



Avaya Solution & Interoperability Test Lab

Configuring Avaya Communication Manager for Media Encryption – Issue 1.0

Abstract

These Application Notes present a sample configuration using the Avaya Communication Manager Media Encryption feature to enhance security for a network comprised of an Avaya S8700 Media Server, Avaya S8300 Media Server, and Avaya G350 Media Gateways. The Avaya S8700 Media Server is in one logical location, controlling a G350 Media Gateway in another logical location across a WAN. These Application Notes show how Media Encryption can be configured when a server at one location controls Media Gateways that can be distributed around the enterprise. In another logical location, an S8300 Media Server is configured as an independent call server controlling a second G350 Media Gateway. The S8300 Media Server and S8700 Media Server are networked using H.323 Signaling Groups and IP Trunk Groups that also utilize media encryption. These Application Notes focus on the Communication Manager configuration of the Network Regions, Codec Sets, H.323 Signaling Groups, and IP Trunk Groups. The approach documented in these Application Notes can be used with other Media Servers (e.g., the Avaya S8500 Media Server) and Media Gateways (e.g., the Avaya G700 Media Gateway). Detailed status screens for active calls are presented, to reinforce understanding of the configuration.

1. Introduction and Scope

These Application Notes present a sample configuration using the Avaya Communication Manager Media Encryption feature to enhance security for a network comprised of an Avaya S8700 Media Server, Avaya S8300 Media Server, and Avaya G350 Media Gateways. The Avaya S8700 Media Server is in one logical location, controlling a G350 Media Gateway in another logical location across a WAN. These Application Notes show how Media Encryption can be configured when a server at one location controls Media Gateways that can be distributed around the enterprise. In another logical location, an S8300 Media Server is configured as an independent call server controlling a second G350 Media Gateway. The S8300 Media Server and S8700 Media Server are networked using H.323 Signaling Groups and IP Trunk Groups that also utilize media encryption. These Application Notes focus on the Communication Manager configuration of the Network Regions, Codec Sets, H.323 Signaling Groups, and IP Trunk Groups. In Section 6, detailed status screens for active calls are presented, to reinforce understanding of the configuration.

1.1. Overview of Media Encryption Feature

The Avaya Communication Manager Media Encryption feature is one component of an overall network security plan, complementing other techniques used to secure communications on a network, such as VPN and firewall technology to secure perimeter entry into a network. However, unlike other technologies employing encryption to enhance security, the Communication Manager Media Encryption feature does not increase the amount of bandwidth required on the LAN or WAN. That is, for a given set of codec parameters, a media connection employing encryption consumes the same bandwidth as an unencrypted media connection among the same devices. This is because only the media payload within the Real Time Protocol (RTP) portion of an IP Packet is encrypted, according to an algorithm and key materials communicated at call setup. A detailed description of the key exchange procedures is beyond the scope of this document. However, suffice it to say that the session keys distributed to an IP Telephone, IP Softphone, or Media Gateway at call setup are also sent in an encrypted communication.

Avaya Communication Manager provides a flexible, configurable choice of the encryption algorithm, as described in these Application Notes. One pre-standard algorithm, whose availability pre-dates Avaya Communication Manager 2.0, is called the Avaya Encryption Algorithm (AEA, also referred to as AEA-2 to reflect the subtle point that the first generally available use of AEA was in fact a second generation of the algorithm). AEA uses a 104-bit key, and has the attractive characteristic that using AEA has no effect on the capacity of the various resources (e.g., TN2302 Media Processor, or the integrated media processing resources on a G350 or G700 Media Gateway).

Beginning in Communication Manager 2.0 and Avaya IP Telephone firmware version 2.0, Avaya introduced support for the Advanced Encryption Standard (AES). AES is a Federal Information Processing Standard (FIPS) Publication (FIP-197) that specifies a cryptographic algorithm for use by U.S. Government organizations to protect sensitive, unclassified

information. AES specifies three possible key sizes, and the Avaya implementation uses AES operating in 128-bit Counter mode (AES-128-CTR) using a 128-bit key. The stronger encryption afforded by using AES with 128 bit keys has the consequence that a given media processor's capacities are reduced by 25% when using AES, for a given set of codec parameters. For example, whereas a TN2302 Media Processor could process 64 simultaneous G.711MU streams or 32 simultaneous G.729 streams, with or without AEA, the maximum simultaneous capacities with AES compression would be 48 (G.711MU) and 24 (G.729) respectively. Given that media processor capacities are affected by the stronger AES encryption, but are unaffected by AEA, it may be desirable to use the AES algorithm judiciously, where security considerations are paramount.

Figure 1 provides a high-level overview of the network used to verify these Application Notes. Avaya equipment is labeled with red text, and Cisco equipment is labeled with blue text. Note that Media Encryption could be used with other types of Avaya Media Servers and Media Gateways. For example, the same approach documented in these Application Notes could be used if Site A contained an S8500 Media Server and G650 Media Gateway, and Site B or Site C contained a G700 Media Gateway.

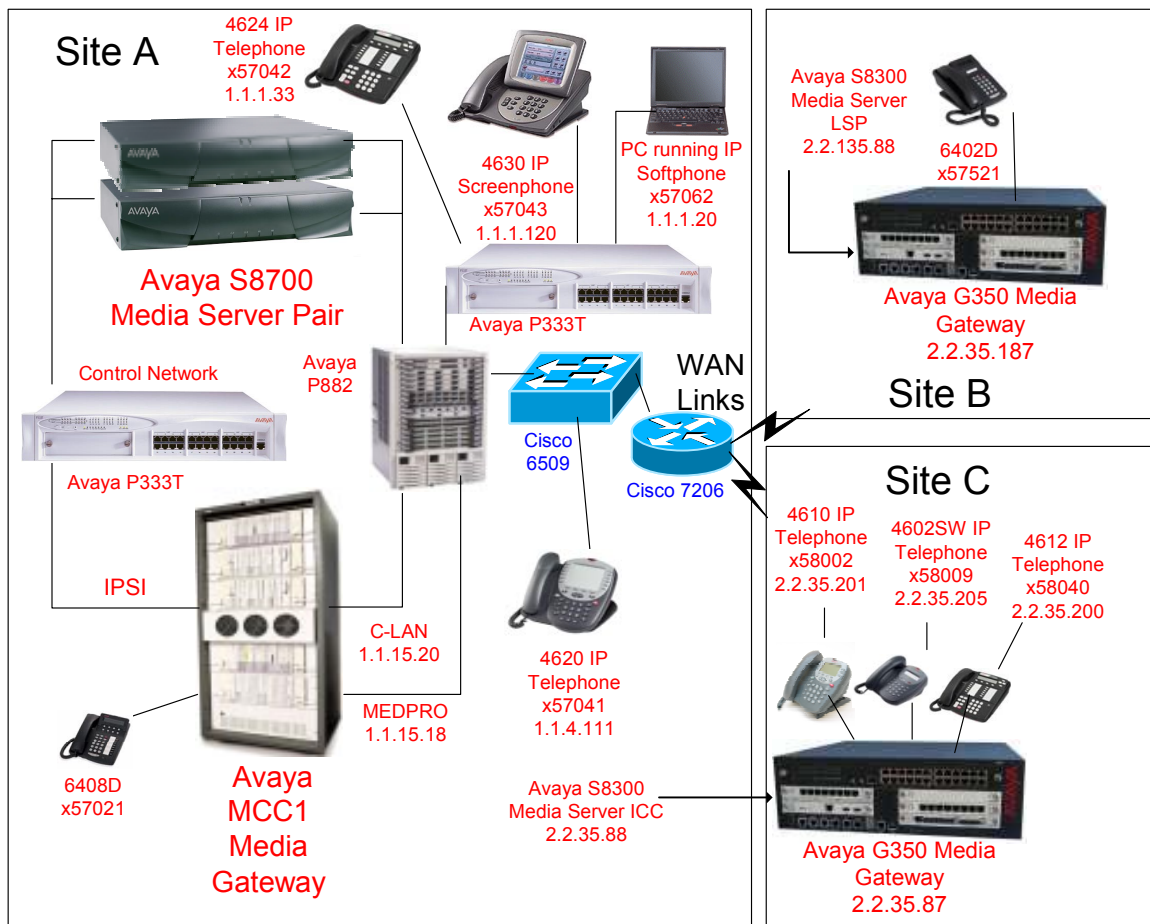


Figure 1: Network Overview

Figure 1 will assist the reader in following the Avaya Communication Manager configuration and detailed call status verifications presented in these Application Notes. Since the networking configuration of the sites is not the focus of this document, a detailed illustration of the equipment performing the WAN links to the remote sites has been omitted from **Figure 1**.

1.2. Example Media Encryption Objectives for the Figure 1 Network

For the purposes of illustrating the flexibility of the feature and the considerations that apply to media encryption, these Application Notes will assume the following high-level objectives for the network of **Figure 1**. Of course, each customer's objectives will vary. Section 6 shows sample calls fulfilling these objectives.

- Media connections that remain within any of the sites should be optimized for the highest quality audio experience, and utilize the fewest resources from Media Gateways, while still preferring encryption of the media streams. Assume the majority of all calls are intra-site calls, motivating a concern for optimizing capacities for Media Gateway resources, while still providing additional security via media encryption. These objectives will be satisfied in these Application Notes by configuring the G.711MU codec and the Avaya Encryption Algorithm (AEA) for media connections within each site. The G.711MU codec provides the highest quality audio among the available codec choices, while utilizing the fewest resources, where required, from a media processing resource in a Media Gateway. Moreover, when the AEA media encryption algorithm is used, there is no effect on the number of simultaneous audio terminations supported by a media processor, independent of the codec used. For example, the Avaya TN2302AP can support up to 64 G.711MU audio terminations, whether AEA media encryption is used or not. Therefore, G.711MU and AEA encryption are used to satisfy the objective for the best quality audio, secured by media encryption, while retaining the highest attainable capacity for Media Gateway resources.
- Media connections between Site A and Site B, whose G350 is controlled by the S8700 Media Server at Site A, must satisfy a primary objective to reduce the amount of bandwidth required over the WAN between the sites, while still achieving a high quality audio experience. Since the preponderance of calls are intra-site, and the less frequent inter-site calls are thought to have higher security requirements in general, there is a preference to use the strongest media encryption algorithm natively supported by the end devices. These objectives will be satisfied in these Application Notes by configuring the G.729 codec for inter-site calling, with a preference to use the Advanced Encryption Standard (AES) for media connections over the WAN, while still allowing AEA to be used across the WAN for devices that are not capable of AES. Of course, there are other means besides choosing an appropriate codec to reduce the bandwidth required between sites. For example, silence suppression or RTP header compression could be used, but these topics are outside the intended scope of this document.
- Media connections to Site C, which has an independent S8300 Media Server, must again satisfy the objective to reduce the amount of bandwidth required over the WAN between

the sites. Assume that calls across the WAN to Site C always require the strongest media encryption, independent of the native capabilities of the end devices. These objectives will be satisfied in these Application Notes by again configuring the G.729 codec for inter-site calling, but now requiring AES encryption for media connections over the IP Trunk Group to Site C. Any AEA-only devices needing to communicate between sites will have media processing resources assigned automatically to honor the requirement that the media encryption algorithm used over the WAN be AES, while still retaining AEA encryption over the LAN to any AEA-only end device.

A five digit Uniform Dial Plan (UDP) is used to facilitate calling among the sites. Unique ranges of extensions are associated with each site as follows. Site A, the location with the Avaya S8700 Media Server and MCC1 Media Gateway, uses extensions in the range 570xx. Site B, the location with the G350 Media Gateway controlled by the Avaya S8700 Media Server, uses the extension range 575xx. Site C, the location with the independent Avaya S8300 Media Server within the G350 Media Gateway, has the extension range 58xxx. The Avaya S8700 Media Server and Avaya S8300 Media Server are connected with an H.323 Signaling Group and IP Trunk Group, whose configuration is fully described herein. The Avaya UDP configuration steps are not described in detail, since there is no new routing consideration introduced by the use of media encryption in the network.

2. Equipment and Software Validated

Table 1 shows the relevant equipment and version information used in the sample configuration. A mix of Avaya IP Telephones, running different firmware versions, is used to illustrate the Communication Manager behavior under a range of scenarios. Note that the Avaya IP Telephones running 2.0 firmware are capable of both AES and AEA, whereas the Avaya IP Telephones running 1.8 firmware are capable of AEA, but not AES.

Network Component	Version Information
Avaya S8700 Media Server	Communication Manager 2.0 Load 219.0
Avaya S8300 Media Server	Communication Manager 2.0 Load 219.0
Avaya TN2312AP IPSI in MCC1	HW32 FW006
Avaya TN799DP C-LAN in MCC1	TN799DP HW01 FW009
Avaya TN2302AP MEDPRO in MCC1	TN2302AP HW03 FW071
Avaya G350 Media Gateway, Site B, containing MM312 Media Module (24 port DCP)	FW 21.20.1
Avaya G350 Media Gateway, Site C, containing MM314 Media Module (24 port inline power switch)	FW 21.20.1
Avaya IP Softphone	5.0.5 (AEA or AES)
Avaya IP Softphone for Pocket PC	Version 2.0 Load 63 (AEA)
Avaya 4602 IP Telephone	1.8 (AEA)
Avaya 4610 IP Telephone	2.0 (AEA or AES)
Avaya 4612 IP Telephone	1.8 (AEA)

Network Component	Version Information
Avaya 4620 IP Telephone	2.0 (AEA or AES)
Avaya 4624 IP Telephone	1.8 (AEA)
Avaya 4630 IP Screenphone	2.0 (AEA or AES)

Table 1 – Equipment Version Information

3. Conventions and Assumptions

In these Application Notes, Avaya Communication Manager administration software screens are shown with a gray shaded background. These administration software screens are also referred to as “SAT” (System Access Terminal) screens in this document. In some instances, the information from the original SAT screen has been edited for brevity and clarity in presentation. Throughout this document, each SAT screen capture is preceded by the text that references the screen capture. Therefore, individual screen captures are not labeled with figure identifiers.

In general, the document presents only those configuration steps that are relevant to Media Encryption or security. Initial configuration of the Media Servers and Media Gateways is outside of the scope of this document. Steps that aid in understanding the overall configuration, but are not specific to Media Encryption, are shown with “display” or “list” commands. Configuration steps directly associated with Media Encryption are shown using the relevant “add” and “change” commands.

It is assumed that the appropriate license files and authentication files have been installed on each of the Avaya Media Servers, and that login and password credentials are available to the reader. The Media Encryption feature is controlled via a license file. To verify that the installed license file grants permission to use Media Encryption, use the command “display system-parameters customer-options” as shown below. Ensure that the “Media Encryption Over IP” option shows “y” on Page 4. If the Media Encryption feature is not enabled, a new license must be obtained before following the remaining steps in these Application Notes.

```

display system-parameters customer-options                               Page 4 of 11
                                OPTIONAL FEATURES

Emergency Access to Attendant? y                                     ISDN Feature Plus? y
  Enable 'dadmin' Login? n                                           ISDN Network Call Redirection? y
  Enhanced Conferencing? y                                           ISDN-BRI Trunks? y
    Enhanced EC500? y                                               ISDN-PRI? y
  Extended Cvg/Fwd Admin? y                                           Local Spare Processor? n
  External Device Alarm Admin? n                                       Malicious Call Trace? y
  Five Port Networks Max Per MCC? n                                     Media Encryption Over IP? y
    Flexible Billing? n                                               Mode Code for Centralized Voice Mail? n
  Forced Entry of Account Codes? n
  Global Call Classification? n
  Hospitality (Basic)? y
  Hospitality (G3V3 Enhancements)? y
    IP Trunks? y
    IP Attendant Consoles? y
    IP Stations? y
  Internet Protocol (IP) PNC? n
    Multiple Level Precedence & Preemption? n
    Multimedia Appl. Server Interface (MASI)? n
    Multimedia Call Handling (Basic)? n
    Multimedia Call Handling (Enhanced)? n
    Multinational Locations? n
    Multiple Locations? y
    Personal Station Access (PSA)? y
  Multifrequency Signaling? y

```

4. Avaya S8700 Media Server Configuration

This section presents relevant configuration steps for the Avaya S8700 Media Server.

4.1. IPSI Configuration

The following illustrates the configuration of the IPSI in the MCC1 Media Gateway. “Socket Encryption” can be used to secure the signaling link between the S8700 Media Server and the IPSI. Encrypting this signaling link secures the communication of media encryption session keys to the TN2302 Media Processors.

```

change ipserver-interface 1                                           Page 1 of 1
  IP SERVER INTERFACE (IPSI) ADMINISTRATION - PORT NETWORK 1
  IP Control? y                                                       Socket Encryption? y
    Administer secondary ip server interface board? n
    Enable QoS? n

Primary IPSI
-----
Location: 1AXX
Host: 198.151.254.101
DHCP ID: ipsi-A01a

```

4.2. Node Names

The following list command output illustrates a subset of the “node-names” that map logical names to IP addresses. These node names are presented because they will appear in other screens, such as the screens defining the IP interfaces and the H.323 Signaling Group to the S8300 Media Server in Site C. The author’s editorial comments are shown after the “#” in the screen capture. These comments do not appear in the actual screen output.

```
list node-names
```

Page 1

		NODE NAMES				
Type	Name	IP	Address			
IP	CLAN-EPN1	1	.1	.15	.20	# IP Tel in Site A register here
IP	EPN1-PROWL1	1	.1	.15	.18	# Media Processor in Site A
IP	G350-2-Right	2	.2	.135.87		# G350 In Site B
IP	G350-Right	2	.2	.35	.87	# G350 in Site C
IP	S8300-G350-LSP	2	.2	.135.88		# S8300-LSP in Site B, not described
IP	S8300-in-G350	2	.2	.35	.88	# S8300 standalone in Site C

4.3. IP Interfaces

The following screen illustrates the IP interfaces. In this example, the C-LAN and MEDPRO interfaces reside in network region 1.

```
list ip-interface
```

IP INTERFACES

ON	Type	Slot	Code	Sfx	Node Name	Subnet Mask	Gateway Address	Net Rgn	VLAN
y	C-LAN	01A05	TN799	D	CLAN-EPN1	255.255.255.0	1.1.15.1	1	n
y	MEDPRO	01A06	TN2302		EPN1-PROWL1	255.255.255.0	1.1.15.1	1	n

4.4. Communication Manager Configuration For the G350 Media Gateway in Site B

The following screen illustrates the Communication Manager configuration of the G350 Media Gateway in Site B. The screen was captured after the G350 Media Gateway had registered with the C-LAN in the MCC1 Media Gateway. Note that the "Encrypt Link" field (shown in bold) has been set to "y" to enable encryption of the H.248 signaling used to control the G350 Media Gateway. When media encryption will be used, H.248 signaling encryption is essential to secure key exchanges with the G350. The Network Region number "3" has been shown in bold because these Application Notes present a means to control codec and media encryption behavior for intra-region and inter-region media paths. Calls between Site A and Site B will be between network region 1 and network region 3.

```
change media-gateway 1
```

Page 1 of 1

MEDIA GATEWAY

```

Number: 1
Type: g350
Name: G350-Right
Serial No: 03IS07589448
Network Region: 3
Registered? y
IP Address: 2 .2 .135.87
FW Version/HW Vintage: 21 .20 .1 /49
MAC Address: 00:04:0d:29:c9:91
Encrypt Link? y
Location: 3
Controller IP Address: 1 .1 .15 .20
Site Data:
Slot  Module Type      Name
V1:   S8300              ICC MM
V2:
V3:
V4:
V5:
V6:   MM312              DCP MM
V7:   virtual-analog    ANA VMM
V8:
V9:

```

4.5. H.323 Signaling Group and IP Trunk Group (to Site C)

This section focuses on the parameter settings of the H.323 Signaling Group and IP Trunk Group used to connect with the S8300 Media Server in Site C. As per the example objectives, the media flowing over this path will use G.729 and AES media encryption.

Signaling Group 26 is created to establish an H.323 signaling link between a C-LAN in the MCC1 and the S8300 Media Server in Site C. The Signaling Group number is not relevant; use any available Signaling Group number.

This Signaling Group uses the C-LAN whose node-name is “CLAN-EPN1” as the near end, and the S8300 Media Server node-name “S8300-in-G350” as the far end. Retain the default near-end listen port (1720) and enter 1720 as the far-end listen port. The “Far-end Network Region” is set to “4” so that the codec set and encryption algorithm can be uniquely controlled for calls using this Signaling Group. The “Media Encryption” field is set to “y”, and a password is entered in the “Passphrase” field. In Section 5.3, the same “Passphrase” must be entered when configuring the corresponding Signaling Group on the S8300 Media Server.

Signaling Group 26 will be associated with Trunk Group 26 in a subsequent step.

```
add signaling-group 26                                     Page 1 of 5
                                     SIGNALING GROUP
Group Number: 26      Group Type: h.323
Remote Office? n      Max number of NCA TSC: 0
SBS? n                Max number of CA TSC: 0
Trunk Group for Channel Selection:      Trunk Group for NCA TSC:
Supplementary Service Protocol: a      Network Call Transfer? n

Near-end Node Name: CLAN-EPN1      Far-end Node Name: S8300-in-G350
Near-end Listen Port: 1720      Far-end Listen Port: 1720
Far-end Network Region: 4
LRQ Required? n      Calls Share IP Signaling Connection? y
RRQ Required? n
Media Encryption? y      Bypass If IP Threshold Exceeded? n
Passphrase: *
DTMF over IP: in-band      Direct IP-IP Audio Connections? y
                                     IP Audio Hairpinning? y
                                     Interworking Message: PROGRESS
```

Next, a Trunk Group is established for calls to and from the S8300 Media Server. Most fields can be left to their defaults. Data has been entered in the fields shown in bold.

```

add trunk-group 26                                     Page 1 of 22
                                                    TRUNK GROUP
Group Number: 26          Group Type: isdn          CDR Reports: y
  Group Name: Encrypted-to-S8300-G350      COR: 1      TN: 1      TAC: 126
  Direction: two-way      Outgoing Display? y      Carrier Medium: IP
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

  Trunk Hunt: cyclical          QSIG Value-Added? n
                              Digital Loss Group: 18
Calling Number - Delete:      Insert:      Numbering Format:
  Bit Rate: 1200      Synchronization: async  Duplex: full
Disconnect Supervision - In? y  Out? n
Answer Supervision Timeout: 0

```

Page forward and add the members of the Trunk Group. When the members are initially added, the keyword “ip” is entered in the “Port” field (not illustrated), and the Signaling Group number is added in the “Sig Grp” field. After the members are added, subsequent displays of the screen will show an identifier in the “Port” field, as shown in the screen that follows. These logical Port identifiers for IP Trunks will be used in other types of screens, such as the status screens for active calls shown in Section 6. The number of rows or members added here will determine the number of simultaneous calls allowed on the IP Trunk Group linking the Avaya S8700 Media Server with the S8300 Media Server in Site C. The number of members should match on both sides of the Trunk Group.

```

display trunk-group 26                               Page 6 of 22
                                                    TRUNK GROUP
Administered Members (min/max): 1/4
GROUP MEMBER ASSIGNMENTS      Total Administered Members: 4

  Port      Code Sfx Name      Night      Sig Grp
1: T00096
2: T00097
3: T00098
4: T00099
5:
6:
.....

```

Next, the Signaling Group is associated with the Trunk Group. Using the command “change signaling-group 26”, enter the number 26 in the “Trunk Group for Channel Selection” field.

```

change signaling-group 26                                     Page 1 of 5
                                SIGNALING GROUP
Group Number: 26      Group Type: h.323
Remote Office? n      Max number of NCA TSC: 0
SBS? n                Max number of CA TSC: 0
                                Trunk Group for NCA TSC:
Trunk Group for Channel Selection: 26
Supplementary Service Protocol: a      Network Call Transfer? n

Near-end Node Name: CLAN-EPN1      Far-end Node Name: S8300-in-G350
Near-end Listen Port: 1720      Far-end Listen Port: 1720
                                Far-end Network Region: 4
LRQ Required? n      Calls Share IP Signaling Connection? y
RRQ Required? n
Media Encryption? y      Bypass If IP Threshold Exceeded? n
Passphrase: *
DTMF over IP: in-band      Direct IP-IP Audio Connections? y
                                IP Audio Hairpinning? y
                                Interworking Message: PROGRESS

```

4.6. Network Regions

The configuration of network region 1 is illustrated below. The “Codec Set” of Page 1 is set to “1”. Therefore, Codec Set 1 will be used for intra-region calls among devices at Site A. Per the example objectives, Codec Set 1 will be configured to use G.711MU and AEA encryption in Section 4.7.

```

change ip-network-region 1                                   Page 1 of 19
                                IP NETWORK REGION
Region: 1
Location: 1      Home Domain:
Name: MCC1-in-lab
                                Intra-region IP-IP Direct Audio: yes
AUDIO PARAMETERS      Inter-region IP-IP Direct Audio: yes
Codec Set: 1      IP Audio Hairpinning? y
UDP Port Min: 2048
UDP Port Max: 3028      RTCP Reporting Enabled? y
                                RTCP MONITOR SERVER PARAMETERS
                                Use Default Server Parameters? y
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 34
Audio PHB Value: 46
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 7
Audio 802.1p Priority: 6      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

```

On Page 3, the codec-set to use for connections from region 1 to other regions is configured. Recall that the G350 Media Gateway was defined in region 3. A “3” is entered in the “codec-set” column of the bolded row defining the region 1-3 connectivity. In Section 4.7, Codec Set 3 will be configured to achieve the objective to use G.729 and prefer to use AES, but allow AEA. Similarly, a “4” is entered in the “codec-set” column of the bolded row defining the region 1-4 connectivity. In Section 4.7, Codec Set 4 will be configured to achieve the objective to require G.729 and AES over the H.323 Trunk Group to the S8300 Media Server.

```

change ip-network-region 1                                     Page 3 of 19
                    Inter Network Region Connection Management
src dst
rgn rgn      codec-set  direct-WAN  WAN-BW-limits  Intervening-regions
1  1         1
1  2         1           Y           :NoLimit
1  3         3           Y           :NoLimit
1  4         4           Y           :NoLimit
1  5         5           Y           :NoLimit
1  6
.....

```

Once the network region connectivity for region 1 to region N is defined, the connectivity for region N to region 1 is automatically populated with the symmetric configuration.

The following screen illustrates the configuration for network region 3. Observe that calls within region 3 will use codec-set 1 (i.e., same as calls within region 1). Calls between region 3 (Site B) and region 4 (Site C) will use codec-set 4 (i.e., same as calls between region 1 and region 4).

```

change ip-network-region 3                                     Page 3 of 19
                    Inter Network Region Connection Management
src dst
rgn rgn      codec-set  direct-WAN  WAN-BW-limits  Intervening-regions
3  1         3           Y           :NoLimit
3  2         1           Y           :NoLimit
3  3         1
3  4         4           Y           :NoLimit
3  5
3  6
.....

```

4.7. Codec Sets

Codec Set 1 has been configured for intra-region connectivity in region 1. Per the objectives in Section 1, within region 1, the codec used is G.711MU, and AEA media encryption is preferred.

```

change ip-codec-set 1                                         Page 1 of 1
                    IP Codec Set

Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression  Per Pkt    Size(ms)
1: G.711MU      n           2          20
2:
3:
4:
5:
6:
7:

Media Encryption
1: aea
2: none
3:

```

Codec Set 3 has been configured for inter-region connectivity between region 1 and region 3 (Site B). Per the objectives, the codec to use is G.729, with AES media encryption preferred. AEA media encryption has also been allowed. AEA-only IP Telephones in region 1 will communicate securely with users in Region 3 using AEA.

```

change ip-codec-set 3                                     Page 1 of 1
                IP Codec Set
Codec Set: 3
Audio          Silence      Frames      Packet
Codec          Suppression  Per Pkt    Size(ms)
1: G.729          n           2          20
2:
3:
4:
5:
6:
7:

Media Encryption
1: aes
2: aea
3:

```

Codec Set 4 has been configured for inter-region connectivity between region 1 and region 4 (Site C). Per the objectives, the codec to use is G.729, with AES media encryption required. As will be illustrated further in Section 6, any AEA-only IP Telephones will automatically be serviced in a way fulfilling the objective to require AES over the WAN to the S8300. A media processing resource will automatically be inserted where necessary to allow any AEA-only devices to communicate using AEA within their region (i.e., on the LAN) while communicating using AES between regions (i.e., on the WAN).

```

change ip-codec-set 4                                     Page 1 of 1
                IP Codec Set
Codec Set: 4
Audio          Silence      Frames      Packet
Codec          Suppression  Per Pkt    Size(ms)
1: G.729          n           2          20
2:
3:
4:
5:
6:
7:

Media Encryption
1: aes
2:
3:

```

4.8. Call Routing

Traditional UDP call routing is established such that a dialed number 58xxx is routed to Trunk Group 26, passing the dialed 58xxx digits to the S8300 Media Server.

The command “save translation” must be entered to save configuration changes.

5. Avaya S8300 Media Server Configuration (Site C)

This section presents configuration steps for the Avaya S8300 Media Server in Site C.

5.1. Node Names

The following list command output illustrates a subset of the “node-names” that map logical names to IP addresses. These node names are presented because they will appear in other screens, such as the screens defining the IP interfaces and the H.323 Signaling Group to the S8700 Media Server. An S8300 Media Server has its “procr” interface defined through the web configuration screens that are outside the scope of this document.

```
list node-names
```

Type	Name	IP Address	
IP	CLAN_MultiCon	1 .1 .15 .20	# C-LAN at Site A
IP	procr	2 .2 .35 .88	# defined through Web interface

5.2. Communication Manager Configuration of the G350 Media Gateway in Site C

The following screen illustrates the Communication Manager configuration of the G350 Media Gateway in Site C. The screen was captured after the G350 Media Gateway had registered with the S8300 Media Server. Note that the “Encrypt Link” field (shown in bold) has been set to “y” to enable encryption of the H.248 signaling used to control the G350 Media Gateway. The Network Region has been shown in bold because these Application Notes present a means to control codec and media encryption behavior for intra-region and inter-region media paths.

```
change media-gateway 1
```

MEDIA GATEWAY		
Number: 1	IP Address: 2 .2 .35 .87	
Type: g350	FW Version/HW Vintage: 21 .20 .1 /49	
Name: G350-Right	MAC Address: 00:04:0d:29:c9:8d	
Serial No: 03IS07589449	Encrypt Link? y	
Network Region: 1	Location: 1	
Registered? y	Controller IP Address: 2 .2 .35 .88	
	Site Data:	
Slot	Module Type	Name
V1:	S8300	ICC MM
V2:		
V3:		
V4:		
V5:		
V6:	MM314	ETH 24P MM
V7:	virtual-analog	ANA VMM
V8:		
V9:	gateway-announcements	ANN VMM

5.3. H.323 Signaling Group and IP Trunk Group (to Site A)

This section focuses on the parameter settings of the H.323 Signaling Group and IP Trunk Group used to communicate with Site A. The media flowing over this path will use G.729 and AES media encryption.

Signaling Group 3 is created to establish an H.323 signaling link between the S8300 Media Server and the C-LAN in the MCC1 at Site A. The Signaling Group number is not relevant; use any available Signaling Group number.

This Signaling Group uses the node-name “procr” as the near end, and the node name corresponding to the C-LAN in the MCC1, “CLAN_MultiCon” as the far end. Retain the default near-end listen port (1720) and enter 1720 as the far-end listen port. The “Far-end Network Region” is set to “3” so that the codec set and encryption behavior can be uniquely controlled for calls using this Signaling Group. The “Media Encryption” field is set to “y”, and a password is entered in the “Passphrase” field. The “Passphrase” must match the one entered in Section 4.5, where the corresponding Signaling Group on the S8700 Media Server is described.

Signaling Group 3 will be associated with Trunk Group 3 in a subsequent step. Note that the number of the Signaling Group and the “Far-end Network Region” number need not be coordinated with the numbers used on the S8700 Media Server.

```
add signaling-group 3                                     Page 1 of 5
                                     SIGNALING GROUP
Group Number: 3           Group Type: h.323
Remote Office? n         Max number of NCA TSC: 0
SBS? n                   Max number of CA TSC: 0
                                     Trunk Group for NCA TSC:
Trunk Group for Channel Selection:
Supplementary Service Protocol: a
Near-end Node Name: procr           Far-end Node Name: CLAN_MultiCon
Near-end Listen Port: 1720         Far-end Listen Port: 1720
                                     Far-end Network Region: 3
LRQ Required? n         Calls Share IP Signaling Connection? y
RRQ Required? n
Media Encryption? y           Bypass If IP Threshold Exceeded? n
Passphrase: *
DTMF over IP: in-band   Direct IP-IP Audio Connections? y
                                     IP Audio Hairpinning? y
                                     Interworking Message: PROgress
```

Next, a Trunk Group is established for calls to and from the S8700 Media Server. The Media Encryption feature does not change the Trunk Group configuration procedure. Most fields can be left to their defaults. Particularly relevant fields are shown in bold.

```

add trunk-group 3                                     Page 1 of 22
                                                    TRUNK GROUP
Group Number: 3                                     Group Type: isdn          CDR Reports: y
  Group Name: Encrypt-To-S8700-Multi                COR: 1                   TN: 1          TAC: 103
  Direction: two-way                                Outgoing Display? y     Carrier Medium: IP
  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

  Trunk Hunt: cyclical                               QSIG Value-Added? n
                                                    Digital Loss Group: 18
Calling Number - Delete:      Insert:          Numbering Format:
  Bit Rate: 1200              Synchronization: async  Duplex: full
Disconnect Supervision - In? y Out? n
Answer Supervision Timeout: 0

```

Page forward and add the members. When the members are initially added, the keyword “ip” is entered in the “Port” field (not illustrated), and the Signaling Group number is added in the “Sig Grp” field. After the members are added, subsequent displays of the screen will show an identifier in the “Port” field, as shown in the screen below. These logical Port identifiers for IP Trunks will be used in other types of screens, such as the status screens for active calls shown in Section 6. The number of rows or members added here will determine the number of simultaneous calls allowed on the IP Trunk Group linking the Avaya S8300 Media Server with the S8700 Media Server. The number of members should match on both sides of the Trunk Group.

```

display trunk-group 3                               Page 6 of 22
                                                    TRUNK GROUP
Administered Members (min/max): 1/4
GROUP MEMBER ASSIGNMENTS                          Total Administered Members: 4

  Port      Code Sfx Name      Night      Sig Grp
1: T00009
2: T00010
3: T00011
4: T00012
5:
6:
.....

```

Next, the Signaling Group is associated with the Trunk Group. Using the command “change signaling-group 3”, enter the number 3 in the “Trunk Group for Channel Selection” field.

```

change signaling-group 3                                     Page 1 of 5
                                SIGNALING GROUP
Group Number: 3      Group Type: h.323
                    Remote Office? n      Max number of NCA TSC: 0
                    SBS? n                Max number of CA TSC: 0
                                           Trunk Group for NCA TSC:
Trunk Group for Channel Selection: 3
    Supplementary Service Protocol: a
    Near-end Node Name: procr              Far-end Node Name: CLAN_MultiCon
    Near-end Listen Port: 1720             Far-end Listen Port: 1720
                                           Far-end Network Region: 3
    LRQ Required? n                        Calls Share IP Signaling Connection? y
    RRQ Required? n
    Media Encryption? y                    Bypass If IP Threshold Exceeded? n
    Passphrase: *
    DTMF over IP: in-band                  Direct IP-IP Audio Connections? y
                                           IP Audio Hairpinning? y
                                           Interworking Message: PROGRESS

```

5.4. Network Regions

The configuration of network region 1 is illustrated with the following screens. The “Codec Set” on Page 1 is set to “1”. Codec Set 1 will be used for intra-region calls among devices at Site C.

```

change ip-network-region 1                                 Page 1 of 19
                                IP NETWORK REGION
    Region: 1
Location: 1      Home Domain:
    Name: S8300-in-G350
                                Intra-region IP-IP Direct Audio: yes
                                Inter-region IP-IP Direct Audio: yes
                                IP Audio Hairpinning? y
AUDIO PARAMETERS
Codec Set: 1
UDP Port Min: 2048
UDP Port Max: 3028
                                RTCP Reporting Enabled? y
                                RTCP MONITOR SERVER PARAMETERS
                                Use Default Server Parameters? y
DIFFSERV/TOS PARAMETERS
    Call Control PHB Value: 34
    Audio PHB Value: 46
802.1P/Q PARAMETERS
    Call Control 802.1p Priority: 7
    Audio 802.1p Priority: 6
                                AUDIO RESOURCE RESERVATION PARAMETERS
                                RSVP Enabled? n
H.323 IP ENDPOINTS
    H.323 Link Bounce Recovery? y
    Idle Traffic Interval (sec): 20
    Keep-Alive Interval (sec): 5
    Keep-Alive Count: 5

```

On Page 3, the codec-set to use for inter-region calls from region 1 to other regions is configured. Recall that the far-end of the Signaling Group to the S8700 Media Server was configured to be region 3. A “3” is entered in the “codec-set” column of the bolded row defining the region 1-3 connectivity. Codec Set 3 will be configured to achieve the objective to require G.729 and AES over the H.323 Trunk Group to the S8700 Media Server. Note that the codec set number need not match the configuration on the S8700 Media Server.

```

change ip-network-region 1                                     Page 3 of 19
                    Inter Network Region Connection Management
src dst
rgn rgn      codec-set  direct-WAN  WAN-BW-limits  Intervening-regions
1  1         1
1  2         2             y          :NoLimit
1  3         3             y          :NoLimit
.....

```

5.5. Codec Sets

```

change ip-codec-set 1                                       Page 1 of 1
                    IP Codec Set
Codec Set: 1
Audio      Silence      Frames      Packet
Codec      Suppression   Per Pkt    Size(ms)
1: G.711MU      n           2          20
2:
3:
4:
5:
6:
7:
Media Encryption
1: aea
2: none
3:

```

Codec Set 3 has been configured for inter-region connectivity between region 1 and region 3. Per the objectives, the codec to use is G.729, with AES media encryption required. As illustrated in Section 6, any AEA-only IP Telephones will be serviced in a way that fulfills the objective to require AES over the WAN to Site A. Media processors will automatically be inserted where necessary to allow any AEA-only devices to communicate using AEA within their region (i.e., on the LAN) while communicating using AES between regions (i.e., on the WAN).

```

change ip-codec-set 3                                       Page 1 of 1
                    IP Codec Set
Codec Set: 3
Audio      Silence      Frames      Packet
Codec      Suppression   Per Pkt    Size(ms)
1: G.729        n           2          20
2:
3:
4:
5:
6:
7:
Media Encryption
1: aes
2:
3:

```

5.6. Call Routing

Traditional UDP call routing is established such that a dialed number 57xxx is routed to Trunk Group 3, passing the dialed 57xxx digits to the S8700 Media Server.

The command “save translation” must be entered to save configuration changes.

6. Verify Connectivity

The configuration described herein has been verified extensively. The following subsections illustrate in detail the expected behavior using the configuration presented in these Application Notes. Each end-user device listed in **Table 1** has at least one call status screen included in the sections below. The initial sections present greater details for completeness. Subsequent sections omit screen captures for status pages that are not necessary to understand the behavior.

6.1. Local Intra-Region Calls at Site A (S8700 Site)

This section shows detailed status screens for calls between users at the S8700 Site. Per the example objectives implemented in these Application Notes, such a call will use G.711MU with AEA media encryption.

6.1.1. Call Between an Avaya IP Telephone (4620) and a non-IP Telephone

The following screens show details for a call involving an Avaya 4620 IP Telephone with extension 57041 and an Avaya DCP Telephone (6408D, but phone type is not relevant) with extension 57021 on port 1B1701.

status station 57041		Page 1 of 6
GENERAL STATUS		
Administered Type: 4620	Service State: in-service/off-hook	
Connected Type: 4620	Parameter Download: complete	
Extension: 57041	SAC Activated? no	
Port: S00008	User Cntrl Restr: none	
Call Parked? no	Group Cntrl Restr: none	
Ring Cut Off Act? no	CF Destination Ext:	
Active Coverage Option: 1		
EC500 Status: N/A	Off-PBX Service State: N/A	
Message Waiting:		
Connected Ports: 01B1701		

From Page 3, observe the phone is registered to the C-LAN with IP Address 1.1.15.20, and is considered to be in network region 1. Since the call includes an IP Telephone and a non IP-Telephone, it will require a media processing resource. The TN2302 with IP address 1.1.15.18, also in network region 1, is chosen. Note that the G.711MU codec is in use.

```

status station 57041                                     Page 3 of 6
                CALL CONTROL SIGNALING
                Switch      IP      IP
                Port      Switch-end IP Addr:Port  Set-end IP Addr:Port
IP Signaling: 01A0517  1. 1. 15. 20  :1720  1. 1. 4.111:3694
                H.245:
                Node Name:      CLAN-EPN1
Network Region:      1              1
                AUDIO CHANNEL
                Switch      IP      IP
                Port      Other-end IP Addr :Port  Set-end IP Addr:Port
G.711MU  Audio: 01A0607  1. 1. 15. 18  :2172  1. 1. 4.111:2546
                Node Name:      EPN1-PROWL1
Network Region:      1              1
                Audio Connection Type: ip-tdm
                Product ID and Release: IP_Phone 2. 0

```

From Page 5, observe AEA encryption is used between the Avaya IP Telephone and the TN2302 media processing resource.

```

status station 57041                                     Page 5 of 6
                CONNECTED PORTS
                src port: S00008
                MP      HP
ip-start:  1. 1. 4.111:2546
ip-end:    1. 1. 15. 18:2172  01A0607
audio: G.711MU      encryption:aea  ss:off  pkt:20ms
                dst port: 01B1701

```

6.1.2. Call Between Avaya 4620 and Avaya 4624 IP Telephones

The following screens show details for a call involving an Avaya 4620 IP Telephone with extension 57041 and an Avaya 4624 Telephone with extension 57042.

```

status station 57042                                     Page 1 of 5
                GENERAL STATUS
Administered Type: 4624      Service State: in-service/off-hook
Connected Type: 4624      Parameter Download: complete
Extension: 57042      SAC Activated? no
Port: S00004      User Cntrl Restr: none
Call Parked? no      Group Cntrl Restr: none
Ring Cut Off Act? no  CF Destination Ext:
Active Coverage Option: 1
                EC500 Status: N/A      Off-PBX Service State: N/A
                Message Waiting:
Connected Ports: S00008

```

From Page 3, observe the phone (1.1.1.33) is registered to the C-LAN with IP Address 1.1.15.20, and is considered to be in network region 1. Since the call is between two IP Telephones, the media can flow directly between the IP Telephones. Note that the G.711MU codec is in use.

```

status station 57042                                     Page 3 of 5
                CALL CONTROL SIGNALING
                Switch      IP
                Port      Switch-end IP Addr:Port  Set-end IP Addr:Port
IP Signaling: 01A0517    1. 1. 15. 20 :1720    1. 1. 1. 33:5696
                H.245:
                Node Name:      CLAN-EPN1
Network Region:      1                1
                AUDIO CHANNEL
                Switch      IP
                Port      Other-end IP Addr :Port  Set-end IP Addr:Port
G.711MU   Audio:      1. 1. 4.111 :2546    1. 1. 1. 33:2424
                Node Name:
Network Region:      1                1
                Audio Connection Type: ip-direct
                Product ID and Release: IP_Phone 1.800

```

From Page 4, observe the use of AEA encryption between the two Avaya IP Telephones.

```

status station 57042                                     Page 4 of 5
                CONNECTED PORTS
                src port: S00004
                MP      HP
ip-start:  1. 1. 1. 33:2424
ip-end:    1. 1. 4.111:2546
audio: G.711MU      encryption:aea  ss:off  pkt:20ms
                dst port: S00008

```

6.1.3. Call Between an Avaya IP Telephone (4620) and IP Softphone for Pocket PC

The Avaya IP Softphone for Pocket PC supports G.711 and AEA encryption. The following screen shows the Avaya IP Softphone for Pocket PC registered as extension 57063. Observe the background color where the text “57063 Registered” appears.



When the IP Softphone for Pocket PC is involved in a call using AEA encryption, the background color changes to green as illustrated below.



This background color is not changed to green unless media encryption is in use.

The following screen shows the S8700 Media Server SAT screen for this same encrypted call involving the IP Softphone for Pocket PC (x57063, IP address 1.1.9.5) and the 4620 IP Telephone (x57041, IP address 1.1.4.111). Observe the “ip-direct” media path from the 4620 to the IP Softphone for Pocket PC using G.711MU and AEA encryption.

```
status station 57063                                     Page 4 of 5
                                     CONNECTED PORTS
src port: S00010
                                     MP      HP
ip-start: 1. 1. 9. 5:2048
ip-end:   1. 1. 4.111:2654
audio: G.711MU      encryption:aea  ss:off  pkt:20ms
dst port: S00008
```

6.2. Local Intra-Region Call at Site C (Avaya 4612 and Avaya 4610)

This section shows status screens for an active call between two IP Telephone users at Site C. Per the example objectives implemented in these Application Notes, such a call will use G.711MU with AEA media encryption. The behavior for local calls at Site C is the same as the behavior for local calls at Site A (presented in Section 6.1). Therefore, details for calls involving other types of local devices are not presented.

The following screens show a call between an Avaya 4612 IP Telephone (2.2.35.200) with extension 58040 and an Avaya 4610 Telephone (2.2.35.201) with extension 58002.

```
status station 58040                                     Page 1 of 5
                                     GENERAL STATUS
Administered Type: 4612      Service State: in-service/off-hook
Connected Type: 4612        Parameter Download: complete
Extension: 58040            SAC Activated? no
Port: S00000                User Cntrl Restr: none
Call Parked? no            Group Cntrl Restr: none
Ring Cut Off Act? no       CF Destination Ext:
Active Coverage Option: 1
EC500 Status: enabled      Off-PBX Service State: in-service/idle
Message Waiting:
Connected Ports: S00009
```

From Page 4, observe the use of the AEA encryption algorithm, with the media flowing directly between the two Avaya IP Telephones.

```

status station 58040                                     Page 4 of 5
                CONNECTED PORTS
    src port: S00000
                MP      HP
ip-start:  2.  2. 35.200:2510
ip-end:    2.  2. 35.201:2610
  audio: G.711MU      encryption:aea  ss:off  pkt:20ms
                dst port: S00009

```

6.3. Calls Between Site A and Site B (G350 Site Controlled by S8700)

This section shows detailed status screens for calls between users at the S8700 Site (Site A) and users at the site with the G350 that is controlled by the S8700 (Site B). Per the example objectives, such calls will use G.729, with either AES or AEA media encryption used “over the WAN”, according to the native capabilities of the devices involved in the connection.

6.3.1. Call Between a non-IP Telephone at each site

The following screens show details for a call involving an Avaya DCP Telephone at Site A and an Avaya DCP Telephone connected to port 1V601 on the G350 Media Gateway at Site B. Only the most relevant status page is shown, since prior sections have illustrated the more detailed screens. Note that the call uses the G.729 codec and AES media encryption, between the TN2302 Media Processor (1.1.15.18) at Site A and the integrated media processing resources on the G350 Media Gateway (2.2.135.87) at Site B. The call uses AES because AES is the preferred encryption algorithm, per the sample objectives, and both media processors are capable of AES. Any call between sites that involves two non-IP end user devices will use G.729 and AES.

```

status station 57021                                     Page 3 of 4
                CONNECTED PORTS
    src port: 01B1701
                MP      HP
ip-start:  1.  1. 15. 18:2316      01A0604
ip-end:    2.  2.135. 87:2052      001V102
  audio: G.729      encryption:aes  ss:off  pkt:20ms
                dst port: 001V601

```

6.3.2. Call Between an AES-capable Avaya IP Telephone (4630) or Avaya IP Softphone at Site A and a Non-IP Telephone at Site B

The following screens show a call involving an Avaya 4630 IP Telephone (1.1.1.120) with extension 57043 at Site A, and a digital Telephone at Site B.

```

status station 57043                                     Page 1 of 6
GENERAL STATUS
Administered Type: 4630                               Service State: in-service/off-hook
Connected Type: 4630                                 Parameter Download: complete
Extension: 57043                                     SAC Activated? no
Port: S00011                                         User Cntrl Restr: none
Call Parked? no                                     Group Cntrl Restr: none
Ring Cut Off Act? no                               CF Destination Ext:
Active Coverage Option: 1

EC500 Status: N/A                                   Off-PBX Service State: N/A
Message Waiting:
Connected Ports: 001V601

```

From Page 3, observe the IP Telephone's registration and firmware version.

```

status station 57043                                     Page 3 of 6
CALL CONTROL SIGNALING
Switch IP IP
Port Switch-end IP Addr:Port Set-end IP Addr:Port
IP Signaling: 01A0517 1. 1. 15. 20 :1720 1. 1. 1.120:3190
H.245:
Node Name: CLAN-EPN1
Network Region: 1 1
AUDIO CHANNEL
Switch IP IP
Port Other-end IP Addr :Port Set-end IP Addr:Port
G.729A Audio: 1 2. 2.135. 87 :2084 1. 1. 1.120:2946
Node Name: G350-2-Right
Network Region: 3 1
Audio Connection Type: ip-tdm
Product ID and Release: IP_Phone 2. 0

```

From Page 5, observe the use of G.729 and AES encryption between the Avaya 4630 IP Telephone (1.1.1.120) and the integrated media processing resources on the G350 Media Gateway (2.2.135.87) at Site B. The call uses AES because AES is configured as the preferred encryption algorithm, and the Avaya 4630 IP Telephone, running 2.0 firmware, is capable of AES encryption.

```

status station 57043                                     Page 5 of 6
CONNECTED PORTS
src port: S00011
MP HP
ip-start: 1. 1. 1.120:2946
ip-end: 2. 2.135. 87:2084 001V103
audio: G.729A encryption:aes ss:off pkt:20ms
dst port: 001V601

```

The following screens are presented to show that an Avaya IP Softphone is also capable of AES encryption. Note from Page 3 the Product ID of "IP_Soft". The Avaya IP Softphone ("road warrior" mode) at Site A is in a call with the DCP Telephone connected to port 1v601 of the G350 Media Gateway at Site B.

```

status station 57062                                     Page 3 of 6
                CALL CONTROL SIGNALING
                Switch      IP
                Port      Switch-end IP Addr:Port      Set-end IP Addr:Port
IP Signaling: 01A0517      1. 1. 15. 20      :1720      1. 1. 1. 20:28305
H.245:
Node Name:      CLAN-EPN1
Network Region: 1
                AUDIO CHANNEL
                Switch      IP
                Port      Other-end IP Addr :Port      Set-end IP Addr:Port
G.729A      Audio: 1      2. 2.135. 87      :2074      1. 1. 1. 20:2048
Node Name:      G350-2-Right
Network Region: 3
Audio Connection Type: ip-tdm
Product ID and Release: IP_Soft      5.500

```

Once again, from Page 5, observe the use of G.729 and AES encryption between the PC running the Avaya IP Softphone (1.1.1.20) and the integrated media processing resources on the G350 Media Gateway (2.2.135.87) at Site B. The call uses AES because AES has been configured as the preferred encryption algorithm, and the Avaya IP Softphone, running 5.05 software, is capable of the AES encryption algorithm.

```

status station 57062                                     Page 5 of 6
                CONNECTED PORTS
                src port: S00003
                MP      HP
ip-start:      1. 1. 1. 20:2048
ip-end:        2. 2.135. 87:2074      001V102
audio: G.729A      encryption:aes      ss:off      pkt:20ms
                dst port: 001V601

```

6.3.3. Call Between an AEA-only Avaya IP Telephone (4624) at Site A and a DCP Telephone at Site B

The following screens show details for a call involving an Avaya 4624 IP Telephone at Site A with extension 57042 and an Avaya DCP Telephone connected to port 1v601 of the G350 Media Gateway at Site B.

```

status station 57042                                     Page 3 of 6
                CALL CONTROL SIGNALING
                Switch      IP
                Port      Switch-end IP Addr:Port      Set-end IP Addr:Port
IP Signaling: 01A0517      1. 1. 15. 20      :1720      1. 1. 1. 33:5696
H.245:
Node Name:      CLAN-EPN1
Network Region: 1
                AUDIO CHANNEL
                Switch      IP
                Port      Other-end IP Addr :Port      Set-end IP Addr:Port
G.729A      Audio: 1      2. 2.135. 87      :2066      1. 1. 1. 33:2424
Node Name:      G350-2-Right
Network Region: 3
Audio Connection Type: ip-tdm
Product ID and Release: IP_Phone      1.800

```

From Page 5, observe the use of G.729 and AEA encryption between the Avaya 4624 IP Telephone and the integrated media processing resources on the G350 Media Gateway (2.2.135.87) at Site B. Since the Avaya 4624 IP Telephone, running 1.8 firmware, is capable of the AEA encryption algorithm, but not the AES encryption algorithm, Communication Manager establishes the connection to the remote G350 media processor using AEA.

```

status station 57042                                     Page 5 of 6
                                     CONNECTED PORTS
      src port: S00004
                                     MP      HP
ip-start: 1. 1. 1. 33:2424
ip-end:   2. 2.135. 87:2066      001V102
  audio: G.729A      encryption:aea  ss:off  pkt:20ms
                                     dst port: 001V601

```

6.4. Calls Between S8700 Site and S8300 Site over the IP Trunk Group

This section illustrates the behavior of representative calls between Sites A and Site C over the IP Trunk Group. The sample objectives require such calls to use G.729 and the AES encryption algorithm over the WAN.

6.4.1. Call involving an AES-capable IP Telephone (4620) in Site A and an AES-capable IP Telephone (4610) in Site C

The following screens show details for a call involving two Avaya IP Telephones that are capable of AES media encryption. One is the Avaya 4620 IP Telephone with extension 57041 registered with the S8700 in Site A, presented previously. The other is an Avaya 4610 IP Telephone (2.2.35.201) with extension 58002, registered with the S8300 Media Server in Site C. Although the behavior of this call could be captured from either server, the first screens are captured from the S8300 Media Server, since all prior screens have been from the S8700 Media Server. From Page 3 below, observe that the call is considered a call between region 1 and region 3, because the far-end of the Signaling Group defined on the S8300 Media Server has been configured to be region 3.

```

status station 58002                                     Page 3 of 5
                                     CALL CONTROL SIGNALING
Switch                               IP
Port                               Switch-end IP Addr:Port   Set-end IP Addr:Port
IP Signaling: PROCR                 2. 2. 35. 88   :1720           2. 2. 35.201:4069
H.245:
Node Name:
Network Region:                     1                               1
                                     AUDIO CHANNEL
Switch                               IP
Port                               Other-end IP Addr :Port   Set-end IP Addr:Port
G.729A   Audio:                     1. 1. 4.111   :2546           2. 2. 35.201:2610
Node Name:
Network Region:                     3                               1
Audio Connection Type: ip-direct
Product ID and Release: IP_Phone 2. 0

```

From Page 4, observe the use of G.729 and AES encryption, with the media flowing directly between the Avaya 4610 IP Telephone and the Avaya 4620 IP Telephone.

```

status station 58002                                     Page 4 of 5
                                     CONNECTED PORTS
src port: S00009
MP      HP
ip-start: 2. 2. 35.201:2610
ip-end:   1. 1. 4.111:2546
audio: G.729A      encryption:aes  ss:off  pkt:20ms
dst port: T00009

```

An alternate way to observe the call behavior for a call involving a Trunk Group is to use the “status trunk” command, as illustrated below from the S8700 Media Server.

```

status trunk 26/2                                       Page 1 of 2
                                     TRUNK STATUS
Trunk Group/Member: 0026/002           Service State: in-service/active
Port: T00097                           Maintenance Busy? no
Signaling Group ID:                    CA-TSC state: not allowed
Connected Ports: S00008

Port      Near-end IP Addr : Port   Far-end IP Addr : Port
Signaling: 01A0517   1. 1. 15. 20   : 11364       2. 2. 35. 88   : 1720
H.245:
G.729   Audio:       1. 1. 4.111   : 2546       2. 2. 35.201   : 2610
H.245 Tunneled in Q.931? no
Audio Connection Type: ip-direct

```

Page 2 shows the use of the AES encryption algorithm.

```

status trunk 26/2                                       Page 2 of 2
                                     CONNECTED PORTS
src port: T00097
MP      HP
ip-start: 2. 2. 35.201:2610
ip-end:   1. 1. 4.111:2546
audio: G.729      encryption:aes  ss:off  pkt:20ms
dst port: S00008

```

6.4.2. Call involving an AES-capable IP Telephone (4620) in Site A and an AEA-only IP Telephone (4612) in Site C

This section illustrates the behavior when an IP Telephone that is not capable of the AES media encryption needs to communicate across the H.323 Signaling Group and IP Trunk Group that has been configured to require AES via the codec set administration. In this case, an Avaya 4612 IP Telephone (2.2.35.200), running 1.8 firmware, with extension 58040 on the S8300 Media Server, is communicating with an Avaya 4620 IP Telephone registered to the S8700 Media Server at Site A. The following screens are from the S8300 Media Server.

```

status station 58040                                     Page 3 of 6
                                     CALL CONTROL SIGNALING
Switch IP
Port Switch-end IP Addr:Port Set-end IP Addr:Port
IP Signaling: PROCR 2. 2. 35. 88 :1720 2. 2. 35.200:4069
H.245:
Node Name:
Network Region: 1 1
                                     AUDIO CHANNEL
Switch IP
Port Other-end IP Addr :Port Set-end IP Addr:Port
G.711MU Audio: 1 2. 2. 35. 87 :2088 2. 2. 35.200:2510
Node Name:
Network Region: 1 1
Audio Connection Type: ip-tdm
Product ID and Release: IP_Phone 1.800

```

From Page 5, observe that a G.711MU connection is established between the 4612 IP Telephone (2.2.35.200) and a media processing resource on the local G350 Media Gateway (2.2.35.87). This intra-region connection uses G.711MU and AEA encryption. Across the “WAN”, a media processing resource on the G350 Media Gateway (2.2.35.87) is communicating using G.729 and AES encryption directly to the AES-capable Avaya 4620 IP Telephone whose IP Address is 1.1.4.111.

```

Status station 58040                                     Page 5 of 6
                                     CONNECTED PORTS
src port: S00000
MP HP
ip-start: 2. 2. 35.200:2510
ip-end: 2. 2. 35. 87:2088 001V105
audio: G.711MU encryption:aea ss:off pkt:20ms
ip-start: 2. 2. 35. 87:2084 001V104
ip-end: 1. 1. 4.111:2546
audio: G.729 encryption:aes ss:off pkt:20ms
dst port: T00009

```

From the S8700 Media Server, this same call appears as an “ip-direct” connection from the local AES-capable Avaya 4620 IP Telephone (1.1.4.111) to the media processing resource on the G350 Media Gateway (2.2.35.87) using G.729 and AES over the IP Trunk (T00097).

```

status station 57041                                     Page 4 of 5
                                     CONNECTED PORTS
src port: S00008
                                     MP      HP
ip-start: 1. 1. 4.111:2546
ip-end:   2. 2. 35. 87:2084
audio: G.729A      encryption:aes  ss:off  pkt:20ms
dst port: T00097

```

6.4.3. Call involving an AES-capable IP Telephone (4610) at Site C and an AEA-only IP Telephone (4624) at Site A

This section is much like the prior, except that in this case, the IP Telephone (57042) that is incapable of AES is located at Site A. Fundamentally, the resulting behavior is the same. The Media Server with the non-AES capable phone will insert a media processor so that the configured requirement for AES communication over the IP Trunk Group is honored. The following screens show the status from the S8700 Media Server.

```

status station 57042                                     Page 3 of 6
                                     CALL CONTROL SIGNALING
Switch      IP      IP
Port        Switch-end IP Addr:Port  Set-end IP Addr:Port
IP Signaling: 01A0517  1. 1. 15. 20 :1720  1. 1. 1. 33:5696
H.245:
Node Name:    CLAN-EPN1
Network Region: 1
                                     AUDIO CHANNEL
Switch      IP      IP
Port        Other-end IP Addr :Port  Set-end IP Addr:Port
G.711MU      Audio: 01A0605  1. 1. 15. 18 :2596  1. 1. 1. 33:2424
Node Name:    EPN1-PROWL1
Network Region: 1
Audio Connection Type: ip-tdm
Product ID and Release: IP_Phone 1.800

```

From Page 5, observe that a G.711MU connection is established between the 4624 IP Telephone (1.1.1.33) and a local media processing resource (1.1.15.18). This intra-region connection uses G.711MU and the AEA encryption algorithm. Across the “WAN” and IP Trunk, another local media processing resource is communicating using G.729 and AES encryption directly to the AES-capable Avaya 4610 IP Telephone (2.2.35.201) over the IP Trunk (T00096).

```

status station 57042                                     Page 5 of 6
                                     CONNECTED PORTS
src port: S00004
                                     MP      HP
ip-start: 1. 1. 1. 33:2424
ip-end:   1. 1. 15. 18:2596      01A0605
audio: G.711MU      encryption:aea  ss:off  pkt:20ms
ip-start: 1. 1. 15. 18:2592      01A0606
ip-end:   2. 2. 35.201:2610
audio: G.729      encryption:aes  ss:off  pkt:20ms
dst port: T00096

```

As illustrated below, from the S8300 Media Server, this same call appears as an “ip-direct” connection from the local AES-capable Avaya 4610 IP Telephone (2.2.35.201) to the media processing resource at Site A (1.1.15.18) using G.729 and AES over the IP Trunk (T00011).

```

status station 58002                                     Page 4 of 5
                CONNECTED PORTS
    src port: S00009
                MP      HP
ip-start: 2. 2. 35.201:2610
ip-end: 1. 1. 15. 18:2592
audio: G.729A      encryption:aes  ss:off  pkt:20ms
                dst port: T00011
  
```

6.4.4. Call involving an AEA-only IP Telephone (4602SW / 1.8 Firmware) in Site C and an AES-capable IP Telephone (4620) in Site A

This section is similar to Section 6.4.2, except that in this case, a 4602SW IP Telephone running firmware version 1.8 is used in Site C, merely to show an example of a call using the 4602SW. The following screens show the status from the S8300 Media Server. Extension 58009 is a 4602SW (2.2.35.205) running firmware 1.8.

```

status station 58009                                     Page 1 of 6
                GENERAL STATUS
Administered Type: 4602      Service State: in-service/off-hook
Connected Type: 4602      Parameter Download: complete
Extension: 58009      SAC Activated? no
Port: S00005      User Cntrl Restr: none
Call Parked? no      Group Cntrl Restr: none
Ring Cut Off Act? no      CF Destination Ext:
Active Coverage Option: 1
                EC500 Status: N/A      Off-PBX Service State: N/A
                Message Waiting:
Connected Ports: T00009
  
```

From Page 3, observe the registration status of the IP Telephone as well as its firmware version.

```

status station 58009                                     Page 3 of 6
                CALL CONTROL SIGNALING
                Switch      IP      IP
                Port      Switch-end IP Addr:Port      Set-end IP Addr:Port
IP Signaling: PROCR      2. 2. 35. 88      :1720      2. 2. 35.205:4600
H.245:
Node Name:
Network Region: 1      1
                AUDIO CHANNEL
                Switch      IP      IP
                Port      Other-end IP Addr :Port      Set-end IP Addr:Port
G.711MU Audio: 1      2. 2. 35. 87      :2110      2. 2. 35.205:2388
Node Name:
Network Region: 1      1
Audio Connection Type: ip-tdm
Product ID and Release: IP_Phone 1.800
  
```

From Page 5, observe that a G.711MU connection is established between the 4602SW IP Telephone (2.2.35.205) and a local media processing resource (2.2.35.87). This intra-region connection uses G.711MU and the AEA encryption algorithm. Across the “WAN” and IP Trunk, another local media processing resource is communicating using G.729 and AES encryption directly to the AES-capable Avaya 4620 IP Telephone (1.1.4.111) over the IP Trunk (T00009).

```

status station 58009                                     Page 5 of 6
                CONNECTED PORTS
                src port: S00005
                MP      HP
ip-start:      2.  2. 35.205:2388                        001V102
ip-end:        2.  2. 35. 87:2110
audio: G.711MU      encryption:aea  ss:off  pkt:20ms
ip-start:      2.  2. 35. 87:2112                        001V103
ip-end:        1.  1.  4.111:2546
audio: G.729      encryption:aes   ss:off  pkt:20ms
                dst port: T00009

```

6.5. Calls Between Site B and Site C

Although no new concepts are illustrated, the status of calls between Site B and Site C are presented for completeness.

6.5.1. Call involving an AES-capable IP Telephone (4610 / 2.0 Firmware) in Site C and a Digital Phone in Site B

The following screen, captured from the S8700 Media Server, shows a call between a DCP phone at Site B (x57521) and the 4610 IP Telephone at Site C (x58002, IP Address 2.2.35.201). The resultant media path is “ip-direct” between the G350 Media Gateway (2.2.135.87) and the 4610 IP Telephone, using G.729 and AES.

```

status station 57521                                     Page 4 of 5
                CONNECTED PORTS
                src port: 001V601
                MP      HP
ip-start:      2.  2.135. 87:2102                        001V103
ip-end:        2.  2. 35.201:2106
audio: G.729      encryption:aes   ss:off  pkt:20ms
                dst port: T00097

```

The following screen from the S8700 Media Server illustrates the “status trunk” information for this same call. Note that the call from Site B to Site C can use the same H.323 Signaling Group and IP Trunk Group used for the calls previously illustrated from Site A to Site C.

```

status trunk 26/2                                     Page 3 of 3
                CONNECTED PORTS
                src port: T00097
                MP      HP
ip-start:      2. 2. 35.201:2106
ip-end:        2. 2.135. 87:2102                      001V103
audio: G.729      encryption:aes  ss:off  pkt:20ms
                dst port: 001V601

```

6.5.2. Call involving an AEA-only IP Telephone (4612 / 1.8 Firmware) in Site C and a Digital Phone in Site B

The following screen, captured from the S8700 Media Server, shows a call between a DCP phone at Site B (x57521) and the 4612 IP Telephone at Site C (x58040, IP Address 2.2.35.200). The connection uses G.729 and AES between the G350 Media Gateway in Site B (2.2.135.87) and the G350 Media Gateway in Site C (2.2.35.87). The G350 Media Gateway in Site C is inserted to allow the connection to use AES over the “WAN”.

```

status station 57521                                 Page 4 of 5
                CONNECTED PORTS
                src port: 001V601
                MP      HP
ip-start:      2. 2.135. 87:2106                      001V103
ip-end:        2. 2. 35. 87:2402
audio: G.729      encryption:aes  ss:off  pkt:20ms
                dst port: T00098

```

The following screen, captured from the S8300 Media Server, shows the same call. Observe the local connection between the AEA-only IP Telephone (2.2.35.200) and the G350 Media Gateway in Site C (2.2.35.87) using G.711MU and AEA encryption. Over the “WAN” using the IP Trunk, the connection uses G.729 and AES.

```

status station 58040                                 Page 5 of 6
                CONNECTED PORTS
                src port: S00000
                MP      HP
ip-start:      2. 2. 35.200:3016
ip-end:        2. 2. 35. 87:2406                      001V103
audio: G.711MU      encryption:aea  ss:off  pkt:20ms
ip-start:      2. 2. 35. 87:2402                      001V102
ip-end:        2. 2.135. 87:2106
audio: G.729      encryption:aes  ss:off  pkt:20ms
                dst port: T00009

```

6.6. Example of using Service Observing with Media Encryption

Even if the Media Encryption feature is used to enhance security, it is still possible to use other Communication Manager features to tap into the media stream where customer needs dictate. For example, the “service observing” feature is commonly used to observe agents in call centers, and service observing is also one approach used by call recording applications. The configuration of the “service observing” feature is outside the scope of these Application Notes. However, the following example illustrates the behavior when service observing is used.

The following is an example of a call that began as an intra-region “ip-direct” call between two of the Avaya IP Telephones at Site A that have been used throughout these examples. This initial status is illustrated from the S8700 Media Server below.

```
status station 57042                                     Page 4 of 5
                                     CONNECTED PORTS
src port: S00004
                                     MP      HP
ip-start: 1. 1. 1. 33:2424
ip-end:   1. 1. 4.111:2546
audio: G.711MU          encryption:aea  ss:off  pkt:20ms
dst port: S00008
```

Now, use the “service observing” feature to observe the call from station 57021 (port 1B1701), a DCP Telephone at Site A. The resultant connection is illustrated below.

```
status station 57041                                     Page 1 of 7
                                     GENERAL STATUS
Administered Type: 4620          Service State: in-service/off-hook
Connected Type: 4620            Parameter Download: complete
Extension: 57041                SAC Activated? no
Port: S00008                    User Cntrl Restr: none
Call Parked? no                Group Cntrl Restr: none
Ring Cut Off Act? no           CF Destination Ext:
Active Coverage Option: 1
EC500 Status: N/A              Off-PBX Service State: N/A
Message Waiting:
Connected Ports: 01B1701       S00004
```

The media path is changed from “ip-direct” to “ip-tdm” using the resources of a local media processor (1.1.15.18).

```

status station 57041                                     Page 3 of 7
                CALL CONTROL SIGNALING
                Switch IP
                Port Switch-end IP Addr:Port Set-end IP Addr:Port
IP Signaling: 01A0517 1. 1. 15. 20 :1720 1. 1. 4.111:3694
H.245:
Node Name: CLAN-EPN1
Network Region: 1 1
                AUDIO CHANNEL
                Switch IP
                Port Other-end IP Addr :Port Set-end IP Addr:Port
G.711MU Audio: 01A0603 1. 1. 15. 18 :2128 1. 1. 4.111:2546
Node Name: EPN1-PROWL1
Network Region: 1 1
Audio Connection Type: ip-tdm
Product ID and Release: IP_Phone 2. 0

```

All “IP legs” of the call can remain encrypted, as illustrated below.

```

status station 57041                                     Page 5 of 7
                CONNECTED PORTS
                src port: S00008
                MP HP
ip-start: 1. 1. 4.111:2546
ip-end: 1. 1. 15. 18:2128 01A0603
audio: G.711MU encryption:aea ss:off pkt:20ms
                dst port: 01B1701

```

Each IP Telephone’s connection to a media processor satisfies the objectives for encryption that have been configured for local intra-region connections (i.e., G.711MU and AEA encryption).

```

status station 57041                                     Page 6 of 7
                CONNECTED PORTS
                src port: S00008
                MP HP
ip-start: 1. 1. 4.111:2546
ip-end: 1. 1. 15. 18:2128 01A0603
audio: G.711MU encryption:aea ss:off pkt:20ms
ip-start: 1. 1. 15. 18:2124 01A0604
ip-end: 1. 1. 1. 33:2424
audio: G.711MU encryption:aea ss:off pkt:20ms
                dst port: S00004

```

The “service observing” feature behaves as usual. Here are status screens associated with the station doing the observing.

```

status station 57021                                     Page 1 of 5
                GENERAL STATUS
Administered Type: 6408D+                               Service State: in-service/off-hook
Connected Type: 6408D+                                 Parameter Download: complete
Extension: 57021                                       SAC Activated? no
                Port: 01B1701                          User Cntrl Restr: none
Call Parked? no                                       Group Cntrl Restr: none
Ring Cut Off Act? no                                  CF Destination Ext:
Active Coverage Option: 1

                EC500 Status: N/A                       Off-PBX Service State: N/A
Message Waiting:
Connected Ports: S00004                               S00008

```

The observing station can hear the other parties in the connection.

```

status station 57021                                     Page 3 of 5
                CONNECTED PORTS
                src port: 01B1701
                MP           HP
ip-start:      1. 1. 15. 18:2124                       01A0604
ip-end:        1. 1. 1. 33:2424
audio: G.711MU encryption:aea ss:off pkt:20ms

                dst port: S00004

```

All connections remain encrypted on the LAN.

```

status station 57021                                     Page 4 of 5
                CONNECTED PORTS
                src port: 01B1701
                MP           HP
ip-start:      1. 1. 15. 18:2128                       01A0603
ip-end:        1. 1. 4.111:2546
audio: G.711MU encryption:aea ss:off pkt:20ms

                dst port: S00008

```

7. Conclusion

As illustrated in these Application Notes, Avaya Communication Manager enables customers to enhance security for IP Telephony using the Media Encryption feature. Customers can satisfy varying security objectives for different parts of a network using a flexible and granular configuration approach. A network can logically be partitioned into different “network regions”, and encryption decisions can be controlled for connections within a given region, and for connections from a given region to any other region (i.e., similar to codec selection). If encryption is desired, a choice of encryption algorithms is provided. As illustrated in these Application Notes, Communication Manager evaluates the capabilities of the end devices in a connection and makes intelligent choices to honor the configured encryption requirements.

©2004 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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 interoplabinotes@list.avaya.com