

Network Switch Software Documentation

11/24/21

1.	Revision Table	3
2.	Default Users	4
3.	Port Numbering	5
4.	Serial Console	5
4.1.	BIST REPORT	5
4.2.	BIST TEST	5
4.3.	DHCP CLIENT	5
4.4.	GET ARP	6
4.5.	GET DHCP	6
4.6.	GET DROP	6
4.7.	GET LINK STATUS	6
4.8.	GET LACP	6
4.9.	GET MULTICAST	6
4.10.	GET PORT COUNTERS	6
4.11.	GET SERDES STATUS	7
4.12.	GET VLAN	7
4.13.	CLEAR PORT COUNTERS	7
4.14.	NTP	7
4.15.	PING ENABLE	8
4.16.	PBIST CONFIGURE	8
4.17.	SET DHCPSEVER	9
4.18.	SET IGMP	10
4.19.	SET PORT ROUTE	10
4.20.	SET PORT SPEED	10
4.21.	SET SNMP	11
4.22.	SET VLAN	12
4.23.	SET MTU	13
4.24.	SET LUA	13
4.25.	SYSLOG	13
4.26.	SWITCH REPORT	13
4.27.	STATIC	14
4.28.	SSH	14
4.29.	WEBSERVER	14
4.30.	VERSION	14
4.31.	EXIT	14
5.	User Triggered Network Access Functions	15
5.1.	SNMP	15
5.2.	SSH Access	18
5.3.	TFTP Client	19
5.4.	Secure FTP	20
5.5.	SYSLOG Usage	21
5.6.	Firmware Version Server	24
5.7.	NTP Client/Server	24
5.8.	DHCP Client/Server/Static	24
6.	Configuration Files	25

1. Revision Table

Date	Revisions
7/31/20	Added rev table. Changed passwords/default users in section 2 Changed all DHCP commands Changed all SNMP commands Changed all VLAN commands Updated SNMP examples for V3 and MIB usage in section 5
09/08/20	Updated DHCP and VLAN commands
08/27/21	Added command descriptions for GET ARP GET DHCP GET DROP GET LACP GET MULTICAST SET VLAN LACP SET LUA SET MTU Removed commands SET POLARITY SET FEC
11/24/21	Added commands SCRUB ALL MEMORY SET LACP

2. Default Users

At factory boot/reflash, there are two users and passwords configured

Username = root

Password = amphenol

This will allow direct Linux command line access when using an SSH connection. Direct Linux command line access is not allowed using the serial port.

Username = admin

Password = amphenol

This will allow access to the switch's CLI functions to manage all port/routing/etc parameters. This username/password can be accessed through the serial port and SSH.

The web interface, if enabled, provides a single password and no username for login.

The password for login to the web interface is "amphenol"

3. Port Numbering

Any command in the CLI that requires a value for a PORT will support a series of range/descriptions. Examples are as follows

- “9” → a single port such as port #9
- “5,6,7” or “10,22,35” → individual port numbers
- “9-20” → specify a range of ports from port 9 through port 20
- “*” → include all available ports
- “1,4,7,20-30” → specify ports 1,4,7 and port numbers 20 through 30

4. Serial Console

The following sections detail the commands available in the CLI Switch Software.

4.1. BIST REPORT

The command will display the results of the previously issued BIST/PBIST test.

Examples:

- “BIST REPORT” → displays the test results of the previously run BIST TEST
- “BIST REPORT PBIST” → display the test results for the PBIST power-on test results

4.2. BIST TEST

This command will perform a user-initiated bit-test using internal/external loopback mode on a selected port. The default is internal loopback mode.

Examples:

- “BIST TEST 22” → Runs an internal loopback test for port 22
 - “BIST TEST 12-20 EX” → Runs an external loopback test for ports 12 through 20.
- This requires the ports are physically looped back onto each other at the pin/hardware level.

4.3. DHCP CLIENT

This command is used to enable/disable the DHCP client process on both the Management and Fabric ports. If the DHCP client is set too, then the IP settings should be configured using the STATIC command.

Examples:

- “DHCPCLIENT ON” → Turns on the DHCP Client process for the fabric side port
- “DHCPCLIENT OFF M” → Turns off the DHCP client process for the management port

4.4. GET ARP

This command can be used to view the current ARP table for all discovered IP addresses and their associated MAC addresses.

Note that IP addresses associated with a VLAN that is set to “Private” access mode may not have MAC addresses shown or the MAC address may be all zero. A “Private” VLAN is essentially Layer2 routing only therefore ARP packets are not processed by the switch and MAC discovery is not currently implemented for “Private” VLANs.

4.5. GET DHCP

This command returns the debug/trace status of the DHCP server across all VLANs. This can be used to view the DHCP messages between the switch and any clients.

4.6. GET DROP

This command returns a debug trace of all drop counters for the ports and internal bridge functions within the switch.

4.7. GET LINK STATUS

This command will produce a report of the link/speed/duplex/polarity status for all ports on the switch.

4.8. GET LACP

This command returns a port list of all ports that have negotiated a LACP aggregation link with an outside link partner(s).

4.9. GET MULTICAST

This command returns a list of all multicast addresses and list of all ports that have subscribed, using IGMP, to any of the multicast streams. Note that this requires IGMP to be active.

4.10. GET PORT COUNTERS

This command will produce a report of all TX, RX, and RX Error counters on the switch.

Examples: “GET PORT”

This command will show the counters for all ports.

Examples: “GET PORT 2 COUNTERS”

This command will show only the counters for port #2

4.11. GET SERDES STATUS

This command can be used to generate an eye-diagram of the receiver for any port.

Example: "GET SERDES STAUS 25"

This will provide an ascii style eye diagram print out over the CLI and also a value indicating the height and width of the inbound eye.

4.12. GET VLAN

This command will return the parameters/settings for the currently selected VLAN, any specific VLAN by index, or show a list of all configured VLANs.

Examples:

"GET VLAN" → shows a parameter/settings list for the currently selected VLANs

"GET VLAN 5" → shows the parameter/settings for VLAN index 5

"GET VLAN ALL" → shows the parameter/settings for all enabled VLANs

4.13. CLEAR PORT COUNTERS

The command can be used to clear all of the counters or counters on a specified port.

Example: "CLEAR PORT"

This command will clear all the port counters on all ports.

Example: "CLEAR PORT 10 COUNTERS"

This command will clear only the counters on Port 10

4.14. NTP

This command is used to enable the NTP client/server and set the external NTP sync address.

Examples:

"NTP ON 129.6.15.32" → This will set the NTP process to "ON" and the system will synchronize with an external server at 129.6.15.32. Note that this also requires the management/fabric port to be linked to a worldwide available network

"NTP ON" or "NTP OFF" → This can be used to enable/disable the NTP client/server process

4.15. PING ENABLE

This command is used to enable/disable the keepalive/ping/heartbeat function. This function allows the software to ping a remote host and track the number of pings and replies. The ping results are viewable under the “SWITCH REPORT” function

Example:

“PING ON” → this will turn on/off a currently configured ping function

“PING ON 192.169.1.1 5” → this will turn on the ping function and will issue pings to IP 192.169.1.1 at an interval of 5 seconds per ping

4.16. PBIST CONFIGURE

This command is used to define the ports that will be tested, at power up, using the on-board loopback test capability.

Example:

“PBIST CONFIGURE OFF” → disable all ports for pbist test

“PBIST CONFIGURE *” → enable all ports for pbist test

“PBIST CONFIGURE 1,2,5-10” → set ports 1,2,5,6,7,8,9,10 pbist testing

4.17. SET DHCPSEVER

This command is used to enable/disable the DHCP server function on the system. When enabled, the software can assign DHCP addresses to outside devices and its own management/fabric port.

These commands apply on a per VLAN basis allowing the user to specify individual DHCP settings for each VLAN. See the command "SET VLAN" to specify the current VLAN target that these commands will apply to.

Examples:

"SET DHCPSEVER ON" This will turn on (or off) the DHCP Server Function

"SET DHCPSEVER SUBNET 192.168.1.0": Assigns the subnet address for the DHCP Server

"SET DHCPSEVER BASE 192.168.1.50": Assigns the starting addresses for DHCP handout

"SET DHCPSEVER RANGE 50": Assigns the IP address range (0-255) for the addresses

"SET DHCPSEVER GATEWAY 192.168.1.1": Assigns the IP address gateway

"SET DHCPSEVER NETMASK 255.255.255.0": Assigns the netmask.

"SET DHCPSEVER TFTPSEVER 192.168.1.10": Assigns TFTP Server for DHCP Option 66

"SET DHCPSEVER TFTPFILE boot.bin": Assigns TFTP boot file for DHCP Option 67

"SET DHCPSEVER RESTART": this will kill and restart the DHCP server

The DHCP Server will handout addresses for each VLAN configured on the switch.

By default, the switch provides four VLANs as defined below

VLAN1: Ports 1,2,3,4,5,6,7,8,41

VLAN2: All remaining ports (NOTE: routing is disabled by default on these ports)

During DHCP assignment, the addresses for the DHCP Server are offset for each VLAN.

Using the defaults, the DHCP Server is configured as follows

SUBNET:192.168.1.0

BASE:192.168.1.50

RANGE:50

VLAN1: allows IP Assignments in the range of 192.168.1.50 through 192.169.1.100

VLAN2: allows IP Assignments in the range of 192.168.2.50 through 192.169.2.100

Note: After changing any DHCP settings, the user should issue the command "SET DHCPSEVER RESTART" to apply the new values in the DHCP process.

4.18. SET IGMP

Enable/Disable IGMP snooping on all VLANs. When enabled, each individual VLAN will track IGMP v2/v3 membership request messages. The messages will be used to enable/disable packet replication/mirroring for multicast packets on each VLAN. If IGMP is disabled, then multicast packets will flood all ports on each VLAN.

Example:

“SET IGMP ON” → Enable IGMP snooping

4.19. SET LACP

This command allows assignment of any ports into an LACP/LAG group. Examples of this command are as follows.

Example:

“SET LACP 1 5,6,7” → sets ports 5,6,7 into LACP aggregation group #1

“SET LACP RESPAWN” → rebuild the LACP indexes and attempt to renegotiate a LACP link

4.20. SET PORT ROUTE

Enable/Disable routing on a port. When enabled, this port will be fully routable as an any-to-any vlan/maclearning network port.

Example: “SET ROUTE 27 ON”

This will turn routing “ON” for Port#27

4.21. SET PORT SPEED

Configure the link speed for individual ports. These can be 10/100/1G/10G/SFI/OFF

Note that “OFF” will electrically disable the port and remove it from the routing pool.

Note: All 10GBase-T ports are auto-negotiated for speed, no user intervention is needed.

Example: “SET PORT 30 10G”

This will set Port#30 to a speed of 10Gb/s

4.22. SET SNMP

This command is used to enable/disable SNMP server and configure the V1/V2/V3 settings.

Example:

“SET SNMP ON” → activate the SNMP traps

“SET SNMP RESTART” → restart the SNMP traps

“SET SNMP OFF” → disable the SNMP process

SNMP V1 and V2 Examples:

“SET SNMP V1 ADDR 192.168.8.2” → assign the server IP for SNMP

“SET SNMP V1 PORT 162” → assign the port number for SNMP

“SET SNMP V1 COMMUNITY public” → assign the community value

“SET SNMP V1 COMMUNITY OFF” → disable the V1 or V2 SNMP functions

“SET SNMP V1 TRAPS ON” → enable/disable outbound SNMP traps

Note: The user can use values “SNMP V1” or “SNMP V2” for configuring either settings for v1 and v2 mode.

SNMP V3 Examples:

“SET SNMP V3 USER admin” → set the login username

“SET SNMP V3 PASSWORD mypassword” → set the authentication and private password

“SET SNMP V3 AUTH MD5” → set the authentication mode to MD5 or SHA or OFF

“SET SNMP V3 PRIV DES” → set the privacy encoding mode to DES or AES or OFF

“SET SNMP V3 ADDR 192.168.8.2” → assign the server IP for SNMP

“SET SNMP 192.168.8.22” → assign the server IP to 192.168.8.22 for outbound SNMP traps

“SET SNMP V3 TRAPS OFF” → enable/disable outbound SNMP traps

4.23. SET VLAN

This command is used to assign up to the individual VLANs assignments for port grouping, aggregation, and to specify the current VLAN target for subsequent “SET VLAN” commands

“SET VLAN 10” → This command will select VLAN #10 within the range of 0-127. This command format is used to set the currently selected VLAN that subsequent commands will target.

“SET VLAN 12 815” → This command will select VLAN #12 and set its VLAN-ID tag to 815

“SET VLAN PORTS 1,2,3,4” → assign ports 1,2,3,4 the currently selected VLAN

“SET VLAN PORTS OFF” → this will remove all physical ports from the currently selected VLAN and disable/revoke this VLAN from the active pool.

“SET VLAN TARGET 900” → assign the currently selected VLAN for egress on VLAN-ID 900. This will cause all outbound packets on the currently selected VLAN to egress on the VLAN associated with VLAN-ID tag 900. This can be used to configure port aggregation between VLANs.

“SET VLAN ACCESS XXXXX” → this command configures the VLAN for either “private” or “routeable” mode. In private mode, only IP addresses on the assigned VLAN can communicate. In “routeable” mode, IP/MAC address pairs are used to perform Layer3 bridging between VLANs and the associated gateways.

Example: SET VLAN ACCESS PRIVATE
 SET VLAN ACCESS ROUTEABLE

“SET VLAN MODE XXXXX” → this command configures the VLAN mode for either “WAN”, “LAN” or “TAGGED” mode.

Examples:

SET VLAN WAN → this command configures the selected VLAN to operate as an uplink/wan port. Any addresses not associated with IP addresses on the assigned VLANs will be routed out of the switch on the “WAN” port.

SET VLAN LAN → this command configures the selected VLAN to operate as an untagged downstream port for standard IPv4 addresses.

SET VLAN TAGGED → this command configures the selected VLAN to operate in 802.11 tagged mode so that only packets that match the assigned VLAN tag can be switched/routed on the vlan.

Note: After the user has applied all VLAN updates, issue the command “SET VLAN RESTART” to rebuild the VLAN structure and apply all changes.

4.24. SET MTU

This command will globally adjust the packet MTU size on the switch. The default MTU is 1500 and can be set to a maximum of 9000. The current MTU size can be seen under the “SWITCH REPORT” readout.

4.25. SET LUA

This command is for debug/extended configuration only and can be used to enable the default MARVELL LUA command line interpreter. “SET LUA ENABLE” will shift the CLI to use the LUA menu. The command “CLIEXIT” will return back to the standard high level CLI/menu.

4.26. SCRUB ALL MEMORY

This command is used to erase the operating system and filesystem image, returning the system to a raw factory state. The format for the command is “SCRUB ALL MEMORY {PASSWORD}” where the password is the main login password used to access the CLI.

4.27. SYSLOG

This command configures the syslog capabilities of the software. If enabled, all entered commands will be echoed to a remote SYSLOG server. The default port for SYSLOG is 514.

Example:

“SYSLOG ON 192.169.1.21” → turn on syslog functions to target server 192.169.1.21

“SYSLOG OFF” → disable syslog functions

“SYSLOG ON 192.169.1.23 999” → turn on syslog to target server 192.169.1.23 using port 999

4.28. SWITCH REPORT

This command provides a summary of entire operating state of the switch. This includes PCB/Component temperatures, ip address, time/date stamps, server controls, and additional values.

Example: "SWITCH REPORT"

4.29. STATIC

This command is used to assign the manual IP/Netmask/Gateway/DNS addresses to the management/fabric port. These will be used when the DHCPCLIENT is "OFF".

Examples:

"STATIC IP 192.169.1.44 M" → This will set the static IP setting to 192.169.1.44 for the Management port

"STATIC IP 192.169.1.45" → This will set the static IP setting to 192.169.1.45 for the fabric port.
Similar methods can be used for Netmask, Gateway, and DNS ports.

4.30. SSH

This command is used to enable/disable SSH access to the system.

Examples:

"SSH ON" → Activate the SSH process for Linux/cli access

"SSH OFF" → Disable the SSH process

4.31. WEBSERVER

This command is used to enable/disable the webserver capabilities of the system.

Examples:

"WEBSERVER ON" → Activate webserver and allow user access from a browser

"WEBSERVER OFF" → Disable the webserver

4.32. VERSION

This command reports the version of the CLI software for switch management functions.

4.33. EXIT

This command exits the current CLI session and returns to the login prompt.

5. User Triggered Network Access Functions

5.1. SNMP

If enabled, an SNMP MIB/Browser and/or trap receiver can be used to communicate with the system software.

A typical browser such as the iReasoning MIB Browser may be used. The browser should target the IP address of the controller (default 192.169.1.44)

Link up/down traps can be received at default address 192.169.1.21, or a different address as configured by the user. This can be adjusted using the SNMP command in the CLI to define the remote address (i.e. the PC that is running the MIB/Browser/Trap-Receiver)

Note that the appropriate MIB modules should be loaded using the File->Load/Unload MIBs.

The screenshot shows the iReasoning MIB Browser application. The MIB Tree on the left displays a hierarchy starting from 'iso.org.dod.internet.mgmt.mib-2', with expanded sections for 'system', 'interfaces', 'snmp', and 'ifMIBObjects'. The 'ifTable' is selected under 'ifMIBObjects'. The 'Result Table' on the right displays a list of interface entries with columns for Name/OID, Value, Type, and IP:Port. The table contains 20 entries, all of type 'OctetString' and pointing to IP address '192.169.1.44:161'. A status bar at the bottom shows the path: 'iso.org.dod.internet.mgmt.mib-2.ifMIB.ifMIBObjects.ifTable'.

Name/OID	Value	Type	IP:Port
ifName.2	eth0	OctetString	192.169.1.44:161
ifName.3	eth1	OctetString	192.169.1.44:161
ifName.37	aldrinphy0	OctetString	192.169.1.44:161
ifName.38	aldrinphy1	OctetString	192.169.1.44:161
ifName.39	aldrinphy2	OctetString	192.169.1.44:161
ifName.40	aldrinphy3	OctetString	192.169.1.44:161
ifName.41	aldrinphy4	OctetString	192.169.1.44:161
ifName.42	aldrinphy5	OctetString	192.169.1.44:161
ifName.43	aldrinphy6	OctetString	192.169.1.44:161
ifName.44	aldrinphy7	OctetString	192.169.1.44:161
ifName.45	aldrinphy8	OctetString	192.169.1.44:161
ifName.46	aldrinphy9	OctetString	192.169.1.44:161
ifName.47	aldrinphy10	OctetString	192.169.1.44:161
ifName.48	aldrinphy11	OctetString	192.169.1.44:161
ifName.49	aldrinphy12	OctetString	192.169.1.44:161
ifName.50	aldrinphy13	OctetString	192.169.1.44:161
ifName.51	aldrinphy14	OctetString	192.169.1.44:161
ifName.52	aldrinphy15	OctetString	192.169.1.44:161
ifName.53	aldrinphy16	OctetString	192.169.1.44:161
ifName.54	aldrinphy17	OctetString	192.169.1.44:161
ifName.55	aldrinphy18	OctetString	192.169.1.44:161
ifName.56	aldrinphy19	OctetString	192.169.1.44:161
ifName.57	aldrinphy20	OctetString	192.169.1.44:161
ifName.58	aldrinphy21	OctetString	192.169.1.44:161

iso.org.dod.internet.mgmt.mib-2.ifMIB.ifMIBObjects.ifTable

iReasoning MIB Browser

FileEditOperationsToolsBookmarksHelp

Address: 192.169.1.44Advanced...OID: .1.3.6.1.2.1.31.1.1Operations: Get NextGo

SNMP MIBs

MIB Tree

iso.org.dod.internet.mgmt.mib-2

system

sysDescr

sysObjectID

sysUpTime

sysName

sysServices

interfaces

snmp

ifMIB

ifMIBObjects

ifTable

ifTableLastChange

Result Table

Trap Receiver x

OperationsTools

linkDown

linkDown

linkUp

linkUp

linkUp

linkUp

linkUp

linkUp

Description

Source

Time

Severity

Source: 192.169.1.44Timestamp: 37 minutes 42 secondsSNMP Version: 2

Trap OID: linkUpCommunity: secret

Variable Bindings:

Name: sysUpTime.0Value: [TimeTicks] 37 minutes 42 seconds (226236)

Name: snmpTrapOIDValue: [OID] linkUp

Name: ifDescr.71Value: [OctetString] AldrinPort-35

Name: snmpTrapEnterprise.0Value: [OID] .1.3.6.1.4.1.8072.3.2.10

NameifTable

OID.1.3.6.1.2.1.31.1.1

MIBIF-MIB

SyntaxSEQUENCE OF IfEntry

Accessnot-accessible

Statuscurrent

DefVal

AugmentsifEntry

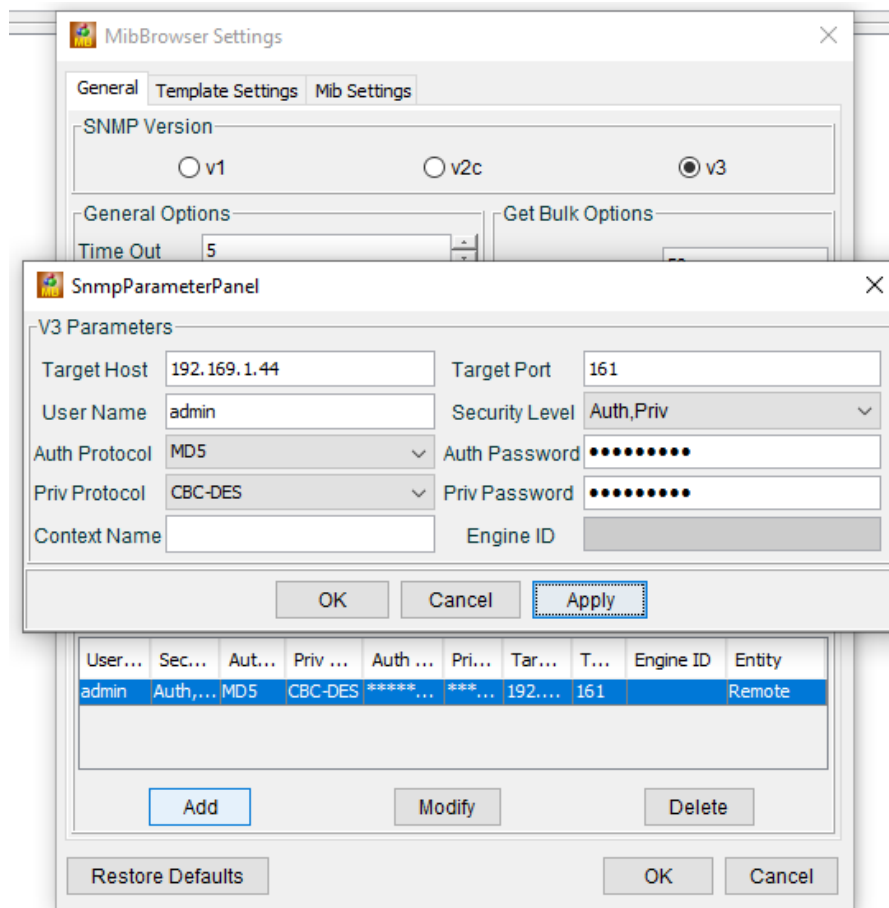
A list of interface entries. The number of entries is given by the value of ifNumber. This table contains additional objects for the interface table.

iso.org.dod.internet.mgmt.mib-2.ifMIB.ifMIBObjects.ifTable

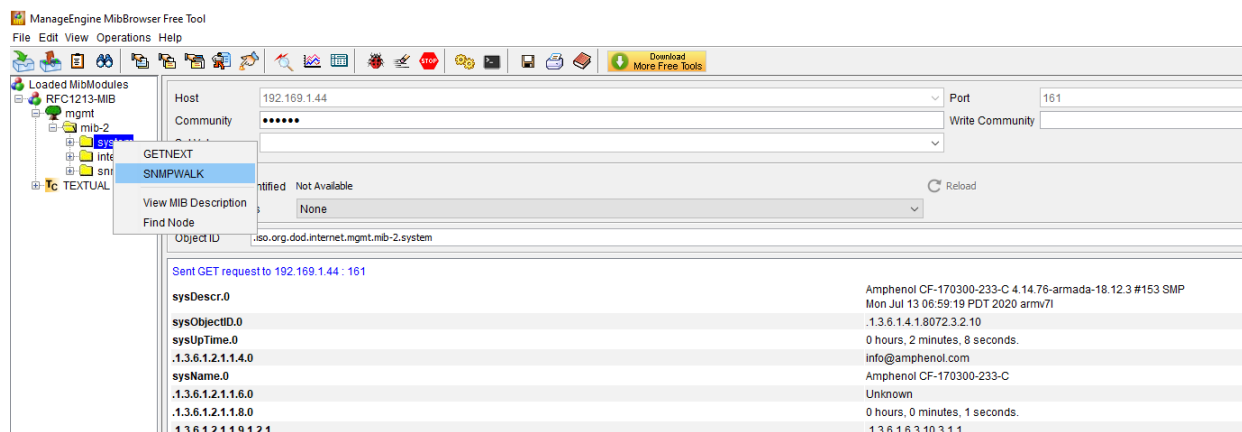
16

Additionally, for SNMPv3 login access. The MIB Browser from ManageEngine provides free usage for SNMPv3.

The Edit->Settings window allows the user to specify the login credentials for SNMPv3 and validate with the server for MIB access.

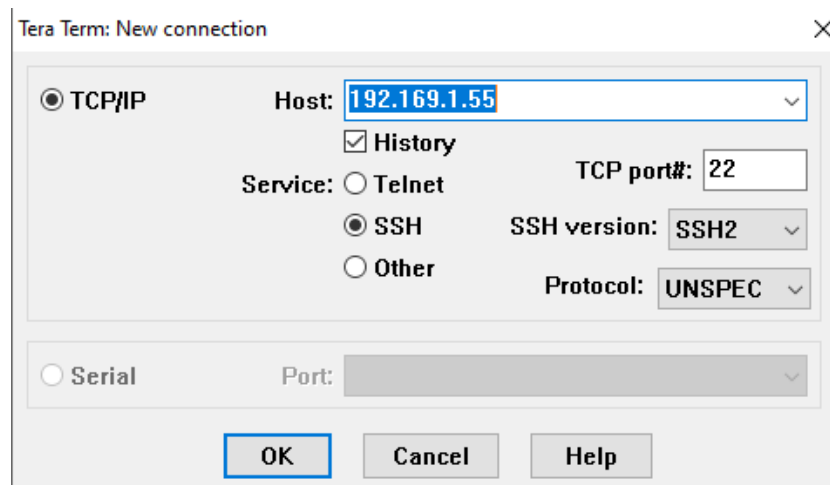


Once authenticated, the user can right click on the specific MIBs in the MIB tree and perform a get/walk function.



5.2. SSH Access

If enabled, a remote client can login to the system's local IP address using SSH such as through Putty or TeraTerm/etc.



A key-exchange will occur along with a username/password combination.

The username/password can be

- 1) Default "root" login to gain direct access to the Linux command line shell.
- 2) Default "switch" login to gain direct access to the CLI for network switch management

5.3. TFTP Client

TFTP transfers can be issued manually using the Linux “tftp” command with the options shown below

Usage: tftp [OPTIONS] HOST [PORT]

Transfer a file from/to tftp server

- l FILE Local FILE
- r FILE Remote FILE
- g Get file
- p Put file
- b SIZE Transfer blocks of SIZE octets

An example is “tftp -l test1 -r test2 -p 192.169.1.33”

This will transfer file “Test1” to the TFTP server at 192.169.1.33 and it will be named “Test2” when saved on the remote server.

To test this, use the TFTP64 server program

5.4. Secure FTP

A secure FTP transfer may be performed using the linux SCP command with the following parameters

```
usage: scp [-346BCpqrTv] [-c cipher] [-F ssh_config] [-i identity_file]
        [-J destination] [-l limit] [-o ssh_option] [-P port]
        [-S program] source ... target
```

To test this, use the buru secure ftp demo program.

Buru must be setup as follows:

From windows command line type

```
"buru user add theuser"
```

Follow the prompts to assign a password to the username "theuser"

```
"buru path -v / -p c:\ftp -u theuser"
```

This will set the path "c:\ftp" as the home directory for "theuser"

```
"buru run"
```

This will start the server

From the linux command line shell, issue a command such as

```
sshpass -p thepassword scp -S dbclient ledtest theuser@192.169.1.21:/
```

The "sshpass -p thepassword" sets the password to be used

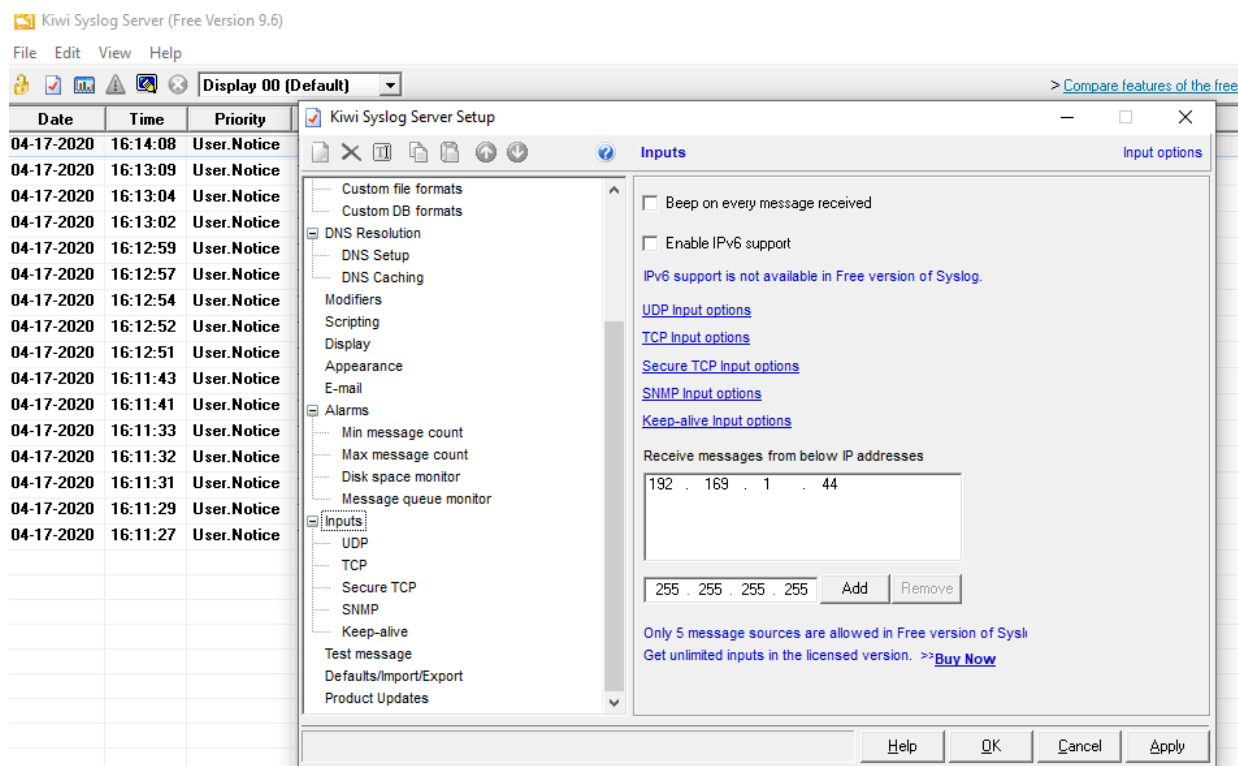
The "scp ledtest theuser@192.169.1.21:/" calls the scp (secure file transfer program) to transfer the file ledtest to the server at 192.169.21. The username for the server login is "theuser" Ensure that the buru server is located at 192.169.1.21 or similar address/etc.

Completion of this command will then transfer the file "ledtest" to the server's user path "c:\ftp" using secure file transfer protocol

5.5. SYSLOG Usage

The SYSLOG function can be used with the “Kiwi Syslog Server Free Version 9.6”
Install the SYSLOG program on a remote PC.

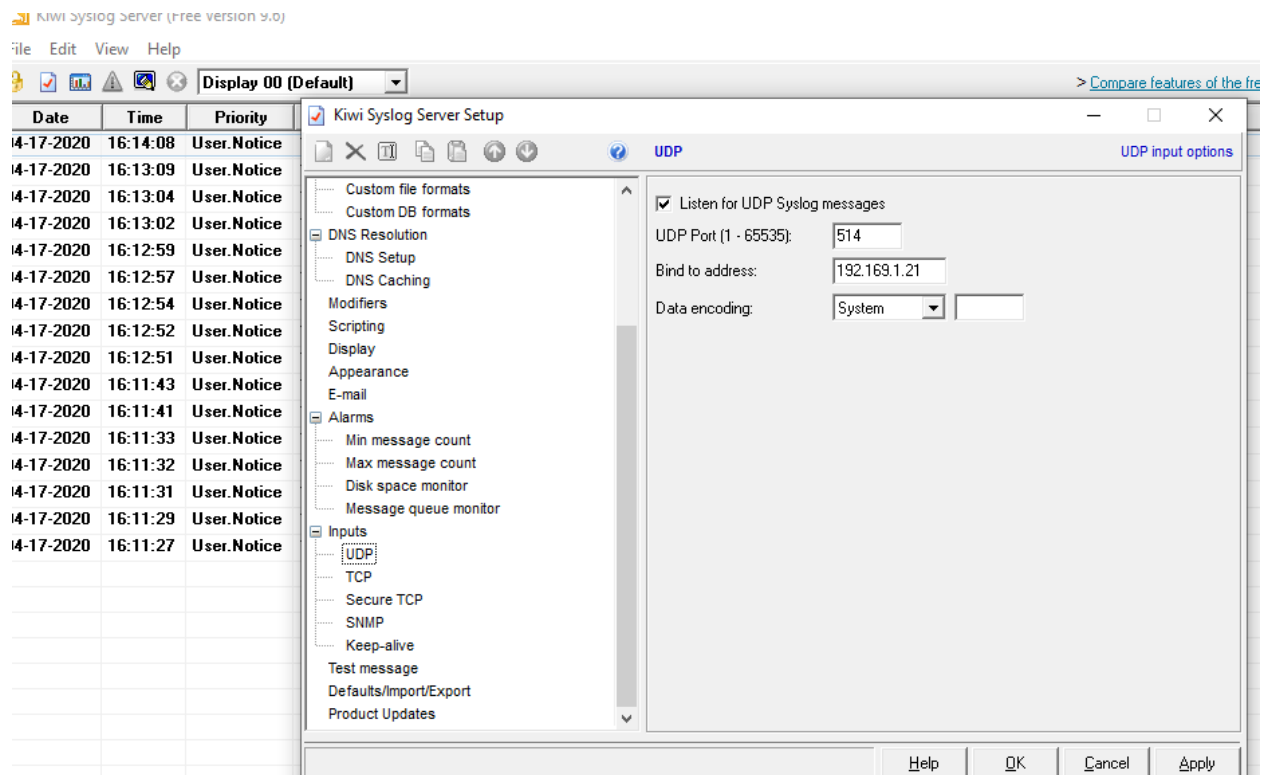
Configure the File→Setup→Inputs to allow the syslog server to receive messages from the IP address of the physical switch unit.



Configure the Inputs→UDP to allow the software to listen to UDP Syslog messages.

Ensure that the “bind to address” is the IP address of the PC that is running the Kiwi Syslog Server.

Ensure that the physical switch software is configured to target the same IP/Port so that it will broadcast SYSLOG messages to the proper PC/SyslogServer



Once configured, all entered commands and events on the CLI should be remotely logged by the syslog server.

Kiwi Syslog Server (Free Version 9.6)

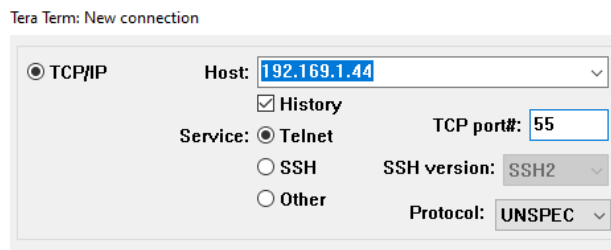
File Edit View Help

 Display 00 (Default) ▼

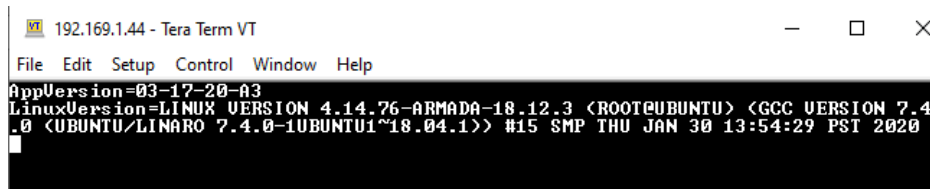
Date	Time	Priority	Hostname	Message
04-17-2020	16:14:08	User.Notice	192.169.1.44	SANDIA TTYS0: SW RE
04-17-2020	16:13:09	User.Notice	192.169.1.44	SANDIA TTYS0: SW RE
04-17-2020	16:13:04	User.Notice	192.169.1.44	SANDIA TTYS0: SW RE
04-17-2020	16:13:02	User.Notice	192.169.1.44	SANDIA TTYS0: SW RE
04-17-2020	16:12:59	User.Notice	192.169.1.44	SANDIA TTYS0: SW RE
04-17-2020	16:12:57	User.Notice	192.169.1.44	SANDIA TTYS0: SW RE
04-17-2020	16:12:54	User.Notice	192.169.1.44	SANDIA TTYS0: PING ON
04-17-2020	16:12:52	User.Notice	192.169.1.44	SANDIA TTYS0: ?
04-17-2020	16:12:51	User.Notice	192.169.1.44	SANDIA SANDIA: LOGIN ACCEPTED
04-17-2020	16:11:43	User.Notice	192.169.1.44	SANDIA SANDIA: SESSION LOGOUT
04-17-2020	16:11:41	User.Notice	192.169.1.44	SANDIA TTYS0: SE RO 2 ON
04-17-2020	16:11:33	User.Notice	192.169.1.44	SANDIA TTYS0: ?
04-17-2020	16:11:32	User.Notice	192.169.1.44	SANDIA TTYS0: GE LI
04-17-2020	16:11:31	User.Notice	192.169.1.44	SANDIA TTYS0: GE PD
04-17-2020	16:11:29	User.Notice	192.169.1.44	SANDIA TTYS0: SW RE
04-17-2020	16:11:27	User.Notice	192.169.1.44	SANDIA SANDIA: LOGIN ACCEPTED

5.6. Firmware Version Server

A TCP Firmware Version Server is enabled on Port 55 of the IP address for the management/fabric port. Connecting to this IP and Port Combination will provide a single reply echo of the CLI version and the Linux O/S version.



An example response is shown below



5.7. NTP Client/Server

The NTP protocol client/server runs at boot if enabled in the configuration. The default is to be enabled.

The NTP client attempts to access the NTP East Coast Server at 129.6.15.32 (ntp-d.nist.gov) for time synchronization.

Remote network devices can then access the NTP Server on the board (using the board's static/dhcp assigned address) to then perform relay synchronization using the NTP time stamps.

5.8. DHCP Client/Server/Static

Three IP assignment methods are available. DHCP Server, Client and Static mode.

The default is to have the management port appear at 192.169.1.44 and the fabric port will attempt to obtain a DHCP address from a remote DHCP server/router.

The DHCP mode and/or static IP assignments can be adjusted through the CLI menu.

6. Configuration Files

The switch boot configuration is stored as an ascii readable text file in the “/etc/amphenol.cfg” file. An example view is shown below.

```
/ #
/ # cat /etc/amphenol.cfg
#PHYSICAL,SPEED,MODE,ROUTE,TXP,RXP,TXAMP,TXEMP0,TXEMP1,TXAMPB,TXEMP0B,TXEMP1B,FEC,OFF
0,3,16,1,0,0,0,4,0,0,9,10,1,0
1,3,16,1,0,0,0,4,0,0,9,10,1,0
2,3,16,1,0,0,0,4,0,0,9,10,1,0
3,3,16,1,0,0,0,4,0,0,9,10,1,0
4,3,16,0,0,0,0,4,0,0,9,10,1,0
5,3,16,0,0,0,0,4,0,0,9,10,1,0
6,3,16,0,0,0,0,4,0,0,9,10,1,0
7,3,16,0,0,0,0,4,0,0,9,10,1,0
8,3,16,1,0,0,0,4,0,0,9,10,1,0
9,3,16,1,0,0,0,4,0,0,9,10,1,0
10,3,16,1,0,0,0,4,0,0,9,10,1,0
11,3,16,1,0,0,0,4,0,0,9,10,1,0
12,3,16,0,0,0,0,4,0,0,9,10,1,0
13,3,16,0,0,0,0,4,0,0,9,10,1,0
14,3,16,0,0,0,0,4,0,0,9,10,1,0
15,3,16,0,0,0,0,4,0,0,9,10,1,0
```

This example shows the configuration for the network ports. The amphenol.cfg file also contains all other startup/control values for SSH/DHCP/etc.

This file can be moved/imaged between different systems using the linux shell and sftp/tftp/ftp access. The linux shell can be accessed through an SSH connection with the software.