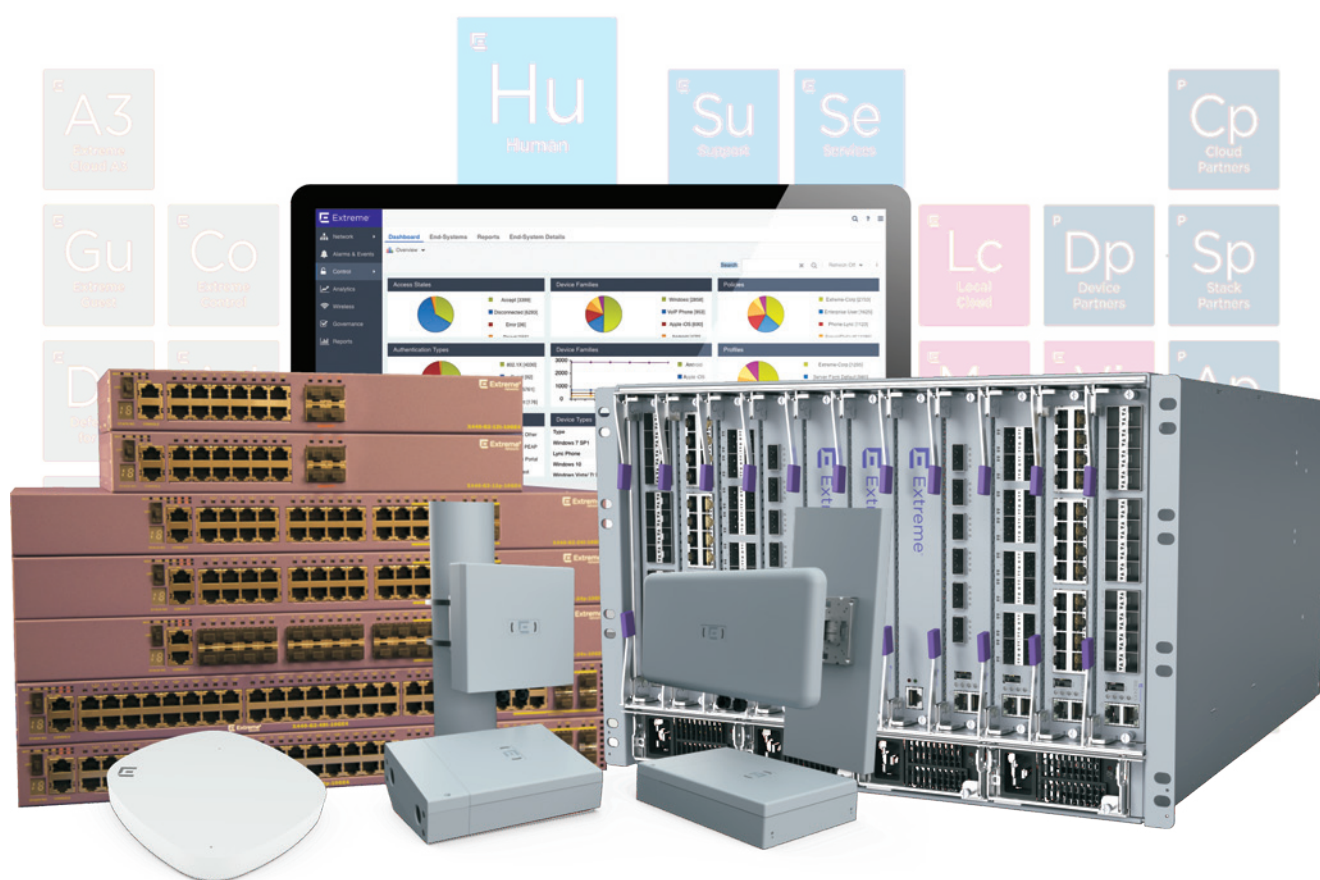# NETWORK SOLUTIONS

Extreme Networks Solutions from Professionals

IT-Union GmbH & Co. KG

BUSINESS IT-SOLUTIONS

Warum IT-Union

- **Managed Service & 24x7 Support**

- **Seit 1997 Partner von Extreme Networks**

- **15+ zertifizierte System-Ingenieure (ECE)**

- **Schnelle Reaktionszeiten & hohe Flexibilität**

- **25+ Jahre Erfahrung & tiefgreifendes Know-how**

Nutzen Sie unser Wissen und unsere Erfahrung

Die Mitglieder der IT-Union GmbH & Co. KG gehören zu den ältesten und höchst zertifizierten Extreme Networks Partnern in Deutschland. Seit 1997 beraten, installieren und betreuen wir Netzwerke mit Produkten und Lösungen dieses Herstellers. Die IT-Union unterstützt Sie u. a. mit 15 zertifizierten System-Ingenieuren (ECE) kompetent und branchenübergreifend in Projekten mit unterschiedlichster Größenordnung und Komplexität. Das Servicecenter unserer Gruppe bietet Ihnen hierbei individuelle Konzepte inkl. 24x7 Service, flankiert durch ein eigenes Servicelager Die IT-Union ist Mitglied im globalen Extreme Networks Partner Advisory Council (Global PAC).

IT-Union

Die IT-Union GmbH & Co. KG (ITU) wurde 2008 als Systemhausverbund gegründet und ist eine gemeinsames Tochterunternehmen von den Gesellschaftern BMAnetworks (Hamburg), GORDION (Troisdorf) und INDASYS (Stuttgart) und VINTIN (Schweinfurt). Mit weiteren Büros in Kiel, Fulda und Malters (CH) verfügt die ITU derzeit über sieben Standorte. Die ITU betreut branchenübergreifend Kunden, von Enterprise bis Carrier, und bietet Lösungen mit Fokus auf die Themen:

- **Analyzing**

- **Outsourcing**

- **IT-Sicherheit**

- **Datennetzwerktechnik**

- **Managed- / Cloud-Services**

- **Triple-Play Metronetzwerke**

IT-UNION – SECURE NETWORKS

Die Mitglieder der IT-Union sind bereits seit den frühen 90er Jahren am Markt und verfügen allesamt über ein tiefes Know-how im Bereich der IT. Durch die langjährige Erfahrung unserer Spezialisten in Kombination mit einem überregionalen sowie flexiblen Service- und Support ist die ITU ein idealer Partner rund um das Thema IT – sowohl für öffentliche Auftraggeber und Organisationen, als auch für Unternehmen in jeglicher Größe.

IT (●) UNION

BMA networks   **GORDION.**   **indasys** connectivity   **VINTIN** make IT unique

Unser Fokus

Wir bieten Ihnen langjährige Erfahrung, tiefgreifendes Know-how und hohe Flexibilität, insbesondere zu folgenden Schwerpunkt-Themen:

Datennetzwerktechnik

- Wireless LAN
- Loadbalancing
- WLAN Suite Survey
- IPv4 zu IPv6 Migration
- Triple Play – Metronetze
- Analysen für LAN / WLAN
- Routing, VPN, u.v.m. – WAN
- Server, Storage, Virtualisierung
- RZ-Infrastruktur, Switching, u.v.m. – LAN

IT-Sicherheit und Datenschutz

- Sandboxing
- VPN, SSL, SD-WAN
- Datenschutzconsulting
- Email-, Web- und IoT-Security
- SSO, Authentifizierung, NAC
- Firewalling, Content Security, u.v.m.
- Security Information & Event Mgmt. (SIEM)

Outsourcing, Managed / Cloud-Services

- BPO, Outtasking
- Training und Zertifizierungen
- Systemadministration, Monitoring, u.v.m.
- 24x7-Services (SLA, Spare Parts, u.v.m.)
- Hybride Infrastrukturen u.a. AWS und Azure

NORD

Kiel
BMAnetworks GmbH
Preetzer Chaussee 55
24222 Schwentinental

Telefon 0431 97449 0
Email   vertrieb.ki@it-union.eu

Hamburg
BMAnetworks GmbH
Albert-Einstein-Ring 5
Arelia-Haus, 22761 Hamburg

Telefon 0431 97449 0
Email   vertrieb.hh@it-union.eu

MITTE

Köln
GORDION
Data Systems Technology GmbH
Mottmannstraße 13
53842 Troisdorf

Telefon 02241 4904 0
Email   vertrieb.kln@it-union.eu

Schweinfurt
VINTIN GmbH
Felix-Wankel-Straße 4
97526 Sennfeld

Telefon 09721 67594 10
Email   vertrieb.sw@it-union.eu

Fulda
VINTIN GmbH
Rangstraße 39
36043 Fulda

Telefon 0661 2503859 0
Email   vertrieb.fd@it-union.eu

SÜD

Stuttgart
indasys connectivity GmbH
Leitzstraße 4c
70469 Stuttgart

Telefon 0711 896659 115
Email   vertrieb.st@it-union.eu

CH

Malters
VINTIN GmbH
Bahnhofstrasse 7
CH-6102 Malters

Telefon +41 41 5600067
Email   vertrieb.ch@it-union.eu

Contents

Customer-Driven Networking

Since 1996, Extreme Networks has been pushing the boundaries of networking technology, driven by a vision of making it simpler and faster as well as more agile and secure. But our higher purpose has always been helping our customers connect beyond the network… strengthening their relationships with those they serve. Today, we call that Customer-Driven Networking.

From global enterprises and high-profile sports leagues, to small towns and college campuses, Extreme customers all have one thing in common: unmatched agility thanks to a network that helps them digitally transform the way they operate.

EXTREME AT-A-GLANCE
- NASDAQ: EXTR
- Founded in 1996
- Headquartered in San Jose, CA
- 3,000+ employees worldwide
- 50.000+ global customers
- 9.000+ technology partners
- 100% insourced service & support
- Industry's first 1G/10G Switch

OUR TECHNOLOGIES
- Management and automation
- Analytics and visibility
- Security and access control
- ExtremeSwitching
- ExtremeRouting
- ExtremeWireless

Anything is Possible with the Right Combination of Elements

Complete software, hardware, and human solutions

Extreme Networks Solutions

Automated Campus Enterprise Solutions

The enterprise campus has become one of the most vexing environments in which to manage IT. You need to rapidly onboard BYOD users and Internet connected devices, quickly deploy the new digital technology that your organization requires, prevent cyber-attacks at every entry point, and do it all while delivering a consistent and personalized user experience. Extreme's Automated Campus solution makes it all possible with simplicity, security, and intelligence that are second to none.

Extreme's Automated Campus uses **simple policy-driven automation** to enable networking teams to be more responsive, reduce operations costs and increase their ability to innovate.
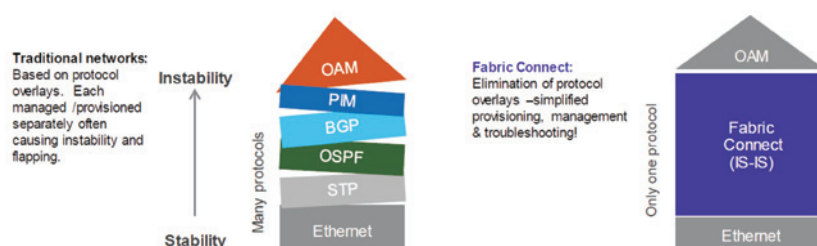
Consists of: Fabric Connect (and Fabric Attach) with NAC / Policy / Application Analytics and Management

Products: VSP, ERS and EXOS switches with Extreme Wireless Solutions and Extreme Management Center (ExtremeControl, ExtremeAnalytics, ExtremeManagement and IGE)

Fabric Connect: Technology at a Glance

- Based on an enhanced form of the IEEE/ IETF standard Shortest Path Bridging.
- Leverages carrier grade IS-IS (routing protocol) as the L2/L3 control plane.
- Defines a next generation VLAN called an ISID (Independent Service Identifier)
- I-SID is added at the edge of the network, therefore, standards-based Ethernet hardware 5-6 years old can reside in the network core. Doesn't need to be Extreme end to end!

Fabric Connect enables dramatic simplification of today's rigid and complex networks

Ethernet Fabrics

Compared to classic hierarchical Ethernet architectures, Ethernet fabrics provide higher levels of performance, utilization, availability, and simplicity. They have the following characteristics at a minimum:

- **Flatter:** Ethernet fabrics eliminate the need for STP, while still being completely interoperable with existing Ethernet networks.

- **Flexibility:** Can be architected in any topology to best meet the needs of any variety of workloads.

- **Resiliency:** Multiple "least cost" paths are used for high performance and high reliability.

- **Elasticity:** Easily scales up and down at need.

More advanced Ethernet fabrics have innovated more aggressively in the control and management spheres.

- They are self-forming and function as a single logical entity, in which all switches automatically know about each other and all connected physical and logical devices.

- Management can then be domainbased rather than device-based and defined by policy rather than repetitive procedures.

- These features, along with virtualization-specific enhancements, make it easier to explicitly address the challenges of VM automation within the network, thereby facilitating better IT automation.

Fabric Connect Benefits

A completely new way to build networks, Extreme Fabric Connect delivers a simplified, agile and resilient infrastructure that makes network configuration and deployment of new services faster and easier. A standards-based network virtualization technology based on an enhanced implementation of IEEE 802.1aq Shortest Path Bridging and IETF RFC 6329, Extreme Fabric Connect combines decades of experience to deliver a next-generation technology that combines the best of Ethernet with the best of IP. Extreme Fabric Connect creates a multi-path Ethernet network that leverages IS-IS routing to dynamically build a topology between nodes. Traffic always takes the shortest, most efficient path from source to destination, guaranteeing optimal performance and failover.

- Eliminating Complexity: From 10+ Protocols to 1
- Faster Time-to-Service: 11x Better with Edge-Only Provisioning
- Better Time-to-Repair: Eliminating Hop-by- Hop Gives 6.5x Improvement
- Enhanced Business Continuity: 13 Minutes to 320 Milliseconds
- Invisible Core: Simplified Security
- Automated IoT: Plug and Play through Elastic Networks
- Multicast Made Easy: 28x Scalability
- Resource Efficient: 1/10th of the Resources, 1/10th of the Time
- Workflow Automation: Accelerating Business Outcomes
- Flexible network topologies: Fabric Connect can run over any physical topology
  whether it be rings, full mesh, partial mesh, or any combination

Fabric Attach Benefits

Extreme Fabric Attach works in conjunction with a Fabric Connect network to deliver network services automation and dynamic auto-attach. Specifically, Fabric Attach enables non-fabric devices, whether end points, edge switches or APs, to participate in the fabric in order to provide auto-attach of users and devices into the assigned fabric-based services.

- Automation: Fabric Attach delivers automation to network provisioning, attachment and control without complex centralized programming of legacy protocols.
- Reduced administration: Fabric Attach can provide huge IT opex savings with adds moves and changes.
- Scalability: Fabric Attach provides additional scalability for Fabric Connect cores by providing the same service attachment function without participating as an SPB node.
- Elasticity: The entire network becomes a truly elastic resource where services only exist while people or devices are connected and using business applications.

Agile Data Center Solutions

Challenges in the Data Center (The Problem)

A rapidly changing global economy means that enterprises need to respond to shifting market dynamics, competitive threats, and customer demands quickly. Most organizations have recognized the need to become more agile and have embraced new digital and IT transformation initiatives and DevOps principles. These initiatives are all focused on rethinking how they architect and operate their IT infrastructure to enable faster time to market, competitive advantage, and higher quality customer experiences.

As a result, in the data center – where it stores, manages, and disseminates data, the network must provide the requisite connectivity and services for an ever-changing and always-on environment when and where it is needed. To provide that level of agility and enable new sources of digital revenue, organizations need to implement greater levels of network automation, visibility, and device programmability. Automation promises to reduce time to value and create greater operational agility. Since it is difficult to automate what is not understood, organizations will require deeper visibility into their networks to intelligently automate changes with context.

Data Center Networks Must Enable – Enterprises to obtaining the business outcome of digital transformation with a flexible, vendor interoperable architectures offering simple automation, visibility and valuable analytics. This will significantly reduce difficulties and delays provisioning and troubleshooting network services and devices, work within budget constraints, improve network performance, decrease complexity and leverage current cloud trends.

Data Center Markets and Use Cases Must – Span all vertical markets and address customers of any size. Common use cases include general purpose networks, IP Storage, Big Data (Hadoop), High Performance Computing and Data Backup.

Delivering Features and Benefits With Extreme Solutions

Helping customers consider, select, and deploy data center network solutions for current and planned needs is top priority. Using repeatable reference network architectures that have been engineered and tested to address specific use cases and deployment scenarios provide the blueprints by which data centers are built. Solutions centered around IP Fabrics both within the data center and inter-connecting data centers are core building blocks for enterprises.

Data Center IP Fabric solutions facilitate server & services connectivity within the data center supporting Layer 2 and Layer 3 networks. The flagship solution includes SLX switches and routers for spine, leaf and border leaf architectures and can be deployed flexibly in an IP Fabric of any scale. IP Fabric solutions leverage a BGP underlay with an EVPN overlay using VXLAN to provide simplicity, interoperability, and scale-out capabilities in the data center. This allows customers to build networks of any size without having to constantly re-tool the network. Key highlights of the solution include:

- Industry Standard BGP underlay with EVPN overlay supporting vendor interoperability
- Embedded Automation for Plug-n-Play IP Fabric provisioning
- Spine/Leaf Architecture – Scalable deployments from small to 1000's of switches per fabric
- Insight Architecture with On-board Guest VM for network visibility and other value-added capabilities
- Extreme Management Center providing a Single Pane of Glass into the end-to-end network, including the Data Center

Data Center Interconnect (DCI) solutions deliver extension of Layer 2 and/or Layer 3 networks across multiple data centers over any existing IP/WAN. The flagship offering includes SLX switching and routing platforms providing virtual tunnel endpoint (VTEP) high availability and redundancy across a WAN. Ideally, a DCI solution supports BGP for the underlay and BGP-EVPN for the overlay with VXLAN – the same exact technologies as the data center IP Fabric. There are no dependencies on the existing data center infrastructure or IP/WAN, making it simple to drop in the solution without disrupting the existing environment. Key highlights of the solution include:

- Seamless Extension, supporting Layer 2 and/or Layer 3
- Flexible Interoperability working with any data center and WAN
- Logical VTEP for Built-in High Availability
- Insight Architecture with On-board Guest VM for network visibility
- Extreme Management Center providing a Single Pane of Glass into the end-to-end network, including the Data Center Interconnect
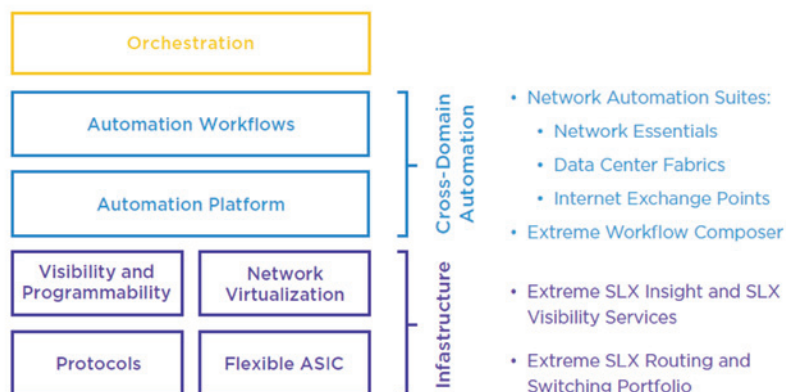
Extreme's Agile Data Center Value

Automation – Improve and accelerate IT agility with options to automate at your pace. From simple embedded automation for Day-0 provisioning to customizable solutions from Extreme or 3rd parties such as Ansible, up to full cross domain IT automation with Extreme Workflow Composer.

Visibility – Network visibility from wire to workload deliver pervasive real-time monitoring and intelligent automated actions leveraging the guest VM capabilities. Integration with Extreme Analytics will give a deeper look into application telemetry with valuable and timely information regarding what is going across the data center networks.

Adaptability – Delivers agility at all layers of the data center stack with programmable ASICs in the hardware, open APIs for interoperability and future proof designs adaptable to emerging speeds, standards, and protocols. Design it once with the ability to future proof and easily adjust to meet business requirements without a rip and replace of hardware.

Better financing options and services get you up and running quicker, keep your network optimized, and prevent outages. Extreme Capital Solutions provide the financing options that best fit your needs. Our services can provide 24/7 operation support, including maintenance, professional services, and training. Our support center (GTAC) provides technical support 24 hours a day, 365 days a year. SupportNet offerings let you choose the exact level of service ideal for your organization.

Extreme Agile Data Center ensures agility at all layers of the data center stack
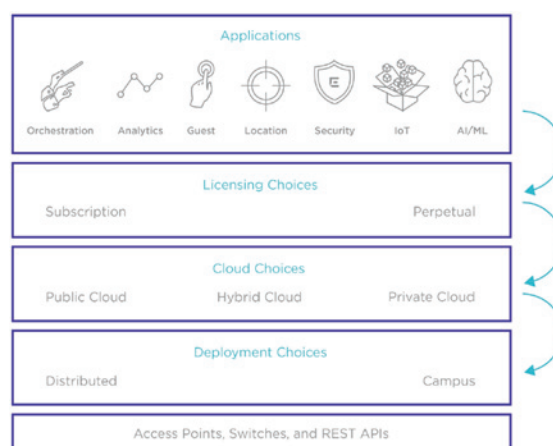
Smart OmniEdge Enterprise Solutions

The network edge is where digital transformation is won or lost. It's where your organization engages customers, where mobile transactions occur, where IoT devices connect, and where you make the first stand against cyber threats. Extreme's Smart OmniEdge network solution provides a unified wired/ wireless infrastructure for cloud or premise deployment, augmented with AI-powered applications and managed through a single pane of glass. The result? A network that delivers a consistent customer-driven experience, contains costs, and enables competitive advantage through innovation and rapid new service delivery.

Smart OmniEdge Framework

The framework for Smart OmniEdge is a unique set of architectural, strategic, product and service offerings that enable unprecedented intelligence, security, and adaptability for Enterprises. It comprises a secure, unified wired and wireless infrastructure, managed through a single pane of glass and complemented by a broad portfolio of applications.

New technologies being introduced as part of the Extreme Networks' Smart OmniEdge launch are designed specifically to enhance the edge network experience, and include:

- **ExtremeAI for Smart OmniEdge**
  Provides customers technological advances in Wi-Fi RF management that save time, effort and money, while improving the user experience.

- **ExtremeCloud Appliance**
  Designed for customers who love the simplicity of ExtremeCloud and want an on-premise solution, ExtremeCloud Appliance delivers cloud-like simplicity, management with tightly integrated services and features on-premise deployments require, complemented with simplified licensing. ExtremeCloud Appliance is also available as a virtual machine (VM) for customers that have their own private cloud services.

- **Extreme Extended Edge Switching**
  Delivers an innovative technology that collapses multiple network layers into a single logical switch, enhancing the intelligence of edge switches, while flattening the network and eliminating deployment complexity. The result is a simplified operational model that reduces costs.

- **Extreme Defender for IoT**
  A comprehensive solution that simplifies onboarding and securing of wired IoT devices. Extreme Defender for IoT provides centralized visibility and management, and connects via a secured transport with the ExtremeCloud Appliance, to ensure secure access of IoT devices onto the network, analyze traffic flows and pinpoint anomalies. The solution works with Extreme FabricConnect or over third-party networks to protect IoT devices, and is ideal for healthcare environments.

A Versatile, Easy-to-Deploy option for the Switched Edge

Network complexity remains an ongoing challenge for today's network administrator. This challenge is especially acute when extending the wired infrastructure into new enterprise environments. Installing new switches (or moving existing switches) brings with it a heavy administrative overhead – with each switch and switch port needing its own set-up and provisioning. Furthermore, the administrator must ensure that provisioned services match what the edge switch can support.

What if there was a simpler and easier way to deploy, set-up and administer the edge of your network? Extreme's Extended Edge Switching is a solution hat lets you deploy and oversee a more versatile and easily managed switched infrastructure that seamlessly extends advanced network services to the edge.
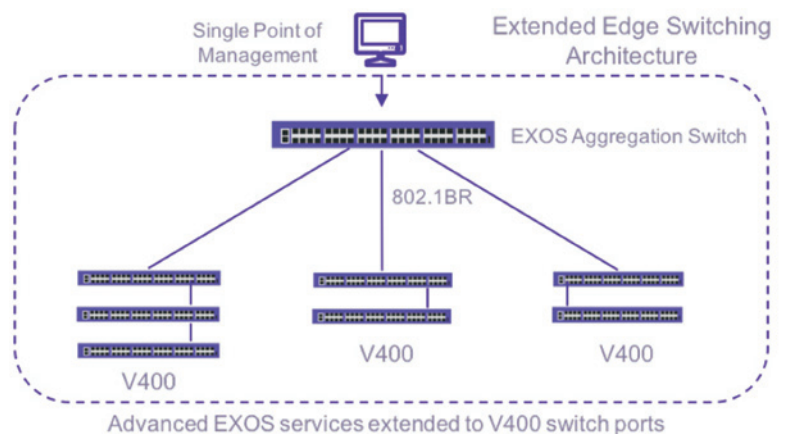
Extreme Networks Extended Edge Switching

Extended Edge Switching is an innovative solution that simplifies the deployment and operation of edge switches – especially across a campus switched network. Based on the IEEE 802.1BR specification, Extended Edge Switching collapses multiple network layers into a single-tier unified services architecture that can greatly reduce the complexity of the traditional two and three-tier switch architectures. The result is a simplified operational model that reduces costs.

Highlights

- Seamlessly extend advanced switching features to the network edge
- Collapse multiple network layers into a single logical services architecture
- Centralized, single point of control for reduced complexity and operational expense
- Plug and play edge switch installation – just connect and power-up
- Deploy scalable cost-efficient networks supporting thousands of extended remote ports
- Versatile design options – all based on the 802.1BR standard

With an Extended Edge Switching solution, economical edge switches are meshed with more advanced aggregation switches to form a single logical switch (see Figure 1). Advanced services can then be seamlessly delivered to the edge switch, providing cost-effective price per-port functionality – without compromising performance. The solution in essence creates a single switching system that is independent of physical location. This versatility allows enterprises to quickly add wired ports wherever needed across the campus. Extended Edge Switching extends aggregation switch features to V400 devices while providing a single point of management

Advanced EXOS services extended to V400 switch ports

The Extreme Edge Switching solution effectively replaces the traditional full-function access switch with a V400 device. The V400 in turn is transparently managed and controlled by the EXOS aggregation switch, eliminating the need to manually provision and configure the individual V400 device. Within this architecture, V400 devices can be seen as functioning as "virtual line cards" of the EXOS aggregation switch – all operating within a larger "distributed chassis" domain. The V400 and the EXOS aggregation switch use the standard 802.1BR protocol to communicate with one another.

As opposed to deploying and maintaining a network of full-function access switches in a remote wiring closet, the Extended Edge Switching solution with the V400 Series delivers the following capabilities and benefits:

Simplified, Single Point of Management

V400 edge switches and ports are configured and managed through the EXOS aggregation switch interface, or alternatively viExtreme Management Center software. The network administrator can centrally configure services and/or network policies across the campus from a single point in the network.

Seamless Unified Services

V400 edge devices/ports all offer the same unified network services and software features since they are an extension of the EXOS aggregation switch. This includes Extreme Policy and advanced Layer 3 Services, such as OSPF. Streamlined Licensing and Maintenance The flattened architecture of the Extended Edge Switching network simplifies the provisioning and support of edge device ports. Software licensing, service turn-up, and debugging/maintenance can all be done centrally from the EXOS aggregation switch.

Plug and Play Edge Deployment

V400 edge devices support plug and play installation. After physically connecting the V400 edge device and powering it up, it automatically finds the central EXOS aggregation switch. It then downloads its configuration from the EXOS aggregation switch and is ready to operate. There's no need to connect a local console to configure V400 edge devices or ports.

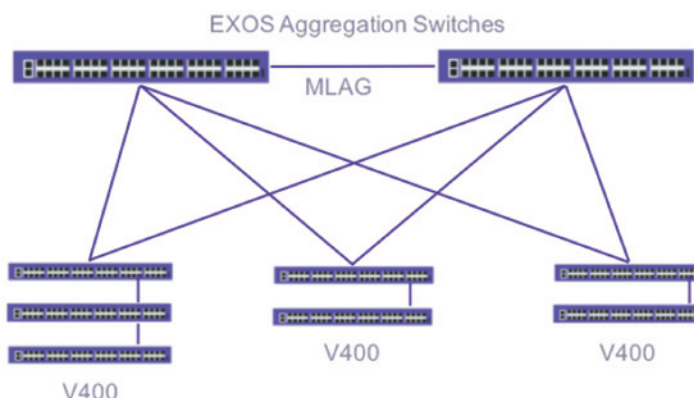## Unified Control Plane Eliminates Complex Protocols

The Extended Edge Switching domain employs a unified control and forwarding plane, eliminating the need for Layer 2 Shortest Path Bridging (STP) or complex Layer 3 protocols, like OSPF. Multi-pathing is also supported from edge devices to aggregation switches with all links active and load-balanced to optimize performance and provide resiliency.

Cascading of Edge Devices for Flexible Design

V400 devices can be cascaded to create a virtual stacking capability. Up to four (4) V400 edge devices can be cascaded off a single high-speed link or alternatively via a LAG back to the EXOS aggregation switch. This minimizes the need for individual fiber cable runs from each V400 device, providing flexible deployment either within the wiring closet or at the network edge.

High-Availability, Redundant Options

EXOS aggregation switches can be linked together via an MLAG to create a highly redundant design that minimizes service interruption in event of a failure of one of the aggregation switches. V400 switches can be separately connected to each EXOS aggregation switch to minimize the impact of any aggregation switch failure or interruption of service.

Redundant design can be created using an Redundant design can be created using an MLAG between EXOS aggregation switches.
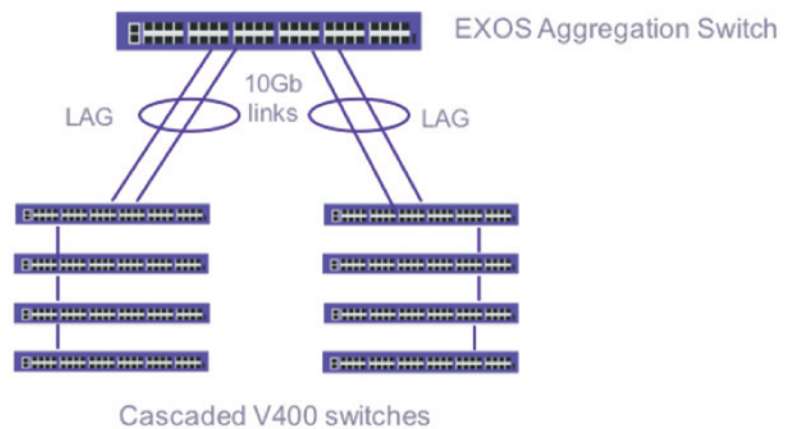
Extended Edge Switching brings campus networks into the modern era by enabling enterprises to build networks that deliver:

Simplified Management – A single point of control along with the reduction of unnecessary network layers helps eliminate individual switch touch points, thereby reducing maintenance time and costs.

Advanced Services to the Edge – By meshing the feature-rich services of the aggregation switch with the entry-level V400 device,advanced Layer 2/3 services and policy can be flexibly extended to the edge. Costeffective price-per-port functionality is delivered without compromising performance.

Scale-out Networking – The Extended Edge Switching architecture can operate over longdistance links, independent of physical location. This allows enterprises to easily add ports whenever and wherever needed across the campus without adding complexity.

V400 switches can be cascaded to provide a virtual stacking capability.

In summary, Extended Edge Switching technology offers a level of flexibility, ease of deployment, and total cost of ownership unmatched by traditional access, aggregation, and small-core chassis solutions.

Extended Edge Switching Supported Platforms

The ExtremeSwitching X590, X670-G2 and X690 Series platforms are supported as EXOS aggregation switches within an Extended Edge Switching design.

ExtremeCloud Appliance

Unified Wired and Wireless for Campus, Private Cloud and Hybrid Cloud Deployments
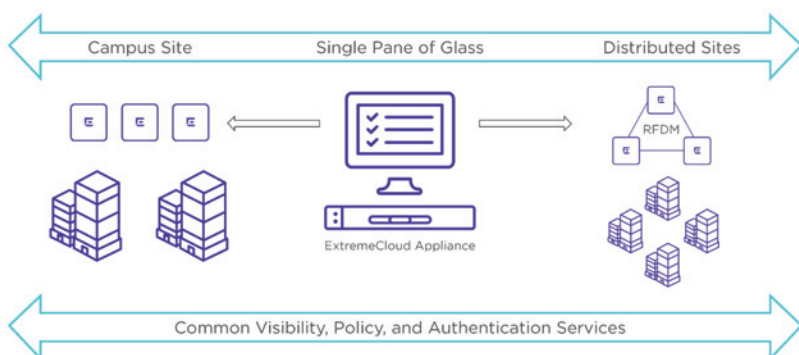
ExtremeCloud Appliance is a key offering within the Extreme Smart OmniEdge solution which was designed for customers who love the simplicity of ExtremeCloud but require an on-premise solution. ExtremeCloud Appliance delivers cloud-like simplicity, management with tightly integrated services and features on-premise deployments require, complemented with simplified licensing. ExtremeCloud Appliance is also available as a virtual machine (VM) for customers that have their own private cloud services.

- High-performance, enterprise-class WLAN appliances
- Scalable to over 4.000 managed devices per wireless appliance
- Seamless roaming with centralized and distributed data forwarding
- Virtualized management and control planes for cloud deployments
- High-availability architecture for real-time voice/video/data applications
- Flexible platform automatically adapts to underlying virtual resources
- Unified wired and wireless management

On-Premise and Private Cloud

While ExtremeCloud delivers the public cloud and subscript ion opt ions, ExremeCloud Appliance complements it for premise and private cloud solutions.

ExtremeCloud Appliance shares the same unified wired and wireless UI and workflows with ExtremeCloud, but includes the additional functionality required for a robust on-premise, campus and private cloud, distributed solution.

ExtremeCloud Appliance On-Premise and Hybrid Cloud

Highlights

- Purpose built with a unique operating model that scales to address the growth of mobility and IoT
- Cloud-like simplicity with unified management and integrated services for any type of on-premise deployment
- Delivers a consistent customer-driven experience across campus and distributed environments
- User interface and workflows make network enhancements and changes quick and agile, achieving your digital transformation goals faster
- Augment your IT with ExtremeAI service for proact ive artificial intelligence to adapt RF to your Wi-Fi network for the ultimate customer experience
- Leverage the integrated location analytics to understand visitor foot fall, density and traffic flow
- Hosts ExtremeDefender for IoT to simply and securely onboard IoT devices
- Certified with many of Ext eme's powerful management, location and security applications
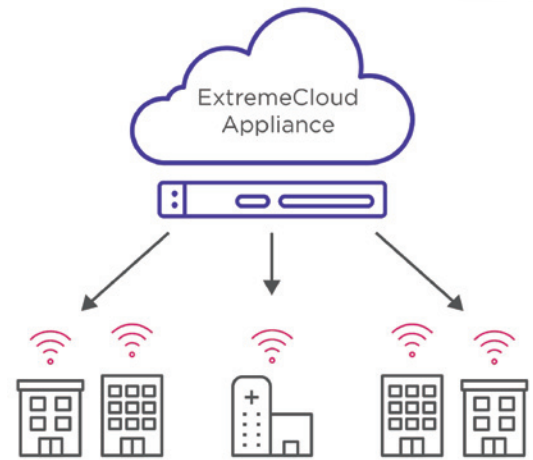- 100% in-sourced support for fast and accurate resolution

Designed to handle the dense user environments of campuses, as well as many distributed branch sites, or the combination of both, ExtremeCloud Appliance ensures enterprises have the maximum agility to tune their networks to meet their specific needs, without compromising functionality.

Campus Solution

ExtremeCloud Appliance leverages the award winning features from ExtremeWireless campus solutions. Incorporating the policy and role based BYOD on-boarding, flow-based technology for dense user solutions, and integrated application visibility and control applied at the access point s to deliver the best customerdriven experience.

ExtremeCloud Appliance Campus Solution
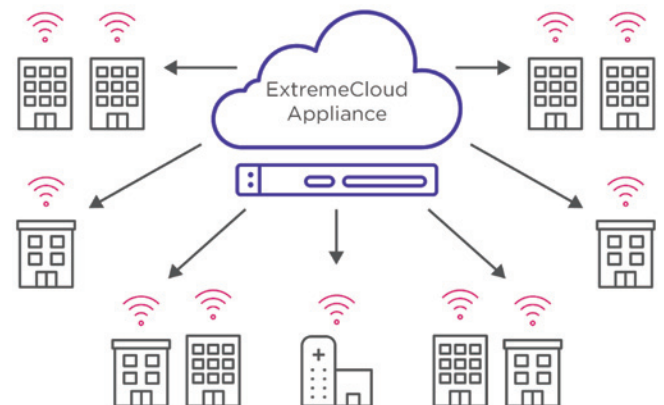
Private Cloud Distributed Solution

For enterprises who need to manage many branch locations while remotely troubleshooting centrally, ExtremeCloud Appliance leverages the heritage and experience achieved from delivering WiNG solutions to the Fortune 10 0 , with easy on-boarding of guest , social media, to site survivable branch offices, ExtremeCloud Appliance incorporates the best of breed solution for distributed solutions. Branch sites of up to 128 access point s will be site survivable and not require local controller appliances.

ExtremeCloud Appliance Private Cloud Distributed Solution

Campus and Private Cloud Solution

Enterprises, like retail and healthcare, may have large campuses, while needing to support many remote branches and offices. Smart OmniEdge is ideal for these deployments, leveraging ExtremeCloud Appliance to manage to the remote sites as well as the campus, providing a single-paneof- glass for managing and maintaining both distributed and campus solutions.

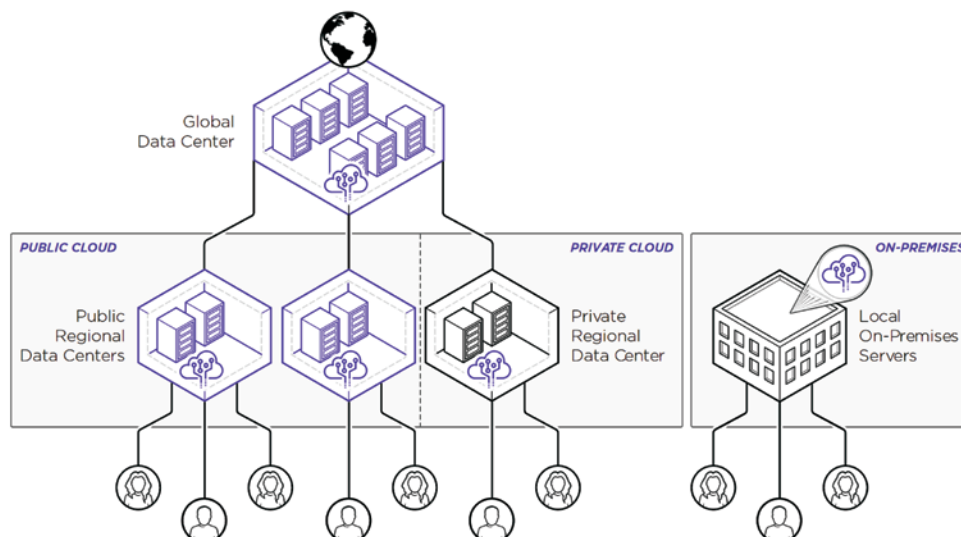*ExtremeCloud Appliance Campus and Private Cloud Solution*

ExtremeCloud IQ

Machine Learning and AI-driven Wired and Wireless Network Management Offering Intuitive Configuration Workflows, Real-Time and Historical Monitoring, Comprehensive troubleshooting and integrated network applications

ExtremeCloud IQ is an industry-leading and visionary approach to cloud-driven networking, built from the ground up to take full advantage of Extreme's end-to-end networking solutions. ExtremeCloud IQ delivers unified, full-stack management of wireless access points, switches, and routers and enables onboarding, configuration, monitoring, troubleshooting, reporting, and more. Using innovative machine learning and artificial intelligence technologies, ExtremeCloud IQ analyzes and interprets millions of network and user data points, from the network edge to the data center, to power actionable business and IT insights, and deliver new levels of network automation and intelligence.

ExtremeCloud IQ operates on Extreme's fourth generation Cloud Services architecture, capable of supporting millions of infrastructure devices and hundreds of millions of clients per Regional Data Center. All Extreme Cloud Services components are hosted in secure SOC Type 1 data centers with 24/7 monitoring, scheduled backups, and built-in disaster recovery capabilities. The ExtremeCloud IQ offers rapid feature velocity, increased availability, and advanced flexibility desired for modern access network management.

HIGHLIGHTS

Full Stack Management
- Native cloud management for Wi-Fi, Switching, and SD-WAN unified networks 360

Dashboards and Insights
- Machine Learning derived insights drive a comprehensive visual dashboard of location, devices, and users

Network Health
- Real-time and historical view of client and device health with built-in remediation tools

Application Visibility and Control
- Visibility and control of application usage for professional and recreational applications and network services

Comparative Analytics
- Anonymously compare operational and performance-based metrics to those of other organizations of a similar size and vertical

Auto-Provisioning
- With zero-touch deployment, automatically apply configuration policies

Extreme Cloud Services also provides a full suite of cloud-optimized open APIs for developers to create 3rd party applications and user experiences including user onboarding mechanisms, proximity-based services, presence and location analytics, and more.

Deployment options include Public Cloud, Private Cloud, and a Local Cloud solution.

Deployment Choices

Extreme offers three cloud deployment options – Public, Private or On-Premises – that support one goal: to provide you with maximum flexibility, continuous innovation, and a consistent user experience. Moreso, our 100% software-centric architecture is Cloud-Hosting agnostic, supporting AWS, Google, MSFT and more.

- **Public Cloud**
  Extreme provides access to a hosted service which removes infrastructure management and costs, provides data privacy and protection, unmatched reliability, and continuous delivery of innovations.

- **Private Cloud**
  For businesses who want or need to isolate management services in their own controlled environment, Extreme packages ExtremeCloud IQ into a private cloud offering which enables the same services as the public cloud (e.g. ML, AI, data stores etc.) all hosted within customers' or partners' private cloud instance.

- **On-Premises**
  The on-premises option provides Extreme's cloud service in a format which can be hosted on-premises at your site.

Regardless of which option you choose, ExtremeCloud IQ offers the same capabilities and feature sets. More so, as your requirements change, so too can your deployment – there is no need to rip and replace.

Your Network. Your Way. Complete Solution Flexibility with ExtremeCloud IQ
Through value-based licensing/SaaS tiering, Extreme Networks is making it even easier for you to grow as you go, both in a technical and commercial sense. We offer the most flexible, feature-rich, application tiers tailored to every business, budget, and IT needs, that delivers the management, intelligence and assurance your business requires.

	ExtremeCloud™ IQ Connect	ExtremeCloud™ IQ Pilot	ExtremeCloud™ IQ Co-Pilot (COMING SOON)	ExtremeCloud™ IQ Auto-Pilot (COMING SOON)
Availability	PUBLIC	PUBLIC PRIVATE LOCAL	PUBLIC PRIVATE	PUBLIC PRIVATE
Feature Set	Free device management for access points, switches, and routers	EVERYTHING IN CONNECT, PLUS: Advanced infrastructure management, reporting, and remediation tools	EVERYTHING IN PILOT, PLUS: Machine Learning-derived insights and intelligence	EVERYTHING IN CO-PILOT, PLUS: Advanced Actionable AI
Unique Features	• Device onboarding • Guided Configuration • Centralized Management • Wi-Fi Planner • Basic Monitoring Tools • Essential Security	• Advanced Topology View • Troubleshooting Heuristics • Contextualized Optimization • Role Based Profiling • Advanced 360° Reporting • Comparative Analytics	• Supervised ML Insights & Tuning • Automated Bug Fixes • ML Issue Resolution • Automated RMA • Advanced NAC Integration • Multi-Cloud Support	• AI Configuration • AI DFS Optimization • AI-Driven Quarantine • AI Segmentation • AI Anomaly Detection • AI WIPS

Extreme Defender for IoT

Simple Security for Your Critical Endpoints

The Internet of Things (IoT) is having a profound impact in every industry. According to survey data, 63% IT organizations have witnessed a 50% increase in the number of endpoints that are connecting to the network1. By 2020, Gartner estimates that 20.4 billion connected things will be in use by organizations worldwide. Although IoT growth is really being driven by 3 main subsectors: Smart Cities (26%), Industrial IoT (24%) and Connected Health (20%), there really isn't a single vertical industry that isn't experiencing growth in the number of end points that are connecting to the network.

The Challenge of Implementing IoT Security

Although the threat of attack is very real, there are many factors that make securing specific IoT devices a challenge. First, just the sheer number and diversity of endpoints, many of which might not be within IT's direct control. They might be owned by the facilitaties management team, operational teams or clinician staff within a hospital. Furthermore, many of these devices were not originally designed to be Internet-connected and lack embedded security.

Some of the Specific Security Challenges of Connected Devices Include:

- May contain older, non-supported operating systems such as Windows 95/ 98 and can no longer be patched.
- Lack of personal firewall, anti-virus and encrypt ion on many devices.
- In some industries (ie. healthcare) devices must go through an expensive, time consuming recertification process to remain in compliance if a change is made to the device (ie. security patch).
- In many cases, devices connecting to the wired network are more exposed. Specific issues include aging edge switches with feature disparity across the network.

Securing Devices with Extreme Defender for IoT

Extreme Defender for IoT is a unique, award-winning solution that delivers security for end points which have limited or even no embedded security capabilities. It is especially targeted to aging wired devices that need to roam around a room, a building or even a campus.

It complements a customer's existing security infrastructure by adding in-line defense directly at the IoT device itself. And it can be deployed over any network infrastructure to enable secure IoT management without significant network changes.

Extreme Defender Components

Extreme Defender consists of the following components:

- **Defender Application:** A user friendly application that enables the centralized creation of security profiles for groups of IoT devices. Once profiles are created, non-technical staff can securely onboard and move their devices. They can also monitor and track their assets through intuitive dashboards and centralized inventory.
- **Defender Adapter and the ExtremeWireless 3912i Indoor Access Point:** Provides a proxy service for the Defender application to both manage and secure IoT devices. Their specific role is to monitor traffic flows – with full Layer 2 to 7 visibility – to ensure that the device is operating according to its expected behavior. The Defender Adapter is a single port device that sits between the network and the IoT device providing in-line defense. The AP3912 is a multi-port unit that supports multiple devices in a single room.
- **ExtremeCloud Appliance:** Available as a hardware based or virtual-appliance, the ExtremeCloud Appliance, is a premise-based solution that provides cloud-like management and controller functionality for Extreme Smart OmniEdge (wired and wireless) solutions. With a full suite of rich APIs to customize applications, it is the supported plat form for the Defender Application.

Defender Adapter – In-line Security for Vulnerable Wired Devices

The Defender for IoT Adapter delivers enterprise-grade performance and personalized protect ion for vulnerable wired devices. Placed between the network and the device, the Defender Adapter works in conjunct ion with the Defender Application (a value add application on the ExtremeCloud Appliance) to secure, isolate, track and monitor IoT devices.

Secures

The primary function of the Defender Adapter is to enforce policies that are cent rally created by the Defender Application, ensuring that the IoT device connected to it operates according to its expected behavior. The profile provides a list of authorized devices and traffic flows to limit what the IoT device receives and transmit s, as well as who or what the device can communicate with. The Defender Adapter will then monitor all traffic to and from the device with full L2-7 visibility and block any traffic that is out of profile.

Isolates

A unique at tribute of the Defender for IoT solution is that it can isolate groups of IoT devices into their own secure zone/ network segment. The role of the Defender Adapter is to ensure the secure attachment of IoT devices into the specified secure zone. These secure zones can be IPSec tunnels overlaid onto 3rd party networks, Fabric Connect virtualized hyper-segments, or just VLAN-based. For Fabric Connect networks, support for auto-attach (IEEE draft 80 2.1Qcj) provides the ability for the Adapter to signal Fabric Attach to automatically create the required services (VLAN and ISID mapping) on the edge access switch, providing auto-provisioning from the network edge into the network core. If device moves to another point of attachment, the network service configuration moves with it .

Tracks

The Defender Adapter is future proofed, with an integrated BTLE/ 80 2.15.4 radio for extended connectivity to Internet of Things (IoT) sensors and devices. This includes support for support for Thread and other higher level IoT protocols that support sensor networks and smart building automation. Integrated iBeacon can be used for locating critical assets.

Powers

The energy efficient Defender Adapter uses 802.3af Power over Ethernet (PoE) in normal operating mode. For deployments where the Defender Adapter is paired to a device that requires power, such as an IP camera or a phone, it supports PoE pass-through to that device when it is connected to an IEEE 802.3at PoE+ capable edge switch.
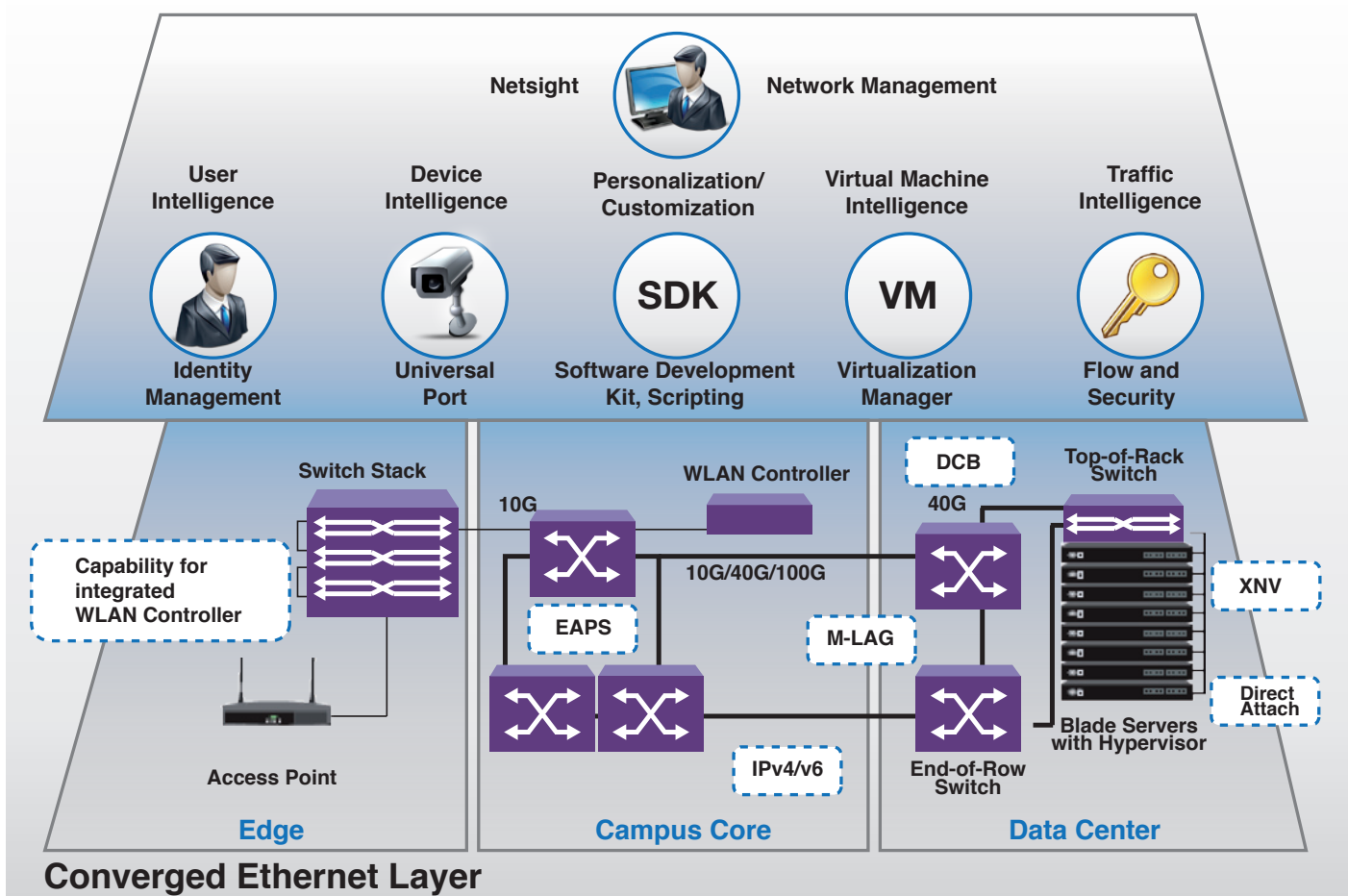
ExtremeXOS™

ExtremeXOS Network Operating System

Extreme Networks has changed the industry by creating ExtremeXOS – a highly available and extensible software foundation for converged networks. ExtremeXOS raises the bar for availability, which is critical when offering carrier-grade voice and video services over IP and for supporting mission-critical business applications such as CRM. A more available network can also lower operational costs by drastically reducing emergency maintenance. ExtremeXOS allows you to extend the capabilities of your network via dynamic loading of applications, XML APIs and CLI scripting. It allows you to integrate specialized application appliances such as security and VoIP monitoring devices into your network via XML, as well automatically configuring edge ports for security and VoIP using its Universal Port event based activation of scripts.

ExtremeXOS has a rich set of Layer 2 and Layer 3 control protocols, provides flexibility on the design of highly resilient networks and 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 can help secure the network using IPv6 Access Control Lists and help provide investment protection for your network. Security capabilities provide network access control integrated with end point integrity checking, and network control and management plane protection. ExtremeXOS has been deployed in production networks since 2003.

ExtremeXOS Intelligence Layer

What are the benefits of ExtremeXOS?

- **It's a High Availability Architecture:** The high availability of ExtremeXOS creates a resilient infrastructure capable of maximum network integrity for mission-critical applications. Different from the traditional Monolithic Operating Systems, ExtremeXOS solves the last single point of failure, i.e. the Operating System. If a management process fails in ExtremeXOS, this process can be stopped, re-started or replaced while the switch is still in operation. Whereas Monolithic OS's require a reboot resulting in a typical outage of 3-5 minutes.

- **It's an easy to manage architecture:** Universal Port dramatically simplifies rollout of VoIP via auto-configuration of edge ports and phones.

- **It's an open architecture:** There are endless possibilities for further expanding the capabilities of the network, by integrating third-party applications. An example of this is the VoIP application layer monitoring agent developed by Avaya to simulate and closely monitor the behaviour of VoIP connections in a network.

- **It's a secure architecture:** Security of the entire network infrastructure is protected with ExtremeXOS. For Example management traffic is secured through authentication and encryption. In addition access control works with or without dedicated authentication support on client devices, such as VoIP phones.

Configuration Management (CLI/SNMP/XML/Scripts)

ExtremeXOS Application Modules

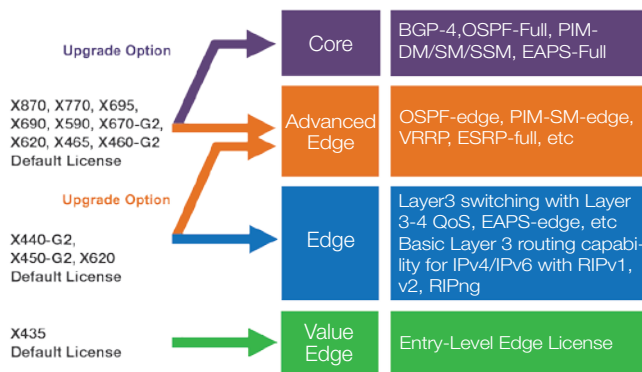sFlow, SSH2, OSPF, VRRP, Network Login 802.1x, STP, EAPS, ESRP

ExtremeXOS Kernel-Loadable Modules

ExtremeXOS Kernel

Hardware Abstraction Layer

Hardware

ExtremeXOS Modular Operating System

ExtremeXOS feature matrix

Upgrade Option

X870, X770, X695, X690, X590, X670-G2, X620, X465, X460-G2 Default License

Core: BGP-4, OSPF-Full, PIM-DM/SM/SSM, EAPS-Full

Advanced Edge: OSPF-edge, PIM-SM-edge, VRRP, ESRP-full, etc

Upgrade Option

X440-G2, X450-G2, X620 Default License

Edge: Layer3 switching with Layer 3-4 QoS, EAPS-edge, etc Basic Layer 3 routing capability for IPv4/IPv6 with RIPv1, v2, RIPng

X435 Default License

Value Edge: Entry-Level Edge License

Please refer to the individual products for the XOS upgrade part codes.

Preparation — Administrator

1. Administrator configures VoIP policies (VoIP VLAN, Dot1p priority, etc)
2. Administrator pushes policies to switch

Operation

3. After 802.1x authentication, phone sends LLDP messages with model, PoE, serial number, etc.
4. Switch configures VLAN, Dot1p priority, AC_s and PoE on the port
5. Switch VLAN, Call Server, E911 Location, QoS, etc to the phone

VoIP Auto configuration with ExtremeXOS Universal Port

Traditional Monolithic vs. Modular operating system quick comparison		
	Monolithic	**Modular**
Single memory address for all modules	✔	✘
Start and stop processes with switch running	✘	✔
Dynamically load and unload modules without rebooting the switch	✘	✔
Continues to run with crashed modules	✘	✔

ExtremeXOS Universal Port

Universal port manager simplifies rollouts via auto-configuration of edge ports and phones. Deploying VoIP endpoints is as easy as opening the package, pro-gramming the extension and plugging into the network.

Ethernet Automatic Protection Switching (EAPS)

Ethernet Automatic Protection Switching (EAPS) is Extreme Networks' solution for fault-tolerant network topologies. EAPS is a feature of ExtremeXOS and is responsible for sub 50 millisecond network recovery. This revolutionary technology provides end users with a seamless experience when network failure does occur and does so with radical simplicity.

Why do converged networks need an easy to manage architecture?

In order to realise many of the benefits of a converged network, IT managers have been looking for ways to simplify and in some cases automate the deployment of VoIP endpoints such as laptops with soft phones, WiFi base stations and IP Handsets.
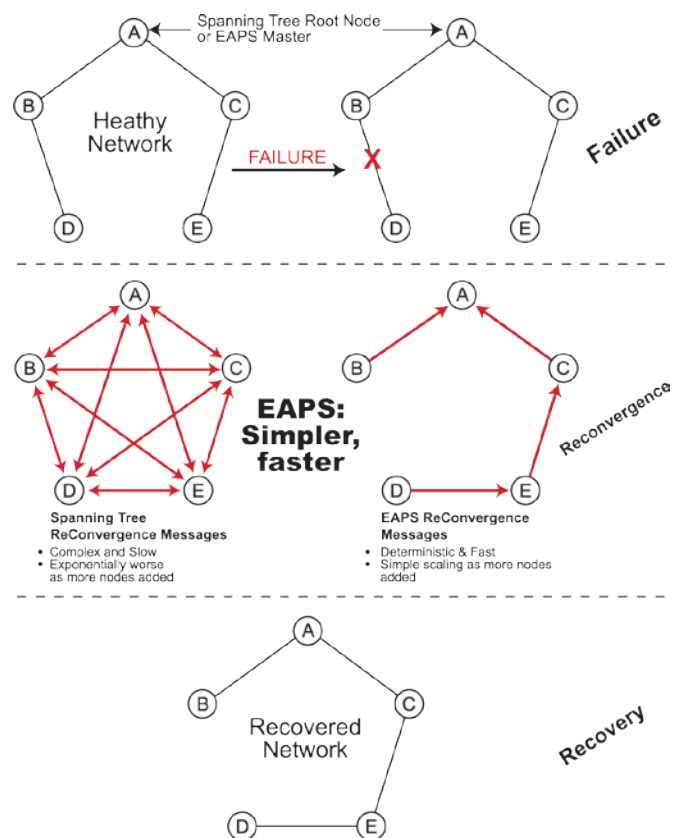
What was needed was the ability for the port on a data switch to understand the nature of the device connecting to it, for example what is its power requirement and does it require connecting to a specific Virtual Local Area Network (VLAN) for voice?

Why do Converged Networks require High Availability?

As the trend to consolidate business critical application onto IP Networks continues, it has been realised that the network infrastructure as a whole has to continue running even if individual connections are lost. Traditional technologies such as spanning tree protocol (STP) were developed to establish redundant network paths so that data could be automatically redirected to alternate routes. However, with delay sensitive applications such as Video or VoIP, the time it takes for the network path to re-converge using STP can result in connections timing out and in some cases dropped. The impact of this is frustration for users in dropped calls or video sessions, and it increases the strain on the network as applications attempt to re-establish sessions. Extreme Networks address these issues with their Ethernet Automatic Protection Switching (EAPS) protocol delivering high speed sub 50 millisecond network recovery.

Failover time comparison table		
EAPS	Open Standard	<50ms
STP	Open Standard	<30s
Port Fast	Proprietary	<2s
SMLT	Proprietary	<50ms
RSTP	Open Standard	<500ms

Multi-Switch Link Aggregation (M-LAG)

A number of new protocols and approaches have been suggested to address some of the shortcomings of spanning tree protocol. One approach to addressing both the performance as well as the resiliency requirements of these highly virtualized data centers is to extend the link-level redundancy capabilities of link aggregation and add support for device-level redundancy. This can be accomplished by allowing one end of the link aggregated port group to be dual-homed into two different devices to provide device-level redundancy. The other end of the group is still single homed into a single device. See Figure 1 below.

In Figure 1, Device 1 treats the link aggregated ports as a normal link aggregated trunk group, i.e. it does not see anything different. Traffic from Device 1 is distributed across the ports in the group using traditional link aggregation algorithms which would typically hash the traffic across the ports in the group using a variety of hashing algorithms. If one of the links in the group were to go down, traffic would get redistributed across the remaining ports in the group. However, the other end of link aggregated group is where things now function differently. Device 2 and Device 3 now work together to create the perception of a common link aggregated group so that Device 1 doesn't see anything different from a link aggregation perspective, even though the link aggregated ports are now distributed across Device 2 and Device 3, thereby leading to the term

Multi-Switch Link Aggregation (M-LAG). Device 2 and Device 3 communicate information to each other over the Inter Switch Link (ISL) so that forwarding, learning and bridging work consistently without causing any loops. The ISL itself can be a regular LAG. If either the link to Device 1 from Device 2 or Device 3 were to go down, or if Device 2 or Device 3 itself went down, traffic would now get forwarded across the remaining link/device thus providing both link-level and device-level redundancy. The intelligence that allows the ports on Device 2 and Device 3 to present itself as a single link aggregated trunk group to Device 1 today is implemented using mostly proprietary mechanisms, i.e. M-LAG technology is still largely proprietary. However, the proprietary nature of the technology is confined to the layer which presents itself as a distributed link aggregated group, specifically Device 2 and Device 3, both of which should come from the same vendor. Device 1 does not participate in this proprietary protocol, and in fact Device 1 may come from a different vendor and can in fact be a different type of device. For example, Device 1 can be a server which has dual NICs teamed together, while Device 2 and Device 3 can be Ethernet switches from a single vendor. M-LAG can work at different layers from the access to the core of the network. M-LAG can be used in conjunction with traditional link aggregation to increase bandwidth as well as add link-level redundancy between devices. See Figure 2 below.
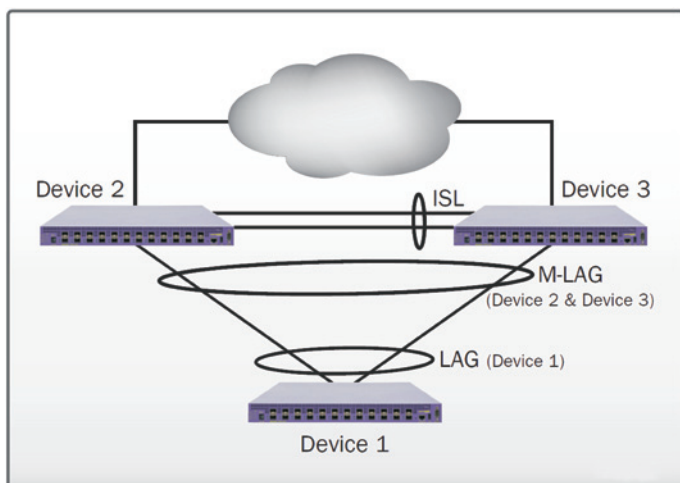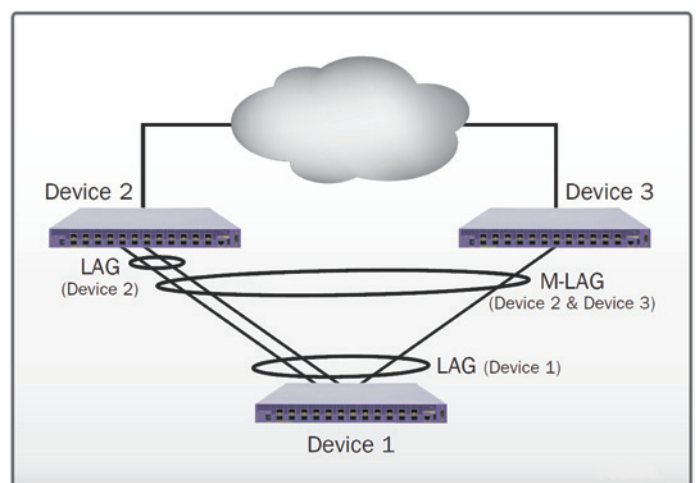

Figure 1

Figure 2

ExtremeSwitching Overview

ExtremeSwitching provides the Nervous System of the Autonomous Enterprise by Delivering Simple, Secure, and Automated Networks

Secure Through a combination of role-based policies, secure link encryption, and hyper-segmentation, we help protect your network from the threat of cyber-attacks and breaches.

Cloud-Driven Combine industry-leading edge to core switches with fourth-generation cloud management to streamline and simplify every aspect of network operations from deployment to support.

Automation Do more with less with a network that simplifies on-onboarding of users and devices; accelerates and optimizes scaling and updating; and couples end-to-end provisioning to your business-driven workflows.

Key Benefits of ExtremeSwitching:

Fabric-Enabled
As a leader in fabric networking, Extreme offers a flexible portfolio of Ethernet and IP fabric solutions. Whether you are transforming your campus, data center, metro, or WAN, our fabric technologies ensure a faster, more flexible, and more secure foundation for your business.

Application Hosting
Extreme Switches can run onboard applications alongside the switch OS – all without impacting performance. This can help provide network insight through on-board analytics applications and even enable new network applications without the need for a separate hardware device.

Secure Link Encryption
Extreme switches help secure your traffic with support for IEEE 802.1AE MACsec across our various switch platforms. MACsec is a hop-by-hop security capability which encrypts/ decrypts packets between connected switches or devices.

Dynamic Role–based Policies
Extreme Switches support a common highly-scalable policy mechanism across wired and wireless devices. These policies are centrally defined but locally enforced at the switch. These policies travel with the user, device, and application as they move through the network.

Rich Telemetry and Analytics
Rich application telemetry combined with ExtremeAnalytics provide comprehensive network and application analytics. Eliminate shadow IT, improve security, and enable faster, more efficient network remediation with full layer 2-7 visibility.
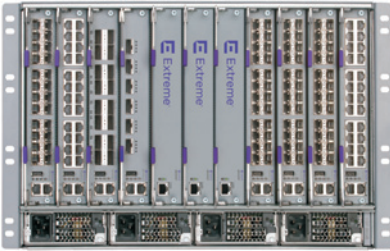
Extended Edge Switching
Extended Edge Switching enables you to scale out your campus access ports in a simple and cost-effective way. Using a combination of controller bridges with low cost access devices, a single logical switch architecture can be created to simplify both deployment and operations.
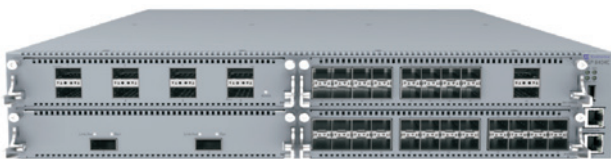
Automated Campus Switching Series

VSP 8600

Description
High-density 100GbE modular core/aggregation switch

Key Features
- High-density, reduced footprint modular chassis solution (7 RU)
- Fabric Connect-capable platform ideal for campus core and aggregation
- Multi-rate 10 / 25 / 40 / 100GbE support
- Over 21 Terabits raw switching capacity
- Up to 192x 10GbE, 128x 40GbE or 48x 100GbE interfaces
- Extreme Fabric Connect
- MACsec and IPv6 support

VSP 8284

Description
High-performance, compact, fixed-format 10 / 40GbE core/ aggregation switch

Key Features
- High-performance, fixed-format 10 / 40GbE switch
- Fabric Connect-capable switch ideal for small core or mass 10GbE aggregation scenarios
- 80x GbE and 4x 40GbE uplink interfaces
- Extreme Fabric Connect and Fabric Attach
- MACsec and IPv6 support
- Distributed virtual routing, PIM and VXLAN gateway capabilities

VSP 8400

Description
Flexible, compact modular 10 / 40 / 100GbE aggregation switch

Key Features
- High-performance modular 10 / 40 / 100GbE Switch
- Fabric Connect-capable switch ideal for high-speed aggregation
- Modular form factor with up to 4 Ethernet switch modules
- Up to 96x 10GbE, 32x 40GbE or 8x 100GbE interfaces
- Extreme Fabric Connect
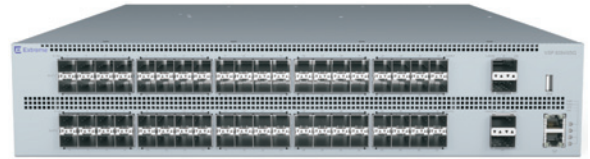- MACsec and IPv6 support
- VXLAN Gateway

VSP 7200

Description
High-performance, compact, fixed-format 10 / 40GbE core/ aggregation switch

Key Features
- High-performance, fixed-format 10 / 40GbE switch
- Fabric Connect-capable switch ideal for small core or mass 10GbE aggregation scenarios
- 80x GbE and 4x 40GbE uplink interfaces
- Extreme Fabric Connect and Fabric Attach
- MACsec and IPv6 support
- Distributed virtual routing, PIM and VXLAN gateway capabilities

![Extreme networks logo]

Agile Data Center Switching Series

SLX 9850

Description
Modular Chassis – Data Center Spine, Super Spine and WAN Edge Router

Key Features
- Purpose-built 100GbE switch for highperformance
- Flexible multi-rate Gigabit Ethernet support: up to 48 ports of 100G, up to 128 ports of 40G, or up to 192 ports of 10G
- 100GbE interface rates
- Supports both conventional Routed IP and/or Fabric-based network deployments
- Raw system capacity of up to 21.6Tbps
- Broad support for IP Routing techniques
- MACsec and IPv6 support

SLX 9740

Description
Border Router with Ultra-Deep Buffers designed for the interconnection point between internal networks and the internet.

Key Features
- High density 100GbE routing platform
- Cost efficient Spine, DCI, Border Leaf and Border Routing deployment options
- Flexible port configurations for high density 10GbE, 25GbE, 40GbE and 100 GbE in 1 & 2 RU form factor
- Industry-leading tunable, deep packet buffers (8GB, 16GB) for bursty traffic patterns
- Carrier-class MPLS, IS-IS/OSPF, BGP/EVPN (VXLAN), VLL/VPLS, COPP

SLX 9540

Description
Next-Generation Fixed Switch with Flexible Edge Connectivity for the Digital Organization

Key Features
- Supports 1GE, 10GE, 40GbE, and 100GbE interface rates
- Ultra-deep 6GB tuneable buffers
- Advanced forwarding - including IPv4, IPv6, MPLS/VPLS, BGP-EVPN and OpenFlow
- Support for up to 1.6Tbps with up to 800Gbps switch fabric capacity and up to 720mpps forwarding performance

SLX 9640

Description
Next Generation Fixed Router to Simplify the Core and Scale the Internet Border and Interconnect

Key Features
- Supports 10GE, 25GbE, 40GbE, 50GbE and 100GbE interface rates
- Ultra-deep buffers for lossless forwarding in demanding data center & WAN applications
- Advanced forwarding - including IPv4, IPv6, MPLS/VPLS, BGP-EVPN, and OpenFlow
- Support for up to 4M IPv4 and 1M IPv6 routes in the Forwarding Information Base (FIB), high policy scale with required statistics and Internet peering

SLX 9240

Description
Programmable, Flexible, High-Density Switch

Key Features
- Supports 10GE, 40GbE, and 100GbE interface rates
- Buffers 24 MB tunable
- Advanced forwarding - including IPv4, IPv6, MPLS/VPLS, BGP-EVPN and OpenFlow
- Max I/O Capacity 6.4Tbps

SLX 9140

Description
Next Generation Programmable Leaf Switch

Key Features
- Supports 1GE, 10GE, 25GE, 40GbE, and 100GbE interface rates
- Buffers 24 MB tunable
- Advanced forwarding - including IPv4, IPv6, MPLS/VPLS, BGP-EVPN and OpenFlow
- Max I/O Capacity 3.6 Tbps

SLX 9030

Description
High-performance 48-Port 10GbE Leaf Switch

Key Features
- Supports 1GE and 10GE interface rates
- Copper ports support 10G, 1G and 100 Meg speeds and Fiber supports 10G and 1G
- Buffers 24 MB tunable
- Advanced forwarding - including IPv4, IPv6, MPLS/VPLS, BGP-EVPN and OpenFlow
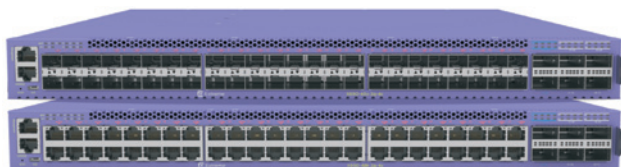- Max I/O Capacity 3.6 Tbps

EXOS Switching Series

X870

Description

High Density, Advanced 100GbE Enterprise LAN and Data Center Spine Switching.

Key Features
- Purpose-built 100GbE switch for highperformance enterprise and cloud data centers.
- Ideal for leaf-spine, as well as TOR eployments
- Non-blocking 6.4Tbps switching capacity
- Supports 10GE, 25GbE, 40GbE, 50GbE, and 100GbE interface rates
- Role-based policy support
- 32x 100 GbE ports
- Option for up to 128x 10GbE or 128x 25GbE ports enables high-density leaf aggregation
- Optional DC power
- Unified, modular XOS operating system

X770

Description

High-density 10/40GbE Top-of-Rack switch.

Key Features
- High-density, low latency TOR switch with 32x 40GbE interfaces
- Option for up to 104 ports of 10GbE
- Role-based policy support
- Low latency (less than 600ns)
- IEEE 1588 Precision Timing Protocol (PTP) support
- Optional DC power
- Unified, modular XOS operating

X695/ X690

Description

High-performance 10/25/100GbE aggregation and leaf switch.

Key Features
- High-density, advanced 10GbE switch for aggregation and core
- Ideal as 10GbE leaf switch with X870
- Non-blocking 1,76Tbps switching capacity
- Supports 10GbE, 25GbE, 40GbE, 50GbE, and 100GbE interface rates
- Role-based policy support
- 48x 10GbE / fiber SFP+ and copper 10GBASE-T models
- Up to 8 high-speed uplinks with 10/25/40/50/100GbE rate options
- Controlling aggregation switch for V300/V400 edge devices with Extreme Extended Edge Switching
- Optional DC power
- Unified, modular XOS operating system

X670-G2

Description

Versatile TOR aggregation switch.

Key Features
- High-performance TOR switch with up to 72x 10GbE fiber interfaces
- Ideal for 10/40GbE leaf and spine architectures
- Role-based policy support
- 40GbE uplinks
- Industry-leading density
- Low latency (less than 600ns)
- IEEE 1588 Precision Timing Protocol (PTP) support
- Controlling aggregation switch for V400 edge
- Optional DC power
- Unified, modular XOS operating system, including heterogeneous stacking

X620

Description

Family of 10GbE edge switches with PoE++ support.

Key Features

- Complete family of 10GBASE-T and SFP+ fiber models
- 10GbE 10 port and 16 port versions
- Ideal for small storage and campus core applications
- Compact 10 port versions for both 10GBASE-T and SFP+ fiber
- Support for 2.5GbE and 5GbE multi-rate as well as 60W PoE++
- Unified, modular XOS operating system, including stacking

X590

Description

High-performance 24-port 10Gb aggregation switch.

Key Features

- High-performance advanced 10GbE switch for aggregation
- Non-blocking 880 Gbps switching capacity
- Supports 10GbE, 25GbE, 40GbE, 50GbE, and 100GbE interface rates
- 48x 10GbE / fiber SFP+ and copper 10GBASE-T models
- Controlling aggregation switch for V400 edge devices with Extreme Extended Edge Switching
- Unified modular XOS operating system.

X465 / X460-G2

Description

Scalable, versatile intelligent aggregation switch with PoE+ support.

Key Features

- Powerful and scalable, versatile intelligent aggregation or edge switch with enhanced PoE+ support
- Role-based policy support
- Up to 3.515W of PoE+ power for up to 90W per port
- 1/2.5GbE multi-rate interface option (up to 24 ports)
- IEEE 1588 Precision Timing Protocol (PTP) support
- Optional DC power
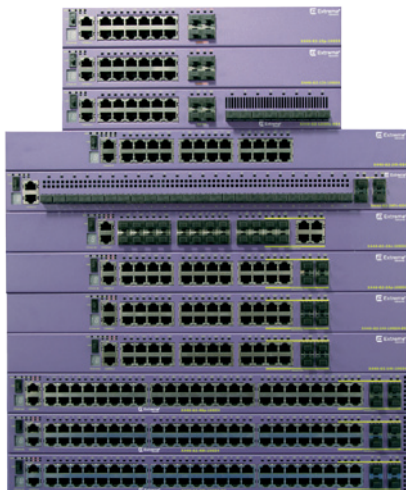- Unified, modular XOS operating system, including heterogeneous stacking

X450-G2

Description

Versatile, cost-effective edge switch with role-based policy.

Key Features

- Cost-effective 10/100/1000GbE switch with 24 or 48 interfaces
- Supports 4 front-mounted 1GbE or 10GbE uplinks
- Available PoE power with up to 30W per port
- Role-based policy support
- Modular, hot-swappable fans and available PoE power supplies
- Unified, modular XOS operating system including heterogeneous stacking

X440-G2

Description
Versatile, cost-effective edge switch with role-based policy

Key Features
- Cost-effective 10/100/1000 switch with 12, 24 or 48 interfaces
- Supports 4 front-mounted 1 GbE or 10 GbE uplinks
- 10MB/100MB half-duplex support
- Available PoE power with up to 30W per port
- Role-based policy support
- Modular, hot-swappable fans and available PoE power supplies
- Unified, modular XOS operating system including heterogeneous stacking

X435-G2

Description
Economical edge switches for distributed enterprises, branches and small sites

Key Features
- Multiple 8-port and 24-port GbE models with up to 4x 2,5GbE ports
- PoE/PoE+ models for powered connection of end points
- Fanless models for silent operation - ideal for classrooms, offices or retail locations
- System that can draw power from an upstream PoE Switch - eliminating need for a separate PSU

V400

Description
Simplified edge switch operation leveraging the power of ExtremeXOS aggregation switches

Key Features
- 24 or 48-port Gigabit Ethernet (non-PoE) models
- 24 or 48-port 80 2.3at PoE models
- 2 or 4-port 10Gbase-X SFP+ uplink ports
- Centralized, single point of control reduces complexity and operational costs (via X690, X670-G2, X590 or X465)
- Plug and play edge installation - just connect and power-up

ExtremeWireless WiNG

ExtremeWireless WiNG is powered by Cloud, ML and AI to deliver enhanced user experiences with effortless networking

ExtremeWireless WiNG is high efficiency, high capacity Wi-Fi that utilizes the latest technologies to optimize and protect bandwidth in all environments.

This solution is ideally suited to handle the increased device density of today's organizations while delivering a consistent experience to all users across the network. Powered by Extreme's WiNG operating system, this legendary distributed architecture places the intelligence at the edge where it unleashes the true capabilities and performance of 802.11ax, without bottlenecks and limits. Extreme's Wi-Fi 6 access points adapt seamlessly to the diverse needs of wireless users and IoT devices and are backwards compatible with all 802.11a/b/g/n/ac devices. Furthermore, ExtremeWireless APs work seamlessly with access switching functions and Fabric Attach to fully automate the AP management providing Zero Touch provisioning to an ExtremeCloud Appliance.

With the ExtremeWireless solution, customers are positioned to take advantage of the industry's latest 802.11ax technology taking the Wi-Fi network to an entirely new level; it uniquely addresses greater capacity, supporting more devices simultaneously and making better use of available spectrum with increased efficiencies, and dynamically adjusting bandwidth for different devices and applications as required. The Extreme solution will enable organizations to connect more devices, more users and more IoT while ensuring a reliable and high-quality user experience to wireless clients

Key features

- Greater Wi-Fi spectrum control which increases efficiencies, supporting each device with greater performance and experience.
- Integrated DPI with application visibility and control.
- Secure zero touch provisioning that significantly reduces deployment time.
- Integrated Layer 2 and 3 stateful firewalls.
- Support for latest WPA3 Wi-Fi security standard delivering robust protections for users and IoT devices.
- State of the art Operating System that is feature-rich and built on field proven technology for cloud and on-premises solutions.
- Ease of use; with a single click you can deliver services and new applications.
- Fast roaming with seamless mobility while delivering more throughput with fewer APs.
- Integrated Bluetooth radio for supporting IoT connectivity or for guest engagement and analytics.
- IEEE 802.3at PoE+ providing full capacity with all features enabled.
- High-performance next generation 802.11ax technology that is designed to leverage the performance improvements delivered with 802.11ac wave 2 together with key technology borrowed from cellular, to increase device capacity and improve spectral efficiency, extracting more out of available Wi-Fi spectrum.
- Highly-flexible and scalable offering both hardware and virtual appliance that support a range of capacities and licensing options. The large capacity appliance scales

ExtremeWireless Appliances

The ExtremeWireless controllers reduce costs and simplify IT efforts by unifying wireless-wired network management using a range of scalable architecture. The wireless controllers provide seamless roaming across deployments and resilient fail-over capabilities – proving the customers reliability.

NX 5500: supports up to 256 Access Points (APs)
NX 7500: supports up to 2.048 APs
NX 9600: supports up to 10.240 APs
VX 9000: supports up to 40.000 APs (VMware, Xen, Hyper-V or Amazon)

ExtremeWireless Access Points

The ExtremeWireless access point technology ensures enterprise-level security and high performance for any LAN environment – from restrictive hotel rooms to the harsh outdoors.

Indoor Access Points
AP310: IEEE 802.11ax, dual radio, 2x2:2, WPA3, up to 1,2Gbps capacity, BLE
AP410: IEEE 802.11ax, tri radio, 4x4:4, WPA3, up to 4,8Gbps capacity, BLE
AP505: IEEE 802.11ax, dual radio, 4x4:4, WPA3, up to 4,8Gbps capacity, BLE
AP510: IEEE 802.11ax, dual radio, 4x4:4, WPA3, up to 4,8Gbps capacity, BLE
AP650: IEEE 802.11ax, dual radio, 4x4:4, WPA3, up to 4,8Gbps capacity, BLE

Outdoor Access Points
AP360: IEEE 802.11ax, dual radio, 2x2:2, WPA3, up to 1,2Gbps capacity, BLE
AP460: IEEE 802.11ax, tri radio, 4x4:4, WPA3, up to 4,8Gbps capacity, BLE
AP560: IEEE 802.11ax, dual radio, 4x4:4, WPA3, up to 4,8Gbps capacity, BLE

ExtremeApplications

Extreme Management Center

A better way to manage your complex network from the network edge to the data center.

The network edge is where organizations engages customers and where IoT devices connect. We integrated Extreme Management Center with our Smart OmniEdge solution, so one can deliver customer-driven experiences.

The enterprise campus has become one of the most vexing environments in which to manage IT. Administrators need to rapidly onboard BYOD users and Internet connected devices, quickly deploy the new digital technology that the organization requires, prevent cyber-attacks at every entry point, and do it all while delivering a consistent and personalized user experience. Our Automated Campus solution makes it all possible with simplicity, security, and intelligence that are second to none.

High levels of virtualization, containerization and cloud environments, combined with enormous traffic, limit visibility in the modern data center. In addition, most data centers face challenges adapting to rapid business changes and virtual environments. Most customers have also grown tired of vendor lock-in and want an open flexible environment.
Here Extreme Management Center, part of our Agile Data Center Networking solution, provides a pragmatic path to automation based on multi-vendor architectures. It gives you the granular visibility and real-time analytics, to make data-based business decisions. Our switches and routers are managed by Extreme Management Center through a single pane of glass, which reduces data center administration and offers you the full view of the network, enables embedded data center fabric automation and delivers cross domain automation with our Workflow Composer.

Our Extreme Management Center offers all you need for data-driven insights, visibility and control with one view from the network edge to the data center. We give customers the choice of hardware appliance or virtual appliance, to meet their IT infrastructure needs.

ExtremeManagement

ExtremeControl

ExtremeAnalytics

ExtremeCompliance

Highlights

Automation from Edge to Data Center in One Single-Pane-of-Glass
- Manage your network with automation from a single pane of glass across virtualized and cloud environments
- Bring new service online fast and reduce human error through built-in fabric provisioning
- Free up IT time to drive innovation with integrated cross domain workflow automation and automated device onboarding

Deep Visibility for Data-Driven Decisions and Fast Issue Resolution
- Get in depth visibility of users, end-devices, and applications across physical and virtual machine (VM) traffic through our Virtual Application
- Get business insights into the performance of applications and the network through streaming application telemetry and deep packet inspection
- Mitigate shadow IT and malicious applications with detailed views of workloads in physical and virtual environments

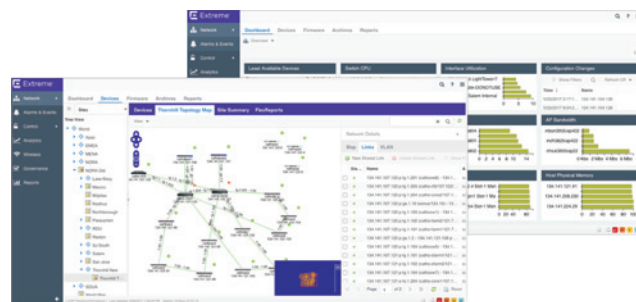**Granular Control to Strengthen Security and Compliance**
- Automatically roll-out consistent policies and automated configuration and compliance monitoring for users and devices
- Enables secure IoT access with real-time policies based on the security posture of IoT devices
- Integrate with existing security applications such as firewalls, MDMs, endpoint security, for rapid and automated mitigation actions

ExtremeControl	ExtremeAnalytics	ExtremeManagement	ExtremeCompliance	ExtremeConnect
Granular policy control	Actionable business insights	Orchestration and automation	Automated configuration compliance	Integration with Vmware, GCP, MS Azure, AWS, OpenStack, Security, etc.
Secure access for users and IoT devices	Network and application performance	Security with hyper-segment	Automate compliance reporting	Open API - Build your own integration
Easy, secure onboarding	Security and forensics	Integrated workflows	GDPR, HIPAA, PCI	

ExtremeManagement
Unified View of Users, Devices and Applications

ExtremeMangement offers a single pane of glass for wired and wireless networks - edge to data center. Zero touch provisioning (ZTP+) helps to bring new infrastructure online quickly. Together with our ExtremeControl it helps to unify the security of all wired and wireless networks with in-depth visibility and control. A granular view of users, devices and applications with an easy to understand dashboard let s you manage inventory and network topology efficiently. Policies and new services such as BYOD can be enabled through the integrated interface of ExtremeManagement and enforced at the network point of entry through ExtremeControl.

Extreme Management Center extends automation from the wireless edge to the data center and across devices of different vendors, so that there is no need to rip out any hardware when deploying our applications. To enhance managing these 3rd party devices, our dashboard shows their topology and discovery.
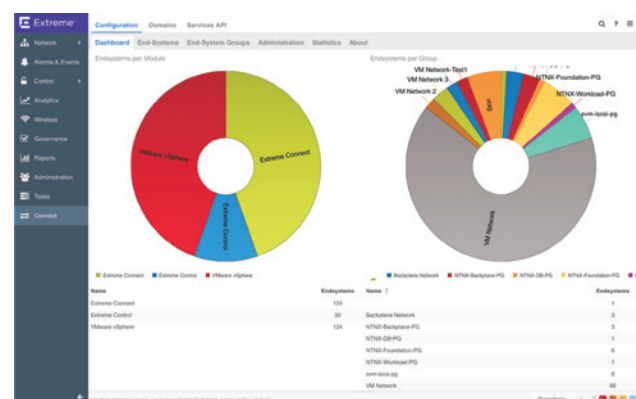
We help to decrease time to service with powerful fabric provisioning built right in. To free up IT time and avoid human error we are offering cross domain workflow automation. Canned workflows for our SLX and VDX switching and routing platforms automate onboarding these devices in a data center. Through the entire network, our applications help to stay compliant with industry standards through automated configuration and compliance monitoring.

Our EXOS switches can be set up as a stack with ZTP+ which enables easy deployment and reduces deployment time. With Fabric

ExtremeConnect
Ecosystem Integration Platform

Management Center is integrated with key enterprise platforms to streamline company business processes, enable more robust data analysis and deliver seamless user experiences. ExtremeConnect offers integration with major enterprise platforms for network security, mobile management, analytics, cloud and data center solutions. Extreme Management Center is integrated into the data center with SLX end-point tracking and integration with VMware vCenter and vSwitch, as well as Distributed Virtual Switches. It offers visiblity and policy provisioning for AWS, MS Azure and GCP.

In addition, we offer a comprehensive suite of open APIs from our network infrastructure portfolio of switches and wireless APs. This includes the classic integration methods like SNMP, Syslog and more efficient integration methods like REST-based APIs (currently under development).

Customers that are using our Extreme Management Center can take advantage of ExtremeConnect to automate day-to-day operations with integrations with third party services like security, mobile device management, analytics, etc.

ExtremeControl

Security Through Visibility and Control

Unify the security of wired and wireless networks with in-depth visibility and control over users, devices and applications. ExtremeControl delivers granular policy controls that enable you to comply to policies and compliance obligations including heterogeneous endpoint environments. Locate, authenticate and apply targeted policies to users and devices as they can easily onboard to the network for secure BYOD, guest access and IoT, all through a single integrated user interface.

ExtremeAnalytics

Insights into Network and Application Performance

Get actionable business insights from your end-to-end network with granular details into the performance of applications and the network through application telemetry and deep packet inspection (DPI). This application speeds up troubleshooting by separating network from application performance so you can quickly identify root -causes. It monitors shadow IT, identifies and reports malicious or unwanted applications, and helps with security compliance.
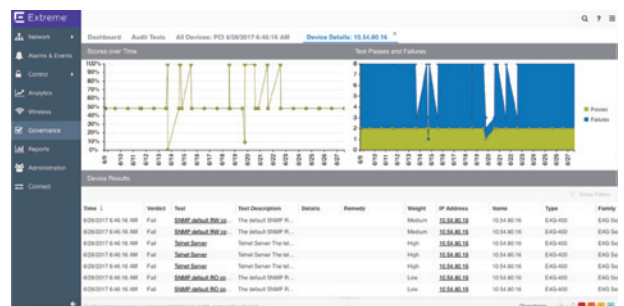

Our ExtremeAnalytics Virtual Analytics Sensor extends application visibility from physical to virtual environments. It eliminates virtualization blind spots with visibility and application performance measurements between VMs on the same host or across hosts on a VMWare virtualized data center. With deep packet inspection, network managers can see and analyze network traffic across multiple layers for real-time accurate information analysis.

Additionally, integration with AWS, MS Azure and GCP provides a unique capability of a single analytics toolset

ExtremeCompliance

Reduce risk and ensure your network configurations comply to HIPAA, PCI and GDPR with our fully automated ExtremeCompliance product (formerly Information Governance Engine), which analyses and assesses network configurations to help determine compliance readiness across wired and wireless networks.

IT-Union GmbH & Co. KG

BUSINESS IT-SOLUTIONS

www.it-union.eu

KIEL — HAMBURG — KÖLN — FULDA — SCHWEINFURT — STUTTGART — MALTERS (CH)