DarkStar®

Lighting the path to network independence

DXMOS v4.3

Command Reference

Notices

Please note the following before using DarkStar equipment.

Trademark

DarkStar® is a registered trademark of XKL®, LLC.

Copyright

Copyright © 2006-2023 XKL, LLC

This document contains information that is protected by copyright. All rights are reserved. Reproduction, adaptation, or translation without prior written permission is prohibited, except as allowed under the copyright laws.

All material contained herein is proprietary to XKL, LLC.

Warranty

The information in this publication is subject to change without notice. The information contained herein should not be construed as a commitment by XKL, LLC.

XKL, LLC shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

U.S. Government Restricted Rights

The Computer Software is delivered as "Commercial Computer Software" as defined in DFARS 48 CFR 252.227-7014.

All Computer Software and Computer Software Documentation acquired by or for the U.S. Government is provided with Restricted Rights. Use, duplication or disclosure by the U.S. Government is subject to the restrictions described in FAR 48 CFR 52.227-14 or DFARS 48 CFR 252.227-7014, as applicable.

Technical Data acquired by or for the U.S. Government, if any, is provided with Limited Rights.

Use, duplication or disclosure by the U.S. Government is subject to the restrictions described in FAR 48 CFR 52.227-14 or DFARS 48 CFR 252.227-7013, as applicable.

Class A Compliance

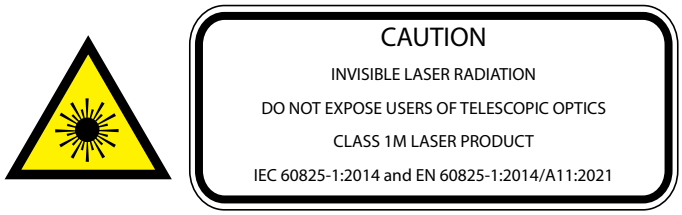
DarkStar equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not operated in accordance with the instruction manual, may cause harmful interference to radio communications.

Operation of this equipment in a residential area may cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Laser Safety

DarkStar products use hazard level 1M laser radiation, which presents a danger to human health.

Do not stare into the lasers or view with non-attenuating optical instruments. Doing so may lead to severe eye damage.



Caution—use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure.

Software Copyright

The software copyright notices are contained in the file located at /CopyrightAndNotices.txt on your DarkStar system.

1 Introduction 1

1.1 Operating System 1
1.2 Syntax Format 1
1.3 Prompts, Modes, and Commands 2
1.3.1 Sub-level Configuration Commands 3
1.4 Keyboard Shortcuts 4
1.5 Command Abbreviations 4
1.6 Command Line Help 5

2 Basic Navigation 7

2.1 disable 8
2.2 enable 8
2.3 configure 8
2.3.1 line 9
2.3.2 management 9
2.3.3 module 10
2.3.4 switch 11
2.4 do 11
2.5 end 11
2.6 exit 11
2.7 logout 12
2.8 no 12
2.9 delete 13
2.10 directory 13
2.11 more 13
2.12 version 14

3 DarkStar System & Configuration Settings 15

3.1 Amplifiers 16
3.1.1 amplifier control automatic 16
3.1.2 Amplifier-Label Keywords 17
3.1.3 show amplifier 18
3.1.4 show running-config amplifier 20
3.2 Controls for Individual Amplifiers 21
3.2.1 control automatic channel-count 21
3.2.2 control manually-set 21
3.2.2.1 control manually-set gain 22
3.2.2.2 control manually-set power 23
3.2.3 shutdown 24

3.2.4 no shutdown 24
3.2.5 los-shutdown 24
3.2.6 no los-shutdown 25
3.3 General Settings 26
3.3.1 app switch 26
3.3.2 banner motd 26
3.3.3 boot 27
3.3.4 boot host dhcp 28
3.3.5 clock 28
3.3.5.1 clock (enable mode) 29
3.3.5.2 clock (configure mode) 29
3.3.6 connect 30
3.3.7 copy 30
3.3.8 description 31
3.3.9 encapsulation 32
3.3.10 fan 34
3.3.10.1 speed 35
3.3.11 hostname 36
3.3.12 idle-mute 37
3.3.13 protection 38
3.3.13.1 protection disable 39
3.3.13.2 clear protection 39
3.3.13.3 show protection 40
3.3.14 sntp 40
3.3.15 switch 41
3.3.15.1 alias local-vif 43
3.3.15.2 alias remote-vif 44
3.3.15.3 alias system id 45
3.3.15.4 local-system 45
3.3.15.5 next-hop system 46
3.3.15.6 destination 46
3.3.15.7 commit 48
3.3.15.8 compare 48
3.3.15.9 revert-to 48
3.3.15.10 show switch 48
3.3.15.11 validate 48
3.3.15.12 end 48
3.3.15.13 exit 49
3.3.16 terminal pager 49
3.3.17 tftp 51
3.3.18 tune 52
3.3.19 tune-for-dmd 52
3.3.20 write 54
3.3.20.1 write memory 54
3.3.20.2 write network 55
3.3.20.3 write terminal 55
3.3.20.4 write erase config 55

4 Networking 56

4.1 telnet 56
4.2 router rip 57
4.2.1 default-information originate 57
4.2.2 network 58
4.2.3 distance 58
4.2.4 passive-interface 59
4.2.5 redistribute 59
4.2.6 version 60
4.2.7 clear rip 60
4.2.8 show rip 60
4.3 ip Commands 61
4.3.1 ip dhcp excluded-address 61
4.3.2 ip dhcp pool 62
4.3.3 ip domain-name 62
4.3.4 ip host 63
4.3.5 ip name-server 63
4.3.6 ip route 64
4.3.7 ip 64
4.3.8 ipv6 address 66
4.3.9 network 66

5 Show Commands 66

5.1 Overview 66
5.2 show running-config 69
5.3 show amplifier 72
5.4 show arp, show ip arp 73
5.5 show calendar, show clock, show time 73
5.6 show debug 73
5.7 show bert 73
5.8 show bert log 73
5.9 show connections 74
5.10 show environment 75
5.11 show file 77
5.12 show flash 78
5.13 show hardware 79
5.14 show hostkey 81
5.15 show hosts 81
5.16 show ip routes 82
5.17 show ip traffic 83

5.18 show led **84**
5.19 show lines **88**
5.20 show logging **88**
5.21 show management **88**
5.22 show memory **90**
5.23 show modules **90**
5.24 show optical itu-grid **94**
5.25 show peers **95**
5.26 show protection **95**
5.27 show rip **95**
5.28 show sntp **95**
5.29 show startup-config **96**
5.30 show tech-support **96**
5.31 show sysinfo **96**
5.32 show switch **96**
5.33 show version **96**
5.34 show vifs **97**

6 Configuring Security 99

6.1 Types of Security **99**
6.2 DXMOS Security Commands **101**
6.2.1 Access Control Lists 102
6.2.1.1 access-list 102
6.2.1.2 access-class 103
6.2.1.3 show running-config access-list 104
6.2.2 Logins and Passwords 104
6.2.2.1 user 105
6.2.2.2 password 105
6.2.2.3 enable secret 106
6.2.2.4 login 107
6.2.2.5 transport input 108
6.2.2.6 session-timeout 108
6.2.3 Preparation for Remote Security 109
6.2.3.1 radius-server host 109
6.2.3.2 radius-server key 110
6.2.3.3 tacacs-server host 110
6.2.3.4 tacacs-server key 111
6.2.3.5 show hostkey 111
6.2.4 AAA Security 112
6.2.4.1 aaa new-model 112
6.2.4.2 aaa authentication login default 113
6.2.4.3 aaa authentication enable default 114
6.2.4.4 aaa authorization exec 115

6.2.4.5 aaa authorization commands 115
6.2.4.6 authorization commands default 116
6.2.4.7 aaa accounting commands 118
6.2.4.8 aaa accounting exec 118

7 **Monitoring & Troubleshooting 119**

7.1 checksum 120
7.2 logging 121
7.2.1 Viewing Buffer Setup and Contents 122
7.2.2 show logging 122
7.2.3 show running-config logging 123
7.3 OTDR Commands 123
7.3.1 otdr 124
7.3.2 show otdr (enable mode) 125
7.4 snmp-server 126
7.5 snmp-traps 130
7.5.1 show running-config snmp 131
7.6 BERT Commands 131
7.6.1 bert log 131
7.6.2 bert transmit 132
7.6.3 bert receive 133
7.6.4 bert restart 133
7.6.5 show bert 133
7.6.6 show bert log 134
7.7 clear 135
7.7.1 ARP (Address Resolution Protocol) Cache 136
7.7.1.1 clear arp-cache 136
7.7.1.2 show arp, show ip arp 136
7.7.2 clear amplifier 137
7.7.3 clear bert 137
7.7.4 clear bert log 137
7.7.5 clear counters 137
7.7.6 clear host 139
7.7.7 clear line 139
7.7.8 clear logging 139
7.7.9 clear management 140
7.7.10 clear module 141
7.7.11 clear rip 141
7.8 Diagnostic Commands 142
7.8.1 debug, undebug all 142
7.8.1.1 show debug 143
7.8.2 verbosity dbg 143
7.9 laser shutdown 144
7.10 loopback 144

7.11 ping, ping6 145
7.12 reboot 146
7.13 reload 148
7.14 show memory 149
7.15 show memory counters management 150
7.16 show tech-support 152
7.17 shutdown 152

A Supplementary Information 153

A.1 Defined States 153
Admin 153
Administrative State 153
BERT Enabled 154
BERT Error Count 154
BERT Status 154
BERT Time 154
Channel 154
Ch 154
Connector 154
CDR Mode 155
CDR Temperature 155
CDR +3.3V Supply Voltage 155
Description 155
Encapsulation 155
Frequency 155
General Status 155
High Alarm 155
High Warn 156
High Warning 156
I2C Address 156
I2C Transaction Error Count 156
IdleTx/Mute 156
Interface 157
Lane <index> 157
Laser Temperature 157
Last Cleared 157
Last Cleared Time Stamp 157
Last Line Chng 157
Link DownTime 157
Line 158
Loopback 158
Low Alarm 158
Low Warn 158
Low Warning 158
Manufacturing Date 159
MFG Date 159
Maximum Reach 159
Module <n / lane> Lane-Status 159

Module <n> Module-Status 159
Module State 159
Module Type 159
OSC - optical service channel 159
Part No. 159
Part Number 159
PRBS Generate 160
PRBS Pattern-Check 160
Rate 160
Receive 160
Reported Wavelength 161
Receiver 161
Rx 161
Rx CDR Firmware 161
Rx Cdr (name, lane) 161
Rx CDR Version 161
Rx Laser Input Power 161
Rx Power 161
RxPow 161
Sensor Reading and Thresholds 162
Sensor Status 162
Serial Number 162
Serial No. 162
Signal Type 162
State Changed 162
Status 162
Status Register Contents 163
Supply Voltage 163
+3.3V Supply Voltage 163
Supported Distance 163
Temperature 163
Time Since Last State Change 163
Total Down 163
Total Down/Error Time 163
Transceiver 163
Transmit 164
Transmitter 164
Tx 164
Tx CDR Firmware 164
Tx Cdr (name, lane) 164
Tx CDR Version 164
Tx Laser 164
Tx Laser Bias Current 165
Tx Laser Output Power 165
Tx Power 165
Vendor 165
Wavelength 165

1

Introduction

1.1 Operating System

DarkStar systems use the DXMOS command line interface (CLI). This chapter contains DXMOS syntax format conventions, keyboard shortcuts, and command summaries. Remaining chapters provide detailed information regarding the CLI commands used to configure and manage DarkStar products.

Reminder: The Systems Guide, found on the XKL website, also provides a wealth of information about our products and how to use them.

1.2 Syntax Format

Table 1-1 shows the conventions used in this guide to represent DXMOS command-line syntax.

TABLE 1-1. Conventions for DXMOS Syntax

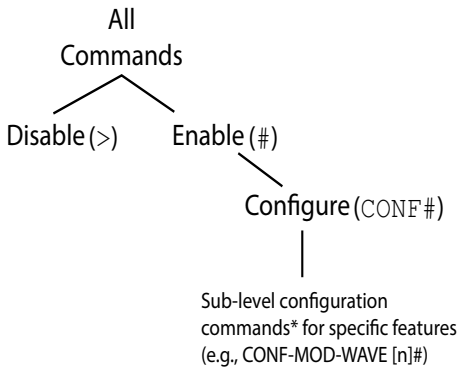
Format	Meaning
`Machine-generated text`	Command line prompt or other machine-generated command line interface (CLI) text. For example: `localhost>`
boldface font	Command line information including commands, command options, and keywords. For example: **show amplifier**
italic font	Arguments that a user supplies, such as free-form input text, passwords, numbers, etc. For example: **snmp-server community** *string*
{}	Curly braces denote required keywords and arguments. The vertical bar(s) between keywords and arguments denotes "or," and means one of multiple terms must be chosen as an option. For example: **{client|osc|trunk}**
[]	Square brackets denote optional keywords or arguments. For example: [no] **snmp-server enable traps**

1.3 Prompts, Modes, and Commands

Important: This guide covers the commands available for this version of the Command Reference. However, there may be some command-associated syntax presented here that is not available for your particular system. To see the exact command syntax available in the current context, either press the <Tab> key or enter a question mark (?). For details, see Command Line Help.

The DarkStar DXMOS essentially has three levels of permission as shown in Figure 1-1: disable mode, enable mode, and configure mode. Disable mode commands (`>` prompt) allow users to view the status of the system, but do not allow any changes to be made to its current state. Enable mode (`#` prompt) requires a password and also allows access to the configure (`CONF#` prompt) mode.

FIGURE 1-1. Permission Levels and Modes Tree



* For a list of sub-level configuration commands, see Table 1-2.

At any enable level, the `exit` command returns to the next level up, while `end` returns to the enable prompt. In configure mode, the `do` keyword executes a top-level command without leaving the current mode. This is very helpful when you are configuring something and want to double-check your work before writing it to memory.

For example, `#` **show ip routes** is an enable mode command, but you can execute it from configure mode by using "do": `CONF#` **do show ip routes**.

1.3.1 Sub-level Configuration Commands

In addition to the commands in the configure mode (indicated by the `CONF#` prompt), there are sub-level configuration commands to set up specific features, each identified by its own prompt. For example, if you are configuring a fan module, you will be entering commands at the `CONF-FAN[n]#` prompt. As you navigate through the system, the prompt provides a sort of sub-level "guide" that changes accordingly. While you are configuring a system, you may see `CONF-MGMT-ETH[n]#`, `CONF-LINE-VTY#`, `CONF-MOD-CLIENT[n]#`, and so on.

In addition to the three permission-level mode commands (`enable`, `configure`, and `disable`), Table 1-2 lists sub-level configuration commands used to set up specific components. **Note:** The table does not necessarily represent all possible sub-level configuration commands or prompts.

TABLE 1-2. Mode Commands Listed by Prompt

Mode/Command	Resulting Prompt
`>` **enable**	Prompt changes to `#`
`#` **configure**	Prompt changes to `CONF#`
`#` **disable**	Prompt changes to `>`
`CONF#` **amplifier**	`CONF-AMP[ampifier-label]#`
`CONF#` **fan**	`CONF-FAN[n]#`
`CONF#` **ip dhcp pool**	`CONF-DHCP-POOL[n]#`
`CONF#` **line vty** `CONF#` **line console**	`CONF-LINE-<VTY|CTY>#`
`CONF#` **management**	The prompt changes depending on the management module you are configuring: - ethernet: `CONF-MGMT-ETH[n]#` - loopback: `CONF-MGMT-LOOP[n]#` - osc: `CONF-MGMT-OSC[n]#`
`CONF#` **module**	The prompt changes depending on the transceiver you are configuring: -client: `CONF-MOD-CLIENT[n]#` -osc: `CONF-MOD-OSC[n]#` -wave: `CONF-MOD-WAVE[n]#` -trunk: `CONF-MOD-TRUNK[n]#`
`CONF#` **router rip**	`CONF-RIP#`
`CONF#` **switch**	`CONF-SWITCH#`

1.4 Keyboard Shortcuts

Table 1-3 lists the keyboard shortcuts that are available in DXMOS:

TABLE 1-3. DXMOS Keyboard Shortcuts

Shortcut	Action
CTRL+A	Go to the beginning of line.
CTRL+B or ←	Go back one character.
CTRL+C	Cancel the current command line input. Canceled commands will not be saved in the command history list.
CTRL+D	Delete the current character.
CTRL+E	Go to end of line.
CTRL+F or →	Go forward one character.
CTRL+K	Delete all characters from the current cursor position to the end of the command line.
CTRL+N or ↓	Scroll forward through the command history.
CTRL+P or ↑	Scroll backward through the command history.
CTRL+R	Redraw the current command input (useful for restoring what was typed if the system writes output to the console while you are entering a command).
CTRL+U	Clear the current command line contents.
CTRL+V	Disregard any special meaning of the character following. The CLI already disregards most special characters and this shortcut is rarely required.
CTRL+Z	Discard the current command line and exit configure mode (equivalent to typing `end` at a configure mode prompt).
<Tab> key or question mark key (?)	Complete partially entered unique keyword. If more than one possible completion exists, it will display a list of choices.
; or !	Ignore rest of line. Use as an initial character to insert comments in the command line.

1.5 Command Abbreviations

Commands may be abbreviated if the command is unique in the current mode. For example, the `show switch` command can be shortened to `sh sw`, but cannot be shortened to `sh s` because there are multiple possible completions. In other words, entering `sh s` will result in additional context-sensitive help choices being shown, followed by `sh s` retained on the input line.

1.6 Command Line Help

Available from any command mode or command line, the tab key <Tab> or question mark key (?) enable you to determine the relevant context-specific commands, keywords and arguments, as well as to auto-fill partial command-line strings. Although the following examples use <Tab>, you can also use "?," as the results are the same.

Note: In these examples, an underscore "_" represents the command-line text cursor, and the spot where you press <Tab>.

One of the commands from Disable Mode (>) is the `show` command. Typing "s" and immediately pressing <Tab> will complete its string.

> s_ Result: > show _

For auto-fill, there should be no space between the letter or partial command string and the text cursor when pressing <Tab>. If the letter or partial command string matches more than one command, those optional commands will be displayed. In this example, `show` is the only available command beginning with "s."

In the result above, auto-fill leaves a single space between the completed string and the text cursor. Depending on the initial command string, pressing <Tab> again may yield a list of added command options. For this example, we show the partial list that appears upon pressing <Tab>:

Result:
```
Information to be displayed, one of the following:
       arp
       bert
       calendar
       chassis
       clock
       connections
       debug
       edfa
       environment
```

From this list, we want `environment` to be the next string in the command line. However, there are two options beginning with an "e"— `environment` and `edfa`. Typing the first letter "e" and pressing <Tab> in this case only narrows the list down to string matches beginning with "e":

> show e_ **Result:**
```
Information to be displayed, one of the following:
       edfa
       environment
```

For a quicker approach, simply type enough of the desired string to differentiate it from all others having the same beginning spelling. Here, we type the partial string "en" and press <Tab> to get `environment`.

> show en_ Result: > show environment _

Additional tab strikes may provide more detail, keywords or arguments from which to choose. If not, the carriage return <cr> symbol will be the only option left. In this example, pressing <Tab> yields added details from which to choose.

Result:
```
specific environmental details one of the following:
 all
 fans
 logging
 power
 temperature
 <cr>
```

Typing "p" for `power` and pressing <Tab> auto-fills the chosen string. The desired command line, as shown below, is now complete.

Result: > **show environment power** _

In this example, pressing <Tab> yet again will yield no further command-line options other than <cr>, which signals that you must press Enter to execute the command.

2

Basic Navigation

As explained in Chapter 1, commands fall into one of three modes: disable, enable, and configure. Enter the modes using the disable, enable, and configure commands, respectively. In addition, when you are configuring certain components, you enter a sub-level mode that contains the relevant commands for that component. For example, if you enter `CONF# router rip`, the prompt changes to `CONF-RIP#`, and you have access to the commands for router RIP configuration. Table 2-1 summarizes the commands used to move between the different modes.

TABLE 2-1. Moving Between Disable, Enable, and Configure Modes

Prompt/Command	Resulting Prompt	Resulting Mode
`>` **enable**	`#`	enable
`#` **configure**	`CONF#`	configure
`#` **disable**	`>`	disable
`#` **exit**	`>`	disable
`CONF#` **end**	`#`	enable
`CONF#` **exit**	`#`	enable
`CONF#` **router rip**	`CONF-RIP#`	router RIP configuration

This section covers the following commands:

- disable
- enable
- configure
- do
- end, exit, logout
- no
- delete
- no, more, version

2.1 disable

Exits enable mode # and returns to the disable mode command-prompt >.

Note: This is the default mode of DXMOS, and only limited commands are available. No commands in this mode can effect any change to system operation or configuration. To unlock the full command set, issue the enable command.

Syntax

 # disable

2.2 enable

From disable mode >, enters the enable mode command-prompt #.

Note: This command is used to unlock the full DXMOS command set. When done viewing or changing settings, issue the disable command to return to disable mode, which will relock the system and prevent accidental or unauthorized system changes.

If an enable mode password is set, the DXMOS prompts for the password before entering enable mode.

Syntax

> enable

2.3 configure

Covered in this section:

- line
- management
- module
- switch

From enable mode, places the DarkStar system into global configuration mode. The command prompt changes to CONF#. To move from CONF# (configure) → # (enable) mode, type end or exit.

Changes made in enable (#) mode immediately affect how the DarkStar is operating. Changes made in configure mode (CONF#) are saved to non-volatile storage using the write memory and write network commands. Any configuration command not saved to memory is lost on the next reboot, reload, or power cycle.

Note: Commands issued from the sub-level configuration mode (e.g., CONF-MGMT-ETH[n]# or CONF-MOD-CLIENT[n]#) do not take effect until the user issues the exit command to return to the next level up (i.e., configure or CONF# mode) or the end command to return to enable mode (#).

If more than one person is logged in and in configure mode (for example, from the console and a remote vty session), the system displays a warning, "Concurrent sessions in configuration mode."

	Commands not covered in this section are Amplifiers, fan, `ip Commands`, and `router rip`. (Click a link to go to the applicable section.)

Syntax

`#` **configure**

2.3.1 line

Places the DarkStar system in line (VTY or CTY) configuration mode. The command prompt changes to `CONF-LINE-<VTY|CTY>#`, depending on your selection. From here you set up many security-related functions, such as passwords, login privileges, and Telnet/SSH access.

Syntax

`CONF#` **line {console|vty}**

Parameters

console	Configures the console (CTY) line.
vty	Configures the virtual terminal (VTY) lines. DarkStar systems have four VTY lines, all configured identically.

Example

```
localhost# configure
localhost CONF# line console
localhost CONF-LINE-CTY# password new-password-string
localhost CONF-LINE-CTY# end
localhost# write memory
Are you sure? (yes/NO) yes
logout
```

2.3.2 management

From configure mode, places the DarkStar system in management configuration mode. After you specify which management interface you wish to configure, the command prompt changes accordingly, depending on what you specified. For example:

- `CONF-MGMT-ETH[n]#`
- `CONF-MGMT-LOOP[n]#`
- `CONF-MGMT-OSC[n]#`

Syntax

`CONF#` **management {ethernet|loopback|osc}** *n*

Parameters

ethernet *n*	The Ethernet interface you wish to configure, an integer. On CMD-based systems, this *n* integer is fixed at *0*. The `management ethernet 0` command corresponds to another port on the switch to which each of the E[*n*] ports are also connected. On non CMD-based systems, this *n* integer matches the E[*n*] numbers on the front panel Ethernet ports. **Note:** To determine whether your system is CMD-based, issue the `show hardware` command.
loopback *n*	The loopback interface you wish to configure, an integer.
osc *n*	The OSC interface you wish to configure, an integer.

Example

```
localhost CONF# management ethernet 0
localhost CONF-MGMT-ETH[0]# ip address 192.168.0.1/24
localhost CONF-MGMT-ETH[0]# exit
Interface Ethernet 0 address set to 192.168.0.1
localhost CONF# exit
localhost# write memory
Destination has 599717888 bytes (149929472 words) available.
Existing file uses 6144 bytes (1536 words).
Are you sure? [yes/NO] yes
```

2.3.3 module

From configure mode, places the DarkStar system in optical transceiver configuration mode. After you specify which module (i.e., transceiver) you wish to configure, the command prompt changes accordingly, depending on what you specified. For example:

```
CONF-MOD-CLIENT[n]#
CONF-MOD-OSC[n]#
CONF-MOD-TRUNK[n]#
CONF-MOD-WAVE[n]#
```

Syntax

`CONF#` **module {client|osc|trunk|wave}** *n*

client *n*	The client transceiver you wish to configure, an integer.
osc *n*	The OSC transceiver you wish to configure, an integer.
trunk *n*	The trunk transceiver you wish to configure, an integer.
wave *n*	The line transceiver you wish to configure, an integer.

Note: For modules with multiple optical lanes, the `n/lane` designation will enable a user to specify a lane. Depending on the system and transceivers used, there may be a number of configurations for lane counts.

Example: CONF# module client 0 / 1 (meaning lane 1 of client 0).

Example

```
localhost CONF# module osc 0
localhost CONF-MOD-OSC[0]# ip address 192.168.0.1/24
localhost CONF-MOD-OSC[0]# exit
Interface OSC 0 address set to 192.168.0.1
localhost CONF# exit
localhost# write memory
Destination has 592738304 bytes (148184576 words) available.
Existing file uses 6144 bytes (1536 words).
Are you sure? [yes/NO] yes
```

2.3.4 switch

Places the DarkStar system in switch configuration mode. Click `switch` to see the section describing this functionality.

2.4 do

Executes any enable mode command (most often the `show` command). From the `CONF#` prompt, precede the command with `do`. For example, `do show time`. See Table 5-1 for more information.

`CONF#` **do show environment**

2.5 end

Exits configuration mode and returns to the top level.

Syntax

`CONF#` **end**

2.6 exit

When issued from a CONF sub-mode (e.g., CONF-MOD-OSC[0]), `exit` moves the prompt to configure mode (CONF). When issued from configure mode (CONF), `exit` moves the prompt to enable mode (#).

When issued on the console (CTY) in enable mode (#), `exit` will log out the user. On CTY, the disable prompt (>) will be presented again. **Note:** If a console password has been set, you must enter a password to return to the disable mode (>) prompt. When issued from a Telnet or SSH connection, from either enable mode (#) or disable mode (>), `exit` will disconnect any Telnet or SSH session and release the VTY line for use by others.

logout *also disconnects Telnet or SSH sessions and releases the line.*

Syntax

`>` **exit**
`#` **exit**
`CONF#` **exit**

Example

```
localhost CONF-MOD-OSC[0]# exit
CONF# exit
localhost# exit
Logging out. Good bye.
localhost>
```

2.7 logout

When issued from a Telnet or SSH connection at the disable (`>`) or enable (`#`) mode, the `logout` command disconnects any Telnet or SSH session, and releases the VTY line for use by others. When performed on the console (CTY), `logout` resets the console line. If a console password has been set, you must enter a password to return to the disable mode prompt.

Typing exit at the enable or disable prompt does the same thing.

Syntax

`>` **logout**

`#` **logout**

2.8 no

Reverses the action of the specified command, in any mode. For example, `no terminal pager` or `no shutdown`.

Syntax

`>` **no** [terminal pager]

`#` **no** [command to be reversed]

`CONF#` **no** [command to be reversed]

2.9 delete

Deletes the specified file from the file system, if the file is not read only.

Do not attempt to delete any files under the following directories. They contain important system data required for proper system operation:

- **/dxmos**
- **/dxmos/sysdesc**
- **/boot**
- **/gateware**

Syntax

`#` **delete** *filename*

Parameters

filename	The file to be deleted.

2.10 directory

Provides a directory listing for the specified file or directory. If no argument is present, it provides a listing of the root directory. **Note:** The `terminal pager` command sets the number of output lines per page.

Syntax

`#` **directory** [*directory*|*filename*]

Parameters

directory	The desired directory.
filename	The filename must be a full path. For example, dxmos/dxmos.exe or /dxmos/dxmos.exe, but not dxmos.exe.

2.11 more

Displays the contents of the specified regular file, a page at a time. Use the `directory` command to list directories and files in the file system. The `more` command does not display the contents of executable files.

- *The terminal pager command enables the setting of lines per page for console output.*
- *The `more` command will paginate (i.e., wait for the user to press the space bar every n lines) if the terminal pager command is set to a non-zero value. By default, the terminal paginate value is zero, so no pagination occurs unless configured by the user. If pagination is ON (non-zero value), the output may also be halted by pressing control-C.*

Syntax

more *file-path*

Parameters

file-path	The filename must be a full path. For example, dxmos/config.dat or /dxmos/config.dat, but not config.dat.

2.12 version

Displays the version of the currently loaded DXMOS software. See also show version.

Syntax

> **version** [verbose]

version [verbose]

3

DarkStar System & Configuration Settings

System settings are those settings that affect the DarkStar itself, such as amplifiers, the location of the boot file, the system host name, message of the day, terminal display behavior, and others.

Amplifiers

- amplifier control automatic
- Amplifier-Label Keywords
- show amplifier
- show running-config amplifier

Controls for Individual Amplifiers

- control automatic channel-count
- control manually-set
- shutdown
- no shutdown

General Settings

- banner motd
- boot
- boot host dhcp
- clock
- connect
- copy
- description
- encapsulation
- fan
- hostname
- idle-mute
- protection
- sntp
- switch
- terminal pager
- tftp
- tune
- tune-for-dmd
- write

3.1 Amplifiers

This section includes the following:

- amplifier control automatic
- Amplifier-Label Keywords
- show amplifier
- show running-config amplifier

The `amplifier` *command set is only available on DarkStar systems with an amplifier installed.*

3.1.1 amplifier control automatic

Configures all EDFAs automatically, based on the user-provided channel count. The user must set this channel-count in order for the EDFAs to be set correctly. DarkStar systems use DXMOS-recommended settings to control the amplifier by automatically adjusting gain or power as necessary. The `channel-count` argument is needed to complete the command.

Reminder: Each amplifier in the DLA & DMD-A is shut down by default, so be sure to run the `no shutdown` command to turn on the respective pump lasers.

Caution: Setting the channel count to a value higher than the actual number of DWDM channels in the fiber will cause each channel to be at a higher power level than the desired target power per channel. This can result in degraded signal quality or even transceiver receiver damage.

Syntax

`CONF#` **amplifier control automatic channel-count {***n***} [***power-per-channel in dBm***]**

Parameters

channel-count *n*	Channel-count integer values range from 1– 96.
power-per-channel in dBm	Sets the optical power per channel in dBm as a decimal value (i.e., nn.n). If not supplied, the factory default power-per-channel will be used, +3.0 dBm.

Example

```
localhost> enable
localhost# configure
localhost CONF# amplifier control automatic channel-count 12 3.0
localhost CONF# amplifier east output edfa
localhost CONF-AMP [east output edfa]# no shutdown
localhost CONF-AMP [east output edfa]# exit
localhost CONF#
```

3.1.2 Amplifier-Label Keywords

Amplifier commands use amplifier-label keywords to specify a particular amplifier. These amplifier-label keywords can be part of an amplifier-specific command prompt or issued from a particular mode (e.g., `>`), depending on the task.

Syntax

`CONF-AMP[amplifier-label]#`

`>` **show amplifier** [amplifier-label]

As the syntax lines above indicate, you can use an amplifier-label keyword to specify an amplifier within a command. Shown below is the `show amplifier` command, issued from the `>` mode, for the "east output edfa" system.

Example

`>` **show amplifier east output edfa**

For details on using the `show amplifier` command with amplifier-labels, see the beginning of the show amplifier section.

While the `show amplifier` and `show running-config amplifier` commands are available from multiple modes, the `CONF-AMP[amplifier-label]#` prompt is required for issuing the other amplifier commands, such as `shutdown` or `no shutdown`.

For instance, from the `CONF#` mode, when you specify a particular amplifier with the *amplifier-label*, the corresponding prompt will change, as shown in Table 3-1.

TABLE 3-1. Amplifier command prompts

amplifier-label	Prompt Changes To...
input raman	`CONF-AMP[input raman]#`
input edfa	`CONF-AMP[input edfa]#`
output edfa	`CONF-AMP[output edfa]#`
east input raman	`CONF-AMP[east input raman]#`
east input edfa	`CONF-AMP[east input edfa]#`
east output edfa	`CONF-AMP[east output edfa]#`
west input raman	`CONF-AMP[west input raman]#`
west input edfa	`CONF-AMP[west input edfa]#`
west output edfa	`CONF-AMP[west output edfa]#`

Note: The amplifier control automatic command, used to automatically set the channel-count for all EDFAs, does not accept amplifier-label keywords.

3.1.3 show amplifier

Displays status of amplifiers, settings, and alarms.

	The `show amplifier` *command is only available on DarkStar systems with an amplifier installed.*

Syntax

`>` **show amplifier** [amplifier-label|summary|all]
`#` **show amplifier** [amplifier-label|summary|all]
`CONF#` **do show amplifier** [amplifier-label|summary|all]

Parameters

amplifier-label	Specifies the amplifier for which to display information. If no parameter is specified, a summary, as described next, is provided. For more details, see Amplifier-Label Keywords.
summary	Displays a brief report of amplifier statistics.
all	Displays detailed information for all amplifiers in the system.

The output below is for a typically configured system. The “Control mode” in the output indicates how the EDFA was configured. Here, it appears as “Automatic (APC).”

For an EDFA configured with the `control manually-set power` command, the “Control mode” would appear as “Manually-set (APC).” For an EDFA configured with the `control manually-set gain` command, the “Control mode” would appear as “Manually-set (AGC).”

Also in the output below, the "Setpoint" displays the EDFA target output power, which is controlled by DXMOS. In this example, the setpoint is determined by the number of DWDM channels in the fiber. This is because the `amplifier control automatic channel-count 12` command was issued.

When configured with the `control manually-set power` or the `control manually-set gain` commands, the "Setpoint" displays the EDFA target optical output power. However, "Total output power" may not be the same as "Setpoint.” One reason for this possible discrepancy is that if there is no input optical power, then the EDFA will be automatically shutdown, and the Setpoint will not be reached.

Example

```
localhost> show amplifier all
Detailed information for Amplifier Input EDFA
  Module is administratively up
  Module Status
    State ................. Up
    Control mode ........... Automatic (APC)
    Channel-count .......... 12
    Setpoint ..............    5.7 dBm
    Case temperature .......   34.3 C
  Pump Status
    Pump bias current ......   81.3 mA (Up)
    Pump EOL bias current ..  960.0 mA
    Pump temperature .......   25.0 C
  Signal Levels
    Input power ............  -12.7 dBm
    Total output power .....    5.7 dBm
    Signal output power ....    5.5 dBm
    Signal gain ............   18.2 dB
  Alarms
     None
  Module Identification
    Role ................... Pre-amplifier
    Path ................... Line input to Channel outputs

Detailed information for Amplifier Output EDFA (BKTel 20dBm)
  Module is administratively up
  Module Status
    State ................. Up
    Control mode ........... Automatic (APC)
    Channel-count .......... 12
    Tx Power/Channel ...........8.0 dBm
    Setpoint ..............   20.0 dBm
    Case temperature .......   35.3 C
  Pump Status
    Pump bias current ......  733.5 mA (Up)
    Pump EOL bias current .. 1038.0 mA
    Pump temperature .......   25.0 C
  Signal Levels
    Input power ............    2.8 dBm
    Total output power .....   19.9 dBm
    Signal output power ....   20.0 dBm
    Signal gain ............   17.1 dB
  Alarms
     None
  Module Identification
    Role ................... Booster
    Path ................... Channel inputs to Line output
```

Tip: As an alternative to the `show amplifier all` command, the `show amplifier summary` command summarizes amplifier information in an easy-to-read, column format, as shown in the example below.

Example

```
localhost> show amplifier summary

                                        Admin  Ctrl   Control   RxPow   TxPow   Module
Amplifier                 Role          State  Mode   Setpoint  (dBm)   (dBm)   State
-----------------------   -------       -----  ----   --------- ------  ------  -------
             Input EDFA    Preamp         Up    APC    5.7 dBm   -12.7    5.7      Up
            Output EDFA   Booster         Up    APC   20.0 dBm    2.8    20.0      Up
```

Note: The "Ctrl Mode" column indicates only the associated mode acronym (e.g., APC) and not the full description—"Automatic (APC)" or "Manually-set (APC)" — as would the `show amplifier all` command.

3.1.4 show running-config amplifier

Displays the settings of amplifiers.

	The `show running-config amplifier` *command is only available on DarkStar systems with an amplifier installed.*

Syntax

`#` **show running-config amplifier**
`CONF#` **do show running-config amplifier** [amplifier-label]

Parameters

amplifier-label	Specifies which amplifier to display information. If no parameter is specified, information is displayed for all amplifiers.

Example

```
localhost CONF-AMP[input edfa]# do show running-config amplifier
running-config:
amplifier input edfa
shutdown
control automatic channel-count 12
exit
amplifier output edfa
description EDFA 20dBm
shutdown
control automatic channel-count 12
exit
```

Note: In the output above, the amplifier-label `input edfa` was used. For more information on amplifier-labels, see Amplifier-Label Keywords.

3.2 Controls for Individual Amplifiers

Available commands:

- control automatic channel-count
- control manually-set
- shutdown
- no shutdown
- los-shutdown
- no los-shutdown

3.2.1 control automatic channel-count

Configures the EDFAs individually, based on the user-provided channel count. The user must set this channel-count in order for the EDFAs to be set correctly. This command is for diagnostic purposes or advanced users, and not commonly used; the `amplifier control automatic` command is used instead.

Caution: Setting the channel count to a value higher than the actual number of DWDM channels in the fiber will cause each channel to be at a higher power level than the desired target power per channel. This can result in degraded signal quality or even transceiver receiver damage.

Syntax

`CONF-AMP[amplifier-label]#` **control automatic channel-count** **{***n***}** **[***power-per-channel in dBm]*

Parameters

channel-count *n*	Channel-count integer values range from 1– 96.
power-per-channel in dBm	Sets the optical power per channel in dBm as a decimal value (i.e., nn.n). If not supplied, the factory default power-per-channel will be used, +3.0dBm.

Example

```
localhost> enable
localhost# configure
localhost CONF# amplifier east output edfa
localhost CONF-AMP[east output edfa]# control automatic channel-count 12 3.0
localhost CONF-AMP[east output edfa]# exit
localhost CONF#
```

3.2.2 control manually-set

These commands individually control each EDFA and Raman in a system. Included are the `control manually-set gain (only EDFA)` and `control manually-set power` commands.

Only one amplifier control command is in effect at any time.

After running the `control manually-set` command(s), run the appropriate `show` command and verify that

the new configuration value is displayed.

3.2.2.1 control manually-set gain

Sets the DarkStar EDFA to Automatic Gain Control mode, or AGC. The user specifies the desired output gain (in dB) as a set point for controlling the amplifier. To maintain constant gain, the amplifier will do the following:

- If input power drops: drop output power and vary pump current as needed.
- If input power increases: increase output power and vary pump current as needed.

Syntax

`CONF-AMP[amplifier-label]#` **control manually-set gain** *gain-in-dB*

Parameters

gain-in-dB	Sets control point in dB as a decimal value (i.e., *nn.n*). Valid range of values is 17.0-29.0.

The example below comes from a system with an "east input edfa." Here, a gain value of 17.0 dB was entered using the `control manually-set gain` command.

The "Control mode" in the output indicates that the EDFA was configured as "Manually-set (AGC)." The "Setpoint" displays the EDFA target optical gain, 17.0 dB. Note that "Total output power" may not be the same as "Setpoint." One reason for this possible discrepancy is that if there is no input optical power, then the EDFA will be automatically shutdown, and the Setpoint will not be reached.

Example

`CONF-AMP[east input edfa]#` **do show amplifier east input edfa**

```
Detailed information for Amplifier East Input EDFA (20dBm East)
  Module is administratively down
  Module Status
    State ................. LOS
    Control mode ........... Manually-set (AGC)
    Channel-count .......... N/A
    Setpoint ..............   17.0 dB
    Case temperature .......   22.9 C
  Pump Status
    Pump bias current ......    0.3 mA (Disabled)
    Pump EOL bias current ..  898.7 mA
    Pump temperature .......   25.0 C
  Signal Levels
    Input power ............ ~-50.1 dBm
    Total output power .....   -inf dBm
    Signal output power ....   -inf dBm
    Signal gain ............    0.0 dB
  Alarms
    LOS/Loss of signal
  Module Identification
    Role ................... Pre-amplifier
    Path ................... East line input to East channel outputs
```

Notes: From the amplifier-labeled command prompt (above), you can also issue the `do show amplifier all` and `do show amplifier summary` commands. See the Amplifier-Label Keywords section for more about amplifier-specific command prompts, and the show amplifier section for more about these related commands. Also, in the output above, the `East Input EDFA` was labeled `20dBm East` by using the description command.

3.2.2.2 control manually-set power

Sets the DarkStar EDFA and Raman to Automatic Power Control mode, or APC. The user specifies the desired output power (in dBm) as a set point for controlling the amplifier. To maintain constant power, the amplifier will do the following:

- If input power drops: increase pump power as needed.
- If input power increases: reduce pump power as needed.

Syntax

`CONF-AMP[amplifier-label]#` **control manually-set power** *power-in-dBm* | *power-in-mW*

Parameters

power-in-dBm	EDFA: Sets control point in dBm as a decimal value (i.e., *nn.n*)
power-in-mW	Raman: Valid range of values depends on system configuration

The example below comes from a system with an "east input edfa." Here, a power value of -10.0 dBm was entered for the `control manually-set power` command.

The "Control mode" in the output indicates that the EDFA was configured as "Manually-set (APC)." The "Setpoint" displays the EDFA target optical power, -10.0 dBm. Note that "Total output power" may not be the same as "Setpoint." One reason for this possible discrepancy is that if there is no input optical power, then the EDFA will automatically be shutdown, and the Setpoint will not be reached.

Example

`CONF-AMP[east input edfa]#` **do show amplifier east input edfa**

```
Detailed information for Amplifier East Input EDFA (20dBm East)
  Module is administratively down
  Module Status
    State ................... LOS
    Control mode ............ Manually-set (APC)
    Channel-count ........... N/A
    Setpoint ..............   -10.0 dBm
    Case temperature .......    23.2 C
  Pump Status
    Pump bias current ......     0.0 mA (Disabled)
    Pump EOL bias current ..   898.7 mA
    Pump temperature .......    25.0 C
  Signal Levels
    Input power ............ ~-50.5 dBm
    Total output power .....    -inf dBm
    Signal output power ....    -inf dBm
    Signal gain ............     0.0 dB
  Alarms
    LOS/Loss of signal
```

```
Module Identification
  Role ..................... Pre-amplifier
  Path ..................... East line input to East channel outputs
```

Notes: From the amplifier-labeled command prompt (above), you can also issue the `do show amplifier all` and `do show amplifier summary` commands. See the Amplifier-Label Keywords section for more about amplifier-specific command prompts, and the show amplifier section for more about these related commands. Also, in the output above, the `East Input EDFA` was labeled `20dBm East` by using the description command.

3.2.3 shutdown

Disables the amplifier by turning off the specified EDFA and Raman pump.

	Be very careful when using this command. Shutting down an amplifier can disrupt customer traffic.

Syntax

`CONF-AMP[amplifier-label]#` **shutdown**

3.2.4 no shutdown

Enables the amplifier by turning on the specified EDFA and Raman pump.

Note: On the DMD-A or DLA, the EDFA and Raman pump will remain disabled (i.e., the XKL factory default) until an automatic channel count or a manually-set power/gain is configured. So before issuing the `no shutdown` command to enable the EDFA pump, issue either the `control automatic channel-count` command, as described in section 3.2.1 or a `control manually-set` command (for `gain` or `power`), as described in section 3.2.2.

Syntax

`CONF-AMP[amplifier-label]#` **no shutdown**

Parameters

no	Enable the amplifier. This is the default setting.

```
localhost# configure
localhost CONF# amplifier input edfa
localhost CONF-AMP[input edfa]# no shutdown
localhost CONF-AMP[input edfa]# exit
localhost CONF# amplifier output edfa
localhost CONF-AMP[output edfa]# no shutdown
localhost CONF-AMP[output edfa]# exit
localhost CONF# exit
localhost#
```

3.2.5 los-shutdown

Enables the amplifier auto-shutdown feature when Loss of Signal occurs. This is the default setting.

Example

```
CONF-AMP[amplifier-label]# los-shutdown
localhost# configure
localhost CONF# amplifier west input raman
localhost CONF-AMP[west input raman]# los-shutdown

West Input Raman: Shutdown due to LOS is enabled.
localhost CONF-AMP[west input raman]# exit
localhost CONF# exit
localhost#
```

3.2.6 no los-shutdown

Disables the amplifier auto-shutdown feature when Loss of Signal occurs.

Syntax

```
CONF-AMP[amplifier-label]# no los-shutdown
```

3.3 General Settings

Available commands:

- app switch
- banner motd
- boot
- boot host dhcp
- clock
- connect
- copy
- description
- encapsulation
- fan
- hostname
- idle-mute
- protection
- sntp
- switch
- terminal pager
- tftp
- tune
- tune-for-dmd
- write

3.3.1 app switch

Switches an automatic path protection (APP) group to a particular interface within the group.

Syntax

`#` **app switch wave {east transport interface number 1|west transport interface number 2}**[force]

Parameters

transport interface number 1	Specifies by interface the APP group to switch.
transport interface number 2	Specifies the target interface.
force	Overrides a locked APP group.

3.3.2 banner motd

Adds or removes a message that displays on the console at login.

Syntax

`CONF#` [no] **banner motd** *delimiter message delimiter*

Parameters

delimiter	Delimits the displayed message. Delimiter value may be any ASCII character not used in the message, but the same delimiter value must be included at the beginning and end of the message.
message	The message text to display at login. Can be multiple lines of plain text.
no	Removes the display message.

3.3.3 boot

The Boot program loads an executable file from either a flash memory or a TFTP location. The Boot program reads the startup-config file to obtain specifications of what to load. (Absent directions, Boot uses a default, "file /dxmos/dxmos.exe.")

This command modifies the boot settings in the running-config by adding or removing entries from a list of file descriptions. To take effect during subsequent reloads, boot settings must be saved in the `startup-config` location.

DXMOS initialization reads a config file from disk. The disk file is called the startup-config.

The running-config contains the config settings from the startup-config currently in memory. If a user makes a configuration setting (i.e., option) change, the running-config will differ from the startup-config. However, when the user issues the "write memory" command, the changes are saved to the startup-config. DXMOS initialization copies startup-config to running-config.

If a user does not issue the "write memory" command to save running-config changes, these changes will be lost, and the existing startup-config on the system disk will remain unchanged.

Note: write memory *writes to the* `startup-config` *location by default.*

If multiple boot locations are specified, the Boot program tries them in the order in which they are specified. Setting multiple boot locations provides a fallback in case the boot image in one location is missing or damaged.

Syntax

`CONF#` [no] **boot file** *executable-file*

`CONF#` [no] **boot tftp** *ip-address filename*

Parameters

file *executable-file*	The system boots with the config.dat file in the system flash memory. This file is also referred to as the startup config file. The executable file must be a full path, such as dxmos/dxmos.exe or /dxmos/dxmos.exe.
tftp *ip-address filename*	The system boots from a file located at *ip-address filename*.
ip-address *filename*	IPv4 or IPv6 address or hostname. The filename must specify the host-specific path to the executable file.
no	Removes the specified boot target.

3.3.4 boot host dhcp

Directs Boot to acquire a configuration file from a remote Dynamic Host Configuration Protocol (DHCP) server, via TFTP. If DHCP identifies a boot file name and TFTP server, Boot acquires the file, and loads DXMOS with that configuration. DHCP configuration is also initiated when no configuration file (`dxmos/config.dat`) is present in flash memory. **Note:** When `boot host dhcp` is present in startup-config, it has precedence over any `boot file` or `boot tftp` commands. The `boot host dchp` command may be useful to provide an initial configuration file when a system is first installed. Thereafter, you should write a new startup-config to reflect customization specific to the individual system.

The remote configuration file must already exist (on the designated TFTP server), and a DHCP server must already be configured to provide a TFTP server host name and boot file name (DHCP options 66 and 67).

Note the following:

- If Boot receives no DHCP offer after 2 minutes, Boot loads DXMOS with the local configuration file (`dxmos/config.dat`). If no local configuration file is present, Boot loads DXMOS without a configuration.
- The DarkStar system includes a DHCP client identifier in its DHCP discovery request.
- On `reload`, directs the Boot program to acquire a configuration file remotely via DHCP.
- For DHCPv4, the DHCP client identifier is "01:" followed by an interface MAC address. For example, an active interface with the MAC address 00:A0:E3:00:01:A8 will have a DHCPv4 client identifier of 01:00:A0:E3:00:01:A8.
- For DHCPv6, the DHCP client identifier is a DUID-EN identifier (see RFC 3315) consisting of an XKL vendor identifier "00:02:00:00:52:9e:" followed by the system (ETH 0) MAC address. For example, a DarkStar system with the system MAC address 00:a0:e3:00:03:46 will have a DHCPv6 client identifier of 00:02:00:00:52:9e:00:a0:e3:00:03:46
- MAC addresses for Ethernet and OSC interfaces are pre-assigned at the factory. You can determine the MAC address for an interface using the command `show interface ethernet` *n*. For Ethernet interfaces 0 through 3, *n*=0, 1, 2, or 3. For OSC 0 through 3, *n*=4, 5, 6, or 7. **Note:** On a CMD system, the Ethernet interfaces 1,2,3 do not exist. To determine if the system is CMD-based, issue the `show hardware` command.

Syntax

`CONF#` [no] **boot host dhcp** [ethernet *n*|osc *n*]

Parameters

ethernet *n*	The Ethernet management interface the system is to use when generating the DHCPv4 client identifier, regardless of which interface makes contact with a server.
osc *n*	The OSC management interface the system is to use when generating the DHCPv4 client identifier, regardless of which interface makes contact with a server.
no	Disables boot host dhcp.

3.3.5 clock

Depending on the mode, the clock command sets two different aspects of the system clock.

- Enable mode: Sets the system time and date.
- Configure mode: Sets the time zone and Daylight Saving Time behavior.

Note: Use `show clock` to display the currently set time and date.

3.3.5.1 clock (enable mode)

Sets the time and date of the DarkStar system clock.

	The system time is in local time, as defined by the current `timezone` and `summer-time` settings (which are set in `configure` mode). If your time zone observes DST, and you are setting the time close to the spring or fall transition, turn off `summer-time` (`configure` mode), set the clock (`enable` mode), then turn on `summer-time` (`configure` mode).

Syntax

`#` **clock set** *`hh:mm:ss day month year`*

`#` **clock {read-calendar|update-calendar}**

Parameters

set *`hh:mm:ss day month year`*	Sets the time for the system clock to the specified time and date.
read-calendar	Copies the time from the calendar chip to the system clock.
update-calendar	Copies the time from the system clock to the calendar chip.

3.3.5.2 clock (configure mode)

Sets the timezone and Daylight Saving Time (DST) behavior of the DarkStar system clock relative to Coordinated Universal time, or UTC. This is not to be confused with the `clock` command in enable mode, which is used to set the time.

	Time zones west of Greenwich time have a negative offset from Greenwich time.

Syntax

`CONF#` **clock timezone** *hrs-offset mins-offset*

`CONF#` **clock summer-time {on|off|usa|eu}**

Parameters

timezone *hrs-offset mins-offset*	Sets the time zone for the system clock to hour-offset and minutes-offset from UTC. For example, United States Pacific time has an hour-offset of -8 (UTC-8). Most time zones have a minutes-offset of 0.
summer-time on|off	`on` displays time with a forward offset of one hour from the system clock time; `off` displays with no adjustment.
summer-time usa|eu	`usa` applies DST rules for the United States; `eu` applies DST rules for the European Union.

3.3.6 connect

Creates a circuit between a client/wave interface and another client/wave interface of the same encapsulation type (e.g., 10gigabitethernet). An interface may be connected to itself, or looped back for testing purposes.

Syntax

`CONF#` [no] **connect** module *n* module *m* **encapsulation** encapsulation-type

Parameters

module *n*	**client** *n* or **wave** *n*
module *m*	**client** *m* or **wave** *m*

encapsulation encapsulation-type	Encapsulation type, which sets the appropriate clock rate.
	Options are:
	`gigabitethernet`
	`10gigabitethernet [fec]`
	`fibrechannel {1g|2g|4g|8g|10g}`
	`sonet {oc48|oc192|oc192 fec}`

no **connect** module *n* module *m*	Disconnect the two specified interfaces.

3.3.7 copy

Copies configuration data, software images, and gateware images to either a new or existing file. This command does not copy folders or directories.

- **If you attempt to overwrite an executable file with a data file, or vice versa, you will see a warning that the two files are of different modes. You will be prompted to confirm your decision before the file overwrite begins.**
- **Before using copy to install a new `dxmos/config.dat` file, be sure the enable password in the new file is known or empty. The system must be reloaded after installing a new dxmos/config.dat file to make the new configuration effective. Beware that a write memory command will overwrite the new file with the running configuration.**

Syntax

`#` **copy** *source-storage-location destination-storage-location*

Parameters

source-storage-location	Specifies the file to be copied, the original file. Must be a full absolute path. The filename should be a path: local paths are relative to the directory root and remote file paths are relative to the TFTP server root. Paths may include a leading forward slash (/). For example, */dxmos/dxmos.exe* and *dxmos/dxmos.exe* refer to the same file, but not *dxmos.exe*.
destination-storage-location	Specifies the target location for the copied file. Must be a full absolute path. The path is interpreted relative to the file system root and may include a leading forward slash (/).

3.3.8 description

Creates a site-configurable label to describe the use of amplifiers and transceivers.

On DQM and DQT systems, the `description` *command is only available for trunks and specific client lanes; the* `description` *command is not available as a configuration command for an entire QSFP+ client transceiver.*

Note: For modules with multiple optical lanes, the `n/lane` keyword will enable a user to specify a lane. Depending on the system and transceivers used, there may be a number of configurations for lane counts.
Example: `CONF-MOD-CLIENT[0/1]# description`

Syntax

`CONF-MOD-CLIENT[n]#` [no] **description** *string*
`CONF-MOD-WAVE[n]#` [no] **description** *string*
`CONF-AMP[amplifier-label]#` [no] **description** *string*

Parameters

string	Label for the module.
no	Removes the label from the module.

3.3.9 encapsulation

Configures the interface encapsulation type, which determines the data rate of an interface. Encapsulation options are system dependent. Also see "Available Protocols, Data Rates and Corresponding Encapsulation" in the Systems Guide on the XKL website.

	If an interface is carrying customer traffic, changing the encapsulation will interrupt that traffic.

Syntax

`CONF-MOD-CLIENT[n]#` **encapsulation** encapsulation-type

`CONF-MOD-WAVE[n]#` **encapsulation** encapsulation-type

encapsulation-type	System-dependent encapsulation types, which set the appropriate clock rate or data framing:
	`gigabitethernet`
	`10gigabitethernet [fec]`
	`fibrechannel {1g|2g|4g|8g|10g}`
	`sonet {oc48|oc192|oc192 fec}`
	`1xCAUI-4`
	`2xCAUI-4`
	`4x100GAUI-2`
	`4x100GAUI-2_ZR`
	`400GAUI-8`
	`400GAUI-8_ZR`

Note: For modules with multiple optical lanes, the `n/lane` keyword will enable a user to specify a lane. Depending on the system and transceivers used, there may be a number of configurations for lane counts.
Example: `CONF-MOD-CLIENT[0/1]# encapsulation`

The following example shows how to specify an encapsulation type for a client. **Note:** Available encapsulation types will depend on your system. For this particular product, a DQT400 series, setting an encapsulation type for a client will result in the same encapsulation type being set for the corresponding wave.

Example

```
CONF# module client 0
CONF-MOD-CLIENT[0/*]# encapsulation 1xCAUI-4
Client 0 encapsulation set to 1xCAUI-4
Wave 0 encapsulation set to 1xCAUI-4
CONF-MOD-CLIENT[0/*]#
```

The following example confirms the encapsulation type for a client 0.

```
CONF-MOD-CLIENT[0/*]# do show modules client 0

Client 0    Up
  Description: .... Seattle_to_Redmond
  Temperature: .... 28 C                        Vendor: ...... OPLINK
  Part No.: ....... QTA1C04L2C000E1A            Serial No.: .. Z201709HX
  Module Type: .... QSFP28                      MFG Date: .... 200422
  Connector: ...... LC                          Channel: ..... N/A
  Wavelength: ..... 1302.35 nm                  Frequency: ... 230193 GHz
  Encapsulation: .. 1xCAUI-4

Client 0/0    Up
  Description: .... Seattle_to_Redmond
  Tx: ............. OK                           Rx: .......... OK
  State Changed: .. 00d 15:42:39                Tx Laser: .... Enabled
  Tx Power: ....... 1.0 dBm                     Rx Power: .... -3.9 dBm
  Loopback: ....... Not Supported               Rate: ........ 25Gb/s
  Last Cleared: ... unknown                     Link Downtime: 00d 00:00:00


Client 0/1    Up
  Description: .... Seattle_to_Redmond
  Tx: ............. OK                           Rx: .......... OK
  State Changed: .. 00d 15:42:40                Tx Laser: .... Enabled
  Tx Power: ....... 1.5 dBm                     Rx Power: .... -3.5 dBm
  Loopback: ....... Not Supported               Rate: ........ 25Gb/s
  Last Cleared: ... unknown                     Link Downtime: 00d 00:00:00


Client 0/2    Up
  Description: .... Seattle_to_Redmond
  Tx: ............. OK                           Rx: .......... OK
  State Changed: .. 00d 15:42:40                Tx Laser: .... Enabled
  Tx Power: ....... 1.9 dBm                     Rx Power: .... -3.4 dBm
  Loopback: ....... Not Supported               Rate: ........ 25Gb/s
  Last Cleared: ... unknown                     Link Downtime: 00d 00:00:00


Client 0/3    Up
  Description: .... Seattle_to_Redmond
  Tx: ............. OK                           Rx: .......... OK
  State Changed: .. 00d 15:42:40                Tx Laser: .... Enabled
  Tx Power: ....... 2.1 dBm                     Rx Power: .... -2.8 dBm
  Loopback: ....... Not Supported               Rate: ........ 25Gb/s
  Last Cleared: ... unknown                     Link Downtime: 00d 00:00:00
```

The following example shows how to use the `connect` command.

Example

```
# configure
CONF# connect client 0 / 0 wave 1 encapsulation 10gigabitethernet
Switch Connect: Connection successful (Client 0/0, Wave 1)
CONF# do show connections
10G Switch Complex connections:
Idx   If1          If2          Channel   If1 Line / Rate     If2 Line / Rate
---   ----------- ----------   -------   ---------------     ----------------
0     Client 0/0   Wave 1       21.0      Up      /10GE       Up      /10GE
```

3.3.10 fan

Places the DarkStar system in fan configuration mode. As viewed from the rear, fan modules are numbered from left to right, 0-2. Some systems have 2 fans in positions 0 and 2. Other systems have 3 fans in positions 0, 1, and 2.

	For more information about viewing fan module information, see show environment.

The command prompt changes to `CONF-FAN[n]#`. Available command is speed.

Syntax

`CONF#` **fan** *fan-module-number*

Parameters

fan-module-number	Opens configuration mode for the fan module to be configured: 0, 1, or 2.

Example

```
# configure
CONF# fan 0
CONF-FAN[0]# speed med
CONF-FAN[0]# exit
CONF# fan 1
CONF-FAN[1]# speed med
CONF-FAN[1]# exit
CONF# fan 2
CONF-FAN[2]# speed med
CONF-FAN[2]# exit
```

3.3.10.1 speed

Sets fan speed. Changing the fan speed to anything other than `auto` disables the automatic fan control for that fan. It is strongly recommended to use the `auto` setting and let the system control the fan speed.

Setting a fixed fan speed will disable automatic fan control. This may result in the system running at abnormally high temperatures.

Syntax

`CONF-FAN[n]#` **speed {auto|high|low|med|***percent-value***}**

Parameters

auto	Sets the fans to automatically adjust their speed. This setting is the default.
high	Sets the fans to the highest possible speed.
low	Sets the fans to the lowest possible speed.
med	Sets the fans to medium speed.
percent-value	Sets the fans to a percentage of their operating speed range, from 1 to 100. 1 = low, 100 = high, 50 = med.

Example

```
localhost# configure

localhost CONF# fan 0
localhost CONF-FAN[0]# speed high
Warning! Operating the fan speeds in manual mode disables automatic fan
control and may result in irreversible damage to the system.

Are you sure? [yes/NO] yes
localhost CONF-FAN[0]# exit
localhost CONF# fan 2
localhost CONF-FAN[2]# speed high
Warning! Operating the fan speeds in manual mode disables automatic fan
control and may result in irreversible damage to the system.
localhost CONF-FAN[2]# exit
```

3.3.11 hostname

Sets the host name for the DarkStar system, as well as the CLI prompt. The default host name for the system is `localhost`.

Syntax

`CONF#` **hostname** *name*

Parameters

name	A string; the DarkStar system name.

Example

```
localhost CONF# hostname newname
newname CONF# exit
newname#
```

3.3.12 idle-mute

Enables and disables the transceiver's optical transmission of PRBS signals during signal error conditions.

When a client interface detects a signal error condition, and idle-mute is enabled, the transmitter of the interface is shut down. Conversely, when a client interface detects a signal error condition, and idle-mute is disabled, the transmitter is not shut down and the interface transmits a PRBS pattern.

The holdoff time is how long you want to wait to apply idle-mute, in hopes that the signal integrity will be restored. If there is no holdoff (or no holdoff time is specified), the transmitter is instantly disabled. If you specify a holdoff time other than 0, the interface will continue to transmit a PRBS pattern until either:

- Signal quality is restored before the holdoff time has expired. In this case, PRBS generation is stopped and the original signal is allowed to pass through again; or,
- The holdoff time expires, at which time the transmitter is disabled.

By default, idle-mute is enabled for client interfaces and disabled for DWDM wave interfaces. In addition, the default holdoff time is 0 milliseconds.

If you run the `show module` command on a client/wave lane, idle-mute status is also displayed. The status messages are listed in the following table.

TABLE 3-2. Idle-Mute Status Messages

Message	Status
`Off`	Part of a connection and the signal is good. Idle Tx and Idle Mute features are not active in this state.
`Idle Tx`	• Part of a connection that has bad signal data AND `idle-mute` is disabled; OR • Not part of a connection and `idle-mute` is disabled.
`Idle Mute`	• Part of a connection that has bad signal data AND `idle-mute` is enabled; OR • Not part of a connection and `idle-mute` is enabled.
`Idle Tx Pending Mute`	Only seen if `idle-mute` is enabled with a non-zero holdoff time configured and there is a connection with bad data. The transmitter will stay in this status until either the data restores integrity (at which time it transitions back to the `Off` status) or the holdoff time elapses (at which time the transmitter is disabled and the status changes to `Idle Mute`).

Syntax

`CONF-MOD-CLIENT[n]#` [no] **idle-mute** [holdoff *milliseconds*]
`CONF-MOD-WAVE[n]#` [no] **idle-mute** [holdoff *milliseconds*]

Parameters

`holdoff` *`milliseconds`*	The delay, in milliseconds, between the instant an interface detects a signal error condition and the instant the transmitter is shutdown. This delay helps alleviate situations where interfaces cycle frequently between up and down states. Values can be between 0 and 100000.
`no idle-mute`	Disables idle-mute.

Example

```
CONF# do show running-config
running-config:
;;;;;;;;
...
exit
module client 0
idle-mute holdoff 100
...
exit
module client 1
idle-mute holdoff 100
...
exit
module client 2
idle-mute holdoff 100
...
exit
...
```

3.3.13 protection

Disables or enables the Optical Path Protection (OPS) feature, involving a primary and backup path. When enabled, the DarkStar system will switch from using the primary path (Line A on front panel) to the backup path (Line B on front panel) when the primary path OSC detects a Loss of Signal alarm (OSC 0). Data is transmitted using that backup path until a `protection disable` or `clear protection` command is issued. See Table 3-3 for protection command behavior.

	Protection commands are available only on systems with redundant interfaces.

Protection consists of the following commands:

- protection disable
- clear protection
- show protection

TABLE 3-3. Protection Command Behavior

If the Current Protection State Is...	And the Active Line/Trunk Is...	Command	Result
enabled	backup	`protection disable`	Sets the primary line as active.
enabled	backup	`no protection disable`	Backup line remains active until primary line is restored with `clear protection` command.
disabled	primary, with LOS		Sets the backup line as active.
enabled	backup	`clear protection`	Resets protection to active line. If the active line is down, the backup line is selected.
disabled	either		Nothing happens, since protection is off (disabled). Use the `[no] protection disable` command to turn protection back on.

3.3.13.1 protection disable

Turns off protection, making the primary line always active. If protection is disabled, the system will not switch to the backup line, even if there is a loss of signal. The `[no] protection disable` command turns protection back on.

Syntax

`CONF#` [no] **protection disable**

3.3.13.2 clear protection

Resets the active path to the primary.

If the protection feature detected a problem with the primary path and switched to the backup path, it will continue to use the backup path until the `clear protection` command is issued. A possible reason for switching to the backup path could be a fiber cut or a disconnection of the fiber on the primary path. Once the primary path health has been restored, use the `clear protection` command to resume use of it.

Syntax

`#` **clear protection**

3.3.13.3 show protection

Displays the current status of protection in the system. This includes the currently selected line (Primary or Backup) and whether protection is enabled. Protection is enabled by default.

This is not the same as show running-config `protection`*, which displays the current configuration settings.*

Syntax

`>` **show protection**

Example

```
localhost# show protection

Line Protection Summary:
  Active Line: Primary
  Protection is Enabled
```

3.3.14 sntp

Specifies one or more Simple Network Time Protocol (SNTP) servers for setting the system clock. Use this command to automatically synchronize the system clock with an external SNTP server.

Syntax

`CONF#` [no] **sntp server** *address*

Parameters

address	IP address or hostname of the SNTP server from which the DarkStar system should set its system clock.
no	Clears the specified SNTP server address.

3.3.15 switch

Note: Applies to DQT100 and DQM100 systems only.

Places a DarkStar system into switch mode (i.e., CONF-SWITCH#), where connection paths are configured, including assigning aliases and descriptions for local and remote systems or interfaces. You can also specify a class for a particular connection, for weighted round robin queuing priority.

Using statistical multiplexing, the internal muxponder handles all data coming to and from the optical transceivers. It combines lanes into virtual interfaces, formats data for transmission, interprets received data, labels outgoing frames, and interprets labels on incoming data to send frames to a particular transceiver.

Syntax

`CONF#` **switch**

A typical workflow might be:

1. Specify the alias of the local-vif, the remote-vif, and relevant systems. Aliases can be a more descriptive name that helps simplify output and thereby makes it easier to set up switching.
2. Specify a local-system and its next-hop path.
3. Specify the destinations for any local-vifs you wish to map, and a routing class for each (if desired). DXMOS has four RR (round robin) classes, 0-3. See destination for more information.
4. Validate and commit your changes. This writes them to the configuration file.

There are two categories of switch commands: configuration commands and action commands.

Switch configuration commands include:

- alias local-vif
- alias remote-vif
- alias system id
- local-system
- next-hop system
- destination

Action commands include:

- commit
- compare
- validate
- show switch
- revert-to
- end
- exit

The following examples in Figure 3-1and Figure 3-2 illustrate how switch commands might be used to specify routing for a ring topology.

FIGURE 3-1. Sample ring topology

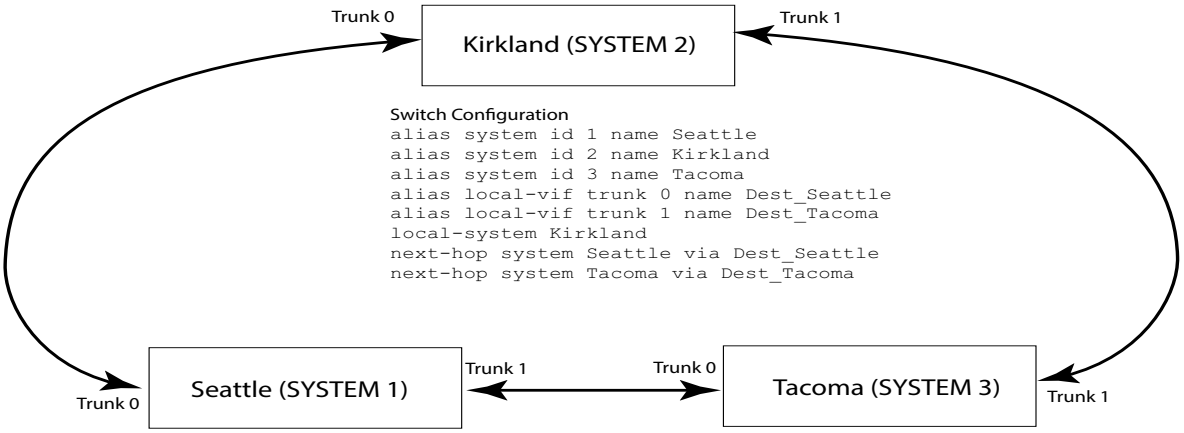
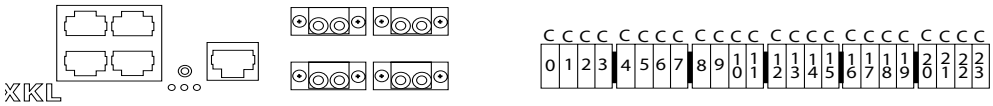


FIGURE 3-2. Switch commands used to specify sample ring topology



Switch Configuration Part 1

```
alias local-vif client 0 name Seattle.c0
alias local-vif client 1 name Seattle.c1
alias local-vif client 2 name Seattle.c2
alias local-vif client 3 name Seattle.c3
alias local-vif client 4 name Seattle.c4
alias local-vif client 5 name Seattle.c5
alias local-vif client 6 name Seattle.c6
alias local-vif client 7 name Seattle.c7
.
.
.
```

Switch Configuration Part 2

```
alias remote-vif Kirkland client 0 name Kirkland.c0
alias remote-vif Kirkland client 1 name Kirkland.c1
alias remote-vif Kirkland client 2 name Kirkland.c2
alias remote-vif Kirkland client 3 name Kirkland.c3
alias remote-vif Kirkland client 4 name Kirkland.c4
alias remote-vif Kirkland client 5 name Kirkland.c5
alias remote-vif Kirkland client 6 name Kirkland.c6
alias remote-vif Kirkland client 7 name Kirkland.c7
.
.
.
```

Switch Configuration Part 3

```
alias remote-vif Tacoma client 0 name Tacoma.c0
alias remote-vif Tacoma client 1 name Tacoma.c1
alias remote-vif Tacoma client 2 name Tacoma.c2
alias remote-vif Tacoma client 3 name Tacoma.c3
alias remote-vif Tacoma client 4 name Tacoma.c4
alias remote-vif Tacoma client 5 name Tacoma.c5
alias remote-vif Tacoma client 6 name Tacoma.c6
alias remote-vif Tacoma client 7 name Tacoma.c7
.
.
.
```

Switch Configuration Part 4

```
destination local-vif Seattle.c0 remote-vif Kirkland.c0
destination local-vif Seattle.c1 remote-vif Kirkland.c1
destination local-vif Seattle.c2 remote-vif Kirkland.c2
destination local-vif Seattle.c3 remote-vif Kirkland.c3
destination local-vif Seattle.c4 remote-vif Kirkland.c4
destination local-vif Seattle.c5 remote-vif Kirkland.c5
destination local-vif Seattle.c6 remote-vif Kirkland.c6
destination local-vif Seattle.c7 remote-vif Kirkland.c7
.
.
.
```

3.3.15.1 alias local-vif

Specifies an optional alias (alternate name) for a local virtual interface. The alias helps users more easily retain and configure interface names.

Syntax

`CONF-SWITCH#` **alias local-vif {client|trunk}** *vif-id* **name** vif-alias [**description** *vif-description*]

`CONF-SWITCH#` **no alias local-vif** [**client|trunk** *vif-id*]

Parameters

client *vif-id*	The `local-vif client` to which you are assigning an alias.
trunk *vif-id*	The `local-vif trunk` to which you are assigning an alias.
name *vif-alias*	The alias you are assigning to the selected `local-vif`.
description *vif-description*	An optional description for the alias you have specified. This can be helpful if the alias needs additional clarity.
no	Removes the alias for the specified local virtual interface from the draft configuration. Note that the `local-vif` is specified using its ID, not its name. The `no alias local-vif` command (without the `client` or `trunk` keyword) will clear all local-vif aliases.

3.3.15.2 alias remote-vif

Specifies an optional alias (alternate name) for a target remote virtual interface. The alias helps users more easily retain and configure interface names. A `remote-vif` alias has three parts: the remote system name, the client name (on the remote system), and the name (alias) being defined. The remote system may be specified by either name or id; the remote client must be specified by id.

Syntax

`CONF-SWITCH#` **alias remote-vif** **{***system-name***|system-id** *system-id***}** **client** *vif-id* **name** *vif-alias* [**description** *vif-description*]

`CONF-SWITCH#` **no alias remote-vif** [*system-name***|system-id** *system-id* **client** *vif-id*]

Parameters

remote-vif *system-name* **remote-vif system-id** *system-id*	The system containing the `remote-vif` to which you are assigning an alias. Can be a name, if you have assigned one using alias system id, or the system's number id in the range [0-63].
client *vif-id*	The `remote-vif client` to which you are assigning an alias.
name *vif-alias*	The alias you are assigning to the specified `remote-vif`.
description *vif-description*	An optional description for the alias you have specified. This can be helpful if the alias needs additional clarity.
no	Removes the alias for the specified remote virtual interface from the draft configuration. Note that the `remote-vif` is specified using the remote system client's ID, not its name. The `no alias remote-vif` command (without the *system name* or `system-id` keyword) will remove all remote-vif aliases.

3.3.15.3 alias system id

Specifies an optional alias (alternate name) for a system id. The alias helps users more easily remember and configure system names.

Syntax

`CONF-SWITCH#` **alias system id** *system-id* **name** *system-name* [**description** *system-description*]

`CONF-SWITCH#` **no alias system id** *system-id*

Parameters

id *system-id*	The ID number [0-63]of the system to which you want to assign an alias.
name *system-name*	The alias you are assigning to the specified system.
description *system-description*	An optional description for the alias you have specified. This can be helpful if the alias needs additional clarity.
no	Removes the alias for the specified system ID from the draft configuration. The `no alias system` command (without `id` keyword) will clear all system aliases.

3.3.15.4 local-system

Specifies the system to be considered the local system in the path you are configuring. The `local-system` name may be specified either by *system-id* or using the alias you created with the `alias system id` command (see alias system id).

A configuration isn't valid until all the system names used in a switch configuration are defined using the `alias system id` *command.*

Syntax

`CONF-SWITCH#` **local-system {***system-name***|id** *system-id***}**

`CONF-SWITCH#` **no local-system**

Parameters

system-id	The ID number of the local system, in the range [0-63].
system-name	The name of the local system, if you have assigned one using alias system id.
no	Removes the local system specification from the draft configuration.

3.3.15.5 next-hop system

Specifies which local trunk to use to reach a remote system. A valid configuration will contain exactly one next-hop specification for each system in the network. The `next-hop system` name must be the alias you created with the `alias system id` command (see alias system id).

	A good switch configuration will have exactly one next-hop specification for every non-local system.

Syntax

`CONF-SWITCH#` **next-hop system {***system-name***|id** *system-id***} via {***trunk-name***| trunk** *vif-id***}** [**description** *next-hop-description*]

`CONF-SWITCH#` **no next-hop** [**system {***system-name***|id** *system-id***}**]

Parameters

system *system-name* **system id** *system-id*	The next system in the network topology. Can be a name, if you have assigned one using alias system id, or the system's number id in the range [0-63].
via *trunk-name* **via trunk** *vif-id*	The trunk to use for connecting to the next system. Can be a name assigned by `alias local-vif trunk` or the trunk id in the range that is system-configuration based.
description *next-hop-description*	An optional description for the next-hop system you have specified. This can detail certain characteristics of the system, for clarity.
no	Removes the specified next-hop from the draft configuration. (The system itself is still in the draft configuration.) The `no next-hop` command (without the `system` keyword) will remove all next-hops.

3.3.15.6 destination

Specifies the end-point of a transmission path, from the starting point (local client interface) to the remote system and client interface.

You can set a round robin (RR) class, if desired. In round-robin scheduling, each client (of a particular class) that seeks attention is dealt with in circular order. DXMOS has four RR classes, 0-3. All members of class 0 are dealt with first, in circular order, until no member is requesting attention. Next, class 1 is considered, then class 2, then class 3. When the output queue is ready for the next packet, class cycling repeats; pending work for class 0 being handled first, followed by class 1, and so on. If no class value is specified in the `destination` command, the default class of 3 (the lowest class) will be applied.

When the remote-vif is specified by name (`remote-client-name`), don't specify `remote-system`, since the remote system is implicit in a remote-vif name.

Syntax

`CONF-SWITCH#` **destination local-vif {***client-name***|client** *vif-id***} remote-vif** *client-name* [**class** *class*] [**description** *destination-description*]

`CONF-SWITCH#` **destination local-vif {***client-name***|client** *vif-id***} remote-system{***system name***|id** *system-id***} remote-vif client** *vif-id* [**class** *class*] [**description** *destination-description*]

`CONF-SWITCH#` **no destination** [**local-vif {***client-name***|client** *vif-id***}**]

Parameters

local-vif *client-name* **local-vif client** *vif-id*	The local client interface (or "starting point") of the path you are specifying. Can be a name assigned by `alias local-vif` or the `client` id in the range that is system-configuration based.
remote-system *system-name* **remote-system id** *system-id*	The system at the end of a specified path (the destination). Can be a name, if you have assigned one using alias system id, or the system's number id in the range [0-63].
remote-vif *client-name* **remote-vif client** *vif-id*	The client interface on the system at the end of a specified path (i.e., the destination). Can be a name assigned by `alias remote-vif` or the `remote-vif client` id.
class *class*	Determines the priority of data frame processing. Can be 0-3. Destinations with a class of 0 will have their data frames processed first. If no class value is specified, the default class of 3 (the lowest class) will be applied.
description *destination-description*	An optional description for the destination system you have specified. This can detail certain characteristics of the system or path, for clarity.
no	Removes the specified local-vif from the draft configuration. The `no destination` command (without the `local-vif` keyword) removes all destinations.

3.3.15.7 commit

Validates and saves the draft switch configuration to the running configuration. If the configuration is not valid, the errors are reported and the configuration is NOT saved to the running configuration.

Syntax

`CONF-SWITCH#` **commit**

3.3.15.8 compare

Displays the differences between draft and running switch configurations.

Syntax

`CONF-SWITCH#` **compare**

3.3.15.9 revert-to

Discards current draft switch settings and reverts to the last-saved configuration.

Syntax

`CONF-SWITCH#` **revert-to {factory-config|running-config}**

factory-config	Resets the switch settings to the default factory settings (clears all settings).
running-config	Resets the switch settings to the last saved running configuration.

3.3.15.10 show switch

Displays the draft switch configuration.

This is very similar to `show running-config`*, except that the switch section is the draft configuration and NOT the running configuration.*

Syntax

`CONF-SWITCH#` **show switch**

3.3.15.11 validate

Verifies the syntax is correct and reports any errors. Validate does not check for completeness or save to the running configuration. Use the `commit` command to validate *and* save to the running configuration.

Syntax

`CONF-SWITCH#` **validate**

3.3.15.12 end

Exits switch configuration mode and returns to enable mode. If the draft configuration contains uncommitted changes, the system prompts you to confirm you really want to end. Whether or not the draft configuration is committed, it is retained for use the next time switch configuration mode is entered.

Syntax

`CONF-SWITCH#` **end**

3.3.15.13 exit

Exits switch configuration mode and returns to configuration mode. If the draft configuration contains uncommitted changes, the system prompts you to confirm you really want to exit. Whether or not the draft configuration is committed, it is retained for use the next time switch configuration mode is entered.

Syntax

`CONF-SWITCH#` **exit**

3.3.16 terminal pager

For commands that support text paging, sets the number of output lines per page and pauses after displaying the lines. When the console output pauses, the user presses the space bar to proceed to the next page.

The value for *n* in the command `terminal pager n` determines the output-line page length, or disables the terminal pager altogether if n=0. You can also disable it with the command `no terminal pager`.

- On first installation, the terminal pager is disabled (i.e., n=0).
- To enable the terminal pager, assign a value for *n* that sets the maximum number of output lines in the page. Even though you can change the command parameters in disable mode (`>`) and enable mode (`#`), you must be in configuration mode (`CONF#`) to make changes that can be saved to the config file.

The `terminal pager` command differences by mode:

- For configuration mode only, the `terminal pager` *n* command can be initiated in one of two ways:
  - Via the config file: During the next reboot or reload, the `terminal pager` command that was saved to the config file is processed (i.e., read and executed), and the console is set to the specified page length (or disabled if n=0 or the command `no terminal pager` was specified).
  - Via a terminal: Setting page length to *n*. **Note:** If the terminal is a VTY (i.e., virtual/remote), and no one is logged in to the console, the page length will also be set in the console.
- From configuration mode, any saved changes become the `default` parameter for disable and enable modes.
- For disable mode and enable mode, the `terminal pager default` command, available in these two modes only, acquires the particular `terminal pager` command specified and saved in configuration mode.

See also the more command.

Syntax

`>` [no] **terminal pager {0|1|***n***|default}**

`#` [no] **terminal pager {0|1|***n***|default}**

`CONF#` [no] **terminal pager {0|1|***n***}**

Parameters

0	The value for *n* that disables the terminal pager. Equivalent to the command `no terminal pager`.
1	Enables the terminal pager with 2 lines per page.
n	Sets the page size to *n* output lines for the terminal. **Note:** *n* can also take values of 0 and 1, as described above.
default	This parameter sets the page size in disable and/or enable mode to the *n* output lines specified (and saved) in configuration mode. **Note:** If no value for *n* `output` lines is specified and saved in configuration mode, the `terminal pager default` command will disable terminal paging in the mode from which it was issued (i.e., disable mode and/or enable mode). And because no *n* value was specified in configuration mode, that mode remains disabled, as well. In other words, not specifying a value for *n* means that *n*=0.
no	The command `no terminal pager` disables the terminal pager. Equivalent to specifying `terminal pager 0`. **Note:** If `no terminal pager` is specified and saved in configure mode, it becomes the `default` parameter for the disable and enable modes.

3.3.17 tftp

The tftp commands transfer files between the DarkStar system and a TFTP server using the management network.

Note: Use of the `tftp` command requires a functioning TFTP server. Configuring TFTP servers is beyond the scope of this documentation.

DNS must be configured with the `ip name-server` *command for* `tftp-server` *to work with a hostname instead of an IP address.*

- **It is possible to corrupt valid storage locations using the `tftp` command. No checks are made to ensure the downloaded data files are legitimate DarkStar system data files. Use the `checksum` command on the retrieved file and manually verify its integrity.**
- **If you attempt to overwrite an executable file with a data file, or vice versa, you will receive a warning that the two files are of different modes. You will be prompted to confirm your decision before the file overwrite begins.**
- **It is possible to use `tftp` to obtain a configuration whose enable password is unknown. Be sure to write down each configuration's enable password in a safe place. Once the password is set and you leave enable mode, there is no way to configure the DarkStar system without entering the password to return to enable mode.**

Syntax

`#` **tftp {get|put}** *`tftp-server source-file-name destination-file-name`*

Parameters

get	Retrieves a file from a remote TFTP server.
put	Places a file on a remote TFTP server, such as `/dxmos/dxmos.exe`. (Aways a good idea to make a backup of this file.)
`tftp-server`	The IP address or the hostname of the TFTP server.
`source-file-name`	File to be transferred. With a `tftp put` command, the *source-file-name* is a path to a file that is located on the local DarkStar file system. For example, `/dxmos/dxmos.exe` or `dxmos/dxmos.exe`. The *destination-file-name* is a path to a file located on the remote TFTP server.
`destination-file-name`	Target location for the file to be transferred. With a `tftp get` command, the *source-file-name* is a path to a file located on the remote TFTP server. The *destination-file-name* is a path to a file that is located on the local DarkStar file system. For example, `/dxmos/dxmos.exe` or `dxmos/dxmos.exe`.

Example

`localhost#` **tftp put 10.1.1.15** */dxmos/dxmos.exe copy-of-dxmos.exe*

3.3.18 tune

Used in wave module config mode, the `tune` command tunes a wave (line) transceiver to a specific channel, frequency, or wavelength.

	Some DarkStar systems come equipped with line transceivers that must be "tuned," specifying the ITU channel of the DWDM wavelength. After tuning the line transceivers, save the system configuration file with the write memory command. See "Connecting a DarkStar System" in the Systems Guide on the XKL website for details on your specific model to see if tuning is required.

Syntax

`CONF-MOD-WAVE[n]#` **tune** **{***channel*|*frequency*|*wavelength***}** *n*

Parameters

channel n	ITU grid channel/spacing indicator. A decimal number (xx.5), where "xx" indicates the channel number and ".5" indicates 50GHz spacing.
frequency n	ITU grid frequency in GHz (a decimal number).
wavelength n	ITU grid wavelength in nm (xxxx.yy).

3.3.19 tune-for-dmd

Systems that do not have integrated mux/demux filters (i.e., transponders) are connected to external optical filters (such as the DarkStar DMD product line). The `tune-for-dmd command` enables you to tune a group of selected channels to match the external channel filter, or a remote DarkStar filterless system. While the `tune` command enables you to tune by channel, frequency or wavelength, `tune-for-dmd` is exclusively channel only.

The `tune-for-dmd` is not saved in the configuration file. The command calls individual tune commands on each wave, and that is what is saved in the system configuration file.

	Some DarkStar systems come equipped with line transceivers that must be "tuned," specifying the ITU channel of the DWDM wavelength. After tuning the line transceivers, save the system configuration file with the write memory command. See "Connecting a DarkStar System" in the Systems Guide on the XKL website for details on your specific model to see if tuning is required.

Syntax

`CONF#` **tune-for-dmd wave** *n* **spacing {50GHz|100GHz} channel-group** *y*

`wave` *n*	The wave module group, *n, can be one of the following:* 00-03, 04-07, 08-11, 12-15, 16-19, 20-23, 24-27, 28-31, 32-35 (i.e., 4 waves) 00-05, 06-11, 12-17, 18-23, 24-29, 30-35 (i.e., 6 waves) 00-11, 12-23, 24-35 (i.e., 12 waves)
50GHz|100GHz	Sets the desired spacing for the channels.
channel-group *y* (50GHz, 4 waves)	Waves can be tuned from channels 14 through 61.5, with each wave in the group having their channels increment by 0.5. Groups are: • 14-15.5 • 38-39.5 • 16-17.5 • 40-41.5 • 18-19.5 • 42-43.5 • 20-21.5 • 44-45.5 • 22-23.5 • 46-47.5 • 24-25.5 • 48-49.5 • 26-27.5 • 50-51.5 • 28-29.5 • 52-53.5 • 30-31.5 • 54-55.5 • 32-33.5 • 56-57.5 • 34-35.5 • 58-59.5 • 36-37.5 • 60-61.5
channel-group *y* (100GHz, 4 waves)	Waves can be tuned from channel 14 through 61, with each wave in the group having their channels increment by one. Groups are: • 14-17 • 38-41 • 18-21 • 42-45 • 22-25 • 46-49 • 26-29 • 50-53 • 30-33 • 54-57 • 34-37 • 58-61
channel-group *y* (50GHz, 6 waves)	Waves can be tuned from channels 14 through 61.5, with each wave in the group having their channels increment by 0.5. Groups are: • 14-16.5 • 38-40.5 • 17-19.5 • 41-43.5 • 20-22.5 • 44-46.5 • 23-25.5 • 47-49.5 • 26-28.5 • 50-52.5 • 29-31.5 • 53-55.5 • 32-34.5 • 56-58.5 • 35-37.5 • 59-61.5
channel-group *y* (100GHz, 6 waves)	Waves can be tuned from channel 14 through 61, with each wave in the group having their channels increment by one. Groups are: • 14-19 • 38-43 • 20-25 • 44-49 • 26-31 • 50-55 • 32-37 • 56-61

channel-group *y* (50GHz, 12 waves)	Waves can be tuned from channels 14 through 61.5, with each wave in the group having their channels increment by 0.5. Groups are: • 14-19.5 • 38-43.5 • 20-25.5 • 44-49.5 • 26-31.5 • 50-55.5 • 32-37.5 • 56-61.5
channel-group *y* (100GHz, 12 waves)	Waves can be tuned from channel 14 through 61, with each wave in the group having their channels increment by one. Groups are: • 14-25 • 38-49 • 26-37 • 50-61

Example

CONF# **tune-for-dmd wave** *00-03* **spacing 50GHz channel-group** *14-15.5*

```
Tuning Wave 0 to channel 14.0...

Wave 0 tuned to channel 14.0.
Tuning Wave 1 to channel 14.5...

Wave 1 tuned to channel 14.5.
Tuning Wave 2 to channel 15.0...

Wave 2 tuned to channel 15.0.
Tuning Wave 3 to channel 15.5...

Wave 3 tuned to channel 15.5.

CONF#
```

3.3.20 write

Use write to view, store, or erase your configuration information. Available write commands include:

- write memory
- write network
- write terminal
- write erase config

3.3.20.1 write memory

Writes the current configuration information of the running-config to non-volatile storage (*location /dxmos/config.dat* in flash memory). **Note:** It's a good idea to use the `tftp put` command to make a backup of the startup-config (/dxmos/config.dat). For more information, refer to the tftp section.

Syntax

`#` **write memory**

3.3.20.2 write network

Writes current configuration information to a remote server using TFTP.

- *XKL strongly encourages a backup of the startup-config data on a remote TFTP server. In the event that backups of the configuration in the DarkStar system flash memory become corrupted, a TFTP backup of your settings allows you to restore your DarkStar system and customer traffic to normal conditions.*
- The tftp-server IP address must be of the same class as the system IP address (IPv4 vs IPv6)
- DNS must be configured with the ip name-server *command for* `tftp-server` *to work with a hostname instead of an IP address.*
- If the file already exists at the remote location, `write network` overwrites it.

Syntax

`#` **write network** *tftp-server filename*

Parameters

tftp-server	Specifies the IP address or hostname of a TFTP server to which the `write network` command saves the current `running-config`.
filename	Specifies the name of the file to which the `write network` command saves the current configuration.

3.3.20.3 write terminal

Writes the current configuration to the console. Identical to the show running-config command.

Syntax

`#` **write terminal**

3.3.20.4 write erase config

Erases configuration information from non-volatile storage (flash memory). The `write erase config` command must be followed with the `reload` command to reinitialize the system using factory default settings.

Caution: Only use these two commands if you want to revert all configuration settings back to factory defaults.

Syntax

`#` **write erase config**
`#` **reload**

4

Networking

There are several steps to connecting your DarkStar to a network. These include establishing connections via Telnet or SSH, specifying the router RIP configuration, setting up various IP parameters, and tuning the system to a specific channel, frequency, or wavelength. The associated commands are as follows:

- telnet
- router rip
- ip Commands

Note: Linked-together systems connect to one another in a LAN segment. If the Ethernet interface on one particular system is shut down (per shutdown command), incoming and outgoing traffic is disconnected on that system. The other systems linked to it remain unaffected.

4.1 telnet

Establishes a telnet connection to the specified host name or IP address. The host replies with a definition of the escape character (Control-Shift-6) and a login prompt. You can close the connection with a `logout` command or by using the Control-Shift-6 escape character. Also, you can close the connection on the remote target with the `exit` command (that is, if the connection is to a Unix like environment or another DarkStar system).

Syntax

`>` **telnet** **{***ip-address*|*name***}**

Parameters

name	The hostname of the server to which you are trying to connect.
ip-address	IPv4 or IPv6 address of the server to which you are trying to connect.

Example

```
localhost> telnet 10.14.1.99
Establishing connection to 10.14.1.99:23.
Connected.
The escape character is '^^' (Control-Shift-6) (octal 036).
password: ...
DarkStar> logout
Connection closed.
localhost>
```

4.2 router rip

Places the DarkStar system in Routing Information Protocol (RIP) configuration mode. Command prompt changes to `CONF-RIP#`.

RIP is a way to dynamically inform routers about networks that are not directly connected to them. It works by sharing information between routers: a router broadcasts all of its connected networks and their ports (a routing table), and updates its own routing table from other routers.

Other router rip mode commands include:

- default-information originate
- network
- distance
- passive-interface
- redistribute
- version
- clear rip
- show rip

See ip Commands *for more RIP-related commands.*

Syntax

`CONF#` [no] **router rip**
`CONF-RIP#`

Parameters

no	Removes all RIP configuration information from the running configuration and disables RIP.

4.2.1 default-information originate

Causes a system to both advertise and accept a default (0/0) route, if one is configured.

Syntax

`CONF-RIP#` [no] **default-information originate**

4.2.2 network

Turns on RIP for a given interface. When disabling RIP on an interface, the DarkStar system no longer shares network connectivity information about that interface.

If you are accessing your DarkStar system by way of Telnet or SSH to a VTY, be careful not to remove RIP routes that you are actively using to configure your system.

Syntax

`CONF-RIP#` [no] **network** *address*

Parameters

address	Turns on RIP for subnets, which contain the specified address.
no	Disables RIP for the specified address.

4.2.3 distance

Specify the preferred routing protocol by setting the administrative RIP distance. Values range from 1-255. If no distance is specified, it is set to 120. See Table 4-1.

Administrative distance is a measure of a protocol's reliability. Often there are multiple possible pathways and protocols that a router can use, and it uses the administrative distance to select a particular option. This is a relative measure of the various routing protocols, and the smaller the value, the more dependable the protocol. If you want to give preference to RIP over other protocols, set the administrative distance to a lower number.

TABLE 4-1. Routing Protocol Default Administrative Distances

Protocol	Distance
Connected interface	0
Static route	1
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route	5
External Border Gateway Protocol (BGP)	20
Internal EIGRP	90
IGRP	100
OSPF	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140
On Demand Routing (ODR)	160
External EIGRP	170
Internal BGP	200
Unknown*	255

Syntax

`CONF-RIP#` **distance**

`CONF-RIP#` **distance** *rip-distance*

`CONF-RIP#` **no distance**

Parameters

rip-distance	The RIP distance, between 1-255. Default is 120.
no	Removes RIP distance setting.

4.2.4 passive-interface

Disables sending of routing updates. The DarkStar continues to collect information, but doesn't send updated information.

Syntax

`CONF-RIP#` [no] **passive-interface {ethernet** *n*|**loopback** *n*|**osc** *n*}

Parameters

ethernet *n*, **loopback** *n*, **osc** *n*	Disables sending of routing updates on the specified interface.
no	Enables sending of routing updates on the specified interface.

4.2.5 redistribute

Redistributes routes from other routing protocols via RIP. Additionally, you can specify the number of hops a connection can make.

Syntax

`CONF-RIP#` [no] **redistribute static metric** [value]

Parameters

metric value	The routing metric to use. If you don't specify `metric` *`value`*, `redistribute static` defaults to a metric of 1. Valid values are 1-16 (infinity).
no	Disables redistribution of static routes.

4.2.6 version

Sets which version of RIP is used by the DarkStar system. The default is RIPv2, with RIPv1 compatibility. In general, this is not something that will need to be addressed. However, if RIP version 1 is the only RIP version in use in the local network, you must use this command to select RIP version 1.

This setting can be overridden by specific interfaces with `ip rip send version` and `ip rip receive version` commands.

	The RIP version that is configured on an interface will override the RIP version set globally by the `router rip` command on that particular interface.

Syntax

`CONF-RIP#` [no] **version** *version-number*

Parameters

version-number	Sets the RIP version number. Valid values are 1 or 2.
no version	A version number is not accepted. Returns RIP version to its default value of 2/1 compatibility mode.

	The RIP version that is configured on an interface will override the RIP version set globally by the `router rip` command on that particular interface.

4.2.7 clear rip

Deletes all routing information acquired by RIP. This information will be repopulated when the next RIP update occurs. This is a quick way to update the local network tables, and is useful when other connections on a network have changed, or some other system has failed or been brought online.

Use the `show` ip routes command to view the system-wide routing table.

Syntax

`#` **clear rip**

4.2.8 show rip

Displays current RIP routing settings, including distance and network addresses.

Syntax

`#` **show running-config rip**

`CONF#` **show rip**

4.3 ip Commands

Most IP-related commands are available in configure mode (`CONF#`). However, there are some that are only available while you are configuring an Ethernet device (`CONF-MGMT-<ETH|OSC|LOOP>[n]#`) or a DHCP pool (`CONF-DHCP-POOL[n]#`). Table 4-2 points to the prompt-associated commands.

TABLE 4-2. IP Commands Sorted by Prompt

Prompt	Available IP Commands
`CONF#`	ip dhcp excluded-address ip dhcp pool (changes prompt to `CONF-DHCP-POOL[n]#`) ip domain-name ip host ip name-server ip route
`CONF-MGMT-<ETH|OSC|LOOP>[n]#`	ip **Note:** The `ip` command includes the following sub-commands: • ip address • ip helper address • ip poison-reverse • ip proxy-arp • ip rip receive version • ip rip send version • ip rip v2-broadcast • ip split-horizon
`CONF-MGMT-ETH[n]#`	ipv6 address
`CONF-DHCP-POOL[n]#`	network

4.3.1 ip dhcp excluded-address

Provides a set of network addresses that the DHCP server should exclude from assigning, even if they fall within the range of addresses defined by a DHCP pool.

Syntax

`CONF#` [no] **ip dhcp excluded-address** *ip-address-start ip-address-stop*

Parameters

ip-address-start	The first address in the excluded set.
ip-address-stop	The last address in the excluded set.
no	End the address exclusion. You must specify the address range.

4.3.2 ip dhcp pool

Enters DHCP configuration submode for a specific pool of network addresses. The command prompt changes to `CONF-DHCP-POOL[n]#`.

Syntax

`CONF#` [no] **ip dhcp pool** *pool-id*

Parameters

pool-id	Enters DHCP configuration submode for a specific pool of network addresses. The *pool-id* is a convenience identifier that enables you to create and manage multiple pools of networks to which DHCP should provide addresses. Can be a string or number.
no	Remove a pool of network addressees from DHCP.

4.3.3 ip domain-name

Specifies an additional search domain on the DNS server that you have specified using ip name-server. When name resolution is performed on an unqualified hostname, lookups will be performed by appending these domain names in the order configured. These lookups apply only to queries that use the cache and DNS, not to statically configured hosts.

Note: The system supports 200 configured domain names.

Syntax

`CONF#` [no] **ip domain-name** *name*

Parameters

name	DNS domain name for the search path.
no	Disables an IP domain-name.

Example

```
localhost# configure
localhost CONF# ip domain-name mydomain.net
localhost CONF# exit
localhost#
```

4.3.4 ip host

Specifies a static mapping of host to address. These are searched in the order specified. They take priority over the DNS cache and name servers.

Syntax

`CONF#` [no] **ip host** *name address*

Parameters

name	Sets the name of the host to which an IP address is assigned.
address	Sets the IP address for the given hostname.
no	The static host name and address to remove.

Example

```
localhost# configure
localhost CONF# ip host myhost 11.2.2.4
localhost CONF# exit
localhost#
```

4.3.5 ip name-server

Specifies an additional name server. Servers are referenced in the order specified.

Syntax

`CONF#` [no] **ip name-server** *address*

Parameters

address	The IP address of the DNS server.
no	The name server IP address to remove.

Example

```
localhost# configure
localhost CONF# ip name-server 11.2.1.8
localhost CONF# exit
localhost#
```

4.3.6 ip route

Adds a static route to the routing table. You can combine this with RIP routing as a backup route. Just make sure to use a higher metric value so there is no conflict with the static route.

Syntax

`CONF#` [no] **ip route** *address/netmask gateway* [metric]

Parameters

address/netmask	Sets the IP address and netmask for the static route. **Note:** Static routes are deleted when the management interface is updated.
gateway	Sets a gateway IP address for the static route.
metric	Specifies the metric value for the static route. Valid range is 0 to 65535. The default metric is 1.
no	Disables a static route in the routing table.

4.3.7 ip

Configures IP settings for an Ethernet interface.

Note: The Ethernet interface can have both an IPv6 and an IPv4 address.

Syntax

`CONF-MGMT-<ETH|OSC|LOOP>[n]#` [no] **ip {address** *ip-address/netmask*|**helper-address** *ip-address***}**

`CONF-MGMT-<ETH|OSC|LOOP>[n]#` [no] **ip {poison-reverse|split-horizon|proxy-arp}**

`CONF-MGMT-<ETH|OSC|LOOP>[n]#` [no] **ip {rip receive version** *rip-version*|**rip send version** *rip-version*|**rip v2-broadcast}**

Parameters

address *ip-address/netmask*	Sets the interface IP address to *ip-address* with a netmask of *netmask*. The *ip-address* is specified in IPv4 format, and *netmask* is specified in Classless Inter-Domain Routing (CIDR) notation. An interface can have multiple IP addresses.
helper-address *ip-address*	Any DHCP request received on this interface will be forwarded to the specified ip address (IPv4 address or host name), which should be the DHCP server providing addresses for the subnet connected to the interface.
no ip address *ip-address/netmask*	Removes the specified IP address. If no address is specified, removes all IP addresses from the interface.
poison-reverse	Enables the poisoning (advertisement with infinite metric 16) of routes that have become unreachable. When combined with split-horizon, routes received from a given subnet are advertised with infinite metric back to the subnet to help prevent routing loops. Enabled in RIP by default.
split-horizon	Prevents RIP from advertising a route out of the interface on which it learned the route to help prevent routing loops. Works in conjunction with poison-reverse. The `split-horizon` is enabled by default.
proxy-arp	Replies to ARP requests with a packet containing the DarkStar's MAC address. The DarkStar then forwards subsequent messages to the intended destination.
rip receive version *rip-version*	Configures the Routing Information Protocol (RIP) version that the interface will receive. Valid values for *rip-version* are `1` or `2` (default). This specifies an individual rip version and overrides the global rip setting in `router rip`.
rip send version *rip-version*	Configures the RIP version that the interface will send. Valid values for *rip-version* are `1` or `2` (default). This specifies an individual rip version and overrides the global rip setting in `router rip`.
rip v2-broadcast	Sends v2 updates as broadcast packets. Enabled by default.
no	Disables the settings specified on that command line.

4.3.8 ipv6 address

Configures IPv6 settings for an Ethernet interface.

An interface can have multiple IPv6 addresses . To remove one IPv6 address (e.g., `FD12:E32:DA22::1/64`), use the command `no ipv6 address FD12:E32:DA22::1/64` .

Notes:

- Only the unicast addressing mode is supported. There is no current support for multicast, anycast, or IPv6 routing protocols.
- The Ethernet interface can have both an IPv6 and an IPv4 address.

Syntax

`CONF-MGMT-ETH[n]#` [no] **ipv6 address** *ipv6-address/prefix-length*

Parameters

ipv6-address	An IPv6 address prefix in the form of eight segments, each a hexadecimal value from 0 to FFFF. Leading zeros can be suppressed. Each segment is separated by a colon; one consecutive run of all-zero segments can be abbreviated as "::". For instance, the abbreviated IPv6 address example used in this section is `FD12:E32:DA22::1/64`, where "::" represents "0000 0000 0000 0000." Also note that the last segment of "1" had its three leading zeros suppressed (i.e., it was originally "0001").
prefix-length	IPv6 prefix length, an integer from 1 to 128.
no ipv6	Removes all IPv6 addresses from the interface.
no ipv6 address *ipv6-address*	Removes the specified address from the interface.

4.3.9 network

Assigns a network for which DHCP should provide addresses.

Syntax

`CONF-DHCP-POOL[n]#` **network** *address/netmask*

Parameters

address/netmask	The range of network addresses for DHCP to use; *address* is specified in IPv4 format, and netmask is specified in Classless Inter- Domain Routing (CIDR) notation.

5

Show Commands

5.1 Overview

The `show` commands display information about how the DarkStar system is configured. Depending on the mode (disable, enable, or configure), `show` has different keywords and displays current active configuration settings or current status of the system and/or components. Most of the `show` keywords are available in disable mode, but there are a few that are only available in the enable and configure modes. Available commands and their equivalents in each mode are listed in Table 5-1. For "running-config" show commands, see Table 5-2.

There are a few things to note about the `show` command:

- In general, `# show run` commands are equivalent to `CONF# show` commands. Refer to the table below for specifics.
- To execute an enable mode `show` command from the `CONF#` prompt, precede it with "do". For example, `do show time`.
- To see the active configuration settings for an option, the complete enable mode command is `# show running-config`.

TABLE 5-1. SHOW Commands by Mode (Not Including "running-config" Commands)

Command in > Disable Mode	Command in # Enable Mode	Command in CONF# Configure Mode
show amplifier	show amplifier	do show amplifier
show arp, show ip arp	show arp show ip arp	do show arp do show ip arp
show bert	show bert	do show bert
show bert log	show bert log	do show bert log
show calendar, show clock, show time	show clock show time show calendar	do show clock do show time do show calendar
show connections	show connections	do show connections
show debug	show debug	do show debug
show environment	show environment	do show environment
	show file	do show file
	show flash	do show flash
show hardware	show hardware	do show hardware
	show hostkey	do show hostkey
show hosts	show hosts	do show hosts
show ip routes	show ip routes	do show ip routes
show ip traffic	show ip traffic	do show ip traffic
show led	show led	do show led
show lines	show lines	do show lines
	show logging	do show logging
show management	show management	do show management
	show memory	do show memory
show modules	show modules	do show modules
show optical itu-grid (show optical wavelength-map)	show optical itu-grid show optical wavelength-map	do show optical itu-grid do show optical wavelength-map
show peers	show peers	do show peers
show protection	show protection	do show protection
	show rip	show rip
show sntp	show sntp	do show sntp
	show startup-config	do show startup-config
	show switch	do show switch
	show tech-support	do show tech-support
show version	show version	do show version
show vifs	show vifs	show vifs do show vifs

TABLE 5-2. Running-Config SHOW Commands

	Command in # Enable Mode	Command in CONF# Configure Mode
show running-config	show running-config	do show running-config
	show running-config access-list	show access-list do show running-config access-list
	show running-config amplifier	show amplifier do show running-config amplifier
	show running-config banner	show banner
	show running-config bert log	show bert log
	show running-config boot	show boot
	show running-config dhcp	show dhcp
	show running-config fan	show fan
	show running-config host	show host do show running-config host
	show running-config line	show line do show running-config line
	show running-config logging	show logging do show running-config logging
	show running-config management	show management do show running-config management
	show running-config module	show module do show running-config module
	show running-config protection	show protection do show running-config protection
	show rip	show rip do show running-config rip
	show running-config snmp	show snmp
	show running-config sntp	show sntp do show running-config sntp
	show running-config static-routes	show static-routes
	show running-config switch (crossbar switch)	show switch (crossbar switch)

5.2 show running-config

Displays current active configuration settings for the specified option. There are several ways to call this command, depending on the permission level, either in enable (#)or configuration (CONF#) mode. See Table 5-2 for the list of command options.

There are many "show" commands that are very similar to "show run" commands. In general, "show" displays what is currently happening with a component (its status), and "show run" displays the configuration settings for a component.

- If you don't specify any options, `CONF# show` displays full configuration information, starting with a string of eight semicolons (;;;;;;;;). **Note:** This information can be captured in a text file, starting with the semicolons, and placed on a TFTP server for later download via the `tftp` command. The dxmos/config.dat file contains all of this information if `write memory` has been used to save configuration edits.
- Shortcuts include `show run` or `show run` <Tab key>.
- The `show running-config` command is identical to the `write terminal` command.

The running config may not yet have been preserved as a file. To preserve it, use the `write memory` command.

Syntax

`#` **show running-config** [See the following optional parameters.]

Parameters

no keyword	Displays complete currently running configuration information for the system.
access-list	Current access lists, if any are configured. For more information, see Access Control Lists.
amplifier	Current amplifier settings, including path, output gain and power, and pump current. For more information, see Amplifiers.
banner	Current banner message.
bert log	Current BERT log setting.
boot	Current boot target settings.
dhcp	Current DHCP network settings.
fan	Current configured fan speed for any fans not in auto mode. This is not the same as show environment fans, which displays the current environmental status of the fan modules.
host	Current hostname and ip domain settings. This is not the same as show hosts.
line	Current line configurations, including passwords, TACACS+ and RADIUS server settings, and AAA-related settings. This is not the same as show lines.
logging	Current logging buffer configuration. For more information, see logging.
management	Current configuration settings for the Ethernet, OSC, and loopback interfaces in the system. This is not the same as show management.
module	Current configuration settings for the transceivers in the system. This is not the same as show modules.
rip	Current RIP routing configuration, including distance and network addresses. For more information, see router rip.
snmp	Current SNMP settings, including trap locations. For more information, see snmp-traps.
sntp	Current SNTP configuration, including the IP address and last sync time of the currently selected SNTP server.
static-routes	Current static routes, if any.
switch	Current crossbar switch settings.

Example

```
localhost# show running-config
running-config:
;;;;;;;;
version 4.0.1
enable
configure
line console
exit
line vty
exit
clock summer-time off
hostname localhost
management ethernet 0
```

```
description Eth
exit
management ethernet 1
description Eth
exit
management ethernet 2
description Eth
exit
management ethernet 3
description Eth
exit
management osc 0
no laser shutdown
description OSC
exit
module client 0
no laser shutdown
no loopback
encapsulation 10gigabitethernet
exit
module client 1
no laser shutdown
no loopback
encapsulation 10gigabitethernet
exit
module client 2
no laser shutdown
no loopback
encapsulation 10gigabitethernet
exit
module client 3
no laser shutdown
no loopback
encapsulation 10gigabitethernet
exit
module wave 0
no laser shutdown
loopback electrical
encapsulation 10gigabitethernet
exit
module wave 1
no laser shutdown
no loopback
encapsulation 10gigabitethernet
exit
module wave 2
no laser shutdown
no loopback
encapsulation 10gigabitethernet
exit
module wave 3
no laser shutdown
```

```
no loopback
encapsulation 10gigabitethernet
exit
module wave 4
no laser shutdown
no loopback
encapsulation 10gigabitethernet
exit
module wave 5
no laser shutdown
no loopback
encapsulation 10gigabitethernet
exit
module wave 6
no laser shutdown
no loopback
encapsulation 10gigabitethernet
exit
module wave 7
no laser shutdown
no loopback
encapsulation 10gigabitethernet
exit
module wave 8
no laser shutdown
no loopback
encapsulation 10gigabitethernet
exit
module wave 9
no laser shutdown
no loopback
encapsulation 10gigabitethernet
exit
management osc 0
module OSC 0
no laser shutdown
description OSC 0
exit
! banner motd should be last in the configuration file for safety.
! A malformed MOTD with a missing ending delimiter will result in
! undefined behavior of any configuration statements after the MOTD.
localhost#
```

5.3 show amplifier

Click show amplifier to see description in its proper context. Also see show running-config amplifier.

5.4 show arp, show ip arp

Click show arp, show ip arp to see descriptions in their proper context.

5.5 show calendar, show clock, show time

All of these commands display the current time and date; the difference is the source.

- `show calendar` displays the current time and date according to the DarkStar system calendar chip.
- `show clock` and `show time` display the current time and date according to the DarkStar system clock.

Syntax

`>` **show calendar** [verbose]

`>` **show clock** [verbose]

`>` **show time** [verbose]

Example

```
localhost> show time
High resolution clock (corrected): 12:26:23 UTC-7 Wed Aug 11 2021
localhost> show time verbose
Date and time from calendar:       12:26:27 UTC-7 Wed Aug 11 2021
High resolution clock (corrected): 12:26:28 UTC-7 Wed Aug 11 2021
High resolution clock (raw):       12:26:29 UTC-7 Wed Aug 11 2021
Clock most recently set at:        03:23:37 UTC-7 Wed Aug 11 2021
localhost>
```

5.6 show debug

Click show debug to see description in its proper context.

5.7 show bert

Click show bert to see description in its proper context.

5.8 show bert log

Click show bert log to see description in its proper context.

5.9 show connections

Displays information about the wave and client interface connections, line status, and line rates. Without a *transport-identifier*, show connections displays information about the connection between two transport interfaces.

Each line in the displayed table describes an active connection between interface 1 and interface 2. See the connect command for additional information.

Syntax

> **show connections** [*transport-identifier*] [verbose]

Parameters

transport-identifier	Display connections to the specified interface. On redundant systems: client *n*, *wave* east *n*, or *wave* west *n* On non-redundant systems: client *n* or *wave n*
verbose	Displays an additional table with details and descriptions of the connected interfaces.

The following uses the connectcommand for the crossbar switch.

Example

```
localhost# show connections

10G Switch Complex connections:
Idx   If1          If2           Channel   If1 Line / Rate     If2 Line / Rate
---   ----------- --------------  -------   -----------------   -------------
0     Client 0      Wave 0          30.0      Up      /10GE       Up      /10GE
1     Client 1      Wave 1          31.0      Up      /10GE       UP      /10GE

localhost# show connections verbose

10G Switch Complex connections:
Idx   If1          If2           Channel   If1 Line / Rate     If2 Line / Rate
---   ----------- --------------  -------   -----------------   -------------
0     Client 0      Wave 0          30.0      Up      /10GE       Up      /10GE
1     Client 1      Wave 1          31.0      Up      /10GE       Up      /10GE

Idx              Interface Description <==> Interface Description
--- ------------------------------------------------------------------------
0                Fairfax router port 3 <==> Chantilly Service Building
1                Fairfax router port 4 <==> Chantilly Parts Building
```

5.10 show environment

Displays operating environment information, including temperature and status of power supply and fan modules.

Running `show environment` without any arguments is equivalent to `show environment all`.

Syntax

`>` **show environment** [all|fans|logging|power|temperature]

Parameters

all	Displays summary of fan and power system status, as well as the Command Loader log.
fans	Displays detailed fan module status and operational parameters.
logging	Displays items in the Command Loader log.
power	Displays detailed power supply module status and operational parameters.
temperature	Displays current temperature readings and temperature operating ranges for many DarkStar components.

Example

```
localhost# show environment all
Power Supply 0: Normal/On
Power Supply 1: Normal/On
Fan Module 0 is present, functioning normally
Fan Module 2 is present, functioning normally
Command Loader Log:
(0x01, time        0) Power up; reloaded per DIP
(0x29, time      257) Successful reload
(0xc5, time 10133150) Commanded reload
(0x29, time 10133407) Successful reload
```

```
localhost# show environment temperature
Temperature (C)               Curr  Low   Low   Fan   High  High  High
Sensor Id                     Temp  Alrm  Warn  Ctrl  Warn  Alrm  Crit
-----------                   ----  ----  ----  ----  ----  ----  ----
OSC 1                           28     0     5    50    65    70    80
OSC 0                           33     0     5    50    65    70    80
Fan 0 Outlet                    26     0     5  none    60    65    70
Fan 2 Outlet                    27     0     5  none    60    65    70
DAMP Board                      28     0     5  none    60    65    70
CMD Outlet                      36     0     5  none    60    65    70
CMD Board                       46     0     5  none    60    65    70
CMD FPGA                        60     0     5    80    95   100   115
C1UB Board                      29     0     5  none    60    65    70
East Input EDFA                 23    -5     0    50    65    70    80
West Input EDFA                 29    -5     0    50    65    70    80
```

```
localhost# show environment power
Power Supply 0 is present, with status: Normal/On
  Position:      Left (as viewed from rear)
  Type:          Front-end
  Manufacturer:  POWER-ONE
  Serial Number: 110615-005Z6
  Part Number:   SFP450-12BG
     Output Voltage:    12.040 V
     Output Current:     2.400 A
     Max Output Power:     450 W
     Min Input Voltage:     90 V
     Max Input Voltage:    264 V

Power Supply 1 is present, with status: Normal/On
  Position:      Right (as viewed from rear)
  Type:          Front-end
  Manufacturer:  POWER-ONE
  Serial Number: 111025-0068F
  Part Number:   SFP450-12BG
     Output Voltage:    12.060 V
     Output Current:     2.400 A
     Max Output Power:     450 W
     Min Input Voltage:     90 V
     Max Input Voltage:    264 V

localhost# show environment fans
Fan 0, is present
  Position: Leftmost (as viewed from rear)
  Control Mode: Auto
 Blower 0, is present
  Position: Left (as viewed from rear)
  Minimum speed is 82 RPS, Maximum speed is 307 RPS
  Target speed is 1 percent, Last read 91 RPS
  No Alarms
 Blower 1, is present
  Position: Right (as viewed from rear)
  Minimum speed is 81 RPS, Maximum speed is 305 RPS
  Target speed is 1 percent, Last read 91 RPS
  No Alarms
Fan 2, is present
  Position: Rightmost (as viewed from rear)
  Control Mode: Auto
 Blower 0, is present
  Position: Left (as viewed from rear)
  Minimum speed is 83 RPS, Maximum speed is 305 RPS
  Target speed is 1 percent, Last read 92 RPS
  No Alarms
 Blower 1, is present
  Position: Right (as viewed from rear)
  Minimum speed is 81 RPS, Maximum speed is 303 RPS
  Target speed is 1 percent, Last read 92 RPS
  No Alarms
```

5.11 show file

Displays information pertaining to the file system.

Syntax

show file info *filename*

show file {descriptors|systems}

Parameters

descriptors	Lists which files are currently in use.
systems	Displays information about the file systems present, including size, type, and location.
info *filename*	Displays information about a specified file, including size, creation date, and last-modified date.

Example

```
localhost# show file descriptors
Scanning all open files...
  Directory '/.' is open.
  Directory '/dump' is open.
  Directory '/gateware' is open.
```

Example

```
localhost# show file systems
File Systems:
 Device          Size            Free         Usage      Type      Flags  Mount
flash0:0      104856 KB          N/A          N/A      System     R/W    --
flash0:1      104856 KB          N/A          N/A      System     R/W    --
flash0:2      629136 KB       590816 KB       6.09%    DXMFS(P)   R/W   /
flash0:3     1048560 KB            0 KB     100.00%    DXMFS      R/W   /dump
flash0:4     2201976 KB      2090996 KB       5.04%    DXMFS      RO    /gateware
flash0:5     1048560 KB          N/A          N/A      DXMFS      R/W    --
flash0:6     1048560 KB          N/A          N/A      DXMFS      R/W    --
flash1:0      104856 KB          N/A          N/A      System     RO     --
flash1:1      104856 KB          N/A          N/A      System     RO     --
flash1:2      629136 KB          N/A          N/A      DXMFS(P)   RO     --
flash1:3     1048560 KB          N/A          N/A      DXMFS      RO     --
flash1:4     2201976 KB          N/A          N/A      DXMFS      RO     --
flash1:5     1048560 KB          N/A          N/A      DXMFS      RO     --
flash1:6     1048560 KB          N/A          N/A      DXMFS      RO     --
```

Example

```
localhost# show file info last.cfg

  File: 'last.cfg'
  Size: 1846 octets    Blocks: 3   regular file
FileNo: 56 Links: 1
Modify: 2014-03-21 11:50:23 -0700
Create: 2014-03-21 11:50:18 -0700
```

5.12 show flash

Lists system flash memory and flash static files such as `factory-boot`.

Syntax

`#` **show flash**

Example

```
localhost# show flash

System flash directory:
flash0:0  (Type: System)
  Static File           Length   Address
   startup-gateware       32768  00000000
   startup-boot            4096  00500000
   backup1-boot            4096  00720000
flash0:1  (Type: System)
  Static File           Length   Address
flash0:2  (Type: DXMFS(P))
  No static flash files. Use 'dir' to list normal files.
flash0:3  (Type: DXMFS)
  No static flash files. Use 'dir' to list normal files.
flash0:4  (Type: DXMFS)
  No static flash files. Use 'dir' to list normal files.
flash0:5  (Type: DXMFS)
  Static File           Length   Address
flash0:6  (Type: DXMFS)
  Static File           Length   Address
flash1:0  (Type: System)
  Static File           Length   Address
   factory-gateware       32768  00000000
   factory-boot            4096  00500000
flash1:1  (Type: System)
  Static File           Length   Address
flash1:2  (Type: DXMFS(P))
  Static File           Length   Address
flash1:3  (Type: DXMFS)
  Static File           Length   Address
flash1:4  (Type: DXMFS)
  Static File           Length   Address
flash1:5  (Type: DXMFS)
  Static File           Length   Address
flash1:6  (Type: DXMFS)
  Static File           Length   Address
```

5.13 show hardware

Displays serial numbers, manufacturing dates, and hardware revision data for DarkStar system-hardware components. Displays the presence of various optical components, such as filters.

Syntax

`>` **show hardware**

Example

```
localhost# show hardware
Hardware:
 DarkStar Model: DLA
 System Part Number: 10002-12601-00
 System Serial Number: 99999988888Z99

  CMD:
     IDROM Standard Version: 2.8
     Board Serial Number: 1060219295T025
     Part Number: 30001-00106-02
     Board Interface Identifier: 1.3.2
     Manufacturing Date: 191022
     Last Write-Protect IDROM Update: 191113
     Last Read/Write IDROM Update: 200203
     Options:
       Base MAC Address: 00:A0:E3:00:0B:9E (8)

  C1UB:
     IDROM Standard Version: 2.8
     Board Serial Number: 1070019275T009
     Part Number: 30001-00107-01
     Board Interface Identifier: 6.0.1
     Manufacturing Date: 191002
     Last Write-Protect IDROM Update: 210114
     Last Read/Write IDROM Update: 220909
     Options:
       System Configuration: 08 0E 60 E6 00 30 03 00 00 00 (10)

  Dual Amplifier (DAMP):
     IDROM Standard Version: 2.8
     Board Serial Number: 1000017075T013
     Part Number: 30001-00100-00
     Board Interface Identifier: 3.4.1
     Manufacturing Date: 170316
     Last Write-Protect IDROM Update: 170320
     Last Read/Write IDROM Update: 170320
```

```
Amplifier daughter (DOSA) 0:
   IDROM Standard Version: 2.8
   Board Serial Number: 1020220181T007
   Part Number: 30001-00102-03
   Board Interface Identifier: 3.5.3
   Manufacturing Date: 200629
   Last Write-Protect IDROM Update: 200720
   Last Read/Write IDROM Update: 200720

Fan 0:
   IDROM Standard Version: 2.7
   Board Serial Number: 0560408242X081
   Part Number: 30001-00056-04
   Board Interface Identifier: 4.1.2
   Manufacturing Date: 080829
   Last Write-Protect IDROM Update: 191204

Fan 2:
   IDROM Standard Version: 2.7
   Board Serial Number: 0560412086H004
   Part Number: 30001-00056-04
   Board Interface Identifier: 4.1.2
   Manufacturing Date: 120326
   Last Write-Protect IDROM Update: 191204

Power Supply 0:
   Manufacturer:  ASTEC
   Serial Number: E735TG0055ACP
   Part Number:   DS550HE-3

Power Supply 1:
   Manufacturer:  ASTEC
   Serial Number: E735TG003PACP
   Part Number:   DS550HE-3

Amplification Module East Output EDFA:
   Manufacturer ...... RED-C
   Model ............. 409470 EDFA
   Serial number ..... 17673
   Hardware version .. 000
   Firmware version .. 001.7
   Firmware date ..... JULY 07 2022
   RefD .............. DC0:P103
Amplification Module West Output EDFA:
   Manufacturer ...... RED-C
   Model ............. 409470 EDFA
   Serial number ..... 07014
   Hardware version .. 000
   Firmware version .. 001.7
   Firmware date ..... JULY 07 2022
   RefD .............. DC0:P102
```

5.14 show hostkey

Click show hostkey to see description in its proper context.

5.15 show hosts

Displays a table of local hostname ↔ IP address assignments. You can manually configure this table using the ip host command.

Not to be confused with `show run host`*, which displays the current configuration settings for the current hostname and IP domain.*

Syntax

`>` **show hosts**

5.16 show ip routes

Displays the current system routing table.

Syntax

> **show ip routes** [detailed]

Parameters

detailed	Displays more details, including link layer information. Returns the following display codes: C = Connected S = Static R = RIP

Example

```
localhost# show ip routes

Codes:  C - Connected, S - Static, R - RIP

Current Route Table:
Org Dest IP/CML         Cost Source           NextHop          Sending To
 C  10.11.0.0/16        0/0  10.15.1.222      10.15.1.222      Active R Active
 C  192.176.242.237/21  0/0  192.176.242.237  192.176.242.237  Active R Active

Routing tables
Internet:
Destination         Gateway            Flags  Refs  Use   Mtu  Prio  Iface
10.15/16            link#4             UC        0     0     -     4  eth3
127.0.0.1           127.0.0.1          UH        2   471  33196    4  lo0
192.172.242.237/21  link#1             UC        0     0     -     4  eth0

Internet6:
Destination         Gateway            Flags  Refs  Use    Mtu  Prio  Iface
::1                 ::1                UH        0    0  33196     4  lo0
fe80::%1/64         link#1             UC        0    0     -     4  eth0
fe80::2a0:e3ff:fe0  00:a0:e3:00:06:a6  UHL       0    0     -     4  lo0
.
.
.
```

5.17 show ip traffic

Displays current IP traffic statistics.

Syntax

`>` **show ip traffic**

Example

```
localhost# show ip traffic

ip:
        165526 total packets received
        0 bad header checksums
        0 with size smaller than minimum
        0 with data size < data length
        0 with header length < data size
        0 with data length < header length
        0 with bad options
        0 with incorrect version number
        0 fragments received
        0 fragments dropped (duplicates or out of space)
        0 malformed fragments dropped
        0 fragments dropped after timeout
        0 packets reassembled ok
        38532 packets for this host
        4159 packets for unknown/unsupported protocol
        0 packets forwarded
        22060 packets not forwardable
        0 redirects sent
        999 packets sent from this host
        0 packets sent with fabricated ip header
        0 output packets dropped due to no bufs, etc.
        299 output packets discarded due to no route
        0 output datagrams fragmented
        0 fragments created
        0 datagrams that can't be fragmented
        0 fragment floods
        0 packets with ip length > max ip packet size
        0 tunneling packets that can't find gif
        0 datagrams with bad address in header
        0 input datagrams checksum-processed by hardware
        0 output datagrams checksum-processed by hardware
        110098 multicast packets which we don't join
```

5.18 show led

Displays a readout of the front panel LEDs and a summary of system status. The output will vary, depending on the DarkStar configuration. Some examples follow.

Syntax

> **show led** [verbose]

Parameters

verbose	System-dependent parameter that provides additional details as applicable.

Examples

(Starting on next page.)

DarkStar DSM10-10

localhost# **show led** verbose

```
System Status:
    | PWR | WRN | ALM |
    |green|amber| red |
    |-----|-----|-----|
    | on  |     |     |

System Status Info:
   System fully operational

Ethernet Link:
    |   E0    |   E2    |
    |---------|---------|
    |on(green)|         |

    |   E1    |   E3    |
    |---------|---------|
    |         |         |

Line/Wave Ports:
  Wave Power (Wave 0 - Wave 9): on

Line/Wave Ports Info:
  Wave 0: on
  Wave 1: on
  Wave 2: on
  Wave 3: on
  Wave 4: on
  Wave 5: on
  Wave 6: on
  Wave 7: on
  Wave 8: on
  Wave 9: on

OSC Ports:
  OSC W Signal: on

Client Ports:
    |    C0     |    C1     |    C2     |    C3     |    C4     |
    | Ok  | Sig | Ok  | Sig | Ok  | Sig | Ok  | Sig | Ok  | Sig |
    |-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
    |     |     |     |     |     |     |     |     |     |     |

    |    C5     |    C6     |    C7     |    C8     |    C9     |
    | Ok  | Sig | Ok  | Sig | Ok  | Sig | Ok  | Sig | Ok  | Sig |
    |-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
    |     |     |     |     |     |     |     |     |     |     |
```

DarkStar DMD-A with OPS

```
localhost# show led

System Status:
    | PWR | WRN | ALM |
    |green|amber| red |
    |-----|-----|-----|
    | on  |     |     |

System Status Info:
   System fully operational

Ethernet Link:
    |   E0    |   E2    |
    |---------|---------|
    |         |on(green)|

    |   E1    |   E3    |
    |---------|---------|
    |         |         |

OSC Ports:
  OSC A: on
  OSC B: on

Protection/Amps:
                    Line
            Active        EDFA
       |   A     B   |  In    Out  |
  ================================
   OK  |       | on    | flash|      |
   WRN |       |       |      |      |
   ALM |       |       |      |      |
```

DarkStar DLA

```
localhost# show led

System Status:
    | PWR | WRN | ALM |
    |green|amber| red |
    |-----|-----|-----|
    | on  |     |     |

System Status Info:
   System fully operational

Ethernet Link:
    |   E0    |   E2    |
    |---------|---------|
    |         |         |

    |   E1    |   E3    |
    |---------|---------|
    |         |on(green)|

OSC Ports:
  OSC West: off
  OSC East: off

Amps:

                EDFA
           West          East
  EDFA |  In    Out  |  In    Out  |
  ================================
   OK  |      |      |      |      |
   WRN |      |on    |      |on    |
   ALM |      |      |      |      |
```

5.19 show lines

Shows the status of console and VTY lines. The current command session is indicated by an asterisk, as shown in the example below.

Not to be confused with `show run line`*, which displays the current SNTP running-config settings and the last sync time of the currently selected SNTP server.*

Syntax

`>` **show lines**

Example

`localhost>` **show lines**

```
Line Information
Line    Location        Idle            Status
0       CTY             0:00:00:00      Logged In*
1       VTY 0           NA              Free
2       VTY 1           NA              Free
3       VTY 2           NA              Free
4       VTY 3           NA              Free
```

5.20 show logging

Click show logging to see description in its proper context.

5.21 show management

Displays current status for management modules. Without any arguments, the `show management` command displays summary information for all configured Ethernet and loopback management modules. It is equivalent to the `show management summary` command.

If OSC transceivers are detected (i.e., are present), the applicable system-dependent OSC ports will display relevant information.

Not to be confused with `show run management`*, which displays the current configuration settings for the specified modules.*

Syntax

`>` **show management** [summary|all|ethernet *n*|loopback *n*|osc *n*|switch]

Important: The `switch` command parameter is not available on all systems. To determine whether the `switch` parameter is available on your system, issue the `show hardware` command. If the system is CMD based, the `switch` command parameter is available.

Parameters

ethernet *n*	When *n* is 0, the command displays the status of the internal Ethernet port 0. You can also use this command to display the status of an OSC transceiver. Depending on system configuration, *n* can be from 4–7, the values representing the internal ports of one or more installed OSC transceivers. **Note:** For systems with the `switch` parameter, values for `ethernet` *n* from 1–3 are invalid.
loopback *n*	*n* refers to a loopback interface, which is a virtual interface that echoes everything sent to it. **Notes:** • *n* can only be 0, as only one loopback address can be configured on any DarkStar system. • If loopback is not configured, it will not be listed in `show management summary` or `show management all`.
osc *n*	*n* refers to a single OSC port for which status will be displayed. Depending on system configuration, *n* can be from 0–3. **Note:** The `show management osc` *n* command is equivalent to the `show management ethernet` *n* command, where *n* is within the applicable OSC-value range for the respective commands. For example, the port for `osc` ***0*** is the same as the port for `ethernet` 4; the port for `osc` 1 is the same as the port for `ethernet` 5, and so on.
switch	For systems equipped with this feature, displays the status of the Ethernet switch's external ports (E0–E3). **Note:** The Ethernet switch acts as a Layer-2 switch, managing the DarkStar system's four front-panel Ethernet ports (E0–E3) to which copper LAN cables connect.
all	This command is a concatenation of all `show management ethernet` *n* commands, including loopback and switch information.
summary	Displays a short summary of information about all Ethernet and loopback management modules that are configured.

The following example shows output for a system with the `switch` parameter.

Example

```
localhost# show management ethernet 0
Ethernet 0 is up, line protocol is up,
  Description is Eth0
  Internet address is 10.15.1.148/16
  IPv6 address is ::ffff:a0f:194/64
  Hardware is Ethernet Switch. MAC address is 00:A0:E3:00:0C:56
  full-duplex mode, link type is 1Gbps (Auto-Negotiated)
  Last State Change: 0:17:00:48 ago
    84883 packets input, 6204187 bytes
    0 no receive buffer, 0 CRC error, 0 overrun
    0 no transmit buffer
```

```
    77 packets output, 7282 bytes
    0 collisions, 0 late collisions,
    0 deferred, 0 lost carrier, 0 no carrier
```

The following example shows the (Ethernet Layer-2) switch for the management interface.

Example

```
localhost# show management switch

    Port         Link          Type         Auto-negotiation    Link-status
-------------  ----------  --------------  ------------------  --------------
e0             1000 Mbps   full-duplex     complete              up
e1             none        half-duplex     not complete        down
e2             none        half-duplex     not complete        down
e3             none        half-duplex     not complete        down
```

5.22 show memory

Click show memory to see description in its proper context.

5.23 show modules

Displays current status for transceivers. Without any arguments, the `show modules` command displays summary information for all included transceiver types (e.g., OSC, client, trunk, wave). Equivalent to `show modules summary`. For information on output fields associated with the `show modules` commands, see Defined States under Supplementary Information in Appendix A.

Not to be confused with `show run module`*, which displays the current configuration settings for the specified* transceivers.

Syntax

`localhost>` **show modules** [summary|all|*module-identifier*][host-side|media-side|verbose]

Parameters

summary	Displays summary information for all transceivers.
all	Displays detailed information for all transceivers, including detailed alarm, temperature, and component make/model information. **Note:** The secondary option, `verbose`, will provide additional module detail.
module-identifier	Specific transceiver type for which to view information. You can also specify a transceiver *n* of a particular transceiver type, where *n* is an integer falling within the range of associated transceivers for that type (e.g., `OSC 0`, `wave 0`).

host-side|media-side verbose	`host-side`—This secondary option includes more details focused on the status of the transceiver module's electrical receiver and transmitter. This is the interface connecting a client module to a wave module inside the system. **Note:** Available only on select systems. `media-side`—This secondary option includes more details focused on the status of the transceiver module's optical receiver and transmitter. **Note:** Available only on select systems. `verbose`—This secondary option provides additional module detail.

Example

```
localhost# show modules osc 0
OSC West    Up
  Description: .... Seattle_to_Redmond
  Tx: ............. OK                          Rx: .......... OK
  State Changed: .. 00d 13:20:52               Channel: ..... N/A
  Tx Laser: ....... Enabled                     Frequency: ... 198406 GHz
  Tx Power: ....... 2.6 dBm                     Wavelength: .. 1511.00 nm
  Rx Power: ....... -19.5 dBm                   Module Type: . SFP
  Loopback: ....... Not Supported               Temperature: . 26 C
  Encapsulation: .. 100Base-FX                  Vendor: ...... SOURCEPHOTONICS
  Last Cleared: ... 00d 13:20:05                Part No.: .... SPC03XLR51CDA
  Link Downtime: .. 00d 00:00:00                Serial No.: .. A36T000517
  Maximum Reach: .. 150 km on SM                MFG Date: .... 10020588
```

Example

```
localhost# show modules
```

Interface	Admin	Line	Rate	RxPow	Ch	Transceiver	Last Line Chg
Client 0	Up	Warning	10Gb/s	<-40.0 dBm	N/A	Alarm	00d 14:00:40
Client 1	Up	Warning	10Gb/s	<-40.0 dBm	N/A	Alarm	00d 14:00:40
Client 2	Up	Warning	10Gb/s	<-40.0 dBm	N/A	Alarm	00d 14:00:40
Client 3	Up	Down	10Gb/s	-31.5 dBm	N/A	Warning	00d 14:00:40
Client 4	Up	Down	10Gb/s	-40.0 dBm	N/A	Warning	00d 14:00:40
Client 5	Up	Down	10Gb/s	-40.0 dBm	N/A	Warning	00d 14:00:40
Client 6	Up	Warning	10Gb/s	<-40.0 dBm	N/A	Alarm	00d 14:00:40
Client 7	Up	Warning	10Gb/s	-40.0 dBm	N/A	Alarm	00d 14:00:40
Client 8	Up	Warning	10Gb/s	-40.0 dBm	N/A	Alarm	00d 14:00:40
Client 9	Up	Warning	10Gb/s	<-40.0 dBm	N/A	Alarm	00d 14:00:40
Wave 0	Up	Up	10Gb/s	-12.6 dBm	30.0	OK	00d 14:00:40
Wave 1	Up	Up	10Gb/s	-13.9 dBm	31.0	OK	00d 14:00:40
Wave 2	Up	Up	10Gb/s	-14.8 dBm	32.0	OK	00d 14:00:40
Wave 3	Up	Up	10Gb/s	-13.4 dBm	33.0	OK	00d 14:00:40
Wave 4	Up	Up	10Gb/s	-13.1 dBm	34.0	OK	00d 14:00:40
Wave 5	Up	Up	10Gb/s	-17.4 dBm	35.0	OK	00d 14:00:40
Wave 6	Up	Up	10Gb/s	-13.3 dBm	36.0	OK	00d 14:00:41
Wave 7	Up	Up	10Gb/s	-13.6 dBm	37.0	OK	00d 14:00:41
Wave 8	Up	Up	10Gb/s	-13.6 dBm	38.0	OK	00d 14:00:41
Wave 9	Up	Up	10Gb/s	-14.0 dBm	39.0	OK	00d 14:00:41
OSC West	Up	Up	100Mb/s	-19.5 dBm	N/A	N/A	00d 14:00:41

```
> means the line state has not changed since DXMOS was restarted.
```

Example

```
localhost# show modules client 2
Client 2    Warning
  Description: .... Seattle_to_Redmond
  Tx: ............. Disabled                    Rx: .......... LOS,LOL
  State Changed: .. 00d 14:04:46               Channel: ..... N/A
  Tx Laser: ....... Disabled                    Frequency: ... 228849 GHz
  Tx Power: ....... -19.0 dBm                   Wavelength: .. 1310.00 nm
  Rx Power: ....... <-40.0 dBm                  Module Type: . SFP+
  Loopback: ....... Off                         Temperature: . 28 C
  Encapsulation: .. 10G Ethernet                Vendor: ...... FINISAR CORP.
  Last Cleared: ... 00d 14:03:57                Part No.: .... FTLX1471D3BCV
  Link Downtime: .. 00d 14:04:44                Serial No.: .. UGS0AP2
  Maximum Reach: .. 10 km on SM                 MFG Date: .... 101023
```

Example

```
localhost> show modules client 0 media-side
                        Client 0 Media-Side Receiver

Rx Loss Of Signal (LOS)
  Lane 0: ..............................................   False
  Lane 1: ..............................................   False
  Lane 2: ..............................................   False
  Lane 3: ..............................................   False

Rx Loss Of Lock (LOL)
  Lane 0: ..............................................   False
  Lane 1: ..............................................   False
  Lane 2: ..............................................   False
  Lane 3: ..............................................   False

Rx Power
  Lane 0: ..............................................    -3.9 dBm
  Lane 1: ..............................................    -3.5 dBm
  Lane 2: ..............................................    -3.4 dBm
  Lane 3: ..............................................    -2.8 dBm

  High Alarm: ..........................................     7.4 dBm (False)
  High Warning: ........................................     4.4 dBm (False)
  Low Warning: .........................................   -10.6 dBm (False)
  Low Alarm: ...........................................   -14.6 dBm (False)


                        Client 0 Media-Side Transmitter
Tx Power
  Lane 0: ..............................................     1.0 dBm
  Lane 1: ..............................................     1.5 dBm
  Lane 2: ..............................................     1.9 dBm
  Lane 3: ..............................................     2.1 dBm

Tx Laser Shutdown
  Lane 0: ..............................................   False
```

```
  Lane 1: ..............................................   False
  Lane 2: ..............................................   False
  Lane 3: ..............................................   False

Tx Fault
  Lane 0: ..............................................   False
  Lane 1: ..............................................   False
  Lane 2: ..............................................   False
  Lane 3: ..............................................   False

Tx Bias
  Lane 0: ..............................................    28.7 mA
  Lane 1: ..............................................    28.1 mA
  Lane 2: ..............................................    27.8 mA
  Lane 3: ..............................................    28.5 mA

  High Alarm: ..........................................    75.0 mA (False)
  High Warn: ...........................................    70.0 mA (False)
  Low Warn: ............................................    20.0 mA (False)
  Low Alarm: ...........................................    15.0 mA (False)

Wavelength: ........................................... 1302.35 nm
Frequency: ............................................  230193 GHz
Channel: ..............................................    N/A
```

5.24 show optical itu-grid

Displays an ITU Grid reference table containing optical channels, their frequencies, and wavelengths.
Note: The `show optical wavelength-map` command yields the same results.

Syntax

`>` **show optical itu-grid**

`>` **show optical wavelength-map**

Example

```
localhost# show optical itu-grid

ITU Index     Channel    Freq (GHz)     Wavelength (nm)
---------     -------    ----------     ---------------
0             0.0         190000         1577.86
1             0.5         190050         1577.44
2             1.0         190100         1577.03
3             1.5         190150         1576.61
4             2.0         190200         1576.20
5             2.5         190250         1575.78
.
.
.
133           66.5        196650         1524.50
134           67.0        196700         1524.11
135           67.5        196750         1523.72
136           68.0        196800         1523.34
137           68.5        196850         1522.95
138           69.0        196900         1522.56
```

5.25 show peers

Displays peer addresses and status.

Syntax

`>` **show peers**

Example

```
localhost# show peers

Codes:  C - Connected, S - Self, A - ARP, R - RIP, @ - Adjacent
        ~ - Deleted

Current Peer Information:
Proto  Peer Address     Int          Idle For        Adjacency        MAC
 C     10.15.1.218      Ethernet 3   00145h:02m:59s  10.15.1.218
 C     192.168.253.250  Ethernet 0   00145h:03m:00s  192.168.253.250
```

5.26 show protection

Click show protection to see description in its proper context.

5.27 show rip

Click show rip to see description in its proper context.

5.28 show sntp

Shows SNTP status, including the IP address and last sync time of the currently selected SNTP server.

Not to be confused with `show run sntp`*, which displays the current SNTP running-config settings and the last sync time of the currently selected SNTP server.*

Syntax

`>` **show sntp**

Example

```
localhost# show sntp

SNTP is operating normally.
The next update will be in 34191 seconds (2016-10-17 23:07:24).
The current server is 10.15.1.99 (stratum 3).
The last update was 9009 seconds ago (2016-10-17 11:07:24).
The last adjustment was -5732 microseconds.
```

5.29 show startup-config

Displays DarkStar system startup and backup configurations from flash memory.

Syntax

`#` **show startup-config**

5.30 show tech-support

Click show tech-support to see description in its proper context.

5.31 show sysinfo

Reports the system configuration of the DarkStar system. These values are not user adjustable, and are intended for diagnostic purposes.

`#` **show sysinfo**

5.32 show switch

Reports the state of the system crossbar switch or a draft version of the stat mux switch configuration. This command is for diagnostic purposes or advanced users, and not intended for general operation.

Syntax

`>` **show switch** [verbose]

5.33 show version

Displays more detailed version information, including DXMOS, boot, and gateware version information, and the time and type of the last boot.

Syntax

`>` **show version** [verbose]

Parameters

verbose	Display additional version information and component revision numbers.

Example

```
localhost> show version

DXM Operating System (DXMOS), XKL LLC
4.0.1-75bfb87cca93 Nov 08 2022  20:01:58 UTC
XKL Part Number: 00000-00204-01
Built from: ssh://git@gitlab.xkl.com/Software/dxmos-4.0.1_rc0.git
Boot String: file flash0:2:dxmos/dxmos.exe
```

```
MiniBoot version 2.2(132)-1
Booted via manual boot
Gateware: startup-gateware P/N: 01000-02421-00
Uptime: 0:00:32:53
Last booted up at: 16:49:16 UTC-8 Tue Nov 8 2022
localhost>
```

5.34 show vifs

Displays current status about virtual interfaces. Without any arguments, the command displays summary information for all transceivers, for all types. Equivalent to `show vifs summary`.

Not to be confused with `show running-config module`, which displays the current running-configuration settings for the specified transceivers.

Syntax

`#` **show vifs** [client|trunk|all|summary]

Parameters

client	Displays information for only the client transceivers. **Note:** The information shown is identical to the client information displayed by the `show vifs` or `show vifs summary` commands.
trunk	Displays information for only the trunk transceiver(s). **Note:** The information shown is identical to the trunk information displayed by the `show vifs` or `show vifs summary` commands.
summary	Displays a short summary of information about all transceivers. **Note:** `show vifs summary` provides the same information as `show vifs`.
all (verbose)	Displays more information for all transceivers, including more detailed alarm information. Adding the keyword verbose provides the most detail, including information on Internal Status Module Status, Lane Power Thresholds, and Lane Tunning Bounds.

Example

```
localhost# show vifs
```

VID	Virtual Interface	Cls	Status	TxTotal	Drop%	RxTotal	Drop%
C0	L1036.c0	2	Alarm	0	0.0	0	0.0
C1		3	Alarm	0	0.0	0	0.0
C2		3	Alarm	0	0.0	0	0.0
C3		3	Alarm	0	0.0	0	0.0
C4		3	Alarm	0	0.0	0	0.0
C5	L1036.c5	1	Alarm	0	0.0	0	0.0
C6		3	Alarm	0	0.0	0	0.0
C7		3	Alarm	0	0.0	1.51e09	99.9
C8		3	Alarm	0	0.0	0	0.0
C9		3	Alarm	0	0.0	0	0.0
C10		3	Alarm	0	0.0	0	0.0
C11		3	Alarm	0	0.0	0	0.0
T0	Destination-LXXX	-	Alarm	0	0.0	0	0.0

6

Configuring Security

The DXMOS includes commands to set up your security protocol. Which command you use will depend on your security approach. This chapter discusses the different types of security and the relevant commands to each.

6.1 Types of Security

Possible approaches include:

- Line passwords.
  - In `CONF-LINE-CTY#` (console) mode, you can use password *password* to configure the console with password protection. However, this is a sort of anonymous login, since no username is associated with the password. That is, each new console connection will request a password, but not a username. By default, the console is always enabled for access, unless you specify otherwise.
  - In `CONF-LINE-VTY#` (virtual terminal) mode, SSH and Telnet are disabled by default. Enter password *password* to enable SSH and Telnet access. You can restrict access to use either SSH or Telnet with transport input [ssh|`telnet`].
- Local users and passwords (also called “local database”). This approach requires a username and password, defined with user *username* password *password*, then login `local` (as opposed to simply `login`). This forces users to enter their username and password every time.
- Remote authentication & authorization using RADIUS. Specifies a RADIUS server to use with AAA services.
- Remote authentication & authorization using TACACS+. Specifies a TACACS+ server to use with AAA services.

To use AAA features, first set up the database, then configure how AAA security vets prospective DarkStar users. Something to keep in mind is that the "line passwords" and "local database" options do not require remote server support, but RADIUS and TACACS+ do.

It is possible to configure more than one security option into a method list, so that if one method doesn’t work, users can still log in with another method; otherwise, no one can log in. For example, consider if RADIUS and local database are both specified. When the RADIUS server goes down, users can still log in with the local users and passwords

For more information on RADIUS and TACAS+, see Preparation for Remote Security. For AAA-related information, see AAA Security.

Table 6-1 shows examples of the different security approaches.

TABLE 6-1. Examples of Possible Security Approaches

Approach	Input Example	Result
Line login with no username	`CONF-LINE-<VTY|CTY>#` **login** `CONF-LINE-<VTY|CTY>#` **password** *xkl*	Anyone can log in, as long as they know the password; authentication is done locally.
Local user database	`CONF-LINE-<VTY|CTY>#` **login** local `CONF#` **user** *joe* **password** *test*	Users must correctly enter their username and password; authentication is done locally.
AAA with line login	`CONF#` **aaa new-model** `CONF#` **aaa authentication login default** line	Anyone can log in as long as they know the password.
AAA with local login	`CONF#` **aaa new-model** `CONF#` **aaa authentication login default** local	Users must correctly enter their username and password.
AAA overrides non-AAA setup	`CONF#` **aaa new-model** `CONF#` **aaa authentication login default** group radius	Overrides line and local methods (the first two entries in this table); authentication is handled by AAA services on a remote RADIUS server.
One method	`CONF#` **aaa new-model** `CONF#` **aaa authentication login default** group radius	Only the RADIUS server is specified. If it goes down, no one can log in.
Using a method list	`CONF#` **aaa new-model** `CONF#` **aaa authentication login default** group radius local	If the RADIUS server is down, the system will try to authenticate using the local database.

Whichever approach you choose, for setup you will be working in two configuration modes, (global) configure and line.

6.2 DXMOS Security Commands

The DarkStar DXMOS includes commands to specify who has access to what, privilege levels, passwords, and how you use AAA services or other authentication methods.

DXMOS security-related commands include:

Access Control Lists

- access-list
- access-class

Logins and Passwords

- user
- password
- enable secret
- login
- transport input
- session-timeout

Preparation for Remote Security

- radius-server host
- radius-server key
- tacacs-server host
- radius-server key

AAA Security

- aaa new-model
- aaa authentication login default
- aaa authentication enable default
- aaa authorization exec
- aaa authorization commands
- authorization commands default
- aaa accounting commands
- aaa accounting exec

Other useful DXMOS commands include:

- show hostkey – Displays the public and private DSA keys used by Secure Shell (SSH).
- show running-config line– Displays the current line settings. (See "line" in "running-config" parameter table.)
- `show lines` – Displays the status of the console and VTY lines.
- show running-config access-list – Displays the running configuration access list.

6.2.1 Access Control Lists

The process for setting up one or more Access Control Lists for your DarkStar system is straightforward: you first define the list(s), then apply to the VTY lines. Each list may have one or many entries.

1. Enter global configuration mode with configure.
2. Define the ACL(s) using access-list.
3. Enter line configuration mode with line `vty`.
4. Enable the ACL using access-class.

6.2.1.1 access-list

Defines an IP Access Control List (ACL) rule for filtering management network traffic (Telnet or SSH only). Incoming router traffic is compared to ACL entries in the order they were entered in the router, as the router searches for matches. The first match defines either deny or permit, and the router denies traffic if no match is found. There is an implied denial for traffic that is not permitted.

All IP ACL masks are saved in the config file in Classless Inter-Domain Routing (CIDR) notation (`/nn`), even if you have explicitly used the IPv4 dotted notation. In addition, the `access-list` command supports the CIDR format for both IPv4 and IPv6, for example:

```
access-list 1 permit 10.14.36.48/15
access-list 1 permit fd16:e32:da22:f02::/94
```

IPv6 supports only the classless CIDR format.

The `access-list` command also supports IP ACL wildcard masks (for IPv4 only) in the earlier "extended IP ACL" or "dotted" format. For example, the following ACL entries are equivalent, since /24 = 0.0.0.255.

```
access-list 10 permit 1.2.3.4/24
access-list 10 permit 1.2.3.4 0.0.0.255
```

Be careful not to confuse this with a subnet mask. The wildcard mask is an inverse of a subnet mask.

As you define an access list, remember that entries are compared in the same order as they are defined. This can result in some unintended permissions or denials. For example, access list 5 has the following entries:

```
access-list 5 deny 10.15.1.0 0.0.0.255
access-list 5 permit 10.15.2.0 0.0.0.255
access-list 5 deny 10.15.2.0 0.0.0.15
```

You then apply this list to connect to the DarkStar system with the command `access-class 5 in`. The following addresses would be permitted or denied as follows.

- `10.15.1.99` would match the first entry and be denied.
- `10.15.2.6` matches both the second and third entries. Since the first entry it matches grants permission, it would be allowed, even though the next entry would have denied it.
- `10.15.3.16` would be denied, since it does not match any entry.

The code example at the end of this section shows definitions for four sample ACLs.

Syntax

`CONF#` [no] **access-list** *list-number* **{deny|permit}** *ip-address mask*

Parameters

list-number	Assigns a number to identify the access list rule.
{deny|permit}	`permit` allows traffic from this address. `deny` prevents traffic from this address.
ip	Specify the beginning IP address in the access list.
mask	Define an IP wildcard mask to specify the end IP address in the access list.
no	Disables an access list.

Example

```
localhost CONF# access-list 1 permit fd16:e32:da22:f02::/64
localhost CONF# access-list 1 deny 2.2.2.2/0
localhost CONF# access-list 10 permit 192.168.254.250/29
localhost CONF# access-list 99 permit 10.14.1.0/24
```

6.2.1.2 access-class

Specifies an access class through which to filter network access.

Syntax

`CONF-LINE-<VTY|CTY>#` [no] **access-class** *list-number* **{in|out}**

Parameters

list-number	Assign the line to be accessible only to connections in the access list identified by *list-number*.
in|out	• **in** - filter Telnet/SSH connection requests to DXMOS, based on the source IP address. • **out** - filter ability to Telnet out of the box (from DXMOS), based on destination IP address.
no	Disables an access class.

6.2.1.3 show running-config access-list

Displays the `running configuration access list`. The command syntax changes slightly depending on the DarkStar mode.

Syntax

`#` **show running-config access-list**

Example

```
localhost# show running-config access-list
running-config:
access-list 1 deny 10.14.16.98/32
access-list 1 permit fd16:e31:da22:f01:2a0:e3ff:fe00:2e1/128
access-list 50 permit 172.30.255.210/32
```

6.2.2 Logins and Passwords

When you create user accounts, you need to specify usernames and passwords. You can also specify if a user has access to enable mode and how long a session can remain idle before timing out.

There are potentially three types of passwords you can specify:

- the password unique to each user for login,
- an anonymous password that everyone uses (no username required), or
- a password that everyone must use to access enable mode (in addition to their unique and/or anonymous password).

To assign an anonymous password, use the password command.

Anonymous passwords are not secure and can seriously compromise your system. XKL recommends creating a unique user account for each person who will be accessing the system.

The flow for setting up user accounts is typically:

1. Create accounts with user. Specify the username, password, and encryption type of the password.
2. Set a password to enter enable mode using enable secret.
3. Use **login [local]** to allow remote logins via the VTY lines and the console line. For more information, see login.
4. Enable Telnet, SSH, or both using transport input.
5. Set how long a session is idle before it times out with session-timeout.

If you choose to use AAA security features, passwords and logins can be overridden by aaa new-model.

6.2.2.1 user

Creates a user account for logging in to the DarkStar system. You can also specify a password that allows a user to login both remotely and from the console.

	To enable user accounts, use the `login local` *command or set up AAA services.*

Syntax

`CONF#` [no] **user** *username* **password** [0|5] *password*

Parameters

username	Sets the name for the new account to username, which may contain only letters, digits, and a hyphen (-).
[0|5]	Sets password input type. If the value is 0, *`password`* is treated as a plaintext string. If the value is 5, *`password`* is treated as an MD5-hashed password. The default is 0
password	Specifies the password for the account.
no user username	Removes *`username`* and its associated password from the local user database.

6.2.2.2 password

Enforces password-protected access to console or VTY lines. A user can have two different passwords: one for remote access, and a different one for console access. DXMOS will accept weak passwords, but prints a warning. Recommended password guidelines are:

1. Contain at least eight characters.
2. Contain at least three of the following:
   - One upper-case character (A, B, C, etc).
   - One lower-case character (a, b, c, etc).
   - One numeric character (0, 1, 2, etc).
   - One special character (!, @, #, etc).

	aaa new-model *overrides passwords set with this command.*

Syntax

`CONF-LINE-<VTY|CTY>#` [no] **password** [0|5] *password*

Parameters

password	Sets the password for the line to `password`. DarkStar systems automatically encrypt a plaintext password as an MD5 hash before storing it.
password 5 *password*	Specifies password as an MD5 hash.
password 0 *password*	Specifies plaintext password. This syntax is equivalent to `password password`.
no	Removes password protection from the line. Removing the VTY password disables all VTY access.

6.2.2.3 enable secret

Sets a password to control access to the DarkStar enable mode.

The only way to clear the enable mode password (for example, if you lose the password), is to call XKL technical support at (U.S.) (866) 949-8340 or (outside U.S.) +1 (608) 807-0033.

Syntax

`CONF#` [no] **enable secret** [0|5] *password*

Parameters

password	Sets the password for enable mode. The DarkStar system automatically encrypts a plaintext password as an MD5 hash before storing it.
enable secret 5 *password*	Specifies a password as an MD5 hash.
enable secret 0 *password*	Specifies a password in plaintext. This command is equivalent to `enable secret password`.
no enable secret	Clears the password and allows user to enter enable mode without a password.

6.2.2.4 login

Enables or disables login from the username/password database. Table 6-2 describes how login behavior varies, depending on which mode you are in.

TABLE 6-2. Login Command Behavior

Prompt/Command	Behavior
`CONF-LINE-VTY#` **login** local	Subsequent new Telnet/SSH sessions will require a user and password from the local database. If there is no user/password set up in the local database, you will not be able to get to a prompt.
`CONF-LINE-VTY#` **login**	A "login" without "local" enables an anonymous login (no user name requested) using the password that was set with the password command. If no password was set, the Telnet/SSH session will end without any prompts.
`CONF-LINE-CTY#` **login** local	Subsequent new console sessions will require a user and password from a local database. If there is no user/password set up in a database, you will not be able to get to a prompt.
`CONF-LINE-CTY#` **login**	After setting a password (with the password command), "login" without "local" enables an anonymous login (no user name requested) using the password that was set. If no password is set, each new console session will start with a prompt without asking for a user name or a password.

VTY lines refuse Telnet connectivity attempts until VTY login is enabled or AAA new-model is set. Logins are always enabled for the console line.

If you use `login local`, then exit without defining any usernames or passwords, you can lock your self out of your system.

- Login settings are overridden by AAA rules when aaa new-model is used.
- VTY lines must have a password set before Telnet or SSH access is granted, unless aaa new-model or `login local` is set with a user database.
- To use stored usernames and passwords with the `local` option, users must first be created with the user command.

Syntax

`CONF-LINE-<VTY|CTY>#` [no] **login** [local]

Parameters

login [local]	Enables logins for VTY lines or CTY line, using stored usernames and passwords for authentication.
no login [local]	Disables logins for VTY lines or CTY line.

6.2.2.5 transport input

Enables or disables Secure Shell (SSH) and Telnet access to VTY lines. **Note:** A configuration change on any VTY line will be applied globally to all VTY lines.

To completely disable logins through VTY lines, use the `no login` *and* aaa new-model *commands.*

Syntax

`CONF-LINE-VTY#` [no] **transport input** [all|ssh|telnet]

Parameters

all	Allows VTY access via both Telnet and SSH.
ssh	Allows VTY access via SSH only.
telnet	Allows VTY access via Telnet only.
no transport input	Disables SSH and Telnet access. The default setting.

6.2.2.6 session-timeout

Specifies the number of minutes until an idle console session (CTY mode) or idle virtual session (VTY mode) times out. By default there is no timeout.

Syntax

`CONF-LINE-CTY#` **session-timeout** *n*

`CONF-LINE-VTY#` **session-timeout** *n*

Parameters

n	Specifies number of minutes until idle session times out and logs you out of the session. Set *n* to zero to return to the default setting (no timeout).

6.2.3 Preparation for Remote Security

If you want to use some form of remote security (for example, AAA), you need to specify the location and server key for the RADIUS or TACACS+ server.

6.2.3.1 radius-server host

Adds or removes a RADIUS host server to be used with AAA.

- When adding a server, you can optionally specify an authorization port, an accounting port, or a RADIUS server key.
- When removing a server, specify only the server host name or IP address.

Syntax

`CONF#` [no] **radius-server host** [auth-port *port*]

`CONF#` [no] **radius-server host** [acct-port *port*]

`CONF#` [no] **radius-server host** [key *host-specific-key*]

Parameters

host	Specifies the hostname or IP address of a RADIUS server. If multiple RADIUS servers are specified, the DarkStar system will use that configuration order when attempting authentication and authorization.
auth-port port	Specifies a host-specific authorization port.
acct-port port	Specifies a host-specific accounting port.
key *host-specific-key*	Specifies a host-specific RADIUS server key. The key must be the last entry on the command line.
no radius-server host *host*	Removes a RADIUS server.

Example

```
localhost CONF# no radius-server host 10.15.1.99
localhost CONF# radius-server host 1.1.1.1 key somekey
localhost CONF# radius-server host 2.2.2.2 key anotherradiuskey
```

6.2.3.2 radius-server key

Specifies the encryption key on the RADIUS server.

- If you have several RADIUS servers and they all have the same encryption key, you can specify a global shared encryption key for all of them.
- If you specify a host-specific key, it will override the global-shared-key. Define a host-specific key using the `radius-server` host command.

Syntax

`CONF#` [no] **radius-server key** *global-shared-key*

Parameters

global-shared-key	A text string. The key must match the encryption key on the RADIUS server. Since spaces are allowed but the leading space is ignored, specify the key as the last item of the radius-server host configuration. Do not use quotes if you use spaces in your key, unless the quotation marks are part of the key.
no radius-server key	Clears the encryption key.

6.2.3.3 tacacs-server host

Adds or removes a TACACS+ host server to be used with AAA.

- When adding a server, you can optionally specify a TACACS+ server key.
- When removing a server, specify only the server host name or IP address.

Syntax

`CONF#` [no] **tacacs-server host** [`key` *host-specific-key*]

Parameters

host	Specifies the hostname or IP address of a TACACS+ server. If multiple TACACS+ servers are specified, the DarkStar system will contact them in the order specified.
`key` *host-specific-key*	Specifies the host-specific TACACS+ server key.
no tacacs-server host *host*	Removes the specified TACACS+ host server.

6.2.3.4 tacacs-server key

Specifies the encryption key on the TACACS+ server.

- If you have several TACACS+ servers and they all have the same encryption key, you can specify a global shared encryption key for all of them.
- If you specify a host-specific key, it will override the global-shared-key. Define a host-specific key using the `tacacs-server host` command.

Syntax

`CONF#` [no] **tacacs-server key** *global-shared-key*

Parameters

global-shared-key	A text string. The key must match the encryption key on the TACACS+ server.
no tacacs-server key	Clears the encryption key.

6.2.3.5 show hostkey

Displays the public and private DSA keys used by SSH.

Syntax

`#` **show hostkey {private|public}**

Parameters

private	Displays the private hostkey for this system.
public	Displays the public hostkey for this system.

6.2.4 AAA Security

Use aaa commands to configure authentication, authorization, and accounting (AAA) by limiting a user's privileges. When AAA authorization is enabled, a user can access enable and configure mode only if the information in their profile allows it.

Flow of setting up AAA security:

1. Enable AAA services with aaa new-model.
2. Configure security protocol parameters (RADIUS, TACACS+) with `Preparation for Remote Security` and define the list of login authentication methods with aaa authentication login default.
3. Define the list of enable mode authentication methods with aaa authentication enable default.
4. Enable or disable the authorization of commands executed on VTY or CTY, if required.
5. Configure authorization with aaa authorization commands (TACACS+ only, since RADIUS combines this with authentication.)
6. Specify who will be logged in directly to enable mode (privilege-level 1) with aaa authorization exec.
7. Configure accounting with aaa accounting commands (optional).

6.2.4.1 aaa new-model

Globally enables or disables the AAA feature.

When AAA new-model is enabled, existing sessions, including the enabling session, do not possess the credentials necessary to authenticate any subsequent commands. They continue using the authentication model already in force, until logged out. If you make any changes to the AAA configuration, those changes won't take effect until you log out and log back in.

Syntax

`CONF#` [no] **aaa new-model**

Parameters

aaa new-model	Enables AAA functionality.
no aaa new-model	Disables AAA functionality.

6.2.4.2 aaa authentication login default

Specifies a list (up to 5 entries) of databases to use for login (each database specifies which clients and users are authorized to request a login).

You may specify up to five databases to try, and they are tried in the order you have specified. If a database does not exist (e.g., no RADIUS servers), the next database is tried. As soon as a database contained in the list is found, the user is accepted or denied using that database.

Use of `none` is dangerous and should be used with extreme caution, even as a final item on a list of methods. For example, a missing username in a local database or an unreachable RADIUS server followed by `none` will give anyone access to the system.

Syntax

`CONF#` [no] **aaa authentication login default** authentication methods

Parameters

authentication methods	Specify one to five of the following:	
	enable	Use the enable password as authentication.
	line	Use the line password as authentication.
	local	Use the local name database as authentication.
	`group` radius	Uses the list of RADIUS servers for authentication.
	group tacacs+	Uses the list of TACACS+ servers for authentication.
	none	Uses no authentication. Good for verifying the server is working properly, but should be used with extreme caution (see warning below).
no	Disables the referenced AAA functionality.	

6.2.4.3 aaa authentication enable default

You can specify an hierarchy of up to five authentication methods. If the first method is not available (e.g., no RADIUS servers are up), the system will try the next method you specified, and so on. It will NOT try the next method if the previous method fails.

Use of `none` is dangerous and should be used with extreme caution, even as a final item on a list of methods. For example, a missing username in a local database or an unreachable RADIUS server followed by `none` will give anyone access to the system.

There is an important distinction between "error" and "fail." An error means that no server could be found, there was some sort of transmission problem, or something similar. On the other hand, if the requested user/password is not found in the database, that is considered a "fail".

Syntax

`CONF#` [no] **aaa authentication enable default** {authentication methods}

Parameters

authentication methods	Specify one to five of the following:	
	enable	Logins will use the enable password for authentication.
	line	Logins through the console will use the line password. Logins through the virtual terminal will require authentication.
	group radius	Logins will require RADIUS authentication.
	group tacacs+	Logins will require TACACS+ authentication.
	none	No authentication is used. This would allow login even if all specified methods returned an error.
no	Disables access to enable mode.	

Example

`localhost CONF#` **aaa authentication enable default** group radius group tacacs+

6.2.4.4 aaa authorization exec

When set, a qualified user is immediately placed in enable mode upon login. A successful authentication request for a user holding privilege level 15 results in an enabled login (TACACS+ only).

Syntax

`CONF#` [no] **aaa authorization exec default group {radius|tacacs+}**

Parameters

group radius	The user group that is configured in the Administrators group on your designated RADIUS computer.
group tacacs+	The user group that is configured in the Administrators group on your designated TACACS+ computer.
no aaa authorization exec	Disables AAA authorization functionality to direct the user to enable mode, if authorized.

6.2.4.5 aaa authorization commands

Enables or disables authorization of commands executed on a VTY session via the TACACS+ server. (By default, command authorization applies to VTY sessions only. Use authorization commands default to enable command authorization for the console session.)

- For a privilege-lowering command that does not terminate a session, such as `exit`, `end`, or `disable`, DXMOS will see TACACS+ authorization for the command and log the result, but always allow the operation to proceed. In this way, a user authorized to enter an elevated mode is not denied the ability to leave it.
- The top-level privilege-lowering commands `exit`and `logout` terminate a session. If TACACS+ denies an exit or logout command, DXMOS honors this denial. This prevents accidental logout from a session intended to be permanent. A permanent session may still be disconnected via a `clear line` command from a suitably authorized login, or externally by using the appropriate Telnet or SSH client escape sequence to break the session.

Syntax

`CONF#` [no] **aaa authorization commands** *privilege-level* **default group tacacs+**

Parameters

privilege-level	Specifies enable mode access: `0` to authorize commands from a VTY in disable mode, `1` to authorize commands from a VTY in enable mode. (This is NOT the same as the privilege level for a TACACS+ or RADIUS Administrative group.)
default group tacacs+	Set the privilege level for the user group that is configured in the Administrators group on your designated TACACS+ computer.
no	Disables AAA authorization functionality.

6.2.4.6 authorization commands default

Enables the authorization of AAA commands used in a console session.

After you have set up the configuration on the TACACS+ server, you need to enable access.

- By default, enabling AAA command authorization turns on authorization for VTY session commands, but not for the console.
- A user who has access to the console is considered to have access to the physical machine and, as such, already has privileges equivalent to root access. Use this command to turn off that access on the console.

This command forces the authorization of console commands in addition to VTY commands. Consider carefully the use of console authorization. An improperly configured system could deny access to essential management commands.

For example, you want the user Fred to have access to fan 0 only, and not have access to fan 2. The TACACS+ server configuration file might look like this:

```
user = fred {
     password = clear fred
     service = shell {
     cmd = enable {
           permit .* }
     cmd = configure { permit .* }
     cmd = fan { permit 0 }            <------ access to fan 0
     set priv-lvl = 15
     }
     }
```

At the console, the running configuration file shows that `authorization commands default` has NOT been set (in line configuration mode). Because it is not enabled, the `aaa authorization commands` statement has no impact on a console session, and Fred can access fan 2.

```
localhost CONF# do show run line

running-config:
tacacs-server host 10.22.5.89
tacacs-server key secretkey
aaa authentication login default group tacacs+
aaa authorization commands 1 default group tacacs+
aaa authentication enable default group tacacs+
aaa new-model
line console
login
break
exit
line vty
login
exit

localhost# configure
localhost CONF# fan 2
localhost CONF-FAN[2]#
```

The next example shows a running-config file using authorization commands default (enabling it). Fred can no longer access fan 2 from the console.

```
localhost CONF-LINE-CTY# do show run line

running-config:
tacacs-server host 10.22.5.89
tacacs-server key secretkey
aaa authentication login default group tacacs+
aaa authorization commands 1 default group tacacs+
aaa authentication enable default group tacacs+
aaa new-model
line console
login
authorization commands default
break
exit
line vty
login
exit

localhost# configure
localhost CONF# fan 2

localhost CONF# Service not allowed.
```

The above examples are for a console session; for a VTY session, Fred cannot access fan 2 regardless of the `authorization commands default` setting. As a result, `aaa authorization commands 1 default group tacacs+` is always in effect during a VTY session.

Syntax

`CONF-LINE-CTY#` [no] **authorization commands default**

Parameters

no	Disables the authorization of AAA commands used in a console session.

6.2.4.7 aaa accounting commands

Enables or disables AAA command accounting functionality for the specified user group and privilege level. A log file is generated that contains information about commands used by that user group/privilege level, including who issued what command, and when.

Syntax

`CONF#` [no] **aaa accounting commands** *privilege-level* **default start-stop group tacacs+**

Parameters

privilege-level	Specifies the enable mode access: `0` for commands from a disabled VTY session; `1` for commands from an enabled VTY session. (This is not to be confused with the privilege level setting in the TACACS+ configuration file.)
default start-stop group tacacs+	The user group that is configured in the Administrators group on your designated TACACS+ computer is to be used for command accounting.
no accounting commands	Disables AAA command accounting functionality.

6.2.4.8 aaa accounting exec

Enables or disables AAA accounting for session start/stops. A separate log is kept of the "start" and "stop" of each session, and another log tracks other session information (which includes user login name, date, IP address, and the originating phone number, if applicable). The two records are linked with one unique session ID.

The extra processing required for this can impact performance and should NOT be used unless it is absolutely required.

Syntax

`CONF#` [no] **aaa accounting exec default start-stop group {radius|tacacs+}**

Parameters

group radius	Enables start-stop logging for the user group that is configured in the Administrators group on your designated RADIUS server.
group tacacs+	Enables start-stop logging for the user group that is configured in the Administrators group on your designated TACACS+ server.
no	Disables AAA accounting for session starts/stops.

7

Monitoring & Troubleshooting

DXMOS provides several ways to monitor your DarkStar system: 1) you can enable basic logging of system events, 2) test fiber with the OTDR, 3) set up SNMP traps, and 4) use `checksum` and `bert logging` to check for quality.

Monitoring commands:

- checksum
- logging
- OTDR Commands
- snmp-server and snmp-traps

Troubleshooting commands:

- BERT Commands
- clear
- Diagnostic Commands and show debug
- laser shutdown
- loopback
- ping, ping6
- reboot
- reload
- show memory
- show memory counters management
- show tech-support
- shutdown

In addition, the LED displays on the front panel can give a good indication of where to begin troubleshooting. There are a set of power-related LEDs, and a set of amplifier/protection (depending on your DarkStar configuration) LEDs.

Note: The following information about the LED displays can also be found in the Troubleshooting chapter of the Systems Guide on the XKL website.

7.1 checksum

For a given file, this command calculates and reports on checksums according to the MD5 hashing and the BSD cksum algorithms, based on the contents of a file. This value is used to verify the file, and can be used to detect corruption, mislabeling, and so on. This is most helpful when verifying that a file was transferred correctly over TFTP to or from the system, by comparing the `checksum` at both sides of the transfer.

The `checksum` reports both a 16-bit (2 byte) sum and a 128-bit (16 byte) MD5 sum.

Syntax

`#` **checksum** *filename*

Parameters

filename	The file to be checked.

7.2 logging

Configures the logging of DarkStar system events in the local circular logging buffer.

The contents of the local circular logging buffer are lost upon system reload.

Syntax

`CONF#` [no] **logging** **{buffer** *events*|**host** *address*|**mark** *syslog mark interval in minutes*|**rate-limit** *limit***}**

Parameters

buffer *events*	Sets the maximum number of events to store in the local circular logging buffer, and turns on logging. Values range from 1 to 10,000. Enabled by default to display 512 events. When the maximum number of specified events (i.e., log entries) is reached, older entries are removed to make room for the newer ones. For example, consider a log that is configured to hold 200 entries. If this log currently holds 100 entries, there will be room for another 100 entries before the log rolls over. If there are 105 events to be added to the log, the original list will discard the oldest (first) 5 entries to make room for the 105 new entries. Alternatively, if the user decreases the number of available entries to 50, only the most recent 50 entries are preserved.
no logging buffer, **logging buffer** *0*	Clears the contents of the local circular logging buffer.
host *address*	Sets `address` as the host to receive syslog messages, and turns on syslog message generation. Use multiple host logging commands to specify multiple hosts. The `no logging host address` command stops syslog logging to the specified host.
rate-limit	Sets the message rate limit in messages per second. Valid range for limit is 0-10000. The rate limit applies only to syslog logging.
syslog mark interval in minutes	Sets the mark interval. The DarkStar system sends a "mark" time-keeping message to syslog hosts at this interval. Valid range is 0-60 minutes.
no logging mark, **logging mark** *0*	Turn off mark event generation. **Note:** Marks show up only at syslog hosts, not in the local logging buffer.

7.2.1 Viewing Buffer Setup and Contents

The commands for viewing the setup and contents of the system event buffer are very similar, and have several syntax formats, depending on the permission level. Table 7-1 lists the commands and their variations.

TABLE 7-1. Logging Display Commands

Displays	Mode Prompt	Command/Syntax
Contents of system event buffer	#	show logging
	CONF#	do show logging
Running configuration of system event buffer	#	show running-config logging
	CONF#	show logging
	CONF#	do show running-config logging

7.2.2 show logging

Displays the contents of the system event logging buffer. Syntax varies slightly depending on the permission level.

Syntax

`#` **show logging**

`CONF#` **do show logging**

Example

```
localhost# show logging

Sep 27 15:52:57:190: System Warm Reload
Sep 27 15:52:57:407: Power Supply 1 is absent (0xB4)
Oct  5 09:09:09:793: Link Down: Management interface OSC 0
Oct  5 09:09:10:757: Link Up: Management interface OSC 0
.
.
.
```

7.2.3 show running-config logging

Displays the running configuration of the system event buffer. Command syntax varies slightly depending on the permission level.

Syntax

`#` **show running-config logging**

`CONF#` **show logging**
`CONF#` **do show running-config logging**

Example

`CONF#` **logging buffer** *200*
`CONF#` **do show running-config logging**

```
running-config:
logging host 10.15.1.99
logging buffer 200
```

7.3 OTDR Commands

An OTDR (Optical Time Domain Reflectometer) device is able to measure the length of an optical fiber.
Note: These commands are available only in systems that include an OTDR-capable OSC transceiver.

There are two main reasons to use an OTDR integrated into a DarkStar product:

- A customer may experience a fiber break or cut somewhere in their network. If the fiber with the break is attached to a DarkStar system at its OTDR-capable transceiver, then DXMOS can report where the break has occurred.
- A customer can also perform an initial deployment OTDR to record the initial condition of their fiber, the information of which will be stored in the OTDR log.

Phantom Readings

The OTDR may report multiple readings in the fiber, locations where a reflection exceeds a threshold. Connectors and poor splicing along the fiber can produce this. Typically, the furthest reading is of interest, as it will be the location of a break in the fiber or the end of the fiber.

The OTDR launches a high power pulse into the fiber in order to detect faults that are as far away as possible. The drawback of this is the difficulty in detecting nearby faults.

To assess the correct distance to the fiber break when the distance is less than 35km:

1. Compare the furthest OTDR reading to the 2nd furthest reading. If the furthest reading is twice the 2nd furthest reading, and the 2nd furthest reading is less than 35km, then the furthest reading is called a phantom reading. It is under such conditions that DXMOS may report the possibility of a phantom reading for fiber breaks within the first 35km of the link.

2. Discard the furthest reading, the phantom. The 2nd furthest reading is the true location of the fiber break or the end of the fiber.

Another way to verify the presence of a break is to issue the `otdr` command from the downstream DarkStar system. This command will report the readings on the return fiber, which is not the same fiber. Nevertheless, if there is a break in the fiber, there is a high probability that both fibers have been broken at the same location.

7.3.1 otdr

Used to test the fiber and return the measured fiber length. The `otdr` command can be run *n* times, where *n* is an integer from 1 - 20. The default is n=1.

Requesting a fiber length measurement via the OTDR feature will disrupt the management OSC.

Syntax

`CONF-MOD-OSC[n]#` **otdr** [*n*]

Example

```
localhost CONF-MOD-OSC[0]# otdr
 Warning! Operating the OTDR feature will temporarily disrupt the
 management OSC on this system and the connected DarkStar system.
 Are you sure? [yes/NO] yes

 OTDR OSC[0] Results: 55.00km
```

Notes:

- The `otdr` command will interrupt the DarkStar OSC management traffic if it has been configured. Expect to see error messages from the connected (downstream) DarkStar system as well as the system where the `otdr` command is issued. Messages such as: `Management interface OSC 0 line is down` and `Management interface OSC 0 line up.`
- Whenever the `otdr` command is run, the results are sent to volatile memory (i.e., RAM), and will be cleared after a reboot. Up to 512 closest events can be logged in memory. The closest reading along the fiber link is the first one in the list, followed by increasingly distant readings.

```
CONF-MOD-OSC[0]# otdr
Warning! Operating the OTDR feature will temporarily disrupt
the management OSC on this system and the connected DarkStar system.
Are you sure? [yes/NO] yes
***OTDR Run: 1/1Management interface OSC 0 line is down.
OTDR osc[0] Results: 5.61km 11.20km*
* 11.20km may be a phantom reading, see the Command Ref for details.
localhost CONF-MOD-OSC[0]# Management interface OSC 0 line up
Management interface OSC 0 line is down.
Management interface OSC 0 line up
```

7.3.2 show otdr (enable mode)

Reports the results of previously exercised OTDR measurements, as follows:

- If no measurement has been made since last power cycle, then `Not Measured` will be reported.
- If the report is `No Reflections Detected in Fiber`, then either no fiber was attached to the DarkStar system or the length of fiber was too long to measure.

Important: The `show otdr` command will neither run the OTDR nor will it interrupt the OSC connection to the adjacent DarkStar system.

Note: The `show otdr` or `show otdr osc` commands will report the results of previously exercised OTDR measurements of all OSCs.

Syntax

`#` **show otdr** [logging|osc *n*]

Parameters

logging	Reports the results of all exercised OTDR measurements of all OSCs.
osc *n*	Reports the results of previously exercised OTDR measurements of OSC *n*.

Example

```
localhost# show otdr

OTDR osc[0] Results: 55.00km
OTDR osc[1] Results: Not Measured
```

7.4 snmp-server

Configures SNMP settings and specifies where to send the SNMP traps. For a trap to be sent to a host, either the global SNMP community must be set, or a host-specific community must be set.

DarkStar systems support both the SNMPv1 and SNMPv2c versions of SNMP. To monitor detailed DarkStar system status, use the XKL-proprietary SNMP management objects and traps defined in the current XKL MIB, which can be obtained from the XKL website.

To monitor a DarkStar system using SNMP, first configure your monitoring system to recognize XKL-specific traps and to access XKL management objects in the SNMP database. Then you can configure the DarkStar SNMP settings and enable asynchronous alarms and alerts ("traps").

Use the `snmp-server` command to configure SNMP settings and enable SNMP traps. The flow for setting up SNMP is shown next.

1) The `community` *`string`* argument is required to set up monitoring.

```
localhost# configure
localhost CONF# snmp-server community string
```

2) Then set up trap generation.

```
localhost CONF# snmp-server host address [Community Name]
localhost CONF# snmp-server enable traps [snmp|xkl|xkl-generic]
```

Syntax

`CONF#` [no] **snmp-server {community** *string*|**contact** *string*|**location** *string*|**chassis-id** *string*}

`CONF#` [no] **snmp-server enable traps** [snmp|xkl|xkl-generic]

`CONF#` [no] **snmp-server disable-v2c**

`CONF#` [no] **snmp-server host** *address* [*Community Name*]

Parameters

chassis-id *string*	A name to help identify the SNMP server. Up to 254 characters.
community *string*	Start a read-only SNMP agent using the community string specified by `string`.
no snmp-server community	Turns off the SNMP agent.
contact *string*	Set SNMP-retrievable contact information to the value of `string`. This value may be accessed through the SNMP variable `SNMPv2-MIB:sysContact.0`.
no snmp-server contact	Sets `contact string` to an empty string.
enable traps [snmp|xkl|xkl-generic]	Turn on sending of SNMP traps. (A host address is also required.) If no traps are specified, they are all turned on. • `snmp` - Turn on only SNMP standard traps • `xkl` - XKL-specific traps (listed in Table 7-2) • `xkl-generic` - A set of cloned standard SNMP traps (listed in Table 7-3)
no snmp-server enable traps [snmp|xkl|xkl-generic]	Disable sending of SNMP traps. You can disable all traps, or only a specific category of traps.
disable-v2c	Disables the use of SNMP version 2c.
no snmp-server disable-v2c	Allows the use of SNMP version 2c.
host *address*	Send SNMP traps to a specific host, specified by `address`, which is either a hostname or an IP address. Multiple hosts may be specified, but only one per invocation of this command.
host address [Community Name]	Specify a `Community Name` to cause traps to use this community string rather than the global `community string` specified for SNMP read operations.
no snmp-server host	Remove an existing target host.
location *string*	Set SNMP-retrievable location information to the value of `string`. This value may be accessed through the SNMP variable `SNMPv2-MIB::sysLocation.0`.
no snmp-server location	Set `location string` to an empty string.

A list of XKL-specific trap types is found in Table 7-2.

TABLE 7-2. XKL-specific Trap Types

Trap Type	Event
xklFanFail	Fan module fault or failure.
xklPowerFail	Power supply module fault or failure.
xklFanUp	Fan module has come online.
xklPowerUp	Power supply module has come online.
xklProtectionPathSwitch	Protection path transition has occurred.
xklTempStatusChange	Temperature status has changed
xklEDFALineChange	EDFA line state has changed.
xklRamanLineChange	Raman line state has changed.
xklEDFAAlarmChange	EDFA alarm/warning state has changed.
xklRamanAlarmChange	Change in Raman alarms/warnings state.
xklPowerSupplyAdded	Power supply module added to the system.
xklPowerSupplyRemoved	Power supply module removed from the system.
xklTransceiverAdded	Transceiver added to the system.
xklTransceiverRemoved	Transceiver removed from the system.

A list of XKL-generic trap types is shown in Table 7-3.

TABLE 7-3. XKL-Generic Trap Types

Trap Type	Event
xklColdStart	System reload due to hard reset or power cycle.
xklWarmStart	System reload due to soft reset, system fault or operator command.
xklLinkDown	Interface entered down state.
xklLinkUp	Interface entered up state.
xklTransportLinkDown	Transport interface entered down state.
xklTransportLinkUp	Transport interface entered up state.

Table 7-4 shows the SNMP standard traps supported by XKL systems.

TABLE 7-4. SNMP Standard Traps

Trap Type	Event
coldStart	A coldStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered.
warmStart	A warmStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself, such that its configuration is unaltered.
linkDown	A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.
linkUp	A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.
authenticationFailure	An authenticationFailure trap signifies that the SNMP entity has received a protocol message that is not properly authenticated. While all implementations of SNMP entities MAY be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.

7.5 snmp-traps

Enables /disables SNMP traps for an OSC, Ethernet, or transport interface. By default, traps are enabled. Only the disabling of SNMP traps (`no snmp-traps`) is written to the configuration file (see the example below).

SNMP traps are configured at the interface level (`eth`, `osc`, `loopback`, `client`, `wave`, etc.).

Syntax

`CONF-MOD-<CLIENT|OSC|WAVE>[n]#` [no] **snmp-traps**

`CONF-MGMT-<ETH|OSC|LOOP>[n]#` [no] **snmp-traps**

Parameters

no	Disables SNMP traps on the interface.
snmp-traps	Reinstates SNMP traps.

Note: For modules with multiple optical lanes, the `n/lane` keyword will enable a user to specify a lane. Depending on the system and transceivers used, there may be a number of configurations for lane counts.
Example: `CONF-MOD-CLIENT[0/1]# snmp-traps`

Example

```
localhost CONF# module client 0
localhost CONF-MOD-CLIENT[0/*]# no snmp-traps
localhost CONF-MOD-CLIENT[0/*]# do show run module client 0

running-config:
module client 0/0
no laser shutdown
no snmp-traps
exit
module client 0/1
no laser shutdown
no snmp-traps
exit
module client 0/2
no laser shutdown
no snmp-traps
exit
module client 0/3
no laser shutdown
no snmp-traps
exit
```

7.5.1 show running-config snmp

Displays current SNMP status, including the IP address and last sync time of the currently selected SNMP server.

Syntax

`#` **show running-config** snmp

Example

```
localhost# show running-config snmp
running-config:
snmp-server community public
snmp-server contact John Doe
snmp-server location Seattle
snmp-server enable traps snmp
snmp-server enable traps xkl
snmp-server enable traps xkl-generic
snmp-server host 10.15.1.99
```

7.6 BERT Commands

The Bit Error Ratio Test or BERT is a method for testing a digital communication channel where a known PRBS (Pseudo Random Bit Stream) pattern emitted by a transmitter is checked by a receiver. Use BERT to test optical cables and/or connections between systems.

BERT PRBS patterns transmitted from one DarkStar system can be received by any other system that is using the same PRBS pattern, not just DarkStar systems. There are framed PRBS signals and unframed PRBS, so they must also match up. For example, a framed PRBS signal cannot be received by an unframed PRBS receiver.

Notes:

- BERT is available on select DarkStar systems, though system setup can differ. For example, you can run BERT on both the line side (i.e., waves) and client side for DQ*10 systems, but only on the line side for the DQ*400. Refer to the Systems Guide on the XKL website for more information.
- The PRBS signal that is available in DarkStar systems is not configurable by the user. If the source provides framed PRBS, then it cannot be changed to support unframed PRBS. Similarly, the PRBS pattern is not configurable by the user (although a pattern is selected by DXMOS).

7.6.1 bert log

The BERT log mechanism records BERT activity to the file system (i.e., the `log/bert/` folder). Additionally, it periodically checks the lines targeted for BERT receive and records their condition to flash memory whenever the bit error count has changed.

Syntax

`CONF#` **bert log** *interval*

`CONF#` **no bert log**

Parameters

interval	Specifies the interval in minutes that the BERT logging mechanism will check for errors on the module targeted for BERT receive. **Note:** Messages are only added to the log file when the number of bit errors has changed since the last time BERT was running on the module.

7.6.2 bert transmit

Initiates transmission of BERT/PRBS on the module specified by `CONF# module {wave|client}`.

Notes:

- Supported data rates for BERT can vary by DarkStar system. From the appropriate CONF# module prompt (e.g., `CONF-MOD-WAVE[n]#`), type the `encapsulation` command followed by pressing the tab key to open help for your DarkStar system. After selecting a data rate, try the `bert transmit` command. DXMOS will inform you if that encapsulation is supported on your system.
- For details about BERT, see the Systems Guide on the XKL website.

Syntax

`CONF-MOD-WAVE[n]#` [no] **bert transmit**

`CONF-MOD-CLIENT[n]#` [no] **bert transmit**

Example

```
local host CONF-MOD-WAVE[3]# bert transmit

BERT transmission started on Wave 3.
```

Example

```
local host CONF-MOD-WAVE[3]# no bert transmit

BERT transmission stopped on Wave 3.
```

Parameters

no bert transmit	Cancels BERT/PRBS transmission on the selected module. **Note:** `no bert transmit` will fail if the module is not already running `bert transmit`.

	Depending on the client mode you specify, bert transmit and bert receive commands apply differently: • *In* `CONF-MOD-CLIENT[n]#` *mode, the bert transmit and bert receive commands apply to all four lanes of the module.* • *In* `CONF-MOD-CLIENT[n/0-3]#` *mode, the bert transmit and bert receive commands apply only to the lane specified as 0, 1,2, or 3 in the prompt.*

7.6.3 bert receive

Initiates reception of BERT/PRBS on the module specified by `CONF#` **module {wave|client}**.

Note: For details about BERT, see the Systems Guide on the XKL website.

Syntax

`CONF-MOD-WAVE[n]#` [no] **bert receive**

`CONF-MOD-CLIENT[n]#` [no] **bert receive**

Parameters

no bert receive	Cancels BERT/PRBS reception on the selected module and generates final test results. **Note:** `no bert receive` will fail if the module is not already running `bert receive`.

7.6.4 bert restart

Clears the BERT receive counters.

Note: If a Loss of Lock (LOL), Loss of Signal (LOS), or Loss of Sync is asserted, all BERT receive counters will continue to accumulate, and may potentially overflow, so issue the `bert restart` command to clear these counters. There is no need to restart `bert receive` once the alarm condition is deasserted, however.

Syntax

`CONF-MOD-WAVE[n]#` **bert restart**

`CONF-MOD-CLIENT[n]#` **bert restart**

7.6.5 show bert

Lists all modules running BERT. Can be used on any module to obtain results up to the time the command was issued. **Note:** For details about BERT, see the Systems Guide on the XKL website.

Syntax

`>` **show bert**

Example

`localhost>` **show bert**

```
   Module     BERT Rx/Tx   BERT Time    Status Bits Rec Errors    BER      Rate
------------ ---------- ------------ ------- -------- ------ ------- --------
Wave 0            Off/On 00d 00:00:00     N/A        0      0     N/A  400Gb/s
Wave 2             On/On 00d 00:01:35      OK   4.3e09 5.8e08 1.3e-01  400Gb/s
Wave 3             On/On 00d 00:01:55      OK   2.7e10      1 3.7e-11  400Gb/s
Wave 4             On/On 00d 00:02:10  LOS/LOL  4.0e15 4.0e15  1.0e00  400Gb/s
Wave 5             On/On 00d 00:01:50  SyncErr  1.0e10 1.0e04 1.0e-06  100Gb/s
```

7.6.6 show bert log

Displays, on the console, the current BERT log file. For each BERT log entry, the log file lists the timestamp, event message, module name, and the number of errors that have occurred over an interval, if reporting on a BERT receive. **Note:** For details about BERT, see the Systems Guide on the XKL website.

Syntax

> **show bert log** [all|recent <count>|status]

Parameters

all	Shows all the events in the log. Typically, this is the maximum of 4000 events, and it may take some time to print. **Note:** The "events" are the same as in **show bert log** recent <count>.
recent <count>	Shows the count of the most recent events in the log. The default is 20 events. The <count> must be greater than or equal to zero.
status	Shows the status of the BERT log. The output shows if logging is enabled, the interval at which the receivers are checked, and the number of events in the log.

Example

```
localhost> show bert log recent
Fri Dec 3 2021 08:41:53: System rebooted
Fri Dec 3 2021 09:45:15: System rebooted
Fri Dec 3 2021 17:07:21: Start BERT transmit on Wave 0
Fri Dec 3 2021 18:08:28: Start BERT receive on Wave 0
Fri Dec 3 2021 18:09:22: BERT report on Wave 0: 0 errors in 54 seconds
```

7.7 clear

There are several `clear` commands that reset or delete DXMOS operational data. For example, the `clear arp-cache` command deletes ARP table entries for all Ethernet interfaces. Clearing a system cache such as ARP, DNS, or RIP has the effect of refreshing the cache, since the cache will repopulate as the next host or IP address updates occur.

Clearing a client or wave transceiver resets the optical hardware and causes some loss of customer traffic. Clearing an OSC transceiver may cause the loss of some management traffic.

The `clear` commands include:

- clear arp-cache
- clear amplifier
- `clear bert`
- `clear bert log`
- clear counters
- clear host
- clear line
- clear logging
- clear management
- clear module
- clear rip

7.7.1 ARP (Address Resolution Protocol) Cache

The ARP cache is an internal table that is used to map IP addresses to the correct Ethernet MAC address. This table (cache) is built as connections are made and addresses are added. Over time, this cache can get quite large, and is periodically purged of addresses that have not been used recently.

If you are having issues with network connectivity, the ARP cache is one place to look. Occasionally, addresses get corrupted and prevent connections. You can look for incomplete or malformed addresses by using the `show arp` command. Sometimes it's necessary to clear the cache and effectively start over, but be aware that clearing the cache can cause some interruptions in data transmission.

7.7.1.1 clear arp-cache

Clears the DarkStar system ARP cache. Use the `show arp` command to view the ARP cache contents.

Syntax

`#` **clear arp-cache**

7.7.1.2 show arp, show ip arp

Displays the ARP cache for Ethernet modules. Without an identifier, displays the cache for all modules.

Syntax

`>` **show arp** [*ip-address*|*hostname*]

`>` **show ip arp** [*ip-address*|*hostname*]

Parameters

ip-address	The IPV4 address of the module for which you want to display the cache.
hostname	The host name for which you want to display ARP cache.

Example

```
localhost# show arp

? (10.16.1.89) at f0:2f:af:e0:de:52 on Ethernet 0     <----- ARP entry
localhost show ip arp

? (10.16.1.89) at f0:2f:af:e0:de:52 on Ethernet 0     <----- IP ARP entry
```

7.7.2 clear amplifier

Resets the specified amplifier.

Traffic on an amplifier will be briefly disrupted by the clear amplifier command

Syntax

`#` **clear amplifier** amplifier-label

7.7.3 clear bert

Turns `bert transmit` and `bert receive` off on all modules. A message is printed for each module and direction that is stopped.

Syntax

`#` **clear bert**

7.7.4 clear bert log

Erases all the entries in the BERT log. It then adds a first message saying that the log has been cleared. The log indexes will start over from 1. This command will prompt for confirmation before running, It may take a while, however, and confirms by completing without error.

Syntax

`#` **clear bert log**

7.7.5 clear counters

Resets packet and byte counters for the specified module. Example: `clear counters management ethernet 0`. Without arguments, `clear counters` clears all counters displayed by the `show (module|management|vif)` command.

Syntax

`#` **clear counters management {ethernet** *n***|osc** *n***|switch}**

`#` **clear counters module** [client *n*|osc *n*| trunk|wave|all]
`#` **clear counters vif** [all]

Note: For modules with multiple optical lanes, the `n/lane` keyword will enable a user to specify a lane. Depending on the system and transceivers used, there may be different configurations for lane counts. Example: `# clear counters module client 0/1`

Important: The `switch` command parameter is available only on CMD based systems. To determine whether the `switch` parameter is available on your system, issue the `show hardware` command. If the system is CMD based, the `switch` command parameter is available.

Parameters

management {ethernet *n*|**osc** *n*|**switch}**	The Ethernet interface on which to clear counters. The `clear counters management ethernet` *n* command: • When *n* equals 0, the command clears the counters on the internal Ethernet port 0. • You can also use this command to clear the counters of an OSC transceiver. Depending on system configuration, *n* can be from 4–7, the values representing the internal ports of one or more installed OSC transceivers. **Note:** For systems with the `switch` parameter, values for `ethernet` *n* from 1–3 are invalid. The `clear counters management osc` *n* command: • Clears the counters of an OSC transceiver. Depending on system configuration, *n* can be from 0–3, the values representing the internal ports of one or more installed OSC transceivers. **Note:** The `clear counters management osc` *n* command is equivalent to the `clear counters management ethernet` *n* command, where *n* is within the applicable OSC-value range for the respective commands. For example, the port for `osc` ***0*** is the same as the port for `ethernet` ***4***; the port for `osc` ***1*** is the same as the port for `ethernet` ***5***, and so on. The `clear counters management switch` command: • For systems equipped with the switch feature, clears the counts of various kinds of packets sent and received on the Ethernet switch's external ports (E0 - E3) and the count of various kinds of packets sent and received by this DarkStar system. **Note:** The Ethernet switch acts as a Layer-2 switch, managing the DarkStar system's four front-panel Ethernet ports (E0–E3) to which copper LAN cables connect.
module [client *n*|osc *n* | trunk|wave *n*]	The transceiver on which to clear counters.
`vif`	Virtual interfaces
all	Clear counters on all of the specified type (management, module, or vif).

7.7.6 clear host

Clears the system DNS cache that maps network host names to IP addresses.

There are a number of reasons you might want to clear the cache. Among them:

- You've made security changes to running-config, and want to assure those changes are applied to all connections.
- An IP address has gone out of date or changed for some reason.
- An address has been entered incorrectly.

Syntax

`#` **clear host**

7.7.7 clear line

Immediately disconnects the terminal session on the designated console or VTY line.

- *The console session will reconnect immediately.*
- *Use the* show lines *command to see which lines are currently connected.*

Syntax

`#` **clear line** *line-number*

Parameters

line-number	The line session to terminate. Console session = `0`, VTY sessions are `1-4`.

7.7.8 clear logging

Clears the DarkStar system event log buffer. This can help prevent confusion when debugging an issue.

Syntax

`#` **clear logging**

7.7.9 clear management

Resets the specified management module or all modules of the given class if a particular module is not specified. This may be useful if a system becomes unresponsive. Example: `clear management osc 0`.

Traffic on a management interface will be briefly disrupted by the clear management command.

Syntax

`#` **clear management** [ethernet *n*|osc *n*|switch|all]

Important: The `switch` command parameter is available only on CMD based systems. To determine whether the `switch` parameter is available on your system, issue the `show hardware` command. If the system is CMD based, the `switch` command parameter is available.

Parameters

ethernet *n*|osc *n*|switch	Specifies the management module class to reset. The `clear management ethernet n` command: • When `n` equals 0, the command clears the counters on the internal Ethernet port 0. • You can also use this command to clear the counters of an OSC transceiver. Depending on system configuration, `n` can be from 4–7, the values representing the internal ports of one or more installed OSC transceivers. **Note:** For systems with the switch parameter, values for `ethernet n` from 1–3 are invalid. The `clear management osc n` command: • Clears the counters of an OSC transceiver. Depending on system configuration, `n` can be from 0–3. **Note:** The `clear management osc n` command is equivalent to the `clear management ethernet n` command, where `n` is within the applicable OSC-value range for the respective commands. For example, the port for `osc` ***0*** is the same as the port for `ethernet` ***4***; the port for `osc` ***1*** is the same as the port for `ethernet` ***5***, and so on. The `clear management switch` command: • For systems equipped with the switch feature, clears the counts of various kinds of packets sent and received on the Ethernet switch's external ports (E0 - E3) and the count of various kinds of packets sent and received by the DarkStar system (from which the command is issued). **Note:** The Ethernet switch acts as a Layer-2 switch, managing the DarkStar system's four front-panel Ethernet ports (E0–E3) to which copper LAN cables connect.
all	The `clear management all` command resets the Ethernet and OSC modules. It does not, however, reset the Ethernet switch (for those systems with this feature).

7.7.10 clear module

Resets the specified physical transceiver, or all transceivers of the given class if a particular transceiver is not specified. This may be useful if a transceiver becomes unresponsive. Example: `clear module client 0`

Clearing a client transceiver resets the optical hardware and causes some loss of customer traffic. Clearing a line transceiver may result in loss of traffic for up to two minutes, while the transceiver initializes itself again.

Syntax

`#` **clear module** [client *n*|osc *n*|trunk |wave *n*|all]

Parameters

client|osc|trunk|wave	Specifies the transceiver class to reset.
n	Number of the particular transceiver you want to clear.
all	Resets all physical transceivers.

Note: For modules with multiple optical lanes, the `n/lane` keyword will enable a user to specify a lane. Depending on the system and transceivers used, there may be a number of configurations for lane counts.
Example: `# clear module client 0/1`

7.7.11 clear rip

Delete all routing information acquired by RIP. This information will be repopulated when the next RIP update occurs. Use the show ip routes command to view the system-wide routing table.

Syntax

`#` **clear rip**

7.8 Diagnostic Commands

This section explains the `debug` and associated `verbosity` commands, both of which help to diagnose system-wide problems. Also described in this section is the `undebug all` (or the identical `no debug`) command that turns off debugging output.

The `debug` and `verbosity` commands should only be used to diagnose specific problems. When debug/verbosity output is active, system performance may be degraded.

7.8.1 debug, undebug all

Turns on/off verbose debugging information for a specified subsystem. Neither `debug` nor `undebug` provide information that is useful during normal DarkStar system operation; debugging information is useful only for diagnosing system problems. In a production network, using `debug` can generate a high volume of trace information at the console and may degrade system performance, so XKL recommends the following

- Use the `debug` command (and `verbosity` command when setting debug message levels) only when working with XKL technical support to diagnose a specific problem with your system.
- Avoid using the `debug` command (as well as the `verbosity` command) in a production network. The system gives high priority to bug reports, so using `debug` may impact business applications.
- To monitor system operations, use the `show` commands, the `logging` command, and SNMP traps to monitor system operations and events, rather than `debug`.

While debugging is enabled, use the `undebug all` command (or `no debug all`) followed by a <cr> to instantly quiet all debugging output. You can type these commands at the console even if the console seems overwhelmed with debug trace messages and fails to echo your keystrokes.

Note: If the amount of debugging information is significant enough to interfere with system operations, disable debugging by running `undebug all` (or `no debug all`).

Syntax

`#` [no] **debug** *argument*

`#` **undebug** all

Parameters

argument	The system modules for monitoring. Contact XKL Technical Support for guidance on using the appropriate argument.
no debug	Disables verbose debugging.

7.8.1.1 show debug

Displays a list of debug flags currently enabled. **Note:** This command is only for use by Technical Support.

Syntax

> **show debug**

7.8.2 verbosity dbg

When the debug command is turned on, you can use the verbosity dbg command to filter the "level" of displayed debug-output messages for modules system-wide.

Note: dbg is one of optional message types that you can select for the verbosity command.

Syntax

verbosity [dbg|hal|msg|net-snmp|warn] *level*

Parameters

verbosity dbg *level*	The *level* parameter is a value from *4-7*—or a value of *-1*—associated with the types of output messages to include for display. The user cannot specify the values 0-3. These levels will always display. For example, verbosity dbg *4*, displays debug messages associated with levels *0* to *4* inclusive. Similarly, each subsequent higher level includes all levels up to and including the specified level. The parameter *level* of *7* provides the most detail and encompasses all levels of debug output messages. With the level value of -1, the verbosity dbg *-1* command sets the default dbg level to 4. Description of each *level*: *0* = Emergency *1* = Alarm *2* = Critical *3* = Error *4* = Warning *5* = Message *6* = Informational *7* = All debug messages, most detail Besides the dbg parameter, the verbosity command also supports the following message-type parameters: • **hal:** for hal-related debugging message (on/off). • **msg:** for error messages. the command verbosity msg *-1* sets the default message level to 1. • **net-snmp:** for net-snmp related debugging message (on/off). • **warn:** for warning/debugging messages. **Note:** The message types **hal** and **net-snmp** require a value, either *1 (display)* or 0 (not-display). Contact XKL Technical Support for guidance with these six additional message types.

7.9 laser shutdown

Powers down the laser transmitter portion of the transceiver.

If write memory *is issued after* `laser shutdown`*, the* `laser shutdown` *command is stored in* `startup-config` *and will take effect during subsequent reloads. To power up* transceivers *following a reload, issue a* `no laser shutdown` *command. To avoid future* transceiver *shutdowns following a reload, issue a* `no laser shutdown` *command followed by* `write memory`.

Syntax

`CONF-MOD-<CLIENT[n]|OSC[n]|WAVE[n]>#` [no] **laser shutdown**

Note: For modules with multiple optical lanes, the `n/lane` keyword will enable a user to specify a lane. Depending on the system and transceivers used, there may be a number of configurations for lane counts.
Example: `CONF-MOD-CLIENT [0/1]# laser shutdown`

7.10 loopback

Enables the chosen loopback mode on the selected interface. Only one loopback mode can be enabled at a time. If you attempt to switch to a loopback that is not supported on the transceiver, the loopback mode will remain unchanged.

Notes:

- Command syntax will differ among systems featuring "loopback" functionality.
- For modules with multiple optical lanes, the `n/lane` keyword will enable a user to specify a lane. Depending on the system and transceivers used, there may be a number of configurations for lane counts.
  Example: `CONF-MOD-CLIENT[0/1]# loopback`

Syntax

`CONF-MOD-<CLIENT[n]|WAVE[n]>#` [no] **loopback {electrical|optical}**
`CONF-MOD-<CLIENT[n]|WAVE[n]>#` [no] **loopback {framed|unframed}**

Parameters

no	Turns loopback mode off.
electrical	Software-generated loopback within the system. As there is no physical connection between the transmitter and receiver ports, the ports themselves are not tested.
optical	Tests the ports and fibers by sending a signal through a physical loopback connection.
framed	Tests the fiber and transceiver ports in optical loopback mode to/from the system. At the loopback, traffic passes through the framing mechanism of the optical transceiver. Test data must be framed Ethernet traffic following the IEEE 802.3-2018 standard.
unframed	Tests the fiber and transceiver ports in optical loopback mode to/from the system. This is simply a connection from the optical receiver to the optical transmitter. Unframed traffic is allowed to pass through, as it does not utilize the transceiver re-framer. Removing the framer may reduce the link quality versus the `loopback framed` mode.

7.11 ping, ping6

Sends test packets to a specific IPv4 or IPv6 address. (Use the `ping6` command for IPv6 addresses.) The `ping` and `ping6` commands send five ICMP echo request packets and reports whether or not responses are received for each. An exclamation point (!) displays for each successful packet and a period (.) is displays for each unsuccessful packet.

	DNS must be configured with the ip name-server *command for* `remote-host` *to work with a hostname instead of an IP address.*

Syntax

`>` **ping** [*remote-host-name*|*ip-address*]

`>` **ping6** [*remote-host-name*|*ip-address*]

Parameters

`remote-host-name`	The destination hostname to which `ping` or `ping6` sends packets.
`ip-address`	The destination IPv4 or IPv6 address to which `ping` or `ping6` sends packets.

Example

```
localhost> ping6 fd16:e32:da22:f01:209:5bff:fee1:5a7e
(fd16:e32:da22:f01:209:5bff:fee1:5a7e)
!!!!!
Done pinging fd16:e32:da22:f01:209:5bff:fee1:5a7e - 5 of 5 packets received
localhost> ping 10.15.1.110
```

7.12 reboot

Reboots the program (i.e., usually DXMOS) from a manually designated file. The operator may designate the DXMOS from the DXMOS file system, or from a remote (TFTP) server. The `reboot` loads the selected program into the processor and starts it; the new program replaces the DXMOS program from which the command is issued. Often, the new program is a fresh copy of DXMOS. However, the new program does not necessarily have to be DXMOS.

This is different from the `reload` command that reloads processor gateware and DXMOS, but leaves the choice of the file up to the system boot loader or boot program.

The `reboot`, like the `reload` command, triggers a "warm boot" of DXMOS without power-cycling or updating system gateware. If the old and new DXMOS running configurations are the same, customer traffic is not disrupted by a warm boot.

Note: If any `reboot` command fails, Boot will run on the console. At that point, recovery is accomplished only by access to the console terminal.

Reboot may disrupt traffic if the startup configuration is not the same as the running configuration.

Syntax

`#` **reboot {file** *file_source*|**next|none|running|tftp** *tftp-server tftp_file_source***}**

Parameters

file *file_source*	Loads and starts the file from a DXMOS file system location.

next	Boots from the next location in the list of boot targets defined in the configuration file. For example, you might add these DXMOS executable files:
	• boot file—A DXMOS executable stored locally on the SD card (i.e., the flash memory) usually in the dxmos directory (e.g., "boot_file_example.exe").
	• boot tftp—A DXMOS executable stored on a server in the tftpboot directory (e.g., "boot_tftp_example.exe").
	After adding the boot targets, issue the `show running-config boot` command to see the listed locations.
	`localhost#` **show running-config boot**
	`boot_file_example.exe`
	`boot_tftp_example.exe`

none	Returns control to the system boot loader or boot program.
running	Reloads and restarts the currently running DXMOS version by re-executing the previous command by which DXMOS was loaded.
tftp *tftp-server*	Boots from the designated TFTP server. Specify an IP address or hostname.
tftp_file_source	Designated file on the TFTP server.

Example

```
localhost# reboot tftp 10.14.1.99 dxmos_prod300_latest.exe
localhost# reboot running
```

7.13 reload

Reloads the processor gateware (or "firmware") and restarts the Boot program. The Boot program loads DXMOS (or another program) as specified by the configuration file.

The `reload` command is appropriate after new processor gateware has been installed in the file system: it causes the new gateware to be installed in the processor. Otherwise, while the processor functions normally, the `reboot` command is more usual.

Note: The `reload` command does not allow the operator to choose a specific file. The file that is booted is determined by the boot commands in the configuration file. Following a reload, the Boot program will load per the first boot entry in the config file. Absent any entries in the file, the Boot program uses “file /dxmos/dxmos.exe.”

When "boot host dhcp" is present in the config file, Boot will attempt to find a configuration file from a DHCP server. If successful, that config file dictates what file to boot.

The `reload` command causes a warm boot that does not affect the transport interfaces (client and line) unless there is a difference between the saved configuration (i.e., `file/dxmos/config.dat`) and the running configuration. To ensure that the transport interfaces are unaffected by `reload`, use the `write memory` command before the reload.

Reload may disrupt traffic if the saved configuration file is not the same as the running configuration.

Syntax

`#` **reload**

7.14 show memory

Displays the current system memory usage.

You may see more show memory commands listed in the CLI help. These are intended for use by XKL support, but are otherwise not likely to be useful to you.

Syntax

`#` **show memory**

Example

`localhost#` **show memory** [See the following optional parameters]

```
Current Memory Usage:
        process          blocks           words
     6764614000               0               0
     6763336000              40            8704
     6763126000               4            8704

    14374 pages of DXMOS fixed allocation.
    13408 pages of mapped system memory.
   496506 pages of system memory available.
   524288 total pages of system memory.

    10178 pages of dynamic memory (included in mapped memory).
```

Parameters

Optionally display memory usage for the following:	
cdr	idrom
cmd-loader	mdio
companion-monitor	mii
compchip-i2c	module
counters	monitor-pio
enviroload	mxp
epmonitor	power
fan	switch
i2c	tpi

Note: Available parameters are system dependent.

7.15 show memory counters management

Displays the memory counters for the internal Ethernet port, the OSC ports (depending on system configuration), and the Ethernet switch's external ports (E0–E3).

Syntax

`#` **show memory counters management {ethernet** *n***|osc** *n***|switch}**

Important: The `switch` command parameter is not available on all systems. To determine whether the `switch` parameter is available on your system, issue the `show hardware` command. If the system is CMD based, the `switch` command parameter is available.

Parameters

ethernet *n*	When *n* is 0, the command displays the memory counters of the internal Ethernet port 0. You can also use this command to display the memory counters of an OSC transceiver. Depending on system configuration, *n* can be from 4–7, the values representing the internal ports of one or more installed OSC transceivers. **Note:** For systems with the switch parameter, values for `ethernet` *n* from 1–3 are invalid.
osc *n*	*n* refers to a single OSC port for which the memory counters will be displayed. Depending on system configuration, *n* can be from 0–3. **Note:** The `show memory counters management osc` *n* command is equivalent to the `show memory counters management ethernet` *n* command, where *n* is within the applicable OSC-value range for the respective commands. For example, the port for `osc` ***0*** is the same as the port for `ethernet` ***4***; the port for `osc` ***1*** is the same as the port for `ethernet` ***5***, and so on.
switch	For systems equipped with this feature, displays the counts of various kinds of packets sent and received on the Ethernet switch's external ports (E0 - E3), as well as the count of various kinds of packets sent and received by the DarkStar system (from which the command is issued). **Note:** The Ethernet switch acts as a Layer-2 switch, managing the DarkStar system's four front-panel Ethernet ports (E0–E3) to which copper LAN cables connect.

Example

```
localhost# show memory counters management switch

          Register (##):           E0          E1          E2          E3       DarkStar
========================== ========== ========== ========== ========== ==========

        RxHiPriorityByte (00):           0           0           0           0           0
          RxUndersizePkt (01):           0           0           0           0           0
             RxFragments (02):           0           0           0           0           0
              RxOversize (03):           0           0           0           0           0
               RxJabbers (04):           0           0           0           0           0
            RxSymbolError (05):           0           0           0           0           0
               RxCRCerror (06):           0           0           0           0           0
         RxAlighmentError (07):           0           0           0           0           0
       RxControl8808Pkts (10):           0           0           0           0           0
             RxPausePkts (11):           0           0           0           0           0
             RxBroadcast (12):           0           2           0          28           4
             RXMulticast (13):           0           0           0           0           0
               RxUnicast (14):           0   514854429   129719563   824526610   100846625
              Rx64Octets (15):           0   730991710   152310060       40193   100770940
        Rx65to127Octets (16):           0   455918547  1036803246      122331       75689
       Rx128to255Octets (17):           0   926215953   141027766           0           0
       Rx256to511Octets (20):           0   778690305   798379051           9           0
      Rx512to2023Octets (21):           0   483638766   930910823       12378           0
     Rx1024to1522Octets (22):           0   360624622   291514089   824351727           0
     Rx1523to2000Octets (23):           0           0           0           0           0
          Rx2001+Octets (24):           0           0           0           0           0
        TxHiPriorityByte (25):           0           0           0           0           0
         TxLateCollision (26):           0           0           0           0           0
             TxPausePkts (27):           0           0           0           0           0
          TxBroadcastPkts (30):           0          32          34           6          30
          TxMulticastPkts (31):           0           0           0           0           0
            TxUnicastPkts (32):           0   602611870   864793968   824713877   100835910
               TxDeferred (33):           0           0           0           0           0
       TxTotalCollision (34):           0           0           0           0           0
    TxExcessiveCollision (35):           0           0           0           0           0
       TxSingleCollision (36):           0           0           0           0           0
     TxMultipleCollision (37):           0           0           0           0           0
               RxByteCnt (40):           0  3453672691  2394750097  3639023838  2162471324
               TxByteCnt (41):           0  3444601488    77995788  1294328297   370120840
          RxDropPackets (42):           0           0           0           0           0
          TXDropPackets (43):           0  1324605177           0           0           0
```

Note: Packets received on the external ports that are not destined for that system will not enter it, and therefore not be counted in the `DarkStar` column (above).

7.16 show tech-support

Displays a large amount of information about DarkStar system operational status and configuration status. This command is intended for use by XKL customer support, and displays all system information in a format that is useful for diagnostics. Typically, an XKL support representative will request that you issue the `show tech-support` command, capture the output, and send it to XKL Support in an email message.

Syntax

`#` **show tech-support**

7.17 shutdown

Shuts down an Ethernet interface or brings it online.

If using SSH or Telnet, be careful not to shutdown the Ethernet interface through which you are connected. Use the "show line" command to help determine the Ethernet interface you are currently using.

Syntax

`CONF-MGMT-<ETH|OSC|LOOP>[n]#` [no] **shutdown**

Parameters

no	Brings the Ethernet module online.

A

Supplementary Information

A.1 Defined States

The following states are reported by DXMOS.

Admin
Administrative State
Admin status is defined differently for an OSC transceiver vs all other types of transceivers. Admin status for an OSC evaluates the Ethernet network status as well as the optical transmission status.

Admin status is the overall status of the transceiver.

Admin Status

Admin Status	Description	
Up	Transceiver Type	Conditions
	OSC	Ethernet network is configured and the module is not shut down by the user.
	Client	The module is not shut down by the user.
	Wave	
Down	Transceiver Type	Conditions
	OSC	Either the Ethernet network is not configured or module is shut down by the user.
	Client	The module is shut down by the user.
	Wave	

BERT Enabled

BERT Enabled Description

BERT Enabled	Description
Transmit, Receive	BERT transmit and receive are in progress.
Transmit	Only BERT transmit in progress.
Receive	Only BERT receive in progress.
No	BERT transmit and receive are inactive.
N/A	Could not determine if BERT is active.

BERT Error Count

The total number of errors detected by the BERT. **Display format:** `n.ddeyy`

BERT Status

BERT Status

BERT Status	Description
Sync Failure	DXMOS BERT reads transceiver if the transceiver detects sync loss.
LOS/LOL	Either Loss of Signal or Loss of Lock has occurred.
OK	BERT test is process.
N/A	The module is absent. It may also be if a module is absent and can still support loopback and not a CFP type transceiver.

BERT Time

The total time that BERT has been in progress (Receive only). **Display format:** `dd hh:mm:ss`

Channel
Ch

The ITU-grid channel for the optical transmitter, as reported by the transceiver (or table lookup by DXMOS. This value is associated with the frequency or wavelength of a DWDM transmitter. Only DWDM transceivers have a channel, others will report N/A. Note that one of these fields must be supplied by the transceiver: Channel, Wavelength, Frequency.
Display format: `nn.m`

Connector

Type of connector based on module type that is used to connect the fiber optics to the transceiver. This data is located in the on-chip memory of the transceiver.

CDR Mode

Reports the operating mode of the CDR in BERT. Based on CDR Types ,(which are currently GN2012 or GN2412).

CDR Mode

CDR Mode	Description
Bypass	Depending upon the rate, this defines that the BERT bypasses the CDR. For lower data rates, 1GE and 1GFC, this mode is set.
Normal	Normal BERT operations. Used for higher data rates.

CDR Temperature

DSM10 only. Temperature of the clock and data recovery (CDR) chip(s). **Display format:** `NN C`

CDR +3.3V Supply Voltage

DSM10 only. The supply voltage to the CDR. **Display format:** `n.mmV`

Description

A user provided description of transceiver. Default is empty string.

Encapsulation

Reports the user-configured encapsulation of the module. Refer to Table : Rate (Encapsulation) Description.

Frequency

The frequency of the optical transmitter, as reported by the transceiver (or table lookup by DXMOS). See Channel. Note that one of these fields must be supplied by the transceiver: Channel, Wavelength, Frequency. **Display format:** `nn GHz`

General Status

Depending on the system, this section can contain the following fields:

--Module State
--Admin OR Administrative State
--Transmitter
--Receiver
--IdleTx/Mute
--Total Down/Total Down/Error Time
--Time Since Last State Change
--Last Cleared Time Stamp
--I2C Transaction Error Count
--Status Register Contents

High Alarm

Occurs when a value exceeds the manufacturer's highest threshold value.

High Warn
High Warning

Occurs when a value is about to exceed the manufacturer's highest threshold value.

I2C Address

The I2C address in the DarkStar system that is used to communicate with the module.

I2C Transaction Error Count

Reports the number of I2C communication errors between DXMOS and the transceiver.

IdleTx/Mute

The information that lets the user know if FEC is supported and how the Tx handles that extra data. Possible output follows:

Idle Tx/Mute Description

CDR Mode	Description
Idle Tx pending Mute	Forward state is Virtual Light hold off.
Idle Mute	Forward state is Virtual Light out.
Off	Forward state is NONE.
Idle Tx with BERT	Forward state is Error Forwarding only if BERT is in progress and system is a DQ*10.
Idle Tx	Forward state is Error Forwarding.
Off	Used for BERT diagnostics.
Transaction Pending	Default Error Forwarding State.

Interface

Interface Description

CDR Mode	Description
OSC	Optical Service Channel is a connection between two adjacent systems in a DWDM link.
Client	The local connection in (and out) of a system. These ports are used to connect the DarkStar system to local customer equipment, such as switches, routers, and other network services.
Wave Trunk	At XKL, "wave" can have multiple meanings: 1) An optical carrier of data. 2) The line transceiver generating this optical carrier, and also called a "wave transceiver," "wave port," or "wave interface." 3) The line counterpart of a particular client. For example, in some DarkStar products, a wave is associated with a client by creating a "connection" in the crossbar switch. The wave can then retransmit a signal received by the client, or conversely, receive a signal that the client can retransmit. The term “trunk” is equivalent to '”wave” and is used exclusively in DQ*100 systems.

Lane <index>

Need definition. TBD.

Laser Temperature

Reports the temperature of the module case. Also see Temperature.
Display format: +/- nn C

Last Cleared
Last Cleared Time Stamp

The time since the error counters were last cleared or when the system gets reloaded. **Display format:** `dd:hh:mm:ss` (day hour:minute:second).

Last Line Chng

Displays how long the transceiver or lane has been in the reported state. For OSC modules, this field is N/A.
Display format: `n.mmey sec` (exponential)

Link DownTime

The total time that a module is administratively up, yet the line is down in an error state or the system is reloading. **Note:** The module is in error state when the Tx is Disabled, Tx is in Fault, Rx in Loss of Lock (LOL), or Rx in Loss of Signal (LOS).
Display format: `dd:hh:mm:ss` (day hour:minute:second).

Line

Lane Status

Line Status	Description	
Absent	The module is not present.	
Up	No optical line alarms and the module is not shut down by the user.	
Alarm	**Condition**	**Description**
	Rx LOS	Optical receiver has LOS.
	Rx LOL	Optical receiver has LOL.
	Tx LOL	Optical transmitter has LOL.
	Tx Fault	Transmission error.
	Sensor	Temperature, Tx Power, Rx Power. Bias Current and Supply Voltage sensors read the alarm bytes from the module.
Warning	Sensor	Temperature, Tx Power, Rx Power. Bias Current and Supply Voltage sensors read the warning bytes from the module.
IO Error	I2C read error	I2C bus is busy.
Down	The module reports Tx is disabled. For example, the user may have shut down the laser, or the module itself fails and cannot transmit data due to an electrical failure.	

Loopback

Reports the loopback capabilities of the module. If loopback is supported, reports the loopback mode currently enabled by the user.

Loopback

Loopback	Description
Not Supported	Loopback is not supported by module.
Electrical	Host-side loopback is enabled.
Optical	Media-side loopback is enabled.
Off	Loopback is disabled.
N/A	The module is absent. It may also be if a module is absent and can still support loopback and not a CFP type transceiver.

Low Alarm

Occurs when a value drops below the manufacturer's lowest threshold value.

Low Warn
Low Warning

Occurs when a value is about to drop below the manufacturer's lowest threshold value.

Manufacturing Date
MFG Date

The manufacture date of the transceiver, as reported by the transceiver. The information is stored in the on-chip memory of the transceiver. **Display format:** `YYMMDD`

Maximum Reach

The maximum supported link length, as reported by the transceiver.

Module <n / lane> Lane-Status

The module-identifier, Module <n / lane>, and the Lane-Status are reported first. The Lane-Status values are shown in Table : Module Status.

Module <n> Module-Status

The module-identifier, Module <n>, and the Module-Status are reported first. The Module-Status values are shown in Table : Lane Status.

Module State

See Line.

Module Type

The transceiver type, as reported by the transceiver.

Module Type Description

Module	Description
SFP	Small Form-factor Pluggable - supports up to 2.5Gbps.
SFP+	Small Form-factor Pluggable plus - supports up to 11Gbps.
CFP	Centum(100) G Form-factor Pluggable - supports up to 100Gbps.
QSFP+	Quad SFP+ - 4 x 10 Gbps (up to 40Gbps).
QSFP28	Quad SFP - up to 100Gbps.
QSFP-DD	Quad SFP Double Density - supports up to 400Gbps.
OSFP	Octal SFP - supports up to 400Gbps.

OSC - optical service channel

An optical channel that connects adjacent DarkStar systems. The OSC provides network connectivity between the management planes in DarkStar systems. The OSC is an out-of-band communication channel.

Part No.
Part Number

The part number is data provided by the vendor and is read from the transceiver.

PRBS Generate

TBD

PRBS Pattern-Check

TBD

Rate

Rate is an alias for encapsulation, which is user configured.

Rate (Encapsulation) Description

Rate		
Summary	Verbose	Description
GE	1G Ethernet	1G Ethernet
10GE	10G Ethernet	10G Ethernet
10GEFEC	10G Ethernet FEC	10G Ethernet with FEC (Forward Error Correction).
OC48	OC48	Sonet OC-48
OC192	OC192	Sonet OC-192
OC192FEC	OC192 FEC	Sonet OC-192 with FEC (Forward Error Correction).
1xFC	1x Fiber Channel	1x Fiber Channel - 1Gbps FC
2xFC	2x Fiber Channel	2x Fiber Channel - 2Gbps FC
4xFC	4x Fiber Channel	4x Fiber Channel - 4Gbps FC
8xFC	8x Fiber Channel	8x Fiber Channel - 8Gbps FC
10xFC	10x Fiber Channel	10x Fiber Channel - 10Gbps FC
1x100GE	1xCAUI-4	1 x 100Gbps CAUI-4 (OpenZR+ mode)
2x100GE	2xCAUI-4	2 x 100Gbps CAUI-4 (OpenZR+ mode)*
3x100GE	3x100GAUI-2	3 x 100Gbps GAUI-2 (OpenZR+ mode)*
4x100GE	4x100GAUI-2	4 x 100Gbps GAUI-2 (OpenZR+ mode)
4x100GE ZR	4x100GAUI-2 ZR	4 x 100Gbps GAUI-2 (ZR Compliant)
400GE	400GAUI-8	400Gbps GAUI-8 (OpenZR+ mode)
400GE ZR	400GAUI-8 ZR	400Gbps GAUI-8 (ZR Compliant)
N/A	N/A	Value for OSC transceivers only
* Not supported in v4.0.1		

Receive

DSM10 only. Reports if BERT Receive is in progress.

BERT Receive Status (DSM10 only)

Receive	Description
On	BERT receive is in progress.
Off	BERT receive is not in progress.

Reported Wavelength

For DSM10/DQ*10. Reports the wavelength of the light of the optical transmitter. See Channel. **Display format:** `DDDD.D nm`

Receiver

Rx

The status of the lane receiver.

Rx Status

Rx Status	Description
IO Error	I2C data transaction error.
LOS	Receiver has Loss of Signal (LOS).
LOL	Receiver has Loss of Lock (LOL).
LOS,LOL	Receiver has both LOS and LOL conditions.
OK	Receiver is operational without errors, alarms, or warnings.
N/A	Module not present.

Rx CDR Firmware

TBD

Rx Cdr (name, lane)

TBD. Also confirm term name.

Rx CDR Version

TBD

Rx Laser Input Power

Reports the optical input power to the receiver. If a multi-lane module, then the Rx Laser Input Power is reported as "Reported By Lane (below)." The value of the Input Power is reported in the Lane section. Also see Rx Power.
Display Format: `+/- nn.m dBm`

Rx Power

RxPow

The optical power received, as reported by the transceiver. If a multi-lane transceiver, Rx power is reported for each lane.
Display Format: `+/- nn.m dBm` OR `N/A`

Rx Power

Rx Power	Explanation
<value>	The receive optical power.
<-40dBm	If the transceiver reports the receive optical power is less than -40dBm, and as this is below the accuracy of the module capabilities, DXMOS reports < -40 instead of the actual value reported by the transceiver.
N/A	Will be result for CFP transceivers if number of optical lanes is greater than 1 or a flag is set and LOW_DBM setting is reached.

Sensor Reading and Thresholds

Readings from each of the module sensors. Each sensor in the module has up to 4 thresholds.

Readings and Thresholds

Threshold	Threshold Definition
high alarm	Factory set. Indicates the need for immediate attention because the reading has exceeded the high condition.
high warn	Factory Set. Indicates that the condition is a heading towards a high alarm condition.
low warn,	Factory Set. Indicates that the condition is a heading towards a low alarm condition.
low alarm	Factory set. Indicates the need for immediate attention because the reading has exceeded the low condition.

Sensor Status

Detailed sensor status of the lane of a transceiver. Each of these fields will have a value shown in the following table.

- Laser Temperature
- Supply Voltage
- Rx Laser Input Power
- Tx Laser Output Power
- Tx Laser Bias Current

Sensor Status Description

Sensor Status	Description
Unsupported	DXMOS does not support this sensor.
High Alarm	Value has exceeded the threshold set in module.
Low Alarm	
OK	No alarm.
N/A	Module is not present.

Serial Number
Serial No.

The serial number provided by the manufacturer. This information is reported by the transceiver.

Signal Type

Reports the user configured encapsulation of the module. See Rate**.**

State Changed

Reports how long after the last change to the lane Rx or Tx status. **Display format:** `nd hh:mm:ss`

Status

TBD

Status Register Contents

Reports the contents of the transceiver status register.

Supply Voltage

+3.3V Supply Voltage

The supply voltage to the transceiver, as reported by the transceiver. +3.3V supply voltage in single-lane modules.
Display format: `s.ddd V`

Supported Distance

If the module reports this value, it represent the maximum supported distance for error-free operation. See Maximum Reach.

Temperature

The case temperature of the transceiver, as reported by the transceiver. The value is read from the module temperature sensor.
Display format: +/- nn C

Time Since Last State Change

See Last Line Chng.

Total Down
Total Down/Error Time

The total time that a module is administratively up, yet the line is down in an error state. **Note:** The module is in error state when the Tx is Disabled, Tx is in Fault, Rx is in Loss of Lock (LOL), or Rx is in Loss of Signal (LOS).

Transceiver

Displays the overall status of the transceiver or lane.

Module Status

Transceiver Status	Description
Absent	Module not present.
OK	Module has no sensor alarms or warnings.
Fault	Could not read module memory or Tx is in Fault state. This state is only available on DQ*100 and DQT400 systems.
Low Power	Module set to Low Power mode. This mode is set in order to protect the module if host cannot cool in high powered mode. This message is only available on DQT400 systems.
Not Ready	The module reports it is not ready. This message is only available on DQ*100 and DQT400 systems.
Alarm	A module alarm threshold has been exceeded. Possible alarms and thresholds are defined by the transceiver and may include: temperature, voltage, Tx/Rx power, bias current, etc. Thresholds are set by the vendor.
Warning	Only displayed for SFP+ transceivers. A module warning threshold has been exceeded. Possible warnings and thresholds are defined by the transceiver and may include: temperature, voltage, Tx/Rx power, bias current, etc. Thresholds are set by the vendor.

Transmit

DSM10 only. Reports if BERT is in progress.

Bert Transmit Status (DSM10 only)

Transmit	Description
On	BERT transmit is in progress.
Off	BERT transmit is not in progress.

Transmitter

Tx

The status of the lane transmitter.

Tx Status

Tx Status	Description
Disabled	Lane is shut down by the user.
LOL	Transmitter has Loss of Lock (LOL) transmission error.
Fault	Transmission error.
Fault,LOL	Both Fault and LOL conditions.
OK	Tx optics is functional.
N/A	Module not present.

Tx CDR Firmware

TBD

Tx Cdr (name, lane)

TBD. Confirm term name.

Tx CDR Version

TBD

Tx Laser

Reports the state of the optical transmitter.

Tx Laser Status

Tx Laser	Explanation
Enabled	Module is not shut down by the user.
Disabled	Module is shut down by the user.

Tx Laser Bias Current

The Tx laser bias current, as reported by the transceiver. If a multi-lane module, then the Tx Laser Bias Current is reported as "Reported By Lane (below)." The value of the Bias Current is reported in the Lane section. **Display format:** ± nn.m mA

In addition to each sensor report, a sensor has up to 4 warning and alarm thresholds that are also reported. These thresholds are set by the transceiver manufacturer.

Sensor Thresholds Description

Threshold	Description
high alarm	Set by the transceiver. Indicates the need for immediate attention because the reading has exceeded the high alarm threshold.
high warn	Set by the transceiver. Indicates a warning condition that should be looked into.
low warn	Set by the transceiver. Indicates a warning condition that should be looked into.
low alarm	Set by the transceiver. Indicates the need for immediate attention because the reading has exceeded the low alarm threshold.

Tx Laser Output Power

Reports the optical output power of transmitter. If a multi-lane module, then the Tx Laser Output Power is reported as "Reported By Lane (below)." The value of the Output Power is reported in the Lane section. Also see Tx Power.

Display format: ± nn.m dBm

Tx Power

The optical power of the transmitter, as reported by the transceiver. **Display Format:** +/- nn.m dBm or N/A

Tx Power

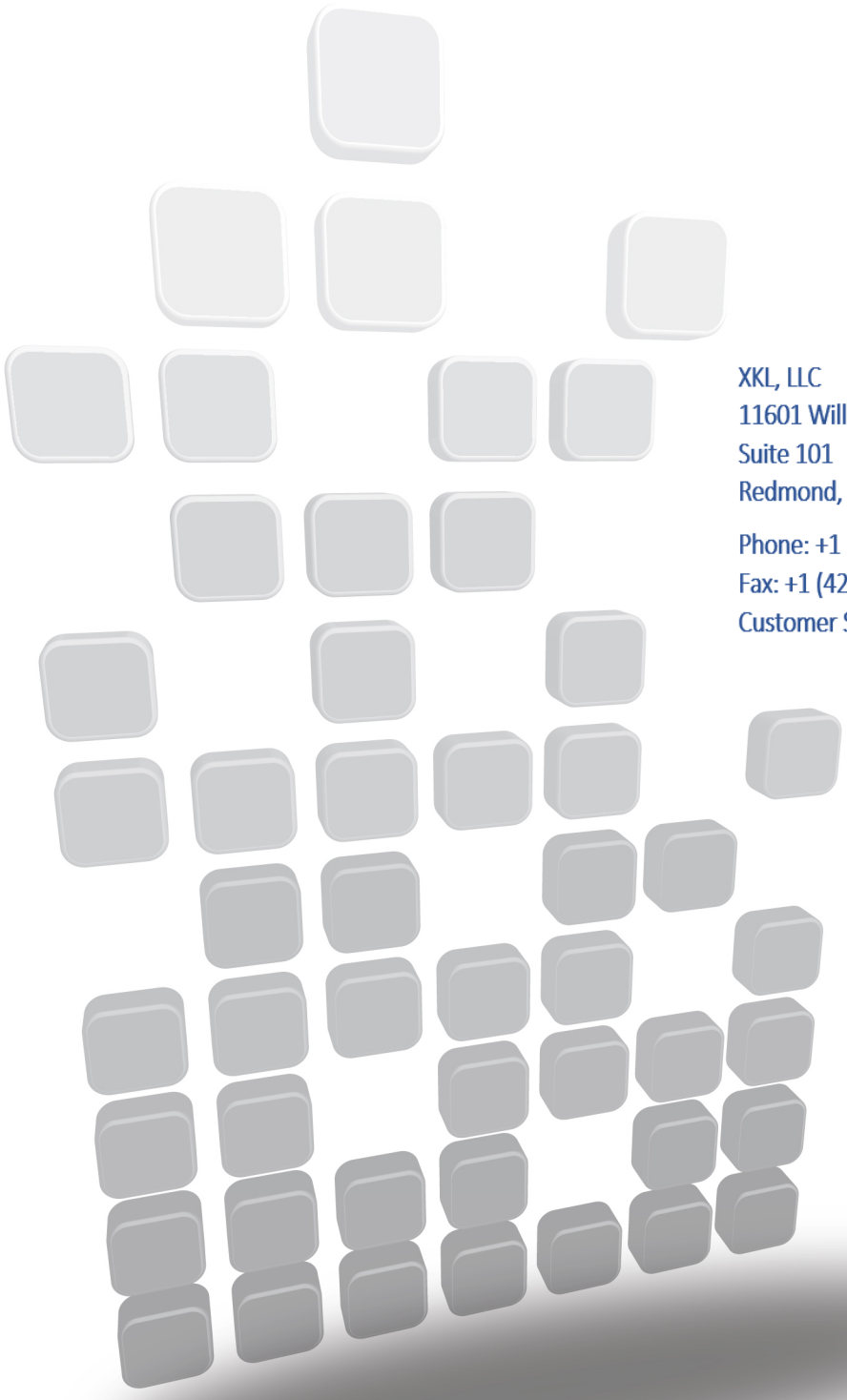
Tx Power	Explanation
<value>	The transmit optical power as reported by the transceiver.
<-40 dBm	If the transceiver reports the transmit optical power is less than -40dBm, and as this is below the accuracy of the module capabilities, DXMOS reports < -40 instead of the actual value reported by the transceiver.
N/A	Will be result for CFP transceivers is number of optical lanes is greater than 1 or a flag is set and LOW_DBM setting is reached.

Vendor

The vendor field data is retrieved from the transceiver. It provides information about who manufactured the transceiver.

Wavelength

The wavelength of the optical transmitter, as reported by the transceiver (or table lookup by DXMOS). See Channel. Note that one of these fields must be supplied by the transceiver: Channel, Wavelength, Frequency. **Display format:** DDDD.D nm.



XKL, LLC
11601 Willows Road NE,
Suite 101
Redmond, WA 98052

Phone: +1 (425) 869-9050
Fax: +1 (425) 861-7863
Customer Support: (866) 949-8340 (U.S. Toll Free)
+1 (608) 807-0033 (Outside U.S.)

www.xkl.com

XKL™