

ExtremeXOS



ExtremeXOS®—a highly available, open and extensible foundation for converged networks.

High Availability Architecture

- Reduce network downtime using hitless failover/upgrade and module level software upgrade
- Prevent system corruption using a memory-protected process model
- Avoid system reboots using self-healing process recovery

Extensible Functionality

- Integrate best-of-breed applications to your network with an open, yet secure XML-based Application Programming Interface (API)
- Integrate Extreme Networks® and third party-developed software applications using an open standards-based POSIX interface
- Extend network functionality and automate management tasks using CLI scripting and Universal Port

Data Center

- Provide insight, control and automation for highly virtualized data centers to the network
- Supports Direct Attach™, which eliminates the virtual switch layer, simplifying the network and improving performance
- Supports Data Center Bridging Capabilities such as Priority Flow Control (PFC) and Enhanced Transmission Selection (ETS)

Extreme Networks has revolutionized the industry by creating ExtremeXOS—a highly available and extensible foundation for converged networks. ExtremeXOS raises the bar for availability, critical for offering carrier-grade voice and video services over IP and to support mission-critical business applications such as CRM. A more available network can also help to lower operational costs by drastically reducing emergency maintenance.

ExtremeXOS allows you to extend the capabilities of your network. It allows you to integrate specialized application appliances such as security devices into your network.

ExtremeXOS has been designed from the ground up to support the next-generation Internet Protocol, IPv6. Even if you are not planning to use IPv6 immediately, ExtremeXOS will secure the network using IPv6 Access Control Lists and provide investment protection for your network.

Security capabilities provide network access control integrated with endpoint integrity checking, and network control and management plane protection. Its innovative Universal Port framework provides dynamic security policies for users as well as auto-configuration of ports and VoIP phones.

ExtremeXOS has been deployed in production networks for over five years, making it the only next generation operating system in the industry that can be safely deployed without “early adopter” risks, and that spans a complete product line from value edge to core Carrier Ethernet.



High Availability Architecture

ExtremeXOS creates a highly available network for voice services and other mission-critical business applications.

Preemptive multitasking and protected memory allow each of many processes—such as resiliency or device management protocols—to run as separate Operating System (OS) processes that are protected from each other.

With process monitoring and restart, ExtremeXOS dramatically increases network availability. Each independent OS process is monitored in real time. If a process becomes unresponsive, actions can be taken such as hitless failover or automatic process restart.

Hitless failover to the redundant management module is available on the BlackDiamond® 8800 series, the BlackDiamond 10808, the BlackDiamond 12804 and the BlackDiamond 20808. In addition, the BlackDiamond 10808, the BlackDiamond 12804 and the BlackDiamond 20808 are capable of hitless upgrade of the OS.

ExtremeXOS also provides the capability of upgrading individual parts of the OS (modules). As an example, upgrading the SSH application will not impact data forwarding.

Multi-Switch LAG (Link Aggregation Groups) can address bandwidth limitations and improve network resiliency, in part by routing network traffic around bottlenecks, reducing the risks of a single point of failure, and allowing load balancing across multiple switches.

Extensible Functionality

ExtremeXOS allows for flexible expansion of network capabilities by providing a means for third-party applications in the network to interact directly with the OS. If you need to extend your network to handle other applications or integrate monitoring software or security devices, ExtremeXOS integrates best-of-breed

solutions with an open yet secure XML-based API. For example, this extensibility allows integration with third-party applications such as security appliances, service provisioning software, and VoIP monitoring solutions to provide a closed loop for new monitoring and response capabilities. It also serves as a framework for integration with management software such as service provisioning solutions.

With its innovative dynamic software loading capability, additional applications can be loaded, started and stopped without impacting traffic forwarding or management of the network. This allows partners of Extreme Networks to provide specific extensions such as VoIP call quality monitoring.

ExtremeXOS offers CLI scripting to allow you to automate regular management tasks and apply them to multiple ports or easily replicate on multiple switches.

Integrated Security

ExtremeXOS guards access to the network through authentication, host integrity checking and dynamic user/time/location-based security policies. It hardens the network infrastructure with Denial of Service (DoS) protection and IP Security to protect the infrastructure, network services, applications and client devices/computers from man-in-the-middle attacks and eavesdropping. It also provides a full suite of secure management protocols using authentication and encryption, ensuring continued control over your infrastructure.

ExtremeXOS Network Login dramatically eases the rollout of user authentication solutions and activation on every port, including device ports such as for printers or VoIP phones, as it offers a choice of 802.1x, Web-based and MAC-based authentication. Host computers without 802.1x support can use Web-based authentication to log into the network or receive limited network access to install 802.1x.

ExtremeXOS IP Security framework protects the network infrastructure, network services such as DHCP and DNS

and even host computers from spoofing and man-in-the-middle attacks. It also provides network protection from statically configured and/or spoofed IP addresses as well as building an external trusted database of MAC/IP/port bindings so that you always know where traffic comes from for immediate defense.

Identity Management allows network managers to track users who access their network. User identity is captured based on NetLogin authentication, LLDP discovery and Kerberos snooping. ExtremeXOS uses the information to then report on the MAC, VLAN, computer hostname, and port location of the user.

Data Center

Data center managers face unique challenges, such as virtual machine mobility and security. ExtremeXOS supports multiple capabilities and features to support this ever-evolving environment.

XNV™ (ExtremeXOS Network Virtualization) is a set of licensable software modules for both the ExtremeXOS based switching product portfolio, as well as for EPICenter®, a network provisioning and management application. XNV brings insight, control and automation for highly virtualized data centers to the network.

ExtremeXOS also supports Direct Attach, which eliminates the virtual switch layer, simplifying the network and improving performance. Direct Attach enables data center simplification by reducing network tiers from 4 or 5 tiers to just 3 or 2 tiers, depending on the size of the data center.

Priority-based Flow Control (PFC), or IEEE 802.1Qbb, allows network traffic to be controlled independently based on Class of Service. PFC allows network traffic that requires lossless throughput to be prioritized, while other traffic types that do not require or perform better without PFC can continue as normal.



www.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 +65 6836 5437

Japan
Phone +81 3 5842 4011