Shelf controller, DCP-SC-28P

User Manual

Release-12.1.1
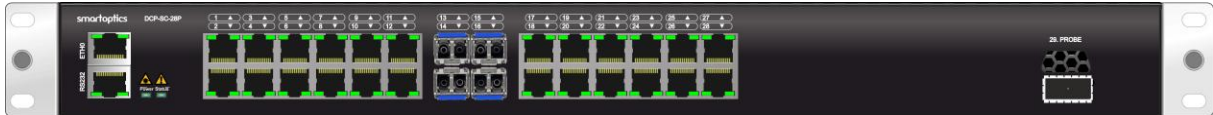
Contents

1 Introduction

1.1 General

This is document is the user manual for shelf controller DCP-SC-28P.

1.2 In commercial confidence

The manual is provided in commercial confidence and shall be treated as such.

1.3 Document Revision History

Revision	Date	Description of changes
10.1.1	2024-11-20	First revision of DCP-SC-28P manual
10.1.2	2024-11-25	Updated fan units
10.1.3	2024-12-04	Alarm list update
10.1.4	2024-12-08	Updated chapter about site requirements
11.0.1	2024-12-12	Updated ETH ports for site requirement Updated with examples for user roles in RADIUS
11.0.2 A	2024-12-17	Updated alarm list
11.0.2 B	2025-01-13	Updated SW upgrade section
11.0.3 A	2025-02-20	Changed order of commands for ILA Added topology update for adding and removing degrees Updated chapter for replacing node members
11.1.1 A	2025-03-25	Added section for OSPF configuration Updated chapter with ILA config
11.3.1 A	2025-04-24	No update
12.0.1 A	2025-06-24	Added reference to shelf controller migration Updated instructions for ILA configuration Added text about same SW for replacement units
12.0.1 B	2025-07-09	Updated text about SW upgrade Updated text about DCP-R replacement

12.0.2 A	2025-08-08	Added table with allowed actions for different users
12.1.1 A	2025-09-08	No update

2 Functional description

2.1 DCP-SC-28P

The main function of the shelf controller is to facilitate bi-directional connectivity between DCP-R:s in each node, between nodes and external networks. It enables centralized management of all nodes.

The shelf controller supports all network topologies which are typically used in this type of environment - single ring and multiple joined rings, partial or full mesh, point to point etc. As the network created by shelf controllers is based on layer-3 links and uses dynamic routing protocol (OSPF) for loop avoidance and redundancy, there is no need to adjust the configuration or deployed protocols for each of the various supported topologies. Node specific OSPF settings are configured through the installation script. Currently one primary and one secondary OSPF gateway are possible to configure.
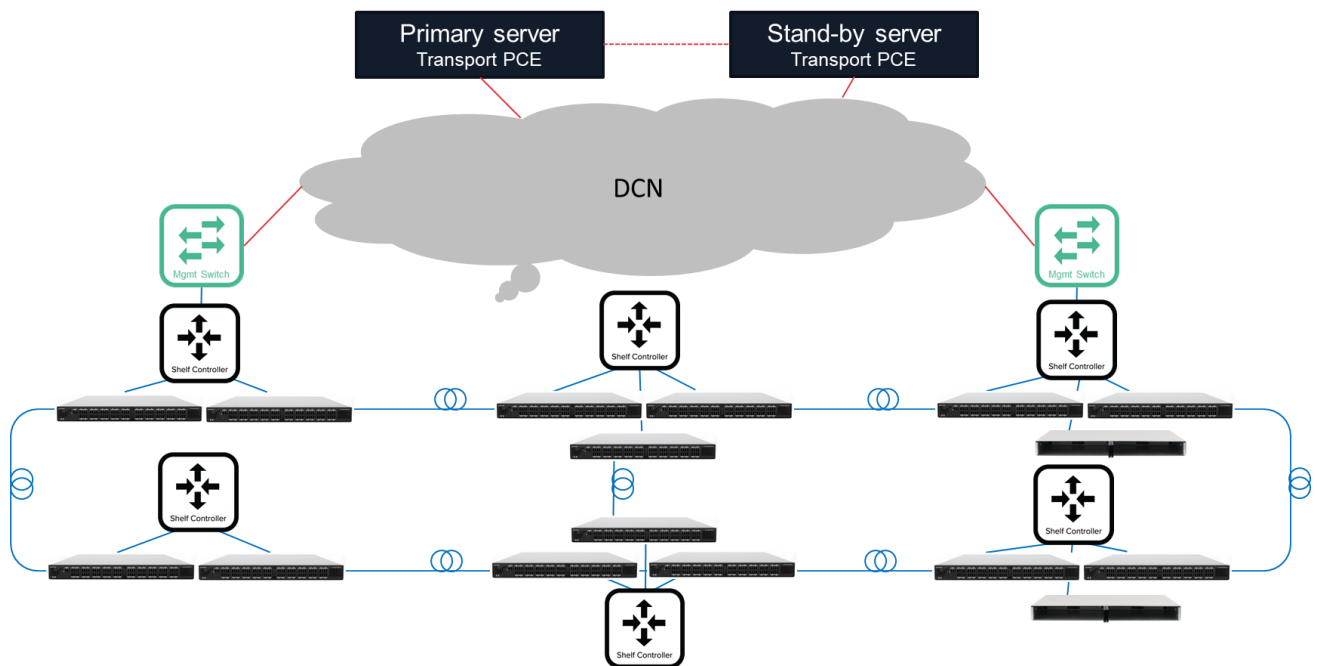
Figure 1. Example network with DCP-R:s and shelf controllers using OSPF configuration.

There is also the choice for the user not to use OSPF internally in the network. If the customer already has DCN connections to all sites and their own redundancy the shelf controller can be configured in "DCN only" configuration. See below an example of such a network.
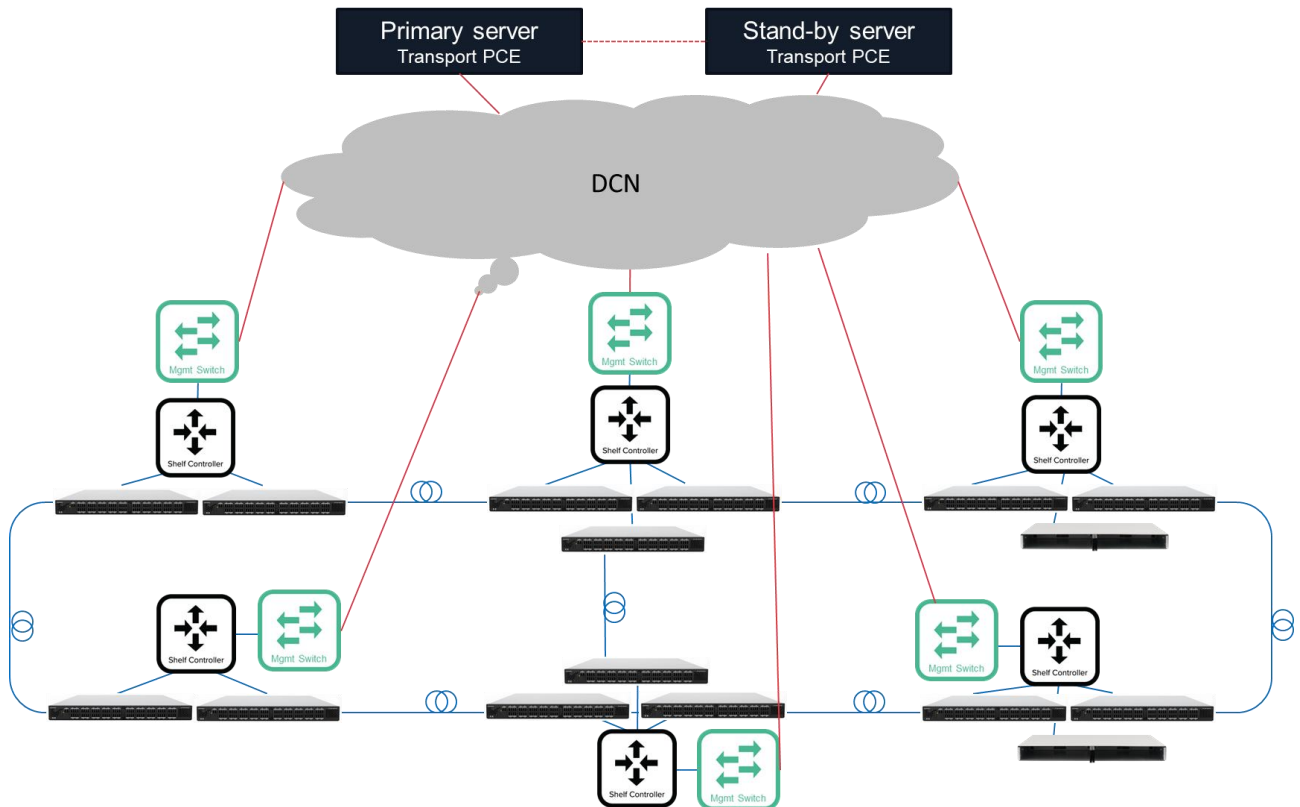
Figure 2. Example network with DCP-R:s and shelf controllers using DCN only configuration.

The hardware in a ROADM node consists of DCP-R unit(s) and the shelf controller DCP-SC-28P. The shelf controller is managing the DCP-R units and should be connected with a connection to the customers' private secure network. If SoSmart software suite is used the shelf controller must have IP connection to the SoSmart server. If management through CLI (managedCLI mode) is used the client (PC) can reach the node either through RS232/Eth0 or SSH. DCP-R CLI through SSH uses other ports than default (22). Please see section **Error! Reference source not found.** for details.

Figure 3. Shelf controller.
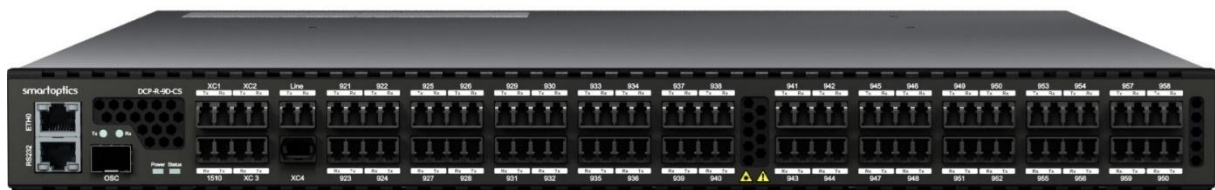
Figure 4. DCP-R unit.

The DCP-R:s in a node together with the shelf controller form a cluster and share data automatically in between each other. The DCP-R:s in a node are called degrees. The number of degrees will be determined by the number of fiber pairs through which the node should be able to communicate. Each DCP-R will get a designated degree number in the installation process. Below is an example of a 3-degree node consisting of 3 DCP-R:s and 1 shelf controller.
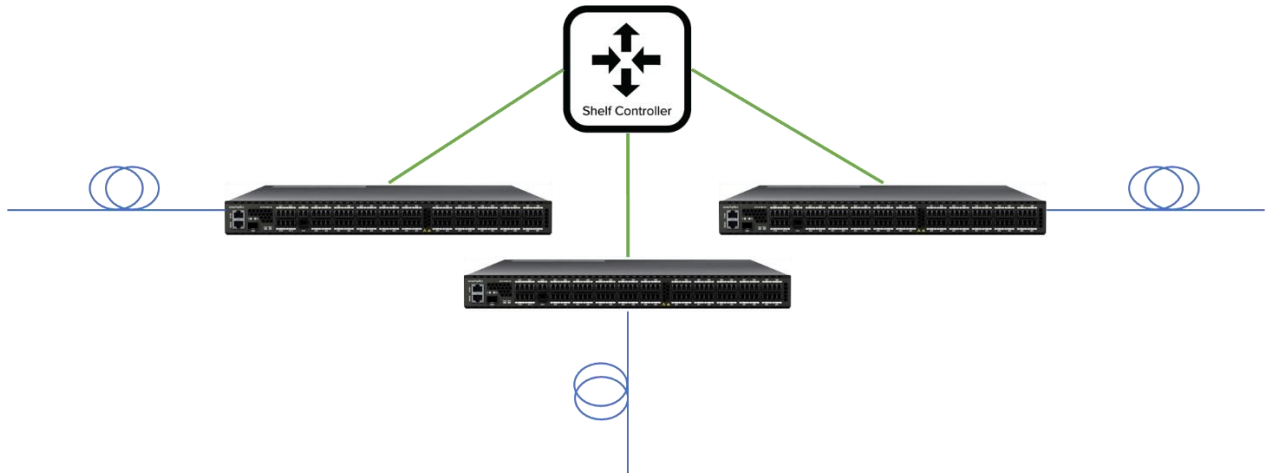
Figure 5. 3-degree node example.

2.2   Physical Description

The DCP-SC-28P is a compact unit, intended for installation in 19" racks or on shelves. The unit height is 1U (1.77 in). Power and fan units are located in the back panel. Management connections are available on the front side of the chassis. All optical connections are done on the front panel. The DCP-SC-28P has a front-to-back airflow. The DCP-SC-28P chassis is populated with 2 redundant power supplies and 1 fan unit (with 4 fans).

The shelf controller DCP-SC-28P has following ports:

- 1x RS232 serial connection

- 1x ETH0 Ethernet connection for local management

- 24x RJ-45 1G Ethernet ports

- 4x SFP+ 10G Ethernet ports

- 1x QSFP-DD probe port
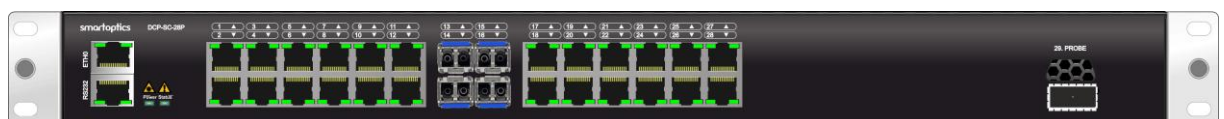
Figure 1.   *Chassis front view of DCP-SC-28P*

The front of the chassis includes one RJ45 Ethernet port and one RS232 serial port for management connections.

Figure 2.   *Chassis rear view of DCP-SC-28P*

2.3 Power supplies

In the figure below two power supplies are shown. The left power supply, DCP-2-PSU-AC-FB, is supporting 100-127 VAC and 200-240 VAC. The right power supply, DCP-2-PSU-DC-FB, supports -40 to -72 VDC. The DCP-SC-28P is dual feed and the power supplies are hot swappable. Both types can be used simultaneously.

Figure 3.   *The DCP-2-PSU-AC-FB and DCP-2-PSU-DC-FB unit.*

Same power supplies are also used in DCP-M, DCP-R and DCP-2 chassis.

2.3.1 Installing Power supplies (AC and/or DC)

1. Slide the power supply module into the power supply slot until you hear a click.
2. Push/pull on the black handle to ensure that it is engaged to the backplane connector.

2.3.2 Replacing a Power supplies

1. Remove the power cord
2. Push the locking lever in towards the power connector.
3. Lift the handle and pull out the power supply.
4. Install the new power supply (as previously described).
5. Reconnect the power cord
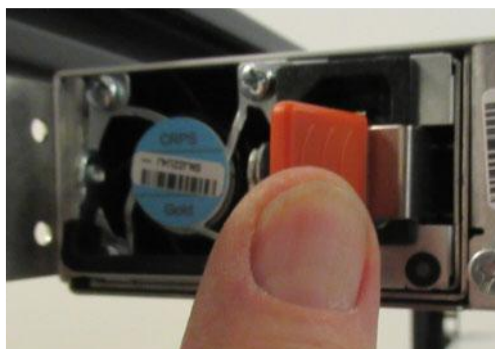
2.4 DCP-FAN-UNIT-01

The DCP-FAN-UNIT-01 is a fan unit that can be used in DCP-2, DCP-M, DCP-SC-28P and DCP-R chassis. This is a package that consists of one frame and 4 individual fan modules. The fan modules are already mounted in the frame and included in the product DCP-FAN-UNIT-01.
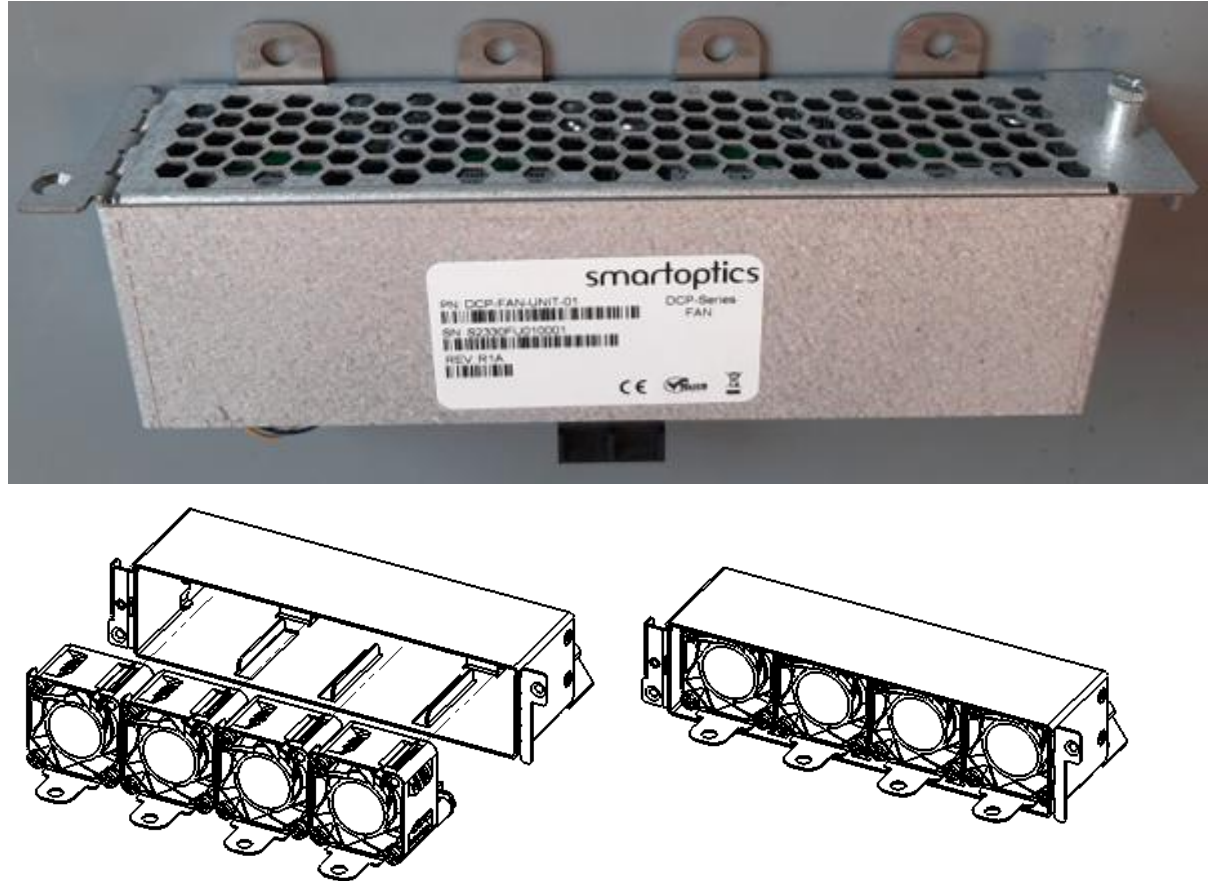
Figure 4.   *The fan module DCP-FAN-UNIT-01.*

The fan modules are hot swappable and can be replaced one by one. One fan module has the part number DCP-FAN-01.

The fan speed is regulated by temperature and the system is designed to operate with 3 fans working. If one fan fails, an alarm will be triggered to exchange the fan module. The fan speed on the remaining fan modules may be increased if the temperature increases. This is regulated automatically.
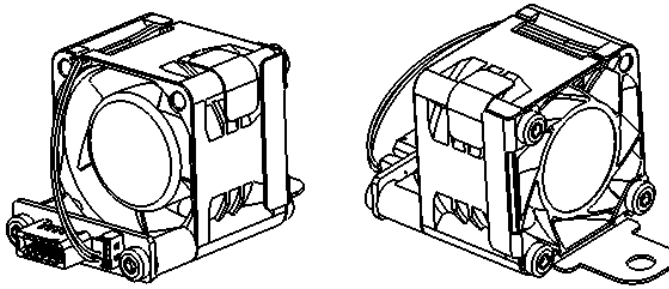
Figure 5. *The fan module DCP-FAN-01.*

2.4.1 Replacing a fan module in DCP-FAN-UNIT-01

1. Remove the protective metallic grid.
2. Remove the failed fan module
3. Insert a new fan module

⚠️ **WARNING** - To avoid injury, keep tools and your fingers away from the fans as you slide the fan module out of the chassis. The fans might still be spinning.
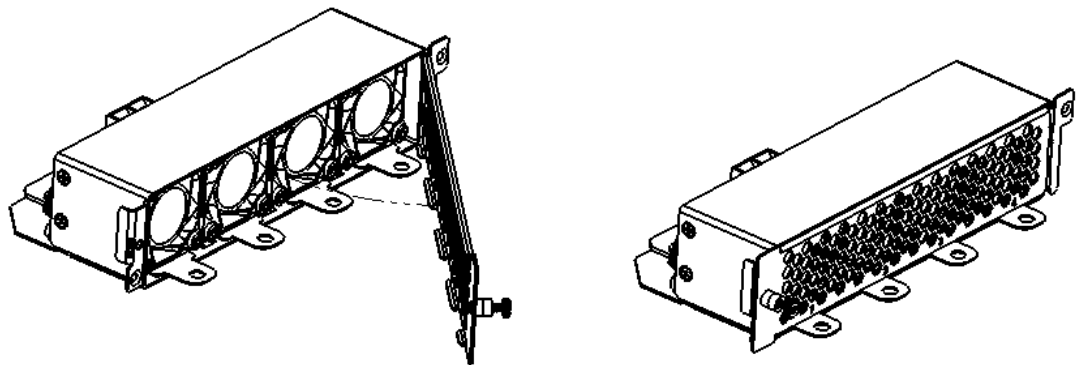
Figure 6. *How to open the protective metallic grid on DCP-FAN-UNIT-01*

2.5 Network Management Interfaces

The network management interfaces are part of the DCP-SC-28P chassis. Management connections are available on the front side of the chassis. The management system collects and controls system relevant information.

The module has:

- RS232 - 1x RS232 port in the front for serial access to the chassis and initial setup.

- ETH0 - 1x 100/1000Base-T "local" port access in the front for engineers onsite. The default IP address of the ETH0 port is 192.168.0.1.

Figure 7.   *Network management communication interfaces in the front of the DCP-SC-28Pchassis.*

2.6   Monitor points

The device components use environmental monitoring hardware to detect transmit power readings, receive power readings, and temperature updates.

2.7   Alarms

The DCP-SC-28Pkeeps a list of the alarms currently detected on the system and collected by the system. When an alarm is detected, it is added to the active alarm list. When the alarm is cleared the alarm is removed from the active alarm list. Previously cleared alarms can be found in the alarm log.

The following information is stored for each alarm:

Start time: The date and time when the alarm was detected.

End time: The date and time when the alarm was cleared.

Location: The entity that caused the alarm.

Severity: The severity of the alarm.

All possible alarms can be listed with the command:
show alarm list

ALARM MESSAGE	LOCATION	SEVERITY	INTERPRETATION
Fan failure	fan-<chassi>/1	Major	Fan unit has failed. Replace within 24 hours.
Fan missing	fan-<chassi>/1	Critical	Fan is missing in chassis.
Power supply failure	psu-<chassi>/1 psu-<chassi>/2	Major	Input AC/DC power is lost on the unit
Power supply missing	psu-<chassi>/1 psu-<chassi>/2	Critical	This alarm appears when the unit is not inserted.
Power supply unsupported	psu-<chassi>/1 psu-<chassi>/2	Major	This alarm appears if an unknown power supply unit is inserted.
External power missing	psu-<chassi>/1 psu-<chassi>/2	Minor	Power cable not connected or external power not active.
Power supply fan failure	psu-<chassi>/1 psu-<chassi>/2	Minor	Fan module inside power unit failed.
Power supply communication failure	psu-<chassi>/1 psu-<chassi>/2	Major	The chassis cannot communicate with the power supply unit
Power supply input voltage high	psu-<chassi>/1 psu-<chassi>/2	Minor	The input voltage is too high
Power supply input voltage low	psu-<chassi>/1 psu-<chassi>/2	Minor	The input voltage is too low
Node member connection lost		Major	Connection to a slave chassis is lost
Software version mismatch	chassis	Major	The chassis has a different SW version than the shlef controller. Note that this alarm is not implmented for ILAs with shelf controllers in R8.1.3

2.8   Backup and restore

The backup and restore functionality are available. This is needed for replacement of DCP-SC-28P.

Backup files can be created and uploaded to a remote server for reference configuration that can be used for fault finding for support.

Only one backup file is allowed. The backup file will be removed at reboot.

3 Installation and Safety

3.1 Safety Precaution

Fasten the chassis securely to a 19"-rack.

Insert the PSU in the chassis and connect it to the power source. The chassis will automatically power up as soon as the PSU is connected.

3.1.1 General Safety Precautions

The following are the general safety precautions:

The equipment should be used in a restricted access location only.

No internal **settings**, adjustments, maintenance, and repairs may be performed by the operator or the user; such activities may be performed only by skilled service personnel who are aware of the hazards involved.

Always observe standard safety precautions during installation, operation, and maintenance of this product.

3.1.2 Electrical Safety Precautions

Warning: Dangerous voltages may be present on the cables connected to the DCP-SC-28P.

Never connect electrical cables to a DCP-SC-28P unit if it is not properly installed and grounded.

Disconnect the power cable before removing a pluggable power supply unit.

Grounding: For your protection and to prevent possible damage to equipment when a fault condition occurs on the cables connected to the equipment (for example, a lightning strike or contact with high voltage power lines), the case of the DCP-SC-28P unit must be properly grounded at all times. Any interruption of the protective (grounding) connection inside or outside the equipment, or the disconnection of the protective ground terminal, can make this equipment dangerous. Intentional interruption is prohibited.

When a DCP-SC-28P is installed in a rack, make sure that the rack is properly grounded and connected to a reliable, low resistance grounding system.

Connect the DCP-SC-28P via an external cable to ground. See Section 3.2.8 for further details.
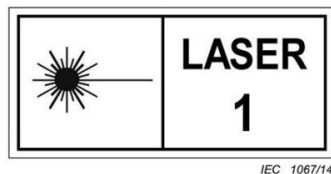
The grounding must also be made through the AC power cable, which should be inserted in a power outlet with a protective ground contact. Therefore, the power cable plug must always be inserted in a socket outlet provided with a protective ground contact, and the protective action must not be negated by use of an extension cord (power cable) without a protective conductor (grounding).

3.1.3   Laser Safety Classification

The DCP-SC-28P complies with Class 1. The incorporated laser has a divergent beam, operates within the wavelength span of 1530 – 1563 nm and has a maximum output of +20 dBm.

The following warning applies to Class 1 laser products.

Invisible Laser Radiation: Do not view directly with optical instruments.

Class 1 Laser Warning.

Laser Safety Statutory Warning and Operating Precautions

All personnel involved in equipment installation, operation, and maintenance must be aware that the laser radiation is invisible. Therefore, the personnel must strictly observe the applicable safety precautions and in particular, must avoid looking straight into optical connectors, either directly or using optical instruments.

In addition to the general precautions described in this section, be sure to observe the following warnings when operating a product equipped with a laser device. Failure to observe these warnings could result in fire, bodily injury, and damage to the equipment.

Warning: To reduce the risk of exposure to hazardous radiation:

Do not try to open the enclosure. There are no user serviceable components inside.

Do not operate controls, adjust, or perform procedures to the laser device other than those specified herein.

Allow only authorized service technicians to repair the unit.

3.1.4   Protection against Electrostatic Discharge

An electrostatic discharge (ESD) occurs between two objects when an object carrying static electrical charges touches or is brought near the other object. Static electrical charges appear as a result of friction between surfaces of insulating materials or separation of two such surfaces. They may also be induced by electrical fields.

Routine activities, such as walking across an insulating floor, friction between garment parts, and friction between objects, can easily build charges up to levels that may cause damage, especially when humidity is low.

Caution: DCP-SC-28P internal boards contain components sensitive to ESD. To prevent ESD damage, do not touch internal components or connectors. If you are not using a wrist strap, before touching a DCP-SC-28P or performing any internal settings on the DCP-SC-28P, it is recommended to discharge the electrostatic charge of your body by touching the frame of a grounded equipment unit.

Whenever feasible during installation, use standard ESD protection wrist straps to discharge electrostatic charges. It is also recommended to use garments and packaging

made of anti-static materials, or materials that have a high resistance, yet are not insulators.

3.1.5   Site Requirements

This section describes the DCP-SC-28P site requirements.

PHYSICAL REQUIREMENTS

The DCP-SC-28P unit can be mounted in a 19-inch, 23-inch, or ETSI rack with the GND cable connected. The rack depth needs to be at least 600 mm.

All the electrical connections are made to the back panel. The optical traffic connections are made in the front panel.

POWER REQUIREMENTS

AC-powered DCP-SC-28P units should be installed within 3m (10 feet) of an easily accessible, grounded AC outlet capable of furnishing the required AC supply voltage, of 100-127VAC (3A) and 200-240VAC (1,5A) maximum.

DC-powered DCP-SC-28P units require a -48VDC (-40V to -72V) (Max 7A @ -48V) DC power source with the positive terminal grounded. In addition, the DC power connector contains the chassis (frame) ground terminal.

AMBIENT REQUIREMENTS

The ambient operating temperature of the DCP-SC-28P is 0° to +45°C/+32° to +113°F, at a relative humidity of 5% to 85% RH non-condensing.

The DCP-SC-28P is cooled by free air convection and a pluggable cooling FAN unit. The DCP supports front-to-back cooling. The air inlets and outlets are positioned in the front and back.

Caution: Do not obstruct these vents.

The DCP-SC-28P contains a fan speed control for lower noise, improved MTBF, and power savings.

ELECTROMAGNETIC COMPATIBILITY CONSIDERATIONS

The DCP-SC-28P is designed to comply with the electromagnetic compatibility (EMC) requirements according to ETSI EN 300 386 V2.1.1 class A. To meet these standards, the following conditions are necessary:

The DCP-SC-28P must be connected to a low resistance grounding system.

The RJ45 Ethernet interfaces ETH0 plus the 24 GBE management ports (1-12 + 17-28) can be used for intra-building connections provided that a Cat 5e (or higher) class shielded cable is used. The cables must not be electrically connected directly to outside-plant cables.

Warning: The intra-building port(s) (ETH0 plus the 24 GBE management ports (1-12 + 17-28)) of the equipment or subassembly is suitable for connection to intra building or unexposed wiring or cabling only. The intra-building port(s) of the equipment or subassembly MUST NOT be metallically connected to interfaces that connect to the OSP or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 ports as described in GR-1089-CORE) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metallically to OSP wiring.

Warning: The intra-building port(s) ETH0 plus the 24 GBE management ports (1-12 + 17-28)) of the equipment or subassembly must use shielded intra-building cabling/wiring that is grounded at both ends.

Maximum allowed cable length for intra-building connections is 100m.

The DCP-SC-28P must be installed in a CBN (common bonding network) per NEBS GR-1089.

The DCP-SC-28P is designed to be used in Network Telecommunication Facilities.

Common DC return (DC-C) Is applicable for the DCP-SC-28P.

3.2 Rack mounting

The following instructions provides detail how to mount the system in racks that are 600 mm to 1200 mm deep (24"- 48").

The system can be mounted in a rack in the following ways:

1. With the front side flush with the front of the rack posts. (Four-Post Rack).

2. With the front side in a recessed position. A recessed position allows a more gradual bend in the fiber-optic cables connected and less interference in the aisle at the front of the rack (Four-Post Rack).

3. With the rack posts mounted to the mid-section of the system (Two-Post Rack).

3.2.1 Rack-mount kit parts list

The following parts are provided with the rack-mount kit.

1. Mid-mount, front right and front left (225mm)
2. Front-mounting Bracket, right and left (700mm)
3. Front bracket extension, right and left (270mm)
4. Front bracket extension, right and left (470mm)
5. Rear-mounting brackets, right and left (142mm)
6. Front-mounting Bracket, right and left (600mm)
7. Rear-mounting brackets, right and left (42mm)
8. Screws, M4x6, Phillips (20 pcs)
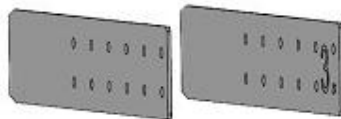
1 Mid-mount, front right and front left (225mm)   **2** Front-mounting bracket, right and left (700mm)
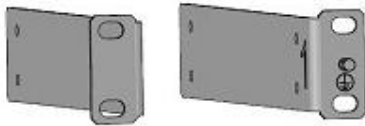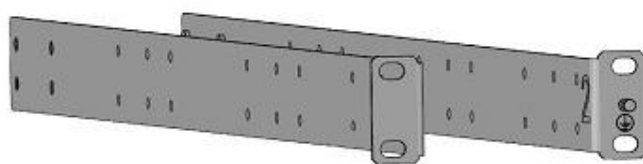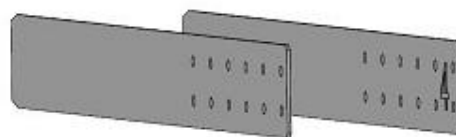
3 Front bracket extension, right and left (270mm)   **4** Front bracket extension, right and left (470mm)
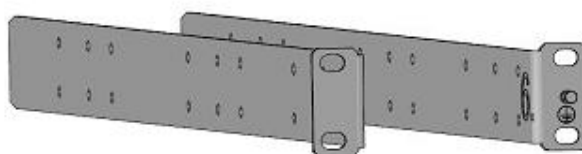
5 Rear-mounting brackets, right and left (142mm)   **6** Front-mounting bracket, right and left (600mm)
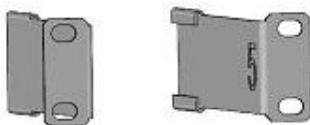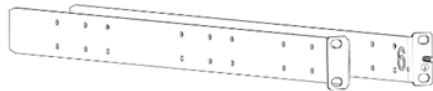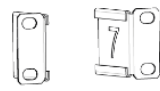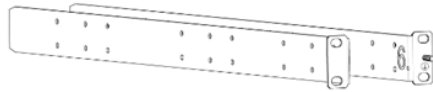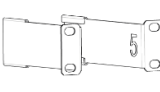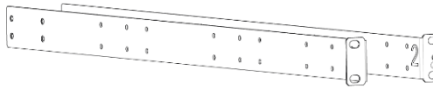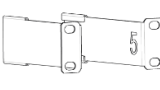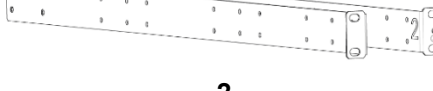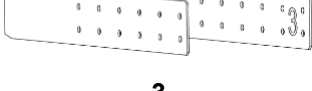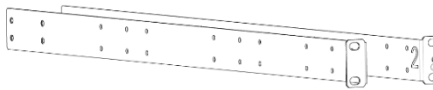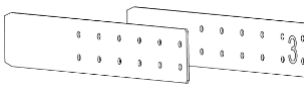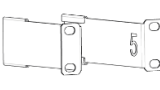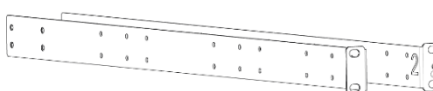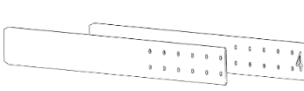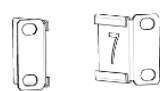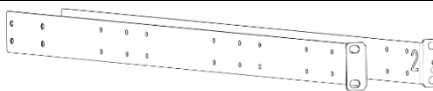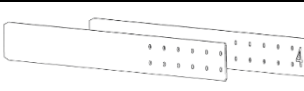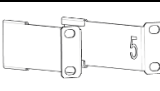
7 Rear-mounting brackets, right and left (42mm)   **8** Screws, M4x6 x 20 pcs

smartoptics

3.2.2 Determining bracket configuration

3.2.2.1 4-Post Rack

The bracket configuration to use depends on the depth of the rack where the system is installed into.
Use the following table to determine the correct bracket configuration.

Rack Depth	Rack-kit Parts		
	Front bracket	**Middle extension**	**Rear bracket**
600 mm 24"	 **6**		 **7**
600 – 700 mm 24" - 28"	 **6**		 **5**
700 – 820 mm 28" - 32"	 **2**		 **5**
800 – 900 mm 32" - 36"	 **2**	 **3**	 **7**
840 – 1000 mm 34" - 40"	 **2**	 **3**	 **5**
1000 – 1100 mm 40" - 44"	 **2**	 **4**	 **7**
1100 – 1200 mm 44" - 48"	 **2**	 **4**	 **5**

3.2.2.2 2-Post Rack

For a 2-post rack, use part number one. Refer to chapter 3.2.6 for mounting instructions.
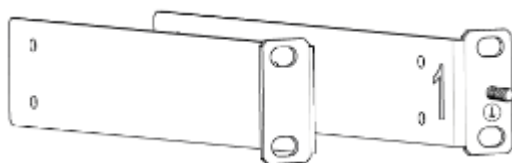
Part number 1.

3.2.3   Chassis flush or recessed position mounting

Complete the following steps to attach the front brackets to the system.

1. Position the right front-mounting bracket with the flat side against the front right side of the system.

2. Insert five M4x6 screws through the vertically aligned holes in the bracket and then into the holes on the side of the system.

3. Position the left front-mounting bracket with the flat side against the front left side of the system.

4. Insert six M4x6 screws through the vertically aligned holes in the bracket and then into the holes on the side of the system.

5. Tighten all the eleven M4x6 screws to a torque of 17 cm-kg (15 in-lb.).

3.2.4   Attaching the bracket extensions to the front brackets

Complete the following steps to attach the extension brackets to the front brackets.

1. Position the right bracket extension along the side of the front-mounting bracket.

2. Insert four M4x6 screws through the vertically aligned holes in the bracket extension and then into the holes on the front-mounting bracket.

3. Repeat step 2 and step 3 to attach the left bracket extension to the front-mounting bracket.

4. Tighten all the eight M4x6 screws to a torque of 17 cm-kg (15 in-lb.).

3.2.5   Attaching the rear brackets to the rack posts

Complete the following steps to attach the rear brackets to the rack posts.

1. Attach the right rear-mounting bracket to the right rear rack post using two screws and two retainer nuts.

2. Attach the left rear-mounting bracket to the left rear rack post using screws and two retainer nuts.

3. Tighten all the screws to a torque of 29 cm-kg (25 in-lb.).

3.2.6   Attaching brackets for mid-mounting

Complete the following steps to attach the front brackets to the system.

1. Position the right mid-mount bracket with the flat side against the right side of the system.

2. Flip it over so that the L-shaped bracket angle is placed inwards.

3. Insert three screws through the vertically aligned holes in the bracket and then into the holes on the side of the system.

4. Position the left mid-mount bracket with the flat side against the left side of the system.

5. Insert four screws through the vertically aligned holes in the bracket and then into the holes on the side of the system.

6. Tighten all seven M4x6 screws to a torque of 17 cm-kg (15 in-lb.).

3.2.7   Installing the system in the rack

Complete the following steps to install the system in the rack.

1. Position the system in the rack, providing temporary support under the system until it is secured to the rack.

2. If applicable, slide the right and left front-mounting brackets into the rear-mounting brackets that should already be mounted at the rear posts of the rack.

3. Attach the right front-mounting bracket to the right front rack post using two screws and two retainer nuts.

4. Attach the left front-mounting bracket to the left front rack post using screws and two retainer nuts.

5. Tighten all the screws to a torque of 29 cm-kg (25 in-lb.).

3.2.8   Protective Ground Terminal

Connecting the DCP chassis to earth ground is required for all DC powered installations, and any AC powered installation where compliance with Telcordia grounding requirements is necessary.

Before connecting power to the device, the grounding terminal must be connected to ground to ensure proper operation and to meet electromagnetic interference (EMI) and safety requirements.

The front rack mount brackets include a grounding terminal. The surface area around this terminal is not painted to provide a good electrical connection. It is located on the right-side front rack mount(s). The front rack mount(s) are also interchangeable between left and right if there is requirement to have the ground terminal on the left side.

The grounding cable should have a cable area of minimum 2.5 mm2 (14 AWG). 14 AWG grounding lugs is included together with the rack mounting kit. The nut size of the grounding terminal is M5 and is also included in the rack mounting kit along with an external toothed locking washer which should be placed between the lug and the nut.
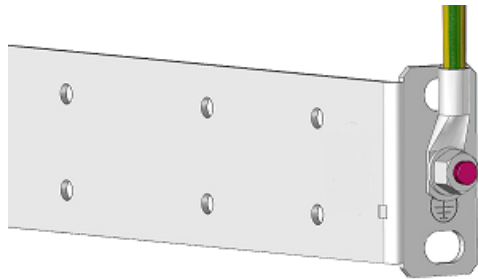
Attach the grounding cable from the grounding terminal to an appropriate grounding point at your site.

Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor.

4 Startup guide

4.1 Package Contents

The DCP-SC-28P package includes the following items:

- 2x Power cord (Model depends on country/region. For AC 1,8m/6 ft. For DC 3m or 5m.)

- 2 x Ethernet patch cords

- RJ45 to DB9 adapter

- Rack-mount kit (Refer to 3.2.1 for contents)

- DCP-SC-28P chassis, incl. PSU:s and fan unit

- Quick Installation Guide

4.2 Initial start up
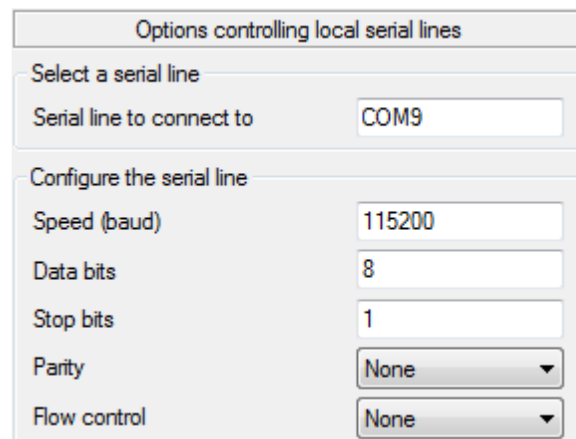
Connect power to the power supplies that are preinstalled in the chassis. The chassis will automatically power up as soon as the first PSU is connected. The power LED turns green.

The fan package starts up after a few seconds.

4.3 Connection to Serial Port

Connect the Serial port of the DCP-SC-28P to a computer using the serial port or a USB/Serial port adapter. Use the following settings for the serial transaction.

Parameter	Setting
Protocol	Serial
Baud rate	115200
Data bits	8
Parity	None
Stop bits	1
Flow control	None

Figure 8.   *COM9 is shown only as an example. Use the appropriate port ID for the connection.*

4.3.1 Serial console cable connectors

You can connect a serial RJ45 console port on the DCP units using the following diagram and table.
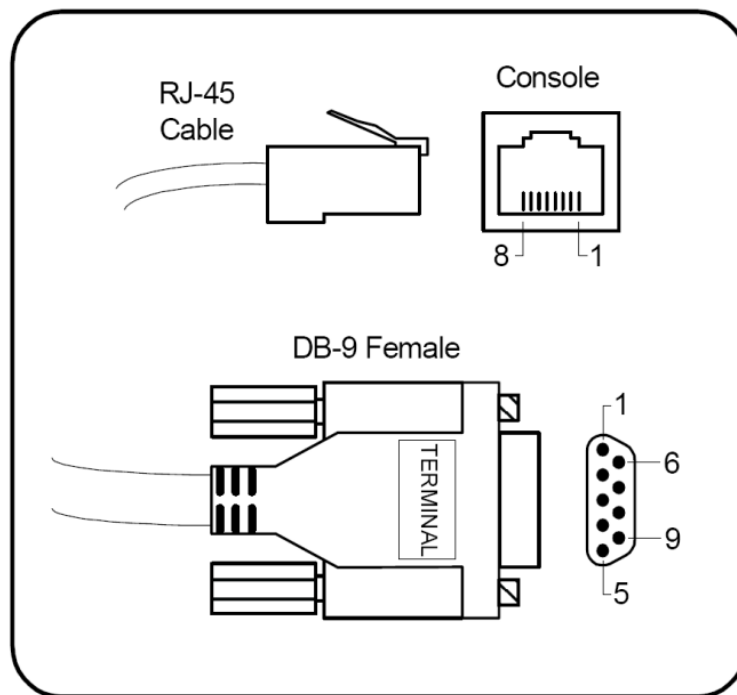
Figure 9.   *Serial Console Cable Connectors*

4.3.2 Console Port Cable Pinouts

Unit Console Port (RJ45)		Serial Port (DB9)	
PIN	Signal	PIN	Signal
1	Not connected		
2	Not connected		
3	Tx Data	2	Rx Data
4	Ground	5	Ground
5	Ground	5	Ground
6	Rx Data	3	Tx Data
7	Not connected		
8	Not connected		

4.4 Installation of shelf controller

The CLI for DCP-SC-28P will be used for all the commands related to ROADM or ILA nodes. There is no need to connect directly to DCP-R or ILA chassis for configuration or monitoring, everything is done from the shelf controller.

The first step is to configure IP settings and connections to external servers like NTP or DNS.

4.4.1 Configuring IP and external servers

4.4.1.1 Configuring IP address

This is done on the same way on the shelf controller as on all other DCP products.
Note that the DCP system use IPv4 today.

```
admin@smartoptics-dcp>config network mgmt ipv4address
<IPv4 address>          - IPv4 address in dotted decimal format.
<netmask>               - IPv4 netmask in dotted decimal format.
[gateway IPv4 address]  - IPv4 gateway address in dotted decimal format.
```

4.4.1.2 Configuring NTP server

It is possible to define two NTP servers. Note that the DCP-SC-28P synchronizes with the NTP servers only when the NTP admin status is up.

```
admin@DCP-19>config ntp
adminStatus      - Configure NTP adminStatus : up / down
primaryServer    - Configure NTP primary server  <primary NTP server IPv4 address>
secondaryServer  - Configure NTP secondary server <secondary NTP server IPv4 address>
admin@DCP-19>config ntp
```

4.4.1.3 Configuring time zone

It is possible to define the time zone for the shelf controller.

```
admin@DCP-19>config timezone
Available timezones:
  Africa/Cairo  America/Anchorage America/Caracas
 America/Chicago America/Denver America/Los_Angeles America/New_York America/Sao_Paulo
  Asia/Dhaka Asia/Dubai Asia/Hong_Kong Asia/Karachi
 Asia/Tokyo  Australia/Adelaide Australia/Brisbane Australia/Darwin
 Australia/Sydney CET CST6CDT EET EST
 EST5EDT EST5EDT Etc/GMT Etc/GMT+0 Etc/GMT+1
 Etc/GMT+10 Etc/GMT+11 Etc/GMT+12 Etc/GMT+2 Etc/GMT+3
 Etc/GMT+4 Etc/GMT+5 Etc/GMT+6 Etc/GMT+7 Etc/GMT+8
 Etc/GMT+9 Etc/GMT-0 Etc/GMT-1 Etc/GMT-10 Etc/GMT-11
 Etc/GMT-12 Etc/GMT-13 Etc/GMT-14 Etc/GMT-2 Etc/GMT-3
 Etc/GMT-4 Etc/GMT-5 Etc/GMT-6 Etc/GMT-7 Etc/GMT-8
 Etc/GMT-9 Etc/GMT0 Etc/UCT Etc/UTC Etc/Universal
 EST5EDT Europe/London Europe/Moscow Europe/Paris GB
 Greenwich HST MET MST MST7MDT
 NZ NZ-CHAT PRC PST8PDT PST8PDT
 Pacific/Honolulu Pacific/Noumea ROC ROK W-SU
 WET Zulu
Time zone:  - Pick a Name from time zone list
admin@DCP-19>config timezone
```

4.4.1.4   Configuring DNS server

It is possible to define two DNS servers.

```
admin@smartoptics-dcp>config network ipv4dns

<primary DNS IPv4 address>    - New primary DNS IPv4-address.
[secondary DNS IPv4 address]  - New secondary DNS IPv4-address (optional).

admin@smartoptics-dcp>config network ipv4dns
```

4.4.2   Configuring ROADM information

This section explains how to configure information about the ROADM node, e.g. node members, node ID, geolocation etc.

4.4.2.1   Connect the DCP-R units to the shelf controller

Before we can communicate to the DCP-R units from the shelf controller it is necessary to connect Ethernet LAN cables.

Connect ETH4 ports on the DCP-R units to the shelf controller. Connect DCP-R degree1 to shelf controller port ETH1. Connect DCP-R degree2 to shelf controller port ETH2 etc.
See example below:

DCN port: ETH28

Shelf controller

ETH1

ETH2

ETH4

ETH4

DCP-R degree 1. Connect port ETH4

DCP-R degree 2. Connect port ETH4
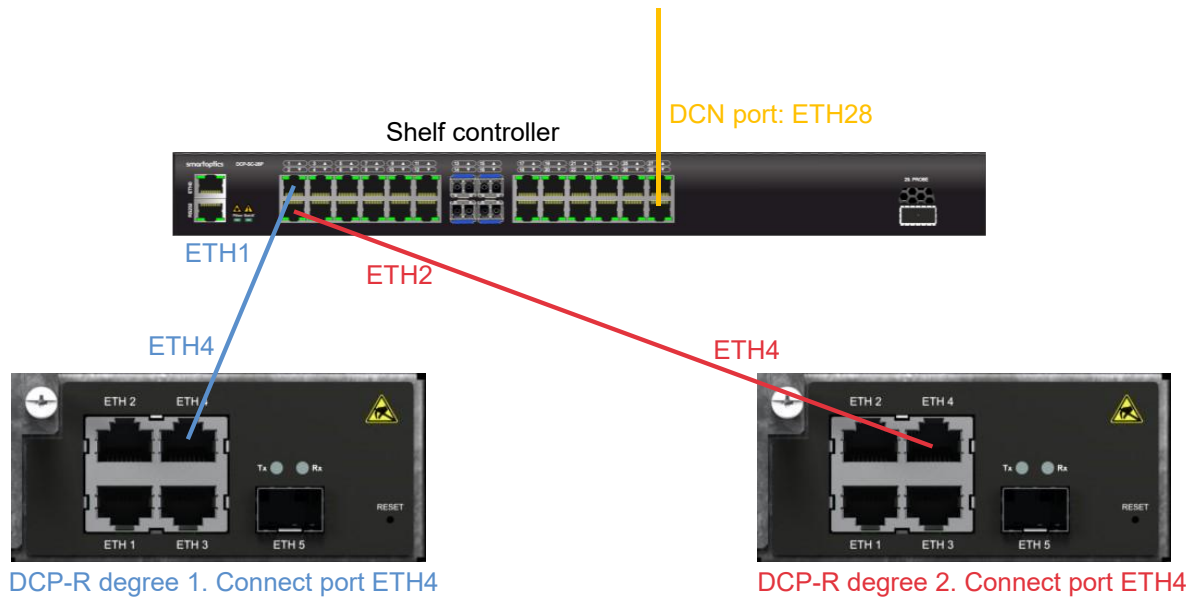
4.4.2.2   Add node members

Add node members that should be included in the ROADM node. The shelf controller DCP-SC-28P will be the master with chassis ID 0. The DCP-R nodes should be added so that degree 1 is same as chassis-1, degree 2 is same as chassis-2 etc.

Type "*config node member add <serial number> chassis-<chassis number>*" for all the members to be added. They should automatically appear in the list "*show node members*". Start with adding the first degree then all remaining degrees in degree number order.

Check that all DCP-R chassis have been added correctly by typing "*show node members*".

4.4.2.3   Config node info

It is necessary to config node ID and geolocation before the node can be mounted in SoSmart.

Configure NodeID, Geolocation, Netconf password (user is admin). Use below CLI commands:
config node info ID

The Node ID of each node will be used later in the SoSmart node mounting sequence. It is important to note the Node ID of each node.
Min number of characters for node ID is 7.
Max number of characters for node ID is 20.

config node info geolocation
config user netconf chpasswd

4.4.2.4 Config node topology

It is necessary to specify the internal topology for all patch cords used between different degrees.

Configure internal topology to setup the XC connections. Use CLI command:
config node topology internal [enter the ports that are connected between the degrees]
This is not needed in managedCLI mode.
If the shuffle box (H-SB-XC-6MPO) is used, see DCP-R manual for details.

After the topology is complete use CLI command:
config node topology apply
This will store the topology database correctly.

4.4.2.5 Configure hostname

It is not mandatory to configure hostname on every degree, but it could make it easier to identify specific units in reports and log files.

Configure hostname for the shelf controller.
config hostname <hostname>

Configure hostname on each of the members.
config chassis [degree No] *hostname*

4.4.3 Configuring ILA information

This section explains how to configure information about the ILA node, e.g. node members, node ID, geolocation etc.

Here are the steps required for configuration of an ILA. This is only a high level schedule, more details are presented in the sub chapters below.

1. Configure managedILA mode on DCP-2 and DCP-SC-28P
2. Connect Ethernet cables between DCP-2 and DCP-SC-28P
3. Add node members
4. Configure node info
5. Configure hostname
6. Configure network tunnels
7. Configure admin status on amplifiers

4.4.3.1 Config managedILA mode

It is necessary to configure both the DCP-2 chassis and the DCP-SC-28P in managedILA mode if it should be used in SoSmart.

Configure managedILA on the DCP-2:
config automationMode managedILA

Configure managedILA on the DCP-SCP-28P:
config automationMode managedILA

4.4.3.2   Connect the DCP-2 ILA chassis to the shelf controller

Before we can communicate to the DCP-2 ILA chassis from the shelf controller it is necessary to connect Ethernet LAN cables.

Connect DCP-2 port ETH4 to shelf controller port ETH1.
Connect slot 1 port ETH1 to shelf controller port ETH2.
Connect slot 2 port ETH1 to shelf controller port ETH3.

See example below:
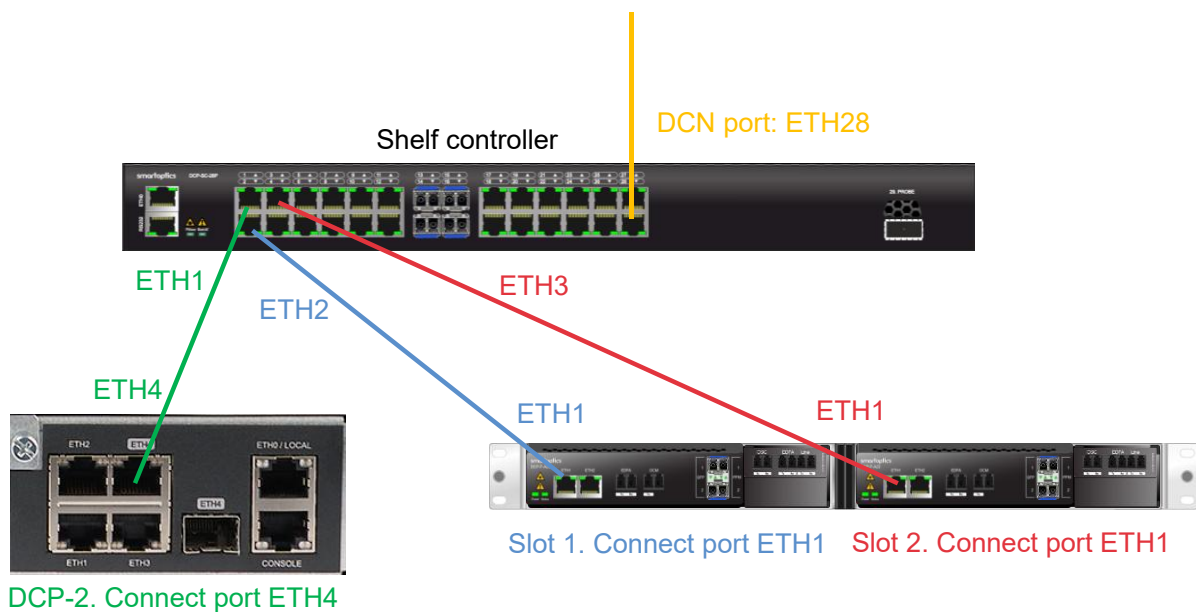
4.4.3.3   Add node members

Add the DCP-2 chassis as a node member that should be included in the ILA node. The shelf controller DCP-SC-28P will be the master with chassis ID 0. The DCP-2 chassis should be added so that it is chassis ID 1.

This configuration is done from the shelf controller.

Type "*config node member add <serial number>*" for the DCP-2 chassis to be added.

Check that the DCP-2 chassis has been added correctly by typing "*show node members*".

4.4.3.4   Config node info

It is necessary to config node ID and geolocation before the node can be mounted in SoSmart.

Configure NodeID, Geolocation, Netconf password (user is admin). Use below CLI commands:
config node info id <Node ID>

The Node ID of each node will be used later in the SoSmart node mounting sequence. It is important to note the Node ID of each node.
Min number of characters for node ID is 7.
Max number of characters for node ID is 20.

config node info geolocation <longitude> <latitude>
config user netconf chpasswd <new password>

4.4.3.5 Configure hostname

It is not mandatory to configure hostname on each slot, but it could make it easier to identify specific units in reports and log files.

Configure hostname for the shelf controller.
config hostname <hostname>

Configure hostname for the DCP-2 chassis.
config chassis 1 hostname <hostname>

Configure hostname on each of the slots.
config slot [slot number] *hostname <hostname>*

4.4.3.6 Configure network tunnel for the OSC

It is necessary to configure a network tunnel from each of the amplifier units in the ILA to towards the DCP-SC-28P. Use ETH1 port in both amplifier units.
config network tunnel if-1/1/2 if-1/1/eth1 untagged
config network tunnel if-1/2/2 if-1/2/eth1 untagged

4.4.3.7 Configure admin status on amplifiers

It is necessary to configure adminStatus to up on the amplifiers. Otherwise, they will not start to amplify light.
config slot 1 interface edfa1 adminStatus up
config slot 2 interface edfa1 adminStatus up

4.5 User accounts

Different users are needed for management of nodes with DCP-SC-28P in SoSmart.
The admin user is used for CLI and SW upgrade function in SoSmart. The netconf user is used for communication between the SoSmart controller and the network elements.

The DCP-R is shipped with 2 default user accounts, admin/admin and netconf/admin.
The admin user cannot be deleted and will always be present in a system. For security reasons, it is recommended to change the admin password.

The admin user account can do both monitoring, configuration and user administration. It is also possible for the admin user to enable additional user accounts:

- readonly
  This account can be used for monitoring and reading, but this user cannot configure anything.
- operator
  This account can be used both for monitoring and configurations. However, this account cannot do user administration.
- sftpuser
  This account can be enabled to handle file management via sftp. It can access folders in the node file system with files for SW upgrade, techlog and PM.

In addition to these accounts, the DCP platform got a root user account that can be used by support to debug issues with the system. By default, this account is only enabled on the console port. This account can also be fully disabled or fully enabled by the user. It is recommended that the customer makes an active decision to decide what level of access the root user should have.

Possible settings:

- disable – The root account is disabled.

- enable – The root account is open over ssh and console.

- enableConsole – The root account is only open on console port.
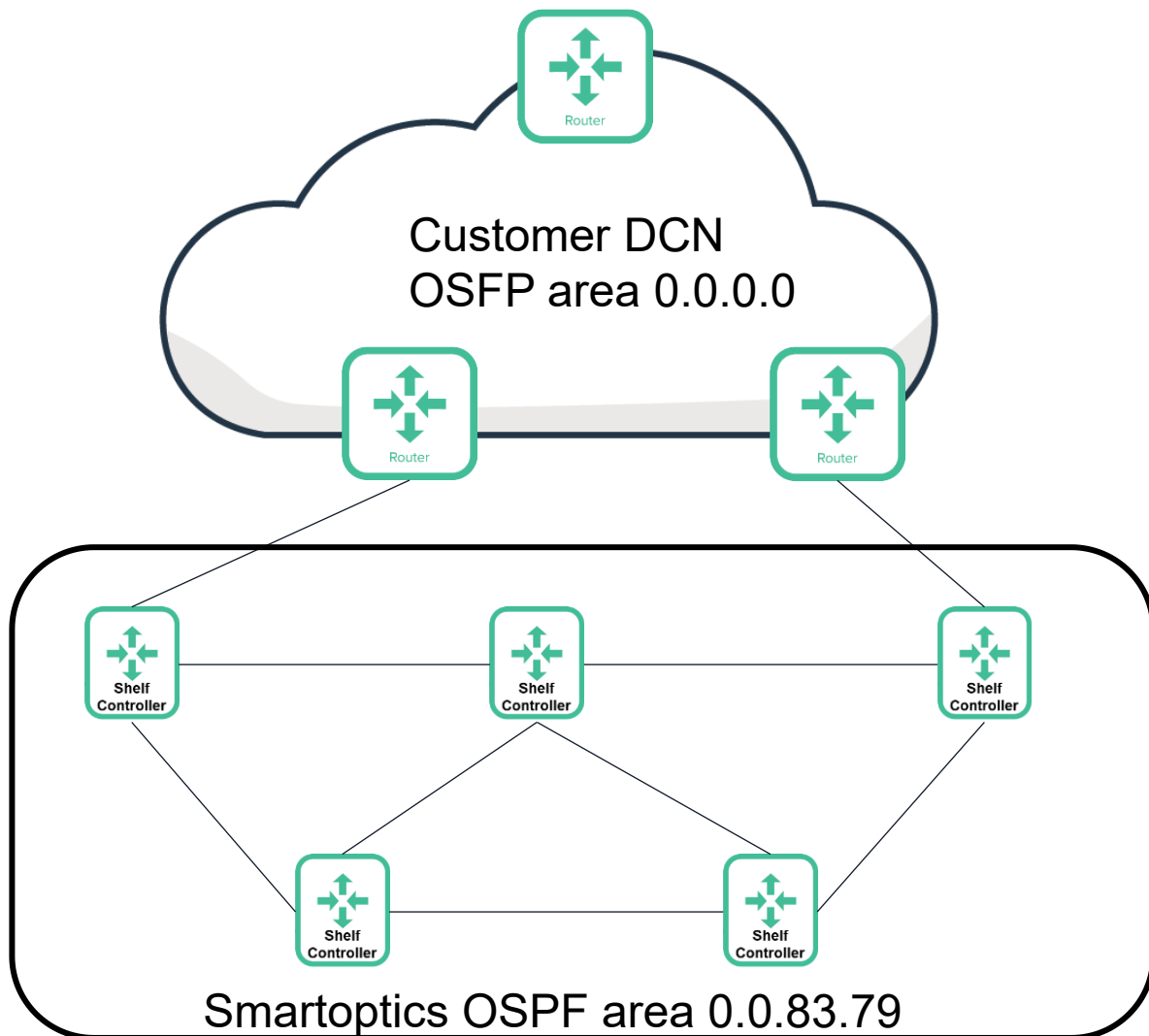
User	Show commands	Config commands	User administration	SFTP File transfer	SW upgrade	Encryption
readonly	Yes					
operator	Yes	Yes			Yes	
admin	Yes	Yes	Yes		Yes	
sftpuser				Yes		
cryptouser	Yes	Yes	Yes		Yes	Yes

5 OSPF configurations

OSPF (Open Shortest Path First) can be utilized to route management traffic within the domain of Smartoptics ROADM equipment. This enables remote access to nodes that are not directly connected to the Data Communication Network (DCN) and provides added redundancy in ring or mesh topologies.

To streamline the setup process, the ability for customers to create custom OSPF configurations is intentionally limited. All ports come preconfigured with the recommended OSPF default settings; however, their administrative status is set to down by default.

For basic use cases, configuration is minimal—simply set the OSPF administrative status to up on the interfaces where OSPF should be active.
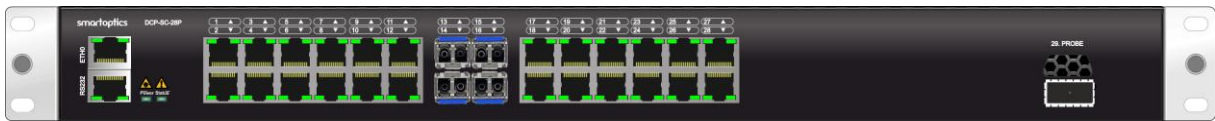
5.1 Configuration example for uplinks with OSPF

In the OSPF uplink scenario illustrated below, two distinct OSPF areas are used to segment the network. he connection between these two areas should be established within the customer's OSPF area (0.0.0.0). In this setup, the DCP-SC-28P shelf controller acts as an Area Border Router (ABR), forming the boundary between the ROADM network and the customer DCN. This helps prevent large routing tables from the DCN from propagating into the ROADM area, maintaining efficiency and scalability within the optical layer. There may be one or multiple uplinks from ROADM or ILA nodes to the customer DCN, depending on redundancy and network design requirements.
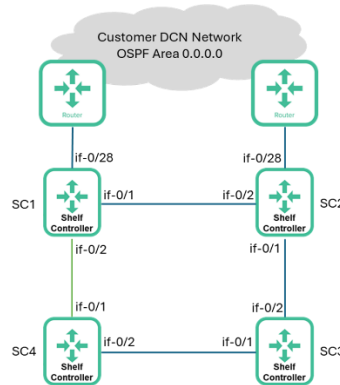
5.1.1 Config for SC1 – Uplink Site (ABR)

Enable OSFP for the Uplink interfaces (if-0/28) that connects to the customer DCN. Enable OSPF for desired degrees (if-0/1 to if-0/12) that connects to internal ROADM/ILA via OSC links.

```
config network ospf interface if-0/28 adminStatus up
config network ospf interface if-0/1 adminStatus up
config network ospf interface if-0/2 adminStatus up
```

5.1.2 Config for SC2 – Uplink Site (ABR)

Enable OSFP for the Uplink interfaces (if-0/28) that connects to the customer DCN. Enable OSPF for desired degrees (if-0/1 to if-0/12) that connects to internal ROADM/ILA via OSC links.

```
config network ospf interface if-0/28 adminStatus up
config network ospf interface if-0/1 adminStatus up
config network ospf interface if-0/2 adminStatus up
```

5.1.3 Config for SC3

Enable OSPF for desired degrees (if-0/1 to if-0/12) that connects to internal ROADM/ILA via OSC links.

```
config network ospf interface if-0/1 adminStatus up
config network ospf interface if-0/2 adminStatus up
```

5.1.4 Config for SC4

Enable OSPF for desired degrees (if-0/1 to if-0/12) that connects to internal ROADM/ILA via OSC links.

```
config network ospf interface if-0/1 adminStatus up
config network ospf interface if-0/2 adminStatus up
```

5.2   Verifying OSPF Status

Run the following command to check OSPF configuration

```
show network ospf status
```

You should see output similar to this:

```
admin@ROADM-A>show network ospf status

OSPF admin status:        up
RouterID:                 10.10.250.130

  Interface  OperStatus  AdminStatus  AreaId     AreaType
  ---------  ----------  -----------  ---------  --------
  if-0/1     down        down         0.0.83.79  NSSA
  if-0/2     up          up           0.0.83.79  NSSA
  if-0/3     up          up           0.0.83.79  NSSA
  ...
  if-0/28    up          up           0.0.0.0    NSSA

============ OSPF network routing table ============
N    10.0.1.0/30          [102] area: 0.0.0.0
                          via 10.10.250.129, e28
N    10.0.2.0/30          [101] area: 0.0.0.0
                          via 10.10.250.129, e28
N    10.0.3.0/30          [101] area: 0.0.0.0
                          via 10.10.250.129, e28
N    10.0.4.0/30          [103] area: 0.0.0.0
                          via 10.10.250.129, e28
N    10.10.250.128/25     [100] area: 0.0.0.0
                          directly attached to e28
N    10.10.250.130/32     [0] area: 0.0.83.79
                          directly attached to lo
N    10.10.250.145/32     [100] area: 0.0.83.79
                          via 10.10.250.145, e2
N    10.10.250.161/32     [100] area: 0.0.83.79
                          via 10.10.250.161, e3
N    10.10.250.177/32     [200] area: 0.0.83.79
                          via 10.10.250.145, e2
                          via 10.10.250.161, e3

============ OSPF router routing table =============
R    10.10.1.1            [102] area: 0.0.0.0, ASBR
                          via 10.10.250.129, e28

============ OSPF external routing table ===========
N E1 0.0.0.0/0            [103] tag: 0
                          via 10.10.250.129, e28




=============== OSPF neighbor table ===============

Neighbor ID      Pri State    Up Time   Address          Interface
--------------   --- -------- --------  --------------   ---------
10.10.250.145      1 Full       7h38m   10.10.250.145    e2
10.10.250.161      1 Full       7h38m   10.10.250.161    e3
10.0.3.1         128 Full       7h38m   10.10.250.129    e28
```

5.3 Configurations for including DCP-2 chassis in OSPF

In this scenario, the management traffic for one or several DCP-2 chassis with transponders that should be routed over the OSPF network. The DCP-2 chassis must be connected to ports 17-20 in R11.1.

Shelf controller, DCP-SC-28P

ETH17 (subnet 192.168.1.1/28)

ETH2

IP 192.168.1.4/28   IP 192.168.1.2/28   IP 192.168.1.5/28

IP 192.168.1.3/28
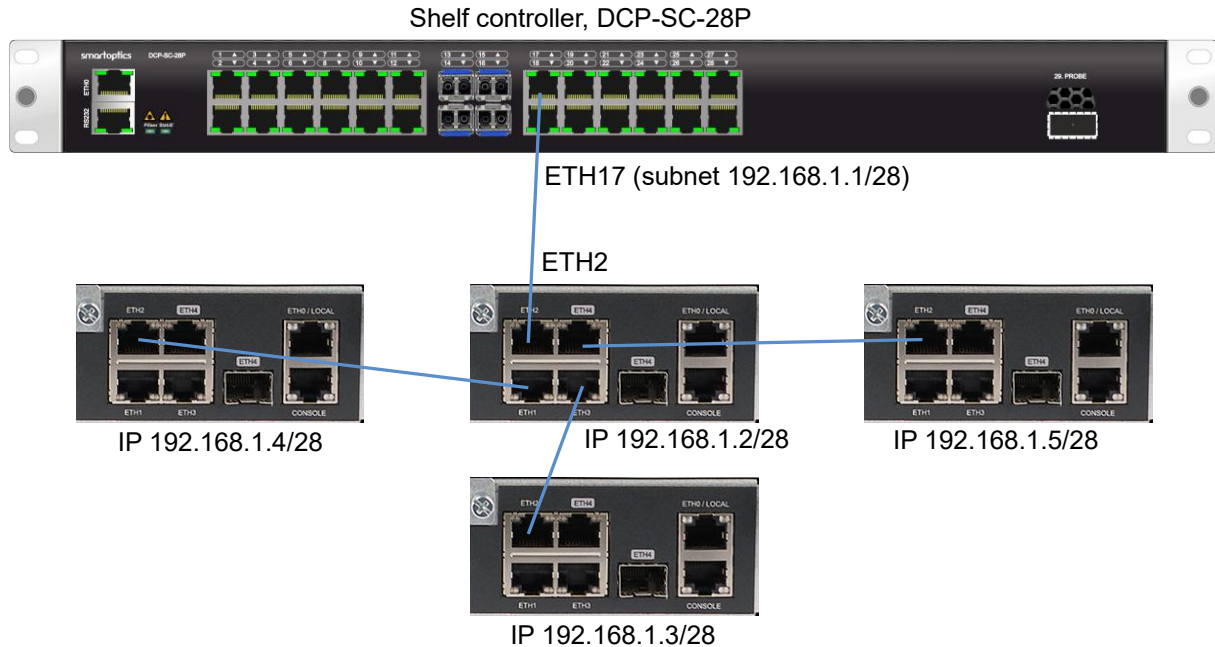
The configuration of the OSPF uplink should be done before the settings in this chapter are performed. Following steps are needed to include DCP-2 transponder chassis in OSPF:

1. Configure the IP address and subnet on the ports connected to the DCP-2 transponder chassis.
   Example:

   ```
   config network if-0/17 ipv4address 192.168.1.1 255.255.255.240
   ```

   Example:

   ```
   admin@localhost>config network if-0/17 ipv4address 192.168.1.1 255.255.255.240
   IP address for interface if-0/17 set to 192.168.1.1, subnet mask 255.255.255.240.
   ```

2. Change OSPF admin status on the ports connected to the DCP-2 transponder chassis

   ```
   config network ospf interface if-0/17 adminStatus up
   ```

   ```
   admin@localhost>config network ospf interface if-0/17 adminStatus up
   Admin status set to 'up'.
   ```

   Continue with port 18-20 if they are used.

3. Connect DCP-2 chassis

5.4 Configuring OSPF Areas

In large networks, it may be necessary to divide the topology into multiple OSPF areas to improve scalability and routing efficiency. Smartoptics systems support this by allowing configuration of custom OSPF area IDs.

You can change the OSPF area in two ways:

5.4.1 Configure a New OSPF Area (Globally)

This method changes the OSPF area ID for all interfaces **except uplink ports.**

5.4.1.1 Configure OSPF area

```
config network ospf areaId <area ID>
```

Example:

```
admin@localhost>config network ospf areaId 0.0.83.79
Area ID set to '0.0.83.79'.
```

5.4.2 Set OSPF Area Per Interface

For more granular control, you can assign specific OSPF areas to individual interfaces.

5.4.2.1 Configuring interface OSPF area

```
config network ospf interface <interface name> areaId <area ID>
```

Example:

```
admin@localhost>config network ospf interface if-0/28 areaId 0.0.83.79
Area ID set to 0.0.83.79 for interface e28.
```

This will set the OSFP individually for the desired interfaces.

6 Shelf controller configurations

This section describes the different shelf controllers' configurations.

6.1 Single shelf controller in a DCP-R node

The main shelf controller in a DCP-R only node controls a number of DCP-R degrees. The example below shows a node with 3 degrees.
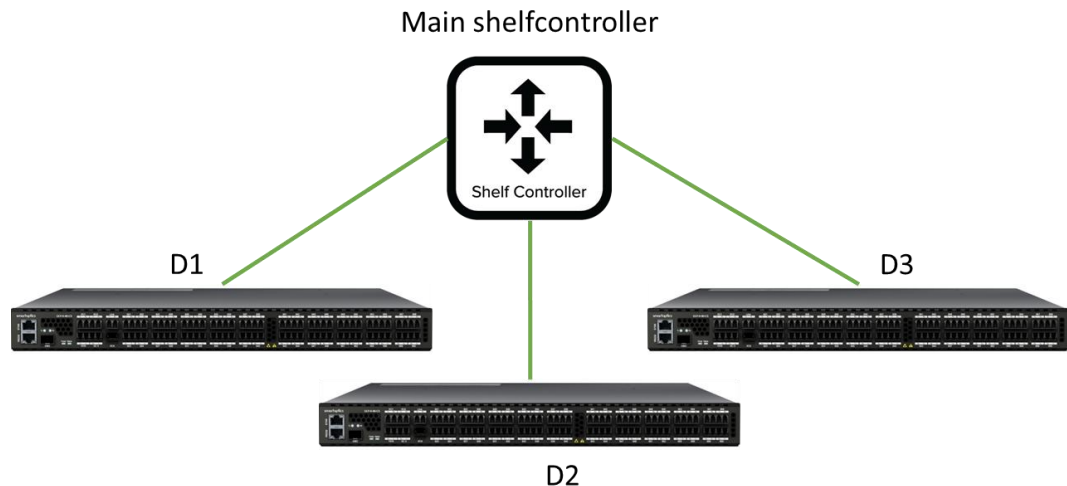
Figure 6. Single shelf controller in a DCP-R node.

6.2 Single shelf controller in a line amplifier node

The line amplifier node also needs a shelf controller to handle management traffic. The line amplifier connections are very similar to the main shelf controller connections with the difference that only one "lan port" is used for management, although it uses two "tunnel ports".

Main shelfcontroller
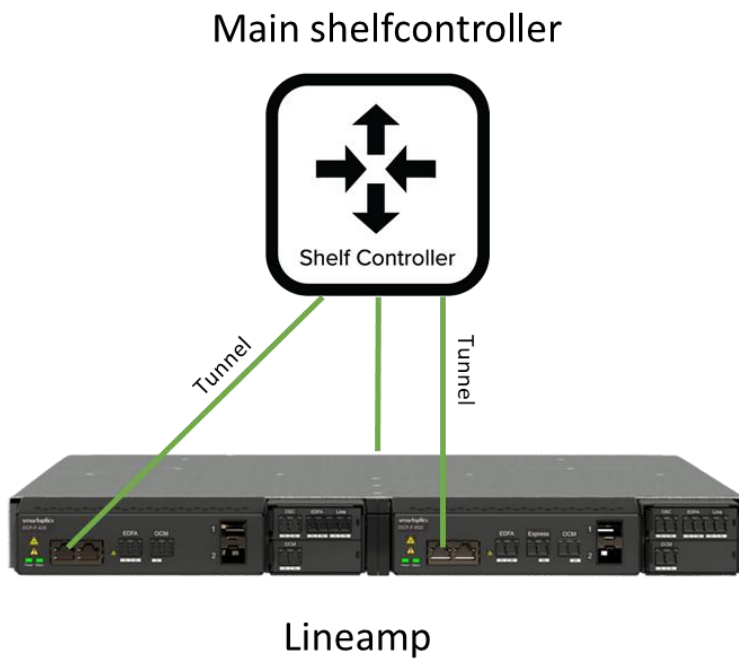
Figure 7. Single shelf controller in a line amplifier node.

6.3 Optically extended shelf controller

This mode is not supported with DCP-SC-28P in R11.1.x.

6.4 Redundant shelf controllers

This mode is not supported in R11.1.x.

7 Shelf controller operational procedures

7.1 DCP-SC-28P replacement

- Make sure that the replacement unit has the same SW release as the unit in the node before you do the replacement.

- Log in to DCP-SC-28P

- Connect the Ethernet cables from the new shelf controller to DCP-R degrees

- Run the command "show network lldp local neighbor" and check that the DCP-R degrees are visible

- *config node member replace <old serial number> <new serial number>*
  Example
  config node member replace S2441SC280020 S2441SC280019

7.2 DCP-SC-28P replacement in an ILA node

- Make sure that the replacement unit has the same SW release as the unit in the node before you do the replacement.

- Log in to DCP-SC-28P

- Connect the Ethernet cables from the new shelf controller to DCP-2

- Run the command "show network lldp local neighbor" and check that the ILA degrees are visible

- *config node member replace <old serial number> <new serial number>*
  Example
  config node member replace S2441SC280020 S2441SC280019

7.3 DCP-R replacement in ROADM node

This replacement instruction is valid when the replacement unit has the same model as the replaced unit, e.g. DCP-R-9D-CS to DCP-R-9D-CS. It is not possible to replace a DCP-R-9D-CS unit with a DCP-R-34D-CS unit with this instruction.

- Make sure that the replacement unit has the same SW release as the unit in the node before you do the replacement.

- Log in to DCP-SC-28P

- Connect the Ethernet cable from the new DCP-R to shelf controller

- Move the fibers from the old DCP-R to the new DCP-R.

- Run the command "show network lldp local neighbor" and check that the DCP-R degrees are visible

- config node member replace <old DCP-R serial number> <new DCP-R serial number>

- Reboot the new DCP-R to restore the traffic

7.4   DCP-2 replacement in ILA node

- Make sure that the replacement unit has the same SW release as the unit in the node before you do the replacement.

- Log in to DCP-SC-28P

- Connect the Ethernet cable from the new DCP-2 to shelf controller

- config node member replace <old DCP-2 serial number> <new DCP-2 serial number>

7.5   SW upgrade of DCP-SC-28P

The SW for both the DCP-SC-28P shelf controller and the DCP-R (ROADM node) or DCP-2 (ILA node) is done in the same process.
This is done in three steps. See CLI manual for more details.

1. Download SW to DCP-SC-28P
   swupgrade download <link to dcp-sc-28p-release-12.1.1.tar file>

   It is also possible to use sftpuser to transfer the file to the /swupgrade/ folder on the DCP-SC-28P, but then it is also necessary to do an internal download as well. Example: (note that it should be the file with dcp-sc-28p in the name)
   swupgrade download file:/swupgrade/dcp-sc-28p-release-12.1.1.tar

2. Install the SW
   All degrees will get the SW when "swupgrade set boot …" command is executed from the shelf controller.
   swupgrade set boot dcp-release-12.1.1

3. Reboot
   Using the "reboot" command from shelf controller will reboot all other degrees at same time.
   reboot

7.6   Reboot of shelf controller or DCP-R

It is possible to reboot the whole node or an individual node member.

For reboot of the whole node:
reboot

For reboot of individual node member:
reboot chassis-<chassis number>

7.7 Add new ROADM degree

A new ROADM degree can be added to the node with the command:

config node member add <serial number> chassis-<chassis number>

A host name for the new degree can be configured with the command:

config chassis [degree No] hostname

The topology on the node should be updated by running the command:
config node topology apply

The topology in SoSmart should be updated by using the action "Update Topology" on the node.

7.8 Remove ROADM degree

The last ROADM degree can be removed from the node with the command:

clear node member

The topology on the node should be updated by running the command:
config node topology apply

The topology in SoSmart should be updated by using the action "Update Topology" on the node.

7.9 Migrate SO-SHELF-CTRL-XX to DCP-SC-28P

From R12.0.1 it is possible to migrate from shelf controller of the type SO-SHELF-CTRL-XX to DCP-SC-28P.
See "SO-SHELF-CTRL_XX_User_Manual_R12.0.1" for more information.

8   SNMP

All SNMP configuration for both DCP-R and DCP-SC-28P is done from the shelf controller.

8.1   General

Simple Network Management Protocol (SNMP) is a protocol used for managing and monitoring network devices.

The DCP-R and DCP-SC-28P support SNMP version 1, 2c and 3. In SNMP version 1 and 2c user authentication is accomplished using community strings.

The default community string for the DCP-SC-28P and DCP-R is 'public'.

For security reasons, it is recommended to change the default community string.

The SNMP Interface supports:

a. SNMPv1 for Traps.

b. SNMPv2c for Traps and for Get operations.

c. SNMPv3 for Get operations.

SNMP Set is not supported.

8.2   SNMPv3 authentication and privacy

For SNMPv3 it is possible to configure multiple users. For each user it is possible to select authentication and privacy options. A wizard with several questions will be started when a new SNMPv3 user is added. Three options for authentication and privacy can be selected:

- noAuthNoPriv = No authentication or privacy will be configured

- authNoPriv = Authentication will be configured, but not privacy

- authPriv = Both authentication and privacy will be configured

```
admin@slotB>config snmp v3 user add

Adding SNMPv3 user.

Username: snmpTest1

Method (noAuthNoPriv, authNoPriv or authPriv): authPriv
Privacy protocol (DES or AES): AES
Privacy passphrase:
Error: Privacy passphrase must be between 12 and 32 characters long.
Privacy passphrase:

Authentication protocol (SHA or MD5): MD5
Authentication passphrase:
Confirm authentication passphrase:

SNMPv3 user 'snmpTest1' added.
```

The SNMPv3 users will only be activated if the SNMPv3 is enabled.

8.3   SNMP MIBS

Smartoptics provides a range of MIBs that can be used to monitor the DCP-R system. These include interface monitoring, port states including optical parameters such as Tx/Rx power levels.

For more specific details of the available SNMP MIBs, please refer to the manual 'DCP MIB description'.

8.4   SNMP Traps

Traps or notifications are messages that alert of events occurring in the DCP-R.

Trap	Description
coldStart	A coldStart trap signifies that the SNMP agent has been restarted.
dcpAlarmNotificationCleared	Sent when alarms are deactivated.
dcpAlarmNotificationCritical	Sent when an alarm of severity critical is activated
dcpAlarmNotificationMajor	Sent when an alarm of severity major is activated
dcpAlarmNotificationMinor	Sent when an alarm of severity minor is activated
dcpAlarmNotificationWarning	Sent when an alarm of severity warning is activated

9 User Access and Authentication

The DCP-R and DCP-SC-28P supports local authentication and Terminal Access Controller Access Control System Plus (TACACS+) to control access to the units.

All configuration for both DCP-R and DCP-SC-28P is done from the shelf controller.

9.1 Local authentication

The local authentication method is always enabled. The authentication is performed against a local database stored in the unit. The default user admin is a local user with default password admin. The admin user can't be removed from the node. Local authentication requires manual updates of usernames and passwords of each unit in the network.

For security reason, it is recommended to change the admin password.

Three user levels are possible: admin, operator and readonly. The admin user exists from start while the other two have to be enabled in CLI by the admin user.

9.2 RADIUS

RADIUS for DCP is implemented according to IETF RFC 2865 and RFC 2866.

The RADIUS remote authentication method is optional and can be enabled/disabled by the administrator. When enabled it establishes a TCP connection with a configured RADIUS server. When the user enters the username, the DCP unit communicates with the RADIUS server and verifies and confirms user credentials against a centralized database stored on the remote RADIUS server.

Note that you always login to chassis 1 when you are talking to a ROADM node. A ROADM node can consist of several DCP-R chassis in a cluster. Changing the password for chassis 1 will change the password for all chassis in the cluster. However, when RADIUS is enabled the RADIUS password will be required to login to the node, i.e. chassis 1. RADIUS is not used for direct login to other chassis.

9.2.1   Parameters used by RADIUS authentication.

Parameter	Description
adminStatus	**up**: Specifies if the RADIUS authentication is enabled **down**: Specifies if the RADIUS authentication is disabled
Timeout	Length of time that the DCP waits to receive a response from a RADIUS server. By default, the DCP waits 3 seconds. It´s possible to configure this value in the range from 0 through 90 seconds.
Retry	Number of times that the unit should try to verify the user's credentials. By default, the value is 1. It´s possible to configure this value in the range from 0 to 5.
primaryServer address	IPaddress or DNS name of the primary RADIUS server.
primaryServer port	RADIUS server port number. Valid values are between 0 and 65535. The default value is 1812.
primaryServer key	Specifies an authentication and encryption key of the primary RADIUS server. The key used by the local unit must match that used by the primary RADIUS server. The length of the key is restricted to 63 characters and can include any printable ASCII characters (If the password includes spaces, enclose the password in quotation marks).
secondaryServer address	IPaddress or DNS name of the secondary RADIUS server.
secondaryServer port	RADIUS server port number. Valid values are between 0 and 65535. The default value is 1812.
secondaryServer key	Specifies an authentication and encryption key of the secondary RADIUS server. The key used by the local unit must match that used by the secondary RADIUS server. The length of the key is restricted to 63 characters and can include any printable ASCII characters (If the password includes spaces, enclose the password in quotation marks).

9.2.2 Configuring RADIUS Authentication

These commands are used to configure the RADIUS settings. The system will only authenticate with the RADIUS server when RADIUS is configured to admin status up.

```
admin@dcpf-189>config aaa radius


adminStatus      - Configure RADIUS admin status.
primaryServer    - Configure RADIUS primary server.
retry            - Configure RADIUS server connection retry attempts.
secondaryServer  - Configure RADIUS secondary server.
timeout          - Configure RADIUS server connection timeout.


admin@dcpf-189>config aaa radius
```

9.2.2.1 Configuring RADIUS Server address

This command is used to configure the RADIUS server's addresses.

```
admin@dcpf-189>config aaa radius primaryServer address 10.10.134.33
Primary RADIUS server address set to '10.10.134.33'.


admin@dcpf-189>config aaa radius secondaryServer address 10.10.134.34
Secondary RADIUS server address set to '10.10.134.34'.
```

9.2.2.2 Configuring RADIUS Key

This command is used to configure the RADIUS server's key.

```
admin@dcpf-189>config aaa radius primaryServer key dcpRADIUSkey
Primary RADIUS server key set to 'dcpRADIUSkey'.


admin@dcpf-189>config aaa radius secondaryServer key dcpRADIUSkey2
Secondary RADIUS server key set to 'dcpRADIUSkey2'.
```

9.2.2.3 Configuring RADIUS Adminstatus

This command is used to enable/disable RADIUS authentication

```
admin@dcpf-189>config aaa radius adminStatus up
RADIUS admin status set to up.
admin@dcpf-189>
```

9.2.3 Show RADIUS status

To display the status for the RADIUS configuration, use the following command:

```
admin@dcpf-189>show aaa radius status


RADIUS admin status     : up

                                              Timeout
  Server     Address       Port  Key           Retry  [seconds]
  ---------  ------------  ----  ------------  -----  ---------
  Primary    10.10.134.33  1812  dcpRADIUSkey   1      3
  Secondary  10.10.134.33  1812  dcpRADIUSkey2  1      3


admin@dcpf-189>
```

9.2.4 Change a RADIUS user's password

To change the RADIUS user password, use the following command:

```
dcp_cli> config user chpasswd
```

The system will prompt the user to ask for old password and new password after the user executes the command.

9.2.5 How to specify user roles in RADIUS

There are three user levels available in the DCP platform: admin, operator and readonly. It is possible to map RADIUS users to any of these groups.

Use the following settings on the RADIUS server to map users to specific groups.

In Vendor-Specific attribute (Type = 26), set Vendor-Id to 30826 (IANA Enterprise Number for Smartoptics), Vendor type to 1, and the Attribute-Specific string to one of admin, operator, readonly.

Here is an example configuration for FreeRADIUS:

- In file: /etc/freeradius/3.0/dictionary add the following line
  $INCLUDE dictionary.smartoptics
- Create also the file /etc/freeradius/3.0/dictionary.smartoptics with the content:
  VENDOR Smartoptics 30826
  BEGIN-VENDOR Smartoptics
  ATTRIBUTE Smartoptics-Userrole 1 string
  END-VENDOR Smartoptics
- Users and their roles are defined in /etc/freeradius/3.0/users like usual using this syntax:
  readonly123   Cleartext-Password := "read123"
  Smartoptics-Userrole := "readonly"

  operator123   Cleartext-Password := "operator123"
  Smartoptics-Userrole := "operator"
- If changes are made to dictionary or users you need to restart Freeradius (as root or using sudo):
  systemctl restart freeradius

9.3 TACACS+

TACACS+ for DCP is implemented according to IETF "The TACACS+ Protocol", draft-ietf-opsawg-tacacs-18. TACACS+ protocol uses Transmission Control Protocol (TCP) as the transport protocol with destination port number 49.

https://datatracker.ietf.org/doc/draft-ietf-opsawg-tacacs/

The TACACS+ remote authentication method is optional and can be enabled/disabled by the administrator. When enabled it establishes a TCP connection with a configured TACACS+ server. When the user enters the username, the DCP unit communicates with the TACACS+ server and verifies and confirms user credentials against a centralized database stored on the remote TACACS+ server.

Note that you always login to chassis 1 when you are talking to a ROADM node. A ROADM node can consist of several DCP-R chassis in a cluster. Changing the password for chassis 1 will change the password for all chassis in the cluster. However, when TACACS+ is enabled the TACACS+ password will be required to login to the node, i.e. chassis 1. TACACS+ is not used for direct login to other chassis.

9.3.1 Parameters used by TACACS+ authentication

Parameter	Description
adminStatus	**up**: Specifies if the TACACS+ authentication is enabled **down**: Specifies if the TACACS+ authentication is disabled
Timeout	Length of time that the DCP waits to receive a response from a TACACS+ server. By default, the DCP waits 3 seconds. It´s possible to configure this value in the range from 1 through 90 seconds.
Retry	Number of times that the unit should try to verify the user's credentials. By default, the value is 1. It´s possible to configure this value in the range from 0 to 5.
primaryServer address	IPaddress or DNS name of the primary TACACS+ server.
primaryServer port	TACACS+ server port number. Valid values are between 0 and 65535. The default value is 49.
primaryServer key	Specifies an authentication and encryption key of the primary TACACS+ server. The key used by the local unit must match that used by the primary TACACS+ server. The length of the key is restricted to 63 characters and can include any printable ASCII characters (If the password includes spaces, enclose the password in quotation marks).
secondaryServer address	IPaddress or DNS name of the secondary TACACS+ server.
secondaryServer port	TACACS+ server port number. Valid values are between 0 and 65535. The default value is 49.
secondaryServer key	Specifies an authentication and encryption key of the secondary TACACS+ server. The key used by the local unit must match that used by the secondary TACACS+ server. The length of the key is restricted to 63 characters and can include any printable ASCII characters (If the password includes spaces, enclose the password in quotation marks).

9.3.2 Configuring TACACS+ Authentication

These commands are used to configure the TACACS+ settings. The system will only authenticate with the TACACS+ server when TACACS+ admin status is up.

```
dcp_cli> config aaa tacplus

adminStatus      - Configure TACACS+ admin status.

primaryServer    - Configure TACACS+ primary server.

retry            - Configure TACACS+ server connection retry attempts.

secondaryServer  - Configure TACACS+ secondary server.

timeout          - Configure TACACS+ server connection timeout.

dcp_cli>
```

9.3.2.1 Configuring TACACS+ Server address

This command is used to configure the TACACS+ server's addresses.

```
dcp_cli> config aaa tacplus primaryServer address 10.10.134.33

Primary TACACS+ server address set to '10.10.134.33'.


dcp_cli>config aaa tacplus secondaryServer address 10.10.134.34

Secondary TACACS+ server address set to '10.10.134.34'.
```

9.3.2.2 Configuring TACACS+ Key

This command is used to configure the TACACS+ server's key.

```
dcp_cli>config aaa tacplus primaryServer key sosrvtest01

Primary TACACS+ server key set to 'sosrvtest01'.


dcp_cli>config aaa tacplus secondaryServer key testing123

Secondary TACACS+ server key set to 'testing123'.
```

9.3.2.3 Configuring TACACS+ Adminstatus

This command is used to enable/disable TACACS+ authentication

```
dcp_cli> config aaa tacplus adminStatus up

TACACS+ admin status set to up.
```

9.3.3   Show TACACS+ status

To display status for a TACACS+, use the following command:

```
dcp_cli> show aaa tacplus status
TACACS+ admin status     : up

                                          Timeout
  Server     Address       Port  Key          Retry  [seconds]
  ---------  ------------  ----  -----------  -----  ---------
  Primary    10.10.134.33  4950  sosrvtest01  1      5
  Secondary  10.10.134.34  49    testing123   1      5
dcp_cli>
```

9.3.4   Change a TACACS+ user's password

If the server is configured with "End User Authentication Settings" it is possible to change the password of the current TACACS+ user via CLI commands on the DCP.

To change the TACACS+ user password, use the following command:

```
dcp_cli> config user chpasswd
```

The system will prompt the user to ask for old password and new password after the user executes the command.

9.3.5   Troubleshooting TACACS+ server connection with NETCAT

In case the DCP unit is not able to connect with the TACACS+ server, there might be some firewall or access list blocking the traffic. Verify the connectivity to the TACACS+ server with netcat by issuing the following commands.

```
dcp_cli> nc <address> <port>
```

Attribute	Description
<address>	Specifies the IP address of the TACACS+ server.
<port>	Specifies the port number of the TACACS+ server. Valid value is between 0 and 65535. Default value is 49.

9.3.1   How to specify user roles in TACACS

There are three user levels available in the DCP platform: admin, operator and readonly. It is possible to map TACACS users to any of these groups.

Use the following settings on the TACACS server to map users to specific groups.

Set attribute userrole=<role> where <role> is one of admin, operator, readonly.
In TACACS+ servers based on https://shrubbery.net/tac_plus/ this can be done as follows:

```
user = albert {
        name = "Albert Einstein"
        login = cleartext "E=mc^2"
        member = "admin"
        service = exec {
                userrole = readonly        <-- this line sets the user role to
'readonly'
        }
}
```

10 Audit Trail

The DCP platform records events that occur within the system and provides logging mechanism for Authentication, Fault management and Accounting.

All configuration for both DCP-R and DCP-SC-28P is done from the shelf controller.

10.1 Authentication

The Access Logs enables tracking of login/logout and password changes activity of users including unsuccessful login events. The last 200 events is kept within the node and for longer history keeping of events an external Syslog should be configured. When the max allowed log entries is reached, the oldest entries are overwritten with new events.

10.1.1 show syslog access

To display access logs, use the following command:

```
dcp_cli> show syslog access

  Time                PID   Remote host     Event

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

  2020-06-02 08:25:42  1021  10.212.148.241  Local User admin logged in
dcp_cli>
```

10.2 Fault management

The Alarm log keeps track of all activated and deactivated alarms occurred within the system. The last 200 events is kept within the node and for longer history keeping of events an external Syslog should be configured. When the max allowed log entries is reached, the oldest entries are overwritten with new events.

10.2.1 show syslog alarm

To display alarm logs, use the following command:

```
dcp_cli>show syslog alarm
  Time             Alarm
  ------------------  --------------------------------------------------------------------------------
  2020-05-29 06:16:13  Alarm "Power supply missing" activated on interface psu-1/2 with severity critical.
dcp_cli>
```

10.3　　　　　Accounting

The Configuration log enables tracking of all config, clear, reboot and swupgrade commands activity within the system. The last 200 events are kept within the node and for longer history keeping of events an external Syslog should be configured. When the max allowed log entries is reached, the oldest entries are overwritten with new events.

10.3.1　show syslog config

To display the configuration logs, use the following command:

```
dcp_cli>show syslog config
  Time                User      Remote host     Event
  ------------------  --------  --------------  --------------------
  2020-06-02 08:49:57  admin@CLI  10.212.148.241  clear alarm log
  2020-06-02 08:50:12  admin@CLI  10.212.148.241  config slot 1 reboot
dcp_cli>
```

11 Syslog

Syslog is a standard log transport mechanism that enables the aggregation of log data into a central repository for archiving, analysis, and reporting. The DCP platform can be configured to forward Access, Alarm and Configuration logs to an external syslog server. It's possible to configure the transport with TCP for reliable and secure log forwarding, or UDP for non-secure forwarding.

All configuration for both DCP-R and DCP-SC-28P is done from the shelf controller.

11.1.1 Parameters to communicate with remote syslog

Parameter	Description
Access	**Disable**: Disables sending access log to remote syslog server. **Enable:** Enables sending access log to remote syslog server.
adminStatus	**up**: Specifies if the remote syslog server is enabled **down**: Specifies if the remote syslog server is disabled
Alarm	**Disable**: Disables sending alarm log to remote syslog server. **Enable:** Enables sending alarm log to remote syslog server.
Config	**Disable**: Disables sending config log to remote syslog server. **Enable:** Enables sending config log to remote syslog server.
Port	Remote syslog server port number. Valid values are between 0 and 65535.
Protocol	**tcp:** Configure remote syslog server network protocol to tcp. **udp**: Configure remote syslog server network protocol to udp.
Primary Server	IP address or DNS name of the primary syslog server.
Secondary Server	IP address or DNS name of the secondary syslog server.

11.1.2 Configuring remote syslog

These commands are used to configure and sending system messages to a specified syslog server.
The system will only send messages to the server when admin status is up.

```
dcp_cli> config syslog remote

access        - Configure sending access log to remote syslog servers.
adminStatus   - Configure remote syslog server admin status.
alarm         - Configure sending alarm log to remote syslog servers.
config        - Configure sending configuration log to remote syslog servers.
primaryServer   - Configure remote primary syslog server.
secondaryServer - Configure remote secondary syslog server.
dcp_cli>
```

11.1.2.1 config syslog remote access enable/disable

This command is used to enable/disable sending access log system messages to remote syslog server.

```
dcp_cli>config syslog remote access enable
Enabled sending access log to remote syslog server.
admin@hostname>config syslog remote access disable
Disabled sending access log to remote syslog server.
dcp_cli>
```

11.1.2.2 config syslog remote adminStatus up/down

This command is used to enable/disable sending system messages to remote syslog server.

```
dcp_cli>config syslog remote adminStatus up
Remote syslog server admin status set to up.
dcp_cli>config syslog remote adminStatus down
Remote syslog server admin status set to down.
dcp_cli>
```

11.1.2.3 config syslog remote alarm enable/disable

This command is used to enable/disable sending alarm log system messages to remote syslog server.

```
dcp_cli>config syslog remote alarm enable
Enabled sending alarm log to remote syslog server.
dcp_cli>config syslog remote alarm disable
Disabled sending alarm log to remote syslog server.
dcp_cli>
```

11.1.2.4 config syslog remote config enable/disable

This command is used to enable/disable sending config log system messages to remote syslog server.

```
dcp_cli>config syslog remote config enable
Enabled sending configuration log to remote syslog server.
dcp_cli>config syslog remote config disable
Disabled sending configuration log to remote syslog server.
dcp_cli>
```

11.1.2.1 config syslog remote primaryServer address <address>

This command is used to configure the IP address of the primary syslog server.

```
dcp_cli> config syslog remote primaryServer address 10.10.11.22
Remote primary syslog server address set to '10.10.11.22'.
dcp_cli>
```

11.1.2.2 config syslog remote primaryServer port <port>

This command is used to configure the remote syslog port number for the primary server.

```
dcp_cli>config syslog remote primaryServer port 514
Remote primary syslog server port set to '514'.
dcp_cli>
```

11.1.2.3 config syslog remote primaryServer protocol <protocol>

This command is used to configure the remote syslog network protocol for the primary server.

```
admin@L8-109-B-D1>config syslog remote primaryServer protocol
tcp udp
admin@L8-109-B-D1>config syslog remote primaryServer protocol udp
Primary remote syslog server network protocol set to udp.
```

11.1.3   show syslog status

To display the status of the configured syslog, use the following command:

```
admin@Stockholm-97>show syslog status
Remote syslog admin status     : up
  Server     Address       Protocol  Port
  ---------  -----------   --------  ----
  Primary    10.10.11.22   udp       514
  Secondary                udp       514


  Log     Remote logging  Facility
  ------  --------------  ---------------
  Access  enabled         auth + authpriv
  Alarm   enabled         local7
  Config  enabled         local6
```

12 Waste management

The HW should be treated as electronic waste when it is decommissioned and taken out of service.

13 Technical Specifications

ENVIRONMENT:	
OPERATING TEMPERATURE	0° C to 45° C
HUMIDITY	5% to 85% RHI
SUPPLY VOLTAGE	Dual feeding DCP-2-PSU-AC-FB: 100-127VAC (3A) and 200-240 VAC (1,5A) DCP-2-PSU-DC-FB: -40 to -72 VDC (7A)
POWER CONSUMPTION DCP-SC-28P	DCP-SC-28P chassis with fans and 2 PSU (AC) Max: 61W at steady state without QSFP-DD at +45 Deg C Typical: 34W at steady state without QSFP-DD at +25 Deg C Max: 47W during startup without QSFP-DD at +25 Deg C
REDUNDANCY	Hot swappable fan & PSUs
COOLING FANS	Front-to-Back straight through airflow
ALTITUDE	3000 m (10.000 ft.)
DIMENSIONS (DCP-R):	
HEIGHT	1.77" (1 RU) (H), 45mm (H)
WIDTH	17.3" (W), 440mm (W)
DEPTH	19.88" (D), 505mm (D)
WEIGHT	~ 5.8 Kg (DCP-SC-28P chassis without PSU) ~ 7.3 Kg (DCP-SC-28P chassis with PSU)

NETWORK MANAGEMENT:	
MANAGEMENT INTERFACES	1 x RS-232 serial port in front side 1 x RJ-45 local craft 10/100/1000 Base-T in front side
SOFTWARE UPGRADE	Traffic hitless – dual image
BOOT TIMING	Booting from Coldstart < 5min Warmstart reboot < 2min
PROTOCOLS	CLI, SNMP, SYSLOG, TACACS+, RADIUS, NETCONF, OSPF

REGULATORY COMPLIANCES	
EMC	Title 47 CFR Part 15 Subpart B EN55024/CISPR24: 2011 + A1:2015 EN55032:2015/CISPR32 ETSI EN 300 386 V2.1.1
SAFETY	CB (IEC 60950-1:2005+A1+A2) ETL (CSA C22.2#62368-1:2014 Ed.2, UL 62368-1:2014 Ed.2)
NEBS	Level 3
LASER SAFETY	IEC 60825-1 : 2007 (2nd Edition) IEC 60825-1:2014 (Third Edition)

13.1 Supported transceivers in SFP/SFP+ port

CERTIFIED TRANSCEIVERS FOR OSC	
PART NUMBER	Description
TBD	