The Extreme Automated Campus

Fabric, Policy, Management, and Analytics

In an industry that's already defined and continually renewed by innovation, Extreme Network's recent announcement of Campus Automation is one of the most significant advances in campus networking and even for networking IT overall. For the first time, all of the essential technologies, products, procedures, services, and support are gathered together and integrated under a single, comprehensive envelope that is already yielding notably improved performance, security, and reliability for mission-critical networks across even the largest organizational settings – campuses and beyond.

Automation itself has always been an important element in many technologies, markets, and applications. Most familiar, of course, is automation in the form of robots performing mechanical tasks in repetitive and even hazardous settings. The concepts and execution behind artificial intelligence and machine learning are more recent developments, enabling sophisticated computer-based solutions than can, in an increasing number of applications, augment and even replace human involvement in complex problems from machine vision and pattern recognition to, as we'll expand on below, many elements of network operations. The goal here is today essential to organizations everywhere: Campus Automation applies advances in network architecture, network management, and related technologies, tools, and techniques to improve the reliability, security, performance, and cost-effectiveness of organizational networks across the globe.

More importantly, Campus Automation is already well beyond the zone of mere interest and research. Instead, it has become an imperative as the network of today is, by analogy, the circulatory system of the organization. Information is in fact a lot like blood – if it can't get where it needs to go, damage often results, and if it leaks, essential security and integrity are likely in doubt. But it's now possible, even as demands on networks continue to grow, to operate and manage large-scale networks with less effort and risk than has ever been possible before, thanks to Campus Automation from Extreme Networks. The keys here are Fabric-based networking, policy-centric network administration, advanced single-pane unified network management, and sophisticated in-depth analytics.

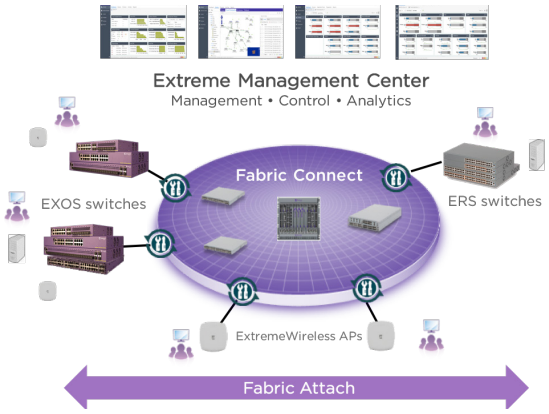


Figure 1: Components of the Automated Campus

Motivations for Campus Automation: Managing Growth, Costs, and Risks

Growing networks, constrained IT budgets, and constant threats to security keep more than a few network and IT managers up at night, and the core challenges to network operations are today quite clear, as follows:

- **Increasing Demand** – Ever-growing numbers of users, devices (and often multiple, simultaneously-in-use devices per user), and a very broad range of applications often with broadband and/or time-bounded constraints, are the major drivers of network growth. New applications and initiatives, including the Internet of Things (IoT), mobility and mobile-first deployments, Cloud-centric IT, enhanced security (to the edge of the network and even into user devices), real-time analytics to understand issues and spot trends, artificial intelligence and machine learning to maximize productivity, and even augmented and virtual reality also place strains on and point out flaws in inadequately-provisioned, poorly-architected, or simply obsolete networks.
- **Reducing Time-to-Solution** – Networks can consume a more-than-considerable amount of time and effort in requirements planning, network design, configuration and deployment, ongoing operational management, and for new installations, extensions to coverage and capacity, reconfigurations, moves/adds/changes, and, of course, upgrades to address growing traffic demands and user/device/application-traffic volumes. The often-significant number of diverse elements required in a given installation, both hardware and software,

demand significant staff time and can consequentially have an adverse impact on operating expense (OpEx), as OpEx has been (historically, anyway) labor-intensive. The solution, though, is now easy: improve network flexibility and operations-staff productivity, both key benefits of Extreme Campus Automation.

- **Managing Complexity** – All too often, the piecemeal/piecewise growth strategy typically historically applied in organizational network evolution results in too many tools, procedures, and techniques at work, precluding fast responsiveness, optimal operations staff productivity, and the degree of accuracy and efficiency required to keep end-users productive as well. A key goal here must be, of course, to reduce the number of "moving parts" required to build and operate any campus network, via automation and consolidation of function into architectures taking advantage of that automation.
- **Optimizing Security, Reliability, Resilience, and Integrity** – Since there is no such thing as absolute security, network operators must maintain constant vigilance over their infrastructure. While necessary, however, such is nearly impossible with traditional networks, given the number of physical elements required, often managed separately. A more integrated strategy, based on the concept of a network Fabric, however, can provide a greater degree of ongoing security, with this feature inherent in the Fabric itself. Ditto for improving overall integrity and reliability as well, and in building networks that eliminate single points of failure – the ultimate in the resilience so essential to organizational success today.
- **Reducing Costs** – Finally, as we noted above, network operating expenses increase with complexity, so traditional interoperability can in fact have a major financial downside (see the sidebar, Campus Automation: The Analyst Perspective, for more on this). Sure, it's possible to build traditional networks that, when running correctly and optimally, anyway, get the job done – unfortunately, they often embody such high operating expenses that cost becomes the overriding factor controlling the evolution of the campus network overall.

Fortunately, it's now possible to address all of the above issues and concerns – and Extreme Networks once again leads the way with solutions centered on advanced, effective Campus Automation.

Campus Automation: Fabric-Based Networking

Extreme's strategy for Campus Automation begins with re-thinking the way networks are conceived, designed, deployed, and managed. At the core (so to speak) is a Fabric-based approach to network architecture – one of the most important advances in the entire history of networking itself.

A Fabric-based network is best thought of as analogous to that more-familiar (for most, anyway) fabric: cloth. Many different forms of cloth are available of course, each designed for a specific mission or application. But all are based on a simple building-block: the thread. Critical here is that individual threads disappear into a given piece of cloth, resulting in an individual and specific fabric that has the form, function, and strength to meet any specific clothing or similar challenge.

Extreme's Fabric-based networks follow this concept. There's no single kind of thread, of course; the familiar building blocks of access points, Ethernet switches, routers and software are still hard at work. So the best way to view Extreme's Fabric-based approach is as an abstraction – network planners, designers, and operators think in terms of functions, goals, and policies, not concrete and often low-level and detailed operations performed on each functional element.

For example, the traditional and very labor-intensive and error-prone hop-by-hop provisioning or configuration otherwise required is eliminated. All operations, including those related to the provisioning of specific services, concern only the edge of the network. The network core is in fact hidden except to certain authorized staff, and both the core and the aggregation are zero-touch in operation. The often-overused term "stealth" is in fact very appropriate here; the actual topology and individual services are hidden from users, most operations staff, and, importantly, hackers and other threats, enhancing both security and integrity.

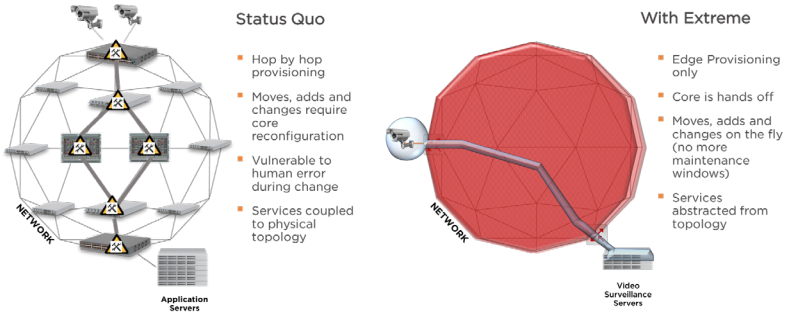


Figure 2: Fabric Connect Eliminates Touch Points

Getting just a little technical, Fabric-based networks have one other very important feature: they are the successor to the diverse (to say the least!) set of protocols developed over the history of networks. Each of these was designed to solve a specific challenge at the time of their development, resulting in a disjoint, stepwise, and essential stopgap evolution of network function. These include such popular and widely-deployed capabilities such as multi-protocol label switching (MPLS), open shortest path first (OSPF), border gateway protocol (BGP) and many more – all of which "work," in the general sense, but all of which include a high degree of interdependency and complexity that invites the opportunity for error and fragility with consequential unnecessary costs.

Instead, Extreme has applied a single protocol – Shortest Path Bridging (SPB), standardized as IEEE 802.1aq and IETF RFC 6329. This technology delivers the full breadth of desired integrated network services including Layer 2 virtualized services, Layer 3 virtualized services (with multiple Virtual Routing and Forwarding instances), and fully optimized IP Routing and IP Multicast services. As a result, Extreme's Fabric-based architecture enables organizations to migrate away from a host of legacy overlay technologies (again, such as STP, OSPF, RIP, BGP and PIM) and to enable all services with a single technology. The result is simplified provisioning with a high degree of simplicity, along with dramatically-lessened opportunities for misconfiguration and sub-optimal performance, improved uptime, scalability, efficiency, performance, stability, and reliability – and, of course, lower operating expense.

Illuminating a bit more here, multicast services, important for many applications today, are implemented with a requirement for PIM (protocol-independent multicast)-based protocols which are notoriously complex to operate, configure, and manage. Extreme offers highly efficient, scalable multicast that doesn't rely on any PIM protocols at all. The result is vastly enhanced scale, performance, and reliability for applications that rely on multicast – with the added benefit of a dramatic simplification of multicast configuration.

Figure 3: Fabric Connect Simplifies the Network

The benefits of Campus Automation in a Fabric-based network are clear:

- **Improved Management Staff Productivity** – Extreme's Fabric-based networks enable faster implementation, configuration, troubleshooting when required, and application deployment, all the end result of the Campus Automation essential to Extreme's solutions. There's less opportunity for misconfiguration resulting from human error, and improved stability also yields lower costs. Services can easily be defined and provisioned (and eliminated when no longer required), and required changes and updates can be performed easily on-the-fly without disruption – and without time-consuming and expensive weekend and evening change windows. The bottom line: enhanced productivity and reduced costs for changes.
- **Simplified On-boarding of Users and Devices** – With the expected surge in IoT devices that are going to need to be supported on campus networks, user and device connectivity must be secure, and must also be plug-and-play. Through a combination of policy and Fabric technology, both users and devices can be identified and then automatically connected to the services they have permission to use – regardless of where and when they are connecting, eliminating the need to hard-wire or pre-provision ports.
- **Increased Network Performance** – This extends well beyond throughput alone, and includes responsiveness and the ability to handle time-bounded traffic like telephony and streaming HD video. The key here is optimized routing, yet another benefit of Fabric-based networking and Extreme Campus Automation.

- **Improved Reliability and Resilience** – While outright hardware failures are indeed very rare today, a cable or power cord might be inadvertently unplugged. This means that load sharing and load balancing and the ability to automatically re-route traffic are essential. An automated campus network also yields enhanced resilience, as the protocol overlays that require each layer to wait for the layer beneath it before connectivity can be re-established (e.g., STP, OSPF then PIM) are eliminated. Services operating at upper layers are thus unaffected by failures of any form. Note again that all of this functionality is provisioned at the edge only; the core is hands-off, including whenever intentional moves/adds/changes and other reconfiguration are required.
- **Enhanced security** – A good number of primitive solutions designed to enhance security today remain in operation, but these often force network managers to accept complexity and degraded resilience in order to secure the network to meet local policies. What's needed instead is true traffic isolation, known as hyper-segmentation, that isolates specific traffic at L2 or L3 and makes these streams invisible outside a given network segment. Should a breach occur, containment to that segment protects even more sensitive parts of the network, resulting in a true dead-end for the hacker.
- **Enhanced regulatory compliance** – Complying with industry-specific and national regulations and requirements, such as HIPAA, credit PCI, SOX, and many more, is easy with enforcement mechanisms, including hyper-segmentation and stealth, built into the network Fabric and controlled via policy and management features.

Policy-Based Network Administration

As is the case with Extreme's network Fabric, policy-based service creation and access is also an abstraction. Network operators specify what services are allowed or prohibited, what traffic should be prioritized, what users are able to access what services and under what circumstances, and many related capabilities with broad flexibility and customization as required. Policies are set, much like written human-resources or BYOD policies, for example, and then automatically configured and enforced within the Fabric.

But the benefits of automated policy-based administration go well beyond simple mechanics. These include the isolation of critical services, enhanced network integrity, granular control over access to each network segment, simplified access permissions definitions – and, of course, re-definition as policies change over time or in response to specific considerations.

And, finally, policies need to be implemented and enforced uniformly across the network, demanding centralized policy creation, implementation, control, and monitoring. Campus Automation goes a long way toward making this objective easy to realize.

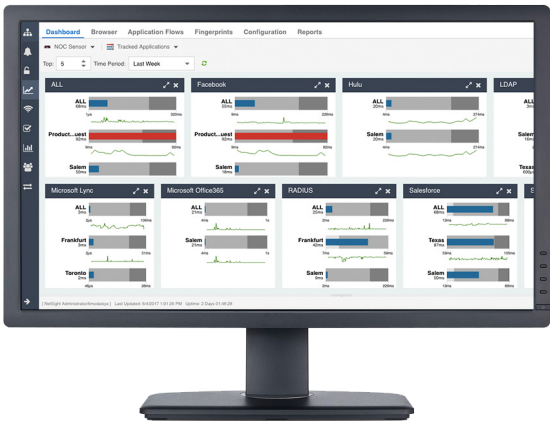
ExtremeControl

Unified, Single-Pane Management

Network management has an unfortunate reputation for complexity, and, as only a relatively few specialized operations staff members have access to the management console, the opportunities for productivity improvements that lower costs and improve the quality of network services are often less than visible to managers. Given the vital importance of management to the success of any network installation, however, Campus Automation also plays a remarkable role in this domain as well.

To begin, a unified wired/wireless, Cloud-based management console functioning across an entire product offering is now essential. Disjointed management services are just as unproductive as disjointed product sets, with the possibility of overlapping settings conflicting with one another and the danger of multiple management databases suffering a similar fate. Management capabilities must be straightforward, easy to use, optimized for a high level of network activity, capable of dealing with large networks carrying mission-critical, real-time data, and provide the visibility and control to efficiently enable simplified, real-time reconfiguration seen regularly as moves, adds, and changes.

And, finally, the management console must be integrated with and driven by policy specification as described above and integrated with network analytics for enhanced visibility, proactive problem detection and resolution, and rapid resolution of challenges should these occur.

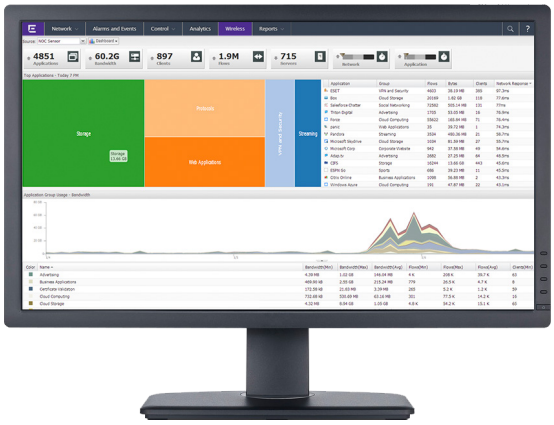


ExtremeManagement

Insight, not Data: Advanced Analytics

Analytics as a concept has been with us for some time, primarily applied to complex scientific and technical computing problems. The concept is simple: process large amounts of often uncorrelated, diverse, disjointed, multi-dimensional, and multi-variate data to discern patterns, quantify issues, and select appropriate actions. Potentially vast amounts of operational data and statistics are gathered in the normal course of network operations, but this data cannot be consumed directly by operations professionals – there's simply too much of it, and even the sharpest minds glaze over when confronted with reams of numerical data.

Properly implemented, network analytics provides the 360-degree, real-time view of everything happening in the network, and yields not just numbers, but actionable intelligence and insight that enable operators to spot and fix problems even before they impact network performance, security, integrity, or end-user productivity. Analytics represents one of the most important (and, today, essential) elements of Campus Automation, and it's now difficult to imagine operating a campus-scale network without this facility.



ExtremeAnalytics

Solutions

Extreme is the leader in Campus Automation, providing solutions that enable the vision we've outlined above to be brought to fruition in networks everywhere. These include the following:

- **Extreme Management Center** – Extreme Management Center is a single-pane unified (wired and wireless) console that operates across the entire Extreme product line – all hardware and software elements of a Campus Automation solution.
- **ExtremeControl**™ – Designed to enable granular policy definition, manage security, and support contemporary IT initiatives like BYOD and IoT, ExtremeControl authorizes both users and devices. It's a standards-based, multi-vendor interoperable access-control solution for wired and wireless LAN and VPN users. ExtremeControl integrates with a wide range of authentication and authorization facilities, for unmatched flexibility and scope of control.

- **ExtremeConnect** – ExtremeConnect provides a set of open APIs that enable the integration of third-party products and services, including security, mobility, management and analytics, and data center and private cloud. So no matter what your IT environment or set of application requirements, ExtremeConnect provides the glue to build world-class solutions.
- **ExtremeManagement** – Includes all functions required to plan, configure, deploy, control, monitor, and optimize campus networks with remarkable ease of use for operations staffs.
- **ExtremeAnalytics** – As we described above, a network analytics facility is today the only way to really understand what's going on inside large-scale networks. ExtremeAnalytics enables operations and other professionals to quickly make discoveries that would otherwise remain hidden, so that threats to performance, security, and integrity can be remediated often before they cause harm.
- **Fabric Connect** – Fabric Connect is Extreme's advanced implementation of the Shortest Path Bridging protocol at the heart of Campus Automation, and sits at the heart of Campus Automation. It enables both Layer-2 and Layer-3 virtualization, network hyper-segmentation, virtual and optimized routing and forwarding, PIM-free multicast, and much more. As we noted above, all services are defined and configured only at the edge of the network, enhancing security and overall network integrity.
- **Fabric Attach** – Fabric Attach is a feature that enables non-fabric-enabled device integration into the Fabric Connect architecture. Fabric Attach communicates upstream to Fabric Connect and ExtremeControl, and enables users and devices connected to Fabric Attach enabled devices to directly access Fabric-based services.
- **Extreme Service and Support** – Rated Number one in the industry in a Gartner peer review, Extreme's talented and highly-trained support professionals are a 100% in-sourced team of experts in products, services, and applications. The average tenure of Extreme's support staff is more than ten years, and each member of the support team have a goal of first-call resolution of issues and overall customer satisfaction – in fact, over 90% of calls to support are resolved by the first staff member contacted.
- **Fabric Connect and VMWare NSX Integration** - Fabric Connect-enabled switches support an integrated hardware virtual tunnel end-point (VTEP) that provides a VXLAN gateway functionality that uses the Open Virtual Switch Data Base (OVSDB) Control Plane Protocol. This functionality enables the seamless integration of an Extreme Fabric Connect network domain with a VMWare NSX controller-managed overlay network. Network segments can be seamlessly and redundantly extended from the NSX domain to the Fabric Connect domain by mapping the overlay Virtual Network ID (VNIDs) to the ISIDs directly within the NSX controller.

The bottom line: Extreme Campus Automation is a unique set of architectural, strategic, and product and service offerings that enable unprecedented simplicity, security, and cost-effective solutions to network installations of any size, scale, or mission. There is no more intelligent and effective set of Campus Automation capabilities anywhere on the planet.

Conclusions

The network as the circulatory system of the organization? Absolutely – that's what networks have become. The network is the essential facility that makes information resources available wherever they need to be reliably, securely, efficiently, and cost-effectively.

The availability of Campus Automation from Extreme Networks represents a breakthrough in accomplishing this mission with unprecedented ease. Fabric-based networking provides a framework for specifying, configuring, operating, and growing networks that is inherently simpler, more secure, and more reliable than legacy architectures. Extreme Campus Automation reduces time to solution, improves security and integrity, and lowers costs across the life cycle of any campus or other medium-to-large-scale network installation. With networks operable as Fabrics, simplified policy definition and enforcement, single-pane cross-element unified management, and unparalleled analytics, networks can be transparent, self-healing, and easy to use, thanks to the advances in network architecture, operational strategies, and the new products and services that we've discussed in this White Paper.

Extreme Networks is ready to take on any network challenge. We're ready to show you how Campus Automation can benefit your network – and your organization – today.

The Analyst Perspective

Given the comprehensive, paradigm-shifting nature of campus automation, the analyst community has been hard at work both synthesizing meaning and forecasting how the future of networking and even IT overall are influenced by its arrival.

We recently spoke with Craig Mathias, Principal at Farpoint Group, for his perspective on the broad range of developments we've discussed in this White Paper. Craig has spent his entire (more than 40 years) career in high tech, with the past quarter century devoted to emerging networking technologies, wireless communications, and mobility, which have clearly been major drivers of networking and IT in their own right.

"While the technologies involved are fascinating, let's cut to the chase," Craig told us. "The most important opportunity today is in boosting productivity, and not just that of the end-users the network is, in fact, built to serve. Instead, we need to look at key possibilities in enhancing the productivity of network planners and network operations managers and staff. That's where Campus Automation truly presents an irrefutable and overwhelming set of arguments for its adoption."

Extreme's newly-integrated Fabric is already field-proven in the product lines recently obtained in the acquisition of Avaya Networking. Adding in policy administration, comprehensive and unified network management, and advanced analytics constitutes a complete solution irrespective of organizational mission. "It's certainly reasonable that a network be viewed as a cost center, as it represents overhead rather than a revenue generator by itself," Craig continued. This provides additional motivation to reduce operating expenses, which is precisely what Extreme's product and service set offers. Being able to administer the network Fabric via abstractions, rather than as (often CLI-based) operations in individual network nodes and segments, means that operations staff productivity could not be greater, and opportunities for errors are dramatically reduced. Security and integrity are also both enhanced. Every organization should consider this approach."

Craig concluded our conversation with a noteworthy observation: "networks only grow over time. The historic mix-and-match interoperability of network components and stepwise and piecewise refinements initially embodying new innovations has encouraged, however, solutions that are complex to understand and manage. Extreme Networks has now changed all that – and as demands on networks continue to grow, these innovations could not have arrived at a more opportune moment in history."