Calix E7 R2.1 Maintenance and Troubleshooting Guide

December 2012

#220-00483, Rev 11

Contents

Chapter 3: Troubleshooting.....135

About This Guide

The *Calix E7 Troubleshooting Guide* includes procedures for monitoring E7 network operation, general troubleshooting, and replacing or installing equipment.

The Calix E7 platform topics in this guide apply to Calix standalone E7-2, Modular Chassis, and E7-20 systems, where E7 is used to refer to the set of products in the platform.

Note: Procedures in this document are based on the E7 user interface from E7 software version R2.1.40 and above.

Intended Audience

This document is intended for use by network planning engineers, CO technicians, and craft and support personnel responsible for network equipment turn-up, service configuration, and maintenance. The procedures in this guide are of a technical nature and should only be performed by qualified personnel. Familiarity with standard telecom and datacom terminology and practices, as well as standards-based Ethernet technologies and conventions, is recommended.

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 E7 documentation set includes:

- *Calix E7-2 Installation Guide*
- *Calix E7-20 Installation Guide*
- *Calix E7 User Guide*
- *Calix E7/E5-400 CLI Reference*
- *Calix E7 GPON Applications Guide*
- *Calix E7 xDSL Application Guide*
- *Calix E7 Active Ethernet Applications Guide*
- *Calix T1 Pseudowire Application Guide for MDU ONTs*
- *Calix E7 Engineering and Planning Guide*
- *Calix E7/E5-400 Software Upgrade Guide*
- *Calix E7 Maintenance and Troubleshooting Guide*

Chapter 1

Monitoring an E7 Network

This chapter describes how to perform E7 device monitoring functions and tasks.

Topics Covered

This chapter covers the following topics and tasks:

- Configuring Ethernet port mirroring
- Configuring a VLAN monitor
- Configuring a power monitor
- Configuring a Syslog server
- Configuring and viewing Ethernet OAM
- Viewing notification logs
- Viewing PON bandwidth reports
- Viewing and deleteing DHCP leases
- Monitoring performance data

Configuring Ethernet Port Mirroring

This topic describes how to configure an E7 Ethernet port to mirror traffic from one or more source GE, 10GE, GPON, or xDSL ports for observation.

Important! Port mirroring should only be enabled on a temporary basis as it causes high CPU utilization.

Configuration guidelines

- The port mirror can only be established between GE, 10GE, GPON, or xDSL ports within a single E7-2 line card.
- The Destination Port must be an Ethernet port.
- The Source Port can be GE, 10GE, GPON, or xDSL ports.

  Note: Ethernet port mirroring is not supported on the E7-20. Alternatively, a port mirror can be established on the upstream router of the aggregation switch.

- By default, both ingress and egress traffic will be mirrored. To mirror only one of those, use the "type" option.
- If the mirrored traffic destination port is a GE port, the mirrored traffic data must be less than 1Gig to ensure the data accuracy.
- The destination port interface of the mirror must be a member of the VLAN carrying the traffic that you want to mirror.
- The following CPU generated frames are passed to a port mirror: RSTP BPDUs, LACP PDUs, IGMP when IGMP snooping is enabled, DHCP when DHCP snooping is enabled, and Management VLAN traffic from the host (Telnet, HTTP, SNMP).
- When a VLAN has the PON Hairpin parameter enabled, the hairpin traffic will not appear on an E7 port mirror.
- If there is a change-tag or add-tag action on the source port interface, the destination port interface must be a member of both VLANs (original and changed or added VLAN).
- The port configured as the destination for mirrored traffic should be reserved for this purpose and not be used for regular network traffic.
- The Monitor Type of mirroring for a source port cannot be edited. Delete the source port from the mirror, and then recreate it with the desired type of mirroring.

Note: TLAN traffic that is hairpinned back on the same GPON OLT port will not appear in an E7 port mirror session.

Parameters for an Ethernet port mirror

Parameter	Description	Valid Options
ID	Ethernet port mirror ID.	1
Destination Port	Ethernet ports specified by card, port type, and port number. For example: 1/g1. Legal values for the port type are "g" (for Gigabit Ethernet), "x" (for 10-Gigabit Ethernet), or "v" (for VDSL2). For modular chassis E7-2, ports are specified by shelf/card/port type and port number. For example: 1/2/v4.	GE:(card/port) 10GE:(card/port) GPONPort:(card/port) 10GE:(card/port) DslPort:(card/port)
Admin State	Service state of the Ethernet port mirroring. Disabling the eth-mirror stops sending the source traffic to the mirror destination. Enabling the eth-mirror restarts the sending of traffic.	enabled disabled
Source Port	Source port to add to the Ethernet mirror.	EthGe:(card/port) Eth10Ge:(card/port)
Monitor Type	Type of traffic to mirror. By default, both ingress and egress traffic will be mirrored. To mirror only one of those, select the "type" option.	off ingress egress both

To configure Ethernet port traffic mirror settings

1. On the Navigation Tree, click any GE or 10GE port.
2. Click the **Eth Mirror** tab.
3. From the menu, click **Create**.
4. In the Create Ethernet Port Mirror dialog box, do the following:
   a. In the ID box, allow the system to set to index, as it will automatically increase to the next available value.
   b. In the Destination Port list, select the Ethernet port to act as a mirror for traffic received from another port on the same card.
   c. In the Admin State list, select whether the port mirror is in service.
      - Disabling the Ethernet mirror stops sending the source traffic to the mirror destination.
      - Enabling the Ethernet mirror restarts the sending of traffic.
   d. Click **Create**.

   The table is updated and shows the newly-created Ethernet port mirror.

For CLI:

- **`create eth-mirror dest-eth-port <card/port ID> [admin-state]`**
- **`set eth-mirror admin-state enabled`**
- **`enable eth-mirror`**
- **`show eth-mirror`**

To add ports to the Ethernet mirror

1. On the Navigation Tree, click any GE or 10GE port.
2. Click the **Eth Mirror** tab.
3. In the table of available Ethernet mirrors, double-click the ID of the Ethernet Mirror on which to add a source port.
4. In the Menu, click **Create** > **Add Source Port**.
5. In the Create Mirror Source Port dialog, do the following:
   a. In the Source Port list, select a port on the same card to act as the source of traffic to be mirrored.
   b. In the Monitor Type list, select the type of traffic to mirror.
      - **both** will mirror both ingress and egress traffic from the source port.
      - **ingress** will mirror only ingress traffic from the source port.
      - **egress** will mirror only egress traffic from the source port.
      - **off** will not mirror traffic from the source port from the source port.
   c. Click **Create**.
   d. In the Create Mirror Source Port dialog box, do the following:
   e. In the Source Port list, select the E7 Ethernet port to add as a traffic source for the Ethernet port mirror.
   f. In the Monitor Type list, select the traffic type to mirror.
   g. Click **Create**.
6. Make the destination port interface of the mirror a member of the VLAN carrying the traffic that you want to mirror. See "Creating VLAN Memberships," in the *Calix E7 User Guide* if necessary. If there is a change-tag action on the source port, add the destination port interface to both the incoming VLAN membership and the change-tag VLAN membership.
7. Repeat Steps 4, 5, and 6 to add other source ports to the Ethernet port mirror to observe.

For CLI:

- **`add eth-port <card/port ID> to-eth-mirror [type]`**
- **`add gpon-port <port ID> to-eth-mirror [type]`**
- **`add dsl-port <port ID> to-eth-mirror [type]`**
- **`add interface <interface name> to-vlan <vlan ID>`**

To delete a source port from an Ethernet port traffic mirror

1. On the Navigation Tree, click any GE or 10GE port.
2. Click the **Eth Mirror** tab.
3. Double-click the ID in the table row to select the Ethernet port mirror and list the mirror source ports.
4. In the Mirror Source Port area of the screen, click the row in the table to select a source port.
5. From the menu, click **Delete**, and then click **Delete** in the verification dialog box.
6. Repeat Steps 4 and 5 to delete any other source ports in the Ethernet mirror.
7. From the menu, click **Apply**.

For CLI:

- `remove eth-port <port ID> from-eth-mirror`
- `remove gpon-port <port ID> from-eth-mirror`
- `remove dsl-port <port ID> from-eth-mirror`

To delete an Ethernet port traffic mirror

1. On the Navigation Tree, click any GE or 10GE port.
2. Click the **Eth Mirror** tab.
3. Click the table row to select the Ethernet port mirror.
4. From the menu, click **Delete**.
5. In the Delete dialog box, click the **Forced** check box to allow the deletion of the port mirror, although there are source ports currently assigned to the port mirror.
6. Click **Delete**.

For CLI:

```
delete eth-mirror
```

Configuring a VLAN Monitor

This topic describes how to configure a E7 monitor for collecting statistics for a specified VLAN on a specified Ethernet interface. The statistics collected are packet counts, similar to the statistics collected for Ethernet ports and ERPS domains.

Note: The VLAN monitor begins collecting statistics when it is created.

Before starting

The VLAN to be monitored must be created on the E7 and the specified Ethernet interface must be added to the VLAN membership.

Parameters for a VLAN monitor

Parameter	Description	Valid Options
ID	Index number of the VLAN monitor.	1–30
VLAN	Name of VLAN or VLAN ID to specify as part of the VLAN monitor.	31 characters
Interface	Ethernet interface to specify as part of the VLAN monitor. **Note:** LAG interfaces are not supported in a VLAN monitor.	EthIntf:(card/GE/port) EthIntf:(card/10GE/port) EthIntf:(card/VDSL2/port)
Admin State	State of the monitor. Disabling the monitor stops the collection of statistics.	enabled disabled

To configure a VLAN monitor

1. On the Navigation Tree, click **VLANs**.
2. Click the **Vlan Monitors** tab.
3. In the menu, click **Create**.
4. In the Create VLAN Monitor dialog box, do the following:
   a. In the ID box, select an index number for the VLAN monitor object.
   b. In the VLAN box, enter the ID or name of the VLAN to specify it as part of the VLAN monitor.
   c. In the Interface box, select the Ethernet interface to specify it as part of the VLAN monitor.
   d. In the Admin State box, select whether the VLAN monitor is in service. The VLAN monitor begins collecting statistics when it is created.
   e. Click **Create**.

   The table is updated with the new VLAN monitor.

5. Double-click on the newly created entry to view the VLAN monitor statistics.

For CLI:

`create vlan-monitor <vlan monitor ID> interface <interface name> vlan <vlan ID>`

The interface can be indicated by a name or a range of Ethernet interfaces specified by a hyphen (for example, 1/g3-1/g8).

- **`set vlan-monitor <vlan monitor ID> admin-state enabled`**
- **`show stats vlan-monitor [<vlan monitor ID>]`**
- **`delete vlan-monitor <vlan monitor ID>`**

Use the following commands to control the VLAN monitor statistics collection:

- If you want to stop the collection of statistics, use either of the following commands:
  - **`disable vlan-monitor <vlan monitor ID>`**
  - **`set vlan-monitor <vlan monitor ID> admin-state disabled`**
- If you want to clear the existing statistics and restart the collection of statistics when the monitor is in the disabled state, use either of the following commands:
  - **`enable vlan-monitor <vlan monitor ID>`**
  - **`set vlan-monitor <vlan monitor ID> admin-state enabled`**

Configuring a Power Monitor

This topic describes how to configure a monitor for the E7 power sources.

Parmeters

You can provision the following parameters for a VLAN monitor:

Parameter	Description	Valid Options
Admin State	Index number of the VLAN monitor.	1–30
Monitor Mode	Name of VLAN or VLAN ID to specify as part of the VLAN monitor.	Source A and B, Source A, Source B, None
Interface	Ethernet interface to specify as part of the VLAN monitor.	EthIntf:(card/GE/port) EthIntf:(card/10GE/port)
Admin State	State of the monitor. Disabling the monitor stops the collection of statistics.	enabled disabled

To configure a power monitor

1. On the Navigation Tree, click **E7**.
   - For the E7-2, click **Shelf#**.
2. In the Work Area, click **Power Zone**.
   - For the E7-20, double-click the power zone of which to set the power monitor.
3. In the Power Zone form, do the following:
   a. In the Admin State list, select whether the monitor is enabled.
   b. In the Monitor Mode list, select which power source is monitored.
4. In the menu, click **Apply**.
5. For the E7-20, click **Table View** to double-click another power zone and configure the power monitor mode.

For CLI:

```
(E7-2 only) set power monitor-mode <mode>
(E7-20 only) set power <zone> <monitor-mode <mode>|admin-state>
```

Note: For the E7 modular chassis system, this command is not supported. Instead, use the **`set shelf`** command to set the power monitoring attributes for an MC shelf.

Configuring a Syslog Server

This topic describes how to configure a E7 Syslog server that can receive system notifications of various types:

- OAMP alarms
- Events
- Database change
- Security
- Threshold crossing alerts (TCA)

Each SYSLOG server record contains the following information:

- DNS resolvable name or IP address
- Description
- Administrative state
- Indication of which OAMP notification types are to be sent to this server

When data is logged via syslog it is assigned a particular severity and logged against a specific facility. The syslog facility is one information field associated with a syslog message and is used to distinguish different classes of syslog messages. There are eight generic facilities (local0 – local7) and those are made available via the E-series provisioning interface to be mapped to things like alarms and events. Each log entry created will be logged against one of those facilities as specified in the E-series provisioning, and the remote syslog server can be configured to treat them independently.

Parameters

You can provision the following parameters for a Syslog server:

Parameter	Description	Valid Options
ID*	Index number of the Syslog server.	1-4
Host*	Hostname or IP address of Syslog server.	31 character text string of hostname or an IP address in "dotted quad" format. For example, "192.168.1.100".
Description	Description of the Syslog server.	31 character text string
Admin State	Admin state of Syslog server.	enabled disabled
Alarm Facility	Syslog facility level to use for alarms.	none, local0, local1, local2, local3, local4, local5, local6, local7
DB Change Facility	Syslog facility level to use for database changes.	none, local0, local1, local2, local3, local4, local5, local6, local7

Parameter	Description	Valid Options
Event Facility	Syslog facility level to use for events.	none, local0, local1, local2, local3, local4, local5, local6, local7
Security Event Facility	Syslog facility level to use for security events.	none, local0, local1, local2, local3, local4, local5, local6, local7
TCA Facility	Syslog facility level to use for TCAs.	none, local0, local1, local2, local3, local4, local5, local6, local7

To configure a Syslog server

1. On the Navigation Tree, click **E7**.
2. Click the **System** > **Syslog** tabs.
3. In the toolbar, click **Create**.
4. In the Create Syslog Server dialog box, do the following:
   a. In the ID list, select an index number for the VLAN monitor object (range 1-4).
   b. In the Host box, enter the name or IP address of the Syslog server.
   c. In the Description box, enter a description for the Syslog server.
   d. In the Admin State list, select whether the Syslog server is in service.
   e. In the Alarm Facility list, select the Syslog facility level to use for alarms.
   f. In the DB Change Facility list, select the Syslog facility level to use for database changes.
   g. In the Event Facility list, select the Syslog facility level to use for events.
   h. In the Security Event Facility list, select the Syslog facility level to use for security events.
   i. In the TCA Facility list, select the Syslog facility level to use for TCAs.
   j. Click **Create**.
5. Double-click on the newly created entry to view the VLAN monitor statistics.

To modify a Syslog server configuration

1. On the Navigation Tree, click **E7**.
2. Click the **System** > **Syslog** tabs.
3. In the list of configured Syslog servers, click to select the server to modify.
4. Modify the parameters, and then click **Apply**.

To delete a Syslog server configuration

1. On the Navigation Tree, click **E7**.
2. Click the **System** > **Syslog** tabs.
3. In the list of configured Syslog servers, click to select the server to delete.
4. In the toolbar, click **Delete**, and then **Delete** again in the dialog box to confirm.

For CLI:

- `show syslog-server`
- `create syslog-server`
- `set syslog-server`
- `enable syslog-server`
- `disable syslog-server`
- `delete syslog-server`

Configuring Interface Quality Audit

High layer protocols, such as ERPS, RSTP or LACP are typically relied on for disabling a failed interface. Certain failure conditions, such as conditions that only affect larger frames, or low Bit Error Ratio (BER) conditions, may impact subscriber traffic but not impact the higher layer protocol enough to cause the interface to be brought out of service. The E7 offers a mechanism to provide a sort of BER threshold in order to prevent these situations from impacting subscriber traffic.

This topic shows you how to configure the Interface Quality Audit (IQA) function periodically checks the number of File Check Sequence (FCS) errors received as a percentage of total frames received on an interface. An interface that exceeds the provisioned thresholds can be set to generate an alarm, switch traffic to an alternate path, or force the interface to an OOS state where operator intervention is required to bring the interface to an operational state by manually disabling the interface, and then re-enabling the interface.

Parameters

You can provision the following parameters for LAG or Ethernet interfaces:

Parameter	Description	Valid Options
Interface Quality Audit Mode	Mode to periodically check the number of File Check Sequence (FCS) errors received as a percentage of total frames received on an interface. An interface that exceeds the provisioned thresholds can be set to one of the following modes: • **no-audit** - disables the Interface Quality Audit (IQA) mode • **alarm-only** - generates an alarm, but, does not take any action on the interface • **disable-interface** – Disable the interface when the threshold is exceeded • **protocol-action** – For ERPS and LAG, only disable the interface if there is an alternate path that is up and available. For non-ERPS and non-LAG interfaces, this is interpreted as “alarm only.”	no-audit, alarm-only ‡, protocol-action, disable-interface
Polling Interval	Number of seconds between interface quality audits that compare errored frames to total received frames.	1-60 1 ‡
Error Threshold	Number of errored frames per million total frames to consider a specific interval as failed.	1-100000 1000 ‡
Polling Window	Number of interface quality audit intervals to consider for failure determination.	10-60 60 ‡
Errored Interval Count	Number of failed audit quality intervals within the polling window that will indicate an interface failure for IQA to take an alarm or OOS action.	1-60 10 ‡
Interval Min Frames	Minimum number of frames that must be received per interval for a specific interval to be considered valid.	1-2147483647 100 ‡

To configure the interface quality audit operation.

1. On the Navigation Tree, click a **GE** or **10GE** port where you want to configure an associated interface.
2. In the Work Area, click **Associated Interface > Provisioning**.
3. In the Interface Quality Audit Mode list, select the mode of operation for the interface when that interface exceeds the provisioned thresholds.
4. In the Polling Interval box, enter the number of seconds between interface quality audits that compare errored frames to total received frames.
5. In the Error Threshold list, select the number of errored-frames-per-million-total-frames to consider a specific interval as failed.
6. In the Polling Window box, enter the number of interface quality audit intervals to consider for failure determination.
7. In the Errored Interval Count box, enter the number of failed audit quality intervals within the polling window that will indicate an interface failure for IQA to take an alarm or OOS action.
8. In the Interval Min Frames box, enter the minimum number of frames that must be received per interval for a specific interval to be considered valid.
9. Click **Apply**.

For CLI:

```
set interface <interface name> [role|description|native-
vlan|mtu|rstp-active|rstp-prio|rstp-path-cost|rstp-bpdu-mac|rstp-
edge|bpdu-guard|immediate-leave|ingress-policy-map|split-horizon-
fwd|lacp-role|lacp-hash-method|lacp-min-ports|lacp-max-ports|lacp-
system-priority|lag-cross-card|lag-cross-card-
revert|trusted|ethertype|iqa-mode|iqa-polling-interval|iqa-error-
threshold|iqa-polling-window|iqa-error-interval-count|iqa-interval-
min-frames|admin-state]
```

Digital Diagnostics Monitoring

Optical SFP transceivers support Digital Diagnostics Monitoring (DDM) functions according to the industry-standard SFF-8472, and is also known as Digital Optical Monitoring (DOM). This feature allows you to monitor real-time parameters of the SFP. The digital diagnostics monitoring (DDM) information for each module includes:

- Temperature (Celsius)
- Transmit Power (mWatts)
- Transmit Bias Current (mAmps)
- Receive Power (mWatts)
- Supply voltage (mVolts)

In the CLI, use: **`show eth-port card/slot/port detail`**

In web browser interface or CMS, look at the Ethernet port status and the detailed information is at the bottom of the screen.

Viewing Notification Logs

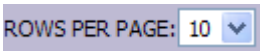
This topic describes how to view the various notification logs available from the E7.

The E7 keeps a record of the last 500 incidents of system activity in the following categories:

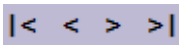
- Alarm assertion and clearing
- Event notifications
- Database changes from provisioning
- Security events from login attempts
- Threshold crossings

To view notification logs

1. On the Navigation Tree, click **E7**.
2. In the Work Area, click **System** > **Logs**.
3. Select the notification log to view:
   - Click **Alarm Log** to view a list of alarms that occurred and when they cleared.
   - Click **Event Log** to view a list of various system activities.
   - Click **DB Change** to view the E7 provisioning changes.
   - Click **Security Log** to view the list of E7 login attempts.
   - Click **TCA Log** to view information on the threshold crossing incidents.
4. View the log data using the Rows Per Page and page browser navigation tools:
   - Use the Rows Per Page drop-down list to control how many rows to display on one log screen page.

   - Use the page browser buttons to view the data on the immediate log pages (back and next) and the first and last pages in the log.

Note: To delete the contents of the log you are viewing, click **Action** > **Clear Log**.

For CLI:

- `show log alarm [all|first *|from-seq * count *|last *|since <YYYY/MM/DD:HH:MM>|from <YYYY/MM/DD:HH:MM> to <YYYY/MM/DD:HH:MM>]`
- `show log dbchange [all|first *|from-seq * count *|last *|since <YYYY/MM/DD:HH:MM>|from <YYYY/MM/DD:HH:MM> to <YYYY/MM/DD:HH:MM>]`
- `show log event [all|first *|from-seq * count *|last *|since <YYYY/MM/DD:HH:MM>|from <YYYY/MM/DD:HH:MM> to <YYYY/MM/DD:HH:MM>]`

- **show log security [all|first *|from-seq * count *|last *|since <YYYY/MM/DD:HH:MM>|from <YYYY/MM/DD:HH:MM> to <YYYY/MM/DD:HH:MM>]**

- **show log tca [all|first *|from-seq * count *|last *|since <YYYY/MM/DD:HH:MM>|from <YYYY/MM/DD:HH:MM> to <YYYY/MM/DD:HH:MM>]**

Viewing PON Bandwidth Reports

This topic describes how to view the various PON bandwidth reports available from the E7. The reports are based on Admitted Bandwidth, which is bandwidth that has been provisioned and enabled on an ONT that is linked on the PON.

Also see "Creating an Ethernet Bandwidth Profile" and "Creating a PON Class of Service" in the *Calix E7 User Guide* or *Calix E7 GPON Applications Guide*.

The E7 can present the provisioned PON bandwidth, the remaining unused PON bandwidth, and the over subscription percentage in the following views:

Aggregate

- Guaranteed traffic includes Expedited Forwarding and CIR component of Assured Forwarding classes.
- Non-guaranteed traffic includes excess (PIR-CIR) component of Assured Forwarding plus Best Effort classes.
- Available Rate will fall to 0 (zero) when Admitted Rate = Maximum Rate for each traffic class. At this point, "Admitted % Max" equals 100%.
- Guaranteed traffic may not be oversubscribed; therefore "Admitted % Max" will never exceed 100%.
- For upstream Non-guaranteed traffic, if additional bandwidth is Admitted to the PON after Available Rate has reached 0 (zero), the "Admitted % Max" will exceed 100% for the Non-Guaranteed traffic type. In the Upstream direction, the Non-guaranteed traffic peak rate will be reduced by the percentage of the subscribed traffic above 100%. Example: if "Admitted % Max" is 200% for Non-Guaranteed traffic, the peak rate of the Non-guaranteed traffic will all be reduced by 50%.

Note: Aggregate values are calculated based on services provisioned on each GPON port.

Per Forwarding Class

- Expedited Forwarding (CIR) traffic is given scheduling priority on the PON and is limited to ~600 Mbps.
- The sum of Expedited Forwarding and Assured Forwarding (CIR) classes is limited to 1200 Mbps. For these classes, the "Admitted % Max" will never exceed 100%.
- Available Rate will fall to 0 (zero) when Admitted Rate = Maximum Rate for each traffic class. At this point, "Admitted % Max" equals 100%.

- Upstream, if additional Best Effort or Assured Forwarding (PIR-CIR) bandwidth is Admitted to the PON after Available Rate has reached 0 (zero), the "Admitted % Max" will exceed 100% for these traffic types. The peak rate for all services in these classes will be reduced by the percentage of the subscribed traffic above 100%. Example: if "Admitted % Max" is 200% for Best Effort and Assured Forwarding (PIR-CIR) traffic classes, the peak rate of each service in these classes is scheduled at a rate equal to 50% of the provisioned PIR for the service.
- Downstream, each traffic class can burst to the full capacity of 2400 Mbps in the absence of other traffic.

Per PON Class of Service

- Each CoS can be provisioned to be Expedited Forwarding, Assured Forwarding, or Best Effort traffic class. Only PON CoS rows applicable to the provisioned traffic classes will be displayed.
- Expedited Forwarding (CIR) traffic is given scheduling priority on the PON and is limited to ~600 Mbps.
- The sum of all CIR classes is limited to the PON capacity. For these classes, the "Admitted % Max" will never exceed 100%.
- Available Rate will fall to 0 (zero) when Admitted Rate = Maximum Rate for each traffic class. At this point, "Admitted % Max" equals 100%.
- Upstream, if additional Best Effort or Assured Forwarding (PIR-CIR) bandwidth is admitted to the PON after Available Rate has reached 0 (zero), the "Admitted % Max" will exceed 100% for these traffic classes. The peak rate for all services in these classes will be reduced by the percentage of the subscribed traffic above 100%. Example: if "Admitted % Max" is 200% for CoS 4, CoS 3 (PIR-CIR), and CoS 2 (PIR-CIR) traffic classes, the peak rate of each service in these classes is scheduled at a rate equal to 50% of the provisioned PIR for the service.
- Downstream, each traffic class can burst to the full capacity of 2400 Mbps in the absence of other traffic.

Bandwidth metrics reported in each view

Maximum Rate	Bandwidth available to the traffic type after higher priority traffic has been admitted. Example: if 300Mbps of Guaranteed bandwidth has been Admitted on the PON, then the Maximum Rate for Non-Guaranteed (Best Effort) traffic is 1200 – 300 = 900 Mbps.
Admitted Rate	Bandwidth that has been provisioned and enabled on an ONT that is linked on the PON.
Available Rate	For each traffic type, Maximum less Admitted bandwidth. If Admitted exceeds Maximum, then Available is 0 (zero).
Admitted % PON	Percent of the PON bandwidth that Admitted represents (Admitted / PON Capacity).
Admitted % MAX	Percent of the Maximum that the Admitted represents (Admitted / Maximum Rate for the traffic type).

To view PON bandwidth reports

1. On the Navigation Tree, double-click an E7 GPON-4 line card, and then click a **GPON** port.
2. In the Work Area, click **Admitted BW Report**, and then select the view of PON bandwidth.
   - **Aggregate**
   - **Per Forwarding Class**
   - **Per Class of Service**

For CLI:

- `show gpon-port [vlans|detail|bandwidth]`
- `show gpon-port <port> [vlans|detail|bandwidth]`

Viewing and Deleting DHCP Leases

This topic shows you how to view or delete E7 system DHCP leases.

To view the E7 DHCP leases

1. On the Navigation Tree, click **E7**.
2. Click **DHCP** > **Leases** to view the E7 leases.

For CLI:

```
show dhcp leases [detail|dsl-bond-interface|gpon-port|interface|ip|mac|ont-port|vlan]
```

To delete a DHCP lease

1. On the Navigation Tree, click **E7**.
2. Click **DHCP** > **Leases** to view the E7 leases.
3. In the list of DHCP leases, click to select the lease you want to delete.
4. In the menu, click **Delete**, and then **Delete** to confirm.

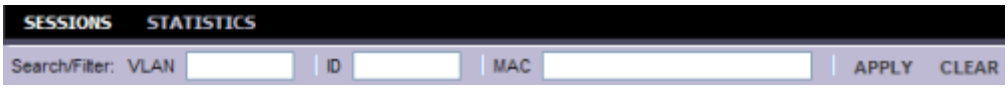
For CLI:

```
delete dhcp lease [detail|dsl-bond-interface|gpon-port|interface|ip|mac|ont-port|vlan]
```

Viewing and Deleting PPPoE Sessions

This topic shows you how to view or delete PPPoE sessions on xDSL ports, xDSL-bonded groups, or ONT Ethernet ports. You can view the PPPoE session specified by using the following filters:

- Specific session ID
- Client MAC address
- VLAN ID



To view the E7 PPPoE sessions

1. On the Navigation Tree, click the xDSL port, xDSL bonded group, or ONT Ethernet port of interest.
2. In the Work Area, click **PPPoE** > **Sessions** to view the PPPoE session on the port or bonded group.
   - Alternatively, you can view the PPPoE session using the filters available in the toolbar.
3. Click **Apply**.

For CLI:

```
show pppoe sessions [detail]
show pppoe sessions id <ses-id> [detail]
show pppoe sessions mac <m-add> [detail|id]
show pppoe sessions ont-port <ont-id/ont-port> [detail|vlan <vlan-
id>]
show pppoe sessions interface <intfc-name> [detail|vlan <vlan-id>]
show pppoe sessions dsl-bond-interface <intfc-name> [detail|vlan
<vlan-i>]
```

To delete a PPPoE session

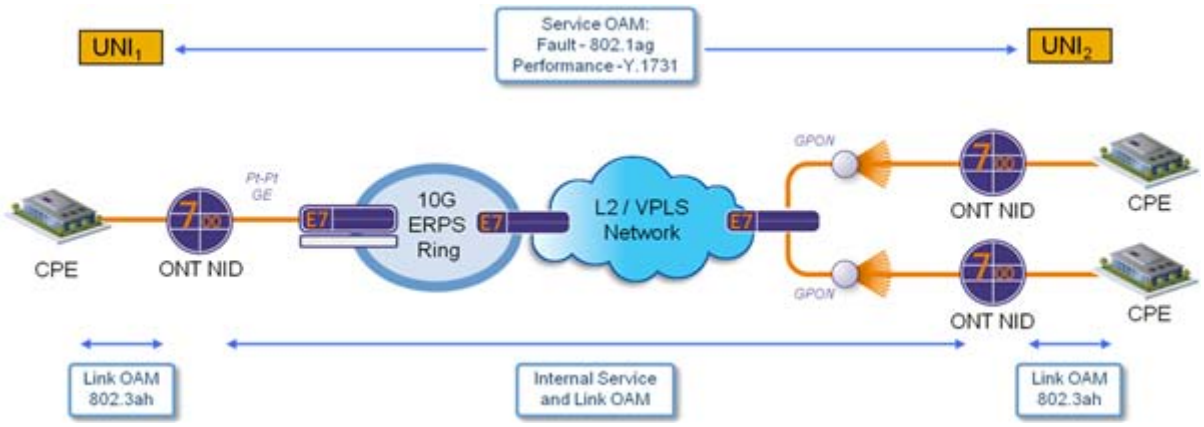
1. On the Navigation Tree, click the ONT Ethernet port of interest.
2. In the Workarea, click **PPPoE** > **Sessions**.
3. Click on the table row that indicates a PPPoE session to select it.
4. In the toolbar, click **Delete**.

For CLI:

```
delete pppoe sessions interface <intfc-name> id <ses-id>
delete pppoe sessions dsl-bond-interface <intfc-name> id <ses-id>
delete pppoe sessions ont-port <ont-id/ont-port>
```

Configuring Ethernet OAM

Operation, Administration and Maintenance (OAM) defines a set of functions designed to monitor network operation, detect and localize network faults, and provide a measure of Network performance. The E7 system supports Ethernet OAM within the Calix 760 ONT series. The ONTs follow the Y.1732, 802.1ag, and MEF 17 standards. The following diagram shows an E7 and point-to-point Ethernet fiber access network supporting Ethernet OAM on the 760GX family of ONTs.



Configuring the E7 Ethernet OAM functionality and initiating various actions and data retrievals from the Ethernet network consists of the following process:

1. Create a Maintenance Entity Group (MEG) and assign a name, VLAN, and MEG level (0-7) that represents where it logically resides within the network.
   - If the MEG auto-discovery parameter is disabled, Remote Maintenance Endpoints should be defined to avoid alarms caused by detecting unknown MEPs.
2. Specify the ONT port or IP host for each reference point to allow continuous monitoring of the paths between the reference points and facilitate fault localization and diagnosis:
   - The ONT ports or IP hosts at the edge of each MEG will be Maintenance Endpoints (MEPs).
   - The ONT ports or IP hosts within each MEG will be Maintenance Intermediate Points (MIPs).
3. The continuity checks begin immediately after the MEP is created, if the Continuity Check parameter is enabled.
4. Initiate a link trace from any MEP to determine what MIPs and MEPs are passed through to get to a specified location.
5. Initiate one of two types of loopbacks:
   - To test the Ethernet OAM protocol, use the Ethernet OAM loopback.
   - To test actual service, use the service loopback.

After performing the procedures in this section, see *Viewing OAM Link Trace and Loopback Test Results* (on page 50).

Configuring an Ethernet OAM Functionality

This topic describes how to configure the system Ethernet OAM object that controls the Ethernet OAM functionality over the entire node. Type, Length, and Value (TLVs) are described in the IEEE 802.1ag standard for Connectivity Fault Management (CFM) as a method of encoding variable-length and/or optional information in a PDU. You can configure the TLVs to include additional information in the various CFM PDUs:

- Continuity Check Messages (CCM) with RDI-remote defect indication
- Link Trace Message (LTM) (MAC trace-route)
- Loopback Message (LBM) (MAC ping)

Not every TLV is applicable for all types of CFM PDUs.

Ethernet OAM domain parameters

You can provision the following parameters for an Ethernet OAM domain:

Parameter	Description	Valid Options
Admin	Enables or disables the Ethernet OAM domain object.	enabled ‡, disabled
Sender ID	Specifies what, if anything, is to be included in the Sender ID TLV transmitted by configured Maintenance Points. All MEGs within the system will use the same sender ID definition. **none** - (default): The Sender ID TLV is not to be sent. **chassis** - The Chassis ID Length, Chassis ID Subtype, and Chassis ID fields of the Sender ID TLV are to be sent, not the Management Address Length or Management Address fields; **management** - The Management Address Length and Management Address of the Sender ID TLV are to be sent, but the Chassis ID Length is to be transmitted with a 0 value,and the Chassis ID Subtype and Chassis ID fields not sent. **both** - The Chassis ID Length, Chassis ID Subtype, Chassis ID, Management Address Length, and Management Address fields are all to be sent.	none ‡, chassis, management, both
Continuity Sender ID	Enables or disables the sending of optional TLVs in the CCM PDU.	enabled, disabled ‡
Continuity Port Status	Enables or disables the sending of optional TLVs in the CCM PDU.	enabled, disabled ‡
Continuity Interface Status	Enables or disables the sending of optional TLVs in the CCM PDU.	enabled, disabled ‡
Loopback Sender ID	Enables or disables the sending of optional TLVs in the LBM PDU.	enabled, disabled ‡
Loopback Data Status	Enables or disables the sending of optional TLVs in the LBM PDU.	enabled, disabled ‡
Link Trace Sender ID	Enables or disables the sending of optional TLVs in the LTM PDU.	enabled, disabled ‡

To configure an Ethernet OAM domain

1. On the Navigation Tree, click **E7**.
2. Click **Ethernet OAM** > **Configuration** from the tabs.
3. In the Ethernet OAM Configuration form, do the following:
   a. In the Admin list, select whether to enable the OAM domain.
   b. In the Sender ID list, select what type of information to use as the Ethernet OAM sender ID.
4. In the CFM TLV Configuration from, select whether to send the optional TLVs for the following:
   - In the Continuity Sender ID checkbox, click to select and send the TLVs in the CCM PDU.
   - In the Continuity Port Status checkbox, click to select and send the TLVs in the CCM PDU.
   - In the Continuity Interface Status checkbox, click to select and send the TLVs in the CCM PDU.
   - In the Loopback Sender ID checkbox, click to select and send the TLVs in the LBM PDU.
   - In the Loopback Data Status checkbox, click to select and send the TLVs in the LBM PDU.
   - In the Link Trace Sender ID checkbox, click to select and send the TLVs in the LTM PDU.

For CLI:

- `set eth-oam-cc`
- `set eth-oam-lb`
- `set eth-oam-lt`
- `set eth-oam-cfg`

Creating a Maintenance Entity Group (MEG)

This topic describes how to create a Maintenance Entity Group (MEG) that consists of Operation, Administration, and Maintenance (OAM) Maintenance Entities (ME), where an ME is an association between two Maintenance End Points (MEP) within an OAM Domain. Each MEP corresponds to a provisioned reference point at the edge of the MEG that requires management.

The MEG defines a logical domain within the Ethernet network. A MEG is associated with a specific VLAN. It is possible to have several MEGs using the same VLAN value.

Ethernet OAM maintenance entity group parameters

You can provision the following parameters for an Ethernet OAM maintenance entity group:

Parameter	Description	Valid Options
Name*	Name of the maintenance entity group. The size of the text string depends on the CCI interworking parameter selected. • 43-character name is allowed if 802.1ag is selected • 13-character name is allowed if Y.1731 is selected	A 43-character text string
VLAN	The VLAN name (or VLAN ID) that the Ethernet OAM PDUs are being carried on coming into the system.	2-4093
Level	MEG Level that distinguishes between OAM frames belonging to different nested MEs. The level represents where a domain logically resides within the network. A larger number has a larger scope within the system. Typically: • The subscriber domain is level 6. • The provider domain is level 4. • The operator domain is level 2. • The link (UNI or NNI) domains are level 0.	0-7
MEG ID Format	MEG ID format specifies whether to interoperate with pure Y.1732 stacks. • A 43-character MEG name is allowed if 802.1ag is selected • A 13-character MEG name is allowed if Y.1731 is selected	8021ag-maid, y1731c
CCM Interval	The interval used when sending a continuity check.	none, 1-sec ‡, 10-sec, 1-min, 10-min
Auto Discovery	Specifies whether the E7 has auto discovery of remote MEPs. • **enabled** - remote MEPs will be detected upon creation or deletion and no alarm occurs. • **disabled** - all remote MEPs planned for the system must be manually provisioned and an alarm occurs with the departure of any provisioned MEP or with the arrival of any undefined MEP.	enabled ‡, disabled
Auto Discovery Timeout	Time to allow continuity check PDUs to go missing before considering a MEP is not transmitting. The value is a decimal (3.5-10.0) that is multiplied with the CCM Interval value.	3.5-10.0 10 ‡
Minimum CC Defect	Minimum continuity check fault required to raise an alarm. • **none** - do not alarm continuity check defects • **rdi** - alarm remote defect indications • **mac** - alarm MAC status defects • **remote** ‡ - alarm remote MEP defects • **error** - alarm receipt of CCM with incorrect time interval • **xcon** - alarm cross-connect defects	none, rdi, mac, remote ‡, error, xcon
Alarm Time	Time that a defect must be present before an alarm occurs (seconds).	0.0-10.0 2.5 ‡
Alarm Reset Period	Time period that a defect must be absent before the associated alarm can be cleared (seconds).	0.0-20.0 10 ‡

*Required field

To create a maintenance entity group (MEG)

1. On the Navigation Tree, click **E7**.
2. Click **Ethernet OAM** > **MEGS** from the tabs.
3. In the menu, click **Create**.
4. In the Create Ethernet OAM MEG dialog box, do the following:
   a. In the Name box, enter a name to assign to the MEG.
   b. In the VLAN box, enter the VLAN name (or VLAN ID) the Ethernet OAM PDUs will be carried on coming into the system.
   c. In the Level box, enter the MEG level.
   d. In the MEG ID Format list, select whether the system interoperates with pure Y.1732 stacks.
   e. In the CCM Interval list, select the interval value for sending a continuity check.
   f. In the Auto Discovery checkbox, leave the box selected to enable the auto discovery of remote MEPs.
   g. In the Auto Discovery Timeout box, enter the decimal value to multiply with the CCM Interval value that indicates the time to allow continuity check PDUs to go missing before considering a MEP is not transmitting.
   h. In the Minimum CC Defect list, select the minimum fault required to raise a continuity check alarm.
   i. In the Alarm Time box, enter the value that indicates the time that a defect must be present before an alarm occurs.
   j. In the Alarm Reset Period box, enter the value that indicates the time that a defect must be absent before the associated alarm can be cleared.
   k. Click **Create**.

For CLI:

- **`create meg <group> vlan <vlan-id> level <m-level>`**
- **`set meg <group>`**

Related topics

- *Adding a Remote Maintenance Entity Point* (on page 45)

Adding a Maintenance End Point (MEP) to a Maintenance Entity Group (MEG)

This topic describes how to identify an ONT port as a Maintenance End Point (MEP) to a specified Maintenance Entity Group (MEG), allowing continuous monitoring of the paths between the end points and facilitating fault localization and diagnosis.

A MEP is a provisioned OAM reference point that can initiate and terminate proactive or diagnostic OAM frames. A MEP defines an edge of an Ethernet OAM domain that could extend beyond the E7 system.

For alarm reporting to occur when MEPs are detected as missing, the initiating MEP must have an accounting of the MEPs from which it is expecting to receive response Continuity Check Messages (CCM). When MEPs are located outside of the E7 system, the initiating MEP can compile a MEP ID list using one of the following methods:

- Reading a remote MEP ID list that you create
- Detecting the MEPs through auto-discovery

Configuration guidelines

- A domain must have at least two MEPs within it, although more are allowed.
- A MEP inherits the VLAN assignment from the associated MEG.
- To change the MEP ID, you must remove it, and then enter the new value for the MEP ID.

Ethernet OAM maintenance end point parameters

You can provision the following parameters for an Ethernet OAM maintenance end point:

Parameter	Description	Valid Options
MEP ID*	Unique index within a MEG to identify the Ethernet OAM maintenance endpoint.	1-8191
MEG*	Name of maintenance entity group (MEG) in which to add the endpoint.	This is a text string.
Port/IP Host*	For ONT Ethernet ports: ONT port indicated by ont-id/ont-port. For ONT Voice ports: IP host indicated for ONT.	For ont-port: f=fast-eth, g=gig-eth, h=hpna-eth, r=video-rf, R=video-hot-rf, t=t1, p=pots. For IP host: SIP, TDM, PWE3, H.248, MGCP. For example, 10001-GE-1, or SIP.
Direction*	MEP direction. • An UP MEP faces into the Relay function of the Bridge and will source and sink OAM frames into or from the switch fabric. Exiting frames, traverse the Bridge Relay function. • A Down MEP faces out of the Switch toward the line or wire side and will source or sink OAM frames to or from the line. Exiting frames, traverse the LAN connection.	up, down
Admin State	Admin state of the port.	enabled ‡, disabled

Parameter	Description	Valid Options
CCM LTM Priority	Priority for which CCM and LTM PDUs are sent by the MEP.	0-7 7 ‡
Continuity Check	Whether the MEP generates continuity check messages (CCMs). Once enabled, a MEP starts sending continuity checks and expects to receive response CCMs from other MEPs in the MEG, resulting in a MEP ID list if the MEG Auto-discovery is enabled.	Y = enabled N = disabled ‡
Frame Measurement Profile	Index of frame-measurement profile to use.	1-20 1 ‡
Delay Loss MAC	If the MEG Auto Discovery parameter is disabled, this indicates the MAC address for delay and loss measurement that the MEP uses to report its PDUs. If the MEG Auto Discovery parameter is enabled,"auto" can be used to indicate that the MAC address is to be auto-discovered.	Six hexadecimal digits in the range 0-FF, optionally separated by colons. Alternatively, "auto" can be used to indicate that the MAC address is to be auto-discovered.
Delay Measurement	Whether the frame delay measurement is performed.	Y = enabled N = disabled ‡
Loss Measurement	Whether the frame loss measurement is performed.	Y = enabled N = disabled ‡

*Required field

To create a maintenance end point (MEP)

1. On the Navigation Tree, click **ONTS**.
2. Click **Provisioning** > **Ethernet OAM** > **MEPS** from the tabs.
3. In the menu, click **Create**.
4. In the Create Ethernet OAM MEP dialog box, do the following:
   a. In the MEP ID box, enter an index value that is unique within the MEG it is to be added.
   b. In the MEG list, select the MEG in which to add the end point.
   c. In the Port/IP Host list, select the ONT Ethernet port or the ONT IP host.
   d. In the Direction list, select the MEP direction.
   e. In the Admin State list, select whether the MEP is active.
   f. In the CCM LTM Priority box, enter the priority value for which the PDUs of continuity check messages and link trace messages are sent by the MEP.
   g. In the Continuity Check list, select whether the MEP generates continuity check messages.
   h. In the Frame Measurement Profile list, select the profile to use for the MEP.
   i. In the Delay Loss MAC box, enter the MAC address for delay and loss measurement that the MEP uses to report its PDUs, or select auto to indicate that the MAC address is to be auto-discovered.

Note: The MEG Auto Discovery parameter must also be enabled for the system to auto discover the end point MAC address.

j. In the Delay Measurement list, select whether the frame delay measurement is performed.

k. In the Loss Measurement list, select whether the frame delay measurement is performed.

l. Click **Create**.

For CLI:

For ONT Ethernet ports:

```
add mep ont-port <port-id> to-meg <name> id <endpoint-id> direction <m-direction>
```

For ONT Voice ports:

```
add mep ont <ont-id> ip-host <sip|tdm-gw|h248|pwe3> to-meg <name> id <endpoint-id> direction <m-direction>
```

- `show mep [detail]`
- `show mep id <endpoint-id> [detail]`
- `show mep ont-port <port-id> [detail]`
- `show mep ont-port <port-id> id <endpoint-id> [detail]`
- `show mep ont <ont-id> ip-host <h-type> [detail]`
- `show mep meg <m-name> [detail]`
- `show mep meg <m-name> id <endpoint-id> [detail]`
- `show mep meg <m-name> ont-port <port-id> [detail]`
- `show mep meg <m-name> ont-port <port-id> id <endpoint-id> [detail]`
- `show mep meg <m-name> ont <ont-id> ip-host <h-type> [detail]`

Related topics

- *Adding a Remote Maintenance Entity Point* (on page 45)
- *Creating a Maintenance Entity Group* (on page 39)

Adding a Maintenance Intermediate Point (MIP) to a Maintenance Entity Group (MEG)

This topic describes how to add a Maintenance domain Intermediate Point (MIP) to a Maintenance Entity Group (MEG). A MIP is a provisioned OAM reference point that is capable of reacting to diagnostic OAM frames initiated by Maintenance Entity Points (MEPs). A MIP does not initiate proactive or diagnostic OAM frames.

Ethernet OAM maintenance intermediate point parameters

You can provision the following parameters for an Ethernet OAM maintenance intermediate point:

Parameter	Description	Valid Options
MIP ID*	Unique index within a MEG to identify the Ethernet OAM maintenance intermediate point.	1-8191
MEG*	Name of maintenance entity group (MEG) in which to add the intermediate point.	Any existing MEG.
Port*	ONT port indicated by ont-id/ont-port. For ONT Ethernet ports only.	Any ONT Ethernet port. For example, 10001-GE-1.
Admin State	Admin state of the port.	enabled ‡, disabled

* Required field
‡ Default

To create a maintenance intermediate point (MIP)

1. On the Navigation Tree, click **ONTS**.
2. Click **Provisioning** > **Ethernet OAM** > **MIPS** from the tabs.
3. In the menu, click **Create**.
4. In the Create Ethernet OAM MIP dialog box, do the following:
   a. In the MIP ID box, enter an index value that is unique within the MEG it is to be added.
   b. In the MEG list, select the MEG in which to add the intermediate point.
   c. In the Port list, select the ONT Ethernet port that is to be designated as the OAM intermediate point.
   d. In the Admin State list, select whether the MEP is active.
   e. Click **Create**.

For CLI:

```
add mip ont-port <port-id> to-meg <name> [admin-state]
```

Adding a Remote Maintenance Entity Point

This topic describes how to add a remote Maintenance End Point (MEP) to a Maintenance Entity Group (MEG) MEP ID list. Adding remote MEPs is only necessary if the following conditions exist:

- The MEG auto-discovery parameter is disabled.
- The MEPs Continuity Checks parameter is enabled.

A MEP defines an edge of an Ethernet OAM domain that could extend beyond the E7 where remote MEPs reside. For alarm reporting to occur when MEPs are detected as missing, the initiating MEP must have an accounting of the MEPs from which it is expecting to receive response Continuity Check Messages (CCM). When MEPs are located outside of the E7 system, the initiating MEP can compile a MEP ID list using one of the following methods:

- Reading a remote MEP ID list that you create
- Detecting the MEPs through auto-discovery

To clear an alarm that indicates a MEP is missing when using the provisioned remote MEP ID list, one of the following must occur:

- The missing MEP ID is deleted from the remote MEP ID list.
- Continuity Check Messages are received from the missing MEP.

Parameters for an Ethernet OAM remote maintenance end point

Parameter	Description	Valid Options
Remote MEP ID*	Unique index within a MEG to identify the Ethernet OAM maintenance intermediate point.	1-8191
MEG*	Name of maintenance entity group (MEG) in which to add the intermediate point.	Any existing MEG.

* Required field

To create a maintenance intermediate point (MIP)

1. On the Navigation Tree, click **ONTS**.
2. Click **Provisioning** > **Ethernet OAM** > **MIPS** from the tabs.
3. In the menu, click **Create**.
4. In the Create Ethernet OAM MIP dialog box, do the following:
   a. In the Remote MEP ID box, enter an index value that is unique within the MEG it is to be added.
   b. In the MEG list, select the MEG in which to add the remote MEP point.
   c. Click **Create**.

For CLI:

- **`add remote-mep id <endpoint-id> to-meg <name>`**
- **`remove remote-mep id <endpoint-id> from-meg <name>`**
- **`show remote-mep`**

Related topics

- *Creating a Maintenance Entity Group* (on page 39)

Creating Frame-Measurement Profiles

This topic describes how to create a frame-measurement profile, allowing you to specify reporting thresholds for certain monitored attributes of Ethernet OAM frame measurements.

Typically, all Maintenance End Points (MEPs) will use the same parameters for measuring the frame delay or frame loss. These parameters are included in the frame-measurement profile that is associated to a MEP. There is a system default profile (1) that can be modified, but not deleted. You can add new profiles at any time.

The frame delay measurements should only be performed for a MEG with only one other MEP. If continuity checks are enabled, the system determines the MAC address of the other end point. If continuity checks are not enabled, the MAC address must be provided for the point you want to measure the frame delay or frame loss.

- **Frame Loss Ratio** - A ratio of the number of service frames not delivered divided by the total number of service frames during time interval T, where the number of service frames not delivered is the difference between the following, expressed as a percentage:
  - Number of service frames arriving at the ingress Ethernet flow point
  - Number of service frames delivered at the egress Ethernet flow point in a point-to-point Ethernet connection
- **Frame Delay** - A round-trip delay for a frame, defined as the time elapsed between the following:
  - Start of transmission of the first bit of the frame by a source node
  - Reception of the last bit of the loop backed frame by the same source node
- **Frame Delay Variation** - A measure of the variations in the frame delay between a pair of service frames, where the service frames belong to the same CoS instance on a point-to-point Ethernet connection.
- **Throughput** - The maximum rate at which no frame is dropped. This is typically measured under test conditions.

Ethernet OAM frame-measurement profile parameters

You can provision the following parameters for an Ethernet OAM frame-measurement profile:

Parameter	Description	Valid Options
Name*	A descriptive name for the profile.	text string
Delay Sampling Rate	Frame delay measurement sampling rate.	1sec‡, 10sec

Parameter	Description	Valid Options
Loss Sampling Rate	Frame loss measurement sampling rate.	1sec‡, 10sec
Loss Measurement Type	Frame loss measurement type.	single-ended‡, dual-ended
NE Loss Ratio Threshold (Max)	Alarm threshold for maximum near-end loss ratio.	0.0000-100.0000 0.1 ‡
NE Loss Ratio Threshold (Clear Max)	Alarm-clearing threshold for the maximum near-end loss ratio.	0.0000-100.0000 0.1 ‡
NE Loss Ratio Threshold (Avg)	Alarm threshold for the average near-end loss ratio. This is a numeric value.	0.0000-100.0000 0.01 ‡
NE Loss Ratio Threshold (Clear Avg)	Alarm-clearing threshold for the average near-end loss ratio.	0.0000-100.0000 0.01 ‡
FE Loss Ratio Threshold (Max)	Alarm threshold for the maximum far-end loss ratio.	0.0000-100.0000 0.1 ‡
FE Loss Ratio Threshold (Clear Max)	Alarm-clearing threshold for the maximum far-end loss ratio. This is a numeric value.	0.0000-100.0000 0.1 ‡
FE Loss Ratio Threshold (Avg)	Alarm threshold for average far-end loss ratio.	0.0000-100.0000 0.01 ‡
FE Loss Ratio Threshold (Clear Avg)	Alarm-clearing threshold for the average far-end loss ratio.	0.0000-100.0000 0.01 ‡
Delay Threshold (Max)	Alarm threshold for the maximum round-trip delay (microseconds).	0-100000 5000 ‡
Delay Threshold (Clear Max)	Alarm-clearing threshold for the maximum delay (microseconds). This is a numeric value.	0-100000 5000 ‡
Delay threshold (Avg)	Alarm threshold for average round-trip delay (microseconds).	0-100000 3000 ‡
Delay threshold (Clear Avg)	Alarm-clearing threshold for average round-trip delay (microseconds).	0-100000 3000 ‡
Delay Variation Threshold (Max)	Alarm threshold for maximum round-trip delay variation (microseconds).	0-100000 2000 ‡
Delay Variation Threshold (Clear Max)	Alarm-clearing threshold for the maximum near-end delay (variation (microseconds).	0-100000 2000 ‡
Delay Variation Threshold (Avg)	Alarm threshold for average round-trip delay variation (microseconds).	0-100000 1000 ‡
Delay Variation Threshold (Clear Avg)	Alarm-clearing threshold for the average round-trip delay variation (microseconds).	0-100000 1000 ‡

*Required field

To create a frame-measure profile

1. On the Navigation Tree, click **E7**.
2. Click **Ethernet OAM** > **Frame Measurement Profiles** from the tabs.
3. In the menu, click **Create**.

4. In the Create Frame Measurement Profile dialog box, do the following:
   a. In the ID list, select a value to assign to the profile you are creating.
   b. In the Delay Sampling Rate list, select the frame delay measurement sampling rate.
   c. In the Loss Sampling Rate list, select the frame loss measurement sampling rate.
   d. In the Loss Measurement Type list, select frame loss measurement type.
   e. In the NE Loss Ratio Threshold boxes, enter values that specify the following values before reporting a threshold-crossing alert:
      - Alarm and alarm-clearing thresholds for the maximum near-end loss ratio.
      - Alarm and alarm-clearing thresholds for the average near-end loss ratio.
   f. In the FE Loss Ratio Threshold boxes, enter values that specify the following values before reporting a threshold-crossing alert:
      - Alarm and alarm-clearing thresholds for the maximum far-end loss ratio.
      - Alarm and alarm-clearing thresholds for the average far-end loss ratio.
   g. In the Delay Threshold boxes, enter values that specify the following values before reporting a threshold-crossing alert:
      - Alarm and alarm-clearing thresholds for the maximum round-trip delay.
      - Alarm and alarm-clearing thresholds for the average round-trip delay.
   h. In the Delay Variation Threshold boxes, enter values that specify the following values before reporting a threshold-crossing alert:
      - Alarm and alarm-clearing thresholds for the maximum delay variation.
      - Alarm and alarm-clearing thresholds for the average delay variation.
5. Click **Create**.

For CLI:

- **`create frame-measure-profile <id>`**
- **`set frame-measure-profile <id>`**

Viewing OAM Link Trace and Loopback Results

Operation, Administration and Maintenance (OAM) defines a set of functions designed to monitor network operation, detect and localize network faults, and provide a measure of Network performance. When the various Ethernet OAM objects are provisioned, the following actions are then possible to initiate. Some are continuous once initiated while others have a limited time before completing.

- Continuity Checks
- Link Trace
- Loopback
- Performance monitoring

Note: Ethernet OAM for the E7 system is only available with the Calix 760GX ONT series.

Continuity Checks

Continuity Check Messages (CCMs) are PDUs sent between MEPs to confirm they can communicate. When a Maintenance End Point (MEP) is provisioned with the Continuity Check parameter enabled, it starts sending Continuity Checks Messages (CCMs) and expects to receive response CCMs from other MEPs in the OAM domain, resulting in a MEP ID list, if the MEG Auto-discovery is enabled. The initiating MEP must have an accounting of the MEPs from which it is expecting to receive response CCMs. When MEPs are located outside of the E7 system, the source MEP can compile a remote MEP ID list using one of the following methods:

- Reading a remote MEP ID list that you create
- Detecting the MEPs through auto-discovery

Link Trace

Link trace is a user-initiated action that identifies the hops between the initiating MEP and a specified reference point within the same domain.

Loopback

Loopback is a user-initiated action that could last a short period of time or remain in effect until terminated. The following types of loopbacks are available from the E7 with the Calix 760 ONT series.

- Multicast Loopback
- Unicast Loopback
- RFC 2544 Loopback

Related topics

- *Configuring Ethernet OAM* (on page 37)
- *Viewing Frame Loss and Delay Statistics* (on page 99)
- *Configuring Ethernet OAM* (on page 37)

Initiating an Ethernet OAM Link Trace and Viewing the Results

This topic describes how to initiate an Ethernet OAM link trace test and view the test results. During the test, the link trace frames are used to identify the path hops between an initiating MEP and a MIP, or an initiating MEP and a peer MEP, and provide fault isolation.

Running a link trace test consists of the following:

- Specify the MEPs where the link trace starts and ends.
- Define a period of time in which the system sends the request and receives responses.
- Retrieve the link trace results that show the individual hops in order from originating MEP to the destination point.

To initiate an OAM link trace test and view the results

1. On the Navigation Tree, click **ONTS**.
2. In the Work Area, click **Ethernet OAM** > **MEPS** in the tabs.
3. In the table of MEG/MEPs provisioned, double-click the MEG/MEP from which you want to initiate a link trace test.
4. In the menu, click **Action** > **Link Trace**.
5. In the Test Link Trace dialog box, do the following:
   a. For the radio buttons, select whether the destination MEP or MIP will be indicated by a MEP ID or a MAC address.
      - If you selected **To MEP**, enter the MEP ID for the destination MEP.
      - If you selected **To MAC**, enter the MAC address for the destination MEP or MIP.
   b. In the Max Hops box, enter the maximum number of hops allowed during the link trace test before aborting the test, preventing the occurrence of a loop.
   c. Click **Run Trace**.
6. In the tabs, click **Link Trace History** to view the link test results.

Note: You can retrieve the results while the link trace test is in process. Look for the status at the end of the individual hops.

For CLI:

- `test link-trace meg <name> ont-port <port-id> to-remote-mep <r-mep-id> [max-hops <hops>]`
  `test link-trace meg <name>`
- `ont-port <port-id> to-mac-address <mac> [max-hops <hops>]`
- `test link-trace meg <name> ont <ont-id> ip-host <type> to-remote-mep <r-mep-id> [max-hops <hops>]`
- `test link-trace meg <name> ont <ont-id> ip-host <type> to-mac-address <mac> [max-hops <hops>]`
- `test link-trace meg <name> mep id <endpoint-id> to-remote-mep <r-mep-id> [max-hops <hops>]`
- `test link-trace meg <name> mep id <endpoint-id> to-mac-address <mac> [max-hops <hops>]`

Note: If no transaction ID is specified, the last link trace is retrieved.

Initiating an OAM Multicast Loopback Test and Viewing the Results

This topic describes how to initiate an Ethernet OAM multicast loopback test that sends packets through the OAM domain and view the test results.

Running a multicast loopback test consists of the following:

- Specifying an initiating MEP, only.
- The initiating MEP sends the request and receives responses from all MEPs, MIPs do not respond.
- The results of the loopback test show the current remote MEP ID list.

To initiate an OAM multicast loopback test and view the results

1. On the Navigation Tree, click **ONTS**.
2. In the Work Area, click **Ethernet OAM** > **MEPS** in the tabs.
3. In the table of MEG/MEPs provisioned, double-click the MEG/MEP from which you want to initiate a link trace test.
4. In the menu, click **Action** > **Multicast Loopback**.
5. In the Test Multicast Loopback dialog box, do the following:
   a. In the Priority list, select the value for the priority of frames with Unicast ETH-LB information.
   b. In the Drop Eligible list, select whether to enable the discard eligibility.
   c. Click **OAM Loopback**.

6. In the tabs, click **OAM Loopback Results** to view the loopback test results.

For CLI:

```
test mcast-loopback meg <m-name> ont-port <port-id> [priority|drop-
eligibility]

test mcast-loopback meg <m-name> ont <ont-id> ip-host <h-name>
[priority|drop-eligibility]

test mcast-loopback meg <m-name> mep id <endpoint-id> [priority|drop-
eligibility]
```

Initiating an Ethernet OAM Unicast Loopback and Viewing the Results

This topic describes how to initiate an Ethernet OAM unicast loopback test that sends packets through the OAM domain and view the test results.

Running a unicast loopback test consists of the following:

- Specifying an initiating MEP, a destination end point, and the number of PDUs sent.
- The initiating MEP sends the request and receives responses.
- The results of the loopback test are available for viewing.

Ethernet OAM unicast loopback test parameters

You can provision the following parameters for an Ethernet OAM unicast loopback test:

Parameter	Description	Valid Options
MEP ID*	Unique index within a MEG to identify the Ethernet OAM maintenance END point. **Note:** Either the MEP ID or the MAC address is required.	1-8191
MAC Address	MAC address of destination endpoint. **Note:** Either the MEP ID or the MAC address is required.	six hexadecimal digits in the range 0-FF, optionally separated by colons
PDU Count	Number of PDUs to send from initiating MEP.	1-1024
Priority	Priority for loopback. This is an integer.	0-7 Alternatively, "use-mep" indicates that the priority in the local MEP should be used.
Drop Eligible	Drop eligibility for PDUs.	enabled, disabled
Data Pattern	Pattern to use in loopback data.	text string
Data Length	Length of loopback data.	0-1400

* Required field

To initiate an OAM unicast loopback test and view the results

1. On the Navigation Tree, click **ONTS**.
2. In the Work Area, click **Ethernet OAM** > **MEPS** in the tabs.
3. In the table of MEG/MEPs provisioned, double-click the MEG/MEP from which you want to initiate a link trace test.
4. In the menu, click **Action** > **Unicast Loopback**.
5. In the Test Unicast Loopback dialog box, do the following:
   a. For the radio buttons, select whether the destination MEP or MIP will be indicated by a MEP ID or a MAC address.
      - If you selected **To MEP**, enter the MEP ID for the destination MEP.
      - If you selected **To MAC**, enter the MAC address for the destination MEP or MIP.
   b. In the PDU Count box, enter the number of PDUs to send from the initiating MEP.
   c. In the Priority list, select the value for the priority of frames with Unicast ETH-LB information.
   d. In the Drop Eligible list, select whether to enable the discard eligibility.
   e. In the Data Pattern box, enter the pattern to use in the loopback data.
   f. In the Data Length box, enter the length of the loopback data.
   g. Click **OAM Loopback**.
6. In the tabs, click **OAM Loopback Results** to view the loopback test results.

For CLI:

- **`test ucast-loopback meg <name> ont-port <port-id>`**
- **`test ucast-loopback meg <name> ont-port <port-id> to-remote-mep <r-mep-id>`**
- **`test ucast-loopback meg <name> ont-port <port-id> to-mac-address <mac>`**
- **`test ucast-loopback meg <name> mep id <endpoint-id>`**
- **`test ucast-loopback meg <name> mep id <endpoint-id> to-remote-mep <r-mep-id>`**
- **`test ucast-loopback meg <name> mep id <endpoint-id> to-mac-address <mac>`**
- **`show loopback meg <name> ont-port <port-id>`**
- **`show-loopback meg <name> mep id <endpoint-id>`**

Initiating an RFC 2544 Loopback and Viewing the Results

This topic describes how to initiate an RFC 2544 Reflector test that is used to verify a circuit's performance and compliance prior to turning the circuit live. This test does not use the Ethernet OAM loopback packets. Instead, a VLAN associated with an ONT port is identified for being placed into service loopback mode where it returns all received non-OAM packets to the central monitor point by swapping the source/destination MAC addresses.

The E7 ONT is not able to generate traffic to test the loopback. Therefore, an external test head or traffic generator must be provided to perform this loopback test. You must specify a destination address equal to the MAC address of the ONT port on the RFC 2544 tester.

To initiate an OAM RFC 2544 loopback test and view the results

1. On the Navigation Tree, click **ONTS**.
2. In the Work Area, click **Provisioned ONTS**, and then click one of the following:
   - To select an ONT Ethernet port, click **Ports**.
   - To select an ONT IP Host, click **IP Hosts**.
3. In the drop-down list at the top of the work area, select the ONT on which to run the test.
4. In the table, double-click either the ONT Ethernet port or the ONT IP Host on which to run the test.

   Note: The selected ONT must have a provisioned service of which to test.

5. If you selected an ONT Ethernet port in Step 4, perform the following steps:
   a. In the ONT Gigabit Ethernet Port form, do the following:
      a. In the Link OAM Events list, select **Y**.
      b. In the Accept Link OAM Loopback, select **Y**, and then click **Apply** in the menu.
   b. In the menu, click **Action** > **OAM** > **RFC2544** > **Test Loopback**.
   c. In the Run Test dialog Service list, select the service provisioned on the port that you want to test. The VLAN specified when the service was provisioned appears in the VLAN field.
   d. Click **Run Test**.
6. If you selected an IP Host in Step 4, click **Action** > **Test RFC2544 Loopback**. The VLAN referenced in the service tag action is automatically configured for the test.
7. When running the actual RFC 2544 test from the test set, you must set the Destination MAC of the 2544 test to the MAC address of the ONT Ethernet port that is performing the loopback function.

8. In the tabs, click **Ethernet OAM** > **OAM Loopback Results** to view the loopback test results.

Note: Use the CLI command **`show ont-port <ont-id/ont-port> detail`** to find the port MAC address.

For CLI:

- **`test rfc2544-loopback start ont <ont-id> ip-host <sip|tdm-gw|h248|mgcp|pwe3> vlan <vlan-id>`**
- **`test rfc2544-loopback start ont-port <port-id> vlan <vlan-id>`**
- **`test rfc2544-loopback stop ont <ont-id>`**

Examples:

- **`test rfc2544-loopback start ont 10001 ip-host sip vlan 77`**
- **`test rfc2544-loopback start ont-port 10001/g1 vlan 78`**
- **`test rfc2544-loopback stop ont 10001`**

Initiating an 802.3ah Loopback Test and Viewing the Results

This topic describes how to initiate an 802.3ah loopback test that monitors individual Ethernet links, link status, and link faults. Link OAM is also used to create local and remote loopbacks on the link between the Calix 76xGX ONTs and the CPE device.

Link OAM provides loopback test capability between two individual Ethernet links. Using this method, the "Source" device sends out a request to the "Destination" device to verify link integrity between the two components. The Destination responds and switches to loopback mode awaiting packet delivery. Once the loopback traffic is sent, the Destination sends the packet back to the Source where it is verified and discarded.

The E7 ONT is not able to generate traffic to test the loopback. Therefore, an external test test head or traffic generator must be provided to perform this loopback test. The 2544 test frames must specify a destination address that is the MAC address of the ONT GE port.

To initiate an OAM 802.3ah loopback test and view the results

1. On the Navigation Tree, click **ONTS**.
2. In the Work Area, click **Provisioned ONTS** > **Ports**.
3. In the drop-down list at the top of the work area, select the ONT on which to run the test.
4. In the table, double-click the ONT Ethernet port on which to run the test.

Note: The selected ONT must have an enabled provisioned service of which to test.

5. In the ONT Gigabit Ethernet Port form, do the following:
   a. In the Link OAM Events list, select **Y**.
   b. In the Accept Link OAM Loopback, select **Y**, and then click **Apply** in the menu.
6. In the menu, click **Action** > **OAM** > **802.3ah > Test Loopback**.
7. In the tabs, click Provisioned **Provisioned ONTS** > **Ports** to view the Link OAM Loopback shown in the Dynamic Status information for the port.

Note: Use the CLI command **`show ont-port <ont-id/ont-port> detail`** to find the port MAC address.

For CLI:

```
set ont-port <ont-id/ont-port> 802.3ah-events enabled 802.3ah-lb-accept
enabled

test 802.3ah-loopback <start|stop> ont-port <port-id>
```

Monitoring E7 Performance Data

This section describes the types of data that are available to determine the E7 performance. The E7 collects statistics and performance monitoring data for the GE and 10GE ports, the PONs well as ONTs.

Performance monitoring data

Each E7 node automatically captures and stores accumulated performance monitoring (PM) data at the ERPS and Ethernet port levels in two time periods:

- In 15-minute periods over 1 day (97 bins)
- In 1-day periods over 7 days (8 bins)

You can also take the following actions:

- Set all PM registers to zero.
- Set all current PM registers (those currently accumulating data) to zero.

Clearing PM registers can be helpful after making repairs or correcting an error condition because you eliminate PM register counts prior to the repair or corrective action.

Statistics

The data captured and stored as statistics accumulate until cleared. If the statistics are never cleared, they reflect all activity since system startup. Each time you invoke the statistics screen, the values are retrieved from the hardware, thereby providing an up-to-date snapshot of system activity. This is in contrast to the performance monitoring data that is sampled every few seconds.

Configuring the Grade-of-Service Profiles

The E7 allows you to set up Grade-of-Service (GOS) profiles that specify reporting thresholds for certain monitored attributes. For example, any time a particular count exceeds a specified threshold within a certain period (either a 15-minute or one-day period), a threshold-crossing alert is generated.

Creating an Ethernet Port GOS Profile

This topic describes how to create an Ethernet port grade-of-service (GoS) profile, allowing you to specify reporting thresholds for certain monitored attributes of an Ethernet port. For example, any time a particular count exceeds a specified threshold within a certain period (either 15 minutes or one day), a threshold-crossing alert is generated.

Global profiles in CMS

Global profiles automate synchronizing profiles across multiple E7 nodes. They support cross-network capabilities such as bulk provisioning. You create a profile once within CMS and apply it across all targeted E7 nodes 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.

1. On the Navigation Tree, click **CMS**.
2. In the Work Area, click **Profile** > **ONT**, and then select the profile to create.

Ethernet port grade of service parameters

You can provision the following parameters for Ethernet port grades of service:

Parameter	Description	Valid Options
ID*	A numeric index value uniquely identifying the Ethernet GoS profile. Index values start with 1.	2-10
Discarded Frames (15 Min) (1 Day)	Number of discarded frames in a 15-minute or 1-day period.	15-Min: 0-1000000000 1-day: 0-1000000000000
Errored Frames (15 Min) (1 Day)	Number of errored frames in a 15-minute or 1-day period.	15-Min: 0-1000000000 1-day: 0-1000000000000

*Required field

To create an Ethernet port grade of service profile

1. On the Navigation Tree, click **E7**.
2. Click **Profiles** > **GOS** > **Ethernet Port** from the tabs.
3. In the Create Ethernet Port Grade of Service dialog box, do the following:
   a. In the ID list, select a value to assign to the GOS profile you are creating.
   b. In the Discarded Frames boxes, enter values that specify how many frames can be discarded in a 15-minute and 1-day period before reporting a threshold-crossing alert.
   c. In the Errored Frames boxes, enter values that specify how many frames can be discarded in a 15-minute and 1-day period before reporting a threshold-crossing alert.
4. Click **Create**.
5. Associate the Ethernet port GoS profile to a specific Ethernet port. See Configuring an Ethernet Port.

For CLI:

```
create eth-gos <gos index> [disc-frames-15-min|disc-frames-1-day|err-frames-15-min|err-frames-1-day]
```

Creating an ONT Ethernet Port GOS Profile

This topic describes how to create an ONT Ethernet port grade-of-service (GoS) profile, allowing you to specify reporting thresholds for certain monitored attributes of an Ethernet port. For example, any time a particular count exceeds a specified threshold within a certain period (15 minutes and one day), a threshold-crossing alert is generated.

ONT Ethernet port grade of service parameters

You can provision the following parameters for Ethernet port GoS:

Parameter	Description	Valid Options
ID*	A numeric index value uniquely identifying the Ethernet GoS profile. Index values start with 1.	2–10
FCS Error (15 min) (1 day)	Number of frames to allow that failed FCS, but had an integral # of octets in a 15-minute or 1-day period.	15-Min: 0–1000000000 Default = 25 1-day: 0–1000000000000 Default = 22500
Excess Collision (15 min) (1 day)	Number of transmission failures due to excess collisions in a 15-minute or 1-day period.	15-Min: 0–1000000000 Default = 25 1-day: 0–1000000000000 Default = 22500
Late Collision (15 min) (1 day)	Number of times to allow collision detected late in the process of frame transmission in a 15-minute or 1-day period.	15-Min: 0–1000000000 Default = 25 1-day: 0–1000000000000 Default = 22500
Long Frame (15 min) (1 day)	Number of frames that are too-long in a 15-minute or 1-day period.	15-Min: 0–1000000000 Default = 25 1-day: 0–1000000000000 Default = 22500
Rx Buffer Overflow (15 min) (1 day)	Number of receiver buffer overflows to allow in a 15-minute or 1-day period.	15-Min: 0–1000000000 Default = 25 1-day: 0–1000000000000 Default = 22500
Tx Buffer Overflow (15 min) (1 day)	Number of transmission buffer overflows in a 15-minute or 1-day period.	15-Min: 0–1000000000 Default = 25 1-day: 0–1000000000000 Default = 22500
Single Collision (15 Min) (1 day)	Number of successful transmissions that had one collision in a 15-minute or 1-day period.	15-Min: 0–1000000000 Default = 25 1-day: 0–1000000000000 Default = 22500
Signal Quality Error (15 min) (1 day)	Number of SQE TEST ERROR messages generated by PLS sublayer in a 15-minute or 1-day period.	15-Min: 0–1000000000 Default = 25 1-day: 0–1000000000000 Default = 22500
Defer Tx (15 min) (1 day)	Number of transmissions deferred because medium was busy in a 15-minute or 1-day period.	15-Min: 0–1000000000 Default = 25 1-day: 0–1000000000000 Default = 22500
Carrier Sense Error (15 min) (1 day)	Number of transmission attempts in which carrier sense was lost or not asserted in a 15-minute or 1-day period.	15-Min: 0–1000000000 Default = 25 1-day: 0–1000000000000 Default = 22500

Parameter	Description	Valid Options
MAC Tx Error (15 min) (1 day)	Number of frames not transmitted due to internal MAC sublayer error in a 15-minute or 1-day period.	15-Min: 0–1000000000 Default = 25 1-day: 0–1000000000000 Default = 22500
Multi Collision (15 min) (1 day)	Number of successful transmissions that had multiple collisions in a 15-minute or 1-day period.	15-Min: 0–1000000000 Default = 25 1-day: 0–1000000000000 Default = 22500
Align Error (15 min) (1 day)	Number of frames that failed FCS and did not have an integral number of octets in a 15-minute or 1-day period.	15-Min: 0–1000000000 Default = 25 1-day: 0–1000000000000 Default = 22500
MAC Rx Error (15 min) (1 day)	Number of frames not received due to internal MAC sublayer error in a 15-minute or 1-day period.	15-Min: 0–1000000000 Default = 25 1-day: 0–1000000000000 Default = 22500

*Required field

To create an GoS profile for ONT Ethernet ports

1. On the Navigation Tree, click **E7**.
2. Click **Profiles** > **GOS** > **ONT Ethernet Port** from the tabs.
3. In the menu, click **Create**.
4. In the Create Ethernet GoS Profile dialog box, do the following:
   a. In the ID list, select a value to idenitify the GoS profile that you are creating.
   b. In the FCS Error boxes, enter values that specify how many missing packets to allow in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.
   c. In the Excess Collision boxes, enter values that specify how many excess collisions to allow in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.
   d. In the Late Collision boxes, enter values that specify how many times to allow a collision to be detected late in the process in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.
   e. In the Long Frame boxes, enter values that specify how many frames to allow that are too long in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.
   f. In the RX Buffer Overflow boxes, enter values that specify how many Rx buffer overflows to allow in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.
   g. In the TX Buffer Overflow boxes, enter values that specify how many Tx buffer overflows to allow in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.

h. In the Single Collision boxes, enter values that specify how many successful transmissions that had one collision to allow in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.

i. In the Signal Quality Error boxes, enter values that specify how many times to allow a SQE TEST ERROR message that is generated by PLS sublayer in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.

j. In the Defer Tx boxes, enter values that specify how many times to allow transmissions deferred because medium was busy in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.

k. In the Carrier Sense Error boxes, enter values that specify how many times to allow transmission attempts in which the carrier sense was lost or not asserted in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.

l. In the MAC Tx Error boxes, enter values that specify how many times to allow frames not being transmitted due to the internal MAC sublayer error in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.

m. In the Multi Collision boxes, enter values that specify how many successful transmissions that had multiple collisions to allow in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.

n. In the Align Error boxes, enter values that specify how many frames to allow that failed FCS and did not have an integral number of octets in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.

o. In the MAC RX Error boxes, enter values that specify how many times to allow frames not being received due to internal MAC sublayer error in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.

5. Click **Create**.

Note: Associate an Ethernet port GoS profile to a specific ONT Ethernet port when provisioning a service.

For CLI:

```
create ont-eth-gos <gos index> [fcs-frames*|excess-coll*|late-coll*|long-
frame*|rx-overflow*|tx-overflow*|single-coll*|multi-coll*|sqe-
count*|deferred-tx*|mac-tx*|carrier-sense-err*|alignment-err*|mac-rx*]
```

Creating an ONT T1/E1 Port GOS Profile

This topic describes how to create an ONT T1/E1 port grade-of-service (GOS) profile, allowing you to specify reporting thresholds for certain monitored attributes of a T1 port. For example, any time a particular count exceeds a specified threshold within a certain period (either 15 minutes or one day), a threshold-crossing alert is generated.

T1 port grade of service parameters

You can provision the following parameters for T1 port grade of service:

Parameter	Description	Valid Options
ID	A numeric index value uniquely identifying the Ethernet GoS profile. Index values start with 1.	2-10
Error Seconds (15 Min) (1 Day)	Number of error seconds in a 15-minute or 1-day period.	15-Min: 0-1000000000 Default = 65 1-day: 0-1000000000000 Default = 58500
Severely Error Seconds (15 Min) (1 Day)	Number of severely error seconds in a 15-minute or 1-day period.	15-Min: 0-1000000000 Default = 10 1-day: 0-1000000000000 Default = 9000
Bursty Error Seconds (15 Min) (1 Day)	Number of bursty error seconds in a 15-minute or 1-day period.	15-Min: 0-1000000000 Default = 10 1-day: 0-1000000000000 Default = 9000
Unavailable Seconds (15 Min) (1 Day)	Number of unavailable seconds in a 15-minute or 1-day period.	15-Min: 0-1000000000 Default = 10 1-day: 0-1000000000000 Default = 9000
Controlled Slip Seconds (15 Min) (1 Day)	Number of controlled slip seconds in a 15-minute or 1-day period.	15-Min: 0-1000000000 Default = 1 1-day: 0-1000000000000 Default = 900

To create a T1/E1 port grade-of-service profile

1. On the Navigation Tree, click **E7**.
2. Click **Profiles** > **GOS** > **T1/E1 Port** from the tabs.
3. In the menu, click **Create**.
4. In the Create ONT T1 Port GOS dialog box, do the following:
   a. In the ID list, select a value to assign to the GOS profile you are creating.
   b. In the Error Seconds boxes, enter values that specify how many error seconds to allow in a 15-minute and 1-day period before reporting a threshold-crossing alert.
   c. In the Severely Error Seconds boxes, enter values that specify how many severely-error seconds to allow in a 15-minute and 1-day period before reporting a threshold-crossing alert.
   d. In the Bursty Error Seconds boxes, enter values that specify how many bursty error seconds to allow in a 15-minute and 1-day period before reporting a threshold-crossing alert.
   e. In the Unavailable Seconds boxes, enter values that specify how many unavailable seconds to allow in a 15-minute and 1-day period before reporting a threshold-crossing alert.

f. In the Controlled Slip Seconds boxes, enter values that specify how many controlled slip seconds to allow in a 15-minute and 1-day period before reporting a threshold-crossing alert.

5. Click **Create**.

6. Associate the T1 port GoS profile to a specific T1 port.

For CLI:

```
create ont-t1-gos <gos index> [es-*|ses-*|bes-*|uas-*|css-*]
```

Creating a PWE3 Service GOS Profile

This topic describes how to create a PWE3 service grade-of-service (GOS) profile, allowing you to specify reporting thresholds for certain monitored attributes of a PWE3 service. For example, any time a particular count exceeds a specified threshold within a certain period (either 15 minutes or one day), a threshold-crossing alert is generated.

PWE3 service GOS parameters

You can provision the following parameters for a PWE3 service grade of service:

Parameter	Description	Valid Options
ID*	A numeric index value uniquely identifying the Ethernet GoS profile. Index values start with 1.	2-10
Missing Packets (15 Min) (1 Day)	Number of missing packets in a 15-minute or 1-day period.	15-Min: 0-1000000000 Default = 65 1-day: 0-1000000000000 Default = 6240
Misordered Packets Unusable (15 Min) (1 Day)	Number of misordered and unusable packets in a 15-minute or 1-day period.	15-Min: 0-1000000000 Default = 65 1-day: 0-1000000000000 Default = 6240
Misordered Packets Dropped (15 Min) (1 day)	Number of misordered and dropped packets in a 15-minute or 1-day period.	15-Min: 0-1000000000 Default = 65 1-day: 0-1000000000000 Default = 6240
Playout Buffer Faults (15 Min) (1 day)	Number of playout buffer faults in a 15-minute or 1-day period.	15-Min: 0-1000000000 Default = 65 1-day: 0-1000000000000 Default = 6240
Malformed Packets (15 Min) (1 day)	Number of malformed packets in a 15-minute or 1-day period.	15-Min: 0-1000000000 Default = 65 1-day: 0-1000000000000 Default = 6240
Stray Packets (15 Min) (1 day)	Number of stray packets in a 15-minute or 1-day period.	15-Min: 0-1000000000 Default = 65 1-day: 0-1000000000000 Default = 6240
Remote Packet Loss (15 Min) (1 day)	Number of remote packets lost in a 15-minute or 1-day period.	15-Min: 0-1000000000 Default = 65 1-day: 0-1000000000000 Default = 6240

Parameter	Description	Valid Options
TDM Lbit Packets sent (15 Min) (1 day)	Number of TDM Lbit packets in a 15-minute or 1-day period.	15-Min: 0-1000000000 Default = 65 1-day: 0-1000000000000 Default = 6240
Errored Seconds (15 Min) (1 day)	Number of errored seconds in a 15-minute or 1-day period.	15-Min: 0-1000000000 Default = 65 1-day: 0-1000000000000 Default = 6240
Severely Errored Seconds (15 Min) (1 day)	Number of severely errored seconds in a 15-minute or 1-day period.	15-Min: 0-1000000000 Default = 10 1-day: 0-1000000000000 Default = 960
Unavailable Seconds (15 Min) (1 day)	Number of unavailable seconds in a 15-minute or 1-day period.	15-Min: 0-1000000000 Default = 10 1-day: 0-1000000000000 Default = 960

*Required field

To create a PWE3 service grade-of-service profile

1. On the Navigation Tree, click **E7**.
2. Click **Profiles** > **GOS** > **PWE3** from the tabs.
3. In the menu, click **Create**.
4. In the Create PWE3 service GOS dialog box, do the following:
   a. In the ID list, select a value to assign to the GOS profile you are creating.
   b. In the Missing Packets Threshold boxes, enter values that specify how many missing packets to allow in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.
   c. In the Misordered Packets Unusable Threshold boxes, enter values that specify how many misordered and unusable packets to allow in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.
   d. In the Misordered Packets Dropped Threshold boxes, enter values that specify how many misordered and dropped packets to allow in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.
   e. In the Playout Buffer Faults Threshold boxes, enter values that specify how many playout buffer faults to allow in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.
   f. In the Malformed Packets Threshold boxes, enter values that specify how many malformed packets to allow in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.
   g. In the Stray Packets Threshold boxes, enter values that specify how many stray packets to allow in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.

h. In the Remote Packet Loss Threshold boxes, enter values that specify how many remote lost packets to allow in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.

i. In the TDM Lbit Packets Sent Threshold boxes, enter values that specify how many TDM Lbit sent packets to allow in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.

j. In the Errored Seconds Threshold boxes, enter values that specify how many errored seconds to allow in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.

k. In the Severely Errored Seconds Threshold boxes, enter values that specify how many severely errored seconds to allow in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.

l. In the Unavailable Seconds Threshold boxes, enter values that specify how many unavailable seconds to allow in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.

5. Click **Create**.

6. Associate the PWE3 service GoS profile to a PWE3 service being provisioned on an ONT T1 port.

For CLI:

```
create ont-pwe3-svc-gos <gos index> [missing-pkts*|misorder-
usable*|misorder-drop*|buffer-err*|malformed-pkts*|stray-pkts*|rmt-
loss*|tdm-lbit-sent*|es*|ses*|uas*]
```

Creating a DSL Port GoS Profile

This topic describes how to create an xDSL port grade-of-service (GoS) profile, allowing you to specify reporting thresholds for certain monitored attributes of an xDSL port. For example, any time a particular count exceeds a specified threshold within a certain period (15 minutes and one day), a threshold-crossing alert is generated.

GOS profiles are always referenced by a unique index number assigned using this command. A profile can be assigned to a specified DSL port by using the "**`set dsl-port * gos *`**" command.

DSL port grade of service parameters

You can provision the following parameters for xDSL port GoS:

Parameter	Description	Valid Options
ID*	A numeric index value uniquely identifying the Ethernet GoS profile. Index values start with 1.	2–10
Code violations Channel (15 min) (1 day)	Number of code violations (channel) in a 15-minute or 1-day period.	15-Min: 0–1000000000 1-day: 0–1000000000000
Code violations Channel Far End (15 min) (1 day)	Number of code violations (channel far end) in a 15-minute or 1-day period.	15-Min: 0–1000000000 1-day: 0–1000000000000
FEC Errors Channel (15 min) (1 day)	Number of forward error corrections (channel) in a 15-minute or 1-day period.	15-Min: 0–1000000000 1-day: 0–1000000000000
FEC Errors Channel Far End (15 min) (1 day)	Number of forward error corrections (channel far end) in a 15-minute or 1-day period.	15-Min: 0–1000000000 1-day: 0–1000000000000
FEC Errors Line (15 min) (1 day)	Number of forward error corrections (line) in a 15-minute or 1-day period.	15-Min: 0–1000000000 1-day: 0–1000000000000
FEC Errors Line Far End (15 min) (1 day)	Number of forward error corrections (line far end) in a 15-minute or 1-day period.	15-Min: 0–1000000000 1-day: 0–1000000000000
Errored Seconds Line (15 Min) (1 day)	Number of errored seconds (line) in a 15-minute or 1-day period.	15-Min: 0–1000000000 1-day: 0–1000000000000
Errored Seconds Line Far End (15 min) (1 day)	Number of errored seconds (line far end) in a 15-minute or 1-day period.	15-Min: 0–1000000000 1-day: 0–1000000000000
Severely Errored Seconds Line (15 min) (1 day)	Number of severely errored seconds (line) in a 15-minute or 1-day period.	15-Min: 0–1000000000 1-day: 0–1000000000000
Severely Errored Seconds Line Far End (15 min) (1 day)	Number of severely errored seconds (line far end) in a 15-minute or 1-day period.	15-Min: 0–1000000000 1-day: 0–1000000000000
Loss of Signal Seconds (15 min) (1 day)	Number of loss of signal seconds (line) in a 15-minute or 1-day period.	15-Min: 0–1000000000 1-day: 0–1000000000000
Loss of Signal Seconds Far End (15 min) (1 day)	Number of loss of signal seconds (line far end) in a 15-minute or 1-day period.	15-Min: 0–1000000000 1-day: 0–1000000000000
Unavailable Seconds Line (15 min) (1 day)	Number of unavailable seconds (line) in a 15-minute or 1-day period.	15-Min: 0–1000000000 1-day: 0–1000000000000
Unavailable Seconds Line Far End (15 min) (1 day)	Number of unavailable seconds (line far end) in a 15-minute or 1-day period.	15-Min: 0–1000000000 1-day: 0–1000000000000
Full Initialization Line (15 min) (1 day)	Number of full initializations (line) in a 15-minute or 1-day period.	15-Min: 0–1000000000 1-day: 0–1000000000000
Failed Initializations (15 min) (1 day)	Number of failed full initializations (line) in a 15-minute or 1-day period.	15-Min: 0–1000000000 1-day: 0–1000000000000
CRC Errors (15 min) (1 day)	Number of CRC errors in a 15-minute or 1-day period.	15-Min: 0–1000000000 1-day: 0–1000000000000
Coding Violations (15 min) (1 day)	Number of coding violations in a 15-minute or 1-day period.	15-Min: 0–1000000000 1-day: 0–1000000000000

*Required field

To create an GoS profile for ONT Ethernet ports

1. On the Navigation Tree, click **E7**.
2. Click **Profiles** > **GOS** > **DSL Port** from the tabs.
3. In the menu, click **Create**.
4. In the Create Ethernet GoS Profile dialog box, do the following:
   a. In the ID list, select a value to idenitify the GoS profile that you are creating.
   b. In the Code violations Channel boxes, enter values that specify how many code violations to allow in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.
   c. In the Code violations Channel Far End boxes, enter values that specify how many code violations at the far end to allow in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.
   d. In the FEC Errors Channel boxes, enter values that specify how many channel forward error corrections to allow in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.
   e. In the FEC Errors Channel Far End boxes, enter values that specify how many channel forward error corrections to allow on the far end in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.
   f. In the FEC Errors Line boxes, enter values that specify how many line forward error corrections to allow on the line in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.
   g. In the FEC Errors Line Far End boxes, enter values that specify how many line forward error corrections to allow on the far end in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.
   h. In the Errored Seconds Line boxes, enter values that specify how many errored seconds to allow on the line in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.
   i. In the Errored Seconds Line Far End boxes, enter values that specify how many errored seconds to allow on the line at the far end in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.
   j. In the Severely Errored Seconds Line boxes, enter values that specify how many severely errored seconds to allow on the line in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.
   k. In the Severely Errored Seconds Line Far End boxes, enter values that specify how many severely errored seconds to allow on the line at the far end in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.
   l. In the Loss of Signal Seconds Line boxes, enter values that specify how many loss of signal seconds to allow on the line in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.

m. In the Loss of Signal Seconds Line Far End boxes, enter values that specify how many loss of signal seconds to allow on the far end line in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.

n. In the Unavailable Seconds Line boxes, enter values that specify how many unavailable seconds to allow on the line in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.

o. In the Unavailable Seconds Line Far End boxes, enter values that specify how many unavailable seconds to allow on the line at the far end in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.

p. In the Full Initializations boxes, enter values that specify how many times to allow full initializations a 15-minute period and a 1-day period before reporting a threshold-crossing alert.

q. In the Failed Full Initializations boxes, enter values that specify how many times to allow failed full initializations in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.

r. In the CRC Errors boxes, enter values that specify how many CRC errors to allow in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.

s. In the Coding Violations boxes, enter values that specify how many coding violations to allow in a 15-minute period and a 1-day period before reporting a threshold-crossing alert.

5. Click **Create**.

Note: Associate an xDSL port GoS profile to a specific xDSL port associated interface when provisioning a service.

For CLI:

```
create dsl-port-gos <index-id>
```

Viewing Ethernet Port Performance Data

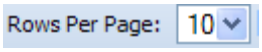
This topic shows you how to view or clear the Ethernet port performance data that the E7 automatically collects and stores. Clearing performance monitoring data can be helpful after making repairs or correcting an error condition.

Ethernet Port Performance Data	
Statistic	**Description**
Number	Specific segment of time in the continuous sequence of captured performance data.
Started At	Time the data capture started for the particular segment number.
Started Sec	Number of seconds in the particular segment of time.
Status	Indicates whether the data capture was completed for the particular segment number.

Received Octets	Number of eight-bit quantities (octets) received on the Ethernet port.
Received Unicast Packets	Number of packets received on the Ethernet port with a Unicast destination MAC address.
Discarded Received Frames	Number of frames discarded upon ingress (received) on the Ethernet port due to exceeding the rate limit policy or size.
Interface Input Errors	Number of frames discarded upon ingress (received) on the Ethernet port due to bad format, alignment, or CRC errors.
Transmitted Octets	Number of eight-bit quantities (octets) sent from the Ethernet port.
Transmitted Unicast Packets	Number of packets sent on the Ethernet port with a unicast destination MAC address.
Received Multicast Packets	Number of packets received on the Ethernet port with a multicast destination MAC address.
Received Broadcast Packets	Number of packets received on the Ethernet port with a broadcast destination MAC address.
Transmitted Multicast Packets	Number of packets sent on the Ethernet port with a multicast destination MAC address.
Transmitted Broadcast Packets	Number of packets sent on the Ethernet port with a broadcast destination MAC address.
In-Octet-TCA	Whether the received octets exceeded the specified threshold during the particular time segment.
In-Ucast-TCA	Whether the received unicast packets exceeded the specified threshold during the particular time segment.
In-Disc-TCA	Whether the frames discarded on ingress exceeded the specified threshold during the particular time segment.
In-Err-TCA	Whether the error frames on ingress exceeded the specified threshold during the particular time segment.
Out-Octet-TCA	Whether the transmitted octets exceeded the specified threshold during the particular time segment.
Out-Ucast-TCA	Whether the number of packets sent from the Ethernet port with a unicast destination MAC address exceeded the specified threshold during the particular time segment.
In-Mcast-TCA	Whether the number of packets received on the Ethernet port with a multicast destination MAC address exceeded the specified threshold during the particular time segment.
In-Bcast-TCA	Whether the number of packets received on the Ethernet port with a broadcast destination MAC address exceeded the specified threshold during the particular time segment.
Out-Mcast-TCA	Whether the number of packets sent on the Ethernet port with a multicast destination MAC address exceeded the specified threshold during the particular time segment.
Out-Bcast-TCA	Whether the number of packets sent on the Ethernet port with a broadcast destination MAC address exceeded the specified threshold during the particular time segment.

To view Ethernet port performance data

1. On the Navigation Tree, click a **GE** or **10GE** Ethernet port.
2. In the Work Area, click **Performance.**
3. Click the tab for the performance data accumulation time period to view:
   - In 15-minute periods over 1 day (97 bins)
   - In 1-day periods over 7 days (8 bins)
4. View the data using the navigation tools:
   - Use the horizontal scroll bar to view all of the performance data categories.
   - Use the Rows Per Page drop-down list to control how many rows to display on one screen page.

   - Use the page browser buttons to view the data on the immediate pages (back and next) and the first and last pages.

For CLI:

```
show pm eth-port <port-id> [1-day all|1-day bin *|1-day current|1-
day last *|15-min all|15-min bin *|15-min current|15-min last *]
```

To clear Ethernet port performance data

1. On the Navigation Tree, click the **GE** or **10GE** Ethernet port.
2. In the Work Area, click **Performance.**
3. Click the tab for the performance data accumulation time period to delete:
   - In 15-minute periods over 1 day (97 bins)
   - In 1-day periods over 7 days (8 bins)
4. Click **Action**, and select one of the following actions:
   - Select **Clear PM Data** to return all PM registers to zero.
   - Select **Clear Current Period PM Data** to return all PM registers currently accumulating data to zero.

For CLI:

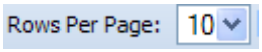
```
clear pm eth-port <port ID> [1-day all|1-day current|15-min all|15-
min current]
```

Viewing DSL Port Performance Data

This topic shows you how to view or clear the DSL port performance data that the E7 automatically collects and stores. Clearing performance monitoring data can be helpful after making repairs or correcting an error condition.

To view DSL port performance data

1. On the Navigation Tree, click an xDSL port.
2. n the Work Area, click **Port** > **Performance.**
3. Choose the set of statistics to view:
   - **Eth** shows the cumulative DSL port Ethernet statistics.
   - **DSL** shows the cumulative DSL port line-level statistics.
4. Click the tab for the performance data accumulation time period to view:
   - **15-Min** for periods over 1 day (97 bins)
   - **1-Day** for periods over 7 days (8 bins)
5. View the data using the navigation tools:
   - Use the horizontal scroll bar to view all of the performance data categories.
   - Use the Rows Per Page drop-down list to control how many rows to display on one screen page.

   - Use the page browser buttons to view the data on the immediate pages (back and next) and the first and last pages.

For CLI:

```
show pm dsl-port <port-id> [1-day all|1-day bin *|1-day current|1-
day last *|15-min all|15-min bin *|15-min current|15-min last *]
```

To clear DSL port performance data

1. On the Navigation Tree, click an xDSL port.
2. n the Work Area, click **Port** > **Performance.**
3. Choose the set of statistics to view:
   - **Eth** shows the cumulative DSL port Ethernet statistics.
   - **DSL** shows the cumulative DSL port line-level statistics.

4. Click the tab for the performance data accumulation time period to view:
   - **15-Min** for periods over 1 day (97 bins)
5. **1-Day** for periods over 7 days (8 bins)
6. Click **Action**, and select one of the following actions:
   - Select **Clear PM Data** to return all PM registers to zero.
   - Select **Clear Current Period PM Data** to return all PM registers currently accumulating data to zero.

For CLI:

```
clear pm dsl-port <port ID> [1-day all|1-day current|15-min all|15-
min current]
```

Viewing DSL Port Statistics

This topic shows you how to view or clear the DSL port statistics that the E7 automatically collects and stores. Clearing statistics can be helpful after making repairs or correcting an error condition.

To view DSL port statistics

1. On the Navigation Tree, click an xDSL port.
2. In the Work Area, click **Port** > **Performance.**
3. Choose the set of statistics to view:
   - **Eth** shows the cumulative DSL port Ethernet statistics.
   - **DSL** shows the cumulative DSL port line-level statistics.
4. Click **Statistics**.
5. Click **Refresh** periodically to see the up-to-date statistics for the E7.

For CLI:

```
show stats dsl-port <port-id>
```

To clear DSL port statistics

1. On the Navigation Tree, click an xDSL port.
2. In the Work Area, click **Performance**.
3. Choose the set of statistics to view:
   - **Eth** shows the cumulative DSL port Ethernet statistics.
   - **DSL** shows the cumulative DSL port line-level statistics.

4. Click **Statistics**.
5. Click **Action** > **Clear Statistics** to clear the cumulative Ethernet port performance statistics.

For CLI:

```
clear stats dsl-port <port-id>
```

Viewing Ethernet Port Statistics

This topic shows you how to view or clear the Ethernet port statistics that the E7 automatically collects and stores. Clearing statistics can be helpful after making repairs or correcting an error condition.

Ethernet Port Statistics	
Statistic	**Description**
Number	Specific segment of time in the continuous sequence of captured performance data.
Started At	Time the data capture started for the particular segment number.
Started Sec	Number of seconds in the particular segment of time.
Status	Indicates whether the data capture was completed for the particular segment number.
Received octets	Number of eight-bit quantities (octets) received on the Ethernet port.
Received unicast packets	Number of packets received on the Ethernet port with a Unicast destination MAC address.
Discarded received frames	Number of frames discarded upon ingress (received) on the Ethernet port due to exceeding the rate limit policy or size.
Interface input errors	Number of frames discarded upon ingress (received) on the Ethernet port due to bad format, alignment, or CRC errors.
Transmitted octets	Number of eight-bit quantities (octets) sent from the Ethernet port.
Transmitted unicast packets	Number of packets sent on the Ethernet port with a unicast destination MAC address.
Received multicast packets	Number of packets received on the Ethernet port with a multicast destination MAC address.
Received broadcast packets	Number of packets received on the Ethernet port with a broadcast destination MAC address.
Transmitted multicast packets	Number of packets sent on the Ethernet port with a multicast destination MAC address.
Transmitted broadcast packets	Number of packets sent on the Ethernet port with a broadcast destination MAC address.
in-octet-tca	Whether the received octets exceeded the specified threshold during the particular time segment.
in-ucast-tca	Whether the received unicast packets exceeded the specified threshold during the particular time segment.
in-disc-tca	Whether the frames discarded on ingress exceeded the specified threshold during the particular time segment.

in-err-tca	Whether the error frames on ingress exceeded the specified threshold during the particular time segment.
out-octet-tca	Whether the transmitted octets exceeded the specified threshold during the particular time segment.
out-ucast-tca	Whether the number of packets sent from the Ethernet port with a unicast destination MAC address exceeded the specified threshold during the particular time segment.
in-mcast-tca	Whether the number of packets received on the Ethernet port with a multicast destination MAC address exceeded the specified threshold during the particular time segment.
in-bcast-tca	Whether the number of packets received on the Ethernet port with a broadcast destination MAC address exceeded the specified threshold during the particular time segment.
out-mcast-tca	Whether the number of packets sent on the Ethernet port with a multicast destination MAC address exceeded the specified threshold during the particular time segment.
out-bcast-tca	Whether the number of packets sent on the Ethernet port with a broadcast destination MAC address exceeded the specified threshold during the particular time segment.

To view Ethernet port statistics

1. On the Navigation Tree, click the **GE** or **10GE** Ethernet port.
2. In the Work Area, click **Performance** > **Statistics**.
3. Click **Refresh** periodically to see the up-to-date statistics for the E7.

For CLI:

```
show stats eth-port <eth-port-id>
```

To clear Ethernet port statistics

1. On the Navigation Tree, click the **GE** or **10GE** Ethernet port.
2. In the Work Area, click **Performance** > **Statistics**.
3. Click **Action** > **Clear Statistics** to clear the cumulative Ethernet port performance statistics.

For CLI:

```
clear stats eth-port <eth-port-id>
```

Viewing ERPS Domain Performance Data

This topic shows you how to view or clear the Ethernet Ring Protection Switching (ERPS) performance data that the E7 automatically collects and stores. Clearing performance monitoring data can be helpful after making repairs or correcting an error condition. For modular chassis systems, this statistics data only applies to shelf 1 in the system.

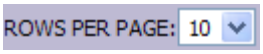
ERPS Domain Performance Data	
Statistic	**Description**
Number	Specific segment of time in the continuous sequence of captured performance data.
Started At	Time the data capture started for the particular segment number.
Started Sec	Number of seconds in the particular segment of time.
Status	Indicates whether the data capture was completed for the particular segment number.
Ring Port Down	Number of times an ERPS ring interface that is directly connected to this E7 (local) is out of service (down).
Ring Port Up	Number of times the ERPS ring service was brought back up from a failed state.
Ring Down	Number of times an ERPS ring interface that is not directly connected (remote) to this E7 is out of service (down).
Ring Up	Number of times an ERPS ring interface that is not directly connected (remote) to this E7 is brought back in service (up) after having been in a failed state (down).
Isolated Node	Number of times both ERPS ring interfaces that are directly connected to the E7 are out of service (down), leaving this node isolated.
Second Master Detected	Number of times that more than one node is designated as the master node in the ERPS ring.
Acting Master	The current node that has assumed the role of the ERPS ring Master because no node was designated as Master.
Health Sequence Error	Number of Ring Health packets lost during the particular time segment.
Bad Packet Received	Number of Bad Packets received on the ERPS ring management VLAN during the particular time segment.

Note: This procedure assumes that an ERPS domain is configured on the E7. See "Creating an ERPS Domain" in the *Calix E7 User Guide*.

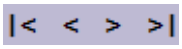
To view ERPS domain performance data or statistics

1. On the Navigation Tree, click **E7**.
2. In the Work Area, click **ERPS.**
3. Double-click the table row that displays the ERPS domain information, click **Performance**, and then select what you want to view.
   - To view the ERPS statistics, click **Statistics**.
   - To view the performance data accumulation over a time period:
     - Click **15 MIN** to view data in 15-minute periods over 1 day (97 bins).
     - Click **1 DAY** to view data in 1-day periods over 7 days (8 bins).

4. View the data using the navigation tools:
   - Use the horizontal scroll bar to view all of the performance data categories.
   - Use the Rows Per Page drop-down list to control how many rows to display on one screen page.

   - Use the page browser buttons to view the data on the immediate pages (back and next) and the first and last pages.

For CLI:

- **`show pm erps-domain <domain name> [1-day all|1-day bin *|1-day current|1-day last *|15-min all|15-min bin *|15-min current|15-min last *]`**
- **`show stats erps-domain <domain name>`**

To clear ERPS performance data and statistics

1. On the Navigation Tree, click **E7**.
2. In the Work Area, click **ERPS.**
3. Double-click the table row that displays the ERPS domain information, and then click **Performance**.
4. Click one of the following sequences:
   - Click **15 MIN** or **1 Day**, and then click **Action**, and select one of the following actions:
     - Select **Clear PM Data** to return all PM registers to zero.
     - Select **Clear Current Period PM Data** to return all PM registers currently accumulating data to zero.
   - Click **Statistics** > **Action** > **Clear Statistics**.

For CLI:

- **`clear pm erps-domain <d-name> [1-day all|1-day current|15-min all|15-min current]`**
- **`clear stats erps-domain <d-name>`**

Viewing ERPS Statistics

This topic shows you how to view or clear the ERPS domain statistics that the E7 automatically collects and stores. Clearing statistics can be helpful after making repairs or correcting an error condition.

ERPS Statistics	
Statistic	**Description**
Number	Specific segment of time in the continuous sequence of captured performance data.
Started At	Time the data capture started for the particular segment number.
Started Sec	Number of seconds in the particular segment of time.
Status	Indicates whether the data capture was completed for the particular segment number.
Ring Down	Number of times an ERPS ring interface that is directly connected to this E7 (local) is out of service (down).
Ring Up	Number of times the ERPS ring service was brought back up from a failed state.
Remote Ring Down	Number of times an ERPS ring interface that is not directly connected (remote) to this E7 is out of service (down).
Remote Ring Up	Number of times an ERPS ring interface that is not directly connected (remote) to this E7 is brought back in service (up) after having been in a failed state (down).
Second Master Detected	Number of times that more than one node is designated as the master node in the ERPS ring.
Health Sequence Error	Number of Ring Health packets lost during the particular time segment.
Bad Packet Received	Number of Bad Packets received on the ERPS ring management VLAN during the particular time segment.
Isolated Node	Number of times both ERPS ring interfaces that are directly connected to the E7 are out of service (down), leaving this node isolated.
Acting Master	The current node that has assumed the role of the ERPS ring Master because no node was designated as Master.
Ring Down TCA	Whether a Ring Down (see above) event exceeded the specified threshold during the particular time segment.
Ring Up TCA	Whether a Ring Up (see above) event exceeded the specified threshold during the particular time segment.
Rmt. Ring Down TCA	Whether a Remote Ring Down (see above) event exceeded the specified threshold during the particular time segment.
Rmt. Ring Up TCA	Whether a Remote Ring Up (see above) event exceeded the specified threshold during the particular time segment.
Sec Master Detected TCA	Whether a Second Master Detected (see above) event exceeded the specified threshold during the particular time segment.
Health Sequence Error TCA	Whether a Health Sequence Error (see above) event exceeded the specified threshold during the particular time segment.
Bad Packet Recv. TCA	Whether a Bad Packet Received (see above) event exceeded the specified threshold during the particular time segment.
Isolated Node TCA	Whether an Isolated Node (see above) event exceeded the specified threshold during the particular time segment.
Acting Master TCA	Whether an Acting Master (see above) event exceeded the specified threshold during the particular time segment.

Note: This procedure assumes that an ERPS domain is configured on the E7.

To view ERPS domain statistics

1. On the Navigation Tree, click **E7**.
2. In the Work Area, click **ERPS**.
3. Double-click the table row that displays the ERPS domain information, and then click **Performance** > **Statistics**.
4. Click **Refresh** periodically to see the up-to-date statistics for the E7.

To clear ERPS domain statistics

1. On the Navigation Tree, click **E7**.
2. In the Work Area, click **ERPS**.
3. Double-click the table row that displays the ERPS domain information, and then click **Performance** > **Statistics**.
4. Click **Action** > **Clear Statistics** to clear the cumulative ERPS performance statistics.

Related topic

- Creating an ERPS Domain

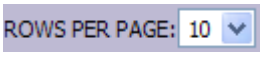
Viewing PON Performance Data

This topic shows you how to view or clear ONT performance data that the E7 automatically collects and stores. Clearing performance monitoring data can be helpful after making repairs or correcting an error condition.

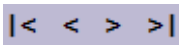
PON Performance Data (Per ONT)	
Statistic	**Description**
Number	Specific segment of time in the continuous sequence of captured performance data.
Started At	Time the data capture started for the particular segment number.
Started Sec	Number of seconds in the particular segment of time.
Status	Indicates whether the data capture was completed for the particular segment number.
BIP Errors Upstream	Number of upstream BIP errors encountered in the interval.
Missed Bursts Upstream	Number of missed upstream bursts encountered in the interval.
GEM HEC Errors Upstream	Number of upstream GEM HEC errors encountered in the interval.
BIP Errors Downstream	Number of downstream BIP errors encountered in the interval.

To view ONT performance data or statistics

1. On the Navigation Tree, click **ONTS**.
2. Click **Provisioned ONTS** > **PON PM (Per ONT)**, and then select what you want to view.
   - To view the ONT statistics, click **Statistics**.
   - To view the performance data accumulation time period to view:
     - Click **15 MIN** to view data in 15-minute periods over 1 day (97 bins).
     - Click **1 DAY** to view data in 1-day periods over 7 days (8 bins).
3. View the data using the navigation tools:
   - Use the horizontal scroll bar to view all of the performance data categories.
   - Use the Rows Per Page drop-down list to control how many rows to display on one screen page.

   - Use the page browser buttons to view the data on the immediate pages (back and next) and the first and last pages.

For CLI:

- **`show pm ont <ont id> [1-day all|1-day bin *|1-day current|1-day last *|15-min all|15-min bin *|15-min current|15-min last *]`**
- **`show stats ont <ont-ID>`**

To clear ONT performance data and statistics

1. On the Navigation Tree, click **ONTS**.
2. Click **Provisioned ONTS** > **PON PM (Per ONT)**, and then select what you want to clear.
   - To select the ONT statistics, click **Statistics**.
   - To select the performance data accumulation time period, choose the time period:
     - Click **15 MIN** to view data in 15-minute periods over 1 day (97 bins).
     - Click **1 DAY** to view data in 1-day periods over 7 days (8 bins).
3. Click **Action**, and select one of the following actions:
   - Select **Clear PM Data** to return all PM registers to zero.
   - Select **Clear Current Period PM Data** to return all PM registers currently accumulating data to zero.

For CLI:

- `clear pm ont <ID> [1-day all|1-day current|15-min all|15-min current]`
- `clear stats ont <ont ID>`

Viewing ONT Port Performance Data

This topic shows you how to view or clear ONT port performance data that the E7 automatically collects and stores. Clearing performance monitoring data can be helpful after making repairs or correcting an error condition.

Note: The performance data is available for the following ONT ports: GE, FE, and T1.

To view ONT port performance data or statistics

1. On the Navigation Tree, click **ONTS**.
2. Click **Provisioned ONTS**, and then double-click the row in the table that indicates the ONT of which you want to view the port performance data.
3. Click **Ports** and then double-click the ONT port of which you want to view the performance data.
4. In the Work Area, click **Performance**, and the select what you want to view the following categories of information.
   - In Octets
   - In Unicast Packets
   - In Broadcast Packets
   - Out Octets
   - Out Unicast Packets
   - Out Broadcast Packets

For CLI:

- `show pm ont-port <port id> [1-day all|1-day bin *|1-day current|1-day last *|15-min all|15-min bin *|15-min current|15-min last *]`
- `show stats ont-port <ont-portID>`

To clear ONT port performance data and statistics

1. On the Navigation Tree, click **ONTS**.
2. Click **Provisioned ONTS**, and then double-click the row in the table that indicates the ONT of which you want to view the performance data.
3. Click **Ports** and then double-click the ONT port of which you want to view the performance data.
4. Click **Action**, and select one of the following actions:
   - Select **Clear Service Stats** and select the service to return all PM registers to zero.
   - Select **Clear Port Stats** to return all PM registers currently accumulating data to zero.

For CLI:

- **clear ont-port <ID>**
- **clear pm ont-port <ID> [1-day all|1-day current|15-min all|15-min current]**
- **clear stats ont-port <ont-portID>**

Viewing ONT Ethernet Port Performance Data

This topic shows you how to view or clear ONT port performance data that the E7 automatically collects and stores. Clearing performance monitoring data can be helpful after making repairs or correcting an error condition.

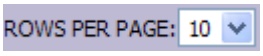
Note: The performance data is available for the following ONT ports: GE, FE, and T1.

ONT Ethernet Port Performance Data	
Statistic	**Description**
Number	Specific segment of time in the continuous sequence of captured performance data.
Started At	Time the data capture started for the particular segment number.
Started Sec	Number of seconds in the particular segment of time.
Status	Indicates whether the data capture was completed for the particular segment number.
FCS Error	The number of frames received on a particular interface that were an integral number of octets in length but failed the frame check sequence (FCS) check. The count is incremented when the MAC service returns the frameCheckError status to the link layer control (LLC) or other MAC user. Received frames for which multiple error conditions are obtained are counted according to the error status presented to the LLC.
Excess Coll	The number of frames whose transmission failed due to excessive collisions.
Late Coll	The number of times that a collision was detected later than 512 bit times into the transmission of a packet.
Rx Frames Too Long	The number of times received frames exceeded the maximum permitted frame size. The count is incremented when the MAC service returns the frameTooLong status to the LLC.
Rx Buff Ovrfl	The number of times that the receive buffer overflowed.
Tx Buff Ovrfl	The number of times that the transmit buffer overflowed.
Sngl Coll	The number of times successfully transmitted frames whose transmission was delayed by exactly one collision.
Multi Coll	The number of times successfully transmitted frames whose transmission was delayed by more than one collision.
Sig Qual Err	The number of times that the SQE test error message was generated by the PLS sublayer.
Defer Tx	The number of frames whose first transmission attempt was delayed because the medium was busy. The count does not include frames involved in collisions.

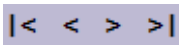
ONT Ethernet Port Performance Data	
Statistic	**Description**
Max Tx Err	The number of frames whose transmission failed due to an internal MAC sublayer transmit error.
Carr Sense Err	The number of times that carrier sense was lost or never asserted when attempting to transmit a frame.
Align Err	The number of received frames that were not an integral number of octets in length and did not pass the FCS check.
MAC Rx Err	The number of frames whose reception failed due to an internal MAC sublayer receive error.

To view ONT Ethernet port performance data or statistics

1. On the Navigation Tree, click **ONTS**.
2. In the work area, click **Provisioned ONTS** > **Provisioning**, and then click a listed ONT ID to select the ONT on which you want to view the port performance data.
   - Alternatively, enter the ONT ID in the toolbar, and then click **Apply**.
3. Click **Ports** > **Ethernet PM**, and then select what you want to view.
   - To view the ONT Ethernet port statistics, click **Statistics**.
   - To view the performance data accumulation time period to view:
     - Click **15 MIN** to view data in 15-minute periods over 1 day (97 bins).
     - Click **1 DAY** to view data in 1-day periods over 7 days (8 bins).
4. View the data using the navigation tools:
   - Use the horizontal scroll bar to view all of the performance data categories.
   - Use the Rows Per Page drop-down list to control how many rows to display on one screen page.

   - Use the page browser buttons to view the data on the immediate pages (back and next) and the first and last pages.

For CLI:

- **`show pm ont-port <port id> [1-day all|1-day bin *|1-day current|1-day last *|15-min all|15-min bin *|15-min current|15-min last *]`**
- **`show stats ont-port <ont-portID>`**

To clear ONT Ethernet port performance data and statistics

1. On the Navigation Tree, click **ONTS**.
2. In the work area, click **Provisioned ONTS** > **Provisioning**, and then click a listed ONT ID to select the ONT on which you want to view the port performance data.
   - Alternatively, enter the ONT ID in the toolbar, and then click **Apply**.
3. Click **Ports** > **Ethernet PM**, and then click one of the following sequences:
   - Click **15 MIN** or **1 Day**, and then click **Action**, and select one of the following actions:
     - Select **Clear PM Data** to return all PM registers to zero.
     - Select **Clear Current Period PM Data** to return all PM registers currently accumulating data to zero.
   - Click **Statistics** > **Action** > **Clear Statistics**.

For CLI:

- **`clear pm ont-port <ID> [1-day all|1-day current|15-min all|15-min current]`**
- **`clear stats ont-port <ont-portID>`**

Viewing ONT Voice (POTS) Port Voice Service Performance Data

This topic shows you how to view ONT Voice (POTS) port voice service performance data that the E7 automatically collects and stores. Refreshing performance monitoring data can be helpful after making repairs or correcting an error condition.

Note: The performance data is available per POTS/Voice port enabled for VoIP (SIP or TDM Gateway) service.

ONT POTS Port Voice Service Performance Data	
VoIP Service Statistic	**Description**
DHCP Attempts	DHCP Discover requests.
DHCP ACKs Received	Successful dhcpAttempts.
DHCP NACKs Received	Unsuccessful dhcpAttempts + catchall counter for all DHCP errors.
Registration Attempts	SIP REGISTER message requests.
Registration Challenges	SIP REGISTER challenge messages received.
Registraton Rejects	SIP REGISTER registration requests rejected/denied.
Registration Grants	SIP REGISTER message requests granted OK.
RTP Packets Sent	Total RTP Packets Sent.
RTP Packets Received	Total RTP Packets Received.
RTP Null IP Sent	Total RTP Packets Sent with 0.0.0.0 for dest addr-sent to put rem on Hold.

ONT POTS Port Voice Service Performance Data	
VoIP Service Statistic	**Description**
RTP Null IP Received	Total RTP Packets Rec with 0.0.0.0 for dest addr-sent to put loc end on Hold.
Missing RTP	Running total of missing received RTP packets. A missing packet may also be counted a s a sequence error.
RTP Packet Size	Last received RTP packet size. 80 - 10ms packet size 160 - 20ms packet size
Received RTP with Bad Src Port Cnt	Running total of received RTP packets whose source UDP port number does not equal the expected remote port number for this line.
Received RTP Comfort Noise Pkts	Running total of received RTP comfort noise(RFC3389) packets for this line. Reception of RTP Comfort noise packets can interfere with FAX and modem calls.
RTP Encode Type	RTP encode type received. G.711 u-law (0).
RTP Sequence Error	Running total of received RTP packets with a detected sequence error.
RTP QoS Stamp	The hex value of the Qos/DiffServ Codepoint byte being stamped in the outgoing IP header of the RTP packet.
Port Input Under Runs	Running total of listens(read requests) that return no RTP packet for this line.
Port Input Activity Counter	Total cumulative usage of the line. This counter is incremented every 100 seconds a call is active.
Tx Error (To Remote Port)	Running total of transmit errors on writes to the remote IP port.
Receive Error (On Local Port)	Running total of received errors on reads of the local IP port. Errors are unexpected packet size or type.
VoIP Call Statistics	**Description**
Inbound Call Attempts	Incoming Calls Received.
Inbound Call Completions	Incoming Calls Completed successfully.
Inbound Call Busy	Incoming Calls Received when line is busy.
Inbound Call Disconnect (by peer)	Incoming Calls disconnected by far end peer.
Inbound Call Disconnect (by ONT)	Incoming Calls disconnected by local ONT OnHook.
Active Call Counter	Total cumulative usage of the line. This counter is incremented every 100 seconds a call is active.
Outbound Call Attempts	Outgoing Calls Attempted.
Outbound Call Completions	Outgoing Calls Completed successful.
Outbound Call Busy	Outgoing Calls that received a BUSY reply.
Outbound Call Disconnects (by peer)	Outgoing Calls disconnected by far end peer.
Outbound Call Disconnects (by ONT)	Outgoing Calls disconnected by local ONT OnHook.
E911 Call Attempts	Emergency 911 Call Attempts.
E911 Call Completions	Emergency 911 Call Attempts Completed successfully.
E911 Call Busy	Emergency 911 Call Attempts that received a BUSY reply
E911 Call Disconnect (by peer)	Emergency 911 disconnected by far end E911 operator.
E911 Call On Hooks	Emergency 911 Call Attempts local OnHook attempts.
Active 911 Call	Indicates a 911 call is currently active on this line. Boolean.

To view ONT port voice service performance data or statistics

1. On the Navigation Tree, click **ONTS**.
2. In the Work Area, click **Ports** > **Voice Svc PM**.
3. In the toolbar, click **Refresh** to view the updated values.

For CLI:

- **`show pm ont-port <port id> [1-day all|1-day bin *|1-day current|1-day last *|15-min all|15-min bin *|15-min current|15-min last *]`**
- **`show stats ont-port <ont-portID>`**
- **`show pots-port`**
- **`show pots-port detail`**
- **`show pots-port <port> [detail|sip-svc|tdm-gw-svc]`**
- **`clear pm ont-port <ID> [1-day all|1-day current|15-min all|15-min current]`**
- **`clear stats ont-port <ont-portID>`**
- **`clear pots-port <p-id> sip-counters`**
- **`clear pots-port <p-id> tdm-gw-counters`**

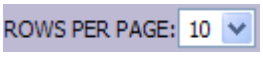
Viewing ONT Port T1/E1 Performance Data

This topic shows you how to view or clear ONT T1 port performance data that the E7 automatically collects and stores. Clearing performance monitoring data can be helpful after making repairs or correcting an error condition.

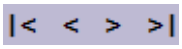
ONT T1/E1 Port Performance Data	
Statistic	**Description**
Number	Specific segment of time in the continuous sequence of captured performance data.
Started At	Time the data capture started for the particular segment number.
Started Seconds	Number of seconds in the particular segment of time.
Status	Indicates whether the data capture was completed for the particular segment number.
Error Seconds	Number of errored seconds encountered in the interval.
Severely Error Seconds	Number of severely-errored seconds encountered in the interval.
Bursty Error Seconds	Number of bursty-errored seconds encountered in the interval.
Unavailable Seconds	Number of unavailable seconds encountered in the interval.
Controlled Slip Seconds	Number of controlled slip seconds encountered in the interval.

To view ONT port performance data or statistics

1. On the Navigation Tree, click **ONTS**.
2. In the work area, click **Provisioned ONTS** > **Ports** > **T1/E1 PM**, and the select what you want to view.
   - To view the ONT port statistics, click **Statistics**.
   - To view the performance data accumulation time period to view:
     - Click **15 MIN** to view data in 15-minute periods over 1 day (97 bins).
     - Click **1 DAY** to view data in 1-day periods over 7 days (8 bins).
3. View the data using the navigation tools:
   - Use the horizontal scroll bar to view all of the performance data categories.
   - Use the Rows Per Page drop-down list to control how many rows to display on one screen page.

   - Use the page browser buttons to view the data on the immediate pages (back and next) and the first and last pages.

For CLI:

- **`show pm ont-port <port id> [1-day all|1-day bin *|1-day current|1-day last *|15-min all|15-min bin *|15-min current|15-min last *]`**
- **`show stats ont-port <ont-portID>`**

To clear ONT port performance data and statistics

1. On the Navigation Tree, click **ONTS**.
2. In the work area, click **Provisioned ONTS** > **Ports** > **T1 PM**, and the select what you want to clear.
   - To select the ONT port statistics, click **Statistics**.
   - To select the performance data accumulation time period:
     - Click **15 MIN** to view data in 15-minute periods over 1 day (97 bins).
     - Click **1 DAY** to view data in 1-day periods over 7 days (8 bins).
3. Click **Action**, and select one of the following actions:
   - Select **Clear PM Data** to return all PM registers to zero.
   - Select **Clear Current Period PM Data** to return all PM registers currently accumulating data to zero.

For CLI:

- **`clear pm ont-port <ID> [1-day all|1-day current|15-min all|15-min current]`**
- **`clear stats ont-port <ont-portID>`**

Viewing ONT PWE3 Service Performance Data

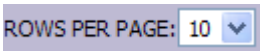
This topic shows you how to view or clear ONT PWE3 service performance data that the E7 automatically collects and stores. Clearing performance monitoring data can be helpful after making repairs or correcting an error condition.

ONT PWE3 Service Performance Data	
Statistic	**Description**
Number	Specific segment of time in the continuous sequence of captured performance data.
Started At	Time the data capture started for the particular segment number.
Started Sec	Number of seconds in the particular segment of time.
Status	Indicates whether the data capture was completed for the particular segment number.
Received Packets	Total number of packets, both payload and signaling, received in the PSN to TDM direction.
Transmitted Packets	Total number of packets, both payload and signaling, transmitted from the TDM to the PSN. The count includes packets whose L-bit is set and may contain no payload.
Missing Packets	Number of lost packets, as indicated by gaps in the control word numbering sequence. Both payload and signaling packets, if any, contribute to this count.
Misordered Usable Packets	Number of packets received out of order, but which were able to be successfully re-ordered and played out. Both payload and signaling packets, if any, contribute to this count.
Misordered Dropped Packets	Number of packets received out of sequence that were discarded, either because the ONT did not support reordering or because it was too late to reorder them. Both payload and signaling packets, if any, contribute to this count.
Buffer Under/Overrun	Number of packets that were discarded because they arrived too late or too early to be played out. Both payload and signaling packets, if any, contribute to this count.
Malformed Packets	Number of malformed packets, such as the packet length was not as expected or the RTP payload type was unexpected. Both payload and signaling packets, if any, contribute to this count.
Stray Packets	Number of packets whose ECID or RTP SSRC failed to match the expected value, or which are otherwise known to have been misdelivered. Stray packets are discarded without affecting any other PM counters. Both payload and signaling packets, if any, contribute to this count.
Remote Packets loss	Number of received packets whose Remote-bit (R-bit) is set, indicating the loss of packets at the far end. Both payload and signaling packets, if any, contribute to this count.

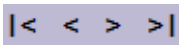
ONT PWE3 Service Performance Data	
Statistic	**Description**
TDM L-Bit Packets Sent	Number of packets transmitted with the L-bit set, indicating a near-end TDM fault. Both payload and signaling packets, if any, contribute to this count.
Error Seconds	Number of errored seconds encountered in the interval.
Severely Error Seconds	Number of severely-errored seconds encountered in the interval.
Unavailable Seconds	Number of unavailable seconds encountered in the interval.

To view ONT PWE3 service performance data or statistics

1. On the Navigation Tree, click **ONTS**.
2. In the Work Area, click **Provisioned ONTs.**
3. In the table, double-click the ONT that has a T1 port provisioned with PWE3 service.
4. In the table of ONT ports, double-click the T1 port that is provisioned with the PWE3 service.
5. Click **PWE3 SVC PM**, and then select the data to view.
   - To view the PWE3 service statistics, click **Statistics**.
   - To view the performance data accumulation time period to view:
     - Click **15 MIN** to view data in 15-minute periods over 1 day (97 bins).
     - Click **1 DAY** to view data in 1-day periods over 7 days (8 bins).
6. View the data using the navigation tools:
   - Use the horizontal scroll bar to view all of the performance data categories.
   - Use the Rows Per Page drop-down list to control how many rows to display on one screen page.

   - Use the page browser buttons to view the data on the immediate pages (back and next) and the first and last pages.

For CLI:

- **`show pm ont-port <port id> pwe3-svc [1-day all|1-day bin *|1-day current|1-day last *|15-min all|15-min bin *|15-min current|15-min last *]`**
- **`show stats ont-port <ont-ID>`**

To clear ONT PWE3 service performance data and statistics

1. On the Navigation Tree, click **ONTS**.
2. In the Work Area, click **Provisioned ONTs.**
3. In the table, double-click the ONT that has a T1 port provisioned with PWE3 service.
4. In the table of ONT ports, double-click the T1 port that is provisioned with the PWE3 service.
5. Click **PWE3 SVC PM**.
6. From the menu, click **Action**, and then select one of the following actions:
   - Select **Clear PM Data** to return all PM registers to zero.
   - Select **Clear Current Period PM Data** to return all PM registers currently accumulating data to zero.

For CLI:

- **`clear pm ont-port <ID> [1-day all|1-day current|15-min all|15-min current]`**
- **`clear stats ont-port <ont ID>`**

Viewing PPPoE Statistics

This topic shows you how to view .

This topic shows you how to view or refresh the PPPoE statistics for performance data that the E7 automatically collectson xDSL ports, xDSL-bonded groups, or ONT Ethernet ports. Refreshing the status information can be helpful after making repairs or correcting an error condition.

DHCP Configuration Dynamic Status Information	
Status	**Description**
Packets Received	The total number of invalid packets received in all Trusted and Untrusted interfaces when DHCP Snooping is enabled. For "Untrusted" interfaces, the total number of ACK, NAK, and OFFER messages received and dropped are shown. For "Trusted" interfaces, the number of invalid DHCP messages received are shown (anything other than Discover, Request, Decline, Release, Inform, ACK, NAK and Offer).
Packets Received Error	
Packets Sent	
Packets Sent Error	
Discovery Received	This counter indicates the total number of valid PADI DISCOVERY messages received on the port with a PPPoE session.
Discovery Received Error	This counter indicates the total number of PADI DISCOVERY messages UNSUCCESSFULLY received on a port with a PPPoE session.

DHCP Configuration Dynamic Status Information	
Status	**Description**
Discovery Sent	This counter indicates the total number of valid PADI DISCOVERY messages sent on the port with a PPPoE session.
Discovery Sent Error	This counter indicates the total number of PADI DISCOVERY messages UNSUCCESSFULLY sent on a port with a PPPoE session.
Offer Received	This counter indicates the total number of valid PADO OFFER messages received on the port with a PPPoE session.
Offer Received Error	This counter indicates the total number of PADO OFFER messages UNSUCCESSFULLY received on a port with a PPPoE session.
Offer Sent	This counter indicates the total number of valid PADO OFFER messages sent on the port with a PPPoE session.
Offer Sent Error	This counter indicates the total number of PADO OFFER messages UNSUCCESSFULLY sent on a port with a PPPoE session.
Request Received	This counter indicates the total number of valid PADR REQUEST messages received on the port with a PPPoE session.
Request Received Error	This counter indicates the total number of PADR REQUEST messages UNSUCCESSFULLY received on a port with a PPPoE session.
Request Sent	This counter indicates the total number of valid PADR REQUEST messages sent on the port with a PPPoE session.
Request Sent Error	This counter indicates the total number of PADR REQUEST messages UNSUCCESSFULLY sent on a port with a PPPoE session.
Session Received	This counter indicates the total number of valid PADS SESSION messages received on the port with a PPPoE session.
Session Received Error	This counter indicates the total number of PADS SESSION messages UNSUCCESSFULLY received on a port with a PPPoE session.
Session Sent	This counter indicates the total number of valid PADS SESSION messages sent on the port with a PPPoE session.PADS
Session Sent Error	This counter indicates the total number of PADS SESSION messages UNSUCCESSFULLY sent on a port with a PPPoE session.
Terminate Received	This counter indicates the total number of valid PADT TERMINATE messages received on the port with a PPPoE session.
Terminate Received Error	This counter indicates the total number of PADT TERMINATE messages UNSUCCESSFULLY received on a port with a PPPoE session.
Terminate Transmitted	This counter indicates the total number of valid PADT TERMINATE messages sent on the port with a PPPoE session.
Terminate Transmitted Error	This counter indicates the total number of PADT SESSION messages UNSUCCESSFULLY sent on a port with a PPPoE session.

To view the PPPoE statistics

1. On the Navigation Tree, click the xDSL port, xDSL bonded group, or ONT Ethernet port of interest.
2. Click **PPPoE** > **Statistics** to view the PPPoE statistics on the port or bonded group.
3. In the toolbar, click **Refresh** to update the collected statistics.
4. In the toolbar, click **Action** > **Clear Statistics** to erase the collected statistics and start collecting a new set of statistics.

For CLI:

```
show stats ont-port <one-id/port-id>
show stats dsl-port <dsl-port-id>
clear stats ont-port <one-id/port-id>
clear stats dsl-port <dsl-port-id> <ethernet|line>
```

Viewing DHCP Statistics

This topic shows you how to view or refresh the DHCP performance data that the E7 automatically collects. Refreshing the status information can be helpful after making repairs or correcting an error condition. For modular chassis systems, this statistics data is merged across all cards in the system.

DHCP Configuration Dynamic Status Information	
Status	**Description**
Error Pkts	The total number of invalid packets received in all Trusted and Untrusted interfaces when DHCP Snooping is enabled. For "Untrusted" interfaces, the total number of ACK, NAK, and OFFER messages received and dropped are shown. For "Trusted" interfaces, the number of invalid DHCP messages received are shown (anything other than Discover, Request, Decline, Release, Inform, ACK, NAK and Offer).
Discard Pkts	The total number of received DHCP packets of the wrong type for a given port. For example, a received DHCP server message on a port where only client messages are expected.
No Option 82 Enabled	When DHCP Snooping and Option 82 are enabled, the total number of packets received on "Untrusted" interfaces where no Option 82 profile is assigned to the interface.
Option 82 Present Dropped	When DHCP Snooping and Option 82 are enabled, and Option 82 is set to "Drop" policy, this value is the total number of packets received on all "Untrusted" interfaces with Option 82 presence.
Option 82 Mismatch	When DHCP Snooping and Option 82 are enabled, this value is the total number of packets received on all "Trusted" interfaces where a valid Option 82 session is not found.
Ack MAC Collision	The number of times when the same VLAN/MAC (client) is on two different ONT Ethernet ports and given two different IP addresses, due to one of the following situations:

DHCP Configuration Dynamic Status Information	
Status	**Description**
	Note: If the same client does appear on a different ONT Ethernet port and is given the *same* IP address, this is considered a station movement and not an error.
Discover Received	This counter indicates the total number of valid DHCP DISCOVERY message received in all interfaces and all vlans with DHCP Snooping enabled.
Discover Sent	This counter indicates the total number of DHCP DISCOVERY message successfully sent in all interfaces and all vlans with DHCP Snooping enabled.
Discover Error	This counter indicates the total number of DHCP DISCOVERY message UNSUCCESSFULLy sent in all interfaces and all vlans with DHCP Snooping enabled.
Offer Received	This counter indicates the total number of valid DHCP OFFER message received in all interfaces and all vlans with DHCP Snooping enabled.
Offer Sent	This counter indicates the total number of DHCP OFFER message successfully sent in all interfaces and all vlans with DHCP Snooping enabled.
Offer Error	This counter indicates the total number of DHCP OFFER message UNSUCCESSFULLY sent in all interfaces and all vlans with DHCP Snooping enabled.
Request Received	This counter indicates the total number of valid DHCP REQUEST messages received in all interfaces and all vlans with DHCP Snooping enabled.
Request Sent	This counter indicates the total number of DHCP REQUEST message successfully sent in all interfaces and all vlans with DHCP Snooping enabled.
Request Error	This counter indicates the total number of DHCP REQUEST message UNSUCCESSFULLY sent in all interfaces and all vlans with DHCP Snooping enabled.
Decline Received	This counter indicates the total number of valid DHCP DECLINE messages received in all interfaces and all vlans with DHCP Snooping enabled.
Decline Sent	This counter indicates the total number of DHCP DECLINE message successfully sent in all interfaces and all vlans with DHCP Snooping enabled.
Decline Error	This counter indicates the total number of DHCP DECLINE message UNSUCCESSFULLY sent in all interfaces and all vlans with DHCP Snooping enabled.
ACK Received	This counter indicates the total number of valid DHCP ACK messages received in all interfaces and all vlans with DHCP Snooping enabled.
ACK Sent	This counter indicates the total number of DHCP ACK message successfully sent in all interfaces and all vlans with DHCP Snooping enabled.
ACK Error	This counter indicates the total number of DHCP ACK message UNSUCCESSFULLY sent in all interfaces and all vlans with DHCP Snooping enabled.
NACK Received	This counter indicates the total number of valid DHCP NACK messages received in all interfaces and all vlans with DHCP Snooping enabled.
NACK Sent	This counter indicates the total number of DHCP NACK message successfully sent in all interfaces and all vlans with DHCP Snooping enabled.

DHCP Configuration Dynamic Status Information	
Status	**Description**
NACK Error	This counter indicates the total number of DHCP NACK message UNSUCCESSFULLY sent in all interfaces and all vlans with DHCP Snooping enabled.
Release Received	This counter indicates the total number of valid DHCP RELEASE messages received in all interfaces and all vlans with DHCP Snooping enabled.
Release Sent	This counter indicates the total number of DHCP RELEASE message successfully sent in all interfaces and all vlans with DHCP Snooping enabled.
Release Error	This counter indicates the total number of DHCP RELEASE message UNSUCCESSFULLY sent in all interfaces and all vlans with DHCP Snooping enabled.
Inform Received	This counter indicates the total number of valid DHCP INFORM messages received in all interfaces and all vlans with DHCP Snooping enabled.
Inform Sent	This counter indicates the total number of DHCP INFORM message successfully sent in all interfaces and all vlans with DHCP Snooping enabled.
Inform Error	This counter indicates the total number of DHCP INFORM message UNSUCCESSFULLY sent in all interfaces and all vlans with DHCP Snooping enabled.

To view DHCP statistics

1. On the Navigation Tree, click **E7**.
2. In the work area, click **DHCP** > **Provisioning** to view the E7 DHCP statistics.

For CLI:

```
show dhcp-cfg
```

To clear the E7 DHCP statistics

1. On the Navigation Tree, click **E7**.
2. Click **DHCP** > **Provisioning** to view the E7 DHCP statistics.
3. In the toolbar, click **Action** > **Clear DHCP Stats**.

For CLI:

```
clear dhcp-cfg counters
```

Viewing LACP Statistics

This topic shows you how to view or refresh the Link Aggregate Group (LAG) Interface performance data that the E7 automatically collects. Refreshing the LAG status information can be helpful after making repairs or correcting an error condition. For modular chassis systems, this statistics data only applies to shelf 1 in the system.

Link Aggregate Group Status Information	
Status	**Description**
Operational Status	Service state of port interface.
Additional Status	Additional messages regarding the LAG status.
RSTP Suppressed	Whether the interface is running rapid spanning tree protocol (RSTP).
Interface Count	Number of Ethernet ports participating in the LAG.
Speed (Mbps)	Speed of ports in the LAG: GE or 10GE.
VLAN Count	Number of VLANs memberships in which the LAG participates.
Tag Action Count	Number of tag actions that are associated with the LAG.
STP State	Whether the LAG is blocking or forwarding.
STP Role	Whether the STP role is disabled or enabled.
STP Effective Priority	Spanning tree protocol (STP) priority of this port interface.
STP Effective Cost	Spanning tree protocol (STP) path cost is the cost of transmitting a frame on to a network through that port. It is assigned according to the speed of the bridge. The slower the media, the higher the cost.
Interface State	Service state of port interface.
STP Designated Cost	Path cost to the Root Bridge from the Designated port on the LAN segment to which this port is attached.
Intf. LACP MAC Address	
Operating As Edge	Indicates whether the interface is provisioned to have RSTP and “Auto edge link” enabled, and the interface has not received any RSTP BPDUs from the bridge to which it is connected. This allows the interface to more quickly transition to the state of forwarding packets.
Rx RSTP BPDU	Number of incoming RSTP BPDUs received by this interface.
Rx STP Config	Number of incoming STP “Configuration” BPDUs received by this interface.
Rx STP Topology Changes	Number of incoming STP “Topology Change” BPDUs received by this interface.
Tx RSTP BPDU	Number of outgoing RSTP BPDUs transmitted by this interface.
Tx STP Config	Number of outgoing STP “Configuration” BPDUs transmitted by this interface.
Tx STP Topology Changes	Number of outgoing STP “Topology Change” BPDUs transmitted by this interface.
Effective Native VLAN	Dynamic attribute based on the native VLAN parameter of the Ethernet port interface or the tag action. • If the Ethernet interface has an add-tag tag-action that matches all traffic (effectively acting as the provisioned native-vlan), the VLAN value in the add-tag tag-action appears. • If there is no such tag-action on the Ethernet interface, then the provisioned native-vlan value appears.

To view LAG group status

1. On the Navigation Tree, click **INTERFACES** and then click **LAGINTF:#**.
   - Alternatively, you can click **CARD1** or **CARD2**, then click **GE#** or **10GE#**, that is a member of a LAG, and then click **Associated Interface**.
2. Click **Refresh** periodically to see the up-to-date statistics for the LAG.

For CLI:

```
show stats lacp [interface <i-name>]
clear stats lacp interface <i-name>
```

Viewing IGMP Statistics

This topic shows you how to view or clear the Internet Group Management Protocol (IGMP) statistics that the E7 automatically collects and stores. The counters are supported on a per-VLAN basis and also show the total value across all IGMP-enabled VLANS. Clearing statistics can be helpful after making repairs or correcting an error condition. For modular chassis systems, this statistics data is merged across all cards in the system.

IGMP Statistics	
Statistic	**Description**
Operational Status	Indicates whether IGMP snoop is enabled for multicast traffic on the VLAN.
IGMPv2 Joins Sent	Number of times the node sends an IGMP "group join" message to the group's transmitter.
IGMPv2 Joins Recv.	Number of times the node received an IGMP "group join" message to forward.
IGMP Leaves Sent	Number of times the node sent an IGMP "group leave" message to the transmitter.
IGMP Leaves Recv.	Number of times the node received an IGMP "group leave" message to forward.
IGMP Group Specific Queries Sent	Number of times the node received an IGMPv2 Multicast Group Query.
IGMP Group Specific Queries Recv.	Number of times the node received an IGMPv2 Multicast Group Query from Multicast sources (typically a multicast capable router).
IGMP Invalid Mesg. Count	Number of times the node received and discarded an invalid IGMP message.
Query Solicits Sent	Number of times the node sent query solicits.
Query Solicits Received	Number of times the node received query solicits.
General Queries Sent	Number of times the node sent general queries.
General Queries Received	Number of times the node received general queries.

To view IGMP statistics

1. On the Navigation Tree, click **E7**.
2. In the Work Area, click **Multicast** > **IGMP**.
3. Click **Refresh** periodically to see the up-to-date statistics for the E7.

To view IGMP counters

1. On the Navigation Tree, click **VLANs**.
2. In the Work Area, click **IGMP Counters**.
3. Click **Refresh** periodically to see the up-to-date statistics for the E7.

To clear IGMP statistics at the system level

1. On the Navigation Tree, click **E7**.
2. In the Work Area, click **Multicast** > **IGMP** > **Action** > **Clear IGMP Statistics**.

To clear IGMP statistics at the VLAN level

1. On the Navigation Tree, click **VLANs**.
2. In the Work Area, click **IGMP Counters** > **Action** > **Clear IGMP Statistics**.

To clear IGMP statistics at the interface level

1. On the Navigation Tree, click **VLANs**.

In the Work Area, click IGMP Counters **>** Action **>** Clear IGMP Statistics**.For CLI:**

```
clear stats igmp-counters
clear interface <intfc-name> igmp-counters
clear interface <intfc-name> vlan <vlan-id> igmp-counters
```

Viewing MEP Statistics

This topic shows you how to view or clear the Maintenance End Points (MEPs) statistics that the E7 automatically collects and stores. Clearing statistics can be helpful after making repairs or correcting an error condition.

The following tables show the types of MEP statistics that you can view.

Maintenance End Point (MEP) Statistics	
Category	**Statistic**
Continuity Check	Quantities for the following: • Continuity Check Messages (CCM) received • Continuity Check Messages (CCM) sent • Remote Defect Indications (RDI) received • Remote Defect Indications (RDI) sent
Loopback	Quantities for the following: • Loopback Messages (LBM) received • Loopback Messages (LBM) sent • Loopback Responses (LBR) received • Loopback Responses (LBR) sent • Loopback Responses (LBR) received out of order • Loopback Responses (LBR) with bad MAC service data unit (MSDU) • Loopback Responses (LBR) with bad sender ID
Link Trace	Quantities for the following: • Link Trace Messages (LTM) received • Link Trace Messages (LTM) sent • Link Trace Responses (LTR) with bad MAC service data unit (MSDU) • Link Trace Responses (LTR) received • Link Trace Responses (LTR) sent • Link Trace Responses (LTR) received that were unexpected
Loss Measurement	Quantities for the following: • Loss Measurement Messages (LMM) received • Loss Measurement Messages (LMM) sent • Loss Measurement Responses (LMR) received • Loss Measurement Responses (LMR) sent
General	Number of times for each condition: • PDUs were received with an invalid Sender ID • PDUs were received with an invalid Port status • PDUs were received with an invalid Interface status • PDUs were received with invalid Sequence errors

To view MEP statistics

1. On the Navigation Tree, click **E7**.
2. In the Work Area, click **Ethernet OAM > MEGS**.
3. In the MEG table, double-click the MEG that has the MEP of which you want to view the statistics.
4. In the MEP table, double-click the MEP of which you want to view the statistics.
5. Click MEP STATS to view the statistics.

6. Click **Refresh** periodically to see the up-to-date statistics.

To clear the MEP statistics

1. On the Navigation Tree, click **E7**.
2. In the Work Area, click **Ethernet OAM > MEPS**, and select the statistics to clear:
   - To clear the loss statistics, click **Frame Loss Stats**. In the menu, click **Action** > **Clear Frame Loss Statistics**.
   - To clear the delay statistics, click **Frame Delay Stats**. In the menu, click **Action** > **Clear Frame Delay Statistics**.

For CLI:

- `show stats meg <name> mep ont-port <port-id> frame-delay`
- `show stats meg <name> mep id <endpoint-id> frame-delay`
- `show stats meg <name> mep ont-port <port-id> frame-loss`
- `show stats meg <name> mep id <endpoint-id> frame-loss`
- `clear stats meg <meg-name> mep ont-port <o-port> [frame-delay|frame-loss]`
- `clear stats meg <meg-name> mep ont <ont-id> ip-host <sip|tdm-gw|h248|pwe3> [frame-delay|frame-loss]`
- `clear stats meg <meg-name> mep id <endpoint-id> [frame-delay|frame-loss]`
- `clear stats meg <meg-name> mip ont-port <o-port> [frame-delay|frame-loss]`

Viewing Frame Loss and Delay Statistics

This topic shows you how to view or clear the frame loss and delay statistics that the E7 automatically collects and stores. The counters are supported on a per-MEG basis. Clearing statistics can be helpful after making repairs or correcting an error condition.

The following Maintenance End Points (MEPs) parameters must be set to enabled for the E7 to collect both types of frame statistics:

- Delay Measurement
- Loss Measurement

Typically, all MEPs will use the same parameters for measuring the frame delay or frame loss. These parameters are included in the frame-measurement profile that is associated to a MEP.

- **Frame Loss Ratio** - A ratio of the number of service frames not delivered divided by the total number of service frames during time interval T, where the number of service frames not delivered is the difference between the following, expressed as a percentage:
  - Number of service frames arriving at the ingress Ethernet flow point
  - Number of service frames delivered at the egress Ethernet flow point in a point-to-point Ethernet connection
- **Frame Delay** - A round-trip delay for a frame, defined as the time elapsed between the following:
  - Start of transmission of the first bit of the frame by a source node
  - Reception of the last bit of the loop backed frame by the same source node
- **Frame Delay Variation** - A measure of the variations in the frame delay between a pair of service frames, where the service frames belong to the same CoS instance on a point-to-point Ethernet connection.
- **Throughput** - The maximum rate at which no frame is dropped. This is typically measured under test conditions.

Frame Delay Statistics (Per MEP)	
Category	**Statistic**
Remote MEP	• MEP ID of the remote MEP • MAC Address of the remote MEP
Round-trip Delay	• Minimum measured round-trip delay between MEPs (in microseconds) • Maximum measured round-trip delay between MEPs (in microseconds) • Average measured round-trip delay between MEPs (in microseconds)
Round-trip Delay Variation	• Minimum time in microseconds • Maximum time in microseconds • Average time in microseconds

Frame Loss Statistics (Per MEP)	
Category	**Statistic**
Remote MEP	• MEP ID of the remote MEP • MAC Address of the remote MEP
Near-end Loss	• Smallest percentage of detected ingress data frame loss • Largest percentage of detected ingress data frame loss • Average percentage of detected ingress data frame loss
Far-end Loss	• Smallest percentage of detected egress data frame loss • Largest percentage of detected egress data frame loss • Average percentage of detected egress data frame loss

To view frame loss or delay statistics

1. On the Navigation Tree, click **E7**.
2. In the Work Area, click **Ethernet OAM > MEPS**, and select the statistics to view:
   - To view the loss statistics, click **Frame Loss Stats**.
   - To view the delay statistics, click **Frame Delay Stats**.
3. Click **Refresh** periodically to see the up-to-date statistics for the E7.

To clear the frame loss or delay statistics

1. On the Navigation Tree, click **E7**.
2. In the Work Area, click **Ethernet OAM > MEPS**, and select the statistics to clear:
   - To clear the loss statistics, click **Frame Loss Stats**. In the menu, click **Action** > **Clear Frame Loss Statistics**.
   - To clear the delay statistics, click **Frame Delay Stats**. In the menu, click **Action** > **Clear Frame Delay Statistics**.

For CLI:

- `show stats meg <name> mep ont-port <port-id> frame-delay`
- `show stats meg <name> mep id <endpoint-id> frame-delay`
- `show stats meg <name> mep ont-port <port-id> frame-loss`
- `show stats meg <name> mep id <endpoint-id> frame-loss`
- `clear stats meg <meg-name> mep ont-port <o-port> [frame-delay|frame-loss]`
- `clear stats meg <meg-name> mep ont <ont-id> ip-host <sip|tdm-gw|h248|pwe3> [frame-delay|frame-loss]`
- `clear stats meg <meg-name> mep id <endpoint-id> [frame-delay|frame-loss]`
- `clear stats meg <meg-name> mip ont-port <o-port> [frame-delay|frame-loss]`

Related topics

- *Creating Frame-Measurement Profiles* (on page 47)

Viewing ONT RF Counters for RF Video Overlay

To view ONT RF counters for RF video overlay

1. In the Navigation Tree, click **ONTs**.
2. In the Workarea, click Provisioned **ONTs** > **Ports**.
3. Scroll down the table to find the ONT AVO port that you want to clear the counters, and then double-click the port to select it.

   The counters and port status are show in the Workarea.

To clear ONT RF counters for RF video overlay

1. In the Navigation Tree, click **ONTs**.
2. In the Workarea, click Provisioned **ONTs** > **Ports**.
3. Scroll down the table to find the ONT AVO port that you want to clear the counters, and then double-click the port to select it.
4. In the menu, click **Action** > **Clear AVO Stats**.

For CLI:

```
clear ont <p-id> rf-burst-counters
```

Chapter 2

Replacing or Installing Equipment

This chapter describes how to replace, remove, or install E7 equipment.

Topics Covered

This chapter covers the following topics and tasks:

- Replacing or adding a line card
- Restoring a backup database
- Deleting an ONT from a PON
- Replacing an ONT
- Adding a Node to an existing ERPS ring
- Changing the role of ERPS ring nodes
- Adding a shelf to a modular chassis system
- Deleting a shelf from a modular chassis system
- Replacing a faulty shelf

Replacing or Adding a Line Card

A configuration database relates to a specific E7 chassis (backplane or modular chassis) and specific card(s) provisioning. Each card in the system has a copy of the database.

This topic describes how to replace an E7 line card with the same or different type of card.

- When you replace a line card with the same type of card:
  - In a multi-card system where the replaced card had provisioned services, the existing database and service provisioning are applied to the new card when it arrives.
  - In a single-card system, the new card starts operating with a default (empty) database. (If a database backup is available, you could provision the new card with provisioned services previously created on the shelf by performing a database restore operation.) When replacing the card in a single-card shelf in a modular chassis, the replacement card must be running R1.2 or later before installing it into the shelf.
- When you replace a line card with a different type of card:
  - The service provisioning records must be deleted before the system will discover the card and add it to the system inventory.
  - The exception to this rule is for an E7-20 GPON-4x to GPON-8x replacement or GPON-8x to GPON-4x replacement, as long as no ONTs are linked on ports 5-8 of the GPON-8x card.

Note: If the replaced card had no provisioned services (Additional Status: default-prov), the card is deleted from the database upon card departure.

Moving cards and chassis ID association

When you install a second card in a duplex system where the card had been previously installed in the same shelf, the card database indicates an association to the shelf (chassis ID). Depending on whether the shelf database has been reset before the card was returned to the shelf, one of the following scenarios results:

- If the system database was NOT reset since the card was removed, the arriving card will be synchronized with the current shelf database and start operating normally.
- If the system database was reset since the card was removed, the arriving card will cause a "Multiple Databases" alarm that indicates that a card is running on a provisioning database that is not the same as that being used by the system.

  Recommended action: Reset the database on the card to discard the card's database and clear the alarm.

Auto Upgrade parameter

The Auto Upgrade parameter indicates whether you want the system to upgrade out-of-revision cards upon arrival. When this parameter is enabled (Y), the system will attempt to bring the new card to the same software version as the Active card, resulting in a downgrade if needed. This process does not require a reboot of the existing card.

1. On the Navigation Tree, click **E7.**
2. Click **System** > **Provisioning** tabs.
3. In the System Provisioning screen, select **Y** (Yes) in the Auto Upgrade list.

ESD ALERT! Beware of electrostatic discharge. Follow standard ESD precautions. Always wear a grounded ESD wristband to avoid damaging the electronic equipment.

To replace an E7 line card

1. If you are replacing the line card with a card of a different type, do one of the following:
   - For replacing an E7-20 GPON-8x with a GPON-4x ensure ONTs are not stranded:
     - Remove any ONT provisioning from ports 5-8 of the OLT, as those ports do not exist on a GPON-4x line card. See *Deleting an ONT from a PON* (on page 113) if necessary.
   - For replacing any other line card with a different card type, delete all the subtending provisioning:
     a. In the Navigation Tree, click **CARD#** to select the card to replace.
     b. From the menu, click **Delete**.
     c. In the dialog box, click the **Forced** checkbox, and then click **Delete**.
2. Disconnect all line interface cables (fibers) and remove all pluggable modules from the card to remove.
3. Remove the line card from the E7 shelf as follows:
   a. On the card faceplate, pull the ejector lever open into the unlocked position to unseat the card.
   b. Carefully slide the card out of the slot, and place it in protective packaging. Return the faulty unit to Calix.
4. Insert a replacement line card into the vacant slot. See "Installing E7 Line Cards" in the *Calix E7 Installation Guide* for detailed instructions.
   - If the card replacement is between E7-20 GPON-4x and GPON-8x cards, an "MEA" alarm appears, as the card provisioning was not deleted and it does not match the provisioned card type. Issue the CLI command **`set card <card number> type gpon-8x (or gpon-4x)`** to clear the alarm.

Note: If you are not installing a replacement card, or no replacement card is available, install a Blank card into the vacant slot.

5. Install pluggable transceiver modules into the card and connect fibers as required. See "Connecting the E7 Line Interfaces" in the *Calix E7 Installation Guide* for detailed instructions.
   - If the card replacement is from an E7-20 GPON-4x to a GPON-8x, enable any of the new OLT ports (5-8) that you want to use, since they default to User-Disabled.
6. If the replacement line card has an earlier software version than the system software, refer to *Upgrading Line Card Software* (on page 107) for instructions on how to upgrade out-of-revision cards on arrival.

For CLI:

```
delete card <card-slot> [forced]
set card <card-slot> type <gpon-8x|gpon-4x>
```

To add an E7 line card

1. On the Navigation Tree, do one of the following:
   - For a standalone system, click **E7**.
   - For a modular chassis system, click **SHELF#** > **SLOT#**.
2. In the menu, click **Create** > **Create Card**.
3. In the Provision dialog box, do the following:
   a. In the Provisioned Type list, select the type of card you will be installing.
   b. In the Admin State list, select whether you want the card enabled.
   c. In the Controller Candidate list, select whether the system will switch to the card to become controller.
   d. Click **OK**.

Note: Alternatively, you can install the card and allow the system to auto-discover it.

For CLI:

```
create card <slot> type <c-type> [controller|admin-state]
```

Performing a Line Card Software Upgrade

This topic describes how to upgrade a single E7 line card from either a network or local software repository. This method is only intended for upgrading out-of-revision cards upon arrival. Performing an entire system upgrade updates the software for the shelf and all cards in the shelf.

Note: Calix strongly recommends that you backup the E7 database before you perform the procedure in this section. Backing up the system database allows you to restore the current network configuration should you experience upgrade difficulties. See Backing Up the System Database for details.

The remote software upgrade process has four main steps:

1. Download the upgrade file from Calix.com and unzip it.
2. Transfer the new software release to the card being upgraded.
3. Reset the card to start operating with the new software.
4. Commit the new card software as the default.

The local software upgrade process has three main steps:

1. Transfer the new software release from the Active card to the card being upgraded.
2. Reset the card to start operating with the new software.
3. Commit the new card software as the default.

Note: During the upgrade, the system raises alarms to indicate the current process. All of these alarms clear when the upgrade process is complete.

Commit or Revert

After the upgrade process has reached the card reset phase, you can choose to either commit the new software release as the default version or revert to the previous software version.

Select the Revert option only if you experience serious upgrade difficulties. See Performing a Software Revert for details.

Auto Upgrade parameter

The Auto Upgrade parameter indicates whether you want the system to upgrade out-of-revision cards upon arrival. When this parameter is enabled (Y), the system will attempt to bring the new card to the same software version as the Active card, resulting in a downgrade if needed.

1. On the Navigation Tree, click **E7.**
2. Click **System** > **Provisioning** tabs.

3. In the System Provisioning screen, select **Y** (Yes) in the Auto Upgrade list.

ALERT! Service affecting procedure. Perform upgrades during a standard maintenance window.

Before starting

- The software files are either transferred to the E7 or located on a remote server. See Performing a Software Upgrade for a procedure on downloading the upgrade files from the Calix website, if necessary.
- The system auto-upgrade must be disabled before the card can be upgraded separate from the E7 system. See Provisioning Basic E7 System Settings.
- You must have an FTP service application installed on your PC to transfer the software release to the E7. An FTP service application is included in the E7 upgrade file, for your convenience.
- The FTP service application must be activated.
- This procedure assumes the following conditions on your PC:
  - Microsoft Windows XP Professional Edition or 2000
  - WinZip application (Start-up configuration set to "Next time start with the Wizard interface")
  - Only one FTP service application is activated. If you are using the FTP server application that is automatically installed with the upgrade software, click C:\CalixESeries\srvconf.exe to ensure the application is active. Also ensure the Windows firewall is configured to allow the exception for the SlimFTPd.exe program (FTP server).

Note: To change the upgrade transfer protocol on the E7, do the following: On the Navigation Tree, click **E7**, and then click **System** > **Provisioning**. In the Upgrade Transfer Protocol drop-down list, select from the available transfer protocols, and then click **Apply**.

To upgrade a card using local software

1. In the Navigation Tree, click a line card.
   - For modular chassis systems, first click a shelf.
2. On the menu, click **Action** > **Upgrade** > **Upgrade Card**.
3. In the Upgrade Card dialog box, do the following:
   a. In the Remote Upgrade list, select **N**.
   b. In the Version box, enter the version of the local software to use for the card upgrade.

      The Running, Committed, and Alternate versions of software are shown in the current work area.

c. In the Force list, indicate whether you want the system to upgrade to the selected file, even if that version is already present on the card.

d. Click **Upgrade Card**.

Wait until an information message indicates the software is ready.

4. Click **Action** > **Upgrade Card** > **Reset Card**, and then Click **Yes** at the prompt.

The card resets and begins using the selected software version.

5. If you want the card to continue using the software upgrade version, click **Action** > **Upgrade Card** > **Commit Card**.

a. In the Commit Card dialog box, select the software version that will become the default software that loads when the card is reset:

- **Running** selects the software version that is currently operating. In this procedure, it is the version that you just transferred and began using with the Reset Card function.
- **Alternate** selects the software version that was previously running on the card.

b. Click **Commit Card**.

6. If you want the card to return to the previous software version, click **Action** > **Upgrade** > **Revert Card**.

a. In the Revert Card dialog box, select the software version that the card reverts to using:

- **Running** selects the software version that is currently operating on the card.
- **Alternate** selects the software version that was previously running on the card.

b. Click **Revert Card**.

7. Either re-open your web browser or clear the cache in your web browser to ensure you are viewing the latest version of the user interface.

For CLI:

```
upgrade card <slot> local version <version ID> [forced] (for standalone
systems)
upgrade card <shelf/card> local version <version ID> [forced] (for modular
chassis systems)
```

To upgrade a card using remote software

1. On the Navigation Tree, click a line card.

- For modular chassis systems, first click a shelf.

2. On the menu, click **Action** > **Upgrade** > **Upgrade Card**.

3. In the Upgrade Card dialog box, do the following if you are using the Calix E-Series File Server application included in the E7 upgrade file:
   a. In the Remote Upgrade list, select **Y**.
   b. In the SFTP/FTP Server box, enter the IP address of your PC.
   c. In the User box, enter the user name for the Calix E-Series File Server application (**upgrade** by default).
   d. In the Password box, enter the password for the Calix E-Series File Server application (**upgrade** by default).
   e. In the Directory Path box, enter the name of the directory that contains the software files. For example, **R01.00.110_EX10_0012**.

   Note: You will find the directory that contains the software files at C:\CalixESeries\software\.

   f. In the Version box, enter the software version that you will be transferring to the E7. (For example, 1.0.99.89.)
   g. In the Force list, indicate whether you want the card to upgrade to the specified version, even if that version is already present on the card.
4. In the Upgrade Card dialog box, do the following if you are using an FTP service application that was previously configured on your PC:
   a. In the Remote Upgrade list, select **Y**.
   b. In the SFTP/FTP Server box, enter the IP address of the file server where the upgrade files are located.
   c. In the User box, enter your user name for the file server.
   d. In the Password box, enter your password for the file server.
   e. In the Directory Path box, enter the path to the top-level directory where the upgrade files are located on the FTP server.
   f. In the Version box, enter the software version that you will be transferring to the E7. (For example, 1.0.99.89.)
   g. In the Force list, indicate whether you want the card to upgrade to the specified version, even if that version is already present on the card.
5. Click **Upgrade Card**.

   Wait until an information message indicates that the software is ready.

   Note: If you suspect that the upgrade process failed, check the upgrade status: On the Navigation Tree, click the line card, and then click **Action** > **Upgrade** > **Upgrade Status**. Also, ensure the FTP software you are using is the only FTP software activated and the Windows firewall configuration is allowing the SlimFTPd.exe program (FTP server).

6. Click **Action** > **Upgrade Card** > **Reset Card**, and then Click **Yes** at the prompt.

The card resets and begins using the selected software version.

7. If you want the card to continue using the software upgrade version, click **Action** > **Upgrade Card** > **Commit Card**.

   a. In the Commit Card dialog box, select the software version that will become the default software that loads when the card is reset:

      - **Running** selects the software version that is currently operating. In this procedure, it is the version that you just transferred and began using with the Reset Card function.
      - **Alternate** selects the software version that was previously running on the card.

   b. Click **Commit Card**.

8. If you want the card to return to the previous software version, click **Action** > **Upgrade** > **Revert Card**.

   a. In the Revert Card dialog box, select the software version that the card reverts to using:

      - **Running** selects the software version that is currently operating on the card.
      - **Alternate** selects the software version that was previously running on the card.

9. Click **Revert Card**.

10. Either re-open your web browser or clear the cache in your web browser to ensure you are viewing the latest version of the user interface.

Note: If it appears that the upgrade process failed, reference the Event Log and Alarm Log to verify and identify the upgrade failure. On the Navigation Tree, click **E7**, and then click **System** > **Logs** > **Event Log**. Check the sequence of Events, and then click **Alarm Log** to check the sequence of Alarms. See "Viewing Alarms and Events" in the *Calix E7 Maintenance and Troubleshooting Guide*.

For CLI:

- **`upgrade card <slot> remote server <ip> user <u-name> directory-path <path> version <version ID> [forced] (for standalone systems)`**
- **`upgrade card <shelf/card> remote server <ip> user <u-name> directory-path <path> version <version ID> [forced] (for modular chassis systems)`**
- **`show upgrade`**
- **`reset card version <version ID> [forced]`**
- **`commit card version <version ID>`**

Examples:

```
upgrade card 1 remote server 192.168.1.1 user ftpuser directory-path /e7code
version 1.0.1.255 forced
```

Switching Control Between Line Cards

This topic describes how to switch system control from the Active card to the standby card. Selecting the Forced option switches the control of the system to the standby card, even if the standby card is not ready. The Active card is the system controller which manages alarms, configuration, and performance monitoring. A "*" is shown next to the card label in the web interface.

To switch system control to the standby card

1. On the Navigation Tree, click **E7**.
2. Click **System** > **Provisioning** > **Action** > **Switch Controller**.
3. Select the Forced checkbox if you want to switch the control to the standby card, even if the standby card is not ready.
4. Click **Yes**.

For CLI:

```
switch controller [forced]
```

Deleting an ONT from a PON

This topic describes how to delete an ONT from an E7 PON system.

The system only allows you to delete an ONT when the provisioning record is not linked to a discovered ONT. You may be required to first delete any service provisioning that exists for that ONT. However, you can use the Forced delete option for the ONT which automatically deletes services and child provisioning. After deleting the ONT from the system, the Global Logical ID for that ONT is then available for re-use.

Note: You can move an ONT to a different PON on the same E7 by unlinking the ONT from a PON, and then linking it to another PON. To unlink all of the ONTs from a GPON card or GPON port, use the **`unlink onts on-gpon-port <card>[/gpon-port]`** command.

To unlink a provisioned ONT from a PON

1. On the Navigation Tree, double-click the **GPON-4** line card and then double-click the **GPON:#** port where the ONT is connected.
2. Click the **ONT:#** that you want to disconnect from the system.
3. From the menu, click **Action** > **Unlink ONT from PON**.

For CLI:

- **`set ont <ont ID> pon-port none`**
- **`unlink onts on-gpon-port <card>[/gpon-port]`**
- **`show ont [details|discovered|discovered on-gpon-port|unassigned]`**

To delete an ONT from a PON

1. Unlink the ONT from the provisioning record as described in the procedure above.
2. On the Navigation Tree, double-click **ONTS**.
3. From the table of ONTs, click the ONT which you want to delete.
4. From the menu, click **Delete**.
5. In the dialog box, click the **Forced** checkbox, and then click **Delete**.

   Note: The Forced action deletes the ONT, even if ports are non-default or services exist. Alternatively, you can remove all associated services before deleting the ONT from a PON.

For CLI:

`delete ont <ont ID> [forced]`

Moving an ONT to a Different PON Port

Physical ONTs can be moved from one port to another port within a node (E7-20, E7-2 standalone or modular chassis), without having to reconfigure services.

To move an ONT to a different PON port

1. Unlink the provisioned ONT from the PON:
   a. On the Navigation Tree, double-click the **GPON-4** line card and then double-click the **GPON:#** port where the ONT is connected.
   b. Click the **ONT:#** that you want to disconnect from the system.
   c. From the menu, click **Action** > **Unlink ONT from PON**.
2. Disconnect the ONT from the current PON port and attach it to the new PON port.

   When the ONT ranges, the E7 will automatically link the ONT provisioning to the ONT.

For CLI:

- `set ont <ont ID> pon-port none`
- `unlink onts on-gpon-port <card>[/gpon-port]`
- `show ont [details|discovered|discovered on-gpon-port|unassigned]`

Replacing an ONT

This topic describes how to replace an ONT with an ONT of the same or different type. Typically, you can preserve the unit's provisioning for the replacement unit.

- If the replacement ONT matches the port descriptions in the provisioning record, modify the ONT record as follows:
  - Set the serial number attribute to match the replacement ONT.
- If the replacement ONT matches the port descriptions in the provisioning record and has additional ports, modify the ONT record as follows:
  - Set the serial number attribute to match the replacement ONT.
  - Select an ONT profile that matches the ONT port configuration.
  - Add services to the new ports.
- If the replacement ONT does not contain all the same ports as the existing provisioning record, delete the existing ONT provisioning, and then create a new provisioning record. See *Deleting an ONT from a PON* (on page 113) and then see "Configuring an ONT" in the *Calix E7 GPON Applications Guide*.
  - Alternatively, delete the existing ONT provisioning that no longer applies or does not match the new ONT, and then modify the provisioning record to include the correct profile and serial number.

Note: You can swap out the ONT at the customer premises before or after changing the ONT serial number in the provisioning record. However, you must unlink the ONT from a provisioning record before you can modify the serial number. If you are using the CLI, use the **`set ont <ont ID> pon-port none`** command. The web interface performs the unlink function with the **Replace** action.

ONT Replacement when operating a RONTA mechanism

To facilitate quick ONT replacement without the use of the E7 management interface or CMS, a technician can use the Registration ID of the failed ONT for the replacement ONT when operating a RONTA mechanism. In the E7, if a Registration ID match is found for a missing ONT, the system will accept the new ONT and update the provisioning record with the serial number of the new ONT. All provisioning associated with the original missing/failed ONT (including ports and services) is sent to the new ONT and service is restored as provisioned.

ONT Software revision

If the software revision of the replacement ONT does not match the E7 software version, the ONT software must be upgraded prior to service activation.

ALERT! This is a service-affecting procedure.

To replace an existing ONT in the system

1. On the Navigation Tree, double-click the **GPON-4** line card and then double-click the **GPON:#** port where the ONT is connected.
2. Click the **ONT:#** that you want to replace.
3. From the menu, click **Action** > **Replace**.
4. In the Replace ONT dialog box, do the following:
   a. In the ONT profile list, select the appropriate default Calix ONT profile or a previously created custom ONT profile.
   b. If the replacement ONT is not a Calix ONT, or you need to create a new ONT profile, see "Configuring an ONT" in the *Calix E7 GPON Applications Guide*.
   c. In the Serial# box, enter the serial number of the replacement ONT.
   d. In the Registration ID box, you can re-use the registration ID from the original ONT installation or enter another value, ensuring the value is unique.
   e. Click **Replace**.

For CLI:

```
set ont <ont ID> [ip-host|rf-avo|profile|serial-number|reg-id|subscriber-
id|description|ont-pwe3-profile|pon-port|admin-state]
```

The ONT to be replaced, must be unlinked from the provisioning record using one of the following commands before you can modify the serial number and link the new ONT to the revised provisioning record.

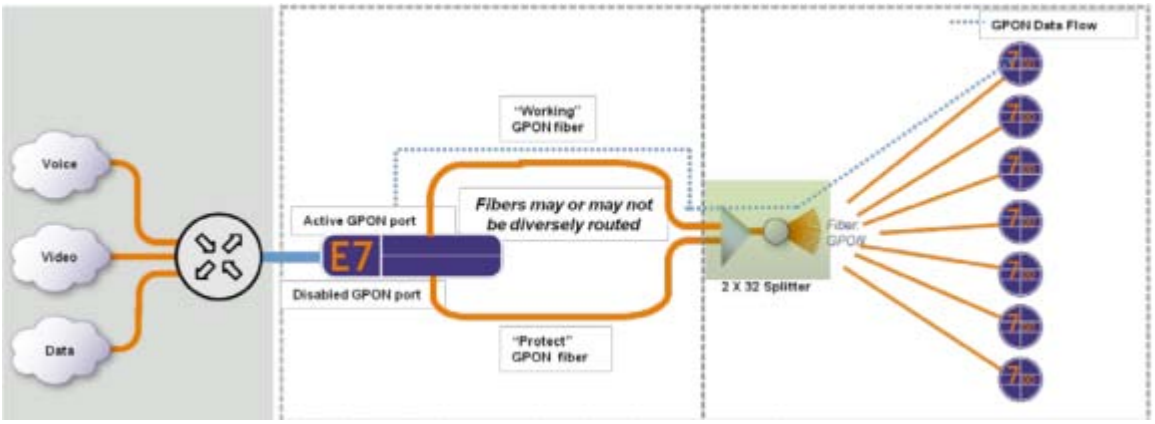
```
set ont <ont ID> pon-port none

unlink onts on-gpon-port <card>[/gpon-port]
```

Protecting PON Equipment

In some applications you may want to protect the GPON equipment and/or fiber facilities. For example, a PON serving high-end residential / resort communities, mobile backhaul services, or business services with strict service level agreements.

The FSAN / ITU has defined the protection types: A, B, and C, providing varying degrees of equipment and fiber protection with increasing levels of equipment redundancy / cost. Type B is shown below and is the most popular. Type B protection uses 2xN splitters and provides feeder fiber protection with no additional PON optical loss, while providing 1:1 GPON OLT equipment protection. In this configuration, two GPON cards provide equipment protection in the same E7 system. In an alternative configuration, the two GPON cards could be in separate E7 systems.



Type B GPON Protection using E7-2 GPON Line Cards

To replace a faulty OLT

1. A "Loss of PON" alarm is raised by the E7 management system (typically within 15 seconds of fault).
2. Disable the failed OLT port or GPON card to ensure that the failure event is not transient.
3. Using the "unlink ONT" command, unlink all ONTs associated with the failed OLT port or GPON card.

   The administrative process of "unlinking" the ONT from the PON allows the ONT database record to go back to an unassigned state where it can be discovered on another PON.
4. Enable the standby OLT port(s). (The standby GPON card should always be enabled.)

   All recently unlinked ONTs will range on the standby OLT ports. Configurations and services will automatically restore as each ONT re-registers with the E7 system. All ONT services should resume in less than 5 minutes.

If an ONT connects to an E7 system that has the ONT's serial number in a pre-provisioned or pre-existing ONT record, the ONT will automatically be linked to the new system and services will resume. Within a single E7 system, the single provisioning record in the database can be associated with any card in the system.

The above operational process requires manual monitoring and intervention to enable the PON protection switch. However, the process could be scripted by an external monitoring system.

Adding a Node to an Existing ERPS Ring

This section describes the process for adding a new E7 node to an existing ERPS ring.

Before starting

Confirm that the following starting conditions are met:

- An ERPS transport ring already exists, with one master node (and network uplink) already configured.
- The ERPS domain name and control VLAN ID are known.
- The service VLAN IDs that are in use are known.
- The new E7 shelf to insert has been installed and powered (but not wired), and configured as follows:
  - The E7 Ethernet port interfaces that you will be using for the node in the ERPS ring are configured as trunk links.
  - The Ethernet ports (all 10GE or GE) that you will be using for the node in the ERPS ring are configured as follows:
    - Duplex = **full**
    - Flow Control = **none**

To add a node to an existing ERPS ring

1. On the Navigation Tree, click **E7**.
2. Click **ERPS** > **Create**.
3. In the Create ERPS Domain dialog box, do the following:
   a. In the Domain Name box, enter the name to assign to the ERPS domain you are creating.
   b. In the ERPS Role list, specify the E7 as a transit node. Only one node in an ERPS domain can be designated as master.
   c. In the Intf 1 (Primary) list, select the Ethernet port interface to assign as Interface 1. The interface is automatically associated with the ERPS domain.
   d. In the Intf 2 (Secondary) list, select the Ethernet port interface to assign as Interface 2. The interface is automatically associated with the ERPS domain.
   e. In the Control VLAN box, enter an ID value to designate a control VLAN. The VLAN is automatically created on the node.
   f. **Note:** Even if no interface is currently using VLAN 1 as the Native VLAN, it is still not available for user provisioning, including use as the ERPS control VLAN.
   g. 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.

h. 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.

i. In the Admin State list, select whether the ERPS domain is in service.

4. Click **Create**.

5. Create the service VLANs on the ring node and add the ERPS domain to each VLAN membership. See "Creating VLAN Memberships" in the *Calix E7 User Guide* for instructions, if necessary.

Note: All nodes in an ERPS ring must have the same IGMP Snooping provisioning on the video VLAN for traffic to flow--either all with snooping (snoop-suppress, proxy) or all without snooping (flood).

6. Set the ring port parameters as follows:

7. Duplex = **full**

8. Flow control = **none**

9. Admin State = **enabled**

10. Insert the new transit node between adjacent nodes in the ERPS ring. For example:

a. Disconnect a cable from the Intf-1 10GE port of an existing node and reconnect it to the Intf-1 10GE port of the new node.

b. Connect a new cable from the Intf-2 10GE port of the new node to the Intf-2 10GE port of the existing node.

Note: A temporary ERPS ring failure will occur that is not service affecting. The master node will enable its secondary port and traffic will continue to flow to all existing nodes as long as the ERPS ring is only broken at one point.

Changing the Role Between ERPS Ring Nodes

This topic describes how to change the Master and Transit role between nodes in an ERPS ring.

To switch roles between ERPS nodes

1. Disable the Secondary ERPS link on the Master node by doing the following:
   a. On the Navigation Tree, double-click the Master node E7 line card that has the Secondary ERPS link, and then click the **GE** or **10GE** port that is the Secondary ERPS link.
   b. In the Admin Status list, select **disabled**.
   c. From the menu, click **Apply**.
2. Change one of the Transit nodes to the Master role, by doing the following:
   a. On the Navigation Tree, click **E7** on the Transit node.
   b. Click **ERPS**, and then click the ERPS domain that you want to edit that is displayed in the table.
   c. In the ERPS Role list, select **master**.
   d. From the menu, click **Apply**.
3. Change the old Master node to a Transit role, by doing the following:
   a. On the Navigation Tree, click **E7** on the old Master node.
   b. Click **ERPS**, and then click the ERPS domain that you want to edit in the displayed table.
   c. In the ERPS Role list, select **transit**.
   d. From the menu, click **Apply**.
4. Re-enable the disconnected ERPS ring port.
   a. On the Navigation Tree, double-click the E7 line card that has the disabled ERPS ring port, and then click the **GE** or **10GE** port that is the disabled ring port.
   b. In the Admin Status list, select **enabled**.
   c. From the menu, click **Apply**.
5. Wait for the changes to settle on a node and the ERPS to stabilize.

For CLI:

- **`set eth-port <port ID> [speed|duplex|flow-ctrl|interface|eth-gos|cos-queue-cfg|bcast-max-rate|unk-mcast-max-rate|dlf-max-rate|lacp-priority|lacp-timeout|admin-state]`**
- **`set erps-domain <domain name> [role|pri-interface|sec-interface|interface-1|interface-2|ctrl-vlan|health-msg-freq|recovery-msg-freq|admin-status]`**

Adding a Shelf to a Modular Chassis System

This topic shows you how to add an E7 shelf to an existing modular chassis system. For instructions on initially configuring a modular chassis system, see "Configuring a Modular Chassis Node" in the *Calix E7 User Guide*.

For instructions on migrating an existing E7 configuration to a modular chassis system, see *Calix Method of Procedure (MOP): Migrating Standalone* E7 *Systems to an* E7 *Modular Chassis*.

Configuration guidelines

Shelves and cards within the Modular Chassis participate in the Control, Network, and Access domains of the system.

- The MCC shelf provides the redundant Control domain for the Modular Chassis and also provides the Network domain connectivity.
- The MCC and MCE shelves span the Access domain to deliver services.
- The MCE shelves only participate in the Access domain. Ethernet interfaces in the Access domain are intended to be tied to the back-office system; part of flow-through service provisioning.

The following guidelines must be adhered to when configuring a modular chassis system:

- A Modular Chassis is managed through a single IP address.
- The MCC must have two-cards defined in it, with exception of the VDSL2-48 Overlay line card which occupies two slots (double-wide) in each individual E7-2 shelf. When the VDSL2-48 card is deployed in the MCC, the MCC will not have a standby controller and is not able to support database redundancy.
- MCE shelves may have one or two cards, as required, where the ports are considered "subscriber ports" and cannot run link protection protocols such as RSTP, LAG, or ERPS.
- When VDSL2-48C line cards are in the MCC and MCE shelves, the cards loose a forward facing SFP+ socket to the chassis' backplane operation. This is not the case with the VDSL2-48 Overlay line card, because it requires no backplane communication to a second card in the same E7-2 chassis.
- Each shelf in the MC is identified by a shelf number, from 1 to 10 where shelf 10 is identified as "0" on the fan-tray assembly and the MCC shelf ID is "1." The shelves may be numbered in any order around the Stacking Ring.
- Any given port or interface in an MC is identified as *shelf/slot/port*.
- One port in each line card in the MCC and MCE shelves is used for the Modular Chassis inter-shelf control path (Stacking Ring).

- The stacking ring can be implemented in one of the following speeds:
  - At 2.5GE rate using SFP sockets when an MC that has only VDSL2 cards
  - At 10GE rate using SFP+ sockets when an MC has either all optical cards or a mix of optical and VDSL2 cards, where the VDSL2 cards are not in the MCC slots
    Note: The stacking ring does not support a 1GE data rate, or a mixed data rate (2.5GE/10GE).
- **For 10GE stacking ring connectivity:**
  - Only E7 10GE ports (SFP+ X3 and X4 ports) may be configured as Stacking Ports. If required by the network design, use 10GE-4 or GPON-4 cards in the shelf that will be designated as the MCC to provide additional 10GE ports for the network uplink or 10GE transport. One Stacking Ring is supported per MC where each shelf has two 10GE stacking ports:
    - For two-card shelves, use port X3 on each line card.
    - For one-card shelves, use ports X3 and X4 on the line card.
  - The X4 port can only be used as the stacking port on the MCC shelf if the backplane links are configured for 10G-A, because 10G-B and 20G use port X4 as a backplane port.
  - A Calix 10GE Direct Attach copper cable must be used for stacking port connections.
- **For 2.5GE stacking ring connectivity:**
  - When the MCC has VDSL2 card(s) installed and they must provide a 10GE port for a transport ring interface or uplink, a 2.5GE stacking ring is required.
  - The E7-2 supports 2.5 Gbps pluggable module interfaces in the SFP ports of the VDSL2-48C and VDSL2-48 cards.
  - For 2.5GE stacking rings, the default stacking interfaces on VDSL2 Linecards will be the first SFP interface designated as "G1". For a single VDSL2 Linecard, the Secondary Default Stacking port will be the second SFP interface designated as "G2."
  - A Calix 2.5GE Direct Attach copper cable must be used for stacking port connections.
  - Although the GPON-4 and 10GE-4 cards support 2.5GE modules in the SFP sockets, including the use of Direct Attach cables, these ports cannot be used for stacking rings.
- All network connections (ERPS, RSTP, LAG, DHC servers, multicast routers, IGMP-enabled video servers, network-facing routers) are made on the Modular Chassis Controller (MCC) shelf.
- All outer VLANs for each service defined on the MC are automatically added to the Stacking Ring domain.
- To retain the E7 IP address for the MCC upon resetting the database, use the "keep-craft-fe" option.

- The Stacking Ring must be a closed ring during normal operations.
- Port mirroring source and destination ports must be on the same E7 line card.
- Split Horizon is only enforced between ports on the same line card.
- An E7-2 MC may form an RSTP Node Protection pair with another E7-2 MC, a standalone E7, or an E5-400.
- An IGMP Querier (multicast source) connection to an MCE port is not supported.
- A complete copy of the provisioning database is maintained on every card within the MC, providing full redundancy across all shelves.
- An MCE shelf establishes communications with the MCC over the stacking ring when the following conditions are met:
  - The MCE is provisioned through shelf creation at the MCC.
  - A Calix-brand Direct Attach copper cable is connected.
- The Craft FE ports can be enabled and configured on MCC shelves, however, the Craft FE ports on MCE shelves are disabled when MCE shelves are in communication with an MCC shelf. If MCE shelves lose communication with the MCC shelf, the Craft FE ports on the MCE shelves become enabled.
- The E7 uses the First Reserved VLAN ID for the stacking ring control VLAN, as configured in the system settings (the default is 1002). Changing this value after a stacking ring has been configured is service affecting for subscribers in the MCE shelves.
- The MCE shelf is used for GE and GPON subscriber port expansion.
- Access Domain Ethernet interface parameters (MCE shelves):
  - The Ethernet interface Role parameter is limited to Access.
  - The DHCP Trust parameter is limited to disabled or N (untrusted).
  - Split Horizon Forwarding parameter is disabled.
  - The BPDU Guard parameter is enabled, by default.
  - The Native VLAN is not supported, however tag actions can be used to match untagged traffic to a VLAN ID.
  - The MCE Ethernet interfaces cannot be designated as a VLAN Router Interface. That is, a static multicast router ('mrouter') interface is not supported as a multicast destination on MCE shelves. Multicast routers are not allowed to source multicast traffic into the network on an Access domain Ethernet port.

Interface role configuration guidelines

	Trunk	Edge	Access
E7-2 MCC	X	X	X
E7-2 MCE			X
Tag Actions		X	X
Native VLAN	X	X	
Networking Protocol (RSTP, ERPS*, LAG)	X	X	

*Edge ports only support RSTP and LAG networking protocols, NOT ERPS.

Before starting

Before starting the procedure below, ensure that the following conditions exist:

- All E7s are running software version R1.2, or later.
- The databases have been backed up for all shelves to be added to a modular chassis, if necessary.
- The existing provisioning on each shelf is retrieved and recorded, if necessary. Any existing provisioning on the shelves will be lost at being added to an MC and should be captured for re-provisioning on the MCC, if necessary.

To add an expansion shelf to a modular chassis system

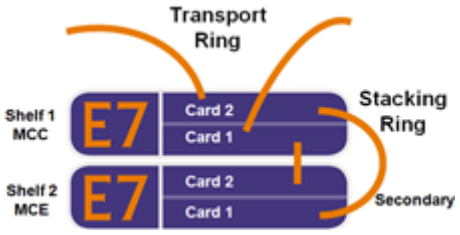
1. Ensure that the cards in the shelf to be installed are in a factory default state.
2. Login to the modular chassis controller.
3. On the Navigation Tree, click **E7**.
4. In the work area, click **System**.
5. In the menu, click **Action** > **Shelf Management** > **Add Shelf**.
6. In the Add Shelf dialog box, do the following:
   a. In the Shelf ID list, select the ID to assign to the shelf, creating a database record.
   b. In the Admin State list, leave the default of **enabled**.
   c. In the Serial Number box, enter the serial number for the shelf that you are installing if you want to prevent any shelf other than the one specified from being accepted by the MCC. Otherwise, leave the value blank for the next shelf connected to the MCC to be accepted. Then, the shelf serial number will be automatically added to the database when the shelf is connected to the MC.
   d. In the Backplane Link list, leave the default setting if two cards are to be installed in the shelf. If the expansion shelf will have only one line card installed and an additional external port is needed, select **none**.
   e. In the Power Monitor Mode list, leave the default setting.

f. In the Card 1 and Card 2 lists, select the type of card that is installed in each slot of the expansion shelf to be added to the MC.

g. In the Stacking Port 1 and Stacking Port 2 lists, leave the default Ethernet ports assigned for each stacking port, if two cards are defined in the shelf. By default, the X3 port on each card is assigned as a stacking port. If there is only one card installed in the shelf, the ports X3 and X4 on the line card must be assigned as the stacking ports.

h. Click **Add**.

7. Connect the MCE shelf stacking ports to MC stacking ports through Calix Direct Attach copper cables.



Connect:

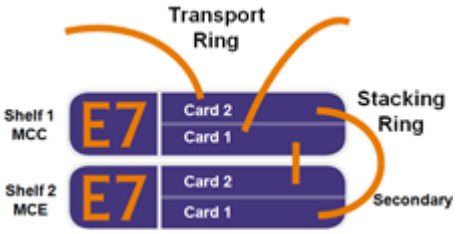
Primary - 1/1/X3 to 2/2/X3

Secondary - 1/2/X3 to 2/1/X3

8. Wait for the "Shelf Ring Port Down" and "Unequipped" alarms to clear.

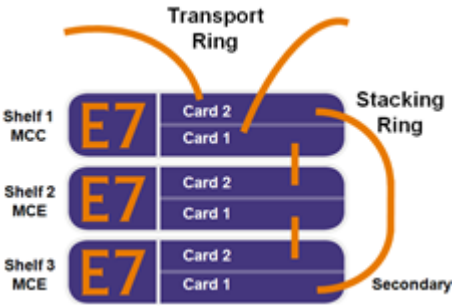
9. Repeat Step 1 through Step 8 to add more MCEs to the MC node. When reconfiguring the stacking port connections to add a shelf to the MC, break the ring at the MCC stacking port 2 (blocking port) to avoid disrupting the communication among the shelves already connected in the stacking ring. For the example configuration in this procedure, the MCC stacking port 2 is 1/2/X3.

Example of stacking port connections



Connect:

- Primary - 1/1/X3 to 2/2/X3
- Secondary - 1/2/X3 to 2/1/X3



Disconnect:

- Secondary - 1/2/X3 to 2/1/X3

Connect:

- Primary - 2/1/X3 to 3/2/X3
- Secondary - 1/2/X3 to 3/1/X3

For CLI:

- **reset database**
- **create shelf <shelf-id>**
- **set shelf <shelf-id> [serial-number]**

Deleting a Shelf from a Modular Chassis System

This topic describes how to delete a Modular Chassis Expansion (MCE) shelf from a Modular Chassis (MC) node.

After deleting the shelf from the system, the Shelf ID is then available for re-use.

Before starting

Before starting the procedure below, check that the following conditions are met:

- All service provisioning is deleted from the shelf.
- All subtended network elements are deleted from the shelf. See *Deleting an ONT from a PON* (on page 113), if necessary.

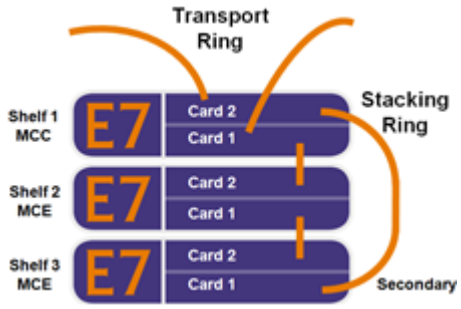
To remove an expansion shelf from a modular chassis node

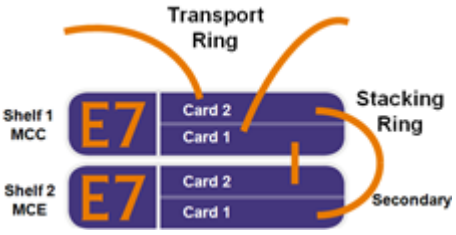
1. On the Navigation Tree, double-click the shelf that you want to delete, and then click **CARD 1**.
2. From the menu, click **Delete**.
3. In the Delete dialog box, click **Delete**.
4. Repeat Step 1 through Step 3, selecting **CARD 2** from the shelf.
5. On the Navigation Tree, click the shelf that you want to delete.
6. From the menu, click **Delete**.
7. In the Delete dialog box, click **Delete**.

   Note: The Forced delete option for the shelf automatically deletes services and child provisioning.

8. Disconnect all line interface cables (fibers) and Stacking Port cable connections from the deleted shelf.
9. Reconfigure the MC Stacking Ports connections, and then wait for the "Shelf Ring Port Down" and "Unequipped" alarms to clear.

Example of stacking port connections





Disconnect:

- Primary - 2/1/X3 to 3/2/X3
- Secondary - 1/2/X3 to 3/1/X3

Connect:

- Primary - 1/1/X3 to 2/2/X3
- Secondary - 1/2/X3 to 2/1/X3

For CLI:

- **`delete ont <ont ID> [forced]`**
- **`delete card <card-slot> [forced]`**
- **`delete shelf <shelf-id> [forced]`**

Converting the Speed of a Modular Chassis Stacking Ring

This topic shows you how to convert the speed for one port in each line card in the MCC and MCE shelves that is used for the Modular Chassis inter-shelf control path (Stacking Ring). The Stacking Ring must be a closed ring during normal operations, yet in a maintenance window, you can disconnect the cables and specify different stacking ring ports without deleting all of the Modular Chassis Expansion (MCE) shelf provisioning.

The stacking ring can be implemented in one of the following speeds:

- At 2.5GE rate using SFP sockets when an MC that has only VDSL2 cards
- At 10GE rate using SFP+ sockets when an MC has either all optical cards or a mix of optical and VDSL2 cards, where the VDSL2 cards are not in the MCC slots

Note: The stacking ring does not support a 1GE data rate, or a mixed data rate (2.5GE/10GE).

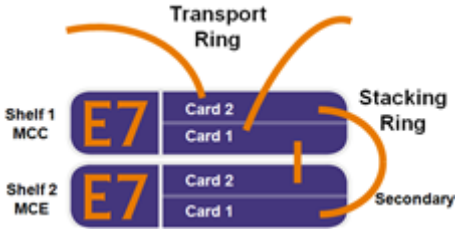
- **For 2.5GE stacking ring connectivity:**
  - When the MCC has VDSL2 card(s) installed and they must provide a 10GE port for a transport ring interface or uplink, a 2.5GE stacking ring is required.
  - The E7-2 supports 2.5 Gbps pluggable module interfaces in the SFP ports of the VDSL2-48C and VDSL2-48 cards.
  - For 2.5GE stacking rings, the default stacking interfaces on VDSL2 Linecards will be the first SFP interface designated as "G1". For a single VDSL2 Linecard, the Secondary Default Stacking port will be the second SFP interface designated as "G2."
  - A Calix 2.5GE Direct Attach copper cable must be used for stacking port connections.
  - Although the GPON-4 and 10GE-4 cards support 2.5GE modules in the SFP sockets, including the use of Direct Attach cables, these ports cannot be used for stacking rings.
- **For 10GE stacking ring connectivity:**
  - Only E7 10GE ports (SFP+ X3 and X4 ports) may be configured as Stacking Ports. If required by the network design, use 10GE-4 or GPON-4 cards in the shelf that will be designated as the MCC to provide additional 10GE ports for the network uplink or 10GE transport. One Stacking Ring is supported per MC where each shelf has two 10GE stacking ports:
    - For two-card shelves, use port X3 on each line card.
    - For one-card shelves, use ports X3 and X4 on the line card.
  - The X4 port can only be used as the stacking port on the MCC shelf if the backplane links are configured for 10G-A, because 10G-B and 20G use port X4 as a backplane port.

- A Calix 10GE Direct Attach copper cable must be used for stacking port connections.

To convert the speed of a modular chassis stacking ring

1. In the Navigation Tree, click the MCE shelf with the highest shelf number (2-10).
2. In the Work Area Shelf # form, specify the Ethernet ports that are assigned as Stacking Port 1 and Stacking Port 2.
   - For 2.5GE stacking rings, typically the stacking interfaces on VDSL2 Linecards will be the first SFP interfaces designated as "GE 1". For a single VDSL2 linecard, stacking port 2 will be the second SFP interface designated as "GE 2."
   - For 10GE stacking rings, typically the X3 port on each card is assigned as the stacking port.
3. In the toolbar, click **Apply**.

   Note: As each MCE shelf is converted, it loses connectivity with the MCC, until the MCC is converted and all MC shelves have a common port speed.
4. In the Navigation Tree, click the MCE shelf with the next highest shelf number (2-9).
5. Repeat Steps 2, 3, and 4 for the remaining shelves in the MC system, including the MCC shelf (shelf 1).
6. Connect the Calix Direct Attach copper cables of the correct speed (10GE or 2.5GE) between the new stacking ports:
   - Attach a cable between card 1 stacking port of each shelf to card 2 stacking port of the following shelf.
   - Complete the stacking ring connections by attaching a cable between card 1 stacking port of the last shelf to card 2 stacking port of the MCC shelf.



7. After the reconfiguration is complete, wait for the "Shelf Ring Port Down" and "Unequipped" alarms to clear.

CLI:

```
set shelf <shelf-id> stacking-port-1 <shelf/card/port> stacking-
port-2 <shelf/card/port>
```

Replacing a Faulty Shelf

This topic shows you how to replace a faulty E7 shelf from the following configurations:

- Standalone E7 shelf
- Modular Chassis Expansion (MCE) shelf
- Modular Chassis Controller (MCC) shelf

To replace a standalone E7 shelf

1. Move the line cards from the faulty shelf to a replacement shelf.
2. Start up the replacement shelf and allow the cards to start up and revert to the default (empty) database.
3. Retrieve a recent database backup for the faulty shelf and restore the database to the replacement shelf, using the "Forced" option. See *Restoring a Backup Database* (on page 148) for instructions.
4. All subscriber services that were provisioned on the faulty shelf are now provisioned on the replacement shelf.
5. Make all connections previously configured on the faulty shelf.

For CLI:

```
load backup from-host <server ID> user <user name> file-path <path>
switch database [forced]
```

To replace an E7 modular chassis expansion shelf

1. Set the shelf serial number to zero, as follows:

   On the Navigation Tree, click **Shelf#**, and then in the Shelf # form, enter **0** and click **Apply** in the menu.
2. Move the line cards from the faulty shelf to a replacement shelf that has no power applied.
3. Start up the replacement shelf and allow the cards to start up and revert to the default (empty) database.
4. Make stacking port connections between the replacement shelf and the MC, using Calix Direct Attach copper cables.
5. Wait for the alarms to clear.
6. All subscriber services that were provisioned on the faulty shelf are now provisioned on the replacement shelf.
7. Make all connections previously configured on the faulty shelf.

For CLI:

```
set shelf <shelf-id> [serial-number]
load backup from-host <server ID> user <user name> file-path <path>
switch database [forced]
```

To replace an E7 modular chassis controller shelf

1. Move the line cards from the faulty shelf to a replacement shelf that has no power applied.
2. Start up the replacement shelf and allow the cards to start up and revert to the default (empty) database.
3. Retrieve a recent database backup for the MC and restore the database to the replacement MCC shelf, using the "Forced" option. See *Restoring a Backup Database* (on page 148) for instructions.
4. Make stacking port connections between the replacement shelf and the MC, using Calix Direct Attach copper cables.
5. Wait for the alarms to clear.
6. All provisioning on the faulty shelf is now on the replacement shelf.
7. Make all connections previously configured on the faulty shelf.

For CLI:

```
load backup from-host <server ID> user <user name> file-path <path>
switch database [forced]
```

Chapter 3

Troubleshooting

This chapter includes information on how to discover potential E7 problems and possible corrective actions. For more information, contact the Calix Technical Assistance Center (TAC). www.calix.com, 877-766-3500, 707-766-3500

Topics Covered

This chapter covers the following sets of topics:

- In-band management system lockout
- Degraded status
- Log in connection
- Abort script
- User password
- Changing the management gateway or management IP
- SNMP communication
- Network connection to host
- Recovering a database or software revision
- Extracting diagnostics
- Resetting the system or line card database
- Recovering from a system lockout
- Line testing POTS port services
- Adding an ONT to quarantine
- Troubleshooting a system connection or a TrapRegFailed alarm
- Manually disconnecting and connecting a system node

Resetting, Restarting, and Rebooting Equipment

This section describes how to reset some equipment to default settings or to the current settings. Other equipment can be restarted or rebooted.

Resetting the System or Card

This topic shows you how to reset the system or line card which allows you to choose to run a software version other than the committed version. For example, after you transferred an alternate version of the software to the E7 system using the Upgrade System operation, that software version will be selectable from the Reset System Action dialog box. For instructions on upgrading the system software, see the *Calix E7 Software Upgrade Guide*.

Note: A reset operation does not affect the version of the default (committed) software.

To reset the E7 system

1. On the Navigation Tree, click **E7**.
2. Click **System** > **Provisioning** > **Action** > **Upgrade** > **Reset System**.
3. In the Reset System Action dialog box, do the following:
   a. Select the software version that you want to run.
   b. Select whether to force the system to run the selected software version, even if the currently running software is more recent than the specified version.
   c. Click **Reset System**.

For CLI:

```
reset system version <version id> [forced]
```

To reset an E7 line card

1. On the Navigation Tree, click a line card.
2. On the menu, click **Action** > **Upgrade** > **Reset Card**.
3. In the Reset Card dialog box, do the following:
   a. Select the software version that you want to run.
   b. Select whether to force the system to run the selected software version, even if the currently running software is more recent than the specified version.
   c. Click **Reset Card**.

For CLI:

- `reset card <slot> version <version id> [forced] (for standalone systems)`
- `reset card <shelf/card> version <version id> [forced] (for modular chassis systems)`

Resetting the System or Line Card Database to Factory Defaults

Use this function to clear the following device configuration information and return the system or line card to the factory defaults.

- Completely erases internal database
- Removes all provisioning
- Use with extreme caution
- Can be done at the E7 node level or individual card level
- IP addresses can remain persistent if desired

For CLI, use the **`keep-craft-fe`** version of the command to keep the system configuration of enabled craft-fe interfaces and global access settings.

Note: Upon resetting the database of a two-card E7 system, only the line card that has the system controller status is discovered by the E7, until provisioning occurs.

CAUTION! Performing a Reset Database action *replaces all provisioning to default values*. This includes disabling the CLI telnet and setting the IP address back to the default and setting the HTTP to secure, requiring https:// in the login.

Warning: Restoring the default configuration deletes all the current settings. Calix strongly recommends that you back up the configuration file before restoring the default configuration.

To restore the system default database

1. On the Navigation Tree, click **E7**.
2. Click **System** > **Provisioning** > **Action** > **Reset Database**.
3. Click the Yes checkbox if you want the Craft port IP setting to survive the database reset operation.
4. Click **Reset Database**.

   Note: The system restarts once the defaults are restored.

5. If you did not select the Yes checkbox and you want to access the E7 again, you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1).

For CLI:

```
reset database [keep-craft-fe]
```

To restore the line card default database

1. On the Navigation Tree, click a line card.
2. On the menu, click **Action** > **Reset Database**.
3. Click the checkbox if you want to keep the craft port IP setting.
4. Click **Reset Database**.

For CLI:

```
reset database card <slot>
```

Rebooting the System or a Line Card

This topic shows you how to reboot the E7 system or a line card in a standalone system and in a modular chassis system.

Note: A reboot operation does not affect the version of the software that is running on the system or card.

To reboot the E7 system or modular chassis shelf

1. On the Navigation Tree, click **E7**.
   - To reboot a modular chassis shelf, click the shelf of interest.
2. Click **System** > **Provisioning** > **Action** > **Reboot**.

For CLI:

```
reboot [system]
```

To reboot an E7 line card

1. On the Navigation Tree, click a line card.
   - For modular chassis systems, first click the shelf where the line card is located.
2. On the menu, click **Action** > **Reboot**.

For CLI:

```
reboot card <slot> (for standalone systems)
reboot card <shelf/card> (for modular chassis systems)
```

Resetting an ONT

This topic shows you how to reset the specified ONT, causing it to restart, re-range, and be discovered.

To reset an ONT

1. On the Navigation Tree, click **ONTs**.
2. In the Workarea, click **Provisioned ONTs** > **Provisioning**.
3. In the table of ONTs, double-click the row with the ONT that you want to reset.
4. In the menu, click **Action** > **Reset ONT**, and then click **reset ONT** to indicate that you want to proceed with the action.

For CLI:

```
reset ont <ONT ID>
reset ont <serial number>
```

Resetting an ONT to the Factory Default

The E7 GPON ONT buttset master reset procedure returns the ONT settings to the factory default.

To reset the ONT to factory default

1. Disconnect power to the ONT.
2. Disconnect the network fiber (pigtail) from the ONT.
3. Connect an RJ-11 terminated buttset to the first (LINE ONE) voice port on the ONT.

   Note: For buttset devices using alligator clips, back-out the Tip and Ring screws and clip the buttset leads to the T and R posts (black to Tip, red to Ring).Verify that the network fiber is disconnected from the ONT.

4. Reapply power to the ONT.
5. For 700G or 700GX ONTs, listen to the buttset and wait until you hear a click sound (approximately 10 seconds for SFU ONTs or 15-20 seconds for MDU ONTs).
6. For 700GE ONTs, wait for the OFF HOOK LED on the ONT to start blinking (approximately 50 seconds for 2 POTS ONTs, 60 seconds for 4 POTS ONTs).

   Note: If digits are entered prior to the ONT being ready (click sound or OFF HOOK Blink), those digits are ignored.

7. Press **"*", "*", "*"** and **"#"** (star, star, star, pound) keys on the buttset key pad. The buttset sounds DTMF tones as the keys are pressed.

8. A voice prompts to acknowledge your selection of requesting an ONT master reset.
9. After the confirmation prompt, press **'1'** to confirm the reset. A voice prompt replies, "ONT Master Reset is completed".
10. Press **'0'** to abort. A voice prompt replies, "ONT Master Reset is cancelled".
11. Continue entering new RONTA commands as required.
12. Re-connect the network fiber to the ONT and wait for the ONT to come on line.

Resetting an xDSL Port Parameters

This topic shows you how to reset an xDSL port on a VDSL2 line card, causing all of the port parameters to return to default values.

To reset an xDSL port

1. On the E7 Navigation Tree, click **Shelf#** > **Card#** > **xDSL#**.
2. In the Workarea, click **Port > Provisioning > Basic**.
3. In the toolbar, click **Action** > **Reset to Default**, and then **Yes** to return the xDSL port to default settings.
4. Click **Apply**.

For CLI:

```
reset dsl-port <port>
```

- **For stand-alone E7-2**, DSL ports are specified by card, port type, and port number. For example: 1/v1.
- **For modular chassis E7-2**, DSL ports are specified by shelf, card, port type, and port number. For example: 1/2/v4.

Restarting a SIP Service on an ONT Port

This topic shows you how to restart a SIP service on a specified Voice port on a GPON ONT, causing the service to re-read the remote configuration file.

To reset a SIP service on an ONT Voice port

1. On the E7 Navigation Tree, click **ONTs**.
2. In the Work Area, click **Provisioned ONTs** > **Services Table**.
3. In the toolbar, select the ONT ID from the drop-down list, and then click **Refresh.**
4. From the table of provisioned services for the ONT, select the SIP service that you want to restart.

5. In the toolbar, click **Action** > **Restart SIP Service**.
6. Click **Apply**.

Syntax:

```
restart ont-port <p-id> sip-svc
```

- **For stand-alone E7-2**, ONT ports are specified by ont-id/ont port number. For example: 1001/p1.
- **For modular chassis E7-2**, DSL ports are specified by shelf, card, port type, and port number. For example: 1/1001/p2.

Restarting a SIP Service on an xDSL Voice Port

This topic shows you the CLI command to use for restarting a SIP service that is provisioned on a VDSL2 card POTS (Voice) port.

```
restart pots-port <port> sip-svc
```

- **For stand-alone E7-2**, POTS ports are specified by card/pots-port number. For example: 2/4.
- **For modular chassis E7-2**, POTS ports are specified by shelf/card/pots-port number. For example: 1/2/4.

Restarting a SIP Remote Configuration Profile

This topic shows you how to restart a SIP remote configuration profile that is assigned to an xDSL port service, causing a restart for system components using the SIP remote configuration profile.

To restart a SIP remote configuration profile

1. On the E7 Navigation Tree, click **Shelf#** > **Card#** > **xDSL#**.
2. In the Workarea, click **Port > Provisioning > Basic**.
3. In the toolbar, click **Action** > **Reset to Default**, and then **Yes** to return the xDSL port to default settings.
4. Click **Apply**.

For CLI:

```
restart dsl-port <port>
```

- **For stand-alone E7-2**, DSL ports are specified by card, port type, and port number. For example: 2/v4.
- **For modular chassis E7-2**, DSL ports are specified by shelf, card, port type, and port number. For example: 1/2/v4.

Recovering the Software

This topic describes how to perform a software revert. A software revert uses the previous software version. New provisioning is not retained, and must be reprovisioned after performing a revert.

To revert to the previous system software version via the CMS or web interface

1. On the Navigation Tree, click **E7**.
2. Click **System** > **Provisioning** > **Action** > **Upgrade** > **Revert System**.
3. In the Revert System Action dialog box, select the software version that the system reverts to using:
   - **Running** selects the software version that is currently operating on the system.
   - **Alternate** selects the software version that was previously running on the system.
4. Click **Revert System**.

Note: You can look at the current Upgrade Status to verify the result of the upgrade process. Click **System** > **Provisioning** > **Upgrade** > **Upgrade Status**.

Note: If it appears that the revert process failed, reference the Event Log and Alarm Log to verify and identify the upgrade failure. See "Viewing Alarms and Events" in the *Calix E7 Maintenance and Troubleshooting Guide*.

For CLI:

- `revert system version <version ID>`
- `show upgrade`

Note: If you suspect that the software revert process failed, use the `show log alarm` command and the `show log event` command to verify and identify the failure.

To revert to a previous version of card software

1. On the Navigation Tree, click a service card.
2. In the menu, click **Action** > **Upgrade** > **Revert Card**.
3. In the Revert Card dialog box, select the software version that the card reverts to using:
   - **Running** selects the software version that is currently operating on the card.
   - **Alternate** selects the software version that was previously running on the card.
4. Click **Revert Card**.

Note: You can look at the current Upgrade Status to verify the result of the upgrade process. Click **Action** > **Upgrade** > **Upgrade Status**.

Note: If it appears that the revert process failed, reference the Event Log and Alarm Log to verify and identify the upgrade failure. See "Viewing Alarms and Events" in the *Calix E7 Maintenance and Troubleshooting Guide*.

For CLI:

- **`revert card <slot> version <version ID>`**
- **`show upgrade`**

Note: If you suspect that the software revert process failed, use the **`show log alarm`** command and the **`show log event`** command to verify and identify the failure.

Recovering a Database

Use the Backup and Restore utility to retrieve a backup copy of the database from a remote FTP or SFTP server and store it on the E7's inactive image. You can then restore the database, where the backup copy becomes the active database on the system.

A configuration database relates to a specific E7 chassis (backplane or modular chassis) and specific card(s) provisioning. Each card in the system has a copy of the database.

CAUTION! Restoring a database *replaces all provisioning in the E7 with the values in the restored database*. This includes replacing the E7 IP address with the restored database setting, requiring you to know what that address is to be able to login to the E7 after the database restore.

Note: Calix strongly recommends that you backup the E7 database before you perform the procedure in this topic.

Basic steps to restore a backup copy of the provisioning database:

1. Retrieve the backup database file from a remote server and load it onto the E7's inactive image.
2. Switch from the current database to the backup version.

When a faulty shelf needs replacement:

a. Retrieve a recent database backup for the faulty shelf.

b. Move the line cards to a new shelf.

c. Allow the cards to start up and revert to the default (empty) database.

d. Restore the database on the new shelf with the **Forced** switch parameter selected.

Before starting

- You must have an FTP service application installed on your PC to transfer the backup file to the E7. An FTP service application is included in the E7 upgrade file, for your convenience.
- Ensure that only one FTP service application is activated. If you are using the FTP server application that is automatically installed with the upgrade software, click **C:\CalixESeries\srvconf.exe** to ensure the application is active. Also ensure the Windows firewall is configured to allow the exception for the SlimFTPd.exe program (FTP server).The FTP service application must be activated.

Windows FTP Service Application

You can use the provided FTP service application to simplify an E7 database backup and restore from your PC. Or, you can use a previously-installed FTP service application on your PC to perform the backup process.

If you choose to automatically install the E7 upgrade file on your PC, the installation includes creating the following directories and installing the Calix E-Series file server:

- **C:\CalixESeries\software** contains the software release
- **C:\CalixESeries\backup** receives the extracted system database
- **C:\CalixESeries\srvconf.exe** opens the Calix E-Series File Server control panel

The following usernames, passwords, and FTP server port are associated with the automatically installed Windows FTP service application:

- **upgrade** is the Upgrade username
- **upgrade** is the Upgrade password
- **backup** is the Backup and Restore username
- **backup** is the Backup and Restore password
- **21** is the FTP server port

Note: You can change the usernames, passwords, and FTP server port by double-clicking **C:\CalixESeries\srvconf.exe** in a Windows Explorer application, which opens the Calix E-Series File Server control panel.

Parameters for loading a backup database

You can provision the following parameters for a database restore:

Parameter	Description	Valid Options
FTP Server IP*	IP address of backup server.	String 31 characters, or "dotted quad" format. For example: "192.168.1.100."
User*	User name on backup server.	String 31 characters
Password*	Password for user name on backup server.	String 31 characters
File Path*	Path to backup directory server.	String 31 characters

* Required fields

To restore a backup database

1. On the Navigation Tree, click **E7**.
2. Click **System** > **Provisioning** > **Action** > **Backup/Restore**.
3. Select **Load** to retrieve a previously archived database backup file.
4. In the Load DB Backup dialog box, do the following:
   a. In the SFTP/FTP Server IP box, type the IP address of the FTP server where the backup file is located.
   b. In the User box, type your user name to log in to the file server.
      - If you are using the Calix E-Series file server, the default user name is **backup**.

c. In the Password box, type your password to log in to the file server.

- If you are using the Calix E-Series file server, the default user name is **backup**.

d. In the File Path box, type the path to the directory where the backup file is located and the file name.

- If you are using the Calix E-Series file server, the FTP server is configured to look for the database backup file in the C:\CalixESeries\backup directory.

5. Click **Load**.
6. Click **Action** > **Backup/Restore** > **Switch** to restore the retrieved database file.
7. In the Switch DB Backup dialog box, select whether to force the switch to the retrieved database file and then click **Switch**.

Note: The **Yes** setting forces the E7 to replace the database with the currently retrieved database file, even if the file was generated on another E7 system.

CAUTION! The E7 system reboots as part of the database-restore process.

8. After the system comes up, perform a system reset.

a. In the Navigation Tree, click **E7**.

b. In the Workarea, click **System** > **Provisioning** > **Action** > **Upgrade** > **Reset System**.

To restore a backup database using CLI

1. Retrieve a previously archived database backup file from a specified file server.

```
load backup from-host <server ID> user <user name> file-path <path>
```

- Example for Calix E-Series File Server application (included in the E7 upgrade file):

```
load backup from-host 192.168.1.1 user backup file-path LAB_2009-08-
01_14_35_02.provdb
```

Note: The Calix E-Series FTP server is configured to look for the database backup file in the C:\CalixESeries\backup directory.

- Example for an FTP service application (previously configured on your PC):

```
load backup from-host 192.168.1.1 user jsmith file-path /e7/LAB_2009-08-
01_14_35_02.provdb
```

Note: When restoring an E7 backup database file from a Windows-based server, use a forward slash (/) as a path separation character when working with FTP application operations. The E7 interprets any backslash in the path string as part of the filename.

2. Switch the database to the file that you just downloaded, resetting the system to operate with the provisioning in the downloaded database.

```
switch database [forced]
```

Note: Using the "forced" option, switches the database, replacing the current database with the database backup retrieved with the "load backup" command, even if the backup file was generated on another system.

3. After performing a database restore, the system must be allowed to come up, and then you must reset the entire system.

```
reset system
```

Restoring a Backup Database

Use the Backup and Restore utility to retrieve a backup copy of the database from a remote FTP or SFTP server and store it on the E7's inactive image. You can then restore the database, where the backup copy becomes the active database on the system.

A configuration database relates to a specific E7 chassis (backplane or modular chassis) and specific card(s) provisioning. Each card in the system has a copy of the database.

CAUTION! Restoring a database *replaces all provisioning in the E7 with the values in the restored database*. This includes replacing the E7 IP address with the restored database setting, requiring you to know what that address is to be able to login to the E7 after the database restore.

Note: Calix strongly recommends that you backup the E7 database before you perform the procedure in this topic.

Basic steps to restore a backup copy of the provisioning database:

1. Retrieve the backup database file from a remote server and load it onto the E7's inactive image.
2. Switch from the current database to the backup version.

When a faulty shelf needs replacement:

a. Retrieve a recent database backup for the faulty shelf.

b. Move the line cards to a new shelf.

c. Allow the cards to start up and revert to the default (empty) database.

d. Restore the database on the new shelf with the **Forced** switch parameter selected.

Before starting

- You must have an FTP service application installed on your PC to transfer the backup file to the E7. An FTP service application is included in the E7 upgrade file, for your convenience.
- Ensure that only one FTP service application is activated. If you are using the FTP server application that is automatically installed with the upgrade software, click **C:\CalixESeries\srvconf.exe** to ensure the application is active. Also ensure the Windows firewall is configured to allow the exception for the SlimFTPd.exe program (FTP server).The FTP service application must be activated.

Windows FTP Service Application

You can use the provided FTP service application to simplify an E7 database backup and restore from your PC. Or, you can use a previously-installed FTP service application on your PC to perform the backup process.

If you choose to automatically install the E7 upgrade file on your PC, the installation includes creating the following directories and installing the Calix E-Series file server:

- **C:\CalixESeries\software** contains the software release
- **C:\CalixESeries\backup** receives the extracted system database
- **C:\CalixESeries\srvconf.exe** opens the Calix E-Series File Server control panel

The following usernames, passwords, and FTP server port are associated with the automatically installed Windows FTP service application:

- **upgrade** is the Upgrade username
- **upgrade** is the Upgrade password
- **backup** is the Backup and Restore username
- **backup** is the Backup and Restore password
- **21** is the FTP server port

Note: You can change the usernames, passwords, and FTP server port by double-clicking **C:\CalixESeries\srvconf.exe** in a Windows Explorer application, which opens the Calix E-Series File Server control panel.

Parameters for loading a backup database

You can provision the following parameters for a database restore:

Parameter	Description	Valid Options
FTP Server IP*	IP address of backup server.	String 31 characters, or "dotted quad" format. For example: "192.168.1.100."
User*	User name on backup server.	String 31 characters
Password*	Password for user name on backup server.	String 31 characters
File Path*	Path to backup directory server.	String 31 characters

* Required fields

To restore a backup database

1. On the Navigation Tree, click **E7**.
2. Click **System** > **Provisioning** > **Action** > **Backup/Restore**.
3. Select **Load** to retrieve a previously archived database backup file.
4. In the Load DB Backup dialog box, do the following:
   a. In the SFTP/FTP Server IP box, type the IP address of the FTP server where the backup file is located.
   b. In the User box, type your user name to log in to the file server.
      - If you are using the Calix E-Series file server, the default user name is **backup**.

c. In the Password box, type your password to log in to the file server.

- If you are using the Calix E-Series file server, the default user name is **backup**.

d. In the File Path box, type the path to the directory where the backup file is located and the file name.

- If you are using the Calix E-Series file server, the FTP server is configured to look for the database backup file in the C:\CalixESeries\backup directory.

5. Click **Load**.
6. Click **Action** > **Backup/Restore** > **Switch** to restore the retrieved database file.
7. In the Switch DB Backup dialog box, select whether to force the switch to the retrieved database file and then click **Switch**.

Note: The **Yes** setting forces the E7 to replace the database with the currently retrieved database file, even if the file was generated on another E7 system.

CAUTION! The E7 system reboots as part of the database-restore process.

8. After the system comes up, perform a system reset.
   a. In the Navigation Tree, click **E7**.
   b. In the Workarea, click **System** > **Provisioning** > **Action** > **Upgrade** > **Reset System**.

To restore a backup database using CLI

1. Retrieve a previously archived database backup file from a specified file server.

```
load backup from-host <server ID> user <user name> file-path <path>
```

- Example for Calix E-Series File Server application (included in the E7 upgrade file):

```
load backup from-host 192.168.1.1 user backup file-path LAB_2009-08-
01_14_35_02.provdb
```

Note: The Calix E-Series FTP server is configured to look for the database backup file in the C:\CalixESeries\backup directory.

- Example for an FTP service application (previously configured on your PC):

```
load backup from-host 192.168.1.1 user jsmith file-path /e7/LAB_2009-08-
01_14_35_02.provdb
```

Note: When restoring an E7 backup database file from a Windows-based server, use a forward slash (/) as a path separation character when working with FTP application operations. The E7 interprets any backslash in the path string as part of the filename.

2. Switch the database to the file that you just downloaded, resetting the system to operate with the provisioning in the downloaded database.

```
switch database [forced]
```

Note: Using the "forced" option, switches the database, replacing the current database with the database backup retrieved with the "load backup" command, even if the backup file was generated on another system.

3. After performing a database restore, the system must be allowed to come up, and then you must reset the entire system.

```
reset system
```

Troubleshooting Specific Issues

In-Band Management System Lockout

Issue

Lockout from the E7 system in-band management.

Recommended action

Correct any of the following possible problem conditions that could lock you and others out from using in-band management (managing through the data ports).

- Deleting the management VLAN.
- Incorrectly configuring the management VLAN.
- Incorrectly configuring the access control settings.
- Disabling all ports.

Note: Be careful not to lock yourself and others out of the system. If you lock yourself (and others) out of the system, you can try using the console port to reconfigure the system. See Recovering from a System Lock-Out.

Degraded Status

Issue

An entity shows the status of "degraded."

Recommended status

Check the alarm list to determine the specific alarm caused by the entity in "degraded" status.

System Disabled

Issue

An entity shows the status of "system disabled."

Recommended status

Check the alarm list to determine the specific alarm caused by the entity in "system disabled" status.

Log In Connection

Issue

No connection to the E7 to log in.

Recommended action

To troubleshoot the log-in connection problem

1. Verify that you are using the correct IP address. The front Craft Ethernet port is at the factory default IP address of 192.168.1.1, if it has not been changed.
2. Verify that the computer connected to the E7 is on the same subnet as the E7, if using a static IP address. Connect a PC to the front craft Ethernet port and configure the PC to obtain a dynamic IP address.
3. Verify that the telnet service is not disabled and that the server port number that the E7 uses for telnet has not changed. The factory default for telnet access is disabled.

Abort Script

Issue

When using a browser to log in to the E7 web interface and encountering the E7 Abort Script dialog box, the progress indicator continuously spins.

Recommended action

Indicate "No" when prompted for an answer in the Abort Script dialog box to allow the E7 to complete the current task and continue in normal operation.

User Password

Issue

You forgot the password to your E7 user account.

Recommended action

Have another E7 user with administrative privileges reset your password. Otherwise, contact Calix for assistance.

Changing the Management Gateway or Management IP

Issue

Attempting to set either the management gateway or the management IP results in an error message, indicating that the management gateway is not reachable.

Recommended action

To change the management IP (to a different subnet for example), do the following:

1. Set the management gateway to 0.0.0.0.
2. Change the management IP to the new address.
3. Set the management gateway to the new address.

SNMP Communication

Issue

The SNMP manager server cannot get information from the E7.

Recommended action

To troubleshoot the SNMP server

1. Ping the E7 from the SNMP server. If you cannot, check the cable, connections and IP configuration.
2. For SNMPv2c, check to see that the community (or trusted host) in the E7 matches the SNMP server's community.
3. For SNMPv3, check to see that the SNMPv3 username in the E7 matches the SNMP server's user information.
4. Incorrectly configuring the access control settings may lock you out from using in-band management. Try using the console port to reconfigure the system.

Network Connection to Host

Issue

Connection between two hosts on a network is questionable.

Recommended action

The E7 command line interface (CLI) offers a Ping utility determines whether there is a problem with the network connection between two hosts. This utility sends echo requests to the address you specify and lists the responses received and their round-trip time. Use the following command:

```
ping <host IP address>
```

Example:

```
ping 172.21.90.187
```

Troubleshooting an E7 or E5-400 System Connection

If you cannot connect to an E5-400 or E7 node from CMS, perform the following troubleshooting steps.

Note: CMS uses an HTTP session to access the embedded Web interface for managing E-Series platforms. If a CMS Desktop user session is open for more than 12 hours, the E7 HTTP session automatically times out. To re-access the Web interface, you must close and re-start CMS Desktop.

To troubleshoot a disconnected E5-400 or E7 device

1. Check the following:
   - If a TrapRegFailed alarm has been raised against the node, see the troubleshooting steps in *Troubleshooting a TrapRegFailed Alarm* (on page 155).
   - Log in to the E5-400 or E7 Web interface, navigate to the Craft Management Interfaces screen, and verify that the IP address in the IP box matches the IP address used in CMS.
   - Ask your CMS system administrator to open a shell on the CMS server and ping the IP address of the node to confirm that it can be reached.
   - If the IP address can be reached and a NTWK DROPPED (Network Dropped) alarm persists, contact Calix TAC to troubleshoot the SNMP setup on the node.
2. Manually connect to the E5-400 or E7 node. See *Manually Disconnecting and Connecting an E5-400 or E7 System Node* (on page 164).

Troubleshooting a TrapRegFailed Alarm

When adding an E-Series node to CMS or manually connecting to a node that is disconnected, the system automatically attempts to add CMS as a trap destination in the node. If successful, the node sends SNMP traps to the CMS server using port 162. If unsuccessful (for example, the node already contains the maximum number of trap destinations), CMS reports a TrapRegFailed alarm.

A TrapRegFailed alarm indicates node SNMP traps sent to the CMS server from the alarmed Calix device are unsuccessful.

Recommended Action

1. In a terminal window or remote telnet or SSH session, log in as a root user on the host server. Verify that the entries in the etc/hosts file are correct:
   - At the command prompt, type the following: **`cat /etc/hosts`**
   - Use a text editor to edit or add the CMS server static IP address and DNS name to match the following example:

```
127.0.0.1       localhost.localdomain   localhost
172.21.90.15    cmsserver
```

   where 172.21.90.15 is the CMS server static IP address and *cmsserver* is the name of the CMS server.

   Note: Restarting the CMS Server is not required.

2. Do one of the following:
   - B6 node: Add the trap destination (in the B6 Web interface, click **System** > **SNMP Traps**).
   - E3/E5-100 node: Delete one of the trap destinations (in the Configurator interface, click **Advanced Applications** > **Access Control** > **SNMP**).
   - E7/E5-400 node: Add or update the trap destination (in the E7 Web user interface, click **Management** > **SNMP** > **TRAP Destination**).
3. (For E-Series devices) Manually register CMS as a trap destination:
   - On the Navigation Tree, click the root region or the parent network group of the node.
   - In the Work Area, click **Network Details**, and then click the node type.
   - In the device list, click the node(s).
   - Click **Action** > **Register Trap**.
4. If the above steps do not clear the alarm, delete and recreate the node in CMS.

Extracting Diagnostics

This procedure describes how to extract diagnostics and various log files from a system, card, or shelf by capturing a file and then transferring it to a designated file server.

For modular chassis systems, Snapshot/Extract extracts the database as well as the system log files from both cards of the Modular Chassis Controller (MCC) shelf, only. It will not extract any log files from the Modular Chassis Expansion (MCE) shelves. Extract Diagnostics retrieves system logs from all cards in the modular chassis system.

For E7 stand-alone systems, system log files from all (both) cards can be retrieved using a snapshot / extract sequence.

Parameters for extracting diagnostics

Parameter	Description	Valid Options
SFTP/FTP Server IP	IP address of server. This is an IP address in "dotted quad" format: "192.168.1.100". Alternatively, "none" can be used to reset the value to "0.0.0.0."	String 31 characters, or "dotted quad" format. For example: "192.168.1.100."
User	Username on the server.	String 31 characters
Password	Password for user name on backup server.	String 31 characters
Directory Path	Directory path on server (*). This is a text string. If you do not specify a directory path, the extracted files are placed in the home directory associated with the remote user.	String 31 characters
Log File Name	Name for the log file archive. This is a text string.	

To create a backup of the database

1. Do one of the following, according to the level of diagnostics that you want:
   - To extract the diagnostics for the E7 system, on the Navigation Tree, click **E7**, and then click the **System** > **Provisioning** tabs.
   - To extract the diagnostics for an E7-2 MC shelf, on the Navigation Tree, click **Shelf#**, and then click the **Provisioning** tab.
   - To extract the diagnostics for a card in an E7 shelf, on the Navigation Tree, click (**Shelf#** for E7-2) **> Card#**.
2. From the menu, click **Action** > **Extract Diagnostics**.
3. In the Extract System Diagnostics dialog box, do the following:
   a. In the SFTP/FTP Server IP box, enter the IP address of the file server.
   b. In the User box, enter your user name for the file server.
   c. In the Password box, enter your password for the file server.

d. In the Directory Path box, enter the path to the directory that will receive the transferred file.

e. In the Log File Name, enter the file name that will be assigned to the extracted diagnostics.

f. Click **Extract (System/ Shelf/Card)**.

For CLI:

```
extract diagnostics system to-host <server-name> user <username>
[directory-path|log-file-name]

extract diagnostics shelf <s-number> to-host <server-name> user
<username> [directory-path|log-file-name]

extract diagnostics card <slot> to-host <server-name> user
<username> [directory-path|log-file-name]
```

Recovering from a System Lockout

If you lock yourself (and others) from the E7, you will need to reload the factory-default configuration file by resetting the database. Returning to the factory-default configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all previous configurations. The user name will be reset to "e7" and the password will be reset to "admin" with the IP address reset to 192.168.1.1.

CAUTION! Performing a Reset Database action *replaces all provisioning to default values*. This includes setting the IP address back to the default and setting the HTTP to secure, requiring https:// in the login.

Warning: Calix strongly recommends that you back up the configuration file before restoring the default configuration.

You can connect locally to the CLI from the E7 serial port and reload the factory-default configuration file with a Command Line Interface (CLI) command.

To reset the database to a factory-default configuration file

1. Verify that your PC is connected to the E7 serial port. See the *Calix E7 Installation Guide* for instructions.
2. On your PC, use a VT100 terminal emulation program to start a console session. For example, launch a HyperTerminal session as follows:
   a. On the Start menu, click **Programs > Accessories > Communications > HyperTerminal**.
   b. In the Connection Description dialog box's Name field, type a name for the session, and then click **OK**. For example, type **E7**.
   c. In the Connect To dialog box, in the Connect Using list, select the PC serial port to which the console cable is connected. For example, click **COM1**.
   d. In the COM# Properties dialog box, on the Port Settings tab, do the following:
      - In the Bits per Second list, click **38400**.
      - In the Data Bits list, click **8**.
      - In the Parity list, click **None**.
      - In the Stop Bits list, click **1**.
      - In the Flow Control list, click **None**.
   e. Click **OK** to connect.
3. In the console window, press the **Enter** key to initiate the console CLI session.

4. Log into the E7 CLI as follows:

   a. At the Username prompt, enter your user name. For example, type **e7** (default).

   b. At the Password prompt, enter your password. For example, type **admin** (default).

   Note: The logon ID and password are case sensitive.

   The *CalixE7*> command prompt displays upon successful login to the E7

5. Enter **`reset database`**.

   The E7 is now re-initialized with a default configuration file including the default user name of "e7" and the default password of "admin".

Line Testing ONT POTS Port Services

The E7 supports GR-909 metallic loop testing on analog POTS service ports of supported ONTs through the integrated test head functionality in the ONT. The E7 conducts the following ONT drop test measurements:

- **Foreign Voltage:** Measures AC and DC voltage across tip-ground and ring-ground. Returns pass or fail.
- **Hazardous Potential Voltage:** Measures AC and DC voltage across tip-ground and ring-ground. Returns pass or fail.
- **Resistive Test:** Measures resistance across tip-ground and ring-ground. Returns pass or fail.
- **Receiver Off-Hook:** Measures resistance at two separate voltage levels and compares the results. Returns yes or no. If it returns yes (the receiver is off-hook), then Ringer Detected will not return any result.
- **Ringer Detected:** Measures the Ringer Equivalency Number (REN) number across the tip-ring. Returns yes or no.

The E7 uses the following thresholds to determine the ONT POTS port drop test pass/fail status:

Measurement	Fail Threshold	Measurement Range
Foreign Voltage	VAC > 10 Vrms VDC > 6 Volts	0.1 - 150 Vrms 0.1 - 150 Volts
Hazardous Potential Voltage	VAC > 50 Vrms VDC > 135 Volts	0.1 - 150 Vrms 0.1 - 150 Volts
Resistive Test	Resistance < 150 kOhms	10 Ohms - 1 MOhms
Receiver Off-Hook	|(Rv1-Rv2)/Rv1| > 0.15	10 Ohms - 150 kOhms
Ringer Detected	REN < 0.175 REN > 5.0	0.15 REN - 5.5 REN

To perform a line test on a POTS service port

1. On the Navigation Tree, click **ONTS**.
2. In the table of ONTs, double-click the ONT on which you want to perform the test, and then click the **ONT Ports** tab.
3. In the table of ONT ports, double-click the POTS port on which you want to perform the test.
4. In the Menu, click **Action** > **Line Test**, and then click **Test** in the Line Test on POTS dialog box.

   The results of the test appear in the dialog box.

For CLI:

```
test pots-svc ont-port <port> [forced]
```

Line Testing Card Voice (POTS) Service

The E7 supports GR-909 metallic loop testing on analog POTS service ports of E7-2 VDSL2-C48 line card, by performing the following drop test measurements:

- **Foreign ElectroMotive Force (FEMF) Test** - Checks for excess voltage on the drop. FEMF may be determined using two- or three-terminal T-G and RG AC voltage and two-terminal T-G and R-G DC voltage.
- **Resistive Faults Test** - Checks for resistive (i.e., DC resistance) faults across T-R (shorts), T-G and R-G (grounds).
- **Receiver-Off-Hook (ROH) Test** - Distinguishes between a T-R resistive fault and an off-hook condition. A receiver-off-hook can be identified by several means. For example, ROH can be determined by measuring the DC resistance at two different test voltage levels and looking for a non-linear relationship in the DC resistance across T-R.
- **Ringers Test** - Determines the presence of appropriate ringer terminations on the customer's line. One method of performing this test uses AC resistance measurements as described in TR-TSY-000231.

To perform a line test on a Card Voice (POTS) service

1. On the Navigation Tree, click an xDSL port.
2. In the Workarea, click **Provisioning**.
3. In the Menu, click **Action** > **Line Test**, and then click **Test** in the Line Test on POTS dialog box.

   The results of the test appear in the dialog box.

For CLI:

```
test pots-svc pots-port <p-port> [forced]
```

Adding an ONT to Quarantine

This topic describes how to effectively remove a suspected faulty ONT from the system by adding it to quarantine.

To add an ONT to quarantine

1. On the Navigation Tree, double-click **ONTS**.
2. Click the **Quarantined ONTS** tabs.
3. From the menu, click **Create**.
4. In the Create Quarantined ONT dialog box, enter the serial number of the ONT that you want to add to quarantine.
5. Click **Create**.
6. To remove an ONT from quarantine, do the following:
   a. On the Navigation Tree, double-click **ONTS**.
   b. Click the **Quarantined ONTS** tabs.
   c. In the table of quarantined ONTs, click the ONT that you want to remove.
   d. From the menu, click **Delete**.

For CLI:

- `add ont serial-number <serial#> to-quarantine`
- `add ont <ont id> to-quarantine`
- `remove ont <ont id> from-quarantine`
- `show ont [quarantine|quarantine detail]`

Manually Disconnecting and Connecting an E7 or E5-400 System Node

When you add an E5-400 or E7 node to CMS, the system automatically confirms that the node can be reached via SNMP approximately once every minute.

You can manually disconnect a unit and reconnect it, for example, after troubleshooting a connection issue.

To manually disconnect (connect) to an E5-400 or E7 node

1. On the Navigation Tree, click the parent network group of the unit.
2. In the Work Area, click **Network Details**, and then click the E5-400 or E7 node type.
3. In the device list, select the unit(s).
4. Click **Action** > **Disconnect** or **Connect**.

Chapter 4

Managing E7 Global Profiles

Global profiles automate synchronizing profiles and templates across multiple E7 networks. They support cross-network capabilities such as bulk provisioning across networks. You create a profile once within CMS and apply it across all targeted E7 networks to ensure consistency across large deployments.

How Global Profile Mapping Works

When you create a global profile, CMS automatically maps or links it with a local node profile. Once linked, the local profiles are automatically synchronized or updated.

Global profiles are mapped or synchronized with local E-Series system nodes when you perform any of the following tasks:

- Create a global profile in CMS.
- Add a new node to CMS.
- Manually synchronize global profiles with nodes.

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

1. The node must be connected to CMS.
2. The Enabled parameter for the global profile must be set to Yes. For the behavior when this parameter is modified, see the explanations below.
3. The Global Profiles Enabled parameter for the node must be set to Yes. For the behavior when this parameter is modified, see the explanations below.

Assuming that the above conditions are met, when you create a global profile, the system checks the local profiles on each node and first compares all profile parameters except the profile ID.

The following table describes how the system maps global profiles created in CMS to local node profiles.

How a global profile maps to a local 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 ID field. If the global profile ID is already used by one of the local profiles, a new local profile is created with "_1" appended to the profile ID.
One or more local profiles match the global profile	The system maps the global profile to the matched local profile with the same profile ID, if it exists. If it does not exist, the system maps to one of the matched local profiles.

To view how a global profile is mapped to individual node profiles, see *Viewing Global Profile Synchronization Details* (on page 168).

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.
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 nodes. For any future nodes 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, nodes already synchronized are not affected. For any future nodes created in CMS, the global profile is not mapped or synchronized.

Modifying the Global Profiles Enabled parameter for a node

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

Synchronizing Global Profiles

Global profiles are automatically synchronized with enabled nodes when you create a global profile.

To view or change the Global Profiles Enabled node parameter, see *Modifying the Enabled Status of a Global Profile* (on page 170).

Use the following procedure to manually synchronize global profiles. When performing a manual synchronization, you select the global profile(s) and synchronize them to all enabled nodes.

Synchronizing a global profile requires Full CMS Administration privileges.

Note: In CMS R11.2, the following applies:
-- Global ONT-related profiles can be shared between E7 GPON and AE ONTs.
-- ONT profiles that describe the configuration of ONTs are not shared globally and CMs synchronization is not supported.

To synchronize global profiles to all enabled nodes

1. On the Navigation Tree, click **CMS**.
2. In the Work Area, click **Profile**, and then click the node type and type of profile to synchronize.
3. In the profile list, select the item(s) 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.

Viewing Global Profile Synchronization Details

Viewing an E7 global profile requires CMS Administration privileges.

To view E7 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.

Modifying the Enabled Status of a Global Profile

Only the enabled status of an E7 global profile can be modified. You can toggle the status of the Enabled field between Y (Yes) and N (No). Setting the field to Y synchronizes the profiles with all nodes that enable global profiles.

To change the properties of a global profile, delete the old profile, create a new profile, and then apply it.

Modifying a global profile requires Full CMS Administration privileges.

To modify the Enabled status of an E7 global profile

1. On the Navigation Tree, click **CMS**.
2. In the Work Area, click **Profile**, and then click the node type and type of profile to modify.
3. Select the profile(s) to modify. When selecting multiple profiles, use Shift+click to select a range of profiles, or Ctrl+click to select one profile at a time.
4. Use the horizontal scroll bar to locate the Enabled column. In the Edit row, modify the field.
5. Click **Apply**. Click **OK** to save the new settings.

Deleting Global Profiles

You can delete E7 global profiles from nodes that have profiles enabled but do not have that profile applied. Deleting a profile does not remove provisioning from a node that has the profile applied.

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

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

Deleting a global profile requires Full CMS Administration privileges.

To delete an E7 global profile

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

Chapter 5

Accessing E-Series System Configuration Settings

CMS supports HTTP and HTTPS sessions with E7 units based upon the device security settings.

To access and modify E7 configuration settings, you must have Full Configuration Management permission as well as Write permission for the region in which the parent network group is nested.

Once you have added an E7 to CMS, on the Navigation Tree, expand the network group and click the unit. Tabs for each configuration area display in the Work Area.

Note: CMS uses an HTTP session to access the embedded Web interface for managing E-Series platforms. If a CMS Desktop user session is open for more than 12 hours, the E7 HTTP session automatically times out. To re-access the Web interface, you must close and re-start CMS Desktop.

For product information and provisioning instructions, log in to the *Calix Resource Center* and follow the link to the Calix Documentation Library. In the navigation pane on the left, click **E-Series** and locate the links to the Calix E7 documentation.

Searching for VLANs

From the Navigation Tree, CMS supports searches that filter on a range of VLANs for a single E-Series unit.

The search tool returns a list of filtered VLANs that are available from the E-Series unit selected in the Navigation Tree.

To search for E-series VLANs

1. In the Navigation Tree, select the **E7** node to expand it, and then click **VLANS**.
2. In the Toolbar, enter values for the VLAN Start and End to define the range of VLANs to search for and display.
3. Click **Refresh** to display the search results in the Work Area.
4. Click on a row of the search results to display the provisioning information of the selected VLAN.
5. Click **Table View** to return to the search results.

Searching for E7 GPON ONTs

This topic describes how to search for E7 GPON ONTs from the E7 Navigation Tree and from the CMS Tools menu. In CMS, there are also many other aspects of the E7 for which you can perform a search.

- Enter specific attributes of an ONT of which the search tool filters.
- The search tool returns a list of filtered items that are available.

Note: Once installed, ONTs and ONT attributes can be immediately accessed in the E7 inventory database in CMS.

To search for ONTs based on status

1. In the Navigation Tree, select the **E7** node to expand it, and then click **ONTS**.
2. In the Toolbar, select whether to search or filter on all of the linked and unlinked ONTs or only the ONTs not linked to the E7.
   - **Not linked** filters on ONTs that have been discovered through the connection to an E7 system, but have not been linked to an ONT profile.
   - **All** filters on both not linked ONTs and linked ONTs, which are discovered ONTs that are linked to an ONT profile.
3. Click **Apply** to display the search results in the Work Area.
4. Click on a listed ONT characteristic to display the provisioning information.
5. Click **Table View** to return to the search results.

To search for ONTs based on ID

1. In the Navigation Tree, select the **E7** node to expand it, and then click **ONTS**.
2. In the Toolbar, enter the ONT ID.
3. Click **Apply** to display the information for the ONT that matches the ID.
4. In the Work Area, click on an ONT characteristic to display the provisioning information.
5. Click **Table View** to return to the search results.

To search for ONTs based on attributes

1. In the Navigation Tree, select the **E7** node to expand it, and then click **ONTS**.
2. In the Toolbar, click **Advanced** to open the Apply ONT Filter dialog box.
3. Enter as many attributes as you want to create a broad or narrow search. Refer to the *Calix E7 GPON Applications Guide* for information on the parameters.

4. Click **Apply** to display the search results in the Work Area.
5. Click on a listed ONT characteristic to display the provisioning information.
6. Click **Table View** to return to the search results.

To search for ONTs using the CMS Tools menu

1. In CMS Desktop, on the **Tools** menu, click **Search** > **E-series** > **E5-300/400/E7** > **ONT**, and then select the filter for the search:
   - **Provisioned ONT**
   - **Discovered ONT**
   - **Quarantined ONT**
2. In the Filter Criteria form, select the criteria for the various categories, if you want to narrow the search.
3. Click **Submit**.
4. The search results include a hyperlink that will take you to the dialog on the PON record in CMS. From here, the user can activate the ONT and create services using the CMS Service dialogue.

- Alternatively, you can select the type of ONT port or service on which to perform the search:
  - **ONT GE**
  - **ONT FE**
  - **ONT HPNA**
  - **ONT T1/E1**
  - **ONT POTS**
  - **ONT Services**
- Alternatively, you can search for cross-platform ONTs:
  a. In CMS Desktop, on the **Tools** menu, click **Search** > **Multi-Platform** > **ONTs (C7, E7, AE)**.
  b. In the Filter Criteria form, select the criteria for the various categories, if you want to narrow the search.
  c. Click **Submit**.
  d. The search results include a hyperlink that will take you to the dialog on the PON record in CMS. From here, the user can activate the ONT and create services using the CMS Service dialogue.

Searching for Configuration Aspects

This topic describes how to search for E7 configuration aspects from the CMS Tools menu.

To search for configuration aspects using the CMS Tools menu

1. In CMS Desktop, on the **Tools** menu, click **Search** > **E-series** > **E5-300/400/E7**, and then select the filter for the search:
   - **E5-400/E7 Node**
   - **System**
   - **Equipment**
   - **GE Port**
   - **10GE Port**
   - **Ethernet Interface**
   - **LAG Interface**
   - **VLAN**
   - **MAC Table**
   - **TAG Action**
   - **GPON**
   - **ONT**
   - **DHCP Leases**
   - **ONT GE**
   - **ONT FE**
   - **ONT HPNA**
   - **ONT T1/E1**
   - **ONT POTS**
   - **ONT Services**
   - **Eth OAM**
1. In the Filter Criteria form, select the criteria for the various categories, if you want to narrow the search.
2. Click **Submit**.
3. The search results include a hyperlink that will take you to the dialog on the PON record in CMS. From here, the user can activate the ONT and create services using the CMS Service dialogue.

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.

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

   - 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.

Chapter 6

Viewing Alarms and Events

This chapter includes the descriptions of the E7 element alarms, the available environmental alarms, and the events that are displayed in the Alarm Table in the web browser interface.

Topics Covered

This chapter covers the following sets of topics:

- Element alarms
- Environmental alarms
- Events

Service and non-service affecting alarms

The following exists:

- **"degraded"** appears for an object (ONT or a Card) status if a non-service affecting alarm is reported against it.
- **“sys-disabled”** appears for an object status if a service affecting alarm is reported against it or any of its parents.

  For example:

  - An ONT parent is the system object.
  - A Card parent is the shelf, and then the system.

Alarm aggregation in CMS

The E7 alarms can also be displayed in the CMS interface alarm panel, if you configure CMS to receive the alarms through an SNMP trap destination. You could filter the alarms by device to display only the E7 alarms. See "Configuring SNMP System Management" in the *Calix E7 User Guide* for details.

Note: While troubleshooting a port that has Admin State = "enabled-no-alarms," either use the CLI command **`show alarm include suppressed`**, or from the web browser interface temporarily set the Admin State to "enabled," and then refresh the alarm panel manually or wait for default refresh rate to see the suppressed alarms.

Element Alarms

The topics in this section describe the possible causes of E7 element alarms and the recommended actions that you should take to clear the conditions that have caused the alarm.

The alarm descriptions also show the following conditions of severity:

- **Warning alarms:** indicate a condition of concern that is not service-affecting.
- **Minor alarms:** typically indicate a problem condition that is not service-affecting.
- **Major alarms:** typically indicate service-affecting conditions.
- **Critical alarms:** can indicate service-affecting conditions.

See Environmental Alarms for information on the conditions and/or equipment that can be monitored on the E7 Alarm Interface module.

backup-files-exist (Backup files exist)

Indicates there is already an existing backup file from previously performing the "Backup/Restore Snapshot" function or the "snapshot database" command to create a database backup file on the E7.

Recommended action

Transfer the captured database file to an external file server, using either the extract function or "extract backup" command. When this operation completes, the database backup file created from the "snapshot database" function is automatically removed from the E7 and the alarm is cleared.

Alternatively, if you choose not to archive the database backup file, use the "delete snapshot" function or the "delete backup" command to delete the existing backup file from the E7, clearing the alarm.

Severity

Warning, non-service-affecting

bad-inventory (Bad inventory data)

Indicates the inventory data of an XFP, SFP, or SFP+ connector inserted into the unit could not be read.

Recommended actions

Replace the XFP, SFP, or SFP+ connector and contact Calix to report the corrupted hardware.

Severity

Major, service-affecting

bank-acting-master (Shelf Acting Master Node)

Indicates there is no shelf in the stacking ring that is designated as the Master node, resulting in this shelf being nominated to act as the Master node.

Recommended action

Contact Calix to report this alarm.

Severity

Information, service-affecting

bank-ring-port-down (Shelf Ring Port Down)

Indicates that a local stacking ring interface is down.

Recommended action

- Check the cable on both sides of the connection.
- Check the provisioning for both ends of the cable connection.

Severity

Major, non-service-affecting

bank-sec-master (Shelf Second Master Node)

Indicates there is more than one shelf in the stacking ring that is designated as the Master node.

Recommended action

Contact Calix to report this alarm.

Severity

Information, service-affecting

boot-data-corrupt (Boot Data Flash is Corrupt)

Indicates that the startup or boot data is corrupt and the E7 might not be running the desired software release.

Recommended action

Perform the "commit system version" command or the "commit system" operation to repair the corruption in Flash memory.

Severity

Major, non-service-affecting

bpdu-guard (BPDU Guard Triggered - Interface Has Been Disabled)

Indicates an interface is disabled due to receiving unexpected RSTP BPDUs.

Recommended action

1. Disable the RSTP remote switch.
2. Toggle the interface by performing a Disable action, and then an Enable action.

Severity

Major, service-affecting

bpdu-unknown (Received Unknown or Incompatible BPDU)

Indicates the interface is receiving spanning tree BPDUs with a destination MAC address that is unsupported or is incompatible with the interface.

- A destination MAC address of 01:00:0C:CC:CC:CD indicates that the remote node is sending Cisco PVSTP+ BPDUs, which are unsupported.
- A destination MAC address of 01:80:C2:00:00:08 indicates that the remote node is sending BPDUs for Provider Bridge operation (802.1ad), but the local interface is provisioned with a role of Edge.

Recommended action

Verify the spanning tree provisioning for the Ethernet interfaces on both nodes in the RSTP link.

Severity

Minor, non-service-affecting

card-hw-failure (Card HW Failure)

The GPON card hardware failed initialization.

Recommended action

Reseat the card in the connector.

If the failure continues, replace the card.

Severity

Critical, service-affecting

card-not-fully-inserted (Card is Not Fully Inserted)

Indicates that a card is not fully inserted in the system.

Recommended action

Push the card into the connector to make full contact.

Severity

Major, service affecting

card-type-differs (Card Type Differs)

The provisioned card is of a different type than what is installed, however, they are still compatible.

Recommended action

Replace the installed card with a card that matches the provisioning. Or, update the provisioning to match the currently installed card type.

Severity

Minor, non-service-affecting

control-vlan-audit-failure (Control VLAN Audit Failure)

The Control VLAN audit has failed.

Recommended action

Contact Calix Technical Assistance for resolution of the condition.

Severity

Critical, service-affecting

db-fail (Database Failure)

Indicates one of the following conditions:

- The E7 read faulty data from the database at startup.
- The E7 read faulty data from the database during a database restore.

Note: When this alarm is present, the system is running on the default database, which has no services provisioned.

Recommended action

Restore a valid database or perform a database reset to start with a default (empty) database.

Severity

Critical, service-affecting

different-version (Running Different Software Version)

Indicates that the alarmed card is running a different software version than the currently-active system controller card.

Recommended action

Perform a software upgrade to update the card to the correct software version.

Severity

Major, non-service-affecting

duplicate-ont-reg-id (Duplicate ONT Registration ID)

Indicates an ONT arrived that reports the same Registration ID as an existing discovered ONT.

Recommended action

Reset one of the discovered ONTs and update the Registration ID (RONTA).

Severity

Minor, non-service-affecting

e5-too-old (E5 May Not Support SFP+ Ports)

Indicates that the E5-400 is a pre-pilot unit that may not support SFP+ modules.

Recommended action

Notify Calix of this alarm.

Severity

Minor, non-service-affecting

efm-down (Eth-OAM EFM Protocol Down)

Indicates that 802.3ah EFM protocol is down.

Recommended action

Disable the EFM protocol on the ONT port to surpress the alarm.

Severity

Major, non-service affecting

eqpt-fail (Equipment Failure)

Indicates that a card hardware failure has been detected. If a system alarm occurs, the backplane could not be read.

Recommended action

Replace the card reporting the failure. Or, if a system alarm occurs, the backplane may need to be replaced.

Severity

Major, non-service-affecting

eqpt-id-fail (Equipment ID Failure)

Indicates that an equipment ID is no longer valid.

Recommended action

Contact Calix to report the alarm.

Severity

Minor, non-service-affecting

erps-acting-master (ERPS Ring - Acting Master Node)

Indicates that an ERPS ring has no E7 designated as the master node. Therefore, this node is acting as the master.

Recommended action

Confirm that the ERPS ring configuration is correct:

- Ensure one of the nodes in the ERPS ring is a master node.
- Ensure the designated master is not bypassed.
- Ensure all interfaces in the ERPS ring are enabled and in service.

Severity

Major, service-affecting

erps-domain-health-compromised (ERPS Domain Health Compromised)

ERPS domain health is compromised.

Recommended action

Contact Calix Technical Assistance for resolution of the condition.

Severity

Major, non-service-affecting

erps-node-isolated (ERPS Isolated Node)

Indicates both ERPS ring interfaces that are directly connected to the E7 are out of service (down), leaving this node isolated.

Recommended action

Check the interface provisioning and physical cables.

Severity

Critical, service-affecting

erps-ring-down (ERPS Ring Down)

Indicates a ERPS ring failure has occurred due to a condition such as a fiber break.

Recommended action

Check the provisioning and physical cables on each side of any identified fiber break.

Severity

Major, non-service-affecting

erps-down-loc (ERPS Ring Down - Local)

Indicates an ERPS ring interface that is directly connected to this E7 (local) is out of service (down).

Recommended action

Check the interface provisioning and physical cable.

Severity

Major, non-service-affecting

erps-sec-master (ERPS Ring - Second Master Node)

Indicates that more than one node is designated as the master node in the ERPS ring.

Recommended action

Designate only one node as the master node and all other nodes as transit nodes in the ERPS ring.

Severity

Major, service-affecting

esc-clock-failures (ESC Clock Failures)

The failure of a clock is detected in the Ethernet switch controller.

Recommended action

Replace the card reporting the failure.

Severity

Critical, service-affecting

eth-intf-down (Ethernet Interface down - LOS)

Indicates that the Ethernet interface is down, due to loss of signal on the interface.

Recommended action

Check the cable and cable connections.

Severity

Major, service-affecting

eth-oam-mep-avg-delay-measurement (Average Delay Measurement)

Indicates that the specified reporting threshold has been exceeded for the average round-trip delay monitored attribute of Ethernet OAM frame measurements.

Severity

Minor, service-affecting

eth-oam-mep-avg-delay-thresh (Average Delay Variation Threshold Exceeded)

Indicates that the specified reporting threshold has been exceeded for the average round-trip delay monitored attribute of Ethernet OAM frame measurements.

Severity

Minor, service-affecting

eth-oam-mep-ccm-loss-of-continuity (CCM Loss of Continuity)

Indicates a loss of continuity between a MEP initiating Continuity Communication Messages (CCMs) and a destination MEP that should be receiving the CCMs and then responding.

Severity

Critical, service-affecting

eth-oam-mep-ccm-rx-interface-not-up (CCM Received with Interface Not Up)

Indicates that a MEP interface is detected as being down because a MEP initiating Continuity Communication Messages (CCMs) and sending to a destination MEP is receiving a response that the interface is down.

Severity

Major, non-service-affecting

eth-oam-mep-ccm-rx-unexpected-meg (CCM Received from Unexpected MEG)

Indicates that a MEP is receiving Continuity Communication Messages (CCMs) from an undiscovered Maintenance Entity Group (MEG).

Severity

Major, non-service-affecting

eth-oam-mep-ccm-rx-unexpected-mep (CCM Received from Unexpected Remote MEP)

Indicates that a MEP is receiving Continuity Communication Messages (CCMs) from a MEP that is not included in the remote MEP ID list.

Severity

Minor, non-service-affecting

eth-oam-mep-ccm-rx-unexpected-period (CCM Received with Unexpected Period)

Indicates that a MEP is receiving Continuity Communication Messages (CCMs) from a destination MEP, but with an unexpected period of time.

Severity

Minor, non-service-affecting

eth-oam-mep-ccm-rx-with-rdi (CCM Received with the RDI Bit Set)

Indicates the Continuity Communication Messages (CCMs) have been received with the Remote Defect Indications (RDI) bit set.

Severity

Minor, non-service-affecting

eth-oam-mep-far-end-avg-loss (Far-End Average Loss)

Indicates that the specified reporting threshold has been exceeded for the far-end average loss ratio monitored attribute of Ethernet OAM frame measurements.

Severity

Minor, service-affecting

eth-oam-mep-far-end-max-loss (Far-End Max Loss)

Indicates that the specified reporting threshold has been exceeded for the maximum far-end loss ratio monitored attribute of Ethernet OAM frame measurements.

Severity

Minor, service-affecting

eth-oam-mep-max-delay-measurement (Maximum Delay Measurement)

Indicates that the specified reporting threshold has been exceeded for the maximum round-trip delay monitored attribute of Ethernet OAM frame measurements.

Severity

Minor, service-affecting

eth-oam-mep-max-delay-variation (Maximum Delay Variation)

Indicates that the specified reporting threshold has been exceeded for the maximum round-trip delay variation monitored attribute of Ethernet OAM frame measurements.

Severity

Minor, service-affecting

eth-oam-mep-near-end-avg-loss (Near-End Average Loss)

Indicates that the specified reporting threshold has been exceeded for the average near-end loss ratio monitored attribute of Ethernet OAM frame measurements.

Severity

Minor, service-affecting

eth-oam-mep-near-end-max-loss (Near-End Max Loss)

Indicates that the specified reporting threshold has been exceeded for the maximum near-end loss ratio monitored attribute of Ethernet OAM frame measurements.

Severity

Minor, service-affecting

fan-fail (Fan failure)

Indicates an E7 fan stopped rotating.

Recommended action

Replace the E7 fan tray.

Severity

Minor, non-service-affecting

gpon-replication-resource-exhausted (GPON Replication Resource Exhausted)

Indicates that the number of hairpin VLANs plus the number of N:1 VLANs has exceeded the limit of 32.

Recommended action

Reduce the number of these VLAN types on the GPON card.

Severity

Major, service-affecting

improper-removal (Improper removal)

Indicates the XFP, SFP, or SFP+ connector of an enabled port has been removed.

Recommended action

- Replace the XFP, SFP, or SFP+ connector.

  or

- Set the admin state of the port to disabled.

Severity

Minor, service-affecting

initial-flash-write-in-prog (Storing databse to flash memory)

Indicates that a card is in the process of writing the database to flash memory and cannot be reset at this time.

Recommended action

Wait for the current process to complete before initiating a card reset.

Severity

Warning, non-service-affecting

interface-quality-audit-failure (Interface Quality Audit Failure)

The Interface Quality Audit (IQA) detects an errored packets value that is over the threshold value.

Recommended action

Check to see if any of the following conditions exist to cause the link failure:

- Fiber is faulty
- Pluggable module is faulty
- Fiber is too long

Severity

Major, service-affecting

lacp-fault (LACP Fault on Port)

Indicates that a port in the link aggregation group (LAG) is unavailable, due to an LACP fault.

Recommended action

- Check the admin status of each Ethernet port and interface that is in the link aggregation group.
- Check the link aggregation and LACP provisioning of Ethernet interfaces on the remote side.

Severity

Minor, service-affecting

lag-intf-down (Aggregation Interface down)

Indicates that the link aggregation group (LAG) is down, due to no active member associations.

Recommended action

- Check the admin status of each Ethernet interface that is in the link aggregation group.
- Check the link aggregation provisioning.
- Check the cable and cable connections.

Severity

Major, service-affecting

loss-of-pon (Last Discovered ONT Went Missing)

Indicates that the last discovered ONT is no longer detected.

Recommended action

Check for a fiber cut or a fiber disconnection.

Severity

Major, service-affecting

loss-of-signal (Loss of signal)

An Ethernet interface is down due to loss of signal on the interface.

Recommended Action

- Check cable.
- Check far end connection and equipment.

Severity

Major, service-affecting

low-sw-res (Low Software Resources)

Indicates an excessive consumption of software resources (memory, CPU time, or file space).

Recommended action

Issue the CLI command **`clear sw-resource-alarm`** that evaluates software resource usage and clears the "low resources" alarm, if appropriate. If the alarm persists, contact the Calix Technical Assistance Center (TAC).

Severity

Minor, non-service-affecting

mismatch-equip (Mismatch Equipment)

Indicates that an Ethernet port or card has an equipment type installed that does not match the provisioning. For an Ethernet port, an SFP module may be inserted into an SFP+ port, or an SFP+ module inserted into an SFP port.

Recommended action

If the alarm is raised against an Ethernet port, install the SFP or SFP+ module in the correct port.

If the alarm is raised against a card on an E7/E5-400 platform, do one of the following:

- Insert a card matching the provisioned card type.
- Delete the provisioned card from the system database, allowing the card to come up.

Severity

Critical, service-affecting

module-fault (Pluggable Module Fault)

Indicates that one of the Ethernet port modules is faulty.

Recommended action

- Replace the faulty Ethernet port module.

  Or

- Set the admin state of the Ethernet port to disabled.

Severity

Minor, service-affecting

module-not-for-stacking (Module Cannot Be Used For Stacking)

Indicates that a module that cannot be used for stacking was inserted in a stacking port.

Recommended action

Replace the module with a Calix direct-attach SFP+.

Severity

Major, service-affecting

multiple-databases (Multiple Databases)

Indicates that a card is running on a provisioning database that is not the same as that being used by the system.

- If the alarm is critical, the database versions are completely different.
- If the alarm is minor, the version on the alarmed card has a more recently updated database version than the system database.

Recommended action

For a critical alarm, reset the database on the card to discard the card's database and clear the alarm.

For a minor alarm, switch control to the card with the more recent database to clear the alarm.

See *Switching Control Between Line Cards* (on page 112).

Severity

Critical, service-affecting

new-release-ready (New Software Release is ready)

Indicates that a new software release has been downloaded into the E7, but the system has not yet been reset to run the new software release.

Recommended action

Note: Calix strongly recommends backing up the database before upgrading the system to new software.

Use either the "reset system" function or "reset system version" command to instruct the E7 to reset and run the new software release.

Alternatively, use either the "delete upgrade system" function or command if you choose not to run the newly-downloaded software release in the E7.

Severity

Warning, non-service-affecting

no-bp-data-path (No Backplane Data Path)

Indicates that there is no backplane data path between the two cards.

Recommended action

Change the backplane link setting.

Severity

Major, service-affecting

no-power (No Power)

Indicates that no power is detected for the object in the E7-20 system.

Recommended action

1. Verify the power cables and the power supply.
2. If the power is not correct, then adjust the provisioning for the power zone.

If this alarm occurs against a card or fan tray, then it is detecting a false failure as the object is receiving some power.

Severity

Critical, service affecting

no-standby-controller (No Standby Controller)

Indicates that the standby system controller is not ready to take control.

Recommended action

Troubleshoot the problem with the standby system controller.

Severity

Minor, non-service-affecting

no-tmg-card

Indicates that the card bank has no timing card present.

Recommended action

Install a card that supports timing into the system.

Severity

Major, non-service affecting

not-oper (Not Operational)

Indicates that the unit has not yet advanced to a fully provisioned state.

Recommended action

Wait for the unit to complete the startup process. If the alarm persists, report to Calix for resolution of the problem.

Severity

Critical, service-affecting

ntp-free-run (No NTP server is available)

Indicates that while one or more NTP servers are provisioned and the admin state is enabled, no NTP server can be reached.

Recommended action

For more information, see the recommended action for the server-specific alarms.

Severity

Major, non-service-affecting

ntp-srv1-down (NTP server-1 is not talking)

Indicates that server 1 is not available.

Recommended action

- Ensure a path exists by pinging the server.
- Ensure that NTP is running on the server.

Severity

Minor, non-service-affecting

ntp-srv2-down (NTP server-2 is not talking)

Indicates that server 2 is not available.

Recommended action

- Ensure a path exists by pinging the server.
- Ensure that NTP is running on the server.

Severity

Minor, non-service-affecting

ntp-srv3-down (NTP server-3 is not talking)

Indicates that server 3 is not available.

Recommended action

- Ensure a path exists by pinging the server.
- Ensure that NTP is running on the server.

Severity

Minor, non-service-affecting

ont-battery-failed (ONT Battery Failed)

Indicates that the battery is faulty and cannot be charged.

Recommended actions

Install a new battery.

Severity

Minor, non-service-affecting

ont-battery-low (ONT Battery is Low)

Indicates that the battery is low, which will soon cause the ONT to stop working.

Recommended action

Restore power to the affected area.

Severity

Minor, service-affecting

ont-battery-missing (ONT Battery is Missing)

The battery is missing from the backup battery unit.

Recommended action

Install a new battery.

Severity

Minor, non-service-affecting

ont-ds1-ais (Alarm Indication Signaling)

Indicates a 1.544 or 2.0 Mbit/s signaling alarm.

Severity

Major, service-affecting

ont-ds1-lof-m (Loss of Framing - Matrix)

Indicates a loss of T1 framing on the PON side.

Severity

Major, service-affecting

ont-ds1-los-lof (Loss of Signal or Loss of Framing)

Indicates that there is a loss of signal or loss of framing (T1 "red" alarm).

Severity

Major, service-affecting

ont-ds1-los-m (Loss of Signal - Matrix)

Indicates a loss of T1 signal on the PON side.

Severity

Major, service-affecting

ont-ds1-rai (Remote Alarm Indication)

Indicates the T1 "yellow" remote alarm.

Severity

Major, service-affecting

ont-eth-down (Loss of Link at ONT Ethernet Port)

Indicates that the link on this port is down.

Recommended action

Check the provisioning and connections on the port.

Severity

Major, service-affecting

ont-mismatch (ONT Provisioning/Equipment Mismatch)

The ONT port provisioning does not match the physical ports of the ONT.

Recommended Action

Update the ONT port provisioning to match the ONT port type.

Severity

Minor, non-service-affecting

ont-missing (ONT Went Missing)

Indicates that a previously provisioned ONT is no longer present on the PON (physical layer).

Recommended Action

- Ensure the ONT is connected and powered at the customer site.
- Ensure that the physical plant between the OLT and ONT is correctly installed.

Severity

Minor, service-affecting

ont-on-battery (ONT is on Battery Power)

The ONT is operating on battery backup power.

Recommended action

Restore power to the affected area.

Severity

Minor, non-service-affecting

ont-post-failed (ONT Self Test Failed)

One of the ONT startup diagnostic self tests failed.

Recommended action

Replace the ONT.

Severity

Minor, service-affecting

ont-prov-error (ONT Provisioning Error)

Indicates that an error has occurred when provisioning an ONT.

Recommended action

Repeat the ONT provisioning.

Severity

Minor, service-affecting

ont-rf-return-laser-eol (RF Return Laser End-of-Life)

The upstream laser for RF-Video Return is near its end-of-life.

Recommended action

Replace the ONT.

Severity

Minor, service-affecting

ont-rf-signal-bad (Downstream RF Signal is Bad)

The downstream RF-Video signal is missing from an enabled RF-Video port.

Recommended action

Check the RF-Video signal.

Severity

Minor, service-affecting

ont-rf-signal-low (Downstream RF Signal is Low)

With the RF Video Service enabled on at least one RF-video port, the downstream RF-video signal is low or missing.

Recommended action

Check the RF-video signal.

Severity

Minor, service-affecting

ont-post-failed

Indicates that one of the ONT startup diagnostic self tests failed.

Recommended action

Replace the failed ONT.

Severity

Minor, service-affecting

ont-sw-mismatch (ONT Software Mismatch)

Indicates that the ONT is running an unexpected software version, possibly caused by a failure during a software download.

Recommended action

Upgrade the ONT software.

Severity

Minor, non-service-affecting

pon-bandwidth-over-subscribed (PON Bandwidth Over-Subscribed)

Indicates the upstream bandwidth (CIR) is over-subscribed.

Recommended action

Reduce the CIR service bandwidth usage.

Severity

Major, service-affecting

pon-laser-eol (OLT PON laser end-of-life)

Indicates that the downstream laser on this PON port is near its end-of-life.

Recommended action

Replace the laser.

Severity

Major, service-affecting

pwe3 far-end loss of pwe3 packets (PWE3 FE LOS PKTS)

The PWE3 far-end indicates the loss of PWE3 packets.

Severity

Major, service-affecting

pwe3 far-end-loss of T1 signal (PWE3 FE LOS SIG)

The PWE3 far end indicates the loss of T1 framed signal.

Severity

Major, service-affecting

pwe3 malformed pwe3 packets (PWE3 Malformed)

Indicates that malformed PWE3 packets have been received.

Severity

Major, service-affecting

rel-not-commit (Release is not Committed)

Indicates that the software release currently running on the E7 is not committed as the default version. If the E7 temporarily loses power while in this condition, the system reverts back to running the previous software release.

Recommended action

Do ONE of the following:

- Use the "Commit System" function or command to make the currently running software release the default software that loads when the system is reset.
- Use the "Revert System" function or command to make the previously running software release the default software that loads when the system is reset.

Severity

Warning, non-service-affecting

restore-file-exists (Restore file exists)

Indicates that an archived database backup file has already been retrieved using the "load backup" function or command.

Recommended action

Use either the "switch database" function or command to switch to the restored backup database file. When the operation completes, the alarm automatically clears.

Alternatively, if you choose not to use the newly-restored database backup file, use either the "delete backup" function or command to delete the backup file, clearing the alarm.

Severity

Warning, non-service-affecting

rfc-2544-lpbk (RFC 2544 Loopback)

Indicates an RFC 2544 loopback is in effect for the address on the specified VLAN in dynamic data.

Recommended action

Issue the **`test rfc2544-loopback stop`** command or action to stop the loopback.

Severity

Major, service-affecting

rdi: crit-alarm (Remote Failure Indication: Critical Alarm)

Indicates an 802.3ah failure in the form of a remote critical alarm.

Recommended action

None

Severity

Major, non-service affecting

rfi: dying-gasp (Remote Failure Indication: Dying Gasp)

Indicates an 802.3ah failure in the form of a dying gasp.

Recommended action

None

Severity

Major, non-service affecting

rfi-sig-loss (Remote Failure Indication: Loss of Receive Signal)

Indicates an 802.3ah failure in the form of a remote loss of signal.

Recommended action

None

Severity

Major, non-service affecting

rstp-fault (RSTP Fault on Interface)

Indicates that an interface is configured for RSTP, but the remote side of the Ethernet interface is not participating in the protocol and may allow for routing loops.

Recommended action

- Check the integrity of the port connection.
- Check the RSTP provisioning of the Ethernet interface on the remote side.

Severity

Minor, non-service-affecting

rstp-multi-pri (RSTP Prot: Multiple Primaries)

Indicates that multiple E7s using the same Node Protection ID are provisioned with the Node Protection Role designated as "Primary."

Recommended action

Correct the provisioning so that the following conditions exist for each pair of node protected E7s:

- The same unique Node Protection ID value is assigned.
- One E7 has the Node Protection Role designated as "Primary" and the other E7 has the Node Protection Role designated as "Secondary."

Severity

Minor, non-service-affecting

rstp-multi-sec (RSTP Prot: Multiple Secondaries)

Indicates that multiple E7s using the same Node Protection ID are provisioned with the Node Protection Role designated as "Secondary."

Recommended action

Correct the provisioning so that the following conditions exist for each pair of node protected E7s:

- The same unique Node Protection ID value is assigned.
- One E7 has the Node Protection Role designated as "Primary" and the other E7 has the Node Protection Role designated as "Secondary."

Severity

Minor, non-service-affecting

rstp-no-pri (RSTP Prot: No Primary Node)

Indicates that while the E7 is part of a RSTP protection pair and has the Node Protection Role designated as "Secondary," it cannot communicate with an E7 that has the Node Protection Role designated as "Primary."

Recommended action

- Ensure that there is an E7 with the Node Protection Role designated as "Primary."
- Ensure that fibers are connected correctly in the network.

- Ensure that the Node Protection ID value is the same on the two E7s that comprise the node protection pair.

Severity

Minor, non-service-affecting

rstp-no-sec (RSTP Prot: No Secondary Node)

Indicates that while the E7 is part of a RSTP protection pair and has the Node Protection Role designated as "Primary," it cannot communicate with an E7 that has the Node Protection Role designated as "Secondary."

Recommended action

- Ensure that there is an E7 with the Node Protection Role designated as "Secondary."
- Ensure that fibers are connected correctly in the network.
- Ensure that the Node Protection ID value is the same on the two E7s that comprise the node protection pair.

Severity

Minor, non-service-affecting

shelf-error (Shelf Error)

Indicates an error has been detected in the configuration of a shelf that is in a Modular Chassis system.

Recommended action

- Disconnect the link on the port reporting the error, if the remote shelf belongs to a different system.

Or

- Modify the provisioning so that the remote shelf can be accepted.

Severity

Minor, non-service-affecting

shelf-ring-port-down (Shelf Ring Port Down)

Indicates that a local stacking ring interface is down on a Modular Chassis (MC).

Recommended action

- Verify that the direct attach cables are securely fastened to the stacking ports on each shelf in the modular chassis.
- Verify that the stacking port provisioning is correctly configured for each shelf in the modular chassis.

Severity

Major, non-service-affecting

software-initialization-in-progress (Software Initialization in Progress)

The software initialization process is taking place.

Recommended action

Wait for the current process to complete and the alarm to clear before attempting any actions that are related to a software upgrade.

Severity

Warning, non-service affecting

stacking-ring-health-compromised (Stacking Ring Health Compromised)

Stacking ring health is compromised.

Recommended action

Contact Calix Technical Assistance for resolution of condition.

Severity

Major, non-service-affecting

svc-with-no-facility (No Ethernet Ports for Service)

Indicates that the interface has provisioned services with no Ethernet ports assigned.

Recommended action

Do one of the following:

- Disable the interface.
- Remove the service provisioning.
- Assign an Ethernet port to the interface.

Severity

Major, service-affecting

switch-control-fault (Switch Control Fault)

Indicates that an attempt to update the switch fabric failed.

Recommended action

Notify Calix of the occurrence of this alarm.

Severity

Critical, service-affecting

switching-power-supply-a-failed (Switching Power Supply A Failed)

Indicates that a failure has been detected in switching power supply A of the alarmed fan tray.

Recommended action

Replace the fan tray.

Severity

Minor, non-service-affecting

switching-power-supply-b-failed (Switching Power Supply B Failed)

Indicates that a failure has been detected in switching power supply B for the alarmed fan tray.

Recommended action

Replace the fan tray.

Severity

Minor, non-service-affecting

timing-failed-device (Timing Device Failed)

Indicates that a failure has been detected in the circuitry that derives the timing for the E7.

Recommended action

Replace the card that is reporting the failure.

Severity

Minor, non-service-affecting

timing-failed-source-a (Timing Source A Failed)

Indicates that the alarmed card detects the timing source A as degraded or failed.

Recommended action

The failure can either be at the timing source or the card. If only one card reports the failure in a duplex system, replace the card that is reporting the failure.

Severity

Minor, non-service-affecting

timing-failed-source-b (Timing Source B Failed) [E7]

Indicates that the alarmed card detects the timing source B as degraded or failed.

Recommended action

The failure can either be at the timing source or the card. If only one card reports the failure in a duplex system, replace the card that is reporting the failure.

Severity

Minor, non-service-affecting

timing-freerun (Timing is Free-Running)

Indicates that the timing subsystems in the E7 have never had a valid timing source.

Recommended action

Correct the problem that is preventing the timing source from reaching the E7.

Severity

Critical, service-affecting

timing-holdover (Timing is in Holdover)

Indicates that the timing subsystems in the E7 do not currently have a valid timing source.

Recommended action

Correct the problem that is preventing the timing source from reaching the E7.

Severity

Minor, non-service-affecting

timing-locked-a (Timing locked on Source A)

Indicates that the timing subsystem on the alarmed card is locked on timing source A.

Severity

Information, non-service-affecting

timing-locked-b (Timing locked on Source B)

Indicates that the timing subsystem on the alarmed card is locked on timing source B.

Severity

Information, non-service-affecting

too-cold (Card too cold)

Indicates that the temperature sensed by the system has fallen below the acceptable operating range.

Recommended action

Ensure that the system cabinet is properly closed. The alarm occurs when the operating temperature is below –45 degrees and it clears when the operating temperature moves above 3–7 degrees.

Severity

Minor, non-service-affecting

too-hot (Card overheating)

Indicates that the temperature sensed by the system is approaching or exceeding the acceptable maximum operating temperature.

Recommended action

Examine the system cabinet and unit to determine the cause of the air-flow failure. The alarm occurs when the operating temperature is above 85 degrees and it clears when the operating temperature moves below 82 degrees.

Severity

Major, non-service-affecting if the temperature is in the maximum operating temperature range of 82 to 86 degrees.

Critical, non-service-affecting if the temperature has exceeded the maximum operating temperature of 87 degrees.

ueq (Unequipped)

Indicates one of the following conditions:

- A removable component, such as the E7 fan tray, has been removed.
- A removable component has failed.

Recommended action

- Add the missing component to the E7.

  or

- Replace the failed E7 component.

Severity

Critical, service-affecting

unrecognized-sfp (Unrecognized SFP)

Indicates that the SFP module is not in the group of modules officially supported by Calix and may not perform optimally.

Recommended action

Replace the SFP module with an officially supported Calix SFP. For part information, see the following Calix Quick Tip bulletins on the Calix website for information on the support for SFP modules and direct attach cables:

- *Calix Equipment Support for SFP Modules*
- *Pairing Bidirectional SFPs to Support Single-Fiber Ethernet Links*

Severity

Major, service-affecting

unsupp-eq (Unsupported Equipment)

Indicates that an uncertified XFP or SFP+ connector was inserted into the E7.

Recommended action

Replace the uncertified XFP or SFP+ connector with one certified by Calix. For part information, see the following Calix Quick Tip bulletins on the Calix website for information on the support for SFP modules and Direct Attach cables:

- *Calix Equipment Support for SFP Modules*
- *Pairing Bidirectional SFPs to Support Single-Fiber Ethernet Links*.

Severity

Major, service-affecting

upgr-in-progress (Software Upgrade in progress)

Indicates that a new software release is currently being downloaded into the E7.

Recommended action

Wait for the download operation to complete, which automatically clears the alarm.

Alternatively, either use the "delete upgrade system" function or command to abort the download operation while it is in progress.

Severity

Warning, non-service-affecting

voip-down (VOIP is unavailable)

VoIP is unavailable.

Recommended action

- Reseat the VDSL2-48C card in the chassis connector.
- If the condition persists, replace the card.

Severity

Critical, service-affecting

voip_line_registration_failure (VOIP line registration failure)

A VoIP line has failed to register.

Recommended action

- Check the provisioning.
- Verify the uplink connectivity.

Severity

Major, service-affecting

voip-low-sw-res (VOIP Low SW Resources)

Indicates excessive consumption of software resources (memory, CPU time, or file space).

Recommended action

Contact Calix Technical Assistance for resolution of condition.

Severity

Minor, service-affecting

XDSL-group-LOS (XDSL Group LOS)

The Loss of Signal (LOS) indicates that the group bonding protocol is not funtioning.

Recommended action

- Ensure that one or more member ports are trained up.
- Verify that the group is operating in the correct bonding scheme (ATM or PTM), and matches the modem to which the group is connected.

Severity

Major, service-affecting

XDSL-group-low-rate-downstream (XDSL Group Low Rate Downstream)

The group is operating at a downstream rate that is lower than the provisioned minimum rate.

Recommended action

Ensure that all member ports are trained up and operating in the correct mode and at the expected rate. Or, reduce the group provisioned downstream minimum rate threshold.

Severity

Major, service-affecting

XDSL-group-low-rate-upstream (XDSL Group Low Rate Upstream)

The group is operating at an upstream rate that is lower than the provisioned minimum rate.

Recommended action

Ensure that all member ports are trained up and operating in the correct mode and at the expected rate. Or, reduce the group provisioned upstream minimum rate threshold.

Severity

Major, service-affecting

XDSL-group-provisioning-failure (XDSL Group Provisioning Failure)

The group provisioning was not successfully written to xDSL hardware.

Recommended action

Remove recent changes to the provisioning, returning to the previous state. Or, modify the provisioning until the alarm clears.

Severity

Critical, service-affecting

XDSL-port-provisioning-failure (XDSL Port Provisioning Failure)

The port provisioning was not successfully written to xDSL hardware.

Recommended action

Remove recent changes to the provisioning, returning to the previous state. Or, modify the provisioning until the alarm clears.

Severity

Critical, service-affecting

Environmental Alarms

The topics in this section describe the conditions and/or equipment that can be monitored from provisioning the E7 rear panel alarm interface module. See the applicable Installation Guide for instructions on how to wire external environmental alarms and audible alarms.

Note: See Element Alarms for information on the possible causes of E7 element alarms and the recommended actions that you should take to clear the conditions that have caused the alarm.

To provision the environmental alarms

1. On the Navigation Tree, click **E7**.
2. In the Work Area, click **Environment**.
3. Double-click the environmental alarm pin to provision.

   Note: EnvPin:1 - EnvPin:8 correlate to Alarm Pins AL0 - AL7 on the alarm interface located on the rear of the E7.

4. In the Environment Pin number dialog box, do the following:
   a. In the admin list, select whether to enable the pin.
   b. In the pin-type list, select whether the pin is an input or output.
   c. In the polarity list, select whether the pin contact is normally open or closed.
   d. In the alarm-type list, select the environmental alarm as described in the remaining topics in this section.
   e. In the severity list, select the level of importance for the alarm.
5. Click **Apply**.

air-compr-fail (Air Compressor Failure)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

air-cond-fail (Air Conditioning Failure)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

air-dry-fail (Air Dryer Failure)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

batt-discharge (Battery Discharging)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

batt-fail (Battery Failure)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

central-pwr-fail (Centralized Power Failure)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

comm-pwr-fail (Commercial Power Failure)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

contact-off-normal (Contact Off-Normal)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

cool-fan-fail (Cooling Fan Failure)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

eng-fail (Engine Failure)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

eng-oper (Engine Operating)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

expl-gas (Explosive Gas)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

fire (Fire)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

fire-detect-fail (Fire Detector Failure)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

flood (Flood)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

fuse-fail (Fuse Failure)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

gen-fail (Generator Failure)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

high-airflow (High Air Flow)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

high-humidity (High Humidity)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

high-temp (High Temperature)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

high-water (High Water)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

intrusion (Intrusion)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

low-batt-volt (Low Battery Voltage)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

low-cable-pressure (Low Cable Pressure)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

low-fuel (Low Fuel)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

low-humidity (Low Humidity)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

low-temp (Low Temperature)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

low-water (Low Water)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

misc (Miscellaneous)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

open-door (Open Door)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

power (Power)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

power-a-fail (Power A Failure)

Indicates an Environmental input pin assigned to this alarm or a card detects a failure to receive power from battery A.

Recommended action

Ensure that the battery is properly connected.

Severity

Major, non-service-affecting

power-b-fail (Power B Failure)

Indicates an Environmental input pin assigned to this alarm or a card detects a failure to receive power from battery B.

Recommended action

Ensure that the battery is properly connected.

Severity

Major, non-service-affecting

pump-fail (Pump Failure)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

rect-fail (Rectifier Failure)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

rect-high-volt (Rectifier High Voltage)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

rect-low-volt (Rectifier Low Voltage)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

security (Security)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

smoke (Smoke)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

thermal (Thermal)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

toxic-gas (Toxic Gas)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

vent-fail (Ventilation Failure)

Indicates an Environmental input pin assigned to this alarm detects a problem condition.

Recommended action

Correct the cause of the detected condition.

Severity

Major, non-service-affecting

Events

The topics in this section describe the possible causes of E7 event notification.

ae-ont-discovered (AE ONT Discovered)

An Active Ethernet (AE) Ont has been discovered by the system.

auto-upgr-fail-commit (Auto Upgrade: Failed to Commit)

The automatic software upgrade process of a E7 line card failed to complete due to the inability to commit to the requested software version.

auto-upgr-fail-run (Auto Upgrade: Wrong Release)

The automatic software upgrade process of a E7 line card did not complete due to the inability to reset and run the new software version.

auto-upgr-fail-trans (Auto Upgrade: Failed File Xfer)

The automatic software upgrade process of a E7 line card did not complete due to a failure during the new software version download.

auto-upgr-in-prog (Auto Upgrade: In Progress)

The automatic software upgrade of a E7 line card is in progress.

auto-upgr-succ (Auto Upgrade: Success)

The automatic software upgrade of a E7 line card was successful.

auto-upgr-too-many-failures (Auto Upgrade: Too many failures)

The automatic software upgrade process will not be attempted due to too many previously occurring failures.

cancel-reset-in-prog (Cancel Reset: In Progress)

A requested cancellation of the card reset sequence has been initiated.

cancel-reset-succ (Cancel Reset: Complete)

The card reset sequence has been cancelled successfully.

cancel-upgr-fail (Cancel Upgrade: Failed)

The requested cancellation of the software upgrade process failed.

cancel-upgr-had-errs (Cancel Upgrade: Had Errors)

A requested cancellation of the software upgrade process failed.

cancel-upgr-in-prog (Cancel Upgrade: In Progress)

A cancellation of the software upgrade process is initiated.

cancel-upgr-succ (Cancel Upgrade: Complete)

A cancellation of the software upgrade process is successfully completed.

card-arrived (Card Event: Arrival)

A newly-installed E7 line card is detected.

card-departed (Card Event: Departure)

An E7 line card has been disconnected from the system.

card-migration-upgrade (Performing Migration Upgrade)

The software on the card is being upgraded via the migration upgrade sequence because the card was running a software release that is incompatible with the current software release running on the system.

commit-fail-commit (Commit: Failed)

A requested "commit" action failed due to the inability to commit to the requested software version.

commit-had-errs (Commit: Had Errors)

A requested "commit" action failed due to errors that occurred.

commit-in-prog (Commit: In Progress)

A "commit" action has been initiated.

commit-succ (Commit: Success)

A requested "commit" action completed successfully.

db-reset (Database Reset)

The database has been reset to the default configuration by request.

delete-upgr-fail (Delete Upgrade: Failed)

A requested cancellation of the software upgrade failed.

delete-upgr-had-errs (Delete Upgrade: Had Errors)

A requested cancellation of the software upgrade failed.

delete-upgr-in-prog (Delete Upgrade: In Progress)

A cancellation of the software upgrade has been initiated.

delete-upgr-succ (Delete Upgrade: Complete)

A requested cancellation of the software upgrade completed successfully.

erps-proto-viol (ERPS Protocol Violation)

A received Ethernet Ring Protection Switching (ERPS) PDU had an error and was discarded.

erps-invalid-prov (ERPS Invalid Provisioning)

The internal Ethernet Ring Protection Switching (ERPS) stack received invalid provisioning information and was discarded. Notify Calix of this event.

fast-igmp-ring-vlan-prov-err (Fast IGMP Ring VLAN Provisioning Error)

A VLAN mapped to the domain is not configured with IGMP snooping enabled.

igmp-group-limit-reached (IGMP Snooping Group Limit Reached)

The IGMP Snooping ability supports a maximum of 800 multicast groups to be snooped across all VLANs in the system at any given point in time. This event is emitted when that limit is reached. Additional attempts to join a multicast group are denied until one or more existing groups are released and multicast entrys are available for use.

ont-arrival (ONT Event: Arrival)

A newly-installed ONT has been detected by the system.

ont-dbg-upgr-fail (ONT Debug Upgrade: Failed)

A requested action for debugging an ONT upgrade has failed.

ont-dbg-upgr-had-errs (ONT Debug Upgrade: Had Errors)

A requested action for debugging an ONT upgrade has failed due to errors occurring.

ont-dbg-upgr-in-prog (ONT Debug Upgrade: In Progress)

A debugging ONT upgrade action is initiated.

ont-dbg-upgr-succ (ONT Debug Upgrade: Complete)

A debugging ONT upgrade action has successfully completed.

ont-departure (ONT Event: Departure)

An ONT has been disconnected from the system.

ont-eth-local-lpbk-end (Local Loopback End)

The ONT Ethernet port is no longer in local loopback.

ont-eth-local-lpbk-start (Local Loopback Start)

An ONT Ethernet port has been placed into local loopback.

ont-eth-rmt-lpbk-end (Remote Loopback End)

The ONT Ethernet port is no longer in remote loopback.

ont-eth-rmt-lpbk-start (Remote Loopback Start)

An ONT Ethernet port as been placed into remote loopback.

ont-link (ONT Event: Link)

A discovered ONT has been linked to a provisioning record.

ont-pre-arrival (ONT Event: Pre-Arrival)

An ONT is beginning the ranging process, which takes place as part of the ONT discovery process.

ont-unlink (ONT Event: Unlink)

An ONT has become unlinked from a provisioning record.

reboot-fail-run (Reboot: Failed)

A requested reboot of the E7 failed due to the inability to reboot and run the committed software version.

reboot-had-errs (Reboot: Had Errors)

A requested reboot of the E7 had errors.

reboot-in-prog (Reboot: In Progress)

A reboot of the E7 has been initiated.

reboot-succ (Reboot: Success)

A reboot of the E7 has completed successfully.

reset-fail-run (Reset: Failed)

A requested reset of the E7 failed due to the inability to reset and run the requested software version.

reset-had-errs (Reset: Had Errors)

A requested reset of the E7 failed due to errors that occurred.

reset-in-prog (Reset: In Progress)

A reset of the E7 has been initiated.

reset-succ (Reset: Success)

A reset of the E7 completed successfully.

restore-had-errs (Database Restore: Had Errors)

Activation of a restored database (from the **`switch database`** command) failed. Possible reasons for the failure:

- The restored database belongs to a different E7 node.
- The format of the restored database is not supported by the current E7 release.

restore-in-prog (Database Restore: In Progress)

Activation of a restored database has been initiated from the **`switch database`** function or command.

restore-succ (Database Restore: Success)

Activation of a restored database (from the **`switch database`** function or command) completed successfully.

revert-fail-commit (Revert: Failed to Commit)

A requested "revert" action failed due to the inability to mark the requested software version as being committed.

revert-fail-run (Revert: Wrong Release)

A requested "revert" action failed due to the inability to reset and run the requested software version.

revert-had-errs (Revert: Had Errors)

A requested "revert" action failed due to errors that occurred.

revert-in-prog (Revert: In Progress)

A "revert" action has been initiated.

revert-succ (Revert: Success)

A requested "revert" action completed successfully.

time-set (Time Set For Slot)

The system time has been initially set.

stk-ring-invalid-prov (Stacking Ring Invalid Provisioning)

The Stacking Ring received invalid provisioning information and discarded it. Notify Calix of this event.

stk-ring-proto-viol (Stacking Ring Protocol Violation)

A received Stacking Ring PDU had an error and was discarded. Notify Calix of this event.

stk-ring-vlan-prov-err (Stacking Ring VLAN Provisioning Error)

A VLAN that is mapped to the Stacking Ring is not configured with IGMP Snooping enabled. Notify Calix of this event.

stp-buf-alloc-fail (STP Buffer Allocation Failure)

Internal resources used for RSTP protocol processing have been temporarily depleted.

stp-invalid-bpdu (STP Invalid BPDU)

A malformed RSTP BDPU packet has been received on the E7 interface.

stp-mem-alloc-fail (STP Memory Allocation Failure)

Internal resources used for RSTP protocol processing have been temporarily depleted.

stp-new-port-role (STP New Port Role)

The RSTP Role (disabled / alternate / backup / root / designated) of this E7 interface has changed.

stp-new-root (STP New Root)

A new node has been elected to be the root node within the spanning tree where this E7 is located.

stp-proto-migr (STP Protocol Migration)

The E7 is receiving STP (as opposed to RSTP) BPDU packets from the node connected to the specified interface.

stp-topo-ch (STP Topology Change)

A change to the spanning tree topology has been detected.

switchover-abort (Switchover: Aborted)

A redundant switchover is aborted.

switchover-in-prog (Switchover: In Progress)

A redundant switchover is initiated.

switchover-succ (Switchover: Complete)

A redundant switchover has successfully completed.

system-time-set (Time Set For System)

The system time was updated.

upgr-fail-run (Upgrade: Reset error)

A E7 software upgrade process failed due to the inability to reset and run the new software version.

upgr-fail-trans (Upgrade: Failed File Xfer)

A E7 software upgrade process did not complete due to failure during the new software version download.

Recommended action

Verify that the following parameters are correct:

- The IP address of the FTP server.
- The username and password on the upgrade server.
- The directory path to the location on the upgrade server where the new software files are located.
- If using a previously-installed FTP server application on your PC, the root directory location set in the FTP server.

When using the automatic method for installing the downloaded zip file, the installer places the E7 upgrade file contents in the following directory and installs the FTP server with the directory set to same directory on your PC:

C:\CalixESeries\software

If you are using the FTP server application that is automatically installed on your PC, enter a dot character (.) to indicate the default directory that is automatically created with the unzip process of the upgrade file.

upgr-had-errs (Upgrade: Had Errors)

An E7 software upgrade process did not complete due to errors occurring.

vlan-mac-learn-thres (VLAN MAC Learning Threshold)

The number of MAC table entries for this interface has reached the maximum value allowed (32000). No additional MAC addresses will be learned.

Appendix A

Reference Information

This appendix provides general reference information about the Calix E7 Ethernet service access platform.

Topics Covered

This appendix covers the following topics:

- System limits
- LED behavior in boot sequence
- Additional status descriptions for line cards
- Using the E7 cut-through Telnet or web interface

System Support Capacities

The Calix E7 system support capacities follow.

General System Support

- 100 user accounts, locally defined (not in the RADIUS)
- 15 simultaneous Netconf sessions for web browser interface
  - The Netconf interface has a 30 minute timeout, which cannot be turned off. The web browser interface has an inactivity timer of approximately 30 minutes.
- 5 simultaneous CLI sessions
  - There is an ENABLE/DISABLE flag in the CLI for session timeout, but the only ENABLE timeout duration supported is 30 minutes.

    There might temporarily be an extra Netconf (16) and an extra CLI session (6), for just the duration of the login process. If the extra session is accepted, then a previous, oldest session is dropped under the assumption that this session is most likely to be idle.
- 5 SNMP Trap destinations (defined by IP address)
- RADIUS
  - 4 authentication RADIUS servers and 4 accounting RADIUS servers are supported
  - All of the authentication RADIUS servers are assumed to have the same authentication information, that is, server replication. The system communicates with the "best" server, and then only sends to the next server if it does not get a response. Where "best" is determined by the success rate of getting responses to recent requests.
- At least 32,000 MAC addresses (E7 line cards share common table)
- VLANs
  - 4090 VLANs (VLANs 1002, 1003, 1004, and 1005 are reserved for system use but can be changed to another range, 1 is untagged)
  - 1 Default Internal VLAN (GE and 10GE ports only)

    This VLAN is utilized to switch all untagged traffic through the system. This VLAN cannot be deleted, but can be changed. Not supported on ONT Ethernet ports.
  - 768 Tag Actions per card (ONT service tag actions are not included in this limit)
  - 48 or fewer VLANs may be set to DHCP Snoop or Proxy (E7-2 only)
  - 24 VLANs or fewer may have a PPPoE profile assigned (E7-2 only)
  - 8 VLANs or fewer in total may have MAC-Forced-Forwarding and/or IP-Src-Verify enabled (E7-2 only)
- 10Gig SFP+/XFP modules and GPON Optical Interface Modules (OIMs) must be keyed

- Ethernet services:
  - 6 Ethernet services allowed on an xDSL port
  - 8 Ethernet services allowed on an ONT Ethernet port
  - 24 or fewer services on a VDSL card may resolve to a VLAN marked as TLAN (This includes the same TLAN on multiple services.)
- Ethernet Frame Size:

  The E7 supports the ability to set the MTU Maximum Transmission Unit size (bytes) on a GE and 10GE port interface to a maximum or 9000 bytes. GPON ONTs and xDSL ports have a fixed MTU value.
  - MTU = 9000 bytes (E7 Ethernet interfaces)
  - MTU = 2000 bytes (700GE and 760GX GPON ONTs)
  - MTU = 1600 bytes (700GX GPON ONTs)
  - MTU = 1500 bytes (E7 xDSL ports)

  The MTU is defined as the maximum size payload of the Ethernet frame, not the Ethernet frame size. In an IP network, this is the largest IP packet that can be transmitted on the Ethernet network without IP packet fragmentation. The Ethernet frame size varies depending on the number of VLAN tags applied to the payload, plus allowances for Preamble/Delimiter and interframe gap.

  + 8 bytes (Preamble/Delimiter)

  + 14 bytes (header not including VLAN tags)

  + 4 bytes (inner VLAN tag)

  + 4 bytes (outer VLAN tag)

  + 4 bytes (trailer)

  + 12 bytes (interframe gap)

  For example:
    - 2000 bytes = MTU
    - 2026 = Max Ethernet frame (with two VLAN tags without Preamble/Delimiter)
    - 2034 = Max Ethernet frame (with two VLAN tags including Preamble/Delimiter)
    - 2046 = Max Ethernet frame (with two VLANs, preamble/Delimiter, and Interframe Gap)

  Maximum throughput

  - To calculate the protocol efficiency for Ethernet:

    Protocol efficiency = Payload size ÷ Frame size

    Maximum efficiency is achieved with the largest allowed payload size.

For example:

1500 bytes (Maximum payload size)

+ 8 bytes (preamble)

+ 14 bytes (header)

+ 4 bytes (trailer)

+ 12 bytes (interframe gap)

= 1538

1500 (payload size) ÷ 1538 (frame size) = 97.53%

- To calculate efficiency for optional 802.1Q tagged Ethernet packets, include 4 bytes in the frame size:

  1500 (payload size) ÷ 1542 (frame size) = 97.28%

- To calculate the protocol overhead for Ethernet as a percentage:

  Protocol overhead = 1 — Protocol efficiency

- To calculate the IP payload throughput:

  Payload Throughput = Efficiency * Net bit rate

  Where the physical layer net bit rate (the wire bit rate) depends on the Ethernet physical layer standard, and may be 10 Mbit/s, 100 Mbit/s, 1 Gbit/s or 10 Gbit/s. Maximum throughput for 100BASE-TX Ethernet is consequently 97.53 Mbit/s without 802.1Q, and 97.28 Mbit/s with 802.1Q.

- ERPS ring
  - 6 ERPS rings per E7-2 system
  - 2 ERPS rings per E7-20 system
  - 2 ERPS rings per VDSL card
  - 1 ERPS domain per E7 interface
  - 32 "units" per ERPS ring

    This number counts all E7 cards located in the ring whether in a dual or single card E7 shelf. This number does not include devices or E7 subtended from the ring.
  - 3 interconnected rings for a "chain of ERPS rings"
  - E5-400/E7-2 counts as 1 unit
  - E7-2 line card counts as 1 unit (up to 2 units per E7-2 shelf)
- 800 Broadcast Video channels using IGMP snooping

- Link Agg Groups
  - 6 Link Aggregation Groups per shelf using GE ports
  - 8 ports per Link Aggregation Group using GE ports
  - 2 Link Aggregation Groups per shelf using 10GE ports
  - 4 ports per Link Aggregation Group using 10GE ports
- Bandwidth Policing for GE and 10GE ports is 1 Mbps up to line rate
- 8 Egress Priority Queues per 1GE or 10GE port (not ONT Ethernet ports!)

  Based on P-bit value with P-bit = 7 highest priority
- Queue Scheduling Algorithm is a strict priority across 8 queues, with maximum and minimum guaranteed bandwidth per class. Tail drop is used when dropping packets from queue.
- 1500 Traffic Rate Limiters per E7 card
  - 1500 independent policy rules
  - Supports 1500 per card with RSTP protection
- Ethernet port mirrors per node: 1
- Profiles and templates per E7
  - 256 Policy Maps
  - 1500 Policies per Policy Map
  - 24 Policy Map Match entries for a VDSL card
  - 1536 Policy Map Match entries for all other card types
  - 1500 Class Maps
  - 100 Class Rules per Class Map
  - 300 subscriber bandwidth profiles (GPON and VDSL together)
  - 32 multicast profiles
  - 5 MVR profiles
  - 255 match lists (GPON and VDSL together)
  - 256 service tag actions
  - 264 VDSL port templates
  - 512 SIP profiles
  - 512 SIP Gateway Profiles (VDSL)
  - 32 TDM Gateway profiles
  - 20 dial plans
  - 8 Ds1PWE3 profiles

- 10 DSCP maps
- 10 IP Precedence maps
- 20 H.248 Gateway profiles
- 20 MGCP Gateway profiles
- 4 ONT PWE3 profiles
- 200 ONT profiles
- 50 PPPoE profiles
- 20 VLAN IGMP profiles
- 16 security profiles
    - security profiles used by VDSL interfaces (including bonded-Links) must have DHCP lease limt = 10 or less

E7 LED Behavior

Line card LEDs

- Service (SRVC) indicates at least 1 port has been provisioned on this slot
- Control (CTRL) green LED indicates active controller, amber LED indicates standby controller
- Fault (FAIL) red LED indicates the card is in fault
- Cards have additional LED states at boot time (see table below)

Port LEDs

- Green LED (Ethernet) that stays on indicates a link with no activity, flashes during activity.
- Green LED (GPON port) that stays on indicates at least 1 ONT is ranged, blinks when the first ONT is ranging.
- Green LED (DSL port) that stays on indicates at least one DSL subscriber port is synched up and operating correctly (the system is up, operational, and ready to or able to pass traffic).
- Green LED (POTS port - VDSL2-48C only) that stays on indicates, indicates at least one POTS subscriber port is operating correctly (the system is up, operational, and is off-hook).
- Red LED (10GE) indicates a module is inserted into a port that is redirected to the backplane.
- Inserting a supported module into a port causes the LED to blink green 3 times, indicating module recognition.
- If no blinking occurs on module insertion, the module is not supported/recognized; An alarm is present in this situation.

Line card LED boot sequence

CTRL LED	SRVC LED	FAIL LED	State Description
Active Card Boot Sequence			
Green	Yellow	Red	Power on
off	Off	Red	NB Execution
1 short green	Off	Red	UB Execution
2 short green	Off	Red	Booting Kernel
3 short green	Off	Red	Application Loading
2 short, 1 long green	Off	Off	Application Initializing
1 short, 1 long green	Off	Off	Database Loading
Green 1 Short Off	Off	Off	Database Activation
Green	Off	Off	Application Startup complete, no services defined
Green	Green	Off	Application startup complete, services defined
Standby Card Boot Sequence			
Green	Yellow	Red	Power On
Off	Off	Red	NB Execution
1 Short Yellow	Off	Red	UB Execution
2 Short Yellow	Off	Red	Booting Kernel
3 Short Yellow	Off	Red	Application Loading
2 Short 1 Long Yellow	Off	Off	Application Initializing
1 Short 1 Long Yellow	Off	Off	Database Loading
Yellow 1 Short Off	Off	Off	Database Activiation
Yellow	Off	Off	Application Startup complete, no services defined
Yellow	Green	Off	Application startup Complete, services defined
Other States			
Off	Off	All Short Red	Equipment Mismatch
Green blinking	Yellow blinking	Red blinking	E7-20 card inserted in E7-2
Pattern & Color Reflects Card Status	All Short Yellow	Off	Flash Write in Progress (database or program update)
Off	Off	2 Short Red	Application Initiated Shutdown
Green	Pattern & color Reflects Service and Flash Write	Red	Equipment Failure for Active Card
yellow	Pattern & color Reflects Service and Flash Write	Red	Equipment Failure for Standby Card
1 Short Green	Off	Off	No Database in Flash on Active Card
1 Short Yellow	Off	Off	No Database in Flash on Standby Card
Off	Off	2 Short 1 Long Red	Waiting for card to cool down before loading application

E7 Line Card Additional Status Descriptions

The table below shows the possible states for an E7 line card Additional Status.

Line Card Additional Status	Description
default-prov	Indicates that the object's parameters have never been changed from default values.
child-prov	Indicates that the object has subtending records provisioned. these may be ports or interfaces that have been updated by the user.
present	Indicates that the object is present.
system-disabled	Indicates an object has a service affecting alarm reported against it, or any of its parents. For example: • An ONT parent is the system object. • A Card parent is the shelf, and then the system.
user-disabled	Indicates an object is disabled by the user (Admin status = disabled).
degraded	Indicates an object (ONT or a Card) has a non-service affecting alarm reported against it.
active	Indicates that the card is the system controller which manages alarms, configuration, and performance monitoring. A "*" is shown next to the card label in the web interface and in the CLI **show card** command results.
standby	Indicates the card is in standby status.

Note: If the card has the default-prov state and does not have the child-prov state, this indicates that the card hierarchy is completely default and will be deleted from the database upon card departure.

Using the E7 Cut-Through Telnet or Web Interface

With the CMS Desktop cut-through feature, you can start a Telnet or web session to do the following:

- Work in the web interface or command line interface (CLI) mode to perform provisioning commands.
- Provision a higher (later) version of software through the CMS server, even though such nodes have not been tested on, and may not work with, the current CMS software server version.

CMS supports a maximum of 15 Web Interface cut-through sessions and 5 Telnet CLI sessions for each E5-400 or E7 node.

Cut-through sessions require Full CMS Administration privileges and Full Provisioning privileges for the node on which you want to establish a connection.

To open to a Telnet session

1. On the Navigation Tree, click a region or network group.
2. In the Work Area, click **Network Details**, and then click the E5-400 or E7.
3. In the Display Name column, right-click the node.
4. From the pop-up menu, select one of the following:
   - **Cut-Through Web** to open a CMS Cut-Through Web window.
   - **Cut-Through Telnet** to open a CMS Telnet Cut-Through CLI window.