

# BlackDiamond® 12804R



*The BlackDiamond 12804R is purpose-built for metro providers to deliver new business and residential services.*

## Features

### High Service Density to Increase Revenue per Subscriber

- Hierarchical Quality of Service (QoS) engine
- vMAN service multiplexing and cross connect
- CLEAR-Flow security engine

### Carrier-Class Scalability to Scale and Manage Networks with Ease

- MAC-in-MAC for Ethernet scaling
- H-VPLS for MPLS scaling
- XML-based service provisioning
- Ethernet ping and traceroute

### Carrier-Class Availability for Quality Subscriber Experience

- Redundant system design
- ExtremeXOS™ modular operating system
- Ethernet Automatic Protection Switching (EAPS) network resiliency protocol

The metro Ethernet market continues to grow, but increased competition and customer churn have metro service providers demanding solutions that increase revenue and lower operational costs. Designed from the ground-up for high service density, the BlackDiamond 12804R enables metro service providers to increase revenue with more subscribers, and more services per subscriber.

BlackDiamond 12804R allows a single Ethernet network to deliver both residential and business services. Residential services include triple play—where each subscriber can be directed to unique content providers for telephony services, IPTV, Internet access, and more. Business services include standard E-Line and E-LAN to connect multiple sites, plus tiered Internet access and VoIP to each business with hierarchical bandwidth and content re-direction controls.

New technology innovations built into the BlackDiamond 12804R make scaling and managing larger networks easy. Services are protected with carrier-class hardware, software, and network protection capabilities.

## Target Applications

- Triple play of Internet access, IP Telephony, IP Television (IPTV), and more to residential subscribers
- Prioritized VPN, Internet access, Voice-over-IP (VoIP) and other applications over E-Line or multi-point E-LAN connections to business customers.
- Aggregating residential triple play and business services on a common platform

*Extreme Networks once again brings key technological innovations to the metro Ethernet market, enabling rich revenue-generating services with carrier-class scalability and availability.*



## High Service Density

Rich bandwidth granularity and service prioritization of the BlackDiamond 12804R enable the triple play of voice, video and data, and more to each residential subscriber. The same Ethernet network delivers point-to-point (E-Line) and multi-point (E-LAN, VPLS) business services for site-site connectivity, tiered Internet access and prioritized Voice-over-IP to each enterprise customer.

### Tiered Bandwidth Control

#### Hierarchical QoS

The hierarchical QoS engine in the BlackDiamond 12804R allows bandwidth limits per service, per subscriber and per port. Thousands of subscribers with varying service requirements can share the same gigabit or 10 gigabit port, enabling scalable residential DSL and cable triple play; subscribers from each DSLAM or CMTS are aggregated into a shared connection to the BlackDiamond 12804R for service control.

A business service example is prioritized E-Line with 2M for bronze, 10M for silver, 20M for gold customers. For each silver customer, the 2M, 10M or 20M can be further allocated based on their application priority. A single gigabit port can have thousands of gold, silver and bronze subscribers.

#### Ingress and Egress Control

The BlackDiamond 12804R supports the Hierarchical QoS (H-QoS) controls for ingress and egress, so bandwidth can be reserved to the subscriber for applications such as video on demand as well as from the subscriber for Peer-to-Peer applications. The controls also allow managing bandwidth to and from other

application and bandwidth providers, extending both the network reach and unique services a metro provider can offer to its subscribers.

### Granular Content Delivery

#### Service Multiplexing

The BlackDiamond 12804R offers multiple services to be multiplexed to each subscriber. DSL and cable subscribers aggregated into a common port can use different Internet Service Providers (ISPs) for Internet access—each subscriber can be routed on a unique vMAN to the respective ISP. Similarly, the video content from the metro provider can be distributed based on unique services purchased by a subscriber.

Traffic from each business customer can be classified by a combination of VLAN, vMAN, Port and Priority fields. This classification is used to map each business customer to unique vMAN and H-QoS settings that maintain the traffic prioritization of each customer over the metro network.

#### vMAN Cross-Connect

vMAN cross-connect allows bridging regional VLANs and vMANs to connect business sites. For a business that uses

different VLANs or vMANs per site, the metro service provider can translate the customer tags between the sites, so the business can leave its internal infrastructure unchanged. This is useful in mergers and acquisitions and other activities that require convergence of multiple networks.

### Advanced Services Engines

The BlackDiamond 12804R is designed from the ground-up to support new revenue-generating services.

#### CLEAR-Flow Security Engine

CLEAR-Flow is a fundamental new approach to detect and block security attacks at 10 gigabit speeds. With the monitoring and programming scale of Extreme Networks fourth generation ASICs, ExtremeXOS and memory architectures, CLEAR-Flow on the BlackDiamond 12804R examines each and every packet, at line-rate, and immediately acts upon rogue traffic, protecting each subscriber and their networks.

## Business Services

- High speed Internet access
- Voice-capable Ethernet-based Internet access service
- Tiered Internet access services with rate limiting
- E-Line services for point-to-point leased line replacement
- E-LAN services for metro TLS replacing Frame Relay and ATM networks
- VPN services over MPLS-based backbone

## Residential Services

- DSLAM and CMTS aggregation for residential triple play
- High speed Internet access
- Bandwidth-based Internet access services
- Local Voice
- Long Distance Voice
- IP TV Multi-cast
- HDTV
- Uni-cast video on demand
- Network-hosted digital video recording

## Single Physical Network

*Highly Available, Resilient, Scalable, Virtualized*

## Carrier-Class Scalability

Service providers now need solutions that allow them to support larger number of residential and business users spread over multiple sites and using a variety of applications, all on the same network. The BlackDiamond 12804R delivers new technology innovations to scale and manage large networks with ease.

### Network Scaling

#### vMAN Scaling

By allowing overlapping VLANs in a network, vMANs enable metro providers to scale to a large number of customers. The vMAN technology alone, however, does not reduce the number of MAC addresses each switch must support. Further, even with vMAN, each traditional Ethernet switch can still only support 4,000 vMANs, a constraint as metro Ethernet networks scale to bigger deployments.

#### vMAN Peering

vMAN translation on Network-to-Network Interface (NNI) ports combined with H-QoS allows the BlackDiamond 12804R to peer with other network and application providers and extend network reach. Traffic to and from each peer can be controlled per vMAN and per class of service.

#### MAC-in-MAC

The MAC-in-MAC protocol, based on the emerging IEEE 802.1ah standard, allows the metro provider to scale the network with Ethernet technology, maintaining management and operational simplicity and lower costs. MAC-in-MAC encapsulates vMAN traffic into an additional Ethernet header for routing within the

core. Therefore, core Ethernet switches only need to learn the MAC addresses of edge switches that are directly connected to the core, and not the MAC addresses inside the customer VLANs. MAC-in-MAC also provides a higher number of vMAN instances for scaling to more subscribers.

#### MPLS Scaling

A metro provider can map each vMAN to a unique MPLS tunnel. By taking advantage of the Layer 2 traffic per customer and the hierarchical hub-and-spoke connectivity at the MPLS edge, H-VPLS provides a scaleable approach to build an MPLS core.

#### Multicast Scaling

The BlackDiamond 12804R delivers multicast performance to thousands of concurrent multicast streams. The switch fabric uses multiple references to a packet's memory, avoiding multiple packet copies. This design enables efficient replication of multicast traffic for applications such as video distribution.

### Service Provisioning

#### Policy Templates

The use of policy files on the BlackDiamond 12804R allows simpler management of large number of subscribers and services.

#### Secured Access

Beyond the flexible CLI support, protocols such as SSH2, SCP and SNMPv3 prevent the interception of management communications and man-in-the-middle attacks.

#### XML Interface

In addition to CLI and SNMP, BlackDiamond 12804R enables a metro provider to build a rich service-aware OSS by leveraging XML. The XML interface allows easier integration and scales to a large number of subscriber and service configurations.

### Service Diagnostics

BlackDiamond 12804R supports a full range of fault-management capabilities to quickly detect service failure in large networks. Beyond standard Layer 3 features such as SNMP traps, IP ping and traceroute, the Layer 2 connectivity fault management tools being standardized with IEEE 802.1ag are also supported. These tools offer Layer 2 ping, traceroute, and continuity checks, so any link or switch failure can be quickly detected and corrected.



## Carrier-Class Availability

With increasing applications supported by a service provider, any network downtime means lost revenue and increased customer dissatisfaction. BlackDiamond 12804R offers comprehensive high-availability with resilient hardware, modular software, and protection switching features, providing a high-quality customer experience.

### Redundant Hardware Design

#### Advanced System Design

BlackDiamond 12804R uses a passive backplane complemented by high availability design elements such as isolated control and data planes, hardware-based traffic monitoring, redundant controller boards for power distribution, and redundant fan control and environmental monitoring to identify anomalies before they effect network availability. Resiliency is integral to each component including memory where ECC technology is used to automatically correct memory errors. Optimized multicast replication, large packet buffers for traffic bursts and large address tables for subscriber scale further maintain service availability and performance with a varying traffic mix.

#### Redundant Management and Switching Modules

In the rare case of component failures, redundant Management Switch Module (MSM) blades on the BlackDiamond 12804R provide high availability. The MSMs operate in a 1:1 (primary:standby) redundant configuration. If the primary MSM fails, the standby MSM assumes the primary role and supports the full load of all I/O modules.

#### Redundant Power Supplies

BlackDiamond 12804R 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 N + N configuration to provide input power redundancy for a fully loaded chassis.

### Modular ExtremeXOS Software

#### Hitless Software Upgrade

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

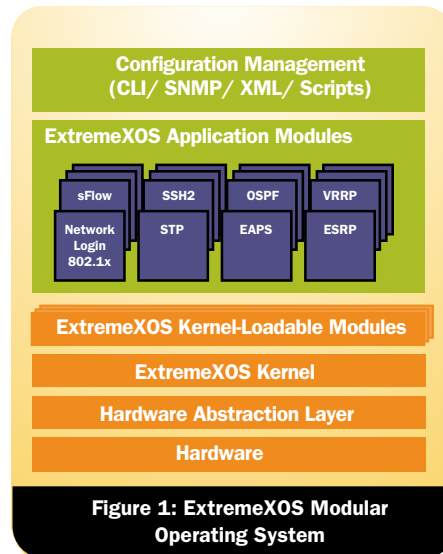


Figure 1: ExtremeXOS Modular Operating System

#### True Preemptive Multitasking and Protected Memory

BlackDiamond 12804R allows each of the many tasks—such as Open Shortest Path First (OSPF) and Spanning Tree—to run as separate operating-system processes that are protected from each other as shown in Figure 1.

#### Process Monitoring and Restart

ExtremeXOS dramatically increases network availability by monitoring independent operating system processes in real time. If any of the processes 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 operating system image and restarting the switch. New functionality can be added to the switch on the fly.

### Network Resiliency Protocols

#### Ethernet Automatic Protection Switching (EAPS)

EAPS allows the IP network to provide the level of resiliency and uptime that users expect from their traditional SONET networks. EAPS is superior to the Spanning Tree or Rapid Spanning Tree protocols, offering sub-second (less than 50 milliseconds) recovery.

#### Spanning Tree/Rapid Spanning Tree Protocols

BlackDiamond 12804R supports Spanning Tree, VLAN Spanning Tree, Rapid Spanning Tree (IEEE 802.1w), and Multiple Spanning Trees (IEEE 802.1s) protocols for Layer 2 resiliency.

#### Layer 3 Routing and Redundancy Protocols

BlackDiamond 12804R supports a comprehensive range of routing protocols including BGP and OSPF, with graceful restart extensions to avoid route flapping and improve network uptime. Redundancy protocols including VRRP and ESRP allow dynamic routing around individual switch or server downtime at Layer 2 or Layer 3.

#### Equal Cost Multipath

Equal Cost Multipath allows 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 grouping of multiple links on a single logical connection (called a trunk). When one link in a trunk fails, traffic is routed to the remaining links in the trunk.





# 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
- draft-ietf-idr-restart-10.txt (Graceful Restart Mechanism for BGP)

### 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
- Multicast VLAN Registration
- 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 SNMP, 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.extremenetworks.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-5R: MSM modules contain both the control plane as well as the switch fabric for the BlackDiamond 12804.
- GM-20XTR: 20-port Gigabit Ethernet module. Each port can be used for 10/100/1000BASE-T or mini-GBIC connectivity (requires mini-GBIC modules)
- XM-2XR: 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 x 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-5R 8.75 lb (4.0 kg)
- G20XTR 8.5 lb (3.9 kg)
- XM-2XR 7.25 lb (3.3 kg)

### Power

- Chassis with Fan Trays: 45W, 48V, 1.0A (Heat Dissipation: 154 BTU)
- MSM-5R: 200W, 48V, 3.3A (Heat Dissipation: 683 BTU)
- GM-20XTR Module: 169W, 48V, 3.5A (Heat Dissipation: 577 BTU)
- XM-2XR Module: 150W, 48V, 2.9A (Heat Dissipation: 512 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

### BlackDiamond 12804R

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 AC PSU
60021	BlackDiamond 1200W -48V DC PSU	BlackDiamond 1200W -48V DC PSU
65011	BlackDiamond 12800 MSM-5R	BlackDiamond 12800 Management Switch Module w/ Rate Limiting
66011	BlackDiamond 12800 GM-20XTR	BlackDiamond 12800 20-port 1000BASE-X SFP/1000T Module with Rate Limiting
66051	BlackDiamond 12800 XM-2XR	BlackDiamond 12800 2-port 10G XENPAK Module with Rate Limiting
67010	BlackDiamond 12800 MPLS Feature Pack	BlackDiamond 12800 ExtremeXOS MPLS Feature Pack
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](http://www.extremenetworks.com)

email: [info@extremenetworks.com](mailto: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

© 2006 Extreme Networks, Inc. All rights reserved. Extreme Networks Confidential and Proprietary.  
 Extreme Networks, the Extreme Networks Logo, BlackDiamond and ExtremeXOS are either registered trademarks or trademarks of Extreme Networks, Inc. in the United States and/or other countries.  
 Specifications are subject to change without notice.