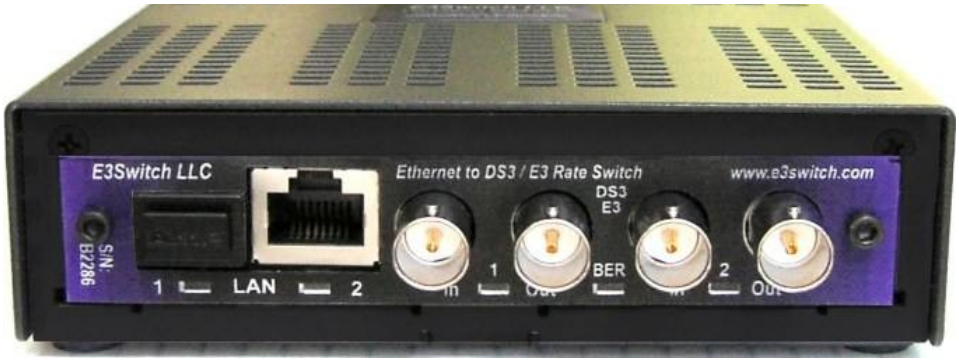
DS3/E3 WAN Monitor with Ethernet Output for HDLC/PPP Applications V5.4

September 14th, 2011



Operating Information

Legal Preface:

LIMITED WARRANTY
E3Switch LLC (E3Switch) guarantees that every unit is free from physical defects in material and workmanship under normal use for one year from the date of purchase, when used within the limits set forth in the Specifications section of this User Guide. If the product proves defective during the warranty period, contact E3Switch Technical Support in order to obtain a return authorization number. When returning a product from outside of the United States of America, clearly state "NOT A SALE. RETURNED FOR REPAIR" on the commercial invoice; and failing to do so, the customer will be responsible for imposed duties and taxes. All customers are responsible for shipping and handling charges for returned items.

IN NO EVENT SHALL E3SWITCH'S LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) RESULTING FROM THE USE OF THE PRODUCT OR ITS DOCUMENTATION, EVEN IF E3SWITCH HAS BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES. E3Switch makes no warranty or representation, expressed, implied, or statutory, with respect to its products or the contents or use of this documentation and specifically disclaims its quality, performance, merchantability, or fitness for any particular purpose. E3Switch reserves the right to revise or update its products or documentation without obligation to notify any individual or entity. Please direct all inquiries to:

E3Switch LLC
80 Coronado Ave
San Carlos, CA 94070
U.S.A.
http://www.ds3switch.com, support@ds3switch.com
TEL: +1-650-241-9941

FCC STATEMENT
This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

INDUSTRY CANADA NOTICE
This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le present appareil numerique n'emet pas de bruits radioelectriques depassant les limites applicables aux appareils numeriques de la class A prescrites dans le Reglement sur le brouillage radioelectrique edicte par le ministere des Communications du Canada

EUROPEAN UNION (EU) STATEMENT
This product is in conformity with the protection requirements of EU Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. The manufacturer cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to CISPR 22/European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

Attention:
This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

International Electrotechnical Commission (IEC) Statement

TABLE OF CONTENTS

Chapter 1: Description and Requirements

The E3Switch WAN Monitor described herein allows HDLC/PPP packets on a T3/DS3/E3 WAN to be easily monitored/recorded via output to an Ethernet port. Inline capability alleviates the necessity for additional WAN tap-hardware. Dual WAN inputs allow monitoring of WAN traffic in each direction.

Fanless operation and extremely low part-count design allows use with greater reliability and in harsh environments. All units are rack mountable. NEBS Level 3 multicard chassis with redundant power are available.

Single or dual LAN output is available in a variety of RJ45 or SFP copper or optical formats at either 100Mbit or GbE/GigE rates depending upon software options purchased. Jumbo 9600-byte frame size is available. If purchased, the second LAN port is available for out-of-band management. An appropriate SFP transceiver must be supplied if the second SFP LAN port is to be used.

Management functions include both comprehensive SNMP statistics with link up/down and DS3 FEAC notifications as well as one-click HTTP, user-friendly, color-coded monitoring of link operational status and bit-error rate. Both HTTP and SNMP management of the Monitor is possible either in-band through the same LAN port as data being recorded or out-of-band if the software option to enable the second LAN port has been purchased.

The WAN circuit being monitored may contain CRC-16/32 or no CRC encoding. The WAN circuit may be framed or unframed, but must contain no T1/E1 channels (unchannelized). X43 scramble decoding is available..

LAN output is typically sent to a recording device. LAN packet format is specified by the user at the layer-2 level. MAC header, VLAN, Ethertype, MPLS and pseudowire control word are all manually specified in the unit's configuration settings.

For ease of installation, the Monitor does not require a configuration setup and will typically work immediately upon connection of LAN and telecom cables. Some modification of default IP management addresses or header output for data recording would typically be desired.

The hot-swappable Monitor card may be purchased in standalone or multi-card chassis and draws a minimal 6 watts of power. Standalone, single units ship in high-reliability, fan-free 1U chassis with rackmount brackets and are available in a 100-240VAC or a ±35-75 volt DC models. NEBS-III, redundant-power multicard chassis are available in 6-slot/1U and 20-slot/3U versions.

Chapter 2: Quick Set-up

Attach the WAN Monitor to a power source. The front panel lights should illuminate. Green is normal; orange indicates an error.

Depending upon the LAN options purchased, HTTP/SNMP management of the unit may be through either RJ-45 LAN Port 2 or through the SFP LAN port. Likewise, WAN data to be recorded may be output through either LAN port. These LAN port assignments are found in the HTTP settings web screen of the unit. Typically, the default configuration has the RJ-45 port assigned to the data recording device and the management interface through the SFP port if purchased or the same RJ-45 port if not.

Attach an Ethernet UTP5 cable from your LAN equipment to the desired LAN port. The Monitor can perform automatic MDIX cross-over vs. straight-through cable adaptation. The monitor's LAN light will change from orange to green if a properly negotiated link has been established. **The network equipment attached to the LAN port of the Monitor should be set for autonegotiation mode in order to allow the Monitor to negotiate a 100Mbit full-duplex connection.** Disabling autonegotiation or using old LAN

equipment may result in the attached LAN equipment configuring to half-duplex mode, resulting in CRC errors and packet loss. Refer to the interoperability section of this document for more information

Use only 75-ohm coaxial cables to attach the WAN Monitor to the DS3/E3 circuit. The monitor is attached either inline with each WAN circuit cable or, alternatively, to a WAN tap. For inline use, the WAN cable in one direction should be attached to the "In" WAN Port 1 and continues to the remote location via the "Out" WAN Port 1. The other circuit direction comes to the "In" WAN Port 2 from the remote location, and proceeds via the "Out" WAN Port 2 to the the local equipment. For use with a WAN tap, the "Out" ports are not utilized and may be left open.

Once the monitor is receiving a valid TDM signal without alarms, the DS3/E3 Port LED will change from orange to green.

Refer to the management chapter of this manual if HTTP or SNMP operating statistics are desired or to change the default administrator password or administrative contact/location information.

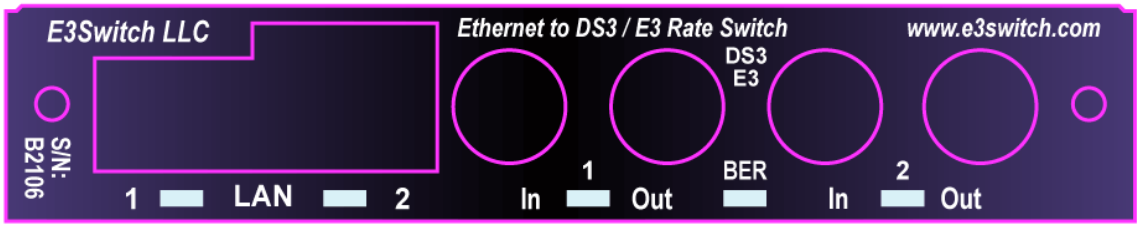
Further HTTP management of the monitor via LAN is required in the following situations:

- if using long (>68m) DS3 coaxial cables
- to set CRC and scrambling to match the WAN circuit being monitored
- to change the default administrator password. This is suggested, as configuration cannot be modified after 5 minutes of any power cycle if the default password has not been changed
- to change the management IP address of the unit
- to set detailed LAN packet header format for packets from the WAN

There is no further configuration or setup required for the Monitor.

Chapter 3: Front Panel

Front Panel Indicators



All Indicators:	Green indicates normal operation. Orange indicates an error condition. Black indicates a disabled port.
DS3/E3 1/2:	Green if the unit is receiving a valid WAN signal with no alarm conditions. Flashes black each time a packet is received on this port Orange steady indicates loss of the incoming WAN AMI signal. Flashes orange/green if incoming signal exists, but an alarm condition is being received.
BER:	Green if OK. Orange flash for each BPV bit error. Orange steady for absence of DS3/E3 receive signal, loss of frame lock onto receive bit-stream, drive-level fault on transmit cable, or excessive receive bit errors. Note: In a dual DS3/E3 unit, the BER will reflect the status of the operational link if one fails.
LAN1/2:	Green when a properly negotiated 100/1000BaseTX Full-Duplex or SFP LAN connection exists. Flashes black each time a packet is received on this port. Orange indicates no valid connection.

Chapter 4: Remote Management HTTP and SNMP

Monitors contain both an HTTP management interface, which may be accessed via a web browser, and an SNMPv2c agent through either LAN port (if second SFP LAN port has been purchased/enabled)

Unit's IP/MAC Address

The source Ethernet MAC address of E3Switch Monitors is 00:50:C2:6F:xx:xx. The Monitor's current IP and MAC addresses are always both shown at the HTTP management screen.

The Monitor's management interface can be initially contacted at either its automatic link-local IP address e3switch.local as described below or at its initial numeric IP address described below. Note that after initial setup, an operator may have changed the contact IP address to a new value and the initial addresses below may not work. Prior to operator reconfiguration the unit will respond to HTTP, SNMP and ping requests to its initial IP address.

For initial communication with the Monitor, it may be necessary to set the network address of the host port communicating with the Monitor to 169.254.xxx.xxx with subnet mask 255.255.0.0. Security protocols advise routers not to forward packets with these link-local IP addresses, so a direct connection is advised. Once initial contact has been established with the HTTP management interface of the Monitor, the Monitor's IP address can be set to a new, static value if desired.

If a unit's operator-configured IP address is lost or forgotten, it can be recovered as described later in this chapter.

Other than the e3switch.local addresses described below, all IP addresses used within the Monitor's management interface must be in xxx.xxx.xxx.xxx numeric format rather than a human-readable DNS-resolvable hostname.

Automatic Link-Local IP Address

E3Switch products are shipped with an initial IP address that conforms to recent zero-configuration link-local standards. This allows multiple E3Switch Monitors on the same IP network to initialize with unique IP addresses without conflict and allows simple ping/HTTP/SNMP access to the Monitors using hostnames e3switch.local or e3switch-2.local,... provided that, free, ZeroConf mDNS software has been installed on the machine attempting to communicate with the Monitor. **Do not prefix www.** prior to e3switch.local. www.e3switch.local will not work.

If multiple WAN Monitors are powered-up on a connected LAN, they will negotiate between themselves to determine which is assigned name e3switch.local and which receives e3switch-2.local and so on. Since the assigned name will not necessarily be fixed to a particular unit after power cycles, the system manager will probably want to use/set the monitor's numeric IP address sometime during or after initial installation.

Web descriptions are available for ZeroConf mDNS and Link-local IPV4LL ip addresses. Free ZeroConf software such as Bonjour for Windows or Avahi is available for Windows/Linux/Unix machines.

Initial Numeric IP Address

The Monitor can also be contacted at its initial default IP numeric address which always takes the form 169.254.aa.bbb. Units typically have the initial IP address listed on top of the chassis or can be initially contacted at the IP address above where aa.bbb matches the serial number listed on the front label.

- The Monitor's current IP and MAC addresses are both shown at the HTTP management screen.

Unknown IP Address Recovery

The following methods may be used to determine a Monitor's IP address if lost or forgotten. Note that once determined, management communication with the unit may only be possible from a host configured to the same IP subnet address if the unit's default router address is invalid.

To manually discover a unit's IP address, unplug all LAN and BNC cables from the Monitor and power cycle the unit. 30 seconds after powerup, the Monitor will begin blinking out its IP address on the leftmost LED. Each digit is counted up as an orange blink with a pause between digits and a short blink for a 0. A decimal in the IP address is indicated with a green blink. For example, <orange><orange><pause><short-orange><pause><green>... would be an IP address that begins “20.”

For those with access to packet sniffers, upon power-up, the Monitor will broadcast several gratuitous ARP packets on its network ports which can be examined with a sniffer or packet monitoring software to determine a unit's IP address. The source Ethernet MAC address of such packets and E3Switch Monitors is 00:50:C2:6F:xx:xx. Tcpdump or Wireshark are two readily available software packages to examine network packets.

Additionally, examination of the MAC address table of an attached LAN switch or router may provide the IP address if the E3Switch MAC address prefix (00:50:C2:6F:xx:xx) can be located.

Management Passwords

The HTTP management statistics page is initially accessible without a password. The HTTP settings page is initially modifiable within the first several minutes after powerup with username *admin* and no password. If the unit has not had its default password changed, after several minutes the settings page will be locked for security reasons. It is desirable to change the default password of the unit. For security reasons, changing the default password of the unit must be done within the first several minutes of any powerup. If

the HTTP management password is lost or forgotten, it may be reset by accessing the HTTP management settings within the first minute after powerup and with no BNC cables attached to the unit.

SNMP statistics may initially be accessed using the read-only community name *public*. Write-community names and variable access authorization may be set through the HTTP management interface.

Security

Please also refer to the password section above.

HTTP Interface Security

Access to the HTTP management interface statistics and settings pages can be selectively limited to users knowing the HTTP management password, which is transmitted securely on the network using MD5 encoding. New values of management settings, or modifications of the administrator password are not encrypted and are visible to users monitoring network packets, as is statistical data requested by an MD5 authorized user or any information visible on a HTTP page.

When logging out from any secure webpage, the browser window should always be closed! Browsers typically continue to send administrator credentials continuously even after apparent logout.

SNMP Security

The Monitor implements SNMPv2c, which is inherently an insecure protocol; however, the Monitor enhances security by implementing view-based access management (VACM), which can restrict read or write access to specific management settings and statistics. When shipped, the Monitor allows read access to “safe” SNMP statistics and prohibits read and write access to statistics and settings which could allow determination of network topology or interfere with normal link traffic. The VACM configuration can be updated through the HTTP management interface to meet the user's needs, and most SNMP variables can also be set through the HTTP management interface in a more secure manner than SNMP allows.

– SNMP VACM Security Warning –
As shipped, the default “safe_ro_view” is secure but not private.
View based access model VACM for SNMPv2c provides good restriction
of access to only specified statistics but no data privacy and
minimal user authentication. When a specific variable is enabled
for reading or writing, from a security perspective it should
be considered either public for reading or public for writing.
Alternatively, most configuration parameters can be set through
the HTTP password-protected interface which is secure.
Viewing snmpd.conf exposes it and community names to visibility by
3rd party network sniffers. All SNMPv2c data on the network
is visible. All community names can be "guessed" and, when used,
become visible to sniffers. Source IP addresses of requests
can be forged. Enabling a write community should be considered
insecure with respect to the specific view variables enabled.
Variables in the groups: interface, ds3, dot3 & mau, control the
link datapath; allowing write access allows disabling the link.
Specific variables disabled for all write users are secure.
Specific statistics disabled for all read users are invisible
and secure.

HTTP Management

The Monitor contains a comprehensive, user-friendly HTTP management interface which allows a manager to monitor bit-error-rates on the DS3/E3 link, lost packets, and user-friendly status messages at a single,

color-coded HTTP screen. A screenshot is available at www.e3switch.com. Most settings that can be modified via SNMP can also be set through the HTTP interface in a more user-friendly manner.

Refer to the configuration section of this document for guidance on specific settings.

Event Log File

A timestamped log of operating status and events may be accessed at the HTTP management administration page.

Resetting

Two options for resetting the Monitor may be accomplished at the HTTP management administration page. A management software reset will reset counters, statistics, MIB variables, and management software of the Monitor without interrupting data flow on the WAN. A hardware reset will temporarily interrupt WAN data flow as if the Monitor had experienced a power cycle. If upgrading firmware, for new functionality to take effect a hardware reset is required after the upgrade but need not be initiated immediately. A software reset is not appropriate after upgrading firmware, as only the management CPU would be reset while the WAN packet transfer CPU would be operating with the older, incompatible version of firmware.

SNMP

The Monitor contains an SNMP agent which can respond to version 1 and version 2c requests for network statistics from remote SNMP clients. The agent can also generate notifications of important network events such as when network ports go up/down or experience high error rates. These trap notifications can be sent to multiple hosts if desired, and using free or commercial software, the receiving hosts can log the notifications or even generate email or pager messages for network managers.

SNMPv2c is inherently an insecure protocol, so the Monitor implements VACM to restrict access to "safe" statistics and settings. Please refer to the security discussion section of this document.

SNMP configuration of various parameters such as community names and trap destinations is accessed through the HTTP management interface and is implemented as a configuration file having an snmpd.conf structure. Snmpd.conf is described by third parties in publicly available documents.

Statistics and settings accessible via SNMP are called MIB-variables and are organized in a hierarchical tree topology. The MIB variable trees implemented by the Monitor include recent versions of the DS3/E3, interface, MAU, dot3, and many of the typical IP-network MIB trees. The full list of MIB trees available is listed by viewing the system.sysORTable of the Monitor. As mentioned earlier, access to certain trees or variables is initially disabled for security reasons, but can be set as the user wishes through the VACM settings. The Monitor can typically return 1000 MIB variables per second in bulk requests and support SNMP response message sizes up to 5000 bytes.

Upgrading Firmware

For activation of additional capabilities of the Monitor, see the "Feature Activation" section. Feature upgrades do not necessarily require a firmware upgrade.

Firmware upgrades may be transferred to the Monitor via the LAN port. A hardware reset, which will interrupt link data flow for several seconds, will be required at some point after the transfer in order to begin using the new firmware. Instructions for performing the TFTP transfer are included with all firmware shipments. The most common source of problems when performing upgrades is attempting a TFTP transfer in ASCII or text mode rather than binary or image mode.

Feature Activation/Upgrade

For activation of additional capabilities of the Monitor after initial purchase, supply the factory with the serial number from the *front* of your Monitor (also shown at the HTTP management page for recent

firmware) and purchase an alphanumeric “factory upgrade key” which is entered at the HTTP management screen.

Chapter 5: Operating Modes and Configuration

Telecom

There are several, low-level configuration settings for TDM ports; though, typically, the default settings are appropriate:

- E3 vs DS3
- cable length (for long DS3 runs only)
- unframed or M13 or C-Bit (for DS3 only)
- CRC length (none/16/32)
- scrambling on/off
- fractional or full-rate utilization

Use a “DS3” configuration setting for North America, Japan, and South Korea; otherwise, “E3” speed.

The cable length setting will transmit a slightly stronger signal on long DS3 coax runs.

Circuit Clock Speed

In the event of incoming clock loss when the monitor is insert inline with the WAN circuit, the transmit clock will automatically switch to a locally generated DS3/E3 clock source.

The receive clock speeds are shown at the bottom of the unit's HTTP management statistics page to assist timing diagnosis.

DS3 Circuit ID PMDL

DS3 Path Maintenance Data Link (PMDL) identification messages associated with C-Bit framed DS3 links may be received. Circuit ID messages convey human-readable, configurable, physical location information of the DS3 source equipment. PMDL Circuit ID messages facilitate confirmation of the data source when presented with a pair of unlabeled BNC cables.

Port to Port Packet Flow

LAN-to-LAN

Full LAN-to-LAN packet flow can be enabled on a unit, if desired. This might be useful if it was desirable for incoming SFP management packets to exit the copper LAN Port 2 of the unit, along with the packets carrying TDM data, in order to be recorded. LAN-to-LAN unidirectional flow for monitoring may also be configured if desired.

LAN-to-LAN should be used cautiously to avoid overloading bandwidth limitations of the unit.

Loopback

C-Bit T3 TDM ports will not respond to FEAC loopback requests.

LAN Port Settings

The hardware for two LAN ports exist on all Monitors shipped; however, entry-level models ship with only 100Base-TX mode on LAN Port 2 enabled. See upgrades section of this manual to enable these additional features if required:.

- GbE, GigE 1000Base-T for the RJ-45 LAN Port 2
- SFP LAN Port 1 which can accept optical or copper (100/1000) SFP transceivers.
- If SFP port has been enabled, either LAN port can be configured as a dedicated out-of-band management port if desired.
- jumbo frames (9600 bytes)

See the "Interoperability" section of this manual for information on packet lengths and detailed port connection/autonegotiation discussion.

The autonegotiation mode of the Monitor must match the autonegotiation mode of attached LAN equipment. If autonegotiation is enabled on the Monitor it must be enabled on the attached equipment. If disabled on the Monitor, it must be disabled on the attached equipment. This requirement is necessary to fulfill 802.3 standards which mandate a fallback to half-duplex operation if an autonegotiation mismatch exists. The Monitors require full duplex LAN connections to operate.

LAN Port Speed

1000Mbit/s LAN speeds are only available via the SFP port or if GbE LAN has been purchased.

100Mbit/s is generally preferred over 1000Mbit/s, which generates significantly more power-requirements, heat, and radiated noise even in the absence of packet flow.

1000Mbit/s LAN port speed may be desireable when one LAN port is configured to monitor the other LAN port in addition to receiving incoming DS3/E3 data. In such a case, the data rate that the LAN port is expected to transmit (the sum of all ports that could be a data source for the LAN port) may be greater than 100Mbit/s. The HTTP management statistics screen will show overflow errors if a port's data rates are exceeded.

Setting more than one LAN port to 1000Mbit/s is not recommended and may result in underflow/overflow errors in certain high packet load, memory-intensive cases.

Autonegotiation Problems

There are rare cases with older LAN equipment in which it may be necessary to disable autonegotiation. If CRC-errors or short packet errors are seen in the management statistics of the LAN port, the attached LAN equipment has probably configured itself to half-duplex mode and colliding packets are being lost. In such a case, autonegotiation should be disabled on both the Monitor and the attached LAN equipment, with both forced to 100BaseTX full-duplex. Autonegotiation interoperability and standards were not well understood by the industry at the inception of 100BaseTX, resulting in some older LAN equipment not understanding the Monitor's autonegotiation advertisement of strictly full-duplex capability.

SFP Second LAN Port

The SFP LAN Port 1 hardware exists on all Monitors shipped and may be enabled as purchased or enabled by purchasing an upgrade password. This upgrade allows an SFP transceiver to enable out-of-band management or data transfer through either LAN port, or enable fiber-optic LAN connections of 10km or more. Refer to interoperability section of this document for compatible SFP transceivers.

Dedicated Management/Data LAN Ports

If the SFP Second LAN Port is in use, then either LAN port may be configured to pass TDM data packets or, selectively, to pass only management or only TDM data packets when such can be determined.

If a LAN port is configured for TDM data-only packets, the unit will drop incoming management packets on that LAN port. On a "data-only" LAN port, these management unicast packets and management broadcast/multicast packets may not be forwarded to the second LAN even if LAN-to-LAN traffic flow is configured.

VLAN

In some firmware versions it is possible to configure a VLAN ID for packets containing TDM data.

VLAN configuration settings shown at the HTTP management page may also be set for communication with the Monitor's management entity.

As shipped, the unit will accept *management* packets with any VLAN tags and attempt to respond to the same. For more robust performance, specific VLAN tag settings can be configured.

Chapter 6: Interoperability

LAN

The LAN ports of the Monitor support, at a minimum, all 100BaseTX Full-Duplex Ethernet connections up to maximum line lengths and are set to auto-MDI/MDIX to automatically detect/correct crossover vs straight LAN cable and autonegotiate for full-duplex and pause frame modes with the attached LAN equipment. Passwords may be purchased to upgrade to enhanced LAN port modes as described elsewhere in this manual.

The management agent accepts and responds with packets having MTU of 1350 bytes in order to automatically allow room for security protocol overheads.

HDLC WAN frames can be longer than Ethernet standards. WAN frames longer than MTU setting configuration will be truncated to the MTU of the LAN.

Autonegotiation problems

There are rare cases with older LAN equipment in which it may be necessary to disable autonegotiation. If CRC-errors or short packet errors are seen in the management statistics of the LAN port, the attached LAN equipment has probably configured itself to half-duplex mode and colliding packets are being lost. In such a case, autonegotiation should be disabled on both the Monitor and the attached LAN equipment with both forced to 100BaseTX full-duplex. Autonegotiation interoperability and standards were not well understood by the industry at the inception of 100BaseTX, resulting in some older LAN equipment not understanding the Monitor's autonegotiation advertisement of strictly full-duplex capability.

It is highly desirable to leave autonegotiation enabled so that changing attached LAN equipment does not result in the new equipment defaulting to half-duplex if set to autonegotiate.

SFP LAN Port 1

This port is designed to be compatible with inexpensive, high-quality, copper or fiber-optic, SFP transceivers from Finisar, which allows LAN connections of 10km or more. Most other industry-standard SFP transceivers will work as well; however, fiber-optic features such as temperature and optical transmit/receive power and alarms will only be available if using Finisar transceivers. Non-Finisar copper, RJ45 SFP transceivers may only operate in 1000Base-T mode, while recommended transceivers from Finisar, and possibly Avago or 3Com will operate in 100Base-TX mode as well.

Pause Frames

The Monitor generates no pause frames and ignores pause command frames sent to it.

Telecom

Monitoring is possible for a variety of E3 or T3/DS3 links (with appropriate media Monitors) such as fiber optic, microwave radio, laser, copper, satellite, or a combination; however, the attachment interface is always via 75-ohm copper coaxial rather than optical. The TDM circuit may be either framed or unframed and supports both M13, M23, clear-channel, C-Bit, and G.751 framing. C-Bit framing is suggested for DS3 links.

Chapter 7: Telecom Connections

Framing and Physical Link

The unit can monitor a variety of E3, T3/DS3 links (with the appropriate media Monitor) such as fiber optic, microwave radio, laser, copper, satellite, or a combination. The Monitor may be used with a standard (i.e., M13, M23, clear-channel, C-Bit or G.751) framed or unframed, full-rate E3 or T3/DS3 link with AMI and HDB3 or B3ZS encoding. C-Bit framing is recommended for DS3 links. The Monitor will report PMDL Circuit ID present on C-Bit links.

Each Monitor regenerates the timing clock of the received TDM bit-stream, within E3 and T3/DS3 standards. High-accuracy receive clock rates are displayed at the unit's HTTP management page.

Telecom Cabling

For the E3 or T3/DS3 connection, 75-ohm coaxial cables with BNC connectors are required. It is important that 75-ohm cable be used and not 50-ohm cable. For long connections or in electrically noisy environments it may be important to use a high-quality 75-ohm cable which will have more consistent shielding and conduction. The maximum length of each cable shall be 440 meters for E3 or 300 meters for T3/DS3, but the acceptable cable lengths of equipment attached to the Monitor must be met as well. For lengths over 135 meters, testing in field should be used to determine whether bit error rates are acceptable. Long cable lengths also require careful selection of cable type and attention to sources of external noise.

Third-party fiber to copper media Monitors can be used with the E3Switch Monitor to implement fiber-optic DS3/E3 links; however, refer to the interoperability section of this document for vendors to avoid.***

Chapter 8: LAN Connections and Performance

LAN Ports

Each LAN port implements the following features to maximize LAN compatibility and link utilization and minimize packet loss:

- autosense/autoconfiguration/autonegotiation with the attached LAN.
- 100Mbit/sec data rates (1000Mbit/s via SFP or if GbE upgrade purchased).
- full-duplex LAN connection.
- 1650-byte packet acceptance (1350 for mgmt and 9600 for jumbo).

These features and their ramifications are discussed below in more detail.

Autonegotiation

The network equipment attached to the LAN port of the Monitor should be set for autonegotiation mode in order to allow the Monitor to negotiate a 100Mbit full-duplex connection.

There are rare cases with older LAN equipment in which it may be necessary to disable autonegotiation. If CRC-errors or short packet errors are seen in the management statistics of the LAN port, the attached LAN equipment has probably configured itself to half-duplex mode and colliding packets are being lost. In such a case, autonegotiation should be disabled on both the Monitor and the attached LAN equipment, with both forced to 100BaseTX full-duplex. Autonegotiation interoperability and standards were not well understood by the industry at the inception of 100BaseTX, resulting in some older LAN equipment not understanding the Monitor's autonegotiation advertisement of strictly full-duplex capability.

It is highly desirable to leave autonegotiation enabled so that changing attached LAN equipment does not result in the new equipment defaulting to half-duplex if set to autonegotiate. Autonegotiation must always be enabled for 1000Mbit/s links.

LAN Cabling

It is important to use the correct cabling for proper operation. Use UTP Category 5 network cable with RJ-45 connectors for the LAN ports, and do not exceed 100 meters (328 feet) in length. Either a straight-through or crossover cable may be used.

Chapter 9: LAN Packet Format for WAN Data Encapsulation

Header Format for WAN Data Encapsulation

Either raw WAN HDLC bytes may be placed on the LAN with no MAC header prepended, or layer 2 headers may be configured for the LAN packets that encapsulate the WAN data. If desired, a MAC header is manually specified at the Monitor's HTTP administration screen and consists of:

ffffffffffff - Destination MAC address (ffffffffffff suggested)

0050c26f3000 - Source MAC address (0050c26f3001 suggested)

81000064 - add VLAN if not blank (81000064 suggested)

8847 - add EtherType if not blank (8847 suggested)

ff0001ff - add MPLS if not blank (ff0001ff suggested)

☒ - add Pseudowire Control Word to MPLS

MTU

WAN HDLC packets that are longer than the LAN MTU configured at the Monitor's HTTP administration screen will be truncated to fit within the specified LAN MTU. 9600-byte jumbo MTU capability may be purchased as an option.

Transport Layer

LAN packets are configured with simple MAC Layer 2 addressing which may include a simple, fixed MPLS header. IP Layer 3 addressing is not supported.

Chapter 10: Troubleshooting

General

A great deal of diagnostic information is available by accessing the HTTP management interface of the Monitor. Refer to the management section of this document for additional information.
The Monitor's *front panel lights can provide useful information* but are often under-utilized. They are simple to read and can indicate where a data connection is being lost. It can be very helpful to learn their meaning and monitor flashes as a packet is received at each port.

Incoming Circuit ID is shown at the top of the Monitor's HTTP management page for C-Bit DS3 links, facilitating confirmation of the remote data transmitter when presented with a pair of unlabeled BNC cables.

The Ethernet networks to which the Monitor connects are complex and may contain thousands of devices, each of which requires proper configuration and performance. As such, network configuration and topology issues dominate when problems arise. When troubleshooting, solutions can be reached more rapidly by remembering that *the most frequent cause of problems arises from improper network configurations*.

The next most frequent source of problems generally arises from *faulty cabling or connectors* or incorrect cable type. Cabling must be UTP5 or better for LAN and 75-Ohm rather than 50-Ohm for TDM. If long TDM cable runs or an electrically noisy environment exists, high-quality coaxial cable will be required.

The least frequent cause of problems will be the hardware of the Monitor itself. This statement is not due to a narcissistic point of view, but rather to the simplicity of configuration features on the Monitor and the low-component count. A microwave radio link, for example, has waveguides that can fill with water, antennas that can become misaligned, foreign objects that can block the path. From a failure point of view, the Monitor is a simpler device.

Performance

Performance issues are addressed in the prior chapters.

Interoperability

The interoperability section of this manual should be reviewed to ensure that appropriate equipment is connected to the Monitor. Connected LAN equipment should adhere to 802.3 standards.

Pinging

Ping is not reliable. The protocol which ping programs use does not guarantee delivery of the data packets. **Ping programs from major software and hardware corporations are known to contain bugs, both in packet content and function**. Generally, however, nearly all of the ping packets on a test network that is not over-loaded should get through; if fewer are received, there is probably a problem.

The ping program is a useful, simple test for a TCP/IP Ethernet network. It is a program that sends a data packet from a source machine to a destination machine, which then returns a response packet. There is a plethora of information about ping and the free public-domain ping utilities available. Ping is often supplied as a standard operating system utility, and often the command "ping" followed by the destination machine's IP address or hostname is all that is required to be typed at the source machine's command line.

The default ping generates approximately one 64-byte packet per second. This is not a robust test. If convenient, locate a ping program or set command line parameters to generate perhaps 50 pings per second and try both small packets and large 1400-byte packets. Be aware that packets larger than 1400 bytes sometimes uncover bugs in the software of ping programs.

Step-by-Step Diagnosis

This section assumes that communication between two machines at opposite ends of the E3, T3/DS3 link (herein the link) is failing. If this is a test in the laboratory or without a TDM circuit present, be sure to read the previous "Laboratory Testing" section first.

1. If access to the HTTP management interface of the Monitor is possible, many useful status messages will be displayed. Typically, any message highlighted in orange should be of concern. Error counters are of lesser concern if they are not incrementing, and some link errors would be normal as link cables are initially connected.

   The DS3/E3 ***BER*** *light of the Monitor should be illuminated and green*. This indicates that a valid, DS3/E3 waveshape is being received without bit errors and with proper framing. Refer to the front panel section of this document for other light colors.

   The DS3/E3 ***port*** *light of the Monitor should be illuminated and green*. This indicates that a valid, carrier signal is being received on the WAN. Refer to the front panel section of this document for other light colors.

2. *Ensure a proper LAN cable is being used*. Straight-through or crossover cabling is acceptable. The LAN light of the Monitor port to which any LAN is attached should be illuminated and green. If not, ensure that the attached equipment is set for autonegotiation and can accept 100BaseTX Full-Duplex links. Refer to front panel section of this document for other LAN light colors.

3. The network equipment attached to the LAN port of the Monitor should be set for autonegotiation mode in order to allow the Monitor to negotiate a 100Mbit full-duplex connection. Forcing either the Monitor's or attached equipment's LAN port to 100Mbit full-duplex may not allow the proper autonegotiation and LAN connection to occur. There are rare cases with older LAN equipment in which it may be necessary to disable autonegotiation. **If CRC-errors or short packet errors are seen in the management statistics of the LAN port, the attached LAN equipment has probably configured itself to half-duplex mode and colliding packets are being lost**. In such a case, autonegotiation should be disabled on **both** the Monitor and the attached LAN equipment with both forced to 100BaseTX full-duplex. Autonegotiation interoperability and standards were not well understood by the industry at the inception of 100BaseTX, resulting in some older LAN equipment not understanding the Monitor's autonegotiation advertisement of strictly full-duplex capability.

4. Monitor lights during packet transmission:
   - With LANs attached, verify, perhaps using pings, that data packets generated by a local machine cause the Monitor's light of the connected LAN port to blink. If not, determine if there is an intermediate router or piece of equipment that is not properly forwarding the data packets to the Monitor. Examine the Link/Activity light on the source machine and any intermediate machines to ensure they behave properly (usually flicker) as well.

5. Enlist the aid of a sniffer program to view at the source and destination machines exactly what data packets are being sent and received. Free public-domain programs such as Wireshark are readily available.

Chapter 11: Third Party Copyright Notices

E3Switch is grateful for and contributes to open source software development which may be protected by the following copyright notices and license terms:

eCos License

E3Switch gratefully acknowledges the contributions of the eCos developers and community. Current eCos source files are available at http://ecos.sourceware.org/ E3Switch implementation-specific modifications to those files are available by contacting E3Switch LLC.

The FreeBSD Copyright

Copyright 1994-2006 The FreeBSD Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE FREEBSD PROJECT ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FREEBSD PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the FreeBSD Project.

The Net-SNMP Copyright

---- Part 1: CMU/UCD copyright notice: (BSD like) -----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000
Copyright 1996, 1998-2000 The Regents of the University of California

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Apache License

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

1. You must give any other recipients of the Work or Derivative Works a copy of this License; and

2. You must cause any modified files to carry prominent notices stating that You changed the files; and

3. You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

4. If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

The SHA2 Copyright

FIPS 180-2 SHA-224/256/384/512 implementation
Last update: 05/23/2005
Issue date: 04/30/2005
*
Copyright (C) 2005 Olivier Gay <olivier.gay@a3.epfl.ch>
All rights reserved.
*
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.
3. Neither the name of the project nor the names of its contributors
may be used to endorse or promote products derived from this software
without specific prior written permission.
*
THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The BZIP2 License

E3Switch gratefully acknowledges Julian Seward, Cambridge, UK. jseward@bzip.org for his selfless contribution of bzip2/libbzip2 version 1.0.4 of 20 December 2006

The atHTTPD License

E3Switch gratefully acknowledges Anthony Tonizzo (atonizzo@gmail.com) for his selfless contribution of athttpd to the eCos community.

Chapter 12: Technical Specifications and Standards

Please see separate specification datasheet.