Automated Campus Solutions for the Enterprise

Extreme Fabric Connect: Paving the Way to Digital Transformation

Digital transformation — driven by the desire of enterprises to be more agile and competitive — has become a top mandate for almost every IT and business leader. But the success of this transformation is intertwined with the enterprise network. As IoT devices continue to proliferate, applications become more networked, and security ever more paramount, the network is the key to this transformation. A simpler and more flexible network architecture is required, in particular one that doesn't require a trade-off with security or resiliency.

Delivering Value

So-called MAC's (Moves, Adds and Changes) have always been on top of mind for network operators. Enterprise networks need to constantly adapt to the ever-changing business needs. In addition, security requirements have become ever more stringent.

Extreme Automated Campus – a software-enabled networking architecture – fully automates "MAC's" and provides a highly efficient, easy-to-operate network infrastructure. It also allows segmentation of the network into securely separated zones available anywhere across the network infrastructure. Wired and wireless end-points can be dynamically placed into their corresponding secure network zones and, if applicable, predefined traffic policies applied automatically.

With Extreme Automated Campus, a "zero-touch" enterprise network infrastructure can be deployed. End-points, based on their access rights, can connect anywhere to the infrastructure and automatically gain controlled access to their assigned network services – without the need for a network operator to adjust any configuration.

Inherent Automation and Central Orchestration

Endpoint-attachment automation for wired and wireless end-points with policy enforcement: A centrally-orchestrated Network Access Control (NAC) and Policy Framework allows zero-touch end-point authentication and dynamic application of end-point policies anywhere in the infrastructure. The NAC and Policy Framework, using standard authentication mechanisms (e.g., EAP/NEAP), ensures that end-points join their assigned network service. Their access rights and policy attributes then follow them throughout the infrastructure, whether they are wired- or wireless-attached.

Plug-and-play deployments and zero-touch core: Based on the NAC authentication, policies are not only dynamically applied to the user or device joining the network, but the correct network services (e.g., IP Subnet) and secure zones (e.g., VRF) are also extended to the attachment point of the device. By leveraging Fabric Connect as the core routing infrastructure in an Extreme Automated Campus, all routing needs are handled by one routing protocol – whether for IPv4 or IPv6 bridged, unicast or multicast traffic, including VRFs. This reduces overhead and simplifies deployments significantly. Extending network services across the Automated Campus network is typically done at the network access point only and does not require any configuration changes in the network core.

Integration with VMware NSX: An Automated Campus network can also be seamlessly integrated with an VMware NSX controller-managed overlay network. Fabric Connect-enabled switches support an integrated hardware virtual tunnel end-point (VTEP) that provides VXLAN gateway functionality using the Open Virtual Switch Data Base (OVSDB) Control Plane Protocol. Network segments can be seamlessly and redundantly extended from the NSX domain to the Fabric Connect domain by mapping the Network Virtual ID (VNIDs) to the Fabric Connect ISID's directly within the NSX controller.

SDN vs. Software-Enabled Networking

In contrast to an SDN networking approach – where all switching elements of a network are programmed by an external controller – the Extreme Automated Campus approach leverages an extensible Link-State Protocol (IS-IS RFC6329 and IEEE 802.1aq) for its end-to-end network automation. Using a network protocol, instead of an out-of-band external mechanism, provides the significant benefit of a built-in self-healing capability, making it extremely robust and scalable.

External automation requirements to tie the network into business workflow requirements can be satisfied either by Extreme Management Center (XMC), with its built-in workflow composer capabilities, or by an external workflow composer tool. Northbound interfaces are provided either by XMC's REST interfaces or by direct programming to the REST interfaces of the switching elements.

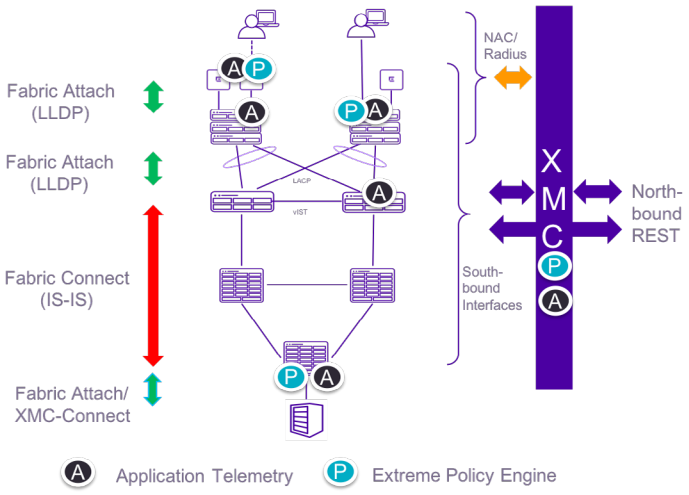

Figure 1: *Deeper Dive - Automated Campus Protocols*

Fabric Attach, an LLDP-based service signaling protocol, is used as the fabric attachment infrastructure to signal service attachment from the wireless access point all the way to the distribution layer enabling a seamless automation mechanism without the need for any manual network scripting.

Optionally, Open Virtual Switch (OVS) based servers can leverage Fabric Attach capabilities as well.

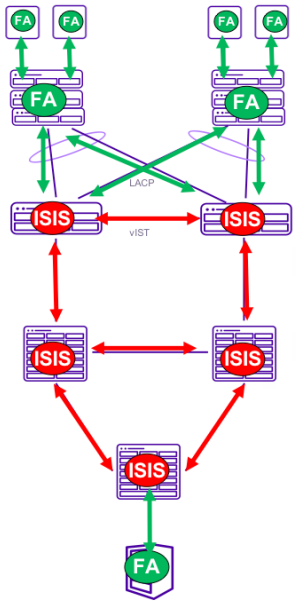

Figure 2: *Fabric Attachment Infrastructure*

Network Services in an Automated Campus Infrastructure

Typically network operators think in terms of VLANs, IP Subnets and VRFs. Those connectivity configurations are treated as network services in an Automated Campus infrastructure and are named Virtual Network Services (VSNs). VLAN extensions across a network infrastructure are called L2 VSNs, VRFs extended across the network are called L3 VSNs. The ease of extending VSNs across an Automated Campus, and the fact that only one instance of IS-IS is being used for any routing function, ensures the simplicity of the Automated Campus solution.

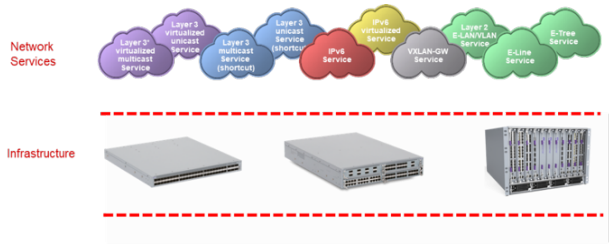

Figure 3: *Abstracting Service from Infrastructure: Network as a Plug and Play Utility*

Evolving a Network to an Automated Campus

While green-field deployments are the most straightforward option for a new Automated Campus deployment, so called brown-field deployments are more common. Since any common bridging and routing protocol is supported by an Automated Campus solution, it can seamlessly interface to an existing infrastructure. Thus, solutions where one building is operated as an Automated Campus while another building is running in traditional mode are very common. If the benefits of an Automated Campus are needed while leaving the traditional network in place, Extreme Fabric Connect provides the ability to build an overlay infrastructure over the existing infrastructure – without the need to rip and replace the existing network. This overlay, for example, could allow a VRF-based IP multicast service to be extended anywhere required, without the need to build a multicast-enabled underlay network.

A common approach to migrating a traditional network to an Automated Campus solution is to extend the existing network core with a pair of Extreme Fabric Connect core nodes and migrate the distribution layers over to the new core over time, thus slowly gaining the benefits of full network automation.

An Automated Campus solution allows scaling networks not only to tens of thousands of network switches and access points, but also allows spanning the network fabric across long distance links – even around the globe if required. The benefits of an end-to-end automated network solution can thus be extended beyond a single Enterprise Campus.

Extreme Management Center™

The Extreme Management Center user interface unifies all the capabilities in a single easy-to-use web-based interface. With Extreme Management Center, critical network information is accessible and easy to use. This powerful tool enables both managers and technical staff to be more efficient in their provisioning, monitoring, reporting, analysis, troubleshooting and problem-solving tasks.

Dashboards streamline network monitoring with consolidated status of all the devices and the ability to drill down for finer detail. State-of-the-art reporting provides historical and real-time data for high level network summary information and/or details. The reports and other views are interactive, allowing users to choose the specific variables they need when analyzing data. Web-based FlexViews enable real-time diagnostics.
Inventory Management - Automates management of device configurations, firmware, and hardware/software inventories. It also provides tools to capture, modify, load, and verify. It also provides tools to capture, modify, load, and verify configurations

User Interface - Unified web-based interface and fine-grained interactive search for network analysis, problem solving, help desk visibility and reporting

Alarm Management - Core to any management platform, provides event-based and performance-based alarms indicating trouble or potential trouble areas

Application Analytics – Extreme Analytics analyzes context-based application information to deliver business insights on applications, users, locations and devices. These insights help you improve the security posture of your organization and track shadow IT, unapproved, malicious application

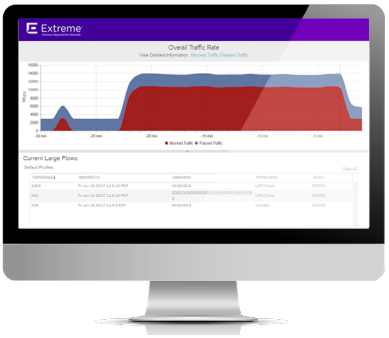

Figure 4: *Extreme Management Center Application*

Automated Campus Fabric Management – Fabric Manager not only visualizes the fabric configuration and service distribution and forwarding paths, it also enables extensive GUI based provisioning capabilities.

ExtremeControl – Controls user and device access across both wired and wireless networks with granular visibility and in-depth control. It matches endpoints with attributes, such as user, time, location or access type, to create an all-encompassing contextual identity. This identity then follows a user, no matter from where or how they connect to the network.

Extreme Connect – Provides a set of open APIs to enable the integration of third party software and products with Extreme Management Center. This includes integration with other management platforms, such as VMware VSphere and Citrix, to build world-class management solutions.

Extreme Automated Campus Components	
Function	**Porftfolio / Network Nodes**
Core and Aggregation nodes	ExtremeSwitching Virtual Services Platform (VSP) switches
Access Switches	ExtremeSwitching EXOS and ERS switches
Wireless Access Points	Extreme Wireless and Extreme Wireless WiNG APs
Network Management	Extreme Management Center

Summary

Extreme Automated Campus provides inherent end-to-end network automation, visibility and analytics on top of a market proven, standards-based network architecture. Using Extreme's Automated Campus solution, you can:

- Enable end-point mobility, security and segmentation through a fully automated controller-less Ethernet Fabric solution
- Optimize agility for typical Moves, Adds and Changes (MACs) throughout your infrastructure
- Improve operations with pervasive traffic visibility to quickly identify problems, accelerate mean-time-to-resolution, and improve overall service levels
- Accelerate business innovation through powerful north-bound interfaces for flexible network programming
- Leverage the plug-and-play capabilities of the network infrastructure to quickly deploy new projects, while avoiding schedule maintenance windows for every network change

Extreme™
Customer-Driven Networking

http://www.extremenetworks.com/contact