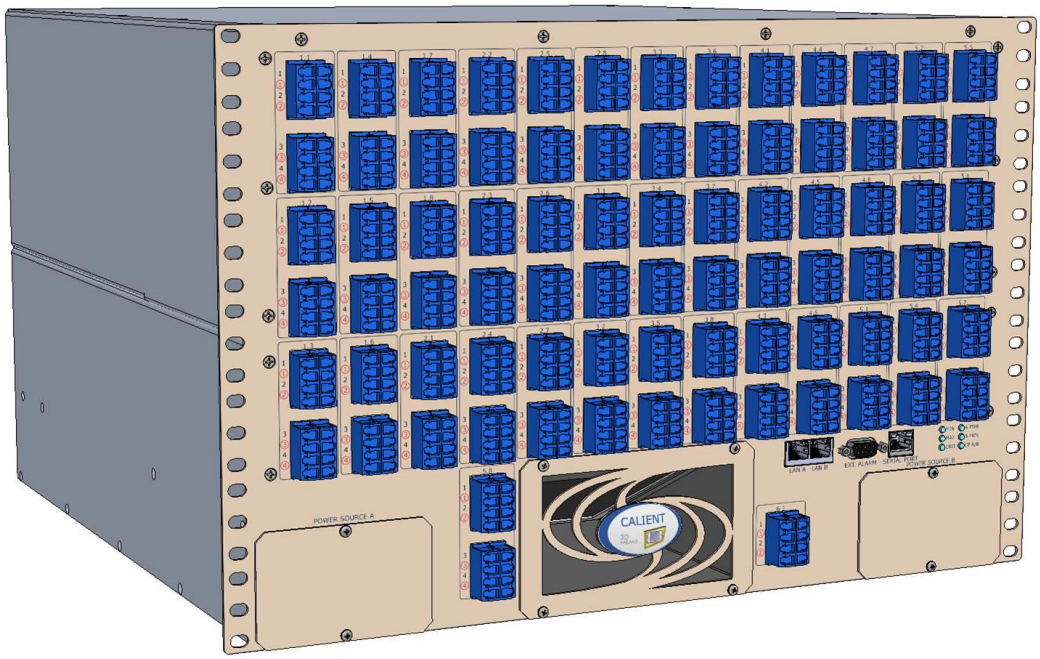
CALIENT

3D MEMS

Move the light, not the fiber

OCS Troubleshooting and Alarm Reference Guide



Confidential and Proprietary Information

CALIENT Technologies
25 Castilian Drive
Goleta, CA 93117 USA
Phone: +1.805.562.5500
www.calient.net

Service and Support

CALIENT offers a wide range of product support programs including installation support, repair services, maintenance services and technical training.

If you need technical assistance with CALIENT’s products, please visit our automated customer support portal at http://support.calient.net or email support@calient.net.

If you are experiencing a service-affecting emergency, please contact us on the following numbers:

Within US: 1.877.682.1160
International: International Call Prefix + Country Code + 1.877.682.1160

If your call is not answered immediately, please leave a message. Messages are retrieved continuously.

Document Part Number: 460181-00, Rev. A2

Revision History

Date	Version	Description	Author(s)
01/21/2013	—	Legacy documentation	T. Douglas
05/12/2015	A1	Update with latest troubleshooting and alarm info; implement new user doc formatting	T. Schilz
07/17/2015	A2	Add procedure for making CP2 active without enabling redundancy	M. Deacon, T. Schilz

Table of Contents

List of Figures

List of Tables

1 TROUBLESHOOTING

This section provides a guide to basic troubleshooting for the CALIENT S320 Optical Circuit Switch (OCS), including initial steps required to detect the source of the problem and a listing of common problems.

1.1 Preliminary Steps

1.1.1 Power

Following are some preliminary steps that can be performed to help determine the cause of a malfunctioning power module.

1. Check the LED on the power module. It should be lit solid green, as shown in Figure 1.

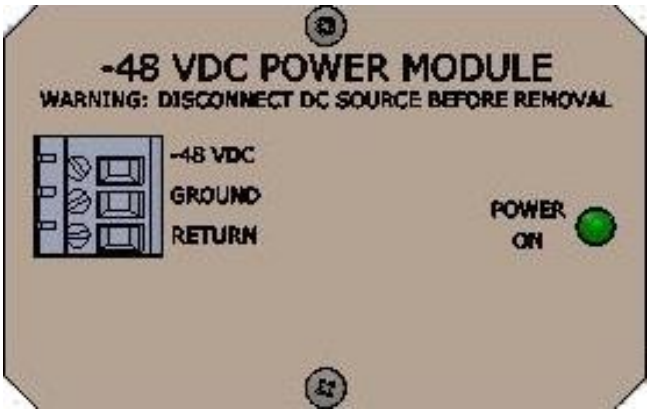


Figure 1 – OCS Power Module (Close Up)

2. If the LED is not illuminated, perform the following steps:
   a. Verify the power source.
   b. Ensure that the chassis is properly grounded.
   c. If the LED remains unlit, replace the power module.

Note

Refer to section 1.1.2 for an explanation of how to replace the power module.

1.1.2 Replacing the Power Module

1.1.2.1 Removing the Module

The following procedure describes how to safely remove the OCS's -48 VDC power module:

1. Turn off or disconnect the module's power supply.
2. Unscrew and remove the top and bottom screws from the power module faceplate. This step requires a Phillips screwdriver.
3. Carefully remove the power module from its housing, pulling it straight toward you, away from the OCS chassis and level with the floor.
4. Unplug the connector tail at the rear of the module.

1.1.2.2 Installing the Module

The following procedure describes how to install a new power module in the CALIENT OCS chassis:

1. Attach the DC power module to the connector tail.
2. Push the DC power module straight into the receptacle, keeping it level with the floor as you do so.
3. Insert and tighten the top and bottom screws.
4. Power up the new module.

Note

CALIENT recommends that each power module be connected to an independent power feed.

1.1.3 Verifying Communication Interfaces

1.1.3.1 Serial Port Connectivity

The following procedure describes how to verify serial port connectivity on the S320 OCS:

1. Locate the Serial Port found on the lower-right front of the OCS chassis, as shown in Figure 2 and Figure 3.

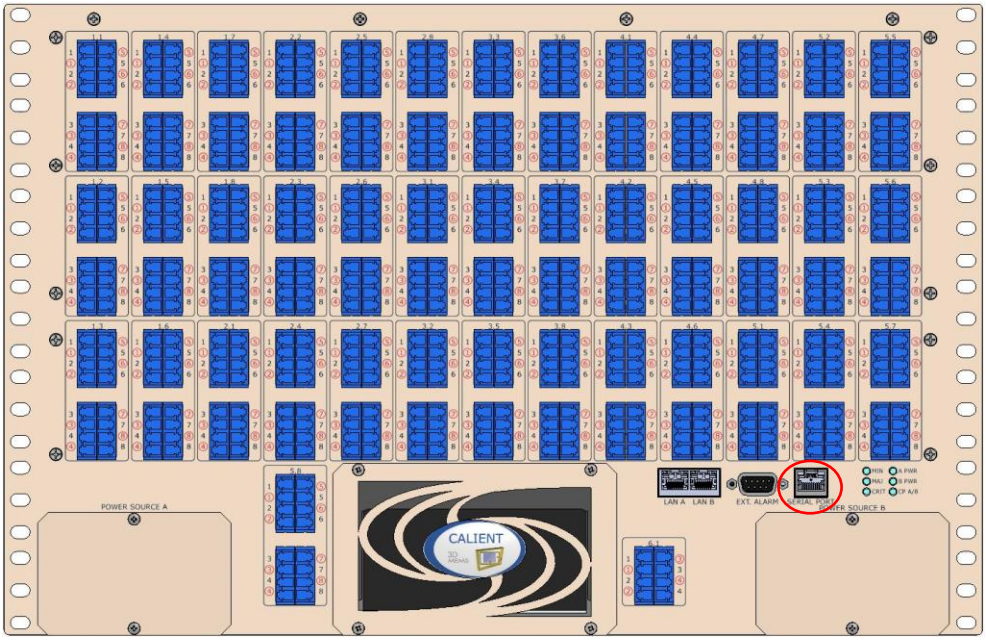


Figure 2 – Serial Port on OCS Chassis

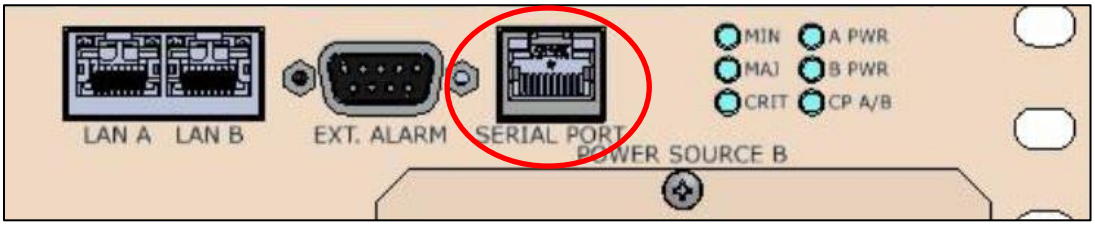


Figure 3 – OCS Serial Port (Close Up)

2. Locate the RJ-45 end of the serial cable that comes with the S320 OCS.
3. Plug the RJ-45 connector into the Serial Port on the front of the OCS chassis (Figure 3).

   Once connected to the OCS, you should be able to communicate with the TL1 Agent through the console or a PC using a standard terminal emulation program with a baud rate of 115200.
4. Verify that a login prompt appears on the console and that you can log into the switch using `root` as the login name and no password.

   If the uboot prompt => appears instead of the login prompt, it means the CP uboot sequence has been interrupted. If this happens, run the following command:

   ```
   // boot system without file system check
   ```

```
=> run sdboot

// boot system with file system check (fsck)

=> run sdboot2
```

1.1.3.2 Ethernet Connectivity

The following procedure describes how to verify Ethernet connectivity on the S320 OCS:

1. Locate the Ethernet ports—labeled LAN A (eth2) and LAN B (eth0)—found on the lower-right front of the OCS chassis, as shown in Figure 4 and Figure 5.

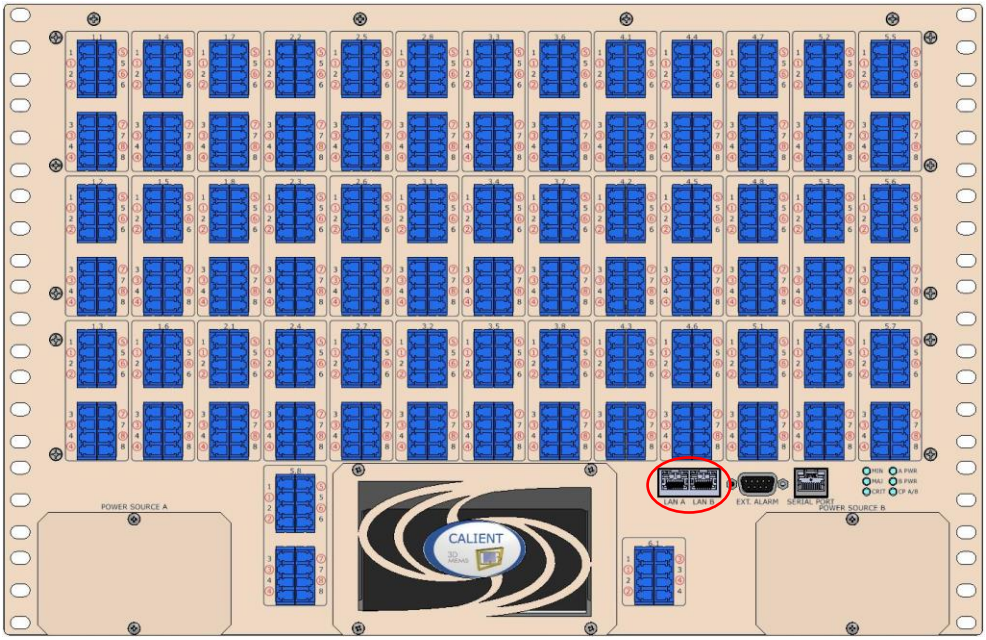


Figure 4 – Ethernet Ports on OCS Chassis

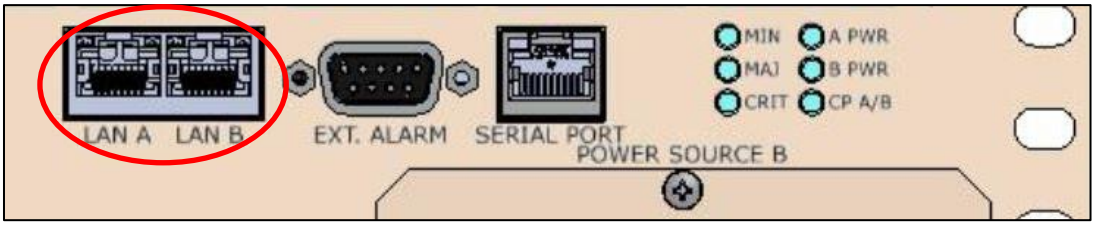


Figure 5 – OCS Ethernet Ports (Close Up)

2. Locate one of the two Ethernet cables that come with the S320 OCS.
3. Plug one end of the cable into either of the Ethernet ports (LAN A or LAN B).

4. Verify that the Ethernet cable is properly connected to the OCS by connecting to the switch via SSH.
5. If you are unable to connect to the OCS via SSH, check the Ethernet configuration on the switch by performing the following steps:
   a. Log in to the switch through the serial port.
   b. Type the following command:

      ```
      gxc-config-network –show
      ```
6. If the network configuration is incorrect or incomplete, configure the network with valid parameters by typing the following command:

   ```
   gxc-config-network –setup
   ```

1.1.4 Verifying Software Version and Services

1.1.4.1 Software Version

The following procedure describes how to verify the software version installed on the OCS:

1. Log in to the switch via SSH using `root` as the login name and no password.
2. Type the following command:

   ```
   gxc-listversions
   ```

   The system will list all software versions installed on the switch and indicate which one is active.

1.1.4.2 Services

The following procedure describes how to verify which services are running on the OCS:

1. Enter the following command:

   ```
   pl
   ```

   The system will list all services running on the switch and show the status of each.

1.2 Common Problems

Table 1 lists common problems and the alarm-clearing procedures that can be implemented to resolve them. For a comprehensive list of alarms, refer to section 2.2.

Note

Unless stated otherwise, all commands listed in this section are non-service affecting and will not impact traffic throughput.

Table 1 – Common Problems

Problem	Resolution

A service is not available or is not running on the OCS	• Login to the OCS through SSH using `root` as the login and leaving the password blank.
	• Run the `df -kh` command and make sure both / and /opt partitions have adequate space (they should not be at 100% utilization).
	• Check the software version installed on the OCS. Type the following command to list the versions installed and to determine which version is active:
	`gxc-listversions`
	• If the disk is full, remove the old version of software. Type the following command:
	`gxc-removeversion <non-active-version>`
	• Run the `pl` command to list all the services and their status.
	• If one or more services are not running, run the `gxc-start` command to start all services.
	• Make sure all services are running using the `pl` command.

Input power is unavailable	• Make sure the Input OMM Alarm is not active by listing all alarms using the `RTRV-ALM-ALL` TL1 command. • Make sure the laser source is ON and the input power is below the threshold limit. • Make sure the fiber is clean and properly connected to the input port. • Make sure either the TL1 (using `RTRV-PORT-SUM`) or Web GUI interface (navigate to Ports > Summary page) shows input power. • Verify that the port has power. If the problem persists, contact CALIENT Support for further analysis.

Problem	Resolution
Output power is unavailable	• Make sure the Output OMM Alarm is not active by listing all alarms using the `RTRV-ALM-ALL` TL1 command. • Make sure either the TL1 (using `RTRV-PORT-SUM`) or Web GUI interface (navigate to Ports > Summary page) shows input power. • Verify that the port has power. • Ensure that a cross-connect is associated with the port. If the problem persists, contact CALIENT Support for further analysis.
Web GUI is not accessible	• Check the software version installed on the OCS using the `gxc-listversions` command, which lists all versions installed and shows which one is active. • Run the `pl` command to list all services and their status. • If one or more services are not running, enter the `gxc-start` command to start all services. If the problem persists, contact CALIENT Support for further analysis.
Alarm LED (critical, major or minor) is illuminated	• Check for active alarms on the OCS using the TL1 `RTRV- ALM-ALL` command or the Web GUI interface (log in using `admin` as the login and `pxc***` as the password). • Make sure an active alarm is present on the OCS and that it matches the externally reported symptoms. • If you find a matching alarm, refer to the alarm-clearing procedures in section 1.2.1. If an alarm matching the hardware symptoms is not listed, contact CALIENT Support for further analysis.

1.2.1 Clearing Common Alarms

Table 2 lists various common alarms and the procedures used to clear them.

Table 2 – Clearing Procedures for Common Alarms

Alarm	Clearing Procedure

Disk Usage Exceeded Threshold	• Check to see if any other systemwide alarms are active using the TL1 command `RTRV-ALM-ALL`.
	• Run the `df -kh` command to ensure that both / and /opt partitions have adequate space (it should not be at 100% utilization).
	• It may be necessary to perform a cleanup of the log files /corefiles if the disk is full.
	• Check the software version installed on the switch. Type the following command to list the versions installed and to determine which version is active:
	`gxc-listversions`
	• If the disk is full, remove the old version of software with the following command:
	`gxc-removeversion <non-active-version>`

Fan Control Unit Access Failed	This alarm indicates I2C access to the fan control unit has failed. **NOTE:** The fan may still be functioning properly when this type of alarm occurs. • Check to see if any other systemwide alarms are active using the TL1 command `RTRV-ALM-ALL`. • Run the `gxc-reboot` command. If a reboot does not clear the alarm, perform a hard power cycle of the switch. **NOTE:** *A hard power cycle will be service affecting.* This error condition will not impact services or system performance; however, it should be fixed to ensure the long-term health of the system. Contact CALIENT Support for further analysis.

Alarm	Clearing Procedure
Temperature Sensor Unit Access Failed	This alarm indicates I2C access to the temperature sensor unit has failed. **NOTE:** The temperature sensor unit may still be functioning properly when this type of alarm occurs. • Check to see if any other systemwide alarms are active using the TL1 command `RTRV-ALM-ALL`. • Run the `gxc-reboot` command. If a reboot does not clear the alarm, perform a hard power cycle of the switch. **NOTE:** *A hard power cycle will be service affecting.* This error condition will not impact services or system performance; however, it needs to be corrected to ensure the long-term health of the system. Contact CALIENT Support for further analysis.
Switch UI Board Access Failed	This alarm indicates I2C access to the switch control unit has failed. **NOTE:** The switch control unit may still be functioning properly when this type of alarm occurs. • Check to see if any other systemwide alarms are active using the TL1 command `RTRV-ALM-ALL`. • Run the `gxc-reboot` command. If a reboot does not clear the alarm, perform a hard power cycle of the switch. **NOTE:** *A hard power cycle will be service affecting.* This error condition will not impact services or system performance; however, it needs to be corrected to ensure the long-term health of the system. Contact CALIENT Support for further analysis.
Fan Alarm	• Check to see if any other systemwide alarms are active using the TL1 command `RTRV-ALM-ALL`. • Log in to the OCS through SSH and run the `uifanctrl -r 4` command.

Alarm	Clearing Procedure
	• Verify that both fans are working. • Run the `gxc-reboot` command. If a reboot doesn't clear the alarm, perform a hard power cycle of the switch. **NOTE:** *A hard power cycle will be service affecting.* If the problem persists, the fans may be faulty. Replace the fan module or contact CALIENT Support for assistance.
CPU Overutilized	• Check to see if any other systemwide alarms are active using the TL1 command `RTRV-ALM-ALL`. • Verify that CPU utilization is greater than 70% by running the `top` command, which provides the average CPU utilization. • Run the `gxc-start` command to restart all services. • If the alarm doesn't clear, run the `gxc-reboot` command. If the problem persists, there may be a problem starting services or running the system with services. Contact CALIENT Support for further analysis.
Input/Output OMM	• Check to see if any other systemwide alarms are active using the TL1 command `RTRV-ALM-ALL`. • Run the `gxc-start` command to restart all services. • If the alarm doesn't clear, run the `gxc-reboot` command. • If the alarm persists, run the `gxc-shutdown` command to power cycle the switch. **NOTE:** Before running the `gxc-shutdown` command, make sure someone is physically near the switch to perform a power cycle (or if remote access is an option, to toggle the power feed for the switch). **NOTE:** *Both shutdown and a hard power cycle are service affecting.*

Alarm	Clearing Procedure
Ethernet Alarm	• Check to see if any other systemwide alarms are active using the TL1 command `RTRV-ALM-ALL`. • Make sure the network cables are properly connected to the Ethernet ports (LAN A and LAN B) on the switch. • Make sure the network cable connected to the Ethernet source is working properly. • Make sure the IP address is correct; the factory default IP address of the switch is 192.168.0.2. • Make sure the IP address configured for the switch is reachable via ping and is free of IP conflicts in the network. If the problem persists, contact CALIENT Support for further analysis.
Loss-Based Alarm (Optical Loss)	• Check to see if any other systemwide alarms are active using the TL1 command `RTRV-ALM-ALL`. • Make sure the optical cable connected to the port is clean. • Check the output power with an external meter, and make sure the output via TL1 or the Web GUI is the same. • Make sure all services are operational and the problem is isolated to a specific port(s). If the problem occurs across multiple ports, look for systemwide alarms. • Delete and re-establish the connection on the same ports, and verify the loss. If the problem persists, contact CALIENT Support for further analysis.

1.3 Removing Data Before an RMA

CALIENT recommends deleting company-sensitive passwords and networking configurations from the system before initiating an RMA of any OCS. To remove this information, issue the `gxc-config-network – clean` command from the SSH command line prompt.

Note

The cleanup process requires an administrative shutdown of the system. In the example below, the administrator has opted to power down the switch, overriding other users on the system.

Running the `gxc-config-network – clean` command will delete all network configurations and remove all configured user and password data. This command is available in software release 5.2.8d and later. If your OCS is running an earlier version of the software, please contact CALIENT for support.

The `gxc-config-network - clean` command performs the following operations on both the Active and Standby CP, as shown in the sample output below:

```
10:25:34 root@switch757:/opt/installtemp]$gxc-config-network --clean

**Warning**: This will RESET all network settings (Including ip
addresses) , SSH known_hosts entries and  authorized_keys and gxc
services are brought down.

Do you want to continue? (YES/NO):YES Stopping Gxc services

PHPServices [STOPPED]

WebServices [STOPPED]

TL1Service  [STOPPED]

xConnectProvisioner     [STOPPED]

SwitchMatrix[STOPPED]

NodeServices[STOPPED]

Authentication    [STOPPED]

DeviceManager     [STOPPED]

AlarmServices     [STOPPED]

CfgReg[STOPPED]

EventServices     [STOPPED]
```

```
EventConsumer     [STOPPED]

NamingService     [STOPPED]

DspServices [STOPPED]


Switch Reset to Factory defaults on Active CP

-------------------------------------------

Reset ethB Network configuration  Reset ethA Network configuration
Reset Resolve configuration

Reset SSH known_hosts entries  Reset SSH authorized_keys entries

**Warning** If selected YES below, the system will be
administratively powered down.

**Warning** If selected NO below, Configuration files are reset and
gxc services are stopped. SSH connectivity is  available as is until
the system is rebooted. Please proceed with gxc-shutdown

Do you want to continue with administrative power down? (YES/NO): YES

Broadcast message from root (pts/0) (Tue Jan 14 10:30:35 2014):

The system is going down for system halt NOW!  INIT: Sending
processes the TERM signal  Shutting down ntpd: [  OK  ]

Stopping High-Availability services: Done.

Stopping Vixie-cron.

Stopping portmap daemon: portmap.  Stopping ha_logd: stopped
Stopping sshd: [  OK  ]

Shutting down interface eth0:  bonding: bond0: link status
definitely down for interface eth0, disabling it

bonding: bond0: now running without any active interface !  [  OK  ]

bonding: bond0: released all slaves  Stopping Switch-ctrl: [  OK  ]

Shutting down loopback interface:  [  OK  ]  Stopping syslogd/klogd:
done

Deactivating swap...

Unmounting local filesystems...

mount: you must specify the filesystem type md: stopping all md
devices.

Disabling non-boot CPUs...

Task migration/1 (pid = 17) is on                (state = 2, flags =
cpu 1                                                      84208040)
```

```
Task desched/1 (pid = 30) is on cpu 1                    (state = 2, flags = 84208040)
Task kblockd/1 (pid = 153) is on cpu 1                   (state = 2, flags = 84208040)
Task kmmcd (pid = 169) is on cpu 1                       (state = 2, flags = 84208040)
Task xfsconvertd/1 (pid = 327) is on cpu 1 84208040)     (state = 2, flags =
Task kjournald (pid = 1110) is on cpu 1                  (state = 2, flags = 84208040)
Task udevd (pid = 1134) is on cpu 1                      (state = 2, flags = 400140)
Task kjournald (pid = 1224) is on cpu 1                  (state = 2, flags = 84208040)
Task rest-cgi-php (pid = 7206) is on cpu 1 400000)       (state = 2, flags =
Task rest-cgi-php (pid = 7207) is on cpu 1 400000)       (state = 2, flags =
Task rest-cgi-php (pid = 7211) is on cpu 1 400040)       (state = 2, flags =
Task rc (pid = 18660) is on cpu 1                        (state = 2, flags = 400000)
Task udevd (pid = 20294) is on cpu 1                     (state = 2, flags = 400140)
Task sleep (pid = 20413) is on cpu 1                     (state = 2, flags = 400000)
Power down.
System Halted, OK to turn off power.
```

1.4 Making CP2 the Active CP

The following procedure describes how to make CP2 (typically, the Standby CP) the Active CP on startup without enabling redundancy. This procedure can be implemented as a workaround if CP1 fails to boot.

1. Connect to the OCS serial console using PuTTY or similar.
2. Power cycle the OCS.
3. At the `autoboot` prompt, press any key:

   ```
   Hit any key to stop autoboot:  10
   ```

4. At the `UBoot` prompt, enter the following:

   ```
   setenv bootdelay 3
   setenv standby 'cpld write 2'
   setenv bootcmd 'run standby'
   saveenv
   ```

5. Power cycle the OCS.

2 ALARM AND EVENT MONITORING

2.1 Alarm Severity

The S320 OCS generates an alarm when it detects a problem with a physical entity or software component that can potentially compromise the system's operation. Table 3 describes the four levels of alarm severity generated by the system.

Table 3 – Alarm Severity Levels

Severity	Description
CR	**Critical Alarm** – This alarm is generated when a situation is detected that affects the operating stability of a component. Critical alarms can be service affecting and *require immediate action*.
MJ	**Major Alarm** – This alarm is generated when a situation is detected that significantly affects the operating stability of at least one component. Usually operation can continue without disruption to areas that are not impacted by the failed component. Major alarms *require immediate corrective action* to restore the equipment's operating stability.
MN	**Minor Alarm** – This alarm is generated when a situation is detected that *minimally* affects the operating stability of at least one component. For the most part, the equipment can operate normally under this condition, though the affected component may cause some degradation of service. Minor alarms *require investigation within 24 hours* to determine their potential impact on the equipment and to prevent the event from escalating to a more severe state.
NA	**Not Alarmed** – This classification applies to non-service-affecting events that do not generate an alarm.

Using the Alarm Config screen in the Web GUI, the severity of alarm events can be changed from CR to MJ to MN, or even NA. However, changing an alarm event's severity to NA will disable all alarms for that event.

2.2 Alarms and Alarm-Clearing Actions

Table 4 lists all alarms supported on the S320 OCS, including the alarm description, condition type, default severity level and clearing action.

Table 4 – Comprehensive Alarm List

Alarm Description	Condition Type	Severity	Action
Connection Loss Above Threshold	TRANCONN_POWER_ LOSS_ALARM	MN	Check connections and stability of input power.
CP Role Changed	EQPT-PROTNA	MJ	This alarm is generated when a failover from the Active CP to the Standby CP occurs, and the Standby CP becomes active. Contact CALIENT Support for more detail and/or assistance.
CPU Over Utilized	PROCROVLD	NA	Not service affecting; check for any abnormal activities on the system. Run the #top H from SSH shell for more information on the overload process.
Disk Usage Exceeded Threshold	T-DISK	MJ	Cleanup of logfiles/ corefiles (by customer) may be required.
External Link A Down	LINK_A_DOWN_ALARM	CR	Check Ethernet link A.
External Link B Down	LINK_B_DOWN_ALARM	CR	Check Ethernet link B.
Fan Control Unit Access Failed	FAN_ACCESS_ALARM	MJ	I2C access to the fan control unit has failed.
Fan Failed	FAN	MJ	Hot-swappable; keep spare in case of failure.
Input OMM Interrupt Failure	OMM Failure	CR	Requires further analysis by CALIENT Support.
Memory Usage Exceeded Threshold	T-MEM	MJ	Check for any abnormal behavior. Restart services or reboot the system.
No Standby Card Available	EQPT-PROTNA	MJ	This alarm occurs when a failover from the Active CP to the Standby CP is tried, and the Standby CP is not available. Contact CALIENT Support for assistance.

Alarm Description	Condition Type	Severity	Action
Output OMM Interrupt Failure	OMM Failure	CR	Requires further analysis by CALIENT Support.
Power Feed Unit A Failed	PWR_FEEDA_ALARM	MJ	Check Power Feed (Power Module) A. Hot-swappable (see section 1.1.2); keep a spare in case of failure.
Power Feed Unit B Failed	PWR_FEEDB_ALARM	MJ	Check Power Feed (Power Module) B. Hot-swappable (see section 1.1.2); keep a spare in case of failure.
Switch UI Board Access Failed	SWUIBOARD_ACCESS_ ALARM	MJ	I2C access to switch control has failed.
Temperature Exceeded	T-T	MJ	Check ambient temp to see if it has exceeded the specified threshold.
Temperature Sensor Unit Access Failed	TEMP_ACCESS_ALARM	MJ	I2C access to temperature sensors has failed.
Transit Connection Receive Signal Critical	T-INOPTCRIT	CR	Check input port power, as well as the fiber and connector.
Transit Connection Receive Signal Degraded	T-INOPTDEGR	MJ	Check input port power, as well as the fiber and connector.
Transit Connection Transmit Signal Critical	T-OUTOPTCRIT	CR	Check input and output port power. Recreate connection, if needed.
Transit Connection Transmit Signal Degraded	T-OUTOPTDEGR	MJ	Check input and output port power. Recreate connection, if needed.

2.3 Monitoring Alarms and Events

Alarms indicate that a problem exists within the OCS. The source of the problem can be either hardware based or software based.

Alarms are generated by faults crossing a threshold for a sustained period of time (i.e., soak interval). Information specific to each of the alarms defined within the system is written to an alarm log and can be accessed using the RTRV-LOG-ALM command.

Events are simple text strings that contain a limited amount of data. They provide an audit trail of provisioning activities. Events are written to an event log and can be accessed using the RTRV-LOG-EVT command.

Note

Before you begin issuing commands, make sure you have logged into the system using the ACT-USER command, or you will receive a PLNA (Privilege Login Not Active) error message.

2.3.1 RTRV-ALM-XXX: Retrieve Alarms

Which alarms get retrieved depends on the event types specified. Table 5 lists commands that can be used to monitor various alarm/event types.

Table 5 – Alarm/Event Types

Alarm/Event Monitoring Commands	Description
RTRV-ALM-ALL	Retrieves a list of all active alarms
RTRV-ALM-COM	Retrieves common alarms that are uncategorized
RTRV-ALM-CRS	Retrieves alarms related to transit connections
RTRV-ALM-ENV	Retrieves environmental alarms
RTRV-ALM-EQPT	Retrieves equipment-related commands

2.3.2 RTRV-ALM-XXX Output Format

RTRV-ALM-XXX commands share the same output format. Sample output for each type of alarm retrieval command is provided in the following sections.

2.3.2.1 RTRV-ALM-ALL: Retrieve All Alarms

The RTRV-ALM-ALL command retrieves all alarms present on the system, regardless of the specified type.

Input Format Syntax:

```
agent> RTRV-ALM-ALL;
```

Output Format Syntax:

```
SID DATE TIME M CTAG COMPLD
"<AID>:<ntfcncde>,<condtype>,<srveff>,<ocrdat>,<ocrtm>:[condd
escr>]"
;
```

Input Format:

```
agent> RTRV-ALM-ALL;
```

Output Format:

```
TL1AGENT 12-02-01 08:48:18
M 0 COMPLD
"1.2.2>1.3.3:CR,T-INOPTCRIT,SA,12-02-01,07-11-04:\"AlarmId=6:
Description=Transit Connection Receive Signal  Critical\"";
```

2.3.2.2 RTRV-ALM-COM: Retrieve Common Alarms

The RTRV-ALM-COM command retrieves all alarms belonging to a common category.

Input Format Syntax:

```
agent> RTRV-ALM-COM;
```

Output Format Syntax:

```
SID DATE TIME M CTAG COMPLD
"<AID>:<ntfcncde>,<condtype>,<srveff>,<ocrdat>,<ocrtm>:[condd
escr>]"
;
```

Input Format:

```
agent> RTRV-ALM-COM;
```

Output Format:

```
agent> rtrv-alm-com; TL1AGENT 12-05-01 15:06:51
;
```

2.3.2.3 RTRV-ALM-CRS: Retrieve Connection Alarms

This command retrieves alarm information for a specified connection or all connections.

Input Format Syntax:

```
RTRV-ALM-CRS;
```

Output Format Syntax:

```
SID DATE TIME
M  CTAG COMPLD
"<AID>:<ntfcncde>,<condtype>,<srveff>,<ocrdat>,<ocrtm>:[condd
escr>]"
;
```

Input Format:

```
agent> RTRV-ALM-CRS;
```

Output Format:

```
agent> rtrv-alm-crs;  TL1AGENT 12-05-01 15:06:51
M  0 COMPLD
"21.1>29.1:CR,T-INOPTCRIT,SA,06-02-06,02-28-59:\"AlarmId=20:
Description=Transit Connection Receive Signal   Critical\""
;
```

2.3.2.4 RTRV-ALM-ENV: Retrieve Environmental Alarms

This command retrieves alarm information related to temperature and other environmental data.

Input Format Syntax:

```
agent> RTRV-ALM-ENV;
```

Output Format Syntax:

```
SID DATE TIME  M  CTAG COMPLD
"<AID>:<ntfcncde>,<condtype>,<srveff>,<ocrdat>,<ocrtm>:[condd
escr>]"
;
```

Input Format:

```
agent> RTRV-ALM-ENV;
```

Output Format:

```
TL1AGENT 12-05-01 15:06:51
M  0 COMPLD
/* Active Alarm List Empty */
;
```

2.3.2.5 RTRV-ALM-EQPT: Retrieve Equipment Alarms

This command retrieves alarms related to equipment failure.

Input Format Syntax:

```
RTRV-ALM-EQPT;
```

Output Format Syntax:

```
SID DATE TIME  M CTAG COMPLD
"<AID>:<ntfcncde>,<condtype>,<srveff>,<ocrdat>,<ocrtm>:[condd
escr>]";
```

Input Format:

```
agent> RTRV-ALM-EQPT;
```

Output Format:

```
TL1AGENT 12-05-01 15:06:51
M  0 COMPLD
"0.28:MJ,REPLUNITMISS,NSA,08-02-12,18-55-19:\"AlarmId=5:
Description=Card    Missing\""
;
```

2.3.3 RTRV-LOG-ALM: Retrieve Alarm Log

This command retrieves the alarm log according to the specified filter conditions.

Input Format Syntax:

```
RTRV-LOG-ALM:[TID]:[<src>]:[CTAG]::[<ntfcncde>],[<condtype>],
[<srveff>];
```

Output Format Syntax:

```
SID DATE TIME  M  CTAG COMPLD
"<AID>:<nrfcncde>,<condtype>,<srveff>,<ocrdat>,<ocrtm>:[<cond
descr>]"
```

Input Format:

```
agent> RTRV-LOG-ALM;
```

Output Format:

```
TL1AGENT 12-02-01 08:48:40
M  0 COMPLD
```

```
"1.2.2>1.3.3:CR,T-INOPTCRIT,SA,12-02-01,06-17-04:\"AlarmId=5:
Description=Transit Connection Receive Signal  Critical\""

"1.2.2>1.3.3:CL,T-INOPTCRIT,SA,12-02-01,07-10-04:\"AlarmId=5:
Description=Transit Connection Receive Signal  Critical\""

"1.2.2>1.3.3:CR,T-INOPTCRIT,SA,12-02-01,07-11-04:\"AlarmId=6:
Description=Transit Connection Receive Signal  Critical\"";
```

2.3.4 RTRV-LOG-EVT: Retrieve Log Event

This command retrieves the event log according to the specified filter conditions.

Input Format Syntax:

```
RTRV-LOG-EVT:[TID]:[<src>]:[CTAG]::[<condtype>];
```

Output Format Syntax:

```
SID DATE TIME  M  CTAG COMPLD

"<AID>:<condtype>,<condeff>,<ocrdat>,<ocrtm>,[<conddescr>]";
```

Input Format:

```
agent> RTRV-LOG-EVT;
```

Output Format:

```
agent> rtrv-log-evt:

TL1AGENT 70-01-02 12:27:15

M  0 COMPLD

"TL1Service:SVC-REG,TC,70-01-02,10-50-24:\"Service
registered\""

"System:S-CFG,TC,70-01-02,11-02-17:\"System configuration
changed\""  "System:S-CFG,TC,70-01-02,11-02-17:\"System
configuration changed\""  "System:S-CFG,TC,70-01-02,11-02-
01:\"System configuration changed\""  "admin:SEC-LOGON,TC,70-
01-02,11-02-43:\"User     login\""

;"WebService:SVC-ALW,TC,08-02-12,15-24-25:\"Service
enabled\""

;
```

3 AUTONOMOUS MESSAGES

Autonomous messages are used to report alarms, configuration changes or condition changes. Many of these messages, such as those relating to alarm conditions, are spontaneously generated by the system itself without intervention. Other messages, such as those relating to the reporting of periodic condition states, are scheduled by the OCS operator.

3.1 Autonomous Message Commands

3.1.1 ALW-MSG: Allowing Autonomous Messages

This command re-enables the TL1 agent's ability to send autonomous messages during the current session. Autonomous messages can be inhibited based on severity. This command is issued after issuing the INH-MSG command (section 3.1.2) earlier in the session.

Table 6 – Autonomous Message Parameters

Parameter	Description
ntfcncde	This optional parameter is for Telcordia compliance.
msgtype	This parameter is not optional and specifies the type of autonomous message that can be sent: namely, ALL, ALM, EVT and DBCHG.

Input Format Syntax:

```
ALW-MSG:[TID]:[<src>]:[CTAG]::[<ntfcncde>],<msgtype>;
```

Output Format Syntax:

```
SID DATE TIME
M  CTAG COMPLD
```

Input Format:

```
agent> alw-msg:::::,all;
```

Output Format:

```
SB-LAB-1 08-02-13 16:08:42
M  0 COMPLD
;
```

3.1.2 INH-MSG: Inhibiting Autonomous Messages

This command is used to disable current user sessions from receiving autonomous messages. Use the ALW-MSG command (section 3.1.1) to re-enable a user session to receive autonomous messages.

Note

This command is only valid for the current session. The next time you log in, the TL1 agent will resume sending autonomous messages.

Input Format Syntax:

```
INH-MSG:[TID]:[<src>]:[CTAG]::[<ntfcncde>],<msgtype>;
```

Output Format Syntax:

```
SID DATE TIME
M  CTAG COMPLD
```

Input Format:

```
agent> INH-MSG:::::,all;
```

Output Format:

```
SJC-LAB-1 08-02-13 16:09:48
M  0 COMPLD
```

4 MONITORING ALARMS IN AUTOMATED MODE

Generation of TL1 autonomous alarm messages (REPT-ALM-XXX {ALL, CRS, EQPT, ENV}) is based on fault conditions. It is necessary to monitor all autonomous messages related to alarms.

4.1 Setting Up Autonomous Message Monitoring

The following procedure describes how to set up autonomous message monitoring:

1. Connect the monitoring software tool to the OCS through a TL1 session.

> **Note**
>
> Before you begin issuing commands, make sure you have logged into the system from the automated monitoring workstation using the ACT-USER command, or you will receive a PLNA (Privilege Login Not Active) error message.

2. To collect all autonomous messages, screen for REPT-ALM-XXX messages and parse the following message fields for evaluation:
   - <ntfcncde> – Notification code (CR = Critical, MJ = Major, MN = Minor, CL = Clear)
   - <condtype> – Condition type
   - <srveff> – Service affecting (SA = Service Affecting; NSA = Not Service Affecting)
   - <AlarmId> – Alarm identification reference (integer value)

4.2 Sample Autonomous Alarm Message

Following is a sample autonomous alarm message for CRS (cross-connect) alarms:

```
*C 6 REPT ALM CRS

"2.5.1>2.5.2:CR,T-INOPTCRIT,SA,12-04-16,15-06-58,,:\"AlarmId=34:
Description=Transit    Connection  Receive Signal Critical\""

;
```