BlackDiamond® 12804C

The BlackDiamond 12804C — Taking application performance to the next level.

Designed to Enforce Application Performance

- Quality of Service (QoS) and performance providing application scalability
- System scalability for multicast applications
- Scalable management through extensibility

Voice-Class Availability

- Redundant hardware design
- ExtremeXOS™ modular operating system
- High availability network using Ethernet Automatic Protection Switching (EAPS)

Resiliency Under Attack

- Threat detection and response with CLEAR-Flow Security Rules Engine
- Layer 3 Virtual Switching to separate customer domains
- Hardened network infrastructure

As today's enterprise networks continue to converge, there is an increasing need for application-level awareness within the core and aggregation layers of the network. As the leader in open converged networks, Extreme Networks® provides a new level of intelligence for Ethernet networking with the BlackDiamond 12804C switch.

The BlackDiamond 12804C delivers deterministic performance independent of what features are enabled and is capable of maintaining this performance under various failure conditions and/or under network attacks.

The BlackDiamond 12804C, like the BlackDiamond 10808, incorporates programmable ASIC technology. This programmability helps ensure that the platform will support emerging protocols without costly hardware upgrades—thus offering great investment protection.

The BlackDiamond 12804C is ideal for core or aggregation applications requiring high-performance, scalability and a high level of resiliency. Even more importantly, BlackDiamond 12804C is designed 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 12804C truly stands alone.

Target Applications

BlackDiamond 12804C has been designed to excel in a wide array of applications, including:

- Core applications for small and medium enterprises
- Traditional gigabit or 10 Gigabit Ethernet aggregation switch for secure environments

The BlackDiamond 12804C delivers the capability to enforce application performance security that scales to 10 gigabit rates, and voice-class availability.

Designed to Enforce Application Performance

The BlackDiamond 12804C provides deterministic performance independent of which features are enabled.

Application Scalability

QoS Performance

BlackDiamond 12804C delivers deep packet buffers throughout the architecture, helping ensure 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 advanced 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 compute engines.

Low Latency

When selecting a networking switch for converged 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 12804C is ideal for converged applications.

Jumbo Frame Support

Jumbo frames of up to 9,216 bytes in length are supported by the BlackDiamond 12804C. 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 12804C 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 (IGMPv2 & v3) and Protocol Independent Multicast (PIM). Both Sparse Mode and Dense Mode PIM are supported.

Scalable Management Through Extensibility

Ease of Management

Extreme Networks has developed tools that save you time and resources in managing your network. EPICenter® provides all fault configuration, accounting, performance, and security functions to manage Extreme Networks' multi-layer switching equipment in a converged network. EPICenter Policy Manager provides layer-independent policy enforcement for Layers 1 – 4. Our software application, ServiceWatch®, delivers powerful Layers 4 – 7 monitoring and management for mission-critical network services.

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 (see Figure 1).

Converged Network Analyzer

Switches from Extreme Networks provide high quality QoS on the LAN. Converged Network Analyzer (CNA) from Avaya® provides the ability to enhance Extreme Networks LAN advantages with the ability to optimize QoS on the WAN. CNA coupled with Extreme Networks infrastructure and QoS on the LAN provides an optimized end-to-end IP network for Voice-over-IP (VoIP) and other business-critical applications.

Extreme Networks has embedded Avaya's CNA monitoring software in its ExtremeXOS based switches. CNA makes networks more reliable by addressing issues with inconsistent application performance over IP WAN networks. CNA software monitors the IP network for problems that affect the user experience of and other applications. The optional Adaptive Path Controller module uses these assessment results to actively avoid problems in the network by selecting a better-performing alternative path whenever one is available. The result is consistent end-to-end QoS across the network.
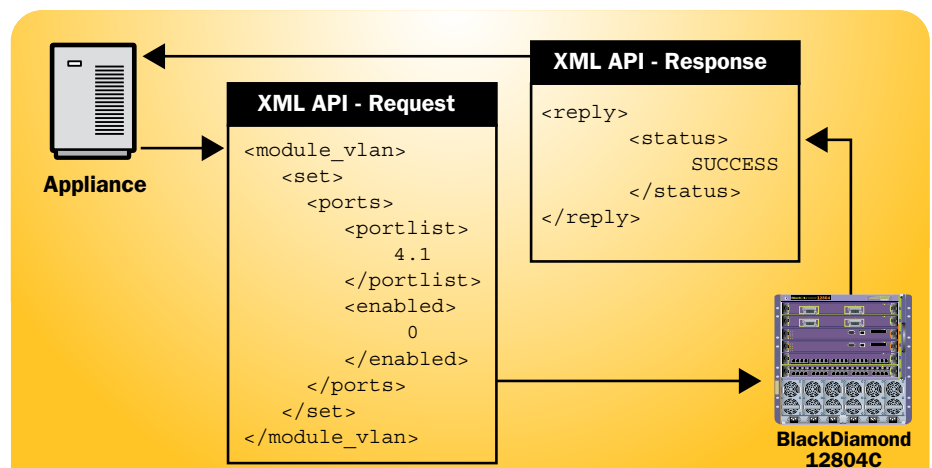

Figure 1: Extensibility with XML

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 12804C allows every active component (including the operating system) to be upgraded without taking the switch out of service. BlackDiamond 12804C also utilizes ExtremeXOS, the industry-leading modular operating system from Extreme Networks, that raises the availability of the switch. Network level resiliency protocols are added to increase the availability of the network.

Redundant Hardware Design

Fully Redundant Management Modules (1:1)

BlackDiamond 12804C is configured with a hitless failover mechanism so that if one Management Switch Module (MSM) fails, the second MSM will automatically take over management and switching responsibility for the entire switch. This feature is critical for networks running voice and other mission-critical applications.

Advanced Chassis Design for Availability

BlackDiamond 12804C include 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 12804C supports a set of redundant power configurations that can load share up to six internal power supplies simultaneously. These power supplies can be configured in an N + 1 configuration for power supply redundancy or in an N + N configuration to provide input power redundancy for a fully loaded chassis.

Modular Operating System for Non-stop Operations

Hitless Software Upgrade

The BlackDiamond 12804C supports hitless software upgrade, allowing the switch to be upgraded without the need for a maintenance window or bringing the switch off line. This increases network uptime and allows BlackDiamond 12804C to take advantage of new software features without the need for a network outage.

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 OS tasks that are protected from each other as shown in Figure 2.

Process Monitoring and Restart

ExtremeXOS dramatically increases network availability by monitoring the independent OS processes in real time. 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 without loading a new OS image and restarting the switch. New functionality can be added to the switch on the fly.

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. 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 12804C supports Spanning Tree, VLAN Spanning Tree (802.1D), and Rapid Spanning Tree (802.1w) 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. ExtremeXOS 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 links to be load balanced for performance and cost savings while also supporting redundant failover. If a link fails, traffic is automatically routed to the remaining links 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.
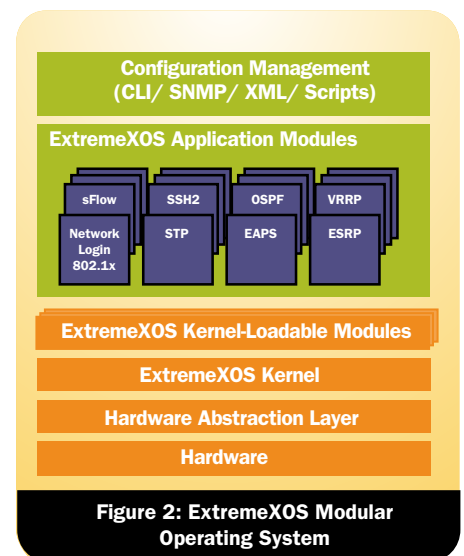

Configuration Management (CLI/ SNMP/ XML/ Scripts)

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

Resiliency Under Attack

BlackDiamond 12804C delivers a new level of security to Ethernet core networking. BlackDiamond 12804C 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 12804C 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 Virtualized Security Resources (VSRs) for further analysis of suspicious traffic in the network. VSRs are virtually available across the entire multi-gigabit network thus enabling cost-effective scalability of the security solution.

For example, Extreme Networks Sentriant™ VSR can add/modify the BlackDiamond 12804C 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

The BlackDiamond 12804C 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 12804C supports thousands of ACLs based on Layer 2, 3 or 4-header information such as the MAC address or IP source/destination address.

Layer 3 Virtual Switching

With Layer 3 Virtual Switching, the BlackDiamond 12804C brings the concept of virtualization to multi-layer switching. Layer 3 Virtual Switching allows partitioning of a single switch into many virtual routers. A Layer 3 virtual switch 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 3: Layer 3 Virtual Switching).
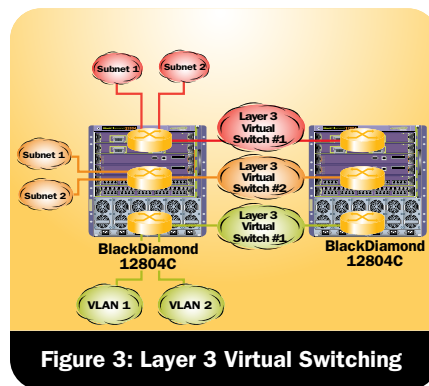

Figure 3: Layer 3 Virtual Switching

Network traffic can be secluded into separate virtual domains to minimize security threats. Separate route tables for each virtual switch enables route isolation. Layer 3 Virtual Switching also allows the operator to use overlapping IP address spaces and support multiple communities of interest to share a single physical networking infrastructure.

Hardened Network Infrastructure

Denial of Service Protection

BlackDiamond 12804C 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 eliminates 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

The use of protocols like SSH2, SCP and SNMPv3 supported on the BlackDiamond 12804C switch prevents 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 valid messages and attacking routing sessions.

Automated Attack Mitigation

1. An infected source enters the network.

2. BlackDiamond 12804C static ACLs and CLEAR-Flow rules filter out DoS attacks, determine traffic class as 'suspicious'.

3. Selectively port-mirror traffic to Sentriant for further analysis.

4. Sentriant continues to watch suspicious traffic and uses its internal rules to escalate traffic-class from suspicious to high level alert.

5. Sentriant initiates a dynamic ACL on the BlackDiamond 12804C. BlackDiamond 12804C applies the dynamic ACL in real-time and continues to port mirror suspicious traffic. Sentriant also sends the mitigation action to Extreme Networks' EPICenter network management software.

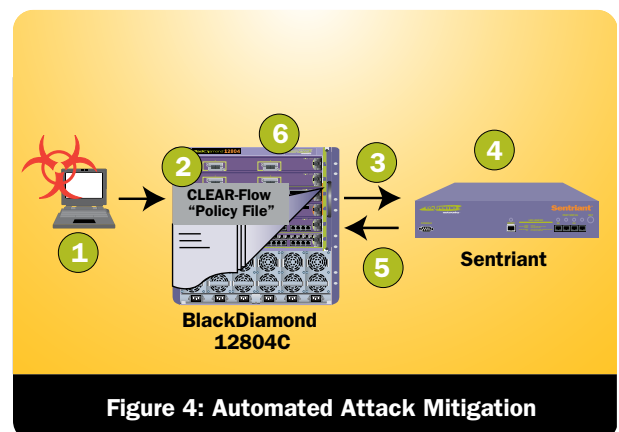6. EPICenter works with core and edge switches to enforce the security policy (mitigation action).

Figure 4: Automated Attack Mitigation

Target Applications

Enterprise Core

The BlackDiamond 12804C provides the small to medium enterprise with an ideal core switch solution that satisfies their complete network needs. The CLEAR-Flow Security Rules Engine and Layer 3 virtual switching capability of the BlackDiamond 12804C have set the bar for core security. The extensibility offered by ExtremeXOS allows the enterprise core to be tightly integrated with best-in-class security products.
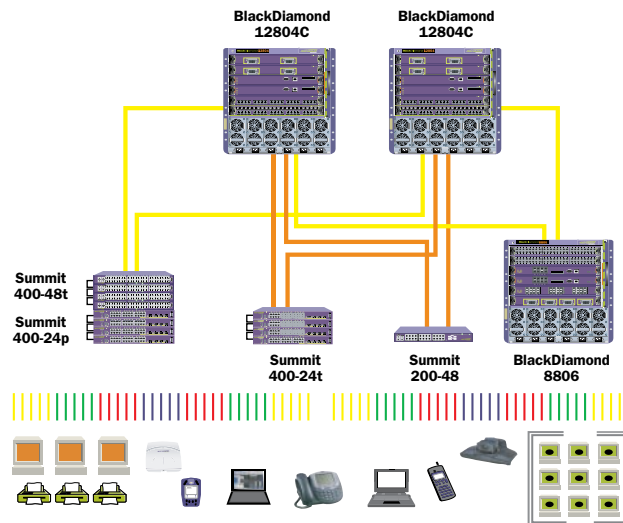
Traditional Aggregation Layer

While Extreme Networks believes that a two-tier network is a simpler approach, the layout of a building or campus wiring plan sometimes requires an aggregation layer. This layer typically aggregates gigabit or 10 gigabit uplinks from edge switches and connects up to the core through gigabit and/or 10 Gigabit Ethernet uplinks. The BlackDiamond 12804C switch addresses the need for high-performance and fault-tolerance connectivity required for the aggregation layer.
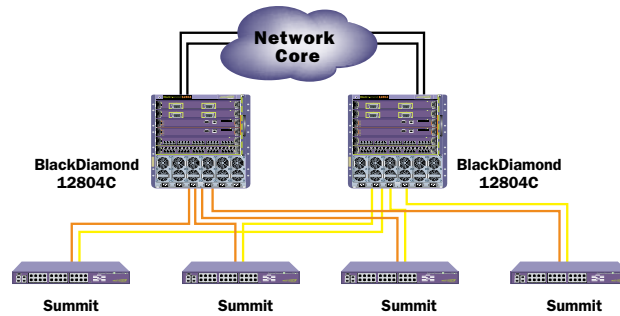
Technical Specifications

ExtremeXOS 11.4 Supported Protocols

General Routing and Switching
- RFC 1812 Requirements for IP Version 4 Routers
- RFC 1519 CIDR
- RFC 1256 IPv4 ICMP Router Discovery (IRDP)
- 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 1866 HTML – Used for webbased Network Login
- RFC 2068 HTTP server – Used for webbased Network Login
- RFC 2338 VRRP
- RFC 3619 Ethernet Automatic Protection Switching (EAPS) and EAPSv2
- IEEE 802.1D – 1998 Spanning Tree Protocol (STP)
- IEEE 802.1w – 2001 Rapid Reconfiguration for STP, RSTP
- IEEE 802.1s – 2004 Multiple Instances of STP, MSTP
- EMISTP, Extreme Multiple Instances of Spanning Tree Protocol
- PVST+, Per VLAN STP (802.1Q interoperable)
- Extreme Standby Router Protocol (ESRP)
- IEEE 802.1Q – 1998 Virtual Bridged Local Area Networks
- IEEE 802.1AB – LLDP Link Layer Discovery Protocol
- Extreme Discovery Protocol (EDP)
- Static Unicast Routes
- Loop detection via Layer 2 ELRP
- Software Redundant Ports

VLANs, vMANs + MAC-in-MAC
- IEEE 802.1Q VLAN Tagging
- IEEE 802.3ad Static load sharing configuration and LACP based dynamic configuration
- IEEE 802.1v: VLAN classification by Protocol and Port
- Port-based VLANs
- Protocol-based VLANs
- Multiple STP domains per VLAN
- Virtual MANs (vMANs)
- IEEE 802.1ah MAC-in-MAC Provider Bridging

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
- Policy-based mapping/overwriting of DiffServ code points. 1.p priority

RIP
- RFC 1058 RIP v1
- RFC 2453 RIP v2

OSPF
- RFC 2328 OSPF v2 (including MD5 authentication)
- RFC 1587 OSPF NSSA Option
- RFC 1765 OSPF Database Overflow
- RFC 2370 OSPF Opaque LSA Option
- RFC 3623 OSPF Graceful Restart

BGP4
- 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 2842 Capabilities Advertisement with BGP-4
- RFC 2918 Route Refresh Capability for BGP-4

IPv4 Multicast
- RFC 1112 IGMP v1
- RFC 2236 IGMP v2
- RFC 3376 IGMP v3
- IGMP v1/v2/v3 Snooping with Configurable Router Registration Forwarding
- IGMP Filters
- Static IGMP Membership
- RFC 2362 PIM-SM
- PIM-DM Draft IETF PIM Dense Mode draft-ietf-idmr-pim-dm-05.txt, draft-ietf-pim-dm-new-v2-04.txt
- RFC 3569, draft-ietf-ssm-arch-06.txt PIM-SSM PIM Source Specific Multicast

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 – 1908 SNMP v2c, SMIv2 and Revised MIB-II
- RFC 2570 – 2575 SNMPv3, user based security, encryption and authentication
- RFC 2576 Coexistence between SNMP Version 1, Version 2 and Version 3
- RFC 1757 RMON 4 groups: Stats, History, Alarms and Events
- RFC 2021 RMON2 (probe configuration)
- RFC 2668 802.3 MAU MIB
- RFC 1643 Ethernet MIB
- RFC 1493 Bridge MIB
- RFC 1354 IPv4 Forwarding Table MIB
- RFC 2737 Entity MIB v2
- RFC 2233 Interface MIB
- RFC 3621 PoE-MIB (BlackDiamond 8800 only)
- RFC 1354 IP Forwarding Table MIB
- RFC 1724 RIPv2 MIB
- RFC 1850 OSPFv2 MIB
- RFC 1657 BGP-4 MIB
- Draft-ietf-idr-bgp4-mibv2-02.txt – Enhanced BGP-4 MIB
- draft-ietf-pim-mib-v2-o1.txt
- RFC 2787 VRRP MIB
- RFC 2925 Ping/Traceroute/NSLOOKUP MIB
- Draft-ietf-bridge-rstpmib-03.txt – Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol
- Secure Shell (SSH-2) client and server
- Secure Copy (SCP-2) client and server
- Secure FTP (SFTP) server
- IEEE 802.1ag L2 Ping and traceroute
- SFlow version 5
- Configuration logging
- Multiple Images, Multiple Configs
- BSD System Logging Protocol (SYSLOG), with Multiple Syslog Servers
- 999 Local Messages (criticals stored across reboots)
- ExtremeWare vendor MIBs (includes FDB, PoE, CPU, Memory MIBs) http://www.extremenet-works.com/services/documentation

Security
- Routing protocol MD5 authentication (see above)
- 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
- 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 for Network Login (all modes)
- Fallback to local database (MAC and Web-based methods)
- Guest VLAN for 802.1x
- SSL/TLS transport – used for for web-based Network Login, (requires export controlled encryption module)
- MAC Address Security – Lockdown and Limit
- RFC 3046 IP Address Security – DHCP Option 82
- IP Address Security – Gratuitous ARP Protection
- Layer 2/3/4 Access Control Lists (ACLs)
- CLEAR-Flow, threshold based alerts and action
- Layer 3 Virtual Switching

Denial of Service Protection
- 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 ratelimiting 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

Technical Specifications

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

IPv6
- Hardware-enabled IPv6
- RFC 2460, Internet Protocol, Version 6 (IPv6) Specification
- RFC 2461, Neighbor Discovery for IP Version 6, (IPv6)
- RFC 2462, IPv6 Stateless Address Auto configuration – Router Requirements
- 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 1981, Path MTU Discovery for IPv6, August 1996 – Router requirements
- RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture
- RFC 3587, Global Unicast Address Format
- RFC 2710, IPv6 Multicast Listener Discovery v1 (MLDv1) Protocol
- RFC 3810, IPv6 Multicast Listener Discovery v2 (MLDv2) Protocol
- RFC 2740, OSPF for IPv6
- RFC 2080, RIPng
- RFC 2893, Configured Tunnels
- RFC 3056, 6to4
- Static Unicast routes for IPv6
- Telnet server over IPv6 transport
- SSH-2 server over IPv6 transport
- Ping over IPv6 transport
- Traceroute over IPv6 transport

General Specifications

Switching Capacity
- 160 Gbps total switching capacity, with 9 microsecond latency for 64-byte packets

MSM and I/O Modules
- MSM-5: MSM modules contain both the control plane as well as the switch fabric for the BlackDiamond 12804.
- GM-20XT: 20-port Gigabit Ethernet module. Each port can be used for 10/100/1000BASE-T or mini-GBIC connectivity (requires mini-GBIC modules)
- GM-20T: 20-port 10/100/1000BASE-T Gigabit Ethernet module (RJ-45)
- XM-2X: 2-port 10G module. XENPAK modules required.

Power Supply Options
Both AC and DC power supplies are available
- AC power supplies can run from 90-264 VAC, and deliver
    - 700W at 90V to 120V, or
    - 1200W at 200V to 240V
- 48V DC power supplies deliver 1200W of power

Physical Specifications

Dimensions
- Chassis: 17.5" high x 17.51" wide x 18.23" deep (44.45 cm x 44.5 cm x 46.3 cm)
- MSM Module Dimensions: 1.63" high x 15.26" wide x 15.25" deep (4.1 cm x 38.8 cm x 38.7 cm)

- I/O Module Dimensions: 1.63" high x 15.26" wide 15.25" deep (4.1 cm x 38.8 cm x 38.7 cm)

Weight
- Empty Chassis: 65 lb (29.5 kg)
- Power Supply: 7 lb (3.2 kg)
- MSM-5 8.5 lb (3.9 kg)
- G20XT 8.5 lb (3.9 kg)
- G20T 7.5 lb (3.4 kg)
- XM-2X 7 lb (3.2 kg)

Power
- Chassis with Fan Trays: 45W, 48V, 1.0A (Heat Dissipation: 154 BTU)
- MSM-5: 185W, 48V, 3.3A (Heat Dissipation: 632 BTU)
- GM-20XT Module: 161W, 48V, 3.5A (Heat Dissipation: 549 BTU)
- GM-20T Module: 149W, 48V, 3.5A (Heat Dissipation: 509 BTU)
- XM-2X Module: 132W, 48V, 2.9A (Heat Dissipation: 450 BTU)

Operating Specifications

- Operating Temperature Range 0°C to 40°C (32 F to 104 F)
- Operating Humidity:10% to 95% relative humidity, non-condensing
- Transportation Temperature:-40°C to 70°C (-40 F to 158 F)
- Storage and Transportation Humidity:10% to 95% relative humidity, non-condensing

Regulatory/Safety Standards

North American Safety of ITE
- UL 60950-1:2003 1st Ed., Listed Device (US)
- CSA 22.2#60950-1-03 1st Ed.(Canada)
- Complies with FCC 21CFR Chapter1, Subchapter J(US Laser Safety)
- CDRH Letter of Approval (US FDA Approval)
- IEEE 802.3af 6-2003 Environment A for PoE Applications

European Safety of ITE
- EN60950-1:2001
- EN 60825-1+A2:2001 (Lasers Safety)
- TUV-R GS Mark by German Notified Body
- 73/23/EEC Low Voltage Directive

International Safety of ITE
- CB Report & Certificate per IEC 60950-1:2001+All Country Deviations
- AS/NZX 3260 (Australia /New Zealand)

EMI/EMC Standards

North America EMC for ITE
- FCC CFR 47 part 15 Class A (USA)
- ICES-003 Class A (Canada)
- European EMC standards
- EN 55022:1998 Class A
- EN 55024:1998 Class A
    - includes IEC 61000-4-2, 3, 4, 5, 6, 8, 11
- EN 61000-3-2,3 (Harmonics & Flicker)
- ETSI EN 300 386:2001 (EMC Telecommunications)
- 89/336/EEC EMC Directive

International EMC Certifications
- CISPR 22:1997 Class A (International Emissions)
- CISPR 24:1997 Class A (International Immunity)
- IEC/EN 61000-4-2 Electrostatic Discharge, 8kV Contact, 15kV Air, Criteria A

- IEC/EN 61000-4-3 Radiated Immunity 10V/m, Criteria A
- IEC/EN 61000-4-4 Transient Burst, 1kV, Criteria A
- IEC/EN 61000-4-5 Surge, 2kV, 4kV, Criteria A
- IEC/EN 61000-4-6 Conducted Immunity, 0.15-80MHz, 10V/m unmod. RMS, Criteria A
- IEC/EN 61000-4-11 Power Dips & Interruptions, >30%, 25 periods, Criteria C

Country Specific
- VCCI Class A (Japan Emissions)
- AS/NZS 3548 ACA (Australia Emissions)
- CNS 13438:1997 Class A (BSMI-Taiwan)
- NOM/NYCE (Mexico)
- MIC Mark, EMC Approval (Korea)

Environmental
- EN/ETSI 300 019-2-1 v2.1.2 - Class 1.2 Storage
- EN/ETSI 300 019-2-2 v2.1.2 - Class 2.3 Transportation
- EN/ETSI 300 019-2-3 v2.1.2 - Class 3.1e Operational
- EN/ETSI 300 753 (1997-10) - Acoustic Noise
- NEBS GR-63 Issue 2 - Sound Pressure
- ASTM D3580 Random Vibration Unpackaged 1.5G

Warranty
- 1-year on Hardware
- 90-days on Software

Ordering Information

Part Number	Name	Description
65040	BlackDiamond 12804 6-slot Chassis	BlackDiamond 12804 6-slot Chassis (includes fan tray and blank front panels)
60020	BlackDiamond 700W/1200W PSU	BlackDiamond 700W/1200W 100-240V PSU
60021	BlackDiamond 1200W DC PSU	BlackDiamond 1200W -48V DC PSU
65010	BlackDiamond 12800 MSM-5	BlackDiamond 12800 Management Switch Module
66010	BlackDiamond 12800 GM-20XT	BlackDiamond 12800 20-port 1000BASE-X SFP / 1000T RJ-45 Module
66030	BlackDiamond 12800 GM-20T	BlackDiamond 12800 20-port 10/100/1000BASE-T (RJ-45) module
66050	BlackDiamond 12800 XM-2X	BlackDiamond 12800 2-port 10G XENPAK Module
41112	BlackDiamond 8800/BlackDiamond 12800 Spare PSU/Fan Controller	BlackDiamond 8800/BlackDiamond 12800 Spare PSU/Fan Controller board
41121	BlackDiamond 8800/BlackDiamond 12800 Spare Blank Panel	BlackDiamond 8800/BlackDiamond 12800 Spare Blank Panel
41151	BlackDiamond 8800/BlackDiamond 12800 Cable Management Clip Kit	BlackDiamond 8800/BlackDiamond 12800 Cable Management Clip Kit
65043	BlackDiamond 8806/BlackDiamond 12804 Spare Fan Tray	BlackDiamond 8806/BlackDiamond 12804 Spare Fan Tray
65046	BlackDiamond 8806/BlackDiamond 12804 Mid Mount Kit	BlackDiamond 8806/BlackDiamond 12804 Mid Mount Kit
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, upto 300m on multi-mode fiber and up to 10km on single-mode fiber, SC connector
10051	SX mini-GBIC	Mini-GBIC, SFP, 1000BASESX, LC Connector
10052	LX mini-GBIC	Mini-GBIC, SFP, 1000BASELX, LC connector
10053	ZX mini-GBIC	Mini-GBIC, SFP, Extra long distance SMF 70 Km/21 dB budget, LC connector

www.extremenetworks.com   **email: info@extremenetworks.com**