DCP-110

Technical Description

dcp-release-12.1.3

Contents

1 Introduction

This manual provides the technical description for DCP-110. The DCP-110 is a muxponder card in the DCP-series that can be mounted in DCP-2 chassis.

1.1 General

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 1. *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.

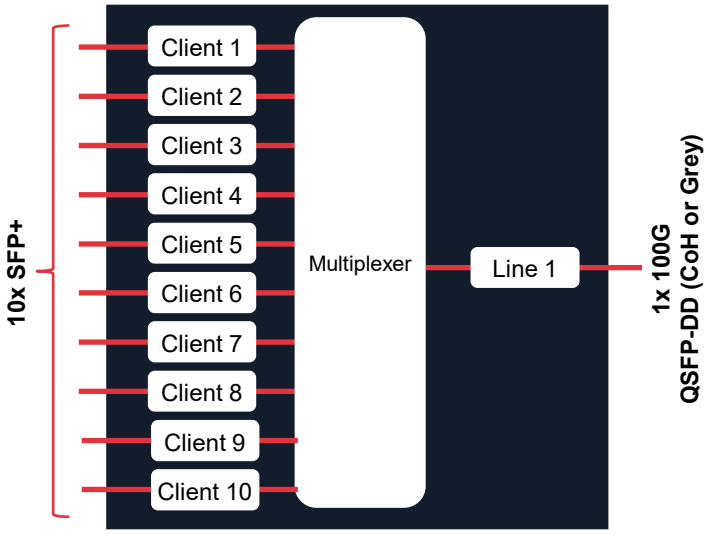


Figure 2. *Functional diagram for DCP-110.*

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.

1.2 In commercial confidence

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

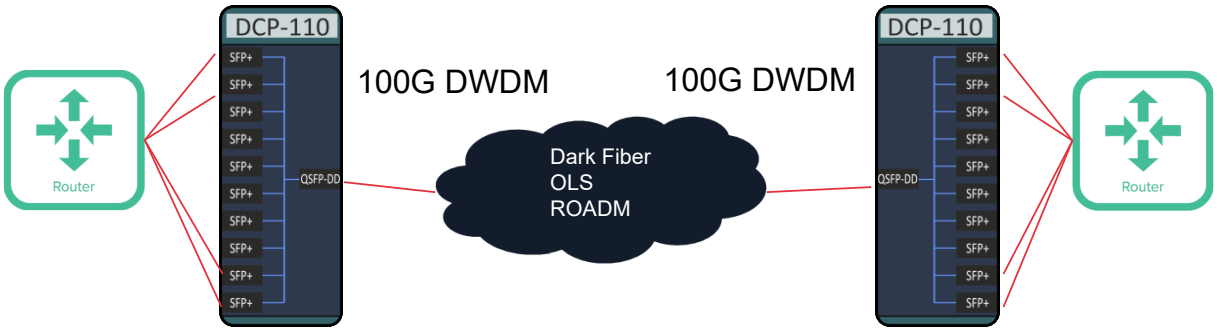
1.3 Document Revision History

Revision	Date	Description of changes
9.0.1 A	2024-01-19	First version of DCP-110 Technical description manual for R9.0.1
9.0.1 PB1	2024-03-26	Updated TQD011 from CMIS 4.1 to CMIS 5.0
10.0.1 A	2024-07-01	Updated traffic mode Updated chapter about encryption Added support for settable dispersion range Added alarms for encryption
10.0.2 A	2024-09-05	No update
11.0.1 A	2024-12-12	Added chapter about fiber intrusion alarm
12.0.1 A	2025-06-24	Added a chapter about dynamic update of certified transceiver list
12.1.1 A	2025-09-08	No update
12.1.3 A	2025-10-23	Added reference to encryption config in DCP-Series_User_Manual

2 Applications

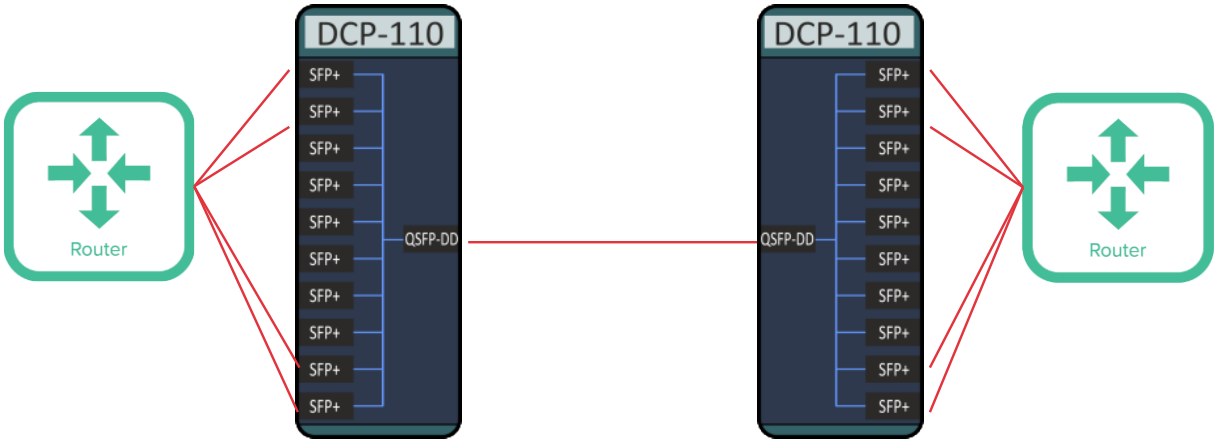
The DCP-110 can work as a muxponder with 10x10G clients aggregated over a 100G line. The 100G line signal can be transported over dark fiber or any DWDM capable line system, including:

- DCP-F
- DCP-R
- DCP-M



2.1 Transport over dark fiber

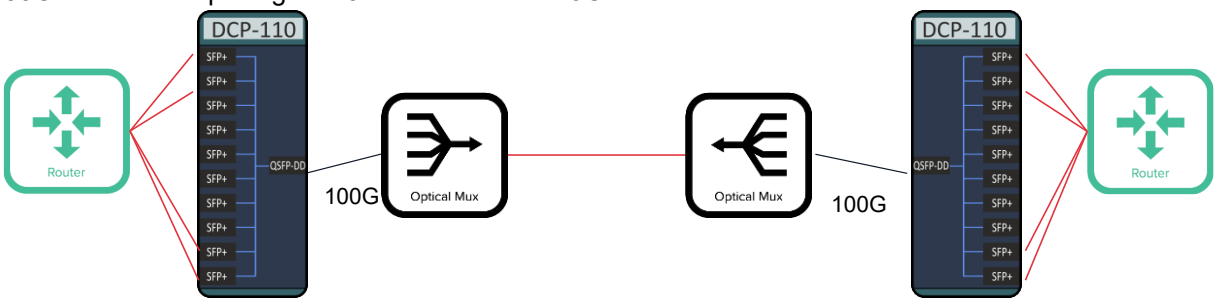
DCP-110 can be used over dark fiber without filters for multiplexing up to 10x10G on same fiber pair. Maximum distance and attenuations can be found in the data sheets for the supported grey QSFP28 and coherent DWDM QSFP-DD transceivers.



2.2 Transport over passive DWDM filters

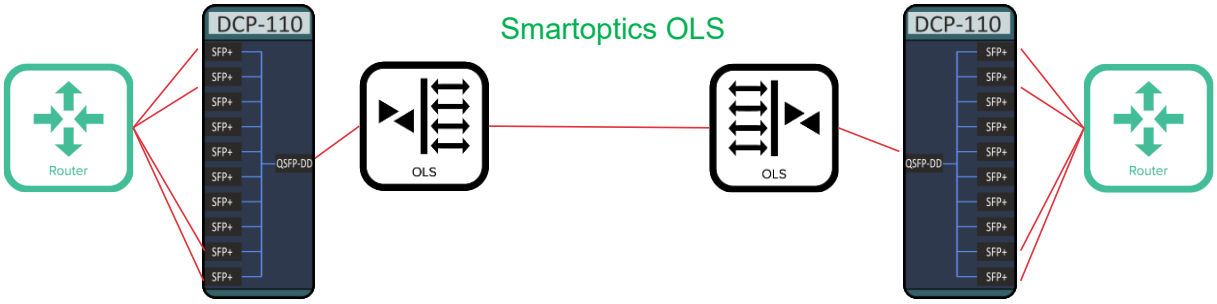
It is possible to run DCP-110 over passive DWDM filters.
For 100G QPSK the 3dB BW is around 35GHz so 100G can be used in systems with

50GHz channel spacing and 3dB filter BW of >40GHz.



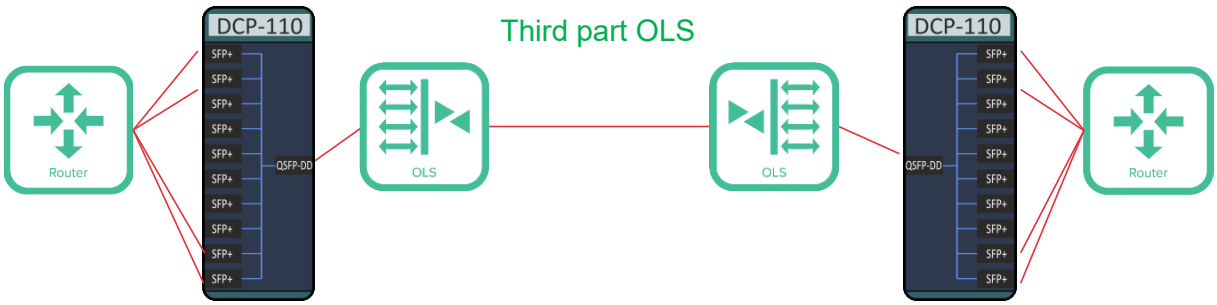
2.3 Transport over DCP-M, DCP-F, DCP-R

DCP-110 can be used over DCP-M, DCP-F and DCP-R line systems.



2.4 Transport over third party line system

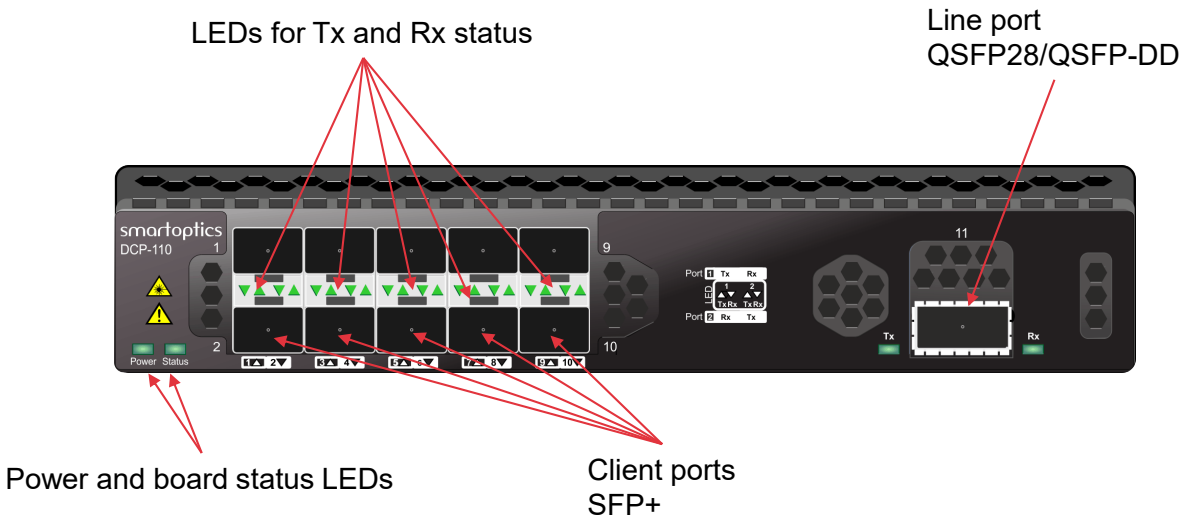
It is possible to use DCP-110 as an alien traffic unit that is connected to a third-party line system.



3 Functional description

3.1 Front layout

The front layout of DCP-110 is quite simple and it is dominated by the SFP+ ports for the clients and the QSFP28/QSFP-DD port for the line. The front also contains some LEDs.



Traffic LEDs for Tx and Rx ports can show Green or Yellow light.
Green means OK.
Yellow means that there is a warning or alarm.

The LED for board status can show Green or Red light.
Green means OK.
Red means that there is a critical or major active alarm.

3.1.1 Traffic LEDs

The traffic LED's are used to indicate the status of the traffic.

Rx Off	Not receiving any light.
Rx Fault (yellow)	Receiving light but with alarm (loss of lock).
Rx On (green)	Receiving light and lock on the signal.
Tx Off	Tx is disabled.
Tx Fault (yellow)	An active alarm on the transmitter side (e.g Tx Faulty).
Tx On	Transmitting and no active alarm.

Traffic case	Traffic LED function

Rx	Tx	Rx	Tx
Off	Off		
Off	Fault		
Off	On		
Fault	Off		
On	Off		
On	Fault		
On	On		
Fault	Fault		

3.1.2 Status LED

The status LED is Red during startup (both warm start and cold start).

When the software is up and running it shall reflect the highest severity of the module.

Green No active alarms.

Red At least 1 active Critical or Major alarm.

3.2 Client port configuration

The client side can support SFP+ transceivers that follows the SFP+ MSA. Each of the 10 client ports can be configured individually with different settings and transceivers independently of the other ports. Note that only 10GBE signal format is possible.

Different options of SFP+ transceivers can be used, e.g. SR, LR, ER, ZR.

See chapter Technical Specifications for supported formats and transceivers.
FEC can be enabled or disabled on the client port.

All client ports have the possibility to use third party SFP+ as long as they have supported formats and follow the SFP+ MSA.

3.3 Line port configuration

The line side can use either grey 100G QSFP28 or coherent DWDM 100G QSFP-DD. The line port can be configured and activated independently from the client ports.

3.3.1 Frequency settings and channel plan

It is possible to set the central frequency for the Tx laser from 191.30 THz to 196.10 THz in steps of 6.25GHz or 50GHz. The granularity will depend on the selected grid spacing. It is possible to select 6.25GHz or 50GHz grid spacing.

Same frequency that is used on the Tx port is then automatically used on the Rx side as well. It is not possible to have different frequencies on the transmitter and receiver.
The default central frequency on all tuneable QSFP-DD is 193.10 THz.

3.3.2 Settable output power

Most coherent DWDM transceiver have a VOA integrated on the Tx port. This parameter can be set from the SW.

3.3.3 Settable loss threshold

DCP-110 will use the loss threshold advertised by the QSFP-DD, but it is also possible to change this threshold manually by using the CLI commands “useLosOverride” and “ losThreshold”. See CLI manual for more info.

3.3.4 Settable alarm thresholds for low and high input power

DCP-110 will use the alarm thresholds for low and high input power advertised by the QSFP-DD, but it is also possible to change those thresholds manually by using the CLI commands “rxPowerAlarmThreshold”, “highRxThreshold” and “lowhRxThreshold”. See CLI manual for more info.

3.3.5 Traffic modes

DCP-110 supports only one traffic mode, mux:10x10G-100G.

3.3.6 FEC

It is possible to enable and disable FEC for grey optics on the line side. Most formats require FEC to be enabled, e.g. SR4, CWDM4, ER4, ZR4.
For LR4 and LR4-10L it is possible to run without FEC, but for LR4-10L we still recommend FEC to be enabled for better performance.

Note that the FEC might not always lock in correctly after configuration changes. Then the CLI may report loss of lock. This can be solved by toggling the FEC on both sides of the link.

3.3.7 Settable dispersion range

The DSPs inside coherent QSFP-DDs can compensate for chromatic dispersion in a defined range. For each transceiver there is a default value for the min and max chromatic dispersion. From R10.0.1 it is possible to change those values within the specification of the transceiver.

Settable dispersion range is supported on DCP-110 with following coherent QSFP-DDs:

TQD011-TUNC-SO, TQD017-TUNC-SO

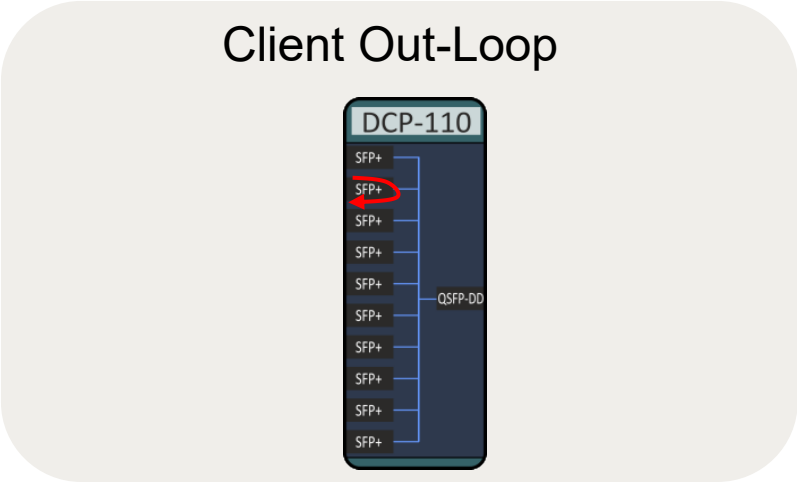
3.4 Loop back

Two different loop back settings are possible for the client side. A warning will be raised during the time that a port is configured in loop back mode.

In this release it is only the client loopback that is implemented, but line side loopback is considered for later releases.

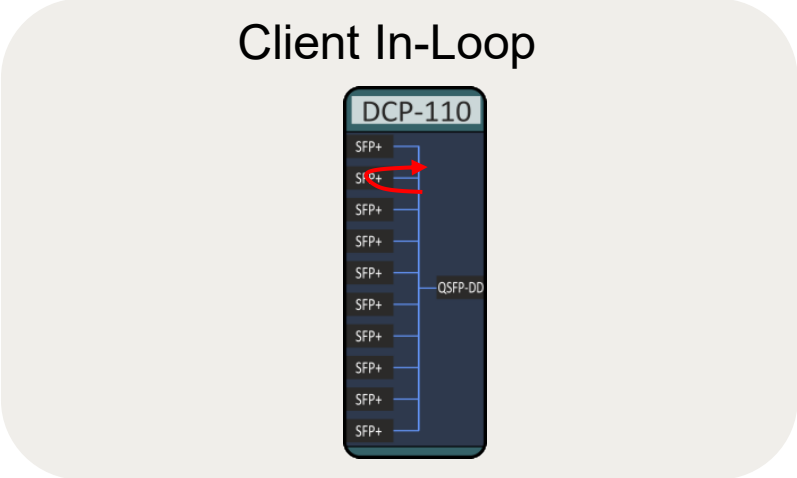
3.4.1 Client Out-loop

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. The loop is mainly done on the ports of the ASIC sitting after the SFP+. No real data processing is done inside the ASIC for the looped signal.



3.4.2 Client In-loop

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 DCP-110 before it is looped back to the line side.



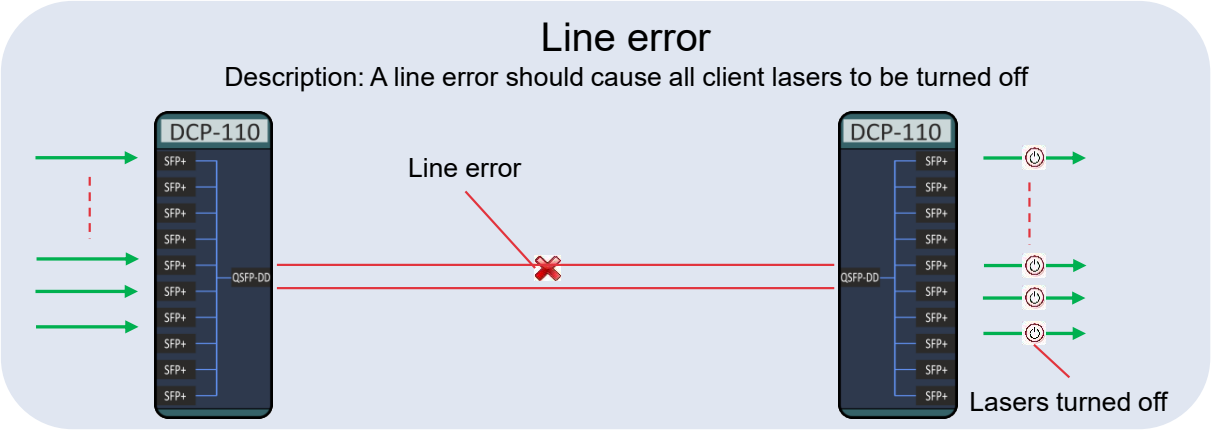
3.5 Link loss forwarding

Link loss forwarding is a setting that can be enabled or disabled via CLI commands. Link loss forwarding can be disabled by setting client laser forced on to enable. Default is that link loss forwarding is on. When link loss forwarding is enabled the client lasers will be turned off in case of an error on the line side

It is possible to use both client link loss forwarding and line link loss forwarding if the coherent QSFP-DD can support it.

3.5.1 Line Link Loss Forwarding

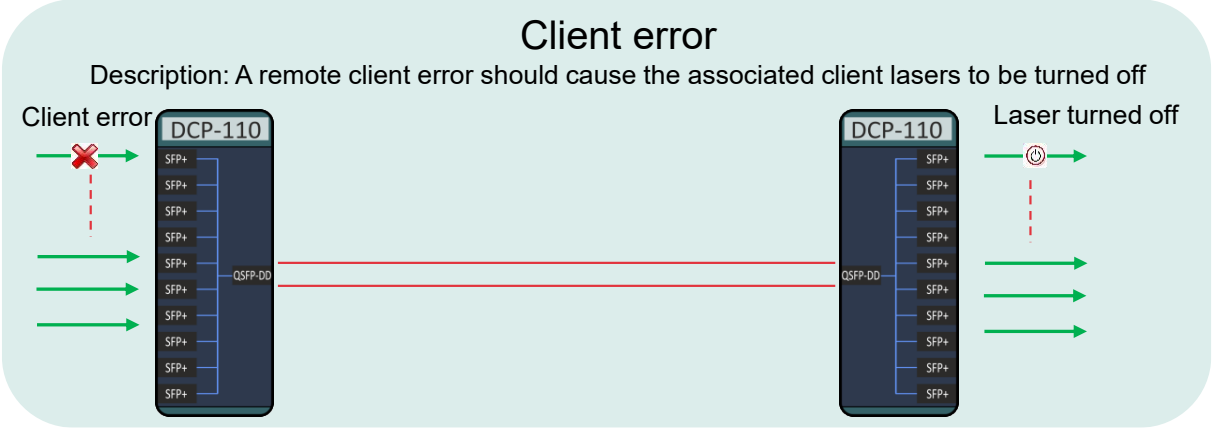
If the link loss forwarding is enabled (client laser forced on = disabled) then all client lasers will be automatically turned off if there is a line error..



3.5.2 Client Link Loss Forwarding

If the link loss forwarding is enabled (client laser forced on = disabled) then the corresponding client lasers on the remote site will be automatically turned off if there is a local client error.

This feature is only possible on coherent QSFP-DDs that support this feature, e.g. TQD011-TUNC-SO.



3.6 Performance monitoring

Many optical performance parameters are available on the DCP-110. The performance value presented is the current value for the last second. Accumulated or historical data are not presented.

Performance parameters on board level

Parameter	Unit	Description
Temperature	C°	Board temperature

Table 1. Performance parameters on board level

Performance parameters on client ports

Parameter	Unit	Description
Total Optical Rx power	dBm	Total received power for all lanes
Optical Rx power	dBm	Received power level per lane
Optical Tx power	dBm	Transmitted power level per lane
Total Optical Tx power	dBm	Total transmitted power for all lanes
Temperature	C°	QSFP28 temperature
Tx bias current	mA	Laser bias current

Table 2. Performance parameters on client ports

Performance parameters on the line ports

Parameter	Unit	Description
Total Optical Rx power	dBm	Total received power
Optical Signal Rx power	dBm	Received signal power level
Optical Tx power	dBm	Transmitted power level
Tx bias current	mA	Laser bias current
Temperature	C°	QSFP56-DD temperature
OSNR	dB	Optical signal to noise ratio
CD	ps/nm	Chromatic dispersion
DGD	ps	Differential Group Delay
Pre-FEC BER	Errors/s	BER before error correction
Pre-FEC BER avg	Errors/s	Average BER before error correction
Post-FEC BER	Errors/s	BER after error correction
Uncorrected BER	Errors/s	Uncorrected errors
Uncorrected BER avg	Errors/s	Average uncorrected errors
PDL	dB	Polarization Dependent Loss
SOP	Rad/s	State of polarization
Q-value	dBQ	Quality of transmission performance related to BER
Q-margin	dB	Margin for Quality of transmission performance related to BER

Table 3. Performance parameters on the line port

It is also possible to monitor FEC counters by using the command "*show interface diagnostics*".
Two values will be shown for each parameter, per second value and accumulated value.

Performance parameters for FEC counters

Parameter	Unit	Description
Uncorrected errors	errors	Number of errors that have not been corrected

Corrected errors	errors	Number of errors that have been corrected
Corrected 0 -> 1	errors	Number of bits identified as 0, but that have corrected to 1.
Corrected 1 -> 0	errors	Number of bits identified as 1, but that have corrected to 0.

Table 4. FEC counters in interface diagnostics

3.7 In-band management

In-band management is not supported in this release.

3.8 Encryption

DCP-110 is HW prepared with a crypto chip to support encryption, but it is also required to have a QSFP-DD that supports encryption and a SW encryption license. QSFP-DDs based on OpenROADM standard support encryption. Following coherent QSFP-DDs can be used for encryption: TQD017-TUNC-SO (100G-400G) and TQD011-TUNC-SO (100G)

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

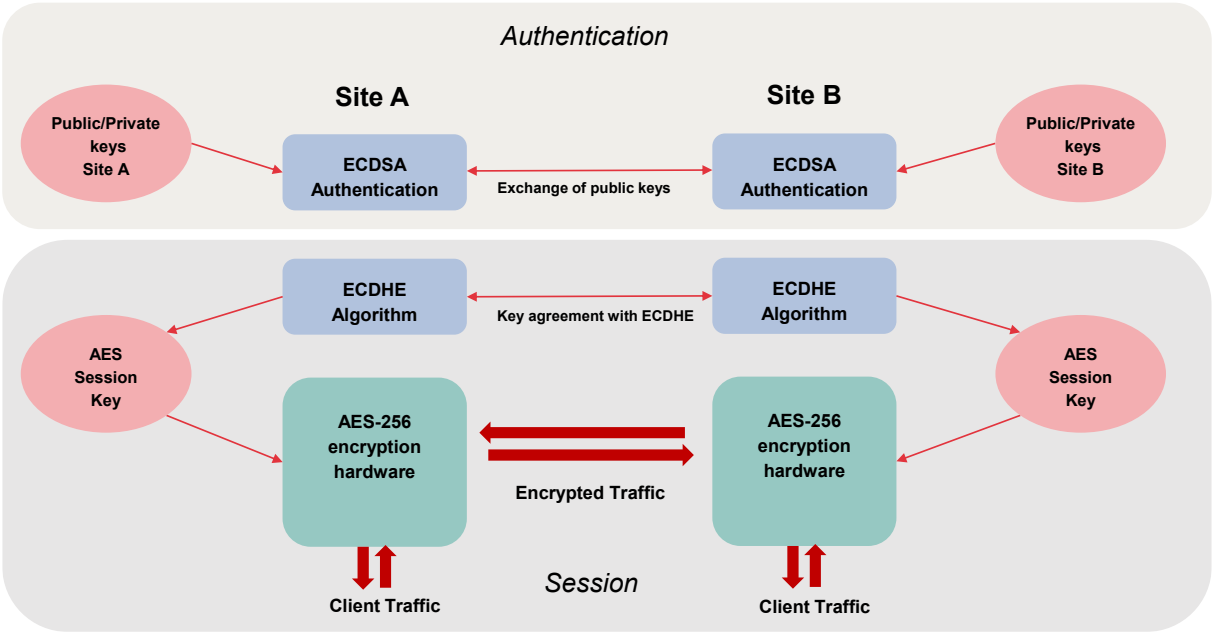
Authentication and key exchange details:

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



When encryption is enabled, the latency will increase 2.35µs per side.

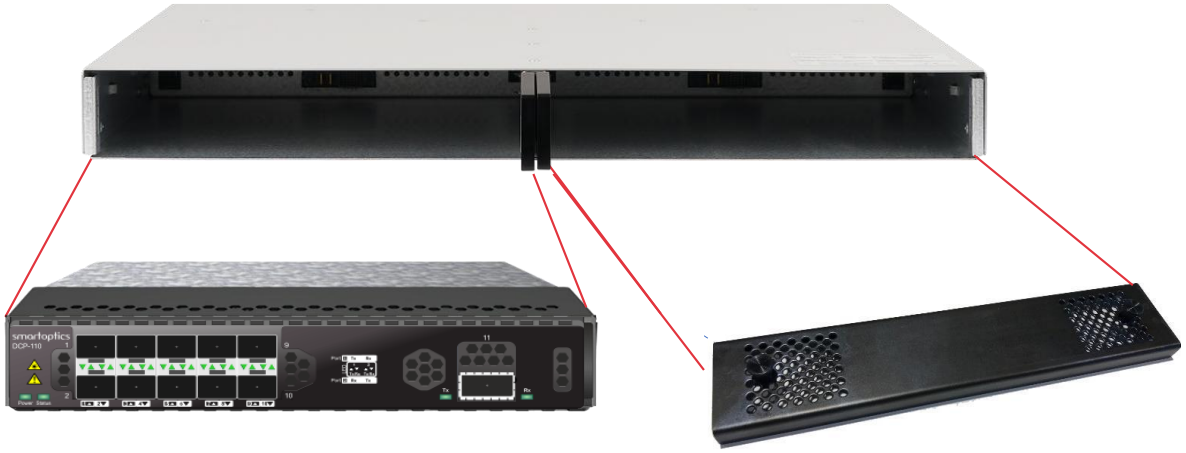
See “DCP-Series_User_Manual” for info how to configure encryption.

3.8.1 Fiber intrusion alarm

When encryption is used, it is possible to configure a fiber intrusion threshold.
A fiber intrusion alarm will be triggered if the power level on the line side is below the configured threshold.

3.9 Temperature requirements

The 400G QSFP56-DD modules are sensitive to high temperatures and can even shut down itself if the temperature is too high. It is important to get best possible air flow for cooling. When DCP-110 is used in DCP-2 chassis it is mandatory to use a blind panel in the other slot if no other card is already used there. The blind panel will ensure that the air for cooling will take the optimum path through the chassis.



It is also important to use two power supplies in the chassis so that air flow on the back side will be correct. If one power supply is missing some of the air will leak out through the empty slot and the cooling will not be optimized.

Note that the FAN units are essential for the cooling and the DCP-110 will not work without them. During FAN unit replacement there is a risk that the temperature will rise quickly and that the QSFP-DD will turn off. For this reason it is recommended to do FAN unit replacements during a service window.

3.9.1 Temperature alarms in QSFP-DD

The temperature of the QSFP56-DD is presented in the CLI and there are three alarm levels related to this:

- “High temperature warning”: Will give a warning if the temperature of the QSFP56-DD exceeds 75 deg C for TQD011-TUNC-SO. (Other units may have different limits).
  The alarm will automatically be cleared when the temperature drops below the limit again.
- “High temperature alarm”: Will raise a critical alarm if the temperature of the QSFP56-DD exceeds 80 deg C for TQD011-TUNC-SO. (Other units may have different limits).
  In this case it is critical to find out why the temperature is so high and to fix it.
  The alarm will automatically be cleared when the temperature drops below the limit again.
- “High temperature shutdown”: The QSFP56-DD will shut down to protect itself from being damaged due to high temperature. This will typically happen when the QSFP-DD temperature is around 85 deg C for TQD011-TUNC-SO. (Other units may have different limits). A critical alarm will also be raised at the same time.

This alarm will not automatically be cleared when the temperature drops below the limit again. Here it is necessary to toggle the admin status of the port so that the QSFP56-DD can be restarted.

3.10 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.

The alarms available for DCP-110 are listed in the table below:

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”
Loopback enabled	if-<chassi>/<slot>/<Interface>	Warning	Loopback Enabled is raised when an interface is configured in loopback mode.
Loss of lock	if-<chassi>/<slot>/<Interface>	Critical	Loss of lock has been detected on the interface. Check that the input signal format is correct.
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.
Transmitter failure	if-<chassi>/<slot>/<Interface>	Major	The transceiver is not transmitting. Replace the optical module.
Transceiver missing	if-<chassi>/<slot>/<Interface>	Critical	The Transceiver has been removed. Insert an Transceiver or disable the alarm with “clear interface portreset <interface_id>”
High temperature warning	if-<chassi>/<slot>/<Interface>	Warning	The temperature of the QSFP56-DD has exceeded the limit 75 deg C. Check if the second slot in DCP-2 has a card or a

			dummy front panel. If not, insert a dummy front panel to improve air flow.
High temperature alarm	if-<chassi>/<slot>/<Interface>	Critical	The temperature of the QSFP56-DD has exceeded the limit 80 deg C. Check if the second slot in DCP-2 has a card or a dummy front panel. If not, insert a dummy front panel to improve air flow.
High temperature shutdown	if-<chassi>/<slot>/<Interface>	Critical	The QSFP56-DD has shutdown due to high temperature.. Check if the second slot in DCP-2 has a card or a dummy front panel. If not, insert a dummy front panel to improve air flow. Restart the QSFP56-DD by toggling the admin status of the interface.
eMMC failure		Minor	The memory is not formatted. Contact support.
Channel authentication key mismatch	trp-<chassi>/<slot>/<Interface	Critical	This alarm indicates that the encryption channel authentication id key mismatch with the key from the remote end.
AES/GMAC tag mismatch	trp-<chassi>/<slot>/<Interface	Critical	This alarm indicates that modification of the encrypted payload have occurred. This alarm could also be triggered as a result of link errors.

Table 5. Alarm list

3.11 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 transceivers that should be treated as certified. See DCP-Series_User_Manual for more information.

4 Spare part handling

4.1 Replacing DCP-110 card

A new DCP-110 card that is inserted in same slot as the replaced unit will automatically get the same configuration as the previous one. If the SW revision on the new card is different it is necessary to upgrade the SW to same release as the chassis.

The SW for the new traffic card can be upgraded by running the same swupgrade commands as for the whole DCP-2 chassis. It is only the boards with the wrong SW that will be upgraded. DCP-2 chassis and other slot modules with correct SW from start will not be affected by the upgrade.

Note that the QSFP-DD from a newly replaced DCP-110 card may be quite hot. The fan units may not start with full speed when the new DCP-110 card is inserted. This means that there is a risk that the QSFP-DD may reach the temperature for shutdown and not start up. Then it is necessary to wait until the QSFP-DD has cooled down and then toggle the admin status of the port or reinsert the QSFP-DD again.

4.2 Replacing FAN unit in DCP-2 chassis

Note that the FAN units are essential for the cooling and the DCP-110 will not work without them. During FAN unit replacement there is a risk that the temperature will rise quickly and that the QSFP-DD will turn off. For this reason it is recommended to do FAN unit replacements during a service window.

5 Technical Specifications

CERTIFIED TRANSCEIVERS FOR CLIENT SIDE OF DCP-110	
PART NUMBER	Description
SO-SFP-10GE-SR	SFP+ 10G MR 850nm MM 300m
SO-SFP-10GE-LR	SFP+ 10G MR 1310NM SM 10KM
SO-SFP-10GE-ER-DXXX	SFP+ 10G MR DWDM 100GHz 40km D9200-D9600
SO-SFP-10GE-ZR-DXXX	SFP+ 10G MR DWDM 100GHZ 80KM D9200-D9600
SO-SFP-10GE-ER-CXX	SFP+ 10G MR CWDM 40km 1470-1610nm
SO-SFP-10GE-ZR-CXX	SFP+ 10G MR CWDM 80KM 1470-1610NM

Table 6. Client transceivers

CERTIFIED TRANSCEIVERS FOR LINE SIDE OF DCP-110	
TQD011-TUNC-SO	QSFP-DD 100G ETHERNET/OTN/OPENROADM, COHERENT TUNABLE SM 450KM ENCRYPTION CMIS5.0 LC
TQD017-TUNC-SO	QSFP-DD OTN HIGH TX POWER COH TUNABLE FLEXGRID ENCRYPTION CMIS5.0
SO-QSFP28-SR4	QSFP28, 100G Ethernet SR4, MM 4x 850nm, 100m, 1.9dB, MPO
SO-QSFP28-LR4	QSFP28, 100G Ethernet LR4, OTU4, SM 1296/1300/1305/1309nm, 10km, 6.3dB, LC
SO-QSFP28-LR4-10L	QSFP28, 100G Ethernet LR4, SM 1296/1300/1305/1309nm, 10km, 6.3dB, LC
SO-QSFP28-CWDM4	QSFP28, 100G Ethernet CWDM4, SM 1271/1291/1311/1331nm, 2km, 5dB, LC
SO-QSFP28-ER4	QSFP28, 100G Ethernet 100G 4WDM-40, SM 1296/1300/1305/1309nm, 40km, 18dB, LC

SO-QSFP28-ZR4	QSFP28, 100G Ethernet ZR4, SM 1296/1300/1305/1309nm, 80km, 31dB, LC

Table 7. Line transceivers

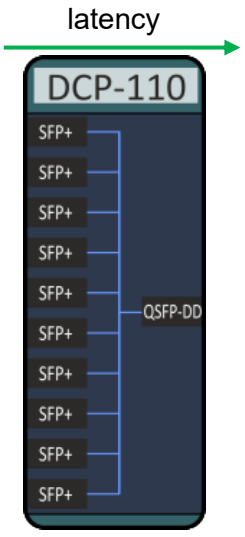
GENERAL	
OPERATING TEMPERATURE	0° C to 45° C
POWER CONSUMPTION	DCP-110 <20W SFP+ <2.3W QSFP28 <5W QSFP56-DD <17W Max total <60 W Typical power, full populated card with LR at 25° C = 52 W
MTBF	TBD years TBD FITs
LATENCY	Latency for TQD011-TUNC-SO[1] 100G OFEC: 11 µs Max X µs for the card [1]Only for 100G The latency will increase 2.35 µs when encryption is enabled Latency is for one direction through the card from client to line or vice versa. 

Table 8. General parameters for DCP-110