C7 R8.0 Provisioning Guide

November 2012

 # 220-00494, R11

Contents

About This Guide.....15

What You Need to Know.....16

Intended Audience.....17

Prerequisites.....18

Related Documentation.....19

Chapter 1: Getting Started.....20

Supported Hardware and Software.....21

Configure Your PC to Connect to the C7 Using iMS.....22

C7 Factory Settings for the Front Ethernet Port.....22
PC Configuration.....22
Configuring Your PC to Connect to the C7.....22
Connecting Your PC to the C7 Front Ethernet Port (E1).....23
Connecting to the Serial Management Ports.....23

Start Calix C7 iMS.....24

One-Time Install of the Java Runtime Environment.....24
Starting C7 iMS from the Front Ethernet (E1) Port.....24
Startup View of Your Network.....24

Starting CMS Desktop.....26

iMS and CMS Views.....29

Screen Components.....31

Menu.....31
Toolbar.....34
Work Area.....35
Selection Filter.....35

Navigating and Selecting Objects.....36

Navigate and Select Objects.....36

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Selecting Multiple Objects on the Navigation Tree 36
Selecting a Range of Objects on the Navigation Tree 36
Navigating in the Work Area 37
Selecting a Range of Objects in the Work Area 37
Filtering Objects for Display in the iMS Work Area 38

Useful Techniques 40

Switch Between Table and Form Views in the iMS Work Area 40
View Parameter Definitions 41
Sort by Column 41
Move Table Columns 41
Resize Table Columns 42
Hiding Table Columns 42
Generate a Custom Report 42
Status Monitor 43
Refresh 43

Chapter 2: Performing Network-Level Tasks 45

Define Network Nodes 46

Change Network Date and Time 48

Managing C7 Security 49

Categories and Access Privileges 49
Other User Attributes 50
Implement Built-In and Custom Security Templates 51
Create User Accounts 53
Delete User Accounts 54
Viewing and Editing User Security Information 54
Secure Shell and SFTP Operations 54
Changing the Password 55
Allowing Messages 56
Inhibiting Messages 56
Inhibiting a User 56
Allowing a User 57
Viewing User Session Information 57
Logging Out a User 58
View and Edit Global Security 59
Remote Authentication via RADIUS 60
SSH Security Overview 64
SSH Security Setup 66
Serial Port Access 67
Access Control List 67

View General Network Information 69

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

View and Modify SNMP Settings 70

Configure Grades of Service 73

Overview of Grade of Service Profiles 73
Create a Grade of Service Profile 75

Configure Network Profiles and Templates 77

Managing Global C7 Profiles in CMS 77
Creating a Traffic Profile 89
Creating an xDSL Template 94
ONT Profile Parameters 108

Configure a Data Communication Channel 110

SONET DCC Tunneling 113

DCC Tunnel Considerations 113
End-to-End with the VIA Parameter 114
Protection 114
Data Links 114
Creating DCC Tunnels 115
Modifying a Cross-Connect Type 116

Viewing and Printing Alarms, Events, and Logs 117

Viewing Alarms 117
View a Filtered Alarm List (C7 only) 117
Other Viewing Options 118
Viewing Events 118
Alarm and Event Display Options 120
Viewing Logs 121
Resetting History Logs 122
Generating Custom Print Reports 122

Working with System Cross-Connections 124

Cross-Connect Viewing Options 124
View a List of Cross-Connections and Hops 127
Work with VP Cross-Connects 128
Add Drops to STS, VP, and VC Cross-Connects 133
Delete Cross-Connects and Hops 135

Bandwidth Reservation for Traffic Flows 138

Bandwidth Constraint IDs 139
Bandwidth Links 143

AMP Routing 149

Configuring the Remote AMP Ports for Management 151
Creating the In-Band Management Channel 152
Enable Routing for the Management Channel 153

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Chapter 3: Performing C7 Node-Specific Tasks 155

Node Assignment and Configuration 156

Assign C7 Shelves to a Node 156
Define the C7 Node Type 156
Configure Two Nodes in an ODC-120 158
Configure a Node to Use a Test Head 158

Alarm-Related Tasks 160

Set Alarm Cut-Off Attributes 160
Set Alarm Reporting for Multi-Shelf C7 Nodes.....160
View Node-Specific Alarms.....161
Set Environmental Alarm Attributes 161

Chapter 4: Performing C7 Shelf-Specific Tasks 163

View Shelf Status.....164

Set Shelf Power Parameters 166

Common Controller Tasks.....168

Configuration Rules for AMP and ATP Ethernet Login Channels 168
Configure the AMP or ATP Front Ethernet Port (E1) 170
Configure the AMP or ATP Rear Ethernet Port (E2).....171
Configure the AMP or ATP In-Band Management Ethernet Port (E3) 171
Configure Static IP Routes to the AMP or ATP Card 180
Configuring RAP-10GE In-Band Management Ethernet Port (E4).....182

Timing.....184

Overview of Timing Scenarios and Parameters.....184
Timing Parameters.....185
Configure Shelf Timing 187
Configure Timing for Third-Party Equipment.....189
Holdover Timing.....190

Shelf View—Bandwidth.....191

Viewing the Fan Tray.....192

Configuring Equipment Protection 193

Equipment Protection.....193
About 1:1 Equipment Protection 193
About 1:N Equipment Protection.....195
Metallic Services Protection Modules 198
Configuring 1:1 Equipment Protection 199
Configuring 1:N Equipment Protection.....201

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Protection Switching User Commands....204

Guidelines for Using Equipment Protection Switching 204
Switching Commands 205

Chapter 5: Provisioning Network Transport 209

Overview of Transport Protection....210

Protecting Traffic on Optical Fibers....210
UPSR with Packet Aggregation 212
1+1 Linear Automatic Protection Switching 213
1:1 Linear Automatic Protection Switching....214

Configuring an ERPS Transport Ring....215

Configuration Rules for an ERPS Transport Ring....217
Quick Turn-Up Outline for ERPS Transport....218
Configure an ERPS Transport Ring....219

Configuring RSTP Protected Links....234

Configure an RSTP Transport Ring 235

Creating a VLAN Interface for RSTP 236

Configuring Linear Point-to-Point Ethernet Transport with RSTP or LAG....239

Configure a Linear Point-to-Point Ethernet Transport with LAG 242

Configuring UPSR with Packet Aggregation....245

Quick Turn-Up Outline 247
Configure Optical Transport Topology and Protection 248

Configuring DS3p Transport Links 250

Configuring T1 IMA Transport....252

Quick Turn-Up Outline for T1 IMA Transport 252
Configuration Rules for T1 IMA Transport 252
T1 Port Parameters for Use in an IMA Group 254
Configure T1 Ports for Use in an IMA Group 255
Configure HDSL Ports for IMA Transport with IMA-12 Cards 256
Configure ATM Resource Ports for IMA Service (IMA-12 Cards) 257
Create an IMA Group and Add T1s....258
Configure an IMA Group for ATM Transport....260
Other IMA Group Fields for ATM Transport....261

Configuring T1 Transport Groups....263

Quick Turn-Up Outline for T1 TDM Transport....263
Configuration Rules for T1 TDM Transport....263
Configure Ports for T1 Transport 265

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configure HDSL Ports for TDM Transport 266
Create a T1 Transport Group....268
Assign Ports to a T1 Transport Group 270

Chapter 6: Activating C7 Subscriber Service 273

Before You Begin 274

Running a Pre-Service DSL Test with Single-End Line Testing (SELT)....275

Creating a Global Video Subscriber Template....276

(EXA) xDSL Subscriber Templates....276
(EXA) ONT Subscriber Templates....279
(MP) ADSL2-Based Video Subscriber Template 280
(MP) VDSL2-Based Video Subscriber Template 284
(MP) ONT Video Subscriber Template 287

Creating a Global Data Subscriber Template....289

Creating a Global Subscriber Template by Importing a C7 Network Template 292

Modifying Subscriber Templates 293

Creating a Subscriber Uplink ID....294

Multiple Port Service Activation....295

Activating Subscribers 295
Viewing Subscriber Services 295
Reconfiguring Subscribers (Using CMS) 296
Deleting Subscriber Services (Using CMS) 298

Single-Port and ONT Service Activation....301

Activating Subscribers 302
Viewing C7 Service Activation Details 303
Performing a Subscriber Search....303
Deleting Video Streams 305
Modifying Port Settings....305

Configuring the xDSL Power Shutdown Priority 306

Video Provisioning Features in CMS 307

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Chapter 7: Provisioning Ethernet-over-SONET Services.....309

Required Setup 310

Starting Point 310
Ethernet-over-SONET Transport Rules 310
Prerequisites for Provisioning Service Drops 311
Configuring Ethernet Ports.....312

Ethernet-over-SONET Provisioning Tool.....314

Work Area.....315
Using the Tool.....317
Deleting Provisioning 320

Creating Ethernet-over-SONET Components Manually 322

Create an Extended LAN (XLAN) 323
Create Logical Switches for Shelves in the XLAN 324
Assign VTI Ports to Logical Switches.....325
Create STS Paths for Ethernet Transport 326
Cross Connecting VTI Ports to STS Paths 327
Configuring Ethernet Ports.....330
Assigning Ethernet Ports to an LSwitch 331
Creating a Virtual LAN (VLAN) 332
Creating an Ethernet Traffic Profile.....332
Creating VLAN Ports.....333

Chapter 8: Provisioning Ethernet and IP Services 335

Ethernet Uplink and Downlink Provisioning Tools.....336

Chapter 9: Provisioning OCn Optical Services.....339

Overview of OCn Optical Port Parameters 340

Configuring OCn Optical Ports 344

Configure OCn Optical Port Parameters for Transport 344
Configure OCn Optical Port Parameters for Services 345
Change the Line Rate on a RAP-OCn or RAP2-OCn 346

Configuring OCn Optical Service Protection 348

OCn Optical Services Protection Parameter Overview 348
Configure Line Protection 349
Facility Level Protection Switching.....350

Creating STS Paths 352

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

STS Path Parameters 352
STS Mapping Rules 355
Create and Configure STS Paths 355
Delete an STS Path 357

Creating STS Cross-Connections 358

Create STS Cross-Connections 358
Cross-Connection Parameters for Viewing 359

Chapter 10: Provisioning DS3 Services 363

DS3 Card, Port, and Cross-Connection Descriptions 364

Overview of DS3 Port Parameters 364
Overview of Cross-Connection Parameters 368

Configuring DS3 Equipment Protection 369

Configuring DS3 Service 370

STS Mapping and Cross-Connections for DS3s Hi-Cap Service 370
Configure DS3s Ports for Hi-Cap Service 372
Configure DS3p Ports for ATM Traffic 373

Chapter 11: Provisioning DS1 Services 375

DS1 Port and Cross-Connection Descriptions 376

Overview of DS1 Port Parameters 376
Overview of DS1 Cross-Connect Parameters 382

Configuring DS1 Equipment Protection 383

Configuring DS1 Services 384

Configure DS1 Ports for Hi-Cap Service
over SONET or ATM Network (C7 Prov., Help) 384
Cross-Connect DS1 Ports for Hi-Cap Service 385
Configure DS1 Ports for TDM Service 386
Cross-Connect DS1 Ports for TDM Service 387
Configure T1 Ports for ATM Service 390

Configuring T1 IMA Groups 392

Create an IMA Group and Add T1s 392
Configure an IMA Group for ATM Uplink 394

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Chapter 12: Provisioning DS0 Services.....397

DS0 Port and Cross-Connection Descriptions 398

Overview of DS0 Port Parameters.....398
Overview of DS0 Port Connection Status Parameters.....401
Redlining Ports 402
Overview of DS0 Cross-Connect Parameters.....402

Configuring GR-303 Services 404

Quick GR-303 Configuration Process.....404
GR-303 Interface Group Parameter Descriptions 406
Create a GR-303 Interface Group.....408
View or Modify Attributes of a GR-303 Interface Group 410
Configure a T1 Port for a GR-303 Switch Interface 410
Assign T1 Ports to a GR-303 Interface Group 412
Creating a Voice Concentration Shelf.....414
Configure DS0 Ports for Service.....416
Cross-Connect DS0 Ports to GR-303 Interface Group CRVs 417
View CRVs.....419
Check That It All Works 419
View and Modify EOC and TMC Parameters.....420
Delete a CRV to DS0 Cross-Connect 421
Remove DS1 Associations from a GR-303 Interface Group 421
Remove a GR-303 Interface Group 422
Maximizing Bandwidth by "Hair-Pinning" T1 Circuits 422
Configuring a DS1 Port for Hi-Cap Service.....423
Creating Hi-Cap DS1 Cross-Connections.....423
Completing the Hair-Pinned Circuit.....424
DS0 Remote Voice Concentration 424

Configuring GR-57 Services 436

Quick GR-57 Service Configuration Process 436
Configure DS0 Ports for GR-57 Interface 437
Setting DS0 Port Parameters.....437
Cross-Connect Host, Remote DS0 Ports (GR-57) 438
Check That It All Works 439

Configuring GR-8 Services 440

Quick GR-8 Configuration Process 440
Create a GR-8 Interface Group.....440
View Attributes of a GR-8 Interface Group.....442
Configure a T1 Port for a GR-8 Switch Interface 443
Assign T1 Ports to a GR-8 Interface Group 445
View GR-8 Interface Group DS1s.....446
Cross-Connect DS0 Ports to a GR-8 Interface Group 447
View Cross-Connection Parameters.....449

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Check That It All Works 450
Remove GR-8 Cross-Connects and Interface Groups....450

Configuring Universal Services 452

Configure Remote Ports for Universal POTS and UVG Services 452
Configure Host Ports for Universal POTS and UVG Uplinks 453
Configure Ports for Coin Service 454
Configure Ports for EBS Service....456
Cross Connect DS0 Ports for Universal Switched Services....457

Configuring Non-Switched Services....459

Configure Ports for TO and PLAR Service....459
Set DS0 Port Parameters 461
Convert Ports Between 4-Wire and 2-Wire TO 462
Cross-Connect Ports for TO and PLAR Service 463
Configure Ports for DDS 465
Configure DS0 DP-6 and OCU DP-6 Ports....467
Cross-Connect Ports for DDS Service 467

Chapter 13: Provisioning C7 xDSL Services....471

Quick ADSL Configuration Process 472

Applying xDSL Templates 473

ADSL Tone Configurations 473

Configure the Network Uplink—Overview....474

Configure Network Uplink 476

Configuring xDSL Ports....479

Configuring the xDSL Power Shutdown Priority 480

Overview of VC Cross-Connection Parameters....481

VC Cross-Connection Requirements for ADSL 484

Common ADSL cross-connection requirements....484

Create a VC Cross-Connection for ADSL or VDSL Service 485

Check That It All Works....486

ADSL Port Retraining....487

ADSL Performance Monitoring 488

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Chapter 14: Provisioning HDSL Services 491

Overview of HDSL Port Parameters 492

Configuring HDSL Equipment Protection 496

Configuring HDSL for Hi-Cap DS1 Service.....497

Configure HDSL Ports for Hi-Cap Service 497
Cross-Connect HDSL Ports for Hi-Cap Service 498

Configuring HDSL for TDM Transport 500

Configuring HDSL for TDM Service 501

Configure HDSL Ports for TDM Service.....501
Create T0 Timeslot Cross-Connections 502

Viewing HTU.....504

Chapter 15: Provisioning PWE3 Services 505

Overview of the Calix C7 PWE3 Solution 506

PWE Card Descriptions.....507

PWE3 Timing and Clock Recovery Considerations 509

Synchronization of PWE3 Timing 511
PWE3 Timing Recommendations 512

PWE Card Settings 514

PWE Card Port Settings 516

UDP Port Settings.....519

PWE3 Application Architecture.....522

Hi-CAP Service Delivery 522
Fractional T1 Service Delivery 524

Provisioning SAToP over RAP-10GE ERPS Transport 532

Overview of Configuration.....532
Configuring the DS1-12 PWE Port Settings.....533
Configuring T1-8 PWE Port Settings.....534
Optional: Create PWE3 Template.....535
Creating Service VLAN (S-VLAN) for Source and Destination Nodes 538
Creating the VLAN Interface (VLAN-IF) Across the ERPS Domain 540
Using the PWE3 Provisioning Tool 541

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Provisioning Local Hairpinning of Full T1 (DACS) 547

Configure DS1 Ports 547
Configuring the PWE Card for Hairpinning 548
Configuring PWE Endpoints 548
Configuring Host/IP Information for Hairpinning 548

Provisioning Fractional T1 Service over Aggregated Ethernet 550

Configuring DS1 Ports 551
Creating Digital Cross-Connects for the PWE 552
Configuring the PWE Endpoint A 553
Configure the Host/IP Information for Endpoint A 554
Configuring the PWE Endpoint B 555
Configuring the Host/IP Information for Endpoint B 556

Provisioning Multiprotocol Hi-CAP T1 Service over SAToP 557

Creating the S-VLAN 558
Creating an ATM Traffic Profile 559
Provisioning Traffic Profiles using the PWE3 Bandwidth Tool 559
Provisioning the DS1 port for Hi-Cap Service 562
Create the Multiprotocol VLAN-IF for the PWE Card 562
Create the VLAN-IF for the Physical Uplink Interface (EGW card) 563
Create an IP Host for the PWE card 564
Creating the PWE Endpoint for the Pseudowire 564
Create the VLAN Interface for the PWE End Point 565
Confirming the Configuration 566

Troubleshooting PWE Services 568

Bit Error Rate Testing (BERT) Overview 569
DS1/T1 Loop-back 572

Chapter 16: Appendix A: C7 Service States 575

Primary Service State 576

Secondary Service State 577

Chapter 17: Appendix B: Security Log Events 579

Chapter 18: Appendix C: List of Acronyms 581

Chapter 19: Appendix D: PWE Card Capacities 585

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

About This Guide

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

What You Need to Know

Calix Integrated Management System (iMS) and Calix Management System (CMS) are graphical user interfaces that you use to configure and monitor all of the C7 nodes on a network.

CMS is client/server application used to manage multiple Calix C7 networks, E5-100 service units, E5-300/400 nodes, E7 GPON or AE networks, B6 AE networks, and F5 and FiberDrive Gigabit Passive Optical Network (GPON) platforms.

With iMS and CMS, you can do the following:

- View a diagram of your network topology.
- Configure all aspects of a C7 network.
- Manage timing and synchronization.
- View current alarms, including online help information for alarms.
- View and clear performance monitoring registers.

You start iMS by using Internet Explorer to connect to any C7 node in the network. See *Configure Your PC to Connect to the C7* (on page 22).

At the C7 network level in CMS, you can perform the same provisioning operations using a similar user interface as iMS.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Intended Audience

The C7 Provisioning Guide is for those personnel responsible for network hardware and software installation, node and network setup, and services configuration.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Prerequisites

The information and procedures in this guide assume the following:

- The C7 shelf (or shelves) are properly installed and tested.
- All required materials are onsite.
- The user has experience and comfort with computer systems, software, and electronic test equipment.
- The user has knowledge of telecommunications and engineering standards.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Related Documentation

You can access Calix product documentation from the Calix Resource Center online at *www.calix.com* (*https://www.calix.com/portal/site/resourcecenter/*).

The Calix C7 Release R8.0 documentation set includes:

- *Calix C7 Engineering & Planning Guide*
- *Calix Upgrade Program (CUP) Application Guide*
- *Calix C7 Provisioning Guide*
- *Calix C7 GPON Applications Guide*
- *Calix C7 Broadband Data Services Guide*
- *Calix C7 Video Services Guide*
- *Calix C7 Voice Services Guide*
- *Calix C7 VoIP Services Guide*
- *Calix C7 Ethernet and IP Services Guide*
- *Calix C7 Maintenance Guide*
- *Calix C7 Troubleshooting Guide*
- *Calix C7 TL1 Management Interface Reference*
- *Calix C7 SNMP MIBs*
- *Calix 76xGX SBU/MDU ONT Installation Guide*
- *Calix 76xGX-R (Rack Mount) SBU/MDU ONT Installation Guide*
- *Calix 700GE SFU ONT Installation Guide*

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Chapter 1

Getting Started

This section describes the use of Calix C7 integrated Management Software (iMS) and Calix Management System (CMS) user interface, as well as information on configuring in-band management, viewing and printing alarms, working with system cross connections, and managing security.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Supported Hardware and Software

Network Software Version

In C7 release 8.0, the software version numbering scheme, with four fields, has the following format:

<Major>.<Minor>.<Point>.<Dev>

For example, 8.0.1.1

- **Major** releases contain large scale architectural changes, paradigm shifts, or completely new features on a large scale.
- **Minor** releases contain new features which enhance or improve the product relative to the base Major release.
- **Point** releases contain issue resolutions, but may also contain minor enhancements and features.
    - The first Controlled Availability (CA) release will have the Point field set to "1," as in 8.0.**1**.1. Further CA releases will use single digits from "2-9."
    - The General Availability (GA) releases will have the Point field set to a single digit number (usually the last CA number used).
    - The first Maintenance Availability (MA) release will have the Point field set to "10," as in 8.0.**10**.200. Further MA releases will use increments of "10" on the point release (for example, 20, 30 …).
    - The Limited Distribution Availability (LDA) releases utilize the minor digit in the point field (for example, "2" in 8.0.1**2**.320).
- **Dev** releases contain issue resolutions or minor enhancement changes from the point release on which it is based.

All fields are integers ranging from 0-999

Calix C7 iMS

To review the iMS system requirements, see the latest C7 Release Notes, accessible online on the Calix Customer Resource Center at www.calix.com.

CMS Desktop

To review the CMS host server system and client requirements, see the latest Calix Management System (CMS) Release Notes, accessible online on the Calix Customer Resource Center at www.calix.com.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configure Your PC to Connect to the C7 Using iMS

You must configure the Ethernet port of your computer before making the first connection to your C7 network.

Once connected, you can change Ethernet log-on parameters on the C7 to support connections following your company standards.

C7 Factory Settings for the Front Ethernet Port

The C7 shelf ships with the front Ethernet port (E1) on the AMP or ATP card active and set to the following configuration:

- **IP:** 192.168.1.1
- **Subnet:** 255.255.255.0
- **Gateway:** 0.0.0.0

PC Configuration

Configure the Ethernet port on your PC to the following settings:

- **IP:** 192.168.1.2 (The last number can be 2 to 254. Calix recommends 2.)
- **Subnet:** 255.255.255.0
- **Gateway:** (Leave this setting blank).

Configuring Your PC to Connect to the C7

This procedure applies to PCs running Microsoft Windows XP or Windows 2000. Before making changes (see Steps 2 and 3), be sure to record your current settings to restore them later, if needed.

To configure your PC to connect to the C7

1. On the Start menu, click **Settings** > **Network Connections**. Right-click **Local Area Connection**, and then click **Properties**.
2. In the Local Area Connection Properties dialog box:
   a. On the General tab, click **Internet Protocol (TCP/IP)**.
   b. Verify that the check box for Internet Protocol (TCP/IP) is selected.
   c. Click **Properties**.
3. In the Internet Protocol (TCP/IP) Properties dialog box:

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

a. Click the **Use the Following IP Address** option to select it.

b. In the IP Address box, type **192.168.1.2**

c. In the Subnet Mask box, type **255.255.255.0**

d. In the Default Gateway box, verify that it is blank.

e. Leave both DNS Server address boxes empty.

4. Click **OK** in all open dialog boxes to save your network connection settings.

Connecting Your PC to the C7 Front Ethernet Port (E1)

Use a straight-through Ethernet cable (with RJ-45 connector) to connect your PC to the Calix C7 shelf.

Connect one end of the cable to your PC Ethernet port. Connect the other end of the cable to the E1 Ethernet port on the front of the AMP or ATP card (located in the center slot of the C7 shelf).

Connecting to the Serial Management Ports

This section describes how to connect your PC to the RS-232 serial management ports on the Calix C7. Front (S1) and rear (S2) serial ports are located on the AMP or ATP control card in a C7 shelf. The S1 and S2 ports provide local console access to the C7 TL1 interface.

Note: The S1 and S2 ports do not provide access to iMS.

Serial port connections to the C7 TL1 interface are established through a console session. You can use any standard terminal emulation software (such as HyperTerminal or ProComm Plus) to establish the console connection. For example, PCs running Microsoft Windows XP or 2000 are typically equipped with HyperTerminal by default. Optionally, you can also connect to the C7 TL1 interface via telnet.

Follow the procedures in the order listed below to connect to the C7 TL1 interface via a serial management port.

1. To connect to your pc to the C7
2. To configure your PC COM port and the C7 serial port settings
3. To log in to the C7 TL1 interface

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Start Calix C7 iMS

Start the C7 iMS application by entering the IP address of the C7 shelf into your browser's Address box.

One-Time Install of the Java Runtime Environment

C7 iMS operates using Java Runtime Environment (JRE) software. If JRE is not installed on your PC, click the **Java Runtime** link on the opening Web page to download the latest version.

Note: Attempts to connect to iMS that fail or return an error message typically indicate that JRE is not installed on your PC. Install JRE before attempting to connect to iMS again.

Starting C7 iMS from the Front Ethernet (E1) Port

Complete the steps below to start C7 iMS from the front Ethernet (E1) port.

To start C7 iMS from the front Ethernet (E1) port

1. Start Internet Explorer, and then in the Address box enter **192.168.1.1** for the front Ethernet port (E1) IP address of the C7.

   Note: You can enter other IP addresses assigned to the C7 shelf after you configure the Ethernet port to your standards.

2. On the initial screen, click **Calix iMS**.
3. In the Login to iMS dialog box, do the following:
   a. In the User box, type **sysadmin**.
   b. In the Password box, type **sysadmin**.
   c. Click **OK**.

To ensure system security, Calix recommends changing the default **sysadmin** user name and password after logging in for the first time.

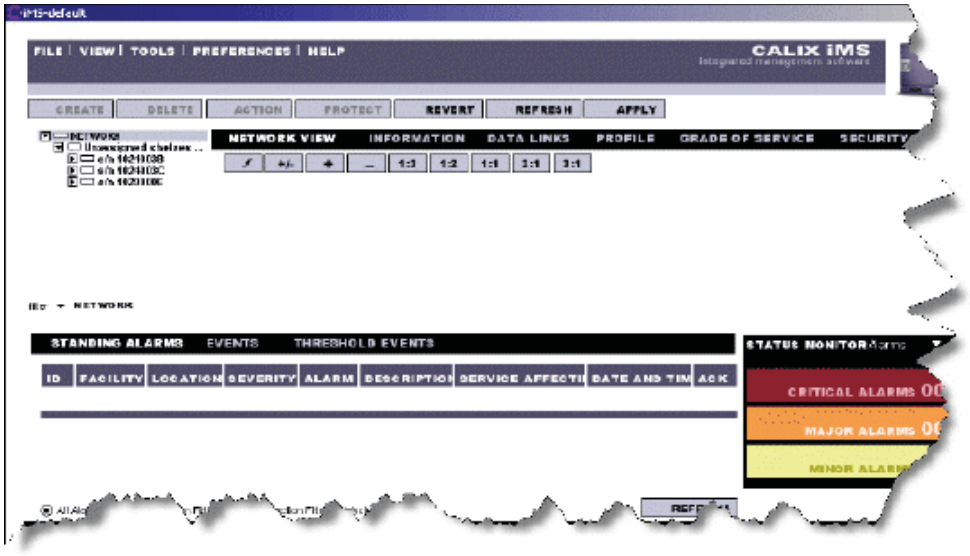
Startup View of Your Network

The first time you log in to a new C7 network, you will see the following:

- An empty Work Area with no network topology.
- One entry in the Navigation Tree named Unassigned Shelves.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

You must use the **Add Shelves to Network** tool to group shelves into nodes. See *Define Network Nodes* (on page 46).



Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Starting CMS Desktop

Once the CMS server software and CMS Desktop have been installed and you have verified that the CMS server is operating, as the system administrator, start CMS from a PC or workstation. You can then create CMS users, regions, networks, and review or change the system defaults.

Security recommendations for CMS system administration

After logging in to CMS for the first time, Calix strongly recommends that you do the following:

- Change the password of the rootgod user (Step 3 in the following procedure).
- Create another user under the Administrators user group for the purpose of managing CMS system security. (For instructions, see the topic, "Creating a CMS User," in the *Calix Management System (CMS) Guide*.

Information you need to open CMS Desktop

To log in to CMS Desktop, you need the following:

- CMS user name and password, provided by your CMS system administrator.

  Note: The initial default user name is **rootgod** and the initial default password is **root**.

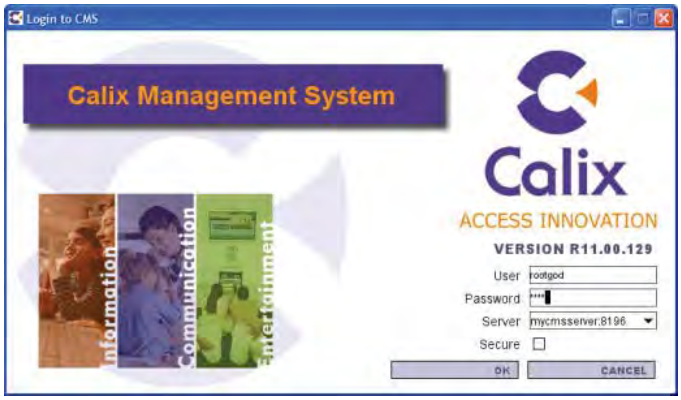
- The IP address or DNS name of your server, provided by your CMS or UNIX system administrator.
- The port number on the CMS server (typically 8196), provided by your UNIX system administrator.
- If you are remotely accessing a network protected by a firewall, you may need to connect via a Virtual Private Network (VPN) in order to access the host server. Contact your IT or CMS system administrator for your company requirements.

To start CMS Desktop

1. From the Windows Start menu, click **Programs** > **Calix** > **Start CMS**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

2. At the Login screen, do the following:



a. In the **User** box, type the user name.

b. In the **Password** box, type the password.

c. In the **Server** box, type the IP address or DNS name of your CMS server, followed by the port number (by default, 8196). Use the format *[server_ID]*:*[port number]*, where *[server_ID]* is the IP address or DNS name of your CMS server.

d. (Optional) Select the **Secure** check box for a secure (SSH) connection to the CMS server.

e. Click **OK**.

If the CMS Desktop version is different than the version on the CMS server, a popup message prompts you to synchronize to the software version on the CMS server. To do so, click **Yes**, and then log in again to open CMS Desktop.

In CMS Desktop, your user ID displays at the bottom of the screen on the left side of the status bar.

3. After logging in to CMS for the first time, Calix strongly recommends that you change your password, as follows:

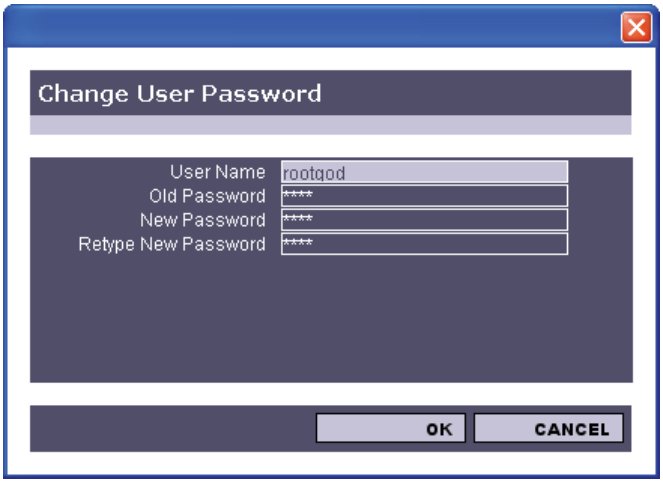
a. On the Navigation Tree, click **CMS**.

b. In the Work Area, click **Security** > **Users**.

c. Expand the security domain and **Administrators** user group, and then click the **rootgod** user account.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

d. Click **Action** > **Change Password**. The Change User Password dialog box opens.



e. In the **Old Password** box, type **root**.

f. In the **New Password** and **Retype New Password** boxes, type the new password.

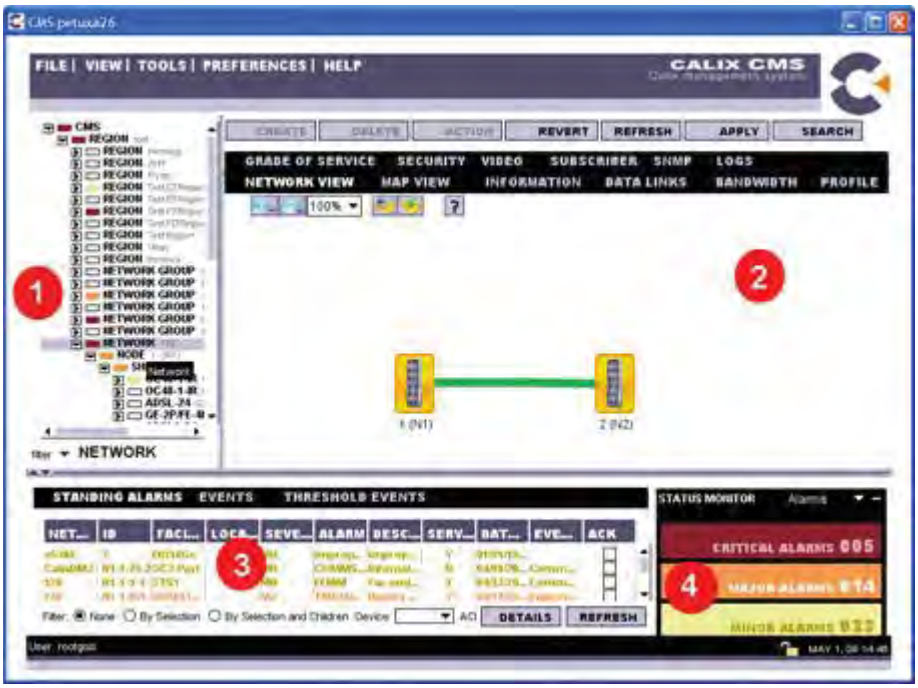
Note: User account passwords are case-sensitive. The required password length and minimum number of numeric and special characters are determined by the CMS security settings set by your CMS system administrator. Special characters are as follows: @.#$%{}!_?-

g. Click **OK**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

iMS and CMS Views

The main screen in iMS and CMS Desktop is divided into four frames:



1. **Navigation Tree:** Displays a customizable, hierarchical list of network element objects: networks, nodes, shelves, cards, ports, and paths. CMS additionally displays administrative settings at the highest level, followed by a root region and regions and network groups for organizing network elements.
2. **Work Area:** When the Subscriber Search pane is not displayed (CMS only), this area of the screen displays information about the level selected on the Navigation Tree. At the network or node level and below on the Navigation Tree, the Work Area provides access to view or modify network and node configuration settings. On the Navigation Tree, you can drill down to view details down to the port or path level in the Work Area. In CMS Desktop, to toggle to the configuration menus from the Subscriber Search pane, at the top of the screen, click the **Previous Panel** link; to toggle back to the Subscriber Search pane, click the **Last Search** link.
3. **Status Monitor**: Displays a count of critical, major, and minor alarms. In addition, you can use the drop-down menu to the right of Status Monitor and select **Resource** to display total memory allocated and in use by the application.
4. **Alarm Table:** Displays a customizable table of all standing alarms, events, and threshold events.

At the bottom of the screen, the status bar displays the user name on the left side and the date and time (for CMS, the CMS server time) on the right side.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Screen Components

Menu

The C7 iMS and CMS menu bars provide pull-down menus to navigate within the system, to create, edit and retrieve data, and to perform various other actions.

Using the File Menu

The File menu is context sensitive. Items may appear **highlighted** (available) or dimmed (unavailable) depending on the currently active object.

Using the Tools Menu

The Tools menu provides several links to tools, tasks, and additional menus.

Refresh All

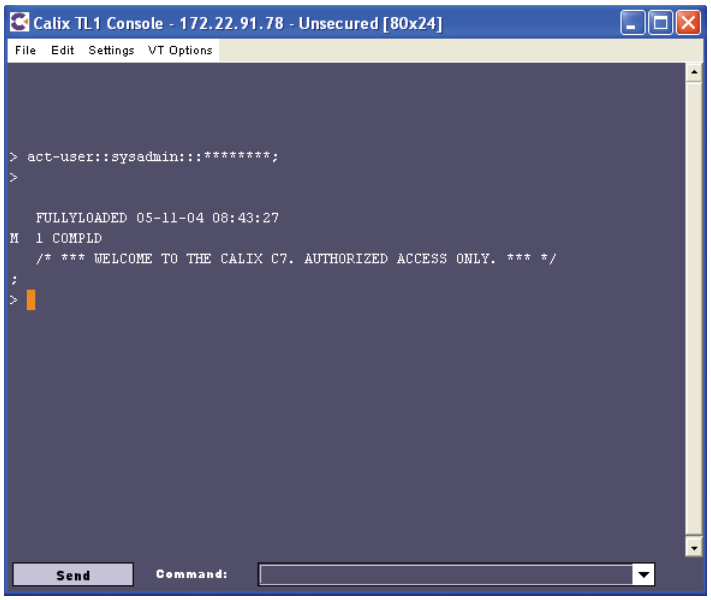
Use the Refresh All function to collapse the Navigation Tree to the card level. This is useful when you have expanded a large number of cards to view ports and now want to view only cards within the shelves.

Note: If your mouse is pointed to a port when you click Refresh All, all ports for this card continue to display in the Navigation Tree.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Telnet Console

Use the Telnet Console function to open the Calix TL1 Console window.



Enable Events

Clearing the Enable Events check box disables all database change event handling from the C7. This does not include real-time information such as alarms and events. When the check box is cleared, the system effectively does not automatically update the view of the network if an entity has changed. It is not recommended to leave the Enable Events check box disabled (cleared) for extended periods.

See also

- *Define Network Nodes* (on page 46) for information on adding shelves to a network.
- *Calix C7 Maintenance Guide* for information regarding Extend Provisioning and Bulk Reprovisioner.
- *Calix C7 Broadband Data Services Guide* for information on data provisioning.
- *Calix C7 Video Services Guide* for information on video provisioning.

Using the View Menu

The View menu provides a series of check boxes that enable you to hide and show the screen components.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Select the Navigation Tree check box to display the Navigation Tree panel. Clear the check box to remove the Navigation Tree panel from view.

Select the Details check box to display the Work Area. Clear the Details check box to remove the Work Area from view.

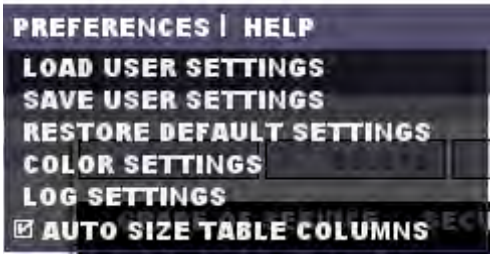
Select the Alarm Table check box to display the Alarm Table area. Clear the Alarm Table check box to remove the Alarm Table area from view.

Select the Ports in Shelf View check box to display a graphical representation of ports in the C7 shelf. Clear the check box to remove the ports from view.

Using the Preferences Menu

Using the Preferences menu you can set various interface settings, save and load user settings, and manage table column sizing.

Note: Preferences that you set only pertain to your workstation and not to the entire system.

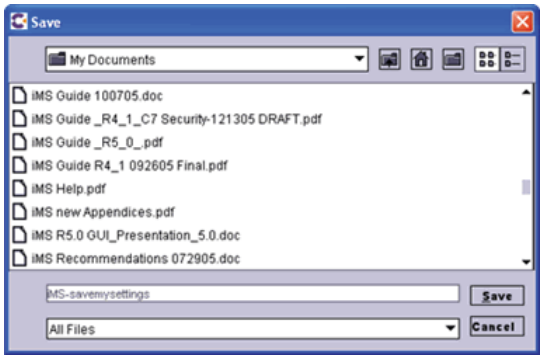


Load User Settings

Use the Load User Settings function to install user settings that you have previously saved using the Save User Settings function.

Save User Settings

Use the Save User Settings function to save your settings in a .txt file to your PC.



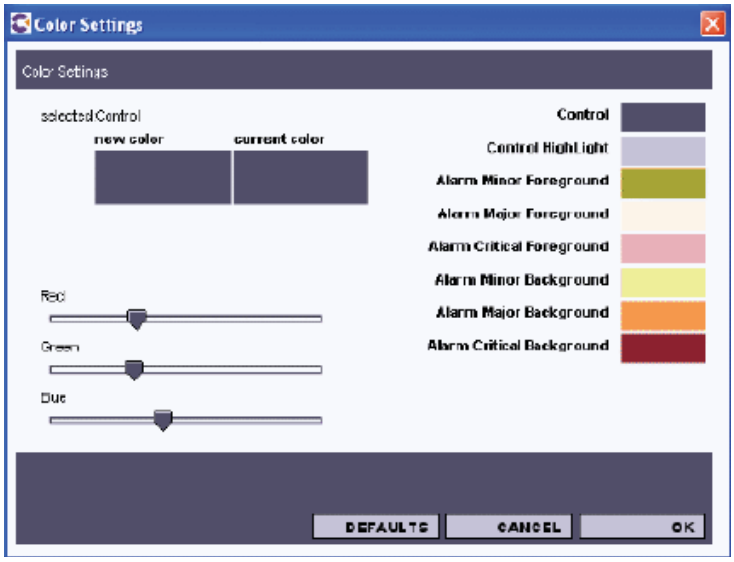
Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Restore Default Settings

Use the Restore Default Settings function to restore the default settings within the iMS application. This only affects how the data is displayed; it does not change any C7 system settings.

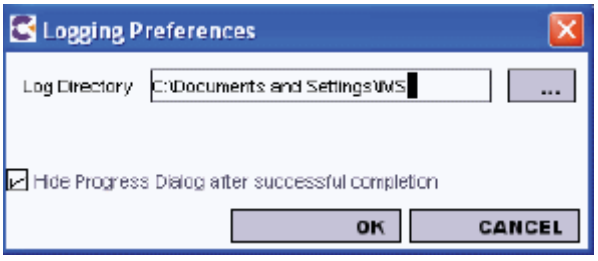
Color Settings

Use the Color Settings function to set the color features for various actions and conditions.



Log Settings

Use the Log Settings function to set the location of the log file (ntuser.dat.LOG).



Auto Size Table Columns

Select or clear the Auto Size Table Columns check box as appropriate.

Toolbar

CREATE | DELETE | ACTION | REVERT | REFRESH | APPLY | SEARCH

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

The C7 iMS and CMS toolbar contains tool buttons for commonly used menu options. The Create, Delete, and Action buttons on the toolbar are context sensitive. Each button displays **highlighted** (available) or dimmed (unavailable) depending on the currently active object in the Work Area. Each of these buttons invokes various tools and menu options or opens particular dialog boxes depending on the currently active object and tab.

You use the Apply button to apply configuration setting changes that are made in the Work Area.

The Search button (only available in CMS) opens a tool for performing a searches or creating inventory reports for various objects, such as regions, networks, and equipment.

Work Area

Tabs are displayed at the top of the iMS Work Area and the Alarm Table. The tabs that display change based on the currently selected object in the Navigation Tree.

Selection Filter

The Selection Filter is used to display specific types of C7 objects in the Work Area. Filtering is effective when you are working with a large number of C7 cards, ports, or cross-connections and need to display a subset in the Work Area. The Selection Filter is explained in more detail later in this section.

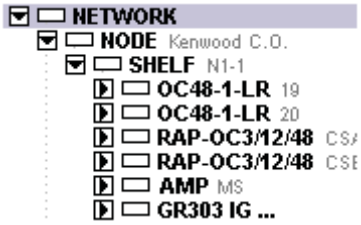
Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Navigating and Selecting Objects

Navigate and Select Objects

The C7 Navigation Tree works just like navigating files on your computer.

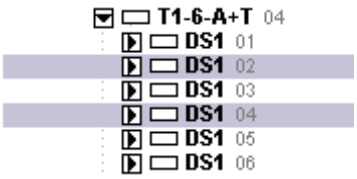
- Click the triangle icon to expand and collapse levels on the tree.
- The status box next to each object name shows the alarm status for that object.
- Click an object name to display that object in the Work Area.



Selecting Multiple Objects on the Navigation Tree

Use the Windows standard Ctrl key + click technique on the Navigation Tree to select multiple objects for display in the Work Area.

Using this method, you can only select objects of the **same type as the first object selected**. For example, if the first object you select is a DS1 port, you can then only select other DS1 ports.

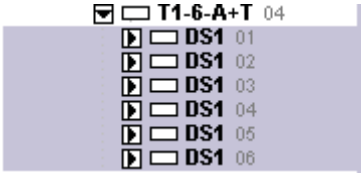


Selecting a Range of Objects on the Navigation Tree

Use the Windows standard Shift + click technique on the Navigation Tree to select a continuous range of objects for display in the Work Area.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

You can select a range across multiple levels of the hierarchy, but your selected range only contains objects of the **same type as the first object clicked**. For example, if the first object you click is a DS1 port, you can then press the Shift key and click a range across multiple cards, but only other DS1 ports are selected.



Navigating in the Work Area

You can double-click some objects in the Work Area to navigate to the next lower level in the network.

- **Network View**

  Double-click a node in the Network View to open the Node View for that node.
- **Node View**

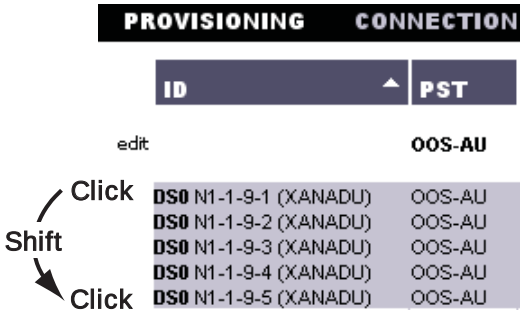
  Double-click a shelf in Node View to open the Shelf View for that shelf.
- **Shelf View**

  Double-click a card in the Shelf View to open the **Provisioning** tab for that card.

Selecting a Range of Objects in the Work Area

Use the Windows standard Shift key + click technique in the Work Area to select a range of objects for editing. Make changes using the Edit Row at the top of the table.

After selecting a range of objects, any changes in the Edit Row are applied to all selected objects.



Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

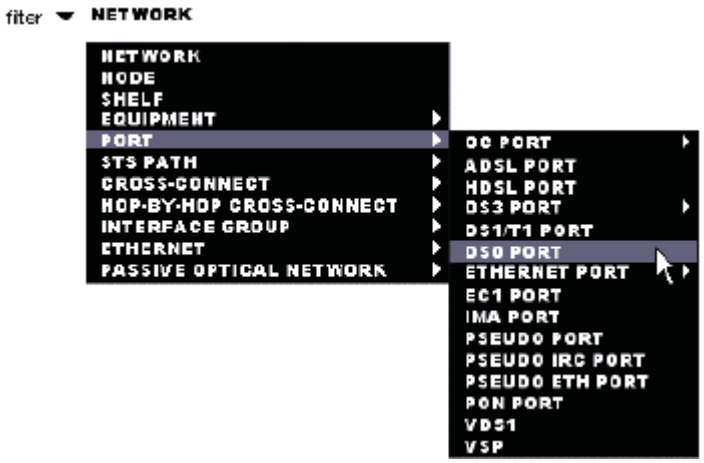
Filtering Objects for Display in the iMS Work Area

Use the Selection Filter to display objects of a specified type in the Work Area. Using the filter, you can select all objects of the specified type below the currently selected level on the Navigation Tree.

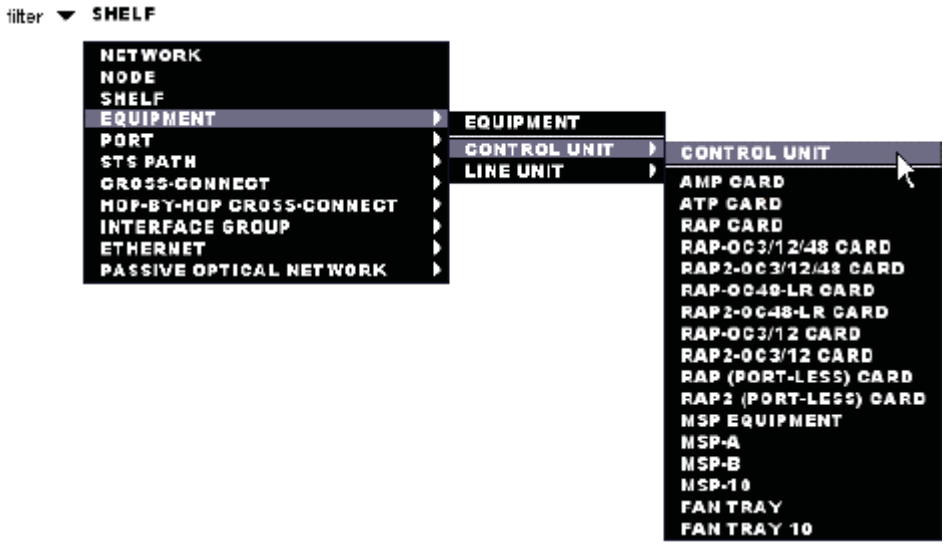
For example, clicking Shelf 1 of Node 1 on the Navigation Tree, and then clicking **Port** > **DS0 Port** in the Selection Filter displays all DS0 ports in Shelf 1 of Node 1 in the Work Area.

If you first click the Network level on the Navigation Tree, and then click **Port** > **DS0 Port**, all DS0 ports in the entire network are displayed in the Work Area.

Filtering is useful when you are working with a large number of C7 cards or ports and need to view a subset of those cards or ports.



With the Selection Filter, you can also quickly select equipment to display in the Work Area.



Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

You can display provisioning information on all equipment, all control units, all line units, or you can limit the display to a particular equipment, control unit, or line unit type.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Useful Techniques

Several productivity enhancing techniques are provided to customize your views in the C7 iMS.

Switch Between Table and Form Views in the iMS Work Area

In form view, right-click the form title, then click **Switch To Table**.

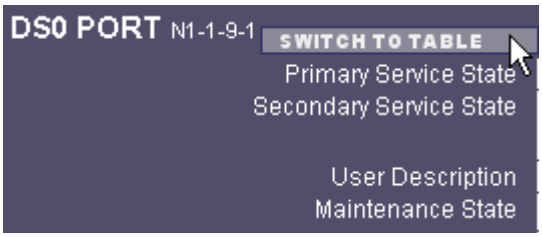
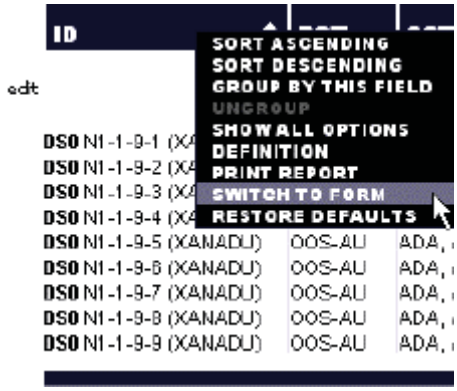
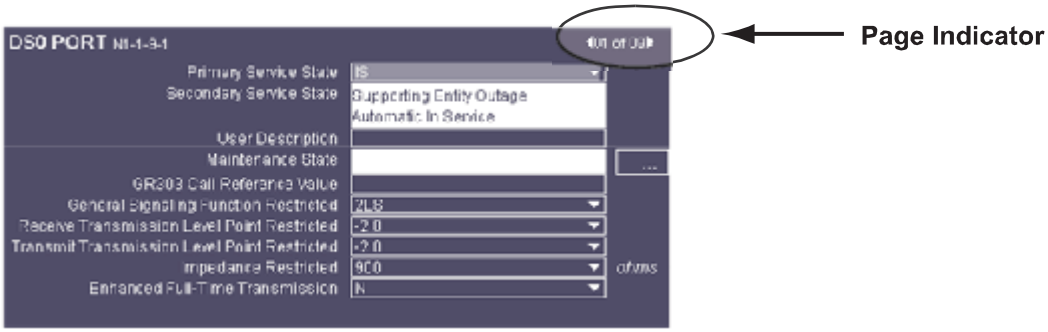


Table view is the default view when you have multiple objects selected. However, you can choose to view each selected object in form view: right-click a column label, then click **Switch to Form**.



After switching to form view, step through the display of each selected object by clicking the page indicator at the upper-right corner of the form.



Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

View Parameter Definitions

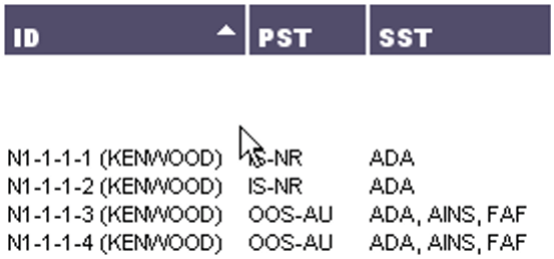
In table view, hold your mouse pointer over any column label to display the full parameter name and a brief definition.

In table view, right-click any column label and then click **Definition** to see a list of definitions for all parameters in the view.

Sort by Column

In table view, click a column label to sort by that parameter, in ascending order.

Click the same label again to switch to descending order.



Move Table Columns

In table view, click a column label and drag it to the left or right to change the column position in the table.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Resize Table Columns

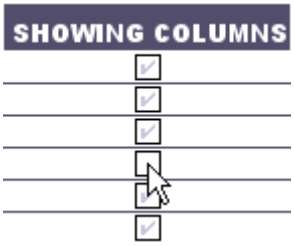
In table view, hold your mouser pointer between two column labels until you see a double-sided arrow, then click and drag to the left or right to expand or shrink the width of a column.

Hiding Table Columns

Complete the steps below to hide table columns.

To hide table columns

1. In table view, right-click any column label, then click **Show All Options** to open the Options (Table Options) dialog box.
2. In the Showing Columns column, click the check boxes to do the following:



   - Clear a check box to hide a column from view.
   - Select a check box to show a column.
3. Click **OK** to apply your changes.

You can also use the Options dialog box to set column sorting, size, order, and grouping.

Generate a Custom Report

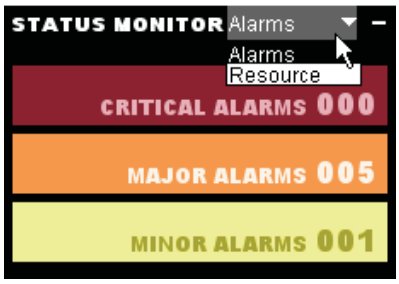
You can generate and print a report of any information in the Work Area that is in table view.

Before generating a print report, be sure you have listed the items that you want.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Status Monitor

You can use the Status monitor to view alarm counts. Selecting **Alarms** from the drop-down menu displays critical, major, and minor alarm counts. In addition, you can use the drop-down menu to select **Resource** to display total memory allocated and in use by the iMS application.



Refresh

During any iMS procedure, you can confirm your work by clicking the **Refresh** button located on the iMS toolbar or the **Refresh** button located in the Alarm Table area. Upon refresh, the displayed values should correspond to the newly entered parameters or most recent action. The refresh action retrieves configuration updates, such as modified parameters and status changes.

Note that C7 iMS does not automatically refresh the display of certain dynamic state changes, such as performance data counters. Clicking the **Refresh** button refreshes the iMS display so that you can view the most recent data.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Chapter 2

Performing Network-Level Tasks

This section covers the steps involved in defining network nodes, configuring a Data Communications Channel (DCC), SONET DCC tunneling, various service and traffic profiles, bandwidth reservation, SNMP settings, and changing the network date and time.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Define Network Nodes

The first step in turning up a new C7 network is to use the *Add Shelves to Network* tool to identify unassigned C7 shelves and group the shelves into nodes.

Information to collect before defining nodes

Before using the *Add Shelves to Network* tool, collect the following information about the network:

- Serial numbers for each C7 shelf in the network (located on the right side of each shelf)
- Serial number of the shelf to serve as the network Administration Master
- Number of shelves (and location of each) per node

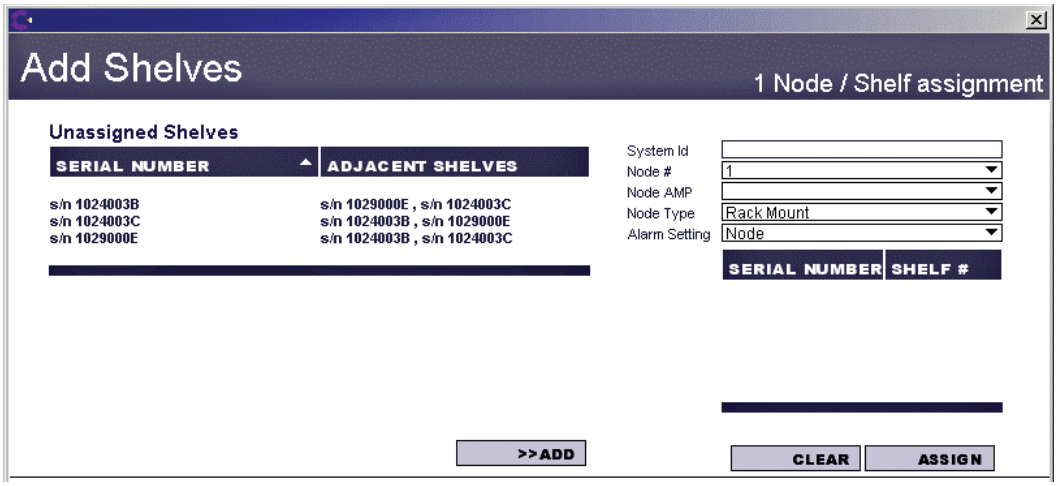
Recommendations

Consider the following when establishing a C7 network:

- Calix recommends (and managing C7 networks in CMS requires) using unique node ID numbers across all of your C7 networks. Using unique node ID numbers simplifies future merging of networks, if required.
- Calix recommends turning up your entire network at once whenever possible. For information about adding nodes to a closed ring or to the middle of a linear chain, see the *Calix C7 Maintenance Guide*.

To define nodes in the network

1. On the Tools menu, click **Add Shelves to Network** to open the Add Shelves dialog box.
2. In the Unassigned Shelves area, click the serial number of a C7 shelf to assign, and then click **Add**. To assign multiple C7 shelves to the same node, press the **Ctrl** key and click the serial numbers of the shelves to group into a node, and then click **Add**.



Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

3. In the node information area (on the right):

   a. In the System ID box, type a node name (up to 20 characters in length).

   Note: To manage a node in CMS, a node name is required. The node name cannot include a colon (:) or a comma (,).

   b. In the Node # list, select an ID number for the node (1 to 255).

   c. In the Node AMP list, select a shelf to host the primary AMP (or ATP) for the node (for alarm reporting purposes).

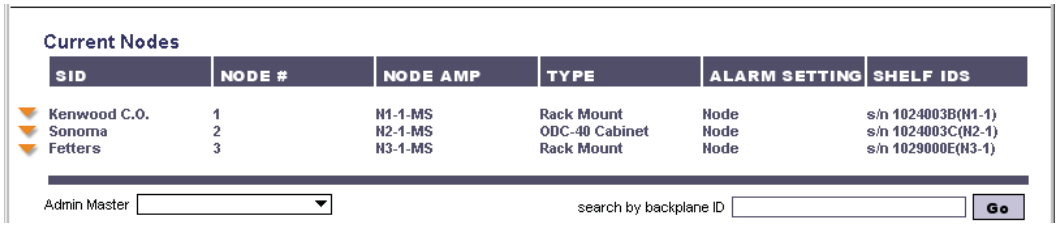
   Note: The node AMP (or ATP) card detects and reports environmental alarms for the node. If you fail to specify a node AMP, the node will not report alarms.

   d. In the Node Type list, select the type of node hosting the C7 shelf (or shelves). For example, click **Rack Mount** for an indoor node or select an ODC cabinet type.

   e. In the Alarm Setting list, click **Node** (to report alarms for this node only) or **Network** (to report all network alarms from this node), as required.

   Note: Calix recommends that no more than two C7 nodes in the network should report network alarms.

4. Click **Assign** to create and display the new node in the Current Nodes area.



5. To create additional nodes, repeat Steps 2 through 4.

ALERT! Potential Service-Affecting Procedure. If the network Admin Master shelf is already assigned, changing the Admin Master node location may cause a service-affecting communication outage on the network. Proceed with caution.

6. In the Current Nodes area, in the Admin Master list, select one shelf to serve as the Administration Master shelf for the C7 network.

   Note: The Admin Master AMP is responsible for downloading the current AMP software into any new AMP that arrives in the C7 network.

7. Click **Next** to save all node definitions and configuration updates.

After the *Add Shelves to Network* tool exits, the assigned C7 nodes display in the Work Area.

Note: In the Alarm Summary area, several timing alarms may display. Ignore these alarms for now—they will clear when you provision shelf timing.

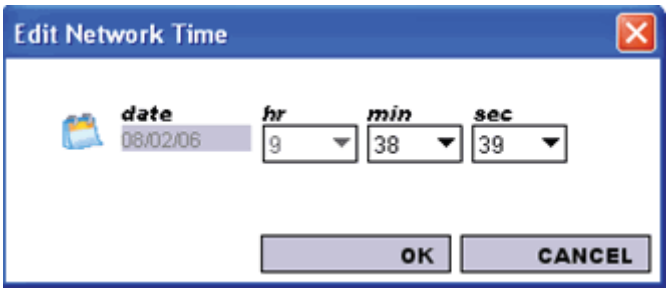
Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Change Network Date and Time

Complete the steps below to adjust the date and time for your network.

To change network date and time

1. In the lower right corner of the main screen, click the current date and time setting to open the Edit Network Time dialog box.



2. To change the date, click the calendar icon and then do the following:
   a. To select a different year, click the **>>** or **<<** button to scroll to the year.
   b. To select a different month, click the **>** or **<** button to scroll to the month.
   c. To select a different day, click a date to select it.
   d. Click **OK** to confirm the change.
3. To change the time, do the following:
   a. In the hours list, select an hour.
   b. In the minutes list, select a minute.
   c. In the seconds list, select a second.
   d. Click **OK** to confirm the change.
   e. To change the time format from military to universal (AM/PM) time, in the lower right corner of the main screen, right-click the time setting and select or clear the check box.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Managing C7 Security

Using CMS, you can manage user access and the connection security mode for multiple C7 networks. For more information, refer to the *Calix Management System (CMS) Guide*.

Managing C7 security using iMS involves ensuring appropriate access to the system for valid users, while inhibiting access by unauthorized personnel. This section introduces and describes:

- Security administration features
- Security implementation procedures
- Remote Authentication Dial In User Service (RADIUS)
- Secure Shell (SSH) protocol
- Secure and insecure modes
- Access Control List (ACL)

For a list of events that can be recorded in the C7 security log see *Appendix B: Security Log Events* (on page 579).

Categories and Access Privileges

When setting up a new user account, a system administrator must first decide what areas of the C7 system the user should have access to, and the level of user access privilege (UAP). Oh The categories below represent five functional areas within the system that a user may have access to, and the tasks associated with each category:

1. **Memory Administration (UapMa):** Provisioning, modifying, deleting, and retrieving resources within the system.
2. **Maintenance (UapMt):** Switching protection, retrieving performance monitoring data, and conducting surveillance of alarms, events and conditions.
3. **Test (UapTs):** Implementing metallic testing within the system.
4. **System Administration (UapSy):** Protecting the system from undesirable or devastating actions.

   A UapSy privilege is required for:

   - All network-wide provisioning (for example, traffic profiles, ONT profiles, ADSL templates)
   - Shelf turn up and provisioning
   - Node provisioning
   - Backup and restore operations
   - Link provisioning
   - Management interface provisioning

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

5. **Security (UapSe):** All Security-related features, including:
    - User provisioning
    - Login session management
    - Password rules
    - Security log retrieval
    - User Access Control List (ACL) provisioning
    - Security (user) templates
    - RADIUS
    - SSH

For each of the categories above, the administrator must also specify the level of user access privilege: None (no access), Minimum (read-only access), or Full (unrestricted access).

Other User Attributes

In addition to assigning access privileges for each of the system categories above, the system administrator sets values for the following user attributes:

- **User ID:** An alphanumeric character string (4 to 10 characters) unique to each user.
- **Security template (Template ID):** A set of pre-defined attributes that a system administrator may apply to specific users. The system contains 5 built-in templates designed for functional roles within the network. A system administrator may create an additional 20 customer-defined templates. Note that you can modify the 5 built-in templates, but you cannot rename them. If you do not specify a security template, the "DEFAULT" template is used.
- **Password:** User account passwords are case-sensitive. The required password length and minimum number of numeric and special characters are determined by the C7 network security settings (set at the network level under **Security** > **Global**). Special characters are as follows: @#$%{}!_?
- **Password aging interval (P-Age):** An integer less than or equal to 999 (days), but typically 45 to 60. At the end of the interval, the system notifies the user each time they log in to change their password.

  Note: If you set this parameter to 0, the user password never expires. This is not recommended.

- **Password change days (P-Change):** The number of days (0 to 999) that a user has between the time they are first notified to change their password and the time their User ID is disabled.
- **Timeout:** The amount of time (in minutes) of inactivity that must pass before the system automatically ends the user session.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- **Node AID (NODEAID):** The node access identifier parameter indicates if the Access IDentifier (AID) code used in TL1 commands or responses should include the node identifier. If set to Y (Yes), the AID responses to this user contain node identifiers. Yes is the default setting. Consider setting the parameter to N (No) for Operations Systems users (such as NMA).
- **Enter ADA (ENTERADA):** This parameter determines whether or not the user can perform a TL1 ENT command on an object that is in an Automatically Default Assigned (ADA) state.

Implement Built-In and Custom Security Templates

C7 security templates ease the task of user provisioning for a system administrator. The system comes with one default template and four pre-defined templates based on the role or job function of the user:

- **Deflt:** Default
- **CoTech:** Central Office Technician
- **OpTech:** Outside Plant Technician
- **SrvOrd:** Service Order Clerk
- **SysAdmin:** System Administrator

In addition, the system administrator can create up to 20 customer-defined templates for the C7.

Built-In Security Template Attributes

The table below lists the attribute values for each of the built-in security templates:

Name	UapMa	UapMt	UapTs	UapSy	UapSe	P-Age	P-Change	Timeout
Default	Min	Min	Min	Min	Min	30	3	10
CoTech	Full	Full	Min	Min	Min	30	3	10
OpTech	Min	Min	Min	Min	Min	30	3	10
SrvOrd	Full	Min	Min	Min	Min	30	3	10
SysAdmin	Full	Full	Full	Full	Full	30	3	10

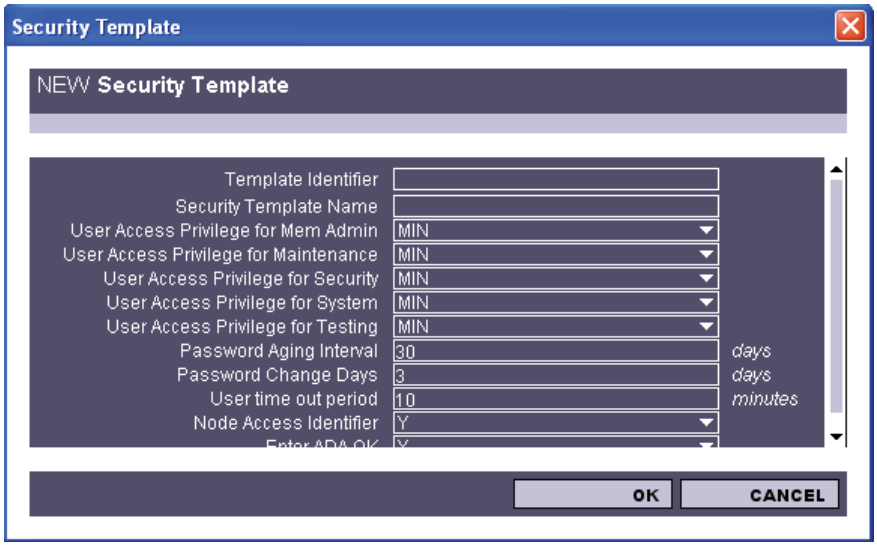
Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Creating a Custom Security Template

Follow the steps below to create a custom security template for your network.

To create a custom security template

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Security** > **Template**.
3. On the toolbar, click **Create**.
4. In the New Security Template dialog box:



a. In the Template Identifier box, enter a number between 1 and 20.
b. In the Security Template Name box, enter a name for the security template.
c. In the User Access Privilege for Mem Admin list, select the access value.
d. In the User Access Privilege for Maintenance list, select the access value.
e. In the User Access Privilege for Security list, select the access value.
f. In the User Access Privilege for System list, select the access value.
g. In the User Access Privilege for Testing list, select the access value.
h. In the Password Aging Interval box, enter the number of days.
i. In the Password Change Days box, enter the number of days.
j. In the User Time Out Period box, enter the number of minutes.
k. In the Node Access Identifier list, click **Y** (Yes) or **N** (No).
l. In the Enter ADA OK list, click **Y** (Yes) or **N** (No).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

5. Click **OK** to create the new security template.

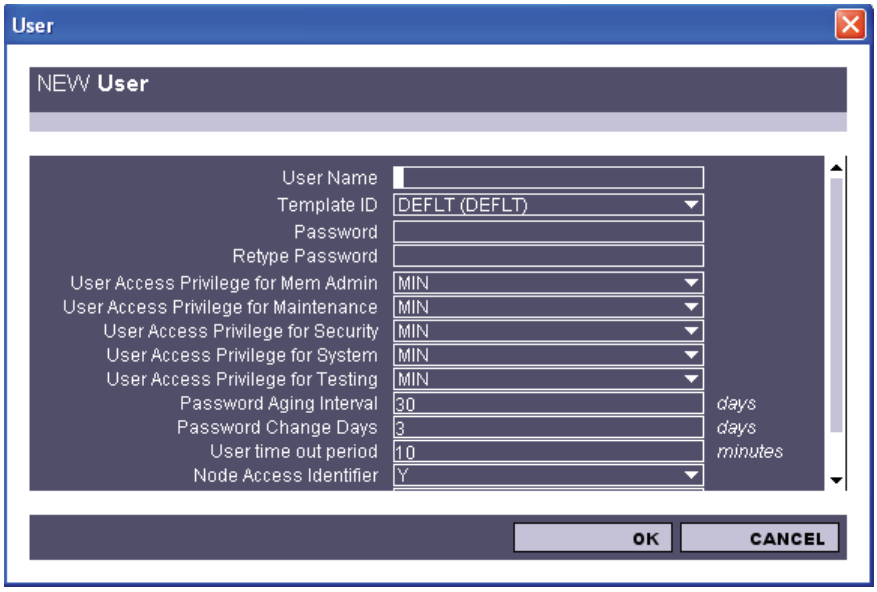
Repeat Steps 3 through 5 to create additional security templates.

Create User Accounts

You can create a maximum of 100 user accounts in a C7 network. Up to 12 user sessions can be simultaneously active. Use this procedure to create a new user account for the C7 network.

To create a new user account

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Security** > **User**.
3. On the toolbar, click **Create** to open the User dialog box.
4. In the User dialog box, do the following:



a. In the User Name box, enter a user name.

b. In the Template ID list, select a security template ID.

c. In the Password box, enter a valid password.

d. In the Retype Password box, retype the password that you entered in the Password box.

Note: The remaining new-user parameters are automatically populated by the selected security template. However, you can individually enter new values.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

5. Click **OK** to create the new user.

Repeat Steps 3 through 5 to create additional new users.

Delete User Accounts

Complete the steps below to remove a user account from the C7 network.

Note: Once a user is deleted, all outstanding login sessions for that user are immediately terminated.

To delete a user account

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Security** > **User**.
3. Click a user ID to select it.
4. On the toolbar, click **Delete**. In the Confirmation dialog box, click **OK** to confirm the account deletion.

Viewing and Editing User Security Information

To view user security details, you must have a Minimum Security privilege level. To edit security settings, you must have a Full Security privilege level.

To view and edit user security details

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Security** > **User**.
3. Click a user row to edit.
4. In the Edit Row, select a new value from the parameter list, or type a new value, as appropriate. Modify other parameters as needed.
5. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your configuration settings.

Secure Shell and SFTP Operations

The system provides a Backup and Restore (BAR) function that allows you to store and retrieve C7 configuration information on a per shelf basis. The BAR operation works in conjunction with an FTP server in insecure mode and works over a secure TCP channel with an SSH File Transfer Protocol (SFTP) server in Secure Shell (SSH) mode.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

If the C7 network is in secure mode, BAR operations always communicate over SFTP. Conversely, if the C7 network is in non-secure mode, BAR operations always communicate over FTP.

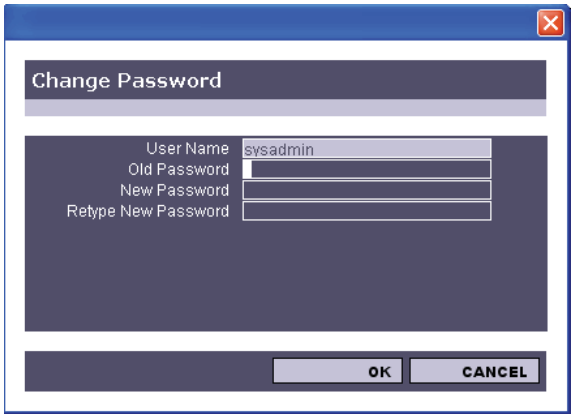
If using a Sun Solaris SFTP server, you must use the OpenSSH SFTP Version 3 (v3) protocol for secure BAR operations.

See the *C7 Maintenance Guide* for detailed instructions on performing BAR operations.

Changing the Password

To change the password for your user profile

1. On the Navigation Tree, click the Network level.
2. In the Work area, click **Security** > **User**.
3. On the toolbar, click **Action** > **Change Password** > **Own** to open the Change Password dialog box.



4. In the Change Password dialog box, update your password:
   a. In the Old Password box, type your old password.
   b. In the New Password box, type your new password.
   c. In the Retype New Password box, re-type your new password.

Note: User account passwords are case-sensitive. The required password length and minimum number of numeric and special characters are determined by the C7 network security settings (set at the network level under **Security** > **Global**). Special characters are as follows: @#$%{}!_?

5. Click **OK** to save your changes.

The system allows system administrators to modify the passwords of other users. To do so, at Step 3, click **Action** > **Change Password** > **Others**. In the Change Password dialog box, in the User Name box, type the user ID to modify. Then follow Steps 4 and 5 to change the password.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Allowing Messages

To allow messages, you must have a Full Security privilege level.

To allow messages

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Security** > **User**.
3. Click the appropriate user row.
4. On the toolbar, click **Action** > **Allow** > **Messages**. In the Confirmation dialog box, click **OK**.

Inhibiting Messages

To inhibit messages, you must have a Full Security privilege level.

To inhibit messages

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Security** > **User**.
3. Click the appropriate user row.
4. On the toolbar, click **Action** > **Inhibit** > **Messages**. In the Confirmation dialog box, click **OK**.

Inhibiting a User

Security administrators with Full Security privileges can disable (inhibit) a user. Once a user is inhibited, all outstanding login sessions for that user are immediately terminated.

Follow the steps below to inhibit a user session.

To inhibit a user

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Security** > **User**.
3. Click the appropriate user row.
4. On the toolbar, click **Action** > **Inhibit** > **User**. In the Confirmation dialog box, click **OK**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Allowing a User

Security administrators with Full Security privileges can re-instate (allow) a user.

Follow the steps below to allow a user to re-establish a session.

To allow a user

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Security** > **User**.
3. Click the appropriate user row.
4. On the toolbar, click **Action** > **Allow** > **User**. In the Confirmation dialog box, click **OK**.

Viewing User Session Information

In addition to the security parameters described above, the Session Work Area provides this security information:

- **MSCHANNELID:** The serial or Ethernet port address of the AMP or the ATP card.
- **LOGIN TIME:** Date and time that the user logged in to the system.
- **LAST ACTIVITY:** Date and time of the last activity logged by the system for this user.
- **INHMSG:** Indicates whether the user has been inhibited from receiving alarms, network events or other non-alarmed conditions.
- **SECUMSG:** Indicates whether security messages are being received for this user session.
- **RESTR:** Indicates whether the user has access to restricted commands and parameters.
- **IDLE:** Shows how many minutes the user has been idle.

Viewing sessions of other users requires Full Security privileges.

Up to 12 user sessions can be simultaneously active.

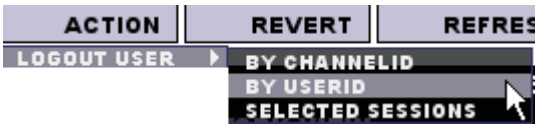
To view user session information

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Security** > **Session**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Logging Out a User

The system provides three options for a security administrator with Full security privileges to log out a user from a specific C7 shelf:



- **By Channel ID:** Identifies the user session based on the serial or Ethernet port address of the AMP or ATP card.
- **By User ID:** Identifies the user based on the user login name.
- **Selected Sessions:** Logs out one or more users from selected sessions (see Step 3 below).

To log out a user

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Security** > **Session**.

   (To ensure that all active user sessions are displayed, click **Refresh**.)
3. Click the appropriate user row. To apply the action to multiple users, use Ctrl+click to select each user to log out.
4. On the toolbar, click **Action** > **Logout User**, and then select the appropriate log-out option.
5. In the Confirmation dialog box, click **OK**.
6. In the message dialog box, click **OK**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

View and Edit Global Security

Follow the steps below to view and edit the global security settings.

Default security settings

The following table lists the default security settings which affect all C7 users.

Parameter	Description
Password Length	Minimum number of characters required for user passwords. Valid options are from 4 to 10 characters. The default is 6.
Minimum Special Characters	Minimum number of special characters required for user passwords. Valid options are from 0 to 10. The default is 0 (zero). **Note:** Special characters that can be used when changing passwords are the "at" symbol [@], number symbol [#], dollar sign [$], percent symbol [%], open curly bracket [{], closed curly bracket [}], exclamation mark [!], underscore [_], and question mark [?].
Minimum Numeric Characters	Minimum number of numeric characters (0 to 9) required for user passwords. Valid options are from 0 to 10. The default is 2.
Maximum Invalid Attempts	The number of times that a C7 user can attempt to log in to C7 if they supply an invalid password. Valid options are integers from 2 to 10. The default setting is 3. The Telnet session is dropped when this number of successive login failures has been reached. The valid range is 2 to 10. The default value is 3.
Sub String	Determines whether the password can contain the user name as a substring. Valid options are Y (Yes) and N (No). The default is N (No).
Login Banner	String of up to 79 characters displayed after each login. The default value is: *** WELCOME TO THE CALIX C7. AUTHORIZED ACCESS ONLY. ***
User Authorization Mode	The method used for user authorization. Valid options are Local and RADIUS. The default setting is Local. • **Local:** Local authorization mode. • **RADIUS:** If set to the Remote Authentication Dial In User Service (RADIUS) authentication mode, the C7 acts as a RADIUS client with the

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Parameter	Description
	remote RADIUS protocol performing user login request authorization. For additional information, see *Remote Authentication via RADIUS* (on page 60). **Note:** For the C7 to act as a RADIUS client, the C7 AMP Ethernet port "Channel Access Privilege" (CHAP) must be configured to allow access.
Only connect via Secure Shell (SSH)	When enabled (Y), activate Secure Shell for all login channels. For additional information, see *SSH Security Overview* (on page 64).
Routing Enabled	If enabled (Y), static routes provisioned on an AMP are used to route incoming packets from one management interface to another. If disabled (N), the AMP only functions as an IP host.

To view and edit global security settings

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Security** > **Global**.
3. Modify the global security parameters as needed. Refer to the preceding table for explanations of each field.
4. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your changes.

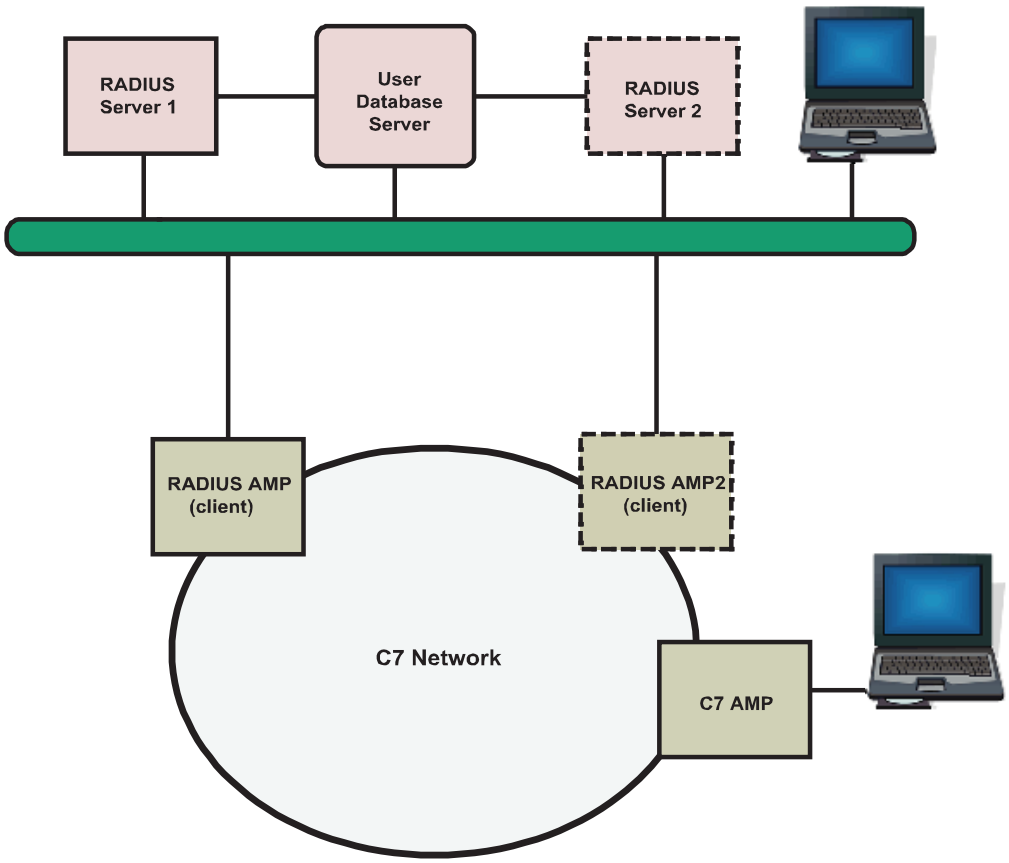
Remote Authentication via RADIUS

You can configure the C7 to perform login authentication via the Remote Authentication Dial In User Service (RADIUS) protocol. For redundancy, the C7 is provisioned with a primary and secondary location of the RADIUS server in the event that one of them is unavailable. All transmissions between the C7 and the RADIUS server are encrypted and authenticated using a "shared secret" known to both the C7 client and the RADIUS server. If no response is received from the primary RADIUS server within a specified number of retries, the request is automatically resubmitted using a secondary server address if one is available.

One C7 AMP is designated as the primary RADIUS client. A second can be configured as a secondary client and used only if the primary AMP is not functioning. The RADIUS client(s) must have IP connectivity to the RADIUS server(s). The RADIUS system administrator enters users into the RADIUS user database outside of the C7 applications. After a successful login, users are granted their appropriate C7 permissions by the RADIUS server.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

The diagram below illustrates the connectivity of the RADIUS servers, the user database server, and the C7 network.



RADIUS Parameters

Use the following parameters to configure the external RADIUS server for C7 networks:

Parameter	Description	Valid Options
IP Interface Address 1	The IP address of the primary RADIUS server.	IPv4 format, Class A, B, or C Default: 0.0.0.0
IP Port 1	The port used for sending UDP packets to the primary RADIUS server.	Default: 1812
IP Interface Address 2	The IP address of the secondary RADIUS server.	IPv4 format, Class A, B, or C Default: 0.0.0.0
IP Port 2	The port used for sending UDP packets to the secondary RADIUS server.	Default: 1812
Timeout	Number of seconds to wait for a response from the RADIUS server before retransmitting or aborting.	Integer from 5 to 60 Default: 8

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

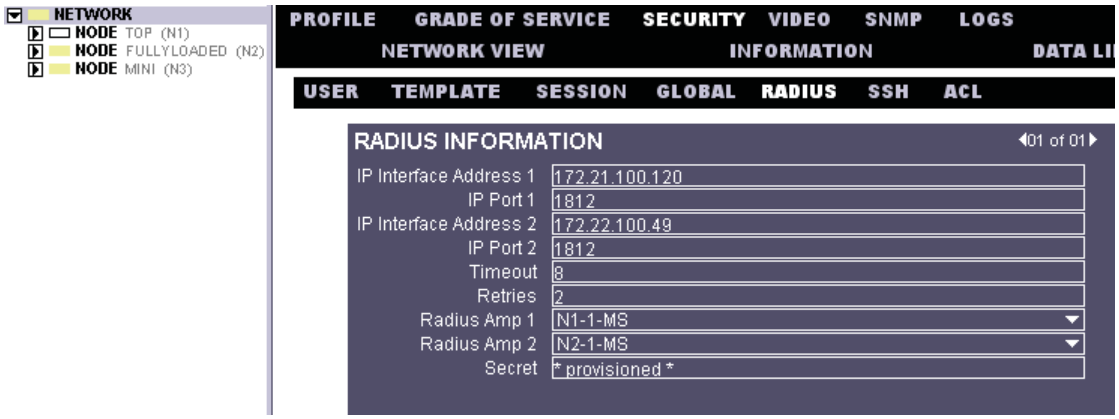
Parameter	Description	Valid Options
Retries	The number of times the client tries to access the primary RADIUS server before it resubmits the request to the secondary RADIUS server or aborts.	Integer from 0 to 5 Default: 3
RADIUS AMP 1	Primary AMP to use as a RADIUS client. If used, the primary AMP card must have IP connectivity to the RADIUS server	Default: NONE
RADIUS AMP 2	Secondary (alternate) AMP to use as a RADIUS client. If used, the secondary AMP card must have IP connectivity to the RADIUS server.	Default: NONE
Secret	The "shared secret" known to both the RADIUS client (the C7) and the RADIUS server. To maintain the integrity of the secret, "*** provisioned ***" is displayed in the text box after you have typed the value. The shared secret cannot be retrieved for display, even by the system administrator.	This string must match the string configured in the RADIUS server.

Viewing and Editing RADIUS Information

Follow the steps below to view and edit RADIUS information.

To view and edit RADIUS information

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Security** > **Radius**.



3. Enter the appropriate server and client information.
4. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your changes.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Sample RADIUS Vendor Specific Attribute Dictionary

The following is a sample Vendor Specific Attribute (VSA) dictionary used when configuring the RADIUS server.

Note: Calix has a unique vendor ID of **6321**.

```
#
#VENDOR vendor_name vendor_id
#
#ATTRIBUTE attrib_name attrib_id syntax_type vendor_name
#VALUE attrib_name value_name int_value
#

VENDOR Calix 6321
#
# calix dictionary
#

# Attribute for User access privilege - memory administration
ATTRIBUTE    Calix-C7-Uap-MA     201    integer   Calix
VALUE Calix-C7-Uap-MA    No_Access            0
VALUE Calix-C7-Uap-MA    Read_Only_Access     1
VALUE Calix-C7-Uap-MA    Full_Access          2

# Attribute for User access privilege - maintenance
ATTRIBUTE    Calix-C7-Uap-MT     202    integer   Calix
VALUE Calix-C7-Uap-MT    No_Access            0
VALUE Calix-C7-Uap-MT    Read_Only_Access     1
VALUE Calix-C7-Uap-MT    Full_Access          2

# Attribute for User access privilege - security
ATTRIBUTE     Calix-C7-Uap-SE     203    integer   Calix
VALUE Calix-C7-Uap-SE    No_Access            0
VALUE Calix-C7-Uap-SE    Read_Only_Access     1
VALUE Calix-C7-Uap-SE    Full_Access          2

# Attribute for User access privilege - test
ATTRIBUTE     Calix-C7-Uap-TE     204    integer   Calix
VALUE Calix-C7-Uap-TE    No_Access            0
VALUE Calix-C7-Uap-TE    Read_Only_Access     1
VALUE Calix-C7-Uap-TE    Full_Access          2

# Attribute for User access privilege - system
ATTRIBUTE     Calix-C7-Uap-SY     205    integer   Calix
VALUE Calix-C7-Uap-SY    No_Access            0
VALUE Calix-C7-Uap-SY    Read_Only_Access     1
VALUE Calix-C7-Uap-SY    Full_Access          2

# user session idle timeout in minutes
ATTRIBUTE  Idle-Timeout  28  integer

# “reply message” is interpreted as the desired login banner.
# Multiple Reply_Message attributes may be used, in which case
# they are concatenated/displayed on separate lines.
ATTRIBUTE  Reply-Message  18  string
```

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

SSH Security Overview

The C7 provides enhanced security features to protect the system. Using the Secure Shell (SSH) protocol, the C7 provides several secure tunneling capabilities; secure file transfer, and authentication to ensure session confidentiality and integrity. Both ends of the SSH client/server connection are authenticated using a digital certificate, and passwords are protected by encryption.

A C7 system operating in secure mode provides:

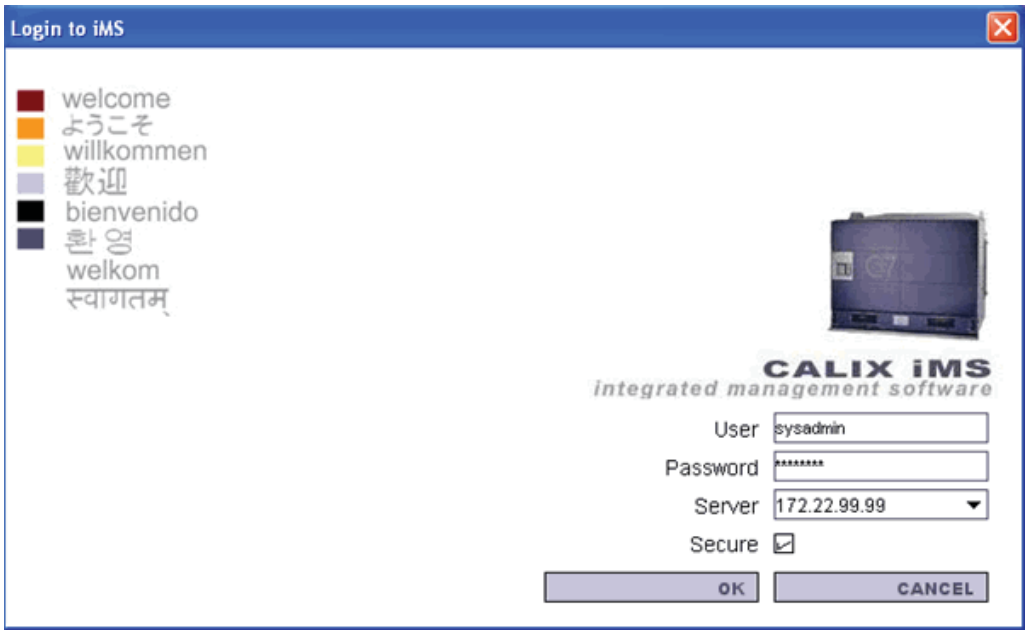
- Support for SSH Server 2.0.
- Port forwarding for Telnet, iMS, and TCP connections.
- Support for SSH File Transfer Protocol (SFTP) Server.
- Secure backup and restore (BAR) functions.

All TCP access to management interfaces are restricted to SSH.

Serial port access is restricted to the serial port on the AMP or ATP assigned as the Admin Master.

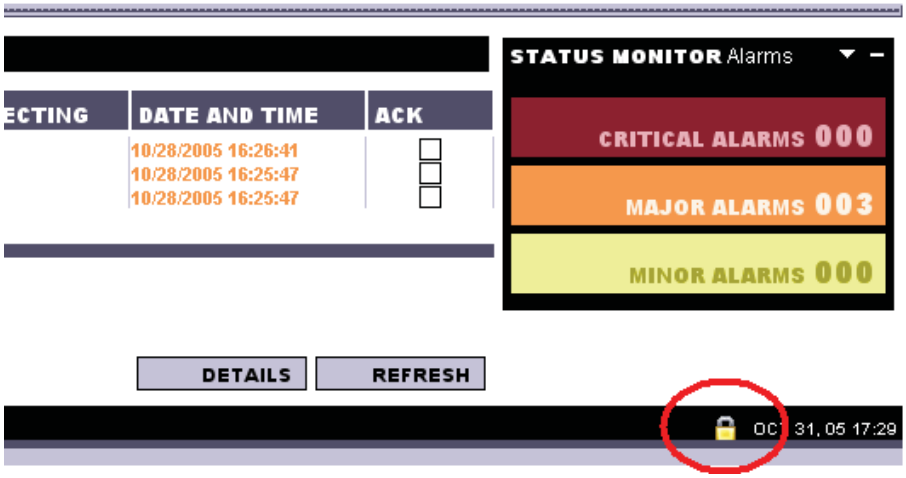
Establishing a Secure Connection

When you log in to the system, select the Secure check box to establish a secure connection to the C7 network. Clear the **Secure** check box to establish a non-secure connection to the C7 network. The default is non-secure mode (cleared).



Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

The lock icon indicates whether or not the network is in non-secure mode (open lock) or secure mode (closed lock), as shown in the following figure.



SSH Cipher and Hash Settings

The C7 with SSH employs cipher and hash functions to ensure data integrity and security. A cipher is an algorithm for performing encryption. A hash function takes a variable-length input sequence of bytes and computes a fixed-length sequence. The fixed length is considerably shorter than the typical length of the input.

SSH HASH

- **SHA1:** Secure Hashing Algorithm 1 (SHA1) is a one-way hash function producing a 160-bit hash value.
- **SHA1-96:** This is the truncated 96-bit cryptographic hash value of the 160-bit SHA1 computation.
- **MD5:** Message Digests (MD) are one-way hash functions. The MD5 algorithm produces a 128-bit hash value.
- **MD5-96:** MD5-96 operates on 64-byte blocks of data. Padding requirements are specified in RFC-1321 and are part of the MD5 algorithm.

SSH Cipher

- **AES:** Advanced Encryption Standard (AES) has a fixed block size of 128 bits and a key size of 128, 192 or 256 bits. AES is designed to be more secure than DES.
- **3DES:** Encrypts plain text with one key, decrypts the resulting ciphertext with a second key (which, because the key is different, does not actually decrypt the data but re-encrypts it in a different way), and then encrypts the result of the second operation with the first key again.
- **Blowfish:** The BlowFish encryption algorithm allows data to be encrypted and decrypted using the same key. This allows data to be stored or securely transmitted. The BlowFish algorithm can generate several different values when it encrypts the same data.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

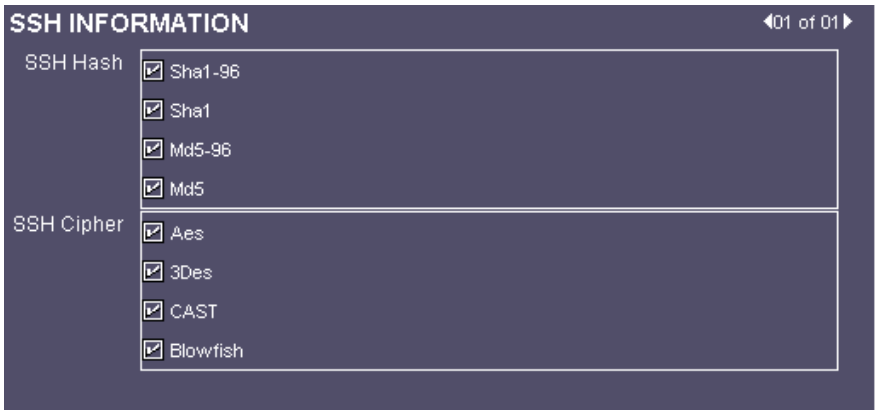
- **CAST:** CAST is an algorithm with a design similar to Blowfish, with key-dependent S-Boxes, a non-invertible F function, and a Feistel network-like structure (called a substitution-permutation network).

Viewing and Editing SSH Information

Follow the steps below to view and edit SSH information.

To view and edit SSH information

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Security** > **SSH**.
3. Select or clear the SSH hash and cipher check boxes as appropriate.



4. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your changes.

SSH Security Setup

The SSH service is activated at the network level and is set as a network-wide attribute.

C7 SSH security guidelines

- The SSH server allows a maximum of 20 connections.
- If the C7 network is in secure mode, the C7 blocks all serial connections except for the serial port (S1) on the Admin Master AMP or ATP card. In addition, the timeout value of any user logged in through S1 on the Admin Master is capped to 5 minutes when security is enabled. For inactivity exceeding 5 minutes, the system automatically logs the user out regardless of the provisioned timeout value.
- If the C7 network is in secure mode, Telnet cannot be used for a TL1 session over TCP. Only SSH connections initiated from an SSH client are allowed. Such an application can be downloaded from the C7 AMP web server (TL1 console).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- If the C7 network is in non-secure mode, you can still connect securely with SSH. Upon switching to secure mode the C7 drops all insecure sessions. Subsequent TCP connections are only allowed through a secure SSH connection.

Serial Port Access

When C7 security is enabled and the SSH service is activated, all sessions through serial ports are disabled except for the AMP or ATP administrative master serial port. Additionally, only the System Administrator can access the system through the AMP or ATP administrative master serial port.

Access Control List

The C7 network supports an access control list (ACL) to provide an additional layer of system security. The ACL is used to control and filter communication traffic between the C7 network and external interfaces. You can configure up to 20 IP addresses or subnets that the C7 uses for access control. When you define entries in the ACL, the C7 disregards any IP-based communication originating from IP addresses not listed in the ACL. If there are no ACL entries, all source addresses are accepted.

The ACL does not limit access from the local host. You can always access services directly by starting the management software or TL1 from a direct connection to the C7 AMP or ATP administrative master serial port (in secure or non-secure mode).

The FTP server IP address used for Backup and Restore (BAR) operations must be entered into the ACL if the ACL is in effect (that is, one or more ACL entries are already configured). If for any reason the FTP server IP address is denied, the FTP-initiated connection and BAR operation fails. Conversely, if the ACL in not in effect (there are no entries in the ACL), you do not need to add the FTP server IP address to the ACL.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring the ACL

Configuring the access control list requires Full Security privileges.

ALERT! When you define entries in the ACL, the C7 disregards any IP-based communication originating from IP addresses not listed in the ACL. If you inadvertently create an ACL, you must log in to the C7 via the serial port of the Admin Master and delete the ACL in order to allow acceptance of other source addresses.

To configure the access control list

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Security** > **ACL**.
3. On the toolbar, click **Create** to open the Create ACL dialog box.

4. Enter the IP address in the IP address box.
5. Enter the IP mask in the IP mask box.
6. Click **OK**.

Deleting Entries in the ACL

You cannot modify entries in the ACL. You must delete existing entries and configure new ones. Deleting entries in the access control list requires Full Security privileges.

To delete entries in the access control list

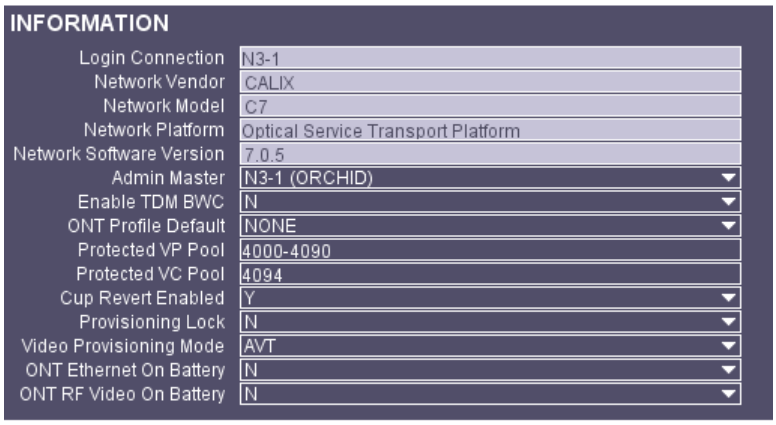
1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Security** > **ACL**.
3. Select one or more ACL entries to delete.
4. On the toolbar, click **Delete**. In the Confirmation dialog box, click **OK**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

View General Network Information

To view network information

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Information** to view general information about your system.



How to override a provisioning lockout

The C7 invokes a provisioning lockout on its user interfaces during certain sensitive operations to prevent user-invoked changes from adversely affecting the system database. The C7 locks out provisioning during shelf database backups and during the equipment reset phase of an upgrade. The provisioning lockout automatically lifts when the operation completes.

If a session disconnect occurs during the lockout period (for example, if the interface window is accidentally closed, or a network interruption prevents the CUP from completing), the provisioning lockout will not be lifted, and a "Requested Command(s) Inhibited" message will display upon all subsequent provisioning attempts. If a sustained provisioning lockout occurs due to a disconnection, you can override the lockout as described below.

To manually override a provisioning lockout

From the CMS or iMS interface:

1. On the Navigation Tree, click the **Network** level.
2. In the Work Area, click **Information**.
3. On the Information panel, set the Provisioning Lock parameter to **N** (No) and click **Apply**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

View and Modify SNMP Settings

The Simple Network Management Protocol (SNMP) agent is located on the AMP/ATP card. It performs alarm and performance data collection for the C7 network. You can view and modify the SNMP general, trap, and Access Control List (ACL) settings.

General SNMP settings

- **Community string:** Identifies the security password that the SNMP manager uses when performing SNMP Get operations. (SNMP Set operations are not supported in this release of the C7.) The community string is case sensitive. The default value is **public**.
- **Trap port:** Identifies the management port for sending out SNMP traps. For the C7, the trap port is the access identifier (AID) of an Ethernet port on an AMP card. The format is N[node number]-[shelf number]-MS-[port number], where node number is 1-255, shelf number is 1-5, and port number is E1, E2, or E3, for example: **`N1-2-MS-E2`**.

Trap settings

You can specify up to four unique SNMP trap destinations using the following settings:

- **UDP port:** Identifies the port where the trap is to be sent. Port values can be in the range 1 through 65535.
- **Trap community string:** Identifies the security password to use when sending traps. The trap community string is case sensitive.
- **Version:** Identifies the SNMP protocol version to use when sending traps. The C7 supports SNMP versions V1, V2c, and V3.
- **IP address:** Identifies the IP address where traps are sent. Use an IP address with all zeros (0.0.0.0) to disable a specific trap.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

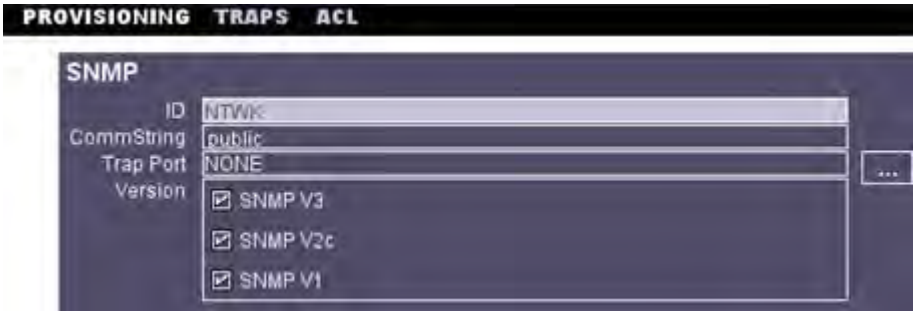
Access control list (ACL) settings

The access control list consists of up to 10 IP addresses for each C7 network. If you do not specify any IP addresses in the access control list, all source addresses are accepted.

- **IP address:** Identifies the IP address of the SNMP manager that is allowed to make requests to the C7 network.
- **Mask:** Identifies the mask to apply to the corresponding IP address.

To modify SNMP settings

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **SNMP** to open the SNMP panel, and then do one of the following:
   - To modify general SNMP settings (community string and trap port), go to Step 3.
   - To modify the settings for any of the four traps, go to Step 4.
   - To modify the access control list, go to Step 5.
3. To modify the general SNMP settings, do the following:



   a. In the Work Area, click **Provisioning**.

   b. In the CommString (Community String) box, type the case-sensitive community string.

   c. Click the ellipsis button to the right of the Trap Port box to open the Select Trap Port dialog box. Select the Shelf and Port to specify the trap port, and then click **OK**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

4. To modify individual SNMP trap settings, do the following:

   a. In the Work Area, click **Traps**.

   b. In the UDP Port box, type the number of the port, or accept the default of 162.

   c. In the CommString (Community String) box, type the case-sensitive community string for the trap.

   d. In the Version list, click **V1, V2C, or V3** to specify the SNMP version.

   e. In the IP box, type the IP address.

   f. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save the changes.

5. To modify the access control list, in the Work Area, click **ACL**, and then add or delete an entry:

   a. To add an entry to the list, do the following:

      - On the toolbar, click **Create**.
      - In the Create ACL dialog box, type the IP address and mask to use, and then click **OK**.
      - In the Confirmation dialog box, click **OK**.

   b. To delete an entry from the list, do the following:

      - Click the row to delete.
      - On the toolbar, click **Delete**.
      - In the Confirmation dialog box, click **OK**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configure Grades of Service

Overview of Grade of Service Profiles

A grade of service (GoS) profile consists of a set of parameters that specify thresholds for performance monitoring. When you create a port or a path, you can specify that the system monitor performance based on a set of defaults, or a set of user-defined grade of service profiles.

Note: In the Create Grade of Service Profile dialog box, hold your mouse pointer over any parameter box to display the valid range of a parameter.

Location

Specifies the location (near end or far end) where the performance data is monitored.

Time period

Specifies the time period (either a 15-Minute or Daily Interval) that performance monitoring data is collected.

Grade of Service profile identifier (ID)

A number that uniquely identifies a set of defined performance parameters that monitor the grade of service thresholds. You can create up to 20 sets of GOS thresholds for each facility. Enter a number from 1 through 20 to customize a set of GOS thresholds for your network.

Description (DESC)

A user-defined character string of up to 11 characters. This parameter helps track the link, port, profile, or cross-connect.

Selected GoS profile parameters are listed below, in alphabetical order.

Coding violations – line (CV-L)

Specifies the threshold for bit interleaved parity (BIP) errors that are detected at the line layer at the near end or far end node. Each error increments the register.

Enter an integer between 1 and 1,048,575.

Coding violations – path (CV-P)

Specifies the threshold for bit interleaved parity (BIP) errors that are detected at the path layer. Each error increments the register on the near-end or far-end node.

Enter an integer between 1 and 1,048,575.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Errored Seconds – Line (ES-L)

Specifies the threshold (in seconds) during which—at any point during the second—at least one of the following errors was detected or present at the line layer at the near end or far end node:

- Section layer Bit Interleaved Parity (BIP) error
- Severely Errored Frame defect
- Loss of Signal

Enter an integer between 1 and 65,535.

Errored seconds – path (ES-P)

Specifies the threshold (in seconds) during which—at any point during the second—at least one of the following errors was detected or present at the path layer on the near-end or far-end node:

- Section layer Bit Interleaved Parity (BIP) error
- Severely Errored Frame defect
- Loss of Signal

Enter an integer between 1 and 65,535.

Loss of signal count (LOSC) (ADSL, near end only)

Specifies the number of times an LOS condition was set.

LOSC also represents the number of modem retrains in the time period. The 15-minute default threshold is 3. The 1-day default threshold is 10.

Severely errored framing/alarm indication signal seconds (SAS-P)

Specifies the threshold for the number of 1-second intervals containing one or more severely errored framing (SEF) defects or one or more alarm indication signal (AIS) defects.

Severely errored seconds – line (SES-L)

Specifies the threshold (in seconds) during which one of the following errors was detected or present at the line layer on either the near end or far end node:

- Section layer Bit Interleaved Parity (BIP) error
- Severely Errored Frame defect
- Loss of Signal

Enter an integer between 1 and 65,535.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Severely errored seconds – path (SES-P)

Specifies the threshold (in seconds) during which one of the following errors was detected or present at the path layer on the near end or far end node:

- Section layer Bit Interleaved Parity (BIP) error
- Severely Errored Frame defect
- Loss of Signal

Enter an integer between 1 and 65,535.

Percent utilization, ingress (PERU, near end only)

Specifies the ingress threshold percentage of utilization for the path.

Percent utilization – path, egress (PERUE, near end only)

Specifies the egress threshold percentage of utilization for the path.

Unavailable Seconds Threshold – Path (UAS-P)

Specifies the threshold (in seconds) during which the path is unavailable.

Enter an integer between 1 and 65,535.

Create a Grade of Service Profile

To create a grade of service profile

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Grade Of Service**, and then click a facility tab.
3. On the toolbar, click **Create** to open the Create Grade of Service dialog box.
4. In the Create Grade of Service dialog box, do the following:
   a. In the Grade of Service Profile ID box, type a number (1 through 20) to identify the new profile.
   b. In the Description box, type a name to describe the profile. (Maximum 11 characters.)
   c. Click **Next**.

Note: In the Create Grade of Service Profile dialog box, hold your mouse pointer over any parameter input box to display the valid range of a parameter.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

5. Enter values for 15-Minute Near End Registers. Click **Next**.
6. Enter values for 1-Day Near End Registers. Click **Next**.
7. Enter values for 15-Minute Far End Registers. Click **Next**.
8. Enter values for 1-Day Far End Registers. Click **OK**.

To view or modify a grade of service profile

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Grade Of Service**, and then click a facility tab.
3. At the bottom of the work area, select the parameters to display. Click a radio button to the right of Location to toggle between near end and far end parameters, or a radio button to the right of Interval to toggle between 15-minute and 1-Day (daily) parameters.
4. To modify a Grade of Service:

   Note: You cannot edit the Default Grade of Service.

   a. Select the Grade of Service in the list.

   b. In the Edit row, double-click an existing parameter value and type a new value. Repeat this step for each parameter you are modifying.

   c. After the last value you are modifying has been changed, press the Tab or Enter key.

   Note: Step 4c is required, otherwise the last value you modified will not be included when you apply the changes.

   An orange arrow displays to the left of the Grade of Service indicating that a change in pending.

   d. Click **Apply**, and then **OK** to save the changes.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configure Network Profiles and Templates

This section introduces and describes:

- Managing global C7 profiles in Calix Management System (CMS)
- C7 Traffic profiles
- C7 xDSL port templates

Managing Global C7 Profiles in CMS

Global profiles automate synchronizing profiles and templates across multiple C7 networks. They support cross-network capabilities such as bulk provisioning across networks and inter-network A-to-Z provisioning. You create a profile once within CMS and apply it across all targeted C7 networks to ensure consistency across large deployments.

When you create a global profile, the profile is automatically downloaded to the networks in the CMS management domain that enable global profile updates. CMS supports the following C7 profiles:

- **Traffic Profiles –** Define the bandwidth characteristics of a subscriber data connection across the network. For descriptions of profile parameters, see *Overview of Traffic Profiles* (on page 90).
- **xDSL Templates –** Define the bandwidth characteristics of the modem connection with the ADSL or xDSL line card port. For descriptions of template parameters, see *Overview of ADSL Template Parameters* (on page 95)
- **Ethernet Bandwidth Profiles –** On a Local Bridge, define the bandwidth attributes of subscriber-facing VLAN Interfaces (VLAN-IFs).
- **Ethernet Profiles –** For Ethernet-over-SONET provisioning, define the maximum bandwidth rate allowed on a VLAN.
- **EXA Video MVR Profiles –** Configure a list of multicast VLANs on which EXA Powered video subscribers can receive video streams.
- **EXA Video Multicast Profiles –** Specify the maximum number of streams that an EXA Powered video subscriber can join simultaneously, as well as the MVR profile to use.
- **Video Channel Profile –** Define a global video channel lineup.
- **Video Channel Templates –** Define the transport connections for each video channel.
- **ONT Profiles –** Define the physical characteristic of the ONT. For descriptions of profile parameters, see *ONT Profile Parameters* (on page 107).
- **VLAN-IF Templates –** Define the VLAN interface parameters used by all new connections assigned to the virtual bridge.
- **PWE3 Templates –** Defines the parameters for transporting pseudowire traffic across two endpoints.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

For additional information about video services, see the *Calix C7 Video Services Guide*. For additional information about data services, see the *Calix C7 Broadband Data Services Guide*.

You can also export selected global profiles and templates from the CMS server, and import them into other CMS servers. For more information, see the *Calix Management System (CMS) Guide*.

How Global Profile Mapping and Synchronization Work

When you create a global profile, CMS automatically maps or links it with a local C7 network profile. Once linked, if the global profile is modified, the local profiles are automatically synchronized or updated.

Global profiles are mapped or synchronized with local C7 networks when you perform any of the following tasks:

- Create or modify a global profile in CMS.
- Add a new C7 network to CMS.
- Manually synchronize global profiles with C7 networks.

For global profiles to be mapped to and synchronized with local C7 network profiles, all of the following conditions must be met:

1. The C7 network must be connected to CMS.
2. The Enabled parameter for the global profile must be set to Yes.
3. The Global Profiles Enabled parameter for the C7 network must be set to Yes.

Note: Yes is the default setting when you create a global profile or C7 network. For the behavior when these parameters are modified, see the explanations.

If all of the above conditions are met, when you create a global C7 profile in CMS, the system checks the local profiles on each C7 network and first compares all profile parameters except the profile ID and profile description.

The following tables describe how the system maps global profiles created in CMS to local C7 network profiles.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

How a global profile maps to a local profile (other than a C7 video channel profile)

None of the local profiles match the global profile	The system creates a local profile with the @ symbol as the prefix in the profile Description field. If the global profile ID is already used by one of the local profiles, the system creates a local profile with a new profile ID and maps to it.
One or more local profiles match the global profile	The system maps the global profile to the local profile with the same profile ID, if it exists; otherwise, the system maps the global profile to one of the matched local profiles. **Note:** For all global profiles except ADSL templates, the matched local profile description is updated to match the global profile description.

How a global profile maps to a C7 video channel profile

None of the local profiles match the global profile	The system creates a local profile with the @ symbol as the prefix in the Channel Description field. If the global profile IP address is already used by one of the local profiles, a local video channel profile is not created.
One or more local profiles match the global profile	The system maps the global profile to the matched local profile with the same IP address, if it exists. If it does not exist, a local video channel profile is not created.

To view how a global profile is mapped to network profiles, see *Viewing Global Profile Synchronization Details* (on page 86).

Modifying the Enabled parameter for a global profile

1. If you create a global profile with the Enabled parameter set to No, the global profile does not map to or synchronize with local profiles on C7 networks.
2. If you modify the Enabled parameter for an existing global profile from No to Yes, the global profile maps to and synchronizes with enabled C7 networks. For any future C7 networks created in CMS, the global profile is also mapped and synchronized.
3. If you modify the Enabled parameter for an existing global profile from Yes to No, C7 networks already synchronized are not affected. For any future C7 networks created in CMS, the global profile is not mapped or synchronized.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Modifying the Global Profiles Enabled parameter for a C7 network

1. If you create a C7 network with the Global Profiles Enabled parameter set to No, global profiles do not map to or synchronize with the profiles on that C7 network.
2. If you modify the Global Profiles Enabled parameter for an existing C7 network from No to Yes, the global profiles map and synchronize with the C7 network.
3. If you modify the Global Profiles Enabled parameter for an existing C7 network from Yes to No, the existing profiles on the C7 network are not affected. For any future global profiles created or modified in CMS, the local profiles are not mapped or synchronized.

Creating Global Profiles

This topic includes instructions to:

- Create a global video channel profile
- Create a global video channel template
- Create a global VLAN-IF Template
- Create a global Ethernet-over-SONET traffic profile
- Create a global ONT profile

See also:

- *Creating a Video or Data Subscriber Template* (on page 276)
- *Creating a Global Profile by Importing a C7 Network Profile* (on page 84)

Creating a global C7 profile requires Full CMS Administration privileges.

To create a global video channel profile

See the topic, "Importing or Manually Defining a Video Channel Lineup," in the *Calix C7 Video Services Guide*.

To create a global video channel template

For more information, see the *Calix C7 Video Services Guide*.

1. On the Navigation Tree, click **CMS**.
2. In the Work Area, click **Profile** > **C7** > **Video Channel Template**.
3. Click **Create**. A New Template window opens.
4. In the Video Channel Template dialog box, do the following:
   a. In the Template ID field, enter a number from 1 to 20.
   b. In the Description box, type a name to describe the template (maximum of 10 characters; global profile descriptions are automatically prefixed with the "@" symbol when you create them).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

c. In the Enabled list, select **Y** (Yes) to apply to all connected networks. Select **N** (No) to create the global profile but not apply it immediately.

5. In the Video Channels Available to be Created area, do the following:
   a. Select the video channels to add to the template. Use Shift+click to select a range of channels, or Ctrl+click to select channels one at a time.
   b. Click **Add** to place the channels in the Video Channels in the Template to be Created area.
6. Click **Add Template** to complete the template creation process.

To create a global VLAN-IF template

For more information, see the *Calix C7 Ethernet and IP Services Guide* and the *Calix C7 Broadband Data Services Guide.*

1. On the Navigation Tree, click **CMS**.
2. In the Work Area, click **Profile** > **C7** > **VLAN-IF Template**.
3. Click **Create**. A New Template window opens.
4. In the VLAN-IF Template dialog box, do the following:
   a. In the Template Identifier box, type a number to identify the new traffic profile (1 through 20).
   b. In the Description box, type a name to describe the profile (maximum of 10 characters; global profile descriptions are automatically prefixed with the "@" symbol when you create them).
   c. Enter values for each of the remaining parameters.
   d. In the Enabled box, accept **Y** (Yes) to apply to all connected networks. Select **N** (No) to create the global profile but not apply it immediately.
5. Click **OK** to create the template.

To create a global Ethernet-over-SONET traffic profile

For more information, see the Calix Management System (CMS) Guide.

1. On the Navigation Tree, click **CMS**.
2. In the Work Area, click **Profile** > **C7** > **Ethernet Profile**.
3. Click **Create**.
4. In the Ethernet Traffic Profile dialog box, do the following:
   a. In the Identifier box, type an ID number for the profile (from 1 to 100).
   b. In the Bandwidth box, type the maximum Ethernet port transmission rate (in Mbps).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

c. In the Enabled box, select **Y** (Yes) to apply to all connected networks. Select **N** (No) to create the global profile but not apply it immediately.

5. Click **OK** to create the template.

To create a global ONT profile

For more information, see the *Calix C7 Ethernet and IP Services Guide.*

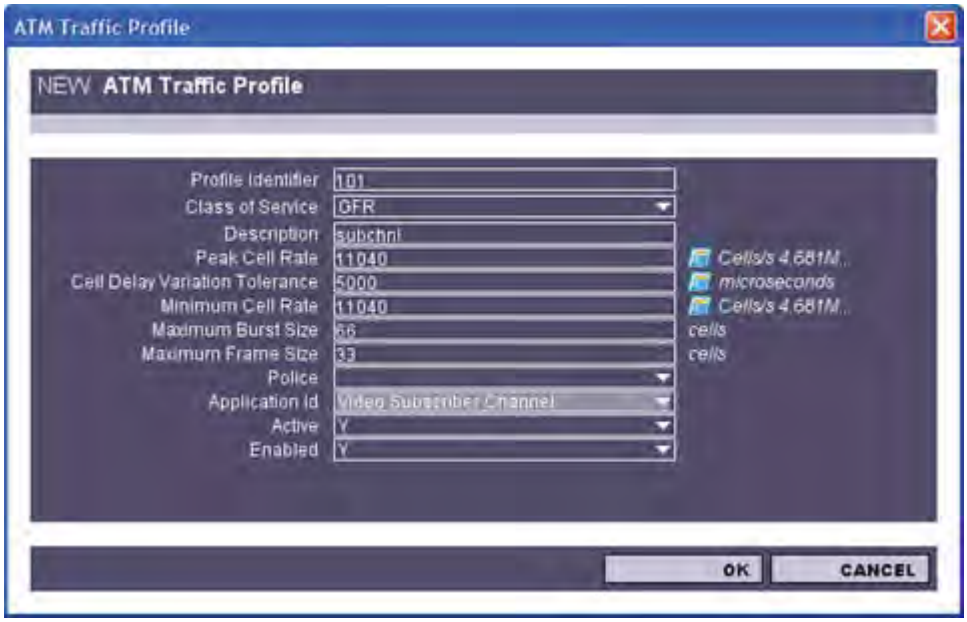
1. On the Navigation Tree, click **CMS**.
2. In the Work Area, click **Profile** > **C7** > **ONT Profile**.
3. Click **Create**.
4. In the ONT Profile dialog box, do the following:
   a. In the Identifier box, type an ID number for the profile (from 1 to 50).
   b. In the Vendor ID box, type an identifier to indicate the vendor (maximum four characters).
   c. In the Number of POTS, DS1, Ethernet, Gigabit Ethernet, RF Video, and HPNA Ports boxes, select or type the number of ports for the profile (valid values are 0, 2, 4, and 8 for POTS ports, 0 through 12 for DS1, Ethernet, and Gigabit Ethernet ports, 0 through 4 for RF video ports, and 0 through 16 for HPNA ports).
   d. In the Enabled box, select **Y** (Yes) to apply to all connected networks. Select **N** (No) to create the global profile but not apply it immediately.
5. Click **OK** to create the template.

Sample Global Traffic Profiles

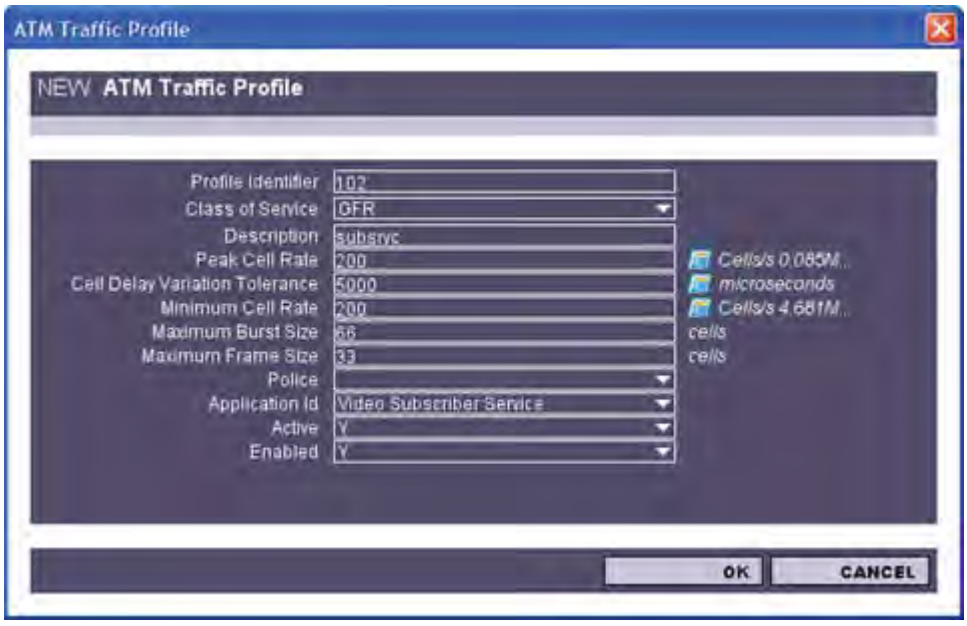
The screenshots below show sample values for global traffic profiles required for subscriber activation. Also see *Traffic Profile Parameter Descriptions* (on page 90).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

The following illustration shows the settings for a Video Subscriber Channel, using GFR, and a maximum bandwidth of 4.68 Mbps.

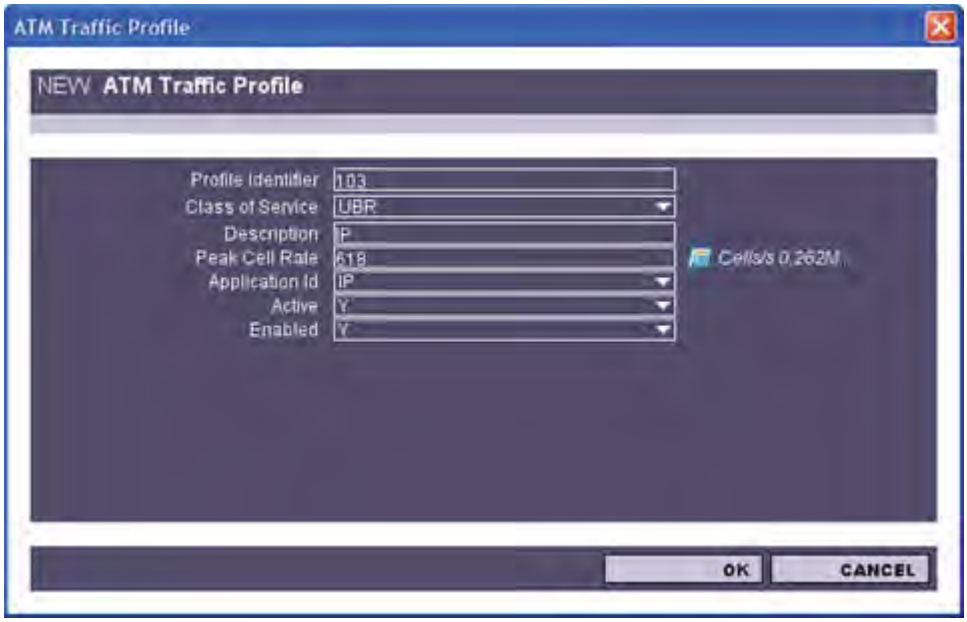


The following illustration shows the settings for a Video Subscriber Service, using GFR, and a maximum bandwidth of 0.085 Mbps.



Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

The following illustration shows the settings for an IP channel, using UBR, and a maximum bandwidth of 0.26 Mbps.



Creating a Global Profile by Importing a C7 Network Profile

You can create a global profile by importing a profile from a local C7 network.

Note: When you import a C7 network profile, the system adds the @ symbol to the front of the global profile description.

Importing a C7 network profile requires Full CMS Administration privileges.

To create a global profile by importing a C7 network profile

1. On the Navigation Tree, select a C7 network.
2. In the Work Area, click **Profile**, and then click the type of profile or template to import.
3. In the profile list, select the template(s) to import. When selecting multiple profiles, use Shift+click to select a range of profiles, or Ctrl+click to select one profile at a time.
4. Click **Action** > **Import to Global Templates**, and then click **OK** to confirm the action.

   If the import is successful, a message box displays indicating that the action completed; click **OK** to close the box. If a global profile already exists that matches the parameters of a local profile, a Task Progress window opens indicating the profile was not created.
5. To view the new global profile(s), on the Navigation Tree, click **CMS** > **Profile** > **C7**, and then click the type or profile or template.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Modifying Global Profiles

Most global profile fields cannot be modified. To change properties of a non-modifiable global profile, delete the old profile and create a new profile and apply it.

You can toggle the status of the Enabled profile field between Y (Yes) and N (No). Setting the field to Y synchronizes the profiles with all networks that enable global profiles, for example, when you enable profile that has not yet been enabled. Disabling a profile prevents it from being copied to any new networks, but does not remove the profile from the CMS database.

Modifying a global profile requires Full CMS Administration privileges.

To modify a global profile

1. On the Navigation Tree, click **CMS**.
2. In the Work Area, click **Profile** > **C7**, and then click the type of profile or template to modify.
3. In the profile list, select one or more profiles to modify.
4. In the Edit row, modify one or more of the available fields (such as the Description, Active, Enabled, or ISDEFAULT columns). After modifying a non-list field, press Tab or Enter.

   An orange arrow displays to the left of the profile(s) you are modifying.
5. Click **Apply**. Click **OK** to save the new settings.

Synchronizing Global Profiles

Global C7 profiles and templates are automatically synchronized with enabled networks when:

- You create a global profile.
- CMS connects to each C7 network.

To view or change the Global Profiles Enabled network parameter, see the Calix Management System (CMS) Guide.

You can also manually synchronize global profiles. When performing a manual synchronization, you specify the profiles to be updated:

- Select the global profiles and synchronize them to all enabled networks.
- Select a network and synchronize global profiles to that network.

Synchronizing a global profile requires Full CMS Administration privileges.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

To synchronize global profiles to all enabled networks

1. On the Navigation Tree, click **CMS**.
2. In the Work Area, click **Profile** > **C7**, and then click the type of profile or template to synchronize.
3. In the profile or template list, select one or more of the items to synchronize.
4. Click **Action** > **Synchronize**.
5. In the Confirmation dialog box, click **OK**.
6. To view the status of the synchronization, click **Action** > **Details**. A detail screen opens for each selected profile with details of the operation.

To synchronize global profiles to a specified network

1. On the Navigation Tree, click the network to synchronize.
2. In the Work Area, click **Profile**, and then click the type of profile or template to synchronize.
3. In the profile or template list, select one or more of the items to synchronize.
4. Click **Action** > **Synchronize**.
5. In the Confirmation dialog box, click **OK**.

Viewing Global Profile Synchronization Details

Viewing an E-Series global profile requires CMS Administration privileges.

To view E-Series global profile synchronization details

1. On the Navigation Tree, click **CMS**.
2. In the Work Area, click **Profile**, and then click the device type and the type of profile.
3. In the profile list, select the profile to view.
4. Click **Action** > **Details**. The Detailed Status window opens.

   In the Detailed Status window, the Profile ID column displays the profile ID for each network or node (which may be different than the global profile ID, depending on how CMS mapped to the local network when the global profile was created). The Sync Status column displays the current status of the synchronization.
5. Click **OK** or **Cancel** to close the window.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

xDSL Profiles for Data and Video Service on the Same Port or Bonding Group

When you use the subscriber activation tools to configure both data and video services on the same xDSL port or bonding group (whether you configure both services at the same time, or add one service at a time), the CMS system applies the rules in the following tables to combine the attributes from the xDSL profiles associated with the data and video subscriber templates.

xDSL profile attribute	What gets applied
Signal-to-Noise Ratio (SNR)	The value from the video subscriber template.
Upstream Rate (Max./Min.)	For ports on ADSL2-based cards or ONT Ethernet ports: The higher of the data 1, data 2, or video subscriber template values, with the following exception: If the IP VC is GFR, the values from the data 1, data 2, and video subscriber templates are added, up to the maximum allowed for the port or bonding group.
Downstream Rate (Max./Min.)	The values from the data (for both services, if provisioned) and video subscriber templates are added up to the maximum rate allowed for the port or bonding group. For maximum achievable rates, see *xDSL Template and Port Parameter Descriptions* (on page 99).
Service Type	The value from the video subscriber template.
Channel Latency	Interleaved.

Notes:

- Ensure that the correct port bandwidth will result when the rates for video and data (in the xDSL templates) are combined.
- For VDSL2 ports in ADSL2+ mode, if PTM encapsulation is required, set **PTM Encapsulation Override = Y (Yes)** in the xDSL templates to be used.

When you remove services from the Service screen or using the Delete Subscriber tool, CMS applies the rules in the following table.

Action	What gets applied
Delete both data and video services	The video subscriber template settings.
Delete video service and retain data service	The data subscriber template settings for data service 1 + data service 2.
Delete data service and retain video service	The video subscriber template settings.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Enabling a Global Profile

Enabling a global profile requires Full CMS Administration privileges.

To enable a global profile

1. On the Navigation Tree, click **CMS**.
2. In the Work Area, click **Profile**, and then the type of profile or template to enable.
3. Select the profile to enable. It displays in the edit row.
4. In the Enabled column, select **Y** (Yes) from the drop-down list.
5. Click **Apply**, and then click **OK** to save the new settings.

Deleting Global Profiles

You can delete global profiles from networks that have profiles enabled but do not have that profile applied. Deleting a profile does not remove provisioning from a network that has the profile applied.

A successful deletion (where the profile is not used in any enabled networks) removes the profile from the CMS database. An unsuccessful deletion (where one or more networks actively use the profile) flags the profile as disabled, but CMS retains it in the database and on the networks that use it. If a global template or profile is used in a data or video subscriber template, it is not deleted.

An optional force delete removes the profile from all connected networks where it is not in active use, and erases it from the database. It does not delete the provisioning from equipment that uses it.

Deleting a global profile requires Full CMS Administration privileges.

To delete a global profile

1. On the Navigation Tree, click **CMS**.
2. In the Work Area, click **Profile** > **C7**, and then click the type of profile or template to delete.
3. Click **Delete**. A confirmation screen opens.
4. (Optional) Click the Force Delete check box.
5. Click **OK** to delete the profile.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Creating a Traffic Profile

To create a C7 traffic profile

1. Do one of the following:
   - Create a global profile in CMS that is synchronized to all connected C7 networks. On the Navigation Tree, click highest level (**CMS**). On the toolbar, click **Profile** > **C7** > **Traffic Profile**.
   - Create a local profile at the network level or in C7 iMS. On the Navigation Tree, click the Network level. On the toolbar, click **Profile** > **Traffic Profile**.
2. On the toolbar, click **Create** to open the New Traffic Profile dialog box.
3. In the Traffic Profile dialog box, do the following:
   a. In the Profile Identifier box, type a number to identify the new traffic profile (1 to 488).

   Note: Profile IDs 489 to 500 are default global traffic profiles provided with CMS. You can modify or delete them, if needed.

   b. In the Description box, type a name to describe the profile (up to 10 characters for a CMS global profile, or up to 11 characters for a local C7 profile; for global profiles created in CMS, the system adds an @ symbol prefix to the description to designate a global profile).
4. Configure the traffic profile:
   a. In the Class of Service list, select a service category. The list of traffic descriptors changes according to the class of service.

   Note: UBR/UBR+ is not enforced on subscriber VCs if the uplink resides in the same C7 shelf as the subscriber card (e.g., ADSL or OLT).

   b. Enter values for each traffic descriptor that applies to the service category.

   Note: For some fields, such as the Peak Cell Rate, you can toggle units between Mbps and cells per second (cps) by clicking the calculator icon to the right of the box. If you enter a value first, clicking the calculator icon converts the value between Mbps and cps units.

   c. In the Application ID list, select an application type.
   d. (CMS only) In the Active list, select **Y** (Yes) to make the global profile active. Select **N** (No) to create the global profile but designate it as inactive.
   e. (CMS only) In the Enabled box, accept **Y** (Yes) to apply to all connected networks. Select **N** (No) to create the global profile but not apply it immediately.
5. Click **OK** to save the new profile.

Repeat Steps 3 through 5 to create additional profiles.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Traffic Profile Parameters

To configure a traffic profile, begin by selecting a Class of Service (COS). You can then configure the specific parameters associated with that COS. The C7 allows for the creation of up to 500 traffic profiles (1 to 500).

Traffic profile identifier (ID)

A number is used to uniquely define the bandwidth parameters for a class-of-service category. You can create up to 500 traffic profiles for the system. Enter a number between 1 and 500.

Traffic profile parameter overview

The table below outlines the COS categories and the parameters associated with each. It is followed by a description of each parameter.

Service Category	CDVT	PCR	SCR0	SCR01	MCR	MBS	MFS	CELLTAG	POLICE
CBR	✔	✔	--	--	--	--	--	--	✔
VBRRT	✔	✔	✔	✔	--	✔	--	✔	✔
VBRNRT	✔	✔	✔	✔	--	✔	--	✔	✔
UBR	--	✔	--	--	--	--	--	--	--
GFR	✔	✔	--	--	✔	✔	✔	✔	✔
UBR+	--	✔	--	--	✔	--	--	--	--

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Class of Service (COS)

You can specify a specific class of service for the connection from one of six service categories:

- **CBR** (constant bit rate): For real-time applications that require constant or guaranteed bandwidth (such as telephone conversations), primarily for T1 and DS0 services. An ATM cross-connect with this COS has all the specified bandwidth reserved for its use. However, unused bandwidth on this cross-connect may be "loaned" to cross-connects with some other COS for bursting traffic.
- **VBRRT*** (real-time variable bit rate): For real-time data applications that have bursty traffic patterns. For cross-connects with this COS, you can specify a peak bandwidth and sustained bandwidth, the average of which is reserved for the cross-connect. However, unused bandwidth on this cross-connect may be "loaned" to cross-connects with some other COS for bursting traffic.
- **VBRNRT*** (non real-time variable bit rate): For non-real-time applications that have bursty traffic patterns. For cross-connects with this COS, you can specify a peak bandwidth and sustained bandwidth, the average of which is reserved for the cross-connect. However, unused bandwidth on this cross-connect may be "loaned" to cross-connects with some other COS for bursting traffic.
- **GFR** (guaranteed frame rate): For non-real-time applications, primarily video services, that require a guaranteed minimum bandwidth. If and when additional bandwidth is available, the network carries traffic in excess of the guaranteed minimum rate. An ATM cross-connect with this COS will have all the specified bandwidth reserved for its use. However, unused bandwidth on this cross-connect may be "loaned" to cross-connects with some other COS for bursting traffic. You can only build a GFR cross-connect if all the requested bandwidth is available and the bandwidth does not exceed 50% of the STS capacity (for multi-shelf cross-connects).
- **UBR** (unspecified bit rate): For non-real-time applications that have no performance requirements, such as xDSL Internet connections. An ATM cross-connect with this COS has no bandwidth limitations or guarantees. It is a best-effort service, susceptible to cell loss and bandwidth starvation in congested networks. (To prevent bandwidth starvation, bandwidth can be reserved by using bandwidth constraints.) A peak cell rate (PCR) can be assigned to this COS, but it is not enforced. The peak rate for UBR traffic is able to burst, borrowing unused bandwidth from other cross-connects as needed.
- **Note**: UBR maximum upstream throughput is 2 Mbps. If PCR is not specified, 384 Kbps is the minimum throughput.
- **UBR+** (unspecified bit rate plus): For non-real-time applications that require control of the peak rate provisioned for a subscriber, such as for FTTP Internet traffic and tiered services. UBR+ differs from UBR in the following two ways: 1) Its peak cell rate (PCR) is enforced in most* applications and 2) a minimum cell rate (MCR) can optionally be specified to reserve bandwidth on a link, although not on the C7 switch fabric. (Calix recommends that you use bandwidth constraints to reserve bandwidth on a link and the C7 switch fabric.) By specifying a PCR, you can implement tiered services or keep high-usage subscribers from using up all available bandwidth.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Note: *The VBRRT and VBRNRT classes of service are not supported on Calix ONTs. Therefore, when creating traffic profiles that will be applied to ONT Ethernet port cross-connects, do not use VBRRT or VBRNRT as the COS.

*** Note:** The UBR+ PCR is not enforced on single-shelf drops from an uplink to subscribers on ADSL or OLTB cards (OLTG and VDSL2-based cards do not have this limitation). In this configuration, you can limit the downstream data rate by increasing the video bandwidth on the port (if video service is present on the same port) or by adjusting the ADSL port train rate properties (for data only). For OLTG and VDSL2-based cards, the UBR+ PCR is enforced regardless of the uplink location.

Note: If you do not set MCR and PCR values when using UBR+, it behaves like UBR: the minimum cell rate defaults to zero and the peak cell rate defaults to the line rate.

Note: Calix recommends using UBR+ profiles for data/internet services such that the PCR value can be configured to differentiate various levels of service (for example, 1-Mbps, 2-Mbps, 4-Mbps data service).

Cell Delay Variation Tolerance (CDVT)

Indicates the maximum variance (in microseconds) of cell delay that is acceptable. Cell delay occurs when cells from two or more ATM connections are multiplexed and the cells of one ATM connection are delayed while cells of another ATM connection are inserted at the output of the multiplexer. CDVT is an integer and cannot be 0.

The minimum guaranteed CDVT for CBR connections is 5,000,000 ÷ PCR.

For VBRRT, VBRNRT, and GFR connections, the parameter value must be equal to or greater than (1 ÷ PCR01) x 1,000,000.

Peak Cell Rate (PCR01)

Identifies how quickly cells arrive from the same ATM connection (the fastest cell rate is displayed). The rate is specified in cells per second. This parameter is applicable for all the supported classes of service. PCR01 is an integer and cannot be 0.

Use the following formula to convert bits per second (bps) to cells per second:

bps ÷ 424 = cells per second

You must round the number down to the lower integer.

Sustainable Cell Rate for CLP=0 (SCR0)

Indicates the average maximum rate of cells that do not have CLP=0 over the lifetime of a connection. The rate is specified in cells per second. The parameter is applicable only to the VBRRT and VBRNRT classes of service. Scr0 is an integer and must be less than PCR01.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Sustainable Cell Rate for CLP=0 and 1 (SCR01)

Indicates the average maximum rate of cells (regardless of their CLP bit setting) over the lifetime of the connection. The rate is specified in cells per second. The parameter is applicable only to the VBRRT and VBRNRT classes of service. Scr01 is an integer and must be less than PCR01.

Minimum Cell Rate (MCR)

Specifies a guaranteed minimum cell rate that the connection supports. The rate is specified in cells per second. This parameter is applicable only to the GFR and UBR+ class of service. MCR is an integer and must be less than PCR01. (For UBR+, Calix recommends that you use bandwidth constraints instead of MCR to reserve bandwidth on a link.)

Maximum Burst Size (MBS)

Specifies the maximum number of consecutive cells that the source may send before the cells are tagged or discarded. This parameter is only applicable to the VBRRT, VBRNRT, and GFR classes of services. The parameter value can only be a non-zero integer.

Maximum Frame Size (MFS)

Specifies the maximum number of cells in a frame. This parameter is applicable only to the GFR class of service. MFS is an integer.

Cell tagging (CELLTAG)

Specifies whether the cells that exceed the specification should be tagged with CLP=1. The parameter is applicable to the GFR, VBRNRT, and VBRRT classes of service. The default value is N (No).

Policing (POLICE)

Specifies whether rate policing is turned on. This parameter is only applicable to the CBR, VBRRT, VBRNRT, and GFR classes of service.

The processing required to support policing results in a total available bandwidth reduction of approximately 20%. The default value is Y (Yes).

Application ID (APPID)

Specifies the type of video service application. Assign an ID to associate a video application with the profile. For descriptions of the options for this parameter, see the *Calix C7 Video Services Guide*.

When creating a C7 traffic profile for Ethernet data-only services, leave the Application ID field empty.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Creating an xDSL Template

xDSL templates enable you to define and apply port settings for C7 ADSL and VDSL cards to match your service offerings. Default xDSL templates for each xDSL service type are provided. See *Default xDSL Templates* (on page 95).

Creating a custom xDSL template often only involve changing a few parameters from the defaults such as the service type, maximum upstream rate, and maximum downstream rate. Other parameters can be modified based on your needs. See *xDSL Template and Port Parameter Descriptions* (on page 99).

Adding an xDSL template in CMS creates a global template that is copied to all connected C7 networks.

To create a C7 xDSL template

1. Do one of the following:
   - Create a global template in CMS that is synchronized to all connected C7 networks. On the Navigation Tree, click highest level (**CMS**). On the toolbar, click **Profile** > **C7** > **xDSL Template**.
   - Create a local template at the network level or in C7 iMS. On the Navigation Tree, click the Network level. On the toolbar, click **Profile** > **xDSL Template**.
2. On the toolbar, click **Create** to open the xDSL Template dialog box.
3. In the xDSL Template dialog box:
   a. In the Template Identifier box, type an ID number to identify the new profile (from 1 to 50, or from 300 to 500 for global CMS templates; from 1 to 50 for local C7 templates).
   b. In the Description box, type a name to describe the profile (up to 10 characters for a CMS global template, or up to 11 characters for a local C7 template; for global templates created in CMS, the system adds an @ symbol prefix to the description).
   c. In the Service Type list, select a service type from among the nine default C7 ADSL or service types or two VDSL service types.

   Note: The default attributes from the service type display. Use the defaults as a baseline from which to define your custom template.

   Tip: Position the mouse pointer over an input box to display the valid range for the parameter.

   d. Type or select values for each of the fields.

   Note: For VDSL2 ports in ADSL2+ mode, if PTM encapsulation is required, set PTM Encapsulation Override = **Y (Yes)** in the xDSL template.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

e. (CMS only) In the Active list, select **Y** (Yes) to make the global template active. Select **N** (No) to create the global template but designate it as inactive.

f. (CMS only) In the Enabled box, accept **Y** (Yes) to apply to all connected networks. Select **N** (No) to create the global template but not apply it immediately.

4. Click **OK** to save the new template.

Default xDSL Templates

The C7 provides nine default ADSL templates and two default VDSL templates. These templates are based on the various xDSL standards. You can apply xDSL templates to any ADSL or xDSL port within the system to define the service attributes for that port. You can create up to 250 different xDSL templates, or you can use any of the default C7 templates.

Also see *xDSL Template and Port Parameter Descriptions* (on page 99).

ADSL templates

The following tables show the attributes of the nine default ADSL templates. The first table defines the legacy ADSL templates (pre-ADSL2+) that can be applied to any ADSL port. The second table defines the templates that can be applied to ADSL2+ ports only.

Parameter	MM	G.Lite	T1.413	G.DMT
Profile Identifier (ID)	MM	GLITE	T1413	GDMT
Description (DESC)	MM	GLITE	T1413	GDMT
Service Type (SRVTYPE)	MM	GLITE	T1413	GDMT
Packet Mode (PKTMODE)	Default	Default	Default	Default
Packet VPI (PKTVPI)	See note.	See note.	See note.	See note.
Packet VCI (PKTVCI)	See note.	See note.	See note.	See note.
Report Remove/Restore (RPTRMVRST)	[no entry]	[no entry]	[no entry]	[no entry]
Channel Latency (CHNLLAT)	INTLV	INTLV	INTLV	INTLV
Trellis Coding (TC)	ENABLED	ENABLED	ENABLED	ENABLED
Maximum Downstream Rate (XRDS)	8160 Kbps	1536 Kbps	8160 Kbps	8160 Kbps
Minimum Downstream Rate (MRDS)	384 Kbps	384 Kbps	384 Kbps	384 Kbps
Maximum Downstream SNR Margin (XMDS)	16 dB	16 dB	16 dB	16 dB
Target Downstream SNR Margin (TMDS)	8 dB	8 dB	8 dB	8 dB
Minimum Downstream SNR Margin (MMDS)	0 dB	0 dB	0 dB	0 dB
Maximum Interleaving Latency Downstream (INLVLATDS)	AUTO	AUTO	AUTO	AUTO
Minimum Impulse Noise Protection Downstream (MININPDS)	[no entry]	[no entry]	[no entry]	[no entry]
Maximum Upstream Rate (XRUS)	800 Kbps	512 Kbps	800 Kbps	800 Kbps
Minimum Upstream Rate (MRUS)	128 Kbps	128 Kbps	128 Kbps	128 Kbps
Maximum Upstream SNR Margin (XMUS)	16 dB	16 dB	16 dB	16 dB
Target Upstream SNR Margin (TMUS)	8 dB	8 dB	8 dB	8 dB
Minimum Upstream SNR Margin (MMUS)	0 dB	0 dB	0 dB	0 dB

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Parameter	MM	G.Lite	T1.413	G.DMT
Maximum Interleaving Latency Upstream (INTLVLATUS)	AUTO	AUTO	AUTO	AUTO
Minimum Impulse Noise Protection Upstream (MININPUS)	[no entry]	[no entry]	[no entry]	[no entry]
PTM Encapsulation Override (PTMOVER)	[no entry]	[no entry]	[no entry]	[no entry]
ATM Header Compression (AHC)	[no entry]	[no entry]	[no entry]	[no entry]
Enhanced Impulse Noise Protection (EINP)	[no entry]	[no entry]	[no entry]	[no entry]

Note: Packet VPI and VCI (PKTVPI and PKTVCI) are required when the Packet Mode value is set to Y (Yes), which is only applicable when the xDSL template is applied to an xDSL port on a VDSL card.

ADSL2+ templates

Parameter	MM2+	ADSL2+	ADSL2	READSL2	ANNEXM
Profile Identifier (ID)	MM2+	ADSL2+	ADSL	REASDSL2	ANNEXM
Description (DESC)	MM2+	ADSL2+	ADSL	REASDSL2	ANNEXM
Service Type (SRVTYPE)	MM2+	ADSL2+	ADSL	REASDSL2	ANNEXM
Packet Mode (PKTMODE)	Default	Default	Default	Default	Default
Packet VPI (PKTVPI)	See note.	See note.	See note.	See note.	See note.
Packet VCI (PKTVCI)	See note.	See note.	See note.	See note.	See note.
Report Remove/Restore (RPTRMVRST)	[no entry]	[no entry]	[no entry]	[no entry]	[no entry]
Channel Latency (CHNLLAT)	INTLV	INTLV	INTLV	INTLV	INTLV
Trellis Coding (TC)	ENABLED	ENABLED	ENABLED	ENABLED	ENABLED
Maximum Downstream Rate (XRDS)	32736 Kbps	32736 Kbps	16352 Kbps	1536 Kbps	32736 Kbps
Minimum Downstream Rate (MRDS)	384 Kbps	384 Kbps	384 Kbps	384 Kbps	384 Kbps
Maximum Downstream SNR Margin (XMDS)	16 dB	16 dB	16 dB	16 dB	16 dB
Target Downstream SNR Margin (TMDS)	6 dB	6 dB	6 dB	6 dB	6 dB
Minimum Downstream SNR Margin (MMDS)	0 dB	0 dB	0 dB	0 dB	0 dB
Maximum Interleaving Latency Downstream (INLVLATDS)	Auto	Auto	Auto	Auto	Auto
Minimum Impulse Noise Protection Downstream (MININPDS)	[no entry]	[no entry]	[no entry]	[no entry]	[no entry]
Maximum Upstream Rate (XRUS)	800 Kbps	800 Kbps	800 Kbps	512 Kbps	800 Kbps
Minimum Upstream Rate (MRUS)	128 Kbps	128 Kbps	128 Kbps	128 Kbps	128 Kbps
Maximum Upstream SNR Margin (XMUS)	16 dB	16 dB	16 dB	16 dB	16 dB
Target Upstream SNR Margin (TMUS)	6 dB	6 dB	6 dB	6 dB	6 dB
Minimum Upstream SNR Margin (MMUS)	0 dB	0 dB	0 dB	0 dB	0 dB
Maximum Interleaving Latency Upstream (INTLVLATDS)	AUTO	AUTO	AUTO	AUTO	AUTO
Minimum Impulse Noise Protection Upstream (MININPUS)	1 Symbol	1 Symbol	1 Symbol	1 Symbol	1 Symbol
PTM Encapsulation Override (PTMOVER)	[no entry]	[no entry]	[no entry]	[no entry]	[no entry]
Power Management MODE (PMMODE)	L0	L0	N/A	N/A	L0
L0 Time (L0TIME)	255 sec.	255 sec.	N/A	N/A	255 sec.
L2 Time (L2TIME)	255 sec.	255 sec.	N/A	N/A	255 sec.
L2 Entry Time Threshold (L2ENTRYT)	1800 sec.	1800 sec.	N/A	N/A	1800 sec.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Parameter	MM2+	ADSL2+	ADSL2	READSL2	ANNEXM
L2 Minimum Aggregate Transmit Power Reduction (L2MINATPR)	255 dB	255 dB	N/A	N/A	255 dB
L2 Max Aggregate Tx Pwr Reduction (L2ATPR)	3 dB	3 dB	N/A	N/A	3 dB
L2 Minimum Data Rate in Low Power Mode (L2MINR)	1024 Kbps	1024 Kbps	N/A	N/A	1024 Kbps
L2 Entry Rate Threshold (L2ENTRYR)	1	1	N/A	N/A	1
L2 Exit Rate Threshold (L2EXITR)	512 Kbps	512 Kbps	N/A	N/A	512 Kbps
ATM Header Compression (AHC)	N	N	N	N	N
Enhanced Impulse Noise Protection (EINP)	[no entry]	[no entry]	[no entry]	None	[no entry]
Rate Adaptation MODE Downstream (RAMODEDS)	Init	Init	N/A	N/A	Init
Rate Adaptation Upshift Margin DownStream (RAUMDS)	9 dB	9 dB	N/A	N/A	9 dB
Rate Adaptation Downshift Margin DownStream (RADMDS)	3 dB	3 dB	N/A	N/A	3 dB
Rate Adaptation Upshift Time Downstream (RAUTDS)	60 sec.	60 sec.	N/A	N/A	60 sec.
Rate Adaptation Downshift Time Downstream (RADTDS)	60 sec.	60 sec.	N/A	N/A	60 sec.
Rate Adaptation MODE Upstream (RAMODEUS)	Init	Init	N/A	N/A	Init
Rate Adaptation Upshift Margin Upstream (RAUMUS)	9 dB	9 dB	N/A	N/A	9 dB
Rate Adaptation Downshift Margin Upstream (RADMUS)	3 dB	3 dB	N/A	N/A	3 dB
Rate Adaptation Upshift Time Upstream (RAUTUS)	60 sec.	60 sec.	N/A	N/A	60 sec.
Rate Adaptation Downshift Time Upstream (RADTUS)	60 sec.	60 sec.	N/A	N/A	60 sec.

Note: Packet VPI and VCI (PKTVPI and PKTVCI) are required when the Packet Mode value is set to Y (Yes), which is only applicable when the xDSL template is applied to an xDSL port on a VDSL card.

Considerations for ADSL2+ Annex M

- The first occurrence (per card) of setting an ADSL2 port to use the Annex M service type causes a retrain of all CPE connected to the card (up to 24 ports). Provisioning additional Annex M ports on the same card does not cause further CPE retrains.
- The ITU ADSL2+ G.992.5 standard states: "When deployed in the same cable as ADSL-over-POTS (Annex A/G.992.1, Annexes A & B/G.992.2, Annex A/G.992.3, Annex A/G.992.4 and Annex A/G.992.5), there may be a spectral compatibility issue between the two systems due to the overlap of the Annex M upstream channel with the ADSL-over-POTS downstream channel at frequencies above 138 kHz." Calix has performed crosstalk testing and noted no performance degradation related to this issue. However, use care when mixing Annex M with Annex A service types in the same binder group. As a best practice, avoid mixing Annex M with Annex A whenever possible to eliminate potential crosstalk issues.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

VDSL templates

The following tables show the attributes of the two default VDSL templates that can be applied to VDSL2 ports.

Parameter	VDSL2MM	VDSL2
Profile Identifier (ID)	VDSL2MM	VDSL2
Description (DESC)	VDSL2MM	VDSL2
Service Type (SRVTYPE)	VDSL2MM	VDSL2
Packet Mode (PKTMODE)	Yes	Yes
Packet VPI (PKTVPI)	0	N/A
Packet VCI (PKTVCI)	35	N/A
xDSL Line Profile (XDSLLINEPROF)	8D	8D
Report Remove/Restore (RPTRMVRST)	N	N
Channel Latency (CHNLLAT)	INTLV	INTLV
Maximum Downstream Rate (XRDS)	512000 Kbps	512000 Kbps
Minimum Downstream Rate (MRDS)	64 Kbps	64 Kbps
Maximum Downstream SNR Margin (XMDS)	16 dB	16 dB
Target Downstream SNR Margin (TMDS)	6 dB	6 dB
Minimum Downstream SNR Margin (MMDS)	0 dB	0 dB
Maximum Interleaving Latency Downstream (INLVLATDS)	Auto	Auto
Minimum Impulse Noise Protection Downstream (MININPDS)	1/2 Symbol	1/2 Symbol
Maximum Upstream Rate (XRUS)	512000 Kbps	512000 Kbps
Minimum Upstream Rate (MRUS)	64 Kbps	64 Kbps
Maximum Upstream SNR Margin (XMUS)	16 dB	16 dB
Target Upstream SNR Margin (TMUS)	6 dB	6 dB
Minimum Upstream SNR Margin (MMUS)	dB	0 dB
Maximum Interleaving Latency Upstream (INTLVLATUS)	AUTO	AUTO
Minimum Impulse Noise Protection Upstream (MININPUS)	1/2 Symbol	1/2 Symbol
PTM Encapsulation Override (PTMOVER)	N	N/A
Power Management MODE (PMMODE)	L0	N/A
L0 Time (L0TIME)	255 sec.	N/A
L2 Time (L2TIME)	255 sec.	N/A
L2 Entry Time Threshold (L2ENTRYT)	1800 sec.	N/A
L2 Minimum Aggregate Transmit Power Reduction (L2MINATPR)	255 dB	N/A
L2 Max Aggregate Tx Pwr Reduction (L2ATPR)	3 dB	N/A
L2 Minimum Data Rate in Low Power Mode (L2MINR)	1024 Kbps	N/A
L2 Entry Rate Threshold (L2ENTRYR)	512 Kbps	N/A
L2 Entry Rate Threshold (L2ENTRYR)	[no entry]	N/A
L2 Exit Rate Threshold (L2EXITR)	[no entry]	N/A

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Parameter	VDSL2MM	VDSL2
ATM Header Compression (AHC)	N	N/A
Enhanced Impulse Noise Protection (EINP)	None	None
Rate Adaptation MODE Downstream (RAMODEDS)	Init	N/A
Rate Adaptation Upshift Margin DownStream (RAUMDS)	9 dB	N/A
Rate Adaptation Downshift Margin DownStream (RADMDS)	3 dB	N/A
Rate Adaptation Upshift Time Downstream (RAUTDS)	60 sec.	N/A
Rate Adaptation Downshift Time Downstream (RADTDS)	60 sec.	N/A
Rate Adaptation MODE Upstream (RAMODEUS)	Init	N/A
Rate Adaptation Upshift Margin Upstream (RAUMUS)	9 dB	N/A
Rate Adaptation Downshift Margin Upstream (RADMUS)	3 dB	N/A
Rate Adaptation Upshift Time Upstream (RAUTUS)	60 sec.	N/A
Rate Adaptation Downshift Time Upstream (RADTUS)	60 sec.	N/A
Power Management MODE (PMMODE)	L0	N/A
UpStream Start Tone Band 0 (US0ST)	0	N/A
UpStream End Tone Band 0 (US0ET)	0	N/A
DownStream Start Tone Band 1 (DS1ST)	0	N/A
DownStream End Tone Band 1 (DS1ET)	0	N/A
PSD Mask Upstream (US0PSD)	Eu32	Eu32
Notch 1 Start - Notch 4 Start (VNSTART1 - VNSTART4)	0 kHz	0 kHz
Notch 1 Stop to Notch 4 Stop (VNSTOP1 - VNSTOP4)	0 kHz	0 kHz
RFI 1 Start - RFI 4 Start (VRSTART1 - VRSTART4)	0 kHz	0 kHz
RFI 1 Stop - RFI 4 Stop (VRSTOP1 - VRSTOP4)	0 kHz	0 kHz

xDSL Template and Port Parameter Descriptions

This topic describes the configurable parameters for xDSL ports. The abbreviated name shown in parentheses represents the parameter ID in the Provisioning table view when multiple ports are selected.

Primary Service State (PST): At the port level, the PST specifies the default state of the equipment once it is installed. The values are IS (in-service) or OOS (out-of-service). The default value is IS. You can also use this parameter to pre-provision a port, where the IS default value places the equipment in-service once installed.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

User Description (USERDESCR): A user-defined character string of up to 11 characters. This optional field allows you to provide any additional information about a port.

Basic Settings

xDSL Group (GROUPADDR): (For ADSL2/COMBO2-24A and VDSL2-based cards only) Displays which bonded group the port belongs to (if any).

xDSL Template (XDSLTEMPLATE): Specifies a template to apply to define the xDSL port service attributes. You can choose one of the nine default C7 ADSL templates, one of the two C7 VDSL templates, or one of up to 250 custom templates of your creation.

- At the port level: Select a template ID from the list to apply its attributes to the xDSL port. The parameter values from that template automatically display on the port. You can then adjust the values supplied by the template on a per-parameter basis, as needed.
- When creating a new xDSL template: Type a value not used by an existing template from 1 to 50, or from 300 to 500.

Service Type (SRVTYPE): Specifies the operating modes that dictate the handshaking protocol, channel capacity, and other physical line characteristics based on xDSL specifications.

For ADSL select one of the following values:

- **MM2+** (multi-mode 2+) – Allows the port to automatically detect and train up to the service type supported by the CPE; supports ADSL2+, ADSL2, and READSL2 standards as well as G.DMT, T1-413, and G.Lite standards
- **ADSL2+** – ADSL2+ standards specification; supports ADSL2+, ADSL2, and READSL2 standards
- **ADSL2** – ADSL2 standards specification; supports both ADSL2 and READSL2 standards
- **READSL2** (Reach Extended ADSL2): READSL2 standards specification; supports both READSL2 and ADSL2 standards
- **ANNEXM** – ADSL2/ADSL2+ Annex M standards specification
- **MM** (multi-mode) – Enables the port to automatically detect and train up to the service type supported by the CPE; supports G.DMT, T1-413, and G.Lite standards
- **GDMT** – GDMT standards specification
- **T1413** – T1.413 standards specification
- **GLITE** – G.Lite standards specification

The default value is *MM2+* for ADSL2+ ports and *MM* for legacy ADSL ports. To train up, the CPE must support the selected mode.

For VDSL select one of the following values:

- **VDSL2** – VDSL2 (ITU-T G.993.2) standards specification for the following profiles: 8a, 8b, 8c, 8d, 12a*, 12b*, 17a* (* 5-Band plan only)

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- **VDSL2MM** (VDSL multi-mode) – Enables the port to automatically detect and train up to the service type supported by the CPE; supports both VDSL2 and all ADSL standards listed above

Packet Mode (PKTMODE): Defines whether a port operates in packet mode (Y) or ATM mode (N). Packet mode must be set to Y for all ports on VDSL cards that use VDSL2 and VDSL2MM service types. Ports using any of the ADSL service types listed above can be set to either packet mode or ATM mode.

Note: For xDSL templates with a "Default" Packet Mode, packet mode (Y) is applied to ports on VDSL cards and ATM mode (N) is applied to ports on ADSL cards.

Packet VPI (PKTVPI): The VP value assigned to the VC, applicable to all service types except VDSL2. Valid range is from 0 to 255. The default is 0.

Packet VCI (PKTVCI): The VC value assigned to the VC, applicable to all service types except VDSL2. Valid range is from 32 to 65535. The default is 35.

xDSL Line Profile (XDSLLINEPROF): (xDSL ports only) The VDSL2 profile used for the port, applicable for VDSL2 and VDSLMM service types only. The following profiles are available:

- (3-Band plan) NA, 8a, 8b, 8c, 8d
- (5-Band plan) NA, 8a, 8b, 8c, 8d, 12a, 12b, 17a
- The default is 8d.

Note: For VDSL2-based cards, the 'Band Plan' parameter is available at the card level, under the Provisioning tab in the Work Area.

Grade of Service (GOS): The ID number (and description) of a defined Grade of Service profile. Grade of Service profiles define PM counter thresholds. To apply a Grade of Service profile, select a profile ID from the list. You can apply the default Grade of Service profile (DEFLT) defined by the Standards, apply a custom profile, or select OFF to disable reporting of threshold crossing alerts. The default value is OFF.

Report Remove/Restore (REPTRMVRST): Enables/disables reporting of port remove/restore events (including modem retrains) in the system event logs. Reporting of these events can congest the system event logs. Y (Yes) enables reporting, N (No) disables reporting. The default value is N.

Channel Latency (CHNLLAT): Specifies the operating mode of the primary channel. Select one of the following values:

- **FAST** – Specifies a minimum of 4 ms delay
- **INTLV** – Specifies a delay greater than or equal to 5 ms

The default value is INTLV, recommended for supporting video services on the xDSL port.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Trellis Coding (TC): (set in the xDSL template only) Enables trellis coding to improve the DSL system performance. Trellis coding is a method of forward error correction in which each signal element is assigned a value based on phase and amplitude to help the receiving modem determine if the element is received in error. It is used to meet performance margin requirements for long loops, or increase the transmission throughput under a specified performance margin; provides increased gain against background and cross-talk noise. The default value is ENABLED. Select DISABLED to turn off this performance enhancement.

Max Downstream Rate (XRDS): Specifies the maximum downstream rate. This parameter is specified in kilobits per second (kbps).

- For ADSL ports, enter a number from 64 to 32,736 (conditional), in increments of 32.

  Note: The maximum rate depends on the xDSL service type used. For example, for MM2+, ADSL2+, and Annex M service types, the maximum downstream rate is 32,736 kbps.

- For xDSL ports on VDSL cards, enter a number from 64 to 100,000 (conditional), in increments of 32. For VDSL2 and VDSLMM service types, the maximum configurable downstream rate is 512,000 kbps; however, the maximum achievable downstream rates are listed below:
  - 3-band plan; 8a, 8b, 8c, 8d profile; Max: 50,000 kbps downstream
  - 5-band plan; 8a, 8b, 8c, 8d profile; Max: 80,000 kbps downstream
  - 5-band plan; 12a, 12b profile; Max: 80,000 kbps downstream
  - 5-band plan; 17a profile; Max: 100,000 kbps downstream

  Note: The maximum achievable downstream rates are also limited by CPE variability.

Min Downstream Rate (MRDS): Specifies the minimum downstream rate. This parameter is specified in kbps.

- For ADSL ports, enter a number from 64 to 32,736 (conditional), in increments of 32. (See the note for XRDS for ADSL ports, above.)
- For xDSL ports on VDSL cards, enter a number from 64 to 100,000 (conditional), in increments of 32. (See the rates for XRDS xDSL ports, above.)

Maximum Downstream SNR Margin (XMDS): Specifies the maximum signal-to-noise ratio in dB for the downstream direction. Select a value from 0 to 31.

Target Downstream SNR Margin (TMDS): Specifies the target signal-to-noise ratio in dB for the downstream direction. Select a value from 0 to 15.

Minimum Downstream SNR Margin (MMDS): Specifies the minimum signal-to-noise ratio in dB for the downstream direction. Select a value from –32 to +15.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Max Interleaving Latency Downstream (INLVLATDS): Specifies the tolerable delay of the data transmission in milliseconds (ms) for the downstream direction on an interleaved channel (if the Channel Latency parameter value is INTLV). Select AUTO, or a number from 5 to 64 ms based on the following guidelines:

- Select a lower number to prioritize delay over performance (less delay).
- Select a higher number to prioritize performance over delay (more delay).
- Select AUTO to optimize latency between delay and error performance.

Minimum Impulse Noise Protection Downstream (MININPDS): (For ADSL2/COMBO2-24A and VDSL2-based cards only) Downstream minimum noise protection.

Max Upstream Rate (XRUS): Specifies the maximum upstream rate. This parameter is specified in Kbps.

- For ADSL ports without Annex M, enter a number from 0 to 2048 (conditional), in increments of 32 Kbps.
- For ADSL ports with Annex M, enter a number from 0 to 3072, in increments of 32 Kbps.
- For xDSL ports on VDSL cards, enter a number from 0 to 60,000 (conditional), in increments of 32 Kbps. For VDSL2 and VDSLMM service types, the maximum configurable upstream rate is 512,000 kbps; however, the maximum achievable upstream rates are listed below:
  - 3-band plan; 8a, 8b, 8c, 8d profile; Max: 10,000 kbps upstream
  - 5-band plan; 8a, 8b, 8c, 8d profile; Max: 18,000 kbps upstream
  - 5-band plan; 12a, 12b profile; Max: 60,000 kbps upstream
  - 5-band plan; 17a profile; Max: 60,000 kbps upstream

Note: The maximum achievable upstream rates are also limited by CPE variability.

Min Upstream Rate (MRUS): Specifies the minimum upstream rate. This parameter is specified in Kbps.

- For ADSL ports without Annex M, enter a number from 0 to 2048 (conditional), in increments of 32 Kbps.
- For ADSL ports with Annex M, enter a number from 0 to 3072, in increments of 32 Kbps.
- For xDSL ports on VDSL cards, enter a number from 0 to 60,000 (conditional), in increments of 32 Kbps. (See the rates for XRUS, above.)

Maximum Upstream SNR Margin (XMUS): Specifies the maximum signal-to-noise ratio in dB for the upstream direction. Select a value from 0 to 31.

Target Upstream SNR Margin (TMUS): Specifies the target signal-to-noise in dB ratio in the upstream direction. Select a value from 0 to 15.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Minimum Upstream SNR Margin (MMUS): Specifies the minimum signal-to-noise ratio in dB for the upstream direction. Select a value from –32 to +15.

Max Interleaving Latency Upstream (INLVLATUS): Specifies the tolerable delay of the data transmission in milliseconds (ms) for the upstream direction on an interleaved channel (if the Channel Latency parameter value is INTLV). Select AUTO, or a number from 5 to 64 ms based on the following guidelines:

- Enter a lower number to prioritize delay over performance (less delay).
- Enter a higher number to prioritize performance over delay (more delay).
- Enter AUTO to optimize latency between delay and error performance.

Minimum Impulse Noise Protection Upstream (MININPUS): (For ADSL2/COMBO2-24A and VDSL2-based cards only) Upstream minimum noise protection.

Advanced ADSL2+ parameters

The following additional parameters apply to ADSL2+ capable ports only and to ports set to the VDSL2MM service type compatible with ADSL2+ CPE:

PTM Encapsulation Override (PTMOVER): (xDSL ports on VDSL2-based cards only) If set to **Y** (Yes), the default encapsulation for ADSL2+ mode operation is overridden, and PTM encapsulation is used. (**Note:** Requires corresponding feature support on the CPE)

Power Management MODE (PMMODE): There are four options for ADSL Power Management states:

- **L0** – Specifies to operate in full power mode at all times. May not be supported by all CPE.
- **L2** – Specifies a low power state for use when there is little or no traffic. When traffic decreases, the ADSL2 transitions into L2 low power mode and overall power consumption is reduced. L2 allows keep-alive traffic and returns to L0 mode within 2 DMT frames. Wideband energy transmitted during L2 mode. May not be supported by all CPE.
- **L2L3** – Specifies either L2 or L3 power management state. May not be supported by all CPE.
- **L3** – Specifies a sleep mode when power is not required. The L3 power state is used when the user in not on-line and there is no traffic on the ADSL2 connection. When in L3 power management mode, the ADSL2 connection goes though an initialization process before the connection can be re-established. May not be supported by all CPE. **Note:** L3 power management state is not supported in this Release.

L0 Time (L0TIME): Minimum L0 Time interval between L2 exit and next L2 entry. The range is 0 to 255 seconds. The default value is 255. May not be supported by all CPE.

L2 Time (L2TIME): Minimum L2 time interval between L2 entry and first L2 trim. The range is 0 to 255 seconds. The default value is 255. May not be supported by all CPE.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

L2 Entry Time Threshold (L2ENTRYT): Minimum interval of time (in seconds) that the net data rate should stay below the L2-ENTRY-RATE (L2ENTRYR) before autonomous entry into low power state (L2). The value range is 900 to 65535 seconds. The default value is 180. May not be supported by all CPE.

L2 Max Aggregate Tx Pwr Reduction (L2ATPR): Maximum Aggregate Transmit Power Reduction in dB per L2 trim. The default value is 3. May not be supported by all CPE.

L2 Min Aggregate Tx Pwr Reduction (L2MINATPR): (VDSL cards only) Minimum Aggregate Transmit Power Reduction in dB per L2 trim. The default value is 3. May not be supported by all CPE.

L2 Minimum Data Rate in Low Power Mode (L2MINR): Minimum net data rate (in Kbps) during the low power state (L2). If the actual user data rate is lower than L2MINR, raw cells are injected to maintain the provisioned value. The range is 256 to 1024 Kbps. The default value is 1024. May not be supported by all CPE.

L2 Entry Rate Threshold (L2ENTRYR): Downstream data rate threshold (in Kbps) that triggers autonomous entry into low power state (L2). The value range is 1 to 1024. The value must be less than or equal to L2EXITR. The default value is 1. May not be supported by all CPEs.

L2 Exit Rate Threshold (L2EXITR): Downstream data rate threshold (in Kbps) that triggers autonomous exit from low power state (L2). The range is 1 to 1024 Kbps. The value must be less than L2MINR. The default value is 512. May not be supported by all CPE.

Rate Adaptation MODE DownStream (RAMODEDS): Specifies whether the data rate for the downstream signal is allowed to vary dynamically as the noise level varies. There are two values:

- **Init** – The rate remains at its initial rate upon train-up and does not change.
- **Dynamic** – The rate is allowed to change automatically in response to changes in the noise level. (Note that this may not be supported by all CPE.)

Rate Adaptation Upshift Margin DownStream (RAUMDS): Applies only when dynamic rate adaptation is specified. Specifies the noise margin in decibels (dB) that triggers an increase in the downstream data rate. For the increase to occur, the noise margin must stay above this value for the time specified in Rate Adaptation Upshift Time DownStream (RAUTDS). The range of values is 0 to 31 dB. RAUMDS must be greater than RADMDS.

Rate Adaptation Downshift Margin DownStream (RADMDS): Applies only when dynamic rate adaptation is specified. Specifies the noise margin in decibels (dB) that triggers a decrease in the downstream data rate. For the decrease to occur, the noise margin must stay below this value for the time specified in Rate Adaptation Downshift Time DownStream (RAUTDS). The range of values is 0 to 31 dB. RAUMDS must be greater than RADMDS.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Rate Adaptation Upshift Time Downstream (RAUTDS): Applies only when dynamic rate adaptation is specified. Specifies the duration in seconds that the downstream noise margin must stay above the Rate Adaptation Upshift Margin Downstream (RAUMDS) before the modem increases the downstream data rate. The valid range is 0 to 16383 seconds. 0 disables the feature.

Rate Adaptation Downshift Time Downstream (RADTDS): Applies only when dynamic rate adaptation is specified. Specifies the duration in seconds that the downstream noise margin must stay below the Rate Adaptation Downshift Margin Downstream (RADMDS) before the modem decreases the downstream data rate. The valid range is 0 to 16383 seconds. 0 disables the feature.

Rate Adaptation MODE UpStream (RAMODEUS): Specifies the rate adaptation mode upstream. There are two values:

- **Init** – The rate remains at its initial rate upon train-up and does not change.
- **Dynamic** – The rate is allowed to change automatically in response to changes in the noise level. (Note that this may not be supported by all CPE.)

Rate Adaptation Upshift Margin UpStream (RAUMUS): Applies only when dynamic rate adaptation is specified. RAUMUS must be greater than RADMUS. The default value is 9 dB.

Rate Adaptation Downshift Margin UpStream (RADMUS): Applies only when dynamic rate adaptation is specified. RAUMDS must be greater than RADMDS. The default value is 3 dB.

Rate Adaptation Upshift Time UpStream (RAUTUS): Applies only when dynamic rate adaptation is specified. Specifies the number of seconds for rate adaptation upshift. The default value is 30.

Rate Adaptation Downshift Time UpStream (RADTUS): Applies only when dynamic rate adaptation is specified. Specifies the number of seconds for rate adaptation downshift. The default value is 30.

The start and end tones parameters below, also known as start and end bins, can only be set using an xDSL template and define the low and high ranges of frequency bands used for the upstream and downstream signals. When high-power long-distance signals are carried in the same binder group as low-power short-distance signals, crosstalk can occur between the signals. To prevent crosstalk in some situations, you can specify start and end tones that define different frequency bands for different signals. The default value for start and end tones, 0, means the feature is disabled.

UpStream Start Tone (US0ST): Specifies the upstream start tone index. US0ST must be less than or equal to US0ET. See *ADSL Tone Configurations* (on page 473) for valid ranges. The default value is 0.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

UpStream End Tone (US0ET): Specifies the upstream end tone index. US0ET must be greater than or equal to US0ST. See *ADSL Tone Configurations* (on page 473) for valid ranges. The default value is 0.

DownStream Start Tone (DS1ST): Specifies the downstream start tone index. DS1ST must be less than or equal to DS1ET. See *ADSL Tone Configurations* (on page 473) for valid ranges. The default value is 0.

DownStream End Tone (DS1ET): Specifies the downstream end tone index. DS1T must be greater than or equal to DS1ST. See *ADSL Tone Configurations* (on page 473) for valid ranges. The default value is 0.

ATM Header Compression (AHC): If set to **Y** (Yes), ATM header compression is implemented, leaving more bits available for data. (Applicable to xDSL ports on ADSL2-24A, COMBO2-24A, and VDSL2-based cards.)

Note: On ADSL2-24A and COMBO2-24A cards, an increase in the downstream data rate is only realized with this feature if Conexant-based CPE also implements ATM header compression.

VDSL2-based cards only support ATM header compression with Broadcom-based CPEs.

Power Spectral Density (PSD) parameters (xDSL ports on VDSL cards only)

Upstream 0 PSD Mask (US0PSD): The upstream 0 PSD mask to be allowed by the near-end xTU on the line. The default setting is Eu64.

Notch 1 - Notch 4 Start (VNSTART1 - VNSTART4): Specifies the start frequencies (in KHz) for PSD shaping notches 1 to 4. The default value is 0 (do not use).

Notch 1 - Notch 4 Stop (VNSTOP1 - VNSTOP4): Specifies the stop frequencies (in KHz) for PSD shaping notches 1 to 4. The default value is 0 (do not use).

RFI 1 - RFI 4 Start (VRSTART1 - VRSTART4): Specifies the start frequencies (in KHz) for RFI notches 1 to 4. The default value is 0 (do not use).

RFI 1 - RFI 4 Stop (VRSTOP1 - VRSTOP4): Specifies the stop frequencies (in KHz) for RFI notches 1 to 4. The default value is 0 (do not use).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

ONT Profile Parameters

The system provides a complete set of pre-defined Calix 700 ONT profiles. The ONT profiles define the total number of each type of port on an ONT.

Note: Calix 700 ONT profiles are system defined and cannot be deleted or edited.

The matrix below displays the feature, the model affected, and the number of ports per ONT for each feature:

ONT MATRIX	710GX	711GX	712GX	714GX	720GX	721GX	722GX	724GX	725GX	711GE	716GE	716GE-I	717GE	721GE	725GE	726GE	726GE-I	727GE	742GE	743GE	744GE	760GX	762GX	763GX	766GX	767GX	740G	765G
POTS Ports	2	2	2	4	2	2	2	4	2	2	2	2	4	2	2	2	2	4	2	2	2	8	8	8	8	8	2	8
10/100/1000 Optical Ethernet																			2	2								
10/100/1000 Ethernet	1	1	1	1	1	1	1	1	1	2	2	4	2	2	2	2	4	2			2	4	8	8	4	4	1	4
10/100 Ethernet		1		1		1	1	1	1					1	1	1		1									1	
RF Video					1	1	1	1	1					1	1	1	1	1				4	4	8	4	4	1	4
High Power RF Video																						1	1		1			1
T1 Ports (G.824)																				2	2				8	8	2	4
E1 Ports (G.823)																				2	2				8	8		
700 Encl. & 761	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙		⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙						⊙	
760 Encl. & MDU6-I																						⊙	⊙	⊙	⊙			⊙
Rack Mount Option																								⊙	⊙	⊙		⊙
HPNA			⊙				⊙																					
1610nm RF Return									⊙						⊙									⊙		⊙		
TDM POTS	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙													⊙	⊙	⊙	⊙	⊙	⊙	⊙
VoIP POTS	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙
TDM T1																									⊙	⊙	⊙	⊙
PWE3 T1																				⊙	⊙					⊙	⊙	
BPON	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙																		⊙	
1.2G GPON	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙																		⊙	
2.5G GPON	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙
Active Ethernet	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙
1 GHZ RF					⊙	⊙	⊙	⊙	⊙					⊙	⊙	⊙		⊙				⊙	⊙	⊙	⊙	⊙	⊙	⊙
Home Gateway										⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙										
TDM C7 GPON	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙													⊙	⊙	⊙	⊙	⊙	⊙	⊙
TDM F5/FD GPON	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙																		⊙	
All IP E7 GPON	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙		
All IP C7 GPON	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙		
All IP F5/FD GPON	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙		⊙	⊙		⊙		⊙										
6158	Updated 10/24 /2012																											

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Global ONT profile parameters

Parameter	Description
Profile Identifier (OntProfAid)	Optical Network Termination Profile Access Identifier. Valid parameters are integers from 1 to 20.
Vendor ID (VENDOR)	The vendor identifier for the ONT using this profile. A valid value is a string of 4 characters assigned to the ONT vendor. The vendor ID is case sensitive.
Description (DESC)	A user-defined description field for this profile. A valid value is a string up to 31 characters long. The default value is the template address/index number.
Number of POTS ports (NUMPOTS)	Specifies the number of POTS ports supported on the ONT. Valid parameters are integers from 0 to 24. The default value is 4.
Number of DS1 ports (NUMDS1)	Specifies the number of DS1 ports supported on the ONT. Valid parameters are integers from 0 to 12. The default value is 0.
Number of Ethernet ports (NUMETH)	Specifies the number of Ethernet ports supported on the ONT. Valid parameters are integers from 0 to 12. The default value is 1.
Number of Gigabit Ethernet ports	Specifies the number of Gigabit Ethernet ports supported on the ONT. Valid parameters are integers from 0 to 12. The default value is 1.
Number of RF Video ports (NUMRFVID)	Specifies the number of RF Video (COAX) output ports supported on the ONT. Valid parameters are 0 through 12. The default value is 1.
Number of HPNA ports (NUMHPNA)	Specifies the number of HPNA output ports supported on the ONT. Valid parameters are 0 to 16. The default value is 1.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configure a Data Communication Channel

After you connect a network, the C7 system uses the data communication channel (DCC) to automatically discover the relationship between all C7 shelves. The data communication channel exists between shelves in a node and between nodes in a network.

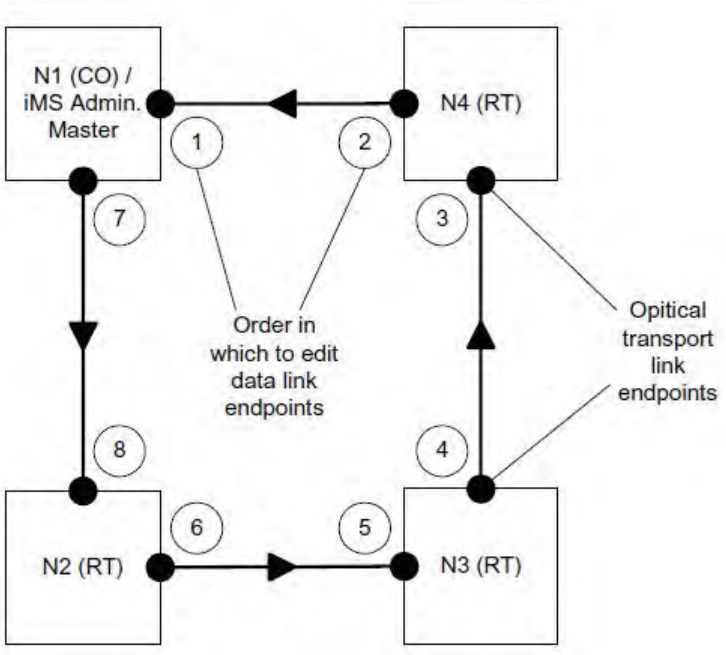
Typically a C7 network operates with line data communication channel (LDCC) links that use the line overhead in the SONET frame for the DCC, and is the default setting for C7 shelves. When a C7 network is connected to a third-party fiber ring, the DCC might need to be set to one of the following:

- SDCC that uses the section overhead in the SONET frame for data communications.
- ICC that uses the payload of a virtual channel for data communications.

Changing the DCC to ICC

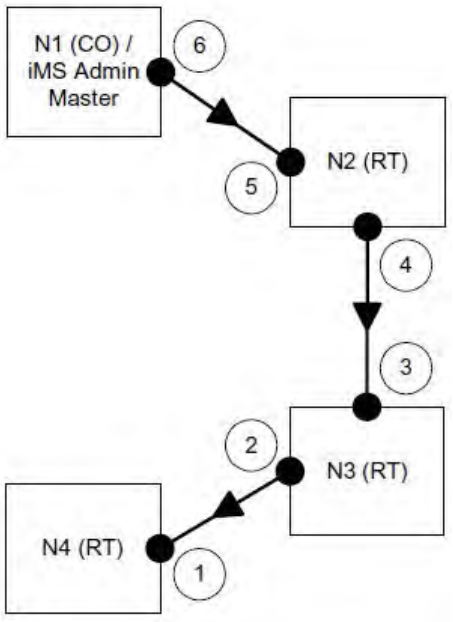
To use ICC as the link type, an STS path acts as the virtual channel (ICCVC).

Use the following diagrams to determine the order in which to change links to ICC.



Order for editing optical transport link endpoints to ICC in a four-node UPSR (ring) topology

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.



Order for editing optical transport link endpoints to ICC in a four-node linear chain topology

To change the path of the data communication link

1. On the Navigation Tree, click the C7 Network level.
2. In the Work Area, click **Data Links** > **Link Endpoints** to display the list of data communication channel link endpoints.
3. Click a transport link endpoint to edit.

   Note: Calix recommends that you edit data link endpoints one at a time. For ICC links, refer to the diagrams above to determine the edit order.

4. In the edit row, under Link Type, select a type of data communication channel (**LDCC**, **SDCC**, or **ICC**) from the list.
5. (For ICC links) In the edit row, select the STS to use for the ICCVC and optionally specify a VP and VC to use. If you do not specify the VP and VC, the defaults VP 0 and VC 24 are used.

   Note: Both link endpoints for each data link must use the same VPI/VCI.

6. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save the configuration.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Note for ICC links: In protected systems, a minor COMLNKDOWN alarm displays until both endpoints in a data link have been changed to ICC and the link is established. For unprotected point-to-point links, a non-service affecting loss of communication with the shelf or node occurs until both endpoints are changed. If you have just edited the second endpoint in the data link, wait until the COMLNKDOWN alarm clears or the shelf communication is established before editing the next endpoint. If an alarm persists, contact Calix Technical Support for assistance.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

SONET DCC Tunneling

The SONET standard includes four embedded in-fiber, out-of-band, Data Communications Channels (DCCs) as part of its fundamental overhead. DCCs can be used for communicating alarm, event, and configuration messages between C7 or third-party network elements, or between C7 or third-party network elements and Calix or third-party management systems.

There is one channel of Section DCC (SDCC) bytes, and three channels of Line DCC (LDCC) bytes. SDCC channels have the three bytes, D1 to D3, in the section overhead. LDCC channels have nine bytes, D4 to D12, in the line overhead that are collectively known as LDCC.

The nine byte LDCC may also be considered as three triplets, as follows:

- CC3D4 through D6 – LDCC1
- D7 through D9 – LDCC2
- D10 through D12 – LDCC3

DCC tunneling is a method for transporting SONET signaling information from one SONET port facility to another. Tunnels are created automatically when you create a DCC cross-connect. All additional DCC cross-connects between the same two OCn ports use the same tunnel. Cross-connects between different OCn ports use different tunnels.

Tunneling allows transport of third-party equipment signaling bytes from one side of a C7 network to another. With tunneling, the third-party equipment can transparently communicate through the C7 network. The C7 has no knowledge of the data carried by the DCC bytes, and changes no behavior because of it.

You can tunnel any DCC triplet (SDCC, LDCC1, LDCC2 and LDCC3) to any other triplet. For example:

- SDCC to SDCC
- SDCC to LDCC1
- LDCC2 to SDCC

DCC Tunnel Considerations

SONET DCC tunnels on a C7 shelf have the following restrictions:

- 2 tunnels per RAP-OCn card
- 4 tunnels per OCn card

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

End-to-End with the VIA Parameter

When creating an end-to-end DCC triplet connection, you can supply an optional VIA parameter. The VIA parameter allows the triplet data to tunnel from one network element to another using a different triplet in the intermediate network elements. For example, you can tunnel SDCC from one network element to another, but use LDCC1 in the intermediate network elements.

The VIA parameter only applies to multi-shelf connections. When cross-connecting within a single shelf, do not use this parameter.

Protection

DCC tunnel connections may be protected if the facility is part of a Link Access Procedure (LAPS) protection scheme using the DCC tunnel data from the active LAPS facility.

Note: The SDCC cross connects can only be built as unprotected.

Data Links

You can use section DCC or line DCC for C7 inter-shelf communication. To determine if the section or line DCC is already being used for inter-shelf communication, view the C7 working data link properties.

To view C7 working data link properties

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Data Links** > **Working Links** to display all data communications channels in the Work Area.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Creating DCC Tunnels

You can create a DCC tunnel from existing data cross-connects between optical cards. By default, the internal C7 to C7 cross-connects use LDCC. Cross-connects to third-party equipment typically use SDCC. You can use LDCC for cross-connects to third-party equipment by changing the internal cross-connects to SDCC.

Note: The SDCC cross connects can only be built as unprotected.

To create a DCC tunnel

1. On the Navigation Tree, expand the optical transport cards to view the OC ports.
2. Use Ctrl+click to select the ports.
3. In the Work Area, click **Cross Connect** to view the DCC Work Area.
4. On the toolbar, click **Create** to open the Select Cross-Connect Endpoints dialog box.
5. In the Source area, select the DCC endpoints:
   a. In the Shelf list, select the shelf containing the DCC endpoint.
   b. In the Type list, select the optical card.
   c. In the list of ports, select all of the ports to cross connect.
6. Click **SRC**.
7. In the Destination area, select the DCC endpoints:
   a. In the Shelf list, select the shelf containing the DCC endpoint.
   b. In the Type list, select the optical card.
   c. In the list of ports, select all of the ports to cross-connect.
8. Click **DEST**.
9. In the Required Parameters area:
   a. In the Cross-Connect Path list, select the path type for the cross-connection. For end-to-end cross-connections, Working and Protect (WORK + PROT) and Unprotected (UNPROT) are valid options. For a cross-connection hop, Working Only (WORK ONLY), Protection Only (PROT ONLY), and Unprotected (UNPROT) are valid options.
   b. In the Channel via which DCC Cross Connects are Set Up list, select the type of DCC.
10. Click **OK** to create the cross-connect.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Modifying a Cross-Connect Type

To modify the C7 data link on a shelf you are directly connected to, first modify the remote endpoint. Then modify the local endpoint. When both endpoints reside on other shelves, you can modify either endpoint first.

Note: Modifying the DCC type raises a COMMSLINKDOWN alarm that clears when both endpoints in the data link are changed and the link is established.

ALERT! This procedure is a service-affecting operation.

To modify a cross-connect type

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Data Links** > **Link Endpoints** to display all link endpoints.
3. Click the **All Link Endpoints** radio button to display all link endpoints or click the **Only Non-Communicating Link Endpoints** radio button to display only the non-communicating link endpoints.
4. Click the endpoint to modify.
5. From the Link Type list, select the DCC type to change.
6. Click the other endpoint of the cross-connect.
7. From the Link Type list, select the DCC type to change.
8. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save the changes.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Viewing and Printing Alarms, Events, and Logs

Viewing Alarms

In the Alarm Table, you can do the following:

- View all alarms and events.
- View a list of alarms filtered by network topology (network, node, or shelf) or a Selection Filter category.
- Customize the display of alarms and events.
- Generate a list of alarms or events for viewing or printing in HTML and CSV formats.
- Display an Alarm Details dialog box, where you can view help information on most alarms displayed in the Alarm Table.

Options for viewing alarms

Using the Navigation Tree and the Selection Filter, you can narrow the list of alarms that appear in the Alarm Table.

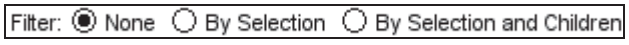
Option	Details
Use the Navigation Tree	View alarms for a selected level on the Navigation Tree. For example, display the alarms for a network, node, or shelf.
Use the Selection Filter	Access the Selection Filter at the network level or below on the Navigation Tree. View alarms specific to one of the available filters. For example, display alarms relating to a port type or an interface group.

View a Filtered Alarm List (C7 only)

By default, all standing alarms appear in the Alarm Table. Use this procedure to display specific C7 alarms based on network topology and selection criteria that you choose.

To view a filtered alarm list

1. On the Navigation Tree, click the level to filter alarms.
2. Below the Alarm Table select one of the following:



   - **None** to display no alarms for the system.
   - **By Selection** to display only those alarms on the Navigation Tree level selected in Step 1.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- **By Selection and Children** to display alarms on the selected Navigation Tree level and all subordinate levels.

3. (Optional) On the Navigation Tree, apply a filter criterion:

a. Below the Navigation Tree, click the label to the right of **filter.**

b. Select a category (for example, Equipment), and then if applicable, a subcategory.

Other Viewing Options

You can also use the display panel on the C7 fan tray to view and troubleshoot alarms. For more information, see the *Calix C7 Troubleshooting Guide* and the *Calix C7 Maintenance Guide*.

Viewing Events

In the Events and Threshold Events tabs in the Alarm Table, you can view the most recent C7 non-alarm events and conditions, including threshold crossing events. Threshold crossing events are performance statistics that exceed defined threshold settings.

You can view the 300 most recent events and threshold crossings. For older information, you can query the logs of historical events in CMS Web.

What you can view

In the Events and Threshold Events tabs in the Alarm Table, the following information appears:

Event Parameter	Description
Network (C7 only)	Network name
ID	Network address (for example, N1-1-2-4) where the event or threshold crossing occurred
Facility	Type of facility (for example, ADSL port) that was affected
Location	For applicable parameters, indication of whether the event occurred at the near or far end

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Event Parameter	Description
Event	Type of event
Description	Description of the event parameter (for example, Loss of Signal)
Effect	Effect of the threshold violation on the system: CL = Cleared; SC = Standing Condition; TC = Transient Condition.
Date and Time	Beginning date and time for the event or performance monitoring period
Monitored Value	Current value of the parameter for threshold crossing events
Threshold Value	Outer limit value(s) for the parameter for threshold crossing events
Time Period	Interval for threshold crossing data: 15-Minute Interval or 1-Day for threshold crossing events. **Note:** Time periods for 1-day parameters begin and end at midnight.

To view events

1. In the Alarm Table, do one of the following:
   - Click **Events** to view non-alarm events and conditions.
   - Click **Threshold Events** to view threshold crossing events.
2. (Optional) In the Maximum Rows list, click the maximum number of rows of data to view. Options are 50 (default), 100, 200, or 300.

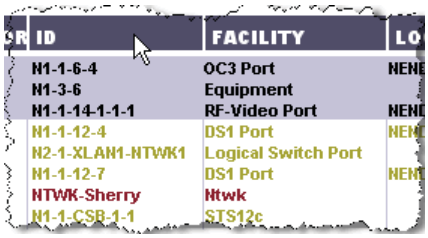
Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Alarm and Event Display Options

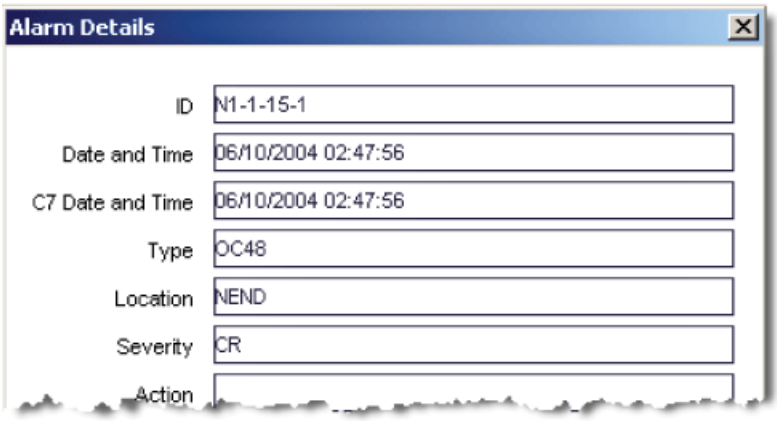
You can customize the lists of network alarms and events in the Alarm Table, as well as the C7 logs.

Options for displaying alarms

The table below describes the options for viewing and customizing the appearance of alarms, events, and logs.

Option	Details
Perform a quick sort by a column	 Click a column heading. For example, to sort by access identifier, click the ID heading.
Customize the appearance or generate a report	Choose the information to display or use a sort or group command to display entries by a field that you choose. Right-click a column heading to open a popup menu with the following options: **Sort Ascending (Descending):** Sort the entries by a column heading that you select. **Group By This Field:** Group the entries by a column heading that you select. **Show All Options:** Open a dialog box with options for customizing the display. **Print Report:** Generate an HTML or CSV report for viewing or printing. **Restore Defaults:** Return to the factory-set display defaults.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Option	Details
View details of an alarm	 In the Alarm Table, click an alarm row, and then click **Details** to open a summary of the alarm. The Alarm Details dialog box provides alarm information, including online help, about a single alarm. **Note:** In CMS, corrective actions for supported non-Calix devices are not displayed in the Alarm Details window. For troubleshooting steps, refer to the device-specific documentation.

Viewing Logs

There are five history logs provided for each C7 shelf:

- Alarm Logs
- Event Logs
- Threshold Crossing Logs
- Security Logs
- DBChange Logs

Use the Logs feature in the C7 to view and print alarm and event logs, security logs, and database change logs. You can create customized reports by specifying your own report start date and adjusting the report display.

Logs include histories of alarm and event notifications for all equipment and facilities, service state changes, protection switchovers, threshold crossing events, remove and restore events, security events (such as login attempts and user changes), and database change notifications.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Resetting History Logs

The Alarm Log can store a maximum of 500 entries. The Event, Threshold Crossing, Security and DBChange Logs can each store a maximum of 300 entries. All counts are on a per-shelf basis. The oldest entries are discarded first when the log is full—FIFO. With the exception of the Security Logs, the history logs can be individually reset.

If a log is full and the system discards the oldest entries, a message is displayed in the Condition Status box of the Shelf panel (Work Area, Shelf View). This is an informational message and does not require any action.

The procedure below describes how to reset History Logs.

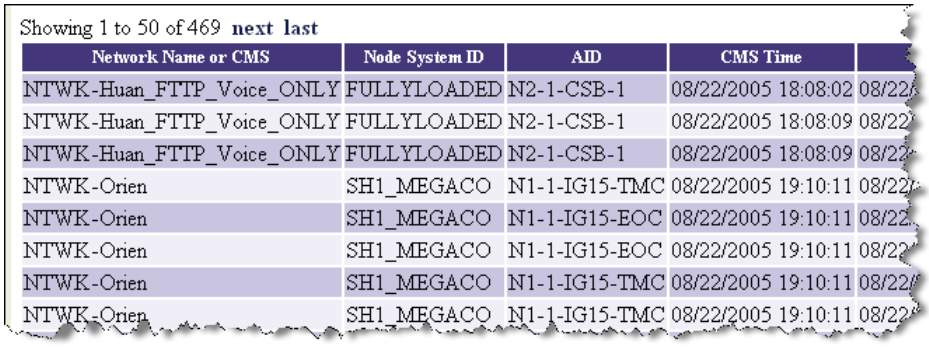
Note: If you reset the logs from the Network level, the selected log type is reset for every C7 shelf in the network. A record of any log reset is stored in the respective log.

To reset History Logs

1. On the Navigation Tree, click the Shelf or Network level.
2. In the Work Area, click the **Logs** tab, and then click the appropriate History Log sub-tab (Alarm Logs, Event Logs, Threshold Crossing Logs, Security Logs, or DBChange Logs).
3. From the toolbar, click **Action** > **Reset Logs**.
4. In the message dialog box, click **OK**.

Generating Custom Print Reports

You can generate and print a report of the standing alarms, non-alarm events and conditions, or threshold crossing events listed in the Alarm Table, as well as C7 network logs.


Showing 1 to 50 of 469 next last

Network Name or CMS	Node System ID	AID	CMS Time	
NTWK-Huan_FTTP_Voice_ONLY	FULLYLOADED	N2-1-CSB-1	08/22/2005 18:08:02	08/22/
NTWK-Huan_FTTP_Voice_ONLY	FULLYLOADED	N2-1-CSB-1	08/22/2005 18:08:09	08/22
NTWK-Huan_FTTP_Voice_ONLY	FULLYLOADED	N2-1-CSB-1	08/22/2005 18:08:09	08/22
NTWK-Orien	SH1_MEGACO	N1-1-IG15-TMC	08/22/2005 19:10:11	08/22/
NTWK-Orien	SH1_MEGACO	N1-1-IG15-EOC	08/22/2005 19:10:11	08/22
NTWK-Orien	SH1_MEGACO	N1-1-IG15-EOC	08/22/2005 19:10:11	08/22
NTWK-Orien	SH1_MEGACO	N1-1-IG15-TMC	08/22/2005 19:10:11	08/22/
NTWK-Orien	SH1_MEGACO	N1-1-IG15-TMC	08/22/2005 19:10:11	08/22

Before generating a print report, format the Alarm Table entries for printing using the available display options.

Tip: Hovering the mouse pointer over a column header opens a pop-up window with a more complete description of the column contents.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Report format options

The CMS provides two format options for generating and printing reports: HTML and CSV (comma delimited).

- With **HTML** format (default), a new browser window opens with the report contents. Use the commands on the browser File menu to save or print the report.
- For **CSV** format, you can open or save the report file on your PC, and then use your default spreadsheet application features to format and print the report.

Tip: Spreadsheet applications may reformat the imported report content based on auto-recognized formats, making the information unrecognizable. To avoid this problem, apply a text-only format to the imported data.

To generate an alarm report

1. (Optional) To include only specific entries in the report, use Ctrl+click to select entries one at a time, or Shift+click to select a range of entries.
2. Right-click anywhere in the heading row to open a pop-up menu, and then click **Print Report**.
3. In the Report Options dialog box, do the following:
   a. (Optional) By default, a generic report title appears. In the **Report Title** box, type a name for the report.
   b. In the Report On area, by default the **All Entries** option is selected. If you selected specific items in Step 1, click **Selected Entries**.
   c. To generate an HTML report:
      - In the Format area, click **HTML Report**
      - At the bottom of the dialog box, click **View** to open the report window.
   d. To generate a comma delimited report
      - In the Format area, click **CSV Report**.
      - At the bottom of the dialog box, click **View** to open the report using your default spreadsheet application, or **Save** to save the file on your local drive and later import the file into a spreadsheet application such as Excel.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Working with System Cross-Connections

Cross-Connect Viewing Options

When you create a cross-connection, the C7 creates the required number of hops, or logical connections, on the shelves within the network. A path is defined from a source endpoint to a destination endpoint. For a protected cross-connect, the C7 creates a working path and a protect path.

Features for Viewing Cross-Connects

The default view of cross-connects in the system is end-to-end; cross-connects on the selected level of the Navigation Tree are listed showing only the source and destination endpoints, not all of the hops in between. Alternatively, you can view all hops along cross-connect paths in a hop-by-hop view. The system includes several options for viewing cross-connects and hops:

- At the card, port, or path level on the Navigation Tree, you can view and print a list of end-to-end cross-connects.
- At any level on the Navigation Tree, you can view and print a list of end-to-end or hops for a specific cross-connect category.
- You can view multiple cross-connects or hops together in table view or one-by-one in form view. If a single cross-connect is provisioned at the location you are viewing, it automatically appears in form view.
- For a single cross-connect, you can view the associated hops and for ATM cross-connects performance monitoring information.

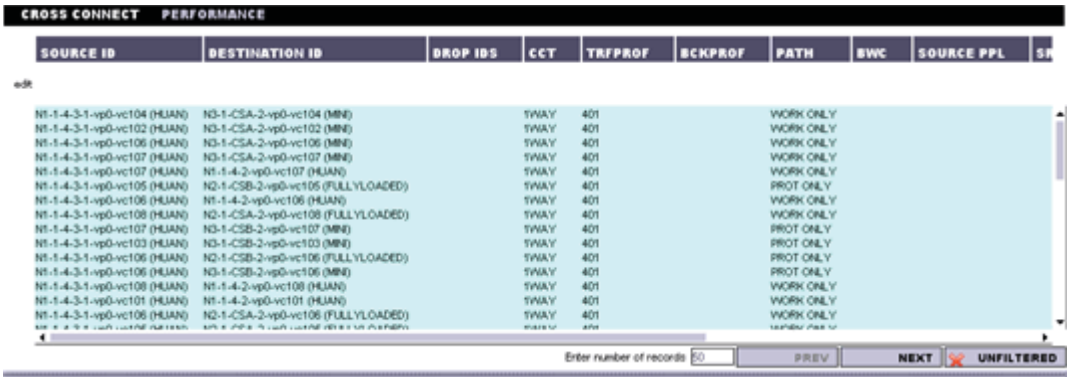
Video Cross-Connects

Video cross-connects are color-coded with a blue background except when viewed at the IRC card level on the Navigation Tree. For more information about video cross-connects, see the *Calix C7 Video Services Guide*.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

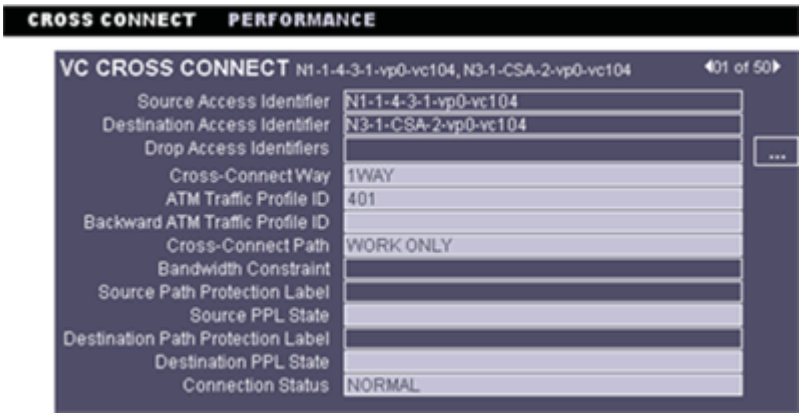
Table View and Form View

In table view, the source and destination IDs and other cross-connect parameters appear in a list format.



By default, 50 items are displayed per screen. If more than 50 cross-connects are provisioned at the location you are viewing, use the **Next** and **Prev** buttons to view the list. You can also modify the number of cross-connects to display on a screen. To do so, in the Enter Number of Records box, type the number of cross-connects to view per screen, and then click **Refresh**.

In form view, the cross-connect information appears for a single cross-connect. When you view multiple cross-connects in form view, use the arrows in the top right corner to move forward or backward one record at a time.



Cross-connection parameters differ depending on the type of service being carried. For information about specific parameters, see the individual service sections in this guide.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

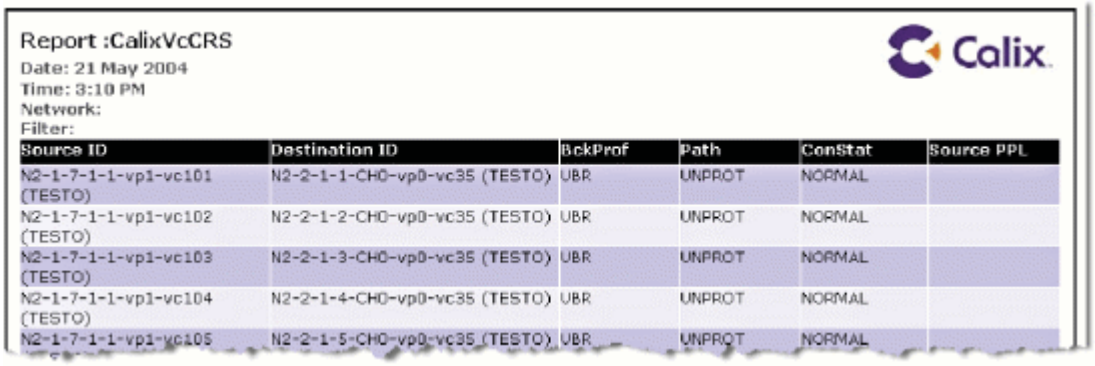
Cross-Connect Display Options

In table view, you can change the display format for a list of cross-connects. To do so, right-click in a column heading to open a display menu with the following options:

- **Sort Ascending (Descending):** Sorts the list by the selected field.
- **Group By This Field (Ungroup):** Groups the list by the selected field. In the cross-connect list, use the expand and collapse buttons to view or hide grouped entries.
- **Show All Options:** Opens the Options dialog box, where you can set the default sort order, choose the columns to display, and change the column order and width.
- **Print Report:** Prints the list you are viewing.
- **Switch to Form:** Switches to form view.
- **Restore Defaults:** Reverts to default display settings.

Cross-Connect Print Report

You can generate an HTML report of the cross-connects that you are viewing by selecting the **Print Report** option.



Report :CalixVcCRS

Date: 21 May 2004
Time: 3:10 PM
Network:
Filter:

Source ID	Destination ID	BckProf	Path	ConStat	Source PPL
N2-1-7-1-1-vp1-vc101 (TESTO)	N2-2-1-1-CHO-vp0-vc35 (TESTO)	UBR	UNPROT	NORMAL	
N2-1-7-1-1-vp1-vc102 (TESTO)	N2-2-1-2-CHO-vp0-vc35 (TESTO)	UBR	UNPROT	NORMAL	
N2-1-7-1-1-vp1-vc103 (TESTO)	N2-2-1-3-CHO-vp0-vc35 (TESTO)	UBR	UNPROT	NORMAL	
N2-1-7-1-1-vp1-vc104 (TESTO)	N2-2-1-4-CHO-vp0-vc35 (TESTO)	UBR	UNPROT	NORMAL	
N2-1-7-1-1-vp1-vc105	N2-2-1-5-CHO-vp0-vc35 (TESTO)	UBR	UNPROT	NORMAL	

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

View a List of Cross-Connections and Hops

Note: To view cross-connects at the optical card level, you must click a port or path.

To view end-to-end cross-connects at the card, port, or path level

At the card, port, or path level on the Navigation Tree, you can view end-to-end cross-connections. For a description of display options, see Display options.

1. On the Navigation Tree, click the level to view cross-connects.
2. In the Work Area, click **Cross Connect**.

   At the xDSL, DS1, or T1 port level, or at the STS path or pseudo port (PP) level on an optical card, click a cross-connect category tab.

   At the DS1, T1, or HDSL port level, you can also click **Timeslot Cross Connect** to view timeslot cross-connects.

To view a category of end-to-end cross-connects or hops

At any level on the Navigation Tree, you can view a category of end-to-end or hop-by-hop cross-connections using the Selection Filter. For a description of display options, see Display options.

1. On the Navigation Tree, click the level to view cross-connects.
2. Below the Navigation Tree, click to the right of the **filter**, and then do one of the following:
   - Click **Cross-Connect** and select a cross-connect category.
   - Click **Hop-by-Hop Cross-Connect** and select a cross-connect category.

   The selected list is displayed in the Work Area.

To view hops for a single cross-connect

This procedure assumes that you are viewing a list of cross-connects or hops. For a description of display options, see *Cross-connect viewing options* (on page 124).

1. In the cross-connect or hop list, select a single item.
2. On the toolbar, click **Action** > **End-to-End Cross-Connect Detail View** to open the End-to-End Cross-Connect Detail dialog box.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Work with VP Cross-Connects

Use VP cross-connects to enable Virtual Path switching, typically to aggregate ATM traffic from external or subtended devices, or from another C7 network.

You can create VP cross-connections between external ATM interface ports only, including STS facilities, IMA groups, DS3p, T1, or xDSL ports.

Overview of VP Cross-Connection Parameters

The parameters listed below define the characteristics of a virtual path connection. For existing VP cross-connections, you can view these in the Provisioning Work Area. The abbreviated name shown in parentheses represents the parameter ID in the Provisioning table view when multiple cross-connects are selected.

Source Virtual Path Identifier (SOURCE ID)

Specifies the address of the source endpoint of the virtual path connection. See VP Access Identifier below.

Destination Virtual Path Identifier (DESTINATION ID)

Specifies the address of the destination endpoint of the virtual path connection. See VP Access Identifier below.

Drop Access Identifiers (DROP IDS)

Specifies the location in the cross-connection where traffic is dropped along the path to the endpoint. This parameter pertains to drop-and-continue applications.

VP Access Identifier

The VP Access Identifier (AID) pertains to the SOURCE ID, DESTINATION ID, and DROP IDS parameters. These addresses read from left to right, depending on the facility type:

On an IMA group: **`NODE-SHELF-SLOT-IMA-VP`**

On a DS3-12p card, or VC in a DS1-12, T1-6, T1-6 A+T, or HDSL card: **`NODE-SHELF-SLOT-PORT-VP`**

On an xDSL channel: **`NODE-SHELF-SLOT-PORT-CH-VP`**

On an STS facility: **`NODE-SHELF-SLOT-PORT-STS-VP`**

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Parameter	Description
NODE	A number from 1 through 255. This number specifies the address of the C7 node in the network.
SHELF	A number from 1 through 5. This number specifies the address of the C7 shelf on the node.
SLOT	CSA, CSB or a number from 1 through 20. This number specifies the slot on the C7 shelf where the card resides.
PORT or IMA	This number specifies the port or IMA group: • For an IMA group, a number from 1 through 16 • For T3p or T1, a number from 1 through 12 • For an xDSL channel, a number from 1 through 24 • For an STS port: a number from 1 through 4 (OC card), or CSA or CSB (RAP-OC card)
CH or STS (xDSL channel or STS facility only)	This number specifies: • One of two logical channels (0 or 1) within a DSL port, or • The STS ID (from 1 through 48)
VP	A number that specifies the virtual path identifier (VPI). The valid range is a number from 1 through 4090. **Note:** VPIs 4000 through 4090 are typically assigned to a VP pool for end-to-end protected VP cross-connects. These VPIs are automatically used by the system when you create a VP cross-connect with a WORK + PROT path (see the PATH parameter below). To view or change the Protected VP Pool range used in your network, in the Navigation Tree, click the Network level, and in the Work Area, click **Information**.

Cross Connect Way (CCT)

Specifies the cross-connection as a one or two-way connection.

- **2WAY:** Traffic flows in both directions on the connection.
- **1WAY:** Traffic flows in one direction on the connection.

The default value is 2WAY.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

ATM Traffic Profile ID (TRFPROF)

Specifies which traffic profile to apply to the forward direction of a connection. Specify a system- or user-defined profile (user-defined profiles are numbered from 1 through 500) for specific class-of-service connections. The default value is UBR.

Backward ATM Traffic Profile ID (BCKPROF)

Specifies which traffic profile to apply to the backward direction of a connection. Specify a system- or user-defined profile for specific class-of-service connections.

If you do not specify a traffic profile for the backward direction when you create the cross-connection, it is treated as symmetrical and the value from the Traffic Profile parameter is used.

Cross-Connect Path (PATH)

Specifies the type of path (connection) you are creating through the network.

- **WORK ONLY:** Creates a virtual path that is the working path through the network.
- **PROT ONLY:** Creates a virtual path that is the protecting path through the network.
- **WORK + PROT:** Creates both the working and protect paths.
- **UNPROT:** Creates an unprotected connection.

Bandwidth Constraint (BWC)

Specifies the Bandwidth Constraint that is applied to this cross-connection. A user-defined bandwidth constraint is a number from 1 through 100.

Source Path Protection Label (SOURCE PPL)

Specifies the Packet Protection Label (PPL) associated with the protection path on the source endpoint, if applicable.

Source PPL State (SRC PPL STATE)

Indicates the possible trouble condition, irregularities, errors, or off-normal conditions for the source Packet Protection Label.

Destination Path Protection Label (DESTINATION PPL)

Specifies the Packet Protection Label (PPL) associated with the protection path on the destination endpoint, if applicable.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Destination PPL State (DST PPL STATE)

Indicates the possible trouble condition, irregularities, errors, or off-normal conditions for the destination Packet Protection Label.

Connection Status (CONSTAT)

Indicates the status of the connection.

Configuration Guidelines for VP Cross-Connects

Follow these guidelines when creating a VP cross-connect:

- You must create VP cross-connects between two external ATM ports only (External Interface = Y; Interface Type = UNI or NNI).
- The valid VPI range for VP cross-connects is 1 through 4090. VPIs 4000 through 4090 are assigned by default to a VP pool for end-to-end protected VP cross-connects.
- The same VPI value cannot be used more than once on the same port.
- A VP cross-connect for ATM aggregation must use a different VPI value than the VPI values used for VC cross-connects for ADSL services.

Create a VP Cross-Connection

To create a VP cross-connect

1. On the File menu, click:
   - (in iMS) **Create** > **Cross-Connect** > **VP**
   - (in CMS) **Create** > **C7** > **Cross-Connect** > **VP**
2. In the Select Cross-Connect Endpoints dialog box, Source area, define the source endpoint:
   a. In the Shelf list, select the C7 shelf where the near-end port is located.
   b. In the Type list, select **(n) VP**, where n is the near-end external facility type.
   c. In the facility list, select the near-end external port or facility.
   d. (For an ADSL port) In the ADSL Channel list, click the channel value (0 or 1) for the near-end port.
   e. In the VP box, type the VPI value for the cross-connect.
   f. (Optional) To generate the next consecutive VPI value the next time you specify an endpoint in the Source area, select the Auto-increment check box.
   g. Click **SRC** to add the endpoint to the Source column in the Cross-Connects To Be Created area.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

3. In the Destination/Drop area, define the destination endpoint:
   a. In the Shelf list, select the C7 shelf where the far-end port is located.
   b. In the Type list, select **(n) VP**, where n is the far-end external facility type.
   c. In the facility list, select the far-end external port or facility.
   d. (For an ADSL port) In the ADSL Channel list, click the channel value (0 or 1) for the far-end port.
   e. In the VP box, type the VPI value for the cross-connect.
   f. (Optional) To generate the next consecutive VPI value the next time you specify an endpoint in the Destination area, select the Auto-increment check box.
   g. Click **DEST** to add the endpoint to the Destination column in the Cross-Connects To Be Created area.
4. In the Required Parameters area:
   a. In the Cross-Connect Way list, click **2WAY** (default).
   b. In the ATM Traffic Profile ID list, select a traffic profile.
   c. (Optional) In the Backward ATM Traffic Profile ID list, select a traffic profile.
   d. In the Cross-Connect Path list, select a protection configuration.
   e. (Optional) in the Bandwidth Constraint list, select the bandwidth constraint ID to use for the cross-connection based on your site requirements.
5. Click **OK** to create the VP cross-connection.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Add Drops to STS, VP, and VC Cross-Connects

Video cross-connects

Video cross-connects are color-coded with a blue background except when viewed at the IRC card level on the Navigation Tree. For more information about video cross-connects, see the *Calix C7 Video Services Guide*.

Rules for adding drops to cross-connections

- You can only add drops to one-way STS, VP, or VC cross connections.
- You can only add a drop to a cross-connection hop. The source and destination endpoints for the hop, as well as the drop that you are adding, must all be located on the same C7 shelf.

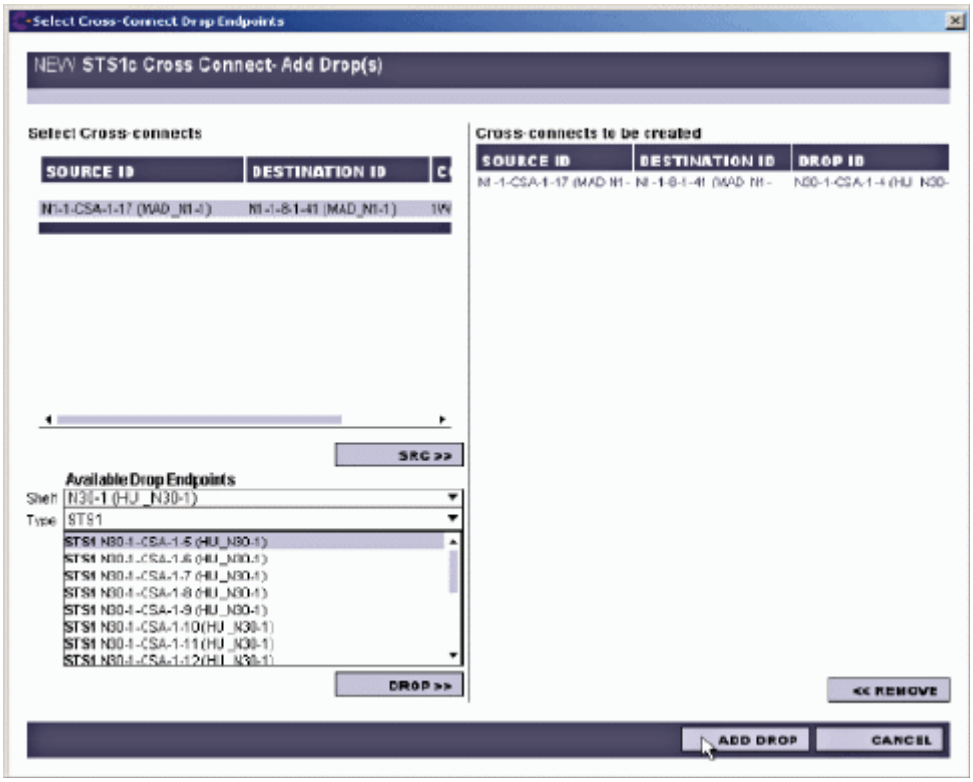
To add drops to cross-connects

1. On the Navigation Tree, click a level to view the cross-connects.
2. In the Selection Filter, click **Hop-by-Hop Cross-Connect**, and then click the cross-connection category to view.
3. In the hop list, use Ctrl+click to select one or more hops, and then click **Create** > **Add Drop(s)**.
4. In the Select Cross-Connect Drop Endpoints dialog box:
   a. In the Select Cross-Connects list, use Ctrl+click to select one or more cross-connects.
   b. Click **SRC** to move the Source and Destination IDs to the Cross-Connects To Be Created list.
   c. In the Shelf list under Available Drop Endpoints, select a shelf.
   d. In the Type list, select the type of drop that you are adding.
   e. For VP and VC cross-connects only, specify the VP and VC numbers for the drop endpoint(s). To have the system assign consecutive VC numbers for multiple drops, select the Auto-Increment check box.
   f. In the endpoint list, select available endpoints for each of the cross-connects specified in Step 4a.
   g. Click **Drop** to add the endpoints to the Cross-Connects To Be Created list.

Note: The number of rows under the Source and Destination ID columns must match the number of rows under the Drop ID column. To remove rows from the Cross-Connects To Be Created list, click the rows, and then click **Remove**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

h. Click **Add Drop**.



Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Delete Cross-Connects and Hops

You can delete end-to-end cross-connects and cross-connect hops from List View or from the End-to-End Cross-Connect dialog box.

Video cross-connects

Video cross-connects are color-coded with a blue background except when viewed at the IRC card level on the Navigation Tree. For more information about video cross-connects, see the *Calix C7 Video Services Guide*.

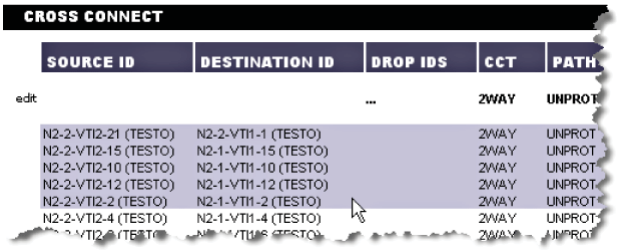
Cross-connects terminating on a virtual bridge

Use the default setting (**N**) in the VB ports parameter **Pinned** column to automatically delete associated VLAN-VB ports and VB ports when a cross-connect is deleted. If the parameter setting is (**Y**), the automatic VLAN-VB ports and VB ports deletion is prevented.

To delete cross-connects or hops

This procedure assumes that you are viewing cross-connects or hops in List View. If you are in Form View, skip Step 1.

1. In the cross-connect list, use Ctrl+click to select the cross-connects to delete.



2. Do one of the following:

   - On the toolbar, click **Delete** > **Delete Cross Connects** to use the default deletion settings.

   Note: For some cross-connects, the Delete Cross-Connect dialog box opens. Leave the Force Delete check box cleared and the Path list blank to accept the default settings.

   - On the toolbar, click **Delete** > **Advanced Delete Cross Connect** to open the Advanced Cross Connect Delete dialog box and change the deletion settings. For an explanation of the deletion features in this dialog box, see the topic below this procedure.

3. Click **OK** to confirm the deletion.

Advanced Delete dialog box

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

WARNING! Use of the settings on the Advanced Cross Connect Deletion dialog box can result in a disruption of service. Be sure that you understand the consequences of each deletion operation that you perform.

You can choose the deletion scope and method, delete an active link, and specify a path for deletion. As a general rule, use the default deletion settings. In special cases, you can use the deletion settings described below to edit or troubleshoot cross-connects.

By default the branch, or network scope, of selected end-to-end cross-connects are deleted. Select the **Delete Hop** option to delete only the first the hop in the selected cross-connects.

By default only the cross-connects or hops you have selected are deleted. Select the **Source Only** or **Destination Only** method to delete all cross-connects that have the same source (or destination) endpoint as the selected cross-connects.

By default the C7 prevents you from deleting a cross-connect with an active link. The **Forced Flag** check box enables you to perform a deletion regardless of whether the link is active.

By default all paths (working, protected, or unprotected) are deleted. You can use one of the options in the Path list to limit the deletion operation to a specific cross-connect path. For example, in conjunction with the Source Only or Destination Only method (see above), you could delete all unprotected paths from a specific port.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

To delete hops using the End-to-End dialog box

This procedure assumes that you are viewing cross-connects or hops in List View. If you are in Form View, skip Step 1.

1. Click a single item in the Work Area, and then on the toolbar, click **Action** > **End-to-End Cross-Connect Detail View** to open the End-to-End Cross-Connect Detail dialog box.
2. In the End-to-End Cross-Connect Detail dialog box, do one of the following:
   - To delete specific hops, click one or more hops in the list, and then click **Delete Hops**.
   - To delete all hops for the cross-connect, click **Delete All** to open the Delete Cross Connect dialog box. Typically you use the default deletion settings (leave the Force Delete check box cleared and the Path list blank). In special cases, you can use the Force Delete check box to delete an active link, or the Path list to specify a cross-connect path for deletion.

   Warning! Use of the Force Delete setting can result in a disruption of service. Be sure that you understand the consequences of each deletion operation that you perform.
3. In the Confirmation dialog box, click **OK** to confirm the deletion.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

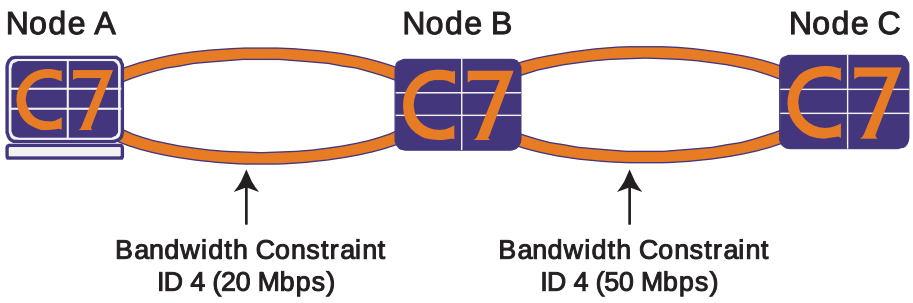
Bandwidth Reservation for Traffic Flows

Note: This topic only applies to the Multiprotocol switch fabric.

You can optimize bandwidth usage by engineering traffic flows onto different paths through a C7 network. For example, you might choose to send TDM voice traffic and data traffic in different STS paths around a network ring.

First, configure the maximum bandwidth allocated to internal transport links in the C7 by creating bandwidth constraint IDs. Then, assign the bandwidth constraint ID to transport links to define a path and set the maximum bandwidth of the path through the network.

You can assign the same bandwidth constraint ID to different links in the network provisioned with different assigned bandwidth. For example, in a network with nodes A, B, and C, you can assign 20 Mbps to bandwidth constraint ID 4 on the link from A to B, and then assign 50 Mbps to bandwidth constraint ID 4 from the link from B to C, as shown in the illustration below. In this example, node A is a remote terminal sending UBR Internet traffic to node B in a central office. Node B aggregates UBR traffic from several remote terminals, and sends it to node C in another central office.



The bandwidth constraint ID number is an identifier that defines the path through a network. The path itself does not determine the amount of bandwidth that can pass through a link in the path. The path defines the physical connections from one point to another, not the amount of traffic each section can allow.

UBR cross-connects do not require a minimum bandwidth, so it is possible to route traffic onto a link with no available bandwidth. To prevent this, you can reserve bandwidth on a link for UBR traffic by specifying a bandwidth constraint ID and assigning bandwidth to it. You can then create a UBR cross-connect specifying that bandwidth constraint ID. Applying a bandwidth constraint reserves bandwidth for the UBR connection that cannot be used by other cross-connects. This is the minimum reserved bandwidth for the UBR connection; the maximum bandwidth can exceed this, utilizing unused bandwidth on the transport link.

Note: If multiple UBR cross-connects specify the same bandwidth constraint ID, they will share the reserved minimum bandwidth. However, they will also share the maximum available bandwidth on the link.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

For example, to reserve a minimum of 100 Mbps for UBR traffic:

1. Create bandwidth constraint ID 3.
2. Create a bandwidth link and assign it 100 Mbps of bandwidth and apply bandwidth constraint ID 3.
3. Create a cross-connect between two bandwidth link endpoints with bandwidth constraint ID 3.

You cannot apply bandwidth constraints to existing cross-connects. You must delete the existing cross-connects, and create new ones with the bandwidth constraint. You can use the Bulk Reprovisioner tool for this purpose. For information, see the *Calix C7 Maintenance Guide*.

When you reserve bandwidth, you can optionally define high water marks to notify you when traffic on a link passes a defined percentage of the maximum throughput. When the bandwidth usage in a link rises above the high water mark, it triggers a standing condition to indicate high bandwidth usage.

Note: In OCn fiber ring configurations with protected traffic, you must leave bandwidth unreserved for internal system overhead. If no available unreserved bandwidth exists for system overhead, you are unable to create protected cross-connects. Depending on the size of the ring and traffic patterns, this system overhead typically requires 500 Kbps to 1 Mbps of bandwidth.

Bandwidth Constraint IDs

When creating cross-connects you can specify a bandwidth constraint ID to route traffic over a predefined path through the network. If unspecified, the system selects any available path. When you specify a bandwidth constraint ID, the connection establishes only over internal transport links using that constraint that have reserved and available bandwidth. Otherwise, the connection request fails.

For a protected cross-connect, you must specify the constraint on both the working and protection paths, and there must be sufficient reserved and available bandwidth on both paths.

If you do not specify a bandwidth constraint ID when creating the cross-connection, the C7 uses the default settings. In this case, the cross-connect bandwidth comes only from the non-reserved bandwidth pool on each link. If there is insufficient unreserved bandwidth available on a selected path, the cross-connect fails.

Each C7 network can contain up to 100 user-defined bandwidth constraint IDs. The user-defined bandwidth constraint IDs can be created, edited, or deleted as needed. The C7 has three predefined bandwidth constraint IDs, TDM, Video Subscribers (VIDSUB) and Video on Demand (VOD), which cannot be edited or deleted. Each link in the network can support up to 10 different bandwidth constraint IDs.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

You can reserve a different amount of bandwidth throughput on the same bandwidth constraint ID across different links in the network. Once defined, you can assign a bandwidth constraint ID when creating Virtual Path (VP), Virtual Channel (VC), T1, or a Video VC cross-connect. You then apply the bandwidth reservation to the cross-connected link ends or when creating new cross-connects.

You can assign bandwidth constraint IDs on internal C7 links to:

- an STS-1, STS-3c, STS-12c, or STS-48c on an optical port
- a DS3p port
- an IMA group
- a DS1 configured for NNI

TDM Bandwidth Constraint ID

The C7 comes with a predefined default TDM bandwidth constraint ID for use by TDM cross-connects. This bandwidth constraint ID is disabled by default. When enabled, all new TDM cross-connects are automatically assigned the TDM bandwidth constraint ID. All newly provisioned TDM traffic follows that defined path through the network. You assign a TDM bandwidth constraint when creating a bandwidth link.

If the TDM bandwidth constraint ID is enabled, no TDM services can be provisioned through any link that does not have the TDM bandwidth constraint ID applied, even if the link has available bandwidth. You typically use the TDM bandwidth constraint ID to engineer TDM traffic onto a different STS path through the network than an STS path carrying data traffic (such as Internet access).

Note: Once enabled, Calix does not recommend disabling the TDM bandwidth constraint while there are cross-connects using it. Doing so results in inefficient bandwidth usage.

To enable TDM bandwidth constraints

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Information** to open the Information panel.
3. In the Enable TDM BWC list, click **Y** (Yes) to enable bandwidth constraints.
4. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your changes.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

To disable TDM bandwidth constraints

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Information** to open the Information panel.
3. In the Enable TDM BWC list, click **N** (No) to disable bandwidth constraints.
4. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your changes.

Video Subscriber Constraint ID

The C7 has a predefined default Video Subscriber (VIDSUB) bandwidth constraint ID that is used by the system to reserve the current in-use video bandwidth for ADSL ports.

Note: The VIDSUB bandwidth constraint ID is for C7 system use only; do not use this constraint ID when provisioning video or other services.

Video on Demand Bandwidth Constraint ID

The C7 has a predefined default Video on Demand (VOD) bandwidth constraint ID for VOD links. You typically use the VOD bandwidth constraint ID to engineer VOD traffic in the opposite direction through a network than broadcast video traffic. You assign a VOD bandwidth constraint when creating a bandwidth link. See the *Calix C7 Video Services Guide* for information about configuring video services.

View Bandwidth Constraint IDs

Use the procedure below to view existing bandwidth constraints.

To view bandwidth constraint IDs

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Bandwidth** > **Constraints** to display all defined bandwidth constraint IDs.

Create a Bandwidth Constraint ID

Create a bandwidth constraint ID to help define a path through a C7 network.

To create a bandwidth constraint ID

1. On the File menu, click:
   - (in iMS) **Create** > **Network** > **Bandwidth** > **Bandwidth Constraint**

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- (in CMS) **Create** > **C7** > **Network** > **Bandwidth** > **Bandwidth Constraint**

2. In the Bandwidth Constraint dialog box:
   a. In the Bandwidth Constraint ID box, type the bandwidth constraint ID (an integer from 1 through 100).
   b. In the Description of Bandwidth Constraint box, type a description.
3. Click **OK** to save the bandwidth constraint ID.

Modify a Bandwidth Constraint ID

You can modify the description of a defined bandwidth constraint ID.

To modify a bandwidth constraint ID description

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Bandwidth** > **Constraints** to display all defined bandwidth constraint IDs.
3. Select a bandwidth constraint ID.
4. Edit the description as needed.
5. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save the configuration.

Delete a Bandwidth Constraint ID

You can delete bandwidth constraint IDs if they are not in use by any link in the network.

To delete bandwidth constraint ID

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Bandwidth** > **Constraints** to display all defined bandwidth constraint IDs.
3. Select a bandwidth constraint ID.
4. On the toolbar, click **Delete**. In the Confirmation dialog box, click **OK** to delete the bandwidth constraint ID.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Bandwidth Constraint Parameters

When creating a custom bandwidth constraint ID, you specify the following parameters:

- **Bandwidth Constraint Access Identifier (BwcAid):** The number that uniquely defines the bandwidth constraint to use. This ID can be applied to any optical STS path (set to NNI mapping), DS3 port, DS1 port (set to UNI or NNI mapping), or IMA port used as a transport link between C7 shelves. You can create up to 100 bandwidth constraint IDs in each C7 network. Enter a number between 1 and 100.
- **Description of Bandwidth Constraint (DESCRIPTION):** A user-defined character string of up to 31 characters. This parameter helps you track the bandwidth constraint.

When linking a bandwidth constraint ID to a transport link, you specify the following parameters:

- **Transmit Provision Limit (TXPROVLIMIT):** Bandwidth, in Kbps, reserved for the constraint on the transport link in the egress or transmit direction (A to B). When you create a bandwidth constraint link, there is no default value in this field.
- **Transmit Notification Threshold (TXTHRESHOLD):** The percent threshold at which the TXBWNTFY condition is raised. This condition indicates that bandwidth usage for the constraint in the transmit (A to B) direction exceeds the specified value. If set to OFF, no condition is raised. The default value is 95.
- **Receive Provision Limit (RXPROVLIMIT):** Bandwidth, in Kbps, reserved for the constraint on the transport link in the ingress or receive direction (B to A). The default value is 0.
- **Receive Notification Threshold (TXTHRESHOLD):** The percent threshold at which the RXBWNTFY condition is raised. This condition indicates that bandwidth usage for the constraint in the receive (B to A) direction exceeds the specified value. If set to OFF, no condition is raised. The default value is 95.

Bandwidth Links

Link Endpoints define transmit (Tx) and receive (Rx) limits and thresholds. The Link Pairs function correlates the link endpoints into pairs so you can edit both sides of the link at the same time and avoid a link property mismatch.

When reserving bandwidth for a bandwidth constraint on a link, you can specify the following parameters separately for each direction in a link (Tx and Rx):

- Maximum allowed bandwidth. The default is 0 Kbps.
- High water mark threshold, which is the threshold for reporting high bandwidth usage on the link endpoint, is specified as an integer percentage in the range 0 through 100. The default is 95 percent.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

The constraint data at the two ends (Tx and Rx) of a link should match for the same direction. If the two ends do not match, the C7 raises a Bandwidth Constraint Far-End Mismatch (BWCFEMM) alarm to indicate the mismatch. This alarm clears when the mismatch clears.

Bandwidth Limits

When the maximum allowed bandwidth is entered or edited, the new value is limited on the upper end by the unreserved and unused portion of the link bandwidth. The total combination of all reserved bandwidth and the current unreserved bandwidth in use cannot exceed the bandwidth of the link.

You can lower the bandwidth reservation to zero. However, the change does not affect current traffic. Only newly created cross-connects are subjected to the new constraints. Lowering the reservation to zero is often used when moving traffic from one path to another in a network. For example, if the bandwidth constraint carries VOD traffic and the bandwidth limit is set to zero, all new VOD flows use another route through the network. Once all VOD flows terminate, you can delete the bandwidth constraint and associations on the old link.

High Water Marks

You can set thresholds, called high water marks, to notify you when traffic on a link with reserved bandwidth exceeds a defined percentage of the maximum allowed. When the bandwidth usage in a link rises above the high water mark, it triggers a Receive Bandwidth Usage Notification (RXBWNTFY) or Transmit Bandwidth Usage Notification (TXBWNTFY) standing condition to indicate high bandwidth usage in the Threshold Events area of the Alarm Table. It is also logged in the Threshold Crossing Log. The condition clears when usage drops below the threshold.

A value of 0 means that a threshold crossing reports if any cross-connect uses this link. A value of 100 indicates that no threshold crossings are reported.

The default high water mark threshold is 95 percent of the maximum bandwidth. The threshold remains at the same percentage when the reserved bandwidth value is modified. You can modify the high water mark percentage as needed.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Create a Bandwidth Link

You can create a bandwidth link and reserve bandwidth on the link up to the maximum unreserved available bandwidth on the link. You must specify the maximum bandwidth in at least one direction when you create a new bandwidth link. Each link can have either zero or one bandwidth constraint.

If you reduce the reserved bandwidth below the current usage, a Receive Bandwidth Limit Exceeded (RXBWLMT) or Transmit Bandwidth Limit Exceeded (TXBWLMT) minor alarm raises to indicate that the bandwidth reserved is below the current usage. The alarm clears automatically when the actual usage goes below the reserved bandwidth.

Note: For bidirectional traffic, such as TDM voice, apply bandwidth link parameters on both A to B and B to A directions. For unidirectional traffic, such as VOD, configure in the A to B direction only. Typically, you configure the link to apply to both A and B endpoints.

To create a bandwidth link

1. On the File menu, click:
   - (in iMS) **Create** > **Network** > **Bandwidth** > **Bandwidth Link**
   - (in CMS) **Create** > **C7** > **Network** > **Bandwidth** > **Bandwidth Link**
2. In the Create Bandwidth Links dialog box, Source area:
   a. In the Shelf list, select a shelf containing the link endpoint.
   b. In the Type list, select the type of link.
   c. In the BWC list, select the bandwidth constraint ID to apply.
   d. Click **Add A and B** to apply the bandwidth link in two directions, or click **Add A only** to apply the bandwidth link in one direction.
   e. In the A->B ProvLimit text box, type the bandwidth limit for the A to B direction in Kbps.
   f. In the A->B Threshold text box, type the high water mark threshold for the A to B direction in percent, from 1 through 100.
   g. In the B->A ProvLimit text box, type the bandwidth limit for the B to A direction in Kbps.
   h. In the B->A Threshold text box, type the high water mark threshold for the B to A direction in percent, from 1 through 100.
3. Click **Add** to add the provisioning to the Bandwidth Links To Be Created.
4. Repeat Steps 2 and 3 as needed to create additional bandwidth links.
5. When you are done creating bandwidth links, click **OK** to create the links.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

View Bandwidth Links

You can view all existing bandwidth links in the C7 network.

To view bandwidth links

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Bandwidth** > **Link Pairs** to display all defined bandwidth links.

Modify a Bandwidth Link

You can increase the reserved bandwidth on a link up to the available unreserved capacity of the link. The total of all reserved bandwidth cannot exceed the link bandwidth.

You can also modify the high water mark (threshold) for reporting high capacity use on the bandwidth constraint from 0 to 100 percent. Modifying the reserved bandwidth also modifies the amount of traffic that triggers high water mark notification (since the high water mark is a percentage of the reserved bandwidth), but does not change the defined percentage.

For example, if you reserve 10 Mbps and set the high water mark at 90 percent, the notification triggers when traffic becomes greater than 9 Mbps (10 Mbps X 90% = 9 Mbps). If you then raise the bandwidth reservation to 20 Mbps, the high water mark notification does not trigger until traffic becomes greater than 18 Mbps (20 Mbps X 90% = 18 Mbps).

Reserved bandwidth on a link can be reduced with no restrictions. However, the change does not affect current traffic. Only newly created cross-connects are subjected to the new constraints.

Reducing reserved bandwidth on a link carrying traffic can potentially activate the high water mark trigger. For example, if a link has reserved bandwidth of 20 Mbps with a high water mark of 90 percent, and currently carries 14 Mbps of traffic, no high water mark triggers (20 Mbps X 90% = 18 Mbps). However, if the reserve bandwidth is reduced to 15 Mbps and the high water mark remains at 90 percent, the same 14 Mbps of traffic on the link triggers the high water mark notification (15 Mbps X 90% = 13.5 Mbps).

Note: When modifying bandwidth links, you should modify both link endpoints (the link pair) at the same time to avoid a mismatch of bandwidth link properties. See *Modify Link Pairs* (on page 147) for information about modifying bandwidth link pairs.

To modify bandwidth links

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Bandwidth** > **Link Endpoints** to display all defined bandwidth link endpoints.
3. Select a bandwidth link.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

4. Modify the bandwidth link properties as needed.
5. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save the configuration.

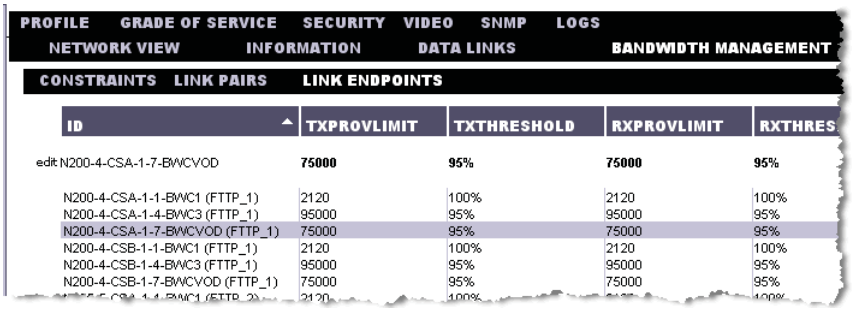
Delete a Bandwidth Link

You can delete a bandwidth link if it no traffic is reserved on it.

When you delete bandwidth links, you should delete both link endpoints (the link pair). See *Delete a Bandwidth Link Pair* (on page 148) for information about how to delete bandwidth link pairs.

To delete a bandwidth link

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Bandwidth** > **Link Endpoints** to display all defined bandwidth link endpoints.
3. Select a bandwidth link.



4. On the toolbar, click **Delete**. In the Confirmation dialog box, click **OK** to delete the link.

Modify Link Pairs

You can modify both sides of the cross-connect link at the same time to give them both the same attributes and avoid a mismatch. If the two ends are mismatched, the C7 raises a Bandwidth Constraint Far-End Mismatch (BWCFEMM) alarm to indicate the mismatch. This alarm clears when the mismatch clears.

To modify bandwidth link pairs

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Bandwidth** > **Link Pairs** to display all defined link pairs.
3. Select a link pair.
4. Edit the link pair properties as needed.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

5. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save the configuration.

Delete a Bandwidth Link Pair

You can delete a bandwidth link pair if no traffic is reserved on it.

To delete a bandwidth link pair

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Bandwidth** > **Link Pairs** to display all defined bandwidth link pairs.
3. Select a bandwidth link pair.
4. On the toolbar, click **Delete**. In the Confirmation dialog box, click **OK** to delete the link.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

AMP Routing

The AMP and ATP cards provide routing capabilities that allow you to access third-party devices—called hosts—connected to C7 shelves. AMP routing consists of two primary connectivity applications:

- Peer-to-peer (AMP-to-AMP) routing
- Multipoint routing

Peer-to-peer routing

In a peer-to-peer routing configuration, you set up a cross connection between the E3 port of the AMP or ATP card on Shelf A and a cross connection between the E3 port of the AMP or ATP card on Shelf B. You must set up the cross-connect as 2-way (2WAY) and apply an In-Band (INBANDMGT) traffic profile (at both endpoints). The AMP routing feature provides A-to-Z connection provisioning that enables you to specify the source and destination ports, and allows the system to automatically configure the circuit. Designate the E3 port in Shelf A as the endpoint cross-connect source and the E3 port in Shelf B as the destination. Designate the cross-connect path as unprotected.

See *Working with System Cross-Connections* (on page 124) for details on setting up cross connections.

After you have configured the cross-connection, static routes must be provisioned to allow traffic to pass via the AMP E3 port.

Multipoint routing

In a multipoint configuration you can access host devices connected to C7 shelves through a router connected to the C7 network or via a C7 GE-2p card acting as a router. In these configurations, you set up a cross connection between the E3 port of the AMP or ATP card and the OCn port in each C7 shelf that has an external host device connected to the shelf. From the GUI, in the Select Cross-Connect Endpoints dialog box, make sure that you set the Cross-Connect Way parameter to 2WAY and apply an In-Band (INBANDMGT) traffic profile.

After you have configured the cross-connection, static routes must be provisioned to allow traffic to pass via the AMP E3 port.

Refer to the *Calix C7 Broadband Data Services Guide* for details on setting up the GE-2p card for multipoint routing.

Bandwidth

The AMP routing feature provides about 100 Kbps of bandwidth.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Creating static routes

All host devices that connect to TCP/IP networks have a unique IP address. Your organization's LAN administrator manages and assigns IP addresses. IP addresses include a network number and a host device number. Additionally, subnet masks are used to define subnetworks. The subnet mask allows IP and routing protocols to locate network and host devices.

If the IP address of a third-party host device is not located on the same subnet as its corresponding C7 AMP or ATP card, you must create a static route to enable connectivity. In this case, the C7 shelf with an attached host device must have a static route to the external host device. The C7 checks its routing table for routes to external host devices that are not connected to the C7 network and not within the C7 subnet. The entry of the host device route in the static route table ensures that IP packets addressed to the external host device are properly routed.

Prior to creating a static route, check with your LAN administrator to ensure that the appropriate IP addresses and subnet masks are correctly assigned.

Configure Static IP Routes to the AMP or ATP Card (on page 179) for details on setting up and configuring static IP routes.

Remote management for subtended devices

For specific application details, see the *Calix C7 Application Guide: Configuring Remote Management for Subtended Devices*.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring the Remote AMP Ports for Management

To establish a management channel through the remote C7 AMP card, you must configure its rear (E2) and in-band (E3) management ports with IP addresses. Management traffic from the network routes to the E3 port, and then out to the subtended device through the E2 port. The AMP E2 and E3 port IP addresses must belong to different subnets to facilitate routing.

To configure the remote C7 AMP E2 and E3 management ports

1. On the Navigation Tree, click the C7 shelf to configure.
2. In the Work Area, click **Login Channel**.
3. In the Ethernet Rear Access panel, set the following parameters for the AMP E2 port:
   a. In the Channel Access Privilege list, click **FULLACC** (Full Access).
   b. In the IP Address box, type the IP address of the E2 port.
   c. In the Sub-Network Mask box, type the subnet mask.
   d. In the Gateway box, leave the box blank.

   Note: Do not assign a Gateway address to the E2 port.
4. In the Ethernet In Band Management panel, set the following parameters for the AMP E3 port:
   a. In the Channel Access Privilege list, click **FULLACC** (Full Access).
   b. In the IP Address box, type the IP address of the E3 port.
   c. In the Sub-Network Mask box, type the subnet mask.
   d. In the Gateway box, type the IP address of the default gateway router.

   Note: For remote AMP cards, the next router interface (hop) in the path to the office LAN serves as the gateway. Typically, this interface lies on the other end of the in-band management cross-connect, and must also belong to the same IP subnet as the remote AMP E3 port.

   e. In the Encapsulation Type, select the encapsulation type for the E3 port, **Bridged** or **Routed**.
5. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your changes.

The router interface serving as the gateway for the remote AMP card must have an IP address that belongs to the same subnet as the E3 port. Depending on your configuration, this gateway router interface may reside on the office C7 shelf (when a GE-2p or AMP card provides the link to the office LAN), or on an upstream ATM router (when an ATM interface provides the link to the office LAN).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Further, on that gateway router, you must create a static route to the IP subnet of the remote AMP E2 port to provide a routing path to the host device. The remote AMP E3 port serves as the next hop for this static route.

Creating the In-Band Management Channel

To establish the management channel, create an in-band management cross-connect between the remote C7 shelf and the office C7 shelf. The remote AMP E3 port provides the source endpoint for the cross-connect. Select the destination endpoint according to the card type providing the link to the office LAN at the far end.

Protection for the in-band management VC is not currently supported.

To configure an in-band management channel

1. On the Navigation Tree, click the Network level.
2. On the File menu, click:
   - (in iMS) **Create** > **Cross-Connect** > **VC**
   - (in CMS) **Create** > **C7** > **Cross-Connect** > **VC**
3. In the Select Cross-Connect Endpoints (New Virtual Channels) dialog box, Source area, define the source endpoint:
   a. In the Shelf list, select the remote C7 shelf.
   b. In the Type list, click **AMP Ethernet Port**.
   c. In the port list, select the AMP E3 port on the remote C7 shelf.
   d. Click **SRC** to add the endpoint to the Source column in the Cross-Connects To Be Created area.
4. In the Destination/Drop area, define the destination endpoint:
   a. In the Shelf list, select the office C7 shelf.
   b. In the Type list, select the port type providing the cross-connect destination endpoint:
      - For Ethernet, click **Virtual Router Port**.
      - For an AMP E3 port, click **AMP Ethernet Port**.
      - For an ATM uplink port, select the appropriate port facility type.
   c. In the port list, select the port providing the destination endpoint.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

d. If applicable, specify the VPI/VCI address for the cross-connect:
   - In the VP box, type a VPI value.
   - In the VC box, type a VCI value.

e. Click **DEST** to add the endpoint to the Destination column in the Cross-Connects To Be Created area.

5. In the Required Parameters area:
   a. In the Cross-Connect Way list, click **2WAY**.
   b. In the ATM Traffic Profile ID list, click **INBANDMGMT**.
   c. In the Backward ATM Traffic Profile ID list, click **INBANDMGMT**.
   d. In the Cross-Connect Path box, select a protection configuration (**UNPROT** or **WORK + PROT**).
6. Click **OK** to create the management channel cross-connection.

Enable Routing for the Management Channel

You must enable global AMP routing to allow C7 AMP cards to route in-band management traffic.

Use the following procedure to set up the AMP routing feature.

ALERT! For security purposes, do not enable the AMP routing feature unless you must allow access third-party host devices connected to C7 shelves. Access to your LAN and C7 network can be obtained via a remote C7 shelf with the AMP routing feature enabled.

To enable routing on C7 AMP cards

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Security** > **Global** to display the Global Security Settings Panel.
3. On the Routing Enabled list, click **Y** (Yes), to enable AMP routing.
4. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Chapter 3

Performing C7 Node-Specific Tasks

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Node Assignment and Configuration

Assign C7 Shelves to a Node

Complete the steps below to assign C7 shelves to a node:

To assign one or more C7 shelves to an existing node

1. On the Tools menu, click **Add Shelves to Network** to open the Add Shelves dialog box.
2. In the Current Nodes area, select a node to display its properties in the upper right corner of the dialog box.
3. In the Unassigned Shelves area, select a C7 shelf and then click **Add** to assign the shelf to the node.
4. Repeat Step 3 to add other C7 shelves to the node.
5. When you are done adding shelves to the node, click **Assign**.
6. Repeat Steps 2 through 5 to add C7 shelves to another node, or click **Next** to exit.

Define the C7 Node Type

Node types are typically defined during initial turn-up using the Add Shelves to Network tool. However, you can modify the provisioned C7 node type to account for changes made in the field, including cabinet replacement or augmentation. Set the C7 node type using the Mount Type parameter at the node level of the Navigation Tree.

The Mount Type parameter determines the power input threshold at which C7 shelves in the node report the Power Exceeded alarm. The threshold varies based on node type and whether the cabinet power system has been enhanced to supply additional power capacity to C7 shelves in the node.

The node Mount Type options are described below:

Mount Type	Node Type Description	Power Input Alarm Threshold
Rack Mount	Any C7 indoor node in rack-mount configuration.	1425W
ODC-10	ODC-10 cabinet with standard power system (2 rectifier modules; C7 shelves fused at 20A).	725W
ODC-20	ODC-20 cabinet with standard power system (2 rectifier modules; C7 shelves fused at 20A).	950W
ODC-20 (Power Upgrade)	ODC-20 cabinet with power system upgrade (3 or more rectifier modules; C7 shelves fused at 30A).	1620W
ODC-20 (Power Upgrade	ODC-20 cabinet with power system and cooling upgrades (3 or more rectifier modules; C7 shelves fused at 30A; door-mounted heat	1620W

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Mount Type	Node Type Description	Power Input Alarm Threshold
& Heat Exchanger)	exchanger).	
ODC-40	ODC-40 cabinet with standard power system (2 rectifier modules; C7 shelves fused at 20A).	950W
ODC-40 (Power Upgrade)	ODC-40 cabinet with power system upgrade (3 or more rectifier modules; C7 shelves fused at 30A).	1620W
ODC-40 (Power Upgrade & Heat Exchanger)	ODC-40 cabinet with power system and cooling upgrades (3 or more rectifier modules; C7 shelves fused at 30A; door-mounted heat exchanger).	1620W
ODC-80	ODC-80 cabinet with standard power system (2 rectifier modules per power shelf; C7 shelves fused at 20A).	950W
ODC-80 (Power Upgrade)	ODC-80 cabinet with power system upgrade (3 or more rectifier modules per power shelf; C7 shelves fused at 30A).	1620W
ODC-80 (Power Upgrade & Heat Exchanger)	ODC-80 cabinet with power system and cooling upgrades (3 or more rectifier modules per power shelf; C7 shelves fused at 30A; door-mounted heat exchanger).	1620W
ODC-120 Top	Top node (3 upper shelves) of 2-node ODC-120 cabinet (2 rectifier modules per power shelf; C7 shelves fused at 20A).	950W
ODC-120 Bottom	Bottom node (3 lower shelves) of 2-node ODC-120 cabinet (2 rectifier modules per power shelf; C7 shelves fused at 20A).	950W
ODC-120 Top (Power Upgrade)	Top node (3 upper shelves) of 2-node ODC-120 cabinet (3 or more rectifier modules per power shelf; C7 shelves fused at 30A).	1620W
ODC-120 Bottom (Power Upgrade)	Bottom node (3 lower shelves) of 2-node ODC-120 cabinet (3 or more rectifier modules per power shelf; C7 shelves fused at 30A).	1620W
ODC-120 Top (Power Upgrade & Heat Exchanger)	Top node (3 upper shelves) of 2-node ODC-120 cabinet (3 or more rectifier modules per power shelf; C7 shelves fused at 30A; door-mounted heat exchanger).	1620W
ODC-120 Bottom (Power Upgrade & Heat Exchanger)	Bottom node (3 lower shelves) of 2-node ODC-120 cabinet (3 or more rectifier modules per power shelf; C7 shelves fused at 30A; door-mounted heat exchanger).	1620W
ODC-1000	ODC-1000 cabinet with standard cooling system.	1620W
ODC-1000 (High Capacity Heat Exchanger)	ODC-1000 cabinet with cooling system upgrade (high capacity door-mounted heat exchanger).	1620W
ODC-2000	Standard ODC-2000 cabinet.	1620W
ODC-3000	Standard ODC-3000 cabinet.	1620W
ODC-4000 Top	Top node (upper shelves) of 2-node ODC-4000 cabinet.	1620W
ODC-4000 Bottom	Bottom node (lower shelves) of 2-node ODC-4000 cabinet.	1620W

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

To define the C7 node type

1. On the Navigation Tree, click the Node level.
2. In the Work Area, click **Node View**.
3. In the Node panel, do the following:
   a. In the Mount Type list, select the type of mounting or enclosure hosting the C7 node. For example, click **Rack Mount** for an indoor node or select the appropriate ODC cabinet type.
   b. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK**.

Repeat Steps 1 through 3 as needed for other C7 nodes.

Configure Two Nodes in an ODC-120

A C7 node configuration allows up to five C7 shelves in a node. In a fully loaded ODC-120 cabinet configuration with six C7 shelves installed, you need to specify two nodes in the cabinet. You can use the Mate Node parameter to identify the two nodes in the cabinet as mates.

To set the Mate Node parameter

1. On the Navigation Tree, click the Node level.
2. In the Work Area, click **Node View** to display the Node panel.
3. In the Mate Node list, click the mate node.
4. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save the changes.

Configure a Node to Use a Test Head

After installing an external test head or ATP card in a C7 network node, you need to create a test group before you can use the test head to perform metallic testing. Things to keep in mind:

- Each shelf in a test group must have its own AMP or ATP card.
- You must install the test head or AMP card before creating a test group.
- You must create a test group for each node that has a test head or ATP card installed.
- Optionally, you can create multiple test groups within a node, each containing different C7 shelves.

For more information on metallic testing, see the *Calix C7 Troubleshooting Guide*.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

To create a test group

1. On the Navigation Tree, click the C7 node that has the external test head or ATP card installed.
2. On the toolbar, click **Create** to open the Test Group dialog box.
3. In the Test Group dialog box, do the following:
   a. In the Test Master list, select an AMP or ATP card to manage the test group. By default, the system software selects an AMP or ATP card (not necessarily the node AMP).
   b. In the Shelves list, select all the C7 shelves to include in the test group. If you are creating a single test group for the node, select all shelves in the node.
   c. Click **OK** to create the test group.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Alarm-Related Tasks

Set Alarm Cut-Off Attributes

On the C7 system, you can set an alarm cutoff to operate in 1 of 3 modes:

- **Delayed:** Alarm cutoff is delayed to allow an announcement. The audible alarm sounds for 5 seconds and then shut off.
- **Immediate:** The alarm cutoff occurs automatically and immediately at the near-end node. The audible alarm is not sounded at the near end.
- **Manual:** The audible alarm sounds continuously until the OPR-ACO command is executed, or there is manual intervention at the shelf.

To set the alarm cutoff (ACO) mode

1. On the Navigation Tree, click the Node level.
2. In the Work Area, click **Node View**.
3. In the Alarm Cutoff Mode box, select the appropriate mode value.
4. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your configuration.

Set Alarm Reporting for Multi-Shelf C7 Nodes

To ensure that C7 remote nodes properly report alarms for the entire C7 network to the switch, specify the primary AMP or ATP card in each multi-shelf C7 node.

To configure alarm reporting in a multi-shelf C7 node

1. On the Navigation Tree, click the Node level.
2. In the Work Area, click **Node View**.
3. In the Node area:
   a. In the Node AMP list, select the shelf ID that contains the primary AMP or ATP card.
   b. In the Alarm Scope list, verify that the Alarm Scope is properly set for this node for your network configuration:
      - If the AMP functions as the primary AMP for the C7 network, select **Network**.
      - (Recommended) If the AMP does not function as the primary AMP for the network, select **Node**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Note: Calix recommends that no more than two C7 nodes in a C7 network be configured for network alarms.

c. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your changes.

Repeat Steps 1 through 3 as needed for other C7 nodes.

View Node-Specific Alarms

Complete the steps below to view system alarms associated with a node:

To view node-specific alarms

1. At the lower left corner of the Alarm Table, click **By Selection**.
2. On the Navigation Tree, click a node to view alarms associated with it. The alarms specific to your choice appear in the Alarm Table.
3. If desired, choose a different node to view its alarms.
4. To view all system alarms, click **By Selection and Children**.

Set Environmental Alarm Attributes

Use this procedure to set environmental alarm attributes. Note that the Environmental Input table displays the default system assignments and parameter values for 8 alarm types.

To set environmental alarm attributes

1. On the Navigation Tree, click the Node level.
2. In the Work Area, click **Environment**.
3. Click an alarm input to place it in the Edit Row to modify its parameter values:
   a. In the Notification Code list, click an alarm severity: **MN** (Minor), **MJ** (Major), or **CR** (Critical).
   b. In the Alarm Type list, select an alarm type.
   c. In the Polarity list, select to indicate if the status points are **NORMOPEN** (Normally Open) or **NORMCLOSED** (Normally Closed).
   d. In the Alarm Message box, type a text message (up to 11 characters) to include in notifications for this alarm type.
4. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your configuration settings.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Chapter 4

Performing C7 Shelf-Specific Tasks

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

View Shelf Status

On the Navigation Tree, you can click the C7 shelf to view the graphical representation of the shelf, the shelf information area, and the timing information.

The Shelf panel provides the following information:

Category 3 Shutdown: This is the amount of time to wait before powering down category 3 type equipment during a power failure. The valid range is 0 to 480 minutes.

Power Level: This indicates the maximum power level (in watts) that the C7 shelf is allowed to consume across all cards within the shelf.

Power Dissipation: This indicates the maximum power (in watts) that the C7 shelf has been budgeted to dissipate across all cards within the shelf.

Environment: This indicates whether the C7 shelf is provisioned to be in a controlled or uncontrolled environment.

Power Input: This indicates the type of DC power being supplied to the C7 shelf:

- **DC Source A**
- **DC Source B**
- **Both DC Sources**

Default Virtual Bridge: This simplifies the provisioning of VLAN interfaces by designating a single virtual bridge within a shelf so all subsequent VLAN references can be made without specifying the virtual bridge number.

Backplane ID

Equipment Type: This indicates the type of C7 shelf:

- **C7-SHELF-10C** – C7 Shelf, Cabinet, 10 Slots (CO)
- **C7-SHELF-10M** – C7 Modified Shelf, Cabinet, 10 Slots (M)
- **C7-SHELF-20** – C7 Shelf, 20 Slots
- **C7-SHELF-20C** – C7 Shelf, Cabinet, 20 Slots20-slots (CO)
- **C7-SHELF-20HD** – C7 Shelf, 20 Slots, High Density

Provision Capacity Used: This indicates the percentage in use of RAP flash memory in a C7 shelf. The valid range is 1 to 100. Note that the Provisioning Capacity Overflow alarm is raised if the amount of active images in the RAP card is using a significant amount of the RAP memory (90% or more). Images are directly related to the type of cards active in the C7 shelf. At 100%, the RAP card does not have any space available to store new images. The upgrade application (CUP) will fail if you are upgrading the shelf.

Condition Status: Reports the detected status of the C7 shelf.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Condition	Description
Admin Master AMP not present	No admin master is detected on the network. End-to-end provisioning may not work.
BAR in progress	A backup and restore process is in progress.
Cold reset of database	A deletion of the shelf database and reset to default values is in progress.
DCA Failure	No DC power is detected on power terminal A.
DCB Failure	No DC power is detected on power terminal B.
Disjoint Domain	A minor alarm on this shelf is part of a disjoint domain.
Duplicate Admin Master provisioned	More than one Admin Master AMP or ATP is detected on the network.
Inhibit Upgrade	Upgrade of the standby RAP is inhibited.
Invalid Backplane ID	The detected backplane ID is not valid.
Normal	The shelf is operating normally.
Remote Alarm	A remote alarm is detected on another shelf.
Shelf Lost Communication	The shelf has lost communication.
Software Download	A software download is in progress.
System Reboot	A system reboot is in progress.

Serial Number: Reports the serial number assigned to the shelf.

Common Language ID: This indicates the Common Language Equipment Identifier (CLEI) code of the C7 shelf.

Part Number: This identifies the Calix part number for the C7 shelf.

Hardware Revision: This identifies the revision number of the C7 shelf.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Set Shelf Power Parameters

You can configure the following power settings on a C7 shelf:

- **Power Input:** Specifies how DC power is supplied to the shelf.
- **Category 3 Shutdown:** Specifies the maximum amount of time (in minutes) that cards assigned to power category 3 will remain powered up after the shelf switches to emergency backup power.

Power Input source

Set the Power Input parameter to apply DC power to terminal A, terminal B, or both terminals (default setting). The C7 raises an alarm if DC power is not detected on the terminal(s) specified by the Power Input parameter setting.

To set Power Input source

1. On the Navigation Tree, click the shelf for setting the Power Input parameter.
2. In the Work Area, click **Shelf View**.
3. In the Shelf area, in the Power Input list, select the choice that matches your power connection to the C7:
   - DC Source A
   - DC Source B
   - Both DC Sources (default)
4. On the toolbar, click **Apply** to save your changes. In the Confirmation dialog box, click **OK**.

Category 3 Shutdown timer

The C7 can automatically disable xDSL data services in a remote cabinet when a power fault occurs, to reduce power consumption and extend battery life. Use the C7 power management feature to protect high-priority services such as lifeline POTS. All C7 xDSL cards feature a Power Category parameter that can be set for either Category 1 or Category 3 priority.

When an AC power failure occurs, the C7 disables DSL cards provisioned for Category 3 priority. Cards provisioned for Category 1 are kept in service as long as sufficient backup power to the shelf is sustained. You can set a shelf-level delay timer for Category 3 shutdowns, from 0 to 480 minutes. The default setting is 10 minutes. For COMBO cards, only DSL ports are shut down when the timer expires, while DS0 ports remain in service.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Before setting the Category 3 Shutdown timer, verify which environmental alarm pin pair on the rear of the shelf is wired for power management. All C7 cabinets are pre-wired at the factory with the AC Fail alarm on environmental alarm pin pair 8 to trigger power shutdown in the event of a loss of AC power. Further, the software on all C7 shelves automatically associates alarm type "Power" to environmental alarm pin pair 8.

You can modify the Category 3 shutdown delay timer for the C7 shelf from the default (10 minutes).

To set the Category 3 Shutdown delay timer

1. On the Navigation Tree, click the C7 shelf to configure.
2. In the Work Area, click **Shelf View**.
3. In the Shelf field, in the Category 3 Shutdown box, type a delay timer value from 0 to 480 minutes.
4. On the toolbar, click **Apply** to update settings. In the Confirmation dialog box, click **OK**.

To set the Power Category parameter for an xDSL card, see *Configuring the xDSL Power Shutdown Priority* (on page 306).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Common Controller Tasks

Configuration Rules for AMP and ATP Ethernet Login Channels

The C7 Ethernet management ports (hosted on C7 AMP or ATP cards) consist of two out-of-band and one-in-band management port for system management over TCP/IP connections. Use these recommendations and configuration rules to configure the management ports.

Recommended Ethernet management port usage

Calix recommends using the Ethernet management ports for the following connections:

- **Front out-of-band Ethernet management port (E1):** Use the front (E1) port to connect a PC directly to the front of the C7 and start the management software.
- **Rear out-of-band Ethernet management port (E2):** Use the rear (E2) port to connect the C7 to a LAN. You can assign a gateway address to the E2 port to allow management access from other IP networks, but this prevents using the E3 port on that C7.
- **In-band management port (E3):** Use the in-band (E3) port to access the C7 remotely through an internal channel across the C7 network. You must assign a gateway address to the E3 channel to use in-band access (which prevents assigning a gateway address from being associated with the E2 port on that C7).

Static IP routes are required to connect a C7 AMP or ATP card to an IP network that is routed through a gateway other than the default gateway. For more information, see *Configure Static IP Routes to the AMP or ATP Card* (on page 179).

Ethernet management port parameters

Use the following parameters to configure the E1, E2, and E3 ports and to create static IP routes:

- **IP Address or IP Route:** The destination subnet IP address. For routes from the Management slot, this address must be on the same subnet as one of the E1, E2, or E3 ports.
- **Sub-network Mask or Mask:** Destination IP subnet mask.
- **Gateway:** "Next hop" IP host address, typically a router.
- **MAC Address (E1, E2, and E3 ports only):** Media Access Control address that identifies a device at the MAC layer in the network architecture.
- **Routing Metric (static IP routes only):** The metric used by the routing protocol. The default is 1. Higher metrics make the route less favorable; metrics are counted as additional hops to the destination network or host.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Ethernet management port configuration rules

These configuration rules apply to configuring Ethernet management ports on an AMP or ATP card:

- All three ports must have IP addresses on separate subnets.
- Only one port per card can have a gateway address assigned to it. The remaining two ports must have a gateway setting of 0.0.0.0.
- The gateway IP address assigned to a port must be in the same subnet as the port IP address.

Examples of configuring IP addresses

Valid IP configuration	Not a valid IP configuration
E1 IP: 192.168.1.1 E2 IP: 192.22.1.1 E3 IP: 166.25.90.212	E1 IP: 192.168.1.1 E2 IP: 192.168.1.20 E3 IP: 166.25.90.212
This configuration is valid because all the IP addresses are on different subnets.	This configuration is not valid because the E1 and E2 IP addresses are on the same subnet.

Examples of configuring gateway addresses

Valid gateway configuration	Not a valid gateway configuration	Not a valid gateway configuration
E1 IP: 192.168.1.1 Gateway: 0.0.0.0 E2 IP: 192.22.1.1 Gateway: 0.0.0.0 E3 IP: 166.25.90.212 Gateway: 166.25.90.1	E1 IP: 192.168.1.1 Gateway: 0.0.0.0 E2 IP: 192.22.1.1 Gateway: 0.0.0.0 E3 IP: 166.25.90.212 Gateway: 172.25.90.1	E1 IP: 192.168.1.1 Gateway: 0.0.0.0 E2 IP: 192.22.1.1 Gateway: 192.22.1.8 E3 IP: 166.25.90.212 Gateway: 166.25.90.1
This configuration is valid because only one channel has a gateway assigned and the gateway is on the same subnet as the channel IP address.	This configuration is not valid because the E3 IP and gateway addresses are on different subnets.	This configuration is not valid because E2 and E3 both have assigned gateways.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configure the Channel Access Privilege, IP Address, Sub-network Mask, and Gateway address of the E3 port on the AMP or ATP card to configure in-band management.

Channel access parameters

You should check and set the applicable channel access privilege parameters. The privilege options are:

- **Fullacc:** Full access. This allows full access for entering commands and receiving autonomous messages. Full access is the default.
- **Noacc:** No access. The channel does not have external access.
- **Automsg:** Autonomous message only. This allows only autonomous messages to be sent out the channel. Note that this value cannot be set from the GUI.

Configure the AMP or ATP Front Ethernet Port (E1)

The Administration and Management Processor (AMP) and Administration and Testing Processor (ATP) cards support an Ethernet login channel (E1) for direct connection using an RJ-45 socket on the front of the card. When configured, the E1 channel provides an access point for administering a C7 network from a connected PC.

Ethernet Front Access (E1) channel configuration process

Configuring the E1 channel on the C7 requires the following actions:

- Obtain assignments from your network administrator for IP and Sub-network Mask.
- Leave the Gateway parameter at 0.0.0.0.
- Configure the Ethernet Front Access parameters on the selected AMP or ATP card using the network addresses supplied by the administrator.

To configure an Ethernet login channel

1. On the Navigation Tree, click the shelf containing the ATM uplink and AMP or ATP card.
2. In the Work Area, click **Login Channel** to open the Ethernet Front Access panel.
3. For the Ethernet port you are configuring, set the following parameters:
   a. In the Channel Access Privilege list, select the access level.
   b. In the IP Address box, type the assigned IP address.
   c. In the Sub-network Mask box, type the assigned mask.
   d. In the Gateway box, type the assigned address.
4. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your changes.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configure the AMP or ATP Rear Ethernet Port (E2)

The Administration and Management Processor (AMP) and Administration and Testing Processor (ATP) cards support an Ethernet login channel (E2) for wire-wrap connections on the backplane. When configured, the E2 channel provides an access point for administering a C7 network from a LAN connection.

Ethernet Rear Access (E2) channel configuration process

Note: If a Gateway address is assigned to the E2 channel, you cannot use the E3 channel.

Configuring the E2 channel on the C7 requires the following actions:

- Obtain assignments from your network administrator for IP address and sub-network mask.
- Obtain a Gateway address from your network administrator if the E2 channel is used for access from networks other than the LAN.
- Configure the Ethernet Rear Access parameters on the selected AMP or ATP card using the network addresses supplied by the administrator.

To configure an Ethernet login channel

1. On the Navigation Tree, click the shelf containing the ATM uplink and AMP or ATP card.
2. In the Work Area, click **Login Channel** to open the Ethernet Rear Access panel.
3. For the Ethernet port you are configuring, set the following parameters:
   a. In the Channel Access Privilege list, select the access level.
   b. In the IP Address box, type the assigned IP address.
   c. In the Sub-network Mask box, type the assigned mask.
   d. In the Gateway box, type the assigned address.
4. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your changes.

Configure the AMP or ATP In-Band Management Ethernet Port (E3)

The Administration and Management Processor (AMP) and Administration and Testing Processor (ATP) cards support an internal Ethernet login channel (E3) used for in-band connections. When configured, the E3 channel provides an access point for administering a C7 network over an ATM cross-connect.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Ethernet In-Band ATM Management (E3) channel configuration process

Configuring the E3 channel on the C7 requires the following actions:

- Obtain assignments from your network administrator for IP, Sub-network Mask, and Gateway addresses.
- Configure the Ethernet In-band ATM Management parameters on the selected AMP or ATP card using the network addresses supplied by the administrator.
- Create a VC cross-connection between the selected AMP or ATP card and a network-facing (uplink) card on the same shelf.

To configure an Ethernet login channel

1. On the Navigation Tree, click the shelf containing the ATM uplink and AMP or ATP card.
2. In the Work Area, click **Login Channel** to display the Ethernet In Band ATM Management panel.
3. For the Ethernet port you are configuring, set the following parameters:
   a. In the Channel Access Privilege list, select the access level.
   b. In the IP Address box, type the assigned IP address.
   c. In the Sub-network Mask box, type the assigned mask.
   d. In the Gateway box, type the assigned address.
   e. In the Encapsulation Type list, select **Bridged** or **Routed**.
4. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your changes.

To configure a VC cross-connection from the uplink to the E3 port

1. On the File menu, click:
   - (in iMS) **Create** > **Cross-Connect** > **VC**
   - (in CMS) **Create** > **C7** > **Cross-Connect** > **VC**
2. In the New Virtual Channels dialog box, Source area:
   a. In the Shelf list, select the shelf containing the uplink card.
   b. In the Type box, select the uplink facility type:
      - For an ATM uplink, select the facility type: **(STSn) VC**, **DS1 Port VC**, or **DS3 Port VC**, for example.
      - For a GE-2p Ethernet uplink:
        - Click **Virtual Router Port Select from List** to support a routed encapsulated VC; required if the destination AMP E3 port is in the same shelf.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- Click **Virtual Bridge Port Select from List** to support a bridged encapsulated VC.

c. In the endpoints list, select the uplink port:

- For an ATM uplink, select the uplink port/facility.
- For a GE-2p Ethernet uplink, select the VR port on the uplink virtual router.

d. If applicable (for an ATM uplink facility), specify the VPI/VCI address for the cross-connect:

- In the VP box, type a VPI value.
- In the VC box, type a VCI value.

e. Click **SRC** to place the source endpoint in the Cross-Connects To Be Created area.

3. In the Destination/Drop area:

a. In the Shelf list, select a shelf containing an AMP or ATP card.

b. In the Type box, click **AMP Ethernet Port**.

c. In the endpoints list, select an AMP E3 port.

d. Click **DEST** to place the destination endpoint in the Cross-Connects To Be Created area.

4. In the Required Parameters area:

a. In the Cross-Connect Way box, click **2WAY**.

b. In the ATM Traffic Profile ID box, click **INBANDMGMT**.

c. Leave the Backward ATM Traffic Profile ID box blank.

d. In the Cross-Connect Path box, select a protection configuration (**UNPROT** or **WORK + PROT**).

5. Click **OK** to create the in-band management connection.

Configuring In-Band Management

The Administration and Management Processor (AMP) and Administration and Testing Processor (ATP) cards support an internal Ethernet login channel (E3) used for in-band connections. When configured, the E3 channel provides an access point for administering a C7 network over an ATM cross-connect.

Before starting

Before starting the Quick in-band management configuration process, check the following conditions:

- An ATM uplink card installed and wired.
- Your computer is connected to a C7.
- The management software application is started.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Information you need

You need to have the following information on-hand to complete in-band management configuration:

- Assignments from your network administrator for IP, Subnet Mask, and Gateway addresses.
- VP and VC values for the ATM uplink.

Ethernet login channel configuration rules

These configuration rules apply to configuring Ethernet login channels on a single AMP or ATP card:

- All three channels must have IP addresses on separate subnets.
- Only one channel on an AMP or ATP card can have a gateway address assigned to it. The remaining two channels must have a gateway setting of 0.0.0.0.
- The gateway address assigned to a channel must be on the same subnet as the channel IP address.
- The ATM cross-connect for an E3 in-band channel must go to a port in the same shelf as the AMP or ATP card containing the E3 channel.

Quick in-band management configuration process flow

1. Configure ATM uplink.
2. Configure in-band management port (E3) on the AMP or ATP card.
3. Cross-connect the E3 port to the ATM uplink.
4. Check that it all works.

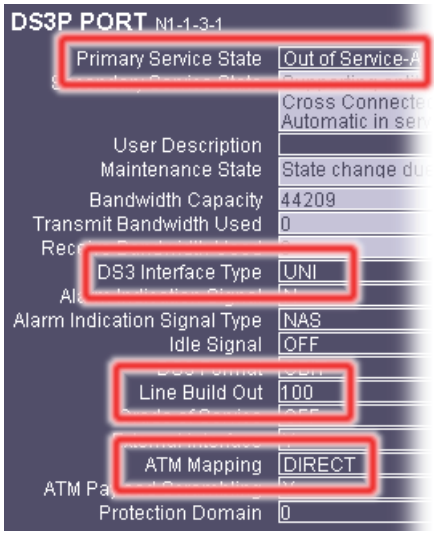
Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring a DS3 Port for ATM Uplink

Complete the steps below to configure a DS3 port for an ATM uplink.

To configure a DS3 port for ATM uplink

1. On the Navigation Tree, click a DS3-12p card to view the ports, and then click a DS3 port to select it.
2. In the Work Area, click **Provisioning** to view the DS3 Port parameters panel.
3. In the DS3 Port parameters panel:



   a. In the Primary Service State list, click **OOS** (Out of Service) to place the port out of service.
   b. In the DS3 Interface Type list, click **UNI**.
   c. In the Line Build Out box, type the distance in feet from the C7 to the ATM switch.
   d. In the ATM Mapping list, select the ATM mapping type used by the ATM switch.
4. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your changes.
5. In the Primary Service State list, click **IS** (In Service) to place the port back in service.
6. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your changes.

Configure ATM Uplink Port

You can configure a port on any ATM capable card for uplink to an ATM switch. This section includes an example of configuring a port on a DS3-12p card to provide access to the data network.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Requirement for ATM Uplink Used for In-Band Management

The ATM uplink card and the AMP or ATP card must be in the same C7 shelf when configuring in-band management.

DS3 Port Parameters for an ATM Uplink

You should check and set three parameters to configure a DS3 port for ATM uplink:

Parameter	Value
Interface	UNI
ATM Mapping	Set to match your ATM switch setting, PLCP or DIRECT.
Line Build Out	Set to match the distance in feet from the C7 to the ATM switch.

Configure In-Band Ethernet Port (E3)

Configure the E3 port on the AMP or ATP card to support in-band management.

Ethernet In-Band ATM Management Parameters

You should check and set the applicable parameters to configure Ethernet in-band management.

Parameter	Description
Channel Access Privilege	Identifies the access level. Channel access privilege options are: • **Fullacc:** Full access. This allows full access for entering commands and receiving autonomous messages. Full access is the default. • **Noacc:** No access. The channel does not have external access. • **Automsg:** Autonomous message only. This allows only autonomous messages to be sent out the channel. Note that this value cannot be set from the GUI.
IP Address	Identifies the IP address used when accessing the Ethernet port.
Sub-network Mask	Identifies the mask used on the IP Address.
Gateway	Only one gateway address can be configured on an AMP or ATP card. Configuring in-band management prevents using a gateway address on the E1 (front) or E2 (rear) Ethernet ports.
MAC Address	Identifies the Media Access Control layer address of the E3 port. (Not configurable)

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Parameter	Description
Encapsulation Type	Specifies the encapsulation type to use for transmitted traffic. • **Routed:** RFC 2684 Routed encapsulation (IP over ATM). • **Bridged** RFC 2684 Bridged encapsulation (IP over Ethernet over ATM).

Configuring an Ethernet Login Channel

Complete the steps below to configure an Ethernet login channel.

To configure an Ethernet login channel

1. On the Navigation Tree, click the shelf containing the ATM uplink and AMP or ATP card.
2. In the Work Area, click **Login Channel** to display the Ethernet In Band ATM Management panel.
3. For the Ethernet port you are configuring, set the following parameters:
   a. In the Channel Access Privilege list, select the access level.
   b. In the IP Address box, type the assigned IP address.
   c. In the Sub-network Mask box, type the assigned mask.
   d. In the Gateway box, type the assigned address.
   e. In the Encapsulation Type list, select **Bridged** or **Routed**.
4. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your changes.

Create VC Cross-Connection

You can create a VC cross-connection between an ATM port or STS and the E3 port on the AMP or ATP card. This section includes an example of creating a VC cross-connection to a port on a DS3-12p card to provide access to the data network.

Required Order for Cross-Connection Endpoints

When configuring a cross-connection for in-band management, set up the cross-connection endpoints using the following order:

- The Source endpoint must be the uplink.
- The Destination endpoint must be the E3 port.

If you see an error message stating, "Invalid Access Identifier," you entered the Source and Destination endpoints in the wrong order.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring a VC Cross-connect from the Uplink Card to the C7 E3 Port

Complete the steps below to configure a VC cross-connect from the uplink card to the C7 E3 port.

To configure a VC cross-connection from the uplink card to the E3 port

1. On the File menu, click:
   - (in iMS) **Create** > **Cross-Connect** > **VC**
   - (in CMS) **Create** > **C7** > **Cross-Connect** > **VC**
2. In the New Virtual Channels dialog box, Source area:
   a. In the Shelf list, select the shelf containing the uplink card.
   b. In the Type box, select the uplink facility type:
      - For an ATM uplink, select the facility type: **(STSn) VC**, **DS1 Port VC**, or **DS3 Port VC**, for example.
      - For a GE-2p Ethernet uplink:
        - Click **Virtual Router Port Select from List** to support a routed encapsulated VC; required if the destination AMP E3 port is in the same shelf.
        - Click **Virtual Bridge Port Select from List** to support a bridged encapsulated VC.
   c. In the endpoints list, select the uplink port:
      - For an ATM uplink, select the uplink port/facility.
      - For a GE-2p Ethernet uplink, select the VR port on the uplink virtual router.
   d. If applicable (for an ATM uplink facility), specify the VPI/VCI address for the cross-connect:
      - In the VP box, type a VPI value.
      - In the VC box, type a VCI value.
   e. Click **SRC** to place the source endpoint in the Cross-Connects To Be Created area.
3. In the Destination/Drop area:
   a. In the Shelf list, select a shelf containing an AMP or ATP card.
   b. In the Type box, click **AMP Ethernet Port**.
   c. In the endpoints list, select an AMP E3 port.
   d. Click **DEST** to place the destination endpoint in the Cross-Connects To Be Created area.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

4. In the Required Parameters area:
   a. In the Cross-Connect Way box, click **2WAY**.
   b. In the ATM Traffic Profile ID box, click **INBANDMGMT**.
   c. Leave the Backward ATM Traffic Profile ID box blank.
   d. In the Cross-Connect Path box, select a protection configuration (**UNPROT** or **WORK + PROT**).
5. Click **OK** to create the in-band management connection.

Check That It All Works

After the ports and cross-connections are configured, an instance of the management software can be started by opening the IP Address of the E3 port.

Things to check

You can confirm that in-band management is available by:

- Checking the Primary Service State of the ATM uplink port. On the Navigation Tree, click the uplink port and check the following parameters:
  - Primary Service State is **IS-NR** (In-Service Normal).
  - Secondary Service State is normal.
- Connecting a PC to the same sub-net as the E3 port and entering the IP address of the E3 port in Internet Explorer.

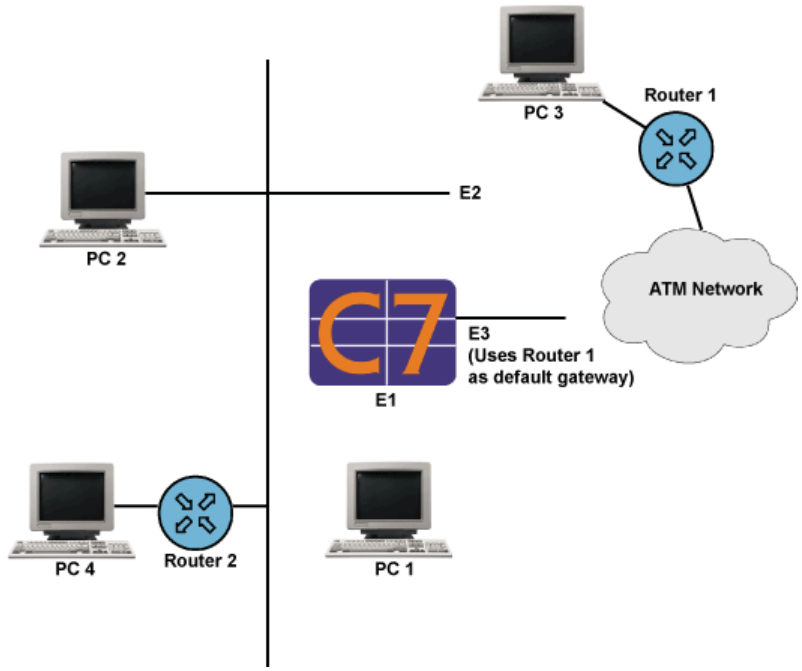
Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configure Static IP Routes to the AMP or ATP Card

You use static IP routes to create access points for administering the C7 network from an IP network routed through a gateway other than the default Ethernet gateway. The AMP and ATP cards support up to 20 static IP routes (not including the default route).

When a static IP route is needed

The following diagram illustrates a static IP route scenario:



In this example, PC 4 is routed through a gateway (Router 2), while the E3 port is configured as the default gateway. Additionally, PC4 requires a static IP route in order to connect with the C7 shelf.

Configuration process for adding static IP routes to AMP or ATP card

Configuring multiple IP networks to access the C7 for in-band management requires the following actions:

- Configure the AMP or ATP Ethernet port that will be used as the gateway default. For instructions, see *Configure the AMP or ATP rear Ethernet port (E2)* (on page 171) or *Configure the AMP or ATP in-band management Ethernet port (E3)* (on page 171).
- For each IP network or destination address that you need to add a static IP route, obtain assignments from your network administrator for IP, sub-network mask, and gateway addresses.
- Configure new static routes on the selected AMP or ATP card.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

To add static IP routes to the AMP or ATP card

1. On the Navigation Tree, click the AMP or ATP card on the shelf containing the ATM uplink.
2. On the File menu, click **Create** > **Ethernet and IP** > **IP Route** to open the IP Route dialog box.
3. In the IP Route dialog box and set the following parameters:
   a. In the Router Address box, type the assigned IP address.
   b. In the IP Route box, type the assigned IP address.
   c. In the Mask box, type the assigned mask.
   d. In the Gateway box, type the assigned address.
   e. Click **Add** to add the route to the IP Route(s) to be created list.
   f. Repeat Steps 3a through 3e for each additional static IP route.
   g. Click **Create** to save your changes.
4. Check that the static IP route works by completing the procedure "To ping from the AMP or ATP."

To ping from the AMP or ATP

1. On the Navigation Tree, click the AMP or ATP card on the shelf containing the ATM uplink.
2. In the Work Area, click **Static Routes**.
3. On the toolbar, click **Action** > **Ping Host** to open the AMP IP Ping Host dialog box.
4. In the AMP IP Ping Host dialog box, do the following:
   a. In the AMP Address box, select the AMP to ping.
   b. In the Host IP Address box, type the host IP address.
   c. Adjust the Ping Timeout, Ping Count, Ping Interval, and Ping Packet Size as needed.
   d. Click **Ping Host**.
5. To close the Host IP Address dialog box, click **Cancel**.

To delete static IP routes from AMP or ATP

WARNING! Do not delete a currently-active route.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

1. On the Navigation Tree, click the AMP or ATP card on the shelf containing the ATM uplink.
2. In the Work Area, click the **Static Routes** tab.
3. Select a static IP route to display it in the edit line.
4. On the toolbar, click **Delete**. In the Confirmation dialog box, click **OK**, and then click **Apply** to save your changes.

Configuring RAP-10GE In-Band Management Ethernet Port (E4)

The Resource Arbitration Processor (RAP-10GE) card supports an internal Ethernet login channel (E4) used for in-band connections. When configured, the E4 channel provides an access point for administering a C7 network.

Note: You can provision either the E3 or the E4 port for in-band management, because they share the same MAC Address.

Ethernet In-Band VLAN Management (E4) channel configuration process

Configuring the E4 channel on the C7 requires the following actions:

1. Obtain assignments from your network administrator for IP, Sub-network Mask, and Gateway addresses.
2. Create an in-band management VLAN on the C7 shelf.
3. Configure the Ethernet In-band VLAN Management parameters on the selected RAP-10GE card using the network addresses supplied by the administrator.
4. Once a management VLAN is established, you can create VLAN-IFs to associate RAP-10GE port interfaces to the management VLAN, enabling in-band management over those links.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

To configure an Ethernet login channel

1. If the management VLAN does not already exist on the shelf, create the VLAN from the File menu: click **Create** > **C7** > **Ethernet and IP** > **S-VLAN**, and then create a VLAN for the in-band management. See *Creating a VLAN* (on page 227) for instructions, if necessary.
2. On the Navigation Tree, click the shelf containing the RAP-10GE card.
3. In the Work Area, click **Login Channel** to display the Ethernet In-Band VLAN Management panel.
4. For the Ethernet port you are configuring, set the following parameters:
   a. In the Channel Access Privilege list, select the access level.
   b. In the IP Address box, type the assigned IP address.
   c. In the Sub-network Mask box, type the assigned mask.
   d. In the Gateway box, type the assigned address.
   e. In the VLAN Tag list, select the VLAN ID for the in-band management VLAN.
5. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your changes.

To create a VLAN interface for RAP-10GE ports

1. On the CMS File menu, click **Create** > **C7** > **Ethernet and IP** > **VLAN Interface**.
2. In the VLAN Interface dialog box, do the following:
   a. In the Bridge/Uplink Shelf list, select the shelf where the RAP-10GE card is located.
   b. In the VLAN list, select the in-band management VLAN.
   c. Select the **Bridge** button, and then select **Local** from the list.
   d. In the Equipment/Group list, select the system address of the RAP-10GE card.
   e. In the Interfaces list, select the system address of the RAP-10GE port to associate with the management VLAN.
   f. In the Port Type list, select **Trunk**.
3. Click **Add** to place the new VLAN interface into the VLAN Interface Object(s) To Be Created area.
4. Click **Create** to create a VLAN interface for the management VLAN and the RAP-10GE port.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Timing

Overview of Timing Scenarios and Parameters

You can configure a C7 shelf to run in one of three timing modes:

- **External:** A pair of external Building Integrated Timing Supply (BITS) clock inputs acts as the reference source.
- **Line:** One OCn, DS3, or DS1 interface acts as the primary reference, and another interface as the optional secondary reference.
- **Freerun:** The internal clock provides the timing reference.

By default, a C7 shelf starts in external timing mode with a composite clock reference. The shelf passes the timing to all other interfaces via the RAP common control card.

Note: For C7 shelves with DDS applications, Calix recommends that signals at DS0 level interconnections be timed off of the same composite clock source generated by the Building Integrated Timing Supply (BITS).

RAP2/RAP3/RAP2-OCn/RAP-10GE timing features and considerations

RAP and RAP-OCn cards support only an external composite clock input. RAP2, RAP3, RAP2-OCn, and RAP-10GE cards can support an external composite clock or DS1 clock input, and can provide a composite clock or DS1 clock output.

The following configuration rules apply to the RAP2, RAP3, RAP2-OCn, and RAP-10GE cards:

- In redundant configurations, both cards in the same shelf must be RAP2, RAP3, or RAP2-OCn (or any combination of the two), or both RAP-10GE to support new timing features.
- If RAP cards are mixed (RAP, RAP2, and RAP3 only), the RAP2/RAP3 cards only support the timing features of the RAP.
- If replacing a RAP2, RAP3, or RAP2-OCn card with a RAP card with timing features enabled, the RAP cannot be placed in-service and an Equipment Mismatch Alarm is raised. You must first disable the timing features.

Holdover timing

If a timing source is not of adequate quality or is lost (for instance, due to a cable pull), the C7 switches to holdover timing mode.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Compliant with GR-1244 (Section 5.2), Calix RAP cards ensure that holdover timing never degrades to worse than a Stratum 3 quality level after switching to holdover timing. If the Stratum 1 clock source is lost, the first frame slip can be expected to occur in 6 minutes, and up to 255 times in the next 24-hour period. In approximately 104 days, the clock signal would reach Stratum 3 stability of +/– 4.6 x 10^{-6}.

Timing automatically switches back from holdover to the configured timing mode when a timing source becomes available.

Timing Parameters

Line timing

- **Primary Timing Source**

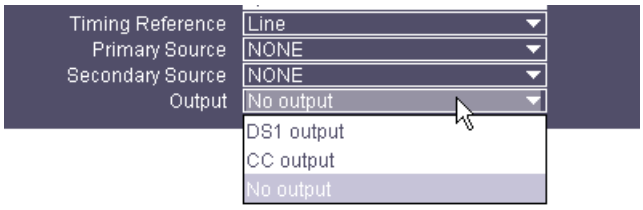
  When the Timing Reference is set to **Line**, this parameter indicates the working line of the primary timing interface.

- **Secondary Timing Source**

  When the Timing Reference is set to **Line**, this parameter indicates the working line of the secondary timing interface. If both the working and protect of the primary timing interface fail, this interface is used as the system timing source.

- **Output**

  The following parameters are associated with the timing interface (Output) when the Timing Reference is set to **Line (**or **Free run)**:



  - **DS1 output:** Use this setting to output external DS1 timing.
  - **CC output:** Use this setting to output composite clock timing.
  - **No output:** Use this setting to not output a timing signal.

- **DS1 Format**

  This parameter indicates the format for the transmitted and/or received timing DS1 signals. Options include:

  - **SF:** Superframe.
  - **ESF Not Synchronized:** Extended Superframe with no synchronous timing quality indication.
  - **ESF Synchronized:** Extended Superframe with synchronous timing quality indication.
  - **UF:** Unframed.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

External timing

- **Primary Derived DS1**

  Used to specify the source of the primary Derived DS1.

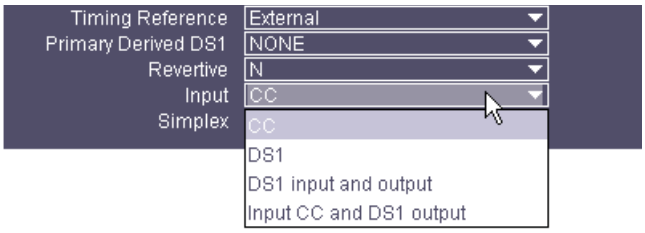
  Note: None indicates that no derived DS1 is to be generated.

- **Revertive**

  Set the Revertive parameter to **Y** (Yes) if timing should revert to the primary timing source when the primary timing source is restored after a failure. The default value is **N** (No).

- **Input**

  The following parameters are associated with the timing interface (Input) when the Timing Reference is set to **External**:



  - **CC** (composite clock): Composite clock is used as the source of system timing.
  - **DS1:** External DS1 is used as the source of system timing.
  - **DS1 input and output:** External DS1 is used as the source of system timing and output is DS1 timing.
  - **Input CC and DS1 output:** Composite clock is used as the source of system timing and output is DS1 timing.

- **DS1 Format**

  This parameter indicates the format for the transmitted and/or received timing DS1 signals. Options include:

  - **SF:** Superframe.
  - **ESF Not Synchronized:** Extended Superframe with no synchronous timing quality indication.
  - **ESF Synchronized:** Extended Superframe with synchronous timing quality indication.
  - **UF:** Unframed.

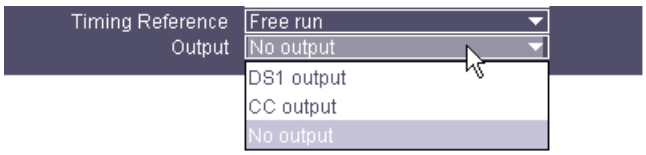
- **Simplex:** Set this to **Y** (Yes) if a redundant Composite Clock or external DS1 timing source is unavailable. This suppresses the alarm that would be generated due to a secondary timing source failure.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Freerun timing

- **Output**

  The following parameters are associated with the timing interface (Output) when the Timing Reference is set to **Free run**:



  - **DS1 output:** Use this setting to output derived DS1 timing.
  - **CC output:** Use this setting to output composite clock timing.
  - **No output:** Use this setting to not output a timing signal.

Configure Shelf Timing

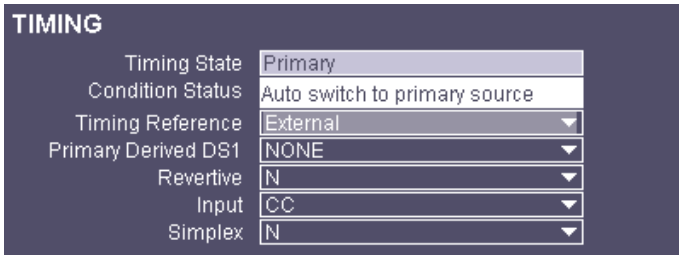
Complete the steps below to configure timing on a C7 shelf.

External timing configuration

This example assumes you are using a redundant external clock (Simplex-No), and that you do not want to revert to a primary timing source when the primary source is restored following a failure (Revertive-No).

To configure the shelf for external timing

1. On the Navigation Tree, click a shelf to set its timing mode.
2. In the Work Area, click **Shelf View**.
3. In the Timing panel:



   a. In the Timing Reference list, click **External**.

   b. In the Primary Derived DS1 list, verify the default value **None**.

   c. In the Revertive list, verify the default value **N**.

   d. In the Input list, select the appropriate timing interface.

   e. In the Simplex list, verify the default value **N**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

4. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your timing configuration for the shelf.

After configuring the shelf for external timing, the timing alarm for the shelf clears if timing sources are available.

UPSR protection for line timing

Complete the steps below to configure a C7 shelf with UPSR protection to use line timing from a working card.

To configure a shelf with UPSR protection for line timing

1. On the Navigation Tree, click a shelf to select it.
2. In the Work Area, click **Shelf View**.
3. In the Timing panel:
   a. In the Timing Reference list, click **Line**.
   b. In the Primary Source list, click a port to act as the primary timing source.
   c. In the Secondary Source list, click a port to act as the secondary timing source.
   d. In the Output list, select the output timing interface type.
4. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your timing configuration for the shelf.

LAPS protection for line timing

Complete the steps below to configure a C7 shelf with LAPS protection to use line timing from a working card.

Note: When using LAPS protection, both the primary and secondary timing sources must be working cards.

To configure the shelf with LAPS protection for line timing

1. On the Navigation Tree, click a shelf to select it.
2. In the Work Area, click **Shelf View**.
3. In the Timing panel, do the following:
   a. In the Timing Reference list, click **Line**.
   b. In the Primary Source list, click a port to act as the primary timing source.
   c. In the Secondary Source list, click a port to act as the secondary timing source.
   d. In the Output list, select the output timing interface type.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

4. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your timing configuration for the shelf.

Configure Timing for Third-Party Equipment

The C7 can function as a BITS Composite Clock (CC) or Timing Signal Generator (TSG) timing reference for third-party equipment. You can use the RAP2, RAP2-OCn, or RAP-10GE card to provide the following timing references:

- Composite Clock (CC) output
- DS1 output (non-traffic bearing)
- Derived DS1

The distance between the source of the CC (the TSG) and the third-party equipment receiving the CC signal must not exceed 1500 feet.

Complete the steps below to configure a C7 shelf to provide reference timing for third-party equipment.

To configure the shelf to provide timing to third-party equipment

1. On the Navigation Tree, click a C7 shelf to set its timing mode.
2. In the Work Area, click **Shelf View**.
3. In the Timing panel:
   a. In the Timing Reference list, click **External**.
   b. In the Primary Derived DS1 list, specify the source of the primary Derived DS1.

   Note: None indicates that no derived DS1 is to be generated.

   c. In the Revertive list, verify the default value **N**.
   d. In the Input list, click **DS1 input and output** or **Input CC and DS1 output**.

   Note: If the C7 shelf receives a timing reference from a BITS composite clock (CC), you can only set the shelf to provide a DS1 output timing reference.

   e. In the Simplex list, verify the default value **N**.

   Note: You can set Simplex to **Y** (Yes) if a redundant Composite Clock or external DS1 timing source is unavailable.
4. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your timing configuration for the shelf.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Holdover Timing

The C7 enters Holdover timed mode when one of the following conditions exists:

- All sources are disqualified in Line timed mode.
- Both sources are disqualified in External timed mode.

The Holdover timed mode asserts a frequency relative to the internal timing crystal, which had been previously calculated during a valid external or line timed mode. This averaging of frequency assures the accuracy of the output frequency of all interfaces of the C7, thereby achieving the goals of Stratum timing.

In Holdover mode, the SONET line interfaces are configured with Stratum 3 in their output messages since the holdover accuracy, transient, wander, and drift have been qualified to a Stratum 3 level. The average value disregards recent high levels of frequency or Total Immersion Excursion (TIE).

The C7 automatically recovers from holdover timing once a qualified timing source becomes available.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Shelf View—Bandwidth

The Shelf View provides consumed and available bandwidth information for the C7 shelf.

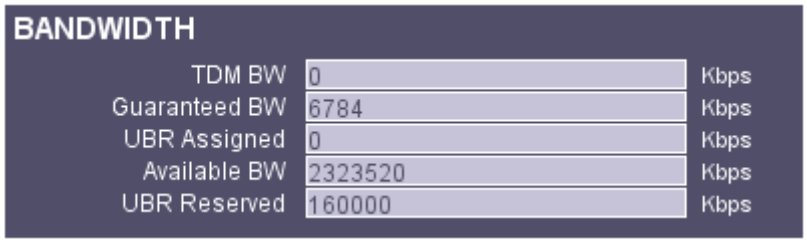
Note: Information in the Bandwidth panel is for display only and cannot be edited.

Bandwidth parameters

- **TDM BW:** Total TDM bandwidth currently consumed on the shelf (TDM bandwidth consists of voice traffic). This BW is allocated for TDM services to cards including, but not limited to, T1, VGP, and VIPR cards.
- **Guaranteed BW:** Total guaranteed bandwidth (excluding TDM) consumed on the shelf, allocated for cross-connects that use CBR or GFR traffic profiles.
- **UBR Assigned:** Total UBR bandwidth assigned to cards with UBR and UBR+ services. The system automatically defines and distributes this BW among C7 cards according to a weighted distribution.
- **Available BW:** Total bandwidth remaining that can be allocated for guaranteed services. This bandwidth includes the "UBR Assigned" BW, which means that provisioning more guaranteed services will decrease the amount of UBR bandwidth allocated to other cards.
- **UBR Reserved:** Total user-defined UBR bandwidth reserved for cards in the shelf. This reduces the amount of available bandwidth.

To view the Bandwidth panel

1. On the Navigation Tree, click the Shelf level.
2. In the Work Area, click **Shelf View** to display the Bandwidth panel.

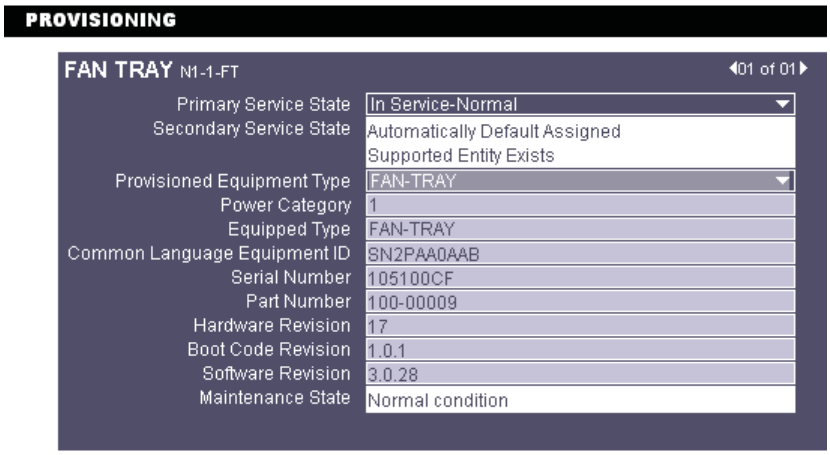


Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Viewing the Fan Tray

To view fan tray information

1. On the Navigation Tree, click the Shelf level, and then click **Fan Tray**.
2. In the Work Area, click **Provisioning** to display the Fan Tray panel.



Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring Equipment Protection

This section describes how to configure equipment protection for redundant cards. Equipment protection is optional.

Equipment Protection

What is equipment protection?

Equipment protection substitutes a backup card for an active card, if the active card fails. The backup card protects one or more cards of the same type located in the same C7 shelf.

Note: For RAP common control cards, the C7 system automatically configures equipment protection when cards are physically installed in the C7 shelf.

Equipment protection requires at least one pair of cards (designated as working and protect) operating together in a protection group.

- The working card is the primary active card that transmits and receives traffic.
- The protect card stands by and becomes active only if a failure occurs on the working card.

The C7 supports 1:1 and 1:N equipment protection schemes.

About 1:1 Equipment Protection

What is 1:1 protection?

With 1:1 equipment protection, you can pair one protect card with one working card of the same type. This association is called a protection group. If the working card fails, traffic from the working card switches to the protect card. Until the failure clears, the service is unprotected.

Note: The line cards in the Calix C7 cannot have any cross-connections to accept the configuration of equipment protection. Therefore, if you have a line card currently configured in a C7 shelf and intend to add equipment protection, you must reconfigure the card.

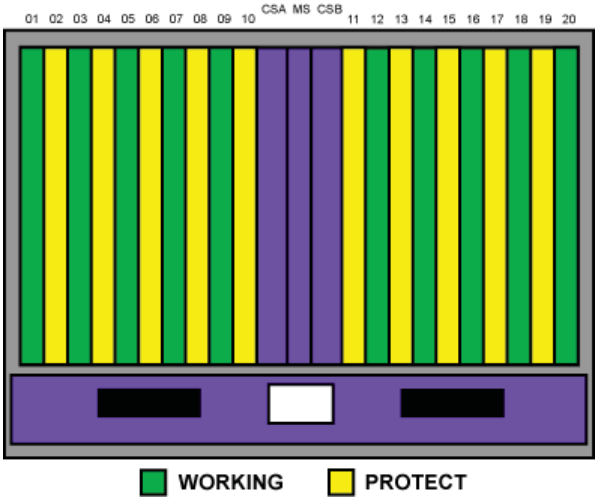
Reversion and 1:1 protection

Reversion allows for traffic to switch back to the original working card once the failure condition clears. The Revertive (RVRTV) parameter controls this capability. For 1:1 equipment protection, reversion is optional.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Card placement for 1:1 equipment protection

The C7 shelf is divided into a left side (slots 1 through 10) and a right side (slots 11 through 20). Card placement on the left side of the shelf mirrors card placement on the right side of the shelf. Slot assignments for 1:1 protection must use adjacent pairs.



Left side of shelf:

- Install working cards into odd-numbered slots (1, 3, 5, 7, or 9).
- Install protect cards into even-numbered slots (2, 4, 6, 8, or 10).
- A working card can only be protected by a card in the slot to its immediate right.

Right side of shelf:

- Install working cards into even-numbered slots (12, 14, 16, 18, or 20).
- Install protect cards into odd-numbered slots (11, 13, 15, 17, or 19).
- A working card can only be protected by a card in the slot to its immediate left.

Slot reference for 1:1 protection

The following table lists the working and protect slot assignments for 1:1 protection. The assignments also appear on the top edge of the fan tray, beneath the slots on each C7 shelf.

Slot # (left side)	Slot # (right side)	Plug-in Card (1:1)
Slot 1	Slot 20	Working
Slot 2	Slot 19	Protect
Slot 3	Slot 18	Working
Slot 4	Slot 17	Protect
Slot 5	Slot 16	Working

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Slot # (left side)	Slot # (right side)	Plug-in Card (1:1)
Slot 6	Slot 15	Protect
Slot 7	Slot 14	Working
Slot 8	Slot 13	Protect
Slot 9	Slot 12	Working
Slot 10	Slot 11	Protect

About 1:N Equipment Protection

What is 1:N protection?

With 1:N equipment protection, you can pair one protect card with up to nine working cards (1:9) of the same type. This association is called a protection group. For VIPR cards only, the 1:N equipment protection allows you to pair one protect card with up to three working cards (1:3). If any working card fails, traffic from the working card switches to the protect card. Until the failure clears, the service is unprotected.

Note: The line cards in the Calix C7 cannot have any cross-connections to accept the configuration of equipment protection. Therefore, if you have a line card currently configured in a C7 shelf and intend to add equipment protection, you must reconfigure the card.

Reversion and 1:N protection

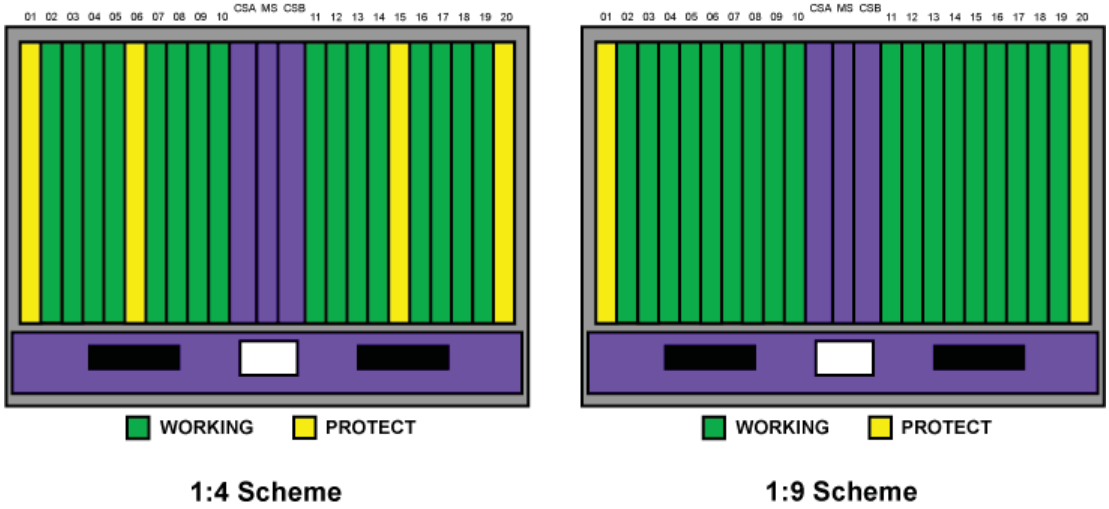
Reversion allows for traffic to switch back to the original working card once the failure condition clears. The Revertive (RVRTV) parameter controls this capability. For 1:N protection, reversion is required. Use the Redundancy Priority (RNPRTY) parameter to prioritize specific working cards for protection within a group by assigning priority numbers.

Card placement for 1:N equipment protection

The C7 shelf is divided into a left side (slots 1 through 10) and a right side (slots 11 through 20). Card placement on the left side of the shelf mirrors card placement on the right side of the shelf. Slot assignment for 1:N protection requires consecutive adjacent slots from the protect card inward, toward the center of the shelf. The protect card always sits outside of the working cards it protects.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Each side of a shelf can host up to two 1:N protection groups—either a single protection group of up to 9 working cards (1:9 scheme) or two protection groups of up to 4 working cards apiece (1:4 scheme) or in the case of VIPR cards, 3 working cards apiece. You may use fewer than the maximum number of cards per 1:N protection group, provided the working cards occupy the inward slots adjacent to the protect card.



Left side of shelf:

1:4 scheme:

- Install protect cards into slots 1 or 6.
- For a protect card in slot 1, install up to 4 working cards into slots 2–5 in ascending order (2, 3, 4, 5).
- For a protect card in slot 6, install up to 4 working cards into slots 7–10 in ascending order (7, 8, 9, 10).
- Slots 3–5 or 8–10 may house working cards only if the slot to the immediate left of each also contains a working card.

1:9 scheme:

- Install a protect card into slot 1.
- Install up to 9 working cards into slots 2–10 in ascending order (2, 3, 4, 5, 6, 7, 8, 9, 10).
- Slots 3–10 may house working cards only if the slot to the immediate left of each also contains a working card.

Right side of shelf:

1:4 scheme:

- Install protect cards into slots 15 or 20.
- For a protect card in slot 15, install up to 4 working cards into slots 11–14 in descending order (14, 13, 12, 11).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- For a protect card in slot 20, install up to 4 working cards into slots 16–19 in descending order (19, 18, 17, 16).
- Slots 11–13 or 16–18 may house working cards only if the slot to the immediate right of each also contains a working card.

1:9 scheme:

- Install a protect card into slot 20.
- Install up to 9 working cards into slots 11–19 in descending order (19, 18, 17, 16, 15, 14, 13, 12, 11).
- Slots 11–18 may house working cards only if the slot to the immediate right of each also contains a working card.

Slot Reference for 1:N Protection

The following table lists the working and protect slot assignments for 1:N protection. The assignments also appear on the top edge of the fan tray, beneath the slots on each C7 shelf.

Slot # (left side)	Slot # (right side)	Plug-in Card (1:4)	Plug-in Card (1:9)
Slot 1	Slot 20	Protect	Protect
Slot 2	Slot 19	Working	Working
Slot 3	Slot 18	Working	Working
Slot 4	Slot 17	Working	Working
Slot 5	Slot 16	Working	Working
Slot 6	Slot 15	Protect	Working
Slot 7	Slot 14	Working	Working
Slot 8	Slot 13	Working	Working
Slot 9	Slot 12	Working	Working
Slot 10	Slot 11	Working	Working

Note: Slot assignments for the 1:4 scheme also apply to 1:3 and 1:2 schemes. Slot assignments for the 1:9 scheme also apply to 1:8, 1:7, 1:6, and 1:5 schemes. Any slot not included in a protection group can be used for general purposes.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Metallic Services Protection Modules

Use Metallic Services Protection (MSP) modules to protect C7 metallic interface cards (DS1, DS3, HDSL) in a C7 shelf.

Metallic Services Protection Modules

To enable equipment protection for metallic interface cards, the C7 uses Metallic Services Protection (MSP) modules installed in the C7 shelf. The MSPs allow the C7 to switch protected services to the backup card in a protection group if the active card experiences a failure. You can install up to two MSPs per shelf.

One MSP module provides protection for half of the C7 shelf: MSP-A for the left side and MSP-B for the right side. The MSP-A and MSP-B units are not interchangeable. The modules slide in behind the fan tray and connect directly into connectors on the backplane. Insert or remove the MSP modules using ejector mechanisms similar to a plug-in card ejector.

Are MSPs required?

MSP modules are only required for C7 metallic interface cards when supporting 1:N equipment protection schemes or 1:1 protection schemes using slots 5 and 6 or 15 and 16. Metallic interface card protection includes DS1, DS3 (DS3E-4p and DS3-12s cards only), HDSL, and IMA-12 cards. The standard C7 shelf supports 1:1 metallic protection without the use of an MSP, with the exception of protection between slots 5/6 and 15/16. The 1:N metallic protection scheme requires an MSP.

Non-metallic interface cards **do not** require the use of MSPs to support equipment protection. Cards that are able to be protected but do not require MSPs include optical interface cards as well as IRC, VIPR, and VGP cards.

Protected Services

You can mix protected and unprotected service types on a protected T1 card. However, only the protected service types are protected if the card fails. The following DS3 and T1 services can be protected by a metallic equipment protection group:

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- **T1-8 PWE:** Hi-Cap T1s (powered and non-powered), fractional T1 service, GR-08 spans, and D4 spans.
- **T1-6 A+T:** UNI/NNI T1s (powered and non-powered), clear-channel T1s (powered and non-powered), channelized T1, T1s in IMA groups (powered and non-powered), and GR-08 spans.
- **T1-6:** Clear-channel T1s (powered and non-powered), channelized T1, and GR-08 spans.
- **DS1-12 PWE:** Hi-Cap T1s (powered and non-powered), fractional T1 service, GR-08 spans, and D4 spans.
- **DS1A-12:** All services
- **DS3E-4p:** All services
- **DS3-12s:** All services
- **IMA-12:** All services

The following services cannot be protected by a metallic equipment protection group:

- **T1-8 PWE:** GR-303 spans, T1TG spans
- **T1-6 A+T:** GR-303 spans, T1TG spans
- **T1-6:** GR-303 spans, T1TG spans
- **DS1-12 PWE:** GR-303 spans, T1TG spans
- **DS3-12p:** No services protected

MSP Installation Requirements

Install metallic services protection modules to support 1:N equipment protection schemes or 1:1 protection schemes using slots 5 and 6 or 15 and 16. MSP-A and MSP-B are not interchangeable. Install the MSP modules as follows:

- Insert MSP-A into the left side of the shelf. MSP-A provides protection for slots 1 through 10 only.
- Insert MSP-B into the right side of the shelf. MSP-B provides protection for slots 11 through 20 only.

Configuring 1:1 Equipment Protection

This section describes how to configure redundant cards into a 1:1 protection group.

Equipment protection parameters

Use the following parameters to configure equipment protection for redundant cards.

Protection Unit (PROTN): Specifies the slot address of the protect card. See the Card ID parameter.

Redundancy Priority (RNPRTY): Not applicable. This parameter applies to 1:N protection only.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Revertive (RVRTV): Specifies whether the system switches traffic back to the original working card once the failure condition clears. The default value is N.

- Enter **Y** to automatically switch traffic back to the original working card once the failure condition clears.
- Enter **N** to continue carrying traffic on the protect card once the failure condition clears.

Before you configure 1:1 protection

Verify correct slot placement of working and protect cards for 1:1 equipment protection before continuing.

1:1 protection group configuration

To configure a 1:1 protection group

1. On the Navigation Tree, click the C7 shelf containing the cards to configure.
2. On the File menu, click:
   - (in iMS) **Create** > **Protection** > **Equipment Protection**
   - (in CMS) **Create** > **C7** > **Protection** > **Equipment Protection**
3. In the Protect dialog box:
   a. In the Shelf list, select the shelf to configure.
   b. In the Card Type list, select the card type to configure.

   Note: The specified cards appear in the table at the bottom of the window. By default, all cards initially display **W** (Working) in the Select W/P row.
4. Configure the protect card:
   a. On the slot number table, locate the column for the protect card slot.
   b. In that column, on the Select W/P row, click **P** (Protect).
   c. (Optional) On the Revertive row, click **Y** (Yes) to enable equipment reversion.
5. Configure the working card:
   a. On the slot number table, locate the column for the working card slot.
   b. In that column, on the PROTN row, click the slot number of the protect card.
   c. In that column, on the Priority row, click **N** for no priority. (Because the IRC only supports 1:1 protection, there is no priority.)
6. Click **OK** to save your settings.

Removing cards from a 1:1 protection group

You may remove a card from a protection group only if no cross-connects exist on the card.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

To remove cards from a 1:1 protection group

1. On the Navigation Tree, click the working card in the protection group.
2. In the **Provisioning** Work Area:
   a. In the Primary Service State list, click **OOS** to take the card out of service.
   b. In the Protection Unit list, click **NONE**.
   c. On the toolbar, click **Apply** to update settings. In the Confirmation dialog box, click **OK**.
3. On the Navigation Tree, click the protect card in the protection group.
4. Repeat Step 2 for the protect card.
5. To place an unprotected card back in service, do the following:
   a. On the Navigation Tree, click the card to modify.
   b. In the **Provisioning** Work Area, in the Primary Service State list, click **IS**.
   c. On the toolbar, click **Apply** to update settings. In the Confirmation dialog box, click **OK**.

Configuring 1:N Equipment Protection

This section describes how to configure redundant cards into a 1:N protection group.

Equipment protection parameters

Use the following parameters to configure equipment protection for redundant cards.

Protection Unit (PROTN): Specifies the slot address of the protect card. See the Card ID parameter.

Redundancy Priority (RNPRTY): This parameter applies to 1:N protection only. It is used to set the priority of working cards within the same protection group by assigning a priority number from 1 to 9. A lower number equals higher priority. Cards assigned a lower number will preempt any protection already in effect for cards with a higher number. The default value is 5.

Revertive (RVRTV): Specifies whether the system switches traffic back to the original working card once the failure condition clears. The default value is N.

- Enter **Y** to automatically switch traffic back to the original working card once the failure condition clears.
- Enter **N** to continue carrying traffic on the protect card once the failure condition clears.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Before you configure 1:N protection

Verify correct slot placement of working and protect cards for 1:N equipment protection before continuing. For guidelines, see *About 1:N Equipment Protection* (on page 195).

1:N protection group configuration

To configure a 1:N protection group

1. On the Navigation Tree, click the shelf containing the cards to configure.
2. On the File menu, click:
   - (in iMS) **Create** > **Protection** > **Equipment Protection**
   - (in CMS) **Create** > **C7** > **Protection** > **Equipment Protection**
3. In the Protect dialog box:
   a. In the Shelf list, select the shelf to configure.
   b. In the Card Type list, select the card type to configure.

   Note: The specified cards appear in the table at the bottom of the window. By default, all cards initially display **W** (Working) in the Select W/P row.
4. Configure the protect card:
   a. On the slot number table, locate the column for the protect card slot.
   b. In that column, on the Select W/P row, click **P** (Protect).
   c. In that column, on the Revertive row, click **Y** (Yes) to enable equipment reversion.
5. Configure each working card:
   a. On the slot number table, locate the column for the working card slot.
   b. In that column, on the PROTN row, click the slot number of the protect card.
   c. In that column, on the Priority row, click a priority number for this working card.
6. Click **OK** to save your settings.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Removing cards from a 1:N protection group

You may remove a card from a protection group only if no cross-connects exist on the card.

To remove cards from a 1:N protection group

1. On the Navigation Tree, click a working card in the protection group.
2. In the **Provisioning** Work Area, do the following:
   a. In the Primary Service State list, click **OOS** to take the card out of service.
   b. In the Protection Unit list, click **NONE**.
   c. On the toolbar, click **Apply** to update settings. In the Confirmation dialog box, click **OK**.
3. Repeat Steps 1 and 2 for each working card in the protection group.
4. On the Navigation Tree, click the protect card in the protection group.
5. Repeat Step 2 for the protect card.
6. To place an unprotected card back in service, do the following:
   a. On the Navigation Tree, click the card to modify.
   b. In the **Provisioning** Work Area, in the Primary Service State list, click **IS**.
   c. On the toolbar, click **Apply** to update settings. In the Confirmation dialog box, click **OK**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Protection Switching User Commands

Protection switching provides failure protection for redundant equipment. This section describes how to manage protection switching operations for C7 equipment.

You can use the switching commands to manually control the operational states of redundant equipment, including applying and removing state-change restrictions to specific units and manually executing protection switches.

Typically, protection switching can operate in either revertive or non-revertive mode. In revertive mode, service and functionality are automatically restored to the original working facility when the failure condition clears. In non-revertive mode, the protection facility continues to perform in working mode until a user-initiated intervention occurs.

Guidelines for Using Equipment Protection Switching

Use the following guidelines to effectively operate equipment protection switching:

- Secondary Service State (SST) STBYS (standby switched) is only used for a protect card with revertive protection. This indicates that the protect card is active due to a manual switch.
- There are six SSTs that apply to equipment protection:
  - WRK (working)
  - NBK (no backup)
  - STBYH (standby hot)
  - STBYC (standby cold)
  - STBYI (standby inhibited)
  - STBYS (standby switched)
- An inhibit switch command on a 1:N protection group effectively disables switching for the entire group.
- Switching commands for equipment protection can only be used when the entities are in appropriate secondary states. The table below shows each equipment protection switching command, the target equipment of the command, the required SST of the target equipment, and the result of the command.
- Avoid pulling an active card from a shelf. Instead, perform a 'soft' protection switch, and then remove the card after the switchover completes and the card enters standby mode.

Note: *STBYx* can be SST of STBYH, STBYC, or STBYS as appropriate.

Switch Command	Target of the Command	Required SST of the Target Card	Result of the Command
Allow Switch to Working	Primary card	STBYI	Primary card transitions to SST of

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Switch Command	Target of the Command	Required SST of the Target Card	Result of the Command
			STBYx. Switching is enabled if SST is STBYH.
Allow Switch to Protection	Protect card	STBYI	Protect card transitions to SST of STBYx. Switching is enabled if SST is STBYH.
Allow Switch Duplex	RAP card	STBYI	Standby RAP transitions to STBYx. Switching is enabled if SST is STBYH.
Inhibit Switch to Working	Primary card	STBYx	Primary card transitions to SST of STBYI. Switching is disabled.
Inhibit Switch to Protection	Protect card	STBYx	Protect card transitions to SST of STBYI. Switching is disabled.
Inhibit Switch to Duplex	RAP card	STBYx	Standby RAP card transitions to STBYI. Switching is disabled.
Switch to Protect	Primary card	WRK	Service switches to Protect card.
Switch to Working	Protect card	WRK	Service switches back to Primary card.
Switch to Duplex	RAP card	WRK	Common control function switches to the other RAP card.

See *Secondary Service State* (on page 577) for additional information.

Switching Commands

You can allow, inhibit, and execute protection switching operations from the GUI. The related commands are described below:

Allow > **Switch to Working:** Permits a protection unit in 1:1 or 1:n protection schemes to switch to working mode, if required. Use this command to release a protection unit from an inhibit-switching state (that is, after an **Inhibit** > **Switch to Working** command has been applied).

Allow > **Switch to Protection:** Permits a working unit in 1:1 or 1:n protection schemes to switch to protection mode, if required. Use this command to release a working unit from an inhibit-switching state (that is, after an **Inhibit** > **Switch to Protection** command has been applied).

Allow > **Switch Duplex:** Permits redundant RAP cards to switch between active and standby modes by releasing the RAPs from an inhibit-switching state (that is, after an **Inhibit** > **Switch Duplex** command has been applied). Apply this command to the standby RAP only.

Note: For RAP-OC cards (equipped with an optical interface port), only the control processing functions of the RAP card are affected by the **Allow** > **Switch Duplex** command. RAP optical facilities must be provisioned for protection separately (as part of a Facility Protection Group), and are not affected by the **Allow** > **Switch Duplex** command.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Inhibit > **Switch to Working:** Restricts a protection unit from switching to working mode in 1:1 or 1:n protection schemes. To release a protection unit from the inhibit-switching state, use the **Allow** > **Switch to Working** command.

Inhibit > **Switch to Protection:** Restricts a working unit from switching to protection mode in 1:1 or 1:n protection schemes. To release a working unit from the inhibit–switching state, use the **Allow** > **Switch to Protection** command.

Inhibit > **Switch Duplex:** Restricts redundant RAP cards from switching between active and standby modes. To release the RAPs from the inhibit–switching state, apply the **Allow** > **Switch Duplex** command to the standby RAP. Apply this command to the standby RAP only.

Note: For RAP-OC cards (equipped with an optical interface port), only the control processing functions of the RAP card are affected by the **Inhibit** > **Switch Duplex** command. RAP optical facilities must be provisioned for protection separately (as part of a Facility Protection Group), and are not affected by the **Inhibit** > **Switch Duplex** command.

Switch > **Switch to Working:** Performs a manual switch of a protected service from a protection unit to a working unit in 1:1 or 1:n protection schemes.

Switch > **Switch to Protection:** Performs a manual switch of a protected service from a working unit to protection unit in 1:1 or 1:n protection equipment schemes.

Switch > **Switch Duplex:** Performs a manual switch of active and standby modes between redundant RAP cards. Apply this command to the active RAP only. Operating a Switch Duplex command on a RAP card opens the Confirm Reset Equipment dialog box. You can select the **Force** check box to request a forced switch even if otherwise prohibited.

Note: For RAP-OC cards equipped with an optical interface port, performing a duplex switch only switches the control processing functions to the standby RAP card. To switch the optical transport services, you must initiate a SONET line protection switch. User-initiated switch commands (that is, **Forced**, **Lockout**, and **Manual** switches) remain active until released by the **Release Switch** command or overridden by a higher priority protection switch request. See *Facility Level Protection Switching* (on page 350) for additional information.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Chapter 5

Provisioning Network Transport

This section provides information on protecting traffic on optical fibers, protection configurations, 1+1 Linear Automatic Protection Switching (LAPS), and 1:1 LAPS. Additionally, detailed information is provided for configuring:

- Ethernet Ring Protection Switching (ERPS) transport ring
- Rapid Spanning Tree Protocol (RSTP) Ethernet transport ring
- Linear Ethernet Transport with RSTP or Link Aggregation Group (LAG)
- UPSR with Packet Aggregation
- DS3p Transport Links
- T1 IMA
- T1 Transport Groups

See also

- *Configuring Ethernet Transport* (on page 310)

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Overview of Transport Protection

Protecting Traffic on Optical Fibers

Facility protection switching improves the survivability of networks by substituting a standby facility when failures occur. You can configure the C7 to protect traffic that flows over any optical facility.

Optical ports cannot be configured to protect ports located on the same card. When configuring optical port protection, the system automatically designates an optical port on an adjacent card as the protect path. Therefore, you must install an optical card of the same type in the appropriate slot next to the optical card with the working port. For more information about equipment protection schemes, see *Configuring Equipment Protection (on page 193)*.

Supported protection configurations

The C7 supports both line and path traffic protection configurations:

- A line is the transmission medium and the associated equipment that transports information between two nodes: one that originates the line signal and one that terminates it.
- A path is the logical end-to-end connection through a network.

Line protection configurations

The C7 supports the following types of line protection:

- 1+1 Linear Automatic Protection Switching (LAPS 1+1)
- 1:1 Linear Automatic Protection Switching (LAPS 1:1)

Note: Calix recommends the use of LAPS 1+1.

Note the following configuration rules for LAPS 1:1:

- Once cross-connects have been established, LAPS 1:1 cannot be upgraded to LAPS 1+1.
- Cross-connects from a GE-2p card to a LAPS 1:1 connection in the same shelf are not supported.
- LAPS 1:1 connections cannot participate as a drop or multicast for STS cross-connects.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Path protection configurations

The C7 supports the following types of path protection:

- Unidirectional Path Switched Ring (UPSR) with Packet Aggregation (SONET and packet traffic)
- Ethernet Ring Protection Switching (ERPS)
- Rapid Spanning Tree Protocol (RSTP)

Bridged and unbridged protection

Bridged protection uses both the working and the protect paths. The system duplicates the traffic and sends it over the working and the protect paths at the same time. This kind of protection is also called **1+1** protection because it uses both paths.

Unbridged protection sends traffic over the working path until there is a failure. When there is a failure, the system switches traffic to the protect path. The traffic remains unprotected until service is restored on the working path. Unbridged protection is referred to as **1:1** protection because the protect path is available for extra traffic until there is a failure.

Extra traffic and 1:1 protection

Because 1:1 protection switches traffic to the protect path only when the working path fails, you can configure extra, low-priority traffic to be sent over the protect path until there is a failure. On failure, the system drops the extra traffic and begins to transmit the regular traffic over the protect path.

Unidirectional and bidirectional protection

In both bridged (1+1) and unbridged (1:1) protection configurations, you configure a working path and a protect path for both the transmit and receive directions. You can choose either unidirectional or bidirectional protection.

With unidirectional protection, when the working path fails (either transmit or receive), the system switches the traffic from the working path to the protect path. Traffic in the other direction remains unaffected.

With bidirectional protection, when the working path fails (either transmit or receive), the system switches both working paths to the protect paths.

Just because your traffic is bidirectional does not mean your transport protection needs to be bidirectional. In fact, unidirectional protection is the better option in most cases because unidirectional protection switching happens faster.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

System reversion

The ability of the system to switch traffic back to the original active link once the failure condition clears is user-configurable. The revertive (RVRTV) parameter controls this capability.

The wait-to-restore (WTR) parameter specifies the amount of time (in minutes) for the system to wait before restoring the working port.

Facility-level protection switching

The system provides the capability to initiate a SONET line or path protection switch request. User switch requests are initiated with these commands:

- **Lockout:** Lockout of protection line, lockout of working line, or lockout for path protection switching.
- **Forced:** Forced switch of working line to protection line, force switch of protection line to working line, or forced path protection switch.
- **Manual:** Manual switch of working line to protection line, manual switch of protection line to working line, or manual path protection switch.

UPSR with Packet Aggregation

SONET ring topologies are fully protected from both equipment and facility failures, making them the most robust topology from a network availability standpoint. The C7 supports SONET Unidirectional Path Switched Ring (UPSR) with distributed packet aggregation (known as UPSR with Packet Aggregation). Typically in a UPSR SONET ring, fixed quantities of bandwidth in 50 Mbps (STS-1) increments must be nailed up between each Remote Terminal (RT) and Central Office Terminal (COT). Thus, if each of four RTs required 10 Mbps of capacity to a COT, a total of 200 Mbps (4 x 50 Mbps) of bandwidth would have to be allocated from the total capacity of the ring (1 STS-1 per RT).

The packet aggregation capability of the C7 allows a single SONET payload (STS-1, STS-3c, STS-12c, and so forth) to be shared by multiple shelves on a ring for packet-based traffic. Since the C7 packetizes POTS traffic within the network, the four-RT configuration would require only one STS-1, preserving the capacity of the ring for future growth. New nodes can be added to an existing SONET ring at any time without disrupting service to existing customers.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

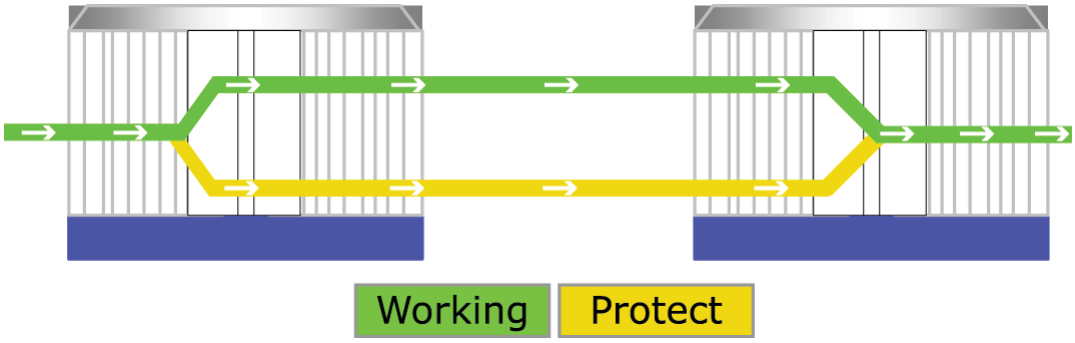
1+1 Linear Automatic Protection Switching

You can protect a network of C7 shelves using 1+1 Linear Automatic Protection Switching (LAPS).

Note: Calix strongly recommends a LAPS 1+1 bi-directional protection scheme for optical interfaces that require protection.

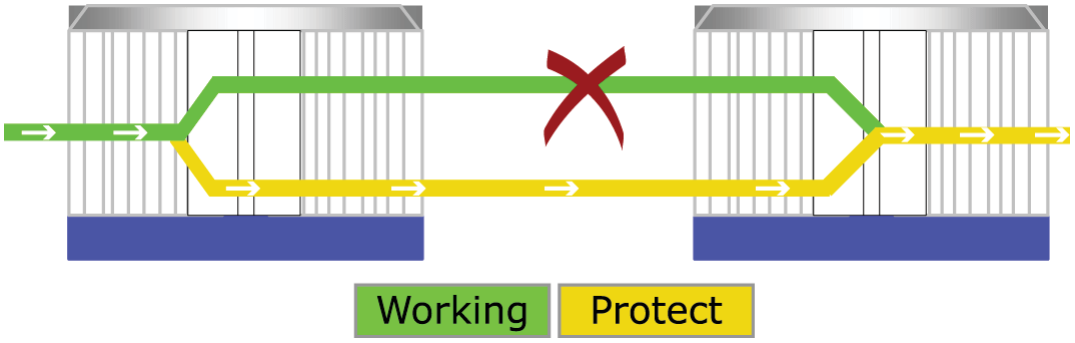
LAPS 1+1 in normal operation

Bridged (1+1) protection uses both the working and the protect lines (fibers) to send traffic simultaneously to the next node. That is, the system duplicates the traffic and sends it over both the working and the protect lines at the same time.



LAPS 1+1 failure scenario

With bridged protection, when the system detects a failure on the working line, the receiving shelf switches to select traffic from the protect line. The line remains unprotected until service is restored on the working line.



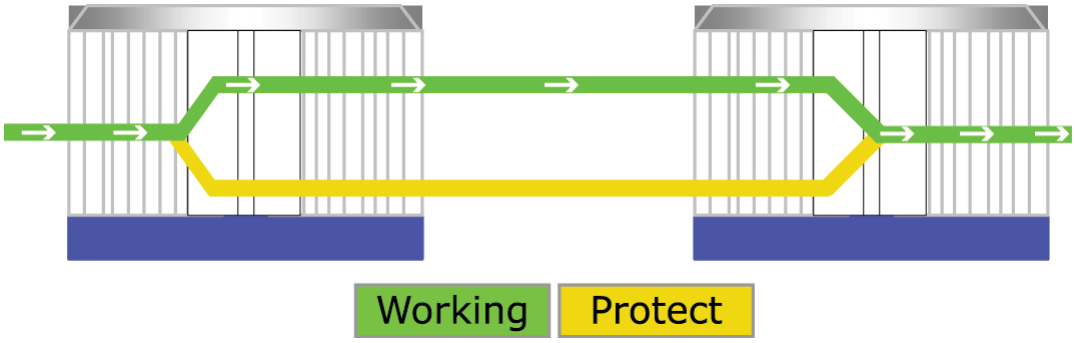
Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

1:1 Linear Automatic Protection Switching

You can protect a network of C7 shelves using 1:1 Linear Automatic Protection Switching (LAPS).

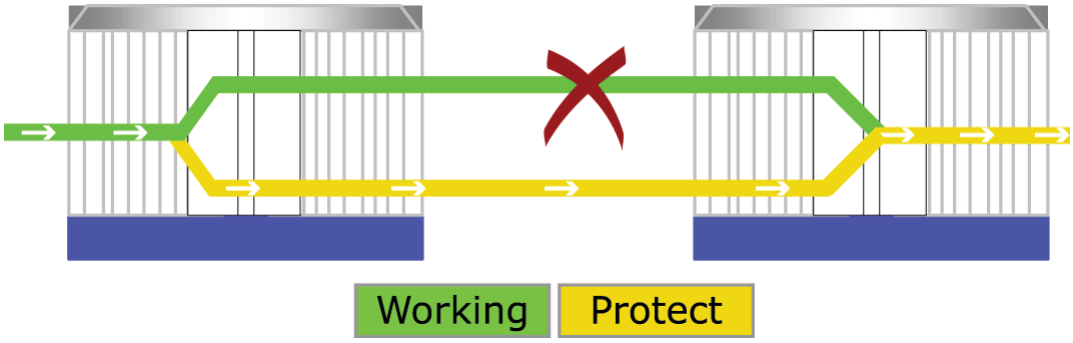
LAPS 1:1 in normal operation

Unbridged (1:1) protection sends traffic over the working line (fiber) until there is a failure. When there is a failure, the system switches traffic to the protect line. The service remains unprotected until the working line is restored.



LAPS 1:1 failure scenario

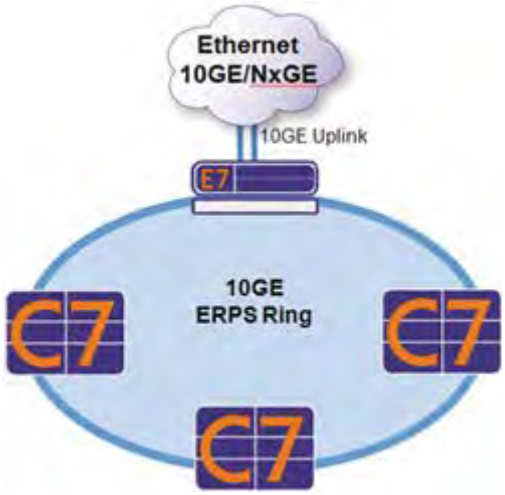
With unbridged protection, when the system detects a failure on the working line, the receiving shelf switches to select traffic from the protect line. The service remains unprotected until the working line is restored.



Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring an ERPS Transport Ring

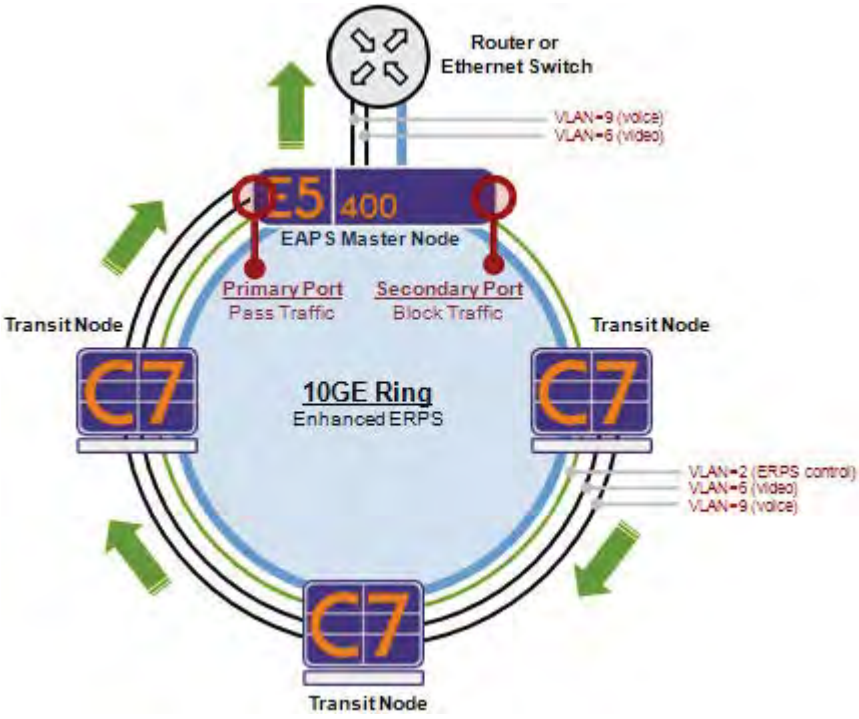
With the RAP-10GE, the C7 allows for provisioning of Ethernet Ring Protection Switching (ERPS), a ring protection protocol. You can configure an ERPS domain to protect a group of virtual local area networks (VLANs) that carry traffic around a transport ring of 1GE interfaces or 10GE interfaces. Typically, a 10GE ERPS ring is used for the main transport ring with an E7 providing a protected 10GE uplink. Up to a total of 16 nodes (C7 or E7) are allowed in a single ERPS ring.



Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

ERPS ring VLAN configuration

When an ERPS ring is provisioned, the service VLANs and the control VLAN that passes control packets between all the nodes of the ring are provisioned on each node of the ring. Multiple VLANs can be configured across the same physical ring for further separation of traffic. For example, two logical VLANs can be configured for data and video traffic.



ERPS ring normal operation

With ERPS, one node in the ring is designated as the ring master and all other nodes are considered transit nodes. The master node is responsible for protecting the Ethernet ring from network loops as well as coordinating the flushing of bridging tables. During normal operation, the entire VLAN group assigned to an ERPS ring is enabled on the primary port and blocked on the secondary port of the ring, as shown in the following diagram.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

ERPS Ring Topology—Normal Operational Model

ERPS ring failure detection

The ERPS protocol allows three methods of detecting a ring failure:

- Loss of signal from the link which generates a link down message
- Master node detects loss of network / ring heartbeat
- IEEE 802.1ag connectivity check message can generate a link down message

When an ERPS ring is created, a control VLAN is created on each node in the ring. This control VLAN passes control packets between all the nodes of the ring. The master node uses this control VLAN to send health packets around the ring.

The master node then looks for the receipt of the health PDU on the secondary port. If the health PDU is not received in the designated timeframe, a ring failure is declared. When a ring failure occurs, the master node flushes its bridging table for the ring-based VLANs, except the control VLAN. The master node then enables the secondary port for the ring-based VLANs and instructs the transit nodes to flush their local bridging tables and begins learning the new topology. The following diagram illustrates the change in traffic flow when a network link failure occurs.

ERPS Ring Topology—Network Link Failure Mode

Configuration Rules for an ERPS Transport Ring

Follow these guidelines when configuring an Ethernet transport ring with ERPS:

- A single ERPS ring is supported per C7 system.
- An ERPS ring supports up to 16 shelves (C7 and E7 combined).
- Designate one node in the ring as the master node.
- Designate the remaining nodes in the ring as transit nodes.
- On the master node, designate a primary and secondary port.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- All Ethernet ports in an ERPS ring must be the same speed (all GE ports or all 10GE ports).
- Configure the following parameters for each node in an ERPS ring:
  - Designate a control VLAN with the same ID on each node.
  - Create service VLANs on each node and then associate the VLANs to the ERPS domain.
  - For video traffic, all nodes in an ERPS ring must have the same IGMP snoop configuration on the VLAN—either all enabled or all disabled.
- Select a control VLAN ID that is NOT used for any services on the network.
- The ERPS ring control VLAN passes only ERPS control protocol data units and heartbeats; it cannot be provisioned to pass subscriber traffic.
- IGMP is enabled for all ports designated as ring ports if the ports belong to the same VLAN.

Note: The RAP-10GE card's Ethernet ports interface to the Local Bridge (EXA switch fabric) only. To forward traffic to/from a C7 Virtual Bridge (for services delivery on the C7 Multiprotocol architecture) currently requires a physical Ethernet link between the 1GE ports on a RAP-10GE card and a VB-based Ethernet line card, with all involved ports (10GE, 1GE, 1GE) added to the same service VLAN ID(s).

Quick Turn-Up Outline for ERPS Transport

Use this quick turn-up outline to get an ERPS transport ring for 10GE traffic up and running.

Starting point

Before starting this quick turn-up process, check to see that the following conditions are met:

- All shelves in the ring transport network have been installed and powered.
- AMP (or ATP) and RAP-10GE cards have been installed in the C7 shelves.
- Cables have been connected between the RAP-10GE cards in each C7 shelf around the ring.
- The network uplink (E7) for the ring has been configured.

Quick turn-up steps

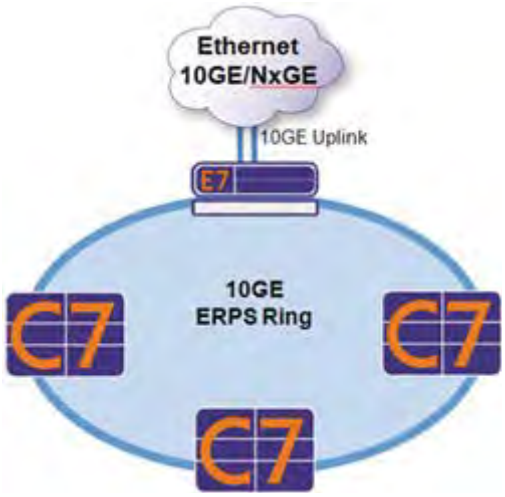
1. Configure your computer to connect to the front Ethernet port (E1) on a C7 AMP or ATP card.
2. Connect to the E1 port and start the management software.
3. Define network nodes.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

4. Set shelf timing for all C7 shelves. See *Configure Shelf Timing* (on page 187) for instructions.
5. Create and configure ERPS domain on each shelf for the transport ring.
   a. Create the ERPS domain that includes the Ethernet ports, control VLAN, and node role (Master or Transit).
   b. Create the service VLANs.
   c. Create a VLAN interface by setting the role for Ethernet ring ports to trunk and adding the ERPS domain to the service VLANs.
   d. Add any uplink or downlink Ethernet port interfaces to service VLANs.

Configure an ERPS Transport Ring

This topic describes how to configure an ERPS 10GE transport ring with multiple C7 shelves and utilizing an E7 as the ring uplink.



Before starting the configuration

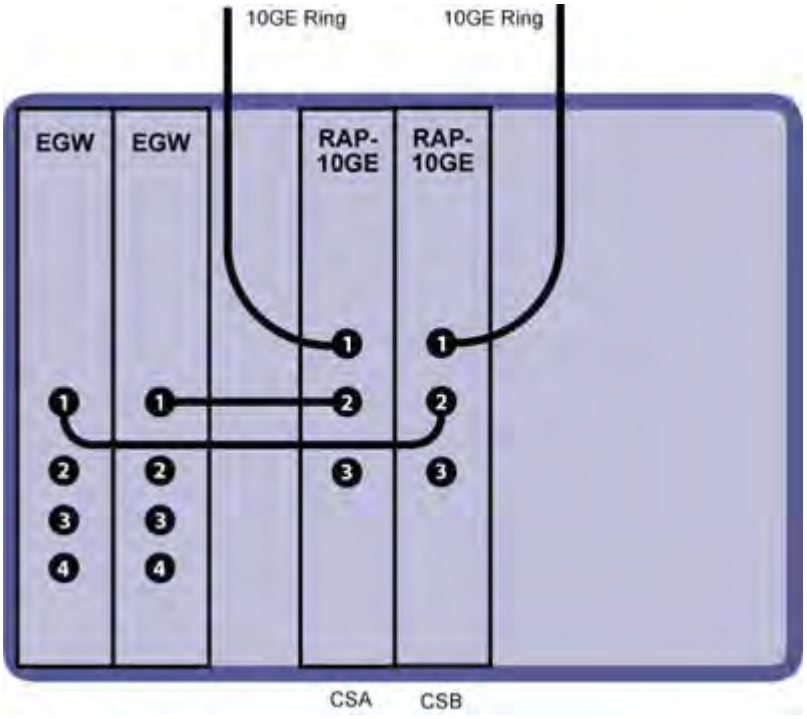
Before you begin the ERPS configuration process, determine the ERPS domain configuration and connect the equipment in a transport ring:

- Connect the nodes in a ring configuration:
  - Connect the Primary port of the master node to the interface port of the transit node.
  - Connect the interface port of each transit node to the interface port of the next transit node.
  - Complete the ring by connecting the last interface port of the last transit node to the Secondary port of the master node.
- Connect an E7 node as the uplink for the ring, using redundant 10GE links.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- Determine the following aspects of the ERPS domain:
  - The domain name
  - Which node to designated as the master node
  - The control and service VLAN IDs that you will use for each node

    For example:
    - "10GE Ring" for Domain Name
    - VLAN 10 for ERPS control
    - VLAN 11 for Video
    - VLAN 12 for VoIP
    - VLAN 13 for Data
- Ensure the RAP-10GE cards (2) are installed in the C7 shelves for the transport ring.



Note: The RAP-10GE card's Ethernet ports interface to the Local Bridge (EXA switch fabric) only. To forward traffic to/from a C7 Virtual Bridge (for services delivery on the C7 Multiprotocol architecture) currently requires a physical Ethernet link between the 1GE ports on a RAP-10GE card and a VB-based Ethernet line card, with all involved ports (10GE, 1GE, 1GE) added to the same service VLAN ID(s).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

ERPS domain parameters

You can provision the following parameters for a node configured in an ERPS domain:

Parameter	Description	Valid Options
Source shelf	System address of the shelf to add to the ERPS domain. The identifiers consist of: (Node#)-(Shelf#)	Any node/shelf connected in the ERPS ring.
Address	System address of the ERPS domain to create. The identifiers consist of: (Node#)-(Shelf#)-(ERPS#).	Match of the node/shelf selected for source shelf, plus ERPS#.
Primary Slot	Address of the slot location for the primary interface to the ring. The identifiers consist of: (Node#)-(Shelf#)-(CS#).	Match of the node/shelf selected for source shelf, plus CSA or CSB.
Primary	Address of primary interface to the ring. The identifiers consist of: (Node#)-(Shelf#)-(CS#)-(1).	Match of the node/shelf selected for source shelf, plus CS# and the port identifier 1 for the 10GE XFP, or 2 or 3 for 1GE SFPs.
Secondary Slot	Address of the slot location for the secondary interface to the ring. The identifiers consist of: (Node#)-(Shelf#)-(CS#)	Match of the node/shelf selected for source shelf, plus CSA or CSB.
Secondary	Address of secondary interface to the ring. The identifiers consist of: (Node#)-(Shelf#)-(CS#)-(1)	Match of the node/shelf selected for source shelf, plus CS# and the port identifier 1 for the 10GE XFP, or 2 or 3 for 1GE SFP.
Description	A text description to identify or characterize the ERPS domain.	String of 31 characters
Control VLAN	ID of control VLAN. Use a VLAN ID that is NOT used for any services on the network.	Unused IDs from 2-4094
Health Message Frequency	Health message frequency, in seconds.	1-10 Default = 5
Recovery Message Frequency	Limit for health message response, in seconds.	1-10 Default = 1
Is Master	Operation of the node in the ERPS domain.	N = No (transit) Y = Yes (master)

To create an ERPS transport ring

1. On the Navigation Tree, click the **Shelf** level.
2. From the CMS menu, click **File** > **Create** > **C7** > **Ethernet and IP** > **ERPS Domain**.
3. In the ERPS Domain dialog box, do the following:
   a. In the Shelf box, select the system address of the shelf to add to the ERPS domain. The identifiers consist of: (Node#)-(Shelf#). For example, N1-2.
   b. In the Address box, select the system address of the ERPS domain to create. The identifiers consist of: (Node#)-(Shelf#)-(ERPS#). For example, N1-2-ERPS1.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

c. In the Primary Slot box, select address of the slot location for the primary interface to the ring. The identifiers consist of: (Node#)-(Shelf#)-(CS#). For example, N1-2-CSA.

d. In the Primary box, select address of the primary interface to the ring. The identifiers consist of: (Node#)-(Shelf#)-(CS#)-(interface#). For example, N1-2-CSA-1.

e. In the Secondary Slot box, select address of the slot location for the secondary interface to the ring. The identifiers consist of: (Node#)-(Shelf#)-(CS#). For example, N1-2-CSB.

f. In the Secondary box, select address of the secondary interface to the ring. The identifiers consist of: (Node#)-(Shelf#)-(CS#). For example, N1-2-CSB-1.

g. In the Description box, enter a text description to identify the ERPS domain. Calix highly recommends that you enter the same description for all of the nodes configured in the ERPS domain.

h. In the Control VLAN box, enter an ID for the VLAN that passes the ERPS control PDU's and heartbeats. The VLAN is automatically created on the shelf. The Control VLAN ID must be configured the same for all nodes in the ERPS domain.

Note: When selecting the Control VLAN ID, use an ID that is NOT used for any services on the network.

i. In the Health Message Frequency box, enter a value that specifies the interval for sending a Health message out to the nodes in the ERPS domain.

j. In the Recovery Message Frequency box, enter a value that specifies the interval for sending a Recovery message out to the nodes in the ERPS domain.

k. In the Is Master box, select whether the node is designated as the master or transit node. Only one node in an ERPS domain can be designated as master. For example, selecting Y designates the node as the master role.

4. Click **Add** to move the configuration to the ERPS Domain objects to be created area.
5. Click **Create** to complete the ERPS domain object creation for the node.
6. Repeat Step 2 through Step 5 to add other nodes in the same network to the ERPS domain.
7. If the traffic VLANs do not already exist on the shelf, create them from the File menu.
   a. Click **Create** > **Ethernet and IP** > **S-VLAN**.
   b. Create a VLAN for each service that will be transported around the ring. See *Creating a VLAN* (on page 227) for instructions.
8. Repeat Step 7 for other shelves in the network that are part of the ERPS domain.
9. From the File menu, click **Create** > **Ethernet and IP** > **VLAN Interface**, and then create a VLAN interface to associate the ERPS domain with each service VLAN that will be transported around the ring. For instructions, see *Creating a VLAN Interface for ERPS Domain* (on page 233).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

10. Repeat Step 9 for other shelves in the network that are part of the ERPS domain.

11. Provision an E7 as the uplink for the ring, using redundant 10GE links with RSTP. See the *Calix E7 User Guide* for instructions.

Note: The RAP-10GE card's Ethernet ports interface to the Local Bridge (EXA switch fabric) only. To forward traffic to/from a C7 Virtual Bridge (for services delivery on the C7 Multiprotocol architecture) currently requires a physical Ethernet link between the 1GE ports on a RAP-10GE card and a VB-based Ethernet line card, with all involved ports (10GE, 1GE, 1GE) added to the same service VLAN ID(s).

VLAN Guidelines and Parameters

Configuration guidelines for VLANs

Follow these guidelines when configuring VLANs:

- By default, a VLAN is created on the shelf VB1, but, it is duplicated on all bridges in the shelf, Local and Virtual.
- Each shelf supports up to 4088 VLANs (VLAN 2-4093, less four configurable reserved VLANs).
    - In addition to reserved VLANs 0-1 and 4094-4095, the C7 reserves four additional VLANs for internal use. The starting reserved VLAN ID is configurable at the network level, and establishes four consecutive reserved VLANs. The default starting value is 1002, which establishes 1002-1005 as reserved VLANs.
- Application Modes:
    - Each VLAN must be configured with an Application Mode setting to define its forwarding mode.
    - (Virtual Bridge only) In multi-shelf applications, VLANs with the same ID should be configured with the same Application Mode.
    - RSTP link protection is not supported for VLANs with Application Mode = 'S-Tag Switch' or 'VLAN per Port' (requiring any 'Edge' port tag actions).
    - VLANs with different Application Modes can share the same Ethernet uplink/downlink, with the following exceptions:
        - S-Tag Switch mode: If RSTP is utilized on an Ethernet link, or the bridge spans two cards, you cannot add VLANs with 'S-Tag Switch' mode to the same bridge.
        - VLAN per Port mode (requiring any 'Edge' port tag actions): If RSTP is utilized on a downlink, you cannot add VLANs with 'VLAN per Port' mode to the same bridge. However, VLANs with 'VLAN per Port' mode and no tag actions ('Trunk' VB ports) do not have this limitation.
- Only one type of Tag action can be applied per VLAN (on its Edge ports).
- Priority Queues:

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- The number of priority queues (NUMPRIO) setting for a VLAN is enforced at all its subscriber-facing VLAN Interfaces (VLAN-IFs) except for the following:
  - VLAN-IFs using UBR cross-connects to ADSL/ADSL2-based card ports or BPON ONT Ethernet ports.
  - VLAN-IFs comprised of "MP" VCs (for RG support). In this case, the number of priority queues is fixed at 8, regardless of the NUMPRIO setting.
- Priority queuing of downstream traffic occurs within individual VLANs. It does not occur across all VLANs on the shelf or even across all VLANs associated with the same subscriber port.
- Priority queuing and bandwidth allocation are separate operations.
  - Bandwidth is shared equally by all VLAN-IFs of the same traffic class (such as UBR/EIR or GFR/CIR) regardless of the priority level of the traffic in the queue(s) of each VLAN.
  - Traffic of any priority on VLAN-IFs with committed bandwidth (GFR/CIR) takes precedence over traffic of any priority on VLAN-IFs with best-effort bandwidth (UBR/EIR).

- Service Security:
  - DHCP Snoop tracks all DHCP activity on the VLAN, creates/updates a table of DHCP leases granted, and enables other security capabilities. (Enabled when DHCP L2 Relay Mode = 'Snoop.')

Note: The C7 LDRA for IPv6 support is only supported if DHCP L2 Relay = Relay, not Snoop.

  - IP Source Verification drops frames that do not have a valid IP/MAC source address learned through DHCP snooping or static assignment. (Automatically enabled with DHCP Snoop.)
  - MAC Forced Forwarding (MACFF) can be used in VLAN per Service applications to ensure that traffic from one subscriber interface cannot be sent directly to another, reducing the chance that malicious traffic can be transmitted between ports. (Enabled when DHCP L2 Relay Mode = 'Snoop' and MAC Force Forward = 'Y.')
  - DHCP Lock prevents MAC spoofing by denying DHCP service to host MAC addresses previously learned on and currently associated with a different subscriber port. With DHCP Lock enabled, a MAC address learned on one port cannot be used again on any other port served by the VLAN until the DHCP lease expires or the entry is manually deleted. (Enabled when DHCP L2 Relay Mode = 'Snoop' and DHCP Lock = 'Y.')

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

VLAN parameters

You can configure the following parameters for a VLAN:

Parameter	Description	Valid Options
Address (ID)	System address of the VLAN to create. The identifiers consist of: (Node#)-(Shelf#)-(VB#)-(VLAN#).	Unused IDs from 2–4093, less four reserved VLANs
Description (DESC)	A text description to identify or characterize the VLAN. (Optional)	A string up to 31 characters
Number Priority (NUMPRIO)	Defines the number of 802.1q priority-bit queues to enable at the VLAN-IFs associated with the VLAN. P-bits map to priority queues as follows: • **1:** Map P-bits 0 to 7 to a single queue (treat all traffic equally). • **2:** Map P-bits 0 to 5 to queue 1 (lower-priority) and P-bits 6 and 7 to queue 2 (higher priority). • **4:** Map P-bits 0 and 1 to queue 1 (lowest-priority), P-bits 2 and 3 to queue 2, P-bits 4 and 5 to queue 3, and P-bits 6 and 7 to queue 4 (highest priority). • **8:** Map each P-bit to a single queue, from queue 1 (lowest priority) to queue 8 (highest priority). Set the number of queues based on the number of different services expected on the VLAN. Calix recommends 1 for a single service VLAN, 4 for voice+video+data on one VLAN, and 4—8 for transparent LAN service. **Note:** This parameter does not alter the P-bit values within Ethernet frames; it only enables P-bit queues within the C7.	1‡, 2, 4, 8
STB Relay ARP (STBRLYARP)	**Note:** This parameter is only supported if it was already enabled on the VLAN prior to upgrading to R8.0. It must be disabled to use MACFF (recommended). Once disabled, it cannot be re-enabled. (This only applies to VLANs with Application Mode = 'VLAN per Service' or 'VLAN per Port,' and subscriber VLAN-IFs with Port Type = 'Edge' and Port Direction = 'Downstream.') For use with EXA Powered video, this parameter enables or disables STB directed ARP relay. Enabling this function guarantees that upstream routing equipment can refresh and create ARP entries for STBs.	N (No)‡ Y (Yes)
DHCP Lock (DHCPLOCK)	(This only applies to VLANs with Application Mode = 'VLAN per Service' or 'VLAN per Port,' and DHCP L2 Relay Mode = 'Snoop.') Prevents MAC spoofing by denying DHCP service to host MAC addresses previously learned on and currently associated with a different subscriber port. With DHCP Lock enabled, a MAC address learned on one port cannot be used again on any other port served by the VLAN until the DHCP lease expires or the entry is manually deleted. **Note:** DHCP Lock provides Denial of Service (DoS) protection against MAC spoofing, independent of the IP source verification functionality that is enabled with DHCP Snoop.	N (No) Y (Yes)‡
MAC Force Forward (MFF)	(This only applies to VLANs with Application Mode = 'VLAN per Service,' DHCP L2 Relay Mode = 'Snoop,' and STB Relay ARP = 'N.') Enables or disables MAC Forced Forwarding, which screens upstream packets at the subscriber port and only allows through those packets with a destination MAC address that matches the upstream access router (the known IPv4 gateway). MAC FF supports the following: • IP hosts learned via DHCP Snooping • IP hosts statically provisioned (IP and MAC)	N (No)‡ Y (Yes)

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Parameter	Description	Valid Options
Application Mode (APPMODE)	Defines a forwarding mode to use. **VLAN Per Service:** Forwards based on S-tag + MAC address (learning bridge enabled) unless DHCP L2 Relay = Snoop. Edge ports are only considered 'trusted' interfaces when configured for RSTP. **VLAN Per Port:** Forwards to Trunk ports based on S-tag + MAC address (learning bridge enabled); forwards to Edge ports based on S-tag only if single-tagged, or S-tag + C-tag if double-tagged (learning bridge disabled) **S-Tag Switch:** Forwards based on S-tag only (no learning bridge). May be used for IP DSLAM aggregation applications. **Routed:** Forwards per Layer 3 rules and decisions. Only applicable to VLANs on a Virtual Bridge. For VLANs on the Local Bridge, this Application Mode is translated to 'VLAN Per Service.' May be used for L3 RBE/DCHP proxy or L3 PPPoE relay applications. **Transparent LAN Service:** Forwards based on TLAN tag (S-tag) + MAC address (learning bridge enabled). All Edge ports on a TLAN are considered 'trusted' interfaces that can be flooded.	VLAN Per Port VLAN Per Service S-Tag Switch Routed Transparent LAN Service Default setting: Blank
IGMP Mode (IGMPMODE)	For use with EXA Powered video. VLANs carrying multicast traffic must use IGMP Snoop or Proxy mode. **Snoop:** The IGMP Snoop mode forwards IGMPv2 messages between the upstream router/querier and STBs with report suppression. **Proxy:** (Recommended) IGMP Proxy enables a more robust IGMPv2 implementation, scaling to the maximum number of subscribers and channels. In this mode, a shelf-level proxy IP address is used as the source address in IGMP messages sent upstream.	None ‡ Snoop Proxy
Circuit ID/Interface ID (OPTION82)	(This only applies to VLANs with DHCP L2 Relay Mode = 'Relay' or 'Snoop.') Specifies the Option 82 Circuit ID (DHCPv4) or Interface ID (DHCPv6) format to use. For settings other than 'None,' the C7 adds the Circuit/Interface ID string to DHCP frames when forwarding upstream, and removes the string when forwarding downstream. **Standard:** Calix standard syntax. **DSL Forum 1:** DSL Forum 1 syntax. **None:** Disables use of the Circuit/Interface ID.	Standard DSL Forum 1 None ‡
Remote ID Option (RMTIDOPT)	(This only applies to VLANs with DHCP L2 Relay Mode = 'Relay' or 'Snoop.') Specifies the Option 82 Remote ID format to use. For settings other than 'None,' the C7 adds the Remote ID string to DHCP frames when forwarding upstream, and removes the string when forwarding downstream. **Standard:** Calix standard syntax. (Only for use when the Circuit/Interface ID also uses the Calix standard syntax.) **Descriptor:** Calix descriptor syntax, which is the user-defined description of the subscriber port. (Only for use with xDSL ports; for use with any Circuit/Interface ID syntax, or none at all.) **None:** Disables use of the Remote ID.	Standard Descriptor None ‡
DHCP L2 Relay Mode (L2RLYMODE)	(This only applies to VLANs with Application Mode = 'VLAN per Service' or 'VLAN per Port.') Specifies the DHCP relay mode per VLAN. **Relay:** Enables additional packet processing for DHCP packets as follows: • the ability to drop or filter DHCP packets, based on the VLAN-IF 'DHCP Directionality' and 'Option 82 Action' setting. • the ability to insert option 82 information as per TR-101, based on the 'Circuit ID/Interface ID' and 'Remote ID Option' settings (above). **Snoop:** In addition to enabling the relay functionality described above, enables DHCP snooping to track all DHCP activity on the VLAN. This enables other security features, such as IP Source Verification, MACFF, and DHCP Lock. **None:** Disables additional packet processing for DHCP packets. DHCP packets are forwarded as usual, except for broadcast DHCP messages in the VLAN per Service application to VLAN-IFs with Port Direction = 'Downstream.'	None ‡ Relay Snoop

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Parameter	Description	Valid Options
Create Uplink	For use with VLANs that are part of an Ethernet uplink. If set to other than none, CMS creates an uplink AID for use with subscriber activation tools. **VB:** Creates an uplink AID for the VLAN on the selected Virtual Bridge. **Local:** Creates an uplink AID for the VLAN on the Local Bridge (RAP-10GE). **Both:** Create both uplinks AIDs listed above.	None ‡ VB Local Both

‡ Default value

Creating a VLAN

Follow the steps below to create a VLAN.

To create a VLAN

1. On the Navigation Tree, click the Network level.
2. On the File menu, click **Create** > **C7** > **Ethernet and IP** > **S-VLAN**.
3. In the S-VLAN dialog box, do the following:
   a. In the Shelf list, select the shelf containing the Ethernet uplink card.
   b. In the VB list, select the virtual bridge on which to create the VLAN.

   Note: A VLAN is created on the shelf VB1, but, it is duplicated on all bridges in the shelf, Local and Virtual.

   c. In the Address list, select the VLAN ID to create.
   d. (Optional) In the Description box, type a brief description for the VLAN.
   e. Set the rest of the parameters as required for your application.
4. Click **Add** to place the VLAN into the S-VLAN(s) To Be Created area.
5. Repeat steps 3 and 4 as required for your application.
6. Click **Create** to save the new VLAN(s).

VLAN-IF Guidelines and Parameters

Configuration guidelines for VLAN-IFs

Follow these guidelines when configuring VLAN-IFs:

- You can create VLAN Interfaces (VLAN-IFs) on established S-VLANs only.
- The subscriber ports of EXA Powered cards are restricted to association with one switch fabric per VLAN. That is, the same VLAN (same VLAN ID) on a Virtual Bridge (Multiprotocol switch fabric) and the shelf-wide Local Bridge (the RAP-10GE EXA switch fabric) cannot be associated with subscriber ports on the same EXA Powered card.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- Creating VLAN-IF templates (to define VLAN-IF parameter settings) helps simplify the VLAN-IF creation process, particularly for subscriber-side interfaces, which are typically added repetitively.
- If you delete a VLAN-IF, all of its sub-component objects are deleted.
- **For the C7 Multiprotocol architecture (VLANs on a Virtual Bridge):**
  - When you create a VLAN-IF for an Ethernet port, the following objects are created: a VB port (on the Ethernet port) and VLAN/VB port association. If the VB port type = Edge, a CVID registration entry is also created for the Edge port to define its tag actions.
  - When you create a VLAN-IF for a subscriber port (xDSL or ONT Ethernet), the following objects are created: a VB port (VC endpoint), VLAN/VB port, VC cross-connect to the subscriber port, and (if the VB port type = Edge, as is typically the case), a CVID registration (CVID Reg) entry to define its tag actions.

  Note: For VLAN-IFs involving VDSL2 ports in Packet Mode: If the VDSL2 subscriber port and the uplink are located in different shelves, the VLAN must be replicated on both shelves (same ID and Application Mode). VLAN replication is done automatically by the 'Create VLAN Interface' tool, as required.

  - You can create multiple VLAN-IFs for a VB port that maps to an Ethernet port. If such a VB port is reused, the same port type ("Trunk" or "Edge") must be applied to all VLAN-IFs using that port. However, VB ports that provide VC endpoints can each comprise only one VLAN-IF.
  - The 'Create VLAN Interface' tool does not currently support VLAN-to-VLAN connections across Virtual Bridges (VB-to-VB cross-connects). Such connections must be built manually.
  - If you manually create the objects that comprise a VLAN-IF (VB port & VLAN/VB port), a VLAN-IF record is automatically added to the VLAN properties.
- **For the C7 EXA architecture (VLANs on the Local Bridge):** When you create a VLAN-IF on the Local Bridge (including the EXA switch fabric), the VLAN membership is created for the port without creating a VB port, VLAN/VB port, or VC cross-connect. However, most parameters provisioned on these individual objects still apply and are provisioned as part of the VLAN Interface dialog. For example, although no VB port object is created, an "Edge" or "Trunk" port type is still specified. If port type = Edge, a CVID registration entry is created to define tag actions.

VLAN-IF parameters

You can configure the following parameters for a VLAN-IF:

Parameter	Description	Valid Options
Bridge/Uplink Shelf (ID)	System address of the shelf with the provisioned VLAN to add/connect to a specified subscriber interface or uplink interface. The identifiers consist of: (Node#)-(Shelf#).	Any shelf in the network. (Node#)-(Shelf#)

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Parameter	Description	Valid Options
VLAN (VLAN)	The ID of the VLAN to add/connect to a specified subscriber interface or uplink interface.	Any established VLAN Default: The lowest-numbered VLAN
Bridge	If this radio button is selected, the list choice indicates the bridge where the VLAN resides. **Local:** One of the following: • The shelf-wide local bridge for services over the EXA architecture. The EXA switch fabric of the RAP-10GE is only available to the OLTG-4E and VDSL2-based EXA Powered cards. • The local bridge of the OLTG-4/4E card, for local layer 2 switching. **VB ID#:** A Virtual Bridge residing in the same shelf or a remote shelf, where the external port is located. The identifiers consist of: (Node#)-(Shelf#)-(VB#).	Local, VB ID#
ATM Uplink	Related to xDSL ports and ATM uplinks. For details, see Creating a VLAN Interface to an ATM Uplink in the *C7 Broadband Data Services Guide*.	STS, DS3p, IMA, AP
Interface Shelf	(Only when Bridge = VB) System address of the shelf with subscriber or Ethernet interface to connect/add to the specified VLAN. The identifiers consist of: (Node#)-(Shelf#).	Any shelf in the network. (Node#)-(Shelf#)
Equipment/Group	System address (plus card type) of the card with subscriber or Ethernet interface to add/connect to the specified VLAN. **Note:** (Virtual Bridge only) If the selected equipment is an OLT or xDSL card, the dialog may expand to include VC settings for cross-connecting the selected port to the VLAN.	All cards in the network with interfaces that can connect to a VLAN
Interfaces	System address of the subscriber or Ethernet interface to add/connect to the specified VLAN.	Subscriber or Ethernet interface on the selected card
Template (TEMPLATE)	Specifies a VLAN-IF template to use, where the template settings will be applied to the VLAN Interface objects.	Any established VLAN-IF template

‡ Default value

Parameter	Description	Valid Options
Port Type (PORTTYPE)	Defines the port role (functions to perform) per IEEE and DSL Forum TR-101 specifications. **Trunk:** Port is S-VLAN aware only, sends and receives only tagged frames, supports EtherType re-stamping **Edge:** Port is C-VLAN aware, sends and receives tagged and untagged frames, can perform tag actions	Trunk ‡ Edge
Protocol Parameters		
ARP Learning (ARP)	(This only applies to VLANs with Application Mode = 'Routed.') Indicates whether ARP can be used to find IP hosts on the link.	Y (Yes) ‡ N (No)
DHCP Directionality (DHCPDIR)	(This only applies to VLANs with Application Mode = 'VLAN per Service' or 'VLAN per Port' and DHCP L2 Relay Mode = 'Relay' or 'Snoop.') Indicates what types of DHCP messages received on this port to forward or drop. **None:** All DHCP packets are dropped. **Client:** All DHCP Offer and Ack messages are dropped. **Server:** All DHCP Discover and Request messages are dropped.	None Server Client ‡

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Parameter	Description	Valid Options
Lease Limit	(This applies to the following VLANs: • Application Mode = 'Routed.' • Application Mode = 'VLAN per Service' or 'VLAN per Port,' and DHCP L2 Relay Mode = 'Snoop.') Limits the number of hosts that can be learned on a port.	Unlimited, or 1—128 Default: 16
IGMP Type (IGMP)	For Multiprotocol video delivery (VB-based), indicates whether IGMP messages (channel change requests) must be supported on this link. • **IGMP None:** IGMP messages are dropped. Multicast video is also dropped. • **IGMP Sink:** Designates the port to 'sink' or pull (receive) ingress broadcast video content. This should also be selected to pass multicast video for all configurations (IGMP Proxy or Static/Non-IGMP). • **IGMP Source:** Designates the port to 'source' or push (send) egress broadcast video content. For EXA Powered video delivery (RAP-10GE-based), these parameters have the following purpose: • **IGMP None:** N/A. • **IGMP Sink:** Designates a router port, which allows video to quickly recover from system topology changes from RSTP/ERPS link events. Up to four RAP-10GE Ethernet ports can be designated as router ports. • **IGMP Source:** N/A.	IGMP None ‡ IGMP Sink IGMP Source
Encapsulation Type (ENCAP)	Ethernet encapsulation type to use on egress packets.	Ethernet V2 ‡
DOS Protection (DOS)	For VLANs with Application Mode = Routed: Verifies that the source address of a packet is legal for the interface on which it arrived. Only allows traffic to originate from the source IP address that was given through an authenticated means, such as DHCP or statically assigned. For VLANs with Application Mode = Routed, VLAN Per Service, or VLAN Per Port: This function also disables the VB port if excessive traffic of the following type is detected: Traffic destined for a VR IP address or traffic that requires the C7 to relay, snoop, or proxy.	Y (Yes) ‡ N (No)
Port Direction (DIRN)	Indicates whether ingress packets with a destination on the same bridge can be forwarded directly to the destination port or must be forced upstream for authentication. **Both** allows for unrestricted forwarding between VB ports on a bridge/VLAN **Downstream** forces all ingress traffic upstream	Both (Unsecure) ‡ Downstream (Secure)
Option 82 Action (OPT82ACT)	(This only applies to VLANs with Application Mode = 'VLAN per Service' or 'VLAN per Port' and DHCP L2 Relay Mode = 'Relay' or 'Snoop.') Specifies an action to take when DHCP packets containing existing Option 82 data are received. **None:** Retain existing Option 82 data on forwarded packets; or, insert Option 82 data if it is not present. **Drop:** Drop packets that contain Option 82 data. **Pass:** Pass packets unmodified, with or without Option 82 data. **Overwrite:** Overwrite Option 82 data on forwarded packets. **Note:** If using the C7 LDRA for IPv6 support, use the following settings to support DHCPv6 message exchanges: 'PASS' for uplink-side VLAN-IFs, 'DROP' for subscriber-side VLAN-IFs.	NONE ‡ DROP PASS OVERWRITE

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Parameter	Description	Valid Options
PPPoE Access Concentrator (PPPOEAC)	Indicates whether communication with an upstream PPPoE access concentrator must be supported on this link. This parameter is required for the following applications: • L3 PPPoE • L3 PPPoA-to-PPPoE inter-working/translation • L2 PPPoA-to-PPPoE inter-working/translation This parameter is not required for the following application: • L2 PPPoE Key: L3 = L3 PPPoE Relay applications, with Routed-mode VLAN on a Virtual Bridge (MP switch fabric). L2 = L2 PPPoE support, with L2 VLAN modes, MP or EXA switch fabric.	Y (Yes) N (No) ‡
PPPoE Subscriber (PPPOESUB)	Indicates whether PPPoE subscriber session messages must be supported on this link. This parameter is required for the same applications listed above.	Y (Yes) N (No) ‡
STP Parameters (Applicable only if Interface != ERPS domain.)		
STP (STP)	Indicates whether an Ethernet interface will belong to a Spanning Tree group for link redundancy. **Off:** No STP/RSTP support **1D Addr:** Supports 802.1d bridge group MAC address **1AD Addr:** Supports 802.1ad bridge group MAC address **1D Tunnel:** Supports tunneling of subscriber RSTP BPDUs for TLAN service (no RSTP connection on link to the subscriber switch).	Off ‡ 1D Addr 1AD Addr 1D Tunnel
STP Cost (STPCOST)	Indicates the cost value of the switch port in an STP group. If redundant links to the root are available, the higher cost port is blocked.	1–200,000,000 Defaults: 4 (GE); 19 (FE)
STP Priority (STPPRIO)	Indicates the switch priority value, used to determine the root switch for STP.	0–240, in increments of 16 Default: 128
Bandwidth Parameters (Applicable only if Bridge = VB and Equipment/Group = OLT or xDSL card.)		
Traffic Profile	Defines the forward traffic profile ID for a cross-connect.	Valid profile ID
Backwards Traffic Profile	(Optional) Defines the backward traffic profile ID for a cross-connect.	Valid profile ID
Cross-Connect Path	Defines the protection path of the cross-connect. (For more details, see the Calix C7 Provisioning Guide.)	Work only Prot only Work + Prot Unprot
BW Constraint [3]	(Optional) Defines the BWC ID for the cross-connect. (For more details, see the Calix C7 Provisioning Guide.)	Valid BWC ID
Protection Class	(Only applicable for VIDVCs.) Bridged: Bandwidth is assigned on both sides of the SONET ring. Unbridged: Only the working side of the SONET ring is assigned bandwidth while the protection side is in standby mode.	Bridged Unbridged
Local Bridge Parameters (Applicable only if Bridge = Local and Equipment/Group != RAP-10GE.)		
Tx Ethernet BW Profile	Required for VLAN-IFs from Local VLANs to EXA Powered subscribers.	Valid profile ID
Rx Ethernet BW Profile	Required for VLAN-IFs from Local VLANs to EXA Powered subscribers.	Valid profile ID
MCAST Profile	A preexisting MCAST Profile ID, required for EXA Powered video applications.	Valid profile ID

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Parameter	Description	Valid Options
Network-Side Parameters (Applicable only if Port Type = Trunk.)		
Local SVLAN ID (LSVID)	Specifies the VLAN ID on the line to translate to the local S-VLAN ID, and vice versa. Applies only to VB ports with Port Type = Trunk (Optional) **Note:** This is not applicable to the RAP-10GE.	Any valid VLAN ID Default: The local S-VLAN ID (no translation)
S-Tag Type (STAGTYPE)	Specifies the S-VLAN EtherType re-stamping to perform. Applies only to Trunk ports.	C-Tag 8100 ‡ C-Tag 9100 S-Tag 88A8
User-Side Parameters (Applicable only if Port Type = Edge.)		
Priority (PRIO)[1] (802.1q Priority Bits Policy)[2]	Specifies the Priority (P-bit) queuing value to apply to forwarded packets. **Priority 0**–**7**: Priority bit value to apply (0 is lowest priority, 7 is highest priority). **Copy Bits:** Honors (copies) the P-bit value from received packets to forwarded packets. Promotes CVID p-bits to SVID p-bits. **DSCP:** Supports DSCP-based prioritization, mapping DSCP values to P-bits for prioritization at the Layer 2 level within the C7.	Priority 0–7* Copy Bits DSCP Bits Default: 0
S-VLAN ID (SVID)[1]	Not in the dialog box, but taken from the VLAN ID parameter within the selected VLAN-IF. Specifies the service VLAN (S-VLAN) tag ID to apply to incoming, forwarded packets (S-tag to "push" on untagged traffic, or to "promote" C-tagged traffic to). **2**–**4093:** The S-VLAN ID (SVID) number to apply to forwarded packets.	2–4093
CVid Access ID (ID) (TL1: LC)[1]	Specifies the local, customer VLAN ID on the line for which to perform tag actions. This value completes the CVID Reg entry ID, where the identifiers consist of: (Node#)-(Shelf#)-(VB#)-(VB port#)-**(local VLAN ID#)**. Valid values include: **Untagged:** Identifies incoming traffic as untagged (no local VLAN ID) or only priority-tagged. **2**–**4093:** Identifies incoming traffic as single-tagged with this local customer VLAN ID (CVID) number. **DFLT:** Identifies incoming traffic as single-tagged: the Default wildcard accepts any local customer VLAN ID (CVID) number.	Untagged (1) 2–4093 DFLT*
Relay C-Tag (RCVID) (TL1: RC)[1]	Specifies the C-tag to use on forwarded double-tagged packets (i.e., the translated CVID value). **None:** Specifies that no C-Tag will be added (pushed) to forwarded packets. If the incoming traffic is tagged, the CVID will be promoted to the SVID (or translated to the SVID, if different). (single-tagged) **2**–**4093:** Specifies the C-tag to apply (push) to forwarded packets. (double-tagged) **DFLT:** Specifies that an unknown/default C-tag on incoming traffic will be maintained on forwarded packets. (double-tagged, such as for TLS)	None 2–4093* DFLT*

‡ Default value

[1] TL1 parameter labels (LC, SVID, PRIO, and RC) may be used as shorthand throughout this guide

[2] Label used in VLAN-IF Templates. No other user-side parameters are available in VLAN-IF Templates.

3 Not available in VLAN-IF Templates.

* Not applicable for routed VLANs

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Creating a VLAN Interface for ERPS Domain

A VLAN interface for ERPS domain provides a logical interface into a VLAN by binding an ERPS group provisioned on RAP-10GE ports to the VLAN, effectively creating switch ports on the VLAN.

Note: A VLAN must be configured with one or more VLAN interfaces to pass traffic.

To create a VLAN interface for ERPS domain

1. On the Navigation Tree, click the Network level.
2. On the File menu, click **Create** > **C7** > **Ethernet and IP** > **VLAN Interface** to open the VLAN Interface dialog box.
3. In the Bridge/Uplink Shelf list, select the shelf where the RAP-10GE card connected in the ERPS ring resides.
4. In the VLAN list, select an existing VLAN ID to associate to the ERPS domain.
5. Click the **Bridge** radio button. In the Bridge list, select **Local** to display the ERPS domain.
6. In the Equipment/Group list, select the ERPS domain group.
7. In the Interfaces list, select the system address of the ERPS domain.
8. For the Port Type parameter, **Trunk** displays.
9. In the DHCP Directionality list, select **None**.
10. In the IGMP Type list, select **None**.
11. In the Encapsulation Type list, select **Ethernet V2**.
12. In the DOS Protection list, select **N**.
13. In the Port Direction list, select **Both (Unsecure)**.
14. Leave the remaining parameter selections blank.
15. Click **Add** to place the new VLAN-IF into the VLAN Interface Object(s) To Be Created area.
16. Click **Create** to create a VLAN-IF associating the VLAN to the ERPS domain.
    All RAP-10GE ports configured in the ERPS domain are associated with the specified VLAN.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring RSTP Protected Links

This section shows you how to configure an Ethernet transport ring and point-to-point transport links using rapid spanning tree protocol (RSTP) path protection.

Path Protection

RSTP is primarily designed to reroute traffic, prevent network loops in Ethernet topologies, and provide service restoration when two or more links terminate at the same location through point-to-point or ring network topologies. See the *Calix C7 Ethernet and IP Service Guide* for detailed information on RSTP.

- **In small-scale ring topologies**, RSTP can provide service restoration within several seconds, depending on the number of Ethernet hops that RSTP must converge before forwarding traffic. This configuration is not recommended for large-scale ring topologies. See *Configure an RSTP Transport Ring* (on page 235).
- **In point-to-point configurations**, RSTP can provide service restoration within a few hundred milliseconds, depending upon which device is designated as the root bridge and how it handles topology convergence. See *Configuring Linear Ethernet Transport with LAG* (on page 242).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configure an RSTP Transport Ring

This topic shows you how to configure an Ethernet transport ring with RAP-10GE ports and using rapid spanning tree protocol (RSTP) path protection.

The C7 supports Rapid Spanning Tree Protocol (RSTP) standard IEEE 802.1w method of protecting configurations by automating active paths selection.

When connecting devices around a transport ring using RSTP, the devices should all be connected to like ports. For example, all GE ports or all 10GE ports should be used.

Note: If a device connected to the C7 only supports STP, the C7 falls back to STP, ensuring seamless protocol interoperability. The C7 RSTP does not interoperate with PVSTP (Cisco proprietary STP).

Before you start the configuration:

Before you begin to configure an RSTP transport ring, ensure the following conditions are met:

- Ensure the RAP-10GE cards (2) are installed in each shelf that comprise the transport ring.
- Connect the equipment in a transport ring configuration. (Physically connecting two nodes together enables the RSTP protocol.) The C7 can support up to 11 nodes in an RSTP transport ring.
- If you are configuring a 10GE transport ring, connect an E7 node as the uplink for the ring, using redundant 10GE links.
- Ensure all connected network devices outside the RSTP transport ring are already configured for RSTP.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

To configure an Ethernet ring with RSTP

1. If the traffic VLANs do not already exist on the shelf, create the VLANs.
   a. From the CMS File menu, click **Create** > **C7** > **Ethernet and IP** > **S-VLAN.**
   b. Create the service VLANs that will be transported around the ring, on each shelf in the ring. See *Creating a VLAN* (on page 227) for instructions.
2. On the Navigation Tree, click the **Network** level.
3. From the CMS File menu, click **Create** > **C7** > **Ethernet and IP** > **VLAN Interface**.
4. Configure a VLAN Interface for each link around the transport ring, with the following required settings:
   - Bridge = Local
   - Port Type = trunk
   - Override Template Parameters
     - STP Enabled

   For detailed provisioning steps, see *Creating a VLAN Interface for RSTP* (on page 236).

Note: The C7 default value for RSTP Priority allows the network to operate correctly using RSTP links. The designation of the root bridge happens automatically as part of the RSTP protocol and does not require special provisioning of the C7.

Creating a VLAN Interface for RSTP

A VLAN interface can provide a logical interface into a VLAN by binding a port to a specified VLAN, effectively creating switch ports on the VLAN.

Note: A VLAN must be configured with one or more VLAN interfaces to pass traffic.

To create a VLAN interface for RSTP

1. On the Navigation Tree, click the Network level.
2. If the traffic VLANs do not already exist on the shelf, create them. From the File menu, click **Create** > **C7** > **Ethernet and IP** > **S-VLAN**, and then create a VLAN for each service that will be transported on the links. See *Creating a VLAN* (on page 227) for instructions.
3. On the File menu, click **Create** > **C7** > **Ethernet and IP** > **VLAN Interface** to open the VLAN Interface dialog box.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

4. In the Bridge/Uplink Shelf list, select the shelf with the ports where you want to configure RSTP.
5. In the VLAN list, enter the VLAN ID to associate to the port(s), or select it from the list.
6. Click the **Bridge** button, and then select **Local** to view the interfaces associated with the EXA switch fabric.
7. In the Equipment/Group list, select the RAP-10GE card or provisioned group (LAG).
8. In the Interfaces list, select a RAP-10GE port.
9. In the Template list, leave the selection blank.
10. In the Port list, select **Trunk**.
11. For the remaining VLAN-IF parameters, confirm the following settings:
    - Set ARP Learning to **Y** for H.248/routed VLAN applications.
    - Set DHCP Directionality to **None** or **Server** for ONT SIP applications, as required. Or, select Client for a LAG interface.
    - Set DOS Protection to **N**.
    - Set Port Direction to **Both (Unsecure)**.
    - Set S-Tag Type to match the EtherType stamping setting at the far end of the link (**C-Tag 8100**, **C-Tag 9100**, or **S-Tag 88A8**).
    - For all other settings, leave the selections blank to accept the defaults.
    - To support RSTP on the Ethernet link, complete the additional sub-steps below. Otherwise, in the STP list, click **OFF** to disable RSTP.
        - In the STP list, select a MAC (**1D Addr** or **1AD Addr**) for rapid spanning tree protocol (RSTP) bridge protocol data units (BPDUs).
          1D Addr results in the C7 transmitting BPDUs with a DA of 01:80:C2:00:00:00. Use this selection when the C7 is connected to an 802.1d compliant switch with redundant link.
          1AD Addr results in the C7 transmitting BPDUs with a DA of 01:80:C2:00:00:08. Use this selection when the C7 is connected to an 802.1ad compliant switch with redundant link.

Note: The value used must match the provisioning of the network element on the other end of the link. That is, both ends of an RSTP span must use the same MAC address value for BPDUs.

        - In the STP Cost box, type a value (1-200000000) to set the cost of transmitting a frame on to a network through that port or leave the box blank to accept the default of 4. The cost is assigned according to the speed of the bridge. The slower the media, the higher the cost.
        - In the STP Priority box, type one of the values to set the priority of this port interface or leave the box blank to accept the default of 128. The choices are multiples of 16 (0-240).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Note: The C7 default value for RSTP Priority allows the network to operate correctly using RSTP links. The designation of the root bridge happens automatically as part of the RSTP protocol and does not require special provisioning of the C7.

- In the Port VLAN ID box, leave the box blank.
- In the Port Type list, click **Trunk**.

12. Click **Add** to place the new VLAN interface into the VLAN Interface Object(s) To Be Created area.
13. To configure a protected Ethernet link, repeat Step 2 through Step 12 above to create a VLAN interface for another Ethernet port or group in the same bridge. Make sure that RSTP is enabled.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring Linear Point-to-Point Ethernet Transport with RSTP or LAG

The following methods of point-to-point link protection are supported on RAP-10GE, EGW, GE-2E, and GE-2p/FE-4p Itemp interfaces:

- Link Aggregation Group (LAG) standard IEEE 802.1AX (also known as IEEE 802.3ad)
- Rapid Spanning Tree Protocol (RSTP) standard IEEE 802.1w

Link Aggregation on the C7 interfaces

The C7 supports Link Aggregation for bonding multiple GE links into a single link aggregation group with a single logical Ethernet interface. Link aggregation expands the bandwidth of the logical interface beyond the capacity of a single link and also provides link redundancy between devices even if one of the links fails. A visual example of link aggregation is shown below. See *Configure a Linear point-to-Point Ethernet Transport with LAG* (on page 242) for instructions.

Two main types of link aggregation groups are supported on the C7:

- LAGs with members on a single RAP10-GE when delivering services across the EXA switch fabric.
- LAGs with members on one or two GE cards (EGW, GE-2E, and GE-2p/FE-4p Itemp) when delivering services across the multiprotocol switch fabric.

Link aggregation group configuration guidelines

The general rules for configuring a LAG on a C7 are as follows:

- The maximum LAG group is 2G.
- Ports that are configured for link aggregation are all part of a link aggregation group.
- All members of a LAG must be of the same data rate and in full-duplex mode.
- RSTP is supported between LAGs.
- All members of a LAG must be associated with the same bridge. That is, either Local (EXA) or VB (multiprotocol).
- ERPS enabled LAG groups are not supported.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- Standards based implementation allows for interoperability with other Calix and 3rd Party products.
- When a LAG is created, the RAP provides the MAC address to the LAG and stores it with the LAG ID in the database, allowing the LAG to receive the same MAC address after a shelf reboot.
- Logical link IDs are assigned to LAGs starting with the lowest slot, lowest port group member. If a LAG is removed or added, the link ID table is recreated and each of the remaining ports receive a new link ID.
- In some cases, the failover times for LAGs on FE interfaces of EGW cards may range to 500ms.

The rules for EXA link aggregation groups on RAP-10GE cards are as follows:

- A LAG can be configured with member GE ports on the same RAP-10GE card.
- LAG groups are constrained to a single card. The GE interfaces from different RAP-10GEs cannot be aggregated in a single LAG group.
- An EXA LAG configured on a RAP-10GE card cannot be configured with a GE port from one of the GE cards.
- Both Marker Protocol and Link Aggregation Control Protocol (LACP) are supported as a means for determining the state of the aggregated link.
- The maximum LAG group Bandwidth = 2 Gbps.

The rules for multiprotocol link aggregation groups on EGW, GE-2E, or GE-2p/FE-4p cards are as follows:

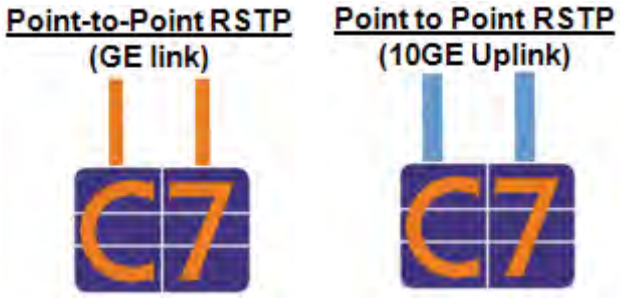
- A LAG can be configured with member GE ports on the same card or different cards for the same virtual bridge.
- A multiprotocol LAG configured on a GE card cannot be configured with a RAP-10GE port as one of the participating ports.
- Link Aggregation Control Protocol (LACP) is supported as a means for determining the state of the aggregated link.
- The maximum LAG group ingress bandwidth corresponds to the amount of shelf bandwidth (2.5 Gbps total) allocated to the Ethernet cards.
- The following number of members in a LAG are supported:
  - GE interfaces - 4
  - FE interfaces - 8
- Although 4 GE ports can be used in a LAG, the ingress capacity is limited to the amount of packet bandwidth allocated to the individual Ethernet cards (< 2.5 Gbps).
- When ingress traffic overruns the bandwidth available to the cards, there are two levels of priority:

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- Level 1 ATM Class of Service (CoS): The C7 prioritizes traffic based on the relative ATM CoS priorities (CBR, GFR, UBR/UBR+). That is, traffic terminating on UBR VCs will be dropped before traffic that is destined for GFR VCs.
- Level 2 Ethernet P-bits: The C7 prioritizes traffic within an individual flow/ATM VC based on 802.1p P-bit markings.

RSTP configurations on C7 interfaces

RSTP allows for a network design to include redundant network links and provides a backup path to an Ethernet device if one of the active links fails. This is achieved without having to be concerned with network loops or manually enabling the backup links. The advantage of RSTP as a C7 network redundancy protocol over link aggregation is the ability to protect rings of subtended devices, such as a C7 aggregating multiple E5-100 units in a Calix ODC remote terminal.



RSTP configuration guidelines

The rules for RSTP on the RAP-10GE interfaces are as follows:

- All RAP-10GE interfaces are supported.
- Point-to-Point and Ring configurations are supported.
- Point-to-Point Link Aggregated RSTP configurations are supported.
- RAP-10GE interfaces are in a different RSTP Bridge group than all other C7 Line Units.
- The RAP-10GE interfaces used should all be like ports. For example, either two GE or two 10GE ports should be used.
- Up to 11 shelves are supported in a ring.
- Standards based implementation allows for interoperability with other Calix and 3rd Party products.

The rules for RSTP on the multiprotocol GE interfaces are as follows:

- Point-to-Point Link Aggregated RSTP configurations are supported.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Link aggregation groups with RSTP configurations

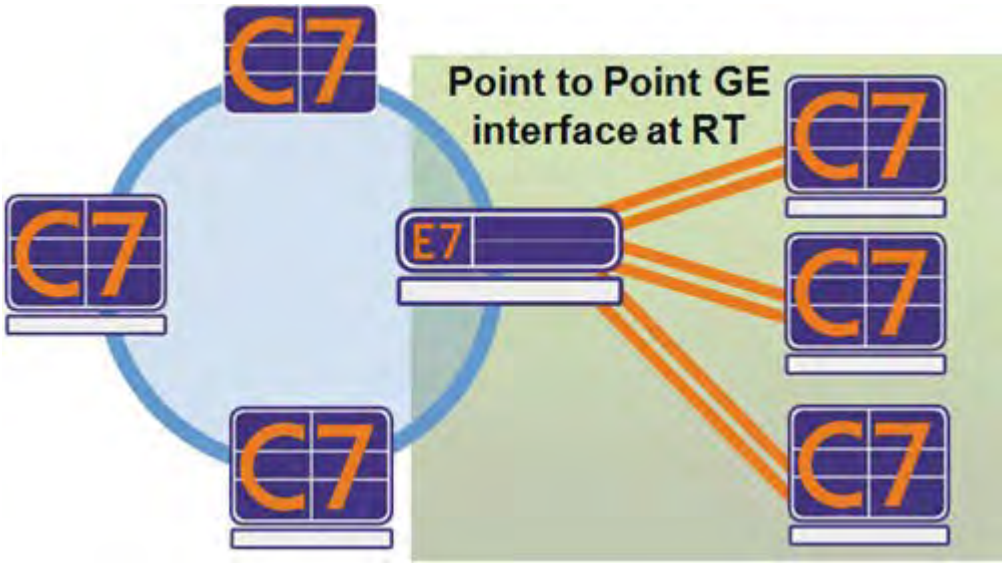
When a device is connected to the C7 using a link aggregation group that is connected to multiple ports on the same C7 card, the link aggregation does not provide equipment redundancy within the C7, but does provide link failure prevention. Link aggregation is often used with RSTP to provide a combination of equipment redundancy and increased bandwidth. LAGs on non-RAP Ethernet cards can span across multiple cards, and, therefore offer equipment-level protection. RSTP can also run on top of LAGS that span cards. The diagram below shows a simplified configuration that supports two LAG groups on separate cards with RSTP enabled to provide protection across the cards.

Configure a Linear Point-to-Point Ethernet Transport with LAG

This topic shows you how to configure a linear, or point-to-point, arrangement with the C7 which supports protected connectivity to remote devices using a link aggregation group (LAG) for port / link redundancy.

Link aggregation groups (LAGs) provide increased bandwidth across a point-to-point link. A LAG can also provide link redundancy, at reduced bandwidth during a link failure. See *Configuring near Point-to-Point Ethernet Transport with RSTP or LAG* (on page 239) for the configuration guidelines.

Note: The C7 also supports enabling of RSTP on LAG groups.



Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Link-aggregation group parameters

You can provision the following parameters for a LAG:

Parameter	Description	Valid Options
Shelf	System address of the shelf where the RAP-10GE card is located. The identifiers consist of: (Node#)-(Shelf#)	Any node/shelf with RAP-10GE cards connected in the network.
Group	System address of the LAG to create. The identifiers consist of: (Node#)-(Shelf#)-(LAG#).	Match of the node/shelf selected for shelf, plus LAG#.
Available Ethernet Port Members	Ports on RAP-10GE cards in the selected shelf that are available for LAG configuration. The identifiers consist of: (Node#)-(Shelf#)-(CS#)-(#).	Match of the node/shelf selected for source shelf, plus CSA-# or CSB-#.
Existing Ethernet Port Members	Proposed ports to be configured as a LAG. The identifiers consist of: (Node#)-(Shelf#)-(CS#)-(#).	Any port listed as available.
Description	Descriptive label for the LAG.	String 31 characters
Distribution Algorithm	Individual traffic flows will only use a single link in the Link Aggregation Group (LAG). The link used for each packet is based on a hash algorithm. The Distribution Algorithm for multiprotocol LAG has to be **Both** (for Source and Dest MAC).	Source MAC Dest MAC Both
Max Transmission Unit	Maximum Transmission Unit size (bytes) is the largest protocol data unit that the layer can pass onwards. **Note:** Only Ge-2p/EGW supports 1500-byte frames.	1500-9000

To configure a linear point-to-point Ethernet transport with LAG

1. On the Navigation Tree, click the **Shelf** level.
2. From the Work Area, click **Create** > **Link Aggregation Group**.
3. In the New Link Aggregation Group area of the dialog box, do the following:
   a. In the Shelf box, select the shelf where you want to create the LAG.
   b. In the Group box, select the system address of the LAG to be created.
4. In the Members area of the dialog box, do one of the following:
   - For EXA LAGs, select the RAP10-GE ports that will participate in the LAG by Ctrl+click. For example, either Ctrl+click the **CSA-2** and **CSA-3** ports, or the **CSB-2** and **CSB-3** ports. Click **Add** to move the links from the Available Members list to the Existing Members list.

   Note: The selected GE ports must be on the same RAP-10GE card.

   - For multiprotocol LAGs, select the GE ports that will participate in the LAG by Ctrl+click. Click **Add** to move the links from the Available Members list to the Existing Members list.
5. In the Attributes area of the dialog box, do the following:

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

a. In the Description box, enter a descriptive title for the LAG.

b. In the Distribution Algorithm list, select whether the individual traffic flows use a single link in the Link Aggregation Group (LAG). Calix recommends leaving the default value of **Both**. For multiprotocol LAGs, you must select **Both**.

c. In the Max Transmission Unit box, leave the box blank to accept the default value of 2048.

6. Click **Add>>**, and then **OK** to complete the creation of a link aggregation group. The LAG appears in the Navigation Tree under the shelf selected in Step 3a.

7. To add or remove LAG members, click the LAG level in the Navigation Tree, and then click the button to the right of the Link Agg Members area.

8. If the traffic VLANs do not already exist on the shelf, create the VLANs as follows:

   - From the File menu, click **Create** > **C7** > **Ethernet and IP** > **S-VLAN**, and then create a VLAN for each service that will be transported on the links. See *Creating a VLAN* (on page 227) for instructions.

9. Create a VLAN interface to add the LAG interface to a service VLAN and to configure the interface for RSTP, if desired. See *Creating a VLAN Interface for RSTP* (on page 236) for instructions.

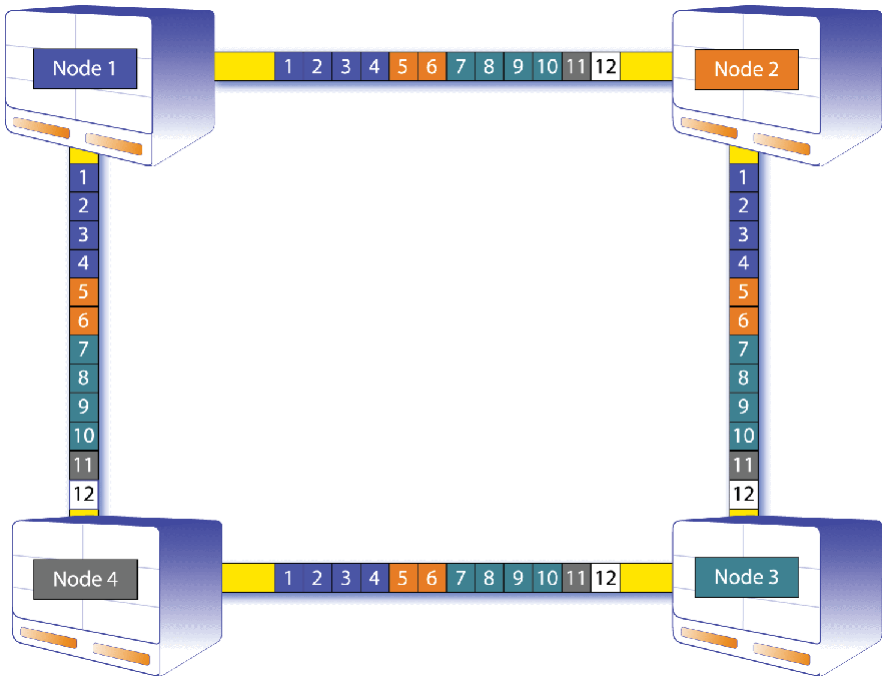
Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring UPSR with Packet Aggregation

You can carry both SONET and packet traffic on a C7 ring using Unidirectional Path Switched Rings (UPSR) with Packet Aggregation. SONET UPSR provides path-level protection that supports uninterrupted transmission.

UPSR provides duplicate fiber paths around the optical ring. In a UPSR counter rotating fiber configuration, working traffic flows in one direction and protection traffic flows in the opposite direction. If a problem is encountered in the working path, the receiving node switches to the path coming from the opposite direction.

In a sample network of a four-node, OC-12 UPSR, each node contributes traffic to the ring.



A traditional SONET network transports services from each node in the same transport path on every link through the network. Services from multiple nodes cannot be carried in the same path. Services from a single node with different exit points in the network must also use separate paths. For example, ADSL services must travel on paths configured for packet traffic, while services like DS3 SONET must travel on paths configured for SONET traffic. To provide more efficient bandwidth usage, the C7 provides UPSR with Packet Aggregation to allow multiple nodes on the ring to share the same bandwidth and transport path.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

UPSR with Packet Aggregation

UPSR with Packet Aggregation is a packet-based path protection configuration that protects packet and SONET traffic on a ring topology. Using this protection configuration, services from multiple nodes can share the same bandwidth and transport path. This distributed aggregation statistically multiplexes packet traffic from any node onto a pool of bandwidth shared across the transport network. The result frees unused bandwidth so that there is more efficient use of bandwidth.

Path protection and packet aggregation

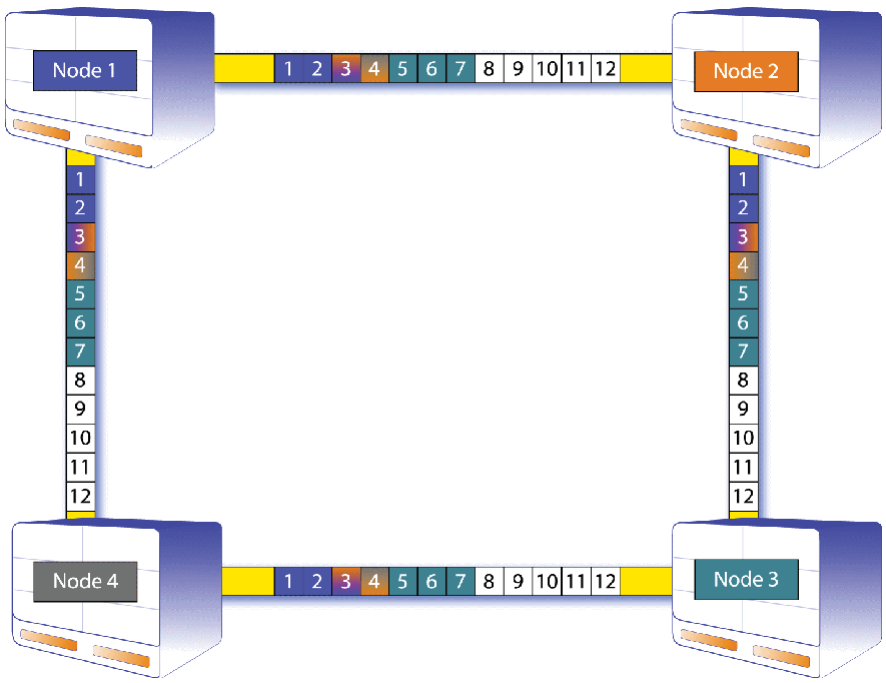
Using this distributed aggregation capability, you can configure one (or more) STS to add and drop packet traffic at multiple nodes. This protection configuration provides the benefits of SONET survivability with bandwidth management efficiency gained from aggregation.

Bandwidth management on the C7

Bandwidth management involves deciding what traffic is highest priority, ensuring that it gets the bandwidth it needs, and deciding how to handle the lower-priority traffic. The C7 supports traditional SONET bandwidth management capabilities as well as ATM traffic shaping and aggregating capabilities.

Packet aggregation and bandwidth management

In the same four-node, OC-12 ring configured as a UPSR with Packet Aggregation, bandwidth allocation is more efficient because packet traffic from different nodes can share the same transport path. You can configure each transport path to the maximum capacity.



Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Quick Turn-Up Outline

Starting point

Before starting this quick turn-up process, check to see that the following conditions are met:

- All shelves in the network have been installed and powered.
- AMP (or ATP), RAP, and optical transport cards (if needed) have been installed in the shelves.
- Optical fibers for transport have been connected to the RAP optical ports, or ports on optical transport cards in each shelf.

Quick turn-up steps

1. Configure your computer to connect to the front Ethernet port (E1) on a C7 AMP or ATP card.
2. Connect to the E1 port and start the management software.
3. Define network nodes.
4. Define transport topology and protection.
5. Set shelf timing for all shelves.
6. Configure STS paths for transport.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configure Optical Transport Topology and Protection

Before you configure an optical port as a transport link, see the complete list of port parameter descriptions.

Information to collect before configuring topology and protection

Prior to configuring your network topology and protection scheme, you should collect the following information:

- Optical port IDs
- Protection Domain number to use
- Protection scheme to use
- Number and size of STS paths

To configure optical ports for transport

1. On the Navigation Tree, click Network level, and then set the Selection Filter by clicking **Port** > **OC Port** > **OC Port**.

   Note: To further narrow the displayed facilities, set the filter to match the OC rate you are using, such as **OC48 Port**.

2. In the Work Area, select all the optical ports for the transport links in the network. Use Ctrl+click to select one port at a time, or Shift+click to select a range of ports.
3. Edit the transport parameters:
   a. For the EXT (External) interface parameter, verify the value **N** (No) is set.
   b. For the PDOM (Protection Domain) parameter, enter a number (0 through 10000) for each port, and then press **Enter**. (Note that each port on the ring must have the same PDOM number and the number must not be used by any other transport topology in the network.)
4. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save the configuration.
5. In the Work Area, click **Protection**.
6. On the toolbar, click **Create** to open the OCn Port Protection dialog box.
7. In the OCn Port Protection dialog box:
   a. In the Shelf list, select a shelf.
   b. In the Line Rate box, select the rate for your network.
   c. In the Working AID box, select an OC port to serve as the working path in the network. (Note that the system automatically designates a port on an adjacent card as the protect path.)

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

d. Click **Add** to place the ports in the Protection Pairs To Be Created area.

8. Repeat Step 7 for each additional C7 shelf to be used for transport in the ring.
9. In the Protection Scheme box, select the protection scheme for the network.
10. Click **OK** to save your configuration.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring DS3p Transport Links

Use these procedures to configure a DS3 transport link between two C7 shelves delivering ATM services such as DSL.

Rules for configuring DS3p transport

Follow these rules when configuring DS3p (DS3-4p, DS3E-4p, or DS3-12p) transport in your network:

- Configure the remote DS3p ports before configuring the central office DS3p ports.
- Two DS3p cards can support a maximum of 12 transport links between them.
- All DS3p transport links within a network must be on the same protection domain.
- Use DS3p transport links to carry ATM traffic only.
- A C7 network using DS3 transport can be provisioned with up to 16 hops.

To configure DS3p transport

1. On the Navigation Tree, click a DS3p card to view the ports.
2. Use Ctrl+click to select each DS3p port to configure for transport.
3. In the **Provisioning** Work Area, click the first port in the list, and then Shift+click the last port in the list to select all of the ports for editing.
4. Take the ports out of service, and set the interface type:
   a. In the PST (Primary Service State) list, click **OOS** (Out of Service) to place the port(s) out of service.
   b. In the INTF (DS3 Interface Type) box, click **NNI**.
   c. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your changes.
5. Re-select the ports as in Step 3, and then set the External Interface:
   a. In the External (External Interface) box, click **N**.
   b. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your changes.
6. Re-select the ports as in Step 3, and then set the Protection Domain:
   a. In the PDOM (Protection Domain) list, enter a number and press **Enter**.
   b. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your configuration.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

To view DS3p transport links

1. On the Navigation Tree, click the Network level.
2. In the Work Area, click **Data Links** > **Link Endpoints** to display the transport links.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring T1 IMA Transport

Quick Turn-Up Outline for T1 IMA Transport

Use this quick turn-up outline to get T1 transport for IMA traffic up and running.

Starting point

Before starting this quick turn-up process, check to see that the following conditions are met:

- All C7 shelves in the T1 transport network have been installed and powered.
- AMP (or ATP), RAP, and T1-6 A+T or IMA-12 cards have been installed in the C7 shelves.
- Cables have been connected to the T1 cards in each C7 shelf.

Quick turn-up steps

1. Configure your computer to connect to the front Ethernet port (E1) on a C7 AMP or ATP card.
2. Connect to the E1 port and start the management software.
3. Define network nodes.
4. Set shelf timing for all C7 shelves.
5. Create and configure IMA Groups for IMA transport.

For information on setting up an ATM uplink, see the *Calix C7 Broadband Data Services Guide*.

Configuration Rules for T1 IMA Transport

Use these procedures for configuring a transport link between two C7 shelves using Inverse Multiplexing for ATM (IMA).

IMA group creation rules

Follow these rules when planning and configuring IMA groups for your network:

Using T1-6 A+T Cards	Using IMA-12 cards
• All T1 ports in an IMA group must be on the same T1-6 A+T card. • All T1 ports must be configured with DS1 Mapping set to N/A prior to adding to an IMA group. • The sum of VPs plus VCs of type	• T1 ports in an IMA group can be on one or more T1-6, T1-6 A+T, HDSL2/4-6, or IMA-12 cards. • All T1 ports must be configured with DS1 Mapping set to SEQ prior to associating with an ATM resource port

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Using T1-6 A+T Cards	Using IMA-12 cards
CBR, VBR, and GFR cannot exceed 60 VCs per card. • The number of VCs of type UBR or UBR+ cannot exceed 600 VCs per card. Create IMA groups on multiple cards if you require more than 600 UBR or UBR+ VCs. • A T1-6 A+T card can be configured for 1:n equipment protection if none of its ports are configured for TDM traffic. • Only 1 internal communications channel (ICC) is supported per card when using 1:n equipment protection.	and adding to an IMA group. • The sum of VPs plus VCs of type CBR, VBR, and GFR cannot exceed 384 VCs per card. • The number of VCs of type UBR or UBR+ cannot exceed 4,096 VCs per card. • An IMA-12 card can be configured for 1:n equipment protection.

A C7 network using IMA transport can be configured with multiple hops if remote shelves support data only. If remote shelves support TDM voice, only one hop can be configured.

T1 IMA transport process description

Complete the following steps for each node to set up T1 transport using IMA interfaces:

Using T1-6 A+T Cards	Using IMA-12 cards
• Configure the T1 ports. • Create an IMA group and add T1 ports. • Configure the IMA group.	• Configure the DS1 or HDSL ports for use in the IMA group. • Configure the ATM Resource ports (optional). **Note:** ATM Resource ports can also be automatically configured when you assign them to an IMA group. • Create an IMA group and add DS1 or ATM Resource ports. • Configure the IMA group.

The C7 nodes self-discover after you configure the IMA groups for each node.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

T1 Port Parameters for Use in an IMA Group

You can configure ports on a T1-6 A+T or IMA-12 card for either a DS1 or T1 signal type.

The following table lists the parameters used to configure a port for use in an IMA group.

Parameter	Value
DS1 Format (required)	ESF (Extended Super Frame)
DS1 Line Coding (required for T1 A+T cards only)	B8ZS
DS1 Map (required)	T1-6 A+T: N/A (No mapping applied) IMA-12: SEQ (Sequential)
DS1 Type	T1-6 A+T: Set to DS1 or T1 per your site requirement. IMA-12: DS1 only.
Equalization (Used with DS1 type)	300 feet (default) Set per your site requirement.
Power (Used with T1 type)	Sink (default) or Source Set per your site requirement. Selecting source puts –130 Volts on the T1 line.
Attenuation (Used with T1 type)	0.0 dB (default) or –7.5, –15.0, –22.5 dB Set per your site requirement.
Timing Mode	The T1 port timing adopts the setting (Source or Loop) of the IMA group. For details, see *Configure an IMA Group for ATM Transport* (on page 260). Calix recommends that the T1 port timing mode match the IMA group setting. **Note:** For an IMA-12 card, if T1 ports used in the IMA group are located on a different card, the IMA group must use Source timing. In this case, to use timing derived from a T1 port in the IMA group, set the C7 shelf to Line timing with the appropriate T1 port as the timing reference.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configure T1 Ports for Use in an IMA Group

This procedure describes configuring DS1 and T1 ports for IMA traffic before adding them to an IMA group.

To configure DS1 or T1 ports for use in an IMA group

1. On the Navigation Tree, click a T1-6 A+T or an IMA-12 card to view the ports, and then use Ctrl+click to select each port to configure one at a time.
2. In the Provisioning Work Area, click the first port in the list, and Shift+click on the last port in the list to select the range of ports for editing.
3. In the Edit Row, place the ports out of service and set the DS1 signal type.
   a. In the PST (Primary Service State) list, click OOS (Out of Service).
   b. In the DS1 Type list, click DS1 or T1, per your site requirement.
   c. On the toolbar, click Apply. In the Confirmation dialog box, click OK.
4. Re-select the same ports selected in Step 2.
5. In the Edit Row, set the following port parameters and place the ports back in service:
   a. In the FMT (DS1 Format) list, click ESF.

   Note: For DS1 ports on an IMA-12 card, ESF is the only option.

   b. In the LINECDE (DS1 Line Coding) list, click B8ZS.
   c. In the DS1MAP (DS1 Mapping) list, do one of the following:
      - (For ports used with a T1-6 A+T card) Click N/A.
      - (For ports used with an IMA-12 card) Click SEQ.

   Note: Steps 5d and 5e only apply to ports set to a T1 signal type.

   d. In the DS1PWR (DS1 Power) list, click Sink or Source as required for your site.
   e. In the DS1ATTN (DS1 Attenuation) list, select an attenuation dB value as required for your site.
   f. In the Timing Mode list, Calix recommends using the setting (Source or Loop) of the IMA group.
   g. In the PST (Primary Service State) list, click IS (In Service).
   h. On the toolbar, click Apply. In the Confirmation dialog box, click OK to save your changes.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configure HDSL Ports for IMA Transport with IMA-12 Cards

This procedure describes how to configure an HDSL port for IMA transport using the IMA-12 card, before associating it with an ATM resource port (AP).

To configure an HDSL port for IMA transport

1. On the Navigation Tree, click an HDSL card to view the ports.
2. Use Ctrl+click to select each HDSL port to configure.
3. Place the port out of service:
   a. In the **Provisioning** Work Area, in the Primary Service State (PST) list, click **OOS** (Out of Service).
   b. On the toolbar, click **Apply** to place the port out of service. In the Confirmation dialog box, click **OK**.
4. Set the following required parameters:
   a. In the DS1 Format list, click **ESF**.
   b. In the Line Power list, click **SINK** or **SOURCE** as required for your site.
   c. If you are applying a grade of service, in the Grade of Service list click **DEFLT** or select a grade of service profile number that you have created for HDSL service.
   d. In the Line Type list, click **2WIRE** or **4WIRE** as required for your site.
   e. In the Terminal Type list, click **COT** if the port will interface with an HTU-R unit, or **RT** if the port will interface with an HTU-C unit.
   f. In the Signal-to-Noise Margin Threshold and Loop Attenuation Threshold boxes, type the values required for your site.
   g. In the DS1 Map list, click **SEQ**.
   h. In the Timing Mode list, click **SOURCE**.
   i. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your changes.
5. Place the port back in service:
   a. In the Primary Service State list, click **IS** (In Service).
   b. On the toolbar, click **Apply** to place the port back in service. In the Confirmation dialog box, click **OK**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configure ATM Resource Ports for IMA Service (IMA-12 Cards)

Optionally configure the ATM Resource ports for IMA service before adding them to an IMA group.

Note: ATM Resource ports can also be automatically configured when you assign them to an IMA group.

To configure ATM Resource ports for use in an IMA group

1. On the Navigation Tree, click the shelf containing the IMA-12 card.
2. Double-click the IMA-12 card to view its ports.
3. Click the ATM Resource Port that you want to provision.
4. In the Work Area, click the **Provisioning** tab.
5. In the User Description box, enter the description.
6. In the ATM Mapping list, confirm that the default, **IMA**, is selected.

   Note: ATM Resource Ports must be configured with ATM Mapping set to IMA for use in an IMA Group.

7. Click the ellipsis button to the right of the DS1 Physical Location ID box to open the Choose T1 Port from the List to Associate with this AP dialog box. Select the T1 or HDSL port and then click **OK**.
8. In the Payload Scrambling list, leave the field blank.
9. In the ATM Monitoring list, leave the field blank.

   Note: ATM Monitoring applies only to NNI and UNI interfaces.

10. In the Grade of Service list, select the Grade of Service profile identifier or leave the field blank.
11. In the Protection Domain (PDOM) box, leave the field blank.
12. Place the ATM Resource into service as follows:
    a. In the Primary Service State list, click **IS**.
    b. On the toolbar, click Apply to place the port in service. In the Confirmation dialog box, click **OK**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Create an IMA Group and Add T1s

Create one or more IMA groups, and then add multiple T1 or ATM resource ports:

- For a T1-6 A+T card, add T1 ports from a single card.
- For an IMA-12 card, add ATM resource ports associated with one or more T1-6, T1-6 A+T, HDSL, or IMA-12 cards.

This section includes these procedures:

- Create an IMA group.
- Add DS1 or ATM resource ports to an IMA group (IMA-12 cards).
- Add T1 ports to an IMA group (T1-6 A+T cards).

Recommendations for IMA 1.0 compatibility

Use the following practices to ensure compatibility with external devices using IMA 1.0:

- Use sequential T1 ports in an IMA group.

  OK: Create an IMA group with ports 1 through 3.

  Not OK: Create an IMA group with ports 1, 3, and 5.
- Wire ports on the Calix T1-6 A+T or IMA-12 card to the matching port number on the external device.
- On T1-6 A+T cards, you may need to configure the IMA Group to force compatibility with IMA 1.0 devices and older routers. Change the ALTV_1 parameter to Y (Yes) if you have difficulty connecting to an external device using IMA 1.0.

If you are connecting to another C7 shelf or an IMA 1.1-compatible device, these steps are not required.

To create an IMA group

1. On the File menu, click:
   - (in iMS) **Create** > **Ports**
   - (in CMS) **Create** > **C7** > **Ports**
2. In the Ports - Provisioning by Port Type dialog box:
   a. In the Shelf list, select the shelf where the T1-6 A+T or IMA-12 card for the IMA group is located.
   b. In the Port Type list, click **IMA Group**.
   c. In the list of available IMA Groups, select a group on the T1-6 A+T or IMA-12 card to contain the IMA group.
   d. Click **Add** to place the selected IMA group in the To Be Created Ports list.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

e. Click **OK** to create the IMA group.

Note: For a T1-6 A+T card, all the T1 ports added to an IMA group must be on the same card.

To add DS1 or ATM resource ports to an IMA group (IMA-12 cards)

1. On the Navigation Tree, click the shelf containing the IMA-12 card, then click the IMA group to modify.

   Note: Select an IMA group ID on the IMA-12 card (correct node, shelf, and slot).

2. In the Work Area, on the Provisioning tab, click the ellipsis button next to the Physical Location Identifiers box to open the New Add AP for IMA dialog box.
3. In the New Add AP for IMA dialog box, do the following:
   a. To add DS1 ports, click **Choose T1 Port from the list**.

      —or—

      To add ATM resource ports, click **Choose AP Port from the list**.

   Note: DS1 ports must be from T1 cards in the same shelf as the IMA-12 card. If DS1 ports are added, corresponding ATM Resource Ports are automatically provisioned.

   Note: Before ATM resource ports can be added, they must be associated with DS1 ports from supported cards [see *Configure the ATM Resource Ports (optional)*, above].

   b. In the Available Ports list, press the **Ctrl** key and click the ports to add to the IMA group.
   c. Click **Add** to add the ports to the Selected Ports list.
   d. Click **OK** to add the ports to the IMA group.

To add T1 ports to an IMA group (T1-6 A+T cards)

1. On the Navigation Tree, click the shelf containing the T1-6 A+T card, then click the IMA group to modify.
2. In the Work Area, on the Provisioning page, click the button next to the Physical Location Identifiers box to open the New Add T1 IMA dialog box.
3. In the New Add T1 IMA dialog box, do the following:
   a. In the Available Ports list, press the **Ctrl** key and click the T1 ports to add to the IMA group.
   b. Click **Add** to add the ports to the Selected Ports list.
   c. Click **OK** to add the ports to the IMA group.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configure an IMA Group for ATM Transport

IMA group parameters for ATM transport

Check and set the following parameters to configure an IMA group for ATM transport:

Parameter	Description and Value
Mapping	The IMA mapping parameter indicates how the internal fixed length packets are mapped at the IMA interface. Set to NNI (Network-to-Network Interface).
External Interface	Indicates if the IMA group is an internal or external path in the network. Set to N.
Protection Domain	A number greater than 0. The IMA groups at each node must use the same Protection Domain (PDOM) number for the transport path to be recognized. The Protection Domain number must also be different from any other PDOM number assigned to other transport topologies in the network.
Timing Mode	Specifies the timing source for the IMA group: • SOURCE (default): T1 port transmit timing is derived from the C7 system timing. • LOOP: T1 port transmit timing is derived from the corresponding T1 port receive recovered timing, whether internal or external. To use this option, set one end of the IMA link (usually the far-end end) to LOOP, and the other end to SOURCE. Loop timing is independent of shelf timing. **Note:** For an IMA-12 card, if T1 ports used in the IMA group are located on a different card, the IMA group must use Source timing. In this case, to use timing derived from a T1 port in the IMA group, set the C7 shelf to Line timing with the appropriate T1 port as the timing reference.

Configure an IMA group for ATM

Configure an IMA group to transport ATM traffic between nodes.

To configure an IMA group for transport

1. On the Navigation Tree, click the shelf where the IMA group is located, and then click IMA Groups, and click the IMA group being used for transport.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

2. In the **Provisioning** Work Area, set the External Interface to N:
   a. In the External Interface list, click **N**.
   b. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your change.
3. Set other required parameters:
   a. In the Mapping list, click **NNI**.
   b. In the Protection Domain box, type a number greater than 0 and not used for any other transport topology in the network.
   c. In the Timing Mode list, click **Loop** or **Source**, per your site requirements.
   d. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your changes.

Other IMA Group Fields for ATM Transport

The IMA group parameters listed below are not typically changed from the default values.

Parameter	Description
Primary Service State	Specifies the primary service condition of the IMA group. By default this is set to In Service (IS).
Secondary Service State	Specifies the service condition of the IMA group when the Primary Service State is in the Out of Service (OOS) state.
Bandwidth Capacity	Displays the total packet payload capacity that the IMA group can carry in Kbps.
Transmit Bandwidth Used	Displays the total packet payload capacity in Kbps that has been allocated to VP and VC cross-connects leaving the shelf on the IMA group. The value may be greater than the bandwidth capacity if the IMA group has been over subscribed.
Receive Bandwidth Used	Displays the total packet payload capacity in Kbps that has been allocated to VP and VC cross-connects entering the shelf on the IMA group. The value may be greater than the bandwidth capacity if the group has been over subscribed.
Physical Location Identifier	Displays the physical location of the port(s).
Minimum Number of Facilities	Minimum number of required active links for the IMA group to remain in a working state. If the number of active links falls below the specified minimum, a service-affecting alarm (INSUFLNK, or Insufficient Links) is raised for the IMA group. When creating an IMA group, the default is 1.
Max Diff Delay	The maximum number of milliseconds of differential delay that can be tolerated among the links. When creating an IMA group, the default value is 25.
Inhibited	Controls whether the group is allowed to become operational and carry ATM data. The default is N (do not inhibit).
Frame Length	The IMA frame length used by the IMA group. The options are 32, 64, 128, and Max. The default is 128.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Parameter	Description
ALTV1_0	Alternative IMA version 1.0. This parameter is only used for interoperability with older IMA external interfaces, and is not applicable for ATM transport. The default is N.
Symmetry	Displays the symmetry mode. Currently the C7 is configured to operate only in Symmetrical Configuration and Operation mode.
Clock Mode	Specifies the transmit clock mode for an IMA group. Currently the C7 is configured to only support the Common Transmit Clock mode.
Grade of Service	The grade of service that is applied to the IMA group. When creating an IMA group, the default is OFF.
Link Grade of Service	The grade of service that is applied to the IMA links. When creating an IMA group, the default is OFF.
ATM Monitoring	Set this parameter to Y (Yes) to enable ATM diagnostic monitoring. If enabled, an ATM OAM loopback is used to verify point-to-point connectivity with the next line unit. It applies only to ATMNNI and ATMUNI interfaces. The default value is Y for internal interfaces and N (No) for external interfaces.
Payload Scrambling	Configures whether the IMA group is set to enable or disable the scrambling of ATM cells. When configuring for ATM transport, set this parameter to N (disable).
Tx IMA Group ID	The transmit Group ID for the transmit end of the IMA link. You can optionally assign a value from 1 to 255. If not specified, the system assigns the group ID when the IMA group is created.
Tx IMA Group Version	Specifies the transmitted IMA version. The default is 1.1.

For instructions on removing an IMA group, see the *Calix C7 Maintenance Guide*.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring T1 Transport Groups

Quick Turn-Up Outline for T1 TDM Transport

Use this quick turn-up outline to get T1 transport for TDM traffic up and running.

Starting point

Before starting this quick turn-up process, check to see that the following conditions are met:

- All C7 shelves in the T1 transport network have been installed and powered.
- AMP (or ATP) and RAP cards have been installed in the C7 shelves.
- T1-6, T1-8 PWE or DS1-12 PWE cards have been installed in the C7 shelves.

  Note: T1-6 and T1-8 PWE cards support repeater powering; the DS1-12 PWE card requires an external repeater shelf.

- Cables have been connected to the T1 cards in each C7 shelf.

Quick turn-up steps

1. Configure your computer to connect to the front Ethernet port (E1) on a C7 AMP or ATP card.
2. Connect to the E1 port and start the management software.
3. Define network nodes.
4. Set shelf timing for all C7 shelves.
5. Create and configure T1 Groups for TDM transport.

Configuration Rules for T1 TDM Transport

Use these procedures for configuring a T1 transport group to carry TDM traffic between two C7 shelves.

Traffic types supported on T1 transport

You can transport the following services using T1 Transport Groups:

- GR-303 interface groups support DS0 services for 2-wire ground start (2GS), 2-wire loop start (2LS), and 2-wire coin (2COIN) services.
- GR-8 interface groups support DS0 services for 2-wire ground start (2GS), 2-wire loop start (2LS), and 2-wire coin (2COIN) services. GR-8 Mode 1, as well as Mode 2 Coin, only supports non-concentrated services. GR-8 Mode 2 GS and LS support only supports concentrated services.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- GR-57 services support GS, LS, UVG, Coin, PLAR, DID, DDS without error correction (non-concentrated only), 2-wire and 4-wire TO (non-concentrated only), and EBS (non-concentrated only).

T1 transport group creation rules

Follow these rules when planning to configure a T1 transport group to carry TDM traffic on your network:

- In a copper-fed system, an AMP or ATP card is required in the C7 shelves on both sides of a T1 Transport Group (T1TG).
- A maximum of 28 T1 or HDSL ports (or a combination T1 and HDSL ports) can be added to a single T1TG.
- Using a GR-303 Interface Group is not supported on a shelf that is also configured with an RDT T1TG.
- T1TGs support transport over one point-to-point link. Linear chain topologies are not supported.
- Traffic on a T1TG cannot connect to a T1 or HDSL port on the same card. For example, if ports 1 and 2 are part of a T1TG, they cannot connect to port 3 on the same card for GR-303 connection to a switch.
- An HDSL2/4-6 card cannot be used as a switch interface.
- You can have up to 15 shelf-based interface groups per C7 shelf, including voice concentration groups, GR-303 interface groups, H.248 interface groups, and T1TGs. See *GR-8 Interface Group Configuration Rules* (on page 440) for GR-8 slot-based interface groups.

Quick T1 Transport Group process description

Complete the following steps for each node to set up a T1TG for carrying TDM traffic:

- Configure T1 or HDSL ports for transport.
- Create a T1 Transport Group.
- Add ports to the T1 Transport Group.

After you configure the T1 Transport Groups for each node, the communications data links come up and the nodes communicate with each other.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configure Ports for T1 Transport

T1 port parameters for T1 Transport

You can configure ports on a DS1-12 PWE card, T1-6, T1-6 A+T, or T1-8 PWE card for either a DS1 or T1 signal type. Both types can be used in a T1 Transport Group.

The following table lists the parameters used to configure a port for a T1 Transport Group.

Parameter	Value
DS1 Format	ESF (Extended Super Frame)
Equalization (Used with DS1 type)	300 feet (default) Set per your site requirement.
DS1 Line Coding	B8ZS
DS1 Type	DS1 or T1 Set per your site requirement.
DS1 Power (Used with T1 type)	Sink (default) or Source Set per your site requirement. Selecting source puts –130 V on the T1 line.
DS1 Attenuation (Used with T1 type)	0.0 dB (default) or –7.5, –15.0, –22.5 dB Set per your site requirement.
DS1 Map	SEQ
Timing Mode	Source

Configure T1 ports for use in a T1 Transport Group

This procedure shows you how to configure a T1 port for use in a T1 Transport Group.

To configure T1 ports for T1 transport

1. On the Navigation Tree, click a shelf containing T1 ports to use in a T1 Transport Group.
2. On the Selection Filter, click **Port** > **DS1/T1 Port** to display all DS1 and T1 ports from the selected shelf in the Work Area.
3. In the **Provisioning** Work Area, use Ctrl+click to select all T1 ports to configure for use in an interface group. Select at least 2 T1 ports on separate cards.
4. Place the ports out of service:
   a. In the Edit Row, in the PST (Primary Service State) list, click **OOS** (Out of Service).
   b. In the DS1TYPE (DS1 Type) list, click **DS1** or **T1**.
   c. On the toolbar, click **Apply** to place the ports out of service. In the Confirmation dialog box, click **OK**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

5. Re-select the same T1 ports selected in Step 3.
6. In the Edit Row, set the following DS1 parameters:
   a. In the PST (Primary Service State) list, click **IS** (In Service).
   b. In the FMT (DS1 Format) list, click **ESF**.
   c. (For DS1 ports only) In the EQLZ (Equalization) box, type an equalization distance required for your site.
   d. In the LINECDE (DS1 Line Coding) list, click **B8ZS**.
   e. (For T1 ports only) Change the power and attenuation settings per your site.
   f. In the DS1MAP (DS1 Map) list, click **SEQ**.
   g. In the TMGMODE (Timing Mode) list, click **Source**.
   h. On the toolbar, click **Apply** to place the ports back in service and to apply the parameter settings. In the Confirmation dialog box, click **OK** to save your configuration settings.

Configure HDSL Ports for TDM Transport

You can configure an HDSL port for TDM transport between two C7 shelves.

Rules for configuring the line type on HDSL ports

The following rules apply to configuring the line type for HDSL ports:

- You can configure up to 6 ports as 2-wire or up to 3 ports as 4-wire, or create a combination of 2-wire and 4-wire ports.
- For a 4-wire line type, you can only use ports 1, 3, and 5. Before you configure a 4-wire port, you must delete the next consecutive port from the card (for example, to set port 1 to 4-wire, delete port 2).

HDSL port parameters for TDM transport

The following table lists the parameters for configuring an HDSL port for TDM transport.

Parameter	Value
DS1 Format (required)	Set to ESF or SF per your site requirement.
Line Power	Set to SINK (default) or SOURCE per your site requirement.
Grade of Service	Set to OFF (default), DEFLT, or a pre-defined grade-of-service profile number, per your site requirement.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Parameter	Value
Line Type	Set to 2WIRE (default) or 4WIRE, per your site requirement.
Terminal Type	• Set to COT (default) if the port is located on the COT shelf (that is, the IDT in the T1 transport group). • Set to RT if the port is located on the remote shelf (the RDT in the T1 transport group).
Signal-to-Noise Ratio Margin Threshold (near-end)	Set to a value from 1 to 15 (or set to 0 to disable) per your site requirement.
Loop Attenuation Threshold (near-end)	Set to a value from 1 to 127 (or set to 0 to disable) per your site requirement.
DS1 Map	Set to SEQ.

Configure HDSL ports for TDM

This procedure shows you how to configure an HDSL port for TDM traffic.

To configure an HDSL port for TDM traffic

1. On the Navigation Tree, click an HDSL card to view the ports, and then click the HDSL port to be configured for TDM traffic.
2. In the **Provisioning** Work Area, place the port out of service:
   a. In the Primary Service State (PST) list, click **OOS** (Out of Service).
   b. On the toolbar, click **Apply** to place the port out of service. In the Confirmation dialog box, click **OK**.
3. Set the following required parameters:
   a. In the DS1 Format list, click **ESF** or **SF** as required for your site.
   b. In the Line Power list, click **SINK** or **SOURCE** as required for your site.
   c. If you are applying a grade of service, in the Grade of Service list click **DEFLT** or select a grade of service profile number that you have created for HDSL service.
   d. In the Line Type list, click **2WIRE** or **4WIRE** as required for your site.
   e. In the Terminal Type list, click **COT** if the port is located in the COT (that is, the IDT shelf in the T1TG) or **RT** if the port is located in the RT (the RDT in the T1TG).
   f. In the Signal-to-Noise Margin Threshold and Loop Attenuation Threshold boxes, type the values required for your site.
   g. In the DS1 Map list, click **SEQ**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

h. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your changes.

4. Place the port back in service:

   a. In the Primary Service State list, click **IS** (In Service).

   b. On the toolbar, click **Apply** to place the port back in service. In the Confirmation dialog box, click **OK**.

Create a T1 Transport Group

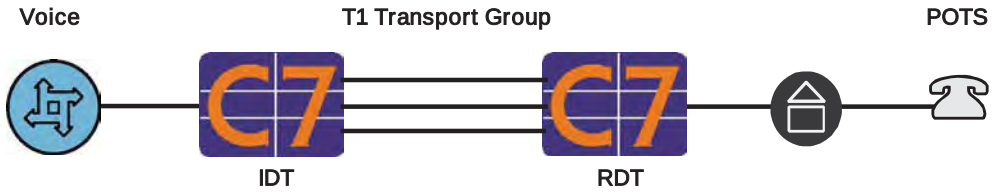
Create a T1 Transport group on each shelf.

T1 Transport Group network topologies

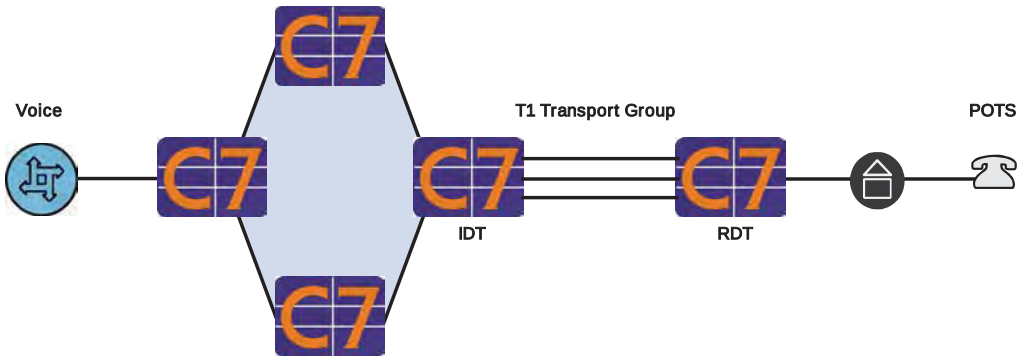
T1 TDM transport supports 1 hop from the RDT node to the IDT node. The 1-hop restriction does not prevent the TDM traffic from being passed onto fiber transport.

Two possible network topologies include:

- Point-to-point, where the shelf with the IDT has a direct connection to a Class 5 switch.



- Copper-fed link off a fiber ring, where the shelf with the IDT passes the copper-fed traffic onto fiber transport for switch connection at another node.



Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

For this procedure:

- IDT refers to the interface group closer to the network and looking toward the subscriber (such as at a central office node).
- RDT refers to the interface group closer to the subscriber and looking toward the network (such as at an outdoor cabinet).

To create a T1 Transport Group

1. On the File menu, click **Create** > **Interface Group** > **T1 Transport** > **T1 Transport Group** to open the Create T1 Transport Group dialog box.
2. Which node are you configuring?
   a. If you are at the IDT, finish with Step 3.
   b. If you are at the RDT, finish with Step 4.
3. In the Create T1 Transport Group dialog box, set the following interface group parameters for the IDT node:
   a. In the Shelf list, select the shelf ID for the IDT.
   b. In the IDT Interface Group list, select an IG number in the list.
   c. Ignore the entry in the second Shelf list.
   d. In the RDT Interface Group list, click **Type In An RDT** from the list.
   e. In the Please Type In RDT box, type the interface group ID to use at the RDT. For example: **N2-1-IG1**.
   f. Click **OK** to create the interface group.
4. In the Create T1 Transport Group dialog box, set the following interface group parameters for the RDT node:
   a. Ignore the entry in the top Shelf list.
   b. In the IDT Interface Group list, click **Type In An IDT** from the list.
   c. In the Please Type In IDT box, type the interface group ID to use at the IDT. For example: **N1-1-IG1**.
   d. In the second Shelf list, select the shelf ID for the RDT.
   e. In the RDT Interface Group list, select an IG number in the list.
   f. Click **OK** to create the interface group.

T1TG alarms after creating a T1 Transport Group

When you create a T1 Transport Group, the system reports two alarms for failures on the Embedded Operation Channel (EOC) and Timeslot Management Channel (TMC) communications channels. These alarms clear as soon as you create a T1 Transport Group on the shelf at the opposite end and connect the shelves with T1 or HDSL interfaces.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Assign Ports to a T1 Transport Group

After configuring T1 or HDSL ports for T1 transport, you can assign up to 28 ports to a T1 interface group.

Rules for assigning ports to a T1 Transport Group

- You must correctly configure T1 or HDSL ports for use in an interface group before you can assign them to a group. The default settings on a new T1 port are the correct settings for use in an interface group. The default settings on a new HDSL port must be changed in order to use the port in a T1 interface group.

  If a port is not configured correctly, the system rejects the assignment to an interface group and displays the following error message:

  `The port parameters are invalid for assigning a DS1 IG.`

- Each T1 or HDSL line between an IDT and RDT must be connected to ports that are assigned the same link number.

  Example: The T1 port assigned to DS1 number 1 in the RDT interface group (e.g. N2-1-IG1-**1**), must be physically connected to the T1 port assigned to DS1 number 1 in the IDT interface group (e.g. N1-1-IG1-**1**).

- A maximum of four ports on a T1-6 or HDSL2/4-6 card can support primary or secondary interface group links (links 1 or 2). The remaining two ports can be assigned to any interface group as link 3 or higher.

  If more than four ports on a card are assigned as primary or secondary interface group links, the system rejects the assignment to an interface group and displays the following error message:

  `Card does not have enough available HDLCs to complete the request.`

  In such cases, assign the primary and secondary links to ports on a different T1-6 or HDSL2/4-6 card.

- For T1-8 PWE and DS1-12 PWE cards, there is no limitation regarding the number of ports that can be assigned to the primary or secondary interface group links.

Recommendations for assigning ports to a T1 interface group

- Assign two T1 or HDSL ports to an interface group, with ports on separate cards, assigned to links 1 and 2. This provides protection against equipment failure for the EOC and TMC communication channels.
- Distribute T1 or HDSL port assignments evenly across multiple cards to provide protection against equipment failure for subscriber traffic.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Assign T1 or HDSL ports to a T1 Transport Group

The following procedure assumes that you are adding T1 ports to a T1 transport group.

To assign ports to a T1 transport group

1. On the File menu, click:
   - (in iMS) **Create** > **Interface Group** > **T1 Transport** > **T1 TG DS1**
   - (in CMS) **Create** > **C7** > **Interface Group** > **T1 Transport** > **T1 TG DS1**
2. In the Interface Group DS1 dialog box, Available T1 Ports area:
   a. In the Shelf list, select a shelf containing T1 Transport Groups.
   b. In the Interface Group list, select an interface group on the selected shelf.
   c. In the available T1 ports list, use Ctrl+click to select the T1 ports to add to the interface group. DS1 numbers are assigned to the ports in the order that you click them.
   d. Click **Add** to place the T1 ports with assigned DS1 numbers in the T1 Ports To Be Added to Interface Group as IG-DS1 list.
3. When you are done adding ports, click **OK** to create the T1 assignments.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Chapter 6

Activating C7 Subscriber Service

Use the subscriber service activation tools to activate and reconfigure C7 voice, video, and data services on a per-subscriber or per port/ONT basis. From a single screen, you can activate service on multiple subscriber ports across multiple C7 networks.

In the Add Subscriber Services dialog box, you can:

- Create and apply logically distinct CMS-specific video and data templates for flexible service bundling.
- Enter activation parameters using context-sensitive fields for specific subscriber cards.
- Change the uplink for existing subscriber services.

In the Services screen at the port level (for xDSL ports and ONTs), you can:

- Activate service.
- Modify and delete port settings.
- Verify data and video service.

See the *Calix C7 Broadband Data Services Guide* for information on configuring broadband data services.

See the *Calix C7 Video Services Guide* for information on configuring video services.

See the *Calix C7 Voice Services Guide* and *Calix C7 VoIP Services Guide* for information on configuring voice and VoIP services.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Before You Begin

Before you activate subscriber service, you must complete the following:

- Create ATM traffic profiles for video channel and data transport. For more information, see the *C7 Video Services Guide* and *C7 Broadband Data Services Guide*. For examples, see *Sample Global ATM Traffic Profiles* (on page 82). For data subscriber templates for use with an ATM uplink, you can optionally create global ADSL templates. For more information, see *Overview of Global Profiles (on page 77)*.
- Verify that the uplink to be used by the subscribers is listed in the Subscriber > Uplinks work area on the C7 network. If needed, create one. See *Creating a Subscriber Uplink* (on page 294).
- Create video and data subscriber templates for your subscribers. See *Creating a Video Subscriber Template* (on page 276) and *Creating a Global Data Subscriber Template* (on page 289).
- Enable global profiles on all C7 networks you are applying the profiles to. For more information, see Viewing or Managing C7 Network Parameters.

To simplify provisioning of services for new subscribers, create subscriber templates that define your different service offerings only *once*, instead of repeatedly provisioning the configuration information every time you add a new subscriber. Subscriber templates are applied to access ports by the *Add Subscriber* tool and in the Services screen when you add new subscriber connections to the network.

You can configure subscriber templates for xDSL, bonding group, or ONT Ethernet access port types. When creating a data subscriber template, you further define a template type based on the subscriber access port:

- "xDSL - EXA," "BondingGroup - EXA," and "ONT - EXA" template types utilize the C7 EXA Powered switch fabric, requiring RAP-10GE cards for shelf control.
- "xDSL," "BondingGroup," and "ONT" template types utilize the C7 Multiprotocol switch fabric, and can be used with any shelf control card.

You can create multiple templates to support various types of service offered. For example, “DSL Gold” and "DSL Platinum" for Internet subscribers; “ONT 10Mbps” and "ONT 15Mbps" for ONT Internet subscribers; and so on.

Once the above requirements are met, have on hand the following information to begin activating services:

- The port address (network, node, shelf, and card, and number) for each subscriber.
- The uplink AID for each subscriber.
- The services (video, data, voice) to be activated for each subscriber.
- The data and video subscriber templates to use for each service.
- The bandwidth constraint IDs to use, if any, to use for data and video subscriber services.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Running a Pre-Service DSL Test with Single-End Line Testing (SELT)

Calix Management System (CMS) supports pre-service Single-End Line Testing (SELT) from these Calix C7 cards that use the Conexant G24 DSL chipset:

- ADSL2-24
- COMBO2-24

Run SELT prior to adding a DSL modem and subscriber service. The test parameters returned by SELT include the date and time of the test, a test validity indicator, loop length (measured in feet), loop end (open or closed circuit), and the upstream and downstream Shannon Capacity (theoretical maximum bandwidth of the copper pair, measured in bits per second).

For details about running a SELT pre-service test, refer to the *Calix C7 Troubleshooting Guide* or the *Calix C7 Broadband Data Service Guide.*

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Creating a Global Video Subscriber Template

This section includes the following topics:

- *(EXA) xDSL Subscriber Templates* (on page 279)
- *(EXA) ONT Subscriber Templates* (on page 279)
- *(MP) ADSL2-Based Video Subscriber Template* (on page 280)
- *(MP) VDSL2-Based Video Subscriber Template* (on page 283)
- *(MP) ONT Video Subscriber Template* (on page 287)

You can create up to 500 global video subscriber templates in CMS.

Creating a video subscriber template requires Full CMS Administration privileges.

(EXA) xDSL Subscriber Templates

This procedure applies to EXA subscribers on C7 VDSL2-based card ports; ADSL2+ or VDSL2 CPE is expected.

Prerequisites:

- VLAN-IF Template for video service, with MCAST Profile
- An xDSL service template for video, appropriate for the expected xDSL CPE

  Note: In xDSL subscriber templates, you can enter override values for the min/max downstream and upstream rates in the referenced xDSL template. This allows you to provision more service offerings with fewer xDSL templates. For example, for multiple service offerings, one xDSL template can be used in multiple subscriber templates, using override values to specify the differences in supported rates.

- xDSL Bonding Group(s) created, as required.

  Note: The aggregate min/max rates set during the creation of Bonding Groups are overridden by the Bonding Group bandwidth min/max rates in subscriber templates.

- VLAN-IF Template for data service
- Ethernet Bandwidth Profiles for data service
- An xDSL service template for data, appropriate for the expected xDSL CPE

To create a video subscriber template (for VDSL2-based card ports)

1. On the Navigation Tree, click the CMS level.
2. In the Work Area, click **Subscriber Templates** > **C7** > **Video**.
3. On the toolbar, click **Create** to open the Subscriber Template (New C7 Video Subscriber Template) dialog box.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

4. In the Template ID box, type an available ID number (from 1 to 500) for the new template.
5. In the Description box, type a brief description for the template (up to 32 characters in length).

Note: For the next step, perform only step 6 or only step 7, depending on whether or not bonding groups are used.

6. (Non-bonding only) For subscribers on individual xDSL ports, do the following:
   a. In the Template Type list, select **xDSL-EXA**.
   b. In the xDSL Template list, select an xDSL service template to apply to xDSL ports.

Note: The xDSL service template will be different for ADSL2+ versus VDSL2 CPE. Be sure to select the appropriate template; in turn, be sure to note which video subscriber templates are intended for which xDSL CPE.

   c. (Optional) In the xDSL template override text boxes, enter override values for the min/max downstream and min/max upstream rates. If overrides are used, all four values must be entered.
7. (Bonding only) For subscribers on xDSL port bonding groups, do the following:
   a. In the Template Type list, select **BondingGroup-EXA**.
   b. In the xDSL Template list, select an xDSL service template to apply to the individual member ports of the bonding group.

Note: The service type within the selected xDSL Template should match what is already used by the member ports of the bonding group(s), set during the creation of the bonding group(s).

Note: For Bonding Groups on VDSL2-based cards, xDSL templates with the following service types can be used: VDSL2, VDSL2MM, ADSL2, ADSL2+, ANNEXM, GDMT, GLITE, MM, MM+, READSL2, T1413

   c. (Optional) In the xDSL template override text boxes, enter override values for the min/max downstream and min/max upstream rates. If overrides are used, all four values must be entered.
   d. Enter the bonding group rates as follows:
      - Group Min Downstream Rate: Combined min downstream rates of all member ports.
      - Group Max Downstream Rate: Combined max downstream rates of all member ports, plus a cushion of 32 kbps.
      - Group Min Upstream Rate: Combined min upstream rates of all member ports.
      - Group Max Upstream Rate: Combined max upstream rates of all member ports, plus a cushion of 32 kbps.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Note: These rates will override the aggregate rates set during the creation of Bonding Groups. Individual member port rates will be set by the selected xDSL Template or its override values (if present).

8. In the VLAN-IF Template list, select the ID of the VLAN-IF template created for video service (with MCAST Profile).
9. For the EXA Video VLAN-IF, in the Tx/Rx EthBW Prof list, select **None**.
10. Click **Create** to save the new Subscriber Template.

To create a data subscriber template (VDSL2)

1. On the Navigation Tree, click the CMS level.
2. In the Work Area, click **Subscriber Templates > Data**.
3. On the toolbar, click **Create**.
4. Choose the following settings:
   - ID = <unused ID>
   - Description = <text description>
   - (Non-bonding only)
     - Template Type = XDSL-EXA
     - xDSL Template = <ID of the xDSL template created for data service>
     - (Optional) In the xDSL template override text boxes, enter override values for the min/max downstream and min/max upstream rates. If overrides are used, all four values must be entered.
   - (Bonding only)
     - Template Type = BondingGroup-EXA
     - xDSL Template = <ID of the xDSL template created for data service>
     - (Optional) In the xDSL template override text boxes, enter override values for the min/max downstream and min/max upstream rates. If overrides are used, all four values must be entered.
     - Group Min Downstream Rate = Combined min downstream rates of all member ports.
     - Group Max Downstream Rate = Combined max downstream rates of all member ports, plus a cushion of 32 kbps.
     - Group Min Upstream Rate = Combined min upstream rates of all member ports.
     - Group Max Upstream Rate = Combined max upstream rates of all member ports, plus a cushion of 32 kbps.
   - VLAN-IF Template = <ID of the VLAN-IF template created for data service>

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- Data VLAN-IF > Tx/Rx EthBW Prof = <IDs of profiles created for this application>

Note: The Tx/Rx EthBW Prof fields should be set to "None" if Ethernet Bandwidth Profiles are specified in the VLAN-IF template.

5. Click **Create** to save the new Subscriber Template.

(EXA) ONT Subscriber Templates

This procedure applies to EXA subscribers on GPON ONT Ethernet ports (OLTG-4E card).

Prerequisites:

- VLAN-IF Template for video service, with MCAST Profile
- VLAN-IF Template for data service
- Ethernet Bandwidth Profiles for data service

To create a video subscriber template (for ONT Ethernet ports)

1. On the Navigation Tree, click the CMS level.
2. In the Work Area, click **Subscriber Templates** > **C7** > **Video**.
3. On the toolbar, click **Create** to open the Subscriber Template (New C7 Video Subscriber Template) dialog box.
4. In the Template ID box, type an available ID number (from 1 to 500) for the new template.
5. In the Description box, type a brief description for the template (up to 32 characters in length).
6. In the Template Type list, select **ONT-EXA**.
7. In the VLAN-IF Template list, select the ID of the VLAN-IF template created for video service (with MCAST Profile).
8. For the EXA Video VLAN-IF, in the Tx/Rx EthBW Prof list, select **None**.
9. Click **Create** to save the new Subscriber Template.

To create a data subscriber template (GPON ONT)

1. On the Navigation Tree, click the CMS level.
2. In the Work Area, click **Subscriber Templates > Data**.
3. On the toolbar, click **Create**.
4. Choose the following settings:

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- ID = <unused ID>
- Description = <text description>
- Template Type = ONT-EXA
- VLAN-IF Template = <ID of the VLAN-IF template created for data service>
- Data VLAN-IF > Tx/Rx EthBW Prof = <IDs of profiles created for this application>

Note: The Tx/Rx EthBW Prof fields should be set to "None" if Ethernet Bandwidth Profiles are specified in the VLAN-IF template.

5. Click **Create** to save the new Subscriber Template.

(MP) ADSL2-Based Video Subscriber Template

This procedure applies to subscribers on C7 ADSL2-based card ports; ADSL2/2+ CPE is expected.

Prerequisites:

- A traffic profile for the IP VC has already been created.
- Traffic profiles for Video Subscriber Channels (VSCs) and Video Subscriber Service (VSS) have already been created.
- An xDSL service template for video has already been created, and is appropriate for the expected xDSL CPE.

Note: In xDSL subscriber templates, you can enter override values for the min/max downstream and upstream rates in the referenced xDSL template. This allows you to provision more service offerings with fewer xDSL templates. For example, for multiple service offerings, one xDSL template can be used in multiple subscriber templates, using override values to specify the differences in supported rates.

Note: If your video network utilizes multicast boot channels, contact the Calix Technical Assistance Center (TAC) for specific configuration recommendations for the middleware server and STB vendors you are using.

To create a video subscriber template (for ADSL2-based card ports)

1. On the Navigation Tree, click the CMS level.
2. In the Work Area, click **Subscriber Templates** > **C7** > **Video**.
3. On the toolbar, click **Create** to open the Subscriber Template (New C7 Video Subscriber Template) dialog box.
4. In the Template ID box, type an available ID number (from 1 to 500) for the new template.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

5. In the Description box, type a brief description for the template (up to 32 characters in length).

Note: For the next step, perform only step 6 or only step 7, depending on whether or not bonding groups are used.

6. (Non-bonding only) For subscribers on individual xDSL ports, do the following:
   a. In the Template Type list, select **xDSL**.
   b. In the xDSL Template list, select an xDSL service template to apply to xDSL ports.
   c. (Optional) In the xDSL template override text boxes, enter override values for the min/max downstream and min/max upstream rates. If overrides are used, all four values must be entered.
7. (Bonding only) For subscribers on xDSL port bonding groups, do the following:
   a. In the Template Type list, select **BondingGroup**.
   b. In the xDSL Template list, select an xDSL service template to apply to the individual member ports of the bonding group.

Note: The service type within the selected xDSL Template should match what is already used by the member ports of the bonding group(s), set during the creation of the bonding group(s).

Note: For Bonding Groups, only xDSL templates with the following service types can be used:
• VDSL2-based cards: VDSL2, VDSL2MM, ADSL2, ADSL2+, ANNEXM, GDMT, GLITE, MM, MM+, READSL2, T1413
• ADSL2A-based cards: ADSL2, ADSL2+, ANNEXM, READSL2

   c. (Optional) In the xDSL template override text boxes, enter override values for the min/max downstream and min/max upstream rates. If overrides are used, all four values must be entered.
   d. Enter the bonding group rates as follows:
      - Group Min Downstream Rate: Combined min downstream rates of all member ports.
      - Group Max Downstream Rate: Combined max downstream rates of all member ports, plus a cushion of 32 kbps.
      - Group Min Upstream Rate: Combined min upstream rates of all member ports.
      - Group Max Upstream Rate: Combined max upstream rates of all member ports, plus a cushion of 32 kbps.

Note: These rates will override the aggregate rates set during the creation of Bonding Groups. Individual member port rates will be set by the selected xDSL Template or its override values (if present).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

8. In the Video Service Info area, do the following:

   a. In the Maximum Streams box, enter the total number of video streams allowed per subscriber port, and click **Update** to view the parameters for video subscriber VCs.

   b. In each Subscriber Vid Ch Stream row, do the following

      - Edit the VP and VC values as required.
      - In the Trf Prof list, confirm/select the correct profile for video channel streams.

   c. In the Subscriber Service Stream row, do the following:

      - Edit the VP and VC values as required.
      - In the Trf Prof list, confirm/select the correct profile.

   d. For the Subscriber IP Channel Stream row, perform one of the following steps:

      - (For L2 video only) Select the Subscriber IP Channel Stream row and click **Remove**. This stream should not be present for L2 video service models.
      - (For L3/Routed video) In the Subscriber IP Channel Stream row, do the following:
        - Edit the VP and VC values as required. If packet mode is disabled (optional for ADSL2+ CPE), this VPI/VCI will be used for the IPVC. Otherwise, this VPI/VCI will be ignored, and the system will automatically create an endpoint (EP) connection ID for the IPVC instead.
        - In the Trf Prof list, confirm/select the correct profile.
        - Edit the other parameters as required.

   Note: If the traffic profile is UBR and the Path is protected, you must select the 'Bridged' protection class (PC).

   Note: If a back traffic profile (**Back Trf Prof**) is not selected, the standard profile (**Trf Prof**) is used for back traffic.

   Note: If the subscriber will also have data service, confirm that the Path setting of the Subscriber IP Channel Stream row matches that of the Data VC row in the Data Subscriber template. To access the Data Subscriber template, in the Work Area, click **Subscriber Templates** > **C7** > **Data**.

   e. In the **Video Bandwidth** box, enter the maximum amount of bandwidth allowed for video services at the subscriber drop. This should be based on the following calculations:

      - The sum of the highest-rate video streams simultaneously allowed on the port. This does not include the bandwidth of the data carousel channels on the Subscriber Service stream, or the bandwidth of the IPVC in the Subscriber IP Channel stream; the bandwidth for these streams is accounted for in ADSL port parameters.

   f. In the Max Loan Bandwidth box, type the maximum amount of bandwidth that can be loaned to UBR traffic when not in use by video.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

9. Click **Create** to save the new Subscriber Template.

Verifying the ADSL SNR margin value

After an ADSL template has been applied to a video subscriber template, Calix recommends checking the actual downstream Signal-to-Noise Ratio (SNR) margin on the provisioned ports.

To support the typical bandwidth requirement for video + data service, Calix recommends an actual downstream SNR margin of 10 dB or higher. If the actual SNR margin is lower than 10 dB, you may need to adjust the bandwidth on your Internet VC, or limit your configuration to one video stream per set top box. (A minimum SNR margin of 8 dB may work in some environments, but this increases the chance of encountering bandwidth-related problems in the future, which could require maintenance or reconfiguration of the IPTV installation.)

To view the actual downstream SNR margin settings for your network, check the ADSL Call Status screen.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

(MP) VDSL2-Based Video Subscriber Template

This procedure applies to subscribers on C7 VDSL2-based card ports; ADSL2+ or VDSL2 CPE is expected.

Prerequisites:

- A traffic profile for the IP VC has already been created.

  Note: Traffic profiles for Video Subscriber Channels (VSCs) and Video Subscriber Service (VSS) are not required. As described in the procedure below, VSC-related parameters are ignored and VSS-related parameters are deleted.

- An xDSL service template for video has already been created, and is appropriate for the expected xDSL CPE.

  Note: In xDSL subscriber templates, you can enter override values for the min/max downstream and upstream rates in the referenced xDSL template. This allows you to provision more service offerings with fewer xDSL templates. For example, for multiple service offerings, one xDSL template can be used in multiple subscriber templates, using override values to specify the differences in supported rates.

Note: If your video network utilizes multicast boot channels, contact the Calix Technical Assistance Center (TAC) for specific configuration recommendations for the middleware server and STB vendors you are using.

To create a video subscriber template (for VDSL2-based card ports)

1. On the Navigation Tree, click the CMS level.
2. In the Work Area, click **Subscriber Templates** > **C7** > **Video**.
3. On the toolbar, click **Create** to open the Subscriber Template (New C7 Video Subscriber Template) dialog box.
4. In the Template ID box, type an available ID number (from 1 to 500) for the new template.
5. In the Description box, type a brief description for the template (up to 32 characters in length).

   Note: For the next step, perform only step 6 or only step 7, depending on whether or not bonding groups are used.

6. (Non-bonding only) For subscribers on individual xDSL ports, do the following:
   a. In the Template Type list, select **xDSL**.
   b. In the xDSL Template list, select an xDSL service template to apply to xDSL ports.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Note: The xDSL service template will be different for ADSL2+ versus VDSL2 CPE. Be sure to select the appropriate template; in turn, be sure to note which video subscriber templates are intended for which xDSL CPE.

c. (Optional) In the xDSL template override text boxes, enter override values for the min/max downstream and min/max upstream rates. If overrides are used, all four values must be entered.

7. (Bonding only) For subscribers on xDSL port bonding groups, do the following:

a. In the Template Type list, select **BondingGroup**.

b. In the xDSL Template list, select an xDSL service template to apply to the individual member ports of the bonding group.

Note: The service type within the selected xDSL Template should match what is already used by the member ports of the bonding group(s), set during the creation of the bonding group(s).

Note: For Bonding Groups, only xDSL templates with the following service types can be used:
• VDSL2-based cards: VDSL2, VDSL2MM, ADSL2, ADSL2+, ANNEXM, GDMT, GLITE, MM, MM+, READSL2, T1413
• ADSL2A-based cards: ADSL2, ADSL2+, ANNEXM, READSL2

c. (Optional) In the xDSL template override text boxes, enter override values for the min/max downstream and min/max upstream rates. If overrides are used, all four values must be entered.

d. Enter the bonding group rates as follows:

- Group Min Downstream Rate: Combined min downstream rates of all member ports.
- Group Max Downstream Rate: Combined max downstream rates of all member ports, plus a cushion of 32 kbps.
- Group Min Upstream Rate: Combined min upstream rates of all member ports.
- Group Max Upstream Rate: Combined max upstream rates of all member ports, plus a cushion of 32 kbps.

Note: These rates will override the aggregate rates set during the creation of Bonding Groups. Individual member port rates will be set by the selected xDSL Template or its override values (if present).

8. In the Video Service Info area, do the following:

a. In the Maximum Streams box, enter the total number of video streams allowed per subscriber port, and click **Update** to view the parameters for video subscriber VCs.

b. In the Subscriber Vid Ch Stream rows, ignore all parameters (they are not applicable for VDSL2-based cards, yet they cannot be removed from the tool).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

c. Select the Subscriber Service Stream row and click **Remove**. This stream is not applicable for VDSL2-based cards, and should be removed from the tool.

d. For the Subscriber IP Channel Stream row, perform one of the following steps:

- (For L2 video only) Select the Subscriber IP Channel Stream row and click **Remove**. This stream should not be present for L2 video service models.
- (For L3/Routed video only) In the Subscriber IP Channel Stream row, do the following:
  - Edit the VP and VC values as required. If packet mode is disabled (optional for ADSL2+ CPE), this VPI/VCI will be used for the IPVC. Otherwise, this VPI/VCI will be ignored, and the system will automatically create an endpoint (EP) connection ID for the IPVC instead.
  - In the Trf Prof list, confirm/select the correct profile.
  - Edit the other parameters as required.

Note: If the traffic profile is UBR and the Path is protected, you must select the 'Bridged' protection class (PC).

Note: If a back traffic profile (**Back Trf Prof**) is not selected, the standard profile (**Trf Prof**) is used for back traffic.

Note: If the subscriber will also have data service, confirm that the Path setting of the Subscriber IP Channel Stream row matches that of the Data VC row in the Data Subscriber template. To access the Data Subscriber template, in the Work Area, click **Subscriber Templates** > **C7** > **Data**.

e. In the **Video Bandwidth** box, enter the maximum amount of bandwidth allowed for video services at the subscriber drop. This should be based on the following calculations:

- The sum of the highest-rate video streams simultaneously allowed on the port, plus the expected* bandwidth required for data carousel channels on the port. This does not include the bandwidth of the IPVC, as this is accounted for in xDSL port parameters.

***Note:** The expected bandwidth required for data carousel channels can be determined as follows: In simplest terms, this should be the sum of the maximum number of data carousels that will be joined at the same time. If the bandwidth differs between individual data carousels, consider the various combinations of data carousel channels that may join simultaneously, and choose the combination with the highest-bandwidth sum.

f. In the Max Loan Bandwidth box, type the maximum amount of bandwidth that can be loaned to UBR traffic when not in use by video.

9. Click **Create** to save the new Subscriber Template.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Verifying the ADSL SNR margin value

After an ADSL template has been applied to a video subscriber template, Calix recommends checking the actual downstream Signal-to-Noise Ratio (SNR) margin on the provisioned ports.

To support the typical bandwidth requirement for video + data service, Calix recommends an actual downstream SNR margin of 10 dB or higher. If the actual SNR margin is lower than 10 dB, you may need to adjust the bandwidth on your Internet VC, or limit your configuration to one video stream per set top box. (A minimum SNR margin of 8 dB may work in some environments, but this increases the chance of encountering bandwidth-related problems in the future, which could require maintenance or reconfiguration of the IPTV installation.)

To view the actual downstream SNR margin settings for your network, check the ADSL Call Status screen.

(MP) ONT Video Subscriber Template

This procedure applies to subscribers on GPON ONT Ethernet ports.

Prerequisite:

- A traffic profile for the IP VC has already been created.

  Note: Traffic profiles for Video Subscriber Channels (VSCs) are not required. As described in the procedure below, VSC-related parameters are ignored.

Note: If your video network utilizes multicast boot channels, contact the Calix Technical Assistance Center (TAC) for specific configuration recommendations for the middleware server and STB vendors you are using.

To create a video subscriber template (for ONT Ethernet ports)

1. On the Navigation Tree, click the CMS level.
2. In the Work Area, click **Subscriber Templates** > **C7** > **Video**.
3. On the toolbar, click **Create** to open the Subscriber Template (New C7 Video Subscriber Template) dialog box.
4. In the Template ID box, type an available ID number (from 1 to 500) for the new template.
5. In the Description box, type a brief description for the template (up to 32 characters in length).
6. In the Template Type list, select **ONT**.
7. In the Video Service Info area, do the following:

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

a. In the Maximum Streams box, enter the total number of video streams allowed per subscriber port, and click **Update** to view the parameters for video subscriber VCs.

b. In the Subscriber Vid Ch Stream rows, ignore all parameters (they are not applicable for OLTG cards, yet they cannot be removed from the tool).

c. For the Subscriber IP Channel Stream row, perform one of the following steps:

- (For L2 video only) Select the Subscriber IP Channel Stream row and click **Remove**. This stream should not be present for L2 video service models.
- (For L3/Routed video only) In the Subscriber IP Channel Stream row, do the following:
  - Edit the Index ID as required.
  - In the Trf Prof list, confirm/select the correct profile.
  - Edit the other parameters as required.

Note: If the traffic profile is UBR and the Path is protected, you must select the 'Bridged' protection class (PC).

Note: If a back traffic profile (**Back Trf Prof**) is not selected, the standard profile (**Trf Prof**) is used for back traffic.

Note: If the subscriber will also have data service, confirm that the Path setting of the Subscriber IP Channel Stream row matches that of the Data VC row in the Data Subscriber template. To access the Data Subscriber template, in the Work Area, click **Subscriber Templates** > **C7** > **Data**.

d. In the **Video Bandwidth** box, enter the maximum amount of bandwidth allowed for video services at the subscriber drop. This should be based on the following calculations:

- The sum of the highest-rate video streams simultaneously allowed on the port, plus the expected* bandwidth required for data carousel channels on the port, plus the bandwidth of the IPVC if using a GFR traffic profile.

***Note:** The expected bandwidth required for data carousel channels can be determined as follows: In simplest terms, this should be the sum of the maximum number of data carousels that will be joined at the same time. If the bandwidth differs between individual data carousels, consider the various combinations of data carousel channels that may join simultaneously, and choose the combination with the highest-bandwidth sum.

Note: GPON subscribers in the AVT provisioning mode do not require an aggregated data carousel channel.

e. In the Max Loan Bandwidth box, type 0.

8. Click **Create** to save the new Subscriber Template.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Creating a Global Data Subscriber Template

To simplify provisioning of services for new subscribers, create subscriber templates that define your different service offerings only *once*, instead of repeatedly provisioning the configuration information every time you add a new subscriber. Subscriber templates are applied to access ports by the *Add Subscriber* tool and in the Services screen when you add new subscriber connections to the network.

You can configure subscriber templates for xDSL, bonding group, or ONT Ethernet access port types. When creating a data subscriber template, you further define a template type based on the subscriber access port:

- "xDSL - EXA," "BondingGroup - EXA," and "ONT - EXA" template types utilize the C7 EXA Powered switch fabric, requiring RAP-10GE cards for shelf control.
- "xDSL," "BondingGroup," and "ONT" template types utilize the C7 Multiprotocol switch fabric, and can be used with any shelf control card.

You can create multiple templates to support various types of service offered. For example, “DSL Gold” and "DSL Platinum" for Internet subscribers; “ONT 10Mbps” and "ONT 15Mbps" for ONT Internet subscribers; and so on.

To create a data subscriber template

Prerequisites:

- (Optional) VLAN-IF Template, to define settings for subscriber-side VLAN interfaces.
- (MP only) Traffic Profile(s) for data service.
- (EXA only) Ethernet Bandwidth Profile(s) for data service.
- (xDSL only) xDSL Template(s) created, appropriate for the expected CPE.

  Note: In xDSL subscriber templates, you can enter override values for the min/max downstream and upstream rates in the referenced xDSL template. This allows you to provision more service offerings with fewer xDSL templates. For example, for multiple service offerings, one xDSL template can be used in multiple subscriber templates, using override values to specify the differences in supported rates.

- (xDSL only) xDSL Bonding Group(s) created, as required.

  Note: The aggregate min/max rates set during the creation of Bonding Groups are overridden by the Bonding Group bandwidth min/max rates in subscriber templates.

Procedure:

1. On the Navigation Tree, click the CMS level.
2. In the Work Area, click **Subscriber Templates** > **C7** > **Data**.
3. On the toolbar, click **Create** to open the Subscriber Template dialog box.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

4. In the Template ID box, type an ID number (from 1 to 500) for the new template.
5. In the Description box, type a brief description for the template (up to 32 characters).
6. In the Template Type list, select the type of subscriber port for the template:
   - **xDSL**, **BondingGroup**, and **ONT** types apply to data services delivered over the C7 Multiprotocol switch fabric.
   - **xDSL - EXA**, **BondingGroup - EXA**, and **ONT - EXA** types apply to data services delivered over the C7 EXA switch fabric.
7. (xDSL, non-bonding only) For subscribers on individual xDSL ports, do the following:
   a. In the xDSL Template list, select an xDSL service template to apply to xDSL ports.
   b. (Optional) In the xDSL template override text boxes, enter override values for the min/max downstream and min/max upstream rates. If overrides are used, all four values must be entered.
8. (xDSL, bonding only) For subscribers on xDSL port bonding groups, do the following:
   a. In the xDSL Template list, select an xDSL service template to apply to the individual member ports of the bonding group.

   Note: The service type within the selected xDSL Template should match what is already used by the member ports of the bonding group(s), set during the creation of the bonding group(s).

   Note: For Bonding Groups, only xDSL templates with the following service types can be used:
   • VDSL2-based cards: VDSL2, VDSL2MM, ADSL2, ADSL2+, ANNEXM, GDMT, GLITE, MM, MM+, READSL2, T1413
   • ADSL2A-based cards: ADSL2, ADSL2+, ANNEXM, READSL2

   b. (Optional) In the xDSL template override text boxes, enter override values for the min/max downstream and min/max upstream rates. If overrides are used, all four values must be entered.
   c. In the Bonding Group bandwidth boxes, enter the group rates as follows:
      - Min DS Rate: Combined min downstream rates of all member ports.
      - Max DS Rate: Combined max downstream rates of all member ports, plus a cushion of 32 kbps.
      - Min US Rate: Combined min upstream rates of all member ports.
      - Max US Rate: Combined max upstream rates of all member ports, plus a cushion of 32 kbps.

   Note: These rates will override the aggregate rates set during the creation of Bonding Groups. Individual member port rates will be set by the selected xDSL Template or its override values (if present).
9. (Optional) In the VLAN-IF Tmplt list, select a VLAN-IF template.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Note: You can use VLAN-IF templates to define settings for subscriber-side VLAN interfaces. Calix recommends selecting a VLAN-IF template appropriate for your application. Otherwise, after adding subscriber connections, you must confirm that all subscriber-side VLAN interfaces have correct settings for your application.

10. (MP only) In the Data Service area, do the following:

- Edit the VP/VC (xDSL) or index (ONT) values, as required.
- In the Trf Prof list, select the desired traffic profile. (This overrides the value in the VLAN-IF Template, if used.)

Note: Select a predefined "MP" Traffic Profile when the Data Subscriber Template is used for the following:
• L2 unicast video + data (RG Support)
• L2 unicast video

Note: If a back traffic profile (**Back Trf Prof**) is not selected, the standard profile (**Trf Prof**) is used for back traffic.

- Select the desired protection path ('Unprot' for uplinks and subscribers in the same shelf). (This overrides the value in the VLAN-IF Template, if used.)

Note: For L3/Routed video support, confirm that the Path setting of the Data VC matches that of the Subscriber IP Channel Stream row in the Video Subscriber template. To access the Video Subscriber template, in the Work Area, click **Subscriber Templates** > **C7** > **Video**.

11. (EXA Only) In the Data Service area, do the following:

- In the TxEthBW Prof list, select a transmit Ethernet bandwidth traffic profile. (This overrides the value in the VLAN-IF Template, if used.)

Note: If a receive traffic profile (**RxEthBW Prof**) is not selected, the transmit profile (**TxEthBW Prof**) is used for receive traffic.

12. Click **Create** to save the new Subscriber Template.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Creating a Global Subscriber Template by Importing a C7 Network Template

In CMS you can create a global subscriber template by importing a subscriber template from a local C7 network.

You can import a global subscriber template from two locations:

- From a selected C7 network.
- From a selected ADSL port or an ONT (when importing subscriber services provisioned using TL1 or iMS)

If a C7 network subscriber template is set up to support both video and data service, when you import the template, the system creates two global subscriber templates: one for video and one for data.

Importing a C7 network subscriber template requires Full CMS Administration privileges.

To create a global subscriber template by importing a C7 network template

1. On the Navigation Tree, select a C7 network.
2. In the Work Area, click **Subscriber**.
3. In the template list, select the template(s) to import. To import multiple subscriber templates, use Shift+click to select a range of templates, or Ctrl+click to select one template at a time.
4. Click **Action > Import to Global Subscriber Template**, and then click **OK** to confirm the action.

   For a successful import, a message box displays indicating that the action completed; click **OK** to close the box. If a global subscriber template already exists that matches the parameters of a local profile, a Task Progress window opens indicating the template was not created.
5. To view the new global subscriber template(s), on the Navigation Tree, click **CMS > Subscriber Template**, and then click the type of template (**Video** or **Data**).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Modifying Subscriber Templates

If you change a Subscriber Template after it has been applied, CMS gives you the option of reconfiguring subscribers using that template.

The Template Change Status of a subscriber template indicates the status of subscribers' services using the template:

- **Not Modified** – The subscriber template has not been modified after creation.
- **Not Applied** – The subscriber template has been modified after creation, and the template was in use before modification. If the state is in "Not Applied", some subscriber services are not synchronized with the subscriber template. You can reconfigure the subscribers by going to **Action** > **Reconfigure Subscribers** to have the subscriber services reconfigured with the template. You can choose the networks to which the changes apply.
- **Fully Applied** – The subscriber template has been modified after creation. And either the template is not in use or the change has been applied to the subscriber services which uses the template.

To Edit a Subscriber Template

1. On the Navigation Tree, click **CMS**.
2. In the Work Area, click **Subscriber Templates** > **Video** or **Data**.
3. Select the template in the template list.
4. Click **Action** > **Edit**.
5. Make any necessary changes.
6. Click **Update**. CMS displays the Reconfigure Subscribers window.
7. Select the networks in which to reconfigure subscribers. All subscribers in the selected networks that use the template will be reconfigured. Any unselected networks will be unaffected.
8. Click **OK**.

If you do not select all networks, the Template Change Status of the template will be Not Applied. You can apply the changes to all networks at any time by selecting **Action** > **Reconfigure Subscribers**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Creating a Subscriber Uplink ID

Before adding video, data, or SIP ONT voice subscribers to an uplink, you must first identify the uplink in CMS by creating an uplink AID.

Note: The Uplinks list was introduced in CMS release 11.0. During a CMS server software upgrade to release 11.0, uplinks that have already been configured are automatically added to the Uplinks list. Uplinks configured after an upgrade to release 11.0 must be added to the Uplinks list using the following procedure.

To create an uplink ID to use for subscriber activation (CMS only)

1. On the Navigation tree, select the C7 network to configure.
2. In the Work area, click **Subscriber** > **Uplinks**.
3. On the toolbar, click **Create** to open the Uplink AID dialog box.
4. In the Uplink ID box, type an index ID number for the uplink.
5. In the Uplink Type list, select one of the following options to identify the uplink type:
   - **VLAN:** For Ethernet uplinks using a Virtual Bridge (Multiprotocol).
   - **Local VLAN:** For Ethernet uplinks using the Local Bridge (EXA).
6. If you selected 'Local VLAN' in Step 5, skip to Step 7. Otherwise, for VB-based VLANs, do the following:
   a. In the Shelf Address list, select the shelf containing the uplink card.
   b. In the Uplink Address list, select the system address of uplink. For example, for a VB-based VLAN, select the uplink Virtual Bridge.
7. In the S-VLAN list, select the service VLAN ID.
8. (Optional) In the Description box, type a brief description for this uplink VLAN.
9. Click **OK** to add the VLAN to the uplink list for CMS subscriber activation tools.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Multiple Port Service Activation

Activating Subscribers

For detailed information on activating subscribers, refer to the following Calix C7 documentation:

- *Calix C7 Broadband Data Service Guide*
- *Calix C7 Video Services Guide*
- *Calix C7 VoIP Service Guide*
- *Calix C7 GPON Applications Guide*

Viewing Subscriber Services

For services provisioned using the CMS, you can view a list of ports with services.

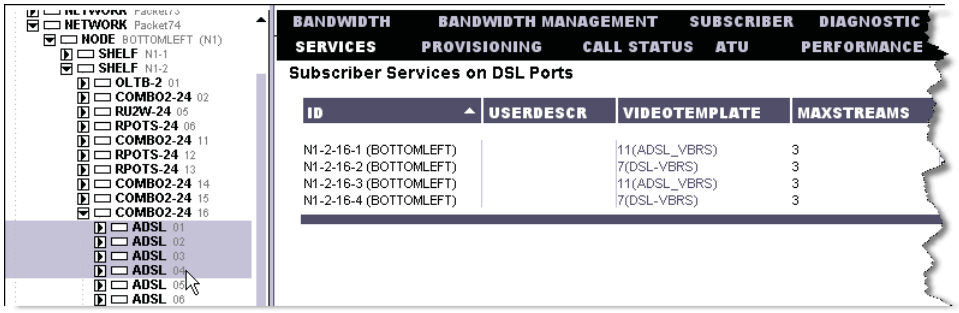
To view services on multiple ADSL, COMBO, or RPOTS ports and BPONs or GPONs

1. On the Navigation Tree, select the ports or PONs to view. Use Shift+click to select a range of ports, or Ctrl+click to select one port at a time.

   Note: If the Services tab is not already selected in the Work Area, select it.

   Tip: You can select view ports or PONs from multiple cards and multiple networks in a single list, as long as you select those of the same type. For example, use Ctrl+click to select ADSL ports on more than one ADSL or COMBO card.

   In the Work Area, the subscriber service information displays in List View.



2. Optionally, customize the list display or print a report. To do so, move the cursor over a table column heading, and then right-click to open a pop-up menu with these options.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Reconfiguring Subscribers (Using CMS)

The *Reconfigure Subscriber* tool allows you to make the following changes to multiple subscriber ports at once:

- Change the subscriber templates applied to subscriber access ports.
- Change the video or data uplink.
- Add video, data, or voice service to a subscriber with another service already provisioned.

After you specify the desired changes, the *Reconfigure Subscriber* tool performs the following provisioning tasks:

- Automatically applies a subscriber template to the selected access ports to update the service attributes.

  Note: For Bonding Group (xDSL group) subscriber templates, the xDSL template values are applied to each member port while the group min/max rates are applied to the entire group. The previous configuration of the group or member ports is overwritten.

- Automatically deletes existing subscriber cross-connects and creates new connections to a different uplink. Once the cross-connections are established, the subscriber port(s) can pass traffic.
- For Ethernet uplinks, automatically creates the VB ports and VLAN/VB port associations on the uplink (to support the subscriber VCs) using system defaults. The default settings should suffice for most applications, but can be modified afterward if required.

Before using the Reconfigure Subscriber tool

- This tool is available in CMS only, and requires Full CMS Administration privileges.
- To determine which subscriber ports require reconfiguration, using the *Subscriber Search* tool to search by subscriber ID or other criteria may be useful. For more information, see the *Calix CMS Guide*.
- Subscriber templates should be created in advance as needed
- Global profiles must be enabled for the network containing the subscriber port(s): On the Navigation Tree, select the Region or Network Group for the Network. In the Work Area, click **Network Details** and confirm that GLOBALPROFILEENABLED = Y for the network.
- Uplinks should be created and identified in CMS in advance as needed.
- For information about these requirements and configuring subscriber services, see the *Calix C7 Video Services Guide,* the *Calix C7 Broadband Data Services Guide,* or the *Calix C7 Voice Services Guide*.

ALERT! Reconfiguring subscriber services is service-affecting. Reconfiguring cross-connects temporarily disrupts service as the connections are deleted and rebuilt.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Using the Reconfigure Subscriber tool

To reconfigure subscribers (single or multiple subscribers)

1. On the Tools menu, click **Subscriber Provisioning** > **Reconfigure Subscriber**.
2. In the Reconfigure Subscriber Services dialog box, do the following:
   a. In the Select Network area, select the region and network containing the subscriber port(s) to configure.
   b. Below the Select Network area, select the port type, C7 shelf and slot containing the subscriber port(s), and the port(s) to reconfigure.

   Tip: In the Subscriber Ports list, use Shift+click to select a range of ports, or Ctrl+click to select one port at a time.
3. For the port(s) selected in Step 2, click the check boxes to the left of services to reconfigure, and select the desired parameters.

   Note: For detailed information on parameters for each type of service, see the *Calix C7 Video Services Guide,* the *Calix C7 Broadband Data Services Guide,* or the *Calix C7 Voice Services Guide.*
4. Click **Add** to place the subscriber services into the Subscriber Services To Be Reconfigured area.
5. Click **Create** to activate the subscribers.

   A Task Progress window opens to display the progress of the requested service activation. If a service cannot be activated, the reason for the error will be listed (for example, insufficient bandwidth).

Note: If existing video or data provisioning on a subscriber port is not visible to CMS or not compatible with the subscriber services to add, an error may occur with the following message: "Please clear video and data services (Click Action > Clear Video and Data Services) and try again." Follow these instructions, or for information on what this action does, refer to *Deleting Subscriber Connections* (on page 298).

Note: For bonding groups, this tool configures identical data rates on each member port, as the same xDSL template values are applied. After using this tool, you can configure disparate data rates across member ports as required by line conditions.

Using the Services tab

To reconfigure subscribers (one subscriber at a time)

1. On the navigation tree, select the subscriber to reconfigure.
2. In the work area, click the **Services** tab.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

3. Click the check boxes to the left of services to reconfigure, and select the desired parameters.
4. Click **Apply** and click **OK**.

Deleting Subscriber Services (Using CMS)

There are three ways to remove subscriber services from a port:

- Use the *Remove Subscriber Services* tool
- Use the Services tab of a subscriber port (select and apply a blank subscriber template)
- Use the *Clear Video and Data Services* action

Refer to the table below for the operational details of each technique.

Removal Technique	Operational Details		
	Number of Ports	Services Removed	Depth of Removal
Remove Subscriber Services tool	Multiple ports at once	Data, video, or both.	Best-effort removal of services visible to CMS
Services Tab	One port at a time	Data, video, or both.	Best-effort removal of services visible to CMS
Clear Video and Data Services action	One port at a time	Both data and video at once.	Comprehensive, forced removal of all data and video provisioning on a port. Typically used if adding RG video and data services fails.

ALERT! Service affecting procedure. Deleting cross-connects disrupts service on the subscriber port.

Using the Remove Subscriber Services tool

The *Remove Subscriber Services* tool allows you to delete subscriber connections from access ports and to remove existing service attributes that may be applied to the ports. The *Delete Subscriber* tool automatically deletes all data and video cross-connections according to the options you select.

To remove subscriber services (using the Remove Subscriber Services tool)

1. On the Tools menu, click **Subscriber Provisioning** > **Remove Subscriber Services** to open the Remove Subscriber Services dialog box.
2. In the Remove Subscriber Services dialog box, do the following:
   a. In the Select Network area, select the region and network containing the subscriber port(s) to modify.
   b. In the Port Type list, select the type of subscriber port(s) to modify.
   c. In the Shelf Address list, select the shelf where the subscriber port(s) are located.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

d. In the Subscriber Slot list, select the slot containing the subscriber port(s) to modify.

e. In the Subscriber Port list, click the port to modify. To select multiple ports, press the **Ctrl** key and click the ports to modify.

3. Select the **Remove Data Service 1** check box to delete the data 1 connections from the selected port(s).

4. Select the **Remove Data Service 2** check box to delete the data 2 connections from the selected port(s).

5. Select the **Remove Video Service** check box to delete video connections from the selected port(s).

6. Click **Add** to place the configuration(s) into the Subscriber Services To Be Deleted area.

7. (Option) Repeat Steps 2–5 to add other subscriber connections to the list as needed.

Note: To delete subscriber voice services, you can select **DS0 Port** in Step 2b, and then select the **Remove Voice Service** check box. For more information, refer to the *C7 Voice Services Guide*.

8. Click **Delete** to delete the subscriber connection(s) from the selected port(s).

Using the Services tab

To remove subscriber services

Modifying a single port through the Services screen requires Full CMS Administration privileges.

1. Using either the CMS search tool or the Navigation Tree, select an xDSL, POTS, or COMBO port, or an ONT.

   The provisioning screen for that port opens with the Services tab selected.

2. Click the arrow to the left of the port listing to view the fields.

3. For each service you are removing, do the following:

   - (For video service) Select **Remove Services** in the Video Template list.
   - (For a data service) Select **Remove Services** in the Data Template list.
   - (For a voice service) Select **Remove Services** in the Shelf list.

4. Click **Apply**, then click **OK** to save the new settings.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Using the Clear Video and Data Services action

Typically used if adding RG video and data services fails, this action initiates a comprehensive, forced removal of all data and video provisioning on a port. This action will make the following provisioning changes:

- Remove video and data services regardless of how the provisioning got on the port (TL1, iMS, CMS, etc.).
- Delete video and data service records from the CMS database
- Delete the associated video subscriber object (VID-SUB) from the C7
- Delete any associated cross-connects from the C7
- If the port was associated with a VLAN as an uplink or EPG source, delete the associated VB Port, VLAN-IF and CVID Reg objects from the C7

Note: This action does not remove DS0, DS1 or RFVID services. This action does not modify ADSL or xDSL port rate attributes or xDSL group rate attributes.

To remove subscriber services (using the Clear Video and Data Services action)

1. On the navigation tree, select the ADSL port, xDSL port, xDSL Group, or ONT for the subscriber.
2. In the work area, click the **Services** tab.
3. Click **Action > Clear Video and Data Services**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Single-Port and ONT Service Activation

The Services screen in CMS offers a single location for turning up video, data, and voice subscriber services for ADSL, POTS, and COMBO ports and PON ONTs. You can also determine if data and video services have been provisioned outside of CMS. You can apply or override C7 port and ONT port settings if needed.

For information about activating service on Active Ethernet ONTs, see Activating AE ONT Service.

The Services screen uses global subscriber profiles and templates to simplify activating services across copper and fiber lines:

- For information about defining and using profiles, see *Managing Global C7 Profiles* (on page 77).
- For information about setting up subscriber templates, see *Creating a Global Video Subscriber Template* (on page 276) and *Creating a Global Data Subscriber Template* (on page 289). For information about C7 provisioning, see the Calix C7 documentation.

The Services screen is context sensitive based on the type of port or ONT. Only services that apply to the port type or ONT display on screen. For ONTs that provide multiple Ethernet and voice ports, the Services screen contains multiple settings for each port. For Multiple Dwelling Unit (MDU) ONTs, the Services tab contains all MDU ports, so that any port can be assigned to any subscriber.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

C7 Status field messages

The following table describes the Status field messages on the C7 Services screen and the available options.

Status Field Messages	Description	What You Can Do
Provisioned with CMS	The service on the port has been provisioned *at one time* using the Services screen or the Add/Reconfigure Subscriber tools in CMS. This status means of one of two conditions: • The service settings displayed in CMS are the active settings. • The original service parameters have been modified outside of the Services screen or subscriber activation tools in CMS, such as using TL1 or C7 iMS.	If you are responding to a trouble ticket involving video or data service, perform these steps (service-affecting) to clear the current data and video service settings and activate service: • In the port or ONT Services screen, click **Action** > **Clear Video and Data Services**. • Use the CMS Services screen or Add Subscriber tool to activate service. If you are modifying voice service or responding to a trouble ticket involving voice service, use the CMS Services screen or Add Subscriber tool to reconfigure service.
Externally Provisioned	The service has been activated using outside of the Services screen and subscriber activation tools in CMS, such as using TL1 or C7 iMS.	If you are responding to a trouble ticket involving video or data service, perform these steps (service-affecting) to clear the current data and video service settings and activate service: • In the port or ONT Services screen, click **Action** > **Clear Video and Data Services**. • Use the CMS Services screen or Add Subscriber tool to activate service.
Not Provisioned with CMS	The service type has never been provisioned using the Services screen or the Add/Reconfigure Subscriber tools in CMS.	Use CMS to activate subscriber services.

Activating Subscribers

For detailed information on activating subscribers, refer to the following Calix C7 documentation:

- *Calix C7 Broadband Data Service Guide*
- *Calix C7 Video Services Guide*
- *Calix C7 VoIP Service Guide*
- *Calix C7 GPON Applications Guide*

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Viewing C7 Service Activation Details

When service provisioning is not successful, it is often helpful to view a log that lists the service provisioning details. The Service Details log includes the reasons for failure and any errors reported by the C7.

To view a log of service provisioning details for a C7 port or ONT

1. On the Navigation Tree or from CMS Desktop Search tool results, navigate to a port or ONT.
2. Click **Action** > **List Service Details**.

Note: Enabling or disabling an RF Video port is not recorded in the service details for the ONT.

Performing a Subscriber Search

Using the CMS Desktop, you can search across Calix ONTs or ports for two distinct types of user interfaces:

- Find a subscriber interface with provisioned services, based on the Subscriber ID and Description search criteria.
- Find a subscriber interface with or without provisioned services, based on the Network and Port ID information search criteria.

Based on company policies and procedures, the subscriber ID can be a telephone number or another subscriber identifier.

When performing a subscriber search, keep in mind the following guidelines.

- The Subscriber search locates a subscriber based on the following:
  - Data entered in the Subscriber and Description fields on the Services screen in CMS.
  - Data entered when provisioning on supported Calix devices, such as the Name and Telephone fields for ports on E3/E5-100 service units.
  - Node and port information for a subscriber interface can locate interfaces that have yet to be provisioned for service.
- The IP/MAC search retrieves data from Calix AE ONT, C7, E3/E5-100, E7 network elements related to subscriber equipment devices downstream from ONT Ethernet interfaces.
- Partial matches (equivalent to a "contains" match) are acceptable search strings.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Cross-platform subscriber port refresh frequency

Review the following system rules to understand how the CMS system refreshes subscriber port information for availability in subscriber searches:

- For Calix AE ONT, C7, E3/E5-100, and E7 network elements, subscriber information that is entered using the Services screen is stored directly on the CMS database and reflects the currently provisioned data.
- For Calix C7 subscriber changes provisioned using TL1 or C7 iMS, the CMS database is updated via C7 database change events at the time the changes are made.
- For Calix E3/E5-100 and E7 network elements, subscriber information that is entered on the local device is uploaded to the CMS database during scheduled inventory snapshot tasks. By default, the CMS system refreshes the subscriber port information once a week (on Tuesday at 1:00 AM). Depending on your company needs, it may be beneficial to increase the refresh frequency, for example, to occur daily. To change the frequency, contact Calix Technical Support.

Important: After a CMS software server upgrade, the E-Series scheduled task frequency resets to the default schedule. You must reset a customized refresh schedule after each CMS upgrade.

To perform a subscriber search

Note: The Subscriber Search pane displays in the Work Area when you launch CMS Desktop. Step 1 below is only required if you are currently viewing the administrative and configuration Work Area menus in CMS Desktop.

1. (Optional) To return to the results of a previous search, in the drop-down list to the right of the Last Search link, select Subscriber or IP/MAC, depending on the search type you are looking up.

   At the top of the screen, click the **Last Search** link. (Alternatively, in the status bar at the bottom of the CMS Desktop screen, click the magnifying glass icon, or on the Tools menu, click **Subscriber Search**.)

2. In the Subscriber box, enter the information on which to perform the search:

   - Enter all or part of a subscriber ID or AID. Include any characters, such as dashes, as used in the subscriber record or AID. For example:

     7072936500

   - Enter the network name, followed by a colon (:) to search for all ports on an E-series node or C7 network whose name contains the entered name. For example:

     c762:

   - Enter the network, followed by a colon (:), and then the node AID to search for only the ports whose network name contains the entered name and AID string. For example:

     c762:N1-1-1

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- Enter a MAC address or IP Host address.

3. Execute the search:
   - Click **Subscriber** to view the results of a search based on subscriber information.
   - Click **IP/MAC** to view the results of a search based on an IP host or MAC address.
4. Click the subscriber ID hyperlink to view the Services screen for the port or ONT.

Deleting Video Streams

In the Services screen for ADSL ports and ONTs, you can delete specific video streams provisioned at the port or ONT.

To delete video streams to an xDSL port or ONT

1. On the Navigation Tree, select the xDSL port or ONT.
2. On the toolbar, click **Action** > **Delete Video Stream**. In the Confirm Delete Video Stream dialog box, click **OK**.
3. In the Video Service List dialog box, click the check box to the left of each video stream to delete. Click **OK**.

   A Task Progress window displays the progress of the deletion.

Modifying Port Settings

Modify port settings through the Service screen by selecting different options in drop-down lists or entering new values in text boxes.

ALERT! Modifying subscriber services is service-affecting. Reconfiguring cross-connects temporarily disrupts service as the connection is deleted and rebuilt.

Modifying a single port through the Services screen requires Full CMS Administration privileges.

To modify settings for a single port

1. Using either the CMS search tool or the Navigation Tree, select an ADSL, POTS, or COMBO port, or ONT. The provisioning screen for that port opens with the Services tab selected.
2. Edit as needed.
3. Click **Apply**, then click **OK** to save the new settings.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring the xDSL Power Shutdown Priority

You can configure the xDSL power shutdown priority on a per-card basis:

- **1** (Category 1): Keeps all xDSL ports in service as long as sufficient power to the shelf is sustained.
- **3** (Category 3): Disables all xDSL ports on the card once the shelf delay timer expires, to conserve power for other high-priority services. Category 3 is the default priority for all xDSL cards.

Note: The Category 2 option is not currently supported.

To set the power shutdown priority for xDSL cards

1. On the Navigation Tree, click a C7 shelf containing an xDSL card.
2. Click the xDSL card to configure, and then in the Work Area, click the **Provisioning** tab.
3. In the Power Category list, click **1** or **3** to assign a power shutdown priority to the card.
4. On the toolbar, click **Apply** to update settings. In the Confirmation dialog box, click **OK**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Video Provisioning Features in CMS

Importing and Synchronizing a Video Channel Lineup

You can use CMS Desktop to create a global video channel lineup, and then synchronize the channel lineup across C7 networks that use the profile. Specifically, you can do the following:

- Create a video channel profile to match the starting encoding rates for the deployment.
- Upload a list of channels from a CSV file. Alternatively, you can define the channel profiles directly in CMS.
- Synchronize the video global channel lineup to enabled C7 networks, or apply it only to networks that you specify.

With the upload feature, you can import an entire video channel lineup or groups of channels to your existing channel lineup.

For details on using the global video channel lineup feature in CMS, refer to the *Calix C7 Video Services Guide*.

Modifying a Video Channel Profile and Applying to C7 Networks

In CMS you can modify a video channel profile (change the multicast IP address, ATM traffic profile, or channel description) and apply the modifications to networks you specify that use the profile.

Each provisioned video channel uses an ATM traffic profile that defines the bandwidth at which the channel is encoded. If the bandwidth does not match the requirements of the channel encoder, video quality can be degraded, prompting you to update the profile.

For details on modifying a video channel profile, refer to the *Calix C7 Video Services Guide*.

Deleting Video Streams

In the Services screen for ADSL ports and ONTs, you can delete specific video streams provisioned at the port or ONT.

For the procedure to delete video streams, see *Deleting Video Streams* (on page 305).

Troubleshooting Video Problems

In CMS you can isolate and eliminate network issues to troubleshoot video problems based on video packet flow analysis in the C7 network.

You can view dropped video packets based on a user-defined drop tolerance for:

- All channels on a subscriber C7 card (ADSL2-24, COMBO2-24, and COMBO2-24D cards only)

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- One or more channels on a C7 shelf
- One or more channels across a C7 network

When you view dropped packets, CMS retrieves the packet flow for the specified channels or channel and compares it to the same packet flow after a 10-second interval.

For the procedures to troubleshoot video problems, refer to the *Calix C7 Video Services*.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Chapter 7

Provisioning Ethernet-over-SONET Services

Use the Ethernet-over-SONET Provisioning tool in CMS to provision Ethernet-over-SONET transport and service drops on C7 networks across multiple shelves.

With the Ethernet-over-SONET Provisioning tool, you can:

- Turn up new Ethernet-over-SONET services.
- Modify existing Ethernet-over-SONET services. For example, add STSs to, or remove STSs from, an XLAN; add additional XLANs to a network; or add or remove service drops.
- Delete Ethernet-over-SONET services.

Note: To create an XLAN across multiple Ethernet cards on a single shelf, you must manually create the required components. For information, see *Creating Ethernet-over-SONET Components Manually* (on page 322).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Required Setup

This section includes rules and guidelines for setting up Ethernet-over-SONET network equipment, transport, and service drops.

For descriptions and illustrations of Ethernet network terms, see the *Calix C7 Engineering and Planning Guide*.

Once you have set up the physical equipment and provisioned the ports for service, you can use the Ethernet-over-SONET Provisioning tool to provision transport and service drops.

Starting Point

Before starting the Ethernet-over-SONET configuration process, verify that the following conditions are met:

- Equipment protection is configured for C7 optical transport cards, if required.
- Optical transport is established to all C7 nodes to comprise the XLAN.
- The C7 synchronous Ethernet (GE-4s or FE-12s) cards are installed at each C7 shelf providing Ethernet services.

  Note: GE-4s cards are equipped with 4 Gigabit Ethernet (GE) ports. FE-12s cards are equipped with 12 Fast Ethernet (FE) ports. A minimum of two Ethernet ports are typically required for service: one at each C7 terminal providing the XLAN ingress and egress points, such as an uplink and service drop or two service drops (for transparent LAN service).

- For GE-4s cards, SFPs are installed and wired with a fiber-optic jumper or Ethernet cable for each required port.
- For FE-12s cards, 10/100 Ethernet interface adapters are installed on the C7 backplane and wired with an Ethernet cable.

Ethernet-over-SONET Transport Rules

Follow these rules and guidelines when planning to configure Ethernet transport for your network:

- C7 network transport must be provisioned. Use of the Ethernet-over-SONET Provisioning tool assumes that the data links between C7 shelves in the network remain up and that the shelves do not reboot during the provisioning operation.
- Review the C7 shelf bandwidth requirements for each XLAN you create. See "XLAN Bandwidth Considerations" in the *Calix C7 Engineering and Planning Guide*.
- A C7 network supports up to 100 XLANs. The most common configuration is one XLAN per C7 network.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- Ethernet bandwidth is allocated in STS-1 increments from 1 to 21. Each XLAN supports a maximum of 21 STSs. You can use the Ethernet-over-SONET Provisioning tool to create the STSs or create the STSs before using the tool. In either case, only unused STS-1 facilities are available for use. If you create STS-1 facilities before using the Ethernet-over-SONET Provisioning tool, use Pass Through (PT) STS1 mapping.
- A GE-4s card can support two Ethernet Packet Rings or linear chains, or four point-to-point configurations. Note that each end of the point-to-point configuration can only have one port of the GE-4s assigned to it.
- An FE-12s card can support two virtually concatenated payloads, either two point-to-point configurations or one Ethernet Packet Ring or linear chain with east and west directions. Note that each end of the point-to-point configuration can only have one port of the FE-12s assigned to it.
- An Ethernet Packet Ring or linear chain network is capable of surviving a break caused by a card failure or removal. Note that in the case of a linear chain, traffic is switched past the card.

Prerequisites for Provisioning Service Drops

Before adding service drops using the Ethernet-over-SONET Provisioning tool:

- You must create Ethernet traffic profiles on the network to define the maximum bandwidth allowed onto the VLAN from the Ethernet ports. For information on creating global Ethernet traffic profiles and applying them to C7 networks, see the *Calix Management System (CMS) Guide*.
- You must configure ports on the C7 FE-12s and GE-4s cards for service, including enabling the tagging and policing parameters, if required. For information on how to perform this task, see *Configuring Ethernet Ports* (on page 311).
- The Ethernet-over-SONET Provisioning tool enables you to create VLANs. Optionally, you can create VLANs manually before using the tool.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring Ethernet Ports

Configure the Ethernet ports on GE-4s or FE-12s cards for service as described below. Note the following:

- When tagged, only traffic from assigned VLANs passes on that port.
- With policing, the Ethernet traffic profile assigned to the VLAN is enforced for that card.

Ethernet port parameters

You can provision the following parameters for GE-4s or FE-12s Ethernet ports:

Parameter	Valid Options (GE Ports)	Valid Options (FE Ports)	Default Value
Tagged	Y (Yes) N (No)	Y (Yes) N (No)	N
Maximum Transmission Unit	64–9022 (bytes)	64–9022 (bytes)	1522
Policing	Y (Yes) N (No)	Y (Yes) N (No)	N
Speed	Automatic 1000 (Mbps)	Automatic 10 (Mbps) 100 (Mbps)	Automatic
Duplex	Automatic Full	Automatic Half Full	Automatic
Laser Enabled	Y (Yes) N (No)	N/A	Y

Note: Some Ethernet devices do not support automatic detection of transmission rate or duplex mode. If connecting to such a device, specify the transmission rate (Speed) and duplex mode (Duplex) on the port instead of accepting the default **Automatic** option.

To configure a GE port for service

1. On the Navigation Tree, click the shelf containing the GE-4s card.
2. Double-click the card to view its ports, and then click the GE port to configure.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

3. In the **Provisioning** Work Area, place the port out of service:
   a. In the Primary Service State list, click **OOS**.
   b. On the toolbar, click **Apply** to place the port out of service. In the Confirmation dialog box, click **OK**.
4. Set the following GE port parameters:
   a. In the Tagged list, click **Y** or **N** according to your application requirements.
   b. In the Maximum Transmission Unit box, type an MTU value or accept the default.
   c. In the Policing list, click **Y** or **N** according to your application requirements.
   d. In the Speed list, click **Automatic**. If the far-end device does not support automatic detection, click **1000** (Mbps).
   e. In the Duplex list, click **Automatic**. If the far-end device does not support automatic detection, click **Full**.
   f. In the Laser Enabled list, click **Y** to enable the transceiver.
   g. In the Primary Service State list, click **IS**.
   h. On the toolbar, click **Apply** to update settings and place the port into service. In the Confirmation dialog box, click **OK**.

To configure an FE port for service

1. On the Navigation Tree, click the shelf containing the FE-12s card.
2. Double-click the card to view its ports, and then click the FE port to configure.
3. In the **Provisioning** Work Area, place the port out of service:
   a. In the Primary Service State list, click **OOS**.
   b. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK**.
4. Set the following FE port parameters:
   a. In the Tagged list, click **Y** or **N** according to your application requirements.
   b. In the Maximum Transmission Unit box, type an MTU value or accept the default.
   c. In the Policing list, click **Y** or **N** according to your application requirements.
   d. In the Speed list, click **Automatic**. If the far-end does not support automatic detection, click **10** or **100** (Mbps) to match the setting on the far-end.
   e. In the Duplex list, click **Automatic**. If the far-end does not support automatic detection, click **Full** or **Half** to match the setting on the far-end.
   f. In the Primary Service State list, click **IS**.
   g. On the toolbar, click **Apply** to update settings and place the port into service. In the Confirmation dialog box, click **OK**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

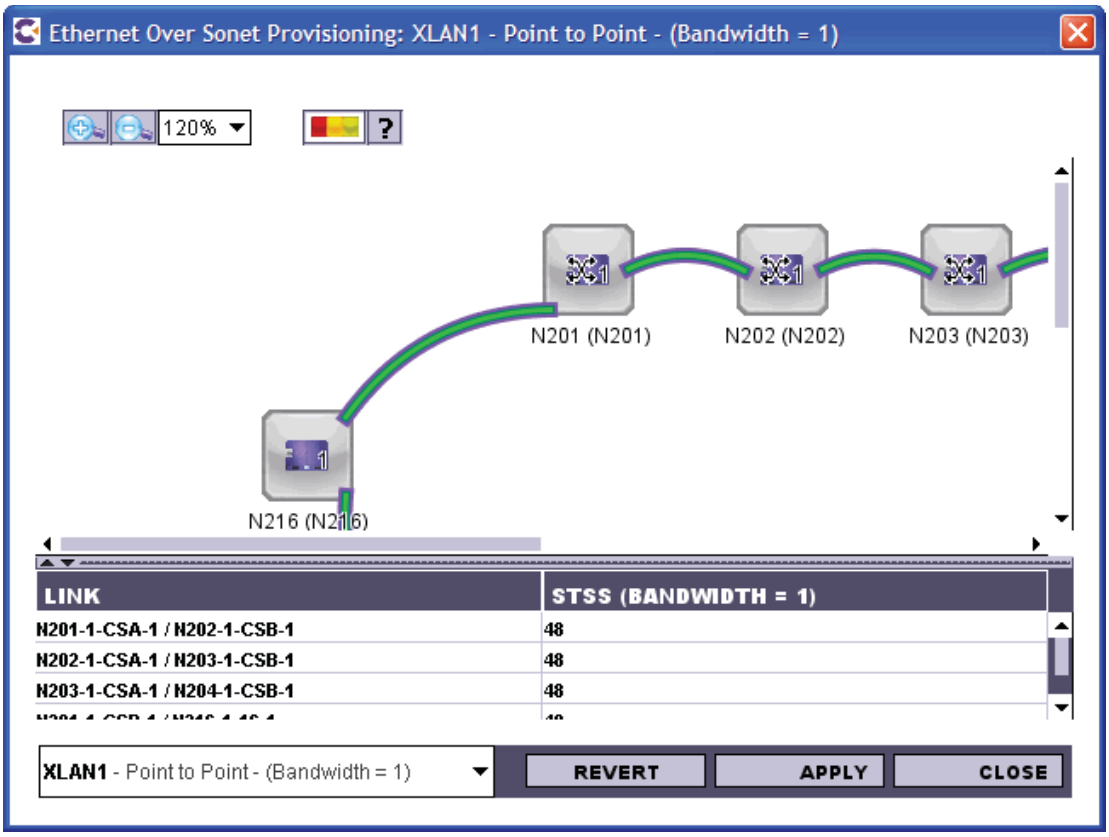
Ethernet-over-SONET Provisioning Tool

With a graphical representation of the network topology, you can automate the creation of Extended LANs (XLANs), Logical Switches (LSwitches) and Logical Switch Ports (LSwitchPorts), STS-1 facilities, Virtual Transport Interfaces (VTIs), and cross-connects. The tool also automates adding Ethernet ports to an LSwitchPort, creating Virtual LANs (VLANs), and adding Ethernet ports to a VLAN to provision service drops (VLAN ports).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Work Area

When you launch the Ethernet-over-SONET Provisioning tool, a separate CMS window opens to display the Ethernet-over-SONET Provisioning Work Area. The Work Area displays a graphical representation of the Extended LAN (XLAN) with all C7 network shelves and transport facilities passing through them.



The Work Area has two panes:

- The topology pane on the top where you select LSwitches and transport links and add Ethernet service drops.
- The STS pane on the bottom where you view and assign STS facilities to each link added to the XLAN.

Use the drop-down list at the bottom left of the Work Area to create an XLAN, or to view a different XLAN topology when more than one XLAN has been created.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Visual indicators in the XLAN topology pane

- **LSwitch icon:** The LSwitch has been defined and you can add Ethernet services on that shelf.

- **Network link—no edges:** The network link is not selected for inclusion in the XLAN. A thin line in the middle indicates multiple links exist between the nodes.

- **Network link—solid edges:** The network link is selected and included in the XLAN. For multiple links, all links are selected.

- **Network link—dashed edges:** For multiple links, at least one, but not all of the links are selected and included in the XLAN.

In the preceding multi-node C7 network illustration, XLAN1 has a bandwidth of 1 STS (indicated by "Bandwidth = 1" in the right column heading in the STSs pane).

Revert and Apply buttons

After you have selected the LSwitches and assigned the STS facilities to each XLAN link, clicking **Apply** saves the settings. To revert to the XLAN topology since the last changes were applied, click **Revert**.

Note: Revert cannot undo the settings once you click **Apply**.

Display options

In the upper-left corner of the XLAN topology pane, you can:

- Change the display scale by clicking the magnification icons or selecting a zoom setting in the list.
- View a legend of the icons used for C7 nodes and transport links by clicking the question mark icon.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Using the Tool

Use the Ethernet-over-SONET Provisioning tool to provision or modify Ethernet-over-SONET transport and services on a C7 network. Using the Provisioning tool requires Full CMS Administration privileges.

ALERT! Changing the LSwitch and STS-1 link assignments when Ethernet-over-SONET services are provisioned on the network is service affecting.

To provision or modify Ethernet-over-SONET transport

Note: Modifying an XLAN to remove a provisioned LSwitch or network link deletes the affected LSwitch entity and associated VTIs, LSwitchPorts, and cross-connects. This action also deletes any STS-1 facilities that were originally created using the Ethernet-over-SONET Provisioning tool.

1. On the Navigation Tree, click the C7 network.
2. Click **Tools** > **Ethernet-over-SONET Provisioning** > **Ethernet-over-SONET Provisioning**. The Ethernet-over-SONET Provisioning tool Work Area opens.
3. In the XLAN list at the bottom left of the Work Area, select an XLAN to view or modify, or create a new XLAN.

   To create a new XLAN, click **<Create New XLAN>** to open the Create New XLAN dialog box, and then do the following:

   a. In the XLAN box, type a number ID (from 1 to 100) for the XLAN.

   b. In the Name box, type a name (maximum of 31 characters) for the XLAN.

   c. In the Bandwidth list, select the number of STS-1 paths to assign to this XLAN.

   d. In the Topology list, select the topology used by the XLAN.

   e. Click **OK** to create the XLAN.

   f. In the bottom left of the Work Area, select the XLAN in the XLAN list.

   In the topology pane, the XLAN displays showing the nodes, shelves, and any provisioned LSwitches and links.

   Tip: Hover the mouse pointer over a node icon, LSwitch icon, or network link to view a Tooltip with details of the element.

4. In the topology pane, click the shelves inside the nodes to select two or more LSwitch shelves on which to drop Ethernet traffic. An LSwitch icon displays on each shelf you select. To remove an LSwitch from a shelf, click the LSwitch icon.
5. In the topology pane, set the network links to define the XLAN:

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- Click each network link to include. When multiple links exist between shelves, the links display in a popup menu. Click the check box next to a link to include it. Solid edges indicate that the link is included in the XLAN. Dashed edges indicate that the link is partially included.
- To remove a link from the XLAN, click the link, and, for multiple links between shelves, clear the check box(es) of the links to exclude.

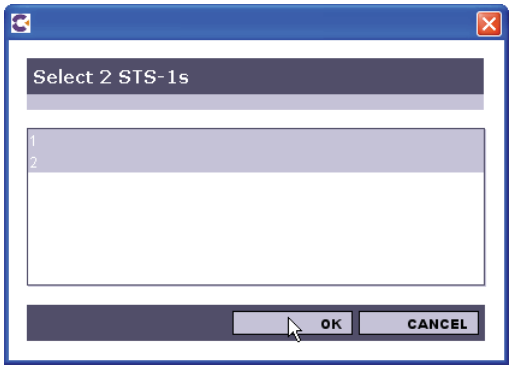
The selected endpoint AIDs display in the STS panel.

6. In the STSs pane, review the STS-1 assignments.

Note: Only unused STS-1 facilities display in the pane, regardless of whether they have been previously created. By default, the numerically highest available STS-1 facilities are assigned to a data link when you first select it.

To select or change the STS-1s that display:

- Click in the STS column to open the Select STS window for the link.



- From the list of available STSs, select one or more STS-1 to carry Ethernet traffic, and then click **OK**.
- Repeat the preceding steps as needed to assign STS facilities to all the links within the XLAN.

7. Create service drops, as follows:

a. Move the cursor over a shelf with an LSwitch icon.

b. Right-click, and then click **Provision VLAN Ports (Drops)**. The Provision VLAN Ports dialog box opens.

c. In the VLAN ID list, select an existing VLAN, or type a new VLAN number (from 1 to 4095) to associate it with the service drop.

Note: To add more than one VLAN port to an Ethernet port that already has a VLAN port associated with it, the Tagging parameter for the port must be set to Y (Yes).

d. In the Profile list, select an Ethernet Traffic Profile.

e. In the Available Ethernet Ports list, select the port(s) on which to create a service drop.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

f. Click **Create** to add the port to the Existing VLAN Ports list.

g. Click **OK**.

8. To delete service drops, do the following:

a. Move the cursor over a shelf with an LSwitch icon.

b. Right-click, and then click **Provision VLAN Ports (Drops)**. The Provision VLAN Ports dialog box opens.

c. In the Existing VLAN ports list, select the port(s) to delete.

d. Below the list, click **Delete**.

e. Click **OK**.

9. At the bottom of the XLAN Provisioning window, click **Apply**.

A task progress window opens to display the actions taken and any errors that occur.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Deleting Provisioning

Use the Ethernet-over-SONET Provisioning tool to delete provisioning. You can optionally delete the Extended LAN (XLAN) with the provisioning.

ALERT! Deleting Ethernet-over-SONET provisioning when services are provisioned on the network is service-affecting.

Using the Ethernet-over-SONET Provisioning tool requires Full CMS Administration privileges.

To delete Ethernet-over-SONET provisioning

Note: Deleting Ethernet-over-SONET provisioning removes all LSwitches, LSwitchPorts, VTIs, cross-connects between VTIs and STS facilities associated with the XLAN, as well as any STS-1 facilities that were created using the Ethernet-over-SONET Provisioning tool (STS-1 facilities created outside the tool are not deleted). Using the procedure below, you can optionally remove the XLAN.

1. On the Navigation Tree, click the C7 network containing the XLAN.
2. Click **Tools > Ethernet-over-SONET Provisioning**. The Ethernet-over-SONET Provisioning tool Work Area opens.
3. In the XLAN list at the bottom left of the Work Area, select the XLAN to display it.
4. For each shelf with an LSwitch, remove all existing service drops (VLAN ports), as follows:
   a. Move the cursor over a shelf with an LSwitch icon.
   b. Right-click, and then click **Provision VLAN Ports (Drops)**. The Provision VLAN Ports dialog box opens.
   c. In the Existing VLAN ports list, select all the port(s).
   d. Below the list, click **Delete**.
   e. Click **OK**.
5. In the topology pane, do the following:
   - Click each LSwitch icon inside a node to remove it (you must first complete Step 4 if the LSwitch contains service drops).
   - Click each network link with solid or dashed edges (links included in the XLAN topology), and then clear all check boxes to remove the link from the XLAN.
   - Repeat this step until all LSwitches icons have been removed and all network links are unselected.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

6. Click **Apply**. In the XLAN deletion Confirmation dialog box, click **Yes** to delete the XLAN, or **No** to remove provisioning but keep the XLAN.

   In the Service Affecting dialog box, click **Yes** to complete the deletion.

   A task progress window opens to display the progress of the deletion.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Creating Ethernet-over-SONET Components Manually

Use the procedures in this section to manually create an XLAN across multiple Ethernet cards on a single shelf and the required components.

Required tasks for provisioning transport

To configure Ethernet-over-SONET transport manually, you must complete the following tasks:

- Create an Extended LAN (XLAN) on the C7 network.
- Create a Logical Switch (LSwitch) on each C7 shelf that participates in the XLAN.
- Assign Virtual Transport Interface (VTI) ports to each LSwitch.
- Create STS paths for transport on the optical ports.
- Cross connect the VTI ports to the STS paths.

Required tasks for provisioning service drops

To configure Ethernet-over-SONET services manually, you must complete the following tasks:

- Configure the Ethernet ports for service.
- Assign Ethernet ports to an LSwitch to join the XLAN.
- Create service VLANs on the XLAN.
- Create Ethernet traffic profiles for the VLANs.
- Create VLAN ports by mapping Ethernet ports to VLANs.

Configuration guidelines for transport

Follow these guidelines when configuring Ethernet-over-SONET transport:

XLAN: An XLAN is a network-wide entity comprised of "virtually concatenated" STS-1 paths for Ethernet transport.

- You can specify the "size" (bandwidth) of the XLAN, from 1 to 21 STS-1s.
- Not all C7 shelves in a network must belong to the XLAN.

LSwitch: An LSwitch performs traffic switching between the optical transport and Ethernet service ports on a C7 shelf.

- Each shelf that participates in an XLAN must be equipped with an LSwitch.
- A C7 shelf may belong to multiple XLANs, provided you create an LSwitch for each XLAN.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

VTI ports: Virtual Transport Interface (VTI) ports provide cross connect endpoints for the LSwitches (to the transport facilities).

- Assign one or two VTI ports to the LSwitch, depending on the transport configuration.
- LSwitches in point-to-point configurations or at the end of linear chains require only one VTI port.
- LSwitches in packet rings or in the middle of linear chains require two VTI ports—one VTI port facing each adjacent shelf (east and west).

STS paths: The C7 automatically "virtually concatenates" multiple STS-1 paths together to provide the aggregate bandwidth.

- Create STS paths on optical transport ports in the XLAN to carry Ethernet traffic. You can create multiple STS paths (in STS-1 increments) to achieve the desired transport bandwidth on the link.
- Create the same number of STS paths on every transport port in the XLAN, matching the bandwidth allocated to the XLAN. For example, if the XLAN is 3 STSs in size, create 3 STS-1 paths on each transport port.
- The STS Mapping parameter must be set to Pass Through (PT).

VTI/STS cross connects:

- Cross-connect the LSwitch VTI ports to the STS path(s) on the transport ports.
- STS-VTI and VTI-STS Cross connects between C7 shelves cannot be configured as protected, as they use existing SONET protection. Always configure STS-VTI and VTI-STS cross connects as unprotected.
- For packet rings or linear chains, you must create two cross connects per LSwitch (west-side STS path to the west VTI port; east-side STS path to the east VTI port).
- For packet rings or linear chains, you must create the cross connects in a specific order—hop-by-hop in one logical direction around the ring. Failure to adhere to this pattern raises Far-End Mismatch alarms.
- On any C7 shelf in a ring or chain not equipped with an LSwitch, create pass-through cross connects between the west- and east-side transport STSs.

Create an Extended LAN (XLAN)

Create an extended LAN (XLAN) on the C7 network to reserve bandwidth on the optical transport facilities for Ethernet services traffic. Specify the topology type for the XLAN from among the following:

- **P2P (Point to Point):** A point-to-point connection between two C7 shelves.
- **Linear (Linear Chain):** A linear chain of three or more C7 shelves.
- **EPR (Ethernet Packet Ring):** Any number of C7 shelves arranged in a ring configuration.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

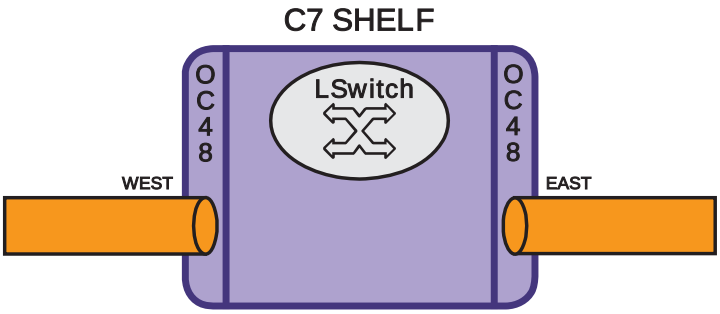
To create an XLAN

1. On the File menu, click:
   - (in iMS) **Create** > **Ethernet Over SONET** > **XLAN**
   - (in CMS) **Create** > **C7** > **Ethernet Over SONET** > **XLAN**
2. In the Create New XLAN dialog box:
   a. In the XLAN box, type an ID number for the XLAN (from 1 to 100).
   b. In the Name box, type a name for the XLAN (up to 31 characters).
   c. In the Bandwidth list, select the amount of bandwidth to allocate to this XLAN, in STS-1 (51.84 Mbps) increments.
   d. In the Topology list, select the network topology for the XLAN (**EPR**, **P2P**, or **Linear**).
3. Click **OK** to create the XLAN.

Create Logical Switches for Shelves in the XLAN

The LSwitch serves as the logical switching interface between the optical transport port(s) and the Ethernet service ports on the C7 shelf. Each C7 shelf that participates in the XLAN must be equipped with an LSwitch.

Create logical switches (LSwitches) on individual C7 shelves to associate those shelves with an XLAN.



To create LSwitches on C7 shelves to join the XLAN

1. On the File menu, click:
   - (in iMS) **Create** > **Ethernet Over SONET** > **Logical Switch**
   - (in CMS) **Create** > **C7** > **Ethernet Over SONET** > **Logical Switch**

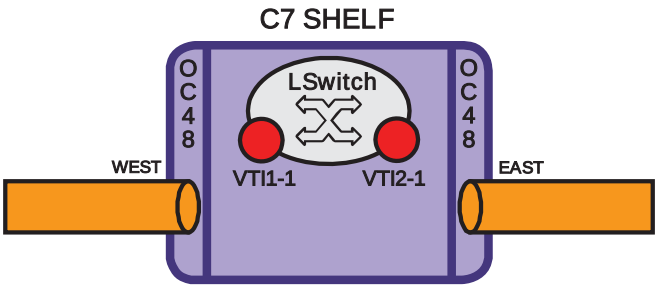
Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

2. In the Logical Switch dialog box, do the following:
   a. In the Extended LAN list, select the XLAN to join.
   b. In the C7 shelves list, press the **Ctrl** key and click the C7 shelves to add to the XLAN.
   c. Click **Add** to place the shelves in the Logical Switches To Be Added list.
3. Click **OK** to create LSwitches on the selected C7 shelves (to add the shelves to the XLAN).

Assign VTI Ports to Logical Switches

LSwitches use Virtual Transport Interface (VTI) ports to connect to the transport facilities. The VTI ports terminate the cross connects to the optical transport card.

Each LSwitch requires either one or two VTI ports, depending on the XLAN topology. An LSwitch in a point-to-point configuration or at the end of a linear chain topology requires only one VTI port. LSwitches in packet rings or in the middle of a linear chain topology require two VTI ports—one VTI port for each adjacent shelf (east and west).



Note: C7 networks typically employ packet rings for transport. Therefore, the following procedure assumes you are assigning two VTI ports to each LSwitch.

To assign VTI ports to an LSwitch

1. On the File menu, click:
   - (in iMS) **Create** > **Ethernet Over SONET** > **Logical Switch Port**
   - (in CMS) **Create** > **C7** > **Ethernet Over SONET** > **Logical Switch Port**
2. In the Logical Switch Port Provisioning dialog box:
   a. In the Shelf list, select a C7 shelf equipped with an LSwitch.
   b. In the Port Type list, click **VTI**.
   c. In the ports list, press the **Ctrl** key and click two VTI ports to add to the LSwitch.
   d. In the LSwitch list, select the LSwitch to which the VTI ports will be assigned.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

e. In the Port ID box, click **NTWK1** to associate the first VTI port with one logical "side" of the LSwitch (for example, the "west" side port of the LSwitch).

Note: When two VTI ports are selected, the system automatically associates the second VTI port to the other logical "side" of the LSwitch, **NTWK2** (for example, the "east" side port).

f. Click **Add** to place the selected VTI ports into the Ports To Be Added area.

3. Repeat Step 2 to assign VTI ports to additional LSwitches (C7 shelves) on the XLAN.
4. Click **OK** to create the VTI assignments.

Create STS Paths for Ethernet Transport

Create STS paths on the optical transport ports to carry Ethernet traffic. Management traffic typically does not require more than one STS-1 of bandwidth. However, if your XLAN shall carry subscriber traffic as well as management traffic, you can create multiple STS-1 paths on each optical port to achieve the desired aggregate transport bandwidth.

Create the same number of STS paths on all transport ports in the XLAN. The number of STS-1 paths you create should match the bandwidth allocated to the XLAN to avoid a bottleneck at the optical port. The system automatically concatenates the STS-1s together to provide the aggregate bandwidth.

In packet ring and linear chain configurations, be sure to create an equal number of STS paths on both the east and west optical transport ports per shelf. The STS Mapping parameter must be set to Pass Through (PT).

To create STS paths for Ethernet-over-SONET transport

1. On the File menu, click:
   - (in iMS) **Create** > **STS Path**
   - (in CMS) **Create** > **C7** > **STS Path**
2. In the Create SONET Transport Signal Facilities dialog box:
   a. In the Shelf list, select the C7 shelf containing the optical transport card(s).
   b. In the Port list, select the optical port on which to create the STS path.
   c. In the Rate list, click **STS1**.
   d. In the STS list, select the STS path ID to create.

Note: For multiple STS-1s, use Ctrl+click to select one STS at a time, or Shift+click to select a range of STSs equal the bandwidth allocated to the XLAN. For example, if the XLAN is equal to 3 STSs in size, select 3 STS-1s to create on the transport port.

e. Click **Add** to place the selected STS(s) into the STS To Be Created area.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

3. Repeat Step 2 to add STS paths on additional optical transport ports.
4. Click **Next**.
5. In the STS(n)s dialog box, do the following:
   a. In the User Description box, type a short description for the STS paths. For example, type **EoS Transport**.
   b. In the STS Mapping list, click **PT** (Pass Through).
   c. Set the remaining parameter values as required for your site or accept the defaults.
6. Click **OK** to create the specified STS paths.

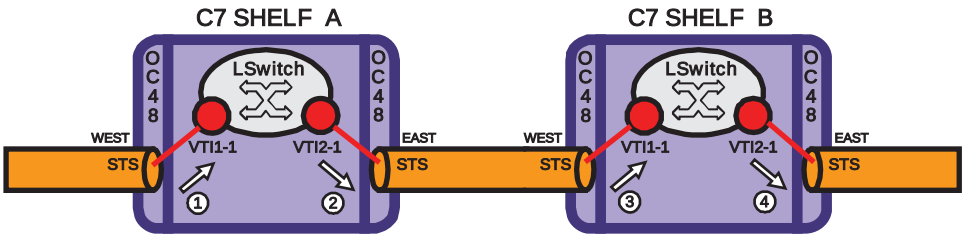
Cross Connecting VTI Ports to STS Paths

Cross connect STS paths on the C7 optical transport port(s) to the LSwitch VTI port(s) to enable Ethernet-over-SONET transport. For C7 shelves in packet ring configurations, you must create two cross connects (or two sets of cross connects, when mapping to multiple STS-1s at each optical port) per C7 shelf: from the VTI ports on each side of the LSwitch to the STS paths on the west-side and east-side optical transport ports.

For packet ring configurations (and linear chains), you must create the cross connects in a specific order to avoid Far-End Mismatch (FEMM) alarms. Create the cross connects hop-by-hop in the same logical direction around the ring. Further, you must specify alternating source and destination endpoint types (STS and VTI ports) on each successive cross connect (or set of cross connects) that you create. For any C7 shelves in the ring that **are not** equipped with LSwitches, create pass-through cross connects between the STS paths on the west- and east-side optical transport ports.

As a rule, follow a logical arrow hop-by-hop around the ring when creating the cross connects. For example, specify an STS as the source endpoint and a VTI port as the destination endpoint for the first cross connect. Reverse the endpoint types for the next cross connect on the same C7 shelf. Repeat this pattern on each shelf in the ring or chain that belongs to the same XLAN. Failure to adhere to this pattern will cause an infinite loop and raise Far-End Mismatch alarms.

All LSwitches in an XLAN must be cross-connected to the same number of STS paths.



In the illustrated example, the cross connects are created in the following order:

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

LSwitch	Cross connect	Source	Destination
C7 Shelf A	1	West STS	VTI1-1
	2	VTI2-1	East STS
C7 Shelf B	3	West STS	VTI1-1
	4	VTI2-1	East STS

The cross-connect endpoints have the following Access Identifier (AID) formats:

AID Format	Description
N{1-255}-{1-6}-VTI{1-80}-{1-21}	STS on a VTI. Format = (Node Id)-(Shelf #)-(VTI #)-(STS #)
N{1-255}-{1-6}-{1-20}-{1-12}	STS1 path in a DS3-12 card.
N{1-255}-{1-6}-{1-20}-{1-12}-{1-48}	STS path in an OCn card. STS1 can be any number between 1 and 48. However, STS3c/12c/48c can only provisioned as particular STS numbers: • STS3c can be 1, 4, 7, ..., 46 between 1 and 48. • STS12c can be 1, 13, 25 and 37. • STS48c can only be 1.
N{1-255}-{1-6}-{CSA,CSB}-{1}	Identifier of a port on a RAP card.
N{1-255}-{1-6}-{CSA,CSB}-{1}-{1-48}	STS path in a RAP-OC card.

The following log excerpt shows an example of STS and VTI cross connects:

```
N31-1-CSA-1-13,N31-1-VTI1-1:2WAY
N31-1-CSA-1-14,N31-1-VTI1-2:2WAY
N31-1-CSA-1-28,N31-1-VTI3-1:2WAY
N31-1-CSA-1-29,N31-1-VTI3-2:2WAY
N31-1-CSA-1-30,N31-1-VTI3-3:2WAY
N31-1-CSA-1-31,N31-1-VTI3-4:2WAY
N31-1-CSA-1-32,N31-1-VTI3-5:2WAY
N31-1-CSA-1-33,N31-1-VTI3-6:2WAY
N31-1-CSA-1-34,N31-1-VTI3-7:2WAY
N31-1-CSA-1-35,N31-1-VTI3-8:2WAY
N31-1-CSA-1-36,N31-1-VTI3-9:2WAY
N31-1-CSA-1-37,N31-1-VTI3-10:2WAY
N31-1-CSA-1-38,N31-1-VTI3-11:2WAY
N31-1-CSA-1-39,N31-1-VTI3-12:2WAY
```

The procedures below reflect the provisioning practice for VTI/STS cross connects in a C7 ring or chain per the pattern illustrated in the example above (west to east, or clockwise around a ring).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

To cross connect the "west" STS to the first VTI port

1. On the File menu, click **Create** > **Cross-Connect** > **STS1** to open the Select Cross-Connect Endpoints dialog box.
2. In the Source area, define the source endpoint for the cross connect as follows:
   a. In the Shelf list, select the C7 shelf hosting the LSwitch.
   b. In the Type list, click **STS1**.
   c. In the list of STS paths, select the STS-1(s) on the west-side optical transport port to cross connect.
   d. Click **SRC** to add the Source endpoint to the Cross-Connects To Be Created area.
3. In the Destination/Drop area, define the destination endpoint for the cross connect as follows:
   a. In the Shelf list, select the same C7 shelf from Step 2.
   b. In the Type list, click **VTI**.

   Note: The available parameters change based on the endpoint type selected.

   c. In the VTI list, select the first VTI port to cross connect. For example, select VTI1 (**Nn-n-VTI1**).
   d. In the VTI STS Port box, type a logical port number or range of numbers (equal to the number of STS-1s selected, 1 to 21) to use on the VTI port to terminate the cross connect. For example, type **1-2**.
   e. Click **DEST** to add the Destination endpoint to the Cross-Connects To Be Created area.
4. In the Required Parameters area, do the following:
   a. In the Cross-Connect Way list, click **2WAY**.
   b. In the Cross-Connect Path list, click **UNPROT**.
5. Click **OK** to create the cross connects.

To cross connect the second VTI port to the "east" STS

1. On the File menu, click **Create** > **Cross-Connect** > **STS1** to open the Select Cross-Connect Endpoints dialog box.
2. In the Source area, define the source endpoint for the cross connect as follows:
   a. In the Shelf list, select the C7 shelf hosting the LSwitch.
   b. In the Type list, click **VTI.**

   Note: The available parameters change based on the endpoint type selected.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

c. In the VTI list, select the second VTI port to cross connect. For example, select VTI2 (**Nn-n-VTI2**).

d. In the VTI STS Port box, type the logical port number to use on the VTI port to terminate the cross connect.

e. In the VTI STS Port box, type a logical port number or range of numbers (equal to the number of STS-1s) to use on the VTI port to terminate the cross connect. For example, type **1-2**.

f. Click **SRC** to add the Source endpoint to the Cross connects To Be Created area.

3. In the Destination/Drop area, define the destination endpoint for the cross connect as follows:

   a. In the Shelf list, select the same C7 shelf from Step 2.

   b. In the Type list, click **STS1**.

   c. In the list of STS paths, select the STS-1(s) on the east-side optical transport port to cross connect.

   d. Click **DEST** to add the Destination endpoint to the Cross-Connects To Be Created area.

4. In the Required Parameters area, do the following:

   a. In the Cross-Connect Way list, click **2WAY**.

   b. In the Cross-Connect Path list, click **UNPROT**.

5. Click **OK** to create the cross connects.

Repeat these two procedures on each successive LSwitch (C7 shelf) in the XLAN. Continue creating cross connects hop-by-hop in the same logical direction (west to east, for example), with alternating source and destination endpoint types (STS and VTI ports) on each successive cross connect. If you do not follow the same pattern and order, the system will raise Far-End Mismatch alarms.

On any pass-through C7 shelf in the ring/chain (that is, any shelf **not** equipped with an LSwitch), create pass-through cross connects between the STS paths on the west- and east-side optical transport ports.

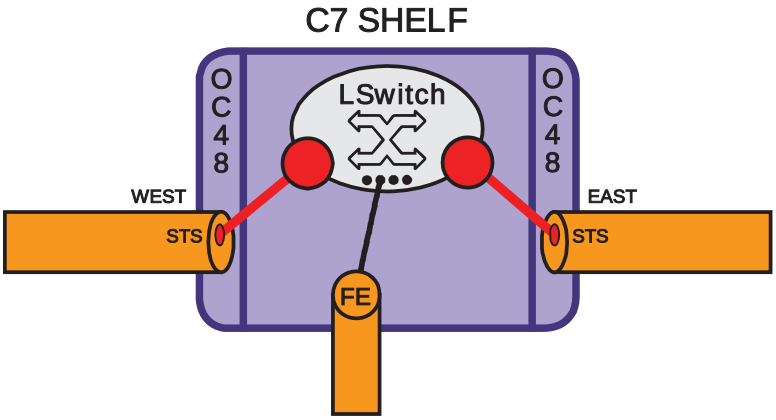
Configuring Ethernet Ports

For descriptions of parameters and a procedure for configuring Ethernet port, see *Configuring Ethernet Ports* (on page 311).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Assigning Ethernet Ports to an LSwitch

A Logical Switch (LSwitch) performs traffic switching between Ethernet service ports and the optical transport ports on a C7 shelf. To add Ethernet service ports to an XLAN, you must assign the Ethernet ports to an LSwitch. Once the Ethernet ports are assigned to an LSwitch, those ports can pass traffic on the XLAN.



To assign Ethernet ports to the LSwitch

1. On the File menu, click:
   - (in iMS) **Create** > **Ethernet Over SONET** > **Logical Switch Port**
   - (in CMS) **Create** > **C7** > **Ethernet Over SONET** > **Logical Switch Port**
2. In the Logical Switch Port Provisioning dialog box, Available Ports area:
   a. In the Shelf list, select the C7 shelf containing the Ethernet port to add to an LSwitch.
   b. In the Port Type list, click **Fast Ethernet SONET Port** or **Gigabit Ethernet SONET Port.**
   c. In the port list, select the FE or GE port to assign to an LSwitch.
   d. In the LSwitch list, select the LSwitch to which the Ethernet port will be assigned.
   e. In the Port ID box, type the first logical port ID number on the LSwitch to which the Ethernet port will be mapped.
   f. Click **ADD** to place the selected FE or GE port into the Ports To Be Added area.
3. Repeat Step 2 to assign additional Ethernet ports to LSwitches on other shelves in the XLAN.
4. Click **OK** to add the Ethernet port(s) to the LSwitch(es).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Creating a Virtual LAN (VLAN)

Create Virtual LANs (VLANs) to separate traffic into different bridging domains on the XLAN. If the XLAN carries traffic from multiple networks, create VLANs to segregate the traffic appropriately.

To create a VLAN

1. On the File menu, click:
   - (in iMS) **Create** > **Ethernet Over SONET** > **VLAN**
   - (in CMS) **Create** > **C7** > **Ethernet Over SONET** > **VLAN**
2. In the Create New VLAN dialog box:
   a. In the XLAN list, select the XLAN to which the VLAN belongs.
   b. In the VLAN ID box, type an ID number for the VLAN (from 2 to 4094).
3. Click **OK** to create the VLAN.

Creating an Ethernet Traffic Profile

Ethernet traffic profiles define the maximum bandwidth rate allowed onto a VLAN. You can create up to 100 Ethernet traffic profiles for various service offerings. Apply Ethernet traffic profiles when you create VLAN ports (i.e., map Ethernet ports to a VLAN).

To create an Ethernet traffic profile

1. On the File menu, click:
   - (in iMS) **Create** > **Ethernet Over SONET** > **Ethernet Traffic Profile**
   - (in CMS) **Create** > **C7** > **Ethernet Over SONET** > **Ethernet Traffic Profile**
2. In the new Ethernet Traffic Profile dialog box:
   a. In the Identifier box, type an ID number for the profile (from 1 to 100).
   b. In the Bandwidth box, type the maximum transmission rate (in Mbps).
3. Click **OK** to create the profile.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Creating VLAN Ports

Enable switching on the VLANs by creating VLAN ports (mapping Ethernet ports to VLANs), effectively creating switch ports for the VLAN. A VLAN port is a logical interface into a VLAN.

To create VLAN ports

1. On the File menu, click:
   - (in iMS) **Create** > **Ethernet Over SONET** > **VLAN Port**
   - (in CMS) **Create** > **C7** > **Ethernet Over SONET** > **VLAN Port**
2. In the VLAN Port Provisioning dialog box, Available Ports area:
   a. In the Shelf list, select the C7 shelf containing the Ethernet port to map.
   b. In the Port Type list, click **Ethernet Port**.
   c. In the port list, select the Ethernet port to map to the VLAN.
   d. In the XLAN list, select the XLAN hosting the target VLAN.
   e. In the VLAN ID box, type the VLAN ID number to which the Ethernet port will map.
   f. In the Profile list, select an Ethernet traffic profile to assign to the VLAN.
   g. Click **ADD** to place the VLAN port into the Ports To Be Added area.
3. Repeat Step 2 to create additional VLAN ports (map additional Ethernet ports to the VLAN).
4. Click **OK** to create the VLAN port(s).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Chapter 8

Provisioning Ethernet and IP Services

The C7 operates as both an ATM and Ethernet access switch. Enhanced packet switching capabilities enable the C7 to operate as an extensible IP DSLAM.

The C7 provides the following Layer 2 Ethernet services to support IEEE 802.1D ("customer bridging") and 802.1ad ("provider bridging") standards:

- VLAN per service
- VLAN per port
- Transparent LAN service (TLS)
- S-VLAN switching

The C7 also supports Layer 3 Ethernet routing.

For detailed information regarding Ethernet and IP services, refer to the following Calix C7 documentation:

- *Calix C7 Engineering and Planning Guide*
- *Calix C7 Ethernet and IP Services Guide*
- *Calix C7 Broadband Data Service Guide*
- *Calix C7 Video Services Guide*
- *Calix C7 VoIP Service Guide*

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Ethernet Uplink and Downlink Provisioning Tools

Data Uplinks and Downlinks

CMS and C7 iMS provide tools for creating Ethernet uplinks and downlinks to subtended devices for the following service applications:

- RBE/DHCP model (Routed, Layer 3)
- PPPoE relay model (Routed, Layer 3)

Application-specific Ethernet Uplink and Downlink provisioning tools automatically create the necessary Ethernet service elements for each application to simplify uplink and downlink provisioning. You simply specify the virtual bridge and VLAN on that virtual bridge and CMS or C7 iMS configures the interface with the appropriate parameters necessary.

For information about using the tools, see the *Calix C7 Broadband Data Services Guide*.

DSLAM Aggregation

The ATM-to-Ethernet Aggregation tool provides a simple way to aggregate downstream ATM DSLAMs (on OCx, DSx and IMA interfaces) to an Ethernet uplink.

Using the VLAN per port model, the ATM to Ethernet Aggregation tool maps downstream ATM VP/VC values to single-tagged or double-tagged (S-Tag/C-Tag) Ethernet VLANs. When used for ATM DSLAMS, this tool simplifies the bridging of contiguous ranges of VC values within the context of a defined VP (representing an ATM DSLAM). It supports DSLAM-per-VP segmentation (one DSLAM per VLAN) as well as multiple DSLAMs (with identical VP/VC values) on the same VLAN by providing VC-to-CVID (C-Tag) offsets.

For information about using the tool, see the *Calix C7 Broadband Data Services Guide*.

Video Uplinks and Downlinks

CMS and C7 iMS provide tools for creating the following:

- Ethernet uplinks for video service
- Ethernet downlinks to subtended Calix service units

For information about using the tools, see the *Calix C7 Video Services Guide*.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

VoIP Uplinks and Subtended Services

CMS and C7 iMS provide tools for creating Ethernet uplinks for the following applications:

- H.248 service
- ONT SIP service

CMS and C7 iMS also provide tools for configuring these subtended VoIP services:

- TDM voice gateway for subtended VoIP lines
- Ethernet downlink for subtended services (connecting directly to the subtended service unit or indirectly through an aggregation switch)

For information about using these tools, see the *Calix C7 VoIP Services Guide*.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Chapter 9

Provisioning OCn Optical Services

This section describes the C7 OCn optical cards and ports. Instructions are provided for configuring optical ports, optical services, and protection for service, line, and facility level protection switching. Creating STS paths and STS cross-connections are also explained.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Overview of OCn Optical Port Parameters

System defaults for optical port parameters

Parameter	Default Value
Primary Service State (PST)	IS – In Service
Transmit S1 (TxS1)	Yes
Receive S1 (RxS1)	Yes
Laser Enable (LSREN)	Yes
External Interface (EXT)	No
Far End Performance Monitoring (FEPM)	No
Alarm Profile (ALMPROF)	AISNR – Alarm Indication Signal Not Reported
Signal Degraded Bit Error Rate (SDBER)	5
Signal Failed Bit Error Rate (SFBER)	3
Grade of Service (GOS)	DEFLT – Default
Protection domain (PDOM)	0

The following parameters are associated with optical ports. The abbreviated name shown in parentheses represents the parameter ID in the Provisioning table view when multiple ports are selected.

OC Port Identifier (ID)

Specifies the location (node, shelf, slot) of the OC port being configured. The address reads from left to right as follows:

```
NodeID-ShelfID-SlotID-OCPortID
```

NodeID is a number between 1 and 255. This number specifies the address of the C7 node in the network.

ShelfID is a number between 1 and 5. This number specifies the address of the C7 shelf on the node.

SlotID is a number between 1 and 20. This number specifies the slot on the C7 shelf where the OC card resides.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

OCPortID is a number between 1 and 4 for OC3-4 and OC12-4 cards. This number can only be 1 for OC48-1 and RAP-OC cards. This number specifies the particular port you are currently configuring.

Description (DESC)

Description is a user-defined character string of up to 11 characters. This parameter helps you track the link, port, profile, or cross-connect.

Primary Service State (PST)

PST specifies the default state of the equipment once it is installed. The values are IS (in-service) or OOS (out-of-service). The default value is IS.

You can also use this parameter if you are pre-provisioning a system. If pre-provisioning, the IS default value means the equipment is in-service once it is installed.

Transmit S1 (TXS1)

This parameter determines whether to process the S1 byte on the outgoing signal.

Specify N (No) to ignore the outgoing S1 synchronization status nibble and Y (Yes) to act upon it. The default value is N.

Receive S1 (RXS1)

This parameter determines whether to process the S1 byte on the incoming signal.

Specify N (No) to ignore the incoming S1 sync status nibble and Y (Yes) to act upon it. The default value is N.

Laser Enable (LSREN)

This parameter enables signal transmission over this facility. The default value is Y (Yes). Enter N (No) to receive signals only.

External Interface (EXT)

This parameter determines if the facility connects to an external interface or another node in the same network.

The default value is N (No)—the facility connects to another C7 node.

Set the value to Y (Yes) if the port connects to an external interface.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Far End Performance Monitoring (FEPM)

This parameter allows you to enable performance monitoring on the far-end node. It monitors both regular performance monitoring data and grade-of-service threshold violations.

The default value is N (No), meaning performance monitoring is disabled.

Set the value to Y (Yes) to enable performance monitoring and to count grade-of-service threshold violations.

Alarm Profile (ALMPROF)

This parameter identifies if the AIS or LOS is an alarmed or non-alarmed event. Parameter options are:

- **AISCR:** Specifies that the AIS alarm is critical and generates a critical alarm.
- **LOSNR:** Specifies that the LOS alarm is not reported and does not generate an autonomous report.
- **AISNR:** Specifies that the AIS alarm is not reported and does not generate an autonomous report.

The default value is AISNR.

Signal Degrade Bit Error Rate (SDBER)

This parameter is used to set the threshold value above which the bit error rate of the facility constitutes a degraded signal. When the bit error rate exceeds the threshold specified in this parameter, the system raises a signal degraded bit error rate (SDBER) alarm. SDBER parameter values are:

- 6 (value of 10 to the negative 6)
- 7 (value of 10 to the negative 7)
- 8 (value of 10 to the negative 8)
- 9 (value of 10 to the negative 9)

The default value is 6.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Signal Failed Bit Error Rate (SFBER)

This parameter is used to set the threshold value above which the bit error rate of the facility constitutes a failed signal. When the bit error rate exceeds the threshold specified in this parameter, the system raises a signal failed bit error rate (SFBER) alarm. SFBER parameter values are:

- 3 (value of 3 to the negative 10)
- 4 (value of 4 to the negative 10)
- 5 (value of 5 to the negative 10)

The default value is 3.

Protection Domain (PDOM)

This parameter associates a transport facility into a protection domain for use in an end-to-end connection configuration. The protection domain must be a unique non-zero integer.

For line protected configurations (LAPS), each fiber pair in the network has a unique protection domain.

For path protected configurations, **ALL** the fiber pairs that create the path-protected network have a unique protection domain.

Enter 0 to indicate that the facility is not to be used for end-to-end connections or for drop points (where traffic is dropped from the network). The default value is 0.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring OCn Optical Ports

Configure OCn Optical Port Parameters for Transport

Before you configure an optical port as a transport link, see the complete list of *OCn Optical Port Parameters* (on page 340).

Information to collect before configuring topology and protection

Before configuring your network topology and protection scheme, you should collect the following information:

- Optical port IDs
- Protection Domain number to use
- Protection scheme to use
- Number and size of STS paths

To configure optical ports for transport

1. On the Navigation Tree, click the Network level.
2. On the Selection Filter, click **Port** > **OC Port** > **OC Port** to view all optical ports in the Work Area.

   Tip: To further narrow the displayed facilities, set the filter to match the OC rate you are using, such as **OC48 Port**.

3. In the Work Area, use Ctrl+click to select all the optical ports for the transport links in the network.
4. Edit the transport parameters:
   a. In the EXT (External) interface list, verify the value **N** (No) is set.
   b. For the PDOM (Protection Domain) parameter, type a number (0 through 10000) for each port, and then press Enter.

   Note: Each port on the ring must have the same PDOM number and the number must not be used by any other transport topology in the network. Enter 0 to indicate that the facility is not to be used for end-to-end connections or for drop points (where traffic is dropped from the network).

   c. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save the configuration.
5. In the Work Area, click **Protection**.
6. On the toolbar, click **Create** to open the Create OCn Port Protection dialog box.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

7. In the Choose Working and Protect Ports area of dialog box:
   a. In the Shelf list, select a shelf.
   b. In the Line Rate box, select the rate for your network.
   c. In the Working AID box, select an OC port to serve as the working path in the network.

   Note: Optical ports cannot be configured to protect ports located on the same card. The system automatically designates a port on an adjacent card as the protect path. The designated port is displayed in the Protect AID box.

   d. Click **Add** to place the ports in the Protection Pairs To Be Created area.
8. Repeat Step 7 for each additional C7 shelf to use for transport in the ring.
9. In the Protection Options area, in the Protection Scheme box, select the protection scheme for the network.

   Note: Calix strongly recommends a LAPS 1+1 bi-directional protection scheme for optical interfaces that require protection.

10. Click **OK** to save your configuration.

Configure OCn Optical Port Parameters for Services

Complete this procedure to define the services parameters for an optical port.

See also *OCn Optical Port Parameters* (on page 340) for additional information.

To define optical port parameters

1. On the Navigation Tree, double-click the optical card to expand the tree. Click the port to provision.
2. In the **Provisioning** Work Area, and verify that the ID entry matches the address for the port you wish to configure (for example, N1-1-20-1 = Node 1, Shelf 1, Card 20, Port 1).
3. Place the optical port out of service:
   a. In the Primary Service State list, click **OOS** (Out of Service).
   b. On the toolbar, click **Apply** to place the port out of service. In the Confirmation dialog box, click **OK**.
4. Set the remaining port parameters and place the port back in service:
   a. In the External Interface (EXT) list, click **Y** (Yes).
   b. Verify that the remainder of the parameter values for the optical port is acceptable. Modify any default values, as necessary.
   c. In the Primary Service State list, click **IS** (In Service).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

d. On the toolbar, click **Apply** to place the port back in service and apply the port parameters. In the Confirmation dialog box, click **OK** to save your configuration settings.

Change the Line Rate on a RAP-OCn or RAP2-OCn

Rules for changing the line rate

The following rules apply when changing the line rate on a RAP-OCn or RAP2-OCn card:

- The RAP-OCn or RAP2-OCn card must be in standby mode before you change the line rate.

  Note: To change the line rate on an in-service simplex RAP-OCn or RAP2-OCn card, call the Technical Assistance Center (TAC) for assistance.

- When *decreasing* the line rate, no STSs can be provisioned outside the acceptable range of the new rate. The current packet bandwidth used by the port cannot exceed the new maximum bandwidth. If the RAP-OC port has STS paths (and cross-connections) provisioned on it outside of the capabilities of the new line rate, you must delete the cross connections and STS paths before changing the line rate.

Important: The RAP card reboots during this procedure. For unprotected cross-connections on this RAP card, this is a service-affecting procedure.

To change the RAP-OCn or RAP2-OCn line rate

1. Verify that the yellow (Stby) LED is lit on the protect (standby) card, and that the green (Active) LED is lit on the working (active) card. If they are not, troubleshoot the issue before continuing.
2. If you are changing the line rate for the working (active) RAP card, perform a manual switch to the duplex equipment:
   a. In the management interface, on the Navigation Tree, click the card to replace.
   b. If not already selected, click **Provisioning** to open the Provisioning Work Area.
   c. On the toolbar, click **Action** > **Switch** > **Switch Duplex**. In the Confirmation dialog box, click **OK** to perform the switch.
   d. Wait until the yellow (Stby) LED remains lit for the card.
3. In the management interface, on the Navigation Tree, click the Shelf level, and then click the standby RAP card.
4. In the **Provisioning,** Work Area, place the port out of service:
   a. In the Primary Service State list, click **OOS** (Out of Service) to place the port out of service.
   b. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

5. Set the line rate:
   a. In the Line Rate list, select the line rate.
   b. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save the change.
6. Place the port back in service:
   a. In the Primary Service State list, click **IS** (In Service) to place the port back in service.
   b. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK**.
7. Release the manual protection switch if you set it in Step 2, as follows:
   a. Click the optical port or STS Path where the protection switch was operated.
   b. On the toolbar, click **Action** > **Release Switch**.
   c. In the Confirmation dialog box, click **OK**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring OCn Optical Service Protection

OCn Optical Services Protection Parameter Overview

This section describes the parameters that must be configured for facility protection.

Identifier

Working AID: Specifies the address of the working port in the facility protection group. The port can be an OC-3, an OC-12, or an OC-48.

Protect AID: Specifies the address of the protecting port in the facility protection group. The port can be an OC-3, an OC-12, or an OC-48.

Protection Scheme

Specifies the protection scheme for the optical port. Specify 1+1 Linear Automatic Protection Switching (LAPS), 1:1 LAPS, UPSR, or UPSR with Packet Aggregation.

Note: Calix strongly recommends using a UPSR with Packet Aggregation protection scheme whenever possible. When fiber routing and node placement do not permit the configuration of a ring topology and LAPS protection is required, Calix recommends using a LAPS 1+1 bi-directional protection scheme.

Revertive (RVRTV)

Specifies if the system switches traffic back to the original card once the failure condition clears. The default value is N.

- Enter Y (Yes) to automatically switch traffic back to the original Working card or port once the failure condition clears.
- Enter N (No) for the Protect card or port to continue to carry traffic once the failure condition clears.

Equipment protection for the RAP common control cards is always non-revertive (N) and cannot be provisioned to be revertive.

Note: Optical transport services on a RAP-OCn card must be provisioned as part of a Facility Protection Group to be protected. An optical port protection for a RAP-OCn card can only be provided by a second RAP-OCn card of the same type. Additionally, you must initiate a SONET line protection switch request to switch the optical transport services. See *Facility Level Protection Switching* (on page 350) for additional information.

1:N equipment protection is always revertive (Y).

Only 1:1 equipment protection and optical line protection configurations (LAPS) can be provisioned as revertive or non-revertive.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Payload Defect Indication (PDIP)

Enables or disables a protection switch on a PDI-P defect. Set to Y (Yes) to allow protection switching when PDI-P (Payload Defect Indicator-Path) is detected. Set to N (No) to prevent protection switching when PDI-P is detected.

Wait To Restore (WTR)

Specifies the amount of time (in minutes) for the system to wait before restoring the working port. Specify a value between 5 and 12 minutes. The default value is 5 minutes.

This parameter only applies if the RVRTV parameter value is Y (Yes).

Configure Line Protection

Before configuring line protection, you must understand Line Protection Configurations.

Line protection scheme options include:

- Line: LAPS 1+1 unidirectional
- Line: LAPS 1+1 bidirectional
- Line: LAPS 1:1 unidirectional
- Line: LAPS 1:1 bidirectional

See also *Provisioning Network Transport* (on page 209).

Note: In this section RAP-OCn refers to both RAP-OCn and RAP2-OCn cards.

Optical port protection configuration rules and recommendations

- Optical ports cannot be configured to protect ports located on the same card.
- The OCn port used to protect the working OCn port must be the same type, for example an OC-12 to protect an OC-12.
- The port number of the OCn working card must match the port number of the OCn port of the protect card.
- The RAP-OCn port used to protect the working OCn port must be the same type on the adjacent RAP-OCn card.
- Calix recommends that optical cards with corresponding working and protect ports be placed in adjacent slots in the C7 shelf.
- Calix strongly recommends a LAPS 1+1 bi-directional protection scheme for external optical interfaces that require protection.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

To configure line protection

1. On the Navigation Tree, click an optical port.
2. In the Work Area, click **Protection**.
3. On the File menu, click:
   - (in iMS) **Create** > **Protection** > **Port Protection**
   - (in CMS) **Create** > **C7** > **Protection** > **Port Protection**
4. In the OCn Port Protection dialog box, Choose Working and Protect Ports area:
   a. In the Shelf list, select a shelf.
   b. In the Line Rate box, select the rate for your network.
   c. In the Working AID box, select an OC port to serve as the working port.
   d. Click **Add** to place the ports in the Protection Pairs To Be Created area.
5. In the Protection Options area:
   a. In the Protection Scheme box, select the Line LAPS protection scheme.
   b. In the Revertive list, click **Non-Revertive** or **Revertive**.
   c. In the Payload Defect Indication, select **Y** (Yes) to enable or **N** (No) to disable.
   d. In the Wait to Restore list, select the number of minutes.
6. Click **OK** to save your configuration.

Facility Level Protection Switching

The system provides the capability to initiate a SONET line or path protection switch request. Switch requests are initiated with these commands:

- **Lockout:** Lockout of protection line, lockout of working line, or lockout for path protection switching. This command locks out the entity identified by the AID from carrying active traffic. The lockout command takes priority over a forced switch command and overrides any forced switch in effect. Use the **Release Switch** command to clear the lockout command.
- **Forced:** Forced switch of working line to protection line, force switch of protection line to working line, or forced path protection switch. A forced switch switches traffic away from the entity identified by the AID. This overrides any failures and prevents future failures from initiating a protection switch. Any manual switch in effect is overridden and cleared. The forced switch command can be overridden only by a lockout command.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- **Manual:** Manual switch of working line to protection line, manual switch of protection line to working line, or manual path protection switch. This command switches traffic away from the entity identified by the AID, unless the entity being switched to has failed, or a manual, forced, or lockout switch is already in effect. This is cleared by any subsequent protection switch caused by an autonomous failure of the entity being switched to. A subsequent forced or lockout command overrides the manual switch command. The **Release Switch** command can also be used to clear the manual switch command.

Operate protection switching

Operate a protection switch on an optical port or STS Path as follows:

To operate line or path protection switching

1. On the Navigation Tree, click the optical port or STS Path operating the protection switch.
2. On the toolbar, click **Action** > **Operate Switch**, and then select one of the switch commands:
   - **Lockout**
   - **Forced**
   - **Manual**
3. In the Confirmation dialog box, click **OK**.
4. In the Result dialog box, click **OK**.

Release protection switching

Use the following procedure to release protection switching from an optical port or STS Path.

To release protection switching

1. On the Navigation Tree, click the optical port or STS Path where the protection switch was operated.
2. On the toolbar, click **Action** > **Release Switch**.
3. In the Confirmation dialog box, click **OK** to release the protection switch.
4. In the Result dialog box, click **OK**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Creating STS Paths

STS Path Parameters

The following parameters are associated with STS paths. The abbreviated name shown in parentheses represents the parameter ID in the Provisioning table view when multiple paths are selected.

STS Path Identifier (ID)

Specifies the location of the STS path being configured. Read the address left to right:

```
N{NodeID}-{ShelfID}-{SlotID}-{PortID}-{PathID}
```

NodeID is a number between 1 and 255. This number specifies the address of the C7 node in the network

ShelfID is a number between 1 and 5. This number specifies the address of the C7 shelf on the node.

SlotID is a number between 1 and 20. This number specifies the slot on the C7 shelf where the card resides. If the port is on a RAP card, this number can be CS-A or CS-B.

PortID represents the number of the port on the card in the slot. This number can be 1, 2, 3, or 4 for OC3-4 and OC12-4 cards. This number can only be 1 for OC48-1 and RAP-OCn cards.

PathID represents the number of the STS path.

Primary Service State (PST)

Specifies the default state of the equipment once it is installed. The values are IS (in-service) or OOS (out-of-service). The default value is IS.

You can also use this parameter if you are pre-provisioning a system. If pre-provisioning, the IS default value means the path is in-service once the equipment is installed.

STS Mapping (MAP)

Indicates the type of traffic going over STS path:

- **PT** (Pass Through): Pass the STS path through the shelf without terminating it.
- **ASYNC** (Asynchronous): Map DS3s traffic to an STS-1 path.

  Use the ASYNC setting only for the paths that are used as endpoints, such as DS3s services. For STS paths in between the endpoints, use Pass Through (PT). For STS-1 cross-connects, you must create an STS-1 PT on each transport card in the ring.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- **ATMNNI** (ATM Network-to-Network Interface): Connect packet traffic to another C7 node.
- **ATMUNI** (ATM User-to-Network Interface): Connect packet traffic to an external interface for most cases.

  The C7 supports both ATMUNI and ATMNNI mapping for connecting to external devices. You should match the STS Mapping to the configuration of the external device.

Payload Scrambling (PYLDSCRM)

Indicates whether payload scrambling for ATM cells is enabled or disabled:

- **Y** (Yes): Set to Y to enable payload scrambling. When you create an STS path, Y is the default when STS mapping is ATMUNI or ATMNNI.
- **N** (No): Set to N to disable payload scrambling.

ATM Monitoring (ATMMON)

Indicates whether ATM Diagnostic Monitoring is enabled or disabled. This parameter is set to Y (Yes) to enable ATM diagnostic monitoring on the STS path. If enabled, an ATM OAM loopback is used to verify point-to-point connectivity with the next line unit. It applies only to ATMNNI and ATMUNI interfaces. The default value is Y (Yes) for internal interfaces and N (No) for external interfaces.

Trace Identifier Mismatch Detection (TIMDET)

Indicates whether or not the trace identifier mismatch detection feature is enabled. The default value is OFF. Specify ON to enable the detection feature.

Expected Path Trace (EXPTRC)

This parameter is the expected Path Trace (J1) content. It is a user-defined character string. The maximum length of the string is 62 characters. The system automatically adds a carriage return (CR) and line feed (LF) to the end of the string to make it 64 characters.

Transmit Path Trace (TRC)

Indicates the path trace to transmit. It is a user-defined character string. The maximum length of the string is 62 characters. The system automatically adds a carriage return (CR) and line feed (LF) to the end of the string to make it 64 characters.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Far End Performance Monitoring (FEPM)

Enables performance monitoring and grade-of-service threshold violations on the far-end node:

- **Y** (Yes): Set to Y to enable performance monitoring and to count grade-of-service threshold violations.
- **N** (No): Set to N to disable performance monitoring. The default value is N (No).

Alarm Profile (ALMPROF)

Identifies if the AIS or LOS is an alarmed or non-alarmed event:

- **AISCR:** Specifies the AIS alarm is critical and generates a critical alarm.
- **LOSNR:** Specifies the LOS alarm is not reported and does not generate an autonomous report.
- **AISNR:** Specifies the AIS alarm is not reported and does not generate an autonomous report.

The default value is AISNR.

Signal Degrade Bit Error Rate (SDBER)

Sets the threshold value above which the bit error rate of the facility constitutes a degraded signal:

- 6 (value of 10 to the negative 6)
- 7 (value of 10 to the negative 7)
- 8 (value of 10 to the negative 8)
- 9 (value of 10 to the negative 9)

When the bit error rate exceeds the threshold specified in this parameter, the system raises a signal degraded bit error rate (SDBER) alarm.

The default value is 6.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Signal Failed Bit Error Rate (SFBER)

Sets the threshold value above which the bit error rate of the facility constitutes a failed signal:

- 3 (value of 3 to the negative 10)
- 4 (value of 4 to the negative 10)
- 5 (value of 5 to the negative 10)

When the bit error rate exceeds the threshold specified in this parameter, the system raises a signal failed bit error rate (SFBER) alarm.

The default value is 4.

Grade of Service Identifier (GOS)

Identifies the specific Grade of Service for Performance Monitoring (PM) applied to the STSn facility:

- **DEFLT:** Specifies the default values defined by applicable standards.
- **OFF:** Indicates that reporting of Threshold Crossing Alerts are turned off.
- **ID:** User-defined GOS profiles. Valid ID numbers are 1 through 20. See *Overview of Grade of Service Profiles* (on page 73) for additional information.

The default value is OFF.

STS Mapping Rules

The following rules apply when setting port STS mapping and external interface parameters:

- For internal facing STS1 facilities with DS3s endpoints (external connections), set the STS1 to Asynchronous (ASYNC) at the source and destination shelves, and Pass Through (PT) for all intermediate shelves, with the external interface set to No (N).
- For end-to-end SONET cross-connects through the ring, set the STS mapping for internal ports to PT, with the external interface set to N. Set the STS mapping for the endpoints to PT, with the external interface set to Yes (Y).
- For internal STS maps on the transport ring, set the STS mapping to ATM Network to Network Interface (ATMNNI), with the external interface set to N.
- For externally facing ports, set the STS mapping to ATM User to Network Interface (ATMUNI), with the external interface set to Y.

Create and Configure STS Paths

The C7 supports SONET transport signal (STS) paths for STS-1, STS-3c, STS-12c, and STS-48c.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Required: Match STS levels and numbers

STS levels and ID numbers must be the same around the UPSR ring.

Example: If you have an OC-48 port with 2 STS12c paths:

- STS-N1-1-2-1-**1**
- STS-N1-1-2-1-**13**

It must be connected to another OC-48 port with 2 STS12c paths using the same STS ID numbers above (in this example, 1 and 13).

STS path default parameters

When you create an STS path, you must define the type of traffic going over the connection (STS mapping). You can modify any of the other parameters; however, in most cases the default value is sufficient.

Parameter	Default Value
User Description	Optional field for entering a description of the STS path.
STS Mapping	**ASYNC** for STS1 or STS3c **PT** for STS12c
Payload Scrambling (PYLDSCRM)	**Y** (enabled) when STS Mapping is set to **ATMUNI** or **ATMNNI**.
Trace Identifier Mismatch Detection (TIMDET)	Off
Expected Path Trace (EXPTRC)	Null
Transmit Path Trace (TRC)	Null
Far End Performance Monitoring (FEPM)	No
Alarm Profile (ALMPROF)	Alarm Indication Signal Not Reported (AISNR)
Signal Degraded Bit Error Rate (SDBER)	6
Signal Failed Bit Error Rate (SFBER)	4
Grade of Service Profile (GOS)	OFF

To create an STS path for transport

1. On the File menu, click:
   - (in iMS) **Create** > **STS Path**
   - (in CMS) **Create** > **C7** > **STS Path**

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

2. In the Create SONET Transport Signal Facilities dialog box:
   a. In the Shelf list, select a shelf containing an optical transport card.
   b. In the Port list, select an optical port where the STS is to be created.
   c. In the Rate list, select an STS rate.
   d. In the available STS list, use Ctrl+click to select the STSs to create on the selected port.
   e. Click **Add** to place the selected STSs in the STS To Be Created area.
3. Repeat Step 2 for all transport ports.

   Note: Each port used for transport must also be designated for the STS path.
4. Click **Next**.
5. In the STS1s dialog box:
   a. (Optional) In the User Description box, type a short description.
   b. In the STS Mapping list, select the value required for the path.
   c. Change the default path parameters as needed for your situation.
   d. Click **OK** to create the STS paths.

The system is now ready for service provisioning.

Delete an STS Path

Use the procedure below to remove an STS path from the system.

Note: You must remove any cross-connections associated with the specific STS path before you can delete the path.

To delete an STS path

1. On the Navigation Tree, click the Shelf level.
2. On the Selection Filter, click **STS Path** > **STS Path**.
3. In the Work Area, click the STS Path for deletion.
4. On the toolbar, click **Delete**. In the Confirmation dialog box, click **OK** to confirm the deletion.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Creating STS Cross-Connections

Create STS Cross-Connections

After configuring a SONET transport signal (STS) path, you can create STS-1, STS-3c, STS-12c, or STS-48c cross-connections for service. All STS cross-connections sharing the same parameter values can be created in one procedure.

Related topics

- *View a List of Cross-Connections and Hops* (on page 126)
- *Add Drops to STS, VP, and VC Cross-Connects* (on page 132)
- *Delete Cross-Connects and Hops* (on page 134)

Cross-connection parameters

You set the following parameters when you create a cross-connection:

Cross-Connect Parameters	Default
Cross-Connect Way	2WAY
Cross-Connect Path (Required)	Must be specified when you create the cross-connection. For end-to-end cross-connections, Working and Protect (WORK + PROT) and Unprotected (UNPROT) are valid options. For a cross-connection hop, Working Only (WORK ONLY), Protection Only (PROT ONLY), and Unprotected (UNPROT) are valid options.

Note: The C7 uses SONET as the transport mechanism for the clear channel DS3s Hi-Cap service application. A DS3 cross-connection is done by mapping DS3 signals into an STS-1. At its destination, it is dropped as a DS3 and processed by DS3 equipment.

This procedure assumes that you are creating an STS-1 cross-connection. For other STS levels, the Type list in the Select Cross-Connect Endpoints dialog box (Steps 4 and 5) defaults to the STS level of the path you select.

Before creating a DS3 cross-connection for Hi-Cap service, check the parameter settings at the STS path level. Set the STS Mapping (Map) parameter for the source and destination paths to Asynchronous (ASYNC), and for each STS path between the endpoints to Pass Through (PT). See *STS Mapping for DS3s Hi-Cap Service* (on page 370).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

To create STS cross-connections

1. On the Navigation Tree, click the STS path where you want to create a cross-connection.
2. In the Work Area, click **Cross Connect**.
3. On the toolbar, click **Create** > **STS1 Cross Connect** to open the Select Cross-Connect Endpoints dialog box.
4. In the Source area of the dialog box:
   a. In the Shelf list, select the shelf where the source port is located.
   b. In the Type list, select the cross-connection type.
   c. In the ports list, use Ctrl+click to select a source port for each cross-connection to create.
   d. Click **SRC** to move the selected port(s) to the Source column Cross-Connects To Be Created area.
5. In the Destination/Drop area:
   a. In the Shelf list, select the shelf where the destination port is located.
   b. In the Type list, select the cross-connection type.
   c. In the ports list, use Ctrl+click to select the destination ports for the cross-connection(s).
   d. Click **DEST** to move the port(s) to the Destination column in the Cross-Connects To Be Created list.
6. In the Required Parameters area of the dialog box, do the following:
   a. In the Cross-Connect Way list, set the value per your service requirements: **1WAY** or **2WAY** (default).
   b. In the Cross-Connect Path list, select the path type.
7. Click **OK** to create the cross-connection(s).

Cross-Connection Parameters for Viewing

This section describes the parameters you can view for existing cross-connects.

See also

- *View a List of Cross-Connections and Hops* (on page 126)
- *Delete Cross-Connects and Hops* (on page 134)

Source Identifier (Source ID)

Specifies the access identifier, or network address, of the source endpoint of the cross-connection.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Destination Identifier (Destination ID)

Specifies the address of the destination endpoint of the cross-connect.

Drop Location (Drop IDS)

Specifies the port or path in the cross-connection where traffic is dropped along the path to the endpoint.

See also *Add Drops to STS, VP, and VC Cross-Connects* (on page 132).

Connection Type (CCT)

Specifies whether the cross-connection is set up as a one-way or a two-way connection.

Path

Specifies whether the cross-connection is both working and protect or unprotected. (For cross-connect hops, the possible path types are working only, protect only, or unprotected.)

Connection Status (CONSTAT)

The status of the cross-connection:

Display Status	Meaning
NORMAL	Connection is normal.
APPCRSMM	Application Cross-Connect Mismatch. The cross-connect was created by an application, identified by an Application ID in the traffic profile. The application has detected that this cross-connect exists in the RAP database, but not in the application database.
AUDITE	Provisioning of the cross-connection was rejected by an inter-shelf audit.
AUDITMM	Audit mismatch. The shelf audit found an inconsistency in the cross-connection.
COMMFAIL	Communication Failure. A failure occurred with the card while establishing the cross-connection.
EQPTE	Provisioning of the cross-connection was rejected by the card.
FEMM	Far-end mismatch. The inter-shelf audit found an inconsistency in the cross-connection.
NRDY	The connection is not ready to carry traffic.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Display Status	Meaning
PPLMM	Path Protection Label Mismatch. One of the following three conditions was detected in regards to the cross-connection: • An incorrect PPL • A PPL with no control VC • An incorrect mate PPL
PROVFAIL	Provisioning Failure. The card did not accept the cross-connection.
RDY	The cross-connection is ready to carry traffic.
VIDCRSMM	Video Cross-Connect Mismatch. The video application on the IRC detected that the cross-connect exists in its database, but does not exist in the RAP database.
VIDPARMMM	Video Parameter Mismatch. The video application on the IRC detected that the cross-connect has different parameter values in its database and the RAP database.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Chapter 10

Provisioning DS3 Services

This section describes DS3 cards, ports, and cross-connections. Instructions are provided for configuring equipment protection and DS3 services.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

DS3 Card, Port, and Cross-Connection Descriptions

Overview of DS3 Port Parameters

The section provides information on parameters associated with a DS3 port. You can edit most of them.

DS3 Port Access Identifier (ID): The address of the DS3 port you are viewing or modifying. The address reads from left to right:

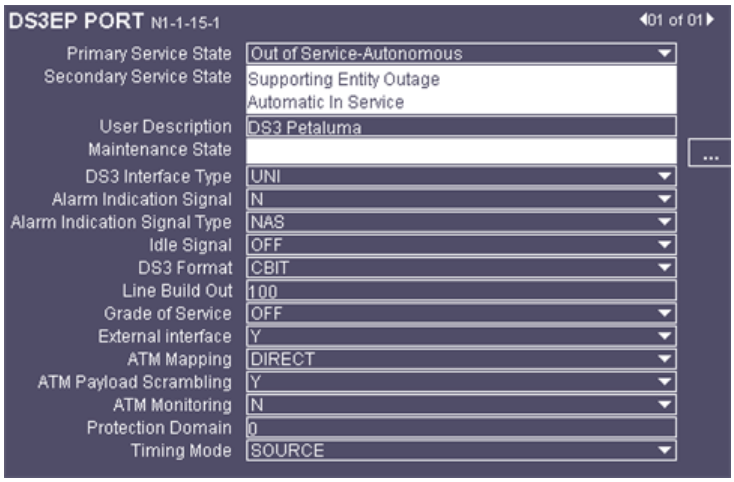
```
NodeID-ShelfID-SlotID-PortID
```

NodeID is a number between 1 and 255. This number specifies the address of the C7 node in the network.

ShelfID is a number between 1 and 5. This number specifies the address of the C7 shelf on the node.

SlotID is a number between 1 and 20. This number specifies the slot on the C7 shelf where the card resides.

PortID is a number between 1 and 4 for a DS3-4p card and between 1 and 12 for DS3-12p and DS3/EC1-12s cards. This number specifies the port on the DS3 card.



Primary Service State (PST): Indicates the service state that the DS3 port transitions to after you execute a provisioning command.

Secondary Service State (SST): Provides additional and relevant state information of the DS3 port.

User Description (USERDESCR): User description field.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Maintenance State (Maintenance): Displays any standing conditions currently affecting the port. If you are viewing the port in Form View, click the ellipsis button to the right of the Maintenance State field to view a list of the conditions.

DS3 Interface Type (INTF): The type of interface the DS3 provides. When the equipment type is DS3-12s, the interface type must be CCHAN. When the equipment type is DS3-4p or DS3-12p, the interface type must be either NNI or UNI.

Alarm Indication Signal (AIS): Controls how AIS is transmitted from this DS3 port:

- **Y** (Yes) sets the port to continuously transmit AIS.
- **N** (No) set the port to normal operation where AIS is transmitted only when a loss is detected.

Alarm Indication Signal Type (AIST): Specifies the type of AIS signal that is transmitted, and the AIS signal mode expected on input, should a failure condition occur. Note that for the DS3-4p or DS3-12p card, the only value accepted is NAS (North American Standard).

Idle Signal (IDLE): Indicates the transmission or non-transmission of the Idle signal. For the DS3-12s (CCHAN) card, Idle is transmitted only in the Ingress direction and not the Egress direction. For the DS3-4p and DS3-12p card, Idle is transmitted only in the Egress direction.

DS3 Format (FMT): Specifies the DS3 signal format. When the interface is UNI or NNI, the format must be CBIT. When the interface is CCHAN, either CBIT or M23 is valid.

Line Build Out (LBO): Specifies the line build out setting. The value range is 1 to 450 feet.

Grade of Service (GOS): Uniquely identifies one entry in the Grade of Service table that contains the performance parameters and their associated threshold values that apply to the DS3 port.

External Interface (EXTERNAL): Indicates whether or not the DS3 port represents an external path through the network.

ATM Mapping (ATM): Specifies how the ATM payload maps into the DS3 frame. Valid mapping variables are Direct or PLCP (Physical Layer Convergence Protocol) mapping.

Note: The ATM Mapping parameter is not applicable if the interface type is set to Clear Channel (CCHAN).

ATM Payload Scrambling (PYLDSCRM): Indicates whether payload scrambling for ATM cells is enabled or disabled:

- **Y** (Yes): To enable payload scrambling.
- **N** (No): To disable payload scrambling.

Note: The Payload Scrambling parameter is not applicable if the interface is set to Clear Channel (CCHAN).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

ATM Monitoring (ATMMON): Set to **Y** (Yes) to enable ATM diagnostic monitoring on the STS path. If enabled, an ATM OAM loopback ping is injected on VP0-VC3 to verify point-to-point connectivity with the next line unit. It applies only to ATM NNI and ATM UNI interfaces. The default value is **Y** for internal interfaces and **N** for external interfaces.

Protection Domain (PDOM): A unique integer that associates facility protection groups (FFPs) into a coordinated protection domain.

Timing Mode (TMGMODE): Specifies the timing source for the DS3E-4p T3 port transmit signal:

- **Loop:** T3 port transmit timing is sourced from the corresponding T3 port receive recovered timing.
- **Source:** T3 port transmit timing is sourced from the C7 system timing. Source is the default timing mode.

Note: TMGMODE is only relevant to DS3E-4p cards.

Default port parameters for a DS3-12s port

Parameter	System Default
DS3 Interface (INTF)	CCHAN (Clear Channel)
Alarm Indication Signal (AIS)	N (No)
Alarm Indication Signal Type (AIST)	North American Standard (NAS)
Idle Signal (IDLE)	OFF
DS3 Format (FMT)	CBIT (C-Bit parity format)
Line Build Out (LBO)	100 feet
Grade of Service (GOS)	OFF
External Interface (Ext)	Y (Yes)
Primary Service State (PST)	IS (In-service)

Default port parameters for a DS3-4p, DS3E-4p, or DS3-12p port

Parameter	System Default
DS3 Interface (INTF)	NNI (Network-to-Network Interface) or UNI (User-to-Network Interface)
Alarm Indication Signal (AIS)	N (No)
Alarm Indication Signal Type (AIST)	North American Standard (NAS)

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Parameter	System Default
Idle Signal (IDLE)	OFF
DS3 Format (FMT)	CBIT (C-Bit parity format)
Line Build Out (LBO)	100 feet
ATM Mapping (ATM)	Direct mapping (Direct)
Grade of Service (GOS)	OFF
Protection Domain (PDOM)	0
External Interface (EXTERNAL)	Y (Yes)
ATM Payload Scrambling (PYLDSCRM)	Y (Yes)
Timing Mode (TMGMODE) *Valid for DS3E-4p cards only.*	Source
Primary Service State (PST)	In-Service (IS)

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Overview of Cross-Connection Parameters

This section describes the parameters you can view for existing cross-connects.

Source STSn identifier (ID)

Specifies the address of the source endpoint of the cross-connection being created. STSn can be STS1, STS3c, STS12c, or STS48c.

Drop location (DropAddr)

Specifies the location in the cross-connection where traffic is dropped along the path to the endpoint. The value of this parameter is a cross-connection identifier.

Connection type (CCT)

Specifies the cross-connection as a one or two way connection.

- **2WAY:** Traffic flows in both directions on the connection.
- **1WAY:** Traffic flows in one direction on the connection.

The default value is 2WAY.

DS3 cross-connect defaults

Cross-Connect Parameter	DS3 Default
Connection Type (CCT)	2WAY
Cross-Connect Protection (PROTN)	N
Path (PATH)	UNPROT

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring DS3 Equipment Protection

The C7 supports 1:1 and 1:N equipment protection for DS3-12s cards and 1:1 equipment protection for DS3E-4p cards.

See *Configuring Equipment Protection* (on page 193) for detailed information on metallic services protection modules, equipment protection parameters, 1:1 equipment protection, configuring 1:1 equipment protection, 1:N equipment protection, and configuring 1:N equipment protection.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring DS3 Service

This section describes:

- STS mapping for DS3s Hi-Cap service
- Configuring DS3s ports for Hi-Cap service
- Configuring DS3 ports for ATM traffic

See also *Configuring DS3p Transport Links* (on page 250) for detailed information on setting up and provisioning DS3 transport.

STS Mapping and Cross-Connections for DS3s Hi-Cap Service

The C7 uses SONET as the transport mechanism for the clear channel DS3s Hi-Cap service application. A DS3s is carried across the SONET network as a DS3-mapped STS-1 devoted as a single DS3 with full-rate service. A DS3s cross-connection is done by mapping DS3 signals into an STS-1 Synchronous Payload Envelope (SPE) signal in accordance with SONET standards. At its destination, it is dropped as a DS3 and processed by DS3 equipment.

Note that the DS3 is treated as a single entity and mapped directly into an STS-1 SPE. This is referred to as asynchronous DS3 mapping. With asynchronous DS3 mapping, you can only cross-connect or add or drop signals at the STS-1 level.

Calix recommends that you set up your STS paths and STS mapping for DS3s service prior to configuring and provisioning the DS3s ports.

Before creating a DS3 cross-connection for Hi-Cap service, check the parameter settings at the STS path level. Follow the procedure below to set the STS Mapping (Map) parameter for the source and destination paths to Asynchronous (**ASYNC**), and for each STS path between the endpoints to Pass Through (**PT**).

To view and edit STS1 Mapping

1. On the Navigation Tree, click the STS1 level of the applicable optical port.
2. In the Work Area, click **Provisioning**.
3. In the STS1 Mapping list, click **ASYNC** if this is a source or destination path, or click **PT** if this is an STS path between the endpoints.

Repeat Steps 1 through 3 for the source and destination paths and each STS path between the endpoints for the DS3 connection.

See *Creating STS Paths* (on page 352) for additional information.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

To create a DS3 port STS1 cross-connection

1. On the Navigation Tree, click the DS3 port where you want to create a cross-connection.
2. In the Work Area, click **Cross Connect**.
3. On the toolbar, click **Create** > **STS1 Cross Connect** to open the Select Cross-Connect Endpoints dialog box.
4. In the Source area of the dialog box:
   a. In the Shelf list, select the shelf where the source port is located.
   b. In the Type list, select the cross-connection type **T3** or **STS1**.
   c. In the Ports list, use Ctrl+click to select a source port for each cross-connection to create.
   d. Click **SRC** to move the selected port(s) to the Source column Cross-Connects To Be Created list.
5. In the Destination/Drop area:
   a. In the Shelf list, select the shelf where the destination port is located.
   b. In the Type list, select the cross-connection type **T3** or **STS1**.
   c. In the Ports list, hold down the **Ctrl** key and click the destination ports for the cross-connection(s).
   d. Click **DEST** to move the port(s) to the Destination column in the Cross-Connects To Be Created list.
6. In the Required Parameters area of the dialog box, do the following:
   a. In the Cross-Connect Way list, set the value per your service requirements: **1WAY** or **2WAY** (default).
   b. In the Cross-Connect Path list, select the path type.
7. Click **OK** to create the cross-connection(s).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configure DS3s Ports for Hi-Cap Service

You can use the DS3-12s card to deliver Hi-Cap services. You create a DS3 clear channel pipe (full bandwidth availability—no framing or control bits required) that transports services from point A to point B with no effect on the payload.

DS3s port parameters for Hi-Cap service

The ports on the DS3-12s card are set up for Hi-Cap service as a default. The parameters used to configure a port for Hi-Cap service are follows:

Parameter	Value
DS3 Interface Type (fixed)	CCHAN
DS3 Format	CBIT (default) or M23 (also M13) (Set to match the incoming signal at the port.)
Line Build Out	100 feet (default) (Set per your site requirement.)

To configure a DS3s port for Hi-Cap service

1. On the Navigation Tree, click a DS3-12s card to view the ports, and then click a DS3 port to configure for Hi-Cap service.
2. In the **Provisioning** Work Area, take the port out of service:
   a. in the Primary Service State (PST) list, click **OOS** (Out of Service).
   b. On the toolbar, click **Apply** to place the port out of service. In the Confirmation dialog box, click **OK**.
3. Set the following parameters and place the port back in service:
   a. In the Primary Service State list, click **IS** (In Service).
   b. In the DS3 Format list, click **CBIT** or **M23** to match the signal received at the port.
   c. In the Line Build Out box, type a distance in feet as required for your site.
   d. On the toolbar, click **Apply** to place the port back in service. In the Confirmation dialog box, click **OK** to save your changes.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configure DS3p Ports for ATM Traffic

You can use the DS3-4p, DS3E-4p, or DS3-12p cards to provide an interface to an ATM switch or router for ATM services.

DS3p port parameters for ATM

You should check and set the following parameters to configure a DS3 port for ATM:

Parameter	Value
Interface	UNI (default)
Line Build Out	100 feet (default) (Set to match the distance in feet from the C7 to the ATM switch.)
ATM Mapping	DIRECT (default) or PLCP (Set to match your ATM switch setting.)
ATM Payload Scrambling	Yes (default) or No (Set to match your ATM switch setting.)

The default settings for ports on the DS3-4p, DS3E-4p, or DS3-12p are usually correct.

To configure a DS3p port for ATM

1. On the Navigation Tree, click a DS3-4p, DS3E-4P, or DS3-12p card to view the ports. Click a DS3 port to select it.
2. In the **Provisioning** Work Area, place the port out of service and set the following parameters:
   a. In the Primary Service State list, click **OOS** (Out of Service).
   b. In the DS3 Interface Type list, click **UNI**.
   c. In the Line Build Out box, type the distance in feet from the C7 to the ATM switch.
   d. In the ATM Mapping list, select the ATM mapping type used by the ATM switch.
   e. In the ATM Payload Scrambling list, click **Y** (Yes) or **N** (No) to match the setting used by the ATM switch.
   f. On the toolbar, click **Apply** to place the port out of service and apply the settings. In the Confirmation dialog box, click **OK** to save your changes.
3. Place the port back in service:
   a. In the Primary Service State list, click **IS** (In Service).
   b. On the toolbar, click **Apply** to place the port back in service. In the Confirmation dialog box, click **OK**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Chapter 11

Provisioning DS1 Services

This section describes C7 DS1 and T1 port parameters and equipment protection. Instructions are provided for configuring DS1 services and T1 IMA groups.

See also

- For information on setting up and provisioning T1 Transport Groups, see *Configuring T1 Transport Groups* (on page 263).
- For information on setting up and provisioning IMA Transport Groups, see *Configuring T1 IMA Transport* (on page 252).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

DS1 Port and Cross-Connection Descriptions

Overview of DS1 Port Parameters

The section provides information on parameters associated with a DS1/T1 port. The abbreviated name shown in parentheses represents the parameter ID in the Provisioning table view when multiple ports are selected in CMS.

Parameters display based on the card type and the selected DS1 Type parameter, which designates the port as a DS1 or a T1 port.

DS1 or T1 Port Identifier (ID)

The access identifier (AID) of the DS1 or T1 port that you are viewing or modifying. The AID reads from left to right:

NODE-SHELF-SLOT-PORT

NODE is a number between 1 and 255. This number specifies the address of the C7 node in the network.

SHELF is a number between 1 and 5. This number specifies the address of the C7 shelf on the node.

SLOT is a number between 1 and 20. This number specifies the slot on the C7 shelf where the card resides.

PORT is a number between 1 and 6 for T1-6 or T1-6 A+T cards, 1 and 8 for a T1-8 PWE card, or 1 and 12 for DS1A-12 and DS1-12 PWE cards. This number specifies the port on the card.

Primary Service State (PST)

Indicates the service state that the DS1 port transitions to after you execute a provisioning command. See *Primary Service State* (on page 576) for more information.

Secondary Service State (SST)

Provides additional state information of the DS1 port. See *Secondary Service State* (on page 577) for more information.

User Description (USERDESCR)

The user description field.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Maintenance State (Maintenance)

Displays any standing conditions currently affecting the port. If you are viewing the port in Form View, click the ellipsis button to the right of the Maintenance State field to view a list of the conditions.

IG-DS1 Access Identifier (IGDS1)

The address of the DS1 within the interface group. The format of a DS1 identifier for a GR-303 or T1TG group is (Node Id)-(Shelf #)-(IG Id)-(DS1 #). The format of a DS1 identifier for a GR-8 interface group is (Node Id)-(Shelf #)-(Slot #)-(IG Id)-(DS1 Identifier).

DS1 Format (FMT)

Specifies the DS1 framing format:

- **ESF** (Extended Superframe): ESF is used for voice services such as GR-303 or fractional T1.
- **SF** (Superframe): SF is used for fractional T1 or D4 voice service.
- **UF** (Unframed): UF is used for Hi-Cap service.

Equalization (EQLZ)

Specifies the short-haul line build out equalization setting for the port in feet. This parameter applies only when the DS1 Type is DS1.

DS1 Line Coding (LINECDE)

Specifies the DS1 line coding of a port:

- **AMI:** alternate mark inversion coding
- **B8ZS:** bipolar with 8 zero substitution coding

DS1 Type (DS1TYPE)

Designates the port as a DS1 or a T1 port:

- DS1 is typically specified for short-haul digital cross-connect.
- T1 is typically specified for long-haul transmissions.

Note: Ports on the DS1A-12 card support only the DS1 signal type.

DS1 Power (DS1PWR)

Indicates whether the line supplies power. This parameter applies only when the DS1 Type is T1. The values are SINK and SOURCE.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

DS1 Attenuation (DS1ATTN)

Indicates the attenuation for the transmitted signal over the T1 line. This parameter applies only when the DS1 Type is T1. The values are –15 dB, –22.5 dB, –7.5 dB, and 0.0 dB.

Grade of Service (GOS)

Uniquely identifies one entry in the Grade of Service table that contains the performance parameters and their associated threshold values that apply to the DS1 port.

DS1 Map (DS1MAP)

Designates how the payload signal at a specific port maps to a DS1 frame:

- **N/A:** No mapping is performed at the port.
- **NNI:** ATM network-to-network interface.
- **UNI:** ATM user-to-network interface.
- **SEQ:** Specified so that DS0 numbering occurs with the DS0 number equal to the time slot number.
- **PWUNSTRUCT:** Unstructured (clear-channel) T1 service in PWE3 SAToP packet format (RFC 4553).
- **PWSTRUCT:** Structured service (Fractional) T1 service in PWE3 CESoPSN packet format (RFC 5086).

External Interface (EXTERNAL)

Indicates whether or not the DS1 port represents an external path through the network. The value should be set to **Y** (Yes) when the port is an external interface. It should be set to **N** (No) when the port is connected to other shelves within a network of C7s. This parameter applies when the DS1 Map is set to NNI and UNI.

Protection Domain (PDOM)

A unique integer that associates a transport facility into a protection domain that is used for A to Z connection provisioning. The PDOM for each domain must be a unique non-zero integer. The value of 0 indicates that the facility is not to be used for A to Z connections.

Payload Scrambling (PYLDSCRM)

Configures whether to enable or disable the scrambling of ATM cells. This parameter applies when the DS1 Map is set to UNI or NNI.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

ATM Monitoring (ATMMON)

Set to **Y** (Yes) to enable ATM diagnostic monitoring on the STS path. If enabled, an ATM OAM loopback ping is injected on VP0-VC3 to verify point-to-point connectivity with the next line unit. It applies only to ATM NNI and ATM UNI interfaces. The default value is Y for internal interfaces and N for external interfaces.

Timing Mode (TMGMODE)

Indicates the timing source for the DS1 port transmit signal:

- **LOOP:** For PWE applications (DS1MAP=PWUNSTRUCT), LOOP indicates that the T1 transmission timing (from backplane toward the CPE direction) is derived from the far-end device recovered timing. Loop timing is independent of shelf timing. For T1 cross-connects (DS1MAP=N/A), LOOP indicates that the T1 transmission timing is regenerated by using AAL1 Synchronous Residual Time Stamp (SRTS).
- **SOURCE:** T1 transmission timing is derived from the C7 system timing.

  Note: Loop timing is typically used for unframed (UF) signals. Source timing is used for framed (SF or ESF) signals.

- **ADAPT**: (PWE card only) This method uses the average arrival time of the packets to derive the transmitter's clock. This is possible since the source device is producing bits at a constant rate determined by its clock. By averaging the arrival times, the Packet Delay Variance (PDV) can be negated and the original sender's clock recovered.
- **DIFF**: (PWE card only) This method employs a residual timestamp at the sender based on the difference between the shared reference clock and the T1/DS1 line. The receiver uses the timestamps in the received frames against its own time reference to correctly adjust its own T1 line timing. When a traceable clock is available between the two devices, this mechanism produces lower jitter than adaptive clock recovery.

ATM Resource Port Location (PLOCN)

The AID of the associated ATM resource port.

Inband Loopback Code (IBLBCODE)

(PWE card only) If the inband code is detected in the egress direction, a terminal loopback is automatically performed on the DS1 port. If the inband code is detected in the ingress direction, a facility loopback is automatically performed on the DS1 port.

Channel Associated Signaling (CAS)

Enables or disables whether signaling bits are carried in the TDM data, as well as in the signaling substructure. This parameter affects all pseudowires on the port.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Default port parameters for a DS1A-12 port

Parameter	System Default
DS1 Format	UF
Equalization	300 feet
DS1 Line Coding	B8ZS
DS1 Type	DS1
Grade of Service	OFF
DS1 Map	N/A
Timing Mode	LOOP

Default port parameters for a DS1-12 PWE or T1-8 PWE port

Parameter	System Default
DS1 Format	UF
Equalization[1]	300 feet
DS1 Line Coding	B8ZS
DS1 Type	DS1
DS1 Power[2]	SINK
DS1 Attenuation[2]	0.0
Grade of Service[1]	OFF
DS1 Map	PWUNSTRUCT
Timing Mode	DIFF
Inband Loopback Code	00001

[1] Displays when the DS1 Type is set to DS1.

[2] Displays when the DS1 Type is set to T1.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Default port parameters for a T1-6 or T1-6 A+T port

Parameter	System Default
DS1 Format	ESF
Equalization[1]	300 feet
DS1 Line Coding	B8ZS
DS1 Type	DS1
DS1 Power[2]	SINK
DS1 Attenuation[2]	0.0
Grade of Service[1]	OFF
DS1 Map	SEQ
External Interface	Y[3]
Protection Domain	0[3]
ATM Monitoring	N[3]
Timing Mode	SOURCE

[1] Displays when the DS1 Type is set to DS1.

[2] Displays when the DS1 Type is set to T1.

[3] Default parameter applies to the T1-6 A+T card only

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Overview of DS1 Cross-Connect Parameters

Source Identifier (Source ID)

Specifies the access identifier, or network address, of the source endpoint of the cross-connection.

Connection Type (CCT)

Specifies the cross-connection as a one or two way connection.

- **2WAY:** Traffic flows in both directions on the connection.
- **1WAY:** Traffic flows in one direction on the connection.

The default value is 2WAY.

Cross-Connect Path (PATH)

Specifies the type of path (connection) you are creating through the network.

- **WORK ONLY:** Creates a succession of virtual connections that are the working path through the network.
- **PROT ONLY:** Creates a succession of virtual connections that are the protecting path through the network.
- **WORK + PROT:** Creates both the working and protect paths.
- **UNPROT:** Creates an unprotected connection.

DS1 cross-connect default parameters

Cross-Connect Parameter	DS1 Default
Connection Type (CCT) (For DS1 cross-connections, 2WAY is the only valid connection type.)	2WAY
Cross-Connect Protection (PROTN)	N
Hop-By-Hop (HBH)	NOTHBH
Path (PATH)	UNPROT

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring DS1 Equipment Protection

The C7 supports 1:1 and 1:N equipment protection for DS1-12 PWE, DS1A-12, IMA-12, T1-6, T1-6 A+T, and T1-8 PWE cards.

See *Configuring Equipment Protection* (on page 193) for detailed information on metallic services protection modules, equipment protection parameters, configuring 1:1 equipment protection, and configuring 1:N equipment protection.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring DS1 Services

Configure DS1 Ports for Hi-Cap Service over SONET or ATM Network (C7 Prov., Help)

You can use DS1-12 PWE, DS1A-12, T1-6, T1-6 A+T, and T1-8 PWE cards to deliver Hi-Cap services. You create a DS1 clear channel pipe (full bandwidth availability—no framing or control bits required) that transports services from point A to point B with no effect on the payload.

See *Configuring HDSL for Hi-Cap DS1 Service (iMS, Help)* (on page 497) for information on configuring an HDSL port for Hi-Cap service.

DS1 port parameters for Hi-Cap service

You can configure ports on a DS1-12 PWE, T1-6,T1-6 A+T, or T1-8 PWE card for either a DS1 or T1 signal type. Both signal types can be used for Hi-Cap services. Ports on the DS1A-12 card support only the DS1 signal type.

The following table lists the parameters used to configure a port for Hi-Cap service.

Parameter	Value
DS1 Format	UF **Note:** Use the following procedure to apply port parameter changes all at once. To set the DS1 Format to UF independently, the DS1 Map value must first be set to N/A.
DS1 Map	N/A (no mapping applied)
DS1 Line Coding	B8ZS or AMI Set per your site requirement.
Timing Mode	Loop

To configure a DS1 port for Hi-Cap service

1. On the Navigation Tree, click a DS1 or T1 card to view the ports, and then click a DS1 port to configure for Hi-Cap service.
2. In the **Provisioning** Work Area, place the port out of service and set the DS Type:
   a. In the PST (Primary Service State) list, click **OOS** (Out of Service).
   b. In the DS1TYPE (DS1 Type) list, click **DS1** or **T1**, per your site requirements.
   c. On the toolbar, click **Apply** to place the port out of service. In the Confirmation dialog box, click **OK**.
3. Set the following parameters and place the port back in service:
   a. In the PST list, click **IS** (In Service).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

b. In the FMT (DS1 Format) list, click **UF** (unframed).

c. (For DS1 ports only) In the EQLZ (Equalization) box, type an equalization distance as required for your site.

d. In the LINECDE (DS1 Line Coding) list, select the line coding that matches the signal received at the port.

e. (For T1 ports only) Change the power and attenuation settings per your site requirements.

f. In the DS1MAP (DS1 Map) list, click **N/A**.

g. In the TMGMODE (Timing Mode) list, click **Loop**.

h. On the toolbar, click **Apply** to place the port back in service. In the Confirmation dialog box, click **OK** to save your changes.

Cross-Connect DS1 Ports for Hi-Cap Service

This topic describes how to create cross-connections for DS1 Hi-Cap service.

Related topics

- *View a List of Cross-Connections and Hops* (on page 126)
- *Delete Cross-Connects and Hops* (on page 134)

Cross-connection parameters

Set the following parameters when you create a cross-connection:

Cross-Connect Parameters	Default
Connection Type	2WAY
Cross-Connect Path (Required)	Must be specified when you create the cross-connection. For end-to-end cross-connections, Working and Protect (WORK + PROT) and Unprotected (UNPROT) are valid options. For a cross-connection hop, Working Only (WORK ONLY), Protection Only (PROT ONLY), and Unprotected (UNPROT) are valid options.

Note: The ability to cross connect Full T1 or T1 timeslots between ports on the same card is only supported for PWE3-capable cards.

To create Hi-Cap DS1 cross-connections

1. On the Navigation Tree, click a port where you want to create a cross-connection.
2. In the Work Area, click **Cross Connect**.
3. On the toolbar, click **Create** > **T1 Cross Connect** to open the Select Cross-Connect Endpoints dialog box.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

4. In the Source area of the dialog box:
   a. In the Shelf list, select the shelf where the source port is located.
   b. In the Type list, click **T1**.
   c. In the Ports list, click the port that is the source for the cross-connection.
   d. Click **SRC** to place the source port in the Cross-Connects To Be Created list.
5. In the Destination/Drop area of the dialog box, do the following:
   a. In the Shelf list, select the shelf where the destination port is located.
   b. In the Type list, click **T1**.
   c. In the Ports list, click the port that is the destination for the cross-connection.
   d. Click **DEST** to move the destination port to the Cross-Connects To Be Created list.
6. Repeat Steps 4 and 5 for each additional cross-connection you are creating.
7. In the Cross-Connect Path list in the Required Parameters area, select the path type for the cross-connection: Working Only, Protect Only, Working and Protect, or Unprotected.
8. Click **OK** to save the cross-connection.

Configure DS1 Ports for TDM Service

You can use DS1-12 PWE, T1-6, T1-6 A+T, and T1-8 PWE cards to provide a switch interface for TDM services.

T1 port parameters for TDM traffic

You can configure ports on a DS1-12 PWE, T1-6, T1-6 A+T, and T1-8 PWE card for either a DS1 or T1 signal type. Both signal types can be used for TDM traffic.

The following table lists the parameters used to configure a port for TDM traffic.

Parameter	Valid values for TDM service
DS1 Format	ESF or SF Set per your site requirement.
DS1 Line Coding	B8ZS (default) or AMI Set per your site requirement.
DS1 Map	SEQ
Timing Mode	Source

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

To configure a DS1 port for TDM traffic

1. On the Navigation Tree, click a T1 card to view the ports, and then click a DS1 port to configure for TDM traffic.
2. In the **Provisioning** Work Area, place the port out of service and set the DS1 Type:
   a. In the PST (Primary Service State) list, click **OOS** (Out of Service).
   b. In the DS1TYPE (DS1 Type) list, click **DS1** or **T1**, depending on your site requirement.
   c. On the toolbar, click **Apply** to place the port out of service and apply the DS1 Type. In the Confirmation dialog box, click **OK**.
3. Set the following parameters and place the port back in service:
   a. In the PST list, click **IS** (In Service).
   b. In the FMT (DS1 Format) list, click **ESF** or **SF** as required for your site.
   c. (For DS1 ports only) In the EQLZ (Equalization) box, type an equalization distance as required for your site.
   d. In the LINECDE (DS1 Line Coding) list, select the line coding that matches the signal received at the port.
   e. (For T1 ports only) Change the power and attenuation settings per your site requirements.
   f. In the DS1MAP (DS1 Map) list, click **SEQ**.
   g. In the TMGMODE (Timing Mode), click **SOURCE**.
   h. On the toolbar, click **Apply** to place the port back in service and to apply the settings. In the Confirmation dialog box, click **OK** to save your changes.

Cross-Connect DS1 Ports for TDM Service

This topic describes how to create cross-connections for DS1 TDM service. You can cross-connect a DS1 or T1 port for either T0 service or T1 timeslot service.

Related topics

- *View a List of Cross-Connections and Hops* (on page 126).
- *Delete Cross-Connects and Hops* (on page 134).

Allowed port types

When creating DS1 cross-connections for TDM service, the following rules apply:

- For T0 service, either the source or the destination endpoint must be a T1 timeslot. The other endpoint must be a DS0 port.
- For T1 timeslot service, both the source and destination endpoints must be T1 timeslots.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Cross-connection parameters

Set the following parameters to create a cross-connection:

Cross-Connect Parameters	Default values and other information
Connection Type	2WAY
Number of Signaling Bits	• For cross-connections other than DS0 clear channel, the correct default is automatically applied based on the DS1 format of the endpoint (4 for ESF or 2 for SF). • To create DS0 clear channel cross-connections (for example, timeslots reserved for data), you must override the default setting and type 0 in this field.
Number of DS0s in the Same VC	1 (For fractional T1 service, numbers from 2 to 24 are valid.)
Nailed Up	N (No)

Notes:

- This procedure assumes that you are creating a cross-connection with a T1 timeslot as the source endpoint and a T0 port as the destination endpoint. The port types you use may vary depending on your site requirements.
- The ability to cross connect Full T1 or T1 timeslots between ports on the same card is only supported for PWE3-capable cards.
- The parameter settings in Step 7 (Connection Type, Number of Signaling Bits, Number of DS0s in the Same VC, and Nailed Up) are applied to all cross-connections that you create at one time. If you are creating cross-connections with different parameter values, you must repeat this procedure in its entirety for those cross-connections.

To create DS1 cross-connections for TDM traffic

1. On the Navigation Tree, click a port where you want to create a cross-connection.
2. In the Work Area, click **Timeslot Cross Connect**.
3. On the toolbar, click **Create** > **T0 Cross Connect** to open the Select Cross-Connect Endpoints dialog box.
4. In the Source area of the dialog box:
   a. In the Shelf list, select the shelf where the source port is located.
   b. In the Type list, click **T1 Timeslot**.
   c. In the Ports list, select the source port for the cross-connection.
   d. In the Timeslot box, type the number of the timeslot (1 through 24) to use for the first cross-connection. If you are creating multiple cross-connections using the same port, select the **Auto-increment** check box to automatically advance to the next timeslot once you click SRC in Step 4e.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

e. Click **SRC** to move the source port to the Cross-Connects To Be Created list. If you are using the **Auto-increment** check box, click **SRC** again for each timeslot to add.

f. Repeat Step 4 for any additional source ports to specify.

5. In the Destination area:

a. In the Shelf list, select the shelf where the destination port is located.

b. In the Type list, click **T0**.

c. In the Ports list, select the destination port for the cross-connection.

d. Click **DEST** to move the destination port to the Cross-Connects To Be Created list.

e. Repeat Step 5 to specify any additional destination ports.

6. If you are configuring service over fiber transport, go to Step 7.

If you are configuring service over T1 transport, in the IDT Route area do the following:

a. In the Cross-Connects To Be Created area, use Ctrl+click to select the cross-connections to add to a single transport group.

b. In the Shelf list, select the shelf with the IDT interface for the T1 transport group.

c. In the transport group list, select the T1 transport group.

d. Click **IDT** to assign the IDT to the selected ports.

Repeat Step 6 if you need to assign a different IDT route to cross-connections that you have specified.

7. In the Required Parameters area, select the parameter values per your site requirements, or accept the default values.

8. Click **OK** to create the cross-connections.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configure T1 Ports for ATM Service

You can use the T1-6 A+T or IMA-12 card to provide an interface to an ATM switch or router for ATM services.

T1 port parameters for ATM traffic

You can configure ports on the T1-6 A+T or IMA-12 card for either a DS1 or T1 signal type. Both signal types can be used for ATM traffic.

The following table lists the parameters used to configure a port for ATM traffic.

Parameter	Value
DS1 Map (required)	UNI
External Interface (required)	Y (Yes)
Payload Scrambling	N (No) or Y (Yes) The default is N. Set to match the signal received at the port.
DS1 Format	ESF (default) or SF Set to match the signal received at the port.
DS1 Line Coding	B8ZS (default) or AMI Set to match the signal received at the port.
DS1 Type	DS1 or T1 Set per your site requirement.
Equalization (Used with DS1 type)	300 feet (default) Set per your site requirement.
Power (Used with T1 type)	Sink (default) or Source Set per your site requirement. Selecting source puts –130V on the T1 line.
Attenuation (Used with T1 type)	0.0 dB (default) or –7.5, –15.0, –22.5 dB Set per your site requirement.

To configure a DS1 port for ATM traffic

1. On the Navigation Tree, click a T1 card to view the ports, and then click a DS1 port to configure for TDM traffic.
2. In the **Provisioning** Work Area, place the port out of service and set the DS1 Type:
   a. In the Primary Service State (PST) list, click **OOS** (Out of Service).
   b. In the DS1 Type list, select **T1**.
   c. On the toolbar, click **Apply** to place the port out of service and apply the DS1 Type. In the Confirmation dialog box, click **OK** to display parameters for a T1 signal type.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

3. Set the External Interface parameter to Y:
   a. In the External Interface list, click **Y**.
   b. On the toolbar, click **Apply** to set the port for an external interface. In the Confirmation dialog box, click **OK**.
4. Place the port back in service and set the remaining required parameters:
   a. In the Primary Service State list, click **IS** (In Service).
   b. In the DS1 Format list, click **ESF** or **SF** to match the signal received at the port.
   c. In the DS1 Line Coding list, select the line coding that matches the signal received at the port.
   d. In the DS1 Power list, click **Sink** or **Source** as required for your site.
   e. In the DS1 Attenuation list, select an attenuation dB value as required for your site.
   f. In the DS1 Map list, click **UNI**.
   g. In the Payload Scrambling list, click **Y** or **N** to match the signal received at the port.
   h. On the toolbar, click **Apply** to place the port back in service and apply the parameter settings. In the Confirmation dialog box, click **OK** to save your changes.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring T1 IMA Groups

For information about setting up T1 IMA links for C7 transport, see *Configuring T1 IMA Transport* (on page 252).

For information about setting up an ATM uplink, see the *Calix Broadband Data Services Guide.*

Create an IMA Group and Add T1s

Create one or more IMA groups, and then add multiple T1 or ATM resource ports:

- For a T1-6 A+T card, add T1 ports from a single card.
- For an IMA-12 card, add ATM resource ports associated with one or more T1-6, T1-6 A+T, HDSL, or IMA-12 cards.

This section includes these procedures:

- Create an IMA group.
- Add DS1 or ATM resource ports to an IMA group (IMA-12 cards).
- Add T1 ports to an IMA group (T1-6 A+T cards).

Recommendations for IMA 1.0 compatibility

Use the following practices to ensure compatibility with external devices using IMA 1.0:

- Use sequential T1 ports in an IMA group.

  OK: Create an IMA group with ports 1 through 3.

  Not OK: Create an IMA group with ports 1, 3, and 5.
- Wire ports on the Calix T1-6 A+T or IMA-12 card to the matching port number on the external device.
- On T1-6 A+T cards, you may need to configure the IMA Group to force compatibility with IMA 1.0 devices and older routers. Change the ALTV_1 parameter to Y (Yes) if you have difficulty connecting to an external device using IMA 1.0.

If you are connecting to another C7 shelf or an IMA 1.1-compatible device, these steps are not required.

To create an IMA group

1. On the File menu, click:
   - (in iMS) **Create** > **Ports**
   - (in CMS) **Create** > **C7** > **Ports**

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

2. In the Ports - Provisioning by Port Type dialog box:
   a. In the Shelf list, select the shelf where the T1-6 A+T or IMA-12 card for the IMA group is located.
   b. In the Port Type list, click **IMA Group**.
   c. In the list of available IMA Groups, select a group on the T1-6 A+T or IMA-12 card to contain the IMA group.
   d. Click **Add** to place the selected IMA group in the To Be Created Ports list.
   e. Click **OK** to create the IMA group.

Note: For a T1-6 A+T card, all the T1 ports added to an IMA group must be on the same card.

To add DS1 or ATM resource ports to an IMA group (IMA-12 cards)

1. On the Navigation Tree, click the shelf containing the IMA-12 card, then click the IMA group to modify.

   Note: Select an IMA group ID on the IMA-12 card (correct node, shelf, and slot).

2. In the Work Area, on the Provisioning tab, click the ellipsis button next to the Physical Location Identifiers box to open the New Add AP for IMA dialog box.
3. In the New Add AP for IMA dialog box, do the following:
   a. To add DS1 ports, click **Choose T1 Port from the list**.

      —or—

      To add ATM resource ports, click **Choose AP Port from the list**.

   Note: DS1 ports must be from T1 cards in the same shelf as the IMA-12 card. If DS1 ports are added, corresponding ATM Resource Ports are automatically provisioned.

   Note: Before ATM resource ports can be added, they must be associated with DS1 ports from supported cards [see *Configure the ATM Resource Ports (optional)*, above].

   b. In the Available Ports list, press the **Ctrl** key and click the ports to add to the IMA group.
   c. Click **Add** to add the ports to the Selected Ports list.
   d. Click **OK** to add the ports to the IMA group.

To add T1 ports to an IMA group (T1-6 A+T cards)

1. On the Navigation Tree, click the shelf containing the T1-6 A+T card, then click the IMA group to modify.
2. In the Work Area, on the Provisioning page, click the button next to the Physical Location Identifiers box to open the New Add T1 IMA dialog box.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

3. In the New Add T1 IMA dialog box, do the following:
   a. In the Available Ports list, press the **Ctrl** key and click the T1 ports to add to the IMA group.
   b. Click **Add** to add the ports to the Selected Ports list.
   c. Click **OK** to add the ports to the IMA group.

Configure an IMA Group for ATM Uplink

Configure an IMA group as an external interface for passing ATM traffic to an ATM switch or router.

IMA group parameters for an ATM uplink

Check and set these parameters to configure an IMA group for ATM uplink:

Parameter	Value
Mapping	The IMA mapping configures how the internal fixed length packets are mapped at the IMA interface. Set to UNI (User Network Interface).
External Interface	Indicates if the IMA group is an internal or external path in the network. Set to Y (yes).
Payload Scrambling	Configures whether to enable or disable the scrambling of ATM cells. Set this parameter to Y (enable) or N (disable) to match the signal received at the IMA group.
Timing Mode	Specifies the timing source for the IMA group: • **LOOP:** T1 transmission timing is derived from the far-end device recovered timing. Loop timing is independent of shelf timing. • **SOURCE:** (Default) Transmission timing is derived from the C7 system timing. **Note:** Use Source timing mode when: • An IMA-12 card uses an HDSL or T1 port that is not on the same card. • The far-end uplink device uses recovered (Loop) timing.

The IMA group parameters listed below are not typically changed from the default values:

Parameter	Description
Primary Service State	Specifies the primary service condition of the IMA group. By default this parameter is set to In Service (IS).
Secondary Service State	Specifies the service condition of the IMA group when the Primary Service State is in the Out of Service (OOS) state.
Bandwidth Capacity	Displays the total packet payload capacity that the IMA group can carry in Kbps.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Parameter	Description
Transmit Bandwidth Used	Displays the total packet payload capacity in Kbps that has been allocated to VP and VC cross connects leaving the shelf on the IMA group. The value may be greater than the bandwidth capacity if the IMA group has been over subscribed.
Receive Bandwidth Used	Displays the total packet payload capacity in Kbps that has been allocated to VP and VC cross connects entering the shelf on the IMA group. The value may be greater than the bandwidth capacity if the IMA group has been over subscribed.
Physical Location Identifier	Displays the physical location of the port(s).
Minimum Number of Facilities	Minimum number of required active links for the IMA group to remain in a working state. If this minimum value is exceeded, a service-affected alarm is raised for the IMA group. When creating an IMA group, the default is 1.
Max. Diff. Delay	The maximum number of milliseconds of differential delay that is tolerated among the links. When creating an IMA group, the default value is 25.
Inhibited	Configures whether the group is allowed to become operational and carry ATM data. The default is N (do not inhibit).
Frame Length	The IMA frame length used by the IMA group. The options are 32, 64, 128, and Max. The default is 128.
ALTV1_0	Specifies whether the IMA group uses the alternative IMA version 1.0. Setting this parameter to N (No) uses IMA version 1.1, which in many cases is backward-compatible with external devices using IMA 1.0. Set the parameter to Y (Yes) to force compatibility with devices using alternative IMA 1.0, such as older Cisco routers. The default is N.
Symmetry	Displays the symmetry mode. Currently the C7 is configured to operate only in Symmetrical Configuration and Operation mode.
Clock Mode	Specifies the transmit clock mode for an IMA group. Currently the C7 is configured to only support the Common Transmit Clock mode.
Grade of Service	The grade of service that is applied to the IMA group. When creating an IMA group, the default is OFF.
Link Grade of Service	The grade of service that is applied to the IMA links. When creating an IMA group, the default is OFF.

Configure the IMA group as an uplink

Configure the IMA group providing the uplink as an external UNI interface.

Note: In Step 4 in the following procedure, you must change the External Interface parameter independently from changing any other parameter. Because the External Interface parameter is Y (Yes) by default, you can often skip this step.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

To configure an IMA group for ATM uplink

1. On the Navigation Tree, click the shelf containing the IMA group providing the uplink.
2. Click IMA Groups, then click the IMA group to configure.
3. In the Work Area, on the Provisioning tab, take the IMA group out of service:
   a. In the Primary Service State list, click **OOS**.
   b. Click **Apply** to place the IMA group out of service. In the Confirmation dialog box, click **OK**.
4. Designate the IMA group as an the external interface:
   a. In the External Interface list, click **Y**.
   b. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your changes.
5. Set the mapping, payload scrambling, and other parameters:
   a. In the Mapping list, click **UNI**.
   b. In the Payload Scrambling list, click **Y** (enable) or **N** (disable) to match the signal received at the IMA group.
   c. Set the remaining parameter values according to your requirements. Default values are typically acceptable.
   d. In the Primary Service State list, click **IS**.
   e. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your changes.

After creating an IMA group and configuring its T1 links for use with another vendor's hardware, check for the following two problems:

- IMA alarms or link alarms are raised and cleared repeatedly.
- The maintenance state for the IMA group is other than normal condition. (In the Work Area, view the maintenance state on the Provisioning tab.)

One possible cause of these problems is an IMA idle cell setting that is not compatible with the other vendor's hardware.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Chapter 12

Provisioning DS0 Services

This section describes DS0 cards, ports, and cross-connections. Detailed information is provided for configuring GR-303, GR-57, GR-8, universal, and non-switched services.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

DS0 Port and Cross-Connection Descriptions

Overview of DS0 Port Parameters

General Signaling Function (GSFn)

Indicates the signaling used by the port, such as loop-start for POTS. The valid values for GSFn depend on the card and can include: 2COIN, 2EBS, 2GS, 2LR, 2LS, 2LSGS, 2NO, 2NOS, 2RVOD, 2RVOI, 2RVOW, 4D0, 4DU, 4NO, and 4NOS.

GSFN Value	Description
Switched Signaling	
2LS	Two-wire POTS loop-start current feed signaling per GR-303. With loop-start, a phone line or trunk is seized (started) by bridging through a resistance (the tip and ring) of the telephone line giving it a supervisory signal. Normal single line phones and key systems typically work on loop-start lines.
2COIN	Two-wire dial tone first coin signaling per GR-303. Dial-Tone-First (DTF) coin telephone service is a loop-start service with modified and additional signaling requirements. This service allows coin pay phones to be used as emergency call stations without first depositing coins.
2EBS	Two-wire Enhanced Business Set (EBS) signaling. This signaling interface supports the Nortel EBS (P-Phone) service. Simultaneous voice and extended signaling services are provided on the same loop.
2GS	Two-wire ground-start current feed signaling per GR-303. With ground-start signaling, a ground signal is sent over the trunk ring lead and is received over the trunk tip lead. Ground-start signaling is a type of analog voice-grade access signaling that requires the customer interface to provide a ground on the ring conductor at the network interface to initiate service requests.
2LSGS	Two-wire loop-start or ground-start signaling per GR-303. With loop-start signaling, a closure signal is sent through the loop formed by the trunk leads. Loop-start and ground-start signaling is a way of signaling on subscriber trunks where one side of the two-wire trunk (typically the ring conductor) is briefly grounded to obtain dial tone. PBXs typically work better on ground-start trunks. Normal single line phones and key systems typically work on loop-start.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

GSFN Value	Description
2RVOD	Two-wire loop-reverse-battery supervision signaling with delay dial outpulsing per GR-303. The network element supplies battery. Loop-reverse-battery is a type of switched-access line DC signaling that uses loop-open and loop-closure signals in one direction, and normal battery polarity and reverse battery polarity in the other direction to indicate on-hook and off-hook signals. With delay dial outpulsing, a steady signal is sent to the switch and is removed when the trunk is ready to receive digits. In this operation, the originating end seizes the line, waits to determine if the far end is on-hook, and then outpulses digits. If the far end is off-hook, the originating end waits until the far end is on-hook before outpulsing digits.
2RVOI	Two-wire loop-reverse-battery supervision signaling with immediate dial outpulsing per GR-303. The network element supplies battery. Loop-reverse-battery is a type of switched-access line DC signaling that uses loop-open and loop-closure signals in one direction, and normal battery polarity and reverse battery polarity in the other direction to indicate on-hook and off-hook signals. With immediate dial operation, no start dial signals are used. On outgoing calls, the system waits after sending the seizure signal before sending the digits to the switch. This allows the switch time to attach a digit receiver to the call.
2RVOW	Two-wire loop-reverse-battery supervision signaling with wink-start outpulsing per GR-303. The network element supplies battery. Loop-reverse-battery is a type of switched-access line DC signaling that uses loop-open and loop-closure signals in one direction, and normal battery polarity and reverse battery polarity in the other direction to indicate on-hook and off-hook signals. With wink-start outpulsing, a momentary signal (wink) is sent to the switch. The originating end seizes the line by going off-hook. Outpulsing starts after acknowledgment from the other end. Wink-start outpulsing provides an integrity check that helps to identify a malfunctioning trunk and allows the network to transmit a re-order tone to the calling party.
Non-switched signaling	
2NO	Two-wire transmission only signaling per GR-57. A transmission only signaling interface is used where there is no circuit associated signaling or the signaling is provided by in-band tones.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

GSFN Value	Description
2NOS	Two-wire transmission only signaling, sealing current supplied per GR-57. A transmission only signaling interface is used where there is no circuit associated signaling or the signaling is provided by in-band tones. On two-wire interfaces the sealing current is applied to the tip and ring conductors.
4NO	Four-wire transmission only signaling per GR-57. A transmission only signaling interface is used where there is no circuit associated signaling or the signaling is provided by in-band tones.
4NOS	Four-wire transmission only signaling, sealing current supplied per GR-57. A transmission only signaling interface is used where there is no circuit associated signaling or the signaling is provided by in-band tones. On four-wire interfaces the sealing current is applied to the simplex of the cable pairs.
4D0	DS0-DP6 port signaling interface. The Calix DS0 DP-6 card provides six DDS interfaces, each supporting software-selectable data rates: 2400, 4800, 9600, 56000, and 64000 (clear channel) Kbps.
4DU	OCU-DP6 port signaling interface. The Calix OCU DP-6 card provides six DDS interfaces, each supporting software-selectable data rates: 2400, 4800, 9600, 56000, and 64000 (clear channel) Kbps.
PLAR Signaling	
2LR	Two-wire Private Line Automatic Ringdown (PLAR) signaling per GR-57. PLAR signaling types are associated with private line voiceband services. PLAR circuits have statically configured endpoints and do not require the user dialing to connect calls. A PLAR connection is often referred to as a "bat-phone" because when one end goes off hook the other end rings.

Transmit Transmission Level Point (TTLP)

Sets the signal power ratio for transmitting toward the equipment. The transmission level point is the decibel value of the ratio of the power of a 1004 Hz signal at a point to the power of the same signal at a reference point on the digital side of the codec. An increase in the TTLP results in a gain toward the digital side.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Receive Transmission Level Point (RTLP)

Sets the signal power ratio for receiving from the equipment. The transmission level point is the decibel value of the ratio of the power of a 1004 Hz signal at a point to the power of the same signal at a reference point on the digital side of the codec. An increase in the RTLP results in a gain toward the analog side.

Impedance

Indicates the expected impedance of the line in Ohms.

Enhanced Business Service Level (EBSLVL)

Sets the transmission level of the secondary signaling channel for Nortel Enhanced Business Service on a DMS100 switch. Settings are AUTO, HIGH, and LOW.

Enhanced Full-Time Transmission (EFTT)

Enables or inhibits transmission of the audio channel even when the subscriber is on-hook and the phone has not recently been rung.

- **Y** (Yes): Enables transmission
- **N** (No): Inhibits transmission

Overview of DS0 Port Connection Status Parameters

The following parameters display in the Connection Status tab for DS0 ports:

CONN (Connection Status): This parameter indicates if a call is currently active (Y or N).

RXSIG (Receive Signal): This parameter indicates the current signaling in the receive direction. RXSIG is

a string value. RXSIG is optional, and does not apply to ONT DS0s.

TXSIG (Transmit Signal): This parameter indicates the current signaling in the transmit direction. TXSIG

is a string value. TXSIG is optional, and does not apply to ONT DS0s.

RCVR (Receiver State): This parameter indicates whether the receiver is off hook or on hook. RCVR is optional.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Redlining Ports

Redline is an optional secondary state on a DS0 port indicating that a circuit requires special handling. Often used for emergency or 911 phone lines, redlining a DS0 port adds an extra level of protection to a special circuit to prevent accidental deletion. If a redlined DS0 port is cross-connected, the redline must be manually removed from the port before the cross-connect can be deleted.

To redline a DS0 port

1. On the Navigation Tree, expand the shelf and click the DS0 port to redline.
2. In the Work Area, click **Provisioning**.
3. On the toolbar, click **Action** > **Redline Ports**.
4. In the Confirmation dialog box, click **OK** to confirm the redline.

To remove a redline from a DS0 port

1. On the Navigation Tree, expand the shelf and click the DS0 port to remove the redline.
2. In the Work Area, click **Provisioning**.
3. On the toolbar, click **Action** > **Deactivate Redlined Ports**.
4. In the Confirmation dialog box, click **OK** to confirm the deletion.

Overview of DS0 Cross-Connect Parameters

Use the parameters listed in this section to create DS0 cross-connections through a C7 network.

Source identifier (Source ID)

Specifies the access identifier, or network address, of the source endpoint of the cross-connection.

Connection type (CCT)

Specifies the cross-connection as a two-way (**2WAY**) connection.

Number of signaling bits (NUMSIGBITS)

Specifies the number of bits in the subscriber signaling channel:

- **0** – Disables signaling for clear channel operation on robbed-bit TDM transport links.
- **2** – Sets signaling for the SF format used by D4 channel banks. DS0 Yellow and DS0 AIS signals are disabled.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- **3** – Sets signaling for GR-8 signals.
- **4** – Sets signaling for GR-303 and internal transport of GR-57.

The default value is 4.

Number of DS0s (NUMDS0S)

Specifies the number of DS0s to create in the same VC. When a value greater than 1 is specified, consecutive DS0s are connected starting with the source and destination DS0s.

This parameter ensures that the delay is the same within the set of DS0s. This is needed for transport that cannot tolerate differing frame delays among DS0s from the same port, such as the DDS error correction channel.

The default value is 1.

Echo Cancelation Mode (ECMODE)

Specifies whether the line uses the echo cancelation features from the interface group (Use IG) or echo cancelation is turned off (Off).

The default value is Use IG.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring GR-303 Services

The C7 provides two methods for configuring GR-303 services:

- Non-concentrated mode
- DS0 Remote Voice Concentration mode

DS0 Remote Voice Concentration mode provides a new model for Time Division Multiplexing (TDM) connections between a network interface group and C7 POTS cards. The remote voice concentration feature increases transport efficiencies and enables DS0 over-subscription. Only active calls are assigned DS0s over the inter-C7 transport links as opposed to the current non-concentrated method for provisioned lines. This feature removes the 3,168 provisioned POTS lines per C7 shelf limitation provided in the non-concentrated mode and provides 3,168 active POTS calls per optical card.

See *DS0 Remote Voice Concentration* (on page 424) for detailed information.

Quick GR-303 Configuration Process

Use the Quick GR-303 Configuration Process to get GR-303 service up and running using these standard recommendations suitable for most situations.

Note: You can have up to 15 shelf-based interface groups per C7 shelf, including voice concentration groups, GR-303 interface groups, H.248 interface groups, and T1 transport groups. See *GR-8 Interface Group Configuration Rules* (on page 440) for GR-8 slot-based interface groups.

Services covered

This section covers configuring a T1 port for GR-303 interface and configuring DS0 ports for POTS service. Configuration parameters for Coin and other DS0 services are also addressed.

Starting point

Before starting this Quick GR-303 Configuration Process, check the following conditions are met:

- Transport is configured.
- Remote DS0 service cards are installed and wired.
- DS1 network interface cards are installed and wired to a GR-303 switch interface.

Information you need

You need to have the following information on-hand to complete GR-303 provisioning:

- Switch type for the GR-303 interface

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- Line build out distance from the C7 to the switch
- Transmission level and impedance values for services you plan to configure
- Number of DS1s between the C7 and the switch
- Number of Virtual DS1s (VDS1s) for each C7 remote shelf (if you are using the remote voice concentration feature)

Remote voice concentration

Remote voice concentration enables a more efficient allocation of bandwidth on the transport path between the C7 shelf containing POTS service cards and the C7 shelf hosting the GR-303 interface to a Class 5 switch. Bandwidth is allocated in DS1 increments; each virtual DS1 reserved on the transport path allows for up to 24 active calls from the designated remote C7 shelf. Once a voice concentration shelf is created, the number of virtual DS1s reserved on the transport path can be dynamically increased or decreased, without re-provisioning the GR-303 interface or the CRV cross-connects.

Configuration rules for concentrated and non-concentrated modes

- You cannot configure DS0 voice concentration and non-concentrated cross-connections in the same interface group for the same C7 shelf.
- An interface group can have mixed (concentrated and non-concentrated) modes to different shelves.
- A shelf can have different modes back to different interface groups.
- You cannot assign a Voice Concentration Shelf to an interface group when the interface group has cross-connections to that shelf unless you check the Reprovision DS0s box to convert the existing non-concentrated DS0 cross-connects to the concentrated mode. If you do not want to convert existing cross-connects to the concentrated mode as part of the process of adding a Voice Concentration Shelf, you must:
  - Delete existing cross connects (using the Bulk Reprovisioner tool).
  - Create the Voice Concentration Shelf.
  - Re-create the deleted cross connects (using the Bulk Reprovisioner tool).
- Remote voice concentration does not apply to ONT DS0 ports, because PON applications already concentrate ONT DS0s. You can mix ONT and non-ONT DS0 ports in a concentration shelf with a common GR-303 group association, but the ONT DS0s do not use the concentration shelf VDS1s.

Converting existing non-concentrated DS0 cross-connects to the concentrated mode

The system provides two methods of reprovisioning existing DS0 cross-connections in a GR-303 non-concentrated interface group to a GR-303 concentrated interface group:

- Bulk Reprovisioner tool. See *Converting Existing CRVs* (on page 429).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- Reprovision check box in the Voice Concentration Shelf dialog box. See *Creating a Voice Concentration Shelf* (on page 414).

Use the Reprovision DS0s check box in the Voice Concentration Shelf dialog box to reprovision existing DS0 cross-connections in the interface group. If you select this option, the system deletes the existing DS0 cross-connects and reprovisions the cross-connects after the Voice Concentration Shelf is created. Voice services are not available for the affected DS0 cross-connects during the reprovisioning process.

Quick GR-303 configuration process flow

- Create a GR-303 interface group.
- Configure a T1 port for a GR-303 switch interface.
- Assign a T1 port to a GR-303 interface group.
- Create a Voice Concentration Shelf (if using the Remote Voice Concentration method)

  Note: If there are pre-existing non-concentrated DS0 cross-connections in the interface group, you must convert them to the concentrated mode when assigning a Voice Concentration Shelf to the interface group.

- Configure DS0 ports for service.
- Associate Call Reference Values (CRV) to an interface group.
- Check that it all works.

GR-303 Interface Group Parameter Descriptions

When you create a GR-303 interface group, you set values (or confirm system default values) for the following parameters:

GR-303 Interface Group Access Identifier (IGAID)

The address of the GR-303 interface group you are creating. The address consists of: (Node Id)-(Shelf#)-(IG#). Valid parameters are Node{1–255}-Shelf{1–5}-Interface Group{1–16}.

Primary AMP (PRIAMP)

Identifies the primary AMP or ATP card that manages the EOC channel for the GR-303 interface group.

Secondary AMP (SECAMP)

Identifies the secondary AMP or ATP card that manages the EOC channel for the GR-303 interface group and provides redundant protection for the Primary AMP. The Primary AMP and Secondary AMP must be separate cards.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Switch Type (SWTYPE)

Indicates the type of switch that the GR-303 interface group connects to (for example, 5ESS or DMS10).

T308 Timer (T308)

Specifies the maximum length of time in seconds that the remote digital terminal waits for a reply to a RELEASE message. The default value is 4. Valid parameters are 2 to 5 seconds.

T303 Timer (T303)

Defines the maximum length of time in milliseconds that the remote digital terminal waits for a reply to a SETUP message. The default value is 700. Valid parameters in steps of 500 milliseconds are 700, 1200, 1700, 2200, 2700, 3200, 3700, 4200, and 4700.

T396 Timer (T396)

Specifies the length of time in milliseconds that the remote digital terminal waits for a reply to a SETUP message following the initial expiration of timer T303. The default value is 14700. Valid parameters in steps of 1000 milliseconds are 700, 1700, 2700, 3700, 4700, 5700, 6700, 7700, 8700, 9700, 10700, 11700, 12700, 13700 and 14700.

T397 Timer (T397)

Specifies the maximum length of time in seconds the remote digital terminal waits for the integrated digital terminal to acknowledge an INFORMATION message that indicates that a customer who had been generating a permanent signal has returned on-hook. The default value is 120. Valid parameters in seconds are 60, 120 and 180.

EOC Alarm Report (EOCALMREP)

Indicates which alarms are to report through the EOC interface. The EOC can report alarms for the shelf IG (interface group), the entire network, or no alarms at all. The default value is Network.

Note: If network-wide EOC alarm reporting is enabled for multiple GR-303 groups connected to the same switch, the switch receives duplicate alarms.

EOC Up Service States (EOCUPSST)

Specifies whether or not to report service state changes to the switch if the EOC link is down. Some switches, such as the DMS100, do not audit the CRVs when the EOC link is re-established. In this situation the switch continues to have the incorrect service state, which can cause a traffic disruption. When set to Y (Yes), this parameter sends service state notifications for all provisioned CRVs when the EOC link comes up. The default value is N (No).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Flow Through

Indicates flow-through provisioning. This provisionable option in a Class-5 switch, when enabled, causes the switch to send provisioning messages over the EOC of a given GR-303 interface group to manage analog line terminations in the RDT. The switch will Create, Delete, Remove from Service, and audit each CRV in the RDT when this option is enabled. If the switch invokes analog line termination and flow-through provisioning is enabled, then the RDT should not issue any service state notifications to the switch for that line. If flow-through provisioning is disabled, then the RDT should always issue service state notifications for all lines. The default value is N.

Create a GR-303 Interface Group

Create an interface group on a C7 shelf containing an AMP or ATP card and select a second C7 shelf with an AMP or ATP card to provide redundancy.

GR-303 configuration rules

Follow these rules when configuring GR-303 services in your network:

- Each interface group can support 1 to 2048 Call Reference Values (CRVs).
- A C7 shelf can be configured with up to 15 GR-303 interface groups.

  Note: You can have up to 15 shelf-based interface groups per C7 shelf, including voice concentration groups, GR-303 interface groups, H.248 interface groups, and T1 transport groups. See *GR-8 Interface Group Configuration Rules (iMS, Help)* (on page 440) for GR-8 slot-based interface groups.

- An AMP or ATP card can manage up to 15 GR-303 interface groups distributed across multiple shelves.
- The AMP or ATP card that manages a GR-303 interface group does not have to be located on the same shelf where the interface group is located.
- GR-303 interface groups must be configured on the same shelf where the T1 ports for the switch interface are located.
- Using a GR-303 interface group is not supported on a C7 shelf that is also configured with an RDT T1 Transport Group.
- If T1 transport is not used between C7 shelves, the maximum number of fiber links between the remote endpoint of a subscriber channel and its GR-303 T1 is 15.
- If T1 transport is used between C7 shelves, the maximum number of fiber links is 10.
- A maximum of 4 ports on a T1-6 or T1-6 A+T card can support primary or secondary GR-303 links (links 1 or 2). The remaining 2 ports can be assigned to any GR-303 group as link 3 or higher.

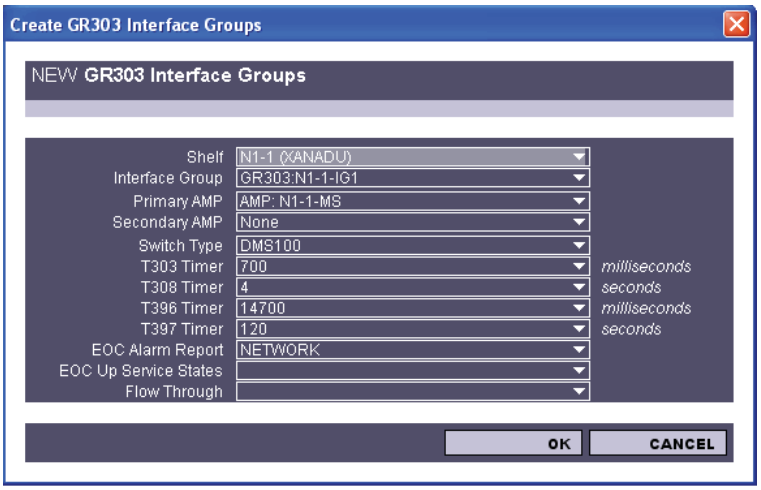
  Note: Calix recommends that the primary and secondary links reside on different T1-6 or T1-6 A+T cards.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- For T1-8 PWE and DS1-12 PWE cards, there is no limitation regarding the number of ports that can be assigned to the primary or secondary interface group links.
- DS1 ports must be configured for GR-303 service before they can be assigned to an interface group.
- Configure service on DS0 ports to match the switch service configuration before associating the DS0 ports to an interface group. If there is a service mismatch, the switch attempts to overwrite the port configuration.
- If multiple interface groups from a single C7 shelf connect to the same switch, only one interface group should report EOC alarms. Set the EOC Alarm Report (EOCALMREP) parameter to NETWORK for one interface group and set the remaining interface groups to NONE.

To create a GR-303 interface group

1. On the File menu, click:
   - (in iMS) **Create** > **Interface Group** > **GR303** > **GR303 Interface Group**
   - (in CMS) **Create** > **C7** > **Interface Group** > **GR303** > **GR303 Interface Group**
2. In the Create GR303 Interface Groups dialog box, set the following interface group parameters:



   a. In the Shelf list, select the shelf that contains the T1 interface to the switch.

   b. In the Interface Group list, the default is the next available IG number for the selected shelf. Leave the default or click a different IG number in the list.

   c. In the Primary AMP list, select an AMP or ATP to manage the interface group.

   d. In the Secondary AMP list, select an AMP or ATP to protect the Primary AMP.

   e. In the Switch Type list, select the type of switch for the interface group connection.

Note: Because the Timer parameters are automatically set according to the type of switch you select, leave these parameters at their default values.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

f. In the EOC Alarm Report list, select the alarm reporting level. The default is **Network** to send all alarms in the C7 network to the switch.

Note: Set the EOC Alarm Report option to **Network** for at least one GR-303 interface group. Enable network-wide EOC alarm reporting for multiple GR-303 interface groups connected to the same switch results in the switch receiving duplicate alarms.

g. In the EOC Up Service State, click **Y** or **N** to report service state changes to the switch if the EOC link is down.

h. In the Flow Through list, click **Y** or **N** to match the setting used by the switch.

3. Click **OK** to create the interface group.

GR-303 alarms after creating an Interface Group

When you create a GR-303 Interface Group, the system reports two alarms for failures on the EOC and TMC communications channels. These alarms clear as soon as you connect the C7 shelf to a Class 5 switch with the primary or secondary DS1 interface.

View or Modify Attributes of a GR-303 Interface Group

When you create a GR-303 interface group, the C7 system automatically assigns default values to the interface group parameters. In most instances, these default values are sufficient and should not require modification.

If it is necessary to modify the parameters, complete the steps below.

To view or modify GR-303 interface group attributes

1. On the Navigation Tree, click the C7 shelf containing the GR-303 interface group.
2. On the Selection Filter, click **Interface Group** > **GR303** to display all the GR-303 interface groups associated with the shelf in the Work Area, and then click an interface group to select it.
3. In the Edit Row, select one or more parameters to modify.
4. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your configuration settings.

Configure a T1 Port for a GR-303 Switch Interface

DS1 facilities provide the links to the switch for GR-303 interfaces. You can use the following DS1 cards for switch interface service:

- DS1-12 PWE
- T1-6
- T1-6 A+T

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- T1-8 PWE card

You can configure the DS1 ports for either a DS1 or T1 signal type. Both types can be used in a GR-303 Interface Group. A common configuration is to use DS1 ports on a central office shelf connected to a switch. Before continuing, verify that the T1 cards are installed and wired out to the switch. Refer to the *Calix C7 Installation Guide* for installations instructions.

You can configure up to 28 DS1 ports to serve each GR-303 interface group.

T1 port parameters

The following table lists the parameters used to configure a port for a GR-303 switch interface.

Parameter	Value
DS1 Format	ESF
DS1 Line Coding	B8ZS
DS1 Map	SEQ
DS1 Type	DS1 or T1
Timing Mode	Source
If DS1 Type = DS1	
Equalization	Distance to switch
If DS1 Type = T1	
DS1 Power	Sink (default) or Source Set per your site requirement.
DS1 Attenuation	0.0 dB (default) or –7.5, –15.0, –22.5 dB Set per your site requirement.

This procedure describes configuring DS1 ports for a GR-303 switch interface. The default port parameters are suitable for use.

To configure a T1 port for a GR-303 switch interface

1. On the Navigation Tree, click a C7 shelf containing an interface group and assigned T1 ports.
2. On the Selection Filter, click **Port** > **DS1/T1 Port** to display all DS1/T1 ports from the selected shelf in the Work Area.
3. In the **Provisioning** Work Area, use Ctrl+click to select all T1 ports to configure for use in an interface group.

   Recommendation: Click at least two T1 ports on separate cards.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

4. In the Edit Row, place the ports out of service and set the DS1 Type:
   a. In the PST (Primary Service State) list, click **OOS** (Out of Service).
   b. In the DS1TYPE (DS1 Type) list, click **DS1** or **T1**.
   c. On the toolbar, click **Apply** to place the ports out of service and apply the DS1 Type. In the Confirmation dialog box, click **OK**.
5. Select the same ports as in Step 3, and set the port parameters to the following values:
   a. In the FMT (DS1 Format) list, click **ESF**.
   b. (For DS1 ports only) In the EQLZ (Equalization) box, type the distance in feet from the C7 to the switch.
   c. In the LINECDE (DS1 Line Coding) list, click **B8ZS**.
   d. (For T1 ports only) Change the power and attenuation settings per your site requirements.
   e. In the DS1MAP (DS1 Map) list, click **SEQ**.
   f. In the TMGMODE (Timing Mode) list, click **Source**.
   g. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to confirm the changes.
6. Select the same ports as in Step 3, and in the Edit Row, place the ports back in service:
   a. In the PST (Primary Service State) list, click **IS** (In Service).
   b. On the toolbar, click **Apply** to place the ports back in service. In the Confirmation dialog box, click **OK**.

Assign T1 Ports to a GR-303 Interface Group

After configuring T1 ports for GR-303 switch interface, assign from 2 to 28 T1 ports to an interface group.

Configure T1 ports first (required)

You must have T1 ports correctly configured for use in an interface group before you can assign them to a group. The default settings on a new T1 port are the correct settings for use in an interface group.

If a T1 port is not configured correctly, the system rejects assignment to an interface group and displays the following error message:

```
"The T1 port parameters are invalid for assigning a DS1 IG."
```

Match interface group DS1 numbers with the switch (required)

The DS1 assignment numbers for a C7 interface group must match the DS1 numbers configured at the switch.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Example: If the T1 port N1-1-4-6 is assigned to DS1 number 1 in the interface group N1-1-IG1-1, it must also be configured as DS1 number 1 at the switch.

Maximum of 4 primary and secondary links on a T1-6 card (restriction)

A maximum of 4 ports on a T1-6 card can support primary or secondary interface group links (links 1 or 2). The remaining 2 ports can be assigned to any interface group as link 3 or higher.

If more than 4 ports on a T1-6 card are assigned as primary or secondary interface group links, the system rejects assignment to an interface group and displays the following error message:

```
"Card does not have enough available HDLCs to complete the request."
```

In such cases, assign the primary and secondary links to ports on a different T1-6 card.

Note: For T1-8 PWE and DS1-12 PWE cards, there is no limitation regarding the number of ports that can be assigned to the primary or secondary interface group links.

Recommendations for assigning T1 ports to an interface group

- Assign 2 T1 ports to an interface group, with ports on separate T1 cards, assigned to links 1 and 2. Provides protection against equipment failure for the EOC and TMC communication channels.
- Distribute T1 port assignments evenly across multiple T1 cards to provide protection against equipment failure for subscriber traffic.

To assign T1 ports to a GR-303 interface group

1. On the Navigation Tree, click the shelf level.
2. On the File menu, click **Create** > **Interface Group** > **GR303** > **Interface Group DS1** to open the Interface Group DS1 dialog box.
3. In the Available T1 Ports area do the following:
   a. In the Shelf list, select a shelf containing a GR-303 interface group.
   b. In the Interface Group list, select an interface group on the selected shelf.
   c. In the available T1 ports list, hold down the **Ctrl** key and click T1 ports to add to the interface group.

   Note: DS1 numbers are assigned to the ports in the order that you add them.

   d. Click **Add** to place the T1 ports with assigned DS1 numbers in the T1 Ports To Be Added To Interface Groups As IG-DS1 area.
4. When you are done adding ports, click **OK** to create the T1 assignments.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Creating a Voice Concentration Shelf

This procedure describes how to configure a remote voice concentration shelf for concentrating GR-303 services.

Prior to setting up a remote concentration shelf, see *Converting Existing CRVs* (on page 429) to determine which method to use to convert existing CRVs.

Note: If you are configuring non-concentrated GR-303 services, skip this procedure and go to *Configure DS0 Ports for Service* (on page 416).

Number of VDS1s (TDM VCs) and the concentration ratio

The number of Virtual DS1s (VDS1s) in conjunction with concentration ratio is calculated in the following manner:

```
Number TDM VCs = (DS0s in shelf / 24) / ratio desired
```

Note: If result is not a whole number, round up to nearest whole number.

Shown below are two examples of the calculation.

Assuming that you want to set a concentration ratio of 4:1 and you have 96 DS0s in the RT, the formula produces:

```
(96 / 24) / 4 = 1 VDS1
```

Assuming you want to set a concentration ratio of 4:1 and you have 97 DS0s in the RT, the formula produces:

```
(97 / 24) / 4 = 1.01 rounded up to 2 VDS1s
```

Note: VDS1s (TDM VCs) are not created at this point—VDS1s specified for the remote C7 shelf are created when the DS0 cross-connections are configured in the remote shelf.

Call capacity alarm threshold

Use the CAP Alarm Threshold % field in the Voice Concentration Shelf dialog box to set the call capacity threshold. If the number of active calls reaches or exceeds this percentage of the total calls, an alarm is raised.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

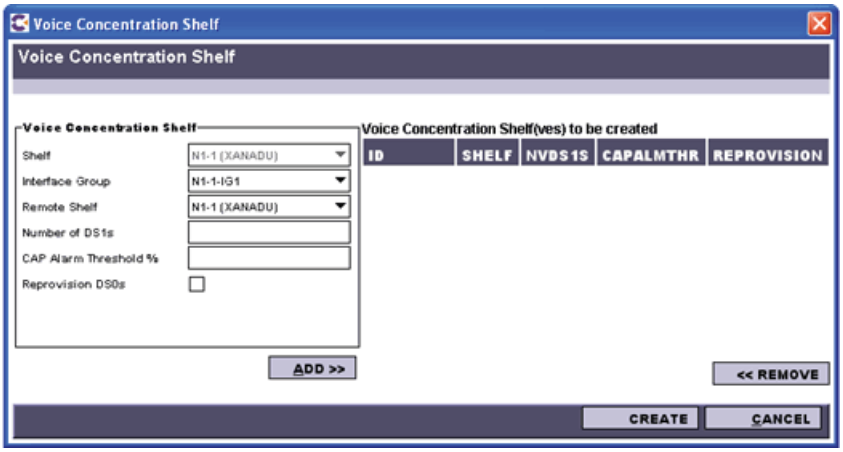
Create the voice concentration shelf

Follow this procedure to create a voice concentration shelf to concentrate GR-303 services.

ALERT! Selecting the Reprovision DS0s check box is a service-affecting operation.

To create a voice concentration shelf

1. On the Navigation Tree, click the Shelf level.
2. On the File menu, click:
   - (in iMS) **Create** > **Interface Group** > **GR303** > **Voice Concentration Shelf**
   - (in CMS) **Create** > **C7** > **Interface Group** > **GR303** > **Voice Concentration Shelf**



3. In the Voice Concentration Shelf dialog box, Voice Concentration Shelf area:
   a. In the Shelf list, click the associated C7 shelf.
   b. In the Interface Group list, click the interface group.
   c. In the Remote Shelf list, click the remote C7 shelf providing POTS.
   d. In the Number of VDS1s box, type the number of Virtual DS1s allocated for this association.

Note: This number determines the call capacity for the interface group to the associated C7 shelf.

   e. In the CAP Alarm Threshold % box, type the percentage at which to raise an alarm if the number of active calls reaches or exceeds this percentage.
   f. Select the Reprovision DS0s check box if you want to reprovision existing DS0 cross-connects within the selected interface group to the Voice Concentration Shelf. If selected, the system deletes the existing DS0 cross-connects and reprovisions the cross-connects after the Voice Concentration Shelf is created.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

4. Click **Add** to move the specified information to the Voice Concentration Shelf(ves) To Be Created area.
5. Repeat Steps 3 and 4 for additional Voice Concentration Shelves.
6. Click **Create**.

Configure DS0 Ports for Service

Remote DS0 ports provide a subscriber interface for DS0 services. Configure the remote ports for the type of DS0 service delivered.

DS0 port parameters for POTS service

The default setting for DS0 ports on RPOTS-24, RU2W-24, and COMBO cards is for POTS service.

Parameter	Value
General Signaling Function (GSFn)	2LS
Receive Transmission Level Point (RTLP)	–2.0 dB
Transmit Transmission Level Point (TTLP)	–2.0 dB
Impedance	900

Configuring DS0 services other than POTS

Ports on DS0 equipment can be configured for many DS0 switched services.

- Coin service can be configured on the first four ports of the RU2W-24 card. Set the GSFN parameter to 2COIN.
- Other DS0 services can be configured on all ports of the RPOTS-24, RU2W-24, and COMBO-24 cards (not COMBO2-24, COMBO2-24A, and COMBO2-24D cards). Set the GSFN parameter to a service type.

To set DS0 port parameters

1. On the Navigation Tree, click a C7 shelf containing DS0 ports to select it.
2. On the Selection Filter, click **Port** > **DS0 Port** to display all DS0 ports from the selected shelf in the Work Area.
3. In the Work Area, click **Provisioning** to view the DS0 port parameters.
4. Click the first DS0 port, and then Shift+click the last DS0 port to select a range of ports to configure.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

5. Place the ports out of service and set the DS0 parameters:
   a. In the PST (Primary Service State) list, click **OOS** (Out of Service).
   b. In the GSFN (General Signaling Function) list, select a signal type.
   c. In the RTLP (Receive Transmission Level Point) list, select a decibel value.
   d. In the TTLP (Transmit Transmission Level Point) list, select a decibel value.
   e. In the Impedance list, select an impedance setting of **600** or **900** ohms.
   f. On the toolbar, click **Apply** to place the ports out of service and apply the DS0 parameter settings. In the Confirmation dialog box, click **OK**.
6. Re-select the same range of ports to configure as selected in Step 4.
7. Place the ports back in service:
   a. In the PST list, click **IS** (In Service).
   b. On the toolbar, click **Apply** to place the ports back in service. In the Confirmation dialog box, click **OK**.

Cross-Connect DS0 Ports to GR-303 Interface Group CRVs

Call Reference Values (CRVs) are used to build translation tables on the Class 5 switch that map remote connections to internal circuits at the switch.

Call Reference Value parameter descriptions

When you create cross-connections between CRVs and DS0 facilities (ports), you set the values for the following parameters:

- **Call Reference Value Access Identifier (CrvAid):** Identifies the CRV (circuit) address of a subscriber line in a GR-303 interface group. The access identifier consists of (Node ID)-(Shelf #)-(Interface Group #)-(CRV #). Valid parameters are: Node{1-255}-Shelf{1-5}-IG{1-15}-CRV{1-2048}.
- **Physical Location (PLOCN):** Identifies the physical location of the subscriber line associated with a CRV within the C7 network. The identifiers consist of: (Node ID)-(Shelf #)-(Slot #)-(RPOTS Port #).

Use the procedure below to cross-connect DS0 ports to interface group CRVs.

To associate CRVs with DS0 ports

1. On the File menu, click:
   - (in iMS) **Create** > **Interface Group** > **GR303** > **CRV**
   - (in CMS) **Create** > **C7** > **Interface Group** > **GR303** > **CRV**

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

2. In the Select Cross-Connect Endpoints dialog box, Source area:
   a. In the Shelf list, select a shelf containing a GR-303 interface group.
   b. In the Type list, click **CRV/Channel/Line**.
   c. In the GR303/08/H248 list, select an interface group on the selected shelf.
   d. In the CRV/Channel/Line box, type a range of CRV numbers equal to the number of DS0 ports to provision.
   e. Click **SRC** to place the ports in the Cross-Connects To Be Created area.
3. In the Destination area:
   a. In the Shelf list, select the shelf where the DS0 ports are located.
   b. In the Type list, click **T0** (default).
   c. In the Slot list, click the slot containing the card with the DS0 ports.
   d. In the Ports list, use Ctrl+click to select the DS0 ports to associate with CRVs.
   e. Click **DEST** to place the ports in the Cross-Connects To Be Created area.
4. If you are configuring service over fiber transport, go to Step 5.

   If you are configuring service over T1 transport, in the IDT Route area do the following:
   a. In the Cross-Connects To Be Created area, select all of the T0 ports.
   b. In the Shelf list, select the shelf with the IDT interface for the T1 Transport Group.
   c. In the T1TG list, select the T1 Transport Group configured as the IDT interface.
   d. Click **Add** to assign the IDT to the selected ports.
5. Repeat Steps 2 through 4 to associate additional T0 ports on other shelves with CRVs.
6. In the Required Parameters area, leave all fields blank to accept the system default settings.

   Note: See *Overview of DS0 Cross-Connect Parameters* (on page 402) for additional information on these settings.
7. When you are done associating T0 ports, click **OK** to create the associations.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

View CRVs

The procedure below describes how to view all CRV parameters.

To view all CRVs

1. On the Navigation Tree, click the Network level.
2. On the Selection Filter, click **Interface Group** > **GR-303**.
3. In the Work Area, click the **CRV** tab to display the CRVs associated with the interface group.

See *Cross-Connect DS0 Ports to GR-303 Interface Group CRVs* (on page 417) for details on adding CRVs.

See *Delete a CRV to DS0 Cross-Connect* (on page 420) for details on removing CRVs.

Check That It All Works

After the C7 and the switch are configured, service is available. Subscribers can place a voice call.

The following quick checks can confirm that service is available:

- Check there are no alarms in the Alarm Table referring to the interface group you created.
- Check there are no alarms at the switch referring to the interface group you created.
- Check that the EOC and TMC links are up and are on active and standby states respectively.
- Check the service state for each T1 assigned to the interface group is in service and normal.
- Check for dial tone on at least one port of each card that you just assigned a CRV.
- Place a call from one CRV to another CRV that you just assigned.

If service is not available, check DS0 troubleshooting techniques in the *Calix C7 Troubleshooting Guide*.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

View and Modify EOC and TMC Parameters

The procedure below describes how to view and edit the EOC and TMC parameters. This procedure involves the following parameters:

Data Link Profile Access Identifier (ID IG/SAPI): The address of the GR-303 data link profile entity. The access identifier consists of: (Node ID)-(Shelf #)-(IG #)-(SAPI #). Valid parameter values are Node {1-255}-Shelf {1-5}-IG{1-16}-SAPI{0-1}.

Maximum Information Frames (MaxIFrame): Specifies the maximum number of information frames that can be outstanding at Layer 2 using LAPD. Valid values are 1 through 7.

N200: Specifies the maximum number of times a frame can be re-transmitted at Layer 2 using LAPD. Valid parameter values are 1 through 10.

T200: Specifies the maximum length of time in milliseconds that a data link layer entity waits for acknowledgement of a transmitted frame. Valid parameter values are 100, 150, 200, 250, 300, and 350 (milliseconds).

T203: Specifies the maximum time in seconds that a data link remains idle before it verifies the path between the switch and the C7. Valid parameter values are 10 to 300 seconds in intervals of 10 seconds (for example, 10, 20, 30 … 280, 290, 300 seconds).

Parameter values

Your Class 5 switch automatically sets the default data link profile parameters for your GR-303 interface group. In most instances, you should not have to modify these parameters.

To view and modify EOC and TMC parameters

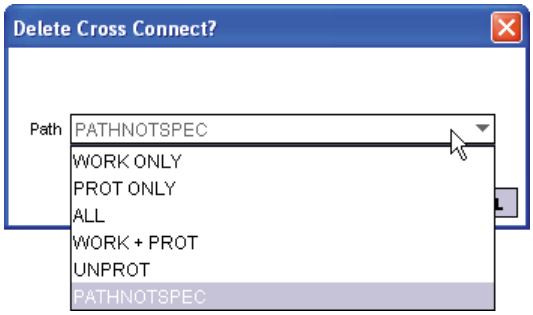
1. On the Navigation Tree, click a GR-303 interface group.
2. In the Work Area, click the **EOC and TMC** tab to view the parameter values for the interface group.
3. In the Edit Row, click a parameter to modify and then select a new parameter value from the list. Modify other parameters as needed.
4. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your configuration settings.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Delete a CRV to DS0 Cross-Connect

To delete a CRV cross-connect

1. On the Navigation Tree, click a GR-303 interface group to select it.
2. In the Work Area, click the **Cross Connects** tab.
3. Click a row to select it.
4. On the toolbar, click **Delete** > **Delete Cross Connects**.
5. In the Delete Cross Connect dialog box:



   a. In the Path list, select the path.

   b. Click **OK**.

Repeat Step 3 through 5 to delete other cross-connections.

Remove DS1 Associations from a GR-303 Interface Group

To remove a DS1 association from a GR-303 interface group

1. On the Navigation Tree, click a GR-303 interface group to select it.
2. In the Work Area, click the **IG-DS1** tab to display the DS1s associated with the interface group.
3. Click a DS1 row to select it, and then click the **Remove** button. In the Delete DS1 Interface Dialog box, click **OK** to confirm the DS1 association removal.

   Note: Select the Force Delete check box if needed to override an existing parameter setting in an attempt to execute the command.

   Note: The system does not allow you to remove all DS1s if there is at least one CRV. The primary or the secondary DS1 must be available.

Repeat Step 3 to remove other DS1 associations.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Remove a GR-303 Interface Group

You cannot remove a GR-303 interface group containing provisioned subtended facilities or CRV associations. If necessary, see the following:

- *Delete a CRV to DS0 Cross-Connect* (on page 420)
- *Remove DS1 Associations from a GR-303 Interface Group* (on page 421)

To remove a GR-303 interface group from the network

1. On the Navigation Tree, click a GR-303 interface group to select it.
2. In the Work Area, click the **Provisioning** tab.
3. On the toolbar, click **Delete**. In the Confirmation dialog box, click **OK** to confirm the removal of the GR-303 interface group.

Maximizing Bandwidth by "Hair-Pinning" T1 Circuits

"Hair-pinning" is a technique used to free up bandwidth for other services on a SONET ring.

Hair-pinning involves wiring Tx and Rx ports on a C7 T1 card (or two T1 cards in the same location) to each other. That is, you wire the Tx connector for port 1 to the Rx connector for port 2, and the Tx connector for port 2 to the Rx connector for port 1. You can use either the T1-6 or T1-6 A+T card.

To set up a hair-pinned connection, you perform these tasks in this order:

- Configure a DS1 port for Hi-Cap service at each end of the circuit—the central office and the remote terminal.
- Create a cross-connection between the central office and remote terminal.
- Create a GR-303 interface group at the remote terminal.
- "Hair-pin" T1 ports at the remote terminal.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring a DS1 Port for Hi-Cap Service

To configure a DS1 port for Hi-Cap service

1. On the Navigation Tree, click a DS1 or T1 card to view the ports, and then click a DS1 port to configure for Hi-Cap service.
2. In the Work Area, click the **Provisioning** tab to view the port parameters.
3. On the Provisioning tab, place the port out of service and set the DS1 type:
   a. In the Primary Service State (PST) list, click **OOS** (Out of Service).
   b. In the DS1 Type list, click **DS1**.
   c. On the toolbar, click **Apply** to place the port out of service. In the Confirmation dialog box, click **OK**.
4. On the Provisioning tab, place the port back in service and set the remaining required parameters:
   a. In the Primary Service State list, click **IS** (In Service).
   b. In the DS1 Format list, click **UF**.
   c. In the Equalization box, type an equalization distance as required for your site.
   d. In the DS1 Line Coding list, select the line coding that matches the signal received at the port.
   e. In the DS1 Mapping list, click **N/A**.
   f. On the toolbar, click **Apply** to place the port back in service. In the Confirmation dialog box, click **OK** to save your changes.

Creating Hi-Cap DS1 Cross-Connections

To create Hi-Cap DS1 cross-connections

1. On the Navigation Tree, click a port where you want to create a T1 cross-connection.
2. In the Work Area, click **Cross Connect**.
3. On the toolbar, click **Create** > **T1 Cross Connect** to open the Select Cross-Connect Endpoints dialog box.
4. In the Source area of the dialog box:
   a. In the Shelf list, select the C7 shelf where the source port is located.
   b. In the Type list, click **T1**.
   c. In the ports list, click the port that is the source for the cross-connection.
   d. Click **SRC** to place the source port in the Cross-Connects To Be Created area.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

5. In the Destination/Drop area:
   a. In the Shelf list, select the shelf where the destination port is located.
   b. In the Type list, click **T1**.
   c. In the ports list, click the port that is the destination for the cross-connection.
   d. Click **DEST** to move the destination port to the Cross-Connects to be Created area.
6. Repeat Steps 4 and 5 for each additional cross-connection you are creating.
7. In the Cross-Connect Way list, accept the default **2WAY**.
8. In the Cross-Connect Path list, select the path type for the cross-connection: Work Only, Protect Only, Working and Protect, or Unprotected.
9. Click **OK** to save the cross-connection.

Completing the Hair-Pinned Circuit

To complete a T1 Hi-Cap hair-pinned circuit, do the following:

- *Create a GR-303 interface group* (on page 408) at the remote terminal.
- Wire together the Tx and Rx ports within a single T1 card or on two T1 cards at the same location. You wire the Tx connector for port 1 to the Rx connector for port 2, and the Tx connector for port 2 to the Rx connector for port 1. To wire together Tx and Rx ports, use jumpers at a cross box or DSX patch panel, or use a special adapter plug designed for that purpose, available from Calix—the DS1/T1 Cross-Connect Module, part number 100-00311 DS1/T1.

DS0 Remote Voice Concentration

The C7 provides DS0 remote voice concentration for GR-303 interface groups to increase transport efficiencies and enable DS0 over-subscription services. The remote voice concentration feature provides a new model for Time Division Multiplexing (TDM) connections between a network interface group and C7 POTS cards. Only active calls are assigned DS0s over the inter-C7 transport links as opposed to the current non-concentrated method where a DS0 is allocated for each provisioned line. This feature removes the 3,168 provisioned POTS lines per C7 shelf limitation and provides 3,168 *active* POTS calls per optical card.

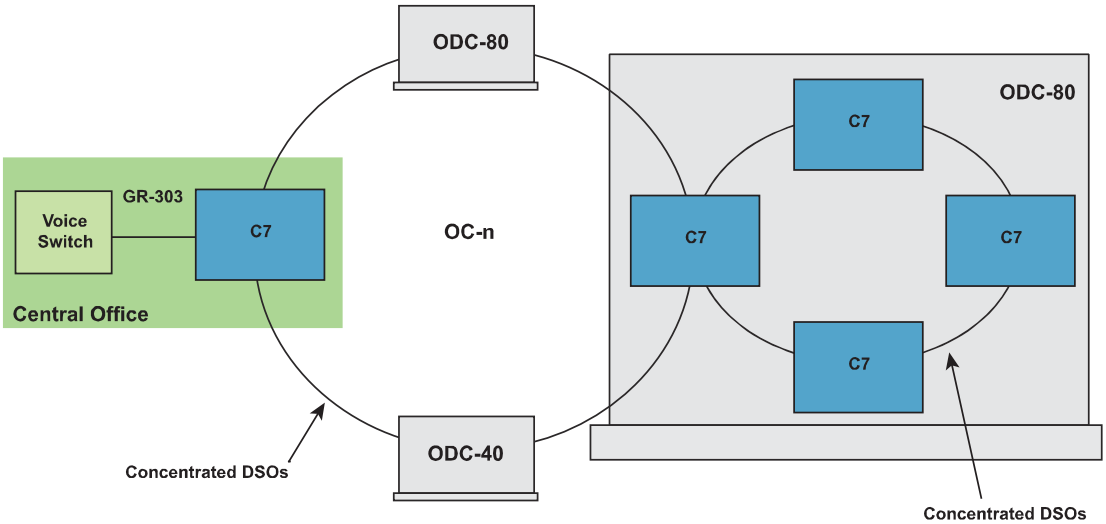
Application benefits

The primary benefits of remote voice concentration include:

- Bandwidth saving relative to the current non-concentrated method over transport links. The typical bandwidth saving is generally equivalent to the voice concentration ratio.
- Bandwidth saving across the C7 backplane on COT shelves.
- Support of up to 3,168 active calls per C7 optical card.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- Eliminates the need for C7 T1-6 cards and physical loopbacks in the remote C7 node that was associated with the hair-pinning technique.
- When delivering voice services, the maximum C7 ring/network size increases from 8 to 16 C7 shelves due to decreases in delay.



Traffic between the remote C7 nodes central office C7 shelves is carried in the C7 internal format with 24 DS0s per TDM VC at 3.392 Mbps, but the DS0s are concentrated.

In the non-concentrated model, subscribers DS0s have specific timeslots within a TDM VC. The non-concentrated transport method continues to be the default mode of system operations.

In the new concentrated model, DS0 timeslots are dynamically assigned within TDM VCs. You define the number of TDM VCs associated with a specific interface group and the concentration ratio is dynamically changed based on the number of TDM VCs. The concentrated model improves transport bandwidth capacity and significantly increases C7 network scalability for delivering voice services.

For the concentrated format, you need to specify the connection from an RT shelf to a particular switch GR-303 interface group to be concentrated, and specify the maximum number of Virtual DS1s (VDS1s) to be used on the transport link. (Note that this assignment has to be done prior to setting any DS0 cross-connects to the C7 shelf). Concentration is determined by the ratio between the maximum number of Virtual DS1s and the number of subscriber lines. The C7 minimizes the number of DS1s used by filling one internal DS1 first before placing DS0s on the next one.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Switch Interfaces, Services, and Transport

DS0 remote voice concentration can be used for connection to GR-303 switch interfaces.

Note: Remote concentration for Voice over IP (VOIP) is described in the *Calix C7 VoIP Services Guide*.

Virtual DS1s used to concentrate the DS0s over the transport links is independent of the number of DS1s forming the GR-303 interface to the switch. The C7 shelf containing the switch interface can provide a second level of concentration and aggregates traffic from multiple RT shelves into the interface group to the external voice switch.

The C7 system allows you to customize concentration ratios to meet your traffic requirements. You associate the shelf to be concentrated to the interface group and specify the number of TDM VCs for the shelf. Each shelf association can have a different number of TDM VCs depending on your preferred concentration ratio. With dynamic timeslot assignments, voice timeslots are only allocated when they are used.

The C7 DS0 remote voice concentration feature can be used with any DS0 service, POTS, and switched specials that use GR-303 voice interfaces. It can be utilized over OC-48, OC-12, OC-3, and DS3 transport links between POTS/switched specials cards. You can configure DS0 voice concentration and non-concentrated voice transport in the C7 network with no impact on system functionality. However, you cannot configure DS0 voice concentration and non-concentrated cross-connections in the same interface group for the same C7 shelf.

Traffic from a T1 Transport Group (T1TG) can be combined in the same interface with concentrated POTS and Voice Gateway Processor (VGP) traffic.

Topologies

DS0 remote voice concentration supports the following topologies:

- C7 shelves from a single C7 node or different nodes can use a single switch interface group.
- Traffic into a single switch interface group can be a mix of concentrated traffic from some C7 shelves and non-concentrated from other C7 shelves. For example, if the C7 network has a mix of large and small nodes, you have the option to only concentrate the traffic from larger nodes and not concentrate traffic from the smaller nodes and still share a common switch interface between them.
- For applications that contain FTTP, the Voice Gateway Processor (VGP) can be remotely located or centrally located. In either case, FTTP traffic can be mixed with concentrated DS0 voice traffic into a single switch interface group. Note that the FTTP traffic does not use the concentration shelf TDM VCs.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- There is no additional signal processing delay associated with concentration, therefore the size of a C7 network carrying POTS is the same as the non-concentrated case—a maximum of 16 shelves from the shelf containing the POTS interface to the shelf containing the switch interface group.

Bandwidth, Capacity, and Operational Elements

Each internal DS1 occupies 3.392 Mbps and carries 24 concentrated DS0s. The traffic is carried as concentrated through the C7 shelf and therefore uses less of the backplane packet capacity.

The maximum number of POTS lines per C7 shelf is 11,712. Any part or all of this capacity can be supported on a single fiber ring. The maximum capacity of a SONET ring, or multiple rings on a single card (for example, on an OC-12 card) is 11,712 lines and 3,168 concentrated DS0s (132 Virtual DS1s).

In a mix of concentrated and non-concentrated configurations, the 132 Virtual DS1s are used in two ways:

- In the concentrated mode, each VDS1 comprises 24 concentrated DS0s.
- In the non-concentrated mode, each internal DS1 supports 24 lines.

The link capacity is the sum of the two.

Managing concentrated links

To manage concentrated links the following functions are supported:

- Traffic statistics, including per shelf concentration statistics, are provided to determine the number of Virtual DS1s required per shelf.
- Packet statistics to show the minimum and maximum range of UBR traffic available with voice concentration.
- Ability to increase or decrease the number of Virtual DS1s provisioned to a particular C7 shelf.
- Bandwidth use monitoring: The system raises a minor traffic capacity alarm when a pre-set percentage of link utilization is exceeded. You can provision this parameter.

Configuring Remote Voice Concentration

Concentrated and non-concentrated modes

You cannot configure DS0 voice concentration and non-concentrated cross-connections in the same interface group for the same C7 shelf. An interface group can have mixed (concentrated and non-concentrated) modes to different shelves. A shelf can have different modes back to various interface groups.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

You cannot assign a Voice Concentration Shelf to an interface group when the interface group has pre-existing cross-connections to that shelf. The system provides two methods of reprovisioning existing DS0 cross-connections in a GR-303 interface group:

- Bulk Reprovisioner tool
- Reprovision check box in the Voice Concentration Shelf dialog box

Use the Reprovision DS0s check box in the Voice Concentration Shelf dialog box to reprovision existing DS0 cross-connections in the interface group. If you select this option, the system deletes the existing DS0 cross-connects and reprovisions the cross-connects after the Voice Concentration Shelf is created. Voice services are not available for the affected DS0 cross-connects during the reprovisioning process.

Number of VDS1s (TDM VCs) and the concentration ratio

The number of Virtual DS1s (VDS1s) in conjunction with concentration ratio is calculated in the following manner:

```
Number TDM VCs = (DS0s in shelf / 24) / ratio desired
```

Note: If result is not a whole number, round up to nearest whole number.

Shown below are two examples of the calculation.

Assuming that you want to set a concentration ratio of 4:1 and you have 96 DS0s in the RT, the formula produces:

```
(96 / 24) / 4 = 1 VDS1
```

Assuming you want to set a concentration ratio of 4:1 and you have 97 DS0s in the RT, the formula produces:

```
(97 / 24) / 4 = 1.01 rounded up to 2 VDS1s
```

Note: VDS1s (TDM VCs) are not created at this point--VDS1s specified for the remote C7 shelf are created when the DS0 cross-connections are configured in the remote shelf.

Configuration process flow

To configure remote voice concentration, you must complete the following tasks:

- Create a GR-303 interface group. See *Create a GR-303 Interface Group* (on page 408).
- Assign IG-DS1s to the interface group. See *Assign T1 Ports to a GR-303 Interface Group* (on page 412).
- Create the Voice Concentration Shelf. See *Creating a Voice Concentration Shelf* (on page 414).

  Note: Convert existing CRVs if needed. See *Converting Existing CRVs* (on page 429).

- Provision DS0 cross-connections in the remote shelf. For instructions, see *Configuring GR-303 Services* (on page 404).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

You associate the shelf to be concentrated to the interface group and specify the number of Virtual DS1s (TDM VCs) for the shelf. Each shelf association can have a different number of TDM VCs depending on your preferred concentration ratio.

For additional information on provisioning DS0 cross-connections, see *Provisioning DS0 Services (on page 397)*.

Converting Existing CRVs

The C7 system provides two methods for converting existing CRVs prior to setting up a Remote Voice Concentration shelf. You can use the Reprovision DS0s check box or the Bulk Reprovisioner tool.

Reprovision DS0s check box (Method 1)

Use the Reprovision check box in the Voice Concentration Shelf dialog box as another method if you want to reprovision existing DS0 cross-connects within the selected interface group to the Voice Concentration Shelf. If selected, the system deletes the existing DS0 cross-connects and reprovisions the cross-connects after the Voice Concentration Shelf is created. See *Creating a Voice Concentration Shelf* (on page 414) for additional information.

Bulk Reprovisioner tool (Method 2)

The Bulk Reprovisioner tool conversion method consists of the following tasks:

- Cut (delete) all CRVs terminating on the C7 shelf that need to be converted for use by the remote voice concentration method. See the *Calix C7 Maintenance Guide* for detailed instructions.
- Create the Voice Concentration shelf. This should be the shelf where the Bulk Reprovisioner tool was used to delete the cross-connections. Specify the number of VDS1s. See *Creating a Voice Concentration Shelf* (on page 414) for information on setting up and configuring a Voice Concentration shelf.
- Use the Bulk Reprovisioner tool to paste (add) the CRVs back to the shelf. See the *Calix C7 Maintenance Guide* for detailed instructions.
- Verify that only the maximum number of TDM VCs was set up.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

To cut (delete) CRVs terminating on the C7 shelf

See the *Calix C7 Maintenance Guide* for detailed instructions on creating and using a Bulk Provisioning task.

1. On the Navigation Tree, click the shelf, card, or port that contains the source endpoints of the cross-connections to reprovision.
2. Open the Bulk Provisioning Task dialog box and name the task:
   a. On the toolbar, click **Tools** > **Bulk Reprovisioner** > **Create Task**.
   b. In the Warning dialog box, click **OK**.
   c. Optional) In the Task Name box, type a name. By default, the current date and time appear in the box.
   d. Click **OK**.
3. In the Filters pane, set the filters to use for retrieving cross-connections:
   a. Click the **T0** check box to indicate the type of cross-connections to retrieve.
   b. (Optional) To set each cross-connection parameter filter, click the Ellipsis button to the right of the filter box to open the Select Items dialog box.
   c. Use Ctrl+click to select up to five available parameter values to include in the filter, and then click **OK**.
   d. The values you selected are displayed in the filter box. Multiple values are separated by commas. If all values are not in view, place your cursor over the filter box to view them in a ToolTip, or click inside the filter box and use your arrow keys to scroll through the list.
4. Click **Retrieve**.

   Cross-connection retrieval may take several minutes, during which time the message **`"Getting cross-connects"`** appears in the Log pane. The message **`"Done receiving cross-connects"`** indicates that the retrieval is complete. If you need to stop a retrieval that is in progress, click **Stop**.
5. In the Cross-Connects pane, click the **T0** tab.
6. Do one of the following:
   - Select the cross-connections to include, and then click **Toggle Cut/Paste**. To select a range of cross-connections, click in the Status (St) column of the first row, and then Shift+click the last row in the range. To select individual rows, Ctrl+click each row to include.
   - Select individual **C&P** (Cut and Paste) check boxes to include specific cross-connections.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

7. Click **Start** to begin the bulk reprovisioning task.

   The task takes several minutes to complete. During this time, the colored shapes in the Status (St) column change as each cross-connection gets updated.

Note: Create the Voice Concentration Shelf and then proceed to the next procedure to paste (add) the CRVs back to the shelf. See *Creating a Voice Concentration Shelf* (on page 414) for information on setting up and configuring a Voice Concentration shelf.

To paste (add) the CRVs back to the C7 shelf

1. Open the existing bulk reprovisioning task.
2. In the Cross-Connects pane, click the **T0** tab.
3. Select the cross-connections to include.

   Note: Select the T0 cross-connections that were deleted in the initial procedure used to "cut" the CRVs terminating on the C7 shelf. They are indicated by a black square in the Status (St) column.

4. Click **Start** to begin the bulk reprovisioning task.

   The task takes several minutes to complete. During this time, the colored shapes in the Status (St) column change as each cross-connection gets updated.

Verify TDM VCS

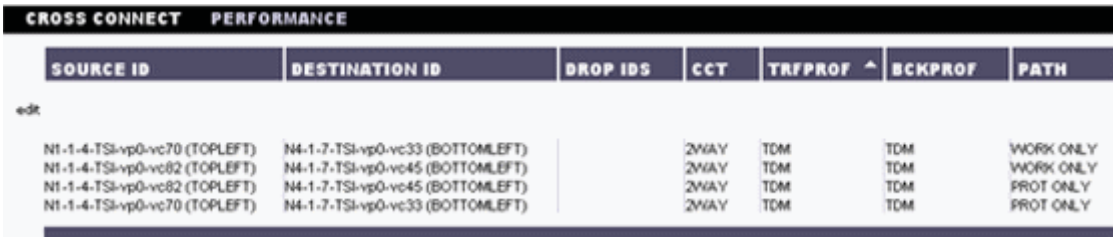
Use the following procedure to verify that only the maximum number of TDM VCs was set up.

To verify the maximum number of TDM VCs

1. On the Navigation Tree, click the Shelf level.
2. In the Selection Filter, click **Cross-Connect** > **Virtual Circuit** to open the Cross-Connect Filter dialog box.
3. In the Cross-Connect Filter dialog box, click the **Values** button associated with the ATM Traffic Profile ID field to open the Filter Values dialog box.
4. In the Filter Values dialog box, select the **TDM (TDM)** check box. Click **OK**.
5. In the Cross-Connect Filter dialog box, click **OK**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

6. In the Work Area, verify the TDM VCs.



Viewing DS0 Voice Concentration PM

Traffic Performance Monitoring (PM) parameters

- **PSTARTTIME** – Peak Start Time. The time at the start of the peak hour. Traffic statistics are gathered in one-hour segments from the time the counters are reset.
- **PTRAF** – Peak Hour Traffic. The amount of traffic carried during the peak traffic hour. Traffic for each hour is measured in Centa Call Seconds (CCS). Centa Call Seconds are used to indicate the number of seconds of telecommunications traffic, in an hour. One Centa Call Second is 100 seconds of utilization. The peak traffic hour data is reset when the traffic counters are reset.
- **PBUSY** – Peak Hour All Circuits Busy. The number of seconds that all circuits were busy during the peak traffic hour.
- **PORIG** – Peak Hour Originations. The number of originations from the subscriber end in the peak traffic hour.
- **PTERM** – Peak Hour Terminations. The number of calls terminating on a local subscriber in the peak traffic hour.
- **PBORIG** – Peak Hour Blocked Originations. The number of calls not started by a local subscriber because all circuits were busy during the peak traffic hour.
- **PBTERM** – Peak Hour Blocked Terminations. The number of calls unable to terminate on a local subscriber because all circuits were busy during the peak traffic hour.
- **TSTARTDAY** – Total Start Day. The day that the traffic counters were last reset.
- **TSTARTTIME** – Total Start Time. The time that the traffic counters were last reset.
- **TTRAF** – Total Traffic. The total amount of traffic since the counters were last reset. The measurement is provided in Centa Call Seconds. One Centa Call Second is 100 seconds of circuit utilization.
- **TBUSY** – Total All Circuits Busy. The number of seconds that all circuits were busy since the counters were last reset.
- **TORIG** – Total Originations. The number of originations from the subscriber end since the counters were last reset.
- **TTERM** – Total Terminations. The number of calls terminating on a local subscriber since the counters were last reset.
- **TBORIG** – Total Blocked Originations The number of calls not started by a local subscriber because all circuits were busy since the counters were last reset.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- **TBTERM** – Total Blocked Terminations The number of calls unable to terminate on a local subscriber because all circuits were busy since the counters were last reset.

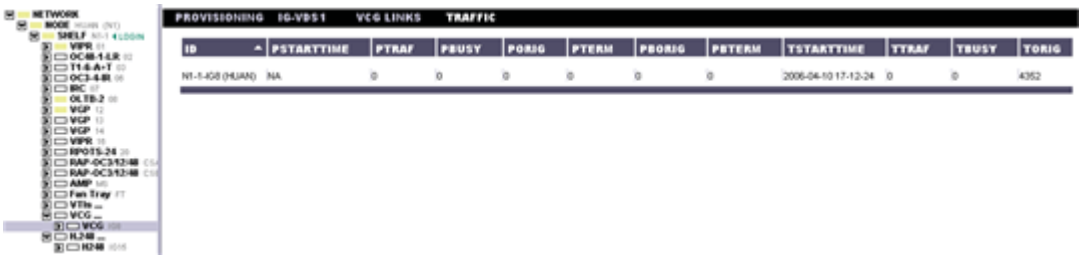
Viewing call processing and voice concentration statistics

Use the procedure below to retrieve and display call processing and concentration statistics.

To view call processing and voice concentration statistics

1. On the Navigation Tree, select an interface group.
2. In the Work Area, click the **Traffic** tab to display the traffic statistics.

Note: Voice concentration shelves must be configured to generate traffic data for statistics.



Removing a Voice Concentration Shelf

The system allows you to switch from a concentrated model back to a non-concentrated model.

To remove a Voice Concentration Shelf and revert to a non-concentrated model

1. Delete T0 cross-connections in the shelf switching from the new concentration model to the non-concentrated model. See *View a List of Cross-Connections and Hops* (on page 126) and *Delete Cross-Connects and Hops* (on page 134).
2. Delete the associated voice concentration shelf from the network interface group:
   a. On the Navigation Tree, click the interface group (for example GR-303).
   b. In the Work Area, click the **Voice Conc Shelves** tab.
   c. Click the voice concentration shelf (row) to delete.
   d. On the toolbar, click **Delete**.
   e. In the Confirmation dialog box, click **OK** to confirm the deletion.
3. Recreate the deleted DS0s cross-connections from Step 1 using the non-concentrated model. See *Configuring GR-303 Services* (on page 404) and *Cross-Connect DS0 Ports to GR-303 Interface Group CRVs* (on page 417).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

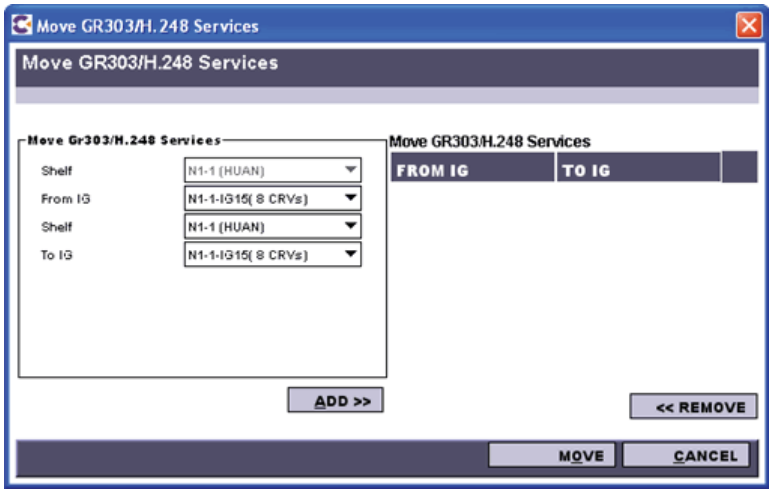
Moving GR-303 Services

The C7 system provides a method of moving GR-303 interface groups from one C7 shelf to another C7 shelf. Typically, interface groups are moved from a remote shelf to a new interface group located on a centrally located shelf. If you are using a new destination interface group, make sure you have created the interface group prior to running the "Move GR-303 Services" procedure.

ALERT! Moving GR-303 services is a service-affecting operation. Services are not available while the system deletes and reprovisions the interface groups.

To move GR-303 services

1. On the Navigation Tree, click a GR-303 interface group.
2. In the Work Area, click the **Voice Conc Shelves** tab.
3. From the toolbar, click **Action** > **Move GR303/H.248 Services** to open the Move GR303/H.248 Services dialog box.



4. In the Move GR303/H.248 Services area, do the following:
   a. In the upper Shelf list, select the shelf that contains the source interface group.
   b. In the From IG list, select the interface group to move.
   c. In the lower Shelf list, select the destination shelf.
   d. In the To IG list, select the destination interface group.

Note: This is typically a new interface group.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

5. Click **Add** to move the From IG and To IG information to the Move GR303/H.248 Services area.

   Note: If you are moving cross-connections from the remote interface group to an existing interface group, they must not have any overlap in CRV numbers.

6. Click **Move**. In the Confirmation dialog box, click **OK** to confirm the move.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring GR-57 Services

Quick GR-57 Service Configuration Process

Use the Quick GR-57 Services Configuration Process to get DS0 service up and running using standard Calix recommendations suitable for most situations.

Note: You can have up to 15 shelf-based interface groups per C7 shelf, including voice concentration groups, GR-303 interface groups, H.248 interface groups, and T1 transport groups. See *GR-8 Interface Group Configuration Rules* (on page 440) for GR-8 slot-based interface groups.

Services covered

This quick start covers configuring host DS0 ports for a GR-57 interface and remote DS0 ports for POTS and EBS service. Configuration parameters for Coin and UVG service are also presented.

Starting point

Before starting this Quick GR-57 Switched Services Configuration Process, check the following conditions are met:

- Transport is configured.
- Remote DS0 service cards are installed and wired.
- Host DS0 service cards are installed and wired to a GR-57 switch interface.

Information you need

You need to have the following information on-hand to complete GR-57 provisioning.

- Transmission level and impedance values for the GR-57 switch interface.
- Transmission level and impedance values for any DS0 services that you plan to configure.

Quick GR-57 configuration process flow

1. Configure host DS0 ports for GR-57 interface.
2. Configure remote DS0 ports for service.
3. Cross-connect DS0 ports.
4. Check that it all works.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configure DS0 Ports for GR-57 Interface

Host DS0 ports provide a GR-57 switch interface for DS0 services. Remote DS0 ports provide a subscriber interface for DS0 services. You configure the host ports for the type of service connected to the switch, and the remote ports for the type of DS0 service delivered.

Configuring host and remote DS0 ports services

Ports on host and remote DS0 equipment can be configured for many DS0 switched services:

- POTS service for ports on HPOTS-24 and HU2W-24 host cards and RPOTS-24 and RU2W-24 remote cards.
- Coin service on the first four ports of the HU2W-24 host card and the first four ports of the RU2W-24 remote card. Set the GSFN parameter to 2COIN.
- UVG service on DS0 ports on the HPOTS-24 and HU2W-24 host cards and RPOTS-24 and RU2W-24 remote cards. Set the GSFN parameter to a UVG service type.
- EBS service on the HEBS-12 host card and REBS-12 remote card. Port parameters on an HEBS-12 and REBS-12 cards are set for EBS service.

See *Overview of DS0 Port Parameters* (on page 398) for additional information on GSFN parameters.

Setting DS0 Port Parameters

To set DS0 port parameters

1. On the Navigation Tree, click a C7 shelf containing DS0 ports.
2. On the Selection Filter, click **Port** > **DS0 Port** to view all DS0 ports from the selected shelf in the Work Area.
3. In the **Provisioning** Work Area, click the first DS0 port to configure, and then Shift+click the last DS0 port to select a range of ports to configure.
4. Place the ports out of service and set the following DS0 parameters:
   a. In the PST (Primary Service State) list, click **OOS** (Out of Service).
   b. In the GSFN (General Signaling Function) list, select a signal type.
   c. In the Receive Transmission Level Point list, select a decibel value.
   d. In the TTLP (Transmit Transmission Level Point) list, select a decibel value.
   e. In the Impedance list, click an impedance of **600** or **900** ohms.
   f. On the toolbar, click **Apply** to place the ports out of service and apply the DS0 port parameters. In the Confirmation dialog box, click **OK** to save the DS0 port configuration.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

5. Re-select the same range of ports to configure as selected in Step 3, and place them back in service:
   a. In the PST list, click **IS** (In Service).
   b. On the toolbar, click **Apply** to place the ports back in service. In the Confirmation dialog box, click **OK**.

If you have just set DS0 host port parameters, repeat Steps 1 through 5 for the corresponding remote ports.

Cross-Connect Host, Remote DS0 Ports (GR-57)

To establish GR-57 universal service, cross-connect the remote DS0 service ports to the host (office) DS0 ports providing the GR-57 switch interface. If you are not configuring subscriber service for GR-57, skip this section.

Cross-connection guidelines for GR-57 service

Follow these guidelines when cross-connecting DS0 ports:

- Specify the host (office) DS0 ports as the Source endpoints of the T0 cross-connects.
- Specify the remote DS0 ports as the Destination endpoints of the T0 cross-connects.
- Specify an equal number of Source and Destination DS0 ports to cross-connect.

To create a DS0 cross-connection

1. From the File menu, click:
   - (in iMS) **Create** > **Cross-Connect** > **T0**
   - (in CMS) **Create** > **C7** > **Cross-Connect** > **T0**
2. In the Select Cross-Connect Endpoints dialog box, Source area:
   a. In the Shelf list, select a C7 shelf where source remote DS0 ports are located.
   b. In the Type list, click **T0** (default).
   c. In the Slot list, select the slot containing the remote card.
   d. In the ports list, use Ctrl+click to select the DS0 ports for the sources of the cross-connections.
   e. Click **SRC** to place the ports in the Cross-Connects To Be Created area.
3. In the Destination area:
   a. In the Shelf list, select the shelf where the destination host DS0 ports are located.
   b. In the Type list, click **T0** (default).
   c. In the Slot list, select the slot containing the host card.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

d. In the ports list, use Ctrl+click to select the DS0 ports for the destinations of the cross-connections.

Note: The number of ports you select must match the number of ports you specified in Step 2d.

e. Click **DEST** to place the ports in the Cross-Connects To Be Created area.

4. If you are configuring service over fiber transport, go to Step 5.

   If you are configuring service on a TO-6 card using T1 transport, in the IDT Route area do the following:

   a. In the Cross-Connects To Be Created area, select all of the T0 ports.

   b. In the Shelf list, select the shelf with the IDT interface for the T1 Transport Group.

   c. In the T1TG list, select the T1 Transport Group configured as the IDT interface.

   d. Click **IDT** to add the selected T1TG to the IDT column in the Cross-Connects To Be Created area.

5. In the Required Parameters area:

   a. In the Cross-Connect Way list, click **2WAY**.

   b. For the remaining parameters, accept the defaults.

   Note: See *Overview of DS0 Cross-Connect Parameters* (on page 402) for additional information for these settings.

6. Click **OK** to create the cross-connections.

Check That It All Works

After the C7 and the switch are configured, service is available. Subscribers can place a voice call.

The following quick checks can confirm that service is available:

- Check there are no alarms at the switch referring to the host interfaces you created.
- Check for dial tone on at least one port of each remote card that you configured.
- Place a call from one remote DS0 port to another remote DS0 port that you configured.

If service is not available, check DS0 troubleshooting techniques in the *Calix C7 Troubleshooting Guide*.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring GR-8 Services

Quick GR-8 Configuration Process

This quick start covers configuring a T1 port for a GR-8 interface and cross connecting DS0 ports for universal switched services.

Use the Quick GR-8 Configuration Process to get GR-8 service up and running using standard Calix recommendations suitable for most situations.

Starting point

Before starting this Quick GR-8 Configuration Process, verify that the following conditions are met:

- Transport is configured.
- Remote DS0 service cards are installed and wired.
- DS1 network interface cards are installed and wired to a GR-8 switch interface.
- DS0 ports must be configured prior to creating a cross-connection from the remote DS0 port to the GR-8 interface group. You must know the line build out distance from the C7 to the switch, and the transmission level and impedance values for services you plan to configure.

Quick GR-8 configuration process flow

1. Create a GR-8 interface group.
2. Configure a T1 port for a GR-8 switch interface.
3. Assign a T1 port to a GR-8 interface group.
4. Create cross-connections from DS0 ports to an interface group.
5. Check that it all works.

Create a GR-8 Interface Group

Using GR-8 interface groups, you can configure the C7 system to function as a GR-8 interface to the switch. GR-8 interface groups can be configured to support non-concentrated calls (Mode I) or 2:1 concentrated calls (Mode II).

GR-8 Interface Group Configuration Rules

The following rules apply to configuring GR-8 interface groups on the C7:

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- You can create a maximum of six GR-8 interface groups on a single T1 card, and a maximum of 120 GR-8 interface groups on a C7 shelf (assuming all cards on the shelf are T1 cards).
- A GR-8 interface group can consist of ports on only one T1 card. It cannot include ports from multiple cards.
- If T1 transport is not used between C7 shelves, the maximum number of fiber links between the remote endpoint of a subscriber channel and its GR-8 T1 is 15.
- If T1 transport is used between C7 shelves, the maximum number of fiber links is 10.
- DS1 ports must be configured for GR-8 service before they can be assigned to an interface group.
- A T1 transport group IDT and a GR-8 interface group that uses it to connect to its subscribers cannot have their T1 lines intermixed on the T1 cards.
- If the DS1-12 PWE, T1-6, T1-6 A+T, or T1-8 PWE card is protected, provision Equipment Protection Switching before creating GR-8 interface groups.

Note: The GR-8 slot-based interface groups do not affect the number of shelf-based interface groups permitted in a C7 shelf. In addition to GR-8 interface groups, you can have up to 15 shelf-based interface groups per C7 shelf, including voice concentration groups, GR-303 interface groups, H.248 interface groups, and T1 transport groups.

Creating the GR-8 Interface Group

GR-8 interface group parameters

You can provision the following parameters for a GR-8 interface group:

Parameter	Definition	Valid Options	Default Value
Shelves	C7 shelf to host the GR-8 interface group.	Any shelf in the network	Selected shelf
GR8 Cards	T1 card to host the GR-8 interface group.	Any T1 card in the shelf	T1 card in lowest-numbered slot
New GR8 Address (ID)	System address of the GR-8 interface group to create.	Any unused IG numbers per slot (1–6)	Next available IG number on slot
Switch Type (SWITCHTYPE)	Specifies the type of switch that the GR-8 interface group shall connect to.	5ESS, DMS100, DMS10, EWSD, GTD5	DMS100
Mode Type (GR8TYPE)	Type of timeslot allocation. Mode 1 is unconcentrated, Mode 2 is concentrated (2:1).	Mode1 Mode2	Mode2
Alarm Bits (ALARMBITS)	Specifies the number of alarm bits used by the switch. Varies by mode type.	13 (Mode 1) 16 (Mode 2)	16

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

To create a GR-8 interface group

1. On the Navigation Tree, click the C7 shelf to host the interface group.
2. On the File menu, click:
   - (in iMS) **Create** > **Interface Group** > **GR8** > **GR8 Interface Group**
   - (in CMS) **Create** > **C7** > **Interface Group** > **GR8** > **GR8 Interface Group**
3. In the Create New GR8 dialog box:
   a. In the Shelves list, select the shelf that contains the T1 interface to the switch.
   b. In the GR8 Cards list, select the T1 card (slot) to host GR-8 interface group.
   c. In the New GR8 Address list, accept the default, or select the new GR-8 interface group number.
   d. In the Switch Type list, select the type of Class 5 switch to which the GR-8 group connects.
   e. In the Mode Type list, click **Mode 1** or **Mode 2**.

   Note: For FTTP support, select **Mode 2** operation only.

   f. In the Alarm Bits list, click **13** or **16** (13- or 16-bit alarm).
4. Click **OK** to create the GR-8 interface group.

View Attributes of a GR-8 Interface Group

After creating a GR-8 interface group, you can view its attributes. The settings below can be viewed, but not modified.

GR-8 Interface Group (ID)

Indicates the address of the GR-8 interface group, consisting of:
`Node(1-255)-Shelf(1-5)-Slot(1-20)-Interface Group(1-6)`.

GR-8 Mode Type (GR8TYPE)

The mode, or type of timeslot allocation, for the GR-8 interface group. Mode 1 indicates a non-concentrated interface. Mode 2 indicates an interface with 2:1 concentration.

Alarm Bits (ALMBITS)

The number of alarm bits (13 or 16) used by the switch.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

To view GR-8 interface group attributes

1. To view a single GR-8 interface group, do the following:
   a. On the Navigation Tree, expand the C7 shelf and click an interface group.
   b. In the Work Area, click the **Provisioning** tab to view the interface group parameters.
2. To view multiple GR-8 interface groups on a shelf, do the following:
   a. On the Navigation Tree, click the C7 shelf containing the GR-8 interface groups.
   b. On the Selection Filter, click **Interface Group** > **GR-8**.

Configure a T1 Port for a GR-8 Switch Interface

DS1 facilities provide the links to the switch for GR-8 integrated interfaces. You can use the following DS1 cards for switch interface service:

- DS1-12 PWE
- T1-6
- T1-6 A+T
- T1-8 PWE

You can configure the DS1 ports for either a DS1 or T1 signal type as required for your application. Typically, DS1 ports in a central office shelf connect to the switch using the DS1 signal type. Before continuing, verify that the T1 cards are installed and wired out to the switch. Refer to the *Calix C7 Installation Guide* for installations instructions.

Configuration guidelines for DS1 switch interface ports

Follow these guidelines when configuring DS1 ports to provide a switch interface:

- You can configure up to 2 DS1 ports to serve a GR-8 interface group operating in Mode II; both ports must reside on the same T1 card.
- You must configure DS1 ports for service before assigning them to an interface group.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

T1 port parameters

You can provision the following parameters for T1 ports providing switch interface links.

Parameter	Value
DS1 Format	SF
DS1 Line Coding	B8ZS or AMI
DS1 Map	SEQ
DS1 Type	DS1 or T1
Timing Mode	Source
If DS1 Type = DS1	
Equalization	Distance to switch
If DS1 Type = T1	
DS1 Power	Sink (default) or Source Set per your site requirement.
DS1 Attenuation	0.0 dB (default) or –7.5, –15.0, –22.5 dB Set per your site requirement.

To configure a T1 port for a GR-8 switch interface

1. On the Navigation Tree, click a C7 shelf containing a GR-8 interface group and assigned T1 ports.
2. On the Selection Filter, click **Port** > **DS1/T1 Port** to view all DS1 ports from the selected shelf in the Work Area.
3. In the Work Area, use Ctrl+click to select the T1 ports to configure.

   Tip: You can configure T1 ports for use in multiple GR-8 interface groups at the same time.

4. In the Edit Row, place the DS1 ports out of service and set the DS1 Type:
   a. In the PST (Primary Service State) list, click **OOS** (Out of Service).
   b. In the DS1TYPE (DS1 Type) list, click **DS1** or **T1**.
   c. On the toolbar, click **Apply** to apply the DS1 Type and to place the ports out of service. In the Confirmation dialog box, click **OK** to display parameters for a DS1 signal type.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

5. Re-select the same T1 ports that you selected in Step 3, and modify the following parameters in the Edit Row:
   a. In the FMT (DS1 Format) list, click **SF** (Super Frame).
   b. (For DS1 ports only) In the EQLZ (Equalization) box, type the distance in feet from the C7 to the switch.
   c. In the LINECDE (DS1 Line Coding) list, click **AMI**.
   d. (For T1 ports only) Change the power and attenuation settings per your site requirements.
   e. In the DS1MAP (DS1 Map) list, click **SEQ**.
   f. In the TMGMODE (Timing Mode) list, click **Source**.
   g. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to display parameters for a DS1 signal type.
6. Re-select the same T1 ports you selected in Steps 3, and place the ports in service:
   a. In the Edit Row, set the PST (Primary Service State) to **IS** (In Service).
   b. On the toolbar, click **Apply** to update the settings and place the ports back in service. In the Confirmation dialog box, click **OK** to save your configuration settings.

Assign T1 Ports to a GR-8 Interface Group

After configuring T1 ports, you can assign up to four T1 ports for Mode 1, or two T1 ports for Mode 2, to a GR-8 interface group.

Prior to assigning T1 ports to a GR-8 interface group

The following rules apply when assigning T1 ports to a GR-8 interface group:

- All T1 ports assigned to an interface group must be on the same T1 card.
- T1 ports must be configured for use in a GR-8 interface group before you assign them to an interface group.
- DS1 identifiers for a GR-8 interface group must match span letters configured at the switch. In GR-8 Mode 1, you assign T1 ports to spans A, B, C, and D. In Mode 2, you assign T1 ports to spans AB and CD.
- Once assigned to an interface group, DS1s cannot be edited without removing them from the interface group and reassigning them.

To assign T1 ports to a GR-8 interface group

1. On the File menu, click:
   - (in iMS) **Create** > **Interface Group** > **GR8** > **GR8 Interface Group DS1**
   - (in CMS) **Create** > **C7** > **Interface Group** > **GR8** > **GR8 Interface Group DS1**

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

2. In the Interface Group DS1 dialog box:
   a. In the Shelf list, select a C7 shelf hosting the GR-8 interface group.
   b. In the Interface Group list, select the GR-8 interface group to receive DS1 assignments.
   c. In the list of available T1 ports, click the DS1 port(s) to assign to the GR-8 interface group.

   Note: The order in which you select ports determines the DS1 link identifier (A, B, C, and D in GR-8 Mode 1; AB, CD in Mode 2) for the interface group.

   d. Click **Add** to place the T1 port in the T1 Ports To Be Added As IG-DS1 area.
3. When you are done adding ports, click **OK** to create the IG-DS1 assignments.

View GR-8 Interface Group DS1s

After you configure T1 ports and assign them to a GR-8 interface group, you can view the DS1 identification parameters by completing the procedure below.

DS1 Access Identifier (ID)

The address of the DS1 line termination, also referred to as the DS1 number or span, in the GR-8 interface group, consists of Node(1–255)-Shelf(1–5)-Slot(1–20)-Interface Group(1–6)-DS1(A, B, C, D, AB, or CD). For GR-8 Mode 1, the DS1 can be A, B, C, or D. For Mode 2, the DS1 can be AB or CD.

DS1 Port Access Identifier (DS1 IG)

The DS1 port access identifier consists of Node(1–255)-Shelf(1–5)-Slot(1–20)-Port ID(1–6).

Service State (SVCSTATE)

This parameter specifies the service state of the DS1 port.

To view DS1s assigned to GR-8 interface groups

1. On the Navigation Tree, expand the C7 shelf and click a GR-8 interface group.
2. In the Work Area, click the **IG-DS1** tab to view the DS1s.
3. To view multiple GR-8 interface groups on a shelf, do the following:
   - On the Navigation Tree, click the shelf containing the GR-8 interface groups.
   - On the Selection Filter, click **Interface Group** > **GR-8**.
   - In the Work Area, click the **IG-DS1** tab to view the DS1s.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Cross-Connect DS0 Ports to a GR-8 Interface Group

GR-8 interface groups support DS0 services configured on RPOTS-24, RU2W-24, and COMBO cards.

Prior to cross-connecting DS0 ports to a GR-8 interface group

The following configuration rules apply to cross-connecting DS0 ports to a GR-8 interface group:

- You must provision the DS0 ports before cross-connecting them to a GR-8 interface group.

  See also:

  - *Configure Remote Ports for Universal POTS and UVG Services* (on page 452)
  - *Configure Ports for Coin Service* (on page 454)
- Once a cross-connection has been added to a GR-8 interface group, you cannot modify the General Signaling Function (GSFn) parameter without deleting and rebuilding the cross-connect.
- You can add cross connections to a GR-8 interface group as long as you do not exceed the maximum number of channels for the interface group.

Maximum number of channels for GR-8 interface groups

The following table shows how many cross-connections you can make based on the number of T1 ports associated with your GR-8 interface group:

GR-8 Mode	DS1 Spans in Interface Group	Maximum Number of Cross Connects
Mode 1	A	24
Mode 1	A and B	48
Mode 1	A, B, and C	72
Mode 1	A, B, C, and D	96
Mode 2	AB	48
Mode 2	AB and CD	96

Note: In this procedure, the number of DS0 ports and channels must match (see Step 6); otherwise no cross-connections are made.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

To cross-connect DS0 ports to GR-8 interface group

1. On the Navigation Tree, click a GR-8 interface group.
2. In the Work Area, click **Channel**.
3. On the toolbar, click **Create** > **T0 Cross Connect** to open the Select Cross-Connect Endpoints dialog box.
4. In the Source area of the dialog box:
   a. In the Shelf list, select the shelf containing the GR-8 interface group.
   b. In the Type list, click **CRV/Channel/Line**.
   c. In the GR303/08/H248 list, select the interface group.
   d. In the CRV/Channel/Line box, type a range of integers using a dash between integers (for example, 1-24), or type an integer, to specify the channel number(s) for the destination DS0 ports.

   Note: You cannot reuse channel numbers that have already been assigned to the GR-8 interface group.

   e. Click **SRC** to list the channels in ascending numeric order in the Cross-connections to be created list under the Source column.
5. In the Destination area:
   a. In the Shelf list, select a shelf containing a remote DS0 card.
   b. In the Type list, click **T0**.
   c. In the Slot list, select the slot occupied by the DS0 card.
   d. In the list of DS0 ports, select available ports. Use Ctrl+click to select ports one at a time, or Shift+click to select a range of ports. Destination ports are assigned in ascending order to the channels selected in Step 4.
   e. Click **DEST** to assign the selected ports to the source channels.
   f. Repeat Step 5 until you have selected the DS0 ports to cross-connect to the interface group.
6. In the Cross-Connects To Be Created list, scroll to the bottom of the list to make sure that the number of channels under the Source column matches the number of DS0 ports under the Destination column.
   - To add DS0 ports and channels, repeat Steps 4 and 5.
   - To remove rows from the list, highlight one or more rows, and then click **Remove**.
7. If you are configuring service over fiber transport, go to Step 8.

   If you are configuring service over T1 transport, in the IDT Route area, do the following:
   a. In the Cross-Connects To Be Created area, select all of the DS0 ports.
   b. In the Shelf list, select the shelf with the IDT interface for the T1 Transport Group.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

c. In the T1TG list, select the T1 Transport Group configured as the IDT interface.

d. Click **IDT** to assign the IDT to the selected ports.

8. In the Required Parameters area, set the parameters per your site requirements.

   Note: See *Overview of DS0 Cross-Connect Parameters* (on page 402) for additional information for these settings.

9. Click **OK** to create the cross-connections.

View Cross-Connection Parameters

GR-8 interface group cross-connect parameters

Source ID: The address of the GR-8 interface group channel in the following format: [Node ID(1–255)]-[shelf number(1–5)]-[slot number(1–20)]-[IG number(1–6)]-[channel number(1–96)].

Destination ID: The address of the remote DS0 port associated with the GR-8 interface group.

Connection Type (CCT): Specifies the type of cross-connect. For GR-8, the value is set to two-way (2WAY).

Number of Signaling Bits (NUMSIGBITS): Specifies the type of signaling used on T1 TDM facilities. For GR-8 provisioning, the value is set to 3 (GR8).

Number of DS0s (NUMBDS0S): Specifies the number of DS0s that were created in the same VC. For GR-8, the value is set to 1.

Nailed Up (NAILEDUP): Indicates whether a connection is maintained over T1 transport when no call is active. When you create a DS0 cross-connect, the default is Y (Yes) for GR-8 Mode I and for GR-8 Mode II Coin service. For all others, the default is N (No).

IG Details (IGDETAIL): Provides the access identifier of the IDT as well as protection information for the hops between the GR-8 interface group and the subscriber DS0 card. (The information in this parameter displays from the IGS and PROTN T1 parameters).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Viewing channel parameters

Use the procedure below to view GR-8 interface group cross-connect parameters.

To view the channel parameters of a GR-8 interface group

1. On the Navigation Tree, click a GR-8 interface group.
2. In the Work Area, click the **Channel** tab to view the current cross-connect parameters for the interface group.
3. On the toolbar, click **Action** > **View IG Details** to view details.

Check That It All Works

Once the C7 and the switch are configured, service is available. Subscribers can place a voice call.

The following quick checks can confirm that service is available:

- Check that there are no alarms in the Alarm Table referring to the interface group you created.
- Check that there are no alarms at the switch referring to the interface group you created.
- Verify that the service state for each T1 assigned to the interface group is in service and normal.
- Check for dial tone on at least one port of each card that you just assigned a channel.
- Place a call from one channel to another channel that you just assigned.

If service is not available, check DS0 troubleshooting techniques in the *Calix C7 Troubleshooting Guide*.

Remove GR-8 Cross-Connects and Interface Groups

Deleting a cross-connect from a GR-8 interface group

You can delete a GR-8 cross-connection from either endpoint of the cross-connection. Follow this procedure to delete a cross-connect from the endpoint closest to the switch.

To delete cross-connections from a GR-8 interface group

1. On the Navigation Tree, click a GR-8 interface group.
2. In the Work Area, click the **Channel** tab.
3. Use Ctrl+click to select one or more cross-connections for deletion.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

4. On the toolbar, click **Delete** > **Delete Cross Connects**. In the Confirmation dialog box, click **OK** to confirm the deletion.

Removing a DS1 association

Prior to removing a DS1 association from a GR-8 interface group, you must delete all cross-connects.

To remove a DS1 association from a GR-8 interface group

1. On the Navigation Tree, click a GR-8 interface group.
2. In the Work Area, click the **IG-DS1** tab.
3. Use Ctrl+click to select one or more DS1s for deletion.
4. On the toolbar, click **Delete**. In the Confirmation dialog box, click **OK** to confirm the DS1 removal.

Deleting a GR-8 interface group

Before you can delete a GR-8 interface group, you must delete its cross-connects and remove its DS1 associations. For details, see the procedures above.

To delete a GR-8 interface group from the network

1. On the Navigation Tree, click a GR-8 interface group.
2. In the Work Area, click the **Provisioning** tab.
3. On the toolbar, click **Delete**. In the Confirmation dialog box, click **OK** to confirm the deletion.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring Universal Services

Configure Remote Ports for Universal POTS and UVG Services

DS0 port parameters for POTS service

The default setting for DS0 ports on RPOTS-24, RU2W-24, and COMBO cards is for POTS service.

Parameter	Value
General Signaling Function (GSFn)	2LS
Receive Transmission Level Point (RTLP)	–2.0 dB
Transmit Transmission Level Point (TTLP)	–2.0 dB
Impedance	900

DS0 port parameters for UVG service

DS0 ports on RPOTS-24, RU2W-24, and COMBO-24 cards (not COMBO2-24, COMBO2-24A, and COMBO2-24D) can be configured for universal voice grade (UVG) service.

Parameter	Value
General Signaling Function (GSFn)	2GS, 2LSGS, 2RVOD, 2RVOI, 2RVOW
Receive Transmission Level Point (RTLP)	–2.0
Transmit Transmission Level Point (TTLP)	–2.0
Impedance	600

To set DS0 port parameters

1. On the Navigation Tree, click a C7 shelf containing DS0 ports.
2. On the Selection Filter, click **Port** > **DS0 Port** to view all DS0 ports from the selected shelf in the Work Area.
3. In the Work Area, click **Provisioning** to view the DS0 port parameters.
4. Click the first DS0 port, and then Shift+click the last DS0 port to select a range of ports to configure.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

5. Place the ports out of service and set the DS0 parameters:
   a. In the PST (Primary Service State) list, click **OOS** (Out of Service).
   b. In the GSFN (General Signaling Function) list, select a signal type.
   c. In the RTLP (Receive Transmission Level Point) list, select a decibel value.
   d. In the TTLP (Transmit Transmission Level Point) list, select a decibel value.
   e. In the Impedance list, select an impedance value.
   f. On the toolbar, click **Apply** to place the ports out of service and apply the DS0 port parameters. In the Confirmation dialog box, click **OK** to save the DS0 port configuration.
6. Re-select the same range of ports to configure as in Step 4.
7. Place the ports back in service:
   a. In the PST (Primary Service State) list, click **IS** (In Service).
   b. On the toolbar, click **Apply** to place the DS0 ports back into service. In the Confirmation dialog box, click **OK**.

Configure Host Ports for Universal POTS and UVG Uplinks

DS0 port parameters for POTS service on a GR-57 switch interface

Support for POTS service on a GR-57 switch interface is the default setting for ports on HPOTS-24 and HU2W-24 cards.

Parameter	Value
General Signaling Function (GSFn)	2LS
Receive Transmission Level Point (RTLP)	0.0 dB
Transmit Transmission Level Point (TTLP)	0.0 dB
Impedance	900

DS0 port parameters for UVG uplink

Parameter	Value
General Signaling Function (GSFn)	2GS, 2LSGS, 2RVOD, 2RVOI, 2RVOW
Receive Transmission Level Point (RTLP)	–2.0
Transmit Transmission Level Point (TTLP)	–2.0
Impedance	900

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

To set DS0 port parameters

1. On the Navigation Tree, click a C7 shelf containing DS0 ports to select it.
2. On the Selection Filter, click **Port** > **DS0 Port** to view all DS0 ports from the selected shelf in the Work Area.
3. In the Work Area, click **Provisioning**.
4. Click the first DS0 port, and then Shift+click the last DS0 port to select a range of ports to configure.
5. Place the ports out of service and set the DS0 parameters:
   a. In the PST (Primary Service State) list, click **OOS** (Out of Service).
   b. In the GSFN (General Signaling Function) list, select a signal type.
   c. In the RTLP (Receive Transmission Level Point) list, select a decibel value.
   d. In the TTLP (Transmit Transmission Level Point) list, select a decibel value.
   e. In the Impedance list, select an impedance value.
   f. On the toolbar, click **Apply** to place the ports out of service and apply the DS0 port parameters. In the Confirmation dialog box, click **OK** to save the DS0 port configuration.
6. Re-select the same range of ports to configure as selected in Step 4.
7. Place the ports back in service:
   a. In the PST (Primary Service State) list, click **IS** (In Service).
   b. On the toolbar, click **Apply** to place the DS0 ports back into service. In the Confirmation dialog box, click **OK**.

Configure Ports for Coin Service

DS0 remote port parameters for Coin service

Coin service can be configured on an RU2W-24 card for ports 1 through 4.

Parameter	Value
General Signaling Function (GSFn)	2COIN
Receive Transmission Level Point (RTLP)	–2.0
Transmit Transmission Level Point (TTLP)	–2.0
Impedance	900

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

DS0 host port parameters for Coin uplink

Coin service can be configured on a HU2W-24 card for ports 1 through 4.

Parameter	Value
General Signaling Function (GSFn)	2COIN
Receive Transmission Level Point (RTLP)	0.0
Transmit Transmission Level Point (TTLP)	0.0
Impedance	900

To set DS0 port parameters

1. On the Navigation Tree, click a C7 shelf containing DS0 ports to select it.
2. On the Selection Filter, click **Port** > **DS0 Port** to view all DS0 ports from the selected shelf in the Work Area.
3. In the Work Area, click the **Provisioning** tab.
4. Click the first DS0 port, and then Shift+click the last DS0 port to select a range of ports to configure.
5. Place the ports out of service and set the DS0 parameters:
   a. In the PST (Primary Service State) list, click **OOS** (Out of Service).
   b. In the GSFN (General Signaling Function) list, select a signal type.
   c. In the RTLP (Receive Transmission Level Point) list, select a decibel value.
   d. In the TTLP (Transmit Transmission Level Point) list, select a decibel value.
   e. In the Impedance list, select an impedance value.
   f. On the toolbar, click **Apply** to place the ports out of service and apply the DS0 port parameters. In the Confirmation dialog box, click **OK** to save the DS0 port configuration.
6. Re-select the same range of ports to configure as in Step 4.
7. Place the ports back in service:
   a. In the PST (Primary Service State) list, click **IS** (In Service).
   b. On the toolbar, click **Apply** to place the DS0 ports back into service. In the Confirmation dialog box, click **OK**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configure Ports for EBS Service

DS0 remote port parameters for EBS service

Enhanced Business Service (EBS) can be configured on an REPS-12 remote card.

Parameter	Value
General Signaling Function (GSFn)	2EBS
Receive Transmission Level Point (RTLP)	–3.5 dB
Transmit Transmission Level Point (TTLP)	–3.5 dB
Impedance (Cannot change)	900
Enhanced Business Service Level (EBSLVL)	AUTO

DS0 host port parameters for EBS uplink

EBS can be configured on an HEPS-12 host card.

Parameter	Value
General Signaling Function (GSFn)	2EBS
Receive Transmission Level Point (RTLP) (Cannot change)	0.0 dB
Transmit Transmission Level Point (TTLP) (Cannot change)	0.0 dB
Impedance (Cannot change)	900
Enhanced Business Service Level (EBSLVL)	AUTO

To set DS0 port parameters

1. On the Navigation Tree, click a C7 shelf containing DS0 ports to select it.
2. On the Selection Filter, click **Port** > **DS0 Port** to view all DS0 ports from the selected shelf in the Work Area.
3. In the Work Area, click **Provisioning**.
4. Click the first DS0 port, and then Shift+click the last DS0 port to select a range of ports to configure.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

5. Place the ports out of service and set the DS0 port parameters:
   a. In the PST (Primary Service State) list, click **OOS** (Out of Service).
   b. In the GSFN (General Signaling Function) list, select a signal type.
   c. In the RTLP (Receive Transmission Level Point) list, select a decibel value.
   d. In the TTLP (Transmit Transmission Level Point) list, select a decibel value.
   e. In the Impedance list, verify setting of **900** ohms.
   f. On the toolbar, click **Apply** to place the ports out of service and apply the DS0 port parameters. In the Confirmation dialog box, click **OK** to save the DS0 port configuration.
6. Re-select the same range of ports to configure as in Step 4.
7. Place the ports back in service:
   a. In the PST (Primary Service State) list, click **IS** (In Service).
   b. On the toolbar, click **Apply** to place the DS0 ports back into service. In the Confirmation dialog box, click **OK**.

Cross Connect DS0 Ports for Universal Switched Services

This topic describes how to create DS0 cross-connections for universal service.

See also:

- *View a List of Cross-Connections and Hops* (on page 126)
- *Delete Cross-Connects and Hops* (on page 134)

DS0 cross-connection default parameters

Cross-Connect Parameter	DS0 Default
Connection Type	2WAY
Number of signaling bits (NSG)	4
Number of DS0s (NDS0)	1
Nailed Up	Y (Yes) for EBS; N (No) for others

To create a DS0 to DS0 cross-connection

1. On the File menu, click:
   - (in iMS) **Create** > **Cross Connects** > **T0**
   - (in CMS) **Create** > **C7** > **Cross Connects** > **T0**

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

2. In the Select Cross-Connect Endpoints dialog box, Source area:
   a. In the Shelf list, select a shelf where source DS0 ports are located.
   b. In the Type list, click **T0** (default).
   c. In the Slot list, select the slot containing the source card.
   d. In the ports list, select the source ports for the cross-connections. Use Ctrl+click to select one port at a time, or Shift+click to select a range of ports.
   e. Click **SRC** to place the ports in the Cross-Connects To Be Created area.
3. In the Destination area:
   a. In the Shelf list, select the shelf where the destination DS0 ports are located.
   b. In the Type list, click **T0** (default).
   c. In the Slot list, select the slot containing the destination card.
   d. In the ports list, select the destination ports for the cross-connections. Use Ctrl+click to select one port at a time, or Shift+click to select a range of ports.
   e. Click **DEST** to place the ports in the Cross-Connects To Be Created area.
4. If you are configuring service over fiber transport, go to Step 5.

   If you are configuring service over T1 transport, in the IDT Route area do the following:
   a. In the Cross-Connects To Be Created area, select all of the T0 ports.
   b. In the Shelf list, select the shelf with the IDT interface for the T1 Transport Group.
   c. In the Equipment list, select a card containing DS0 ports.
   d. In the T1TG list, select the T1 Transport Group configured as the IDT interface.
   e. Click **IDT** to assign the IDT to the selected ports.
5. In the Required Parameters area, set the parameters per your site requirements.
6. Click **OK** to create the cross-connections.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring Non-Switched Services

Configure Ports for TO and PLAR Service

You can configure remote and host DS0 ports to provide non-switched services of Private Line Automatic Ring-down (PLAR) and 2-wire and 4-wire Transmission Only (TO).

2-Wire non-switched service support

Non-switched 2-wire services are supported on the following cards:

- RPOTS-24

  Private Line Automatic Ring-Down (PLAR) and Transmission Only (TO)
- HPOTS-24

  Private Line Automatic Ring-Down (PLAR) and Transmission Only (TO)
- COMBO-24

  Private Line Automatic Ring-Down (PLAR) and Transmission Only (TO)
- RU2W-24

  Private Line Automatic Ring-Down (PLAR) and Transmission Only (TO)
- HU2W-24

  Private Line Automatic Ring-Down (PLAR) and Transmission Only (TO)
- TO-6

  Up to 12 ports of 2-wire Transmission Only (TO) service.
- HDSL2/4-6

  Up to 6 ports of Private Line Automatic Ring-Down (PLAR) and Transmission Only (TO). PLAR service can only be configured over an HDSL T1 transport group.

4-wire non-switched service support

Services for 4-Wire Transmission Only (TO) are supported on the following cards:

- TO-6

  Supports 6 ports of 4-wire service.
- HDSL2/4-6

  Supports 3 ports of 4-wire service.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

DS0 port parameters for 2-wire TO service

Parameter	Value
General Signaling Function (GSFn)	2NOS – sealing current applied (default) 2NO[1] – no sealing current
Receive Transmission Level Point (RTLP)	–2.0 dB (default) Range of –7.0 to +3.0 dB **Values for a TO-6 card:** 0.0 dB (default) Range of –9.0 to +6.0 dB
Transmit Transmission Level Point (TTLP)	–2.0 dB (default) Range of –3.0 to +7.0 dB **Values for a TO-6 card:** 0.0 dB (default) Range of 0.0 to +9.0 dB
Impedance	900 Ohms (default) or 600 Ohms

[1] The RPOTS-24 and RU2W-24 cards do not support 2NO.

DS0 port parameters for 4-wire TO service

Parameter	Value
General Signaling Function (GSFn)	4NOS – sealing current applied (default) 4NO – no sealing current
Receive Transmission Level Point (RTLP)	0.0 dB (default) Range of –9.0 to +6.0 dB
Transmit Transmission Level Point (TTLP)	0.0 dB (default) Range of –6.0 to +9.0 dB
Impedance	600 Ohms (default) or 150, 900, or 1200 Ohms

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

DS0 port parameters for PLAR service

Parameter	Value
General Signaling Function (GSFn)	2LR
Receive Transmission Level Point (RTLP)	–2.0 dB Range of –7.0 to +3.0 dB
Transmit Transmission Level Point (TTLP)	–2.0 dB Range of –3.0 to +7.0 dB
Impedance	900 Ohms (default) or 600 Ohms

Set DS0 Port Parameters

To set DS0 port parameters

1. On the Navigation Tree, click a C7 shelf containing DS0 ports to select it.
2. On the Selection Filter, click **Port** > **DS0 Port** to view all DS0 ports from the selected shelf in the Work Area.
3. In the Work Area, click **Provisioning**.
4. Click the first DS0 port, and then Shift+click the last DS0 port to select a range of ports to configure.
5. Place the ports out of service and set the DS0 port parameters:
   a. In the PST (Primary Service State) list, click **OOS** (Out of Service).
   b. In the GSFN (General Signaling Function) list, select a signal type.
   c. In the RTLP (Receive Transmission Level Point) list, select a decibel value.
   d. In the TTLP (Transmit Transmission Level Point) list, select a decibel value.
   e. In the Impedance list, select an impedance value.
   f. On the toolbar, click **Apply** to place the ports out of service apply the DS0 port parameters. In the Confirmation dialog box, click **OK** to save the DS0 port configuration.
6. Re-select the same range of ports to configure as selected in Step 4.
7. Place ports back in service:
   a. In the PST (Primary Service State) list, click **IS** (In Service).
   b. On the toolbar, click **Apply** to place the DS0 ports back into service. In the Confirmation dialog box, click **OK**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Convert Ports Between 4-Wire and 2-Wire TO

The TO-6 card supports 6 ports configured for 4-wire transmission only (TO) service or 12 ports configured for 2-wire transmission only service. The HDSL2/4-6 card supports up to 3 ports configured for 4-wire TO service, and up to 6 ports configured for 2-wire service.

This section includes procedures to convert a 4-wire port on a TO-6 card into 2 ports of 2-wire service, and to combine 2 ports of 2-wire service into a single 4-wire port.

See also *Configure HDSL Ports for TDM Service* (on page 501).

To convert a 4-wire port to 2 ports of 2-wire service

Note: You convert a 4-wire port to 2 ports of 2-wire service by changing the GSFN parameter of the 4-wire port to 2-wire service and adding an even numbered port next to it.

1. On the Navigation Tree, click an odd-numbered port on a TO-6 card.
2. In the **Provisioning** Work Area, place the port out of service and set the GSFN parameter:
   a. In the PST (Primary Service State) list, click **OOS** (Out of Service).
   b. In the GSFN (General Signaling Function) list, click **2NOS** or **2NO** to set a 2-wire TO signal type.
   c. On the toolbar, click **Apply** to place the port out of service and apply the GSFN parameter. In the Confirmation dialog box, click **OK** to save the DS0 port configuration as a 2-wire port.
3. Place the port back in service:
   a. In the PST (Primary Service State) list, click **IS** (In Service).
   b. On the toolbar, click **Apply** to place the DS0 port back into service. In the Confirmation dialog box, click **OK**.
4. On the Navigation Tree, click the T0-6 card.
5. On the toolbar, click **Create** to open the Ports – Provisioning by Port Type dialog box.
6. In the Ports – Provisioning by Port Type dialog box:
   a. In the Shelf List, select the shelf where the TO-6 card is located. (default)
   b. In the Port Type list, click **DS0 Port**. (default)
   c. In the available ports list, click the even-numbered port ID that is one greater than the odd-numbered port you selected in Step 1.
   d. In the General Signaling Function list, click **2NOS** or **2NO** to set the new port for a 2-wire T0 signal type.
   e. Click **Add** to place the port in the TO-6 ports to be created list.
   f. Click **OK** to create the port.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

To convert 2 ports of 2-wire service to a 4-wire port

Note: You convert 2 ports of 2-wire service to a 4-wire port by deleting an even numbered 2-wire port and changing the GSFN parameter of the odd numbered port next to it to 4-wire service.

1. On the Navigation Tree, click an even-numbered port on a TO-6 card to select it.
2. On the toolbar, click **Delete**. In the Confirmation dialog box, click **OK** to delete the selected port.

   Note: The **Forced** check box in the Confirmation dialog box enables you to perform a deletion regardless of whether the port is in a redlined state.

3. On the Navigation Tree, click the odd-numbered port, one number less than the even-numbered port you deleted.
4. In the **Provisioning** Work Area, place the port out of service and set the GSFN parameter:
   a. In the PST (Primary Service State) list, click **OOS** (Out of Service).
   b. In the GSFN (General Signaling Function) list, click **4NOS** or **4NO** to set a 4-wire signal type.
   c. On the toolbar, click **Apply** to place the port out of service and apply the GSFN parameter. In the Confirmation dialog box, click **OK** to save the DS0 port configuration as a 4-wire port.
5. Place the port back in service:
   a. In the PST (Primary Service State) list, click **IS** (In Service).
   b. On the toolbar, click **Apply** to place the DS0 port back into service. In the Confirmation dialog box, click **OK**.

Cross-Connect Ports for TO and PLAR Service

Create cross-connections between DS0 ports configured for PLAR or TO service.

Match General Signaling Functions between cross-connected ports

When you create a cross-connection between to DS0 ports, the General Signaling Function (GSFn) for the source and destination ports must match the service type.

Four General Signaling Function settings can be used for a Transmission Only service type; 2NO, 2NOS; 4NO, and 4NOS. A port using any TO General Signaling Function can be cross-connected to another port using any TO function.

For example, a port using 2-wire TO (2NO) can be cross-connected to a port using 2-wire TO with sealing current applied (2NOS).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

If you attempt to cross-connect DS0 ports with incompatible General Signaling Functions, the system rejects the cross-connection and displays the following error message: "**Data not consistent.**"

DS0 cross-connection parameters for TO and PLAR service

Cross-Connect Parameter	DS0 Default
Connection Type	2WAY
Number of signaling bits (NSG)	0
Number of DS0s (NDS0)	1
Nailed Up	Y (Yes) for TO N (No) for PLAR

To create a DS0 to DS0 cross-connection

1. On the File menu, click:
   - (in iMS) **Create** > **Cross-Connect** > **T0**
   - (in CMS) **Create** > **C7** > **Cross-Connect** > **T0**
2. In the Select Cross-Connect Endpoints dialog box, Source area:
   a. In the Shelf list, select a C7 shelf where source DS0 ports are located.
   b. In the Type list, click **T0** (default).
   c. In the Slot list, select the slot containing the source card.
   d. In the ports list, use Ctrl+click to select the DS0 ports for the sources of the cross-connections.
   e. Click **SRC** to place the ports in the Cross-Connects To Be Created area.
3. In the Destination area:
   a. In the Shelf list, select the shelf where the destination DS0 ports are located.
   b. In the Type list, click **T0** (default).
   c. In the Slot list, select the slot containing the destination card.
   d. In the ports list, use Ctrl+click to select the DS0 ports for the destinations of the cross-connections.
   e. Click **DEST** to place the ports in the Cross-Connects To Be Created area.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

4. If you are configuring service over fiber transport, go to Step 5.

   If you are configuring service over T1 transport, in the IDT Route area do the following:

   a. In the Cross-Connects To Be Created area, select all of the T0 ports.

   b. In the Shelf list, select the shelf with the IDT interface for the T1 Transport Group.

   c. In the T1TG list, select the T1 Transport Group configured as the IDT interface.

   d. Click **IDT** to assign the IDT to the selected ports.

5. In the Required Parameters area, set the parameters per your site requirements. For specific settings, refer to the table preceding this procedure.

6. Click **OK** to create the cross-connections.

Configure Ports for DDS

The procedure in this section describes how to provision a DS0 DP-6 or OCU DP-6 port for Digital Data System (DDS) service. During this procedure, you set values (or confirm system default value settings) for the parameters described below.

Note: For C7 shelves with DDS applications, Calix recommends that signals at DS0 level interconnections be timed off of the same composite clock source generated by the Building Integrated Timing Supply (BITS). See *Timing* (on page 184) for additional information.

General Signaling Function (GSFN)

This parameter determines the signaling used by the port:

- 4D0 for a DS0 DP-6 port
- 4DU for an OCU DP-6 port

Rate

A user-selectable data rate assigned to a DDS port:

- 2400 Kbps
- 4800 Kbps
- 9600 Kbps
- 56000 Kbps (Default)
- 64000 Kbps

Secondary Channel (SC)

This parameter is only valid for an OCU DP-6 port. The default value is N (No).

Note: If your OCU DP-6 port rate is set to 64 Kbps, this parameter must be set to N (No).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Error Correction (EC)

The DS0 DP-6 and OCU DP-6 cards can accommodate six DDS channels. DDS service can be transported using either one or two DS0s. Each channel requires one DS0 if operating without error correction, and two DS0s if error correction is enabled with data rates of 56000 Kbps or 64000 Kbps. Data rates less the 56000 Kbps require one DS0 with or without error correction.

The Error Correction default value is N (No).

Zero Code Suppression (ZCS)

The default value for Zero Code Suppression is Y (Yes).

Note: If your port rate is set to 64000 Kbps, this parameter must be set to N (No).

Latching Loopback Timeout (TIMEOUT)

When set to 0, latching loopback continues to operate, but it cancels the timer if active. If greater than 0, the new timeout value is applied to the currently active latching loopback or subsequent loopback. If the new timeout value is greater than the previous value, the difference is applied to the currently outstanding timer. If the new timeout value is less than the previous value, the loopback terminates. If the new timeout value is the same as before, no further action is required. The default value is 0.

Latching Loopback Enable (LLBE)

The default value is Y (Yes).

Parameter	Value
General Signaling Function	OCU DP-6: 4DU DS0 DP-6: 4D0
Rate	56000 Kbps
Secondary Channel	N (No)
Error Correction	N (No)
Zero Code Suppression	Y (Yes)
Latching Loopback Timeout	0
Latching Loopback Enable	Y (Yes)

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configure DS0 DP-6 and OCU DP-6 Ports

To configure DS0 DP-6 and OCU DP-6 ports

1. On the Navigation Tree, click a DS0 DP-6 or OCU DP-6 port to select it.
2. In the Work Area, click the **Provisioning** tab.
3. Verify that the default setting is acceptable for each of the following parameters, or select a parameter to change its value:
   - General Signaling Function
   - Rate
   - Secondary Channel
   - Error Correction
   - Zero Code Suppression
   - Latching Loopback Timeout
   - Latching Loopback Enable
4. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save the port configuration.

Cross-Connect Ports for DDS Service

This section describes how to create DS0 cross-connections for non-switched services.

Related topics

- *Cross-Connect DS1 Ports for Hi-Cap Service* (on page 385)
- *View a List of Cross-Connections and Hops* (on page 126)
- *Delete Cross-Connects and Hops* (on page 134)

When cross-connecting DDS ports, if error correction is enabled you must cross-connect both the primary (PR) channel and the error correction (EC) channel.

DS0 cross-connection parameters for DDS Service

Cross-Connect Parameter	DS0 Default
Connection Type	2WAY (default)
Number of signaling bits (NSG)	0
Number of DS0s (NDS0)	1 (default)
Nailed Up	Y (Yes)

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

To cross connect a DS0 DP-6 port to an OCU DP-6 port

1. On the Navigation Tree, click a DS0-DP6 port.
2. In the Work Area, click **Cross Connect**.
3. On the toolbar, click **Create** > **TO Cross Connect** to open the Select Cross-Connect Endpoints dialog box.
4. In the Source area, create a DDS source endpoint:
   a. In the Shelf box, select a C7 shelf containing DS0-DP6 equipment.
   b. In the Type box, click **TO (DDS)**.
   c. In the Slot list, select the slot containing the source card.
   d. In the ports list, select a T0 port.
   e. Click **SRC** to place the source end point in the Cross-Connects To Be Created area.
5. In the Destination area, do the following to create a DDS destination endpoint:
   a. In the Shelf box, select a shelf containing OCU-DP6 equipment.
   b. In the Type box, click **TO (DDS)**.
   c. In the Slot list, select the slot containing the destination card.
   d. In the ports list, select a T0 port.
   e. Click **DEST** to place the destination end point in the Cross-Connects To Be Created area.
6. If you are configuring service over fiber transport, go to Step 7.

   If you are configuring service over T1 transport, in the IDT Route area do the following:
   a. In the Cross-Connects To Be Created area, select all of the T0 ports.
   b. In the Shelf list, select the shelf with the IDT interface for the T1 Transport Group.
   c. In the T1TG list, select the T1 Transport Group configured as the IDT interface.
   d. Click **IDT** to assign the IDT to the selected ports.
7. In the Required Parameters area, do the following:
   a. In the Number of Signaling Bits box, click **0 (CLEAR CH)**.
   b. In the Nailed Up list, select **Y**.
   c. For all other cross-connection parameters, accept the default settings.
8. Click **OK** to save the cross-connect provisioning.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

To cross connect a DS0 DP-6 or OCU DP-6 port to a T1 port

1. On the Navigation Tree, click a DS0-DP6 or OCU-DP6 port.
2. In the Work Area, click **Cross Connect**.
3. On the toolbar, click **Create** > **TO Cross Connect** to open the Select Cross-Connect Endpoints dialog box.
4. In the Source area, create a DDS source endpoint:
   a. In the Shelf box, select a C7 shelf containing DS0-DP6 or OCU-DP6 equipment.
   b. In the Type box, click **TO (DDS)**.
   c. In the Slot list, select the slot containing the source card.
   d. In the ports list, select a T0 port.
   e. Click **SRC** to place the source end point in the Cross-Connects To Be Created area.
5. In the Destination area, create a T1 destination endpoint:
   a. In the Shelf box, select a shelf containing T1-6 equipment.
   b. In the Type box, click **T1 Timeslot**.
   c. In the Slot list, select the slot containing the destination card.
   d. In the ports list, select a T1 port.
   e. In the Timeslot box, enter the number of the timeslot.
   f. Click **DEST** to place the destination end point in the Cross-Connects To Be Created area.
6. If you are configuring service over fiber transport, go to Step 7.

   If you are configuring service over T1 transport, in the IDT Route area do the following:
   a. In the Cross-Connects To Be Created area, select all of the T0 ports.
   b. In the Shelf list, select the shelf with the IDT interface for the T1 Transport Group.
   c. In the T1TG list, select the T1 Transport Group configured as the IDT interface.
   d. Click **IDT** to assign the IDT to the selected ports.
7. Click **OK** to save the cross-connect provisioning.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Chapter 13

Provisioning C7 xDSL Services

This section describes ADSL and VDSL cards, ports, cross-connections, and DSL services. Instructions are provided for:

- Configuring ADSL services with DS3, IMA, and optical uplinks
- Configuring VDSL services with Ethernet uplinks

For descriptions of the remaining xDSL template parameters, see *xDSL Template and Port Parameter Descriptions* (on page 99).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Quick ADSL Configuration Process

The high-level process for turning up broadband data service on the Calix C7 is described below.

Starting point

Before starting the configuration process, check that the following conditions are met:

- Transport is established to all C7 nodes providing broadband data service.
- The uplink card is installed and wired.
- The xDSL and OLT service cards are installed and wired.
- (PON/FTTP applications only) The ONTs are installed, wired, turned up and ranged.

Configuration process overview

The Calix C7 broadband data service configuration process follows:

1. Verify that all required equipment is installed and wired.
2. Configure profiles and templates.
    - (For C7 networks using the EXA switch fabric) Create Ethernet bandwidth profiles for subscriber cross-connects.
    - (For C7 networks using the Multiprotocol switch fabric) Create traffic profiles for subscriber cross-connects.
    - Create VLAN-IF templates to define subscriber connection attributes.
    - (xDSL only) Create xDSL templates to define port settings.
    - (xDSL only, if required) Configure bonding groups.
    - Create subscriber templates to define your different broadband data service offerings.
3. Configure Ethernet links according to the supported data service model.
4. Configure subscriber connections.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Applying xDSL Templates

You can apply xDSL templates to any ADSL or xDSL port within the system to define the service attributes for that port. You can apply the templates in following methods:

- Apply a template you created:
  - 250 different xDSL templates
- Apply a default template:
  - 9 default ADSL templates
  - 2 default VDSL templates

Note: The default templates are based on the various xDSL standards.

You apply an xDSL template to an ADSL or xDSL port by selecting the template ID (from the xDSL Template Identifier list) in the following instances:

- When configuring the port for service.
- When defining a subscriber template.

The xDSL template attributes are applied when you apply the subscriber template to the access port using the *Add Subscriber* tool or port Services screen in CMS.

See Configuring Subscriber Connections for instructions.

ADSL Tone Configurations

In most situations the default tone configurations defined by the chipset are sufficient for ADSL service. In cases where you are troubleshooting noise or crosstalk issues across bindings, you may need to customize the index of the start and end tones in upstream and downstream directions. By default the tone parameters are set to 0, and the configured values of the remaining tone settings are ignored.

ADSL tone configurations can only be set using TL1 commands. For more information, refer to the *Calix TL1 Management Reference Guide*.

Ranges and defaults for the supported service types are shown in the following table:

Service Type	DSST	DSET	USST	USET
G.DMT, G.LITE, T1.413, ADSL2	32–255	32–255	6–31	6–31
ADSL2+	32–511	32–511	6–31	6–31
ANNEXM	64–511	64–511	6–63	6–63

Note: The tone configuration feature does not apply to the MM2+, MM service types.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configure the Network Uplink—Overview

This section describes how to configure a network uplink for xDSL services.

Supported access

The following xDSL cards can be deployed in a Calix network:

- Legacy ADSL cards: The C7 supports ADSL access ports for *data only* using the following cards: ADSL-24, p/n 100-00022; COMBO-24 dualslot, p/n 100-00097

  Note: Legacy ADSL cards support video services in the VCVT mode only, which is not supported in R8.0. Therefore, video services are not supported on these legacy cards in C7 R8.0.

- ADSL2-based cards: The C7 supports ADSL2/2+ and ADSL access ports for data and video using the following cards: ADSL2-24, ADSL2-24A, COMBO2-24, COMBO2-24A, and COMBO2-24D.

  Note: ADSL2-based cards support video services in the AVT mode, which is supported in R8.0.

- VDSL2-based cards: The C7 supports VDSL2, ADSL2/2+, and ADSL access ports for data and video using the following cards: VDSL2-24 and COMBO2-24V.

  Note: The ADSL2-24A, COMBO2-24A, VDSL2-24, and COMBO2-24V cards support G.998.1 (G.Bond) xDSL pair bonding.

  Note: The VDSL2-24 and COMBO2-24V cards also G.998.2 bonding with VDSL2 or ADSL2 fallback service types with PTM encapsulation on the line.

Detailed descriptions of the supported standards and rates are listed in the datasheet of each card.

Supported uplinks

The C7 supports Ethernet and ATM uplink types for data, video, and VoIP services.

C7 Ethernet Uplinks (Multiprotocol switch fabric):

For configurations using a Virtual Bridge (Multiprotocol switch fabric), the C7 supports Ethernet uplinks using the Ethernet Gateway (EGW), GE-2E, GE-2p, and GE-2p/FE-4p cards, each of which is equipped with two Gigabit Ethernet (GE) ports and two or four 10/100 Fast Ethernet (FE) ports.

Note: For simplicity, subsequent references to "Ethernet cards" apply to EGW, GE-2E, GE-2p, and GE-2p/FE-4p cards.

Ethernet uplink cards support the following VLAN application modes:

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- VLAN Per Service (for L2 DHCP relay and L2 PPPoE support; video ingress, RG support; GPON SIP)
- VLAN Per Port (for L2 DHCP relay and L2 PPPoE support)
- Routed (for L3 DHCP relay/proxy and PPPoE relay support; video ingress, non-RG support; H.248 gateway)
- S-Tag Switch (for IP DSLAM aggregation)
- Transparent LAN Service

C7 Ethernet Uplinks (EXA switch fabric):

For configurations using the shelf-wide Local Bridge (EXA switch fabric), the C7 supports Ethernet uplinks using the RAP-10GE. With this type of uplink, the following VLAN application modes are supported:

- VLAN per service model (for L2 DHCP relay and L2 PPPoE support; GPON SIP)
- VLAN per port model (for L2 DHCP relay and L2 PPPoE support)
- Transparent LAN service

C7 ATM Uplinks:

For a list of C7 ATM uplink cards, refer to an earlier version of the *Calix C7 Broadband Data Services Guide*.

General uplink requirements

Follow these general requirements when establishing an uplink for ADSL services:

- The uplink card can reside in any C7 shelf or node.
- Typically, one uplink suffices to serve most xDSL services in the network. However, you can configure multiple uplinks as required for your xDSL applications (separate uplinks for Internet and video services, for example).
- If you require redundant uplinks for card types that support equipment protection, the protection group must be configured before you configure the uplink port for service.

Starting point

Before starting the uplink/downlink configuration process, confirm that the following conditions are met:

- Transport is established to all C7 nodes providing broadband data service.
- The Ethernet card providing the uplink interface(s) is installed and wired.
- The EGW or GE-2p/FE-4p providing the downlink interface(s) is installed and wired.
- Traffic profiles have been created as required.
- The following templates have been created as required: xDSL, data subscriber, VLAN-IF.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configure process

For the VLAN per service model for **data applications**, perform the following steps to configure an Ethernet uplink.

1. Configure the Ethernet port for service.
2. Create a VLAN.
3. Create a VLAN interface to an Ethernet port.
4. (For multi-shelf applications) Create a cross-connect between VLANs.

For detailed procedures, as well as instructions on setting up uplinks for the other service models, refer to the *Calix C7 Broadband Data Services Guide, Calix C7 Video Services Guide,* or *Calix C7 VoIP Services Guide*.

Configure Network Uplink

The tasks required to configure the supported uplink types for xDSL services are listed below. For detailed instructions to perform these tasks, refer to the *Calix C7 Broadband Data Services Guide and* the *Calix C7 Video Services* as appropriate for your xDSL application(s).

Configure an OCn optical uplink

Perform the following steps to configure an OCn optical uplink:

1. Configure the OCn optical port for service.
   - Set the External Interface parameter to **Y** (Yes).
   - Set the remaining port parameter values to match the settings on the far end.
2. Configure an STS facility on the OCn optical port.
   - Set the STS Mapping parameter to **ATMUNI**.
   - Set the remaining STS parameter values to match the settings on the far end.

Configure a DS3 uplink

Configure a DS3 uplink as follows:

- Configure the DS3 port for service.
  - Set the DS3 Interface Type parameter to **UNI**.
  - Set the External Interface parameter to **Y** (Yes).
  - Set the remaining port parameter values to match the settings on the far end.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configure an IMA uplink using the IMA-12 card

This section describes how to configure an IMA interface using the IMA-12 card to provide Internet uplink service.

Note: If you are *NOT* using an IMA facility for your Internet uplink, skip this section.

The IMA-12 card provides a high-density ATM interface of up to 24 Mbps to establish IMA groups for Internet uplinks.

The IMA-12 card supports two modes of operation; direct interface and resource mode. The direct interface is provided via the card's 12 DSX level T1 interfaces. Individual DS1 ports on the card can be associated with a corresponding ATM resource port (16 logical resource port interfaces) on the card to operate in the resource mode. In resource mode, the IMA-12 card can be used to create logical IMA links across non-IMA cards in the same C7 shelf. This mode can also be used across more than one IMA-12 card.

Note: Resource mode has several uses, including: creating IMA transport over T1 and T1 HDSL; creating groups of eight IMA links across multiple C7 cards (same shelf); and putting previously unused DS1 ports in a C7 shelf in service via IMA interfaces.

ATM Resource Ports extend IMA to the following Calix C7 cards:

- HDSL2/4-6
- T1-6
- T1-6 A+T
- IMA-12

Note: See the *Calix Engineering and Planning Guide* for additional information on the IMA-12 card.

You use the following basic steps for provisioning an IMA uplink using an IMA-12 card:

- Configure the ATM Resource Ports
- Configure the DS1 ports for use in an IMA group
- Create an IMA group and add DS1 ports
- Configure the IMA group as an uplink

For detailed uplink provisioning instructions, refer to the *Calix C7 Broadband Data Services Guide*.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configure an IMA uplink using the T1-6 A+T card

Perform the following steps to configure an IMA uplink:

1. Configure the T1 ports for use in an IMA group.
   - Set the DS1 port type as a T1 (set the DS1TYPE parameter to **T1**)
   - Set the following T1 port parameter values: set FMT to **ESF**, LINECDE to **B8ZS**, DS1MAP to **N/A**.
   - Set the remaining T1 port parameter values to match the settings on the far end.
2. Create an IMA group and add the T1 links to it.
3. Configure the IMA group for service.
   - Set the Mapping parameter to **UNI**.
   - Set the External Interface parameter to **Y** (Yes).
   - Set the remaining parameter values to match the settings on the far end.

Configure a T1 UNI uplink

Perform the following steps to configure a T1 UNI uplink:

1. Configure the DS1 port type as a T1 (set the DS1TYPE parameter to **T1**).
2. Configure the T1 port for service.
   - Set the DS1 Mapping parameter to **UNI**.
   - Set the External Interface parameter to **Y** (Yes).
   - Set the remaining T1 port parameter values to match the settings on the far end.

For detailed uplink provisioning instructions, refer to the *Calix C7 Broadband Data Services Guide* and the *Calix C7 Video Services* as appropriate for your ADSL application(s).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring xDSL Ports

This topic describes how to configure C7 xDSL ports for service. All ports sharing the same xDSL template can be configured in one procedure.

You often configure multiple xDSL ports at the same time. This procedure includes steps to filter the Navigation Tree to show only xDSL ports on a selected node.

To configure xDSL ports for service

1. On the Navigation Tree, click a C7 node containing xDSL equipment to select it.
2. In the Selection Filter, click **Port** > **xDSL** Port to display all xDSL ports at the selected node.
3. In the Provisioning Work Area, click the first xDSL port in the list, scroll to the bottom of the list, and then Shift+click the last xDSL port in the list to select all ports for editing.
4. In the Edit Row, place the ports out of service and select an xDSL template:
   a. In the PST(Primary Service State) list, click **OOS** (Out of Service).
   b. In the Profile column, select an xDSL Template to provide values to the xDSL port parameters.

   Note: The xDSL template name is not saved with the port parameters. The template is only used to provide values to the other xDSL port parameters.

   c. On the toolbar, click **Apply** to place the ports out of service and apply the xDSL template. In the Confirmation dialog box, click **OK** to save your changes.
5. In the Work Area, re-select the ports that you selected in Step 3.
6. Place the ports back in service:
   a. In the Edit Row, in the PST, click **IS** (In Service).
   b. On the toolbar, click **Apply** to place the ports back in service. In the Confirmation dialog box, click **OK**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring the xDSL Power Shutdown Priority

You can configure the xDSL power shutdown priority on a per-card basis:

- **1** (Category 1): Keeps all xDSL ports in service as long as sufficient power to the shelf is sustained.
- **3** (Category 3): Disables all xDSL ports on the card once the shelf delay timer expires, to conserve power for other high-priority services. Category 3 is the default priority for all xDSL cards.

Note: The Category 2 option is not currently supported.

To set the power shutdown priority for xDSL cards

1. On the Navigation Tree, click a C7 shelf containing an xDSL card.
2. Click the xDSL card to configure, and then in the Work Area, click the **Provisioning** tab.
3. In the Power Category list, click **1** or **3** to assign a power shutdown priority to the card.
4. On the toolbar, click **Apply** to update settings. In the Confirmation dialog box, click **OK**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Overview of VC Cross-Connection Parameters

The parameters listed below define the characteristics of a virtual channel connection. For existing VC cross-connections, you can view these on the Provisioning tab in the Work Area. The abbreviated name shown in parentheses represents the parameter ID in the Provisioning table view when multiple cross-connects are selected.

Source Virtual Channel Identifier (SOURCE ID)

Specifies the address of the source endpoint of the virtual channel connection. See ADSL VC Access Identifier below.

Destination Virtual Channel Identifier (DESTINATION ID)

Specifies the address of the destination endpoint of the virtual channel connection. See ADSL VC Access Identifier below.

Drop Access Identifiers (DROP IDS)

Specifies the location in the cross-connection where traffic is dropped along the path to the endpoint. This parameter pertains to drop-and-continue applications. See ADSL VC Access Identifier below.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

ADSL VC Access Identifier

The ADSL VC Access Identifier pertains to the SOURCE ID, DESTINATION ID, and DROP IDS parameters. These addresses read from left to right:

NODE-SHELF-SLOT-PORT-CH-VP-VC

Parameter	Description
NODE	A number between 1 and 255. This number specifies the address of the C7 node in the network.
SHELF	A number between 1 and 5. This number specifies the address of the C7 shelf on the node.
SLOT	CSA, CSB or a number between 1 and 20. This number specifies the slot on the C7 shelf where the card resides.
PORT	A number between 1 and 24. This number specifies the port number on the card.
CH	The channel number on an ADSL card. This number identifies the logical channel 0 on an ADSL card. This identifier appears only on ADSL cards. Channel number is one of two logical channels within the DSL port.
VP	A number that specifies the virtual path identifier (VPI). VPI 0 is reserved for use in ATM VC cross-connections. The valid range is a number from 0 to 4095 inclusive. VPIs 4000 through 4090 inclusive are assigned by default to a VP pool for end-to-end protected VP cross-connects. VPIs 4094 and 4095 are reserved for C7 system use.
VC	A number from 32 through 32767 inclusive. This numbers specifies the virtual channel identifier (VCI). VCIs 0 through 31 are reserved and cannot be provisioned.

Cross Connect Way (CCT)

Specifies the cross-connection as a one or two-way connection.

- **2WAY:** Traffic flows in both directions on the connection.
- **1WAY:** Traffic flows in one direction on the connection.

The default value is 2WAY.

Traffic Profile ID (TRFPROF)

Specifies which traffic profile to apply to the forward direction of a connection. Specify a user-defined profile number (between 1 and 500) for specific class-of-service connections.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Backward Traffic Profile ID (BCKPROF)

Specifies which traffic profile to apply to the backward direction of a connection. Specify a user-defined profile number (between 1 and 500) for specific class-of-service connections.

If you do not specify a traffic profile for the backward direction, the system assumes this cross-connection is symmetrical and applies the value from the Traffic Profile parameter.

Cross-Connect Path (PATH)

Specifies the type of path (connection) you are creating through the network.

- **WORK ONLY:** Creates a succession of virtual connections that are the working path through the network.
- **PROT ONLY:** Creates a succession of virtual connections that are the protecting path through the network.
- **WORK + PROT:** Creates both the working and protect paths.
- **UNPROT:** Creates an unprotected connection.

Bandwidth Constraint (BWC)

Specifies the Bandwidth Constraint that is applied to this cross-connection.

Source Path Protection Label (SOURCE PPL)

Specifies the Packet Protection Label (PPL) associated with the protection path on the source endpoint, if applicable.

Source PPL State (SRC PPL STATE)

Indicates the possible trouble condition, irregularities, errors, or off-normal conditions for the source Packet Protection Label.

Destination Path Protection Label (DESTINATION PPL)

Indicates the PPL association for the cross-connect destination endpoint, if applicable.

Destination PPL State (DST PPL STATE)

Indicates the possible trouble condition, irregularities, errors, or off-normal conditions for the destination Packet Protection Label.

Connection Status (CONSTAT)

Indicates the status of the connection.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

VC Cross-Connection Requirements for ADSL

This topic describes creating VC cross-connections from many ADSL ports to a single uplink. All ADSL ports connected by VCs sharing the same traffic profile can be cross-connected in one procedure.

See also:

- *View a List of Cross-Connections and Hops* (on page 126)
- *Delete Cross-Connects and Hops* (on page 134)

Common ADSL cross-connection requirements

- All of the ADSL port VP and VC settings are usually the same and are determined by the type of ADSL modem used. Check the subscriber ADSL modem documentation for the correct values. The most common values are VP=0 and VC=35.
- Many ADSL ports will be cross-connected to a single uplink.
- For ATM uplink types, an Internet Service Provider assigns the VP and VC settings used at the uplink.
- All cross-connections will use the same VP setting at the uplink.
- Each cross-connection will have a unique VC setting at the uplink. The value for a VC setting must be from 32 through 32767 inclusive. Values 0 through 31 are reserved and cannot be provisioned.
- Cross-connection type is 2WAY.
- The ATM traffic profile and Backward ATM traffic profile is usually UBR. You can create and use your own traffic profile.
- The cross-connect path is usually set for Working plus Protect paths. Use Unprotected if the ADSL ports and uplink port are on the same shelf.

See *Overview of VC Cross-Connection Parameters* (on page 481) for additional information.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Create a VC Cross-Connection for ADSL or VDSL Service

Using the C7 multiprotocol switch fabric, typically you cross-connect many xDSL ports to a single uplink.

To build cross-connections, use the subscriber activation tools in the management interface. For instructions, see the *Calix C7 Broadband Data Services Guide*.

To manually build a cross-connect from one or more xDSL ports to an uplink facility, you can use the VLAN Interface (VLAN-IF) tool as detailed in the *Calix C7 Broadband Data Services Guide*.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Check That It All Works

After the ports and cross-connections are configured, service is available. A subscriber with a PC connected to a DSL modem can now log on and connect to the Internet.

The following quick checks can confirm that service is available:

- Check the Primary Service State of the ATM uplink port or path. On the Navigation Tree, click the uplink port or path and check the following parameters:
  - Primary Service State is IS-NR (In-Service Normal).
  - Secondary Service State is normal.
- Connect a PC and DSL modem to the subscriber and connect to the Internet.
- If the router at the network end is not connected to the Internet, you can still check service by pinging the IP address of the router.

If service is not available, check DSL troubleshooting techniques in the *Calix C7 Troubleshooting Guide*.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

ADSL Port Retraining

The system provides an initialize command that instructs the C7 to initialize an xDSL port that causes a retraining of the xDSL port. Retraining basically provides a link rate re-negotiation. Executing this command causes the modem to re-negotiate the connection. This interrupts the subscriber data transfer for the duration of the retrain.

ALERT! Initializing (retraining) an xDSL port is a service-affecting operation.

To initialize (retrain) an xDSL port

1. On the Navigation Tree, click the xDSL port to retrain.
2. In the Work Area, click the **Provisioning** tab.
3. On the toolbar, click **Action** > **Initialize**.
4. In the Confirmation dialog box, click **OK** to send the selected action.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

ADSL Performance Monitoring

The system provides Performance Monitoring (PM) at the port level for two time periods:

- Incremental counts captured in 15-minute intervals for the current period and for the past eight hours (divided into 32 separate 15-minute intervals).
- Daily counts captured in one-day intervals for the current 24-Hour period, and the 6 previous 24-hour periods.

Options for viewing xDSL PM registers on the C7 include the following:

- View any of the current or past 15-minute or daily interval data.
- View PM data captured at the near-end or the far-end node.
- Automatically poll PM registers every 3, 5, 10, 20, or 30 seconds to view increases in PM statistics for the selected polling frequency.
- Set all current PM registers (those currently accumulating data) to zero. This can be helpful after making repairs or correcting an error condition. By clearing the PM registers, you eliminate PM register counts prior to the repair or corrective action.

Follow the steps below to monitor xDSL physical port PM statistics.

To monitor xDSL physical port performance statistics

1. On the Navigation Tree, do the following:
   a. Double-click the card on which to monitor performance to expand the view.
   b. Click a port on which to view performance data.
   c. For viewing multiple ports, use Ctrl+click to select individual ports, or Shift+click to select a range of ports.
2. In the Work Area, click **Performance** > **xDSL**.
3. In the bottom of the Work Area:

   a. Click **Far End** to retrieve performance registers at the far-end node, or accept the default, **Near End**, to retrieve PM registers at the near-end node.
   b. Click **Daily Interval** to retrieve PM data from a one-day register, or accept the default, **15 Minute Interval**, to retrieve PM registers from a 15-minute interval.
   c. In the Interval list, select a previous interval, or accept the default to retrieve the interval that is currently accumulating PM data.

Note: In the Validity column, Partial indicates that the interval that displays in the Work Area is currently accumulating PM data.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

d. (Optional) Select the **Show GOS threshold values** check box to view the grade of service values alongside actual values.

4. Do one of the following:

   - On the toolbar, click **Refresh** to load the selected PM statistics in the Work Area.
   - In the bottom of the Work Area, in the **Poll Frequency** list, select a value (in seconds) to automatically refresh the PM statistics every 3, 5, 10, 20, or 30 seconds.

5. (Optional) Clear the current PM registers:

   Note: PM registers can only be cleared for an interval that has not yet completed.

   a. In the Work Area, click the row(s) of the port(s) on which to clear PM registers.

   b. On the toolbar, click **Action** > **Clear PM Registers**.

   c. Click **Refresh**.

   Note: The value in the **Validity** column changes to **Adjusted** to indicate that you have cleared the PM registers.

For additional PM information, see the *Calix C7 Troubleshooting Guide*.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Chapter 14

Provisioning HDSL Services

This section describes HDSL cards, ports, and services. Instructions are provided for configuring equipment protection, Hi-Cap DS1 service. Links are provided to instructions for provisioning HDSL ports for IMA or TDM transport.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Overview of HDSL Port Parameters

The following parameters are associated with an HDSL port. The abbreviated name shown in parentheses represents the parameter ID in the Provisioning table view when multiple ports are selected.

HDSL Port Identifier (ID)

Specifies the address of the HDSL port. The address reads from left to right:

NODE-SHELF-SLOT-PORT

NODE is a number between 1 and 255. It specifies the address of the C7 node in the network.

SHELF is a number between 1 and 5. It specifies the address of the C7 shelf on the node.

SLOT is a number between 1 and 20. It specifies the slot on the C7 shelf where the card resides.

PORT is a number between 1 and 6 on the HDSL2/4-6 card. It specifies the port on the card.

Primary Service State (PST)

Specifies the default state of the equipment. Provisionable values are IS (in-service) and OOS (out-of-service). If pre-provisioning a port, you can use the default IS value to place the port in service once the equipment is inserted in the shelf.

When the equipment is inserted, the PST value appears as IS-NR (in-service, normal), OOS-AU (Out of Service-Autonomous), OOS-MA (Out of Service-Management), or OOS-AUMA (Out of Service-Autonomous and Management). Autonomous indicates the port is out-of-service due to fault conditions; management means that the port has been administratively placed out-of-service.

Secondary Service State (SST)

Displays one or more additional service states applicable to the port.

User Description (USERDESC)

Enables you to type a description of the port (11 characters maximum).

Maintenance State

Displays any standing conditions currently affecting the port. If you are viewing the port in Form View, click the ellipsis button to the right of the Maintenance State field to view a list of the conditions.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Line Power (DS1PWR)

Specifies whether the line supplies power. Set to SINK if the HDSL card does not supply line power. Set to SOURCE if the card supplies line power.

Interface Group DS1 (IGDS1)

Displays the DS1 line termination within a T1 interface group. This parameter only applies when the HDSL port has been assigned to a T1 transport group.

DS1 Format (FMT)

Specifies the DS1 signal format:

- For Hi-Cap DS1 service, set to UF (Unframed), and set the DS1 Map parameter to N/A.
- For IMA transport using the IMA-12 card, set to Extended Super Frame (ESF), and set the DS1 Map parameter to SEQ.
- For TDM transport, set to either Extended Super Frame (ESF) or Super Frame (SF) per your site requirement, and set the DS1 Map parameter to SEQ.
- For T0 TDM service, set to either ESF (Extended Super Frame) or SF (Super Frame) per your site requirement, and set the DS1 Map parameter to SEQ.

Grade-of-Service (GOS)

Identifies the grade of service profile for monitoring performance on the facility:

- **OFF:** (default) is used to specify that performance monitoring continues, but threshold crossing alerts (TCA) are not sent.
- **DEFLT:** is specified to use the C7 system default values.
- If you have defined an HDSL grade-of service profile, you can set the parameter to a specific profile number.

See also *Overview of Grade of Service Profiles* (on page 73).

Line Type (LINETYPE)

Specifies whether the line type is set to 2-wire or 4-wire mode. The following rules apply to configuring the line type for HDSL ports:

- On an HDSL2/4-6 card, you can configure up to 6 ports as 2-wire or up to 3 ports as 4-wire, or create a combination of 2-wire and 4-wire ports.
- For a 4-wire line type, you can only use ports 1, 3, and 5. Before you configure a 4-wire port, you must delete the next consecutive port from the card (for example, to set port 1 to 4-wire, delete port 2).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Terminal Type (TERMTYPE)

Specifies whether the HDSL port is designated as the central office terminal (COT) or the remote terminal (RT) end of the HDSL line:

- For DS1 Hi-Cap and TDM services, you typically set the Terminal Type to COT regardless of the location of the HDSL2/4-6 card in the network.
- For TDM transport, you must set one end of the HDSL line to COT and the other end to RT. To configure HDSL ports for a T1 transport group, you typically set the port on the IDT shelf as COT and the port on the RDT shelf as RT.

Signal-to-Noise Margin Threshold (SNRTHR)

Specifies a threshold (from 1 to 15 dB) for the signal-to-noise ratio (SNR) margin, as measured from the near end. The SNR margin is the maximum decrease in equalized noise, or the maximum increase in equalized signal, that the line can tolerate and still maintain a bit error rate of 10-7. When the SNR margin is lower than the configured threshold, an SNRMARGIN alarm is raised. A value of 0 disables this parameter.

Loop Attenuation Threshold (LOOPATTENTHR)

Specifies a threshold for loop attenuation (from 1 to 127 dB), as measured from the near end. Typical values are in the range 20 to 40 dB. When the loop attenuation is higher than the configured value, a LOOPATTEN alarm is raised. A value of 0 disables this parameter.

DS1 Map (DS1MAP)

Specifies the mapping of the payload to perform. For Hi-Cap services, set to N/A. For T1 transport and fractional T1 service, set to Sequential (SEQ). See also the **DS1 Format** parameter.

Timing Mode (TMGMODE)

Indicates the timing mode. The values are:

- **LOOP:** T1 transmission timing is derived from the far-end device recovered timing. Loop timing is independent of shelf timing. Loop is the default.
- **SOURCE:** T1 transmission timing is derived from the C7 system timing.

Note: Loop timing is typically used for unframed (UF) signals. Source timing is used for framed (SF or ESF) signals.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Default port parameters for an HDSL port

Parameter	System Default
Primary Service State	IS (In Service)
DS1 Format	UF (Unframed)
Line Power	SINK
Grade of Service	OFF
Line type	2-WIRE
Terminal unit type	COT (Central Office Terminal)
Signal-to-noise margin threshold (near-end)	6 dB
Loop attenuation threshold (near-end)	20 dB
DS1 Map	N/A
Timing Mode	Loop

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring HDSL Equipment Protection

The C7 supports 1:1 and 1:N equipment protection for HDSL2/4-6 cards.

See *Configuring Equipment Protection* (on page 193) for detailed information on metallic services protection modules, equipment protection parameters, configuring 1:1 equipment protection, and configuring 1:N equipment protection.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring HDSL for Hi-Cap DS1 Service

Configure HDSL Ports for Hi-Cap Service

Ports on the HDSL2/4-6 card can be configured to deliver Hi-Cap DS1 services. You create a DS1 clear channel pipe (full-bandwidth availability with no framing or control bits) that transports services from the source to the destination with no effect on the payload.

Rules for configuring the line type on HDSL ports

The following rules apply to configuring the line type for HDSL ports:

- You can configure up to 6 ports as 2-wire or up to 3 ports as 4-wire, or create a combination of 2-wire and 4-wire ports.
- For a 4-wire line type, you can only use ports 1, 3, and 5. Before you configure a 4-wire port, you must delete the next consecutive port from the card (for example, to set port 1 to 4-wire, delete port 2).

HDSL port parameters for Hi-Cap service

The following table lists the parameters required to configure an HDSL port for Hi-Cap service.

Parameter	Value
DS1 Format (required)	Set to UF (Unframed).
Line Power	Set to SINK (default) or SOURCE per your site requirement.
Grade of Service	Set to OFF (default), DEFLT, or a pre-defined grade-of-service profile number, per your site requirement.
Line Type	Set to 2WIRE (default) or 4WIRE.
Terminal Type	Set to COT (default).
Signal-to-Noise Ratio Margin Threshold (near-end)	Set to a value from 1 to 15 (or 0 to disable), per your site requirement.
Loop Attenuation Threshold (near-end)	Set to a value from 1 to 127 (or 0 to disable), per your site requirement.
DS1 Map	Set to N/A (no mapping required).
Timing Mode	Set to Loop (default).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

To configure an HDSL port for Hi-Cap service

1. On the Navigation Tree, click an HDSL card to view the ports, and then click the HDSL port to configure for Hi-Cap service.
2. In the **Provisioning** Work Area, place the port out of service:
   a. In the Primary Service State (PST) list, click **OOS** (Out of Service).
   b. On the toolbar, click **Apply** to place the port out of service. In the Confirmation dialog box, click **OK**.
3. Set the following required parameters:
   a. In the DS1 Format list, select **UF** (unframed).
   b. In the Line Power list, click **SINK** if the HDSL card does not power the line, or **SOURCE** if the HDSL card powers the line.
   c. If you are applying a grade of service, in the Grade of Service list select **DEFLT** or a grade of service profile number that you have created for HDSL service.
   d. In the Line Type list, click **2WIRE** or **4WIRE** as required for your site.
   e. In the Signal-to-Noise Ratio Margin Threshold box, type the value required for your site.
   f. In the Loop Attenuation Threshold box, type the value required for your site.
   g. In the DS1 Mapping list, click **N/A**.
   h. On the toolbar, click **Apply**. In the Confirmation dialog box, click **OK** to save your changes.
4. Place the port back in service:
   a. In the Primary Service State list, click **IS** (In Service).
   b. On the toolbar, click **Apply** to place the port back in service. In the Confirmation dialog box, click **OK**.

Cross-Connect HDSL Ports for Hi-Cap Service

This topic describes how to create HDSL cross-connections for Hi-Cap DS1 service.

Related topics

- *View a List of Cross-Connections and Hops* (on page 126)
- *Delete Cross-Connects and Hops* (on page 134)

Cross-connection endpoints for HDSL Hi-Cap DS1 service

One end of an HDSL cross-connection that is configured for Hi-Cap DS1 service must be connected to an HDSL port. The other end can be either an HDSL or a DS1 port.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

See also *Configure HDSL Ports for Hi-Cap Service* (on page 497).

Cross-connection parameters

Set the following parameters when you create a cross-connection:

Cross-Connect Parameters	Default
Cross-Connect Way	2WAY
Cross-Connect Path (Required)	Must be specified when you create the cross-connection. For end-to-end cross-connections, Working and Protect (WORK + PROT) and Unprotected (UNPROT) are valid options. For a cross-connection hop, Working Only (WORK ONLY), Protection Only (PROT ONLY), and Unprotected (UNPROT) are valid options.

To create Hi-Cap DS1 cross-connections

1. On the Navigation Tree, click a port where you are creating a cross-connection.
2. In the Work Area, click **Cross-Connect**.
3. On the toolbar, click **Create** > **T1 Cross Connect** to open the Select Cross-Connect Endpoints dialog box.
4. In the Source area of the dialog box:
   a. In the Shelf list, select the shelf where the source port is located.
   b. In the Type list, click a service type (**HDSL** or **T1**).
   c. In the ports list, click the HDSL or DS1 port that is the source for the cross-connection.
   d. Click **SRC** to place the source port in the Cross-Connects To Be Created area.
5. In the Destination/Drop area:
   a. In the Shelf list, select the shelf where the destination port is located.
   b. In the Type list, click a service type **(HDSL** or **T1**).
   c. In the Ports list, click the HDSL or DS1 port that is the destination for the cross-connection.
   d. Click **DEST** to move the destination port to the Cross-Connects To Be Created area.
6. Repeat Steps 4 and 5 for each additional cross-connection you are creating.
7. In the Required Parameters area, in the Cross-Connect Path list, select the path type for the cross-connection: **Work Only**, **Prot Only**, **Work + Protect**, or **Unprot**.
8. Click **OK** to save the cross-connection.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring HDSL for TDM Transport

For IMA transport, see the following topics:

- *Configure HDSL Ports for IMA Transport* (on page 256)
- *Create an IMA Group and Add T1s* (on page 257)

For TDM transport, see the following topics:

- *Configure HDSL Ports for TDM Transport* (on page 266)
- *Assign Ports to a T1 Transport Group* (on page 270)

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring HDSL for TDM Service

This section describes configuring HDSL ports for T0 TDM service.

Configure HDSL Ports for TDM Service

Rules for configuring the line type on HDSL ports

The following rules apply to configuring the line type for HDSL ports:

- You can configure up to 6 ports as 2-wire or up to 3 ports as 4-wire, or create a combination of 2-wire and 4-wire ports.
- For a 4-wire line type, you can only use ports 1, 3, and 5. Before you configure a 4-wire port, you must delete the next consecutive port from the card (for example, to set port 1 to 4-wire, delete port 2).

HDSL port parameters for TDM service

Use the following parameters to configure an HDSL port for T0 TDM service:

Parameter	Value
DS1 Format (required)	Set to ESF or SF per your site requirement.
Line Power	Set to SINK (default) or SOURCE per your site requirement.
Grade of Service	Set to OFF (default), DEFLT, or a pre-defined grade-of-service profile number, per your site requirement.
Line Type	Set to 2WIRE (default) or 4WIRE.
Terminal Type	Set to COT (default).
Signal-to-Noise Ratio Margin Threshold (near-end)	Set to a value from 1 to 15 (or set to 0 to disable) per your site requirement.
Loop Attenuation Threshold (near-end)	Set to a value from 1 to 127 (or set to 0 to disable) per your site requirement.
DS1 Map	Set to SEQ.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Create T0 Timeslot Cross-Connections

Creating HDSL cross-connections for T0 TDM (fractional T1) service is described below.

Related topics

- *View a List of Cross-Connections and Hops* (on page 126)
- *Delete Cross-Connects and Hops* (on page 134)

Cross-connection endpoints for HDSL TDM services

One end of an HDSL cross-connection that is configured for TDM service must be connected to an HDSL timeslot. The other end can be an HDSL timeslot, a T1 timeslot, or a DS0 port.

See also

- *Configure DS1 Ports for TDM Service* (on page 386)
- *Configuring Universal Services* (on page 452)
- *Configuring Non-Switched Services* (on page 459)

Cross-connection parameters

Cross-Connect Parameter	Default Value
Connection Type	2WAY
Number of signaling bits (NSG)	4
Number of DS0s (NDS0)	1
Nailed Up	N

Note: For T0 data service (such as ISDN and DDS), it is recommended to set the Number of signaling bits (NSG) to 0.

To create a T0 TDM cross-connection

1. On the Navigation Tree, click a port where a cross-connection is to be created.
2. In the Work Area, click **Timeslot Cross Connect**.
3. On the toolbar, click **Create** > **T0 Cross Connect** to open the Select Cross-Connect Endpoints dialog box.
4. In the Source area of the dialog box:
   a. In the Shelf list, select the shelf where the source port is located.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

b. In the Type list, click a service type: **HDSL Timeslot**, **T1 Timeslot**, **T0**, or **T0 (DDS)**.

c. (T0 or T0 (DDS) service only) In the Slot list, select the slot for the card to use for the cross-connection.

d. In the list of ports, select the source port for the cross-connection.

e. (HDSL and T1 Timeslot only) In the T1 Timeslot box, type the number of the timeslot to use for the cross-connection.

f. Click **SRC** to move the port to the Cross-Connects To Be Created area.

5. In the Destination area:

a. In the Shelf list, click the shelf where the destination port is located.

b. In the Type list, click a service type: **HDSL Timeslot**, **T1 Timeslot**, **T0**, or **T0 (DDS)**.

c. (T0 or T0 DDS only) In the Slot list, select the slot for the card to use for the cross-connection.

d. In the list of ports, select the destination port for the cross-connection.

e. (HDSL Timeslot or T1 Timeslot only) In the T1 Timeslot box, type the number of the timeslot to use for the cross-connection.

f. Click **DEST** to move the port to the Cross-Connects To Be Created area.

6. In the IDT Route area, specify all internal T1 transport groups along the cross-connection in order from source to destination:

a. In the Shelf list, select the shelf with the internal transport group.

b. In the available transport group list, select the transport group.

c. Click **IDT** to move the transport group to the Cross-Connects To Be Created area.

d. Repeat Step 6 for each additional internal T1 transport group.

7. Repeat Steps 4 through 6 for each additional cross-connection that you are creating.

8. Set the Required Parameters to match your configuration (or leave them blank to accept the default values).

9. Click **OK** to save your cross-connections.

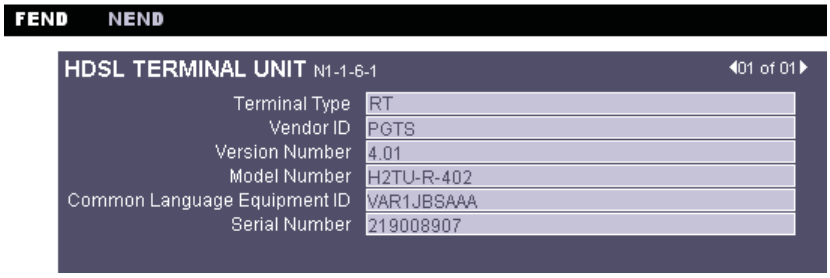
Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Viewing HTU

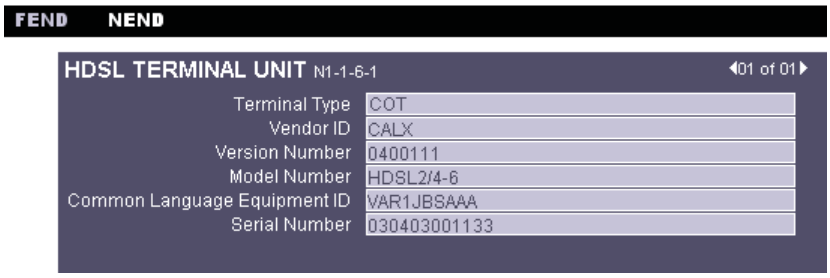
A C7 HDSL2 port works in conjunction with HDSL Transceiver Units (HTUs) to establish HDSL transmissions at the T1 data rate. Follow the steps below to view basic HTU data.

To view HTU information

1. On the Navigation Tree, click the HDSL port that is connected to the HTU-R (remote) unit.
2. In the Work Area, click the **FEND** tab to view HTU-R information.



3. In the Work Area, click the **NEND** tab to view HTU-C (central office) information.



Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Chapter 15

Provisioning PWE3 Services

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Overview of the Calix C7 PWE3 Solution

PWE3 is a standards based (RFC3916) mechanism that emulates the essential attributes of Frame Relay, Asynchronous Transfer Mode (ATM), Ethernet, Time Division Multiplex (TDM), and Synchronous Optical Networking / Synchronous Digital Hierarchy (SONET/SDH) over a Public Switched Network (PSN) using Internet Protocol (IP) or Multi-protocol Label Switching (MPLS) transport. This robust solution offers high density, 1:N protected T1 pseudowire aggregation for B-Series, E-Series, and P-Series products.

A Pseudowire connects two TDM circuits over a packet switched Ethernet network. In the most basic example, two T1 endpoints are connected together, converting a T1 signal into Ethernet frames and transported over an asynchronous Ethernet network. On the receiving end, the Ethernet frames are converted back to TDM T1 signaling. This technology is often referred to as **P**seudo**W**ire **E**nd-to-End Emulation, or **PWE3**.

T1 TDM transport benefits from it's inherit internal signal timing mechanism. Ethernet packet networks however do not have this same timing mechanism (asynchronous delivery) so PWE must accommodate this disparity via other methods. Using the Calix solution, timing is recovered using adaptive or differential clock recovery algorithms using Structure-Agnostic TDM over Packet (SAToP) encapsulation or Circuit Emulation Service over Packet Switched Network (CESoPSN) which are both discussed in detail in a later section.

In addition to delivering end to end T1 service, the C7 provides a TDM voice switch interface which can be used for aggregating T1s originating from any Calix Unified Access endpoint. Platforms supported include the E7-2 or E7-20 GPON or AE OLT or the B6 AE OLT solution with various ONT models.

Pseudowire Encapsulation Types

There are two types of PWE3 encapsulation for the C7 platform, each with its own advantages.

PWE3 Encapsulation Types		
TDM PW Type	**TDM Service Supported**	**Comments**
SAToP (RFC4553)	Unframed	For Transport of Clear Channel/High CAP T1 services
CESoPSN (RFC5086)	Framed, Channelized	For Transport of Fractional T1 services (DDS, ISDN, Fractional T1 data)

Two C7 line cards are available for delivering aggregated T1 services over an All IP network using the PWE3 architecture.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

PWE Card Descriptions

The Calix C7 PWE cards support integrated Bit Error Rate Test (BERT), high-density GR-303, and span powering of T1 repeaters. Both cards provide the same software features and functionality and are fully interchangeable. Each card differs only at the physical layer, including differences in port density and the T1-8 PWE cards repeater powering support.

Each card provides the following pseudowire services:

- Standards based PWE3 support (per port)
- SAToP or CESoPSN transport
- Adaptive and Differential Timing Modes
- Supports PWE3 service interoperability with the Calix B6 using 766GX running in Active Ethernet mode

In addition, each card supports the following TDM Services (via multiprotocol)

- Standards based TDM support (per port)
- GR-303, GR-08 Mode I or II, and D4 Switch Interface for voice services
- Unstructured Hi-Cap services and Channelized DS0 services (per port)
- Structured Service (Non-switched special circuits, Fractional T1 services)
- T1 Transport (T1-TG) in SONET or Ethernet transport networks
- Compatible with RAP-10GE or with any previously released multi-protocol RAPs

The Calix PWE3 solution also includes the following carrier robustness and troubleshooting tools:

- 1:1 Equipment Protection Scheme (EPS) and 1:N EPS (N=1, 4 or 9)
- Integrated Bit Error Rate Test (BERT)
- Loop Code Detection (Inband Loopback)
- Repeater Powering (T1-8 PWE only)

Note: C7 Release 8.0 provides TDM support for T1s in a GPON environment served by 74xGE and 766GX ONTs. End-to-End PWE3 support for C7 GPON ONTs will be supported in a future release.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

DS1-12 PWE card

The EXA powered DS1-12 PWE line card provides 12 DSX-1 Hi-Cap, asynchronous interfaces or synchronous interfaces per card. Each DS1 interface can be individually configured to support synchronous (DS0 visible) or asynchronous (Hi-Cap) interfaces in either TDM or Pseudowire mode. The card can be deployed in GR-8 (mode 1 or 2), GR-303 to a Class 5 switch, as a subscriber interface, or as a network interface device.

The DS1-12 PWE card can be inserted into any of the 20 universal slots in the C7 shelf. Physical access to each DS1 interface is provided through standard 25-pair RJ-21 connectors mounted on the back of the C7 shelf. The card provides up to 240 DS1 terminations per shelf.

T1-8 PWE card

The C7 EXA powered T1-8 PWE card provides 8 line-powered or 8 non-powered DS1 interfaces. Each card can be individually configured to support synchronous (DS0 visible) or asynchronous (Hi-Cap) interfaces in TDM or Pseudowire mode. Each T1 interface provides -130 VDC @ 60 mA power for up to 7 repeaters. When used on DS1 interfaces, link powering can be turned off to provide DSX-1 level outputs. The T1-8 PWE card can be deployed in GR-8 (mode 1 or 2), or used as a GR-303 interface to a Class 5 switch, inter-terminal transport, subscriber interface, or network interface.

The T1-8 PWE card can be inserted into any of the 20 universal slots in the C7 shelf. Physical access to each DS1 interface is provided through standard 25-pair RJ-21 connectors mounted on the back of the C7 shelf. The card provides up to 160 T1s per C7 shelf with repeater powering support on each port.

The repeater power feature supports up to 7 repeaters at a distance of up to 5k ft between repeaters (at -130 VDC, 60 mA).

T1-8 PWE Card Power Consumption	
Function	**Power Consumption**
DSx Level Output	16 Watts
Powered T1	3.875 Watts each additional
Total	47 Watts maximum/card

Note: DS1-12 PWE and T1-8 PWE line cards function with any multi-protocol Calix RAP card. When used in a multi-protocol environment, a GE card is also required in the same C7 shelf to interface to an E5 or E7 transport device.

Note: The DS1-12 PWE and T1-8 PWE cards support carrier grade fail over protection for these carrier services. Both cards support 1:1 and 1:N equipment protection schemes.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

PWE3 Timing and Clock Recovery Considerations

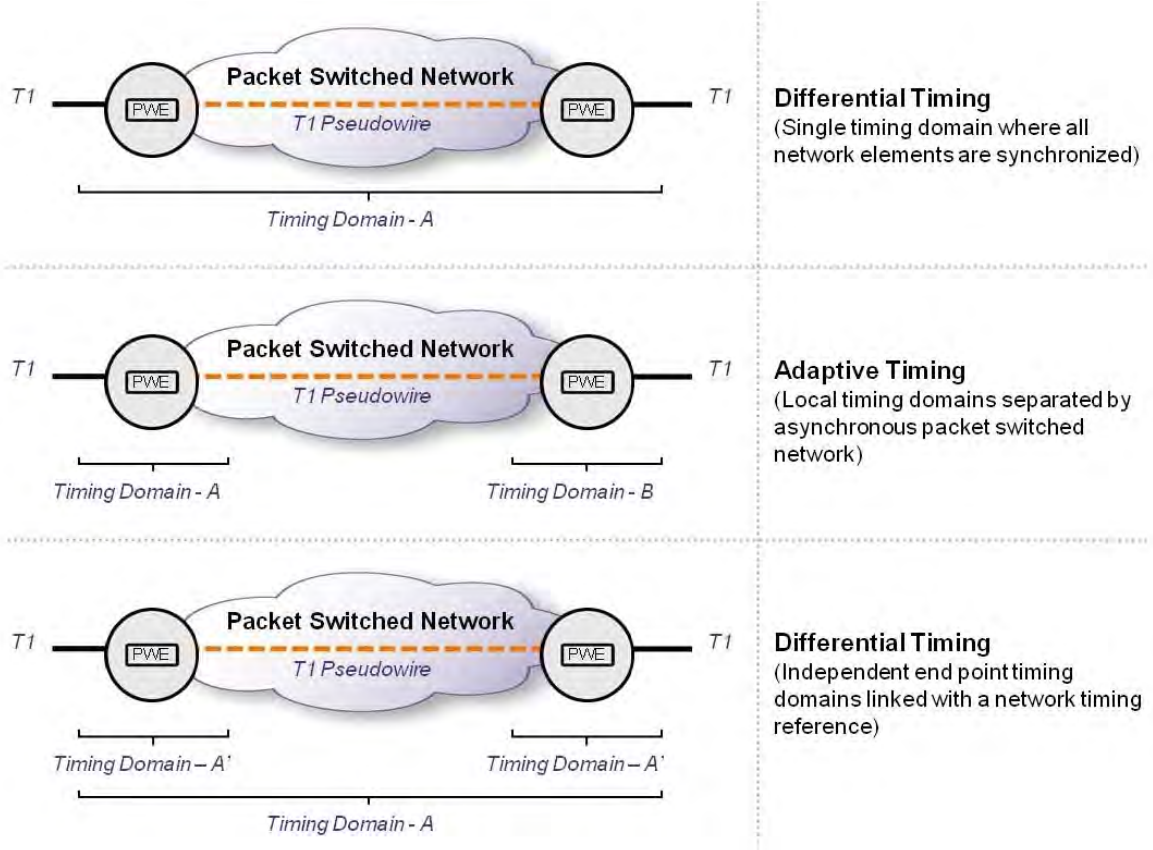
Ethernet networks handle system clocking different from SONET networks. SONET networks require that each node recovers its timing off of the previous node. Thus, any node in the system can trace its timing back to the Central Office Terminal (COT) and the network clock is considered "traceable." In the case of T1 service, having a traceable network clock means that the T1 service clock at any given node is the same as any other node.

In an Ethernet network each node may have its own timing source, thus the network clock may not be traceable from one location to the next. Given this lack of traceability, the T1 service clock is no longer guaranteed to be the same at different nodes. The receiver's service clock now needs to be recovered using timing information stored inside the Ethernet frame. The DS1-12 PWE and T1-8 PWE line units support Adaptive Clock Recovery, Differential Clock Recovery, Source and Loop timing.

- Adaptive Clock Recovery – This method uses the average arrival time of the packets to derive the transmitter's clock. This is possible since the source device is producing bits at a constant rate determined by its clock. By averaging the arrival times, the Packet Delay Variance (PDV) can be negated and the original sender's clock recovered.
- Differential Clock Recovery – This method employs a residual timestamp at the sender based on the difference between the shared reference clock and the T1/DS1 line. Thus, the receiver utilizes the timestamps in the received frames against its own time reference to correctly adjust its own T1 line timing. When a traceable clock is available between the two devices, this mechanism will produce lower jitter than adaptive clock recovery.
- Source Timing - Source timing is act of using a local source clock as the timing reference. This local source may be an injected clock via a BITS interface; derived from the PON, or directly from a different received T1 (GR-303 line, etc.)
- Loop Timing - Loop timing entails looping the received T1 clock back, using it to time the T1 transmissions.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

The figure below shows the relationship between network reference clock and the use of differential and adaptive timing methods for service clock recovery.



The advantage of adaptive clock recovery is that it does not require a traceable clock source at both locations of the T1 circuit. This solution covers deployments that contain any combination of asynchronous and synchronous T1 services where greater delay and jitter can be accommodated.

T1 Pseudowire planning guidelines:

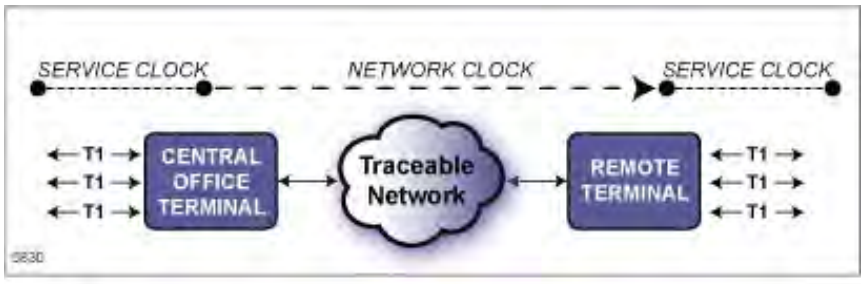
- Within a Layer 2 network, T1 services from a remote PWE line unit are typically placed in a single VLAN for transport between the remote pseudowire devices and the IP gateway. Multiple remote locations may be split into separate VLANs for ease of network planning and operation if desired.
- Transport of T1 services over a packet network requires a CoS priority and sufficient bandwidth allocation within the packet network to reduce latency and packet loss. T1 service VLANS should be given a high 802.1p priority "p-bit" value.
- Each Calix C7 line unit is provisioned with a static IP address for the SAToP interworking function (an IP host). Each T1 pseudowire end point thus has a unique source and destination IP address corresponding to the line unit with a UDP port ID for the individual T1 circuit on the card. Alternatively, the end user may choose to assign a single IP Host to a PWE card and unique UDP per port.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Synchronization of PWE3 Timing

As telecom operators seek to lower costs by switching from legacy SONET networks to IP based Ethernet networks, Ethernet-based TDM solutions such as PWE3 are gaining increasing significance. Of great concern is the difference in "system clocking" technologies used between SONET and Ethernet networks:

- **SONET Networks** - SONET networks require that each node recovers its timing off of the previous node. In other words, any node in the system traces its timing back to the Central Office Terminal (COT) and the network clock is considered “traceable.” In the case of T1 service, having a traceable network clock means that the T1 service clock at any given node is the same as any other node.
- **Ethernet Networks** - Ethernet networks do not have the same strict clocking requirements as SONET networks. In an Ethernet network, each node may have its own timing source (thus the network clock may not be traceable). Given this lack of traceability, the T1 service clock is no longer guaranteed to be the same at different nodes. The receiver’s service clock must now be recovered using timing information stored inside the Ethernet frame. As the network expands, the packets may be re-timed at each node. Larger networks may also have more traffic congestion which causes additional routing delay. These delays complicate the clock recovery algorithm and at some point, simple recovery is no longer possible. When this occurs, a timing protocol or traceable clock must be extended to each end point of the T1 pseudowire.



Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

PWE3 Timing Recommendations

Depending on the desired services, Calix recommends adopting the following timing methods. The chart below provides information on where the C7 is located in the network and what timing method to use on each end of the circuit.

Timing Recommendations for Unstructured Services				
Deployment Scenario		**Recommended Timing Method**		
PWE Network Side	**PWE Subscriber Side**	**Network Side Timing**	**Subscriber Side Timing**	**T1 Terminating Device Timing**
Location with traceable clock	Shared traceable clock as network interface	Loop	Differential	Loop
Location with traceable clock	Location without traceable clock (such as 10GE fed Remote Terminal)	Loop	Adaptive	Loop
Location without traceable clock (such as 10GE fed Remote Terminal)	Same shelf or Central Office/Remote Terminal as network interface	Loop	Adaptive	Loop
Location without traceable clock (such as 10GE fed Remote Terminal)	Another location without traceable clock (such as 10GE fed Remote Terminal)	Loop	Adaptive	Loop
Location with traceable clock	Shared traceable clock from network interface	Differential	Differential	Unknown
Location with traceable clock	Location without traceable clock (such as 10GE fed Remote Terminal)	Adaptive	Adaptive	Unknown
Location without traceable clock	Same shelf or Central office/Remote Terminal as network interface	Adaptive	Adaptive	Unknown
Location without traceable clock	Another location without traceable clock	Adaptive	Adaptive	Unknown

Timing Recommendations for Structured Services			
Deployment Scenario		**Recommended Timing Method**	
PWE Network Side	**PWE Subscriber Side**	**Network Side Timing**	**Subscriber Side Timing**
Location with traceable clock	Shared traceable clock as network interface	Source	Source

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

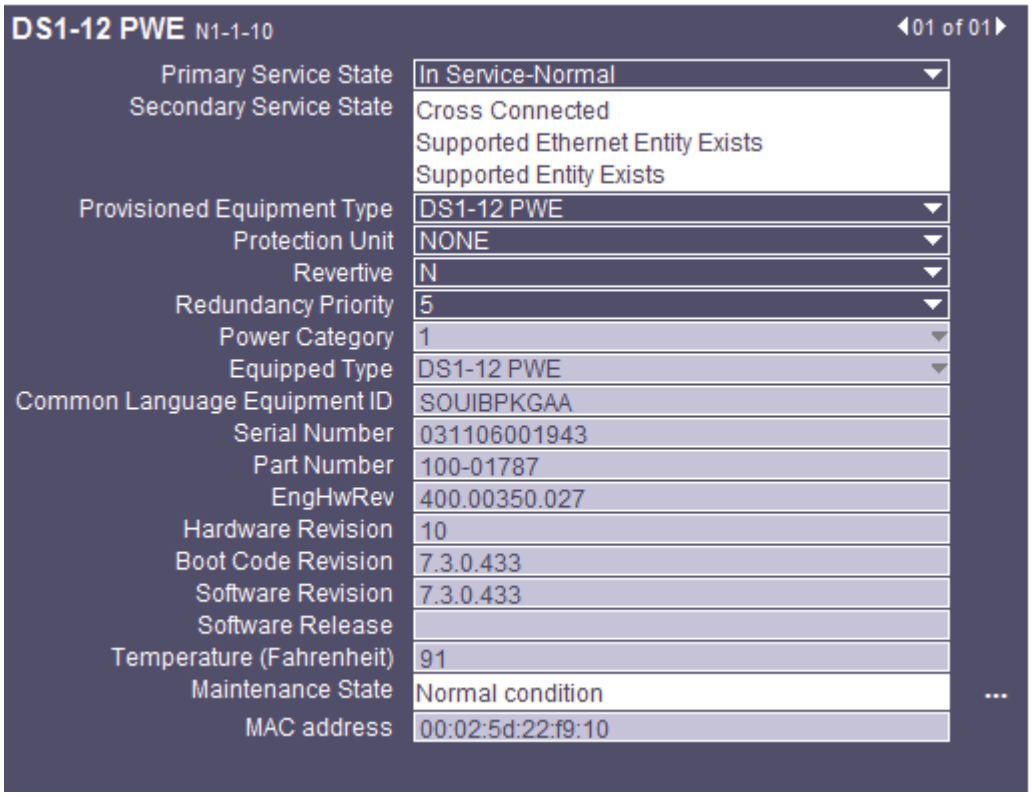
General Notes on Timing Options

- Loopback - Differential Timing mode provides the lowest wander at Network/Central office end of PWE.
- Differential = Differential mode provides the lowest latency.
- For Unstructured services, valid timing modes are source, loop, adaptive, or differential.
- For Structured services, both T1 endpoints must be set to source timing.
- Use of differential timing mode on the subscriber side assumes that both subscriber and network interfaces are within the same timing domain.
- When loop timing is used at the central office (network side), any T1 terminating equipment at the far end (customer side) must also use loop timing.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

PWE Card Settings

Once installed in the C7 shelf, CMS displays the following inventory information for either the DS1-12 PWE or T1-8 PWE card:



PWE Card Setting Field Descriptions		
Field Name	**Field Description**	**Field Type**
Primary Service State	Indicates the service state that the port transitions to after you execute a provisioning command.	alpha - drop down list
Secondary Service State	Provides additional state information of the port.	alpha - drop down list
Provisioned Equipment Type	During card creation, the card type can be pre-provisioned for assignment to a given C7 chassis slot.	alpha - drop down list
Protection Unit	If a 2nd card of the same type is used within the C7 chassis, you can specify which slot will serve as the protection unit.	None or slot location of protection unit (N1-1-x)
Revertive	In 1:1 protection schemes, Reversion allows for traffic to switch back to the original working card once the failure condition clears. The Revertive (RVRTV) parameter controls this capability. For 1:N protection, reversion is required. Use the Redundancy Priority (RNPRTY) parameter to prioritize specific working cards for protection within a group by assigning priority numbers.	Yes or No Y=revertive N=non-revertive

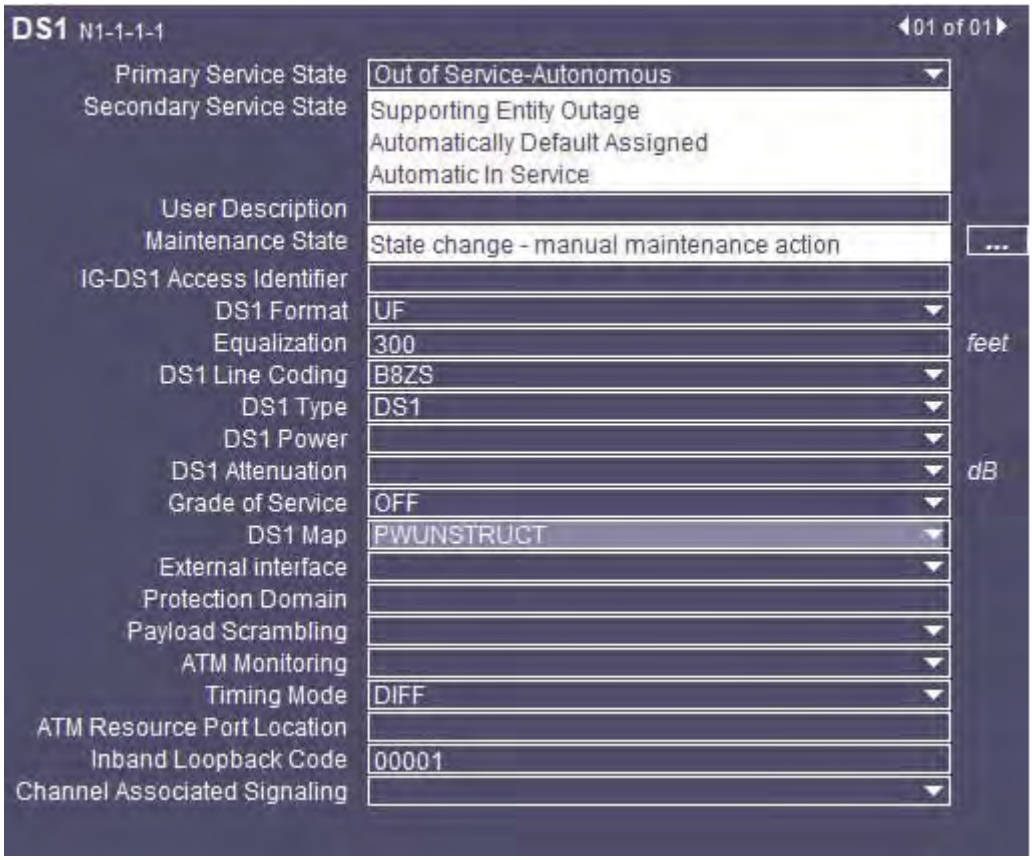
Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

PWE Card Setting Field Descriptions		
Redundancy Priority	Used in 1:N protection schemes only, cards in a protection group can be given a priority as to which protection unit is brought online in a protection switch condition. . It gives the priority of this working equipment versus other working equipment protected by the same protection card. Equipment given a smaller RNPRTY number pre-empts any protection already in effect for equipment given a larger RNPRTY number. When equipment fails with the same RNPRTY number as the already protected equipment, no protection switch will occur.	numeric (1-9)
Power Category	The system minimizes power dissipation during power failure (battery backup). Following power failure the system enters power-save mode. Upon entering this mode, the C7 turns off the PWE3 cards. The period in which the system enters power-save mode after a power failure is provisionable. Three power categories are created: Category 1 cards that do not get shut down during battery backup (AC power failure). Category 2 cards that get shut down after 2 hours. Category 3 cards that get shut down after the period of time specified by PWRCAT3 (up to a maximum of 30 minutes). The system defaults are that POTS, DS1, PWE3, DS3, and optics are category 1 and ADSL are category 3. Presently, no Category 2 cards are supported.	Numeric (1-3)
Equipped Type	Indicates the exact type of equipment plugged into the slot. If the Equipped Type doesn't match the Provisioned Equipment Type, an equipment mismatch alarm is raised.	Auto-populated
Common Language Equipment ID	CLEI code for the equipment type installed.	Auto-populated
Serial Number	The serial number of the card.	Auto-populated
Part Number	The Calix part number of the card.	Auto-populated
EngHwRev	Existing hardware revision level of the card.	Auto-populated
Hardware Revision	Hardware Revision running on the Card	Auto-populated
Bootcode Revision	Firmware bootstrap revision for the card.	Auto-populated
Software Revision	If used, the software revision running on the card (for example, R10).	Auto-populated
Software Release	Software Release Number (for example, 8.0.0)	Auto-populated
Temperature (Fahrenheit)	The internal temperature of the card.	Integer, Auto-populated
Maintenance State	The current maintenance state of the card.	Integer, Auto-populated
MAC Address	The assigned MAC Address of the card.	Mac Address 00:00:00:00:00:00

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

PWE Card Port Settings

The following options are configurable for each PWE T1 Port to be provisioned.



PWE Port Setting Field Descriptions		
Field Name	**Field Description**	**Values**
Primary Service State	Indicates the service state that the port transitions to after you execute a provisioning command.	OOS (Out of Service) IS (In Service)
Secondary Service State	Provides additional state information of the port. Varies dependent upon Primary Service State	Varies based on PSS.
User Description	The user description field.	alphanumeric
Maintenance State	Displays any standing conditions currently affecting the port. If you are viewing the port in Form View, click the ellipsis button to the right of the Maintenance State field to view a list of possible conditions.	N/A
IG-DS1 Access Identifier	The address of the DS1 within the interface group. The format of a DS1 identifier for a GR-303 or T1TG group is (Node Id)-(Shelf #)-(IG Id)-(DS1 #). The format of a DS1 identifier for a GR-8 interface group is (Node Id)-(Shelf #)-(Slot #)-(IG Id)-(DS1 Identifier).	Platform specific

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

PWE Port Setting Field Descriptions		
DS1 Format	Specifies the DS1 signal format: **ESF** (Extended Superframe): ESF is used for voice services such as GR-303 or fractional T1. **SF** (Superframe): SF is used for fractional T1 or D4 voice service. **UF** (Unframed): UF is used for Hi-Cap service.	UF ‡, ESF, SF
Equalization	Specifies the attenuation distortion equalization setting (line build-out) for the port in feet. This parameter applies only when the DS1 Type is DS1.	1-655 feet 300 feet ‡
DS1 Line Coding	Specifies the DS1 line coding of a port: **AMI:** alternate mark inversion coding **B8ZS:** bipolar with 8 zero substitution coding	B8ZS ‡, AMI
DS1 Type	Designates the port as a DS1 or a T1 port: DS1 is typically specified for cross-office connections. T1 is typically specified for long-haul transmissions. **Note**: Ports on the DS1A-12 card support only the DS1 signal type.	DS1 ‡, T1
DS1 Pwr	T1 only. Configure the DS1 Powering method per site requirements. If Source is chosen, -130 V is provided on the T1 line.	Sink ‡, Source
DS1 Attn	T1 only. Set the amount of attenuation needed on the T1 line. Attenuation can be added in increments of 7.5 dB	0.0 db ‡, -7.5 dB, -15 dB, -22.5 dB
Grade of Service	Uniquely identifies one entry in the Grade of Service table that contains the performance parameters and their associated threshold values that apply to the DS1 port.	OFF ‡, ON
DS1 Map	Designates how the payload signal at a specific port maps to a DS1 frame: **N/A:** No mapping is performed at the port. **NNI:** ATM network-to-network interface. Not applicable in PWE3 environment. **UNI:** ATM user-to-network interface. Not applicable in PWE3 environment. **SEQ:** Specified so that DS0 numbering occurs with the DS0 number equal to the time slot number. **PWUNSTRUCT:** Unstructured (clear-channel) T1 service in PWE33 SAToP packet format (RFC 4553). **PWSTRUCT:** Structured service (Fractional) T1 service in PWE33 CESoPSN packet format (RFC 5086).	PWUNSTRUCT ‡, N/A, NNI, UNI, SEQ, PWSTRUCT
External Interface	Not applicable in PWE environment Indicates whether or not the DS1 port represents an external path through the network. The value should be set to **Y** (Yes) when the port is an external interface. It should be set to **N** (No) when the port is connected to other shelves within a network of C7s. This parameter applies when the DS1 Map is set to NNI.	Yes or No Null ‡
Protection Domain (PDOM)	A unique integer that associates a transport facility into a protection domain that is used for A to Z connection provisioning. The PDOM for each domain must be a unique non-zero integer. The value of 0 indicates that the facility is not to be used for A to Z connections.	integer

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

PWE Port Setting Field Descriptions		
Payload Scrambling	Not applicable in PWE environment. Configures whether to enable or disable the scrambling of ATM cells. This parameter applies when the DS1 Map is set to UNI or NNI.	Yes or No
ATM Monitoring	Not applicable in PWE environment. Set to **Y** (Yes) to enable ATM diagnostic monitoring on the STS path. If enabled, an ATM OAM loopback ping is injected on VP0-VC3 to verify point-to-point connectivity with the next line unit. It applies only to ATM NNI and ATM UNI interfaces. The default value is Y for internal interfaces and N for external interfaces.	Yes or No Default is environment specific
Timing Mode	Indicates the timing source for the DS1 port transmit signal: **LOOP:** T1 transmission timing is derived from the far-end device recovered timing. Loop timing is independent of shelf timing. Applies to PWE3 service only. For traditional T1 service, refer to ATM Clock Recovery Methods. **SOURCE:** T1 transmission timing is derived from the C7 system timing. **ADAPT**: This method uses the average arrival time of the packets to derive the transmitter's clock. This is possible since the source device is producing bits at a constant rate determined by its clock. By averaging the arrival times, the Packet Delay Variance (PDV) can be negated and the original sender's clock recovered. **DIFF**: This method employs a residual timestamp at the sender based on the difference between the shared reference clock and the T1/DS1 line. The receiver uses the timestamps in the received frames against its own time reference to correctly adjust its own T1 line timing. When a traceable clock is available between the two devices, this mechanism produces lower jitter than adaptive clock recovery.	DIFF ‡, LOOP, SOURCE, ADAPT
ATM Resource Port Location	Not applicable in PWE environment. The AID of the associated DS1 port.	
Inband Loopback Code	PWE Cards only. If the inband code is detected in the egress direction, a terminal loopback is automatically performed on the DS1 port. If the inband code is detected in the ingress direction, a facility loopback is automatically performed on the DS1 port.	00001 ‡
Channel Associated Signaling	Enables or disables whether signaling bits are carried in the TDM data, as well as in the signaling substructure. This parameter affects all pseudowires on the port.	Yes, No Null ‡

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

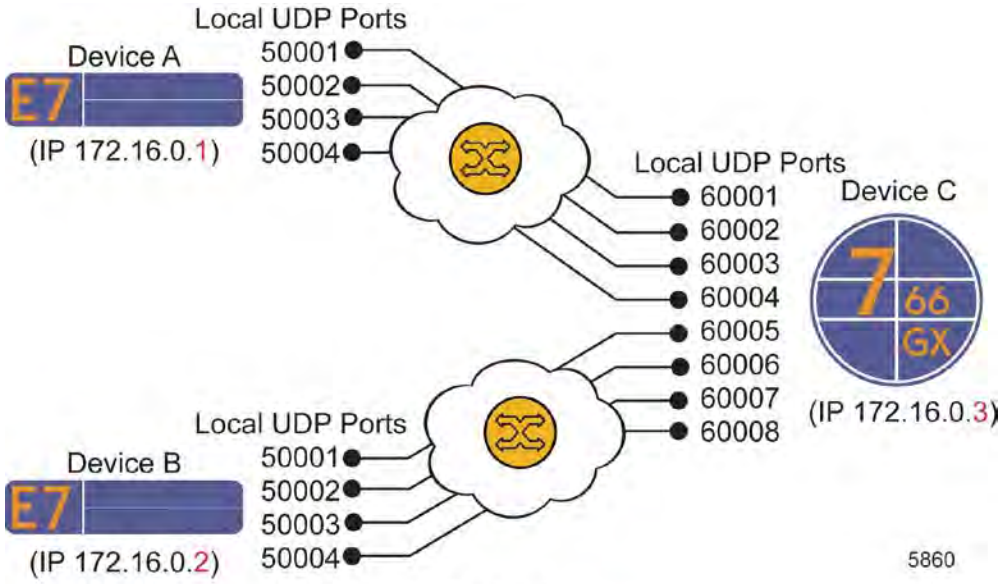
UDP Port Settings

In a properly configured system, the combination of an IP address and UDP port number uniquely identifies the pseudowire (known as the pseudowire "label"). This information is associated with the physical T1 port and directs the pseudowire payload to the proper T1 (TDM) port with the combination of the IP address and the UDP port number being unique for each circuit. The UDP port number must be agreed upon by both ends of the pseudowire such that each local device has to point to the correct Remote IP/UDP port.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

In the diagram below, an appropriate UDP port number scheme is shown. Notice that the local UDP port values repeat themselves from device to device however the far end values (766GX ONT) remain unique.

Note: Care must be taken when aggregating pseudowires from multiple devices to a single device (as in the example below) such that each pseudowire is uniquely "labeled".



Device A
IP Address 172.16.0.1

T1 Port 1 = Local UDP Port 50001 - Maps to Remote IP 172.16.0.3 UDP Port 60001
T1 Port 2 = Local UDP Port 50002 - Maps to Remote IP 172.16.0.3 UDP Port 60002
T1 Port 3 = Local UDP Port 50003 - Maps to Remote IP 172.16.0.3 UDP Port 60003
T1 Port 4 = Local UDP Port 50004 - Maps to Remote IP 172.16.0.3 UDP Port 60004

Device B
IP Address 172.16.0.2

T1 Port 1 = Local UDP Port 50001 - Maps to Remote IP 172.16.0.3 UDP Port 60005
T1 Port 2 = Local UDP Port 50002 - Maps to Remote IP 172.16.0.3 UDP Port 60006
T1 Port 3 = Local UDP Port 50003 - Maps to Remote IP 172.16.0.3 UDP Port 60007
T1 Port 4 = Local UDP Port 50004 - Maps to Remote IP 172.16.0.3 UDP Port 60008

Device C
IP Address 172.16.0.3

T1 Port 1 = Local UDP Port 60001 - Maps to Remote IP 172.16.0.1 UDP Port 50001
T1 Port 2 = Local UDP Port 60002 - Maps to Remote IP 172.16.0.1 UDP Port 50002
T1 Port 3 = Local UDP Port 60003 - Maps to Remote IP 172.16.0.1 UDP Port 50003
T1 Port 4 = Local UDP Port 60004 - Maps to Remote IP 172.16.0.1 UDP Port 50004
T1 Port 5 = Local UDP Port 60005 - Maps to Remote IP 172.16.0.2 UDP Port 50001
T1 Port 6 = Local UDP Port 60006 - Maps to Remote IP 172.16.0.2 UDP Port 50002
T1 Port 7 = Local UDP Port 60007 - Maps to Remote IP 172.16.0.2 UDP Port 50003
T1 Port 8 = Local UDP Port 60008 - Maps to Remote IP 172.16.0.2 UDP Port 50004

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

From a practical standpoint, Calix recommends that UDP port numbering schemes are consistent throughout your network. For example:

UDP Port Number Range	Application
10001-10024	Reserve for Use with T1 Port 1
10101-10124	Reserve for Use with T1 Port 2
10201-10224	Reserve for Use with T1 Port 3

By implemented a consistent numbering scheme, you can readily determine the intended destination of the device simply by viewing its UDP port number.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

PWE3 Application Architecture

In the following section, high level architecture drawings are provided to help familiarize plant engineers with the network topology. PWE3 applications can be broken down into two distinct models:

- Hi-Cap Service Delivery (Unstructured T1 Service over SAToP)
- Fractional T1 Service Delivery (Structured T1 Service over CESoPSN)

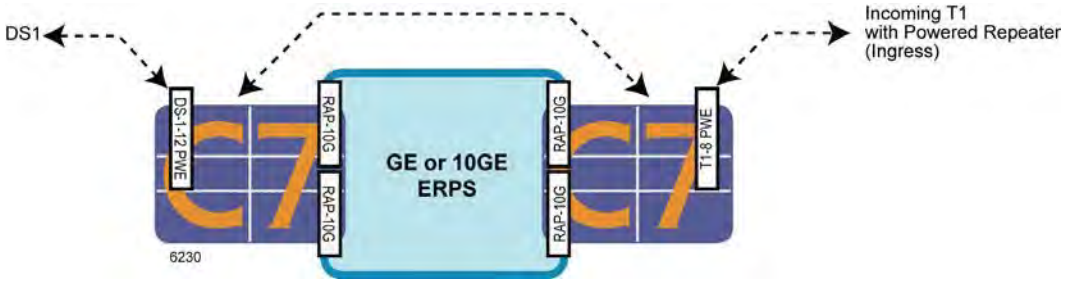
Hi-CAP Service Delivery

Hi-Cap Service over Ethernet Transport (SAToP)

In this basic PWE3 architecture, Hi-Cap end to end asynchronous 1.544 Mbps circuits are sent over Ethernet (SAToP). In this example, the TDM T1 circuit from the end user arrives at the C7 from the source (remote) and is converted to PWE by the T1-8 PWE card and carried via Ethernet packets over the existing RAP-10GE in the C7 shelf.

Note: This architecture is also supported when used in conjunction with an E5-400 or E7 transport hub.

Note: A DS1-12 PWE card could also be used at the remote end to accept the incoming T1 circuit.



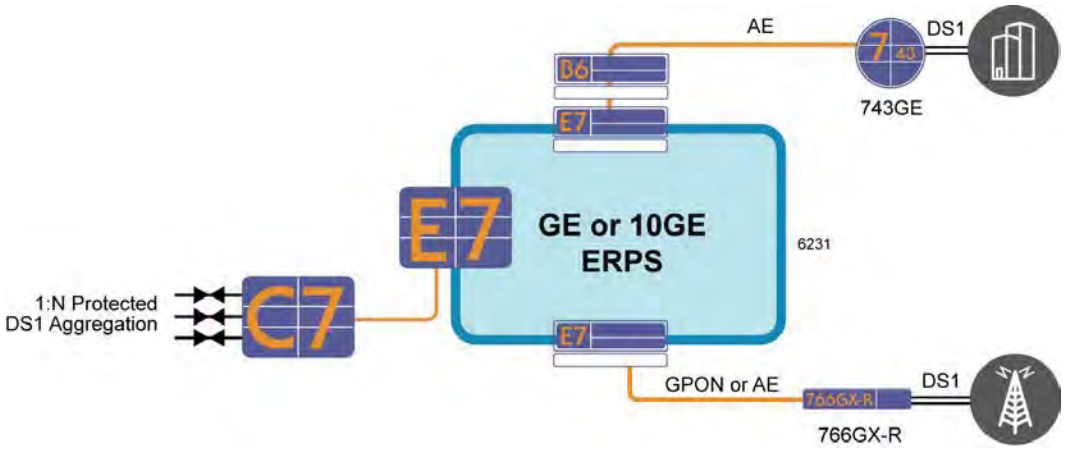
With the T1-8 PWE card, T1's over 6,000 feet from the TDM egress are also supported.

DS1 PWE3 Aggregation over Ethernet (SAToP)

The application below provides DS1 PWE3 Aggregation for packetized Ethernet traffic (SAToP). In this example, the TDM T1 circuit from the subscriber enters the Ethernet network from an AE or GPON ONT attached to an E7-20, E7-2, or B6 shelf and is aggregated into the CO via a stand-alone C7 shelf with a DS1-12 PWE card. In this configuration, up to 240 DS1 terminations can be processed and handed off to the network.

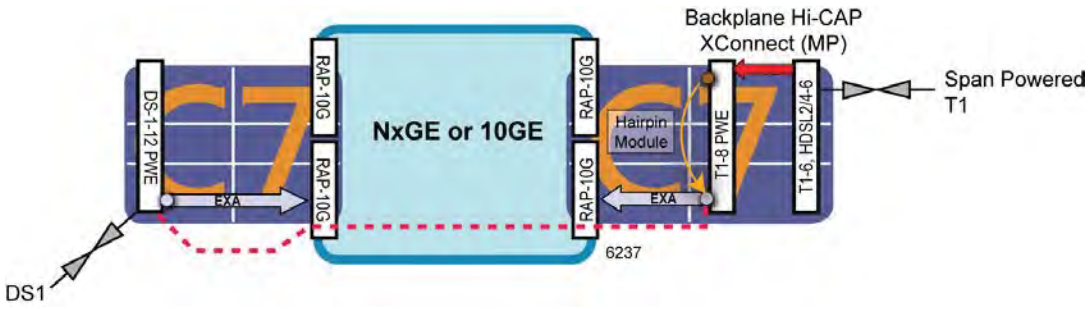
Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Note: The DS1-12 PWE equipped C7 shelf providing the aggregation function can be equipped with either a RAP-10GE or multi-protocol RAPs in this configuration.



Hi-Cap Service Delivery over Non-PWE3 Capable T1 Cards

In the example below, service delivery of existing (or new) T1 Hi-Cap circuits over packetized Ethernet (SAToP) can be configured for Non-PWE capable T1 line cards such as the T1-6 or HDSL2/4-6 card. In this configuration, individual T1's from these cards are cross-connected to a port on the PWE cards as traditional TDM Hi-Cap cross connects. Traffic from the port is physically connected to another port operating in PWE mode via an optional loopback module (also known as a Hairpin module). The PWE3 circuit then carries all traffic as PWE to the C7 shelf in the central office. The C7 terminates the PWE on the DS1-12 PWE card and delivers a traditional T1 circuit to the network.



The loopback (hairpin) module supports up to 12 interfaces and can be used on T1-8 PWE or DS1-12 PWE in this configuration. Since the PWE cards in this application support the conversion from TDM to PWE in lieu of non-PWE capable line cards, Calix recommends using the DS1-12 PWE card to maximize port count (per slot) since repeater powering (T1-8 PWE) is not needed in this configuration.

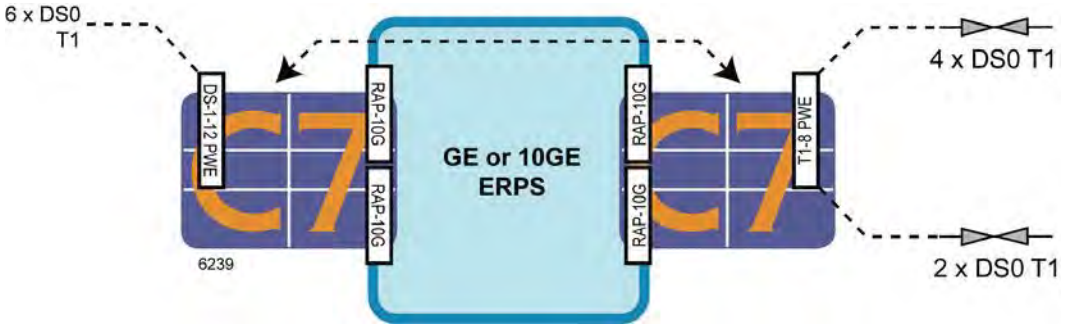
Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Fractional T1 Service Delivery

TDM Applications: Fractional T1 Circuit over Ethernet Aggregated by DS1-12 PWE3

Circuit Emulation Service over Packet Switched Networks (CESoPSN) is an architecture that supports transport of structured T1s across a Public Switched Network. Although this architecture has less tolerance for jitter/wander, a source timing schema is implemented to ensure trouble-free transport end to end.

Fractional T1 service delivery provides n x DS0 services to end customers requiring less than a full 1.544Mbps of bandwidth to a given location. The circuits can be used to deliver non-switched special circuits to the end customer and are carried over Ethernet transport via CESoPSN. Each T1 port on a DS1-12 PWE or T1-8 PWE supports up to (24) T1 timeslots for Fractional T1 services.



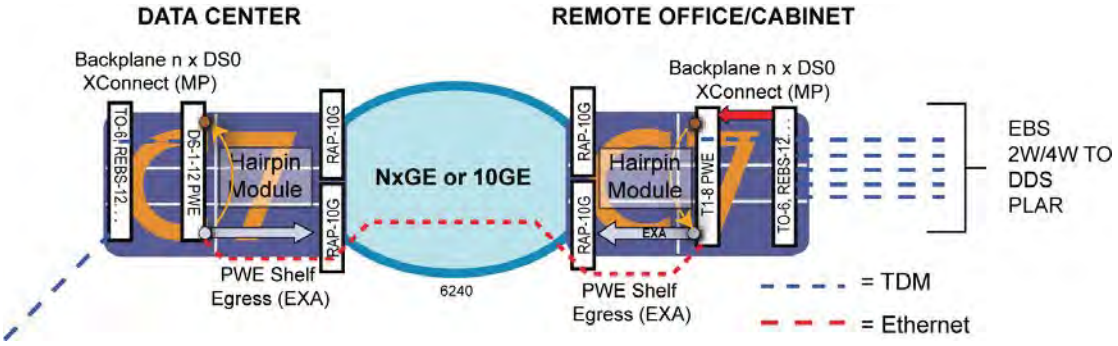
In the example above, the TDM Fractional T1 circuit from the end user ingresses into the T1-8 PWE cards and is transported over Ethernet back to the central office. The DS1-12 PWE card aggregates this Fractional T1 circuit for hand off as a non-switched fractional T1 interface. In this example, the T1-8 PWE card in the remote shelf is delivering 2 fractional services to an end user. The first is carrying (4) T1 timeslots, and the second is carrying (2) T1 timeslots. In the CO shelf, the DS1-12 PWE card aggregates these (6) T1 timeslots into a single T1 interface for delivery to the network. Alternately, a DS1-12 PWE card could also be used at the remote end to ingress the T1 circuit.

Note: T1 timeslots provisioned into a single PWE bundle must be contiguous. Non-contiguous timeslot allotment within a single PWE bundle is not supported.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

TDM Applications: Transport of DS0 Specials over Ethernet (CESoPSN)

Either of the C7 PWE cards can be leveraged to transport existing and new DS0 special circuits over Ethernet. Individual DS0's from special circuit cards, such as the REBS-12, TO-6, OCU-DP or RU2W-24 cards can be cross connected to a port on the PWE cards as a simple TDM T1 timeslot cross connect. All traffic from that port is then physically connected to another port operating in PWE3 mode via loopback (hairpin) module. The PWE3 port then carries all traffic as PWE to the C7 shelf in the central office and then converts the traffic back to TDM DS0s for transport on the network.



The loopback (hairpin) module supports up to 12 interfaces and can be deployed on either the T1-8 PWE or the DS1-12 PWE card in this environment.

Note: Use the DS1-12 PWE card whenever possible in order to maximize ports per C7 card slot (and where repeater powering is not required).

About the DS1/T1 Cross Connect Module

The cross-connecting of circuits described above is facilitated by the use of a Calix DS1/T1 Cross Connect module. This module terminates circuits via an Amphenol connector on the back of the C7 chassis by any PWE card populated slot.

From a port mapping perspective, the hairpin (cross-connect) module is configured as follows:

Port	Maps To Port	TDM Port	PWE Port
1	2	1	2
3	4	3	4
5	6	5	6
7	8	7	8
9	10	9	10
11	12	11	12

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

PWE Bundle Capacities

When deploying DS0 specials over Ethernet using a combination of Multiprotocol RAPs and GE Interfaces to E7 or E5 shelves, all PWE3 traffic is carried via a trunk VC built between the PWE card and the Ge-2P or GE-2E card. Each trunk VC supports up to 24 PWE bundles.

Note: The number of bundles supported per trunk VC is dependent on the number of T1 timeslots mapped to each bundle. The table below illustrates this relationship.

T1 Timeslots per PWE Bundle	PWE Bundles per Trunk VC
1	24*
2-12	16
12-24	12
* The 24 bundles per trunk VC capacity is achieved when all DS0s are set to one.	

If more than 24 PWE bundles are required from the PWE card, **additional trunk VCs must be created** to avoid traffic congestion (dropped packets). Calix recommends you build trunk VCs with a single bundle to carry the maximum 24 T1 timeslots. As additional T1 timeslots are added to the trunk VC, additional provisioning is not required on the PWE side. By doing so, you can avoid having to create additional trunks (with associated VLANs) on the same card, and ultimately avoids service disruptions when adding/editing VCs and DS0s.

Note: Internal logic is included in that a semantics check is performed when additional bundles are created that are not needed and/or creates a service degradation issue for existing subscribers.

In addition, PWE cards offer the following capacities:

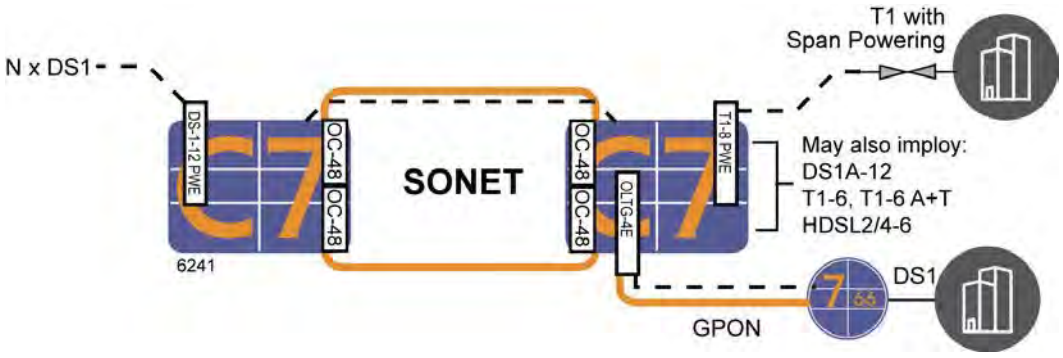
PWE Card Bundle Capacities				
Bundle Count	**Protocol Type**	**Timing**	**DS1-12 PWE card**	**T1-8 PWE card**
SAToP PWE Bundles Note: Each SAToP T1 uses a signal PWE bundle	Packet Sampling (Multiprotocol or EXA)	.5 ms	12 (per card)	8 (per card)
		1 ms	12 (per card)	8 (per card)
CESoPSN PWE Bundles Note: A single PWE bundle can support from 1-24 CESoPSN T1 timeslots.	Packet Sampling (Multiprotocol)	.5 ms	112 (per card) 24 (per Trunk VC with 1 DS0 per bundle) 16 (per Trunk VC with 2-12 DS0s per bundle) 12 (per Trunk VC with greater than 12 DS0s per bundle)	96 (per card) 24 (per Trunk VC with 1 DS0 per bundle) 16 (per Trunk VC with 2-12 DS0s per bundle) 12 (per Trunk VC with greater than 12 DS0s per bundle)

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

PWE Card Bundle Capacities				
		1 ms	208 (per card) 24 (per Trunk VC with 1 DS0 per bundle) 16 (per Trunk VC with 2-12 DS0s per bundle) 12 (per Trunk VC with greater than 12 DS0s per bundle)	192 (per card) 24 (per Trunk VC with 1 DS0 per bundle) 16 (per Trunk VC with 2-12 DS0s per bundle) 12 (per Trunk VC with greater than 12 DS0s per bundle)
	Packet Sampling (EXA)	.5 ms	136	120
		1 ms	240	192

TDM Applications: Hi-Cap Services

Hi-Cap service delivery provides an end to end asynchronous 1.544Mbps circuit to end users and is represented by the following diagrams for C7 networks:



In the example above, the TDM Hi Cap T1 circuit from the end user ingresses into the C7 network via copper feed at the T1-8 PWE or DS1-12 PWE card and on fiber via GPON T1 capable ONTs (for example, 766GX or 74xGE ONTs). The T1 circuit is then transported over SONET back to the central office and mapped to the DS1-12 PWE card for hand off into the network. This functionality is identical in design to the workings of the DS1A-12, T1-6, and HDSL 2/4-6 cards with respect to Hi-Cap transport. Circuits are AAL1 mapped across SONET transport and cross connected end to end in the other node. Note that the CSP can mix and match the PWE cards in the C7 along with the older cards for support of Hi-Cap circuits across SONET transport. In this example, all traffic traverses the multiprotocol switch fabric of the RAP-10GE or any of the older multiprotocol RAPs.

Note: The above configuration functions identically to that of the DS1A-12, T1-6, and HDSL 2/4-6 cards as it pertains to Hi-Cap transport.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

TDM Applications: Structured Services

In the following example, the TDM Fractional T1 circuit from the end user ingresses into the C7 network T1-8 PWE or DS1-12 PWE cards and is transported over SONET back to the central office. These DS0s are aggregated by the DS1-12 PWE card for delivery to the network as non-switched fractional T1 interfaces.

In this example, the T1-8 PWE card in the remote shelf is handing off 2 fractional services to an end user. The first is carrying (4) T1 timeslots, and the second is carrying (2) T1 timeslots. In the CO shelf, the DS1-12 PWE card aggregates these (6) T1 timeslots into a single T1 interface for handoff into the network. N x DS0 T1 timeslots are converted into the C7 backplane format and mapped across SONET transport and cross connected to their mating card in the opposite node. Note that the CSP can mix and match the PWE cards in the C7 along with the older cards for support of fractional T1 circuits across SONET transport. In this example, all traffic traverses the multiprotocol switch fabric of the RAP-10GE or any of the older multiprotocol RAPs.

Note: The above configuration functions identically to that of the T1-6 and HDSL 2/4-6 cards as it pertains to Fractional T1 services.

TDM Application: Local Hairpinning of Full T1 or T1 Timeslots (DACS)

In the example below, the T1 circuit from the end user ingresses into the C7 network T1-8 PWE or DS1-12 PWE cards and exits on a different port on the same card.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

In this example, the ability to cross connect Full T1 or T1 timeslots from port A to port B on the same card is new to the C7, and is enabled on the PWE cards with RAP-10GE or multiprotocol RAPs. Often referred to as a Digital Access Cross Connect (DACS) application, this service allows CSPs to digitally cross connect incoming fractional T1 circuits from one location to another, or an entire T1. The PWE cards enable this functionality on the same slot, preserving shelf capacity for other services.

TDM Applications: T1 Transport Groups (T1TG)

In the example below, a subtended C7 node is served by a T1 transport group on the T1-8 PWE card.

In this configuration, the T1-8 PWE card should be used for T1 Transport Group applications due to its ability to support repeater powering.

Note: Functionally, the DS1-12 PWE could be used as well with an external repeater shelf if desired.

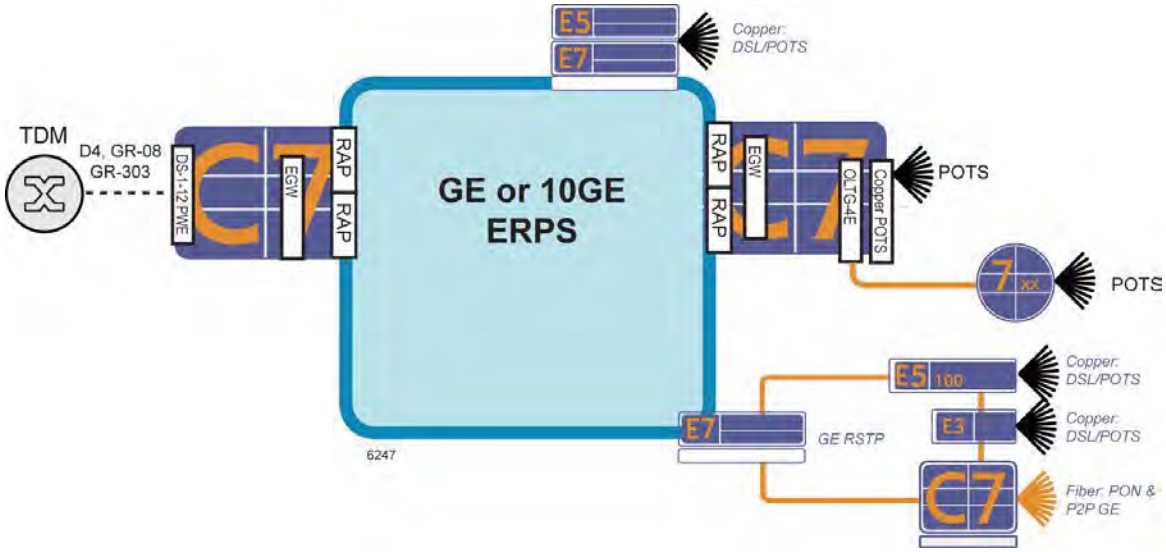
The use of the PWE cards for T1TG is supported via the multiprotocol interface to the RAP-10GE or legacy RAP cards. Long haul transport back to the main shelf in the central office is via standard SONET architecture. T1 transport group functionality on the PWE cards is identical to that of the T1-6 card and the same rules apply.

Note: When feeding a node with T1TG that also requires data services, an IMA-12 card is required for data services.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

TDM Application: Voice Switch Interface

n the example below, the PWE cards are serving as a TDM voice switch interface for Calix POTS interfaces over copper or fiber.



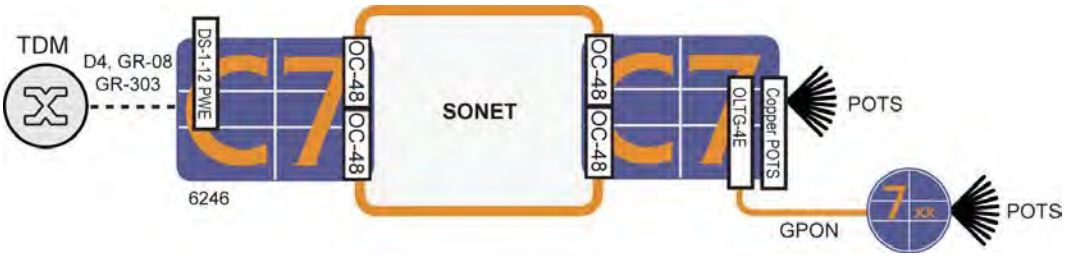
In most instances, the DS1-12 PWE card should be used for this application due to its greater density.

Note: The T1-8 PWE card is compatible with this configuration however with fewer ports, fewer overall lines are supported.

The use of the PWE cards for TDM voice interface is supported via the Multiprotocol (MP) interface to the RAP-10GE or other legacy RAP cards. TDM voice switch interface functionality on the PWE cards is identical to that of the T1-6 card and the same rules apply. The benefit of the PWE cards is the increased density for switch interfaces and the ability to support an increased number of interface groups (minimizes slot consumption in C7 shelves). In the case of Ethernet transport, voice traffic from remote C7 shelves must first be converted to the TDM Gateway protocol (via the EGW card) before interfacing the DS1-12 PWE or T1-8 PWE. The DS1-12 PWE and T1-8 PWE cards support D4 (nailed up), GR-08 Mode I & II, and GR-303 switch interfaces.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

In the example below, the DS1-12 PWE or T1-8 PWE card supports D4, GR-08 Mode I & II, and GR-303 switch interfaces across the SONET based network (OC-48 RAP card). As in the example above, TDM voice switch interface functionality on the PWE cards is identical to that of the T1-6 card (with the same rules applying).



Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Provisioning SAToP over RAP-10GE ERPS Transport

To turn up PWE services in this architecture, the following steps are required:

1. Configure DS1-12 PWE port settings (near end)
2. Configure T1-8 PWE port settings (far end)
3. Optional: Create PWE3 Template (CMS > Profile > C7 > PWE3 Template
4. Create service VLAN (S-VLAN) for Source and Destination nodes of the end to end circuit
5. Create VLAN-IF across ERPS Domain

Starting point

Before starting the turn-up process, check to see that the following conditions are met:

- All C7 shelves in the T1 transport network have been installed and powered.
- AMP (or ATP) and RAP cards have been installed in the C7 shelves.
- T1-8 PWE or DS1-12 PWE cards have been installed in the C7 shelves.

  Note: T1-8 PWE cards support repeater powering; the DS1-12 PWE card requires an external repeater shelf.

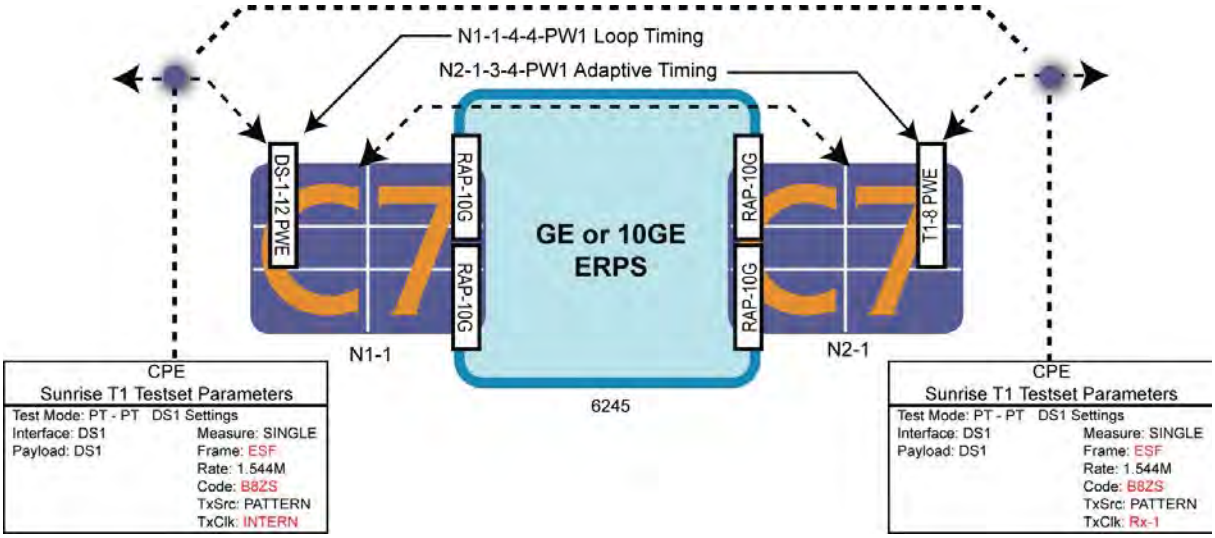
- Cables have been connected to the T1 cards in each C7 shelf.

Overview of Configuration

The configuration that follows depicts an end-to-end pseudo-wire network between a DS1-12 PWE3 card and a T1-8 PWE3 card. The source device (DS1-12 PWE card) uses Loopback Timing (also known as Loop Timing) while the Destination device (T1-8 PWE card) uses Adaptive Timing. In this configuration, Structure Agnostic TDM over Packet (SAToP) protocol is used over a RAP-10GE ERPS transport.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

The illustration below reflects the appropriate timing settings for each end of the pseudowire.



Configuring the DS1-12 PWE Port Settings

To configure the COT shelf DS1 port for clear channel, Hi-Cap service, complete the following steps:

To configure the COT shelf DS1 port

1. Within CMS, navigate to the appropriate DS1 port on the DS1-12 PWE card.

   Note: Accept all defaults that are pre-populated with the following exceptions:

2. In the DS1 Format list, select Unframed (UF) from the drop-down list.
3. In the DS1 Map list, select PWUNSTRUCT from the drop-down list.
4. In the Timing Mode list, select LOOP or ADAPT. For complete timing mode options and recommendations, see *PWE3 Timing Recommendations* (on page 511).
5. Verify Channel Associated Signaling is set to off (default).
6. From the work area top menu bar, click **Apply**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring T1-8 PWE Port Settings

To configure the RT shelf DS1 port for clear channel, Hi-Cap service, complete the following steps:

To configure the RT shelf DS1 port

1. Within CMS, navigate to the appropriate DS1 port on the T1-8 PWE card.

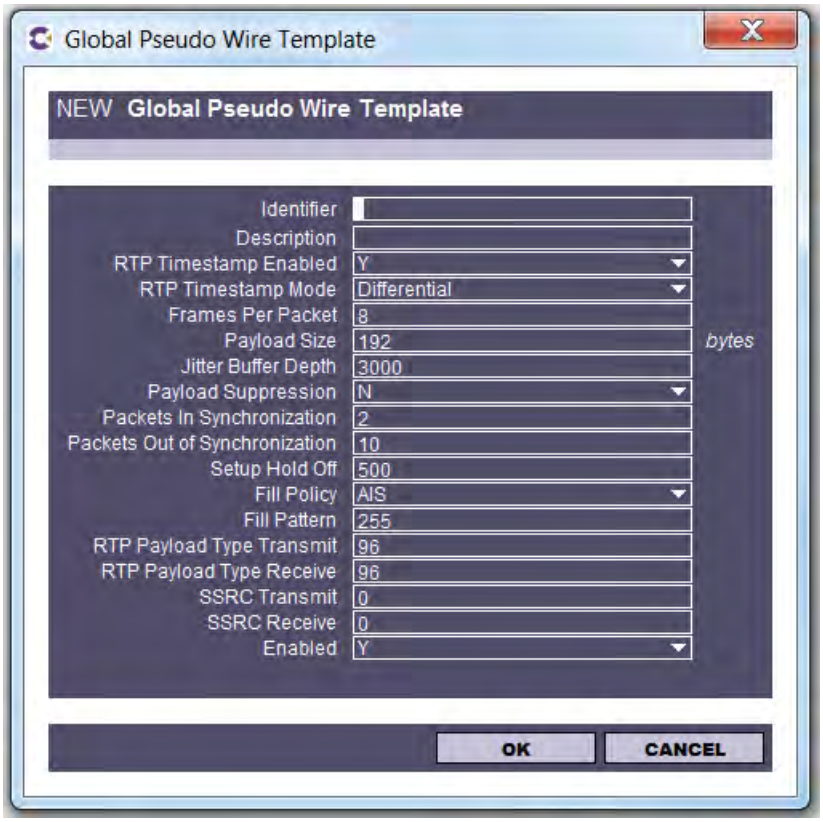
   Note: Accept all defaults that are pre-populated with the following exceptions:

2. In the DS1 Format list, select Unframed (UF) from the drop-down list.
3. In the DS1 Map list, select PWUNSTRUCT from the drop-down list.
4. In the Timing Mode list, select ADAPT. For complete timing mode options and recommendations, see *PWE3 Timing Recommendations* (on page 511).
5. Verify Channel Associated Signaling is set to off (default).
6. From the work area top menu bar, click **Apply**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Optional: Create PWE3 Template

To simplify provisioning of the PWE circuit, a Global Pseudo Wire Template can be pre-configured and applied to the PWE port on the card.



Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Create PWE Profile Field Definitions		
Paramter	**Description**	**Valid Options**
Identifier	The Identifier is displayed in the list of available profiles in all C7 PWE Profile drop-down lists within CMS.	N/A
Description	Description of the Profile	N/A
RTP Timestamp Enabled	The RTP timestamps are used for carrying timing information over the network. With set to Yes, RTP headers are enabled on transmitted packets.	Y ‡ N
RTP Timestamp Mode	Clock source mode to use for RTP. Absolute - *One* of the PWE endpoints sets timestamps using the clock recovered from the incoming attached TDM circuit. The timestamps are closely correlated with the sequence numbers. All SAToP implementations that support RTP Header usage must support Absolute mode. Differential - *Both* PWE endpoints have access to a common high quality timing source, and this source controls timestamp generation.	differential ‡ absolute
Frames Per Packet	Number of T1 frames per packet (PWSTRUCT services only). When operating in ESF mode, CAS must equal Yes. Allowable values in ESF mode = 4, 6, 8, 12, and 24. When operating in SF mode, CAS must equal yes. Allowable values in SF mode = 4, 6, and 12.	Integer (4-40) 8 ‡
Payload Size	Packet size in bytes. Applies to SAToP transport only. Note: If PWE endpoints reside on an E7 GPON network, increase the C7 PWE payload size to 204 bytes.	96 - 1152 bytes 192 bytes ‡
Jitter Buffer Depth (1)	Jitter compensation value that offsets packet delay variations. The jitter buffer depth is entered/displayed in microseconds (µs), but represents a specific number of packets. Use the following formulas to calculate desired jitter buffer depth for your environment: Packet interval = (Payload Size in Bytes / 193) x 1000 µs Jitter buffer depth = Packet interval x <number of packets> From any entered value in microseconds, the system 1) calculates the number of packets, 2) rounds up to the nearest whole number, and 3) uses a number of packets based on the following mapping to powers of 2: • 2-3 packets calculated: 2 packets used • 4-7 packets calculated: 4 packets used • 8-15 packets calculated: 8 packets used • 16-31 packets calculated: 16 packets used • 32-63 packets calculated: 32 packets used • 64+ packets calculated: 64 packets used For example: • Default packet interval = (192 / 193) x 1000 µs = 994.8 µs • Default jitter buffer depth = 3000 µs • Calculated number of packets = 3000 / 994.8 = 3.01 packets • Rounded up to 4 packets • Internally-used jitter buffer depth = 4 packets, or 3979.3 µs	Packet interval x 2, 4, 8, 16, 32, or 64 packets (in µs) 3000 µs ‡ (Actual value may be greater than entered value. See description and example.)
Payload Suppression	In order to conserve bandwidth, payload suppression is allowed. Under certain conditions, packets may be sent with less than full payloads, buy adding "fill" bytes to packets or packets can be sent without any payload at all, thereby conserving bandwidth.	Yes = Suppression allowed No ‡

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Create PWE Profile Field Definitions		
Packet in Synchronization	The number of consecutive "In Sync" packets required to exit the **L**oss **O**f **P**ackets **S**tate (LOPS). Occurs with zero PWE packets are received.	Integer (1-10) 2 ‡
Packets Out of Synchronization	The number of consecutive "Out of Sync" packets missed before LOPS state is entered.	Integer (1-15) 10 ‡
Setup Hold Off	This timer allows for configuration of a time-out delay while PW circuit is establishing a connection (per RFC5604 requirements).	Integer (milliseconds) 5000 ‡
Fill Policy	Policy to be applied when the CE-bound Jitter buffer reports an overflow or underflow condition. When received packets contain an alarm condition (L-bit is asserted), the near-end device will attempt to condition the outgoing TDM signal. When this occurs, the packet does not contain valid TDM payload data from the far-end (or may be "empty as described above) such that the near-end must fill the TDM signal to complete the packet. Note: When AIS is applied, any "short" packets are filled with all "1's". Note: AIS applies to PWUNSTRUCT configurations only.	AIS or User AIS ‡
Fill Pattern	User defined Fill Pattern to be used towards the T1 port. if the fill policy is configured to "user", then the fill pattern is used to fill the TDM signal under any alarm condition. If the user defines 255 (AIS pattern), then behaves as Fill Policy.	Integer (1-255) 255 ‡ (AIS pattern)
RTP Payload Type Transmit	RTP Payload type to be used to transmit and receive PWE packets. The RTP payload type in the RTP header includes a 7-bit value that is used to define the format of the payload and how the receiver is to interpret the payload. PWE typically uses a value of 96. The transmitted packets in this case contain this value in the RTP header.	Integer (0-127) 96 ‡
RTP Payload Type Receive	RTP Payload expected to be received from far end PWE packet. Same as transmit above except this applies to received packets only. The opposite end might have to adjust its transmit value to this value for inter-op purposes. Note: The ONT in a PWE configuration always uses the same value for transmit and receive.	Integer (0-127) 96 ‡
SSRC Transmit	SSRC (Synchronization Source Identifier) is the value to be transmitted to the far end node. This 32-bit value in the RTP header is used to uniquely identify the packet source. All transmitted packets contain this value if set.	Integer 0 ‡ (Off)
SSRC Receive	SSRC value expected to be received at the far end node. Same as above but for received packets.	Integer 0 ‡ (Off)
Enabled	Should this profile be enabled on the PWE network?	Y N ‡ Disabled

‡ = Default value.

(1) Any value of jitter buffer depth will introduce some packet delay. To lower the latency of end-to-end traffic, do one of the following:

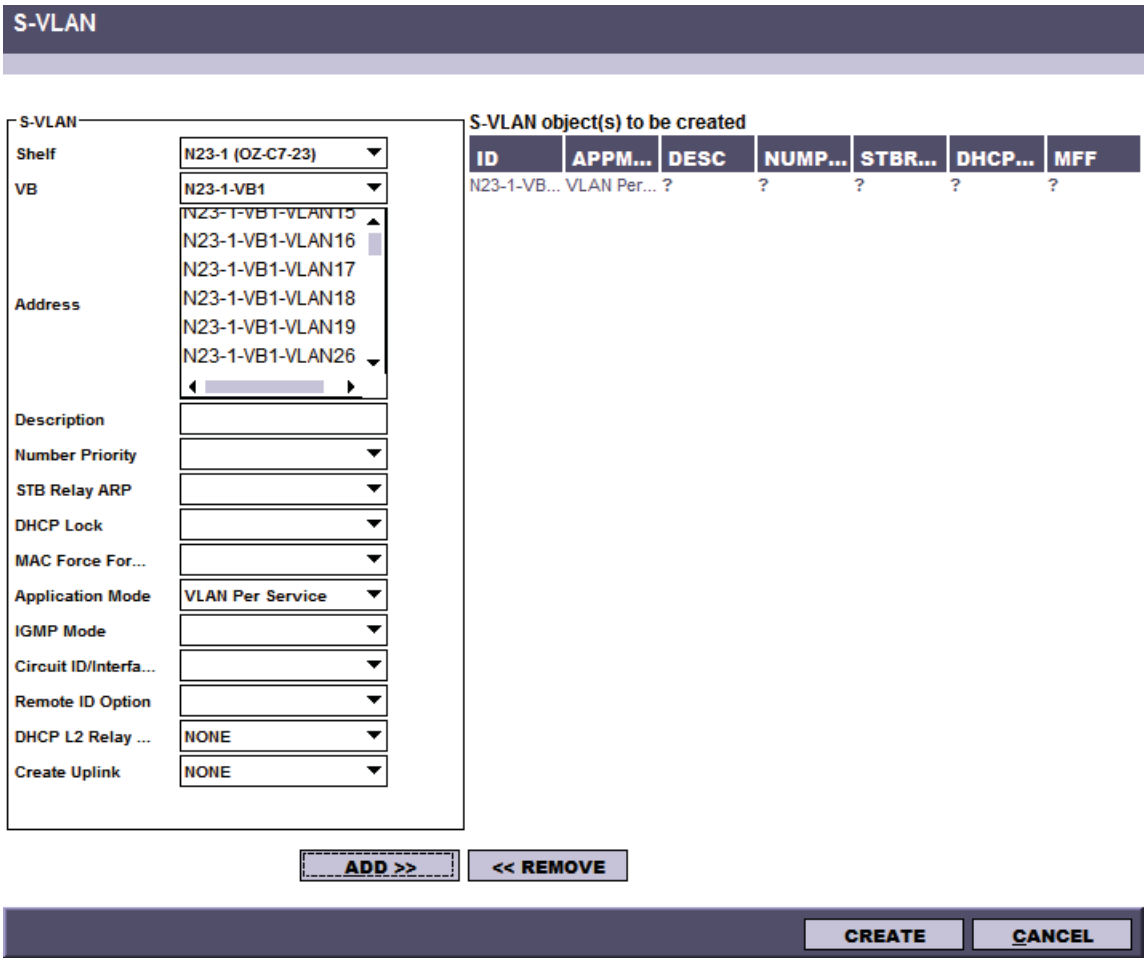
- Use a smaller payload size: This option maintains the same level of jitter buffer depth, but increases the traffic rate. The jitter buffer depth is the same in terms of packets buffered (e.g. 4), but smaller in value (microseconds) because of the decreased packet interval.
- Use a smaller jitter buffer depth: This option maintains the same traffic rate, but is less immune from packet delay variations (jitter). You can monitor the PM counters to see if there are any anomalies, such as packet loss.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Creating Service VLAN (S-VLAN) for Source and Destination Nodes

With both endpoint ports configured, a service VLAN must be created at each end to uniquely identify the end-to-end traffic.

For general guidelines and a list of S-VLAN parameters, see *VLAN Guidelines and Parameters* (on page 223).



To create a service VLAN at the source and destination nodes of the PWE circuit

1. Within CMS, navigate to the shelf where the VLAN will be created.
2. From the Work Area menu bar, select **Create > VLAN > S-VLAN**
3. From the Create S-VLAN screen, configure the following variables:
   a. Verify the Shelf and VB settings are pointing to the shelf where you want to create the service VLAN.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Note: A VLAN is created on the current virtual bridge and is replicated on all bridges in the shelf (local or virtual).

b. In the Address list, select the VLAN ID to create.

c. (Optional) In the Description box, type a brief description for the VLAN.

d. In the Application Mode List, select the appropriate mode for the PWE service:

- **VLAN per Port**
- **VLAN per Service**

Note: The remaining options are not supported for PWE service

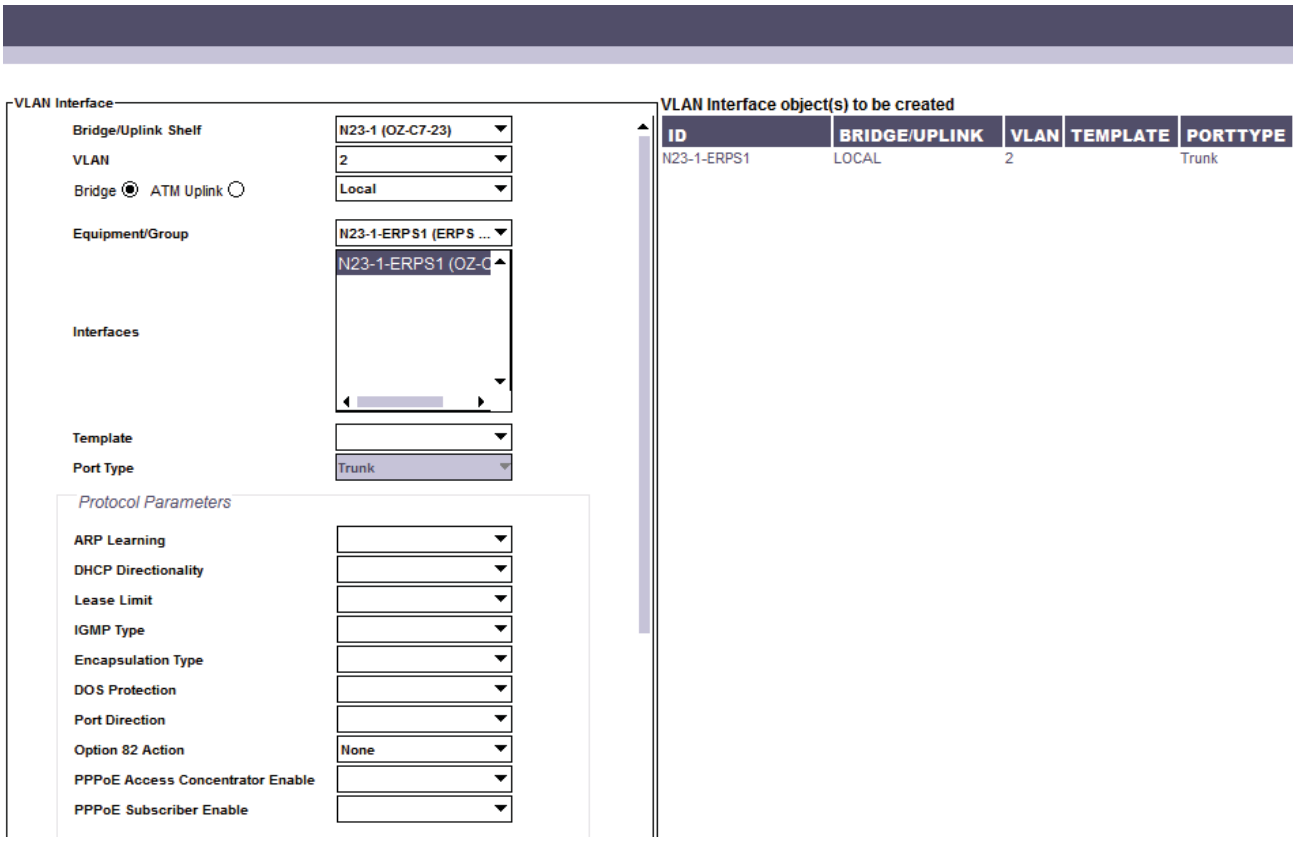
4. In the DHCP L2 Relay box, choose None.
5. When complete, click **Add**, and then click **Create**.
6. Repeat steps 1 through 5 for the far end node of the PWE circuit.

Note: When creating the far end circuit, ensure the shelf and virtual bridge location are as desired and that the VLAN ID matches for each end of the circuit.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Creating the VLAN Interface (VLAN-IF) Across the ERPS Domain

With the S-VLANs configured, both the near end and far end VLAN interface must be provisioned to transport the traffic across the ERPS domain.



To create the VLAN Interface at the source and destination nodes of the PWE circuit

1. Within CMS, navigate to the shelf where the VLAN will be created.
2. From the Work Area menu bar, select **Create > VLAN > VLAN-IF > VLAN Interface**

   Note: Accept all default values in the steps below except as indicated.

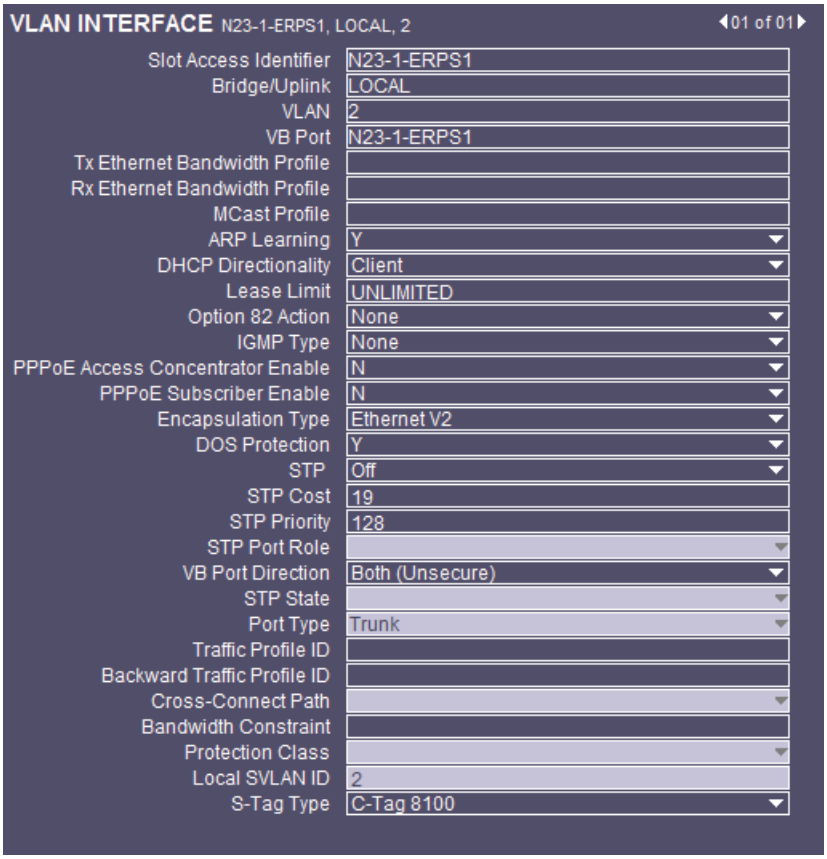
3. From the Create VLAN Interface screen, configure the following variables:
   a. Verify the correct Shelf and Service VLAN settings are selected.
   b. Select Local from the drop-down list in the Bridge/ATM Uplink field.
   c. In the Equipment/Group list, select the previously configured ERPS Domain.
   d. In the Port Type field, select **Trunk**.
   e. In the Option-82 Action box, select None.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

4. When complete, click **Add**, and then click **Create**.
5. Create a separate VLAN Interface for the far end node of the PWE circuit by repeating steps 1 through 4 above.

Note: When creating the far end circuit, ensure the shelf and virtual bridge location are as desired and that the VLAN ID matches for each end of the circuit.

Once complete, VLAN Interfaces associated with specific S-VLANs can be viewed by selecting an S-VLAN from the Shelf VLAN screen and expanding the VLAN-IF tab in the Work Area.



Using the PWE3 Provisioning Tool

With DS1 ports, Service VLANs, and VLAN interfaces pre-provisioned, pseudo-wire endpoints must be associated with their corresponding VLAN interfaces. To facilitate this task, Calix has developed a PWE3 Tool to simplify this process.

The purpose of the tool is configure each endpoint of the pseudowire and associate the UDP Port number and VLAN interface of the circuit. The tool performs the following functions:

1. *Create a PWE Service* (on page 542) type and apply a global template.
2. *Configure Endpoint A* (on page 543) (Shelf, Equipment type/ Port/ PWE port/ VLAN

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

3. *Associate Endpoint A* (on page 544) with the appropriate Host/IP Address
4. *Configure Endpoint B* (on page 544) (Shelf, Equipment type/ Port/ PWE port/ VLAN
5. *Associate Endpoint B* (on page 545) with the same Host/IP Address as Endpoint A.

Create PWE Service

Create a PWE Service type and apply a global template.

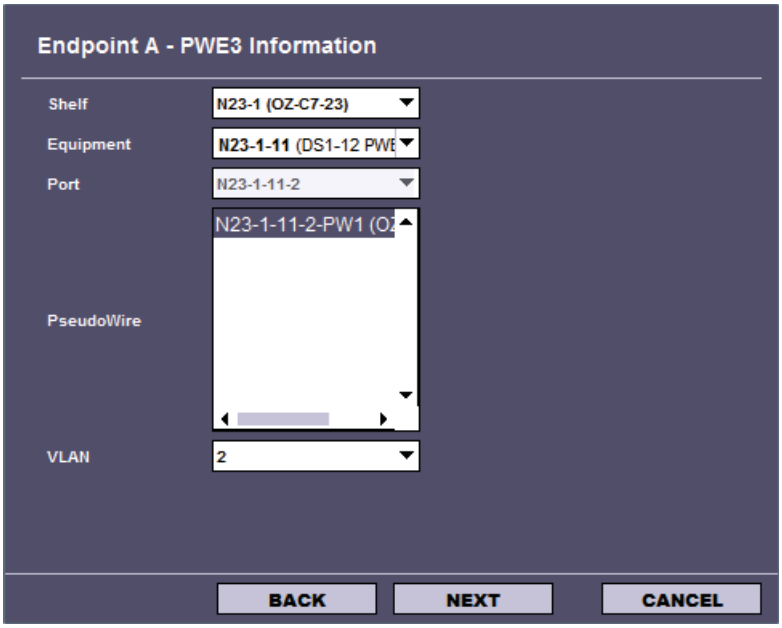
To create a PWE service

1. From the Tools menu, select PWE3 Tool.
2. Select T1 as the service type for this circuit.
3. Add a description of the circuit.
4. (Optional) Apply a pre-configured PWE3 template to the circuit.
5. Click **Next.**

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configure Endpoint A

Configure Endpoint A to define the shelf, PWE card type (equipment), PWE card port number, the PWE port, and the VLAN interface to use.



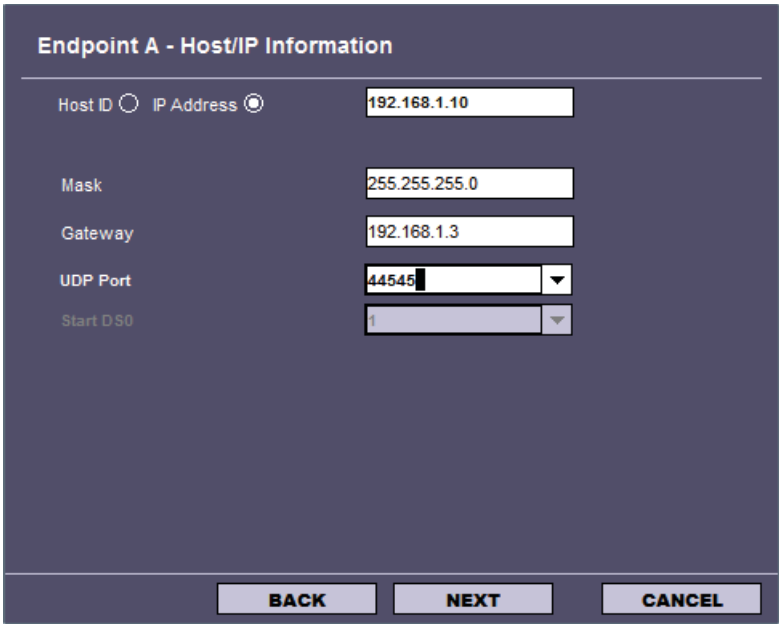
To configure Endpoint A

1. From the Endpoint A - PWE3 Information screen, do the following:
   a. Select the C7 shelf where the PWE card resides.
   b. Select which PWE card you are attaching to.
   c. Select the port of the PWE card for the circuit.
   d. Select the PWE port within the card port.
   e. Select the VLAN interface previously configured.
2. Click **Next**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configure the Host/IP Information for Endpoint A

With the PWE service defined with its associated equipment, the EndPoint requires an IP address such that the far end can communicate with it.



To configure the Host/IP information

1. From the Endpoint A - Host/IP Information screen, do the following:
   a. Choose the appropriate radio button based on whether you are using a pre-existing IP Host or an IP Address.

   Note: If the IP address option is chosen, a new IP Host will automatically be created.

   Note: For PWE, you can assign a single IP Host per PWE card or you can assign an IP Host per port. When a single IP Host per card is chosen, each card port must use a unique UDP port number.

   b. Accept the default Mask and IP Gateway or modify based on your environment
   c. Assign the Endpoint A UDP Port number.
2. Click **Next**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring Endpoint B

Configure Endpoint B to define the shelf, PWE card type (equipment), PWE card port number, the PWE port, and the VLAN interface to use.

To configure Endpoint B

1. From the Endpoint B - PWE3 Information screen, do the following:
   a. Select the C7 shelf where the PWE card resides.
   b. Select the far end PWE card you are attaching to.
   c. Select the port of the PWE card for the circuit.
   d. Select the PWE port within the card port.
   e. Select the VLAN interface previously configured (same VLAN as EndPoint A).
2. Click **Next**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configure Host/IP Information for Endpoint B

With the PWE service defined with its associated equipment, the EndPoint requires an IP address such that the far end can communicate with it.

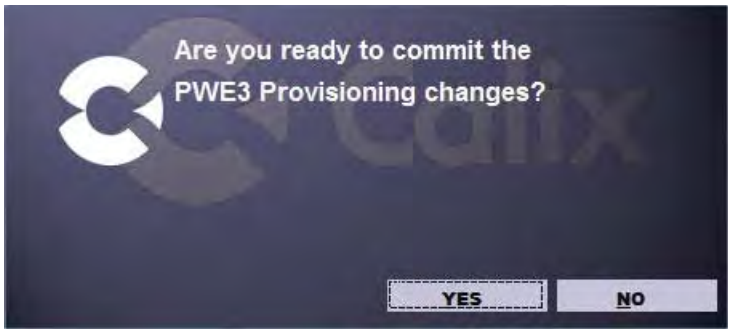
To configure the Host/IP information

1. From the Endpoint B - Host/IP Information screen, do the following:
   a. Choose the appropriate radio button based on whether you are using a pre-existing IP Host or an IP Address.

Note: If the IP address option is chosen, a new IP Host will automatically be created.

Note: For PWE, you can assign a single IP Host per PWE card or you can assign an IP Host per port. When a single IP Host per card is chosen, each card port must use a unique UDP port number.

   b. Accept the default Mask and IP Gateway or modify based on your environment
   c. Assign the Endpoint B UDP Port number.
   d. Accept the default Starting DS0 number.
2. Click **Finish**.



3. At the Confirmation dialog box, commit the changes by selecting **Yes**.

The PWE circuit is now configured.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Provisioning Local Hairpinning of Full T1 (DACS)

The ability to cross connect Full T1 or T1 timeslots from port A to port B on the same card is new to the C7, and is enabled on the PWE cards with RAP-10GE or multiprotocol RAPs. Often referred to as a Digital Access Cross Connect (DACS) application, this service allows CSPs to digitally cross connect incoming fractional T1 circuits from one location to another, or an entire T1. The PWE cards enable this functionality on the same slot, preserving shelf capacity for other services.

To complete this configuration:

1. Verify DS1 ports are formatted and mapped appropriately.
2. Perform Hair Pin Provisioning
3. Select Hair Pin Service Type
4. Select PW Endpoints
5. Associate Endpoints with Host/IP addresses
6. Verify configured PWE Endpoints

Configure DS1 Ports

In this configuration, two DS1 ports will be digitally cross-connected on the same card slot.

To configure the PWE card DS1 port

1. Within CMS, navigate to the PWE card to provision and select any DS1 port on the card.
2. Verify that the DS1 format for each port to be hairpinned is set to **Unframed.**
3. Verify the DS1 Mapping is set to **PWUNSTRUCT**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring the PWE Card for Hairpinning

With DS1 ports identified, the PWE card to be used for hairpinning must be provisioned.

To configure the PWE card

1. Within CMS, navigate to the PWE card in the left hand navigation pane.
2. From the Work Area Action menu, select Hair Pin Provisioning.
3. In the Hair Pin Service Types screen, do the following:
   a. Select T1 as the service type.
   b. Add a service description (i.e., hairpin_P1_P2)
4. Click **Next**.

Configuring PWE Endpoints

Each endpoint is now selected and "hairpinned" to the other pseudo-port.

To hairpin the endpoints

1. From the PW Endpoint A dialogue box, select the PWE card port and PWE port. Click **Next.**
2. From the PW Endpoint B dialogue box, select the same PWE port and PWE port to hairpin. Click **Next**.

Configuring Host/IP Information for Hairpinning

With the PWE hairpinning service defined with its endpoints, configure a Host/IP address such that the hairpin is complete.

To configure Host/IP information for the Hairpin

From the Hair Pin Common Information dialogue screen, perform the following

1. From the Endpoint A - Host/IP Information screen, do the following:
   a. Choose the appropriate radio button based on whether you are using a pre-existing IP Host or an IP Address.

Note: If the IP address option is chosen, a new IP Host will automatically be created.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

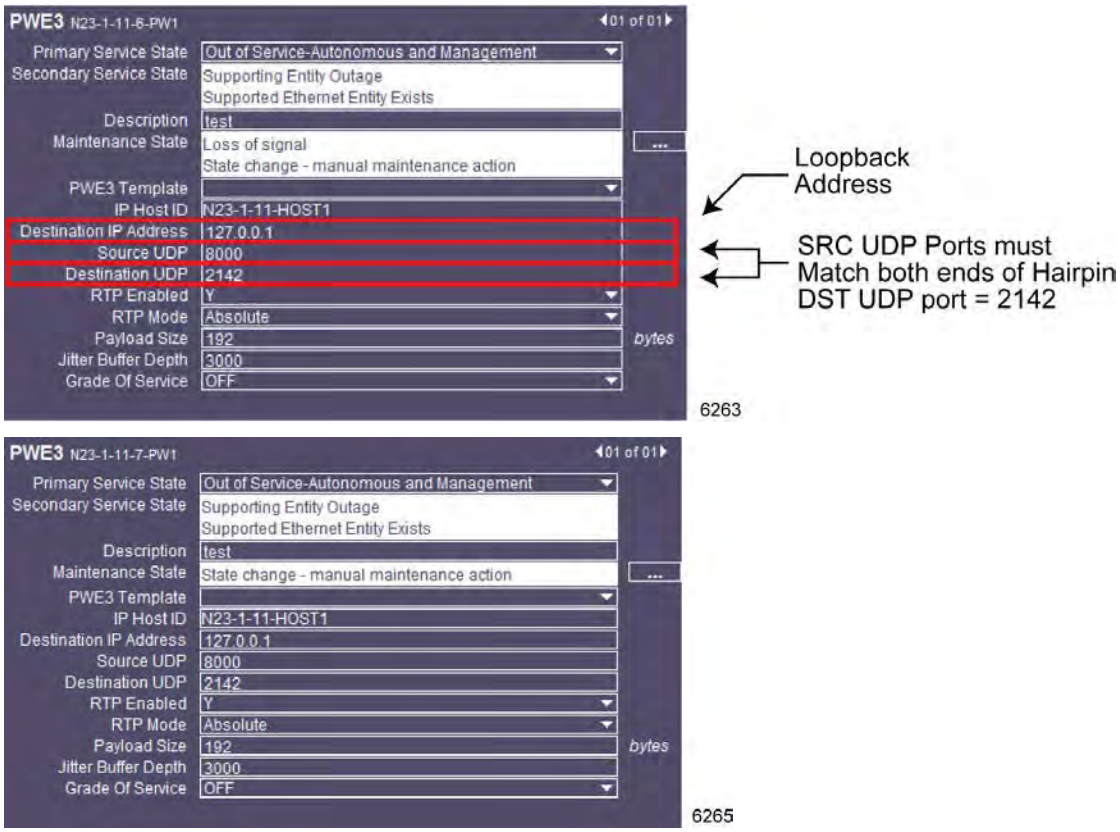
Note: For PWE, you can assign a single IP Host per PWE card or you can assign an IP Host per port. When a single IP Host per card is chosen, each card port must use a unique UDP port number.

b. Accept the default Mask and IP Gateway or modify based on your environment

c. Assign the Destination UDP port value of 2142.

d. Provision the Service VLAN for the circuit.

2. Verify configured PWE endpoints by navigating to the PW hairpin circuits on the DS1 card.



3. Verify the PWE configuration via TL1 by executing the following command:

```
>rtrv-pw::n23-1-all
```

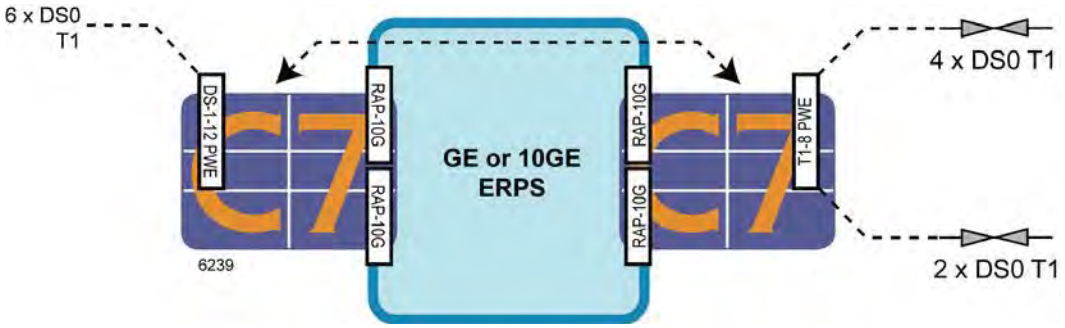
Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Provisioning Fractional T1 Service over Aggregated Ethernet

Circuit Emulation Service over Packet Switched Networks (CESoPSN) is an architecture that supports transport of structured T1s across a Public Switched Network. Although this architecture has less tolerance for jitter/wander, a source timing schema is implemented to ensure trouble-free transport end to end.

Fractional T1 service delivery provides n x DS0 services to end customers requiring less than a full 1.544Mbps of bandwidth to a given location. The circuits can be used to deliver non-switched special circuits to the end customer and are carried over Ethernet transport via CESoPSN. Each T1 port on a DS1-12 PWE or T1-8 PWE supports up to (24) T1 timeslots for Fractional T1 services.

Note: T1 timeslots in this PWE configuration must be contiguous in nature (must use the next sequential timeslot in the PWE bundle).



To complete this configuration:

1. Verify DS1 ports are formatted and mapped appropriately.
2. Configure Service Type for DS0 Cross-Connects
3. Configure PWE Endpoint A
4. Configure PWE Endpoint A HOST/IP Information
5. Configure Endpoint B
6. Configure PWE Endpoint B HOST/IP Information
7. Verify configured PWE Endpoints

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring DS1 Ports

In this configuration, two DS1 ports will be digitally cross-connected on different shelves across a GE, 10GE or ERPS domain.

To configure the PWE card DS1 port

1. Within CMS, navigate to the appropriate DS1 port on the DS1-12 PWE card.

   Note: Accept all defaults that are pre-populated with the following exceptions:

   a. From the DS1 format drop-down list, select **ESF** (Extended Super Frame)

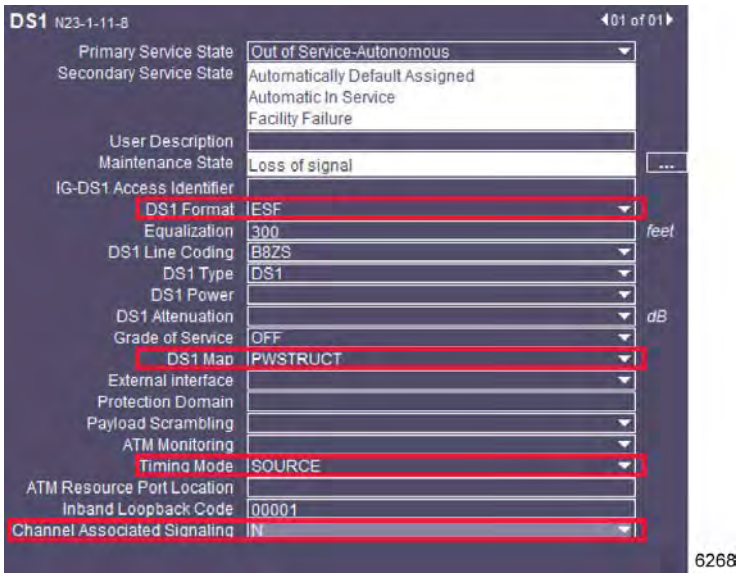
   b. From the DS1 Map drop-down list, select **PWSTRUCT**.

   c. From the Timing Mode drop-down list, select **SOURCE**.

   d. Verify the Channel Associated Signaling (CAS) value is set to No (**N**).

   Note: If CAS is enabled in this environment (such as with Robbed Bit Signaling), the resulting DS0 payload is reduced to 56 Kbps instead of the desired 64 Kbps.

2. Click **Apply**.



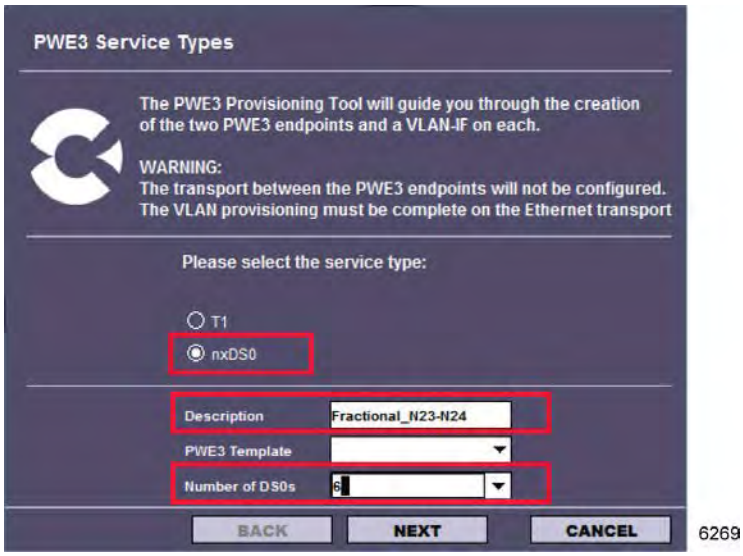
Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Creating Digital Cross-Connects for the PWE

You now must define the cross-connects for the PWE circuit and specify the number of contiguous DS0s to create.

To provision cross-connects

1. Within CMS, at the PWE card level, launch the PWE Tool from the Tools menu.
2. Select the Cross-Connect option under service type.
3. Add a clear description for the PWE3 service being created
4. From the drop-down list, select the number of DS0's to provision for use by the PWE service.

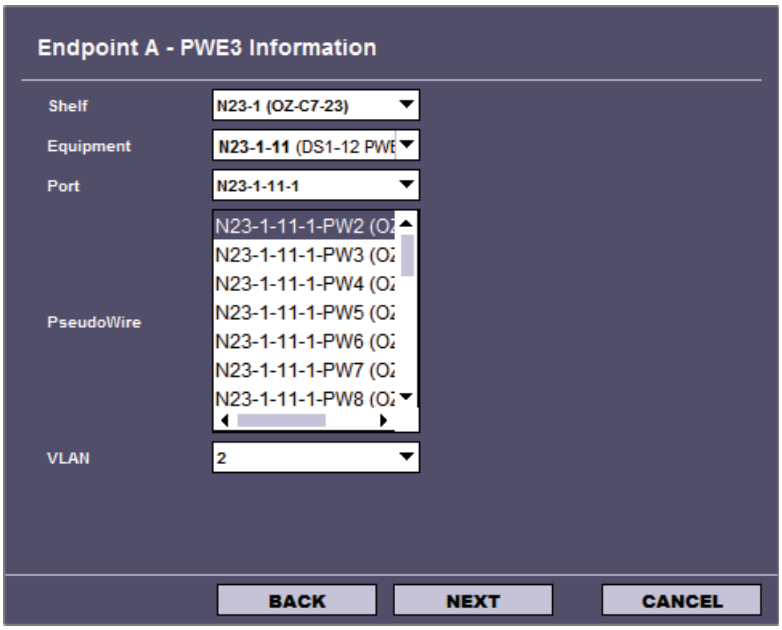


5. Click **Next**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring the PWE Endpoint A

Configure Endpoint A to define the shelf, PWE card type (equipment), PWE card port number, the PWE port, and the VLAN interface to use.



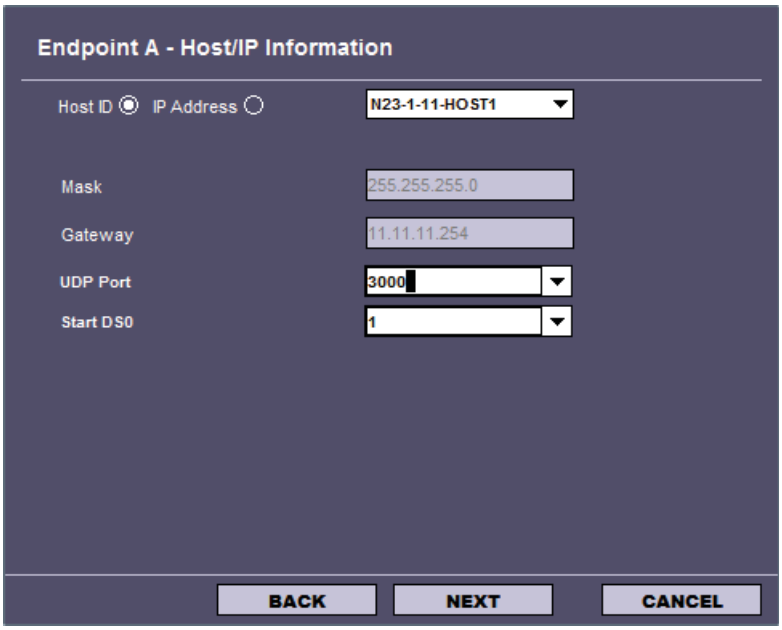
To configure Endpoint A

1. From the Endpoint A - PWE3 Information screen, do the following:
   a. Select the C7 shelf where the PWE card resides.
   b. Select which PWE card you are attaching to.
   c. Select the port of the PWE card for the circuit.
   d. Select the PWE port within the card port.
   e. Select the VLAN interface previously configured.
2. Click **Next**.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configure the Host/IP Information for Endpoint A

With the PWE service defined with its associated equipment, the EndPoint requires an IP address such that the far end can communicate with it.



To configure the Host/IP information

1. From the Endpoint A - Host/IP Information screen, do the following:
   a. Choose the appropriate radio button based on whether you are using a pre-existing IP Host or an IP Address.

   Note: If the IP address option is chosen, a new IP Host will automatically be created.

   Note: For PWE, you can assign a single IP Host per PWE card or you can assign an IP Host per port. When a single IP Host per card is chosen, each card port must use a unique UDP port number.

   b. Accept the default Mask and IP Gateway or modify based on your environment
   c. Assign the Endpoint A UDP Port number.
   d. From the drop-down list, select the starting DS0 number for the PWE service.

   Note: In this release, only consecutive (contiguous) DS0 ports are provisionable.

2. Click **Next**.

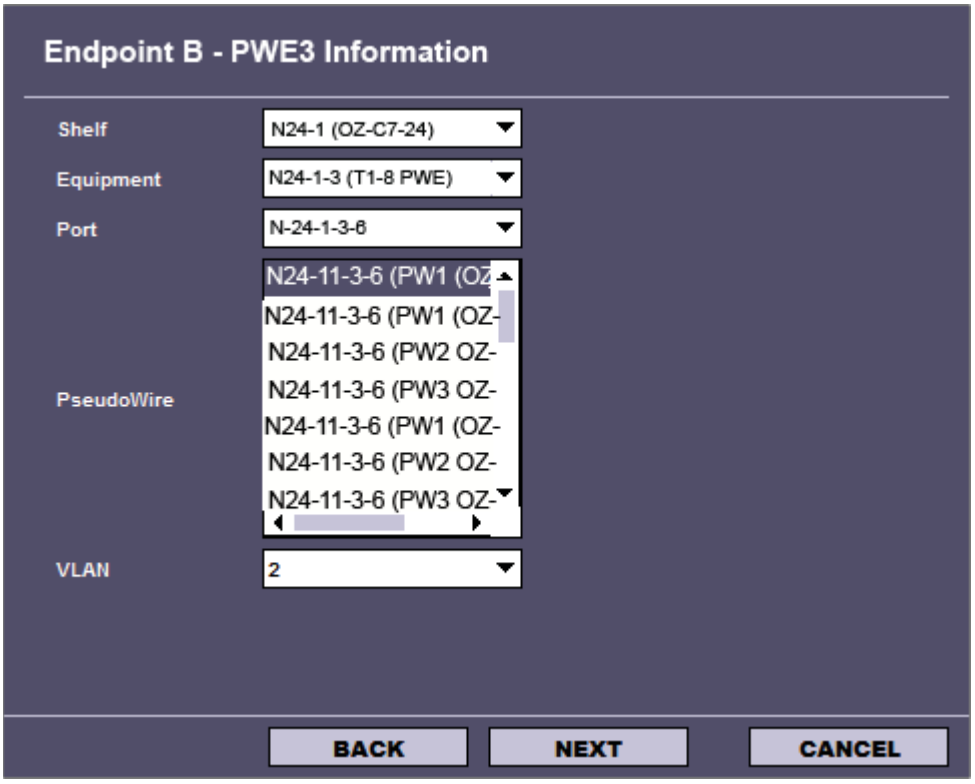
Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring the PWE Endpoint B

Configure Endpoint B to define the shelf, PWE card type (equipment), PWE card port number, the PWE port, and the VLAN interface to use.

To configure Endpoint B

1. From the Endpoint B - PWE3 Information screen, do the following:
   a. Select the C7 shelf where the PWE card resides.
   b. Select the far end PWE card you are attaching to.
   c. Select the port of the PWE card for the circuit.
   d. Select the PWE port within the card port.
   e. Select the VLAN interface previously configured (same VLAN as EndPoint A).
2. Click **Next**.



Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Configuring the Host/IP Information for Endpoint B

With the PWE service defined with its associated equipment, the EndPoint requires an IP address such that the far end can communicate with it.

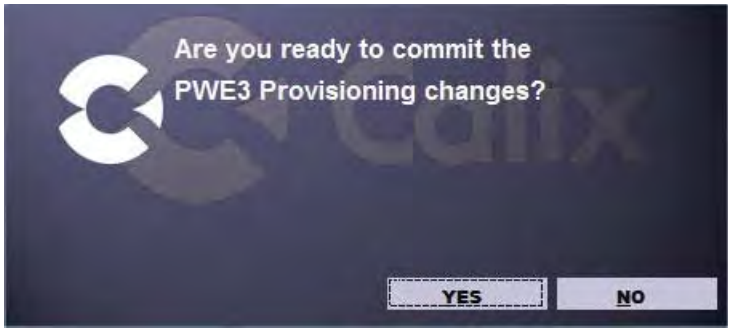
To configure the Host/IP information

1. From the Endpoint B - Host/IP Information screen, do the following:
   a. Choose the appropriate radio button based on whether you are using a pre-existing IP Host or an IP Address for Endpoint B.

   Note: If the IP address option is chosen, a new IP Host will automatically be created.

   Note: For PWE, you can assign a single IP Host per PWE card or you can assign an IP Host per port. When a single IP Host per card is chosen, each card port must use a unique UDP port number.

   b. Accept the default Mask and IP Gateway or modify based on your environment
   c. Assign the Endpoint B UDP Port number.
   d. Accept the default Starting DS0 number.
2. Click **Finish**.



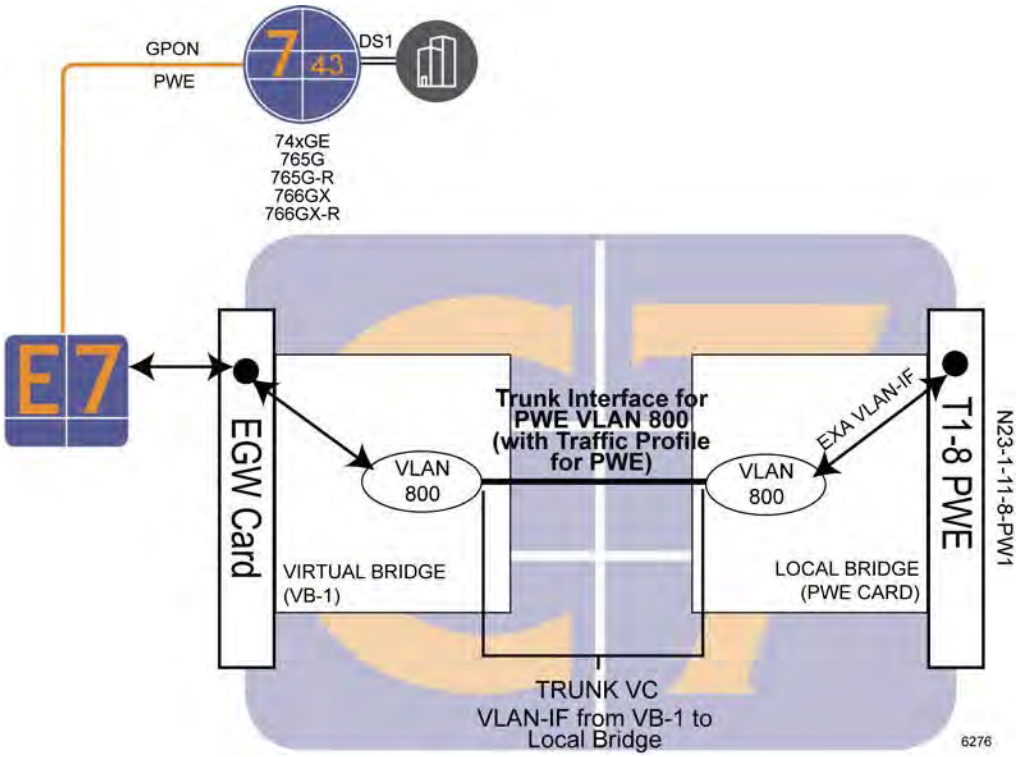
3. At the Confirmation dialog box, commit the changes by selecting **Yes**.

The PWE circuit is now configured.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Provisioning Multiprotocol Hi-CAP T1 Service over SAToP

In this application, the C7 PWE card does pwe3 on both the near and far end. In this case it is converting pwe3 on the external interface to a traditional circuit switched T1 internally. This application is similar to connecting a PWE3 circuit to a traditional (legacy) T1 on the C7 shelf.



To configure PWE services in a multi-protocol environment, perform the following steps. In the overview below, each step is identified as either a configuration item on the Multiprotocol fabric or the EXA domain on the ETW card).

To configure multi-protocol PWE services

1. Create an S-VLAN (EXA/MP)
2. Choose a pre-existing or create a new ATM Traffic profile for the class of service to be created (MP Trunk).
3. Using the PWE Bandwidth Tool:
   a. Select the service type and create appropriate profiles.
   b. Define the number of circuits and payload
   c. Configure the PWE cards DS1 port (EXA/MP)

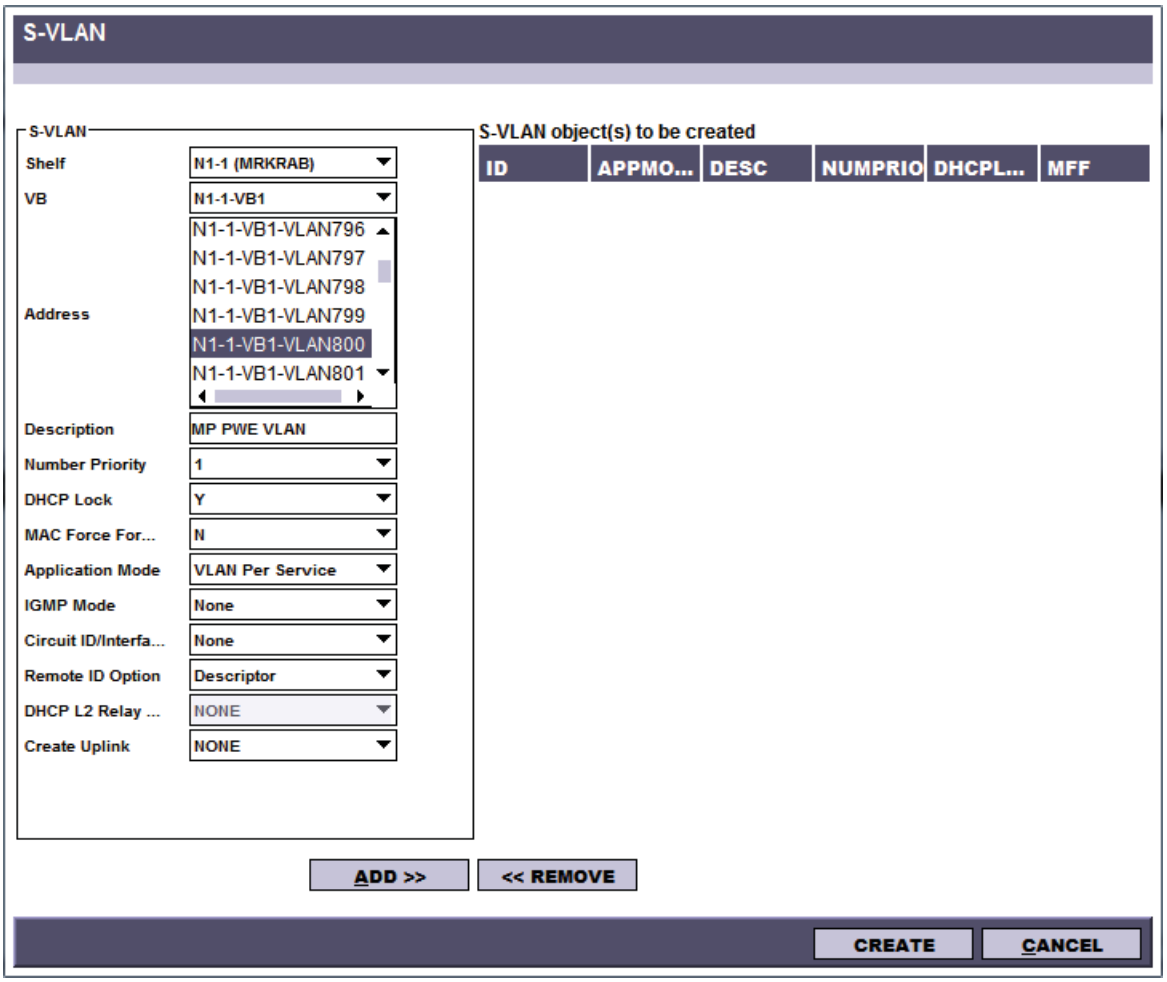
Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

d. Create the VLAN Interface for the PWE card (MP)
e. Create the VLAN Interface for the physical uplink interface (MP)
f. Create the IP Host for the PWE card (EXA/MP)
g. Configure the PWE Endpoints (EXA/MP)
h. Create the VLAN Interface for the local PWE Endpoints (EXA/MP)
i. Verify the configuration

Creating the S-VLAN

The first step is to create a Service VLAN for carrying the PWE traffic across shelves Virtual bridge.

To create a Service VLAN (S-VLAN)



Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

To create a service VLAN for the EXA domain on the EGW card

1. Within CMS, navigate to the shelf where the VLAN will be created.
2. From the Work Area menu bar, select **Create > VLAN > S-VLAN.**
3. From the Create S-VLAN screen, configure the following variables:
   a. Verify the Shelf, VB settings, and service VLAN are pointing to the shelf where you want to create the service VLAN.

   Note: A VLAN is created on the current virtual bridge and is replicated on all bridges in the shelf (local or virtual).

   b. In the Address list, select the VLAN ID to create.
   c. (Optional) In the Description box, type a brief description for the VLAN.
   d. In the Application Mode List, select **VLAN per Service.**

   Note: The remaining options are not supported for PWE service
4. In the DHCP L2 Relay box, choose None.
5. When complete, click **Add**, and then click **Create**.

Creating an ATM Traffic Profile

The multi-protocol trunk interface requires an ATM Traffic profile be selected (or created) to identify the class of service of the port. Choose a previously created ATM traffic profile or create a new one.

Refer to *Creating a Traffic Profile* (on page 89) under Managing Global C7 Profiles in CMS, discussed previously in this guide.

Provisioning Traffic Profiles using the PWE3 Bandwidth Tool

For customization, you may create traffic profiles for managing packets across the PWE network.

To facilitate the creation of PWE traffic profiles within CMS, Calix has developed a PWE3 Bandwidth Tool. This tool automatically calculates the appropriate values based on the expected number of PWE services to be offered on the port.

Note: In C7 Release 8.0, pre-configured profiles are embedded in CMS for use in PWE provisioning. Use these profiles as a guide when creating custom profiles within your specific environment.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

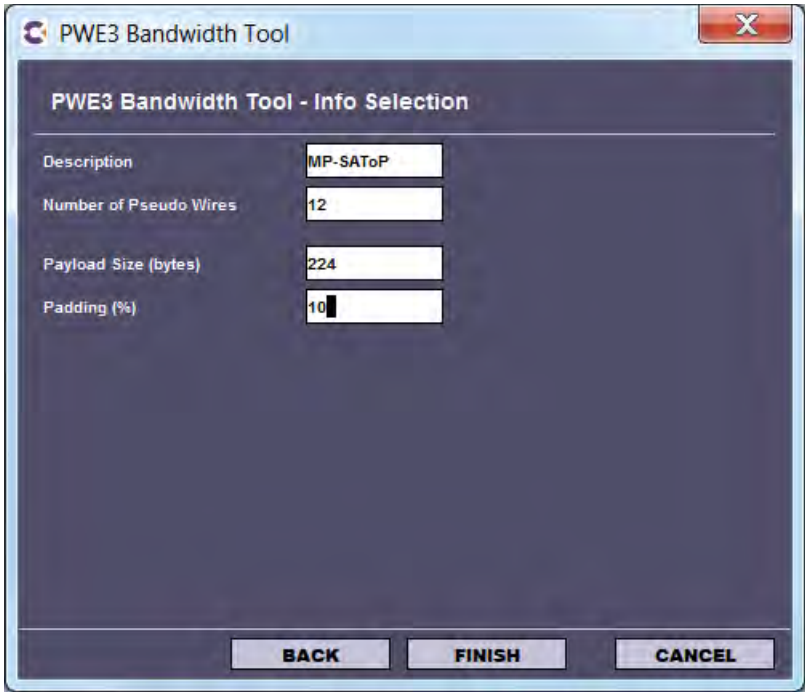
To create a new traffic profile for PWE

1. Within CMS at the Network level, navigate to Network > Profile > Traffic Profile > Create PWE3 Bandwidth Tool.
2. At the PWE3 Bandwidth Tool window, configure the following parameters:
   a. Select the service type for the circuit.
   b. Select the Traffic Profile Type for the circuit (ATM Traffic Profile).

3. From the Info Selection screen, do the following:
   a. Choose a name for the PWE circuit.
   b. Enter the maximum number of PWE circuits with this service.
   c. Enter the appropriate payload size (bytes) dependent on the service type.
   d. Accept the default padding level of 10%.
   e. Click **Finish** to save the changes.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

f. From the Confirmation screen, choose **Yes** to commit the changes.

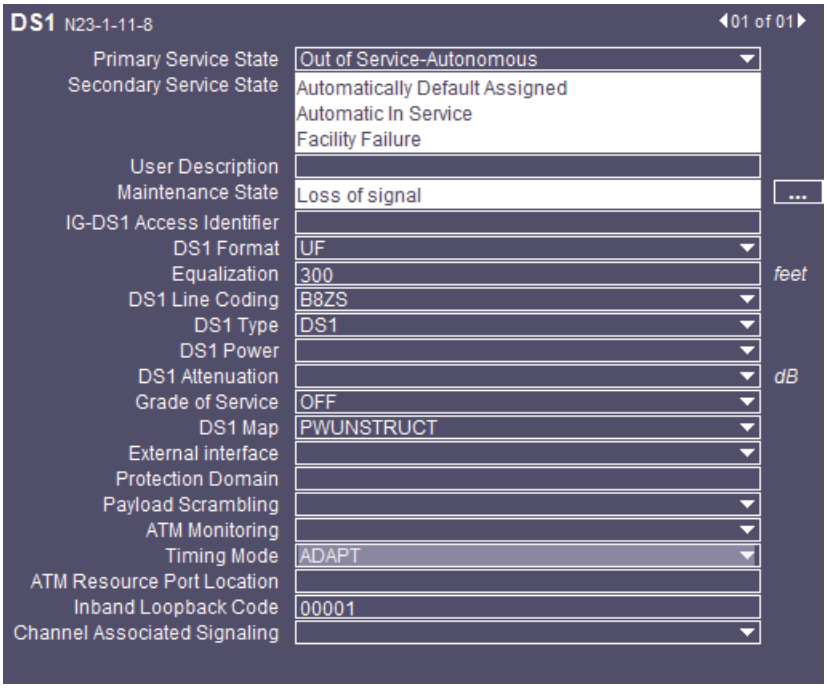


The newly created PWE3 Bandwidth Profile is added to the Traffic Profile list.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Provisioning the DS1 port for Hi-Cap Service

with PWE bandwidth profiles created, the DS1 port must now be configured for Hi-Cap services.



To configure the DS1 port for Hi-Cap service

1. Within CMS, navigate to the appropriate DS1 port on the DS1-12 PWE card.

   Note: Accept all defaults that are pre-populated with the following exceptions:

2. Under DS1 Format, select Unframed (UF) from the drop-down list.
3. Under DS1 Map, select PWUNSTRUCT from the drop-down list.
4. Since there is a common clock on the C7 shelf, set the Timing Mode to ADAPT.
5. Verify Channel Associated Signaling is set to off (default).
6. From the work area top menu bar, click **Apply**.

Create the Multiprotocol VLAN-IF for the PWE Card

With the DS1 port configured, the VLAN interface for the PWE card must be configured.

To create the VLAN-IF for the PWE card

1. Within CMS, navigate to the PWE card level and click the VLAN-IF tab in the work area.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

2. On the top menu bar, select **Create > VLAN-IF > VLAN Interface**

   Note: Accept all default values in the steps below except as indicated.

3. From the Create VLAN Interface screen, configure the following variables:
   a. Verify the correct Shelf and Service VLAN settings are selected.
   b. Select an available Virtual Bridge in the Bridge/ATM Uplink field.
   c. Select the Interface shelf where the VLAN-IF will reside.
   d. Choose the appropriate PWE line card where the VLAN-IF will be created.
   e. Under port type, choose Trunk.
4. School down to the Bandwidth Parameters section of the VLAN-IF creation screen and do the following:
   a. Choose a pre-configured or customized PWE traffic profile from the drop-down list.
5. When complete, click **Add**, and then click **Create**.

Create the VLAN-IF for the Physical Uplink Interface (EGW card)

With the VLAN-IF configured for the PWE card, the physical uplink interface for the EGW card must be created.

To create the physical uplink interface

1. Within CMS, navigate to the EGW cards GE port in the navigation tree.
2. In the work area, choose the VLAN-IF tab
3. From the work area menu, choose Create > VLAN-IF > VLAN Interface.
4. From the Create VLAN-IF screen, do the following:
   a. Ensure the appropriate Bridge/Uplink Shelf is chosen.
   b. Select the matching VLAN from the PWE card VLAN-IF
   c. Choose the appropriate Virtual Bridge from the drop-down list.
   d. Ensure the appropriate C7 shelf is selected in the Interface Shelf box.
   e. Choose the EGW card slot and port from the Equipment/Group drop-down list.
   f. Choose the appropriate interface for the card in that slot.
   g. Ensure the port type is set to Trunk.
5. Click **Add** and then click **Create** to add the VLAN-IF.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Create an IP Host for the PWE card

With both VLAN-IFs configured, an IP Host must be defined to provide an IP address, MAC Mask, and Gateway address for the PWE card traffic.

To create an IP Host for the PWE card

1. Within CMS, navigate to the PWE card level in the navigation tree.
2. From the Provisioning Tab in the work area, choose Create > IP Host ID
3. From the IP Host ID screen, do the following:
   a. Ensure the proper shelf is selected for the IP Host.
   b. Choose the appropriate PWE card for the shelf selected.
   c. Choose any available IP Host from the drop-down list in the Address field.
   d. Select an IP Address for the port on the PWE card.
   e. Select an IP Mask for the port as required.
   f. Choose a Gateway address as required.
4. Click **Add**, and then **Create** to save the IP Host ID for the PWE card port.

Creating the PWE Endpoint for the Pseudowire

The PWE endpoint must now be created for the MP SAToP configuration.

To configure the PWE endpoint

1. Within CMS, navigate to the PWE card within the C7 shelf
2. From the appropriate DS1 port on the card, click **Create** to open the PWE3 Endpoint dialogue box.
3. From the PWE3 dialogue box, accept the default values except as noted here:
   a. Ensure the Shelf and PWE3 Card selected are as intended.
   b. Choose the appropriate DS1 port from the DS1/T1 drop-down list.
   c. Select a DS1 PW port from the drop-down list.
   d. Name the circuit.
   e. Enter the Source UDP port number for the circuit.
   f. Enter the Destination UDP port number for the circuit.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Note: The Source and Destination UDP port numbers must match on each end of the circuit.

g. Select the IP Host name created above from the drop-down list.

h. Enter the Destination IP address of the circuit (the IP address of the ONT attached to the end of the pseudo-wire [via the E7 gateway]).

i. Ensure RTP is enabled and that the RTP mode is set to Absolute.

j. Under payload size, enter any value between 96-1152.

Note: The payload size entered must be in increments of 32.

k. Click **Add** and then Click **Create** to save the Endpoint settings.

Create the VLAN Interface for the PWE End Point

As a final step in creating the Hi-Cap T1 Service over a Multiprotocol circuit (SAToP), the VLAN-IF between the Local Bridge and the PWE Endpoint must be created.

To create the VLAN-IF for the PWE endpoint

1. Within CMS, navigate to the PW Endpoint just created.
2. From the VLAN-IF tab in the work area, choose Create > VLAN-IF > VLAN Interface
3. Accept the default values (or leave blank) all fields except as follows:
   a. Choose a matching VLAN ID for the Local bridge side of the circuit (to match the service VLAN for the DS1)
   b. In the Bridge/ATM Uplink field, choose Bridge and then choose Local.
   c. Select the PWE Card on the local bridge (C7).
   d. In the User-Side Parameters section, ensure Relay Change Tag (C-Tag) action is set to None.
4. Click Add and then click Create to save the VLAN-IF settings.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Confirming the Configuration

With all components completed, the configuration must be verified. Each component of the circuit can be verified using the TL1 interface included within CMS.

The various components of the Hi-Cap (SAToP) Multiprotocol and EXA PWE circuit are summarized in the table below.

Note: To access the TL1 interface from within the CMS Main Menu, choose **Tools > Telnet Console**

TL1 Command	Command Description	Expected Output
rtrv-vlan-IF::n1-1-all::::vlan=800, bridge=local	Retrieve details of all VLAN-IF's associated with Shelf N1-1 with a VLAN ID of 800 attached to the local bridge	N1-1-5-1-PW1::VLAN=800, BRIDGE=LOCAL, ARP=Y, ENCAP=ETHERNETV2, STP=OFF, DIRN=BOTH, STAGTYPE=CTAG_8100, PORTTYPE=EDGE, CVID-UNTAGGED, SVID=800, PRIO=0, RCVID=NONE, LEASEMT=16, MATCHLIST=NONE.
rtrv-pw::n1-1-all	Retrieve details of all PW circuits associated with shelf N1-1	N1-1-5-1-PW1::IPHOSTID=N1-1-5-HOST1, DSTIP=192.168.3.3,SRCUDP=1024, DSTUDP=1024,RTPTS=Y,RTPTSMODE=ABS, OCTETALIGN=N,PYLDSIZE=192,JBUFDEPTH=3000, GOS=DEFLT,DESC=\"PWE-C7-E7GPON-ONT\": OOS-AUMA,SGEO&SDEE
rtrv-t1::n1-1-5-all	Retrieve details of all DS1 ports configured on slot 5 of the shelf N1-1	"N1-1-5-1::TYPE=DS1,T1MAP=PWUNSTRUCT, EQLZ=100,FMT=UF,LINECDE=B8ZS,GOS=OFF, TMGMODE=ADAPT,IBLBCODE=00001,:OOS-AUMA, AINS&FAF&SDEE"
rtrv-vlaN-iF::n1-1-all::::vlan=800,bridge=n1-1-vb1	Retrieve details of all VLAN-IFs on Shelf N1-1 with a VLAN ID of 800 and a virtual bridge connection (VB-1)	N1-1-9-1::VLAN=800,BRIDGE=N1-1-VB1, ARP=Y,DHCPDIR=SERVER,OPT82ACT=PASS, IGMP=NONE,PPPOEAC=N,PPPOESUB=N, LSVID=800,ENCAP=ETHERNETV2,DOS=N, STP=1D_ADDR,STPCOST=19,STPPRIO=128, DIRN=BOTH,STAGTYPE=CTAG_8100, PORTTYPE=TRUNK,STPST=DISCARD, ROLE=ALTERNATE,RXETHBWPROF=NONE, TXETHBWPROF=NONE,LEASELMT=UNLIMITED N1-1-5::VLAN=800,BRIDGE=N1-1-VB1, ARP=N,DHCPDIR=CLIENT,OPT82ACT=PASS, IGMP=NONE,PPPOEAC=N,PPPOESUB=N, LSVID=800,ENCAP=ETHERNETV2,DOS=Y, STP=OFF,STPCOST=100,STPPRIO=128, DIRN=BOTH,STAGTYPE=CTAG_8100, PORTTYPE=TRUNK,RXETHBWPROF=NONE, TXETHBWPROF=NONE,LEASELMT=16

For the configuration above, it is also expected that you verify the PWE endpoint on the far end. In our example, The PWE endpoint exists as an E7 GPON PWE circuit. To ensure compatibility, verify the T1 PWE profile and any related service tag actions do not conflict with the above parameters.

Verify the following for the PWE parameters associated with the E7 GPON PWE circuit.

- The timing clock on the far end device is set to Adaptive
- Jitter buffer is set to 1500 microseconds

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- RTP is Enabled
- Packet size matches the packet size of the C7' s PWE card endpoint.
- RTP Timestamp mode is set to absolute.

Note: For any service tag actions associated with the circuit, ensure the P-Bit Source is set to Specify P-bit and the P-Bit value is given a high 802.1p priority (5 or above).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Troubleshooting PWE Services

When troubleshooting PWE services, Calix recommends the following general guidelines:

When provisioning PWE services, use the TL1 command at each provisioning step to confirm various service set-up parameters were executed as intended.

Note: To access the TL1 interface from within the CMS Main Menu, choose **Tools > Telnet Console**

Pseudowire Statistics

To view PWE statistics, run the initialize stats and retrieve stats command from the TL interface:

```
>INIT-STAT-PW::N1-1-8-2-PW1
>RTRV-STAT-PW::N1-1-8-2-PW1
MANU 11-05-01 13:01:54
M 1 COMPLD
   N1-1-8-2-
PW1::INOCT=326724486,OUTOCT=326732392,RXPKTS=4950371,TXPKTS=4950542,
RXRBITPKTS=0,RXLBITPKTS=0,RXMBITPKTS=0,OOWPKTS=0,BODPKTS=0;
   /* One record processed */
```

Verify IP Host Connectivity at the PWE port

To verify IP Host connectivity at the PWE port, pin the IP Hosts IP address using the TL1 interface.

```
> PING-IP-HOST::N1-1-8-2-PW1::::IP=192.168.99.100
MANU 11-05-01 06:40:01
M  1 COMPLD
   "N1-1-8:0:IP=192.168.99.100,PASS=Y,NPASS=1,NFAIL=0,MS=4,"
   "N1-1-8:1:IP=192.168.99.100,PASS=Y,NPASS=2,NFAIL=0,MS=4,"
   "N1-1-8:2:IP=192.168.99.100,PASS=Y,NPASS=3,NFAIL=0,MS=4,"
   "N1-1-8:3:IP=192.168.99.100,PASS=Y,NPASS=4,NFAIL=0,MS=4,"
   "N1-1-8:4:IP=192.168.99.100,PASS=Y,NPASS=5,NFAIL=0,MS=4"
   /* 5 records processed */
```

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Retrieving TDM Interface Statistics

TDM interface statistics can be retrieved or cleared on a per port basis using the TdmIf getstats or TdmIf clrstats commands:

```
/t/wp2/TdmIf getstats <portId>
/t/wp2/TdmIf clrstats <portId>
```

To view statistics for the PWE card in slot 8, port 1, do the following:

```
N1-1-8> TdmIf getstats 1
ces_rx_err_overrun = 0x0000000000000000
ces_tx_err_underrun= 0x0000000000000000
```

Bit Error Rate Testing (BERT) Overview

The DS1-12 PWE and T1-8 PWE cards include a set of troubleshooting tools to help lower overall service expense and OPEX. Beyond the diagnostic loop code functionality, the DS1-12 PWE and T1-8 PWE cards provide an integrated Bit Error Rate Test (BERT) functionality for each of the DS1/T1 ports on the card.

The DS1-12 PWE and T1-8 PWE support the ability to run Bi-Directional BERT testing without the need for an expensive handheld tester (such as a T-BERD). BERT is a testing method for DS1/T1 that uses predetermined stress patterns consisting of a sequence of logical ones and zeros generated by a pseudo-random binary sequencer. A BERT can be run towards the facility or towards the equipment depending on which end the technician is wanting to test.

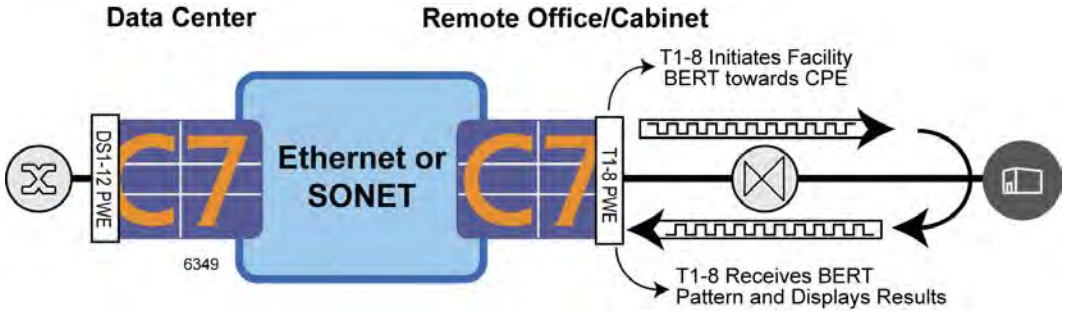
A BERT typically consists of a test pattern generator and a receiver that can be set to the same pattern. Technicians can use this integrated BERT function for both service turn up assurance and troubleshooting "in service" T1 links. BERT testing is service affecting by nature and should be used only in cases where traffic is impaired or suspended, or as part of an ongoing Quality Assurance regimen performed during a maintenance window.

The PWE cards can run BERT patterns on a port by port basis both towards the network and towards the subscriber.

Note: Once a BERT is in place, it will continue to run until the technician releases the test, similar to a loopback test.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

The following diagram depicts a Facility BERT towards the CPE device. From a remote location, the technician can initiate a loop towards the CPE or a repeater and have the T1-8 PWE card initiate the test and receive the return pattern for analysis and display.



BERT patterns allow the technician to test and diagnose in the field. The user can run this on an individual T1 on a PWE card port while all the other T1's continue to carry live traffic.

Traditionally a service technician would have to physically interface the T1 circuit for test with an external tester using the 4W interface on the C7 fan tray. While effective, this involves the need for a handheld tester, and also a truck roll. The technician would typically need to access the T1 at either the customer premise or at the C7 shelf where the T1 interfaces to the network. This can be particularly challenging for a CLEC, who may have the C7 shelf co-located within an incumbent's Central office, with limited access.
With integrated BERT support, the technician can run the same test from their Network Operations Center (NOC) via TL1, iMS or CMS, thus eliminating the need for an expensive tester or truck roll.

Guidelines for Integrated BERT function

Keep the following points in mind when performing BERT:

- BERT is supported on port by port basis for DS1-12 PWE and T1-8 PWE cards
- Test results are valid in an Ethernet or SONET transport environment
- PWE port must be Out Of Service (OOS) prior to running a BERT
- Transport between T1 end points must be provisioned before attempting a BERT
- Valid BERT direction includes Facility or Terminal
- BERT runs continuously until released
- Far end of test must be placed in loopback prior to initiating BERT
- Valid for ports configured as Unframed (Hi Cap only)
- Supported patterns:

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

- QRSS (Quasi Random Signal Source) – A pseudorandom binary sequencer which generates every combination of a 20-bit word, repeats every 1,048,575 bits, and suppresses consecutive zeros to no more than 14. It contains high-density sequences, low-density sequences, and sequences that change from low to high and vice versa. This pattern is also the standard pattern used to measure jitter.
- All Ones – A pattern composed of one's only. This pattern causes the repeater to consume the maximum amount of power. If DC to the repeater is regulated properly, the repeater will have no trouble transmitting the long ones sequence. This pattern should be used when measuring span power regulation.
- All Zeros – A pattern composed of zeros only. It is effective in finding equipment provisioned incorrectly for AMI.

Performing a Bit Error Rate Test

Prior to setting up a Bit Error Rate Test, ensure the following conditions are met:

- A DS1-12 PWE or T1-8 PWE card has been installed in the C7 shelf.
- The end-to-end PWE network uses an Ethernet or SONET based transport
- The PWE T1 End Points have been provisioned for service
- The port(s) to be tested are configured for Unframed, Hi-Cap service.

To configure a BERT

1. On one end of the PWE circuit, place the T1 port into the "Terminal" loopback mode:
   a. On the Navigation Tree, select the T1 port to place into loopback.
   b. In the Work Area, click the **Provisioning** tab.
   c. On the toolbar, click **Action > Operate Loopback > Terminal**.
2. On the other end of the PWE circuit, place the T1 port OOS:
   a. On the Navigation Tree, select the T1 port to perform the BER test.
   b. In the Work Area, click the **Provisioning** tab.
   c. Change the Primary Service State to Out Of Service (OOS).
   d. On the toolbar, click **Apply**, and then click **OK**.
3. Start the BERT test:
   a. With the T1 port still selected, in the Work Area, click the **BERT** tab.
   b. On the toolbar, click **Action > Operate BERT**
   c. In the Type list, select **Terminal**.
   d. In the Pattern list, select **QRSS**.
   e. Click **OK** to start the test.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

4. View and refresh results, and confirm that the BER is within acceptable limits.
5. End the test and return ports to previous settings:
   - For the T1 port performing the BERT, from the toolbar, click **Action > Release BERT**.
   - For the T1 port in loopback, from the toolbar, click **Action > Release Loopback**.

During BER testing, packets will be analyzed continuously and results displayed on the BERT table within CMS.

Retrieve the BERT statistics by selecting the line item in the BERT table for the DS1 service being analyzed. The data displayed is based on the last completed test run or the current test in progress.

Value	Description
Elapsed Time	Total elapsed since the BERT was initiated.
Bit Errors	Number of Bit Errors since the last Pattern Sync detected. The value will be zero if Pattern Sync is lost or has not been detected.
Elapsed Time since Synchronization is detected	Total elapsed time since Sync detected. 0- means no Sync.

Note: To stop the collection of Bit Error Rate data, choose Action > Release BERT.

DS1/T1 Loop-back

The PWE line units support two forms of loopbacks (administrative loopbacks and inband loop code detection) to assist technicians in turn up and troubleshooting. The loopbacks under software control are enabled in the C7 management interfaces. The following loopbacks under software control are supported on the DS-1/T1 interfaces on the PWE line units:

- Terminal
- Payload
- Facility

The loopbacks can be initiated via TL1, iMS and CMS.

Note: Administrative loopbacks override any active inband loopbacks. Care should be taken by the technician to coordinate loop back activity.

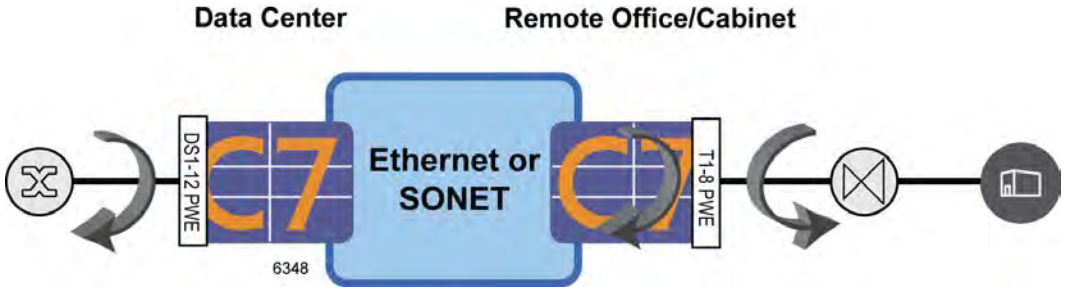
Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Logical loopback types

Depending on the transmission protocol, various parts of a signal can be looped back. Four types of loopbacks can be operated or released by a network element:

- Terminal (near end): The transmit signal loops back toward the terminal after it has passed through the framer, just before it reaches the external facility.
- Payload (far end): The signal entering the facility is looped back toward the facility after it passes through the framer. Only the payload is looped back. The card strips off the framing overhead and regenerates it.
- Facility (far end): The signal entering the facility is looped back toward the facility before it has passed through the framer. The signal loops back immediately after it arrives on the card.
- In band loopbacks: The C7 PWE cards supports T1 in-band loop code detection for troubleshooting T1 traffic over DS1/T1 lines. This in-band loopback is configured at the PWE card port and is enabled and disabled by inserting a specific repeating bit pattern into the DS1/T1 bit stream. In-band loopbacks allow the service provider to test DS1 circuits independently of the access network (C7) by isolating the transport side of the circuit. The inband loop code pattern is user configurable for each segment of the network. Testing is initiated externally from the C7 network using a third-party communication analyzer, such as a T-BERD test set.

In the diagram below, the user would configure a specific loopback pattern for each segment of the circuit (DS1-12 PWE or T1-8 PWE), and then publish those loop codes to ATT or Sprint for use in troubleshooting. Additionally, two commonly used inband loop codes, FAC2, and NREM are user selectable options for the DS1-12 PWE and T1-8 cards in the CMS and iMS.



Note: If the inband code is detected in the **egress** direction, a terminal loopback is automatically performed on the DS1 port. If the inband code is detected in the **ingress** direction, a facility loopback is automatically performed on the DS1 port.

Inband Loop-back Operation

Inband Loop-up and Loop-down codes are used when loopback activation and deactivation is required.

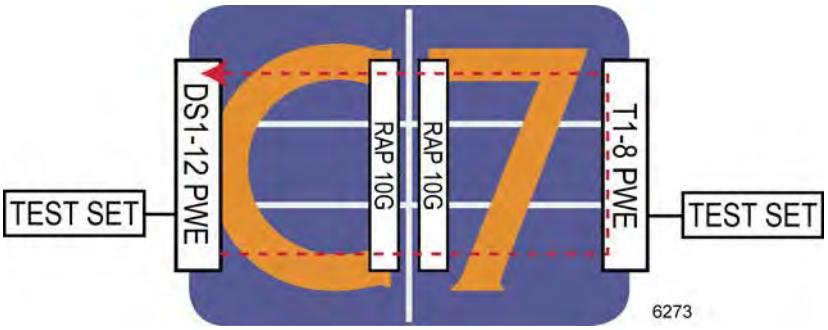
Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

In the configuration below, a T1-8 PWE card port is cross-connected to a DS1-12 PWE card port via normal means. Port settings include unframed DS1 service with loop timing in effect. Ports on both cards are connected to a test set (such as a T-BERD tester).

To initiate a loopback test

Note: The following test is service affecting. Make sure this test is performed during a maintenance window or planned outage only.

1. Send an inband loopup code such as 00001 from the T-BERD.
2. Verify the following on the test set:
   a. Signal is present
   b. Framing is Sync'd
   c. DS1 Line Coding displays B8ZS
   d. Pattern Sync is "up" (loopup is functioning)
3. To terminate the inband loopback and return to normal operation (in service), send a loop-down code of 001



Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Appendix A

Appendix A: C7 Service States

This section describes service states for C7 cards, ports, STS Paths, cross-connections, fan tray, and IMA groups. Service states for the C7 include the Primary Service State (PST), Primary Service State Qualifier (PSTQ), and the Secondary Service State (SST).

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Primary Service State

PSTs and PSTQs supported by the C7 are listed in the following table.

Primary Service State and Qualifier	Description
IS-NR	In-Service and Normal. The entity is fully operational and available for providing its provisioned functions. Normal indicates that no service-affecting conditions exist.
OOS-AU	Out of Service and Autonomous. The entity is not operational and not available to provide any of its provisioned functions. The Autonomous qualifier indicates it is out of service due to fault conditions. Since MA is not present it is administratively allowed to perform its functions.
OOS-AUMA	Out of Service and Autonomous and Management. The entity is not operational and not available to provide any of its provisioned functions due to an autonomous event. The Management qualifier indicates that it has been administratively placed out of service. An administratively suspended entity does not generate alarms.
OOS-MA	Out of Service and Management. The entity is out of service and not available to provide any of its provisioned functions. The Management qualifier indicates that it has been administratively placed out of service. An administratively suspended entity does not generate alarms.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Secondary Service State

SSTs supported by the C7 are listed in the following table.

Secondary Service State	Description
ADA	Automatically Default Assigned. The entity was automatically assigned default provisioning. Editing operations are permitted in the ADA service state.
AINS	Automatic In Service. The entity is delayed before transitioning to IS-NR state. The transition is pending the correction of off-normal conditions.
CRS	Cross Connected. The entity is currently supporting at least one cross-connection. The entity cannot be deleted without first deleting the cross-connections associated with the entity.
DGN	Diagnose. The ADSL line is initializing.
FAF	Facility Failure. FAF is assigned to a port when a problem has been detected with its associated facility.
FLT	Fault. Equipment entity is out of service due to a fault or a circuit has a fault along the path.
IDLE	Idle. The line is able to provide service, but is currently idle.
LPBK	Loopback. The entity is in loopback mode.
MEA	Mismatch of Equipment and Attributes. Improper equipment is installed or there are improper attributes.
MT	Maintenance. The entity has been manually removed from service for maintenance activity. Diagnostic traffic can be carried. Alarm reporting is suppressed.
NBK	No Backup. There is no backup for the entity provisioned with backup.
PRI	Protection Release Inhibited. The entity is inhibited from release from protection.
PUA	Provisioning Unavailable.
PWR	Power. A power management activated condition has occurred. Power is abnormal or there is a defect in the power.
RDLD	Red Lined. The entity can only be deleted with the proper specifications.
SB	Suspend Both. For example, suspend both Tx and Rx.
SDEE	Supported Entity Exists. The entity is currently supporting other

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Secondary Service State	Description
	entities and cannot be deleted without deleting the supported entities or without having special delete privileges.
SETH	Supported Ethernet Entity. The entity is currently associated with an Ethernet entity, such as an LSwitch or VLAN. It cannot be deleted without first removing the association.
SFFP	Supported Fast Facility Protection. The entity is currently supporting an FFP and cannot be deleted without first deleting the associated FFP.
SGEO	Supporting Entity Outage. The entity is unable to provide service because an entity supporting it has an outage.
STBYC	Standby Cold. The backed up entity is not synchronized. It may be in the process of initializing or cannot initialize. If it cannot initialize, then an additional SST qualifies.
STBYH	Standby Hot. The entity is able to immediately take over from any one of the entities it is backing up. (An exception is LAPD links that cannot be switched during an equipment protection switch.)
STBYI	Standby Inhibited. The entity has another entity designated as its backup but protection switching has been inhibited. The STBYI state has a higher priority than the STBYC state.
STBYS	Standby Switched. This indicates that the standby entity has taken over the role of the backed up entity in a revertive system.
STMG	Supported Timing Reference. The entity is currently being used as a timing reference and cannot be deleted without first changing the timing reference to another entity.
SWTCH	Switching system activity. The entity has been removed from service because of switching system.
TS	Test. There is metallic testing activity.
UAS	Unassigned. The entity has not been assigned with the necessary provisioning data.
UEQ	Unequipped. The entity is not physically present.
WRK	Working. The redundant entity is currently providing the provisioned service.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Appendix B: Security Log Events

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

The events that can be recorded in the C7 security log are listed in the following table.

Event	Description
CANC	A user's session was canceled.
CHAP	CHange Access Privileges. Access privileges for a management port were changed.
LOGBUFR90	The security log buffer is 90% full.
LOGBUFROVFL	Log buffer overflow for the security log.
LOGIN	A user logged in.
LOGINFAIL	A user's login attempt failed.
LOGOUT	A user logged out.
MGMTIF	The Management Interface IP Address was modified.
NORADAMP	Both provisioned RADIUS client AMPs are not functioning. For recommended actions, see the *Calix C7 Troubleshooting Guide*.
NORADSERV	Both provisioned RADIUS servers are unresponsive. For recommended actions, see the *Calix C7 Troubleshooting Guide*.
NORMAL	Normal condition exists.
PIDEXP	A user's password expired.
RADAMPFAIL	The primary RADIUS client AMP is not functioning. For recommended actions, see the *Calix C7 Troubleshooting Guide*.
RADSERVFAIL	The primary RADIUS server is unresponsive. For recommended actions, see the *Calix C7 Troubleshooting Guide*.
SECUDENY	A user was denied access due to insufficient privileges.
SSHFAIL	A failure of the designated AMP's secure shell application to start. It must be cleared by resetting that AMP. For recommended actions, see the *Calix C7 Troubleshooting Guide*.
SYSSECUPROV	System security data has been modified in the management interface or using the ED-SYS-SECU TL1 command.
TMPLPROV	A security template was provisioned.
USERPROV	A user was provisioned.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Appendix C: List of Acronyms

Acronym	Description
AAL	ATM Adaptation Layer
AMP	Administration and Maintenance Processor
APC	Angled Physical Contact (connector)
ATM	Asynchronous Transfer Mode
ATP	Administration and Test Processor
AVO	Analog Video Overlay
BERT	Bit Error Rate Test
BPON	Broadband Passive Optical Network
BWCID	Bandwidth Constraint ID
CATV	Cable Television
CBR	Constant Bit Rate
CBT	Composite Triple Beat
CESoPSN	Circuit Emulation Service over Packet Switched Network
CMS	Calix Management System
CNR	Carrier to Noise Ratio
CoS	Class of Service
CPE	Customer Premises Equipment
CRV	Call Reference Value

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Acronym	Description
CSO	Composite Second Order
CTB	Composite Triple Beat
CUP	Calix Upgrade Program
CWDM	Coarse Wavelength Division Multiplexing
DACS	Digital Access & Cross-Connect System
DBA	Dynamic Bandwidth Allocation
EGW	Ethernet Gateway card
EDFA	Erbium-Doped Fiber Amplifier
EPG	Electronic Programming Guide
ERPS	Ethernet Ring Protection Switching
EXA	Ethernet eXtensible Architecture
FTTP	Fiber to the Premises
GA	General Availability
GbE	Gigabit Ethernet
GEM	GPON Encapsulation Method
GFR	Guaranteed Frame Rate
GPON	Gigabit Passive Optical Network
GSFn	General Signaling Function
HPNA	Home Phoneline Networking Alliance
IAD	Integrated Access Device
IG	Interface Group
IGMP	Internet Group Management Protocol
IMA	Inverse Multiplexing over ATM
iMS	integrated Management System
IPTV	Internet Protocol Television
IRC	IP Resource Card
IS	In Service (primary service state)
LACP	Link Aggregation Control Protocol
LAG	Link Aggregation Group
MCR	Minimum Cell Rate
MDU	Multi-Dwelling Unit

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Acronym	Description
MPLS	Multi-Protocol Label Switching
MSTV	Microsoft TV protocol
MTU	Multi-Tenant Unit
OAM	Operation, Administration, and Maintenance
OCMI	ONT Management Control Interface
ODN	Optical Distribution Network
OLTB	Optical Line Termination BPON-2 port
OLTG	Optical Line Termination GPON-4 port or GPON-4E port
OMCC	ONT Management and Control Channel
OMCI	ONT Management and Control Interface
ONT	Optical Network Terminal
OOS	Out of Service (primary service state)
OSP	Outside Plant
OTDR	Optical Time Domain Reflectometer
PCR	Peak Cell Rate
PDV	Packet Delay Variance
PLOAM	Physical Layer OAM
PON	Passive Optical Network
PPV	Pay Per View
PST	Primary Service State
PWE3	**P**seudo**W**ire **E**nd-to-**E**nd **E**mulation
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
RAP	Resource Arbitration Processor
RF	Radio Frequency
RTLP	Receive Transmission Level Point
SAI	Service Area Interface
SAToP	Structure-Agnostic TDM over Packet
SB	Suspend Both (secondary service state)
SBU	Small Business Unit

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Acronym	Description
SDBER	Signal Degraded Bit Error
SFU	Single Family Unit (an ONT designed for residential use)
SST	Secondary Service State
SVS	Switched Video Services
SWRD	Single Wire Return Device
T1TG	T1 Transport Group
TF	Transmitter Failure
TC	Transmission Convergence
TCA	Threshold Crossing Alert
TLS	Transparent LAN Service
TL1	Transaction Language 1
TTLP	Transmit Transmission Level Point
UBR	Unspecified Bit Rate
UNI	User Network Interface
UPC	Ultra Physical Contact (connector)
VB	Virtual Bridge
VC	Virtual Channel
VCG	Voice Concentration Group
VDS1	Virtual DS1
VGP	Voice Gateway Processor
VIPR	Voice over IP Resource
VOD	Video on Demand
VoIP	Voice over Internet Protocol
VP	Virtual Path
VR	Virtual Router
VRP	Video Return Path
WDM	Wavelength Division Multiplexing

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

Appendix D: PWE Card Capacities

Description	DS1-12 PWE	T1-8 PWE
Ports	12	8
Repeater Powering	No	60 ma constant current source at -130 VDC (up to 7 repeaters)
GR-303 Interface Groups	Up to 12	Up to 8
GR-08 Interface Groups (Mode I)	Up to 3	Up to 2
GR-08 Interface Groups (Mode II)	Up to 6	Up to 4
GR-303 CRV per IG	2048	2048
GR-08 CRV per IG	96	96
IP Hosts	Up to 12	Up to 8
VLAN Models	VLAN Per Service VLAN Per Subscriber (Single or Double Tagged)	VLAN Per Service VLAN Per Subscriber (Single or Double Tagged)
Hops in between T1 End Points	TDM: 20 C7 codes PWE (C7 only): 16 total PWE (C7/E7 Mixed): 16 total	TDM: 20 C7 nodes PWE (C7 only): 16 total PWE (C7/E7 Mixed): 16 total

PWE Card Bundle Capacities				
Bundle Count	**Protocol Type**	**Timing**	**DS1-12 PWE card**	**T1-8 PWE card**
SAToP PWE Bundles Note: Each SAToP T1 uses a single PWE bundle	Packet Sampling (Multi-protocol or EXA)	.5 ms	12 (per card)	8 (per card)
		1 ms	12 (per card)	8 (per card)

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.

CESoPSN PWE Bundles Note: Each CESoPSN T1 uses bundles as shown	Packet Sampling (Multi-protocol)	.5 ms	112 (per card) 24 (per Trunk VC with 1 DS0 per bundle) 16 (per Trunk VC with 2-12 DS0s per bundle) 12 (per Trunk VC with greater than 12 DS0s per bundle)	96 (per card) 24 (per Trunk VC with 1 DS0 per bundle) 16 (per Trunk VC with 2-12 DS0s per bundle) 12 (per Trunk VC with greater than 12 DS0s per bundle)
		1 ms	208 (per card) 24 (per Trunk VC with 1 DS0 per bundle) 16 (per Trunk VC with 2-12 DS0s per bundle) 12 (per Trunk VC with greater than 12 DS0s per bundle)	192 (per card) 24 (per Trunk VC with 1 DS0 per bundle) 16 (per Trunk VC with 2-12 DS0s per bundle) 12 (per Trunk VC with greater than 12 DS0s per bundle)
	Packet Sampling (EXA)	.5 ms	136	120
		1 ms	240	192

Proprietary Information: Not for use or disclosure except by written agreement with Calix.
© Calix. All Rights Reserved.