



Total Access 5000 Series

FTTP

Fiber to the Premises

P/N: 65K110FTTP

Basic Configuration Guide

To the Holder of this Document

This document is intended for the use of ADTRAN customers only for the purposes of the agreement under which the document is submitted, and no part of it may be used, reproduced, modified or transmitted in any form or means without the prior written permission of ADTRAN.

The contents of this document are current as of the date of publication and are subject to change without notice.

Trademark Information

“ADTRAN” and the ADTRAN logo are registered trademarks of ADTRAN, Inc. Brand names and product names included in this document are trademarks, registered trademarks, or trade names of their respective holders.

Disclaimer of Liability

The information or statements given in this document concerning the suitability, capacity, or performance of the mentioned hardware or software products are given “as is”, and any liability arising in connection with such hardware or software products shall be governed by ADTRAN’s standard terms and conditions of sale unless otherwise set forth in a separately negotiated written agreement with ADTRAN that specifically applies to such hardware or software products.

To the fullest extent allowed by applicable law, in no event shall ADTRAN be liable for errors in this document for any damages, including but not limited to special, indirect, incidental or consequential, or any losses, such as but not limited to loss of profit, revenue, business interruption, business opportunity or data, that may arise from the use of this document or the information in it.



Important Notice on Product Safety

This product may present safety risks due to laser, electricity, heat, and other sources of danger.

Only trained and qualified personnel may install, operate, maintain or otherwise handle this product and only after having carefully read the safety information applicable to this product.

Safety and Regulatory information is provided in this document and/or a separate Safety and Regulatory document that is part of the product-applicable document set.



Copyright © 2020 ADTRAN, Inc.
All Rights Reserved.

Revision History

Rev A	January 2020	Initial release.
-------	--------------	------------------

Table of Contents

Overview	21
Scope of this Guide	21
In this Guide	21
Hazard and Advisory Symbols	23
Related Online Documentation and Resources.....	24

Fiber to the Premises Overview27

1.1	Scope	27
1.2	In this Section.	27
1.3	GPON Overview.....	28
1.3.1	Customer VLAN (C-VLAN) Model	30
1.3.2	N:1 Service VLAN (S-VLAN) Model	31
1.3.3	Hybrid N+1:1 Combined VLAN Model	32
1.4	Fiber to the Premises with Active Ethernet Overview	33
1.4.1	Customer 1:1 VLAN (C-VLAN) Model	34
1.4.2	N:1 Service VLANs Model	35
1.5	Voice Overview	37
1.5.1	GR-303 Description	37
1.5.2	MGCP Description	37
1.5.2.1	Call Agent and Endpoint Communication.	38
1.5.2.2	Standards	38
1.5.3	SIP Description	39
1.5.3.1	Benefits	39
1.5.3.2	Terminating Multimedia Communications (Five SIP Facets)	40
1.5.3.3	SIP Pre-Installation Requirements	40
1.6	Command Line Interface Overview	42
1.6.1	Command Modes	42
1.6.2	CLI Shortcuts	43
1.6.3	CLI Error Messages	44
1.6.4	CLI Input Descriptions	45
1.6.5	CLI Login	47
1.7	User Interface	47

GPON Provisioning using CLI.49

2.1	Scope of this Section	49
2.2	In this Section.	49

2.3	Provisioning	50
2.3.1	OLT/PON Provisioning	50
2.3.1.1	Enable the OLT Module	50
2.3.1.2	Provision the PON	50
2.3.1.3	Enter the Registration-ID	53
2.3.1.3.1	Registration-ID Entry for Total Access 3xx	53
2.3.1.3.2	Registration-ID Entry for Total Access 421x /Total Access 421xw	55
2.3.1.3.3	Total Access 421x/Total Access 421xw LEDs	56
2.3.1.3.4	Registration-ID Entry for Total Access 3xx Residential Gateway	57
2.3.1.3.5	Registration-ID Entry for Total Access 324RG and 334RG	58
2.3.1.3.6	Registration-ID Entry for Total Access 324 3rd Generation and Total Access 374	59
2.3.1.3.7	Registration-ID Entry for Total Access 4xx	60
2.3.1.4	Discover the ONT	61
2.3.2	Service Provisioning	62
2.3.2.1	Voice	62
2.3.2.1.1	SIP	62
2.3.2.1.2	MGCP	62
2.3.2.1.3	GR-303	62
2.3.2.1.4	Select Your Voice Option	63
2.3.2.1.5	SIP OMCI Voice	63
2.3.2.1.6	SIP Non-OMCI Voice	64
2.3.2.1.7	MGCP OMCI Voice	64
2.3.2.1.8	MGCP Non-OMCI Voice	65
2.3.2.1.9	GR-303 Voice	65
2.3.2.2	Data	66
2.3.2.3	Video	66
2.3.2.4	RF-Video	66
2.3.2.5	Transport Layer Security (TLS)	66
2.3.2.5.1	Select Your TLS Option	67
2.3.2.5.2	TLS Single Tag Configuration	67
2.3.2.5.3	TLS Double Tag Configuration	67
2.3.3	Create an EVC	68
2.3.4	Set the Voice Service Mode on the ONT	73
2.3.5	Provision the Port on the ONT	74
2.3.5.1	Ethernet	74
2.3.5.2	FXS	75
2.3.5.3	RF-Video	76
2.3.5.4	Virtual Gigabit Interface	77
2.3.5.5	VDSL Interface	78
2.3.5.6	Provision the EFM Port	81
2.3.6	Create an IP Host	82
2.3.7	Create an EVC-Map	83
2.3.8	Provision the SIP Trunk	93
2.3.8.1	Configure additional SIP Trunks	94
2.3.9	Provision the MGCP Profile	95

2.3.10	Provision Non-OMCI MGCP Endpoints	96
2.3.11	Provision the SIP Dialing Profile	98
2.3.11.1	Dial Plan Pattern Restrictions.	98
2.3.11.2	SPRE Pattern Restrictions	99
2.3.11.3	External Line Code Restrictions	100
2.3.11.4	Dial Plan Provisioning	101
2.3.12	Provision Class of Service (CoS) (Optional)	104
2.3.13	Provision for Global Voice (Optional)	105
2.3.14	Provision the Voice User	106
2.3.15	Provision the Media Profile (Optional)	107
2.3.16	Provision the CODEC Profile (Optional)	108
2.3.17	Provision the Call Feature Profile (Optional)	109
2.3.18	Provision the OMCI SIP Users	111
2.3.19	Provision OMCI MGCP Endpoints	113
2.3.20	Provision GR-303	114

Provisioning using the Web GUI.115

3.1	Scope of this Section	115
3.2	In this Section.	115
3.3	Provisioning	116
3.3.1	OLT/PON Provisioning.	116
3.3.1.1	Enable the OLT Module	116
3.3.1.2	Provision the PON	117
3.3.1.3	Enter the Registration-ID	119
3.3.1.3.1	Registration-ID Entry for Total Access 3xx	120
3.3.1.3.2	Registration-ID Entry for Total Access 421x /Total Access 421xw	122
	Total Access 421x/Total Access 421xw LEDs	123
3.3.1.3.3	Registration-ID Entry for Total Access 3xx Residential Gateway	124
	Set Registration ID Activation using a Telco Butt Set	124
3.3.1.3.4	Registration-ID Entry for Total Access 324RG and 334RG	126
3.3.1.3.5	Registration-ID Entry for Total Access 324 3rd Generation and Total Access 374.	127
3.3.1.3.6	Registration-ID Entry for Total Access 4xx	128
3.3.1.4	Discover the ONT.	129
3.3.2	Service Provisioning.	130
3.3.2.1	Voice	130
3.3.2.1.1	SIP	130
3.3.2.1.2	MGCP	130
3.3.2.1.3	GR-303.	130
3.3.2.1.4	Select Your Voice Option	131
3.3.2.1.5	SIP OMCI Voice	131
3.3.2.1.6	SIP Non-OMCI Voice	132
3.3.2.1.7	MGCP OMCI Voice	133
3.3.2.1.8	MGCP Non-OMCI Voice	134

3.3.2.1.9	GR-303 Voice	135
3.3.2.2	Data	136
3.3.2.3	Video	137
3.3.2.4	RF-Video	138
3.3.2.5	TLS	139
3.3.2.5.1	Select Your TLS Option	140
3.3.2.5.2	TLS Single Tag Configuration	140
3.3.2.5.3	TLS Double Tag Configuration	141
3.3.3	Create an EVC	142
3.3.4	Set the Voice Service Mode on the ONT	145
3.3.5	Provision the Port on the ONT	146
3.3.5.1	Ethernet	147
3.3.5.2	FXS	148
3.3.5.3	RF-Video	149
3.3.5.4	Virtual Gigabit Interface	150
3.3.6	Create an IP Host	151
3.3.7	Create an EVC-Map	153
3.3.8	Provision the SIP Trunk	159
3.3.9	Provision the MGCP Profile	161
3.3.10	Provision Non-OMCI MGCP Endpoints	162
3.3.11	Provision the SIP Dialing Profile	163
3.3.11.1	Dial Plan Pattern Restrictions	163
3.3.11.2	SPRE Pattern Restrictions	164
3.3.11.3	External Line Code Restrictions	165
3.3.11.4	Dial Plan Provisioning	166
3.3.12	Provision the Common Profiles (Optional)	167
3.3.12.1	Provision the Call Features Profile	167
3.3.12.2	Provision the Media Profile	169
3.3.12.3	Provision the Codec Profile	170
3.3.13	Provision Class of Service (CoS) (Optional)	171
3.3.14	Provision for Global Voice (Optional)	172
3.3.15	Provision the Voice User	173
3.3.16	Provision the OMCI SIP Users	174
3.3.17	Provision OMCI MGCP Endpoints	176
3.3.18	Provision GR-303	177

Provisioning Active Ethernet using CLI 179

4.1	Scope of this Section	179
4.2	In this Section	179
4.3	Provisioning	180
4.4	In this Section	180
4.4.1	OLT/PON Provisioning	180
4.4.1.1	Enable the OLT Module	180

4.4.1.2	Discover the ONT	181
4.4.1.3	ONT Inband Management Provisioning	182
4.4.2	Service Provisioning	183
4.4.2.1	Voice	183
4.4.2.1.1	SIP	183
4.4.2.1.2	MGCP	183
4.4.2.1.3	GR-303	183
4.4.2.1.4	Select Your Voice Option	184
4.4.2.1.5	SIP OMCI Voice	185
4.4.2.1.6	SIP Non-OMCI Voice	186
4.4.2.1.7	MGCP OMCI Voice	187
4.4.2.1.8	MGCP Non-OMCI Voice	188
4.4.2.1.9	GR-303 Voice	189
4.4.2.2	Data	190
4.4.2.3	Video	191
4.4.2.4	TLS	192
4.4.3	Create an EVC	193
4.4.4	Set the Voice Service Mode on the ONT	198
4.4.5	Provision the Port on the ONT	199
4.4.5.1	Ethernet	199
4.4.5.2	FXS	200
4.4.5.3	Virtual Gigabit Interface	201
4.4.6	Create an IP Host	202
4.4.7	Create an EVC-Map	203
4.4.8	Provision the SIP Trunk	213
4.4.9	Provision the MGCP Profile	214
4.4.10	Provision Non-OMCI MGCP Endpoints	215
4.4.11	Provision the SIP Dialing Profile	217
4.4.11.1	Dial Plan Pattern Restrictions	217
4.4.11.2	SPRE Pattern Restrictions	219
4.4.11.3	External Line Code Restrictions	220
4.4.11.4	Dial Plan Provisioning	220
4.4.12	Provision Class of Service (CoS) (Optional)	223
4.4.13	Provision for Global Voice (Optional)	224
4.4.14	Provision the Voice User	225
4.4.15	Provision the Media Profile (Optional)	226
4.4.16	Provision the CODEC Profile (Optional)	228
4.4.17	Provision the Call Feature Profile (Optional)	229
4.4.18	Provision the OMCI SIP Users	231
4.4.19	Provision OMCI MGCP Endpoints	233
4.4.20	Provision GR-303	234

Provisioning Active Ethernet using the Web235

5.1	Scope of this Section	235
5.2	In this Section	235

5.3	Provisioning	236
5.3.1	OLT/PON Provisioning	236
5.3.1.1	Enable the OLT Module	236
5.3.1.2	Discover the ONT	236
5.3.1.3	ONT Inband Management Provisioning	238
5.3.2	Service Provisioning	239
5.3.2.1	Voice	239
5.3.2.1.1	SIP	239
5.3.2.1.2	MGCP	239
5.3.2.1.3	GR-303	239
5.3.2.1.4	Select Your Voice Option	240
5.3.2.1.5	SIP OMCI Voice	241
5.3.2.1.6	SIP Non-OMCI Voice	242
5.3.2.1.7	MGCP OMCI Voice	243
5.3.2.1.8	MGCP Non-OMCI Voice	244
5.3.2.1.9	GR-303 Voice	245
5.3.2.2	Data	246
5.3.2.3	Video	247
5.3.3	Create an EVC	248
5.3.4	Set the Voice Service Mode on the ONT	251
5.3.5	Provision the Port on the ONT	252
5.3.5.1	Ethernet Port Provisioning	253
5.3.5.2	FXS Port Provisioning	254
5.3.5.3	Virtual Gigabit Interface	255
5.3.6	Create an IP Host	256
5.3.7	Create an EVC-Map	258
5.3.8	Provision the SIP Trunk	263
5.3.9	Provision the MGCP Profile	265
5.3.10	Provision Non-OMCI MGCP Endpoints	266
5.3.11	Provision the SIP Dialing Profile	267
5.3.11.1	Dial Plan Pattern Restrictions	267
5.3.11.2	SPRE Pattern Restrictions	269
5.3.11.3	External Line Code Restrictions	270
5.3.11.4	Dial Plan Provisioning	271
5.3.12	Provision the Common Profiles (Optional)	272
5.3.12.1	Provision the Call Features Profile	272
5.3.12.2	Provision the Media Profile	274
5.3.12.3	Provision the Codec Profile	276
5.3.13	Provision Class of Service (CoS) (Optional)	277
5.3.14	Provision for Global Voice (Optional)	278
5.3.15	Provision the Voice User	279
5.3.16	Provision the OMCI SIP Users	280
5.3.17	Provision OMCI MGCP Endpoints	282
5.3.18	Provision GR-303	283

GPON Configurations285

6.1	Scope of this Section	285
6.2	In this Section.	285
6.3	VLAN/TLS/IPTV Examples	286
6.3.1	1:1 Customer VLAN (C-VLAN) Examples	287
6.3.1.1	Example 1:1 Example	288
6.3.2	N:1 Service VLAN (S-VLAN) Examples	290
6.3.2.1	N:1 Service VLAN Example 1	291
6.3.2.2	N:1 Service VLAN Example 2	294
6.3.3	Hybrid N+1:1 Combined VLAN Examples	297
6.3.3.1	Hybrid N+1:1 Example 1	298
6.3.3.2	Hybrid N+1:1 Example 2	301
6.4	TLS Configuration Examples	304
6.4.1	TLS Example 1.	304
6.4.2	TLS Example 2.	305
6.4.3	IPTV Configuration Examples	307

Active Ethernet Configurations.309

7.1	Scope of this Section	309
7.2	In this Section.	309
7.3	1:1 Customer VLAN (C-VLAN) Examples	310
7.3.1	Example 1:1 Example	311
7.4	N:1 Service VLANs	313
7.4.1	N:1 Service VLAN Example 1	314
7.4.2	N:1 Service VLAN Example 2	317
7.5	Hybrid N+1:1 Combined VLAN Examples	320
7.5.1	Hybrid N+1:1 Example 1	321
7.5.2	Hybrid N+1:1 Example 2	324
7.6	TLS Examples	327
7.6.1	TLS Example 1.	327
7.6.2	TLS Example 2.	328

Traffic Management331

8.1	Scope of this Section	331
8.2	In this Section.	331
8.3	Shapers, GPON	332

8.3.1	Downstream Shaping	332
8.3.2	Upstream Shaping	333
8.4	Provisioning using CLI	334
8.4.1	Downstream Shaper	334
8.4.2	Downstream Shaper for Multiple Customers	334
8.4.2.1	P-Bit to Queue Mapping	334
8.4.2.2	EVC Map to QoS Map	334
8.4.2.3	Queue Scheduling	335
8.4.3	Upstream Shaper	335
8.4.3.1	Upstream Shaping Example	336
8.4.3.2	Downstream GPON QoS for User Fairness	337
8.4.3.2.1	Total Minimum Rate Threshold Provisioning	339
8.4.3.2.2	Per Service Model	339
8.4.3.2.3	Single Subscriber Per ONT Model Example	341
8.4.3.2.4	Example Scenario	344
	Scenario 1 - Congested PON	345
	Scenario 2 - Congested PON	345
	Scenario 3 - Uncongested PON	347
	Scenario 4 - Uncongested PON	348
8.4.4	Web	349
8.4.4.1	Downstream Shaper Provisioning	349
8.4.4.2	Downstream Shaper Provisioning for Multiple Customers	349
8.4.4.2.1	P-Bit to Queue Mapping	349
8.4.4.2.2	EVC Map to QoS Map	350
8.4.4.2.3	Queue Scheduling	350
8.5	Example	351
8.5.1	Step 1: Create Unique Queues for Each Port	351
8.5.2	Step 2: Attach the Downstream Queue Profiles and Upstream Channels to Each Port	351
8.5.3	Step 3: Attach the Downstream Shapers to the Specified Queues from the Map Profiles	351
8.5.4	Step 4: Attach the Upstream Shapers to the Specified Channels	352
8.5.5	Attach/Detach Interface to the Shaper	352
8.6	Shapers, AE (Example)	353
8.6.1	Provisioning	353
8.6.1.1	CLI	353
8.6.1.1.1	Downstream Shaper Provisioning	353
8.6.1.1.2	Upstream Shaper Provisioning	354
8.6.2	Web	355
8.6.2.1	Downstream Shaper Provisioning	355
8.6.2.2	Upstream Shaper Provisioning	355
8.7	Policers, AE (Example)	357
8.7.1	Provisioning	357
8.7.1.1	CLI	357

8.7.2	Web	358
SFP Information		361
9.1	Scope of this Section	361
9.2	In this Section.	361
9.3	Information Command	362
9.3.1	Example	362
3rd Party ONT Provisioning for Active Ethernet		363
10.1	Scope of this Section	363
10.2	In this Section.	363
10.3	Provisioning	364
10.3.1	Example Provisioning.	365
Home Phoneline Networking Alliance		367
11.1	Scope of this Section	367
11.2	In this Section.	367
11.3	Introduction to HPNA	368
11.4	Provisioning	368
IEEE 802.1X		371
12.1	Scope of this Section	371
12.2	In this Section.	371
12.3	Introduction	372
12.3.1	Port-Based Authentication	372
12.3.2	RADIUS Relay Agent	373
12.3.2.1	RADIUS Attributes	373
12.4	Provisioning	375
12.4.1	Step 1: Provision a Subtended Host for RADIUS Client	375
12.4.2	Step 2: Provision a RADIUS Server and Group	377
12.4.3	Step 3: Provision the ONT Port	378
12.4.4	Step 4: Provision the RADIUS Relay Agent	379
12.4.5	Step 5: Enable System-Wide 802.1X Authentication	382
12.5	Show Commands	383
12.5.1	Status Commands	383

12.5.1.1	GPON Port Status	383
12.5.1.2	GPON Port Provisioning.	383
12.5.1.3	ONT Port Status.	383
12.5.1.4	ONT Port Provisioning	384
12.5.1.5	ONT Gigabit Port 802.1X Status	384
12.5.1.6	Radius Relay Agent Status	384
12.5.2	Performance-Monitoring Commands	385
12.5.2.1	Current ONT 802.1X Statistics.	385
12.5.2.2	Previous ONT 802.1X Statistics.	385
12.5.2.3	Current ONT Radius Statistics	385
12.5.2.4	Previous ONT Radius Statistics	386
12.5.2.5	Current Relay Agent Statistics	386
12.5.2.6	Previous Relay Agent Statistics	386
12.6	Provisioning Examples.	387
12.6.1	Example 1 - One RADIUS Server in the Network with RADIUS Relay	387
12.6.2	Example 2 - Two RADIUS Servers in the Network without RADIUS Relay Agent	389

Activation Mode391

13.1	Scope of this Section	391
13.2	In this Section.	391
13.3	Manual Activation.	392
13.3.1	Pro	392
13.3.2	Con.	392
13.4	Auto-Discovery.	393
13.4.1	Pros	393
13.4.2	Cons.	393
13.5	Auto-Activation.	394
13.5.1	Pros	394
13.5.2	Cons.	394
13.6	Registration-ID Activation.	395
13.6.1	Pros	396
13.6.2	Cons.	397

ONT Capability Provisioning399

14.1	Scope of this Section	399
14.2	In this Section.	400
14.3	Adding a New ONT Part Number.	401

14.4 Removing an ONT Part Number 402

14.5 Adding a Vendor Name 403

14.6 Removing a Vendor Name..... 404

14.7 Restoring a Fixed Part Number Entry to Default Value 405

14.8 Restoring Vendor Entry to Default Value 406

14.9 ONT Capability Provisioning Terms 408

Warranty and Contact Information409

List of Figures

Figure 1-1.	Total Access 5000 GPON General Application Diagram	29
Figure 1-2.	1:1 Customer VLAN Diagram	30
Figure 1-3.	N:1 Service VLAN Diagram	31
Figure 1-4.	Hybrid N+1:1 Combined VLAN Diagram	32
Figure 1-5.	Total Access 5000 Active Ethernet General Application Diagram	33
Figure 1-6.	Customer 1:1 VLAN Diagram	34
Figure 1-7.	N:1 Service VLAN Diagram	35
Figure 1-8.	Hybrid N+1:1 Combined VLAN Diagram	36
Figure 1-9.	MGCP Network	37
Figure 1-10.	ONT MGCP Endpoints	38
Figure 1-11.	Total Access 5000 Logon Screen	47
Figure 1-12.	User Statistics Dialog Box	48
Figure 2-1.	401 Web GUI Display	60
Figure 3-1.	OLT Card Service Provisioning	116
Figure 3-2.	PON Provisioning	117
Figure 3-3.	401 Web GUI Display	128
Figure 3-4.	ONT Provisioning	129
Figure 3-5.	Create EVC	142
Figure 3-6.	Edit EVC	143
Figure 3-7.	Edit EVC	144
Figure 3-8.	Voice Service Mode	145
Figure 3-9.	ONT Port Provisioning	146
Figure 3-10.	ONT Port Provisioning	147
Figure 3-11.	FXS Port Provisioning	148
Figure 3-12.	RF-Video Port Provisioning	149
Figure 3-13.	IP-Host Create Menu	151
Figure 3-14.	IP-Host Provisioning	151
Figure 3-15.	EVC-Map Create	153
Figure 3-16.	EVC-Map Edit	154
Figure 3-17.	EVC-Map Advanced	157
Figure 3-18.	EVC-Map IGMP	157
Figure 3-19.	SIP Trunk Create	159
Figure 3-20.	Dial Plan Provisioning	166
Figure 3-21.	SIP User Create	174
Figure 3-22.	SIP User Edit	175
Figure 5-1.	OLT Card Service Provisioning	236
Figure 5-2.	GE Provisioning	237
Figure 5-3.	ONT Inband Management Provisioning	238
Figure 5-4.	Create EVC	248
Figure 5-5.	Edit EVC	249
Figure 5-6.	Edit EVC	250
Figure 5-7.	Voice Service Mode	251
Figure 5-8.	ONT Port Provisioning	252

Figure 5-9.	ONT Ethernet Port Provisioning	253
Figure 5-10.	FXS Port Provisioning	254
Figure 5-11.	IP-Host Create Menu	256
Figure 5-12.	IP-Host Provisioning	256
Figure 5-13.	EVC-Map Create	258
Figure 5-14.	EVC-Map Edit	259
Figure 5-15.	EVC-Map Advanced	261
Figure 5-16.	EVC-Map IGMP	261
Figure 5-17.	SIP Trunk Create	263
Figure 5-18.	Dial Plan Provisioning	271
Figure 5-19.	SIP User Create	280
Figure 5-20.	SIP User Edit	281
Figure 6-1.	1:1 Customer VLAN Diagram	287
Figure 6-2.	N:1 Service VLAN Diagram	290
Figure 6-3.	Hybrid N+1:1 Combined VLAN Diagram	297
Figure 7-1.	1:1 Customer VLAN Diagram	310
Figure 7-2.	N:1 Service VLAN Diagram	313
Figure 7-3.	Hybrid N+1:1 Combined VLAN Diagram	320
Figure 8-1.	GPON Downstream Shaping Hierarchy	333
Figure 8-2.	Per PON Bandwidth Thresholds Example	338
Figure 8-3.	Downstream QoS for Single Subscriber	341
Figure 8-4.	Example Provisioning of Weights and Minimum Rates	344
Figure 12-1.	Port Authentication Overview	372
Figure 14-1.	Adding a New ONT Part Number	401
Figure 14-2.	Removing an ONT Part Number	402
Figure 14-3.	Adding a Vendor Name	403
Figure 14-4.	Removing Vendor Name	404
Figure 14-5.	Entry Before being Restored to Default Value	405
Figure 14-6.	Restored Entry to Default Value	405
Figure 14-7.	Restoring Vendor Entry to Default Value	406
Figure 14-8.	Restored Entry to Default Value	407

List of Tables

Table 1.	List of Topics in the Guide	21
Table 2.	Related Online Documents and Resources	24
Table 1-1.	Section 1 Topics	27
Table 1-2.	Five Facets of SIP	40
Table 1-3.	Command Modes	42
Table 1-4.	CLI Shortcuts	43
Table 1-5.	Error Messages	44
Table 1-6.	Input Descriptions	45
Table 2-1.	Section 1 Topics	49
Table 2-2.	Activation Mode	51
Table 2-3.	Range Description	51
Table 2-4.	Inband Management	52
Table 2-5.	Registration-ID	53
Table 2-6.	ONT Status	53
Table 2-7.	Registration-ID Acceptance	54
Table 2-8.	Registration-ID Status	54
Table 2-9.	Front Panel LEDs	56
Table 2-10.	Discover the ONT	61
Table 2-11.	Voice Options	63
Table 2-12.	EVC and TLS	67
Table 2-13.	Voice Options	67
Table 2-14.	Non-Default Metro Ethernet Network Interface	69
Table 2-15.	MAC-Switching	69
Table 2-16.	Subscriber Modes	70
Table 2-17.	Discover the ONT	73
Table 2-18.	Port Type	74
Table 2-19.	VDSL Deployment Syntax	79
Table 2-20.	IP Host Management	82
Table 2-21.	Interface Type	83
Table 2-22.	Subscriber Modes	85
Table 2-23.	Authentication Mode Description	86
Table 2-24.	DHCPv6 Access Modes	87
Table 2-25.	Supported Variables	88
Table 2-26.	Additional EVC-Map Configurations	91
Table 2-27.	Dial Plan Options	101
Table 2-28.	SPRE Options	102
Table 2-29.	External Line Code Options	103
Table 2-30.	Media Profile Options	107
Table 2-31.	CODEC Profile Options	108
Table 2-32.	Call Feature Profile Options	109
Table 2-33.	SIP Voice User Options	111
Table 3-1.	Section 3 Topics	115
Table 3-2.	Range Description	118

Table 3-3.	Registration-ID	119
Table 3-4.	ONT Status	120
Table 3-5.	Registration-ID Acceptance	120
Table 3-6.	Registration-ID Status	121
Table 3-7.	Front Panel LEDs	123
Table 3-8.	ONT Discovery Method	129
Table 3-9.	Voice Options	131
Table 3-10.	EVC and TLS	139
Table 3-11.	Voice Options	140
Table 3-12.	MAC-Switching	143
Table 3-13.	Port Type	146
Table 3-14.	Interface Type	155
Table 3-15.	Authentication Method	156
Table 3-16.	Common Profiles	167
Table 3-17.	Call Feature Profile Options	167
Table 3-18.	Media Profile Options	169
Table 3-19.	CODEC Profile Options	170
Table 4-1.	Section 4 Topics	179
Table 4-2.	Inband Management	182
Table 4-3.	Voice Options	184
Table 4-4.	Non-Default Metro Ethernet Network Interface	193
Table 4-5.	MAC-Switching	194
Table 4-6.	Subscriber Modes	195
Table 4-7.	Discover the ONT	198
Table 4-8.	Port Type	199
Table 4-9.	IP Host Management	202
Table 4-10.	Interface Type	203
Table 4-11.	Subscriber Modes	204
Table 4-12.	Authentication Mode Description	205
Table 4-13.	DHCPv6 Access Modes	206
Table 4-14.	Supported Variables	207
Table 4-15.	Additional EVC-Map Configurations	210
Table 4-16.	Dial Plan Options	221
Table 4-17.	SPRE Options	222
Table 4-18.	External Line Code Options	222
Table 4-19.	Media Profile Options	226
Table 4-20.	CODEC Profile Options	228
Table 4-21.	Call Feature Profile Options	229
Table 4-22.	SIP Voice User Options	231
Table 5-1.	Section 5 Topics	235
Table 5-2.	Inband Management	238
Table 5-3.	Voice Options	240
Table 5-4.	Port Type	252
Table 5-5.	Interface Type	260
Table 5-6.	Authentication Method	260
Table 5-7.	Common Profiles	272

Table 5-8.	Call Feature Profile Options	272
Table 5-9.	Media Profile Options	274
Table 5-10.	CODEC Profile Options	276
Table 6-1.	Section 6 Topics	285
Table 7-1.	Section 7 Topics	309
Table 8-1.	Section 8 Topics	331
Table 8-2.	Congested PON Example 1	345
Table 8-3.	Congested PON Example 2	345
Table 8-4.	Uncongested PON Example 1	347
Table 8-5.	Uncongested PON Example 2	348
Table 9-1.	Section 9 Topics	361
Table 10-1.	Section 10 Topics	363
Table 11-1.	Section 11 Topics	367
Table 12-1.	Section 12 Topics	371
Table 12-2.	RADIUS Attributes	373
Table 12-3.	Inband Management	376
Table 12-4.	Additional Options	378
Table 12-5.	Additional Options	381
Table 13-1.	Section 13 Topics	391
Table 14-1.	Section 14 Topics	400

Overview

This guide provides installation instructions for provisioning Fiber to the Premises (FTTP). This guide provides both CLI and GUI instructions.

Scope of this Guide

The Total Access 5000 Series FTTP Basic Configuration Guide is designed for planning a network or provisioning service. This guide provides application and technology overviews, example configurations, and provisioning steps to help you get service up and running. Use this guide as a base for tailoring your system to your specific requirements.

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 Guide

This guide contains the topics listed in [Table 1](#).

Table 1. List of Topics in the Guide

Section	Topic	Scope
1	“Fiber to the Premises Overview”	This section provides an overview of provisioning FTTP to a customer’s premises.
2	“GPON Provisioning using CLI”	This section provides provisioning for GPON using CLI.
3	“Provisioning using the Web GUI”	This section provides provisioning for GPON using the Web GUI.
4	“Provisioning Active Ethernet using CLI”	This section provides the minimum amount of steps required to provision a GPON module for the FTTP application using Active Ethernet and CLI.
5	“Provisioning Active Ethernet using the Web”	This section provides the minimum amount of steps required to provision a GPON module for the FTTP application using Active Ethernet using the Web GUI.
6	“GPON Configurations”	This section provides examples of common Total Access 5000 GPON configurations.
7	“Active Ethernet Configurations”	This section provides examples of common Total Access 5000 Active Ethernet configurations.
8	“Traffic Management”	This section covers Traffic Management (shapers and policers) provisioning that can be applied to your network.

Table 1. List of Topics in the Guide (Continued)

Section	Topic	Scope
9	“SFP Information”	This section provides the command to display the CLEI code information of an installed SFP in the selected GPON OLT.
10	“3rd Party ONT Provisioning for Active Ethernet”	This section provides the minimum steps required for third party ONT provisioning for an Active Ethernet (AE) deployment. It also provides an example deployment
11	“Home Phoneline Networking Alliance”	This section provides a brief overview of Home Phoneline Networking Alliance (HPNA), and how to provision for HPNA
12	“IEEE 802.1X”	This section provides an overview of the IEEE 802.1X feature, provisioning options, useful show commands, and example provisioning for this feature.
13	“Activation Mode”	This section provides four different methods for activating your GPON ONT. Each method contains a list of pros and cons associated with that registration method.
14	“ONT Capability Provisioning”	This section provides a method to configure the OLT for the expected functionality of an ONT. The main purpose of this feature is to ease integration of new ONTs into the system.
15	“Warranty and Contact Information”	This section provides Warranty and contact information.
	“Acronyms”	This section provides a list of acronyms used throughout this guide,

Hazard and Advisory Symbols

The following Hazard symbols are used throughout this guide:

**WARNING!**

Warning: Service affecting. Possible risk of system failure.

**CAUTION!**

Caution: Indicates that a failure to take or avoid a specific action could result in a loss of data.

**NOTICE!**

Notice: Provides information that is essential to the completion of a task.

**NOTE**

Note: Information that emphasizes or supplements important points of the main text.

Related Online Documentation and Resources

Refer to [Table 2](#) for additional information on Total Access 5000 FTTP applications.

Documentation for ADTRAN Carrier Networks products is available for viewing and download directly from the ADTRAN Support Community website.

Go to: <https://supportforums.adtran.com/welcome>

Registration is required.

Table 2. Related Online Documents and Resources

Title	Part Number	Description
Total Access 5000 Series System Deployment Guides		
Total Access 5000 Series Common Modules Basic Configuration Guide	65K97CMN-29	Provides the minimum configuration steps needed to provision the Common Modules for all Total Access 5000 Series platforms. Use this guide to perform initial provisioning of System Controller Modules (SCMs), Switch Modules (SMs), and Management and Switch Modules (MSMs).
Total Access 5000 Series System Guides		
Total Access 5000/5006 Chassis Installation Guide	65KCHASSIS-5	Provides a comprehensive description of and installation instructions for Total Access 5000/5006 Chassis and associated components. Use this information to install a new Chassis, to make SMIO3 alarm, clock, and test bus connections, and to install modules in the Chassis.
Total Access 5004 Chassis Installation Guide	65K4CHASSIS-5	Provides a comprehensive description of and installation instructions for Total Access 5004 Chassis and associated components. Use this information to install a new Total Access 5004 Chassis and to install Common modules in the Chassis.
Total Access 5000/5006 Engineering Guide	65K100ENG-7	Provides engineering specifications for the Total Access 5000/5006 Chassis and components, including Line, Access, and Fan Modules. Use this information during network planning, when ordering new or replacement components, and for an overall understanding of the Total Access 5000/5006 product line.

Table 2. Related Online Documents and Resources (Continued)

Title	Part Number	Description
<i>Total Access 5004 Engineering Guide</i>	65K499ENG-7	Provides engineering specifications for the Total Access 5004 Chassis and components, including Line, Access, and Fan Modules. Use this information during network planning, when ordering new or replacement components, and for an overall understanding of the Total Access 5004 product line.
<i>Total Access 5000 Series CLI Dictionary</i>	65K103CLI-35	Provides Command Line Interface (CLI) commands for the ADTRAN Total Access 5000 Series products. This guide gives detailed descriptions of the commands, descriptions of the syntax, and usage examples for each supported product. Use this guide in conjunction with the applicable system deployment guide when using CLI to deploy your application.
<i>Total Acc4ess 5000 IO Modules and compatibility Matrix</i>	N/A	Provides information pertaining to the Total Access 5000 Series I/O modules and rear/front blank panels. Use the comparison matrix in this guide to match the correct I/O Module to the available Total Access 5000 Series Access and Line Modules. To access the matrix, go to http://www.adtran.com
<i>ADTRAN Pluggable Optics Compatibility Matrix</i>	N/A	Provides an online tool that enables selective filtering to identify the ADTRAN approved optical modules that are applicable for a specific application. To access the matrix, go to: http://www.adtran.com/sfp
<i>Total Access 5000 Series Load Calculation Guidelines</i>	N/A	Provides maximum current draw and heat dissipation specifications for all Total Access 5000 Series Chassis and modules and Optical Network Edge (ONE) modules. Use this information to determine the number of modules that can be safely installed in the Chassis to ensure that the Chassis is not overloaded. To o access the matrix, go to: http://www.adtran.com
<i>Total Access 5000 Switch Module Application Guide</i>	65KSMAPP-49	Provides information on provisioning the Total Access 5000 Switch Module for Link Aggregation, Y-Cable Redundancy or RADIUS.
<i>Total Access 5000 GPON User Interface Guide</i>	65K110GPON-31	Describes and defines the ADTRAN user interface for the GPON Optical Line Termination. Use this guide as a reference when provisioning with the Web.

Table 2. Related Online Documents and Resources (Continued)

Title	Part Number	Description
<i>Total Access 5000 Active Ethernet User Interface Guide</i>	65K83AE-31	Describes and defines the ADTRAN user interface for the Active Ethernet Access Module. Use this guide in conjunction with the applicable system deployment guide when using Web to deploy your application.

1 Fiber to the Premises Overview

1.1 Scope

This section provides an overview of provisioning FTTP to a customer's premises.

1.2 In this Section

This section contains the topics listed in [Table 1-1](#).

Table 1-1. Section 1 Topics

Sub-Section	Topic	See Page ...
1.3	GPON Overview	28
1.4	Fiber to the Premises with Active Ethernet Overview	33
1.5	Voice Overview	37
1.6	Command Line Interface Overview	42
1.7	User Interface	47

1.3 GPON Overview

Gigabit Passive Optical Network (GPON) technology provides a consistent and common approach to advancing the public communications network using:

- Traditional telephone services [Plain Old Telephone Service (POTS)]
- High speed data services
- Video services (CATV overlay or video over IP).

The GPON network consists of an Optical Line Terminal (OLT) located at the central office and the Optical Network Terminal (ONT) located at the customer's premises. Between them lies the Optical Distribution Network (ODN) comprised of fibers and passive splitters or couplers. A splitter is a device that divides an optical signal into two or more signals, each carrying a selected frequency range. It can also reassemble signals from multiple signal sources into one signal.

The GPON technology is based on Passive Optical Network (PON) technology. Traditionally, telecommunication networks use devices that require power to transmit data from one point to another including processors, memory chips, repeaters, and relays. With passive optical networks, components that need power to transmit data between the central office and the customer premises are replaced by passive components that guide traffic based on splitting optical wavelengths to end points along the way. These passive components, such as splitters and coupler devices, work by passing or restricting light and do not require power to transmit data.

In a PON, a single piece of fiber can be run from the serving exchange out to a subdivision or office park. Then, individual fiber strands can be run to each building. Also, serving equipment can be split from the main fiber using passive splitters or couplers. This allows one piece of fiber cable from the exchange to the customer to be shared by many customers, thereby dramatically lowering the overall costs of deployment for Fiber To The Premises (FTTP) applications.

GPON offers the following features:

- Consistent Operations, Administration, and Maintenance (OAM)
- Traffic management and flow-through provisioning
- Resiliency through dynamic circuit removal and restoration
- Electrical and Optical Ethernet connections to the customer

[Figure 1-1](#) on page 29 is an example of a GPON application.

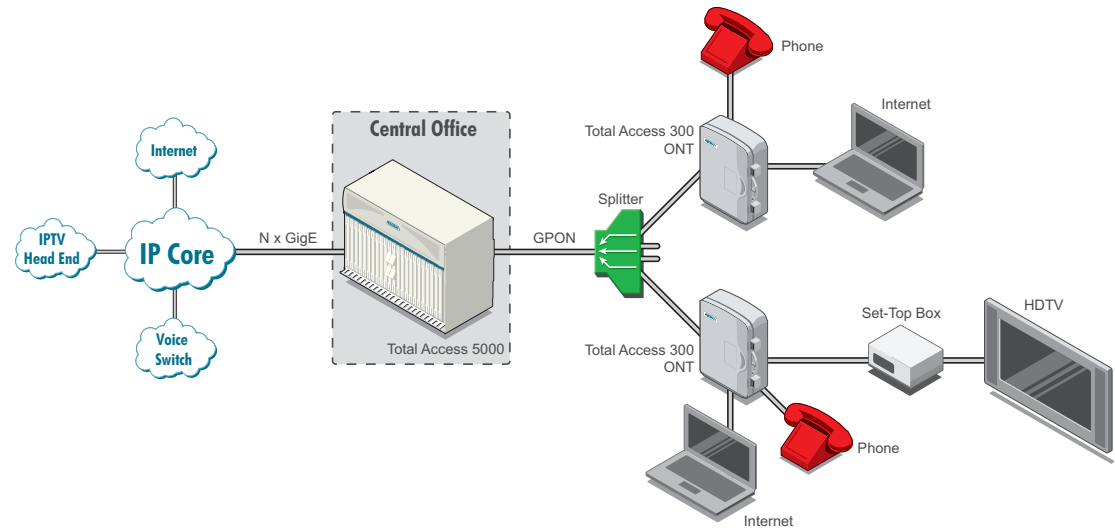


Figure 1-1. Total Access 5000 GPON General Application Diagram

1.3.1 Customer VLAN (C-VLAN) Model

Figure 1-2 displays a Total Access 5000 with a 1:1 Customer VLAN(C-VLAN) model. The C-VLAN model creates a VLAN for each subscriber. All services (Data, Video, etc.) provided to the customer are carried on the same VLAN. The number of VLANs required is equal to the number of subscribers serviced.

An advantage of the C-VLAN model is security. Each subscriber is isolated from other subscribers on separate VLANs. Another advantage is the similarity to older ATM based configurations. The main disadvantage of the C-VLAN model is the lack of multicast replication. A separate copy of each multicast stream must be sent to the Total Access 5000 for each user requesting it. These copies inefficiently use uplink bandwidth, thus limiting the size of the subscriber base for each Total Access 5000.

Figure 1-2 illustrates a 1:1 Customer VLAN model inside a Total Access 5000. When provisioning a C-VLAN each VLAN requires an EVC and an EVC Map to connect the EVC to the correct UNI port.

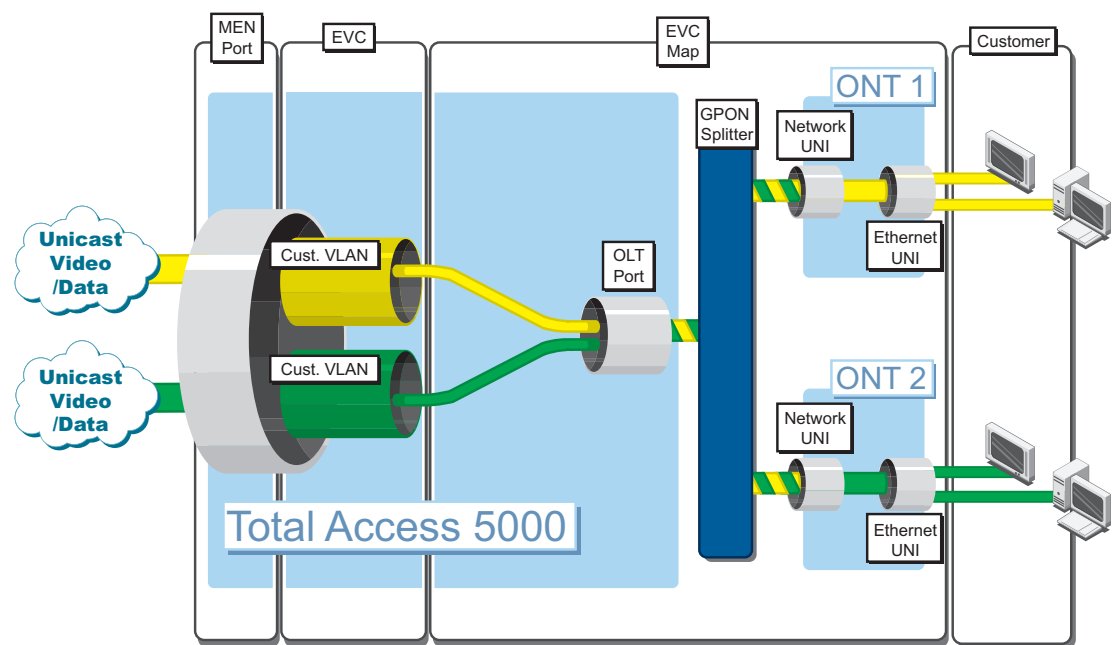


Figure 1-2. 1:1 Customer VLAN Diagram

1.3.2 N:1 Service VLAN (S-VLAN) Model

Figure 1-3 displays a Total Access 5000 with a N:1 Service VLAN model. The N:1 Service VLAN model creates one VLAN for each provided service (Data, Video, etc.). This service VLAN is shared by multiple (N) subscribers.

The N:1 Service VLAN model allows for the replication of multicast traffic to multiple users. This replication makes more efficient use of uplink bandwidth. The N:1 Service VLAN model may also have advantages when adding video to an existing network, as the addition of a video VLAN will not disrupt the existing data VLAN. A disadvantage of this model is that the Total Access 5000 must provide additional security as the subscribers are not on isolated VLANs.

Figure 1-3 illustrates a N:1 Service VLAN model inside a Total Access 5000. When provisioning a S-VLAN each VLAN requires an EVC and an EVC Map to connect the EVC to the required UNI port. Therefore each UNI port will have one EVC Map for each service passing through it.

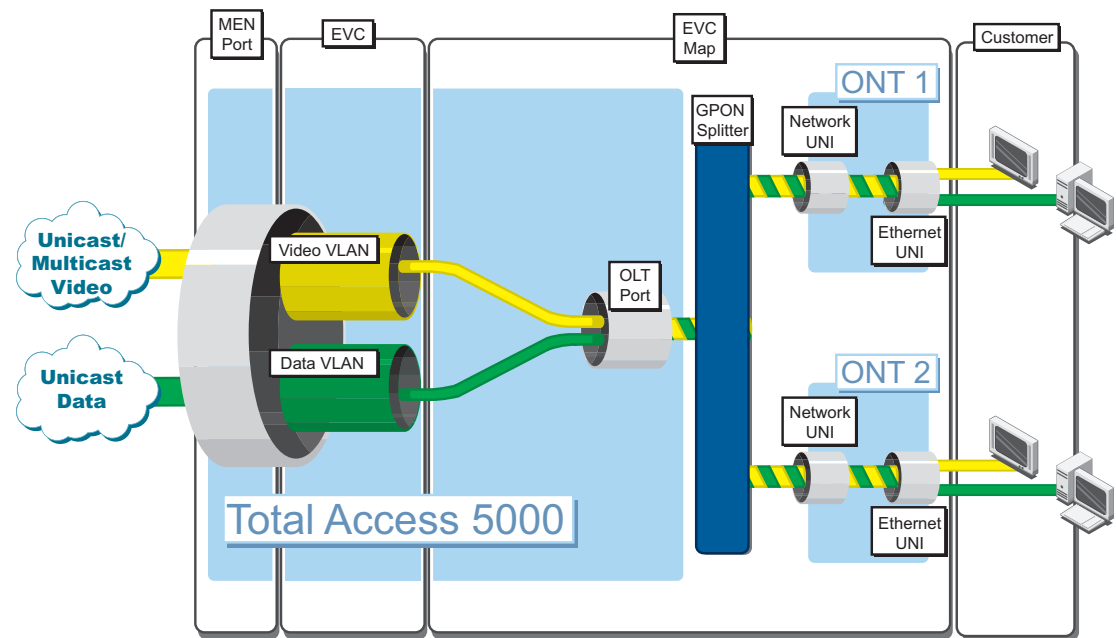


Figure 1-3. N:1 Service VLAN Diagram

1.3.3 Hybrid N+1:1 Combined VLAN Model

The following configuration examples provision a Total Access 5000 with a Hybrid N+1:1 VLAN (Combined VLAN) model. The Combined VLAN model creates a VLAN for each subscriber that handles data and unicast video traffic. A separate shared VLAN is created for multicast video and IGMP traffic, this allows for multicast replication. The number of VLANs required is equal to the number of subscribers serviced plus one, (N+1:1).

This model provides all of the advantages of the C-VLAN, (i.e. security, simplified operations, etc.) while removing its biggest disadvantage, no multicast replication.

Figure 1-4 illustrates a Hybrid N+1:1 VLAN model inside a Total Access 5000. When provisioning a Combined VLAN each VLAN requires an EVC and an EVC Map to connect the EVC to the each required UNI port. Therefore each UNI port will have one EVC Map for Unicast and Data and another for Multicast.

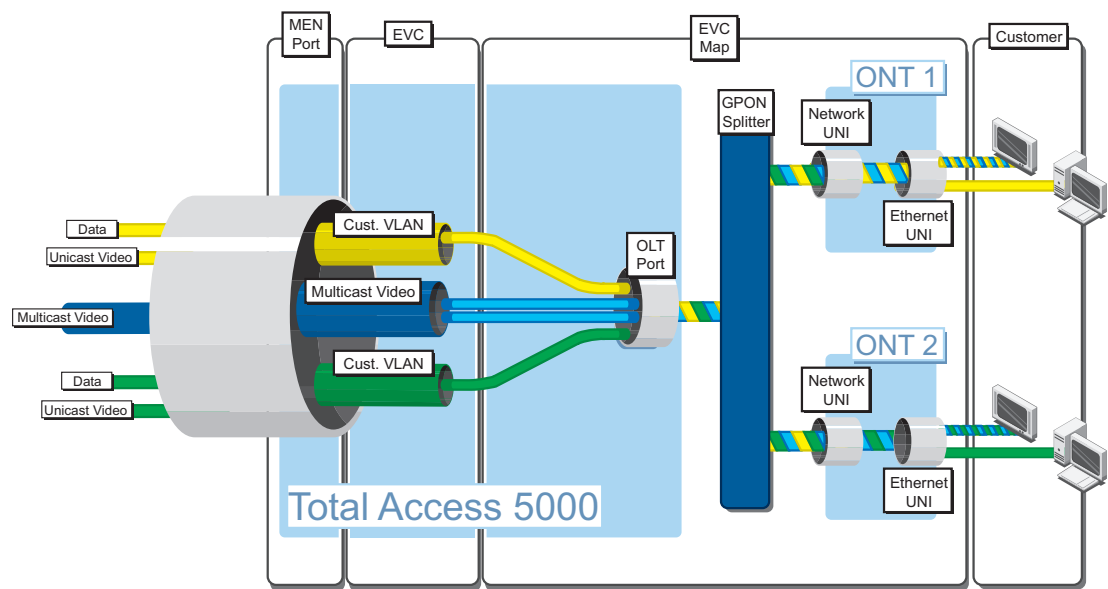


Figure 1-4. Hybrid N+1:1 Combined VLAN Diagram

1.4 Fiber to the Premises with Active Ethernet Overview

The increasing popularity of bandwidth intensive applications has driven the demand for fiber access. Two of the most popular standards-based deployment options for fiber media from the central office (CO) to the customer premises are Passive Optical Networks (PONs) and Active Ethernet networks. Since the Active Ethernet deployment method uses standard Ethernet frames, no transition protocol is required. This technology provides a consistent and common approach to providing triple play services using the public communications network for:

- Traditional telephone services [Plain Old Telephone Service (POTS)]
- High speed data services
- Video services

The optical network consists of an Optical Line Terminal (OLT) located at the central office and Optical Network Terminals (ONTs) located at the customer premises. To allow for the transmission of downstream and upstream traffic on one single fiber, different wavelengths are used for each direction. Downstream traffic uses 1490 nm, while upstream traffic is carried on 1310 nm. The ONT employs a bi-directional SFP that is a complement to the bi-directional SFP used in the OLT.

Supported distances for bi-directional SFPs range from 10 km up to 80 km.

Figure 1-5 displays an Active Ethernet general application diagram.

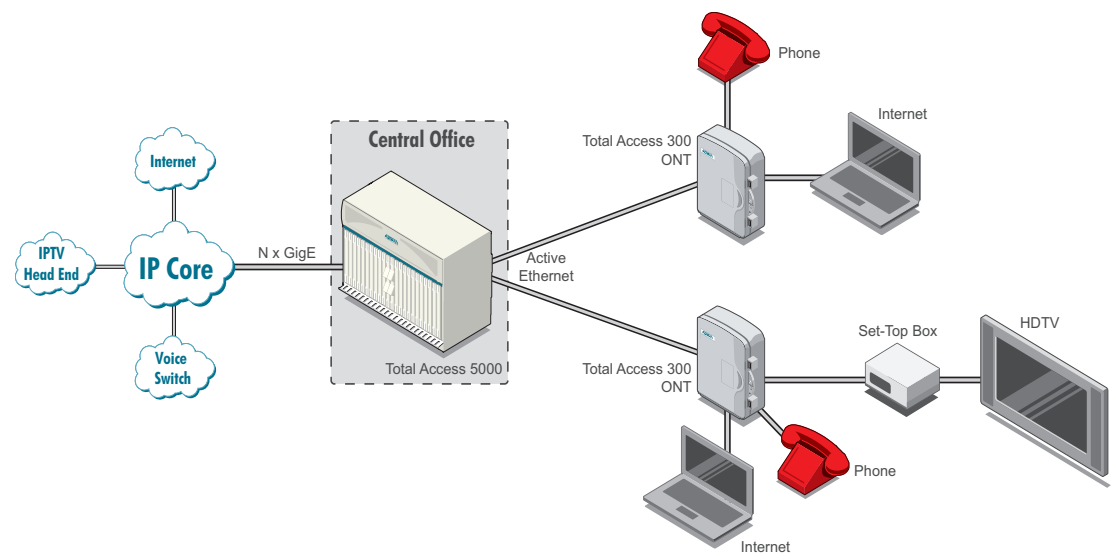


Figure 1-5. Total Access 5000 Active Ethernet General Application Diagram

1.4.1 Customer 1:1 VLAN (C-VLAN) Model

The following configuration examples provision a Total Access 5000 with a Customer 1:1 VLAN (C-VLAN) model. The C-VLAN model creates a VLAN for each subscriber. All services (Data, Video, etc.) provided to the customer are carried on the same VLAN. The number of VLANs required is equal to the number of subscribers serviced.

An advantage of the C-VLAN model is security. Each subscriber is isolated from other subscribers on separate VLANs. Another advantage is the similarity to older ATM based configurations. The main disadvantage of the C-VLAN model is the lack of multicast replication. A separate copy of each multicast stream must be sent to the Total Access 5000 for each user requesting it. These copies inefficiently use uplink bandwidth, thus limiting the size of the subscriber base for each Total Access 5000.

Figure 1-6 illustrates a 1:1 Customer VLAN model inside a Total Access 5000. When provisioning a C-VLAN each VLAN requires an EVC and an EVC Map to connect the EVC to the correct UNI port.

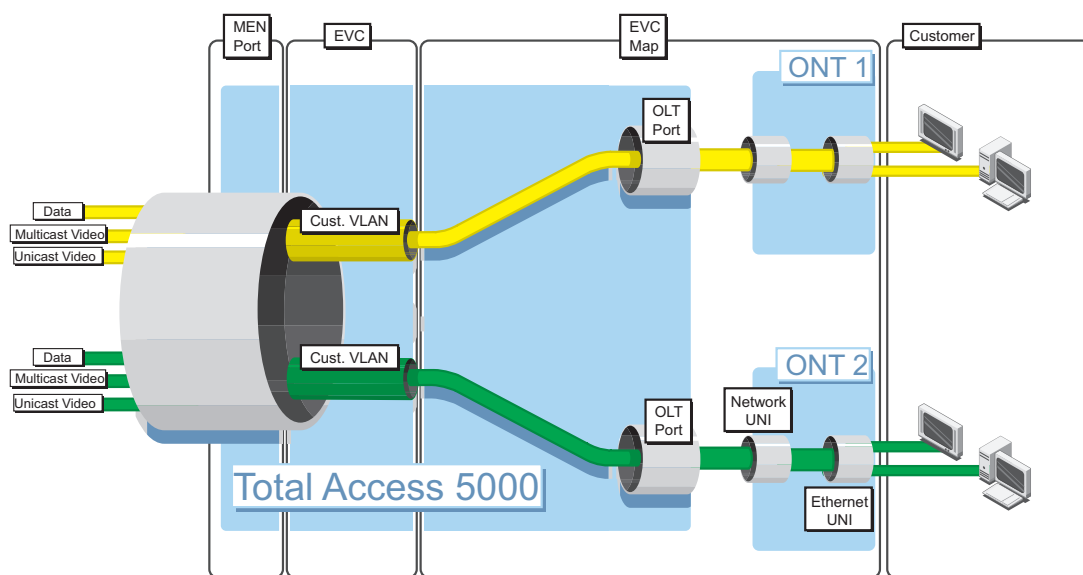


Figure 1-6. Customer 1:1 VLAN Diagram

1.4.2 N:1 Service VLANs Model

The following configuration examples provision a Total Access 5000 with a N:1 Service VLAN model. The N:1 Service VLAN model creates one VLAN for each provided service (Data, Video, etc.). This service VLAN is shared by multiple (N) subscribers.

The N:1 Service VLAN model allows for the replication of multicast traffic to multiple users. This replication makes more efficient use of uplink bandwidth. The N:1 Service VLAN model may also have advantages when adding video to an existing network, as the addition of a video VLAN will not disrupt the existing data VLAN. A disadvantage of this model is that the GigaBit Multi-Service Edge Switch must provide additional security as the subscribers are not on isolated VLANs.

Figure 1-7 illustrates a N:1 Service VLAN model inside a Total Access 5000. When provisioning a S-VLAN each VLAN requires an EVC and an EVC Map to connect the EVC to the each required UNI port. Therefore each UNI port will have one EVC Map for each service passing through it.

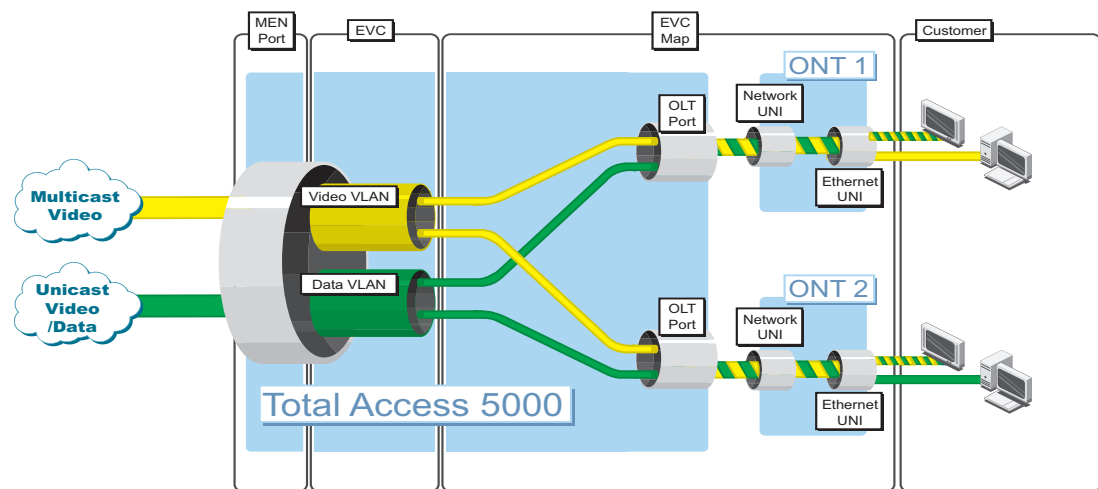


Figure 1-7. N:1 Service VLAN Diagram

1.4.3 Hybrid N+1:1 Combined VLAN Model

The following configuration examples provision a Total Access 5000 with a Hybrid N+1:1 VLAN (Combined VLAN) model. The Combined VLAN model creates a VLAN for each subscriber that handles data and unicast video traffic. A separate shared VLAN is created for multicast video and IGMP traffic, this allows for multicast replication. The number of VLANs required is equal to the number of subscribers serviced plus one, (N+1:1).

This model provides all of the advantages of the C-VLAN, (i.e. security, simplified operations, etc.) while removing its biggest disadvantage, no multicast replication.

Figure 1-8 illustrates a Hybrid N+1:1 VLAN model inside a Total Access 5000. When provisioning a Combined VLAN each VLAN requires an EVC and an EVC Map to connect the EVC to the each required UNI port. Therefore each UNI port will have one EVC Map for Unicast and Data and another for Multicast.

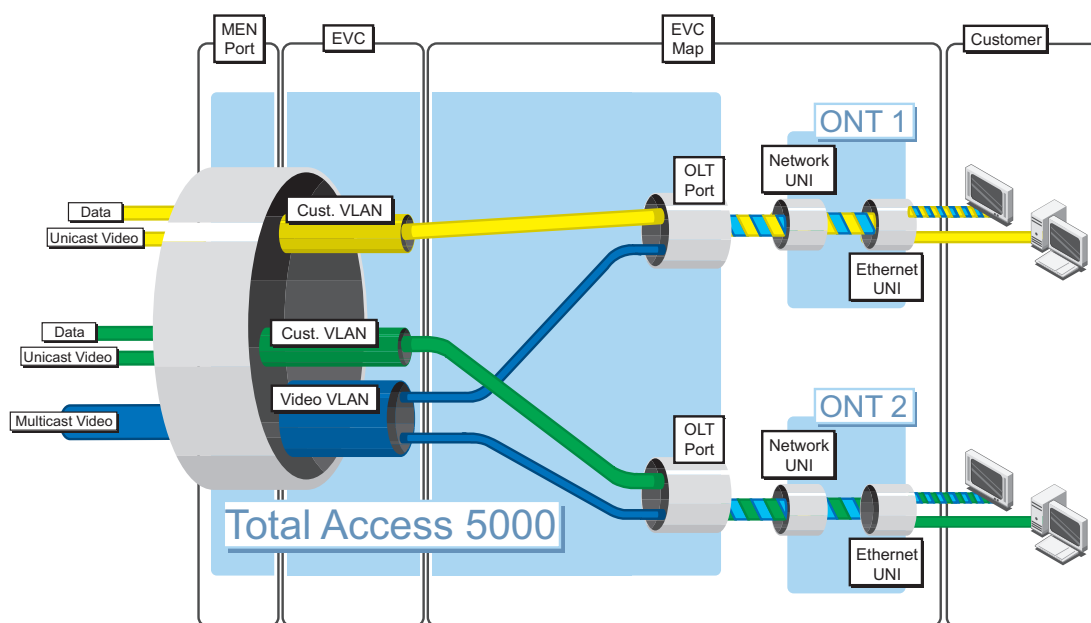


Figure 1-8. Hybrid N+1:1 Combined VLAN Diagram

1.5 Voice Overview

The Total Access 5000 Series allows you to choose from several different delivery options from traditional Generic Requirement 303 (GR-303) to VoIP options such as Session Initiation Protocol (SIP) or Media Gateway Control Protocol (MGCP).

1.5.1 GR-303 Description

GR-303 is a Telcordia standard interface to a Class 5 telephone switch to a digital loop carrier (DLC). This is the primary interface to the telco switch from the outside world. In order to connect directly to the PTSN, IP phones and IP telephony gateways must adhere to GR-303.

1.5.2 MGCP Description

Media Gateway Control Protocol (MGCP) is an IP telephony signaling protocol from the Internet Engineering Taskforce (IETF). MGCP requires the use of softswitches for call control and resembles the telephony model of the circuit-switched PTSN more than SIP. The softswitch is aware of the entire call throughout its duration and enables operator intervention like the PTSN.

MGCP works between a call agent or ONT MGCP Endpoint controller, usually a software switch, and a ONT MGCP Endpoint with internal endpoints. The call agents create and manage media sessions with endpoints of physical or virtual data sources through the ONT MGCP Endpoint. The ONT MGCP Endpoint is the network device that converts voice signals carried by telephone lines into data packets carried over the Internet or other packet networks. In this network structure, the FTTP ONT product functions as an ONT MGCP Endpoint.

ONT MGCP Endpoints communicate with analog endpoints (telephones and fax through foreign exchange station (FXS) interfaces) in a manner configured by the call agent. MGCP is the protocol used for communication between the call agent and the ONT MGCP Endpoint. In network structures that include multiple call agents and ONT MGCP Endpoints, call agents communicate with other call agents using SIP and ONT MGCP Endpoints communicate with other ONT MGCP Endpoints using Realtime Transport Protocol (RTP) or Realtime Control Protocol (RTCP). See [Figure 1-9](#) for an illustration of how MGCP functions in the network.

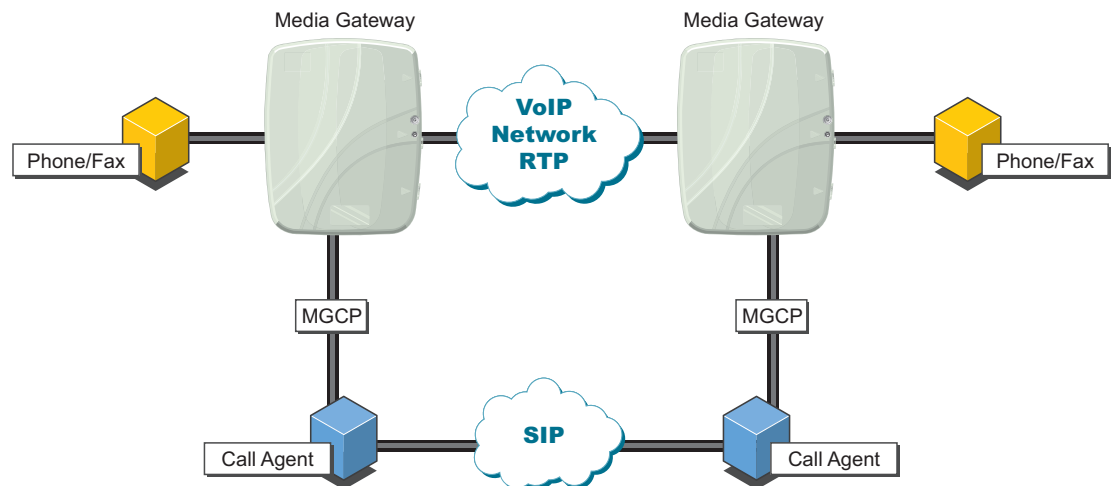


Figure 1-9. MGCP Network

1.5.2.1 Call Agent and Endpoint Communication

ONT MGCP Endpoints use MGCP to communicate with call agents, which use SIP to communicate with other call agents. ONT MGCP Endpoints communicate with other ONT MGCP Endpoints via RTP over the VoIP network, thus creating a VoIP call from analog sources. Signals from the ONT MGCP Endpoint are transmitted to the call agent directly from a specified FXS port. Each port is named in order to synchronize the signals. Every MGCP command includes a transaction ID, acknowledgment, and a response. See [Figure 1-10](#) for a description of how ONT MGCP Endpoints communicate with call agents (via MGCP).

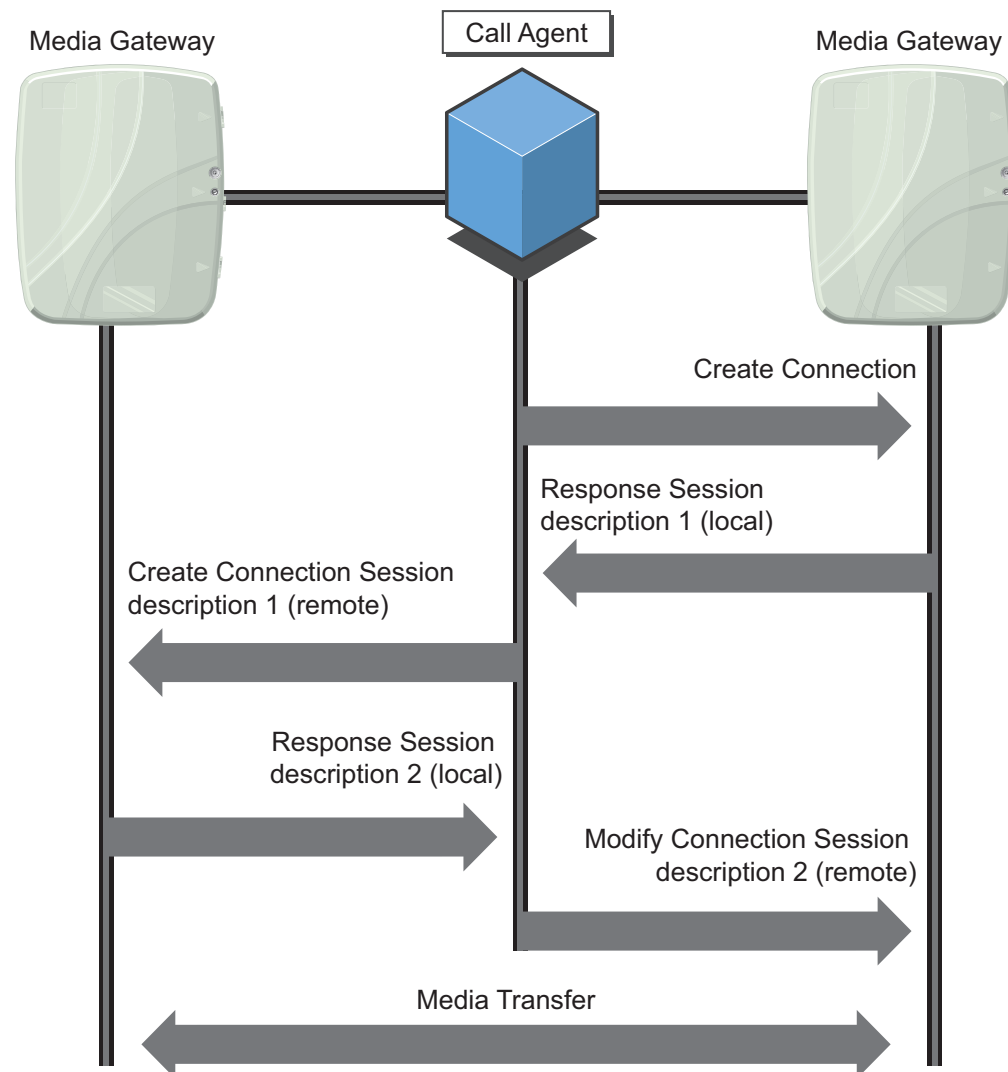


Figure 1-10. ONT MGCP Endpoints

1.5.2.2 Standards

There are two MGCP standards. The latest version, MGCP 1.0bis, is derived from RFC 3435. The older version, MGCP 0.1/NCS 1.0, is based on a PacketCable™ derivative. Different call agents can use different MGCP standards, so it is important to configure gateways and call agents to use the same standards.

1.5.3 SIP Description

SIP is an IP telephony signaling protocol that is widely used to start and terminate voice calls over the Internet. Supporting two-way and multi-party calls, SIP can be used for any real-time media transmission over an IP network, including video calling and conferencing.

SIP, the IETF protocol for VoIP (Voice over Internet Protocol), is defined in RFC 3261. SIP makes use of network entities called SIP proxies (external to the Total Access 5000 system) to help route requests to the user's current location, authenticate and authorize users for services, implement provider call-routing policies, and provide features to users. SIP messages carry session descriptions that allow participants to agree on a set of compatible media types.

SIP voice user provisioning is done in two parts. All profiles (media, codec-list, call-feature, sip-trunk and dialing) are centrally provisioned and can be shared across multiple voice users. SIP users are provisioned on the access modules and centrally provisioned profiles are connected to these users on need basis.

Most of the profiles or various attributes in a profile are optional and have default value associated with them. There are only few attributes that are mandatory to bring up sip voice user. Sip-trunk is considered as a mandatory profile and proxy & registrar primary ip address attributes must be configured and attached to a voice user. Similarly connection to fxs port, sip-identity, auth name and sip-trunk are mandatory parameters for SIP voice user to be ready for activation.

The SIP voice user is expected to go running once it has all mandatory and non-conflicting parameters. There is a time lag (~10 sec) between change in configuration in the centrally provisioned profiles and the ONT getting the updated configuration.

1.5.3.1 Benefits

Service provider customers deploy VoIP technologies in general to reduce capital and operational expenses. Key aspects of benefits include the following:

- Reduced equipment, maintenance and support costs by capping or replacing legacy Class 5 and Class 4 switch networks.
- Reduced transport costs for long-distance and international traffic through use of compressed voice on packet data networks.
- Elimination of TDM networks for the local Public Telephone Service Network (PTSN) and convergence on all-packet networks for access and edge infrastructure.
- Reduction of operations personnel breadth and level of expertise by reducing or eliminating TDM switching specialties.
- Enhanced feature flexibility and expedited feature availability through deployment of SIP call-routing and media-server feature creation.

The SIP gateway functionality can take the place of an integrated GR-303 interface but with slightly lower cost points. However, the network host for the SIP gateway will now be a soft-switch instead of a class 5 switch as typically used for GR-303.

1.5.3.2 Terminating Multimedia Communications (Five SIP Facets)

For establishing and terminating multimedia communications, SIP supports the five facets listed in [Table 1-2](#).

Table 1-2. Five Facets of SIP

Facet	Description
User location	The user location determines the end system used for communication.
User availability	The user availability determines the willingness of the called party to engage in communication.
User capability	The user capability determines the form of media and media parameters used for communication.
Session setup	The session setup establishes the session parameters for the caller and calling party.
Session management	The session management manages the transfer and termination of services, modifies the session parameters, and invokes services.

1.5.3.3 SIP Pre-Installation Requirements

Ensure the following items are complete before deploying SIP:

- Select, install, and configure one or more SIP proxies on the data network.

A softswitch is a high-performance network server or cluster capable of supporting thousands (or even hundreds of thousands) of customer calls and provides SIP proxy functionality. Most dedicate a part of their internal network to voice traffic, either physically (via dedicated network resources) or logically (using virtual LANs) in order to provide the low-latency, low-loss transport environment that IP voice requires.

- Configure existing (or new, or expanded) data network routers and switches to transport VoIP traffic throughout their network, from the access network, across edge networks to their server core, and via transport networks to peer IP networks or other PSTN edge gateways.
- Select and install PSTN gateways to convert packet-voice to/from TDM-voice to enable interworking between legacy segments of their network and new VoIP segments.

Often a customer will have already deployed VoIP for long-distance transport, and will have replaced their Class 4 network (tandem switches) with softswitch technology before transitioning their access network. The result is an expanding VoIP core with various gateways around the edge connecting to the traditional PSTN. Eventually the VoIP domain grows large enough to overtake the PSTN and the perspective effectively reverses.

- Select and install additional VoIP equipment such as media gateways (for voice mail, announcements, conferencing, IVR services, etc.) and session border controllers (to provide security with peer VoIP networks, cellular networks, etc.).

- Integrate the above components with existing or new OSSs, and define the set of voice services that can be supported.

In general, the service creation environment and the integration environment are more flexible than for the traditional PSTN, but the integration effort can still be significant. For many customers the transition to IP-based service delivery is sufficient reason to replace some existing service provisioning systems, though many maintain existing systems for network transport and circuit maintenance.

Once the basic VoIP infrastructure is in place, the customer must install and configure the access network hardware to provide a VoIP interface for the customers.

1.6 Command Line Interface Overview

This section details the following information:

- Command Modes
- CLI Shortcuts
- CLI Error Messages
- CLI Input Descriptions

1.6.1 Command Modes

The NetVanta CLI has the following three command modes:

- Basic
- Application
- Enable

Each mode supports a specific set of commands. For example, all interface configuration commands are accessible only through the Enable mode.

[Table 1-3](#) shows a brief description of each command mode.

Table 1-3. Command Modes

Mode	Access by...	Prompt	Use this mode to...
Basic	Beginning a session	>	■ Display system information ■ Show status or statistics
Enable	Entering Enable mode while in the Basic mode as follows: > enable	#	■ Manage running configurations ■ Enter configuration modes ■ View security settings
Application	Performing a common function with a reduced set of commands	#	■ Copy system provisioning ■ Execute standard test procedures

1.6.2 CLI Shortcuts

Use the CLI shortcuts to help configure the product. [Table 1-4](#) provides a list of CLI shortcuts.

Table 1-4. CLI Shortcuts

Shortcut	Description
Up arrow or CTRL + P	Use the up arrow to re-display a previously entered command. The up arrow can cycle through all commands entered starting with the most recent command.
TAB	After entering a partial, but unique, command, press the TAB to complete the command. The command displays on the command prompt and waits for input.
?	Use the ? for any of the following: ■ Display a list of all subcommands in the current mode. ■ Display a list of available commands beginning with certain letter(s). ■ Obtain syntax help for a specific command by entering the command, a space, and then a question mark (?). The CLI displays the range of values and a brief description of the next parameter expected for that particular command.
CTRL + A	Use CTRL + A to jump to the beginning of the displayed command line.
CTRL + E	Use CTRL + E to jump to the end of the displayed command line.
CTRL + U	Use CTRL + U to clear the current displayed command line.
Auto finish	Enter enough letters to identify a command as unique. For example, entering int eth 1 at the Global Configuration prompt provides access to the configuration parameters for the specified Ethernet interface.

1.6.3 CLI Error Messages

Table 1-5 lists and defines some of the more common error messages given in the CLI.

Table 1-5. Error Messages

Message	Helpful Hints
%Ambiguous command	This message occurs when multiple commands can be derived from the input. Try using the "?" command to determine the error. Refer to Section 1.6.2, "CLI Shortcuts" on page 43 for more information.
%Unrecognized command	This message occurs when a single command is entered that fails to match any supported commands. Try using the "?" command to determine the error. Refer to Section 1.6.2, "CLI Shortcuts" on page 43 for more information.
%Invalid or incomplete command	This message occurs when the command is not properly finished. Try using the "?" command to determine the error. Refer to Section 1.6.2, "CLI Shortcuts" on page 43 for more information.
%Invalid input detected at "^" marker	The error in command entry is located where the caret (^) mark appears. Enter a question mark at the prompt. The system displays a list of applicable commands or gives syntax information for the entry.

1.6.4 CLI Input Descriptions

Table 1-6 lists and defines the inputs used throughout the CLI.

Table 1-6. Input Descriptions

Input Syntax	Input Example	Description
<x-y>	-2-4000	Use this input to enter a range by entering the x and y variables. The x and y variables are numeric and can be negative.
<x-n>	1-n	Use this input to enter an infinite range by entering the x variable. The x variable is numeric and can be negative.
<x>	0	Use this input to enter a single number.
<x,y-z,a>	-1,4-10,20-22	Use this input to enter a comma delimited numeric list without spaces. This input can include ranges.
<HH:MM:SS>	12:30:01	Use this input to enter the time in hour-minute-second format.
<HH:MM>	12:30	Use this input to enter the time in hour-minute format.
MONTH	MAR	Use this input to enter the month. Use the full month name or the 3-letter abbreviation. This input is not case sensitive.
HHH	010	Use this input to enter a numeric hex. The number of "H"s designates the number of hex digits allowed.
WORD	MAP_1	Use this input to enter a string without spaces. This input is case sensitive.
LINE	MAP 2	Use this input to enter a string allowing spaces. This input is case sensitive.
LIST	1,3-7,9,10	Use this input to enter a comma delimited numeric list without spaces. This input can include ranges.
<character>	A	Use this input to enter any single alpha character.
A.B.C.D		Use this input to enter an IP address.
xx:xx:xx:xx:xx:xx		Use this input to enter a MAC address.
<shelf/slot/port>	1/1/1	Use this input to enter the shelf, slot, and port.
<shelf/slot/port:channel>	1/1/1:1	Use this input to enter the shelf, slot, port and channel.
<shelf/slot/WORD>	1/1/MAP	Use this input to enter the shelf, slot, and WORD.
<shelf/slot>	1/S	Use this input to enter the shelf and slot.
<shelf/WORD>	1/DEFAULT	Use this input to enter the shelf and WORD.
<shelf>	1	Use this input to enter the shelf number. Only shelf 1 is supported.

Table 1-6. Input Descriptions (Continued)

Input Syntax	Input Example	Description
<slot/port>	1/1	Use this input to enter the slot and port.
<slot>	1	Use this input to enter the slot. Valid inputs are 0 - 22 for module slots, A for SM A, B for SM B, S for the SCU, and F for the fan module.
<port>	1	Use this input to enter the port number.

1.6.5 CLI Login

Access the management and provisioning features for the NetVanta products by CLI using a standard DB-9 serial cable to connect to the console port located on the unit. Also, access the CLI through Telnet.

To establish CLI communication with the product, perform the following steps:

1. Connect to the craft interface using a VT100 terminal or PC with VT100 emulation software configured with the following parameters:
 - Any of the following baud rates: 9600, 19200, 38400, 57600, or 115200
 - 8 data bits
 - No parity
 - 1 stop bit
 - No flow control
2. Once connected, press ENTER several times to access the CLI.

1.7 User Interface

The NetVanta User Interface requires a web browser. Complete the following steps to log in to the system.

To access the Web GUI, complete the following steps:

1. Enter the NetVanta IP Address in the Address Bar of the web browser, and then press ENTER.

The NetVanta Logon screen appears, as illustrated in [Figure 1-11](#).



Figure 1-11. Total Access 5000 Logon Screen

**NOTE**

Because this document supports both the Total Access 5000 and 5006 systems, the screen headings may display Total Access 5000 or Total Access 5006 depending on the system in use.

2. In the **Username:** field, enter the username.
3. In the **Password:** field, enter the password.

**NOTE**

The default username and password for the system are ADMIN and PASSWORD. The username and password fields are case sensitive.

4. Click **Login** or press ENTER.

If the username and password are valid, the User Statistics dialog box appears as illustrated in [Figure 1-12](#).



Figure 1-12. User Statistics Dialog Box

5. Click **OK** to continue.
6. The NetVanta **User Interface** appears starting with the System Status Screen.

2 GPON Provisioning using CLI

2.1 Scope of this Section

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



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.

2.2 In this Section

This section contains the topics listed in [Table 2-1](#).

Table 2-1. Section 1 Topics

Sub-Section	Topic	See Page ...
2.3	Provisioning	50

2.3 Provisioning

Provisioning is a two-step process.

First, the OLT/PON needs to be provisioned. Then the Service State for each needs to be assigned. Complete the following when deploying an FTTP application using the CLI.

- [“OLT/PON Provisioning”](#) below
- [“Service Provisioning”](#) on page 62

2.3.1 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 services.

2.3.1.1 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>`

2.3.1.2 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 [“Hazard and Advisory Symbols”](#) on page 23.

1. Access the GPON interface.
`ChassisID(config)#interface gpon <shelf/slot/port>`
2. Set the activation mode.
Refer to [Table 2-2](#) on page 51 for a list of the Activation Modes.



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 [Table 2-2](#) on page 51.



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.

Table 2-2. Activation Mode

Activation Mode	Command
Auto Activate	ChassisID(config-gpon x/x/x)# activation-mode auto-activate
Auto Discover	ChassisID(config-gpon x/x/x)# activation-mode auto-discover
Manual	ChassisID(config-gpon x/x/x)# activation-mode manual
Registration	ChassisID(config-gpon x/x/x)# activation-mode registration [lock-serial-number unlock-serial-number]

**NOTE**

For the differences on Lock Serial Number and Unlock Serial Number, refer to [Section 13, “Activation Mode”](#) on page 391.

3. Select a range indication for the PON.

- **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).
ChassisID(config-gpon x/x/x)#**range [extended|maximum|standard]**
Refer to [Table 2-3](#) for range descriptions.

Table 2-3. Range Description

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

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

**NOTE**

This step requires an EVC to be configured that matches the provisioned S-tag. ADTRAN recommends the EVC be configured for MAC-Switched mode, instead of Tag-Switched mode.

ChassisID(config-gpon x/x/x)#**subtended-host <ont-id> s-tag <2-4094>**

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

ChassisID(config-gpon x/x/x)#**subtended-host <ont-id> s-tag-priority <0-7>**

6. Select the method of inband management.

Refer to [Table 2-4](#) on page 52 for the inband management options.

Table 2-4. Inband Management

Inband	Command	Description
Static IP	<code>ChassisID(config-gpon x/x/x)#subtended-host <ont-id> ip address a.b.c.d a.b.c.d</code>	Set the static IP address and subnet mask for the ONT's inband management. If selected, continue to step 7.
DHCP IP	<code>ChassisID(config-gpon x/x/x)#subtended-host <ont-id> ip address dhcp</code>	Allocate the IP address for the ONT's inband management dynamically using DHCP. If selected, continue to step 8.

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

`ChassisID(config-gpon x/x/x)#subtended-host <ont-id> ip default-gateway A.B.C.D`

8. Enable or disable Forward Error Correction (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. To disable, use the no form of this command.

`ChassisID(config-gpon x/x/x)#downstream fec enable`

- 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.

9. Enable or disable FEC for upstream traffic toward the OLT. To disable, use the no form of this command.

`ChassisID(config-gpon x/x/x)#upstream fec enable`

- The ONT may or may not support the capability to apply FEC encoding to the upstream data.
- Enabling upstream FEC adds more overhead on the PON channel due to the addition of parity bytes and reduces the total combined fixed and assured rates per PON by rough 6%.

10. Enable the interface.

`ChassisID(config-gpon x/x/x)#no shutdown`

11. If using DHCP address, view the DHCP address for a GPON subtended-host.

`ChassisID(config-gpon x/x/x)#do show interfaces gpon <shelf/slot/pont> subtended-host`



What's Next

- For Registration-ID activation, continue to [Section 2.3.1.3, "Enter the Registration-ID"](#) on page 53.
- For all other activation modes, continue to [Section 2.3.1.4, "Discover the ONT"](#) on page 61.

2.3.1.3 Enter the Registration-ID



CAUTION!

Do not duplicate the same Registration-ID to two different ONTs to be activated on the OLT. As an example, ONT A has S/N S1 and Registration-ID R1 and is UP; another ONT B, has S/N S2 and Registration-ID R2. ONT B becomes faulty and needs replacement. When the technician removes ONT B and adds a new ONT in place of B with a Registration-ID R1, ONT B would not come UP and cause a duplicate Registration-ID error at the OLT. If the technician did not resolve the duplicate Registration-ID and leave the ONT connected, ONT A would still be UP and running. After an OLT reboot, there is a chance that the ONT replaced at B would get the service of ONT A.

The registration-ID steps vary depending on your ONT. Use [Table 2-5](#) to navigate to your next step.

Table 2-5. Registration-ID

Registration-ID Procedure	See Page
Section 2.3.1.3.1, "Registration-ID Entry for Total Access 3xx"	53
Registration-ID Entry for Total Access 421x /Total Access 421xw	55
Registration-ID Entry for Total Access 3xx Residential Gateway	57
Registration-ID Entry for Total Access 324RG and 334RG	58
Registration-ID Entry for Total Access 324 3rd Generation and Total Access 374	59
Registration-ID Entry for Total Access 4xx	60

2.3.1.3.1 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 2-6](#).

Table 2-6. 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, lift up phone receiver and listen. 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 XXXXXXXXXXXX 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 2-7](#).

Table 2-7. 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 2-8](#).

Table 2-8. 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.
11. If error, return to Step 1.



What's Next

Continue to [Section 2.3.1.4, "Discover the ONT"](#) on page 61.

2.3.1.3.2 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 house 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 **NTWK** on the ONT will be ON at the end of the process. Refer to [Table 2-9](#) on page 56 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 2-9](#) on page 56 for a list of LEDs.

2.3.1.3.3 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 2-9](#).

Table 2-9. 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 [Section 2.3.1.4, "Discover the ONT"](#) on page 61.

2.3.1.3.4 Registration-ID Entry for Total Access 3xx Residential Gateway

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 [Section 2.3.1.4, “Discover the ONT”](#) on page 61.

2.3.1.3.5 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 house 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 step 7.
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 [Section 2.3.1.4, "Discover the ONT"](#) on page 61.

2.3.1.3.6 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 disabled.



What's Next

Continue to [Section 2.3.1.4, "Discover the ONT"](#) on page 61.

2.3.1.3.7 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 2-1](#) 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 2-1](#)).

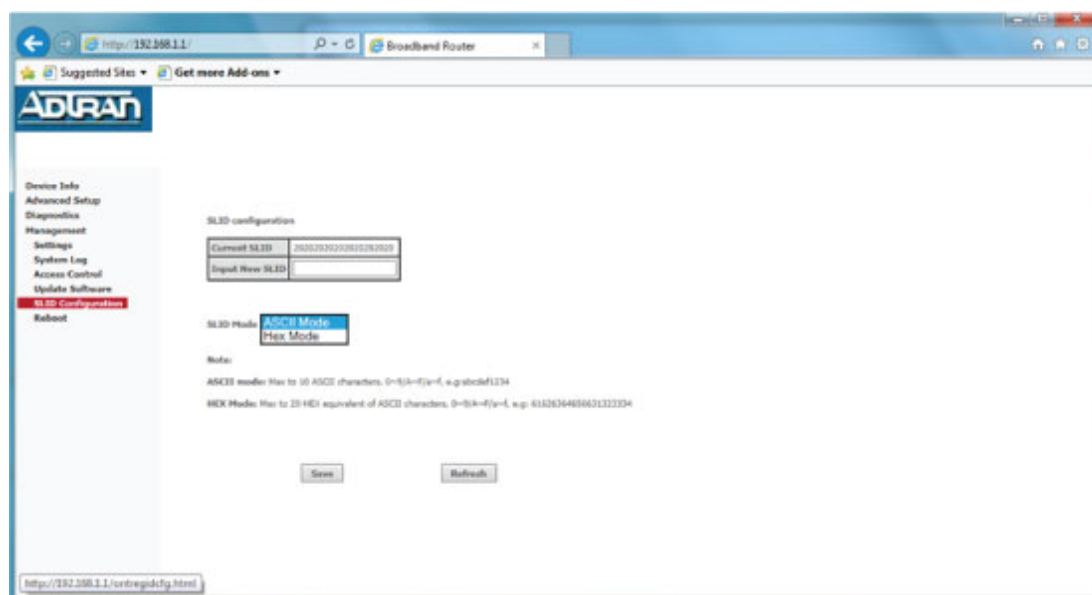


Figure 2-1. 401 Web GUI Display

6. Navigate to Management>SLID Configuration (see the menu tree in [Figure 2-1](#)).
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 [Section 2.3.1.4, “Discover the ONT”](#) on page 61.

2.3.1.4 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. Discover the ONT.

Refer to [Table 2-10](#) for the selected activation method.

Table 2-10. Discover the ONT

Activation Mode	Command
Manual or Auto-Discovery	<code>ChassisID(config-ont ont-id@x/x/x)#serial-number line</code> Substitute LINE with the ONT serial number. Example ADTN12345678.
Auto-Activate	N/A
Registration-ID Lock-SN or Registration-ID Unlock-SN	<code>ChassisID(config-ont ont-id@x/x/x)#registration-id <number 10></code> The Registration-ID requires a 10 digit number to match the Registration-ID programmed into the ONT by the installer. If using the NG-PON2 4x10/10GigE OLT (P/N 1187514F1), the Registration-ID can be more than 10 digits and may contain alphanumeric characters.

3. Enable the ONT interface.

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

4. Return to the Global Configuration Command Set.

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

2.3.2 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:

- [Section 2.3.2.1, "Voice"](#) below
- [Section 2.3.2.2, "Data"](#) on page 66
- [Section 2.3.2.3, "Video"](#) on page 66
- [Section 2.3.2.4, "RF-Video"](#) on page 66
- [Section 2.3.2.5, "Transport Layer Security \(TLS\)"](#) on page 66

2.3.2.1 Voice

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

2.3.2.1.1 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 multimedia 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.

2.3.2.1.2 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.

2.3.2.1.3 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.

2.3.2.1.4 Select Your Voice Option

Use [Table 2-11](#) to determine your voice option and navigate to your next step. If you're unsure of your voice option, refer to ["Voice"](#) on page 62.

Table 2-11. Voice Options

Option	See Page
SIP OMCI Voice	63
SIP Non-OMCI Voice	64
MGCP OMCI Voice	64
MGCP Non-OMCI Voice	65
GR-303 Voice	65

2.3.2.1.5 SIP OMCI Voice

To provision for SIP OMCI 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 ["Hazard and Advisory Symbols"](#) on page 23

1. [Section 2.3.3, "Create an EVC"](#) on page 68
2. [Section 2.3.4, "Set the Voice Service Mode on the ONT"](#) on page 73
3. [Section 2.3.5, "Provision the Port on the ONT"](#) on page 74
4. [Section 2.3.6, "Create an IP Host"](#) on page 82
5. [Section 2.3.7, "Create an EVC-Map"](#) on page 83
6. [Section 2.3.8, "Provision the SIP Trunk"](#) on page 93
7. [Section 2.3.11, "Provision the SIP Dialing Profile"](#) on page 98
8. [Section 2.3.18, "Provision the OMCI SIP Users"](#) on page 111

2.3.2.1.6 SIP Non-OMCI Voice

To provision for SIP OMCI 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 [“Hazard and Advisory Symbols”](#) on page 23.

1. [Section 2.3.3, “Create an EVC”](#) on page 68
2. [Section 2.3.4, “Set the Voice Service Mode on the ONT”](#) on page 73
3. [Section 2.3.5, “Provision the Port on the ONT”](#) on page 74
4. [Section 2.3.6, “Create an IP Host”](#) on page 82
5. [Section 2.3.7, “Create an EVC-Map”](#) on page 83
6. [Section 2.3.8, “Provision the SIP Trunk”](#) on page 93
7. [Section 2.3.11, “Provision the SIP Dialing Profile”](#) on page 98
8. [Section 2.3.12, “Provision Class of Service \(CoS\) \(Optional\)”](#) on page 104
9. [Section 2.3.13, “Provision for Global Voice \(Optional\)”](#) on page 105
10. [Section 2.3.14, “Provision the Voice User”](#) on page 106

2.3.2.1.7 MGCP OMCI Voice

To provision for SIP OMCI 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 [“Hazard and Advisory Symbols”](#) on page 23.

1. [Section 2.3.3, “Create an EVC”](#) on page 68
2. [Section 2.3.4, “Set the Voice Service Mode on the ONT”](#) on page 73
3. [Section 2.3.5, “Provision the Port on the ONT”](#) on page 74
4. [Section 2.3.6, “Create an IP Host”](#) on page 82
5. [Section 2.3.7, “Create an EVC-Map”](#) on page 83
6. [Section 2.3.9, “Provision the MGCP Profile”](#) on page 95
7. [Section 2.3.19, “Provision OMCI MGCP Endpoints”](#) on page 113

2.3.2.1.8 MGCP Non-OMCI Voice

To provision for SIP OMCI 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 [“Hazard and Advisory Symbols”](#) on page 23.

1. [Section 2.3.3, “Create an EVC”](#) on page 68
2. [Section 2.3.4, “Set the Voice Service Mode on the ONT”](#) on page 73
3. [Section 2.3.5, “Provision the Port on the ONT”](#) on page 74
4. [Section 2.3.6, “Create an IP Host”](#) on page 82
5. [Section 2.3.7, “Create an EVC-Map”](#) on page 83
6. [Section 2.3.9, “Provision the MGCP Profile”](#) on page 95
7. [Section 2.3.10, “Provision Non-OMCI MGCP Endpoints”](#) on page 96

2.3.2.1.9 GR-303 Voice

To provision for GR-303 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 [“Hazard and Advisory Symbols”](#) on page 23.

1. [Section 2.3.4, “Set the Voice Service Mode on the ONT”](#) on page 73
2. [Section 2.3.5, “Provision the Port on the ONT”](#) on page 74
3. [Section 2.3.20, “Provision GR-303”](#) on page 114

2.3.2.2 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 [“Hazard and Advisory Symbols”](#) on page 23.

1. [Section 2.3.3, “Create an EVC”](#) on page 68
2. [Section 2.3.5, “Provision the Port on the ONT”](#) on page 74
3. [Section 2.3.7, “Create an EVC-Map”](#) on page 83

2.3.2.3 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 [“Hazard and Advisory Symbols”](#) on page 23.

1. [Section 2.3.3, “Create an EVC”](#) on page 68
2. [Section 2.3.5, “Provision the Port on the ONT”](#) on page 74
3. [Section 2.3.7, “Create an EVC-Map”](#) on page 83

2.3.2.4 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 refer to the applicable documents listed in [“Hazard and Advisory Symbols”](#) on page 23.

1. [Section 2.3.5, “Provision the Port on the ONT”](#) on page 74

2.3.2.5 Transport Layer Security (TLS)

Transport Layer Security (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 2-12](#) for an available list of TLS options.

Table 2-12. 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

2.3.2.5.1 Select Your TLS Option

Use [Table 2-13](#) to determine your TLS option and navigate to your next step.

Table 2-13. Voice Options

Option	See Page
TLS Single Tag Configuration	67
TLS Double Tag Configuration	67

2.3.2.5.2 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 [“Hazard and Advisory Symbols”](#) on page 23.

1. [Section 2.3.3, “Create an EVC”](#) on page 68
2. [Section 2.3.5, “Provision the Port on the ONT”](#) on page 74
3. [Section 2.3.7, “Create an EVC-Map”](#) on page 83

2.3.2.5.3 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 [“Hazard and Advisory Symbols”](#) on page 23.

1. [Section 2.3.3, “Create an EVC”](#) on page 68
2. [Section 2.3.5, “Provision the Port on the ONT”](#) on page 74
3. [Section 2.3.7, “Create an EVC-Map”](#) on page 83

2.3.3 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.

- 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.

- 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.
- 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 2-14](#) on page 69 can be used to provision the EVC to use a non-default Metro Ethernet Network Interface.

Table 2-14. Non-Default Metro Ethernet Network Interface

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

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

The commands listed in [Table 2-15](#) can be used to enable or disable MAC-Switching.

Table 2-15. MAC-Switching

Service	Command	Definition
Voice/Video/Data	<code>ChassisID(config-evc name)#mac-switched</code>	Enabled
Single/Double Tag TLS	<code>ChassisID(config-evc name)#no mac-switched</code>	Disabled

6. If provisioning Single Tag TLS, continue to step [12](#). If provisioning for Double Tag TLS, continue to step [7](#). For all other services, continue to step [9](#).

7. Enable double-tag-switching.

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

8. If provisioning Double Tag TLS, continue to step [12](#). For all other services, continue to step [9](#).

9. 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`

10. If provisioning for voice or data, skip to step [12](#). If provisioning for video, set a priority value for the IGMP packets.

`ChassisID(config-evc name)#subscriber igmp priority <0-7>`

11. 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]`

12. Enable the EVC.

`ChassisID(config-evc name)#no shutdown`

13. Return to the Global Configuration Command Set.

`ChassisID(config-evc name)#exit`

If currently provisioning for video, continue to step 11. If currently provisioning for voice or data, skip to What's Next.

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

Refer to [Table 2-16](#) for a list of available subscriber modes.

Table 2-16. 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.

15. 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.

16. Repeat step 14 - 15 for each access module that will carry IGMP traffic.
17. 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>
```

18. 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 Multicast 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 [Section 2.3.4, “Set the Voice Service Mode on the ONT”](#) on page 73.
- For video, data, or TLS provisioning, continue to [Section 2.3.5, “Provision the Port on the ONT”](#) on page 74.

2.3.4 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 2-10](#) for the selected activation method.

Table 2-17. Discover the ONT

Activation Mode	Command
SIP	ChassisID(config)# voice protocol ont-id@<shelf/slot/port> sip
MGCP	ChassisID(config)# voice protocol ont-id@<shelf/slot/port> mgcp
GR-303	ChassisID(config)# voice protocol ont-id@<shelf/slot/port> 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 [Section 2.3.5, "Provision the Port on the ONT"](#) on page 74.

2.3.5 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 2-18](#) to determine your port type and navigate to your next step.

Table 2-18. Port Type

Service	ONT	Type	See Page
Data/Video/TLS	Non-Remote Gateway	Ethernet	Below
	Remote Gateway	Virtual Gigabit Interface	77
	GPON MDU	VDSL Interface	78
Voice	All ONTs	FXS	75
RF-Video	All ONTs	RF-Video	76

2.3.5.1 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>
```

2. Set the number of mac addresses allowed.
 - 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.
 - If the mac address limit is disabled, it opens unlimited mac addresses on the UNI and the limit is per the hardware resources available.

```
ChassisID(config-giga-eth x/x/x@x/x/x)#mac limit <1-n>
```

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, data, or TLS provisioning, continue to [Section 2.3.7, "Create an EVC-Map"](#) on page 83.

2.3.5.2 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>
```

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 [Section 2.3.6, "Create an IP Host"](#) on page 82.
- For GR-303 provisioning, continue to [Section 2.3.20, "Provision GR-303"](#) on page 114.

2.3.5.3 RF-Video

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

1. Access the video port.

```
ChassisID(config)#interface rf-video <ont-id/0/1>@<shelf/slot/port>
```

2. Enable the video port.

```
ChassisID(config-rf-video x/x/x@x/x/x.gpon)#no shutdown
```

3. Enable video return (SWRD).

```
ChassisID(config-rf-video x/x/x@x/x/x.gpon)#video-return
```

4. Return to the Global Configuration Command Set.

```
ChassisID(config-rf-video x/x/x@x/x/x.gpon)#exit
```

What's Next

For RF-Video, this completes provisioning. Services should be up and running. To provision another service, continue to [Section 2.3.2, "Service Provisioning"](#) on page 62.

2.3.5.4 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, data, or TLS provisioning, continue to [Section 2.3.7, "Create an EVC-Map"](#) on page 83.

2.3.5.5 VDSL Interface

To provision the VDSL interface, complete the following:

1. Access the Global Configuration Command Set.

```
ChassisID#configure terminal
```

2. Access the VDSL Interface Configuration Command Set.

```
ChassisID(config)#interface vdsl <ont-id/0/vdsl-port>@<shelf/slot/
port>.gpon
```

3. Enter a text description of the interface.

```
ChassisID(config-vdsl x/x/x@x/x/x)#description LINE
```

4. Enable the VDSL link up/down alarm.

```
ChassisID(config-vdsl x/x/x@x/x/x)#alarm enable link-down
```

5. Set the service mode.

The DSL service mode must be set for each port.

```
ChassisID(config-vdsl x/x/x@x/x/x)#service-mode vdsl2
```

6. Configure the minimum and maximum downstream payload rates from the VTU-C to the VTU-R.

```
ChassisId(config-vdsl x/x/x@x/x/x)#latency-path payload-rate downstream
0 minimum <32-150000> maximum <32-150000>
```

7. Configure the minimum and maximum upstream payload rates from the VTU-R to the VTU-C.

```
ChassisId(config-vdsl x/x/x@x/x/x)#latency-path payload-rate upstream 0
minimum <32-96000> maximum <32-96000>
```

8. Configure the downstream minimum, target, and maximum noise margins the VTU-R receiver shall tolerate.

```
ChassisID(config-vdsl x/x/x@x/x/x)#dmf-options snr-margin downstream
margins minimum <0.0-31.0> target <0.0-31.0> maximum <0.0-31.0>
```

9. Configure the upstream minimum, target, and maximum noise margins the VTU-R receiver shall tolerate.

```
ChassisID(config-vdsl x/x/x@x/x/x)#dmf-options snr-margin upstream
margins minimum <0.0-31.0> target <0.0-31.0> maximum <0.0-31.0>
```

10. Enable all required hamband notches to reduce hamband interference.

```
ChassisId(config-vdsl x/x/x@x/x/x)#dmf-options hamband-notch
[1.8|3.5|7.0|10.1|14.0|18.06|21.00|24.89|28.00]
```

11. Provision the downstream latency path delay.

```
ChassisId(config-vdsl x/x/x@x/x/x)#latency-path delay downstream 0 <1-
63>
```

12. Provision the upstream latency path delay.

```
ChassisId(config-vdsl x/x/x@x/x/x)#latency-path delay upstream 0 <1-63>
```

13. Provision the upstream latency path initialization policy to maximize data rate.

```
ChassisId(config-vdsl x/x/x@x/x/x)#latency-path init-policy upstream 0
data-rate
```

14. Provision the downstream latency path initialization policy to maximize data rate.

```
ChassisId(config-vdsl x/x/x@x/x/x)#latency-path init-policy downstream 0 data-rate
```

15. Provision the upstream latency path minimum Impulse Noise Protection (INP) to maximize data rate.

```
ChassisId(config-vdsl x/x/x@x/x/x)#latency-path inp upstream 0 <0-16>
```

16. Provision the downstream latency path minimum Impulse Noise Protection (INP) to maximize data rate.

```
ChassisId(config-vdsl x/x/x@x/x/x)#latency-path inp downstream 0 <0-16>
```

17. Provision the upstream latency path type to interleave.

```
ChassisId(config-vdsl x/x/x@x/x/x)#latency-path type upstream 0 interleave
```

18. Provision the downstream latency path type to interleave.

```
ChassisId(config-vdsl x/x/x@x/x/x)#latency-path type downstream 0 interleave
```

19. Provision the upstream power backoff to custom.

```
ChassisId(config-vdsl x/x/x@x/x/x)#power-back-off upstream mode custom
```

20. Provision downstream rate adaption to begin at startup.

```
ChassisId(config-vdsl x/x/x@x/x/x)#rate-adaption downstream startup
```

21. Provision upstream rate adaption to begin at startup.

```
ChassisId(config-vdsl x/x/x@x/x/x)#rate-adaption upstream startup
```

22. Using [Table 2-19](#) and the CLI help prompts, type a variation of the following command:

```
ChassisID(config-vdsl x/x/x)#deployment region 1 scenario 2 other-service 1 application-standard 1 band-plan 1 band-profile 7 psd-u0 1 psd-mask 1
```

Refer to the following for the VDSL deployment syntax:

Table 2-19. VDSL Deployment Syntax

Syntax	Description
Deployment Region	Selects what group spectral masks to be used. North America is the only supported region. Enter 1 to select North America.
Scenario	Determines the usage of lower band frequencies. Exchange is the only supported option. Enter 2 to select Exchange.
Other-service	Selects the other-service sharing the spectrum with VDSL. Typically, the choice will be POTS. The options are as follows: ■ 1 - POTS ■ 4 - ADSL

Table 2-19. VDSL Deployment Syntax (Continued)

Syntax	Description
Application-standard	For VDSL1 (G.993.1) in North America, select ANSI; for VDSL1 in Europe, select ETSI; for VDSL2 (G.993.2), select ITU. The options are as follows: ■ 1 - ANSI ■ 2 - ETSI ■ 4 - ITU
Band-plan	Represents the highest supported band edges for each band carrier group. The option is as follows: ■ 1 - A-998
Band-profile	Selects the characteristics such as PSD and transmit power. This option defaults to 8A. The options are as follows: ■ 1 - 8A - Typical Application: Exchange (CO) ■ 2 - 8B - Typical Application: Exchange (CO) ■ 3 - 8C - Typical Application: Cabinet (RT) ■ 4 - 8D - Typical Application: Exchange (CO) or Cabinet (RT) ■ 5 - 12A - Typical Application: Exchange (CO) or Cabinet (RT) ■ 6 - 12B - Typical Application: Exchange (CO) or Cabinet (RT) ■ 7 - 17A - Typical Application: Cabinet (RT) or MDU
PSD-u0	Determines whether the use of the U0 band is enabled; yes is the recommended default. This is located immediately above POTS/IDSN. The options are as follows: ■ 1 - Enable ■ 2 - Disable
PSD-mask	The PSD mask is applied to the U0; EU 32 is the only supported option. Enter 1 to select EU 32.

**NOTE**

This is not a complete list of options. Some options can dynamically appear and disappear depending on previous selections within the command.

23. Enable the interface.

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

24. Return to the Enable prompt.

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

**What's Next**

For video or data provisioning, continue to [Section 2.3.5.6, "Provision the EFM Port"](#) on page 81.

2.3.5.6 Provision the EFM Port

To provision the EFM port, complete the following:

1. Access the EFM Group Interface Configuration Command Set.

```
ChassisID(config)#interface efm-port <ont-id/0/vdsl-port>@<shelf/slot/
port>.gpon
```

2. Configure the maximum limit of learned MAC addresses for the EFM port interface.

```
ChassisID(config-efm-port x/x/x@x/x/x)#mac limit <1-n>
```

3. Enable the EFM interface.

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

4. Return to the Global Configuration Command Set.

```
ChassisID(config-efm-port x/x/x@x/x/x)#exit
```

5. Return to the Enable prompt.

```
ChassisID(config-atm x/x/x@x/x/x)#end
```

6. Verify the EFM port is In Service.

```
ChassisID#show interfaces efm-port <ont-id/0/vdsl-port>@<shelf/slot/
port>.gpon
```

```
efm-port 1/0/1@1/6/1 is IS and active
```

	Receive	Transmit
Packets	: 0	0
Octets	: 0	0
Overflow	pkt : na	0
Overflow	oct : na	0

What's Next

For video, data, or TLS provisioning, continue to [Section 2.3.7, "Create an EVC-Map"](#) on page 83.

2.3.6 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 2-20](#) for a list of IP host options.

Table 2-20. IP Host Management

IP Host	Command	Description
Static IP	<code>ChassisID(config-ip-host name ont-id@x/x/x)#ip address a.b.c.d a.b.c.d</code>	Set the static IP address and subnet mask for the IP host interface. Continue to step 3.
DHCP	<code>ChassisID(config-ip-host name ont-id@x/x/x)#ip address dhcp</code>	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 [Section 2.3.7, "Create an EVC-Map"](#) on page 83.

2.3.7 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 2-21](#) 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 2-21. 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
	Remote Gateway	Virtual Gigabit-Ethernet	ChassisID(config-evc-map name x/x)# connect uni virtual gigabit-ethernet <ont-id/0/eth-port>@<shelf/slot/pon- port>.gpon
	GPON MDU	EFM	ChassisID(config-evc-map name x/x)# connect uni efm-port <ont-id/0/vdsl- port>@<shelf/slot/port>
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 [16](#). If provisioning for video or TLS, set the subscriber IGMP mode.

- 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.

```
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 16.



NOTICE!

Steps 10 - 15 are only for provisioning TLS. If you are provisioning for voice, video, or data, continue to step 16.

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 27. If provisioning for Double Tag TLS, continue to step 14.

14. Set the C-tag.

```
ChassisID(config-evc-map name x/x)#men-c-tag <2-4094>
```

15. If provisioning for Double Tag TLS, continue to step 27.

16. Set the subscriber modes.

Refer to [Table 2-22](#) on page 85 for a list of available subscriber modes.



NOTE

PPPoE does not support video services.

Table 2-22. Subscriber Modes

Mode	Steps
DHCPv4	Complete the following steps: 1. Apply DHCP for subscriber authentication for the EVC-Map. <code>ChassisID(config-evc-map name x/x)#subscriber access dhcp mode authenticate</code> 2. Discard PPPoE discovery traffic for the EVC-Map. <code>ChassisID(config-evc-map name x/x)#subscriber access pppoe mode block</code>
DHCPv6	Complete the following: 1. Apply DHCP for subscriber authentication for the EVC-Map. <code>ChassisID(config-evc-map name x/x)#subscriber access dhcp6 mode authenticate</code> For a list of DHCPv6 options refer to Table 2-24 on page 87. 2. Discard PPPoE discovery traffic for the EVC-Map. <code>ChassisID(config-evc-map name x/x)#subscriber access pppoe mode block</code>
PPPoE	Complete the following steps: 1. Discard DHCP traffic for the EVC-Map. <code>ChassisID(config-evc-map name x/x)#subscriber access dhcp mode block</code> 2. Apply PPPoE for subscriber authentication for the EVC-Map. <code>ChassisID(config-evc-map name x/x)#subscriber access pppoe mode authenticate</code>

- 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 [“”](#) on page 87 for relay agent provisioning steps.

Refer to [Table 2-23](#) on page 86 for a description of the authentication modes.

Table 2-23. 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 encapsulating 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 2-24](#) on page 87 for a list of available access modes.

Table 2-24. DHCPv6 Access Modes

Access Mode	Command	Description
Authenticate	<code>ChassisID(config-evc-map name x/x)# subscriber access dhcpv6 mode authenticate</code>	Use DHCPv6 for authentication, allow link local IPv6 packets.
Same as DHCPv4	<code>ChassisId(config-evc-map name x/x)# subscriber access dhcpv6 mode same- as-dhcpv4</code>	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	<code>ChassisId(config-evc-map name x/x)# subscriber access dhcpv6 mode transparent</code>	Ignore DHCPv6 packets. Ignore link local IPv6 packets.
Block	<code>ChassisId(config-evc-map name x/x)# subscriber access dhcpv6 mode block</code>	Discard DHCPv6 packets. Blocks link local IPv6 packets.
Snoop	<code>ChassisId(config-evc-map name x/x)# subscriber access dhcpv6 mode snoop</code>	Process DHCP without performing authentication.

17. 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 on the following page 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

- 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 2-25 lists the variables supported by the NetVanta products and the information inserted into the Circuit/Remote ID for each variable.

Table 2-25. 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.
\$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
\$serialnum\$	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.

18. 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 2-25](#) on page 88 for a list of supported variables.

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

19. 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 2-25](#) on page 88 for a list of supported variables.

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

20. 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.

21. 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 2-25](#) on page 88 for a list of supported variables.

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

22. 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 2-25](#)
- on page 88 for a list of supported variables.

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

23. 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.

24. 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 intermediate-agent
```

- b. Configure the format of the Circuit ID. Refer to
- [Table 2-25](#)
- on page 88 for a list of supported variables.

```
ChassisID(config-evc-map name x/x)#subscriber access pppoe intermediate-agent circuit-id WORD
```

25. Enable Intermediate Agent Remote ID insertion.

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

26. Apply any additional EVC-Map configurations.

**NOTE**

The following configurations listed in [Table 2-26](#) on page 91 are optional and not required to pass single-tagged traffic.

Table 2-26. 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.
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.

Table 2-26. Additional EVC-Map Configurations (Continued)

Option	Command	Description
Matching Multicast	<code>ChassisID(config-evc-map name x/x)#match [broadcast l2cp multicast unicast untagged]</code>	Configures the ingress matching criteria to include multicast traffic.
Network Ingress Filter	<code>ChassisID(config-evc-map name x/x)#network-ingress-filter men-pri <0-7> list</code>	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	<code>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]</code>	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.

27. 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 [Section 2.3.8, “Provision the SIP Trunk”](#) on page 93.
- For OMCI MGCP and Non-OMCI MGCP provisioning, continue to [Section 2.3.9, “Provision the MGCP Profile”](#) on page 95.
- For non-remote gateway ONT video or data provisioning, this completes provisioning. Services should be up and running. To provision another service, continue to [Section 2.3.2, “Service Provisioning”](#) on page 62.
- For TLS, this completes provisioning. Services should be up and running. To provision another service, continue to [Section 2.3.2, “Service Provisioning”](#) on page 62.
- For Shaper provisioning, continue to [Section 8, “Traffic Management”](#) on page 331.

2.3.8 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 Switch Module 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. There is a limit of 5 trunks that can be 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.

2.3.8.1 Configure additional SIP Trunks

Before provisioning an additional SIP Trunk, the following restrictions should be observed.

- Up to five SIP Trunks can be provisioned per OLT
- Only one SIP Trunk is allowed per ONT or Subscriber

To provision an additional SIP Trunk, complete the following steps:

1. Access the SIP Trunk Configuration Command Set.

```
ChassisID(config)#
```

2. Create a second SIP Trunk.

```
ChassisID(config)#voice sip-trunk name
```

Where "name" is the designation for the second SIP Trunk, (i.e., T02).

3. Set the SIP User interface.

```
ChassisID(config-sip-trunk 02)#voice user sip 1/0/1@1/19/1
```

Where the SIP User's interface is 1/0/1@1/19/1.

4. Assign the second SIP Trunk to this user.

```
ChassisID(config-voice-user-sip 1/0/1@1/19/1)#sip-trunk T02
```



What's Next

For Non-OMCI and OMCI SIP provisioning, continue to [Section 2.3.11, "Provision the SIP Dialing Profile"](#) on page 98.

2.3.9 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 Non-OMCI MGCP provisioning, continue to [Section 2.3.10, "Provision Non-OMCI MGCP Endpoints"](#) on page 96.
- For OMCI MGCP provisioning, continue to [Section 2.3.19, "Provision OMCI MGCP Endpoints"](#) on page 113.

2.3.10 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.

```
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 [Section 2.3.2, "Service Provisioning"](#) on page 62.

2.3.11 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.

2.3.11.1 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`

2.3.11.2 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**

2.3.11.3 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.
- 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**

2.3.11.4 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>]**

- 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 2-27](#) for a list of dial plan options.

Refer to [Table 2-28](#) on page 102 for a list of SPRE options.

Table 2-27. 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 Section 2.3.17, "Provision the Call Feature Profile (Optional)" on page 109.

Table 2-27. 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 – 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 – 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).

Table 2-28. 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 2-29](#) for a list of External Line Code options.

Table 2-29. 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 – indicates a constant dial tone is heard. ■ Stutter – indicates an intermittent dial tone is heard.



What's Next

- For Non-OMCI SIP provisioning, continue to [Section 2.3.12, "Provision Class of Service \(CoS\) \(Optional\)"](#) on page 104.
- For OMCI SIP provisioning, continue to [Section 2.3.15, "Provision the Media Profile \(Optional\)"](#) on page 107.

2.3.12 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 be 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 [Section 2.3.13, "Provision for Global Voice \(Optional\)"](#) on page 105.

2.3.13 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 [Section 2.3.14, "Provision the Voice User"](#) on page 106.

2.3.14 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 [Section 2.3.2, "Service Provisioning"](#) on page 62.

2.3.15 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 2-30](#) for a list of media profile options.

Table 2-30. 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.
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 [Section 2.3.16, "Provision the CODEC Profile \(Optional\)"](#) on page 108.

2.3.16 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 2-31](#) for a list of CODEC options.

Table 2-31. 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 [Section 2.3.17, “Provision the Call Feature Profile \(Optional\)”](#) on page 109.

2.3.17 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 2-32](#) for a list of call feature options.

Table 2-32. 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.

Table 2-32. Call Feature Profile Options (Continued)

Command	Description
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.
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 [Section 2.3.18, "Provision the OMCI SIP Users"](#) on page 111.

2.3.18 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 2-33](#) for a list of connection options.

Table 2-33. 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 Identity	End-point Index	Admin State	Oper State	Registration 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 [Section 2.3.2, “Service Provisioning”](#) on page 62.
- To provision for Shapers, continue to [Section 8, “Traffic Management”](#) on page 331.

2.3.19 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 [Section 2.3.2, "Service Provisioning"](#) on page 62.

2.3.20 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 [Section 2.3.2, "Service Provisioning"](#) on page 62.

3 Provisioning using the Web GUI

3.1 Scope of this Section

This section provides provisioning for GPON using the Web GUI.



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.

3.2 In this Section

This section contains the topics listed in [Table 3-2](#).

Table 3-1. Section 3 Topics

Sub-Section	Topic	See Page ...
3.3	Provisioning	116

3.3 Provisioning

To provision FTTP, complete the following using the Web GUI:

- [“OLT/PON Provisioning”](#) below
- [“Service Provisioning”](#) on page 130

3.3.1 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.

3.3.1.1 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

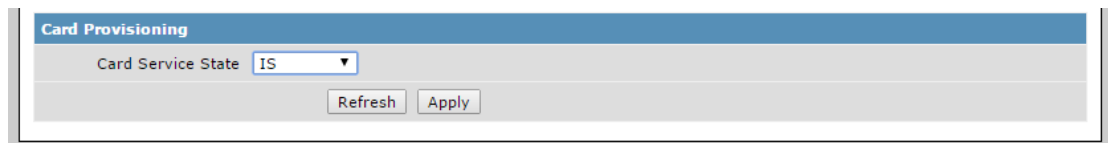


Figure 3-1. OLT Card Service Provisioning

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

3.3.1.2 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 [“Hazard and Advisory Symbols”](#) on page Intro-23.

1. Navigate to the OLT PON Provisioning menu.

Modules > GPON OLT > Provisioning > PON

PON	Service State	Downstream FEC	Deployment Range	Activation Mode
Template				
☐ PON-1	OOS-UAS	☐ Enabled	Standard	Auto-Discovery
☐ PON-2	OOS-UAS	☐ Enabled	Standard	Auto-Discovery
☐ PON-3	OOS-UAS	☐ Enabled	Standard	Auto-Discovery
☐ PON-4	OOS-UAS	☐ Enabled	Standard	Auto-Discovery
☐ PON-5	OOS-UAS	☐ Enabled	Standard	Auto-Discovery
☐ PON-6	OOS-UAS	☐ Enabled	Standard	Auto-Discovery
☐ PON-7	OOS-UAS	☐ Enabled	Standard	Auto-Discovery
☐ PON-8	OOS-UAS	☐ Enabled	Standard	Auto-Discovery

Figure 3-2. 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 [Section 13, “Activation Mode”](#) on page 391.

- 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 [Section 13, “Activation Mode”](#) on page 391.
- 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).
4. Refer to [Table 3-2](#) for range descriptions.

Table 3-2. 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.
- 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 [Section 3.3.1.3, "Enter the Registration-ID"](#) on page 119.
- For all other activation modes, continue to [Section 3.3.1.4, "Discover the ONT"](#) on page 129.

3.3.1.3 Enter the Registration-ID

The registration-ID steps vary depending on your ONT. Use [Table 3-3](#) to navigate to your next step.

Table 3-3. Registration-ID

Registration-ID Procedure	See Page
Section 3.3.1.3.1, "Registration-ID Entry for Total Access 3xx"	120
Section 3.3.1.3.2, "Registration-ID Entry for Total Access 421x /Total Access 421xw"	122
Section 3.3.1.3.3, "Registration-ID Entry for Total Access 3xx Residential Gateway"	124
Section 3.3.1.3.4, "Registration-ID Entry for Total Access 324RG and 334RG"	126
Section 3.3.1.3.5, "Registration-ID Entry for Total Access 324 3rd Generation and Total Access 374"	127
Section 3.3.1.3.6, "Registration-ID Entry for Total Access 4xx"	128

3.3.1.3.1 Registration-ID Entry for Total Access 3xx

To enter a Registration-ID for 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 3-4](#).

Table 3-4. 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 the phone receiver. A dial tone should be heard.



NOTE

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

6. Enter: *001234*XXXXXXXXXX*XXXXXXXXXX* (where XXXXXXXXXXXX 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 3-5](#).

Table 3-5. 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 3-6](#).

Table 3-6. 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 [Section 3.3.1.4, "Discover the ONT"](#) on page 129.

3.3.1.3.2 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 3-7](#) on page 3-123 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 3-7](#) on page 3-123 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 3-7](#).

Table 3-7. 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 least 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 [Section 3.3.1.4, "Discover the ONT"](#) on page 129.

3.3.1.3.3 Registration-ID Entry for Total Access 3xx Residential Gateway

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

- Automatic Serial Number Activation. This is 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 [Section 3.3.1.4, "Discover the ONT"](#) on page 129.

3.3.1.3.4 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 step 7.
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 [Section 3.3.1.4, "Discover the ONT"](#) on page 129.

3.3.1.3.5 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 disabled.



What's Next

Continue to [Section 3.3.1.4, "Discover the ONT"](#) on page 129.

3.3.1.3.6 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 3-3](#) 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 3-3](#)).

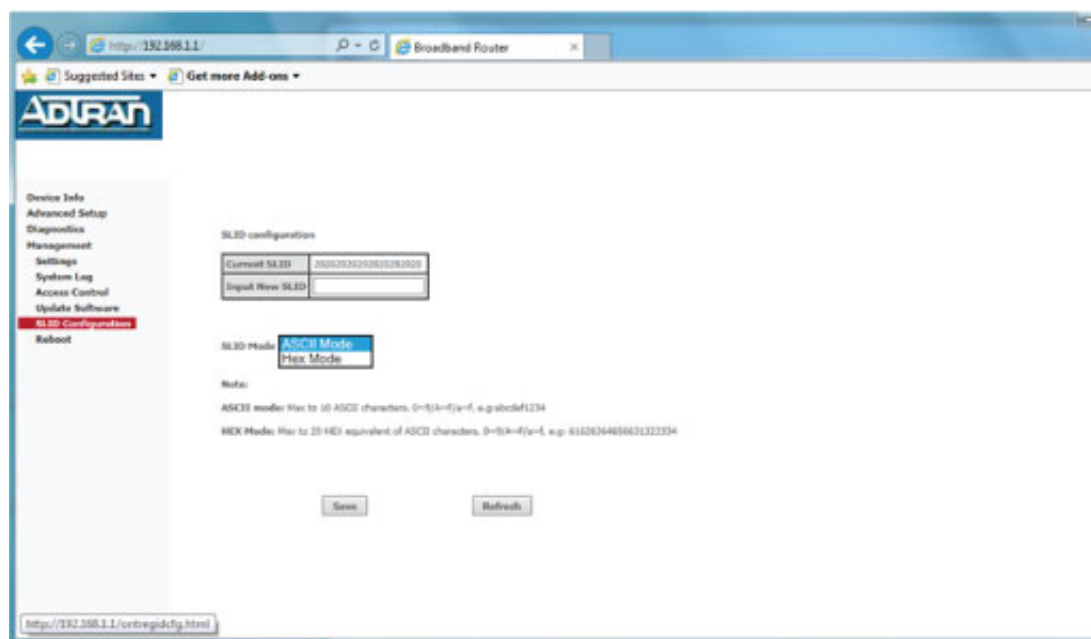


Figure 3-3. 401 Web GUI Display

6. Navigate to Management>SLID Configuration (see the menu tree in [Figure 3-3](#)).
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 [Section 3.3.1.4, “Discover the ONT”](#) on page 129.

3.3.1.4 Discover the ONT

To discover the ONT, complete the following steps:

1. Navigate to the ONT Provisioning menu.

Modules > GPON OLT > Provisioning > ONT

Figure 3-4. ONT Provisioning

2. Discover the ONT. Follow the steps in [Table 3-8](#) 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 3-8. 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.

3.3.2 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:

- [3.3.2.1](#) below
- [Section 3.3.2.2, "Data"](#) on page 136
- [Section 3.3.2.3, "Video"](#) on page 137
- [Section 3.3.2.4, "RF-Video"](#) on page 138

3.3.2.1 Voice

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

3.3.2.1.1 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.

3.3.2.1.2 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.

3.3.2.1.3 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.

3.3.2.1.4 Select Your Voice Option

Use [Table 3-9](#) to determine your voice option and navigate to your next step. If you're unsure of your voice option, refer to [Section 3.3.2.1, "Voice"](#) on page 130.

Table 3-9. Voice Options

Option	See Page
Section 3.3.2.1.5, "SIP OMCI Voice"	Below
Section 3.3.2.1.6, "SIP Non-OMCI Voice"	132
Section 3.3.2.1.7, "MGCP OMCI Voice"	133
Section 3.3.2.1.8, "MGCP Non-OMCI Voice"	134
Section 3.3.2.1.9, "GR-303 Voice"	135

3.3.2.1.5 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 ["Hazard and Advisory Symbols"](#) on page Intro-23.

1. [Section 3.3.3, "Create an EVC"](#) on page 142
2. [Section 3.3.4, "Set the Voice Service Mode on the ONT"](#) on page 145
3. [Section 3.3.5, "Provision the Port on the ONT"](#) on page 146
4. [Section 3.3.6, "Create an IP Host"](#) on page 151
5. [Section 3.3.7, "Create an EVC-Map"](#) on page 153
6. [Section 3.3.8, "Provision the SIP Trunk"](#) on page 159
7. [Section 3.3.11, "Provision the SIP Dialing Profile"](#) on page 163
8. [Section 3.3.16, "Provision the OMCI SIP Users"](#) on page 174

3.3.2.1.6 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 [“Hazard and Advisory Symbols”](#) on page Intro-23.

1. [Section 3.3.3, “Create an EVC”](#) on page 142
2. [Section 3.3.4, “Set the Voice Service Mode on the ONT”](#) on page 145
3. [Section 3.3.5, “Provision the Port on the ONT”](#) on page 146
4. [Section 3.3.6, “Create an IP Host”](#) on page 151
5. [Section 3.3.7, “Create an EVC-Map”](#) on page 153
6. [Section 3.3.8, “Provision the SIP Trunk”](#) on page 159
7. [Section 3.3.11, “Provision the SIP Dialing Profile”](#) on page 163
8. [Section 3.3.13, “Provision Class of Service \(CoS\) \(Optional\)”](#) on page 171
9. [Section 3.3.14, “Provision for Global Voice \(Optional\)”](#) on page 172
10. [Section 3.3.15, “Provision the Voice User”](#) on page 173

3.3.2.1.7 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 [“Hazard and Advisory Symbols”](#) on page Intro-23.

1. [Section 3.3.3, “Create an EVC”](#) on page 142
2. [Section 3.3.4, “Set the Voice Service Mode on the ONT”](#) on page 145
3. [Section 3.3.5, “Provision the Port on the ONT”](#) on page 146
4. [Section 3.3.6, “Create an IP Host”](#) on page 151
5. [Section 3.3.7, “Create an EVC-Map”](#) on page 153
6. [Section 3.3.9, “Provision the MGCP Profile”](#) on page 161
7. [Section 3.3.17, “Provision OMCI MGCP Endpoints”](#) on page 176

3.3.2.1.8 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 [“Hazard and Advisory Symbols”](#) on page Intro-23.

1. [Section 3.3.3, “Create an EVC”](#) on page 142
2. [Section 3.3.4, “Set the Voice Service Mode on the ONT”](#) on page 145
3. [Section 3.3.5, “Provision the Port on the ONT”](#) on page 146
4. [Section 3.3.6, “Create an IP Host”](#) on page 151
5. [Section 3.3.7, “Create an EVC-Map”](#) on page 153
6. [Section 3.3.9, “Provision the MGCP Profile”](#) on page 161
7. [Section 3.3.10, “Provision Non-OMCI MGCP Endpoints”](#) on page 162

3.3.2.1.9 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 [“Hazard and Advisory Symbols”](#) on page Intro-23.

1. [Section 3.3.4, “Set the Voice Service Mode on the ONT”](#) on page 145
2. [Section 3.3.5, “Provision the Port on the ONT”](#) on page 146
3. [Section 3.3.18, “Provision GR-303”](#) on page 177

3.3.2.2 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 [“Hazard and Advisory Symbols”](#) on page Intro-23.

1. [Section 3.3.3, “Create an EVC”](#) on page 142
2. [Section 3.3.5, “Provision the Port on the ONT”](#) on page 146
3. [Section 3.3.7, “Create an EVC-Map”](#) on page 153

3.3.2.3 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 [“Hazard and Advisory Symbols”](#) on page Intro-23.

1. [Section 3.3.3, “Create an EVC”](#) on page 142
2. [Section 3.3.5, “Provision the Port on the ONT”](#) on page 146
3. [Section 3.3.7, “Create an EVC-Map”](#) on page 153

3.3.2.4 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 [“Hazard and Advisory Symbols”](#) on page Intro-23.

1. [Section 3.3.5, “Provision the Port on the ONT”](#) on page 146.

3.3.2.5 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 3-10](#) for an available list of TLS options.

Table 3-10. 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

3.3.2.5.1 Select Your TLS Option

Use [Table 3-9](#) to determine your TLS option and navigate to your next step.

Table 3-11. Voice Options

Option	See Page
TLS Single Tag Configuration	Below
TLS Double Tag Configuration	141

3.3.2.5.2 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 [“Hazard and Advisory Symbols”](#) on page Intro-23.

1. [Section 3.3.3, “Create an EVC”](#) on page 142
2. [Section 3.3.5, “Provision the Port on the ONT”](#) on page 146
3. [Section 3.3.7, “Create an EVC-Map”](#) on page 153

3.3.2.5.3 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 ["Hazard and Advisory Symbols"](#) on page Intro-23.

1. [Section 3.3.3, "Create an EVC"](#) on page 142
2. [Section 3.3.5, "Provision the Port on the ONT"](#) on page 146
3. [Section 3.3.7, "Create an EVC-Map"](#) on page 153

3.3.3 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

Name	S-Tag	Admin State	Status	Switching Mode	MAC Aging Time	IGMP Priority	IGMP Version	CE-VLAN Preservation
system-management-evc	247	Enabled	Running	MAC	5	5	2	Enabled

Create EVC
Operation **Create**
Name

Figure 3-5. 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 (see [Figure 3-6](#) on page 143).

Figure 3-6. 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 3-12. 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.

Name	Slot	Status	Proxy Host IP Address	Last Member Query Interval (ms)	Last Member Query Count	Mode
VIDEO	A	Not running, EVC does not exist	10.10.10.1	1000	2	Proxy

Create IGMP EVC

IGMP EVC Name: EVC Name : 4096 Select an existing EVC.

Slot: 1 Select a slot for connection to the IGMP EVC.

Create

Figure 3-7. 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 3-145.
- For video or data provisioning, continue to [Section 3.3.5, “Provision the Port on the ONT”](#) on page 146.
- For TLS provisioning, continue to [Section 3.3.7, “Create an EVC-Map”](#) on page 153.

3.3.4 Set the Voice Service Mode on the ONT

1. Navigate to the ONT Provisioning menu.

Modules > GPON OLT > Provisioning > ONT

Figure 3-8. 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 65K110GPON-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 65K110GPON-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 [Section 3.3.5, "Provision the Port on the ONT"](#) on page 146.

3.3.5 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

PON: 1 ▼ ONT: 1 ▼ Port Type: Ethernet ▼

Add Del	Refresh Apply				
☐ Port	Operational State	Service State	Description	Auto Detection Configuration	MAC Limit
▼ Template	 	 	 	 	
Add Del	Refresh Apply				

Figure 3-9. ONT Port Provisioning

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

Table 3-13. Port Type

Service	ONT	Type	See Page
Data/Video	Non-Remote Gateway	Ethernet	147
	Remote Gateway	Virtual Gigabit Interface	150
Voice	All ONTs	FXS	148
RF-Video	All ONTs	RF-Video	149

3.3.5.1 Ethernet

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

1. Set the number of MAC addresses allowed.

PON: ONT: Port Type:

Port	Operational State	Service State	Description	Auto Detection Configuration	MAC Limit
Template					

Add Del Refresh Apply

Figure 3-10. 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 [Section 3.3.7, "Create an EVC-Map"](#) on page 153.

3.3.5.2 FXS

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

PON: ONT: Port Type:

Port	Operational State	Service State	Description	Tx Gain	Rx Gain	Impedance	Service Mode
▼ Template							

Add Del Refresh Apply

Figure 3-11. 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 [Section 3.3.6, "Create an IP Host"](#) on page 151.
- For GR-303 provisioning, continue to [Section 3.3.18, "Provision GR-303"](#) on page 177.

3.3.5.3 RF-Video

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

PON: ONT: Port Type: Display: ☐ Video Return Path

Port	Operational State	Service State	Description	Video-LOS Alarm	Video-OOR Low Alarm	Video-OOR High Alarm	Video Return
Template							

Figure 3-12. RF-Video Port Provisioning

1. Enable the video return.
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 [Section 3.3.2, "Service Provisioning"](#) on page 130.

3.3.5.4 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 [Section 3.3.6, “Create an IP Host”](#) on page 151.
- For video or data provisioning, continue to [Section 3.3.7, “Create an EVC-Map”](#) on page 153.

3.3.6 Create an IP Host

1. Navigate to the IP Host Provisioning menu.

Modules > GPON OLT > Provisioning > IP Host

PON: ONT: Display: ☒ Last Active Error

Del	IP Host Name	Mode	IP Address	Subnet Mask	Gateway IP address	Connected Service	Connected Pseudowire Channels	Operational Status	Last Error
☐									

Note: IP-Host must have a connection to enable changing the service state.

Edit/Create

IP-Host Name

Figure 3-13. IP-Host Create Menu

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

PON: ONT: Display: ☒ Last Active Error

Del	IP Host Name	Mode	IP Address	Subnet Mask	Gateway IP address	Connected Service	Connected Pseudowire Channels	State	Last Error
☐	TEST	Static	0.0.0.0	0.0.0.0	0.0.0.0	None	None	Fields Not Set	No service/interface attached to IP-Host

Note: IP-Host must have a connection to enable changing the service state.

Edit/Create

IP Host Name **TEST**

IP Allocation

IP Address IP Allocation must be static to edit this field.

Subnet Mask IP Allocation must be static to edit this field.

Gateway IP Allocation must be static to edit this field.

State IP Host must have a connection and be allocated using DHCP or have a connection and a non-zero IP Address and Gateway IP to set service state

Create IP Host Connection

Connection Type

Channel Number

TEST IP Host Connections

Del	Connection	Service/Interface	Channel	Status
☐				

Figure 3-14. 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 [Section 3.3.7, "Create an EVC-Map"](#) on page 153.

3.3.7 Create an EVC-Map

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

1. Access the Interface Map.

Modules > GPON OLT > Provisioning > Interface Map

Name	Subscriber Interface	EVC Name	EVC S-Tag	C-Tag	Service State	Status
2						

Create/Edit

Map Name *Case sensitive search for Interface Map by name.*

Figure 3-15. 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.

Edit Interface Map		
Operation	Edit	
Map Name	EVC-Map Example	A user-specified name meant to identify the ethernet flow uniquely.
Description		A user-specified description of the flow.
Service State	Not Ready ▼	
Status	Disabled	
Subscriber Interface		
Interface Type	Gigabit-Ethernet ▼	Type is required to create a new map.
PON	1 ▼	PON number.
ONT	1 ▼	ONT number.
ONT Port	1 ▼	ONT port number.
Upstream Channel	None ▼	Upstream channel number.
VLAN Configuration		
EVC Name	None ▼	EVC 'Name:S-Tag'. Ethernet Virtual Connections can be created from the sidebar Services EVCs page.
S-Tag Priority	Marked ▼	Upstream priority used by the EVC on traffic and P-Bit value when priority method is 'Marked'. When Inherit is selected, use the priority of the ingress traffic.
C-Tag	None ▼	Customer Tag - the inner tag attached to all upstream data associated with this EVC Map. If EVC preserve CE-VLAN ID is enabled then the C-tag must be set to None.
C-Tag Priority	Marked ▼	If a C-Tag is specified, this priority will be assigned to the C-tag. If the priority tag is marked, then this value must be set. When Inherit is selected, use the priority of the ingress traffic.
Authentication Configuration		
DHCP Processing	Authenticate ▼	Set the DHCPv4 processing mode. Authenticate - use DHCP for subscriber authentication, Block - block DHCP, Transparent - ignore DHCP, Snoop - Process DHCP without performing authentication.
DHCPv6 Processing	Same As DHCPv4 ▼	Set the DHCPv6 processing mode. Authenticate - use DHCPv6 for subscriber authentication, Block - block DHCPv6, Transparent - ignore DHCPv6, Same As DHCPv4 - Use same mode on DHCPv6 as what is provisioned on DHCPv4
PPPoE Processing	Authenticate ▼	Set the PPPoE processing mode. Authenticate - use PPPoE for subscriber authentication, Block - block PPPoE, Transparent - ignore PPPoE.
Advanced Configuration		
Show Advanced	Advanced	Selecting button will toggle the display of the Advanced Configuration.
IGMP		
Show IGMP	IGMP	Selecting button will toggle the display of the IGMP configuration.
Cancel Apply		

Figure 3-16. EVC-Map Edit

3. Set the Service State to **Active**.

4. Select the Interface Type. Use [Table 3-14](#) to determine the type and the steps to complete.

Table 3-14. 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.
 - 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 3-15](#) on page 3-156 to determine the authentication and steps required.

**NOTE**

PPPoE does not support video services.

Table 3-15. 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 65K110GPON-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**.

Matching Criteria	
CE-VLAN Tagged or Untagged	Match on a specific customer tag by choosing the tag id. To match on untagged traffic, choose 'None'. To match all traffic, choose 'Tagged or Untagged'.
P-Bit 1 0 0 0 4	Customer Ingress P-Bit matching criteria. Hold Ctrl or Shift to select multiple P-Bit Values.
Network P-Bit 1 0 0 0 4	Network Ingress P-Bit matching criteria. Hold Ctrl or Shift to select multiple P-Bit values.
DSCP List	Customer Ingress Differentiated Services Code Point in matching criteria. List (12, 18, 27); Range (7-19); or Combination (1-6, 8, 12-19).
Multicast ☐ Enabled	Include multicast traffic in matching criteria.

Figure 3-17. 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**.

IGMP	
Show IGMP Hide IGMP	Selecting button will toggle the display of the IGMP configuration.
IGMP Authentication Enable	Enable/disable authentication of source MAC addresses used in IGMP messages. The default is Enable, which requires source MAC addresses of the IGMP messages to have been authenticated using another protocol. When disabled, the IGMP messages will be processed regardless of the source MAC address.
IGMP Mode Block	The IGMP Mode associated with each EVC map. Processing Enabled - process IGMP messages based on provisioned IGMP mode on the EVC, Block - discard all IGMP messages, Transparent - Pass IGMP messages transparently, Forking - Copy upstream IGMP messages from the Video Map to this Map.
Router IP 0.0.0.0	The source IP address that the DSLAM places in IGMP messages destined for the subscriber. This value only applies when IGMP is in proxy mode.
Multicast Bandwidth 0 ☐ Enabled	Maximum downstream bandwidth(Kbps) available for this map. Joins for the subscriber's multicast streams are checked to not exceed this bandwidth when enabled.
Multicast Groups 6 ☐ Enabled	Maximum multicast groups allowed for this map. Joins for the subscriber's multicast streams are checked to not exceed this maximum when enabled.
Immediate Leave Disabled	Enable/disable smart immediate leave. Disable is the equivalent of setting Last Member Query Count to 0.
Cancel Apply	

Figure 3-18. 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 [Section 3.3.8, “Provision the SIP Trunk”](#) on page 159.
- For OMCI MGCP and Non-OMCI MGCP provisioning, continue to [Section 3.3.9, “Provision the MGCP Profile”](#) on page 161.
- For remote gateway, refer to the [ADTRAN 400 Series Residential Gateway ONT Basic Configuration Guide](#).
- For non-remote gateway ONT video or data provisioning, this completes provisioning. Services should be up and running. To provision another service, continue to [Section 3.3.2, “Service Provisioning”](#) on page 130.
- For TLS, this completes provisioning. Services should be up and running. To provision another service, continue to [Section 3.3.2, “Service Provisioning”](#) on page 130.

3.3.8 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**

Trunk	
Trunk Name	Trunk's 2 digit identifier following T. ex. T01
Primary Proxy	IP address or host name of the primary proxy server.
Primary Proxy Port	UDP port number of primary proxy server: 1 - 65535.
Secondary Proxy	IP address or host name of the secondary proxy server.
Secondary Proxy Port	UDP port number of secondary proxy server: 1 - 65535.
Outbound Primary Proxy	IP address or host name of the primary outbound proxy server.
Outbound Primary Proxy Port	UDP port number of primary outbound proxy server: 1 - 65535.
Outbound Secondary Proxy	IP address or host name of the secondary outbound proxy server.
Outbound Secondary Proxy Port	UDP port number of secondary outbound proxy server: 1 - 65535.
Primary Registrar	IP address or host name of the primary registrar.
Primary Registrar Port	UDP port number of primary registrar: 1 - 65535.
Secondary registrar	IP address or host name of the secondary registrar.
Secondary Registrar Port	UDP port number of secondary registrar: 1 - 65535.
Maximum Registrations	Maximum concurrent registrations: 1-32.
Registrar Expiration Time	Expiration time in seconds: 30-2147483647.
Require Expiration Header	☐ Enabled
Domain	Domain Name.
Dial-string Source	Request URI Use to specify the dial-string source for the SIP server.
Keep alive method	None The keep-alive method to use for SIP registrar connections.
Keep alive interval	Interval in seconds: 30 - 3600.
Registration-failure Retry Timer	Retry time in seconds: 10 - 604800.
Rollover Timer	Time to wait before rolling over to next server: seconds 1-32.
Request URI Resolution	☐ Enabled Enables the local unit to resolve the domain before resolving the request uniform resource identifier (URI).
Request URI Host Format	Domain Used to format the Request uniform resource identifier (URI) for SIP messages.
From Header Format	Domain Specifies the Host field formatting for the From header.
To Header Format	Domain Used to configure the To header host format of SIP trunk messages.
Alert Information URL	Specifies the Alert-Info HyperText Transfer Protocol (HTTP) universal resource locator (URL) header format.
Require 100rel	☐ Enabled Include 100rel in Require Header.
Support 100rel	☐ Enabled Include 100rel in Support Header.
User-agent	Default Used to configure the To header host format of SIP trunk messages.
User Supplied agent	Used if User-agent is set to User Supplied. Maximum of 128 characters.
SIP Authentication	☐ Enable SIP Server authentication
SIP DSCP	Differentiated Services Code Point for SIP packets: 0 - 63.
RTP DSCP	Differentiated Services Code Point for RTP packets: 0 - 63.
Trust Domain	☐ This Trunk is connected to a trust domain
P-Asserted-Identity required	☐ A P-Asserted-Identity header is required for this trust domain
Apply Cancel	

Figure 3-19. 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 65K110SM-31).
10. Click **Apply**.



What's Next

For Non-OMCI and OMCI SIP provisioning, continue to [Section 3.3.11, "Provision the SIP Dialing Profile"](#) on page 163.

3.3.9 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 [Section 3.3.17, “Provision OMCI MGCP Endpoints”](#) on page 176.
- For Non-OMCI MGCP provisioning, continue to [Section 3.3.10, “Provision Non-OMCI MGCP Endpoints”](#) on page 162.

3.3.10 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 [Section 3.3.2, "Service Provisioning"](#) on page 130.

3.3.11 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.

3.3.11.1 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`

3.3.11.2 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**

3.3.11.3 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 (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**

3.3.11.4 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 3-20. 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 [Section 3.3.12, “Provision the Common Profiles \(Optional\)”](#) on page 167.
- For Non-OMCI SIP provisioning, continue to [Section 3.3.13, “Provision Class of Service \(CoS\) \(Optional\)”](#) on page 171.

3.3.12 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 65K110SM-31). Creating Common Profiles is optional for your network. If these profiles are not required, continue to [Section 3.3.16, "Provision the OMCI SIP Users"](#) on page 174.

Refer to [Table 3-16](#) for a list of the supported profiles.

Table 3-16. Common Profiles

Profile	Support	See Page
Call Feature	SIP	167
Media	SIP/MGCP	169
Codec	SIP/MGCP	170

3.3.12.1 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 3-17](#) for a list of call feature options.

Table 3-17. 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 outbound caller ID from this endpoint.

Table 3-17. Call Feature Profile Options (Continued)

Option	Description
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.
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 [Section 3.3.12.2, "Provision the Media Profile"](#) on page 169.

3.3.12.2 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 3-18](#) for a list of media profile options.

Table 3-18. 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.
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 [Section 3.3.12.3, "Provision the Codec Profile"](#) on page 170.

3.3.12.3 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 3-19](#) for a list of CODEC options.

Table 3-19. 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 [Section 3.3.16, "Provision the OMCI SIP Users"](#) on page 174.
- For OMCI MGCP continue to [Section 3.3.17, "Provision OMCI MGCP Endpoints"](#) on page 176.

3.3.13 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 be 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 65K110SM-31).

5. Click **Apply**.



What's Next

Continue to [Section 3.3.14, "Provision for Global Voice \(Optional\)"](#) on page 172.

3.3.14 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](#).



What's Next

Continue to [Section 3.3.15, "Provision the Voice User"](#) on page 173.

3.3.15 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 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>.

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 [Section 3.3.2, "Service Provisioning"](#) on page 130.

3.3.16 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

The screenshot displays the 'Users' tab in the provisioning web GUI. At the top, there are tabs for 'Trunk', 'Users', and 'Dialing Profiles'. Below the tabs, there are filter fields: 'Filter By:', 'Slot:', 'Pon/AE Port:', and 'Ont:', followed by an 'Apply' button. A table with 7 columns is shown, with a 'Refresh' button to its right. Below the table is a 'Create/Edit Centralized User' section. This section contains four input fields with labels and ranges: 'Slot' (Slot(1-22)), 'GPON/AE PORT' (GPON PORT(1-8)/AE PORT(1-24)), 'ONT' (GPON ONT(1-64)/AE ONT(1)), and 'Identifier' (Endpoint Index(1-10)). At the bottom of this section are 'Edit' and 'Create' buttons.

Figure 3-21. 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**. [Figure 3-22](#) on page 175 is displayed.

Provision SIP User		
Endpoint Index		
Endpoint Index	1/0/1@1/1/1	
Description		<i>A description of this voice user. Maximum of 20 characters.</i>
Identity		<i>SIP identity</i>
Trunk		<i>Trunk's 2 digit identifier following T. ex. T01</i>
Username		<i>Username for authentication to SIP server</i>
Password		<i>Password for authentication to SIP server</i>
Dialing Plan Profile		<i>Dialing Plan Profile used with this voice user</i>
Codec List Profile		<i>Codec Profile used with this voice user</i>
Media Profile		<i>Media Profile used with this voice user</i>
Call Feature Profile		<i>Call Feature Profile used with this voice user</i>
FXS Port	v	<i>FXS port connected to this voice user</i>
Service State	Active	
Oper Status	DOWN	
Last Error	Voice user not connected to valid FXS port	
Cancel Apply		

Figure 3-22. 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 Dialing 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 [Section 3.3.2, "Service Provisioning"](#) on page 130.

3.3.17 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 [Section 3.3.2, "Service Provisioning"](#) on page 130.

3.3.18 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 [Section 3.3.2, "Service Provisioning"](#) on page 130.

4 Provisioning Active Ethernet using CLI

4.1 Scope of this Section

This section provides the minimum amount of steps required to provision a GPON module for the FTTP application using Active Ethernet and CLI.



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.

4.2 In this Section

This section contains the topics listed in [Table 4-1](#).

Table 4-1. Section 4 Topics

Sub-Section	Topic	See Page
4.3	Provisioning	180

4.3 Provisioning

4.4 In this Section

To provision the OLT/PON, complete the following:

- [Section 4.4.1, “OLT/PON Provisioning”](#) below
- [Section 4.4.2, “Service Provisioning”](#) on page 183

4.4.1 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.

4.4.1.1 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 [Section 4.4.1.2, “Discover the ONT”](#) on page 181.

4.4.1.2 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 [Section 4.4.1.3, "ONT Inband Management Provisioning"](#) on page 182.

4.4.1.3 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 4-2](#) for the inband management options.

Table 4-2. 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**

4.4.2 Service Provisioning

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

- [Section 4.4.2.1, "Voice"](#) below
- [Section 4.4.2.2, "Data"](#) on page 190
- [Section 4.4.2.3, "Video"](#) on page 191

4.4.2.1 Voice

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

4.4.2.1.1 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.

4.4.2.1.2 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.

4.4.2.1.3 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.

4.4.2.1.4 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 [Section 4.4.2.1, "Voice"](#) on page 183.

Table 4-3. Voice Options

Option	See Page
Section 4.4.2.1.5, "SIP OMCI Voice"	185
Section 4.4.2.1.6, "SIP Non-OMCI Voice"	186
Section 4.4.2.1.7, "MGCP OMCI Voice"	187
Section 4.4.2.1.8, "MGCP Non-OMCI Voice"	188
Section 4.4.2.1.9, "GR-303 Voice"	189

4.4.2.1.5 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.

1. [Section 4.4.3, "Create an EVC"](#) on page 193
2. [Section 4.4.4, "Set the Voice Service Mode on the ONT"](#) on page 198
3. [Section 4.4.5, "Provision the Port on the ONT"](#) on page 199
4. [Section 4.4.6, "Create an IP Host"](#) on page 202
5. [Section 4.4.7, "Create an EVC-Map"](#) on page 203
6. [Section 4.4.8, "Provision the SIP Trunk"](#) on page 213
7. [Section 4.4.11, "Provision the SIP Dialing Profile"](#) on page 217
8. [Section 4.4.18, "Provision the OMCI SIP Users"](#) on page 231

4.4.2.1.6 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.

1. [Section 4.4.3, "Create an EVC"](#) on page 193
2. [Section 4.4.4, "Set the Voice Service Mode on the ONT"](#) on page 198
3. [Section 4.4.5, "Provision the Port on the ONT"](#) on page 199
4. [Section 4.4.6, "Create an IP Host"](#) on page 202
5. [Section 4.4.7, "Create an EVC-Map"](#) on page 203
6. [Section 4.4.8, "Provision the SIP Trunk"](#) on page 213
7. [Section 4.4.11, "Provision the SIP Dialing Profile"](#) on page 217
8. [Section 4.4.12, "Provision Class of Service \(CoS\) \(Optional\)"](#) on page 223
9. [Section 4.4.13, "Provision for Global Voice \(Optional\)"](#) on page 224
10. [Section 4.4.14, "Provision the Voice User"](#) on page 225

4.4.2.1.7 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.

1. [Section 4.4.3, "Create an EVC" on page 193](#)
2. [Section 4.4.4, "Set the Voice Service Mode on the ONT" on page 198](#)
3. [Section 4.4.5, "Provision the Port on the ONT" on page 199](#)
4. [Section 4.4.6, "Create an IP Host" on page 202](#)
5. [Section 4.4.7, "Create an EVC-Map" on page 203](#)
6. [Section 4.4.9, "Provision the MGCP Profile" on page 214](#)
7. [Section 4.4.19, "Provision OMCI MGCP Endpoints" on page 233](#)

4.4.2.1.8 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.

1. [Section 4.4.3, "Create an EVC"](#) on page 193
2. [Section 4.4.4, "Set the Voice Service Mode on the ONT"](#) on page 198
3. [Section 4.4.5, "Provision the Port on the ONT"](#) on page 199
4. [Section 4.4.6, "Create an IP Host"](#) on page 202
5. [Section 4.4.7, "Create an EVC-Map"](#) on page 203
6. [Section 4.4.9, "Provision the MGCP Profile"](#) on page 214
7. [Section 4.4.10, "Provision Non-OMCI MGCP Endpoints"](#) on page 215

4.4.2.1.9 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.

1. [Section 4.4.4, “Set the Voice Service Mode on the ONT”](#) on page 198
2. [Section 4.4.5, “Provision the Port on the ONT”](#) on page 199
3. [Section 4.4.20, “Provision GR-303”](#) on page 234

4.4.2.2 Data

To provision for data, complete the following steps:



NOTE

This is a general set of instructions to turn up data.

1. [Section 4.4.3, “Create an EVC”](#) on page 193
2. [Section 4.4.5, “Provision the Port on the ONT”](#) on page 199
3. [Section 4.4.7, “Create an EVC-Map”](#) on page 203

4.4.2.3 Video

To provision for video, complete the following:

**NOTE**

This is a general set of instructions to turn up video.

1. [Section 4.4.3, “Create an EVC”](#) on page 193
2. [Section 4.4.5, “Provision the Port on the ONT”](#) on page 199
3. [Section 4.4.7, “Create an EVC-Map”](#) on page 203

4.4.2.4 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.

1. [Section 4.4.3, “Create an EVC”](#) on page 193
2. [Section 4.4.5, “Provision the Port on the ONT”](#) on page 199
3. [Section 4.4.7, “Create an EVC-Map”](#) on page 203

4.4.3 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.
- 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.
- 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.
- 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 4-4](#) can be used to provision the EVC to use a non-default Metro Ethernet Network Interface.

Table 4-4. 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>

Table 4-4. Non-Default Metro Ethernet Network Interface (Continued)

Interface	Command
LAG group	<code>ChassisID(config-evc name)#connect men-port lag-group <shelf/slot/group></code>

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

The commands listed in [Table 4-5](#) can be used to enable or disable MAC-Switching.

Table 4-5. MAC-Switching

Service	Command	Definition
Voice/Video/Data	<code>ChassisID(config-evc name)#mac-switched</code>	Enabled
Single Tag TLS	<code>ChassisID(config-evc name)#no mac-switched</code>	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 4-6](#) on page 195 for a list of available subscriber modes.

Table 4-6. 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:

- 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 Multicast 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 [Section 4.4.4, “Set the Voice Service Mode on the ONT”](#) on page 198.
- For video, data, or TLS provisioning, continue to [Section 4.4.5, “Provision the Port on the ONT”](#) on page 199.

4.4.4 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 4-7](#) for the selected activation method.

Table 4-7. Discover the ONT

Activation Mode	Command
SIP	ChassisID(config)#voice protocol ONT-ID@<shelf/slot/port>.gigabit-ethernet sip
MGCP	ChassisID(config)#voice protocol ONT-ID@<shelf/slot/port>.gigabit-ethernet mgcp
GR-303	ChassisID(config)#voice protocol ONT-ID@<shelf/slot/port>.gigabit-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 [Section 4.4.5, "Provision the Port on the ONT"](#) on page 199.

4.4.5 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 4-8](#) to determine your port type and navigate to your next step.

Table 4-8. Port Type

Service	Type	See Page
Data/Video	Ethernet	199
Voice	FXS	200

4.4.5.1 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/eth-
port>@<shelf/slot/port>.gigabit-ethernet
```

2. Set the number of mac addresses allowed.

- 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 [Section 4.4.7, "Create an EVC-Map"](#) on page 203.

4.4.5.2 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 [Section 4.4.6, "Create an IP Host"](#) on page 202.
- For GR-303 provisioning, continue to [Section 4.4.20, "Provision GR-303"](#) on page 234.

4.4.5.3 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 [Section 4.4.7, "Create an EVC-Map"](#) on page 203.

4.4.6 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. To create an IP Host, complete the following steps:

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 4-9](#) for a list of IP host options.

Table 4-9. IP Host Management

IP Host	Command	Description
Static IP	<code>ChassisID(config-ip-host name ont-id@x/x/x)#ip address A.B.C.D A.B.C.D</code>	Set the static IP address and subnet mask for the IP host interface. Continue to step 3.
DHCP	<code>ChassisID(config-ip-host name ont-id@x/x/x)#ip address dhcp</code>	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 [Section 4.4.7, "Create an EVC-Map"](#) on page 203.

4.4.7 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.

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

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 4-10](#) 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 4-10. Interface Type

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

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, for example, 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 4-11 for a list of available subscriber modes.



NOTE

PPPoE does not support video services.

Table 4-11. 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

Table 4-11. Subscriber Modes (Continued)

Mode	Steps
DHCPv6	Complete the following: 1. Apply DHCP for subscriber authentication for the EVC-Map. <code>ChassisID(config-evc-map name x/x)#subscriber access dhcp mode authenticate</code> For a list of DHCPv6 options refer to Table 4-13. 2. Discard PPPoE discovery traffic for the EVC-Map. <code>ChassisID(config-evc-map name x/x)#subscriber access pppoe mode block</code>
PPPoE	Complete the following steps: 1. Discard DHCP traffic for the EVC-Map. <code>ChassisID(config-evc-map name x/x)#subscriber access dhcp mode block</code> 2. Apply PPPoE for subscriber authentication for the EVC-Map. <code>ChassisID(config-evc-map name x/x)#subscriber access pppoe mode authenticate</code>

- 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 [Section 15](#), “Configure the Relay Agent.” on page 206 for relay agent provisioning steps.

Refer to [Table 4-12](#) for a description of the authentication modes.

Table 4-12. 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.

Table 4-12. Authentication Mode Description (Continued)

Authentication Mode	Description
PPPoE Processing	Point to Point Protocol over Ethernet (PPPoE) processing is a network protocol for encapsulating 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 4-13](#) for a list of available access modes.

Table 4-13. DHCPv6 Access Modes

Access Mode	Command	Description
Authenticate	<code>ChassisID(config-evc-map name x/x)# subscriber access dhcpv6 mode authenticate</code>	Use DHCPv6 for authentication, allow link local IPv6 packets.
Same as DHCPv4	<code>ChassisId(config-evc-map name x/x)# subscriber access dhcpv6 mode same- as-dhcpv4</code>	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	<code>ChassisId(config-evc-map name x/x)# subscriber access dhcpv6 mode transparent</code>	Ignore DHCPv6 packets. Ignore link local IPv6 packets.
Block	<code>ChassisId(config-evc-map name x/x)# subscriber access dhcpv6 mode block</code>	Discard DHCPv6 packets. Blocks link local IPv6 packets.
Snoop	<code>ChassisId(config-evc-map name x/x)# subscriber access dhcpv6 mode snoop</code>	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

- 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 4-14](#) lists the variables supported by the NetVanta products and the information inserted into the Circuit/Remote ID for each variable.

Table 4-14. 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

Table 4-14. Supported Variables (Continued)

Variable	Output Description
\$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.
\$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
\$serialnum\$	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 4-14](#) on page 207 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 4-14](#) on page 207 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 4-14](#) on page 207 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 4-14](#) on page 207 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 intermediate-agent
```

- b. Configure the format of the Circuit ID. Refer to [Table 4-14](#) on page 207 for a list of supported variables.

```
ChassisID(config-evc-map name x/x)#subscriber access pppoe intermediate-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 4-15](#) are optional and not required to pass single-tagged traffic.

Table 4-15. 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.

Table 4-15. Additional EVC-Map Configurations (Continued)

Option	Command	Description
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.
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.

Table 4-15. Additional EVC-Map Configurations (Continued)

Option	Command	Description
Matching Multicast	<code>ChassisID(config-evc-map name x/x)#match [broadcast l2cp multicast unicast untagged]</code>	Configures the ingress matching criteria to include multicast traffic.
Network Ingress Filter	<code>ChassisID(config-evc-map name x/x)#network-ingress-filter men-pri <0-7> LIST</code>	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	<code>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]</code>	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 [Section 4.4.8, “Provision the SIP Trunk”](#) on page 213.
- For OMCI MGCP and Non-OMCI MGCP provisioning, continue to [Section 4.4.9, “Provision the MGCP Profile”](#) on page 214.

4.4.8 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 [Section 4.4.11, "Provision the SIP Dialing Profile"](#) on page 217.

4.4.9 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 [Section 4.4.19, "Provision OMCI MGCP Endpoints"](#) on page 233.
- For Non-OMCI MGCP provisioning, continue to [Section 4.4.10, "Provision Non-OMCI MGCP Endpoints"](#) on page 215.

4.4.10 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.

```
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 [Section 4.4.2, "Service Provisioning"](#) on page 183.

4.4.11 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.

4.4.11.1 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`

4.4.11.2 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**

4.4.11.3 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 (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**

4.4.11.4 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 4-16](#) on page 221 for a list of dial plan options.

Table 4-16. 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 Section 4.4.17, “Provision the Call Feature Profile (Optional)” on page 229.
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 – 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 – 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 4-17](#) for a list of SPRE options.

Table 4-17. 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 4-18](#) for a list of External Line Code options.

Table 4-18. 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 [Section 4.4.15, “Provision the Media Profile \(Optional\)”](#) on page 226.
- For Non-OMCI SIP provisioning, continue to [Section 4.4.12, “Provision Class of Service \(CoS\) \(Optional\)”](#) on page 223.

4.4.12 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 be 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 [Section 4.4.13, “Provision for Global Voice \(Optional\)”](#) on page 224.

4.4.13 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 (RTP).

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 [Section 4.4.14, "Provision the Voice User"](#) on page 225.

4.4.14 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 [Section 4.4.2, "Service Provisioning"](#) on page 183.

4.4.15 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 4-19](#) for a list of media profile options.

Table 4-19. 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 4-19. 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 [Section 4.4.16, "Provision the CODEC Profile \(Optional\)"](#) on page 228.

4.4.16 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 4-20](#) for a list of CODEC options.

Table 4-20. 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 [Section 4.4.17, “Provision the Call Feature Profile \(Optional\)”](#) on page 229.

4.4.17 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 4-21](#) for a list of call feature options.

Table 4-21. 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.

Table 4-21. Call Feature Profile Options (Continued)

Command	Description
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.
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 [Section 4.4.18, "Provision the OMCI SIP Users"](#) on page 231.

4.4.18 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 4-22](#) for a list of connection options.

Table 4-22. 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 Identity	End-point Index	Admin State	Oper State	Registration 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 [Section 4.4.2, “Service Provisioning”](#) on page 183.
- To provision for shapers, continue to [Section 8.3, “Shapers, GPON”](#) on page 332.

4.4.19 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 [Section 4.4.2, "Service Provisioning"](#) on page 183.

4.4.20 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 [Section 4.4.2, "Service Provisioning"](#) on page 183.

5 Provisioning Active Ethernet using the Web

5.1 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.

5.2 In this Section

This section contains the topics listed in [Table 5-1](#).

Table 5-1. Section 5 Topics

Sub-Section	Topic	See Page
5.3	Provisioning	236

5.3 Provisioning

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

- [Section 5.3.1, “OLT/PON Provisioning”](#) below
- [Section 5.3.2, “Service Provisioning”](#) on page 239

5.3.1 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.

5.3.1.1 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 5-1. OLT Card Service Provisioning

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

5.3.1.2 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.

1. Navigate to the Active Ethernet GE Provisioning menu.

Modules > GPON OLT > Provisioning > GE

Port	Description	Service State	Speed
Template			
☐ GE-1		IS	Auto
☐ GE-2		OOS-UAS	Auto
☐ GE-3		OOS-UAS	Auto
☐ GE-4		OOS-UAS	Auto
☐ GE-5		OOS-UAS	Auto
☐ GE-6		OOS-UAS	Auto

Figure 5-2. GE Provisioning

2. Set the port Service State to **IS** on the selected port number.
3. Click **Apply**.

What's Next

Continue to [Section 5.3.1.3, "ONT Inband Management Provisioning"](#) on page 238.

5.3.1.3 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 > GPON OLT > Provisioning > ONT

Figure 5-3. ONT Inband Management Provisioning

- 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 5-2](#) for the inband management options.

Table 5-2. 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 > GPON OLT > Status > ONT > ONT**) and check the Subtended Host check box. Scroll to the right to see the IP address.

5.3.2 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:

- [Section 5.3.2.1, "Voice"](#) Below
- [Section 5.3.2.2, "Data"](#) on page 246
- [Section 5.3.2.3, "Video"](#) on page 247

5.3.2.1 Voice

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

5.3.2.1.1 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.

5.3.2.1.2 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.

5.3.2.1.3 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.

5.3.2.1.4 Select Your Voice Option

Use [Table 5-3](#) to determine your voice option and navigate to your next step. If you're unsure of your voice option, refer to [Section 5.3.2.1, "Voice"](#) on page 239.

Table 5-3. Voice Options

Option	See Page
Section 5.3.2.1.5, "SIP OMCI Voice"	241
Section 5.3.2.1.6, "SIP Non-OMCI Voice"	242
Section 5.3.2.1.7, "MGCP OMCI Voice"	243
Section 5.3.2.1.8, "MGCP Non-OMCI Voice"	244
Section 5.3.2.1.9, "GR-303 Voice"	245

5.3.2.1.5 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.

1. [Section 5.3.3, "Create an EVC"](#) on page 248
2. [Section 5.3.4, "Set the Voice Service Mode on the ONT"](#) on page 251
3. [Section 5.3.5, "Provision the Port on the ONT"](#) on page 252
4. [Section 5.3.6, "Create an IP Host"](#) on page 256
5. [Section 5.3.7, "Create an EVC-Map"](#) on page 258
6. [Section 5.3.8, "Provision the SIP Trunk"](#) on page 263
7. [Section 5.3.11, "Provision the SIP Dialing Profile"](#) on page 267
8. [Section 5.3.16, "Provision the OMCI SIP Users"](#) on page 280

5.3.2.1.6 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.

1. [Section 5.3.3, "Create an EVC"](#) on page 248
2. [Section 5.3.4, "Set the Voice Service Mode on the ONT"](#) on page 251
3. [Section 5.3.5, "Provision the Port on the ONT"](#) on page 252
4. [Section 5.3.6, "Create an IP Host"](#) on page 256
5. [Section 5.3.7, "Create an EVC-Map"](#) on page 258
6. [Section 5.3.8, "Provision the SIP Trunk"](#) on page 263
7. [Section 5.3.11, "Provision the SIP Dialing Profile"](#) on page 267
8. [Section 5.3.13, "Provision Class of Service \(CoS\) \(Optional\)"](#) on page 277
9. [Section 5.3.14, "Provision for Global Voice \(Optional\)"](#) on page 278
10. [Section 5.3.15, "Provision the Voice User"](#) on page 279

5.3.2.1.7 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.

1. [Section 5.3.3, "Create an EVC"](#) on page 248
2. [Section 5.3.4, "Set the Voice Service Mode on the ONT"](#) on page 251
3. [Section 5.3.5, "Provision the Port on the ONT"](#) on page 252
4. [Section 5.3.6, "Create an IP Host"](#) on page 256
5. [Section 5.3.7, "Create an EVC-Map"](#) on page 258
6. [Section 5.3.9, "Provision the MGCP Profile"](#) on page 265
7. [Section 5.3.17, "Provision OMCI MGCP Endpoints"](#) on page 282

5.3.2.1.8 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.

1. [Section 5.3.3, “Create an EVC”](#) on page 248
2. [Section 5.3.4, “Set the Voice Service Mode on the ONT”](#) on page 251
3. [Section 5.3.5, “Provision the Port on the ONT”](#) on page 252
4. [Section 5.3.6, “Create an IP Host”](#) on page 256
5. [Section 5.3.7, “Create an EVC-Map”](#) on page 258
6. [Section 5.3.9, “Provision the MGCP Profile”](#) on page 265
7. [Section 5.3.10, “Provision Non-OMCI MGCP Endpoints”](#) on page 266

5.3.2.1.9 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.

1. [Section 5.3.4, "Set the Voice Service Mode on the ONT"](#) on page 251
2. [Section 5.3.5, "Provision the Port on the ONT"](#) on page 252
3. [Section 5.3.18, "Provision GR-303"](#) on page 283

5.3.2.2 Data

To provision for data, complete the following steps:



NOTE

This is a general set of instructions to turn up data.

1. [Section 5.3.3, “Create an EVC”](#) on page 248
2. [Section 5.3.5, “Provision the Port on the ONT”](#) on page 252
3. [Section 5.3.7, “Create an EVC-Map”](#) on page 258

5.3.2.3 Video

To provision for video, complete the following:

**NOTE**

This is a general set of instructions to turn up video.

1. [Section 5.3.3, “Create an EVC”](#) on page 248
2. [Section 5.3.5, “Provision the Port on the ONT”](#) on page 252
3. [Section 5.3.7, “Create an EVC-Map”](#) on page 258

5.3.3 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

The screenshot shows the 'EVC' configuration page with the 'IGMP' tab selected. At the top, there are '10' and 'Del' buttons, and 'Refresh' and 'Apply' buttons. Below this is a table with the following data:

Name	S-Tag	Admin State	Status	Switching Mode	MAC Aging Time	IGMP Priority	IGMP Version	CE-VLAN Preservation
system-management- evc	247	Enabled	Running	MAC	5	5	2	Enabled

Below the table, there is a 'Create EVC' section. It includes a 'Name' input field, a 'Retrieve' button, and a 'Create' button. The 'Operation' is set to 'Create'.

Figure 5-4. 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 ([Figure 5-5](#) on page 249) will open.

Edit EVC		
Operation	Edit	
Name	EVC Name	<i>The name of the selected EVC.</i>
Admin State	Disabled ▼	<i>Specify the admin state of the EVC</i>
S-Tag		<i>Service provider VLAN ID used to identify traffic in this EVC. Enter nothing here, or enter 'None' to remove the s-tag from this EVC.</i>
Mac Switched	☐	<i>Enable MAC switching for this EVC</i>
Double Tag Switched	☐	<i>Enable double tag switching for this EVC</i>
Preserve CE VLAN ID	☒	<i>CE-VLAN is preserved in EVC as payload</i>
Subscriber IGMP Priority	5 ▼	<i>P-bit value of IGMP packets</i>
IP IGMP Version	v2 ▼	<i>IGMP Version</i>
MEN Ports		
Interface Type	default-ethernet ▼	<i>The type of interface to add as a men port.</i>
Slot	1 ▼	<i>The slot the interface exists on.</i>
Port		<i>The item to add as a men-port.</i>
Add Remove		
Cancel Apply		

Figure 5-5. 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.

Name	Slot	Status	Proxy Host IP Address	Last Member Query Interval (ms)	Last Member Query Count	Mode
VIDEO	A	Not running, EVC does not exist	10.10.10.1	1000	2	Proxy

Create IGMP EVC

IGMP EVC Name: EVC Name : 4096 Select an existing EVC.

Slot: 1 Select a slot for connection to the IGMP EVC.

Create

Figure 5-6. 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 [Section 5.3.4, "Set the Voice Service Mode on the ONT"](#) on page 251.
- For video or data provisioning, continue to [Section 5.3.5, "Provision the Port on the ONT"](#) on page 252.

5.3.4 Set the Voice Service Mode on the ONT

1. Navigate to the ONT Provisioning menu.

Modules > GPON OLT> Provisioning > ONT

Display: ☒ Basic ☐ Level ☐ Management IP (Subtended Host)

Del	ONT	Admin State	Operational State	Description	MAC Spoofing Allowed	Advanced Encryption Standard	Part Number	Registration ID	Provisioned SN	Discovered SN	Uptime
Del	Template										
	1	IS	UP		☒ Enabled ☐ Disabled	☐ Enabled	1287781F1		ADTN150800C	ADTN150800C	0 days, 03 hours, 41 minutes, 03 seconds

Del Refresh Apply

Figure 5-7. 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](#).

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 [Section 5.3.5, "Provision the Port on the ONT"](#) on page 252.

5.3.5 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

PON: 1 ▼ ONT: 1 ▼ Port Type: Ethernet ▼

Add Del				Refresh Apply	
Port	Operational State	Service State	Description	Auto Detection Configuration	MAC Limit
▼ Template					
Add Del				Refresh Apply	

Figure 5-8. ONT Port Provisioning

- 2. Select your PON.
- 3. Select your ONT.
- 4. Select the Port Type. Use [Table 5-4](#) to determine your port type and navigate to your next step.

Table 5-4. Port Type

Service	ONT	Type	See Page
Data/Video	Non-Remote Gateway	Ethernet Port Provisioning	253
	Remote Gateway	Virtual Gigabit Interface	255
Voice	All ONTs	FXS Port Provisioning	254

5.3.5.1 Ethernet Port Provisioning

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

1. Set the number of MAC addresses allowed.

PON: ONT: Port Type:

Port	Operational State	Service State	Description	Auto Detection Configuration	MAC Limit
▼ Template					

Add Del Refresh Apply

Figure 5-9. ONT Ethernet Port Provisioning

- 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 [Section 5.3.7, "Create an EVC-Map"](#) on page 258.

5.3.5.2 FXS Port Provisioning

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

PON: ONT: Port Type:

Add		Del								Refresh	Apply
Port	Operational State	Service State	Description	Tx Gain	Rx Gain	Impedance	Service Mode	6			
☐											
☐											
Template											
Add		Del								Refresh	Apply

Figure 5-10. 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 [Section 5.3.6, “Create an IP Host”](#) on page 256.
- For GR-303 provisioning, continue to [Section 5.3.18, “Provision GR-303”](#) on page 283.

5.3.5.3 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 [Section 5.3.6, “Create an IP Host”](#) on page 256.
- For video or data provisioning, continue to [Section 5.3.7, “Create an EVC-Map”](#) on page 258.

5.3.6 Create an IP Host

- 1. Navigate to the IP Host Provisioning menu.
Modules > GPON OLT> Provisioning > IP Host

PON: ONT: Display: ☒ Last Active Error

Del	IP Host Name	Mode	IP Address	Subnet Mask	Gateway IP address	Connected Service	Connected Pseudowire Channels	Operational Status	Last Error
☐									

Note: IP-Host must have a connection to enable changing the service state.

Edit/Create

IP-Host Name

Figure 5-11. IP-Host Create Menu

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

PON: ONT: Display: ☒ Last Active Error

Del	IP Host Name	Mode	IP Address	Subnet Mask	Gateway IP address	Connected Service	Connected Pseudowire Channels	State	Last Error
☐	TEST	Static	0.0.0.0	0.0.0.0	0.0.0.0	None	None	Fields Not Set	No service/interface attached to IP-Host

Note: IP-Host must have a connection to enable changing the service state.

Edit/Create

IP Host Name **TEST**

IP Allocation

IP Address IP Allocation must be static to edit this field.

Subnet Mask IP Allocation must be static to edit this field.

Gateway IP Allocation must be static to edit this field.

State IP Host must have a connection and be allocated using DHCP or have a connection and a non-zero IP Address and Gateway IP to set service state

Create IP Host Connection

Connection Type

Channel Number

Del	TEST IP Host Connections		
Connection	Service/Interface	Channel	Status
☐			

Figure 5-12. 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 [Section 5.3.7, "Create an EVC-Map"](#) on page 258.

5.3.7 Create an EVC-Map

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

- 1. Access the Interface Map.

Modules > GPON OLT > Provisioning > Interface Map

Del

Refresh

Apply

☐	Name	Subscriber Interface	EVC Name	EVC S-Tag	C-Tag	Service State	Status	2
Del								

Create/Edit

Map Name

Case sensitive search for Interface Map by name.

Edit

Create

Figure 5-13. EVC-Map Create

- 2. Enter the new EVC-Map name into the Map Name field and click the Create button. See [Figure 5-14](#) on page 259.



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.

Edit Interface Map		
Operation	Edit	
Map Name	EVC-Map Example	<i>A user-specified name meant to identify the et</i>
Description		<i>A user-specified description of the flow.</i>
Service State	Not Ready ▼	
Status	Disabled	
Subscriber Interface		
Interface Type	Gigabit-Ethernet ▼	<i>Type is required to create a new map.</i>
PON	1 ▼	<i>PON number.</i>
ONT	1 ▼	<i>ONT number.</i>
ONT Port	1 ▼	<i>ONT port number.</i>
Upstream Channel	None ▼	<i>Upstream channel number.</i>
VLAN Configuration		
EVC Name	None ▼	<i>EVC 'Name:S-Tag', Ethernet Virtual Connection sidebar Services EVCs page.</i>
S-Tag Priority	Marked ▼	0 ▼
C-Tag	None ▼	<i>Customer Tag - the inner tag attached to all up this EVC Map. If EVC preserve CE-VLAN ID is e be set to None.</i>
C-Tag Priority	Marked ▼	0 ▼
Authentication Configuration		
DHCP Processing	Authenticate ▼	<i>Set the DHCPv4 processing mode. Authenticate authentication, Block - block DHCP, Transpare Process DHCP without performing authenticatio</i>
DHCPv6 Processing	Same As DHCPv4 ▼	<i>Set the DHCPv6 processing mode. Authenticate subscriber authentication, Block - block DHCPv DHCPv6, Same As DHCPv4 - Use same mode c provisioned on DHCPv4</i>
PPPoE Processing	Authenticate ▼	<i>Set the PPPoE processing mode. Authenticate authentication, Block - block PPPoE, Transpare</i>
Advanced Configuration		
Show Advanced	Advanced	<i>Selecting button will toggle the display of the A</i>
IGMP		
Show IGMP	IGMP	<i>Selecting button will toggle the display of the I</i>
Cancel Apply		

Figure 5-14. EVC-Map Edit

- Set the Service State to **Active**.
- Select the Interface Type. Use [Table 5-5](#) on page 260 to determine the type and the steps to complete.

Table 5-5. 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 5-6](#) to determine the authentication and steps required.

**NOTE**

PPPoE does not support video services.

Table 5-6. 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**.

Matching Criteria	
CE-VLAN	Tagged or Untagged Match on a specific customer tag by choosing the tag id. To match on untagged traffic, choose 'None'. To match all traffic, choose 'Tagged or Untagged'.
P-Bit	4 5 6 7 Customer Ingress P-Bit matching criteria. Hold Ctrl or Shift to select multiple P-Bit Values.
Network P-Bit	4 5 6 7 Network Ingress P-Bit matching criteria. Hold Ctrl or Shift to select multiple P-Bit values.
DSCP List	Customer Ingress Differentiated Services Code Point in matching criteria. List (12, 18, 27), Range (7-19), or Combination (1-6, 8, 12-19).
Multicast	☐ Enabled Include multicast traffic in matching criteria.

Figure 5-15. 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**.

IGMP	
Show IGMP	Hide IGMP Selecting button will toggle the display of the IGMP configuration.
IGMP Authentication	Enable Enable/disable authentication of source MAC addresses used in IGMP messages. The default is Enable, which requires source MAC addresses of the IGMP messages to have been authenticated using another protocol. When disabled, the IGMP messages will be processed regardless of the source MAC address.
IGMP Mode	Block The IGMP Mode associated with each EVC map. Processing Enabled - process IGMP messages based on provisioned IGMP mode on the EVC, Block - discard all IGMP messages, Transparent - Pass IGMP messages transparently, Forking - Copy upstream IGMP messages from the Video Map to this Map.
Router IP	0 . 0 . 0 . 0 The source IP address that the DSLAM places in IGMP messages destined for the subscriber. This value only applies when IGMP is in proxy mode.
Multicast Bandwidth	0 ☐ Enabled Maximum downstream bandwidth(Kbps) available for this map. Joins for the subscriber's multicast streams are checked to not exceed this bandwidth when enabled.
Multicast Groups	6 ☐ Enabled Maximum multicast groups allowed for this map. Joins for the subscriber's multicast streams are checked to not exceed this maximum when enabled.
Immediate Leave	Disabled Enable/disable smart immediate leave. Disable is the equivalent of setting Last Member Query Count to 0.
Cancel Apply	

Figure 5-16. 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 [Section 5.3.8, “Provision the SIP Trunk”](#) on page 263.
- For OMCI MGCP and Non-OMCI MGCP provisioning, continue to [Section 5.3.9, “Provision the MGCP Profile”](#) on page 265.
- For remote gateway ONT video or data provisioning, continue to [Section 5.3.2, “Service Provisioning”](#) on page 239.
- For non-remote gateway ONT video or data provisioning, this completes provisioning. Services should be up and running. To provision another service, continue to [Section 5.3.2, “Service Provisioning”](#) on page 239.

5.3.8 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 (see [Figure 5-17](#) on page 263).

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

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

Trunk	
Trunk Name	Trunk's 2 digit identifier following T. ex. T01
Primary Proxy	IP address or host name of the primary proxy server.
Primary Proxy Port	UDP port number of primary proxy server: 1 - 65535.
Secondary Proxy	IP address or host name of the secondary proxy server.
Secondary Proxy Port	UDP port number of secondary proxy server: 1 - 65535.
Outbound Primary Proxy	IP address or host name of the primary outbound proxy server.
Outbound Primary Proxy Port	UDP port number of primary outbound proxy server: 1 - 65535.
Outbound Secondary Proxy	IP address or host name of the secondary outbound proxy server.
Outbound Secondary Proxy Port	UDP port number of secondary outbound proxy server: 1 - 65535.
Primary Registrar	IP address or host name of the primary registrar.
Primary Registrar Port	UDP port number of primary registrar: 1 - 65535.
Secondary Registrar	IP address or host name of the secondary registrar.
Secondary Registrar Port	UDP port number of secondary registrar: 1 - 65535.
Maximum Registrations	Maximum concurrent registrations: 1-32.
Registrar Expiration Time	Expiration time in seconds: 30-2147483647.
Require Expiration Header	☐ Enabled
Domain	Domain Name.
Dial-string Source	Request URI Use to specify the dial-string source for the SIP server.
Keep alive method	None The keep-alive method to use for SIP registrar connections.
Keep alive interval	Interval in seconds: 30 - 3600.
Registration-failure Retry Timer	Retry time in seconds: 10 - 604800.
Rollover Timer	Time to wait before rolling over to next server: seconds 1-32.
Request URI Resolution	☐ Enabled Enables the local unit to resolve the domain before resolving the request uniform resource identifier (URI).
Request URI Host Format	Domain Used to format the Request uniform resource identifier (URI) for SIP messages.
From Header Format	Domain Specifies the Host field formatting for the From header.
To Header Format	Domain Used to configure the To header host format of SIP trunk messages.
Alert Information URL	Specifies the Alert-Info HyperText Transfer Protocol (HTTP) universal resource locator (URL) header format.
Require 100rel	☐ Enabled Include 100rel in Require Header.
Support 100rel	☐ Enabled Include 100rel in Support Header.
User-agent	Default Used to configure the To header host format of SIP trunk messages.
User Supplied agent	Used if User-agent is set to User Supplied. Maximum of 128 characters.
SIP Authentication	☐ Enable SIP Server authentication
SIP DSCP	Differentiated Services Code Point for SIP packets: 0 - 63.
RTP DSCP	Differentiated Services Code Point for RTP packets: 0 - 63.
Trust Domain	☐ This Trunk is connected to a trust domain
P-Asserted-Identity required	☐ A P-Asserted-Identity header is required for this trust domain
Apply Cancel	

Figure 5-17. 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 [Section 5.3.11, "Provision the SIP Dialing Profile"](#) on page 267.

5.3.9 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 [Section 5.3.17, “Provision OMCI MGCP Endpoints”](#) on page 282.
- For Non-OMCI MGCP provisioning, continue to [Section 5.3.10, “Provision Non-OMCI MGCP Endpoints”](#) on page 266.

5.3.10 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 [Section 5.3.2, "Service Provisioning"](#) on page 239.

5.3.11 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.

5.3.11.1 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`

5.3.11.2 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**

5.3.11.3 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 (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**

5.3.11.4 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**

The screenshot displays the 'Dialing Profiles' configuration page. At the top, there are tabs for 'Trunk', 'Users', and 'Dialing Profiles'. Below these, a 'Profile:' dropdown is set to 'DEFAULT_DP', with a 'Del' button and an 'Add New Profile:' field with an 'Add' button. A 'Profile Description:' field with an 'Apply' button is also present. The 'Dial Plan' tab is selected, showing sub-tabs for 'Special Prefix', 'External Line Code', and 'Summary'. A table lists existing dial plans with columns for 'Dial Plan Pattern', 'Dial Plan Type', 'Emergency Number', and 'External Line Code'. Below the table, the 'Create Dial Plan' section includes fields for 'Dial Plan Type' (set to 'Always Permitted'), 'Emergency Number' (checkbox 'Enabled'), 'External Line Code' (dropdown 'Optional'), and 'Dial Plan Pattern' (text input). Instructions and a hint are provided for each field.

Figure 5-18. 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 [Section 5.3.12, “Provision the Common Profiles \(Optional\)”](#) on page 272.
- For Non-OMCI SIP provisioning, continue to [Section 5.3.13, “Provision Class of Service \(CoS\) \(Optional\)”](#) on page 277.

5.3.12 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 [Section 5.3.16, "Provision the OMCI SIP Users"](#) on page 280.

Refer to [Table 5-7](#) for a list of the supported profiles.

Table 5-7. Common Profiles

Profile	Support	See Page
Call Feature	SIP	272
Media	SIP/MGCP	274
Codec	SIP/MGCP	276

5.3.12.1 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 5-8](#) for a list of call feature options.

Table 5-8. 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 outbound caller ID from this endpoint.

Table 5-8. Call Feature Profile Options (Continued)

Option	Description
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.
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 [Section 5.3.12.2, "Provision the Media Profile"](#) on page 274.

5.3.12.2 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 5-9](#) for a list of media profile options.

Table 5-9. 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 5-9. 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 [Section 5.3.12.3, "Provision the Codec Profile"](#) on page 276.

5.3.12.3 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 5-10](#) for a list of CODEC options.

Table 5-10. 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 [Section 5.3.16, "Provision the OMCI SIP Users"](#) on page 280.
- For OMCI MGCP continue to [Section 5.3.17, "Provision OMCI MGCP Endpoints"](#) on page 282.

5.3.13 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 be 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](#).

5. Click **Apply**.



What's Next

Continue to [Section 5.3.14, "Provision for Global Voice \(Optional\)"](#) on page 278.

5.3.14 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](#).



What's Next

Continue to [Section 5.3.15, "Provision the Voice User"](#) on page 279.

5.3.15 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 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>.

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 [Section 5.3.2, "Service Provisioning"](#) on page 239.

5.3.16 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

Trunk **Users** Dialing Profiles

Filter By: Slot: Pon/AE Port: Ont:

4	Del	Refresh				
User Index	Identity	FXS Port	Oper Status	Reg State	Codec In Use	2
4	Del	Refresh				

Create/Edit Centralized User

Slot		Slot(1-22).
GPON/AE PORT		GPON PORT(1-8)/AE PORT(1-24).
ONT		GPON ONT(1-64)/AE ONT(1).
Identifier		Endpoint Index(1-10).

Figure 5-19. SIP User Create

2. Enter the slot number.
3. Enter the GPON/GPON OLT port.
4. Enter the ONT.
5. Enter a unique identifier number.
6. Click **Create**. The provision SIP User menu appears (see [Figure 5-20](#) on page 281).

Provision SIP User		
Endpoint Index		
Endpoint Index	1/0/1@1/1/1	
Description		<i>A description of this voice user. Maximum of 20 characters.</i>
Identity		<i>SIP identity</i>
Trunk		<i>Trunk's 2 digit identifier following T. ex. T01</i>
Username		<i>Username for authentication to SIP server</i>
Password		<i>Password for authentication to SIP server</i>
Dialing Plan Profile		<i>Dialing Plan Profile used with this voice user</i>
Codec List Profile		<i>Codec Profile used with this voice user</i>
Media Profile		<i>Media Profile used with this voice user</i>
Call Feature Profile		<i>Call Feature Profile used with this voice user</i>
FXS Port	v	<i>FXS port connected to this voice user</i>
Service State	Active	
Oper Status	DOWN	
Last Error	Voice user not connected to valid FXS port	
Cancel Apply		

Figure 5-20. 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 Dialing 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 [Section 5.3.2, "Service Provisioning"](#) on page 239.

5.3.17 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/GPON OLT 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 [Section 5.3.2, "Service Provisioning"](#) on page 239.

5.3.18 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 [Section 5.3.2, "Service Provisioning"](#) on page 239.

6 GPON Configurations

6.1 Scope of this Section

This section provides examples of common Total Access 5000 GPON configurations.



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.

6.2 In this Section

This section contains the topics listed in [Table 6-1](#).

Table 6-1. Section 6 Topics

Sub-Section	Topic	See Page
6.3	TLS Configuration Examples	304

6.3 VLAN/TLS/IPTV Examples

This section includes provisioning examples for the following:

- [Section 6.3.1, “1:1 Customer VLAN \(C-VLAN\) Examples”](#) on page 287
- [Section 6.3.2, “N:1 Service VLAN \(S-VLAN\) Examples”](#) on page 290
- [Section 6.3.3, “Hybrid N+1:1 Combined VLAN Examples”](#) on page 297
- [Section 6.4.1, “TLS Example 1”](#) on page 304
- [Section 6.4.2, “TLS Example 2”](#) on page 305
- [Section 6.4.3, “IPTV Configuration Examples”](#) on page 307

6.3.1 1:1 Customer VLAN (C-VLAN) Examples

The following configuration examples provision a Total Access 5000 with a 1:1 Customer VLAN (C-VLAN) model. The C-VLAN model creates a VLAN for each subscriber. All services (Data, Video, etc.) provided to the customer are carried on the same VLAN. The number of VLANs required is equal to the number of subscribers serviced.

An advantage of the C-VLAN model is security. Each subscriber is isolated from other subscribers on separate VLANs. Another advantage is the similarity to older ATM based configurations. The main disadvantage of the C-VLAN model is the lack of multicast replication. A separate copy of each multicast stream must be sent to the Total Access 5000 for each user requesting it. These copies inefficiently use uplink bandwidth, thus limiting the size of the subscriber base for each Total Access 5000.

Figure 6-1 illustrates a 1:1 Customer VLAN model inside a Total Access 5000. When provisioning a C-VLAN each VLAN requires an EVC and an EVC Map to connect the EVC to the correct UNI port.

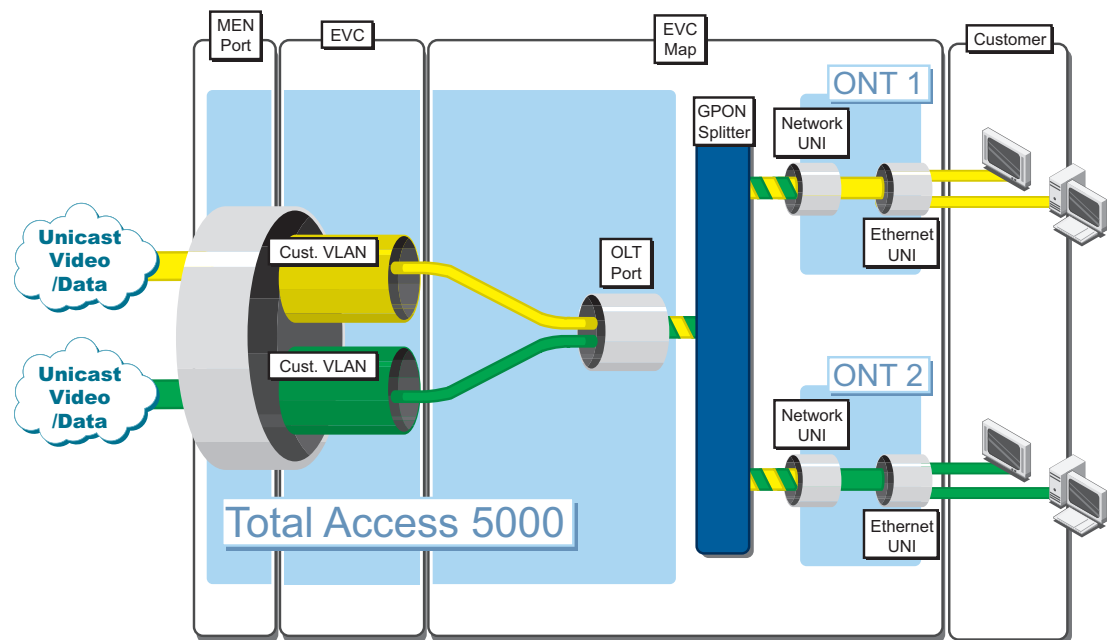


Figure 6-1. 1:1 Customer VLAN Diagram

The following examples configure a Total Access 5000 with a 1:1 Customer VLAN model and the following attributes:

GPON application with a DHCP Subscriber Authentication with Option 82 Subscriber Protocol

6.3.1.1 Example 1:1 Example

1. Create an EVC for each customer

```
ChassisID#configure terminal
ChassisID(config)#evc CUST1_EVC
ChassisID(config-evc CUST1EVC)#s-tag 100
ChassisID(config-evc CUST1EVC)#double-tag-switched
ChassisID(config-evc CUST1EVC)#connect men-port default-ethernet
ChassisID(config-evc CUST1EVC)#no preserve-ce-vlan
ChassisID(config-evc CUST1EVC)#no shutdown
ChassisID(config-evc CUST1EVC)#exit
ChassisID(config)#exit

ChassisID#configure terminal
ChassisID(config)#evc CUST2_EVC
ChassisID(config-evc CUST2EVC)#s-tag 200
ChassisID(config-evc CUST2EVC)#double-tag-switched
ChassisID(config-evc CUST2EVC)#connect men-port default-ethernet
ChassisID(config-evc CUST2EVC)#no preserve-ce-vlan
ChassisID(config-evc CUST2EVC)#no shutdown
ChassisID(config-evc CUST2EVC)#exit
ChassisID(config)#exit
```

2. Create an EVC Map per customer (ONT).

The example shows the provisioning of 2 ONTs.

PON 1, ONT ID 1, ONT port 1

```
ChassisID(config)#evc-map MAP_CUST1 1/5
ChassisID(config-evc-map MAP_CUST1 1/5)#connect uni gigabit-ethernet 1/
0/1@1/5/1
ChassisID(config-evc-map MAP_CUST1 1/5)#connect evc CUST1_EVC
ChassisID(config-evc-map MAP_CUST1 1/5)#men-pri 0
ChassisID(config-evc-map MAP_CUST1 1/5)#subscriber access dhcp mode
block
ChassisID(config-evc-map MAP_CUST1 1/5)#subscriber igmp mode block
ChassisID(config-evc-map MAP_CUST1 1/5)#subscriber access pppoe mode
block
ChassisID(config-evc-map MAP_CUST1 1/5)#subscriber access static-ip
1.2.3.3 00:01:02:03:04:05 1.2.3.254 00:01:02:00:00:00
ChassisID(config-evc-map MAP_CUST1 1/5)#subscriber arp mode proxy
ChassisID(config-evc-map MAP_CUST1 1/5)#no shutdown
ChassisID(config-evc-map MAP_CUST1 1/5)#exit
```

PON 2, ONT ID 1, ONT port 1

```
ChassisID(config)#evc-map MAP_CUST2 1/5
ChassisID(config-evc-map MAP_CUST2 1/5)#connect uni gigabit-ethernet 1/
0/1@1/5/2
ChassisID(config-evc-map MAP_CUST2 1/5)#connect evc CUST2_EVC
ChassisID(config-evc-map MAP_CUST2 1/5)#men-pri 0
ChassisID(config-evc-map MAP_CUST2 1/5)#subscriber access dhcp mode
block
ChassisID(config-evc-map MAP_CUST2 1/5)#subscriber igmp mode block
ChassisID(config-evc-map MAP_CUST2 1/5)#subscriber access pppoe mode
block
```

```
ChassisID(config-evc-map MAP_CUST2 1/5)#subscriber access static-ip  
1.2.3.4 00:01:02:03:04:06 1.2.3.254 00:01:02:00:00:00  
ChassisID(config-evc-map MAP_CUST2 1/5)#subscriber arp mode proxy  
ChassisID(config-evc-map MAP_CUST2 1/5)#no shutdown  
ChassisID(config-evc-map MAP_CUST2 1/5)#exit
```

6.3.2 N:1 Service VLAN (S-VLAN) Examples

The following configuration examples provision a Total Access 5000 with a N:1 Service VLAN model. The N:1 Service VLAN model creates one VLAN for each provided service (Data, Video, etc.). This service VLAN is shared by multiple (N) subscribers.

The N:1 Service VLAN model allows for the replication of multicast traffic to multiple users. This replication makes more efficient use of uplink bandwidth. The N:1 Service VLAN model may also have advantages when adding video to an existing network, as the addition of a video VLAN will not disrupt the existing data VLAN. A disadvantage of this model is that the Total Access 5000 must provide additional security as the subscribers are not on isolated VLANs.

Figure 6-2 illustrates a N:1 Service VLAN model inside a Total Access 5000. When provisioning a S-VLAN each VLAN requires an EVC and an EVC Map to connect the EVC to the each required UNI port. Therefore each UNI port will have one EVC Map for each service passing through it.

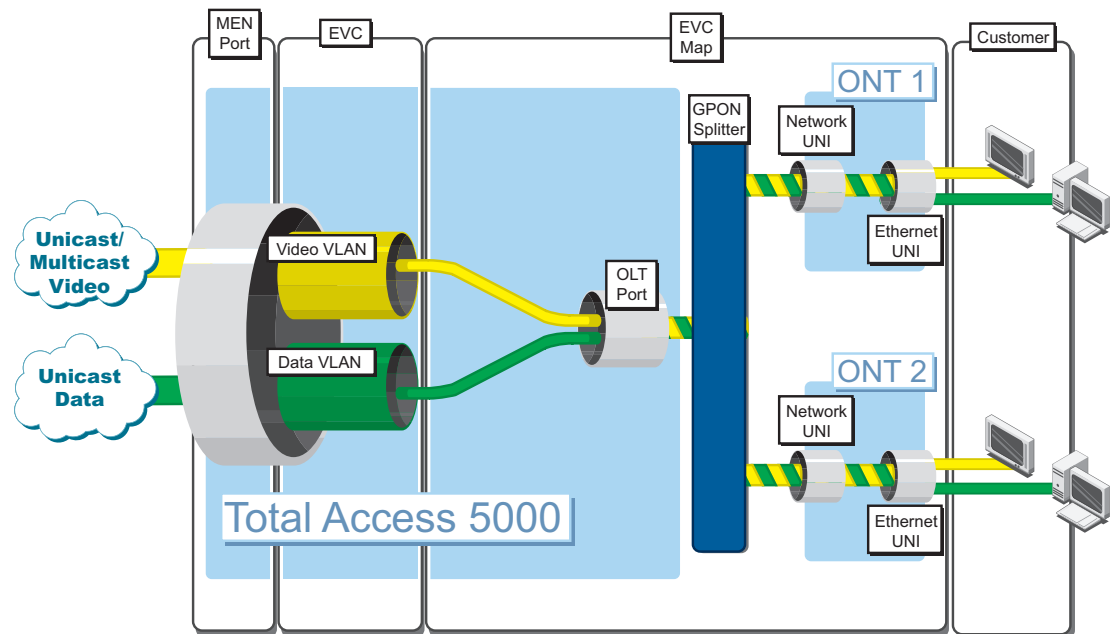


Figure 6-2. N:1 Service VLAN Diagram

6.3.2.1 N:1 Service VLAN Example 1

This example displays data and video on the same port.

1. Create an EVC for each service.

```
ChassisID#configure terminal
ChassisID(config)#evc DATA_EVC
ChassisID(config-evc DATA_EVC)#s-tag 101
ChassisID(config-evc DATA_EVC)#connect men-port default-ethernet
ChassisID(config-evc DATA_EVC)#mac-switched
ChassisID(config-evc DATA_EVC)#no preserve-ce-vlan
ChassisID(config-evc DATA_EVC)#no shutdown
ChassisID(config-evc DATA_EVC)#exit

ChassisID(config)#evc VIDEO_EVC
ChassisID(config-evc VIDEO_EVC)#s-tag 1001
ChassisID(config-evc VIDEO_EVC)#connect men-port default-ethernet
ChassisID(config-evc VIDEO_EVC)#no preserve-ce-vlan
ChassisID(config-evc VIDEO_EVC)#subscriber igmp priority 3
ChassisID(config-evc VIDEO_EVC)#no shutdown
ChassisID(config-evc VIDEO_EVC)#exit
```

2. Set up per-EVC, per-slot IGMP settings on both GPON and switch modules. The IGMP proxy mode used in this example.

```
ChassisID(config)#ip igmp evc VIDEO_EVC 1/5 mode proxy
ChassisID(config)#ip igmp evc VIDEO_EVC 1/5 proxy host ip address
10.20.200.1
ChassisID(config)#ip igmp evc VIDEO_EVC 1/5 proxy last-member-query
count 2
ChassisID(config)#ip igmp evc VIDEO_EVC 1/5 proxy last-member-query
interval 1000

ChassisID(config)#ip igmp evc VIDEO_EVC 1/A mode proxy
ChassisID(config)#ip igmp evc VIDEO_EVC 1/A proxy host ip address
10.20.200.1
ChassisID(config)#ip igmp evc VIDEO_EVC 1/A proxy last-member-query
count 2
ChassisID(config)#ip igmp evc VIDEO_EVC 1/A proxy last-member-query
interval 1000
```

3. Create an EVC Map per customer (ONT) for each service. Use the set-top box MAC address to distinguish its traffic.

- a. Create the video EVC Maps.

PON 1, ONT ID 1, ONT port 1, match set-top box

```
ChassisID(config)#evc-map VIDEO_MAP_CUST1 1/5
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#connect uni gigabit-
ethernet 1/0/1@1/5/1
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#connect evc VIDEO_EVC
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#men-pri 3
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#match source mac-
address 00:02:02:00:00:00 ff:ff:ff:00:00:00
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#match untagged
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber igmp mode
processing-enabled
```

```
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber igmp
immediate-leave
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber igmp proxy
router ip address 10.20.200.2
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber access
dhcp mode authenticate
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber access
pppoe mode block
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber arp mode
proxy
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber access
dhcp option-82
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber access
dhcp option-82 remote-id
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#description
REMI_VIDEO_CUST1
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#no shutdown
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#exit
```

PON 1, ONT ID 2, ONT port 1, match set-top box

```
ChassisID(config)#evc-map VIDEO_MAP_CUST2 1/5
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#connect uni gigabit-
ethernet 2/0/1@1/5/1
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#connect evc VIDEO_EVC
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#men-pri 3
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#match source mac-
address 00:02:02:00:00:00 ff:ff:ff:00:00:00
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#match untagged mac-
address 00:02:02:00:00:00 ff:ff:ff:00:00:00
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber igmp mode
processing-enabled
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber igmp
immediate-leave
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber igmp proxy
router ip address 10.20.200.2
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber access
dhcp mode authenticate
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber access
pppoe mode block
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber arp mode
proxy
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber access
dhcp option-82
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber access
dhcp option-82 remote-id
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#description
REMI_VIDEO_CUST2
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#no shutdown
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#exit
```

- b. Create the data EVC Maps.

PON 1, ONT ID 1, ONT port 1, match all other

```
ChassisID(config)#evc-map DATA_MAP_CUST1 1/5
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#connect uni gigabit-
ethernet 1/0/1@1/5/1
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#connect evc DATA_EVC
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#men-pri 0
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access dhcp
mode authenticate
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber igmp mode
block
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access
pppoe mode block
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber arp mode
proxy
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access dhcp
option-82
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access dhcp
option-82 remote-id
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#description
REMI_DATA_CUST1
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#no shutdown
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#exit
```

PON 1, ONT ID 2, ONT port 1, match all other

```
ChassisID(config)#evc-map DATA_MAP_CUST2 1/5
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#connect uni gigabit-
ethernet 2/0/1@1/5/1
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#connect evc DATA_EVC
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#men-pri 0
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access dhcp
mode authenticate
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber igmp mode
block
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access
pppoe mode block
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber arp mode
proxy
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access dhcp
option-82
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access dhcp
option-82 remote-id
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#description
REMI_DATA_CUST2
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#no shutdown
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#exit
```

6.3.2.2 N:1 Service VLAN Example 2

This example displays data and video on different ONT ports.

1. Create an EVC for each service.

```
ChassisID#configure terminal
ChassisID(config)#evc DATA_EVC
ChassisID(config-evc DATA_EVC)#s-tag 101
ChassisID(config-evc DATA_EVC)#connect men-port default-ethernet
ChassisID(config-evc DATA_EVC)#mac-switched
ChassisID(config-evc DATA_EVC)#no preserve-ce-vlan
ChassisID(config-evc DATA_EVC)#no shutdown
ChassisID(config-evc DATA_EVC)#exit

ChassisID(config)#evc VIDEO_EVC
ChassisID(config-evc VIDEO_EVC)#s-tag 1001
ChassisID(config-evc VIDEO_EVC)#connect men-port default-ethernet
ChassisID(config-evc VIDEO_EVC)#no preserve-ce-vlan
ChassisID(config-evc VIDEO_EVC)#subscriber igmp priority 3
ChassisID(config-evc VIDEO_EVC)#no shutdown
ChassisID(config-evc VIDEO_EVC)#exit
```

2. Set up per-EVC, per-slot IGMP settings on both GPON and switch modules. The IGMP snooping mode used in this example.

```
ChassisID(config)#ip igmp evc VIDEO_EVC 1/5 mode snooping
ChassisID(config)#ip igmp evc VIDEO_EVC 1/5 proxy last-member-query
count 2
ChassisID(config)#ip igmp evc VIDEO_EVC 1/5 proxy last-member-query
interval 1000
ChassisID(config)#ip igmp evc VIDEO_EVC 1/A mode snooping
ChassisID(config)#ip igmp evc VIDEO_EVC 1/A proxy last-member-query
count 2
ChassisID(config)#ip igmp evc VIDEO_EVC 1/A proxy last-member-query
interval 1000
```

3. Create an EVC Map per customer (ONT) for each service.

These examples show DHCP authentication for video and PPPoE authentication for data.

- a. Create the video EVC Maps.

PON 1, ONT ID 1, ONT port 2

```
ChassisID(config)#evc-map VIDEO_MAP_CUST1 1/5
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#connect uni gigabit-
ethernet 1/0/2@1/5/1
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#connect evc VIDEO_EVC
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#men-pri 3
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber igmp mode
processing-enabled
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber igmp
immediate-leave
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber access
dhcp mode authenticate
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber access
pppoe mode block
```

```

ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber arp mode
proxy
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber access
dhcp option-82
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber access
dhcp option-82 remote-id
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#description
REMID_VIDEO_CUST1
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#no shutdown
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#exit

```

PON 1, ONT ID 2, ONT port 2

```

ChassisID(config)#evc-map VIDEO_MAP_CUST2 1/5
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#connect uni gigabit-
ethernet 2/0/2@1/5/1
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#connect evc VIDEO_EVC
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#men-pri 3
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber igmp mode
processing-enabled
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber igmp
immediate-leave
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber access
dhcp mode authenticate
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber access
pppoe mode block
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber arp mode
proxy
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber access
dhcp option-82
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber access
dhcp option-82 remote-id
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#description
REMID_VIDEO_CUST2
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#no shutdown
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#exit

```

b. Create the data EVC Maps.

These examples show the addition of a customer-specific C-tag toward the network.

PON 1, ONT ID 1, ONT port 1

```

ChassisID(config)#evc-map DATA_MAP_CUST1 1/5
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#connect uni gigabit-
ethernet 1/0/1@1/5/1
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#connect evc DATA_EVC
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#men-pri 0
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#men-c-tag 101
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access dhcp
mode block
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber igmp mode
block
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access
pppoe mode authenticate
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber arp mode
proxy

```

```
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access
pppoe intermediate-agent
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access
pppoe intermediate-agent remote-id
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#description
REMIID_DATA_CUST1
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#no shutdown
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#exit
```

PON 1, ONT ID 2, ONT port 1

```
ChassisID(config)#evc-map DATA_MAP_CUST2 1/5
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#connect uni gigabit-
ethernet 2/0/1@1/5/1
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#connect evc DATA_EVC
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#men-pri 0
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#men-c-tag 102
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access dhcp
mode block
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber igmp mode
block
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access
pppoe mode authenticate
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber arp mode
proxy
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access
pppoe intermediate-agent
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access
pppoe intermediate-agent remote-id
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#description
REMIID_DATA_CUST2
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#no shutdown
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#exit
```

6.3.3 Hybrid N+1:1 Combined VLAN Examples

The following configuration examples provision a Total Access 5000 with a Hybrid N+1:1 VLAN (Combined VLAN) model. The Combined VLAN model creates a VLAN for each subscriber that handles data and unicast video traffic. A separate shared VLAN is created for multicast video and IGMP traffic, this allows for multicast replication. The number of VLANs required is equal to the number of subscribers serviced plus one, (N+1:1).

This model provides all of the advantages of the C-VLAN, (i.e. security, simplified operations, etc.) while removing its biggest disadvantage, no multicast replication.

Figure 6-3 illustrates a Hybrid N+1:1 VLAN model inside a Total Access 5000. When provisioning a Combined VLAN each VLAN requires an EVC and an EVC Map to connect the EVC to the each required UNI port. Therefore each UNI port will have one EVC Map for Unicast and Data and another for Multicast.

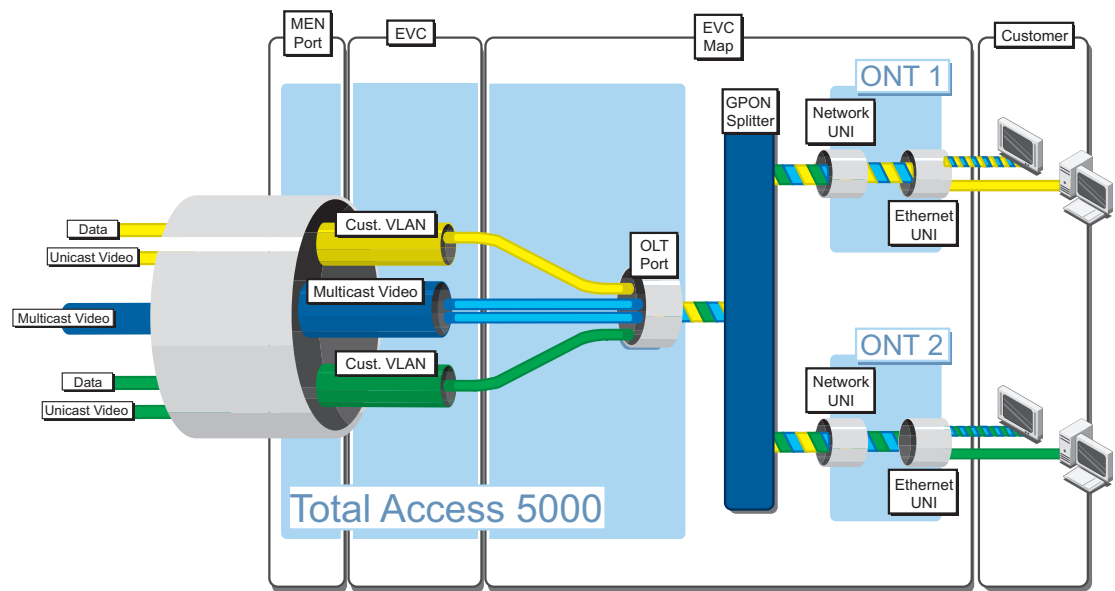


Figure 6-3. Hybrid N+1:1 Combined VLAN Diagram

The following examples configure a Total Access 5000 with a Hybrid N+1:1 VLAN model and the following attributes: GPON application with a redundant GE uplink and DHCP Subscriber Authentication

6.3.3.1 Hybrid N+1:1 Example 1

This example shows a 1:1 customer VLAN with multicat replication (Hybrid/Split VLAN).

1. Create an EVC for each customer and a single EVC for video.

```
ChassisID#configure terminal
ChassisID(config)#evc CUST1_EVC
ChassisID(config-evc CUST1_EVC)#s-tag 100
ChassisID(config-evc CUST1_EVC)#mac-switched
ChassisID(config-evc CUST1_EVC)#connect men-port default-ethernet
ChassisID(config-evc CUST1_EVC)#no preserve-ce-vlan
ChassisID(config-evc CUST1_EVC)#no shutdown
ChassisID(config-evc CUST1_EVC)#exit
ChassisID(config)#exit
```

```
ChassisID#configure terminal
ChassisID(config)#evc CUST2_EVC
ChassisID(config-evc CUST2_EVC)#s-tag 200
ChassisID(config-evc CUST2_EVC)#mac-switched
ChassisID(config-evc CUST2_EVC)#connect men-port default-ethernet
ChassisID(config-evc CUST2_EVC)#no preserve-ce-vlan
ChassisID(config-evc CUST2_EVC)#no shutdown
ChassisID(config-evc CUST2_EVC)#exit
ChassisID(config)#exit
```

```
ChassisID(config)#evc VIDEO_EVC
ChassisID(config-evc VIDEO_EVC)#s-tag 1001
ChassisID(config-evc VIDEO_EVC)#connect men-port default-ethernet
ChassisID(config-evc VIDEO_EVC)#no preserve-ce-vlan
ChassisID(config-evc VIDEO_EVC)#subscriber igmp priority 3
ChassisID(config-evc VIDEO_EVC)#no shutdown
ChassisID(config-evc VIDEO_EVC)#exit
```

2. Set up per-EVC, per-slot IGMP settings on both GPON and switch modules. The IGMP proxy mode used in this example.

```
ChassisID(config)#ip igmp evc VIDEO_EVC 1/5 mode proxy
ChassisID(config)#ip igmp evc VIDEO_EVC 1/5 proxy host ip address
10.20.200.1
ChassisID(config)#ip igmp evc VIDEO_EVC 1/5 proxy last-member-query
count 2
ChassisID(config)#ip igmp evc VIDEO_EVC 1/5 proxy last-member-query
interval 1000

ChassisID(config)#ip igmp evc VIDEO_EVC 1/A mode proxy
ChassisID(config)#ip igmp evc VIDEO_EVC 1/A proxy host ip address
10.20.200.1
ChassisID(config)#ip igmp evc VIDEO_EVC 1/A proxy last-member-query
count 2
ChassisID(config)#ip igmp evc VIDEO_EVC 1/A proxy last-member-query
interval 1000
```

3. Create an EVC Map per customer (ONT) for each service.

These examples show DHCP authentication.

PON 1, ONT ID 1, ONT port 1, match multicast traffic

```
ChassisID(config)#evc-map VIDEO_MAP_CUST1 1/5
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#connect uni gigabit-
ethernet 1/0/1@1/5/1
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#connect evc VIDEO_EVC
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#men-pri 3
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#match multicast
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber igmp mode
processing-enabled
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access dhcp
mode block
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber igmp
immediate-leave
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber igmp proxy
router ip address 10.20.200.2
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#no shutdown
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#exit
```

PON 1, ONT ID 2, ONT port 1, match multicast traffic

```
ChassisID(config)#evc-map VIDEO_MAP_CUST2 1/5
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#connect uni gigabit-
ethernet 2/0/1@1/5/1
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#connect evc VIDEO_EVC
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#men-pri 3
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#match multicast
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber igmp mode
processing-enabled
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access dhcp
mode block
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber igmp
immediate-leave
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber igmp proxy
router ip address 10.20.200.2
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#no shutdown
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#exit
```

PON 1, ONT ID 1, ONT port 1, match all other

```
ChassisID(config)#evc-map DATA_MAP_CUST1 1/5
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#connect uni gigabit-
ethernet 1/0/1@1/5/1
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#connect evc CUST1_EVC
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#men-pri 0
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access dhcp
mode authenticate
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber igmp mode block
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access pppoe
mode block
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber arp mode proxy
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access dhcp
option-82
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access dhcp
option-82 remote-id
```

```
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#description  
REMID_DATA_CUST1
```

```
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#no shutdown
```

```
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#exit
```

PON 1, ONT ID 2, ONT port 1, match all other

```
ChassisID(config)#evc-map DATA_MAP_CUST2 1/5
```

```
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#connect uni gigabit-  
ethernet 2/0/1@1/5/1
```

```
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#connect evc CUST2_EVC
```

```
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#men-pri 0
```

```
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access dhcp  
mode authenticate
```

```
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber igmp mode block
```

```
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access pppoe  
mode block
```

```
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber arp mode proxy
```

```
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access dhcp
```

```
option-82
```

```
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access dhcp
```

```
option-82 remote-id
```

```
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#description
```

```
REMID_DATA_CUST2
```

```
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#no shutdown
```

```
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#exit
```

6.3.3.2 Hybrid N+1:1 Example 2

This example shows N:1 service VLANs for data and Hybrid/Split VLAN for video.

1. Create an EVC each for data and video.

```
ChassisID#configure terminal
ChassisID(config)#evc DATA_EVC
ChassisID(config-evc DATA_EVC)#s-tag 101
ChassisID(config-evc DATA_EVC)#connect men-port default-ethernet
ChassisID(config-evc DATA_EVC)#mac-switched
ChassisID(config-evc DATA_EVC)#no preserve-ce-vlan
ChassisID(config-evc DATA_EVC)#no shutdown
ChassisID(config-evc DATA_EVC)#exit

ChassisID(config)#evc VIDEO_EVC
ChassisID(config-evc VIDEO_EVC)#s-tag 1001
ChassisID(config-evc VIDEO_EVC)#connect men-port default-ethernet
ChassisID(config-evc VIDEO_EVC)#no preserve-ce-vlan
ChassisID(config-evc VIDEO_EVC)#subscriber igmp priority 3
ChassisID(config-evc VIDEO_EVC)#no shutdown
ChassisID(config-evc VIDEO_EVC)#exit
```

2. Set up per-EVC, per-slot IGMP settings on both GPON and switch modules. The IGMP proxy mode used in this example.

```
ChassisID(config)#ip igmp evc VIDEO_EVC 1/5 mode proxy
ChassisID(config)#ip igmp evc VIDEO_EVC 1/5 proxy host ip address
10.20.200.1
ChassisID(config)#ip igmp evc VIDEO_EVC 1/5 proxy last-member-query
count 2
ChassisID(config)#ip igmp evc VIDEO_EVC 1/5 proxy last-member-query
interval 1000

ChassisID(config)#ip igmp evc VIDEO_EVC 1/A mode proxy
ChassisID(config)#ip igmp evc VIDEO_EVC 1/A proxy host ip address
10.20.200.1
ChassisID(config)#ip igmp evc VIDEO_EVC 1/A proxy last-member-query
count 2
ChassisID(config)#ip igmp evc VIDEO_EVC 1/A proxy last-member-query
interval 1000
```

3. Create an EVC Map per customer (ONT) for set-top box multicast traffic. Use **match multicast** to distinguish this traffic.

PON 1, ONT ID 1, ONT port 1, match multicast

```
ChassisID(config)#evc-map VIDEO_MAP_CUST1 1/5
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#connect uni gigabit-
ethernet 1/0/1@1/5/1
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#connect evc VIDEO_EVC
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#men-pri 3
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#match multicast
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber igmp mode
processing-enabled
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access dhcp
mode block
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber igmp
immediate-leave
```

```
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber igmp proxy
router ip address 10.20.200.2
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#no shutdown
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#exit
```

PON 2, ONT ID 1, ONT port 1, match multicast

```
ChassisID(config)#evc-map VIDEO_MAP_CUST2 1/5
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#connect uni gigabit-
ethernet 1/0/1@1/5/2
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#connect evc VIDEO_EVC
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#men-pri 3
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#match multicast
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber igmp mode
processing-enabled
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access dhcp
mode block
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber igmp
immediate-leave
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber igmp proxy
router ip address 10.20.200.2
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#no shutdown
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#exit
```

4. Create an EVC Map per customer (ONT) for non-multicast traffic.

PON 1, ONT ID 1, ONT port 1, match all other

```
ChassisID(config)#evc-map DATA_MAP_CUST1 1/5
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#connect uni gigabit-
ethernet 1/0/1@1/5/1
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#connect evc DATA_EVC
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#men-pri 0
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access dhcp
mode authenticate
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber igmp mode block
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access pppoe
mode block
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber arp mode proxy
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access dhcp
option-82
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access dhcp
option-82 remote-id
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#description
REMID_DATA_CUST1
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#no shutdown
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#exit
```

PON 2, ONT ID 1, ONT port 1, match all other

```
ChassisID(config)#evc-map DATA_MAP_CUST2 1/5
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#connect uni gigabit-
ethernet 1/0/1@1/5/2
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#connect evc DATA_EVC
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#men-pri 0
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access dhcp
mode authenticate
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber igmp mode block
```

```
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access pppoe  
mode block
```

```
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber arp mode proxy  
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access dhcp  
option-82  
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access dhcp  
option-82 remote-id  
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#description  
REMID_DATA_CUST2  
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#no shutdown  
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#exit
```

6.4 TLS Configuration Examples

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 card. If the VLAN becomes MAC-switched, TLS no longer functions.

6.4.1 TLS Example 1

This example displays a single tagged TLS service.

1. Create an EVC for each TLS service.

```
ChassisID#configure terminal
ChassisID(config)#evc CUST1_EVC
ChassisID(config-evc CUST1_EVC)#s-tag 100
ChassisID(config-evc CUST1_EVC)#connect men-port default-ethernet
ChassisID(config-evc CUST1_EVC)#no mac-switched
ChassisID(config-evc CUST1_EVC)#no-preserve-ce-vlan
ChassisID(config-evc CUST1_EVC)#no shutdown
ChassisID(config-evc CUST1_EVC)#exit
```

```
ChassisID(config)#evc CUST2_EVC
ChassisID(config-evc CUST2_EVC)#s-tag 200
ChassisID(config-evc CUST2_EVC)#connect men-port default-ethernet
ChassisID(config-evc CUST2_EVC)#no mac-switched
ChassisID(config-evc CUST2_EVC)#no-preserve-ce-vlan
ChassisID(config-evc CUST2_EVC)#no shutdown
ChassisID(config-evc CUST2_EVC)#exit
```

2. Create an EVC Map per customer (ONT)

PON 1, ONT ID 1, ONT port 1

```
ChassisID(config)#evc-map MAP_CUST1 1/5
ChassisID(config-evc-map MAP_CUST1 1/5)#connect uni gigabit-ethernet 1/
0/1@1/5/1
ChassisID(config-evc-map MAP_CUST1 1/5)#connect evc CUST1_EVC
ChassisID(config-evc-map MAP_CUST1 1/5)#men-pri 0
ChassisID(config-evc-map MAP_CUST1 1/5)#subscriber access dhcp mode
transparent
ChassisID(config-evc-map MAP_CUST1 1/5)#subscriber igmp mode
transparent
ChassisID(config-evc-map MAP_CUST1 1/5)#subscriber access pppoe mode
transparent
ChassisID(config-evc-map MAP_CUST1 1/5)#subscriber arp mode transparent
ChassisID(config-evc-map MAP_CUST1 1/5)#no shutdown
ChassisID(config-evc-map MAP_CUST1 1/5)#exit
```

PON 2, ONT ID 1, ONT port 1

```
ChassisID(config)#evc-map MAP_CUST2 1/5
ChassisID(config-evc-map MAP_CUST2 1/5)#connect uni gigabit-ethernet 1/
0/1@1/5/2
ChassisID(config-evc-map MAP_CUST2 1/5)#connect evc CUST2_EVC
ChassisID(config-evc-map MAP_CUST2 1/5)#men-pri 0
```

```

ChassisID(config-evc-map MAP_CUST2 1/5)#subscriber access dhcp mode
transparent
ChassisID(config-evc-map MAP_CUST2 1/5)#subscriber igmp mode
transparent
ChassisID(config-evc-map MAP_CUST2 1/5)#subscriber access pppoe mode
transparent
ChassisID(config-evc-map MAP_CUST2 1/5)#subscriber arp mode transparent
ChassisID(config-evc-map MAP_CUST2 1/5)#no shutdown
ChassisID(config-evc-map MAP_CUST2 1/5)#exit

```

6.4.2 TLS Example 2

This example displays a double-tagged TLS service (MEN C-tag added and stripped by Total Access 5000 system).

1. Create an EVC for each TLS service.

```

ChassisID#configure terminal
ChassisID(config)#evc CUST1_EVC
ChassisID(config-evc CUST1_EVC)#s-tag 100
ChassisID(config-evc CUST1_EVC)#connect men-port default-ethernet
ChassisID(config-evc CUST1_EVC)#no mac-switched
ChassisID(config-evc CUST1_EVC)#double-tag-switched
ChassisID(config-evc CUST1_EVC)#no-preserve-ce-vlan
ChassisID(config-evc CUST1_EVC)#no shutdown
ChassisID(config-evc CUST1_EVC)#exit

ChassisID(config)#evc CUST2_EVC
ChassisID(config-evc CUST2_EVC)#s-tag 200
ChassisID(config-evc CUST2_EVC)#connect men-port default-ethernet
ChassisID(config-evc CUST2_EVC)#no mac-switched
ChassisID(config-evc CUST2_EVC)#double-tag-switched
ChassisID(config-evc CUST2_EVC)#no-preserve-ce-vlan
ChassisID(config-evc CUST2_EVC)#no shutdown
ChassisID(config-evc CUST2_EVC)#exit

```

2. Create an EVC Map per customer (ONT)

PON 1, ONT ID 1, ONT port 1

```

ChassisID(config)#evc-map MAP_CUST1 1/5
ChassisID(config-evc-map MAP_CUST1 1/5)#connect uni gigabit-ethernet 1/
0/1@1/5/1
ChassisID(config-evc-map MAP_CUST1 1/5)#connect evc CUST1_EVC
ChassisID(config-evc-map MAP_CUST1 1/5)#men-pri 0
ChassisID(config-evc-map MAP_CUST1 1/5)#subscriber access dhcp mode
transparent
ChassisID(config-evc-map MAP_CUST1 1/5)#subscriber igmp mode
transparent
ChassisID(config-evc-map MAP_CUST1 1/5)#subscriber access pppoe mode
transparent
ChassisID(config-evc-map MAP_CUST1 1/5)#subscriber arp mode transparent
ChassisID(config-evc-map MAP_CUST1 1/5)#men-c-tag 101
ChassisID(config-evc-map MAP_CUST1 1/5)#no shutdown
ChassisID(config-evc-map MAP_CUST1 1/5)#exit

```

PON 2, ONT ID 1, ONT port 1

```
ChassisID(config)#evc-map MAP_CUST2 1/5
ChassisID(config-evc-map MAP_CUST2 1/5)#connect uni gigabit-ethernet 1/
0/1@1/5/2
ChassisID(config-evc-map MAP_CUST2 1/5)#connect evc CUST2_EVC
ChassisID(config-evc-map MAP_CUST2 1/5)#men-pri 0
ChassisID(config-evc-map MAP_CUST2 1/5)#subscriber access dhcp mode
transparent
ChassisID(config-evc-map MAP_CUST2 1/5)#subscriber igmp mode
transparent
ChassisID(config-evc-map MAP_CUST2 1/5)#subscriber access pppoe mode
transparent
ChassisID(config-evc-map MAP_CUST2 1/5)#subscriber arp mode transparent
ChassisID(config-evc-map MAP_CUST2 1/5)#men-c-tag 102
ChassisID(config-evc-map MAP_CUST2 1/5)#no shutdown
ChassisID(config-evc-map MAP_CUST2 1/5)#exit
```

6.4.3 IPTV Configuration Examples

1. Creating the EVC

```
ChassisID(config)#evc IGMP_EVC
ChassisID(config-evc IGMP_EVC)#s-tag 108
ChassisID(config-evc IGMP_EVC)#mac-switched
ChassisID(config-evc IGMP_EVC)#connect men-port default-ethernet
ChassisID(config-evc IGMP_EVC)#no preserve-ce-vlan
ChassisID(config-evc IGMP_EVC)#no shutdown
ChassisID(config-evc IGMP_EVC)#exit
```

2. Configuring the OLT for IGMP

```
ChassisID(config)#ip igmp evc IGMP_EVC 1/21 mode proxy
ChassisID(config)#ip igmp evc IGMP_EVC 1/21 proxy last-member-query
interval 2000
ChassisID(config)#ip igmp evc IGMP_EVC 1/21 proxy last-member-query
count 2
```

3. Enabling the UNI Ports

```
ChassisID(config)#interface gigabit-ethernet 5/0/1@1/21/3
ChassisID(config-giga-eth 5/0/1@1/21/3)#no shutdown
ChassisID(config-giga-eth 5/0/1@1/21/3)#exit
ChassisID(config)#interface gigabit-ethernet 5/0/2@1/21/3
ChassisID(config-giga-eth 5/0/2@1/21/3)#no shutdown
ChassisID(config-giga-eth 5/0/2@1/21/3)#exit
```

Single UNI Port Configured with CE-VLAN-ID Matching Criteria

```
ChassisID(config)#evc-map VIDEO-1 1/21
ChassisID(config-evc-map VIDEO-1 1/21)#connect uni gigabit-ethernet 5/
0/1@1/21/3
ChassisID(config-evc-map VIDEO-1 1/21)#connect evc IGMP_EVC
ChassisID(config-evc-map VIDEO-1 1/21)#subscriber igmp mode processing-
enabled
ChassisID(config-evc-map VIDEO-1 1/21)#subscriber igmp immediate-leave
ChassisID(config-evc-map VIDEO-1 1/21)#subscriber igmp proxy router ip
address 10.13.107.254
ChassisID(config-evc-map VIDEO-1 1/21)#match ce-vlan-id 201
ChassisID(config-evc-map VIDEO-1 1/21)#no shutdown
ChassisID(config-evc-map VIDEO-1 1/21)#exit
```



NOTE

Multiple UNI Ports (Same ONT) Configured with No Matching Criteria

UNI 1 EVC Map

```
ChassisID(config)#evc-map VIDEO-1 1/21
ChassisID(config-evc-map VIDEO-1 1/21)#connect uni gigabit-ethernet 5/
0/1@1/21/3
ChassisID(config-evc-map VIDEO-1 1/21)#connect evc IGMP_EVC
ChassisID(config-evc-map VIDEO-1 1/21)#subscriber igmp mode processing-
enabled
ChassisID(config-evc-map VIDEO-1 1/21)#subscriber igmp immediate-leave
ChassisID(config-evc-map VIDEO-1 1/21)#subscriber igmp proxy router ip
address 10.13.107.254
```

```
ChassisID(config-evc-map VIDEO-1 1/21)#no shutdown
ChassisID(config-evc-map VIDEO-1 1/21)#exit
```

UNI 2 EVC Map

```
ChassisID(config)#evc-map VIDEO-2 1/21
ChassisID(config-evc-map VIDEO-2 1/21)#connect uni gigabit-ethernet 5/
0/2@1/21/3
ChassisID(config-evc-map VIDEO-2 1/21)#connect evc IGMP_EVC
ChassisID(config-evc-map VIDEO-2 1/21)#subscriber igmp mode processing-
enabled
ChassisID(config-evc-map VIDEO-2 1/21)#subscriber igmp immediate-leave
ChassisID(config-evc-map VIDEO-2 1/21)#subscriber igmp proxy router ip
address 10.13.107.254
ChassisID(config-evc-map VIDEO-2 1/21)#no shutdown
ChassisID(config-evc-map VIDEO-2 1/21)#exit
```

7 Active Ethernet Configurations

7.1 Scope of this Section

This section provides examples of common Total Access 5000 Active Ethernet configurations.



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.

7.2 In this Section

This section contains the topics listed in [Table 7-1](#).

Table 7-1. Section 7 Topics

Sub-Section	Topic	See Page
7.3	1:1 Customer VLAN (C-VLAN) Examples	310
7.4	N:1 Service VLANs	313
7.5	Hybrid N+1:1 Combined VLAN Examples	320
7.6	TLS Examples	327

7.3 1:1 Customer VLAN (C-VLAN) Examples

The following configuration examples provision a Total Access 5000 with a 1:1 Customer VLAN (C-VLAN) model. The C-VLAN model creates a VLAN for each subscriber. All services (Data, Video, etc.) provided to the customer are carried on the same VLAN. The number of VLANs required is equal to the number of subscribers serviced.

An advantage of the C-VLAN model is security. Each subscriber is isolated from other subscribers on separate VLANs. Another advantage is the similarity to older ATM based configurations. The main disadvantage of the C-VLAN model is the lack of multicast replication. A separate copy of each multicast stream must be sent to the Total Access 5000 for each user requesting it. These copies inefficiently use uplink bandwidth, thus limiting the size of the subscriber base for each Total Access 5000.

Figure 7-1 illustrates a 1:1 Customer VLAN model inside a Total Access 5000. When provisioning a C-VLAN each VLAN requires an EVC and an EVC Map to connect the EVC to the correct UNI port.

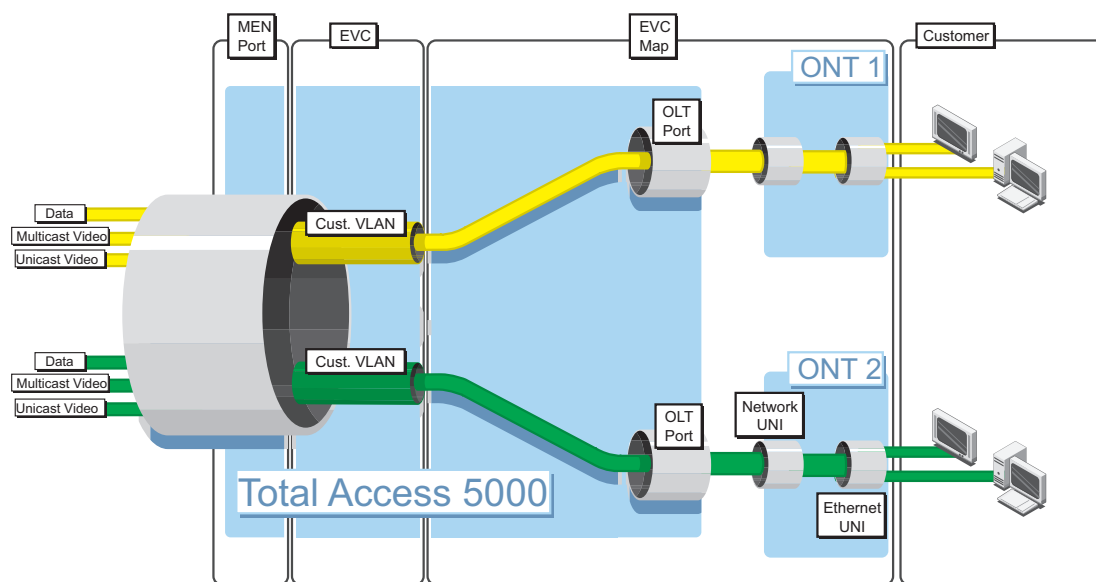


Figure 7-1. 1:1 Customer VLAN Diagram

7.3.1 Example 1:1 Example

1. Create an EVC for each customer

```
ChassisID#configure terminal
ChassisID(config)#evc CUST1_EVC
ChassisID(config-evc CUST1_EVC)#s-tag 100
ChassisID(config-evc CUST1_EVC)#mac-switched
ChassisID(config-evc CUST1_EVC)#connect men-port default-ethernet
ChassisID(config-evc CUST1_EVC)#no preserve-ce-vlan
ChassisID(config-evc CUST1_EVC)#no shutdown
ChassisID(config-evc CUST1_EVC)#exit
ChassisID(config)#exit

ChassisID#configure terminal
ChassisID(config)#evc CUST2_EVC
ChassisID(config-evc CUST2_EVC)#s-tag 200
ChassisID(config-evc CUST2_EVC)#mac-switched
ChassisID(config-evc CUST2_EVC)#connect men-port default-ethernet
ChassisID(config-evc CUST2_EVC)#no preserve-ce-vlan
ChassisID(config-evc CUST2_EVC)#no shutdown
ChassisID(config-evc CUST2_EVC)#exit
ChassisID(config)#exit
```

2. Create an EVC Map per customer (ONT).

The example shows the provisioning of 2 ONTs.

OLT Port 1, ONT port 1

```
ChassisID(config)#evc-map MAP_CUST1 1/5
ChassisID(config-evc-map MAP_CUST1 1/5)#connect uni gigabit-ethernet 1/
0/1@1/5/1.gigabit-ethernet
ChassisID(config-evc-map MAP_CUST1 1/5)#connect evc CUST1_EVC
ChassisID(config-evc-map MAP_CUST1 1/5)#men-pri 0
ChassisID(config-evc-map MAP_CUST1 1/5)#subscriber access dhcp mode
block
ChassisID(config-evc-map MAP_CUST1 1/5)#subscriber igmp mode block
ChassisID(config-evc-map MAP_CUST1 1/5)#subscriber access pppoe mode
block
ChassisID(config-evc-map MAP_CUST1 1/5)#subscriber access static-ip
1.2.3.3 00:01:02:03:04:05 1.2.3.254 00:01:02:00:00:00
ChassisID(config-evc-map MAP_CUST1 1/5)#subscriber arp mode proxy
ChassisID(config-evc-map MAP_CUST1 1/5)#no shutdown
ChassisID(config-evc-map MAP_CUST1 1/5)#exit
```

OLT Port 2, ONT port 1

```
ChassisID(config)#evc-map MAP_CUST2 1/5
ChassisID(config-evc-map MAP_CUST2 1/5)#connect uni gigabit-ethernet 1/
0/1@1/5/2.gigabit-ethernet
ChassisID(config-evc-map MAP_CUST2 1/5)#connect evc CUST2_EVC
ChassisID(config-evc-map MAP_CUST2 1/5)#men-pri 0
ChassisID(config-evc-map MAP_CUST2 1/5)#subscriber access dhcp mode
block
ChassisID(config-evc-map MAP_CUST2 1/5)#subscriber igmp mode block
ChassisID(config-evc-map MAP_CUST2 1/5)#subscriber access pppoe mode
block
```

```
ChassisID(config-evc-map MAP_CUST2 1/5)#subscriber access static-ip  
1.2.3.4 00:01:02:03:04:06 1.2.3.254 00:01:02:00:00:00  
ChassisID(config-evc-map MAP_CUST2 1/5)#subscriber arp mode proxy  
ChassisID(config-evc-map MAP_CUST2 1/5)#no shutdown  
ChassisID(config-evc-map MAP_CUST2 1/5)#exit
```

7.4 N:1 Service VLANs

The following configuration examples provision a Total Access 5000 with a N:1 Service VLAN model. The N:1 Service VLAN model creates one VLAN for each provided service (Data, Video, etc.). This service VLAN is shared by multiple (N) subscribers.

The N:1 Service VLAN model allows for the replication of multicast traffic to multiple users. This replication makes more efficient use of uplink bandwidth. The N:1 Service VLAN model may also have advantages when adding video to an existing network, as the addition of a video VLAN will not disrupt the existing data VLAN. A disadvantage of this model is that the Product Name must provide additional security as the subscribers are not on isolated VLANs.

Figure 7-2 illustrates a N:1 Service VLAN model inside a Total Access 5000. When provisioning a S-VLAN each VLAN requires an EVC and an EVC Map to connect the EVC to the each required UNI port. Therefore each UNI port will have one EVC Map for each service passing through it.

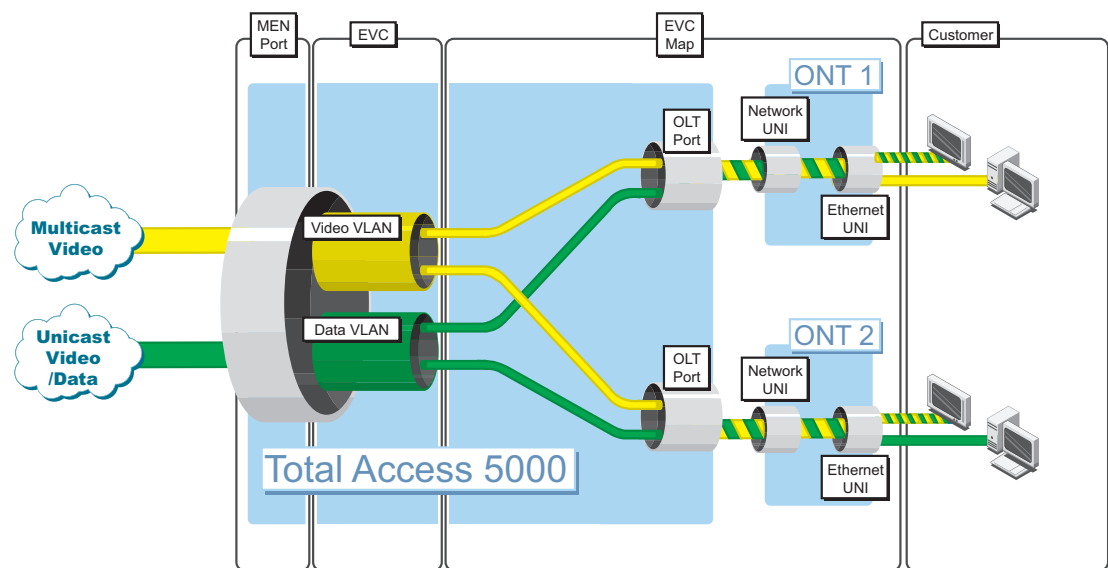


Figure 7-2. N:1 Service VLAN Diagram

7.4.1 N:1 Service VLAN Example 1

The following example displays data and video on same ONT port.

1. Create an EVC for each service.

```
ChassisID#configure terminal
ChassisID(config)#evc DATA_EVC
ChassisID(config-evc DATA_EVC)#s-tag 101
ChassisID(config-evc DATA_EVC)#connect men-port default-ethernet
ChassisID(config-evc DATA_EVC)#mac-switched
ChassisID(config-evc DATA_EVC)#no preserve-ce-vlan
ChassisID(config-evc DATA_EVC)#no shutdown
ChassisID(config-evc DATA_EVC)#exit

ChassisID(config)#evc VIDEO_EVC
ChassisID(config-evc VIDEO_EVC)#s-tag 1001
ChassisID(config-evc VIDEO_EVC)#connect men-port default-ethernet
ChassisID(config-evc VIDEO_EVC)#no preserve-ce-vlan
ChassisID(config-evc VIDEO_EVC)#subscriber igmp priority 3
ChassisID(config-evc VIDEO_EVC)#no shutdown
ChassisID(config-evc VIDEO_EVC)#exit
```

2. Set up per-EVC, per-slot IGMP settings on both Active E and switch modules (proxy mode used in this example).

```
ChassisID(config)#ip igmp evc VIDEO_EVC 1/5 mode proxy
ChassisID(config)#ip igmp evc VIDEO_EVC 1/5 proxy host ip address
10.20.200.1
ChassisID(config)#ip igmp evc VIDEO_EVC 1/5 proxy last-member-query
count 2
ChassisID(config)#ip igmp evc VIDEO_EVC 1/5 proxy last-member-query
interval 1000

ChassisID(config)#ip igmp evc VIDEO_EVC 1/A mode proxy
ChassisID(config)#ip igmp evc VIDEO_EVC 1/A proxy host ip address
10.20.200.1
ChassisID(config)#ip igmp evc VIDEO_EVC 1/A proxy last-member-query
count 2
ChassisID(config)#ip igmp evc VIDEO_EVC 1/A proxy last-member-query
interval 1000
```

3. Create an EVC Map per customer (ONT) for each service. Use the set-top box MAC address to distinguish its traffic.

- a. Create the video EVC Maps.

OLT port 1, ONT port 1, match set-top box

```
ChassisID(config)#evc-map VIDEO_MAP_CUST1 1/5
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#connect uni gigabit-
ethernet 1/0/1@1/5/1.gigabit-ethernet
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#connect evc VIDEO_EVC
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#men-pri 3
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#match source mac-
address 00:02:02:00:00:00 ff:ff:ff:00:00:00
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber igmp mode
processing-enabled
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber igmp
immediate-leave
```

```

ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber igmp proxy
router ip address 10.20.200.2
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber access
dhcp mode authenticate
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber access
pppoe mode block
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber arp mode
proxy
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber access
dhcp option-82
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber access
dhcp option-82 remote-id
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#description
REMI_VIDEO_CUST1
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#no shutdown
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#exit

```

OLT port 2, ONT port 1, match set-top box

```

ChassisID(config)#evc-map VIDEO_MAP_CUST2 1/5
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#connect uni gigabit-
ethernet 1/0/1@1/5/2.gigabit-ethernet
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#connect evc VIDEO_EVC
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#men-pri 3
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#match source mac-
address 00:02:02:00:00:00 ff:ff:ff:00:00:00

ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber igmp mode
processing-enabled
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber igmp
immediate-leave
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber igmp proxy
router ip address 10.20.200.2
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber access
dhcp mode authenticate
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber access
pppoe mode block
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber arp mode
proxy
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber access
dhcp option-82
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber access
dhcp option-82 remote-id
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#description
REMI_VIDEO_CUST2
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#no shutdown
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#exit

```

- b. Create the data EVC Maps.

OLT port 1, ONT port 1, match all other

```
ChassisID(config)#evc-map DATA_MAP_CUST1 1/5
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#connect uni gigabit-
ethernet 1/0/1@1/5/1.gigabit-ethernet
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#connect evc DATA_EVC
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#men-pri 0
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access dhcp
mode authenticate
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber igmp mode
block
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access
pppoe mode block
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber arp mode
proxy
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access dhcp
option-82
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access dhcp
option-82 remote-id
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#description
REMI_DATA_CUST1
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#no shutdown
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#exit
```

OLT port 2, ONT port 1, match all other

```
ChassisID(config)#evc-map DATA_MAP_CUST2 1/5
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#connect uni gigabit-
ethernet 1/0/1@1/5/2.gigabit-ethernet
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#connect evc DATA_EVC
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#men-pri 0
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access dhcp
mode authenticate
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber igmp mode
block
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access
pppoe mode block
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber arp mode
proxy
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access dhcp
option-82
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access dhcp
option-82 remote-id
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#description
REMI_DATA_CUST2
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#no shutdown
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#exit
```

7.4.2 N:1 Service VLAN Example 2

This example displays data and video on different ONT ports.

1. Create an EVC for each service.

```
ChassisID#configure terminal
ChassisID(config)#evc DATA_EVC
ChassisID(config-evc DATA_EVC)#s-tag 101
ChassisID(config-evc DATA_EVC)#connect men-port default-ethernet
ChassisID(config-evc DATA_EVC)#mac-switched
ChassisID(config-evc DATA_EVC)#no preserve-ce-vlan
ChassisID(config-evc DATA_EVC)#no shutdown
ChassisID(config-evc DATA_EVC)#exit

ChassisID(config)#evc VIDEO_EVC
ChassisID(config-evc VIDEO_EVC)#s-tag 1001
ChassisID(config-evc VIDEO_EVC)#connect men-port default-ethernet
ChassisID(config-evc VIDEO_EVC)#no preserve-ce-vlan
ChassisID(config-evc VIDEO_EVC)#subscriber igmp priority 3
ChassisID(config-evc VIDEO_EVC)#no shutdown
ChassisID(config-evc VIDEO_EVC)#exit
```

2. Set up per-EVC, per-slot IGMP settings on both Active E and switch modules (snooping mode used in this example).

```
ChassisID(config)#ip igmp evc VIDEO_EVC 1/5 mode snooping
ChassisID(config)#ip igmp evc VIDEO_EVC 1/5 proxy last-member-query
count 2
ChassisID(config)#ip igmp evc VIDEO_EVC 1/5 proxy last-member-query
interval 1000
ChassisID(config)#ip igmp evc VIDEO_EVC 1/A mode snooping
ChassisID(config)#ip igmp evc VIDEO_EVC 1/A proxy last-member-query
count 2
ChassisID(config)#ip igmp evc VIDEO_EVC 1/A proxy last-member-query
interval 1000
```

3. Create an EVC Map per customer (ONT) for each service.

These examples show DHCP authentication for video and PPPoE authentication for data.

- a. Create the video EVC Maps.

OLT port 1, ONT port 2

```
ChassisID(config)#evc-map VIDEO_MAP_CUST1 1/5
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#connect uni gigabit-
ethernet 1/0/2@1/5/1.gigabit-ethernet
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#connect evc VIDEO_EVC
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#men-pri 3
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber igmp mode
processing-enabled
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber igmp
immediate-leave
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber access
dhcp mode authenticate
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber access
pppoe mode block
```

```

ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber arp mode
proxy
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber access
dhcp option-82
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber access
dhcp option-82 remote-id
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#description
REMIID_VIDEO_CUST1
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#no shutdown
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#exit

```

OLT port 2, ONT port 2

```

ChassisID(config)#evc-map VIDEO_MAP_CUST2 1/5
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#connect uni gigabit-
ethernet 1/0/2@1/5/2.gigabit-ethernet
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#connect evc VIDEO_EVC
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#men-pri 3
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber igmp mode
processing-enabled
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber igmp
immediate-leave
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber access
dhcp mode authenticate
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber access
pppoe mode block
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber arp mode
proxy
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber access
dhcp option-82
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber access
dhcp option-82 remote-id
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#description
REMIID_VIDEO_CUST2
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#no shutdown
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#exit

```

b. Create the data EVC Maps.

These examples show the addition of a customer-specific C-tag toward the network.

OLT port 1, ONT port 1

```

ChassisID(config)#evc-map DATA_MAP_CUST1 1/5
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#connect uni gigabit-
ethernet 1/0/1@1/5/1.gigabit-ethernet
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#connect evc DATA_EVC
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#men-pri 0
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#men-c-tag 101
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access dhcp
mode block
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber igmp mode
block
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access
pppoe mode authenticate
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber arp mode
proxy

```

```
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access
pppoe intermediate-agent
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access
pppoe intermediate-agent remote-id
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#description
REMIID_DATA_CUST1
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#no shutdown
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#exit
```

OLT port 2, ONT port 1

```
ChassisID(config)#evc-map DATA_MAP_CUST2 1/5
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#connect uni gigabit-
ethernet 1/0/1@1/5/2.gigabit-ethernet
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#connect evc DATA_EVC
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#men-pri 0
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#men-c-tag 102
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access dhcp
mode block
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber igmp mode
block
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access
pppoe mode authenticate
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber arp mode
proxy
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access
pppoe intermediate-agent
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access
pppoe intermediate-agent remote-id
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#description
REMIID_DATA_CUST2
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#no shutdown
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#exit
```

7.5 Hybrid N+1:1 Combined VLAN Examples

The following configuration examples provision a Total Access 5000 with a Hybrid N+1:1 VLAN (Combined VLAN) model. The Combined VLAN model creates a VLAN for each subscriber that handles data and unicast video traffic. A separate shared VLAN is created for multicast video and IGMP traffic, this allows for multicast replication. The number of VLANs required is equal to the number of subscribers serviced plus one, (N+1:1).

This model provides all of the advantages of the C-VLAN, (i.e. security, simplified operations, etc.) while removing its biggest disadvantage, no multicast replication.

Figure 7-3 illustrates a Hybrid N+1:1 VLAN model inside a Total Access 5000. When provisioning a Combined VLAN each VLAN requires an EVC and an EVC Map to connect the EVC to the each required UNI port. Therefore each UNI port will have one EVC Map for Unicast and Data and another for Multicast.

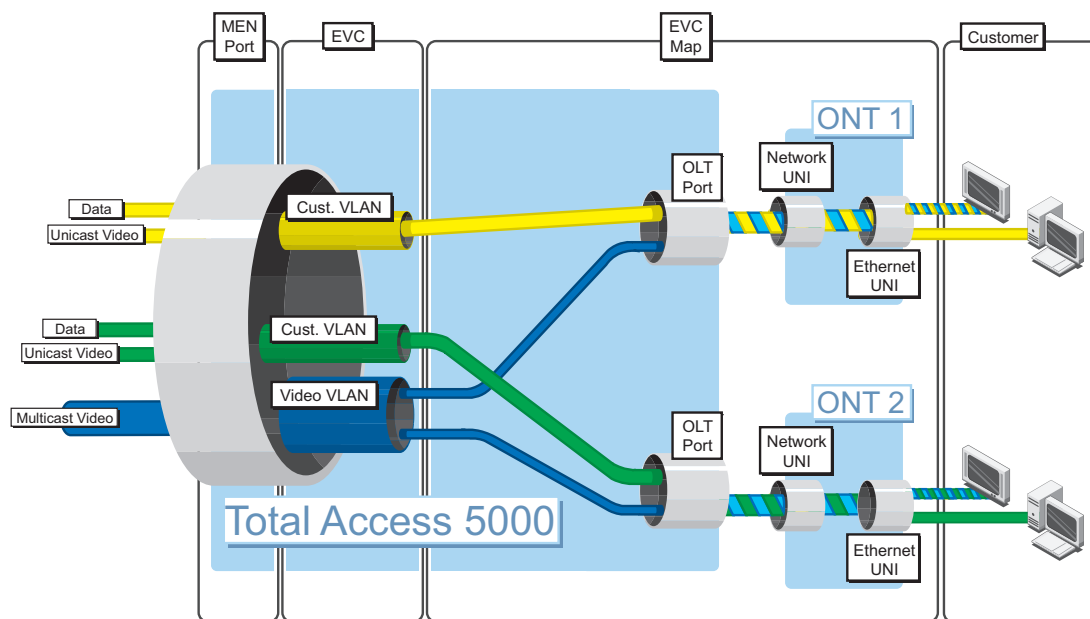


Figure 7-3. Hybrid N+1:1 Combined VLAN Diagram

7.5.1 Hybrid N+1:1 Example 1

This example displays customer VLANs with multicast replication (Hybrid/Split VLAN).

1. Create an EVC for each customer and a single EVC for video.

```
ChassisID#configure terminal
ChassisID(config)#evc CUST1_EVC
ChassisID(config-evc CUST1_EVC)#s-tag 100
ChassisID(config-evc CUST1_EVC)#connect men-port default-ethernet
ChassisID(config-evc CUST1_EVC)#mac-switched
ChassisID(config-evc CUST1_EVC)#no preserve-ce-vlan
ChassisID(config-evc CUST1_EVC)#no shutdown
ChassisID(config-evc CUST1_EVC)#exit

ChassisID(config)#evc CUST2_EVC
ChassisID(config-evc CUST2_EVC)#s-tag 200
ChassisID(config-evc CUST2_EVC)#connect men-port default-ethernet
ChassisID(config-evc CUST2_EVC)#mac-switched
ChassisID(config-evc CUST2_EVC)#no preserve-ce-vlan
ChassisID(config-evc CUST2_EVC)#no shutdown
ChassisID(config-evc CUST2_EVC)#exit

ChassisID(config)#evc VIDEO_EVC
ChassisID(config-evc VIDEO_EVC)#s-tag 1001
ChassisID(config-evc VIDEO_EVC)#connect men-port default-ethernet
ChassisID(config-evc VIDEO_EVC)#no preserve-ce-vlan
ChassisID(config-evc VIDEO_EVC)#subscriber igmp priority 3
ChassisID(config-evc VIDEO_EVC)#no shutdown
ChassisID(config-evc VIDEO_EVC)#exit
```

2. Set up per-EVC, per-slot IGMP settings on both AE and GigE SMs (proxy mode used in this example).

```
ChassisID(config)#ip igmp evc VIDEO_EVC 1/5 mode proxy
ChassisID(config)#ip igmp evc VIDEO_EVC 1/5 proxy host ip address
10.20.200.1
ChassisID(config)#ip igmp evc VIDEO_EVC 1/5 proxy last-member-query
count 2
ChassisID(config)#ip igmp evc VIDEO_EVC 1/5 proxy last-member-query
interval 1000

ChassisID(config)#ip igmp evc VIDEO_EVC 1/A mode proxy
ChassisID(config)#ip igmp evc VIDEO_EVC 1/A proxy host ip address
10.20.200.1
ChassisID(config)#ip igmp evc VIDEO_EVC 1/A proxy last-member-query
count 2
ChassisID(config)#ip igmp evc VIDEO_EVC 1/A proxy last-member-query
interval 1000
```

3. Create an EVC Map per customer (ONT) for each service.

These examples show DHCP authentication.

OLT port 1, ONT port 1, match multicast traffic

```
ChassisID(config)#evc-map VIDEO_MAP_CUST1 1/5
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#connect uni gigabit-
ethernet 1/0/1@1/5/1.gigabit-ethernet
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#connect evc VIDEO_EVC
```

```
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#men-pri 3
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#match multicast
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber igmp mode
processing-enabled
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber access
dhcp mode block
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber igmp
immediate-leave
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber igmp proxy
router ip address 10.20.200.2
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#no shutdown
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#exit
```

OLT port 2, ONT port 1, match multicast traffic

```
ChassisID(config)#evc-map VIDEO_MAP_CUST2 1/5
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#connect uni gigabit-
ethernet 1/0/1@1/5/2.gigabit-ethernet
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#connect evc VIDEO_EVC
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#men-pri 3
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#match multicast
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber igmp mode
processing-enabled
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber access
dhcp mode block
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber igmp
immediate-leave
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber igmp proxy
router ip address 10.20.200.2
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#no shutdown
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#exit
```

OLT port 1, ONT port 1, match all other

```
ChassisID(config)#evc-map DATA_MAP_CUST1 1/5
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#connect uni gigabit-
ethernet 1/0/1@1/5/1.gigabit-ethernet
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#connect evc CUST1_EVC
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#men-pri 0
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access dhcp
mode authenticate
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber igmp mode
block
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access
pppoe mode block
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber arp mode
proxy
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access dhcp
option-82
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access dhcp
option-82 remote-i
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#description
REMID_DATA_CUST1
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#no shutdown
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#exit
```

OLT port 2, ONT port 1, match all other

```
ChassisID(config)#evc-map DATA_MAP_CUST2 1/5
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#connect uni gigabit-
ethernet 1/0/1@1/5/2.gigabit-ethernet
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#connect evc CUST2_EVC
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#men-pri 0
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access dhcp
mode authenticate
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber igmp mode
block
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access
pppoe mode block
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber arp mode
proxy
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access dhcp
option-82
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access dhcp
option-82 remote-id
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#description
RE MID_DATA_CUST2
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#no shutdown
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#exit
```

7.5.2 Hybrid N+1:1 Example 2

This example shows N:1 service VLANs for data and hybrid/split VLAN for video.

1. Create an EVC each for data and video.

```
ChassisID#configure terminal
ChassisID(config)#evc DATA_EVC
ChassisID(config-evc DATA_EVC)#s-tag 101
ChassisID(config-evc DATA_EVC)#connect men-port default-ethernet
ChassisID(config-evc DATA_EVC)#mac-switched
ChassisID(config-evc DATA_EVC)#no preserve-ce-vlan
ChassisID(config-evc DATA_EVC)#no shutdown
ChassisID(config-evc DATA_EVC)#exit

ChassisID(config)#evc VIDEO_EVC
ChassisID(config-evc VIDEO_EVC)#s-tag 1001
ChassisID(config-evc VIDEO_EVC)#connect men-port default-ethernet
ChassisID(config-evc VIDEO_EVC)#no preserve-ce-vlan
ChassisID(config-evc VIDEO_EVC)#subscriber igmp priority 3
ChassisID(config-evc VIDEO_EVC)#no shutdown
ChassisID(config-evc VIDEO_EVC)#exit
```

2. Set up per-EVC, per-slot IGMP settings on both AE and GigE SMs (proxy mode used in this example).

```
ChassisID(config)#ip igmp evc VIDEO_EVC 1/5 mode proxy
ChassisID(config)#ip igmp evc VIDEO_EVC 1/5 proxy host ip address
10.20.200.1
ChassisID(config)#ip igmp evc VIDEO_EVC 1/5 proxy last-member-query
count 2
ChassisID(config)#ip igmp evc VIDEO_EVC 1/5 proxy last-member-query
interval 1000

ChassisID(config)#ip igmp evc VIDEO_EVC 1/A mode proxy
ChassisID(config)#ip igmp evc VIDEO_EVC 1/A proxy host ip address
10.20.200.1
ChassisID(config)#ip igmp evc VIDEO_EVC 1/A proxy last-member-query
count 2
ChassisID(config)#ip igmp evc VIDEO_EVC 1/A proxy last-member-query
interval 1000
```

3. Create an EVC Map per customer (ONT) for set-top box multicast traffic. Use **match multicast** distinguish this traffic

OLT port 1, ONT port 1, match multicast

```
ChassisID(config)#evc-map VIDEO_MAP_CUST1 1/5
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#connect uni gigabit-
ethernet 1/0/1@1/5/1.gigabit-ethernet
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#connect evc VIDEO_EVC
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#men-pri 3
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#match multicast
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber igmp mode
processing-enabled
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber access
dhcp mode block
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber igmp
immediate-leave
```

```

ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber igmp proxy
router ip address 10.20.200.2
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#no shutdown
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#exit

```

OLT port 2, ONT port 1, match multicast

```

ChassisID(config)#evc-map VIDEO_MAP_CUST2 1/5
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#connect uni gigabit-
ethernet 1/0/1@1/5/2.gigabit-ethernet
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#connect evc VIDEO_EVC
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#men-pri 3
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#match multicast
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber igmp mode
processing-enabled
ChassisID(config-evc-map VIDEO_MAP_CUST1 1/5)#subscriber access
dhcp mode block
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber igmp
immediate-leave
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#subscriber igmp proxy
router ip address 10.20.200.2
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#no shutdown
ChassisID(config-evc-map VIDEO_MAP_CUST2 1/5)#exit

```

4. Create an EVC Map per customer (ONT) for non-multicast traffic.

OLT port 1, ONT port 1, match all other

```

ChassisID(config)#evc-map DATA_MAP_CUST1 1/5
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#connect uni gigabit-
ethernet 1/0/1@1/5/1.gigabit-ethernet
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#connect evc DATA_EVC
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#men-pri 0
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access dhcp
mode authenticate
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber igmp mode
block
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access
pppoe mode block
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber arp mode
proxy
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access dhcp
option-82
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#subscriber access dhcp
option-82 remote-id
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#description
REMID_DATA_CUST1
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#no shutdown
ChassisID(config-evc-map DATA_MAP_CUST1 1/5)#exit

```

OLT port 2, ONT port 1, match all other

```

ChassisID(config)#evc-map DATA_MAP_CUST2 1/5
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#connect uni gigabit-
ethernet 1/0/1@1/5/2.gigabit-ethernet
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#connect evc DATA_EVC
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#men-pri 0
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access dhcp

```

```
mode authenticate
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber igmp mode
block
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access
pppoe mode block
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber arp mode
proxy
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access dhcp
option-82
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#subscriber access dhcp
option-82 remote-id
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#description
REMIID_DATA_CUST2
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#no shutdown
ChassisID(config-evc-map DATA_MAP_CUST2 1/5)#exit
```

7.6 TLS Examples

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 card. If the VLAN becomes MAC-switched, TLS no longer functions.

7.6.1 TLS Example 1

This example displays a single tagged TLS service.

1. Create an EVC for each TLS service.

```
ChassisID#configure terminal
ChassisID(config)#evc CUST1_EVC
ChassisID(config-evc CUST1_EVC)#s-tag 100
ChassisID(config-evc CUST1_EVC)#connect men-port default-ethernet
ChassisID(config-evc CUST1_EVC)#no mac-switched
ChassisID(config-evc CUST1_EVC)#no-preserve-ce-vlan
ChassisID(config-evc CUST1_EVC)#no shutdown
ChassisID(config-evc CUST1_EVC)#exit
```

```
ChassisID(config)#evc CUST2_EVC
ChassisID(config-evc CUST2_EVC)#s-tag 200
ChassisID(config-evc CUST2_EVC)#connect men-port default-ethernet
ChassisID(config-evc CUST2_EVC)#no mac-switched
ChassisID(config-evc CUST2_EVC)#no-preserve-ce-vlan
ChassisID(config-evc CUST2_EVC)#no shutdown
ChassisID(config-evc CUST2_EVC)#exit
```

2. Create an EVC Map per customer (ONT)

OLT Port 1, ONT port 1

```
ChassisID(config)#evc-map MAP_CUST1 1/5
ChassisID(config-evc-map MAP_CUST1 1/5)#connect uni gigabit-ethernet 1/
0/1@1/5/1.gigabit-ethernet
ChassisID(config-evc-map MAP_CUST1 1/5)#connect evc CUST1_EVC
ChassisID(config-evc-map MAP_CUST1 1/5)#men-pri 0
ChassisID(config-evc-map MAP_CUST1 1/5)#subscriber access dhcp mode
transparent
ChassisID(config-evc-map MAP_CUST1 1/5)#subscriber igmp mode
transparent
ChassisID(config-evc-map MAP_CUST1 1/5)#subscriber access pppoe mode
transparent
ChassisID(config-evc-map MAP_CUST1 1/5)#subscriber arp mode transparent
ChassisID(config-evc-map MAP_CUST1 1/5)#no shutdown
ChassisID(config-evc-map MAP_CUST1 1/5)#exit
```

OLT Port 2, ONT port 1

```
ChassisID(config)#evc-map MAP_CUST2 1/5
ChassisID(config-evc-map MAP_CUST2 1/5)#connect uni gigabit-ethernet 1/
0/1@1/5/2.gigabit-ethernet
ChassisID(config-evc-map MAP_CUST2 1/5)#connect evc CUST2_EVC
ChassisID(config-evc-map MAP_CUST2 1/5)#men-pri 0
```

```
ChassisID(config-evc-map MAP_CUST2 1/5)#subscriber access dhcp mode
transparent
ChassisID(config-evc-map MAP_CUST2 1/5)#subscriber igmp mode
transparent
ChassisID(config-evc-map MAP_CUST2 1/5)#subscriber access pppoe mode
transparent
ChassisID(config-evc-map MAP_CUST2 1/5)#subscriber arp mode transparent
ChassisID(config-evc-map MAP_CUST2 1/5)#no shutdown
ChassisID(config-evc-map MAP_CUST2 1/5)#exit
```

7.6.2 TLS Example 2

This example displays a double-tagged TLS service (MEN C-tag added and stripped by Total Access 5000 system).

1. Create an EVC for each TLS service.

```
ChassisID#configure terminal
ChassisID(config)#evc CUST1_EVC
ChassisID(config-evc CUST1_EVC)#s-tag 100
ChassisID(config-evc CUST1_EVC)#connect men-port default-ethernet
ChassisID(config-evc CUST1_EVC)#no mac-switched
ChassisID(config-evc CUST1_EVC)#double-tag-switched
ChassisID(config-evc CUST1_EVC)#no-preserve-ce-vlan
ChassisID(config-evc CUST1_EVC)#no shutdown
ChassisID(config-evc CUST1_EVC)#exit

ChassisID(config)#evc CUST2_EVC
ChassisID(config-evc CUST2_EVC)#s-tag 200
ChassisID(config-evc CUST2_EVC)#connect men-port default-ethernet
ChassisID(config-evc CUST2_EVC)#no mac-switched
ChassisID(config-evc CUST2_EVC)#double-tag-switched
ChassisID(config-evc CUST2_EVC)#no-preserve-ce-vlan
ChassisID(config-evc CUST2_EVC)#no shutdown
ChassisID(config-evc CUST2_EVC)#exit
```

2. Create an EVC Map per customer (ONT)

OLT Port 1, ONT port 1

```
ChassisID(config)#evc-map MAP_CUST1 1/5
ChassisID(config-evc-map MAP_CUST1 1/5)#connect uni gigabit-ethernet 1/
0/1@1/5/1.gigabit-ethernet
ChassisID(config-evc-map MAP_CUST1 1/5)#connect evc CUST1_EVC
ChassisID(config-evc-map MAP_CUST1 1/5)#men-pri 0
ChassisID(config-evc-map MAP_CUST1 1/5)#subscriber access dhcp mode
transparent
ChassisID(config-evc-map MAP_CUST1 1/5)#subscriber igmp mode
transparent
ChassisID(config-evc-map MAP_CUST1 1/5)#subscriber access pppoe mode
transparent
ChassisID(config-evc-map MAP_CUST1 1/5)#subscriber arp mode transparent
ChassisID(config-evc-map MAP_CUST1 1/5)#men-c-tag 101
ChassisID(config-evc-map MAP_CUST1 1/5)#no shutdown
ChassisID(config-evc-map MAP_CUST1 1/5)#exit
```

OLT Port 2, ONT port 1

```
ChassisID(config)#evc-map MAP_CUST2 1/5
ChassisID(config-evc-map MAP_CUST2 1/5)#connect uni gigabit-ethernet 1/
0/1@1/5/2.gigabit-ethernet
ChassisID(config-evc-map MAP_CUST2 1/5)#connect evc CUST2_EVC
ChassisID(config-evc-map MAP_CUST2 1/5)#men-pri 0
ChassisID(config-evc-map MAP_CUST2 1/5)#subscriber access dhcp mode
transparent
ChassisID(config-evc-map MAP_CUST2 1/5)#subscriber igmp mode
transparent
ChassisID(config-evc-map MAP_CUST2 1/5)#subscriber access pppoe mode
transparent
ChassisID(config-evc-map MAP_CUST2 1/5)#subscriber arp mode transparent
ChassisID(config-evc-map MAP_CUST2 1/5)#men-c-tag 102
ChassisID(config-evc-map MAP_CUST2 1/5)#no shutdown
ChassisID(config-evc-map MAP_CUST2 1/5)#exit
```


8 Traffic Management

8.1 Scope of this Section

This section covers Traffic Management (shapers and policers) provisioning that can be applied to your network.

8.2 In this Section

This section contains the topics listed in [Table 8-1](#).

Table 8-1. Section 8 Topics

Sub-Section	Topic	See Page
8.3	Shapers, GPON	332
8.4	Provisioning using CLI	334
8.5	Shapers, AE (Example)	353
8.7	Policers, AE (Example)	357

8.3 Shapers, GPON

Shaping is a mechanism used at egress to smooth out bursts of traffic. Unlike a policer, which discards large bursts of traffic, shapers work on queues. The bursts in traffic can appear smoothed because of the queue function. The shaper acts more like a rate limiter. The port shaper uses a token bucket (much like a policer); however, when large bursts are received, the packets are delayed rather than discarded immediately. When a packet arrives at the shaper, if there are sufficient tokens available, the packet is transmitted without delay. If there are insufficient tokens in the bucket, the packet is delayed until there are enough tokens in the bucket to allow transmission.

The benefit of a shaper is that it will not drop frames with a small burst of traffic, but it does potentially add latency (delay).

The GPON FTTP application supports downstream and upstream shapers. In downstream, the shapers are per queue (in turn based P-Bits) and per ONT. In upstream, the shapers are per ONT or per ONT Channel (TCONT).

8.3.1 Downstream Shaping



NOTE

For Total Access 5000 System Release 7.1 and above, oversubscription is supported for downstream. All provisioned ONTs connected to a PON can have more than 2.5 Gig rate provisioned.

The purpose of downstream shaping (see [Figure 8-1](#) on page 8-333) is to provide the ability to provision different rates for the same services for customers being serviced from the same ONT or user network interface (UNI).

This can be done using a combination of quality of service (QoS) map profiles and downstream shapers. The QoS map profiles allow the user to map any given p-bit(s) to any class of service (CoS) queue. This allows the user to place different services which have the same p-bit priority, into different queues. This contrasts with what was done before where all traffic went through the System CoS Map which would simply map p-bit X to queue Y. The benefit of this is that now you may provision separate downstream shapers with different rates on the outputs of the CoS queues. This gives you the ability to service multiple customers from the same ONT but still provide them with separate rates of service.

Weighted Fair Queue (WFQ) provides similar behavior to the shapers in that the inputs to the WFQ are weights and queue groupings. These weights can be changed to allow one service to have a higher priority than the other services in the same WFQ.



NOTE

The WFQ does not act unless there is enough downstream congestion. It is not necessary to provision the WFQ to obtain the required functionality.

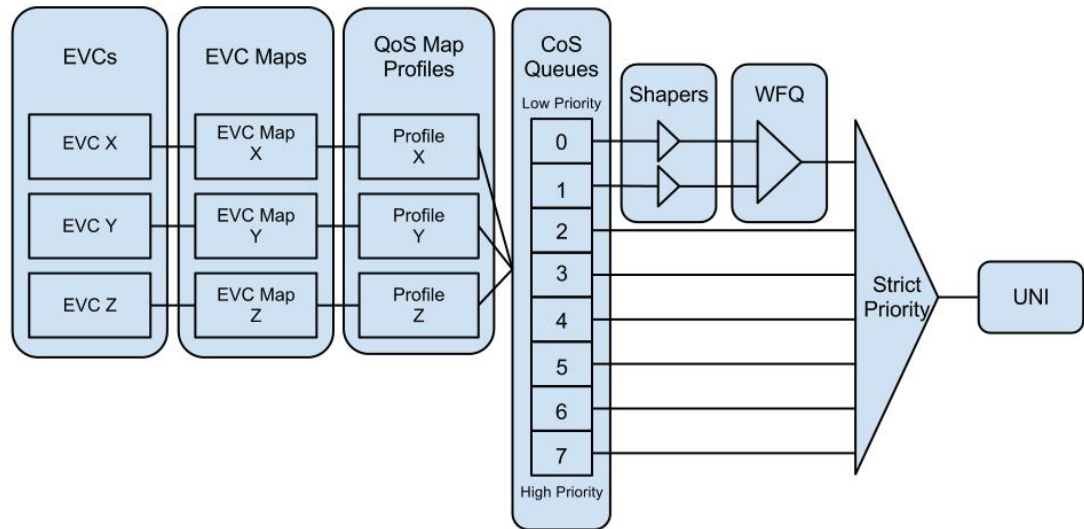


Figure 8-1. GPON Downstream Shaping Hierarchy

8.3.2 Upstream Shaping

In previous releases, provisioning more data bandwidth than existed on the PON was not allowed. This was nominally 1.2 Gbps upstream and 2.4 Gbps downstream. Upstream shaping now allows oversubscription of bandwidth but adds the option of guaranteed and/or not guaranteed bandwidth.

In the upstream direction, there are three bandwidth values that are provisioned in a shaper when the shaper is attached to a GPON channel (upstream from ONT). The shaper rate is the maximum rate the service receives or the PIR (Peak Information Rate). There are two options to assign a guaranteed upstream rate:

- Fixed Bandwidth
- Assured Bandwidth

The Committed Information Rate (CIR) must be less than or equal to PIR for a service. If CIR equals the PIR, then all service bandwidth is guaranteed. If CIR is less than PIR, the bandwidth between CIR and PIR is not guaranteed. This bandwidth is labeled “best effort” ($\text{PIR} - \text{CIR} = \text{best effort}$). The total CIR of all service endpoints on the PON cannot exceed the upstream PON bandwidth.

Fixed bandwidth is used for services requiring low/fixed latency. The service is granted the same upstream bandwidth in every upstream allocation period. Even if no traffic is sent, fixed bandwidth is allocated transmit time and thus this bandwidth is not available for best-effort use.

Assured bandwidth is also guaranteed, but the bandwidth is averaged over multiple allocation periods. A service may get no bandwidth in one allocation cycle and more in another. Unlike fixed bandwidth, unused assured bandwidth is available for best-effort use by other traffic flows/subscribers.

Typically, the service is configured with either fixed or assured bandwidth but not both. CLI allows both to be configured. If configured with both, the fixed plus assured bandwidth must be less than the PIR and both fixed and assured count toward the total PON CIR bandwidth.

8.4 Provisioning using CLI

8.4.1 Downstream Shaper

To provision the downstream shaper, complete the following steps:



NOTE

Provisioning downstream shapers is not required for normal operation.

1. Access the Global Configuration Command Set.
`ChassisID#configure terminal`
2. Access the Shaper Configuration Command Set.
`ChassisID(config)#shaper WORD <shelf/slot>`
3. Configure the shaped traffic that egresses at a rate up to the value specified.
`ChassisID(config-shaper name x/x)#rate <m-n>`
4. Attach the shaper to the selected GPON ONT port and configure a list of queues on the interface to shape.
`ChassisID(config-shaper name x/x)#per remote-device <ont-id>@<shelf/slot/port>.gpon queue [LIST|<0-7>]`
5. Enable the shaper.
`ChassisID(config-shaper name x/x)#no shutdown`
6. Return to the Global Configuration Command Set.
`ChassisID(config-shaper name x/x)#exit`

8.4.2 Downstream Shaper for Multiple Customers

To provision the downstream shaper for multiple customers, complete the following steps:



NOTE

Provisioning the shaper is not required for normal operation.

8.4.2.1 P-Bit to Queue Mapping

1. Access the Global Configuration Command Set.
`ChassisID#configure terminal`
2. Create a QoS map profile.
`ChassisID(config)#qos map-profile WORD`
3. Map the p-bit to the selected queue.
`ChassisID(config qos-map profile name)#p-bit X queue Y`

8.4.2.2 EVC Map to QoS Map

1. Access the Global Configuration Command Set.
`ChassisID#configure terminal`
2. Access the EVC Map Configuration Command Set.
`ChassisID(config)#evc-map WORD <shelf/slot>`

3. Connect the EVC-Map to a QoS map profile.

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

**NOTE**

The EVC Map still needs to be connected to an EVC and an UNI to function properly.

8.4.2.3 Queue Scheduling

1. Access the Global Configuration Command Set.

```
ChassisID#configure terminal
```

2. Enter the configuration mode for the selected CoS queue.

```
ChassisID(config)#queue remote-device <ont-id>@<shelf/slot/port>.gpon [LIST|<0-7>]
```

3. Group the CoS queue (X) and the CoS queue under it (X-1) in the same WFQ.

```
ChassisID(config-queue x@x/x/x)#cos group lower-adjacent
```

4. Set the weight that this queue (X) will have for the WFQ.

```
ChassisID(config-queue x@x/x/x)#weight Y
```

**NOTE**

To ungroup queue X from the WFQ, set its CoS back to X using the following command:

```
ChassisID(config-queue x@x/x/x)#cos X
```

8.4.3 Upstream Shaper

To provision the upstream shaper, complete the following steps:

1. Access the Global Configuration Command Set.

```
ChassisID#configure terminal
```

2. Access the Shaper Configuration Command Set.

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

3. Configure the shaper traffic that egresses at a rate up to the value specified.

```
ChassisID(config-shaper name x/x)#rate <m-n>
```

4. Provision the assured bandwidth.

```
ChassisID(config-shaper name x/x)#gpon channel assured-bandwidth <0,64-1244160>
```

5. Provision the fixed bandwidth.

```
ChassisID(config-shaper name x/x)#gpon channel fixed-bandwidth <0,64-1244160>
```

6. Attach the shaper to the required upstream channel.

**NOTE**

ADTRAN supports four upstream shapers per ONT, but these must be connected to different channels. The interface maps are not restricted to one map to one shaper, but it could be multiple interface maps to one shaper. The Total Access 5000 GPON 2.5G 2-Port Access Module (P/N 1187500E1) does not support multiple upstream shaper channels.

```
ChassisID(config-shaper name x/x)#per interface gpon <ont-id/0/
port>@<shelf/slot/port> channel <1-4>
```

7. Enable the shaper.

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

8. Return to the Global Configuration Command Set.

```
ChassisID(config-shaper name x/x)#exit
```

8.4.3.1 Upstream Shaping Example



NOTE

- The interface is the GPON interface, not the ethernet interface. For multiple upstream shapers on the same ONT, the interface will be the same, but the channel will be different.
- The channel makes a distinction between the two upstream shapers.
- The **connect gpon upstream channel <1-4>** command is added to the EVC Map. It connects the upstream shaper to the EVC Map.

```
shaper "11_downstream" 1/13
per remote-device 11@1/13/1.gpon queue 0
rate 200000
gpon channel assured-bandwidth 0
gpon channel fixed-bandwidth 0
no shutdown

shaper "11_upstream_ch1" 11@1/13/1.gpon
per interface gpon 11/0/1@1/13/1.gpon channel 1
rate 1024
gpon channel assured-bandwidth 0
gpon channel fixed-bandwidth 0
no shutdown

shaper "11_upstream_ch2" 11@1/13/1.gpon
per interface gpon 11/0/1@1/13/1.gpon channel 2
rate 1024
gpon channel assured-bandwidth 0
gpon channel fixed-bandwidth 0
no shutdown

evc-map "11_p1_data" 1/13
connect evc "AUTOGEN_101_0"
connect uni gigabit-ethernet 11/0/1@1/13/1.gpon
connect gpon upstream channel 1
subscriber access static-ip 192.168.1.241 00:00:00:00:00:00 192.168.1.254
00:00:00:00:00:00
men-pri 4
men-c-tag-pri 0
subscriber access dhcpv6 relay-agent mode disable
no shutdown

evc-map "11_p2_data" 1/13
connect evc "AUTOGEN_101_0"
connect uni gigabit-ethernet 11/0/2@1/13/1.gpon
connect gpon upstream channel 2
subscriber access static-ip 192.168.1.242 00:00:00:00:00:00 192.168.1.254
00:00:00:00:00:00
```

```
men-pri 0
men-c-tag-pri 0
subscriber access dhcpv6 relay-agent mode disable
no shutdown
```

8.4.3.2 Downstream GPON QoS for User Fairness

Figure 8-2 provides an example of an alternative QoS model. This model provides per service rate guarantees for each SFU ONT on the PON.

Two rates Min-Rate and PIR are specified for the queue associated with the high-speed internet access (HSIA) traffic class for each ONT.



NOTE

The rates are actually specified in a shaper associated with a queue.

The design allows the ability to also provision an optional PIR for the queue associated with the Video on Demand (VoD) traffic class.

The PIR is the peak rate possible for a given queue provided there is enough bandwidth left on the PON. The Min-Rate is a minimum rate provided under the condition there is enough bandwidth left on the PON after servicing the higher priority traffic classes.

The aggregate Min-Rate for HSIA cannot be oversubscribed on a PON. Min-Rate is used to derive corresponding internal PON level weight used by the PON level scheduler for HSIA traffic. The PON weight will be selected such that the HSIA traffic is provided Min-Rate bandwidth when the PON is congested and there is enough bandwidth after accounting for higher priority traffic classes.

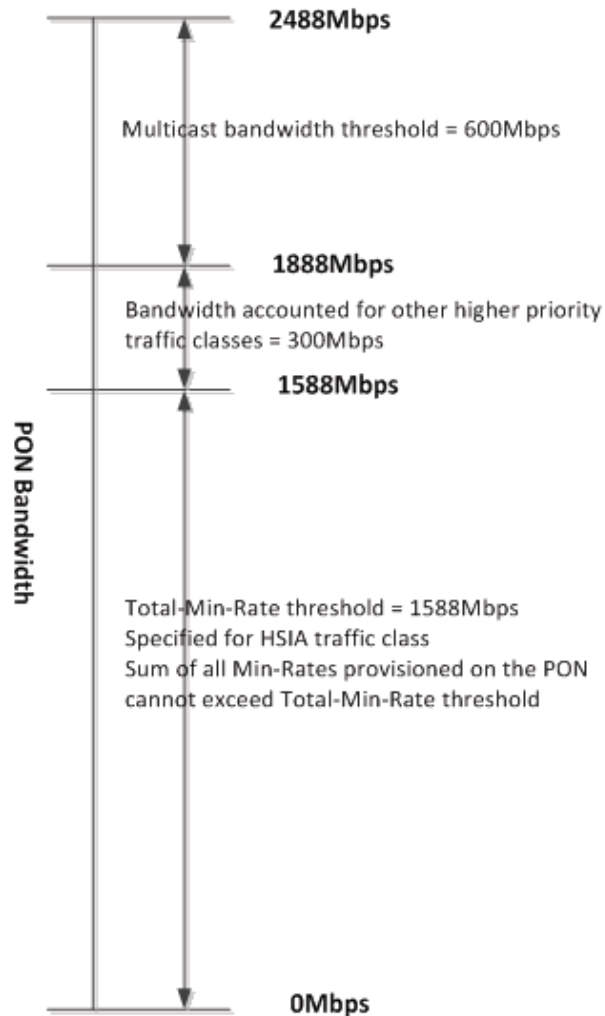


Figure 8-2. Per PON Bandwidth Thresholds Example

A PON level threshold - Total Minimum Rate Threshold must be provisioned. This is the sum of all Min-rates provisioned on the PON. This threshold must be provisioned at the Total Access 5000 node commissioning time (or new OLT installation time) prior to provisioning any subscriber services. By default, the threshold is set to full GPON bandwidth (2488 Mbps). The operator is expected to set it to a value less than or equal to 2488 Mbps - Multicast bandwidth threshold.

8.4.3.2.1 Total Minimum Rate Threshold Provisioning

To provision the total minimum rate threshold, complete the following:



NOTE

GPON QoS is only supported on the GPON OLT 8X SFP Access Module (P/N 1187503F1) and the 8-Port OLT 2nd Generation (P/N 1187503F2). It is not supported on any other GPON Access Modules.

1. Access the Global Configuration Command Set.
ChassisID#**configure terminal**
2. Provision the shaper on the selected OLT module.
ChassisID(config)#**interface gpon <shelf/slot/port>**
3. Set the total minimum rate threshold on the PON.
ChassisID(config-gpon x/x/x)#**thresholds total-min-rate <0-n>**

8.4.3.2.2 Per Service Model

The Single Subscriber Per ONT model provides per subscriber rate guarantees for each ONT on the PON. The min-rate (assured rate) and PIR (maximum rate) can be set for the aggregate output of these queues for each ONT. The sum of all the min-rates on the PON cannot exceed the total min-rate threshold value provisioned on the GPON interface. This ensures that min-rate cannot be oversubscribed on a PON, although the PIR can still be oversubscribed on the PON. During congestion, bandwidth will be allocated to the ONT based on the subscribed min-rate.

The shaper is associated with an input queue on a particular ONT's traffic management block.

To specify the Minimum Rate to a downstream shaper, complete the following:

1. Access the Global Configuration Command Set.
ChassisID#**configure terminal**
2. Access the Shaper Configuration Command Set.
ChassisID(config)#**shaper WORD <shelf/slot>**
3. Configure the shaper traffic that egresses at a rate up to the value specified in kbps.
ChassisID(config-shaper name x/x)#**rate <m-n>**
4. Set the new minimum rate parameter in kbps.
ChassisID(config-shaper name x/x)#**min-rate <0-n>**
The OLT ensures the total minimum rate configured on the downstream shapers on a PON cannot exceed the total minimum rate threshold.
Provisioning will be rejected if the total minimum rates on the downstream shapers exceed the total minimum rate threshold on the GPON interface.
5. Attach the shaper to the selected GPON ONT port and configure a list of queues on the interface to shape.
ChassisID(config-shaper name x/x)#**per remote-device <ont-id>@<shelf/slot/port>.gpon queue [LIST|<0-7>]**

6. Enable the shaper.

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

7. Verify the configuration of the Total Minimum Threshold on the GPON interface and the sum of the shaper Minimum Rates.

```
ChassisID(config-shaper name x/x)#do show interface gpon <shelf/slot/port>
```

**NOTE**

The show interface gpon <shelf/slot/port> command also shows how much Minimum Rate bandwidth is still available.

```
gpon 1/2/1 is IS and up
Number of Configured ONTs      : 7
Number of Discovering ONTs     : 1
Number of Unrecognized ONTs    : 0
Number of Operational ONTs     : 6
Number of Available HW Resour  : 959
```

**NOTE**

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

```
Longest Fiber Distance      : ont-12, 230m
Shortest Fiber Distance     : ont-2, 162m
Oversubscription Allowed    : true
Multicast CAC Status        : admitting
DS Total-min-rate thresh kbps : 540000
```

**NOTE**

DS Total-min-rate thresh kbps shows what is configured for 'thresholds total-min-rate'

	Downstream	Upstream
Max Provisionable BW	kbps : 2488320	1244160
Configured PIR BW	kbps : 11000000	0
Configured Fixed BW	kbps : na	0
Configured Assured BW	kbps : na	0
Configured min-rate BW	kbps : 380000	na

**NOTE**

Configured min-rate BW shows the sum of the configured 'min-rate' commands on the shapers

Available PIR BW	kbps : 2488320	1244160
Available CIR BW	kbps : na	1153872
Available min-rate BW	kbps : 160000	na

**NOTE**

Available min-rate BW shows 'thresholds total-min-rate' minus sum of configured 'min-rate' commands on shapers

Current PIR BW	kbps : 10999989	7488
Current CIR BW	kbps : na	13008

8.4.3.2.3 Single Subscriber Per ONT Model Example

Figure 8-3 displays downstream QoS for the single subscriber per ONT model.

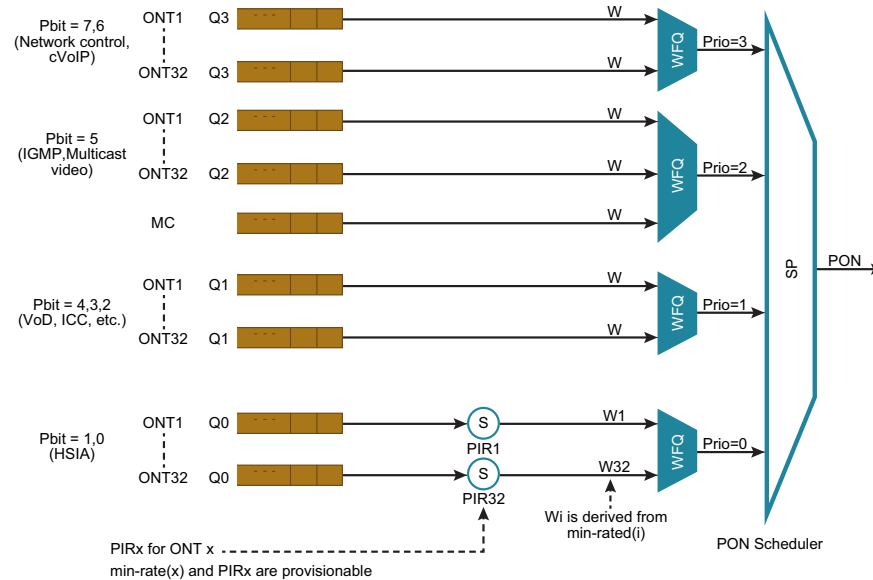


Figure 8-3. Downstream QoS for Single Subscriber

The WFQ is applied per priority group so downstream traffic for all ONTs on the PON are in the WFQ for each priority queue.

The following example configuration is for the single subscriber per ONT model. Downstream traffic with a P-bit of 0 is placed in queue 0. Downstream traffic with a P-bit of 1 is placed in queue 1. For this example, only queue 0 and queue 1 are shaped so the min-rate and PIR will only apply to those queues.

```

evc-map "s2-01-data" 1/2
  connect evc "DATA_1201"
  connect uni gigabit-ethernet 1/0/1@1/2/1.gpon
  men-pri 0
  men-c-tag-pri 0
  no shutdown

evc-map "s2-02-data" 1/2
  connect evc "DATA_1202"
  connect uni gigabit-ethernet 2/0/1@1/2/1.gpon
  men-pri 0
  men-c-tag-pri 0
  no shutdown

evc-map "s2-03-data" 1/2
  connect evc "DATA_1203"
  connect uni gigabit-ethernet 3/0/1@1/2/1.gpon
  men-pri 0
  men-c-tag-pri 0
  no shutdown

```

```
evc-map "s2-04-data" 1/2
  connect evc "DATA_1204"
  connect uni gigabit-ethernet 4/0/1@1/2/1.gpon
  men-pri 0
  men-c-tag-pri 0
  no shutdown

evc-map "s2-05-data" 1/2
  connect evc "DATA_1205"
  connect uni gigabit-ethernet 5/0/1@1/2/1.gpon
  men-pri 0
  men-c-tag-pri 0
  no shutdown

evc-map "s2-06-data" 1/2
  connect evc "DATA_1206"
  connect uni gigabit-ethernet 6/0/1@1/2/1.gpon
  men-pri 0
  men-c-tag-pri 0
  no shutdown

qos cos-map 0 0 1
qos cos-map 1 2 3
qos cos-map 2 4 5
qos cos-map 3 6 7

queue remote-device 1@1/2/1 0
  cos 0
  weight 100

queue remote-device 2@1/2/1 0
  cos 0
  weight 100

queue remote-device 3@1/2/1 0
  cos 0
  weight 100

queue remote-device 4@1/2/1 0
  cos 0
  weight 100

queue remote-device 5@1/2/1 0
  cos 0
  weight 100

queue remote-device 6@1/2/1 0
  cos 0
  weight 100

interface gpon 1/2/1
  thresholds total-min-rate 600000
  no shutdown

shaper "01_downstream" 1/2
  per remote-device 1@1/2/1.gpon queue 0
  rate 1000000
  min-rate 150000
  no shutdown
```

```
shaper "02_downstream" 1/2
  per remote-device 2@1/2/1.gpon queue 0
  rate 1000000
  min-rate 150000
  no shutdown

shaper "03_downstream" 1/2
  per remote-device 3@1/2/1.gpon queue 0
  rate 1000000
  min-rate 100000
  no shutdown

shaper "04_downstream" 1/2
  per remote-device 4@1/2/1.gpon queue 0
  rate 1000000
  min-rate 100000
  no shutdown

shaper "05_downstream" 1/2
  per remote-device 5@1/2/1.gpon queue 0
  rate 1000000
  min-rate 50000
  no shutdown

shaper "06_downstream" 1/2
  per remote-device 6@1/2/1.gpon queue 0
  rate 1000000
  min-rate 50000
  no shutdown
```

8.4.3.2.4 Example Scenario

Figure 8-4 displays 3 ONTs using UvClass 12, 13, and 16G subscriber profiles. The Minimum Rates provisioned for these ONTs are 35M, 45M, and 55M, respectively. The PIRs provisioned for those ONTs are 49.5M, 82.5M, and 300M, respectively. The operator provisions the weights 90 for Q1 and 10 for Q0.

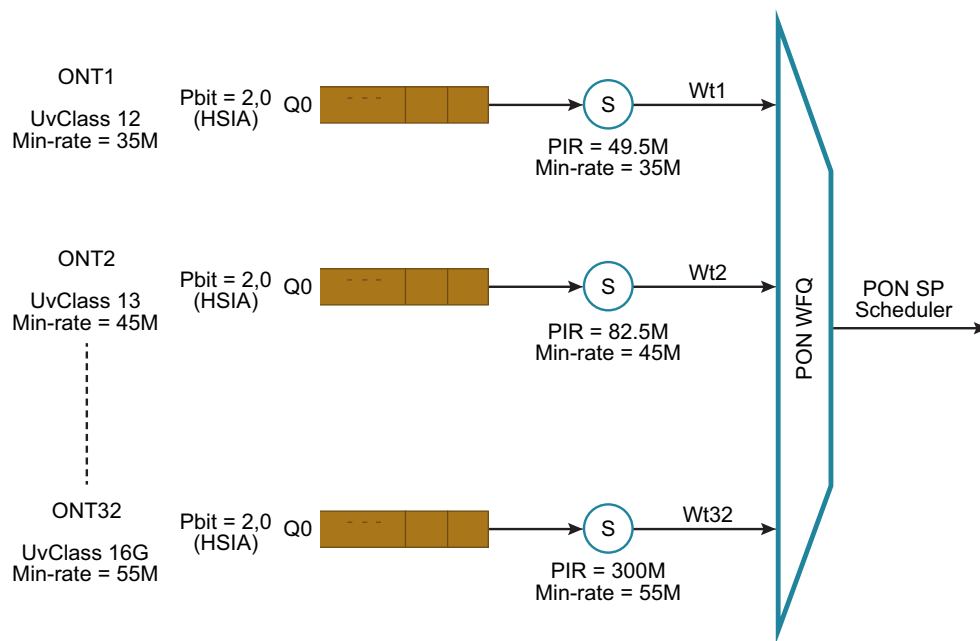


Figure 8-4. Example Provisioning of Weights and Minimum Rates

Assuming the PIR rates are not reached, bandwidth is allocated on the PON based on the weights Wt^i . In terms of rate guarantees, examine both congested and uncongested examples.

Scenario 1 - Congested PON

Since the Minimum Rate derived weights are applied at the PON level, Minimum Rate is guaranteed for each ONT when ALL ONTs have traffic to send provided the higher priority traffic classes (Q3, Q2, and Q1 traffic) is negligible. If all the ONTs are sending data at rates more than their respective Minimum Rates, every ONT will get bandwidth equal to the provisioned Minimum Rate.

[Table 8-2](#) considers a fully populated PON with 32 active ONTS, even if not listed explicitly.

Table 8-2. Congested PON Example 1

Description	Rate
ONT1 HSIA Bandwidth	35M
ONT2 HSIA Bandwidth	45M
ONT3-32 HSIA Bandwidth	-
ONT32 HSIA Bandwidth	55M

Scenario 2 - Congested PON

If the actual available bandwidth for HSIA is less than the sum of Minimum Rates of the active ONTs, the bandwidth is distributed among the ONTs in proportion to their Minimum Rates. In this case, each ONT will get less than its Min-Rate for its HSIA traffic. This is due to the higher priority traffic classes taking up more than their budgeted bandwidth.

[Table 8-3](#) considers a fully populated PON with 32 active ONTS, even if not listed explicitly.

Table 8-3. Congested PON Example 2

Description	Rate
Total Line Rate	2488M
Total MC Bandwidth Threshold	1000M
Total MC Bandwidth (Actual)	1000M
Non-MC High Priority Traffic Class Bandwidth (Budgeted)	300M
Total Minimum Rate Threshold	1188M
Actual Available Bandwidth for HSIA	88M

Table 8-3. Congested PON Example 2 (Continued)

Description	Rate
ONT1 HSIA Bandwidth - (Minimum Rate = 35M, PIR = 300M)	= Lower {Wt1/?Wti of actual available HSIA bandwidth, PIR1} = Lower {~22M, 300M} = ~22M
ONT2 HSIA bandwidth (Min-rate = 45M, PIR = 1000M)	= Lower { Wt2/?Wti of actual available HSIA bandwidth, PIR2} = Lower {~29M, 1000M} = ~29M
ONT32 HSIA bandwidth (Min-rate = 55M, PIR = 1000M)	= Lower { Wt32/?Wti of actual available HSIA bandwidth, PIR32} = Lower {~36M, 1000M} = ~37M

Scenario 3 - Uncongested PON

If the actual available bandwidth for HSIA is more than the sum of Min-Rates (and even if it is less than the Total-Min-Rate threshold), the bandwidth is distributed among the ONTs in proportion to their Min-Rates. In this case, each ONT will get more than its Min-Rate for its HSIA traffic.

Table 8-4 considers a fully populated PON with 32 active ONTS, even if not listed explicitly.

Table 8-4. Uncongested PON Example 1

Description	Rate
Total Line Rate	2488M
Total MC Bandwidth Threshold	1000M
Non-MC High Priority Traffic Class Bandwidth (Budgeted)	300M
Non-MC High Priority Traffic Class Bandwidth (Actual)	600M
Total Minimum Rate Threshold	1188M
Actual Available Bandwidth for HSIA	888M
ONT1 HSIA Bandwidth (Minimum Rate = 35M, PIR = 300M)	= Lower {Wt1/?Wti of actual available HSIA bandwidth, PIR1} = Lower {~226M, 300M} = ~226M
ONT2 HSIA bandwidth (Min-rate = 45M, PIR = 1000M)	= Lower { Wt2/?Wti of actual available HSIA bandwidth, PIR2} = Lower {~291M, 1000M} = ~291M
ONT32 HSIA bandwidth (Min-rate = 55M, PIR = 1000M)	= Lower { Wt32/?Wti of actual available HSIA bandwidth, PIR32} = Lower {~371M, 1000M} = ~371M

Scenario 4 - Uncongested PON

If the actual available bandwidth for HSIA is more than the Total-Min-Rate threshold, the bandwidth is distributed among the ONTs in proportion to their Min-Rates. In this case, each ONT will get more than its Min-Rate for its HSIA traffic and some may even reach their peak rates.

Table 8-5 considers a fully populated PON with 32 active ONTS, even if not listed explicitly.

Table 8-5. Uncongested PON Example 2

Description	Rate
Total Line Rate	2488M
Total MC Bandwidth Threshold	1000M
Non-MC High Priority Traffic Class Bandwidth (Budgeted)	300M
Non-MC High Priority Traffic Class Bandwidth (Actual)	0M
Total Minimum Rate Threshold	1188M
Actual Available Bandwidth for HSIA	1488M
ONT1 HSIA Bandwidth (Minimum Rate = 35M, PIR = 300M)	= Lower {Wt1/?Wti of non-MC bandwidth, PIR1} = Lower {~387M, 300M} = ~300M
ONT2 HSIA bandwidth (Min-rate = 45M, PIR = 1000M)	= Lower { Wt2/?Wti of non-MC bandwidth, PIR2} = Lower {~522M, 1000M} = ~522M
ONT32 HSIA bandwidth (Min-rate = 55M, PIR = 1000M)	= Lower { Wt32/?Wti of non-MC bandwidth, PIR32} = Lower {~666M, 1000M} = ~666M

8.4.4 Web



NOTE

Total Access 5000 Release 8.5 does not support configuring downstream QoS using the User Interface.

8.4.4.1 Downstream Shaper Provisioning

To provision the downstream shaper, complete the following steps:



NOTE

Provisioning the shaper is not required for normal operation.

1. Access the Shaper.

GPON OLT > Provisioning > Shaper



NOTE

To create or retrieve a shaper, enter the shaper name and select **Go**.

2. Select **Downstream** for the Shaper Direction.
3. Configure the shaped traffic that egresses at a rate up to the value specified.
4. Attach the shaper to the selected GPON ONT port and configure a list of queues on the interface to shape.
5. Select **Apply** to enable the shaper.

8.4.4.2 Downstream Shaper Provisioning for Multiple Customers

To provision the downstream shaper for multiple customers, complete the following steps:



NOTE

Provisioning the shaper is not required for normal operation.

8.4.4.2.1 P-Bit to Queue Mapping

1. Access the QoS Map Profile.
(active) Switch Module > Provisioning > Network Tab
2. Enter a QoS map profile name and select **Create**.
3. Enter a description.
4. Map the p-bit to the selected queue.
5. Select **Go**.

8.4.4.2.2 EVC Map to QoS Map

1. Access the Interface Map

GPON OLT > Provisioning > Interface Map

2. Connect the EVC Map to a QoS map profile.

GPON OLT > Provisioning > Interface Map > Traffic Classification > QoS Map-Profile > QoS Profile Name



NOTE

The EVC Map still needs to be connected to an EVC and an UNI to function properly.

8.4.4.2.3 Queue Scheduling

1. Access the Queue.

GPON OLT > Provisioning > Queue

2. Select **Explicit** for the method of the selected CoS queue.

3. Group the CoS queue (X) and the CoS queue under it (X-1) in the same WFQ by assigning the same Weight Percent.



NOTE

To ungroup queue X from the WFQ, set its CoS back to X using the following command:
`ChassisID(config-queue x@x/x/x)#cos X`

8.5 Example

The following provides a sample configuration for provisioning shapers.

8.5.1 Step 1: Create Unique Queues for Each Port

```
qos map-profile INET-PORT1
  p-bit 0 queue 0
  p-bit 1-3 queue 4
  p-bit 4-5 queue 5
  p-bit 6 queue 6
  p-bit 7 queue 7

qos map-profile INET-PORT2
  p-bit 0 queue 1
  p-bit 1-3 queue 4
  p-bit 4-5 queue 5
  p-bit 6 queue 6
  p-bit 7 queue 7
```

8.5.2 Step 2: Attach the Downstream Queue Profiles and Upstream Channels to Each Port

```
evc-map INET-PON1-1-ONT1-PORT1
  connect evc INET
  connect uni gigabit-ethernet 1/0/1@1/1/1
  connect qos downstream map-profile INET-PORT1
  connect gpon upstream channel 1
  men-pri 0
  no shutdown

evc-map INET-PON1-1-ONT1-PORT2
  connect evc INET
  connect uni gigabit-ethernet 1/0/2@1/1/1
  connect qos downstream map-profile INET-PORT2
  connect gpon upstream channel 2
  men-pri 0
  no shutdown
```

8.5.3 Step 3: Attach the Downstream Shapers to the Specified Queues from the Map Profiles

```
shaper DOWN-INET-PON1-1-ONT1-PORT1 1/1
  per remote-device gpon 1@1/1/1 queue 0
  rate 10000
  no shutdown

shaper DOWN-INET-PON1-1-ONT1-PORT2 1/1
  per remote-device gpon 1@1/1/1 queue 1
  rate 20000
  no shutdown
```

8.5.4 Step 4: Attach the Upstream Shapers to the Specified Channels

```
shaper UP-INET-PON1-1-ONT1-PORT1 1@1/1/1
  per interface gpon 1/0/1@1/1/1 channel 1
  rate 10000
  no shutdown

shaper UP-INET-PON1-1-ONT1-PORT2 1@1/1/1
  per interface gpon 1/0/1@1/1/1 channel 2
  rate 20000
  no shutdown
```

8.5.5 Attach/Detach Interface to the Shaper

```
(shaper)#shaper "372E_21_DATA_DOWN" 1/4
(shaper)#do show run shaper "372E_21_DATA_DOWN" 1/4
shaper "372E_21_DATA_DOWN" 1/4
  per interface gigabit-ethernet 1/4/1 queue 0
  rate 1000000
  no shutdown

(shaper)#no per interface
(shaper)#do show run shaper "372E_21_DATA_DOWN" 1/4
shaper "372E_21_DATA_DOWN" 1/4
  rate 1000000
  no shutdown

(shaper)#per remote-dev 1@1/4/1 queue 0
(shaper)#do show run shaper "372E_21_DATA_DOWN" 1/4
shaper "372E_21_DATA_DOWN" 1/4
  per remote-device 1@1/4/1.gigabit-ethernet queue 0
  rate 1000000
  no shutdown

(shaper)#no per remote-device 1@1/4/1.gigabit-ethernet queue 0
(shaper)# per interface gigabit-ethernet 1/4/1 queue 0
(shaper)#do show run shaper "372E_21_DATA_DOWN" 1/4
shaper "372E_21_DATA_DOWN" 1/4
  per interface gigabit-ethernet 1/4/1 queue 0
  rate 1000000
  no shutdown
```

8.6 Shapers, AE (Example)

Shaping is a mechanism used at egress to smooth out bursts of traffic. Unlike a policer, which discards large bursts of traffic, shapers work on queues. The bursts in traffic can appear smoothed because of the queue function. The shaper acts more like a rate limiter. The port shaper uses a token bucket (much like a policer); however, when large bursts are received, the packets are delayed rather than discarded immediately. When a packet arrives at the shaper, if there are sufficient tokens available, the packet is transmitted without delay. If there are insufficient tokens in the bucket, the packet is delayed until there are enough tokens in the bucket to allow transmission.

The benefit of a shaper is that it will not drop frames with a small burst of traffic, but it does potentially add latency (delay).

8.6.1 Provisioning

The Active Ethernet FTTP application supports downstream and upstream shapers. In downstream, the shapers are per priority queue per port. In upstream, the shapers are per ONT.

8.6.1.1 CLI

8.6.1.1.1 Downstream Shaper Provisioning

Shapers are applied per physical port. To provision the shaper parameters, complete the following steps:



NOTE

Provisioning the downstream shaper is not required for normal operation.

1. Access the Shaper Configuration prompt.

```
ChassisID(config)#shaper WORD <shelf/slot>
```

2. Configure the shaped traffic that egresses at a rate up to the value specified.

```
ChassisID(config-shaper name x/x)#rate <0-n>
```

3. Attach the shaped traffic to the gigabit-ethernet interface.



NOTE

The shaper can be attached to a single queue on a port (e.g. queue 5) or to all the queues on a port (e.g. queue 0-7). The shaper can NOT be attached to a subset of queues on a port (e.g. queue 0-4). Two different shapers can be attached to two different queues on the same port.

```
ChassisID(config-shaper name x/x)#per interface gigabit-ethernet
<shelf/slot/port> queue [LIST|<0-7>]
```

4. Enable the shaper.

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

5. Return to the Global Configuration prompt.

```
ChassisID(config-shaper name x/x)#exit
```

8.6.1.1.2 Upstream Shaper Provisioning

Upstream Shapers are applied per ONT. To provision the upstream shaper parameters, complete the following steps:

**NOTE**

Provisioning the upstream shaper is not required for normal operation.

1. Access the Shaper Configuration prompt.

```
ChassisID(config)#shaper WORD <1@shelf/slot/port>
```

2. Configure the shaped traffic that egresses at a rate up to the value specified.

```
ChassisID(config-shaper name x/x)#rate <0-n>
```

3. Attach the shaped traffic to the ONT.

The gigabit-ethernet index **must** be the same as the index in step 1.

**NOTE**

The shaper will be attached on ALL queues for the ONT. There is no per-queue shaping options for upstream shaping. Only one upstream shaper per ONT is allowed.

```
ChassisID(config-shaper name x/x)#per interface gigabit-ethernet  
<1@shelf/slot/port>
```

4. Enable the shaper.

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

5. Return to the Global Configuration prompt.

```
ChassisID(config-shaper name x/x)#exit
```

8.6.2 Web

8.6.2.1 Downstream Shaper Provisioning

Shapers are applied per physical port. To provision the shaper parameters, complete the following steps:



NOTE

Provisioning the downstream shaper is not required for normal operation.

1. Access the Shaper.

AE 24-Port > Provisioning > Shaper



NOTE

To create or retrieve a shaper, enter the shaper name and select **Go**.

2. Assign a unique name to the shaper.
3. Select the **Go** button.
4. Select **Downstream** for the Shaper Direction.
5. Configure the shaped traffic that egresses at a rate up to the value specified.
6. Attach the shaped traffic to the gigabit-ethernet interface.



NOTE

The shaper can be attached to a single queue on a port (e.g. queue 5) or to all the queues on a port (e.g. queue 0-7). The shaper can NOT be attached to a subset of queues on a port (e.g. queue 0-4). Two different shapers can be attached to two different queues on the same port.

7. Select **Apply** to enable the shaper.

8.6.2.2 Upstream Shaper Provisioning

Upstream Shapers are applied per ONT. To provision the upstream shaper parameters, complete the following steps:



NOTE

Provisioning the upstream shaper is not required for normal operation.

1. Access the Shaper.

AE 24-Port > Provisioning > Shaper



NOTE

To create or retrieve a shaper, enter the shaper name and select **Go**.

2. Assign a unique name to the shaper.
3. Select the **Go** button.
4. Select **Upstream** for the Shaper Direction.
5. Configure the shaped traffic that egresses at a rate up to the value specified.
6. Attach the shaped traffic to the ONT.



NOTE

The shaper will be attached on ALL queues for the ONT. There is no per-queue shaping options for upstream shaping. Only one upstream shaper per ONT is allowed.

7. Select **Apply** to enable the shaper.

8.7 Policers, AE (Example)

Policing is a rate-based admission control function that uses a leaky/token bucket algorithm. The purpose of a policer is to keep non-conforming traffic from entering the network and degrading other customers and/or services.

8.7.1 Provisioning

8.7.1.1 CLI

The policer can be used to limit bandwidth in specified traffic flows. To provision for policing, complete the following steps:



NOTE

The policer is not required for normal operation.

1. Access the Policer Configuration prompt.

```
ChassisID(config)#policer WORD <shelf/slot>
```

2. Configure the committed information rate (CIR) in kbps.

The CIR is the rate up to which service frames are delivered according to the service performance objectives.

```
ChassisID(config-policer name x/x)#cir <0-n>
```

3. Configure the committed burst size (CBS).

The CBS is the maximum available bytes for a burst of ingress traffic sent at the port speed while still conforming to the CIR.

```
ChassisID(config-policer name x/x)#cbs <0-n>
```

4. Configure the excess information rate (EIR) in kbps.

```
ChassisID(config-policer name x/x)#eir [<0-n>|max-bandwidth]
```

5. Configure the excess burst size (EBS).

The EBS is the maximum available bytes for a burst of ingress traffic sent at the port speed while still conforming to the EIR.

```
ChassisID(config-policer name x/x)#ebs <0-n>
```

6. Set the EVC ingress. The EVC ingress represents upstream to the customer.

```
ChassisID(config-policer name x/x)#per custom evc-map WORD ingress
```

7. Enable the Policer.

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

8. Return to the Global Configuration prompt.

```
ChassisID(config-policer name x/x)#exit
```

8.7.2 Web

The policer can be used to limit bandwidth in specified traffic flows. To provision for policing, complete the following steps:



NOTE

The policer is not required for normal operation.

1. Access the Policer.

AE 24-Port > Provisioning > Policer



NOTE

To create or retrieve a policer, enter the shaper name and select **Go**.

2. Assign a unique name to the policer.
3. Select the **Go** button.
4. At the Per Custom evc-map, assign an EVC Map to this policer.
5. Configure the committed information rate (CIR) in kbps.

The CIR is the rate up to which service frames are delivered according to the service performance objectives.

6. Configure the committed burst size (CBS).

The CBS is the maximum available bytes for a burst of ingress traffic sent at the port speed while still conforming to the CIR.

7. Configure the excess information rate (EIR) in kbps.

8. Configure the excess burst size (EBS).

The EBS is the maximum available bytes for a burst of ingress traffic sent at the port speed while still conforming to the EIR.

9. Set the EVC ingress. The EVC ingress represents upstream to the customer.

10. Select **Apply** to enable the Policer.

9 SFP Information

9.1 Scope of this Section

This section provides the command to display the CLEI code information of an installed SFP in the selected GPON OLT.

9.2 In this Section

This section contains the topics listed in [Table 9-1](#).

Table 9-1. Section 9 Topics

Sub-Section	Topic	See Page
9.3	Information Command	362

9.3 Information Command

To display the CLEI code information, use the following command:

ChassisID#show interfaces gpon <shelf/slot/port> pluggable

9.3.1 Example

The following example displays the CLEI code information of the SFP installed in port 1 of the OLT installed in slot 5 of the Total Access 5000.

ChassisID#show interfaces gpon 1/5/1 pluggable

gpon pluggable port 1/5/1 is Up

Pluggable Type	: SFP
Pluggable Connector Type	: Fiber SC
Capabilities	: Pluggable/VOLTAGE Readable
Port Status	: Present/Valid/ADTRAN Supported/Tx Enabled
Vendor Name	: ADTRAN
Vendor Part Number	: 1442530G1
Vendor Serial Number	: X11-04-001034
ADTRAN CLEI	: BVL3AHFDAA
Tx Power	: 30 tenths of dBm
Tx Bias	: 18 milliAmps
Temperature	: 37 Celsius
Voltage	: 3
Alarms	:

10 3rd Party ONT Provisioning for Active Ethernet

10.1 Scope of this Section

This section provides the minimum steps required for third party ONT provisioning for an Active Ethernet (AE) deployment. It also provides an example deployment.

10.2 In this Section

This section contains the topics listed in [Table 10-1](#).

Table 10-1. Section 10 Topics

Sub-Section	Topic	See Page
10.3	“Provisioning”	364

10.3 Provisioning

It is assumed that the ONT will be provisioned independently of the OLT. The new provisioning of the EVC Map is available through the Total Access 5000 CLI and **not** through AOE or the user interface. Also, for these applications the following limitations are still to be addressed:

- Match untagged, match multicast, and match unicast operation for EVC Maps
- Inheriting the vlan priority bits in the CE-VLAN to use as the vlan priority bits in the S-tag
- S-tag priority bits for a flow can only be set with the **men-pri** command
- The operation of the **mac limit** command has not been fully verified
- EVC Map must be connected to an EVC with **preserve-ce-vlan** disabled
- A feature that allows a user to move any Ethernet Device that has been successfully authenticated using DHCP between different ports of an ADTRAN AE or GPON ONT. This move would be done without requiring the manual intervention in the OLT/ONT by the installer. It should be noted that ONT ports must be provisioned for their specific service (either multicast and/or unicast). For example, if an Ethernet device is moved from a multicast port to a unicast only port, it cannot be expected to function. It is assumed that the installer is moving between ports with similar provisioning. The only function required by the user will be a resetting of the Ethernet Device. If the single ONT is used in a multi-dwelling unit application, then this feature removes the protection against mac-spoofing.

The AE deployment supports connecting to third party ONTs that are managed from a separate server. To provision a third party ONT for AE deployment, complete the following steps:

1. Attach the third party ONT to a front panel port on the Active Ethernet 24-Port Access Module.
2. Access the Global Configuration Command Set.
`ChassisID#configure terminal`
3. Access the Gigabit-Ethernet Interface Configuration Command Set.
`ChassisID(config)#interface gigabit-ethernet <shelf/slot/port>`
4. Provision the port speed to match the installed SFP.
`ChassisID(config-giga-eth x/x/x)#speed [100|1000]`
5. Enable the port.
`ChassisID(config-giga-eth x/x/x)#no shutdown`
6. Provision the EVCs (voice, data, and video) for the ONT.
7. Provision the EVC Maps similar to what is done for an ADTRAN ONT, but connect the UNI interface to the OLT front panel port attached to the third party ONT.
`ChassisID(config-evc-map name x/x)#connect uni gigabit-ethernet <shelf/slot/port>`
8. If multiple EVC Maps share the same UNI, set the EVC Map to match the CE-VLAN.
`ChassisID(config-evc-map name x/x)#match ce-vlan-id <0-4094>`

10.3.1 Example Provisioning

In this example the following VLANs are used for the various services in the network:

- DATA = 90
- VIDEO = 115
- VOICE = 116
- Management = 200

It is assumed that the ONT will be configured to expect these services on the same VLANs, except for management. In this example, it is assumed that the ONT sends/receives management traffic untagged. The expected configuration of the ONT determines the '**match ce-vlan-id ***' commands. In this case, since management is not tagged that evc-map will not have a match criteria.

1. Provision the gigabit-ethernet ports attached to the 3rd party ONT.

```
ChassisID#configure terminal
ChassisID(config)#interface gigabit-ethernet 1/3/1
ChassisID(config-giga-eth 1/1/1)#speed 1000
ChassisID(config-giga-eth 1/1/1)#no shutdown
ChassisID(config-giga-eth 1/1/1)#exit
```

2. Create an EVC for each service.

```
ChassisID(config)#evc data-evc
ChassisID(config-evc data-evc)#s-tag 90
ChassisID(config-evc data-evc)#connect men-port default-ethernet
ChassisID(config-evc data-evc)#mac-switched
ChassisID(config-evc data-evc)#no preserve-ce-vlan
ChassisID(config-evc data-evc)#no shutdown
ChassisID(config-evc data-evc)#exit
```

```
ChassisID(config)#evc video-evc
ChassisID(config-evc video-evc)#s-tag 115
ChassisID(config-evc video-evc)#connect men-port default-ethernet
ChassisID(config-evc video-evc)#mac-switched
ChassisID(config-evc video-evc)#no preserve-ce-vlan
ChassisID(config-evc video-evc)#no shutdown
ChassisID(config-evc video-evc)#exit
```

```
ChassisID(config)#evc voice-evc
ChassisID(config-evc voice-evc)#s-tag 116
ChassisID(config-evc voice-evc)#connect men-port default-ethernet
ChassisID(config-evc voice-evc)#mac-switched
ChassisID(config-evc voice-evc)#no preserve-ce-vlan
ChassisID(config-evc voice-evc)#no shutdown
ChassisID(config-evc voice-evc)#exit
```

```
ChassisID(config)#evc mgmt-evc
ChassisID(config-evc mgmt-evc)#s-tag 200
ChassisID(config-evc mgmt-evc)#connect men-port default-ethernet
ChassisID(config-evc mgmt-evc)#mac-switched
ChassisID(config-evc mgmt-evc)#no preserve-ce-vlan
ChassisID(config-evc mgmt-evc)#no shutdown
ChassisID(config-evc mgmt-evc)#exit
```

3. Set up per-EVC, per-slot IGMP Settings on both the Active Ethernet 24-Port Access Module and GigE SM (proxy mode used in this example).

```
ChassisID(config)#ip igmp evc video_evc 1/3 proxy host ip address
10.20.200.1
```

```
ChassisID(config)#ip igmp evc video_evc 1/3 mode proxy
```

```
ChassisID(config)#ip igmp evc video_evc 1/A proxy host ip address
10.20.200.1
```

```
ChassisID(config)#ip igmp evc video_evc 1/A mode proxy
```

4. Create an EVC Map per customer (ONT) for each service.

a. Create the video EVC Map.

```
ChassisID(config)#evc-map video_map_cust1 1/3
```

```
ChassisID(config-evc-map video_map_cust1 1/3)#connect evc video_evc
```

```
ChassisID(config-evc-map video_map_cust1 1/3)#connect uni gigabit-
ethernet 1/3/1
```

```
ChassisID(config-evc-map video_map_cust1 1/3)#match ce-vlan-id 115
```

```
ChassisID(config-evc-map video_map_cust1 1/3)#men-pri 5
```

```
ChassisID(config-evc-map video_map_cust1 1/3)#men-c-tag-pri 0
```

```
ChassisID(config-evc-map video_map_cust1 1/3)#subscriber igmp mode
processing-enabled
```

```
ChassisID(config-evc-map video_map_cust1 1/3)#subscriber igmp
immediate-leave
```

```
ChassisID(config-evc-map video_map_cust1 1/3)#subscriber igmp proxy
router ip address 10.20.200.1
```

```
ChassisID(config-evc-map video_map_cust1 1/3)#no shutdown
```

```
ChassisID(config-evc-map video_map_cust1 1/3)#exit
```

b. Create the data EVC Map.

```
ChassisID(config)#evc-map data_map_cust1 1/3
```

```
ChassisID(config-evc-map data_map_cust1 1/3)#connect evc data_evc
```

```
ChassisID(config-evc-map data_map_cust1 1/3)#connect uni gigabit-
ethernet 1/3/1
```

```
ChassisID(config-evc-map data_map_cust1 1/3)#match ce-vlan-id 90
```

```
ChassisID(config-evc-map data_map_cust1 1/3)#men-pri 0
```

```
ChassisID(config-evc-map data_map_cust1 1/3)#men-c-tag-pri 0
```

```
ChassisID(config-evc-map data_map_cust1 1/3)#no shutdown
```

```
ChassisID(config-evc-map data_map_cust1 1/3)#exit
```

c. Create the voice EVC Map.

```
ChassisID(config)#evc-map voice_map_cust1 1/3
```

```
ChassisID(config-evc-map voice_map_cust1 1/3)#connect evc voice_evc
```

```
ChassisID(config-evc-map voice_map_cust1 1/3)#connect uni gigabit-
ethernet 1/3/1
```

```
ChassisID(config-evc-map voice_map_cust1 1/3)#match ce-vlan-id 116
```

```
ChassisID(config-evc-map voice_map_cust1 1/3)#men-pri 7
```

```
ChassisID(config-evc-map voice_map_cust1 1/3)#men-c-tag-pri 0
```

```
ChassisID(config-evc-map voice_map_cust1 1/3)#no shutdown
```

```
ChassisID(config-evc-map voice_map_cust1 1/3)#exit
```

d. Create the management EVC Map.

```
ChassisID(config)#evc-map mgmt_map_cust1 1/3
```

```
ChassisID(config-evc-map mgmt_map_cust1 1/3)#connect evc mgmt_evc
```

```
ChassisID(config-evc-map mgmt_map_cust1 1/3)#connect uni gigabit-
ethernet 1/3/1
```

```
ChassisID(config-evc-map mgmt_map_cust1 1/3)#men-pri 3
```

```
ChassisID(config-evc-map mgmt_map_cust1 1/3)#men-c-tag-pri 0
```

```
ChassisID(config-evc-map mgmt_map_cust1 1/3)#no shutdown
```

```
ChassisID(config-evc-map mgmt_map_cust1 1/3)#exit
```

11 Home Phoneline Networking Alliance

11.1 Scope of this Section

This section provides a brief overview of Home Phoneline Networking Alliance (HPNA), and how to provision for HPNA.

11.2 In this Section

This section contains the topics listed in [Table 11-1](#).

Table 11-1. Section 11 Topics

Sub-Section	Topic	See Page
11.3	"Introduction to HPNA"	368
11.4	"Provisioning"	368

11.3 Introduction to HPNA

HPNA is an alliance of leading technology companies that promote the adoption of a high performance existing-wire home networking standard for applications such as triple-play service. HPNA features guaranteed QOS, remote management and diagnostics. It operates up to 320 Mbps over both coaxial and phone wires.

HPNA utilizes coaxial media and mixed phone/coaxial media for the following:

- Networking over coaxial cable typically used in media servers and Set Top Box (STB) home networking applications
- MUX access over coaxial cables
- Networking over mixed phone wires and coaxial cables for use in FTTP PONs for home networking and multimedia applications

11.4 Provisioning

Data services for HPNA are configured on the OLT.



NOTE

No provisioning is required when setting up HPNA on the ONT. Firmware must be downloaded to the GG3211 during boot-up in order for HPNA to be functional. However, the ONT currently does not support any dynamically configurable options for HPNA.

To provision for HPNA on the OLT, complete the following:

1. Access the Ethernet interface of the OLT.

```
ChassisID(config)#interface gigabit-ethernet 1/0/3@<shelf/slot/port>
```

2. Enable the HPNA interface of the OLT.

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

3. Return to the Enable prompt.

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

4. Verify the provisioning.

```
ChassisID#show interface gigabit-ethernet 1/0/3@<shelf/slot/port>
```

```
giga-eth 18/0/3@1/1/1 is IS and up
```

```
Auto Detect Configuration : Auto-Auto
Maximum MAC Allowed      : 8
Loopback Configuration   : No Loopback
Max Frame Size           : 2000
Pause Time               : 0
PPPoE Filter             : Allow
Power Control            : Disabled
Configuration Status     : 1000 Full
Configuration            : Parent Dependent
Data Communicaton Protocol: DCE
```

	Input Stats	Output Stats
Running Totals:		
Packets	44744494	45001695
Bytes	1407644792	1552135366
Unicasts	44744494	45001693
Broadcasts	0	2

Multicasts	0	0
Errors	0	0
Discards	0	0
Runts	0	
Giants	0	
Frame Errors	0	
CRC Errors	0	

**NOTE**

For a list of additional HPNA status commands, refer to the [Total Access 5000 Series CLI Dictionary](#).

12 IEEE 802.1X

12.1 Scope of this Section

This section provides an overview of the IEEE 802.1X feature, provisioning options, useful show commands, and example provisioning for this feature.



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.

12.2 In this Section

This section contains the topics listed in [Table 12-1](#).

Table 12-1. Section 12 Topics

Sub-Section	Topic	See Page
12.3	“Introduction”	372
12.4	“Provisioning”	375
12.5	“Show Commands”	383
12.6	“Provisioning Examples”	387

12.3 Introduction

Port authentication is used by a network operator to securely verify the intended equipment is installed. The device being validated is called the Supplicant, and is commonly a gateway device installed at the customer site. An access device (such as a DSLAM, OLT, or even an ONT) employs an IEEE 802.1X Authenticator Port Access Entity (PAE) to communicate with the Supplicant using Extensible Authentication Protocol (EAP) messages. The Authenticator PAE on the access device also communicates with a network operator's authentication server (typically a RADIUS server) to perform the authentication.

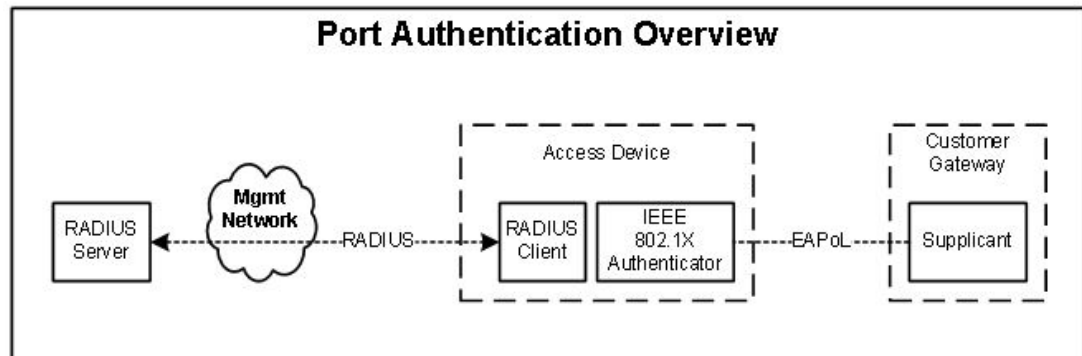


Figure 12-1. Port Authentication Overview

At a high level, the Authenticator PAE on the access device serves as a form of communication bridge for the EAP message exchange between the Supplicant and the Server. The PAE is also responsible for enforcing the authentication status (authorized or unauthorized) to allow or block the customer traffic entering the network.

The information exchanged between the Supplicant and the Server depends on the type of authentication requested by the Server.

12.3.1 Port-Based Authentication

Typically, the Supplicant provides a single Ethernet Medium Access Controller (MAC) that faces the Wide Area Network (WAN). This MAC communicates with the access device via a physical or logical Ethernet connection, such as an EFM-Port, an EFM-Group, or a native Ethernet connection. It is also common for this Supplicant WAN-facing MAC to be a routing interface, which implies that all outbound traffic from this MAC has a single fixed source MAC address.

The IEEE 802.1X standard is designed to manage Authenticators on a per interface basis. The ADTRAN implementation of IEEE 802.1X is consistent with authentication on the basis of physical or logical interface.

The Authenticator PAE on the access device instantiates one Authenticator entity on each of its subscriber-facing Ethernet MAC interfaces (which can be an EFM-Port, EFM-Group, or native Ethernet connection). The Authenticator PAE supports managed objects and maintains authentication state machines on each of these Authenticators. Since there is assumed to be one MAC address per Supplicant port, the access device learns this MAC address from the incoming Extensible Authentication Protocol Over Local Area Network (EAPoL) packets and uses it as a key parameter in the validation and enforcement of the authentication state.

The access device can support multiple services over each Ethernet interface. These services are realized using VLANs to separate the traffic and EVC-Maps as the provisioning model. All

of the services for a given subscriber interface are assumed to be terminated by a single Supplicant MAC, and also a single Supplicant MAC address. The Authentication status (authorized or unauthorized) for the port is enforced equally for all services on that port. If the port is IEEE 802.1X authorized, then all customer traffic is allowed on the MAC address learned from the Supplicant. If the port is IEEE 802.1X unauthorized, then no customer traffic is allowed on that MAC address.

12.3.2 RADIUS Relay Agent

In order to avoid providing public addresses for the RADIUS clients in the network, a RADIUS relay agent can be placed between the RADIUS clients and the RADIUS authentication server. The RADIUS clients communicate with the Authentication server through the RADIUS relay agent.

Each RADIUS client operates the same whether talking directly to the authentication server or to the relay agent. This allows for deployment with or without the relay agent without any changes to the RADIUS client software. The RADIUS client is configured with the IP address and shared secret of the authentication server. The RADIUS relay agent acts as a NAT gateway between the RADIUS client and the authentication server. Optionally, it can also enforce common values for RADIUS message attributes like NAS-Identifier and NAS-IP-Address for all RADIUS messages being sent to the Authentication server.

12.3.2.1 RADIUS Attributes

RADIUS messages can include combinations of the attributes listed in [Table 12-2](#).

Table 12-2. RADIUS Attributes

Attribute	Meaning	Example	RADIUS Messages
Message-Authenticator(80)	RADIUS message authenticator	Per RADIUS RFC	Access-Request Access-Challenge Access-Accept Access-Reject
State(24)	RADIUS message state	Per RADIUS RFC	Access-Request (for challenges) Access-Challenge
User-Name(1)	Supplicant EAP-Identity	Per supplicant	Access-Request Access-Challenge Access-Accept Access-Reject
NAS-IP-Address(4)	RADIUS client IP address (binary)	10.100.42.95	Access-Request
Calling-Station-Id(31)	Supplicant MAC address (ASCII)	00-A0-C8-A7-AC-CE	Access-Request
NAS-Identifier(32)	ASCII TID of the PAE host system	TA5000-Huntsville	Access-Request
EAP-Message(79)	EAP message to/from the Supplicant	N/A	Access-Request (for challenges) Access-Challenge Access-Accept Access-Reject

Table 12-2. RADIUS Attributes (Continued)

Attribute	Meaning	Example	RADIUS Messages
NAS-Port-Id(87)	ASCII identifier of the PAE Access-Request port hosting the Supplicant	eth 1/17/1	Access-Request
Vendor-Specific(26)	Vendor-specific attribute with sub-attributes: ■ Vendor ID (binary) ■ 101: ASCII Vendor name ■ 102: ASCII slot part number	■ Adtran (664) ■ ADTRAN ■ 1187121L1	Access-Request
Session-Timeout(27)	Session timeout (binary). Sets the PAE reauth or supplicant-side timeout	N/A	Access-Accept Access-Challenge
Termination-Action(29)	Termination action (binary). The presence of this attribute is used by the PAE to interpret its response to the Session-Timeout	N/A	Access-Accept Access-Challenge

12.4 Provisioning

To provision for IEEE 802.1X authentication, complete the following.

12.4.1 Step 1: Provision a Subtended Host for RADIUS Client

Provision the subtended host that will be used by the RADIUS client. It is necessary to create an EVC that connects the subtended host to a VLAN and a physical interface that faces the RADIUS server.

1. Create an EVC.

- a. Access the Global Configuration Command Set.

ChassisID#configure terminal

- b. Access the EVC Interface Configuration Command Set.

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

ChassisID(config)#evc WORD

- c. Set the S-tag for the EVC.

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

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

The default interface is set in the Switch Module provisioning.

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

- e. Enable the EVC.

ChassisID(config-evc name)#no shutdown

2. Provision the subtended host.

- a. Access the GPON Interface Configuration Command Set.

ChassisID(config)#interface gpon <shelf/slot/port>

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

ChassisID(config-gpon x/x/x)#subtended-host <ont-id> s-tag <2-4094>

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

ChassisID(config-gpon x/x/x)#subtended-host <ont-id> s-tag-priority <0-7>

- d. Select the method of inband management.

Refer to [Table 12-3](#) for the inband management options.

Table 12-3. Inband Management

Inband	Command	Description
Static IP	<code>ChassisID(config-gpon x/x/x)#subtended-host <ont-id> ip address a.b.c.d a.b.c.d</code>	Set the static IP address and subnet mask for the ONT's inband management. If selected, continue to step e.
DHCP IP	<code>ChassisID(config-gpon x/x/x)#subtended-host <ont-id> ip address dhcp</code>	Allocate the IP address for the ONT's inband management dynamically using DHCP. If selected, continue to step f.

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

`ChassisID(config-gpon x/x/x)#subtended-host <ont-id> ip default-gateway A.B.C.D`

- f. Set the activation mode.

`ChassisID(config-gpon x/x/x)#activation-mode auto-activate`

- g. Enable the OLT interface.

`ChassisID(config-gpon x/x/x)#no shutdown`

- h. 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`

- i. Return to the Global Configuration Command Set.

`ChassisID(config-gpon x/x/x)#exit`

12.4.2 Step 2: Provision a RADIUS Server and Group

To provision a RADIUS server(s) and group, complete the following:

1. Access the RADIUS Server Command Set.

```
ChassisID(config)#port-auth server radius WORD
```

2. Set the IP address of the RADIUS server.

```
ChassisID(config-server-radius radserver)#ip-address A.B.C.D
```

3. Set the shared secret.

```
ChassisID(config-server-radius radserver)#key WORD
```

4. Return to the Global Configuration Command Set.

```
ChassisID(config-server-radius radserver)#exit
```

5. Access the RADIUS Group Command Set.

```
ChassisID(config)#port-auth group radius WORD
```

6. Add the RADIUS server to the RADIUS group.

```
ChassisID(config-group-radius radgroup)#add server WORD sequence-number  
<1-4>
```

7. Set the NAS-Port-ID format.

This provides an interface description format that identifies the physical interface used for authenticating subscribers.



NOTE

For the FTTP application, the NAS Port ID string should end in "\$ontslot\$. \$ontport\$". For example, a suitable NAS Port ID format string would be "PON_1/1/\$slot\$/ \$port\$: \$ont\$. \$ontslot\$. \$ontport\$".

```
ChassisID(config-group-radius radgroup)#nas-port-id WORD
```

8. Return to the Global Configuration Command Set.

```
ChassisID(config-group-radius radgroup)#exit
```

12.4.3 Step 3: Provision the ONT Port

To provision the ONT port, complete the following:

1. Access the interface of the ONT.

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

- 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.
- If using an 1108VP GPON MDU, use efm-port as the selected interface. For all other ONTs, use gigabit-ethernet.

2. Enable the Ethernet interface of the ONT.

```
ChassisID(config-interface x/x/x@x/x/x.gpon)#no shutdown
```

3. Connect the ONT to the selected IP host and RADIUS server group.

```
ChassisID(config-interface x/x/x@x/x/x.gpon)#port-auth connect
subtended-host WORD radius group WORD
```

4. Use [Table 12-4](#) for any additional provisioning options.

Table 12-4. Additional Options

Command	Description	Default
ChassisID(config-interface x/x/x@x/x/x.gpon)#port-auth port-control [auto force-authorized force-unauthorized]	If the port mode is set to auto, the Supplicant via RADIUS is authenticated before traffic passes through the network. If the port mode is set to force-authorized or force-unauthorized, the authorization is fixed.	force-authorized
ChassisID(config-interface x/x/x@x/x/x.gpon)#port-auth timeout quiet-period <1-65535>	This sets the allotted time before the 802.1X PAE restarts after a failed 802.1X authorization attempt.	60
ChassisID(config-interface x/x/x@x/x/x.gpon)#port-auth timeout server <1-4294967295>	This sets the allotted time for the Access Module to contact the RADIUS server(s).	30

5. Return to the Global Configuration Command Set.

```
ChassisID(config-interface x/x/x@x/x/x.gpon)#exit
```

12.4.4 Step 4: Provision the RADIUS Relay Agent

1. Create a private IP Host.

- a. Access the Global Configuration Command Set.

ChassisID#configure terminal

- b. Access the IP Host Configuration Command Set.

Substitute WORD for 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.

ChassisID(config)#interface ip-host WORD <shelf/slot>



NOTE

IP Host names are case sensitive.

- c. Set the static IP address and subnet mask for the IP Host interface.

ChassisID(config-ip-host name x/x)#ip address A.B.C.D A.B.C.D



NOTE

Configure the private IP Host's IP address as the default gateway address for all subtended hosts using the relay.

- d. Disable the default gateway.

ChassisID(config-ip-host name x/x)#no default-gateway



NOTE

The IP address should be unique among other IP Hosts in the system.

- e. Enable the IP Host.

ChassisID(config-ip-host name x/x)#no shutdown

2. Create a public IP Host.

- a. Access the Global Configuration Command Set.

ChassisID#configure terminal

- b. Access the IP Host Configuration Command Set.

Substitute WORD for 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.

ChassisID(config)#interface ip-host WORD <shelf/slot>



NOTE

IP Host names are case sensitive.

- c. Set the static IP address and subnet mask for the IP host interface.

ChassisID(config-ip-host name x/x)#ip address A.B.C.D A.B.C.D

- d. Assign the IP address of the default gateway.

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



NOTE

The IP address should be unique among other IP Hosts in the system.

- e. Enable the IP Host.

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

3. Create an EVC for the private IP Host.

- a. Access the Global Configuration Command Set.

`ChassisID#configure terminal`

- b. Access the EVC Interface Configuration Command Set.

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

`ChassisID(config)#evc WORD`



NOTE

EVC names are case sensitive.

- c. Set the S-tag for the EVC.

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

- d. Apply this EVC to the private IP Host.

`ChassisID(config-evc name)#connect ip-host WORD <shelf/slot>`

- e. Enable the EVC.

`ChassisID(config-evc name)#no shutdown`

- f. Return to the Global Configuration Command Set.

`ChassisID(config-evc name)#exit`

4. Provision the System Management EVC for the public IP Host.

- a. Access the System Management EVC Interface Configuration Command Set.

`ChassisID(config)#system-management-evc`

- b. Set the system management VLAN to the required ID.

`ChassisID(config-sys-mgmt-evc)#s-tag <1-4094>`

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

The default interface is set in the Switch Module provisioning.

`ChassisID(config-sys-mgmt-evc)#connect men-port default-ethernet`

- d. Apply this EVC to the public IP Host.

`ChassisID(config-sys-mgmt-evc)#connect ip-host WORD <shelf/slot>`

5. Configure the RADIUS Relay Agent.



NOTE

The RADIUS relay can use UDP source ports 1025-65535 to communicate with the authentication server.

- a. Access the RADIUS Relay Command Set.

`ChassisID(config)#port-auth radius-relay WORD <shelf/slot>`

- b. Connect the public IP Host to the RADIUS relay.

`ChassisID(config-relay name x/x)#connect public ip-host WORD <shelf/slot>`

- c. Use [Table 12-5](#) for any additional provisioning options.

Table 12-5. Additional Options

Command	Description
<code>ChassisID(config-relay name x/x)#radius-attribute nas-identifier word</code>	Configures the RADIUS relay to ensure that the NAS-Identifier attribute value matches the configured string. If the string includes the token "\$accessnodeid\$", then the system TID will be inserted in its place.
<code>ChassisID(config-relay name x/x)#radius-attribute nas-ip-address public-ip</code>	Configures the RADIUS relay to ensure that the NAS-IP-Address attribute value matches the public IP Host's IP address.
<code>ChassisID(config-relay name x/x)#radius-attribute user-name calling-station-id</code>	Configures the RADIUS relay to ensure that the User-Name attribute value is the MAC address contained in the Calling-Station-ID attribute.
<code>ChassisID(config-relay name x/x)#radius-attribute vendor-specific id <number> sub-type <number> sub-value word</code>	Configures the Vendor-Specific attribute.
<code>ChassisID(config-relay name x/x)#radius-attribute calling-station-id mac-delimiter [colons hyphens]</code>	Configures the RADIUS Relay to regulate the Calling-Station-Id attribute value. If the value appears to represent a MAC address, ensure the delimiter is the selected type (colons or hyphens), updating the value if necessary.
<code>ChassisID(config-relay name x/x)#radius-attribute allow <attribute name></code>	Configure the RADIUS Relay to filter messages to only allow the specified RADIUS attributes. There should be one "radius-attribute allow <attribute name>" command for each attribute type that should be allowed through the Relay.
<code>ChassisID(config-relay name x/x)#radius-attribute allow attribute-id *</code>	Configures the RADIUS Relay to filter messages as the above command. However, this command provides the flexibility to select any attribute by attribute ID.
<code>ChassisID(config-relay name x/x)#radius-attribute allow all</code>	Configures the RADIUS Relay to not filter attributes from RADIUS messages.

- d. Enable the interface.

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

- e. Return to the Global Configuration Command Set.

`ChassisID(config-relay name x/x)#exit`

12.4.5 Step 5: Enable System-Wide 802.1X Authentication

Use the following command to enable IEEE 802.1X for the entire system:



NOTE

The per-port settings take effect only if the system-level port-auth setting is enabled.

`ChassisID(config)#port-auth`

12.5 Show Commands

Use the following commands for viewing status and provisioning information.

12.5.1 Status Commands

12.5.1.1 GPON Port Status

ChassisID#show interface gpon <shelf/slot/port>

```

gpon 1/19/2 is IS and up
  Number of Configured ONTs           : 1
  Number of Discovering ONTs          : 0
  Number of Unrecognized ONTs         : 0
  Number of Operational ONTs          : 1
  Number of Available HW Resour       : 959
  Longest Fiber Distance               : ont-1, 159m
  Shortest Fiber Distance              : ont-1, 159m
  Oversubscription Allowed             : true
                                     Downstream      Upstream
Max Provisionable BW                  kbps : 2488320    1244160
Configured PIR BW                     kbps : 0          0
Configured Fixed BW                   kbps : na         0
Configured Assured BW                 kbps : na         0
Configured min-rate BW                kbps : 0          na
Available PIR BW                      kbps : 2488320    1244160
Available CIR BW                      kbps : na         1194848
Available min-rate BW                 kbps : 2488000    na
Current PIR BW                        kbps : 0          0
Current CIR BW                        kbps : na         0

```

12.5.1.2 GPON Port Provisioning

ChassisID#show run interface gpon <shelf/slot/port>

```

interface gpon 1/19/2
  activation-mode auto-activate
  subtended-host 1 ip address 192.168.10.121 255.255.255.0
  subtended-host 1 ip default-gateway 192.168.10.1
  subtended-host 1 s-tag 410
  no shutdown

```

12.5.1.3 ONT Port Status

ChassisID#show remote-device <ont ID>@<shelf/slot/port>

```

remote-device ont 1@1/19/2.gpon
ont 1@1/19/2 is IS and up
  Uptime                       : 0 days, 01 hours, 15 minutes, 54 seconds
  Description                   :
  Activated Serial Number       : CIGG60871237
  Ont Software Version          : H00.01.0004.K1
  Ont Boot Software Version     : na
  Ont Upgrade Status            : Not Started
  Ont Part Number               : 00102-00002-21

```

```
Ont RSSI                                dBm : -17.4
Ont Upstream BIP                        : 0
Ont Downstream BIP                      : 0
Ont RDI                                 : 0
Ont RX Ploam CRC Error                  : 0
Ont US Good DBRu                        : 0
Ont US Bad DBRu                         : 0
Ont Equalization Delay                  bit : 265555
Ont Fiber Distance                      m  : 159
Ont ACS Server Profile                  :
Ont ACS Username                        :
Ont last error                          : VoIP provisioning: VoIP IP host not
supported
```

12.5.1.4 ONT Port Provisioning

```
ChassisID#show run interface gigabit-ethernet <ont ID>@<shelf/slot/port>
interface gigabit-ethernet 1/0/1@1/19/2.gpon
  mac limit 8
  no shutdown
  port-auth timeout quiet-period 60
  port-auth timeout server 30
```

12.5.1.5 ONT Gigabit Port 802.1X Status

```
ChassisID#show port-auth interface gigabit-ethernet <RD ID/0/RD
port>@<shelf/slot/port>
interface gigabit-ethernet 1/0/1@1/19/2 is IS and up
  EAPoL Protocol Version      : 0
  PAE Capabilities            : authenticator only
  Authenticator State         : initialize
  Backend Auth State          : initialize
  Port Auth Status            : unauthorized
  Control Direction           : both
  Port Control                 : force authorized
  Re-authentication           : disabled
  Last Config Error           : none
```

12.5.1.6 Radius Relay Agent Status

```
ChassisID#show port-auth radius-relay WORD <shelf/slot>
port-auth radius-relay basicRelay 1/A is IS and up
  Valid Client Requests       : 0
  Valid Server Challenges     : 0
  Valid Server Accepts        : 0
  Valid Server Rejects        : 0
  Invalid Message Authenticator : 0
  Invalid Client Packet Format : 0
  Invalid Server Packet Format : 0
  Unknown Client Code          : 0
  Unknown Server Code          : 0
  Client Dropped               : 0
  Client Missing Attribute     : 0
  Unknown Server               : 0
  Last Error                   : Running
```

12.5.2 Performance-Monitoring Commands

12.5.2.1 Current ONT 802.1X Statistics

ChassisID#show port-auth statistics interface gigabit-ethernet
<RD ID>/<RD port>@<shelf/slot/port> performance-statistics 15-minute

gigabit-ethernet 1/0/1@1/19/2 15-Min PM (Current)

	Receive	Transmit
EAPoL Total Frames	: 0	0
EAP Request ID Frames	: na	0
EAP Request Frames	: na	0
EAP Response ID Frames	: 0	na
EAP Response Frames	: 0	na
EAP Length Error Frames	: 0	na
EAPoL Start Frames	: 0	na
EAPoL Logoff Frames	: 0	na
EAPoL Invalid Frames	: 0	na

12.5.2.2 Previous ONT 802.1X Statistics

ChassisID#show port-auth statistics interface gigabit-ethernet <RD ID>/<RD port>@<shelf/slot/port> performance-statistics 15-minute 1

gigabit-ethernet 1/0/1@1/19/2 15-Min PM (1) 09/10 17:15

	Receive	Transmit
EAPoL Total Frames	: 0	0
EAP Request ID Frames	: na	0
EAP Request Frames	: na	0
EAP Response ID Frames	: 0	na
EAP Response Frames	: 0	na
EAP Length Error Frames	: 0	na
EAPoL Start Frames	: 0	na
EAPoL Logoff Frames	: 0	na
EAPoL Invalid Frames	: 0	na

12.5.2.3 Current ONT Radius Statistics

ChassisID#show port-auth server subtended-host <RD ID>@<shelf/slot/port>
performance-stat 15-minute

1@1/19/2 15-Min PM (Current)

	Receive	Transmit
Access Request Packets	: na	0
Access Rerequest Packets	: na	0
Access Challenge Packets	: 0	na
Access Accept Packets	: 0	na
Access Reject Packets	: 0	na
Invalid Packets	: 0	na
Bad Authenticators	: 0	na
Client Timeouts	: 0	na
Unknown Types	: 0	na
Packets Dropped	: 0	na

12.5.2.4 Previous ONT Radius Statistics

ChassisID#show port-auth server subtended-host <RD ID>@<shelf/slot/port>
performance-stat 15-minute 1

1@1/19/2 15-Min PM (1) 09/10 17:30

	Receive	Transmit
Access Request Packets	: na	0
Access Rerequest Packets	: na	0
Access Challenge Packets	: 0	na
Access Accept Packets	: 0	na
Access Reject Packets	: 0	na
Invalid Packets	: 0	na
Bad Authenticators	: 0	na
Client Timeouts	: 0	na
Unknown Types	: 0	na
Packets Dropped	: 0	na

12.5.2.5 Current Relay Agent Statistics

ChassisID#show port-auth radius-relay WORD <shelf/slot> performance-stat
15-minute

port-auth radius-relay 1/A basicRelay is IS and up

Current Interval (11:15)

Valid Client Requests	: 0
Valid Server Challenges	: 0
Valid Server Accepts	: 0
Valid Server Rejects	: 0
Invalid Message Authenticator	: 0
Invalid Client Packet Format	: 0
Invalid Server Packet Format	: 0
Unknown Client Code	: 0
Unknown Server Code	: 0
Client Dropped	: 0
Client Missing Attribute	: 0
Unknown Server	: 0

12.5.2.6 Previous Relay Agent Statistics

ChassisID#show port-auth radius-relay WORD <shelf/slot> performance-stat
15-minute 1

port-auth radius-relay 1/A basicRelay is IS and up

Current Interval (11:00)

Valid Client Requests	: 0
Valid Server Challenges	: 0
Valid Server Accepts	: 0
Valid Server Rejects	: 0
Invalid Message Authenticator	: 0
Invalid Client Packet Format	: 0
Invalid Server Packet Format	: 0
Unknown Client Code	: 0
Unknown Server Code	: 0
Client Dropped	: 0
Client Missing Attribute	: 0
Unknown Server	: 0

12.6 Provisioning Examples

12.6.1 Example 1 - One RADIUS Server in the Network with RADIUS Relay

In this example the following is assumed:

- One RADIUS server
- Relay Agent
- RADIUS client active on slot 1/17 with an IP address of 10.100.42.95
 - ◆ RADIUS traffic on VLAN 4092 on the gigabit-ethernet interface 1/2/8
- Subscriber on Gig-port 1/0/1@1/17/1

1. Enable port authentication for the system.

```
ChassisID(config)#port-auth
```

2. Define the RADIUS server and server group.

```
ChassisID(config)#port-auth server radius radiusServer
ChassisID(config-server-radius radiusServer)#ip-address 10.47.84.20
ChassisID(config-server-radius radiusServer)#key secret
```

```
ChassisID(config)#port-auth group radius radiusGroup
ChassisID(config-group-radius radgroup radiusGroup)#add server
radiusServer sequence-number 1
ChassisID(config-group-radius radgroup radiusGroup)#nas-port-id PON_1/
1/$slot$/$port$:$ont$.$ontslot$.$ontport$
```

3. Provision the subtended host that will be used by the RADIUS client. It is necessary to create an EVC that connects the subtended host to a VLAN and a physical interface that faces the RADIUS server.

```
ChassisID(config)#evc evc-4092
ChassisID(config-evc evc-4092)#s-tag 4092
ChassisID(config-evc evc-4092)#connect men-port gigabit-ethernet 1/2/8
ChassisID(config-evc evc-4092)#connect ip-host PRIVATE 1/A
ChassisID(config-evc evc-4092)#mac-switched
ChassisID(config-evc evc-4092)#no shutdown
```

```
ChassisID(config)#interface gpon 1/17/1
ChassisID(config-gpon 1/17/1)#subtended-host 1 s-tag 4092
ChassisID(config-gpon 1/17/1)#subtended-host 1 s-tag priority 1
ChassisID(config-gpon 1/17/1)#subtended-host 1 ip address 10.100.42.95
255.255.255.0
ChassisID(config-gpon 1/17/1)#subtended-host 1 ip default-gateway
10.100.42.254
ChassisID(config-gpon 1/17/1)#no shutdown
```

4. Provision the System Management EVC for the public IP Host.

```
ChassisID(config)#system-management-evc
ChassisID(config-sys-mgmt-evc)#s-tag 2094
ChassisID(config-sys-mgmt-evc)#connect men-port default-ethernet
ChassisID(config-sys-mgmt-evc)#connect ip-host PUBLIC 1/A
```

5. Provision a private IP Host.

```
ChassisID(config)#interface ip-host PRIVATE 1/A
ChassisID(config-ip-host PRIVATE 1/A)#ip address 10.100.42.254
255.255.255.0
ChassisID(config-ip-host PRIVATE 1/A)#no default-gateway
ChassisID(config-ip-host PRIVATE 1/A)#no shutdown
```

6. Create a Public IP Host.

```
ChassisID(config)#interface ip-host PUBLIC 1/A
ChassisID(config-ip-host PUBLIC 1/A)#ip address 10.47.84.200
255.255.255.0
ChassisID(config-ip-host PUBLIC 1/A)#default-gateway 10.47.84.254
ChassisID(config-ip-host PUBLIC 1/A)#no shutdown
```

7. Configure the RADIUS Relay Agent.

```
ChassisID(config)#port-auth radius-relay basicRelay 1/A
ChassisID(config-relay basicRelay 1/A)#connect public ip-host PUBLIC 1/
A
ChassisID(config-relay basicRelay 1/A)#radius-attribute nas-identifier
EXAMPLE
ChassisID(config-relay basicRelay 1/A)#radius-attribute nas-ip-address
public-ip
ChassisID(config-relay basicRelay 1/A)#radius-attribute user-name
calling-station-id
ChassisID(config-relay basicRelay 1/A)#radius-attribute vendor-specific
id 193 sub-type 101 sub-value EXAMPLE
ChassisID(config-relay basicRelay 1/A)#no shutdown
```

8. Enable the ONT interfaces for the subscriber ports. Configure port authentication parameters on the gigabit-ethernet port including the associated RADIUS server group.

```
ChassisID(config)#interface gigabit-ethernet 1/0/1@1/17/1
ChassisID(config-giga-eth 1/0/1@1/17/1.gpon)#no shutdown

ChassisID(config)#interface gigabit-ethernet 1/0/1@1/17/1
ChassisID(config-giga-eth 1/0/1@1/17/1)#port-auth port-control auto
ChassisID(config-giga-eth 1/0/1@1/17/1)#port-auth timeout quiet-period
20
ChassisID(config-giga-eth 1/0/1@1/17/1)#port-auth timeout server 30
ChassisID(config-giga-eth 1/0/1@1/17/1)#port-auth connect subtended-
host radius group radiusGroup
ChassisID(config-giga-eth 1/0/1@1/17/1)#no shutdown
```

12.6.2 Example 2 - Two RADIUS Servers in the Network without RADIUS Relay Agent

- Two RADIUS servers (A, B) in the network
 - ◆ System groups both servers into the same server group
 - ◆ Server A is queried first, with fallback to server B
- RADIUS client active on slot 1/17 with IP address 10.100.42.95
 - ◆ RADIUS traffic on VLAN 4092 on gigabit-ethernet interface 1/2/8
- Subscriber on Gig-port 1/0/1@1/17/1

1. Enable port authentication for the system.

```
ChassisID(config)#port-auth
```

2. Define the RADIUS servers and server group.

```
ChassisID(config)#port-auth server radius radiusServerA
ChassisID(config-server-radius radiusServer)#ip-address 10.47.84.20
ChassisID(config-server-radius radiusServer)#key secret

ChassisID(config)#port-auth server radius radiusServerB
ChassisID(config-server-radius radiusServer)#ip-address 10.47.84.21
ChassisID(config-server-radius radiusServer)#key secret
```

```
ChassisID(config)#port-auth group radius radiusGroup
ChassisID(config-group-radius radiusGroup)#add server radiusServer
sequence-number 1
ChassisID(config-group-radius radiusGroup)#add server radiusServer
sequence-number 1
ChassisID(config-group-radius radiusGroup)#nas-port-id nas-port-id
PON_1/1/$slot$/$port$:$ont$.$ontslot$.$ontport$
```

3. Provision the subtended host that will be used by the RADIUS client. It is necessary to create an EVC that connects the subtended host to a VLAN and a physical interface that faces the RADIUS server.

```
ChassisID(config)#evc evc-4092
ChassisID(config-evc evc-4092)#s-tag 4092
ChassisID(config-evc evc-4092)#connect men-port gigabit-ethernet 1/2/8
ChassisID(config-evc evc-4092)#mac-switched
ChassisID(config-evc evc-4092)#no shutdown
```

```
ChassisID(config)#interface gpon 1/17/1
ChassisID(config-gpon 1/17/1)#subtended-host 1 s-tag 4092
ChassisID(config-gpon 1/17/1)#subtended-host 1 s-tag priority 1
ChassisID(config-gpon 1/17/1)#subtended-host 1 ip address 10.100.42.95
255.255.255.0
ChassisID(config-gpon 1/17/1)#subtended-host 1 ip default-gateway
10.100.42.254
ChassisID(config-gpon 1/17/1)#no shutdown
```

4. Enable the ONT interfaces for the subscriber ports. Configure port authentication parameters on the gigabit-ethernet port including the associated RADIUS server group.

```
ChassisID(config)#interface gigabit-ethernet 1/0/1@1/17/1
ChassisID(config-giga-eth 1/0/1@1/17/1.gpon)#no shutdown
ChassisID(config)#interface gigabit-ethernet 1/0/1@1/17/1
```

```
ChassisID(config-giga-eth 1/0/1@1/17/1.gpon)#port-auth port-control
auto
ChassisID(config-giga-eth 1/0/1@1/17/1.gpon)#port-auth timeout quiet-
period 20
ChassisID(config-giga-eth 1/0/1@1/17/1.gpon)#port-auth timeout server
30
ChassisID(config-giga-eth 1/0/1@1/17/1.gpon)#port-auth connect ip-host
radiusIpHost radius group radiusGroup
ChassisID(config-giga-eth 1/0/1@1/17/1.gpon)#no shutdown

ChassisID(config)#interface gigabit-ethernet 1/0/1@1/17/2
ChassisID(config-giga-eth 1/0/1@1/17/2.gpon)#port-auth port-control
auto
ChassisID(config-giga-eth 1/0/1@1/17/2.gpon)#ort-auth timeout quiet-
period 20
ChassisID(config-giga-eth 1/0/1@1/17/2.gpon)#port-auth timeout server
30
ChassisID(config-giga-eth 1/0/1@1/17/2.gpon)#port-auth connect ip-host
radiusIpHost radius group radiusGroup
ChassisID(config-giga-eth 1/0/1@1/17/2.gpon)#no shutdown
```

13 Activation Mode

13.1 Scope of this Section

This section provides four different methods for activating your GPON ONT. Each method contains a list of pros and cons associated with that registration method.

13.2 In this Section

This section contains the topics listed in [Table 13-1](#).

Table 13-1. Section 13 Topics

Sub-Section	Topic	See Page
13.3	“Manual Activation”	392
13.4	“Auto-Discovery”	393
13.5	“Auto-Activation”	394
13.6	“Registration-ID Activation”	395

13.3 Manual Activation



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.

13.3.1 Pro

Manual activation provides the most control to service operators.

13.3.2 Con

Only ONTs specifically entered into the OLT are allowed to be active on the PON.



What's Next

- For CLI Manual Activation, continue to [Section 2.3.1, “OLT/PON Provisioning”](#) on page 50.
- For Web Manual Activation, continue to [Section 2.3.1, “OLT/PON Provisioning”](#) on page 50.

13.4 Auto-Discovery

Auto-Discovery mode adds the ability to discover a new ONT when connected but does not activate the new ONT until the required provisioning is entered into the OLT. The discovery operation is performed every 20 seconds. The feature allows selecting the appropriate ONT SN from a list of “discovered” ONT SNs when provisioning the SN information into the OLT. The first three steps in “Manual Activation” are still needed but the SN can be selected from the list rather than typed in by hand.

13.4.1 Pros

- Provides a very secure method as the serial number (S/N) of the unit must match the S/N configured in the Total Access 5000 OLT.
- Provides the most efficient manner to provision the S/N and the desired ONT-ID number between 1 - 32/64 depending on your OLT.

13.4.2 Cons

- Prior to beginning the installation process, the S/N of the ONT must be known by the group that provisions the Total Access 5000 and by the installation group. The unit with the same S/N must be selected by the person installing the ONT and must be installed at the precise location that was pre-provisioned at the Total Access 5000.
- Process can be very difficult to coordinate S/N of the ONTs between the two groups.



What's Next

- For CLI Auto-Discovery, continue to [Section 3.3.1, “OLT/PON Provisioning”](#) on page 116.
- For Web Auto-Discovery, continue to [Section 3.3.1, “OLT/PON Provisioning”](#) on page 116.

13.5 Auto-Activation

Auto-Activation mode is the most open (insecure) version of the activation modes. This mode periodically (every 20 seconds) scans the GPON interface for any newly added ONT and automatically assigns an ONT-ID, learns the SN, and activates the ONT.

Caution is advised when using this mode. If an ONT needs to be replaced then the replacement ONT will automatically be discovered and activated using a new ONT-ID. The replaced ONT's services will not be moved to the new ONT because there is no way for the OLT to know that the new ONT is a replacement device instead of a new device. The proper way to replace an ONT in this mode is to edit, in the OLT, the SN of the ONT to be replaced to match the new ONT SN value. Then the replacement ONT can be attached and all services will be associated to the new ONT.

13.5.1 Pros

- Provides the easiest method to use in the field because the unit is automatically discovered by the OLT and is automatically assigned an ONT-ID between 1 and 32/64.

13.5.2 Cons

- Provides the most insecure method.
- Assigns ONT-ID automatically, therefore the management and provisioning of services is more difficult.
- Creates a difficulty to provision services to the correct ONT-ID if several ONTs have been placed in the field prior to provisioning the OLT. If all ONTs on the same PON have the same service profile it becomes easier to provision, but the location of the ONT must match the provisioning OLT for billing and management purposes.
- Creates an ONT replacement problem. The replaced services will not be moved to the new ONT because there is no way for the OLT to know that the new ONT is a replacement device as opposed to a new device. The proper method to replace an ONT in this mode is to edit, in the OLT, the S/N of the ONT to be replaced to match the new ONT S/N value. Then the replacement ONT can be attached and all services will be associated to the new ONT.



What's Next

- For CLI Auto-Activation, continue to [Section 3.3.1, "OLT/PON Provisioning"](#) on page 116.
- For Web Auto-Activation, continue to [Section 3.3.1, "OLT/PON Provisioning"](#) on page 116.

13.6 Registration-ID Activation

Registration-ID Activation provides two methods for use:

- Lock Serial Number
- Unlock Serial Number



NOTE

If the Registration-ID is programmed into the ONT, it is ignored unless the PON is set to the Registration-ID method.

Registration-ID activation offers a secure way to add only ONTs that are expected to be installed without requiring the installer to know the SN of the ONT being installed. SNs are programmed into ONTs at the factory and cannot be changed. Using the manual or auto-discovery activation modes would normally mean that a specific ONT device must be installed at a specific location before the OLT will activate it. Registration-ID activation allows a unique 10-digit number to be programmed into the ONT by the installation technician during installation. The matching Registration-ID is provisioned into the OLT instead of the SN along with the ONT-ID value. Once the ONT is discovered the ONT will be activated using the Registration-ID without regard to the SN value programmed by the factory for the first activation. Future activations of the ONT will match the Registration-ID and the SN. The ONT SN will be displayed in the learned SN and the provisioned SN column.



NOTE

The Serial Number and Registration-ID are matched only in loc

There is another advantage Registration-ID activation mode offers over the previous methods. ONT replacement is significantly simplified using this method. In lock mode, if the S/N is provisioned at the OLT, the S/N must be either removed or changed in a replacement scenario. In unlock mode, as long as either Registration-ID or S/N matches the ONT connected to the PON, the ONT would come UP.

The only action that needs to be performed on the ONT is that the replacement ONT must be provisioned with the same Registration-ID that is programmed into the OLT for that associated ONT. ONT Replacement should follow these steps to ensure successful replacement:



NOTE

The following steps apply to both modes. In the lock mode, if there is a S/N (learned or provisioned) that needs to be removed or matched with the ONT being replaced.

1. Disconnect the ONT to be replaced from the fiber.
2. Provision the correct Registration-ID into the replacement ONT (see [“Enter the Registration-ID”](#) on page 53).
3. Connect the replacement ONT to the fiber.



NOTE

A replacement ONT will not be activated as long as another ONT is activated that contains the same Registration-ID. This prevents removing services from a customer should a duplicate Registration-ID be accidentally entered into a new ONT being installed on the fiber. Only an ONT in the “Discovering” state will be replaced when a Registration-ID is matched to a new ONT.

When there is only a S/N programmed for the ONT and no Registration-ID provisioned at the OLT, if preferable, you can change to any one of the Registration-ID modes. In both cases, the ONTs would come up.

If Registration-IDs are provisioned only at the OLT, then unlock mode would bring UP the ONTs (as S/N match) whereas lock mode would not as it requires both S/N and Registration-ID (which are not programmed in ONT in this case) and so lock mode would not be able to activate the ONTs.

If S/N and Registration-ID are provisioned at the OLT, unlock mode matches the S/N or Registration-ID, whereas lock mode matches the S/N and Registration-ID.

The unlock serial number option of the Registration-ID mode allows customers to deploy Registration-ID provisioned ONTs, on top of brownfield networks that previously only used serial number registration (instead of registration ID). This is done by changing the mode of the PON to "Registration ID" mode with suboption unlock-serial-number. In this mode, if the OLT has a provisioned SN that matches the ONT's SN, then the ONT will register with the matching ONT ID in the OLT. The registration ID will not be asked from the ONT in this case. Thus provisioned serial number is prioritized over registration ID. If there is no provisioned serial number then the provisioned Registration ID will be requested from the ONT and matched upon. If this also fails then the OLT alarms that an unknown Serial Numbered ONT has been connected.

This mode will help customers when they have many ONTs installed and running in the field that were registered via serial number. Now the customer wants to move their network to a registration ID mode without isolating/blocking the previous installed base of ONTs. In the updated "unlock-serial-number" mode, the user's ONTs would automatically register on the PON since they have provisioned Serial Numbers in the OLT

Another scenario is when a user either has ONTs that do not support Registration-ID mode or they want to continue deploying existing ONTs (without Registration IDs) and new ONT's (with Registration-ID), but keep them in the same network. This new mode (registration ID unlock) gives the user the ultimate flexibility in deploying a network. Even if a user would like to continue installing via serial number up to some date in the future, they can still convert the PON to this mode and seamlessly transition from "serial" number deployments to "registration-ID" deployments, without further NOC intervention.

**NOTE**

If the activation mode is lock-serial number, then future activations of the ONT will match both the Registration-ID and the SN. If the activation mode is unlock-serial number, then future activations of the ONT will match either the SN or the Registration-ID and the SN take higher precedence over Registration-ID.

13.6.1 Pros

- Provides the most secure method of registration.
- Provides the easiest method to administrate. The installer does not need to know the S/N of the unit being installed.
- Provides for easier ONT replacement. If the activation registration lock-serial-number method is used, the installer only needs to know the registration ID. Only one change needs to be made to achieve complete service migration to the replacement ONT.
 - ◆ The management team must delete the ONT S/N from the OLT provisioning. Applicable to lock mode only. In unlock mode, either S/N or Registration-ID need to match to bring up the ONT.

- ◆ When replacing the ONT in the field, re-entering the same Registration ID used by the previous ONT is all that needs to be done.

13.6.2 Cons

- Provides a potential insecure activation method when using the activation registration unlock-serial-number command.



CAUTION!

Do not duplicate the same Registration-ID to two different ONTs to be activated on the OLT.

As an example, ONT A has S/N S1 and Registration-ID R1 and is UP another ONT B has S/N S2 and Registration-ID R2.

ONT B becomes faulty and needs replacement. When the technician removes ONT B and adds a new ONT in place of B with a Registration-ID R1, ONT B would not come UP and cause a duplicate Registration-ID error at the OLT. If the technician did not resolve the duplicate Registration-ID and leave the ONT connected, ONT A would still be UP and running. After an OLT reboot, there is a chance that the ONT replaced at B would get the service of ONT A.

- Can potentially create an ONT replacement problem. The new or replacement ONT can remove the service of another ONT already operating in the field.
- Allows the service of another ONT to accidentally be taken by the newly installed ONT if the Registration-ID is duplicated by the technician during installation of the new, replacement ONT.



What's Next

- For CLI Registration-ID activation, continue to [Section 2.3.1.2, "Provision the PON"](#) on page 50.
- For Web Registration-ID activation, continue to [Section 2.3.1.2, "Provision the PON"](#) on page 50.

14 ONT Capability Provisioning

14.1 Scope of this Section

The ONT Capability Provisioning feature provides a method to configure the OLT for the expected functionality of an ONT. The main purpose of this feature is to ease integration of new ONTs into the system.

There are two tables associated with this new feature. The first table (refer to [Figure 14-1](#) on page 401) is used for referencing an ONT by its part number. The second table (refer to [Figure 14-3](#) on page 403) is used for referencing an ONT by its four-character vendor name. Each table has fixed entries that cannot be removed, although they can be modified for test purposes. These tables govern the behavior of all ONTs on all PONs on a shelf. **Any change to a table entry for a specific ONT part number or vendor name, will affect every ONT with that part number or vendor name connected to any PON on the Total Access 5000 shelf.** Because of this, it is not recommended that an existing fixed ONT capability be changed except in a lab environment. These fixed entries are marked by a "*" in column 1 under the Def (Default) heading. If one of these fixed entries is inadvertently modified from those values set by ADTRAN when the product was shipped, it will be noted by a second "*" in column 3. A "no" command can be used on a fixed entry to return it to its default values. Refer to [Section 14.7, "Restoring a Fixed Part Number Entry to Default Value"](#) on page 405 for this procedure.

When a new ONT (one not already in either table) is going to be introduced into the system, ADTRAN recommends adding a single ONT of the new type to the system, and getting its capability settings correct before adding remaining ONTs of this type into the system. This will ensure the table settings take effect for all ONTs of this type.

For a list of terms associated with Capability Provisioning, refer to [Section 14.9, "ONT Capability Provisioning Terms"](#) on page 408.



CAUTION!

This feature should be used with extreme care. It creates shelf-wide provisioning that could be service-affecting if used incorrectly. Changes to these provisioning items are not guaranteed to take place until the next ONT activation.

14.2 In this Section

This section contains the topics listed in [Table 14-1](#).

Table 14-1. Section 14 Topics

Sub-Section	Topic	See Page
14.3	Adding a New ONT Part Number	401
14.4	Removing an ONT Part Number	402
14.5	Adding a Vendor Name	403
14.6	Removing a Vendor Name	404
14.7	Restoring a Fixed Part Number Entry to Default Value	405
14.8	Restoring Vendor Entry to Default Value	406
14.9	ONT Capability Provisioning Terms	408

14.3 Adding a New ONT Part Number

In the following example, part number 123xxxx is being added to the part number table.



NOTE

Each table (part number table and vendor name table) can have new entries added to them to help facilitate the setup of new ONTs. These new entries can be removed from the table if not needed. These entries will not have "*" in any column under the **Def** heading.

To add a new ONT part number to a PON, complete the following.

```
TA5000#configure terminal
```

```
TA5000(config)#ont-capability part-number 123xxxx
```

```
ONT Capability Part number "123xxxx" created
```

```
TA5000(config-ont-cap-part-num 123xxxx)#ont-type
```

```
adtran300      -Adtran 2nd Generation 300 series
adtran400      -Adtran 4th Generation 400 series
adtran600      -Adtran XGSPON 600 series
adtranmdu      -Adtran MDU 8P-8VDSL2
generic        -Set ONT Type to generic
```



NOTE

Set any non-ADTRAN ONT to "generic".

```
ONT Capability Part number "123xxxx" created
```

```
TA5000(config-ont-cap-part-num 123xxxx)#do show ont-capability
```

The following table is displayed:

```
TA5K-TEST1#configure terminal
TA5K-TEST1(config)#ont-capability part-number 123xxxx
ONT Capability Part number "123xxxx" created
TA5K-TEST1(config-ont-cap-part-num 123xxxx)#do show ont-capability
User Defined Supported ONTs
```

Def	Part Number	Product Name	ONT Type	DBR	EXT	Capabilities Supported				T1	Mgt	NSR
						64b	R11	EXT	Cnt			
*	1179870F1	508UP OUTDOOR MDU 8	adtranmdu	F	T	F	T	F	T	515	32	
*	1179870F2	508UP OUTDOOR MDU 8	adtranmdu	F	T	F	T	F	T	515	32	
*	123xxxx	generic	generic	F	F	F	F	F	F	515	32	
*	1287701G1	TA351 2ND GEN OUTDO	adtran300	F	T	F	T	F	T	515	32	

Figure 14-1. Adding a New ONT Part Number

14.4 Removing an ONT Part Number

In the following example, part number 123XXXX is being removed.



NOTE

The “no” command can be used on a new entry to remove it from the table.

To remove an ONT part number, complete the following:

TA5000(config)#no ont-capability part-number 123xxxx

TA5000(config)#do show ont-capability

The following table is displayed:

```
TA5K-TEST1<config>#no ont-capability part-number 123xxxx
TA5K-TEST1<config>#do show ont-capability
  User Defined Supported ONTs
```

				Capabilities Supported									
				64b	R11	T1		Mgt	NSR				
Def	Part Number	Product Name			ONT Type	DBR	EXT	EXT	Cnt	Rtp	Pro	Id	Grt
*	1179870F1	508UP	OUTDOOR	MDU 8	adtranmdu	F	T	F	T	F	T	515	32
*	1179870F2	508UP	OUTDOOR	MDU 8	adtranmdu	F	T	F	T	F	T	515	32
*	1287701G1	TA351	2ND GEN	OUIDO	adtran300	F	T	F	T	F	T	515	32

Figure 14-2. Removing an ONT Part Number

14.5 Adding a Vendor Name

In the following example, vendor name ABCD is being added.

To add a new vendor name, complete the following:

```
TA5000#configure terminal
```

```
TA5000 (config)#ont-capability vendor-name ABCD
```

```
ONT Capability Vendor "ABCD" created
```

```
TA000(config-ont-cap-vendor ABCD)#do show ont-capability
```

The following table is displayed:

TA5K-TEST1#configure terminal													
TA5K-TEST1(config)#ont-capability vendor-name ABCD													
ONT Capability Vendor "ABCD" created													
TA5K-TEST1(config-ont-cap-vendor ABCD)#do show ont-capability													
User Defined Supported ONTs													
Def	Part Number	Product Name	ONT Type	DBR	EXT	64b EXT	R11 Cnt	Supported Rtp	Supported Tl	Mgt Id	NSR Grt		
*	1179870F1	508UP OUTDOOR MDU 8	adtranmdu	F	I	F	I	F	I	515	32		
*	1179870F2	508UP OUTDOOR MDU 8	adtranmdu	F	I	F	I	F	I	515	32		
*	1287701G1	IA351 2ND GEN OUTDO	adtran300	F	I	F	I	F	I	515	32		
*	1287702G1	IA352 2ND GEN OUTDO	adtran300	F	I	F	I	F	I	515	32		
*	1287702G1C	IA352 2ND GEN OUTDO	adtran300	F	I	F	I	F	I	515	32		
*	1287702G1Q	IA352 2ND GEN OUTDO	adtran300	F	I	F	I	F	I	515	32		
*	1287702G3	IA352H 2ND GEN OUTDO	adtran300	F	I	F	I	F	I	515	32		
*	1287711G1	IA361 2ND GEN OUTDO	adtran300	F	I	F	I	F	I	515	32		
*	1287712G1	IA362 2ND GEN OUTDO	adtran300	F	I	F	I	F	I	515	32		
*	1287712G1Q	IA362 2ND GEN OUTDO	adtran300	F	I	F	I	F	I	515	32		
*	1287712G3	IA362H 2ND GEN OUTDO	adtran300	F	I	F	I	F	I	515	32		
*	1287713G1	IA364 2ND GEN OUTDO	adtran300	F	I	F	I	F	I	515	32		
*	1287715G1	IA362R 2ND GEN OUTDO	adtran300	F	I	F	I	F	I	515	32		
*	1287722G1	IA372 2ND GEN OUTDO	adtran300	F	I	F	I	F	I	515	32		
*	1287722G2	IA372R 2ND GEN OUTDO	adtran300	F	I	F	I	F	I	515	32		
*	1287735G1	IA324 2ND GEN INDOO	adtran300	F	I	F	I	F	I	515	32		
*	1287735G2	IA324 2ND GEN INDOO	adtran300	F	I	F	I	F	I	515	32		
*	1287736G1	IA334 2ND GEN INDOO	adtran300	F	I	F	I	F	I	515	32		
*	1287736G2	IA334 2ND GEN INDOO	adtran300	F	I	F	I	F	I	515	32		
*	1287781F1	424RG 4th GEN INDOO	adtran400	F	I	F	I	T	T	515	32		
*	1287781F2	424RG 4th GEN INDOO	adtran400	F	I	F	I	T	T	515	32		
*	1287786F1	401 4th GEN INDOO	adtran400	F	I	T	T	T	T	515	32		
*	1287787F1	411 4th GEN INDOO	adtran400	F	I	T	T	T	T	515	32		
*	1287787F1N	411 4th GEN INDOO	adtran400	F	I	T	T	T	T	515	32		
*	1287800F1	602 XGS-PON INDOO	adtran600	F	I	T	T	F	I	515	32		
*	1287801F1	400 4th Gen INDOO	generic	F	F	F	T	F	I	0	32		
*	1287802F1	452 4th GEN OUTDOOR S	adtran400	F	I	T	T	T	T	515	32		
*	1287803F1	454 4th GEN OUTDOOR S	adtran400	F	I	T	T	T	T	515	32		
*	1287812F1	462 4th GEN OUTDOOR S	adtran400	F	I	T	T	T	T	515	32		
*	1287813F1	464 4th GEN OUTDOOR S	adtran400	F	I	T	T	T	T	515	32		
*	1287823F1	621X XGS-PON INDOO	adtran600	F	I	T	T	F	I	515	32		
*	1287823F1T	621X XGS-PON INDOO	adtran600	F	I	T	T	F	I	515	32		
*	1287823F2	621X XGS-PON INDOO	adtran600	F	I	T	T	F	I	515	32		
*	1287825F1	601X XGS-PON INDOO	adtran600	F	I	T	T	F	I	515	32		
*	1287835F1	424 4th GEN INDOO	adtran400	F	I	T	T	T	T	515	32		
*	1287835F1C	324 4th GEN INDOO	adtran400	F	I	T	T	T	T	515	32		
*	GFLI100	generic	F	F	F	T	F	T	I	515	6		
*	GFLI110	generic	F	F	F	T	F	T	I	515	6		
*	GFLI130	generic	T	F	F	T	F	T	I	515	6		
*	GFLI131	generic	T	F	F	T	F	T	I	515	6		
*	GFLI300	generic	F	F	F	T	F	T	I	515	6		
** indicates a unmodified default entry													
** * indicates a modified default entry													
User Defined Supported ONTs													
Def	Vendor Name	Product Name	ONT Type	DBR	EXT	64b EXT	R11 Cnt	Supported Rtp	Supported Tl	Mgt Id	NSR Grt		
*	ABCD	ActionTec defaults	generic	F	F	F	F	F	F	515	32		
*	ATFJ	CIG defaults	generic	T	F	F	T	F	T	515	32		
*	CIGG	CIG defaults	generic	F	T	F	F	T	T	3	32		
*	IPHO	IPHOTONIX defaults	generic	F	T	F	T	F	T	100	32		
*	XAVI	XAVI defaults	generic	T	F	F	T	F	T	515	32		
** indicates a unmodified default entry													
** * indicates a modified default entry													

Figure 14-3. Adding a Vendor Name

14.6 Removing a Vendor Name

In the following example, vendor name ABCD is being removed.

To remove a vendor name, complete the following:

TA5000#configure terminal

TA5000 (config)#no ont-capability vendor-name ABCD

TA5000(config)#do show ont-capability

The following table is displayed:

TA5K-TEST1(config)#no ont-capability vendor-name ABCD												
TA5K-TEST1(config)#do show ont-capability												
User Defined Supported ONTs												
Def	Part Number	Product Name	ONT Type	DBR	EXT	64b EXT	R11 Cnt	Rtp	T1 Pro	Mgt Id	NSR Grt	
*	1179870F1	508UP OUTDOOR MDU 8	adtranmdu	F	I	F	I	F	I	515	32	
*	1179870F2	508UP OUTDOOR MDU 8	adtranmdu	F	I	F	I	F	I	515	32	
*	1287701G1	TA351 2ND GEN OUTDO	adtran300	F	I	F	I	F	I	515	32	
*	1287702G1	TA352 2ND GEN OUTDO	adtran300	F	I	F	I	F	I	515	32	
*	1287702G1C	TA352 2ND GEN OUTDO	adtran300	F	I	F	I	F	I	515	32	
*	1287702G1Q	TA352 2ND GEN OUTDO	adtran300	F	I	F	I	F	I	515	32	
*	1287702G3	TA352H 2ND GEN OUTDO	adtran300	F	I	F	I	F	I	515	32	
*	1287711G1	TA361 2ND GEN OUTDO	adtran300	F	I	F	I	F	I	515	32	
*	1287712G1	TA362 2ND GEN OUTDO	adtran300	F	I	F	I	F	I	515	32	
*	1287712G1Q	TA362 2ND GEN OUTDO	adtran300	F	I	F	I	F	I	515	32	
*	1287712G3	TA362H 2ND GEN OUTDO	adtran300	F	I	F	I	F	I	515	32	
*	1287713G1	TA364 2ND GEN OUTDO	adtran300	F	I	F	I	F	I	515	32	
*	1287715G1	TA362R 2ND GEN OUTDO	adtran300	F	I	F	I	F	I	515	32	
*	1287722G1	TA372 2ND GEN OUTDO	adtran300	F	I	F	I	F	I	515	32	
*	1287722G2	TA372R 2ND GEN OUTDO	adtran300	F	I	F	I	F	I	515	32	
*	1287735G1	TA324 2ND GEN INDOO	adtran300	F	I	F	I	F	I	515	32	
*	1287735G2	TA324 2ND GEN INDOO	adtran300	F	I	F	I	F	I	515	32	
*	1287736G1	TA334 2ND GEN INDOO	adtran300	F	I	F	I	F	I	515	32	
*	1287736G2	TA334 2ND GEN INDOO	adtran300	F	I	F	I	F	I	515	32	
*	1287781F1	424RG 4th GEN INDOO	adtran400	F	I	F	I	T	T	515	32	
*	1287781F2	424RG 4th GEN INDOO	adtran400	F	I	F	I	T	T	515	32	
*	1287786F1	401 4th GEN INDOO	adtran400	F	I	T	T	T	T	515	32	
*	1287787F1	411 4th GEN INDOO	adtran400	F	I	T	T	T	T	515	32	
*	1287787F1N	411 4th GEN INDOO	adtran400	F	I	T	T	T	T	515	32	
*	1287800F1	602 XGS-PON INDOO	adtran600	F	I	T	T	F	T	515	32	
*	1287801F1	400 4th Gen INDOO	generic	F	F	F	I	F	T	0	32	
*	1287802F1	452 4th GEN OUTDOOR S	adtran400	F	I	T	T	T	T	515	32	
*	1287803F1	454 4th GEN OUTDOOR S	adtran400	F	I	T	T	T	T	515	32	
*	1287812F1	462 4th GEN OUTDOOR S	adtran400	F	I	T	T	T	T	515	32	
*	1287813F1	464 4th GEN OUTDOOR S	adtran400	F	I	T	T	T	T	515	32	
*	1287823F1	621X XGS-PON INDOO	adtran600	F	I	T	T	F	T	515	32	
*	1287823F1T	621X XGS-PON INDOO	adtran600	F	I	T	T	F	T	515	32	
*	1287823F2	621X XGS-PON INDOO	adtran600	F	I	T	T	F	T	515	32	
*	1287825F1	601X XGS-PON INDOO	adtran600	F	I	T	T	F	T	515	32	
*	1287835F1	424 4th GEN INDOO	adtran400	F	I	T	T	T	T	515	32	
*	1287835F1C	324 4th GEN INDOO	adtran400	F	I	T	T	T	T	515	32	
*	GFLI100		generic	I	F	F	I	F	T	515	6	
*	GFLI110		generic	F	F	F	I	F	T	515	6	
*	GFLI130		generic	I	F	F	I	F	T	515	6	
*	GFLI131		generic	I	F	F	I	F	T	515	6	
*	GFLI300		generic	F	F	F	I	F	T	515	6	
** indicates a unmodified default entry												
** * indicates a modified default entry												
User Defined Supported ONTs												
Def	Vendor Name	Product Name	ONT Type	DBR	EXT	64b EXT	R11 Cnt	Rtp	T1 Pro	Mgt Id	NSR Grt	
*	ATFJ	ActionTec defaults	generic	I	F	F	I	F	T	515	32	
*	CIGG	CIG defaults	generic	F	I	F	F	T	T	3	32	
*	IPHO	IPHOTONIX defaults	generic	F	I	F	I	F	T	100	32	
*	XAVI	XAVI defaults	generic	I	F	F	I	F	T	515	32	
** indicates a unmodified default entry												
** * indicates a modified default entry												

Figure 14-4. Removing Vendor Name

14.7 Restoring a Fixed Part Number Entry to Default Value

In the following example, part number 1179870F2 is being restored to its default value.

Note that the value for part number 1179870F2 under the **Rll Cnt** heading is “F”. The default value should be “T”. The variation is denoted by “*”. Note the change in [Figure 14-6](#).

To restore a fixed entry to its default value, complete the following:

```
TA5000#configure terminal
```

```
TA5000(config)#no ont-capability part-number 1179870F2
```

```
TA5000(config)#do show ont-capability
```

The following table is displayed:

```
TA5K-TEST1#show ont-capability
User Defined Supported ONTs
```

Def	Part Number	Product Name	ONT Type	DBR	EXT	64b EXT	Rll Cnt	Supported Rtp	Tl Pro	Mgt Id	NSR Grt
*	1179870F1	508UP OUTDOOR MDU 8	adtranmdu	F	T	F	T	F	T	515	32
*	1179870F2	508UP OUTDOOR MDU 8	adtranmdu	F	T	F	F	F	T	515	32
*	1287701G1	TA351 2ND GEN OUTDO	adtran300	F	T	F	T	F	T	515	32
*	1287702G1	TA352 2ND GEN OUTDO	adtran300	F	T	F	T	F	T	515	32
*	1287702G1C	TA352 2ND GEN OUTDO	adtran300	F	T	F	T	F	T	515	32
*	1287702G1Q	TA352 2ND GEN OUTDO	adtran300	F	T	F	T	F	T	515	32
*	1287702G3	TA352H 2ND GEN OUTDO	adtran300	F	T	F	T	F	T	515	32

Figure 14-5. Entry Before being Restored to Default Value

```
TA5K-TEST1#configure terminal
TA5K-TEST1(config)#no ont-capability part-number 1179870F2
TA5K-TEST1(config)#do show ont-capability
User Defined Supported ONTs
```

Def	Part Number	Product Name	ONT Type	DBR	EXT	64b EXT	Rll Cnt	Supported Rtp	Tl Pro	Mgt Id	NSR Grt
*	1179870F1	508UP OUTDOOR MDU 8	adtranmdu	F	T	F	T	F	T	515	32
*	1179870F2	508UP OUTDOOR MDU 8	adtranmdu	F	T	F	T	F	T	515	32
*	1287701G1	TA351 2ND GEN OUTDO	adtran300	F	T	F	T	F	T	515	32
*	1287702G1	TA352 2ND GEN OUTDO	adtran300	F	T	F	T	F	T	515	32
*	1287702G1C	TA352 2ND GEN OUTDO	adtran300	F	T	F	T	F	T	515	32
*	1287702G1Q	TA352 2ND GEN OUTDO	adtran300	F	T	F	T	F	T	515	32
*	1287702G3	TA352H 2ND GEN OUTDO	adtran300	F	T	F	T	F	T	515	32

Figure 14-6. Restored Entry to Default Value

14.8 Restoring Vendor Entry to Default Value

In the following example, vendor IPHO is being restored to its default value.

To restore an entry to its default value, complete the following:

```
TA5000#configure terminal
```

```
TA5000(config)#do show ont-capability
```

The following table is displayed:

Note the variation is denoted by “*”.

' * ' indicates a unmodified default entry											
' * * ' indicates a modified default entry											
User Defined Supported ONTs				Capabilities Supported							
Def	Vendor Name	Product Name	ONT Type	DBR	EXT	64b EXT	R11 Cnt	Rtp	T1 Prv	Mgt Id	NSR Grt
*	ATFJ	ActionTec defaults	generic	T	F	F	T	F	T	515	32
*	CIGG	CIG defaults	generic	F	T	F	F	T	T	3	32
* *	IPHO	IPHOTONIX defaults	generic	F	T	F	T	F	T	100	6
*	XAVI	XAVI defaults	generic	T	F	F	T	F	T	515	32

Figure 14-7. Restoring Vendor Entry to Default Value

As the table indicates, the IPHO entry has been modified.

Restoring the vendor IPHO to its default values is on the next page.

To restore a fixed entry to its default value, complete the following:

```
TA5000#configure terminal
```

```
TA5000(config)#no ont-capability vendor-name IPHO
```

```
TA5000(config)#do show ont-capability
```

The following table is displayed:

Note that the IPHO entry has returned to its Default Value.

TA5K_TEST1#configure terminal											
TA5K_TEST1(config)#no ont-capability vendor-name IPHO											
TA5K_TEST1(config)#do show ont-capability											
User Defined Supported ONTs											
Capabilities Supported											
Def	Part Number	Product Name	ONT Type	DBR	EXT	64b EXT	R11 Cnt	Rtp	T1 Pro	Mgt Id	NSR Grt
*	1179870F1	508UP OUTDOOR MDU 8	adtranmdu	F	T	F	T	F	T	515	32
*	1179870F2	508UP OUTDOOR MDU 8	adtranmdu	F	T	F	T	F	T	515	32
*	1287701G1	TA351 2ND GEN OUTDO	adtran300	F	T	F	T	F	T	515	32
*	1287702G1	TA352 2ND GEN OUTDO	adtran300	F	T	F	T	F	T	515	32
*	1287702G1C	TA352 2ND GEN OUTDO	adtran300	F	T	F	T	F	T	515	32
*	1287702G1Q	TA352 2ND GEN OUTDO	adtran300	F	T	F	T	F	T	515	32
*	1287702G3	TA352H 2ND GEN OUTDO	adtran300	F	T	F	T	F	T	515	32
*	1287711G1	TA361 2ND GEN OUTDO	adtran300	F	T	F	T	F	T	515	32
*	1287712G1	TA362 2ND GEN OUTDO	adtran300	F	T	F	T	F	T	515	32
*	1287712G1Q	TA362 2ND GEN OUTDO	adtran300	F	T	F	T	F	T	515	32
*	1287712G3	TA362H 2ND GEN OUTDO	adtran300	F	T	F	T	F	T	515	32
*	1287713G1	TA364 2ND GEN OUTDO	adtran300	F	T	F	T	F	T	515	32
*	1287715G1	TA362R 2ND GEN OUTDO	adtran300	F	T	F	T	F	T	515	32
*	1287722G1	TA372 2ND GEN OUTDO	adtran300	F	T	F	T	F	T	515	32
*	1287722G2	TA372R 2ND GEN OUTDO	adtran300	F	T	F	T	F	T	515	32
*	1287735G1	TA324 2ND GEN INDOO	adtran300	F	T	F	T	F	T	515	32
*	1287735G2	TA324 2ND GEN INDOO	adtran300	F	T	F	T	F	T	515	32
*	1287736G1	TA334 2ND GEN INDOO	adtran300	F	T	F	T	F	T	515	32
*	1287736G2	TA334 2ND GEN INDOO	adtran300	F	T	F	T	F	T	515	32
*	1287781F1	424RG 4th GEN INDOO	adtran400	F	T	F	T	T	T	515	32
*	1287781F2	424RG 4th GEN INDOO	adtran400	F	T	F	T	T	T	515	32
*	1287786F1	401 4th GEN INDOO	adtran400	F	T	T	T	T	T	515	32
*	1287787F1	411 4th GEN INDOO	adtran400	F	T	T	T	T	T	515	32
*	1287787FiN	411 4th GEN INDOO	adtran400	F	T	T	T	T	T	515	32
*	1287800F1	602 XGS-PON INDOO	adtran600	F	T	T	T	F	T	515	32
*	1287801F1	400 4th Gen INDOO	generic	F	F	F	T	F	T	0	32
*	1287802F1	452 4th GEN OUTDOOR S	adtran400	F	T	T	T	T	T	515	32
*	1287803F1	454 4th GEN OUTDOOR S	adtran400	F	T	T	T	T	T	515	32
*	1287812F1	462 4th GEN OUTDOOR S	adtran400	F	T	T	T	T	T	515	32
*	1287813F1	464 4th GEN OUTDOOR S	adtran400	F	T	T	T	T	T	515	32
*	1287823F1	621X XGS-PON INDOO	adtran600	F	T	T	T	F	T	515	32
*	1287823FiT	621X XGS-PON INDOO	adtran600	F	T	T	T	F	T	515	32
*	1287823F2	621X XGS-PON INDOO	adtran600	F	T	T	T	F	T	515	32
*	1287825F1	601X XGS-PON INDOO	adtran600	F	T	T	T	F	T	515	32
*	1287835F1	424 4th GEN INDOO	adtran400	F	T	T	T	T	T	515	32
*	1287835FiC	324 4th GEN INDOO	adtran400	F	T	T	T	T	T	515	32
*	GFLT100		generic	T	F	F	T	F	T	515	6
*	GFLT110		generic	F	F	F	T	F	T	515	6
*	GFLT130		generic	T	F	F	T	F	T	515	6
*	GFLT131		generic	T	F	F	T	F	T	515	6
*	GFLT300		generic	F	F	F	T	F	T	515	6
'*' indicates a unmodified default entry											
'* *' indicates a modified default entry											
User Defined Supported ONTs											
Capabilities Supported											
Def	Vendor Name	Product Name	ONT Type	DBR	EXT	64b EXT	R11 Cnt	Rtp	T1 Pro	Mgt Id	NSR Grt
*	ATFJ	ActionTec defaults	generic	T	F	F	T	F	T	515	32
*	CIGG	CIG defaults	generic	F	T	F	F	T	T	3	32
*	IPHO	IPHOTONIX defaults	generic	F	T	F	T	F	T	100	32
*	XAVI	XAVI defaults	generic	T	F	F	T	F	T	515	32

Figure 14-8. Restored Entry to Default Value

14.9 ONT Capability Provisioning Terms

The following terms are used when implementing Capability Provisioning.

- **dbru-status** - Dynamic bandwidth reports upstream status support (default value = false). This defines whether the ONT supports explicit status reporting of its buffer status for dynamic bandwidth allocation as defined in ITU-T G.998.
- **extended-64bit-pm** - Ethernet frame extended PM 64 bit support (default value = false). This defines whether the ONT supports ethernet frame extended PM 64 bit as defined in ITU-T G.998.
- **extended-pm** - Ethernet Frame Extended PM support (default value = false). This defines whether the ONT supports ethernet frame extended PM as defined in ITU-T G.998.
- **mgmt-me-id** - IP host management ME id (default value = 515). This defines the instance ID of the managed entity used for IP host management at the ONT.
- **nsr-grant-size** - Non-status reporting grant size in bytes/frame (default value = 32). This defines the number of bytes per frame granted for idle slot detection on non-status reporting ONTs on the PON. This number includes 5 bytes for the GEM header. This is a per PON implementation, so the grant size used by the PON will be that of the ONT with the highest required nsr-grant-size.
- **ont-type** - Ont type/generation (default value = generic). This item indicates the type or generation of the ONT. There are types listed for ADTRAN ONTs, as well as a generic selection for non-ADTRAN ONTs.
- **product-name** - ONT product name (default value = ""). This is the name (45 characters maximum) that will be displayed when the **show ont-capability**, the **show remote-devices <remote-index>**, and **show running-config ont-capability** commands are selected. If the product name is longer than 21 characters, it will be truncated in the table displayed by the **show ont-capability** command, but it should display in its entirety in the **show remote-devices <remote-index>** and the **show running-config ont-capability** commands.
- **rolling-counter** - Rolling counter PM support (default value = false). This item defines whether the ONT supports continuous accumulation PM as defined in ITU-T G.998.
- **rtp** - Real-time transport protocol PM support (default value = false). This item defines whether the ONT supports RTP PM history data as defined in ITU-T G.998.
- **t1-prov** - T1 provisioning over OMCI support (default value = false). This item defines whether the ONT supports T1 provisioning over OMCI as defined in ITU-T G.998.

15 Warranty and Contact Information

15.1 Warranty

Warranty information can be found at:

www.adtran.com/warranty.

15.2 Contact Information

For all customer support inquiries, please contact **ADTRAN** Customer Care:

Contact	Support	Contact Information
Customer Care	From within the U.S. From outside the U.S. Technical Support: ■ Web: Training: ■ Email: ■ Web:	1.888.4ADTRAN (1.888.423.8726) + 1.256.963.8716 www.adtran.com/support training@adtran.com www.adtran.com/training www.adtranuniversity.com
Sales	Pricing and Availability	1.800.827.0807

Acronyms

ADTRAN	Advanced Transmissions
ARP	Address Resolution Protocol
CLEI	Common Language Equipment Identification
CLI	Command Line Interface
CRC	Cyclic Redundancy Checks
C-VLAN	Customer VLAN
DBRu	Dynamic Bandwidth Report upstream
DCE	Data Communications Equipment
DHCP	Dynamic Host Configuration Protocol
DLC	Digital Loop Carrier
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
EVC	Ethernet Virtual Connection
FTTP	Fiber to the Premises
FXS	Foreign Exchange Service
GEM	GPON Encapsulated Method
GFP	Generic Framing Procedure
GPON	Gigabit Passive Optical Network
GR-303	Generic Requirement 303
IETF	Internet Engineering Taskforce
IP	Internet Protocol
LED	Light Emitting Diode
MDU	Multi-unit Dwellings Unit
MGCP	Media Gateway Control Protocol
NAS	Network Access Server
ODN	Optical Distribution Network
OLT	Optical Line Terminal
ONT	Optical Network Terminal
PIR	Peak Information Rate
PON	Passive Optical Network
POTS	Plain Old Telephone Service
PPP	Point to Point Protocol
PPPoE	Point to Point Protocol over Ethernet
PSTN	Public Switched Telephone Network
RSSI	Received Signal Strength Indicator

RTP	Real-Time Transport Protocol
RTCP	Realtime Control Protocol
SFP	Small Form-factor Pluggable
SIP	Session Initiation Protocol
S-Tag	Service Tag
TDM	Time-division Multiplexing
TLS	Transport Layer Security
UNI	User to Network Interface
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol