UPS Solidswitch 1400

User Guide

BTU Research LLC
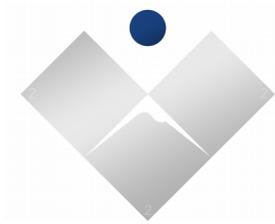UPS Solidswitch 1400
User Guide

Acknowledgments

The product described in this manual, is a licensed product of BTU Research LLC.
All other products or trademarks are property of their respective owners.

BTU Research LLC
UPS Solidswitch 1400
User Guide

Table of Contents

This page is intentionally left blank

Introduction

UPS SolidSwitch is a powerful 240W 4+1 Port, outdoor PoE switch. It's designed to perform the functions of a midspan switch combined with an inclusive UPS and internal power source, to provide hours of emergency back-up. Power of up to 60W is available to all SolidSwitch POE ports.

Up to 240W	Up to 60W	Up to 90-264VAC 50/60Hz	Up to 1400Wh
Total Power Output	Power Output Per Port	Power Input	Standby Power

Innovative

UPS SolidSwitch is made possible by BTU's "Uninterruptible Power (over Ethernet) Supply"™. A disruptive technology that ensures a reliable and consistent power connection through a switching mechanism to an internal battery source. The UPS SolidSwitch operates so efficiently, the transition is undetectable. In the creation of UPS SolidSwitch, we intended to add a new dimension to network infrastructure and were uncompromising in it's design and engineering. In doing so, we created a new standard to deliver what we believe is the most versatile, outdoor POE Switch, bringing UPS anywhere to ensure always on power everywhere.

Rugged

Housed in a die cast metal enclosure and built to be fully submersible. It's compact profile is made possible by the use of advanced PCB mounted 500W power supplies. The space, traditionally used in conventional switches to house large open framed AC/DC power supplies, makes way for a powerful 350Wh Li-Ion Power Pack. A specially designed "Extended Runtime Cover" is available to house up to 3 additional equally powerful packs, to increase emergency supply up to 1400Wh.

Smart

At initial power up, the SolidSwitch microprocessor takes inventory of the internal emergency power sources and estimates the energy levels in each of the available resources. This estimate of each resource will be updated when the known status is achieved and will be re-evaluated every 1 second, to sense changes and make adjustments to the available inventory.

The switching from an AC power source to the main backup battery pack is controlled by hardware, eliminating CPU latency and ensuring glitch free operation. Management of auxiliary power packs is handled by a microprocessor, which powers all ports until the battery resources are completely exhausted.

SolidSwitch provides the network capability to shut down selected devices or to program the orderly shutdown of devices, when resources have been depleted to predetermined levels. Battery maintenance is also programmed into the device to ensure PowerPak life is maximized.

Features

UPS SolidSwitch contains an all-inclusive, uniquely intuitive web based configuration and management tool, with timed restart capabilities to ensure permanent changes are effected unmistakably. Instant PoE monitoring and controls report exact per port power consumption, while simply enabling power recycling to edge devices on the fly. The sophisticated on board UPS and emergency backup is fully monitored twice per second to access real time mains power status, PowerPak charge status, capacity, and estimated emergency run time. Simplified management is provided through preconfigured VLAN tables and individual port membership.

Enterprise Authentication

Management authentication begins on the local device database and may be extended to remote authentication sources (AAA) by use of remote authentication extensions in the switch. This is simply facilitated through the configuration of the applicable settings for the extension type desired and then enabling that extension. Included extensions – TACACS and Radius.

Switch Feature Details

- VLAN table management across all ports is used for VLAN membership and VLAN trunking on the uplink.
- Permanent VLAN (PVLAN) for all ports is used for tagging ingress traffic.
- Renumbering of the management interface is made possible with attachment to 1 of 4094 active VLANS if so required.

- 802.1X port-by-port basis (wired ports)

Management Services
- SNMP V3 Support with SHA/MD5 AES/DES encryption options
- NTP with support for local time
- Radius (user authentication)
- TACACS (user authentication)

Integrated Switch Features
- Full VLAN and QoS support
- Fast Link-up option to significantly reduce link-up time
- Auto-negotiation and Auto-MDI / MDI-X support
- 1000BASE-T/100BASE-TX/10BASE-Te IEEE 802.3 (Wired ports)
- 1000BASE-T/1000BASE-X/1000BASE-SX/1000BASE-LX (SFP)
- MIB counters (34 per port) for fully compliant statistics gathering
- IEEE 802.1X access control (Port and MAC address based)
- IGMP v1/v2/v3 snooping for multicast packet filtering
- IPv6 multicast listener discovery (MLD) snooping
- IPv4/IPv6 QoS support, QoS / CoS packet prioritization
- 802.1p QoS packet classification with 4 priority queues
- Broadcast storm protection
- Four priority queues with dynamic packet mapping for:
  - IEEE 802.1p
- IPv4 DIFFSERV
- IPv6 Traffic Class
- MAC filtering function to filter/forward unknown uni-cast, multicast and VLAN packets
- Jumbo packet support up to 9000 bytes (configurable)
- Port mirroring/monitoring/sniffing with ingress and/or egress traffic to any port

WEB INTERFACE

Solidswitch default IPv4 address is 10.4.1.80 for the first-time configuration, please configure your computer network interface to the following IPv4 parameters:

- IP Address within the 10.4.1.0/255.255.255.0 space.

    ○ Example: 10.4.1.10

- Network Mask 255.255.255.0

Once your machine is configured with the above temporary network parameters, with a Ethernet cable attached to one of the wired ports, the Web Interface can be reached using the following address

https://10.4.1.80/

The switch may also be configured by way of the command shell via ssh2 protocol.

Default Access Credentials

The default username and password is admin/admin.

For security purposes the password should be changed immediately.

Web Interface Color Scheme

The default web interface color scheme may be changed under the settings → system → general section. A new color scheme maybe applied after saving by using the "apply" button.

Web Interface Color Scheme

Dark   Apply Now

Save Settings

UPS Command Post

The main web page is used to monitor unit status, PoE ports status, such as Ethernet Link connection speed, PoE power consumption, and total unit PoE power consumption. The statistics on this web page are updated automatically every few seconds.
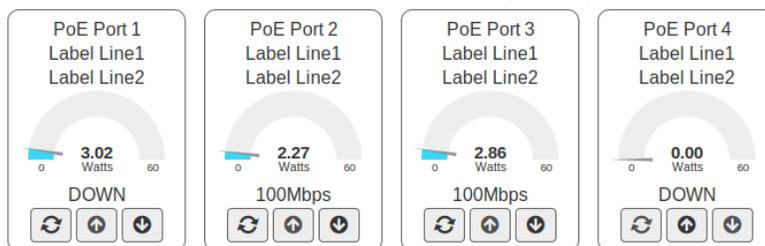
Port status

- Individual port descriptions

- Status information, including power consumption

- Network link state

- Link speed

Each port also includes quick access controls, used easily power down, power up, or power-cycle the port.

Power Status

The units connection to MAINS power is displayed as *On-Line* or *Off-Line*. When Off-Line the "Storage Mode" function can be invoked here. The button to invoke the shutdown / storage mode is ONLY visible in the absence of MAINS power. Under normal operating conditions the feature is made unavailable.

Battery Status

Battery status, for batteries 1 thru 4 capacity is illustrated with a bar graph, percentage, and service state. The service states are idle, charging, or in-service.

Battery Status

Battery	Capacity	% Capacity	State
#1 Installed		100.00	Idle
#2 Installed		100.00	Idle
#3 Installed		100.00	Idle
#4 Installed		100.00	Idle

Configuration Management

Configuration data is stored in two data sets, permanent, and cache. Permanent memory persists through a power off, where the cache is a copy of the permanent memory created at system startup. The difference between these configuration sets is determined by computing a checksum of the entire configuration data. Each data set checksum is displayed on the Configuration screen.

```
Configuration Summary
   Location                      Checksum
   NVM (Permanent)               0xE7A8EAFF
   Config Cache                  0xE7A8EAFF
   Active (Running)              0xE7A8EAFF
```

Configuration cache becomes "the running configuration" when activated.

The data transfer from permanent *to* cache *to* activation is executed automatically on power up.

Configuration Management Conventions

After initial system power up, the cache may be reconfigured, activated, then optionally written to permanent memory. The configuration cache can be written direction to permanent memory skipping the activation step, however we advise the configuration be activated before the commit to permanent memory where possible, to avoid a system lockout condition. The system configuration tool will prompt to initiate an *automatic* restart when activating the configuration. This automatic restart will provide a stop gap with a clean restart from the last permanent memory configuration prior to the cache activation. In the event there is a error in the configuration, for example IP numbering or VLAN access etc., the automatic restart will trigger, and bring the switch back up with the last saved configuration, helping recover access to the switch. When using *automatic* restart, it is important to "commit changes" within 5 minutes of the activation to preserve the activated changes. The action of committing to permanent memory will cancel the pending restart. If you fail to commit to permanent

memory after activation, the automatic restart will trigger a system reboot after 5 minutes, consequently discarding changes in the configuration cache.

Configuration Actions

Each configuration action is preceded with a confirmation step. The activation is a two step confirmation, the second step providing the option for the *automatic* restart. You may use your best judgment as to when to deploy the *automatic* restart..

Configuration Actions

→ Activate Changes → Commit Changes   Restore From NVM
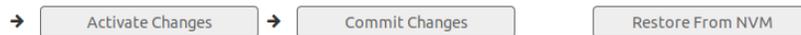
Export / Import by HTTP

Configuration can be downloaded for archival purposes. If the physical asset should need to be replaced, the saved configuration can be uploaded to reproduce the exact configuration as before.

Configuration Export

Download a copy of the NVM configuration data. The export data can be used as to restore configuration settings later.

Export Configuration

Configuration Import

Upload a previously exported configuration file.

Select Configuration File   Upload

System Actions

Reboot action will invoke a internal operating system reboot.

Factory Default will stage the factory default database to be installed on the next system reboot.

Reboot   Factory Default

System Configuration

System Access Credentials

The system supports up to 32 unique users. This management screen allows you to simply add a user by username. The users password, and optional public key data can be configured by the entry in the user table row. Non administrative users can be inhibited by toggling the lockout feature.

Local User Access Table

Users			Level	Lockout
admin	Change Password	Set Public Key	Level 1	Disabled

Create a new user

	Create

System Network Configuration

By default the Solidswitch is configured from the factory with the following address:

IP Address: 10.4.1.80

Along side the static address is a DHCP client service that will solicit a local DHCP server if one is reachable on the local network segment. The purpose of the DHCP client is to support internet connectivity for software updates and network time support. If you wish to statically number the device, you may simply disable the DHCP Client service. Once the DHCP client service is disabled, a gateway IP address field is then presented, which will be used to establish a default IP route.

DHCP Client Service Enabled

Dynamic Address

DHCP Client Enabled

Static Addressing Example

Static Network Address

Address	10.4.1.80
Subnet Mask	255.255.255.0
Gateway	10.4.1.252

DNS

Primary	8.8.8.8
Secondary	4.2.2.1

If the DHCP Client service is enabled, the switch may still be reached at the static address. The static address is configured as a sub interface at all times. Default routes supplied by the DHCP Server will supersede static route configuration when DHCP Client service is enabled and active.

System General Settings

Time and Date

This section provides a method to configure the local time zone information for the Solidswitch, and to configure the current date and time. The on-screen date and time should update once per second.

Local Time Zone

Zone Central

Save Settings

Current Time and Date

Friday February 1st 2019, 07:44:03 AM

Set Time and Date

Month	Day	Year	Hour	Minute	Meridiem	Set
February	1	2019	7	43	AM	SET

Web Interface Color Scheme

The user may define either a light or dark color schema, and then make the change active.

Web Interface Idle Timeout

Sets the session idle time in seconds that are allowed to pass before invalidating authentications.

Log System Load Interval

This feature will log the system CPU load to the event buffer at a time interval specified. Zero seconds inhibits logging. Use care in selecting the time interval so not to over run the length of the event buffer flushing potentially useful information. 600-1500 seconds are ideal, with 600 seconds marking the event log only 144 times per 24 hour period.

Switch Configuration

Switch configuration is applied from the configuration cache on system startup. New switch configurations may be applied on demand at run time via the Configuration page.

Switch Global

Global switch settings

VLAN

Enable or disable 802.1q/VLAN Aware. This setting dictates how the switch handles VLAN tags. If Global VLAN is enabled the PVLAN and VLAN configuration becomes active, if disabled, the PVLAN and VLAN table configuration is not activated. This setting essentially makes the switch VLAN aware, enabling 802.1q.

> !Caution   *PVLAN functionality as well as VLAN Tables must be carefully configured prior to enabling the global VLAN feature in order to avoid a undesired network connectivity*

loss. Use the automatic restart feature if it all possible. If you are confident the configuration will work and a connectivity loss is expected the new configuration can simply be committed to permanent memory.

Jumbo Frame Support

Enable or disable the passing of jumbo frames across the switch, jumbo frames may have a unit size of up to nine thousand bytes.

MTU / Maximum Transmission Unit

Configure the maximum Ethernet frame size that is allowed to traverse the switch. Frames larger than the specification will be dropped at the ingress port.

IGMP snooping

Enable or Disable IGMP snooping.

When IGMP snooping is disabled, all multicast frames received by the switch will flood all ports.

When IGMP snooping is enabled, IGMP messages will be sent to the management processor. Join and Query messages will be investigated and forwarded out of relevant active ports except the port of origin. The information gathered from IGMP join or leave messages is used to dynamically construct a multicast group forward table for specified groups. A additional feature, *unknown multicast forward* controls flooding for multicast traffic, as it is learned by the switch. Disabled, multicast traffic is flooded by default until a join request *trims* the flooding of said *group* to the interested port(s). Enabled completely restricts flooding of unknown multicast groups until a join(s) on a port show interest in a group.

Router ports

Routers/Queriers deserve all multicast traffic to be re-made available past their routed interfaces if so requested. Ports designated as router ports are flooded with all multicast traffic.

Router Learning

The switch can learn interfaces connected to multicast routers by IGMP queries received and automatically included them in forwarding of all multicast traffic to those interfaces.

Switch Ports

Each individual port can be configured with two short lines (32 chars max.) of descriptive information. This label information propagates to the main Command Post screen and through the SNMP interface descriptions.

Switch Ports

Port	Label Line 1	Label Line 2	Network	PoE	Authentication
Port 1	Label Line1	Label Line2	⊘ Enabled	⚡Enabled	None
Port 2	Label Line1	Label Line2	⊘ Enabled	⚡Enabled	None
Port 3	Label Line1	Label Line2	⊘ Enabled	⚡Enabled	None
Port 4	Label Line1	Label Line2	⊘ Enabled	⚡Enabled	None
SFP Port					
Port 5	Label Line1	Label Line2	⊘ Enabled		

[Update Port Configuration]

Ports can can have their network and power functions turned permanently on or off from initial switch power on.

Switch VLAN

VLANs explained: VLAN is a way of creating multiple virtual switches inside one physical switch. Each LAN is assigned a Number. The number also has a optional priority level. The VLAN Number is used to control which packets are allowed to enter and exit each port on the switch. The switch also has a number of automatic functions for adding and stripping tags from packets entering and exiting specific ports, to ease the administration of VLANs.

Tag Insertion and Removal

Tag insertion is enabled on all ports when the VLAN feature is enabled. At the ingress port, untagged packets are tagged with the ingress port's default tag. The default tag is separately programmable for each port. The switch does not add tags to already tagged packets unless double tagging is enabled.

At the egress port, tagged packets will have their 802.1Q VLAN tags removed if un-tagging is enabled in the VLAN table entry. This feature is controlled on a per-port basis. Untagged packets will not be modified if 802.1Q is enabled.

PVLAN

PVLAN (Permanent VLAN) Configuration determines how a ports ingress VLAN behavior is defined. The PVLAN function could be assimilated as a high way entrance ramp for packets not yet marked with a VLAN tag to receive a TAG (insertion) on entry, so that they are allowed to exit other ports on the switch configured with VLAN Table configuration.

Filter Action attribute controls how to handle packets as they arrive on the port of interest.

- Tagged

- UnTagged

- All Packets

Port	PVLAN #	Ingress Filter	Tag Action	Priority
Port 1	1	Disabled	Accept Untagged	0
Port 2	1	Disabled	Accept Untagged	0
Port 3	1	Disabled	Accept Untagged	0
Port 4	1	Disabled	Accept Untagged	0
SFP Port				
Port 5	1	Disabled	Accept Untagged	0
SFP Port				
Port 6	1	Disabled	Accept Untagged	0

VLAN Tables

VLAN Table configuration controls which ports are members of a specific VLAN and what type of membership they have.

Memberships

- Tagged

  - Allow VLAN packets out of the interface tags left alone.

- UnTagged

  - Allow VLAN packets out of the interface, however the tags will be stripped

VLAN Add VLAN	Port 1	Port 2	Port 3	Port 4	Port 5 (SFP)	
	-N/A-	-N/A-	-N/A-	-N/A-	-N/A-	Add

System Services

PoE Shutdown

In the event the system looses MAINS power, individual ports may be configured to power off when the remaining aggregated capacity reaches a specific level. Ports that are powered off by this mechanism will automatically be powered back on when the MAIN power returns.

Shutdown Service

Shutdown Disabled   The service must be enabled for the rules below to be in effect

Shutdown Configuration

Port	Enable | Disable	Shutdown when Less than % capacity remaining	
Port 1	Disabled	—————◯—————	80 %
Port 2	Disabled	—————◯—————	80 %
Port 3	Disabled	—————◯—————	80 %
Port 4	Disabled	—————◯—————	80 %

Update Shutdown Settings

PoE Schedule

The PoE schedule service must be enabled prior for any recurring or one-shot rule to be armed.

Recurring Rules

The PoE Schedule can be used to create recurring power operations. A single recurring operation may be configured to execute changes to one or more ports. Each rule can be configured to run on a specific day of the week, and at a specified time of day. Each rule can execute a single power-on, power-off, power-cycle function to the ports selected.

One-Shot Rules

The PoE One-Shot Schedule maybe used to execute one time power operation for a specified date and time in the future.

Terminal Server

The terminal service may be used to bridge a local serial device to a remote network client or server. The terminal service includes several protocols, including raw, telnet, and telnet + RFC2217.   When selecting RFC2217, remote configuration of the local serial parameters are facilitated. The configuration page provides access to set default serial parameters used on system startup, and TCP/IP port selection that the terminal service will listen for connections on.

| Service | ⊘ Disabled |
| Operation Mode | Raw |

Serial Port Parameters

Port Speed	9600
Data bits	8
Stop bits	1
Parity	NONE

Network Parameters
| TCP/IP Port | 2001 |

MQTT Service

MQTT stands for MQ Telemetry Transport. It is a publish/subscribe, extremely simple and lightweight messaging protocol, designed for constrained devices and low-bandwidth, high-latency or unreliable networks. The design principles are to minimize network bandwidth and device resource requirements, while also attempting to ensure reliability and some degree of assurance of delivery. These principles also turn out to make the protocol ideal of the emerging "machine-to-machine" (M2M) or "Internet of Things" world of connected devices, and for mobile applications where bandwidth and battery power are at a premium.

Solidswitch is capable of publishing in JSON format; the data used on the diagnostics screen every 60 seconds to a MQTT broker. Solidswitch also publishes topics that can be published on to provide remote control over PoE functionality. This remote control capability can be used to power-on, power-off, or power-cycle to any PoE port.

The embedded MQTT client can be configured to connect to a user defined broker securely. Information on the topics, how to subscribe, or publish to them is available [TD.403].

Example MQTT Client Configuration

Client Configuration

MQTT Server (Broker)	10.4.1.70
MQTT Port	1883
Username	MQTTL3SSUser
Password	MQTTLSecret
Fallback Topic	BTU_1B3586
Group Topic	solidswitch
Topic	solidswitch
Full Topic	cmnd/solidswitch

Update MQTT Settings

For advanced users, topics can also be gleaned with relative ease by observation of broker logs.

SNMP Service

Simple network monitoring service (SNMP) is a protocol broadly used in the networking industry to monitor the health and function of networking devices. Solidswitch supports two version of the SNMP protocol version 2c (UN-encrypted) and the later version 3 (encrypted).

The SNMP Service configuration screen provides access SNMP system variables, as well as service configuration parameters regarding connectivity, protocol, and credentials.

SNMP Service
Simple Network Management Protocol

SNMP Service	Disabled
SNMP Mode	SNMP v3
Sys Contact	admin@somedomain.com
Sys Description	Solidswitch 1400
Sys Name	L3SS
Sys Location	default location
Username	snmpuser
Encryption Scheme	MD5 / DES
Authentication Password	authpass
Encryption Password	cryptpass

Save Settings

NTP Service

The Network Time Protocol (**NTP**) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. By default this service is enabled on Solidswitch, and is configured to use public NTP servers.

Service	⊘ Enabled
NTP Peer 1	pool.ntp.org
NTP Peer 2	pool.ntp.org

Update NTP Settings

HTTP Service

The HTTP server can be configured to use alternative port numbers to accommodate various network configurations.   Alternative port numbers must be greater than 1024 and less than 65535 to be valid. A change in port numbers requires the current configuration to be saved, and a system reload prior to the new port numbers to take effect.

Server port configuration

HTTP PORT   80
HTTPS PORT   443   (e.g. 8443)

Save Settings

Rsyslog Service

Rsyslog service may be enabled to transmit system events in syslog protocol (RFC-3164) format to a remote server. The messages are transmitted on UDP port 514.

Example Rsyslog configuration screen:

RSYSLOG Service	⊘ Disabled
Remote Log Host	10.4.1.70

Save Settings

Authentication Extensions

RADIUS Service

RADIUS authentication extension service configuration page

The local user authentication database can be extended to authorize users based on remote authentication services. The RADIUS service must be enabled and configured prior to selecting the RADIUS *authentication extension* from the System Access Credentials page.

Radius Service	⊘ Disabled
Radius Server	10.4.1.70
Server Secret	testing123
Response Timeout	3 Seconds
Save Settings	

TACACS Service

TACACS authentication extension service configuration page.

The local user authentication database can be extended to authorize users from a remote TACACS service. The TACACS service must be enabled and configured prior to selecting the TACACS *authentication extension* from the System Access Credentials page.

TACACS Service	⊘ Disabled
Server Address	10.4.1.70
Server Key	testing123
Save Settings	

LLDP Service

Solidswitch has a internal LLDP daemon that is capable of advertising the local chassis description through it's network connected links. The service must be enabled for use as it is disabled by default. Once the service is enabled the the system must be reloaded prior to service startup. When the service is running LLDP messages received on various ports will be digested and information learned displayed on the LLDP information page. LLDP information is also available through the CLI.

Connection Monitor Service

The connection monitor service may be used to cycle power to a PoE connected device so long as the PoE device is on the same network numbering schema as the switch administration service address.

The Host Address of the PoE device and Fail Count are user defined.

Port	Monitoring State	Host Address	Fail Count	Status	Last Activity Timestamp
Port 1	⊘ Disabled		5	Not-Monitored	N/A
Port 2	⊘ Disabled		5	Not-Monitored	N/A
Port 3	⊘ Disabled		5	Not-Monitored	N/A
Port 4	⊘ Disabled		5	Not-Monitored	N/A

Operational Description

The Connection Monitor service will transmit a PING request to the HOST address every sixty seconds, and reset power if the address becomes unresponsive.   The power for the port will be switched "Off", and then "On" after the number of failed ICMP responses reach the user defined fail count.

Network Ports

Switch → Network Ports → Port 0..10 Information Page

Each network port has a information page that describes port related networking information such as line state, transmit and receive counters, symbol errors, CRC errors, discards, and pause frames.

Dynamic ALU entries specific to the port.

Port specific STP information such as role, state, path costs and more.

Spanning Tree Protocol

Spanning tree protocol engine is enable by default. The spanning tree parameters for each port on the switch may be tuned for user defined specifications.   Settings → Switch → Ports page contains per port user parameters such as state, path cost, and priority. A information summary about timing and topology changes maybe learned from the STP Information page on the web interface as well as the CLI.

Global STP Settings Configuration

Setting Name	Default Value
Hello Time	2
Max Age	20
Forward Delay	6
TX Hold	15
Priority	0x8000 / 32768

Dynamic Address Lookup Table

The Address Lookup Table explains what LAN stations are in reach through the local switch fabric and which ports are associated with learned addresses.

The web interface and CLI have a reset function that may be used to flush the table.

Port Mirroring

A diagnostic mechanism that enables a user to copy all data traffic transmitted or received on one switch port to a second switch port. This diagnostic tool maybe used in conjunction with specialized software to analyze data traffic content or statistics gathering for troubleshooting, or security purposes.

Source Port	Destination Port	
Port 1	Port 1	Disable

To enable the mirror function, a source port and destination port, must be selected.

The mirror function will automatically be disabled on the next reload if not disabled by the user before hand.

Port mirror function is also configurable using the CLI.

Ping Utility

The ping utility enables the user to verify host access from the management interface of the solidswitch. ICMP message round trip time can be used to understand general performance metrics related to a specific host. Host, Message Count, and TTL are user defined inputs to the function. Output will displayed in near real time to the output pane below.

A ping utility is also available in the CLI.

Diagnostics

The diagnostics screen displays low level system information about the Solidswitch. The screen contains product identification, serial number, MAC address, power status, battery equipment, PoE power usage, and many other operational metrics.

Identification

Product Serial Number	0A80C204341004527C93A000A0000000
MAC Address	00:54:00:1B:25:BC
Firmware Release	20190127
System Runtime (HHMMSS)	64:24:19
System Loads	0.88 0.87 0.85
Current Timestamp	Friday February 1st 2019, 07:47:17 AM
Power Output Limit	150.0W

Power

A/C	1
Internal Power	
+24 PSU	30.18
+24 ORED	30.15
+3.3	3.29
+54 A	53.87
+24 B	53.81

Batteries Installed

	Installed	Charging	V	I	aBCap	dBCap
Battery 1	0	0	12.18	-43.11	0.00	0.00
Battery 2	0	0	5.02	-59.76	0.00	0.00
Battery 3	0	0	4.61	-32.01	0.00	0.00
Battery 4	0	0	4.50	-48.66	0.00	0.00

PoE Power Output

Port 1
PD Class Class 4
Channel 1 3.02   Channel 2 0.00
Sub Total 3.02

Port 2
PD Class Class 4
Channel 1 1.30   Channel 2 0.99
Sub Total 2.28

Port 3
PD Class Class 0
Channel 1 2.89   Channel 2 0.00
Sub Total 2.89

Port 4
PD Class Unknown
Channel 1 0.00   Channel 2 0.00
Sub Total 0.00
Total PoE Consumption 8.18

PoE PSE C Die Temp

TPS 1	154.76	TPS 2	149.72
Init	Passed	Init	Passed

Event Buffer

The event buffer is a facility that stores events of interest to NVM (non volatile memory). The system is capable of tracking the last 1024 entries on a first-in last-out convention. Recorded events may persist between reload and between software upgrades. The event log may be cleared using a reset function available in the web interface and CLI.

Software Updates

The UPS Solidswitch is capable of firmware upgrades. The software section from the settings menu displays several paths for upgrading the firmware.

The first method is automatic update. Automatic update requires that the switch IP Address, Gateway, and DNS settings are configured for internet access. This can also be accomplished using the Embedded DHCP Client. The automatic update check interval is configured to query every 24 hours.

Software Upgrade Actions

Check to see if a remote software update is available (requires internet connectivity).

Check & Install

The second method is to upload the firmware upgrade to the switch using the firmware upload function. This option could be used in a situation where the Solidswitch is not connected to the public internet.

Firmware Upload

Select the firmware upgrade file the click "Upload" to start the upgrade process.

Select Firmware File

Upload

SSH Command Line Interface

Solidswitch includes a line interface configuration shell accessible over the ssh2 protocol.

The majority of network configuration of the SolidSwitch can be accomplished through this configuration shell if desired. Some configuration of ancillary services, PoE scheduling for example, must be configured through the web interface. Configuration of these ancillary services through the configuration shell may be done in a future firmware release.

The configuration shell is a rather intuitive interface, simply typing a question mark followed by an "Enter Key" will display available commands, their respective descriptions, and accepted arguments on the session terminal.

SSH Authentication

The SSH2 command shell supports both password and public/private key authentication. In order to use the public/private key authentication, the public portion of the key should be transferred to the Solidswitch through the access credentials section of the web tool or by using *sshconfig* sub feature of the command shell.

SSH Public Key Generation

The following command can be used on most Linux distributions to generate a public/private RSA key.

```
# ssh-keygen -t rsa
```

The output of the ssh-keygen command should emit something to the effect of:

```
Your public key has been saved in … /.ssh/id_rsa.pub
```

The contents of the *id_rsa.pub* file is the public part of the generated RSA key.

Configuration Output

The show configuration command can be used to dump or display the entire configuration of the switch to the session terminal window.

Command example:

`#show configuration<CR>`

The configuration of the switch is articulated through a mechanism that formats the configuration in such a way so that it may be re-applied back through the configuration shell if need be.

Configuration Input

`#configure terminal<CR>`

Then cut and paste the configuration text in whole or in part into the session terminal.

Configuration Management

Just like the web interface, activation and commit of the running configuration "configuration cache" can be accomplished with the following command examples

Automatic Reload In 5 Minutes:

`#reload in 5<CR>`

Activate the running configuration:

`#activate <CR>`

Write the configuration cache to permanent memory:

`#write memory<CR>`

Cancel the pending reload:

`#reload cancel<CR>`

Configuration Export / Import

Using special remote filename extensions the system configuration database may be exported and staged for importing using the SFTP function of the SSH2 protocol.

Command Examples:

Configuration Export

```
$ scp admin@10.4.1.80:/dbcfgsave.dat ./dbcfgsave.dat
admin@10.4.1.80's password:
dbcfgsave.dat                                          100%   14KB   2.3MB/s   00:00
```

Configuration Import

```
$ scp ./dbcfgsave.dat admin@10.4.1.80:/dbcfgsave.dat
admin@10.4.1.80's password:
dbcfgsave.dat                                          100%   14KB   2.4MB/s   00:00
```

After uploading the configuration database, The imported data is staged for installation on the next restart. A system reload must be issued to proceed.

System Software Upgrade

```
$ scp /upgrades/ssfwupgrade_2020mmDD.bin admin@10.4.1.80:/ssfwupgrade.bin
admin@10.4.1.80's password:
ssfwupgrade_2020mmDD.bin                               100%   19MB   3.9MB/s   00:04
```

After uploading system firmware, The upgrade process automatically begins. This event would be recorded in the system event buffer.

```
[12/09/2019 17:54:27.873] (5) software upgrade started via scp
```

If the software upload is valid, and the uploaded version is newer than the currently installed version, the system will automatically reload, and the new software will be installed.

SSH Command Shell continued.

tftp-config put

Export and transmit configuration database to remote TFTP server.

```
tftp-config put HOST PORT PATH<CR>
```

tftp-config get

Receive configuration database from remote TFTP server, stage for import on reload.

```
tftp-config get HOST PORT PATH<CR>
```

tftp-upgrade

Download firmware upgrade from remote TFTP server, initiate firmware upgrade process.

```
tftp-upgrade HOST PORT PATH<CR>
```

telemetry

Display system telemetry on the terminal

```
Telemetry [interval in seconds]<CR>
```

port-mirror

Enable port mirror function

```
port-mirror src PORT dst PORT<CR>
```

port-mirror disable

Disable port mirror function

```
port-mirror disable<CR>
```

System Recovery

If the system IP address information becomes lost you may recover the information from a power – on event. After the system power-on event, the SolidSwitch will transmit a UDP message to the local broadcast address on port 514. The contents of the message will describe the current interface numbering schema.

System Network Discovery

The following is an example of capturing the broadcast message using the *ngrep* tool. The message may also be captured with Wireshark packet analyzer. The broadcast message is transmitted approximately 60 seconds after a power on.

```
# sudo ngrep -W byline port 514
interface: enp3s0 (10.4.1.0/255.255.255.0)
filter: ( port 514 ) and ((ip || ip6) || (vlan && (ip || ip6)))
#
U 10.4.1.186:55016 -> 255.255.255.255:514 #1
<15>Dynamic Interface:
inet addr:10.4.1.186  Bcast:10.4.1.255  Mask:255.255.255.0
inet6 addr: fe80::254:ff:fe00:1/64 Scope:Link
Static Interface:
inet addr:10.4.1.80  Bcast:10.4.1.255  Mask:255.255.255.0
```

Configuration Database Factory Restore

The SolidSwitch also has a mechanism to reset the internal configuration database back to original factory default settings by way of the micro SD card slot.

To setup a micro SD card perform the following:

1. Format the card with a single fat32 partition.

2. Create a text file the root directory of the card named "commands.txt"

3. The contents of "commands.txt" is a single line containing exactly: "system:default"

4. Power down, then Power up the system, wait 60 seconds, power down.

5. Pull the micro SD card, check the root file system for a new file "command_result.txt"

   command_result.txt contents:

   ```
   Fri Feb  8 20:32:40 UTC 2019
   command: default
   default dataset init
   cardcommands done
   ```

On the next power-on the system will adopt factory default configuration settings.