BlackDiamond 10808

BlackDiamond® 10808—Redefining the Intelligent Core.

Security

- Threat detection and response with CLEAR-Flow Security Rules Engine
- Layer 3 virtual switching
- Hardened network infrastructure

Voice-Class Availability

- Redundant hardware design
- Modular operating system for non-stop operation with ExtremeXOS® Operating System (OS)
- High availability network using Ethernet Automatic Protection Switching (EAPS)

Scalable Performance

- System scalability with large table sizes, port capacity
- Quality of Service (QoS) and multicast performance providing application scalability
- Scalable management through extensibility

BlackDiamond 10808 hardware supports a wide array of protocols. In addition, BlackDiamond 10808 incorporates programmable ASIC technology. This programmability ensures that the platform will support emerging protocols without costly hardware upgrades—thus offering great investment protection.

These applications require high-performance, scalability and the highest level of resiliency. Even more importantly, BlackDiamond 10808 is de-signed to help meet tomorrow's needs as well as today's. Extensibility is the key to building intelligent core networks that can adapt and respond to changing requirements over time; this is where BlackDiamond 10808 truly stands alone.

Target Applications

BlackDiamond 10808 has been designed to excel in a wide array of applications, including:

- Enterprise backbone switch for high-performance networks
- Enterprise data center switch providing server interconnection for mission-critical applications
- Switch for Carrier Ethernet core and distri-bution delivering triple play services
- Switch for Internet exchanges providing high-bandwidth Layer 2 interconnection
- Interconnect switch for High Performance Cluster Computing (HPCC) delivering solutions to complex computing problems

BlackDiamond 10808 delivers security that scales to 10 gigabit rates, voice-class availability and pre-dictable performance.

Security

BlackDiamond 10808 delivers a new level of security to Ethernet core networking. BlackDiamond 10808 complements the perimeter firewalls by protecting the "soft interior" of the network that currently goes unprotected. Utilizing the industry's most advanced CLEAR-Flow Security Rules Engine, BlackDiamond 10808 can be programmed to automatically detect and mitigate security threats in seconds.

Threat Detection and Response

CLEAR-Flow Security Rules Engine

CLEAR-Flow Security Rules Engine provides first order threat detection and mitigation and mirrors traffic to security resources for further analysis of suspicious traffic in the network. Security resources are virtually available across the entire multi-gigabit network thus enabling cost-effective scalability of the security solution.

Sentriant® security appliance can add/modify the BlackDiamond 10808 switch's CLEAR-Flow rules and Access Control Lists (ACLs) to inspect additional traffic or change inspection thresholds thereby allowing an automated system to fine-tune inspection rules in real-time.

Port Mirroring

Providing intrusion detection and prevention, BlackDiamond 10808 supports many-to-one and cross-module port mirroring. This can be used to mirror traffic to an external network appliance such as an intrusion detection device for trend analysis or be utilized by a network administrator as a diagnostic tool when fending off a network attack.

Line-Rate Access Control Lists

ACLs are one of the most powerful tools to control network resource utilization and to secure and protect the network. BlackDiamond 10808 supports up to 128K ACLs based on Layer 2, 3 or 4 header information such as the MAC address or IP source/destination address.

Virtual Router

With Layer 3 Virtual Switching, BlackDiamond brings the concept of virtualization to multi-layer switching. Layer 3 Virtual Switching allows partitioning of a single switch into many virtual routers. A virtual router has the same capabilities and properties as a physical router does. It inherits all the same routing mechanisms for configuration, operation and troubleshooting. As a result, each virtual switch domain can be separately managed and isolated for security safety measures (refer to Figure 1: Layer 3 Virtual Switching).
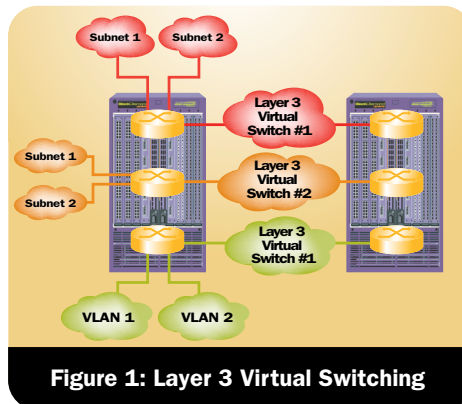

Figure 1: Layer 3 Virtual Switching

Network traffic can also be secluded into separate virtual domains to minimize security threats. The design of virtual switch domains enables logical separation of route tables. Multiple route tables enable route isolation, which allows the operator to make use of overlapping IP address spaces. Overlapping IP address spaces allow multiple communities of interest to share a single physical networking infrastructure.

Hardened Network Infrastructure

Denial of Service Protection

BlackDiamond 10808 handles Denial of Service (DoS) attacks gracefully. If the switch detects an unusually large number of packets in the CPU input queue, it will assemble ACLs that automatically stop these packets from reaching the CPU. After a period of time, the ACLs are removed. If the attack continues, they are reinstalled.

ASIC-based Longest Prefix Match

Longest Prefix Match (LPM) routing elimin-ates the need for control plane software to learn new flows and allows the network to be resilient under a DoS attack. With LPM the CPU is not burdened with forwarding the "first packet" to any unrecognized destination, freeing the CPU for critical tasks.

Secure Management

Protocols like SSH2, SCP and SNMPv3 supported by a BlackDiamond 10808 series switch prevent the interception of management communications and man-in-the-middle attacks.

MD5 Authentication of Routing Protocols

MD5 authentication of routing protocols prevents attackers from tampering with valid messages and attacking routing sessions.

Voice-Class Availability

A high-performance network connection, whether used to connect PCs and IP telephones at the access layer or to interconnect servers in a cluster, is only useful if it is also highly available. BlackDiamond 10808 utilizes the industry-leading ExtremeXOS modular operating system that raises the availability of the switch. Network level resiliency protocols are added to increase the availability of the network.

Redundant Hardware Design

Redundant Management Modules

BlackDiamond 10808 is configured so that if one Management Switch Module (MSM) fails, the second MSM will automatically take over management responsibility for the entire switch. This feature is critical for networks running voice and other mission-critical applications.

Advanced Chassis Design for Availability

BlackDiamond 10808 includes a passive backplane complemented by high-availability design elements such as isolated control and data planes, redundant controller boards for power distribution and fan control, and environmental monitoring to identify anomalies before they affect network availability.

Redundant Load Sharing Power Supplies

BlackDiamond 10808 supports a set of redundant power configurations that can load share up to six internal power supplies simultaneously. Four power supplies in a 3 + 1 redundancy configuration can power a fully loaded chassis with gigabit or 10 Gigabit Ethernet ports. Six power supplies in a 3 + 3 configuration can provide input power redundancy.

Modular Operating System for Non-stop Operation

True Preemptive Multitasking and Protected Memory

ExtremeXOS allows each of the many tasks—such as Open Shortest Path First (OSPF) and Spanning Tree—to run as separate operating system tasks that are protected from each other as shown in Figure 2.

Process Monitoring and Restart

ExtremeXOS dramatically increases network availability by monitoring in real time the independent operating system processes. If any of them become unresponsive, or stop running, they are automatically restarted.

Loadable Software Modules

The modular design of ExtremeXOS allows the extension of switch functionality. New functionality can easily be added to the switch.

High Availability Network Protocols

Ethernet Automatic Protection Switching

EAPS allows the IP network to provide the level of resiliency and uptime that users expect from their traditional voice networks. EAPS is superior to the Spanning Tree or Rapid Spanning Tree Protocols, offering sub-second (less than 50 milliseconds) recovery and delivers consistent failover regardless of number of VLANs, number of network nodes or network topology. In most situations, VoIP calls don't drop and digital video feeds don't freeze or pixelize because EAPS enables the network to recover almost transparently from link failure.

Spanning Tree/Rapid Spanning Tree Protocols

BlackDiamond 10808 supports Spanning Tree (802.1D), Per VLAN Spanning Tree (PVST+), Rapid Spanning Tree (802.1w) and Multiple Instances of Spanning Tree (802.1s) protocols for Layer 2 resiliency.

Software Enhanced Availability

Software enhanced availability allows users to remain connected to the network even if part of the network infrastructure is down. The BlackDiamond 10808 switch constantly checks for problems in the network connections using advanced Layer 3 protocols such as OSPF (with graceful restart), VRRP and ESRP (ESRP supported in Layer 2 or Layer 3), and dynamically routes around the problem.

Equal Cost Multipath

Equal Cost Multipath enables uplinks to be load balanced for performance and cost savings while also supporting redundant failover. If an uplink fails, traffic is automatically routed to the remaining uplinks and connectivity is maintained.

Link Aggregation (802.3ad)

Cross-module link aggregation enables trunking of up to eight links on a single logical connection, for up to 80 Gbps of redundant bandwidth per logical connection.
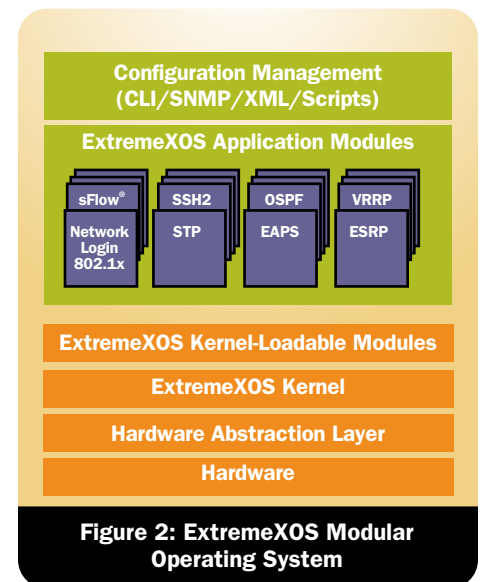

Configuration Management (CLI/SNMP/XML/Scripts)			
ExtremeXOS Application Modules			
sFlow®	SSH2	OSPF	VRRP
Network Login 802.1x	STP	EAPS	ESRP
ExtremeXOS Kernel-Loadable Modules			
ExtremeXOS Kernel			
Hardware Abstraction Layer			
Hardware			

Figure 2: ExtremeXOS Modular Operating System

Scalable Performance

Offering industry-leading 10 gigabit and Gigabit Ethernet port density, BlackDiamond 10808 scales to meet the immediate requirements and anticipates future requirements of even very demanding IPv4 and IPv6 environments.

System Scalability

Port Density

Port density is critical to the scalability of a switching solution. The moment a single additional port is needed above and beyond what is available with any single switch, hierarchical switching is required. As soon as more than one switch is needed for an application, up to half of each switch's bandwidth may need to be dedicated just for switch interconnects. As a result, the network becomes much more complex and expensive.

It is always desirable for a single switch to support more ports than initially required. This "headroom" helps to future-proof the network design (refer to Figure 4: Port Capacity).

Application Scalability

QoS Performance

BlackDiamond 10808 delivers deep packet buffers throughout the architecture, helping ensure to that even in times of congestion, packets can be queued and reliably delivered (rather than being discarded). While this adds latency under such times of stress, less ad-vanced switches will instead discard the excess traffic. By buffering the traffic, servers do not need to timeout and retransmit traffic—greatly increasing the efficiency of both the network and the computer engines.

Low Latency

When selecting a networking switch for high-performance applications, selecting low-latency alternatives for the networking component provides added margin for latency introduced by other elements. With the low switching latency of 9 microseconds for 64-byte packets, BlackDiamond 10808 is ideal for high-performance applications.

Jumbo Frame Support

Jumbo frames of up to 9,216 bytes in length are supported by BlackDiamond 10808. Jumbo frames are particularly important in high-performance cluster computing applications, where studies have shown their use can reduce server CPU loads by as much as 50%. Jumbo frames also reduce protocol overhead and ensure higher overall network throughput—since protocol headers are fixed size, larger frames have a higher ratio of packet payload to packet header.

Multicast

BlackDiamond 10808 builds on Extreme Networks® leadership position in IP multicast, supporting hardware identification and replication of multicast traffic. Extreme Networks unique switch fabric architecture need not store and forward multiple copies of the same packet across the fabric. This ensures excellent multicast performance without impacting other traffic running through the switch. Multicast features include Internet Group Management Protocol (IGMP v1, v2 & v3) and Protocol Independent Multicast (PIM), Dense Mode (DM), Sparse Mode (SM) and Source Specific Mode (SSM).

Scalable Management Through Extensibility

Ease of Management

Extreme Networks has developed tools that save you time and resources in managing your network. EPICenter™ provides fault, configuration, accounting, performance, and security functions to manage Extreme Networks multi-layer switching equipment in a converged network.

Extensibility to Integrate New Applications

ExtremeXOS allows for flexible expansion of network capabilities by providing a mechanism for third-party applications in the network to interact directly with the operating system. ExtremeXOS uses a secure XML-based API to integrate with best-of-breed monitoring and security devices. This extensibility allows integration with third-party applications to provide a closed loop for new monitoring and response capabilities.
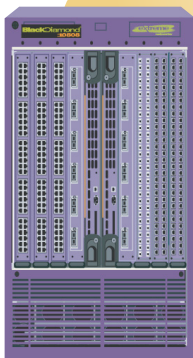
I/O Modules	Port Capacity
60-port 10/100/1000BASE-T (RJ-45)	48-10GBASE-X (XENPAK) ports
60-port 1000BASE-X (SFP)	480-10/100/1000BASE-T ports
20-port 1000BASE-X (SFP)	480-1000BASE-X SFP ports
6-port 10GBASE-X (XENPAK)	
2-port 10GBASE-X (XENPAK)	

Hybrid module with:
     2-port 10GBASE-X (XENPAK)
     20-port 1000BASE-X (SFP)
     20-port 10/100/1000BASE-T (RJ-45)	

Figure 3: Port Capacity

Target Applications

Enterprise Core

BlackDiamond 10808 provides the medium to large enterprise an ideal core switch solution that satisfies their complete network needs. The CLEAR-Flow Security Rules Engine and Layer 3 virtual switching capability of BlackDiamond 10808 has set the bar for core security.
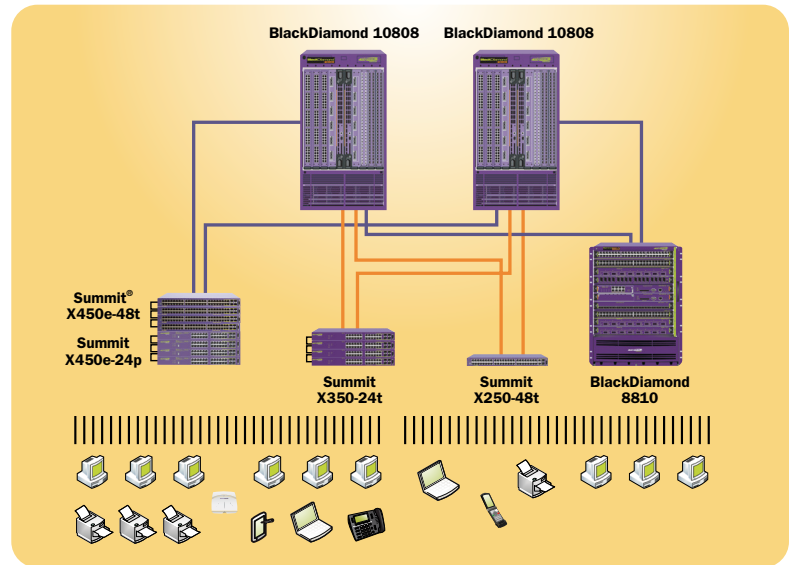

Carrier Ethernet Core and Distribution

Carrier Ethernet networks are typically composed of three device types—Customer Edge, Provider Edge and Provider Aggregation. Not all networks will use all three devices. For example, an IPTV network may be deployed using only a provider aggregation switch at a provider point of presence. BlackDiamond 10808 is ideally suited for either provider aggregation or point of presence within Carrier Ethernet networks.
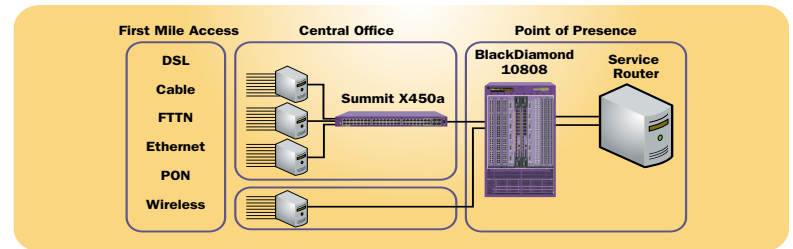
Internet Exchanges

An Internet Exchange Point (IXP) allows different Internet Service Providers (ISPs) to exchange Internet traffic between their autonomous systems by means of mutual peering agreements. IXPs are typically used by ISPs to reduce dependency on their respective upstream providers; furthermore, they are used to increase efficiency and fault-tolerance. BlackDiamond 10808 addresses the need for high-performance and fault-tolerant connectivity required for IXPs using gigabit and 10 Gigabit Ethernet as the interconnect technology, along with resiliency technologies such as EAPS.
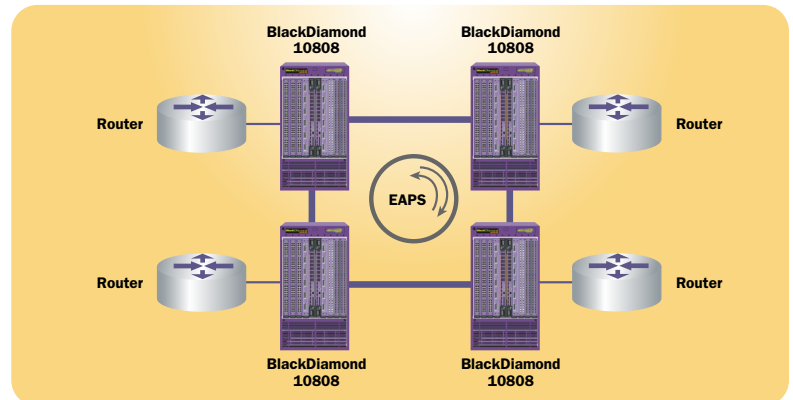
Technical Specifications

ExtremeXOS 12.4
Supported Protocols

Switching

- RFC 3619 Ethernet Automatic Protection Switching (EAPS) and EAPSv2
- IEEE 802.1D – 1998 Spanning Tree Protocol (STP)
- IEEE 802.1D – 2004 Spanning Tree Protocol (STP and RSTP)
- IEEE 802.1w – 2001 Rapid Reconfiguration for STP, RSTP
- IEEE 802.1Q – 2003 (formerly IEEE 802.1s) Multiple Instances of STP, MSTP
- EMISTP, Extreme Multiple Instances of Spanning Tree Protocol
- PVST+, Per VLAN STP (802.1Q interoperable)
- Draft-ietf-bridge-rstpmib-03.txt – Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol
- Extreme Standby Router Protocol™ (ESRP)
- IEEE 802.1Q – 1998 Virtual Bridged Local Area Networks
- IEEE 802.3ad Static load sharing configuration and LACP based dynamic configuration
- Software Redundant Ports
- IEEE 802.1AB – LLDP Link Layer Discovery Protocol
- LLDP Media Endpoint Discovery (LLDP-MED), ANSI/TIA-1057, draft 08
- Extreme Discovery Protocol (EDP)
- Extreme Loop Recovery Protocol (ELRP)
- Extreme Link State Monitoring (ELSM)
- IEEE 802.1ag L2 Ping and traceroute, Connectivity Fault Management
- ITU-T Y.1731 Frame delay measurements

Management and Traffic Analysis

- RFC 2030 SNTP, Simple Network Time Protocol v4
- RFC 854 Telnet client and server
- RFC 783 TFTP Protocol (revision 2)
- RFC 951, 1542 BootP
- RFC 2131 BOOTP/DHCP relay agent and DHCP server
- RFC 1591 DNS (client operation)
- RFC 1155 Structure of Mgmt Information (SMIv1)
- RFC 1157 SNMPv1
- RFC 1212, RFC 1213, RFC 1215 MIB-II, Ethernet-Like MIB & TRAPs
- RFC 1573 Evolution of Interface
- RFC 1650 Ethernet-Like MIB (update of RFC 1213 for SNMPv2)
- RFC 1901, 1905 – 1908 SNMP v2c, SMIv2 and Revised MIB-II
- RFC 2576 Coexistence between SNMP Version 1, Version 2 and Version 3
- RFC 2578 – 2580 SMIv2 (update to RFC 1902 – 1903)
- RFC 3410 – 3415 SNMPv3, user based security, encryption and authentication
- RFC 3826 – The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model
- RFC 1757 RMON 4 groups: Stats, History, Alarms and Events
- RFC 2021 RMON2 (probe configuration)
- RFC 2613 SMON MIB

- RFC 2925 Ping/Traceroute MIB
- RFC 2668 802.3 MAU MIB
- draft-ietf-hubmib-mau-mib-v3-02.txt
- RFC 1643 Ethernet MIB
- RFC 1493 Bridge MIB
- RFC 2096 IPv4 Forwarding Table MIB
- RFC 2737 Entity MIB v2
- RFC 2233 Interface MIB
- RFC 3621 PoE-MIB (PoE switches only)
- IEEE 802.1ag MIB
- Secure Shell (SSH-2) client and server
- Secure Copy (SCP-2) client and server
- Secure FTP (SFTP) server
- sFlow version 5
- Configuration logging
- Multiple Images, Multiple Configs
- RFC 3164 BSD Syslog Protocol with Multiple Syslog Servers
  - 999 Local Messages (criticals stored across reboots)
- Extreme Networks vendor MIBs (includes FDB, PoE, CPU, Memory MIBs)
- XML APIs over Telnet/SSH and HTTP/HTTPS
- Web-based device management interface – ExtremeXOS ScreenPlay™
- IP Route Compression

Security, Switch and Network Protection

- Secure Shell (SSH-2), Secure Copy (SCP-2) and SFTP client/server with encryption/authentication (requires export controlled encryption module)
- SNMPv3 user based security, with encryption/authentication (see above)
- RFC 1492 TACACS+
- RFC 2138 RADIUS Authentication
- RFC 2139 RADIUS Accounting
- RFC 3579 RADIUS EAP support for 802.1x
- RADIUS Per-command Authentication
- Access Profiles on All Routing Protocols
- Access Policies for Telnet/SSH-2/SCP-2
- Network Login – 802.1x, Web and MAC-based mechanisms
- IEEE 802.1x – 2001 Port-Based Network Access Control for Network Login
- Multiple supplicants with multiple VLANs for Network Login (all modes)
- Fallback to local authentication database (MAC and Web-based methods)
- Guest VLAN for 802.1x
- RFC 1866 HTML – Used for Web-based Network Login and ExtremeXOS ScreenPlay
- SSL/TLS transport – used for Web-based Network Login and ExtremeXOS ScreenPlay (requires export controlled encryption module)
- MAC Security – Lockdown and Limit
- IP Security – RFC 3046 DHCP Option 82 with port and VLAN ID
- IP Security – Trusted DHCP Server
- Layer 2/3/4 Access Control Lists (ACLs)
- RFC 2267 Network Ingress Filtering
- RPF (Unicast Reverse Path Forwarding) Control via ACLs
- Wire-speed ACLs
- Rate Limiting/Shaping by ACLs
- IP Broadcast Forwarding Control
- ICMP and IP-Option Response Control
- SYN attack protection

- CPU DoS Protection with traffic rate-limiting to management CPU
- Robust against common Network Attacks:
  - CERT (http://www.cert.org)
  - CA-2003-04: "SQL Slammer"
  - CA-2002-36: "SSHredder"
  - CA-2002-03: SNMP vulnerabilities
  - CA-98-13: tcp-denial-of-service
  - CA-98.01: smurf
  - CA-97.28:Teardrop_Land -Teardrop and "LAND" attack
  - CA-96.26: ping
  - CA-96.21: tcp_syn_flooding
  - CA-96.01: UDP_service_denial
  - CA-95.01: IP_Spoofing_Attacks_and_ Hijacked_ Terminal_Connections
  - IP Options Attack
- Host Attacks
  - Teardrop, boink, opentear, jolt2, newtear, nestea, syndrop, smurf, fraggle, papasmurf, synk4, raped, winfreeze, ping –f, ping of death, pepsi5, Latierra, Winnuke, Simping, Sping, Ascend, Stream, Land, Octopus

Security, Router Protection
Requires Edge License or above

- IP Security – DHCP enforcement via Disable ARP Learning
- IP Security – Gratuitous ARP Protection
- IP Security – DHCP Secured ARP/ARP Validation
- Routing protocol MD5 authentication

Security Detection and Protection
In Core and Aggregation Products only

- CLEAR-Flow, threshold-based alerts and actions

IPv4 Host Requirements

- RFC 1122 Host Requirements
- RFC 768 UDP
- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 826 ARP
- RFC 894 IP over Ethernet
- RFC 1027 Proxy ARP
- RFC 2068 HTTP server
- IGMP v1/v2/v3 Snooping with Configurable Router Registration Forwarding
- IGMP Filters
- PIM Snooping
- Static IGMP Membership
- Multicast VLAN Registration (MVR)

IPv4 Router Requirements
Requires Advanced Edge License or above

- RFC 1812 Requirements for IP Version 4 Routers
- RFC 1519 CIDR
- RFC 1256 IPv4 ICMP Router Discovery (IRDP)
- Static Unicast Routes
- Static Multicast Routes
- RFC 1058 RIP v1
- RFC 2453 RIP v2
- Static ECMP
- RFC 1112 IGMP v1

Technical Specifications

IPv4 Router Requirements continued

Requires Advanced Edge License or above

- RFC 2236 IGMP v2
- RFC 3376 IGMP v3
- RFC 2933 IGMP MIB
- RFC 2096 IPv4 Forwarding Table MIB
- RFC 1724 RIPv2 MIB
- RFC 2338 VRRP
- RFC 2787 VRRP MIB
- RFC 2328 OSPF v2 (Edge-mode)
- OSPF ECMP
- OSPF MD5 Authentication
- RFC 1587 OSPF NSSA Option
- RFC 1765 OSPF Database Overflow
- RFC 2370 OSPF Opaque LSA Option
- RFC 3623 OSPF Graceful Restart
- RFC 1850 OSPFv2 MIB
- RFC 2362 PIM-SM (Edge-mode)
- RFC 2934 PIM MIB
- RFC 3569, draft-ietf-ssm-arch-06.txt PIM-SSM PIM Source Specific Multicast
- draft-ietf-pim-mib-v2-o1.txt
- Mtrace, a "traceroute" facility for IP Multicast: draft-ietf-idmr-traceroute-ipm-07
- Mrinfo, the multicast router information tool based on Appendix-B of draft-ietf-idmr-dvmrp-v3-11

IPv6 Host Requirements

Current support on ExtremeXOS based Summit series, BlackDiamond 8800 series, BlackDiamond 10808 series and BlackDiamond 12800 series

- RFC 5095, Internet Protocol, Version 6 (IPv6) Specification
- RFC 4861, Neighbor Discovery for IP Version 6, (IPv6)
- RFC 2463, Internet Control Message Protocol (ICMPv6) for the IPv6 Specification
- RFC 2464, Transmission of IPv6 Packets over Ethernet Networks
- RFC 2465, IPv6 MIB, General Group and Textual Conventions
- RFC 2466, MIB for ICMPv6
- RFC 2462, IPv6 Stateless Address Auto configuration – Host Requirements
- RFC 1981, Path MTU Discovery for IPv6, August 1996 – Host requirements
- RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture
- RFC 3587, Global Unicast Address Format
- Telnet server over IPv6 transport
- SSH-2 server over IPv6 transport
- Ping over IPv6 transport
- Traceroute over IPv6 transport

IPv6 Interworking and Migration

Current support on ExtremeXOS based Summit series, BlackDiamond 8800 series, BlackDiamond 10808 series and BlackDiamond 12800 series

- RFC 2893, Configured Tunnels
- RFC 3056, 6to4

IPv6 Router Requirements

Current support on ExtremeXOS based Summit series, BlackDiamond 8800 series, BlackDiamond 10808 series and BlackDiamond 12800 series

- RFC 2462, IPv6 Stateless Address Auto configuration – Router Requirements
- RFC 1981, Path MTU Discovery for IPv6, August 1996 – Router requirements
- RFC 2710, IPv6 Multicast Listener Discovery v1 (MLDv1) Protocol
- RFC 3810, IPv6 Multicast Listener Discovery v2 (MLDv2) Protocol
- Static Unicast routes for IPv6
- RFC 2080, RIPng
- Static ECMP

Core Protocols for Layer 2, IPv4 and IPv6

Requires Core License or above

- EAPSv2 Shared Ports – multiple interconnections between rings
- PIM-DM Draft IETF PIM Dense Mode draft-ietf-idmr-pim-dm-05.txt, draft-ietf-pim-dm-new-v2-04.txt
- RFC 3618 Multicast Source Discovery Protocol (MSDP)
- RFC 3446 Anycast RP using PIM and MSDP
- RFC 2740 OSPFv3, OSPF for IPv6 – *Current support on Summit series with Core License or above, BlackDiamond 8800 series, BlackDiamond 10808 series, and BlackDiamond 12800 series*
- RFC 1771 Border Gateway Protocol 4
- RFC 1965 Autonomous System Confederations for BGP
- RFC 2796 BGP Route Reflection (supersedes RFC 1966)
- RFC 1997 BGP Communities Attribute
- RFC 1745 BGP4/IDRP for IP-OSPF Interaction
- RFC 2385 TCP MD5 Authentication for BGPv4
- RFC 2439 BGP Route Flap Damping
- RFC 2918 Route Refresh Capability for BGP-4
- RFC 3392 Capabilities Advertisement with BGP-4
- RFC 4360 BGP Extended Communities Attribute
- RFC 4486 Subcodes for BGP Cease Notification message
- draft-ietf-idr-restart-10.txt Graceful Restart Mechanism for BGP
- RFC 4760 Multiprotocol extensions for BGP-4
- RFC 1657 BGP-4 MIB
- Draft-ietf-idr-bgp4-mibv2-02.txt – Enhanced BGP-4 MIB
- RFC 1195 Use of OSI IS-IS for Routing in TCP/IP and Dual Environments (TCP/IP transport only)
- RFC 2763 Dynamic Hostname Exchange Mechanism for IS-IS
- RFC 2966 Domain-wide Prefix Distribution with Two-Level IS-IS
- RFC 2973 IS-IS Mesh Groups
- RFC 3373 Three-way Handshake for IS-IS Point-to-Point Adjacencies
- RFC 3784 IS-IS Externs for Traffic Engineering (wide metrics only)
- Draft-ietf-isis-restart-02 Restart Signaling for IS-IS

- Draft-ietf-isis-ipv6-06 Routing IPv6 with IS-IS – *Current support on Summit series with Core License or above, BlackDiamond 8800 series, BlackDiamond 10808 series, and BlackDiamond 12800 series*
- Draft-ietf-isis-wg-multi-topology-11 Multi Topology (MT) Routing in IS-IS

QoS and VLAN Services

Quality of Service and Policies

- IEEE 802.1D – 1998 (802.1p) Packet Priority
- RFC 2474 DiffServ Precedence, including 8 queues/port
- RFC 2598 DiffServ Expedited Forwarding (EF)
- RFC 2597 DiffServ Assured Forwarding (AF)
- RFC 2475 DiffServ Core and Edge Router Functions

VLAN Services: VLANs, vMANs

- IEEE 802.1Q VLAN Tagging
- IEEE 802.1v: VLAN classification by Protocol and Port
- Port-based VLANs
- Protocol-based VLANs
- MAC-based VLANs
- Multiple STP domains per VLAN
- Upstream Forwarding Only/Disable Flooding
- RFC 5517 Private VLANs
- VLAN Translation
- IEEE 802.1ad Provider Bridge Network, virtual MANs (vMANs)
- vMAN Ethertype Translation/Secondary vMAN Ethertype
- Multicast Support for PVLAN
- Multicast Support for VLAN Aggregation
- VLAN Aggregation (Requires Advanced Edge License or above)

Advanced VLAN Services, MAC-in-MAC

Requires Advanced Edge License or above (BlackDiamond 10808 and BlackDiamond 12800 series only)

- VLAN Translation in vMAN environments
- vMAN Translation
- IEEE 802.1ah/D1.2 Provider Backbone Bridges (PBB)/MAC-in-MAC

MPLS and VPN Services

Multi-Protocol Label Switching (MPLS)

Requires MPLS Layer 2 Feature Pack License

- RFC 2961 RSVP Refresh Overhead Reduction Extensions
- RFC 3031 Multiprotocol Label Switching Architecture
- RFC 3032 MPLS Label Stack Encoding
- RFC 3036 Label Distribution Protocol (LDP)
- RFC 3209 RSVP-TE: Extensions to RSVP for LSP Tunnels
- RFC 3630 Traffic Engineering Extensions to OSPFv2
- RFC 3811 Definitions of Textual Conventions (TCs) for Multiprotocol Label Switching (MPLS) Management
- RFC 3812 Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB)
- RFC 3813 Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB)

Technical Specifications

MPLS and VPN Services continued

Multi-Protocol Label Switching (MPLS)

Requires MPLS Layer 2 Feature Pack License
- RFC 3815 Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)
- RFC 4090 Fast Re-route Extensions to RSVP-TE for LSP (Detour Paths)
- RFC 4379 Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures (LSP Ping)

Layer 2 VPNs

Requires MPLS Layer 2 Feature Pack License
- RFC 4447 Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)
- RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks
- RFC 4762 Virtual Private LAN Services (VPLS) using Label Distribution Protocol (LDP) Signaling
- RFC 5085 Pseudowire Virtual Circuit Connectivity Verification (VCCV)
- draft-ietf-bfd-base-09.txt Bidirectional Forwarding Detection
- RFC 5542 Definitions of Textual Conventions for Pseudowire (PW) Management
- RFC 5601 Pseudowire (PW) Management Information Base (MIB)
- RFC 5602 Pseudowire (PW) over MPLS PSN Management Information Base (MIB)
- RFC 5603 Ethernet Pseudowire (PW) Management Information Base (MIB)
- draft-ietf-l2vpn-vpls-mib-02.txt Virtual Private LAN Services (VPLS) Management Information Base

General Specifications

Switching Capacity

- 1.28 Tbps total switching capacity, with 9 microsecond latency for 64-byte packets

Port Capacity

- 48 ports of 10 Gigabit Ethernet
- 480 1000BASE-X SFP ports
- 480 10/100/1000BASE-T ports
- Future support for the emerging 40 and 100 Gigabit Ethernet standards

Management Switch Module

Management Switch Module Options
Management modules contain both the control plane as well as the switch fabric for the BlackDiamond 10808. Both MSMs are TCAM-based, and support Longest Prefix Match (LPM) routing. Two initial versions of MSM are available:
- **MSM-1:** The MSM-1 includes support for up to 112,000 MAC addresses, 112,000 IP, routes and 64,000 ACLs. MSM-1 is designed for most mid-sized to large enterprises. MPLS is not supported on the MSM-1
- **MSM-1XL:** The MSM-1XL includes support for up to 224,000 MAC addresses, 224,000 Layer 3 LPM Entries, and 128,000 ACLs. MSM-1XL is required to run MPLS

I/O Module Options

G60T
60-port 10/100/1000BASE-T Gigabit Ethernet module (RJ-45)

G60X
60-port 1000BASE-X Gigabit Ethernet module
- SFP modules required. SFP options include:
  - SX (up to 550m)
  - LX (up to 5km as per standard; up to 10km with 2 Extreme Networks optics)
  - ZX (up to 70km)

G20X
20-port 1000BASE-X Gigabit Ethernet module
- SFP modules required. SFP options include:
  - SX (up to 550m)
  - LX (up to 5km as per standard; up to 10km with 2 Extreme Networks optics)
  - ZX (up to 70km)

10G6X
6-port 10 Gigabit Ethernet module
- XENPAK modules required. XENPAK options include:
  - SR (up to 300m)
  - LR (up to 10km)
  - ER (up to 40km)
  - ZR (up to 80km)
  - LX4 (up to 300m MMF, 10km SMF)

10G2X
2-port 10 Gigabit Ethernet module
- XENPAK modules required. XENPAK options include:
  - SR (up to 300m)
  - LR (up to 10km)
  - ER (up to 40km)
  - ZR (up to 80km)
  - LX4 (up to 300m MMF, 10km SMF)

10G2H Hybrid module with:
2-port 10 gigabit
- XENPAK modules required. XENPAK options include:
  - SR (up to 300m)
  - LR (up to 10km)
  - ER (up to 40km)
  - ZR (up to 80km)
  - LX4 (up to 300m MMF, 1 km SMF)

20-port 1000BASE-X Gigabit Ethernet
- SFP modules required. SFPoptions include:
  - SX (up to 550m)
  - LX (up to 5km as per standard; up to 10km with 2 Extreme Networks optics)
  - ZX (up to 70km)

20-port 10/100/1000BASE-T Gigabit Ethernet (RJ-45)

Power Supply Options

Both AC and DC power supplies are available.
- AC power supplies can run from 100Volt to 240Volt, and deliver
  - 700W at 90V to 110V, or
  - 1200W at 200V to 220V
- 48V DC power supplies deliver 1200W of power

Physical Specifications

Dimensions

Chassis:
38.5" high (22 RU) x 17.3" wide x 21" deep (98.0 cm x 44.0 cm x 53.3 cm)

MSM Module Dimensions:
22.7" high x 17.9" deep x 1.7" width (57.7 cm x 45.5 cm x 4.3 cm)

I/O Module Dimensions:
22.7" high x 19.6" deep x 1.7" width (57.7 cm x 49.8 cm x 4.3 cm)

Weight

Empty Chassis: 105 lb (47.7 kg)
Power Supply: 7 lb (3.2 kg)
MSM-1 Module: 10.5 lb (4.8 kg)
MSM-1XL Module: 10.7 lb (4.9 kg)
G60T Module: 8.5 lb (3.9 kg)
G60X Module: 9.25 lb (4.2 kg)
G20X Module: 9.25 lb (4.2 kg)
10G6X Module: 7.75 lb (3.5 kg)
10G2X Module: 7.75 lb (3.5 kg)
10G2H Module: 8.5 lb (3.9 kg)
Chassis, fully loaded (max.): 242 lb (110 kg)

Power

Chassis with Fan Trays: 250W, 48V, 5.2A (Heat Dissipation: 853 BTU)
MSM-1, MSM-1XL: 335W, 48V, 7.0A (Heat Dissipation: 1144 BTU)
G60T: 220W, 48V, 4.6A (Heat Dissipation: 751 BTU)
G60X: 223W, 48V, 4.7A (Heat Dissipation: 761 BTU)
G20X: 140W, 48V, 2.9A (Heat Dissipation: 478 BTU)
10G6X: 230W, 48V, 4.8A (Heat Dissipation: 785 BTU)
10G2X: 145W, 48V, 3.0A (Heat Dissipation: 495 BTU)
10G2H: 223W, 48V, 4.7A (Heat Dissipation: 761 BTU)
Fully Loaded System (Chassis + 2 x MSM + 8 x 10G6X): 2760W (Heat Dissipation: 9,421 BTU)

Operating Specifications

Operating Temperature: 0° to 40° C
Storage Temperature: -40° to 70° C
Operating Humidity: 10% to 95% relative humidity, non-condensing EN60068 to Extreme IEC68 schedule

Technical Specifications

Regulatory/Safety

Safely Standards
- UL 1950 3rd Edition 2/93,
  (U.S. Safety of ITE)
- cULus Listed Equivalent to CAN/CSA-22.2
- No. 950-M93 (Canadian Safety of ITE)
- Low Voltage Directive (LVD)
  (European Safety Directive)
- CB Report and Certificate
  (International Safety of ITE)
- IEC60950:1991/A1-4 2nd Edition
  (European Safety of ITE)
- TUV GS Mark (German Notified Body)
- EN60950:1992/A1-4,A11+ Deviations
  (European Safety of ITE)
- S/NZS 3260 (Australia Safety Standard)
- S Mark (Argentina Safety Approval)
- GOST (Russian Federation Certificate)
  Laser Devices
- EN60825-1,2:1994, A11:1996
  (European Safety of Lasers Products)
- FCC 21 CFR Subpart J
  (U.S. Safety of Laser Products)
- CDRH Letter of Approval (U.S. FDA Approval)

EMI/EMC Standards
- FCC 47 CFR Part 15 Class A (U.S. Emissions)
- ICES-003 Class A (Canada Emissions)
- 89/336/EEC EMC Directive
  (European Requirements)
- CISPR22:1997 Class A
  (International Emissions)
- EN55022:1998 Class A (European Emissions)
- EN55024:1998 includes EN61000-4-
  2,3,4,5,6,8,11 (European Immunity)
- EN61000-3-2,3 (European Harmonics & Flicker)
- AS/NZS 3548 (Australia Emissions)
- VCCI Class A (Japan Emissions)
- CNS 13438:1997 Class A (Taiwan Emissions)
- MIC Mark (Korean Emissions &
  Immunity Approval)
- NOM/NYCE (Mexican Product Safety &
  EMC Authorities)
- Telcordia GR-1089 (Bellcore Emissions &
  Immunity Standard)

Telecom Standards
- EN 300 386-2 v1.1.3 (1997-12)
  (European Telecom Standard)

Environmental Standards
- EN60068 to Extreme IEC68 schedule
- ETS 300 019 to Extreme schedule
- Telcordia GR-63-Core (Bellcore Environmental
  & Safety Standard)

Warranty
- Ltd. 1-year on Hardware
- 90-days on Software
- For warranty details, visit
  www.extremenetworks.com/go/warranty

Ordering Information

Part Number	Name	Description
60011	BlackDiamond 10808 Chassis	BlackDiamond 10808 10-slot Chassis (Includes Fan Tray)
60020	BlackDiamond 10808 / BlackDiamond 8800 700W/1200W PSU	BlackDiamond 10808/BlackDiamond 8800 700W/1200W 100-240V PSU
60021	BlackDiamond 10808 / BlackDiamond 8800 1200W DC PSU	BlackDiamond 10808/BlackDiamond 8800 1200W -48V DC PSU
60015	BlackDiamond 10808 MSM-1 Mgmt Module	BlackDiamond 10808 Management and Switch Fabric Module 1
60016	BlackDiamond 10808 MSM-1XL Mgmt Module	BlackDiamond 10808 Management and Switch Fabric Module 1XL
61010	BlackDiamond 10808 G60X	BlackDiamond 10808 60-port 1000BASE-X SFP Module
61011	BlackDiamond 10808 G20X	BlackDiamond 10808 20-port 1000BASE-X SFP Module
61030	BlackDiamond10808 G60T	BlackDiamond 10808 60-port 10/100/1000BASE-T RJ-45 Module
61050	BlackDiamond 10808 10G6X	BlackDiamond 10808 6-port 10GBASE-X XENPAK Module
61051	BlackDiamond 10808 10G2X	BlackDiamond 10808 2-port 10GBASE-X XENPAK Module
61071	BlackDiamond 10808 10G2H	BlackDiamond 10808 hybrid module with - 2-port 10GBASE-X XENPAK - 20-port 1000BASE-X SFP - 20-port 10/100/1000BASE-T RJ-45
60012	BlackDiamond 10808 Spare Fan Tray	BlackDiamond 10808 Spare Fan Tray
60013	BlackDiamond 10808 Spare PSU Controller	BlackDiamond 10808 Spare PSU Controller
62001	BlackDiamond 10808 Blank Front Panel	BlackDiamond 10808 Blank Front Panel
62011	BlackDiamond 10808 Mid Mount Kit	BlackDiamond 10808 Mid Mount Kit
62012	BlackDiamond 10808 Spare Filter 3-pack	BlackDiamond 10808 Spare Filter 3-pack
62020	BlackDiamond 6808/10808 Cable Mgmt	BlackDiamond 6808/10808 Cable Management
86101	Universal Port Feature Pack	ExtremeXOS Universal Port Feature Pack
10110	SR XENPAK	10 Gigabit Ethernet XENPAK Transceiver, 850nm, up to 300m on multimode fiber, SC connector
10111	LR XENPAK	10 Gigabit Ethernet XENPAK Transceiver, 1310nm, up to 10km on single-mode fiber, SC connector
10112	ER XENPAK	10 Gigabit Ethernet XENPAK Transceiver, 1550nm, up to 40km on single-mode fiber, SC connector
10113	ZR XENPAK	10 Gigabit Ethernet XENPAK Transceiver, 1550nm, up to 80km on single-mode fiber, SC connector
10114	LX4 XENPAK	10 Gigabit Ethernet WWDM XENPAK Transceiver, 1310nm, up to 300m on multi-mode fiber and up to 10 km on a single-mode fiber, SC connector
10051	SX SFP	SFP, 1000BASE-SX, LC Connector
10052	LX SFP	SFP, 1000BASE-LX, LC connector
10053	ZX SFP	SFP, Extra long distance SMF 70 Km/21 dB budget, LC connector