

**Hierarchical Command Line Interface
for
OmniConverter[®] and *RuggedNet*[®]
Single Pair Ethernet
Managed Switch Products**

USER MANUAL

Table of Contents

1.0	Overview	4
1.1	New Features.....	4
2.0	Module Default Settings	5
3.0	Hierarchical CLI Commands	7
3.1	Configuration Mode (config)	9
3.1.1	AAA Command	10
3.1.2	ACL Command	13
3.1.3	BWP Command	15
3.1.4	CONTACT Command	17
3.1.5	COS Command	19
3.1.6	ETHERTYPE Command.....	21
3.1.7	IGMP Command.....	22
3.1.8	IP Command.....	25
3.1.9	LAG Command	29
3.1.10	LLDP Command	33
3.1.11	LOCATION Command	35
3.1.12	LR Command.....	37
3.1.13	MLD Command.....	38
3.1.14	MODBUS Command	41
3.1.15	MODULE Command.....	46
3.1.16	MRP Command	48
3.1.17	PORT Command	53
3.1.18	PORTACCESS Command.....	56
3.1.19	PROTOCOL Command	57
3.1.20	PSE Command	59
3.1.21	SPANTREE Command	63
3.1.22	SMTP Command	67
3.1.23	SNMP Command.....	70
3.1.24	SNTP Command.....	73
3.1.25	SSH Command.....	74
3.1.26	SWITCH Command.....	76
3.1.27	SWITCHPORT Command	77
3.1.28	SYSLOG Command	79
3.1.29	USER Command	81
3.1.30	VLAN Command.....	84
3.2	SHOW Command	85
3.3	FWLOAD Command	87
3.4	MACTABLE Command	88
3.5	PING Command	89
3.6	RESTART Command	91
3.7	RESTORE Command	92
3.8	SAVE Command	93
3.9	SERUPDATE Command	94
3.10	SPLASH Command	95
3.11	TIME Command	97
3.12	TRAPHOST Command	98
3.13	TRAPS Command	100

4.0	Appendix A: Firmware Update	101
4.1	Overview	101
4.2	Save Current Settings	101
4.3	Copy the Files to Your Hard Drive	101
4.4	Updating the Firmware Using FTP	101
5.0	Copyright Statement	105
6.0	Customer Support Information	106

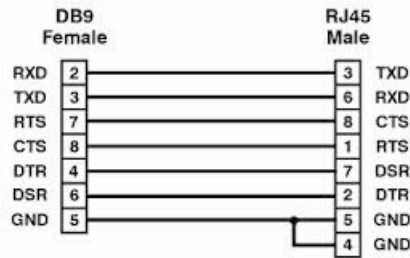
1.0 OVERVIEW

The Hierarchical Command Line Interface (CLI) provides configuration and monitoring for the OmniConverter and RuggedNet SPE managed switch products.



The CLI can be accessed through the serial console port or through the Ethernet ports using Telnet or SSH. To configure the module using the serial port, attach a DB-9 serial (RS-232) equipped computer with terminal emulation software such as Procomm or Putty to the serial port on the module using a RJ-45 to DB-9 serial cable (not included). Some computers do not come with DB-9 serial port connectors and may require a USB-to-serial port adapter.

The port is a standard RS-232 asynchronous serial interface. The serial ports is configured for 57,600bps, 1 stop, 8 data, parity none. The serial adapter cable pin-outs are illustrated below.



Standard RJ-45 to DB-9 serial cable pin-out

1.1 NEW FEATURES

Firmware 3.1 initial release

2.0 MODULE DEFAULT SETTINGS

Each module is configured with the following defaults:

IPv4

IP Address	192.168.1.220
IP Subnet Mask	255.255.255.0
IP Gateway	192.168.1.1

IPv6

IPv6 Interface	stateless
IPV6 Address	fe80::206:87ff:fe01:ec15
IPV6 Gateway Address	fe80::1

Protocols

IP	enabled
Telnet	enabled
FTP	disabled
DHCP Client	disabled
Flow Control	disabled

Passwords

Serial	public (username: admin)
FTP	public (username: admin)
Telnet	public (username: admin)
SSH	public (default username: admin)

SNMPv1/v2c Communities

Read Community Name	public
Write Community Name	private
SNMPv1/v2c agent	enabled

SNMPv3 Parameters

SNMPv3 agent	enabled
User 1 Type	admin
User 1 Name	admin
User 1 security level	noAuthNoPriv
User 1 privacy password	privateadmin
User 1 privacy encryption	DES
User 1 authentication password	privateadmin
User 1 authentication hashing	MD5

User 2 Type	read-only
User 2 Name	guest
User 2 security level	noAuthNoPriv
User 2 privacy password	publicguest
User 2 privacy encryption	DES
User 2 authentication password	publicguest
User 2 authentication hashing	MD5
User 3 Type	deny
User 3 Name	guest1
User 3 security level	noAuthNoPriv
User 3 privacy password	publicguest
User 3 privacy encryption	DES
User 3 authentication password	publicguest
User 3 authentication hashing	MD5
User 4 Type	deny
User 4 Name	guest2
User 4 security level	noAuthNoPriv
User 4 privacy password	publicguest
User 4 privacy encryption	DES
User 4 authentication password	publicguest
User 4 authentication hashing	MD5

General SNMP Parameters

SNMP trap type	SNMPv2c
SNMP UDP Trap Port Number	162

The switches support a common password per user account for the Serial Console, Telnet, FTP and SSH. The password is configured using the *user* command. Passwords for SNMPv1 are configured using the *snmp* command. It is highly recommended that the passwords be changed in order to prevent unauthorized access to the module.

Once accessed, the **Password Entry** screen is displayed. Type the username and password. Press <ENTER>.

```

Omnitron Systems Technology, Inc.                               GLPoE/M v3.1
Copyright 2017-2025 OST, Inc.

-----

Omnitron Systems Technology   Technical Support:   (949) 250-6510
38 Tesla                     Sales/Products:   (800) 675-8410
Irvine, CA 92618              On the web at:   www.omnitron-systems.com
-----

IP address      10.10.8.211
MAC             00-06-87-04-93-10
Serial number   00738745

GLPoE/M login:

```

Module login screen and prompt will vary depending on the model.

3.0 HIERARCHICAL CLI COMMANDS

When there is a successful login, the module will present a “#” prompt indicating access to the hierarchical Command Line Interface.

Enter ? to view the options. When the *exit* command is entered, the module returns to the log-in screen.

```
#
Possible next parameters:
  config      enter configuration mode
  exit        exit current nesting level
  fwload      firmware load configuration
  mactable    mac table status
  no          negate a command
  ping        ping a remote device
  restart     restart module
  restore     restore module defaults
  save        save configuration changes into permanent memory
  serupdate   upload firmware update via the serial port
  show        show configured settings
  splash      splash screen user configuration
  time        time of day configuration
  traphost    snmp trap host configuration
  traps       snmp trap configuration
#
```

The command prompt will change depending on the level of the hierarchical command structure. The hierarchical command has a “#” prompt and the configuration mode (*config*) has a “<cfg>#” prompt. . There are multiple prompts under the configuration mode.

To exit any level of the hierarchical command structure, enter the *exit* command. When *exit* is entered the next highest level of the hierarchical command structure will be entered. When *exit* is entered at the highest level of the hierarchical command structure “#” the module returns to the log-in screen.

Auto completion of a specific command is supported using the <tab> key and entering the ? key. If the cursor is sitting at the end of or in the middle of a command option and the <tab> or the ? key is entered, auto completion of a command will display: “Auto Completion Applied” if only one matching completion is available; “Possible Completions” if multiple completion options are available, followed by a list of valid options; “No Possible Completions Available” if there are no completion options available.

Hierarchical Command Structure

A command prompt indicates the nesting level. Command can be associated with multiple command prompts and nesting levels.

Commands are followed by user input entries and possible command line syntax values. Command line syntax is listed as [name:format], indicating a user defined configuration item.

name indicates the object name that is used in the command

format indicates the valid format for the object

A valid command line will be a prompt and a sequence of one or more objects.

Example:

```
(cfg)# aaa ty tacacs+ host [ipHost1:ipAddr]
```

(cfg)# configuration nesting level prompt

aaa ty tacacs+ host command string

[ipHost1:ipAddr] object name and format

Each command will have a syntax help table to assist with the required values.

General Command Syntax		
Prompt	Base Command	Description
#	?	displays the list of available commands
#	no	negates a command
#	exit	exits current nesting level
#	config	enters the configuration mode
(cfg)#	?	displays the list of available commands
(cfg)#	no	negates a command
(cfg)#	exit	exits configuration mode
(cfg)#	port select <pNum>	enters the port configuration mode
(cfg-if)<pNum>	?	displays the list of available commands
(cfg-if)<pNum>	no	negates a command
(cfg-if)<pNum>	exit	exits port configuration mode

Other nesting levels are available depending on the command options. Each section covers the available nesting levels for that command option.

3.1 CONFIGURATION MODE (CONFIG)

The *config* command sets the module into the configuration mode, allowing access to the configuration command options.

```
# config
Nesting level change accepted

(cfg) #
```

Enter a ? to display the available configuration command options.

```
(cfg) # ?
Possible next parameters:
  aaa          authentication, authorization, accounting configuration
  acl          access control list configuration for management access
  bwp          bandwidth profile configuration
  contact      contact closure status
  cos          class of service configuration
  ethertype    ethertype tag identification configuration
  exit         exit current nesting level
  igmp         internet group management protocol configuration
  ip           IP configuration
  lag          link aggregation group configuration
  lldp         link layer discovery protocol (LLDP) configuration
  location     location configuration
  lr           link redundancy configuration
  mld          multicast listener discovery configuration
  modbus       modbus protocol configuration
  module       module global configuration
  mrp          media redundancy protocol (MRP) configuration
  no           negate a command
  port         port attribute configuration
  portaccess   port access configuration
  protocol     protocol configuration
  pse          power source equipment (PSE) configuration
  smtp         smtp configuration
  snmp         simple network management protocol user configuration
  sntp         simple network time protocol (SNTP) configuration
  spanntree    spanning tree configuration
  ssh          secure shell (SSH) configuration
  switch       physical DIP switch configuration
  switchport   vlan interface configuration
  syslog       system log message configuration
  user         user configuration
  vlan         vlan configuration

(cfg) #
```

The *exit* command option exits the current nesting level.

Not all commands are available depending on the model. SPOE versus Non-SPOE, RuggedNet versus OmniConverter.

3.1.1 AAA Command

The *aaa* command provides the ability to delete all configured AAA settings and restore to factory defaults, to select the configuration type and authentication method and enable RADIUS, TACACS+ and 802.1X. Use the *show aaa* command from the # prompt to determine the state of the protocol (disabled or enabled).

```
(cfg)# aaa
Possible next parameters:
  <cr>
  802.1x      port based access control (802.1X)
  dall       delete all aaa configured settings and restore defaults
  guestvlan  802.1X guest vlan authentication
  meth       authentication method
  radius     radius protocol
  tacacs+    TACACS+ protocol
  ty         configuration type
(cfg)# aaa

(cfg)# port select 1
Nesting level change accepted

(cfg-if) [1]# aaa
Possible next parameters:
  ty         configuration type

(cfg-if) [1]# aaa ty
Possible next parameters:
  802.1x     port based access control (802.1X)

(cfg-if) [1]# aaa ty 802.1x
Possible next parameters:
  auth       802.1X reauthorize time
  guestvlan  802.1X guest vlan authentication
  ptype      port authentication mode
  retry      802.1X EAP retry time
  vid        guest VLAN ID
  xmode      802.1X mode
(cfg-if) [1]# aaa ty 802.1x
```

The command options available following the *aaa* command are shown below.

The *aaa* command option disables/enables AAA. The *no* command negates the command.

The *802.1x* command option disables/enables port based access control, default is disabled. The *no* command negates the command.

The *dall* command option deletes all AAA configured setting and restores factory defaults.

The *guestvlan* command option disables/enables guest VLAN access, default is disabled. The *no* command negates the command.

The *meth* command option selects the authentication method (*local*, *tacacs+* or *radius*).

The *radius* command option disables/enables RADIUS (RFC 2865, RFC 2866), default is disabled. The *no* command negates the command.

The *tacacs+* command option disables/enables TACACS+, default is disabled. The *no* command negates the command.

The *ty* command option configures the AAA protocol type, TACACS+ or RADIUS.

tacacs+

host configures ip host server address

key configures the secret key for the server

l4 configures the layer 4 port number in the following order: authentication / authorization port (a1) and accounting port (a3)

to configures the server timeout before error declared. The default value is 60 seconds

radius

host configures ip host server address

key configures the secret key for the server

l4 configures the layer 4 port number in the following order: authentication / authorization port (a1) and accounting port (a3)

tran configures the number of RADIUS server request retries. The default is 2

to configures the server timeout before error declared. The default value is 60 seconds

Command options under the *port select <pNum> ty 802.1x* command.

The *auth* command option configures the 802.1X reauthorization timer. A zero value disables the timer.

The *guestvlan* command option enables guest VLAN access via 802.1X.

The *ptype* command option selects the port authentication mode:

auto configures 802.1X authentication on the port.

mac configures 802.1X MAC bypass authentication on the port.

on configures a port to be authorized, disabling 802.1X EAP.

off configures a port to be unauthorized, blocking the port permanently and disabling 802.1X EAP.

The *retry* command option configures the 802.1X retry time (1 to 60 seconds) for new EAP request identify PDU. The default time value is 30 seconds.

The *vid* command configures the guest VLAN ID.

The *xmode* command option configures how the 802.1X frames are handled.

discard when 802.1X is disabled, 802.1X frames are discarded.

peer when 802.1X is enabled and protocol is operating.

tunnel when 802.1X is disabled, 802.1X frames are tunneled.

The following command configures the IP address [ipHost1:ipAddr] of the RADIUS server.

```
(cfg)# aaa ty radius host [ipHost1:ipAddr]
```

The following command enables RADIUS.

```
(cfg)# aaa radius
```

To view the changes or display the AAA configuration settings, use the *show aaa* command from the # prompt.

AAA Command Syntax	
(cfg)# aaa	(cfg)# aaa ty radius key
(cfg)# no aaa	(cfg)# aaa ty radius key [aKey:string0..63]
(cfg)# aaa dall	(cfg)# aaa ty radius l4 [a1:1-65535] [a3:1-65535]
(cfg)# aaa guestvlan	(cfg)# aaa ty radius tran [rNum:0-10]
(cfg)# no aaa guestvlan	(cfg)# aaa ty radius to [toVal:1-60]
(cfg)# aaa radius	(cfg)# aaa meth [authList:authString]
(cfg)# no aaa radius	(cfg)# port select <pNum> (accesses next nesting level)
(cfg)# aaa tacacs+	(cfg-if)>pNum># aaa ty 802.1x ptype auto
(cfg)# no aaa tacacs+	(cfg-if)>pNum># aaa ty 802.1x ptype mac
(cfg)# aaa 802.1x	(cfg-if)>pNum># aaa ty 802.1x ptype on
(cfg)# no aaa 802.1x	(cfg-if)>pNum># aaa ty 802.1x ptype off
(cfg)# aaa ty tacacs+ host	(cfg-if)>pNum># aaa ty 802.1x auth [aTime:0-65535]
(cfg)# aaa ty tacacs+ host [ipHost1:ipAddr]	(cfg-if)>pNum># aaa ty 802.1x retry [rTime:1-60]
(cfg)# aaa ty tacacs+ key [aKey:string0..63]	(cfg-if)>pNum># aaa ty 802.1x vid [gVid:1-4095]
(cfg)# aaa ty tacacs+ key	(cfg-if)>pNum># aaa ty 802.1x xmode discard
(cfg)# aaa ty tacacs+ l4 [a1:1-65535] [a3:1-65535]	(cfg-if)>pNum># aaa ty 802.1x xmode peer
(cfg)# aaa ty tacacs+ to [toVal:1-60]	(cfg-if)>pNum># aaa ty 802.1x xmode tunnel
(cfg)# aaa ty radius host	(cfg-if)>pNum># aaa ty 802.1x guestvlan
(cfg)# aaa ty radius host [ipHost1:ipAddr]	(cfg-if)>pNum># no aaa ty 802.1x guestvlan
(cfg)# aaa ty radius host [ipHost1:ipAddr] [ipHost2:ipAddr]	

Syntax	Name Description	Format Values
[ipHost1:ipAddr]	ip host address 1	ipv4 or ipv6 address
[ipHost2:ipAddr]	ip host address 2	ipv4 or ipv6 address
[aKey:string0..63]	server key	string 0-63 characters
[a1:1-65535]	authentication/authorization port #	1-65535
[a3:1-65535]	accounting port #	1-65535
[toVal:1-60]	server timeout before error declared	1-60 sec
[rNum:0-10]	RADIUS server request retry count	0-10 sec
[authList:authString]	authentication list	local, tacacs, or radius with commas
[aTime:0-65535]	802.1X reauthorize time	0-65535 sec
[rTime:1-60]	802.1X EAP retry time	1-60 sec
[gVid:1-4095]	guest VLAN ID	1-4095

3.1.2 ACL Command

The *acl* command provides the ability to enable/disable default ACL behavior, delete all ACL configured settings and restore to factory defaults and add/modify or delete an ACL instance. Use the *show acl* command from the # prompt to determine the state of each command option (disabled or enabled).

```
(cfg)# acl ?
Possible next parameters:
  <cr>
  dflt          default for items not found in ACL list
  dall         delete ACL configured settings, instances, restore defaults
  index        ACL instance

(cfg)# acl

(cfg)# acl index 1
Nesting level change accepted

(cfg-acl) [1]# ?
Possible next parameters:
  dst          TCP/UDP destination port
  exit         exit ACL instance
  ipend        end IP address
  ipsrc        source IP address
  prefix       subnet mask or prefix length
  proto        protocol
  ty           ACL access type

(cfg-acl) [1]#
```

The command options available following the *acl* command are shown below.

The *acl* command option disables/enables ACL. The *no* command negates the command.

The *dall* command option deletes all configured ACL filters and restores factory defaults.

The *dflt* command option selects a default behavior for items not found in the ACL list. The default is permit.

The *index* command option allows the configuration of ACL instances. The *no* command negates the command.

Command options under the *index idx ins* command.

The *dst* command option selects a TCP or UDP destination port number for an ACL filter.

The *exit* command option exits the current nesting level.

The *ipend* command option configures the IP end address for an ACL filter.

The *ipsrc* command option configures the IP source address for an ACL filter. The source IP address for ARP is the Send IP Address.

The *prefix* command option configures the subnet mask of prefix length.

The *proto* command option configures the protocol as *arp*, *icmp*, *ip*, *tcp* or *udp*.

The *ty* command option configures the ACL access type as *deny* or *permit*.

To allow access to a device, the module must be configured to allow (permit) ARP and IP. Since ICMP is part of the IP protocol, it must be explicitly excluded. ACL filters are processed in the order displayed.

```
(cfg)# acl dall

(cfg)# acl index 1
(cfg-acl) [1]# ipsrc 172.16.9.1
(cfg-acl) [1]# ipend 172.16.9.5
(cfg-acl) [1]# proto icmp
(cfg-acl) [1]# ty deny
(cfg-acl) [1]# exit

(cfg)# acl index 2
(cfg-acl) [2]# ipsrc 172.16.9.1
(cfg-acl) [2]# ipend 172.16.9.5
(cfg-acl) [2]# proto ip
(cfg-acl) [2]# ty permit
(cfg-acl) [2]# exit

(cfg)# acl index 3
(cfg-acl) [3]# ipsrc 172.16.9.5
(cfg-acl) [3]# prefix 24
(cfg-acl) [3]# proto arp
(cfg-acl) [3]# ty permit
(cfg-acl) [3]# exit
```

To view the changes or display the ACL configuration settings, use the *show acl* command from the # prompt.

It is recommended that ACL policies be added prior to enabling ACLs to avoid the possible loss of connectivity to the module while accessing the module using the Ethernet interface.

ACL Command Syntax	
(cfg)# acl	(cfg-acl)# ipend [ipAddr:ipAddr]
(cfg)# no acl	(cfg-acl)# ipend [ipAddr:ipAddr]
(cfg)# acl dflt permit	(cfg-acl)# prefix [plen:1-128]
(cfg)# acl dflt deny	(cfg-acl)# ty permit
(cfg)# acl dall	(cfg-acl)# ty deny
(cfg)# no acl index [idx:1-200]	(cfg-acl)# proto arp
(cfg)# acl index [idx:1-200]	(cfg-acl)# proto icmp
(cfg)# acl index [idx] (accesses next nesting level)	(cfg-acl)# proto ip
(cfg-acl)# acl index [idx:1-200]	(cfg-acl)# proto tcp
(cfg-acl)# acl index [idx:1-200] ins	(cfg-acl)# proto udp
(cfg-acl)# ipsrc [ipAddr:ipAddr]	(cfg-acl)# dst [ipPort:_1-65535]
(cfg-acl)# ipend	(cfg-acl)# exit

Syntax	Name Description	Format Values
[idx:1-200]	ACL add/modify/delete instance #	1-200
[ipAddr:ipAddr]	source or end IP address value	ipv4 address
[plen:1-128]	subnet mask or prefix length value	1-128
[ipPort:-1-65535]	TCP/UDP destination port value or #	1-65535

3.1.3 BWP Command

The *bwp* command provides the ability to configure bandwidth profiles associated with each port. Bandwidth profiles control the amount of bandwidth allowed to each port.

```
(cfg)# bwp ?
Possible next parameters:
  dall          delete bandwidth configured settings, restore defaults
  fwmix         port queue global fairweight mixture

(cfg)# bwp
Possible next parameters:
  dall          delete bandwidth configured settings, restore defaults
  fwmix         port queue global fairweight mixture

(cfg)# bwp fwmix
Possible next parameters:
  mVal         Eight global queue values separated by commas, value 0-100

(cfg)# port select 1
Nesting level change accepted

(cfg-if) [1]# bwp
Possible next parameters:
  cn           class of service name
  que         type of egress queue

(cfg-if) [1]# bwp
```

The command options available using the *bwp* command are shown below.

The *dall* command option deletes all configured bandwidth profiles.

The *fxmix* command option configures the global fairweight mix for queues 7 - 0 and is used when *que fairweight fw* or *que qlist fw* is selected. All eight egress queue must be defined by the command *q7,q6,q5,q4,q3,q2,q1,q0* where *qx* indicates the weight for the specific queue (0-100 are valid entries. The sum of all weighed values is 128 or less). The queues are separated by a comma (,).

Command options under the *port select <pNum>* command.

The *cn* command option associates a configured Class of Service profile to the select port. The *no* command negates the command.

The *que* command option configures the type of egress queueing used (fairweight, starving or individually configured).

- fairweight* all queues are setup for weighted fair queuing using the *fwmix* setting
- starving* all queues are set up to starving (strict) priority
- qlist* each of the eight queues are set up individually: *q7,q6,q5,q4, q3, q2, q1,q0* where *qx* can be one of two values (*sp* or *fw*):
 - sp* queue is set to strict priority. The listing of strict priority queues starts at highest priority queue (queue 7) and can only be selected from the highest queue sequentially without mixtures of weighted values between strict priority queues
 - fw* queue is set to fairweight priority

The following are some legal combinations:

fw,fw,fw,fw,fw,fw,fw,fw (default fairweight)

sp,sp,sp,sp,sp,sp,sp,sp,sp (default starving)

sp,sp,fw,fw,fw,fw,fw,fw

sp,sp,sp,sp,fw,fw,fw,fw

The following are not a legal combinations:

sp,fw,fw,sp,fw,fw,fw,fw

fw,sp,sp,sp,sp,sp,sp

sp,fw,fw,fw,fw,fw,fw,sp

The actual weight for a queue type of *fw* is from the respective queue weight from the *fwmix* setting

To configure a class of service name to a bandwidth profile, use the following commands.

```
(cfg)# port select 1
Nesting level change accepted

(cfg-if) [1]# bwp cn Data

(cfg-if) [1]#
```

To view the changes or display the BWP configuration settings, use the *show bwp* command from the # prompt.

BWP Command Syntax	
(cfg)# bwp dall	(cfg-if)<pNum># bwp que fairweight
(cfg)# bwp fwmix [mVal:mx,mx,mx,mx,mx,mx,mx,mx]	(cfg-if)<pNum># bwp que starving
(cfg)# port select <pNum> (accesses next nesting level)	(cfg-if)<pNum># bwp que qlist [qval:qx,qx,qx,qx,qx,qx,qx,qx]
(cfg-if)<pNum># bwp cn [cName:string0..45]	(cfg-if)<pNum># exit
(cfg-if)<pNum># no bwp cn	

Syntax	Name Description	Format Values
[mVal:mx,mx,mx,mx,mx,mx,mx,mx]	Eight global queue	0-100, separated by commas
[cName:string0..45]	class of service name	string 0-45 characters
[qval:qx,qx,qx,qx,qx,qx, qx,qx]	Eight queues q7-q0	fw or sp, separated by commas
[cirRate:0-10000000]	committed egress information rate	0-10000000 kb/sec
[equeue:0-7]	egress queue selection	0-7
[cirRate:64-10000000]	committed ingress information rate	64-10000000 kb/sec
[cbsSize:2-256]	committed burst size	2-256 KB

3.1.4 CONTACT Command

Only supported on the RuggedNet SPE switch products.

The *contact* command provides the ability to assign a failure types and names to the contact closure and digital input.

```
(cfg)# contact
Possible next parameters:
  dall          delete 'contact' configured settings, restore defaults
  mode          contact closure alarm output mode
  nmc           name of the normally closed relay
  nmi           name of the digital input sense
  nmo           name of the normally open relay

(cfg)# contact
```

The command options available using the *contact* command are shown below.

The *dall* command option deletes all contact configured settings and restores factory defaults.

The *mode* command option selects the type of error that will cause the output relay to close; forced, input, none, power, temp. Multiple selections can be entered.

- forced* manually close the relay
- input* an error condition is declared when the alarm input is detected as closed
- none* function is disabled
- power* an error condition is declared when the internal power is greater or less than 5% of nominal input voltage
- temp* an error condition is declared when a temperature violation is detected

The *nmc* command option configures the name of the normally closed relay contacts.

The *nmi* command option configures the name for the digital input.

The *nmo* command option configures the name for the normally opened relay contacts.

To name the digital input, use the following command.

```
(cfg)# contact nmi "open door alarm"
```

To configure the alarm relay to activate on the digital input detection, use the following command.

```
(cfg)# contact mode input
```

To view the changes or display the CONTACT configuration settings, use the *show contact* command from the # prompt.

Contact Command Syntax	
(cfg)# contact dall	(cfg)# contact mode power temp
(cfg)# contact mode none	(cfg)# contact mode temp
(cfg)# contact mode forced	(cfg)# contact nmc
(cfg)# contact mode input	(cfg)# contact nmc [cName:string0..64]
(cfg)# contact mode input power	(cfg)# contact nmi
(cfg)# contact mode input temp	(cfg)# contact nmi [cName:string0..64]
(cfg)# contact mode input power temp	(cfg)# contact nmo
(cfg)# contact mode power	(cfg)# contact nmo [cName:string0..64]

Syntax	Name Description	Format Values
[cName:string0..64]	name of the relay or alarm input	string 0-64 characters

3.1.5 COS Command

The *cos* command provides the ability to configure Class of Service profiles that can be associated with a configured bandwidth profile.

```
(cfg)# cos ?
Possible next parameters:
  dall          delete CoS configured settings, instances, restore defaults
  name          class of service identifier

(cfg)# cos

(cfg)# cos name voice
Nesting level change accepted

(cfg-cos)[voice]# ?
Possible next parameters:
  dflt          default class classification
  dscp          layer 3 IP priority
  exit          exit CoS instance
  mode          mode classification mode
  pcp           layer 2 priority bits

(cfg-cos)[voice]#
```

The command options available using the *cos* command are shown below.

The *dall* command option deletes all configured CoS profiles and restores factory defaults.

The *name* command option configures the name of the class of service profile. The *no* command negates the command.

Command options under the *name <cName>* command.

The *dflt* command option modifies the default class classification. Ingress frames not meeting any configured CoS profile is assigned the default class classification.

The *dscp* command option sets the profile based on the IP priority bits of the ingress frame.

The *exit* command option exits the current nesting level.

The *mode* command option configures the ingress classification mode.

- ip* selects IP only classification (DSCP), layer 2 classification is ignored
- ipoverl2* selects IP classification (DSCP) priority over layer 2 classification (PCP) if both are present
- l2* selects layer 2 classification (PCP) only, IP classification is ignored
- l2overip* select layer 2 classification (PCP) over IP classification (DSCP), if both are present
- none* neither layer 2 or IP classification are used

On an access port, only untagged frames are accepted with the following format: Data.

On a tunnel port, zero or one tag is allowed for DSCP selection with the following formats: Data Only or Ethertype (8100) and Data.

On a trunk port, zero, one, or two layers of tags are allowed for DSCP selection with the following formats:

- Data Only or
- Ethertype (8100) and Data or

Ethertype (88a8) and Data or
 Ethertype (88a8) and Ethertype (8100) and Data or
 Ethertype (8100) and Ethertype (8100) and Data.

The default CoS classification of Layer2 over IP classification indicates mapping Layer 2 PCP to their respective queues, i.e. PCP 0 to queue 0, PCP 1 to queue 1, etc. and if not tagged then IP DSCP 0x00-0x07 is mapped to queue 0, 0x08-0x0f to queue 1, etc.

If a CoS is assigned to a port those associations that are defined are mapped to the explicit egress queue defined. Received traffic that does not match one of the defined associations is mapped to the default queue.

If no CoS is assigned to a port, the egress frame will use the default CoS classification value of 1. The *pcp* command option sets the profile based on the PCP bit of the ingress frame.

The *pcp* command option sets the priority and class of the PCP bit of the ingress frame.

Multiple CoS profile filters with the same name can be configured and applied to a single port by associating the CoS profile with a Bandwidth profile. If the ingress frame does not meet any of the configured CoS profiles, the ingress traffic will use the default class classification.

To configure a class of service profile, use the following commands.

```
(cfg)# cos name data
Nesting level change accepted

(cfg-cos) [data]# pcp 0..1 class 0
(cfg-cos) [data]# pcp 2..3 class 2
(cfg-cos) [data]# pcp 4..6 class 4
(cfg-cos) [data]# pcp 7 class 7

(cfg-cos) [data]#
```

To view the changes or display the COS configuration settings, use the *show cos* command from the # prompt.

COS Command Syntax	
(cfg)# cos dall	(cfg-cos)<cName># mode ipoverl2
(cfg)# no cos name [cName:string1..45]	(cfg-cos)<cName># mode l2
(cfg)# cos name [cName] (accesses next nesting level)	(cfg-cos)<cName># mode l2overip
(cfg-cos)<cName># pcp [pcpList:0..7 none] class [cClass:0-7]	(cfg-cos)<cName># mode none
(cfg-cos)<cName># pcp [pcpList:0..7 none] class [cClass:0-7]	(cfg-cos)<cName># dflt [class:0-7]
(cfg-cos)<cName># dscp [dList:0..63 none] class [cClass:0-7]	(cfg-cos)<cName># exit
(cfg-cos)<cName># mode ip	

Syntax	Name Description	Format Values
[cName:string1..45]	class of service name	string 1-45 characters
[pcpList:0..7 none]	layer 2 priority bits	0-7, none
[dList:0..63 none]	layer 3 IP priority	0-63, none
[class:0-7] or [cClass:0-7]	CoS classification	0-7

3.1.6 ETHERTYPE Command

The *ethertype* command provides the ability to configure the protocol used to encapsulate a VLAN tagged frame. Ethertype is a two-octet field in an Ethernet frame indicating which protocol is used to encapsulate tag information in the frame data.

```
(cfg)# ethertype ?  
Possible next parameters:  
  dall          delete ethertype configured settings, restore defaults  
  trunk         provider network Ethertype  
  
(cfg)# ethertype
```

The options available using the *ethertype* command are shown below.

The *dall* command option deletes all configured ethertype settings and restores to factory defaults.

The *trunk* command option configures the Ethertype for provider tagged frames. The default is 8100.

Use the following commands to configure the provider tag for a Ethertype value of 88a8.

```
(cfg)# ethertype trunk 88a8
```

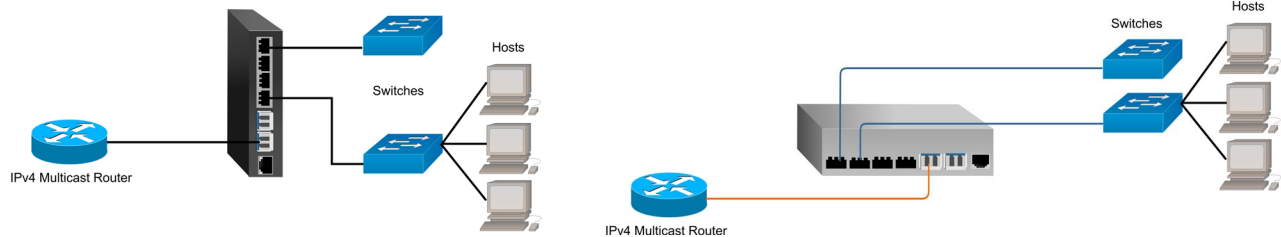
To view the changes or display the ETHERTYPE configuration settings, use the *show ethertype* command from the # prompt.

Ethertype Command Syntax	
(cfg)# ethertype dall	(cfg)# ethertype trunk [ethertypeVal:hex16]

Syntax	Name Description	Format Values
[ethertypeVal:hex16]	provider network Ethertype	4 ascii hex characters

3.1.7 IGMP Command

The module supports IGMPv1, v2, or v3 IPv4 snooping based upon RFC 4541, which defines the basic operation of an IGMP snooping switch. IGMP is used to modify the default router behavior for IPv4 Multicast Packets which are flooded to all ports. IGMP provides a method for forwarding IPv4 Multicast Packets to only the ports with hosts that want to receive the packets. IGMP communications occur between IPv4 Multicast Routers and Hosts.



IPv4 Multicast Packets have an address range of 224.0.0.0 to 239.255.255.255.

The *igmp* command provides the ability to configure IGMP on the module. Use the *show igmp* command from the # prompt to determine the state of each command option (disabled or enabled).

```
(cfg)# igmp ?
Possible next parameters:
  dall          delete IGMP settings, instances, restore defaults
  flood         flooding of all unrecognized IGMP groups
  snooping      IGMP snooping
  to            IGMP route aging in seconds
  vid           VLAN ID

(cfg)# igmp

(cfg)# igmp vid 1 grp 224.0.0.1
Nesting level change accepted

(cfg-igmp) [vid 1, 224.0.0.1]# ?
Possible next parameters:
  aging         IGMP route subject to aging out
  exit          exit IGMP instance
  no            negate a command
  ph           host port
  pr           router port

(cfg-igmp) [vid 1, 224.0.0.1]#
```

The command options available using the *igmp* command are shown below.

The *dall* command option deletes all IGMP configured settings and restore factory defaults.

The *flood* command option disables/enables flooding of unrecognized IGMP routes. The *no* command negates the command.

The *snooping* command option disables/enables IGMP snooping. The *no* command negates the command.

The *to* command option selects the timeout value in seconds to automatically remove a route from the forwarding database. The timeout never expires with a value of 0.

The *vid* command option selects the VLAN ID. The *no* command negates the command.

Command options under the *vid* <*vVid*> *grp* <*ipAddr*> command.

The *aging* command option selects the timeout value in seconds to automatically remove a route from the forwarding database. The timeout never expires with a value of 0. The *no* command negates the command.

The *exit* command option exits the current nesting level.

The *no* command option negates a command.

The *ph* command option selects the host port(s) on the module for a defined route.

The *pr* command option selects the router port(s) on the module for a defined route.

To automatically enable IGMP snooping on a VLAN ID, use the following commands.

```
(cfg)# igmp vid 1
(cfg)# igmp snooping
```

To manually configure a IGMP route with the multicast IP address of 255.100.100.1 and the multicast router and host ports.

```
(cfg)# igmp vid 1 grp 255.100.100.1
(cfg-igmp) [vid 1, 255.100.100.1]# pr 1
(cfg-igmp) [vid 1, 255.100.100.1]# ph 3
(cfg-igmp) [vid 1, 255.100.100.1]# exit

(cfg-igmp)#exit

(cfg)#
```

To view the changes or display the IGMP configuration settings, use the *show igmp* command from the # prompt.

There are common variables that are shared between the IGMP and MLD protocols. The variables are Snooping (enable / disable), Flooding Unrecognized Groups (enable / disabled) and Route Aging timer. If either protocol changes the shared variables, they will be changed under both protocols (IGMP and MLD). Example: If Snooping is enabled under MLD, Snooping will be enabled under IGMP.

IGMP Command Syntax	
(cfg)# igmp dall	(cfg)# igmp vid [vVid:1-4095] grp [ipAddr:ipAddrv4]
(cfg)# igmp flood	(cfg)# no igmp vid [vVid:1-4095] grp [ipAddr:ipAddrv4]
(cfg)# no igmp flood	(cfg)# igmp vid [vVid] grp [ipAddr] (accesses next nesting level)
(cfg)# igmp snooping	(cfg-igmp)# ph [hNum:f1,f2,1..8 all]
(cfg)# no igmp snooping	(cfg-igmp)# pr [rNum:f1,f2,1..8 all]
(cfg)# igmp to [toVal:0-65535]	(cfg-igmp)# aging
(cfg)# igmp vid [vVid:1-4095]	(cfg-igmp)# no aging
(cfg)# no igmp vid [vVid:1-4095]	(cfg-igmp)# exit

Syntax	Name Description	Format Values
[toVal:0-65535]	IGMP route aging	0-65535 sec
[vVid:1-4095]	VLAN ID	1-4095
[ipAddr:ipAddrv4]	IGMP group IPv4 address	ipv4 address
[hNum:f1,f2,1..4 all]	host port number (on module)	f1,f2,1..4, or all
[rNum:f1,f2,1..4 all]	router port number (on module)	f1,f2,1..4, or all

3.1.8 IP Command

The *ip* command provides the ability to configure the IPv4 and IPv6 parameters on the module. Also, specific protocol options can be disabled or enabled. Use the *show ip* command from the # prompt to determine the state of each command option (disabled or enabled).

```
(cfg)# ip ?
Possible next parameters:
  addr          IPv4 or IPv6 address
  circuitid     DHCPv4 Relay Agent Circuit ID
  dall         delete IP configured settings, restore defaults
  dhcp         DHCPv4 protocol
  dhcpv6       DHCPv6 protocol
  dns          Domain Name System
  dnsaddr      domain name system ip address
  gw           gateway address
  ipv4         IPv4 enable/disable address
  ipv6         IPv6 enable/disable address
  net          IPv4 subnet mask
  relay        DHCPv4 relay agent (option 82)
  remoteid     Relay Agent Remote ID
  rserv        DHCP Relay Server
  rtype        DHCP Relay client type
  stateless    IPv6 stateless
  v6circuitid  DHCPv6 Relay Interface-ID
  v6relay      DHCPv6 relay agent
  v6remoteid   DHCPv6 Relay Agent Remote-ID

(cfg)# ip
```

The commands options available using the *ip* command are shown below.

The *addr* command option configures the IPv4 and IPv6 addresses of the module.

The *circuitid* command option disables/enables the Agent Circuit ID for DHCP Option 82 on the module.

The *no* command negates the command.

The *dall* command option deletes all IP configured settings and restores factory defaults.

The *dhcp* command option disables/enables DHCPv4 protocol on the module. The *no* command negates the command.

The *dhcpv6* command option disables/enables DHCPv6 protocol on the module. The *no* command negates the command.

The *dns* command option disables/enables DNS protocol on the module. The *no* command negates the command.

The *dnsaddr* command option configures the DNS IP address of the module.

The *gw* command option configures the gateway IP address of the module.

The *ipv4* command option disables/enables IPv4 protocol on the module. The *no* command negates the command.

The *ipv6* command option disables/enables IPv6 protocol on the module. The *no* command negates the command.

The *net* command option configures the subnet mask of the module.

The *relay* command option disables/enables DHCPv4 Relay function (option 82) on the module. The *no* command negates the command.

The *remoteid* command option disables/enables DHCPv4 Relay Agent Remote ID. The *no* command negates the command.

The *rsvr* command option configures the IPv4/IPv6 address of the DHCP Relay Server.

The *rtype* command option configures the DHCPv4 Relay Client type; *drop*, *keep* or *replace*.

The *stateless* command option disables/enables Stateless operation on the module. The *no* command negates the command.

The *v6circuitid* command option disables/enables DHCPv6 Relay Interface-ID, dflt enabled. The *no* command negates the command.

The *v6relay* command option disables/enables DHCPv6 relay agent, dflt disabled. The *no* command negates the command.

The *v6remoteid* command option disables/enables DHCPv6 Relay Agent Remote-ID, dflt enabled. The *no* command negates the command.

Stateful configuration requires a IPv6 service to provide the IPv6 address to the client (module) and requires both client and server to maintain the “state” of the address. Stateless provides auto configuration of IPv6, allowing the client (module) to self configure the IPv6 address. The advantage is that the IPv6 service is not required to store any dynamic state information about any individual clients. A network can use both stateful and stateless auto configuration at the same time.

IPv6 stateful can be entered by the user and does not require an IPv6 service. However, if DHCPv6 is enabled the address will be acquired via DHCPv6 information provided by the server.

To configure the IPv4 address on the module, use the following command.

```
(cfg)# ip addr 192.168.1.100
```

To configure the IPv6 address on the module, use the following commands.

```
(cfg)# no ip stateless  
(cfg)# ip addr 2001::a0a:652 prefix 64
```

To enable the DHCPv6 address on the module, use the following command.

```
(cfg)# ip dhcpv6
```

To view the changes or display the IP configuration settings, use the *show ip* command from the # prompt.

DHCPv4 Relay Process

The DHCP Relay Agent relays DHCP messages between DHCP clients and DHCP servers. A DHCP relay agent receives any DHCP broadcasts and forwards them to the specified DHCP server IP address.

1. The DHCP client generates a DHCP request.
2. The DHCP relay agent receives the broadcast DHCP request packet and inserts the relay agent information option (option 82) into the packet. The relay agent information option contains related sub options (Circuit ID and Remote ID).
3. The DHCP relay agent sends the DHCP packet to the DHCP server.
4. The DHCP server receives the packet, uses the sub options to assign IP addresses and other configuration parameters to the packet, and forwards the packet back to the DHCP relay agent.
5. The sub option fields are removed by the relay agent and the IP address information is forwarded to the client.

If DHCP Relay Agent Circuit ID is enabled and the DHCP Relay Client Type is set to Replace, the Circuit ID will be set as “br0” instead of the associated port number.

If the module is configured as the 2nd DHCP Relay agent in a network, the unicast DHCP packets from the first DHCP Relay agent are forwarded to the DHCP Server.

DHCPv6 Relay Process

DHCPv6 client obtains an IPv6 address and other network configuration parameters from a DHCPv6 server through a DHCPv6 relay agent.

1. The DHCPv6 client sends a Solicit message to the multicast address FF02::1:2 of all the DHCPv6 servers and relay agents.
2. After the Solicit message is received, the DHCPv6 relay agent encapsulates the message into a Relay-forward message, and sends the message to the DHCPv6 server.
3. When the DHCPv6 server receives the Relay-forward message, the DHCPv6 server:
 - Provides an IPv6 address and other required parameters.
 - Adds them to the Relay-reply message.
 - Sends the Relay-reply message to the DHCPv6 relay agent.
4. Once the DHCPv6 relay agent receives the Relay-reply message, the DHCPv6 relay agent will send the reply to the DHCPv6 client.
5. The DHCPv6 client uses the IPv6 address and other network parameters to complete the network configuration.

IP Command Syntax	
(cfg)# ip dall	(cfg)# no ip ipv6
(cfg)# ip addr [ipAddr:ipAddr]	(cfg)# ip relay
(cfg)# ip addr [ipAddr:ipAddr] link	(cfg)# no ip relay
(cfg)# ip addr [ipAddr:ipAddr] prefix [plen:1-128]	(cfg)# ip remoteid
(cfg)# ip net [subnet:ipAddrv4]	(cfg)# no ip remoteid
(cfg)# ip gw [gateway:ipAddr]	(cfg)# ip stateless
(cfg)# ip dnsaddr [ipAddr:ipAddr]	(cfg)# no ip stateless
(cfg)# ip circuitid	(cfg)# ip v6circuitid
(cfg)# no ip circuitid	(cfg)# no ip v6circuitid
(cfg)# ip dhcp	(cfg)# ip v6relay
(cfg)# no ip dhcp	(cfg)# no ip v6relay
(cfg)# ip dhcpv6	(cfg)# ip v6remoteid
(cfg)# no ip dhcpv6	(cfg)# no ip v6remoteid
(cfg)# ip dns	(cfg)# ip rserv [ipAddr:ipAddr]
(cfg)# no ip dns	(cfg)# ip rtype drop
(cfg)# ip ipv4	(cfg)# ip rtype keep
(cfg)# no ip ipv4	(cfg)# ip rtype replace
(cfg)# ip ipv6	

Syntax	Name Description	Format Values
[ipAddr:ipAddr]	IPv4 or IPv6 address	ipv4 or ipv6 address
[plen:1-128]	subnet mask or prefix length	1-128
[subnet:ipAddrv4]	IPv4 subnet mask	subnet mask address
[gateway:ipAddr]	gateway address	gateway ip address

3.1.9 LAG Command

The *lag* command provides the ability to configure the ports on the module to support Link Aggregation Group and Link Aggregation Control Protocol. Use the *show lag* command from the # prompt to determine the state of the command option (disabled or enabled).

```
(cfg)# lag ?
Possible next parameters:
  <cr>
  dall          delete LAG configured settings, restore defaults
  fwd           frame forwarding algorithm
  lp            aggregator logical port number
  spri         system priority

(cfg)# lag

(cfg)# lag lp 12
Nesting level change accepted

(cfg-lag) [12]#
Possible next parameters:
  act          maximum number of active ports in a LAG
  active       LAG active mode
  aggrk        aggregator admin key
  exit         exit LAG instance
  fast        port fast timeout
  key         port auto key adjust
  lag         LAG module/aggregator
  no         negate a LAG option

(cfg-lag) [12]#

(cfg)# port select 1
Nesting level change accepted

(cfg-if) [1]# lag ?
Possible next parameters:
  clr          clear statistic counters
  lp           aggregator logical port number
  ppri        port priority
  proto       LACP protocol configuration

(cfg-if) [1]# lag
```

The command options available using the *lag* command are shown below.

The *lag* command option disables/enables LAG protocol. The *no* command negates the command.

The *dall* command option deletes all LAG configured settings and restores to factory defaults.

The *fwd* command option configures the frame forwarding algorithm: std or xor.

The *lp* command option sets the logical port number for LAG.

The *spri* command option configures the system priority.

Command options under the *lp <lNum>* command.

The *act* command option selects the maximum number of active ports in a Link Aggregation Group.

The *active* command option disables/enables port active mode and enables/disables port passive mode.

The *no* command negates the command.

The *aggrk* command option sets the link aggregation group key.

The *exit* command option exits the current nesting level.

The *fast* command option disables/enables LACP fast transmission mode and enables/disables slow transmission mode. The *no* command negates the command.

The *key* command option disables/enables automatic key adjustment and enables/disables manual key usage. The *no* command negates the command.

The *lag* command option disables/enables LAG on the module. The *no* command negates the command.

The *no* command option negates a command.

Command options under the *port select <pNum>* command.

The *clr* command option allows the port statistic counters to be cleared to zero.

The *lp* command option sets the logical port number for LAG.

The *ppri* command option configures the port priority.

The *proto* command option configures how the LAG protocol will be handled.

discard LACP is disabled, LACP frames are discarded

peer LACP is enabled, LAG is enabled

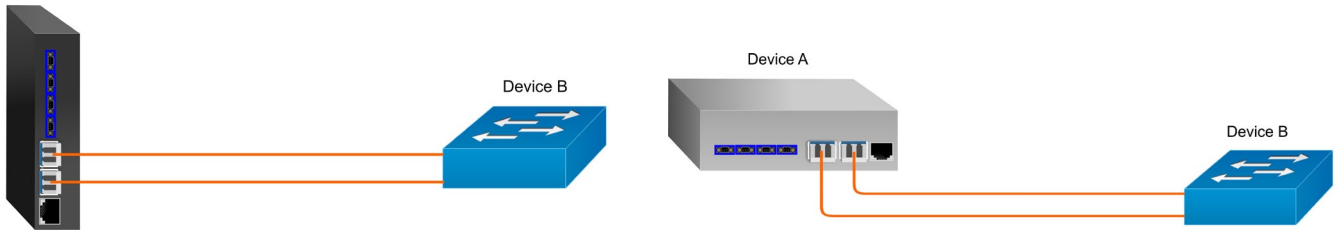
static LACP is disabled, LAG is enabled

tunnel LACP is disabled, LACP frames are tunneled, LAG is disabled

NOTE: Ports 1-4 do not support Static LAG manual configuration, also known as no LACP LAG.

The following example configures LACP/LAG on Fiber Port 1 and Fiber Port 2.

Device A



```
# config
Nesting level change accepted

(cfg)# port select f1
Nesting level change accepted

(cfg-if) [f1]# lldp proto tunnel
(cfg-if) [f1]#exit

(cfg)# port select f2
Nesting level change accepted

(cfg-if) [f2]# lldp proto tunnel
(cfg-if) [f1]#exit

(cfg)# lag lp L3
Nesting level change accepted

(cfg-lag) [13]#
(cfg-lag) [13]# act 2
(cfg-lag) [13]# lag
(cfg-lag) [13]# exit

(cfg)# lag

(cfg)#
```

To view the changes or display the LAG configuration settings, use the *show lag* command from the # prompt.

LAG Command Syntax	
(cfg)# lag	(cfg-lag)# lag
(cfg)# no lag	(cfg-lag)# no lag
(cfg)# lag dall	(cfg-lag)# aggrk [kVal:0-65535]
(cfg)# lag spri [sNum:0-65535]	(cfg-lag)# act [aNum:1-4]
(cfg)# lag fwd std	(cfg-lag)# exit
(cfg)# lag fwd xor	(cfg)# port select <pNum> (accesses next nesting level)
(cfg)# lag lp [INum:l1..l8] (accesses next nesting level)	(cfg-if)#<pNum> lag ppri [priNum:0-65535]
(cfg-lag)# lag lp [INum:l1..l8]	(cfg-if)#<pNum> lag proto discard
(cfg-lag)# active	(cfg-if)#<pNum> lag proto peer
(cfg-lag)# no active	(cfg-if)#<pNum> lag proto static
(cfg-lag)# fast	(cfg-if)#<pNum> lag proto tunnel
(cfg-lag)# no fast	(cfg-if)#<pNum> lag lp [INum:l1..l8]
(cfg-lag)# key	(cfg-if) <pNum> lag clr
(cfg-lag)# no key	(cfg-if)# exit

Syntax	Name Description	Format Values
[sNum:0-65535]	system priority	0-65535
[INum:l1..l8]	aggregator logical port number	l1-l8
[kVal:0-65535]	aggregator admin key	0-65535
[aNum:1-4]	max number of active ports in a LAG	1-4
[priNum:0-65535]	port priority	0-65535

3.1.10 LLDP Command

The IEEE 802.1ab Link Layer Discovery Protocol defines a standard way for Ethernet devices to advertise information about themselves to their neighbors and store information they discover from other device.

The *lldp* command provides the ability to configure the LLDP agent on the module.

```
(cfg)# lldp ?
Possible next parameters:
  dall          delete LLDP configuration settings, restore defaults
  txfin        fast message transmission interval
  txhld        multiplier of txrate for TTL value in PDU
  txrt         lldp normal transmission interval

(cfg)# lldp

(cfg)# port select 1
Nesting level change accepted

(cfg-if) [1]# lldp
Possible next parameters:
  mode          lldp mode
  proto         protocol configuration
  tlv           optional LLDP TLVs to send

(cfg-if) [1]# lldp
```

The command options available using the *lldp* command are shown below.

The *dall* command option deletes all LLDP configuration settings.

The *txfin* command option specifies the time interval between transmissions during fast transmission periods. The range is 1 to 3,600 seconds and the default value is 1 second.

The *txhld* command option configures the variable used as a multiplier of the Normal Transmission Interval to determine the time remaining before information in the outgoing LLDP PDU is no longer valid. The range is 1 to 10 and the default is 4.

The *txrt* command option configures the transmission frequency of LLDP updates in seconds. The range is 5 to 65,534 seconds and the default is 30 seconds.

Command options under the *port select <pNum>* command.

The *mode* command option configures the port to *receive*, *transmit*, or *transmit/receive* LLDP Protocol Data Units (PDUs).

The *proto* command option configures how LLDP PDUs are processed.

- discard* LLDP is disabled, LLDP frames are discarded
- peer* LLDP is enabled and protocol is operating
- tunnel* LLDP is disabled, LLDP frames are tunneled

The *tlv* command option selects which optional TLVs to include in the transmit LLDP PDUs. The *no* command negates the command.

- mgt* management address
- pdes* port description, same as port name
- sysname* system name, same as sysName object

sysdes system description, same as sysDescr object
syscap system capabilities

To tunnel LLDP on ports 1 and 2, use the following commands.

```
(cfg)# port select 1
Nesting level change accepted

(cfg-if) [1]# lldp proto tunnel
(cfg-if) [1]#exit

(cfg)# port select 2
Nesting level change accepted

(cfg-if) [2]# lldp proto tunnel
(cfg-if) [2]#exit

(cfg)#
```

To view the changes or display the LLDP configuration settings, use the *show lldp* command from the # prompt.

LLDP parameters that are not supported are *reinitDelay*, *txFastInit* and *txCredit*.

The *reinitDelay* sets the time from port disable to reinitialization. This parameter is not set.

The *txFastInit* configures the the number of LLDP PDUs that are transmitted during a fast transmission period. This parameter is set to 4.

The *txCredit* sets the maximum number of consecutive LLDP PDUs that can be transmitted at any time. This parameter is not set.

LLDP Command Syntax	
(cfg)# lldp dall	(cfg-if)#<pNum> lldp tlv pdes
(cfg)# lldp txfin [tSec:1-3600]	(cfg-if)#<pNum> no lldp tlv pdes
(cfg)# lldp txhld [tVal:2-10]	(cfg-if)#<pNum> lldp tlv sysname
(cfg)# lldp txrt [tSec:5-32768]	(cfg-if)#<pNum> no lldp tlv sysname
(cfg)# port select <pNum> (accesses next nesting level)	(cfg-if)#<pNum> lldp tlv sysdes
(cfg-if)#<pNum> lldp mode rxtx	(cfg-if)#<pNum> no lldp tlv sysdes
(cfg-if)#<pNum> lldp mode txonly	(cfg-if)#<pNum> lldp tlv syscap
(cfg-if)#<pNum> lldp mode rxonly	(cfg-if)#<pNum> no lldp tlv syscap
(cfg-if)#<pNum> lldp mode none	(cfg-if)#<pNum> lldp proto discard
(cfg-if)#<pNum> lldp tlv mgt	(cfg-if)#<pNum> lldp proto peer
(cfg-if)#<pNum> no lldp tlv mgt	(cfg-if)#<pNum> lldp proto tunnel

Syntax	Name Description	Format Values
[tSec:1-3600]	fast message transmission interval	1-3600 sec
[tVal:2-10]	multiplier of txrate for TTL value	2-10
[tSec:5-32768]	lldp normal transmission interval	5-32768 sec

3.1.11 LOCATION Command

The *location* command provides the ability to configure the physical location of the module including address, city, state, zip code, altitude, latitude and longitude.

```
(cfg)# location ?
Possible next parameters:
  addr          address and street
  alt           altitude
  city          city
  dall          delete 'location' configured settings, restore defaults
  lat           latitude
  long          longitude
  post          postal code/zipcode
  state         state/province name

(cfg)# location
```

The command options available using the *location* command are shown below.

The *addr* command option configures the physical module address.

The *alt* command option configures the module altitude for above or below sea level.

The *city* command option configures the city.

The *dall* command option deletes all location settings and restores factory defaults.

The *lat* command option configures the module latitude from -90.000000 degrees to +90.000000.

The *long* command option configures the module longitude from -180.000000 degrees to +180.000000.

The *post* command option configures the postal zone or zip code.

The *state* command option configures the state.

To configure the location for the module, use the following commands.

```
(cfg)# location addr "38 Tesla"
(cfg)# location city "Irvine"
(cfg)# location state "Ca"
(cfg)# location post 92618

(cfg)#
```

When configuring text based names, such as 38 Tesla, the text name must be in “ ” for the command to be valid (*location addr “38 Tesla”*). If the text based name does not have any spaces between the words, then “ ” are not necessary (*location addr 38_Tesla*).

To view the changes or display the LOCATION configuration settings, use the *show location* command from the # prompt.

LOCATION Command Syntax	
(cfg)# location dall	(cfg)# location post [mPost:string0..16]
(cfg)# location addr	(cfg)# location lat
(cfg)# location addr [mAddr:string0..32]	(cfg)# location lat [mLat:_90-90]
(cfg)# location city	(cfg)# location long
(cfg)# location city [mCity:string0..32]	(cfg)# location long [mLong:_180-180]
(cfg)# location state	(cfg)# location alt
(cfg)# location state [mState:string0..32]	(cfg)# location alt [mAlt:_1000000-10000000]
(cfg)# location post	

Syntax	Name Description	Format Values
[mAddr:string0..32]	address and street names	string 0-32 characters
[mCity:string0..32]	city name	string 0-32 characters
[mState:string0..32]	state name	string 0-32 characters
[mPost:string0..16]	postal code or zip code	string 0-16 characters
[mLat:_90-90]	latitude	-90.000000 - 90.000000 degrees
[mLong:_180-180]	longitude	-180.000000 - 180.000000 degrees
[mAlt:_1000000-10000000]	altitude	-1,000,000 - 10,000,000 meters

3.1.12 LR Command

The *lr* command configures the module for link redundancy. When configured for link redundancy, the module will transmit and receive traffic on the primary port (F1) and no traffic on the backup port (F2). When a fiber failure occurs on the primary port, the module will switch over to the backup port within 50msec.

Use the *show lr* command from the # prompt to determine the state of the command option (disabled or enabled).

```
(cfg)# lr ?
Possible next parameters:
  <cr>
  dall      delete redundancy configured settings, restore defaults
  ret       return to working port

(cfg)# lr
```

The command options available using the *lr* command are shown below.

The *lr* command option disables/enables link redundancy. The *no* command negates the command.

The *dall* command option deletes all link redundancy configuration settings and restores factory defaults.

The *ret* command option disables/enables the return to the primary link when the link failure has been resolved. The *no* command negates the command.

To enable link redundancy and configure the link not to return to the primary link when the link failure has been fixed, use the following command.

```
(cfg) lr
```

To enable link redundancy and configure the link to return to the primary link when the link failure has been fixed, use the following command.

```
(cfg) lr ret
(cfg) lr
```

To enable link redundancy, the on-board DIP switches (hardware controlled) must be disabled. Use the *no module dipsw* command from the <cfg># prompt to disable the DIP-switches. Verify the configuration by using the *show switch* command from the # prompt.

To view the changes or display the LR configuration settings, use the *show lr* command from the # prompt.

LR Command Syntax	
(cfg)# lr	(cfg)# lr ret
(cfg)# no lr	(cfg)# no lr ret
(cfg)# lr dall	

3.1.13 MLD Command

Multicast Listener Discovery (MLD) snooping allows the switch to view MLD packets and make decisions based on their content. MLD uses source-based filtering, which enables hosts and routers to specify which multicast sources should be allowed or blocked for a specific multicast group.

MLD snooping constrains IPv6 multicast traffic at Layer 2 by configuring Layer 2 LAN ports to forward IPv6 multicast traffic only to those ports that want to receive it.

The *mld* command provides the ability to configure MLD on the module. Use the *show mld* command from the # prompt to determine the state of the command option (disabled or enabled).

```
(cfg)# mld ?
Possible next parameters:
  dall          delete MLD configured, instances, restore defaults
  flood        MLD route subject to aging out
  snooping     MLD snooping
  to          MLD route aging
  vid         VLAN ID

(cfg)# mld

(cfg)# mld vid 1 grp ff02::1:ff4b:521
Nesting level change accepted

(cfg-mld) [vid 1, ff02::1:ff4b:521]#
Possible next parameters:
  aging        route subject to aging out
  exit        exit MLD instance
  no          negate a MLD option
  ph          host port
  pr          router port

(cfg-mld) [vid 1, ff02::1:ff4b:521]#
```

The command options available using the *mld* command are shown below.

The *dall* command option deletes all MLD configured settings and restores factory defaults.

The *flood* command option disables/enables the flooding all unrecognized MLD groups. Use the *no* command to negate the command.

The *snooping* command option disables/enables snooping. Use the *no* command to negate the command.

The *to* command option configures the MLD route aging time in seconds. The default value is 60 seconds.

The *vid* command option configures the VLAN ID associated with the MLD group.

grp configures the IP address of the MLD group.

Command options under the *vid <vVid> grp <ipAddr>* command.

The *aging* command option selects the timeout value in seconds to automatically remove a route from the forwarding database. The timeout never expires with a value of 0.

The *exit* command option exits the current nesting level.

The *no* command option negates a command.

The *ph* command option configures the port number that is connected to the MLD host. This can be a single or multiple ports.

The *pr* command option configures the port number that is connected to the MLD router. This can be a single or multiple ports.

To enable MLD snooping and flood with snooping timeout value to 45 seconds, use the following commands.

```
(cfg)# mld snooping
(cfg)# mld flood
(cfg)# mld to 45

(cfg)#
```

To configure a VLAN ID to the MLD interface, use the following commands.

```
(cfg)# mld vid 1

(cfg)#
```

To configure a manual MLD multicast group for “ff02::1:ff4b:531” on VLAN ID 1 with router port on Port 2 and host port on Port 4, use the following commands.

```
(cfg)# mld vid 1 grp ff02::1:ff4b:531
Nesting level change accepted

(cfg-mld) [vid 1, ff02::1:ff4b:531]# pr 2
(cfg-mld) [vid 1, ff02::1:ff4b:531]# ph 4
(cfg-mld) [vid 1, ff02::1:ff4b:531]# aging
(cfg-mld) [vid 1, ff02::1:ff4b:531]# exit

(cfg)#
```

To view the changes or display the MLD configuration settings, use the *show mld* command from the # prompt.

There are common variables that are shared between the IGMP and MLD protocols. The variables are Snooping (enable / disable), Flooding Unrecognized Groups (enable / disabled) and Route Aging timer. If either protocol changes the shared variables, they will be changed under both protocols (IGMP and MLD). Example: If Snooping is enabled under MLD, Snooping will be enabled under IGMP.

MLD Command Syntax	
(cfg)# mld dall	(cfg)# mld vid [vVid:1-4095] grp [ipAddr:ipAddrv6] (accesses next nesting level)
(cfg)# mld flood	(cfg-mld)# ph [hNum:f1,f2,1..4 all]
(cfg)# no mld flood	(cfg-mld)# pr [rNum:f1,f2,1..4 all]
(cfg)# mld snooping	(cfg-mld)# aging
(cfg)# no mld snooping	(cfg-mld)# no aging
(cfg)# mld to [toVal:0-65535]	(cfg-mld)# exit
(cfg)# mld vid [vVid:1-4095]	(cfg)# exit
(cfg)# no mld vid [vVid:1-4095]	
(cfg)# no mld vid [vVid:1-4095] grp [ipAddr:ipAddrv6]	

Syntax	Name Description	Format Values
[toVal:0-65535]	MLD route aging	0-65535 sec
[vVid:1-4095]	VLAN ID	1-4095
[ipAddr:ipAddrv6]	MLD group address IPv6	ipv6 address
[hNum:f1,f2,1..4 all]	host port number (on module)	f1,f2,1..4, or all
[rNum:f1,f2,1..4 all]	router port number (on module)	f1,f2,1..4, or all

3.1.14 MODBUS Command

MODBUS is commonly used in industrial environments to monitor, gather, process, and transfer real-time data between devices. Many devices such as PLCs, intelligent devices, sensors, and instruments use MODBUS for SCADA (Supervisory Control And Data Acquisition Systems). SCADA is a system of software and hardware elements that allows industrial organizations to control industrial processes locally or at remote locations.

The MODBUS protocol is a request-response protocol between the Client and Server. A client can request the MODBUS server to act, and the server will respond with that action.

MODBUS awareness on the OmniConverter and RuggedNet products is MODBUS-TCP Server functionality.

The *modbus* command provides the ability to configure the Modbus-TCP server on the module. Use the *show modbus* command from the # prompt to display the configuration.

```
(cfg)# modbus ?
Possible next parameters:
  dall          delete all configured settings and restore defaults
  sto           session timeout value 0-900
  tcpserver     enable/disable tcpserver
  tsport        tcpserver port value 1-65535

(cfg)# modbus
```

The options available using the *modbus* command are shown below.

The *dall* command deletes all Modbus configured settings and restores factory defaults.

The *sto* command configures the session timeout for Modbus-TCP client connections.

The *tcpserver* command disables/enables the Modbus-TCP Server.

The *tsport* command configures the TCP port for the Modbus-TCP server function.

To enable MODBUS server, use the following commands.

```
(cfg)# modbus tcpserver

(cfg)#
```

To view the changes or display the MODBUS configuration settings, use the *show modbus* command from the # prompt.

MODBUS Command Syntax	
(cfg)# modbus dall	(cfg)# modbus tcpserver
(cfg)# modbus tsport [pNum:1-65535]	(cfg)# no modbus tcpserver
(cfg)# modbus sto [sTim:0-900]	

Syntax	Name Description	Format Values
[pNum:1-65535]	tcp server port number	1-65535 characters
[sTim:0-900]	tcp server session time out	0-900 seconds

The following Modbus function codes are recognized by the module.

Function Codes	
Function Code	Function Description
1 (0x01)	Read Coils; read up to 2000 contiguous coils
2 (0x02)	Read Discrete Inputs; read up to 2000 contiguous discrete inputs
3 (0x03)	Read Holding Registers; read up to 125 consecutive holding registers
4 (0x04)	Read Input Registers; read up to 125 consecutive input registers
5 (0x05)	Write Single Coil
6 (0x06)	Write Single Register
15 (0x0F)	Write Multiple Coils; write a sequence of up to 1968 coils at once.
16 (0x10)	Write Multiple Registers; write 1 to 123 registers in one command
22 (0x16)	Mask Write Register; result = (current AND And_Mask) OR (Or_Mask AND (NOT And_Mask))
23 (0x17)	Read/Write Multiple Registers; perform one read operation and one write operation in a single transaction.

Modbus defines a data model consisting of a set of registers which can be read and written using the Modbus-TCP protocol.

Data Model		
Block Address Range	Block Name	Block Contents
000001 - 065536	Coils	read-write booleans
100001 - 165536	Discrete Inputs	read-only booleans
300001 - 365536	Input Registers	read-only 16-bit integers (int16_t or uint16_t)
400001 - 465536	Holding Registers	read-write 16-bit integers (int16_t or uint16_t)

Modbus-TCP client applications register mapping.

Aggregate Data Types	
New Data Type Description	Modbus Mapping
read-only 32-bit integer (int32_t or uint32_t)	2 Consecutive Input Registers (MSB at offset 3, LSB at offset 0)
read-write 32-bit integer (int32_t or uint32_t)	2 Consecutive Holding Registers (MSB at offset 3, LSB at offset 0)
read-only 64-bit integer (int64_t or uint64_t)	4 Consecutive Input Registers (MSB at offset 3, LSB at offset 0)
read-write 64-bit integer (int64_t or uint64_t)	4 Consecutive Holding Registers (MSB at offset 3, LSB at offset 0)
read-only string (NULL terminated)	((LEN + 1) / 2) Input Register(s)
read-write string (NULL terminated)	((LEN + 1) / 2) Holding Register(s)

Modbus Discrete Input represents a single-bit of read-only state information. This data type is used to report read-only boolean status information from the module.

Discrete Input					
Start Address	Item Size	Num Items	Description	ON	OFF
1	1	32	Fiber Port 1..32 Linked	Linked	Not Linked
33	1	32	RJ-45 Port 1..32 Linked	Linked	Not Linked
65	1	32	RJ-45 Port 1..32 Full Duplex	FDX	HDX
97	1	32	RJ-45 Port 1..32 Flow Control Enabled	Enabled	Disabled
300	1	1	Alarm relay activation state; RuggedNet Only	Relay Energized	Relay De-energized
301	1	1	Alarm input state; RuggedNet Only	Open	Closed
400	1	32	PoE Port Powered Status for Port 1..32 PoE Models only	Powering	Not Powering

A Modbus Coil represents a single-bit of read-write state information.

Coil Assignments					
Start Address	Item Size	Num Items	Description	ON	OFF
1	1	32	Fiber Port 1..32 Enabled	Port Enabled	Port Disabled
33	1	32	RJ-45 Port 1..32 Enabled	Port Enabled	Port Disabled
100	1	1	Reboot Module	Reboot	NA
101	1	1	Reboot Module to Backup Image	Swap+ Reboot	NA
102	1	1	Restore Defaults and Reboot	Restore+ Reboot	NA
103	1	1	Restore Defaults and Reboot with -keep option	RestoreKeep+ Reboot	NA
200	1	1	Clear portstats for all ports	Clear All Counts	NA
201	1	32	Clear portstats for Fiber Port 1..32	Clear Per-Port Counts	NA
233	1	32	Clear portstats for RJ-45 Port 1..32	Clear Per-Port Counts	NA
300	1	1	Save current settings	Save current settings	NA

A Modbus Input Register represents a sixteen-bit word of read-only state information.

Input Register Assignments				
Start Address	Item Size	Num Items	Description	Data Type
1	1	1	Magic/Vendor	uint16_t (0x0687)
2	1	1	Format Code	uint16_t (0x100)
100	33	1	Model Name	string(0..64+NULL)
133	33	1	Serial Number	string(0..64+NULL)
166	33	1	Base MAC	string(0..64+NULL)
199	33	1	Model Family	string (0..64+NULL)
232	33	1	Model Number	string (0..64+NULL)
265	5	1	Mfg Date YYYYMMDD	string (0..8+NULL)
270	1	1	Number of Fiber Ports	uint16_t
271	1	1	Number of Copper Ports	uint16_t
272	1	1	Number of PoE Capable Ports	uint16_t
300	64	1	Firmware Version	string(0..127+NULL)
364	64	1	Backup Firmware Version	string(0..127+NULL)
428	64	1	Bootloader Firmware Version	string(0..127+NULL)
600	1	1	Input Voltage A	uint16_t, mV
601	1	1	Input Voltage B (RuggedNet dual input only)	uint16_t, mV
602	1	1	Current Usage	uint16_t, A * 10
603	1	1	Temperature in Celsius	int16_t, C * 10, -3276.8 to 3276.7
700	1	1	CPU Utilization	uint16_t, 0..100%
701	1	1	RAM Utilization	uint16_t, 0..100%
702	1	1	Code Flash Utilization	uint16_t, 0..100%
703	2	1	Uptime (seconds)	uint32_t, 0..2^32-1
800	1	32	PoE Port Power Usage for Port 1..32 (PoE Models Only)	uint16_t (W * 10)
832	1	32	PoE Port Power Class for Port 1..32 (PoE Models Only)	uint16_t
900	1	32	Fiber Port Type 1..32 (1=SFP, 2=FF, 3=LC, 4=UTP)	enum
932	1	32	Fiber Port Speed 1..32 (1=10, 2=100, 3=1000, 4=10000, 5=2500, 6=5000)	enum
964	1	32	Copper Port Speed 1..32 (1=10, 2=100, 3=1000, 4=10000, 5=2500, 6=5000)	enum

Input Register Assignments				
Start Address	Item Size	Num Items	Description	Data Type
1000	4	32	Rx Bytes On Fiber Port 1..32	uint64_t
1128	4	32	Tx Bytes On Fiber Port 1..32	uint64_t
1256	4	32	Rx Frames On Fiber Port 1..32	uint64_t
1384	4	32	Tx Frames On Fiber Port 1..32	uint64_t
1512	4	32	CRC Errors On Fiber Port 1..32	uint64_t
1640	4	32	Tx Pause Frames On Fiber Port 1..32	uint64_t
1768	4	32	Rx Pause Frames On Fiber Port 1..32	uint64_t
1896	4	32	Rx Bytes On RJ-45 Port 1..32	uint64_t
2024	4	32	Tx Bytes On RJ-45 Port 1..32	uint64_t
2152	4	32	Rx Frames On RJ-45 Port 1..32	uint64_t
2280	4	32	Tx Frames On RJ-45 Port 1..32	uint64_t
2408	4	32	CRC Errors On RJ-45 Port 1..32	uint64_t
2536	4	32	Tx Pause Frames On RJ-45 Port 1..32	uint64_t
2664	4	32	Rx Pause Frames On RJ-45 Port 1..32	uint64_t

A Modbus Holding Register represents a sixteen-bit word of read-write state information.

Holding Register Assignments				
Start Address	Item Size	Num Items	Description	Data Type
1	128	1	Chassis Name	string(0..255+NULL)
129	128	1	Module ID	string (0..255+NULL)
257	128	1	System Contact	string(0..255+NULL)
385	128	1	System Location	string(0..255+NULL)
600	33	1	Alarm Digital Input Name (RuggedNet Only)	string (0..64+NULL)
633	33	1	Alarm Relay Normally Open Name (RuggedNet Only)	string (0..64+NULL)
666	33	1	Alarm Relay Normally Close Name (RuggedNet Only)	string (0..64+NULL)
1000	23	32	Fiber Port Name 1..32	string (0..45+NULL)
1736	23	32	Copper Port Name 1..32	string (0..45+NULL)
2500	33	1	Time of Day (24hr): MM/DD/YYYY HH:MM:SS	string(0..64+NULL)
2533	3	1	Time Zone Abbreviation	string(0..5+NULL) - see User Manual or run 'zone -h' for list of valid time zone abbreviations

3.1.15 MODULE Command

The *module* command provides the ability to configure the serial interface baud rate, chassis name, module identifier and enable/disable hardware DIP-switches. Use the *show module* command from the # prompt to determine the state of the command option (disabled or enabled).

```
(cfg)# module ?
Possible next parameters:
  baud          serial port baudrate
  dall          delete module configured settings, restore defaults
  dipsw         global DIP switch configuration
  id            module identification
  nm           location name
  prmpt        CLI prompt
  sysContact    system contact
  sysLoc       system location

(cfg)# module
```

The command options available using the *module* command are shown below.

The *baud* command option configures the baud rate of the serial interface. The default rate is 57,600bps.

The *dall* command option restores the factory defaults of all module settings.

The *dipsw* command option disables/enables the hardware DIP-switches and prevents the CLI commands from overriding the functions. Use the *no* command to allow the soft switches or to disable the hardware DIP-switches.

The *id* command option configures the module identifier. The module identifier can be any 0-255 alphanumeric character string.

The *nm* command option configures the chassis name. The chassis name can be any 0-255 alphanumeric character string.

The *prmpt* command option configures the name associated with the module prompt.

The *sysContact* command option configures the system contact name.

The *sysLoc* command option configures the system location name.

To change the baud rate of the serial port, use the following command.

```
(cfg)# module baud 115200
(cfg)#
```

To view the changes or display the MODULE configuration settings, use the *show module* command from the # prompt.

MODULE Command Syntax	
(cfg)# module dall	(cfg)# module prmpt [pName:string0..32]
(cfg)# module baud [baudRate:300..115200]	(cfg)# module dipsw
(cfg)# module id	(cfg)# no module dipsw
(cfg)# module id [modId:string0..255]	(cfg)# module sysContact
(cfg)# module nm	(cfg)# module sysContact [sysContactName:string0..255]
(cfg)# module nm [locationName:string0..255]	(cfg)# module sysLoc
(cfg)# module prmpt	(cfg)# module sysLoc [sysLocName:string0..255]

Syntax	Name Description	Format Values
[baudRate:300..115200]	serial port baud rate	300,1200,4800,9600,19200,...115200
[modId:string0..255]	module identification	0-255 characters
[locationName:string0..255]	location name	0-255 characters
[pName:string0..32]	CLI prompt	0-32 characters
[sysContactName:string0..255]	system contact name	0-255 characters
[sysLocName:string0..255]	system location name	0-255 characters

3.1.16 MRP Command

IEC 62439-2 defines Media Redundancy Protocol (MRP) as a ring protocol that is used in high availability industrial networks.

In an MRP ring, the ring manager is named Media Redundancy Manager (MRM) and the ring clients are named Media Redundancy Clients (MRCs).

MRM and MRC ring ports support three status: disabled, blocked, and forwarding. Disabled ring ports drop all the received frames. Blocked ring ports drop all the received frames except the MRP control frames. Forwarding ring ports forward all the received frames.

During normal operation, the network works in the Ring-Closed status. In this status, one of the MRM ring ports is blocked, while the other is forwarding. Conversely, both ring ports of all MRCs are forwarding. Loops are avoided because the physical ring topology is reduced to a logical stub topology.

In case of failure, the network works in the Ring-Open status. For instance, in case of failure of a link connecting two MRCs, both ring ports of the MRM are forwarding; the MRCs adjacent to the failure have a blocked and a forwarding ring port; the other MRCs have both ring ports forwarding. Also, in the Ring-Open status, the network logical topology is a stub.

The *mrp* command provides the ability to configure MRP on the module. Use the *show mrp* command from the # prompt to determine the state of the command option (disabled or enabled).

```
(cfg)# mrp ?
Possible next parameters:
  <cr>
  dall          delete MRP settings, instances, restore defaults
  pn           MRP profile name

(cfg)# mrp

(cfg)# mrp pn protect
Nesting level change accepted

(cfg-mrp) [protect]#
Possible next parameters:
  dom          ring domain id
  exit         exit MRP instance
  pri          ring priority
  rec          recovery time
  role         MRP role
  rp1          ring port 1
  vid          MRP vlan id

(cfg-mrp) [protect]#

(cfg)# port select 1
Nesting level change accepted

(cfg-if) [1]# mrp ?
Possible next parameters:
  <cr>
  port         forwarding MRP

(cfg-if) [1]# mrp
```

The command options available using the *mrp* command are shown below.

The *mrp* command option disables/enables MRP on the module. The *no* command negates the command.

The *dall* command option deletes all MRP settings, instances and restores factory default settings.

The *pn* command option configures the MRP profile instance name.

Command options under the *pn <pName>* command.

The *dom* command option sets the MRP domain identification number (UUID) via 32 hexadecimal characters. The default value is “FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFFFF”.

The *exit* command option exits the current nesting level.

The *pri* command option configures the MRP instance priority.

The *rec* command option configures the MRP maximum recovery time.

The *role* command option configures the MRP role for the module: MRC or MRM.

mrc configures media redundancy client.

mrp configures media redundancy manager.

The *rp1* command option configures the port number for Ring Port 1.

rp2 configures the port number for Ring Port 2.

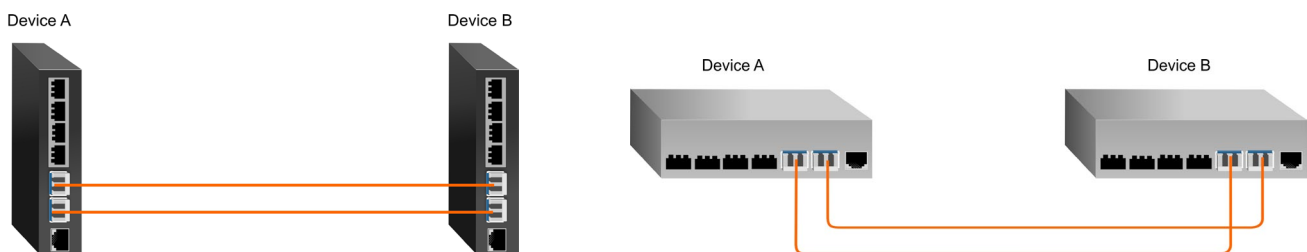
The *vid* command option selects the VLAN MRP protocol Identification.

Command options under the *port select <pNum>* command.

The *mrp* command option disables/enables a port as an MRP ring port if associated with a port. The *no* command negates the command.

The *port* command option disables/enables normal MRP operations on a port when associated with an MRP instance. The *no* command negates the command.

The following script is an example of a MRP configuration.



Device A Setup

```
(cfg)# vlan dall
(cfg)# switchport dall

(cfg)# vlan vid 100
(cfg)# vlan vid 111

(cfg)# port select 4

(cfg-if)[4]# switchport mode tunnel
(cfg-if)[4]# switchport vid 100
(cfg-if)[4]# exit

(cfg)# port select f1
(cfg-if)[f1]# switchport mode trunk
(cfg-if)[f1]# switchport vidtrunk 1,100..102
(cfg-if)[f1]# exit

(cfg)# port select f2
(cfg-if)[f2]# switchport mode trunk
(cfg-if)[f2]# switchport vidtrunk 1,100..102
(cfg-if)[f2]# exit

(cfg)# mrp dall
(cfg)# port select f1
(cfg-if)[f1]# mrp
(cfg-if)[f1]# exit

(cfg)# port select f2
(cfg-if)[f2]# mrp
(cfg-if)[f2]# exit

(cfg)# mrp
(cfg)# mrp pn mrm_100
(cfg-mrp)# rp1 F1 rp2 F2
(cfg-mrp)# role mrm
(cfg-mrp)# rec 200
(cfg-mrp)# vid 100
(cfg-mrp)# dom FFFFFFFF-FFFF-F112-2334-455666778899
(cfg-mrp)# pri 200
(cfg-mrp)# exit

(cfg)#
```

Module is configured as the Media Redundancy Manager (MRM)

Device B Setup

```
(cfg)# vlan dall
(cfg)# switchport dall

(cfg)# vlan vid 100
(cfg)# vlan vid 111

(cfg)# port select 4

(cfg-if)[4]# switchport mode tunnel
(cfg-if)[4]# switchport vid 100
(cfg-if)[4]# exit

(cfg)# port select f1
(cfg-if)[f1]# switchport mode trunk
(cfg-if)[f1]# switchport vidtrunk 1,100..102
(cfg-if)[f1]# exit

(cfg)# port select f2
(cfg-if)[f2]# switchport mode trunk
(cfg-if)[f2]# switchport vidtrunk 1,100..102
(cfg-if)[f2]# exit

(cfg)# mrp dall
(cfg)# port select f1
(cfg-if)[f1]# mrp
(cfg-if)[f1]# exit

(cfg)# port select f2
(cfg-if)[f2]# mrp
(cfg-if)[f2]# exit

(cfg)# mrp
(cfg)# mrp pn mrc_100
(cfg-mrp)# rp1 F1 rp2 F2
(cfg-mrp)# role mrc
(cfg-mrp)# rec 200
(cfg-mrp)# vid 100
(cfg-mrp)# dom FFFFFFFF-FFFF-F112-2334-455666778899
(cfg-mrp)# pri 200
(cfg-mrp)# exit

(cfg)#
```

Module is configured as the Media Redundancy Client (MRC)

To view the changes or display the MRP configuration settings, use the *show mrp* command from the # prompt.

MRP Command Syntax	
(cfg)# mrp	(cfg-mrp)# rec [rTime:200,500]
(cfg)# no mrp	(cfg-mrp)# vid [vlanId:1-4095]
(cfg)# mrp dall	(cfg-mrp)# exit
(cfg)# no mrp pn [pName:string1..32]	(cfg)# port select <pNum> (accesses next nesting level)
(cfg)# mrp pn [pName:string1..32] (accesses next nesting level)	(cfg-if)#<pNum> mrp
(cfg-mrp)# rp1 [pNum1] rp2 [pNum2]	(cfg-if)#<pNum> no mrp
(cfg-mrp)# role mrc	(cfg-if)#<pNum> mrp port
(cfg-mrp)# role mrm	(cfg-if)#<pNum> no mrp port
(cfg-mrp)# dom [dId:hex128]	(cfg-if)#v exit
(cfg-mrp)# pri [priNum:0-65535]	

Syntax	Name Description	Format Values
[pName:string1..32]	MRP profile name	1-32 character
[pNum1:f1,f2,1..4 all]	ring port 1	f1,f2,1..4, or all
[pNum2:f1,f2,1..4 all]	ring port 2	f1,f2,1..4, or all
[dId:hex128]	ring domain id	32 ascii hex characters
[priNum:0-65535]	ring priority	0-65535
[rTime:200,500]	recovery time	200, 500 sec
[vlanId:1-4095]	MRP vlan id	1-4095

3.1.17 PORT Command

The *port* command provides the ability to configure each port with specific parameters. Use the *show port* command from the # prompt to determine the state of the command option (disabled or enabled).

```
(cfg)# port ?
Possible next parameters:
  dall      delete configured port settings, restore defaults
  select    port selection

(cfg)# port

(cfg)# port select 1
Nesting level change accepted

(cfg-if) [1]# ?
Possible next parameters:
  aaa      authentication, authorization, accounting configuration
  bwp      bandwidth profile configuration port instance
  cabletest cable instance testing
  exit     exit port interface configuration
  lag      link aggregation group configuration
  lldp     link layer discovery protocol (LLDP) configuration
  mrp      port MRP
  no       negate a command
  port     port instance configuration
  portaccess port access configuration
  portstat port statistic configuration
  pse      power source equipment (PSE) configuration
  spantree spanning tree configuration
  switchport vlan interface configuration

(cfg-if) [1]#

(cfg-if) [1]# port ?
Possible next parameters:
  flow      flow control
  learning  MAC learning
  loop      loop protection
  loopt     loop protection transmit interval
  mirror    mirror source port
  mo        port rate, negotiation, duplex setting
  name      port name
  output    port output
  secure    unknown Multicast/Unicast addresses

(cfg-if) [1]# port
```

The command options available using the *port* command are shown below.

The *dall* command option deletes all configured port attributes and restores factory default settings.

The *select* command option selects the port number to be configured.

Command options under the *port select <pNum>* command.

The *flow* command option disables/enables flow control on the selected port. The *no* command negates the command.

The *learning* command option disables/enables MAC learning on the selected port. The *no* command negates the command.

The *loop* command option disables/enables loop protection on the selected port. The *no* command negates the command.

The *loopt* command option configures the loop protection transmit interval from 1-60s.

The *mirror* command option disables/enables port mirroring. The *no* command negates the command.

The *mo* command option configures rate (10/100/1000), mode (an or man) and duplex (fdx or hdx) for the selected RJ-45 copper port.

The *name* command option configures the name for the selected port.

The *output* command option disables/enables the selected port. The *no* command negates the command.

The *secure* command option disables/enables the ability to drop unknown Multicast/Unicast addresses on the selected port. The *no* command negates the command.

To configure port F1 for manual operation, use the *mo* command.

```
(cfg)# port select f1
Nesting level change accepted

(cfg-if) [f1]# port mo man
(cfg-if) [f1]# exit

(cfg)#
```

The example below enables port mirroring of Port 1 to Port 2.

```
(cfg)# port select 1
Nesting level change accepted

(cfg-if) [1]# port mirror 2
(cfg-if) [1]# exit

(cfg)#
```

To view the changes or display the PORT configuration settings, use the *show port* command from the # prompt.

The *mo* command option provides configuration of the fixed RJ-45 port. The *mo* command option is a valid command to configure the fiber ports for AN or MAN only. **The module only supports auto-negotiation when configured for 1000. So when the 1000, Man, FDX or 1000, Man, HDX is used, the module still auto-negotiates with its link partner.**

The 1G fiber port will operate AN, 1000, FDX or Man, 1000, FDX.

The SPE ports are configured for AN, 10M, FDX.

When loop protection is enabled on a port, the port will generate Configuration Test Protocol (CTP) frames. When the module receives its own CTP message either on the generating port or another port, loop prevention will automatically block the port from sending out normal user data until the loop is removed.

When a port is blocked, the port will continue to send out periodic CTP frames in order to determine if the block has been removed. When the module does not receive its own CTP message either on the generating or another port, the port will be unblocked.

When port security is enabled on a port, the port will dropped all unknown Unicast and Multicast addresses. When port security is disabled, frames with unknown Unicast and Multicast addresses will be forwarded based on VLAN forwarding and learned MAC address forwarding rules.

PORT Command Syntax	
(cfg)# port dall	(cfg-if)#<pNum> no port output
(cfg)# port select [pNum:f1,f2,1..8 all,mgt1] (accesses next nesting level)	(cfg-if)#<pNum> port secure
(cfg-if)#<pNum> port flow	(cfg-if)#<pNum> no port secure
(cfg-if)#<pNum> no port flow	(cfg-if)#<pNum> port mirror [sourcePort:f1,f2,1..4]
(cfg-if)#<pNum> port learning	(cfg-if)#<pNum> no port mirror
(cfg-if)#<pNum> no port learning	(cfg-if)#<pNum> port name [name:string1..45]
(cfg-if)#<pNum> port loop	(cfg-if)#<pNum> port mo [rate,mode,dup:(10..10000), (an,man),(fdx,hdx)]
(cfg-if)#<pNum> no port loop	(cfg-if)#<pNum> port loopt [lTime:1-60]
(cfg-if)#<pNum> port output	(cfg-if)#<pNum> exit

Syntax	Name Description	Format Values
[pNum1:f1,f2,1..4 all,mgt1]	port selection	f1,f2,1..4, all, mgt1
[sourcePort::f1,f2,1..4]	mirror source port	f1,f2,1..4
[lTime:1-60]	loop protection transmit interval	1-60 sec
[rate,mode,dup:(10..10000),(an,man), (fdx,hdx)]	port rate, negotiation, duplex setting	(10..10000), mode (an,man), dup (fdx,hdx)
[name:string1..45]	port name	1-45 characters

3.1.18 PORTACCESS Command

The *portaccess* command provides the ability to control data access to each port on the module. Port Access can be configured to disable user access or enable user access. Port Access enables an administrator to control user access while maintaining port configuration for easy disabling or enabling of customer service. Use the *show portaccess* command from the # prompt to determine the state of the command option (disabled or enabled).

```
(cfg)# portaccess ?
Possible next parameters:
  dall          delete port access settings, restore defaults

(cfg)# portaccess

(cfg)# port select 1
Nesting level change accepted

(cfg-if) [1]# portaccess ?
Possible next parameters:
  <cr>

(cfg-if) [1]#
```

The command options available using the *portaccess* command are shown below.

The *dall* command option deletes all configured port access settings and restores factory defaults.

Command options under the *port select <pNum>* command.

The *portaccess* command option disables/enables the selected port. The *no* command negates the command.

To disable access to Port 2, use the following commands.

```
(cfg)# port select 2
Nesting level change accepted

(cfg-if) [2]# portaccess
(cfg-if) [2]# exit

(cfg)#
```

To view the changes or display the PORTACCESS configuration settings, use the *show portaccess* command from the # prompt.

PORTACCESS Command Syntax	
(cfg)# portaccess dall	(cfg-if)#<pNum> portaccess
(cfg)# port select <pNum> (accesses next nesting level)	(cfg-if)#<pNum> no portaccess

3.1.19 PROTOCOL Command

The *protocol* command provides the ability to enable/disable specific protocols available on the module. FTP, HTTP, HTTPS, IP, serial, Telnet and flow control can be configured using the *protocol* command.

Use the *show protocol* command from the # prompt to determine the state of the command option (disabled or enabled).

```
(cfg)# protocol ?
Possible next parameters:
  cfn          SSL/TLS certificate file name
  dall        delete protocol settings, restore defaults
  flow        flow control
  ftp         FTP protocol
  http        HTTP protocol (web page)
  https       HTTPS protocol (web page)
  ip          IP protocol
  l2cp        L2CP Tunneling
  serial      serial console port
  telnet      Telnet protocol

(cfg)# protocol
```

The command options available using the *protocol* command are shown below.

The *cfn* command option configures the SSL/TLS certificate file name for the module.

The *dall* command option deletes all configured protocol settings and restores factory defaults.

The *flow* command option disables/enables global flow control on the module. The *no* command negates the command.

The *ftp* command option disables/enables FTP protocol on the module. The *no* command negates the command.

The *http* command option disables/enables HTTP protocol on the module. The *no* command negates the command.

The *https* command option disables/enables HTTPS protocol on the module. The *no* command negates the command.

The *ip* command option disables/enables IPv4 protocol on the module. The *no* command negates the command.

The *l2cp* command option disables/enables L2CP protocol on the module. The *no* command negates the command.

The *serial* command option disables/enables the serial console port on the module. The *no* command negates the command.

The *telnet* command option disables/enables Telnet protocol on the module. The *no* command negates the command.

To enable FTP, use the following command. By default, FTP is disabled.

```
(cfg)# protocol ftp
```

To disable Telnet, use the following command. By default, Telnet is enabled.

```
(cfg)# no protocol telnet
```

To view the changes or display the PROTOCOL configuration settings, use the *show protocol* command from the # prompt.

If HTTPS is enabled and a certificate file is not configured via the *cfn* command, the self-generated certificate is used. If HTTPS is enabled and a certificate file is configured via the *cfn* command the user downloaded certificate is used. If HTTPS is enabled, SSL 2 & 3 and TLS 1.2 are used for web page access.

PROTOCOL Command Syntax	
(cfg)# protocol dall	(cfg)# protocol https
(cfg)# protocol cfn	(cfg)# no protocol https
(cfg)# protocol cfn [fileName:string0..45]	(cfg)# protocol ip
(cfg)# protocol flow	(cfg)# no protocol ip
(cfg)# no protocol flow	(cfg)# protocol l2cp
(cfg)# protocol ftp	(cfg)# no protocol l2cp
(cfg)# no protocol ftp	(cfg)# protocol serial
(cfg)# protocol http	(cfg)# no protocol serial
(cfg)# no protocol http	(cfg)# protocol telnet
	(cfg)# no protocol telnet

Syntax	Name Description	Format Values
[fileName:string0..45]	SSL/TLS certificate file name	0-45 characters

3.1.20 PSE Command

Only supported on OmniConverter and RuggedNet SPoE models.

The *pse* command provides the ability to configure SPoE scheduler, heartbeat parameters, LLDP-MED and SPoE power mode on each RJ-45 port.

The SPoE Scheduler provides the ability to configure the time and day for SPoE power to be turned On and Off. Up to 100 scheduling events can be configured.

Use the *show pse* command from the # prompt to determine the state of the command option (disabled or enabled).

```
(cfg)# pse ?
Possible next parameters:
  dall          delete PSE settings, instances, restore defaults
  idx           PoE scheduler index
  sched         enable global pse scheduling

(cfg)# pse

(cfg)# pse idx 1
Nesting level change accepted

(cfg-pse)[1]#
Possible next parameters:
  exit          exit schedule instance
  no            negate a PSE option
  pn           PoE scheduler profile name
  port         port list
  sched        schedule power on and off time
  schedule     enable specific schedule

(cfg-pse)[1]#

(cfg)# port select 1
Nesting level change accepted

(cfg-if)[1]# pse
Possible next parameters:
  hdfs         heartbeat restart defer
  heartbeat    heartbeat ping
  i            heartbeat interval
  lldp-med     LLDP-MED support for PoE PDs
  mode         pse mode
  pderr        number consecutive lost heartbeats for error
  pdint        number of times to restart PD after error
  pdip         ip address of PD for heartbeat
  pdmo         error mode action for PD error
  reset        restart PoE power

(cfg-if)[1]# pse
```

The command options available using the *pse* command are shown below.

The *dall* command option deletes all configured PSE settings and restores factory defaults.

The *idx* command option configures the PoE Scheduling index number (or sequence number). Multiple scheduling indexes can be configured.

The *schedule* command option disables/enables PSE power scheduler. The *no* command negates the command.

Command options under the *idx* command.

The *exit* command option exits the current nesting level.

The *no* command negates the PSE command options.

The *pn* command option configures the name of the scheduling profile for the selected scheduling index.

The *port* command option configures the port numbers associated with the selected scheduling index.

The *sched* command option configures the on time and off time for the selected scheduling index.

The *schedule* command option disables/enables the selected scheduling index. The *no* command negates the command.

Command options under the *port select <pNum>* command.

The *hdftr* command option selects the transmission interval delay before heartbeat pings are restarted after a reset.

The *heartbeat* command option disables/enables the heartbeat signal used to verify connectivity to the PD. *heartbeat* is disabled by default. The *no* command negates the command.

The *i* command option configures the transmission interval of the heartbeat signal. The default value is 1 second.

The *lldp-med* command option disables/enables LLDP-MED support for PoE PDs. The *no* command negates the command.

The *mode* command option configures the power sourcing mode for the selected port. PoE power can be auto detect or disabled (off).

<i>auto</i>	selects PSE enabled, advertising max power possible
<i>off</i>	selects PSE disabled

The *pderr* command option configures the number of consecutive lost heartbeats before an error condition is declared. The default value is 3 lost heartbeat signals.

The *pdint* command option configures the number of times a PD is restarted when *pdmode* is set to restart. The default value is 0 indicating no limit to the number of restarts.

The *pdip* command option configures the IP address of the PD. The IP address of the PD is used for the heartbeat signal.

The *pdmo* command option configures what action is taken when a heartbeat error condition is detected.

<i>restart</i>	forces a power down and power up on the PSE ports
<i>ignore</i>	no action when error condition is entered
<i>shutdown</i>	shutdown PSE power for errored port

The *reset* command option removes and reapplies power to the selected port.

To reset the power to Port 1, use the following commands.

```
(cfg)# port select 1
Nesting level change accepted

(cfg-if) [1]# pse reset
(cfg-if) [1]# exit

(cfg)#
```

To schedule a time for PSE power to be turned ON (7:00AM) and OFF (7:00PM) on Port P1, use the following commands.

```
(cfg)# pse idx 1
Nesting level change accepted

(cfg-pse) [1]# port 1
(cfg-pse) [1]# sched 7:00:00 19:00:00
(cfg-pse) [1]# exit

(cfg)#
```

To enable heartbeat on Port 1, use the following command.

```
(cfg)# port select 1
Nesting level change accepted

(cfg-if) [1]# pse heartbeat
(cfg-if) [1]# pse pdip 192.168.1.230
(cfg-if) [1]# exit

(cfg)#
```

To view the changes or display the PSE configuration settings, use the *show pse* command from the # prompt.

PSE Command Syntax	
(cfg)# pse dall	(cfg-if)#<pNum> pse mode off
(cfg)# pse sched	(cfg-if)#<pNum> pse reset
(cfg)# no pse sched	(cfg-if)#<pNum> pse heartbeat
(cfg)# no pse idx [idx:1-100]	(cfg-if)#<pNum> no pse heartbeat
(cfg)# pse idx [idx:1-100] (accesses next nesting level)	(cfg-if)#<pNum> pse lldp-med
(cfg-pse)# port [cList:1..8 all]	(cfg-if)#<pNum> no pse lldp-med
(cfg-pse)# sched [onTime:time none]	(cfg-if)#<pNum> pse i [iTime:1-300]
(cfg-pse)# sched [onTime:time none] [offTime:time none]	(cfg-if)#<pNum> pse pderr [eNum:1-100]
(cfg-pse)# sched [onTime:time none] [offTime:time none] [sDays:days]	(cfg-if)#<pNum> pse hdfrr [iTime:10-300]
(cfg-pse)# pn [pName:string0..32]	(cfg-if)#<pNum> pse pdint [initNum:0-16384]
(cfg-pse)# schedule	(cfg-if)#<pNum> pse pdip [iAddr:ipAddr]
(cfg-pse)# no schedule	(cfg-if)#<pNum> pse pdmo restart
(cfg-pse)# exit	(cfg-if)#<pNum> pse pdmo ignore
(cfg) port select <pNum> (accesses next nesting level)	(cfg-if)#<pNum> pse pdmo shutdown
(cfg-if)#<pNum> pse mode auto	(cfg-if)#<pNum> exit

Syntax	Name Description	Format Values
[idx:1-100]	PoE scheduler index	1-100
[cList:1..4 all]	port list	1..4, or all
[onTime:time none]	time of day power enabled	24hr:min:sec or none
[offTime:time none]	time of day power disabled	24hr:min:sec or none
[sDays:days]	days scheduled	Sun,Mon,Tue,Wed,Thu,Fri,Sat
[pName:string0..32]	PoE scheduler profile name	0-32 characters
[iTime:1-300]	heartbeat interval	1-300 sec
[eNum:1-100]	# consecutive lost heartbeats for error	1-100
[iTime:10-300]	heartbeat restart defer	10-300 sec
[initNum:0-16384]	times to restart PD after error	0-16384
[iAddr:ipAddr]	ip address of PD for heartbeat	ip address

3.1.21 SPANTREE Command

Multiple Spanning Tree Protocol (MSTP) is a protocol that creates multiple spanning trees (instances) each of which can be mapped to one or more VLANs. This allows groups of VLANs to be configured with the same root bridge and forwarding topology.

The *spantree* command provides the ability to configure Multiple Spanning Tree Protocol (MSTP). Use the *show spantree* command from the # prompt to determine the state of the command option (disabled or enabled).

```
(cfg)# spantree ?
Possible next parameters:
  bage          bridge aging timeout
  bpri          bridge priority
  dall          delete spantree settings, instances, restore defaults
  fwd           forward delay time
  hello         time between hello messages
  mstp          MSTP instance selection name
  stp           spanning tree

(cfg)# spantree

(cfg)# spantree mstp protect
Nesting level change accepted

(cfg-mstp)[protect]#
Possible next parameters:
  exit          exit MSTP instance
  port          port list
  vid           VLAN list

(cfg-mstp){protect}#

(cfg)# port select 1

(cfg-if)[1]# spantree
Possible next parameters:
  bpduguard     port is disabled when BPDU received
  pcost         port path cost
  portfast      forwarding immediately & bypass listening
  ppri          port priority
  proto         protocol configuration
  rootguard     port is disabled if designated as root

(cfg-if)[1]# spantree
```

The command options available using the *spantree* command are shown below.

The *bage* command option sets the time period before the MAC addresses are removed from the table.

The *bpri* command option sets the bridge priority ID for the port. The root bridge is the port with the lowest bridge priority ID.

The *dall* command option deletes all configured Spanning Tree settings and restores factory defaults.

The *fwd* command option sets the time before a port transitions to a forwarding state.

The *hello* command option sets the time period between hello-time Bridge Protocol Data Units (BPDUs).

The *mstp* command option configures the name of the MSTP instance.

The *stp* command option disables/enables spanning tree protocol. The *no* command negates the command.

Command options under the *mstp <pname>* command.

The *exit* command option exits the current nesting level.

The *port* command option configures the ports associated with the spanning tree instance

The *vid* command option configures the VLANs associated with the spanning tree instance.

Command options under the *port select <pNum>* command.

The *bpduguard* command option disables/enables the selected port from receiving BPDUs. The *no* command negates the command.

The *pcost* command option sets the cost of the path. The path cost is based on the speed of the physical interface speed.

The *portfast* command option disables/enables forwarding of BPDUs immediately and bypasses listening. The *no* command negates the command.

The *ppri* command option sets the priority of the port. The state of the port is determined by the port cost and port priority values.

The *proto* command option configures the protocols.

discard RSTP/MSTP are disabled, BPDU frames are discarded

mstp MSTP is enabled and protocol is operational

rstp RSTP is enabled and protocol is operating

tunnel RSTP/MSTP are disabled, BPDU frames are tunneled

The *rootguard* command option disables/enables the selected port if designated as root. The *no* command negates the command.

To configure Port 1 for RSTP with port priority and path cost, use the following commands.

```
(cfg)# port select 1
Nesting level change accepted

(cfg-if) [1]# spantree proto rstp
(cfg-if) [1]# spantree ppri 96
(cfg-if) [1]# spantree pcost 10000
(cfg-if) [1]# exit

(cfg)#
```

To configure Port 2 for MSTP, use the following commands.

```
(cfg)# port select 2
Nesting level change accepted

(cfg-if) [2]# spantree proto mstp
(cfg-if) [2]# exit

(cfg)# spantree mstp network
Nesting level change accepted

(cfg-mstp) [network]# vid 1
(cfg-mstp) [network]# port 2
(cfg-mstp) [network]# exit

(cfg)#
```

To view the changes or display the SPANTREE configuration settings, use the *show spantree* command from the # prompt.

Bridge Priority (*bpri*):

The bridge with the lowest priority is elected as the root bridge for the domain. The Bridge Priority can be modified in increments of 4096 from 0 to 61,440. The default Bridge Priority is 32,768.

Bridge Age Time:

The amount of time a module saves configuration BPDUs. A value from 6 - 40 seconds is valid. The default Max Age Time is 20 seconds.

Hello Time (*hello*):

The Root sends configuration BPDUs every 2 seconds. A value from 1 - 5 seconds is valid. The default Hello Time is 2 seconds.

Forward Delay (*fwd*):

The time interval for listening and learning states. A value from 4 - 30 seconds is valid. The default Forward Delay is 15 seconds.

MAC Address Aging (*bage*):

The time before the MAC address is removed from the MAC table. A value from 10 - 630 seconds is valid. The default MAC Aging Time is 300 seconds.

Port Priority (*ppri*):

If two paths have the same port cost, the bridges must select a preferred path. Port Priority is used to determine the preferred path. A value from 0 - 240 (in increments of 16), with 240 being the highest priority, is allowed. The default Port Priority is 128.

Path Cost (*pcost*):

The cost of a port is typically based on port speed. The faster the port, the lower the port cost. See table below. A value from 1 - 200,000,000 is valid. The default Path Cost is 20,000.

BPDU Guard (*bpduguard*)

BPDU Guard is used to protect the Spanning Tree Topology from BPDU related attacks. BPDU Guard must be enabled on a port that should never receive a BPDU from the connected device.

Port Fast (*portfast*)

Port Fast allows ports to enter a forwarding state in four seconds. Port Fast allows faster convergence on ports that are attached to end stations and do not present the potential to cause forwarding loops.

Root Guard (*rootguard*)

Root Guard ensures that the port on which root guard is enabled is the designated port.

Spanning Tree Protocol uses path cost and port priority to determine the best path. The table below shows the recommended path cost based on link speed.

Link Speed	Recommended Value
10Mbps	2,000,000
100Mbps	200,000
1Gbps	20,000
10Gbps	2,000
100Gbps	200

Recommended Port Cost vs Link Speed

The port with the lowest path cost has the highest priority.

By default, Spanning Tree Protocol is tunneled. Use the *proto* command to change the way the module handles the protocols.

SPANTREE Command Syntax	
(cfg)# spantree stp	(cfg-if)#<pNum> spantree ppri [pPri:0-240]
(cfg)# no spantree stp	(cfg-if)#<pNum> spantree pcost [pCost:1-200000000]
(cfg)# spantree dall	(cfg-if)#<pNum> spantree proto discard
(cfg)# spantree bage [timeout:6-40]	(cfg-if)#<pNum> spantree proto mstp
(cfg)# spantree hello [htime:1-5]	(cfg-if)#<pNum> spantree proto rstp
(cfg)# spantree fwd [ftime:4-30]	(cfg-if)#<pNum> spantree proto tunnel
(cfg)# spantree bpri [bPri:0-61440]	(cfg-if)#<pNum> spantree bpduguard
(cfg)# no spantree mstp [pname:string1..32]	(cfg-if)#<pNum> no spantree bpduguard
(cfg)# spantree mstp [pname:string1..32] (accesses next nesting level)	(cfg-if)#<pNum> spantree portfast
(cfg-mstp)# vid [vList:vlanlist]	(cfg-if)#<pNum> no spantree portfast
(cfg-mstp)# port [pList:f1,f2,1..4 all]	(cfg-if)#<pNum> spantree rootguard
(cfg-mstp)# exit	(cfg-if)#<pNum> no spantree rootguard
(cfg) port select <pNum> (accesses next nesting level)	(cfg-if)#<pNum> exit

Syntax	Name Description	Format Values
[timeout:6-40]	bridge aging timeout	6-40 sec
[htime:1-5]	time between hello messages	1-5 sec
[ftime:4-30]	forward delay time	4-30 sec
[bPri:0-61440]	bridge priority	0-61440, multiples of 4096
[pname:string1..32]	MSTP instance name	1-32 characters
[vList:vlanlist]	VLAN list	1-4095
[pList:f1,f2,1..4 all]	port list	f1,f2,1..4 or all
[pPri:0-240]	port priority	0-240
[pCost:1-200000000]	port path cost	1-200000000

3.1.22 SMTP Command

The *smtp* command provides the ability to configure the Simple Mail Transfer Protocol (SMTP) parameters on the module. The SMTP is a communication protocol for electronic mail transmission.

When using Simple Mail Transfer Protocol (SMTP) to send mail, it optionally uses a combination of StartTLS and Transport Layer Security (TLS) or Secure Sockets Layer (SSL) to encrypt the mail. StartTLS is a protocol command used to inform the email server that the email client wants to upgrade from an insecure connection to a secure one using TLS or SSL.

Use the *show smtp* command from the # prompt to determine the state of the command option (disabled or enabled).

```
(cfg)# smtp ?
Possible next parameters:
  <cr>
  dall          delete SMTP settings, restore defaults
  from          email from-address
  host          mail server IP address or domain
  idx           SMTP email instance index
  name          user name
  port          SMTP destination port
  pw            user password
  starttls     STARTTLS function
  test         SMTP test message
  tls          TLS (Transport Layer Security)

(cfg)# smtp

(cfg)# smtp idx 1
Nesting level change accepted

(cfg-smtp) [1]#
Possible next parameters:
  exit          exit from SMTP recipient instance
  level         minimum level for SMTP entries
  recipient     email recipient

(cfg-smtp) [1]#
```

The command options available using the *smtp* command are shown below.

The *smtp* command option disables/enables SMTP event forwarding. The *no* command negates the command.

The *dall* command option deletes all configured SMTP settings and restores factory defaults.

The *from* command option configures the email address of the person the email is from.

The *host* command option configures the IP address of the SMTP mail server or domain.

The *idx* command option configures the instance index number.

The *name* command option configures the user name to be used to log into the email server.

The *port* command option configures the SMTP port number. The default port number is 25.

The *pw* command option configures the password for the selected email account.

The *starttls* command option disables/enables the STARTTLS function. The *no* command negates the command.

The *test* command option sends a test email to the email server at the specified severity level.

<i>alert</i>	alert SMTP level selection (level 1)
<i>critical</i>	critical SMTP level selection (level 62)
<i>debug</i>	debug SMTP level selection (level 7, lowest priority)
<i>emergency</i>	emergency SMTP level selection (level 0, highest priority)
<i>error</i>	error SMTP level selection (level 3)
<i>info</i>	info SMTP level selection (level 6)
<i>notice</i>	notice SMTP level selection (level 5)
<i>warning</i>	warning SMTP level selection (level 4)

The *tls* command option disables/enables Transport Layer Security (TLS). The *no* command negates the command.

Command options under the *idx <Idx>* command.

The *exit* command option exits the current nesting level.

The *level* command option configures the syslog minimum severity error for forwarding events.

<i>alert</i>	alert SMTP level selection (level 1)
<i>critical</i>	critical SMTP level selection (level 2)
<i>debug</i>	debug SMTP level selection (level 7, lowest priority)
<i>emergency</i>	emergency SMTP level selection (level 0, highest priority)
<i>error</i>	error SMTP level selection (level 3)
<i>info</i>	info SMTP level selection (level 6)
<i>notice</i>	notice SMTP level selection (level 5)
<i>warning</i>	warning SMTP level selection (level 4)

The *recipient* command option configures the email address from the selected recipient.

To configure SMTP forwarding, use the following commands.

```
(cfg)# smtp host 192.168.1.1
(cfg)# smtp name abc@xyz.com
(cfg)# pw 123456
(cfg)# smtp from bill@gmail.com

(cfg)# smtp

(cfg)#
```

To view the changes or display the SMTP configuration settings, use the *show smtp* command from the # prompt.

SMTP Command Syntax	
(cfg)# smtp	(cfg)# smtp test error [msg:string1..160]
(cfg)# no smtp	(cfg)# smtp test info [msg:string1..160]
(cfg)# smtp dall	(cfg)# smtp test notice [msg:string1..160]
(cfg)# smtp host [hName:string0..253]	(cfg)# smtp test warning [msg:string1..160]
(cfg)# smtp name [uName:string0..254]	(cfg)# no smtp idx [sldx:1-25]
(cfg)# smtp pw [uPw:string0..32]	(cfg)# smtp idx [sldx:1-25] (accesses next nesting level)
(cfg)# smtp from [fAddr:string0..254]	(cfg-smtp)# recipient [eAddr:string1..254]
(cfg)# smtp port [pNum:1-65535]	(cfg-smtp)# level alert
(cfg)# smtp starttls	(cfg-smtp)# level critical
(cfg)# no smtp starttls	(cfg-smtp)# level debug
(cfg)# smtp tls	(cfg-smtp)# level emergency
(cfg)# no smtp tls	(cfg-smtp)# level error
(cfg)# smtp test alert [msg:string1..160]	(cfg-smtp)# level info
(cfg)# smtp test critical [msg:string1..160]	(cfg-smtp)# level notice
(cfg)# smtp test debug [msg:string1..160]	(cfg-smtp)# level warning
(cfg)# smtp test emergency [msg:string1..160]	(cfg-smtp)# exit

Syntax	Name Description	Format Values
[hName:string0..253]	mail server IP address or domain	0-253 characters
[uName:string0..254]	user name	0-254 characters
[uPw:string0..32]	user password	0-32 characters
[fAddr:string0..254]	email from-address	0-254 characters
[pNum:1-65535]	SMTP destination port	1-65535
[sldx:1-25]	SMTP email instance index	1-25
[msg:string1..160]	SMTP message	1-160 characters
[eAddr:string1..254]	email recipient	1-254 characters

3.1.23 SNMP Command

The *snmp* command provides the ability to configure the SNMP parameters on the module. Use the *show snmp* command from the # prompt to determine the state of the command option (disabled or enabled).

```
(cfg)# snmp ?
Possible next parameters:
  dall          delete SNMP settings, restore defaults
  rd            read community name
  snmpv1       SNMPv1/v2c protocol
  snmpv3       SNMPv3 protocol
  user         user number
  wr           write community name

(cfg)# snmp

(cfg)# snmp user 1
Nesting level change accepted

(cfg-snmp) [1]#
Possible next parameters:
  atype        authentication type
  auth         authentication password
  exit        exit from user instance
  name        user name
  priv        privacy password
  ptype       privacy type
  sec         user security level
  typ         user type

(cfg-snmp) [1]#
```

The command options available using the *snmp* command are shown below.

The *dall* command option deletes all configured SNMP settings and restores factory defaults.

The *rd* command option configures the SNMPv1/2c Read Community Name . The SNMP Read Community Name is necessary for reading (get) data from the module. The name can be any 1-32 alphanumeric character string. The default setting is public.

The *snmpv1* command option disables/enables SNMPv1. The *no* command negates the command.

The *snmpv3* command option disables/enables SNMPv3. The *no* command negates the command.

The *user* command option configures the user number.

The *wr* command option configures the SNMPv1/2c Write Community Name . The SNMP Write Community Name is necessary for writing (set) data to the module. The name can be any 1-32 alphanumeric character string. The default setting is private.

Command options under the *user <uNum>* command.

The *atype* command option configures the authentication hashing method; MD5 or SHA.

The *auth* command option configures the SNMPv3 authentication password for the selected user number. Authentication password can be any 8-32 alphanumeric character string. The default setting is publicguest.

The *exit* command option exits the current nesting level.

The *name* command option configures the user name for the selected user number.

The *priv* command option configures the privacy password for the selected user number.

The *ptype* command option configures the privacy password encryption algorithm; AES or DES.

The *sec* command option configures the security level for the selected user

<i>noAuthNoPriv</i>	no authentication or privacy security
<i>authNoPriv</i>	authentication with no privacy security
<i>authPriv</i>	authentication and privacy security

The *typ* command option configures the SNMP user type for a user account; admin, read-write, read-only or deny.

<i>admin</i>	admin user type, read, write, user allowed
<i>deny</i>	deny user type (no access via SNMP)
<i>readonly</i>	readonly type, no writes allowed
<i>readwrite</i>	readwrite type read and write allowed

To change the write community name, use the following command.

```
(cfg)# snmp wr public
```

To change the authentication hashing for user 1, use the following command.

```
(cfg)# snmp user 1
Nesting level change accepted

(cfg-snmp)[1]# atype sha
(cfg-snmp)[1]# exit

(cfg)#
```

To view the changes or display the SNMP configuration settings, use the *show snmp* command from the # prompt.

SNMP Command Syntax	
(cfg)# snmp dall	(cfg-snmp)# name [uName:string1..32]
(cfg)# snmp rd [pw:string1..32]	(cfg-snmp)# auth [aPw:string8..32]
(cfg)# snmp wr [pw:string1..32]	(cfg-snmp)# priv [pPw:string8..32]
(cfg)# snmp snmpv1	(cfg-snmp)# sec noAuthNoPriv
(cfg)# no snmp snmpv1	(cfg-snmp)# sec authNoPriv
(cfg)# snmp snmpv3	(cfg-snmp)# sec authPriv
(cfg)# no snmp snmpv3	(cfg-snmp)# atype md5
(cfg)# snmp user [uNum:1-4] (accesses next nesting level)	(cfg-snmp)# atype sha
(cfg-snmp)# typ admin	(cfg-snmp)# ptype aes
(cfg-snmp)# typ deny	(cfg-snmp)# ptype des
(cfg-snmp)# typ readonly	(cfg-snmp)# exit
(cfg-snmp)# typ readwrite	

Syntax	Name Description	Format Values
[pw:string1..32]	read or write community name	1-32 characters
[uNum:1-4]	user number	1-4
[uName:string1..32]	user name	1-32 characters
[aPw:string8..32]	authentication password	8-32 characters
[pPw:string8..32]	privacy password	8-32 characters

3.1.24 SNTP Command

The *sntp* command provides the ability to configure the module to request the time and day from a SNTP server. Use the *show sntp* command from the # prompt to determine the state of the command option (disabled or enabled).

```
(cfg)# sntp ?
Possible next parameters:
  <cr>
  dall          delete SNTP settings, restore defaults
  interval      time server request interval
  ip1           time server IP address 1
  ip2           time server IP address 2
  ntp           network time protocol (NTP)
  zone         time zone selection

(cfg)# sntp
```

The command options available using the *sntp* command are shown below.

The *sntp* command option disables/enables SNTP. The *no* command negates the command.

The *dall* command option deletes all configured SNTP settings and restores factory defaults.

The *interval* command option configures the time interval between SNTP requests.

The *ip1* command option configures the IP address 1 of the SNTP servers.

The *ip2* command option configures the IP address 2 of the SNTP servers.

The *ntp* command option disables/enables NTP. The *no* command negates the command.

The *zone* command option configures the time zone.

To enable SNTP services and assign the SNTP server IP address, use the *-ena* and *-ip1* commands.

```
(cfg)# sntp ip1 192.168.1.240
(cfg)# sntp

(cfg)#
```

To view the changes or display the SNTP configuration settings, use the *show sntp* command from the # prompt.

SNTP Command Syntax	
(cfg)# sntp	(cfg)# sntp interval [iTime:1-60]
(cfg)# no sntp	(cfg)# sntp zone [zoneVal:timezone]
(cfg)# sntp ntp	(cfg)# sntp ip1 [serverIp:ipAddr]
(cfg)# no sntp ntp	(cfg)# sntp ip2 [serverIp:ipAddr]
(cfg)# sntp dall	

Syntax	Name Description	Format Values
[iTime:1-60]	time server request interval	1-60
[zoneVal:timezone]	time zone selection	abbreviations
[serverIp:ipAddr]	ime server IP address	ipv4 address for server IP1 and IP2

3.1.25 SSH Command

Secure Shell (SSH) protocol provides authentication, encryption, and the integrity of data transmitted over a network. SSH uses public-key cryptography to authenticate the remote devices and allows the remote devices to authenticate the user. The module supports SSH Version 2.

The *ssh* command provides the ability to configure SSH on the module. Use the *show ssh* command from the # prompt to determine the state of the command option (disabled or enabled).

```
(cfg)# ssh ?
Possible next parameters:
  <cr>
  dall      delete SSH settings, restore defaults
  dsa       DSA key authentication
  genk      generate public/private keys
  pwd       plain text password entry authentication
  rsa       RSA key authentication
  sftp      secure file transfer protocol (scp v2)
  tcp       tcp port

(cfg)# ssh
```

The command options available using the *ssh* command are shown below.

The *ssh* command option disables/enables SSH. The *no* command negates the command.

The *dall* command option deletes all configured SSH settings and restores factory defaults.

The *dsa* command option disables/enables DSA key authentication. The *no* command negates the command.

The *genk* command option generates the public/private key pair. It takes time to generate the public and private keys. Please be patient when using this command.

The *pwd* command option disables/enables plain text password entry authentication. The *no* command negates the command.

The *rsa* command option disables/enables RSA key authentication. The *no* command negates the command.

The *sftp* command option disables/enables secure file transfer. The *no* command negates the command.

The *tcp* command option configures the TCP port used for the SSH session.

The SSH function supports password (plain text) and public key authentication methods. Password is plain text entered in the client application. RSA is a public key generated via the Rivest, Shamir and Adleman algorithm and DSA is a public key generated via the Digital Signature Algorithm.

The default username is admin and the default password is public.

The following commands enable SSH and configures the TCP Port to 23.

```
(cfg)# ssh tcp 23
(cfg)# ssh

(cfg)#
```

To view the changes or display the SSH configuration settings, use the *show ssh* command from the # prompt.

SSH Command Syntax	
(cfg)# ssh	(cfg)# ssh rsa
(cfg)# no ssh	(cfg)# no ssh rsa
(cfg)# ssh dall	(cfg)# ssh sftp
(cfg)# ssh dsa	(cfg)# no ssh sftp
(cfg)# no ssh dsa	(cfg)# ssh tcp [tPort:1-65535]
(cfg)# ssh pwd	(cfg)# ssh genk
(cfg)# no ssh pwd	

Syntax	Name Description	Format Values
[tPort:1-65535]	tcp port	1-65535

3.1.26 SWITCH Command

The *switch* command provides the ability to configure and display the DIP-switches on the module. Use the *show switch* command from the # prompt to determine the state of the command option (disabled or enabled).

```
(cfg)# switch ?
Possible next parameters:
  dall      delete DIP switch settings, restore defaults
  hw        hardware DIP switch function
  sw        software DIP switch function

(cfg)# switch
```

The command options available using the *switch* command are shown below.

The *dall* command deletes all configured DIP-switch setting and restores factory defaults.

The *hw* command option disables/enables selects whether the physical DIP switch settings or the soft DIP switch settings are used.

The *sw* command option disables/enables selects whether the physical DIP switch settings or the soft DIP switch settings are used.

To enable DIP-switch 1, use the following command.

```
(cfg)# switch sw 1

(cfg)#
```

To view the changes or display the SWITCH configuration settings, use the *show switch* command from the # prompt.

SWITCH Command Syntax	
(cfg)# switch dall	(cfg)# switch sw [sNum:1..8 all]
(cfg)# switch hw	(cfg)# no switch sw [sNum:1..8 all]
(cfg)# no switch hw	

Syntax	Name Description	Format Values
[sNum:1..8 all]	software DIP switch number	1-8 or all

3.1.27 SWITCHPORT Command

The *switchport* command provides the ability to configure VLAN interfaces on the module.

```
(cfg)# switchport ?
Possible next parameters:
  dall          delete switchport settings, restore defaults

(cfg)# switchport

(cfg)# port select 1
Nesting level change accepted

(cfg-if) [1]# switchport ?
Possible next parameters:
  mode          port mode type
  nvlan         native vlan assignment for trunk port
  vid           vlan id assignment for access/tunnel port
  vidtrunk      vlan list for trunk port

(cfg-if) [1]# switchport
```

The command options available using the *switchport* command are shown below.

The *dall* command option deletes all configured switch port settings and restores factory defaults.

Command options under the *port select <pNum>* command.

The *switchport* command option configures VLANs on the selected port. The *no* command negates the command.

The *mode* command option configures the port type for the selected port.

<i>access</i>	access port type
	Ingress: Accepts only untagged traffic
	Egress: Traffic follows the assigned VID
<i>tunnel</i>	tunnel port type
	Ingress: Untagged and tagged traffic is accepted
	Egress: Traffic follows the assigned VID
<i>trunk</i>	trunk port type
	Ingress: The trunk VLAN is removed
	Egress: The trunk VLAN is added

The *nvlan* command option configures the trunk port with native VLAN assignment.

The *vid* command option configures a VLAN ID for an access or tunnel port.

The *vidtrunk* command option configures the VLAN IDs assigned to a trunk port.

By default, traffic is allowed to ingress/egress a trunk port unless it is restricted.

When a native VLAN is configured, all untagged traffic on the trunk port is set to the VLAN ID associated with the native VLAN. Traffic assigned to a native VLAN when transmitted on a trunk port is untagged. Untagged traffic received on a trunk port is assigned to the VLAN associated with the native VLAN.

To configure an access port with a VLAN ID, use the following command.

```
(cfg)# vlan vid 100

(cfg)# port select 1
Nesting level change accepted

(cfg-if) [1]# switchport mode access
(cfg-if) [1]# switchport vid 100
(cfg-if) [1]# exit

(cfg)#
```

VLANs must be added using the *vlan* command before they can be associated with a port.

To configure Fiber Port 1 (F1) as a trunk port allowing only VLAN ID 100, use the following command.

```
(cfg)# port select f1
Nesting level change accepted

(cfg-if) [f1]# switchport mode trunk
(cfg-if) [f1]# switchport vidtrunk 100
(cfg-if) [1]# exit

(cfg)#
```

To view the changes or display the SWITCHPORT configuration settings, use the *show switchport* command from the # prompt.

SWITCHPORT Command Syntax	
(cfg)# switchport dall	(cfg-if)#<pNum> switchport vid [vlanId:1-4095]
(cfg)# port select <pNum> (accesses next nesting level)	(cfg-if)#<pNum> switchport nvlan [vlanId:0-4095]
(cfg-if)#<pNum> switchport mode access	(cfg-if)#<pNum> switchport vidtrunk [vlanList:1-4095 all]
(cfg-if)#<pNum> switchport mode tunnel	(cfg-if)#<pNum> exit
(cfg-if)#<pNum> switchport mode trunk	

Syntax	Name Description	Format Values
[vlanId:1-4095]	vlan id assignment for access/tunnel port	1-4095
[vlanList:vlanlist]	vlan list for trunk port	0-4095, all

3.1.28 SYSLOG Command

Syslog is a standard for message logging per RFC 5424. It is used to manage system logs and alerts.

The *syslog* command provides the ability to configure Syslog on the module. Use the *show syslog* command from the # prompt to determine the state of the command option (disabled or enabled).

```
(cfg)# syslog
Possible next parameters:
  <cr>
  dall      delete syslog settings, restore defaults
  erase     erase all current syslog local entries
  fac       facility code
  ip        syslog server IP address
  level     minimum level for syslog entries
  test      generate test syslog entry

(cfg)# syslog
```

The command options available using the *syslog* command are shown below.

The *syslog* command option disables/enables syslog functionality. The *no* command negates the command.

The *dall* command option deletes all configured syslog setting and restores factory defaults.

The *erase* command option erases all the entries in the current syslog.

The *fac* command configures the facility code. The default value is 23.

The *ip* command option configures the syslog server IP address.

The *level* command option configures the syslog minimum severity error for forwarding events.

<i>alert</i>	alert syslog level selection (level 7)
<i>critical</i>	critical syslog level selection (level 6)
<i>debug</i>	debug syslog level selection (level 1)
<i>emergency</i>	emergency syslog level selection (level 8)
<i>error</i>	error syslog level selection (level 5)
<i>info</i>	info syslog level selection (level 2)
<i>notice</i>	notice syslog level selection (level 3)
<i>warning</i>	warning syslog level selection (level 4)

The *test* command option generates a test syslog entry at the specified severity level.

<i>alert</i>	alert syslog level selection (level 7)
<i>critical</i>	critical syslog level selection (level 6)
<i>debug</i>	debug syslog level selection (level 1)
<i>emergency</i>	emergency syslog level selection (level 8)
<i>error</i>	error syslog level selection (level 5)
<i>info</i>	info syslog level selection (level 2)
<i>notice</i>	notice syslog level selection (level 3)
<i>warning</i>	warning syslog level selection (level 4)

To configure the IP address of the syslog server and enable syslog, use the following command.

```
(cfg) # syslog ip 192.168.1.100
(cfg) # syslog

(cfg) #
```

To generate a generates a test syslog entry, use the following command.

```
(cfg) # syslog test alert "This is a test message"
```

To view the changes or display the SYSLOG configuration settings, use the *show syslog* command from the # prompt.

SYSLOG Command Syntax	
(cfg)# syslog	(cfg)# syslog level notice
(cfg)# no syslog	(cfg)# syslog level warning
(cfg)# syslog dall	(cfg)# syslog fac [fCode:16-23]
(cfg)# syslog ip [serverNumIp:ipAddr]	(cfg)# syslog test alert [message:string1..127]
(cfg)# syslog erase	(cfg)# syslog test critical [message:string1..127]
(cfg)# syslog level alert	(cfg)# syslog test debug [message:string1..127]
(cfg)# syslog level critical	(cfg)# syslog test emergency [message:string1..127]
(cfg)# syslog level debug	(cfg)# syslog test error [message:string1..127]
(cfg)# syslog level emergency	(cfg)# syslog test info [message:string1..127]
(cfg)# syslog level error	(cfg)# syslog test notice [message:string1..127]
(cfg)# syslog level info	(cfg)# syslog test notice [message:string1..127]

Syntax	Name Description	Format Values
[serverNumIp:ipAddr]	syslog server IP address	ipv4 address
[fCode:16-23]	facility code	16-2
[message:string1..127]	generate test syslog entry	1-127 characters

3.1.29 USER Command

The *user* command provides the ability to create and modify user accounts. Up to sixteen user accounts can be configured. Use the *show user* command from the # prompt to determine the state of the command option (disabled or enabled).

```
(cfg)# user ?
Possible next parameters:
  artry          number of authentication retries
  ato            authentication timeout
  dall           deletes all users except the admin user, restores defaults
  fsto           ftp session timeout
  lto            lockout timeout
  rename         new user name
  select         select user name
  strongpassword strong password is only accepted

(cfg)# user

(cfg)# user select Bob
Nesting level change accepted

(cfg-user) [Bob]#
Possible next parameters:
  exit           exit from user instance
  kfn            SSH key file name
  pw             user password
  sto            session timeout
  type           user type

(cfg-user) [Bob]#
```

The command options available using the *user* command are shown below.

The *artry* command option sets the number of authentication attempts that a client is allowed to make before authentication lockout.

The *ato* command option sets the time allowed for the completion of an authentication attempt.

The *dall* command option deletes all user profiles except the currently logged in user and restores to factory defaults.

The *fsto* command option configures the FTP session timeout value in seconds.

The *lto* command option configures the lockout timer for a specific user. The default timeout is 300 seconds.

The *rename* command option configures the name of a new user.

The *select* command option selects a user name to be configured. The *no* command negates the command.

The *strongpassword* command option disables/enables strong password control. Password strength is based on the password length of a minimum of eight (8) characters, at least one (1) upper case letter, at least one (1) number or special symbol. When enabled the password must be considered strong or very strong. If not, the password will be rejected and a message of “Password rejected because it is not strong enough” will be displayed. The *no* command negates the command.

Command options under the *select <uName>* command.

The *exit* command option exits the current nesting level.

The *kfn* command option configures the SSH key filename for a specific user.

The *pw* command option configures the password for a new user. This password is used for Serial, FTP, Telnet and SSH.

The *sto* command option configures the session timeout value for a specific user. The default timeout is 300 seconds.

The *type* command option configures the user access type for the user name selected. Each user name can be configured as:

admin admin user type, read, write, user allowed

deny deny user type (no login)

readonly readonly type, no writes allowed

readwrite readwrite type read and write allowed

Username must contain 1-32 characters and may contain a-z, A-Z, 0-9 and the special characters dash (-), underscore (_) and period (.).

Passwords must contain 1-32 printable characters and may contain a-z, A-Z, 0-9 and the special characters ! # \$ % & ' () * + , / : ; < = > ? @ [\] ^ ` { | } ~ and space and the 'New Password (again)' must match.

When changing the session timeout value using the *sto* command, the new value will not take effect until the user logs out and logs back in.

To create a new user, use the following commands.

```
(cfg)# user select Doug
Nesting level change accepted

(cfg-user)[Doug]# type readonly
(cfg-user)[Doug]# pw engineeringvp
(cfg-user)[Doug]# exit

(cfg)#
```

To view the changes or display the USER configuration settings, use the *show user* command from the # prompt.

USER Command Syntax	
(cfg)# user dall	(cfg-user)# type admin
(cfg)# user lto [ltimeout:1-300]	(cfg-user)# type deny
(cfg)# user ato [atimeout:0-300]	(cfg-user)# type readonly
(cfg)# user artry [count:1-5]	(cfg-user)# type readwrite
(cfg)# user fsto [ftimeout:0-3600]	(cfg-user)# pw [uPw:string1..32]
(cfg)# user strongpassword	(cfg-user)# sto [stimeout:0-3600]
(cfg)# no user strongpassword	(cfg-user)# kfn
(cfg)# user rename [uName:string1..32] [newName:string1..32]	(cfg-user)# kfn [filename:string0..45]
(cfg)# no user select [uName:string1..32]	(cfg-user)# exit
(cfg)# user select [uName:string1..32] (accesses next nesting level)	

Syntax	Name Description	Format Values
[ltimeout:1-300]	lockout timeout	1-300 sec
[atimeout:0-300]	authentication timeout	0-300 sec
[count:1-5]	number of authentication retries	1-5
[ftimeout:0-3600]	ftp session timeout	0-3600 sec
[uName:string1..32]	user name	1-32 characters
[newName:string1..32]	new user name	1-32 characters
[uPw:string1..32]	user password	1-32 characters
[stimeout:0-3600]	session timeout	0-3600 sec
[filename:string0..45]	SSH key file name	0-45 characters

3.1.30 VLAN Command

The *vlan* command adds VLAN IDs on the module. Use the *switchport* command to assign the VLAN IDs to specific port numbers.

```
(cfg)# vlan ?
Possible next parameters:
  dall          delete VLAN settings, instances, restore defaults
  vid           VLAN ID

(cfg)# vlan
```

The command options available using the *vlan* command are shown below.

The *dall* command option deletes all configured VLAN settings and restores factory defaults.

The *vid* command option configures a VLAN ID and VLAN name. The *no* command negates the command.

To configure a VLAN instance, use the following command.

```
(cfg)# vlan vid 100 video
(cfg)# vlan vid 200 voice
(cfg)# vlan vid 300 data

(cfg)#
```

To view the changes or display the VLAN configuration settings, use the *show vlan* command from the # prompt.

VLAN Command Syntax	
(cfg)# vlan dall	(cfg)# vlan vid [vlanId:1-4095] [vlanName:string1..64]
(cfg)# vlan vid [vlanId:1-4095]	(cfg)# no vlan vid [vlanId:1-4095]

Syntax	Name Description	Format Values
[vlanId:1-4095]	VLAN ID	1-4095
[vlanName:string1..64]	VLAN name	1-64 characters

3.2 SHOW COMMAND

The *show* command displays the configuration parameters for the select command.

```
# show ?
Possible next parameters:
aaa          authentication, authorization, accounting configuration
acl         access control list configuration for management access
bwp         bandwidth profile configuration
contact     contact closure status
cos         class of service configuration
dir         directory of existing files
ethertype   ethertype tag identification configuration
fload       firmware load configuration
igmp        internet group management protocol configuration
ip          IP configuration
lag         link aggregation group configuration
lldp        link layer discovery protocol (LLDP) configuration
location    location configuration
lr          link redundancy configuration
mactable    mac table status
mld         multicast listener discovery configuration
modbus      modbus protocol configuration
module      module global configuration
mrp         media redundancy protocol (MRP) configuration
port        port attribute configuration
portaccess  port access configuration
portstat    port statistic configuration
protocol    protocol configuration
pse         power source equipment (PSE) configuration
restore     restore module defaults
runningconf running config CLI commands
save        save configuration changes into permanent memory
serupdate   upload firmware update via the serial port
smtp        smtp configuration
sfp         small form pluggable port information
snmp        snmp configuration
sntp        simple network time protocol (SNTP) configuration
spantree    spanning tree configuration
splash      splash screen user configuration
ssh         secure shell (SSH) configuration
switch     physical DIP switch configuration
switchport  vlan interface configuration
syslog      system log message configuration
time        time of day configuration
traphost    snmp trap host configuration
traps       snmp trap configuration
user        user configuration
ver         version status
vlan        vlan configuration

# show
```

The SFP command is only available on models with SFP transceiver ports.

The contact command is only available on RuggedNet models.

Some *show* command have additional options available. Use the ? after to *show* command to see available options for that command (i.e. *show bwp ?*).

```
# show bwp
Possible next parameters:
  <cr>
  pList          port list selection: f1,f2,1..4|all
# show bwp
```

The following *show* command displays the SFP port information.

```
# show sfp f1

Port F1

Address A0 Page Contents
=====
00: 03 04 07 00 00 00 08 00 00 00 00 01 0D 00 00 00 .....
10: 00 00 64 00 41 50 41 43 2D 4F 45 4D 20 20 20 20 ..d.APAC-OEM
20: 20 20 20 20 20 00 00 90 65 41 53 46 50 54 2D 54 32 ...eASFPT-T2
30: 2D 49 20 20 20 20 20 20 20 31 2E 30 20 00 00 00 B6 -I 1.0 ....
40: 00 00 00 00 47 35 31 36 54 32 31 39 30 30 30 32 ....G516T2190002
50: 20 20 20 20 31 36 30 35 30 31 20 20 00 00 00 82 160501 ....
60: 00 00 11 00 A3 99 4D 2A DA 59 3D 91 50 2F 0A 27 .....M*.Y=.P/.'
70: 28 86 35 00 00 00 00 00 00 00 00 00 08 40 63 1D (.5.....@c.
80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

SFP Type: 1000BASE-T
Bit rate: 1300 Mbps
Link length: 100m
Vendor Name: APAC-OEM
Vendor Part Number: ASFPT-T2-I
Vendor Serial Number: G516T2190002
Date Code: 05/01/2016

Temperature: n/a
Vcc: n/a
Bias current: n/a
Tx power: n/a
Rx power: n/a

#
```

To show the version of firmware on the module, use the *show ver* command.

```
# show ver

Model number      2930-1-40-1
Firmware          v3.x.x Mar 04 2025, 14:31:26
Bootstrap         v3.x.x
                  prodRev 10 hwRev 10 pcbRev 00d20100 appAP 0 caps(0x52200004 mtype 168)
#
```

3.3 FWLOAD COMMAND

The *fwload* command downloads the application firmware or bootloader file from a TFTP server.

```
# fwload ?
Possible next parameters:
  file          firmware file selection
  ip            TFTP Server ip address
  ty           firmware file type selection

# fwload
```

The command options available using the *fwload* command are shown below.

The *file* command option selects the firmware file to load on the module.

The *ip* command option configures the IP address of the TFTP server used for upgrading the module firmware.

The *ty* command option selects the firmware type; *app* or *bootloader*.

The filename of the application firmware when using the *fwload* command must be the same as the filename used during the FTP process.

Once the new firmware has been stored on the module, the firmware can be programmed by using the following command:

```
# fwload ty app
# fwload file <filename.dat>

Starting upgrade using file filename.dat
Upgrade complete, reboot pending...
```

To display the available files, use the *show fwload* command from the # prompt.

FWLOAD Command Syntax	
# fwload ty app	# fwload file [fileName:string1..45]
# fwload ty bootloader	# no fwload file [fileName:string1..45]
# fwload ip [tftpServerIp:ipAddr]	

Syntax	Name Description	Format Values
[tftpServerIp:ipAddr]	TFTP Server ip address	ipv address
[fileName:string0..45]	firmware file name	1-45 characters

3.4 MACTABLE COMMAND

The *mactable* command provides the ability to enable/disable MAC learning, add/delete static MAC addresses, clear and display the MAC addresses learned by the module and configure the MAC aging time. Use the *show mactable* command from the # prompt to determine the state of the command option (disabled or enabled).

```
# mactable ?
Possible next parameters:
  aging          mac table aging time
  clr            clear (flushes) the learned MAC addresses
  dall          delete MAC configured settings, instances, restore defaults
  learning       global MAC learning
  mac            MAC address
  port          clear MAC table when any port link down

# mactable
```

The command options available using the *mactable* command are shown below.

The *aging* command option sets the time before a MAC address expires. The default value is 300 seconds.

The *clr* command option clears the learned MAC addresses on the module.

The *dall* command option deletes all MAC configured settings, instances and restores factory defaults.

The *learning* command option disables/enables MAC learning globally on the module. The *no* command negates the command.

The *mac* command option configures a static MAC address to the MAC table of a port or a port associated with a VLAN ID.

The *port* command option disables/enables the clearing of the MAC table when any port link is down. The *no* command negates the command.

To display the MACTABLE configuration settings and MAC addresses discovered, use the *show mactable* command from the # prompt.

MACTABLE Command Syntax	
# mactable dall	# mactable port
# mactable clr	# no mactable port
# mactable aging [ageTime:10-600]	# no mactable mac [macAddress:macAddress]
# mactable learning	# mactable mac [macAddress:macAddress] ports [pList:f1,f2,1..8 all]
# no mactable learning	# mactable mac [macAddress:macAddress] ports [pList:f1,f2,1..8 all] vid [vlanId:1-4095]

Syntax	Name Description	Format Values
[ageTime:10-600]	mac table aging time	10-600 sec
[macAddress:macAddress]	MAC address	xx-xx-xx-xx-xx-xx, xx = 00-ff hex
[pList:f1,f2,1..8 all]	port list	f1,f2,1..8 or all
[vlanId:1-4095]	trunk VLAN ID	1-4095

3.5 PING COMMAND

The *ping* command provides the ability to ping network devices connected to the module. This provides a convenient way to verify connectivity through the CLI interface.

```
# ping ?
Possible next parameters:
  l          transmit buffer size
  n          number of pings
  t          ping the specified ipAddress
  to         timeout to wait for each ping reply
  ttl       time to live count

# ping
```

The command options available using the *ping* command are shown below.

The *l* command option configures the size of the ping frame.

The *n* command option sets the number of pings frames sent. A value of 0 sends pings until interrupted.

The *t* command option configures the destination IP address.

The *to* command option sets the time to wait for each reply.

The *ttl* command option sets the time to live value.

The default parameters for the *ping* command are:

repeatCnt = 3 (*n*), dataMsgLen = 32 (*l*), timeout = 3 (*to*), ttl = 64 (*ttl*)

Issuing a default *ping* command will provide the following result:

```
# ping t 192.168.1.110

Pinging 192.168.1.110 with 32 bytes of data sourced from IP1 (192.168.1.220):

Reply from 192.168.1.110: bytes=32 time=1ms
Reply from 192.168.1.110: bytes=32 time=1ms
Reply from 192.168.1.110: bytes=32 time=1ms

Ping statistics for 192.168.1.110:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

#
```

This command string changes the default settings to:

repeatCnt = 5 (**n**), dataMsgLen = 72 (**l**), timeout = 10 (**to**), ttl = 128 (**ttl**)

```
# ping l 72
# ping n 5
# ping to 10
# ping ttl 128

# ping t 192.168.1.110
Pinging 192.168.1.110 with 72 bytes of data sourced from IP1 (192.168.1.220):

Reply from 192.168.1.110: bytes=72 time=1ms
Reply from 192.168.1.110: bytes=72 time=1ms
Reply from 192.168.1.110: bytes=72 time=1ms
Reply from 192.168.1.110: bytes=72 time=1ms
Reply from 192.168.1.110: bytes=72 time=1ms

Ping statistics for 192.168.1.110:
    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

#
```

PING Command Syntax	
# ping t [ipAddress:ipAddr]	# ping to [tCount:1-30]
# ping n [count:0-65536]	# ping ttl [count:1-255]
# ping l [size:0-1472]	

Syntax	Name Description	Format Values
[ipAddress:ipAddr]	destination ipAddress	ipv4 address
[count:0-65536]	number of pings	0-65535
[size:0-1472]	transmit buffer size	0-1472 bytes
[tCount:1-30]	timeout to wait for each ping reply	1-30 sec
[count:1-255]	time to live count	1-255

3.6 RESTART COMMAND

The *restart* command provide the ability to restart (warm boot) the module.

```
# restart ?  
Possible next parameters:  
  boot          warm boot the module  
  
# restart
```

The command options available using the *restart* command are shown below.

The *boot* command option performs a warm boot on the module.

back makes the backup application image active

To restart the module, use the *restart boot* command.

```
# restart boot
```

To swap the backup and current images and restart the module, use the *restart boot back* command.

```
# restart boot back
```

RESTART Command Syntax	
# restart boot	# restart boot back

3.7 RESTORE COMMAND

The *restore* command provides the ability to restore the module to factory default settings or a specific file.

```
# restore ?
Possible next parameters:
  file          file name
  ty            restore type

# restore
```

The command options available using the *restore* command are shown below.

The *file* command option creates a new local configuration file. Default name is *local*. To name the file, add the name after the *file* command. The *no* command negates the command.

The *ty* command option configures the type of restore.

- factory* restores factory defaults
- keep* restores all but keeps IP settings IP address, subnet, gateway
- file* restores file name
- keep* restores file name but keeps IP settings IP address, subnet, gateway
- local* restores local defaults
- keep* restores local defaults but keeps IP settings IP address, subnet, gateway
- previous* restores previous defaults
- keep* restores previous defaults but keeps IP settings IP address, subnet, gateway

To create a local configuration file based on the current module configuration, use the following command.

```
# restore file
```

To restore the module to factory default settings, use the following command.

```
# restore ty factory
```

The module is rebooted and the factory default settings are restored.

To display the files on the module, use the *show restore* command from the # prompt.

RESTORE Command Syntax	
# restore file	# restore ty local
# no restore file	# restore ty previous
# restore file [fName:string0..45]	# restore ty factory keep
# no restore file [fName:string0..45]	# restore ty file [fName:string0..45] keep
# restore ty factory	# restore ty local keep
# restore ty file [fName:string0..45]	# restore ty previous keep

Syntax	Name Description	Format Values
[fName:string1..45]	file name	0-45 characters

3.8 SAVE COMMAND

The *save* command saves the configuration into permanent memory on the module

```
# save ?  
Possible next parameters:  
  <cr>  
  
# save
```

A *<cr>* after the command, saves the configuration to memory.

3.9 SERUPDATE COMMAND

The *serupdate* command allows the firmware to be updated from the serial console port using the xmodem protocol.

```
# serupdate ?
Possible next parameters:
    trans          transfer the selected file

# serupdate
```

The command options available using the *serupdate* command are shown below.

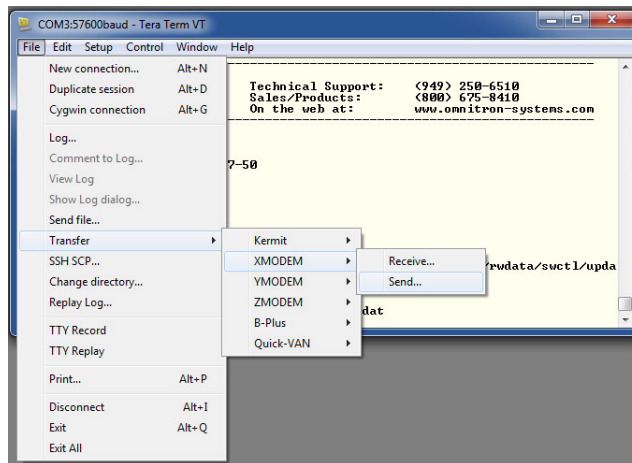
The *trans* command option starts the xmodem process of updating the firmware using the serial console port.

To update the firmware on the module, use the following command.

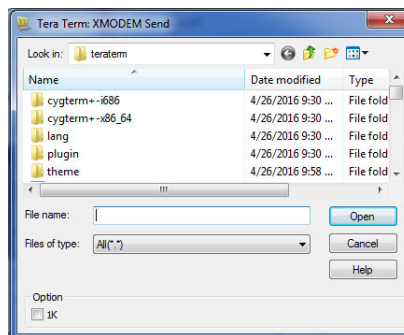
```
# serupdate trans

rc = Firmware download started to destination /usr/bin/rx -bv /rwdataswctl/updates/fw.dat
rx: ready to receive /rwdataswctl/updates/fw.dat
```

The module is ready to receive the firmware using xmodem protocol. Using TeraTerm or Procomm, transfer the firmware to the module.



Select the location of the firmware file.



Updating the firmware using the serial console port can take a very long time. Please be patient when updating the firmware using the serial console port.

To display the SERUPDATE settings, use the *show serupdate* command from the # prompt.

3.10 SPLASH COMMAND

The *splash* command provides the ability to configure a message that is displayed after the module has been restarted or rebooted. The message is displayed after the Entry screen is displayed.

```
# splash ?  
Possible next parameters:  
    warn          warning message  
  
# splash
```

The command options available using the *splash* command are shown below.

The *warn* command option configures the message. Enter the message after the command.

To configure a message, use the *splash warn* command.

```
# splash warn "This product is for the use of authorized users only. Individuals using this  
product without authority are subject to monitoring of their activities."
```

```
Omnitron Systems Technology, Inc.  
Copyright 2017-2021 OST, Inc.
```

```
GHPoE/Mi
```

```
-----  
Omnitron Systems Technology   Technical Support:   (949) 250-6510  
38 Tesla                     Sales/Products:    (800) 675-8410  
Irvine, CA 92618             On the web at:    www.omnitron-systems.com  
-----
```

```
IP address    192.168.1.220  
MAC          00-06-87-02-87-50  
Serial number 00720087
```

```
This product is for the use of authorized user only.  Individuals using this product without  
authority are subject to monitoring of their activities.
```

```
GHPoE/Mi login:
```

To have the same message on multiple lines, the `\n` character can be used to terminate a message line.

```
# splash warn "This product is for the use of authorized users only.\nIndividuals using this  
product without authority are subject to monitoring of their activities."
```

```

Omnitron Systems Technology, Inc.                                GHPoE/Mi
Copyright 2017-2021 OST, Inc.

-----

Omnitron Systems Technology   Technical Support:           (949) 250-6510
38 Tesla                     Sales/Products:             (800) 675-8410
Irvine, CA 92618             On the web at:           www.omnitron-systems.com

-----

IP address    10.10.8.211
MAC           00-06-87-04-93-10
Serial number 00738745

This product is for the use of authorized uses only.
Individuals using this product without authority are subject to monitoring of their activities

GLPoE/M login:

```

To display the SPLASH message, use the *show splash* command from the # prompt.

SPLASH Command Syntax	
# splash warn	# splash warn [wMsg:string0..255]

Syntax	Name Description	Format Values
[wMsg:string0..255]	warning message	0-255 characters

3.11 TIME COMMAND

The *time* command provides the ability to set or display the time of day on the module.

```
# time ?  
Possible next parameters:  
  set          set the time of day and date  
  zone         time zone selection  
  
# time
```

The command options available using the *time* command are shown below.

The *set* command option sets the date and time of day.

The *zone* command option configures the time zone.

To sets the time of day, use the following command.

```
# time set 01/01/2022 07:55:00
```

To view the changes or display the TIME and system uptime, use the *show time* command from the # prompt.

TIME Command Syntax	
# time zone [zoneVal:timezone]	# time set [dateVal:tDate] [timeVal:time]

Syntax	Name Description	Format Values
[zoneVal:timezone]	time zone	abbreviation
[dateVal:tDate]	date	mm/dd/yyyy
[timeVal:time]	time	hh:mm:ss, hh=0-23, mm=0-59, ss=0-59

3.12 TRAPHOST COMMAND

SNMP traps report events that occur during the operation of a network, and may require the attention of the network administrator. The module is capable of sending SNMP traps to eight different SNMP Trap Hosts (IP addresses).

The *traphost* command provides the ability to configure the IP addresses of the SNMP Trap Hosts.

```
# traphost ?
Possible next parameters:
  dall          delete SNMP trap hosts settings, restore defaults
  host          traphost number

# traphost

# traphost host 1
Nesting level change accepted

(cfg host) [1]#
(cfg host) [1]#
Possible next parameters:
  exit          exit from trap host instance
  ip            trap host IP address
  port         trap UDP port number
(cfg host) [1]#
```

The options available using the *traphost* command are shown below.

The *dall* command option deletes all configured trap hosts and restores to factory default. The default setting is 255.255.255.255.

The *host* command option selects the Trap Host number to be configured. Eight different Traps Hosts can be configured.

Command option under *host <hNum>* command.

The *exit* command option exits the current nesting level.

The *ip* command option configures the IP address for the selected Trap Host.

The *port* command option configures the UDP trap port number.

To configure the IP address for Trap Host 1, use the following command.

```
# traphost host 1
Nesting level change accepted

(cfg-host) [1]# ip 192.168.1.100
(cfg-host) [1]# exit

#
```

To view the changes or display the TRAPHOST configuration settings, use the *show traphost* command from the # prompt.

TRAPHOST Command Syntax	
# traphost dall	(cfg-host)# port [pNum:1-65535]
# traphost host [hNum:1-8] (accesses next nesting level)	(cfg-host)# exit
(cfg-host)# ip [ipAddr:ipAddr]	

Syntax	Name Description	Format Values
[hNum:1-8]	traphost number	1-8
[ipAddr:ipAddr]	trap host IP address	ip address
[pNum:1-65535]	trap UDP port numbe	1-65535

3.13 TRAPS COMMAND

The *traps* command provides the ability to enable/disable specific module traps. By default, all traps are enabled. Use the *show traps* command from the # prompt to determine the state of the command option (disabled or enabled).

```
# traps ?
Possible next parameters:
  clear          clear trap log
  dall           delete traps settings, restore defaults
  gen            generate trap
  num            trap number
  type           trap generation type
  user           trap generation SNMP user

# traps
```

The command options available using the *traps* command are shown below.

The *clear* command option clears the current trap log entries.

The *dall* command option deletes all configured trap options and restores to default settings.

The *gen* command option generates a specific trap number.

The *num* command option disables/enables a selected or all traps. The *no* command negates the command.

The *type* command option configures the generation type of the trap; SNMPv2c or SNMPv3.

The *user* command option configures the SNMP user number for the trap generation.

By default, all traps are enabled. Individual traps can be disabled by entering the number of the traps after the *num* command.

The example below disables the link down (#6) trap.

```
# no traps num 6
```

To view the changes or display the TRAPS, use the *show traps* command from the # prompt. To view the Trap Log, use the *show traps log* command from the # prompt.

TRAPS Command Syntax	
# traps dall	# traps type snmpv3
# traps num [tNum:1..63 all]	# traps user [uNum:1-4]
# no traps num [tNum:1..63 all]	# traps gen [gNum:1-63]
# traps type snmpv2c	# traps clear

Syntax	Name Description	Format Values
[tNum:1..63 all]	trap number	1-63 or all
[uNum:1-4]	trap generation SNMP user	1-4
[gNum:1-63]	generate trap	1-63

4.0 APPENDIX A: FIRMWARE UPDATE

4.1 OVERVIEW

Appendix A describes the procedure for updating the firmware using ftp and web interface.

4.2 SAVE CURRENT SETTINGS

Under normal circumstances the current configuration of the module will carry forward to the new version during the update, however, extreme events such as a power outage can lead to settings being lost. Prior to upgrading, it is recommended that the settings be recorded. The settings can be viewed using the Command Line Interface (CLI) over Telnet.

4.3 COPY THE FILES TO YOUR HARD DRIVE

The files should be copied to a convenient location on the hard drive of the workstation. The name of the firmware file is similar to swctl-bsp-prod.dat.

Depending on the operating system of the workstation and/or FTP installation, the name of the files may need to be renamed to the "DOS 8.3 Format". Rename the swctl-bsp-prod.dat to switch.dat and store the files in the root or c:\ directory.

Renaming the file will allow the new file to overwrite the old file, saving memory allocation space on the module. **Filenames must not contain any spaces.**

4.4 UPDATING THE FIRMWARE USING FTP

FTP can be used to update the firmware over a network. Verify the following parameters:

- IP Protocol is turned On and the module has a valid IP Address
- FTP Protocol turned On and a password has been configured

Access the module using Telnet or Serial Console. The default user name and password is: admin, public

Verify the IP address of the module by using the *show ip* command from the # prompt. If the IP address needs to be configured, use the *ip* command from the <cfg># prompt.

```
# show ip

IPv4                enabled
IPv6                enabled

IP 1
  MAC address       00-06-87-02-A5-80
  IPv4 address      192.168.1.126
  IPv4 subnet mask  255.255.255.0
  IPv4 gateway address 192.168.1.1
  DNS               disabled
  DNS address       *
  DHCP              disabled
  Relay             disabled
  Relay Circuit ID  enabled
  Relay Remote ID   enabled
  Relay type        replace
  Relay server IP   0.0.0.0
  v6Relay           disabled
  v6Relay Circuit ID enabled
  v6Relay Remote ID enabled
  IPv6 interface    stateless
  IPv6 address      fe80::206:87ff:fe02:a580/64
                   ::/64
  IPv6 gateway address fe80::1
  DHCPv6            disabled

#
```

Verify FTP is enabled by using the show protocol command from the # prompt.

To enable FTP, use the *protocol ftp* command from the <cfg># prompt.

```
# show protocol

IP protocol          enabled
Telnet protocol     enabled
FTP protocol       disabled
http protocol       enabled
https protocol      enabled
Serial console      enabled
Flow control        disabled

Certificate file     self-generated

#
# config
Nesting level change accepted

(cfg)# protocol ftp

(cfg)# exit
Nesting level change accepted

# show protocol

IP protocol          enabled
Telnet protocol     enabled
FTP protocol       enabled
http protocol       enabled
https protocol      enabled
Serial console      enabled
Flow control        disabled

Certificate file     self-generated

#
```

The default FTP password is public.

To upgrade the application firmware, open a command window and enter the following commands. Bold lettering indicates information to be entered.

```
> ftp 192.168.1.220 <enter module's IP address>
Connected to 192.168.1.220
220 FTP server ready
User (192.168.1.220:(none)): admin <enter login username>
331 User admin OK. Password required
Password: public <enter ftp password>
230 OK. Current directory is /home/admin
ftp> cd updates
250 OK. Current directory is /rwdataswctl/updates
ftp> bin
250 OK. Current directory is /rwdataswctl/updates
ftp> put <location and filename of the application firmware> <enter firmware filename>
200 OK
200 PORT command successful
150 Connecting to port 64533
226-File successfully transferred
226 5.030 seconds (measured here), 6.28 Mbytes per second
ftp: 33112213 bytes sent in 4.97Seconds 6658.40Kbytes/sec.
ftp>quit
```

When the file transfer is complete, the module verifies the file, programs the flash memory and automatically restarts with the newly loaded firmware.

NOTE: Do not remove power during the upgrade procedure until the module has rebooted with the new firmware.

Verify the firmware has been upgraded by using the *show ver* command.

```
# show ver

Model number      9526-0-24-1
Firmware          v2.x Sep 16 2022, 21:05:11
Bootstrap         v2.x.x
                  prodRev 10 hwRev 10 pcbRev 00a90100 appAP 0 caps(0xa0000004 mtype 168)

#
```

5.0 COPYRIGHT STATEMENT

General and Copyright Notice

This publication is protected by U.S. and international copyright laws. All rights reserved. The whole or any part of this publication may not be reproduced, stored in a retrieval system, translated, transcribed, or transmitted, in any form, or by any means, manual, electric, electronic, electromagnetic, mechanical, chemical, optical or otherwise, without prior explicit written permission of Omnitron Systems Technology, Inc.

The following trademarks are owned by Omnitron Systems Technology, Inc.: FlexPoint®, FlexSwitch™, iConverter®, miConverter®, NetOutlook®, OmniLight®, OmniConverter®, RuggedNet®, Omnitron Systems Technology, Inc.™, OST™ and the Omnitron logo.

All other company or product names may be trademarks of their respective owners.

The information contained in this publication is subject to change without notice. Omnitron Systems Technology, Inc. is not responsible for any inadvertent errors.

©2025 Omnitron Systems Technology, Inc.

6.0 CUSTOMER SUPPORT INFORMATION

If you encounter problems while installing this product, contact Omnitron Technical Support:

Phone: (949) 250-6510

Fax: (949) 250-6514

Address: Omnitron Systems Technology, Inc.

38 Tesla

Irvine, CA 92618, USA

Email: support@omnitron-systems.com

URL: www.omnitron-systems.com