Intel® NetStructure™ ZT 8101 10/100 Ethernet Switch

Technical Product Specification

July 2004

Order Number: 273837-004

Contents

Figures

Tables

Revision History

Date	Revision	Description
June 2004	004	Added MTBF data.
May 2004	003	Removed reference to redundancy.
June 2003	002	Updates to Warranty, Customer Support and Certifications sections.
December 2002	001	Initial release of this document.

This page intentionally left blank.

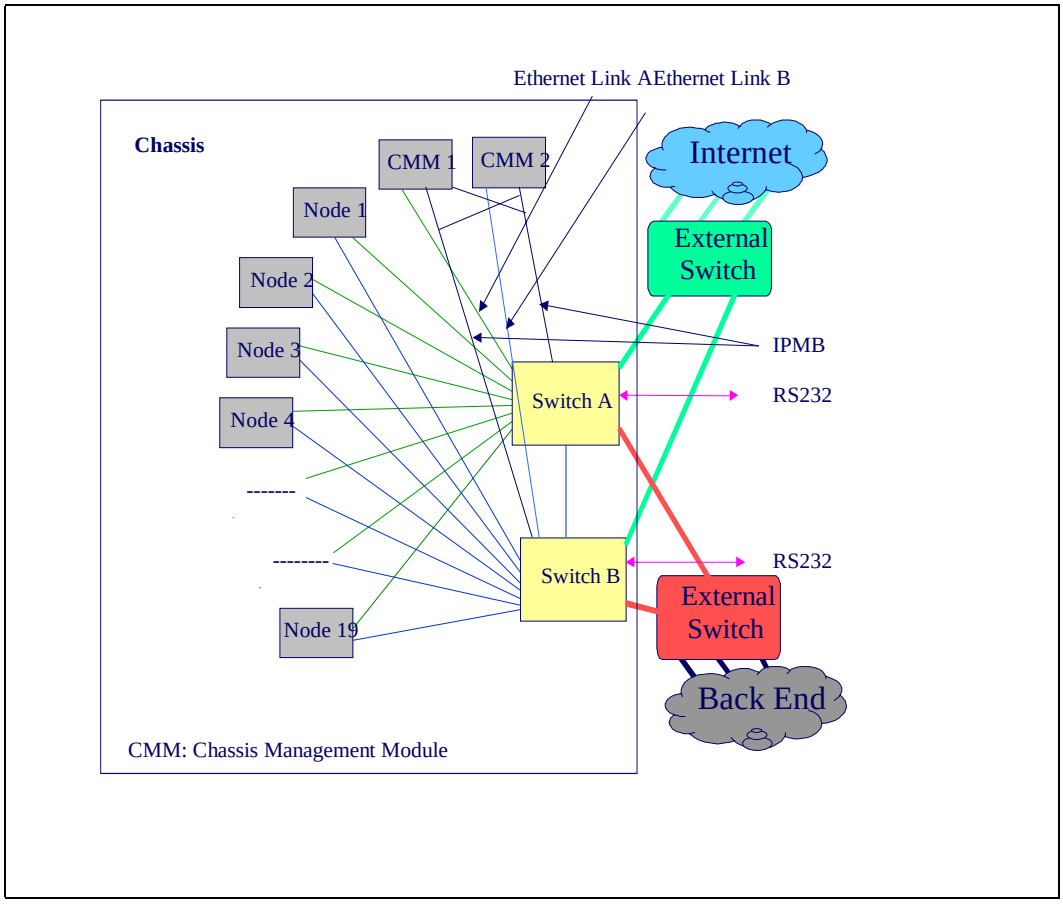
Product Overview 1

The Intel® NetStructure™ ZT 8101 10/100 Ethernet switch is a managed Ethernet switch fabric board, which is designed to fit in a 6U, CompactPCI* form factor and which conforms to the PICMG* 2.16 specifications.

The ZT 8101 switch is a 24-port 100Mbps Ethernet switch with two GbE. There are two GbE and two 10/100Mbps uplink ports on the front panel. Twenty-two 10/100Mbps Ethernet ports are routed to the backplane to provide connections to 19 node slots, two CMM slots, and a redundant switch slot. The printed circuit board dimension is 233 mm (H) x 160 mm (D).

The diagram below shows that two switches can be connected over the backplane to node slots in a dual star configuration as specified in PICMG 2.16.

Figure 1. Two-Switch Configuration



This page intentionally left blank.

PROM Loader 2

After the system boots, the first program executed is the PROM loader. The PROM loader performs the following tasks:

- Runs system memory diagnostics.
- Decompresses RUNTIME from FLASH to system memory for execution.
- Upgrades firmware. Users can upgrade RUNTIME using the Zmodem protocol through the RS-232 port. For instructions, see See “Firmware Upgrade” on page 41.

This page intentionally left blank.

Switch Management 3

The ZT 8101 switch has three methods for configuring switch parameters and viewing switch status and statistics.

3.1 Serial Port

The switch has a serial port on the front panel to which you can attach a terminal or PC running terminal emulation software such as HyperTerminal. The default settings for this serial port are:

- 9600 bps
- Non-Parity
- 8 data bits
- One stop bit
- Flow control off

You can configure the following values:

- **Baud Rate**: Possible baud-rate values are 9600, 38400, 115200.
- **Idle Timeout**: You can specify an idle timeout value, so that the system automatically terminates a user's session after a period of inactivity. Options are Never, 2 minutes, 5 minutes, 10 minutes, and 15 minutes. Never prevents a session from being terminated for idleness.

Note: The other options (flow control, parity, data bits, and stop bits) are not currently configurable.

The serial port requires a cable with a DB-9 terminal adapter and RJ-45 adapter. You can use the Cisco cable kit (Order Number: ACS-DSBUASYN) or make your own. See Appendix G, "Serial Port Requirements" for specifications.

The default user account has empty strings for user name and password. As soon as you create a user, you are prompted to log in as that user and the default account is no longer accessible.

3.2 Telnet Console

The switch's embedded Telnet server allows users from remote systems, which are running a Telnet application over TCP/IP, to log in to the switch, configure it, and view the status of and statistics from the ports. The current implementation allows eight Telnet sessions to be active at the same time.

The Telnet Console interface has the same look and feel as the interface for the serial port.

3.3 Web Console

The switch's embedded Web server allows users from remote systems, which are running a Web browser, to log in to the switch, configure it, and view the status of and statistics from the ports. The current implementation allows 5 HTTP sessions to be active at the same time.

Layer 2 Switch Features 4

This section describes the Layer 2 features that the switch supports.

4.1 Ethernet Port Configurations

4.1.1 Auto-Negotiation and Force Mode

By default, the switch is configured to use auto-negotiation to determine each port's speed and duplex setting. The user can modify this and configure a port to use a specified configuration. The Ethernet ports have the following characteristics:

Table 1. Ethernet Port Characteristics

Ethernet Port	Link Speed	Duplex
Fast Ethernet	10/100 Mbps	Half, Full
Gigabit Ethernet	1000 Mbps	Full

4.1.2 Flow Control

All ports have a traffic limit because they have a limited buffer space to receive incoming frames. Upon reaching the limit, a port either starts dropping packets or triggers flow control. The ZT 8101 switch uses the following methods for flow control:

- **802.3x flow control**: The switch sends PAUSE frames which request remote ports to delay sending packets for a period of time. Sending ports suspend further frame transmission until the specified time period has elapsed.
- **802.3x compliant flow control**: The switch does not send PAUSE frames, but it does respond to them.
- **Back pressure**: The switch fakes a collision and then transmits a jam sequence to ensure all stations are notified of the "collision." This causes the sending ports to trigger their back-off routines and reduces the amount of traffic on the port.

The port type and duplex mode determine which type of flow control is used. The following table lists the port types and their flow control methods.

Table 2. Flow Control Type Determinants

Port Type	Duplex Mode	Flow Control
Fast Ethernet (10/100)	Half	Back pressure
Fast Ethernet (10/100)	Full	802.3x compliant
Gigabit Ethernet	Full	802.3x flow control

Note: By default, flow control is off. If you enable it, it may affect the multicast forwarding rate and packet priority scheduling.

4.1.3 Port Security and MAC Address Learning

For security purposes, you can disable MAC address learning on one or more ports. When MAC address learning is disabled, a port uses the first packet received as a permanent address and accepts broadcast traffic and packets only for that one MAC address. New addresses are not learned.

The default value for each port is learning enabled.

4.2 Port Mirroring

Port mirroring allows the traffic on a particular port to be monitored by sending copies of the packets to a target port. You can then attach a logic analyzer or a RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner. You can configure only one port to be a target port, but you can select multiple ports to be mirrored to this target port.

You can select which traffic is mirrored. For a given mirrored port (or source port), you can select to mirror only incoming traffic, only outgoing traffic, or both.

When mirroring ports, remember the following:

- For optimum performance, you should mirror three or fewer ports at any given time.
- The target port should be operating at the same or higher speed than the source port. If the target port is operating at a lower speed than the source port, packets will be lost.

4.3 Filtering

A filtering database is used to segment the network and control communication between segments. It can also filter packets off the network for intrusion control.

Each port on the switch is a unique collision domain, and the switch filters (discards) packets whose destination lies on the same port as where it originated. This keeps local packets from disrupting communications on other parts of the network.

The switch does some filtering automatically:

- Dynamic filtering - The switch automatically learns and ages MAC addresses and their location on the network. Filtering occurs to keep local traffic confined to its segment.
- Filtering done by the Spanning Tree Protocol - STP filters packets based on topology, making sure that signal loops don't occur.
- Filtering done for VLAN integrity - The switch filters packets from a member of a VLAN (VLAN 2, for example) destined for a device on another VLAN (VLAN 3).

You can also manually configure the switch to drop packets from specified IP addresses.

4.3.1 IP Address Filtering

When filtering by IP address, you have three options. You can have the switch drop the packet based on whether the IP address appears:

- as the source
- as the destination
- in either the source or destination

The table can contain 32 entries, and two table entries are needed to configure a bi-directional filter.

4.4 Forwarding

The switch maintains a forwarding table. This table contains the relationship between destination MAC or IP addresses and the Ethernet port or gateway router the destination resides on. This information is then used to forward packets. This reduces the traffic congestion on the network, because packets, instead of being transmitted to all ports, are transmitted to the destination port only. For example, if Port 1 receives a packet destined for a station on Port 2, the switch transmits that packet through Port 2 only, and transmits nothing through the other ports. This process is referred to as “learning” the network topology.

You can configure forwarding rules for the following:

- MAC address aging
- MAC address forwarding
- IP address to a specified gateway
- IP address to a specified MAC address

4.5 Broadcast and Multicast Storm Control

You can specify thresholds for broadcast or multicast traffic that will activate storm control. When the threshold is exceeded, the switch drops the broadcast or multicast traffic. When traffic levels drop below the threshold, the switch resumes forwarding the traffic again.

The thresholds are applied to all Ethernet ports and cannot be set for individual ports. The threshold specifies in thousands, the number of broadcast or multicast packets per second a port can receive before triggering a storm control response. The possible range is from 0 K to 255 K packets per second. This threshold can be configured to apply to broadcast packets, to multicast packets, or to both.

4.6 Link Aggregation

Link aggregation allows several ports to be grouped together so that they can act as a single port. This is done to either increase the bandwidth of a network connection or to increase fault tolerance. The group has the following assignments:

- **Master port:** This port is the Ethernet port with the lowest port number. All member ports are configured to use its port settings and become members of its VLAN.
- **Anchor port:** This port is in charge of sending control packets, such as spanning tree BPDUs, and the flooding of multicast frames. When a link change event occurs in the group, the anchor port may be re-elected.

When a link aggregation group is deleted or disabled, the ports retain their reassigned port settings. They do not recover their original port settings. For example, suppose that Port 1 belongs to VLAN1 and Port 2 belongs to VLAN2. When you create a group with a starting point of Port 1 and a width of 2, Port 2 will be added to VLAN1 and removed from VLAN2 automatically. If you delete or disable the group later, the Port 2 will still be assigned to VLAN1.

Remember the following guidelines when creating a link aggregation group:

- Up to six groups can be established.
- A group can contain up to eight ports.
- Member ports of a group should always be the same speed and configured in full duplex mode.
- You cannot create a group that includes 10/100 Ethernet ports and 100/1000 Ethernet ports.
- STP will use the port parameters of the master port in the calculation of port cost and in determining the state of the link aggregation group. The following formula is used to calculate the path cost—group path cost = (path cost of master port) minus (number of ports in the group).

4.7 Class of Service Support (CoS)

MAC address priority is a Layer 2 Class of Service. It allows certain frames, based on their MAC address, to receive special handling. The following sections explain how this is done.

4.7.1 MAC Address Priority

The frames can be prioritized based on whether the MAC address appears in:

- the source only
- the destination only
- both the source and destination

Frames that match the criteria are given a priority tag.

4.7.2 Priority Tags

The IEEE 802.1p specification defines a priority tag that is used to classify the frame's forwarding priority. There are eight levels of priority which range is from 0 – 7, with priority 7 as the highest priority.

The switch supports only four hardware priority levels per port, so the eight levels are mapped to four as listed in the table below.

Table 3. Hardware Priority Levels Per Port

Priority in Frames	Priority Queue of ASIC
0 - 1	0
2 - 3	1
4 - 5	2
6 - 7	3

4.7.3 Scheduling

After an Ethernet frame has been prioritized, the switch forwards the Ethernet frame using the strict priority-based scheduling algorithm. With this policy, any packets residing in a higher priority queue are always transmitted first. Only when these queues are empty are packets in lower priority queues transmitted. This scheme can potentially starve packets in lower-priority queues.

Note: If flow control is enabled, a small amount of low priority traffic may be forwarded before high priority traffic.

4.8 VLAN Support

VLANs allow you to group some physical ports as if they were on the same LAN. VLANs can be created either statically or dynamically:

- **Static VLAN—**This VLAN is manually configured on the switch.
- **Dynamic VLAN—**This VLAN uses GVRP (GARP VLAN Registration Protocol) to enable ports to dynamically join a VLAN group.

VLANs reduce traffic because traffic between VLANs is restricted. Bridges forward unicast, multicast, and broadcast traffic only on LAN segments that serve the VLAN to which the traffic belongs.

The switch supports two kinds of VLANs:

- **Port based VLAN—**These VLANs are defined by the physical port connections to the switch and are restricted to the number of ports in the switch. They use untagged frames.
- **IEEE 802.1Q VLAN—**These VLANS are based on a packet-tagging scheme. Packets may be tagged or untagged. A tagged packet's membership in an 802.1Q VLAN is determined by a tag that is inserted in the packet header by the switch or an end node indicating the VLAN number that the packet belongs to. Untagged packets are treated as if they were in a port based VLAN, where a connection to one of the switch's physical ports determines VLAN membership. Physical ports can belong to only one VLAN as an untagged port, but can belong to more than one 802.1Q VLAN as a tagged port. By default, all ports belong to a special VLAN called “default”. This default VLAN is a IEEE 802.1Q VLAN, which has the following unique characteristics:
  - The name and the type fields are read-only.
  - It cannot be deleted.
  - It can contain no VLAN members.
  - Its VID is 1, which cannot be changed.

All user-configured VLANs have the following characteristics:

- The size of VLAN name field is 32 bytes.
- Ingress checking is set to on.
- Up to 32 static VLANs can be configured.

The switch supports a maximum of 255 VLANs (64 static, the rest dynamic).

4.8.1 Static Port-Based VLANs

A port-based VLAN is the easiest type to configure on the switch because you need to specify only the following:

- VLAN name
- Member ports

The complexity of the VLAN configuration is totally hidden. The switch applies the following rules when it creates the VLAN:

- Tagged frames are discarded. With port-based VLANs, frames are assumed to be untagged, so that the VLAN members do not receive frames coming from another VLAN.
- VLAN ID is assigned using an internal algorithm. The switch allocates the largest free VLAN ID which is smaller than 4095 (for example, 4094, 4093, 4092).
- The member port's PVID is assigned as the VLAN ID.
- A port can only belong to one port-based VLAN.
- Port-based VLANs are not included in GVRP advertisement.

4.8.2 Static IEEE 802.1Q VLANs

A static IEEE 802.1Q VLAN is more complex than a port-based VLAN, but it is also more flexible. Tagged ports can belong to more than one VLAN. You can assign ports the following attributes:

- **Tagged Member Port:** When a tagged member port sends a packet, the port changes the packet header to include the 32-bit tag associated with the PVID (Port VLAN Identifier). If the port is attached to a device that is IEEE 802.1Q VLAN compliant, (VLAN-tag aware), the port can be set to tagged.
- **Untagged Member Port:** When an untagged member port receives a tagged packet, the port strips the tag and changes the packet to an untagged packet. If the port is attached to a device that is not IEEE 802.1Q VLAN compliant (VLAN-tag unaware), the port should be set to untagged.
- **Forbidden Port:** When configured as a forbidden port, the port is designated as not being a member of the VLAN and prevents packets tagged with the VLAN's VID from entering the port.
- **Non-member:** This labels the port as not being a member of the VLAN.

You can also enable or disable the following per port for IEEE 802.1Q VLANs:

- GVRP
- Ingress Checking

GVRP must be enabled globally on the switch before individual ports can be enabled.

4.8.3 Global GVRP Settings

The global GVRP flag determines whether GVRP (Group VLAN Registration Protocol) is enabled on the switch so that the switch can share VLAN information with other switches, and VLANs can span multiple switches. When this flag is disabled, VLANs are confined to the physical connections of the switch. By default, this flag is disabled.

GVRP uses the following settings, and they are not configurable:

- Join timer—200 ms
- Leave timer—600 ms
- Leave all timer—10 seconds

4.8.4 Ingress Checking

Ingress checking conditions the forwarding service for an Ethernet port. It has two states:

- **Off:** If an Ethernet port is configured with ingress checking off, all incoming tagged frames are forwarded, even when the receiving port is not a member of the destination VLAN of the frame.
- **On:** If an Ethernet port is configured with ingress checking on, all incoming tagged frames are not forwarded. If the VID in the tagged frame belongs to the VLAN ID set, the frame is forwarded; otherwise the frame is dropped.

The following table summarizes the conditions for forwarding tagged frames.

Table 4. Conditions for Forwarding Tagged Frames

	Tagged Frame with the VID in the VLAN ID Set	Tagged Frame with the VID Not in VLAN ID Set
Ingress Checking On	Forward	Discard
Ingress Checking Off	Forward	Forward

4.9 GMRP

GMRP (Group Multicast Registration Protocol) allows ports to dynamically join multicast groups. It provides a mechanism that allows bridges and end-stations to dynamically register (and subsequently, de-register) group membership information with the MAC bridge attached to the same LAN segment. It also provides a mechanism for that information to be disseminated across all bridges in the bridged LANs that support extended filtering services. The operation of GMRP relies upon the services provided by GARP (Generic Attribute Registration Protocol).

In Release II, the switch will have a global flag to configure the GMRP protocol status for the switch, and its default value will be disabled. The global setting will need to be enabled before individual ports can be enabled. Once enabled, each individual port can be configured to participate in GMRP or not.

The switch will have the following restrictions on members:

- The maximum number of static entries will be 32.
- The maximum number of dynamic entries will be 64.

4.10 Spanning Tree Protocol (IEEE 802.1D)

The Spanning Tree Protocol (STP) prevents loops in a network by allowing only one active path between any two network devices at a time. STP operates on two levels. The switch has a global setting, which either enables all ports to participate in STP or prevents all ports from participating in STP. When STP is globally enabled on the switch, STP can be enabled and disabled on individual ports.

4.10.1 Forwarding Database (Layer 2 Address Table)

The Layer 2 MAC forwarding database contains at most 8 KByte of entries (over 8,000 addresses). The default aging time for dynamically learned entries is 300 seconds. The value is user-configurable; the range is 300 to 1,000,000 seconds. The switch has a minimum learning rate of 3K MAC addresses per second.

When the switch discovers that a topology change has occurred, the STP aging time is decreased to the “Forward Delay” time, which has a default value of 15 seconds. (The default STP aging time is 20 seconds.)

The forwarding database supports two types of static entries: static and black hole.

- **Black Hole**: If a black-hole entry is added for a specified MAC address, the switch discards all frames with the specified MAC address in the source or destination field.
- **Static**: If a static entry is added for a MAC address, the switch forwards all frames with this MAC address to a specified port.

4.10.2 Path Cost Issue

When you enable STP and you do not configure a port cost for a port, the switch assigns a default port cost based on the port’s current link speed.

Table 5. Path Cost

Link Speed	Default Cost	Range
10 Mbps	100	1-65535
100 Mbps	19	1-65535
1000 Mbps	4	1-65535

For the master port of the group, the path cost is the assigned value minus the number of ports in the group. However, if you configure the path cost for the master port, the configured value will be used instead.

This page intentionally left blank.

Network Management 5

5.1 Security

For increased security, the switch supports restricting management access to a specified list of IP addresses. The management station IP address is composed of an IP address and an Ethernet port number. This list determines which stations can request authentication to the switch through the SNMP, Telnet, and Web interfaces. For the request to be considered, the station's IP address must match one in the list. If no addresses are entered into the list, any station can request authentication to the switch. SNMP then uses community strings to control access. The Telnet and Web interfaces use user accounts to enforce security.

5.2 IP Interfaces

An IP interface associates an IP address with a specific VLAN, which allows the VLAN to act as Layer 3 and be configured for RIP and multicasting protocols. Each VLAN must be configured prior to setting up the corresponding IP interface. An IP addressing scheme must then be established and implemented when the IP interfaces are set up on the switch.

5.2.1 System IP Interface

The switch is shipped with one pre-configured IP interface called System. This name cannot be modified. By default, the System IP interface is bound to the default VLAN (VID=1). This VLAN contains all the switch's Ethernet ports.

You can assign or change the IP address of the System IP interface with a manual assignment, BOOP, or DHCP. The switch uses the IP address assigned to the switch as the IP address for the System IP interface.

Note: BOOTP and DHCP are only available for the System IP interface.

5.2.2 Additional IP Interfaces

To add an IP interface to the switch, you must first configure a VLAN and then associate an IP address (subnet mask and gateway) with the VLAN.

Note: The switch must have a manually assigned IP address in order to configure additional IP interfaces.

User defined IP interfaces differ from the System IP interface in the following ways:

- They cannot use BOOTP/DHCP to get a dynamic IP address. They must be assigned a manual IP address.
- They can be renamed. However, when the change is applied, all other settings for the IP interface are changed to their default values. This includes the settings for RIP and the IP multicast protocols.

5.3 SNMP Agent

The switch supports the SNMPv1 agent. The following sections describe which MIBs and traps the switch supports.

- If the support column label is No, the comment field explains why it isn't supported.
- If the support column label is Partial, the comment field gives further explanation.

5.3.1 RFC 1213 (MIB-II)

Table 6. RFC 1213 (MIB-II)

Group	Support	Comment
System (1)	Full	
Interface (2)	Full	
AT (3)	No	Deprecated by NetToMedia table
IP (4)	Partial	IpRouteTable is read-only
ICMP (5)	Full	
TCP (6)	Full	
UDP (7)	Full	
EGP (8)	No	

5.3.2 RFC 1493 (Bridge MIB)

Since the bridge MIB was defined before VLANs were invented, the address table defined in bridge MIB does not have VLAN information. Therefore, all the operations for a learned or dynamic entry in the address table apply only to the default VLAN.

Table 7. RFC 1493 (Bridge MIB)

Group	Support	Comment
Dot1dBase	Full	
Dot1dStp	Full	
Dot1dSr	No	Source Routing is not needed.
Dot1dTp	Full	
Dot1dStaticTable	Full	

5.3.3 RFC 1643 (Ether-Like MIB)

Table 8. RFC 1643 (Ether-Like MIB)

Group	Support	Comment
Dot3StatsTable	Full	
Dot3CollTable	Partial	ASIC has no such counter. All counters are displayed as zeros.

5.3.4 RFC 1757 (RMON)

Table 9. RFC 1757 (RMON)

Group	Support	Comment
Statistics (RMON 1)	Full	
History (RMON 2)	Full	
Alarm (RMON 3)	Full	
Host (RMON 4)	No	
HostTopN (RMON 5)	No	
Matrix (RMON 6)	No	
Filter (RMON 7)	No	
Capture (RMON 8)	No	
Event (RMON 9)	Full	

5.3.5 RFC 1724 (RIP MIB)

Demand circuit is not supported.

Table 10. RFC 1724 (RIP MIB)

Group	Support	Comment
rip2Globals (rip2 1)	Full	
rip2IfStatTable (rip2 2)	Full	
rip2IfConfTable (rip2 3)	Full	
rip2PeerTable (rip2 4)	Full	

5.3.6 RFC 2096 (CIDR MIB)

Table 11. RFC 2096 (CIDR MIB)

Group	Support	Comment
ipCidrRouteNumber	Full	
ipCidrRouteTable	Full	

5.3.7 RFC 2233 (Interface MIB Using SMIv2)

Table 12. RFC 2233 (Interface MIB Using SMIv2)

Group	Support	Comment
ifTable	Partial	Per VLAN counter is not available
ifXTable	Partial	Per VLAN counter is not available
ifStackTable	Full	
ifTestTable	No	Deprecated
ifRcvAddressTable	Partial	No such ASIC counters. All counters display as zero

5.3.8 RFC 2674 (VLAN MIB)

Table 13. RFC 2674 (VLAN MIB)

Group	Support	Comment
dot1dExtBase	Full	
dot1dPriority	Partial	• The dot1dPportNumTrafficClasses is read-only. • The dot1dUserPriorityRegenTable is not supported. • The dot1dPortOutboundAccessPriorityTable is not supported.
dot1dGarp	Full	
dot1dGmrp	Full	
dot1dTpHCPortTable	Full	
dot1dTpPortOverflowTable	Full	
Dot1qBase	Full	
Dot1qTp	Partial	• The dot1qForwardAllTable is not supported. • The dot1qForwardUnregisteredTable is not supported.
Dot1qStatic	Full	
Dot1qVlan	Partial	• The field acceptableframetypes in dot1qPortVlanTable is read-only. • The dot1qLearningConstraintsTable is read-only because SVL is not supported. • All counters are zero in the dot1qPortVlanStatisticsTable. • All counters are zero in the dot1qPortVlanHCStatisticsTable.

5.3.9 Traps

Table 14. Traps

Trap Code	Specific Number	Description
0	0	Cold Start
1	0	Warm Start
2	0	Link Up
3	0	Link Down
4	0	Authentication Failure
5	1	New Root (STP)
5	2	Topology Change (STP)

5.4 TFTP Client

TFTP is a simple protocol used to transfer files without any kind of authentication. It runs on top of UDP, using timeout and retransmission to ensure that data arrives. The switch's TFTP client allows users to copy files from and to a remote system that is running the TFTP server protocol. The TFTP client allows only one user to access it and transfer files.

You can use the TFTP client is to do the following:

- Download firmware.
- Download and upload the switch's configuration file.
- Upload the switch's history log.

Note: Some TFTP servers cannot determine when a transaction is aborted. In these cases, you must reboot the switch, which restarts the TFTP client and re-initializes the TFTP transaction.

5.5 Ping

The Ping utility invokes the ICMP echo request and echo reply messages. A host or gateway sends an ICMP echo request message to a specified destination. Any machine that receives an echo request formulates an echo reply and transmits it to the original sender. The echo request and associated reply can be used to test whether a destination is reachable and responding.

When handling a subnet-broadcast or a directed-broadcast ICMP echo request, the switch forwards the subnet-broadcast or directed-broadcast ICMP echo request to the destination network.

This page intentionally left blank.

Layer 3 Unicast Routing Protocols 6

6.1 ARP Table

The ARP table maintains the mappings from Internet addresses to hardware addresses. There are two types of ARP entries: dynamic and static.

When a static ARP entry is added to the switch's ARP table, the switch does not send an ARP query to the configured IP address. This allows the switch to connect to devices that have not implemented ARP.

The ARP table has the following characteristics:

- Static entries have higher precedence than dynamic entries. Therefore, a static entry will not be overwritten by a dynamic entry.
- The aging time for dynamic entries is 20 minutes. This value is not configurable.
- The table can be up to 2 K in size.
- Up to 32 static entries are allowed in the table.

6.2 Routing Table

TCP/IP routing protocols have ways of discovering the reachable IP address prefixes and, for each prefix, the next-hop router to use to forward data traffic to the prefix. The information exchanged between routers results in an internal database called the routing table, which instructs the router how to forward packets. There are two common implementations for a router's routing table: hash + binary tree algorithm and Patricia tree. Both algorithms have their strengths and weaknesses. Since Layer 3 software is currently configured to use the Patricia tree algorithm, the ZT 8101 switch uses the Patricia tree algorithm.

The switch's routing table has the following characteristics:

- The table can be up to 2 K in size.
- Up to 32 static entries are allowed in the table.

6.3 Multi-Netting

In legacy networks, multi-netting is commonly used to configure a physical router port with more than one IP interface. In a Layer 3 switch, an IP interface is bound to a single VLAN. To accommodate multi-netting, you must configure two or more tagged VLANs to span the same physical ports and then assign each VLAN a different IP address.

The VLANs must include tagged ports, because untagged ports can only belong to one VLAN.

6.4 RIP v1 and RIP v2

RIP is a routing protocol based on the distance-vector algorithm. The ZT 8101 switch supports both RIP v1 and RIP v2. You can configure the following RIP options:

- Enable or disable RIP on the switch.
- Enable or disable transmitting RIP packets on a specified IP interface.
- Enable or disable RIP receiving RIP packets on a specified IP interface.

RIP MD5 authentication is not supported.

Layer 3 Multicast Routing Protocols 7

The ZT 8101 switch supports both DVMRP and PIM-DM, and both protocols can be enabled at the same time. However, an IP interface can only be enabled for one of these protocols.

7.1 Router Ports

When the switch detects routing control packets (RIP, OSPF, DVMRP, and PIM) or IGMP query packets on an Ethernet port of a specific VLAN, the switch automatically designates the port as a dynamic router port. Router ports become default members of the learned multicast groups in the VLAN.

The switch allows you to configure ports as static router ports. These ports also become default members of the learned multicast groups in the VLAN.

7.2 Multicast Forwarding Rules

The forwarding rules depend upon whether the packets need to be forwarded within a VLAN or between VLANs. The following sections describe these rules.

7.2.1 Multicast Forwarding within a VLAN

The following two tables describe the forwarding rules for multicast data within a VLAN. The first table describes the rules for incoming packets, and the second table describes the rules for outgoing packets.

Table 15. Rules for Incoming Packets

Incoming Packet Type	Will be sent to
IP Multicast Data Packet (IGMP and IGMP Snooping is disabled)	VLAN flooding.
Destination Unknown multicast data	Either VLAN flooding, or if the customer requests, dropped.
Router Packet (OSPF, etc.)	Router ports only.
IGMP Report	Router ports only.
IGMP Query	VLAN flooding.
IGMP Leave	Router ports only.
IGMP Group Specific Query	Either VLAN flooding, or if there are group member ports and/or router ports, the data is sent to them.
Multicast data packet destined for a learned multicast group	Group member ports and router ports.

Table 16. Rules for Outgoing Packets

Outgoing Packet Type	Will be sent to
IGMP Query	All VLAN member ports.
IGMP Group Specific Query (IGMP)	Group member ports and router ports.
IGMP Group Specific Query (IGMP Snooping)	The ports that received IGMP leave packets and the router ports.

7.2.2 Multicast Forwarding between VLANs

When a multicast routing protocol is enabled, such as DVMRP or PIM, the multicast data can be forwarded to other IP interfaces, if needed. Either software or hardware can be used to forward an IP multicast packet. The switch currently supports software forwarding.

7.2.2.1 Software Forwarding

To improve switch performance, IP multicast packets are flooded to the VLAN domain and are not sent to switch's CPU. When you enable any multicast routing protocol (DVMRP or PIM-DM), all of the IP multicast packets are sent to switch's CPU to do further forwarding processing.

An internal multicast forwarding cache is used to match an incoming IP multicast packet with a forwarding IP interface. The multicast forwarding cache contains the following information:

- The sender's source IP address
- The sender's multicast group IP address
- A bitmap of forwarding IP interfaces

The multicast group IP address is used as the table's index.

When the switch receives an IP multicast packet, it either builds or updates the internal multicast forwarding cache. The relevant bit in the forwarding bitmap is updated according to the results of multicast routing protocol exchanges and IGMP reports.

The following tables describe the forwarding rules for multicast data.

Table 17. Forwarding Rules for Incoming Multicast Data

Incoming Multicast Data Packets	Behavior	Remarks
Unknown multicast data	• Builds IP multicast cache. • Forwards to the entries in the bitmap for the group.	DVMRP or PIM-DM is enabled.
Known group member multicast data	• Builds IP multicast cache. • Forwards to the entries in the bitmap for the group.	DVMRP or PIM-DM is enabled.

Table 18. Forwarding Rules for Multicast Data to Another IP Interface

Forwarding Multicast Data Packets to another IP interface	Behavior	Remarks
Unknown multicast data	Forwards to router ports.	DVMRP or PIM-DM is enabled.
Known group member multicast data	Forwards to group member ports and router ports.	DVMRP or PIM-DM is enabled.

7.3 IGMP Queries

An IGMP querier sends IGMP Query packets periodically to help to maintain the multicast group information for a VLAN. When IGMP Snooping is enabled for a VLAN, the switch uses the following states to determine whether the VLAN becomes a querier:

- **Non-Querier:** Prevents the VLAN from becoming a querier.
- **V1 Querier:** Enables the sending of IGMPv1 query packets. If no querier is present in the VLAN or the VLAN's IP address is smaller than current V1 querier, the switch becomes the querier for the VLAN. IGMPv2 group specific query and leave packets are not handled.
- **V2 Querier:** If a V1 querier is present in the VLAN, the switch remains silent. If no querier is present in the VLAN or the VLAN's IP address is smaller than current V2 querier, the switch becomes the querier for the VLAN. IGMPv2 group specific query and leave packets are handled.

  When receiving an IGMPv2 leave packet, the IGMP interface issues an IGMPv2 group specific query packet immediately and waits one second to check if any IGMP reports are received on the ports. If not, the port is removed from the IGMP group member list, and the group's multicast data is not forwarded to this port until an IGMP report is received again.

The outgoing ports for the IGMPv1 Query or IGMPv2 Query packets are defined in Multicast Forwarding within a VLAN section.

If the IGMP interface is designated as the IGMP querier, the switch uses the following intervals for sending query packets:

- When you enable IGMP snooping or boot the switch with the querier option enabled, the first query packet will not be sent for 255 seconds. ***This time delay is non-standard.***
- The second query packet will be sent after the "Startup Querier Interval" which is 1/4 * "Query Interval." By default, this is 31 seconds.
- The next query packets will be sent periodically according to the "Query Interval." The default "Query Interval" is 125 seconds.

The following table gives the sequence of these packets.

Table 19. Packet Sequence

Time (seconds)	Description
0	Switch decides to be IGMP Querier for the VLAN
255	1st Query Packet
286	2nd Query Packet (255+31)
411	3rd Query Packet (286+125)
536	4th Query Packet (411+125)
661	5th Query Packet (536+125)

7.4 IGMP Snooping

IGMP Snooping is a feature that reduces the flooding of IP multicast traffic.The default behavior for handling a multicast packet is to flood the packet to all members of a VLAN. With IGMP Snooping, only the active member ports receive the data.

All groups learned by IGMP snooping are recorded in an internal group table with the VLAN ID and multicast group address used as the table's index. This table stores the active member ports for this group. This table can contain a maximum of 128 groups. If the active multicast groups exceed this limit, the new group's data will be flooded in the VLAN.

You can globally enable or disable IGMP Snooping on the switch. You can also enable or disable the snooping for a specific VLAN. You must enable IGMP globally for it to be enabled on a specific VLAN. By default, the IGMP global flag is off and per-VLAN flag is on. Thus, when you enable IGMP globally, it is enabled on all VLANs.

You can configure the switch to snoop and to keep track of IGMP groups. These two interact in the following ways:

- If the IP interface has IGMP Snooping configured for the associated VLAN, the configuration of IGMP Snooping will be overwritten by the IGMP group settings. On such VLANs, the per-VLAN flag is the only available configurable option on the IGMP Snooping screen.
- If the IGMP group settings are disabled on the interface, IGMP Snooping on the VLAN becomes configurable and the switch uses these settings for the VLAN.

Note: The switch supports a maximum of 255 VLANs and a maximum of 128 IGMP Snooping groups. If you create more than 128 VLANs with IGMP Snooping enabled, some of those VLANs will not be added to the IGMP Snooping table and the group's data will be flooded in the VLAN.

7.5 IGMP Group Settings

An IP host uses IGMP to register its IP multicast group membership with the switch. Periodically, the switch queries the multicast group to see if the group is still in use:

- If the group is still active, a single IP host responds to the query, and the group registration is maintained.
- If the group is inactive and a report is not received within the time limit for a response, the group registration is removed.

7.6 DVMRP

DVMRP is a distance-vector routing protocol designed to support the forwarding of multicast datagrams through an inter-network. DVMRP constructs source-rooted multicast delivery trees using the Reverse Path Multicasting (RPM) algorithm. Unlike RIP, DVMRP is concerned with computing the previous hops back to a source. The ZT 8101 switch supports DVMRP v3.

7.7 PIM Dense Mode (PIM-DM)

PIM Dense Mode (PIM-DM) is similar to DVMRP in that it employs the Reverse Path Multicasting (RPM) algorithm. However, there are several important differences between PIM-DM and DVMRP:

- PIM-DM relies on the presence of an existing unicast routing protocol to adapt to topology changes, but it is independent of the mechanisms of the specific unicast routing protocol. In contrast, DVMRP contains an integrated routing protocol that makes use of its own RIP-like exchanges to compute the required unicast routing information.
- Unlike DVMRP, which calculates a set of child interfaces for each (source and group) pair, PIM-DM simply forwards multicast traffic on all downstream interfaces until explicit prune messages are received. PIM-DM is willing to accept packet duplication to eliminate routing protocol dependencies and to avoid the overhead involved in building the parent/child database.

The ZT 8101 switch supports PIM-DM v2.

This page intentionally left blank.

Miscellaneous Switch Features 8

8.1 User Accounts

Two levels of user accounts are supported:

- **Admin:** The user can perform all the operations (configuring, checking status, and rebooting).
- **User**: The user can check the switch's status, view its configuration information, and ping other stations to check communication.

You can create a total of eight accounts, which can be either Admin or User level. At least one Admin-level account must exist.

8.2 General Switch Information

The following fields are embedded to the header of firmware and are displayed in the switch information screen:

- Device Type – Device's model number
- MAC Address – Start MAC address of this device (contains 32)
- Boot PROM Firmware Version, including build number
- Runtime Firmware Version, including build number
- Hardware Version
- Device Serial Number
- System Name supplied by the end user
- System Location supplied by the end user
- System Contact supplied by the end user

These fields are easy to modify for custom requirements.

8.3 Switch Diagnostics

The switch diagnostics are divided into two parts:

- System memory diagnostics: these are executed on the PROM (loader).
- Switch ASIC diagnostics: these are executed on RUNTIME and are only available for manufacturing testing.

8.3.1 System Memory Diagnostics

The PROM loader automatically runs the memory diagnostics each time the switch is booted. It is divided into two parts. The first part tests the data bus and the second part tests the address bus.

8.3.2 Switch ASIC Diagnostics

The following are included in the switch's ASIC level diagnostics.

- Direct Register Testing
- Indirect Register Testing
- Internal Buffers Testing
- ARL L3 Table Testing
- Port Based VLAN Table Testing
- 802.1Q Tagged VLAN Table Testing
- Trunk Group Table Testing
- Trunk Group Bitmap Table Testing
- Inclusive Filter Mask Table Testing
- Inclusive Filter Rules Table Testing
- Layer 2 Multicast Table Testing
- Default IP Router Table Testing
- Layer 3 Interface Table Testing
- External Buffers Testing
- Layer 3 Multicast Table Testing

8.4 History Log

The following table shows the message types and the messages that are currently supported in the history log.

Table 20. History Log Messages (Sheet 1 of 2)

Type	Log Message
Device	System started up
Device	Port 1: link up, 100 Mbps, full duplex
Device	Port 1: link down
Management	Successful log in through Telnet (Username: Edward)
Management	Console session timed out (Username: Edward)
Management	Login failed through Telnet (Username: Edward)
Management	Successful log in through Telnet (Username: Edward)
Management	Telnet session timed out (Username: Edward)

Table 20. History Log Messages (Sheet 2 of 2)

Management	Configuration saved to flash (Username: Edward)
Management	Firmware upgrade was successful (Username: Edward)
Management	Firmware upgrade was unsuccessful! (Username: Edward)
Management	Configuration download was successful (Username: Edward)
Management	Configuration download was unsuccessful! (Username: Edward)
Spanning Tree	Topology change
Spanning Tree	New root
Spanning Tree	Spanning Tree Protocol is enabled
Spanning Tree	Spanning Tree Protocol is disabled
Security	Possible spoofing attack from 00-80-C8-11-22-33 port 1

8.5 Reset Configuration to Factory Default

The switch has a menu option to reset it to factory defaults. It can also be manually reset to the factory defaults from the serial port with the following steps:

1. From the serial interface, reboot switch and wait for the following message to appear:

Please wait, loading Runtime image..... 10%

2. When the above message appears, press the # key.
3. When the “Factory Default Enable” message appears, release the # key.
4. Press the Enter key twice to log in to the system.
5. Reboot the switch with the Save Configuration and Reboot' option.
6. Wait for the switch to boot up.
7. Log in to the system with default username and password.

Note: If you skip Step 5, the default settings are not saved in flash.

8.6 Firmware Upgrade

8.6.1 Upgrade Runtime through TFTP

To upgrade the switch’s firmware, you must first complete the following tasks:

- You must obtain an updated runtime version of the firmware.
- You must copy the firmware to a known directory on a TFTP server.

Once the firmware is on the TFTP server, you can upgrade the switch from the serial, Telnet, or Web interface. Only one TFTP upgrade session is allowed at a time. When the download has completed and the firmware has been written to flash, the switch will automatically reboot and execute the new runtime firmware.

8.6.2 Upgrade Runtime through Zmodem

Generally, TFTP is the first choice to use to upgrade firmware. The Telnet Console and the Web Console both have options for upgrading the firmware using a TFTP server. However, you can also use Zmodem to upgrade the firmware from the serial port. The switch can hold only one image of the firmware.

8.6.2.1 To upgrade the firmware using Zmodem

1. Obtain the runtime firmware.
2. Using Windows HyperTerminal, log in to the switch through the serial port.
3. From the Main Menu, select Reboot and press Enter.
4. When the power on self test message appears, press the # key and wait for the following message:

```
Please change your baud rate to 115200 for the Zmodem upgrade, or
press CTRL+C to go to the BOOT Menu.

If you press CTRL-C, you can configure the baud rate to a different value.
```

5. Change HyperTerminal's baud rate to match the target's setting.
6. Use the Send File function of HyperTerminal to upgrade the firmware.

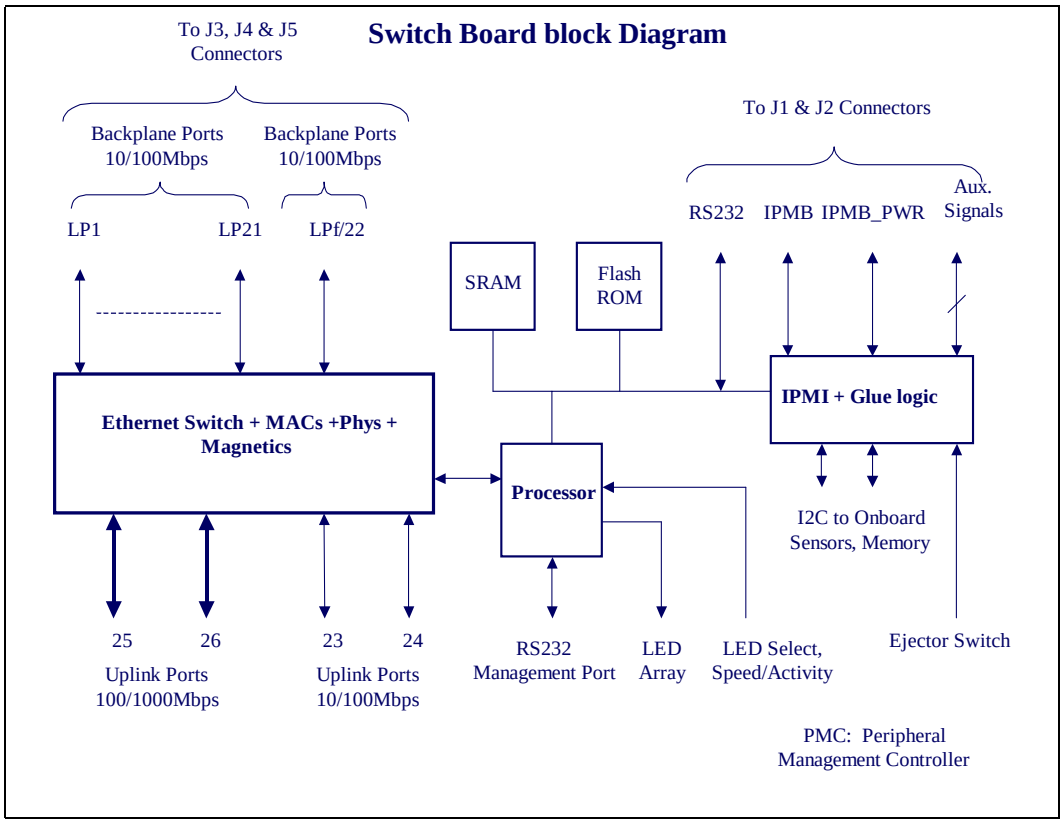
   When the download is completed, Zmodem will display a message indicating that it is done and then a message about loading the Runtime image.
7. Change the baud rate of HyperTerminal back to 9600 bps.
8. Press the Enter key twice.
9. Log in to the switch.
10. From the main menu, select Switch Information and press Enter. Verify the firmware version.

Hardware 9

9.1 Design Summary

In very general terms, the following diagram outlines the basic design of the ZT 8101 switch.

Figure 2. Switch Block Diagram



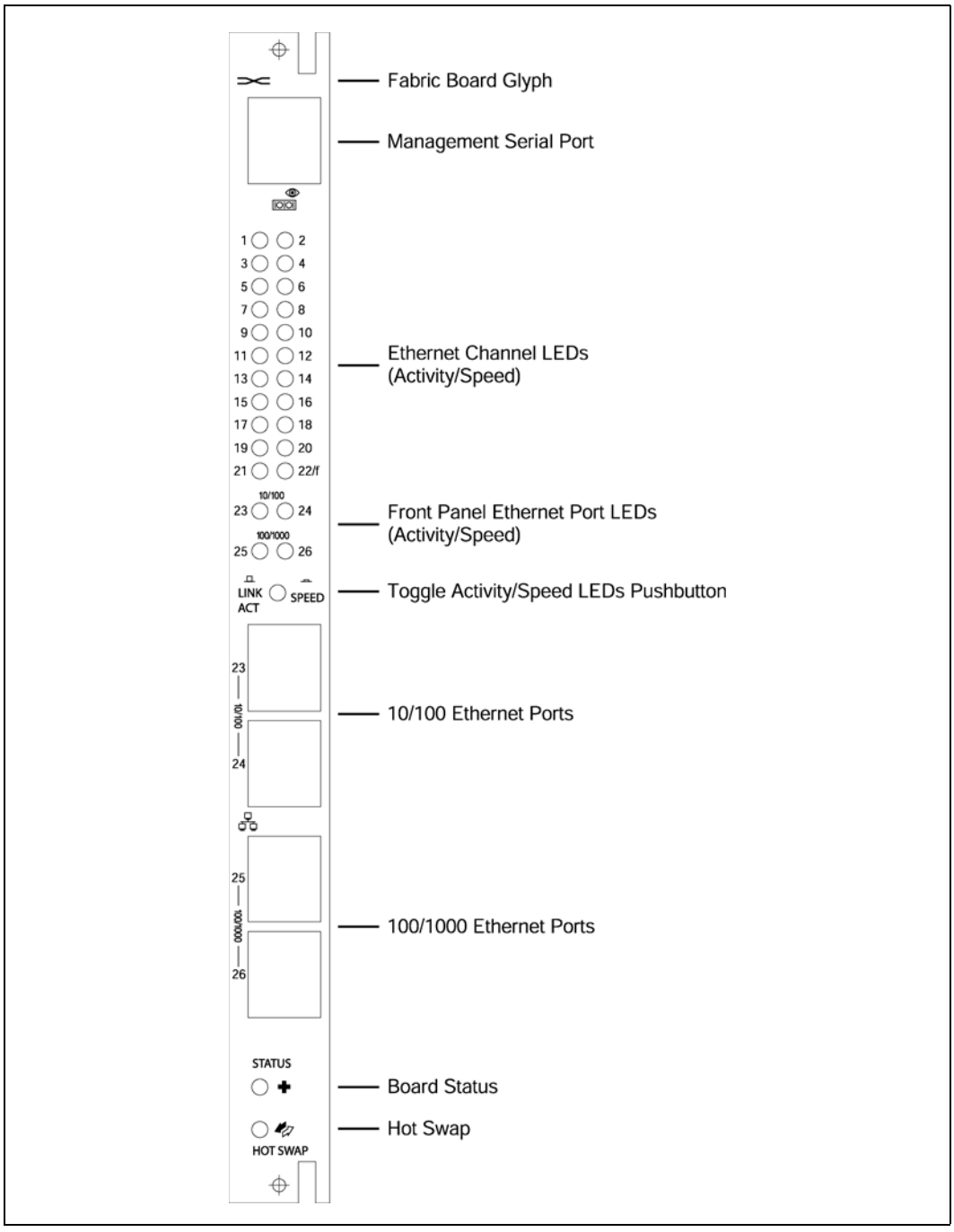
9.2 Physical Board

The ZT 8101 switch complies with the form factor of a 6U CompactPCI card, 160 mm deep. It uses the same connectors as defined by PICMG 2.0 spec for J1 – J5. The pin out is compatible with PICMG 2.16 standard for Switch Fabrics. An Extended Fabric Board J4 key shall be used to prevent the user from inserting this module into a standard node slot.

The ZT 8101 switch has Electro Static Discharge Strips on the top and bottom of the card. See PICMG Spec section 4.1.4 for a detail of the ESD Strips.

The ZT 8101 switch has the following general physical outline and connector placement.

Figure 3. Front Panel



9.3 Power

The power system supports for following feature set:

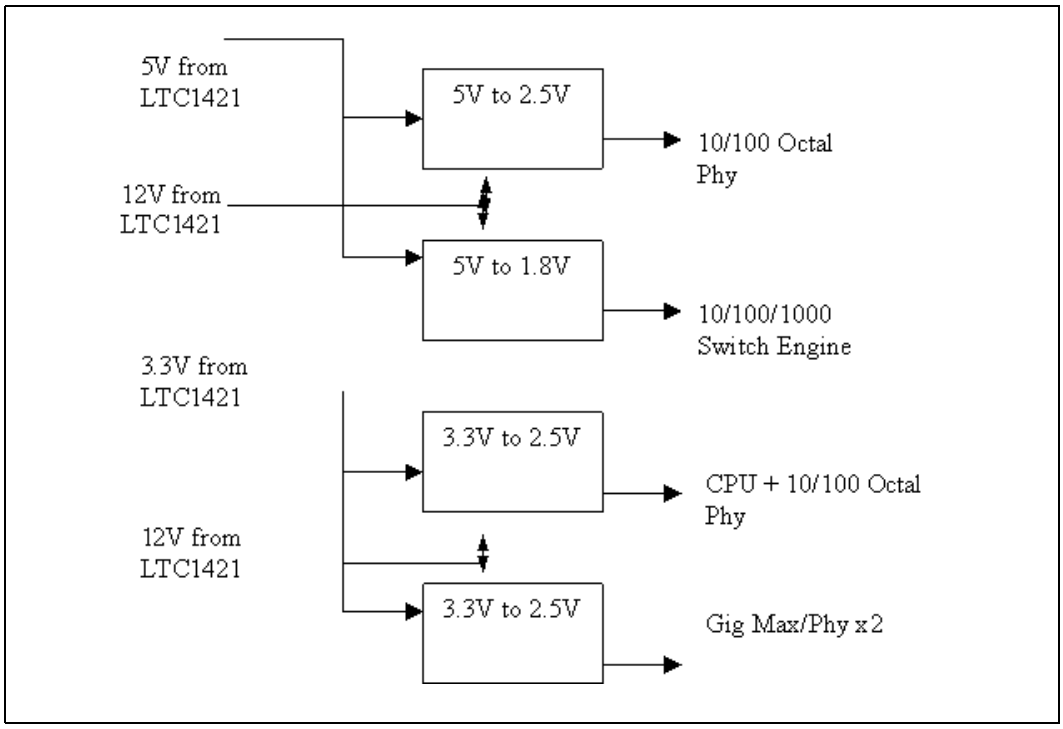
- CompactPCI Hot Swap.
- The ZT 8101 switch runs from a 3.3 V and 5 V supply. The chassis supplies this power from a dedicated reliable power source. The ZT 8101 switch consumes no more than 35 W total.
- The ZT 8101 switch has the following power needs.

Table 21. Voltage and Current Needs

Voltage	Max current	Where used
12 V	20 mA	Regulator control, LTC1421.
5 V	3.1 A	LTC1421, 5 V-to-2.5 V switching circuit input (1.784 A), 5 V-to-1.8 V switching circuit input (2.778 A).
3.3 V	5.038 A	TX3927, PHY, switch engine, regulators to generate 2.5 V.
2.5 V	2.676 A	CPU, PHY, switch engine.

The following diagram outlines the major power systems of the ZT 8101 switch.

Figure 4. Power Systems



9.4 CompactPCI

The ZT 8101 switch complies with PICMG 2.1 Hot Swap specification for insertion and removal of the ZT 8101 board.

The ZT 8101 slot in the chassis will have the BD_SEL# pin grounded. When the ZT 8101 switch is inserted, the hot swap power controller will wait until BD_SEL# is grounded and backplane power has stabilized before ramping up main power to ZT 8101. If backplane power becomes unstable or BD_SEL# goes high, the hot swap power controller will turn off main power to the ZT 8101 switch.

A CPLD is used to control the hot swap LED, and reset to the board. See the Hot Swap section for details on the hot swap logic.

The blue LED will be on at any time it is safe to remove the ZT 8101 switch.

9.5 Power Controller

The hot swap power controller chip is used to ramp voltages and watch for over current. If over current is detected, main power to the ZT 8101 switch will be terminated. Over current is defined as 50 percent over spec.

A time constant of 100uS is used on startup to prevent any surges.

The ZT 8101 switch has a Hot Swap Shield on the back of the board to protect the circuits.

The hot swap power controller chip is a LTC1421 chip.

9.6 Regulators

The ZT 8101 switch generates the on board voltages from both 3.3 V and 5 V.

A switching regulator generates 2.5 V (for two Octal Phy) and 1.8 V (switch engine) from the 5 V. Several LDO regulators generate the 2.5 V needed for the CPU core, 10/100/1000 and Octal Phy.

The switching regulator is a RT-9226B. The 2.5 V LDO regulator is a CS-5253.

9.7 Embedded Controller

The ZT 8101 switch uses the TX-3927 RISC CPU.

9.8 Ethernet

The ZT 8101 switch utilizes a single chip Ethernet switch controller solution that has 24 10/100 ports and 2 GbE ports.

9.9 Local I2C Bus and GPIO

The I2C bus on the ZT 8101 switch for GPIO and system management monitoring uses the following device and address.

Table 22. IO Devices and Addresses

Chip	Device	Address	Description
ATC24C02	24C02	001b	24C02 for storing hardware dependent information

The SCL and DTA signals are tied high to 3.3 V with 1 K ohm resistors.

9.10 GPIO

The following table describes all the GPIO of the TX3927 CPU on the ZT 8101 switch.

Table 23. GPIO Assignments

Label Name	I/O	Chip	Pin	Description
SDA_BRD	I/O	TX3927	127	Local I2C Bus
SCLK_BRD	O	TX3927	128	Local I2C Bus

9.11 Rear Panel Connector

The ZT 8101 rear panel uses the same connectors as a CompactPCI 6U Module. The following tables outline the pins used in J1 through J5. J1 is keyed as code number 3456.

J4 is keyed as code number 1235.

Table 24. J1 Pin Out (Sheet 1 of 2)

	Z	A	B	C	D	E	F
25	GND	EARLY_5V	PreCharge	ENUM#	EARLY_3.3V	EARLY_5V	GND
24	GND	PreCharge	EARLY_5V	-NC-	PreCharge	PreCharge	GND
23	GND	EARLY_3.3V	PreCharge	PreCharge	EARLY_5V	PreCharge	GND
22	GND	PreCharge	GND	EARLY_3.3V	PreCharge	-NC-	GND
21	GND	EARLY_3.3V	PreCharge	PreCharge	-NC-	PreCharge	GND
20	GND	PreCharge	GND	-NC-	PreCharge	PreCharge	GND
19	GND	EARLY_3.3V	PreCharge	PreCharge	GND	PreCharge	GND
18	GND	PreCharge	-NC-	EARLY_3.3V	PreCharge	-NC-	GND
17	GND	EARLY_3.3V	IPMB_SCL	IPMB_SDA	GND	PreCharge	GND

Table 24. J1 Pin Out (Sheet 2 of 2)

	Z	A	B	C	D	E	F
16	GND	PreCharge	GND	-NC-	PreCharge	-NC-	GND
15	GND	EARLY_3.3V	PreCharge	PreCharge	-NC-	PreCharge	GND
12-14							
11	GND	PreCharge	PreCharge	PreCharge	GND	PreCharge	GND
10	GND	PreCharge	GND	EARLY_3.3V	PreCharge	PreCharge	GND
9	GND	PreCharge	PreCharge	PreCharge	GND	PreCharge	GND
8	GND	PreCharge	GND	-NC-	PreCharge	PreCharge	GND
7	GND	PreCharge	PreCharge	PreCharge	GND	PreCharge	GND
6	GND	PreCharge	-NC-	EARLY_3.3V	-NC-	PreCharge	GND
5	GND	-NC-	-NC-	PreCharge	GND	PreCharge	GND
4	GND	IPMB_PWR	HEALTHY#	-NC-	-NC-	-NC-	GND
3	GND	PreCharge	PreCharge	PreCharge	EARLY_5V	PreCharge	GND
2	GND	-NC-	EARLY_5V	-NC-	-NC-	-NC-	GND
1	GND	EARLY_5V	-NC-	-NC-	EARLY_12V	EARLY_5V	GND

Table 25. Backplane Pin Descriptions

Name	Count	Type	Description
EARLY_5V	8	Power	Early 5 V and 5 V power supply pins
EARLY_3.3V	10	Power	Early 3.3 V and 3.3 V power supply pins
IPMB_PWR	1	Power	IPMB power supply pin
HEALTHY#	1	Output	Healthy status
IPMB_SCL	1	Output	IPMB Clock
IPMB_SDA	1	I/O	IPMB Address/Data
ENUM#	1	O	To indicate the switch blade is freshly inserted
EARLY_12V	1	Power	Early 12 V power supply pin
GND	76	Power	GND pins. There are more GND pins at J3~J5.
-NC-			No connected pins.
TOTAL	220		

Table 26. J2 Pin Out

	A	B	C	D	E	F
22	GA4	GA3	GA2	GA1	GA0	GND
21	-NC-	GND	-NC-	-NC-	-NC-	GND
20	-NC-	-NC-	-NC-	GND	-NC-	GND
19	-NC-	GND	-NC-	-NC-	-NC-	GND
18	-NC-	-NC-	-NC-	GND	-NC-	GND
17	-NC-	GND	-NC-	-NC-	-NC-	GND
16	-NC-	-NC-	-NC-	GND	-NC-	GND
15	-NC-	GND	-NC-	-NC-	-NC-	GND
14	PreCharge	PreCharge	PreCharge	GND	PreCharge	GND
13	PreCharge	GND	-NC-	PreCharge	PreCharge	GND
12	PreCharge	PreCharge	PreCharge	GND	PreCharge	GND
11	PreCharge	GND	-NC-	PreCharge	PreCharge	GND
10	PreCharge	PreCharge	PreCharge	GND	PreCharge	GND
9	PreCharge	GND	-NC-	PreCharge	PreCharge	GND
8	PreCharge	PreCharge	PreCharge	GND	PreCharge	GND
7	PreCharge	GND	-NC-	PreCharge	PreCharge	GND
6	PreCharge	PreCharge	PreCharge	GND	PreCharge	GND
5	PreCharge	GND	-NC-	PreCharge	PreCharge	GND
4	-NC-	-NC-	PreCharge	GND	PreCharge	GND
3	-NC-	GND	-NC-	-NC-	-NC-	GND
2	-NC-	-NC-	-NC-	-NC-	-NC-	GND
1	-NC-	GND	-NC-	-NC-	-NC-	GND

Table 27. J3 Pin Out

	A	B	C	D	E	F
19	SGA4	SGA3	SGA2	SGA1	SGA0	GND
18	TX+22	TX-22	GND	-NC-	-NC-	GND
17	RX+22	RX-22	GND	-NC-	-NC-	GND
16	TX+8	TX-8	GND	-NC-	-NC-	GND
15	RX+8	RX-8	GND	-NC-	-NC-	GND
14	TX+7	TX-7	GND	-NC-	-NC-	GND
13	RX+7	RX-7	GND	-NC-	-NC-	GND
12	TX+6	TX-6	GND	-NC-	-NC-	GND
11	RX+6	RX-6	GND	-NC-	-NC-	GND
10	TX+5	TX-5	GND	-NC-	-NC-	GND
9	RX+5	RX-5	GND	-NC-	-NC-	GND
8	TX+4	TX-4	GND	-NC-	-NC-	GND
7	RX+4	RX-4	GND	-NC-	-NC-	GND
6	TX+3	TX-3	GND	-NC-	-NC-	GND
5	RX+3	RX-3	GND	-NC-	-NC-	GND
4	TX+2	TX-2	GND	-NC-	-NC-	GND
3	RX+2	RX-2	GND	-NC-	-NC-	GND
2	TX+1	TX-1	GND	-NC-	-NC-	GND
1	RX+1	RX-1	GND	-NC-	-NC-	GND

Table 28. J4 Pin Out

	A	B	C	D	E	F
25	TX+20	TX-20	GND	-NC-	-NC-	GND
24	RX+20	RX-20	GND	-NC-	-NC-	GND
23	TX+21	TX-21	GND	-NC-	-NC-	GND
22	RX+21	RX-21	GND	-NC-	-NC-	GND
21	-NC-	-NC-	GND	-NC-	-NC-	GND
20	-NC-	-NC-	GND	-NC-	-NC-	GND
19	-NC-	-NC-	GND	-NC-	-NC-	GND
18	-NC-	-NC-	GND	-NC-	-NC-	GND
17	-NC-	-NC-	GND	-NC-	-NC-	GND
16	-NC-	-NC-	GND	-NC-	-NC-	GND
15	-NC-	-NC-	GND	-NC-	-NC-	GND
14	-NC-	-NC-	-NC-	-NC-	-NC-	GND
13	-NC-	-NC-	-NC-	-NC-	-NC-	GND
12	-NC-	-NC-	-NC-	-NC-	-NC-	GND
11	5V	5V	GND	3.3V	3.3V	GND
10	RTS_BP	CTS_BP	TXD_BP	RXD_BP	SMBD	GND
9	DTR_BP	DSR_BP	IPMB_PWR	SMBA	SMBC	GND
8	-NC-	-NC-	-NC-	-NC-	-NC-	GND
7	-NC-	-NC-	-NC-	-NC-	-NC-	GND
6	-NC-	-NC-	-NC-	-NC-	-NC-	GND
5	-NC-	-NC-	-NC-	-NC-	-NC-	GND
4	-NC-	-NC-	-NC-	-NC-	-NC-	GND
3	-NC-	-NC-	-NC-	-NC-	-NC-	GND
2	-NC-	-NC-	-NC-	-NC-	-NC-	GND
1	-NC-	-NC-	-NC-	-NC-	-NC-	GND

Table 29. J5 Pin Out

	A	B	C	D	E	F
22	TX+19	TX-19	GND	-NC-	-NC-	GND
21	RX+19	RX-19	GND	-NC-	-NC-	GND
20	TX+18	TX-18	GND	-NC-	-NC-	GND
19	RX+18	RX-18	GND	-NC-	-NC-	GND
18	TX+17	TX-17	GND	-NC-	-NC-	GND
17	RX+17	RX-17	GND	-NC-	-NC-	GND
16	TX+16	TX-16	GND	-NC-	-NC-	GND
15	RX+16	RX-16	GND	-NC-	-NC-	GND
14	TX+15	TX-15	GND	-NC-	-NC-	GND
13	RX+15	RX-15	GND	-NC-	-NC-	GND
12	TX+14	TX-14	GND	-NC-	-NC-	GND
11	RX+14	RX-14	GND	-NC-	-NC-	GND
10	TX+13	TX-13	GND	-NC-	-NC-	GND
9	RX+13	RX-13	GND	-NC-	-NC-	GND
8	TX+12	TX-12	GND	-NC-	-NC-	GND
7	RX+12	RX-12	GND	-NC-	-NC-	GND
6	TX+11	TX-11	GND	-NC-	-NC-	GND
5	RX+11	RX-11	GND	-NC-	-NC-	GND
4	TX+10	TX-10	GND	-NC-	-NC-	GND
3	RX+10	RX-10	GND	-NC-	-NC-	GND
2	TX+9	TX-9	GND	-NC-	-NC-	GND
1	RX+9	RX-9	GND	-NC-	-NC-	GND

9.12 Watchdog

The switch uses a TX3927 internal watchdog timer and one external watchdog timer inside CPLD.

9.13 Clocks

There are four clock sources:

- 25 MHz for GbE PHY chips
- 125 MHz for switch controller core frequency, Octal PHY SMII clock and GbE PHY GMII clock
- 100 MHz for SDRAM clock
- 8.33 MHz for TX3927.

All of them are generated from oscillator.

9.14 Front Panel

The front panel of the ZT 8101 switch has the following items.

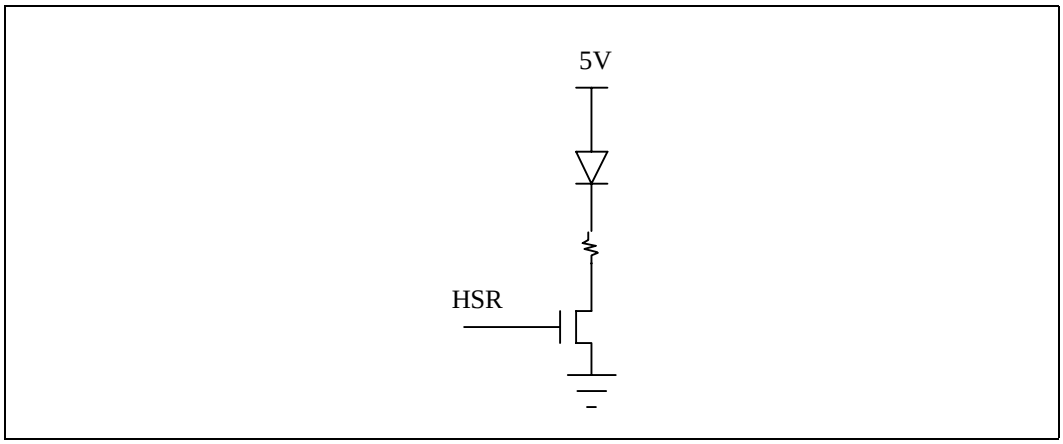
Table 30. Front Panel Items

Item	Description
Ejector switch	This switch tells the hot swap controller if the user wants to remove the card. While this switch is closed, the card cannot physically be removed.
Hot Swap LED	This blue LED tells the user it is safe to remove the ZT 8101 switch. If this LED is **not on,** damage to the chassis, the ZT 8101 switch, or modules in the chassis could result by removing the ZT 8101 switch.
RJ-45 Ports	There are 4 RJ-45 ports. Two of them are for 10BASE-T/100BASE-TX Ethernet ports and two of them are for 100BASE-TX/1000BASE-T Ethernet ports.
Board Status LED	The status LED shows the health of the board and its power state.
Management Serial Port	The serial port allows the user to attach a terminal or a PC running terminal emulation software (such as HyperTerminal) and manage the switch.
Ethernet Channel LEDs	These LEDs indicate either the activity or the speed of the ports.

9.15 Hot Swap

The blue hot swap LED has controlled ejector switch logic, which is powered by early power and the CPLD. A 3.3 V high signal from the CPLD means to turn on the LED. Since a blue LED requires a large forward voltage, it uses the following circuit to drive the blue LED.

Figure 5. Hot Swap LED



A PIO pin is used to indicate that the ejector latch of the switch has been opened. When the user opens the ejector latch of the switch, the PIO pin is pulled low to inform the CPU that hot swap is in progress. When the switch's polling task notices this event, it forces each port into link down mode and then lights a LED to indicate that it is safe to unplug the switch.

9.16 Board Status LED

Table 31. Board Status LED

Status	Meaning
Off	Not powered.
Green	Powered.
Amber	Powered and attention needed. Possible conditions include: • Over temperature • Exceeding voltage limits • IPMB time outs

9.17 Ethernet Channel LEDs

The LED array on the front panel displays information about all the Ethernet links on the board. A green/amber two-color LED is used for each of the 26 Ethernet port connections (24 10/100 + 2 Gigabit). A push button switch just below the array toggles the LED display from Link /Activity mode to Link / Speed mode. The default LED mode is Link /Activity. When the switch button is depressed, the LEDs are in Link/Speed mode.

9.17.1 Link/Activity LED Mode

Table 32. LED Descriptions

Status	Meaning
Off	No Ethernet connection
Solid Green	Good connection, link present
Blinking Green	Port is transmitting or receiving packets (activity is on going)
Solid Amber	Port is not forwarding packets. Management has disabled the port, an address violation has occurred, or STP is blocking the port.

Note: After a port is reconfigured, the port LED can remain amber for up to 30 seconds while STP checks the switch for loop paths.

9.17.2 Link/Speed LED Mode

Table 33. Link/Speed LED Mode

Port Type	Status	Meaning
10/100	Off	10 Mbps
	Solid Green	100 Mbps
100/1000	Solid Green	100 Mbps
	Solid Amber	1000 Mbps

This page intentionally left blank.

Reliability and Serviceability 10

The MTBF of the ZT 8101 is 104,000 hours.

This page intentionally left blank.

ASIC Tables 11

11.1 Fast Filter Processor

The ZT 8101 supports an extensive filtering mechanism and packet classification, which enables a switch application to filter and classify based on certain protocol fields in the packet. You can also filter on specified ingress or egress ports.

Filtering uses two constructs:

- The filter mask defines which fields to filter.
- The rule table defines the filtering options.

11.2 MARL Table

The MARL table is used to limit the flooding domain for a specific multicast MAC address. The table size is 256, but one entry is reserved by ASIC. Both IGMP snooping and GMRP use this table.

Table 34. MARL Table

Functionality	Size
IGMP Snooping	128
Static GMRP Group	32
Dynamic GMRP Group	64
Software Reserved	31
ASIC Reserved	1

This page intentionally left blank.

IEEE Standards and Protocol Compliance A

Table 35. IEEE Standards Support

Feature	Description	Supported
IEEE 802.1D	Bridge specification incorporating Traffic Class Expediting and Dynamic Multicast Filtering	Yes
IEEE 802.1P	Priority queues for QOS	Yes
IEEE 802.3	10Mbps	Yes
IEEE 802.3u	100 Mbps Ethernet	Yes
IEEE 802.3ab	1 GbE on Category 5 UTP cable	Yes
IEEE 802.3ac	Frame Extensions for VLAN tagging on Ethernet	Yes
IEEE 802.3x	Full-duplex Operation/Flow Control on Ethernet	Yes
IEEE 802.3ad	Link Aggregation	Yes
IEEE 802.1Q	VLAN Specification	Yes
RFC 768	Unreliable Data gram Protocol (UDP)	Yes
RFC 783	Trivial File Transfer Protocol (TFTP)	Yes
RFC 791 / 950	Internet Protocol (IP)	Yes
RFC 792	Internet Control Message Protocol (ICMP)	Yes
RFC 826	Address Resolution Protocol (ARP)	Yes
RFC 854 RFC 855 RFC 856 RFC 857	Telnet Telnet Options specification Telnet Binary transmission Telnet Echo option	Yes
RFC 1058	Routing Information Protocol (RIP)	Yes
RFC 1519	Classless Inter-domain Routing (CIDR)	Yes
RFC 1542	BOOTP	Yes
RFC 1723	Routing Information Protocol (RIP) version 2	Yes
RFC 2068	Hyper Text Transfer Protocol (HTTP)	Yes
RFC 2113	IP Router Alerts	No
RFC 2328	Open Shortest Path First (OSPF v2)	No
RFC 2131	BOOTP/DHCP Relay	Yes
RFC 2236	Internet Group Management Protocol (IGMP) version 2	Yes
draft-ietf-idmr-dvmrp-v3-10	DVMRPv3	Yes
draft-ietf-idmr-PIM-DM-spec-01	PIMv2	Yes

This page intentionally left blank.

PICMG Compliance B

Table 36. PICMG Compliance

Number	Feature	Description	Supported
3.13.1	PICMG 2.0 R3.0	CompactPCI Core Specifications	Yes
3.13.2	PICMG 2.11	CompactPCI Power Interface Specifications	Yes
3.13.3	PICMG 2.10	CompactPCI Keying Specifications	Yes
3.13.4	PICMG 2.9	System Management Specifications	Yes
3.13.5	PICMG 2.1	Hot Swap Specifications	Yes
3.13.6	PICMG 2.16	Packet Switching Back plane	Yes

This page intentionally left blank.

Warranty Information C

C.1 Intel® NetStructure™ Compute Boards & Platform Products Limited Warranty

Intel warrants to the original owner that the product delivered in this package will be free from defects in material and workmanship for two (2) year(s) following the latter of: (i) the date of purchase only if you register by returning the registration card as indicated thereon with proof of purchase; or (ii) the date of manufacture; or (iii) the registration date if by electronic means provided such registration occurs within 30 days from purchase. This warranty does not cover the product if it is damaged in the process of being installed. Intel recommends that you have the company from whom you purchased this product install the product.

THE ABOVE WARRANTY IS IN LIEU OF ANY OTHER WARRANTY, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, ANY WARRANTY OF INFRINGEMENT OF ANY OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS, OR ANY WARRANTY ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE.

This warranty does not cover replacement of products damaged by abuse, accident, misuse, neglect, alteration, repair, disaster, improper installation or improper testing. If the product is found to be otherwise defective, Intel, at its option, will replace or repair the product at no charge except as set forth below, provided that you deliver the product along with a return material authorization (RMA) number (see below) either to the company from whom you purchased it or to Intel. If you ship the product, you must assume the risk of damage or loss in transit. You must use the original container (or the equivalent) and pay the shipping charge. Intel may replace or repair the product with either a new or reconditioned product, and the returned product becomes Intel's property. Intel warrants the repaired or replaced product to be free from defects in material and workmanship for a period of the greater of: (i) ninety (90) days from the return shipping date; or (ii) the period of time remaining on the original two (2) year warranty.

This warranty gives you specific legal rights and you may have other rights which vary from state to state. All parts or components contained in this product are covered by Intel's limited warranty for this product. The product may contain fully tested, recycled parts, warranted as if new.

C.1.1 Returning a Defective Product (RMA)

Before returning any product, contact an Intel Customer Support Group to obtain either a Direct

Return Authorization (DRA) or Return Material Authorization (RMA). Return Material

Authorizations are only available for products purchased within 30 days.

Return contact information by geography:

C.1.2 For the Americas

Return Material Authorization (RMA) credit requests e-mail address: requests.rma@intel.com

Direct Return Authorization (DRA) repair requests e-mail address: uspss.repair@intel.com

DRA on-line form: http://support.intel.com/support/motherboards/draform.htm

Intel Business Link (IBL): http://www.intel.com/ibl

Telephone No.: 1-800-INTEL4U or 480-554-4904

Office Hours: Monday - Friday 0700-1700 MST Winter / PST Summer

C.1.3 For EMEA

Return Material Authorization (RMA) e-mail address - emea.fs@intel.com

Direct Return Authorization (DRA) for repair requests e-mail address: emea.fs@intel.com

Intel Business Link (IBL): http://www.intel.com/ibl

Telephone No.: 00 44 1793 403063

Fax No.: 00 44 1793 403109

Office Hours: Monday - Friday 0900-1700 UK time

C.1.4 For APAC

RMA/DRA requests email address: apac.rma.front-end@intel.com

Telephone No.: 604-859-3111 or 604-859-3325

Fax No.: 604-859-3324

Office Hours: Monday - Friday 0800-1700 Malaysia time

Return Material Authorization (RMA) requests e-mail address: rma.center.jpss@intel.com

Telephone No.: 81-298-47-0993 or 81-298-47-5417

Fax No.: 81-298-47-4264

Direct Return Authorization (DRA) for repair requests, contact the JPSS Repair center.

E-mail address: sugiyamakx@intel.co.jp

Telephone No.: 81-298-47-8920

Fax No.: 81-298-47-5468

Office Hours: Monday - Friday 0830-1730 Japan time

If the Customer Support Group verifies that the product is defective, they will have the Direct Return Authorization/Return Material Authorization Department issue you a DRA/RMA number to place on the outer package of the product. Intel cannot accept any product without a DRA/RMA number on the package. Limitation of Liability and Remedies

INTEL SHALL HAVE NO LIABILITY FOR ANY INDIRECT OR SPECULATIVE DAMAGES (INCLUDING , WITHOUT LIMITING THE FOREGOING, CONSEQUENTIAL, INCIDENTAL AND SPECIAL DAMAGES) ARISING FROM THE USE OF OR INABILITY TO USE THIS PRODUCT, WHETHER ARISING OUT OF CONTRACT, NEGLIGENCE, TORT, OR UNDER ANY WARRANTY, OR FOR INFRINGEMENT OF ANY OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS, IRRESPECTIVE OF WHETHER INTEL HAS ADVANCE NOTICE OF THE POSSIBILITY OF ANY SUCH DAMAGES, INCLUDING, BUT NOT LIMITED TO LOSS OF USE, BUSINESS INTERRUPTIONS, AND LOSS OF PROFITS. NOTWITHSTANDING THE FOREGOING, INTEL'S TOTAL LIABILITY FOR ALL CLAIMS UNDER THIS AGREEMENT SHALL NOT EXCEED THE PRICE PAID FOR THE PRODUCT. THESE LIMITATIONS ON POTENTIAL LIABILITIES WERE AN ESSENTIAL ELEMENT IN SETTING THE PRODUCT PRICE. INTEL NEITHER ASSUMES NOR AUTHORIZES ANYONE TO ASSUME FOR IT ANY OTHER LIABILITIES.

Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitations or exclusions may not apply to you.

This page intentionally left blank.

Customer Support D

This appendix offers technical and sales assistance information for this product, and information on returning an Intel NetStructure product for service.

D.1 Technical Support and Return for Service Assistance

For all product returns and support issues, please contact your Intel product distributor or Intel Sales Representative for specific information.

D.2 Sales Assistance

If you have a sales question, please contact your local Intel® NetStructure™ Sales Representative or the Regional Sales Office for your area. Address, telephone and FAX numbers, and additional information is available at Intel's website, located at:

http://www.intel.com/network/csp/sales/

Intel Corporation
Telephone (in U.S.) 1-800-755-4444
Telephone (Outside U.S.) 1-973-993-3030

This page intentionally left blank.

Specifications E

CompactPCI Specification, PICMG 2.16

Less than 35W power consumption

E.1 Power Requirements

Supply Voltage	Vcc	+5 VDC +5%, -3%
Supply Current	Vcc=5.0 VDC	4 A
Supply Voltage	V3.3 V	+3.3 VDC +5%, -3%
Supply Current	V3.3 V=3.3 VDC	6 A
Supply Voltage	V12.0 V	+12 VDC 10%
Supply Current	V12 V=12.0 V	20 mA

E.2 Mechanical

Measures 9.2 x 6.3 (233.35 mm x 160 mm)

Connector: IEC-1076-4-101 (J1-J5)

Width: 0.8 (1 slot - 4HP)

E.3 Environmental

Operating Temperature (requires 200 LFM airflow): 0 to 50^{o} C

Storage Temperature: -25^{o} to +55^{o} C

Non-Condensing Relative Humidity: less than 95^{o} percent at 40^{o} C

E.4 Certifications

- FCC CFR47 Part 15 Class A
- UL/cUL UL1950 3rd edition/CSA C22.2 No. 950-95
- CE Mark
  - — EN55022 Class A
  - — EN55024
  - — EN60950: 1992

- CB report and certificate - IEC 60950 2nd edition
- GR-1089-CORE sections 2, 3

E.5 North America (English Required) (FCC Class A)

FCC Verification Notice

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, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For questions related to the EMC performance of this product, contact:

Intel Corporation
5200 N.E. Elam Young Parkway
Hillsboro, OR 97124
1-800-628-8686

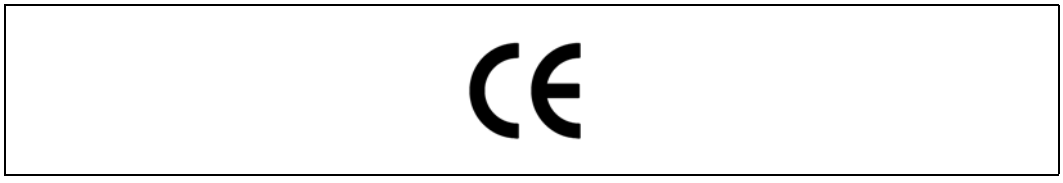
This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates,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

E.6 Canada – Industry Canada (ICES-003 Class A) (English and French-translated below)

CANADA – INDUSTRY CANADA

Cet appareil numérique respecte les limites bruits radioélectriques applicables aux appareils numériques de Classe A prescrites dans la norme sur le matériel brouilleur: “Appareils Numériques”, NMB-003 édictée par le Ministre Canadian des Communications.

(English translation of the notice above) This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the interference-causing equipment standard entitled “Digital Apparatus,” ICES-003 of the Canadian Department of Communications.



Safety Warnings F

Review the following precautions to avoid personal injury and prevent damage to this product or products to which it is connected. To avoid potential hazards, use the product only as specified.

Read all safety information provided in the component product user manuals and understand the precautions associated with safety symbols, written warnings, and cautions before accessing parts or locations within the unit. Save this document for future reference.

Caution: System environmental requirements: Components such as Processor Boards, Ethernet Switches, etc., are designed to operate with external airflow. Components can be destroyed if they are operated without external airflow. External airflow is normally provided by chassis fans when components are installed in compatible chassis. Never restrict the airflow through the unit's fan or vents. Filler panels or air management boards must be installed in unused chassis slots. Environmental specifications for specific products may differ. Refer to product user manuals for airflow requirements and other environmental specifications.

Warning: Device heatsinks may be hot during normal operation: To avoid burns, do not allow anything to touch heatsinks.

Warning: Avoid injury, fire hazard, or explosion: Do not operate this product in an explosive atmosphere.

Caution: Lithium batteries are not field-replaceable units. There is a danger of explosion if a battery is incorrectly replaced or handled. Do not disassemble or recharge the battery. Do not dispose of the battery in fire. When the battery is replaced, the same type or an equivalent type recommended by the manufacturer must be used. Used batteries must be disposed of according to the manufacturer's instructions. Return the unit to Intel for battery service.

Warning: Avoid injury: This product may contain one or more laser devices that are visually accessible depending on the plug-in modules installed. Products equipped with a laser device must comply with International Electrotechnical Commission (IEC) 60825.

F.1 Mesures de sÉcuritÉ

Veuillez suivre les mesures de sécurité suivantes pour éviter tout accident corporel et ne pas endommager ce produit ou tout autre produit lui étant connecté. Pour éviter tout danger, veillez à utiliser le produit conformément aux spécifications mentionnées.

Lisez toutes les informations de sécurité fournies dans les manuels de l'utilisateur des produits composants et veillez à bien comprendre les mesures associées aux symboles de sécurité, aux avertissements écrits et aux mises en garde avant d'accéder à certains éléments ou emplacements de l'unité. Conservez ce document comme outil de référence.

Attention : exigences environnementales du système : les composants tels que les cartes de processeurs, les commutateurs Ethernet, etc., sont conçus pour fonctionner avec un flux d'air externe. Les composants peuvent être détruits s'ils fonctionnent dans d'autres conditions. Le flux d'air externe est généralement produit par les ventilateurs des châssis lorsque les composants sont installés dans des châssis compatibles. Veillez à ne jamais obstruer le flux d'air alimentant le ventilateur ou les conduits de l'unité. Des boucliers ou des panneaux de gestion de l'air doivent être installés dans les connecteurs inutilisés du châssis. Les spécifications environnementales peuvent varier d'un produit à un autre. Veuillez-vous reporter au manuel de l'utilisateur pour déterminer les exigences en matière de flux d'air et d'autres spécifications environnementales.

Avertissement : les dissipateurs de chaleur de l'appareil peuvent être chauds lors d'un fonctionnement normal. Pour éviter tout risque de brûlure, veillez à ce que rien n'entre en contact avec les dissipateurs de chaleur.

Avertissement : évitez les blessures, les incendies ou les explosions. N'utilisez pas ce produit dans une atmosphère présentant des risques d'explosion.

Attention : les batteries au lithium ne peuvent pas être remplacées sur place. Celles-ci peuvent exploser si elles sont incorrectement remplacées ou manipulées. Veillez à ne pas désassembler ni à recharger la batterie. Veillez à ne pas jeter la batterie au feu. Lors du remplacement de la batterie, utilisez le même type de batterie ou un type équivalent recommandé par le fabricant. Les batteries usagées doivent être mises au rebut conformément aux instructions du fabricant. Renvoyez l'unité à Intel pour toute réparation de la batterie.

Avertissement : évitez les blessures. Ce produit peut contenir un ou plusieurs périphériques laser visuellement accessibles en fonction des modules plug-in installés. Les produits équipés d'un périphérique laser doivent être conformes à la norme IEC (International Electrotechnical Commission) 60825.

F.2 SICHERHEITSHINWEISE

Lesen Sie bitte die folgenden Sicherheitshinweise, um Verletzungen und Beschädigungen dieses Produkts oder der angeschlossenen Produkte zu verhindern. Verwenden Sie das Produkt nur gemäß den Anweisungen, um mögliche Gefahren zu vermeiden.

Lesen Sie alle Sicherheitsinformationen in den Benutzerhandbüchern der zu dem Produkt gehörenden Komponenten und machen Sie sich mit den Hinweisen zu den Sicherheitssymbolen, schriftlichen Warnungen und Vorsichtsmaßnahmen vertraut, ehe Sie Teile oder Stellen des Geräts anfassen. Bewahren Sie dieses Dokument gut auf, um später darin nachlesen zu können.

Vorsicht: Anforderungen an die Systemumgebung: Komponenten wie Prozessor-Boards, Ethernet-Schalter usw. sind auf den Betrieb mit externer Luftzufuhr ausgelegt. Diese Komponenten können bei Betrieb ohne externe Luftzufuhr beschädigt werden. Wenn die Komponenten in einem kompatiblen Gehäuse installiert sind, wird Luft von außen normalerweise durch Gehäuselüfter zugeführt. Blockieren Sie niemals die Luftzufuhr der Gerätelüfter oder -ventilatoren. In ungenutzten Gehäusesteckplätzen müssen Füllelemente oder Luftsteuerungseinheiten eingesetzt werden. Die Betriebsbedingungen können zwischen den verschiedenen Produkten variieren. Für die Anforderungen an die Belüftung und andere Betriebsbedingungen siehe die Benutzerhandbücher der jeweiligen Produkte.

Warnung: Die Kühlkörper des Geräts können sich während des normalen Betriebs erhitzen: Um Verbrennungen zu vermeiden, sollte jeder Kontakt mit den Kühlkörpern vermieden werden.

Warnung: Vermeiden Sie Verletzungen, Feuergefahr oder Explosionen: Unterlassen Sie den Betrieb dieses Produkts in einer explosionsgefährdeten Betriebsumgebung.

Vorsicht: Lithiumbatterien sind keine austauschbaren Funktionseinheiten. Bei unsachgemäßem Austausch oder Umgang mit Batterien besteht Explosionsgefahr. Zerlegen Sie die Batterie nicht und laden Sie diese nicht wieder auf. Entsorgen Sie die Batterie nicht durch Verbrennen. Beim Auswechseln der Batterie muss dasselbe oder ein der Händlerempfehlung gleichwertiges Modell verwendet werden. Gebrauchte Batterien müssen entsprechend den Anweisungen des Herstellers entsorgt werden. Bringen Sie das Gerät bitte zur Batteriewartung zu Intel zurück.

Warnung: Vermeiden Sie Verletzungen: Dieses Produkt kann ein oder mehrere Lasergeräte enthalten, die abhängig von den installierten Plug-In-Modulen optisch zugänglich sind. Mit einem Lasergerät ausgestattete Produkte müssen der International Electrotechnical Commission (IEC) 60825 entsprechen.

11.3 NORME DI SICUREZZA

Leggere le norme seguenti per prevenire lesioni personali ed evitare di danneggiare questo prodotto o altri a cui è collegato. Per evitare qualsiasi pericolo potenziale, usare il prodotto unicamente come indicato.

Leggere tutte le informazioni sulla sicurezza fornite nella guida per l'utente relativa al componente e comprendere le norme associate ai simboli di pericolo, agli avvisi scritti e alle precauzioni da adottare prima di accedere a componenti o aree dell'unità. Custodire il presente documento per usi futuri.

Attenzione: rispettare i requisiti ambientali del sistema. I componenti come le schede di processore, i commutatori Ethernet, ecc., sono progettati per funzionare in presenza di un flusso di aria proveniente dall'esterno, in assenza del quale rischiano di danneggiarsi irrimediabilmente. In genere, il flusso di aria esterno viene generato da appositi ventilatori installati contemporaneamente ai componenti nello chassis compatibile. Non ostacolare mai il flusso di aria convogliato dal ventilatore e dai condotti dell'unità. I pannelli di copertura o le schede per il controllo dell'aria devono essere installati negli alloggiamenti vuoti dello chassis. I requisiti ambientali possono variare a seconda del prodotto. Per ulteriori informazioni sui requisiti del flusso di aria e sugli altri requisiti ambientali, consultare la guida per l'utente del prodotto.

Avvertenza: i dissipatori di calore possono scaldarsi durante il funzionamento normale. Per evitare bruciature o danni, evitare il contatto del dissipatore di calore con qualsiasi altro elemento.

Avvertenza: evitare lesioni, possibili cause di incendio o di esplosione. Non usare il prodotto in un'atmosfera in cui sussiste il rischio di esplosione.

Attenzione: le batterie al litio non possono essere sostituite dall'utente. La sostituzione o l'uso non corretto della batteria comporta un rischio di esplosione. Non smontare né ricaricare la batteria. Non gettare la batteria nel fuoco. Per la sostituzione, usare il tipo di batteria identico o equivalente consigliato dal costruttore. Le batterie usate devono essere smaltite rispettando le istruzioni del costruttore. Per la riparazione della batteria, restituire l'unità a Intel.

Avvertenza: evitare le lesioni. Questo prodotto può contenere uno o più dispositivi laser accessibili alla vista, a seconda dei moduli installati. I prodotti provvisti di un dispositivo laser devono essere conformi alla norma 60825 della Commissione elettrotecnica internazionale (IEC).

F.3 INSTRUCCIONES DE SEGURIDAD

Examine las instrucciones sobre condiciones de seguridad que siguen para evitar cualquier tipo de daños personales, así como para evitar perjudicar el producto o productos a los que esté conectado. Para evitar riesgos potenciales, utilice el producto únicamente en la forma especificada.

Lea toda la información relativa a seguridad que se incluye en los manuales de usuario de los distintos componentes y procure familiarizarse con los distintos símbolos de seguridad, advertencias escritas y normas de precaución antes de manipular las distintas piezas o secciones de la unidad. Guarde este documento para consultarlo en el futuro.

Precaución: Requisitos de entorno para el sistema: Los componentes del tipo de placas de procesador, conmutadores de Ethernet, etc., están concebidos para funcionar en condiciones que permitan el paso de aire. Los componentes pueden averiarse si funcionan sin que circule el aire en su entorno. La circulación del aire suele estar facilitada por los ventiladores incorporados en el armazón cuando los componentes están instalados en armazones compatibles. Nunca interrumpa el paso del aire por los ventiladores or los respiraderos. Los paneles de relleno y las placas para el control de la circulación del aire deben instalarse en ranuras del chasis que no estén destinadas a ningún otro uso. Las características técnicas relativas al entorno pueden variar entre productos. Consulte los manuales de usuario del producto si necesita conocer sus necesidades en términos de circulación de aire u otras características técnicas.

Advertencia: En condiciones de funcionamiento normales, los disipadores de calor pueden recalentarse. Evite que ningún elemento entre en contacto con los disipadores para evitar quemaduras.

Advertencia: Riesgos de daños, incendio o explosión: No permita que el aparato funcione en una atmósfera que presente riesgos de explosión.

Precaución: El usuario no debe cambiar las baterías de litio. Si las baterías no se manipulan o cambian correctamente, exite riesgo de explosión. No desmonte ni recargue la batería. Nunca tire las baterías al fuego. Al cambiar la batería, es preciso utilizar el mismo tipo o un tipo equivalente que haya sido recomendado por el fabricante. Las baterías utilizadas deben desecharse según las instrucciones del fabricante. Devuelva la unidad a Intel si la batería necesita algún tipo de operación de mantenimiento.

Advertencia: Daños personales: Este producto puede contener uno o varios dispositivos láser, que estarán a la vista dependiendo de los módulos enchufables que se hayan instalado. Los productos provistos de un dispositivo láser deben ajustarse a la norma 60825 de la International Electrotechnical Commission (IEC).

Serial Port Requirements G

G.1 Pin Assignments

Table 37. RJ-45 Pin Assignments

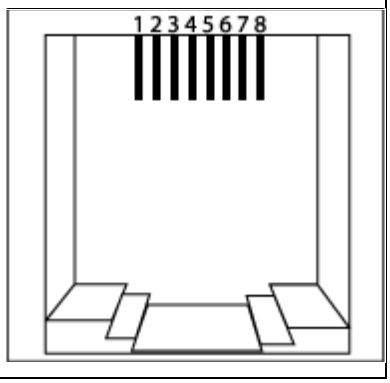
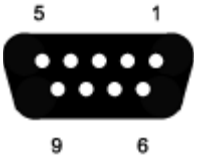
RJ-45 Pin	Signal	
1	RTS	
2	DTR	
3	TxD	
4	GND	
5	GND	
6	RxD	
7	DSR	
8	CTS	

Table 38. DB-9 Pin Assignments

DB-9 Pin	Signal	
1	GND Shield	
2	RxD	
3	TxD	
4	DTR	
5	GND	
6	DSR	
7	RTS	
8	CTS	
9	NC	

G.1.1 Building the Cable

The serial cable allows you to manage the switch from the serial port on the front panel. To build this cable, use a RJ-45 connector for the switch, a DB-9 connector for the terminal, and the following diagram as a guide for the wiring.

Figure 6. Male RJ-45 Connector