January 2008
SW1020A

10/100/1000 Auto Bypass Switch

CUSTOMER SUPPORT INFORMATION

Order toll-free in the U.S.: 877-877-BBOX (outside U.S. call 724-746-5500)
FREE technical support, 24 hours a day, 7 days a week: Call 724-746-5500 or fax 724-746-0746
Mail order: Black Box Corporation, 1000 Park Drive, Lawrence, PA 15055-1018
Web site: www.blackbox.com • E-mail: info@blackbox.com

FEDERAL COMMUNICATIONS COMMISSION
AND
INDUSTRY CANADA
RADIO FREQUENCY INTERFERENCE STATEMENTS

This equipment generates, uses, and can radiate radio-frequency energy, and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio communication. It has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart B of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to take whatever measures may be necessary to correct the interference.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of Industry Canada.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique publié par le Industrie Canada.

1. Specifications

Connectors:

Ethernet:	(6) RJ45 for network path connections, (1) RJ45 for Ethernet remote control interface and path monitoring (PING source)
Serial Control:	(1) DB9F for serial RS232 remote control interface
Power:	(2) IEC320 AC power connectors for redundant power connections

Indicators:

Power supply LEDs:	(2) PS1 and PS2 power supply active indicators
Switch position LEDs:	(2) both switch elements in the A-C connection state (BYPASS), or both switch elements in the B-C connection state (NORMAL)
Network status LEDS:	(2) link and activity indicators for Ethernet remote control interface port

Switches:

A/B Gang switch:	(1) momentary toggle switch
Gang Switch enable:	(1) key-lock switch

Power:

Power supply:	(2) internal 100-240 VAC 50/60 Hz power supplies, 12 VDC 3A regulated output

Physical:

Dimensions:	1.75"(H) X 19"(W) X 10.5"(D) 1U, 19" rack mount chassis
Weight:	6 lbs.

MTBF:
100,000 hours

Altitude Tolerance:
10,000 ft. (3048 m) operating

Temperature Tolerance:
Operating: 32° to 104° F (0° to 40° C)
Storage: -4° to 158° F (-20° to 70° C)

Humidity Tolerance:
Up to 95% non-condensing

2. Introduction

The SW1020A Auto Bypass Switch is a 1U rackmount, dual port RJ45 A/B switch that is designed to automatically switch between a “normal” network path and a “bypass” or “failover” path for 10/100/1000 Ethernet network environments. User configurable parameters control an auto-bypass switching function and an auto-recovery switching function to allow the switch to be used in a variety of applications. For example, the Auto Bypass Switch can be used with in-line network monitoring devices, Intrusion Prevention Systems, etc. to automatically remove these devices from the network during maintenance or should they fail, while simultaneously providing a bypass path to insure continued flow of traffic thru the network. To prevent “flapping” between a failed “normal” path, and the bypass path connections, the auto recovery function can be disabled. This allows the problem in the normal path to be corrected before sending a command to the SW1020A to restore the normal network connections.

In order to be able to perform the auto bypass and auto recovery switching functions, the SW1020A Auto Bypass Switch issues ICMP echo request (PING) packets from an internal Ethernet node to any user configurable IP address on the network. Then if the normal path connections go down for any reason, the SW1020A will no longer be able to PING the IP address specified during configuration, and will automatically disconnect the normal path connections and switch to the bypass/failover path connections. If auto recovery is enabled, the SW1020A will automatically re-connect the normal path connections when it is again able to PING the user specified IP address.

In addition to the PINGs used for auto bypass and auto recovery switching, the SW1020A can also be sent a command on its serial RS232 interface or its Ethernet interface, to cause it to issue a single PING to any IP address on the network. This PING command can be used to test network connectivity during initial installation or when troubleshooting network problems.

As noted previously, the Auto Bypass Switch can automatically switch connection states using its auto bypass and auto recovery switching functions. Or the user can remotely issue switch commands via the SW1020A Ethernet interface or RS232 serial interface. If using the Ethernet interface, three different options exist for remotely controlling the SW1020A – the SW1020A supports telnet access, SNMP SET/GET commands via a proprietary MIB, or html access using any web browser. Manual control of the switch is also provided by a momentary contact toggle switch on the front of the unit. This manual toggle switch can be disabled by removing a front panel keylock switch on the SW1020A.

High reliability non-latching telecommunications relays are used in the SW1020A Auto Bypass Switch. When the SW1020A is powered OFF, these non-latching relays make a connection between the “BYPASS or A” ports and the “COMMON or C” ports for each switching element within the Auto Bypass Switch. Thus for most applications, the bypass path through the SW1020A will be from the COMMON ports to the “BYPASS or A” ports, and the normal path will be from the COMMON ports to the “NORMAL or B” ports. With this configuration, should power to the SW1020A switch fail, the bypass path will automatically be connected (the SW1020A switches to the “BYPASS or A” to COMMON connection state) and remain in this state until power is restored. Once power is restored, the SW1020A Auto Bypass Switch can automatically reconnect the normal path (switch back to the “NORMAL or B” to COMMON connection state) if auto recovery mode is enabled. Or the user can issue a switch command via the RS232 or Ethernet remote control interface, or use the front panel toggle switch to restore the normal connection path.

The Auto Bypass Switch also has the ability to issue either SNMP traps, or UDP syslog messages. These messages can be sent to one or more network administrator systems to provide notification when the SW1020A changes connection states either automatically (auto bypass switching or auto recovery switching) or via manual control (front panel toggle switch or commands received on the RS232 or Ethernet interfaces), and when certain other events occur.

3. Configuration

The internal jumpers and DIP switches inside the SW1020A Auto Bypass Switch have been pre-configured at the factory and should not be changed from their default settings. For reference, the factory default settings are as follows: jumpers W1 & W2 in the 2-3 position, SW1 positions 3, 4, & 6 ON, and SW2 positions 1-8 ON.

jumper W1	1-2 position = no SNMP module, serial RS232 only 2-3 position = SNMP module installed, Ethernet & serial RS232
jumper W2	1-2 position = no SNMP module, serial RS232 only 2-3 position = SNMP module installed, Ethernet & serial RS232
DIP SW1	positions 1 & 2 OFF, and positions 3 & 4 ON to limit to $\leq$ 4 port operation position 5 OFF = SNMP module installed, position 5 ON = RS232 only position 6 OFF = non-latching fiber optic modules, position 6 ON = latching foms or relays position 7 OFF = non-latching relays, position 7 ON = latching relays position 8 OFF (reserved for future use)
DIP SW2	positions 1-8 ON (reserved for future use)

There are, however, several parameters related to TCP/IP operations as well as the auto bypass and auto recovery functions that must be initially configured in order to operate the SW1020A Auto Bypass Switch. These parameters are accessible using either the serial RS232 remote control interface or the Ethernet remote control interface. These parameters include:

- IP address, subnet mask, and gateway address for the Ethernet remote control interface on the SW1020A Auto Bypass Switch (this interface also functions as the internal Ethernet node that acts as the "PING source" used by the auto bypass and auto recovery switching functions). Note that the factory default values for these parameters are 192.168.1.30, 255.255.255.0, and 192.168.1.1 respectively.
- IP address and MAC address of the external Ethernet node that the SW1020A Auto Bypass Switch is to monitor in order to determine when to switch between the normal and the bypass paths. A value of 0.0.0.0 for the monitor IP address disables the auto bypass and auto recovery switching functions.
- Monitor interval – this is the time interval between PINGs issued by the internal Ethernet node in the SW1020A, measured in 100 msec increments. For example, if you want the SW1020A Auto Bypass Switch to issue PINGs every 1.5 seconds then set this value to 15. The valid range is 1 to 255 (0.1 seconds to 25.5 seconds). A value of 0 disables the automatic bypass/recovery functions.
- Monitor fail count – this is the number of successive PING attempts that must fail before the SW1020A Auto Bypass Switch automatically switches to the bypass path and removes the normal connection path. The valid range is 1 to 255. A value of 0 disables the automatic bypass/recovery functions.
- Monitor ok count – this is the number of successive PING attempts that must succeed before the Auto Bypass Switch automatically switches back to the normal path and removes the bypass connection path. The valid range is 1 to 255. A value of 0 disables only the automatic recovery function – automatic bypass will still operate. If auto recovery is disabled the user must manually switch back to the normal path via the front panel toggle switch or by issuing a "set system B" command to the Auto Bypass Switch via the RS232 or Ethernet remote control interface.
- Save – this command saves any changes that are made to the configuration parameters for the next startup. If the Save command is not used, the SW1020A will revert back to the prior configuration settings the next time power is cycled, or after receiving a Reset command.
- Reset – this command restarts the SW1020A Auto Bypass Switch. Any configuration changes that were not first saved will be defaulted back to their prior settings.

For additional details regarding the commands used to set these parameters, see Section 7.

4. Installation

4.1 Find a location suitable for installing the SW1020A Auto Bypass Switch, with access to AC power outlets and the connections you intend to switch through the unit.

4.2 If you intend to use serial control, connect a serial cable to the DB9 RS232 console port. The data rate and format is fixed at 9600 bps, no parity, 8 data bits, 1 stop bit, and no flow control. See Table 6.1 for the DB9 connector pin assignment.

4.3 There are two pairs of RJ45 A/B switch elements within the Auto Bypass Switch. Connect RJ45 cables between the SW1020A and the devices/network connections that you intend to switch. The SW1020A simultaneously connects all 8 pins on each C (COMMON) port to either their respective "BYPASS or A" port, or to their "NORMAL or B" port for both switching elements. Telecommunications relays are used to make these connections between ports, which makes the SW1020A completely transparent to data formats, rates, protocols, etc. Note that the switch provides straight through connections. If your application requires a cross-over cable, use only 1 cross-over cable in that path. Use a straight through cable on the other side of the switch. Non-latching relays are used in the SW1020A Auto Bypass Switch, which default to the "BYPASS or A" to "COMMON or C" connection state when power fails or is removed from the switch. Thus the "BYPASS or A" to "COMMON or C" connections are typically used for the bypass/failover path connections, and the "NORMAL or B" to "COMMON or C" connections are used for the normal path connections.

For example, when used with an Intrusion Prevention System or similar devices, the two "BYPASS or A" ports on the SW1020A are typically connected together with a short patch cable. The "NORMAL or B" ports on the SW1020A are connected to the IN/OUT ports on the IPS. And the "COMMON or C" ports on the SW1020A are used to provide the connections between the firewall and the SW1020A, and between the SW1020A and the first edge router/switch on the network. Thus when in the bypass mode, data will flow between the firewall and one of the "COMMON or C" ports, thru the associated "BYPASS or A" port to the second "BYPASS or A" port via the short patch cable, and then out the second "COMMON or C" port to the edge router/switch. And when in the normal mode, the data will flow between the firewall and one of the "COMMON or C" ports, thru the associated "NORMAL or B" port to the IPS, back from the IPS to the second "NORMAL or B" port, and then out the second "COMMON or C" port to the edge router/switch. See figure 1 below for an example of this configuration.

Typical IPS Configuration

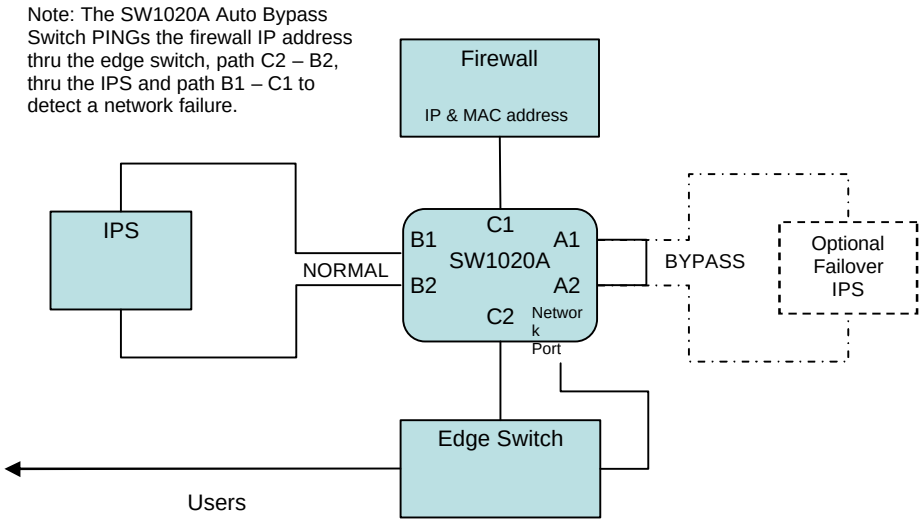

Figure 1

In a typical failover application where a redundant or backup connection is required, the user(s) would be connected to one of the “COMMON or C” ports, with the normal network connection to the respective “NORMAL or B” port, and the failover network connection to the respective “BYPASS or A” port. The Auto Bypass Switch provides two separate A/B switching elements, so two separate host devices can be connected to their own “normal” and “failover” network ports. However, if the auto bypass/recovery functions of the SW1020A are used, both devices will be simultaneously switched between their normal and failover connections when the auto bypass or the auto recovery switching functions occurs. See figure 2 for an example of a failover/backup configuration.

Typical Failover Configuration

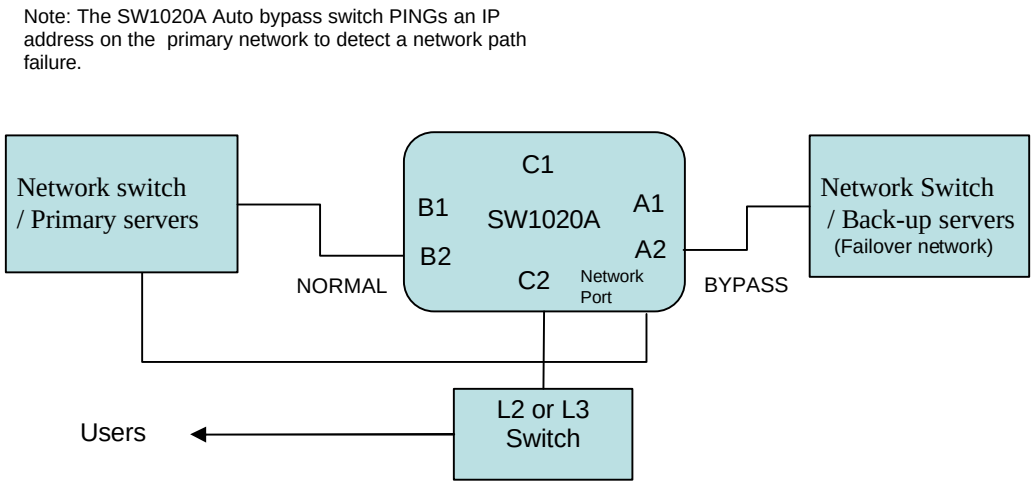

Figure 2.

4.4 Connect a 100-240VAC power source to either power supply connector. If you are using redundant power, connect a power source to both power supply connectors. The indicators PS1 and PS2 on the front of the unit will indicate when each power supply is energized. The switch position LED indicators BYPASS (A) and NORMAL (B) on the front of the unit will light depending on the position of the A/B switching elements within the SW1020A. The BYPASS (A) LED lights when both switching elements in the Auto Bypass Switch are in the “BYPASS or A” to “COMMON or C” connection state, and the NORMAL (B) LED lights when both switching elements within the SW1020A are in the “NORMAL or B” to “COMMON or C” connection state. If one A/B switch element is in the “BYPASS or A” position and the other is in the “BORMAL or B” position, neither LED will be lit (this would occur only if the user issues a “set port n” command that switches only one of the switching elements).

4.5 Before you connect the Auto Bypass Switch’s Ethernet remote control port to your Ethernet network, you should first configure the SW1020A’s TCP/IP related parameters because the default parameters may not work, or could interfere with your network. See Section 3 for a list of the TCP/IP parameters that need to be configured, and see section 7 for a detailed description of the commands used to configure these parameters.

4.6 Once the TCP/IP parameters have been configured, connect the NETWORK port on the Auto Bypass Switch to your layer 2 switch, HUB, or router. If using the SW1020A’s auto bypass/recovery switching functions, this same layer 2 switch/HUB/router should also be connected to the appropriate switch ports on the

SW1020A in order to create the required normal and/or bypass paths through the SW1020A, and to allow the PING packets from the internal Ethernet node on the SW1020A to travel to the desired external Ethernet node on the user's network. See figures 1 & 2 above for examples of typical network connections to the SW1020A Auto Bypass Switch.

In a typical IPS environment, the NETWORK port on the SW1020A would be connected to an unused port on the edge router/switch as noted in the example configuration in figure 1 above. To provide auto bypass switching, the SW1020A should be configured to use the firewall's IP and MAC addresses for the monitor IP address and monitor MAC address parameters. With this configuration, if the SW1020A detects a problem thru the normal path and the IPS to the firewall, it will automatically switch to the bypass path. The auto recovery switching function is typically not used in this type of application, and would normally be disabled. This approach allows the network security manager to verify that when a problem occurs in the normal path thru the IPS (causing the SW1020A to switch to the bypass path), that any problems related to the IPS and the normal path are resolved before the IPS is reconnected to the network. Once these problems have been resolved, the network security manager can then issue a "set system B" command to the SW1020A to switch back to the normal path.

In a typical failover environment, the NETWORK port on the SW1020A would be connected to a layer 2 switch or HUB as described in the example configuration in figure 2 above. To provide auto failover/recovery, the SW1020A should be configured to use the IP and MAC addresses of a device on the "normal" network for the monitor IP address and monitor MAC address parameters. With this configuration, the auto bypass switching function will cause the SW1020A to automatically switch to the failover network if it detects a problem thru the normal path to the device being monitored. And if the auto recovery switching function is enabled, it will cause the SW1020A to automatically switch back from the failover network connection to the normal network connection once the normal network operation is restored (the SW1020A is able to PING the device again on the normal network path).

When using the auto bypass and auto recovery features, the monitorip address and monitormac address parameters can be configured to monitor connectivity to any device within, or outside of the user's network environment. The monitormac address has two modes of operation – it can be manually configured, or it can be set to automatic mode. For automatic mode, simply set the monitormac address parameter to 00 00 00 00 00 00. Then set the monitorip address parameter to the IP address of the device you want to PING in order to monitor the normal network path connections. The SW1020A will issue an ARP request to the gateway router to get the appropriate MAC address it needs to use in the PING packet. Alternately, you can manually enter the appropriate MAC address. If monitoring connectivity to a device on the same subnet as the SW1020A's internal Ethernet node, set the SW1020A's monitorip address and monitormac address parameters to the IP address and MAC address of the device being monitored. If monitoring connectivity to a device on a different subnet/network than the SW1020A's internal Ethernet node, set the SW1020A's monitormac address parameter to the MAC address of the gateway router on the SW1020A's subnet, and set the monitorip address parameter to the IP address of the device being monitored. This allows the PING packet issued by the SW1020A to be routed through the gateway router to the target device on a different subnet/network.

4.7 Once you have configured the TCP/IP parameters, you may also want to configure the SW1020A's access control related parameters. The SW1020A has an internal http server that provides access to its command interface via any web browser. This internal http server can be enabled or disabled. If enabled, a password can also be set, its TCP/IP port number can be configured, and an inactivity timeout can be configured to prevent unauthorized access. The SW1020A also provides telnet access, and SNMP access to its command interface. These interfaces also have additional configuration parameters to restrict unauthorized access. See section 7 for a complete description of theses access control related commands.

5. Operation

Whenever the SW1020A Auto Bypass Switch is powered OFF, or if power fails, the non-latching relays in the SW1020A will be in the "BYPASS or A" to "COMMON or C" connection state, connecting the devices/networks attached to the BYPASS (A) ports to the COMMON (C) ports of both sets of A/B switching elements within the SW1020A. When power is applied to the SW1020A, the appropriate power supply status indicators (PS1 and/or PS2) will light and the BYPASS (A) LED indicator on the front of the unit will also light to show that the non-latching relays in the SW1020A are in the BYPASS (A) position. Both A/B switching elements in the SW1020A will remain in the BYPASS (A) position until the user manually changes switch states via command or via the front panel toggle switch, or if auto recovery switching is enabled and the SW1020A determines that the normal path is available.

5.1 Manual Switching

The SW1020A Auto Bypass Switch can be switched (both sets of ports simultaneously) from the momentary toggle switch located on the front of the unit. This switching action is enabled by the front panel keylock switch, which must be in the position labeled ENABLE for manual switching to occur. When switching using the toggle switch, the switch position LED indicator will light to the appropriate state - BYPASS (A) or NORMAL (B).

5.2 Serial RS232 Switching

The SW1020A Auto Bypass Switch can be switched using commands over a serial communications line. The parameters of the DB9 RS232 console port are fixed at 9600 baud, 8 data bits, no parity, 1 stop, and no flow control (commonly abbreviated as 9600, 8, N, 1, NONE).

When the SW1020A powers up, it will send a sign-on message followed by a prompt character ">" to your serial terminal device. After each command, and any associated response from the unit, it will again issue a prompt character. For systems where the console port is being commanded by software, the software should wait for this prompt character before sending each and every command to the SW1020A.

It is possible to switch either or both sets of switch ports to the BYPASS (A) or NORMAL (B) connection state using the appropriate serial commands. It is also possible to query the position of either or both sets of switch ports using serial commands. The DB9 serial interface is NOT affected by the position of the front panel keylock switch – it will act upon and respond to commands it receives even if the keylock switch is in the DISABLE position.

To display a complete list of the commands available via the serial RS232 interface, type "help" at the command prompt as shown below. For a detailed description of each command, see section 7.

> help

SW1020A CONSOLE COMMANDS:
GET ALL (display all parameters)
GET VERSION (display software versions)
GET[SET] SYSTEM [A/B] (control all system ports)
GET RACK (display all ports)
GET[SET] PORT N [A/B] (control single port)
GET[SET] IPADDRESS [X.X.X.X]
GET[SET] SUBNETMASK [X.X.X.X]
GET[SET] GATEWAY [X.X.X.X]
GET[SET] READCOMMUNITYNAME [string]
GET[SET] WRITECOMMUNITYNAME [string]
GET[SET] WEBENABLE [ON/OFF]
GET[SET] WEBPASSWORD [string]
GET[SET] WEBTIMEOUT [N] (seconds)
GET[SET] WEBPORT [N]

GET[SET] TELNETENABLE [ON/OFF]
GET[SET] TELNETPASSWORD [string]
GET[SET] TELNETTIMEOUT [N] (seconds)
GET[SET] TELNETPORT [N]
GET[SET] MONITORIP [X.X.X.X] (0.0.0.0 to disable)
GET[SET] MONITORMAC [X X X X X X] (X = HEX CHARS)
GET[SET] MONITORINTERVAL [N] (1/10 seconds, 0 to disable)
GET[SET] MONITORFAILCOUNT [N] (0 to disable)
GET[SET] MONITOROKCOUNT [N] (0 = no auto recover)
GET[SET] AUTHENTICATIONTRAP [ON/OFF]
GET[SET] ALERTTYPE [TRAP/SYSLOG]
GET[SET] MANAGER N [X.X.X.X] (0.0.0.0 to disable an entry)
GET MANAGER (display all SNMP managers)
PING X.X.X.X (ICMP ECHO to remote host)
SAVE save settings for next startup
RESET restart (use after SAVE)
>

Notes:

- Commands can be entered in upper or lower case. passwords ARE case sensitive.
- All commands should be terminated with a carriage return (ASCII 13).
- many of the commands can be abbreviated using just first letters, i.e. “g a” for “get all” or “s p 2 a” for “set port 2 a”.

5.3 Ethernet Switching

In order to use the Ethernet NETWORK port, you must set the IPADDRESS, SUBNETMASK, and GATEWAY address of the SW1020A Auto Bypass Switch before connecting to your network (see section 6 for more details).

The SW1020A Auto Bypass Switch can be switched using SNMP commands over a TCP/IP Ethernet network. See the MIB Path Summary in the appendix for a list of SNMP variables and their functions. The SW1020A also supports telnet access, and can be controlled via a telnet session using the same commands as used by the RS232 serial interface. The SW1020A also includes a built in http server that allows all of the commands that are available via the RS232 serial port to be accessed via a web browser interface. See section 8 for a detailed description of this feature.

The NETWORK port on the SW1020A is 10base-T only. There are two status indicators which function as follows. The LINK LED is on whenever the SW1020A network interface is ready for communication. This should happen very shortly after power on, and should go out if there is some problem with the interface detected by the unit. Note that it does not indicate that a valid network connection is made to another device. The ACT LED will blink whenever the SW1020A receives a command from the network interface, when its internal Ethernet node issues a switch command (auto bypass/recovery operation), or when a switching command is issued via the serial port.

After setting up the system and powering up for the first time you may need to change other parameters for your application. These parameters are stored in non-volatile memory and must be made permanent by using the SAVE command. After saving new parameters, it is recommended that you cycle power or use the RESET command to reboot the SW1020A to insure that the newly saved parameters are activated.

6. Network Setup

To perform the initial setup of the SW1020A you can use a serial terminal capable of 9600 baud, no parity, 8 data bits, 1 stop bit, and no flow control. Connect this terminal to the DB9 console connector on the SW1020A using the pinout from table 6.1 below. Use a straight thru M/F cable to connect to an IBM PC standard DB9 serial port.

Table 6.1 – DB9 Pin Assignment

DB9	SIGNAL	DIRECTION
2	RECEIVED DATA	TO TERMINAL
3	TRANSMITTED DATA	FROM TERMINAL
5	GROUND	n/a

Apply power to the system.

After this process is complete you will see a sign-on message displayed on the serial console, e.g.

```
SW1020A Network Agent Version 2.9 JUN 2007
Copyright (C) 2007


System starting ...
console ready.
>
```

At this point the console is ready for the configuration changes necessary before you will be able to communicate with the unit using TCP/IP. You will need to enter an IP address and subnet mask, gateway address, read and write SNMP community names if using SNMP, or a web password for browser access. These parameters then need to be saved into non-volatile memory, and the system will then need to be reset to allow it to reconfigure with the new settings. Any time one or more of these parameters is changed; they must be saved followed by a system reset. The following shows a typical setup session. Change the entered parameters to suit your application requirements. All the console level commands available are described in detail in section 7.

```
>set ipaddress 192.168.1.200
OK
>set subnetmask 255.255.255.0
OK
>set gateway 192.168.1.1
OK
>set readcommunityname public
OK
>set writecommunityname private
OK
>save
OK
>reset
restarting …
```

After the system reinitializes, you will again be greeted by the sign-on message as before. At this time, the unit will respond to SNMP and HTTP messages at the assigned IP address. You can now attach a 10base-T CAT5 cable to the network port and to an available port on your hub/switch/router.

7. Console Commands

The following commands are available from the console prompt of the unit. All commands are case insensitive, although several variable parameters are case sensitive (read/write community names and web password). GET, SET, SYSTEM, and PORT can all be abbreviated by the first letter of the command. This allows shorthand entry of switching commands.

GET ALL

Displays all parameters and settings. An example output is shown below.

```
System Status: B
IP Address: 192.168.1.39
Subnet Mask: 255.255.255.0
Gateway IP Address: 192.168.1.1
Web Enable: Enabled
Web Password: mctech
Web Timeout: 300
Web Port: 80
Telnet Enable: Enabled
Telnet Password: dataman
Telnet Timeout: 80
Telnet Port: 23
Monitor IP Address: 192.168.1.113
Monitor MAC Address: 00 00 00 00 00 00
Monitor Interval: 10
Monitor Fail Count: 5
Monitor Ok Count: 5
Read Community Name: public
Write Community Name: private
Authentication Trap: Disabled
Alert Type: TRAP
SW1020A: 2.9f SEP 2007, SW1020A Rev. D
SNMP Managers:
1: 192.168.1.113
2: 192.168.1.115
3: 192.168.1.149
```

GET VERSION

Displays the software revision of the system.

```
SW1020A: 2.9f SEP 2007, SW1020A Rev. D
```

GET SYSTEM

Displays the system status. This is the same as the status returned by the SNMP variable SW1020AGangPort. It will report “A” if either A/B switch element in the SW1020A is in the BYPASS (A) position, or “B” if both A/B switch elements are in the NORMAL (B) position. This is meaningful only when using system level switching commands.

```
System Status: A
```

SET SYSTEM A[B]

Sets all of the A/B switching elements in the SW1020A to position A (BYPASS) or B (NORMAL).

GET RACK

Displays the connection state of every A/B switching element within the unit. This is the same as the status returned by the SNMP variable SW1020AChannels. It displays a 16 character string showing the status of each switch. Note that the Auto Bypass Switch only uses ports 3 & 4 as A/B switching elements. Ports 1 & 2 are also shown, but do not have any physical connections associated with them. Information in the other 12 positions is not meaningful and will display as "X".

```
Rack Status: AAAAXXXXXXXXXXXX
```

GET PORT N

Displays the status of A/B switching element N (1-16). The response will be "A" for BYPASS or "B" for NORMAL. Note that the SW1020A Auto Bypass Switch uses ports 3 and 4. The other 14 port numbers have no physical connections associated with them and are not used.

```
Port Status: B
```

SET PORT N A[B]

Sets the addressed A/B switching element N (1-16) to position A (BYPASS) or B (NORMAL). Note that the SW1020A Auto Bypass Switch uses ports 3 and 4. The other 14 port numbers have no physical connections associated with them and are not used. Setting the switch state of any of the other 14 positions is not meaningful.

SET IPADDRESS X.X.X.X
GET IPADDRESS

Set or display the current IP address of the network module. Any change will not become permanent until a SAVE operation is performed.

SET SUBNETMASK X.X.X.X
GET SUBNETMASK

Set or display the current subnet mask of the network module. Any change will not become permanent until a SAVE operation is performed.

SET GATEWAY X.X.X.X
GET GATEWAY

Set or display the current gateway IP address of the network module. Any change will not become permanent until a SAVE operation is performed.

SET READCOMMUNITYNAME string
GET READCOMMUNITYNAME
SET WRITECOMMUNITYNAME string
GET WRITECOMMUNITYNAME

Set or display the current read or write community name as specified. Note that these are case sensitive fields. Any change will not become permanent until a SAVE operation is performed.

SET WEBENABLE ON[OFF]
GET WEBENABLE

Set or display the current state of web based access. The network module will not accept any HTTP requests when web enable is off. Any change will not become permanent until a SAVE operation is performed.

SET WEBPASSWORD string
GET WEBPASSWORD

Set or display the current web password. Note that this is a case sensitive field. Any change will not become permanent until a SAVE operation is performed.

SET WEBTIMEOUT seconds
GET WEBTIMEOUT

Set or display the current web timeout in seconds. After a period of inactivity of this many seconds, the network module will request a login. Note that the web timeout cannot be disabled. Any change will not become permanent until a SAVE operation is performed.

SET WEBPORT N
GET WEBPORT

Set or display the current web port number. Changing the web port number from the default can be used to provide an additional level of security. Any change will not become permanent until a SAVE operation is performed.

SET TELNETENABLE ON[OFF]
GET TELNETENABLE

Set or display the current state of telnet based access. The network module will not accept any telnet requests when telnet enable is off. Any change will not become permanent until a SAVE operation is performed.

SET TELNETPASSWORD string
GET TELNETPASSWORD

Set or display the current telnet password. Note that this is a case sensitive field. Any change will not become permanent until a SAVE operation is performed.

SET TELNETTIMEOUT seconds
GET TELNETTIMEOUT

Set or display the current telnet timeout in seconds. After a period of inactivity of this many seconds, the network module will disconnect any current telnet session. Note that the telnet timeout cannot be disabled, it can however, be set arbitrarily large. Any change will not become permanent until a SAVE operation is performed.

SET TELNETPORT N
GET TELNETPORT

Set or display the current telnet port number. Changing the telnet port number from the default can be used to provide an additional level of security. Any change will not become permanent until a SAVE operation is performed.

SET MONITORIP [X.X.X.X]
GET MONITORIP

Set or display the IP address of the device that the SW1020A Auto Bypass Switch is to PING to determine whether or not the normal and/or bypass path is operational. Setting this to 0.0.0.0 disables the auto bypass and the auto recovery functions. Any change will not become permanent until a SAVE operation is performed.

SET MONITORMAC [X X X X X X]
GET MONITORMAC

Set or display the MAC (Ethernet) address of the device that the SW1020A Auto Bypass Switch is to PING to

determine whether or not the normal and/or bypass path is operational. This value is entered as a series of six HEX characters with spaces between each HEX character. If monitoring connectivity to a device on the same subnet as the SW1020A's internal Ethernet node, set the monitormac address parameters to the MAC address of the device being monitored. If monitoring connectivity to a device on a different subnet/network than the SW1020A's internal Ethernet node, set the SW1020A's monitormac address parameter to the MAC address of the gateway router on the SW1020A's subnet. If the monitormac address is set to 00 00 00 00 00 00, the SW1020A will automatically determine the proper MAC address required for the PING packet by issuing an ARP request to the gateway router. Any change will not become permanent until a SAVE operation is performed.

SET MONITORINTERVAL [N]
GET MONITORINTERVAL

Set or display the time interval between PINGs issued by the internal Ethernet node in the SW1020A, measured in 100 msec increments. To issue PINGs every 1.5 seconds, set this value to 15. The valid range is 1 to 255 (0.1 seconds to 25.5 seconds). A value of 0 disables the automatic bypass/recovery functions. Any change will not become permanent until a SAVE operation is performed.

SET MONITORFAILCOUNT [N]
GET MONITORFAILCOUNT

Set or display the number of successive PING attempts that must fail before the SW1020A Auto Bypass Switch automatically switches to the bypass path and removes the normal path connection path. The valid range is 1 to 255. A value of 0 disables the automatic bypass/recovery functions. Any change will not become permanent until a SAVE operation is performed.

SET MONITOROKCOUNT [N]
GET MONITOROKCOUNT

Set or display the number of successive PING attempts that must succeed before the SW1020A Auto Bypass Switch automatically switches back to the normal path and removes the bypass connection path. The valid range is 1 to 255. A value of 0 disables only the automatic recovery function – automatic bypass will still operate if enabled. If auto recovery is disabled the user must manually switch back to the normal path via the front panel toggle switch or by issuing a "set system B" command to the SW1020A Auto Bypass Switch. Any change will not become permanent until a SAVE operation is performed.

SET AUTHENTICATIONTRAP ON[OFF]
GET AUTHENTICATIONTRAP

Set or display the current state of authentication error traps. Authentication traps will be generated when this parameter is set to ON, and not generated when set to OFF. Note that this setting only affects the trap generation, and not how the network module handles an authentication failure. An authentication failure generally means that an SNMP access was attempted with an incorrect community name. Any change will not become permanent until a SAVE operation is performed.

SET ALERTTYPE [TRAP/SYSLOG]
GET ALERTTYPE

Set or display the type of alert messages sent by the SW1020A Auto Bypass Switch when certain events such as a change in switch state occur. The SW1020A can be configured to issue either syslog messages, or SNMP traps. Note that at least one IP address must be entered using the "SET MANAGER N X.X.X.X" command before either syslog messages or traps will be issued. See section 9 for a list of the traps supported by the SW1020A Auto Bypass Switch, and see section 10 for a list of the supported syslog messages.

SET MANAGER N X.X.X.X

Set manager N (1-16) IP address. Up to 16 different network manager devices can be entered as the destination(s) of

SNMP trap messages or UDP syslog messages (depending on the ALERTTYPE setting) that are issued by the SW1020A Auto Bypass Switch. To remove an entry from the list, set the IP address to 0.0.0.0. Any change will not become permanent until a SAVE operation is performed.

GET MANAGER N

Display the IP address of manager N (1-16). If no value is entered for "N", then all managers IP addresses will be displayed.

```
Manager Table:
1: 192.168.1.113
2: 192.168.1.115
3: 192.168.1.149
4: 192.168.1.100
```

PING X.X.X.X

Causes the SW1020A to issue a single ICMP echo request packet to the designated IP address. If a response is received, the SW1020A will display the message "Reply from X.X.X.X". If no response is received within 5 seconds, the SW1020A will display the message "Request timed out".

SAVE

Save settings for next startup. All settings are stored in non-volatile memory and restored upon power on. Changes to parameters will not become permanent unless a SAVE operation is performed.

RESET

Causes a network system reboot and reloads all parameters from stored settings.

HELP

Displays a list of available commands. The help display output is shown below.

>help

SW1020A CONSOLE COMMANDS:
GET ALL (display all parameters)
GET VERSION (display software versions)
GET[SET] SYSTEM [A/B] (control all system ports)
GET RACK (display all ports)
GET[SET] PORT N [A/B] (control single port)
GET[SET] IPADDRESS [X.X.X.X]
GET[SET] SUBNETMASK [X.X.X.X]
GET[SET] GATEWAY [X.X.X.X]
GET[SET] READCOMMUNITYNAME [string]
GET[SET] WRITECOMMUNITYNAME [string]
GET[SET] WEBENABLE [ON/OFF]
GET[SET] WEBPASSWORD [string]
GET[SET] WEBTIMEOUT [N] (seconds)
GET[SET] WEBPORT [N]
GET[SET] TELNETENABLE [ON/OFF]
GET[SET] TELNETPASSWORD [string]
GET[SET] TELNETTIMEOUT [N] (seconds)

GET[SET] TELNETPORT [N]
GET[SET] MONITORIP [X.X.X.X] (0.0.0.0 to disable)
GET[SET] MONITORMAC [X X X X X X] (X = HEX CHARS)
GET[SET] MONITORINTERVAL [N] (1/10 seconds, 0 to disable)
GET[SET] MONITORFAILCOUNT [N] (0 to disable)
GET[SET] MONITOROKCOUNT [N] (0 = no auto recover)
GET[SET] AUTHENTICATIONTRAP [ON/OFF]
GET[SET] ALERTTYPE [TRAP/SYSLOG]
GET[SET] MANAGER N [X.X.X.X] (0.0.0.0 to disable an entry)
GET MANAGER (display all SNMP managers)
PING X.X.X.X (ICMP ECHO to remote host)
SAVE save settings for next startup
RESET restart (use after SAVE)
>

8. Web Browser Interface

The network module provides access to console commands through a web browser interface. When enabled (see SET WEBENABLE command) accessing the default page on the modules IP address (index.html) will present the following page (or similar).
Note: If using a pop up blocker on your web browser, be sure to allow pop ups from the IP address of the SW1020A Auto Bypass Switch, Other wise you could experience trouble receiving a response through the interface.

Figure 8.1 Logon Screen

After successfully entering the correct web password (see SET WEBPASSWORD command) you will get the following page (or similar).

Figure 8.2 Initial Command Screen

IMPORTANT: Do **NOT** click on the "submit" button or press the "enter" key on your keyboard multiple times. The web browser interface on the SNMP module typically takes 5 to 10 seconds to process a command and return a response. Clicking on "submit" or hitting "enter" multiple times while the SNMP module is processing a command can cause the SNMP module to decide that the interface is not functioning properly. If this happens, the SNMP module will become non-responsive until it receives a valid login request i.e. you must re-enter the SNMP module's IP address in the address bar of your web browser, and then re-logon when the logon screen appears.
At this point you may enter any valid command into the text box and click "Send Command" to execute. The following is an example result of the GET ALL command.

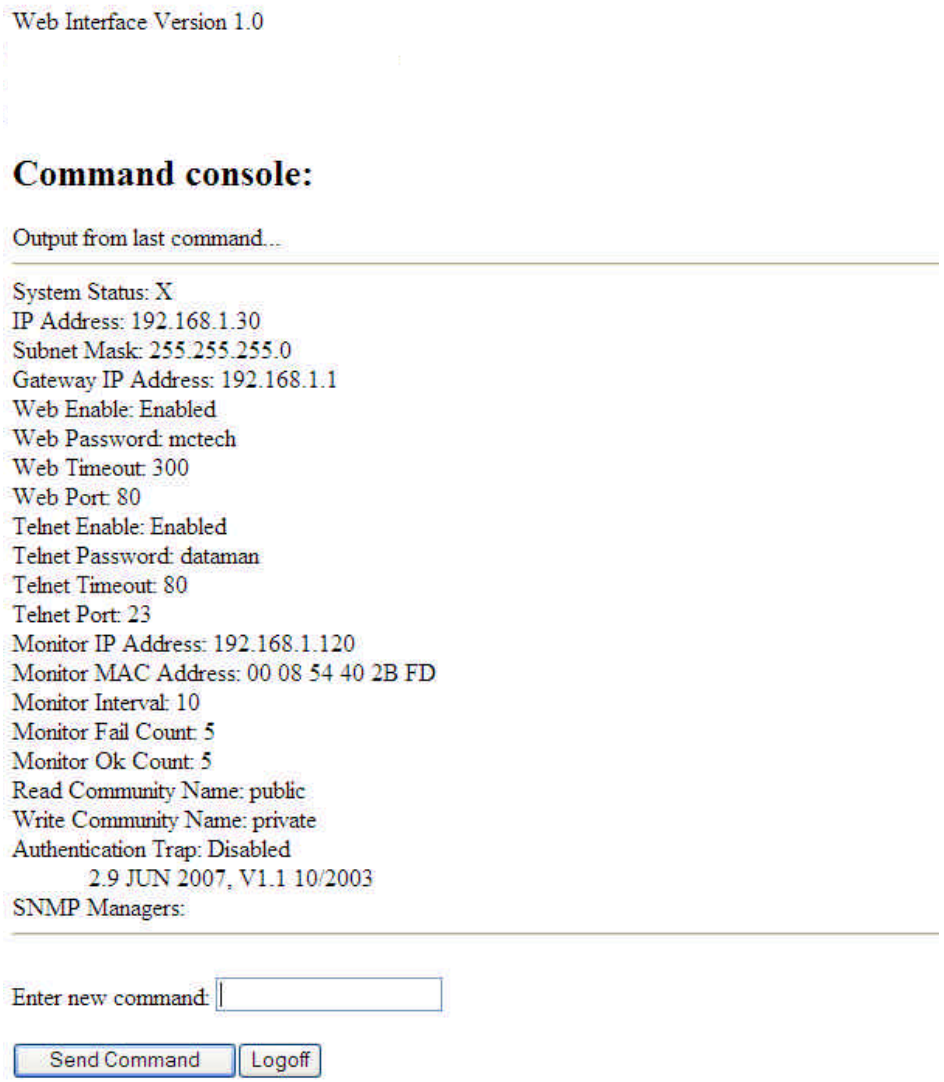

Figure 8.3 Example Command Results Screen

The network controller will allow only one web access session at a time. To free up a session without waiting for the web timeout, click “Logoff”. For this reason, the web timeout should be set to a workable time. Resetting the unit will clear any current web session.

9. Traps Summary

The SW1020A Auto Bypass Switch can be configured to issue an SNMP trap when certain events occur. Use the "SET ALERTTYPE" command to enable traps, and use the "SET MANAGER N X.X.X.X" command to specify the IP addresses of up to 16 different NMS computers that you want to send these traps to (see section 7 for details regarding these commands). The following traps are generated by the SW1020A Auto Bypass Switch. For additional details regarding theses traps, and the SNMP MIB objects supported by the Auto Bypass Switch, please refer to the SW1020A.mib file supplied with your switch.

generic trap 0	coldStart – issued when the unit is powered up, or after a RESET command
generic trap 4	AuthenticationFailure – issued when an invalid SNMP read/write community name is used when attempting to access the Auto Bypass Switch
specific trap 1	KeyLockChange – issued when the front panel keylock switch changes states
specific trap 2	GangSwitchChange – issued when the front panel toggle switch is used to change connection states, or when a "SET SYSTEM" command is used to change connection states
specific trap 4	SwitchPortChange – issued when only one of the two internal switching element in the Auto Bypass Switch changes connections states. This would occur if the "SET PORT N" command was used. This command would not typically be used in an Auto Bypass Switch application.
specific trap 7	PowerStatChange – issued when the status of one of the two internal power supplies changes states (is powered ON or OFF).
specific trap 8	AutoSwitchChange – issued when the Auto Bypass Switch automatically changes connection states via the auto bypass feature, or the auto recovery feature

10. Syslog Messages

The SW1020A Auto Bypass Switch can be configured to issue a syslog message rather than an SNMP trap when certain events occur . To configure the SW1020A to issue syslog messages, you must use the "SET ALERTTYPE" command to select SYSLOG messages, and you need to specify the IP address(es) of the device(s) that will be receiving the syslog messages by using the "SET MANAGER N X.X.X.X" command (see section 7 for details regarding these commands). Once these configuration changes have been made, the SW1020A will issue syslog messages for the following types of events:

- power up cold start, or restart using the RESET command
- SNMP authentication failure (access attempted using incorrect read or write community name)
- change in the state of the front panel keylock switch
- change in the state of both A/B switch elements in the SW1020A Auto Bypass Switch caused by a user initiated command or the front toggle switch
- change in the state of an individual A/B switch element in the SW1020A Auto Bypass Switch caused by a user initiated command
- change in the power ON/OFF state of the two internal power supplies
- change in the state of both A/B switch elements due to the auto bypass or auto recovery switch functions

The syslog messages issued by the SW1020A conform where possible to the general recommendations as described in rfc3164. There is no real time clock within the SW1020A however, so each syslog message uses a default timestamp value of Jan 1 00:00:00. The device receiving the syslog messages will need to apply a timestamp or other identifier if this information is needed. The general format for each syslog message from the SW1020A is as follows:

Jan 1 00:00:00 [SW1020A IP address] Auto Bypass Switch: [specific message based on the event that occurred]

Listed below is each type of syslog message that the SW1020A can issue, followed by the actual syslog message that the SW1020A will send.

power up cold start (or RESET command)
Jan 1 00:00:00 192.168.1.151 Auto Bypass Switch: Switch has been reset.

SNMP authentication failure
Jan 1 00:00:00 192.168.1.151 Auto Bypass Switch: SNMP authentication failure.

keylock switch change disabled to enabled
Jan 1 00:00:00 192.168.1.151 Auto Bypass Switch: Keyswitch change to ON position.

keylock switch change enabled to disabled
Jan 1 00:00:00 192.168.1.151 Auto Bypass Switch: Keyswitch change to OFF position.

gang switch A to B via S S B command (or toggle switch)
Jan 1 00:00:00 192.168.1.151 Auto Bypass Switch: Rack switch from A to B position.

gang switch B to A via S S A command (or toggle switch)
Jan 1 00:00:00 192.168.1.151 Auto Bypass Switch: Rack switch from B to A position.

port 3 change from A to B via S P 3 B command
Jan 1 00:00:00 192.168.1.151 Auto Bypass Switch: Port switch from A to B position.

port 4 change from A to B via S P 4 B command
Jan 1 00:00:00 192.168.1.151 Auto Bypass Switch: Port switch from A to B position.

port 3 change from B to A via S P 3 A command
Jan 1 00:00:00 192.168.1.151 Auto Bypass Switch: Port switch from B to A position.

port 4 change from B to A via S P 4 A command
Jan 1 00:00:00 192.168.1.151 Auto Bypass Switch: Port switch from B to A position.

applied power to PS1 (PS2 already powered up)
Jan 1 00:00:00 192.168.1.151 Auto Bypass Switch: Power supply status changed to two supplies.

removed power from PS1 (PS2 still powered up)
Jan 1 00:00:00 192.168.1.151 Auto Bypass Switch: Power supply status changed to one supply down.

removed power from PS2 (PS1 still powered up)
Jan 1 00:00:00 192.168.1.151 Auto Bypass Switch: Power supply status changed to one supply down.

applied power to PS2 (PS1 already powered up)
Jan 1 00:00:00 192.168.1.151 Auto Bypass Switch: Power supply status changed to two supplies.

auto switch B to A via auto bypass feature
Jan 1 00:00:00 192.168.1.151 Auto Bypass Switch: Automatic switch from B to A position.

auto switch A to B via auto recovery feature
Jan 1 00:00:00 192.168.1.151 Auto Bypass Switch: Automatic switch from A to B position.

1000 Park Drive • Lawrence, PA 15055-1018 • 724-746-5500 • Fax 724-746-0746