Network Switch Software Documentation
09/30/22

Table of Contents

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
01/26/22	Clarified username/password combinations and added/updated commands below SET NAME SET DHCPSERVER HOSTNAME
02/03/22	Added “DISABLE” mode to SET IGMP Several commands have been updated to use the "SET / GET" terminology these commands are DHCPCLIENT, all commands relating to BIST, SYSLOG, NTP, STATIC, SSH, WEBSERVER, VERSION, AND SWTICH REPORT
03/30/22	Added commands SET SPANTREE SET SPANPORTS GET SPANTREE SET QOS BUFFERS Removed obsolete data on configuration files
05/26/22	Added commands SET MIRROR GET MIRROR Extended SPANTREE for assignment per VLAN and RSTP auto-detect
06/20/22	Added commands SET TRUNK GET TRUNK Added option “SET MIRROR VLAN” to mirror an entire VLAN
07/21/22	Changed SET IGMP to SET IGMP SNOOP Added SET IGMP PROXY Added SET IGMP STATIC Added SET TELNET Added SET FEC Added SET RADIUS Added SET TACACS Added dedicated sections on RADIUS/TACAS Added SET ACL and GET ACL

Date	Revisions
08/15/202	Added Commands GET DAEMON SET PIM SET RIP ADDED PIM/RIP commands per VLAN under the “SET VLAN” commands Changed command SET WEBSERVER
09/28/22	Changed GET MIRROR Changed GET VLAN Updated documentation for MIRROR commands

2. Default Users

At factory boot/reflash, the following passwords and login methods are defined

2.1. Telnet/SSH Linux Shell Access

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.

2.2. Telnet/SSH Switch CLI Access

Username = switch
Password = amphenol

This password combination will redirect the telnet/ssh process over to the common CLI switch management task. A secondary login (see below) will then be required.

2.3. Serial RS232 CLI Access

Username = admin
Password = amphenol

This password combination is required at the Serial RS232 port to gain access to the management CLI.

This password combination must also be entered as a secondary security step when using Telnet or SSH (see section above) to access the management CLI over ethernet.

The serial port interface uses a single TX/RX pair and communicates at 115,200 baud, 8 data bits, 1 stop bit, and no parity.

2.4. Webserver

Password = amphenol

The web interface provides a single password only field for accessing the web-based status reporting pages. The web interface, if enabled, provides a single password and no username for login.

2.5. SNMP

Username = admin
Password = amphenol

This password combination is used for SNMPv3 authentication.

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. Command Line Console

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

4.1. GET ACL

This command will display all configured user ACLs for ingress/egress packet filtering.

4.2. 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.

4.3. GET BIST REPORT

The command will display the results of the previously issued BIST/PBIST test.
Examples:
“GET BIST REPORT” → displays the test results of the previously run BIST TEST
“GET BIST REPORT PBIST” → display the test results for the PBIST power-on test results

4.4. GET DAEMON

This command returns the running status of all DAEMON software used to support network switch functions.

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 MIRROR

This command returns the list of all system wide port/packet mirror configurations.
Examples:
"GET MIRROR" → shows the list of all active port/vlan mirror configurations
"GET MIRROR ALL" → shows the complete list of all mirror configurations

4.10. 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.

4.11. 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

4.12. GET TRUNK

This command returns the list of all statically configured trunk ports.

4.13. 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.

4.14. GET SPANTREE

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

Examples:
"GET SPANTREE" → shows a parameter/settings list for the currently selected VLANs
"GET SPANTREE 5" → shows the parameter/settings for VLAN index 5
"GET SPANTREE ALL" → shows the parameter/settings for all enabled VLANs

4.15. GET 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: "GET SWITCH REPORT"

4.16. 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
"GET VLAN PORTS" → show a concise listing of all logical ports and their associated VLANs
"GET VLAN NONE" → shows a list of all ports that are not mapped to any VLAN

4.17. GET VERSION

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

4.18. 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

4.19. SET ACL

This command will allow the user to configure a pass/drop filter on both the ingress and egress directions for any of the logical ports.

The format for this command is as follows

SET ACL [SLOT] [CMD] [PROTOCOL] PORT [NUMBER]

SLOT → value from 1 to 64 to allow the user to select an ACL position

CMD → allowed values are PASS, OFF, or PARK

PASS: will only pass data confirming to the selected protocol
OFF: removes the ACL from the system and clears it
PARK: disables the ACL but leaves it in the configuration so it can be re-enabled

PROTOCOL → allowed values are TCP,UDP,ICMP,ARP, BROADCAST

NUMBER → logical port number to bind the ACL/Filter with

Example:

SET ACL 1 PASS ARP PORT 2
SET ACL 2 PASS TCP PORT 2

This example uses two ACLs and will allow only ARP or TCP traffic to ingress OR egress on Port 2

4.20. SET 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:
“SET BIST FULL EXT” → Runs packet generation testing for external loopback on all ports
“SET BIST FULL” → Runs packet generation testing using internal loopback on all ports
“SET BIST 22” → Runs an internal loopback test for port 22
“SET BIST 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.

4.21. SET DHCPSERVER

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 DHCPSERVER ON” This will turn on (or off) the DHCP Server Function
“SET DHCPSERVER SUBNET 192.168.1.0”: Assigns the subnet address for the DHCP Server
“SET DHCPSERVER BASE 192.168.1.50”: Assigns the starting addresses for DHCP handout
“SET DHCPSERVER RANGE 50”: Assigns the IP address range (0-255) for the addresses
“SET DHCPSERVER GATEWAY 192.168.1.1”: Assigns the IP address gateway
“SET DHCPSERVER NETMASK 255.255.255.0”: Assigns the netmask.
“SET DHCPSERVER TFTPSERVER 192.168.1.10”: Assigns TFTP Server for DHCP Option 66
“SET DHCPSERVER TFTPFILE boot.bin”: Assigns TFTP boot file for DHCP Option 67
“SET DHCPSERVER HOSTNAME hostvlan1” : Assigns the DHCP “host-name” option for the vlan

“SET DHCPSERVER 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 DHCPSERVER RESTART” to apply the new values in the DHCP process.

4.22. SET DHCPCLIENT

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:
"SET DHCPCLIENT ON" → Turns on the DHCP Client process for the fabric side port
"SET DHCPCLIENT OFF M" → Turns off the DHCP client process for the management port

4.23. SET FEC

Enable/Disable forward error correction on a 10G-KR/SFI port.

Example: "SET FEC 25 ON"
This will turn forward error correction on Port 25 to "ON"

The current settings for all FEC modes can be obtained using the "GET LINK" report.

4.24. SET IGMP SNOOP

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 SNOOP ON" → Enable IGMP snooping
"SET IGMP SNOOP OFF" → Disable IGMP snooping and allow multicast to flood on ports per VLAN
"SET IGMP SNOOP DISABLE" → Globally disable all multicast flow across the entire switch fabric

4.25. SET IGMP PROXY

Enable/Disable IGMP Proxy for a WAN port. This setting is only valid when IGMP Snooping is also enabled.

When IGMP Proxy is enabled, any inbound IGMP messages from downstream VLAN/ports will be proxied to the upstream WAN port to allow localized IGMP join/leave/membership messages to be transmitted to an upstream router on the WAN port.

Note: IGMP Proxy requires that IGMP Snooping is enabled
Note: IGMP Proxy requires that one VLAN is designed for the WAN with a single uplink port

Example:
"SET IGMP PROXY ON" → Enable IGMP Proxy functions for forwarding to WAN Port
"SET IGMP PROXY OFF" → Disable IGMP proxy

4.26. SET IGMP STATIC

This command allows the user to configure a port as a static member of a multicast group.
This requires that IGMP SNOOPING is currently enabled on the switch.
A maximum of 32 static groups can be configured.
The command "GET MULTICAST" can be used to view all dynamic and static IGMP multicast paths.

Example:
SET IGMP STATIC 1 ON 225.0.0.1 6 → configures static group #1 to bind port #6 to multicast group 225.0.0.1

SET IGMP STATIC 1 OFF → disables/removes any existing static group assigned to index #1

4.27. 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

4.28. 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.

4.29. SET MIRROR

This command allows assignment of the port/packet mirroring/analyzer configurations of the unit. The command requires two or three parameters depending on the setting.

Example:
"SET MIRROR A BBBB CCCC"
A is the mirror index (1-6)
BBB is the control state (ON, OFF, MAC, SOURCE, SINK)
CCC is an optional parameter (Source, Sink port numbers, or MAC address)

"SET MIRROR 1 ON" → activate mirror index 1
"SET MIRROR 1 MAC" → active mirror index 1 with MAC filter mode
"SET MIRROR 1 OFF" → de-activates mirror index 1
"SET MIRROR 1 SINK 4" → assign logical port 4 as the egress analyzer port for mirrored data

"SET MIRROR 1 SOURCE 1" → source port for mirroring in logical port 1
OR
"SET MIRROR 1 VLAN 2" → mirror all traffic on VLAN 2

"SET MIRROR 1 MAC 00:11:22:33:44:55" → configure the MAC address associated with mirror index 1.

Details about MAC Mode:

When a MAC selection is applied and the mirror is using PORT mode, the system will mirror packets that ingress on the SOURCE port and have the associated MAC address as the destination MAC address contained in the payload of inbound packet.

When a MAC selection is applied in VLAN mode, the system will mirror any packet in the VLAN that has the associated MAC address as the destination MAC address contained in the payload of the inbound packet. Special consideration should be given when Layer3 routing is also applied.

For example:

Port 23 is on VLAN 900 with IP address range 192.168.1.XXX
Port 24 is on VLAN 901 with IP address range 192.168.2.XXX

If the mirror is operating in VLAN mode, all packets assigned to the VLAN source will be considered, regardless of the physical ingress port.

Setting the mirror to “SET MIRROR 1 VLAN 900” would allow traffic that ingresses on Port 24 and uses IP addresses within the VLAN 900 range (i.e. 192.168.1.XXX) since at the point of ingress, those packets would be routing into the VLAN 900 zone.

A recommended approach is to first enable VLAN mirror to observe all traffic on the VLAN and then apply the desired MAC filtering.

NOTE: After adjusting all mirror parameters, issue the command “SET MIRROR REBUILD” to regenerate the mirror configuration in the switch fabric.

4.30. 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.

4.31. SET NAME

This command allows assignment of the switch logical name which is used at the CLI command prompt, SNMP, webserver, and is also listed under the switch report.

Example:
"SET NAME LABUNIT-3" → sets the logical system name to "LABUNIT-3"

4.32. SET NTP

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

Examples:
"SET 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

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

4.33. SET 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:
"SET PBIST CONFIGURE OFF" → disable all ports for pbist test
"SET PBIST CONFIGURE *" → enable all ports for pbist test
"SET PBIST CONFIGURE 1,2,5-10" → set ports 1,2,5,6,7,8,9,10 pbist testing

4.34. SET PIM

This command is used to issue a global setting for PIM multicast on all VLANs.
The command format “SET PIM XXX” . The allowed options are “SSM” , “SM”, “DM”, “PA” and “OFF” as follows

“SSM” → configure for Source Specific Sparse Mode
“SM” → configure for Sparse Mode
“DM” → configure for Dense Mode
“PA” → configure for Passive Mode
“OFF” → disable PIM entirely on the selected VLAN.

NOTE: The rendezvous point for SM mode will be automatically assigned to the VLAN designated as the “WAN” port. Ensure that ONE VLAN is configured for the “WAN” / uplink port prior to using PIM.

NOTE: After configuring PIM, issue the command “SET PIM RESTART” to regenerate the PIM process with all PIM related updates.

4.35. SET 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 “GET SWITCH REPORT” function

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

4.36. 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

4.37. 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

4.38. SET QOS BUFFER

This command is used to enable the global dynamic buffer allocations for the switch across all ports.

Two parameters to this command are the "ALPHA" and the "DEPTH" options.

The ALPHA is the weight factor (0 to 6) which translates to a ratio from 0% to 400% allowing a congested port to consume buffers from non-congested ports.

The DEPTH parameter assigns the number of buffers available to each port.

The default settings are 4 and 16 which map a 1:1 ratio for buffer consumption and 64k packet buffers per port.

The parameters can be tuned to improve data flow under heavy traffic. Its recommended to adjust the ALPHA parameter and then the DEPTH parameter.

Examples:
"SET QOS BUFFER 4 16" → Allocate default values for port congestion buffers

"SET QOS BUFFER 5 16" → Allow a congested port to consume 2x buffers from a non-congested port.

4.39. SET RADIUS

See command “SET TACACS” as the format is the same

4.40. SET RIP

This command issues a global RIP protocol configuration for all VLANs. The command format is “SET RIP XXXX”. The allowed options are “ON”, “V1” , “V2” “NG” , “OFF” as follows

“ON” → activates RIP in default V1/V2 mode
“V1 “ → activates RIP in V1 mode only
“V2 “ → activates RIP in V2/V1 mode only
“NG” → activates RIP using the NextGen RipNG protocol.
“OFF” → RIP processing will be OFF on the selected VLAN

NOTE: After configuring RIP, issue the command “SET RIP RESTART” to regenerate the RIP process with all RIP related updates.

4.41. 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

Note: If AUTH or PRIV is set to "OFF", then all SNMP V3 logins will be disabled.

Note: The SNMP V3 User/Password is also the same user password for the CLI login process

Note: After applying changes, issue the "SET SNMP RESTART" command to restart the SNMP process so the changes take effect.

4.42. SET SPANTREE

This command configures the spanning tree mode for the current VLAN.
The format of the command is “SET SPANTREE [MODE] [VALUE]”

The modes can be as follows
“SPT” → for standard spanning tree support on each vlan
“AUTO” → for standard spanning tree support on each vlan with auto SPT/RSPT
“OFF” → disable spanning tree support on the current vlan
“PRIORITY” → set the priority of the spanning tree bridge to based on the parameter “VALUE”
“RESTART” → restart/regenerate all spanning tree bridges

NOTE: The RESTART command should be issued after changing the Spanning tree configurations. This is required to rebuild the spanning tree.

Example:
“SET SPANTREE SPT” → enable basic spanning tree on the current vlan
“SET SPANTREE PRIORITY 100” → set the current priority of the spanning tree to 100

4.43. SET SPANPORTS

This command assigns the logical ports, in the currently selected VLAN, to be used for the spanning tree bridge process.

Example: “SET SPANPORTS 1,2”

4.44. SET 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:
"SET SYSLOG ON 192.169.1.21" → turn on syslog functions to target server 192.169.1.21
"SET SYSLOG OFF" → disable syslog functions
"SET SYSLOG ON 192.169.1.23 999" → turn on syslog to target server 192.169.1.23 using port 999

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

"SET 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.

4.46. SET SSH

This command is used to enable/disable SSH access to the system.
Examples:
"SET SSH ON" → Activate the SSH process for Linux/cli access
"SET SSH OFF" → Disable the SSH process

4.47. SET TACACS

This command assigns/resets the user/password authentication for a remote TACACS (or RADIUS) server.

The command syntax is as follows

SET TACACS RESTART → restart/regenerate the TACACS authentication config. This command should be issued after changing the TACACS configuration on the switch.

SET TACACS STATE [ON/OFF] → the TACACS state can be set to ON/OFF to allow authentication processing

SET TACACS SECRET [XXXX] → assign the 'Secret' exchange token used for encryption with the server

SET TACACS SERVER [XXXX] → assign the IP address for the server to be used for authentication

SET TACACS PORT [XX] → assign the IP Port used for server communication

Note: This command also is used to configure RADIUS authentication. Use the form "SET RADIUS" and apply the same values as listed above.

4.48. SET TELNET

This command is used to enable/disable TELNET access to the system.
Examples:
"SET TELNET ON" → Activate the Telnet server process for Linux/cli access
"SET TELNET OFF" → Disable the Telnet server process

4.49. SET TRUNK

This command allows assignment of any ports into an static TRUNK group.
Examples of this command are as follows.

Example:
"SET TRUNK 1 5,6,7" → sets ports 5,6,7 into TRUNK Group #1
"SET TRUNK RESPAWN" → rebuild the all TRUNK configurations
"SET TRUNK CLEAR" → clear all TRUNK configurations

4.50. 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 MODE XXXXX" → this command configures the VLAN mode for either "WAN", "LAN" or "TAGGED" mode.

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

"SET VLAN PIM XXXX" → this command is used to configure an individual VLAN for PIM multicast mode. The allowed options are "SSM" , "SM", "DM", "PA" and "OFF" as follows

"SSM" → configure for Source Specific Sparse Mode
"SM" → configure for Sparse Mode
"DM" → configure for Dense Mode
"PA" → configure for Passive Mode
"OFF" → disable PIM entirely on the selected VLAN.

NOTE: The rendezvous point for SM mode will be automatically assigned to the VLAN designated as the "WAN" port. Ensure that ONE VLAN is configured for the "WAN" / uplink port prior to using PIM.

NOTE: After configuring PIM, issue the command "SET PIM RESTART" to regenerate the PIM process with all PIM related updates.

"SET VLAN RIP XXXX" → this command is used to configure an individual VLAN for RIP routing path protocol. The allowed options are "ON", "V1" , "V2" "NG" , "OFF" as follows

"ON" → activates RIP in default V1/V2 mode
"V1 " → activates RIP in V1 mode only
"V2 " → activates RIP in V2/V1 mode only
"NG" → activates RIP using the NextGen RipNG protocol.
"OFF" → RIP processing will be OFF on the selected VLAN

NOTE: After configuring RIP, issue the command "SET RIP RESTART" to regenerate the RIP process with all RIP related updates.

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.

SET VLAN ACCESS PRIVATE → this command configures the selected VLAN for isolated L2 switching only.

SET VLAN ACCESS ROUTEABLE → this command configures the VLAN for Layer3 routing based on IP addresses.

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

4.51. SET WEBSERVER

This command is used to enable/disable the webserver capabilities of the system.
Examples:
"SET WEBSERVER ON" → Activate webserver and allow user access from a browser allowing both HTTP and HTTPS

"SET WEBSERVER HTTPS" → Activate webserver force any HTTP transaction to redirect to HTTPS mode

"SET WEBSERVER OFF" → Disable the webserver

4.52. 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.

4.53. EXIT

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

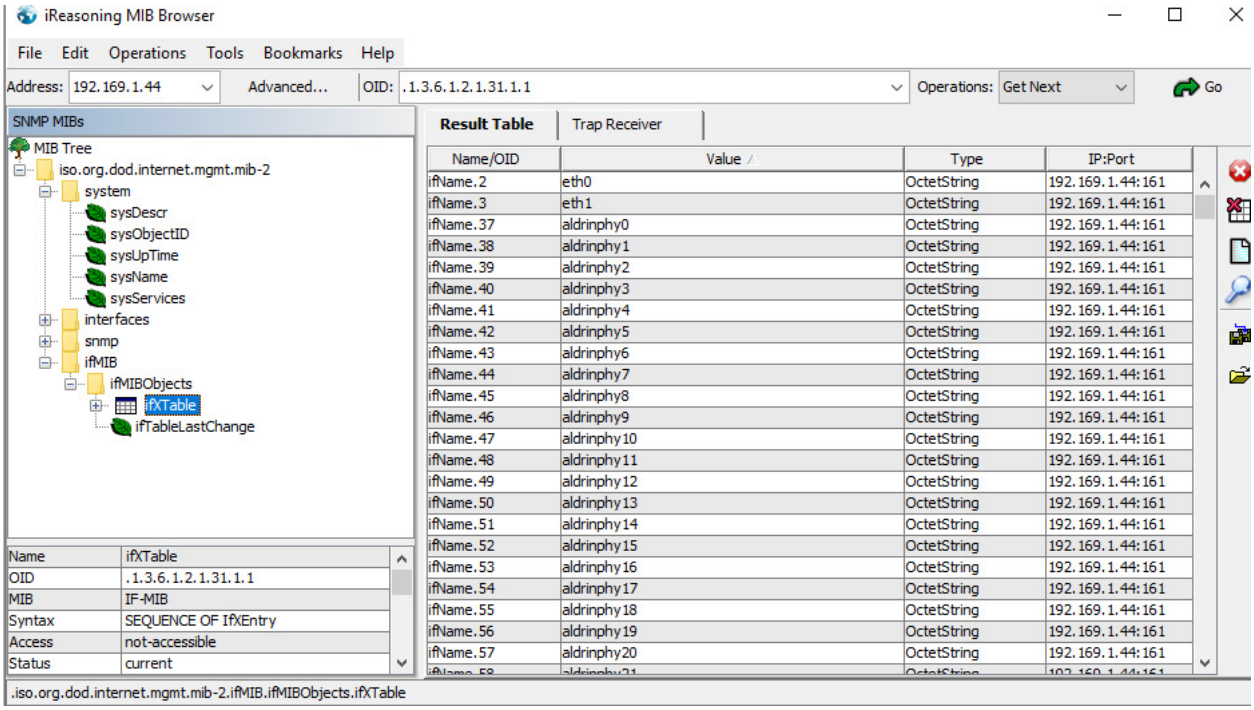
5. Triggered Network Access Functions

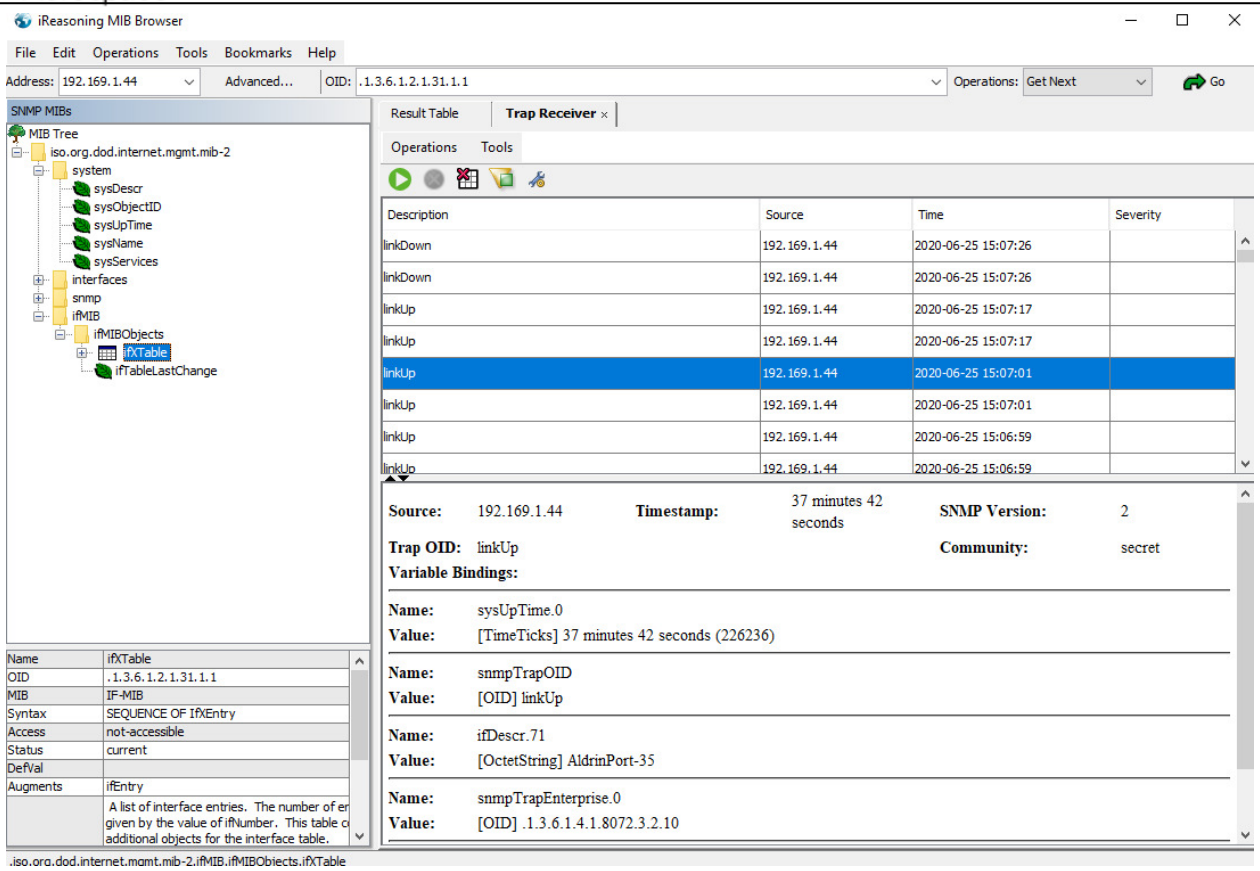
5.1. SNMP

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)

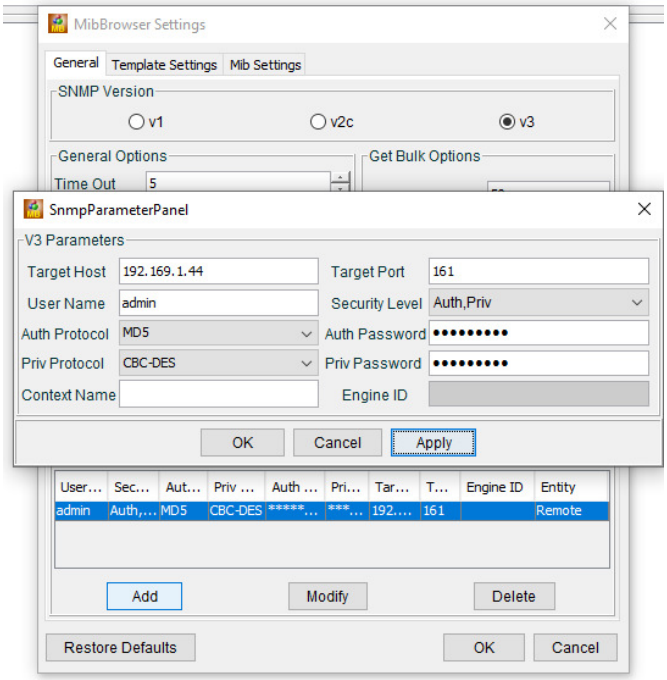
Note that the appropriate MIB modules should be loaded using the File->Load/Unload MIBs.



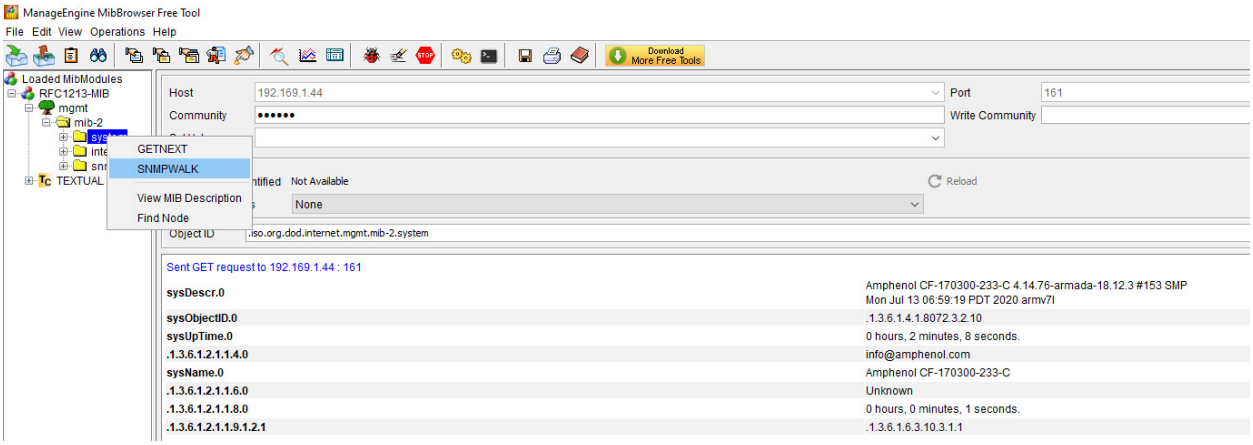

iReasoning MIB Browser
File Edit Operations Tools Bookmarks Help
Address: 192.169.1.44
Advanced...
OID: .1.3.6.1.2.1.31.1.1
Operations: Get Next
Go
SNMP MIBs
MIB Tree
iso.org.dod.internet.mgmt.mib-2
system
sysDescr
sysObjectID
sysUpTime
sysName
sysServices
interfaces
snmp
ifMIB
ifMIBObjects
ifXTable
ifTableLastChange
Result Table
Trap Receiver
Operations
Tools
Description
Source
Time
Severity
linkDown 192.169.1.44 2020-06-25 15:07:26
linkDown 192.169.1.44 2020-06-25 15:07:26
linkUp 192.169.1.44 2020-06-25 15:07:17
linkUp 192.169.1.44 2020-06-25 15:07:17
linkUp 192.169.1.44 2020-06-25 15:07:01
linkUp 192.169.1.44 2020-06-25 15:07:01
linkUp 192.169.1.44 2020-06-25 15:06:59
linkUp 192.169.1.44 2020-06-25 15:06:59
Source: 192.169.1.44
Timestamp: 37 minutes 42 seconds
SNMP Version: 2
Trap OID: linkUp
Community: secret
Variable Bindings:
Name: sysUpTime.0
Value: [TimeTicks] 37 minutes 42 seconds (226236)
Name: snmpTrapOID
Value: [OID] linkUp
Name: ifDescr.71
Value: [OctetString] AldrinPort-35
Name: snmpTrapEnterprise.0
Value: [OID] .1.3.6.1.4.1.8072.3.2.10
Name ifXTable
OID .1.3.6.1.2.1.31.1.1
MIB IF-MIB
Syntax SEQUENCE OF IfXEntry
Access not-accessible
Status current
DefVal
Augments ifEntry
A list of interface entries. The number of er
given by the value of ifNumber. This table c
additional objects for the interface table.
.iso.org.dod.internet.mgmt.mib-2.ifMIB.ifMIBObjects.ifXTable

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.

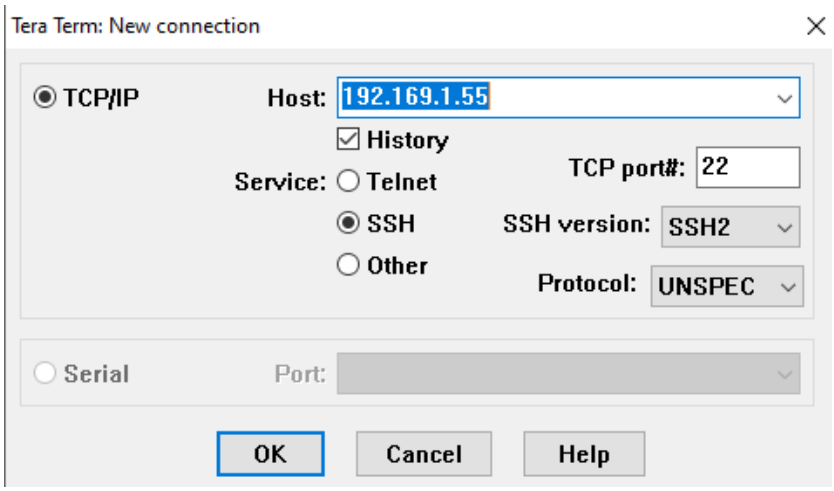


Once authenticated, the user can right click on the specific MIBs in the MIB tree and perform a get/walk function.



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. RADIUS and TACACS Authentication

Remote RADIUS/TACACS servers can be used to provide additional username/password and permissions to allow access to the switch CLI interface.

Two permissions classes are allowed. These are “admin” and “non-admin” users.
A “non-admin” user can only issue “GET” commands to read the switch status/settings.
A “admin” user can issue any of the commands on the system.

5.3.1. TACACS Example

An example tacacs.conf file showing two users is detailed below.

```
key = testing123

user = testuser1 {
        global = cleartext "testpass123"
        service = ppp protocol = ip
            {
            priv = admin
        }
}
user = testuser2 {
        global = cleartext "testpass123"
        service = ppp protocol = ip
            {
        }
}
```

This configuration shows the secret key is “testing123”

This configuration shows a user “testuser1” with password “testpass123” and this user is set to “admin” permissions.

This configuration shows a user “testuser2” with password “testpass123” and this user has no priv level defined, so this user would authenticate as a non-admin user for “GET” level access only.

These files reference the linux “tacplus” server which can be installed under Ubuntu 18.x or Debian Linux.

5.3.2. RADIUS Example

“clients.conf” example
This example shows a RADIUS server configuration which allows any IP address, UDP transport, and assigns a secret phrase to “testing123”

```
client localhost {
        #  allow any IP ADDRESS
        ipaddr = *
        proto = *
        secret = testing123
        require_message_authenticator = no
        nas_type        = other         # localhost isn't usually a NAS...
        limit {
                max_connections = 16
                lifetime = 0
                idle_timeout = 30
        }
}
```

“users.conf” example

This example shows a RADIUS server configuration showing two users.

```
#basic user entries
user1   Cleartext-Password := "flc"
        Service-Type = "Administrative-User"

user2  Cleartext-Password := "flc"
       Service-Type = "Login"
```

user1 with password “flc” and this user will be “Admin” level
user2 with password “flc” and this user will be “Non-Admin” level

These files correspond to the FreeRadius-3.x server which can be installed on Linux directly from the “freeradius.org” website

5.4. 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 TFTPD64 server program

5.5. 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

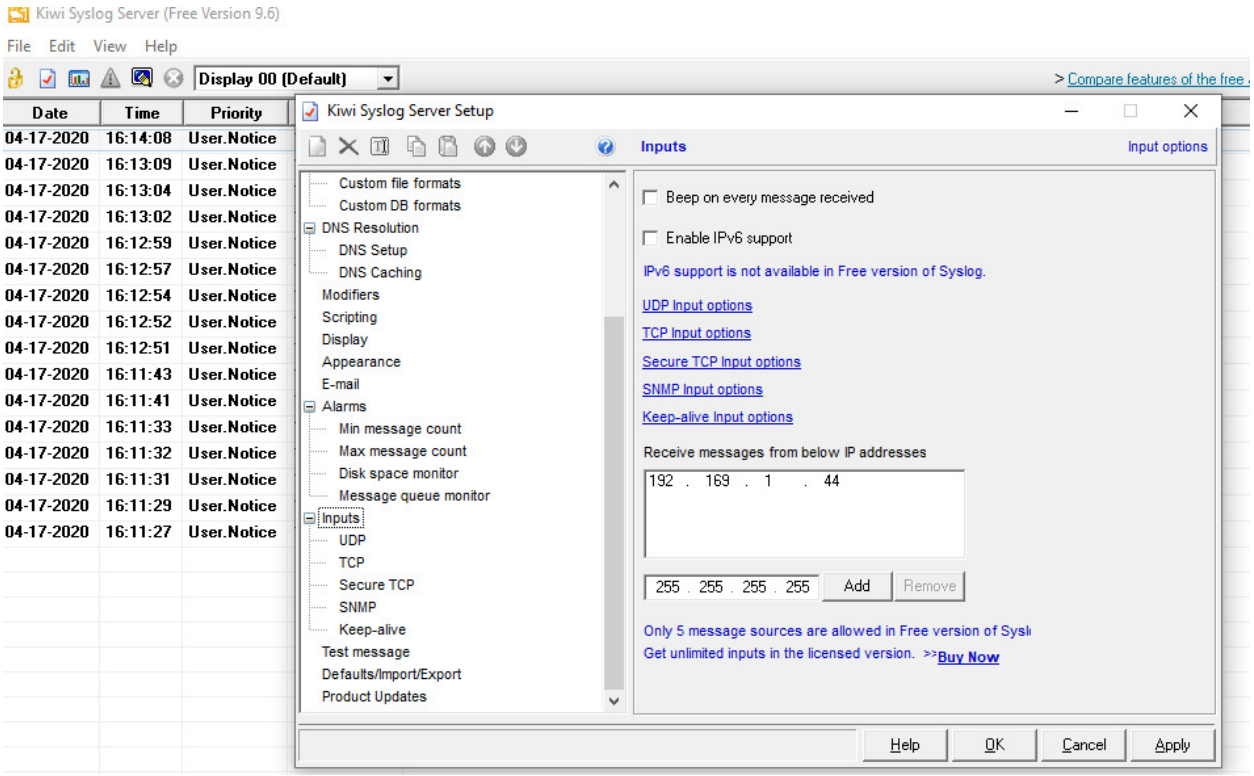
sshpass -p thepassword scp -S dbclient ledtest theuser@192.169.1.21:/

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.

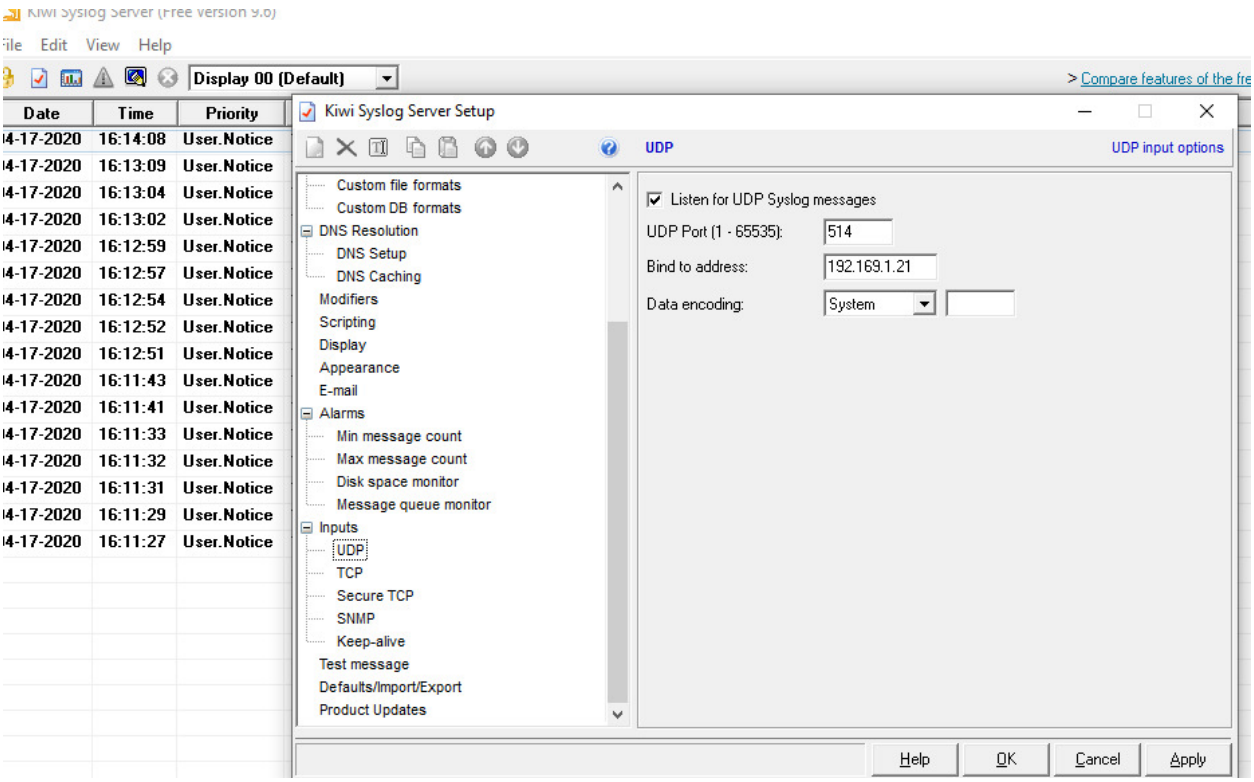
Completion of this command will then transfer the file “ledtest” to the server’s user path “c:\ftp” using secure file transfer protocol

5.6. SYSLOG Usage

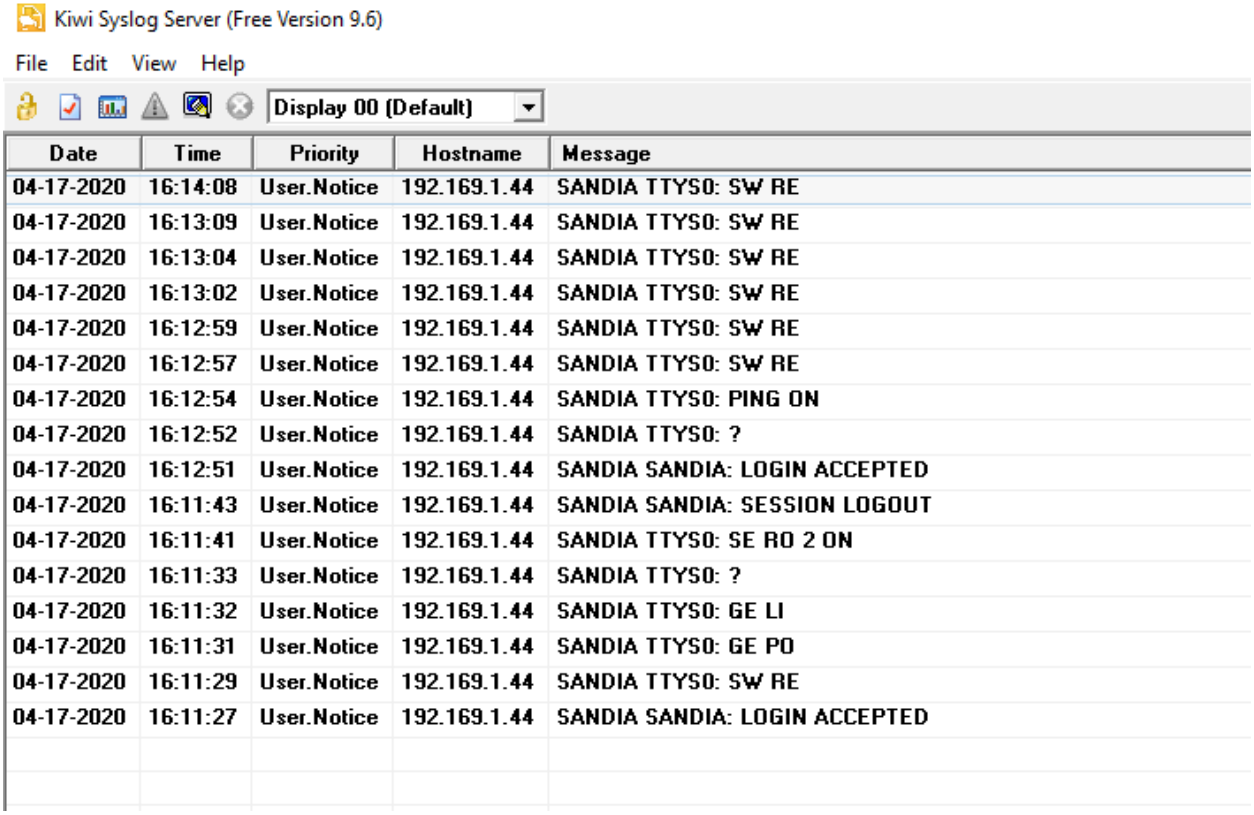
The SYSLOG function can be used with the “Kiwi Syslog Server Free Version 9.6”
Install the SYSLOG program on a remote PC.
Configure the File→Setup→Inputs to allow the syslog server to receive messages from the IP address of the physical switch unit.



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



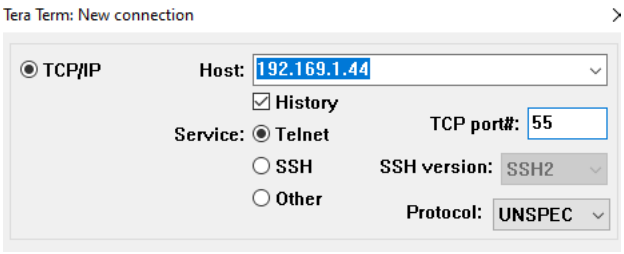
Once configured, all entered commands and events on the CLI should be remotely logged by the syslog server.



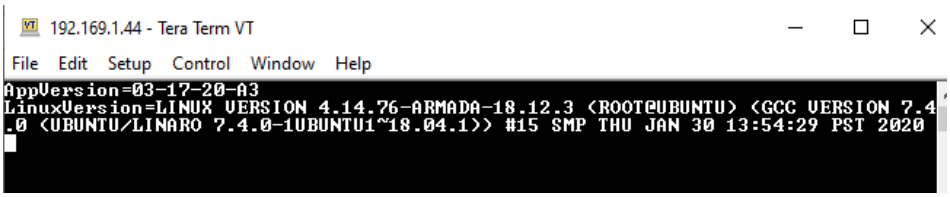
Date	Time	Priority	Hostname	Message
04-17-2020	16:14:08	User.Notice	192.169.1.44	SANDIA TTYS0: SW RE
04-17-2020	16:13:09	User.Notice	192.169.1.44	SANDIA TTYS0: SW RE
04-17-2020	16:13:04	User.Notice	192.169.1.44	SANDIA TTYS0: SW RE
04-17-2020	16:13:02	User.Notice	192.169.1.44	SANDIA TTYS0: SW RE
04-17-2020	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 PO
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

5.7. 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



5.8. 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.

5.9. 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.