NetVanta Unified Communications Technical Note

Installing and Configuring the Polycom SpectraLink 8002

Introduction

The Polycom SpectraLink 8002 is a mobile handset used for workplace IP telephone systems. The handsets operate over an 802.11b wireless Ethernet local area network (LAN), providing users a wireless voice over IP (VoIP) extension. By seamlessly integrating into a Session Initiation Protocol (SIP) environment, handset users are provided with high-quality mobile voice communications throughout the workplace. The handset gives users the freedom to roam throughout the workplace while providing all the features and functionality of a SIP desk phone.

The purpose of this technical note is to provide instructions on installing and configuring the Polycom SpectraLink 8002 to use with NetVanta Unified Communications products.

DHCP Server Configuration

When a SpectraLink handset is powered on, it retrieves its IP address from the Dynamic Host Configuration Protocol (DHCP) server. It also reads DHCP option 66 for the IP address of the Trivial File Transfer Protocol (TFTP) provisioning server. If this option is not present, then SpectraLink handsets will not be provisioned or automatically upgrade their firmware.

To configure the DHCP server option 66 for Windows® Server 2003/2008 and Windows Small Business Server (SBS) 2003/2008:

1. Select **Start > Control Panel > Administrative Tools > DHCP**.
2. Right-click the domain where you want the SpectraLink phones to be provisioned and select **Set Predefined Options**.
3. Look for **Option 66**.
    - If Option 66 *is not* already defined, select **Add**.

      Name **UC Server Provisioning Server**
      Data Type **String**
      Code **66**
      Description **UC Server Provisioning Server IP Address**

    - If Option 66 *is* already defined:
        - If it is defined as a string type and the value is the IP address for the UC server, no action is required.
        - If it is not defined as a string type and/or the value is not the IP address for the UC server, automatic detection of the SpectraLink phones is not possible unless this option can be changed as per the instructions above.
4. Select **OK.**
5. Right-click the **Scope Options** for the domain and select **Configure Options**.
6. Select the check box next to **Option 66**.
7. For the **String** field, enter the IP address of the UC server (for example, **123.45.67.89**).
8. Select **OK.**

NOTE: *For DHCP servers other than Windows Server 2003/2008 and Windows SBS 2003/2008, consult the appropriate documentation and fill in the options as indicated in Step 3.*

Creating the Configuration Files for Provisioning

SpectraLink handsets are provisioned through configuration files located on the TFTP server. The configuration files cannot be automatically created by the UC server; they need to be modified manually on a per-handset basis. The following sections describe how to set up the SpectraLink configuration files.

Extracting the Configuration and Firmware files

Included with this technical note is a zip file containing SpectraLink configuration file templates and firmware files. All but one of these files must be copied to the TFTP folder of the UC server; the remaining file is to be used as a template for creating per-identity configuration files.

1. Extract the following files to *X*:\Program Files\ADTRAN\NetVanta UC Server\Data\TFTP, where *X* is the drive where the UC server program files are installed:

    - pd11gl3.bin
    - pd11wsd.bin
    - pd11wsd3.bin
    - pi110001.bin
    - sip_allusers.cfg
    - slnk_cfg.cfg

2. Extract **sip_xxxx.cfg** to a temporary directory. You will use this file as a template to create identity specific configuration files.

Modifying the System Configuration File

The system configuration file **sip_allusers.cfg** provides common system information for all SpectraLink handsets in the network. It must be modified with site-specific information.

To modify the system configuration file:

1. Open **sip_allusers.cfg**, located in *X*:\Program Files\ ADTRAN\NetVanta UC Server\Data\TFTP, where *X* is the drive where the UC server program files are installed.
2. Replace all instances of **UC_SERVER_IP_ADDRESS** with the IP address for the UC server.
3. Replace **UC_SERVER_PROXY_PORT** with the UC server SIP registration port: **5060**.

Sample contents for the SpectraLink system configuration file:

```
# SIP ALL USERS Configuration file
#-------------------------------------------------------------------------------#
# Codec preference order
CODECS = g711u, g711a
#-------------------------------------------------------------------------------#
#
# This specifies the type of proxy that the PBX uses.
# UC Server's PBX is similar to Asterisk.
#
PROXY1_TYPE  = Asterisk
#-------------------------------------------------------------------------------#
## Proxy configuration
# Replace all instances of 'UC_SERVER_IP_ADDRESS' with the IP address for UC Server
# Replace 'UC_SERVER_PROXY_PORT' with the port for UC Server, default is 5060
PROXY1_ADDR = 192.168.8.83:5060
PROXY1_KEYPRESS_2833 = enable
PROXY1_KEYPRESS_INFO = disable
PROXY1_HOLD_IP0 = disable
PROXY1_PRACK = enable
PROXY1_REREG_SECS=3600
PROXY1_KEEPALIVE_SECS=14
PROXY1_DOMAIN = 192.168.8.83      # Replace this with the IP address for the UC server
PROXY1_CALLID_PER_LINE = disable
PROXY1_MAIL_ACCESS = *4386245
```

Gathering Information

To configure the handset, you need the following information:

SIP User ID: This is equivalent to the identity address that you want to associate with the device.

Authentication User ID: This is the SIP authentication identifier associated with the above identity. This is required by any SIP endpoint to register with the SIP private branch exchange (PBX).

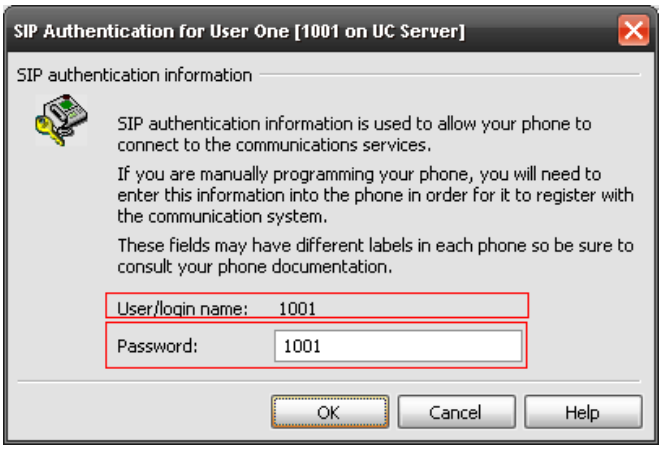
Authentication Password: This is the SIP authentication password associated with the above identity.

Determining the Authentication ID and Password as the User (that owns the identity)

1. Start the UC client.
2. Log in as the user you want to associate to the device.
3. In the bottom left pane, take note of the identity name.

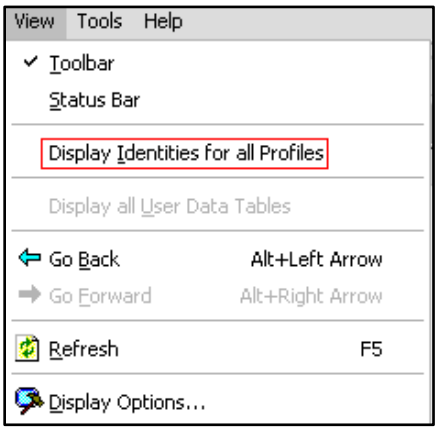
4. Select the icon on the right and select **SIP Authentication**.

5. Record the **User/login name** and **Password** from the following dialog box. You will need them later when you configure the device.

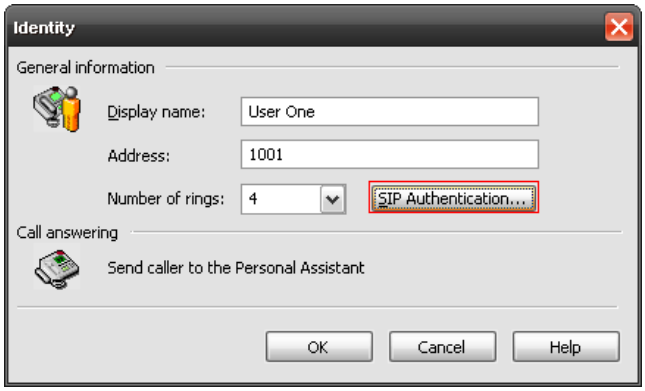


Determining the Authentication ID and Password as the Administrator

1. Start the UC client.
2. Log in as the administrator, or with an authentication that has access to the administrator system profile.
3. Select the **Identities** tab in the left pane.
4. Navigate to **View > Display Identities for all Profiles**.



5. Find the identity in the list that you want to use and double-click the entry.
6. Select **SIP Authentication**.



7. Record the **User/login name** and **Password** from the following dialog box. You will need them later when you configure the device.

Creating the Identity Configuration Files

Each handset requires an individual configuration file whose name is based on the identity being assigned to the handset. These configuration file names are formatted **as sip_xxxx.cfg,** where **xxxx** is the identity address. For example, if a handset is being assigned identity 3562, then the corresponding configuration file name is **sip_3562.cfg**. The file **sip_xxxx.cfg** is included in the zip file accompanying this technical note; it will be used as a template for creating these identity configuration files.

To create an identity configuration file:

1. Open **sip_xxxx.cfg**.
2. Replace the value after the equal sign (=) for the following parameters:

   LINEx = The identity number

   LINEx_CALLID = The Caller ID sent for outgoing calls

   LINEx_AUTH = The user name and password to authenticate with the UC server. The user name and password should be separated by a semi-colon (**;**). For example, **1001; 1001**.

   Refer to *Gathering Information on page 5* to obtain the SIP authentication user name and password for the identity.

   If the handset only requires one identity, you can duplicate the first line definition for the second and third line definitions. This configures the handsets for three lines on which you can make and receive calls with the same identity. If the handset requires multiple identities, you can add additional identities by configuring them for the second and/or third line definitions. Only one line definition is required.

3. Save the file as **sip_xxxx.cfg**. For example, if the value for **LINE1** is **1001**, the file should be saved as **sip_1001.cfg**.
4. Repeat Steps 1 through 3 for any additional SpectraLink handsets.

Sample contents for the identity configuration file:

```
# SIP Identity Configuration file

#-------------------------------------------------------------------------------------------------#

# Line definitions

#  Line definitions do not necessarily have to have different extensions
LINE1           = 1005
LINE1_PROXY     = 1
LINE1_CALLID    = Jon Doe
LINE1_AUTH      = 1005; 1005


# Two lines may map to the same extension to allow second incoming calls.
# To add additional lines to the primary identity, duplicate the information from LINE1
LINE2           = 1005
LINE2_PROXY     = 1
LINE2_CALLID    = Jon Doe
LINE2_AUTH      = 1005; 1005


# You can add an additional identity
LINE3           = 3041 #
LINE3_PROXY     = 1 # This is the proxy configured in sip_allusers, you should not need to change this
LINE3_CALLID    = Jon ext 3041
LINE3_AUTH      = 3041; 3041
```

Programming the Favorite Dialed Number List

The handset can also be programmed to store favorite numbers (speed dial) by adding favorites to the identity configuration file.

To add favorites to the handset:

1. Open **sip_xxxx.cfg** for the identity configuration file you wish to modify (where **xxxx** is the corresponding identity for a particular handset).

2. At the bottom of the file you can add entries by following the instructions in that section.

Sample values for “favorites” configuration:

```
#  Favorite Dialed Number list.
#   For the 8002 you can define up to 8 total entries including any defined in
#   sip_allusers.cfg. The 8020 and 8030 can support up to 15.
#   You can enclose a string in quotes to allow for spaces.
#   Each favorite can be complete SIP URI
#   Format is:
#       FAVORITE = dial_string; username
#

#    The username can be blank and can include escaped chars.
#FAVORITE = "3001"; "Bob"
#FAVORITE = 3032; "Jill in Accounting"
#FAVORITE = 3013; "SoundPoint 3013"
#FAVORITE = 3020; "Jane"
#FAVORITE = "93035551212"; "Richard's Cell"
#

#   Favorites can also be configured to prompt users to enter more digits. Users will
#   be prompted with characters inside the <>'s.
#   In the below example if the Feature Access Code for call forwarding is #21
#   When the user selects the Favorites option and then Call Forward they would
#   see "Call Forward Enter Destination:"
#   They would then have a chance to enter the fwd destination before pressing the send key
#FAVORITE =  #21<Enter Destination:>; "Call Forward"
#   In the example below the user would be prompted "Call Pickup Pickup Number:
#   to enter a call pickup number # for a call pickup Feature Access Code starting with *5
#FAVORITE =  *5<Pickup Number:>; "Call Pickup"
#-------------------------------------------------------------------------------------------------#

FAVORITE = "2530"; "Bob Thompson"
FAVORITE = "93035551212"; "Ed Jones Cell"
```

Configuring the Handset

Once the configuration files are in place, the SpectraLink handset must be configured to connect to the wireless network, and must also be configured to use a specific identity (corresponding to a configuration file created in *Creating the Configuration Files for Provisioning on page 3*). This section provides instructions on configuring the SpectraLink 8002 to connect to your wireless network and configuring the handset identity.

NOTE: *The **Wi-Fi Multimedia Quality of Service (WMM QoS)** setting must be enabled on the wireless access point (AP). SpectraLink handsets will not connect to the access point if this option is not enabled. The access point's firmware may need to be updated to support WMM. Consult your wireless access point documentation for information.*

Configuring the Wireless Network Settings

To connect the SpectraLink 8002 to your network, you must configure the wireless network settings to correspond to your network.

Entering and editing Admin menu options:

An asterisk (*) next to an option on the display indicates that it is selected. Use the **Up**, **Down**, and **Select** side buttons and the softkeys to navigate and select:

Up/Down button:	Displays the previous/next menu item.
Select button:	Selects the menu item or option.
OK softkey:	Selects the menu item or option.
Save softkey:	Saves the entry.
Bksp softkey:	Backspaces to allow editing of entry.
Cncl softkey:	Cancels edit and returns to previous menu level.
Up softkey:	Returns to previous menu level.
Exit softkey:	Exits the menu (at the top level).
End Call key:	Exits to standby mode (from any level).

To access the Admin menu:

With the handset powered off, press and hold the **Power Off** key. While holding the **Power Off** key, press and release the **Power On** key. The **Admin** menu will appear.

NOTE: *If an **Admin** password has been previously set, the handset will require that password before revealing the **Admin** menu. The default password is **123456**. If no password is set, the handset will proceed directly to the **Admin** menu.*

Configuring a Static IP Address

1. In the **Admin** menu, scroll down to **Network Config**. Select **OK**.
2. Scroll down to **IP Address**. Select **OK**.
3. Enter the values as follows:

Phone IP:	Enter the IP address to use for the handset.
TFTP Server IP:	Enter the IP address of the UC server which also hosts the TFTP server, holds software images for updating the handsets, and contains the handset files.
Default Gateway:	Enter the IP address of the default gateway on the network.
Subnet Mask:	Enter the subnet mask of the network.
SIP TFTP Server IP:	Enter the IP address of the UC server where the TFTP server is located.

NOTE: *The wireless telephones cannot roam across subnets, since they cannot change IP addresses while operational. Ensure that all APs are attached to the same subnet for proper operation. The handset can change subnets if DHCP is enabled and the handset is powered off then back on when within range of the APs on the new subnet.*

Setting the User Identity on the Handset

To permanently associate the identity with the handset, you will need to program the user ID and password on the handset. Otherwise, you will be prompted for the identity each time the handset is powered on. This identity must correspond to a configuration file created in *Creating the Configuration Files for Provisioning on page 3*. For example, if configuring the handset to use identity 3251, then a configuration file in the TFTP server with the name **sip_3251.cfg** must exist in order for the handset to successfully register with the UC server.

To set the user identity:

1. In the **Admin** menu, scroll down to **Phone Config**. Select **OK**.
2. Scroll down to **SIP Registration**. Select **OK**.
3. While **REG 1 AND LOGIN** is selected, select **OK**.
4. While **Username** is selected, select **OK**.
5. Enter the user name of the identity.
6. Select **OK** and then select **UP**.
7. Scroll down to **Password** and select **OK**.
8. Select **UP**.

Access Point Settings

1. In the **Admin** menu, scroll down to **Network Config**. Select **OK**.
2. Scroll down to **ESS ID**. Select **OK**.
3. Select the option that will enable the handset to acquire APs with the correct Extended Service Set ID (ESSID) each time it is turned on.
    - **Automatic Learn options**: **Broadcast ESSID** must be enabled in the APs for ESSID learning to function when multiple ESSIDs can be detected by the handset from one location. Overlapping wireless systems complicate the use of ESSID learning as the handset in an overlapping area could receive conflicting signals. If this is the situation at your site, use **Static Entry** or **Learn Once** in an area without overlapping ESSIDs.

        – **Learn Once** allows the handset to scan all ESSIDs for a DHCP server. Once an ESSID is located, the handset retains the ESSID from that AP. When overlapping wireless systems exist, the Learn Once feature allows the handset to use only the ESSID established at first learn at all subsequent startups of the phone. This ESSID is retained by the handset until the ESSID option is reselected in the **Admin** menu, thus erasing the stored ESSID.
        – **Learn Always** allows the handset to automatically learn the ESSID at each power on or loss of contact with the wireless LAN (out of range). This may be useful if the handset will be used at more than one site.
        – **Static Entry** allows the ESSID to be entered manually if the APs do not broadcast their ESSID, or if there are overlapping wireless systems in use at the site.
4. Select **OK**.
5. Select **UP**.
6. Scroll down to **Security**. Select **OK**.
7. Scroll down to the security type used on your access point. Select **OK**.

Testing the Configuration

To ensure that the handset is correctly configured, you must run the following tests.

1. **Call to voicemail:** Place a call to the voicemail access number and set the voicemail password for that user.
2. **Internal Call – hard phone/soft phone:** Place a call to a user with a hard phone or soft phone. Make sure there is two-way audio.
3. **Internal Call – handset to handset:** Place a call to another user with a SpectraLink handset. Make sure there is two-way audio.
4. **External Call to PSTN number:** Place a call to a PSTN number through a gateway. Make sure there is two-way audio.

Troubleshooting

Handset Messages

1. **ASSERT xxx c Line yyy.**
   This indicates that the handset has detected a fault from which it cannot recover.
   - Turn the handset off, then on again.
   - If the error still persists, contact Polycom Technical Support and report the error.
2. **Assoc Failed xxxxxxxxxxxx**
   Handset association was refused by the AP; displays medium access control (MAC) address of the failing AP.
   - Check handset and AP security settings.
   - Ensure the AP is configured correctly and WMM is enabled on the AP.
   - Try another AP.
3. **Auth Failed xxxxxxxxxxxx**
   Handset did not receive association response from the AP; displays the MAC address of the failing AP.
   - Check the handset and AP security settings.
   - Ensure the AP is configured correctly and WMM is enabled on the AP.
   - Try another AP.
4. **Auth Timeout xxxxxxxxxxxx**
   Handset did not receive association response from the AP; displays the MAC address of the failing AP.
   - Check the handset and AP security settings.
   - Ensure the AP is configured correctly and WMM is enabled on the AP.
   - Try another AP.

5. **Bad Config**
   A needed configuration parameter has not been set.
   - Check all required handset configuration parameters for valid settings.

6. **Bad ESSID**
   The handset is configured for **static ESSID** (as opposed to **Learn once** or **Learn always**), and no ESSID has been entered.
   - Enter an ESSID in the configuration settings or change to one of the Learn modes.

7. **Bad Network IP**
   The value of the network IP address entered in the handset through the menus or the configuration is missing or invalid.
   - Enter a valid network IP address.

8. **Bad Network Mask**
   The value of the network mask entered in the handset through the menus or the configuration is missing or invalid.
   - Enter a valid network mask.

9. **Battery Failure**
   The battery pack is not functioning.
   - Replace the battery pack with a new or confirmed SpectraLink battery pack. Only SpectraLink battery packs will work.

10. **Battery Failed**
    The battery pack is damaged or incompatible with handset.
    - Replace the battery pack with a new or confirmed SpectraLink battery pack. Only SpectraLink battery packs will work.

11. **Can't Renew DHCP yyy.yyy.yyy.yyy**
    DHCP server is not responding to initial renewal attempt.
    - This is a configuration problem. Check the IP address configuration in the DHCP server.

12. **DHCP Error (1-5)**
    - **DHCP Error 1:** The handset cannot locate a DHCP server. It will try every four seconds until a server is located.
    - **DHCP Error 2:** The handset has not received a response from the server for a request to an IP address. It will retry until a server is found.
    - **DHCP Error 3:** The server refuses to lease the handset an IP address. It will keep trying.
    - **DHCP Error 4:** The server offered the handset a lease that is too short. The minimum lease time is 10 minutes, but Polycom recommends a one hour minimum lease time. The handset will stop trying. Reconfigure the server and cycle the power on the handset.
    - **DHCP Error 5:** Failure during wired equivalent privacy (WEP) key rotation process.

13. **DHCP Lease Exp yyy.yyy.yyy.yyy**

    DHCP is not responding to renewal attempts.

    - The handset failed to renew its DHCP lease, either because the DHCP server is not running, or because the configuration has been changed by the administrator.
    - The handset will attempt to negotiate a new lease, which will either work, or it will change to one of the DHCP errors (1 through 4).

14. **DHCP NACK error yyy.yyy.yyy.yyy**

    DHCP server explicitly refused renewal.

    - The DHCP lease currently in use by the handset is no longer valid, which forces the handset to restart. This problem should resolve itself on the restart. If it does not, check the DHCP server.

15. **Duplicate IP**

    The handset has detected another device with the same IP address.

    - If using DHCP, ensure that the DHCP server is properly configured to avoid duplicate addresses. If using a static IP, be sure that the handset was assigned a unique address.

16. **Internal Err. # #**

    The handset has detected a fault from which it cannot recover.

    - Turn the handset off, then on again.
    - If the error persists, contact Polycom Technical Support and report the error.

17. **No DHCP Server**

    Handset is unable to contact the DHCP server.

    - Ensure that your DHCP server is operational and connected to the wireless local area network (WLAN) or use Static IP configuration in the handset.

18. **No ESSID**

    Attempted to run site survey application without an ESSID set.

    - Statically configure an ESSID in the **Admin** menu.

19. **No Host IP (Addr)**

    The handset is configured for **staticIP** (as opposed to **use DHCP**) and no valid host IP address (the handset's IP address) has been entered.

    - Enter a valid IP address in the configuration settings or change to **use DHCP**.

20. **No IP Address**

    The handset IP address is invalid.

    - Check the IP address of the handset and reconfigure if required, or change to **use DHCP**.

21. **No Net Access**

    Cannot communicate with LAN devices through the WLAN (such as PBX).

    - Verify the AP connectivity to the LAN.
    - Verify that all the WEP settings in the handset match those in the APs.

22. No Net Found or No APs

The handset cannot find any APs. This indicates any of the following:

No Radio Link

- Verify that the AP is turned on. Verify WMM is enabled on the AP. Enabling WMM is mandatory.

No ESSID: Auto-learn not supported (or) incorrect ESSID

- Verify the ESSID of the wireless LAN and reenter it, or, if necessary, initiate one of the automatic learning options to learn it again.

Access point does not support appropriate data rates

- Check the AP configuration.

Out of range

- Try getting closer to an AP. Check to see if other handsets are working within the same range of an AP. If so, check the ESSID of this handset.

Incorrect security settings

- Verify that all the security settings in the handset match those in the APs.

23. No Net Found xxxxxxxxxxxx yy

The handset cannot find a suitable AP. It displays the MAC address and signal strength of best non-suitable AP found.

- Check the AP and handset network settings such as ESSID, Security, Reg domain, and Tx power.
- Ensure the APs are configured correctly.
- Try site survey mode to determine a more specific cause.
- Enable WMM in the APs.

24. No PBX Response

The handset has exceeded its retransmission limit with no ACK response from proxy server.

- Verify that the proxy server IP address and port are properly configured.

25. No SIP DHCP

DHCP is configured but no valid SIP option 43 was found.

- Check the DHCP server configuration for option 43 and reconfigure if required.

26. Press End Call

The far end of a call has hung up.

- Hang up the near end by pressing the END key.

27. Select License

A protocol has not been selected from the license option setting.

- Using the **Admin** menu, select a license option to allow the phone to download the appropriate software.

28. **Server Busy**
    The handset is attempting to download from a TFTP server that is busy and refusing additional downloads.
    - The handset will automatically retry the download every few seconds.

29. **Too Many Errors**
    The handset continues to reset and cannot be recovered.
    - This is a fatal error. Return the handset to Polycom.

30. **Flash Config Error**
    The handset internal configuration is corrupt.
    - Perform Restore Defaults operation via administrator menus.

Download Failures

If you receive the following error: **TFTP ERROR(x):yy**, a failure has occurred during the TFTP download of one of the files. **(x)** is the file number that was being downloaded; **yy** is an error code describing the particular failure. Possible error codes include:

- **01 = TFTP server did not find the requested file.**
  Make sure the relevant configuration files are in the UC server TFTP folder located in *X*:\program files\ ADTRAN\NetVanta UC Server\Data\TFTP, where *X* is the drive where the UC server is installed.
- **16 = No TFTP server address.**
  Check the TFTP server IP configuration in the handset (if static IP address is set) or in the DHCP server.
- **81 = File put into memory did not pass CRC. The handset will attempt to download the file again.**
  Wait for the handset to try again. If the message appears again, the firmware file may be corrupt. Extract the firmware from the zipped archive and try again.
- **FF = Timeout error. TFTP server did not respond within a specified period of time.**
  The handset is unable to communicate with the TFTP server. Restart the handset and try again.