Provision Class of Service (CoS) (Optional)

CoS is an optional provisioning choice that defines the permissions available to a system user for making voice calls. Voice CoS permissions include the type of calls and actions a user can perform.

The default CoS, called DEFAULT_COS, grants permission to place all types of calls is automatically assigned to all voice users.

Creating further CoS entries is only necessary if restrictions are to placed on types of calls the voice user can make.

To create or edit a CoS, complete the following:

1. Access the Voice CoS Command prompt.

   Use the voice class-of-service WORD command to activate the Voice CoS Command Set. Substitute WORD with an alphanumeric string used to identify this CoS. If a CoS with this identifier does not already exist, a new one is created.

   `TA300(config)#`**`voice class-of-service WORD`**

2. If required, apply any necessary calling restrictions.

   All types are enabled by default, so only "no" commands need be entered into a new CoS entity (to deny permission to that call type). Almost all dial plan types are accepted: 900-number, internal, international, local, national, operator-assisted, specify-carrier, toll-free, user1, user2 and user3. Dial plan type always-permitted cannot be denied. In addition, the [no] call-privilege all command can be used to turn on (or off) all permissions at once.

   `TA300(config-cos name)#`**`[no] call-privilege <type>`**

3. Return to the Global Configuration prompt.

   `TA300(config-cos name)#`**`exit`**

4. Access the Voice User Command prompt.

   Substitute NUMBER:20 with a number less than 20 digits long used to identify this user. Generally, the user's phone number is entered here, but it is not necessary. If a User with this identifier does not already exist, a new one is created.

   `TA300(config)#`**`voice user <number>`**

5. Connect the voice user to the new class of service.

   Substitute WORD with the alphanumeric string used to identify the voice class-of-service entity created in step 1.

   `TA300(config-user name)#`**`cos <name>`**

6. Return to the Global Configuration prompt.

   `TA300(config-user name)#`**`exit`**

   Repeat steps 4 - 6 for all voice users to whom the calling restrictions apply.

What's Next

Continue to "Provision for Global Voice (Optional)" on page 1-72.

Provision for Global Voice (Optional)

Global provisioning options are available to set the ONT to perform certain operations, like three-way conferencing, locally.

It is not necessary to change any of these settings if the SIP server is capable of performing them.

To provision the global voice options, complete the following:

1. Set the flashhook mode.

   This command determines if flashhook events will be interpreted locally or will be forwarded to the far end.

   TA300(config)#**voice flashhook mode [interpreted|transparent]**

2. If the flashhook mode is set to interpreted, set the voice conference mode.

   This command determines if voice conferencing bridging will be handled within the unit or from a far-end conferencing server.

   TA300(config)#**voice conference mode [local|network]**

3. If the voice conference mode is set to local, specify the actions performed if the conference originator issues a flashhook once the conference has been established.

   The following options are available:

   - The drop option specifies that the last party added to the 3-way conference will be dropped and the call will continue between the two remaining parties.
   - The ignore option specifies that the flashhook will be ignored. The 3-way conference will continue without interruption.
   - The split option specifies that the 3-way conference will be split into two calls, one between the originator and the first party and one between the originator and second party. When additional flashhooks are issued after the split, they will toggle the originator between the two calls.

   TA300(config)#**voice conference local originator flashhook [drop|ignore|split]**

4. Configure a global starting User Datagram Protocol (UDP) port for Realtime Transport Protocol (RDP).

   Each Access Module in the shelf will use the same starting UDP port. The default port is 10000.

   TA300(config)#**ip rtp udp <1026-60000>**

What's Next

Continue to "Provision the Voice User" on page 1-73.

Provision the Voice User

The user provisioning process is repeated for each individual customer and is typically as automated as possible. Except for the SIP identity which is unique in the system or network. Each user must be associated with a particular FXS port and registered to a specific SIP trunk.

To provision a user to a particular FXS port and registered to a specific SIP trunk, complete the following:

1. Access the Voice User Command prompt.

   Substitute NUMBER:20 with a number less than 20 digits long used to identify this user. Generally, the user's phone number is entered here, but it is not necessary. If a User with this identifier does not already exist, a new one is created.

   ```
   TA300(config)#voice user <NUMBER>
   ```

2. Specify the physical port on the selected access module which the user is associated.

   ```
   TA300(config-user name)#connect fxs 2/<port>
   ```

3. Set the SIP identity.

   The WORD parameter should match the SIP Identity in the SIP call-router. Also a common practice to use the customer's phone number here. It is not necessary, however, and the SIP Identity can be any string that does not contain the following characters: `@^[]{}\|:<>?" and <space>. The <Txx> parameter identifies the trunk that this user should use to contact the SIP server.

   The auth-name and password parameters are optional.

   ```
   TA300(config-user name)#sip-identity <station> <Txx> register auth-name
   <username> password <password>
   ```

4. Return to the Global Configuration prompt.

   ```
   TA300(config-user name)#exit
   ```

What's Next

For Non-OMCI SIP, this completes provisioning. Services should be up and running. To provision another service, continue to "Step 2: Service Provisioning" on page 1-18.

Provision the Media Profile (Optional)

The media profile is created in the Total Access 5000 to provision the Realtime Transport Protocol (RTP) parameters on the access module/remote device.

1. Access the Media Profile Command Set.

   TA5K(config)#**voice profile media WORD**

2. Provision the media profile options.

   Refer to Table 1-30 for a list of media profile options.

Table 1-30. Media Profile Options

Command	Description
`TA5K(config-media-profile name)#`**`rtp frame-packetization [10|20|30]`**	Use this command to configure the RTP frame packetization time in milliseconds.
`TA5K(config-media-profile name)#`**`rtp packet-delay nominal <0-240>`**	Use this command to set the allowable limits of latency on the network. This sets the nominal delay time value in increments of 10 milliseconds.
`TA5K(config-media-profile name)#`**`rtp packet-delay maximum <40-320>`**	Use this command to set the allowable limits of latency on the network. This sets the maximum delay time value in increments of 10 milliseconds.
`TA5K(config-media-profile name)#`**`rtp dtmf-relay enable`**	Use this command to configure the method by which RTP dial tone multi-frequency (DTMF) events are relayed.
`TA5K(config-media-profile name)#`**`rtp qos dscp <0-63>`**	Use this command to configure the maximum RTP quality of service (QoS) parameters for differentiated services code point (DSCP).
`TA5K(config-media-profile name)#`**`rtp local-port [<1026-60000>|RANGE]`**	Use this command to configure the starting RTP UDP port used to source RTP from the ONT.
`TA5K(config-media-profile name)#`**`fax mode modem-passthrough`**	Use this command to switch to passthrough mode on fax or modem tone detection. This command allows modem and fax calls to maintain a connection without altering the signals with the voice improvement settings.

Table 1-30. Media Profile Options (Continued)

Command	Description
TA5K(config-media-profile name)#**echo cancellation enable**	Use this command to improve voice quality for packetized-based voice calls.
TA5K(config-media-profile name)#**flashhook threshold [<40-1550>|RANGE]**	Use this command to configure the minimum and maximum time the switch hook must be held to be interpreted as a flash.
TA5K(config-media-profile name)#**voice-activity-detection enable**	Use this command to enable voice activity detection. When enabled, RTP packets will not be sent during periods of silence.

What's Next

Continue to "Provision the CODEC Profile (Optional)" on page 1-77

Provision the CODEC Profile (Optional)

CODECs are used to convert an analog voice signal to digitally encoded version. Codecs vary in the sound quality, the bandwidth required, the computational requirements, etc.

1. Access the CODEC Profile Command Set.

   TA5K(config)#**voice profile codec-list WORD**

2. Provision the CODEC profile options.

   Refer to Table 1-31 for a list of CODEC options.

Table 1-31. CODEC Profile Options

Command	Description
TA5K(config-codec-list-profile name)#**preference <1-3> codec [g711alaw|g711ulaw|g722|g729]**	Use this command to specify the order of preference for coder-decoders used by the CODEC list.

What's Next

Continue to "Provision the Call Feature Profile (Optional)" on page 1-78.

Provision the Call Feature Profile (Optional)

Call feature options are available to set the access module/remote device to perform certain operations, like three-way conferencing, locally. It is not necessary to change any of these settings if the SIP server is capable of performing them.

1. Access the Call Feature Command Set.

   `TA5K(config)#`**`voice profile call-feature WORD`**

2. Provision the call feature profile options.

   Refer to Table 1-32 for a list of call feature options.

Table 1-32. Call Feature Profile Options

Command	Description
TA5K(config-call-feature name)#**feature-mode network**	Use this command to determine if voice conferencing bridging will be handled within the unit or from a far-end conferencing server.
TA5K(config-call-feature name)#**conference local originator flashhook [drop|ignore|split]**	Use this command if the voice conference mode is set to local, specify the actions performed if the conference originator issues a flashhook once the conference has been established. The following options are available: ■ The drop option specifies that the last party added to the 3-way conference will be dropped and the call will continue between the two remaining parties. ■ The ignore option specifies that the flashhook will be ignored. The 3-way conference will continue without interruption. ■ The split option specifies that the 3-way conference will be split into two calls, one between the originator and the first party and one between the originator and second party. When additional flashhooks are issued after the split, they will toggle the originator between the two calls.
TA5K(config-call-feature name)#**timeouts alerting <0-60>**	Use this command to specify the maximum time a call is allowed to remain in the alerting state. The shorter of this timeout or the configured maximum number of rings will determine how long a call is allowed to ring.
TA5K(config-call-feature name)#**timeouts interdigit <1-16>**	Use this command to specify the maximum time allowed between dialed digits.
TA5K(config-call-feature name)#**transfer-on-hangup enable**	Use this command to enable transfer on hangup. When transferring a call, hanging up initiates the transfer to the destination party.
TA5K(config-call-feature name)#**call-waiting enable**	Use this command to enable call waiting on the subscriber port.
TA5K(config-call-feature name)#**caller-id-inbound enable**	Use this command to allow inbound caller ID to this endpoint.
TA5K(config-call-feature name)#**caller-id-outband enable**	Use this command to allow outband caller ID from this endpoint.
TA5K(config-call-feature name)#**conference [enable|local]**	Use this command to allow the initiation of three-way conference calls. This feature allows multiple parties to communicate at the same time on the same line.

Table 1-32. Call Feature Profile Options (Continued)

Command	Description
`TA5K(config-call-feature name)#`**`emergency-number onhook [inhibit|allow]`**	Use this command to determine if an Emergency call will be dropped or remain open when the call originator goes on-hook. The following options are available: ■ If set to allow, the call will be dropped if the call originator hangs up. This is the default mode. ■ If set to inhibit, the call will remain open until the Emergency Operator terminates the call. While the call is held-up, the local phone will ring and the Emergency Operator will hear a ringback tone.
`TA5K(config-call-feature name)#`**`emergency-number ringing-timeout <1-60>`**	Use this command to set the maximum duration, in minutes, an inhibited call may remain open by an Emergency Operator.

What's Next

Continue to "Provision the OMCI SIP Users" on page 1-81.

Provision the OMCI SIP Users

All profiles (media, CODEC, call-feature, etc.) can be shared across multiple voice users. To create a SIP user, complete the following steps:

1. Access the SIP Voice User Command Set.

   TA5K(config)#**voice user sip <ont-id/0/[1-16]>@<shelf/slot/port>**

2. Assign a description for the voice user.

   TA5K(config-voice-user-sip x/x/x@x/x/x)#**description WORD**

3. Connect the voice user to one or more profiles.

   Refer to Table 1-33 for a list of connection options.

Table 1-33. SIP Voice User Options

Profile	Command
CODEC	TA5K(config-voice-user-sip x/x/x@x/x/x)#**connect profile codec-list WORD**
Dialing	TA5K(config-voice-user-sip x/x/x@x/x/x)#**connect profile dialing WORD**
Call Feature	TA5K(config-voice-user-sip x/x/x@x/x/x)#**connect profile call-feature WORD**
Media	TA5K(config-voice-user-sip x/x/x@x/x/x)#**connect profile media WORD**

4. Connect the SIP voice user to the FXS port.

   TA5K(config-voice-user-sip x/x/x@x/x/x)#**connect fxs <ont-id/0/fxs_Port>@<shelf/slot/port>**

5. Assign an identity (phone number) for the SIP voice user.

   TA5K(config-voice-user-sip x/x/x@x/x/x)#**identity <value>**

6. Specify the SIP trunk through which to register the server. The trunk is specified in the format Txx.

   TA5K(config-voice-user-sip x/x/x@x/x/x)#**sip-trunk Txx**

7. Set the user name that will be required as authentication for registration to the SIP server.

   TA5K(config-voice-user-sip x/x/x@x/x/x)#**auth-name <value>**

8. Set the password that will be required as authentication for registration to the SIP server.

   TA5K(config-voice-user-sip x/x/x@x/x/x)#**password <value>**

9. Enable the SIP voice user.

   TA5K(config-voice-user-sip x/x/x@x/x/x)#**no shutdown**

10. Verify the parameters of the SIP user.

    If mandatory parameters are missing, there is conflicting configuration, or the ONT returns an error while provisioning, last error string displays the appropriate cause of error and puts the voice user in operationally down state. For example if no FXS port is connected to a SIP voice user, it operationally goes down and displays informative message in last error.

```
TA5K(config-voice-user-sip x/x/x@x/x/x)#do show voice user sip <RD_ID/
0/[1-16]@<shelf/slot/port>
```

```
voice user sip 1/0/1@1/16/1 is IS and DOWN
  Description                : 
  Subscriber Identity        : 3012001635
  Fxs Connection             : 1/0/10@1/16/1
  Registration State         : Init
  Codec in Use               : na
  Session                    : Idle
  Last error                 : Voice user not connected to valid FXS port
```

11. Check the status of all SIP voice users running on a card.

```
TA5K(config-voice-user-sip x/x/x@x/x/x)#do show table voice user sip
<shelf/slot/port>
```

```
Subscriber    End-point      Admin   Oper    Registration
Identity      Index          State   State      State         Session
----------    -----------    ------  ------   --------      --------
3012001635     1/0/1@1/16/1    IS      DOWN        na            na
```

What's Next

- For OMCI SIP, this completes provisioning. Services should be up and running. To provision another service, continue to "Step 2: Service Provisioning" on page 1-18.
- To provision for shapers, continue to Appendix C, "Traffic Management"

Provision OMCI MGCP Endpoints

To create the MGCP endpoints, complete the following:

1. Access the Voice User Command Set.

   ```
   ChassisID(config)#voice user mgcp <ont-id/0/[1-16]>@<shelf/slot/port>
   ```

2. Specify the physical port on the selected Access Module to which the user is associated.

   ```
   ChassisID(config-voice user-mgcp x/x/x@x/x/x)#connect fxs <ont-id/0/
   fxs-port>@<shelf/slot/port>
   ```

3. Connect the MGCP voice user to the MGCP profile.

   ```
   ChassisID(config-voice user-mgcp x/x/x@x/x/x)#connect profile mgcp WORD
   ```

4. Enable the VOIP user.

   ```
   ChassisID(config-voice user-sip x/x/x@x/x/x)#no shutdown
   ```

5. Return to the Global Configuration Command Set.

   ```
   ChassisID(config-voice user-sip x/x/x@x/x/x)#exit
   ```

What’s Next

For OMCI MGCP, this completes provisioning. Services should be up and running. To provision another service, continue to “Step 2: Service Provisioning” on page 1-18.

Provision GR-303

To provision for GR-303, complete the following steps:

NOTE

GR-303 is a function of the DS1 Voice Gateway Access Module.

1. Access the Global Configuration Command Set.

   ChassisID#**configure terminal**

2. Access the GR-303 Interface Configuration Command Set.

   ChassisID(config)#**interface gr303-group <shelf/slot/group>**

3. Assign a name to the interface group.

   ChassisID(config-gr303-group x/x/x)#**description LINE**

4. Set the switch-type.

   ChassisID(config-gr303-group x/x/x)#**switch-type [gte-gtd5|lucent-5ess|metaswitch|nortel-dms|siemens-ewsd]**

5. Assign the required physical ports being used as the primary, secondary, and any other GR-303 links.

   a. Set the physical port being used as the primary GR-303 link.

      ChassisID(config-gr303-group x/x/x)#**connect interface t1 <shelf/slot/port> primary**

   b. Set the physical port being used as the secondary GR-303 link.

      ChassisID(config-gr303-group x/x/x)#**connect interface t1 <shelf/slot/port> secondary**

   c. Set the physical port being used as the normal GR-303 link.

      ChassisID(config-gr303-group x/x/x)#**connect interface t1 <shelf/slot/port> normal <3-28>**

   d. Repeat step c to assign the next GR-303 link.

NOTE

The ordering is important. The port of the voice switch and port of the DS1 Voice Gateway assigned to the same GR-303 link must be physically connected.

6. Connect the Call Reference Value (CRV) to the FXS interface.

   ChassisID(config-gr303-group x/x/x)#**connect interface crv <1-2048> interface fxs <1/0/fxs port>@<shelf/slot/port>.gigabit-ethernet**

7. Return to the Global Configuration Command Set.

```
ChassisID(config-gr303-group x/x/x)#exit
```

What's Next

For GR-303 voice, this completes provisioning. Services should be up and running. To provision another service, continue to "Step 2: Service Provisioning" on page 1-18.

Section 2

Provision GPON, Web

Scope of this Section

This section provides the minimum amount of steps required to provision a GPON module for the FTTP application.

NOTE

The provisioning instructions and examples in this guide represent general use cases; they do not address all provisioning scenarios and operator-specific use cases.

In this Section

This section contains the topics listed in Table 2-1.

Table 2-1. Section 2 Topics

Provisioning

Provisioning is done in two steps. Complete the following steps when deploying an FTTP application using the Web GUI.

- "Step 1: OLT/PON Provisioning"
- "Step 2: Service Provisioning" on page 2-16

Step 1: OLT/PON Provisioning

Before you can begin provisioning services, it is first necessary to enable the OLT and PON along with discovering the ONT you will be provisioning for triple-play.

Enable the OLT Module

For services to flow properly, it is necessary to ensure the OLT module is set to In Service. To enable the OLT module, complete the following steps:

1. Navigate to the OLT Card Provisioning menu.

   Modules > GPON OLT > Provisioning > Card

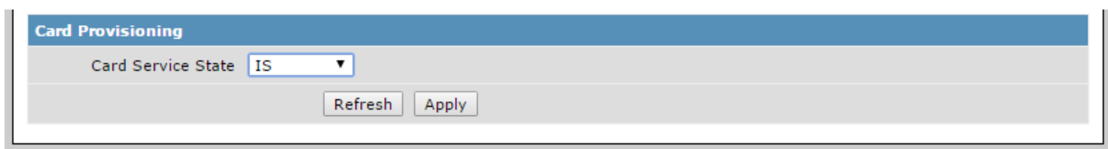


Figure 2-1. OLT Card Service Provisioning

2. Set the card service state to **IS**.
3. Click **Apply**.

Provision the PON

For services to flow properly, it is necessary to ensure the selected PON is set to In Service. It is at this stage that you will also need to choose the Activation Method of the ONT. To enable the PON, complete the following steps:

NOTE

This is a general set of instructions to provision the PON. Optional settings are available. For additional information on these optional settings refer to the applicable documents listed in “Related Online Documentation and Resources” on page Intro-3.

1. Navigate to the OLT PON Provisioning menu.

   Modules > GPON OLT > Provisioning > PON

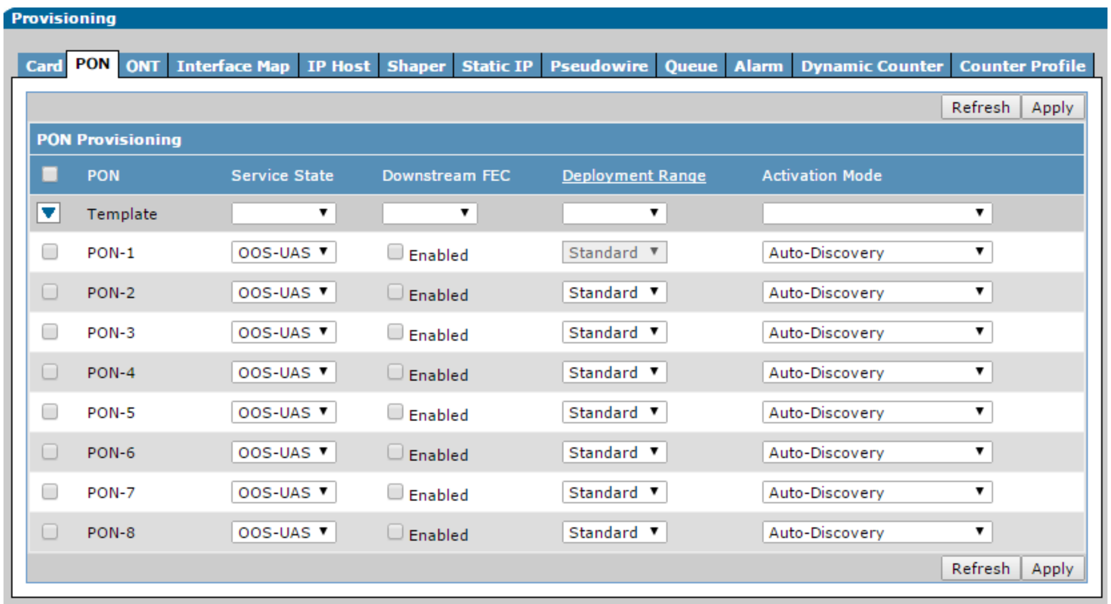


Figure 2-2. PON Provisioning

2. Set the PON Service State to **IS** on the selected PON number.

3. Set the Activation Mode.

NOTE

Notate the Activation Mode for each provisioned PON. This information will be used later when discovering the ONT.

The default mode is Auto-Discovery. For more details about the available modes, refer to Appendix H, “Activation Modes”.

NOTE

- Registration ID, for the ADTRAN 424RG, is performed by Serial Number Activation. This occurs when the ONT is “Discovered” by the OLT.
  If AOE Auto Upgrade is active, a new ONT installation will be detected and a fast blinking FIBER LED will indicate a new software download has commenced. This may take 5 - 10 minutes to complete.
- For the differences on Lock Serial Number and Unlock Serial Number, refer to Appendix H, “Activation Modes”.

4. Select a range indication for the PON.

NOTE

- Standard is the default range.
- For Total Access 5000 System Release 7.1 and above, the GPON 4X SFP OLT (P/N 1187502F1) supports up to 64 ONTs per PON. The GPON 2.5G 2-Port Access Module (P/N 1187500E1) and GPON 2.5G 2X SFP Access Module (P/N 1187501G1) support up to 32 ONTs per PON. For the GPON 4X SFP OLT, the range is reduced by approximately 10km, when the 64 ONT split is used. The GPON OLT 8X SFP (P/N 1187503F1) supports up to 64 ONTs per PON.
- Maximum range is not supported for the GPON OLT 8X SFP (P/N 1187503F1).

Refer to Table 2-2 for range descriptions.

Table 2-2. Range Description

Range	Description
extended	Extended range is 34/37.5km.
maximum	Maximum range is 60km.
standard	Standard range is 20km.

5. Enable or disable FEC for downstream traffic toward the customer ONT.

   FEC helps eliminate packet loss by providing redundancy in the signal. If downstream FEC is enabled, the ONT that supports FEC decoding capability should apply FEC decoding and error-correction to the downstream data flow. The ONT that does not support FEC decoding skips the parity bytes and does not apply FEC decoding and error-correction to the downstream data flow.

NOTE

- FEC decoding does not attempt to correct any transmission errors.
- The activation and deactivation of FEC operates regardless of port status. The behavior during switch-over is undefined and is likely to cause a momentary loss of data.

6. Click **Apply**.

What's Next

- For Registration-ID activation, continue to "Enter the Registration-ID" on page 2-6.
- For all other activation modes, continue to "Discover the ONT" on page 2-15

Enter the Registration-ID

The registration-ID steps vary depending on your ONT. Use Table 2-3 to navigate to your next step.

Table 2-3. Registration-ID

Registration-ID Procedure	See Page
Registration-ID Entry for Total Access 3xx	2-6
Registration-ID Entry for Total Access 421x /Total Access 421xw	2-8
Registration-ID Entry for Total Access 3xx Residential Gateway	2-10
Registration-ID Entry for Total Access 324RG and 334RG	2-12
Registration-ID Entry for Total Access 324 3rd Generation and Total Access 374	2-13
Registration-ID Entry for Total Access 4xx	2-14

Registration-ID Entry for Total Access 3xx

To enter a Registration-ID to the ONT, complete the following steps:

1. Power down the ONT (if powered on).
2. If necessary, disconnect the subscriber POTS wiring.
3. Connect DTMF phone to one of the POTS jacks.
4. Power on the ONT and wait until the unit is ready to accept the Registration-ID. ONT status indications are provided in Table 2-4.

Table 2-4. ONT Status

Status	LED Status
Unit is booting up	Flashing green, then solid yellow
Unit has booted	Off for the initial LED status
Unit is ready to accept the Registration-ID	Flashing red and green quickly

5. Within 10 seconds, pick up phone. A dial tone should be heard.

NOTE

If the Registration-ID is not entered within 300 seconds, hang up and return to step 1.

6. Enter: *001234*XXXXXXXXXX*XXXXXXXXXX* (where XXXXXXXXXX is the Registration-ID for this site).
7. Wait for verification that the ONT understood and accepted the Registration-ID as indicated by the ONT LEDs listed in Table 2-5.

Table 2-5. Registration-ID Acceptance

Status	Description
Success	If verification succeeds, the following attributes apply: ■ LED: Flashing green ■ Tone: Stutter dialtone ■ Caller-ID: **Accepted** and echoing the Registration-ID
Failure	If verification fails, the following attributes apply: ■ LED: Flashing red ■ Tone: Fast busy ■ Caller-ID: If the pattern is entered incorrectly, **Invalid** appears. If the first ID does not match the second, **Re-enter** appears If a failure occurs, hang up and return to step 5.

8. Hang up phone.
9. Wait for validation of the Registration-ID as indicated by the ONT LEDs listed in Table 2-6.

Table 2-6. Registration-ID Status

Status	LED Description
Discovery (validation pending)	Flashing yellow
Success	Solid green
Failure	Solid red
Dark Fiber	Off

10. If success, registration is complete. Disconnect phone & connect house wiring

What's Next

Continue to "Discover the ONT" on page 2-15

Registration-ID Entry for Total Access 421x /Total Access 421xw

To enter a Registration-ID to the SFU ONT (Total Access 421x or Total Access 421xw), complete the following steps:

1. Power down ONT (if powered on), and disconnect the fiber.
2. If necessary, disconnect residence POTS wiring.
3. Connect DTMF phone to one of the POTS jacks.
4. Power on the ONT and wait for the ONT to come up within 2 minutes.
5. Perform a 10 second reset on the ONT by pushing the reset button
6. Wait for the OMCI LED to start flashing.
7. Wait for the OMCI LED to stop flashing, and the SYS LED will come on solid.
8. Once the SYS LED is on solid, wait 40-45 seconds for the POTS LED to start flashing.
9. Take the butt set off-hook. For activating the prompt tone for Registration-ID, dial '*0'. A continuous prompt tone of 450 Hz should be heard.

NOTE

If the Registration-ID is not entered within 300 seconds, hang up and return to step 1.

10. After the prompt tone, dial the Registration-ID value.
    a. Dial the 10 digit number with # at the end to indicate the end of the input string. Digits in the range of 0 to 9 are accepted.
    b. Enter the identical Registration-ID again and press # (as seen in the previous step).
11. If time out tone is played, re-enter the Registration-ID by placing the phone on-hook. Again take the phone off-hook and repeat step 7
12. If Error-tone is played, the input Registration-ID is not accepted. Re-enter the Registration-ID by placing the phone on-hook. Again take the phone off-hook and repeat step 9.
13. If OK tone is played, continuously with small intervals of approximately 2 to 4 seconds, the Registration-ID is accepted. Place the phone on-hook, connect fiber and reboot the ONT.
14. If the Registration-ID entered on the ONT matches the Registration-ID provisioned on the OLT, the ONT will successfully be registered with the OLT. The Network LED on the ONT will be ON at the end of the process. Refer to Table 2-7 on page 2-9 for a list of LEDs.

    If the Registration-ID entered on the ONT does not match the Registration-ID provisioned on the OLT, the SYS LED will keep blinking during the ONT boot-up to indicate the ONT is trying to register itself but cannot complete the process successfully. Refer to Table 2-7 on page 2-9 for a list of LEDs.

Total Access 421x/Total Access 421xw LEDs

The ONT provides front panel LEDs to display status information. The ONT LEDs and status descriptions are shown in Table 2-7.

Table 2-7. Front Panel LEDs

Label	Status	Description
POWER	○ Off	No power
	● Green	Power is On
BATT	○ Off	No battery power
	● Green	Battery installed and charged
	✷ Green Flashing	Battery charging, or operating in depleted condition
SYS	○ Off	Power on, fully functional and ranged and/or synchronized
	● Green	Hardware is 100% operational
	✷ Green Flashing	PON is in ranging and synchronizing mode
	● Red	System failed to boot
Data	○ Off	No data on Ethernet port
	● Green	Data being processed on Ethernet port
NTWK	○ Off	No data being passed
	● Green	Link between Network and ONT established
OMCI	○ Off	Dark Fiber
	● Green	Ranged, Synchronized, and Up on the PON
	✷ Green Flashing	Communicating with OLT and Ranging
POTS 1/2	○ Off	Telephone is on hook
	● Green	At lease one port is Off Hook
	✷ Green Flashing	At least one port off-hook for one-hour or more
Link/ Carrier	○ Off	Ethernet port not active
	● Green	Connection between ONT and CPE router established
	✷ Green Flashing	Traffic on Ethernet port
10/100	○ Off	Ethernet rate up to 10Mbps
	● Green	Ethernet rate up to 100mbps
	✷ Green Flashing	Ethernet rate up to 1000Mbps

What's Next

Continue to "Discover the ONT" on page 2-15

Registration-ID Entry for Total Access 3xx Residential Gateway

There are two methods where the OLT will register the ONT:

- Serial Number Activation (performed by the OLT when the ONT is “Discovered”)
- Registration ID using Telco Butt Set Activation (see below)

Set Registration ID Activation using a Telco Butt Set

To set the Registration ID using a DTMF Keypad on a standard telco Butt Set, complete the following steps:

1. Verify the PON fiber-feed is disconnected from the ONT.
2. Press the **RESET** button on a previously powered-up ONT, or perform an initial power-up on a new ONT.
3. Wait approximately one minute for the start-up to complete, (**PWR** LED is ON and solid; **LOS** LED is ON and solid).
4. Attach the Butt Set to the **POTS** Port 1 and go off-hook.
5. Observe that the reorder tone (fast busy) is generated.

NOTE

The Reorder tone is continuously played after going off-hook until the valid Registration ID password is dialed. See Step 6.

6. On the keypad, dial the registration ID password: **`*123#`**.
7. Observe that the special information tone is generated.

NOTE

This is a fast “Hi-Mid--Low” tone that repeats.

8. On the keypad, press **`*`** to initiate the Registration ID input sequence.
9. Observe that the special information tone stops.
10. Dial the remainder of the Registration ID sequence: **`10 digit`** plus **`#`**.

NOTE

If the Registration ID entered is not valid, the Special Information tone will be re-played. An incorrect Registration ID can be changed by re-entering the Registration ID password (**`*123#`**) and then re-entering a correct Registration ID sequence.

11. Wait 2 seconds. A confirmation tone is generated by the Butt Test Set. This indicates a valid Registration ID was entered.
12. Hang-up the Butt Set.
13. Push the **RESET** button, or power-cycle the ONT.
14. Connect the fiber between the PON and ONT.

15. The ONT should begin Ranging with the new Registration ID. The **PON** LED will blink during Ranging. The **PON** LED will become solid after 20-30 seconds. This indicates the ONT has activated.
16. Once the ONT has Ranged on the PON, the Butt Set Registration ID process is disabled.

NOTE

If AOE Auto Upgrade is active, a new ONT installation will be detected and a fast blinking **PON** LED will indicate a new software download has commenced. This may take 5 - 10 minutes to complete.

What’s Next

Continue to “Discover the ONT” on page 2-15

Registration-ID Entry for Total Access 324RG and 334RG

To set the Registration ID using a DTMF Keypad on a standard telco Butt Set, complete the following steps:

1. Power down ONT (if powered on), and disconnect the fiber.
2. If necessary, disconnect residence POTS wiring.
3. Connect DTMF phone to the first POTS port.
4. Power on the ONT and wait for the ONT to come up. ONT comes up in 25 seconds.
5. Perform 10 sec reset on the ONT by pushing the reset button.
6. Wait 40-45 seconds for the POTS LED to start flashing.
7. Able to get prompt tone even after 300 seconds by dialing '*0'.
8. Take the butt set off-hook. For activating the prompt tone for the Registration-ID, dial '*0'. A continuous prompt tone of 450 Hz should be heard.
9. After the prompt tone, dial the Registration-ID value.
   a. Dial the 10 digit number with # at the end to indicate the end of the input string. Digits in the range of 0 to 9 are accepted.
   b. Enter the identical Registration-ID again and press # (as performed in the previous step).
10. If time out tone is played, re-enter the Registration-ID by placing the phone on-hook. Again take the phone off-hook and repeat step7.
11. If Error-tone is played, the input Registration-ID is not accepted. Re-enter the Registration-ID by placing the phone on-hook. Again take the phone off-hook and repeating step 8.
12. If OK tone is played, continuously with small intervals (approximately 2 to 4 seconds), then Registration-ID is accepted. Place the phone on-hook, connect fiber and reboot the ONT.
13. If the Registration-ID entered on the ONT matches the Registration-ID provisioned on the OLT, the ONT will successfully be registered with the OLT.

What’s Next

Continue to “Discover the ONT” on page 2-15

Registration-ID Entry for Total Access 324 3rd Generation and Total Access 374

1. Verify the ONT is DISCONNECTED from the PON and reset or power-up the unit.
2. Wait approximately 1 minute for start-up to complete. The LEDs will provide the following indications:
   - Total Access 374
     - PWR LED illuminated, solid
     - FAIL LED illuminated, solid
   - Total Access 324 3rd Generation
     - PWR LED illuminated, solid
     - LOS LED illuminated, solid
3. Attach the Butt Set or DTMF phone to POTS port #1 and go off-hook
4. Verify that reorder tone (fast busy) is present.
5. Dial the registration ID entry code - *123#
6. A special information tone will be played to indicate the ONT is ready to accept the registration ID.
7. Enter an asterisk (*), wait for the tone to stop, then enter the 10 digit registration ID, then press on the pound key (#).
8. You should now hear three tones, indicating its ok to hang up the phone/butt set.
9. Reset the ONT, and connect to the PON. Once ONT activation is successful, the MGT, NET, and PWR LEDs should all illuminate green.

Guidelines

Use the following guidelines when provisioning Registration-ID:

- Fast busy is continuously played until the asterisk (*) key is pressed.
- If the registration ID is not valid, the special information tone will be played.
- After entering *123#, the registration ID sequence can be entered (*10-digits#) and changed by re-entering a new registration ID sequence as many times as necessary. The confirmation tone is played each time a valid registration ID sequence is entered.
- Once the ONT is ranged, the registration ID process is disables.

What's Next

Continue to "Discover the ONT" on page 2-15

Registration-ID Entry for Total Access 4xx

> **NOTE**
> This procedure is not applicable to the following Total Access 4xx products: Total Access 421x/421xw and the Total Access 400.

1. Plug in both power and fiber to the ONT and allow the ONT to “range.” This process will take several seconds. The LEDs will indicate that the process is complete.
2. Connect an RJ-45 Ethernet cable from a laptop PC to the Ethernet LAN interface on the 401 ONT. See Figure 1-1 for the location of the LAN interface.
3. Open a web browser on the laptop.
4. Enter the IP address 192.168.1.1 in the address window. A popup window appears that requests user name and password.
5. Enter the use name and password, as follows:
   - User name: **admin**
   - Password: **admin**

   The web GUI screen appears in your web browser (see Figure 1-1).

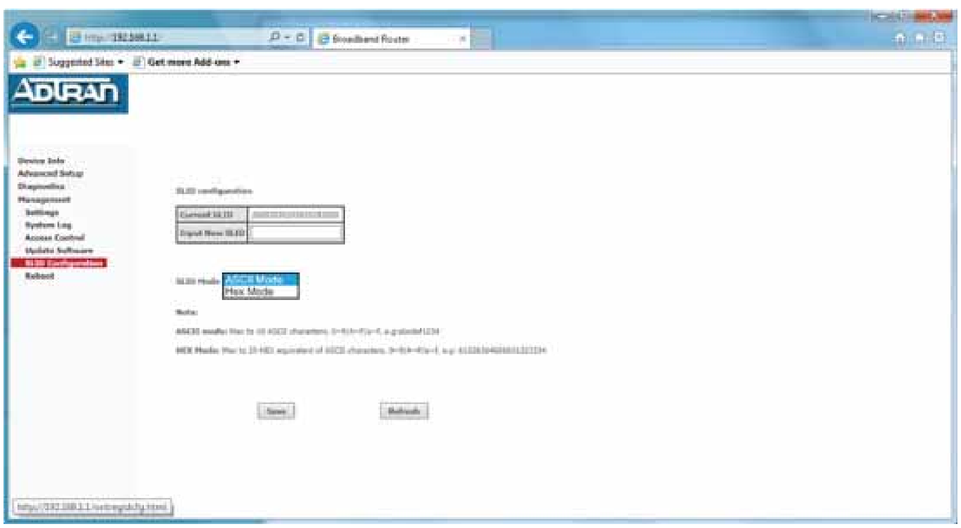


Figure 2-3. 401 Web GUI Display

6. Navigate to Management>SLID Configuration (see the menu tree in Figure 1-1).
7. Enter the Reg ID in the box labeled “Input New SLID.” Press <SAVE>.
8. Reboot the ONT using the option in the web GUI.

   This applies the configuration.

What’s Next

Continue to “Discover the ONT” on page 2-15

Discover the ONT

To discover the ONT, complete the following steps:

1. Navigate to the ONT Provisioning menu.

   Modules > GPON OLT > Provisioning > ONT

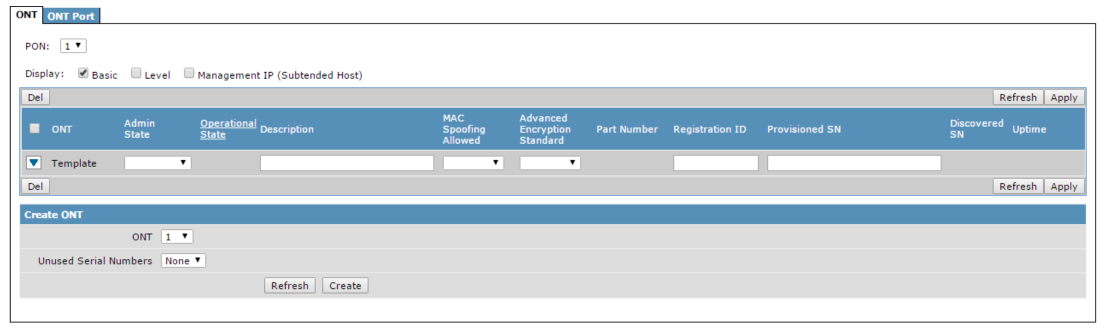


Figure 2-4. ONT Provisioning

2. Discover the ONT. Follow the steps in Table 2-8 for your previously chosen activation mode.

NOTE

If you are uncertain of your selected Activation Mode, refer to the PON Provisioning menu:
Modules > GPON OLT > Provisioning > PON

Table 2-8. ONT Discovery Method

Manual	Auto-Discovery	Auto-Activate	Registration-ID Lock-SN/ Registration-ID Unlock-SN
1. In the Create ONT section, select an unused number for your ONT. 2. In the Provisioned Serial Number, enter the ONT's serial number. 3. Set the Admin State to **IS**. 4. Click **Apply**.	1. In the Create ONT section, select an unused number for your ONT. 2. Select your serial number from the list of Unused Serial Numbers. 3. Click **Create**. 4. Set the Admin State to **IS**. 5. Click **Apply**.	1. In the Create ONT section, select an unused number for your ONT. 2. The ONT's serial number should automatically appear. If not, click **Refresh**. 3. Set the Admin State to **IS**. 4. Click **Apply**.	1. In the Create ONT section, select an unused number for your ONT. 2. In the Registration ID, enter the ONT's registration ID. 3. Set the Admin State to **IS**. 4. Click **Apply**.

Step 2: Service Provisioning

The Total Access 5000 FTTP application supports triple-play provisioning via Web GUI. To begin provisioning services, choose one of the following paths:

- "Voice"
- "Data" on page 2-23
- "Video" on page 2-24
- "RF-Video" on page 2-25

Voice

The Total Access 5000 FTTP application supports Session Initiation Protocol (SIP), Media Gateway Control Protocol (MGCP), and GR-303 voice.

SIP

SIP works in concert with voice and video by enabling and agreeing on characterizations of a session for sharing data. SIP is an application-layer control protocol that can establish, modify, and terminate multimed sessions.

SIP provides two options. The first is provided in the **Voice** menu found under the **Services** option. For purposes of this document, this option is referred to as Non-OMCI. The second option is provided in the **Voice FTTx** menu found under the **Services** option. For purposes of this document, this option is referred to as OMCI.

NOTE

If your deployment uses a Remote Gateway ONT, OMCI (Voice FTTx) is the only supported option.

MGCP

MGCP is a protocol that works hand-in-hand with H.323 and SIP in VoIP services. MGCP works between a call agent or media gateway controller, usually a software switch, and a media gateway with internal endpoints. The media gateway is the network device that converts voice signals carried by telephone lines into data packets carried over the Internet or other packet networks.

MGCP provides two options. The first is provided in the **Voice** menu found under the **Services** option. For purposes of this document, this option is referred to as Non-OMCI. The second option is provided in the **Voice FTTx** menu found under the **Services** option. For purposes of this document, this option is referred to as OMCI.

NOTE

If your deployment uses a Remote Gateway ONT, OMCI (Voice FTTx) is the only supported option.

GR-303

GR-303 is the basic protocol used for POTS service.

NOTE

A Total Access 5000 Voice Gateway Module is required when provisioning GR-303.

Select Your Voice Option

Use Table 2-9 to determine your voice option and navigate to your next step. If you're unsure of your voice option, refer to "Voice" on page 2-16.

Table 2-9. Voice Options

Option	See Page
SIP OMCI Voice	2-18
SIP Non-OMCI Voice	2-19
MGCP OMCI Voice	2-20
MGCP Non-OMCI Voice	2-21
GR-303 Voice	2-22

SIP OMCI Voice

To provision for voice, complete the following steps:

NOTE

This is a general set of instructions to turn up SIP OMCI voice. Optional settings are available. For additional information on these optional settings refer to the applicable documents listed in "Related Online Documentation and Resources" on page Intro-3.

1. "Create an EVC" on page 2-29
2. "Set the Voice Service Mode on the ONT" on page 2-33
3. "Provision the Port on the ONT" on page 2-34
4. "Create an IP Host" on page 2-39
5. "Create an EVC-Map" on page 2-41
6. "Provision the SIP Trunk" on page 2-47
7. "Provision the SIP Dialing Profile" on page 2-51
8. "Provision the OMCI SIP Users" on page 2-64

SIP Non-OMCI Voice

To provision for voice, complete the following steps:

NOTE

This is a general set of instructions to turn up SIP Non-OMCI voice. Optional settings are available. For additional information on these optional settings refer to the applicable documents listed in "Related Online Documentation and Resources" on page Intro-3.

1. "Create an EVC" on page 2-29
2. "Set the Voice Service Mode on the ONT" on page 2-33
3. "Provision the Port on the ONT" on page 2-34
4. "Create an IP Host" on page 2-39
5. "Create an EVC-Map" on page 2-41
6. "Provision the SIP Trunk" on page 2-47
7. "Provision the SIP Dialing Profile" on page 2-51
8. "Provision Class of Service (CoS) (Optional)" on page 2-61
9. "Provision for Global Voice (Optional)" on page 2-62
10. "Provision the Voice User" on page 2-63

MGCP OMCI Voice

To provision for voice, complete the following steps:

NOTE

This is a general set of instructions to turn up MGCP OMCI voice. Optional settings are available. For additional information on these optional settings refer to the applicable documents listed in "Related Online Documentation and Resources" on page Intro-3.

1. "Create an EVC" on page 2-29
2. "Set the Voice Service Mode on the ONT" on page 2-33
3. "Provision the Port on the ONT" on page 2-34
4. "Create an IP Host" on page 2-39
5. "Create an EVC-Map" on page 2-41
6. "Provision the MGCP Profile" on page 2-49
7. "Provision OMCI MGCP Endpoints" on page 2-67

MGCP Non-OMCI Voice

To provision for voice, complete the following steps:

NOTE

This is a general set of instructions to turn up MGCP Non-OMCI voice. Optional settings are available. For additional information on these optional settings refer to the applicable documents listed in "Related Online Documentation and Resources" on page Intro-3.

1. "Create an EVC" on page 2-29
2. "Set the Voice Service Mode on the ONT" on page 2-33
3. "Provision the Port on the ONT" on page 2-34
4. "Create an IP Host" on page 2-39
5. "Create an EVC-Map" on page 2-41
6. "Provision the MGCP Profile" on page 2-49
7. "Provision Non-OMCI MGCP Endpoints" on page 2-50

GR-303 Voice

To provision for voice, complete the following steps:

NOTE

This is a general set of instructions to turn up GR-303 voice. Optional settings are available. For additional information on these optional settings refer to the applicable documents listed in "Related Online Documentation and Resources" on page Intro-3.

1. "Set the Voice Service Mode on the ONT" on page 2-33
2. "Provision the Port on the ONT" on page 2-34
3. "Provision GR-303" on page 2-68

Data

To provision for data, complete the following steps:

NOTE

This is a general set of instructions to turn up data. Optional settings are available. For additional information on these optional settings refer to the applicable documents listed in "Related Online Documentation and Resources" on page Intro-3.

1. "Create an EVC" on page 2-29
2. "Provision the Port on the ONT" on page 2-34
3. "Create an EVC-Map" on page 2-41

Video

To provision for video, complete the following:

NOTE

This is a general set of instructions to turn up video. Optional settings are available. For additional information on these optional settings refer to the applicable documents listed in "Related Online Documentation and Resources" on page Intro-3.

1. "Create an EVC" on page 2-29
2. "Provision the Port on the ONT" on page 2-34
3. "Create an EVC-Map" on page 2-41

RF-Video

To provision for RF-Video, complete the following:

NOTE

This is a general set of instructions to turn up RF-video. Optional settings are available. For additional information on these optional settings refer to the applicable documents listed in "Related Online Documentation and Resources" on page Intro-3.

1. "Provision the Port on the ONT" on page 2-34

TLS

TLS enables the user to tag-switch through the system. The user can send traffic without MAC Security or MAC Limits. Proxy ARP will be disabled as well, so the devices will respond with their own ARP. Using TLS removes the ability to use IGMP replication on this particular port. Since the flow will be tag switched up to the network, the VLANs must be configured in a way that an outer VLAN appears only on a single access module within the entire system. The inner tag (if running double tags) cannot be duplicated within the access module. If the VLAN becomes MAC-switched, TLS no longer functions.

Refer to Table 2-10 for an available list of TLS options.

Table 2-10. EVC and TLS

Mac-Switched		No Mac-Switched
Double-Tag	Not Supported	Double tagged TLS, N end points, S-tag must be unique within the entire Total Access 5000 Network. C-tag must be unique per port.
Single-Tag	Not Supported	E-Line (TLS), Max of 2 endpoints, including men-port

Select Your TLS Option

Use Table 2-9 to determine your TLS option and navigate to your next step.

Table 2-11. Voice Options

Option	See Page
TLS Single Tag Configuration	2-27
TLS Double Tag Configuration	2-28

TLS Single Tag Configuration

To provision TLS Single Tag, complete the following:

NOTE

This is a general set of instructions to turn up TLS. Optional settings are available. For additional information on these optional settings refer to the applicable documents listed in "Related Online Documents and Resources" on page Intro-2.

1. "Create an EVC" on page 2-29.
2. "Provision the Port on the ONT" on page 2-34.
3. "Create an EVC-Map" on page 2-41.

TLS Double Tag Configuration

To provision TLS Double Tag, complete the following:

NOTE

This is a general set of instructions to turn up TLS. Optional settings are available. For additional information on these optional settings refer to the applicable documents listed in "Related Online Documents and Resources" on page Intro-2.

1. "Create an EVC" on page 2-29.
2. "Provision the Port on the ONT" on page 2-34.
3. "Create an EVC-Map" on page 2-41.

Create an EVC

The EVC (Ethernet Virtual Connection) is a centrally managed object defining the properties of a particular S-Tag within a Total Access 5000. The EVC object enables the provisioning of ELINE, E-TREE, and E-LAN applications. EVCs are available for use by all access modules within a shelf.

NOTE

The EVC for SIP/MGCP traffic will be a dedicated EVC because voice traffic requires different Quality of Service (QoS) handling than other data traffic.

To create an EVC, complete the following steps:

1. Navigate to the Create EVC section of the EVC page.

   Services > **EVCs** > **EVC** > **Create EVC**

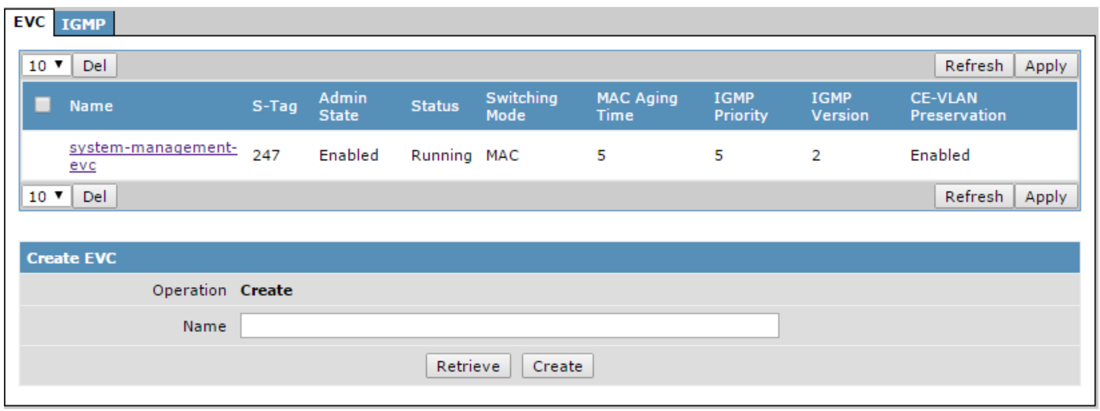


Figure 2-5. Create EVC

2. Enter a unique EVC name into the Name field.

NOTE

EVC names are case sensitive.

3. Click the **Create** button to access the Edit EVC options. The Edit EVC screen will open.

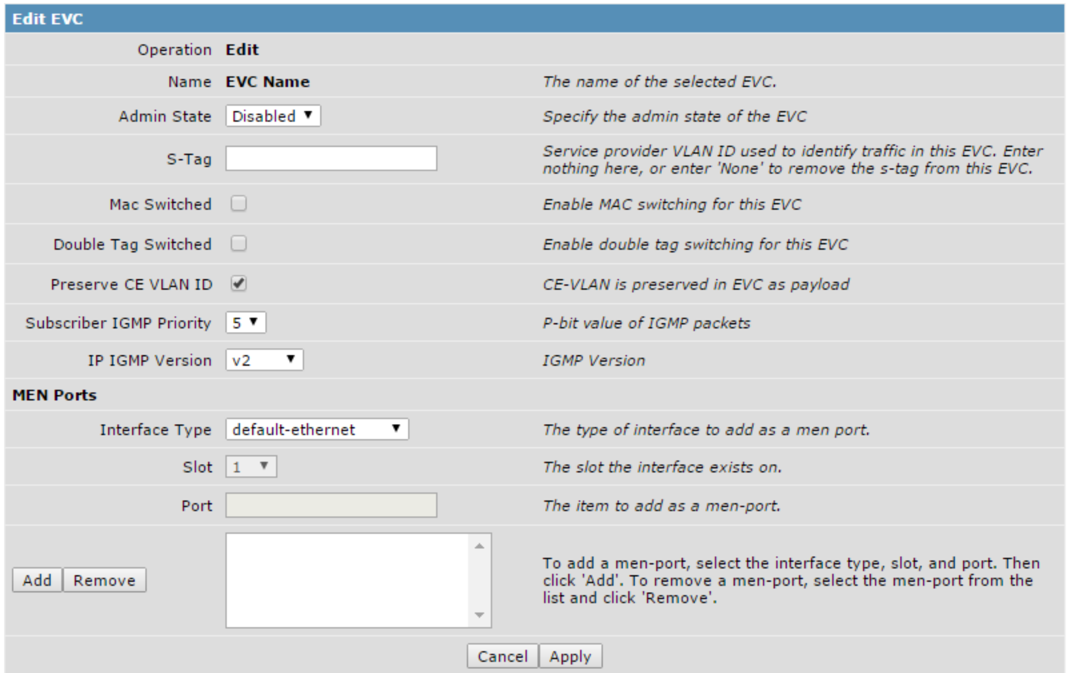


Figure 2-6. Edit EVC

4. Set the Admin State to **Enabled**.
5. Enter the S-Tag for the EVC.
6. Depending on your selected service, enable or disable MAC-Switching..

Table 2-12. MAC-Switching

Service	Definition
Voice/Video/Data	Enabled
Single/Double Tag TLS	Disabled

7. If provisioning Single Tag TLS, continue to step 16. If provisioning for Double Tag TLS, continue to step 8. For all other services, continue to step 10.
8. Enable double-tag-switching.

```
ChassisID(config-evc name)#double-tag-switched
```

9. If provisioning Double Tag TLS, continue to step 16. For all other services, continue to step 10.
10. Disable the Preserve CE-VLAN ID setting on the EVC.
11. If provisioning for video, set the Subscriber IGMP Priority.
If provisioning for voice or data, skip to step 9.
12. Select the Interface Type for the MEN Port(s).

NOTE

For Video Services, **default-ethernet** must be one of your MEN Ports.

13. Select **A** for the MEN port slot.
14. Enter the Port/Group numbers of the MEN Port(s). MEN Port is the upstream network connection for the EVC.
15. Click **Add**.
16. Click **Apply** to enable the EVC.
17. The EVC should be added to the bottom of the EVC list. Verify the Status is **Running**, It may take up to 10 seconds for the Status to change to **Running**.
18. If currently provisioning for voice or data, skip to What's Next. If currently provisioning for video, complete the following:
    a. Select the IGMP tab.

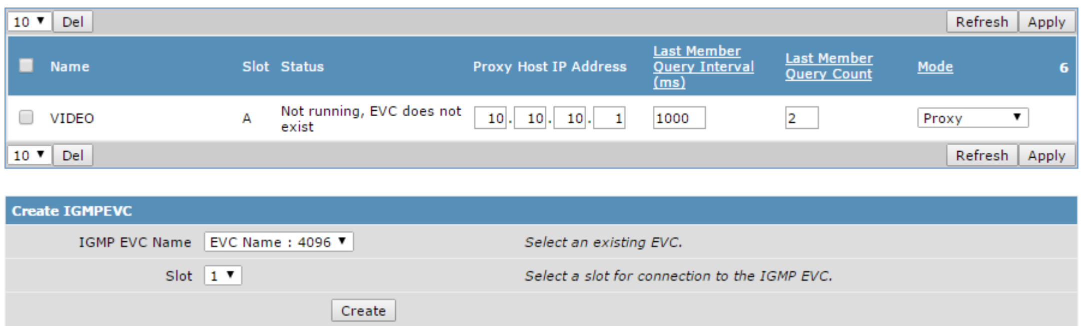


Figure 2-7. Edit EVC

    b. An IGMP EVC connection is required for the switch module (Slot A) and each access module. Select the required EVC name in the IGMP EVC Name drop down.
    c. Select the required slot.
    d. Click the Create button.

19. The IGMP EVC should be added to the bottom of the IGMP EVC list. Verify the Status is **Running**, It may take up to 10 seconds for the Status to change to **Running**.

NOTE

The IGMP EVC for the OLT Slot will not be running until the EVC-Map is created.

What's Next

- For SIP or MGCP provisioning, continue to "Set the Voice Service Mode on the ONT" on page 2-33.
- For video or data provisioning, continue to "Provision the Port on the ONT" on page 2-34
- For TLS provisioning, continue to "Create an EVC-Map" on page 2-41.

Set the Voice Service Mode on the ONT

1. Navigate to the ONT Provisioning menu.

   Modules > GPON OLT > Provisioning > ONT

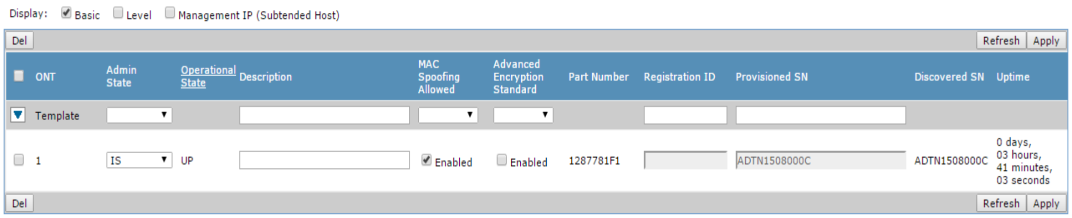


Figure 2-8. Voice Service Mode

2. Click Level and Management IP (Subtended Host) check boxes.

NOTE

You may have to scroll to the right to view all available options.

3. Set the POTS Service Mode.

   For more details about the available modes, refer to the Total Access 5000 GPON User Interface Guide (P/N 65K90GPON-31).

4. Set the VoIP Config Method.

   Remote Gateways require the use of OMCI. For more details about the available methods, refer to the Total Access 5000 GPON User Interface Guide (P/N 65K90GPON-31).

5. Select static or DHCP from the IP Allocation field.
6. If using DHCP, skip to step 10.
7. If using a static IP address for ONT management, enter the IP Address.
8. If using a static IP address for ONT management, enter the Subnet Mask.
9. If using a static IP address for ONT management, enter the Gateway IP Address.

10. Click **Apply**.

NOTE

To view the DHCP address, navigate to the ONT Status Screen (**Modules** > **GPON OLT** > **Status** > **ONT > ONT Status**) and check the Subtended Host check box. Scroll to the right to view the IP address.

What's Next

For SIP, MGCP, GR-303 provisioning, continue to "Provision the Port on the ONT" on page 2-34.

Provision the Port on the ONT

NOTE

If provisioning data and video on the same port, the ONT port only needs to be enabled once.

1. Navigate to the ONT Port Provisioning menu.

   Modules > GPON OLT > Provisioning > ONT > ONT Port

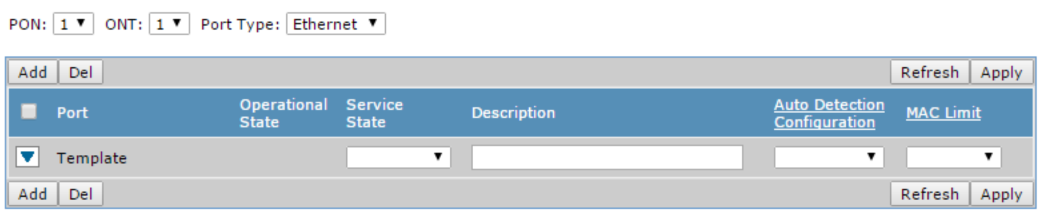


Figure 2-9. ONT Port Provisioning

2. Select your PON.
3. Select your ONT
4. Select the Port Type. Use Table 2-13 to determine your port type and navigate to your next step.

Table 2-13. Port Type

Service	ONT	Type	See Page
Data/Video	Non-Remote Gateway	Ethernet	2-35
	Remote Gateway	Virtual Gigabit Interface	2-38
Voice	All ONTs	FXS	2-36
RF-Video	All ONTs	RF-Video	2-37

Ethernet

After selecting Ethernet as the ONT port type, complete the following steps:

1. Set the number of MAC addresses allowed.

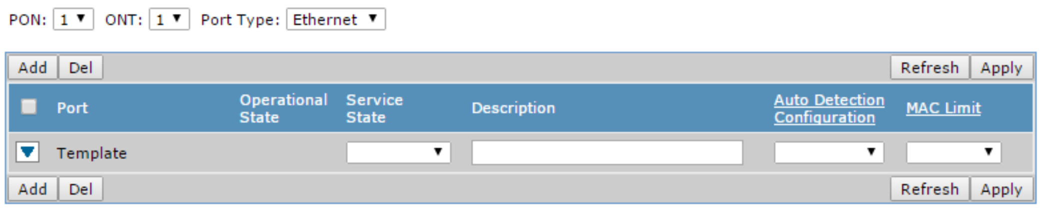


Figure 2-10. ONT Port Provisioning

NOTE

- 16 MAC addresses per ONT are allowed and must be shared by all Ethernet ports on the ONT.
- A value of 0 will actually allow up to 128 MAC addresses to be attributed to the ONT. However, the number of MAC addresses the OLT can support is limited so using more than 16 will severely limit the number of MAC addresses available to other ONTs. No more than 16 static addresses can be configured regardless of the number of MAC addresses allowed by this setting.

2. Set the Service State to **IS** to enable the Ethernet interface of the ONT.
3. Click **Apply**.

What's Next

For video or data provisioning, continue to "Create an EVC-Map" on page 2-41.

FXS

After selecting FXS as the ONT port type, complete the following steps:

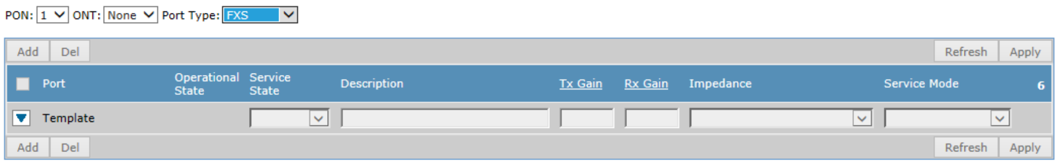


Figure 2-11. FXS Port Provisioning

1. Adjust the Tx Gain for the FXS port between -12.0dB and +6.0dB.
2. Adjust the Rx Gain for the FXS port between -12dB and +6.0dB.
3. Set the Service State to **IS** to enable the FXS interface of the ONT.
4. Click **Apply**.

What's Next

- For SIP or MGCP provisioning, continue to "Create an IP Host" on page 2-39.
- For GR-303 provisioning, continue to "Provision GR-303" on page 2-68.

RF-Video

After selecting RF-Video as the ONT port type, complete the following steps:

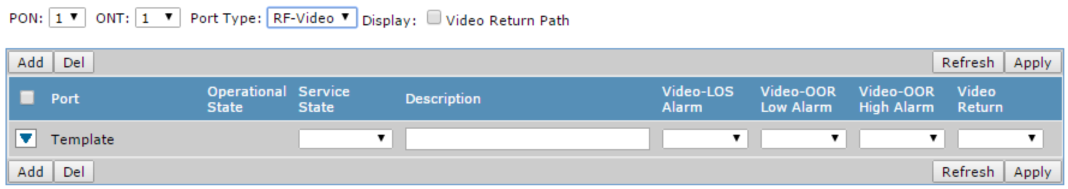


Figure 2-12. RF-Video Port Provisioning

1. Enable the video return (SWRD).
2. Set the Service State to **IS** to enable the RF-Video interface of the ONT.
3. Click **Apply**.

What's Next

For RF-Video, this completes provisioning. Services should be up and running. To provision another service, continue to "Step 2: Service Provisioning" on page 2-16.

Virtual Gigabit Interface

To provision a virtual gigabit interface, complete the following steps:

1. Open a new telnet window and log on to the Total Access 5000 shelf using the same user credentials used for the Web GUI.
2. Access the Enable prompt.

```
ChassisID>enable
ChassisID#
```

3. Access the Global Configuration Command Set.

```
ChassisID#configure terminal
```

4. Access the Virtual Gigabit Ethernet Interface Configuration Command Set.

```
ChassisID(config)#interface virtual-gigabit-ethernet <ont-id/0/
port>@<shelf/slot/port>
```

5. Enable the interface.

```
ChassisID(config-virtualGigabitEthernet x/x/x@x/x/x)#no shutdown
```

6. You may now close out the telnet window.

What's Next

- For SIP or MGCP provisioning, continue to "Create an IP Host" on page 2-39.
- For video or data provisioning, continue to "Create an EVC-Map" on page 2-41.

Create an IP Host

1. Navigate to the IP Host Provisioning menu.

   Modules > GPON OLT > Provisioning > IP Host

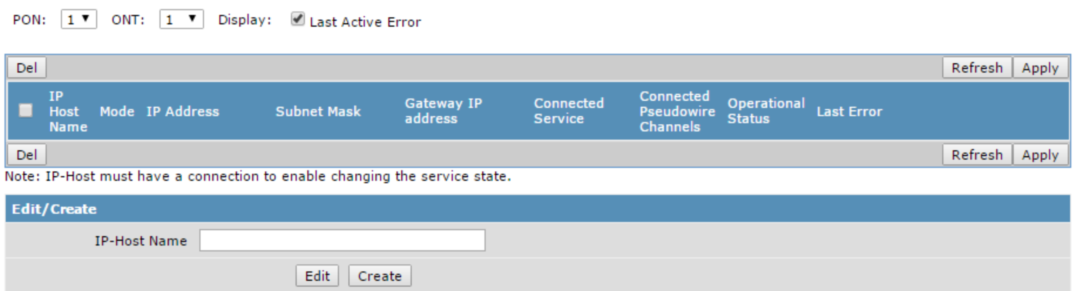


Figure 2-13. IP-Host Create Menu

2. Enter the IP-Host Name.
3. Click **Create**, the Edit/Create screen is displayed.

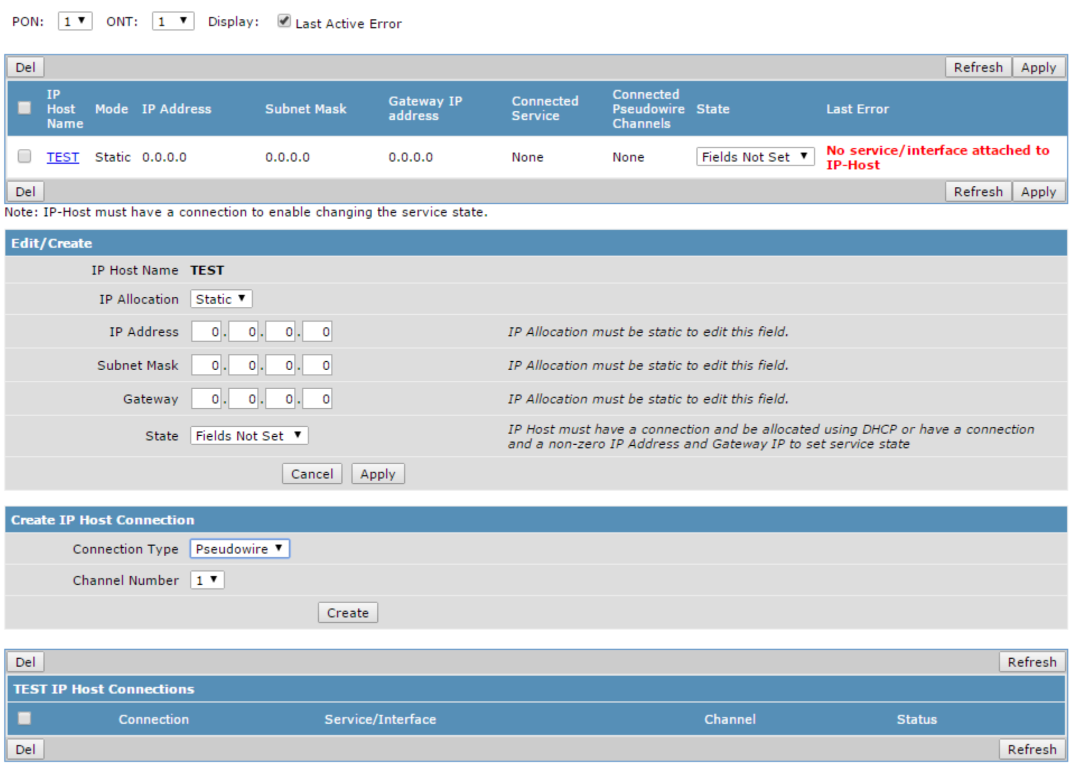


Figure 2-14. IP-Host Provisioning

4. Select the PON number.
5. Select the ONT.
6. In the IP-Host Name field, enter a unique name for the IP-Host.

NOTE

Only two interface IP-host entities can be created per ONT. Attempts to create more than two will be rejected.

7. Select the IP Allocation method. If set to DHCP, skip to step 9.
8. If the allocation method is set to Static, complete the following:
   a. Enter the IP Address.
   b. Enter the Subnet Mask.
   c. Enter the Gateway.
9. If DNS is not required, skip to step 10. If DNS is required, complete the following:
   a. Select Enabled.
   b. Enter the default domain name of the DNS.
   c. Enter the preferred DNS.

      Only 2 addresses can be entered at a time. The first address becomes the preferred DNS and the subsequent address becomes the second priority.

      The DNS must be configured using IP host to resolve FQDN configured in the SIP trunk and MGCP.
10. Click **Apply** in the Edit/Create section.
11. Select the Connection Type in the Create IP Host Connection section.
12. Click **Create**.
13. Verify your IP Host listed state is Active and that there are no errors that appear in the Last Error column.

What's Next

For SIP or MGCP provisioning, continue to "Create an EVC-Map" on page 2-41.

Create an EVC-Map

To create an EVC-Map, complete the following steps:

1. Access the Interface Map.

   Modules > GPON OLT > Provisioning > Interface Map

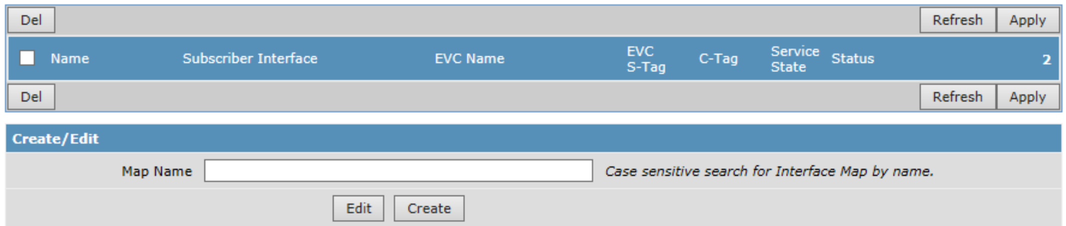


Figure 2-15. EVC-Map Create

2. Enter the new EVC-Map name into the Map Name field and click the Create button.

NOTE

An example name would be DATAMap. If there are spaces in the name, you must use quotes around the name to use show commands.

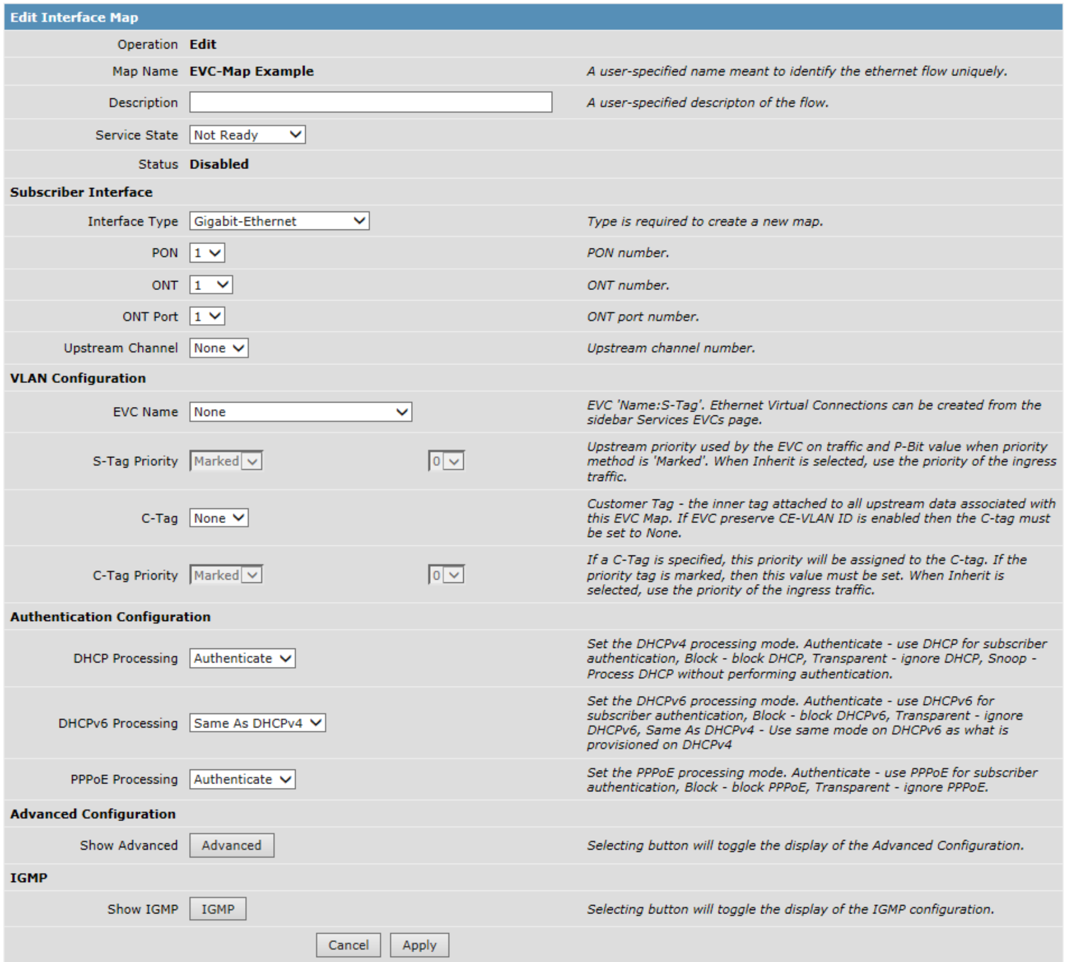


Figure 2-16. EVC-Map Edit

3. Set the Service State to **Active**.
4. Select the Interface Type. Use Table 2-14 to determine the type and the steps to complete.

Table 2-14. Interface Type

Service	ONT	Type	Steps
Data/Video	Non-Remote Gateway	Gigabit-Ethernet	Complete the following steps: 1. Select the OLT Port. 2. Select the ONT. 3. Select the ONT Port. 4. Select the Upstream Channel.
	Remote Gateway	Virtual Gigabit-Ethernet	
Voice	All ONTs	IP Host	Select the IP Host created for this service.

5. Select the EVC created for your selected service.

6. If provisioning for voice or data, skip to step 17. If provisioning for video or TLS, set the subscriber IGMP mode.

NOTE

- Forking is only supported on the Total Access 5000 GPON OLT 8X SFP Access Module (P/N 1187503F1).
- If provisioning for TLS, the IGMP mode must be set to transparent.

7. If provisioning for TLS, skip to step 11. If provisioning for video, continue to step 8.
8. Enable smart immediate leave.

   This function is associated with IGMP snooping or routing whereby the switch or router stops sending immediately the multicast stream when receiving an IGMP leave for the last member on this requesting interface, i.e. without sending one or more group specific queries and waiting for its timeout.
9. Set the IGMP proxy router IP address if the host connected to the ONT cares about the IP address for IGMP query messages.

   The default IGMP proxy router IP address is 0.0.0.0
10. If provisioning for video, skip to step 17.

NOTICE

Steps 11 - 16 are only for provisioning TLS. If you are provisioning for voice, video, or data, continue to step 17.

11. Set the DHCP mode to transparent.
12. Set the PPPoE mode to transparent.
13. Set the ARP mode to transparent.
14. If provisioning for Single TLS, skip to 21. If provisioning for Double Tag TLS, continue to step 15.
15. Set the C-tag.
16. If provisioning for Double Tag TLS, continue to step 21.

17. If provisioning voice, skip to step 21. If you are provisioning for voice or data, configure the Authentication Method. Use Table 2-15 to determine the authentication and steps required.

NOTE

PPPoE does not support video services.

Table 2-15. Authentication Method

Authentication	Steps
DHCPv4 only	Complete the following steps: 1. Set DHCP Processing to Authenticate. 2. Set DHCPv6 Processing to Block. 3. Set PPPoE to Block.
DHCPv6 only	Complete the following: 1. Set DHCP Processing to Block. 2. Set DHCPv6 Processing to Authenticate. 3. Set PPPoE to Block.
DHCPv4 and DHCPv6	Complete the following: 1. Set DHCP Processing to Authenticate. 2. Set DHCPv6 Processing to Same As DHCPv4. 3. Set PPPoE to Block.
PPPoE	Complete the following: 1. Set DHCP Processing to Block. 2. Set DHCPv6 Processing to Block. 3. Set PPPoE to Authenticate.

18. Configure the Relay Agent. If you are unsure about supported options, contact your network administrator. For more information on Relay Agent, refer to the Total Access 5000 GPON User Interface Guide (P/N 65K90GPON-31)
    a. Enter the Circuit ID Format.
    b. Enable or disable Remote ID.
    c. Enter the Remote ID Format.
    d. Enable or disable DHCP Option 82 Insertion.
    e. Enable or disable DHCPv6 Relay Agent.
    f. Enable or disable PPPoE Intermediate Agent.

19. If provisioning a data or video service on a Remote Gateway ONT, complete the following steps:
    a. Click **Advanced**.

Figure 2-17. EVC-Map Advanced

    b. Select the CE-VLAN. The CE-VLAN can be typed in or selected from a drop-down list.

20. If provisioning for video, complete the following steps. If provisioning for data, skip to step 21.
    a. Click **IGMP**.

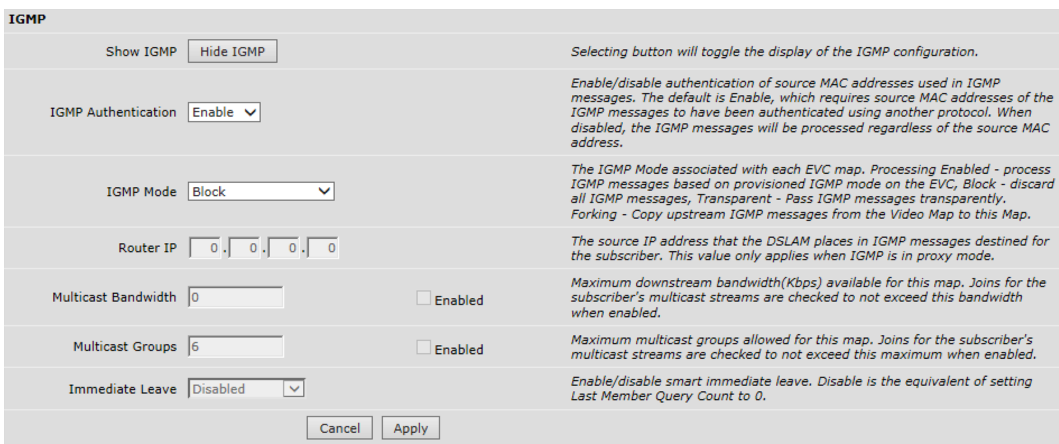


Figure 2-18. EVC-Map IGMP

    b. Set the subscriber IGMP mode.
    c. Enable Immediate Leave.
    d. Set the IGMP proxy router IP address.

21. Click **Apply**.
22. The EVC-Map should be added to the bottom of the EVC-Map list. Verify the Status is **Running**, It may take up to 10 seconds for the Status to change to **Running**.

23. If provisioning video, return to the IGMP EVC list to verify the IGMP EVC for the OLT slot is now **Running**.

What's Next

- For OMCI SIP and Non-OMCI SIP provisioning, continue to "Provision the SIP Trunk" on page 2-47.
- For OMCI MGCP and Non-OMCI MGCP provisioning, continue to "Provision the MGCP Profile" on page 2-49
- For remote gateway ONT video or data provisioning, continue to the Section 2, Step 2: Log On to the ONT in the ADTRAN 400 Series Residential Gateway ONT Basic Configuration Guide (P/N 61287RGONT-29)
- For non-remote gateway ONT video or data provisioning, this completes provisioning. Services should be up and running. To provision another service, continue to "Step 2: Service Provisioning" on page 2-16.
- For TLS, this completes provisioning. Services should be up and running. To provision another service, continue to "Step 2: Service Provisioning" on page 2-16.

Provision the SIP Trunk

The SIP trunk is the logical path to the SIP proxy. The attributes configured on the trunk should be compatible with the corresponding parameters on the SIP proxy. If the system defaults match the capabilities and configured options of the SIP proxy, a small amount of trunk provisioning is required.

All voice trunks are shared across the node, so provisioning of a trunk at the GigE SM makes it available to all gateways.

1. Navigate to the Trunk menu.

   OMCISIP **– Services** > **Voice FTTx** > **SIP** > **Trunk**

   Non-OMCI SIP **– Services** > **Voice** > **SIP** > **Trunk**

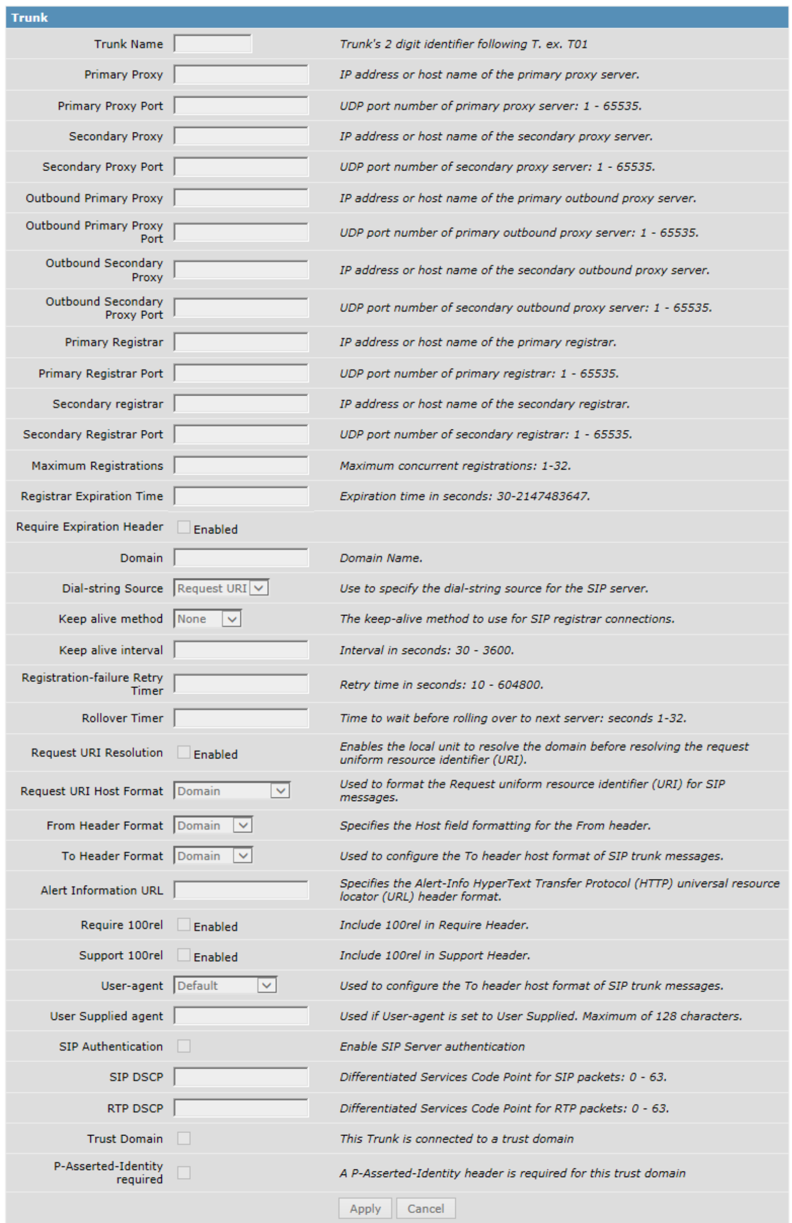


Figure 2-19. SIP Trunk Create

2. Click **Add**.
3. Enter the Trunk's 2 digital identifier following T.
4. Click **OK**.
5. Enter the SIP Primary Proxy IP address.
6. Enter the Primary Registrar IP address.
7. If using a secondary server, enter the SIP Secondary Proxy address.
8. If using a secondary server, enter the Secondary Registrar IP address.
9. If the system defaults match the capabilities and configured options of the SIP proxy, no further provisioning is required. For more details about the available provisioning options, refer to the Total Access 5000 Switch Module User Interface Guide (P/N 65K90SM-31).
10. Click **Apply**.

What's Next

For Non-OMCI and OMCI SIP provisioning, continue to "Provision the SIP Dialing Profile" on page 2-51.

Provision the MGCP Profile

To create the MGCP profile, complete the following:

1. Access the Profiles menu.

   OMCI MGCP **– Services** > **Voice FTTx** > **MGCP** > **Profiles**

   Non-OMCI MGCP **– Services** > **Voice** > **SIP** > **Profiles**

2. Enter the Profile Name.

NOTE

Only one MGCP Profile is supported.

3. Click **Create**, the Provision MGCP Profile screen is displayed.
4. Specify the primary MGCP call agent IP address.

   It is important to identify the call agent to the ONT MGCP Endpoint. Both primary and secondary call agents can be established, but at minimum a primary call agent is required. If a connection with the primary call agent fails, call agents will be tried in the order they are entered in the configuration.

5. Click **Apply**.

What's Next

- For OMCI MGCP provisioning, continue to "Provision OMCI MGCP Endpoints" on page 2-67.
- For Non-OMCI MGCP provisioning, continue to "Provision Non-OMCI MGCP Endpoints" on page 2-50

Provision Non-OMCI MGCP Endpoints

MGCP endpoints are dedicated FXS ports configured to use MGCP to communicate with a call agent.

To create the MGCP profile, complete the following:

1. Navigate to the Endpoints menu.

   Services > **Voice** > **MGCP** > **Endpoints**
2. Enter the slot number of the GPON OLT.
3. Enter a unique MGCP Endpoint Index.
4. Click **Create**.
5. Enter the MGCP Profile to be used by this voice user.
6. Enter the FXS port with which this MGCP endpoint is associated.
7. Click **Apply**.

What's Next

For Non-OMCI MGCP, this completes provisioning. Services should be up and running. To provision another service, continue to "Step 2: Service Provisioning" on page 2-16.

Provision the SIP Dialing Profile

The Dialing Profile is assigned to voice users, and is used to notify the access modules when to stop collecting digits being dialed and begin connecting a phone call. The dial profile creates and stores number-complete templates.

A number-complete template consists of a pattern of digits used by telephone companies when making calls. A typical template would be 555-XXX-XXX. These templates can be expanded to include Dial Plans, External Line Codes and Special Prefix Patterns.

The access module collects digits and looks for a match against the Dial Plans, External Line Codes and Special Prefix (SPRE) Patterns. When the digits dialed match a number-complete template, the dial-string is immediately sent to the server for routing.

For example, a normal phone number consists of the following template: 555-XXX-XXXX (where "X" is a wild card denoting any digit from 1 to 9). The first three digits are the Area Code Designation, the next three digits are the Phone Exchange Designation, and the last four digits are the Local Number Designation.

When a user initiates a phone call, the access module compares the dialed digits to the number-complete template. If the dialed digits are a match (in this case, three 5s followed by seven other digits) the access module immediately sends the complete dial-string to the server. The server then routes and connects the call.

If the user dials a pattern of digits that does not match any number-complete template, the pattern will still be forwarded to the server after the Inter-digit Timeout has expired. Proper definition of the dial plan is recommended for optimum customer experience. At the very least, emergency numbers should be configured to avoid delays in these calls.

The different types of number-complete templates can be chained together to form longer dial-strings with the use of chaining characters ("&"). For example, if a dialing profile contains an External Line Code "9&", a Special Prefix "*70&" and a Dial Plan "555-XXX-XXXX" and the user dials *70,9,555-123-4567, all the digits will be gathered into a single dial-string and sent to the server when the last digit is entered. An External Line Code will only be matched once during a dialing sequence.

Dial Plan Pattern Restrictions

Dial Plan patterns are entered using the **`dial-plan <type> <PATTERN> [emergency-number] [external-line-code <prohibited|required>]`** command. The following types are supported: 900-number, always-permitted, internal, international, local, national, operator-assisted, specify-carrier, toll-free, user1, user2 and user3. Multiple patterns of the same type are allowed. The pattern must be in the form of a phone number or dialing pattern containing wildcards. Available wildcards are: N=2-9, M=1-8, X=0-9, and [abc]=Any digit contained in the bracketed list. When creating a Dial Plan Pattern, the following rules must be observed:

- Templates must have at least one number or wild card.
- The "(' ')" and "-" characters are allowed, but not inside brackets "[ ]".
- A ","is allowed within bracket "[ ]", but not elsewhere.
- Wild cards (MNX) are not allowed inside brackets "[ ]".
- Order of numbers is not enforced within brackets "[ ]".
- The "$" character is allowed, but MUST be the last character in the pattern or standalone.
- If "*" and "#" are entered, they must be the first character in the pattern. They cannot be standalone.

The following are examples of possible Dial Plan patterns:

- For a residential customer:
  - **`dial-plan 900-number 1-900-NXX-XXXX`**
  - **`dial-plan always-permitted 911 emergency-number`**
  - **`dial-plan international 011$`**
  - **`dial-plan local 256-NXX-XXXX`**
  - **`dial-plan local NXX-XXXX`**
  - **`dial-plan national 1-NXX-NXX-XXXX`**
  - **`dial-plan specify-carrier 10-10-XXX$`**
  - **`dial-plan toll-free 1-800-NXX-XXXX`**
  - **`dial-plan toll-free 1-888-NXX-XXXX`**
  - **`dial-plan toll-free 1-877-NXX-XXXX`**
  - **`dial-plan user1 [23456]11`**
- For a business customer (using an external line code):
  - **`dial-plan 900-number 1-900-NXX-XXXX external-line-code required`**
  - **`dial-plan always-permitted 911 emergency-number`**
  - **`dial-plan internal MXXX external-line-code prohibited`**
  - **`dial-plan international 011$ external-line-code required`**
  - **`dial-plan local 256-NXX-XXXX external-line-code required`**
  - **`dial-plan local NXX-XXXX external-line-code required`**
  - **`dial-plan national 1-NXX-NXX-XXXX external-line-code required`**
  - **`dial-plan specify-carrier 10-10-XXX$ external-line-code required`**
  - **`dial-plan toll-free 1-800-NXX-XXXX external-line-code required`**
  - **`dial-plan toll-free 1-888-NXX-XXXX external-line-code required`**
  - **`dial-plan toll-free 1-877-NXX-XXXX external-line-code required`**
  - **`dial-plan user1 [23456]11 external-line-code required`**

SPRE Pattern Restrictions

SPRE patterns are entered using the **`spre <PATTERN> [tone <dial|stutter-dial>]`** command. SPRE Pattern creates special code numbers required to access voice services. A SPRE Pattern must be in the form of a special prefix (spre) code or dialing pattern containing wild cards. Available wild cards are: N=2-9, M=1-8, X=0-9 [abc] = any digit contained within the bracket list. The pattern can end with a chaining character (“&” or “$”) which allows for the collection of more digits before the dial string is sent to the server. Ending the pattern with “&” causes the server to continue to look for another number-complete template (dial plan, external line-code or special prefix pattern) following the SPRE code. Ending it with “$” causes the access module to stop attempting to match additional inputs. However, digits will continue to be collected until after the Inter-Digit time out occurs.The following rules must be observed:

- The Template must begin with an “*” or “#”. An “*” and “#” are not allowed elsewhere in the Template.
- The Template must have at least one number.

- The characters “(“”) and “-” are allowed, but not inside “[ ]”.
- Do not use “,” or “” inside “[ ]”.
- Wild cards (MNX) are not allowed inside “[ ]”.
- The characters “&” and “$” are allowed but must be the last character and cannot be a standalone.

The following are examples of possible SPRE Patterns:

- **`spre *3XX`**
- **`spre *6[37]&`**
- **`spre *72& tone stutter-dial`**
- **`spre *82&`**
- **`spre *9[02]& tone stutter-dial`**
- **`spre *7[45]$`**
- **`spre *[56789]X`**

External Line Code Restrictions

External Line Codes are entered using the **`external-line-code <PATTERN> [tone <dial|stutter-dial>]`** command. An External Line Code must be in the form of a dialing pattern without wild cards. For example, if a user must first dial “8” to obtain an outside line, the entry would be “8&” where the ampersand tells the server that the “8” designates an outside number and to expect more digits in the number-complete template. The pattern can end with a chaining character (“&” or “$”), which allows for collection of more digits before the dial string is sent to the server. Ending the pattern with a “&” causes the server to continue to look for another number-complete template (dial plan or special prefix pattern) following the external line code. An external line code will only be matched once. Ending the pattern with a “$” causes the access module to stop attempting to match additional inputs. However, digits will continue to be collected until after the Inter Digit time out occurs. The following rules must be observed:

- Template must have at least one number (i.e., 0-9).
- Wild cards are not allowed.
- If “*” and “#” are entered, they must be the first character. They cannot be standalone.
- The characters “&” or “$” are allowed but must be the last character and cannot be standalone.

The following is an example of a possible External Line Code:

- **`external-line-code 8& tone dial`**

Dial Plan Provisioning

To provision the dial plan, complete the following:

1. Navigate to the Dialing Profile menu.

   OMCI SIP **– Services** > **Voice FTTx** > **SIP** > **Dialing Profiles**

   Non-OMCI SIP **– Services** > **Voice** > **SIP** > **Dialing Profiles**

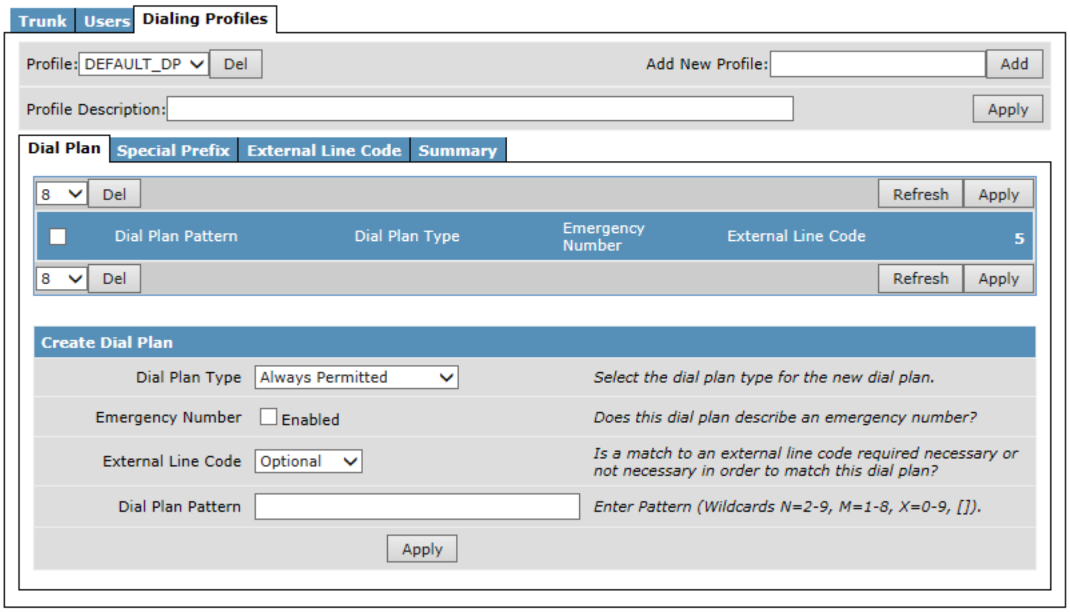


Figure 2-20. Dial Plan Provisioning

2. If you are creating a new dialing profile, enter a new profile name. The name cannot contain the "/" character.
3. Click **Add**.
4. Select the dial plan type for the new dial plan.
5. Enter the Dial Plan Pattern. For Example **`256-NXX-XXXX`**
6. Click **Apply** in the Create Dial Plan section.

What's Next

- For OMCI SIP provisioning, continue to "Provision the Common Profiles (Optional)" on page 2-55.
- For Non-OMCI SIP provisioning, continue to "Provision Class of Service (CoS) (Optional)" on page 2-61

Provision the Common Profiles (Optional)

Both OMCI SIP and OMCI MGCP support the use of common profiles. This feature enables the creation of specific profiles that can be assigned to multiple users.

NOTE

If you are unsure about these options, contact your network administrator. For more details about the available provisioning options, refer to the Total Access 5000 Switch Module User Interface Guide (P/N 65K90SM-31). Creating Common Profiles is optional for your network. If these profiles are not required, continue to "Provision the OMCI SIP Users" on page 2-64.

Refer to Table 2-16 for a list of the supported profiles.

Table 2-16. Common Profiles

Profile	Support	See Page
Call Feature	SIP	2-56
Media	SIP/MGCP	2-58
Codec	SIP/MGCP	2-60

Provision the Call Features Profile

Call feature options are available to set the access module/remote device to perform certain operations, like three-way conferencing, locally. It is not necessary to change any of these settings if the SIP server is capable of performing them.

1. Navigate to the Call Features menu.

   Services > Voice FTTx > Common Profiles > Call Features

2. Provision the call feature profile options.

   Refer to Table 2-17 for a list of call feature options.

Table 2-17. Call Feature Profile Options

Option	Description
Emergency Number Ringing Timeout	Sets the maximum duration, in minutes, an inhibited call may remain open by an Emergency Operator.
Emergency Number Onhook allow	Determines if an Emergency call will be dropped or remain open when the call originator goes on-hook. The following options are available: ■ If set to allow, the call will be dropped if the call originator hangs up. This is the default mode. ■ If set to inhibit, the call will remain open until the Emergency Operator terminates the call. While the call is held-up, the local phone will ring and the Emergency Operator will hear a ringback tone.
Call Waiting	Enables call waiting on the subscriber port.
Caller ID Inbound	Allows inbound caller ID to this endpoint.
Caller ID Outbound	Allows outband caller ID from this endpoint.
Transfer On Hangup	Enables transfer on hangup. When transferring a call, hanging up initiates the transfer to the destination party.
Timeout Alerting	Specifies the maximum time a call is allowed to remain in the alerting state. The shorter of this timeout or the configured maximum number of rings will determine how long a call is allowed to ring.
Timeout Interdigit	Specifies the maximum time allowed between dialed digits.
Conference	Allows the initiation of three-way conference calls. This feature allows multiple parties to communicate at the same time on the same line.

Table 2-17. Call Feature Profile Options (Continued)

Option	Description
Conference Local Originator Flashhook	If the voice conference mode is set to local, specify the actions performed if the conference originator issues a flashhook once the conference has been established. The following options are available: ■ The drop option specifies that the last party added to the 3-way conference will be dropped and the call will continue between the two remaining parties. ■ The ignore option specifies that the flashhook will be ignored. The 3-way conference will continue without interruption. ■ The split option specifies that the 3-way conference will be split into two calls, one between the originator and the first party and one between the originator and second party. When additional flashhooks are issued after the split, they will toggle the originator between the two calls.
Feature Mode	Determines if voice conferencing bridging will be handled within the unit or from a far-end conferencing server.

What’s Next

- Continue to “Provision the Media Profile” on page 2-58.

Provision the Media Profile

The media profile is created in the Total Access 5000 to provision the Realtime Transport Protocol (RTP) parameters on the access module/remote device.

1. Navigate to the Media menu.

   Services > Voice FTTx > Common Profiles > Media

2. Provision the media profile options.

   Refer to Table 2-18 for a list of media profile options.

Table 2-18. Media Profile Options

Option	Description
RTP Frame Packetization	Configures the RTP frame packetization time in milliseconds.
Packet Delay Nominal	Sets the allowable limits of latency on the network. This sets the nominal delay time value in increments of 10 milliseconds.
RTP Packet Delay Maximum	Sets the allowable limits of latency on the network. This sets the maximum delay time value in increments of 10 milliseconds.
RTP DTMF Relay	Configures the method by which RTP dial tone multi-frequency (DTMF) events are relayed.
RTP QoS DSCP	Configures the maximum RTP quality of service (QoS) parameters for differentiated services code point (DSCP).
RTP Local Port Min	Configures the starting RTP UDP port used to source RTP from the ONT.
RTP Local Port Max	Configures the starting RTP UDP port used to source RTP from the ONT.
Fax Mode	Switches to passthrough mode on fax or modem tone detection. This command allows modem and fax calls to maintain a connection without altering the signals with the voice improvement settings.

Table 2-18. Media Profile Options (Continued)

Option	Description
Echo Cancellation	Improves voice quality for packetized-based voice calls.
Flash Hook Min	Configures the minimum time the switch hook must be held to be interpreted as a flash.
Flash Hook Max	Configures the maximum time the switch hook must be held to be interpreted as a flash.
Silence Suppression	Enables voice activity detection. When enabled, RTP packets will not be sent during periods of silence.

What's Next

Continue to "Provision the Codec Profile" on page 2-60.

Provision the Codec Profile

CODECs are used to convert an analog voice signal to digitally encoded version. Codecs vary in the sound quality, the bandwidth required, the computational requirements, etc.

1. Navigate to the CODEC menu.

   Services > Voice FTTx > Common Profiles > Codec

2. Provision the CODEC profile options.

   Refer to Table 2-19 for a list of CODEC options.

Table 2-19. CODEC Profile Options

Option	Description
Preference	Specifies the order of preference for coder-decoders used by the CODEC list.
Codec	Specifies the CODEC.

What's Next

- For OMCI SIP continue to "Provision the OMCI SIP Users" on page 2-64.
- For OMCI MGCP continue to "Provision OMCI MGCP Endpoints" on page 2-67

Provision Class of Service (CoS) (Optional)

CoS is an optional provisioning choice that defines the permissions available to a system user for making voice calls. Voice CoS permissions include the type of calls and actions a user can perform.

The default CoS, called DEFAULT_COS, grants permission to place all types of calls is automatically assigned to all voice users.

Creating further CoS entries is only necessary if restrictions are to placed on types of calls the voice user can make.

To create or edit a CoS, complete the following:

1. Access the Class of Service menu.

   Services > **Voice** > **SIP** > **Class of Service**

2. In the Class of Rules, enter a unique rule name.
3. Click **Create**.
4. By default all the Class of Service options are automatically provisioned with the exception of Disable Call Waiting. Use the check box to either allow or disallow the selected service.

   For more details about the available provisioning options, refer to the Total Access 5000 Switch Module User Interface Guide (P/N 65K90SM-31).

5. Click **Apply**.

What's Next

Continue to "Provision for Global Voice (Optional)" on page 2-62.

Provision for Global Voice (Optional)

Global provisioning options are available to set the ONT to perform certain operations, like three-way conferencing, locally.

It is not necessary to change any of these settings if the SIP server is capable of performing them.

To provision the global voice options, complete the following:

1. Access the Global Voice menu.

   Services > **Voice** > **SIP** > **Options**

2. Provision the options. If you are unsure about supported options, contact your network administrator.

   For more details about the available provisioning options, refer to the Total Access 5000 Switch Module User Interface Guide (P/N 65K90SM-31).

What's Next

Continue to "Provision the Voice User" on page 2-63.

Provision the Voice User

The user provisioning process is repeated for each individual customer and is typically as automated as possible. Except for the SIP identity which is unique in the system or network. Each user must be associated with a particular FXS port and registered to a specific SIP trunk.

To provision a user to a particular FXS port and registered to a specific SIP trunk, complete the following:

1. Access the Voice User menu.

   Services > **Voice** > **SIP** > **Voice Users**
2. Enter the user number for this voice user. This is typically the phone number associated with this user.
3. Select the dialing profile to be used by this user. If you did not create a dialing profile, a default profile (DEFAULT_DP) is provided.
4. Select the class of service to be used by this user. If you did not create a CoS, a default rule (DEFAULT_COS) is provided.
5. Enter the SIP identity.

   The parameters should match the SIP identity in the SIP call-router. A common practice is to also user the customer’s phone number here. It is not necessary, however, and the SIP identity can be any string that does not contain the following characters: `@^[]{}\|:<>?" and <space>.
6. Enter the trunk number created previously.
7. Enter the authentication name. This is typically the phone number associated with this user.
8. Enter the authentication password for this user.
9. Enter the index of the FXS slot/port to be associated with this user. Example: 1/2.
10. Click **Apply**.

What’s Next

For Non-OMCI SIP, this completes provisioning. Services should be up and running. To provision another service, continue to “Step 2: Service Provisioning” on page 2-16.

Provision the OMCI SIP Users

All profiles (media, CODEC, call-feature, etc.) can be shared across multiple voice users. To create a SIP user, complete the following steps:

1. Navigate to the Users menu.

   Services > **Voice FTTx** > **SIP** > **Users**

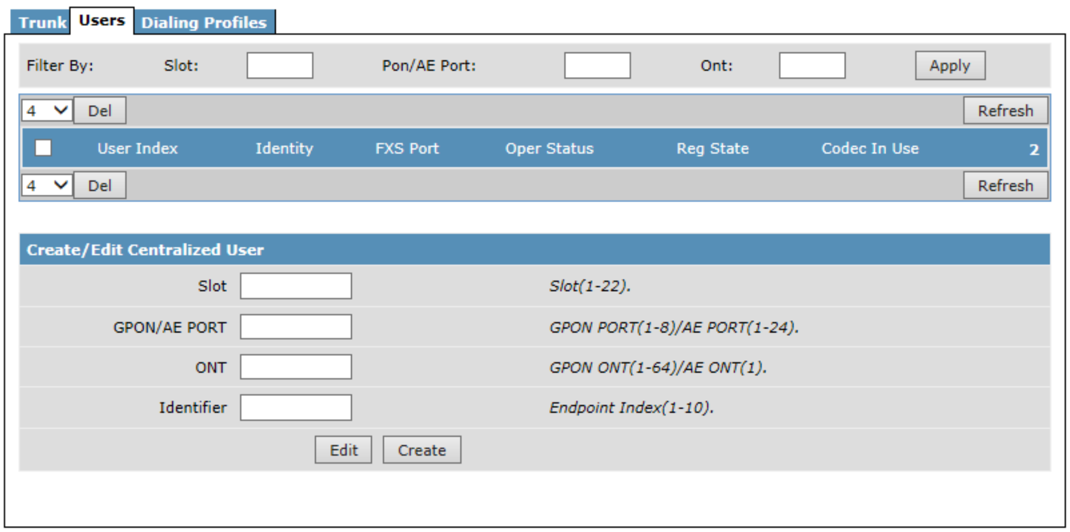


Figure 2-21. SIP User Create

2. Enter the slot number.
3. Enter the GPON/AE port.
4. Enter the ONT.
5. Enter a unique identifier number.
6. Click **Create**. The provision SIP User menu appears.

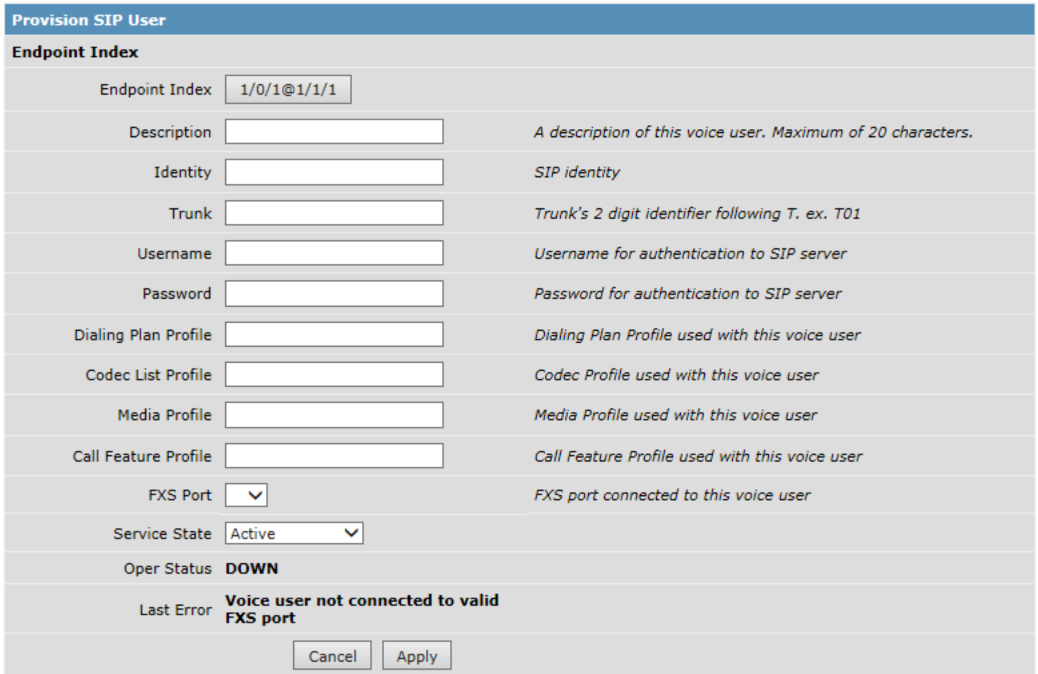


Figure 2-22. SIP User Edit

7. Enter a description for this voice user. This is typically the phone number associated with this user.
8. Enter the SIP identity.
9. It is a common practice to also use the customer's phone number here. It is not necessary, however, and the SIP Identity can be any string that does not contain the following characters: `@^[]{}\|:<>?" and <space>.
10. Enter the trunk number created previously.
11. Enter the username. This is typically the phone number associated with this user.
12. Enter the password for this user.
13. Enter the Dialling Plan Profile to be used for this voice user. ADTRAN provides a default dialing plan profile called DEFAULT_DP.
14. Enter the Codec List Profile to be used for this voice user.

15. Enter the Media Profile to be used for this voice user.
16. Enter the Call Feature Profile to be used for this voice user.
17. Enter the FXS port connected to this voice user.
18. Set the Service State to **Active**.
19. Click **Apply**.

What's Next

For OMCI SIP, this completes provisioning. Services should be up and running. To provision another service, continue to "Step 2: Service Provisioning" on page 2-16.

Provision OMCI MGCP Endpoints

To create the MGCP profile, complete the following:

1. Navigate to the Endpoints menu.

   Services > **Voice FTTx** > **MGCP** > **Endpoints**
2. Enter the slot number.
3. Enter the GPON/AE port.
4. Enter the ONT.
5. Enter a unique identifier number.
6. Click **Create**. The Provision MGCP Endpoint menu appears.
7. Enter the MGCP Profile to be used by this voice user.
8. Enter the Media Profile to be used for this voice user.
9. Enter the Call Feature Profile to be used for this voice user.
10. Enter the FXS port connected to this voice user.
11. Set the Service State to **Active**.
12. Click **Apply**.

What's Next

For OMCI MGCP, this completes provisioning. Services should be up and running. To provision another service, continue to "Step 2: Service Provisioning" on page 2-16.

Provision GR-303

To provision for GR-303, complete the following steps:

1. Access the DS1 Voice Gateway.

   DS1 VG > **Provisioning** > **Card**
2. Set the service state to In Service.
3. Set the Call Control Mode to GR-303.
4. Set the required DS1 ports to In Service.

   DS1 VG > **Provisioning** > **DS1**
5. Assign a name to the interface group.

   DS1 VG > **Provisioning** > **GR-303 > Other Provisioning**
6. Set the switch type.
7. Assign the physical ports, from step 4, being used as the primary, secondary, and normal.

   DS1 VG > **Provisioning** > **GR-303 > Switch DS1s**
8. Set the number of CRVs.

   DS1 VG > **Provisioning** > **GR-303 > Subscribers**
9. Set the Start CRV.
10. Set the Node.
11. Set the Slot.
12. Set the Provisioning Mode to either **GPON** or **Active Ethernet**.
13. Set the start port.
14. Click **Apply**.

What's Next

For GR-303 voice, this completes provisioning. Services should be up and running. To provision another service, continue to "Step 2: Service Provisioning" on page 2-16.

Section 3

Provision Active Ethernet, CLI

Scope of this Section

This section provides the minimum amount of steps required to provision a GPON module for the FTTP application.

NOTE

The provisioning instructions and examples in this guide represent general use cases; they do not address all provisioning scenarios and operator-specific use cases.

In this Section

This section contains the topics listed in Table 3-1.

Table 3-1. Section 3 Topics

Provisioning

Provisioning is done in two steps. Complete the following steps when deploying an FTTP application using the Web GUI.

- "Step 1: OLT/PON Provisioning"
- "Step 2: Service Provisioning" on page 3-5

Step 1: OLT/PON Provisioning

Before you can being provisioning services, it is first necessary to enable the OLT and PON along with discovering the ONT you will be provisioning for triple-play.

Enable the OLT Module

For services to flow properly, it is necessary to ensure the OLT module is set to In Service. To enable the OLT module, complete the following steps:

1. Access the Global Configuration Command Set.

   ```
   ChassisID#configure terminal
   ```

2. Enable the GPON OLT module.

   ```
   ChassisID(config)#no slot shutdown <shelf/slot
   ```

What's Next

- Continue to "Discover the ONT" on page 3-3

Discover the ONT

To discover the ONT, complete the following steps:

1. Access the remote device.

   `ChassisID(config)#`**`remote-device ont <ont-id>@<shelf/slot/port>`**

2. Enable the ONT interface.

   `ChassisID(config-ont ont-id@x/x/x)#`**`no shutdown`**

3. Return to the Global Configuration Command Set.

   `ChassisID(config-ont ont-id@x/x/x)#`**`exit`**

What's Next

- Continue to "ONT Inband Management Provisioning" on page 3-4

ONT Inband Management Provisioning

To provision inband management for an ONT connected to a port on the OLT, complete the following steps:

1. Access the Global Configuration prompt.

   `ChassisID#`**`configure terminal`**

2. Access the Gigabit-Ethernet Interface Configuration prompt.

   `ChassisID(config)#`**`interface gigabit-ethernet <shelf/slot/port>`**

3. Set the S-tag for the subtended host.

   `ChassisID(config-giga-eth x/x/x)#`**`subtended-host s-tag <2-4094>`**

4. Set the S-tag priority for the subtended host.

   `ChassisID(config-giga-eth x/x/x)#`**`subtended-host s-tag-priority <0-7>`**

5. Select the method of inband management.

   Refer to Table 3-2 for the inband management options.

Table 3-2. Inband Management

Inband	Command	Description
Static IP	`ChassisID(config-giga-eth x/x/x)#`**`subtended-host ip address A.B.C.D A.B.C.D`**	Set the static IP address and subnet mask for the ONT's inband management. If selected, continue to step 6
DHCP	`ChassisID(config-giga-eth x/x/x)#`**`subtended-host ip address dhcp`**	Allocate the IP address for the ONT's inband dynamically using DHCP. If selected, continue to step 7

6. If using a static IP address, set the default gateway for the subtended-host.

   `ChassisID(config-giga-eth x/x/x)#`**`subtended-host ip default-gateway A.B.C.D`**

7. Enable the interface.

   `ChassisID(config-giga-eth x/x/x)#`**`no shutdown`**

8. If using a DHCP IP address, view the DHCP address for a AE subtended-host.

   `ChassisID(config-giga-eth x/x/x)#`**`do show interfaces gigabit-ethernet <shelf/slot/pon> subtended-host`**

Step 2: Service Provisioning

The Total Access 5000 FTTP application supports triple-play provisioning via CLI. To begin provisioning services, choose one of the following paths:

- "Voice"
- "Data" on page 3-12
- "Video" on page 3-13

Voice

The Total Access 5000 FTTP application supports Session Initiation Protocol (SIP), Media Gateway Control Protocol (MGCP), and GR-303 voice.

SIP

SIP works in concert with voice and video by enabling and agreeing on characterizations of a session for sharing data. SIP is an application-layer control protocol that can establish, modify, and terminate multimed sessions.

SIP provides two options. The first is provided in the **Voice** menu found under the **Services** option. For purposes of this document, this option is referred to as Non-OMCI. The second option is provided in the **Voice FTTx** menu found under the **Services** option. For purposes of this document, this option is referred to as OMCI.

NOTE

If your deployment uses a Remote Gateway ONT, OMCI (Voice FTTx) is the only supported option.

MGCP

MGCP is a protocol that works hand-in-hand with H.323 and SIP in VoIP services. MGCP works between a call agent or media gateway controller, usually a software switch, and a media gateway with internal endpoints. The media gateway is the network device that converts voice signals carried by telephone lines into data packets carried over the Internet or other packet networks.

MGCP provides two options. The first is provided in the **Voice** menu found under the **Services** option. For purposes of this document, this option is referred to as Non-OMCI. The second option is provided in the **Voice FTTx** menu found under the **Services** option. For purposes of this document, this option is referred to as OMCI.

NOTE

If your deployment uses a Remote Gateway ONT, OMCI (Voice FTTx) is the only supported option.

GR-303

GR-303 is the basic protocol used for POTS service.

NOTE

A Total Access 5000 Voice Gateway Module is required when provisioning GR-303.

Select Your Voice Option

Use Table 3-3 to determine your voice option and navigate to your next step. If you're unsure of your voice option, refer to "Voice" on page 3-5.

Table 3-3. Voice Options

Option	See Page
SIP OMCI Voice	3-7
SIP Non-OMCI Voice	3-8
MGCP OMCI Voice	3-9
MGCP Non-OMCI Voice	3-10
GR-303 Voice	3-11

SIP OMCI Voice

To provision for voice, complete the following steps:

NOTE

This is a general set of instructions to turn up SIP OMCI voice. Optional settings are available. For additional information on these optional settings refer to the applicable documents listed in "Related Online Documentation and Resources" on page Intro-3.

1. "Create an EVC" on page 3-15
2. "Set the Voice Service Mode on the ONT" on page 3-21
3. "Provision the Port on the ONT" on page 3-22
4. "Create an IP Host" on page 3-26
5. "Create an EVC-Map" on page 3-28
6. "Provision the SIP Trunk" on page 3-39
7. "Provision the SIP Dialing Profile" on page 3-43
8. "Provision the OMCI SIP Users" on page 3-59

SIP Non-OMCI Voice

To provision for voice, complete the following steps:

NOTE

This is a general set of instructions to turn up SIP Non-OMCI voice. Optional settings are available. For additional information on these optional settings refer to the applicable documents listed in "Related Online Documentation and Resources" on page Intro-3.

1. "Create an EVC" on page 3-15
2. "Set the Voice Service Mode on the ONT" on page 3-21
3. "Provision the Port on the ONT" on page 3-22
4. "Create an IP Host" on page 3-26
5. "Create an EVC-Map" on page 3-28
6. "Provision the SIP Trunk" on page 3-39
7. "Provision the SIP Dialing Profile" on page 3-43
8. "Provision Class of Service (CoS) (Optional)" on page 3-49
9. "Provision for Global Voice (Optional)" on page 3-50
10. "Provision the Voice User" on page 3-51

MGCP OMCI Voice

To provision for voice, complete the following steps:

NOTE

This is a general set of instructions to turn up MGCP OMCI voice. Optional settings are available. For additional information on these optional settings refer to the applicable documents listed in "Related Online Documentation and Resources" on page Intro-3.

1. "Create an EVC" on page 3-15
2. "Set the Voice Service Mode on the ONT" on page 3-21
3. "Provision the Port on the ONT" on page 3-22
4. "Create an IP Host" on page 3-26
5. "Create an EVC-Map" on page 3-28
6. "Provision the MGCP Profile" on page 3-40
7. "Provision OMCI MGCP Endpoints" on page 3-61

MGCP Non-OMCI Voice

To provision for voice, complete the following steps:

NOTE

This is a general set of instructions to turn up MGCP Non-OMCI voice. Optional settings are available. For additional information on these optional settings refer to the applicable documents listed in "Related Online Documentation and Resources" on page Intro-3.

1. "Create an EVC" on page 3-15
2. "Set the Voice Service Mode on the ONT" on page 3-21
3. "Provision the Port on the ONT" on page 3-22
4. "Create an IP Host" on page 3-26
5. "Create an EVC-Map" on page 3-28
6. "Provision the MGCP Profile" on page 3-40
7. "Provision Non-OMCI MGCP Endpoints" on page 3-41

GR-303 Voice

To provision for voice, complete the following steps:

NOTE

This is a general set of instructions to turn up GR-303 voice. Optional settings are available. For additional information on these optional settings refer to the applicable documents listed in "Related Online Documentation and Resources" on page Intro-3.

1. "Set the Voice Service Mode on the ONT" on page 3-21
2. "Provision the Port on the ONT" on page 3-22
3. "Provision GR-303" on page 3-62

Data

To provision for data, complete the following steps:

NOTE

This is a general set of instructions to turn up data. Optional settings are available. For additional information on these optional settings refer to the applicable documents listed in "Related Online Documentation and Resources" on page Intro-3.

1. "Create an EVC" on page 3-15
2. "Provision the Port on the ONT" on page 3-22
3. "Create an EVC-Map" on page 3-28

Video

To provision for video, complete the following:

NOTE

This is a general set of instructions to turn up video. Optional settings are available. For additional information on these optional settings refer to the applicable documents listed in "Related Online Documentation and Resources" on page Intro-3.

1. "Create an EVC" on page 3-15
2. "Provision the Port on the ONT" on page 3-22
3. "Create an EVC-Map" on page 3-28

TLS

TLS enables the user to tag-switch through the system. The user can send traffic without MAC Security or MAC Limits. Proxy ARP will be disabled as well, so the devices will respond with their own ARP. Using TLS removes the ability to use IGMP replication on this particular port. Since the flow will be tag switched up to the network, the VLANs must be configured in a way that an outer VLAN appears only on a single access module within the entire system. The inner tag (if running double tags) cannot be duplicated within the access module. If the VLAN becomes MAC-switched, TLS no longer functions.

To provision TLS Single Tag, complete the following:

NOTE

This is a general set of instructions to turn up TLS. Optional settings are available. For additional information on these optional settings refer to the applicable documents listed in "Related Online Documentation and Resources" on page Intro-3.

1. "Create an EVC" on page 3-15.
2. "Provision the Port on the ONT" on page 3-22.
3. "Create an EVC-Map" on page 3-28.

Create an EVC

The EVC (Ethernet Virtual Connection) is a centrally managed object defining the properties of a particular S-Tag within a Total Access 5000. The EVC object enables the provisioning of ELINE, E-TREE, and E-LAN applications. EVCs are available for use by all access modules within a shelf.

In a system using an S-VLAN model, each user requires a unique S-VLAN to be tag switched throughout the system. ONTs 1-64 on slot 1 must have different VLANs than users 1-64 on Slot 2.

NOTE

- For Total Access 5000 System Release 7.1 and above, the GPON 4X SFP OLT (P/N 1187502F1) supports up to 64 ONTs per PON. The GPON 2.5G 2-Port Access Module (P/N 1187500E1) and GPON 2.5G 2X SFP Access Module (P/N 1187501G1) support up to 32 ONTs per PON.
- VLANs cannot be duplicated across other nodes.

NOTE

The EVC for SIP/MGCP traffic will be a dedicated EVC because voice traffic requires different Quality of Service (QoS) handling than other data traffic.

NOTICE

- Changing the default IGMP EVC means also changing the default IP IGMP EVC statement for each access module.
- When deleting the default IGMP EVC (IGMP_EVC), ensure that all IGMP-enabled maps associated with the IGMP EVC are disabled as well.

NOTE

- EVC names are case sensitive.
- A default IGMP EVC (IGMP_EVC) is included in the factory default settings, it can be modified and used or deleted.

1. Access the Global Configuration Command Set.

   ChassisID#**configure terminal**

2. Access the EVC Interface Configuration Command Set.

   ChassisID(config)#**evc WORD**

3. Set the S-tag for the EVC.

   ChassisID(config-evc name)#**s-tag <1-4094>**

4. Apply this EVC to the default ethernet interface as a MEN port.

   ChassisID(config-evc name)#**connect men-port default-ethernet**

   The default interface is set in the Switch Module provisioning.

   The commands listed in Table 3-4 can be used to provision the EVC to use a non-default Metro Ethernet Network Interface.

Table 3-4. Non-Default Metro Ethernet Network Interface

Interface	Command
EFM group	`ChassisID(config-evc name)#`**`connect men-port efm-group [<shelf/slot/group>|WORD]`**
Gigabit-Ethernet	`ChassisID(config-evc name)#`**`connect men-port gigabit-ethernet <shelf/slot/group>`**
LAG group	`ChassisID(config-evc name)#`**`connect men-port lag-group <shelf/slot/group>`**

5. Depending on your selected service, enable or disable MAC-Switching.

   The commands listed in Table 3-5 can be used to enable or disable MAC-Switching.

Table 3-5. MAC-Switching

Service	Command	Definition
Voice/Video/Data	`ChassisID(config-evc name)#`**`mac-switched`**	Enabled
Single Tag TLS	`ChassisID(config-evc name)#`**`no mac-switched`**	Disabled

6. If provisioning Single Tag TLS, continue to step 10. For all other services, continue to step 7.
7. Configure the unit to strip the CE-VLAN tag as it is mapped to the EVC in the customer-to-network direction.

   `ChassisID(config-evc name)#`**`no preserve-ce-vlan`**
8. If provisioning for voice or data, skip to step 10. If provisioning for video, set a priority value for the IGMP packets.

   `ChassisID(config-evc name)#`**`subscriber igmp priority <0-7>`**
9. Set the IGMP version.

   V2 is IGMPv2 (RFC 2236). V3 Lite is Lightweight IGMPv3 (RFC 5790).

   `ChassisID(config-evc name)#`**`ip igmp version [v2|v3 lite]`**
10. Enable the EVC.

    `ChassisID(config-evc name)#`**`no shutdown`**
11. Return to the Global Configuration Command Set.

    `ChassisID(config-evc name)#`**`exit`**

    If currently provisioning for video, continue to step 12. If currently provisioning for voice or data, skip to What’s Next.

12. Set the IGMP mode for the GigE SM/access module.

    Refer to Table 3-6 for a list of available subscriber modes.

Table 3-6. Subscriber Modes

Mode	Steps
Proxy	IGMP proxy can be broken down into three functions: ■ Report suppression - Intercepts, absorbs, and summarizes IGMP reports coming from IGMP hosts. IGMP reports are relayed upstream only when necessary, i.e. when the first user joins a multicast group, and once only per multicast group in response to an IGMP query. ■ Last leave - Intercepts absorbs, and summarizes IGMP leaves coming from IGMP hosts. IGMP leaves are relayed upstream only when necessary, i.e. when the last user leaves a multicast group. ■ Query suppression - Intercepts and processes IGMP queries, in such a way that IGMP specific queries are never sent to client ports, and IGMP general queries are relayed only to those clients' ports receiving at least one multicast group. The OLT offers a unique but necessary capability in this respect. TR-156 requires that all IGMP queries be sent over the multicast GEM port. However, the common IGMP processing code of the Total Access 5000 access modules operates per number of ports (or ONTs). The OLT break this TR-156 requirement by only forwarding each proxy agent's query to the intended ONT thereby avoiding an IGMP query storm from causing set top box problems.
Snooping	IGMP snooping is the process of listening to IGMP network traffic. Snooping allows a network switch to listen in on the IGMP conversation between hosts and routers. The switch maintains a map of which links need which multicast streams. These streams can be filtered from the links that do not need them. Snooping allows a switch to only forward multicast traffic to the links that have solicited them. Snooping is not a recommended mode for IGMP.
Transparent	IGMP transparent passes IGMP messages transparently.

```
ChassisID(config)#ip igmp evc WORD <shelf/slot> mode
[proxy|snooping|transparent]
```

NOTE

Ports can be enabled with either snooping or proxy, with additional maps blocking IGMP.

13. Set the IGMP mode for each access module that will carry IGMP traffic.

NOTE

If IGMP processing is enabled, all IGMP-enabled maps in the GPON OLT Access Module must have the same setting.

```
ChassisID(config)#ip igmp evc WORD <shelf/slot> mode
[proxy|snooping|transparent]
```

NOTE

The IGMP EVC for the OLT Slot will not be running until the EVC-Map is created.

14. Repeat step 12 - 13 for each access module that will carry IGMP traffic.
15. If the IGMP mode is set to proxy, complete the following steps:
    a. Set the proxy host IP address.

NOTE

The default proxy host IP address is 0.0.0.0

```
ChassisID(config)#ip igmp evc WORD <shelf/slot> proxy host ip
address A.B.C.D
```

b. Set the proxy last-member-query interval.

The last-member-query interval controls the time-out (in milliseconds) used to detect whether any group receivers remain on an interface after a receiver leaves a group. If a receiver sends a leave-group message, the router sends a group-specific query on that interface. After twice the time specified by this command plus as much as one second longer, if no receiver responds, the router removes that interface from the group and stops sending that group's multicast packets to the interface.

NOTE

The default proxy last-member query interval is 1000.

```
ChassisID(config)#ip igmp evc WORD <shelf/slot> proxy last-member-
query interval <100-65535>
```

c. Set the proxy last-member-query count.

The last-member-query count controls the number of times the last-member-query interval is used.

NOTE

The default proxy last-member query count is 2.

```
ChassisID(config)#ip igmp evc WORD <shelf/slot> proxy last-member-query count <1-255>
```

16. Provision Multicast Content Admission Control (CAC).

The Multicast CAC feature provides the following at a PON-level:

- A provisionable threshold for a multicast bandwidth threshold crossing alarm (TCA). If the multicast bandwidth is above this threshold the alarm is set. Once set, the alarm is cleared when the multicast bandwidth stays below the threshold for at least 5 minutes.
- A provisionable flag to control whether Multicast CAC is enabled or not. If enabled, IGMP joins for new multicast groups are disallowed when the multicast bandwidth is above the threshold.

a. Enable or disable Multicast Content Admission Control (CAC) flag.

```
ChassisID(config)#multicast-cac enable
```

NOTE

Use the no form of this command to disable Multicast CAC.

b. Set the multicast bandwidth threshold for the TCA.

```
ChassisID(config)#thresholds multicast-bandwidth <0-n>
```

NOTE

Use the no form of this command to disable TCA.

The upper limit is technology dependent. If you enter a value that exceeds the upper limit, an error message will indicate the valid rate.

c. Verify the Mutlicast CAC status.

```
ChassisID(config)#do show interfaces gpon <shelf/slot/pon>
```

```
gpon 1/16/1 is UP and Running
  Number of Configured ONTs       : <number>
  Number of Discovering ONTs      : <number>
  Number of Unrecognized ONTs     : <number>
  Number of Operational ONTs      : <number>
  Number of Available HW Resour   : <number>
  Longest Fiber Distance          : <value>
  Shortest Fiber Distance         : <value>
  Oversubscription Allowed        : [true|false]
  Multicast CAC Status            : [accepting|rejecting|disabled]
                                   Downstream          Upstream
```

```
Max Provisionable BW       kbps : value              value
Configured PIR BW          kbps : value              value
Configured Fixed BW        kbps : value              value
Configured Assured BW      kbps : value              value
Available PIR BW           kbps : value              value
Available CIR BW           kbps : value              value
Current PIR BW             kbps : value              value
Current CIR BW             kbps : value              value
```

NOTE

The Number of Available Hardware Resources field displays the remaining number of resources available on the PON.

What's Next

- For SIP or MGCP provisioning, continue to "Set the Voice Service Mode on the ONT" on page 3-21.
- For video, data, or TLS provisioning, continue to "Provision the Port on the ONT" on page 3-22

Set the Voice Service Mode on the ONT

To set the voice service mode, complete the following steps:

1. Access the Global Configuration Command Set.

   ```
   ChassisID#configure terminal
   ```

2. Set the voice service mode for the ONT.

   Refer to Table 3-7 for the selected activation method.

Table 3-7. Discover the ONT

Activation Mode	Command
SIP	ChassisID(config)#**voice protocol ont-id@<shelf/slot/port>.giga-bit-ethernet sip**
MGCP	ChassisID(config)#**voice protocol ont-id@<shelf/slot/port>.giga-bit-ethernet mgcp**
GR-303	ChassisID(config)#**voice protocol ont-id@<shelf/slot/port>.giga-bit-ethernet fxs-signaling**

3. If provisioning OMCI SIP or OMCI MGCP, set the VoIP Config Method.

   Remote Gateways require the use of OMCI.

   a. Access the remote device.

   ```
   ChassisID(config)#remote-device ont <ont-id>@<shelf/slot/port>
   ```

   b. Set the method.

   ```
   ChassisID(config-remote-device ont x@x/x/x)#voip-config method
   [file-retrieval|local-on|omci]
   ```

What's Next

For OMCI SIP, Non-OMCI SIP, OMCI MGCP, Non-OMCI MGCP, or GR-303 provisioning, continue to "Provision the Port on the ONT" on page 3-22.

Provision the Port on the ONT

NOTE

If provisioning data and video on the same port, the ONT port only needs to be enabled once.

Select the Port Type. Use Table 3-8 to determine your port type and navigate to your next step.

Table 3-8. Port Type

Service	Type	See Page
Data/Video	Ethernet	3-23
Voice	FXS	3-24

Ethernet

After selecting Ethernet as the ONT port type, complete the following steps:

1. Access the Ethernet interface of the ONT.

NOTE

The eth-port is the Ethernet port number on the ONT, port is the PON port on the OLT to which the ONT is connected.

```
ChassisID(config)#interface gigabit-ethernet <ont-id/0/eth-
port>@<shelf/slot/port>.gigabit-ethernet
```

2. Set the number of mac addresses allowed.

NOTE

- 16 MAC addresses per ONT are allowed and must be shared by all Ethernet ports on the ONT.
- A value of 0 will actually allow up to 128 MAC addresses to be attributed to the ONT. However, the number of MAC addresses the OLT can support is limited so using more than 16 will severely limit the number of MAC addresses available to other ONTs. No more than 16 static addresses can be configured regardless of the number of MAC addresses allowed by this setting.

```
ChassisID(config-giga-eth x/x/x@x/x/x)#mac limit <0-16>
```

3. Enable the Ethernet interface of the ONT.

```
ChassisID(config-giga-eth x/x/x@x/x/x)#no shutdown
```

4. Return to the Global Configuration Command Set.

```
ChassisID(config-giga-eth x/x/x@x/x/x)#exit
```

What's Next

For video or data provisioning, continue to "Create an EVC-Map" on page 3-28.

FXS

After selecting FXS as the ONT port type, complete the following steps:

1. Access the FXS Interface Configuration Command Set.

   ```
   ChassisID(config)#interface fxs <ont-id/0/fxs-port>@<shelf/slot/
   port>.gigabit-ethernet
   ```

2. Adjust the Tx Gain for the FXS port between -12dB and 6dB.

   ```
   ChassisID(config-fxs x/x/x@x/x/x)#tx-gain <N.N>
   ```

3. Adjust the Rx Gain for the FXS port between -12dB and 6dB.

   ```
   ChassisID(config-fxs x/x/x@x/x/x)#tx-gain <N.N>
   ```

4. Enable the interface.

   ```
   ChassisID(config-fxs x/x/x@x/x/x)#no shutdown
   ```

5. Return to the Global Configuration prompt.

   ```
   ChassisID(config-fxs x/x/x@x/x/x)#exit
   ```

What's Next

- For SIP or MGCP provisioning, continue to "Create an IP Host" on page 3-26.
- For GR-303 provisioning, continue to "Provision GR-303" on page 3-62.

Virtual Gigabit Interface

To provision a virtual gigabit interface, complete the following steps:

1. Access the Virtual Gigabit Ethernet Interface Configuration Command Set.

   ```
   ChassisID(config)#interface virtual-gigabit-ethernet <ont-id/0/
   port>@<shelf/slot/port>
   ```

2. Enable the interface.

   ```
   ChassisID(config-virtualGigabitEthernet x/x/x@x/x/x)#no shutdown
   ```

3. Return to the Global Configuration Command Set.

   ```
   ChassisID(config-virtualGigabitEthernet x/x/x@x/x/x)#exit
   ```

What's Next

For video or data provisioning, continue to "Create an EVC-Map" on page 3-28.

Create an IP Host

Each gateway requires a unique IP address and an EVC-Map to associate the IP address with a particular transport EVC. The EVC, the IP subnet, and any related IP server configurations are typically shared among multiple gateway instances, but can vary.

1. Access the IP Host Configuration Command Set.

   Substitute WORD with an alphanumeric string used to identify the IP Host. If an IP Host with this identifier does not already exist, a new one is created.

NOTE

Only two interface ip-host entities can be created per ONT. Attempts to create more than two will be rejected.

```
ChassisID(config)#interface ip-host WORD ont-id@<shelf/slot/port>
```

2. Select the method of IP host management.

   Refer to Table 3-9 for a list of IP host options.

Table 3-9. IP Host Management

IP Host	Command	Description
Static IP	ChassisID(config-ip-host name ont-id@x/x/x)#**ip address a.b.c.d a.b.c.d**	Set the static IP address and subnet mask for the IP host interface. Continue to step 3.
DHCP	ChassisID(config-ip-host name ont-id@x/x/x)#**ip address dhcp**	Allocate the IP address for this IP host interface dynamically using DHCP. Continue to step 4.

3. If a static IP address is used, assign the IP address of the default gateway.

```
ChassisID(config-ip-host name ont-id@x/x/x)#default-gateway A.B.C.D
```

NOTE

The IP address should be unique in the network.

4. Connect the IP host interface to a SIP or MGCP voice service.

```
ChassisID(config-ip-host name ont-id@x/x/x)#connect service [sip|mgcp]
```

5. Enable the IP host.

```
ChassisID(config-ip-host name ont-id@x/x/x)#no shutdown
```

6. Return to the Global Configuration Command Set.

```
ChassisID(config-ip-host name ont-id@x/x/x)#exit
```

What's Next

For SIP or MGCP provisioning, continue to "Create an EVC-Map" on page 3-28.

Create an EVC-Map

The EVC-Map establishes a connection between the ONT Ethernet Port and the EVC defined, as well as holds C-tag information, if needed. The EVC-Map specifies the criteria required for a particular packet to be classified into the EVC as well as translation parameters for the VLAN ID and P-Bits. The EVC-Map also provides parameters to select how MAC addresses are authenticated and learned.

NOTE

EVC-Map names are case sensitive.

1. Configure the name of the Map that connects to the EVC and the shelf and slot that corresponds to the GPON client.

   ```
   ChassisID(config)#evc-map WORD <shelf/slot>
   ```

2. Set the priority for the traffic. It is recommended that SIP traffic be given a high priority throughout the network. A value of 5 is normally assigned.

   ```
   ChassisID(config-evc-map name x/x)#men-pri <0-7>
   ```

3. Connect the EVC-Map to the UNI port. Use Table 3-10 to determine the type and the command to complete.

NOTE

The eth-port is the Ethernet port # on the ONT, pon-port is the GPON port on the OLT to which the ONT is connected.

Table 3-10. Interface Type

Service	ONT	Type	Command
Data/Video/ TLS	Non-Remote Gateway	Gigabit-Ethernet	`ChassisID(config-evc-map name x/x)# connect uni gigabit-ethernet <ont-id/0/eth-port>@<shelf/slot/pon-port>.gpon`
Voice	All ONTs	IP Host	`ChassisID(config-evc-map name x/x)# connect ip-host WORD <ont-id/0/eth-port>@<shelf/slot/pon-port>`

4. Connect the EVC-Map to the EVC.

   ```
   ChassisID(config-evc-map name x/x)#connect evc WORD
   ```

5. If provisioning for voice or data, skip to step 14. If provisioning for video or TLS, set the subscriber IGMP mode.

NOTE

If provisioning for TLS, the IGMP mode must be set to transparent.

```
ChassisID(config-evc-map name x/x)#subscriber igmp mode
[block|processing-enabled|transparent|forking]
```

6. If provisioning for TLS, skip to step 10. If provisioning for video, continue to step 7.
7. Enable smart immediate leave.

   This function is associated with IGMP snooping or routing whereby the switch or router stops sending immediately the multicast stream when receiving an IGMP leave for the last member on this requesting interface, i.e. without sending one or more group specific queries and waiting for its timeout.

   ```
   ChassisID(config-evc-map name x/x)#subscriber igmp immediate-leave
   ```

8. Set the IGMP proxy router IP address if the host connected to the ONT cares about the IP address for IGMP query messages.

   The default IGMP proxy router IP address is 0.0.0.0

   ```
   ChassisID(config-evc-map name x/x)#subscriber igmp proxy router ip
   address A.B.C.D
   ```

9. If provisioning for video, skip to step 14.

NOTICE

Steps 10 - 14 are only for provisioning TLS. If you are provisioning for voice, video, or data, continue to step 14.

10. Set the DHCP mode to transparent.

    ```
    ChassisID(config-evc-map name x/x)#subscriber access dhcp mode
    transparent
    ```

11. Set the PPPoE mode to transparent.

    ```
    ChassisID(config-evc-map name x/x)#subscriber access pppoe mode
    transparent
    ```

12. Set the ARP mode to transparent.

    ```
    ChassisID(config-evc-map name x/x)#subscriber arp mode transparent
    ```

13. If provisioning for Single TLS, skip to 25.

14. Set the subscriber modes.

    Refer to Table 3-11 for a list of available subscriber modes.

NOTE

PPPoE does not support video services.

Table 3-11. Subscriber Modes

Mode	Steps
DHCPv4	Complete the following steps: 1. Apply DHCP for subscriber authentication for the EVC-Map. `ChassisID(config-evc-map name x/x)#`**`subscriber access dhcp mode authenticate`** 2. Discard PPPoE discovery traffic for the EVC-Map. `ChassisID(config-evc-map name x/x)#`**`subscriber access pppoe mode block`**
DHCPv6	Complete the following: 1. Apply DHCP for subscriber authentication for the EVC-Map. `ChassisID(config-evc-map name x/x)#`**`subscriber access dhcp6 mode authenticate`** For a list of DHCPv6 options refer to Table 3-13. 2. Discard PPPoE discovery traffic for the EVC-Map. `ChassisID(config-evc-map name x/x)#`**`subscriber access pppoe mode block`**
PPPoE	Complete the following steps: 1. Discard DHCP traffic for the EVC-Map. `ChassisID(config-evc-map name x/x)#`**`subscriber access dhcp mode block`** 2. Apply PPPoE for subscriber authentication for the EVC-Map. `ChassisID(config-evc-map name x/x)#`**`subscriber access pppoe mode authenticate`**

NOTE

- The default setting for the DHCPv6 access mode mirrors the DHCPv4 setting, therefore DHCPv6 is enabled by default for all DHCPv4 circuits. To disable DHCPv6 on all existing circuits of an access module enter the following command.

  ```
  ChassisId(config)#force subscriber dhcpv6 disable <shelf/slot>
  ```
- Changing the access mode does not change the relay agent settings. Refer to "Configure the Relay Agent." on page 3-32 for relay agent provisioning steps.

Refer to Table 3-12 for a description of the authentication modes.

Table 3-12. Authentication Mode Description

Authentication Mode	Description
DHCP Processing	Dynamic Host Configuration Protocol (DHCP) is an auto-configuration protocol used to configure network devices in IP networks. A DHCPv4 customer uses the protocol to acquire configuration information such as IP addresses, and default routers from the DHCP server being used by the network. This server maintains all the available IP addresses and configuration information for those addresses in the network. DHCP supports the following options: Authenticate - Indicates that the source and contents of the data will be authorized by DHCP. This can prevent unauthorized access to the network. ADTRAN recommends this option. Block - Indicates that all unauthorized Internet Protocol V4 traffic from unauthorized DHCP users will be blocked. All DHCP messages are blocked from entering the network via this interface mapping. Transparent - Ignores DHCPv4 processing. Snoop - Indicates that any DHCPv4 will be allowed without performing authentication.
PPPoE Processing	Point to Point Protocol over Ethernet (PPPoE) processing is a network protocol for encapsu-lating Point to Point Protocol (PPP) frames inside Ethernet frames. PPPoE is used mainly with Digital Subscriber Lines (DSL) modems over Ethernet. It is also used in Metro Ethernet networks. Because Ethernet networks employ a packet-based data protocol, there is a lack of security to protect against IP and MAC address conflicts. PPPoE establishes a point-to-point connection over the network and then transports data packets between these specific points or interfaces. PPPoE supports the following options: Authenticate - Indicates the MAC address of the subscriber will be authenticated before data is accepted. Block - Indicates that the subscriber will not be authenticated using PPPoE. Transparent - Indicates that no type of authentication will be used and that all PPPoE traffic will be allowed.

Refer to Table 3-13 for a list of available access modes.

Table 3-13. DHCPv6 Access Modes

Access Mode	Command	Description
Authenticate	`ChassisID(config-evc-map name x/x)#` **`subscriber access dhcpv6 mode authenticate`**	Use DHCPv6 for authentication, allow link local IPv6 packets.
Same as DHCPv4	`ChassisId(config-evc-map name x/x)#` **`subscriber access dhcpv6 mode same-as-dhcpv4`**	Mirrors the DHCPv4 authentication Mode. This is the Default mode. ■ If DHCPv4 is set to authenticate, link local IPv6 is allowed and DHCPv6 is used for authentication. ■ If DHCPv4 is set to block, link local IPv6 will also be blocked along with DHCPv6.
Transparent	`ChassisId(config-evc-map name x/x)#` **`subscriber access dhcpv6 mode transparent`**	Ignore DHCPv6 packets. Ignore link local IPv6 packets.
Block	`ChassisId(config-evc-map name x/x)#` **`subscriber access dhcpv6 mode block`**	Discard DHCPv6 packets. Blocks link local IPv6 packets.
Snoop	`ChassisId(config-evc-map name x/x)#` **`subscriber access dhcpv6 mode snoop`**	Process DHCP without performing authentication.

15. Configure the Relay Agent.

    The Total Access 5000 products provide the option to enable a Relay Agent, on an EVC Map, that inserts access loop identification information, in the form of Circuit/Interface ID, Remote ID, and loop characteristic information (as defined in Broadband Forum TR-101), into both DHCPv4 and DHCPv6 packets before forwarding the packets to the DHCP server. This information is used by the DHCP server for authentication purposes.

    DHCPv4 utilizes Option-82 to insert the Circuit ID, Remote ID, and loop characteristics. DHCPv6 utilizes Option-17 to insert a vendor-specific tag containing the loop characteristics, Option-18 to insert the Interface ID (equivalent of DHCPv4 Circuit ID) and Option-37 to insert the Remote ID. The Interface or Circuit ID identifies the access loop logical port on the Total Access 5000 or OSP on which the DHCP message was received. The Remote ID uniquely identifies the user on the access loop on the Total Access 5000 on which the DHCP discovery message was received.

NOTE

Beginning with Total Access 5000 System Release 8.7, the DHCP remote ID is the name of the EVC Map.

The format of the Circuit/Interface ID and Remote ID is a string of variables usually separated by characters (`#` `.` `/` ,etc.) and is limited to 63 total characters. Each variable begins and ends with a dollar sign (**`$`**).

For example, for a circuit in shelf 1, slot 5, port 27, with a VLAN ID of 201. The command below would output the Circuit ID below.

Command:

```
ChassisID(config-evc-map name x/x)#subscriber access dhcp option-82
circuit-id $shelf$/$slot$/$port$/$vid$
```

Circuit ID:

```
1/5/27/201
```

NOTE

- There is only one "remote-id format" storage per EVC Map used for DHCP, DHCPv6 and PPPoE intermediate agent. Changing one of these affects all of the other Remote-id formats on the EVC Map. Enabling remote-id insert on DHCP, DHCPv6 or PPPoE intermediate agent on an EVC map will enable remote-id insert for all services on the EVC Map. DHCP and PPPoE circuit-id and DHCPv6 interface-id format are also shared.
- Enabling loop-characteristic insertion on DHCPv4, DHCPv6, or PPPoE will enable it for all three protocols on that EVC Map.

Table 3-14 lists the variables supported by the Total Access 5000 products and the information inserted into the Circuit/Remote ID for each variable.

Table 3-14. Supported Variables

Variable	Output Description
$accessnodeid$	TID/Chassis-ID if sync enabled; otherwise TID value [1] For Example: TA5000_56
$chassis-id$	TID/Chassis-ID if sync enabled; otherwise chassis-id value [1, 2] For Example: shelf_56
cn	Access node number
$node$	Access node number
$shelf$	Shelf number in the access node
$slot$	Slot number in the shelf
sn	Slot number in the shelf
$port$	Port number is the PON number
ont	ONT number
$ontslot$	ONT Slot number
$ontport$	Port on ONT
vid	VLAN ID on the subscriber interface.
$q-vid$	VLAN ID on the subscriber interface.

Table 3-14. Supported Variables

Variable	Output Description
$pbits$	Ethernet priority bits on the network port interface
map	EVC map name connected to the user sending the DHCP packets [3] For Example: data26map
$serialnumber$	Returns Activated ONT serial number to CIRCUIT-ID and REMOTE-ID fields

1. If TID - System Name Sync is enabled the chassis-id is overwritten with the TID, therefore $accessnodeid$ and $chassis-id$ display equivalent values. If TID - System Name Sync is disabled $accessnodeid$ displays the TID and $chassis-id$ displays the chassis-id.
2. $chassis-id$ is only supported by Total Access 5000 System Release 7.2 forward.
3. map can only be used in the Remote ID.

16. Configure Circuit ID
    a. Enable DHCPv4 Relay Agent. Enabling the Relay Agent inserts the Option-82 Circuit ID.

    `ChassisID(config-evc-map name x/x)#`**`subscriber access dhcp option-82`**

    b. Configure the format of the Circuit ID. Replace WORD in the following command with the Circuit ID. The format of the Circuit ID is a string of variables usually separated by characters (# . / ,etc.). Refer to Table 3-14 on page 3-33 for a list of supported variables.

    `ChassisID(config-evc-map name x/x)#`**`subscriber access dhcp option-82 circuit-id WORD`**

17. Configure the Remote ID
    a. Enable Option 82 Remote ID insertion.

    `ChassisID(config-evc-map name x/x)#`**`subscriber access dhcp option-82 remote-id`**

    b. Configure the format of the Remote ID. The format of the Remote ID is a string of variables usually separated by characters (# . / ,etc.). Refer to Table 3-14 on page 3-33 for a list of supported variables.

    `ChassisID(config-evc-map name x/x)#`**`subscriber access dhcp option-82 remote-id format WORD`**

18. Configure DHCPv6 Relay Agent Insertion

    Configure the DHCPv6 relay agent to insert a custom Circuit ID, a Remote ID and loop characteristics into DHCPv6 packets.

NOTE

DHCPv6 mode must be set to Authenticate, Snoop, or Same-as-DHCPv4.

19. Configure Interface ID
    a. Enable DHCPv6 Relay Agent. Enabling the Relay Agent inserts the Option-18 Interface ID.

    `ChassisID(config-evc-map name x/x)#`**`subscriber access dhcpv6 relay-agent mode enable`**

    or

ChassisID(config-evc-map name x/x)#**subscriber access dhcpv6 relay-agent mode same-as-dhcpv4**

NOTE

Setting the same-as-dhcpv4 option will mirror the provisioned mode of DHCPv4 option-82 relay agent as the effective mode for the DHCPv6 relay-agent.

b. Configure the format of the Interface ID. Replace WORD in the following command with the Interface ID. The format of the Interface ID is a string of variables usually separated by characters (# . / ,etc.). Refer to Table 3-14 on page 3-33 for a list of supported variables.

ChassisID(config-evc-map name x/x)#**subscriber access dhcpv6 relay-agent interface-id format WORD**

20. Configure the Remote ID

a. Enable Option 37 Remote ID insertion.

ChassisID(config-evc-map name x/x)#**subscriber access dhcpv6 relay-agent remote-id insert**

b. Configure the format of the Remote ID. The format of the Remote ID is a string of variables usually separated by characters (# . / ,etc.). Refer to Table 3-14 on page 3-33 for a list of supported variables.

ChassisID(config-evc-map name x/x)#**subscriber access dhcpv6 relay-agent remote-id format WORD**

21. Configure PPPoE Intermediate Agent Insertion

Configure the PPPoE relay agent to insert a custom Circuit ID, a Remote ID and loop characteristics into PPPoE packets.

NOTE

PPPoE mode must be set to Authenticate.

22. Configure Circuit ID.

a. Enable Intermediate Agent, enabling the Intermediate Agent inserts the Circuit ID.

ChassisID(config-evc-map WORD x/x)#**subscriber access pppoe interme-diate-agent**

b. Configure the format of the Circuit ID. Refer to Table 3-14 on page 3-33 for a list of supported variables.

ChassisID(config-evc-map name x/x)#**subscriber access pppoe interme-diate-agent circuit-id WORD**

23. Enable Intermediate Agent Remote ID insertion.

ChassisID(config-evc-map name x/x)#**subscriber access dhcp pppoe intermediate-agent remote-id**

24. Apply any additional EVC-Map configurations.

NOTE

The following configurations listed in Table 3-15 are optional and not required to pass single-tagged traffic.

Table 3-15. Additional EVC-Map Configurations

Option	Command	Description
Static IP	ChassisID(config-evc-map name x/x)#**subscriber access static-ip <subscriber ip> <subscriber mac> <gateway ip> <gateway mac>**	Configures a Static IP on an EVC; the Gateway MAC can be left off and it resolves through ARP or if the MAC is entered as 00:00:00:00:00:00, the MAC resolves through ARP.
S-Tag Priority	ChassisID(config-evc-map name x/x)#**men-pri <0-7>**	Configures the priority level of the criteria for the associated map in the EVC to which the map is connected. When maps are configured for explicit CoS, the P-bit value of the EVC tag for associated frames can always be set to that CoS value.
S-Tag P-Bits	ChassisID(config-evc-map name x/x)#**men-pri inherit**	Configures the S-tag P-bits to the ingress P-bits.
C-Tag P-Bits	ChassisID(config-evc-map name x/x)#**men-c-tag-pri inherit**	Configures the C-tag P-bits to the ingress P-bits.
Double Tag	ChassisID(config-evc-map name x/x)#**men-c-tag <1-4094>**	Configures the inner VLAN tag for this circuit and creates a QinQ-tagged flow towards the network side.
C-Tag Priority	ChassisID(config-evc-map name x/x)#**men-c-tag-pri [<0-7>|inherit]**	Configures the priority level of the MEN C-Tag for the associated map. When maps are configured for explicit CoS, the P-bit value of the MEN C-Tag for associated frames can always be set to that CoS value.

Table 3-15. Additional EVC-Map Configurations (Continued)

Option	Command	Description
Matching CE-VLAN	`ChassisID(config-evc-map name x/x)#`**`match ce-vlan-id <0-4094>`**	Matches the CE-VLAN-ID coming off of the loop.
Matching CE-VLAN Priority	`ChassisID(config-evc-map name x/x)#`**`match ce-vlan-pri <0-7>`**	Configures the ingress matching criteria to include the priority level within the CE VLAN identifier or the map. Use the no form of this command to remove the matching criteria from the map.
Matching Multicast	`ChassisID(config-evc-map name x/x)#`**`match [broadcast|l2cp|multicast|unicast|untagged]`**	Configures the ingress matching criteria to include multicast traffic.
Network Ingress Filter	`ChassisID(config-evc-map name x/x)#`**`network-ingress-filter men-pri <0-7>|list`**	Configures the P-Bit priority (or priorities if more than one P-Bit was provisioned using the LIST command) for traffic entering the network.
MAC OUI	`ChassisID(config-evc-map name x/x)#`**`match source mac-address [xx:xx:xx:xx:xx:xx|xx:xx:xx:xx:xx:xx xx:xx:xx:xx:xx:xx]`**	Allows multiple services to be assigned to the same UNI and be separated by the Organizationally Unique Identifier (OUI) portion of the MAC address.

NOTICE

MAC OUI is only supported for video. If applying MAC OUI to other services, such as data, it can stop that service from functioning properly.

25. Enable the EVC-Map.

```
ChassisID(config-evc-map name x/x)#no shutdown
```

What's Next

- For OMCI SIP and Non-OMCI SIP provisioning, continue to "Provision the SIP Trunk" on page 3-39.
- For OMCI MGCP and Non-OMCI MGCP provisioning, continue to "Provision the MGCP Profile" on page 3-40
- For remote gateway ONT video or data provisioning, continue to
- For non-remote gateway ONT video or data provisioning, this completes provisioning. Services should be up and running. To provision another service, continue to "Step 2: Service Provisioning" on page 3-5.

Provision the SIP Trunk

The SIP trunk is the logical path to the SIP proxy. The attributes configured on the trunk should be compatible with the corresponding parameters on the SIP proxy. If the system defaults match the capabilities and configured options of the SIP proxy, a small amount of trunk provisioning is required.

All voice trunks are shared across the node, so provisioning of a trunk at the GigE SM makes it available to all gateways.

1. Access the SIP Trunk Configuration Command Set.

   Use the **voice sip-trunk <Txx>** command to activate the SIP Trunk Configuration Command Set. <Txx>, in which 'x' represents a number 0-9, is used to identify this trunk. If a trunk with this identifier does not already exist, a new one is created.

   ```
   ChassisID(config)#voice sip-trunk <Txx>
   ```

2. Set the IP address or fully qualified domain name (FQDN) of the primary SIP server to which the trunk will send call-related messages.

   ```
   ChassisID(config-sip-trunk name)#sip proxy primary [A.B.C.D|WORD]
   ```

3. Set the primary SIP registrar full qualified domain name (FQDN) or IP address that is based on the domain naming system (DNS) suffix.

   ```
   ChassisID(config-sip-trunk name)#sip registrar primary A.B.C.D udp <0-
   65535>
   ```

4. Configure the domain name.

   ```
   ChassisID(config-sip-trunk name)#domain WORD
   ```

   If the domain name is configured in the IP host and also in the SIP trunk, then the domain name configured via IP host shall override the domain name configured via trunk for that particular user. For example, if the domain name in the IP host is configured as provider1.telco1.com and the domain name configured in the SIP trunk is configured as provider2.telco2.com, then the domain name for this IP host shall be provider1.telco1.com.

   If the domain name is configured in the SIP trunk profile using FQDNs and the domain name is not defined in the IP host then the domain name for all users shall be the domain name configured in the SIP trunk.

5. If the system defaults match the capabilities and configured options of the SIP proxy, no further provisioning is required.

What's Next

For Non-OMCI and OMCI SIP provisioning, continue to "Provision the SIP Dialing Profile" on page 3-43.

Provision the MGCP Profile

To create the MGCP profile, complete the following:

1. Create the MGCP profile.

   ```
   ChassisID(config)#voice profile mgcp WORD
   ```

2. Specify the primary MGCP call agent host name.

   It is important to identify the call agent to the ONT MGCP Endpoint. Both primary and secondary call agents can be established, but at minimum a primary call agent is required. If a connection with the primary call agent fails, call agents will be tried in the order they are entered in the configuration.

   ```
   TA5K (config-mgcpname)#call-agent primary <IP address>
   ```

What’s Next

- For OMCI MGCP provisioning, continue to “Provision OMCI MGCP Endpoints” on page 3-61.
- For Non-OMCI MGCP provisioning, continue to “Provision Non-OMCI MGCP Endpoints” on page 3-41

Provision Non-OMCI MGCP Endpoints

MGCP endpoints are dedicated FXS ports configured to use MGCP to communicate with a call agent.

To create the MGCP profile, complete the following:

1. Create an endpoint and enter the endpoint configuration.

   The <index> parameter is a numerical value ranging from 1 to 255 that is used to identify the endpoint in the default naming structure.

   Using the no form of this command destroys the specified endpoint, and if necessary, disconnects it from the specified interface.

   `TA300(config)#`**`voice mgcp-endpoint <index>`**

2. Create a textual description of the endpoint.

   Using the no form of this command removes the endpoint's description.

   `TA300(config-mgcp-x)#`**`description WORD`**

3. If required, connect the endpoint to a physical FXS port, rather than a virtual one, on the FTTP ONT product.

NOTE

This command fails if the specified FXS port is already in use on another MGCP endpoint or a configured voice user.

   Using the no form of this command disconnects the endpoint from the physical FXS port and connects it to a virtual port.

   `TA300(config-mgcp-<endpoint>)#`**`connect fxs <slot/port>`**

4. If required, give the endpoint a specific name to be referenced by the call agent.

   By default, when endpoints are created and given an index number, they are named in the following format: aaln/x, where x is the index number.

   `TA300(config-mgcp-<endpoint>)#`**`name WORD`**

5. If required, block caller ID information on an endpoint.

NOTE

This does not affect caller ID delivered in the RTP stream to the FXS port.

   The command blocks caller ID delivery to the connected FXS port, if the caller ID information is presented in the MGCP signaling messages.

   Using the no form of this command allows caller ID information to appear as if it is included in the MGCP message.

   `TA300(config-mgcp-<endpoint>)#`**`block-caller-id`**

6. Specify how long (in milliseconds) the endpoint's battery is removed during a forward disconnect situation.

   In a forward disconnect, the call agent sends a network disconnect (osi), and the specified forward disconnect time matches the battery behavior.

   ```
   TA300(config-mgcp-<endpoint>)#fwd-disconnect delay
   [250|500|750|900|1000|2000|follow-switch]
   ```

   The battery behavior can also be set to follow the Class 5 switch. This depends upon the endpoint's RFC 2833 signaling setting. If the RFC 2833 signaling is enabled, then using the follow-switch parameter means that the Class 5 switch determines the length of time the battery is removed.

7. `TA300(config-mgcp-<endpoint>)#fwd-disconnect delay follow-switch`

What's Next

For Non-OMCI MGCP, this completes provisioning. Services should be up and running. To provision another service, continue to "Step 2: Service Provisioning" on page 3-5.

Provision the SIP Dialing Profile

The Dialing Profile is assigned to voice users, and is used to notify the access modules when to stop collecting digits being dialed and begin connecting a phone call. The dial profile creates and stores number-complete templates.

A number-complete template consists of a pattern of digits used by telephone companies when making calls. A typical template would be 555-XXX-XXX. These templates can be expanded to include Dial Plans, External Line Codes and Special Prefix Patterns.

The access module collects digits and looks for a match against the Dial Plans, External Line Codes and Special Prefix (SPRE) Patterns. When the digits dialed match a number-complete template, the dial-string is immediately sent to the server for routing.

For example, a normal phone number consists of the following template: 555-XXX-XXXX (where “X” is a wild card denoting any digit from 1 to 9). The first three digits are the Area Code Designation, the next three digits are the Phone Exchange Designation, and the last four digits are the Local Number Designation.

When a user initiates a phone call, the access module compares the dialed digits to the number-complete template. If the dialed digits are a match (in this case, three 5s followed by seven other digits) the access module immediately sends the complete dial-string to the server. The server then routes and connects the call.

If the user dials a pattern of digits that does not match any number-complete template, the pattern will still be forwarded to the server after the Inter-digit Timeout has expired. Proper definition of the dial plan is recommended for optimum customer experience. At the very least, emergency numbers should be configured to avoid delays in these calls.

The different types of number-complete templates can be chained together to form longer dial-strings with the use of chaining characters (“&”). For example, if a dialing profile contains an External Line Code "9&", a Special Prefix "*70&" and a Dial Plan "555-XXX-XXXX" and the user dials *70,9,555-123-4567, all the digits will be gathered into a single dial-string and sent to the server when the last digit is entered. An External Line Code will only be matched once during a dialing sequence.

Dial Plan Pattern Restrictions

Dial Plan patterns are entered using the **`dial-plan <type> <PATTERN> [emergency-number] [external-line-code <prohibited|required>]`** command. The following types are supported: 900-number, always-permitted, internal, international, local, national, operator-assisted, specify-carrier, toll-free, user1, user2 and user3. Multiple patterns of the same type are allowed. The pattern must be in the form of a phone number or dialing pattern containing wildcards. Available wildcards are: N=2-9, M=1-8, X=0-9, and [abc]=Any digit contained in the bracketed list. When creating a Dial Plan Pattern, the following rules must be observed:

- Templates must have at least one number or wild card.
- The “(' ')” and “-” characters are allowed, but not inside brackets “[ ]”.
- A “,”is allowed within bracket “[ ]”, but not elsewhere.
- Wild cards (MNX) are not allowed inside brackets “[ ]”.
- Order of numbers is not enforced within brackets “[ ]”.
- The “$” character is allowed, but MUST be the last character in the pattern or standalone.
- If “*” and “#” are entered, they must be the first character in the pattern. They cannot be standalone.

The following are examples of possible Dial Plan patterns:

- For a residential customer:
  - **`dial-plan 900-number 1-900-NXX-XXXX`**
  - **`dial-plan always-permitted 911 emergency-number`**
  - **`dial-plan international 011$`**
  - **`dial-plan local 256-NXX-XXXX`**
  - **`dial-plan local NXX-XXXX`**
  - **`dial-plan national 1-NXX-NXX-XXXX`**
  - **`dial-plan specify-carrier 10-10-XXX$`**
  - **`dial-plan toll-free 1-800-NXX-XXXX`**
  - **`dial-plan toll-free 1-888-NXX-XXXX`**
  - **`dial-plan toll-free 1-877-NXX-XXXX`**
  - **`dial-plan user1 [23456]11`**
- For a business customer (using an external line code):
  - **`dial-plan 900-number 1-900-NXX-XXXX external-line-code required`**
  - **`dial-plan always-permitted 911 emergency-number`**
  - **`dial-plan internal MXXX external-line-code prohibited`**
  - **`dial-plan international 011$ external-line-code required`**
  - **`dial-plan local 256-NXX-XXXX external-line-code required`**
  - **`dial-plan local NXX-XXXX external-line-code required`**
  - **`dial-plan national 1-NXX-NXX-XXXX external-line-code required`**
  - **`dial-plan specify-carrier 10-10-XXX$ external-line-code required`**
  - **`dial-plan toll-free 1-800-NXX-XXXX external-line-code required`**
  - **`dial-plan toll-free 1-888-NXX-XXXX external-line-code required`**
  - **`dial-plan toll-free 1-877-NXX-XXXX external-line-code required`**
  - **`dial-plan user1 [23456]11 external-line-code required`**

SPRE Pattern Restrictions

SPRE patterns are entered using the **`spre <PATTERN> [tone <dial|stutter-dial>]`** command. SPRE Pattern creates special code numbers required to access voice services. A SPRE Pattern must be in the form of a special prefix (spre) code or dialing pattern containing wild cards. Available wild cards are: N=2-9, M=1-8, X=0-9 [abc] = any digit contained within the bracket list. The pattern can end with a chaining character ("&" or "$") which allows for the collection of more digits before the dial string is sent to the server. Ending the pattern with "&" causes the server to continue to look for another number-complete template (dial plan, external line-code or special prefix pattern) following the SPRE code. Ending it with "$" causes the access module to stop attempting to match additional inputs. However, digits will continue to be collected until after the Inter-Digit time out occurs.The following rules must be observed:

- The Template must begin with an "*" or "#". An "*" and "#" are not allowed elsewhere in the Template.
- The Template must have at least one number.

- The characters "("") and "-" are allowed, but not inside "[ ]".
- Do not use "," or "" inside "[ ]".
- Wild cards (MNX) are not allowed inside "[ ]".
- The characters "&" and "$" are allowed but must be the last character and cannot be a standalone.

The following are examples of possible SPRE Patterns:

- **`spre *3XX`**
- **`spre *6[37]&`**
- **`spre *72& tone stutter-dial`**
- **`spre *82&`**
- **`spre *9[02]& tone stutter-dial`**
- **`spre *7[45]$`**
- **`spre *[56789]X`**

External Line Code Restrictions

External Line Codes are entered using the **`external-line-code <PATTERN> [tone <dial|stutter-dial>]`** command. An External Line Code must be in the form of a dialing pattern without wild cards. For example, if a user must first dial "8" to obtain an outside line, the entry would be "8&" where the ampersand tells the server that the "8" designates an outside number and to expect more digits in the number-complete template. The pattern can end with a chaining character ("&" or "$"), which allows for collection of more digits before the dial string is sent to the server. Ending the pattern with a "&" causes the server to continue to look for another number-complete template (dial plan or special prefix pattern) following the external line code. An external line code will only be matched once. Ending the pattern with a "$" causes the access module to stop attempting to match additional inputs. However, digits will continue to be collected until after the Inter Digit time out occurs. The following rules must be observed:

- Template must have at least one number (i.e., 0-9).
- Wild cards are not allowed.
- If "*" and "#" are entered, they must be the first character. They cannot be standalone.
- The characters "&" or "$" are allowed but must be the last character and cannot be standalone.

The following is an example of a possible External Line Code:

- **`external-line-code 8& tone dial`**

Dial Plan Provisioning

To provision the dial plan, complete the following:

1. Access the Global Configuration Command Set.

   ChassisID#**configure terminal**

2. Create or modify a dialing profile.

   ChassisID#**voice profile dialing WORD**

3. Provision the dial-plan options.

   ChassisID(config-dialing-profile WORD)#**dial-plan <type> <pattern> [emergency-number] [external-line-code <required|prohibited>]**

   Refer to Table 3-16 for a list of dial plan options.

Table 3-16. Dial Plan Options

Syntax	Description
type	The following options are available: ■ **always-permitted** – Always Permitted ■ **internal** – Internal Calls ■ **national** – National Calls ■ **toll-free** – Toll Free Calls ■ **900-number** – 900 Number Calls ■ **international** – International Calls ■ **operator-assisted** – Operator Assisted Calls ■ **specify-carrier** – Carrier Specified ■ **user1** – Match User 1 ■ **user2** – Match User 2 ■ **user3** – Match User 3
emergency-number	Emergency Number designates whether this Dial Plan is designated as an Emergency Service. When **Enabled**, this number is designated as an Emergency Service number. For example, "911" is typically reserved as an Emergency Number. Emergency Numbers can be assigned special behaviors not normally found in other calls. For more information, refer to the **voice emergency-number onhook [inhibit|allow]** command in the "Provision the Call Feature Profile (Optional)" on page 3-56.

Table 3-16. Dial Plan Options (Continued)

Syntax	Description
external-line-code	External Line Code describes the behavior of this Dial Plan when an External Line Code is present. The External Line Code should be used when a customer subscribes to the "Hosted PBX", "Centrex" or "Business Group" feature on the server. The External Line Code option identifies whether a Dial Plan Pattern is expected to follow the dialing of an External Line code, which allows for the identification of what would otherwise be contradictory dial plans. The following options are available: ■ Prohibited – Prohibited indicates that this number-complete template will not be matched if an External Line Code has been previously dialed. For example, a user inside a company is trying to connect with another employee inside the same company by dialing an internal four-digit extension number using the pattern "MXXX"; if the user first dials an "8" and then the employee's extension, the pattern will not be matched allowing more digits to be dialed. If the Prohibited option had not been set, the dial string would have been sent to the server as soon as the four digits were entered. This would have been an invalid number and would also prevent longer, external numbers from being dialed.The Prohibited options instructs the server to complete the number dialed only if an external line code is not dialed. This would be of particular importance if some of the employee extensions could be confused with outside numbers (i.e., extension 4111, or 9112). ■ Required – Required indicates that this number-complete template will only be matched if an External Line Code has been previously dialed. For example, if a Dial Plan pattern of "555-XXX-XXXX" is defined as a local number, it will only be matched (and immediately sent in the dial string to the server) if the user first dials the external line code (i.e., "8" for these examples).

NOTE

- To support ten-digit and seven-digit local dialing simultaneously, either the ten-digit dial plan must contain the area code (256-XXX-XXXX, for example) or the seven-digit dial plan should not be specified. If the seven-digit dial plan is not specified, the user will have to wait for the inter-digit timeout to expire before the call will be connected.
- When the external-line-code option is not specified, an external line code is considered optional. This indicates that this number-complete template will be matched regardless of whether or not an External Line Code is present. For example, assume that in order to get to a phone connection outside of a business, the user first must dial "8". If a Dial Plan pattern of "991" is defined with the External Line Code set to "Optional", a user could get an Emergency Operator (911) either by dialing "8911" or "911".

4. Set the star codes for this number (call forwarding, automatic recall, etc).

   ```
   ChassisID(config-dialing-profile WORD)#voice spre *XX
   ```

   Refer to Table 3-17 for a list of SPRE options.

Table 3-17. SPRE Options

Syntax	Description
tone	Specifying a Tone causes the access module to generate a call progress tone after the number-complete template is matched, and before further digits are entered. A tone can only be specified if the SPRE pattern ends with a chaining character. For example, a “&” or a “$” character. The following options are possible: ■ Dial – Dial indicates a constant dial tone is heard. ■ Stutter – Stutter indicates an intermittent dial tone is heard.

5. If this profile is for customers that support the "Hosted-PBX", "Centrex" or "Business Group" feature, specify an external line code.

   ```
   ChassisID(config-dialing-profile WORD)#external-line-code <pattern>
   [tone <dial|stutter-dial>]
   ```

   Refer to Table 3-18 for a list of External Line Code options.

Table 3-18. External Line Code Options

Syntax	Description
tone	Specifying a Tone causes the access module to generate a call progress tone after the number-complete template is matched, and before further digits are entered. A tone can only be specified if the SPRE pattern ends with a chaining character. For example, an “&” or a “$” character. The following options are possible: ■ Dial – Dial indicates a constant dial tone is heard. ■ Stutter – Stutter indicates an intermittent dial tone is heard.

What’s Next

- For OMCI SIP provisioning, continue to “Provision the Media Profile (Optional)” on page 3-52.
- For Non-OMCI SIP provisioning, continue to “Provision Class of Service (CoS) (Optional)” on page 3-49

Provision Class of Service (CoS) (Optional)

CoS is an optional provisioning choice that defines the permissions available to a system user for making voice calls. Voice CoS permissions include the type of calls and actions a user can perform.

The default CoS, called DEFAULT_COS, grants permission to place all types of calls is automatically assigned to all voice users.

Creating further CoS entries is only necessary if restrictions are to placed on types of calls the voice user can make.

To create or edit a CoS, complete the following:

1. Access the Voice CoS Command prompt.

   Use the voice class-of-service WORD command to activate the Voice CoS Command Set. Substitute WORD with an alphanumeric string used to identify this CoS. If a CoS with this identifier does not already exist, a new one is created.

   `TA300(config)#`**`voice class-of-service WORD`**

2. If required, apply any necessary calling restrictions.

   All types are enabled by default, so only “no” commands need be entered into a new CoS entity (to deny permission to that call type). Almost all dial plan types are accepted: 900-number, internal, international, local, national, operator-assisted, specify-carrier, toll-free, user1, user2 and user3. Dial plan type always-permitted cannot be denied. In addition, the [no] call-privilege all command can be used to turn on (or off) all permissions at once.

   `TA300(config-cos name)#`**`[no] call-privilege <type>`**

3. Return to the Global Configuration prompt.

   `TA300(config-cos name)#`**`exit`**

4. Access the Voice User Command prompt.

   Substitute NUMBER:20 with a number less than 20 digits long used to identify this user. Generally, the user's phone number is entered here, but it is not necessary. If a User with this identifier does not already exist, a new one is created.

   `TA300(config)#`**`voice user <number>`**

5. Connect the voice user to the new class of service.

   Substitute WORD with the alphanumeric string used to identify the voice class-of-service entity created in step 1.

   `TA300(config-user name)#`**`cos <name>`**

6. Return to the Global Configuration prompt.

   `TA300(config-user name)#`**`exit`**

   Repeat steps 4 - 6 for all voice users to whom the calling restrictions apply.

What’s Next

Continue to “Provision for Global Voice (Optional)” on page 3-50.

Provision for Global Voice (Optional)

Global provisioning options are available to set the ONT to perform certain operations, like three-way conferencing, locally.

It is not necessary to change any of these settings if the SIP server is capable of performing them.

To provision the global voice options, complete the following:

1. Set the flashhook mode.

   This command determines if flashhook events will be interpreted locally or will be forwarded to the far end.

   TA300(config)#**voice flashhook mode [interpreted|transparent]**

2. If the flashhook mode is set to interpreted, set the voice conference mode.

   This command determines if voice conferencing bridging will be handled within the unit or from a far-end conferencing server.

   TA300(config)#**voice conference mode [local|network]**

3. If the voice conference mode is set to local, specify the actions performed if the conference originator issues a flashhook once the conference has been established.

   The following options are available:

   - The drop option specifies that the last party added to the 3-way conference will be dropped and the call will continue between the two remaining parties.
   - The ignore option specifies that the flashhook will be ignored. The 3-way conference will continue without interruption.
   - The split option specifies that the 3-way conference will be split into two calls, one between the originator and the first party and one between the originator and second party. When additional flashhooks are issued after the split, they will toggle the originator between the two calls.

   TA300(config)#**voice conference local originator flashhook [drop|ignore|split]**

4. Configure a global starting User Datagram Protocol (UDP) port for Realtime Transport Protocol (RDP).

   Each Access Module in the shelf will use the same starting UDP port. The default port is 10000.

   TA300(config)#**ip rtp udp <1026-60000>**

What's Next

Continue to "Provision the Voice User" on page 3-51.

Provision the Voice User

The user provisioning process is repeated for each individual customer and is typically as automated as possible. Except for the SIP identity which is unique in the system or network. Each user must be associated with a particular FXS port and registered to a specific SIP trunk.

To provision a user to a particular FXS port and registered to a specific SIP trunk, complete the following:

1. Access the Voice User Command prompt.

   Substitute NUMBER:20 with a number less than 20 digits long used to identify this user. Generally, the user's phone number is entered here, but it is not necessary. If a User with this identifier does not already exist, a new one is created.

   ```
   TA300(config)#voice user <NUMBER>
   ```

2. Specify the physical port on the selected access module which the user is associated.

   ```
   TA300(config-user name)#connect fxs 2/<port>
   ```

3. Set the SIP identity.

   The WORD parameter should match the SIP Identity in the SIP call-router. Also a common practice to use the customer's phone number here. It is not necessary, however, and the SIP Identity can be any string that does not contain the following characters: `@^[]{}\|:<>?" and <space>. The <Txx> parameter identifies the trunk that this user should use to contact the SIP server.

   The auth-name and password parameters are optional.

   ```
   TA300(config-user name)#sip-identity <station> <Txx> register auth-name
   <username> password <password>
   ```

4. Return to the Global Configuration prompt.

   ```
   TA300(config-user name)#exit
   ```

What's Next

For Non-OMCI SIP, this completes provisioning. Services should be up and running. To provision another service, continue to "Step 2: Service Provisioning" on page 3-5.

Provision the Media Profile (Optional)

The media profile is created in the Total Access 5000 to provision the Realtime Transport Protocol (RTP) parameters on the access module/remote device.

1. Access the Media Profile Command Set.

   TA5K(config)#**voice profile media WORD**

2. Provision the media profile options.

   Refer to Table 3-19 for a list of media profile options.

Table 3-19. Media Profile Options

<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td>TA5K(config-media-profile name)#rtp frame-packetization [10|20|30]</td><td>Use this command to configure the RTP frame packetization time in milliseconds.</td></tr>
<tr><td>TA5K(config-media-profile name)#rtp packet-delay nominal <0-240></td><td>Use this command to set the allowable limits of latency on the network. This sets the nominal delay time value in increments of 10 milliseconds.</td></tr>
<tr><td>TA5K(config-media-profile name)#rtp packet-delay maximum <40-320></td><td>Use this command to set the allowable limits of latency on the network. This sets the maximum delay time value in increments of 10 milliseconds.</td></tr>
<tr><td>TA5K(config-media-profile name)#rtp dtmf-relay enable</td><td>Use this command to configure the method by which RTP dial tone multi-frequency (DTMF) events are relayed.</td></tr>
<tr><td>TA5K(config-media-profile name)#rtp qos dscp <0-63></td><td>Use this command to configure the maximum RTP quality of service (QoS) parameters for differentiated services code point (DSCP).</td></tr>
<tr><td>TA5K(config-media-profile name)#rtp local-port [<1026-60000>|RANGE]</td><td>Use this command to configure the starting RTP UDP port used to source RTP from the ONT.</td></tr>
<tr><td>TA5K(config-media-profile name)#fax mode modem-passthrough</td><td>Use this command to switch to passthrough mode on fax or modem tone detection. This command allows modem and fax calls to maintain a connection without altering the signals with the voice improvement settings.</td></tr>
</table>

Table 3-19. Media Profile Options (Continued)

Command	Description
`TA5K(config-media-profile name)#`**`echo cancellation enable`**	Use this command to improve voice quality for packetized-based voice calls.
`TA5K(config-media-profile name)#`**`flashhook threshold [<40-1550>|RANGE]`**	Use this command to configure the minimum and maximum time the switch hook must be held to be interpreted as a flash.
`TA5K(config-media-profile name)#`**`voice-activity-detection enable`**	Use this command to enable voice activity detection. When enabled, RTP packets will not be sent during periods of silence.

What's Next

Continue to "Provision the CODEC Profile (Optional)" on page 3-55

Provision the CODEC Profile (Optional)

CODECs are used to convert an analog voice signal to digitally encoded version. Codecs vary in the sound quality, the bandwidth required, the computational requirements, etc.

1. Access the CODEC Profile Command Set.

   `TA5K(config)#`**`voice profile codec-list WORD`**

2. Provision the CODEC profile options.

   Refer to Table 3-20 for a list of CODEC options.

Table 3-20. CODEC Profile Options

Command	Description
`TA5K(config-codec-list-profile name)#`**`preference <1-3> codec [g711alaw|g711ulaw|g722|g729]`**	Use this command to specify the order of preference for coder-decoders used by the CODEC list.

What's Next

Continue to "Provision the Call Feature Profile (Optional)" on page 3-56.

Provision the Call Feature Profile (Optional)

Call feature options are available to set the access module/remote device to perform certain operations, like three-way conferencing, locally. It is not necessary to change any of these settings if the SIP server is capable of performing them.

1. Access the Call Feature Command Set.

   `TA5K(config)#`**`voice profile call-feature WORD`**

2. Provision the call feature profile options.

   Refer to Table 3-21 for a list of call feature options.

Table 3-21. Call Feature Profile Options

<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td>TA5K(config-call-feature name)#feature-mode network</td><td>Use this command to determine if voice conferencing bridging will be handled within the unit or from a far-end conferencing server.</td></tr>
<tr><td>TA5K(config-call-feature name)#conference local originator flashhook [drop|ignore|split]</td><td>Use this command if the voice conference mode is set to local, specify the actions performed if the conference originator issues a flashhook once the conference has been established.
The following options are available:
■ The drop option specifies that the last party added to the 3-way conference will be dropped and the call will continue between the two remaining parties.
■ The ignore option specifies that the flashhook will be ignored. The 3-way conference will continue without interruption.
■ The split option specifies that the 3-way conference will be split into two calls, one between the originator and the first party and one between the originator and second party. When additional flashhooks are issued after the split, they will toggle the originator between the two calls.</td></tr>
<tr><td>TA5K(config-call-feature name)#timeouts alerting <0-60></td><td>Use this command to specify the maximum time a call is allowed to remain in the alerting state. The shorter of this timeout or the configured maximum number of rings will determine how long a call is allowed to ring.</td></tr>
<tr><td>TA5K(config-call-feature name)#timeouts interdigit <1-16></td><td>Use this command to specify the maximum time allowed between dialed digits.</td></tr>
<tr><td>TA5K(config-call-feature name)#transfer-on-hangup enable</td><td>Use this command to enable transfer on hangup. When transferring a call, hanging up initiates the transfer to the destination party.</td></tr>
<tr><td>TA5K(config-call-feature name)#call-waiting enable</td><td>Use this command to enable call waiting on the subscriber port.</td></tr>
<tr><td>TA5K(config-call-feature name)#caller-id-inbound enable</td><td>Use this command to allow inbound caller ID to this endpoint.</td></tr>
<tr><td>TA5K(config-call-feature name)#caller-id-outband enable</td><td>Use this command to allow outband caller ID from this endpoint.</td></tr>
<tr><td>TA5K(config-call-feature name)#conference [enable|local]</td><td>Use this command to allow the initiation of three-way conference calls. This feature allows multiple parties to communicate at the same time on the same line.</td></tr>
</table>

Table 3-21. Call Feature Profile Options (Continued)

Command	Description
TA5K(config-call-feature name)#**emergency-number onhook [inhibit|allow]**	Use this command to determine if an Emergency call will be dropped or remain open when the call originator goes on-hook. The following options are available: ■ If set to allow, the call will be dropped if the call originator hangs up. This is the default mode. ■ If set to inhibit, the call will remain open until the Emergency Operator terminates the call. While the call is held-up, the local phone will ring and the Emergency Operator will hear a ringback tone.
TA5K(config-call-feature name)#**emergency-number ringing-timeout <1-60>**	Use this command to set the maximum duration, in minutes, an inhibited call may remain open by an Emergency Operator.

What's Next

Continue to "Provision the OMCI SIP Users" on page 3-59.

Provision the OMCI SIP Users

All profiles (media, CODEC, call-feature, etc.) can be shared across multiple voice users. To create a SIP user, complete the following steps:

1. Access the SIP Voice User Command Set.

   TA5K(config)#**voice user sip <ont-id/0/[1-16]>@<shelf/slot/port>**

2. Assign a description for the voice user.

   TA5K(config-voice-user-sip x/x/x@x/x/x)#**description WORD**

3. Connect the voice user to one or more profiles.

   Refer to Table 3-22 for a list of connection options.

Table 3-22. SIP Voice User Options

Profile	Command
CODEC	TA5K(config-voice-user-sip x/x/x@x/x/x)#**connect profile codec-list WORD**
Dialing	TA5K(config-voice-user-sip x/x/x@x/x/x)#**connect profile dialing WORD**
Call Feature	TA5K(config-voice-user-sip x/x/x@x/x/x)#**connect profile call-feature WORD**
Media	TA5K(config-voice-user-sip x/x/x@x/x/x)#**connect profile media WORD**

4. Connect the SIP voice user to the FXS port.

   TA5K(config-voice-user-sip x/x/x@x/x/x)#**connect fxs <ont-id/0/fxs_Port>@<shelf/slot/port>**

5. Assign an identity (phone number) for the SIP voice user.

   TA5K(config-voice-user-sip x/x/x@x/x/x)#**identity <value>**

6. Specify the SIP trunk through which to register the server. The trunk is specified in the format Txx.

   TA5K(config-voice-user-sip x/x/x@x/x/x)#**sip-trunk Txx**

7. Set the user name that will be required as authentication for registration to the SIP server.

   TA5K(config-voice-user-sip x/x/x@x/x/x)#**auth-name <value>**

8. Set the password that will be required as authentication for registration to the SIP server.

   TA5K(config-voice-user-sip x/x/x@x/x/x)#**password <value>**

9. Enable the SIP voice user.

   TA5K(config-voice-user-sip x/x/x@x/x/x)#**no shutdown**

10. Verify the parameters of the SIP user.

    If mandatory parameters are missing, there is conflicting configuration, or the ONT returns an error while provisioning, last error string displays the appropriate cause of error and puts the voice user in operationally down state. For example if no FXS port is connected to a SIP voice user, it operationally goes down and displays informative message in last error.

```
TA5K(config-voice-user-sip x/x/x@x/x/x)#do show voice user sip <RD_ID/
0/[1-16]@<shelf/slot/port>
```

```
voice user sip 1/0/1@1/16/1 is IS and DOWN
  Description              :
  Subscriber Identity      : 3012001635
  Fxs Connection           : 1/0/10@1/16/1
  Registration State       : Init
  Codec in Use             : na
  Session                  : Idle
  Last error               : Voice user not connected to valid FXS port
```

11. Check the status of all SIP voice users running on a card.

```
TA5K(config-voice-user-sip x/x/x@x/x/x)#do show table voice user sip
<shelf/slot/port>
```

```
Subscriber    End-point      Admin   Oper    Registration
Identity      Index          State   State      State        Session
----------    -----------    ------  ------   --------     --------
3012001635     1/0/1@1/16/1    IS      DOWN        na           na
```

What's Next

- For OMCI SIP, this completes provisioning. Services should be up and running. To provision another service, continue to "Step 2: Service Provisioning" on page 3-5.
- To provision for shapers, continue to Appendix C, "Traffic Management"

Provision OMCI MGCP Endpoints

To create the MGCP endpoints, complete the following:

1. Access the Voice User Command Set.

   ChassisID(config)#**voice user mgcp <ont-id/0/[1-16]>@<shelf/slot/port>**

2. Specify the physical port on the selected Access Module to which the user is associated.

   ChassisID(config-voice user-mgcp x/x/x@x/x/x)#**connect fxs <ont-id/0/fxs-port>@<shelf/slot/port>**

3. Connect the MGCP voice user to the MGCP profile.

   ChassisID(config-voice user-mgcp x/x/x@x/x/x)#**connect profile mgcp WORD**

4. Enable the VOIP user.

   ChassisID(config-voice user-sip x/x/x@x/x/x)#**no shutdown**

5. Return to the Global Configuration Command Set.

   ChassisID(config-voice user-sip x/x/x@x/x/x)#**exit**

What's Next

For OMCI MGCP, this completes provisioning. Services should be up and running. To provision another service, continue to "Step 2: Service Provisioning" on page 3-5.

Provision GR-303

To provision for GR-303, complete the following steps:

NOTE

GR-303 is a function of the DS1 Voice Gateway Access Module.

1. Access the Global Configuration Command Set.

   ```
   ChassisID#configure terminal
   ```

2. Access the GR-303 Interface Configuration Command Set.

   ```
   ChassisID(config)#interface gr303-group <shelf/slot/group>
   ```

3. Assign a name to the interface group.

   ```
   ChassisID(config-gr303-group x/x/x)#description LINE
   ```

4. Set the switch-type.

   ```
   ChassisID(config-gr303-group x/x/x)#switch-type [gte-gtd5|lucent-
   5ess|metaswitch|nortel-dms|siemens-ewsd]
   ```

5. Assign the required physical ports being used as the primary, secondary, and any other GR-303 links.

   a. Set the physical port being used as the primary GR-303 link.

   ```
   ChassisID(config-gr303-group x/x/x)#connect interface t1 <shelf/
   slot/port> primary
   ```

   b. Set the physical port being used as the secondary GR-303 link.

   ```
   ChassisID(config-gr303-group x/x/x)#connect interface t1 <shelf/
   slot/port> secondary
   ```

   c. Set the physical port being used as the normal GR-303 link.

   ```
   ChassisID(config-gr303-group x/x/x)#connect interface t1 <shelf/
   slot/port> normal <3-28>
   ```

   d. Repeat step c to assign the next GR-303 link.

NOTE

The ordering is important. The port of the voice switch and port of the DS1 Voice Gateway assigned to the same GR-303 link must be physically connected.

6. Connect the Call Reference Value (CRV) to the FXS interface.

   ```
   ChassisID(config-gr303-group x/x/x)#connect interface crv <1-2048>
   interface fxs <1/0/fxs port>@<shelf/slot/port>.gigabit-ethernet
   ```

7. Return to the Global Configuration Command Set.

```
ChassisID(config-gr303-group x/x/x)#exit
```

What's Next

For GR-303 voice, this completes provisioning. Services should be up and running. To provision another service, continue to "Step 2: Service Provisioning" on page 3-5.

Section 4

Provision Active Ethernet, Web

Scope of this Section

This section provides the minimum amount of steps required to provision a GPON module for the FTTP application.

NOTE

The provisioning instructions and examples in this guide represent general use cases; they do not address all provisioning scenarios and operator-specific use cases.

In this Section

This section contains the topics listed in Table 4-1.

Table 4-1. Section 4 Topics

Provisioning

Provisioning is done in two steps. Complete the following steps when deploying an FTTP application using the Web GUI.

- "Step 1: OLT/PON Provisioning"
- "Step 2: Service Provisioning" on page 4-5

Step 1: OLT/PON Provisioning

Before you can being provisioning services, it is first necessary to enable the OLT and PON along with discovering the ONT you will be provisioning for triple-play.

Enable the OLT Module

For services to flow properly, it is necessary to ensure the OLT module is set to In Service. To enable the OLT module, complete the following steps:

1. Navigate to the OLT Card Provisioning menu.

   Modules > **AE** > **Provisioning** > **Card**

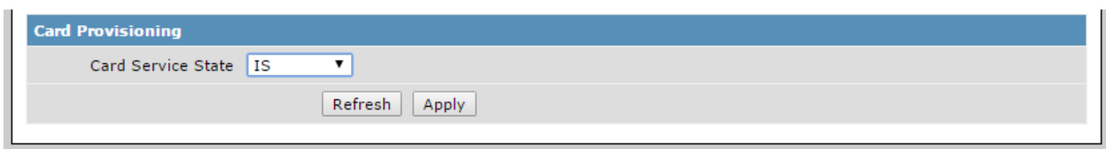


Figure 4-1. OLT Card Service Provisioning

2. Set the card service state to **IS**.
3. Click **Apply**.

Discover the ONT

For services to flow properly, it is necessary to ensure the selected PON is set to In Service. It is at this stage that you will also need to choose the Activation Method of the ONT. To enable the PON, complete the following steps:

NOTE

This is a general set of instructions to provision the PON. Optional settings are available. For additional information on these optional settings refer to the applicable documents listed in "Related Online Documentation and Resources" on page Intro-3.

1. Navigate to the Active Ethernet GE Provisioning menu.

   Modules > AE > Provisioning > GE

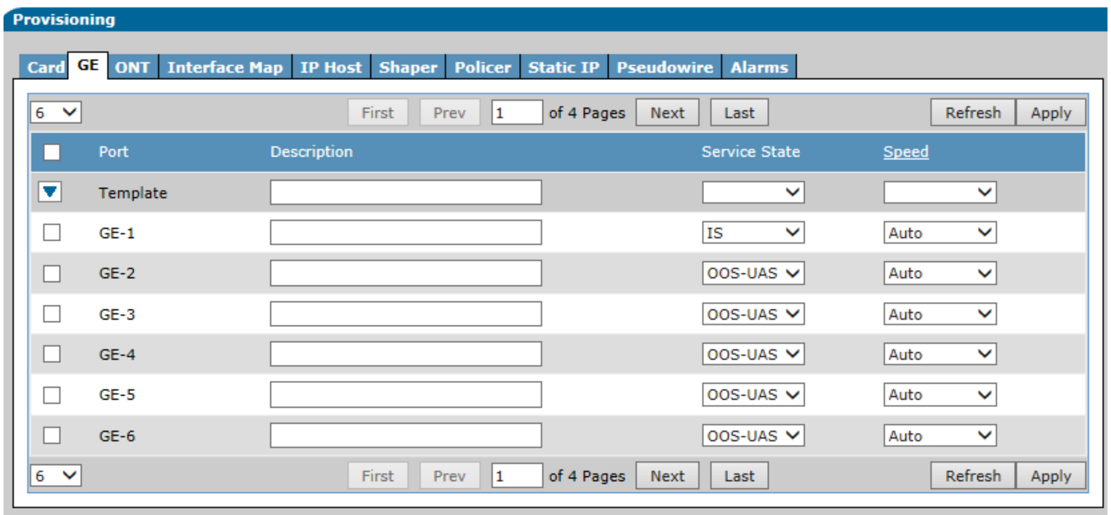


Figure 4-2. GE Provisioning

2. Set the port Service State to **IS** on the selected port number.
3. Click **Apply**.

What's Next

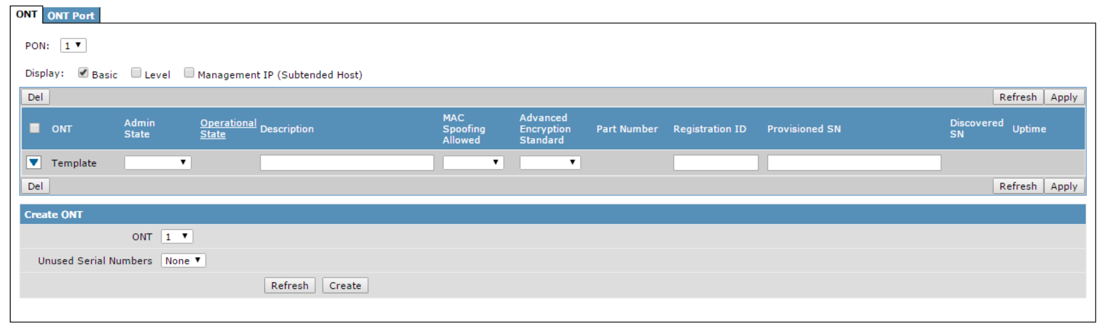
- Continue to "Discover the ONT" on page 2-5

ONT Inband Management Provisioning

To provision inband management for an ONT connected to a port on the OLT, complete the following steps:

1. Navigate to the ONT Provisioning menu.

   Modules > AE > Provisioning > ONT



2. Click Subtended Host check box.
3. Set the S-tag (VLAN ID) for the subtended host.
4. Set the S-tag priority for the subtended host.
5. Select the method of inband management (static or DHCP) from the IP Allocation drop down.

   Refer to Table 4-2 for the inband management options.

Table 4-2. Inband Management

Inband	Steps	Description
Static IP	1. Enter the IP Address for the ONT. 2. Enter the Subnet Mask for the ONT. 3. Enter the default Gateway IP Address for the ONT.	Set the static IP address, subnet mask, and gateway IP address for the ONT's inband management.
DHCP	When selected, you cannot enter an IP Address, Subnet Mask, or Gateway IP as these items are not applicable.	Allocate the IP address for the ONT's inband management dynamically using DHCP.

NOTE

To view the DHCP address, navigate to the ONT Status Screen (**Modules > AE > Status > ONT > ONT**) and check the Subtended Host check box. Scroll to the right to see the IP address.

Step 2: Service Provisioning

The Total Access 5000 FTTP application supports triple-play provisioning via Web GUI. To begin provisioning services, choose one of the following paths:

- "Voice"
- "Data" on page 4-12
- "Video" on page 4-13

Voice

The Total Access 5000 FTTP application supports Session Initiation Protocol (SIP), Media Gateway Control Protocol (MGCP), and GR-303 voice.

SIP

SIP works in concert with voice and video by enabling and agreeing on characterizations of a session for sharing data. SIP is an application-layer control protocol that can establish, modify, and terminate multimed sessions.

SIP provides two options. The first is provided in the **Voice** menu found under the **Services** option. For purposes of this document, this option is referred to as Non-OMCI. The second option is provided in the **Voice FTTx** menu found under the **Services** option. For purposes of this document, this option is referred to as OMCI.

NOTE

If your deployment uses a Remote Gateway ONT, OMCI (Voice FTTx) is the only supported option.

MGCP

MGCP is a protocol that works hand-in-hand with H.323 and SIP in VoIP services. MGCP works between a call agent or media gateway controller, usually a software switch, and a media gateway with internal endpoints. The media gateway is the network device that converts voice signals carried by telephone lines into data packets carried over the Internet or other packet networks.

MGCP provides two options. The first is provided in the **Voice** menu found under the **Services** option. For purposes of this document, this option is referred to as Non-OMCI. The second option is provided in the **Voice FTTx** menu found under the **Services** option. For purposes of this document, this option is referred to as OMCI.

NOTE

If your deployment uses a Remote Gateway ONT, OMCI (Voice FTTx) is the only supported option.

GR-303

GR-303 is the basic protocol used for POTS service.

NOTE

A Total Access 5000 Voice Gateway Module is required when provisioning GR-303.

Select Your Voice Option

Use Table 4-3 to determine your voice option and navigate to your next step. If you're unsure of your voice option, refer to "Voice" on page 4-5.

Table 4-3. Voice Options

Option	See Page
SIP OMCI Voice	4-7
SIP Non-OMCI Voice	4-8
MGCP OMCI Voice	4-9
MGCP Non-OMCI Voice	4-10
GR-303 Voice	4-11

SIP OMCI Voice

To provision for voice, complete the following steps:

NOTE

This is a general set of instructions to turn up SIP OMCI voice. Optional settings are available. For additional information on these optional settings refer to the applicable documents listed in "Related Online Documentation and Resources" on page Intro-3.

1. "Create an EVC" on page 4-14
2. "Set the Voice Service Mode on the ONT" on page 4-17
3. "Provision the Port on the ONT" on page 4-18
4. "Create an IP Host" on page 4-22
5. "Create an EVC-Map" on page 4-24
6. "Provision the SIP Trunk" on page 4-29
7. "Provision the SIP Dialing Profile" on page 4-33
8. "Provision the OMCI SIP Users" on page 4-46

SIP Non-OMCI Voice

To provision for voice, complete the following steps:

NOTE

This is a general set of instructions to turn up SIP Non-OMCI voice. Optional settings are available. For additional information on these optional settings refer to the applicable documents listed in "Related Online Documentation and Resources" on page Intro-3.

1. "Create an EVC" on page 4-14
2. "Set the Voice Service Mode on the ONT" on page 4-17
3. "Provision the Port on the ONT" on page 4-18
4. "Create an IP Host" on page 4-22
5. "Create an EVC-Map" on page 4-24
6. "Provision the SIP Trunk" on page 4-29
7. "Provision the SIP Dialing Profile" on page 4-33
8. "Provision Class of Service (CoS) (Optional)" on page 4-43
9. "Provision for Global Voice (Optional)" on page 4-44
10. "Provision the Voice User" on page 4-45

MGCP OMCI Voice

To provision for voice, complete the following steps:

NOTE

This is a general set of instructions to turn up MGCP OMCI voice. Optional settings are available. For additional information on these optional settings refer to the applicable documents listed in "Related Online Documentation and Resources" on page Intro-3.

1. "Create an EVC" on page 4-14
2. "Set the Voice Service Mode on the ONT" on page 4-17
3. "Provision the Port on the ONT" on page 4-18
4. "Create an IP Host" on page 4-22
5. "Create an EVC-Map" on page 4-24
6. "Provision the MGCP Profile" on page 4-31
7. "Provision OMCI MGCP Endpoints" on page 4-49

MGCP Non-OMCI Voice

To provision for voice, complete the following steps:

NOTE

This is a general set of instructions to turn up MGCP Non-OMCI voice. Optional settings are available. For additional information on these optional settings refer to the applicable documents listed in "Related Online Documentation and Resources" on page Intro-3.

1. "Create an EVC" on page 4-14
2. "Set the Voice Service Mode on the ONT" on page 4-17
3. "Provision the Port on the ONT" on page 4-18
4. "Create an IP Host" on page 4-22
5. "Create an EVC-Map" on page 4-24
6. "Provision the MGCP Profile" on page 4-31
7. "Provision Non-OMCI MGCP Endpoints" on page 4-32

GR-303 Voice

To provision for voice, complete the following steps:

NOTE

This is a general set of instructions to turn up GR-303 voice. Optional settings are available. For additional information on these optional settings refer to the applicable documents listed in "Related Online Documentation and Resources" on page Intro-3.

1. "Set the Voice Service Mode on the ONT" on page 4-17
2. "Provision the Port on the ONT" on page 4-18
3. "Provision GR-303" on page 4-50

Data

To provision for data, complete the following steps:

NOTE

This is a general set of instructions to turn up data. Optional settings are available. For additional information on these optional settings refer to the applicable documents listed in "Related Online Documentation and Resources" on page Intro-3.

1. "Create an EVC" on page 4-14
2. "Provision the Port on the ONT" on page 4-18
3. "Create an EVC-Map" on page 4-24

Video

To provision for video, complete the following:

NOTE

This is a general set of instructions to turn up video. Optional settings are available. For additional information on these optional settings refer to the applicable documents listed in "Related Online Documentation and Resources" on page Intro-3.

1. "Create an EVC" on page 4-14
2. "Provision the Port on the ONT" on page 4-18
3. "Create an EVC-Map" on page 4-24

Create an EVC

The EVC (Ethernet Virtual Connection) is a centrally managed object defining the properties of a particular S-Tag within a Total Access 5000. The EVC object enables the provisioning of ELINE, E-TREE, and E-LAN applications. EVCs are available for use by all access modules within a shelf.

NOTE

The EVC for SIP/MGCP traffic will be a dedicated EVC because voice traffic requires different Quality of Service (QoS) handling than other data traffic.

To create an EVC, complete the following steps:

1. Navigate to the Create EVC section of the EVC page.

   Services > **EVCs** > **EVC** > **Create EVC**

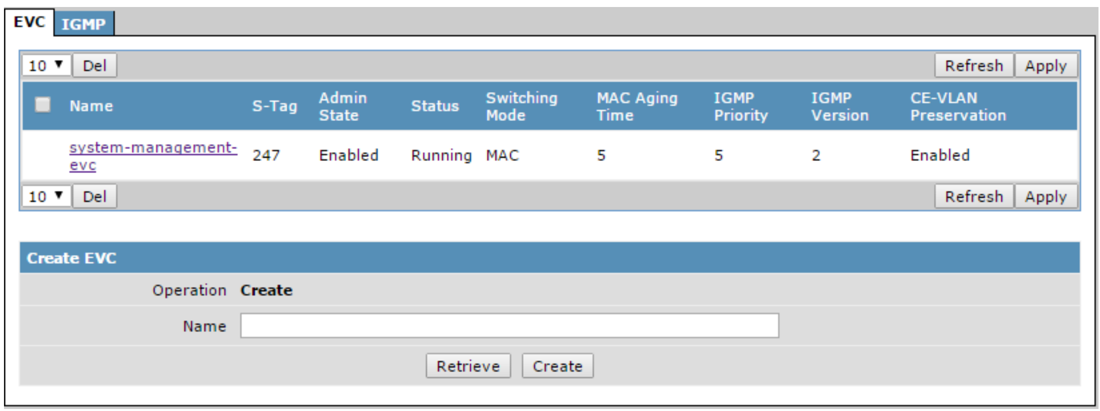


Figure 4-3. Create EVC

2. Enter a unique EVC name into the Name field.

NOTE

EVC names are case sensitive.

3. Click the **Create** button to access the Edit EVC options. The Edit EVC screen will open.

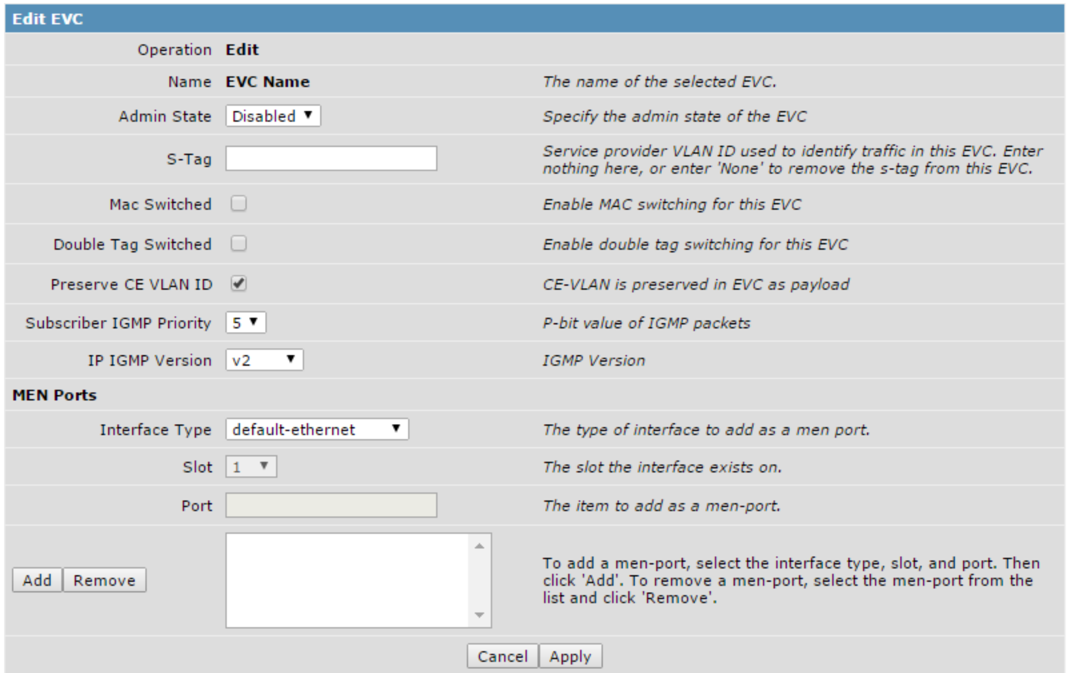


Figure 4-4. Edit EVC

4. Set the Admin State to **Enabled**.
5. Enter the S-Tag for the EVC.
6. Enable Mac Switching on the EVC.
7. Disable the Preserve CE-VLAN ID setting on the EVC.
8. If provisioning for video, set the Subscriber IGMP Priority.
   If provisioning for voice or data, skip to step 9.
9. Select the Interface Type for the MEN Port(s).

NOTE

For Video Services, **default-ethernet** must be one of your MEN Ports.

10. Select **A** for the MEN port slot.
11. Enter the Port/Group numbers of the MEN Port(s). MEN Port is the upstream network connection for the EVC.
12. Click **Add**.
13. Click **Apply** to enable the EVC.
14. The EVC should be added to the bottom of the EVC list. Verify the Status is **Running**, It may take up to 10 seconds for the Status to change to **Running**.

15. If currently provisioning for voice or data, skip to What's Next. If currently provisioning for video, complete the following:
    a. Select the IGMP tab.

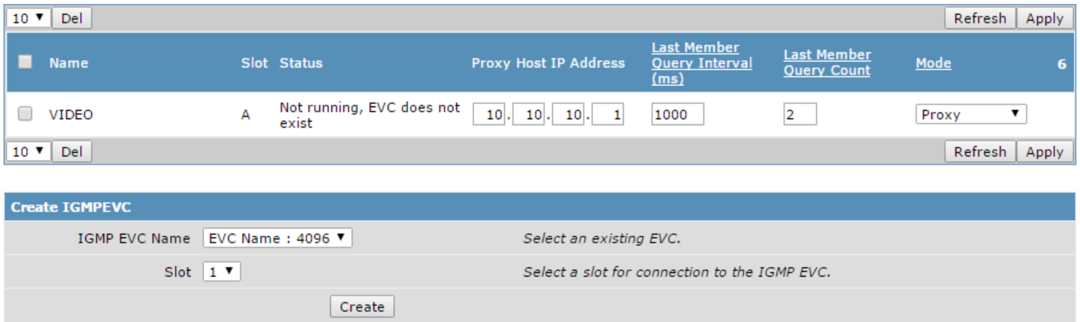


Figure 4-5. Edit EVC

    b. An IGMP EVC connection is required for the switch module (Slot A) and each access module. Select the required EVC name in the IGMP EVC Name drop down.
    c. Select the required slot.
    d. Click the Create button.
16. The IGMP EVC should be added to the bottom of the IGMP EVC list. Verify the Status is **Running**, It may take up to 10 seconds for the Status to change to **Running**.

NOTE

The IGMP EVC for the OLT Slot will not be running until the EVC-Map is created.

What's Next

- For SIP or MGCP provisioning, continue to "Set the Voice Service Mode on the ONT" on page 4-17.
- For video or data provisioning, continue to "Provision the Port on the ONT" on page 4-18

Set the Voice Service Mode on the ONT

1. Navigate to the ONT Provisioning menu.

   Modules > AE > Provisioning > ONT

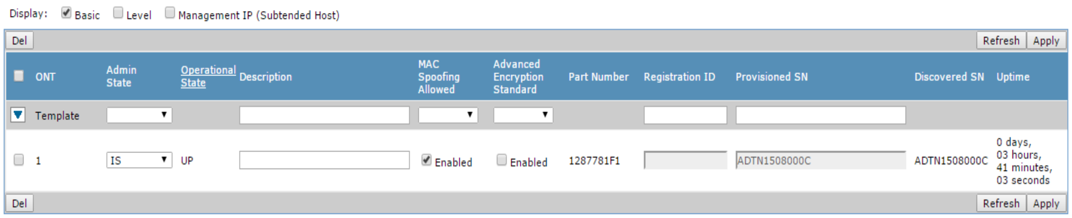


Figure 4-6. Voice Service Mode

2. Click Level and Management IP (Subtended Host) check boxes.

NOTE

You may have to scroll to the right to view all available options.

3. Set the POTS Service Mode.

   For more details about the available modes, refer to the Total Access 5000 GPON User Interface Guide (P/N 65K90GPON-31).
4. Set the VoIP Config Method.

   Remote Gateways require the use of OMCI. For more details about the available methods, refer to the Total Access 5000 GPON User Interface Guide (P/N 65K90GPON-31).
5. If using a static IP address for ONT management, enter the IP Address.
6. If using a static IP address for ONT management, enter the Subnet Mask.
7. If using a static IP address for ONT management, enter the Gateway IP Address.
8. Click **Apply**.

What's Next

For SIP, MGCP, GR-303 provisioning, continue to "Provision the Port on the ONT" on page 4-18.

Provision the Port on the ONT

NOTE

If provisioning data and video on the same port, the ONT port only needs to be enabled once.

1. Navigate to the ONT Port Provisioning menu.

   Modules > **AE** > **Provisioning** > **ONT** > **ONT Port**

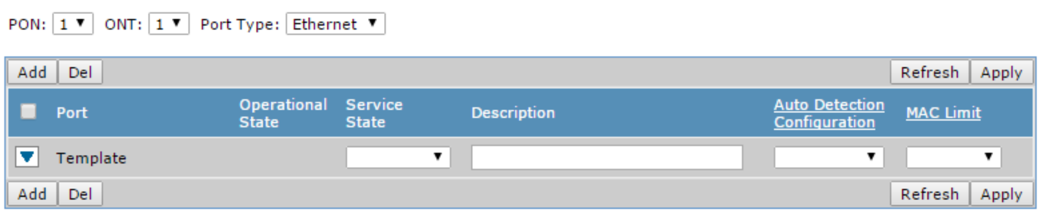


Figure 4-7. ONT Port Provisioning

2. Select your PON.
3. Select your ONT
4. Select the Port Type. Use Table 4-4 to determine your port type and navigate to your next step.

Table 4-4. Port Type

Service	ONT	Type	See Page
Data/Video	Non-Remote Gateway	Ethernet	4-19
	Remote Gateway	Virtual Gigabit Interface	4-21
Voice	All ONTs	FXS	4-20

Ethernet

After selecting Ethernet as the ONT port type, complete the following steps:

1. Set the number of MAC addresses allowed.

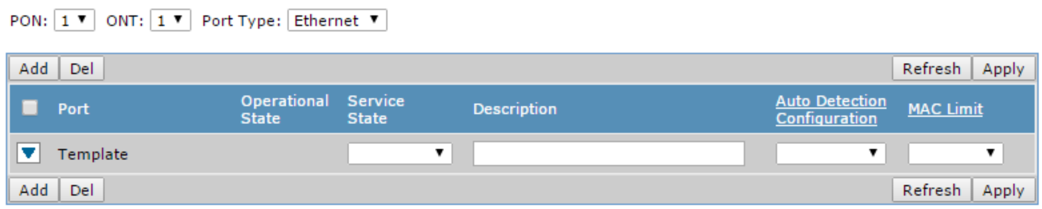


Figure 4-8. ONT Port Provisioning

NOTE

- 16 MAC addresses per ONT are allowed and must be shared by all Ethernet ports on the ONT.
- A value of 0 will actually allow up to 128 MAC addresses to be attributed to the ONT. However, the number of MAC addresses the OLT can support is limited so using more than 16 will severely limit the number of MAC addresses available to other ONTs. No more than 16 static addresses can be configured regardless of the number of MAC addresses allowed by this setting.

2. Set the Service State to **IS** to enable the Ethernet interface of the ONT.
3. Click **Apply**.

What's Next

For video or data provisioning, continue to "Create an EVC-Map" on page 4-24.

FXS

After selecting FXS as the ONT port type, complete the following steps:

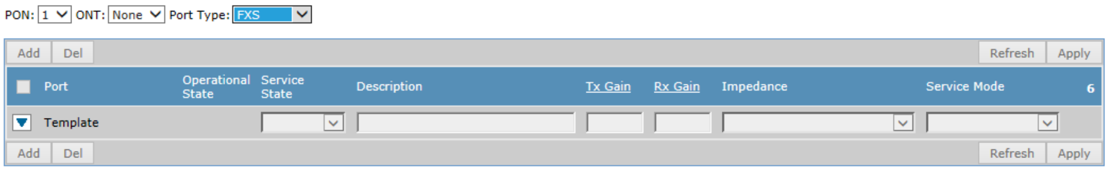


Figure 4-9. FXS Port Provisioning

1. Adjust the Tx Gain for the FXS port between -12.0dB and +6.0dB.
2. Adjust the Rx Gain for the FXS port between -12dB and +6.0dB.
3. Set the Service State to **IS** to enable the FXS interface of the ONT.
4. Click **Apply**.

What's Next

- For SIP or MGCP provisioning, continue to "Create an IP Host" on page 4-22.
- For GR-303 provisioning, continue to "Provision GR-303" on page 4-50.

Virtual Gigabit Interface

To provision a virtual gigabit interface, complete the following steps:

1. Open a new telnet window and log on to the Total Access 5000 shelf using the same user credentials used for the Web GUI.
2. Access the Enable prompt.

   ```
   ChassisID>enable
   ChassisID#
   ```

3. Access the Global Configuration Command Set.

   ```
   ChassisID#configure terminal
   ```

4. Access the Virtual Gigabit Ethernet Interface Configuration Command Set.

   ```
   ChassisID(config)#interface virtual-gigabit-ethernet <ont-id/0/
   port>@<shelf/slot/port>
   ```

5. Enable the interface.

   ```
   ChassisID(config-virtualGigabitEthernet x/x/x@x/x/x)#no shutdown
   ```

6. You may now close out the telnet window.

What's Next

- For SIP or MGCP provisioning, continue to "Create an IP Host" on page 4-22.
- For video or data provisioning, continue to "Create an EVC-Map" on page 4-24.

Create an IP Host

1. Navigate to the IP Host Provisioning menu.

   Modules > AE > Provisioning > IP Host

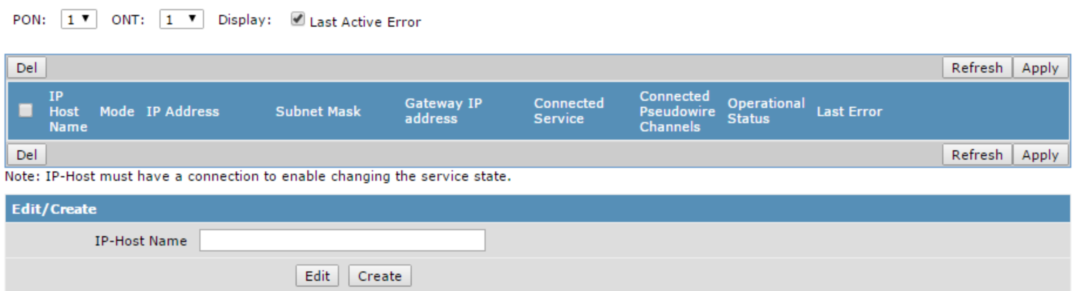


Figure 4-10. IP-Host Create Menu

2. Enter the IP-Host Name.
3. Click **Create**, the Edit/Create screen is displayed.

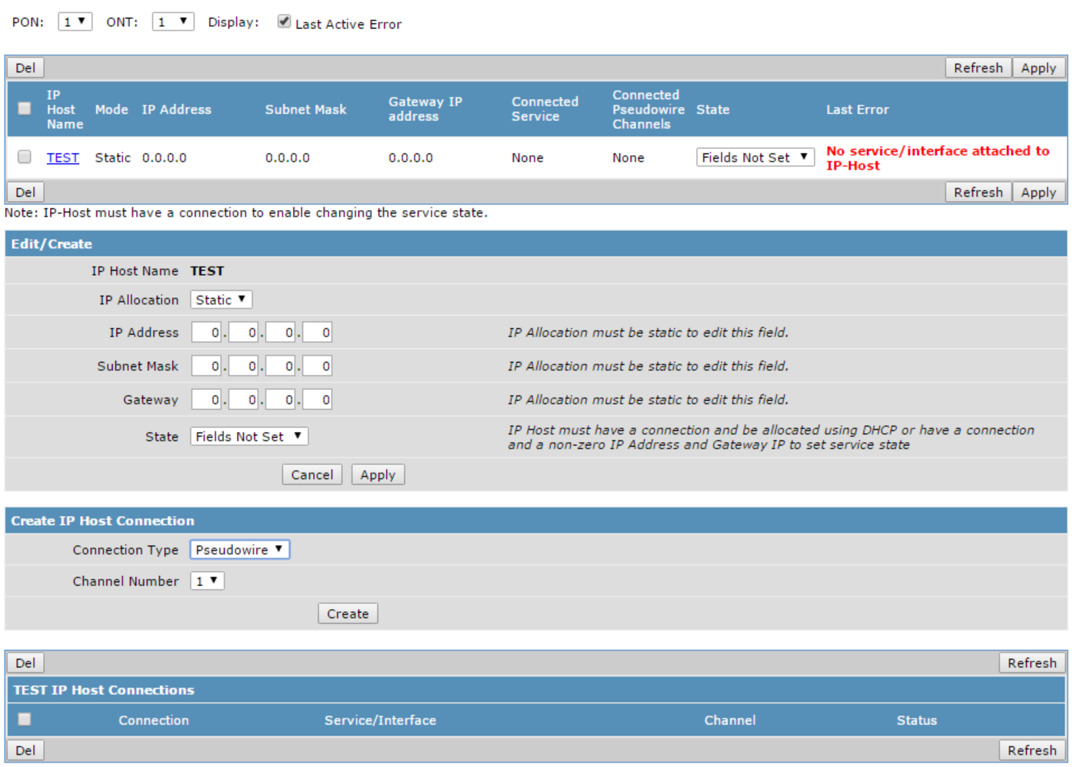


Figure 4-11. IP-Host Provisioning

4. Select the PON number.
5. Select the ONT.
6. In the IP-Host Name field, enter a unique name for the IP-Host.

NOTE

Only two interface IP-host entities can be created per ONT. Attempts to create more than two will be rejected.

7. Select the IP Allocation method. If set to DHCP, skip to step 9.
8. If the allocation method is set to Static, complete the following:
   a. Enter the IP Address.
   b. Enter the Subnet Mask.
   c. Enter the Gateway.
9. If DNS is not required, skip to step 10. If DNS is required, complete the following:
   a. Select Enabled.
   b. Enter the default domain name of the DNS.
   c. Enter the preferred DNS.

      Only 2 addresses can be entered at a time. The first address becomes the preferred DNS and the subsequent address becomes the second priority.

      The DNS must be configured using IP host to resolve FQDN configured in the SIP trunk and MGCP.
10. Click **Apply** in the Edit/Create section.
11. Select the Connection Type in the Create IP Host Connection section.
12. Click **Create**.
13. Verify your IP Host listed state is Active and that there are no errors that appear in the Last Error column.

What's Next

For SIP or MGCP provisioning, continue to "Create an EVC-Map" on page 4-24.

Create an EVC-Map

To create an EVC-Map, complete the following steps:

1. Access the Interface Map.

   Modules > AE > Provisioning > Interface Map

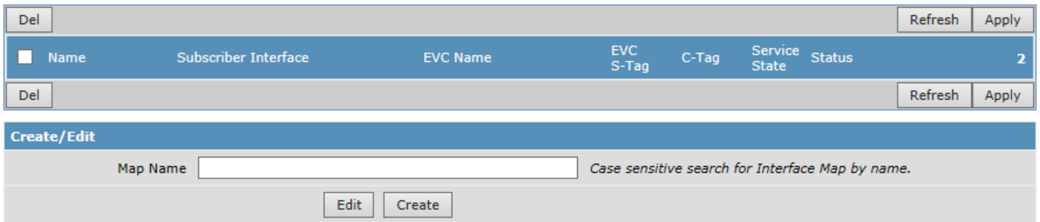


Figure 4-12. EVC-Map Create

2. Enter the new EVC-Map name into the Map Name field and click the Create button.

NOTE

An example name would be DATAMap. If there are spaces in the name, you must use quotes around the name to use show commands.

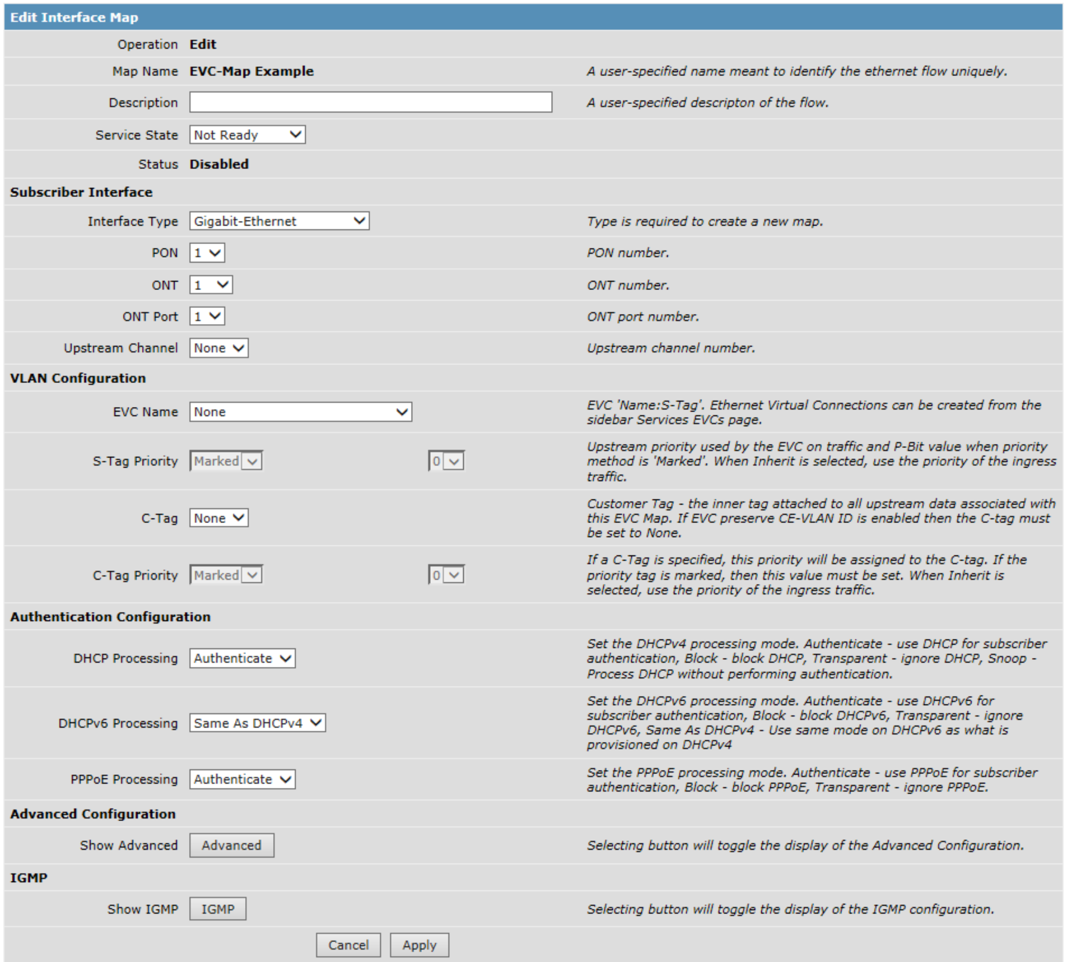


Figure 4-13. EVC-Map Edit

3. Set the Service State to **Active**.
4. Select the Interface Type. Use Table 4-5 to determine the type and the steps to complete.

Table 4-5. Interface Type

Service	ONT	Type	Steps
Data/Video	Non-Remote Gateway	Gigabit-Ethernet	Complete the following steps: 1. Select the OLT Port. 2. Select the ONT. 3. Select the ONT Port. 4. Select the Upstream Channel.
	Remote Gateway	Virtual Gigabit-Ethernet	
Voice	All ONTs	IP Host	Select the IP Host created for this service.

5. Select the EVC created for your selected service.

6. If provisioning voice, skip to step 10. If you are provisioning for voice or data, configure the Authentication Method. Use Table 4-6 to determine the authentication and steps required.

NOTE

PPPoE does not support video services.

Table 4-6. Authentication Method

Authentication	Steps
DHCPv4 only	Complete the following steps: 1. Set DHCP Processing to Authenticate. 2. Set DHCPv6 Processing to Block. 3. Set PPPoE to Block.
DHCPv6 only	Complete the following: 1. Set DHCP Processing to Block. 2. Set DHCPv6 Processing to Authenticate. 3. Set PPPoE to Block.
DHCPv4 and DHCPv6	Complete the following: 1. Set DHCP Processing to Authenticate. 2. Set DHCPv6 Processing to Same As DHCPv4. 3. Set PPPoE to Block.
PPPoE	Complete the following: 1. Set DHCP Processing to Block. 2. Set DHCPv6 Processing to Block. 3. Set PPPoE to Authenticate.

7. Configure the Relay Agent. If you are unsure about supported options, contact your network administrator. For more information on Relay Agent, refer to the Total Access 5000 GPON User Interface Guide (P/N 65K90GPON-31)
    a. Enter the Circuit ID Format.
    b. Enable or disable Remote ID.
    c. Enter the Remote ID Format.
    d. Enable or disable DHCP Option 82 Insertion.
    e. Enable or disable DHCPv6 Relay Agent.
    f. Enable or disable PPPoE Intermediate Agent.

8. If provisioning a data or video service on a Remote Gateway ONT, complete the following steps:
    a. Click **Advanced**.

Figure 4-14. EVC-Map Advanced

    b. Select the CE-VLAN. The CE-VLAN can be typed in or selected from a drop-down list.

9. If provisioning for video, complete the following steps. If provisioning for data, skip to step 10.
    a. Click **IGMP**.

Figure 4-15. EVC-Map IGMP

    b. Set the subscriber IGMP mode.
    c. Enable Immediate Leave.
    d. Set the IGMP proxy router IP address.

10. Click **Apply**.
11. The EVC-Map should be added to the bottom of the EVC-Map list. Verify the Status is **Running**, It may take up to 10 seconds for the Status to change to **Running**.

12. If provisioning video, return to the IGMP EVC list to verify the IGMP EVC for the OLT slot is now **Running**.

What's Next

- For OMCI SIP and Non-OMCI SIP provisioning, continue to "Provision the SIP Trunk" on page 4-29.
- For OMCI MGCP and Non-OMCI MGCP provisioning, continue to "Provision the MGCP Profile" on page 4-31
- For remote gateway ONT video or data provisioning, continue to
- For non-remote gateway ONT video or data provisioning, this completes provisioning. Services should be up and running. To provision another service, continue to "Step 2: Service Provisioning" on page 4-5.

Provision the SIP Trunk

The SIP trunk is the logical path to the SIP proxy. The attributes configured on the trunk should be compatible with the corresponding parameters on the SIP proxy. If the system defaults match the capabilities and configured options of the SIP proxy, a small amount of trunk provisioning is required.

All voice trunks are shared across the node, so provisioning of a trunk at the GigE SM makes it available to all gateways.

1. Navigate to the Trunk menu.

   OMCISIP **– Services** > **Voice FTTx** > **SIP** > **Trunk**

   Non-OMCI SIP **– Services** > **Voice** > **SIP** > **Trunk**

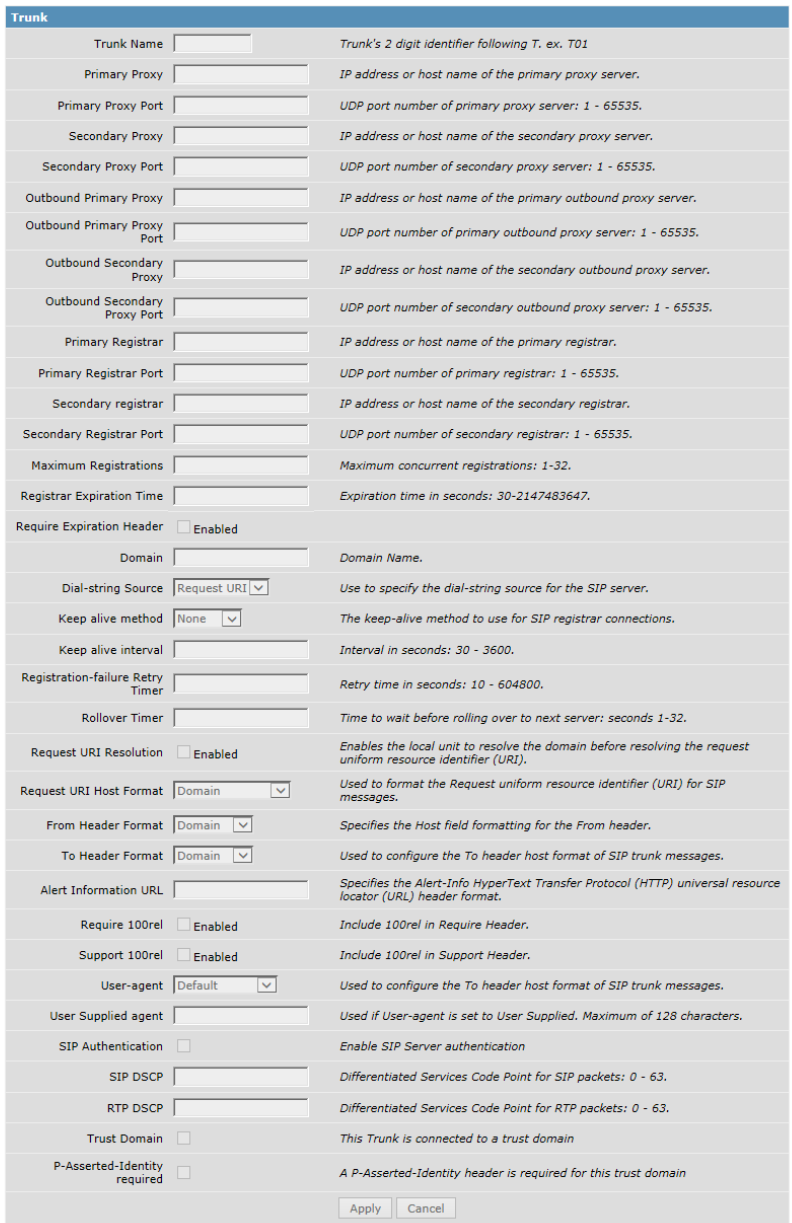


Figure 4-16. SIP Trunk Create

2. Click **Add**.
3. Enter the Trunk's 2 digital identifier following T.
4. Click **OK**.
5. Enter the SIP Primary Proxy IP address.
6. Enter the Primary Registrar IP address.
7. If using a secondary server, enter the SIP Secondary Proxy address.
8. If using a secondary server, enter the Secondary Registrar IP address.
9. If the system defaults match the capabilities and configured options of the SIP proxy, no further provisioning is required. For more details about the available provisioning options, refer to the Total Access 5000 Switch Module User Interface Guide (P/N 65K90SM-31).
10. Click **Apply**.

What's Next

For Non-OMCI and OMCI SIP provisioning, continue to "Provision the SIP Dialing Profile" on page 4-33.

Provision the MGCP Profile

To create the MGCP profile, complete the following:

1. Access the Profiles menu.

   OMCI MGCP **– Services** > **Voice FTTx** > **MGCP** > **Profiles**

   Non-OMCI MGCP **– Services** > **Voice** > **SIP** > **Profiles**

2. Enter the Profile Name.

NOTE

Only one MGCP Profile is supported.

3. Click **Create**, the Provision MGCP Profile screen is displayed.
4. Specify the primary MGCP call agent IP address.

   It is important to identify the call agent to the ONT MGCP Endpoint. Both primary and secondary call agents can be established, but at minimum a primary call agent is required. If a connection with the primary call agent fails, call agents will be tried in the order they are entered in the configuration.

5. Click **Apply**.

What's Next

- For OMCI MGCP provisioning, continue to "Provision OMCI MGCP Endpoints" on page 4-49.
- For Non-OMCI MGCP provisioning, continue to "Provision Non-OMCI MGCP Endpoints" on page 4-32

Provision Non-OMCI MGCP Endpoints

MGCP endpoints are dedicated FXS ports configured to use MGCP to communicate with a call agent.

To create the MGCP profile, complete the following:

1. Navigate to the Endpoints menu.

   Services > **Voice** > **MGCP** > **Endpoints**
2. Enter the slot number of the GPON OLT.
3. Enter a unique MGCP Endpoint Index.
4. Click **Create**.
5. Enter the MGCP Profile to be used by this voice user.
6. Enter the FXS port with which this MGCP endpoint is associated.
7. Click **Apply**.

What's Next

For Non-OMCI MGCP, this completes provisioning. Services should be up and running. To provision another service, continue to "Step 2: Service Provisioning" on page 4-5.

Provision the SIP Dialing Profile

The Dialing Profile is assigned to voice users, and is used to notify the access modules when to stop collecting digits being dialed and begin connecting a phone call. The dial profile creates and stores number-complete templates.

A number-complete template consists of a pattern of digits used by telephone companies when making calls. A typical template would be 555-XXX-XXX. These templates can be expanded to include Dial Plans, External Line Codes and Special Prefix Patterns.

The access module collects digits and looks for a match against the Dial Plans, External Line Codes and Special Prefix (SPRE) Patterns. When the digits dialed match a number-complete template, the dial-string is immediately sent to the server for routing.

For example, a normal phone number consists of the following template: 555-XXX-XXXX (where “X” is a wild card denoting any digit from 1 to 9). The first three digits are the Area Code Designation, the next three digits are the Phone Exchange Designation, and the last four digits are the Local Number Designation.

When a user initiates a phone call, the access module compares the dialed digits to the number-complete template. If the dialed digits are a match (in this case, three 5s followed by seven other digits) the access module immediately sends the complete dial-string to the server. The server then routes and connects the call.

If the user dials a pattern of digits that does not match any number-complete template, the pattern will still be forwarded to the server after the Inter-digit Timeout has expired. Proper definition of the dial plan is recommended for optimum customer experience. At the very least, emergency numbers should be configured to avoid delays in these calls.

The different types of number-complete templates can be chained together to form longer dial-strings with the use of chaining characters (“&”). For example, if a dialing profile contains an External Line Code "9&", a Special Prefix "*70&" and a Dial Plan "555-XXX-XXXX" and the user dials *70,9,555-123-4567, all the digits will be gathered into a single dial-string and sent to the server when the last digit is entered. An External Line Code will only be matched once during a dialing sequence.

Dial Plan Pattern Restrictions

Dial Plan patterns are entered using the **`dial-plan <type> <PATTERN> [emergency-number] [external-line-code <prohibited|required>]`** command. The following types are supported: 900-number, always-permitted, internal, international, local, national, operator-assisted, specify-carrier, toll-free, user1, user2 and user3. Multiple patterns of the same type are allowed. The pattern must be in the form of a phone number or dialing pattern containing wildcards. Available wildcards are: N=2-9, M=1-8, X=0-9, and [abc]=Any digit contained in the bracketed list. When creating a Dial Plan Pattern, the following rules must be observed:

- Templates must have at least one number or wild card.
- The “(' ')” and “-” characters are allowed, but not inside brackets “[ ]”.
- A “,”is allowed within bracket “[ ]”, but not elsewhere.
- Wild cards (MNX) are not allowed inside brackets “[ ]”.
- Order of numbers is not enforced within brackets “[ ]”.
- The “$” character is allowed, but MUST be the last character in the pattern or standalone.
- If “*” and “#” are entered, they must be the first character in the pattern. They cannot be standalone.

The following are examples of possible Dial Plan patterns:

- For a residential customer:
  - **dial-plan 900-number 1-900-NXX-XXXX**
  - **dial-plan always-permitted 911 emergency-number**
  - **dial-plan international 011$**
  - **dial-plan local 256-NXX-XXXX**
  - **dial-plan local NXX-XXXX**
  - **dial-plan national 1-NXX-NXX-XXXX**
  - **dial-plan specify-carrier 10-10-XXX$**
  - **dial-plan toll-free 1-800-NXX-XXXX**
  - **dial-plan toll-free 1-888-NXX-XXXX**
  - **dial-plan toll-free 1-877-NXX-XXXX**
  - **dial-plan user1 [23456]11**
- For a business customer (using an external line code):
  - **dial-plan 900-number 1-900-NXX-XXXX external-line-code required**
  - **dial-plan always-permitted 911 emergency-number**
  - **dial-plan internal MXXX external-line-code prohibited**
  - **dial-plan international 011$ external-line-code required**
  - **dial-plan local 256-NXX-XXXX external-line-code required**
  - **dial-plan local NXX-XXXX external-line-code required**
  - **dial-plan national 1-NXX-NXX-XXXX external-line-code required**
  - **dial-plan specify-carrier 10-10-XXX$ external-line-code required**
  - **dial-plan toll-free 1-800-NXX-XXXX external-line-code required**
  - **dial-plan toll-free 1-888-NXX-XXXX external-line-code required**
  - **dial-plan toll-free 1-877-NXX-XXXX external-line-code required**
  - **dial-plan user1 [23456]11 external-line-code required**

SPRE Pattern Restrictions

SPRE patterns are entered using the **spre <PATTERN> [tone <dial|stutter-dial>]** command. SPRE Pattern creates special code numbers required to access voice services. A SPRE Pattern must be in the form of a special prefix (spre) code or dialing pattern containing wild cards. Available wild cards are: N=2-9, M=1-8, X=0-9 [abc] = any digit contained within the bracket list. The pattern can end with a chaining character ("&" or "$") which allows for the collection of more digits before the dial string is sent to the server. Ending the pattern with "&" causes the server to continue to look for another number-complete template (dial plan, external line-code or special prefix pattern) following the SPRE code. Ending it with "$" causes the access module to stop attempting to match additional inputs. However, digits will continue to be collected until after the Inter-Digit time out occurs.The following rules must be observed:

- The Template must begin with an "*" or "#". An "*" and "#" are not allowed elsewhere in the Template.
- The Template must have at least one number.

- The characters "("") and "-" are allowed, but not inside "[ ]".
- Do not use "," or "" inside "[ ]".
- Wild cards (MNX) are not allowed inside "[ ]".
- The characters "&" and "$" are allowed but must be the last character and cannot be a standalone.

The following are examples of possible SPRE Patterns:

- **`spre *3XX`**
- **`spre *6[37]&`**
- **`spre *72& tone stutter-dial`**
- **`spre *82&`**
- **`spre *9[02]& tone stutter-dial`**
- **`spre *7[45]$`**
- **`spre *[56789]X`**

External Line Code Restrictions

External Line Codes are entered using the **`external-line-code <PATTERN> [tone <dial|stutter-dial>]`** command. An External Line Code must be in the form of a dialing pattern without wild cards. For example, if a user must first dial "8" to obtain an outside line, the entry would be "8&" where the ampersand tells the server that the "8" designates an outside number and to expect more digits in the number-complete template. The pattern can end with a chaining character ("&" or "$"), which allows for collection of more digits before the dial string is sent to the server. Ending the pattern with a "&" causes the server to continue to look for another number-complete template (dial plan or special prefix pattern) following the external line code. An external line code will only be matched once. Ending the pattern with a "$" causes the access module to stop attempting to match additional inputs. However, digits will continue to be collected until after the Inter Digit time out occurs. The following rules must be observed:

- Template must have at least one number (i.e., 0-9).
- Wild cards are not allowed.
- If "*" and "#" are entered, they must be the first character. They cannot be standalone.
- The characters "&" or "$" are allowed but must be the last character and cannot be standalone.

The following is an example of a possible External Line Code:

- **`external-line-code 8& tone dial`**

Dial Plan Provisioning

To provision the dial plan, complete the following:

1. Navigate to the Dialing Profile menu.

   OMCI SIP **– Services** > **Voice FTTx** > **SIP** > **Dialing Profiles**

   Non-OMCI SIP **– Services** > **Voice** > **SIP** > **Dialing Profiles**

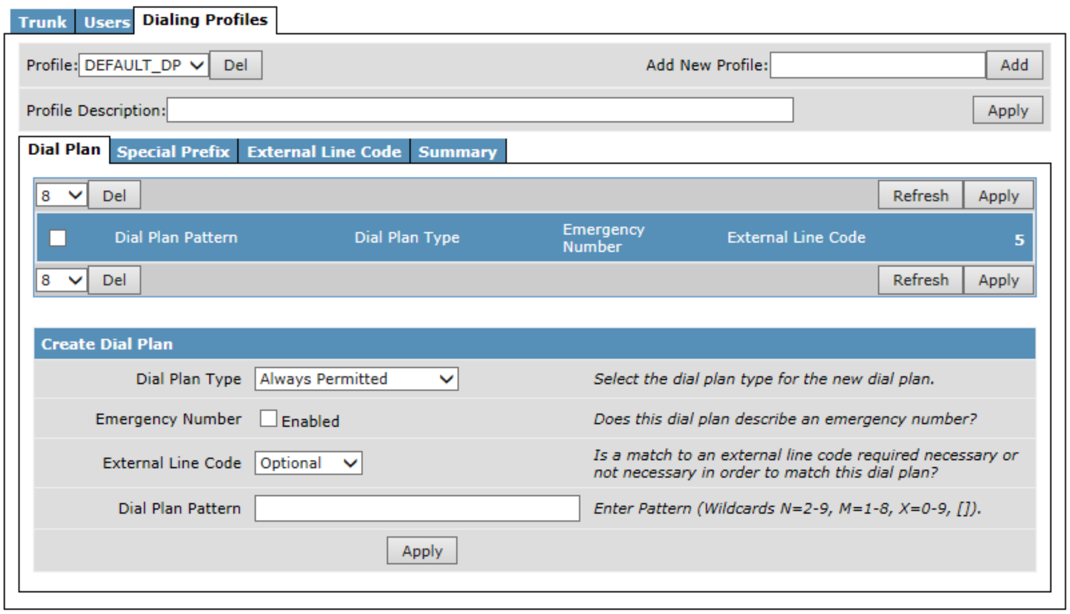


Figure 4-17. Dial Plan Provisioning

2. If you are creating a new dialing profile, enter a new profile name. The name cannot contain the "/" character.
3. Click **Add**.
4. Select the dial plan type for the new dial plan.
5. Enter the Dial Plan Pattern. For Example **`256-NXX-XXXX`**
6. Click **Apply** in the Create Dial Plan section.

What's Next

- For OMCI SIP provisioning, continue to "Provision the Common Profiles (Optional)" on page 4-37.
- For Non-OMCI SIP provisioning, continue to "Provision Class of Service (CoS) (Optional)" on page 4-43

Provision the Common Profiles (Optional)

Both OMCI SIP and OMCI MGCP support the use of common profiles. This feature enables the creation of specific profiles that can be assigned to multiple users.

NOTE

If you are unsure about these options, contact your network administrator. For more details about the available provisioning options, refer to the Total Access 5000 Switch Module User Interface Guide (P/N 65K90SM-31). Creating Common Profiles is optional for your network. If these profiles are not required, continue to "Provision the OMCI SIP Users" on page 4-46.

Refer to Table 4-7 for a list of the supported profiles.

Table 4-7. Common Profiles

Profile	Support	See Page
Call Feature	SIP	4-38
Media	SIP/MGCP	4-40
Codec	SIP/MGCP	4-42

Provision the Call Features Profile

Call feature options are available to set the access module/remote device to perform certain operations, like three-way conferencing, locally. It is not necessary to change any of these settings if the SIP server is capable of performing them.

1. Navigate to the Call Features menu.

   Services > **Voice FTTx** > **Common Profiles** > **Call Features**

2. Provision the call feature profile options.

   Refer to Table 4-8 for a list of call feature options.

Table 4-8. Call Feature Profile Options

Option	Description
Emergency Number Ringing Timeout	Sets the maximum duration, in minutes, an inhibited call may remain open by an Emergency Operator.
Emergency Number Onhook allow	Determines if an Emergency call will be dropped or remain open when the call originator goes on-hook. The following options are available: ■ If set to allow, the call will be dropped if the call originator hangs up. This is the default mode. ■ If set to inhibit, the call will remain open until the Emergency Operator terminates the call. While the call is held-up, the local phone will ring and the Emergency Operator will hear a ringback tone.
Call Waiting	Enables call waiting on the subscriber port.
Caller ID Inbound	Allows inbound caller ID to this endpoint.
Caller ID Outbound	Allows outband caller ID from this endpoint.
Transfer On Hangup	Enables transfer on hangup. When transferring a call, hanging up initiates the transfer to the destination party.
Timeout Alerting	Specifies the maximum time a call is allowed to remain in the alerting state. The shorter of this timeout or the configured maximum number of rings will determine how long a call is allowed to ring.
Timeout Interdigit	Specifies the maximum time allowed between dialed digits.
Conference	Allows the initiation of three-way conference calls. This feature allows multiple parties to communicate at the same time on the same line.

Table 4-8. Call Feature Profile Options (Continued)

Option	Description
Conference Local Originator Flashhook	If the voice conference mode is set to local, specify the actions performed if the conference originator issues a flashhook once the conference has been established. The following options are available: ■ The drop option specifies that the last party added to the 3-way conference will be dropped and the call will continue between the two remaining parties. ■ The ignore option specifies that the flashhook will be ignored. The 3-way conference will continue without interruption. ■ The split option specifies that the 3-way conference will be split into two calls, one between the originator and the first party and one between the originator and second party. When additional flashhooks are issued after the split, they will toggle the originator between the two calls.
Feature Mode	Determines if voice conferencing bridging will be handled within the unit or from a far-end conferencing server.

What's Next

- Continue to "Provision the Media Profile" on page 4-40.

Provision the Media Profile

The media profile is created in the Total Access 5000 to provision the Realtime Transport Protocol (RTP) parameters on the access module/remote device.

1. Navigate to the Media menu.

   Services > Voice FTTx > Common Profiles > Media

2. Provision the media profile options.

   Refer to Table 4-9 for a list of media profile options.

Table 4-9. Media Profile Options

Option	Description
RTP Frame Packetization	Configures the RTP frame packetization time in milliseconds.
Packet Delay Nominal	Sets the allowable limits of latency on the network. This sets the nominal delay time value in increments of 10 milliseconds.
RTP Packet Delay Maximum	Sets the allowable limits of latency on the network. This sets the maximum delay time value in increments of 10 milliseconds.
RTP DTMF Relay	Configures the method by which RTP dial tone multi-frequency (DTMF) events are relayed.
RTP QoS DSCP	Configures the maximum RTP quality of service (QoS) parameters for differentiated services code point (DSCP).
RTP Local Port Min	Configures the starting RTP UDP port used to source RTP from the ONT.
RTP Local Port Max	Configures the starting RTP UDP port used to source RTP from the ONT.
Fax Mode	Switches to passthrough mode on fax or modem tone detection. This command allows modem and fax calls to maintain a connection without altering the signals with the voice improvement settings.

Table 4-9. Media Profile Options (Continued)

Option	Description
Echo Cancellation	Improves voice quality for packetized-based voice calls.
Flash Hook Min	Configures the minimum time the switch hook must be held to be interpreted as a flash.
Flash Hook Max	Configures the maximum time the switch hook must be held to be interpreted as a flash.
Silence Suppression	Enables voice activity detection. When enabled, RTP packets will not be sent during periods of silence.

What's Next

Continue to "Provision the Codec Profile" on page 4-42.

Provision the Codec Profile

CODECs are used to convert an analog voice signal to digitally encoded version. Codecs vary in the sound quality, the bandwidth required, the computational requirements, etc.

1. Navigate to the CODEC menu.

   Services > Voice FTTx > Common Profiles > Codec

2. Provision the CODEC profile options.

   Refer to Table 4-10 for a list of CODEC options.

Table 4-10. CODEC Profile Options

Option	Description
Preference	Specifies the order of preference for coder-decoders used by the CODEC list.
Codec	Specifies the CODEC.

What's Next

- For OMCI SIP continue to "Provision the OMCI SIP Users" on page 4-46.
- For OMCI MGCP continue to "Provision OMCI MGCP Endpoints" on page 4-49

Provision Class of Service (CoS) (Optional)

CoS is an optional provisioning choice that defines the permissions available to a system user for making voice calls. Voice CoS permissions include the type of calls and actions a user can perform.

The default CoS, called DEFAULT_COS, grants permission to place all types of calls is automatically assigned to all voice users.

Creating further CoS entries is only necessary if restrictions are to placed on types of calls the voice user can make.

To create or edit a CoS, complete the following:

1. Access the Class of Service menu.

   Services > **Voice** > **SIP** > **Class of Service**

2. In the Class of Rules, enter a unique rule name.
3. Click **Create**.
4. By default all the Class of Service options are automatically provisioned with the exception of Disable Call Waiting. Use the check box to either allow or disallow the selected service.

   For more details about the available provisioning options, refer to the Total Access 5000 Switch Module User Interface Guide (P/N 65K90SM-31).

5. Click **Apply**.

What's Next

Continue to "Provision for Global Voice (Optional)" on page 4-44.

Provision for Global Voice (Optional)

Global provisioning options are available to set the ONT to perform certain operations, like three-way conferencing, locally.

It is not necessary to change any of these settings if the SIP server is capable of performing them.

To provision the global voice options, complete the following:

1. Access the Global Voice menu.

   Services > **Voice** > **SIP** > **Options**

2. Provision the options. If you are unsure about supported options, contact your network administrator.

   For more details about the available provisioning options, refer to the Total Access 5000 Switch Module User Interface Guide (P/N 65K90SM-31).

What's Next

Continue to "Provision the Voice User" on page 4-45.

Provision the Voice User

The user provisioning process is repeated for each individual customer and is typically as automated as possible. Except for the SIP identity which is unique in the system or network. Each user must be associated with a particular FXS port and registered to a specific SIP trunk.

To provision a user to a particular FXS port and registered to a specific SIP trunk, complete the following:

1. Access the Voice User menu.

   Services > **Voice** > **SIP** > **Voice Users**

2. Enter the user number for this voice user. This is typically the phone number associated with this user.
3. Select the dialing profile to be used by this user. If you did not create a dialing profile, a default profile (DEFAULT_DP) is provided.
4. Select the class of service to be used by this user. If you did not create a CoS, a default rule (DEFAULT_COS) is provided.
5. Enter the SIP identity.

   The parameters should match the SIP identity in the SIP call-router. A common practice is to also user the customer's phone number here. It is not necessary, however, and the SIP identity can be any string that does not contain the following characters:
   `@^[]{}\ |:<>?" and <space>.

6. Enter the trunk number created previously.
7. Enter the authentication name. This is typically the phone number associated with this user.
8. Enter the authentication password for this user.
9. Enter the index of the FXS slot/port to be associated with this user. Example: 1/2.
10. Click **Apply**.

What's Next

For Non-OMCI SIP, this completes provisioning. Services should be up and running. To provision another service, continue to "Step 2: Service Provisioning" on page 4-5.

Provision the OMCI SIP Users

All profiles (media, CODEC, call-feature, etc.) can be shared across multiple voice users. To create a SIP user, complete the following steps:

1. Navigate to the Users menu.

   Services > **Voice FTTx** > **SIP** > **Users**

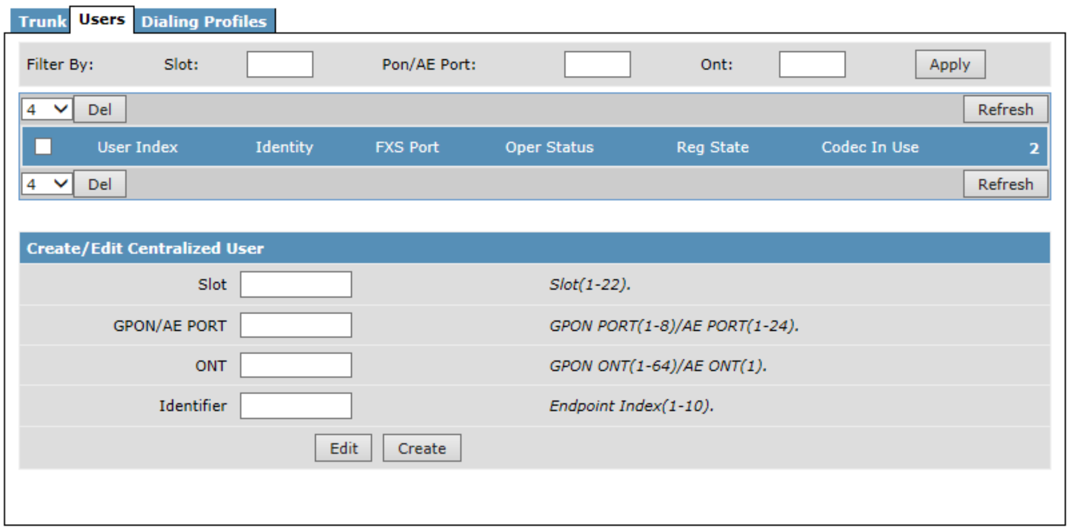


Figure 4-18. SIP User Create

2. Enter the slot number.
3. Enter the GPON/AE port.
4. Enter the ONT.
5. Enter a unique identifier number.
6. Click **Create**. The provision SIP User menu appears.

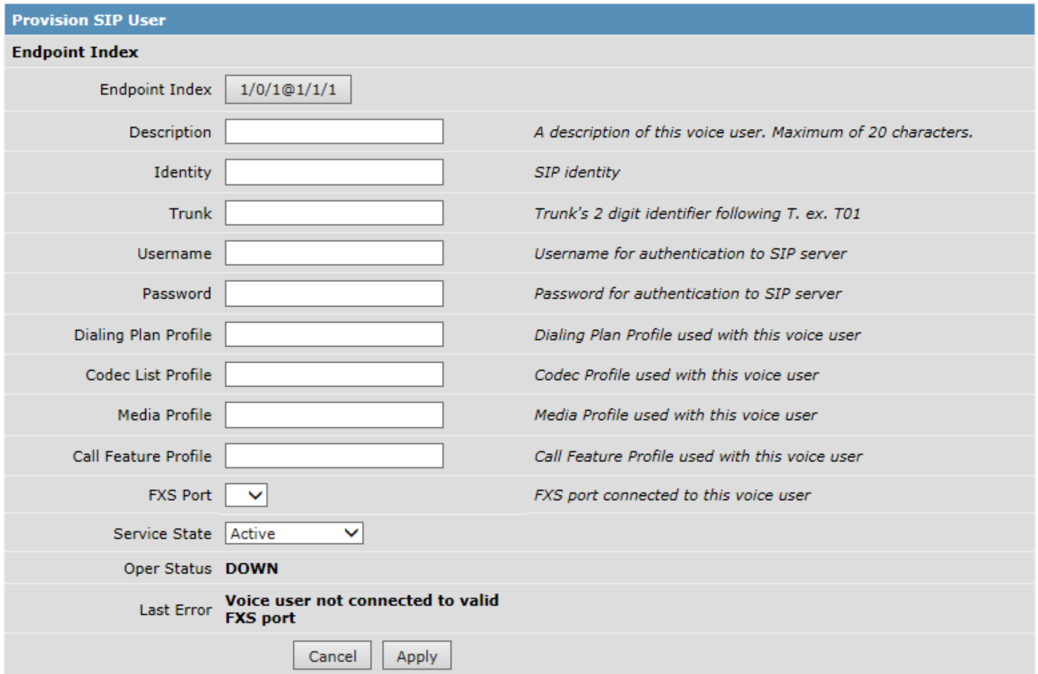


Figure 4-19. SIP User Edit

7. Enter a description for this voice user. This is typically the phone number associated with this user.
8. Enter the SIP identity.
9. It is a common practice to also use the customer's phone number here. It is not necessary, however, and the SIP Identity can be any string that does not contain the following characters: `@^[]{}\ | :<>?" and <space>.
10. Enter the trunk number created previously.
11. Enter the username. This is typically the phone number associated with this user.
12. Enter the password for this user.
13. Enter the Dialling Plan Profile to be used for this voice user. ADTRAN provides a default dialing plan profile called DEFAULT_DP.
14. Enter the Codec List Profile to be used for this voice user.

15. Enter the Media Profile to be used for this voice user.
16. Enter the Call Feature Profile to be used for this voice user.
17. Enter the FXS port connected to this voice user.
18. Set the Service State to **Active**.
19. Click **Apply**.

What's Next

For OMCI SIP, this completes provisioning. Services should be up and running. To provision another service, continue to "Step 2: Service Provisioning" on page 4-5.

Provision OMCI MGCP Endpoints

To create the MGCP profile, complete the following:

1. Navigate to the Endpoints menu.

   Services > **Voice FTTx** > **MGCP** > **Endpoints**
2. Enter the slot number.
3. Enter the GPON/AE port.
4. Enter the ONT.
5. Enter a unique identifier number.
6. Click **Create**. The Provision MGCP Endpoint menu appears.
7. Enter the MGCP Profile to be used by this voice user.
8. Enter the Media Profile to be used for this voice user.
9. Enter the Call Feature Profile to be used for this voice user.
10. Enter the FXS port connected to this voice user.
11. Set the Service State to **Active**.
12. Click **Apply**.

What's Next

For OMCI MGCP, this completes provisioning. Services should be up and running. To provision another service, continue to "Step 2: Service Provisioning" on page 4-5.

Provision GR-303

To provision for GR-303, complete the following steps:

1. Access the DS1 Voice Gateway.

   DS1 VG > **Provisioning** > **Card**
2. Set the service state to In Service.
3. Set the Call Control Mode to GR-303.
4. Set the required DS1 ports to In Service.

   DS1 VG > **Provisioning** > **DS1**
5. Assign a name to the interface group.

   DS1 VG > **Provisioning** > **GR-303 > Other Provisioning**
6. Set the switch type.
7. Assign the physical ports, from step 4, being used as the primary, secondary, and normal.

   DS1 VG > **Provisioning** > **GR-303 > Switch DS1s**
8. Set the number of CRVs.

   DS1 VG > **Provisioning** > **GR-303 > Subscribers**
9. Set the Start CRV.
10. Set the Node.
11. Set the Slot.
12. Set the Provisioning Mode to either **GPON** or **Active Ethernet**.
13. Set the start port.
14. Click **Apply**.

What's Next

For GR-303 voice, this completes provisioning. Services should be up and running. To provision another service, continue to "Step 2: Service Provisioning" on page 4-5.