

**Command Line Interface**  
**for**  
***All OmniConverter<sup>®</sup> and RuggedNet<sup>®</sup>***  
**Managed Switch Products**

**USER MANUAL**

---

# Table of Contents

<b>1.0</b>	<b>Overview</b>	<b>4</b>
1.1	New Features	4
<b>2.0</b>	<b>Command Line Interface (CLI)</b>	<b>5</b>
2.1	CLI Commands	7
2.1.1	Authentication, Authorization and Accounting (AAA)	8
2.1.2	Access Control List (ACL)	13
2.1.3	Bandwidth Profile (BWP)	15
2.1.4	Cable Test (CABLETEST)	19
2.1.5	Contact (CONTACT)	20
2.1.6	Class of Service (COS)	22
2.1.7	File Directory (DIR)	25
2.1.8	Ethertype (ETHERTYPE)	26
2.1.9	Load Firmware (FWLOAD)	27
2.1.10	Internet Group Management Protocol (IGMP)	28
2.1.11	IP (IP)	31
2.1.12	Link Aggregation Groups (LAG)	34
2.1.13	Link Layer Discovery Protocol (LLDP)	38
2.1.14	Physical Location (LOCATION)	42
2.1.15	Link Redundancy (LR)	43
2.1.16	MAC Table (MACTABLE)	45
2.1.17	Multicast Listener Discovery (MLD)	47
2.1.18	Module Settings (MODULE)	49
2.1.19	Media Redundancy Protocol (MRP)	52
2.1.20	Nest (NEST)	57
2.1.21	Ping (PING)	57
2.1.22	Port Attribute (PORT)	59
2.1.23	Port Access (PORTACCESS)	62
2.1.24	Port Statistics (PORTSTAT)	63
2.1.25	Protocol (PROTOCOL)	65
2.1.26	Power Sourcing Equipment (PSE)	66
2.1.27	Restart (RESTART)	71
2.1.28	Restore to Factory Defaults (RESTORE)	72
2.1.29	Save (SAVE)	73
2.1.30	Create and Run a Script File (SCRIPT)	74
2.1.31	Firmware Update using Serial Console (SERUPDATE)	75
2.1.32	SFP (SFP)	77
2.1.33	Display the Common Configuration Parameters (SHOWCONFIG)	79
2.1.34	Short Message Service (SMS)	80
2.1.35	Simple Mail Transfer Protocol (SMTP)	82
2.1.36	Simple Network Management Protocol (SNMP)	85
2.1.37	Simple Network Time Protocol (SNTP)	88
2.1.38	Spanning Tree Protocol (SPAN TREE)	89
2.1.39	Entry Screen Message Display (SPLASH)	93
2.1.40	Secure Shell (SSH)	95
2.1.41	Storm Prevention (STORMCONTROL)	97
2.1.42	DIP-Switch Configuration (SWITCH)	98
2.1.43	VLAN Interface Configuration (SWITCHPORT)	100
2.1.44	Syslog Server Configuration (SYSLOG)	102
2.1.45	Time (TIME)	104
2.1.46	SNMP Trap Host (TRAPHOST)	105
2.1.47	SNMP Traps (TRAPS)	106
2.1.48	User Configuration (USER)	109
2.1.49	Firmware Version (VER)	111
2.1.50	VLAN Table (VLAN)	112
2.1.51	Zone (ZONE)	113

<b>3.0</b>	<b>Appendix A: Firmware Update .....</b>	<b>114</b>
3.1	Overview .....	114
3.2	Save Current Settings .....	114
3.3	Copy the Files to Your Hard Drive .....	114
3.4	Updating the Firmware Using FTP .....	114
<b>4.0</b>	<b>Copyright Statement .....</b>	<b>117</b>
<b>5.0</b>	<b>Customer Support Information .....</b>	<b>117</b>

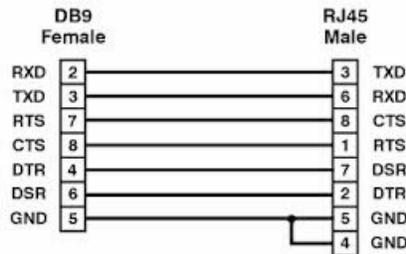
## 1.0 OVERVIEW

The Command Line Interface (CLI) provides configuration and monitoring for all OmniConverter and RuggedNet 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 2.5 adds hierarchical command line interface.

Firmware 2.4 adds DHCPv6 and DHCPv6 Relay functionality.

Firmware 2.3 adds IPv6, IPv6 Multicast Listener Discovery (MLD) Snooping, Multiple Spanning Tree Protocol (MSTP), Short Messaging Service (SMS), PoE power management with LLDP MED and MDI TLV, and PoE Power Multi-Day Scheduler.

## 2.0 COMMAND LINE INTERFACE (CLI)

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.                               GHPoEBT/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      192.168.1.220
MAC             00-06-87-02-87-50
Serial number   00720087

GHPoEBT/Mi login:

```

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

**A model with two (2) fiber uplink ports and four (4) RJ-45 user ports is used for all examples in this user manual.**

**For eight (8) RJ-45 port models or models with one (1) fiber uplink, the *-p* command will indicate the port numbers available:**

```

-p    physical port list, [pList]: {F1,F2,1..4|all}
-p    physical port list, [pList]: {F1,1..4|all}
-p    physical port list, [pList]: {F1,F2,1..8|all}
-p    physical port list, [pList]: {F1,1..8|all}

```

## 2.1 CLI COMMANDS

The commands are presented in alphabetical order and are not meant as a configuration guide. Each command has an explanation and configuration example.

Not all commands are valid for all module types. Commands not available for a specific module type will not be displayed in the CLI Command summary list.

Enter *?* or *help* to view the options. Type *exit* to return to the login screen.

```
>
CLI Command summary
For more help on a specific command, type the <command> -h

Command          Description
?                command summary (same as help command)
aaa              authentication, authorization, accounting configuration
acl              access control list configuration for management access
bwp              bandwidth profile configuration
cabletest        cable test for a copper port
contact          contact closure status
cos              class of service configuration
dir              directory of the existing files
ethertype        ethertype tag identification configuration
exit             exit the CLI session
fwload           firmware load configuration
h                command summary (same as help command)
help             command summary
igmp             internet group management protocol
ip              internet protocol 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 protocol configuration
module           module global configuration
mrp              media redundancy protocol (MRP) configuration
nest             hierarchical CLI session
ping             ping configuration
port             port attribute configuration
portaccess       port access configuration
portstat         port statistic configuration
protocol         protocol configuration
pse              power source equipment (PSE) configuration
restart          restart module
restore          restore module defaults
save             save configuration changes into permanent memory
script           create and execute script files
serupdate        upload firmware update via the serial port
sfp              small form pluggable port information
showconfig       show basic configuration information status
sms              sms texting configuration
smtp             smtp configuration
snmp             simple network management protocol user configuration
sntp             simple network time protocol configuration
spantree         spanning tree configuration
splash           splash screen warning message configuration
ssh              secure shell configuration
stormcontrol     storm control configuration
switch           physical 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
x              exit the CLI session
zone           time zone list

CLI keyboard shortcuts:
Ctrl+A         move the cursor to the beginning of the line
Ctrl+B         move the cursor backward one character
Ctrl+D         delete the character at the cursor
Ctrl+E         move the cursor to the end of the line
Ctrl+F         move the cursor forward one character
Ctrl+K         erase characters from the cursor to the end of the line
Ctrl+L         redisplay the current line on the console
Ctrl+N         or down arrow, display the next command in the commands history buffer
Ctrl+P         or up arrow, display the previous command in the commands history buffer
Ctrl+R         starts a new line with the same command previously shown
Ctrl+U         delete the whole line
Ctrl+W         delete the word to the left of the cursor
Ctrl+X         erase character from the cursor to the beginning of the line
Esc+F         move the cursor forward one word, skipping white space
Esc+B         move the cursor backward one word, skipping white space
Backspace     remove the character to the left of the cursor

>

```

### 2.1.1 Authentication, Authorization and Accounting (AAA)

The module supports Authentication, Authorization and Accounting (AAA), Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access-Control System Plus (TACACS+) and Port Based Network Access Control (802.1X).

AAA is a framework for controlling access to computer resources, enforcing policies, auditing usage and providing the information necessary to bill for services. AAA configures the client type method for console, FTP, SSH, Telnet interfaces and the authentication method TACACS+, RADIUS or local.

Remote Authentication Dial-In User Service (RADIUS) is a client/server system that secures networks against unauthorized access. When a user tries to access a specific module, the RADIUS server is contacted for validation of a correct user name and password.

The user receives one of the following responses from the RADIUS server:

ACCEPT - The user is authenticated.

REJECT - The user is not authenticated and is prompted to reenter the username and password, or access is denied.

CHALLENGE - A challenge is issued by the RADIUS server and is attempting to collect additional information from the user including username and password.

CHANGE PASSWORD - A request is issued by the RADIUS server asking the user to select a new password.

RADIUS is a stateless protocol using UDP, running on Port 1812 between the Client and the Server. A shared secret key is used to encrypt passwords and exchange responses between the client and the server.

Terminal Access Controller Access-Control System Plus (TACACS+) is a connection oriented Authentication, Authorization, and Accounting (AAA) protocol. TACACS+ is used to authenticate, authorize, and for accounting of TCP connections.

TACACS+ implements the following functions:

Authentication is the action of determining the identification of the user (or entity). It also provides complete control of the authentication process through login and password dialog, challenge and response, and messaging support.

Authorization is the action of determining what a user is allowed to do and provides fine-grained control over user capabilities for the duration of the user's session.

Accounting is the action of recording what a user is doing, and/or has done and collects and sends information used for billing, auditing, and reporting to the TACACS+ daemon.

When a user attempts to log in to a device the control passes to the TACACS+ server which provides the challenge and the user provides the response. This is typically user name, password, and other challenge questions. The information passed between the module and the TACACS+ server is encrypted based upon the TACACS+ protocol specification,

The module will eventually receive one of the following responses from the TACACS+ server during the authentication phase:

ACCEPT - The user is authenticated and service may begin. If the module is configured to require authorization, authorization begins.

REJECT - The user has failed to authenticate. The user may be denied further access, or will be prompted to retry the login sequence depending upon how the TACACS+ server is configured.

ERROR - An error occurred at some time during the authentication. If an ERROR response is received, the module will typically try to use an alternative method for authenticating the user.

CONTINUE - The user is prompted for additional authentication information.

Once the Authentication phase is complete, the Authorization phase begins (if configured on the module). The module again contacts the TACACS+ server and it returns an ACCEPT or RETURN authorization response. If an ACCEPT response is returned, the response contains attributes that are used to direct the services that the user can access.

Port Based Network Access Control is defined in IEEE 802.1X. It uses EAPoL (Ethernet Authentication Protocol over LAN) to communicate between the Supplicant (Client), Authenticator (module) and Authentication Server.

The Supplicant, or Client, is connected to a port that needs to be authenticated via the EAP Server. EAP Start Frames are sent from the Supplicant to the Authenticator.

The Authenticator, or switch, requests information from the Supplicant and strips the EAP information from the EAP Ethernet frame and places that information into a RADIUS frame and transmits the frames towards the EAP RADIUS server. The Authenticator also passes information from the EAP Server to the Supplicant in the reverse process.

The EAP Server receives the EAP requests and proceeds with the Challenge-Response sequence and finally allows or denies access to the port.

The *aaa* command provides the ability to configure AAA, RADIUS, TACACS+ and 802.1X parameters. To configure AAA, use the *aaa* option from the CLI prompt. A list of options is displayed when the *aaa -h* command is entered.

```
> aaa -h

Description:
  aaa - authentication, authorization, accounting configuration
Syntax:
  aaa [-h]
  aaa -s
  aaa {-dis|-ena} {aaa|guestvlan|radius|tacacs+|802.1x}
  aaa -ty tacacs+ [-host ipHostList] [-key aKey] [-l4 a1,a3] [-to toVal]
  aaa -ty radius [-host ipHostList] [-key aKey] [-l4 a1,a3] [-tran rNum]
    [-to toVal]
  aaa -ty 802.1x -p pList [-ptype pMode] [-auth aTime] [-retry rTime]
    [-vid gVid] [-dis|-ena guestvlan] [-xmode xModeSel]
  aaa -meth authList
  aaa -dall
Switches:
-auth 802.1X reauthorize time in sec, [aTime]: {0..65535}, dflt 3600
      a value of zero indicates that reauthorization is not required
-dall delete all aaa configured settings and restore defaults
-dis  disable function: {aaa|guestvlan|radius|tacacs+|802.1x}
-ena  enable function: {aaa|guestvlan|radius|tacacs+|802.1x}
      [aaa] authentication, authorization, accounting, dflt disabled
      [guestvlan] 802.1X guest vlan authentication, dflt disabled
      [radius] radius protocol, dflt disabled
      [tacacs+] TACACS+ protocol, dflt disabled
      [802.1x] port based access control (802.1X), dflt disabled
-h    display help information
-host server ip host list, [ipHostList]: {host1,..,hostn}
-key  server key, [aKey]: 1-63 ASCII characters, dflt not defined
-l4   layer 4 port number list, [a1,a3]
      [a1] authentication/authorization port number: {1..65535}
      [a3] accounting port number: {1..65535}
-meth authentication method, [authList]: {local,tacacs+,radius}
-p    physical port list, [pList]: {F1,F2,1..4|all}
-ptype port authentication mode, [pMode]: {auto|mac|on|off}, dflt on
      [auto] standard 802.1X authentication on a port
      [mac] 802.1X MAC bypass authentication on a port
      [on] port is always authorized, 802.1X disabled
      [off] port is always unauthorized
-retry 802.1X EAP retry time in sec, [rTime]: {1..60}, dflt 30
-s     show current configuration
-to   server timeout before error declared in sec, [toVal]: {1..60}, dflt 60
-tran RADIUS server request retry count, [rNum]: {0..10}, dflt 2
-ty   configuration type: {radius|tacacs+|802.1x}
-vid  guest VLAN ID assignment, [gVid]: {1..4095}
-xmode 802.1X mode, [xModeSel]: {discard|peer|tunnel}
      [discard] 802.1X is disabled, 802.1X frames are discarded
      [peer] 802.1X is enabled and protocol is operating
      [tunnel] 802.1X is disabled, 802.1X frames are tunneled

>
```

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

The *-auth* switch configures the 802.1X reauthorization timer. A zero value disables the timer.

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

The *-dis* and *-ena* switches disables/enables one of the following functions:

- aaa* Disables/Enables authentication, authorization, and accounting, default is disabled.
- guestvlan* Disables/Enables guest VLAN access, default is disabled.
- radius* Disables/Enables RADIUS (RFC 2865, RFC 2866), default is disabled.
- tacacs+* Disables/Enables TACACS+, default is disabled.
- 802.1x* Disables/Enables port based access control (IEEE 802.1X), default is disabled

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-host* switch configures the IP address of the host. The *-ty* command specifies the type of host.

The *-key* switch configures the secret key used to encrypt and decrypt AAA PDU information between the host and the server.

The *-l4* switch configures the TCP or UDP port numbers for the AAA protocol in the following order: authentication / authorization port (a1) and accounting port (a3).

The *-meth* switch selects the authentication method (*local*, *tacacs+*, *radius* or *none*).

The *-p* switch selects the port on the module that is associated with the AAA protocol. The default is all ports.

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

The *-s* switch displays current AAA settings.

The *-to* switch configures the AAA server wait timeout value in seconds. When the value expires, the server will declare an ERROR. A value of 0 disables the timer. The default value is 60 seconds.

The *-tran* switch configures the number of times the module transmits a server request before an ERROR is declared. The default is 2.

The *-ty* switch configures the AAA protocol type, RADIUS, TACACS+ or 802.1x.

The *-vid* switch configures the guest VLAN ID.

The *-xmode* switch 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.

To display the configuration, use the *aaa -s* command.

```
> aaa -s

AAA                                disabled
authentication method              local

TACACS+                             disabled
  server(s)
  authentication Port               49
  accounting Port                   49
  key
  timeout (sec)                     60s

RADIUS                               disabled
  server(s)
  authentication Port               1812
  accounting Port                   1813
  key
  timeout (sec)                     60s
  number of retries                 2

802.1X                               disabled (guest VLAN disabled)
  port F1                           tunnel, on
  port F2                           tunnel, on
  port 1                            tunnel, on
  port 2                            tunnel, on
  port 3                            tunnel, on
  port 4                            tunnel, on

>
```

To configure the IP address of the RADIUS server, use the following command.

```
> aaa -host 192.168.1.1 -ty radius
```

To enable RADIUS, use the *aaa -ena radius* command.

```
> aaa -ena radius
```

## 2.1.2 Access Control List (ACL)

The *acl* command provides basic traffic filtering capabilities with Access Control Lists (ACL). Access Control Lists can prevent certain traffic from entering or exiting the management port. ACLs can be configured for ARP, ICMP, IP, TCP and UDP protocols. These protocols can be configured to be permitted or denied access. Two hundred individual ACLs can be configured at one time.

The *acl* command provides the ability to configure ACL traffic filtering. To configure ACL, use the *acl* option from the CLI prompt. A list of options is displayed when the *acl -h* command is entered.

```
> acl -h

Description:
  acl - access control list configuration for management access
Syntax:
  acl [-h]
  acl -s
  acl {-dis|-ena}
  acl {-d idx|-dall}
  acl -dflt {deny|permit}
  acl -a -ipsrc ipAddr[/plen|,ipAddrEnd] [-proto {arp|icmp|ip|tcp|udp}]
      [-ty {deny|permit}] [-dst port]
  acl -ins idx -ipsrc ipAddr[/plen|,ipAddrEnd] [-proto {arp|icmp|ip|tcp|udp}]
      [-ty {deny|permit}] [-dst port]
  acl -m idx [-ipsrc ipAddr[/plen|,ipAddrEnd]] [-proto {arp|icmp|ip|tcp|udp}]
      [-ty {deny|permit}] [-dst port]
Switches:
-a      add ACL
-d      delete ACL, [idx]: {1..200}
-dall   delete all ACL configured settings, instances, and restore defaults
-dflt   default for items not found in ACL list: {deny|permit}, dflt permit
-dis    disable ACL processing, dflt
-ena    enable ACL processing
-h      display help information
-ins    insert before ACL, [idx]: {1..199}
-ipsrc  source IP address, [ipAddr[/plen|,ipAddrEnd]]
        [ipAddr] IP address (individual or starting address)
        [ipAddrEnd] ending IP address if present (all protocols but arp)
        [plen] subnet mask or prefix length
-m      modify ACL, [idx]: {1..200}
-proto  protocol: {arp|icmp|ip|tcp|udp}, dflt ip
-s      show current configuration
-ty     ACL access type: {deny|permit}

>
```

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

The *-a* switch adds a new ACL filter.

The *-d* switch deletes an existing ACL filter by index number.

The *-dall* switch deletes all configured ACL filters and restores factory defaults.

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

The *-dis* switch disables ACL processing.

The *-dst* switch selects a TCP or UDP destination port number for an ACL filter. A value of *-1* does not select a specific TCP or UDP port.

The *-ena* switch enables ACL processing. If the ACL table is empty, the default behavior (*-dflt*) is applied to all Ethernet frames that enter the module.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-ins* switch inserts before ACL.

The *-ipsrc* switch selects the IP source address for an ACL filter. The source IP address for ARP is the Send IP Address.

The *-m* switch modifies an existing ACL filter.

The *-proto* switch selects the protocol:

- arp*        Selects the ARP protocol.
- icmp*      Selects the ICMP protocol.
- ip*         Selects the IP protocol.
- tcp*        Selects the TCP protocol.
- udp*        Selects the UDP protocol.

The *-s* switch displays the configured ACL filters.

The *-ty* switch selects the ACL access type; permit or deny.

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.

To display the configuration, use the *acl -s* command.

```
> acl -s

ACL processing is Disabled
Default ACL behavior is '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.

```
> acl -dall
> acl -a -ipsrc 172.16.9.1,172.16.9.5 -proto icmp -ty deny
> acl -a -ipsrc 172.16.9.1,172.16.9.5 -proto ip -ty permit
> acl -a -ipsrc 172.16.9.5/24 -proto arp -ty permit
> acl -ena

> acl -s

ACL processing is Enabled
Default ACL behavior is 'permit'

#    ACL Details
1    172.16.9.1..172.16.9.5 ICMP via mgt1: deny
2    172.16.9.1..172.16.9.5 IP via mgt1: permit
3    172.16.9.5 ARP via mgt1: permit

>
```

### 2.1.3 Bandwidth Profile (BWP)

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

Bandwidth profiles specifies the average rate of committed and excess Ethernet frames allowed into the provider's network. Bandwidth profiles consist of the following parameters:

#### **Committed Information Rate (CIR)**

CIR specifies the maximum rate Ethernet frames are delivered per service performance objectives. These frames are referred to as being in-profile (green).

#### **Committed Burst Size (CBS)**

CBS is the maximum number of bytes allowed for incoming Ethernet frames maintaining in-profile. The value of CBS will depend on the type of application or traffic being supported. Bursty data applications will require a larger CBS than more constant rate applications.

#### **Egress Committed Information Rate (ECIR)**

ECIR specifies the average rate Ethernet frames egress the port. When configuring ECIR, an egress queue type can be specified (starvation queuing - strict/low latency, weighted fair queuing - high latency or mixed). Starvation queuing processes all high priority traffic before any low priority traffic and uses a strict priority scheme. Weighted fair queuing will process high priority traffic more often than low priority traffic. The default weighted fair queuing mix is 33 (high priority), 25, 17, 12, 6, 3, 2, 1 (low priority).

To configure bandwidth profiles, use the *bwp* option from the CLI prompt. A list of options is displayed when the *bwp -h* command is entered.

```
> bwp -h

Description:
  bwp - bandwidth profile configuration
Syntax:
  bwp [-h]
  bwp -s [-p pNum]
  bwp -dall
  bwp -d -p pNum [-cn cName]
  bwp -p pNum [-que qType] [-ecir cirRate[,eQueue]] [-epol pType]
  bwp -p pNum [-cir cirRate] [-cbs cbsSize] [-pol poltype] [-cn cName]
    [-perf|-noper]
  bwp -fwmix qVal
Switches:
-cbs  committed burst size in KB, [cbsSize]: {2..256}, dflt 15
-cir  committed ingress information rate in kb/sec, [cirRate]: {64..1000000},
      dflt 1000000
-cn   class of service name, [cName]: 1-45 ASCII characters
-d    delete a specific configured profile or restore dflt port configuration
-dall delete all BWP configured bwp settings and restore defaults
-ecir committed egress information rate, [cirRate[,eQueue]]
      [cirRate] in kb/sec: {0,64..1000000}, where 0=max rate, dflt 1000000
      [eQueue]: {0..7}, dflt blank - port based
-epol egress policing type, [pType]: {l1,l2,l3}, dflt l2
-fwmix port queue global fairweight mixture, [qVal]: {q7,q6,q5,q4,q3,q2,q1,q0}
      where 'x' is a specific queue and qx is a value from 0..100 for the
      specific queue and the sum of all queues is 128 max
-h    display help information
-noper no traffic performance monitoring
-p    port number, [pNum]: {F1|F2|1..4}
-perf traffic performance monitoring
-pol  policing count type, [polType]: {l1,l2,l3}, dflt is l2
-que  type of egress queue, [qType]: {fairweight|starving|qlist}
      where qlist is {q7,q6,q5,q4,q3,q2,q1,q0}, where qx is 'sp' or 'fw'
      'sp' indicates strict priority, but 'sp' can only be selected from
      queue 7 sequentially to a lower queue number
      'fw' indicates fairweight
-s    show current configuration

>
```

**NOTE: Port number selection will vary depending on the model.**

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

The *-cbs* switch sets the Committed Burst Size (maximum number of bytes allowed) of the ingress frames.

The *-cir* switch sets the Committed Information Rate of the ingress frames.

The *-cn* switch defines the name of the Class of Service profile.

The *-d* switch deletes the bandwidth profile.

The *-dall* switch deletes all configured bandwidth profiles.

The *-ecir* switch defines the Committed Information Rate of the egress frames.

The *-epol* switch configures the egress policing type used. The options are L1 or L2. The default is L2.

The *-fwmix* switch defines 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 (,).

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-noper* switch disable traffic performance monitoring.

The *-p* switch defines the port associated with the bandwidth profile.

The *-perf* switch enables traffic performance monitoring.

The *-pol* switch defines the policing count as layer 1 (frame + interframe gap + preamble), layer 2 or layer 3 frame types on a per port basis.

The *-que* switch defines the type of egress queueing used (fairweight, starving or individually configured).

- starving* All queues are set up to starving (strict) priority
- fairweight* All queues are setup for weighted fair queueing using the *fwmix* setting.
- 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 (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

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.

The *-s* switch displays the current bandwidth profiles.

To display the configuration, use the *bwp -s* command.

```
> bwp -s

Fairweight mix = 33,25,17,12,6,3,2,1

Port F1:
  ingress cir 1000000kbps, cbs 15 kB, L2 policing
  egress cir 1000000kbps, L2 policing, queue type fairweight
  egress queue rate (kbps) q7/q6/q5/q4/q3/q2/q1/q0 =
    1000000/1000000/1000000/1000000/1000000/1000000/1000000/1000000
  PCP classification over IP
  no performance monitoring
Port F2:
  ingress cir 1000000kbps, cbs 15 kB, L2 policing
  egress cir 1000000kbps, L2 policing, queue type fairweight
  egress queue rate (kbps) q7/q6/q5/q4/q3/q2/q1/q0 =
    1000000/1000000/1000000/1000000/1000000/1000000/1000000/1000000
  PCP classification over IP
  no performance monitoring
Port 1:
  ingress cir 1000000kbps, cbs 15 kB, L2 policing
  egress cir 1000000kbps, L2 policing, queue type fairweight
  egress queue rate (kbps) q7/q6/q5/q4/q3/q2/q1/q0 =
    1000000/1000000/1000000/1000000/1000000/1000000/1000000/1000000
  PCP classification over IP
  no performance monitoring
Port 2:
  ingress cir 1000000kbps, cbs 15 kB, L2 policing
  egress cir 1000000kbps, L2 policing, queue type fairweight
  egress queue rate (kbps) q7/q6/q5/q4/q3/q2/q1/q0 =
    1000000/1000000/1000000/1000000/1000000/1000000/1000000/1000000
  PCP classification over IP
  no performance monitoring
Port 3:
  ingress cir 1000000kbps, cbs 15 kB, L2 policing
  egress cir 1000000kbps, L2 policing, queue type fairweight
  egress queue rate (kbps) q7/q6/q5/q4/q3/q2/q1/q0 =
    1000000/1000000/1000000/1000000/1000000/1000000/1000000/1000000
  PCP classification over IP
  no performance monitoring
Port 4:
  ingress cir 1000000kbps, cbs 15 kB, L2 policing
  egress cir 1000000kbps, L2 policing, queue type fairweight
  egress queue rate (kbps) q7/q6/q5/q4/q3/q2/q1/q0 =
    1000000/1000000/1000000/1000000/1000000/1000000/1000000/1000000
  PCP classification over IP
  no performance monitoring

>
```

To configure a bandwidth profile with performance monitoring on Port 1 for 500Mbps, use the following command.

```
> bwp -p 1 -cir 500000 -perf
> bwp -s -p 1

Fairweight mix = 33,25,17,12,6,3,2,1

Port 1:
  ingress cir 500000kbps, cbs 15 kB, L2 policing
  egress cir 1000000kbps, L2 policing, queue type fairweight
  egress queue rate (kbps) q7/q6/q5/q4/q3/q2/q1/q0 =
    1000000/1000000/1000000/1000000/1000000/1000000/1000000/1000000
  PCP classification over IP
  status in profile, receiving 0 kbps, dropped octets 0

>
```

Performance monitoring provides information on the information on in / out of profile traffic based on the bandwidth profile.

#### 2.1.4 Cable Test (CABLETEST)

The *cabletest* command initiates a cable test on fixed RJ-45 copper ports. The test checks for breaks in the cable and reports how far from the source the cable break is detected. The cable test will interrupt service on the selected port.

To initiate a cable test, use the *cabletest* command from the CLI prompt. A list of options is displayed when the *cabletest -h* command is entered.

```
> cabletest -h

Description:
  cabletest - cable test for a copper port
Syntax:
  cabletest [-h]
  cabletest -p pNum
Switches:
-h      display help information
-p      port number, [pNum]: {1..4}

>
```

**NOTE: Port number selection will vary depending on the model.**

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

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-p* switch selects initiating port for the cable test.

**NOTE: Ports F1 and F2 are not supported.**

In this example, a cable test is initiated on Port 2.

```
> cabletest -p 2

Testing Port number 2: no cable break detected
```

In this example, a cable test is initiated on Port 1 showing a break in the cable.

```
> cabletest -p 1
Testing Port number 1: cable failure detected at 1m from source
```

### 2.1.5 Contact (CONTACT)

**Only supported on the RuggedNet switch products.**

The *contact* command provides the ability to display the status of the contact closure and alarm input. It also provides the ability to assign a failure type and name to the contact closure.

To configure and display the contact closure, use the *contact* command from the CLI prompt. A list of options is displayed when the *contact -h* command is entered.

```
> contact -h

Description:
  contact - contact closure status
Syntax:
  contact [-h]
  contact -mode {none|force|input,power,temp}
  contact [-nmc cName] [-nmi cName] [nmo cName]
  contact -s
  contact -dall
Switches:
-dall  delete all 'contact' configured settings and restore defaults
-h     display help information
-mode  contact closure alarm output mode: {force,input,none,power,temp}
      [force] output contact is activated
      [input] output contact is activated when digital input is open
      [none] output contact is never activated, dflt ""
      [power] output contact activated when internal power alarm is detected
      [temp] output contact activated when temperature violation is detected
-nmc   selects the name of the normally closed relay, dflt ""
-nmi   selects the name of the digital input sense, dflt ""
-nmo   selects the name of the normally open relay, dflt ""
-s     show current status

>
```

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

The *-dall* switch deletes all contact configured settings and restores factory defaults.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-mode* switch selects the type of error that will cause the output relay to close; force, 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* switch configures the name of the normally closed relay contacts.

The *-nmi* switch configures the name for the alarm input.

The *-nmo* switch configures the name for the normally opened relay contacts.

The *-s* switch displays the input status (open or closed) and contact closure status (not activated, activated). Activated indicates a normally open contact has closed or a normally closed contact has opened. Not activated indicates a normally open contact is open or a normally closed contact is closed.

The alarm contact connector is located on the top of the module and is used to detect the state of external alarm conditions.

The pinout for the alarm contact is shown below.

Pin	Function
1	Normally Open - Output
2	Common - Output
3	Normally Closed - Output
4	Detection - Input
5	Detection - Ground

*Alarm Contact Description*

To name the alarm input, use the *contact -nmi* command.

```
> contact -nmi "open door alarm"
> contact -s

Digital input status "open door alarm": open
Contact closure output alarm state: not activated
Contact closure normally open ""
Contact closure normally closed ""
Contact closure output mode: none
  Digital input: N/A
  Power: N/A
  Temperature: N/A

>
```

To configure the alarm relay to activate on the alarm input detection, use the *contact -mode input* command.

```
> contact -mode input
> contact -s

Digital input status "open door alarm": open
Contact closure output alarm state: activated
Contact closure normally open ""
Contact closure normally closed ""
Contact closure output mode: input
  Digital input: open
  Power: N/A
  Temperature: N/A

>
```

## 2.1.6 Class of Service (COS)

The *cos* command provides the ability to configure and display Class of Service profiles associated with each port on the module.

To configure class of service, use the *cos* option from the CLI prompt. A list of options is displayed when the *cos -h* command is entered.

```
> cos -h

Description:
  cos - class of service configuration
Syntax:
  cos [-h]
  cos -s [-cn cName]
  cos {-d -cn cName}|{-dall}
  cos -a -cn cName [-pcp pcpList|-dscp dList -class cClass]
      [-mode cMode] [-dflt class]
  cos -m -cn cName [-pcp pcpList|-dscp dList -class cClass]
      [-mode cMode] [-dflt class]
Switches:
-a      add CoS profile
-class  class of service (egress queue), [cClass]: {0..7}
        [0..7] adds specific class list, 0=lowest, 7=highest priority
-cn     class of service identifier name, [cName]: 1-45 ASCII characters
-d      delete CoS profile
-dall   delete all CoS configured settings, instances, and restore defaults
-dflt   default class classification, [class]: {0..7}, dflt 1
-dscp   layer 3 IP priority, [dList]: {0..63|none}
        examples: 1 or 1,4 or 1..3 or 2..3,6..7 or none
-h      display help information
-m      modify CoS profile
-mode   mode classification mode, [cMode]: {ip|ipoverl2|l2|l2overip|none}
        [ip] ip only classification
        [ipoverl2] ip classification priority over layer 2 PCP
        [l2] layer 2 PCP classification only
        [l2overip] layer 2 PCP classification over IP, dflt
        [none] neither layer 2 or IP classification are used
-pcp    layer 2 priority bits, [pcpList]: {0..7|none}
        examples: 1 or 1,4 or 1..3 or 2..3,6..7 or none
-s      show current configuration

>
```

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

The *-a* switch adds a class of service profile.

The *-class* switch sets the egress queue priority for the ingress frame.

The *-cn* switch defines the name of the class of service profile.

The *-d* switch deletes a class of service profile.

The *-dall* switch deletes all configured CoS profiles and restores factory defaults.

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

The *-dscp* switch defines the profile based on the IP priority bits of the ingress frame.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-m* switch modifies a defined class of service profile.

The *-mode* switch defines the ingress classification mode.

- ip* Selects the IP only classification (DSCP), layer 2 classification is ignored.
- ipoverl2* Selects the IP classification (DSCP) over layer 2 classification (PCP) if both are present.
- l2* Selects the layer 2 classification only (PCP), IP classification is ignored.
- l2overip* Select layer 2 classification (PCP) over IP classification (DSCP) if both are present.
- none* No classification mode is configured.

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* switch defines the profile based on the PCP bit of the ingress frame.

The *-pcp* switch defines the priority of the PCP bit of the ingress frame.

The *-s* switch displays the current class of service profiles.

Class of Service (CoS) is supported by mapping customer frames into eight egress queues based on using the 3-bit Priority Code Point (PCP) field in the VLAN tag.

The priority of ingress frames correspond to eight possible values or priorities (0 through 7). Each frame is mapped to one of eight egress queues based on the PCP priority field. See the default mapping of PCP value to egress queue.

Quality of Service (QoS) Egress Queuing								
Priority Code Point (PCP)	0	1	2	3	4	5	6	7
Egress Queue (Class)	0	1	2	3	4	5	6	7

*Egress Queue vs Frame Priority  
(Default Mapping)*

Class of Service profiles can use DSCP or PCP fields to reclassify and prioritize the ingress frames.

Differentiated Services Code Point (DSCP) profiles are associated with IP priority bits (ipPri). Values are 0 - 63. Priority Code Point (PCP) profiles are associated with the tagged priority bits (pbits). Values are 0 - 7.

Traffic priority can be re-classified by using the *class* or *pcp* command. The *class* command will re-classify which egress priority queue is used. The *pcp* command re-classifies the priority by changing the PCP value.

Traffic is mapped to eight egress queues based on the PCP values. The CoS commands provides the ability to change the egress queue (*class*) or PCP value (*pcp*) or both. PCP values are 0 - 7, 7 being the highest priority. Class values are 0 - 7, 0 being discard and 7 being the highest egress queue. Class values 0 - 7 correspond to egress queues 0 - 7.

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 (Section 6.1.3 and 7.3.4.3). If the ingress frame does not meet any of the configured CoS profiles, the ingress traffic will use the default class classification.

In the example below class of service profile is created.

```
> cos -a -cn data      -pcp 0..1  -class 0
> cos -m -cn data     -pcp 2..3  -class 2
> cos -m -cn data     -pcp 4..6  -class 4
> cos -m -cn data     -pcp 7     -class 7
```

To display the configuration, use the *cos -s* command.

```
> cos -s

Class of Service "data": PCP classification over IP, default class 1
  PCP 0..1, class 0
  PCP 2..3, class 2
  PCP 4..6, class 4
  PCP 7, class 7

>
```

## 2.1.7 File Directory (DIR)

The *dir* command provides the ability to view/delete the files stored on the module.

To view/delete the files stored on the module, use the *dir* command from the CLI prompt. A list of options is displayed when the *dir -h* command is entered.

```
> dir -h

Description:
  dir - directory of the existing files
Syntax:
  dir [-h]
  dir -d fileName
  dir -s
Switches:
-d      delete file, [fileName]
-h      display help information
-s      show available files

>
```

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

The *-d* switch deletes a specific file on the module.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-s* switch displays the files stored on the module.

To display the files stored on the module, use the *dir -s* command.

```
> dir -s

Name                               Size
=====
current.ini                         2746
traplog.txt                         44035
previous.ini                        2750

Total: 3 items listed (49531 bytes)

>
```

## 2.1.8 Ethertype (ETHERTYPE)

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.

To configure the Ethertype, use the *ethertype* command from the CLI prompt. A list of options is displayed when the *ethertype -h* command is entered.

```
> ethertype -h

Description:
  ethertype - ethertype tag identification configuration
Syntax:
  ethertype [-h]
  ethertype -s
  ethertype -trunk ethertypeVal
  ethertype -dall
Switches:
-dall delete all ethertype configured settings and restore defaults
-h     display help information
-trunk provider network Ethertype, [ethertypeVal], dflt 8100
      [ethertypeVal] selects the Ethertype that is used for the selected
      network type, value is entered in hex, typical selection for
      customer networks is 8100, for provider networks 88a8
-s     show current configuration

>
```

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

The *-dall* switch deletes all configured ethertype settings and restores to factory defaults.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-trunk* switch configures the Ethertype for provider tagged frames. The default is 8100.

The *-s* switch displays the Ethertype configuration of the module.

Use the following commands to configure the S-Tag (Provider Tag) for a Ethertype value of 88a8.

```
> ethertype -trunk 88a8
```

To display the Ethertype configuration, use the *ethertype -s* command.

```
> ethertype -s

tunnel (C-TAG) ethertype value   8100
trunk   (S-TAG) ethertype value   88a8

>
```

## 2.1.9 Load Firmware (FWLOAD)

The *fwload* command programs the module with a firmware file that is stored on the module or a firmware file downloaded from a tftp server (use the *-ip* option to configure the tftp server IP address).

To program the firmware stored on the module or tftp server, use the *fwload* command from the CLI prompt. A list of options is displayed when the *fwload -h* command is entered.

```
> fwload -h

Description:
  fwload - firmware load configuration
Syntax:
  fwload [-h]
  fwload -s
  fwload -d fileName
  fwload -f fileName [-t app|bootloader] [-ip tftpServerIp]
Switches:
-d      delete specified firmware file, [fileName]
-f      write specified firmware file, [fileName]
-h      display help information
-ip     TFTP Server ip address, [tftpServerIp]
-s      show current available firmware files
-t      firmware file type: {app|bootloader}, dflt app

>
```

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

The *-d* switch deletes a firmware file on the module.

The *-f* switch selects the firmware file to loaded on the module.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-ip* switch specifies the IP address of the TFTP server used for the upgrading of the firmware on the module.

The *-s* switch displays the list of available files on the module.

The *-t* switch selects the type of file that is upgraded: application or boot loader.

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:

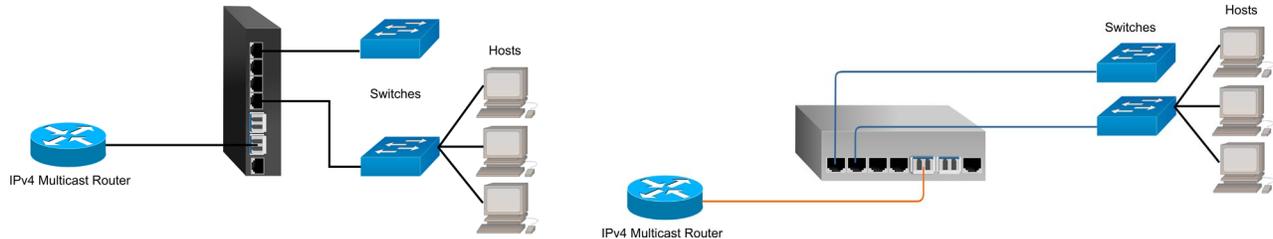
```
> fwload -f <filename.dat>

Starting upgrade using file filename.dat
Upgrade complete, reboot pending...

>
```

## 2.1.10 Internet Group Management Protocol (IGMP)

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.

To configure the IGMP snooping on the module, use the *igmp* command from the CLI prompt. A list of options is displayed when the *igmp -h* command is entered.

```
> igmp -h

Description:
  igmp - internet group management protocol configuration
Syntax:
  igmp [-h]
  igmp -s
  igmp [-dis|-ena flood|snooping] [-to toVal]
  igmp -a -vid vVid [-grp ipAddr -ph hnum -pr rnum [{-dis|ena} aging]]
  igmp -d -vid vVid [-grp ipAddr]
  igmp -m -vid vVid -grp ipAddr [-ph hnum] [-pr rnum] [{-dis|ena} aging]
  igmp -dall
Switches:
-a      add manual forwarding map or IGMP interface
-d      delete existing forwarding map or IGMP interface
-dall   delete all IGMP configured settings, instances, and restore defaults
-dis    disable function: {aging|flood|snooping}
-ena    enable function: {aging|flood|snooping}
        [aging] IGMP route subject to aging out, dflt disable
        [flood] flooding of all unrecognized IGMP groups, dflt disable
        [snooping] IGMP snooping, dflt disable
-grp    IGMP Group Address, [ipAddr]
-h      display help information
-m      modify existing forwarding map
-ph     host port [hnum]: {F1,F2,1..4}
-pr     router port [rnum]: {F1,F2,1..4}
-s      show current configuration
-to     IGMP route aging in seconds, [toVal]: {0..65535}, dflt 60s
-vid    VLAN ID, [vVid]: {1..4095}

>
```

**NOTE: Port number selection will vary depending on the model.**

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

The *-a* switch manually adds a IGMP route, including source router (*-evc*) and destination host (*-grp* IP address).

The *-d* switch deletes an IGMP route.

The *-dall* switch deletes all IGMP configured settings and restore factory defaults.

The *-dis* and *-ena* switches disables/enables aging, flooding and snooping:

*aging* Disables/Enables aging on a specific IGMP route.

*flood* Disables/Enables flooding of unrecognized IGMP routes.

*snooping* Disables/Enables IGMP snooping.

The *-grp* switch selects the specific IGMP multicast IP address group.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-m* switch modifies an existing IGMP route.

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

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

The *-s* switch displays the current IGMP configurations for the module.

The *-to* switch 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* switch selects the VLAN ID.

**NOTE: 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.**

To display the current IGMP configuration, use the *-s* command.

```
> igmp -s

Snooping:           Disabled
IGMP Flooding:      Disabled
Snooping timeout:   60s

IGMP VID Interfaces

>
```

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

```
> igmp -a -vid 1
> igmp -ena snooping
> igmp -s

Snooping:           Enabled
IGMP Flooding:      Disabled
Snooping timeout:   60s

IGMP VID Interfaces
Entry 1 vid 1

>
```

To manually configure a IGMP route, use the *-grp* to define the multicast IP address and the *-pr* and *-ph* to configure the multicast router and host ports.

```
> igmp -a -vid 1 -grp 225.100.100.1 -pr 1 -ph 3
> igmp -ena snooping
> igmp -s

Snooping:           Enabled
IGMP Flooding:      Disabled
Snooping timeout:   60s

IGMP VID Interfaces
Entry 1 vid 1

IP Address      Type      Persistence  Router Port  Host Port  VLAN ID
225.100.100.1  Manual   Static       1             3          1

>
```

## 2.1.11 IP (IP)

The *ip* command provides the ability to configure the IPv4 and IPv6 parameters on the module. DHCP and DHCP relay (option 82) can also be enabled and/or disabled.

To configure IP, use the *ip* command from the CLI prompt. A list of options is displayed when the *ip -h* command is entered.

```
> ip

Description:
  ip - IP configuration
Syntax:
  ip [-h]
  ip -s
  ip [-addr ipAddr[/plen[,link]] [-net subnet] [-gw gateway] [-dns ipAddr]
  ip [{-dis|-ena} circuitid|dhcp|dhcpx6|dns|ipv4|ipv6|relay|remoteid|stateless|
  v6circuitid|v6relay|v6remoteid] [-rserver ipAddr] [-rtype tsel]
  ip -dall
Switches:
-addr  IP address: [ipAddr][[/plen][,link]
       [ipAddr] IP4 or IPv6 address
       [plen] subnet mask or prefix length
       [link] IPv6 address type is link-local, instead of stateful
-dall  delete all IP configured settings and restore defaults
-dns   domain name system ip address, [ipAddr], dflt blank
-dis   disable function: {circuitid|dhcp|dhcpx6|dns|ipv4|ipv6|relay|remoteid|
       stateless|v6circuitid|v6relay|v6remoteid}
-ena   enable function: {circuitid|dhcp|dhcpx6|dns|ipv4|ipv6|relay|remoteid|
       stateless|v6circuitid|v6relay|v6remoteid}
       [circuitid] DHCPv4 Relay Agent Circuit ID enable/disable, dflt enabled
       [dhcp] DHCPv4 protocol enable/disable, dflt disabled
       [dhcpx6] DHCPv6 protocol enable/disable, dflt disabled
       [dns] Domain Name System enable/disable, dflt disabled
       [ipv4] IPv4 enable/disable, dflt enabled
       [ipv6] IPv6 enable/disable, dflt enabled
       [relay] DHCPv4 relay agent (option 82) enable/disable, dflt disabled
       [remoteid] DHCPv4 Relay Agent Remote ID enable/disable, dflt enabled
       [stateless] IPv6 stateless enable/disable, dflt enabled
       [v6circuitid] DHCPv6 Relay Interface-ID enable/disable, dflt enabled
       [v6relay] DHCPv6 relay agent enable/disable, dflt disabled
       [v6remoteid] DHCPv6 Relay Agent Remote-ID enable/disable, dflt enabled
-gw   gateway address, [gateway]
-h    display help information
-net  subnet mask, [subnet]
-rserver DHCP Relay Remote Server IPv4 or IPv6 address, [ipAddr]
-rtype DHCP Relay client type, [tsel]: {drop|keep|replace}, dflt replace
-s    show current configuration

>
```

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

The *-addr* switch configures the IPv4 and IPv6 addresses of the module.

The *-dall* switch deletes all IP configured settings and restores factory defaults.

The *-dis* and *-ena* switches disables/enables the following:

- circuitid* Disables/Enables the Agent Circuit ID for DHCP Option 82 on the module.
- dhcp* Disables/Enables DHCPv4 protocol on the module.
- dhcpx6* Disables/Enables DHCPv6 protocol on the module.

- dns* Disables/Enables DNS protocol on the module.
- ipv4* Disables/Enables IPv4 protocol on the module.
- ipv6* Disables/Enables IPv6 protocol on the module.
- relay* Disables/Enables DHCPv4 Relay function (option 82) on the module.
- remoteid* Disables/Enables DHCPv4 Relay Agent Remote ID.
- stateless* Disables/Enables Stateless operation on the module.
- v6circuitid* Disables/Enables DHCPv6 Relay Interface-ID enable/disable, dflt enabled
- v6relay* Disables/Enables DHCPv6 relay agent enable/disable, dflt disabled
- v6remoteid* Disables/Enables DHCPv6 Relay Agent Remote-ID enable/disable, dflt enabled

The *-gw* switch configures the gateway IP address of the module.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-net* switch configures the subnet mask of the module.

The *-rserver* switch configures the IPv6 address of the DHCP Relay Server.

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

- drop* Drops the DHCPv4 relay frame received on a client port.
- keep* Forwards the DHCPv4 relay frame received on a client to the server port without changing to the DHCP relay options.
- replace* Updates the DHCPv4 relay frame received on a client port with the configured DHCP relay options before forwarding it to the server port.

The *-s* switch displays the current IP configuration.

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.

To configure the IPv4 address on the module, use the *-addr* command.

```
> ip -addr 192.168.1.100
```

To configure the IPv6 address on the module, use the *-dis* and *-addr* commands.

```
> ip -dis stateless
> ip -addr 2001::a0a:652/64
```

To enable the DHCPv6 address on the module, use the *-ena* command.

```
> ip -ena dhcpv6
```

Use the `-s` command to view the IP configuration of the module.

```
> ip -s

IPv4                enabled
IPv6                enabled

IP 1
  MAC address       00-06-87-02-86-E0
  IPv4 address      192.168.1.124
  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:fe02:86e0/64
                   ::/64
  IPv6 gateway address fe80::1
  DHCPv6            disabled

>
```

## 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 client.
5. The sub option fields are removed by the relay agent and the IP address information is forwarded to the client.

### NOTES:

**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.

### **2.1.12 Link Aggregation Groups (LAG)**

Link Aggregation Groups (LAG) and Link Aggregation Control Protocol (LACP) are methods to provide more than one link between two devices and automate the configuration and maintenance of the links. LAG and LACP are defined in the IEEE 802.1ax standard.

Link aggregation as defined in IEEE 802.1ax groups Ethernet interfaces to build a single link layer interface, called a Link Aggregation Group or bundle.

Grouping multiple links between physical interfaces creates a single logical point-to-point link or LAG. The LAG balances traffic across the member links within an aggregated Ethernet group and effectively increases the uplink bandwidth. Another advantage of link aggregation is increased availability, because the LAG is composed of multiple links. If one link fails, the LAG continues to carry traffic over the remaining links.

LAG needs to be configured manually on each pair of physical interfaces. With LAG, all the interfaces must operate at the same speed and be in full-duplex mode.

Link Aggregation Control Protocol (LACP), when enabled, automates the LAG connectivity.

The main purpose of LACP is to automate the configuration and maintenance of Link Aggregation Groups. LACP dynamically adds or deletes individual links to the aggregated bundle and provides the mechanism for recovery from link failures. LACP helps prevent communication failure by detecting misconfigurations on the local end and remote end of the link.

The *lag* command provides the ability to configure the ports on the module to support Link Aggregation Group and Link Aggregation Control Protocol. A list of options is displayed when the *lag -h* command is entered.

```
> lag -h

Description:
  lag - link aggregation group configuration
Syntax:
  lag [-h]
  lag -s [-ver]
  lag -lp lNum [-ena|-dis {active,fast,key,lag}]
      [-aggrk kVal] [-act aNum]
  lag -p pList [-ppri pNum] [-proto pMode] [-lp lNum] [-clr]
  lag [-ena|-dis lag] [-spri sNum] [-fwd {std|xor}]
  lag -dall
Switches:
-act  maximum number of active ports in a LAG, [aNum]: {1..4}, dflt 4
-aggrk aggregator admin key, [kVal]: {0..65535}
-clr  clear statistic counters
-dall delete all LAG configured settings and restore defaults
-dis  disable function: {active,fast,key,lag}
-ena  enable function: {active,fast,key,lag}
      [active] LAG active mode, dflt disable (passive)
      [fast] port fast timeout, dflt disable (slow)
      [key] port auto key adjust, dflt enable (auto)
      [lag] LAG module/aggregator enable/disable, dflt disable
-fwd  frame forwarding algorithm: {std|xor}, dflt std
-h    display help information
-lp   aggregator logical port number, [lNum]: {L1..L8}
-p    group port list, [pList]: {F1,F2,1..4}
-ppri port priority, [pNum]: {0..65535}
-proto LACP protocol configuration, [pMode]: {discard,peer,static,tunnel}
      [discard] LACP is disabled, LACP frames are discarded, LAG is disabled
      [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
-s    show current configuration
-spri system priority, [sNum]: {0..65535}
-ver  verbose show

>
```

**NOTE: Port number selection will vary depending on the model.**

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

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

The *-aggrk* sets the link aggregation group key.

The *-clr* switch allows the port statistic counters to be cleared to zero.

The *-dall* switch deletes all LAG configured setting and restore to factory defaults.

The *-dis* and *-ena* switches disables/enables one of the following functions:

- active*      Disables/Enables port active mode and disables port passive mode.
- fast*        Disables/Enables LACP fast transmission mode and disables slow transmission mode.
- key*         Disables/Enables automatic key adjustment and disables manual key usage.
- lag*         Disables/Enables LAG on the module.

The *-fwd* switch configures the frame forwarding algorithm: std or xor.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-lp* switch sets the logical port number for LAG.

The *-p* switch selects the port to be used for the Link Aggregation Group.

The *-ppri* switch configures the port priority.

The *-proto* switch configures how the LAG protocol will be handled (discard, peer or tunnel)

The *-s* switch displays the configured settings.

The *-spri* switch configures the system priority.

The *-ver* switch displays the extended status screens.

To display the current LAG configuration, use the *lag -s* command.

```
> lag -s

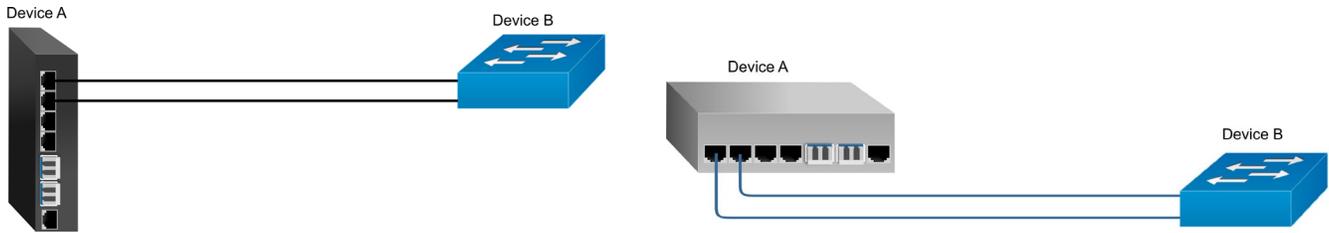
Link aggregation: disabled
System identification: 00-06-87-02-86-E0
System priority: 0
Frame forwarding: Standard

  LAG      Key  LACP  Tx  Aggr  Max
Aggr Mode  Type Role  Rate Key  Act
=====
L1  Disabled  Auto  Passive  Slow  1    4
L2  Disabled  Auto  Passive  Slow  2    4
L3  Disabled  Auto  Passive  Slow  3    4
L4  Disabled  Auto  Passive  Slow  4    4
L5  Disabled  Auto  Passive  Slow  5    4
L6  Disabled  Auto  Passive  Slow  6    4

  LACP      Port  --- Aggregation ---  Partner ---
Port  Protocol  Pri  Status  ID  LP  Sys ID          Port  Pri
=====
F1  Tunnel    32768  Detached  1  L1  00-00-00-00-00-00 0    0
F2  Tunnel    32768  Detached  2  L2  00-00-00-00-00-00 0    0
1   Tunnel    32768  Detached  3  L3  00-00-00-00-00-00 0    0
2   Tunnel    32768  Detached  4  L4  00-00-00-00-00-00 0    0
3   Tunnel    32768  Detached  5  L5  00-00-00-00-00-00 0    0
4   Tunnel    32768  Detached  6  L6  00-00-00-00-00-00 0    0

>
```

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



```

> lldp -proto tunnel -p f1,f2

> lag -p f1 -ppri 100 -proto peer -lp L1
> lag -p f2 -ppri 200 -proto peer -lp L1
> lag -lp L1 -act 2

> lag -ena lag

> lag -s

```

```

Link aggregation: enabled
Link aggregation: enabled
System identification: 00-06-87-02-A5-80
System priority: 0
Frame forwarding: Standard

```

LAG Aggr	Mode	Key Type	LACP Role	Tx Rate	Aggr Key	Max Act
L1	Disabled	Auto	Passive	Slow 1	1	2
L2	Disabled	Auto	Passive	Slow 2	2	4
L3	Disabled	Auto	Passive	Slow 3	3	4
L4	Disabled	Auto	Passive	Slow 4	4	4
L5	Disabled	Auto	Passive	Slow 5	5	4
L6	Disabled	Auto	Passive	Slow 6	6	4

Port	LACP Protocol	Port Pri	--- Aggregation --- Status	ID	LP	----- Partner ----- Sys ID	Port	Pri
F1	Peer	100	Detached	1	L1	00-00-00-00-00-00	0	0
F2	Peer	200	Detached	1	L1	00-00-00-00-00-00	0	0
1	Tunnel	32768	Detached	3	L3	00-00-00-00-00-00	0	0
2	Tunnel	32768	Detached	4	L4	00-00-00-00-00-00	0	0
3	Tunnel	32768	Detached	5	L5	00-00-00-00-00-00	0	0
4	Tunnel	32768	Detached	6	L6	00-00-00-00-00-00	0	0

>

## 2.1.13 Link Layer Discovery Protocol (LLDP)

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. To configure LLDP, use the *lldp* option from the CLI prompt. A list of options is displayed when the *lldp -h* command is entered.

```
> lldp -h

Description:
  lldp - link layer discovery protocol (LLDP) configuration
Syntax:
  lldp [-h]
  lldp -s [-p pList]
  lldp -dall
  lldp [-txfin tSec] [-txhld tVal] [-txrt tSec]
  lldp -p pList [-mode {rxtx|txonly|rxonly|none}]
      [-tlv {mgt,pdes,sysname,sysdes,syscap}] [-proto pMode]
Switches:
-dall  delete all LLDP configuration settings and restore defaults
-h     display help information
-mode  lldp mode: {rxtx|txonly|rxonly|none}
      [none] neither lldp transmitter or receiver is enabled
      [rxonly] lldp receiver is enabled
      [rxtx] both lldp transmitter and receiver enabled, dflt
      [txonly] lldp transmitter is enabled
-p     port list, [pList]: {F1,F2,1..4}
-proto protocol configuration, [pMode]: {discard, peer, tunnel}
      [discard] LLDP is disabled, LLDP frames are discarded
      [peer] LLDP is enabled and protocol is operating
      [tunnel] LLDP is disabled, LLDP frames are tunneled
-s     show current configuration
-tlv  optional TLVs to send: {mgt,pdes,sysname,sysdes,syscap}
      [mgt] management address, dflt enable
      [pdes] port description, same as Port Name, dflt enable
      [sysname] system name, same as sysName object, dflt enable
      [sysdes] system description, same as sysDescr object, dflt enable
      [syscap] system capabilities, dflt enable
-txfin fast message transmission interval in sec, [tSec]: {1..3600}, dflt 1
-txhld multiplier of txrate for TTL value in PDU, [tVal]: {2..10}, dflt 4
-txrt  lldp normal transmission interval in sec, [tSec]: {5..32768}, dflt 30

>
```

**NOTE: Port number selection will vary depending on the model.**

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

The *-dall* switch deletes all LLDP configuration settings.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

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

The *-p* switch associates the port with the LLDP port instance.

The *-proto* switch selects how LLDP PDUs are processed; discard, peer or tunnel.

- peer*        The port will participate in the LLDP process.
- discard*    LLDP frames are dropped and no reply is generated.
- tunnel*     LLDP frames will egress other tunnel ports unchanged.

The *-s* switch displays the current LLDP status.

The *-tlv* switch selects which optional TLVs to include in the transmit LLDP PDUs

- 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

The *-txfin* switch 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* switch 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* switch configures the transmission frequency of LLDP updates in seconds. The range is 5 to 65,534 seconds and the default is 30 seconds.

#### NOTES:

**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.**

Use the *lldp -s* command to display the LLDP status.

```
> lldp -s

LLDP configuration:
Normal transmission interval: 30s
TTL value multiplier: 4
Fast LLDP transmission interval: 1s
Number of fast LLDP messages: 4
Reinitialization delay: 1 sec
Capabilities supported: bridge, CVLAN, SVLAN
Capabilities enabled: bridge, CVLAN, SVLAN
Number of times table data inserted: 1
Number of times table data deleted: 0
Number of times table data dropped: 0
Number of times table data aged out: 0
```

Port F1 Info:

LLDP Protocol: Peer  
LLDP Mode: Receive and Transmit Enabled  
LLDP TLVs included: mgt, pdes, sysname, sysdes, syscap  
LLDP Status: LLDP PDUs are not being received  
LLDP PDUs transmitted: 0  
LLDP PDUs received: 0  
LLDP PDUs discarded: 0  
LLDP Port TLVs discarded: 0  
LLDP Port TLVs unrecognized received: 0  
LLDP Port Age Outs: 0

Port F2 Info:

LLDP Protocol: Peer  
LLDP Mode: Receive and Transmit Enabled  
LLDP TLVs included: mgt, pdes, sysname, sysdes, syscap  
LLDP Status: LLDP PDUs are being received  
LLDP PDUs transmitted: 11  
LLDP PDUs received: 1  
LLDP PDUs discarded: 0  
LLDP Port TLVs discarded: 0  
LLDP Port TLVs unrecognized received: 0  
LLDP Port Age Outs: 0

For remote MAC address 00:06:87:02:13:f0:

ChassisID: mac 00:06:87:02:13:f0  
Port ID: component 1  
Time to Live: 120  
Port Description: Port 1  
System Name: XM5  
System Description: 9600-40-B1 v5.3.6 s/n 00713365  
Capabilities: Bridge  
Capabilities enabled: Bridge  
Management Address: IPv4 - 192.168.1.100  
Management Address: IPv6 - fe80:2::206:87ff:fe02:13f0

Port 1 Info:

LLDP Protocol: Peer  
LLDP Mode: Receive and Transmit Enabled  
LLDP TLVs included: mgt, pdes, sysname, sysdes, syscap  
LLDP Status: LLDP PDUs are not being received  
LLDP PDUs transmitted: 0  
LLDP PDUs received: 0  
LLDP PDUs discarded: 0  
LLDP Port TLVs discarded: 0  
LLDP Port TLVs unrecognized received: 0  
LLDP Port Age Outs: 0

Port 2 Info:

LLDP Protocol: Peer  
LLDP Mode: Receive and Transmit Enabled  
LLDP TLVs included: mgt, pdes, sysname, sysdes, syscap  
LLDP Status: LLDP PDUs are not being received  
LLDP PDUs transmitted: 7805  
LLDP PDUs received: 0  
LLDP PDUs discarded: 0  
LLDP Port TLVs discarded: 0  
LLDP Port TLVs unrecognized received: 0  
LLDP Port Age Outs: 0

```
Port 3 Info:
  LLDP Protocol: Peer
  LLDP Mode: Receive and Transmit Enabled
  LLDP TLVs included: mgt, pdes, sysname, sysdes, syscap
  LLDP Status: LLDP PDUs are not being received
  LLDP PDUs transmitted: 0
  LLDP PDUs received: 0
  LLDP PDUs discarded: 0
  LLDP Port TLVs discarded: 0
  LLDP Port TLVs unrecognized received: 0
  LLDP Port Age Outs: 0
```

```
Port 4 Info:
  LLDP Protocol: Peer
  LLDP Mode: Receive and Transmit Enabled
  LLDP TLVs included: mgt, pdes, sysname, sysdes, syscap
  LLDP Status: LLDP PDUs are not being received
  LLDP PDUs transmitted: 0
  LLDP PDUs received: 0
  LLDP PDUs discarded: 0
  LLDP Port TLVs discarded: 0
  LLDP Port TLVs unrecognized received: 0
  LLDP Port Age Outs: 0
```

>

To tunnel LLDP on all ports, use the *lldp -proto tunnel -p all*.

```
LLDP configuration:
Normal transmission interval: 30s
TTL value multiplier: 4
Fast LLDP transmission interval: 1s
Number of fast LLDP messages: 4
Reinitialization delay: 1 sec
Capabilities supported: Bridge, CVLAN, SVLAN
Capabilities enabled: Bridge, CVLAN, SVLAN
Number of times table data inserted: 0
Number of times table data deleted: 0
Number of times table data dropped: 0
Number of times table data aged out: 0
```

```
Port F1 Info:
  LLDP Protocol: Tunnel
```

```
Port F2 Info:
  LLDP Protocol: Tunnel
```

```
Port 1 Info:
  LLDP Protocol: Tunnel
```

```
Port 2 Info:
  LLDP Protocol: Tunnel
```

```
Port 3 Info:
  LLDP Protocol: Tunnel
```

```
Port 4 Info:
  LLDP Protocol: Tunnel
```

## 2.1.14 Physical Location (LOCATION)

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

To configure the location of the module, use the *location* option from the CLI prompt. A list of options is displayed when the *location -h* command is entered.

```
> location -h

Description:
  location - location configuration
Syntax:
  location [-h]
  location -s
  location [-addr mAddr] [-city mCity] [-state mState] [-post mPost]
           [-lat mLat] [-long mLong] [-alt mAlt]
  location -dall
Switches:
-addr  address, [mAddr]: 1-32 ASCII characters, dflt blank
-alt   altitude, [mAlt]: 1-16 characters, dflt blank
-city  city, [mCity]: 1-32 ASCII characters, dflt blank
-dall  delete all 'location' configured settings and restore defaults
-h     display help information
-lat   latitude, [mLat]: {-90.000000..90.000000}, dflt blank
-long  longitude, [mLong]: {-180.000000..180.000000}, dflt blank
-post  postal code/zipcode, [mPost]: 1-16 ASCII characters, dflt blank
-s     shows current configuration
-state state/province, [mState]: 1-32 ASCII characters, dflt blank

>
```

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

The *-addr* switch configures the physical module address.

The *-alt* switch configures the module altitude for above or below sea level.

The *-city* switch configures the city.

The *-dall* switch deletes all location settings and restores factory defaults.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

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

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

The *-post* switch configures the postal zone or zip code.

The *-s* switch displays the location settings for the module.

The *-state* switch configures the state.

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

```
> location -addr "38 Tesla" -city Irvine -state California -post 92618
> location -s

Address          38 Tesla
City             Irvine
State/province   California
Postal/zipcode   92618
Latitude
Longitude
Altitude

>
```

**NOTE:** 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*).

### 2.1.15 Link Redundancy (LR)

**Link Redundancy is only supported on models with 2 fiber or copper uplink ports.**

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.

To configure link redundancy, use the *lr* option from the CLI prompt. A list of options is displayed when the *lr -h* command is entered.

```
> lr -h

Description:
  lr - link redundancy configuration
Syntax:
  lr [-h]
  lr -s
  lr [-ena|-dis] [-noret|-ret]
  lr -dall
Switches:
-dall  delete all 'lr' configured settings and restore defaults
-dis   disable link redundancy, dflt
-ena   enable link redundancy
-h     display help information
-noret no return to working port
-ret   return to working port, dflt
-s     show current configuration

>
```

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

The *-dall* switch deletes all link redundancy configuration settings and restores factory defaults.

The *-dis* and *-ena* switches disable/enable link redundancy.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-noret* switch disables the return to the primary link when the link failure has been resolved.

The *-ret* switch enables the return to the primary link when the link failure has been resolved.

The *-s* switch displays the current configuration.

Use the *lr -s* command to display the link redundancy configuration.

```
> lr -s

Link redundancy: disabled
Return to primary: disabled

Working port: F1
  Status: not available
  Link: not linked

Protection port: F2
  Status: not available
  Link: not linked

>
```

To enable link redundancy and configure the link not to return to the primary link when the link failure has been fixed, use the *lr -ena -noret* command.

```
> lr -ena -noret
```

**NOTE: To enable link redundancy using the CLI, the on-board DIP switches must be disabled. Use the *module -dis dipsw* command to disable the DIP-switches.**

Use the *lr -s* command to display the link redundancy configuration.

```
> lr -s

Link redundancy: enabled
Return to primary: disabled

Working port: F1
  Status: not available
  Link: not linked

Protection port: F2
  Status: not available
  Link: not linked

>
```

## 2.1.16 MAC Table (MACTABLE)

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.

To display the MAC addresses, use the *mactable-s* command from the CLI prompt. A list of options is displayed when the *mactable -h* command is entered.

```
> mactable

Description:
  mactable - mac table status
Syntax:
  mactable [-h]
  mactable -s [-ver] [-p pNum]
  mactable -clr
  mactable [-aging ageTime] [-add macAddress -p pList [-vid vlan]]
             [-del macAddress] [{-dis|-ena} {learning|port}]
  mactable -dall
Switches:
-add      add static MAC address, [macAddress]
-aging    mac table aging time in sec, [ageTime]: {10..600} dflt 300
-clr      clear (flushes) the learned MAC addresses
-del      delete static MAC address, [macAddress]
-dall     delete all MAC configured settings, instances, and restore defaults
-dis      disable function: {learning|port}
-ena      enable function: {learning|port}
           [learning] global MAC learning, dflt enable
           [port] clear MAC table when any port link down, dflt enable
-h        display help information
-p        port number, [pNum|pList]: {F1|F2|1..4|L1..L8|all}
           adding a unicast static address is only a single port
           adding a multicast static address can be more than one port
-s        show current status
-ver      verbose show
-vid      trunk VLAN ID, [vlan]: {0..4095}

>
```

**NOTE: Port number selection will vary depending on the model.**

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

The *-add* switch allows the configuration of static MAC address to the MAC table.

The *-aging* switch defines the time before a MAC address expires. The default value is 300 seconds.

The *-clr* switch clears the learned MAC addresses.

The *-del* switch allows the deletion of static MAC address from the MAC table.

The *-dis* and *-ena* switches disable and enable global MAC learning and clearing the MAC table when the link is down.

*learning* Enables or disables MAC learning globally on the module.

*port* Enables or disables the clearing of the MAC table when any port link down.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-p* switch selects the port number.

The *-s* switch displays the MAC table.

The *-ver* switch displays the extended show.

The *-vid* switch selects the VLAN ID associated with a MAC entry for a trunk port.

To display the learned MAC addresses on the module, use the *mactable -s* command.

```
> mactable -s

MAC aging = 300s
MAC learning = enabled
MAC flush on link down = enabled

Retrieving MAC Table information - please wait

  [0001] 00-06-87-02-cb-a0s  (M1/1);  [0002] 00-08-54-b3-70-48  (P4/1);

2 out of 8192 entries allocated

>
```

## 2.1.17 Multicast Listener Discovery (MLD)

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.

To configure MLD, use the *mld* command from the CLI prompt. A list of options is displayed when the *mld -h* command is entered.

```
> mld -h

Description:
  mld - multicast listener discovery configuration
Syntax:
  mld [-h]
  mld -s
  mld [-dis|-ena flood|snooping] [-to toVal]
  mld -a -vid vVid [-grp ipAddr -ph hnum -pr rnum [{-dis|ena} aging]]
  mld -d -vid vVid [-grp ipAddr]
  mld -m -vid vVid -grp ipAddr [-ph hnum] [-pr rnum] [{-dis|ena} aging]
  mld -dall
Switches:
-a      add manual forwarding map or MLD interface
-d      delete existing forwarding map or MLD interface
-dall   delete all MLD configured settings, instances, and restore defaults
-dis    disable function: {aging|flood|snooping}
-ena    enable function: {aging|flood|snooping}
        [aging] MLD route subject to aging out, dflt disable
        [flood] flooding of all unrecognized MLD groups, dflt disable
        [snooping] MLD snooping, dflt disable
-grp    MLD Group Address, [ipAddr]
-h      display help information
-m      modify existing forwarding map
-ph     host port [hnum]: {F1,F2,1..4}
-pr     router port [rnum]: {F1,F2,1..4}
-s      show current configuration
-to     MLD route aging in seconds, [toVal]: {0..65535}, dflt 60s
-vid    VLAN ID, [vVid]

>
```

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

The *-a* switch configures a forwarding map or MLD interface.

The *-d* switch deletes an existing forwarding map or MLD interface.

The *-dall* switch deletes all MLD configured settings and restores factory defaults.

The *-dis* switch disables MLD route aging, flooding all unrecognized MLD groups, and snooping.

The *-ena* switch enables MLD route aging, flooding all unrecognized MLD groups, and snooping.

The *-grp* switch configures the IP address of the MLD group.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-m* switch modifies an existing forwarding map.

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

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

The *-s* switch displays the status of the MLD configuration.

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

The *-vid* switch configures the VLAN ID associated with the MLD group.

**NOTE: 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.**

To display the status of the MLD configuration, use the *mld -s* command.

```
> mld -s

Snooping           Disabled
MLD Flooding       Disabled
Snooping timeout   60s

MLD VID Interfaces

>
```

## 2.1.18 Module Settings (MODULE)

The *module* command provides the ability to configure and display specific module settings. The serial interface baud rate, chassis name, module identifier, and enable/disable hardware DIP-switches can be configured using the *module* command.

To configure the module setting, use the *module* command from the CLI prompt. A list of options is displayed when the *module -h* command is entered.

```
> module -h

Description:
  module - module global configuration
Syntax:
  module [-h]
  module -s [all|led|env|mfg|mod]
  module [-bau baudRate] [-id modId]
         [-nm locationName] [-prmt pName] [-dis|-ena dipsw]
  module -dall
Switches:
-bau    serial port baud rate, [baudRate]: {1..9}, dflt 8
        1 = 300bps, 2 = 1200bps, 3 = 2400bps, 4 = 4800bps, 5 = 9600bps,
        6 = 19200bps, 7 = 38400bps, 8 = 57600bps, 9 = 115200bps
-dall   delete all 'module' configured settings and restore defaults
-dis    disable function: {dipsw}
-ena    enable function: {dipsw}
        [dipsw] DIP switch, dflt enable
-h      display help information
-id     module identification, [modId]: 1-255 ASCII characters
-nm     location name, [locationName]: 1-255 ASCII characters
-prmt   prompt string, [pName]: 0 to 32 ASCII characters
-s      show current configuration: {all|led|env|mfg|mod}

>
```

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

The *-bau* switch configures the baud rate of the serial interface. The default rate is 57,600bps.

The *-dall* switch restores the factory defaults of all module setting.

The *-dis* switch disables the hardware DIP-switches and allows CLI commands to override the functions.

The *-ena* switch enables the hardware DIP-switches and prevents the CLI commands from overriding the functions.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-id* switch configures the module identifier. The module identifier can be any 1-255 alphanumeric character string.

The *-nm* switch configures the chassis name. The chassis name can be any 1-255 alphanumeric character string.

The *-prmt* switch configures the name associated with the module prompt.

The *-s* switch displays the module global configuration. Specific parameter can be displayed using the *all*, *led*, *env*, *mfg* or *mod* command.

*all*            Displays all the information on the module. Default if no option is specified.

*led*            Displays the status of the LEDs on the module.

- env* Displays the voltage and temperature parameters.
- mfg* Displays the manufacturing information.
- mod* Displays the module specific information.

To display the status of the LED on the module, use the *module -s led* command.

```
> module -s led

1: Power Supply A      = Grn
2: Power Supply B      = Grn
3: Port F1 100+10      = Off
4: Port F1 1000+10     = Amb, 1Hz
5: Port F2 100+10      = Off
6: Port F2 1000+10     = Grn
7: Port 1 100+10       = Grn
8: Port 1 1000+10      = Off
9: Port 1 PSE Act      = Grn, 1Hz
10: Port 2 100+10      = Grn
11: Port 2 1000+10     = Off
12: Port 2 PSE Act     = Grn
13: Port 3 100+10      = Grn
14: Port 3 1000+10     = Off
15: Port 3 PSE Act     = Grn
16: Port 4 100+10      = Off
17: Port 4 1000+10     = Grn
18: Port 4 PSE Act     = Off
```

**NOTE:** The *module -s led* display will vary depending on the model.

To display all the information about the module, use the *module -s all* command.

```
> module -s all

1: Power Supply A      = Grn
2: Power Supply B      = Grn
3: Port F1 100+10      = Off
4: Port F1 1000+10     = Amb, 1Hz
5: Port F2 100+10      = Off
6: Port F2 1000+10     = Grn
7: Port 1 100+10       = Grn
8: Port 1 1000+10      = Off
9: Port 1 PSE Act      = Grn, 1Hz
10: Port 2 100+10      = Grn
11: Port 2 1000+10     = Off
12: Port 2 PSE Act     = Grn
13: Port 3 100+10      = Grn
14: Port 3 1000+10     = Off
15: Port 3 PSE Act     = Grn
16: Port 4 100+10      = Off
17: Port 4 1000+10     = Grn
18: Port 4 PSE Act     = Off

Model Number: 3319-0-24-2
Serial Number: 20180791
Manufacturing Date: 20180710
Product Revision: 10
Software Revision: v2.x.x

Voltage In PS A: 54.23V
Voltage In PS B: 53.80V
Voltage Out: 3.31V
Total Current: 260mA
Temperature: 51C
CPU Utilization: 12%
RAM Utilization: 44.2MB out of 509MB (8.7%)
Flash Utilization: 204.9MB out of 798MB (25.7%)

Module Type: RuggedNet GHPoE/Mi
Module Identification:
Location Name: GHPoE/Mi
DIP switches: Disabled
Baud rate: 57600 baud
```

To display the environmental information about the module, use the *module -s env* command.

```
> module -s env

Voltage In PS A: 54.67V
Voltage In PS B: 0.00V
Voltage Out: 3.26V
Total Current: 52mA
Temperature: 39C
CPU Utilization: 8%
RAM Utilization: 75.6MB out of 507MB (14.9%)
Flash Utilization: 135.1MB out of 448MB (30.1%)
```

**NOTE:** The *module -s env* display will vary depending on the model.

**When the temperature of the module is less than 0 degrees C, the module temperature reading will display 0 degrees C.**

### **2.1.19 Media Redundancy Protocol (MRP)**

IEC 62439-2 defines Media Redundancy Protocol (MRP) as a ring protocol that is used in high availability industrial networks. MRP is implemented as a ring protocol similar to Ethernet Ring Protocol Switch (ERPS), which allows the ring to recover from a single failure.

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.

To configure MRP, use the *mrp* command from the CLI prompt. A list of options is displayed when the *mrp -h* command is entered.

```
> mrp -h

Description:
  mrp - media redundancy protocol (MRP) configuration
Syntax:
  mrp [-h]
  mrp -s
  mrp {-dis|-ena} mrp
  mrp -p pList {-dis|-ena} {mrp|port}
  mrp -a -pn pName -rp1 pNum -rp2 pNum -role mRole [-dom dId]
      [-pri priNum] [-rec sTime] [-vid vlanId]
  mrp -m -pn pName [-rp1 pNum] [-rp2 pNum] [-role mRole] [-dom dId]
      [-pri priNum] [-rec sTime] [-vid vlanId]
  mrp -d -pn pName
  mrp -dall
Switches:
-a      add MRP instance
-d      delete MRP instance
-dall   delete all MRP configured settings, instances, and restore defaults
-dis    disable function: {mrp|port}
        [mrp] global or port MRP, dflt disabled
        [port] forwarding MRP, dflt enabled
-dom    ring domain id, [dId]: 32 hexadecimal characters
-ena    enable function: {mrp|port}
        [mrp] global or port MRP, dflt disabled
        [port] forwarding MRP, dflt enabled
-h      display help information
-m      modify existing MRP profile
-p      port list, [pList]: {F1,F2,1..4}
-pn     MRP profile name, [pName]: 1 to 32 ASCII characters
-pri    ring priority, [priNum]: {0..65535}, dflt 40960
-rec    recovery time, [rTime]: {200|500}, dflt 200
-role   role, [mRole]: {mrc|mrm}
-rp1    ring port 1, [pNum]: {F1,F2,1..4}
-rp2    ring port 2, [pNum]: {F1,F2,1..4}
-s      shows current configuration
-vid    MRP vlan id assignment, [vlanId]: {1..4095}, dflt 1

>
```

**NOTE: Port number selection will vary depending on the model.**

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

The *-a* switch adds a new MRP instance. If the ring ports associated with the add command are not MRP ports or are already allocated to another instance, an error message of *rpx port x is not a MRP port* or *rpx port x is already a part of an MRP instance* will be displayed

The *-d* switch deletes an existing MRP instance.

The *-dis* switch disables one of the following functions:

- mrp* Globally disables MRP if not associated with a port.
- mrp* Disables a port from being on a MRP ring if associated with a port.  
A port cannot be removed from being an MRP port unless the MRP instance is first deleted and generates an error if attempted.
- port* Disables forwarding of all frames on a port (not participating in normal MRP operations).

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

The *-ena* switch enables one of the following functions:

- mrp* Globally enables MRP if not associated with a port.
- mrp* Enables a port as a MRP ring port if associated with a port.
- port* Enables normal MRP operations on a port when associated with an MRP instance.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-m* switch modifies an existing MRP instance.

The *-p* switch selects one or more port numbers associated MRP or a MRP instance.

The *-pn* switch sets the MRP profile instance name.

The *-pri* switch sets the MRP instance priority for the manager.

The *-rec* switch sets the MRP maximum recovery time.

The *-role* switch sets the MRP role for the module: MRC or MRM.

- mrc* Media redundancy client.
- mrm* Media redundancy manager.

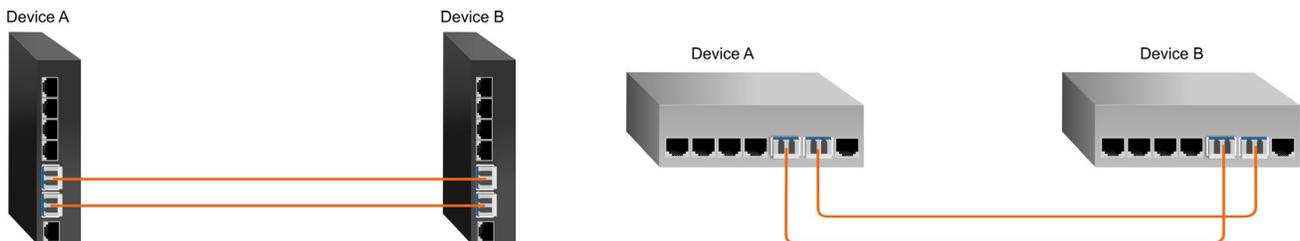
The *-rp1* switch configures the port number for Ring Port 1.

The *-rp2* switch configures the port number for Ring Port 2.

The *-s* switch displays configured settings.

The *-vid* switch selects the VLAN MRP protocol Identification.

The following script is an example of a MRP configuration.



## Device A Setup

Device A (Media Redundancy Manager)
<b>CLI Command</b>
> vlan -rem 2..4095 > vlan -add 2
> switchport -p f1 -vid 2 > switchport -p f2 -vid 2 > switchport -p 2 -vid 2 > switchport -p f1 -mode tunnel > switchport -p f2 -mode tunnel > switchport -p 2 -mode tunnel
> mrp -dis mrp > mrp -p f1,f2 -ena mrp > mrp -a -pn M1 -rp1 f1 -rp2 f2 -role mrm -pri 20000 -rec 200 -vid 2 -dom FFFFFFFF-FFFF-FFFF-FFFF-000000000001 > mrp -ena mrp

Module is configured as the Media Redundancy Manager (MRM)

## Device B Setup

Device B (Media Redundancy Client)
<b>CLI Command</b>
> vlan -rem 2..4095 > vlan -add 2
> switchport -p f1 -vid 2 > switchport -p f2 -vid 2 > switchport -p 2 -vid 2 > switchport -p f1 -mode tunnel > switchport -p f2 -mode tunnel > switchport -p 2 -mode tunnel
> mrp -dis mrp > mrp -p f1,f2 -ena mrp > mrp -a -pn C1 -rp1 f1 -rp2 f2 -role mrc -rec 200 -vid 2 -dom FFFFFFFF-FFFF-FFFF-FFFF-000000000001 > mrp -ena mrp

Module is configured as the Media Redundancy Client (MRC)

## Device A - MRM

```
> mrp -s

MRP                               enabled
MRP associated ports              F1,F2

MRP instance 1 "M1"
  Role                            manager
  Recovery time (ms)              200

  Priority                         20000
  Domain ID                       FFFFFFFF-FFFF-FFFF-FFFF-000000000001
  Ring port 1                      F1
  Ring port 2                      F2
  VLAN ID                          2

  Ring status                       closed
  Ring port 1 status                blocking
  Ring port 2 status                forwarding

  Topology change request interval (ms)  10
  Topology change repeat count           3
  Short test frame interval (ms)         10
  Default test frame interval (ms)       20
  Test monitoring interval count          3

>
```

Ring Port 1 status is indicating the port is blocked and Ring Port 2 status is indicating the port is forwarding traffic.

## Device B - MRC

```
> mrp -s

MRP                               enabled
MRP associated ports              F1,F2

MRP instance 1 "M1"
  Role                            client
  Recovery time (ms)              200

  Domain ID                       FFFFFFFF-FFFF-FFFF-FFFF-000000000001
  Ring port 1                      F1
  Ring port 2                      F2
  VLAN ID                          2

  Ring status                       n/a
  Ring port 1 status                forwarding
  Ring port 2 status                forwarding

  Link down timer interval (ms)        20
  Link up timer interval (ms)          20
  Link change (up or down) count (ms)  4

>
```

Ring Port 1 status and Ring Port 2 status is indicating the port is forwarding traffic.

### 2.1.20 Nest (NEST)

The *nest* command provides the ability to access the hierarchical commands.

To access the hierarchical command line interface, use the *nest* command from the CLI prompt. A list of options is displayed when the *nest -h* command is entered.

```
> nest -h

Description:
  nest - hierarchical CLI session
Syntax:
  nest
  nest -h
Switches:
-h      display help information

>
```

To access the hierarchical interface, enter *nest* at the > prompt.

```
> nest
Nesting level change accepted

#
```

For more information on the hierarchical command line interface, see the

For information on the hierarchical command line interface, see Hierarchical CLI OmniConverter and RuggedNet switches User Manual (3xxxUM-03).

### 2.1.21 Ping (PING)

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.

To configure ping, use the *ping* command from the CLI prompt. A list of options is displayed when the *ping -h* command is entered.

```
> ping -h

Description:
  ping - ping a remote device
Syntax:
  ping [-h]
  ping [-t] ipAddress [-n count] [-l size] [-to tCount] [-ttl count]
Switches:
-h      display help information
-l      transmit buffer in bytes, [size]: {0..1472}, dflt 32
-n      number of pings, [count]: {0..65536}, dflt 3
-t      ping the specified [ipAddress]
-to     timeout in seconds to wait for each reply, [tCount]: {1..30}, dflt 3
-ttl    time to live, [count]: {1..255}, dflt 64

>
```

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

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-l* switch defines the size of the ping frame.

The *-n* switch defines the number of pings frames sent. A value of 0 sends pings until interrupted.

The *-t* switch defines the destination IP address.

The *-to* switch configures the time to wait for each reply.

The *-ttl* switch configures the time to live value.

To ping an IP address, use the *ping -t* command.

```
> 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

>
```

## 2.1.22 Port Attribute (PORT)

The *port* command provides the ability to configure each port with specific parameters.

To configure the attributes of a port, use the *port* command from the CLI prompt. A list of options is displayed when the *port -h* command is entered.

```
> port -h

Description:
  port - port attribute configuration
Syntax:
  port [-h]
  port -s [-p pList]
  port -dall
  port -p pList [-n portName] [-mo pMode] [-loopt lTime]
      [{-dis|-ena} flow|learning|loop|mirror[,sp]|port|secure]
Switches:
-dall  delete configured port attribute settings and restore defaults
-dis   disable function: {flow|learning|loop|mirror|port|secure}
-ena   enable function: {flow|learning|loop|mirror,sp|port|secure}
      [flow] flow control, dflt disable
      [learning] MAC learning, dflt enable
      [loop] loop protection, dflt disable
      [mirror] mirror source port, [sp], dflt disable
      [port] port output, dflt enable
      [secure] drops unknown Multicast/Unicast addresses, dflt disable
-h     display help information
-loopt loop protection transmit interval in sec, [lTime]: {1..60}, dflt 1
-mo    port mode, [pMode]: [{1000|100|10},]{an|man}[,{fdx|hdx}]
-n     port name, [portName]: 1-45 ASCII characters
-p     port list, [pList]: {F1,F2,1..4,mgt1|all}
-s     shows current configuration

>
```

**NOTE: Port number selection will vary depending on the model.**

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

The *-dall* switch deletes all configured port attributes and restores factory default settings.

The *-dis* and *-ena* switches disable or enable the following:

- flow* Disables or enables flow control on a port on the module.
- learning* Disables or enables MAC learning on a port on the module.
- loop* Disables or enables loop protection on a port on the module.
- mirror* Disables or enables port mirroring on the module.
- port* Disables or enables a port on the module.
- secure* Disables or enables the ability to drop unknown Multicast/Unicast addresses on a port on the module.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

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

The *-mo* switch defines configuration of the negotiation, speed and duplex for the RJ-45 copper port.

The *-n* switch defines the name for the selected port.

The *-p* switch defines the port on the module to be used when configuring the attributes.

The *-s* switch displays the attributes associated with each port on the module.

The *-mo* switch provides configuration of the fixed RJ-45 port. The *-mo* switch is a valid switch to configure the fiber ports for AN or MAN only.

The RJ-45 port will operate per the Port Configuration Matrix below.

Port Attribute -mo setting	Port Configuration	RJ-45 Mode of Operation
1000, an, fdx	Based on the link partner	The RJ-45 port is set to auto-negotiation with the following modes advertised: 1000FDX, 1000HDX, 100FDX, 100HDX, 10FDX, 10HDX
1000, an, hdx	Based on the link partner	The RJ-45 port is set to auto-negotiation with the following modes advertised: 1000HDX, 100FDX, 100HDX, 10FDX, 10HDX
100, an, fdx	Based on the link partner	The RJ-45 port is set to auto-negotiation with the following modes advertised: 100FDX, 100HDX, 10FDX, 10HDX
100, an, hdx	Based on the link partner	The RJ-45 port is set to auto-negotiation with the following modes advertised: 100HDX, 10FDX, 10HDX
10, an, fdx	Based on the link partner	The RJ-45 port is set to auto-negotiation with the following modes advertised: 10FDX, 10HDX
10, an, hdx	Based on the link partner	The RJ-45 port is set to auto-negotiation and advertises: 10HDX
1000, man, fdx	Based on the link partner	The RJ-45 port is set to auto-negotiation with the following modes advertised: 1000FDX (When set to 1000, the port is always in AN mode)
1000, man, hdx	Based on the link partner	The RJ-45 port is set to auto-negotiation with the following modes advertised: 1000HDX (When set to 1000, the port is always in AN mode)
100, man, fdx	Man, 100, FDX	The RJ-45 port is set to manual negotiation and is forced to: 100FDX
100, man, hdx	Man, 100, HDX	The RJ-45 port is set to manual negotiation and is forced to: 100HDX
10, man, fdx	Man, 10, FDX	The RJ-45 port is set to manual negotiation and is forced to: 10FDX
10, man, hdx	Man, 10, HDX	The RJ-45 port is set to manual negotiation and is forced to: 10HDX

*RJ-45 Port Configuration Matrix*

**NOTE: 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 per the table above.**

The 1G fiber port will operate per the Port Configuration Matrix below.

Port Attribute -mo setting	Port Configuration	Mode of Operation
an	AN, 1000, FDX	1000M Fiber port set to AN with the followings mode advertised 1000FDX
man	Man, 1000, FDX	1000M Fiber port set to MAN and is forced to 1000FDX

*1G Fiber Port Configuration Matrix*

10G SFP+ ports are set to full duplex, manual operation.

When loop protection is enabled on a port (*-ena loop -p x*), 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 (*-ena secure -p x*), the port will dropped all unknown Unicast and Multicast addresses. When port security is disabled, frames with unknown Unicast and Multicast addresses will be able to transmitted based on VLAN forwarding and learned MAC address forwarding rules.

To configure Port 3 (RJ-45) for 100M FDX manual operation, use the *-mo* command.

```
> port -p 3 -mo 100,man,fdx
```

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

```
> port -p F1 -mo man
```

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

```
> port -p 1 -ena mirror,2
```

To display the port attributes, use the *port -s* command.

```
> port -s

Port F1 is named "Port F1", MTU 10240 bytes
  Port mode is SFP: Copper 1000, AN, FDX (No link)
  Port flow control is disabled
  Port output is enabled
  MAC learning is enabled: active
  Port mirroring is disabled
  Port security is disabled
  Loop protection is disabled
  Loop protection transmit interval is 1 sec
  Loop protection type: none
Port F2 is named "Port F2", MTU 10240 bytes
  Port mode is SFP: Fiber 1000, AN, FDX (No link)
  Port flow control is disabled
  Port output is enabled
  MAC learning is enabled: active
  Port mirroring is disabled
  Port security is disabled
  Loop protection is disabled
  Loop protection transmit interval is 1 sec
  Loop protection type: none
Port 1 is named "Port 1", MTU 10240 bytes
  Port mode is UTP: 1000, AN, FDX (Linked: 1000,FDX,no flow)
  Port flow control is disabled
  Port output is enabled
  MAC learning is enabled: active
  Port mirroring is disabled
  Port security is disabled
  Loop protection is disabled
  Loop protection transmit interval is 1 sec
  Loop protection type: none
```

```

Port 2 is named "Port 2", MTU 10240 bytes
  Port mode is UTP: 1000, AN, FDX (Linked: 1000,FDX,no flow)
  Port flow control is disabled
  Port output is enabled
  MAC learning is enabled: active
  Port mirroring is disabled
  Port security is disabled
  Loop protection is disabled
  Loop protection transmit interval: 1
  Loop protection type: none
Port 3 is named "Port 3", MTU 10240 bytes
  Port mode is UTP: 1000, AN, FDX (No link)
  Port flow control is disabled
  Port output is enabled
  MAC learning is enabled: active
  Port mirroring is disabled
  Port security is disabled
Port 4 is named "Port 4", MTU 10240 bytes
  Port mode is UTP: 1000, AN, FDX (Linked: 100,FDX,no flow)
  Port flow control is disabled
  Port output is enabled
  MAC learning is enabled: active
  Port mirroring is disabled
  Port security is disabled
  Loop protection is disabled
  Loop protection transmit interval: 1
  Loop protection type: none
Management port 1 is named "Mgt1", MTU 1518 bytes

```

### 2.1.23 Port Access (PORTACCESS)

The *portaccess* command provides the ability to control data access to each port on the module. Port Access can be configured to block (Off) user access or enable (On) user access. Port Access enables an administrator to control user access while maintaining port configuration for easy disabling or enabling of customer service.

To configure port access, use the *portaccess* command from the CLI prompt. A list of options is displayed when the *portaccess -h* command is entered.

```

> portaccess -h

Description:
  portaccess - port access configuration
Syntax:
  portaccess [-h]
  portaccess -s
  portaccess {-ena|-dis} -p pList
  portaccess -dall
Switches:
-dall  delete all 'portaccess' configured settings and restore defaults
-dis   disable port access
-ena   enable port access
-h     display help information
-p     port list, [pList]: {F1,F2,1..4|all}
-s     shows the port access configuration

>

```

**NOTE: Port number selection will vary depending on the model.**

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

The *-dis* switch disables access to the selected port.

The *-ena* switch enables access to the selected port.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-p* switch selects the port to be enabled or disabled. The default setting is all.

The *-s* switch displays the port access configuration.

To disable Port 2, use the *portaccess -dis -p 2* command.

```
> portaccess -dis -p 2
```

To display the port access configuration, use the *portaccess -s* command.

```
> portaccess -s  
  
Port F1 enabled  
Port F2 enabled  
Port 1 enabled  
Port 2 disabled  
Port 3 enabled  
Port 4 enabled
```

#### 2.1.24 Port Statistics (PORTSTAT)

The *portstat* command provides the ability to display the port statistics on the module.

To display the port statistics, use the *portstat* command from the CLI prompt. A list of options is displayed when the *portstat -h* command is entered.

```
> portstat -h  
  
Description:  
  portstat - port statistic configuration  
Syntax:  
  portstat [-h]  
  portstat -s -p pNum  
  portstat -clr -p pNum  
Switches:  
-clr  clear port statistics  
-h    display help information  
-p    port number, [pNum]: {F1,F2,1..4|mgt1|all}  
-s    shows current status  
  
>
```

**NOTE: Port number selection will vary depending on the model.**

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

The *-clr* switch clears the current port statistics.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-p* switch selects which port statistic is displayed.

The *-s* switch displays the selected port statistics.

To display the port statistics for Fiber Port 1, use the `portstat -s -p fl` command.

```
> portstat -s -p fl

Transmission Counters                                Receive Counters
Packets                                              2367
Total Octets          715116                        Total Octets          639052
Good Pkts             1766                          Good Pkts             2367
Pause Pkts            0                            Pause Pkts            0
Unicast Pkts         1404                          Unicast Pkts         1346
Multicast Pkts       362                          Multicast Pkts       625
Broadcast Pkts       0                            Broadcast Pkts       396
Errored Pkts         0                            Errored Pkts         0
Dropped Pkts         0                            Dropped Pkts         0
Bad Events           0                            FCS Errors           0
Deferred             0                            Symbol Errors        0
Collisions:
  Total              0                            CRC/Alignment        0
  Single             0                            Undersized           0
  Multiple           0                            Oversized            0
  Late               0                            Fragments            0
  Excessive          0                            Jabber               0
  Alignment          0                            Alignment            0

Transmit Packets by Queue                          Receive Packets by Size
Queue 0          1766                             64 Octets         481
Queue 1           0                             65-127            499
Queue 2           0                             128-255           584
Queue 3           0                             256-511           17
Queue 4           0                             512-1023          786
Queue 5           0                             1024-10240        0
Queue 6           0
Queue 7           0

Tx Throughput          0.024 Mbps      Rx Throughput          0.024 Mbps
Tx Utilization         0.002%         Rx Utilization         0.002%

>
```

## 2.1.25 Protocol (PROTOCOL)

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.

To configure the protocols, use the *protocol* option from the CLI prompt. A list of options is displayed when the *protocol -h* command is entered.

```
> protocol -h

Description:
  protocol - protocol configuration
Syntax:
  protocol [-h]
  protocol -s
  protocol -ena|-dis {flow|ftp|http|https|ip|serial|telnet}
  protocol -cfn filename
  protocol -dall
Switches:
-cfn  SSL/TLS certificate file name, [filename]: 0 to 45 ASCII characters
-dall delete all 'protocol' configured settings and restore defaults
-dis  disable function: {flow|ftp|http|https|ip|serial|telnet}
-ena  enable function: {flow|ftp|http|https|ip|serial|telnet}
      [flow] flow control, dflt disabled
      [ftp] FTP protocol, dflt disabled
      [http] HTTP protocol (web page), dflt enabled
      [https] HTTPS protocol (web page), dflt enabled
      [ip] IP protocol, dflt enabled
      [serial] serial console port, dflt enabled
      [telnet] Telnet protocol, dflt enabled
-h    display help information
-s    show current configuration

>
```

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

The *-cfn* switch sets the SSL/TLS certificate file name for the product.

The *-dis* and *-ena* switches disables or enables the following:

- flow* Disables or enables global flow control on the module.
- ftp* Disables or enables FTP protocol on the module.
- http* Disables or enables HTTP protocol on the module.
- https* Disables or enables HTTPS protocol on the module.
- ip* Disables or enables IPv4 protocol on the module.
- serial* Disables or enables serial console port on the module.
- telnet* Disables or enables Telnet protocol on the module.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-s* switch displays the protocol configuration.

To enable FTP, use the following command.

```
> protocol -ena ftp
```

To disable Telnet, use the following command.

```
> protocol -dis telnet
```

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.

To display the configuration of the protocols, use the *protocol -s* command.

```
> protocol -s

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

>
```

### 2.1.26 Power Sourcing Equipment (PSE)

**Only supported on OmniConverter and RuggedNet PoE models.**

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

The PoE Scheduler provides the ability to configure the time and day for PoE power to be turned On and Off. Up to 100 scheduling events can be configured with a maximum of 8 per port.

To configure the power sourcing options on the RJ-45 ports for a PoE+ model, use the *pse* command from the CLI prompt. A list of options is displayed when the *pse -h* command is entered.

```
> pse -h

Description:
  pse - power source equipment configuration
Syntax:
  pse [-h]
  pse -s [-p pList]
  pse -p pList [-mode pMode] [-reset]
      [{-ena|-dis} {heartbeat|lldp-med|mdi-tlv}]
      [-i iTime] [-pderr eNum] [-hdfr iTime]
      [-pdint initNum] [-pdip ipAddr] [-pdm {restart|ignore|shutdown}]
  pse -a -p pList -sched onTime,offTime,sDays [{-ena|-dis} schedule] [-pn pName]
  pse -m -idx sIdx [-p pList] [-sched [onTime],[offTime],[sDays]] [-pn pName]
      [{-ena|-dis} schedule]
  pse {-ena|-dis} schedule
  pse -d -idx sIdx
  pse -dall
Switches:
-a      add a new PoE scheduler
-d      delete an existing PoE scheduler
-dall   delete all PSE configured settings, instances, and restore defaults
-dis    disable function: {heartbeat|lldp-med|mdi-tlv|schedule}
-ena    enable function: {heartbeat|lldp-med|mdi-tlv|schedule}
        [heartbeat] selects heartbeat ping, dflt disabled
        [lldp-med] selects LLDP-MED support for PoE PDs, dflt enabled
        [mdi-tlv] select IEEE MDI TLV support for PoE PDs, dflt enabled
        [schedule] selects scheduled on/off times, dflt enabled
-h      display help information
-hdfr   heartbeat restart defer in sec, [iTime]: {10..300}, dflt 60
-i      heartbeat interval in sec, [iTime]: {1..300}, dflt 1
-idx    PoE scheduler index
-m      modify existing PoE scheduler
-mode   pse mode, [pMode]: {af|at|off}
        [af] selects PSE enabled, advertising 802.3af
        [at] selects PSE enabled, advertising 802.3af/at, dflt
        [off] selects PSE disabled
-p      port list, [pList]: {1..4}
-pderr  number consecutive lost heartbeats for error, [eNum]: {1..100}, dflt 3
-pdint  number of times to restart PD after error, [initNum]: {0..16384}, dflt 0
        0 = no stop
-pdip   ip address of PD for heartbeat, [ipAddr]
-pdm    error mode action for PD error: {ignore|restart|shutdown}
        [ignore] no action when error condition is entered, dflt
        [restart] forces a power down and power up on the PSE ports
        [shutdown] shutdown PSE power for errored port
-pn     PoE scheduler profile name, [pName]: 1 to 32 ASCII characters
-reset  restart PoE power on selected ports
-s      show current configuration
-sched  schedule power on and off time, [onTime,offTime,sDays]
        [onTime] Time of day when power is enabled, in form of "24hr:min:sec"
        [offTime] Time of day when power is disabled in form of "24hr:min:sec"
        example "07:30:00,18:00:00"
        [sDays] Scheduler days, where the list contains one or more of:
        "Sun,Mon,Tue,Wed,Thu,Fri,Sat", separated by commas, dflt all days

>
```

**NOTE: Port number selection will vary depending on the model.**

To configure the power sourcing options on the RJ-45 ports for a HPoE or HPoEBT model, use the *pse* command from the CLI prompt. A list of options is displayed when the *pse -h* command is entered.

```

> pse -h

Description:
  pse - power source equipment configuration
Syntax:
  pse [-h]
  pse -s [-p pList]
  pse -p pList [-mode pMode] [-reset]
      [{-ena|-dis} {heartbeat|lldp-med|mdi-tlv}]
      [-i iTime] [-pderr eNum] [-hdfr iTime]
      [-pdint initNum] [-pdip ipAddr] [-pdm0 {restart|ignore|shutdown}]
  pse -a -p pList -sched onTime,offTime,sDays [{-ena|-dis} schedule] [-pn pName]
  pse -m -idx sIdx [-p pList] [-sched [onTime],[offTime],[sDays]] [-pn pName]
      [{-ena|-dis} schedule]
  pse {-ena|-dis} schedule
  pse -d -idx sIdx
  pse [{-ena|-dis} pslimit] [-pmax pwrMax]
  pse -dall
Switches:
-a      add a new PoE scheduler
-d      delete an existing PoE scheduler
-dall   delete all PSE configured settings, instances, and restore defaults
-dis    disable function: {heartbeat|lldp-med|mdi-tlv|pslimit|schedule}
-ena    enable function: {heartbeat|lldp-med|mdi-tlv|pslimit|schedule}
        [heartbeat] selects heartbeat ping, dflt disabled
        [lldp-med] selects LLDP-MED support for PoE PDs, dflt enabled
        [mdi-tlv] select IEEE MDI TLV support for PoE PDs, dflt enabled
        [pslimit] selects PSE availability, dflt enabled (global)
        [schedule] selects scheduled on/off times, dflt enabled
-h      display help information
-hdfr   heartbeat restart defer in sec, [iTime]: {10..300}, dflt 60
-i      heartbeat interval in sec, [iTime]: {1..300}, dflt 1
-idx    PoE scheduler index
-m      modify existing PoE scheduler
-mode   pse mode, [pMode]: {af|at|auto|force|off}
        [af] selects PSE enabled, advertising 802.3af
        [at] selects PSE enabled, advertising 802.3af/at
        [auto] selects PSE enabled, advertising max power possible, dflt
        [force] selects PSE enabled and supplying up to 100W of power
        [off] selects PSE disabled
-p      port list, [pList]: {1..4}
-pderr  number consecutive lost heartbeats for error, [eNum]: {1..100}, dflt 3
-pdint  number of times to restart PD after error, [initNum]: {0..16384}, dflt 0
        0 = no stop
-pdip   ip address of PD for heartbeat, [ipAddr]
-pdm0   error mode action for PD error: {ignore|restart|shutdown}
        [ignore] no action when error condition is entered, dflt
        [restart] forces a power down and power up on the PSE ports
        [shutdown] shutdown PSE power for errored port
-pmax   specifies maximum module PSE power (watts), [pwrMax]: {1..n}, dflt 125W
-pn     PoE scheduler profile name, [pName]: 1 to 32 ASCII characters
-reset  restart PoE power on selected ports
-s      show current configuration
-sched  schedule power on and off time, [onTime,offTime,sDays]
        [onTime] Time of day when power is enabled, in form of "24hr:min:sec"
        [offTime] Time of day when power is disabled in form of "24hr:min:sec"
            example "07:30:00,18:00:00"
        [sDays] Scheduler days, where the list contains one or more of:
            "Sun,Mon,Tue,Wed,Thu,Fri,Sat", separated by commas, dflt all days

```

**NOTE: Port number selection will vary depending on the model.**

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

The *-a* switch adds a new PoE scheduling profile.

The *-d* switch deletes an existing PoE scheduling profile.

The *-dis* and *-ena* switches disable or enable PSE functions on the module.

*heartbeat*      Disables/enables the heartbeat signal used to verify connectivity to the PD. *heartbeat* is disabled by default.

*lldp-med*      Disable/enables LLDP-MED support for PoE PDs.

*mdi-tlv*        Disables/enables IEEE MDI TLV support for PoE PDs.

***pslimit* is only available on OmniConverter and RuggedNet HPoE or HPoEBT models.**

*pslimit*        Disables/enables PSE power limit. When enabled the module will not allow a powered device(PD) to request/draw more than the module is capable of providing. The port will be limited to available PSE power.

*schedule*      Disables/enables PSE power scheduler. PoE power on each port can be enabled or disabled based upon the Time of Day. PoE power can be scheduled to be turned ON and OFF multiple times during the day.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-hdfr* switch selects the transmission interval delay before heartbeat pings are restarted after a reset.

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

The *-m* switch modifies an existing PoE schedule.

The *-mode* switch configures the power sourcing mode for the port. PoE power can be disabled, auto detect to 802.3af, auto detect to 802.3af/at, Forced ON or advertise max power.

*auto detect 802.3af*      Enables the PSE function and advertise 802.3af mode (15W).

*auto detect 802.3at*      Enable the PSE function and advertise 802.3af/at mode (30W).

***auto* is only available on OmniConverter and RuggedNet HPoE or HPoEBT models.**

*auto*              Enable the maximum PSE power per the negotiated class will be available. 802.3bt detection/negotiation supports classification up to class 8 devices.

***force* is only available on OmniConverter and RuggedNet HPoE or HPoEBT models.**

*force*             PSE power (60W or 100W depending on the model) is applied regardless of the advertised state of the PD. This feature allows interoperability with pre-802.3bt products.

*off*                Disables the PSE function.

The *-p* switch selects the port number.

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

The *-pdint* switch 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* switch configures the IP address of the PD. The IP address of the PD is used for the heartbeat signal.

The *-pdmo* switch configures what action is taken when a heartbeat error condition is detected.

*ignore* Indicates the error condition is ignored. *ignore* is the default setting.

*restart* Indicates the power to the selected port (PD) is cycled Off and On.

*shutdown* Indicates the power to the selected port (PD) is turned Off.

**The *pmax* is only available on OmniConverter and RuggedNet HPoE or HPoEBT models.**

The *-pmax* switch specifies the maximum PSE power for the module.

The *-pn* switch configures the name of the scheduling profile.

The *-reset* switch removes and reapplies power to the selected port.

The *-s* switch displays the PSE configuration.

The *-sched* switch sets the time when power is applied during the day and when the power is turned off for each port.

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

```
> pse -reset -p 1
```

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

```
> pse -a -sched "07:00:00,19:00:00" -p 1 -ena schedule
```

Use the *pse -s* command to display the PSE configuration. Only the status for Port 1 is shown.

```
> pse -s

Total power available: 125W
Total power supplied: 0.0000W
PSE power limit: enabled

Port 1 PSE status
  PSE port: enabled
  PSE port mode: auto
  LLDP-MED: enabled
  IEEE MDI TLV: enabled
  PD mode/status: not detected
  Voltage supplied: 0.00V
  Current supplied: 0.00mA

  Heartbeat: disabled
  Heartbeat IP address: 0.0.0.0
  Heartbeat interval: 1s
  Heartbeat detection: 3 lost responses
  Heartbeat error action: Ignore
  Heartbeat number of restarts: 0
  Heartbeat defer time after port restart: 60s
  Heartbeat status: Disabled

PoE Scheduler: Globally enabled
1, "", enabled, time on: 07:00:00 time off: 19:00:00 days: Sun,Mon,Tue,Wed,Thu,Fri,Sat
ports: 1
```

## 2.1.27 Restart (RESTART)

The *restart* command provide the ability to restart (warm boot) the module.

Use the *restart* option from the CLI prompt to restart the module. A list of options is displayed when the *restart -h* command is entered.

```
> restart -h

Description:
  restart - restart module
Syntax:
  restart [-h]
  restart -boot [-back]
Switches:
-back  reboot from backup application image
-boot  warm boot the module
-h     display help information

>
```

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

The *-back* switch makes the backup application image active.

The *-boot* switch performs a warm boot on the module.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

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
```

## 2.1.28 Restore to Factory Defaults (RESTORE)

The *restore* command provides the ability to restore the module to factory default settings.

Use the *restore* option from the CLI prompt to restore factory defaults. A list of options is displayed when the *restore -h* command is entered.

```
> restore -h

Description:
  restore - restore module defaults
Syntax:
  restore [-h]
  restore -s
  restore -a [fName]
  restore -d [fName]
  restore -r rType [-keep]
Switches:
-a      add new local default settings file based upon current settings
-d      delete current local default settings file
-h      display help information
-keep   restore all but IP based settings IP address, subnet, gateway
-r      restore default, [rType]: {factory|file,fName|local|previous}
-s      show current configuration files

>
```

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

The *-a* switch creates a new local configuration file.

The *-d* switch deletes the current local configuration file.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-keep* switch maintains the current IP setting after the module has been restored to factory defaults.

The *-r* switch restores the module to factory defaults or to a configuration file stored on the module.

The *-s* switch displays the restore status.

To create a local configuration file based on the current module configuration, use the *restore -a* command.

```
> restore -a
```

To display the restore status, use the *restore -s* command.

```
> restore -s

Name                               Size
=====
discard.ini                         2434
previous.ini                        2793
current.ini                         2794

>
```

To restore the module to factory default settings, use the *restore -r factory* command.

The module is rebooted and the factory default settings are restored.

## 2.1.29 Save (SAVE)

To save the changes when using the CLI, use the *save* command from the CLI prompt. A list of options is displayed when the *save -h* command is entered.

```
> save -h

Description:
  save - save configuration changes into permanent memory
Syntax:
  save
  save -h
  save -s
Switches:
-h      display help information
-s      show current status

>
```

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

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-s* switch displays the current state of the changes made to the module.

Use the *save -s* command to see if the recent changes have been saved.

```
> save -s

Save status: some parameters have been changed and have not been stored into Permanent
memory

>
```

To save the changes, use the *save* command.

```
> save

> save -s

Save status: all parameters have been stored into Permanent memory

>
```

**NOTE:** If power is removed before the *save* command is initiated, the changes made with the CLI are lost.

### 2.1.30 Create and Run a Script File (SCRIPT)

The *script* command provides the ability to create, run and save a configuration file to the module. After a file has been opened, all typed CLI commands are written to the file. None of the commands typed are executed, only written to the open file. After the file is closed, the *-run* command can be used to execute the saved CLI commands.

To create a script file on the module, use the *script* command from the CLI prompt. A list of options is displayed when the *script -h* command is entered.

```
> script -h

Description:
  script - create and execute script files
Syntax:
  script [-h]
  script -s
  script -d scriptName.osf
  script -close
  script -open scriptName.osf
  script -run scriptName.osf
  script -type scriptName.osf
Switches:
-close close the currently open script file
-d      delete script file, [scriptName.osf]
-h      display help information
-open   open script file, [scriptName.osf]
-run    execute script file, [scriptName.osf]
-s      show current script file list
-type   type the selected file, [scriptName.osf]

>
```

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

The *-close* switch stops the capture of all typed commands and saves the file.

The *-d* switch allows a script file to be deleted.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-open* switch starts the capture of all typed commands.

The *-run* switch executes the script file.

The *-s* switch displays the scripts files stored on the module.

The *-type* switch displays the contents of the selected script file.

To create a script file, use the *-open* command. The filename must have the *.osf* extension.

```
> script -open Config.osf
```

All CLI commands typed after the file has been opened is automatically saved in the file. Once complete with the configuration, close the file using the *-close* command.

```
> script -close
```

To execute the script file, use the *script -run <filename>* command.

### 2.1.31 Firmware Update using Serial Console (SERUPDATE)

The *serupdate* command allows the firmware to be updated from the serial console port using the xmodem protocol.

To update the firmware using the serial console port, use the *serupdate* command from the CLI prompt. A list of options is displayed when the *serupdate -h* command is entered.

```
> serupdate -h

Description:
  serupdate - upload firmware update via the serial port
Syntax:
  serupdate [-h]
  serupdate -s
  serupdate [-trans]
Switches:
-h      display help information
-s      show current selection
-trans  transfer the selected file

>
```

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

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-s* switch displays the method of transfer and status.

The *-trans* switch starts the xmodem process of updating the firmware using the serial console port.

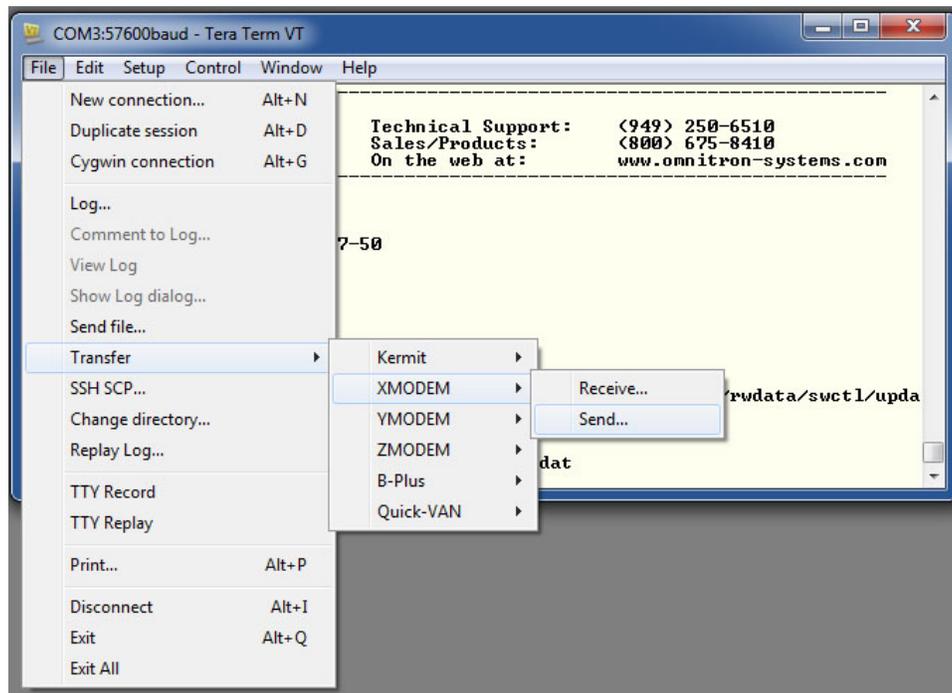
To update the firmware on the module, use the following command.

```
> serupdate -trans

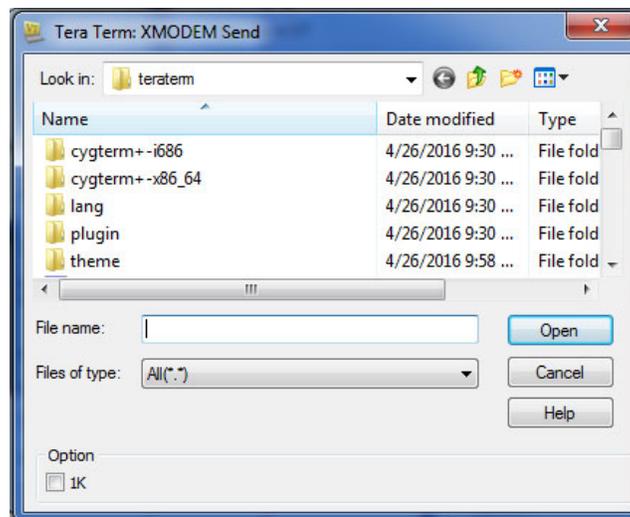
rc = Firmware download started to destination /usr/bin/rx -bv /rwdataswctl/updates/fw.dat
rx: ready to receive /rwdataswctl/updates/fw.dat
```

The module is ready to receive the firmware using xmodem protocol. Using TeraTerm or Procomm, transfer the firmware to the module.

**NOTE: OmniConverter GPoE+/M 8 Port RJ-45 Fixed Fiber models (9520-x-x8-xx - 9531-x-x8-xx) and RuggedNet GPoE+/Mi 8 Port RJ-45 Fixed Fiber models (9540-x-x8-xx - 9551-x-x8-xx) with firmware 2.3.9 cannot be downgraded to any firmware revision. The models can be upgraded from 2.3.9.**



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.

### 2.1.32 SFP (SFP)

#### Only supported on models with SFP ports.

The *sfp* command displays the digital diagnostic information on the selected SFP port.

To display the digital diagnostic information, use the *sfp* command from the CLI prompt. A list of options is displayed when the *sfp -h* command is entered.

```
> sfp -h

Description:
  sfp - small form pluggable port information
Syntax:
  sfp [-h]
  sfp -list
  sfp -s [-p pList]
Switches:
-h      display help information
-list   list all SFP part numbers installed
-p      port list, [pList]: {F1,F2}
-s      show current status

>
```

#### **NOTE: Port number selection will vary depending on the model.**

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

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-list* switch lists the SFP transceivers installed in the module.

The *-p* switch selects the SFP port number.

The *-s* switch displays the digital diagnostic information for the selected port.

To display the SFP transceivers installed in the module, use the *sfp -list* command.

```
> sfp -list

Port = F1: Omnitron, p/n 7207-1, s/n A129070363
Port = F2: Omnitron, p/n 7207-1, s/n B909050136

>
```

To display the information for Fiber Port 1, use the *sfp -s -p fl* command.

```
> sfp -s -p fl

Port = F1

Address A0 Page Contents
=====
00: 03 04 07 00 00 00 02 12 00 01 01 01 0D 00 0C 78 .....x
10: 00 00 00 00 4F 6D 6E 69 74 72 6F 6E 20 53 79 73 ....Omnitron Sys
20: 74 65 6D 73 00 00 06 87 37 32 30 37 2D 31 20 20 tems....7207-1
30: 20 20 20 20 20 20 20 20 30 31 30 30 05 1E 00 03      0100....
40: 00 1A 00 00 45 35 32 39 30 36 30 36 33 39 20 20 ....E529060639
50: 20 20 20 20 31 34 30 36 30 35 20 20 58 B0 01 70      140605 X..p
60: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
70: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
80: FF .....
90: FF .....
A0: FF .....
B0: FF .....
C0: FF .....
D0: FF .....
E0: FF .....
F0: FF .....

Address A2 Page Contents
=====
00: 5A 00 F6 00 55 00 FB 00 92 7C 6B 6C 8A AC 72 10 z...U....|kl..r.
10: 2A 91 02 8E 25 8F 02 C1 12 54 01 A2 0E 8F 02 0E *...%.0...T.....
20: 94 C7 01 7E 76 2E 02 F9 00 00 00 00 00 00 00 00 ...~v.....
30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
40: 00 00 00 00 3E 29 A4 59 BE 29 A4 59 03 E6 F6 3C ....>).Y.) .Y...<
50: 01 B1 00 00 01 00 FB 00 01 00 01 F4 00 00 00 35 .....5
60: 39 30 80 80 0A 08 06 58 2C 00 00 00 00 00 00 F8 90.....X,.....
70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
80: FF .....
90: FF .....
A0: FF .....
B0: FF .....
C0: FF .....
D0: FF .....
E0: FF .....
F0: FF .....

SFP Type: 1000BASE-LX
Bit rate: 1300 Mbps
Wavelength: 1310nm
Link length: 120m
Vendor Name: Omnitron Systems
Vendor Part Number: 7207-1
Vendor Serial Number: E529060639
Date Code: 06/05/2014

Temperature: 41.7C
Vcc: 3.3v
Bias current: 15.0ma
Tx power: -6.2 dBm
Rx power: -7.2 dBm

>
```

### 2.1.33 Display the Common Configuration Parameters (SHOWCONFIG)

The *showconfig* command displays the commonly configured parameters on the module. The parameters that are displayed are: *ver*, *ip*, *port*, *protocol*, *time*, *module*, *pse*, *sfp*, *acl*, *bwp*, *cos*, *ethertype*, *switchport*, *vlan* and *traphost*.

To display the parameters, use the *showconfig* command from the CLI prompt. A list of options is displayed when the *showconfig -h* command is entered.

```
> showconfig -h

Description:
  showconfig - show basic configuration information status
Syntax:
  showconfig [-h]
  showconfig -s [-ver]
Switches:
-h      display help information
-s      show current configuration
-ver    verbose show

>
```

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

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-s* switch displays the current state of each *showconfig* parameter.

The *-ver* switch displays additional commands (*contact*, *lr*, *rstp*, *lag*, *mrp*, *switch*, *portaccess*, *user*, *save*, *aaa*, *igmp*, *lldp*, *sntp*, *ssh*, *smtp*, *snmp*, *stormcontrol* and *traps*).

Use the *showconfig -s* command to display the configuration of the module.

### 2.1.34 Short Message Service (SMS)

The *sms* command provides the ability to configure Short Messaging Service (SMS) on the module. SMS is a protocol used for sending short messages over wireless networks.

SMS uses email to send SMS messages, so an email server must be configured using SMTP prior to configuring the SMS parameters.

To configure the module to support SMS, use the *sms* command from the CLI prompt. A list of options is displayed when the *sms -h* command is entered.

```
> sms -h

Description:
  sms - sms configuration
Syntax:
  sms [-h]
  sms -s
  sms [-ena|-dis sms] [-from fAddr]
  sms -a -phone phoneNum [-level sLevel]
  sms -m -idx sIdx [-phone phoneNum] [-level sLevel]
  sms -d -idx sIdx
  sms -dall
Switches:
-a      add a new SMS phone number
-d      delete an existing SMS phone number
-dall   delete all SMS configured settings and restore defaults
-dis    disable function: {sms}
-ena    enable function: {sms}
        [sms] SMS messaging enable/disable, dflt disabled
-from   email from-address, [fAddr]: 1-254 ASCII characters
-h      display help information
-idx    SMS phone number instance index, [sIdx]
-m      modify an existing SMS phone number instance
-level  minimum level for sms entries, [sLevel]:
        {alert|critical|debug|emergency|error|info|notice|warning}, dflt info
-phone  phone number recipient, [phoneNum]: 1-254 ASCII characters,
        for example: 1112223456@serviceproviderxyz.com
-s      show current configuration

>
```

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

The *-a* switch add a new SMS phone number.

The *-d* switch deletes an existing SMS phone number.

The *-dall* switch deletes all SMS configured settings and restore factory defaults.

The *-dis* and *-ena* switches disables or enables SMS protocol.

The *-from* switch configures the email address of the person the text messages are from.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-idx* switch configures the instance index number.

The *-m* switch modifies an existing instance.

The *-level* switch configures the minimum level for SMS entries.

The *-phone* switch configures the phone number of the SMS recipient.

The *-s* switch displays the configured settings.

Use the `sms -s` command to display the SMS configuration.

```
> sms -s

SMS forwarding    disabled
SMS from address  ""
Phone numbers    none configured
```

The SMS phone number (`-phone`) is the email address associated with the mobile phone. It is determined by using the mobile phone number and mobile service provider gateway domain.

Carrier	SMS gateway domain	MMS gateway domain
Alltel	[10-digit number]@message.alltel.com	[10-digit number]@mms.alltelwireless.com
AT&T	[10-digit number]@txt.att.net	[10-digit number]@mms.att.net
Boost Mobile	[10-digit number]@myboostmobile.com	[10-digit number]@myboostmobile.com
Cricket Wireless	[10-digit number]@sms.cricketwireless.net	[10-digit number]@mms.cricketwireless.net
Google Project Fi	[10-digit number]@msg.fi.google.com	[10-digit number]@msg.fi.google.com
Republic Wireless	[10-digital number]@text.republicwireless.com	
Sprint	[10-digit number]@messaging.sprintpcs.com	[10-digit number]@pm.sprint.com
Straight Talk	[10-digital number]@vtext.com	[10-digit number]@mypixmessages.com
T-Mobile	[10-digit number]@tmomail.net	[10-digit number]@tmomail.net
Ting	[10-digit number]@message.ting.com	
Tracfone		[10-digit number]@mmst5.tracfone.com
U.S. Cellular	[10-digit number]@email.uscc.net	[10-digit number]@mms.uscc.net
Verizon	[10-digit number]@vtext.com	[10-digit number]@vzwpix.com
Virgin Mobile	[10-digit number]@vmobl.com	[10-digit number]@vmpix.com

For example, if the mobile phone number is 555-123-4567 and the mobile service provider is AT&T, the SMS phone number (`-phone`) would be 5551234567@txt.att.net.

To configure a SMS address, use the following command examples.

```
> sms -from bobsmith.92618@gmail.com
> sms -a -phone 5551234567@txt.att.net
Phone number 1 added
> sms -ena sms
> sms -s

SMS forwarding    enabled
SMS from address  bobsmith.92618@gmail.com
Phone number 1:   5551234567@txt.att.net, severity info

>
```

### 2.1.35 Simple Mail Transfer Protocol (SMTP)

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.

To configure the module to support SMTP, use the *smtp* command from the CLI prompt. A list of options is displayed when the *smtp -h* command is entered.

```
> smtp -h

Description:
  smtp - smtp configuration
Syntax:
  smtp [-h]
  smtp -info
  smtp -s
  smtp [-host hName] [-name uName] [-pw uPw] [-from fAddr] [-port pNum]
  [-ena|-dis {smtp,starttls,tls}]
  smtp -a -rec eAddr [-level sLevel]
  smtp -m -idx sIdx [-rec eAddr] [-level sLevel]
  smtp -d -idx sIdx
  smtp -dall
  smtp -test sLevel:msg
Switches:
-a      add a new SMTP email address instance
-d      delete an existing SMTP email address instance
-dall   delete all SMTP configured settings and restore defaults
-dis    disable function: {smtp,starttls,tls}
-ena    enable function: {smtp,starttls,tls}
        [smtp] SMTP function enable/disable, dflt disabled
        [starttls] STARTTLS enable/disable, dflt enabled
        [tls] TLS enable/disable, dflt disabled
-from   email from-address, [fAddr]: 1-254 ASCII characters
-h      display help information
-host   mail server IP address or domain, [hName]: 1-253 ASCII characters
-idx    SMTP email instance index, [sIdx]
-info   displays SMTP email server information and connectivity status
-level  minimum level for smtp entries, [sLevel]:
        {alert|critical|debug|emergency|error|info|notice|warning}, dflt info
-m      modify an existing SMTP email address instance
-name   user name, [uName]: 1-254 ASCII characters
-port   SMTP destination port, [pNum]: {1..65535}, dflt 25
-pw     user password, [uPw]: 1-32 ASCII characters
-rec    email recipient, [eAddr]: 1-254 ASCII characters
-s      show current configuration
-test   SMTP test message, [sLevel:msg]
        [sLevel] {alert|critical|debug|emergency|error|info|notice|warning}
        [msg] 1-160 characters

>
```

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

The *-a* switch adds a new SMTP email address instance.

The *-d* switch deletes an existing SMTP instance.

The *-dall* switch deletes all SMTP settings and restores factory defaults.

The *-dis* switch disables SMTP event forwarding, StartTLS and TLS.

The *-ena* switch enables SMTP event forwarding, StartTLS and TLS.

The *-from* switch configures the email address of the person the email is from.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-host* switch configures the IP address of the SMTP mail server or domain.

The *-idx* switch configures the instance index number.

The *-info* switch displays the SMTP email server information and connectivity status.

The *-level* switch configures the syslog minimum severity error for forwarding events: emergency (highest), alert, critical, error, warning, notice, info (informational), debug (lowest). Only events that have a severity level greater than or equal to the configured level will be generated as an email.

The *-m* switch modifies an existing instance.

The *-name* switch configures the user name to be used to log into the email server.

The *-port* switch configures the SMTP port number. The default port number is 25.

The *-pw* switch configures the password for the selected email account.

The *-rec* switch configures one or more email recipients.

The *-s* switch displays the configured settings.

The *-test* switch send a test email to the email server at the specified severity level.

To display the SMTP parameters, use the *smtp -s* command.

```
> smtp -s

SMTP forwarding      disabled
SMTP host            ""
SMTP user name       ""
SMTP from address    ""
SMTP password        *****
SMTP port number     25
TLS protocol         disabled
TLS STARTTLS option  enabled
Email recipients     none configured

>
```

To configure SMTP forwarding, use the following command examples.

```
> smtp -host 192.168.1.1 -from jsmith@gmail.com
> smtp -name abc@xyz.com -pw 123456
> smtp -a -rec bill@gmail.com

Email recipient 1 added

> smtp -ena smtp
> smtp -s

SMTP forwarding      enabled
SMTP host            192.168.1.1
SMTP user name       abc@xyz.com
SMTP from address    jsmith@gmail.com
SMTP password        *****
SMTP port number     25
TLS protocol         disabled
TLS STARTTLS option  enabled
Email recipient 1    bill@gmail.com, severity info

>
```

### 2.1.36 Simple Network Management Protocol (SNMP)

The *snmp* command provides the ability to configure the SNMP parameters on the module.

To configure the module to support Simple Network Management Protocol (SNMP), use the *snmp* command from the CLI prompt. A list of options is displayed when the *snmp -h* command is entered.

```
> snmp -h

Description:
  snmp - simple network management protocol user configuration
Syntax:
  snmp [-h]
  snmp -s
  snmp [-rd pw] [-wr pw] [-ena|-dis {snmpv1|snmpv3}]
  snmp -user uNum [-typ uTyp] [-name uName] [-auth aPw] [-priv pPw] [-sec uSec]
  [-atype aTy] [-ptype pTy]
  snmp -dall
Switches:
-atype authentication type, [aTy]: {md5|sha}, dflt md5
-auth authentication password, [aPw]: 8-32 ASCII characters
-dall delete all SNMP configured settings and restore defaults
-dis disable function: {snmpv1|snmpv3}
-ena enable function: {snmpv1|snmpv3}
    [snmpv1] SNMPv1/v2c protocol, dflt enabled
    [snmpv3] SNMPv3 protocol, dflt enabled
-h display help information
-name user name, [uName]: 1-32 ASCII characters
-priv privacy password, [pPw]: 8-32 ASCII characters
-ptype privacy type, [pTy]: {aes|des}, dflt des
-rd read community name, [pw]: 1-32 ASCII characters
-s show current configuration
-sec user security level, [uSec]: {noAuthNoPriv,authNoPriv,authPriv}
-typ user type, [uTyp]: {admin|deny|readonly|readwrite}
-user user number, [uNum]: {1..4}
-wr write community name, [pw]: 1-32 ASCII characters

>
```

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

The *-atype* switch configures the authentication hashing method; MD5 or SHA.

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

The *-dis* switch disables SNMPv1 and SNMPv3.

The *-ena* switch enables SNMPv1 and SNMPv3.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-name* switch configures the user name for the selected user.

The *-priv* switch configures the privacy password for the selected user.

The *-ptype* switch configures the privacy password encryption algorithm; AES or DES.

The *-rd* switch 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 *-s* switch displays the SNMP configuration parameters.

The *-sec* switch configures the security level for the selected user

- noAuthNoPriv* Allows access without authentication and without privacy.
- authNoPriv* Allows access with authentication, but without privacy.
- authPriv* Allows access with authentication and with privacy. Authentication and privacy uses different algorithms for encrypting and decrypting SNMPv3 packets.

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

- admin* An admin user has full read/write privileges including user name and password changes.
- read-write* A read-write user has full read/write privileges with the exception of user name and password operations.
- read-only* A read-only user can only view the configuration of the module and will not be allowed to make any changes.
- deny* A deny user does not have any access to the module.

The *-user* switch configures the user number used for the configuration parameters.

The *-wr* switch 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.

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

```
> snmp -wr public
```

To display the SNMP parameters, use the *snmp -s* command.

```
> snmp -s

SNMPv1/v2c agent          enabled
SNMPv3 agent              enabled
Read community name       *****
Write community name      *****

User 1 type               admin
User 1 name                admin
User 1 security level     noAuthNoPriv
User 1 privacy password   *****
User 1 privacy encryption DES
User 1 authentication password *****
User 1 authentication hashing MD5

User 2 type                read-only
User 2 name                 guest
User 2 security level     noAuthNoPriv
User 2 privacy password   *****
User 2 privacy encryption DES
User 2 authentication password *****
User 2 authentication hashing MD5

User 3 type                read-only
User 3 name                 guest1
User 3 security level     noAuthNoPriv
User 3 privacy password   *****
User 3 privacy encryption DES
User 3 authentication password *****
User 3 authentication hashing MD5

User 4 type                read-only
User 4 name                 guest2
User 4 security level     noAuthNoPriv
User 4 privacy password   *****
User 4 privacy encryption DES
User 4 authentication password *****
User 4 authentication hashing MD5

>
```

### 2.1.37 Simple Network Time Protocol (SNTP)

The *sntp* command provides the ability to configure the module to request the time and day from a SNTP server.

To configure the module to support Simple Network Time Protocol (SNTP), use the *sntp* command from the CLI prompt. A list of options is displayed when the *sntp -h* command is entered.

```
> sntp -h

Description:
  sntp - simple network time protocol configuration
Syntax:
  sntp [-h]
  sntp -s
  sntp -dall
  sntp [-ena|-dis ntp|sntp] [-i iTime] [-z zoneVal] [-ip1 serverIP]
      [-ip2 serverIP]
Switches:
-dall  delete all SNTP configured settings and restore defaults
-dis   disable function: {ntp|sntp}
-ena   enable function: {ntp|sntp}
       [ntp] Network Time Protocol
       [sntp] Simple Network Time Protocol
-h     display help information
-i     time server request interval in minutes, [iTime]: {1..60}, dflt 8
-ip1   time server IP address 1, [serverIP]
-ip2   time server IP address 2, [serverIP]
-s     show current configuration
-z     time zone selection, [zoneVal]

To get help screen on time zone values type "zone -h"

>
```

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

The *-dall* switch deletes all settings and restores factory defaults.

The *-dis* and *-ena* switches disable or enable SNTP or NTP on the module.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-i* switch defines the time interval between SNTP requests.

The *-ip1* and *-ip2* switches define the IP addresses of the SNTP servers.

The *-s* switch displays the SNTP configuration.

The *-z* switch defines the time zone.

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

```
> sntp -ena sntp -ip1 192.168.1.240
```

To display the SNTP configuration, use the *sntp -s* command.

```
> sntp -s

SNTP service is enabled, query interval is 8 minutes
Time zone PST (Pacific Standard Time)
Time server 1 IP is 192.168.1.240
Time server 2 IP is 255.255.255.255 (not configured)
```

### 2.1.38 Spanning Tree Protocol (SPANTREE)

Multiple Spanning Tree Protocol (MSTP) is a protocol that creates multiple spanning trees (instances) for each VLAN. This allows each VLAN to be configured with a root bridge and forwarding topology.

The *spantree* command provides the ability to configure Multiple Spanning Tree Protocol (MSTP).

To configure Multiple Spanning Tree Protocol, use the *spantree* command from the CLI prompt. A list of options is displayed when the *spantree -h* command is entered.

```
> spantree -h

Description:
  spantree - spanning tree configuration
Syntax:
  spantree [-h]
  spantree -s [-p pList]
  spantree -dall
  spantree [-bage timeout] [-hello time] [-fwd time] [-bpri bPri]
           [-ena|-dis stp]
  spantree -p pList [-ppri pPri] [-pcost pCost] [-proto pMode]
           [-ena|-dis {bpduguard,portfast,rootguard}]
  spantree -a -pn pName -vid vList -p pList [-proto pMode]
  spantree -d -pn pName
Switches:
-a      add new MSTP instance
-bage   bridge aging timeout in sec, [timeout]: {6..40}, dflt 20
-bpri   bridge priority, [bPri]: {0..61440}, dflt 32768, multiples of 4096
-d      delete MSTP instance
-dall   delete all "spantree" configured settings, instances, & restore defaults
-dis    disable function: {bpduguard,portfast,rootguard,stp}
-ena    enable function: {bpduguard,portfast,rootguard,stp}
        [bpduguard] port is disabled when BPDU received, dflt disabled
        [portfast] forwarding immediately & bypass listening, dflt disabled
        [rootguard] port is disabled if designated as root, dflt disabled
        [stp] Spanning Tree on module, dflt disabled
-fwd    forward delay time in sec, [time]: {4..30}, dflt 15
-h      display help information
-hello  time between configuration message in sec, [time]: {1..5}, dflt 2
-p      port list, [pList]: {F1,F2,1..4|all}
-pcost  port path cost [pCost]: {1..200,000,000}, dflt 20000
-pn     spanning tree instance name, [pName]: 1 to 32 ASCII characters
-ppri   port priority, [pPri]: {0..240} dflt 128, multiples of 16
-proto  protocol configuration, [pMode]: {discard|mstp|rstp|tunnel}
        [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
-s      show current configuration
-vid    VLAN list: {1..4095}

>
```

**NOTE: Port number selection will vary depending on the model.**

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

The *-a* switch adds a MSTP instance.

The *-bage* switch defines the time period before the MAC addresses are removed from the table.

The *-bpri* switch defines the bridge priority ID for the port. The root bridge is the port with the lowest bridge priority ID.

The *-d* switch deletes a MSTP instance.

The *-dall* switch deletes all Spanning Tree settings and restore factory defaults.

The *-dis* switch disables BPDU Guard (bpduguard), Port Fast (portfast), Root Guard (rootguard) and Spanning Tree (stp).

The *-ena* switch enables BPDU Guard (bpduguard), Port Fast (portfast), Root Guard (rootguard) and Spanning Tree (stp).

The *-fwd* switch defines the time before a port transitions to a forwarding state.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-hello* switch defines the time period between hello-time Bridge Protocol Data Units (BPDUs).

The *-p* switch defines the port associated with spanning tree protocol.

The *-pcost* switch defines the cost of the path. The path cost is based on the speed of the physical interface speed.

The *-pn* switch configures the name of the instance.

The *-ppri* switch defines the priority of the port. The state of the port is determined by the port cost and port priority values.

The *-proto* switch configures the protocols.

*discard* RSTP/MSTP protocols are disabled.

*mstp* MSTP is enabled and the protocol is operating.

*rstp* RSTP is enabled and the protocol is operating.

*tunnel* RSTP/MSTP protocols are disabled. BPDU frames are tunneled.

The *-s* switch displays the current Rapid Spanning Tree configuration.

The *-vid* switch configures the VLAN associated with the Spanning Tree instance.

**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.

To configure port priority and path cost, use the *-pcost* and *-ppri* commands.

```
> spantree -p 1 -pcost 10000 -ppri 96
```

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.

To display spanning tree configuration, use the *rstp -s* command.

```
> spantree -s

Bridge Spanning Tree Global Configuration
=====
Spanning tree                               Disabled
Bridge Id
Designated Root
Bridge Priority                               32768
Bridge Max Age                               20
Hello Time                                   2
Forward Delay                                15

Port F1 Configuration
=====
Port Type                                   Tunnel
Spanning Tree Port State                    N/A
Port Priority                                128
Path Cost                                   20000
BPDU Guard                                 Disabled
Port Fast                                  Disabled
Root Guard                                 Disabled

Port F2 Configuration
=====
Port Type                                   Tunnel
Spanning Tree Port State                    N/A
Port Priority                                128
Path Cost                                   20000
BPDU Guard                                 Disabled
Port Fast                                  Disabled
Root Guard                                 Disabled

Port 1 Configuration
=====
Port Type                                   Tunnel
Spanning Tree Port State                    N/A
Port Priority                                128
Path Cost                                   20000
BPDU Guard                                 Disabled
Port Fast                                  Disabled
Root Guard                                 Disabled

Port 2 Configuration
=====
Port Type                                   Tunnel
Spanning Tree Port State                    N/A
Port Priority                                128
Path Cost                                   20000
BPDU Guard                                 Disabled
Port Fast                                  Disabled
Root Guard                                 Disabled
```

```

Port 3 Configuration
=====
Port Type                Tunnel
Spanning Tree Port State N/A
Port Priority             128
Path Cost                20000
BPDU Guard               Disabled
Port Fast                Disabled
Root Guard               Disabled

Port 4 Configuration
=====
Port Type                Tunnel
Spanning Tree Port State N/A
Port Priority             128
Path Cost                20000
BPDU Guard               Disabled
Port Fast                Disabled
Root Guard               Disabled

MSTP Instances
  None

>

```

### 2.1.39 Entry Screen Message Display (SPLASH)

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.

To configure the module with a message, use the *splash* command from the CLI prompt. A list of options is displayed when the *splash -h* command is entered.

```

> splash

Description:
  splash - splash screen warning message configuration
Syntax:
  splash [-h]
  splash -s
  splash -warn wMsg
Switches:
-h      display help information
-s      show current status
-warn   warning message, [wMsg]: 0 to 255 ASCII characters

>

```

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

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-s* switch displays the current message.

The *-warn* switch configures the message.

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."
```

```
> splash -s
```

```
This product is for the use of authorized user 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:
```

### 2.1.40 Secure Shell (SSH)

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.

To configure SSH, use the *ssh* command from the CLI prompt. A list of options is displayed when the *ssh -h* command is entered.

```
> ssh -h

Description:
  ssh - secure shell configuration
Syntax:
  ssh [-h]
  ssh -dall
  ssh -s [-ver]
  ssh [{-dis|-ena} {dsa|pwd|rsa|sftp|ssh}]
    [-tcp tPort] [-genk]
Switches:
-dall  delete all SSH configured settings and restore defaults
-dis   disable function: {dsa|pwd|rsa|sftp|ssh}
-ena   enable function: {dsa|pwd|rsa|sftp|ssh}, dflt all enabled
       [dsa] DSA key authentication
       [pwd] plain text password entry authentication
       [rsa] RSA key authentication
       [sftp] secure file transfer protocol (scp v2)
       [ssh] secure shell protocol
-genk  generate public/private keys
-h     display help information
-s     show current configuration
-tcp   tcp port, [tPort]: {1..65535}, dflt 22
-ver   verbose show

>
```

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

The *-dall* switch deletes all SSH settings and restores factory defaults.

The *-dis* and *-ena* switches disable or enable specific authentication methods and file transfer functions.

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

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-s* switch displays the current configuration.

The *-tcp* switch defines the TCP port used for the SSH session.

The *-ver* switch displays the extended public key screen.

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.

To enable SSH, and set TCP Port 23, use the *-ena* and *-tcp* commands.

```
> ssh -ena ssh -tcp 23
```

To regenerate the public and private keys, use the *-genk* command.

```
> ssh -genk
```

**NOTE: It takes time to generate the public and private keys. Please be patient when using this command.**

To display the SSH configuration, use the *ssh -s* command.

```
> ssh -s

SSH v2                enabled
RSA fingerprint      a7:53:4d:86:69:fe:e6:f3:96:5b:ca:54:a1:be:47:e8
DSA fingerprint      94:6c:52:12:17:e9:ad:a6:ec:34:50:7a:67:0c:08:d4
TCP port number      22
SFTP                  enabled
Plain text authentication enabled
RSA authentication   enabled
DSA authentication   enabled

>
```

## 2.1.41 Storm Prevention (STORMCONTROL)

The *stormcontrol* command provides the ability to configure storm prevent for broadcast, multicast and unicast traffic on each port. When configured, traffic will be blocked when the traffic reaches a certain configurable threshold.

To configure storm prevention on the module, use the *stormcontrol* command from the CLI prompt. A list of options is displayed when the *stormcontrol -h* command is entered.

```
> stormcontrol -h

Description:
  stormcontrol - storm control configuration
Syntax:
  stormcontrol [-h]
  stormcontrol -s [-p pList]
  stormcontrol -p pList [{-dis|-ena} {broadcast,multicast,unicast}]
    [[-level high[,low]]|[-bps high[,low]]]
  stormcontrol -dall
Switches:
-bps  interface bits per second level threshold: {high,low}
      [high] rising level threshold, {100000..1000000000}
      [low] falling level threshold, {100000..1000000000}
-dall  delete all 'stormcontrol' configured settings and restore defaults
-dis   disable function: {broadcast,multicast,unicast}
-ena   enable function: {broadcast,multicast,unicast}
      [broadcast] broadcast storm control, dflt disable
      [multicast] multicast frame storm control, dflt disable
      [unicast] unicast frame storm control, dflt disabled
-h     display help information
-level interface level threshold percentage: {high,low}
      [high] rising level threshold, {0.01..100.00}
      [low] falling level threshold, {0.01..100.00}
-p     port list, [pList]: {F1,F2,1..4|all}
-s     show current configuration

>
```

**NOTE: Port number selection will vary depending on the model.**

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

The *-bps* switch configures the interface high threshold and the optional low threshold values in bits per second.

The *low* value if configured will be less than or equal to the *high* value. If the *low* value is not configured it will be treated as equal to the *high* value.

The *-dall* switch deletes all storm control settings and restores factory defaults.

The *-dis* switch disables one or more of the following functions:

- broadcast* Disables broadcast frame storm control.
- multicast* Disables multicast frame storm control.
- unicast* Disables unicast frame storm control

The *-ena* switch enables one or more of the following functions:

- broadcast* Enables broadcast frame storm control.
- multicast* Enables multicast frame storm control.
- unicast* Enables unicast frame storm control

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-level* switch configures the interface high threshold and the optional low threshold values in percentage of the interface maximum speed.

The *low* value if configured will be less than or equal to the *high* value. If the *low* value is not configured it will be treated as equal to the *high* value.

The *-p* switch configures one or more physical ports on the module.

The *-s* switch displays the current configuration.

To enable broadcast storm prevention on port F2 at a 50% threshold, use the following command.

```
> stormcontrol -p f2 -level 50.0 -ena broadcast
```

To display the storm prevention configuration, use the *stormcontrol -s* command.

```
> stormcontrol -s -p f2

Port F2
  Threshold high           50.00 %
  Threshold low            n/a
  Broadcast storm control  enabled
  Multicast storm control  disabled
  Unicast storm control    disabled
  Status                   not blocking receiving 0.00 %

>
```

### 2.1.42 DIP-Switch Configuration (SWITCH)

The *switch* command provides the ability to configure and display the DIP-switches on the module.

To configure the DIP-switches on the module, use the *switch* command from the CLI prompt. A list of options is displayed when the *switch -h* command is entered.

```
> switch -h

Description:
  switch - physical switch configuration
Syntax:
  switch [-h]
  switch -s
  switch -ena|-dis {hw|{sw,sNum}}
  switch -dall
Switches:
-dall delete all "switch" configured settings and restore defaults
-dis  disable function: {hw|{sw,sNum}}
-ena  enable function: {hw|{sw,sNum}}
      [hw] hardware DIP switch function, dflt enabled
      [sw] software DIP switch function
      [sNum] software DIP switch number to enable or disable: {1..8|all}
-h    display help information
-s    show current configuration

>
```

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

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

The *-dis* switch disables (Off) the selected switch number.

The *-ena* switch enables (On) the selected switch number.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-s* switch displays the configuration of the DIP-switches.

To enable DIP-switch 2, use the *switch -ena 2* command.

```
> switch -dis hw
> switch -ena sw,2
```

To display the configuration of the DIP-switches, use the *switch -s* command.

```
> switch -s

Switch ON Condition      OFF Condition      H/W   Soft
1:   Dual switch        Single switch      Off   Off
2:   Directed switch    Normal switch      Off   On
3:   Redundant uplink   No redundant uplink Off   Off
4:   Return to primary  No return          Off   Off
5:   MAC learning Off   MAC learning On   Off   Off
6:   Force PoE Power    Auto PoE Power     Off   Off
7:   L2CP discard       L2CP tunnel        Off   Off
8:   PoE with reset     PoE with no reset  Off   Off

Hardware DIP switches:  disabled

>
```

DIP-switch settings above are for an OmniConverter and RuggedNet 10GPoEBT, GHPoE and GHPoEBT model.

```
> switch -s

Switch ON Condition      OFF Condition      H/W   Soft
1:   Dual switch        Single switch      Off   Off
2:   Directed switch    Normal switch      Off   On
3:   Redundant uplink   No redundant uplink Off   Off
4:   Return to primary  No return          Off   Off
5:   MAC learning Off   MAC learning On   Off   Off
6:   Pause On           Pause Off          Off   Off
7:   L2CP discard       L2CP tunnel        Off   Off
8:   PoE with reset     PoE with no reset  Off   Off

Hardware DIP switches:  disabled

>
```

DIP-switch settings above are for an OmniConverter and RuggedNet 10GPoE+ and GPoE+ model.

```

> switch -s

Switch ON Condition      OFF Condition      H/W   Soft
1:   Dual switch        Single switch      Off   Off
2:   Directed switch    Normal switch      Off   On
3:   Redundant uplink   No redundant uplink Off   Off
4:   Return to primary  No return          Off   Off
5:   MAC learning Off   MAC learning On   Off   Off
6:   Pause On           Pause Off          Off   Off
7:   L2CP discard       L2CP tunnel        Off   Off
8:   SW8 On              SW8 Off            Off   Off

Hardware DIP switches:  disabled

>

```

DIP-switch settings above are for an OmniConverter and RuggedNet 10G/M, 10G/Mi, G/M and G/Mi model.

### 2.1.43 VLAN Interface Configuration (SWITCHPORT)

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

To configure the VLAN interfaces, use the *switchport* command from the CLI prompt. A list of options is displayed when the *switchport -h* command is entered.

```

> switchport

Description:
  switchport - vlan interface configuration
Syntax:
  switchport [-h]
  switchport [-p pList] -s
  switchport -p pNum -mode {access|tunnel|trunk}
  switchport -p pNum -vid vlanId
  switchport -p pNum -nvlan vlanId
  switchport -p pNum {-add|-rem|-allow} vlanList
  switchport -dall
Switches:
-add   trunk port add VLAN ID list, [vlanList]: {1..4095|all}
-allow trunk port replace current list, [vlanList]: {1..4095|all}
-dall  delete all 'switchport' configured settings and restore defaults
-h     display help information
-mode  port mode type: {access|tunnel|trunk}
       [access] access port type
       [trunk] trunk port type
       [tunnel] tunnel port type
-nvlan native vlan assignment for trunk port, [vlanId]: {0..4095}
       vlanId set to 0 removes the native vlan configuration
-p     port number, [pNum|pList]: {F1|F2|1..4|mgt1}
-rem   trunk port remove VLAN ID, [vlanList]: {1..4095|all}
-s     show current configuration
-vid   vlan id assignment for access/tunnel port, [vlanId]: {1..4095}

>

```

**NOTE: Port number selection will vary depending on the model.**

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

The *-add* switch adds one or more VLANs to an existing trunk port VLAN list.

The *-allow* switch replaces the current VLANs on a trunk port with the provided VLAN list.

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

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-mode* switch configures the port type; access, trunk or tunnel.

- trunk*      When configured as a trunk port:
  - Ingress: The trunk VLAN is removed
  - Egress: The trunk VLAN is added
- tunnel*     When configured as a tunnel port:
  - Ingress: Untagged and tagged traffic is accepted
  - Egress: Traffic follows the assigned VID
- access*     When configured as an access port:
  - Ingress: Accepts only untagged traffic
  - Egress: Traffic follows the assigned VID

The *-nvlan* switch configures the trunk port with native VLAN assignment.

The *-p* switch selects the port number for assignment.

The *-rem* switch removes one or more VLANs from an existing trunk port VLAN list.

The *-s* switch displays the VLAN configuration.

The *-vid* switch configures a VLAN ID to an access or tunnel port.

**NOTE: 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 display the VLAN configuration of the module, use the *switchport -s* command.

```
> switchport -s

Port F1 is an access port type, associated with VLAN ID 1
Port F2 is an access port type, associated with VLAN ID 1
Port 1 is an access port type, associated with VLAN ID 1
Port 2 is an access port type, associated with VLAN ID 1
Port 3 is an access port type, associated with VLAN ID 1
Port 4 is an access port type, associated with VLAN ID 1
Mgt1 is an access port type associated with VLAN ID 1

>
```

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

```
> vlan -add 100
> switchport -p 1 -vid 100
> switchport -s -p 1

Port 1 is an access port type, associated with VLAN ID 100

>
```

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

To configure Uplink Port 1 (F1) as a trunk port, use the following command.

```
> switchport -p f1 -mode trunk
> switchport -s -p f1

Port F1 is a trunk port type, native VLAN ID 1
  included VLANs: 1..4095

>
```

#### 2.1.44 Syslog Server Configuration (SYSLOG)

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

To configure syslog, use the *syslog* command from the CLI prompt. A list of options is displayed when the *syslog -h* command is entered.

```
> syslog -h

Description:
  syslog - system log message configuration
Syntax:
  syslog [-h]
  syslog -s [-log lNum]
  syslog [-ena|-dis] [-ip serverNumIp] [-erase] [-level sLevel] [-fac fCode]
  syslog -test sLevel:message
  syslog -dall
Switches:
-erase erase all current syslog local entries
-dall delete all syslog configured settings and restore defaults
-dis disable syslog on the module, dflt
-ena enable syslog on the module
-fac facility, [fCode]: {16..23}, dflt 23
-h display help information
-ip syslog server IP address, [serverNumIP], dflt 192.168.1.221
-level minimum level for syslog entries, [sLevel]:
  {alert|critical|debug|emergency|error|info|notice|warning}, dflt info
-log show the log entries, [lNum]: {1..1000|all}, dflt 10
-s show current configuration
-test generate test syslog entry, [sLevel:message]
  [sLevel] syslog level
  [message]: 1 to 127 characters

>
```

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

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

The *-dis* switch disables the syslog functionality.

The *-ena* switch enables the syslog functionality. This includes writing to the syslog server.

The *-erase* switch erases all the entries in the current syslog.

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

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-ip* switch configures the syslog server IP address.

The *-level* switch selects the syslog minimum severity error for logging errors.

- alert*            A condition that should be corrected immediately.
- critical*        Hard device errors.
- debug*           Messages that contain information normally of use only when debugging a program.
- emergency*      A panic condition.
- error*            Error conditions.
- info*             Informational messages.
- notice*          Conditions that are not error conditions, but that may require special handling.
- warning*         Warning conditions.

The *-log* switch displays specific number of syslog entries. The default value is 10.

The *-s* switch displays the syslog configuration and the last 10 entries.

The *-test* switch generates a test syslog entry for a specific severity and a specific message.

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

```
> syslog -ip 192.168.1.100 -ena
```

To display the syslog configuration and last 10 entries, use the *syslog -s* command.

```
> syslog -s

Status                            enabled
Server IP address                192.168.1.100
Severity logging level            Info
Facility code                    23
Number of local entries          6

Number of entries
  Debug            0
  Info             0
  Notice           0
  Warning          4
  Error            2
  Critical         0
  Alert            0
  Emergency        0

ID            Level            Time                            Message
=====
6            Warning        01/02/2000 04:05:56 PM        Link up port F2
5            Warning        01/02/2000 04:05:55 PM        PoE status port 2 error 0
4            Warning        01/02/2000 04:05:53 PM        Link up port 2
3            Error           01/02/2000 04:05:52 PM        Link down port F2
2            Warning        01/02/2000 04:05:49 PM        PoE status port 2 error 0
1            Error           01/02/2000 04:05:49 PM        Link down port 2

>
```

The module retains the last 1000 entries.

## 2.1.45 Time (TIME)

The *time* command provides the ability to set or display the time of day on the module.

To configure time on the module, use the *time* command from the CLI prompt. A list of options is displayed when the *time -h* command is entered.

```
> time -h

Description:
  time - time of day configuration
Syntax:
  time [-h]
  time -s
  time -z zoneVal
  time -a timeOfDay [-z zoneVal]
Switches:
-a   set the time of day, [timeOfDay]: "month/day/year 24hr:min:sec"
     example "12/01/2015 13:10:00"
-h   display help information
-s   show current configuration
-z   time zone, [zoneVal]

>
```

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

The *-a* switch sets the time of day.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-s* switch displays the current time of day.

The *-z* switch defines the time zone.

The example below sets the time of day.

```
> time -a "10/10/2019 07:55:00"
```

To display the time of day, use the *time -s* command.

```
> time -s

Time of day: 10/10/2019 07:55:00 PM Pacific Standard Time
sysUpTime: 41191600 (4 days 18 hours 25 minutes 16 secs)

>
```

## 2.1.46 SNMP Trap Host (TRAPHOST)

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.

To configure the Trap Hosts, use the *traphost* command from the CLI prompt. A list of options is displayed when the *traphost -h* command is entered.

```
> traphost -h

Description:
  traphost - snmp trap host configuration
Syntax:
  traphost [-h]
  traphost -s
  traphost -host hNum [-ip ipAddr] [-port pNum]
  traphost -dall
Switches:
-dall  delete all SNMP trap hosts configured settings and restore defaults
-h     display help information
-host  traphost number, [hNum]: {1..8}
-ip    trap host IP address, [ipAddr]
-port  trap port number, [pNum]: {1..65535}, dflt 162
-s     show current configuration

>
```

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

The *-dall* switch deletes configured trap hosts and resets the setting to factory default. The default setting is 255.255.255.255.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-host* switch selects the Trap Host number to be configured. Eight different Traps Hosts can be configured.

The *-ip* switch configures the IP address for the selected Trap Host.

The *-port* switch configures the UDP trap port number.

The *-s* switch displays the SNMP Trap Host settings.

To configure the IP address for Trap Host 1, use the following command.

```
> traphost -host 1 -ip 192.168.1.100
> traphost -s

Trap host #1 IP address 192.168.1.110, UDP port: 162
Trap host #2 IP address 255.255.255.255 (not configured)
Trap host #3 IP address 255.255.255.255 (not configured)
Trap host #4 IP address 255.255.255.255 (not configured)
Trap host #5 IP address 255.255.255.255 (not configured)
Trap host #6 IP address 255.255.255.255 (not configured)
Trap host #7 IP address 255.255.255.255 (not configured)
Trap host #8 IP address 255.255.255.255 (not configured)

>
```

## 2.1.47 SNMP Traps (TRAPS)

The *traps* command provides the ability to enable/disable specific module traps. By default, all traps are enabled.

To enable traps, use the *traps* option from the CLI prompt. A list of options is displayed when the *traps -h* command is entered.

```
> traps -h
Description:
  traps - snmp trap configuration
Syntax:
  traps [-h]
  traps -s
  traps [-dall][[-ena|-dis tNum]
  traps -log [-clr] [-ver]
  traps [-type {snmpv2c|snmpv3}] [-user uNum]
  traps -gen tNum
Switches:
-clr   clear trap log
-dall  delete all 'traps' configured settings and restore defaults
-dis   disable selected trap number, [tNum]: {1..63|all}
-ena   enable selected trap number, [tNum]: {1..63|all}
-gen   generate trap, [tNum]: {1..63}
-h     display help information
-log   display log entries
-s     show current configuration
-type  trap generation type: {snmpv2c|snmpv3}, dflt snmpv2c
-user  trap generation SNMP user, [uNum]: {1..4}, dflt 1
-ver   verbose show
>
```

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

The *-clr* switch clears the current trap log entries.

The *-dall* switch restores all traps to default settings.

The *-dis* switch defines which trap types will be disabled.

The *-ena* switch defines which trap types will be enabled.

The *-gen* switch generates a specific trap number. Traphost must be configured to receive the generated trap.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-log* switch displays the last 100 trap entries.

The *-s* switch displays the current trap configuration.

The *-type* switch configures the generation type of the trap; SNMPv2c or SNMPv3.

The *-user* switch configures the user number for the trap generation.

The *-ver* switch displays the extended help.

Individual traps can be enabled or disabled by entering the name of the traps after the *ena/dis* command.

The example below disables the link down (#6) trap.

```
> traps -dis 6
```

To display the traps, use the *traps -s* command.

```
> traps -s
```

```
SNMP trap type: SNMPv2c
```

```
SNMP trap gen user: 1
```

```
Severity Level: all
```

Trap Type	Status	Severity
1 Module cold start	Enabled	Notice
2 Module reset	Enabled	Warning
4 Module power removed	Enabled	Warning
5 Module power applied	Enabled	Warning
6 Link down	Enabled	Error
7 Link up	Enabled	Warning
8 Primary link up	Enabled	Info
9 Primary link down	Enabled	Error
10 Secondary link up	Enabled	Info
11 Secondary link down	Enabled	Info
12 Standby link up	Enabled	Info
13 Standby link down	Enabled	Info
14 Loop prevention block	Enabled	Warning
15 Loop prevention clear	Enabled	Info
16 Hardware DIP switch change	Enabled	Info
17 Software DIP switch change	Enabled	Info
18 Output relay change	Enabled	Warning
19 Input pin status change	Enabled	Warning
20 Module configuration change	Enabled	Warning
21 Module over temperature	Enabled	Critical
22 Module temperature normal	Enabled	Info
23 Module voltage out of range	Enabled	Error
24 Module voltage range normal	Enabled	Info
25 PoE status error	Enabled	Warning
26 PoE status normal	Enabled	Info
27 ACL access denied	Enabled	Warning
28 Telnet authentication failure	Enabled	Warning
29 Telnet session started	Enabled	Info
30 Telnet session stopped	Enabled	Info
31 FTP authentication failure	Enabled	Warning
32 FTP session started	Enabled	Info
33 FTP session stopped	Enabled	Info
34 Serial console port session started	Enabled	Info
35 Serial console port session stopped	Enabled	Info
36 SSH authentication failure	Enabled	Warning
37 SSH session started	Enabled	Info
38 SSH session stopped	Enabled	Info
39 Wrong password count exceeded	Enabled	Warning
40 SFP inserted	Enabled	Info
41 SFP removed	Enabled	Notice
42 SFP Tx low threshold	Enabled	Error
43 SFP Tx high threshold	Enabled	Error
44 SFP Tx bias current low threshold	Enabled	Error
45 SFP Tx bias current high threshold	Enabled	Error
46 SFP 3.3V low threshold	Enabled	Error

```

47 SFP 3.3V high threshold           Enabled Error
48 SFP temperature low threshold     Enabled Error
49 SFP temperature high threshold    Enabled Error
50 SFP Rx low threshold              Enabled Error
51 SFP Rx high threshold             Enabled Error
52 SFP normal                        Enabled Info
53 Module configuration file corrupted Enabled Info
54 Rate limiting violation           Enabled Info
55 Rate limiting normal              Enabled Info
56 Storm control violation           Enabled Info
57 Storm control clear              Enabled Info
58 Loop prevention block             Enabled Info
59 Loop prevention clear             Enabled Info
>

```

To view the trap log, use the *traps -log* command.

```

> traps -log
Date/Time          Trap # / Description
=====
01/29/2000 07:10:51 PM 34: Serial console port session started user admin
01/29/2000 07:10:13 PM 25: PoE status port 4 error 2
01/29/2000 07:10:07 PM 25: PoE status port 4 error 1
01/29/2000 06:51:32 PM 35: Serial console port session stopped user admin
01/29/2000 06:40:59 PM 25: PoE status port 4 error 2
01/29/2000 06:40:49 PM 25: PoE status port 4 error 1
01/29/2000 06:40:25 PM 34: Serial console port session started user admin
01/29/2000 06:30:48 PM 25: PoE status port 4 error 2
01/29/2000 06:30:43 PM 25: PoE status port 4 error 1
01/29/2000 06:24:02 PM 25: PoE status port 4 error 2

```

## 2.1.48 User Configuration (USER)

The *user* command provides the ability to create and modify user accounts. Up to sixteen user accounts can be configured.

To create or modify user accounts, use the *user* command from the CLI prompt. A list of options is displayed when the *user -h* command is entered.

```
> user

Description:
  user - user configuration
Syntax:
  user [-h]
  user -s
  user [-lto timeout] [-ato timeout] [-artry count] [-fsto timeout]
  user {-d -name uName|-dall}
  user -a -typ uTyp -name uName -pw uPw [-sto timeout]
  user -m [-name uName] [-typ uTyp] [-nname uName] [-pw uPw]
  [-sto timeout] [-kfn filename]
  user -ena|-dis strongpassword
Switches:
-a      add user
-artry  number of authentication retries, [count]: {1..5}, dflt 5
-ato    authentication timeout in sec, [timeout]: {0..300}, dflt 300
-d      delete user
-dall   deletes all users except the logged in user and restores defaults
-dis    disable function: {strongpassword}
-ena    enable function: {strongpassword}
        [strongpassword] strong password is only accepted, dflt disabled
-fsto   ftp session timeout value in sec, [timeout]: {0..3600}, dflt 300
-h      display help information
-kfn    SSH key file name, [filename]: 0 to 45 ASCII characters
-lto    lockout timeout in sec, [timeout]: {1..300}, dflt 300
-m      modify user
-name   user name, [uName]: 1-32 ASCII characters
-nname  new user name, [uName]: 1-32 ASCII
-pw     user password, [uPw]: 1-32 ASCII characters
-s      show current configuration
-sto    session timeout value in sec, [timeout]: {0..3600}, dflt 300
-tyt    user type, [uTyp]: {admin|deny|readonly|readwrite}

>
```

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

The *-a* switch is used to add a user with a unique name and password.

The *-artry* switch defines the number of authentication attempts that a client is allowed to make before authentication lockout.

The *-ato* switch defines the time allowed for the completion of an authentication attempt.

The *-d* switch deletes a user profile by selecting the user number or user name.

The *-dall* switch deletes all user profiles except the currently logged in user.

The *-dis* and *-ena* switches disables or 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 *-fsto* switch configures the FTP session timeout value in seconds.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-kfn* switch defines the username and filename for a specific user.

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

The *-m* switch allows the user account to be modified.

The *-name* switch is used to define the name of a new user.

The *-nname* switch is used to modify the name of a user profile.

The *-pw* switch is used to set the password for a new user. This password is used for Serial, FTP, Telnet and SSH.

The *-s* switch displays the user configuration.

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

The *-typ* switch configures the user access type. Each user name can be configured as:

- admin* An admin user has full read/write privileges including user name and password changes.
- read-write* A read-write user has full read/write privileges with the exception of user name and password operations.
- read-only* A read-only user can only view the configuration of the module and will not be allowed to make any changes.
- deny* A deny user does not have any access to the module.

#### NOTES:

**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 display the user configuration, use the *user -s* command.

```
> user -s

Authentication retries          5
Authentication timeout         300s
FTP Session timeout            300s
Lockout timeout                300s
Strong password check          disabled

User 1 name                    admin
User 1 type                    admin
User 1 password                *****
User 1 SSH keyfile
User 1 session timeout         300s
User 1 status                  serial console port active for 1723s
```

To change the login name, use the *user -m* command.

```
> user -m -name admin -nname Doug
```

### 2.1.49 Firmware Version (VER)

The *ver* command provides the ability to display the firmware version currently running on the module.

A list of options is displayed when the *ver -h* command is entered.

```
> ver -h

Description:
  ver - version status
Syntax:
  ver [-h]
  ver -s
Switches:
-h      display help information
-s      show current status

>
```

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

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-s* switch displays the firmware version on the module.

To display the firmware version on the module, use the *ver -s* command.

```
> ver -s

Model number      3319B-0-24-2
Firmware          v2.x.x  Oct 15 2021, 10:42:38
Bootstrap         v2.x.x
                  prodRev 10 hwRev 10 pcbRev 00ac0100 appAP 0 caps(0x1000067 mtype 168)

>
```

Model number will vary depending on the model.

## 2.1.50 VLAN Table (VLAN)

The *vlan* command adds and displays the configured VLANs on the module.

A list of options is displayed when the *vlan -h* command is entered.

```
> vlan -h

Description:
  vlan - vlan configuration
Syntax:
  vlan [-h]
  vlan -s
  vlan -add vlanId [-vname vlanName]
  vlan -rem vlanList
  vlan -mod vlanId -vname vlanName
  vlan -dall
Switches:
-add  add a VLAN ID, [vlanId]: {1..4095}
-dall delete all VLAN configured settings, instances, and restore defaults
-h    display help information
-mod  modify an existing VLAN ID, [vlanId]: {1..4095}
-rem  remove selected VLANs, [vlanList]: {1..4095|all}
-s    show configuration
-vname VLAN name, [vlanName]: 1-64 ASCII characters

>
```

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

The *-add* switch adds a new VLAN instance.

The *-dall* switch deletes all VLAN configuration setting and restores factory defaults.

The *-h* switch displays the help screen presented above. It is static and provides help information for the specific command.

The *-mod* switch modifies the name of an existing VLAN instance.

The *-rem* switch deletes one or more existing VLAN instances.

The *-s* switch displays the VLAN configuration on the module.

The *-vname* switch specifies a VLAN ID name.

To configure a VLAN instance, use the following command.

```
> vlan -add 200 -vname Video
> vlan -s

VLAN ID 1 "VLAN1"
VLAN ID 100 "data"
VLAN ID 200 "Video"

>
```

Use the *switchport* command to assign the VLAN IDs to specific port numbers.

## 2.1.51 Zone (ZONE)

The *zone* command displays the list of time zone values.

To display the time zone values, use the *zone -h* command from the CLI prompt.

```
> zone -h
```

Zone	Full name	Location	Time Adjustment
GMT	Greenwich Mean Time	Europe	UTC
UTC	Coordinated Universal Time	Europe	UTC
WET	Western European Time	Europe	UTC
Z	Zulu Time Zone	Military	UTC
N	November Time Zone	Military	UTC - 01 hour
O	Oscar Time Zone	Military	UTC - 02 hours
HAT	Heure Avancée de Terre-Neuve	N America	UTC - 02:30 hours
NDT	Newfoundland Daylight Time	N America	UTC - 02:30 hours
ADT	Atlantic Daylight Time	N America	UTC - 03 hours
HAA	Heure Avancée de l'Atlantique	N America	UTC - 03 hours
P	Papa Time Zone	Military	UTC - 03 hours
HNT	Heure Normale de Terre-Neuve	N America	UTC - 03:30 hours
NST	Newfoundland Standard Time	N America	UTC - 03:30 hours
AST	Atlantic Standard Time	N America	UTC - 04 hours
EDT	Eastern Daylight Time	N America	UTC - 04 hours
HAE	Heure Avancée de l'Est	N America	UTC - 04 hours
HNA	Heure Normale de l'Atlantique	N America	UTC - 04 hours
Q	Quebec Time Zone	Military	UTC - 04 hours
EST	Eastern Standard Time	N America	UTC - 05 hours
CDT	Central Daylight Time	N America	UTC - 05 hours
HAC	Heure Avancée du Centre	N America	UTC - 05 hours
HNE	Heure Normale de l'Est	N America	UTC - 05 hours
R	Romeo Time Zone	Military	UTC - 05 hours
MDT	Mountain Daylight Time	N America	UTC - 06 hours
CST	Central Standard Time	N America	UTC - 06 hours
HAR	Heure Avancée des Rocheuses	N America	UTC - 06 hours
HNC	Heure Normale du Centre	N America	UTC - 06 hours
S	Sierra Time Zone	Military	UTC - 06 hours
PDT	Pacific Daylight Time	N America	UTC - 07 hours
HAP	Heure Avancée du Pacifique	N America	UTC - 07 hours
HNR	Heure Normale des Rocheuses	N America	UTC - 07 hours
MST	Mountain Standard Time	N America	UTC - 07 hours
T	Tango Time Zone	Military	UTC - 07 hours
PST	Pacific Standard Time	N America	UTC - 08 hours
AKDT	Alaska Daylight Time	N America	UTC - 08 hours
HAY	Heure Avancée du Yukon	N America	UTC - 08 hours
HNP	Heure Normale du Pacifique	N America	UTC - 08 hours
U	Uniform Time Zone	Military	UTC - 08 hours

Only a partial list is shown.

## **3.0 APPENDIX A: FIRMWARE UPDATE**

### **3.1 OVERVIEW**

Appendix A describes the procedure for updating the firmware using ftp and web interface.

### **3.2 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.

### **3.3 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.**

### **3.4 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

**NOTE: OmniConverter GPoE+/M 8 Port RJ-45 Fixed Fiber models (9520-x-x8-xx - 9531-x-x8-xx) and RuggedNet GPoE+/Mi 8 Port RJ-45 Fixed Fiber models (9540-x-x8-xx - 9551-x-x8-xx) with firmware 2.3.9 cannot be downgraded to any firmware revision. The models can be upgraded from 2.3.9.**

Verify the IP address of the module by using the *ip* command.

```
> ip -s

IPv4                enabled
IPv6                enabled

IP 1
  MAC address       00-06-87-02-86-E0
  IPv4 address      192.168.1.124 (192.168.1.124)
  IPv4 subnet mask  255.255.255.0 (255.255.255.0)
  IPv4 gateway address 192.168.1.1 (*)
  DNS               disabled
  DNS address       *
  DHCP              enabled
  Relay             disabled
  Relay Circuit ID  enabled
  Relay Remote ID   enabled
  Relay type        replace
  Relay server IP   0.0.0.0
  v6Relay           enabled
  v6Relay Circuit ID enabled
  v6Relay Remote ID enabled
  IPv6 interface    stateless
  IPv6 address      fe80::206:87ff:fe02:86e0/64
                   ::/64
  IPv6 gateway address fe80::1
  DHCPv6            disabled
```

To enable FTP, use the *protocol* command.

```
> protocol -ena ftp
```

The default ftp password is public. To change the password, use the *user* command.

```
> user -m -name admin -pw <new password>
```

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 *ver -s* command.

```
> ver -s
```

```
Model number      3342B-0-14-2Z
Firmware          v2.2.x  Oct 15 2021, 10:42:38
Bootstrap         v2.x.x
                  prodRev 10 hwRev 10 pcbRev 00ac0100 appAP 0 caps(0x1000067 mtype 168)
```

## 4.0 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.

©2022 Omnitron Systems Technology, Inc.

## 5.0 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