206.155
     path mtu 1500, ipsec overhead 80, media mtu 1500
     current outbound spi: 1000

     inbound esp sas:
      spi: 0x90942e46(2425630278)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        slot: 0, conn id: 1, crypto map: dyn-map
        sa timing: remaining key lifetime (k/sec): (4607648/3480)
        IV size: 16 bytes
        replay detection support: Y


     inbound ah sas:


     inbound pcp sas:


     outbound esp sas:
      spi: 0x1000(4096)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        slot: 0, conn id: 2, crypto map: dyn-map
        sa timing: remaining key lifetime (k/sec): (4607998/3479)
        IV size: 16 bytes
        replay detection support: Y
```

Syslog debugging can be enabled on the G250-BRI Media Gateway for troubleshooting. Enter the following commands from the console port to enable VPN debugging.

```
G250-BRI-001(super)# set logging session condition isakmp debug

G250-BRI-001(super)# set logging session condition ipsec debug

G250-BRI-001(super)# set logging session enable
```

The following screen shows sample annotated syslog debug messages:

```
!---G250 initiates IKE phase 1 with aggressive mode.

04/01/2005,11:33:43:IPSEC-Informational:
    Call IKE negotiation for outgoing SPD entry 901_1:
        Peers 192.168.1.100<->12.160.179.124

04/01/2005,11:33:43:ISAKMP-Informational:
    Initiating IKE phase 1 negotiation:
        Peers 192.168.1.100<->12.160.179.124, mode aggressive

!---G250 sends IKE phase 1 to the Cisco PIX.

04/01/2005,11:33:43:ISAKMP-Debug:
    Sending vendor ID to 12.160.179.124 (VID length = 16):
        Peers 192.168.1.100<->12.160.179.124
        Avaya Gateway VPN v1.0 (0x133bc1e3f926a020cad5bed4ffe04c8f)

04/01/2005,11:33:43:ISAKMP-Debug:
    Sending vendor ID to 12.160.179.124 (VID length = 16):
        Peers 192.168.1.100<->12.160.179.124
        draft-ietf-ipsec-dpd-00.txt (0xafcad71368a1f1c96b8696fc77570100)

04/01/2005,11:33:43:ISAKMP-Debug:
    Sending vendor ID to 12.160.179.124 (VID length = 16):
        Peers 192.168.1.100<->12.160.179.124
        Avaya VPNos v3.2 (0x4485152d18b6bbcc0be8a8469579ddcc)

04/01/2005,11:33:43:ISAKMP-Debug:
    Sending vendor ID to 12.160.179.124 (VID length = 16):
        Peers 192.168.1.100<->12.160.179.124
        draft-ietf-ipsec-nat-t-ike-00 (0x4485152d18b6bbcd0be8a8469579ddcc)

04/01/2005,11:33:43:ISAKMP-Debug:
    Sending vendor ID to 12.160.179.124 (VID length = 16):
        Peers 192.168.1.100<->12.160.179.124
        draft-ietf-ipsec-nat-t-ike-02 (0xcd60464335df21f87cfdb2fc68b6a448)

04/01/2005,11:33:43:ISAKMP-Debug:
    Sending vendor ID to 12.160.179.124 (VID length = 16):
        Peers 192.168.1.100<->12.160.179.124
        draft-ietf-ipsec-nat-t-ike-02-cisco
(0x90cb80913ebb696e086381b5ec427b1f)

04/01/2005,11:33:43:ISAKMP-Debug:
    Sending vendor ID to 12.160.179.124 (VID length = 16):
        Peers 192.168.1.100<->12.160.179.124
        draft-ietf-ipsec-nat-t-ike-03 (0x7d9419a65310ca6f2c179d9215529d56)

04/01/2005,11:33:43:ISAKMP-Debug:
    Sending vendor ID to 12.160.179.124 (VID length = 16):
        Peers 192.168.1.100<->12.160.179.124
        RFC 3947 (0x4a131c81070358455c5728f20e95452f)
```

```
!---G250 receives IKE phase 1 from the Cisco PIX.

04/01/2005,11:33:43:ISAKMP-Debug:
    Received vendor ID from 12.160.179.124 (VID length = 8):
        Peers 192.168.1.100<->12.160.179.124
        Unknown (0x09002689dfd6b712)

04/01/2005,11:33:43:ISAKMP-Debug:
    Received vendor ID from 12.160.179.124 (VID length = 16):
        Peers 192.168.1.100<->12.160.179.124
        draft-ietf-ipsec-dpd-00.txt (0xafcad71368a1f1c96b8696fc77570100)

04/01/2005,11:33:43:ISAKMP-Debug:
    Received vendor ID from 12.160.179.124 (VID length = 16):
        Peers 192.168.1.100<->12.160.179.124
        Unknown (0x12f5f28c457168a9702d9fe274cc0100)

04/01/2005,11:33:43:ISAKMP-Debug:
    Received vendor ID from 12.160.179.124 (VID length = 16):
        Peers 192.168.1.100<->12.160.179.124
        Unknown (0xc4407a985c6e6e0099e1589b8619aea0)

04/01/2005,11:33:43:ISAKMP-Debug:
    Received vendor ID from 12.160.179.124 (VID length = 16):
        Peers 192.168.1.100<->12.160.179.124
        draft-ietf-ipsec-nat-t-ike-03 (0x7d9419a65310ca6f2c179d9215529d56)

04/01/2005,11:33:43:ISAKMP-Debug:
    Received vendor ID from 12.160.179.124 (VID length = 16):
        Peers 192.168.1.100<->12.160.179.124
        draft-ietf-ipsec-nat-t-ike-02-ci (0x90cb80913ebb696e086381b5ec427b1f)

!---NAT-T is selected.

04/01/2005,11:33:43:ISAKMP-Informational:
    Selected NAT-T draft:
        draft-ietf-ipsec-nat-t-ike-03
        Peers 192.168.1.100<->12.160.179.124

!---NAT device is detected.

04/01/2005,11:33:43:ISAKMP-Informational:
    NAT device detected. We are located in its inner side:
        Peers 192.168.1.100<->12.160.179.124

!---Standard NAT-T UDP port 4500 is selected.

04/01/2005,11:33:43:ISAKMP-Informational:
    NAT-T: floating to ports 4500->4500:
        Peers 192.168.1.100<->12.160.179.124

!---Finished IKE phase 1 with DPD enabled.

04/01/2005,11:33:43:ISAKMP-Informational:
    Finished IKE phase 1 negotiation, creating ISAKMP SA:
```

```
        Peers  192.168.1.100<->12.160.179.124
        Icookie - e2e0c0a74f8dd857, Rcookie - 3187dd855c6f6e00
        esp-aes, esp-sha-hmac, DH group 1, Lifetime 86400 seconds
        NAT-T (inner side), DPD enabled

!---Start DPD keepalive

04/01/2005,11:33:43:ISAKMP-Informational:
    Start DPD keepalive with peer 12.160.179.124:
        Interval - 10 seconds , Retry interval - 2 seconds , Mode - on-demand
        Peers 192.168.1.100<->12.160.179.124

!--- Initiate IKE phase 2

04/01/2005,11:33:43:ISAKMP-Informational:
    Initiating IKE phase 2 negotiation:
        SPD entry - 901_1
        Peers 192.168.1.100<->12.160.179.124

04/01/2005,11:33:43:ISAKMP-Informational:
    Start NAT-T keepalive with peer 12.160.179.124:
        Peers 192.168.1.100<->12.160.179.124

04/01/2005,11:33:43:ISAKMP-Informational:
    Received IKE notify message:
        Type INITIAL_CONTACT (24578)
        Peers 192.168.1.100<->12.160.179.124
        Icookie - e2e0c0a74f8dd857, Rcookie - 3187dd855c6f6e00

!---Finished IKE phase 2, create outbound IPSEC SA.

04/01/2005,11:33:43:ISAKMP-Informational:
    Finished IKE phase 2, creating outbound IPSEC SA:
        SPI 0xdb0b53ca, Peers 192.168.1.100<->12.160.179.124
        Identities: 192.168.202.0/255.255.254.0->192.168.80.0/255.255.240.0
        esp-aes, esp-sha-hmac, 3600 seconds, 4608000 KB, PFS #2
        Tunnel mode
        NAT-T udp encapsulation using:
        draft-ietf-ipsec-nat-t-ike-03, ports 4500->4500

!---Finished IKE phase 2, create inbound IPSEC SA.

04/01/2005,11:33:43:ISAKMP-Informational:
    Finished IKE phase 2, creating inbound IPSEC SA:
        SPI 0x3199, Peers 12.160.179.124<->192.168.1.100
        Identities: 192.168.80.0/255.255.240.0->192.168.202.0/255.255.254.0
        esp-aes, esp-sha-hmac, 3600 seconds, 4608000 KB, PFS #2
        Tunnel mode
        NAT-T udp encapsulation using:
        draft-ietf-ipsec-nat-t-ike-03, ports 4500->4500
```

Enter the following commands on the Cisco PIX to enable VPN debugging.

```
Cisco-PIX# debug crypto isakmp sa

Cisco-PIX# debug crypto ipsec sa
```

The following screen shows sample annotated debug messages from the Cisco PIX.

```
!---Receive IKE phase 1 proposal and process it.

crypto_isakmp_process_block:src:68.38.206.155, dest:12.160.179.124 spt:2070 dpt:500
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 0 against priority 1 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      hash SHA
ISAKMP:      auth pre-share
ISAKMP:      default group 1
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP:      keylength of 128

!--- Attributes for IKE phase 1 offered by the G250 are accepted

ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): processing vendor id payload

ISAKMP (0): processing vendor id payload

!--- Receive DPD support from the G250

ISAKMP (0): remote peer supports dead peer detection

ISAKMP (0): processing KE payload. message ID = 0

ISAKMP (0): processing NONCE payload. message ID = 0

ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing vendor id payload

ISAKMP (0): processing vendor id payload

ISAKMP (0): processing vendor id payload

ISAKMP (0): processing vendor id payload

ISAKMP (0:0): vendor ID is NAT-T
ISAKMP (0): processing vendor id payload

ISAKMP (0:0): vendor ID is NAT-T
ISAKMP (0): processing vendor id payload

ISAKMP (0): ID payload
        next-payload : 10
        type         : 1
```

```
        protocol     : 17
        port         : 0
        length       : 8
ISAKMP (0): Total payload length: 12
ISAKMP (0:0): sending NAT-T vendor ID - rev 2 & 3
ISAKMP (0:0): constructed HIS NAT-D
ISAKMP (0:0): constructed MINE NAT-D
ISAKMP (0:0): Detected port floating
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:68.38.206.155, dest:12.160.179.124 spt:4500 dpt:
4500
OAK_AG exchange
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0:0): Detected NAT-D payload
ISAKMP (0:0): recalc my hash for NAT-D
ISAKMP (0:0): NAT match MINE hash
ISAKMP (0:0): Detected NAT-D payload
ISAKMP (0:0): recalc his hash for NAT-D
ISAKMP (0:0): NAT does not match HIS hash
hash received: ac 1e f2 28 34 4e 3c a6 75 fa f0 de 46 ea 64 31 7b b8 8f 57
his nat hash : fa e 6 88 d2 6a 8 5f 7c f7 37 97 b9 6 5c c5 1 5b ec ab

!--- Finished phase 1 negotiation

ISAKMP (0): SA has been authenticated
return status is IKMP_NO_ERROR
ISAKMP (0): sending INITIAL_CONTACT notify
ISAKMP (0): sending NOTIFY message 24578 protocol 1
VPN Peer: ISAKMP: Added new peer: ip:68.38.206.155/4500 Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:68.38.206.155/4500 Ref cnt incremented to:1 Total VPN
Peers:1
crypto_isakmp_process_block:src:68.38.206.155, dest:12.160.179.124 spt:4500 dpt:
4500
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 3257617987

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_AES
ISAKMP:   attributes in transform:
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (basic) of 3600
ISAKMP:      SA life type in kilobytes
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:      encaps is 61443
ISAKMP:      authenticator is HMAC-SHA
ISAKMP:      group is 2
ISAKMP:      key length is 128

!--- Attributes for IKE phase 2 offered by the G250 are accepted

ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request): proposal part
#1,
  (key eng. msg.) dest= 12.160.179.124, src= 68.38.206.155,
    dest_proxy= 192.168.80.0/255.255.240.0/0/0 (type=4),
    src_proxy= 192.168.202.0/255.255.254.0/0/0 (type=4),
    protocol= ESP, transform= esp-aes esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x420
```

```
ISAKMP (0): processing NONCE payload. message ID = 3257617987

ISAKMP (0): processing KE payload. message ID = 3257617987

ISAKMP (0): processing ID payload. message ID = 3257617987
ISAKMP (0): ID_IPV4_ADDR_SUBNET src 192.168.202.0/255.255.254.0 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 3257617987
ISAKMP (0): ID_IPV4_ADDR_SUBNET dst 192.168.80.0/255.255.240.0 prot 0 port 0IPSE
C(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xdb0b53ca(3674952650) for SA
        from   68.38.206.155 to  12.160.179.124 for prot 3

return status is IKMP_NO_ERROR
ISAKMP (0): sending NOTIFY message 11 protocol 3
crypto_isakmp_process_block:src:68.38.206.155, dest:12.160.179.124 spt:4500 dpt:
4500
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT

!--- Create inbound and outbound IPSec SA

ISAKMP (0): Creating IPSec SAs
        inbound SA from   68.38.206.155 to  12.160.179.124 (proxy   192.168.202.0 to
192.168.80.0)
        has spi 3674952650 and conn_id 2 and flags 421
        lifetime of 3600 seconds
        lifetime of 4608000 kilobytes
        outbound SA from  12.160.179.124 to   68.38.206.155 (proxy    192.168.80.0 to
192.168.202.0)
        has spi 12697 and conn_id 1 and flags 421
        lifetime of 3600 seconds
        lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.160.179.124, src= 68.38.206.155,
    dest_proxy= 192.168.80.0/255.255.240.0/0/0 (type=4),
    src_proxy= 192.168.202.0/255.255.254.0/0/0 (type=4),
    protocol= ESP, transform= esp-aes esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xdb0b53ca(3674952650), conn_id= 2, keysize= 128, flags= 0x421
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 12.160.179.124, dest= 68.38.206.155,
    src_proxy= 192.168.80.0/255.255.240.0/0/0 (type=4),
    dest_proxy= 192.168.202.0/255.255.254.0/0/0 (type=4),
    protocol= ESP, transform= esp-aes esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x3199(12697), conn_id= 1, keysize= 128, flags= 0x421
```

5. Conclusion

As illustrated by these Application Notes, the Avaya IGAR feature works well with the Dynamic CAC-BL reported from a remote Avaya G250-BRI Media Gateway. The number of VoIP calls supported is based on which IP connection is used on the G250-BRI Media Gateway. Upon reaching the CAC-BL, Avaya Communicating Manager will immediately use PSTN facilities allocated for use by the IGAR feature. A VPN tunnel across the Internet can be used between the Avaya G250-BRI Media Gateway with a dynamic IP address and Cisco PIX to back up a primary link.

6. Additional References

The following Applications Notes can be found at http://www.avaya.com.

[1] Configuring Avaya Communication Manager for Avaya S8700 Media Servers and Avaya G600 Media Gateways Controlling Avaya G350 Media Gateways with Avaya S8300 Media Servers as Local Survivable Processors

[2] Configuring DHCP and TFTP Servers On Avaya G350 and G250 Media Gateways for Avaya IP 4600 Series Telephones

[3] Configuring Avaya Communication Manager With Cisco Gatekeepers and Cisco VoIP Gateways

[4] IPSec Virtual Private Network (VPN) between an Avaya G350 Media Gateway with Local Survivable Processor and a Cisco PIX 525 Firewall Controlled by S8700 Media Servers and G650 Media Gateway

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