DCP-Series

User Manual

dcp-release-12.1.3

DCP-2

DCP-PAS-H

DCP-101

DCP-1610

DCP-108

DCP-404

DCP-1203

DCP-110

Contents

1 Introduction

1.1 General

The DCP-series is an optical transmission platform. The DCP-2 is a 19” 1U chassis system with front-to-back airflow. It has 2 slots able to house traffic units. On the back side of the chassis, it has hot-pluggable redundant power supplies and a fan unit including 4 individual fans. The current traffic units include:

- DCP-101 1 x 100G transponder
- DCP-1610 10 x 1G-16G transponder
- DCP-108 8 x 100G transponder
- DCP-404 4x100G to 1x400G muxponder
- DCP-1203 3 x 100/400G transponder
- DCP-110 10x10G to 1x100G muxponder
- DCP-PAS-H A passive holder for passive units from H-series

1.2 DCP-series

The key features for the DCP-series are:

- Open software platform.
- Simple plug and play platform that can be up and running in minutes.
- Redundant, hot pluggable power supplies, for both AC and DC power.
- Management interfaces.
- 1U building practice with front-to-back airflow.
- The unit can be managed/monitored via CLI, SNMP and supports SYSLOG as well as TACACS+ remote authentication

Figure 1-1. Front view of DCP-2 populated with 2x DCP-101 traffic units.

1.3 In commercial confidence

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

1.4 Document Revision History

Revision	Date	Description of changes
8.1.1 A	2023-06-20	Release version of R8.1.1
8.1.2 PA1	2023-08-09	Updated alarm list
8.1.3 PA1	2023-08-10	Added SNMPv3 authentiation and privacy settings Added clarification text for communication failure and SW mismatch alarms
9.0.1 A	2024-01-19	Added chapter with DCP-110
10.0.1 A	2024-06-28	Added altitude Added chapter about waste management Updated chapter about user accounts
10.0.2 A	2024-09-05	Added text about user levels admin, opertor, readonly Added chapters for RADIUS and TACACS settings for different user levels
10.0.2 B	2024-10-24	Updated encryption chapter added DCP-PAS-H
10.1.1 A	2024-11-20	No update
11.0.1 A	2024-12-12	Updated with examples for user roles in RADIUS
11.0.2 A	2024-12-17	Updated alarm list
11.1.1 A	2025-03-26	No update
11.3.1 A	2025-04-24	No update
12.0.1 A	2025-06-16	Added chapter about dynamic update of certified transceiver list
12.0.2 A	2025-08-06	Added table with allowed actions for different users
12.1.1 A	2025-09-08	No update
12.1.3 A	2025-10-23	Updated chapter with encryption to include DCP-1203 and fiber intrusion for all transponders

2 Functional description

2.1 Typical Application

2.1.1 PAM4 Based 100G Ethernet Transport

The DCP-108 is an 8 x 100G transponder with QSFP28 transceivers on all interfaces. The typical application for this product is to convert between QSFP28 SR4, LR4, CWDM4 and QSFP28 PAM4 DWDM. The typical use cases when this is needed are:

- Act as a demarcation point for wholesale applications
- Provide PAM4 support if the switch/router does not support PAM4 optics

This product has to be used together with the DCP-M Open-Line-System in order for the QSFP28 PAM4 DWDM to work.

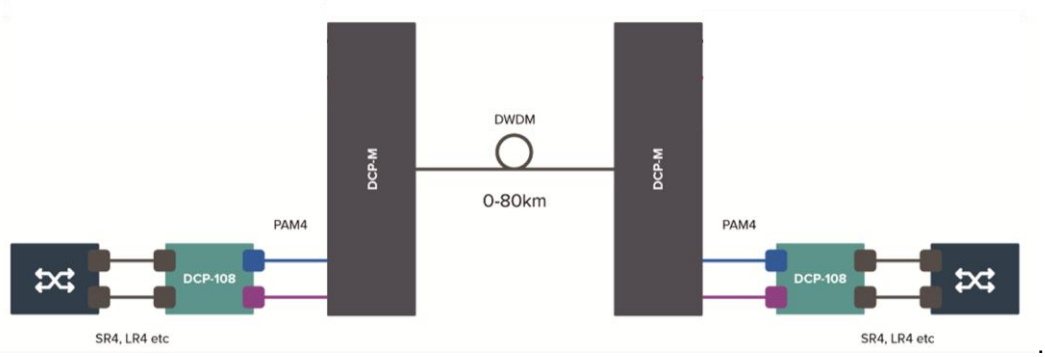


Figure 2-1. Typical application with DCP-2 and DCP-108s as demarcation.

2.1.2 Coherent Based 100G Ethernet Transport

The DCP-101 is a 100G transponder between a QSFP28 and CFP transceiver. Typical applications are DWDM networks or distance extension.
The client equipment is connected to the QSFP28 port via a SR4, LR4, CWDM4, PSM4 or CR4 interface (suitable transceiver must be selected). The DWDM coherent line signal from the CFP is enabling the long-distance transmission and is usually connected to an Open-Line-System, like the Smartoptics DCP-M or DCP-F.

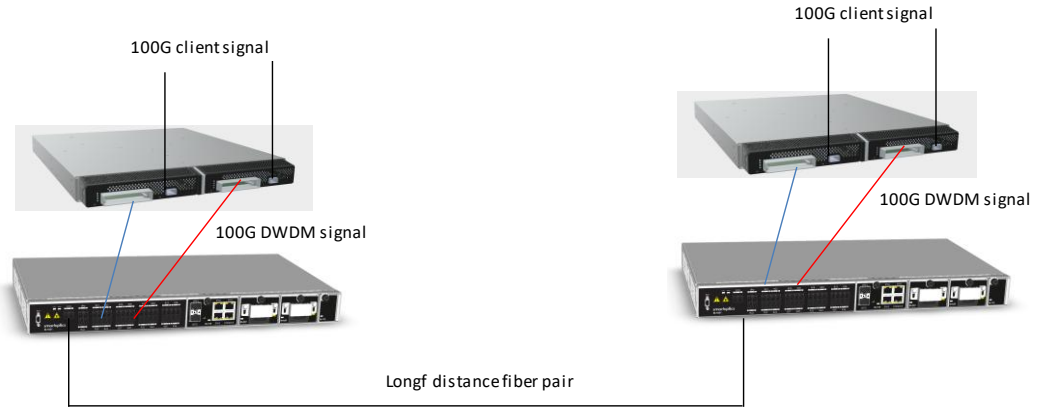


Figure 2-2. Typical application with DCP-2 and DCP-101s as 100G DWDM distance extension solution.

2.1.3 10G/40G Ethernet & 16G Fibre Channel Transport

The below illustration shows one side of a distance extension solution for 10G/40G Ethernet or 16G Fibre Channel with the DCP-1610. 40G Ethernet can be transported using a QSFP+ fanout cable to 4x10G. The DCP-1610 will use 4 transponders and 4 DWDM wavelength to transport the data.

All other protocols can be transported directly over a transponder.

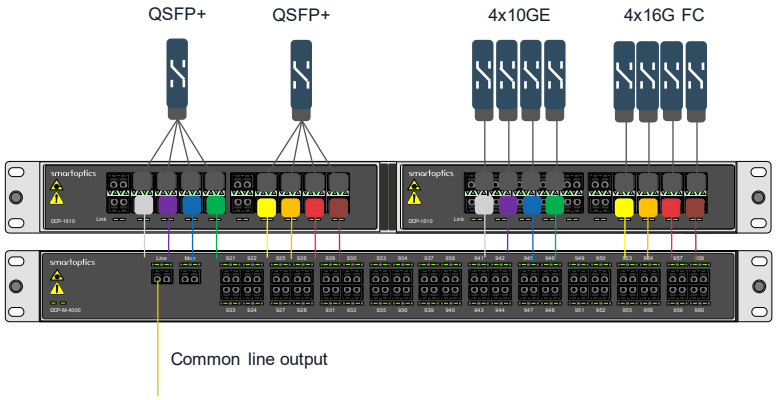


Figure 2-3. Typical transponder application with DCP-1610.

2.2 Physical Description & Plug-in Units

The DCP-2 is a compact unit, intended for installation in 19” racks or on shelves. The unit height is 1U (1.77 in). All power and management connection are in the back panel and all traffic connections are made to the front panel. The DCP has a front-to-back or back-to-front airflow. The DCP-2 chassis is populated with 2 pcs redundant power supplies and 1 fan unit (with 4 fans).

Figure 2-4. DCP-2 chassis front-view and slot nomination.

In the front 2 traffic slots are available. The left slot is called slot “1” and the right slot is nominated as slot “2”. The plug-in units extraction mechanism is based in the center of the chassis.

Figure 2-5. Back view 2 AC power supplies, 1 fan unit (with 4 fans) and network management interfaces.

The back of the DCP-2 chassis houses 4xRJ45 Ethernet ports for management access. ETH4 is a dual personality port and can also be used with an optical SFP interface. The 2 power supplies and fan-unit are hot pluggable. An additional RS-232 serial interface is accessible as console port.

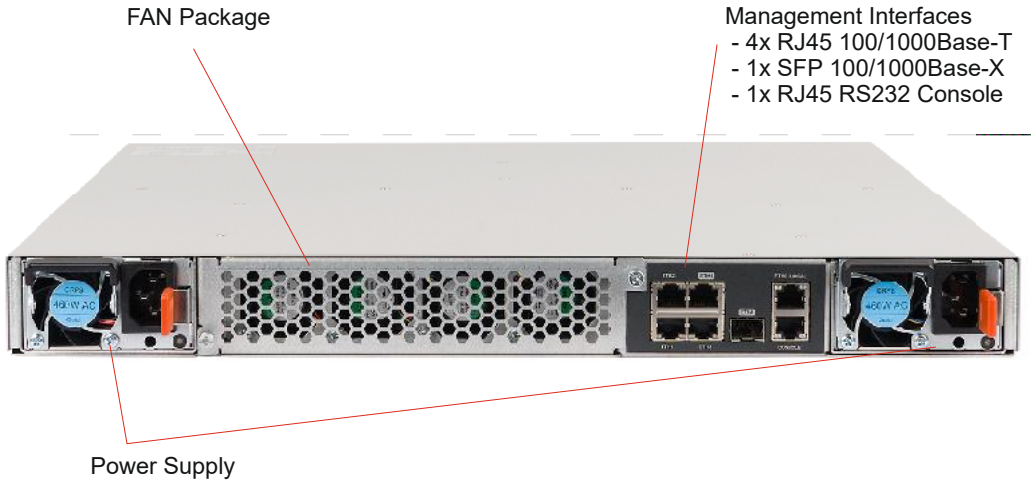


Figure 2-6. DCP-2 chassis back-view.

2.2.1 DCP-108

The DCP-108 consists of eight independent transponders with QSFP28 support on all ports.

In the typical use case the client interfaces will be equipped with QSFP28 transceivers of SR4, LR4 or CWD4 type and the line interfaces will be equipped with PAM4 QSFP28 DWDM transceivers. From software release 5.3.1, 40G or 100G Ethernet is supported on both the client and line side.

Figure 2-7. Front view of DCP-108 plug-in unit.

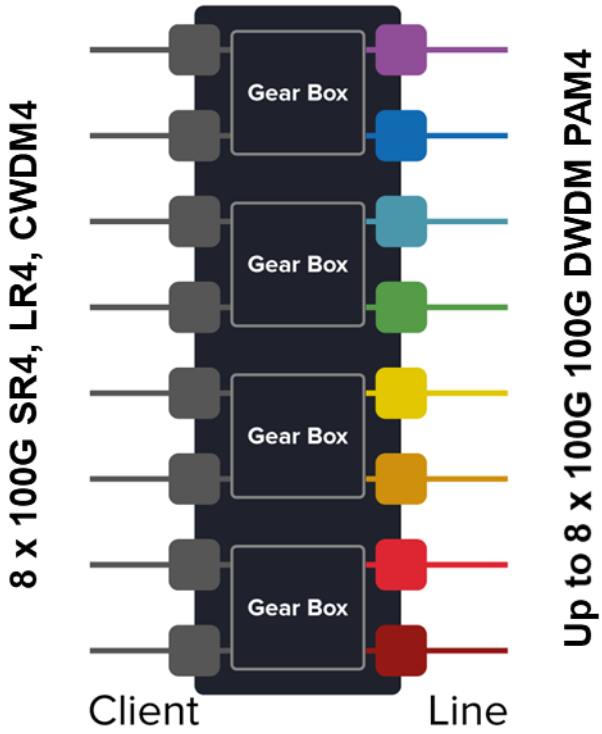


Figure 2-8. Basic function of DCP-108.

2.2.2 DCP-101

The DCP-101 is a 100G transponder between a QSFP28 and CFP transceiver.

The client equipment is connected to the QSFP28 port via a SR4, LR4, CWDM4, PSM4 or CR4 interface (suitable transceiver must be selected). A coherent DWDM CFP is generating the DWDM line signal. The line interface is operated at OTU-4 line rate.

Figure 2-9. Front view of DCP-101 plug-in unit.

The below picture illustrates the function of the DCP-101.

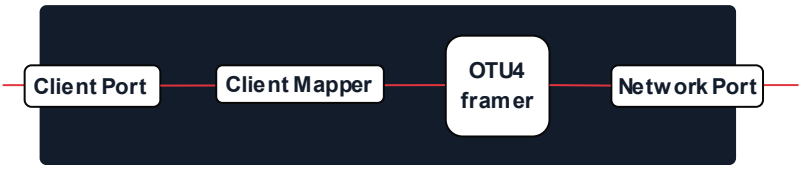


Figure 2-10. Basic function of DCP-101.

2.2.3 DCP-1610

The DCP-1610 is a 10x multilane transponder with 10 independent transponders. Each transponder can handle data-rates from 1G to 14.3 Gbps.

Figure 2-11. Front view of a DCP-1610 traffic unit.

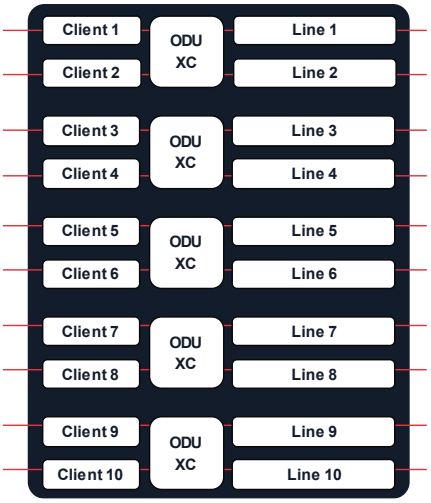


Figure 2-12. Basic function of DCP-1610.

The DCP-1610 supports the following traffic formats:

Service	Client Protocol	Client Datarate	Line Protocol	Line Datarate
1GbE-1GbE	1GbE	1,25 Gbit/s	1GbE	1,25 Gbit/s
1GbE-OTU2	1GbE	1,25 Gbit/s	OTU2	10,709225 Gbit/s
10GbE-10GbE	10GbE	10,3125 Gbit/s	10GbE	10,3125 Gbit/s
10GbE-OTU2e	10GbE	10,3125 Gbit/s	OTU2e	11,095727 Gbit/s
16GFC-16GFC	16GFC	14,025 Gbit/s	16GFC	14,025 Gbit/s
40GbE-40GbE	10GbE	10,3125 Gbit/s	10GbE	10,3125 Gbit/s
8GFC-8GFC	8GFC	8,5 Gbit/s	8GFC	8,5 Gbit/s
8GFC-OTU2	8GFC	8,5 Gbit/s	OTU2	10,709225 Gbit/s
1GbE-1GbE	1GbE	1,25 Gbit/s	1GbE	1,25 Gbit/s
STM64-STM64	STM64	9,95328 Gbit/s	STM64	9,95328 Gbit/s
STM64-OTU2	STM64	9,95328 Gbit/s	OTU2	10,709225 Gbit/s
OTU2e-OTU2e	OTU2e	11,095727 Gbit/s	OTU2e	11,095727 Gbit/s
OTU2-OTU2	OTU2	10,709225 Gbit/s	OTU2	10,709225 Gbit/s
40GbE-OTU2e	10GbE	10,3125 Gbit/s	OTU2e	11,095727 Gbit/s
Supported Encryption Client Formats				
1GbE-OTU2Enc	1GbE	1,25 Gbit/s	OTU2Enc	10,709225 Gbit/s
10GbE-OTU2eEnc	10GbE	10,3125 Gbit/s	OTU2eEnc	11,095727 Gbit/s
STM64-OTU2Enc	STM64	9,95328 Gbit/s	OTU2Enc	10,709225 Gbit/s
16GFC-OTU2xEnc	16GFC	14,025 Gbit/s	OTU2xEnc	14,083928 Gbit/s
8GFC-OTU2Enc	8GFC	8,5 Gbit/s	OTU2Enc	10,709225 Gbit/s
OTU2	OTU2	10,709225 Gbit/s	OTU2Enc	10,709225 Gbit/s
OTU2e	OTU2e	11,095727 Gbit/s	OTU2eEnc	11,095727 Gbit/s
40GbE-OTU2eEnc	40GbE	4 x 10,3125 Gbit/s	OTU2eEnc	4 x 11,095727 Gbit/s
1GbE-OTU2Enc	1GbE	1,250 Gbit/s	OTU2eEnc	11,095727 Gbit/s

Note that DCP-1610 will not recognize 16G FC if FEC is enabled in the FC switches.

2.2.4 DCP-404

The DCP-404 is a muxponder with 4x100G clients and one 400G line. This card will take one slot in a DCP-2 chassis.

Figure 1. *Front view of DCP-404 plug-in unit.*

The client side use QSFP28 pluggables and support 4x100GBE. Different options of QSFP28 pluggables can be used, e.g. SR4, LR4, CWDM4, ER4, ZR4.

The line side use coherent 400G OpenZR+ DWDM QSFP-DD pluggables and grey 400G QSFP-DD pluggables.

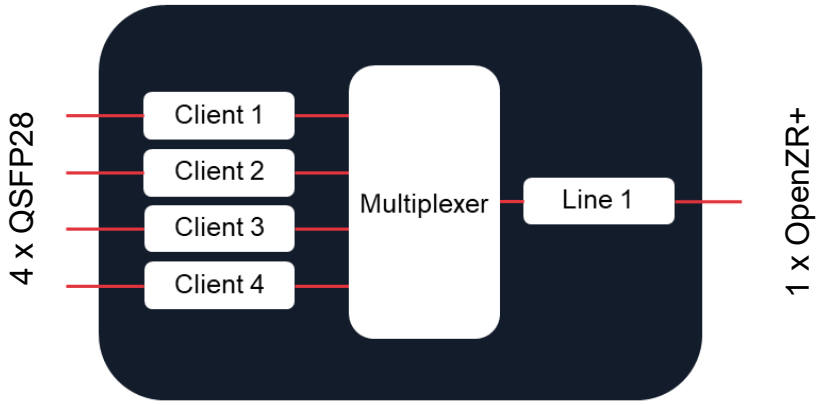


Figure 2. *Functional diagram for DCP-404.*

The line side can be configured line side can be configured to use different bit rates and modulation formats.The following multiplexing combinations are supported:

- 4 x 100G using 400G-16QAM on the line
- 3 x 100G using 300G-8QAM on the line
- 2 x 100G using 200G-QPSK on the line
- 1 x 100G using 100G-QPSK on the line
- 2 x 100G using 200G-16QAM on the line

2.2.5 DCP-1203

The DCP-1203 is a transponder with 3x100/400G clients and 3x100/400G lines. This card will take one slot in a DCP-2 chassis.

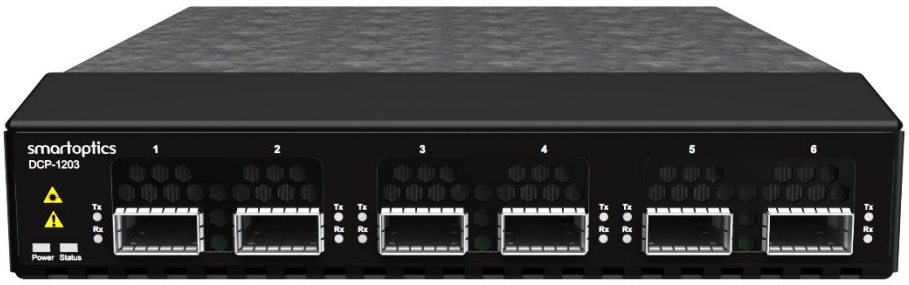


Figure 3. *Front view of DCP-1203 plug-in unit.*

The client side use QSFP28 or QSFP-DD transceivers and support 100GBE and 400GBE. Different options of QSFP28 and QSFP-DD transceivers can be used, e.g. SR4, LR4, CWDM4, ER4, ZR4.

The line side use coherent 100/400G DWDM QSFP-DD transceivers.

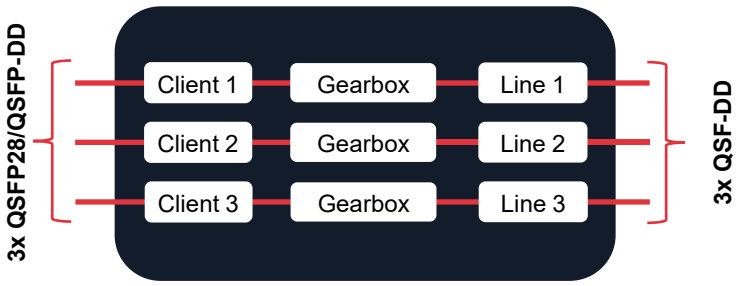


Figure 4. *Functional diagram for DCP-1203.*

The line side can be configured line side can be configured to use different bit rates and modulation formats.The following multiplexing combinations are supported:

- 1 x 100GBE using 100G-QPSK on the line
- 1 x 400GBE using 400G-16QAM on the line

2.2.6 DCP-110

The DCP-110 is a muxponder with 10x10GBE clients and one 100G line. This card will take one slot in a DCP-2 chassis.

Figure 5. *Front view of DCP-110 plug-in unit.*

The client side use SFP+ transceivers and support 10x10GBE. Different options of SFP transceivers can be used, e.g. SR, LR, ER, ZR. See chapter Technical data for supported formats and transceivers.

The line side can use grey QSFP28 or coherent 100G ZR+ DWDM QSFP-DD transceivers.

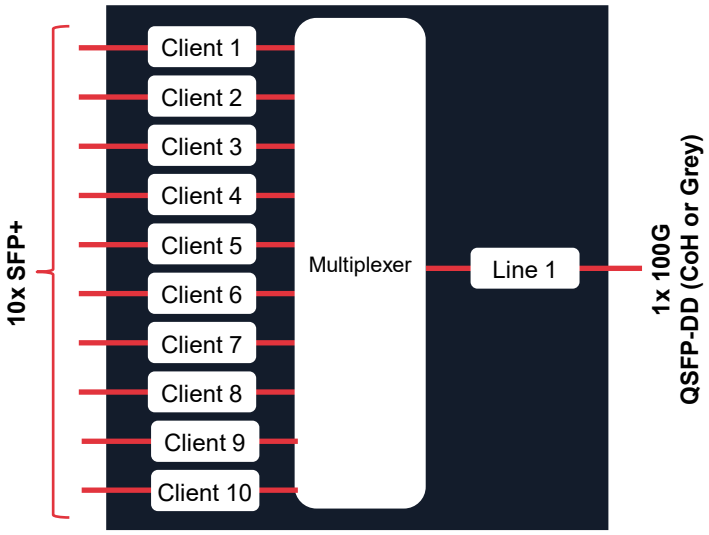


Figure 6. *Functional diagram for DCP-110.*

The line side can be configured to use grey QSFP28 transceivers or coherent 100G QPSK DWDM QSFP-DDs. Note that the DCP-110 card use MLG mapping and it is required that the coherent line transceivers support MLG mode.

2.2.7 DCP-PAS-H

The DCP-PAS-H is a card that can host passive units from the H-series. This card will take one slot in a DCP-2 chassis.

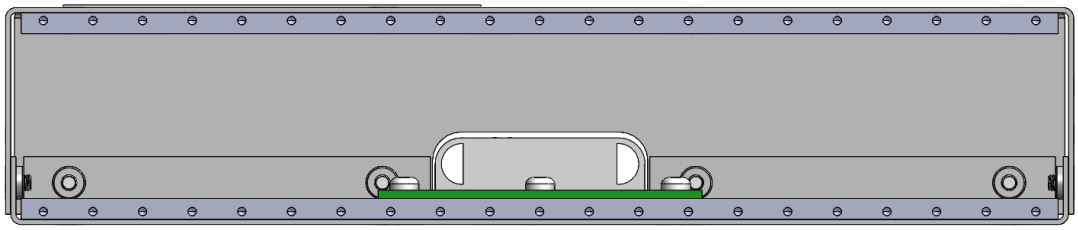


Figure 7. *Front view of DCP-PAS-H plug-in unit.*

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-2 is dual feed and the power supplies are hot swappable. Both types can be used simultaneously.

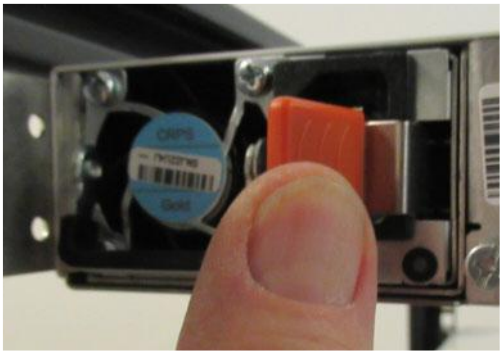
Figure 2-13. The DCP-2-PSU-AC-FB and DCP-2-PSU-DC-FB unit.

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-2-FAN-FB Fan Unit

The DCP-2 has a fan unit which consists of 4 fans. The fan speed is controlled via the MCU and the system is designed to operate with 3 working fans. If one fan fails the other 3 will speed up to compensate and an alarm will trigger to replace the fan unit.

Figure 2-14. The DCP-FAN-FB unit.

2.4.1 Replacing DCP-2-FAN-FB Fan Unit

NOTE - To prevent overheating, install the replacement fan tray immediately after removing the existing fan tray.

1. Loosen the screws on each side of the fan tray faceplate.
2. Grasp both sides of the fan tray and pull it out

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.

2.4.2 Installing DCP-2-FAN-FB Fan Unit

1. Grasp the fan tray on each side and insert it straight into the chassis.
2. Tighten captive screws on each side of the fan tray faceplate to secure it in the chassis to a torque of 17 cm-kg (15 in-lb.)

2.5 Blind Plate

The DCP-2 is delivered with a blind plate. If only 1 traffic module is being used in the DCP-2 chassis this blind plate should be mounted to the empty slot to help guide the airflow through the traffic unit.

Figure 2-15. Blind Plate for DCP-2.

2.6 Network Management Interfaces

The Network Management Interface is a part of the DCP-2 chassis. The interfaces are available at the back panel and shown in the figure below. The management system collects and controls system relevant information.

The module has:

- Console - 1x RJ45 console port for serial access to the chassis and initial setup.
- ETH1/ETH2/ETH3/ETH4 - 4x 100/1000Base-T. Management interfaces to the DCP-2 that can be connected to a DCN network or when connecting multiple chassis to create a larger NE.
- ETH4 - 1x SFP port 100/1000Base-X for optical management access to the NMB that can be connected to a DCN network. The SFP port is shared with the electrical ETH4 port and only one can be used at a time.
- ETH0 - 1x 100/1000Base-T “local” port access to the unit for engineers onsite.

Figure 2-16. View of the network management communication interfaces.

2.7 Management architecture

The below figure shows the principle architecture of the system management. The current implemented APIs are CLI and SNMP.

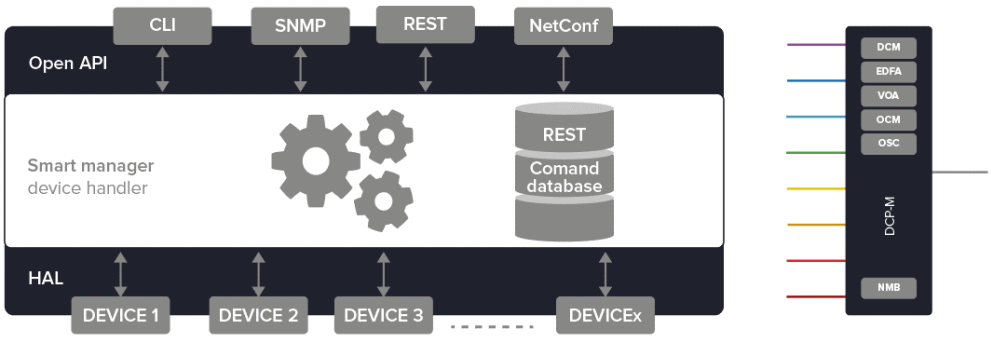


Figure 2-17. Management architecture.

2.8 Monitor points

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

2.9 Alarms

The DCP-2 keeps 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.

ALARM MESSAGE	LOCATION	SEVERITY	INTERPRETATION
Board missing	if-<chassi>/<slot>	Major	The module has been removed. Insert a module or disable the alarm with “clear slot 1/2 boardMissingAlarm”
eMMC Failure		Minor	The memory is not formatted. Contact support.
Fan failure	fan-1/1	Major	Fan unit has failed. Replace within 24 hours.
Fan missing	fan-1/1	Critical	Fan is missing in chassis.
Power supply failure	psu-1/1 psu-1/2	Major	Input AC/DC power is lost on the unit
External power missing	psu-1/1 psu-1/2	Minor	This alarm appears when the external power is not connected or not working.
Power supply fan failure	psu-1/1 psu-1/2	Minor	The fan unit in the power supply has failed
Power supply communication failure	psu-1/1 psu-1/2	Major	The chassis cannot communicate with the power supply unit
Power supply input voltage high	psu-1/1 psu-1/2	Minor	The input voltage is too high
Power supply input voltage low	psu-1/1 psu-1/2	Minor	The input voltage is too low
Power supply missing	psu-1/1 psu-1/2	Critical	This alarm appears when the unit is not inserted.
Communication failure	slot-1/1 slot-1/2	Major	The chassis fails to communicate with the slot module. Chassis version release-x (x >= 7) is able to detect any slot module versions. Older versions than R7.x, e.g R6, will cause Communication Error
Software version mismatch	slot-1/1 slot-1/2	Major	Different SW version in the slot compared to the chassis. This alarm will only be active if the major or minor release version differs. The slot module should be upgraded or downgraded to match the SW version of the chassis. See CLI User manual for how to upgrade/downgrade a slot module. Chassis version release-x (x >= 7) is able to detect

			any slot module versions. Slot modules with R7.x or newer will cause SW version missmatch if they differ from the SW in the chassis.
Unsupported module	slot-1/1 slot-1/2	Minor	A card type or HW revision that is not supported in the release of the chassis
Power supply unsupported	psu-1/1 psu-1/2	Major	A power supply that is not supported in the release of the chassis
Low disk space		 Critical Major Minor	Check current disk space with command “show system diskUsage” <5MB available <7.5MB available <10MB availale

2.10 Backup and restore

The backup and restore functionality can be used to create complete backups of all configurations for chassis and slot modules and then restore exactly same configuration. Only one backup file is allowed. The backup file will be removed at reboot.

A backup is only possible if software version is same on chassis and slot modules.

Restore is only possible if product and hardware revision is same. For HW revision the last character is allowed to be different. For SW the revision must be the same on all characters.
HW example: backup from a R1A can be restored on a R1C but not on a R2A.
SW example: backup from a R7.0.1 can be restored on a R7.0.1 but not on a R7.0.2.

2.11 Dynamic update of certified transceiver list

From R12.0.1 it is possible to update the list of certified transceivers dynamically. The system contains one file with Smartoptics certified transceivers that is installed from start, but it is also possible to add an additional file with other transceivers that should be treated as certified.

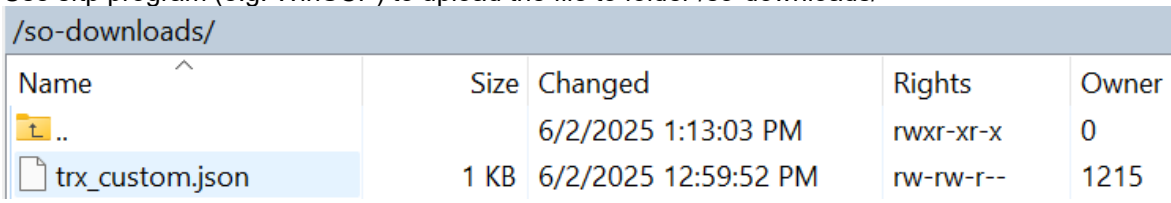
Note that this is only possible to add a file for the list of QSFP-DD and QSFP28 transceivers now. It will also be possible to update the list of certified SFP/SFP+ transceivers in a later release.

The new file must be in json format and follow a certain structure. The picture below shows an example:

```
{
    "transceiverType": "qsfp",
    "optical4LaneTransceiverList": [
        {
            "partNumber": "FTLC9558REPM",
            "description": "QSFP28, 100GBase-SR4, 850nm, MM, 100m@OM4, MPO",
            "vendor": "FINISAR CORP",
            "isAutoNeg": false,
            "isFec": true,
            "isCertified": true
        }
    ]
}
```

Here is the procedure to add a new file with certified transceivers:

1. Enable sfptuser to make it possible to upload the new file.
   config user sfptuser enable
2. Use sftp program (e.g. WinSCP) to upload the file to folder /so-downloads/



3. Fetch the file from file system and reboot

```
admin@hostname>config certified trx qsfp fetch /tmp/so-downloads/trx_custom.json

This command will copy the transceiver custom file to the system and will
overwrite the existing one.
Are you sure you want to continue? (Yes/NO): y

File fetched and pushed to slots. (New slots will automatically get the new file,
but will require a warm reboot after slot insertion)

Please warm reboot the system to take effect.

admin@hostname>reboot

Rebooting slot 1.....done
Rebooting slot 2.....done
Rebooting chassis....done

Reboot in progress. It may take a few minutes for the system to be fully
available again.

Broadcast message from root@hostname (Mon Jun  2 11:03:05 2025):

The system is going down for reboot NOW!
```

4. Check inventory to see that the transceivers has correct descriptions
   show inventory

The new file can be removed from the system with following procedure:

1. Clear the file.

```
admin@hostname>config certified trx qsfp clear

This will remove the transceiver custom file from the system.
Are you sure you want to continue? (Yes/NO): y

Transceiver custom file cleared.

Please warm reboot the system to take effect.
```

2. Reboot

```
admin@hostname>reboot

Rebooting slot 1.....done
Rebooting slot 2.....done
Rebooting chassis....done

Reboot in progress. It may take a few minutes for the system to be fully
available again.

Broadcast message from root@hostname (Mon Jun  2 11:12:04 2025):

The system is going down for reboot NOW!
```

3 Installation and Safety

3.1 Safety Precaution

Fasten the chassis securely to a 19”-rack.

Connect the PSU 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-2.

Never connect electrical cables to a DCP-2 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-2 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-2 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-2 via an external cable to ground. See Section 3.2.8 for further details.

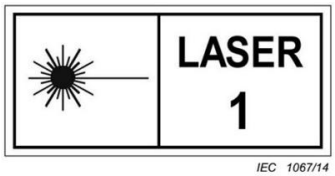
The grounding must also be made through the AC power cable, which should be inserted in a power outlet with a protective ground contact. Therefore, the power cable plug must always be inserted in a socket outlet provided with a protective ground contact, and the protective action must not be negated by use of an extension cord (power cable) without a protective conductor (grounding).

3.1.3 Laser Safety Classification

The DCP-2 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-2 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-2 or performing any internal settings on the DCP-2, 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-2 site requirements.

PHYSICAL REQUIREMENTS

The DCP-2 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-2 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-2 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-2 is 0° to +45°C/+32° to +113°F, at a relative humidity of 5% to 85% RH non-condensing.

The DCP-2 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-2 contains a fan speed control for lower noise, improved MTBF, and power savings.

ELECTROMAGNETIC COMPATIBILITY CONSIDERATIONS

The DCP-2 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-2 must be connected to a low resistance grounding system.

The RJ45 Ethernet interfaces ETH0 – ETH4 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-ETH4 management ports) 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-ETH4 management ports) 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-2 must be installed in a CBN (common bonding network) per NEBS GR-1089.

The DCP-2 is designed to be used in Network Telecommunication Facilities.

Common DC return (DC-C) Is applicable for the DCP-2.

3.2 Rack mounting

The following instructions provides instructions on how to mount the system in racks that are 600 mm to 1200 mm deep.

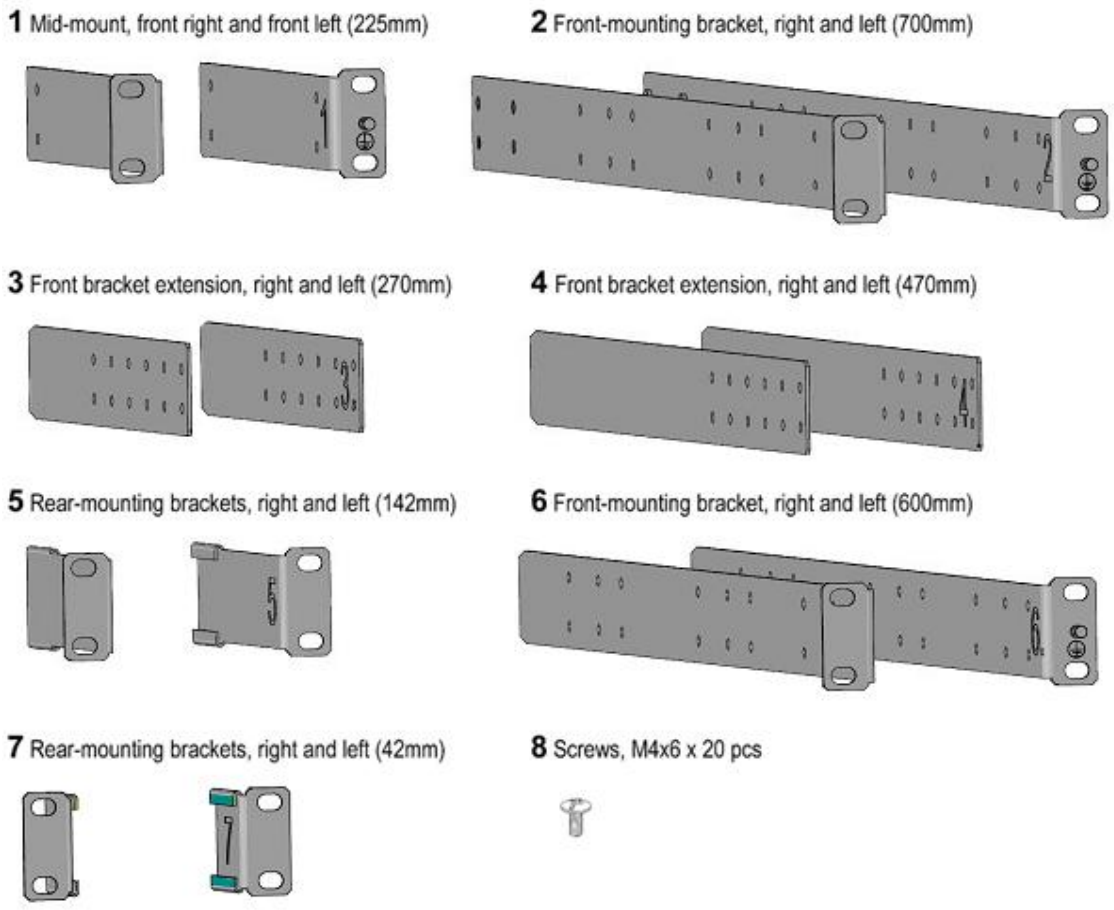
The system can be mounted in a rack in the following ways:

1. With the chassi flush with the front of the rack posts. (Four-Post Rack).
2. With the transponder flush with the front of the rack posts. (Four-Post Rack).
3. 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).
4. 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.

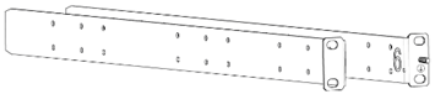
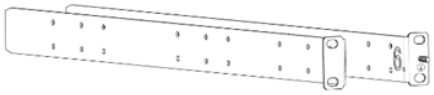
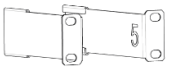
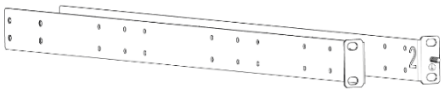
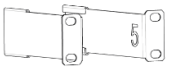
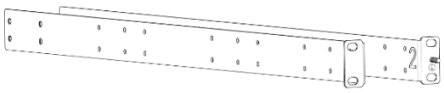
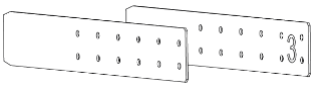
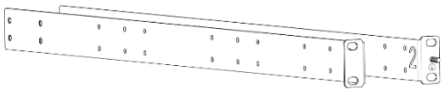
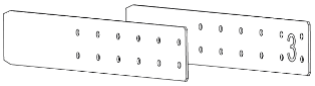
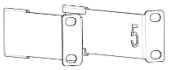
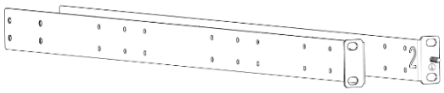
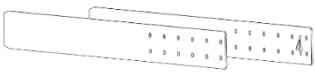
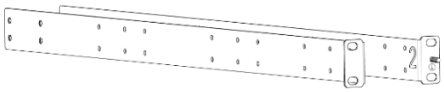
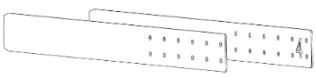
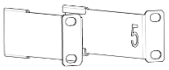
1. Mid-mount, front right and front left (225mm)
2. Front-mounting Bracket, right and left (700mm)
3. Front bracket extension, right and left (270mm)
4. Front bracket extension, right and left (470mm)
5. Rear-mounting brackets, right and left (142mm)
6. Front-mounting Bracket, right and left (600mm)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



3.2.2 Determining bracket configuration

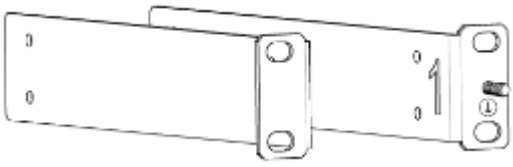
3.2.2.1 4-Post Rack

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-kit Parts		
Rack Depth	**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, Transponder Flush and 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 twelve 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.).

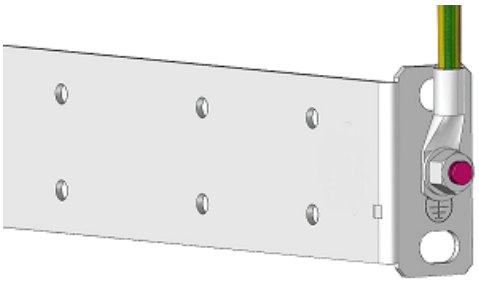
3.2.8 Protective Ground Terminal

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-2 package includes the following items:

- 2x (1,8m/6 ft.) Power cord (model depends on country/region)
- 2 x Ethernet patch cords
- RJ45 to DB9 adapter
- Rack-mount kit (Refer to 3.2.1 for contents)
- DCP-2 chassis, incl. PSU, fan units and blind plate
- Quick Installation Guide

4.2 Initial start up

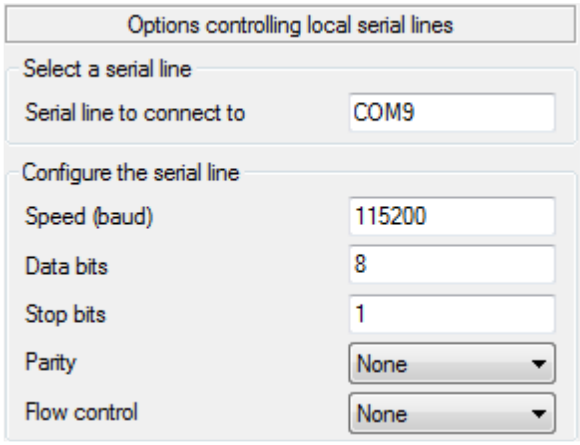
Connect power to the power supplies that are preinstalled in the chassis. The chassis will automatically power up as soon as the first PSU is connected. The power LED turns green.

The fan package starts up after a few seconds.

4.3 Connection to Serial Port

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

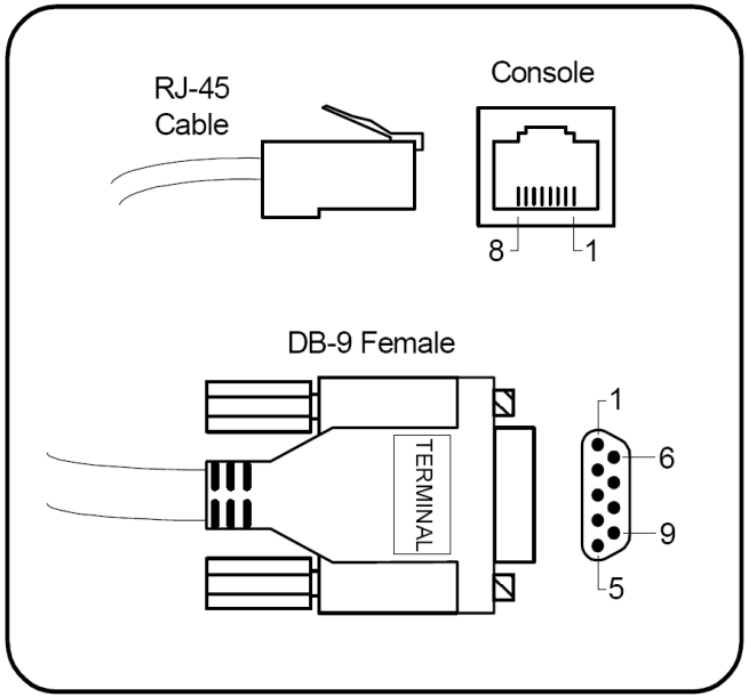
Parameter	Setting
Protocol	Serial
Baud rate	115200
Data bits	8
Parity	None
Stop bits	1
Flow control	None



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.



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 IP setup

After starting the CLI session as described above, a prompt should appear on the screen, showing the factory default name for the node and asking for login information.

```
login as:
```

The factory default login is “admin” with password “admin”.

The default IP address of ETH1-4 is 192.168.1.1.

Use ***‘config network mgmt ipv4address <IP address> <Netmask> [Gateway]’*** query to set the IP address of the node.

For example:

```
admin@smartoptics-dcp>config network mgmt ipv4address 10.10.134.181 255.255.255.0
10.10.134.1

Re-configuring interface network parameters may result in lost connections.
Are you sure you want to continue? (Yes/NO): y

IP address for interface mgmt set to 10.10.134.181, subnet mask 255.255.255.0, default
gateway 10.10.134.1.

admin@smartoptics-dcp>
```

Once the IP, netmask and gateway addresses are suitably set, it should be possible to start an SSH session by connecting one of the ETH1-4 port on the DCP-2 to a switch with a CAT5/6 cable.

Note: ETH0 uses the fixed IP address 192.168.0.1.

```
admin@smartoptics-dcp>show network interfaces

mgmt: eth1, eth2, eth3, eth4
IP Address:      10.10.134.181
Netmask:         255.255.255.0
Default gateway: 10.10.134.1
MAC address:     94:DE:0E:02:05:93

eth0 / local:
IP Address:      192.168.0.1
Netmask:         255.255.255.0
MAC address:     94:DE:0E:02:05:92

DNS primary:     10.10.134.254
DNS secondary:

admin@smartoptics-dcp>
```

4.5 Use CLI interface

After a successful login, some system information is displayed on the screen.

Press the "***?***" key to see an overview of the available commands.

```
bye         - Logout from shell.
clear       - Clear parameter.
config      - Configure system information.
exit        - Logout from shell.
logout      - Logout from shell.
ping        - Send echo messages.
quit        - Logout from shell.
reboot      - Reboot of the system.
show        - Show system information.
swupgrade   - Software image management.
techlog     - upload log for technicians.
traceroute  - Trace route to destination.
```

It is always possible to use "***?***" in order to display more information.

Use the ***tab*** key for command completion.

4.6 User accounts

The DCP-2 is shipped with 1 default user account, admin/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.
- Cryptouser
  This account can handle encryption and do everything that the admin account can do as well. The admin account gets limited functionality when cryptouser is enabled. Traffic affecting actions are not allowed by the admin user when crypto user is enabled.

In addition to the 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.

In crypto mode there will also be a user account called “crypto” and a support root account The support account can be enabled or disabled by the crypto user. By default this account is only enabled on the console port. This account can also be fully disabled or fully enabled by the user.

5 Software upgrade/downgrade

The SW can be upgraded or downgraded with swupgrade commands in CLI. See CLI User Manual for details about SW upgrade/downgrade.

6 SNMP

6.1 General

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

The DCP-2 supports 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-2 is ‘public’.

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

The SNMP Interface supports:

1. SNMPv1 for Traps.
2. SNMPv2c for Traps and for Get operations.
3. SNMPv3 for Get operations.

SNMP Set is not supported.

6.2 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 a number of 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.

```
admin@slotB>config snmp v3 enable

SNMPv3 enabled.
```

6.3 SNMP MIBS

Smartoptics provides a range of MIBs that can be used to monitor the DCP-2 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‘.

6.4 SNMP Traps

Traps or notifications are messages that alert of events occurring in the DCP-2.

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

7 User Access and Authentication

The DCP-2 supports local authentication and Terminal Access Controller Access Control System Plus (TACACS+) to control access to the units.

7.1 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.

7.2 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.

7.2.1 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).

7.2.2 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
```

7.2.2.1 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'.
```

7.2.2.2 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'.
```

7.2.2.3 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>
```

7.2.3 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>
```

7.2.4 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.

7.2.5 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

7.3 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.

7.3.1 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).

7.3.2 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>
```

7.3.2.1 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'.
```

7.3.2.2 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'.
```

7.3.2.3 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.
```

7.3.3 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>
```

7.3.4 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.

7.3.5 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.

7.3.6 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'
        }
}
```

8 Audit Trail

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

8.1 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.

8.1.1 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>
```

8.2 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.

8.2.1 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>
```

8.3 Accounting

The Configuration log enables tracking of all config, clear, reboot and swupgrade commands activity 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.

8.3.1 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>
```

9 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.

9.1.1 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.

9.1.2 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>
```

9.1.2.1 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>
```

9.1.2.2 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>
```

9.1.2.3 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>
```

9.1.2.4 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>
```

9.1.2.5 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>
```

9.1.2.6 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>
```

9.1.2.7 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.
```

9.1.3 show syslog status

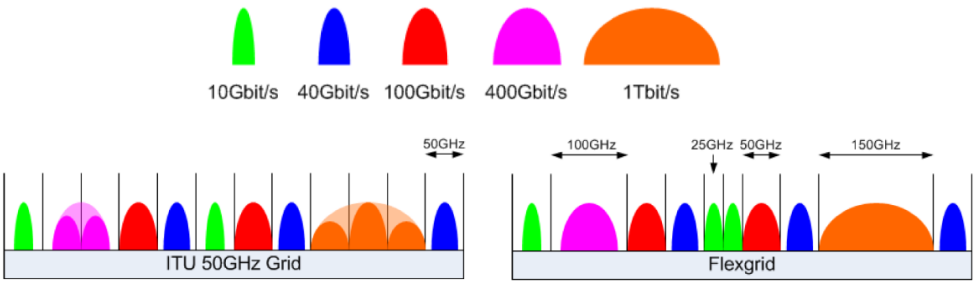
To display the status of the configured syslog, use the following command:

```
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
```

10 DCP-101 Flexible DWDM frequency

A Flexgrid network provides finer wavelength granularity and breaks the spectrum up into smaller frequency slots. The motivations for the flexible grid is to allow a mixed bit rate or mixed modulation format transmission system to allocate frequency slots with different widths so that they can be optimized for the bandwidth requirements of the particular bit rate and modulation scheme.



From SW version R5.2.1, the DCP-101 traffic unit together with SO-CFP-LPC-DWDM supports configuring a nominal central frequency granularity of 6.25 GHz to optimize bandwidth and optical spectrum.

10.1.1 Configuring a DCP-101 transponder with ITU 50 GHz grid

This command is used to configure the wanted channelid where the central frequency are on the 50 GHz grid.

```
admin@DCP-19> config slot 1 interface 1 channelId <channel id>
```

Parameter	Description
<channel id>	It´s possible to configure this value in the range from 9125 to 9610. 9125 means the frequency is 191.25 THz.

10.1.2 Configuring a DCP-101 transponder with 6.25 GHz frequency

This command is used to configure the wanted nominal central frequency with a granularity of 6.25 GHz.

```
admin@DCP-19> config slot 1 interface 1 frequency <frequency>
```

Parameter	Description
<frequency>	Transceiver frequency in THz. It´s possible to configure this value in the range from 191.25000 to 196.10000 with 625 spacing. Eg 191.25000, 191.25625, 191.26250, 191.26875, , 191.27500, 191.28125, 191.28750, 191.29375 etc etc

11 Encryption

Smartoptics supports layer 1 encryption on various traffic units. The traffic units that support encryption have crypto chips that are installed in production. It is also required to have an SW encryption license. For units with QSFP-DD it is also necessary to use transceivers that support encryption.

The encryption solution is based on layer 1 AES-256 GCM encryption with Diffie-Hellman key exchange.

Crypto chip functions:

- Digital signature generation and verification
- Secure storage of certificates, public keys, private and secret keys
- Cryptographic algorithms supported by the crypto chip include ECC, ECDSA signature scheme, SHA and MAC digest algorithms.
- Secure Hash: SHA-256
- MAC Digest: HMAC-SHA256
- Signature Schemes: Elliptic Curve Digital Signature Algorithm (ECDSA) (FIPS 186-4)
- Random Number Generation: True RNG

AES 256 GCM encryption details:

- Data encryption, key generation, certificate generation, key verification and storage of keys is all implemented in the hardware crypto chips
- A new pair of Tx and Rx AES keys are generated every 10 minutes for every active encrypted channel.
- The process of generating a new pair of AES keys for each channel starts by authenticating the boards, and the keys are always randomly generated uniquely for each channel.
- Secret session keys for data encryption are never stored, only temporarily residing in a secure environment
- All private and public keys generated randomly and saved securely inside the crypto chips and the software doesn't have access to the private keys nor to the shared secret generated after a successful Diffie Hellman key exchange
- Support for custom authentication ID for each port

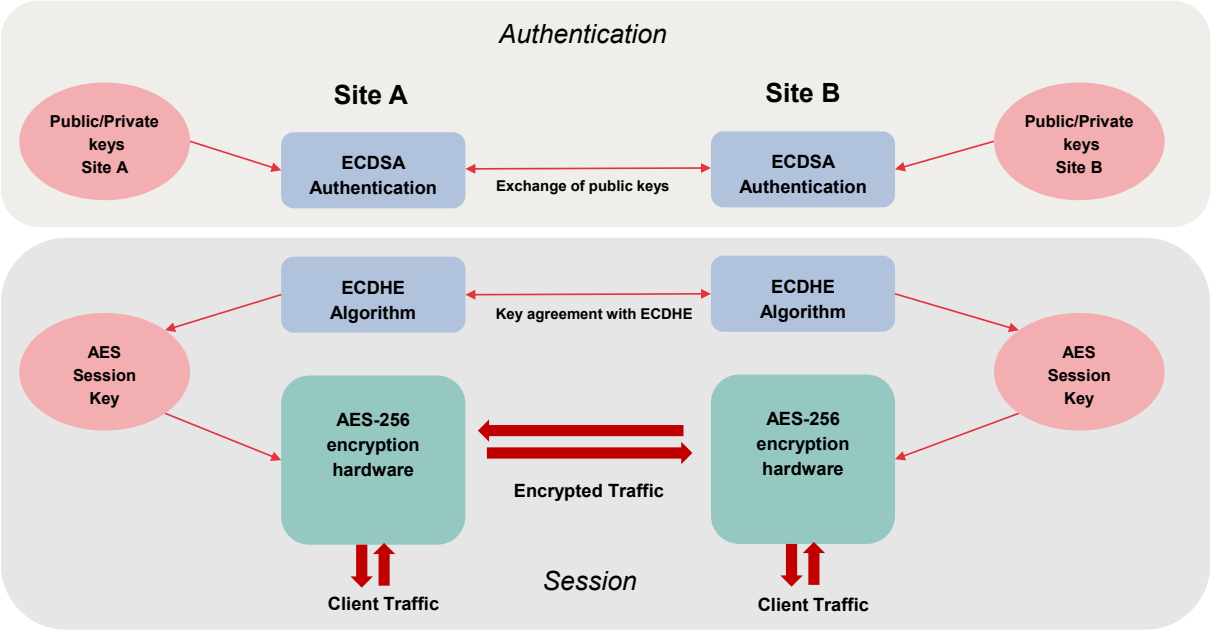
Authentication and key exchange details:

Endpoint Authentication: Elliptic Curve Digital Signature Algorithm (ECDSA)
Pre-defined private/public Elliptic Curve Cryptography (ECC) keys in DCP-1610, DCP-404, DCP-1203 and DCP-110 HW
Optional use of custom certificates for each port

Session Key Agreement: ECC Diffie-Hellman Ephemeral (ECDHE)
Ephemeral (temporary) keys, only used once per session
Perfect forward secrecy

Authenticated Encryption: AES-256 GCM

Advanced Encryption Standard (AES) and Galois Counter Mode (GCM) for encryption and authentication on byte level



Encryption can be enabled on a traffic unit in 5 steps:

1. Create a crypto user account
2. Configure service mode or app code
3. Enable encryption
4. Configure the pre-shared key

For DCP-1610 it is also possible to configure fiber intrusion alarm.

11.1 Create Crypto User Account

When encryption is enabled, the security of the system is hardened. The traditional administrator account will have less privileges which is described below.

A new user named ’crypto’ will be enabled. This new crypto user will have explicit ownership of both traffic and encryption configuration for transponders that are configured with an encryption traffic format. Some system administration features will also be explicitly owned by the crypto user.

The crypto user will have explicit privileges to the following features;

- Configuration of encryption enabled transponders incl. crypto key management
- Software Management (Upgrade/Downgrade/Fallback)
- To reset the unit to factory default
- Reboot of the system or plug-in units

In addition to the ‘crypto’ user account there is also a support root account. The support account can be enabled or disabled by the crypto user. The default setting is that the support root account is disabled.

Before encryption can be used, the system-wide cryptoMode has to be enabled.

```
admin@smartoptics-dcp>config crypto cryptoMode enable
Enabling cryptoMode creates crypto user and shuts down all CLI sessions.
Are you sure you want to continue? (Yes/NO): Yes

Encryption mode enabled. Log in as crypto user to configure encrypted ports.
```

When the command is executed, you will be asked if you would like to continue with enabling the cryptoMode, answer Yes. All connected CLI sessions will be disconnected from the system.

Re-establish a connection to the system and login as ’crypto’ with the password ’crypto’. You will now be asked to set a new password for the crypto user.

It is recommended that this should be a secure password as the crypto user has privileges over encryption configuration.

```
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for crypto
Old password:
New password:
Retype password:
Password for crypto changed by crypto
```

11.2 Configure encryption service mode or app code

Please note that encryption will have to be enabled in both ends of the link and the pre-shared authentication key will have to also match in both ends.

11.2.1 Configuring DCP-1610 service mode for encryption

For DCP-1610 it is required to select a service mode that supports encryption.
The following client traffic formats are supported to be used for encryption.

Client Format	Line Format	Line Datarate
10GbE	OTU2eEnc	11,095727 Gbit/s
STM64	OTU2Enc	10,709225 Gbit/s
16GFC	OTU2xEnc	14,083928 Gbit/s
8GFC	OTU2Enc	10,709225 Gbit/s
OTU2	OTU2Enc	10,709225 Gbit/s
OTU2e	OTU2eEnc	11,095727 Gbit/s
1GbE	OTU2eEnc	11,095727 Gbit/s
40GbE (4x 10GbE)	OTU2eEnc	11,095727 Gbit/s

The example below shows how to select service mode '10GbE-OTU2eEnc'.

```
crypto@smartoptics-dcp>config slot 1 transponder 1 service 10GbE-OTU2eEnc

Transponder '1' service is set to '10GbE-OTU2eEnc'.

if-1/1/1 format is set to OTU2eEnc.
if-1/1/2 format is set to 10GbE.

crypto@smartoptics-dcp>
```

Figure 11-1. Configuring slot 1 transponder 1 to a 10GbE-OTU2eEnc service.

11.2.2 Configuring DCP-404, DCP-1203 and DCP-110 application code for

encryption

For traffic units with QSFP-DD it is required to have coherent QSFP-DDs with application codes that support encryption. QSFP-DDs based on OpenROADM standard support encryption. Following coherent QSFP-DDs can be used for encryption:

- TQD017-TUNC-SO (100G-400G)
- TQD011-TUNC-SO (100G).

Following application codes on QSFP-DD TQD011-TUNC-SO support encryption:

App	Payload Rate	Host Format	Media Format	FEC	Modulation	Media Code	Host Code
4	100G	CAUI-4 C2M (Annex 83E) without FEC	FOIC1-OFEC-QPSK	oFEC	DP-QPSK	CA	41
5	100G	CAUI-4 C2M (Annex 83E) with RS(528,514) FEC	FOIC1-OFEC-QPSK	oFEC	DP-QPSK	CA	42
6	100G	100GAUI-2 C2M (Annex 135G)	FOIC1-OFEC-QPSK	oFEC	DP-QPSK	CA	D
7	100G	OTL4.4 (ITU-T G.709/Y.1331 G.Sup58)See CEI-28G-VSR	FOIC1-OFEC-QPSK	oFEC	DP-QPSK	CA	39

Figure 11-2. Application codes with encryption on TQD011-TUNC-SO.

Following application codes on QSFP-DD TQD017-TUNC-SO support encryption:

App	Payload Rate	Host Format	Media Format	FEC	Modulation	Media Code	Host Code
1	400G	100GAUI-2 C2M (Annex 135G)	FOIC4-oFEC-16QAM	oFEC	DP-16QAM	C7	D
2	300G	100GAUI-2 C2M (Annex 135G)	FOIC3-oFEC-8QAM	oFEC	DP-8QAM	C8	D
3	200G	100GAUI-2 C2M (Annex 135G)	FOIC2-OFEC-QPSK	oFEC	DP-QPSK	C9	D
4	200G	100GAUI-2 C2M (Annex 135G)	FOIC2-OFEC-16QAM	oFEC	DP-16QAM	F2	D
5	100G	100GAUI-2 C2M (Annex 135G)	FOIC1-OFEC-QPSK	oFEC	DP-QPSK	CA	D
6	400G	400GAUI-8 C2M (Annex 120E)	FOIC4-oFEC-16QAM	oFEC	DP-16QAM	C7	11
7	200G	200GAUI-4 C2M (Annex 120E)	FOIC2-OFEC-QPSK	oFEC	DP-QPSK	C9	F
8	200G	200GAUI-4 C2M (Annex 120E)	FOIC2-OFEC-16QAM	oFEC	DP-16QAM	F2	F
9	100G	CAUI-4 C2M (Annex 83E) without FEC	FOIC1-OFEC-QPSK	oFEC	DP-QPSK	CA	41
10	100G	CAUI-4 C2M (Annex 83E) with RS(528,514) FEC	FOIC1-OFEC-QPSK	oFEC	DP-QPSK	CA	42

Figure 11-3. Application codes with encryption on TQD017-TUNC-SO.

The example below shows how to configure application code 1 on a DCP-404.

```
crypto@DCP-2-195>config slot 2 interface 11 transceiver app 4

  App  Payload Rate  Host Format                          Media Format     FEC     Modula
tion  Media Code  Host Code
  ---  ------------  -----------------------------------  ---------------  ------  ------
----  ----------  ---------
  1    100G          CAUI-4 C2M (Annex 83E) without FEC  ZR100-OFEC-QPSK  oFEC    DP-
QPSK     49          41
  4*   100G          CAUI-4 C2M (Annex 83E) without FEC  FOIC1-OFEC-QPSK  oFEC    DP-
QPSK     CA          41
  8    100G          CAUI-4 C2M (Annex 83E) without FEC  OTU4-SCFEC-QPSK  SC-FEC  DP-
DQPSK    CD          41

* = Currently active application code.
This command can be service interrupting.
Are you sure you want to continue? (Yes/NO): y

App '4' is selected
```

Figure 11-4. Configuring app code 1 for DCP-404 in slot 1.

11.3 Enabling encryption on the traffic unit

Enable the encryption on the transponder. This will set the transponder to require a successful key exchange to enable client traffic.

```
crypto@smartoptics-dcp>config slot 1 transponder 1 crypto enable

Encryption enabled for slot 1 transponder 1.

crypto@smartoptics-dcp>
```

Figure 11-5. Enabling encryption on slot 1 transponder 1.

For muxponders it is the same command, but the word *transponder* is exchanged to *muxponder*.

11.4 Configure the pre-shared authentication key (channel authentication id)

It is required to configure a pre-shared authentication key (channel authentication ID) on the line ports that should be encrypted.

You can enter a 64 hexadecimal character string directly or have the system generate one for you by entering ’random’ in place of the ’<channel authentication ID>’.

If you select to generate a random key, you must manually enter it using this command. The random generated key is just displayed and is not automatically applied to the interface.

```
crypto@smartoptics-dcp>config slot 1 interface 1 channelAuthenticationId <channel
authentication id>

crypto@BRU-R1-DCP2-33>config slot 1 interface 2 channelAuthenticationId random

Random generated number for channel authentication ID:
'0f51e2b92d7645780ce45a3e361a702b5de1031badbfa4df41bff73b2b756a23'

Please copy the key above and configure the channel authentication ID with it.

crypto@smartoptics-dcp>
```

Figure 11-6. Configuring the channel authentication ID on slot 1 interface 1 (the line interface of transponder 1).

```
crypto@smartoptics-dcp> config slot 1 interface 1 channelAuthenticationId
0f51e2b92d7645780ce45a3e361a702b5de1031badbfa4df41bff73b2b756a23

Channel authentication ID set on slot 1 interface 1.

crypto@smartoptics-dcp>
```

Figure 11-7. Example showing configuration of a channel authentication ID, the same key must also be configured on the remote end transponder interface.

11.5 Fiber Intrusion Alarm

As a means to help indicate if a fiber may have been tampered with such as trying to tap the fiber for surveillance, the fiber intrusion alarm feature can be enabled. If enabled, this alarm will trigger if the power level into the transponder decreases below 2.0 dBm from the saved threshold.

Note that fiber intrusion is only implemented on DCP-1610 in R10.

Once this alarm is triggered it will not clear unless the alarm is disabled, or a new threshold reference is saved. This is a security feature, to ensure that a potential fiber tap event is visible.

11.5.1 Enabling fiber intrusion alarm

```
crypto@smartoptics-dcp>config slot 1 interface 1 fiberIntrusionAlarm enable

Fiber Instrusion Alarm Rx Power reference threshold value set on slot 1 interface 1.

crypto@smartoptics-dcp>
```

Figure 11-8. Enabling of fiber intrusion alarm.

11.5.2 Disabling fiber intrusion alarm

```
crypto@smartoptics-dcp> config slot 1 interface 1 fiberIntrusionAlarm disable

Fiber Intrusion Alarm disabled on slot 1 interface 1.

crypto@smartoptics-dcp>
```

Figure 11-9. Disabling of fiber intrusion alarm.

11.5.3 Setting fiber intrusion alarm threshold

```
crypto@BRU-R1-DCP2-33>config slot 1 interface 2 fiberIntrusionAlarm limit 3

Fiber intrusion alarm limit is set to 3.0 dBm
```

Figure 11-10. Disabling of fiber intrusion alarm.

11.5.4 Verify status and threshold of fiber intrusion alarm

To verify the status or check the threshold of the fiber intrusion alarm, use the ’show interface detail <interface>’ command.

In this view, you can find the alarm state (enabled/disabled), saved threshold (in dBm) and alarm status (ok/alarm).

```
crypto@smartoptics-dcp> show interface detail if-1/1/1

[This output has been modified to only show relevant information for documentation purposes]

  Interface        : if-1/1/1
  Transponder      : trp-1/1/1

Status:

  Fiber intrusion alarm           : enabled
  Fiber intrusion alarm threshold : -8.60 [dBm]

  Optical Rx power : -6.6 [dBm]
  Optical Tx power : 1.2 [dBm]

Alarms:

  Fiber intrusion            : ok

crypto@smartoptics-dcp>
```

Figure 11-11. Show interface detail contains related information to the Fiber intrusion alarm configuration.

11.6 Alarms related to encryption

11.6.1 Channel authentication key mismatch

Alarm Severity: Critical

This alarm indicates that the encryption channel authentication id key mismatch with the key from the remote end.

11.6.2 AES/GMAC tag mismatch

Alarm Severity: Critical

This alarm indicates that modification of the encrypted payload have occurred. This alarm could also be triggered as a result of link errors.

11.6.3 Fiber intrusion

Alarm Severity: Major

This alarm relates to the 11.5 Fiber Intrusion Alarm feature.

If this alarm has been triggered, it means that the *Optical Rx power* of the interface has gone below the saved *Fiber intrusion alarm threshold.*

12 Loopback

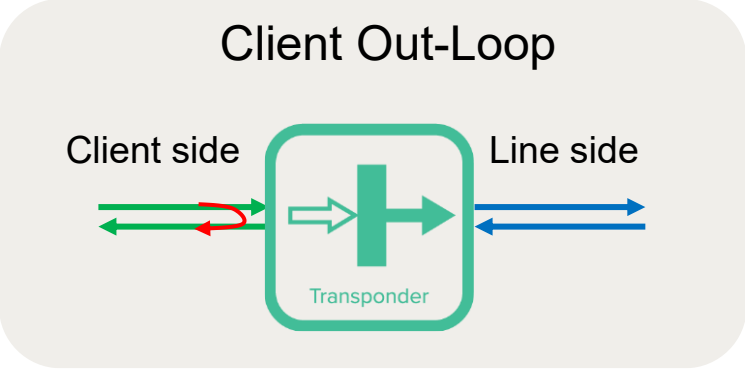
Four different loopback settings are defined, but all options are not available on all traffic cards. The table below shows which loopback options that are available for specific traffic units. A warning will be raised during the time that a port is configured in loop back mode.

Traffic unit	Client Out-loop	Client In-loop	Line Out-loop	Line In-loop
DCP-108	Yes	No	Yes	No
DCP-1610	Yes	No	Yes	No
DCP-101	Yes	No	Yes	No
DCP-404	Yes	Yes	No	No

12.1.1 Client Out-loop

Signal from client side will be looped on the client port back to client side.

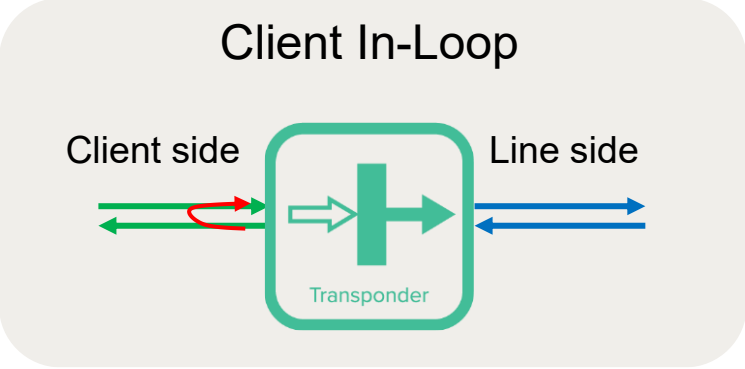
The client out-loop can be used to loop the signal back to the client equipment or to a test instrument connected on the client port.



12.1.2 Client In-loop

Signal from line side will be looped on the client port back to the line side.

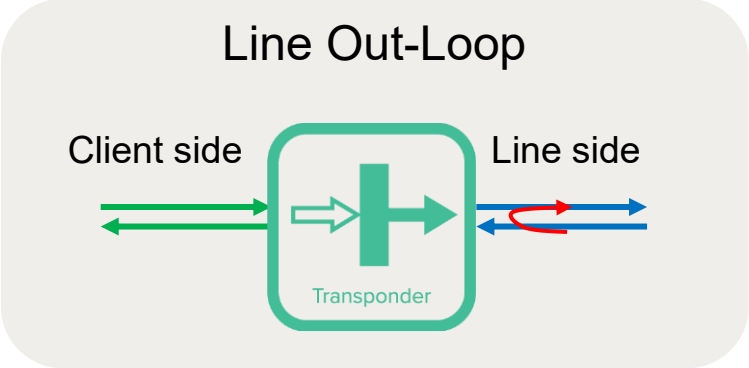
The client in-loop can be used to loop the signal back to the line side without using a patch cord on the client side. In this case the signal will be processed through the electronics in the traffic unit before it is looped back to the line side.



12.1.3 Line Out-loop

Signal from line side will be looped on the line port back to line side.

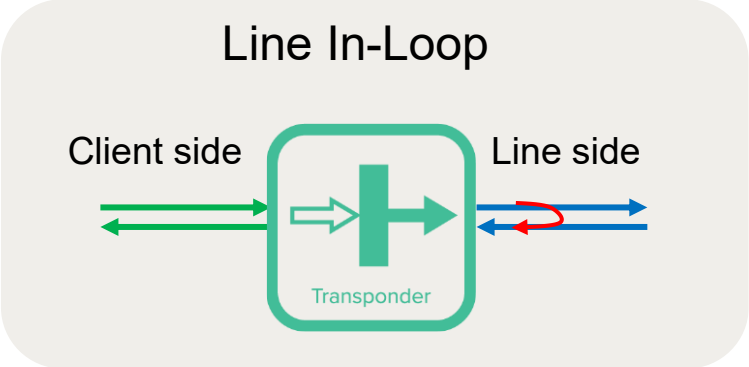
The line out-loop can be used to loop the signal back to the line side without processing data inside the card.



12.1.4 Line In-loop

Signal from client side will be looped on the line port back to client side.

The line in-loop can be used to loop the signal back to the client equipment or to a test instrument connected on the client port. In this case the signal is processed through the electronics in the card.



13 Waste management

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

14 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 (CHASSI ONLY)	DCP-2 chassis with fans and 2 PSU (AC) Min: 14W Max: 17W
DCP-2 + 1 X DCP-101	Min: 55 Watts Average: 56 Watts Max: 60 Watts
DCP-2 + 1 X DCP-1610	Min: 56 Watts Typical: 83 Watts Max: 103 Watts
DCP-2 + 1 X DCP-108	Min: 44 Watts Typical: 80 Watts Max: 125 Watts
DCP-2 + 1 X DCP-404	Min: 51 Watts Typical: 65 Watts Max: 80 Watts
DCP-PAS-H	No power needed
REDUNDANCY	Hot swappable fan & PSUs
COOLING FANS	Front-to-Back straight through airflow
ALTITUDE	3000 m (10.000 ft.)
DIMENSIONS (DCP-2):	
HEIGHT	1.77” (1 RU) (H), 45mm (H)
WIDTH	17.32” (W), 440mm (W)
DEPTH	19.69” (D), 500mm (D)
WEIGHT (WITHOUT TRAFFIC UNITS)	~ 7 Kg

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
NETWORK MANAGEMENT:	
MANAGEMENT INTERFACES	4 x RJ45 LAN ports 10/100/1000Base-T 1 x SFP LAN port 1000 Base-X 1 x RS-232 serial port 1 x RJ-45 local craft 10/100/1000 Base-T
SOFTWARE UPGRADE	Traffic hitless – dual image
BOOT TIMING	Booting from Coldstart < 5min Warmstart reboot < 2min
PROTOCOLS	CLI, SNMP, SYSLOG, TACACS+

Appendix A Latency & Identified Transceivers

See separate ”Technical description” manual for DCP-404, DCP-1610 and DCP-108 transceivers and latency.

DCP-101 Latency

Client Protocol	Line transceiver	Latency
100G	DCP-CFP-C-DWDM	9,3µs
100G with FEC	DCP-CFP-C-DWDM	9,4µs
100G	SR10 or ZR10	0,12µs
100G with FEC	SR10 or ZR10	0,2µs

Certified transceivers DCP-101

Line transceiver
SO-CFP-LPC-DWDM
DCP-CFP-C-DWDM
SO-CFP-C-DWDM
SO-CFP-SR10
Client transceiver
DCP-QSFP28-LR4
DCP-QSFP28-SR4
DCP-QSFP28-ER4
DCP-QSFP28-CWDM4
DCP-QSFP28-PSM4
DCP-QSFP28-LR410L
DCP-QSFP28-AOCXM
DCP-QSFP28-PCUXM-1M, -2M, -3M
DCP-QSFP28-ACUXM-1M, -2M, -3M, -5M

Appendix B List of protocols and ports numbers used by DCP-2

The below table contains information on which services and network protocols are used in the DCP-2 and their intended purpose. This information is useful if the DCP-2 is installed in a secure network where firewalls might need to be configured to allow for full functionality.

Service	Port	Protocol	Description
FTP	21	TCP	Used for software upgrades.
SSH	22	TCP	Used for secure logins to the CLI.
TACACS+	49	TCP	Used for authentication, authorization and accounting (AAA) services
DNS	53	TCP & UDP	Used for mapping host names to IP-addresses.
HTTP	80	TCP	Used for software upgrades.
NTP	123	UDP	Used to synchronize the system against an NTP server.
SNMP	161	UDP	Used for SNMP management and monitoring of the system.
SNMP Trap	162	UDP	Used by SNMP to send traps to the SNMP receiver(s).
Syslog	514	TCP & UDP	Used for system logging
RADIUS	1812	UDP	Used for authentication, authorization and accounting (AAA) services