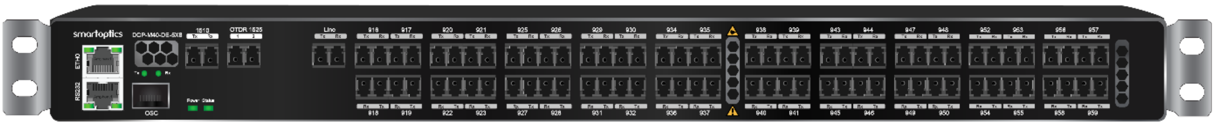
DCP-M-DE

User Manual

dcp-release-12.1.3



DCP-M40-DE-5X8

DCP-M40-DE-1X40

The specifications and information within this manual are subject to change without further notice. All statements, information and recommendations are believed to be accurate but are presented without warranty of any kind. Users must take full responsibility for their application of any products.

Contents

1 Introduction

1.1 General

The DCP-Series is an optical transmission platform. The DCP-M-DE is a disaggregated 19” 1U chassis system for terminal nodes in FOADM networks. All optical components needed for one direction in terminal node are integrated in the chassis. DCP-M-DE has front-to-back airflow. The back side of the chassis has hot-pluggable redundant power supplies and a fan unit including 4 individual fans. DCP-M-DE is available in two versions in this release:

- DCP-M40-DE-5X8 This system is used for networks with a channel plan with guard channels between each group of 8ch. First channel is 916 and last channel is 959.
- DCP-M40-DE-1X40 This system is used for networks with a channel plan with 40 consecutive channels from 921 to 960.

1.2 DCP-M-DE

The key features for the DCP-M-DE series are:

- **Automatic power balancing**
  - Dual equalizers, one for Tx and one for Rx line side
  - Dual OCM for channel monitoring on both Tx and Rx ports on the line side
  - Automatic power balancing in both upstream and downstream
- **High level of traffic format and modulation support. Can support the following:**
  - NRZ modulated wavelength (1-10G Ethernet, 1-16G FC, CPRI 1-10, SONET, SDH, OTN etc)
  - Coherent modulated wavelengths (100G, 200G, 300G & 400G)
  - 400ZR OIF based wavelengths (400G)
- **Optimized for ring and chain applications**
  - Can be used as terminal nodes in active / passive rings
  - Can be used as terminal nodes in active / passive chains

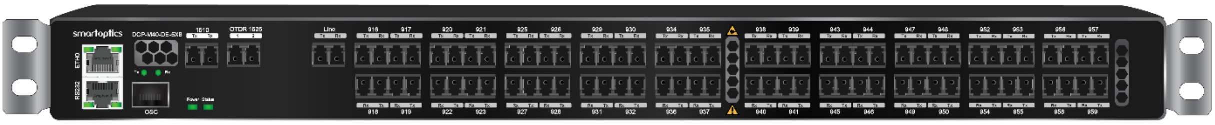


Figure 1. *Front view of DCP-M40-DE-5X8.*

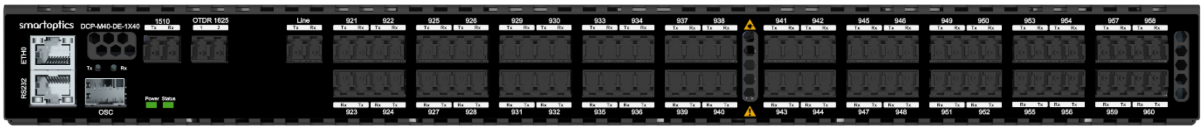


Figure 2. *Front view of DCP-M40-DE-1X40.*

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
12.1.1 A	2025-09-08	First draft of the manual for DCP-M-DE
12.1.1 B	2025-09-25	Changed the title in the file properties for the document
12.1.3 A	2025-10-28	Added list of supported OSC transceivers Added chapter for configuration of optical parameters

2 Functional description

2.1 DCP-M40-DE-5X8

The DCP-M40-DE-5X8 product contains everything needed for one direction in a terminal node in a 1RU chassis. This unit is optimized for transport of NRZ services that can work with limited requirements for dispersion compensation. It can also be used for coherent services up to 400G.

This chassis has front to back air flow and can use AC or DC power. The power and FAN units are redundant and can be replaced. They are accessed from the rear side of the chassis.

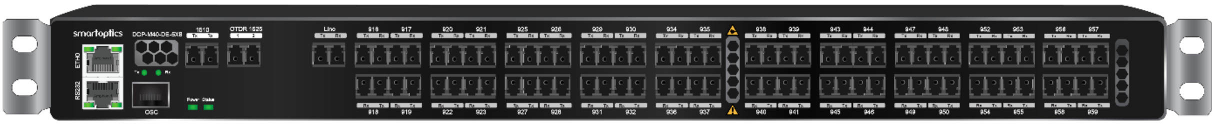


Figure 3. *Chassis front view of DCP-M40-DE-5x8*

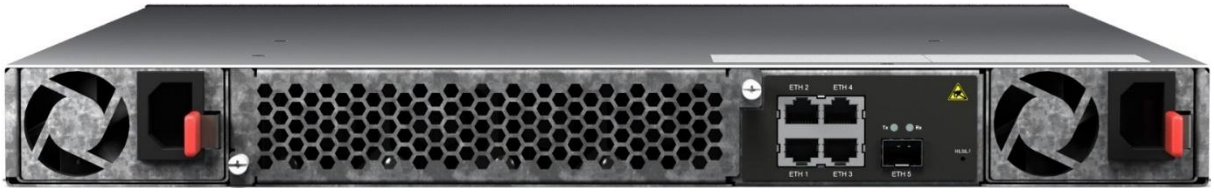


Figure 4. *Chassis rear view of DCP-M40-DE-5X8*

The DCP-M40-DE-5X8 contains a dual equalizer, dual OCM, booster and pre-amplifier, a 40ch mux/demux with 80GHz BW, dual 20km DCMs, a VOA for the line side. OSC filters at 1510nm and OTDR filters for 1625nm. The OSC channel uses a pluggable SFP to support different distances. The 40ch mux/demux is an AWG with 5 bands of 8 x DWDM wavelengths from 916 to 959. One guard channel between each band.

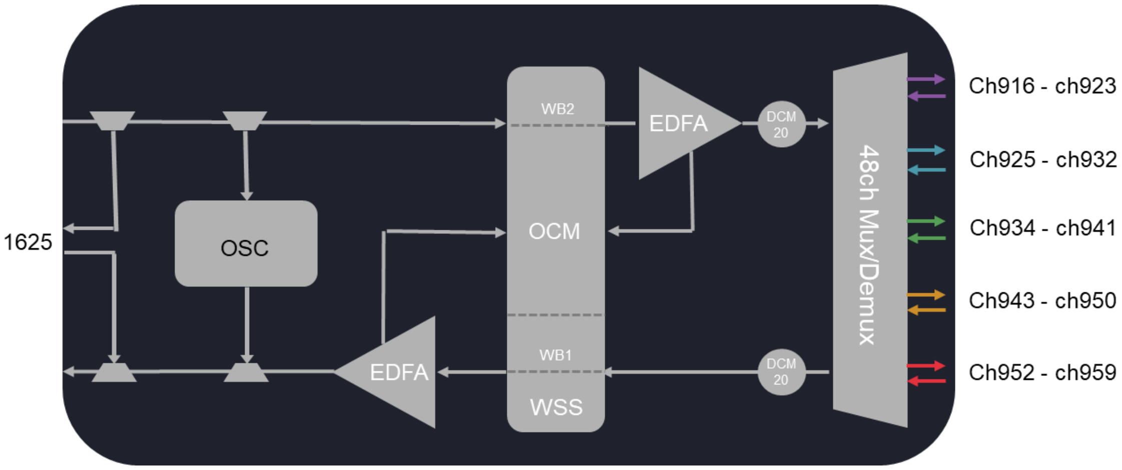


Figure 5. *Functional diagram of DCP-M40-DE-5X8*

2.2 DCP-M40-DE-1X40

The DCP-M40-DE-1X40 product contains everything needed for one direction in a terminal node in a 1RU chassis. This unit is optimized for transport of NRZ services that can work with limited requirements for dispersion compensation. It can also be used for coherent services up to 400G.

This chassis has front to back air flow and can use AC or DC power. The power and FAN units are redundant and can be replaced. They are accessed from the rear side of the chassis.

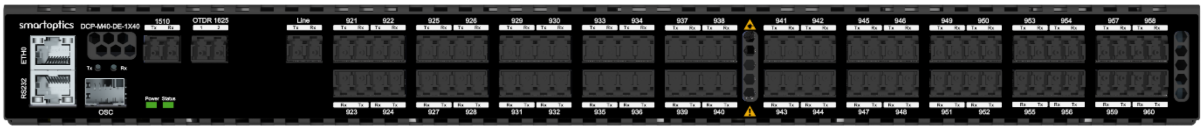


Figure 6. *Chassis front view of DCP-M40-DE-1X40*

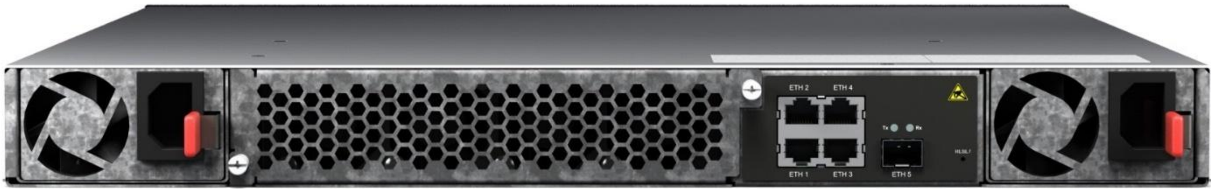


Figure 7. *Chassis rear view of DCP-M40-DE-1X40*

The DCP-M40-DE-1X40 contains a dual equalizer, dual OCM, booster and pre-amplifier, a 40ch mux/demux with 80GHz BW, a VOA for the line side. OSC filters at 1510nm and OTDR filters for 1625nm. The OSC channel uses a pluggable SFP to support different distances. The 40ch mux/demux is an AWG with 40 DWDM channels from 921 to 960.

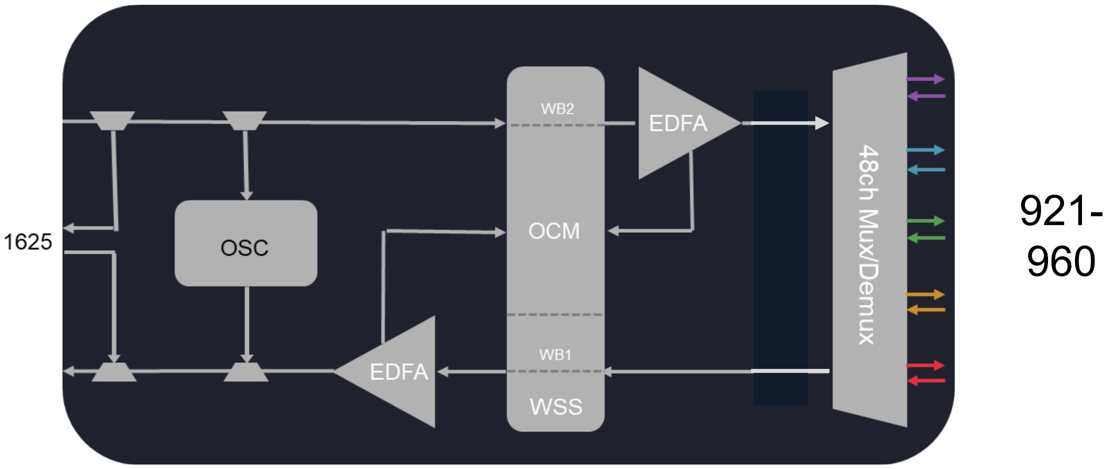


Figure 8. *Functional diagram of DCP-M40-DE-1X40*

2.3 Active / Passive ring application

Many backhaul networks are built with a ring or arc topology where traffic is collected in satellite nodes and transported to a hub location. This is typical for mobile backhaul with 10G or 25G wavelengths today. Coherent 100G signals may be used later.

The satellite sites typically have limited space and power possibilities so passive OADM sites are preferred. However, it could be difficult to reach long distance with passive sites. Smartoptics solution to this is to put active equipment with amplifiers in the hub nodes. Power balancing and monitoring can be done automatically by introducing equalizers and OCMs in the active site, i.e. the hub.

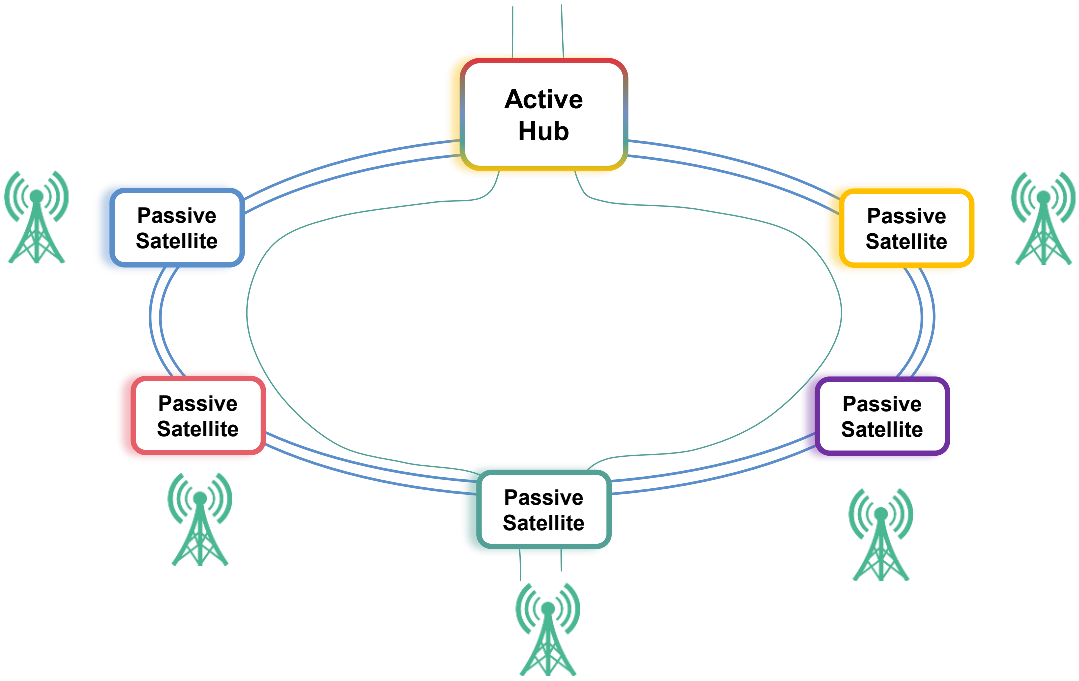


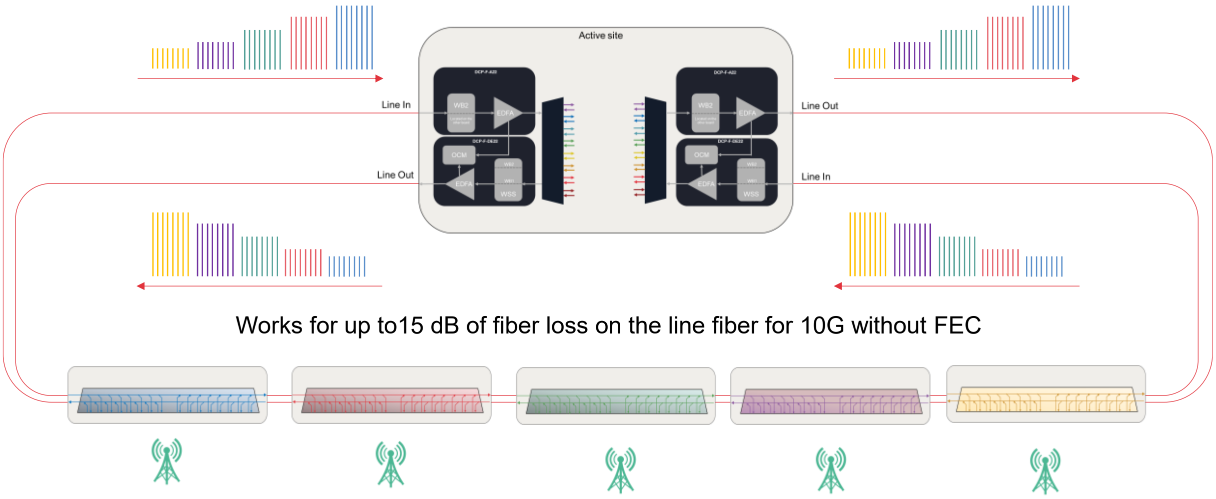
Figure 9. *Ring topology for active / passive network*

The active site can be built with components from the DCP-F series, but the DCP-M-DE products include all necessary components in a 1RU box.

The optical power levels in different OADM nodes will vary depending on fiber attenuation and number of nodes that are passed in the route. This could make it difficult to do the power balancing in the passive sites as well as in the hub site. With Smartoptics dual equalizer solution it is possible to control the optical power levels for both the outgoing and incoming signals in the hub.

The incoming signals in the hub will have different optical levels depending on which node they come from. This is handled by placing an equalizer before the pre-amplifier. Together with the OCM it is possible to run a control loop that will automatically balance all incoming signals before they arrive in the pre-amplifier.

The outgoing signals will be destined for different satellite nodes. The loss to the satellites will be different depending on distance and number of pass-through nodes. This will imply that the optical power will be different in different satellite nodes if they are all equal when they leave the hub node. In order to get similar optical power levels in all satellite nodes it is possible to set different start values in the hub node. This is also done with a an equalizer and OCM.



Works for up to15 dB of fiber loss on the line fiber for 10G without FEC

Figure 10. *Power balancing example for an active / passive ring.*

2.4 Active / Passive chain application

The DCP-M-DE products can also be used for chain applications where multiple nodes will be connected in a chain topology. In this case the hub node in the central site will be an active site while the add/drop nodes will be passive sites.

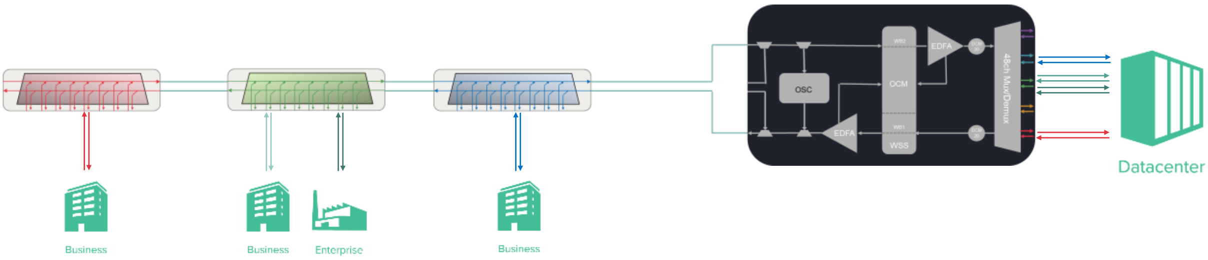


Figure 11. *Chain topology for active / passive network*

2.5 Active / Passive bus application

The DCP-M-DE products can also be used for bus applications where multiple passive nodes will be connected to active end nodes at both ends. This solution is very similar to the ring application, but in this case the ring will not be closed. Here it is also likely that there will be traffic between the two end nodes as well.

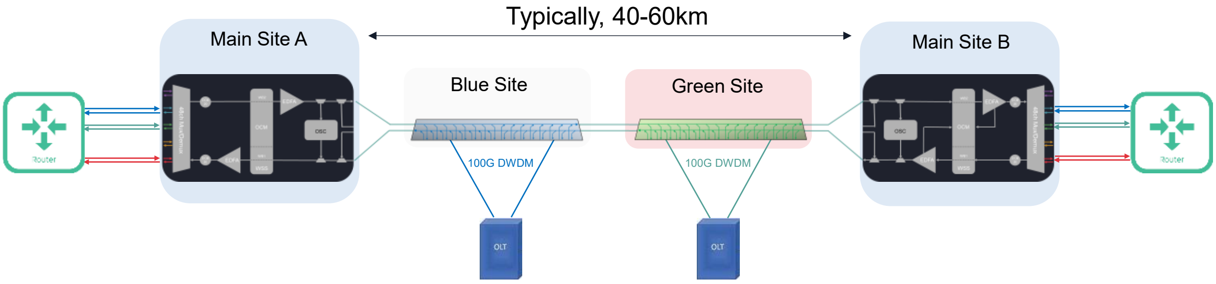


Figure 12. *Bus topology for active / passive network*

2.6 Physical Description

The DCP-M-DE 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 both in the front and rear sides of the chassis. All optical connections are done on the front panel. The DCP has a front-to-back airflow. The DCP-M-DE chassis is populated with 2 redundant power supplies and 1 fan unit (with 4 fans). DCP-M-DE is available in two versions from R11.0.1, DCP-M40-DE-5X8 and DCP-M40-DE-1X40.

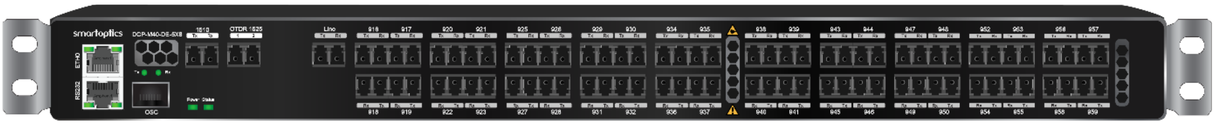


Figure 13. *Chassis front view of DCP-M40-DE-5X8*

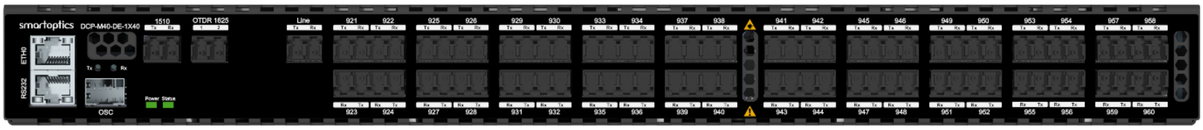


Figure 14. *Chassis front view of DCP-M40-DE-1X40*

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

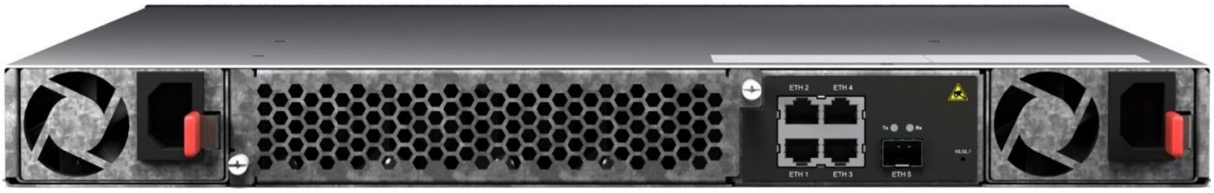


Figure 15. *Chassis rear view of DCP-M40-DE-5X8 and DCP-M-DE-1X40*

The back of the DCP-M-DE chassis houses 4xRJ45 Ethernet ports for management access. The ETH5 port can be used with an optical SFP interface. The 2 power supplies and fan-unit are hot pluggable.

2.7 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-M-DE is dual feed, and the power supplies are hot swappable. Both types can be used simultaneously.

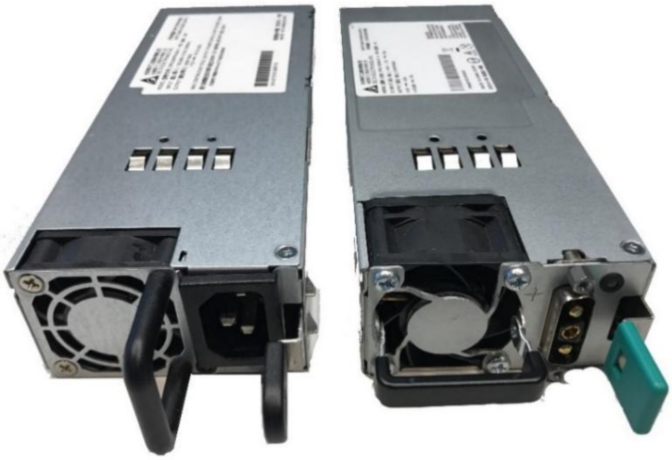


Figure 16. *The DCP-2-PSU-AC-FB and DCP-2-PSU-DC-FB unit.*

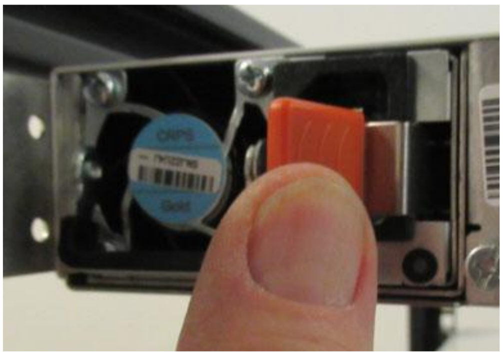
Same power supplies are also used in DCP-M and DCP-2 chassis.

2.7.1 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.

2.7.2 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



CRPS
Gold

2.8 DCP-2-FAN-FB Fan Unit

The DCP-M-DE has a fan unit which consists of 4 fans. The fan speed is controlled via the MCU and the system can 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.

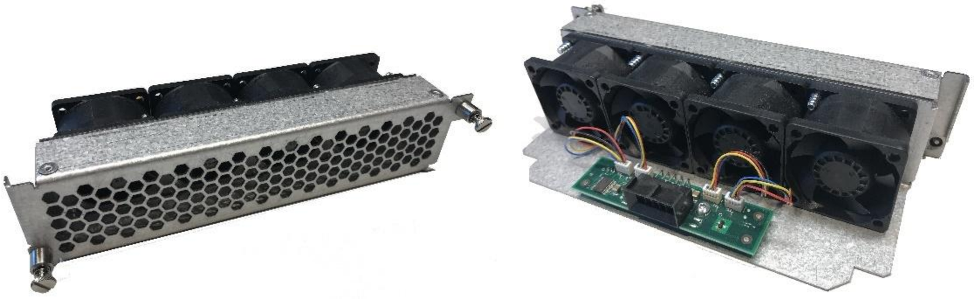


Figure 17. *The DCP-2-FAN-FB unit.*

2.8.1 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.

2.8.2 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.)

Figure 18.

2.9 Network Management Interfaces

The Network Management Interface is a part of the DCP-M-DE chassis. Management connections are available both in the front and rear sides 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.
- ETH1/ETH2/ETH3/ETH4 - 4x 100/1000Base-T interfaces in the back to be connected to the shelf controller. See “Shelf controller User Manual” for details on the functionality of each port.
- ETH5 - 1x SFP port 100/1000Base-X in the back for optical management access to the chassis. See “Shelf controller User Manual” for details on the functionality of each port.
- ETH0 - 1x 100/1000Base-T “local” port access in the front for engineers onsite. Default IP address of the ETH0 port is 192.168.0.1.

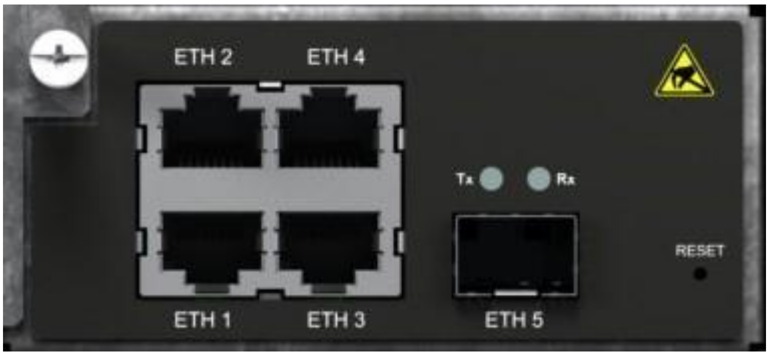


Figure 19. *Network management communication interfaces in the back of the DCP-M-DE chassis.*

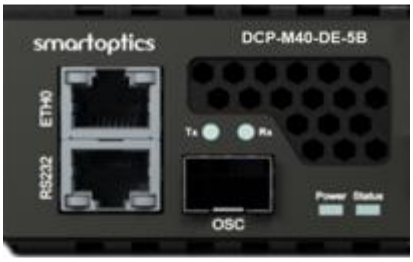


Figure 20. *Network management communication interfaces in the front of the DCP-M-DE chassis.*

2.10 Management architecture

Smartoptics Embedded software is Linux-based and uses Yocto as an open-source collaboration framework. The below figure shows the principal architecture of the system management. The currently implemented APIs are CLI and SNMP. REST and Netconf are planned for future releases.

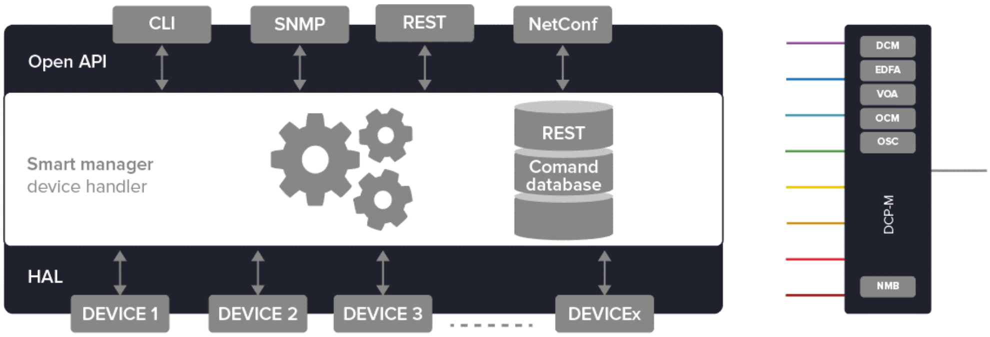


Figure 21. *Management architecture.*

2.11 Monitor points

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

2.12 Alarms

The DCP-M-DE 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
Loss of optical input power	if-<chassi>/<slot>/<Interface>	Critical	The optical power of the interface has gone below the minimum power level. Check the fiber connection and/or clean the fiber connector.
Loss of optical output power	if-<chassi>/<slot>/<Interface>	Critical	
Loss of optical input power(OSC)	if-<chassi>/<slot>/<Interface>	Major	The OSC optical power has gone below the minimum power level. It could be because the remote ends OSC is administratively disabled or that the dark fiber has been cut or disconnected.
Loss of optical input power(Line)	if-<chassi>/<slot>/<Interface>	Critical	The optical input power in to the pre-amplifier is below the minimum level.
Loss of OSC link	if-<chassi>/<slot>/<Interface>	Major	Loss of OSC link indicates there is no communication to the remote hosts OSC channel.
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.
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
Low disk space	chassis	Minor Major Critical	Check current disk space with command “show system diskUsage” <5MB available <7.5MB available <10MB availale
eMMC failure	chassis	Critical	The memory is not formatted. Contact support.

2.13 Backup and restore

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

2.14 Telemetry streaming with gNMI

This section provides details on using gNMI (gRPC Network Management Interface) for DCP-M40-DE-5X8 and DCP-M40-DE-1X40, including connection setup, supported encoding, extensions, and subscription options.

Connection Details

- Port: 57400
- Authentication: Uses the same username and password as SSH.
- Security: Currently operates in an insecure mode.
- Encoding: JSON is the supported encoding format.

gNMI Extensions

Our product supports gNMI extensions, including depth control and master arbitration.

Subscription Modes

gNMI supports different subscription methods for retrieving data:

i. Poll
The client explicitly requests updates by polling the server.

ii. Once
A single snapshot of the requested data is returned.

iii. Stream
A continuous stream of updates is sent based on the chosen mode:

1. Sample Mode
   Data is sent at regular intervals. Configurable interval determines the frequency of updates. Option to suppress redundant updates. Heartbeat ensures periodic updates even if no changes occur.
2. On-Change Mode
   Only sends updates when the data changes.
   Options:
   a. Updates Only: No initial state report; only changes are sent.

b. Suppress Redundant: Only changes are reported (no duplicates).

c. Heartbeat: Periodic updates are sent regardless of suppress redundant settings.

XPath and Wildcard Support

Our implementation provides light support for wildcards in XPath queries, enabling flexible data selection.

This manual serves as a guide for configuring and managing gNMI in DCP products. For additional configuration details, refer to the official gNMI specification.

CLI commands to enable/disable gNMI:

```
root@M40-gNMI>config gnmi service enable
Service: enabled

root@M40-gNMI>config gnmi service disable
Service: disabled
```

2.14.1 Support for secure gNMI with TLS

The DCP-M Network Element (NE) can act as a gNMI server. It is possible to enable an encrypted TLS (Transport Layer Security) session between the client and the NE for gNMI. In standard TLS mode, the NE (DCP-M) will use a certificate that will be validated on the client side. It is also possible to use mutual TLS, mTLS, where both the client and the server will have their own certificates.

CLI commands to enable secure gNMI with TLS:

```
root@M40-gNMI>config gnmi mode secure
Mode: secure

root@M40-gNMI>config gnmi mode insecure
Mode: insecure
```

CLI command to generate a private key:

```
root@M40-gNMI>config gnmi tls privateKey generate
Enter key type [RSA,EC]: EC

Enter Curve (valid curves can be found with 'openssl ecparam -
list_curves'): secp384r1
This operation can take some time, keep patient.
private key generated.
```

CLI command to create a certificate signing request:

```
root@M40-gNMI>config gnmi tls deviceCert csr

Enter Country (C): SE
Enter State (ST): Stockholm
Enter Locality (L): Stockholm
Enter Organization (O): Smartoptics

Generated CSR:
-----BEGIN CERTIFICATE REQUEST-----
MIIBVTCB3QIBADBeMQswCQYDVQQGEwJTRTESMBAGA1UECAwJU3RvY2tob2xtMRIw
EAYDVQQHDAlTdG9ja2hvbG0xFDASBgNVBAoMC1NtYXJ0b3B0aWNzMREwDwYDVQQD
DAhNMzItZ05NSTB2MBAGByqGSM49AgEGBSuBBAAiA2IABF8HTGYTwyoLbyZyV6Rl
bmpTUuV2tv7bhq5fBYVkgdYzR+Az6956fTAPY8OyQTRz1pbyGdh4yctk5DRXQh7l
Fo+akRfMMbWUVJLpUt/HHHjXh5pBdiXe3uaajq7cKxOgO6AAMAoGCCqGSM49BAMC
A2cAMGQCMAxduJQ9YlvNlwyfbJGroIsgWHSmbG2ms6pK9DeLz502xgjMLat/KIQR
Vj3CcMcurwIwaYc8T7uibTGoFKt94PwFv2sNptcs5v1C9gRBCyE8MsL3AmypslY+
op0a/ehVGy/C
-----END CERTIFICATE REQUEST-----
```

CLI command to import a device certificate file:

```
root@M40-gNMI>config gnmi tls deviceCert import device
Input content of cert
-----BEGIN CERTIFICATE-----
<snip>
-----END CERTIFICATE-----, end with an empty line. :
```

CLI command to import a Certificate Authority (CA) certificate file:

```
root@M40-gNMI>config gnmi tls deviceCert import ca
Input content of cert
-----BEGIN CERTIFICATE-----
<snip>
-----END CERTIFICATE-----, end with an empty line. :
```

CLI command to configure mTLS (validate means that mTLS is activated, ignore means that mTLS is deactivated):

```
root@M40-gNMI>config gnmi tls clientCert cert ignore
Client cert: ignore

root@M40-gNMI>config gnmi tls clientCert cert validate
Client cert: validate
```

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-M-DE.

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

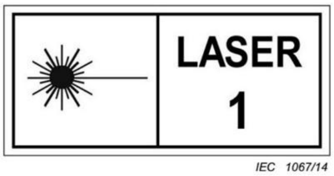
The grounding must also be made through the AC power cable, which should be inserted in a power outlet with a protective ground contact. Therefore, the power cable plug must always be inserted in a socket outlet provided with a protective ground contact, and the protective action must not be negated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

3.1.3 Laser Safety Classification

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

PHYSICAL REQUIREMENTS

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

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

ELECTROMAGNETIC COMPATIBILITY CONSIDERATIONS

The DCP-M-DE 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-M-DE 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-M-DE must be installed in a CBN (common bonding network) per NEBS GR-1089.

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

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

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).

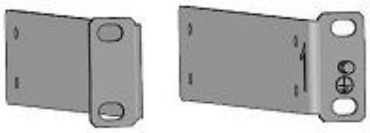
3. With the rack posts mounted to the mid-section of the system (Two-Post Rack).

3.2.1 Rack-mount kit parts list

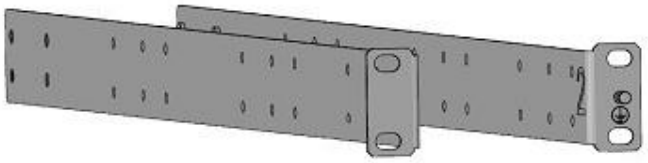
The following parts are provided with the rack-mount kit.

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)

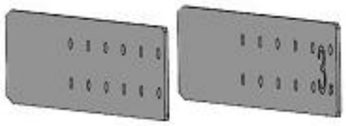
1 Mid-mount, front right and front left (225mm)



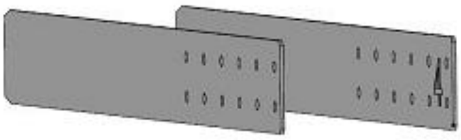
2 Front-mounting bracket, right and left (700mm)



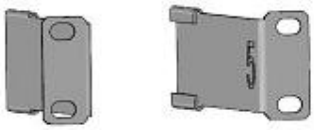
3 Front bracket extension, right and left (270mm)



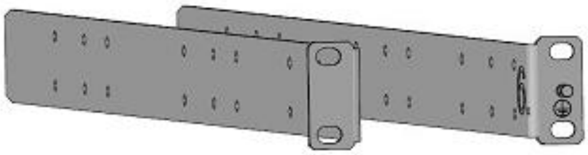
4 Front bracket extension, right and left (470mm)



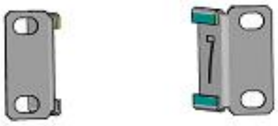
5 Rear-mounting brackets, right and left (142mm)



6 Front-mounting bracket, right and left (600mm)



7 Rear-mounting brackets, right and left (42mm)

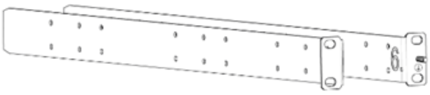
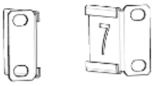
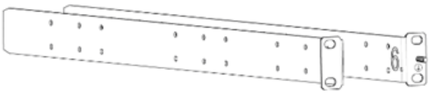
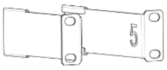
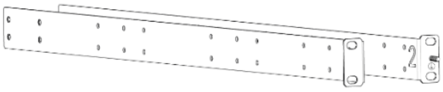
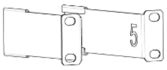
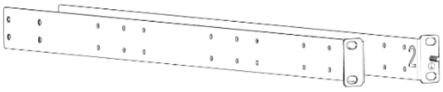
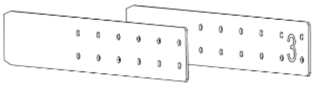
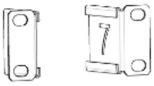
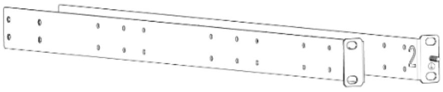
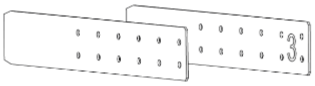
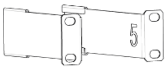
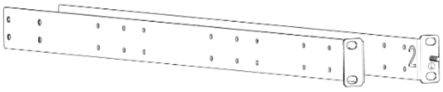
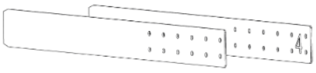
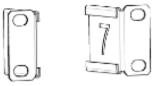
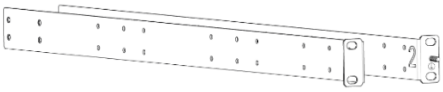
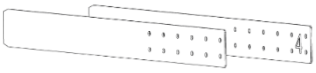
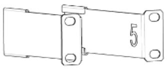


8 Screws, M4x6 x 20 pcs

3.2.2 Determining bracket configuration

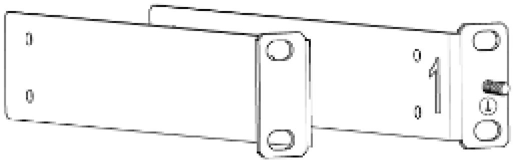
3.2.2.1 4-Post Rack

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 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.).

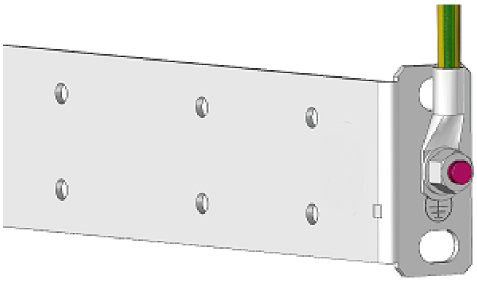
3.2.8 Protective Ground Terminal

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-M-DE 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-M-DE chassis, incl. PSU:s and fan unit
- Quick Installation Guide

4.2 Initial start up

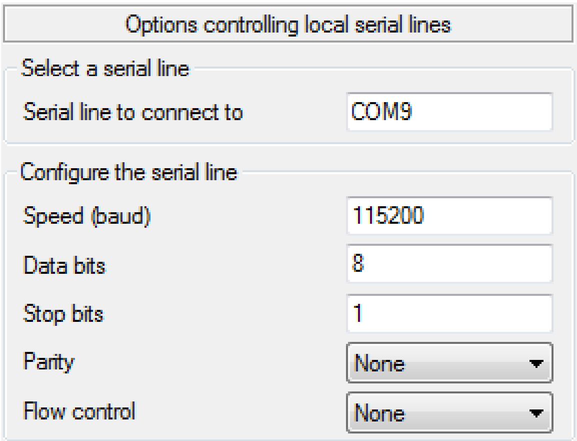
Connect power to the power supplies that are preinstalled in the chassis. The chassis will automatically power up as soon as the first PSU is connected. The power LED turns green.

The fan package starts up after a few seconds.

4.3 Connection to Serial Port

Connect the Serial port of the DCP-M-DE 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



Options controlling local serial lines

Select a serial line

Serial line to connect to: COM9

Configure the serial line

Speed (baud): 115200

Data bits: 8

Stop bits: 1

Parity: None

Flow control: None

Figure 22. *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.

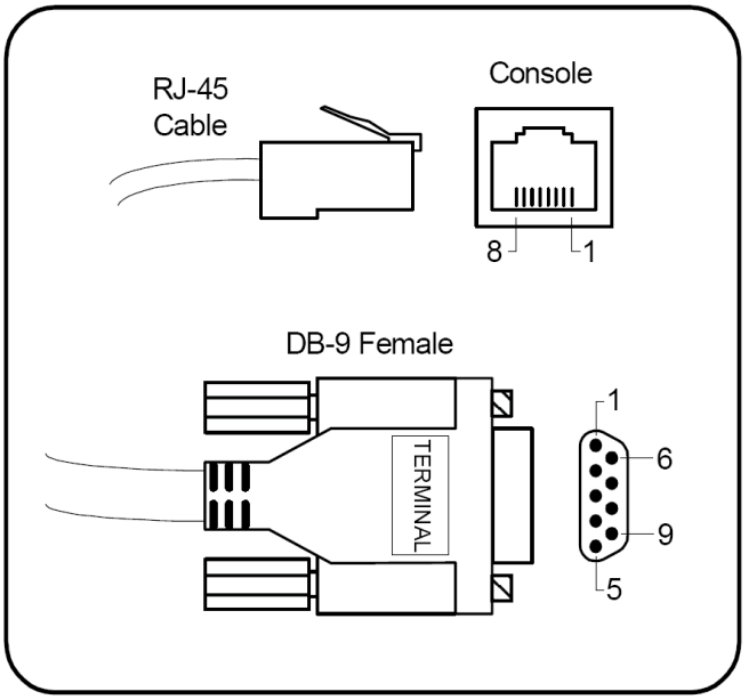


Figure 23. *Serial Console Cable Connectors*

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@DCP-M-19>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@DCP-M-19>
```

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 ports on the DCP-M-DE to a switch with a CAT5/6 cable.

Note: ETH0 uses the fixed IP address 192.168.0.1.

```
admin@DCP-M-19>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@DCP-M-19>
```

4.5 Use CLI interface

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

Then press the ***tab*** key to see an overview of the available queries. You can also type “***?***” to get more detailed information of available commands and options.

```
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 "***tab***" in order to display more information on any query, as for the example which arguments, if any, are required to complete a query.

It is also recommended to start, type the first letters of a query and then use the Tab key to complete the query. This avoids mistakes in typing manually.

4.6 User accounts

The DCP-M-DE 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.

In addition to the admin account the DCP platform has 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: (config system rootaccess <setting>)

- 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.

5 Configuration of optical parameters

This chapter contains information about how to configure the main optical settings for DCP-M-DE units.

Booster and pre-amplifier settings

```
admin@Manchester>config interface if-1/line booster gain 22

This command can be service interrupting.
Are you sure you want to continue? (Yes/NO): y

Set gain for Booster EDFA to 22 dB.

admin@Manchester>config interface if-1/line preamp gain 22

This command can be service interrupting.
Are you sure you want to continue? (Yes/NO): y

Set gain for Pre-amp EDFA to 22 dB.
```

Channel settings
The examples below show settings for the Rx ports. These are the Rx ports on the filter. The signals that are connected to the filter Rx ports will go through the WSS and amplifier before they exit on the line Tx port. WantedPower is the power out from the booster amplifier.
Settings for the Tx ports are similar, but are related to the signals that pass the pre-amplifier and exit on the filter Tx ports.

```
admin@Manchester>config interface if-1/19370000 rx defaultAttenuation 15

Attenuation set to 15 [dB] on interface if-1/19370000.

Default attenuation of channel '19370000' is set to '15.0' [dB].

admin@Manchester>config interface if-1/19370000 rx wantedPower -2

This command can be service interrupting.
Are you sure you want to continue? (Yes/NO): y

`Wanted power` set to -2 [dBm] on interface if-1/19370000.

admin@Manchester>config interface if-1/19370000 rx description test

Description of interface '19370000-rx' is set to 'test'.
```

Multi-set commands can be used to set same configuration on multiple channels.

```
admin@Manchester>config interface if-1/[19210000-19240000,19340000] rx wantedPower -1

This command can be service interrupting.
Are you sure you want to continue? (Yes/NO): y

`Wanted power` set to -1 [dBm] on interface if-1/19210000.

`Wanted power` set to -1 [dBm] on interface if-1/19220000.

`Wanted power` set to -1 [dBm] on interface if-1/19230000.

`Wanted power` set to -1 [dBm] on interface if-1/19240000.

`Wanted power` set to -1 [dBm] on interface if-1/19340000.
```

6 SNMP

6.1 General

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

The DCP-M-DE 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-M-DE 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.

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.

6.3 SNMP MIBS

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

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-M-DE 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.

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.

Note that you always login to chassis 1 when you are talking to a ROADM node. A ROADM node can consist of several DCP-M-DE 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.

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.

7.3 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-M-DE 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.

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.

8 Audit Trail

The DCP platform records events that occur within the system and provides logging mechanisms 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 are kept within the node and for longer history keeping of events an external Syslog should be configured. When the max allowed log entries are 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 are kept within the node and for longer history keeping of events an external Syslog should be configured. When the max allowed log entries are 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 configurations, 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 are 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 send 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 Waste management

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

11 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-M-DE	DCP-M-DE chassis with fans and 2 PSU (AC) Max: TBDW at steady state Typical: TBDW at steady state and +25 Deg C Max: TBDW during startup
REDUNDANCY	Hot swappable fan & PSUs
COOLING FANS	Front-to-Back straight through airflow
ALTITUDE	3000 m (10.000 ft.)
DIMENSIONS (DCP-M-DE):	
HEIGHT	1.77" (1 RU) (H), 45mm (H)
WIDTH	17.3" (W), 440mm (W)
DEPTH	20" (D), 510mm (D)
WEIGHT (WITHOUT TRAFFIC UNITS)	~ TBD Kg (DCP-M-DE chassis without PSU) ~ TBD Kg (DCP-M-DE chassis with PSU)

NETWORK MANAGEMENT:	
MANAGEMENT INTERFACES	4 x RJ45 LAN ports 10/100/1000Base-T in rear side 1 x SFP LAN port 100/1000 Base-X in rear side 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+, gNMI

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)

11.1 Optical parameters for DCP-M-DE

OPTICAL PARAMETERS	
DCP-M-DE PRE-AMPLIFIER OPTICAL SPECIFICATION	
EDFA MAXIMUM TOTAL OUTPUT POWER	20 dBm
EDFA GAIN FLATTENED OPTIMIZED GAIN	22 dB
EDFA SETTABLE GAIN	22-28 dB
EDFA INPUT POWER RANGE	-2 to -30 dBm
EDFA NOISE FIGURE	5,5 dB
MONITOR PORT RATIO	1% (20 dB)
DCP-M-DE BOOSTER-AMPLIFIER OPTICAL SPECIFICATION	
EDFA MAXIMUM TOTAL OUTPUT POWER	20 dBm
EDFA GAIN FLATTENED OPTIMIZED GAIN	22 dB
EDFA SETTABLE GAIN	22-28 dB
EDFA INPUT POWER RANGE	-2 to -30 dBm
EDFA NOISE FIGURE	5,5 dB
MONITOR PORT RATIO	1% (20 dB)

WB OPTICAL SPECIFICATION	
WB RESOLUTION	6,25 GHz (Flexgrid)
WB MIN CHANNEL WIDTH	37,5 GHz
WB MIN CENTER FREQ	191,25 THz
WB MAX CENTER FREQ:	196,125 THz
WB NO CHANNELS (50 GHZ)	96 (191,35 –196,10 THz)
WB NO CHANNELS (100 GHZ)	48 (191,3 –196,1 THz
WB TYPICAL IL ADD SIDE	4 dB
WB TYPICAL IL DROP SIDE	4 dB
OCM OPTICAL SPECIFICATION	
OCM RESOLUTION	3,125 GHz (Flexgrid)
POWER RESOLUTION	0,1 dB
MIN DETECTION LEVEL (50 GHZ)	-40 dBm
ACCURACY	+/-0,7 dB
40CH MUX/DEMUX	
CHANNEL PLAN	192.1-196.0 THz (DCP-M40-DE-1X40) 191.6-195.9 THz with one guard channel after 8ch (DCP-M40-DE-5X8)
CHANNEL SPACING	100GHz
3DB PASSBAND WIDTH	80GHz
INSERTION LOSS	Typical: 4dB Max: 5.5dB

11.2 Supported OSC transceivers

CERTIFIED TRANSCEIVERS FOR OSC	
PART NUMBER	Description
SO-SFP-155M-L80D-C51	SFP STM1/OC3 FE CWDM 80km 1510nm
SO-SFP-155M-L120D-C51	SFP STM1/OC3 FE CWDM 120km 1510nm
SO-SFP-155M-L200D-C51	SFP STM1/OC3 FE CWDM 200km 1510nm
SO-SFP-155M-O-C51-E	SFP 155M OTDR C51 E-tmp
SO-SFP-1G-O-C51-E	SFP 1G OTDR C51 E-tmp
SO-SFP-L80D-C51	SFP 1GE FC CWDM 80km 1510nm
SO-SFP-L120D-C51	SFP 1GE FC CWDM 120km 1510nm
SO-SFP-L160DH-C51	SFP 1GE FC CWDM 160km HP 1510nm
SO-SFP-L160D-C51	SFP 1GE FC CWDM 160km 1510nm
SO-SFP-L50D-C51	SFP, 1G Ethernet, 1G FC, CWDM, 50km, 19dB, LC, 1510nm

Appendix A List of protocols and ports numbers used by DCP-M-DE

The below table contains information on which services and network protocols are used in the DCP-R and their intended purpose. This information is useful if the DCP-M-DE 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

See more info in the Shelf controller user manual for SSH Master, HTTP, SNMP and Netconf ports.