Avaya Solution & Interoperability Test Lab

Application Notes for the Vocera Communications System with Avaya Communication Manager using T1Wink Start and PRI Interface - Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate the Vocera Communications System – Vocera Server, Telephony Server and badges, with Avaya Communication Manager, and Avaya Wireless AP-8.

Emphasis of the testing was placed on verifying reliable integration between the Vocera Telephony Server and Avaya Communication Manager, using the T1/PRI interface.

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

1. Introduction

The Vocera Communications Inc. (Vocera) system enables people to communicate over wireless 802.11b or 802.11g networks. Vocera users speak into a small lightweight wireless device, called a badge. Users communicate by pressing a call button on the badge and saying “key phrases” that the Vocera Server interprets and processes. The badge connects and communicates with other badge devices, or telephone endpoints on Avaya Communication Manger, or to a PSTN endpoint.

These Application Notes describe the configuration used to wirelessly communicate with the Vocera badges and to compliance test the features of the Vocera Communications system with Avaya Communication Manager and Avaya Wireless AP-8s.

1.1. Components

The following three components make up the Vocera Communications system:

- Vocera Badges
- Vocera Server
- Vocera Telephony Server

The Vocera Badges are wireless 802.11b or 802.11g devices that serve as communicators in a wireless environment. Pressing the call button on a badge opens an interface with the Vocera Server which starts the call process.

The Vocera Telephony Server acts as a communication server to service calls between the badge and an endpoint. The Vocera Server stores the user and badge information, and has a speech access interface that allows users to place and receive calls. See **Reference [3]**.

The Vocera Telephony Server connects to the Avaya Communication Server via a Dialogic Telephony hardware interface. Both T1 ISDN-PRI and T1 robbed-bit trunks were setup between the Server’s dialogic interface and Avaya Communication Manager. Calls between badges and Avaya Communication Manager telephones were connected and routed through these trunks. The two server applications, the Vocera Server and Vocera Telephony Server resided in the same physical server platform.

For additional information on the Vocera Communications System, please refer to Vocera documentation **References [4], [5], and [6]**.

Figure 1 illustrates the network configuration used to verify the Vocera Communications solution. The configuration details provided in these Application Notes focus on the interface between Avaya Communication Manager and the Vocera Telephony Server as well as the wireless configuration between the Vocera Badge, and Avaya Wireless AP-8. The configuration is comprised of an Avaya S8500 Media Server and an Avaya G650 Media Gateway, and has connections to Avaya telephones and an ISDN-PRI trunk to the PSTN. The Vocera site is comprised of a PC with Microsoft Windows 2003 Server and a Power Over Ethernet (POE) switch. The Vocera Server and Vocera Telephony Server were installed on the PC prior to the compliance test. Avaya Wireless AP-8s are utilized to provide the wireless network for the Vocera badges.

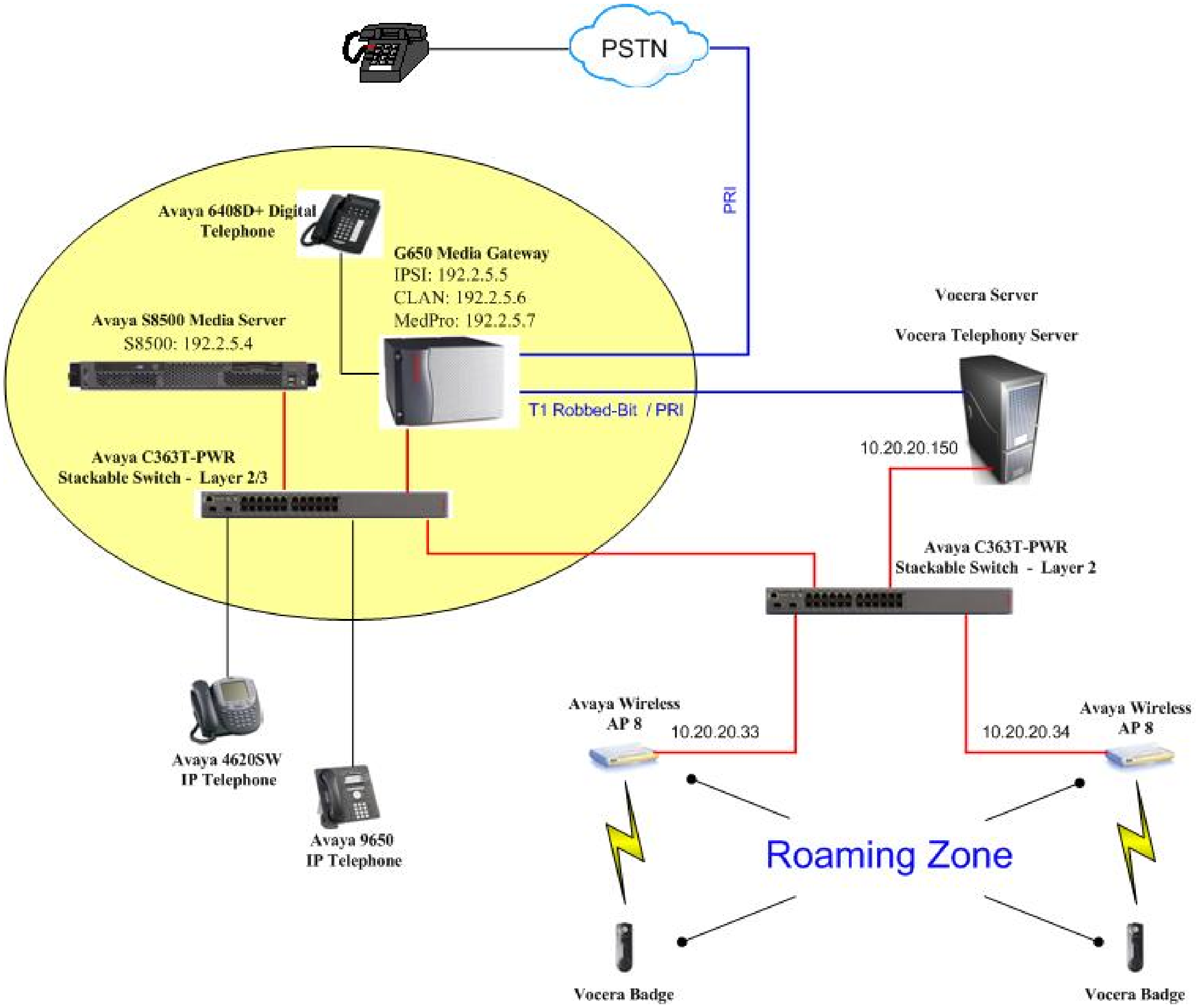


Figure 1 – Network Configuration Diagram

2. Equipment and Software Validated

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

Equipment		Software
Avaya S8500 Server		Avaya Communication Manager 5.0 (R015x.00.0.825.4)
Avaya G650 Media Gateway		
	TN2312BP IP Server Interface TN799DP C-LAN Interface TN2302AP IP Media Processor	HW15 FW030 HW01 FW012 HW20 FW110
Avaya 4625SW IP Telephone		2.8.3
Avaya 9650 IP Telephone		1.2 (H.323)
Avaya 6402 Digital Telephone		-
Avaya C363T-PWR Converged Stackable Switch		4.5.14
Avaya Wireless AP-8		3.4.0 (1146)
Vocera Server and Telephony Server running on Windows 2003 Server		4.0 build 1763
Vocera Badges		
	B1000A (802.11b only)	4.0 build 1763 B1000
	B2000 (802.11b and g)	4.0 build 1763 B2000

Table 1 – Product and Software Version

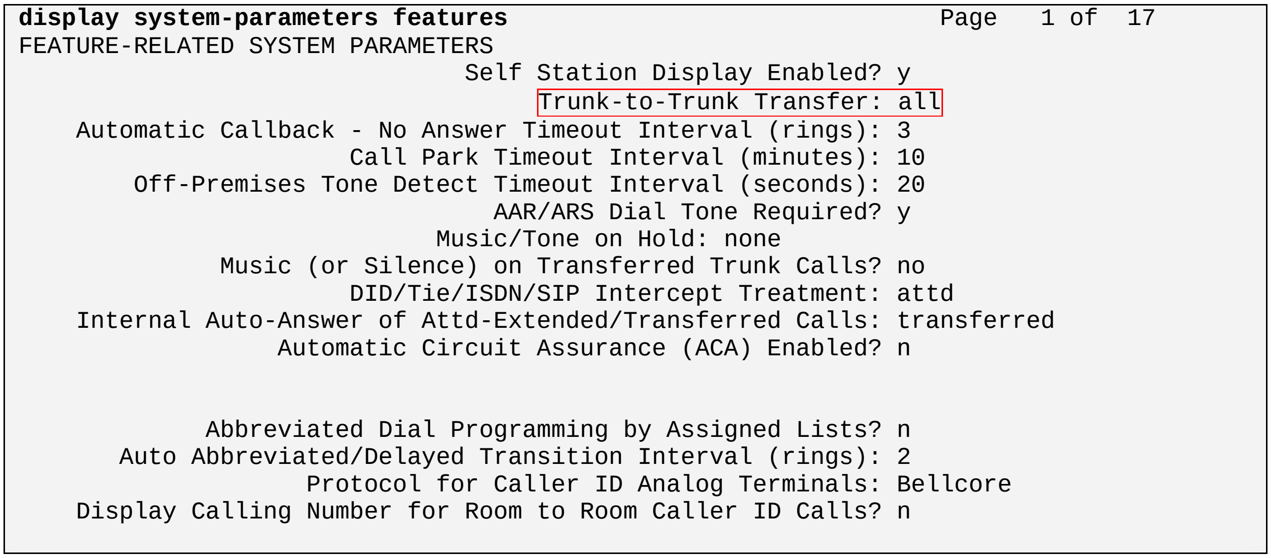
3. Configure Avaya Communication Manager

During the compliance test, the connectivity between Avaya Communication Manager and the Vocera Telephony Server were performed with T1 ISDN-PRI and T1 Wink Start protocols. Before configuring Avaya Communication Manager, the DS1 board must be physically configured to the appropriate T1mode.

When integrating with trunks, it is important to allow trunk-to-trunk transfer so badges can transfer/conference calls, as well as place outbound calls. Trunk to trunk transfer is a global parameter that is enabled in the “system-parameters features” form.

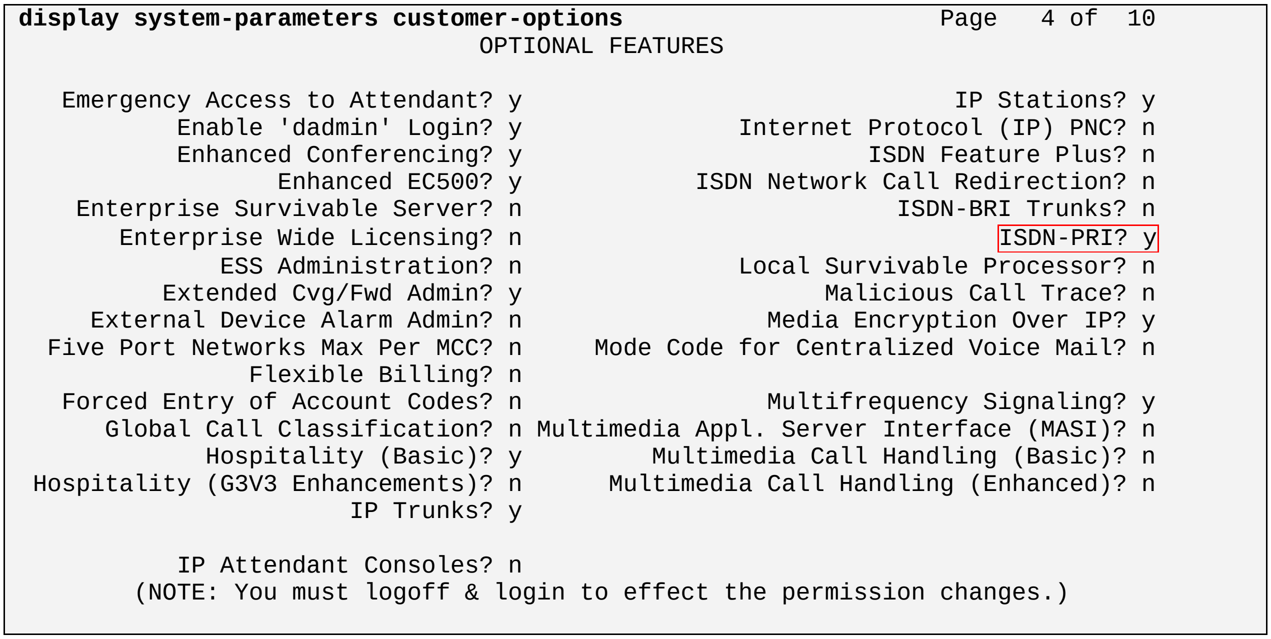
3.1. Configuring System Level Parameters

1. From the System Access Terminal interface enter the **display system-parameters features** command. On Page 1 of the “system-parameters feature” form, verify that the **Trunk-to-Trunk Transfer** field is set to **all**.



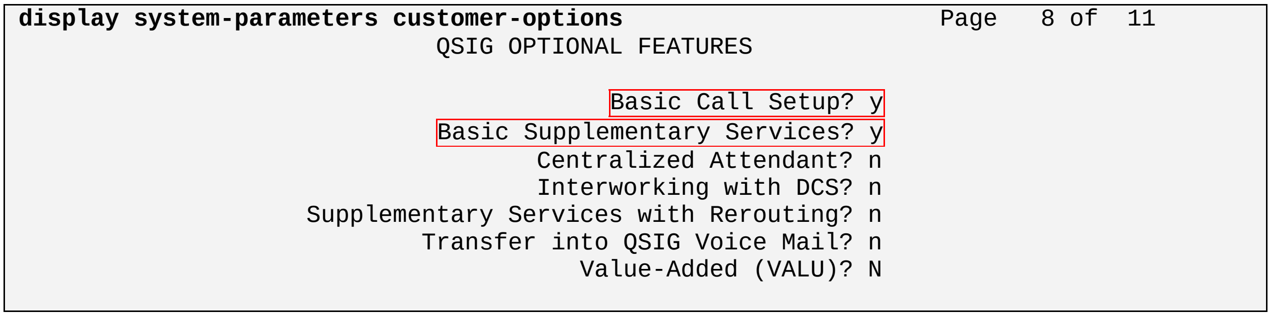
```
display system-parameters features                              Page   1 of  17
FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? y
                                    Trunk-to-Trunk Transfer: all
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y
                             Music/Tone on Hold: none
              Music (or Silence) on Transferred Trunk Calls? no
                       DID/Tie/ISDN/SIP Intercept Treatment: attd
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                  Automatic Circuit Assurance (ACA) Enabled? n


             Abbreviated Dial Programming by Assigned Lists? n
       Auto Abbreviated/Delayed Transition Interval (rings): 2
                    Protocol for Caller ID Analog Terminals: Bellcore
    Display Calling Number for Room to Room Caller ID Calls? n
```

2. Enter the **display system-parameters customer-options** command. On Page 4 of the “system-parameters customer-options” form, verify that the **ISDN-PRI** field is enabled. If not, contact an authorized Avaya account representative to enable this feature.



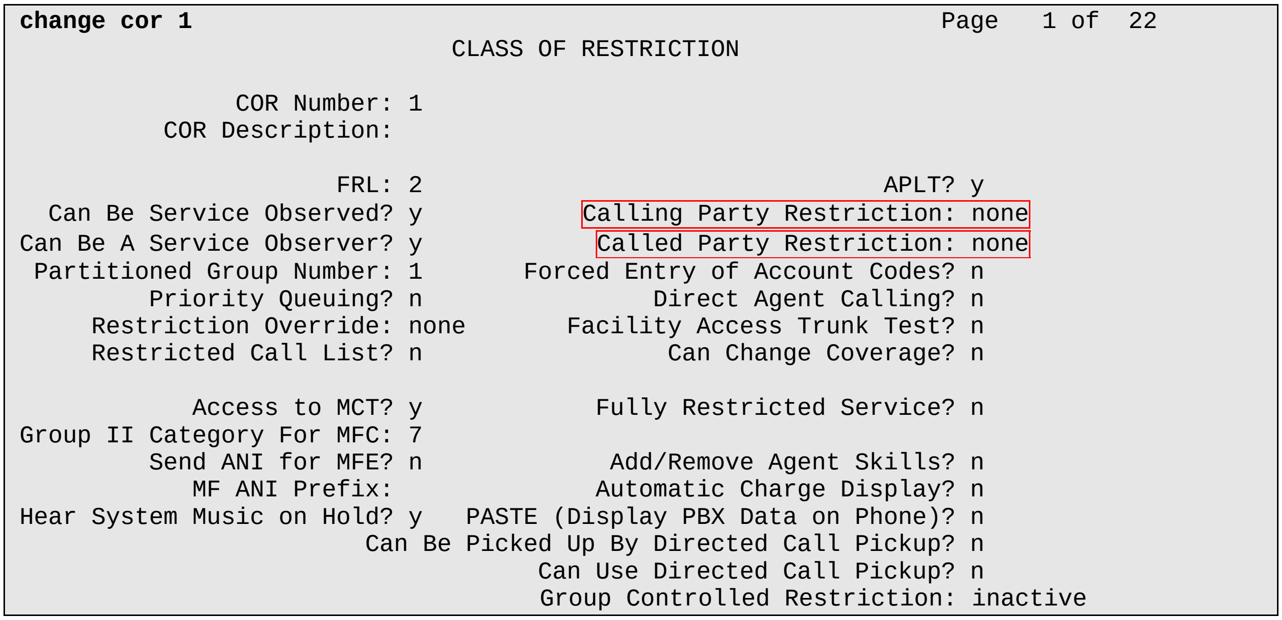
```
display system-parameters customer-options                      Page   4 of  10
                                OPTIONAL FEATURES

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

           IP Attendant Consoles? n
        (NOTE: You must logoff & login to effect the permission changes.)
```

3. On Page 8 of the “system-parameters customer-options” form, verify that the **Basic Call Setup** and **Basic Supplementary Services** fields are enabled. If not, contact an authorized Avaya account representative to enable these features.



```
display system-parameters customer-options                      Page   8 of  11
                             QSIG OPTIONAL FEATURES

                                         Basic Call Setup? y
                             Basic Supplementary Services? y
                                    Centralized Attendant? n
                                    Interworking with DCS? n
                    Supplementary Services with Rerouting? n
                            Transfer into QSIG Voice Mail? n
                                       Value-Added (VALU)? N
```

4. It is important that stations that have access to the Vocera Server are not outward restricted. All stations and trunks have a Class of Restriction (COR) assigned to them. Enter **change cor C,** where **C** is the COR number. Set the **Calling Party Restriction** and **Called Party Restriction** fields to **none** in the COR form for the appropriate COR that is assigned to the stations and trunks. During the compliance test, stations under test were assigned **1** as the COR number.



```
change cor 1                                                    Page   1 of  22
                              CLASS OF RESTRICTION

               COR Number: 1
          COR Description:

                      FRL: 2                                APLT? y
  Can Be Service Observed? y           Calling Party Restriction: none
Can Be A Service Observer? y            Called Party Restriction: none
 Partitioned Group Number: 1       Forced Entry of Account Codes? n
         Priority Queuing? n                Direct Agent Calling? n
     Restriction Override: none       Facility Access Trunk Test? n
     Restricted Call List? n                 Can Change Coverage? n

            Access to MCT? y            Fully Restricted Service? n
Group II Category For MFC: 7
         Send ANI for MFE? n             Add/Remove Agent Skills? n
            MF ANI Prefix:              Automatic Charge Display? n
Hear System Music on Hold? y   PASTE (Display PBX Data on Phone)? n
                        Can Be Picked Up By Directed Call Pickup? n
                                    Can Use Directed Call Pickup? n
                                    Group Controlled Restriction: inactive
```

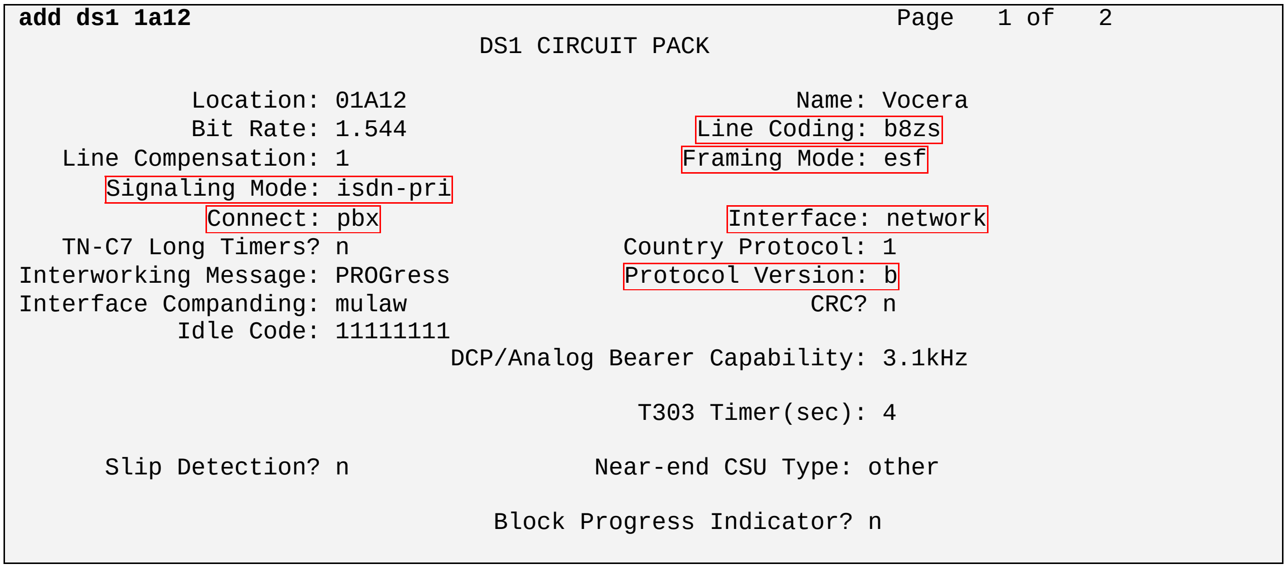
3.2. Configuring T1 ISDN-PRI Trunk

The configuration verified for T1 trunks used the **229xx** extension range for the Vocera Server and Badges. Add the DS1 for the T1 trunks by using the command **add ds1 xxxx**, where **xxxx** is the DS1 board location. In this case the location was **01a12**, where “**01”** is the cabinet number, “**a”** is the carrier number, and “**12”** is the slot number of the DS1 board.

1. The next screen shows the DS1 CIRCUIT PACK form for the ISDN-PRI protocol. Avaya Communication Manager acted as the **network**, and the Vocera Server was the **user**. The following information is provided for configuring the DS1 board.

    - Line Coding: **b8zs**
    - Framing Mode: **esf**
    - Signaling Mode: **isdn-pri**
    - Connect: **pbx**
    - Interface: **network**
    - Protocol Version: **b** (b - NI2, a – 5ESS)

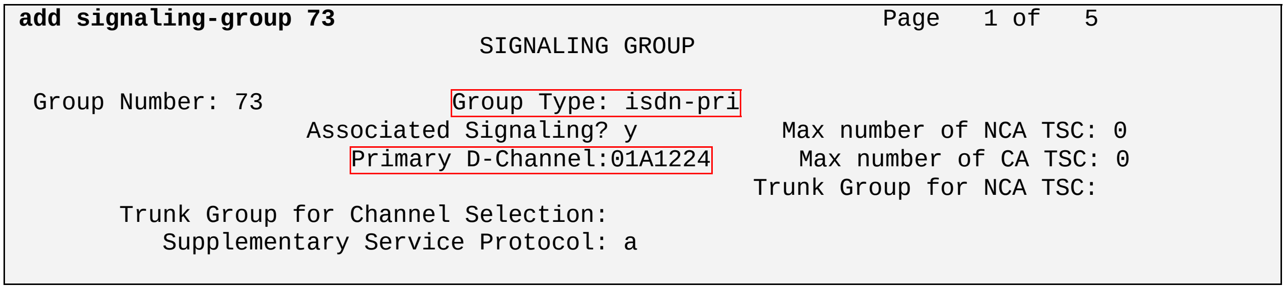
    Default values may be used in the remaining fields.



```
add ds1 1a12                                                 Page   1 of   2
                                DS1 CIRCUIT PACK

            Location: 01A12                           Name: Vocera
            Bit Rate: 1.544                    Line Coding: b8zs
   Line Compensation: 1                       Framing Mode: esf
      Signaling Mode: isdn-pri
             Connect: pbx                        Interface: network
   TN-C7 Long Timers? n                   Country Protocol: 1
Interworking Message: PROGress            Protocol Version: b
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

                                 Block Progress Indicator? n
```

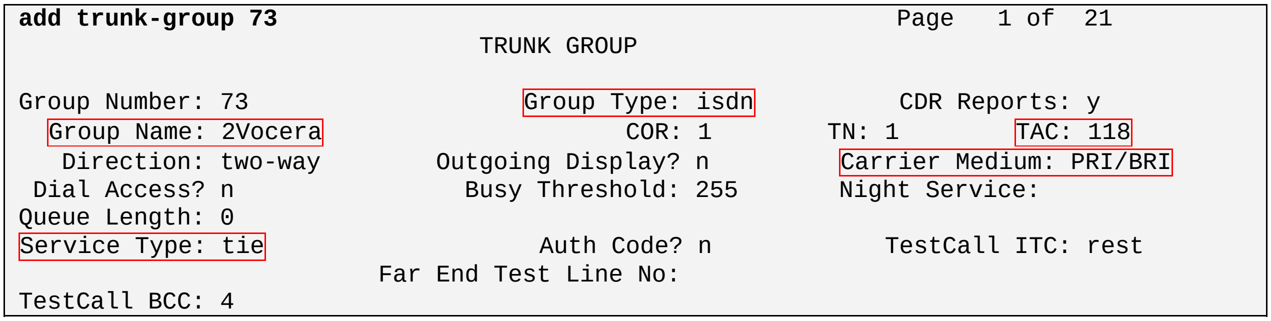
2. Enter the **add signaling-group S** command**,** where **S** is the signaling-group number, to define a new signaling group for the trunk between the Vocera Telephony Server and Avaya Communication Manager. Configuring the signaling-group is a two step procedure:
   - Create a signaling-group and specify the **Group Type** and **Primary D-Channel**. **Note:** Channel 24 on a standard PRI circuit is reserved for signaling.
   - After the trunk-group is created, the **Trunk Group for Channel Selection** field be specified with the trunk group number.

   The following screen shows the first step. The important signaling-group related parameters that were different from the default values are highlighted here.



```
add signaling-group 73                                      Page   1 of   5
                                SIGNALING GROUP

 Group Number: 73             Group Type: isdn-pri
                    Associated Signaling? y          Max number of NCA TSC: 0
                       Primary D-Channel:01A1224      Max number of CA TSC: 0
                                                   Trunk Group for NCA TSC:
       Trunk Group for Channel Selection:
          Supplementary Service Protocol: a
```

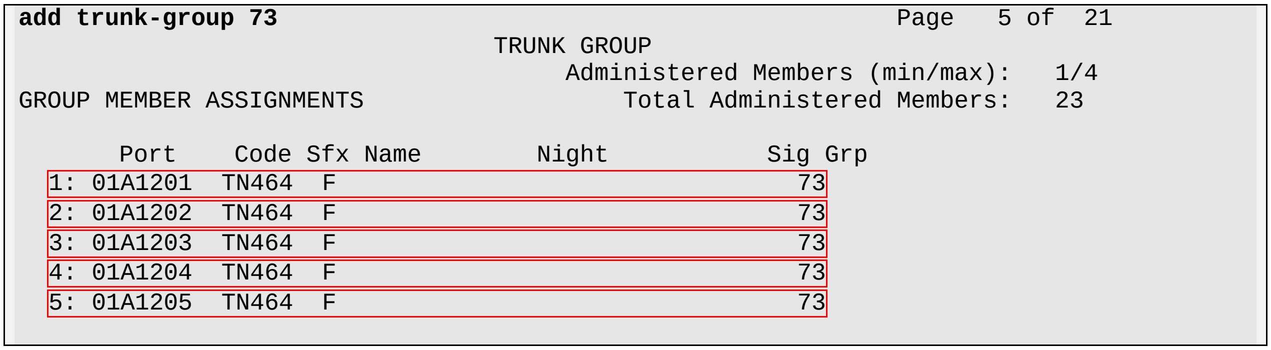
3. Enter the **add trunk-group T** command, where **T** is the trunk-group number, to create a trunk group. The important trunk-group related parameters that were different from the default values are highlighted below.



```
add trunk-group 73                                           Page   1 of  21
                                TRUNK GROUP

Group Number: 73                   Group Type: isdn          CDR Reports: y
  Group Name: 2Vocera                     COR: 1        TN: 1        TAC: 118
   Direction: two-way        Outgoing Display? n         Carrier Medium: PRI/BRI
 Dial Access? n                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
```

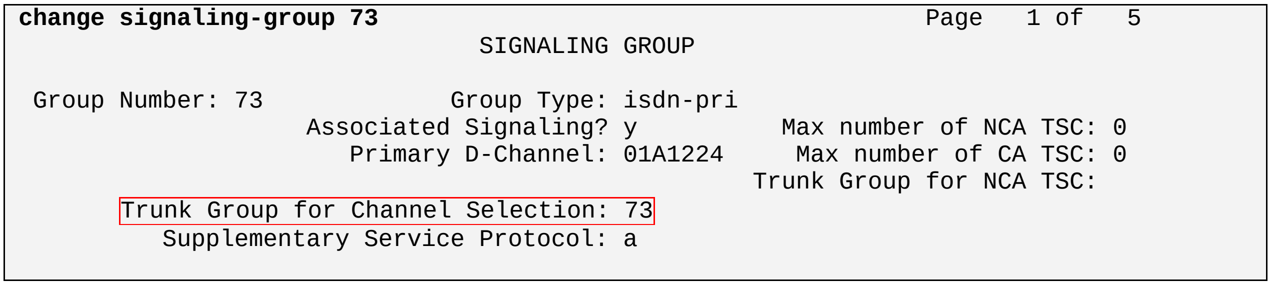
4. On Page 5 of the TRUNK GROUP form, add trunk group members. To add group members, simply populate **Port** with the board location plus the channel number (e.g. board location is 01A12 plus channel 01, rendering 01A1201). Tab to the **Sig Grp** and enter the number assigned to the signaling group as displayed below.

   The following screen shows the first five entries of the **GROUP MEMBER ASSIGNMENTS** page in the TRUNK GROUP form.



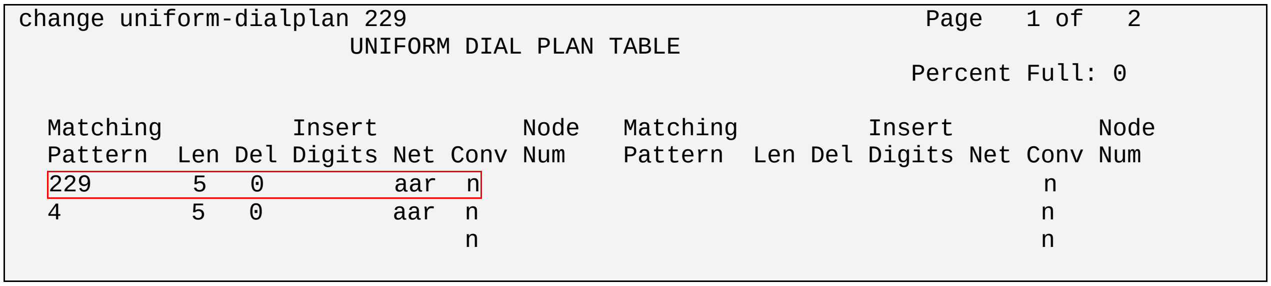
```
add trunk-group 73                                           Page   5 of  21
                                 TRUNK GROUP
                                      Administered Members (min/max):   1/4
GROUP MEMBER ASSIGNMENTS                  Total Administered Members:   23

       Port    Code Sfx Name        Night           Sig Grp
  1: 01A1201  TN464  F                                73
  2: 01A1202  TN464  F                                73
  3: 01A1203  TN464  F                                73
  4: 01A1204  TN464  F                                73
  5: 01A1205  TN464  F                                73
```

5. Enter the **change signaling-group S** command, where **S** is the signaling-group added in **Step 2**, to finish the signal group configuration. The following screen shows the signaling-group configuration. The important parameter in the screen is assigning the **Trunk Group for Channel Selection** field.



```
change signaling-group 73                                      Page   1 of   5
                                SIGNALING GROUP

 Group Number: 73             Group Type: isdn-pri
                    Associated Signaling? y          Max number of NCA TSC: 0
                       Primary D-Channel: 01A1224     Max number of CA TSC: 0
                                                   Trunk Group for NCA TSC:
       Trunk Group for Channel Selection: 73
          Supplementary Service Protocol: a
```

6. Enter **change uniform-dialplan U**, where **U** is the uniform-dialplan number. The following screen shows the Uniform Dial Plan configuration. The 5-digit extension range starting with **229** was used for the Vocera Server and Badges, and utilized Automatic Alternate Routing (AAR).



```
change uniform-dialplan 229                                    Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                              Percent Full: 0

  Matching         Insert          Node   Matching         Insert          Node
  Pattern  Len Del Digits Net Conv Num    Pattern  Len Del Digits Net Conv Num
  229       5   0         aar  n                                       n
  4         5   0         aar  n                                       n
                               n                                       n
```

7. Enter **change aar analysis A**, where **A** is the AAR number. Automatic Alternate Routing (AAR) was used to route calls to the appropriate route pattern.

```
change aar analysis 229                                         Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                                            Percent Full:    1

          Dialed             Total      Route     Call    Node    ANI
          String            Min   Max  Pattern    Type    Num     Reqd
    229                     5     5      73       aar             n
                                                                  n
```

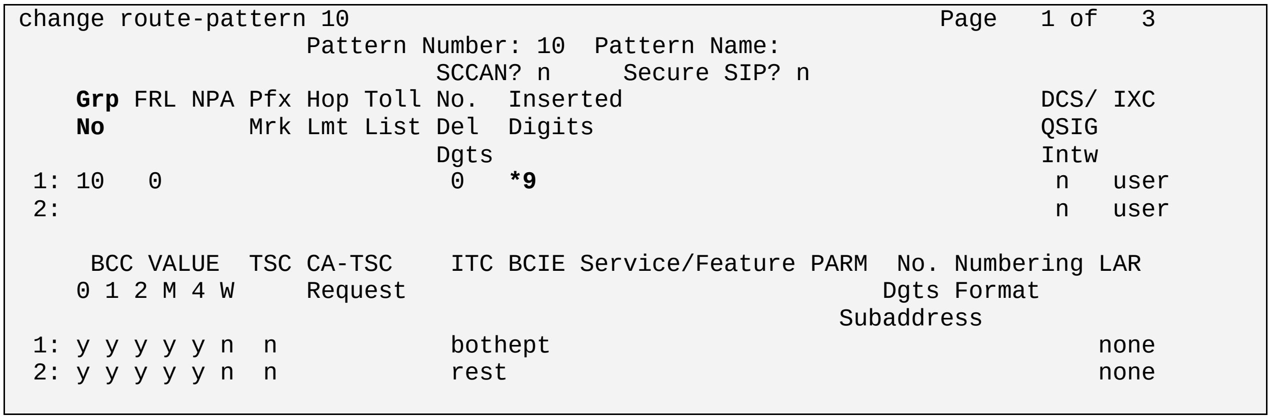
8. Enter **change route-pattern R**, where **R** is the route-pattern number. The route pattern 73 routes calls using trunk group 73.

```
change route-pattern 73                                         Page   1 of   3
                    Pattern Number: 73  Pattern Name: 2Vocera
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                              DCS/ IXC
    No          Mrk Lmt List Del  Digits                                QSIG
                             Dgts                                       Intw
 1: 73   0                                                               n   user
 2:                                                                     n   user
 3:                                                                     n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 3 4 W     Request                                Dgts Format
                                                        Subaddress
 1: y y y y y n  n            rest                                          none
 2: y y y y y n  n            rest                                          none
 3: y y y y y n  n            rest                                          none
```

9. PSTN resources on the Avaya Communication Manager are acquired through Automatic Route Selection (ARS). In this case, only the local area code was setup for both 10 (Home Numbering Plan Area – hnpa) and 11(Foreign Number Plan Area – fnpa) digit outbound dialing. **Change ars analysis XXX**, where **XXX** is the ARS (**Dialed String**) number. The Avaya Communication Manager PSTN trunk used **Route Pattern 10**.

```
change ars analysis 173                                          Page   1 of   x
                             ARS DIGIT ANALYSIS TABLE
                                   Location:  all           Percent Full:    1

          Dialed             Total      Route     Call    Node    ANI
          String            Min   Max  Pattern    Type    Num     Reqd
    173                     11    11     10       fnpa            n
    ..
    ..
    732                     10    10     10       hnpa            n
```

10. Enter **change route-pattern R**, where **R** is the route-pattern number used for the PSTN trunk.   In this case, route-pattern 10 uses trunk **Grp No 10** and a ***9** is inserted to the 10 or 11 digit number dialed by the user.

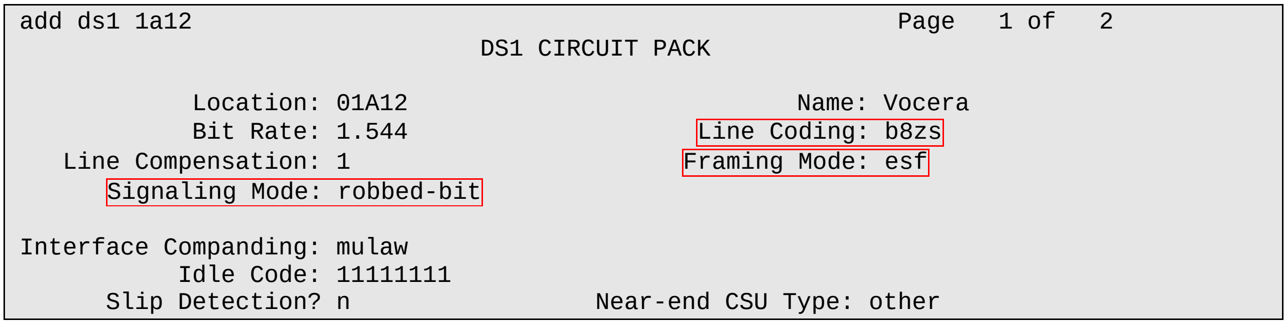


```
change route-pattern 10                                         Page   1 of   3
                    Pattern Number: 10  Pattern Name:
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 10   0                    0   *9                                    n   user
 2:                                                                     n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            bothept                                    none
 2: y y y y y n  n            rest                                       none
```

3.3. Configuring T1 Wink Start Trunk

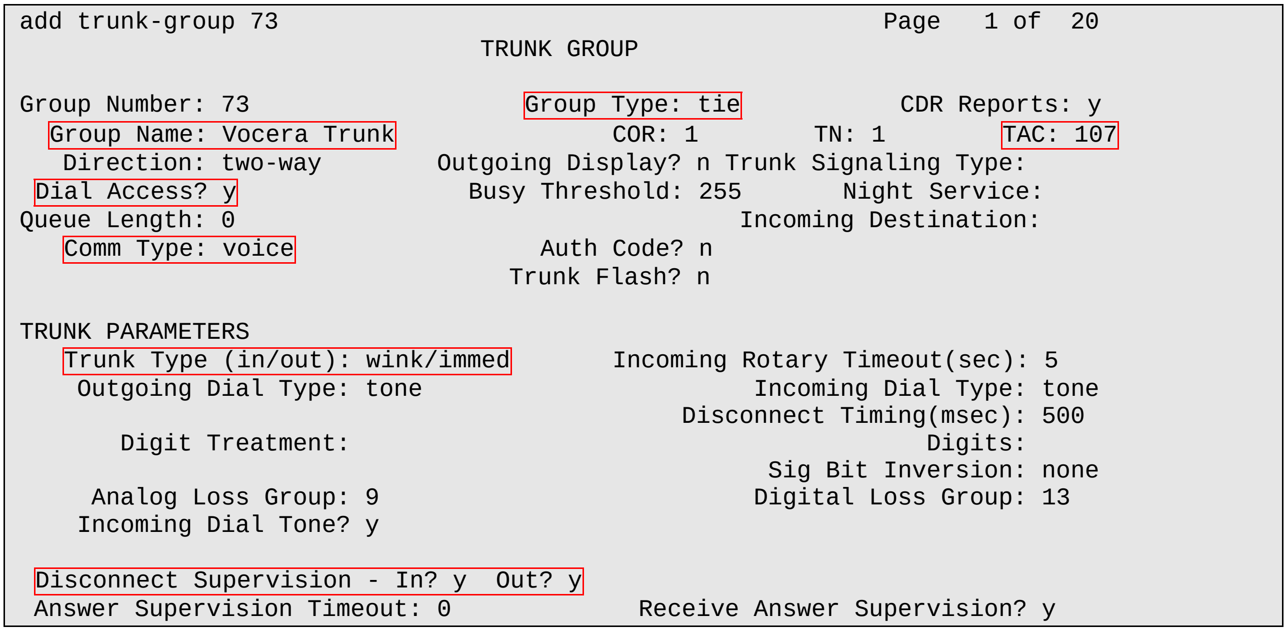
The configuration steps in **Section 3.1** and **3.2** remain the same for T1 Wink Start, except for the following DS1 and trunk group parameters

1. The configuration verified for T1 trunks used the **229xx** extension range for the Vocera Server and Badges. Add the DS1 for the T1 trunks by using the command **add ds1 xxxx**, where **xxxx** is the T1 board location. The DS1 form for the Robbed Bit T1 board is shown here.



```
add ds1 1a12                                                 Page   1 of   2
                                DS1 CIRCUIT PACK

            Location: 01A12                           Name: Vocera
            Bit Rate: 1.544                    Line Coding: b8zs
   Line Compensation: 1                       Framing Mode: esf
      Signaling Mode: robbed-bit

Interface Companding: mulaw
           Idle Code: 11111111
      Slip Detection? n                 Near-end CSU Type: other
```

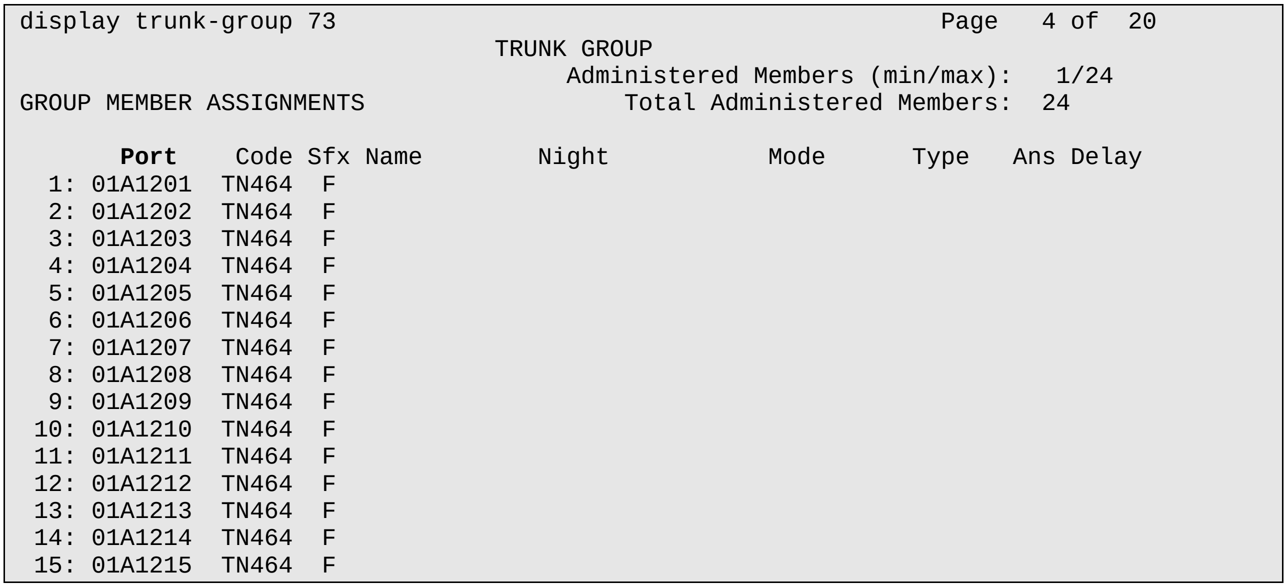
2. Enter the **add trunk-group T** command, where **T** is the trunk-group number, to create a trunk group. The important trunk-group related parameters that were different from the default values are highlighted below.



```
add trunk-group 73                                          Page   1 of  20
                                TRUNK GROUP

Group Number: 73                   Group Type: tie           CDR Reports: y
  Group Name: Vocera Trunk               COR: 1        TN: 1        TAC: 107
   Direction: two-way        Outgoing Display? n Trunk Signaling Type:
 Dial Access? y                Busy Threshold: 255       Night Service:
Queue Length: 0                                   Incoming Destination:
   Comm Type: voice                 Auth Code? n
                                  Trunk Flash? n

TRUNK PARAMETERS
   Trunk Type (in/out): wink/immed       Incoming Rotary Timeout(sec): 5
    Outgoing Dial Type: tone                       Incoming Dial Type: tone
                                              Disconnect Timing(msec): 500
       Digit Treatment:                                        Digits:
                                                    Sig Bit Inversion: none
     Analog Loss Group: 9                          Digital Loss Group: 13
    Incoming Dial Tone? y

 Disconnect Supervision - In? y  Out? y
 Answer Supervision Timeout: 0             Receive Answer Supervision? y
```

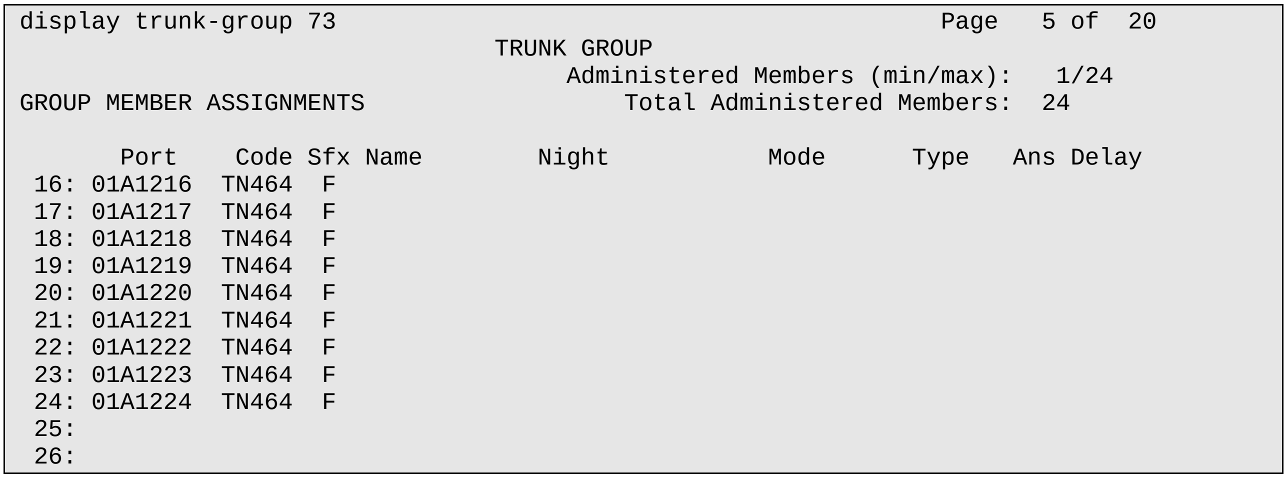
3. On Page 4 of the TRUNK GROUP form, add trunk group members. To add group members, simply populate the 24 ports with the board location plus the channel as displayed below.

   The following two screens show the results of the Group Member assignments page in the TRUNK GROUP form.



```
display trunk-group 73                                          Page   4 of  20
                                 TRUNK GROUP
                                      Administered Members (min/max):   1/24
GROUP MEMBER ASSIGNMENTS                  Total Administered Members:  24

       Port    Code Sfx Name        Night           Mode      Type   Ans Delay
  1: 01A1201  TN464  F
  2: 01A1202  TN464  F
  3: 01A1203  TN464  F
  4: 01A1204  TN464  F
  5: 01A1205  TN464  F
  6: 01A1206  TN464  F
  7: 01A1207  TN464  F
  8: 01A1208  TN464  F
  9: 01A1209  TN464  F
 10: 01A1210  TN464  F
 11: 01A1211  TN464  F
 12: 01A1212  TN464  F
 13: 01A1213  TN464  F
 14: 01A1214  TN464  F
 15: 01A1215  TN464  F
```

Trunk group continues.



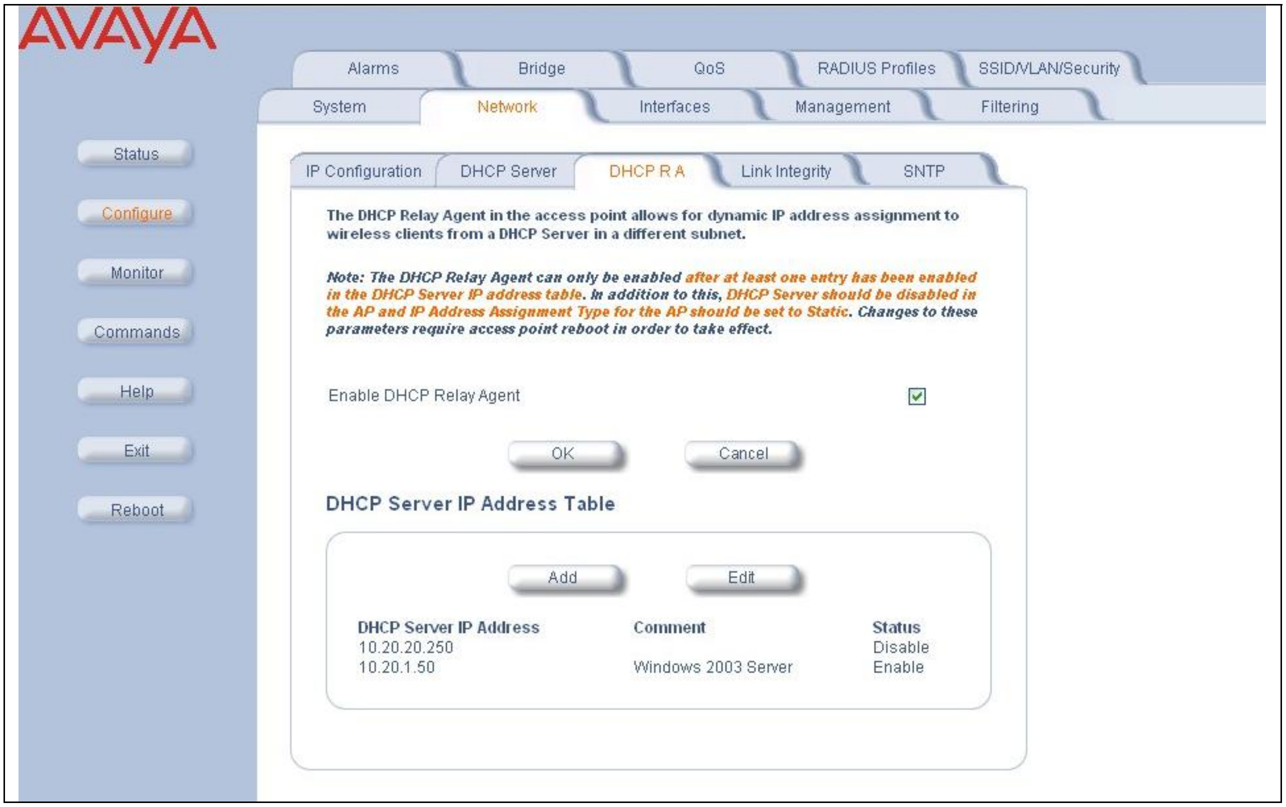
```
display trunk-group 73                                          Page   5 of  20
                                 TRUNK GROUP
                                      Administered Members (min/max):   1/24
GROUP MEMBER ASSIGNMENTS                  Total Administered Members:  24

       Port    Code Sfx Name        Night           Mode      Type   Ans Delay
 16: 01A1216  TN464  F
 17: 01A1217  TN464  F
 18: 01A1218  TN464  F
 19: 01A1219  TN464  F
 20: 01A1220  TN464  F
 21: 01A1221  TN464  F
 22: 01A1222  TN464  F
 23: 01A1223  TN464  F
 24: 01A1224  TN464  F
 25:
 26:
```

4. Configure Avaya Wireless AP-8

Avaya Wireless AP-8s were utilized for providing the wireless network which allowed the Vocera badges to register to the Vocera server. The initial configuration for the Avaya Wireless AP-8 is accomplished through the ScanTool software, which comes with the Avaya Wireless AP-8 software. After the initial configuration, the web interface was utilized to do the configuration modifications. The configuration screens included here show how to configure the **Network**, **Interfaces**, and **Service Set Identifier** (**SSID)**.

1. Use a web browser to access the Management IP address of the Avaya Wireless AP-8. Provide proper credentials to login. Click on the **Configure** button from the main menu on the left. Click the **Network** tab from the right menu and select **DHCP RA** (DHCP Relay Agent) tab from the submenu (**Configure → Network → DHCP RA**). The following screen appears. Enable the DHCP Relay Agent by checking the box. Add the DHCP server by clicking the **Add** button and provide the IP address of the DHCP server.

   After completion of adding DHCP server, click **OK** button.



The DHCP Relay Agent in the access point allows for dynamic IP address assignment to wireless clients from a DHCP Server in a different subnet.

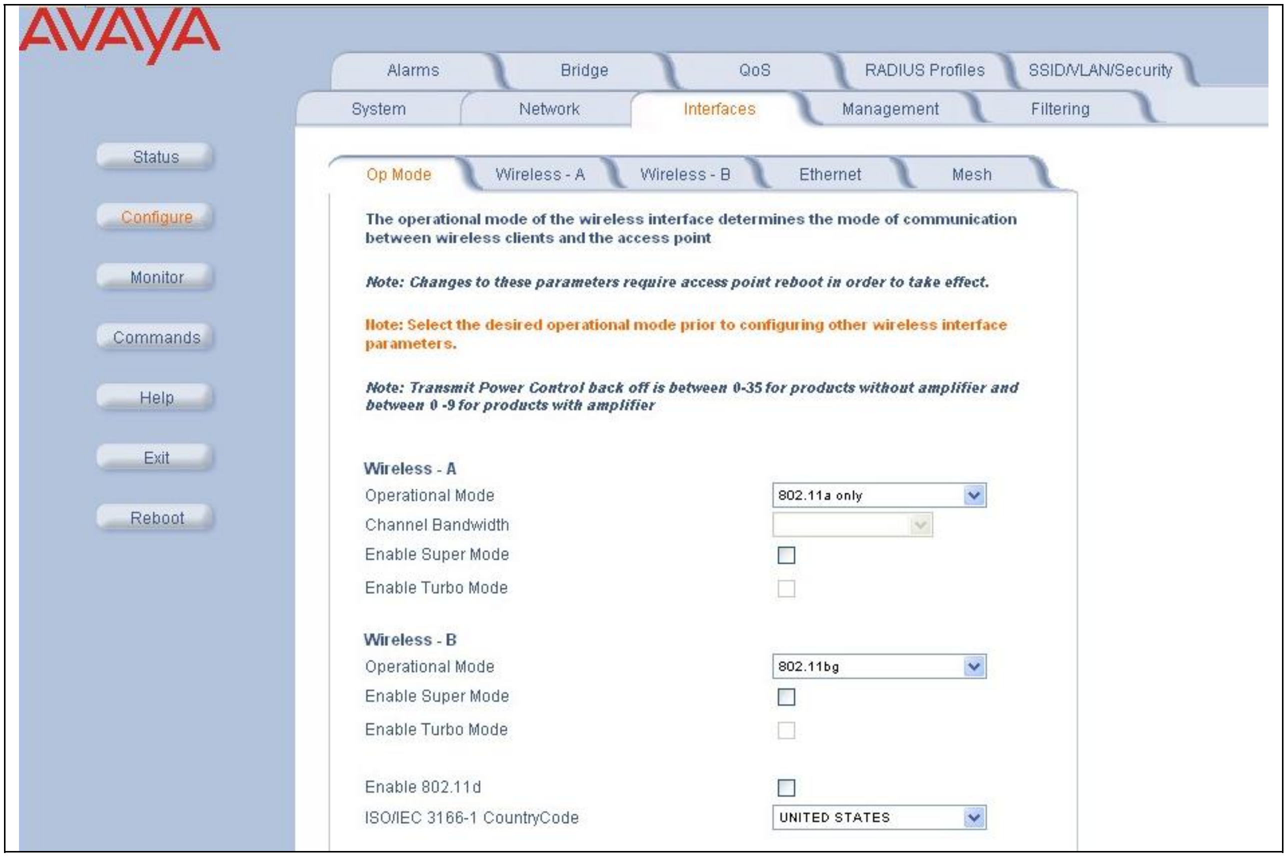
Note: The DHCP Relay Agent can only be enabled after at least one entry has been enabled in the DHCP Server IP address table. In addition to this, DHCP Server should be disabled in the AP and IP Address Assignment Type for the AP should be set to Static. Changes to these parameters require access point reboot in order to take effect.

Enable DHCP Relay Agent ☑

DHCP Server IP Address Table

DHCP Server IP Address	Comment	Status
10.20.20.250		Disable
10.20.1.50	Windows 2003 Server	Enable

2. Navigate to the **Configure → Interfaces → Op Mode** page. For compliance testing, the **Wireless – B** interface was used. Select the **802.11bg** for the Operational Mode field as shown in the following screen.



The operational mode of the wireless interface determines the mode of communication between wireless clients and the access point

Note: Changes to these parameters require access point reboot in order to take effect.

Note: Select the desired operational mode prior to configuring other wireless interface parameters.

Note: Transmit Power Control back off is between 0-35 for products without amplifier and between 0 -9 for products with amplifier

Wireless - A

Operational Mode: 802.11a only

Channel Bandwidth:

Enable Super Mode: □

Enable Turbo Mode: □

Wireless - B

Operational Mode: 802.11bg

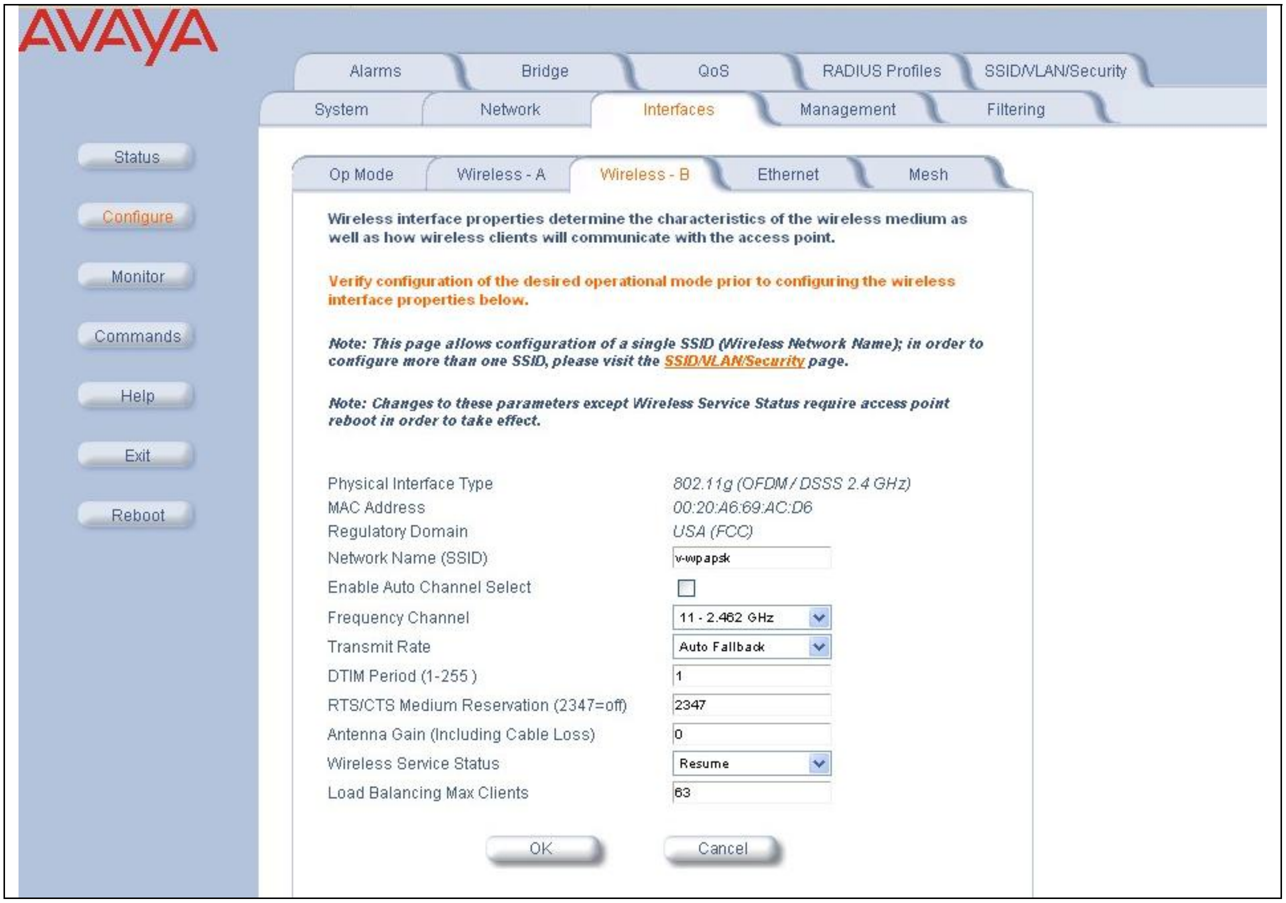
Enable Super Mode: □

Enable Turbo Mode: □

Enable 802.11d: □

ISO/IEC 3166-1 CountryCode: UNITED STATES

3. Navigate to the **Configure → Interfaces → Wireless -B** page. The following screen is displayed. Configure the **Network Name (SSID)** and **Frequency Channel** fields as shown below. For the roaming test, the Frequency Channel field for Avaya Wireless AP-8 was set to Channel **11**.



Wireless interface properties determine the characteristics of the wireless medium as well as how wireless clients will communicate with the access point.

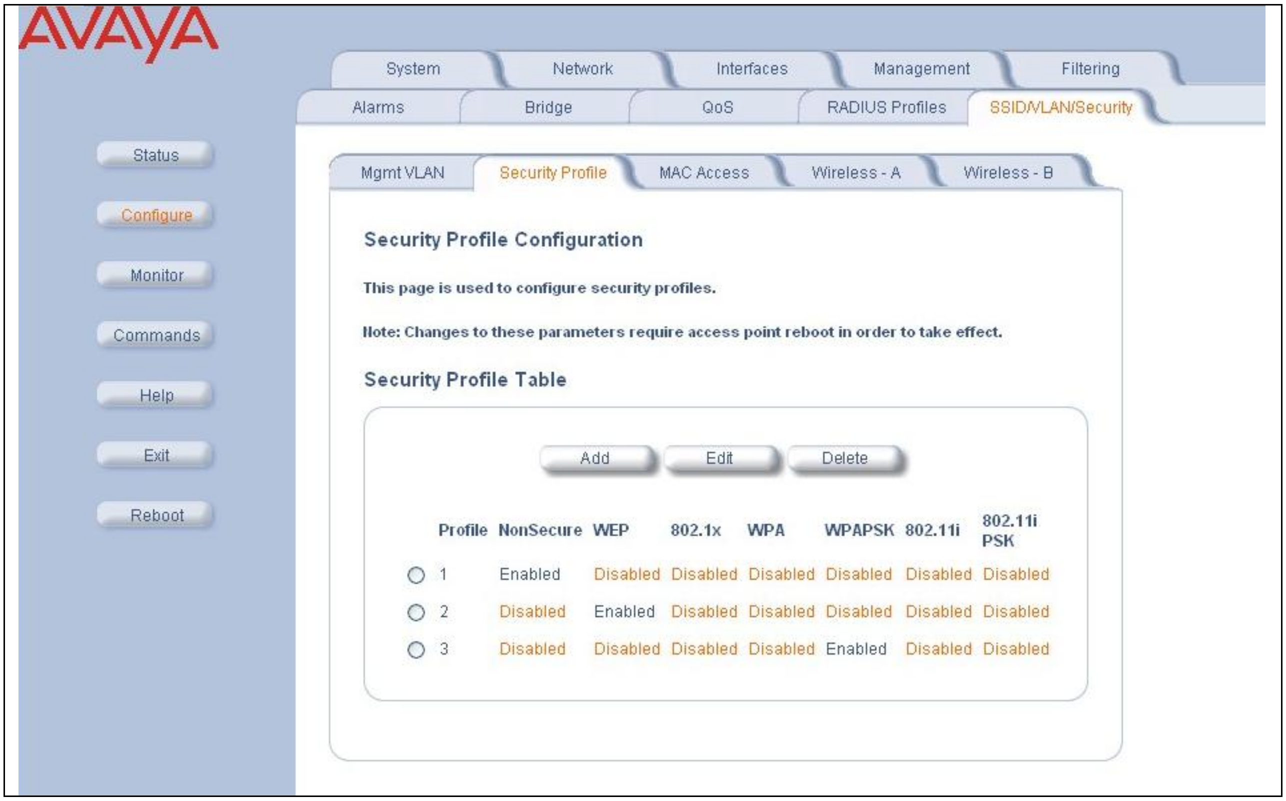
Verify configuration of the desired operational mode prior to configuring the wireless interface properties below.

Note: This page allows configuration of a single SSID (Wireless Network Name); in order to configure more than one SSID, please visit the SSID/VLAN/Security page.

Note: Changes to these parameters except Wireless Service Status require access point reboot in order to take effect.

Physical Interface Type	*802.11g (OFDM / DSSS 2.4 GHz)*
MAC Address	*00:20:A6:69:AC:D6*
Regulatory Domain	*USA (FCC)*
Network Name (SSID)	v-wpapsk
Enable Auto Channel Select	□
Frequency Channel	11 - 2.462 GHz
Transmit Rate	Auto Fallback
DTIM Period (1-255)	1
RTS/CTS Medium Reservation (2347=off)	2347
Antenna Gain (Including Cable Loss)	0
Wireless Service Status	Resume
Load Balancing Max Clients	63

4. Navigate to the **Configure → SSID/VLAN/Security → Security Profile** page. The following screen should be displayed. Compliance testing was performed using non-secure and secure profile configurations. The screen below illustrates three profiles have been added. **Profile 1** as **Non-Secure**, **Profile 2** as **WEP**, and **Profile 3** as **WPAPSK**.



Security Profile Configuration

This page is used to configure security profiles.

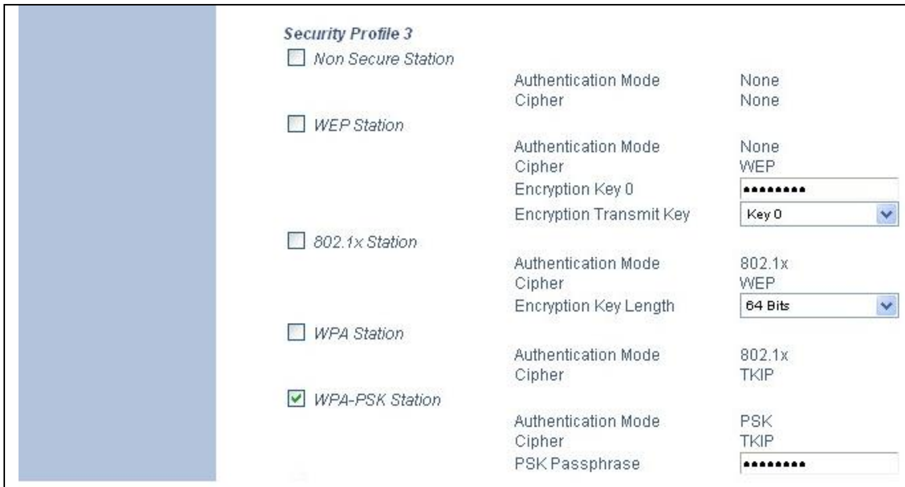
Note: Changes to these parameters require access point reboot in order to take effect.

Security Profile Table

	Profile	NonSecure	WEP	802.1x	WPA	WPAPSK	802.11i	802.11i PSK
○	1	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
○	2	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled
○	3	Disabled	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled

5. To create or modify a **WPA-PSK station** encryption profile, click **Add** or **Edit** button displayed in **Step 4**, then click on the **WEP-PSK Station** box as displayed below. Enter 8 to 63 characters to be used for the **PSK Passphrase** field.

   Note: To communicate between wireless devices, the same PSK Passphrase key needs to be used.



Security Profile 3

☐ *Non Secure Station*

Authentication Mode	None
Cipher	None

☐ *WEP Station*

Authentication Mode	None
Cipher	WEP
Encryption Key 0	••••••••
Encryption Transmit Key	Key 0

☐ *802.1x Station*

Authentication Mode	802.1x
Cipher	WEP
Encryption Key Length	64 Bits

☐ *WPA Station*

Authentication Mode	802.1x
Cipher	TKIP

☑ *WPA-PSK Station*

Authentication Mode	PSK
Cipher	TKIP
PSK Passphrase	••••••••

6. Compliance testing used two AP-8 devices; therefore administration must be repeated on the second AP-8. For the new configuration to take effect, the Avaya Wireless AP-8 must be rebooted. Click the **Commands→ Reboot** tab (not shown) from the main menu.

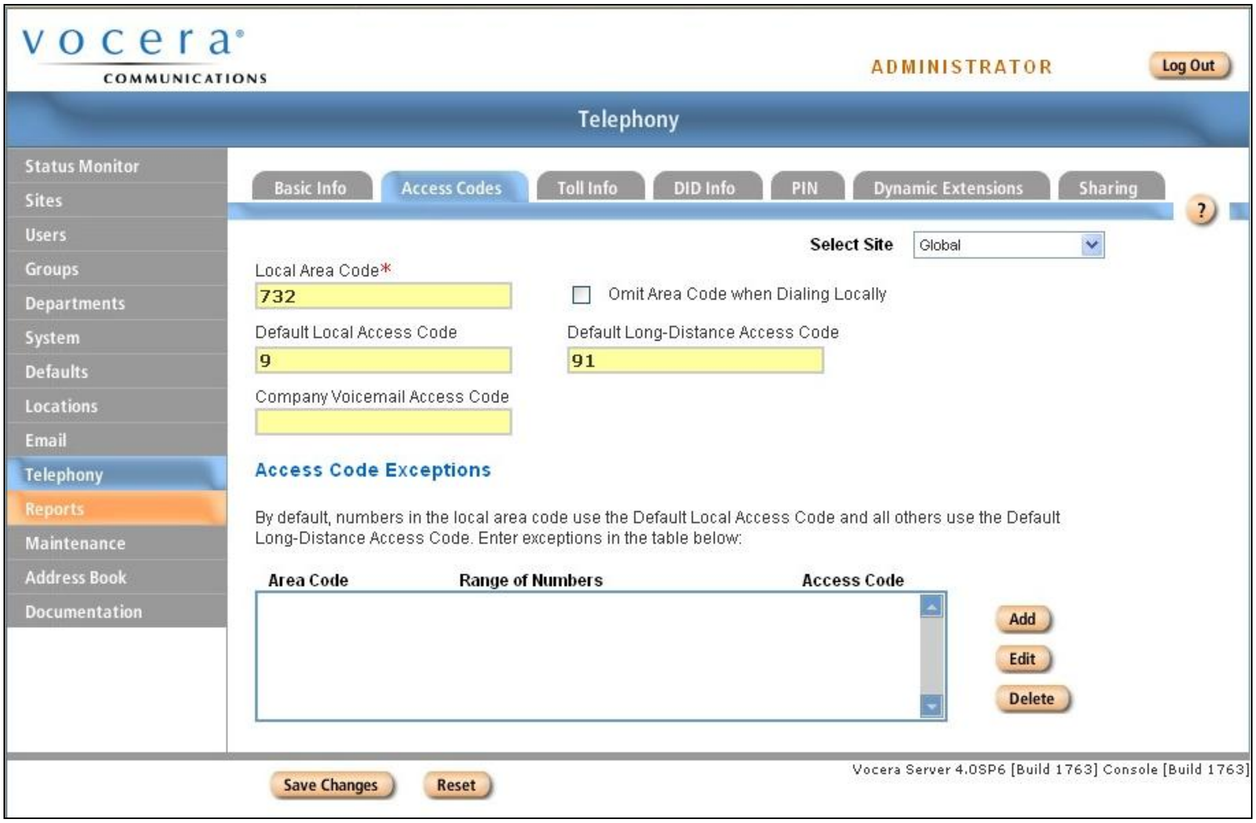
5. Configure the Vocera Communications System

The Vocera Communications System is configured using a web based console interface. Use a web browser to access the IP address of the Vocera Communication System. Log in using the appropriate credentials. Refer to **References [3]**, **[4]**, **[5]**, and **[6]** during configuration of the Vocera product.

1. The following screen shows the telephony configuration used when the Vocera Telephony Server places outbound calls through the PBX.

   Select **Telephony** from the left panel and select the **Access Codes** tab to configure Local and Long Distance Access Code. The **Local Area Code** field should match the local PBX area code configured in ACM (as shown). The **Default Long-Distance Access Code** field is typically the same as the **Default Local Access Code**, followed by a **1**.

   After completion, click the **Save Changes** button.



Select Site: Global

Local Area Code*: 732

□ Omit Area Code when Dialing Locally

Default Local Access Code: 9

Default Long-Distance Access Code: 91

Company Voicemail Access Code:

Access Code Exceptions

By default, numbers in the local area code use the Default Local Access Code and all others use the Default Long-Distance Access Code. Enter exceptions in the table below:

Area Code	Range of Numbers	Access Code

Vocera Server 4.0SP6 [Build 1763] Console [Build 1763]

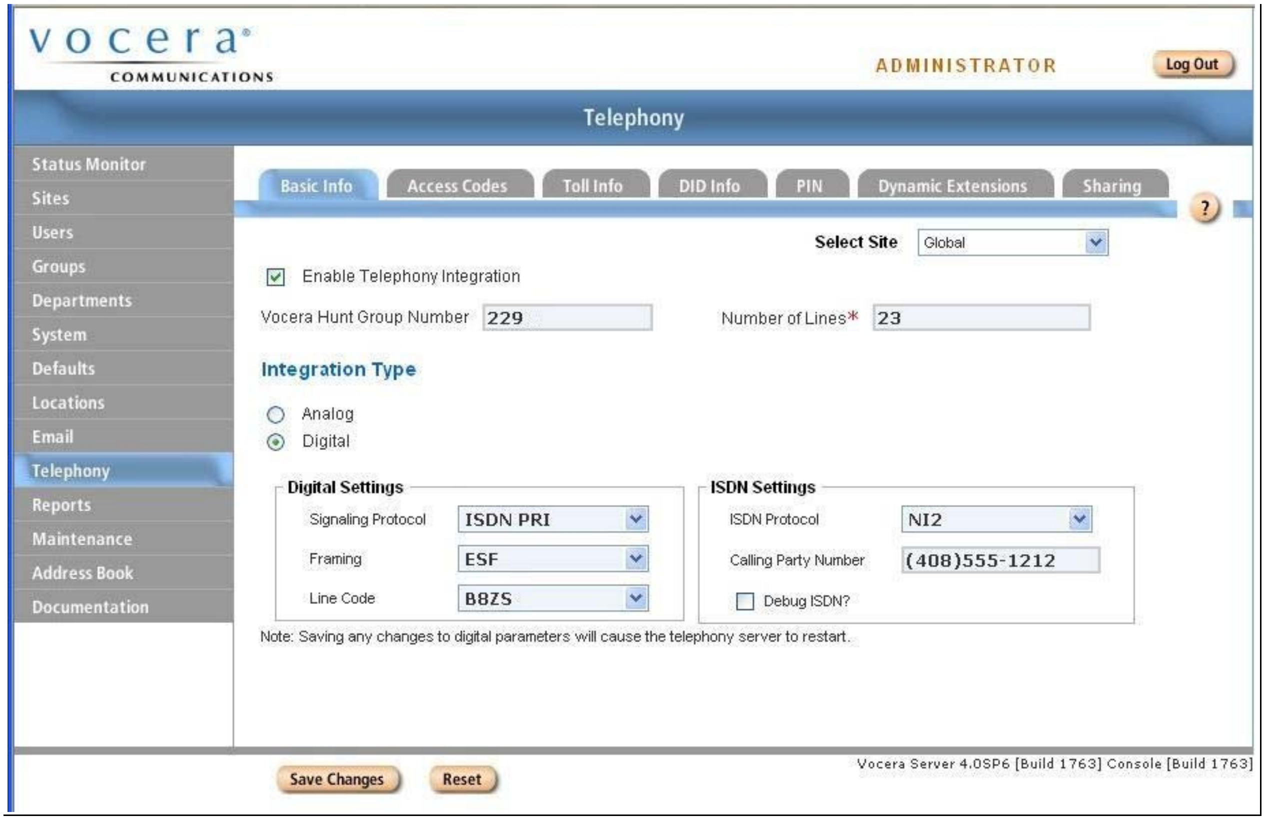
5.1. Configuring the Vocera Telephony Server for T1 ISDN-PRI

The next screen shows the configuration used for the Vocera Telephony server to connect Avaya Communication Manager using an ISDN-PRI T1 trunk. For inbound, there are two ways that a call can reach an individual badge.

- A user calls a Direct Inward Dialing (DID) number for a badge ID. For example, from an Avaya telephone, call 22901 (229xx), where 229 is the access code and xx identifies one of four badges used during compliance, numbered 01, 02, 03, and 04. Therefore, in this example, badge 01 received the incoming call.
- A caller calls the Vocera Hunt Group Number. In this case, the user is greeted by the voice interface, and prompted for a badge user to contact. In this example, 22999 was called.

1. Select **Telephony** from the left panel, and select the **Basic Info** tab. Edit the values as indicated below. They should match the corresponding values in Avaya Communication Manager.
   - Vocera Hunt Group Number: **229**
   - Number of Lines: **23**
   - Integration Type: **Digital**
   - Signaling Protocol: **ISDN PRI**
   - Framing: **ESF**
   - Line Code: **B8ZS**
   - ISDN Protocol: **NI2** (**5ESS** was also Compliance tested)

   After completion, click the **Save Changes** button.



Select Site: Global

☑ Enable Telephony Integration

Vocera Hunt Group Number: 229

Number of Lines*: 23

Integration Type

○ Analog

● Digital

Digital Settings

Signaling Protocol	ISDN PRI
Framing	ESF
Line Code	B8ZS

ISDN Settings

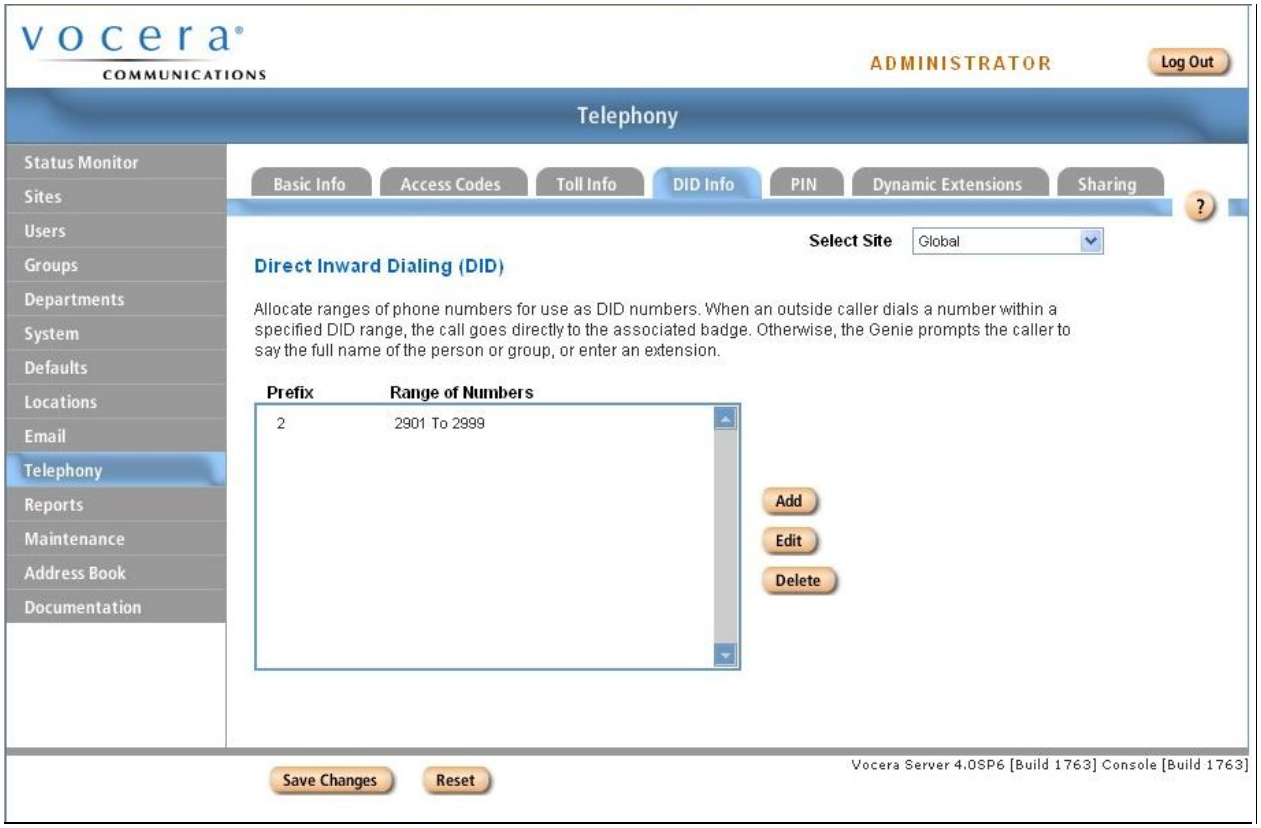
ISDN Protocol	NI2
Calling Party Number	(408)555-1212

□ Debug ISDN?

Note: Saving any changes to digital parameters will cause the telephony server to restart.

Vocera Server 4.0SP6 [Build 1763] Console [Build 1763]

2. Click the **DID Info** tab to start configuring Direct Inward Dialing (DID) for an individual badge. As displayed in the illustration below, the **Range of Numbers** is set from **2901 to 2999**. Click the **Add** button to add a DID range.



Select Site: Global

Direct Inward Dialing (DID)

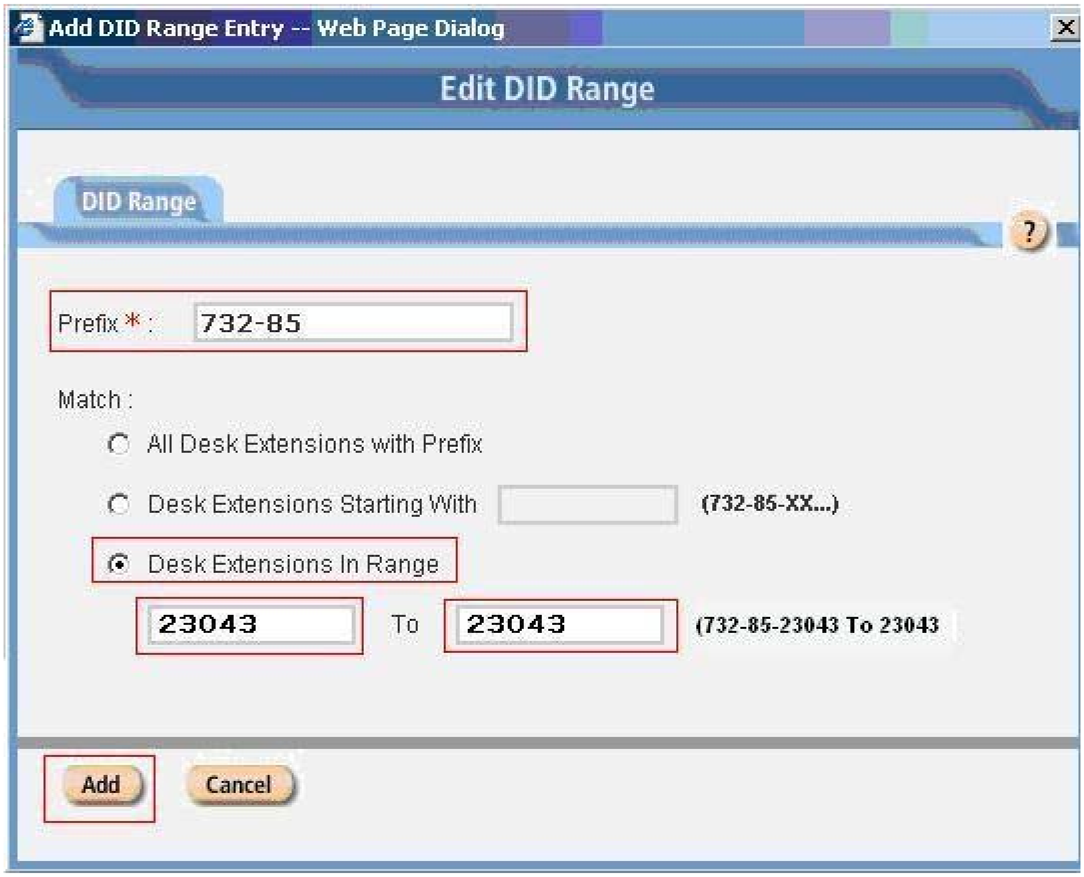
Allocate ranges of phone numbers for use as DID numbers. When an outside caller dials a number within a specified DID range, the call goes directly to the associated badge. Otherwise, the Genie prompts the caller to say the full name of the person or group, or enter an extension.

Prefix	Range of Numbers
2	2901 To 2999

Vocera Server 4.0SP6 [Build 1763] Console [Build 1763]

3. From the **Add DID Range Entry** screen, the **Prefix*** is concatenated with the **Desk Extensions in Range** to form the DID number dialed over the digital trunk to Avaya Communication Manager. The number is interpreted as 732-852-3043 and is dialed out from a Vocera badge to the PSTN resources, as previously setup in route pattern 10 in **Section 3.1.**

   Click the **Add** button to finish the DID configuration.



Prefix * : 732-85

Match :

○ All Desk Extensions with Prefix

○ Desk Extensions Starting With (732-85-XX...)

● Desk Extensions In Range

23043 To 23043 (732-85-23043 To 23043

4. After completion of the Add screen, shown later, click **Save Changes** button.

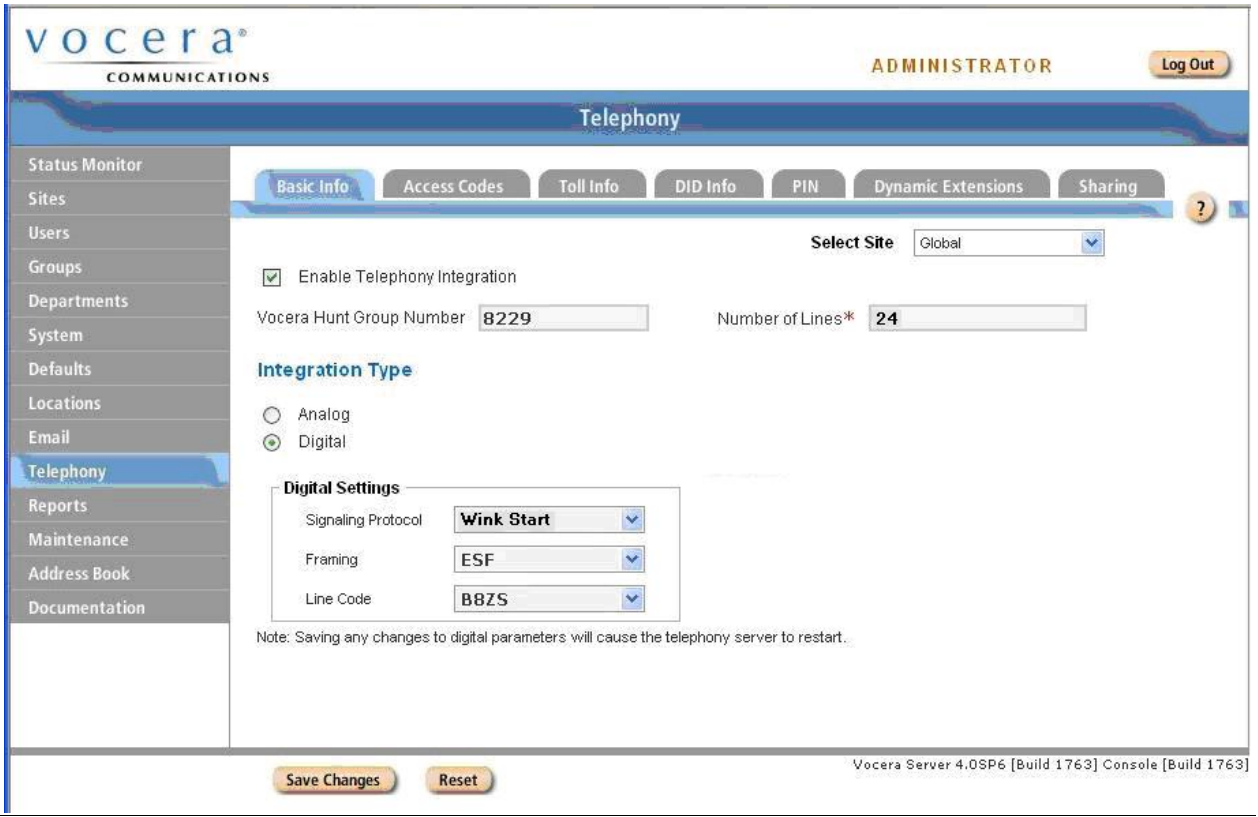
5.2. Configuring the Vocera Telephony Server for Wink Start

Compliance testing was also conducted using a T1 Wink Start trunk between the Vocera Telephony Server and Avaya Communication Manager.

1. The following screen shows the configuration used when Vocera was connected to Avaya Communication Manager using T1 robbed-bit Signaling Mode. **Note:** Should match Avaya Communication Manager.

    - Vocera Hunt Group Number: **8229**
    - Number of Lines: **24**
    - Integration Type: **Digital**
    - Signaling Protocol: **Wink Start**
    - Framing: **ESF**
    - Line Code: **B8ZS**

    After completion, click the **Save Changes** button.



Select Site: Global

☑ Enable Telephony Integration

Vocera Hunt Group Number: 8229

Number of Lines*: 24

Integration Type

○ Analog
● Digital

Digital Settings

Signaling Protocol: Wink Start

Framing: ESF

Line Code: B8ZS

Note: Saving any changes to digital parameters will cause the telephony server to restart.

Vocera Server 4.0SP6 [Build 1763] Console [Build 1763]

5.3. Configuring the Vocera Badges

A Vocera provided script is used to easily download configuration information to the Vocera Badges. The following screen shows the applicable fields that were changed to effect communication between the Vocera Badge and the Avaya Wireless AP-8.

```
AuthenticationType               Open
EncryptionType                   WPAPSK
SSID                             vocera
ServerIPAddr                     10.20.20.150
ShortPreamble                    FALSE
UpdaterIPAddr                    10.20.20.150
WEPKey1                          31323334353637383930313233
WEPKeySlot                       1
```

6. Interoperability Compliance Testing

Interoperability compliance testing covered connectivity, error recovery, and feature functionality. Feature tests verified the ability of the Vocera Server to communicate with Avaya Communication Manager to make and receive calls, transfer calls, and conference calls. Connectivity tests verified that the Vocera Server was able to connect to Avaya Communication Manager over the T1Wink Start and PRI trunks. The test also verified that the Vocera Badges were able to connect to Avaya Wireless AP-8s, and roam between access points. Error recovery testing verified that the Vocera Server was able to recover connectivity to Avaya Communication Manager under a link failure scenario.

6.1. General Test Approach

All test cases were performed manually. The following features and functionality were verified:

- T1 connectivity between Vocera Telephony Server and Avaya Communication Manager, using the ISDN-PRI protocol
- T1 connectivity between Vocera Telephony Server and Avaya Communication Manager, using a Robbed-bit Wink Start trunk.
- Layer 2 Roaming
- Transfer and Conference calls between the Vocera badges and Avaya IP Telephones
- Repeat basic test scenario for WEP and WPAPSK encryption
- Repeat basic test scenario with T1 PRI 5ESS
- Link failure scenario

6.2. Test Results

All test cases passed. The Vocera Communications System provided connectivity to Vocera Badge users over an Avaya wireless infrastructure, and connected to Avaya Communication Manager over the T1 Wink Start and PRI interfaces.

7. Verification Steps

To verify the solution is properly configured, the following steps can be utilized.

- Place calls between the Vocera Badges to verify proper connectivity through the wireless infrastructure. If the Vocera Badge is not able to reach the Vocera Server, verify that the proper encryption key and SSID was configured for the badge and Avaya Wireless AP-8s.
- Place calls in both directions between Vocera Telephony Server and Avaya Communication Manager. If the calls are not successful, verify the proper configuration for the trunk port between Avaya Communication Manager and the Vocera Telephony Server. To check the trunk between Avaya Communication Manager and the Vocera Telephony Server, the following commands were utilized.
    - **test board** (to check the physical connection between Avaya Communication Manager and the Vocera Telephony Server)
    - **status trunk** (to check the trunk between Avaya Communication Manager and the Vocera Telephony Server)

8. Support

For technical support on the Vocera Communications, call Vocera Support at (800) 473-3971 or send email to support@Vocera.com or visit http://vocera.com.

9. Conclusion

These Application Notes describe the configuration steps required for integrating the Vocera Communications System with Avaya Communication Manager. The systems interoperated successfully, providing a suitable solution for wireless access and connectivity between Vocera Badge and Avaya Communication Manager.

10. References

This section references the Avaya and Vocera Communications documentation that are relevant to these Application Notes.

The following Avaya product documentation can be found at http://support.avaya.com.

[1] Feature Description and Implementation For Avaya Communication Manager, Release 5.0, Issue 6, January 2008, Document Number 555-245-205.

[2] Administrator Guide for Avaya Communication Manager, Release 5.0, Issue 4, January 2008, Document Number 03-300509.

The following Vocera Communications product documentation is installed with the server application:

[3] Vocera 4.0 Command Reference

[4] Vocera Configuration Guide, Version 4.0 Build 1759

[5] Vocera Infrastructure Planning Guide, Version 4.0 Build 1759

[6] Vocera Administration Console Reference, Version 4.0 Build 1759

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 DevConnect Program at devconnect@avaya.com.