3631 Wireless Telephone

Administrator Guide

16-602203
Issue 2
March 2007

Notices

© 2007 Avaya Inc.
All Rights Reserved.

Notice
While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

Note:
Using a cell, mobile, or GSM phone, or a two-way radio in close proximity to an Avaya IP Phone might cause interference.

For full legal page information, please see the complete document, Avaya Legal Page for Hardware Documentation, Document number 03-600759.

To locate this document on our website, simply go to http://www.avaya.com/support and search for the document number in the search box.

Documentation disclaimer
Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands, and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer
Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Warranty
Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the following Web site: http://www.avaya.com/support

Copyright
Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Avaya support
Avaya Inc. provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

Contents 3
Chapter 1: Introduction 5
About This Guide 5
Intended Audience 5
Related Documents 5
Chapter 2: Installation and Configuration 6
Configuration Data Storage 6
DHCP 6
46xxsettings.txt file 7
Existing Parameters 7
New Parameters 8
Downloading 46xxsettings File via USB Cable 11
Phone user interface 12
Access Profiles 12
SIM Card 13
Data Stored on SIM Card 13
SIM Card Security 13
TCP/UDP Port Utilization 14
Communication Manager Configuration for 3631 17
Station Screen 17
IP Codec Set Screen 18
IP Address Mapping Screen 18
IP Network Region Screen 18
Initial Configuration: Getting to Dial Tone 19
Minimal Configuration Data 19
Chapter 3: Startup 20
Startup Flow 20
Chapter 4: Software Upgrade 21
Upgrade Configuration File 21
Preparing for Upgrade 21
Chapter 5: Security and QoS 23
Security 23
Installing Digital Certificates 23
QoS 24
Chapter 6: Backup and Restore 26
Backup Over USB Cable 26
Restore Via USB Cable 27
Chapter 7: Diagnostic Tools 28
Site Survey 28
Audio Parameters Display 28
Syslog 28
Copy Syslog Data to PC via USB Cable 29
Chapter 8: Troubleshooting 30
Phone Displays ‘Nearby Networks’ Screen 30

DHCP Error 30
Bad File Server Address! 30
Upgrade Was Not Successful 30
Phone Stuck on ‘Logon Proceeding’ Message 30
Phone Displays ‘Extension in Use’ Message 30
Phone Displays ‘Extension Error’ Message 31
No Audio 31

Chapter 1: Introduction

About This Guide

This guide provides information on how to install, configure, upgrade, maintain, and troubleshoot a 3631 wireless telephone.

Intended Audience

This document is intended for personnel who administer:

- 3631 telephones
- DHCP, HTTP, TFTP and/or other servers to support the 3631 telephones
- Wireless and wired local area networks

Related Documents

- *4600 Series IP Telephone LAN Administrator Guide*
- *Avaya 3631 Wireless Telephone User Guide*
- *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide*

Chapter 2: Installation and Configuration

This chapter provides information on installing and configuring the 3631 telephone.

Configuration Data Storage

The 3631 telephone stores its configuration data in two primary locations:

- The phone's flash memory
- SIM card

The following configuration data is stored in the phone's flash memory:

- IP address parameters
- Call settings
- Dial plan parameters
- Screen and sound settings, ring tones
- Contacts (full listing)—maximum of 500 entries
- Call Log—maximum of 80 entries

The following configuration data is stored on the phone's SIM card:

- WiFi parameters
- Extension
- Contacts (abbreviated list)—maximum of 100 entries

DHCP

The 3631 telephone supports DHCP for IP address assignment and configuration of other telephone parameters.

Like the 46xx and 96xx IP telephones, the 3631 telephone supports Site-Specific Option Numbers (SSON) 242 and 176. The default is 242. Note that this parameter can be changed only through the phone's menu interface.

The following new parameters are unique to the 3631 telephone and can be set through DHCP using either SSON 242 or 176:

- IPADDP2—the IP address assigned to the 3631 telephone for use with the second Access Profile.
- IPADDP3—the IP address assigned to the 3631 telephone for use with the third Access Profile.
- NETMASKP2—the network mask assigned to the 3631 telephone for use with the second Access Profile.
- NETMASKP3—the network mask assigned to the 3631 telephone for use with the third Access Profile.
- GIPADDP2—the gateway IP address used with the second Access Profile.
- GIPADDP3—the gateway IP address used with the third Access Profile.
- DNSSRVRP2—the IP address of the DNS server used with the second Access Profile.
- DNSSRVRP3—the IP address of the DNS server used with the third Access Profile.
- DOMAINP2—the domain name used with the second Access Profile.

- DOMAINP3—the domain name used with the third Access Profile.

46xxsettings.txt file

The 3631 telephone also can be configured through parameters specified in the 46xxsettings.txt file.

The 46xxsettings.txt file can be delivered to the 3631 telephone through either of the following two methods:

- Automatically over-the-air from an HTTP server. The file is delivered whenever the 3631 telephone is restarted.
- Manually via a USB cable connected between the phone and a PC

Existing Parameters

The 3631 telephone supports many of the parameters supported by the 4600 and 9600 series telephones, specifically the common and H.323-related parameters. These include the following:

- APPSTAT
- AUTH
- DHCPSTD
- DNSSRVR
- DOMAIN
- DSCPAUD
- DSCPSIG
- ENHDIALSTAT
- FTPDIR
- FTRPSRVR
- HTTPSRVR
- ICMPDU
- ICMPRED
- LOGLOCAL
- MCIPADD
- MSGNUM
- OPSTAT
- PHNCC
- PHNDPLENGTH
- PHNIC
- PHNLD
- PHNLDLENGTH
- PHNOL
- PROCPSWD
- PROCSTAT
- REREGISTER
- STATIC
- SYSLANG

- UNNAMEDSTAT
- WMLEXCEPT
- WMLHOME
- WMLPORT
- WMLPROXY

New Parameters

The following new parameters are unique to the 3631 telephone and can be set through the 46xxsettings.txt file:

- WTPROF1—the name assigned to the first Access Profile. The default value is null (“”).
- WTPROF2—the name assigned to the second Access Profile. The default value is null (“”).
- WTPROF3—the name assigned to the third Access Profile. The default value is null (“”).
- WTSSIDP1—the enterprise SSID assigned to the first Access Profile. The default value is null (“”).
- WTSSIDP2—the enterprise SSID assigned to the second Access Profile. The default value is null (“”).
- WTSSIDP3—the enterprise SSID assigned to the third Access Profile. The default value is null (“”).
- WTPWRSAV—the power save mode used with the 3631 telephone. This setting may be overridden by the power save mode setting specified with an Access Profile. The default value is 1 (on).
- WTPWRSAVP1—the power save mode used with the first Access Profile. If not specified, the setting specified for WTPWRSAV shall apply. The default value is 1 (on).
- WTPWRSAVP2—the power save mode used with the second Access Profile. If not specified, the setting specified for WTPWRSAV shall apply. The default value is 1 (on).
- WTPWRSAVP3—the power save mode used with the third Access Profile. If not specified, the setting specified for WTPWRSAV shall apply. The default value is 1 (on).
- WTWMM—the WMM mode used with the 3631 telephone. This setting may be overridden by the WMM mode setting specified with an Access Profile. The default value is 0 (off).
- WTWMMP1—the WMM mode used with the first Access Profile. If not specified, the setting specified for WTWMM shall apply. The default value is 0 (off).
- WTWMMP2—the WMM mode used with the second Access Profile. If not specified, the setting specified for WTWMM shall apply. The default value is 0 (off).
- WTWMMP3—the WMM mode used with the third Access Profile. If not specified, the setting specified for WTWMM shall apply. The default value is 0 (off).
- WTSECP1—the security type used with the first Access Profile. The default value is 0 (none).

- WTSECP2—the security type used with the second Access Profile. The default value is 0 (none).
- WTSECP3—the security type used with the third Access Profile. The default value is 0 (none).
- ENCRYPTP1—the encryption type used with the first Access Profile. The default value is 0 (none).
- ENCRYPTP2—the encryption type used with the second Access Profile. The default value is 0 (none).
- ENCRYPTP3—the encryption type used with the third Access Profile. The default value is 0 (none).
- WTKEYP1—the encryption key used with the first Access Profile. The default value is null (“”).
- WTKEYP2—the encryption key used with the second Access Profile. The default value is null (“”).
- WTKEYP3—the encryption key used with the third Access Profile. The default value is null (“”).
- EAPTYPEP1—the EAP method used with the first Access Profile. The default value is 0 (none).
- EAPTYPEP2—the EAP method used with the second Access Profile. The default value is 0 (none).
- EAPTYPEP3—the EAP method used with the third Access Profile. The default value is 0 (none).
- TRUSTCERTS—the CA certificates used with the Access Profiles. The default value is null (“”).
- WTREGDOM—the regulatory domain used by the 3631 telephone. See the following table for supported values for WTREGDOM.

Regulatory Domain/Country	WTREGDOM Value
Argentina	AR
Australia	AU
Austria	AT
Belgium	BE
Brazil	BR
Canada	CA
China	CN
Denmark	DK
Finland	FI
France	FR
Germany	DE
Greece	GR
Ireland	IE

Regulatory Domain/Country	WTREGDOM Value
Italy	IT
Japan	JP
Liechtenstein	LI
Luxembourg	LU
Mexico	MX
Netherlands	NL
New Zealand	NZ
Norway	NO
Portugal	PT
Russia	RU
Singapore	SG
South Korea	KR
Spain	ES
Sweden	SE
Switzerland	CH
Taiwan	TW
United Kingdom	GB
United States	US

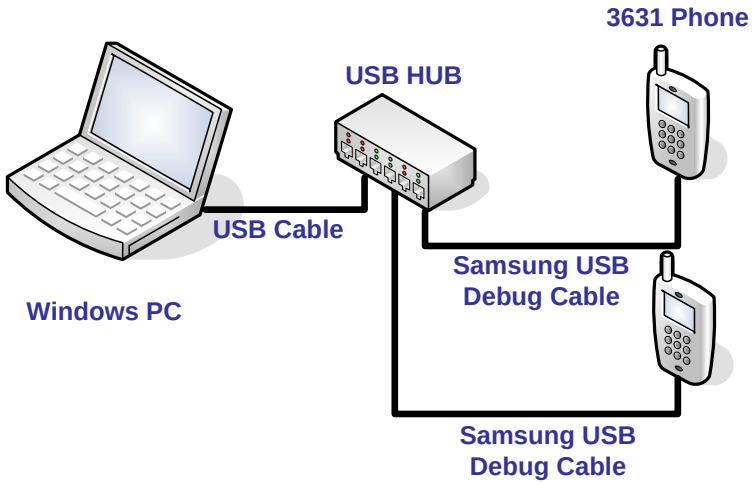
- WTRATE—the data rate used by the 3631 telephone over the wireless link
- WTRTS—the RTS threshold used by the 3631 telephone. The default value is 3000.
- WTFRAG—the fragmentation threshold used by the 3631 telephone. The default value is 3000.
- DNSSRVRP2—the IP address of the DNS server used with the second Access Profile. The default value is 0.0.0.0
- DNSSRVRP3—the IP address of the DNS server used with the third Access Profile. The default value is 0.0.0.0
- DOMAINP2—the domain name used with the second Access Profile. The default value is null (“”).
- DOMAINP3—the domain name used with the third Access Profile. The default value is null (“”).

Downloading 46xxsettings File via USB Cable

The 3631 telephone can support downloading of the 46xxsetings.txt file from a Windows PC that is connected to the phone via a USB cable.

A single PC can be connected to one or multiple phones simultaneously. Connecting to multiple phones requires a USB hub and multiple USB cables.

Connect Samsung USB Debug Cable with the Phone for USB Operations



Note
Only a Samsung cable with an 18-pin connector can be used to support USB operations on the 3631 telephone. This cable is orderable through Avaya. This cable works with the standard Windows USB driver; it is not necessary to install a special USB driver to use this cable.

Use the following procedure to download the 46xxsettings.txt file to the phone via a USB cable.

1. On the 3631 telephone, access the **Advanced Settings** menu
   - Be sure to select the Admin access mode and specify the Admin password (default value is 00000000).
2. From the **Advanced menu**, select the **Service** sub-menu.
3. From the **Service** menu, select **Backup & Restore over USB**
4. From the **Backup & Restore …** menu, select **Download settings file**
   - The "Starting USB driver …" status message is displayed
5. When prompted, insert (or remove and re-insert) the USB cable into its connector on the bottom of the phone.
   - A confirmation window appears, with instructions on copying files.

6. From the Windows PC, drag and drop the 46xxsettings.txt file onto the USB drive folder associated with the phone.
7. Once the file has been copied to the USB drive, return to the phone and select the **Done** softkey.
   - The phone displays a "Downloading file…" status message
8. When the phone displays a "Completed" message, press the **Back** softkey.
   - The phone displays a Confirmation window for restarting the phone.
9. Press the **Restart** softkey to restart the phone and process the new 46xxsettings.txt file.

Phone user interface

The 3631 telephone also can be configured using the phone's display interface and keypad.

For some configuration parameters (i.e., those in the Advanced Settings menu), the phone display interface supports both user (read-only) and administrator (read-write) modes. The admin mode requires a password (the default is 00000000).

For more details on the phone user interface, see the *Avaya 3631 Wireless Telephone User Guide.*

Access Profiles

The 3631 telephone stores configuration information for a particular wireless network in a structure called an Access Profile.

Access Profiles facilitate usage of the telephone in multiple locations, each with different WiFi networks. For example, a phone may have an access profile for a headquarters location and a separate profile for a branch office. Up to three profiles may be stored in the phone.

At startup, the phone attempts to associate with an Access Point using configuration information from its Access Profiles. Each Access Profile is automatically cycled through one time. The cycle stops with the first successful association. The user may interrupt the cycle and manually select a specific Access Profile.

The following configuration data is stored in an Access Profile:
- Profile name
- SSID
- WMM mode
- Power save mode
- Security type
- Encryption type
- Encryption key
- EAP type
- EAP Identity
- EAP username

- EAP password
- Use DHCP
- Phone IP address
- Subnet mask
- Default gateway
- DNS servers
- Domain

SIM Card

The 3631 telephone supports a SIM card for storage of a subset of configuration and user data.

The SIM card is useful in shift environments. Each shift user may have his or her own SIM card that can be inserted/removed from phone at the start/end of the shift. Each individual SIM card can be used to store a single user's personal information such as their extension and private contact numbers.

A SIM card also facilitates provisioning of a replacement 3631 telephone. Users may remove the SIM card from their malfunctioning phone and re-insert it in their new phone. Thus, WLAN connectivity information and (basic) contacts information from the previous phone is preserved in the new phone.

By assigning an optional PIN to a SIM, a user may limit the use of a lost/stolen phone. See the "SIM Card Security" section for more details.

Note:
The 3631 telephone has limited functionality without an installed SIM card. For example, the phone can associate only to discovered APs without security.

Data Stored on SIM Card

The following data is stored on the 3631 telephone's SIM card:

- Access Profiles
- Extension and Password
- Contacts
  - Limited data: just name and single number
- Country

SIM Card Security

A 4-digit PIN code may be assigned to the SIM card. The PIN code is optional and may be disabled through phone user interface.

The user is prompted for the PIN at the startup of the phone. The user must enter the correct PIN code to proceed with the startup process. The default PIN is 1234 ; although, the user may change the PIN through the phone user interface.

Three incorrect PIN attempts in a row disables the SIM card. These attempts may occur over successive startups.

A disabled SIM card may be re-enabled through the PIN Unblocking Key (PUK) process. In this process, a PUK code is required to re-enable the SIM card. A user must enter the PUK code into phone to re-enable the SIM. After 10 unsuccessful PUK code entry attempts, the SIM card is permanently disabled and must be replace

Note
The PUK code is delivered with phone, printed on paper enclosed in the phone box. Avaya does not have a record of the PUK code, so make sure the PUK code is stored securely.

TCP/UDP Port Utilization

Like most network equipment, the Avaya 3631 Wireless Telephones use a variety of protocols, particularly TCP and UDP, to communicate with other equipment in that network - numerous different types of servers, routers, other telephones, etc. Part of this communication identifies which TCP and/or UDP ports each piece of equipment uses to support each protocol and each task within protocol

Depending on your network, you might need to know what ports of ranges are used in the Avaya 3631 Wireless Telephones` operation. Knowing these ports or ranges allows you to appropriately administer your networking infrastructure. In this case, you will find the following material useful.

In Figure1, Figure 2, and Figure 3:

- The box on the left always represents the Avaya 3631 Wireless telephone
- Depending on the diagram, the boxes on the right refer to various pieces of network equipment with which the telephone can (or will) communicate.
- Open-headed arrows (for example,) represent the direction(s) of socket initialization.
- Closed-head arrows (for example,) represent the direction(s) of data transfer.
- The text the arrows point to identifies the port or ports that the Avaya 3631 Wireless Telephones support for the specific situation. Brackets identify ranges when more than one port applies. In addition, the text indicates any additional qualifications or clarification. In many cases, the ports used are the ones called for by IETF or other standards bodies.

Figure 1: Signaling, Audio and Management Diagram

Signaling, Audio and Management

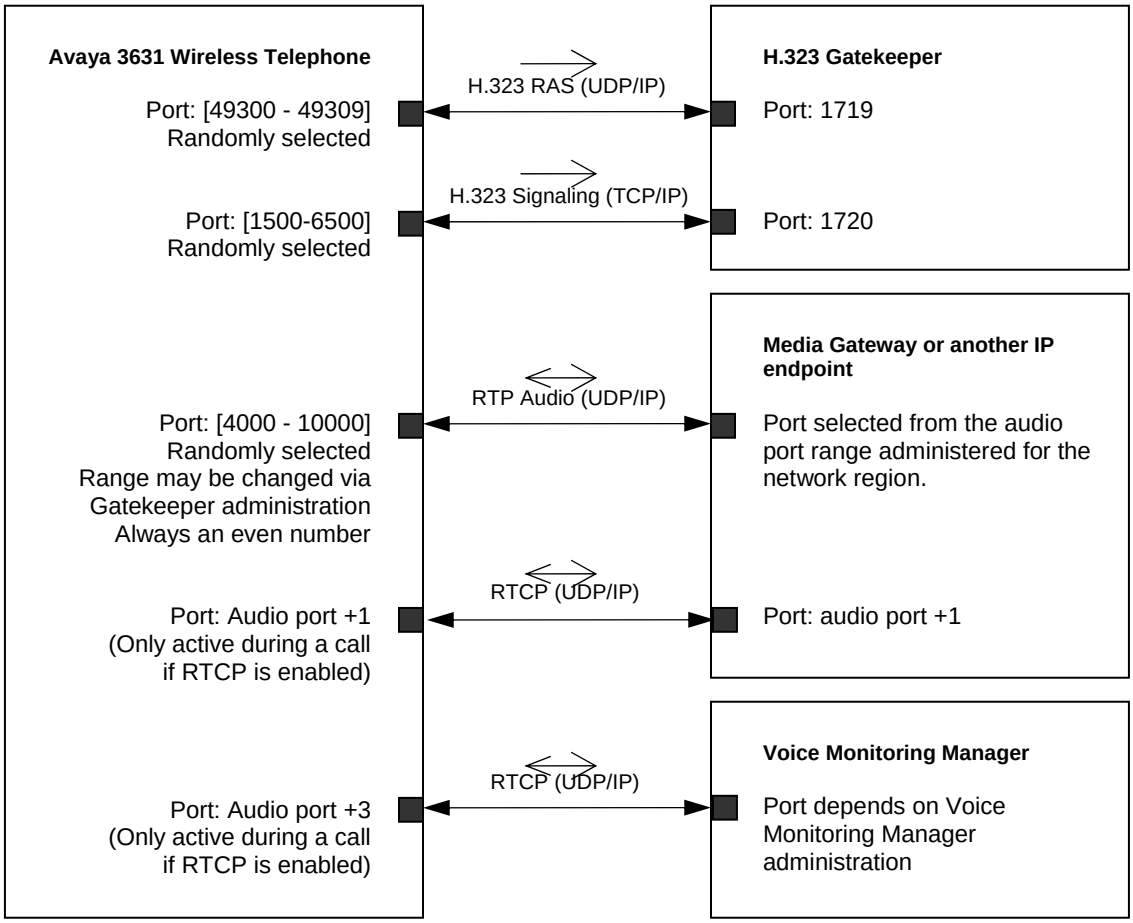


Figure 2: Initialization and Address Resolution Diagram

Initialization and Address Resolution

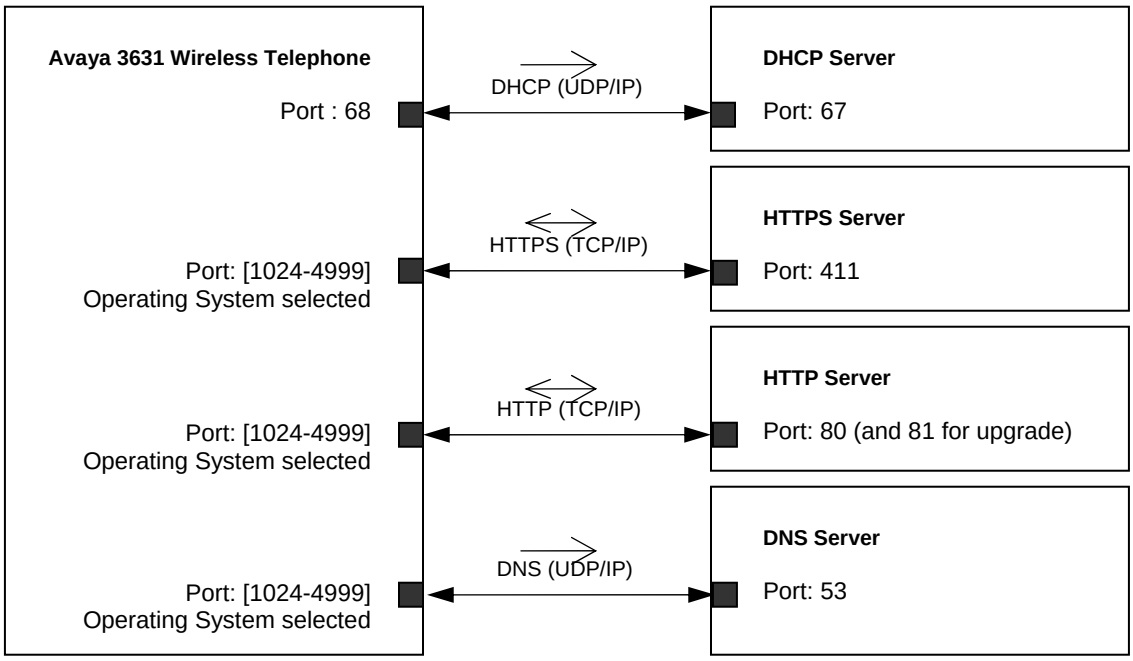
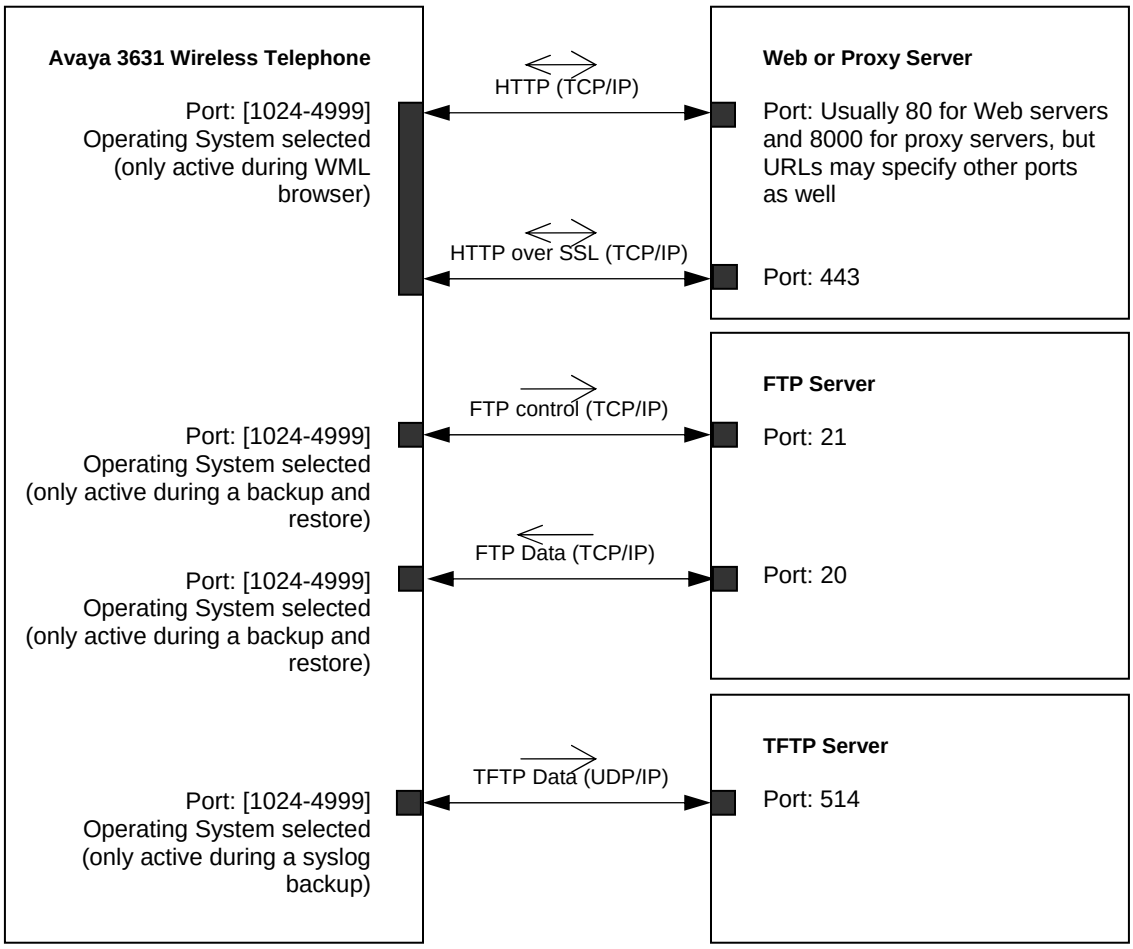


Figure 3: Applications Diagram

Applications



Communication Manager Configuration for 3631

The following sections describe the Communication Manager screens to configure to ensure proper operation of the 3631 phone.

Station Screen

To configure Avaya Communication Manager to support a 3631 telephone, you must create a station record for the phone through the Communication Manager ‘add station’ command. You must enter 4620 as the station type.

The 3631 telephone may be configured as either a primary extension for the user or as bridged extension off of the user’s desktop phone.

All involved stations should have consistent settings for „Direct IP-IP Audio Connections“ and „IP Audio Hairpinning“. If a firewall prohibits direct end to end streams, then „Direct IP-IP Audio Connections“ must be set to „No“.

IP Codec Set Screen

Use the Communication Manager ‘change ip-codec-set x’ command to specify the codecs used by the 3631 phone and other VoIP resources. The following codecs are supported by the 3631 phone:

- G.711
- G.726A-32K
- G.729A
- G.729AB

Set „frames per packet“ to 2 or 3, because the 3631 only supports 20ms packets and 30 ms packets.

IP Address Mapping Screen

Use the Communication Manager ‘change ip-network-map’ command to assign the IP addresses for your 3631 telephones to their appropriate IP network region.

IP Network Region Screen

Use the Communication Manager ‘change ip-network-region *x’* command to configure network region communication settings for the 3631 phones and other VoIP resources.

The first page is used to modify the audio and QoS settings. In the AUDIO PARAMETERS section, use the Codec Set field to specify the codec set used within the region. The UDP port fields specify the UDP port range used for sudio packets. Ensure that no conflicting port filtering is active in a firewall or in the Access Point security settings.

If you are using WMM for QoS on the 3631 phone, use the DIFFSERV/TOS PARAMETERS to set the DiffServ (DSCP) values for Audio and Call Control. The 3631 phone receives these values when it registers with the call server; and it uses these values to set the 802.11e User Priority and Access Category values for the Audio and Call Control (Signaling) packets it transmits. For additional information, see the “QoS” section of this document.

The wireless zone may use several network regions. Nevertheless the same codec sets, or different codec sets with a common subset and order of codecs, must be used. Check page 3 „inter network region connection management“ and specify the correct codec set to be used when communicating between regions.

Initial Configuration: Getting to Dial Tone

There are two main approaches to initial provisioning of the 3631 telephone:

- Open access point
  1. This approach requires an AP with no security, broadcasting its SSID on the network.
  2. The phone automatically discovers this open AP via the 802.11 scanning process.
  3. The user selects this AP from the 'Nearby Networks' menu on the telephone.
  4. The phone associates with this AP, then proceeds to download all its configuration information via DHCP and the 46xxsettings.txt file.

     Note
     This may involve transfer "in the clear" of the phone's WiFi encryption key, since 46xxsettings.txt file data is not encrypted when it is sent over the network.

  5. Once the phone is restarted, it is able to access secure APs using the configuration information acquired via DHCP and the 46xxsettings.txt file.

- Secure access point
  1. The phone is pre-configured with the minimum data required to access a secure AP. This data may be entered manually through the telephone keypad or downloaded in a 46xxsettings.txt file over a USB connection. See the next section, "Minimal Configuration Data," for more information.
  2. The phone downloads its remaining configuration information over-the-air via DHCP and the 46xxsettings.txt file.

Minimal Configuration Data

The following data is the minimum required for associating with an AP, accessing a DHCP server, and accessing a file server from which to download the 46xxsettings.txt file:

- SSID (WTSSIDP[1-3])
- Security Type (WTSECP[1-3])
- Encryption Type (ENCRYPTP[1-3])
- Encryption Key (WTKEYP[1-3])
- EAP Type (EAPTYPEP[1-3])—only required for Security Types, WPA-802.1X or WPA2-802.1X
- Country (WTREGDOM)—only required if outside the United States.
- DHCP SSON—only required if using value other than 242
- File Server IP Address—required if not passed by DHCP

Chapter 3: Startup

The 3631 telephone is started by pressing the End button. There are opportunities throughout the startup process to interrupt processing. This may be accomplished by pressing either the Advanced or Offline softkeys, which provide access to the Advanced and Offline menus, respectively.

Status messages are displayed on the telephone throughout the startup process. There are two modes for startup messages: Normal and Verbose. You may access Verbose messages by pressing the Right navigation key. Once in Verbose mode, you may scroll up or down to view messages.

Startup Flow

Following is a summary of the 3631 telephone startup process.

1. The phone loads software from its flash memory into RAM.
   - The Avaya logo and progress bar are displayed at this stage.
2. The keypad backlight is illuminated.
   - The OneX animation and sound are played.
3. (Optional, but enabled by default.) The phone prompts for the SIM card PIN.
4. The phone attempts to associate with an AP.
   - Access Profile data is used during the association attempt.
   - The user may interrupt automated Access Profile processing and manually select an Access Profile.
5. If association is unsuccessful using Access Profiles, the phone automatically searches for nearby WiFi networks.
   - The user may also initiate the search manually via the Search softkey.
6. (Optional) The phone attempts 802.1X authentication, automatically supplying the user's 802.1X identity, username, and password as necessary.
7. (Optional) The phone contacts the DHCP server to obtain IP address and other information.
   - Alternatively the phone may be configured to use static addressing.
8. The phone performs router discovery.
   - The phone restarts if a router is not found. If there is no router on the network, another machine must be able to reply to the ARP request for the GW IP address.
9. The phone downloads the 46xxsettings.txt file from an HTTP server.
   Note:
   The 3631 downloads the 46xxsettings from an HTTP server. The 46xxsettings file cannot be downloaded using the Communication Manager HTTPS service.
10. The phone checks its firmware version, and initiates an upgrade if necessary.
11. The phone attempts to contact a call server and perform H.323 registration.
12. The phone prompts for an extension and password.
    - The user may invoke unnamed registration by selecting the Guest softkey.
13. The phone proceeds to register the extension with a call server.
    - The user is notified if an extension already is in use.
14. The startup process completes with display of the Call Appearance screen.

Chapter 4: Software Upgrade

The 3631 telephone supports a firmware upgrade program that is invoked automatically during telephone startup. During the upgrade process, the phone downloads a new software image from an HTTP server, erases its current image from memory, and writes the new image.

The telephone first downloads an upgrade configuration file. After receiving the upgrade file, the phone compares its current software version with the version information in the upgrade file. If the versions are different, the phone downloads new binary files in order according to the upgrade file list. If the versions are the same, the upgrade does not execute.

If a problem occurs during downloading (network issue, disconnection, no server response), the phone reboots itself and attempts the upgrade again. This process repeats until it is successful.

Upgrade Configuration File

The 3631 Upgrade Configuration file (3631upgrade.txt) is a simple text file. The file has information about the 3631 upgrade package (model number, date, version, block/file name, block size, checksum…).

In addition to the text file, a digitally signed file (3631upgrade.txt.asc) is provided for security purposes. During an upgrade the phone compares the decrypted signature file with a hash of the upgrade file. If these values are not equal, the upgrade does not proceed.

See the following page for a sample upgrade configuration file.

Preparing for Upgrade

Use the following process to prepare for a 3631 firmware upgrade:

1. Copy the 3631upgrade.txt file to the web server root directory. (This is the same directory as where the 46xxsettings.txt file is stored.)
2. Create a *down* subdirectory under the web server root directory.
3. Copy all 3631 package files—including the 3631upgrade.txt file—to the *down* directory.
   Note:
   You must create a *down* subdirectory with its associated files; otherwise, the upgrade procedure will not execute.
4. Reboot the phones to begin the upgrade.

Following is a sample upgrade configuration file.

```
WIFI PHONE UPGRADE CONFIGURATION

[INFORMATION]
MODEL=SMT-W6100
DOMAIN=Avaya
VER=0.5.2
DATE=2007-01-12 14:47:02
CHKVER=yes
WDTIMER=enable
PRINT_LEVEL=1
COMPRESS=yes

[LIST]
_BLK=k_upgrade
_MNT=none
_FILE=zImage_ug
_AUTH=0
_VER=0.5.2
_SIZE=961608
_CRC=0x65581591

_BLK=r_upgrade
_MNT=none
_FILE=rootfs_ug.cramfs
_AUTH=0
_VER=0.5.2
_SIZE=1327104
_CRC=0xa3dd7d2a

_BLK=k_normal
_MNT=none
_FILE=zImage_nm
_AUTH=1
_VER=0.5.2
_SIZE=961608
_CRC=0x65581591

_BLK=r_normal
_MNT=none
_FILE=rootfs_nm.cramfs
_AUTH=1
_VER=0.5.2
_SIZE=2461696
_CRC=0xc900bc3a

_BLK=home
_MNT=none
_FILE=home.jffs2
_AUTH=1
_VER=0.5.2
_SIZE=16056320
_CRC=0x6447ac80

_BLK=home.compress
_MNT=none
_FILE=home.jffs2.gz
_AUTH=1
_VER=0.5.2
_SIZE=5768390
_CRC=0x0b12d784

_BLK=phone
_MNT=none
_FILE=phone.cramfs
_AUTH=1
_VER=0.5.2
_SIZE=1212416
_CRC=0xda97dbcf

[END]
```

Chapter 5: Security and QoS

Security

The following security methods are supported on the 3631 telephone:

- WEP
  - 40-bit and 128-bit encryption
- WPA --Temporal Key Integrity Protocol (TKIP)
  - With Pre-Shared Key (PSK)
  - With 802.1X Authentication
- WPA2 —Advanced Encryption Standard (AES)
  - With Pre-Shared Key (PSK)
  - With 802.1X Authentication

The following EAP methods are supported in conjunction with 802.1X authentication:

- EAP-TLS
- PEAPv0/EAP-MSCHAPV2
- PEAPv1/EAP-GTC
- LEAP
- TTLS-CHAP
- TTLS-MD5
- TTLS-MSCHAP
- TTLS-MSCHAPV2

Installing Digital Certificates

The 3631 telephone supports installation of digital CA certificates as well as a digital device certificate/private key for use with 802.1X authentication.

All certificates must be in PEM format. The certificates must have the following filenames:

- cacert1.pem—the CA certificate associated with the first Access Profile
- cacert2.pem—the CA certificate associated with the second Access Profile
- cacert3.pem—the CA certificate associated with the third Access Profile
- user_cert.pem—the user/device certificate for the phone. Required for EAP-TLS authentication
- private_key.pem—private key for the phone. Required for EAP-TLS authentication
- private_key_passwd.txt—file containing the password used to encrypt/decrypt the private key. Required for EAP-TLS authentication

CA certificates may be downloaded to the telephone through either of the following methods:

- Automatically over-the-air via the TRUSTCERTS parameter in a 46xxsettings.txt file
- Manually from a PC via the USB cable

To ensure privacy of the private key, it is recommended to download the digital device certificate and private key using the USB cable only

Use the following procedure to download digital certificates to the phone via a USB cable.

1. On the 3631 telephone, access the **Advanced Settings** menu
   - Be sure to select the Admin access mode and specify the Admin password (default value is 00000000).
2. From the **Advanced menu**, select the **Service** sub-menu.
3. From the **Service** menu, select **Backup & Restore over USB**
4. From the **Backup & Restore …** menu, select **Download settings file**
   - The "Starting USB driver …" status message is displayed
5. When prompted, insert (or remove and re-insert) the USB cable into its connector on the bottom of the phone.
   - A confirmation window appears, with instructions on copying files.
6. From the Windows PC, drag and drop the certificate file(s) onto the USB drive folder associated with the phone.
7. Once the file(s) have been copied to the USB drive, return to the phone and select the **Done** softkey.
   - The phone displays a "Downloading file…" status message
8. When the phone displays a "Completed" message, press the **Back** softkey.

The following procedure may be used to view or delete digital certificates installed on the phone:

1. On the 3631 telephone, press the **A** key
2. Press the **Left** navigation key to display the **Log in/Log out** menu.
3. Scroll down and select the **Certificates** entry.
   - The phone displays the list of installed certificates
4. Scroll to the desired certificate and press Select.
5. Scroll to and select the **View** or **Delete** option as appropriate.

QoS

The 3631 telephone supports WMM Basic for QoS. WMM Basic is specified by the WiFi Alliance, and is a subset of the IEEE 802.11e standard. WMM prioritizes voice packets for preferential treatment by APs.

WMM may be enabled/disabled for each Access Profile through the phone's display interface. You may also configure WMM support through the 46xxsettings.txt file.

If WMM is enabled, you must also set the appropriate QoS settings in your Access Points and call server.

In the Access Point, make sure that DiffServ (DSCP) values for packets arriving from the wired network (including those from the call server) are mapped to the desired 802.11e Access Categories.

For Communication Manager, you must set DiffServ values for Audio and Call Control in the IP Network Region screen to ensure proper priority for the phone's audio and voice signaling packets. The 3631 phone receives these values when it registers with the call server; and it uses these values to set the 802.11e User Priority and Access Category values for the Audio and Call Control (Signaling) packets it transmits. The following table shows the 3631 phone's mapping of DiffServ values to 802.11 User Priority and Access Category values.

DiffServ Range (Decimal)	Mapped DiffServ Value	User Priority (UP)	Access Category (AC)
56-63	60	7	AC_VO
48-55	52	6	AC_VO
40-47	46	5	AC_VI
32-39	38	4	AC_VI
24-31	24	3	AC_BE
16-23	18	2	AC_BK
8-15	10	1	AC_BK
0-7	0	0	AC_BE

Note:
The Communication Manager default values for Audio (46) and Call Control (34) map to the Video Access Category (AC_VI) in the 3631 phone.

The 3631 telephone does not support the SpectraLink SVP protocol for QoS, nor does it require installation of the Avaya Voice Priority Processor (AVPP).

Chapter 6: Backup and Restore

The 3631 telephone supports multiple options for backup and restore of a subset of user data. These options include the following:

- Automated backup/restore over-the-air to/from an FTP server
- Manually initiated restore over-the-air from an FTP server
- Manual backup/restore to/from a PC via a USB cable

Parameters for over-the-air backup/restore are specified through the phone user interface (or via the 46xxsettings.txt file). These parameters include the following:

- FTP server IP address (FTPSRVR)
- FTP directory (FTPDIR)
- FTP username/password

The 3631 telephone supports the following two backup files:

- *Ext*_96xxdata.txt
  - where *Ext* is user's extension (e.g., 22335_96xxdata.txt)
- *Ext*_96xxcalllog.txt

The 3631 telephone may share its _96xxdata.txt file with 96xx IP telephones. The file must be stored in a common directory, accessible to both FTP (3631) and HTTP (96xx) servers.

Backup Over USB Cable

Use the following procedure to back up user data to a PC via a USB cable.

1. On the 3631 telephone, access the **Advanced Settings** menu
   - Be sure to select the Admin access mode and specify the Admin password (default value is 00000000).
2. From the **Advanced menu**, select the **Service** sub-menu.
3. From the **Service** menu, select **Backup & Restore over USB**
4. From the **Backup & Restore …** menu, select **Backup user data**
   - The "Starting operation …" status message is displayed
5. When prompted, insert (or remove and re-insert) the USB cable into its connector on the bottom of the phone.
   - A confirmation window appears, with instructions on copying files.
6. From the Windows PC, open the USB drive folder associated with the phone.
7. Drag and drop the *Ext_96xxdata.txt* file and *Ext_96xxcalllog.txt* file from the USB folder to the desired folder on the PC.
8. Once the files have been copied to the desired folder, return to the phone and select the **Done** softkey.
   - The phone displays a "Starting user data backup…" status message
9. When the phone displays a "Completed" message, press the **Back** softkey.

Restore Via USB Cable

Use the following procedure to restore user data from a PC to the phone via a USB cable.

1. On the 3631 telephone, access the **Advanced Settings** menu
   - Be sure to select the Admin access mode and specify the Admin password (default value is 00000000).
2. From the **Advanced menu**, select the **Service** sub-menu.
3. From the **Service** menu, select **Backup & Restore over USB**
4. From the **Backup & Restore …** menu, select **Restore user data**
   - The "Starting user data restore …" status message is displayed
5. When prompted, insert (or remove and re-insert) the USB cable into its connector on the bottom of the phone.
   - A confirmation window appears, with instructions on copying files.
6. From the Windows PC, drag and drop the *Ext_96xxdata.txt* file and *Ext_96xxcalllog.txt* file onto the USB drive folder associated with the phone.
7. Once the files have been copied to the USB drive, return to the phone and select the **Done** softkey.
   - The phone displays a "Restoring data…" status message
8. When the phone displays a "Completed" message, press the **Back** softkey.

Chapter 7: Diagnostic Tools

The following diagnostic tools are provided with the 3631 telephone:

- Site survey
- Audio parameters display
- Syslog

The 3631 telephone does not contain a MIB and does not support the SNMP protocol.

Site Survey

The 3631 telephone provides a basic site survey utility. The utility provides the following details for each discovered AP:

- Currently active channel
- SSID
- RSSI
- Supported data rates
- MAC address

A user may start the site survey by selecting Site Survey from the Advanced Settings menu. The initial display is a list of discovered APs, identifying their SSIDs and active channels. For additional information on a specific AP, the user scrolls to the desired AP and presses the 'Details' softkey.

The administrator can disable user access to the Site Survey utility via a setting in the telephone's Service menu.

Audio Parameters Display

The 3631 telephone can display real-time audio data for the currently active call. The following data is provided:

- Received Coding
- Packet loss
- Packetization delay
- One-way network delay
- Network jitter delay

A user may initiate the display of audio parameters by pressing the Options softkey during an active call, then selecting Audio Parameters.

Syslog

The 3631 telephone can send phone error and event messages to an external system. There are two options for sending messages:

- Automatically over-the-air to a Syslog server
- Manually over a USB cable to a connected PC

To enable automated sending of messages, you must specify the Remote Log Server IP Address in the phone. This is specified via the Advanced Settings menu, IP Addresses sub-menu.

You specify the type of messages sent to a Syslog Server via the Advanced Settings menu/Services sub-menu/Debug Level option. The following message levels may be specified:

- Disabled
- Emergencies
- Alerts
- Critical
- Errors
- Warnings
- Notices
- Information
- Debug

Copy Syslog Data to PC via USB Cable

The 3631 telephone stores syslog data in the following two files on the phone:

- Logfile_1.txt—contains the most recent set of log messages
- Logfile_2.txt—contains the next-to-most recent set of messages

Each file has a maximum size of 32KB.

Use the following procedure to copy syslog data from the phone to a PC via a USB cable.

1. On the 3631 telephone, access the **Advanced Settings** menu
   - Be sure to select the Admin access mode and specify the Admin password (default value is 00000000).
2. From the **Advanced menu**, select the **Service** sub-menu.
3. From the **Service** menu, select **Backup & Restore over USB**
4. From the **Backup & Restore …** menu, select **Copy syslog to PC**
   - The "Starting operation …" status message is displayed
5. When prompted, insert (or remove and re-insert) the USB cable into its connector on the bottom of the phone.
   - A confirmation window appears, with instructions on copying files.
6. From the Windows PC, open the USB drive folder associated with the phone.
7. Drag and drop the *logfile_1.txt* file and *logfile_2.txt* file from the USB folder to the desired folder on the PC.
8. Once the files have been copied to the desired folder, return to the phone and select the **Done** softkey.
   - The phone displays a "Starting syslog backup…" status message
9. When the phone displays a "Completed" message, press the **Back** softkey.

Chapter 8: Troubleshooting

Phone Displays 'Nearby Networks' Screen

- Phone has failed to associate with any Access Point network defined within Access Profiles. Phone has discovered other APs not defined in Access Profiles.
- Check each Access Profile configured in the phone. Verify the following phone settings are correct and match those of AP with which you're trying to associate:
  - SSID, Security Type, Encryption Type, Encryption Key, Country
- Verify APs for Access Profiles are up and that phone is within range of these APs

DHCP Error

- Phone fails to receive all configured parameters (e.g., Call Server IP address) via DHCP
  - Confirm that phone is configured for correct DHCP SSON value. Default is 242, not 176.

Bad File Server Address!

- Phone has failed to find HTTP server from which to download 46xxsettings file
- Confirm phone is configured with correct File Server IP address
  - If phone receives File Server address via DHCP, confirm phone's DHCP SSON setting is correct. Default is 242, not 176.
- Confirm there is network connectivity to server

Upgrade Was Not Successful

- Phone displays message, 'Upgrade was not successful. Upgrade will be retried now.'
- Phone has passed critical stage in upgrade process (erasing memory), but has not successfully downloaded all files.
- Phone will continue to loop in upgrade process until all files are downloaded.
- Confirm upgrade files are in appropriate directories (e.g., 'down') on HTTP server
- Verify there is network connectivity to HTTP Server and that HTTP Server is up

Phone Stuck on 'Logon Proceeding' Message

- Phone is attempting unsuccessfully to contact Call Server
- Verify phone is configured with correct Call Server IP address
  - If phone receives Call Server address via DHCP, confirm phone's DHCP SSON setting is correct. Default is 242, not 176.
- Verify there is network connectivity to Call Server and that Call Server is up

Phone Displays 'Extension in Use' Message

- Message indicates extension entered by user into 3631 phone is currently in use on another phone.
- User has two options:
  - Log in with different extension. User presses 'Retry' softkey, then enters new extension, password

– Log in with original extension, while unregistering extension from other phone. User presses ‘Retry’ softkey, and enters/confirms original extension, password. Then presses ‘Yes’ softkey when prompted to Unregister User.

Phone Displays ‘Extension Error’ Message

- Message indicates extension entered by user into 3631 phone is not recognized on current call server
- Verify extension entered correctly
- Verify call server IP address is correct

No Audio

One or all parties on a call are experiencing no audio. Check the following:

- Ensure Mute button is off on all phones
- Communication Manager ‘Station’ form. All involved stations should have consistent settings for „Direct IP-IP Audio Connections“ and „IP Audio Hairpinning“. If a firewall prohibits direct end to end streams, then „Direct IP-IP Audio Connections“ must be set to „No“. Use ‘Status Station’ command to check results.
- Communication Manager ‘IP-Network-Map’ form. Ensure all endpoint addresses are assigned to appropriate IP network regions
- Communication Manager ‘IP-Network-Region form. Ensure the UDP port fields specify the UDP port range supported by the endpoint. Ensure that no conflicting port filtering is active in a firewall or in the Access Point security settings. The wireless zone may use several network regions. Nevertheless the same codec sets, or different codec sets with a common subset and order of codecs must be used. Check page 3 “inter network region connection management” and ensure the correct codec set is being used if communicating between regions.
- Communication Manager ‘IP-Codec-Set’ form. Ensure the codecs are supported by the endpoints in the call. The following codecs are supported by the 3631 phone:
    - G.711
    - G.726A-32K
    - G.729A
    - G.729AB

  Ensure „frames per packet“ is set to 2 or 3, because the 3631 only supports 20ms packets and 30 ms packets.