BlackDiamond® 6800 Chassis Series

The BlackDiamond 6800—for both large enterprise and carrier networks.

The BlackDiamond 6800 chassis series switches provide world-class Ethernet networks. With the flexibility to act as an aggregation point for a large number of edge switches, its carrier-class reliability and security features, the BlackDiamond 6800 chassis series, provides NEBS Level 3 compliance, in both large enterprise and carrier networks. Additionally, the BlackDiamond 6800 chassis series switches have an extensive offering of interfaces, so your investments in legacy technologies are fully protected. With three sizes of BlackDiamond chassis, a wide range of needs can be met from the edge to the core. All three chassis deliver cutting-edge performance, reliability, and scalability.

Advanced Resiliency for Carrier-Class Performance

- NEBS Level 3 compliance
- Passive backplane supports redundant, load-sharing, hot-swappable switch fabric modules and power supplies
- Hot-swappable I/O modules and fan trays

Industry-Leading Performance

- Wire-speed IP/IPX routing
- Wire-speed switching
- 4,096 IEEE 802.1Q VLANs

Extensive Traffic Management Capabilities

- Policy-based Quality of Service (QoS), including prioritization, bandwidth management and congestion control
- Wire-speed server load balancing, web cache redirection, VLAN switching and routing, DiffServ and IEEE 802.1p

Comprehensive Security Features

- Access Control Lists (ACLs) and access profiles
- RADIUS, SSH2, Network Login

Target Applications

- Highly available network cores and data centers with high density 10/100 and Gigabit Ethernet requirements and 10 Gigabit Ethernet interconnections
- Advanced traffic management for metro revenue-generating, bandwidth-based services

Technical Specifications

BlackDiamond 6800 Series Features

High Availability

The BlackDiamond 6800 series chassis support a passive backplane with redundant load sharing, hot swappable switch fabric modules. The BlackDiamond 6800 modular switching family is configured with an automatic failover mechanism so that if one management switch module (MSM) fails, the second MSM will automatically take over management responsibility for the entire switch. BlackDiamond 6800 can support hitless MSM failover and hitless software upgrades. This feature is critical for both metro and enterprise core networks that run mission-critical applications.

BlackDiamond 6800 series switches are NEBS Level 3 compliant and meet the highest level of quality demanded by network service providers around the world, making it a true carrier class product.

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, digital video feeds don't freeze or pixelize because EAPS enables the network to recover almost transparently from link failure. BlackDiamond 6800 series switches supports Spanning Tree, VLAN Spanning Tree (802.1D), and Rapid Spanning Tree (802.1w) protocols for Layer 2 resiliency. Software-enhanced availability allows users to remain connected to the network even if part of the network infrastructure is down. BlackDiamond 6800 series switches constantly check for problems in the uplink connections using advanced Layer 3 protocols such as OSPF, VRRP and ESRP (ESRP supported in Layer 2 or Layer 3), and dynamically routes around the problem.

Equal Cost Multipath (ECMP) 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 enables trunking of up to eight links on a single logical connection, to provide a single trunk of redundant bandwidth per logical connection.

Extensive Traffic Management Capabilities

Extreme Networks revolutionary rate shaping capabilities provide Layer 3 IP/Ethernet networks that delivers a fixed latency, guaranteed transit path for voice or video traffic equal to that achievable with ATM but at a fraction of the cost and complexity. This makes the implementation of VoIP or VOD or other delay sensitive traffic feasible, without requiring bandwidth over-provisioning.

IETF DiffServ combined with Policy-Based QoS enables classes of services to be defined and enforced end-to-end across the network. Extreme Networks ability to classify packets using Layer 1 through Layer 4 attributes regardless of whether traffic is being switched or routed, combined with the ability to also honor priorities assigned before the traffic entered their network as well as re-write the signaling attributes (i.e. DiffServ), gives service providers unique control of application and service quality. These advanced capabilities ensure high bandwidth management and congestion control.

Providing powerful network visibility, sFlow is a sampling technology that provides the ability to continuously monitor application level traffic flows on all interfaces simultaneously. The sFlow agent is a software process that runs on the BlackDiamond 6800 series switches, and packages data into sFlow datagrams that are sent over the network to an sFlow Collector that has an up-to-the-minute view of traffic across the network. sFlow can be used to troubleshoot network problems, control congestion and to detect network security threats.

Comprehensive Security Features

VMANs allow service providers to securely preserve the integrity of their customers' data while mixing and matching traffic from multiple sources over the same shared backbone. Providing intrusion detection and prevention, BlackDiamond 6800 series switches support line-rate 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.

ACLs are one of the most powerful tools to control network resource utilization and to secure and protect the network. BlackDiamond 6800 series switches support ACLs based on Layer 2, 3 or 4-header information such as the MAC address or IP source/destination address. The use of protocols like SSH2, SCP and SNMPv3 supported by a BlackDiamond 6800 series switch prevents the interception of management communications and man-in-the middle attacks. When a hub or Wireless Access Point (WAP) is attached to a switch running 802.1x, only the first user on the hub or WAP is authenticated; any subsequent users connected to the hub or WAP are allowed to pass unchallenged. Multiple supplicant (client) support on the BlackDiamond 6800 series switches enable multiple clients to be individually authenticated on the same port.

The IPDA SUBNET lookup feature reduces exposure to malicious users or virus infected end clients and accelerates packet forwarding.

BlackDiamond 6800 series switches handle 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.

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' multilayer switching equipment in a converged network. EPICenter Policy Manager provides layer independent policy enforcement for Layers 1 – 4. Extreme Networks' software application, ServiceWatch®, delivers powerful, Layers 4 – 7 monitoring and management for mission-critical network services.

Technical Specifications

ExtremeWare v7.6 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 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 – 2003 Virtual Bridged Local Area Networks
- Extreme Discovery Protocol (EDP)
- Static Unicast Routes
- Extreme Loop Recovery Protocol (ELRP)
- Software Redundant Ports
- IPX RIP/SAP Router specification

VLANs

- IEEE 802.1Q VLAN Tagging
- IEEE 802.3ad Static configuration and dynamic (LACP) for server attached
- IEEE 802.1v: VLAN classification by Protocol and Port
- Port-based VLANs
- MAC-based VLANs
- Protocol-based VLANs
- Multiple STP domains per VLAN
- RFC-3069 VLAN Aggregation for Efficient IP Address Allocation
- Virtual MANs (vMANs)
- VLAN Translation

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
- RED as described in "Random Early Detection Gateways for Congestion Avoidance, Sally Floyd and Van Jacobson"
- RED as recommended in RFC 2309
- Bidirectional Rate Shaping
- Ingress Rate Limiting
- Layer 1-4, Layer 7 (user name) Policy-Based Mapping
- Policy-Based Mapping/Overwriting of DiffServ code points, .1p priority
- Network Login/802.1x and DLCS (Dynamic Link Context System, WINS snooping) based integration with EPICenter Policy Manager for dynamic user/device based policies

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

Note: OSPF Edge License includes 2 active interfaces, router priority 0

IS-IS

- RFC 1142 (ISO 10589), IS-IS protocol
- RFC 1195, Use of OSI IS-IS for routing in TCP/IP and dual environments
- RFC 2104, HMAC: Keyed-Hashing for Message Authentication, IS-IS HMAC-MD5 Authentication
- RFC 2763 (Dynamic Host Name Exchange for IS-IS)

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

IP Multicast

- RFC 2362 PIM-SM
- PIM-DM Draft IETF PIM Dense Mode v2-dm-03
- PIM Snooping
- DVMRP v3 draft IETF DVMRP v3-07
- RFC 1112 IGMP v1
- RFC 2236 IGMP v2
- IGMP Snooping with Configurable Router Registration Forwarding
- IGMP Filters
- Static IGMP Membership
- Static Multicast Routes
- Mtrace, draft-ietf-idmr-traceroute-ipm-07
- Mrinfo

Management and Traffic Analysis

- RFC 2030 SNTP, Simple Network Time Protocol v4
- RFC 1866 HTML – web-based device management and Network Login
- RFC 2068 HTTP server
- 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 1901 – 1908 SNMP Version 2c, 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 2665 Ethernet-Like-MIB
- RFC 1757 RMON 4 groups: Stats, History, Alarms and Events
- RFC 2021 RMON2 (probe configuration)
- RFC 2613 SMON MIB
- RFC 2668 802.3 MAU MIB
- RFC 1643 Ethernet MIB
- RFC 1493 Bridge MIB
- RFC 2737 Entity MIB, Version 2
- RFC 2674 802.1p/802.1Q MIBs
- RFC 1354 IPv4 Forwarding Table MIB
- RFC 2233 Interface MIB
- RFC 2096 IP Forwarding Table MIB
- RFC 1724 RIPv2 MIB
- RFC 1850 OSPFv2 MIB
- RFC 1657 BGPv4 MIB
- 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
- draft-ietf-bridge-8021x-01.txt (IEEE8021-PAE-MIB)
- IEEE 802.1x – 2001 MIB
- Extreme extensions to 802.1x-MIB
- Secure Shell (SSHv2) clients and servers
- Secure Copy (SCPv2) client and server
- Secure FTP (SFTP) server
- sFlow version 5
- NetFlow version 1 export
- Configuration logging
- Multiple Images, Multiple Configs
- BSD System Logging Protocol (SYSLOG), with Multiple Syslog Servers
- Local Messages (criticals stored across reboots)
- IEEE 802.1ab Link Layer Discovery Protocol (LLDP)

ExtremeWare vendor MIBs: Includes ACL, MAC FDB, IP FDB, MAC Address Security, Software Redundant Port, NetFlow, DoS-Protect MIB, QoS policy, Cable Diagnostics, VLAN config, vMAN, VLAN Translation and VLAN Aggregation MIBs

Security

- Routing protocol MD5 authentication (see above)
- Secure Shell (SSHv2),Secure Copy (SCPv2) and SFTP with encryption/authentication
- SNMPv3 user based security, with encryption/authentication (see above)
- RFC 1492 TACACS+
- RFC 2865 RADIUS Authentication
- RFC 2866 RADIUS Accounting
- RFC 3579 RADIUS Support for Extensible Authentication Protocol (EAP)
- RFC 3580 802.1X RADIUS
- RADIUS Per-command Authentication
- MAC based Network Login using RADIUS
- Access Profiles on All Routing Protocols
- Access Profiles on All Management Methods
- Network Login (web-based DHCP/HTTP/RADIUS mechanism)
- RFC 2246 TLS 1.0 + SSL v2/v3 encryption for web-based Network Login
- IEEE 802.1x – 2001 Port-Based Network Access Control for Network Login
- Multiple supplicants for Network Login (web-based and 802.1x modes)
- Guest VLAN for 802.1x
- MAC Address Security – Lockdown, limit and aging
- IP Address Security with DHCP Option 82, DHCP
- Enforce/Duplicate IP Protection via ARP Learning Disable
- Network Address Translation (NAT)
- Layer 2/3/4/7 ACLs
- Source IP Lockdown – Dynamic filtering against invalidly sourced traffic

Technical Specifications

Denial of Service Protection

- RFC 2267 Network Ingress Filtering RPF (Unicast Reverse Path Forwarding) Control via ACLs
- Wire-speed ACLs
- Rate Limiting ACLs
- Rate Shaping by ACLs
- IP Broadcast Forwarding Control
- ICMP and IP-Option Response Control
- Server Load Balancing with Layer 3, 4 Protection of Servers
- SYN attack protection
- FDB table resource protection via IPDA Subnet Lookup
- CPU DOS protection with ACL integration: Identifies packet floods to CPU and sets an ACL automatically, configurable Traffic rate limiting to management CPU/Enhanced DoS Protect
- Unidirectional Session Control

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

Ordering Information

Part Number	Name	Description
50051		BlackDiamond 6804 4-slot chassis (Includes Fan Tray)
50011		BlackDiamond 6808 10-slot chassis (Includes Fan Tray)
53011		BlackDiamond 6816 20-slot chassis (Includes Fan Tray)
50005		BlackDiamond 6800 Series Blank Front Panel
50053		BlackDiamond 6804 Spare Fan Tray
50013		BlackDiamond 6808 Spare Fan Tray
53013		BlackDiamond 6816 Spare Fan Tray
50015	MSM64i	BlackDiamond 6800 64 Gbps Management Switch Fabric Module
50017	MSM-3	BlackDiamond 6800 Management Switch Fabric Module 3
50020		BlackDiamond 6800 iPower Dual-Input 110VAC Power Supply (Includes two L5-20P Power Cords)
50021		BlackDiamond 6800 iPower Single-Input 220VAC Power Supply (Includes L6-20P Power Cord)
50022		BlackDiamond 6800 iPower -48VDC Power Supply
51032	G8Xi	BlackDiamond 6800 8-port 1000BASE-X GBIC Module
51033	G8Ti	BlackDiamond 6800 8-port 100/1000BASE-T RJ-45 Module
51051	G16X[3]	BlackDiamond 6800 16-port 1000BASE-X SFP (mini-GBIC) Module
51052	G24T[3]	BlackDiamond 6800 24-port 10/100/1000BASE-T RJ-45 Module
52011	F48Ti	BlackDiamond 6800 48-port 10/100BASE-TX RJ-45 Module
52012	F96Ti	BlackDiamond 6800 96-port 10/100BASE-TX RJ-21 (Telco) Module
52021	F32Fi	BlackDiamond 6800 32-port 100BASE-FX MMF MT-RJ Module
53041	MPLS	BlackDiamond 6800 Multi-Protocol Label Switching (MPLS) Module
53110	A3cMi	BlackDiamond 6800 4-port OC-3/STM-1 MMF ATM Module
53111	A3cSi	BlackDiamond 6800 4-port OC-3/STM-1 SMF ATM Module
54005	10GX[3]	BlackDiamond 6800 1-port 10GBASE-X XENPAK Module

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

Corporate and North America
Extreme Networks, Inc.
3585 Monroe Street,
Santa Clara, CA 95051 USA
Phone +1 408 579 2800

Europe, Middle East, Africa and South America
Phone +31 30 800 5100

Asia Pacific
Phone +852 2517 1123

Japan
Phone +81 3 5842 4011