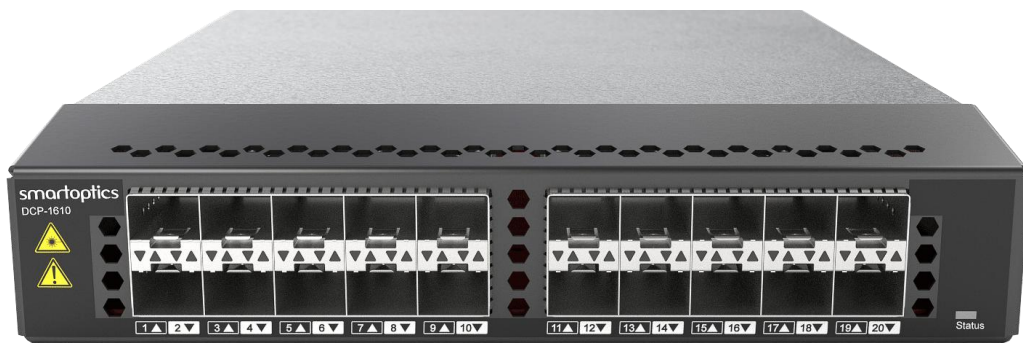# DCP-1610

Technical Description

dcp-release-12.1.1

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

This manual provides the technical description for DCP-1610. The DCP-1610 is a traffic unit with 10 multi-rate transponder functions on same board. The DCP-1610 card belongs to the DCP-series and it can be mounted in DCP-2 chassis.

1.1   General

The DCP-1610 is a high density multilane transponder module for the DCP-2 1U chassis system.

Each DCP-1610 offers ten independent transponders operating from 1G to 16G line rates, enabling 20 x DWDM channels per 1U (40 x DWDM channel per 2U) for high capacity needs.

40G interfaces can be transported via 4x10G wavelength groups with CWDM or DWDM traffic being supported.

The DCP-1610 is perfect for new xwdm transmission installations or as part of any modern disaggregated DWDM deployment strategy (for example any of the Open Source Hardware initiatives) and can be used with any mux/demux platform compliant to ITU DWDM standard G.694.1 or CWDM standard G.694.2.

G.709 FEC is available on all interfaces for 8G/10G/40G protocols to extend the transmission distance in amplified systems.

8G/10G/16G/40G traffic can be encrypted using next generation encryption techniques compliant to FIPS 140-2 Suite B.

For 8G/10G/40G traffic this encryption can be combined with GFEC G.709 for long distance transport.
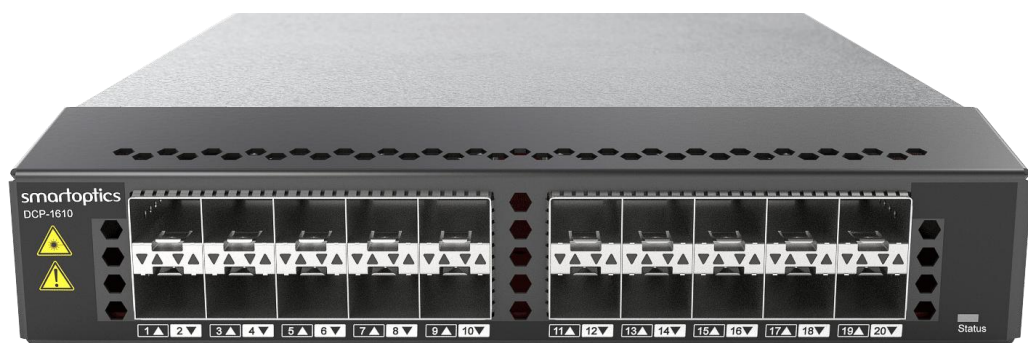
Figure 1.   *Front view of DCP-1610 plug-in unit.*

The DCP-1610 has support for SFP/SFP+ on the client side and SFP+ on the line side. It is possible to configure different signal formats as well as encryption. In addition to the use as transponder, the DCP-1610 can also be used as repeater or media converter
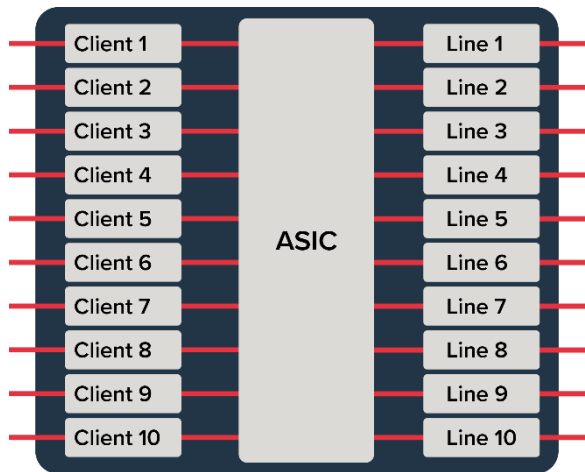
Figure 2. *Functional diagram for DCP-1610.*

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
8.1.1 A	2023-07-05	First draft R8.1.1 Added supported 10G transceivers for converter
8.1.2 A	2023-08-09	Updated alarm list Added link loss forwarding mode
8.1.3 A	2023-08-22	No update
8.1.4 A	2023-10-12	No update
8.1.4 B	2023-10-23	Updated severity on eMMC failure alarm
8.1.5 A	2023-11-02	No updates
8.1.6 A	2023-11-17	Updated severity on eMMC failure alarm
9.0.1 A	2023-01-19	First version R9.0.1
10.0.1 A	2024-06-18	Updated alarm list Note about OTU2-OTU2 traffic format added
10.0.2 A	2024-09-05	No update
11.0.1 A	2024-12-12	Included chapters for configuration of encryption
12.0.1 A	2025-06-24	No update
12.1.1 A	2025-09-08	No update

2 Applications

The DCP-1610 can be used with both grey, CWDM and DWDM optics over both active and passive line systems.

2.1 DCP-1610 over passive line system

It is possible to run DCP-1610 over passive CWDM or DWDM filters.
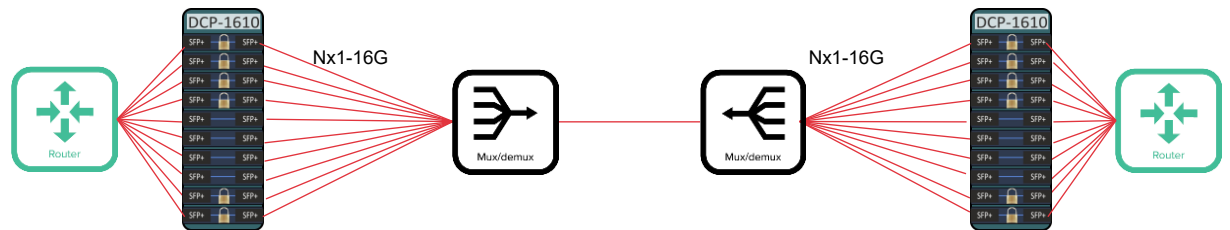
2.2 DCP-1610 over active line system

It is possible to run DCP-1610 over different kinds of active DWDM line systems, e.g. DCP-M, DCP-F, DCP-R or third party.
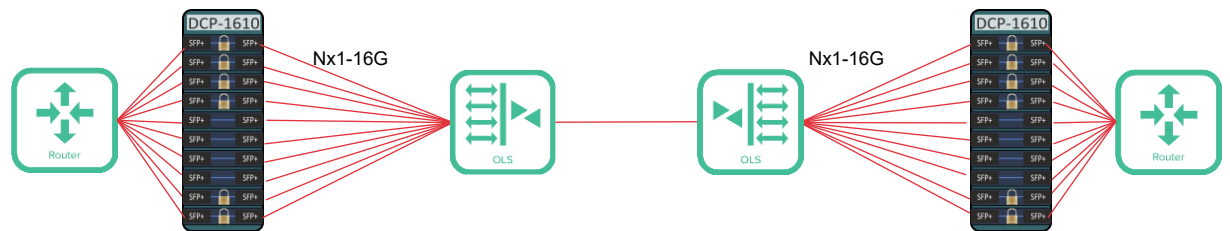
3   Functional description

3.1   Front layout

The front layout of DCP-1610 is quite simple and it is dominated by the SFP/SFP+ ports for the clients and lines. The front also contains some LEDs.

Line ports, SFP+

Client ports, SFP/SFP+
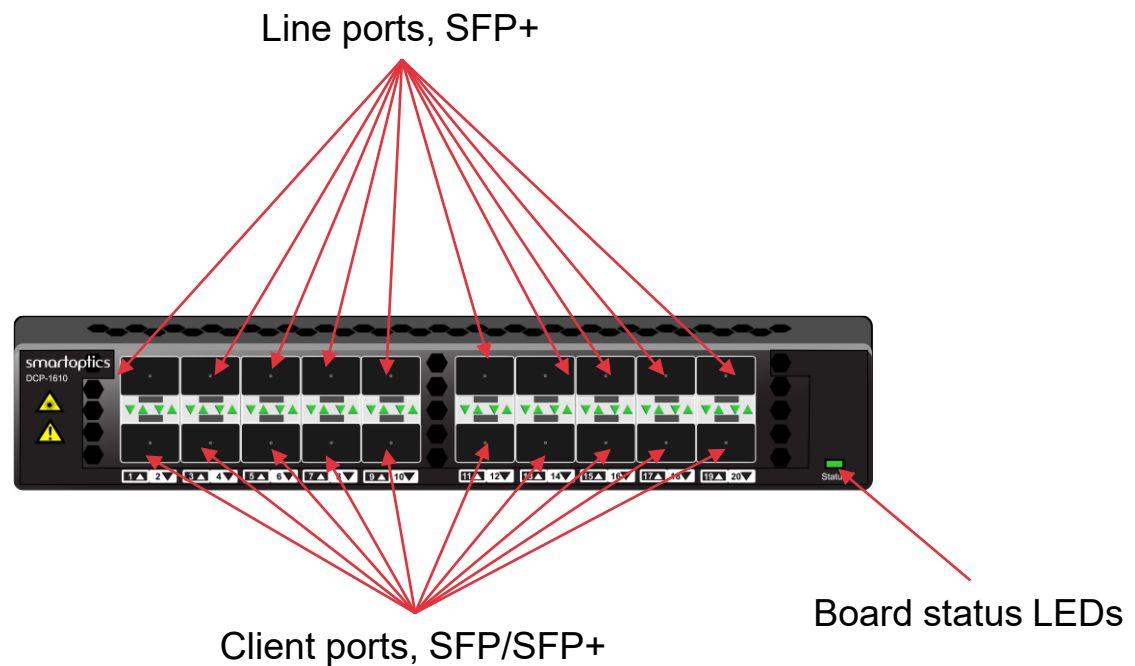
Board status LEDs

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)	○ (off)
Off	Fault	○ (off)	● (yellow)
Off	On	○ (off)	● (green)
Fault	Off	● (yellow)	○ (off)
On	Off	● (green)	○ (off)
On	Fault	● (green)	● (yellow)
On	On	● (green)	● (green)
Fault	Fault	● (yellow)	● (yellow)

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/SFP+ pluggables that follow the SFP/SFP+ MSAs. Each of the 10 client ports can be configured individually with different settings and pluggables independently of the other ports.

Different options of SFP/SFP pluggables can be used, e.g. 1G, 10G, 16G ER, ZR, DWDM, CWDM, 16G. See chapter Technical Specifications for supported formats and pluggables. FEC can be enabled or disabled on the client and line port.

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

3.3 Line port configuration

The line side support SFP+ pluggables with 10G or 16G bit rate that follow the SFP+ MSA. Each of the 10 line ports can be configured individually with different settings and pluggables independently of the other ports.

Different options of SFP+ pluggables can be used, e.g. 10G, 16G ER, ZR, DWDM, CWDM, 16G. See chapter Technical Specifications for supported formats and pluggables.
FEC can be enabled or disabled on the line port.

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

3.3.1 Traffic modes

Different traffic formats can be configured. See table below.

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

Note that OTU2-OTU2 is possible to set on the DCP-1610, but interop with other OTN devices must be tested before use.

3.3.2 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.

Note that the function is loop and continue so traffic will both be looped and continue on the other side.

Client Out-Loop
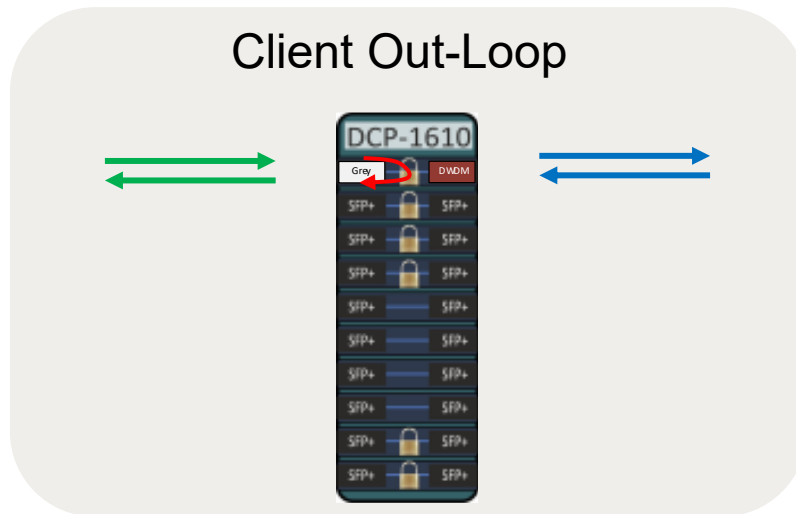
3.3.3   Line Out-loop

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

.

Note that the function is loop and continue so traffic will both be looped and continue on the other side.

Line Out-Loop
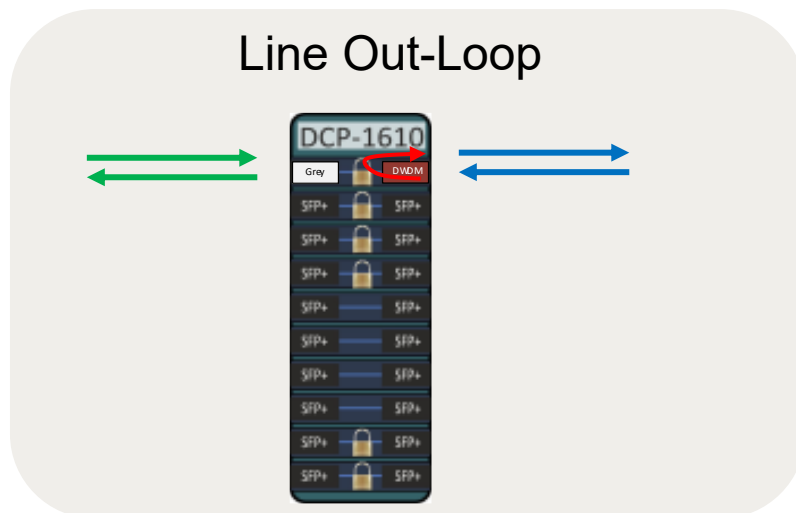
3.4   Link loss forwarding

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 client or line side.

Link loss forwarding for line errors
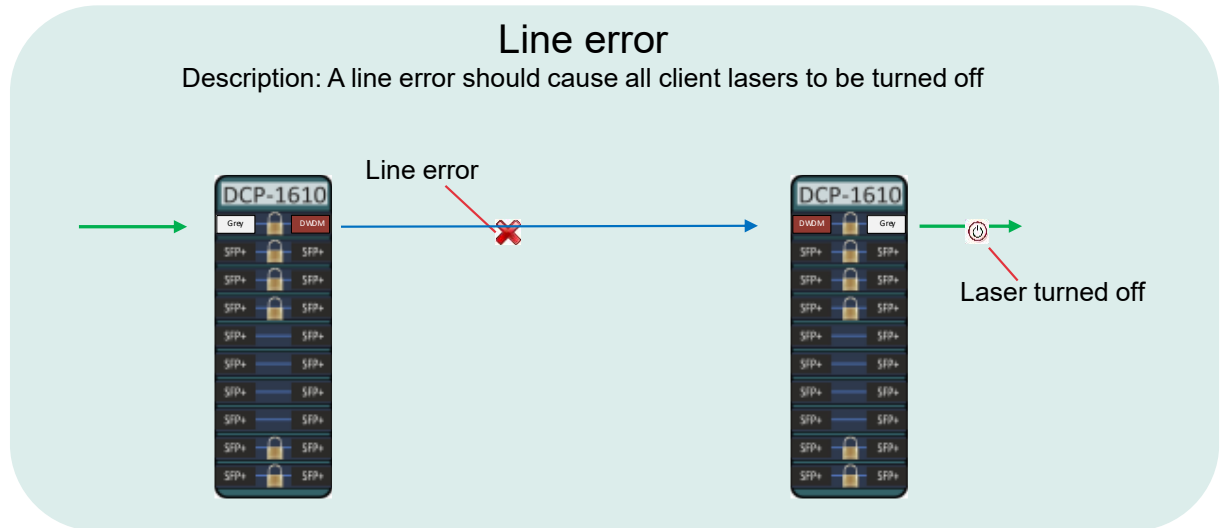
Link loss forwarding for client errors
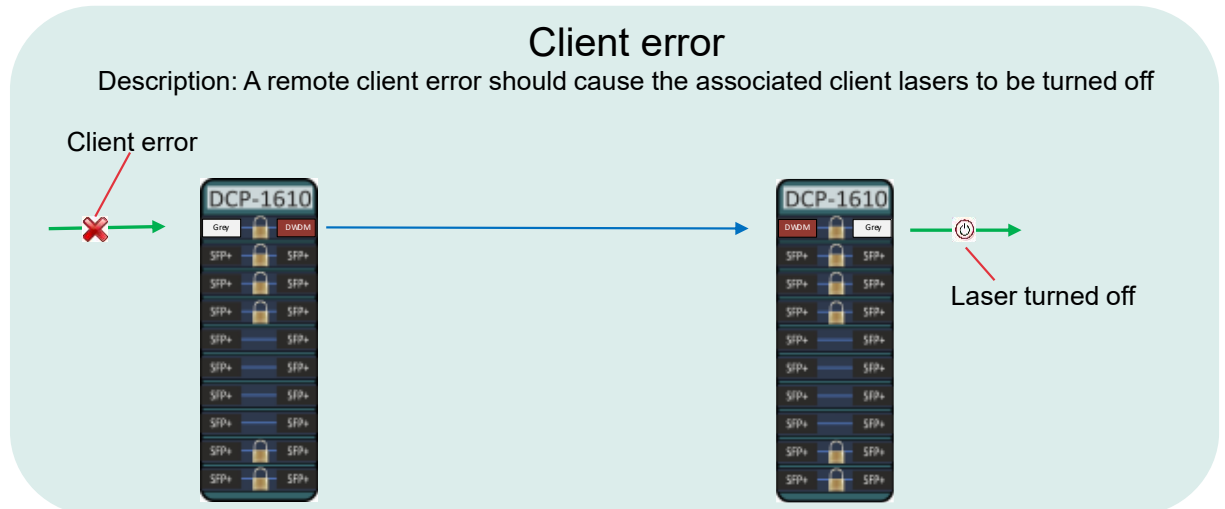
Link loss forwarding mode

It is possible to select if the link loss forwarding should be triggered on both loss of lock (LOL) and loss of signal (LOS) or just loss of signal.

This configuration decides what condition that will result in a Link Loss Forwarding action.

This configuration affects both local LLF(Line to Client on same board) and remote LLF (when the line format is an OTU signal and the LLF action is transmitted to the remote transponder and affects the Client Tx on that transponder).

default - Requires both input signal and lock to activate the remote output signal.

losOnly - Requires only input signal to active the remote output signal.

3.5   Performance monitoring

Many optical performance parameters are available on the DCP-1610. 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
Optical Rx power	dBm	Received power level per lane
Optical Tx power	dBm	Transmitted power level per lane
Temperature	C°	SFP+ temperature
Tx bias current	mA	Laser bias current

Table 2. Performance parameters on client ports

Performance parameters on the line ports

Parameter	Unit	Description
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°	SFP+ temperature

Table 3. Performance parameters on the line port

It is also possible to turn on FEC for some traffic formats and then the FEC counters can be monitored 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. Performance parameters on the line port

Ethernet Invalid Symbols PM counters

From R8.1.1 it is possible to monitor invalid symbol errors in the Ethernet frames on the client and line ports. This monitoring is only available for 10GbE format. Invalid symbols are not presented for other signal formats.

```
            Per second                                Accumulate
            ==========================================  ==========================================
            Ethernet PM TX          Ethernet PM RX      Ethernet PM TX          Ethernet PM RX
            --------------------    --------------------  ---------------------   ---------------------
Interface   Symbols    InvSymbols   Symbols    InvSymbols  Symbols        InvSymbols  Symbols        InvSymbols
=========   --------   ----------   --------   ----------  -------------  ----------  -------------  ----------
DCP-1610
  if-1/1/2  19650696       19801   19649179        19799  1805771465493  1819525411  1805715507732  1819467930
  if-1/1/4         0           0          0            0              0           0              0           0
  if-1/1/6         0           0          0            0              0           0              0           0
  if-1/1/8         0           0          0            0              0           0              0           0
  if-1/1/10        0           0          0            0              0           0              0           0
  if-1/1/12        0           0          0            0              0           0              0           0
  if-1/1/14        0           0          0            0              0           0              0           0
  if-1/1/16        0           0          0            0              0           0              0           0
  if-1/1/18        0           0          0            0              0           0              0           0
  if-1/1/20        0           0          0            0              0           0              0           0
```

3.6 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-1610 are listed in the table below:

| ALARM MESSAGE	LOCATION	SEVERITY	INTERPRETATION
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.
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>"
Fiber intrusion	if-<chassi>/<slot>/<Interface>	Major	The Optical Rx power of the interface has gone below the saved Fiber intrusion alarm threshold
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.
PM-Tx Invalid symbols threshold exceeded [1s]	trp-<chassi>/<slot>/<Interface>	Major	The counter for invalid symbols per second shows a higher number than the configured threshold
PM-Tx Invalid symbols threshold exceeded [1s]	trp-<chassi>/<slot>/<Interface>	Major	The counter for invalid symbols per second shows a higher number than the configured threshold
Loopback enabled	trp-<chassi>/<slot>/<Interface>	Warning	A warning is shown when the interface has loopback enabled
eMMC failure		Minor	The memory is not formatted. Contact support.

Table 5. Alarm list

3.7   Encryption

From DCP-Series R3.1, the DCP-1610 traffic unit of hardware revision R2A and later supports layer 1 AES-256 GCM encryption. The entire client signal, including the header and the checksum is encrypted and authenticated, so that every single bit of the client signal that is being transported across the communications network is ensured maximum

protection. The ODU overhead (ODU OH) remains unencrypted to enable routing decisions in any OTN switching equipment along the way.

The following 6 transponders supports encryption (from left to right); 1, 2, 3, 4, 9 and 10.

Encryption enabled transponders
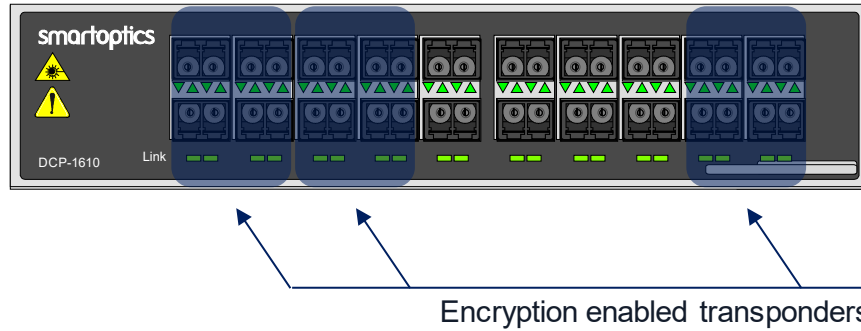
Enabling encryption on the DCP-1610 does not affect transponder configuration options, each transponder function can still be used individually. Each encrypted transponder also have its own independent private keys.

The following client traffic formats are supported to be used for encryption.

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

Table 4. Supported client formats with encrypted line.

See also "DCP-Series User Manaul" for more info about how to configure encryption.

4 Spare part handling

4.1 Replacing DCP-1610 card

A new DCP-1610 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.

5 Configuration of encryption

5.1 User Accounts

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

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

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

- Configuration of encryption enabled transponders incl. crypto key management

- Software Management (Upgrade/Downgrade/Fallback)

- To reset the unit to factory default

- Reboot of the system or plug-in units

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

5.2 Enabling and configuring encryption

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

5.2.1 Enabling cryptoMode

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

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

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

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

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

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

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

5.2.2 Configuring a transponder with encryption

5.2.2.1 Configure the transponder to an encryption capable traffic format

Possible formats to select is any format ending with 'Enc' such as '10GbE-OTU2eEnc'.

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

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

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

crypto@smartoptics-dcp>
```

Figure 5-1. Configuring slot 1 transponder 1 to a 10GbE-OTU2eEnc service.

5.2.2.2 Enabling encryption on the transponder

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

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

Encryption enabled for slot 1 transponder 1.

crypto@smartoptics-dcp>
```

Figure 5-2. Enabling encryption on slot 1 transponder 1.

The pre-shared authentication key (channel authentication ID) is configured on the line ports (uneven interface numbers) such as 1, 3, 5, 7 and 17, 19.

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

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

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

<channel authentication id>  - Encryption channel authentication Id (64 hexadecimal
characters), or 'random' to generate a random ID.

crypto@smartoptics-dcp>
```

Figure 5-3. Configuring the channel authentication ID on slot 1 interface 1 (the line interface of transponder 1).

```
crypto@smartoptics-dcp> config slot 1 interface 1 channelAuthenticationId
24cb6acbb88b44a2865b0987f9da6c73f1abe1598c32d0f7e7c28764b8ab832d

Channel authentication ID set on slot 1 interface 1.

crypto@smartoptics-dcp>
```

Figure 5-4. Example showing configuration of a channel authentication ID, the same key must also be configured on the remote end transponder interface.

5.3   Fiber Intrusion Alarm

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

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

5.3.1 Enabling fiber intrusion alarm

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

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

crypto@smartoptics-dcp>
```

Figure 5-5. Enabling of fiber intrusion alarm.

5.3.2 Disabling fiber intrusion alarm

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

Fiber Intrusion Alarm disabled on slot 1 interface 1.

crypto@smartoptics-dcp>
```

Figure 5-6. Disabling of fiber intrusion alarm.

5.3.3 Verify status and threshold of fiber intrusion alarm

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

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

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

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

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

Status:

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

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

Alarms:

  Fiber intrusion             : ok

crypto@smartoptics-dcp>
```

Figure 5-7. Show interface detail contains related information to the Fiber intrusion alarm configuration.

5.4   Alarms related to encryption

5.4.1   Channel authentication key mismatch

Alarm Severity: Critical

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

5.4.2   AES/GMAC tag mismatch

Alarm Severity: Critical

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

5.4.3   Fiber intrusion

Alarm Severity: Major

This alarm relates to the 5.3 Fiber Intrusion Alarm feature.

If this alarm has been triggered, it means that the _Optical Rx power_ of the interface has gone below the saved _Fiber intrusion alarm threshold._

6 Technical Specifications

CERTIFIED TRANSCEIVERS FOR CLIENT SIDE OF DCP-1610	
PART NUMBER	Description
SO-TSFP-10G-ZR-DWDM-A	SFP+ 10G MR DWDM 50G-T 80KM
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
SO-SFP-16GFC-ER-DXXX	SFP+ 16/8/4G FC DWDM 100GHz 40km
SO-SFP-16GFC-ER-CXX	SFP+ 16/8/4G FC CWDM 40KM 1470NM-1550NM
SO-SFP-1G-10G-SR	SFP+ 1/10G MR 850nm MM 300m
SO-SFP-1G-10G-LR	SFP+ 1/10G MR 1310NM SM 10KM
SO-SFP-10GE-SR	SFP+ 10G MR 850nm MM 300m
SO-SFP-10GE-LR	SFP+ 10G MR 1310NM SM 10KM
SO-SFP-10GE-ACUXM	SFP+ DAC 30AWG Xm active

Table 6. Client transceivers

| CERTIFIED TRANSCEIVERS FOR LINE SIDE OF DCP-1610	
PART NUMBER	Description
SO-TSFP-10G-ZR-DWDM-A	SFP+ 10G MR DWDM 50G-T 80KM
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
SO-SFP-16GFC-ER-DXXX	SFP+ 16/8/4G FC DWDM 100GHz 40km
SO-SFP-16GFC-ER-CXX	SFP+ 16/8/4G FC CWDM 40KM 1470NM-1550NM
SO-SFP-1G-10G-SR	SFP+ 1/10G MR 850nm MM 300m
SO-SFP-1G-10G-LR	SFP+ 1/10G MR 1310NM SM 10KM
SO-SFP-10GE-SR	SFP+ 10G MR 850nm MM 300m
SO-SFP-10GE-LR	SFP+ 10G MR 1310NM SM 10KM
SO-SFP-10GE-ACUXM	SFP+ DAC 30AWG Xm active

Table 7. Line transceivers

GENERAL	
OPERATING TEMPERATURE	0° C to 45° C
POWER CONSUMPTION	Max during startup 86 W Max during operation 69W
MTBF	45 years 2537 FITs

Table 8. General parameters for DCP-1610

Latency is measured by measuring the roundtrip from client to client for one card with a loop on the line side. The result is then divided by 2 to represent the latency for one direction.

The latency in the table below is for one direction through the card from client to line or vice versa.
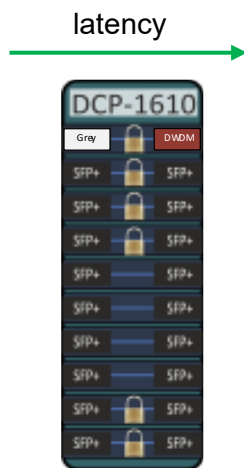
Client Protocol	Traffic service	Latency
1GbE	1GbE-1GbE	7 µs
8GFC	8GFC-8GFC	<4 µs
8GFC	8GFC-OTU2	8 µs
8GFC	8GFC-OTU2Enc	<4 µs
10GbE	10GbE-10GbE	2,6 µs
10GbE	10GbE-OTU2e	7,6 µs
10GbE	10GbE-OTU2eEnc	3,1 µs
16GFC	16GFC-16GFC	<4 µs
16GFC	16GFC-OTU2xEnc	<4 µs
40GbE	40GbE-OTU2e	7,5 µs
40GbE	40GbE-40GbE	2,3 µs
OTU2e	OTU2e-OTU2e	12,5 µs
OTU2e	OTU2e-OTU2eEnc	8,2 µs

Table 9. Latency