Teo Technologies, Inc.
11609 49th Place West
Mukilteo, WA 98275-4255
(800) 524-0024 (425) 349-1000
Fax (425) 349-1010
www.teotech.com

IP Telephone

Network Administration Guide

Software Version xx.04.38, Document #13-280132 Rev. U
September 2021

Contents

Introduction

This manual is intended for use by network administrators.

This Network Administrator's Guide explains network administration and network-based phone configuration for Teo 7810, 7810 TSG series, 4104, and 4101 IP telephones. Troubleshooting procedures are also included in this guide.

Document Overview

Network Setup – setting up the various servers required for a SIP IP system.

Configuring Telephones – configuring telephones via server-based XML files.

XML Configuration Files – XML configuration file structure.

XML Tag Tables – detailed configuration options for each XML parameter.

Security Guidelines – considerations for configuring and deploying telephones in a secure environment.

Telephone Software Updates – updating telephone operating software from a Teo UC, TFTP, HTTP, or HTTPS server.

Appendix A – viewing packet statistics logs in the telephone.

Appendix B – Dial Plan syntax.

Appendix C – network and telephone troubleshooting.

Appendix D – alphabetical index of all XML Tags.

Network Setup

NOTE: When setting up servers and telephones, server names can be entered in place of IP addresses.

LLDP Media Endpoint Discovery (LLDP-MED)

Link Layer Discovery Protocol (LLDP) may be used as a component in network management and network monitoring applications. LLDP Media Endpoint Discovery (LLDP-MED) is an enhancement of LLDP and can be enabled by means of an XML configuration tag or an LCD menu at the phone. LLDP-MED can be used to auto-discover a VLAN, layer 2 priorities, DSCP priorities and PIDF-LO settings as described in subsequent sections.

VLAN Discovery Mode

VLAN Discovery Mode controls how the phone determines the VLAN ID, layer 2 voice priority, layer 2 signal priority, and may also include DSCP voice/signal priority. VLAN Discovery Mode can be set by means of an XML configuration tag or an LCD menu at the phone. VLAN Discovery Mode can be set to one of the following:

- LLDPMED: VLAN is set by means of LLDP-MED (default).
- DHCP: VLAN is set by means of DHCP.
- STATIC: VLAN is set by means of XML configuration tags or the LCD menu at the phone.
- OFF: VLAN operation is disabled.

The phone's current/active VLAN settings can be viewed in LCD menus at the phone.

802.1x Port-based Network Access Control

802.1x Supplicant Enable/Disable

802.1x is a network authentication protocol that opens ports for network access when an organization authenticates a user's identity and authorizes them for access to the network. The user's identity is determined based on their credentials or certificate, which is relayed via a supported network switch for authentication by the RADIUS server. A RADIUS server is required to utilize this phone feature. The RADIUS server is a site responsibility and its configuration is out of the scope of this document so is not described here. The phone's 802.1x supplicant application can be enabled by means of an XML configuration tag or an LCD menu at the phone.

802.1x Extensible Authentication Protocol (EAP) Method

The 802.1x EAP method is the standard authentication protocol by which identifying information is securely sent over the network. The 802.1x EAP method that is used by the phone supplicant can be set by means of an XML configuration tag or an LCD menu at the phone. The 802.1x EAP method can be set to one of the following:

- PEAPv0/MSCHAPv2 (default)
- PEAPv0/GTC

- TTLS/MSCHAPv2
- TTLS/GTC
- FAST
- TLS

802.1x Username

The 802.1x Username that is used by the phone supplicant can be set by means of an XML configuration tag or an LCD menu at the phone. Also, during initialization, if the 802.1x phone supplicant is enabled and the 802.1x Username is NULL, then the user is prompted to enter a username and password.

802.1x Password

The 802.1x Password that is used by the phone supplicant can be set by means of an XML configuration tag or an LCD menu at the phone or is prompted of the user during initialization (see previous paragraph).

PIDF-LO Discovery Mode

PIDF-LO Discovery Mode controls how the phone sets its Presence Information Data Format Location Object (PIDF-LO). PIDF-LO Discovery Mode can be set by means of an XML configuration tag or an LCD menu at the phone. PIDF-LO Discovery Mode can be set to one of the following:

- LLDP-MED: PIDF-LO is set by means of LLDP-MED.
- DHCP: PIDF-LO is set by means of DHCP.
- STATIC: PIDF-LO is set by means of XML configuration tags.
- OFF: PIDF-LO is disabled (default). E911 calls will not include PIDF-LO information.

DHCP Server

Automatic IP Configuration (DHCP)

DHCP (Dynamic Host Configuration Protocol) assigns IP addresses to telephones, and can provide other information to the phones, such as server addresses. When using DHCP, phones do not need to be configured with static IP addresses.

The DHCP server can supply:

- Phone IP Address
- Phone Subnet Mask
- Domain Name
- Default Gateway IP Address (Router)
- DNS Server(s) IP Address
- NTP Server(s) IP Address (Time Server)
- Update Server IP Address (Boot Server Host Name) and protocol
- SIP Proxy IP Address
- VLAN Configuration

Settings not supplied by DHCP must be entered locally at the phone, or in a configuration file which is supplied to the phone via an update server.

Configuring the DHCP Server

The DHCP server requires a scope of IP addresses that can be assigned to the phones. The scope must be configured with the router address, vendor-specific info, and the update server address.

You can use an existing DHCP server for assigning IP addresses to the telephones, or add a new server.

Scope

Select the DHCP server that you will use for assigning IP addresses to telephones.

Add a new scope, and then enter the following:

- A name and description for the scope.
- The start and end of the IP address range that can be assigned to telephones. Do not include telephones and computers in the same address range.
- Any IP addresses that will be excluded from the address range.
- The lease duration for telephone IP addresses. A lease duration of seven days or longer is recommended.

  When the lease expires the phone shows a diagnostic display if idle, while attempting to negotiate a new IP address lease at preset intervals. If the phone is active, the call will be unaffected and the diagnostic display will be shown when the call is cleared.

  If the same IP address is offered by the DHCP server, the phone returns to operation without restarting, otherwise the phone will restart after receiving a new IP address.
- The router or default gateway IP address or server name.
- (Optional) parent domain name, DNS servers, WINS servers.

Activate the scope.

Scope Options

Set these scope options:

2 Time Offset

If your network time server is set to UTC time, enter the hex value for your location's offset from UTC time in seconds.

If your network time server is set to local time, enter **0**.

DHCP Option 002	
Time Zone	**Offset**
Pacific Standard Time	0xffff8f80
Pacific Daylight Time	0xffff9d90
Mountain Standard Time	0xffff9d90
Mountain Daylight Time	0xffffaba0
Central Standard Time	0xffffaba0
Central Daylight Time	0xffffb9b0
Eastern Standard Time	0xffffb9b0
Eastern Daylight Time	0xffffc7c0

3 Router

Enter the router IP address, or enter the server name and click Resolve to look up the proper IP address.

4 Time Server

Enter the time server IP address, or enter the server name and click Resolve to look up the proper IP address. You can enter multiple time servers and order them by preference.

66 Boot Server Protocol/Host Name/Port

Enter the update server protocol, IP address or fully qualified domain name <server>, and the port number <port> as a string value. This value determines server protocol, address, and port used for configuration file downloads as shown in the table below.

The server's fully qualified domain name can include the path to a subdirectory of the server root, such as "http://myserver/teoupdates/7810".

Alternatively, you can use the **UpdateSrvr** parameter in vendor-specific DHCP Option 125 to configure this parameter. In addition, Option 125 allows you to set VLAN and other parameters that may be sufficient to configure phones without an update server.

NOTE: To avoid conflicts, do not set update server parameters in both Option 66 and Option125.

DHCP Option 66		
Option 66 Value	**Protocol Set in the Phone**	**File Transfer Protocol**
teo://<server>	Don't Care	Teo protocol to <server>
https://<server>	Don't Care	HTTPS to <server>:443 (standard port)
https://<server>:<port>	Don't Care	HTTPS to <server>:<port>
http://<server>	Don't Care	HTTP to <server>:80 (standard port)
http://<server>:<port>	Don't Care	HTTP to <server>:<port>
tftp://<server>	Don't Care	TFTP to <server>:69 (standard port)
tftp://<server>:<port>	Don't Care	TFTP to <server>:<port>
<server>	TEO	Teo protocol to <server>
<server>	HTTPS	HTTPS to <server>:443 (standard port)
<server>:<port>	HTTPS	HTTPS to <server>:<port>
<server>:9443	Don't Care	HTTPS to <server>:9443
<server>	HTTP	HTTP to <server>:80 (standard port)
<server>:<port>	HTTP	HTTP to <server>:<port>
<server>:9080	Don't Care	HTTP to <server>:9080
<server>	TFTP	TFTP to <server>:69 (standard port)
<server>:<port>	TFTP	TFTP to <server>:<port>
<server>:9669	Don't Care	TFTP to <server>:9669

120 SIP Server DHCP Option

Enter either an IPv4 address or, **preferably**, a DNS fully-qualified domain name as a string value to be used by the SIP client to locate a SIP proxy server.

Alternatively, you can use the **SipProxyServer** parameter in vendor-specific DHCP Option 125 to configure this parameter. In addition, Option 125 allows you to set VLAN and other parameters that may be sufficient to configure phones without an update server.

NOTE: To avoid conflicts, do not set SIP server address in both Option 120 and Option125.

125 Vendor-Identifying Vendor-Specific

Entries in option 125 can be used to simplify phone configuration. Set up this option to configure VLAN, updates, SIP proxy server, and SIP registrar. Option 125 can contain data for multiple vendors; each vendor's data is identified by their PEN ID and the length of the data.

NOTE: Option 125 requires the Data Type "Encapsulated" and does not allow cut/paste in the Data entry window if using Windows DHCP Server.

1. Create option 125 (Windows Server example):
   a. From the DHCP Tree window, right click on the DHCP server IPv4 scope you wish to configure with Option 125.
   b. Select "Set Predefined Options..."
   c. Set the "Option Class" to "DHCP Standard Options
   d. Click the Add button located under the Option Name. Enter **`Vendor Specific Teo Option`** in the Name field, select "Encapsulated" as the Data Type, enter **`125`** as the Code, and enter **`Option 125 for Teo`** in the Description field.
   e. When completed click OK to add Option 125 to the available Scope Options.
2. In the DHCP Tree window, select the desired scope to contain the new 125 option, once the proper scope is selected, right-click in the Scope Options pane and select "Configure Options". Scroll through the available options and select "125 Teo Private Vendor Specific Option".

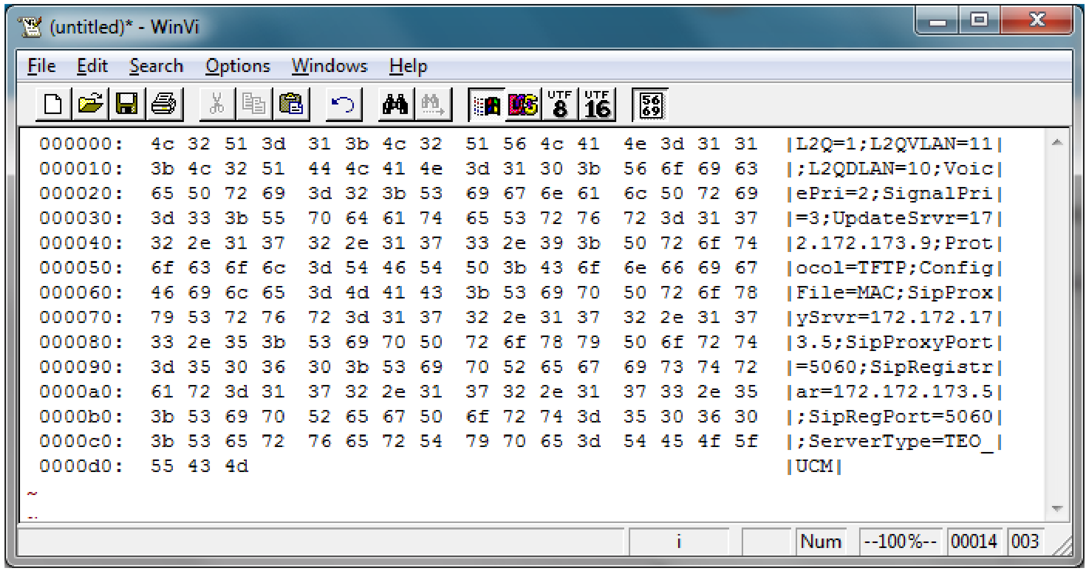
   Determine the parameters required by your system configuration; refer to the table on page 15 for available parameters. The format is *parameter, equal sign, value*, with parameter/value pairs separated by semicolons (no spaces) as in the following example.

   ```
   L2Q=1;L2QVLAN=11;VoicePri=2;SignalPri=3;UpdateSrvr=172.172.173.9;
   Protocol=TFTP;ConfigFile=MAC;SipProxySrvr=172.172.173.5;
   SipProxyPort=5060;SipRegistrar=172.172.173.5;SipRegPort=5060;
   ServerType=TEO_UCM
   ```

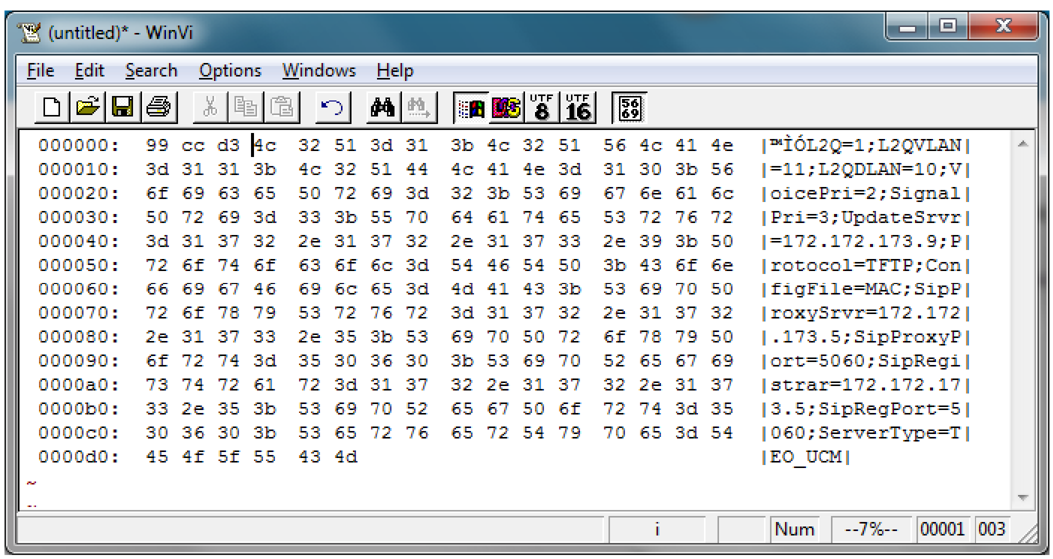
   a. You may wish to use the free WinVi, available from the following url: http://www.winvi.de/en/download.html

      And additionally, an online ASCII to Hex Converter: http://www.dolcevie.com/js/converter.html

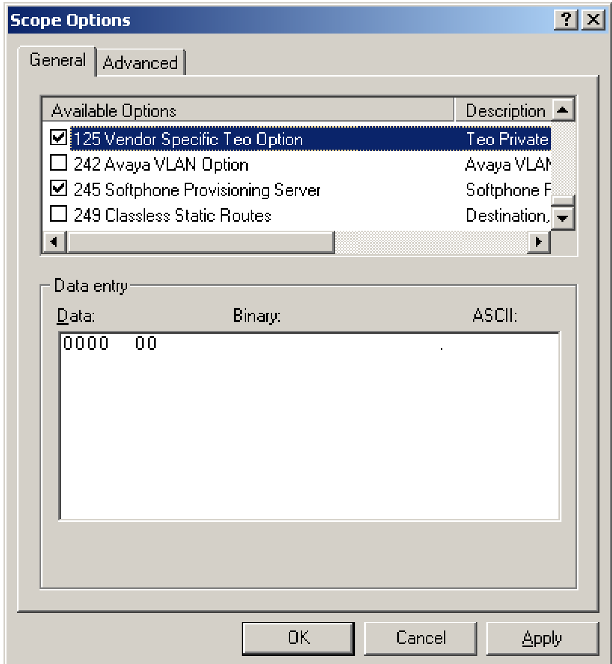
Open WinVi and select Hexadecimal mode from the toolbar. Paste the parameter data string into the WinVi window, assuring there are no additional leading or trailing spaces/characters. WinVi will then display the hex equivalent. Determine the byte length using the line count in the column on the left side of the window. For example, in this case as illustrated below:
([16*13] + 3 = 211 decimal) or D3 hex.



Prepend the converted Teo PEN ID **99CC** and the converted length **D3** in the Hex window, resulting in the following:



Then, if the entry is short, manually enter the hex values in the DHCP Option 125 window (overwrite the existing `00` values):



b. If you prefer, use the netsh command:

`C:\Users\Administrator.PROSERV>netsh`
`netsh>dhcp`
`netsh dhcp>server`
`netsh dhcp server>scope 172.172.173.0` *(example scope)*

Enter the hex data as in the following example.

NOTE: If the data was converted from ASCII, be sure to remove all spaces, colons, returns and line feeds. Data must be contiguous.

```
netsh dhcp server scope>set optionvalue 125 ENCAPSULATED
99ccca4c3251564c414e3d31313b4c3251444c414e3d31303b566f6963655
072693d323b5369676e616c5072693d333b55706461746553727276723d3130
2e31302e38382e353b50726f746f636f6c3d20544654503b436f6e6669674
6696c653d4d41433b53697050726f7879537276723d31302e31302e38382e
373b53697050726f7879506f72743d353036303b53697052656769737472 6
1723d31302e31302e38382e373b5369705265567506f72743d353036303b53
6572766572547970653d54454f5f55434d
```

DHCP Option 125	
Parameter	**Data / Description**
UpdateSrvr	Update server protocol, IP address or fully qualified domain name, and port number. This configures the same parameter as XML tag <update_server>. Refer to the DHCP Option 66 table *(page 10)* for allowed values. *NOTE: To avoid conflicts, do not enter update server parameters in DHCP Option 66 if it is set here.*
ConfigFile	The naming scheme for custom XML configuration files (not used with the Teo protocol). This configures the same parameter as XML tag <config_file_name_base>. **MAC** – Ethernet MAC address *(default)* **LINE** – phone line ID
L2Q	Enables VLAN / Ethernet Layer 2 802.1Q support. This configures the same parameter as XML tags <vlan><enable>. **1** – VLAN enabled **0** – VLAN disabled *(default)* *NOTE: To avoid conflicts, do not enter VLAN data in DHCP Option 242 if it is set here.*
L2QVLAN	Phone VLAN ID. A value of **0** (zero) indicates that the phone does not belong to any VLAN; in this case, the 802.1Q tag specifies only a priority and is referred to as a *priority tag*. This configures the same parameter as XML tags <vlan><id>. **0, 2 – 4094,** *default value = 1111* *NOTE: To avoid conflicts, do not enter VLAN data in DHCP Option 242 if it is set here.*
VoicePri	802.1Q Voice Priority Code Point. This configures the same parameter as XML tags <vlan><voice_pri>. **0 – 7,** *default value = 6*
SignalPri	802.1Q Signaling Priority Code Point. This configures the same parameter as XML tags <vlan><signal_pri>. **0 – 7,** *default value = 6*
SipProxyServer	IP address or fully qualified domain name name of the SIP Proxy Server (SIP Server). This configures the same parameter as XML tag <sip_proxy_addr>. Valid IP address in IPv4 or IPv6 format. *NOTE: To avoid conflicts, do not enter SIP server address in DHCP Option 120 if it is set here.*

DHCP Option 125	
Parameter	**Data / Description**
SipProxyPort	Port number used by the phone to send SIP signaling messages to the SIP Proxy Server. The form is *xxxxx* with leading zeros suppressed. This configures the same parameter as XML tag <sip_proxy_port>. **1025** - **65534,** *default value = 5060*
SipRegistrar	IP address or domain name of the SIP Registrar (most server implementations combine this into a single SIP server application). This configures the same parameter as XML tag <sip_registrar>. If left blank or omitted, <SipProxyServer> will be used. This value is used inside SIP message headers, in the form <line_id>@<SipRegistrar>:<SipRegPort>, to reference the SIP server (e.g. 1000@teo:5060 or 1000@192.168.72.5:5060).
SipRegPort	Port number for the SIP Registrar. This configures the same parameter as XML tag <sip_reg_port>, in the form *xxxxx* with leading zeros suppressed. **1025** - **65534,** *default value = 5060* This value is used inside SIP message headers, in the form <line_id>@<SipRegistrar>:<SipRegPort>, to reference the SIP server.

242 VLAN Configuration

Option 242 may be required by other vendors for configuring the Phone VLAN.

NOTE: To avoid conflicts, do not set VLAN parameters in both Option 242 and Option 125.

If Option 242 is not predefined and available, use the process described under Option 125 above to create it (Windows Server example).

1. From the DHCP Tree window, right click on the DHCP server, IPv4 scope you wish to configure with Option 242.
2. Select "Set Predefined Options..."
3. Set the Option Class to "DHCP Standard Options".
4. Click the Add button located under the Option Name. Enter **`Teo VLAN Option`** in the Name field, select "String" as the Data Type, enter **`242`** as the Code, and enter **`Teo VLAN Activation Control`** in the Description field. When completed click OK.
5. In the Data entry field: enter **`L2Q=1,L2QVLAN=xx`**, where *xx* is the Phone VLAN ID; refer to the DHCP Option 125 table *(page 15)*.

SIP Registrar Server

If no IP address or domain name is specified for the SIP Registrar Server in the telephone's configuration file, the SIP Proxy Server will be used as the SIP Registrar Server address.

This address can also be manually changed at the telephone.

Syslog Server

The Syslog Server records error messages.

The IP address or server name of the Syslog Server can be specified in the telephone's configuration file, or manually entered at the telephone.

Configuring Telephones

Telephone Setup Menus

Most telephone settings can be entered locally through the Installation Options Menu. For descriptions of each setting, as well as instructions for changing or removing PINs, refer to the telephone's Installation Instructions.

Using the Setup Menus

You can enter the Installation Options menu when the phone is idle.

Press the ***SETUP*** key *(7810 series)* or the **MENU** key *(4104, 4101)*.

```
    SETUP MENU
INSTL ADMIN USER
```

Select INSTL *(7810 series, 4104)* or INSTALL *(4101)*.

Entry into the Installation Options menu may be protected by a PIN (Personal Identification Number). Enter your PIN with the dial pad, and then press the ***OK*** key.

```
ENTER PIN:********
£BKSP CLEAR
```

```
INSTALLATION OPTIONS  ¤
 IP  SIP  NET  KEYS
```

When ◀ or ▶ appears in the upper line of the display, you can press the Left or Right Arrow key to see additional menu selections *(7810 series, 4104).*

```
INSTALLATION OPTIONS £¤
 CALL  PIN  RESET UPDATE
```

```
INSTALLATION OPTIONS  £
PCPORT SECRTY LOG
```

XML Configuration Files

XML configuration files can be used to configure telephones from an update server.

Details are in the following chapter.

XML Configuration Files

All telephone configuration options, including many not available locally from the menus, can be specified in XML configuration files. Settings in these files are loaded into the telephone from an update server.

A **global configuration file**, named “TCS7000A.xml”, is loaded first. Settings in this file overwrite any existing local settings. The global file is optional, and only one global file can exist on the update server.

Custom configuration files are unique to each telephone, identified by the primary line ID or the MAC address, if specified in the global configuration file. If not specified, the MAC address is the default setting. Settings in this file overwrite any existing local settings, and any settings loaded from the global file.

All settings are optional. Unused settings may be commented out or not included in the files.

Configuration files can contain sections for specific telephone models. In the sample file on page 24, the first section is loaded into 7810/7810-TSG with or without an 8030X Button Expansion Module. The next section applies only to phones without an 8030X, and the last section applies only to phones with an 8030X.

Editing XML Files

Files can be edited with a dedicated XML editor or any text editor. Although you can manually create the entire file, it is highly recommended that you copy one of the sample files provided by Teo, and edit the copy.

File contents are made up of XML tags, elements and attributes. All tags are optional.

Do not include leading '0' characters in IP addresses.

> Refer to the sample configuration file on page 24. Circled numbers identify the various sections. Blank lines between sections are shown for visual clarity, and are not required.

File Names and Location

Configuration files must be located in the update server root directory, or in a subdirectory of the server root, specified in DHCP Option 66 or Option 125 *(page 10)*.

Name each custom configuration file with the associated Ethernet MAC address *(default)* or the phone’s line ID, and include an ‘.xml’ extension; for example, **00048D0000F5.xml** or **4255663001.xml**.

Note: All configuration files must use the same naming scheme and all capital letters must be used for the name of the MAC.xml file.

To use a line ID naming scheme, add the following line in the global configuration file "TCS7000A.xml", enclosed within the model tag *(page 22)*.

```
<config_file_name_base>LINE</config_file_name_base>
```

XML Declaration ①

The first line in the file defines the XML version and encoding. It is used by XML viewers and editors to control formatting. This line must be entered exactly as shown:

```
<?xml version="1.0" encoding="UTF-8"?>
```

Comments ②

Comments can appear anywhere after the first line, and must be enclosed by `<!--` and `-->`. Comments can be included on lines with XML tags or data, and can span multiple lines. *Do not embed a partial comment within another comment. Include* `<!--` *opening and* `-->` *closing tags for all comments.*

```
<!-- This is a comment. -->
```

If you do not wish to assign a particular parameter, comment out the line or delete the entry.

```
<!-- These six lines have been commented out.
     <key num="4">SD
          <speeddial>12345678900#</speeddial>
          <label>SPDIAL 456-8900</label>
     </key>
-->
```

Root Element ③

All settings are enclosed within a single root element. The schema version is used for telephone compatibility management.

```
<TEO_settings schema_vers="2.0">
             :
             :
</TEO_settings>
```

Telephone Models ④

The model tags enclose all settings for a telephone model or group of models. A configuration can contain multiple model tags.

In the example below, the settings in the first model element apply to 7810 models, with or without an 8030X Button Expansion Module. The second model element contains settings that only apply to 7810-TSG models without an 8030X.

```
<TEO_phone model="7810,7810 + 8030X">
             :
             :
</TEO_phone>

<TEO_phone model="7810-TSG">
             :
             :
</TEO_phone>
```

Allowed TEO_phone model values are:

7810	(7810)
7810 + 8030X	(7810 + 8030X Button Expansion Module)
7810-TSG	(7810-TSG)
7810-TSG + 8030X	(7810-TSG + 8030X Button Expansion Module)
7810PoE-TSGA	(7810PoE-TSGA)
7810PoE-TSGA + 8030X	(7810PoE-TSGA + 8030X Button Expansion Module)
7810PoE-TSGB	(7810PoE-TSGB)
7810PoE-TSGB + 8030X	(7810PoE-TSGB + 8030X Button Expansion Module)
4104	(4104)
4101	(4101)
ALL	(settings apply to all models)

Other Settings

Other configuration settings are enclosed within the tags listed in the tables beginning on page 27.

Sample XML Configuration File

```
①  <?xml version="1.0" encoding="UTF-8"?>

②  <!— Configuration file for Alexander Great (425) 566-3001 -->

③  <TEO_settings schema_vers="2.0">

      <TEO_phone model="7810,7810 + 8030X">
           <sip_proxy_addr source="DHCP4">
                mantaray.undersea.com
           </sip_proxy_addr>
           <sip_proxy_port>5060</sip_proxy_port>
           <sip_registrar>mantaray.undersea.com</sip_registrar>
           <sip_reg_port>5060</sip_reg_port>

           <feature_activator_list>
                <fa index="1">
                     <fa_type>LOCAL CFWD</fa_type>
                </fa>
                <fa index="2">
                     <fa_type>LOCAL DND</fa_type>
                </fa>
           </feature_activator_list>

④          <multi_function_key_list>
                <key num="1" to_num="3">LINE
                     <line_id>8005551212</line_id>
                     <label>Doctor John</label>
                     <sip_name>John Johnson</sip_name>
                     <sip_auth_id>IMAuthorized</sip_auth_id>
                     <sip_password>PassWord</sip_password>
                </key>
                <key num="4">SD
                     <speeddial>4255551234#</speeddial>
                     <label>SPDIAL 555-1234</label>
                </key>
                <key num="5">SD
                     <speeddial>4255554321#</speeddial>
                     <label>SPDIAL 555-4321</label>
                </key>
           </multi_function_key_list>
      </TEO_phone>

      <TEO_phone model="7810">
           <multi_function_key_list>
                <key num="9">FA
                     <fa_index>1</fa_index>
④               </key>
                <key num="10">FA
                     <fa_index>2</fa_index>
                </key>
           </multi_function_key_list>
      </TEO_phone>
```

```
④   <TEO_phone model="7810 + 8030X">
         <multi_function_key_list>
              <key num="29">FA
                   <fa_index>1</fa_index>
              </key>
              <key num="30">FA
                   <fa_index>2</fa_index>
              </key>
         </multi_function_key_list>

         <directory_list clear_list="YES">
              <directory entry="1">
                   <dir_name>Ron B</dir_name>
                   <dir_number>4255556789</dir_number>
              </directory>
              <directory entry="2">
                   <dir_name>Ella H</dir_name>
                   <dir_number>4255556263</dir_number>
              </directory>
         </directory_list>
    </TEO_phone>

③ </TEO_settings>
```

XML Tag Tables

All valid XML tags are listed in the tables below, grouped as follows:

- Update Settings
- Network Settings
- Security Settings
- SIP Settings
- General Phone Settings
- Dial Plan Settings
- MLPP Settings
- Conference, Call Forward, and Voicemail Keys
- Feature Activator Functions
- Multifunction Keys
    - Line Keys
    - Feature Activator Keys
    - DSS Keys
    - ACD Keys
    - Speed Dial Keys
- Call Directory Entries

An alphabetical index of all XML tags is on page 90.

Update Settings

These settings control automatic updating of telephone software and configuration settings from a TFTP, HTTP, HTTPS, or Teo UC server.

<table>
<tr><th colspan="2">Update Settings</th></tr>
<tr><th>XML Tag</th><th>Data / Description</th></tr>
<tr><td><update>
<update_server source="<i>src</i>">
<i>address</i>
</update_server>
<protocol>
<i>type</i>
</protocol>
<https_username>
<i>username</i>
</ https_username >
< https_password >
<i>password</i>
</ https_ password >
<program_auto>
<i>enable</i>
</program_auto>
<program_time>
<i>start hour</i>
</program_time>
<program_window>
<i>hours</i>
</program_window>
<config_auto>
<i>ON/OFF</i>
</config_auto>
<config_time>
<i>start hour</i>
</config_time>
<config_window>
<i>hours</i>
</config_window>
</update></td><td>Update server settings.
<u>update_server</u>: IP address or server name of the Update Server. May be provided by DHCP or statically assigned.
<i>src</i> is source of the IP address:
DHCP4 – use address provided by DHCPv4 Option 66, or Option 125 UpdateSrvr parameter, if available <i>(default)</i>
STATIC – always use default <i>address or name</i>
<i>address or name</i> is the default address in IPv4 or IPv6 format or DNS fully-qualified domain name.
If TFTP, HTTP or HTTPS protocol is used, a path can be appended to the server name. This path is where the digitally signed files are located under the update server root directory.
<u>protocol</u>: <i>type</i> is the protocol type for the download.
Options for type are:
TEO
TFTP
HTTP
HTTPS
NONE
<i>If <update_server source=DHCP4>, the type may be provided by DHCPv4 Option 66 or 125.</i>
<i>username</i> is the HTTPS username when protocol type is HTTPS.
<i>password</i> is the HTTPS password when protocol type is HTTPS.
<u>program_auto</u>: Enable/disable automatic program updates (not used with TEO protocol).
ON
OFF <i>(default)</i></td></tr>
</table>

Update Settings	
XML Tag	**Data / Description**
*(**update** continued)*	program_time: Program update start hour. Program automatic update process begins at a pseudo-random interval after this time each day. **0** - **23**, *default value = 1* program_window: Program update window hours. Program update time for each phone is calculated from program_window, program_time, and the phone's MAC address: Update Time = program_time + ((MAC Address [23:0]) MOD (program_window * 60)) This provides system-wide pseudo-randomly distributed start times at one-minute intervals between program_time (start time) and program_time + program_window (window hours later). Recommended Program window duration is one hour per 60 phones on a single Program server. **1** - **24**, *default value = 3* config_auto: Enable/disable automatic configuration updates (not used with TEO protocol). **ON** **OFF** *(default)* config_time: Configuration update start hour. Configuration automatic update process begins at a pseudo-random interval after this time each day. **0** - **23**, *default value = 1* config_window: configuration update window hours. Configuration update time for each phone is calculated from config_window, config_time, and the phone's MAC address: Update Time = config_time + ((MAC Address [23:0]) MOD (config_window * 60)) This provides system-wide pseudo-randomly distributed start times at one-minute intervals between config_time (start time) and config_time + config_window (window hours later). Recommended configuration window duration is one hour per 60 phones on a single update server. **1** - **24**, *default value = 3*

Update Settings	
XML Tag	**Data / Description**
<**config_file_name_base**> *name base* </**config_file_name_base**>	The naming scheme for custom XML configuration files, either Ethernet MAC address or phone line ID; not used with Teo protocol. Enter this tag in the "TCS7000A.xml" global configuration file or in DHCP Option 125 ConfigFile parameter. **MAC** *(default)* **LINE**

Network Settings

Network Settings	
XML Tag	**Data / Description**
<**ip_dhcp4_enable**> *mode* </**ip_dhcp4_enable**>	Allows the DHCPv4 Server to supply network settings. **ON** *(default)* **OFF** **IPv4_DISABLE –** turns off DHCPv4 and sets the IPv4 address to 0.0.0.0. This setting allows the phone to operate in IPv6-only mode.
<**ip4_phone**> *address* </**ip4_phone**>	IPv4 Address of the Phone *address* is the default phone address in IPv4 format. Note: If <ip_dhcp4_enable> is ON, phone IP address will be configured by DHCPv4; do not set this parameter in the XML file.
<**phone_subnet**> *subnet mask* </**phone_subnet**>	IPv4 subnet mask of the phone. Valid IP address in *xxx.xxx.xxx.xxx* format, omit leading zeroes **(***default value = 255.255.255.0).* Note: If <ip_dhcp4_enable> is ON, subnet mask will be configured by DHCPv4 Option 1; do not set this parameter in the XML file.
<**ip4_gateway_svr**> *address* </**ip4_gateway_svr**>	IPv4 address for the Gateway (router). *address* is the default gateway address in IPv4 format. Note: If <ip_dhcp4_enable> is ON, gateway IP address will be configured by DHCPv4 Option 3; do not set this parameter in the XML file.
<**ip6_phone_config**> *option* </**ip6_phone_config**>	Sets the phone’s IPv6 configuration. **OFF** – Disables the phone’s use of IPv6 addresses. (i.e. IPv4 only) *(default)* **STATIC** – Enables the phone’s use of IPv6 addresses. Global IPv6 addresses are statically (manually) assigned. **AUTO6** – Enables the phone’s use of IPv6 addresses. Global IPv6 addresses are assigned by stateless address autoconfiguration. **DHCP6** – Enables the phone's use of IPv6 addresses. Global IPv6 addresses are assigned by a DHCPv6 server.
<**ip6_router**> *domain name* </**ip6_router**>	IPv6 address for the router that the phone is to use to access external networks when in the STATIC IPv6 mode. Valid IP address in IPv6 format.

Network Settings	
XML Tag	**Data / Description**
<**ip6_phone_global**> **index=**"*index*"> *address* </**ip6_phone_global**>	One of five IPv6 Global Addresses for the phone. *index* is the global address is being set: **G1**, **G2**, **G3**, **G4** or **G5.**
<**network_dad**> *ON/OFF* </**network_dad**>	IPv6 Duplicate Address Detection. In autoconfiguration environments, duplicate addresses can be detected and managed. **ON** *(default)* **OFF**
<**network_echo_reply**> *ON/OFF* </**network_echo_reply**>	Enables the ability to send an Echo Reply message in response to an Echo Request message sent to an IPv6 multicast or anycast address. **ON** *(default)* **OFF**
<**network_ignore_redirects**> *ON/OFF* </**network_ignore_redirects**>	Disables the sending of IPv4 or IPv6 Internet Control Message Protocol (ICMP) redirect messages. **ON** *(default)* **OFF**
<**ip_pri_dns source**="*src*"> *address* </**ip_pri_dns_svr**>	IP Address of the Primary DNS Server. May be provided by DHCP or statically assigned. *src* is source of the IP address: **DHCP4** – use address provided by DHCPv4 Option 6, if available *(default)* **STATIC** – always use default *address* *address* is the default address in IPv4 or IPv6 format.
<**ip_sec_dns**> *address* </**ip_sec_dns**>	IP Address of the Secondary DNS Server. *address* is the default address in IPv4 or IPv6 format. *If <ip_pri_dns_svr source=DHCP4>, the address will be configured by DHCPv4 Option 6, if available.*
<**phone_domain**> *domain name* </**phone_domain**>	The domain name for the enterprise. For example, the "teotech.com" portion of the SIP URI user@teotech.com. Maximum length is 128 ASCII characters. The default is a NULL string. *If <ip_dhcp4_enable> is ON, phone_domain will be configured by DHCPv4 Option 15, if available.*
<**lldpmed_enable**> *ON/OFF* </**lldpmed _enable**>	Allows the user to enable or disable LLDP-MED. **ON** – LLDP-MED is enabled. *(default)* **OFF** – LLDP-MED is disabled.
<**vlan_discovery_mode**> *mode*	The phone's VLAN Discovery Mode.

Network Settings	
XML Tag	**Data / Description**
</**vlan_discovery_mode**>	**LLDPMED** *(default)* **DHCP** **STATIC** **OFF**
<**_8021x_enable**> *ON/OFF* </**_8021x _enable**>	Allows the user to enable or disable 8021.x supplicant. **Note:** The switchport to which the phone is connected must be configured for 802.1x authentication when this value is set to ON. The switchport to which the phone is connected must be configured for multi-domain authentication if the PC port is enabled, otherwise single-host mode is permissible. Switches will use either the LLDP-MED capabilities list from the phone or the response from the RADIUS authentication server to place the phone into the appropriate VOICE domain. For Cisco switches, if the phone is not recognized via LLDP-MED, a Cisco AV pair of “device-traffic-class=voice” can be used to place the phone into the appropriate domain class. **ON** – 802.1x supplicant is enabled. **OFF** – 802.1x supplicant is disabled. *(default)*
<**_8021x_eap_method**> method </**_8021x_eap_method**>	The phone’s EAP Method. **PEAPv0_MSCHAPv2** *(default)* **PEAPv0_GTC** **TTLS_MSCHAPv2** **TTLS_GTC** **FAST** **TLS**
<**_8021x_username**> *username* </**_8021x_username**>	The username used by the phone’s 802.1x supplicant for network access authentication.
<**_8021x_password**> password </**_8021x_password**>	The password used by the phone’s 802.1x supplicant for network access authentication.
<**time_server source**="*src*"> *address or name* </**time_server**>	IP Address of the Primary NTP Time Server. May be provided by DHCP or statically assigned. *src* is source of the IP address: **DHCP4** – use address provided by DHCPv4 Option 4, if available *(default)* **STATIC** – always use default *address or name* *address or name* is the default address in IPv4 or IPv6 format or DNS fully-qualified domain name.
<**time_server2**>	IP Address of optional Secondary NTP Time Server.

Network Settings	
XML Tag	**Data / Description**
address or name </**time_server2**>	*address or name* is the default address in IPv4 or IPv6 format or DNS fully-qualified domain name. *If <time_server source=DHCP4>, the address will be configured by DHCPv4 Option 4, if available.*
<**time_server_key**> *key string 1* : : *key string n* </**time_server_key**>	Authentication String(s) for NTP Time Server(s). Each key string must be in the exact form: keynumber **M** key keynumber: assigned by time server administrator **0 – 65534** key: assigned by time server administrator Multiple keys may be defined; enter each key on a separate line.
<**time_offset**> *hours or seconds* </**time_offset**>	Offset (in hours or seconds) from UTC or time server time. If this parameter value is in the range or **-12** to **12**, it is assumed to be hours. A value in the range **-43200** to **-13** or **13** to **43200** is assumed to be seconds. Pacific Standard Time = –8 Pacific Daylight Time = –7 Mountain Standard Time = –7 Mountain Daylight Time = –6 Central Standard Time = –6 Central Daylight Time = –5 Eastern Standard Time = –5 Eastern Daylight Time = –4 **+43200** to **-43200**, *default value = 0* *If <time_server source=DHCP4>, time_offset will be configured by DHCPv4 Option 2, if available.*

Network Settings	
XML Tag	**Data / Description**
<**dst enabled**="*ON/OFF*"> <**start_date**> *date* </**start_date**> <**end_date**> *date* </**end_date**> <**time_adjust**> *± hr:min* </**time_adjust**> </**dst**>	Enables automatic daylight savings time adjustment at the specified start and end dates each year. *ON/OFF* indicates enabled or disabled. **ON** *(default)* **OFF** *date* is the daylight savings time start date and end date. The dates can be specified as the first, second, third, fourth, or last weekday in a given month, or as a day and month, followed by "at" and the time of day. Examples: fourth Monday January at 3:55pm 28 February at 7:22am *default start date*: second Sunday March at 2:00am *default end date*: first Sunday November at 2:00am *±hr:min* is the amount to adjust the time **+** or **-** **0** – **23** hours **:** **00** – **59** minutes *default value = -1:00*
<**syslog_option**> *logging option* </**syslog_option**>	Logging option for the Syslog Server operation. **NONE** – Disabled / No Logging *(default)* **BASIC** – SIP Phone Error Logs are sent to Syslog server **QOS** – Error Logs and Quality of Service call packet statistics sent
<**ip_syslog source**="*src*" > *address or name* </**ip_syslog**>	IP Address of the Syslog Server. May be provided by DHCP or statically assigned. *src* is source of the IP address: **DHCP4** – use address provided by DHCPv4 Option 7, if available *(default)* **STATIC** – always use default *address or name* *address or name* is the default address in IPv4 or IPv6 format or DNS fully-qualified domain name.

Network Settings	
XML Tag	**Data / Description**
<**vlan**> <**enable**> *ON/OFF* </**enable**> <**id**> *VLAN ID* </**id**> <**voice_pri**> *priority* </**voice_pri**> <**signal_pri**> *priority* </**signal_pri**> </**vlan**>	VLAN / Ethernet Layer 2 802.1Q support. enable: **ON** **OFF** *(default)* *If <ip_dhcp4_enable> is ON, this parameter will be configured by DHCPv4 Option 125 or Option 242 L2Q parameter, if available.* id: Phone VLAN ID A value of **0** (zero) indicates that the phone does not belong to any VLAN; in this case, the 802.1Q tag specifies only a priority and is referred to as a *priority tag*. **0, 2 – 4094**, *default value = 1111* *If <ip_dhcp4_enable> is ON, this parameter will be configured by DHCPv4 Option 125 or Option 242 L2QVLAN parameter, if available.* voice_pri: 802.1Q Voice Priority Code Point **0 – 7**, *default value = 6* *If <ip_dhcp4_enable> is ON, this parameter will be configured by DHCPv4 Option 125 or Option 242 VoicePri parameter, if available.* signal_pri: 802.1Q Signaling Priority Code Point **0 – 7**, *default value = 6* *If <ip_dhcp4_enable> is ON, this parameter will be configured by DHCPv4 Option 125 or Option 242 SignalPri parameter, if available.*
<**dscp_voice**> *DSCP value* </**dscp_voice**>	Layer 3 DiffServ Voice Packet DSCP Value. **0 – 63**, *default value = 46*
<**dscp_signal**> *DSCP value* </**dscp_signal**>	Layer 3 DiffServ Signal Packet DSCP Value **0 – 63**, *default value = 46*
<**nat_keepalive_type**> *type* </**nat_keepalive_type**>	Keeps a connection through a NAT device open. **0** – NAT keepalive is disabled *(default)* **1** – UDP Protocol: A SIP Options message is sent to keep the connection open TCP Protocol: NAT keepalive is maintained by the socket device

Network Settings	
XML Tag	**Data / Description**
<**nat_keepalive_timer**> *domain name* </**nat_keepalive_timer**>	The NAT keepalive rate in seconds. A value of **0** (zero) disables NAT keepalive. **0 – 255** seconds, *default value = 0 (disabled)*

Security Settings

Security Settings	
XML Tag	**Data / Description**
<**install_pin**> *PIN* </**install_pin**>	Protects access to the phone Installation Options Menu. 4 to 20 numeric digits, default value blank (no PIN)
<**pc_port_enable**> *ON/OFF* </**pc_port_enable**>	Allows the user to enable or disable the PC port. **ON** – PC port can be enabled/disabled in the INSTALL menu on the phone. *(default)* **OFF** – PC port is always disabled.
<**arp_star_enable**> *ON/OFF* </**arp_star_enable**>	Enables software that protects against ARP table corruption. **ON** **OFF** *(default)*
<**ocsp_enable**> *ON/OFF* </**ocsp_enable**>	Enables the Online Certificate Service Protocol (OCSP) to check for revoked certificates during a TLS connection between the phone and the SIP Proxy server. **ON** **OFF** *(default)*
<**ocsp_url**> *url* </**ocsp_url**>	Provides the URL to the OCSP responder and is the "–url" argument to the OpenSSL OCSP command. Both HTTP and HTTPS URLs can be specified. Optionally, other OpenSSL OCSP command line arguments can be appended to this parameter only, such as http://192.168.72.48:2560 -validity_period 1200.
<**ocsp_issuer_cert**> *filename.pem* </**ocsp_issuer_cert**>	The .pem file that contains the current OSCP issuer certificate. *filename* includes the full path specification, and can be up to 250 characters.

Security Settings	
XML Tag	**Data / Description**
<**ocsp_va_cert**> *filename.pem* </**ocsp_va_cert**>	The file that contains explicitly-trusted responder certificates. This option must be provided if the certificates are self-signed. *filename* includes the full path specification, and can be up to 250 characters.
<**ocsp_signer_cert**> *filename.pem* </**ocsp_signer_cert**>	The file that contains the certificate used to sign the OCSP request. If *ocsp_signer_key* is not present, the private key is read from this file. If neither option is present, then the OCSP request is not signed. *filename* includes the full path specification, and can be up to 250 characters.
<**ocsp_signer_key**> *filename.pem* </**ocsp_signer_key**>	The file that contains the key used to sign the OCSP request. If this file is not present, the private key is read from *ocsp_signer_cert*. If neither option is present, then the OCSP request is not signed. *filename* includes the full path specification, and can be up to 250 characters.
<**cert_private_phone**> *filename.pem* </**cert_private_phone**>	The file that contains the certificate and private key for the phone. The server must have the certificate and public key in order to validate the phone. *filename* includes the full path specification, and can be up to 250 characters.
<**cert_trusted_ca_list**> *filename.pem* </**cert_trusted_ca_list**>	The file that contains a list of trusted certificate authorities. *filename* includes the full path specification, and can be up to 250 characters.
<**tls_require_cert**> *ON/OFF* </**tls_require_cert**>	Determines whether a valid certificate is required for a TLS connection. If set to OFF, the phone will accept any certificate from the server as valid. **ON** **OFF** *(default)* **Important Note**: This tag must reside in the XML file AFTER the following tags: <cert_private_phone>, <cert_trusted_ca_list>, <ocsp_issuer_cert>, <ocsp_va_cert>, <ocsp_signer_cert> and <ocsp_signer_key>.

Security Settings	
XML Tag	**Data / Description**
<**cal_mode**> *mode* </**cal_mode**>	The phone's Confidential-Access-Level Mode. **NONE** *(default)* **FIXED** **VARIABLE**
<**cal_access_level**> *level* </**cal_access_level**>	The phone's fixed mode Confidential-Access-Level. **0 – 99**
<**cal_matrix**> *integer list* </**cal_matrix**>	An array of 100 integers comprising the phone's Confidential-Access-Level Matrix. This matrix is used for variable mode access-level resolution, where a requested access-level is used as an index into this array to obtain the reflected access-level. The default is an array whose first element is the value 0 and subsequent elements sequentially increase by one until the last value is 99. Each element of the array must be less than 100. Separate array elements with commas. An element of less than zero is valid in order to indicate a requested access level that cannot be resolved. **0**, **1**, **2**, ...**99**

SIP Settings

SIP Settings	
XML Tag	**Data / Description**
<**sip_transport**> *SIP transport type* </**sip_transport**>	Defines the type of SIP transport. **UDP** *(default)* **TCP** **TLS** – uses SIP in the URI **TLS+** – uses SIPS in the URI
<**rport_updates_contact**> *ON/OFF* </**rport_updates_contact** >	Enables phone to use received rport parameters to update its own SIP Contact Header. **ON** **OFF** *(default)*
<**srtp_enable**> *ON/OFF* </**srtp_enable**>	Enables SRTP (Secure Real-time Transport Protocol). **ON** **OFF** *(default)*
<**phone_port**> *port number* </**phone_port**>	Port number used by the phone to receive SIP signaling messages. The form is *xxxxx* with leading zeros suppressed. **1025** - **65534**, *default value = 5060*
<**server_type**> *type* </**server_type**>	The SIP Call Server Type. **GENERIC** *(default)* **AVAYA**
<**sip_user_agent**> *header string* </**sip_user_agent**>	The string used in the SIP User-Agent header. If this string contains **Teo**, the phone will append _<model>/<software_version>_<mac_address> Maximum length is 128 ASCII characters. *default value = Teo*
<**sip_url_type**> *URL type* </**sip_url_type**>	Defines the type of URL that is transmitted in outbound INVITE messages. **SIP** *(default)* **TEL**
<**msg_sum_sub**> *ON/OFF* </**msg_sum_sub**>	Determines whether the phone subscribes to message summary events for Message Waiting Indication. This parameter should be set to **OFF** for Cisco voicemail systems. **ON** *(default)* **OFF**

SIP Settings	
XML Tag	**Data / Description**
<**sip_sub_exp**> *seconds* </**sip_sub_exp**>	The number of seconds that the subscription is valid before the phone must renew its subscription with the SIP Proxy. Valid range is **10** to **7200** seconds (10 seconds to 2 hours) with leading zeros suppressed. *default value = 3600 (1 hour)*
<**sip_attmpt_b4_backup**> *unsuccessful transmissions* </**sip_attmpt_b4_backup**>	The number of unsuccessful transmissions before the phone switches to the Backup Proxy Server in the form *xx* with leading zeros suppressed. **2** to **10**, *default value = 8*
<**sip_retry_reg_timer**> *seconds* </**sip_retry_reg_timer**>	The number of seconds between SIP registration retries. Valid range is **1** to **65535** seconds (1 second to18.2 hours) in the form *xxxxx* with leading zeros suppressed. *default value = 30*
<**session_refresher**> *entity* </**session_refresher**>	The entity that refreshes the SIP session. **NONE** **LOCAL** **REMOTE** **ANY** *(default)*
<**session_timer**> *keep alive* </**session_timer**>	Session timer keep alive mechanism is described in RFC 4028. **REQUIRED** **SUPPORTED** **UNSUPPORTED** *(default)*
<**session_timer_min**> *seconds* </**session_timer_min**>	The minimum value that the phone will accept for the session. This value cannot be larger than the <session_timer_interval>. Valid range is **90** to **2,147,483,647** seconds (1.5 minutes to 68 years) with leading zeros suppressed. *default value = 90*
<**session_timer_interval**> *seconds* </**session_timer_interval**>	The maximum amount of time that can occur between session refresh requests in a dialog before the session will be considered timed out. Valid range is **90** to **2,147,483,647** seconds (1.5 minutes to 68 years) with leading zeros suppressed. *default value = 3600 (1 hour)*
<**sip_refresh_use_update**> *ON/OFF* </**sip_refresh_use_update**>	Enables the use of SIP UPDATE method for session refreshes. **ON** **OFF** *(default)*

SIP Settings	
XML Tag	**Data / Description**
<**phone_context**> *context string* </**phone_context**>	Defines the default phone-context to be used when calling local numbers when the SIP URL type is “tel”. The default setting is a zero length string.
<**sip_privacy_values**> *string* </**sip_privacy_values**>	Defines a string up to 32 characters to be used for the SIP Privacy Header in accordance with RFC 3323.
<**sip_compact_hdrs**> *ON/OFF* </**sip_compact_hdrs**>	Enables the generation of SIP compact headers. **ON** **OFF** *(default)*
<**prack**>*option* </**prack**>	Provisional response acknowledgement (PRACK) is defined in RFC 3262. This parameter should be set to **UNSUPPORTED** for Cisco and BroadSoft platforms. **REQUIRED** **SUPPORTED** *(default if* <server_type> *is* **AVAYA***)* **UNSUPPORTED** *(default if* <server_type> *is* **GENERIC***)*
<**preconditions_tag**> *option* </**preconditions_tag**>	The preconditions tag is defined in RFC 3312. **REQUIRED** **SUPPORTED** **UNSUPPORTED** *(default)*
<**phone_rtp_port**> *port number* </**phone_rtp_port**>	RTP starting port used to send voice packets for the first line appearance. The form is *xxxxx* with leading zeros suppressed. The associated RTCP port is always the next sequential (odd-numbered) port above the RTP port. Subsequent line appearances will automatically be assigned to the next sequential even-numbered port. **16384** - **65534**, *default value = 16384*
<**sdp_anat**> *option* </**sdp_anat**>	Session Description Protocol, Alternative Network Type option tag in SIP header fields. Refer to RFC 4091 and RFC 4092. **REQUIRED** **SUPPORTED** **UNSUPPORTED** *(default)*
<**sip_early_media**> *ON/OFF* </**sip_early_media**>	Allows the phone to play early media (audio) when receiving a SIP 180 response with SDP to an INVITE request. If OFF, any SDP that accompanies a SIP 180 response will be ignored by the phone, early media will not be played, and local ringback will be generated. **ON** *(default)* **OFF**

SIP Settings	
XML Tag	**Data / Description**
<**silence_suppress**> *ON/OFF* </**silence_suppress**>	Allows audio silence suppression. The purpose is to detect silent periods in the voice signal and temporarily discontinue transmission of RTP packets during silence. **ON** **OFF** *(default)*
<**voice_idle_disconnect**> *ON/OFF* </**voice_idle_disconnect**>	When this setting is ON, and the phone does not receive voice packets or a comfort noise packet, it will disconnect the phone after 20 seconds. **ON** **OFF** *(default)*
<**sip_alert_info_list**> <**ai index**="*index*" <**alert_info>** *header string* </**alert_info**> <**ring_type>** *ring type* </**ring_type**> <**auto_answer>** *answer type* </**auto_answer**> </**ai**> : : </**sip_alert_info_list**>	Up to 10 sip_alert_info strings can be configured in this list. index: identifies the sip_alert_info type, **1 – 10**. header string: custom alert-info header string, 128 characters max. When an incoming INVITE request is received with the Alert-Info header field matching this value, the associated ring_type cadence will be used. If the associated answer_type is set for auto answer (and other auto answer criteria are met), the call will be auto answered. ring type: ring type cadence to use when the defined alert_info header string is received, if auto answer is disabled. **AI_RING_NORMAL** 2 sec ON, 4 sec OFF *(default)* **AI_RING_DISTINCTIVE** 0.8 ON, 0.4 OFF, 0.8 ON, 4 OFF **AI_RING_PRIORITY** 0.4 ON, 0.2 OFF, 0.4 ON, 0.2 OFF, 0.8 ON, 4 OFF **AI_RING_INTERCOM** 0.3 ON, 0.2 OFF, 1.0 ON, 0.2 OFF, 0.3 ON, 4 OFF **AI_RING_REMINDER** single burst 0.5 ON answer type: auto answer behavior when the defined alert_info header string is received. **AA_OFF –** auto answer disabled *(default)* **AA_ON_MUTE –** auto answer with muted audio **AA_ON_2WAY –** auto answer with 2-way audio **AA_ON_CSTA** – unconditional auto answer with 2-way audio

SIP Settings	
XML Tag	**Data / Description**
<**sip_proxy_addr source**="*src*"> *address or name* </**sip_proxy_addr**>	IP address or server name of the SIP Proxy Server (Call Server). May be provided by DHCP or statically assigned. *src* is source of the IP address: **DHCP4 –** use address provided by DHCPv4 Option 120, or Option 125 SipProxyServer parameter, if available *(default)* **STATIC –** always use default *address or name* *address or name* is the default address in IPv4 or IPv6 format or DNS fully-qualified domain name.
<**sip_proxy_port**> *port number* </**sip_proxy_port**>	Port number used by the phone to send SIP signaling messages to the Proxy Server. The form is *xxxxx* with leading zeros suppressed. **1025** - **65534**, *default value = 5060* *If <sip_proxy_addr source= DHCP4> the port number will be provided by DHCP Option 125, SipProxyPort parameter, if available.*
<**sip_registrar**> *address or name* </**sip_registrar**>	IP address or domain name of the SIP Registrar (most server implementations combine this into a single SIP server application). If left blank or omitted, <sip_proxy_addr> will be used. This value is used inside SIP message headers, in the form <line_id>@<sip_registrar>:<sip_reg_port>, to reference the SIP server (e.g. 1000@192.168.72.5:5060 or 1000@teo:5060). *If <sip_proxy_addr source= DHCP4> SIP Registrar will be provided by DHCP Option 125, SipRegistrar parameter, if available.*
<**sip_reg_port**> *port number* </**sip_reg_port**>	Port number for the SIP Registrar. **1025** - **65534,** *default value = 5060* This value is used inside SIP message headers, in the form <line_id>@<sip_registrar>:<sip_reg_port>, to reference the SIP server. *If <sip_proxy_addr source= DHCP4> the port number will be provided by DHCP Option 125, SipRegPort parameter, if available.*

SIP Settings	
XML Tag	**Data / Description**
<**sip_registration**> *ON/OFF* </**sip_registration**>	Determines if registration with the SIP Registrar is enabled. If ON is selected, the phone will determine if an IP address is available for the SIP Registrar; if so, it will attempt to register with it. If OFF is selected, registration is not attempted. **ON** *(default)* **OFF**
<**sip_reg_exp**> *seconds* </**sip_reg_exp**>	The number of seconds that the registration is valid before the phone must re-register with the SIP Proxy. Valid range is **10** to **7200** seconds (10 seconds to 2 hours) in the form *xxxx* with leading zeros suppressed. *default value = 3600 (1 hour)*
<**sip_backup_proxy_addr**> *address or name* </**sip_backup_proxy_addr**>	IP address or server name of the SIP Backup Server or Redundant SIP Proxy. *address or name* is the default address in IPv4 or IPv6 format or DNS fully-qualified domain name. *If <sip_proxy_addr source= DHCP4> the address will be provided by DHCP Option 120, if available.*
<**sip_backup_proxy_port**> *port number* </**sip_backup_proxy_port**>	Port number used by the phone to send SIP signaling messages, in the form *xxxxx* with leading zeros suppressed. **1025** - **65534**, *default value = 5060*
<**sip_backup_reg_id**> *address or name* </**sip_backup_reg_id**>	IP address or domain name of the SIP Registrar when the Backup Proxy Server is used (most server implementations combine this into a single SIP server application). If left blank or omitted, <sip_backup_proxy_addr> will be used. This value is used inside SIP message headers, in the form <line_id>@ <sip_backup_reg_id>:<sip_backup_reg_port>, to reference the SIP server (e.g. 1000@192.168.72.5:5060 or 1000@teo:5060).
<**sip_backup_reg_port**> *port number* </**sip_backup_reg_port**>	Port number for the SIP Registrar when the Backup Proxy Server is used. **1025** - **65534,** *default value = 5060* This value is used inside SIP message headers, in the form <line_id>@ <sip_backup_reg_id>:<sip_backup_reg_port>, to reference the SIP server.

SIP Settings	
XML Tag	**Data / Description**
<**sip_backup_reg**> *ON/OFF* </**sip_backup_reg**>	Determines if registration with the Backup SIP Registrar is enabled. If OFF is selected, registration is not attempted. **ON** **OFF** *(default)*
<**sip_backup_reg_exp**> *seconds* </**sip_backup_reg_exp**>	The number of seconds that the registration is valid before the phone must re-register with the Backup SIP Proxy. Valid range is **10** to **7200** seconds (10 seconds to 2 hours) with leading zeros suppressed. *default value = 3600 (1 hour)*
<**global_barge_in_mode**> *ENABLED* </ **global_barge_in_mode** >	Controls phone behavior when a user selects a shared, active call. If ENABLED is selected, the phone will automatically barge-in (aka. bridge) into the call. If DISABLED is selected, the phone will show an indication that barge-in (aka. bridge) is disabled. If PROMPT is selected, the phone will prompt whether the user wants to barge-in (aka. bridge) into the call. **ENABLED** *(default)* **DISABLED** **PROMPT**

SIP Settings	
XML Tag	**Data / Description**
<**sip_server_list**> <**ss index**="*index*"> <**proxy_id>** *IP address* </**proxy_port**> <**proxy_port>** *port_number* </**proxy_port**> <**registrar_id>** *IP address* </**registrar_id**> <**registrar_port>** *port_number* </**registrar_port**> <**registrar_enable>** *ON/OFF* </**registrar_enable** > <**registration_expires>** *seconds* </**registration_expires** > </**ss**> : : </**sip_server_list**>	Up to 10 SIP servers can be configured. index: **1 – 10**, identifies the server, and determines server priority; 1 is the highest priority. proxy_id: SIP Proxy Server IP address in valid IPv4 or IPv6 format. *If <sip_proxy_addr source= DHCP4>, the address will be configured by DHCPv4 Option 120 or Option 125, SipProxyServer parameter, if available.* proxy_port: Port number used by the phone to send SIP signaling messages to the proxy server. The form is *xxxxx* with leading zeros suppressed. *May be configured by DHCPv4 Option 125, SipProxyPort parameter.* **1025** - **65534**, *default value = 5060* registrar_id: IP address or domain name of the SIP Registrar. *May be configured by DHCPv4 Option 125, SipRegistrar parameter.* If left blank or omitted, <proxy_id> will be used. This value is used inside SIP message headers, in the form <line_id>@<registrar_id>:<registrar_port>, to reference the SIP server. registrar_enable: Determines if registration with the SIP Registrar is enabled. If OFF is selected, registration is not attempted. **ON** *(default)* **OFF** registrar_port: Port number for the SIP Registrar. *May be configured by DHCPv4 Option 125, SipRegPort parameter.* **1025** - **65534,** *default value = 5060* registration_expires: The number of seconds that the registration is valid before the phone must reregister with the SIP Proxy. Valid range is **10** to **7200** seconds (10 seconds to 2 hours) with leading zeros suppressed. *default value = 3600 (1 hour)* **NOTE:** Do not use any of the following tags if the sip_server_list tag if used: <sip_proxy_addr> <sip_backup_proxy_addr> <sip_proxy_port> <sip_backup_proxy_port> <sip_registrar> <sip_backup_reg_id> <sip_reg_port> <sip_backup_reg_port> <sip_registration> <sip_backup_reg> <sip_reg_exp> <sip_backup_reg_exp>

PIDF-LO Settings

Settings in this section include PIDF-LO Discovery Mode, PIDF-LO coordinate location and PIDF-LO civic address/location.

PIDF-LO Settings	
XML Tag	**Data / Description**
<**pidflo_discovery_mode**> *mode* </**pidflo_discovery_mode**>	The phone's PIDF-LO Discovery Mode. **LLDPMED** **DHCP** **STATIC** **OFF** *(default)*

PIDF-LO Settings	
XML Tag	**Data / Description**
<**pidflo_coordinates**> <**latitude**> latitude <**/latitude**> <**longitude**> longitude <**/longitude**> <**altitude unit**="*units*"> altitude <**/altitude** > </**pidflo_coordinates**>	The phone's PIDF-LO information as coordinate location where phone is located (for more information, see RFC 5491). latitude: Latitudinal coordinate. <value><direction> where <value> is **0.0 – 90.0** and <direction> is E or W (e.g. 59.96777W) longitude: Longitudinal coordinate. <value><direction> where <value> is **0.0 – 180.0** and <direction> is N or S (e.g. 3.3124N) units: Altitude units. **m** - meters **f** - floors altitude: Altitude coordinate. **-2000.0 – 2000.0,** (e.g. 77 or 228.57 or -33.2)

PIDF-LO Settings	
XML Tag	**Data / Description**
<**pidflo_civic_address**> <**country**>country<**/country**> <**language**> language <**/language**> <**country-subdivision**> country-subdivision <**/country-subdivision**> <**county**>county<**/country**> <**city**>city<**/city**> <**city-division**> city-division <**/city-division**> <**block**>block<**/block**> <**street**>street<**/street** > <**direction**>direction<**/direction**> <**trailing-street-suffix**> trailing-street-suffix <**/trailing-street-suffix**> <**street-suffix**> street-suffix <**/street-suffix** > <**number**>number<**/number**> <**number-suffix**> number-suffix <**/number-suffix**> <**zip**>zip<**/zip**> <**building**>building<**/building**> <**unit**>unit<**/unit**> <**floor**>floor<**/floor**> <**room**>room<**/room**> </**pidflo_civic_address**>	The phone's PIDF-LO information as a civic address where phone is located (for more information, see RFC 5139). country: 2-letter ISO 3166 code identifying country. language: primary language. country-subdivision: country subdivision. county: county city: city city-subdivision: city subdivision block: block street: street direction: direction trailing-street-suffix: trailing street suffix street-suffix: street suffix number: number number-suffix: number-suffix zip: zip building: building direction: direction unit: unit floor: floor room: room

General Phone Settings

Settings in this section include user preference settings, feature activators, multifunction key assignments, call control, call directory, and dialing plans.

General Phone Settings	
XML Tag	**Data / Description**
<**display_contrast**> *contrast level* </**display_contrast**>	This sets the phone display contrast. **1–8**, *default value = 4*
<**speakerphone**> *mode* </**speakerphone**>	Sets the speakerphone mode of operation. **ENABLED** – full speakerphone, non-TSG models only. *(non-TSG default)* **MONITOR** – listen-only mode, microphone is disabled. **DISABLED** – speaker and microphone disabled. *(TSG default)*
<**voice_mode_headset**> *ON/OFF* </**voice_mode_headset**>	Allows the user to select the default voice path for phone calls. When set to ON, calls are routed to the headset jack. **ON** **OFF** *(default)*
<**line_mode**> *mode* </**line_mode**>	Defines the phone's line mode. **NORMAL** *(default)* **WARM** **HOT**
<**hot_warm_username**> *string* </**hot_warm_username**>	Username portion of Request-URI (the address that will be automatically dialed) for Hotline or Warmline calls. This value is only used when <line_mode> is set to WARM or HOT. *string* is determined by the switch platform. Example: 2001 (dial extension 2001)
<**warmline_timeout**> *seconds* </**warmline_timeout**>	Defines the Warmline dial timeout duration in seconds. **2 – 30** seconds, *default value = 3*
<**phone_dial_timeout**> *seconds* </**phone_dial_timeout**>	When off-hook, this is the amount of time the phone waits after a digit is pressed before sending the dialed digits to the SIP Call Server for call processing, if the user does not otherwise initiate sending by pressing the SEND key. A value of **0** (zero) allows an unlimited time for dialing, with no timeout. **0 – 30** seconds, *default value = 10*

General Phone Settings	
XML Tag	**Data / Description**
<**sip_invite_timeout**> *seconds* </**sip_invite_timeout**>	This is the time period that the phone will wait for a response to an INVITE when originating a call. The call will be abandoned if the called party is not detected before the timeout expires. A value of **0** (zero) allows an unlimited time for the server to respond, with no timeout. **0 – 120** seconds, *default value = 40*
<**refer_timeout**> *seconds* </**refer_timeout**	Timeout for call transfers. If the transfer is not completed by this time, the phone clears the calls. **0 – 99**, *default value = 4*
<**phone_max_ringing**> *seconds* </**phone_max_ringing**>	Specifies the maximum number of seconds that the phone will persist in the ringing state for an incoming call. A value of **0** (zero) allows unlimited ringing, with no timeout. **0 – 300** seconds, *default value = 0*
<**phone_max_reorder**> *seconds* </**phone_max_reorder**>	Specifies the maximum number of seconds that the phone will persist in the reorder (disconnected or error) state. A value of **0** (zero) allows the phone to stay in the reorder state forever, with no timeout. **0 – 300** seconds, *default value = 180*
<**ring_offhk_continuous**> *ON/OFF* </**ring_offhk_continuous**>	Determines whether the phone rings normally, or only provides a single burst of ringing when the user is on a call. **ON** – continuous ring when off-hook **OFF** – single ring when off-hook *(default)*
<**ring_pref**> *ringing preference* </**ring_pref**>	Determines the action of the phone when going off hook with the handset, speaker key, or headset key. **RING** – the oldest ringing call is automatically selected; if there is no ringing line appearance, an idle one is selected. *(default)* **IDLE** – an idle line appearance key is automatically selected, even if another one is ringing. **NONE** – automatic line appearance selection is disabled; user must press a line appearance key to answer or originate a call.
<**hand_rcv**> *volume level* </**hand_rcv**>	Sets the handset receive volume. **1 – 8**, *default value = 4*

General Phone Settings	
XML Tag	**Data / Description**
<**hand_xmit**> *volume level* </**hand_xmit**>	Sets the handset transmit gain. **1 – 8**, *default value = 4*
<**head_rcv**> *volume level* </**head_rcv**>	Sets the headset receive volume. **1 – 8**, *default value = 4*
<**head_xmit**> *volume level* </**head_xmit**>	Sets the headset transmit gain. **1 – 8**, *default value = 4*
<**spkr_xmit**> *volume level* </**spkr_xmit**>	Sets the speakerphone transmit gain. **1 – 8**, *default value = 4* *(does not apply to TSG models)*
<**blf_console_base**> *line appearance number* </**blf_console_base**>	Determines the starting line appearance for a Sylantro server-defined Busy Lamp Field (BLF). If this setting is DISABLED, the phone will ignore Sylantro server configuration messages for this feature. **2 – 50** (button number), or **0** (disabled, default)

Dial Plan Settings

A Dial Plan allows the administrator to configure the phone so that specific dial patterns direct the phone to:

General Functionality

- Automatically initiate a call upon recognition of a specific dial pattern
- Add/Replace/Delete a specific prefix pattern
- Add/Replace/Delete a specific suffix pattern
- Generate secondary dial tone upon recognition of a specific dial pattern
- Block access to specific dial patterns

MLPP Specific Functionality

- Add URL parameters to the outbound INVITE
- Add the r-priority to the called party ID display
- Add a Resource Priority Header to the outbound INVITE
- Add a CAL Header to the outbound INVITE

Dial Plan Settings	
XML Tag	**Data / Description**
<**dial_plan**> *dial plan definition* </**dial_plan**>	Defines the phone's Dial Plan. The default dial plan is blank (no dial plan).
<**emergency_number**> *number list* </**emergency_number**>	Defines a comma-separated list of emergency numbers in order to recognize when an emergency outbound call is dialed. When one of these numbers has been dialed, the call cannot be preempted, put on hold, locally conferenced or transferred. Additionally, if PIDF-LO is enabled, the outbound INVITE payload will include PIDF-LO information. The default emergency number list contains only 911.

A dial plan is stored as a text string; a null <dial_plan> does not affect user dialing in any way. The complete BNF (Backus-Naur Form) syntax that defines the structure for the dial plan is in Appendix B on page 82.

The dial plan is set by creating an xml entry which defines how the phone should process dialed strings. The tag for this entry is <dial_plan>.

<dial_plan>*dial plan definition***</dial_plan>**

The dial plan definition is broken down into one or more "components" which provide specific dialing instructions. The components are separated by a "|". (The "|" has other uses depending on where it is used. These cases will be explained in detail later in this section.) As each digit is dialed, it is evaluated by each component from left to right.

<dial_plan>*component1***|***component2***|***componentN***</dial_plan>**

Each component can have three sections: a prefix operation, a dial pattern, and a suffix operation. Note the placement of the brackets.

<dial_plan>{*prefix operation***}***dial string***{***suffix operation***}</dial_plan>**

Special Characters

{ } *(left & right brace/curly brace/curly bracket, ASCII 123 & 125)*
encloses prefix and suffix operations

^ *(circumflex accent/caret/hat, ASCII 94)*
wildcard, matches any dialed digit

| *(vertical bar/vertical line, ASCII 124)*
separates components
in a prefix or suffix, indicates a substitution; characters to the left of the | are replaced by characters to the right

` *(grave accent/acute accent/backquote, ASCII 96)*
in a dial string, instructs the phone to produce a secondary dial tone
in a suffix, indicates a meta operation

Examples

The following is a sample of a dial plan with a single "component". The following dial plan will cause the phone to automatically initiate a call when the user dials "911". Also, at the time of call initiation, the phone replaces "911" with "2584357". You will notice that there are "|" characters which are not acting to separate components, but are part of the prefix and suffix operations.

```
<dial_plan>{911|2584357}911#{|}</dial_plan>
```

The components in the above dial plan can be broken down as follows:

{911|2584357} This is a "prefix operation" and is enclosed within the **{}**. The bar in the prefix operation tells the phone that if the digits in front of the bar are dialed at the beginning of the string, they are to be replaced with the digits after the bar.

911# This is the dial string. If the digits dialed match this string, the phone performs the prefix and suffix operations defined in this component. If the "#" occurs at the end of the dial string, it tells the phone to initiate a call after receiving digits which match those defined in the dial string.

Valid characters for the dial string are:

```
A-Z  a-z  0-9  . @ _ - / \, : ; * ' " ( ) < > ~ + = ? ! $ % &
(space)
```

{|} This is a "suffix operation" and is enclosed within the **{}**. The bar in the suffix operation tells the phone that if the digits in front of the bar are dialed as the last digits in the dialed string, they are to be replaced with the digits after the bar. Since there are no values entered, no operation is performed.

Another single component dial plan is shown below. This dial plan automatically initiates the call after seven characters, if the dialed string begins with a 3, 4, 5, or 9. Also, at the time of call initiation, the prefix "1425" is added to the beginning of the number.

```
<dial_plan>{|1425}[3-5,9]^^^^^^#{|}</dial_plan>
```

{|1425} Since there are no digits in front of the bar in the prefix operation, the digits after the bar are added to the dialed digits, which match the dial string, when the phone sends them out.

[3-5,9] ^^^^^^# A couple of new things are in the dialed string. The square brackets **[]** indicate that the string matches the dialed digits if any of the digits within the brackets are dialed in that position in the string. The dash indicates a range of characters, so **3-5** indicates that the digits 3, 4 or 5 are a match. If any of the digits 3, 4, 5 or 9 are dialed as the first digit, the string is matched. The **^** is a "wild card" which matches any dialed digit in that position in the dial string. In this case, the next 6 digits after the first can be any valid digit. Again the # terminator indicates that once you have a matching string, perform the prefix and suffix operations and then send the resulting digits.

{|} Like the previous example, no suffix operation is to be performed on dialed digits that match the dial string.

Combining the two previous examples results in the following dial plan.

```
<dial_plan>{911|2584357}911#{|}|{|1425}[3-5,9]^^^^^^#{|}</dial_plan>
```

The two components **{911|2584357}911#{|}** and **#{|1425}[3-5,9]^^^^^^#{|}** are separated by a "**|**". If 911 is dialed by the phone user, 2584357 will be immediately dialed by the phone. The first component matches before enough digits are dialed for the second component have a matching string. If 9234567 is dialed, the first component will stop processing after the second digit and the second component will continue process the digits since they meet the requirements of the dial string. The digit string 14259234567 will be sent out. If 811 is dialed, the dial string in neither component is matched and the phone sends out 811 after the dial timeout or after the user enters # from the keypad.

```
<dial_plan>{|}^^`{|}|{|}771900^^^^^^^!{|}|{77|}771^^^^^^^^^^^#{|}</dial_plan>
```

The above dial plan has 3 components. It introduces two more special characters: **`** and **!** . The **`** can have two meanings based on where it is located. The first is as a secondary dial tone indicator when in the dial string. The second is as a meta operation marker, which we will discuss later. The **!** is a block access marker. If the dialed string matches the dial string for this component, the user gets reorder and the phone does not generate a call.

{|}^^`{|} The first component will cause the phone to generate dial tone after the user dials any two digits.

{|}771900^^^^^^^!{|} The second component configures the phone so that for any call that begins with 771900 and has a total of 13 digits (digits shown plus 7 wild card digits), will be restricted.

{77|}771^^^^^^^^^^^#{|} The last component will for a dialed digit string that is 13 characters long and begins with a 77, strip off the 77 and immediately send the remaining string. So if a user dials 7718005551212, the phone will immediately send 18005551212.

MLPP Meta Operation Example

For a detailed explanation of meta operations, refer to the Appendix B on page 82.

```
<dial_plan>{|}911,{|}|{9[0-4]|}9[0-4]{|`R0}</dial_plan>
```

The components in the above dial plan can be broken down as follows:

{|}911,{|} If 911 is dialed, it will be sent without modification (will not be treated as a precedence call). The string is not sent until the user presses send, OK, or the dial timeout occurs.

{9[0-4]||} The phone will strip off the leading two digits if they are 90-94.

**{|`R0}** The ` identifies this as a meta operation string. This string will cause the phone to include a Resource Priority Header for the “dsn” network domain with r-priority identified by the second dialed character.

MLPP Settings

Multilevel Precedence and Preemption (MLPP) can only be implemented in a US Department of Defense network. This service has two parts: precedence and preemption. Precedence involves assigning a priority level to a call. Preemption involves the seizing of a communications channel that is in use by a lower precedence level caller, in the absence of an idle channel. Connections and resources that are in use by MLPP subscribers may be preempted only by higher precedence calls from other MLPP subscribers.

MLPP Settings

XML Tag	Data / Description
<**rph_namespace**> <**net_domain name=**"*netname*"> <**priority index=**"*index*" **disp=**"*name*"**>** *priority* </**priority**> : <**priority index=**"*index*" **disp=**"*name*"**>** *priority* </**priority**> </**net_domain**> : : <**net_domain name=**"*netname*"> <**priority index=**"*index*" **disp=**"*name***>** *priority* </**priority**> *(**rph_namespace** continued)* . . <**priority index=**"*index*" **disp=**"*name***>**	Default Resource Priority Header (RPH) assignment; defines a list of RPH namespaces as defined in RFC 4412. Include a <net_domain> element for each network domain. All network domain definitions (50 max.) are enclosed within the <rph_namespace> </rph_namespace> tags. Each network domain element contains up to 10 priority entries that specify a priority level for a dialed digit, and a character string that is displayed on the phone for the priority call. *netname* is the network domain name, 10 characters max. *priority* is the r-priority level, 15 characters max. *index* identifies the priority entry, and corresponds to a dialed digit. Allowable values are **0 – 9**. *name* is the displayed text, 15 characters max.
	Example Resource Priority SIP header: Resource Priority: dsn-000000.8 \ \ _ *priority* (r-priority) \ _ (precedence domain)

MLPP Settings	
XML Tag	**Data / Description**
priority </**priority**> </**net_domain**> </**rph_namespace**>	└ *netname* (network domain) The phones have three predefined namespaces: <net_domain name="**dsn**"> <priority index="0" disp="FO"> 8 </priority> <priority index="1" disp="F"> 6 </priority> <priority index="2" disp="I"> 4 </priority> <priority index="3" disp="P"> 2 </priority> <priority index="4" disp="R"> 0 </priority> </net_domain> <net_domain name="**q735**"> <priority index="0" disp="0"> 0 </priority> <priority index="1" disp="1"> 1 </priority> <priority index="2" disp="2"> 2 </priority> <priority index="3" disp="3"> 3 </priority> <priority index="4" disp="4"> 4 </priority> </net_domain> <net_domain name="**uc**"> <priority index="0" disp="FO"> 8 </priority> <priority index="1" disp="F"> 6 </priority> <priority index="2" disp="I"> 4 </priority> <priority index="3" disp="P"> 2 </priority> <priority index="4" disp="R"> 0 </priority> </net_domain> To clear a network domain, do not include any priority elements. <**net_domain name=**"*name_to_remove*"> </**net_domain>** To clear all network domains except the built-in defaults, enter "default" as the domain name. <**net_domain name=**"*default*"> </**net_domain>**
<**rsrc_prty_tag**> *option* </**rsrc_prty_tag**>	The resource-priority tag is defined in RFC 4412. **REQUIRED** **SUPPORTED** **UNSUPPORTED** *(default)*
<**max_rph_r_priority**> *index* </**max_rph_r_priority** >	Sets the maximum priority level the phone is allowed to call. Calls dialed with a higher priority than the maximum will be assigned the maximum allowed priority value. **0 – 9**, *default value = 2*

MLPP Settings	
XML Tag	**Data / Description**
<**dscp_mlpp_routine**> *routine DSCP* </**dscp_mlpp_routine**> <**dscp_mlpp_priority**> *priority DSCP* </**dscp_mlpp_ priority**> <**dscp_mlpp_immediate**> *immediate DSCP* </**dscp_mlpp_ immediate**> <**dscp_mlpp_flash**> *flash DSCP* </**dscp_mlpp_flash**> <**dscp_mlpp_override**> *flash override DSCP* </**dscp_mlpp_override**> <**dscp_mlpp_oride_oride**> *flash override override DSCP* </**dscp_mlpp_oride_oride**>	MLPP Layer 3 DiffServ Voice Packet DSCP Value. **0 – 63** *default values:* *routine = 49* *priority = 47* *immediate = 45* *flash = 43* *flash override = 41* *flash override override = 41*
<**preempt_held_timeout**> *seconds* </**preempt_held_timeout**>	When a held call is being preempted, this defines the amount of time before the held call is cleared. **1 – 24** seconds, *default value = 2*

Feature Activator Functions

This section defines the list of available features and associated activators/deactivators that can be assigned to Feature Activator keys *(page 67).* The features must be supported by the Call Server platform.

All tags in the following table must be enclosed within the <**feature_activator_list**> </**feature_activator_list**> tag.

Feature Activator Functions	
XML Tag	**Data / Description**
<**fa index**=”*x*”> </**fa**> *x* corresponds to the dial pad key used to select the Feature Activator from the phone menu: 1-9, 0, *, #	(All additional tags for a feature activator are enclosed within this tag.)

Feature Activator Functions	
XML Tag	**Data / Description**
<**fa_type**> *type* </**fa_type**>	Feature Activator type: **GENERIC** (feature is defined in the XML file) **LOCAL CFWD** (Call Forward, default phone feature) **LOCAL DND** (Do Not Disturb, default phone feature) **PRESENCE** (Teo UC Presence) **DIR CALL PICKUP** (Directed Call Pickup) Local features are defined in the phone, and do not require any additional parameters.
<**description**> *description text* </**description**>	Text shown in the phone display when assigning a feature to a multifunction key, 15 characters max. This text will be used as a key's on-screen label if there is no <label> tag for the key.
<**label**> *label text* </**label**>	On-screen key label, 18 characters max. (7810 series only).
<**prompt**> *prompt text* <**/prompt**>	Prompt shown to the user when the feature is activated, if the feature requires a prompt, 16 characters max.
<**activation**> *activation code* </**activation**>	Code used to activate the feature, if required; for example, ***72**. Additional characters can be included after the code as required by the feature. Refer to the Feature Activation and Deactivation Codes section *(page 60)*.
<**deactivation**> *deactivation code* </**deactivation**>	Code used to deactivate the feature, if required. Refer to the Feature Activation and Deactivation Codes section *(page 60)*.

Feature Activation and Deactivation Codes

Feature activation and deactivation codes are SIP server specific; refer to the server documentation. Both activate and deactivate codes can be specified for a single feature key; in this case, operation toggles between activate and deactivate modes. The "L" option (below) can be used to indicate the activate or deactivate key mode.

Some features require different types of functionality such as additional dialed digits, establishment of another call, and control of the feature key LED. Additional characters can be added to the code string to enable this functionality. Following are some typical feature "star codes" with additional characters:

CALL FORWARD activate *72#DIL (prompts for additional digits, then an auto-originated INVITE is sent with *72 + dialed digits; the feature key LED is turned on)

CALL FORWARD deactivate	*73#-IL	(does not prompt for additional digits; an auto-originated INVITE is sent with *73; the feature key LED is turned off)
CALL PARK	*98#DR-	(prompts for additional digits, then transfers the call to *98 + dialed digits)
CALL UNPARK	*99#DC-	(prompts for additional digits, then an auto-originated call is placed to *99 + dialed digits)
DIRECTED CALL PICKUP	*53#DC -	(prompts for additional digits, then an auto-originated call is placed to *53 + dialed digits)
GROUP CALL PICKUP	*54#-C-	(does not prompt for additional digits; an auto-originated call is placed to *54)

The star code must be followed by a **#** character.

The three characters following the # are defined as follows:

Character 1 – capital letter **D** to prompt the user to dial additional digits
- (hyphen) if no additional digits are required

Character 2 – capital letter **C** to initiate an auto-originated two-way audio call
capital letter **I** to send an auto-originated INVITE without audio
capital letter **R** to transfer an existing call
- (hyphen) if none of the above is required

Character 3 – capital letter **L** to turn on the feature key LED when an 'activate' feature code is sent, or turn off the feature key LED when a 'deactivate' feature code is sent
- (hyphen) indicates no action

Note: If the LED is off when the feature key is pressed, the activate code will be sent; if the LED is on, the deactivate code will be sent. Server feature activation/deactivation may not be synchronized with the phone feature key state (e.g. if the phone restarts due to a power loss). The feature key LED only indicates the phone feature key state; it is not guaranteed to indicate the server feature state.

Conference, Call Forward, and Voicemail Keys

Conference, Call Forward, and Voicemail Keys	
XML Tag	**Data / Description**
<**conference_key**> *conference type* </**conference_key**>	Defines the conference operation assigned to the CONF key on the phone. **TCS LOCAL** – conferences are implemented locally in the phone. *(default)* **CENTRAL 1** – conferences are implemented using a central media server.
<**loc_cfwd_id**> *dial string* </**loc_cfwd_id** >	Dial string for the local Call Forwarding target (forward-to) number, up to 128 characters. **{pause}** inserts a pause into the dial string.
<**loc_cfwd_na_time**> *seconds* </**loc_cfwd_na_time** >	The time an unanswered call rings before it is forwarded by local Call Forwarding. **2** – **99** seconds, *default value = 12*
<**loc_cfwd_opt**> *call type* </**loc_cfwd_opt** >	The type of calls that are forwarded by local Call Forwarding: **OFF** – No calls are forwarded *(default)* **ALL** – All calls **BUSY** – All calls when the phone is busy (no lines are available for incoming calls) **NOANS** – Unanswered calls that ring longer than the time set in *loc_cfwd_na_time* **BSY_NOANS** – All calls when the phone is busy, and unanswered calls
<**sip_call_deflect_id**> *user_id* </**sip_call_deflect_id**>	If the user presses Call Forward Local (CFWD) while a call is ringing, the inbound ringing call will be forwarded to a server-specified destination and the CFWD LED remains off. *user_id* is a valid user account recognized by the server.

Conference, Call Forward, and Voicemail Keys	
XML Tag	**Data / Description**
<**voice_mail**> <**vnumber**> *number* </**vnumber**> <**vserver_type**> *server type* </**vserver_type**> <**vkey position=**"*keynum*"> <**vcode**>*code*</**vcode**> <**vlabel**>*label*</**vlabel**> </**vkey**> : : <**vkey position=**"*keynum*"> <**vcode**>*code*</**vcode**> <**vlabel**>*label*</**vlabel**> </**vkey**> </**voice_mail**>	Configures the VMAIL key and up to 10 voice mail menu keys. vnumber: The number to dial for the voice mail system, 128 characters max. **{pause}** inserts a pause into the dialed string. vserver type: The type of voice mail server (7810 only). **TEO** – Teo UC System *(default)* **CISCO** – Cisco Unity Express **AVAYA** – Avaya Aura/Audix **ASTRSK** – Asterisk **NEC3C** – NEC Univerge 3C **APMAX** – Innovative Systems APMAX **CALLEG** – Callware Callegra **BROAD** – BroadSoft BroadWorks **MITEL** – Mitel Communications Director **GENA2** – Genband A2 **NONE** – no voicemail menu vkey position: The definition for voice mail menu keys (7810 only). *keynum* is the multifunction menu key that is being defined, **1 – 10**. vcode: The string that is dialed for the selected 7810 voice mail menu key, 128 characters max. vlabel: The 7810 on-screen menu key label, 18 characters max.

Multifunction Keys

This section defines multifunction key assignments.

All tags in the following tables must be enclosed within the <**multi_function_key_list**> </**multi_function_key_list**> tag.

All tags for a single key must be enclosed within the <**key** num="*x*"> </**key**> tag.

<table>
<tr><th colspan="2">Multifunction Keys</th></tr>
<tr><th>XML Tag</th><th>Data / Description</th></tr>
<tr><td><key num="<i>x</i>">
  <i>type</i>
</key></td><td>Key Type:
LINE
FA (Feature Activator)
BLF_PRES (Direct Station Selection/Busy Lamp Field, “presence” event type)
BLF_DLOG (Direct Station Selection/Busy Lamp Field, “dialog” event type)
DSS (Direct Station Selection, “dialog:sla” event type)
ACD (Automatic Call Delivery, only enter for the first key of an ACD pair)
SD (Speed Dial)
UNUSED

<i>x</i> is the key number:
7810: 1 – 10
8030X: 11 – 40
4101: 4 – 10 (for keys M1-M7, Speed Dial only)
4104: 1 – 16</td></tr>
<tr><td colspan="2">NOTE: A range of keys of the same type can be defined within a key tag.</td></tr>
<tr><td><key num="<i>y</i>" <i>to_num</i>="<i>z</i>">
  <i>type</i>
</key></td><td><i>y</i> is the first key number, <i>z</i> is the last key number</td></tr>
</table>

Line keys are part of the multifunction keys section.

Line Keys	
XML Tag	**Data / Description**
<**line_id**> *ID* </**line_id**>	SIP Line ID (username or directory number), 128 characters max.
<**sip_name**> *name* </**sip_name**>	SIP Display Name, 128 characters max.
<**sip_auth_id**> *auth ID* </**sip_auth_id**>	SIP Authentication ID, 128 characters max.
<**sip_password**> *password* </**sip_password**>	SIP Authentication Password, 128 characters max.
<**label**> *label text* </**label**>	On-screen key label, 18 characters max. (7810 series only). Default is the line ID unless specified.
<**bla_shared**> *bridged status* </**bla_shared**>	Bridged/Shared Line Appearance: **ON** (shared BLA/SLA) **OFF** (private)
<**alert_auto_answer**> *aa_option* </**alert_auto_answer**>	***Non-TSG models only.*** Enables auto answering on a per line basis for non-CSTA calls. When auto answering is enabled on any line key, a softkey option is provided on the idle phone screen to selectively enable or disable auto answering on-the-fly. Refer to **sip_alert_info_list** *(page 43)* to set up custom alert-info header strings for CSTA calls. **AA_OFF** – calls are never auto answered, unless the alert info header is configured for AA_ON_CSTA. *(default)* **AA_ON_MUTE** – a call that is auto answered will be muted, unless the alert info header is configured for AA_ON_CSTA. **AA_ON_2WAY** – a call that is auto answered will have 2-way audio, provided the alert info header is not configured for AA_ON_MUTE.
<**tone_type**> *tone type* </**tone_type**>	Determines the ringing tone type for a line. **1** – **6**, *default value = 5*

Line Keys	
XML Tag	**Data / Description**
<**control_type**> *ringing type* </**control_type**>	Determines how a line will ring. **ALWAYS** (always ring) *(default)* **NEVER** (never ring) **WAIT2** **WAIT3** **WAIT4** **WAIT5** **WAIT6** **WAIT7** (ring after 7 ring cycles) Note: 1 ring cycle = 6 seconds
<**codec1**> *codec type* </**codec1**>	1st (Preferred) Codec Type: **G711** *(default)* **G729A** **G722**
<**codec2**> *codec type* </**codec2**>	2nd (optional) Codec Type: **G711** **G729A** *(default)* **G722** **NONE**
<**codec3**> *codec type* </**codec3**>	3rd (optional) Codec Type: **G711** **G729A** **G722** *(default)* **NONE**
<**ptime**> *milliseconds* </**ptime**>	The requested packetization time for media transmission to the phone. **10, 20, 30, 40** milliseconds, *default value = 20*
<**jitter_buffer_adaptive**> *buffer type* </**jitter_buffer_adaptive**>	Jitter Buffer Type: **ON** (adaptive) *(default)* **OFF** (fixed)
<**jitter_delay_min**> *milliseconds* </**jitter_delay_min**>	Minimum adaptive Jitter Buffer Delay (only used if jitter_buffer_adaptive is ON): **0 – 280** milliseconds, *default value = 10*
<**jitter_delay_max**> *milliseconds* </**jitter_delay_max**>	Maximum adaptive Jitter Buffer Delay (only used if jitter_buffer_adaptive is ON): **0 – 300** milliseconds, *default value = 100*
<**jitter_delay**> *milliseconds* </**jitter_delay**>	Fixed Jitter Buffer Delay (only used if jitter_buffer_adaptive is OFF): **10 – 90** milliseconds, *default value = 35*

Feature Activator keys are part of the multifunction keys section.

Feature Activator Keys	
XML Tag	**Data / Description**
<**fa_index**> *feature index* </**fa_index**>	Feature preset number; corresponds to the dial pad key used to select the feature when programming at the phone. Features are defined in the <**fa**> tag *(page 59)*. **1 – 9**, **0**, *****, **#**

BLF_PRES, BLF_DLOG, and DSS keys are part of the multifunction keys section.

BLF_PRES, BLF_DLOG, and DSS Keys	
XML Tag	**Data / Description**
<**line_id**> *ID* </**line_id**>	SIP Line (username or directory number), 128 characters max.
<**sip_name**> *name* </**sip_name**>	SIP Display Name, 128 characters max.
<**sip_auth_id**> *auth ID* </**sip_auth_id**>	SIP Authentication ID, 128 characters max.
<**sip_password**> *password* </**sip_password**>	SIP Authentication Password, 128 characters max.
<**label**> *label text* </**label**>	On-screen key label, 18 characters max. (7810 series only).
<**codec1**> *codec type* </**codec1**>	1st (Preferred) Codec Type: **G711** *(default)* **G729A** **G722**
<**codec2**> *codec type* </**codec2**>	1st (optional) Codec Type: **G711** **G729A** *(default)* **G722** **NONE**

BLF_PRES, BLF_DLOG, and DSS Keys	
XML Tag	**Data / Description**
<**codec3**> *codec type* </**codec3**>	2nd (optional) Codec Type: **G711** **G729A** **G722** *(default)* **NONE**
<**ptime**> *milliseconds* </**ptime**>	Packetization time. **10, 20, 30, 40** milliseconds, *default value = 20*
<**jitter_buffer_adaptive**> *buffer type* </**jitter_buffer_adaptive**>	Jitter Buffer Type: **ON** (adaptive) *(default)* **OFF** (fixed)
<**jitter_delay_min**> *milliseconds* </**jitter_delay_min**>	Minimum adaptive Jitter Buffer Delay (only used if jitter_buffer_adaptive is ON): **0 – 280** milliseconds, *default value = 10*
<**jitter_delay_max**> *milliseconds* </**jitter_delay_max**>	Maximum adaptive Jitter Buffer Delay (only used if jitter_buffer_adaptive is ON): **0 – 300** milliseconds, *default value = 100*
<**jitter_delay**> *milliseconds* </**jitter_delay**>	Fixed Jitter Buffer Delay (only used if jitter_buffer_adaptive is OFF): **10 – 90** milliseconds, *default value = 35*
<**speeddial**> *dial string* </**speeddial**>	Speed Dial (DSS) string, up to 128 characters **{pause}** inserts a pause into the dial string. # at the end of the dial string dials the number immediately.

Speed Dial keys are part of the multifunction keys section.

Speed Dial Keys	
XML Tag	**Data / Description**
<**label**> *label text* </**label**>	On-screen key label, 18 characters max. (7810 series only).
<**speeddial**> *dial string* </**speeddial**>	Speed Dial digit/character string, 128 characters max. **{pause}** inserts a pause into the dial string. # at the end of the dial string dials the number immediately.

ACD keys are part of the multifunction keys section. The ACD function is not supported on all switch platforms.

ACD Keys	
XML Tag	**Data / Description**
NOTE: The ACD feature requires two consecutive keys. Enter the following tags and attributes for the first key only.	
<**group_id**> *ACD Group ID* </**group_id**>	ACD Group ID, typically a 4-digit extension, 128 characters max.
<**label_1**> *label text* </**label_1**>	On-screen key label for Login/Logout Key, 18 characters max. (7810 series only).
<**label_2**> *label text* </**label_2**>	On-screen key label for Activate/Deactivate Key, 18 characters max. (7810 series only).

Call Directory Entries

7810 series: Up to 100 Call Directory entries are allowed. Ten entries are displayed on each telephone screen page.

4101: Up to 12 Call Directory entries are allowed. Only one entry at a time is displayed on the telephone screen.

4104: Up to 36 Call Directory entries are allowed. Four entries are displayed on each telephone screen page.

Call Directory Entries	
XML Tag	**Data / Description**
<**directory_list** **clear_list=**"*NO/YES*"> <**directory entry**=”*x*”> <**dir_name**> *label text* </**dir_name**> <**dir_number**> *string* </**dir_number**> </**directory**> : <**directory entry**=”*x*”> <**dir_name**> *label text* </**dir_name**> <**dir_number**> *string* </**dir_number**> </**directory**> </**directory_list**>	*clear_list* determines if the call directory is cleared before making changes. **NO** – only the listed entries are added/changed. **YES** – clears the entire call directory before adding the listed entries. *x* is the call directory entry number, **1 – 100** (7810 series), **1 – 12** (4101), or **1 – 36** (4104). *label text* is the displayed entry name, 19 characters max. (7810 series), 13 characters max. (4101), or 5 characters max. (4104). *string* is the dial digit/character string, 128 characters max. **{pause}** inserts a pause into the dial string. # at the end of the dial string dials the number immediately.

Login/Logout

This section defines Login/Logout controls.

Call Directory Entries	
XML Tag	**Data / Description**
<**login_logout_enable>** *ON/OFF* </ **login_logout_enable**>	Determines whether the 7810 model phone displays the LOGIN/LOGOUT softkey when idle. **ON** – display the LOGIN/LGOUT softkey when idle **OFF** – do not display the LOGIN/LGOUT softkey when idle *(default)*
<**default_logout_line**> default logout line ID </**default_logout_line**>	The default logout line ID. When a user logs out, the phone will un-register the “logged in” SIP line and re-register to this default “logged out” SIP line ID.
<**default_logout_password**> default logout password </**default_logout_password**>	The default logout SIP password. When a user logs out, the phone will use this SIP password to re-register to the default “logged out” line.

Security Guidelines

To ensure secure communications and configuration, the phone should have TLS enabled and required certificates installed. The phone should use HTTPS protocol to update its configuration and have TLS and SRTP enabled for voice communications.

In addition, for configuration security, the phone should use the <MAC> XML option for configuring phones. This is the default option in the phone, it restricts which phone hardware can be used for a specific phone number.

The certificates for the HTTPS server and SIP proxy server need to be included in a file which is downloaded from the configuration server. The XML option for the "filename" is shown below.

Secure/Encrypted Server Communications

Enabling Secure Real-time Transport Protocol (SRTP)

SRTP encrypts voice communications.

XML Tag	Data / Description
<**srtp_enable**> ON </**srtp_enable**>	SRTP encrypts voice communications.

Enabling Transport Layer Security (TLS) and Setting the Port Number

Use TLS to encrypt signaling to the server.

XML Tag	Data / Description
<**sip_transport**> TLS </**sip_transport**	
<**sip_proxy_port**> 5061 </**sip_proxy_port**>	5061 is the default port number for TLS.
<**sip_reg_port**> 5061 </**sip_reg_port**>	
<**phone_port**> 5061 </**phone_port**>	

Using Online Certificate Status Protocol (OSCP) to Verify Certificates

OSCP is an optional method of further checking the validity of the certificate sent by the server to the phone. It checks online with other servers for certificate revocation status.

XML Tag	Data / Description
<**ocsp_enable**> ON </**ocsp_enable**>	Enables the Online Certificate Service Protocol (OCSP) to check for revoked certificates during a TLS connection between the phone and the SIP Proxy server.
<**ocsp_url**> *URL* </**ocsp_url**>	This setting provides the URL to the OCSP responder and is the –url argument to the OpenSSL OCSP command. Both HTTP and HTTPS URLs can be specified.
<**ocsp_issuer_cert**> *filename* </**ocsp_issuer_cert**>	This .pem file contains the current OSCP issuer certificate; it is located in the same location as the configuration files. *filename* includes the full path specification, and can be up to 250 characters.
<**ocsp_va_cert**> *filename* </**ocsp_va_cert**>	This .pem file contains explicitly-trusted responder certificates. This option must be provided if the certificates are self-signed. This file is located in the same location as the configuration files. *filename* includes the full path specification, and can be up to 250 characters.
<**ocsp_signer_cert**> *filename* </**ocsp_signer_cert**>	Sign the OCSP request using the OCSPD certificate specified in the *oscp_signer_cert* file and the key specified in the *oscp_signer_key* file. If neither option is present, then the OCSP request is not signed. These files are located in the same location as the configuration files. *filename* includes the full path specification, and can be up to 250 characters.
<**ocsp_signer_key**> *filename* </**ocsp_signer_key**>	

Phone Certificate and Private Key

XML Tag	Data / Description
<**cert_private_phone**> *filename* </**cert_private_phone**>	This .pem file contains the certificate and private key for the phone. The server must have the certificate and public key in order to validate the phone. *filename* includes the full path specification, and can be up to 250 characters.
<**cert_trusted_ca_list**> *filename* </**cert_trusted_ca_list**>	This .pem file contains a list of trusted certificate authorities. *filename* includes the full path specification, and can be up to 250 characters.
<**tls_require_cert**> ON </**tls_require_cert**>	Determines whether a valid certificate is required for a TLS connection. If set to OFF, the phone will accept any certificate from the server as valid. When attempting to establish a new TLS connection, it is often helpful to set this parameter to OFF so that the validity of the certificate is not checked. This allows debugging of the TLS connection independent of the certificate status. Once the TLS connection is working, setting this parameter to ON will then require valid certificates to establish a connection. **Important Note**: This tag must reside in the XML file AFTER the following tags: <cert_private_phone>, <cert_trusted_ca_list>, <ocsp_issuer_cert>, <ocsp_va_cert>, <ocsp_signer_cert> and <ocsp_signer_key>.

Ports Used by Phone

The following ports are used by the phone during normal operation:

Port	Transport	Protocol	Application
53	UDP	DNS	Domain Name System
68	UDP	DHCP	Dynamic Host Configuration Protocol
69	UDP	TFTP	Update Server[1]
80	TCP	HTTP	Update Server[1]
123	UDP	NTP	Time Server
443	TCP	HTTPS	Update Server[1]
514	UDP	Syslog	Syslog Server[2]
5060[3]	UDP/TCP[4]	SIP	SIP signaling
5061[3]	UDP/TCP[4]	SIP	SIP signaling over TLS
16384[5]	UDP	RTP	SIP Media (voice packets)

Notes:

1. If an Update Server is provisioned, a port will be used during configuration and program downloads. The default port value is dependent on the update server protocol (TEO, HTTPS, HTTP, or TFTP) and can be provisioned via DHCP Option 66 or 125. The default port value can be changed to a different value through this mechanism. TEO protocol uses port 443. Refer to page 10.
2. Syslog must be enabled by the <syslog_option> XML tag. Refer to page 35.
3. Port 5060 is used for unencrypted SIP transport; if TLS is enabled, port 5061 is used instead. This default value can be changed via the <phone_port> XML tag. Refer to page 40.
4. SIP transport protocol (UDP/TCP/TLS) is set via the <sip_transport> XML tag. Refer to page 40.
5. The RTP base port, plus the next 4 ports are used for RTP/RTCP. The RTP base port is programmable (*default value = 16384*). If the phone is configured with the default value, ports 16384 through 16388 are used. This default value can be changed via the <phone_rtp_port> XML tag. Refer to page 42.

SIP Server Access

The password for accessing/registering with the SIP server cannot be viewed in the phone, this password is determined by the SIP server programming. Since this is the primary means of controlling access to the server, it should not be a trivial password. It can be set from the configuration file as part of the programming of the line keys using the <*sip_password*> tag which can be up to 128 characters.

For example:

```
<key num=”1”>LINE
    <line_id>
        1234
    </line_id>
    <sip_name>
        ALEXANDER
    </sip_name>
    <sip_auth_id>
        2235551234
    </sip_auth_id>
    <sip_password>
        PasswordNotSecure
    </sip_password>
    <label>
        John Doe
    </label>
</key>
```

Telephone Software Updates

Installing Files on Server

Teo may supply updates to the telephone operating software. All required files are distributed in a .zip archive; extract the files before installing.

The file **TCS7000B.xml** names the compressed application and boot program files to be downloaded to the phones. The file is supplied with the updates.

Teo UC System

Use the built-in update process through the Admin Portal of the Teo UC Server. Phone software update files can be downloaded directly from the Teo UC Server.

TFTP Update Server

Copy the update configuration file and update program files to the TFTP update server folder specified by the <update>, <server_name> tag in the phone's configuration file or in DHCP Option 66 or Option 125.

HTTP / HTTPS Update Server

Copy the update configuration file and update program files to the update server folder specified by the <update>, <server_name> tag in the phone's configuration file or in DHCP Option 66 or Option 125.

Note: If you are hosting the update files on Microsoft Internet Information Services (IIS), you must use Windows IIS Manager to define the following MIME types. Restart IIS for the changes to take effect.

File Extension	MIME Type
.dig	application/octet-stream
.pem	application/x-x509-ca-cert
.bin	application/octet-stream

Digitally Signed Updates

Files for digitally signed updates must be located in a subfolder under the update server folder specified by the <update>, <server_name> tag in the phone's configuration file or in DHCP Option 66 or Option 125. This subfolder name is specified by the <package> tag in the supplied TCS7000B.xml file, for example, "`TEO_04.03.05.54`".

Appendix A
Viewing Packet Statistics

Packet statistics are tabulated on a per call, per call appearance basis, and may be viewed while a call is in progress or after a call is completed. Counts are updated once a second while a call is in progress. Statistics are saved for the most recent call on each call appearance. As soon as a new call (inbound or outbound) is initiated, statistics for the previous call on that call appearance are lost. Expected arrival times for packet delay calculations are based on the arrival time of the first packet in the call; this reference time is re-established on underflow and overflow events.

The last 50 packet statistics are saved in the packet history.

Packet statistics are viewed through the Packet Diagnostics menu (***Setup*** → ADMIN → DIAG → PACKET). Select ACTIVE to view packet statistics for the currently active call, or HISTORY to view the last 50 recorded packet statistics

For the active call, the codec and jitter buffer settings are displayed first; jitter delay is displayed first when viewing the history. Press the Right or Left Arrow keys to view additional statistics.

A packet statistics summary can also be viewed for calls in the call log by selecting DETAIL.

The following statistics are recorded and displayed:

Codec/Jitter Buffer Settings –codec and associated jitter buffer selections for the current call (not shown in the history, but available for the current call and for calls in the call log). These values are negotiated on a per-call basis.

Jitter Delay – current “start of call” average jitter buffer setting (playout delay) for either fixed delay or calculated adaptive delay. The value displayed is based on the jitter buffer settings of the primary line.

Concealed Packets – total number of packets that were concealed during audio playback; also expressed as a percentage of total packets (concealed packets)/(total number of expected packets). This measurement is done at the audio playback point and correlates to audible dropouts in the voice path due to lost packets, packets received but delayed beyond the jitter buffer playback time, or jitter buffer underflow (no packets in the buffer). During packet concealment, the last received packet is replayed at a reduced level to minimize the audio interruption. Silence is played if multiple packets must be concealed.

Lost Packets – total number of expected packets that were not received; also expressed as a percentage of total packets (lost packets)/(total number of expected packets). Lost packets are computed by comparing the expected packet count (based on RTP packet sequence numbers) to the count of actual packets received. Lost packet counts are a result of network performance and cannot be improved by local jitter buffer settings.

Lost packets = (last RTP sequence number - first RTP sequence number) - number of packets received.

Not Delayed – total number of packets received earlier than 10ms after the expected arrival time; also expressed as a percentage of total packets (not delayed packets)/(total number of expected packets). These are normal packets that have average transmission delay, but with minimal jitter delay or packets that arrive early.

Delayed packets may or may not be played, depending on jitter buffer settings.

Delayed >10ms – total number of packets received later than 10ms after the expected arrival time; also expressed as a percentage of total delayed packets (>10ms packets)/(total number of expected packets).

Delayed >20ms – total number of packets received later than 20ms after the expected arrival time; also expressed as a percentage of total delayed packets (>20ms packets)/(total number of expected packets).

Delayed >30ms – total number of packets received later than 30ms after the expected arrival time; also expressed as a percentage of total delayed packets (>30ms packets)/(total number of expected packets).

Delayed >40ms – total number of packets received later than 40ms after the expected arrival time; also expressed as a percentage of total delayed packets (>40ms packets)/(total number of expected packets).

Delayed >50ms – total number of packets received later than 50ms after the expected arrival time; also expressed as a percentage of total delayed packets (>50ms packets)/(total number of expected packets).

Delayed >60ms – total number of packets received later than 60ms after the expected arrival time; also expressed as a percentage of total delayed packets (>60ms packets)/(total number of expected packets).

Delayed >70ms – total number of packets received later than 70ms after the expected arrival time; also expressed as a percentage of total delayed packets (>70ms packets)/(total number of expected packets).

Delayed >80ms – total number of packets received later than 80ms after the expected arrival time; also expressed as a percentage of total delayed packets (>80ms packets)/(total number of expected packets).

Underflow Events – total number of jitter buffer underflow events. An underflow occurs when the jitter buffer “runs dry”, usually due to an interruption in the packet stream. This causes an audible dropout in the audio playback until enough additional packets are received to fill the jitter buffer to the average value setting.

Overflow Events – total number of jitter buffer overflow events. An overflow sometimes occurs when a burst of packets arrives that exceeds the capacity of the jitter buffer. In this instance, the most recent packets are retained and the earliest packets in the jitter buffer are dropped to make room. This causes an audible “skip” in the audio playback to restore the jitter buffer contents to the average value setting. In some cases, an overflow event may follow an underflow event if a group of packets experience unusual burst delay. An overflow event can also occur on a long-duration call, due to slight differences in packet rates between sender and receiver.

Total Packets – total number of expected packets in the call, based on RTP sequence numbers (last received RTP packet sequence number) – (first received RTP packet sequence number). This number may be higher than the actual number of packets played during a call, since it also includes lost packets and underflow packets.

Appendix B
Dial Plan Syntax

The complete BNF syntax that defines the structure for the dial plan is as follows:

```
<dial_plan> ::= <component>*
<component> ::= <prefix-operation> <dial-pattern> <suffix-operation>
<prefix-operation> ::= "{" <subst-pattern-element>* "|" <dial-character>* "}"
<subst-pattern-element> ::= <dial-character> | <wildcard> | <bracket-expression>
<dial-pattern> ::= <dial-pattern-element>+ [<dial-pattern-terminator>]
<dial-pattern-element> ::= <dial-character> | <wildcard> | <bracket-expression>
                           | <secondary-dialtone-marker>
<dial-pattern-terminator> ::= <initiate-call-marker> | <block-access-marker>
<suffix-operation> ::= "{" <subst-pattern-element>* "|"<dial-character>* [<meta-operation>] "}"
<meta-operation> ::= <meta-operation-marker> <meta-operation-identifiers>
<meta-operation-marker> ::= "`"
<meta-operation-identifiers> ::= <meta-operation-identifier> ["," <meta-operation-identifier>]
<meta-operation-identifier> ::= <priority-id> | <rph-id> | <cal-id>
<priority-id> ::= "P" <priority-index>
<rph-id> ::= "R" <priority-index>
<priority-index> ::= (0 to 49)
<cal-id> ::= "CF" <access-level> | "CV" <access-level>
<access-level> ::= (0 to 99)
<dial-character> ::= <numeric> | <upper-case-alpha> | <lower-case-alpha> | <dial-symbol>
<wildcard> ::= "^"
<bracket-expression> ::= "[" <bracket-element> { "," < bracket-element > } "]"
<bracket-element> ::= <dial-character> | <dial-range>
<dial-range> ::= <dial-character> "-" <dial-character>
<secondary-dialtone-marker> ::= "`"
<initiate-call-marker> ::= "#"
<block-access-marker> ::= "!"
```

A null <dial_plan> does not affect user dialing in any way.

Dial plan components are evaluated from left-to-right until a dial pattern within a component is recognized or the last component is processed. Each <component> specifies a <prefix-operation>, a <dial-pattern>, and a <suffix-operation>. Note that <dial-character> is limited to the following ASCII characters:

```
A-Z  a-z  0-9  . @ _ - / \, : ; * ' " ( ) < > ~ + = ? ! $ % &
(space)
```

The <dial-pattern> may contain any sequence of <dial-character>, <wildcard>, <bracket-expression>, or <secondary-dialtone-marker>, and it may end with a single <initiate-call marker> or <block-access-marker>. The <secondary-dialtone-marker> within the <dial-pattern> directs the phone to generate secondary dial tone, if the current dialed string entry matches the <dial-pattern> sub-string preceding the marker. An <initiate-call-marker> at the end of the <dial-pattern> directs the phone to automatically initiate a call, if the current dialed string entry matches the <dial-pattern> preceding the marker. A <block-access-marker> at the end of the <dial-pattern> directs the phone to immediately cancel the outbound call with reorder tone, if the current dialed string entry matches the <dial-pattern> preceding the marker.

Prefix and suffix operations are applied at the time of call initiation, and only if the <dial-pattern> matches the dialed string entry.

If the leading characters of the dialed string entry matches the prefix pattern preceding the "|", then the leading characters of the dialed string entry are replaced by the substring following the "|". If the prefix pattern preceding the "|" is null, then the substring following the "|" are inserted at the beginning of the dialed string entry. If the substring following the "|" is null, then the leading characters of the dialed string entry are deleted.

If the trailing characters of the dialed string entry match the suffix pattern preceding the "|", then the trailing characters of the dialed string entry are replaced by the substring following the "|" and preceding any <meta-operation>. If the suffix pattern preceding the "|" is null, then the substring following the "|" and preceding any <meta-operation> are inserted at the end of the dialed string entry. If the substring following the "|" and preceding any <meta-operation> is null, then the trailing characters of the dialed string entry are deleted.

Meta Operations

Meta operations construct message headers that meet MLPP requirements.

The <meta-operation> includes the following combinations:

- <priority-id>
- <rph-id>
- <cal-id>
- <priority-id>, <cal-id>
- <rph-id>, <cal-id>

If the <suffix-operation> includes a <priority-id>, then the phone displays the r-priority identified by the second digit of the dialed string entry. If the <suffix-operation> includes an <rph-id>, then the phone displays the r-priority and includes a Resource Priority Header (RPH) in the outgoing INVITE. The RPH includes the network domain identified by the <priority-index> and the r-priority identified by the second digit of the dialed string entry. If the <suffix-operation> includes a <cal-mode-id>, then the phone includes a Confidential Access Level (CAL) header in the outgoing INVITE. The CAL header includes the mode identified by the <cal-mode-id> and the access level identified by the <access-level>.

<priority-index> is used to select a namespace associated with <priority-id> and <rph-id>. Predefined namespaces are selected with the following <priority-index> values:

- 0 selects the "dsn" namespace
- 1 selects the "q735" namespace
- 2 selects the "uc" namespace

Appendix C
Troubleshooting

Teo IP telephones have built-in diagnostic and testing capabilities to quickly isolate problems affecting their operation.

Power-up & Connection Troubleshooting

Whenever power is applied or a connection is made to the LAN or WAN, the phone initiates a startup routine, with progress shown in the display. When the phone and network are fully initialized, the idle display, indicating date and time, will be shown. In cases where full initialization is not attained, the following displays or conditions will be shown continuously until corrected.

Problem Observed	Remedial Action
No display information is shown	Check power connections and source.
NO ETHERNET CONNECTION	Check connections to the LAN or WAN.
CHECKING DHCP.., DISABLE	Verify that the DHCP server is operating and accessible. If the LAN or WAN does not include a DHCP server, select DISABLE to disable IP configuration via DHCP and enter the appropriate IP values (phone IP address, default gateway, subnet mask, update server address) when prompted.
IP4 ADDR=000.000.000.000 EDIT	The phone IP address is a null value. Enter the appropriate phone IP address or name.
GATEWAY= EDIT	The default gateway IP address is a null value. Enter the appropriate gateway IP address or server name.
SUBNET=000.000.000.000 EDIT	The subnet mask is a null value. Enter the appropriate subnet mask.
SELECT UPDATE SERVER TEO TFTP HTTP HTTPS	Select the appropriate type of update server, or NONE if the phone will be manually configured.
UPDATE= DELETE CLEAR 123	The update server IP address is a null value. Enter the appropriate update server IP address or server name.
LINE ID= DELETE CLEAR 123	The Line ID is a null value. Enter the appropriate Line ID number.
AUTH PSWD= DELETE CLEAR 123	The AUTH PSWD (password) is a null value. Enter the appropriate AUTH password.
PROXY= DELETE CLEAR 123	The Proxy server address is a null value. Enter the appropriate Proxy server IP address or server name.

Problem Observed	Remedial Action
REGISTERING LINES	The primary line has not registered with the SIP server. Verify all entries (LINE ID, AUTH ID, AUTH Password, all IP addresses and subnet mask) and re-enter as required.
REGISTERING LINES CONTINUE	The primary line has registered with the SIP server; however, additional lines have not. Verify the LINE ID, AUTH ID and AUTH passwords for all additional lines and re-enter as required.
RESTART WITH NEW VALUES? YES NO	Certain critical values have changed and a restart is required. Select YES unless you need to change some other settings.
DHCPV4 ERROR…RETRYING DISABLE ENBL-8021X	Verify the DHCP server is operating and accessible. If so, you may need to enable 802.1x to gain access to the network. Also check the current VLAN settings at the phone using the INSTL→NET→VLAN→ACTIVE menu. If incorrect, adjust the VLAN Discovery Mode or manual settings accordingly.
PING4 FAILED PRESS ANY KEY TO EXIT	If attempts to ping other IP addresses fail, check the current VLAN settings at the phone using the INSTL→NET→VLAN→ACTIVE menu. If incorrect, adjust the VLAN Discovery Mode or manual settings accordingly. Ping valid addresses using the ADMIN→DIAG→PING Menu.

Call Control Troubleshooting

After the phone is fully initialized (idle display showing), the following call control anomalies may be encountered.

Problem Observed	Remedial Action
All lines indicate the arrival of inbound calls via the key indicators; however, the phone does not ring for some of them.	Verify that the affected lines are not set for NEVER or an extended WAIT interval, using the USER→RING→CONTROL Menu. If this behavior is not desired, change the value of the attribute to “ALWAYS” where applicable.
All lines indicate the arrival of inbound calls via the key indicators; however, the phone never rings.	Verify that “RINGER OFF” is not showing in the display. If it is, use the Volume Up key to set the ringer level to a value higher than OFF.

Diagnostic Troubleshooting

After the phone is fully initialized (idle display showing), the following diagnostic information may be reviewed, using the ADMIN→DIAG Menu.

Diagnostic Mode	Information Provided
LINK option selected:	The LINK option provides information about the network and SIP server status as follows: 1) Status about the network will be displayed: PHY:100MBPS IP:AUTO OK (*DHCP used for IP addressing at phone*) *or* PHY:100MBPS IP:NO AUTO (*DHCP is enabled, and has not completed successfully*) *or* PHY:100MBPS IP:STATIC (*DHCP is disabled, fixed IP addresses are in use at phone*) 2) Registration status for each line will be indicated via line status LED for 2 seconds. Solid Green – Line registration successful with server. Alternating red/green – Line registration in process and un-determinate. Solid Red – Line registration failed. Flashing red – The primary line is active, and secondary line(s) are not registered.
PACKET option selected: and then ACTIVE option selected:	The PACKET option allows the selection of statistics for the current active call (ACTIVE) or a standing aggregate of previous calls (HISTORY). Status indicating the negotiated codec, the received packetization rate and the real-time jitter buffer setting is displayed for the current call as below: G.711/30ms JTR=XX/YYYms¤ ACTIVE CALL Selecting the Right Arrow key in succession will indicate additional status information as below: Total of concealed packets Total of un-received (lost) packets Total of not-delayed (within 10ms) packets Total of delayed (in excess of 10ms) packets Total of delayed (in excess of 20ms) packets

Diagnostic Mode	Information Provided
or HISTORY option selected:	Total of delayed (in excess of 30ms) packets Total of delayed (in excess of 40ms) packets Total of delayed (in excess of 50ms) packets Total of delayed (in excess of 60ms) packets Total of delayed (in excess of 70ms) packets Total of delayed (in excess of 80ms) packets Total of jitter buffer underflow events Total of jitter buffer overflow events Total of expected packets Status for the current “start of call” average jitter buffer setting for either fixed or calculated, adaptive delay for the primary line. JITTER DELAY=XXms ¤ HISTORY Selecting the Right Arrow key in succession will indicate additional status information as below: Total of conceal packets Total of unreceived (lost) packets Total of not-delayed (within 10ms) packets Total of delayed (in excess of 10ms) packets Total of delayed (in excess of 20ms) packets Total of delayed (in excess of 30ms) packets Total of delayed (in excess of 40ms) packets Total of delayed (in excess of 50ms) packets Total of delayed (in excess of 60ms) packets Total of delayed (in excess of 70ms) packets Total of delayed (in excess of 80ms) packets Total of jitter buffer under-flow events Total of jitter buffer over-flow events Total of expected packets

Diagnostic Mode	Information Provided
PING option selected:	The PING option provides the means for measuring single packet network delays. The following IP addresses may be "pinged": PHONE GATEWAY UPDATE SERVER SIP PROXY SERVER NTP SERVER DHCP SERVER SIP REGISTRAR SERVER OTHER* **A valid address must also be entered.* There are three outcomes as the result of a ping: IP ADDRESS NOT SET *In this case enter the appropriate IP address, using the INSTL/IP Menu.* *or* PING4 FAILED PRESS ANY KEY TO CONTINUE *In this case, check Layer 2 802.1Q and other network settings.* *or* PING4 SUCCESSFUL PRESS ANY KEY TO CONTINUE

Contacting Technical Support

If you need assistance configuring your VoIP phones, contact Teo Customer Technical Support.

Teo Technologies, Inc.
Technical Support Department
11609 49th Place West
Mukilteo, WA 98275-4255 USA

Phone: (425) 349-1000
(800) 524-0024
Fax: (425) 349-1010
E-mail: helpdesk@teotech.com
Web: www.teotech.com

Teo is committed to meeting the product needs of our customers. Please write or call us with any suggestions for improvement.

Appendix D
XML Tag Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W