Extreme networks

White Paper

Table of Contents

Fabric Attach Network Automation

Automated Service Attachment for Enterprises

Abstract

One of the key benefits of Extreme Fabric Connect (an enhanced implementation of IEEE 802.1Q Shortest Path Bridging) is simplified operations by replacing current hop-by-hop provisioning practices with edge only provisioning. Fabric Connect delivers a "Zero-Touch-Core" that virtually eliminates the chance of core network misconfiguration.

Extreme Fabric Attach further extends the zero-touch core to the wiring closet by enabling attachment to Fabric Connect virtual services on switches that do not support SPB. Fabric Attach provides automated service creation and attachment for Fabric Attach capable network elements as well as users and IoT devices, either directly on a switch or centrally via RADIUS authentication.

1. Overview

One of the key benefits of Extreme Fabric Connect (an enhanced implementation of SPB) technology is simplified operations through access layer network provisioning. Fabric Connect delivers a "Zero-Touch-Core" that virtually eliminates the chance of core network misconfiguration. It allows simple and secure deployment for any type of network service without the need to make any configuration changes on intermediate/core nodes, even in environments where clients roam.

Extreme Networks developed "Fabric Attach" to extend these same benefits to network elements or hosts that are not Fabric Connect/SPB capable. Extreme Fabric Attach (FA) extends Fabric Connect to deliver an "Autonomic Edge" capability that dramatically reduces the costs of adding new or modifying existing services. Any FA capable device (a switch, server, WLAN AP, IP Camera, etc.) can now be securely connected to the network, authorized for a network service, and attach to the appropriate network service instance – all

automatically and based on policy. This enables Fabric Attach devices to come straight out of the box and can be provisioned onto the network with "Zero Touch"!

Imagine if your operations team could roll out new application services instantly, without the associated risks of touching most or all of your network devices. Extreme commissioned an analysis of Fabric Connect customers with Market Dynamics a couple of years ago. The findings were telling; Fabric Connect customers spent 85% less time and effort configuring their networks to turn up new services. Additionally, on average, Fabric Connect customers went from averaging 3 "human caused errors" during configurations to zero per year.

This Extreme Networks paper explains what Fabric Attach is and how it is used in solutions to automate network service creation and attachment, and removal when a service is no longer required.

2. Fabric Attach – the Ecosystem and Solution

Fabric Attach (FA) fundamentally introduces fully automatic attachment to network services for end users, virtual machines and IoT (Internet of Things) devices to a network infrastructure. Fabric Attach and Fabric Connect are key building blocks of the Extreme Networks Campus architecture.

Fabric Attach enables auto-attach of access layer and edge devices as well as the automatic creation of network services. All network infrastructure supporting Fabric Attach can dynamically create and configure the required services right up to the Fabric Connect core network infrastructure. When the Extreme Control policy engine is in place, it can be used to authenticate and authorize both network devices and users, then create the VLAN and fabric services to automatically connect the user or end device with the appropriate policy and permissions.

2.1 Fabric Attach Elements

It is important to first understand the Fabric Attach "Elements" that provide the automation. The following components detail the functions that each of the Elements deliver.

Fabric Attach uses the Link Layer Discovery Protocol (LLDP) as transport to exchange FA Element and Assignment TLVs between two neighboring systems. In the FA framework, these systems are defined as Elements and their functions are listed below;

Fabric Attach Elements:

- **FA Server:** A switch at the Fabric edge enabled as an FA Server that supports FA Proxy switches and FA Client devices. SPB based FA Servers are Backbone Edge Bridge (BEB) switches that receive requests to create and map VLANs to I-SID based virtual services. VSP and Universal switches are typically deployed as FA Servers
- **FA Proxy:** A non-fabric enabled Extreme switch in FA Proxy mode. FA Proxy switches are wiring closet switches connected to an upstream FA Server Switch. FA Proxy are always switches supporting directly attached users or end devices non-FA devices or FA Client devices. ERS switches and EXOS switches can be deployed as FA proxy switches.
- **FA Client:** A network attached device running the FA agent in FA Client mode. FA Clients can be WLAN Access Points, Open vSwitch, Industrial Ethernet switches either from Extreme or through a third party or IP

Cameras. FA Clients typically request VLAN to I-SID service assignment mappings from the network. They are also the endpoint in the FA ecosystem.

- **FA Policy Server:** Extreme Control RADIUS server, when used in FA solutions, fully automates the provisioning and configuration of services based on centralized authentication (EAP or MAC) and authorization policy of the end-user or end-device. Network service creation (VLAN:I-SID, or VLAN only) can be signaled to the FA Proxy Switch.

2.1.1 Element Connection Model with Fabric Connect

Fabric Attach was initially created to provide an extension of Fabric Connect services to the network edge/access layer with automated service attachment. The basic FA Element connection model requires that an FA Server be in place to support directly connected FA Proxy switches and FA Client devices. Only one FA Element is permitted per port on an FA Server or FA Proxy switch. Physical link redundancy Link Aggregation Group/Multi-Link Trunking (LAG/MLT) is supported if the Element model is followed from a logical connection manner. The LAG creation can even be dynamically generated on Fabric Attach capable EXOS-based switches, provided they are running ExtremeXOS 31.1 (or later). Therefore, when a switch receives Fabric Attach element Type-Length-Value (TLV) based data on two or more ports that have same System-Id, same SMLT-Id, and have a Connection Type of SMLT, it automatically creates a LAG consisting of those ports.

FA Clients can connect directly to the FA Server switch, or directly to an FA Proxy switch. The FA Server is responsible for processing all service assignment mapping requests to bind VLANs to Fabric Connect I-SIDs. All services downstream from the FA Server port are VLAN based from the FA Client or FA Proxy to the FA Server.

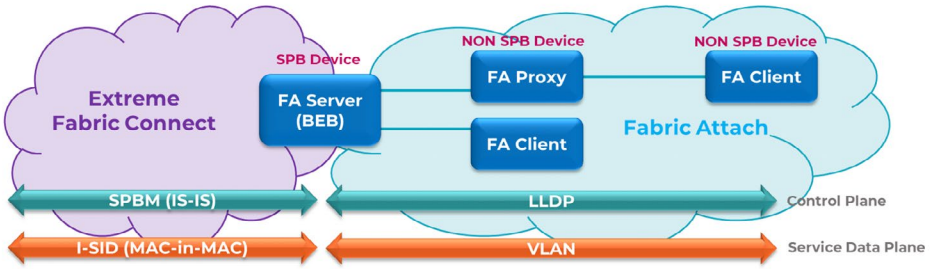

Figure 2.1 – Fabric Attach Element model with Fabric Connect

2.1.2 Non-FA Device Connection Model

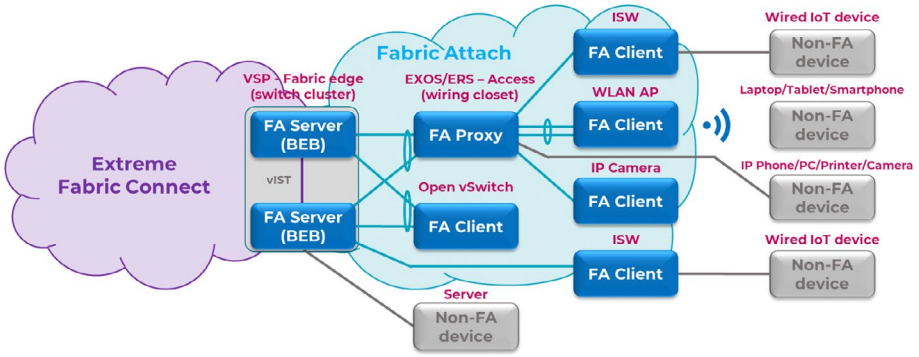

Figure 2.2 – Non-FA Device Connection model with Fabric Attach

Figure 2.2 illustrates the connection of Non-FA devices in the FA connection model. It also illustrates an expanded view of Link Aggregation connections between elements.

Non-FA devices are users or any IoT type device such as IP phones, printers, medical devices, building sensors etc, either wired or WiFi. Non-FA devices are typically connected to wiring closet switches (but not limited to them).

Fabric Attach can auto-attach any FA Client device, automatically building the desired VLAN (typically the management VLAN) with a secure handshake between the FA Server and the FA Client. There are a number of Extreme FA Clients and well as third-party FA Clients in the market today (refer to section 4 of this document).

For the security of Fabric Attach communication in terms of data integrity and authenticity, a keyed-hash message authentication code (SHA-256) can be transmitted within every FA message. By default, on the FA Server/Proxy, message authentication is enabled at the interface level and a default key is defined to provide secure communication. You can configure a different authentication key on an interface (port or MLT) on the FA Server/proxy, to authenticate a client on that interface.

2.2 Fabric Connect Core FA solution

Fabric Attach can be leveraged with a legacy core, as well as, a Fabric Connect enabled core. However, when a Fabric Connect core is present, a full end to end automated service creation and attachment solution can be realized. A Fabric Connect core with Fabric Attach at the access layer provides a completely elastic network infrastructure. One that dynamically creates and extends services when needed and removes or retracts services when no longer required.

All user and device access to the infrastructure can be optionally centrally controlled by Extreme Control to provide authentication, authorization in addition to orchestrating dynamic service creation and attachment at the access layer.

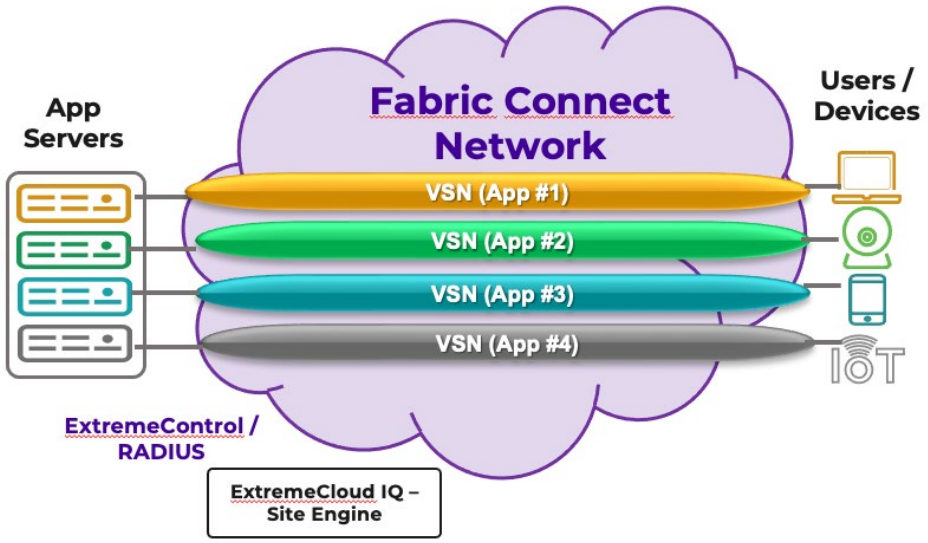

Figure 2.3 – Fabric Connect with Fabric Attach

2.2.1 Extending Services with Fabric Attach

Once a Fabric Attach framework is in place by enabling FA Server and FA Proxy functionality, FA Clients can now be connected to the network edge and request dynamic service extension and attachment. While FA VLAN to I-SID assignment mappings fundamentally create a Layer 2 service connection to a Fabric Connect core, FA can interwork with Layer 3 VPN/VRF services by terminating the L2 virtual network service at the VLAN connected to the Layer 3 virtual network service or VRF.

Fabric Attach works at both the campus as well as the Data Center edge. On the data center side of the network, Fabric Attach works with hypervisors that support Open vSwitch to connect VM applications to a network service. On the campus side of the network, FA Elements are deployed and ready to extend services and attach users and devices to services when they connect.

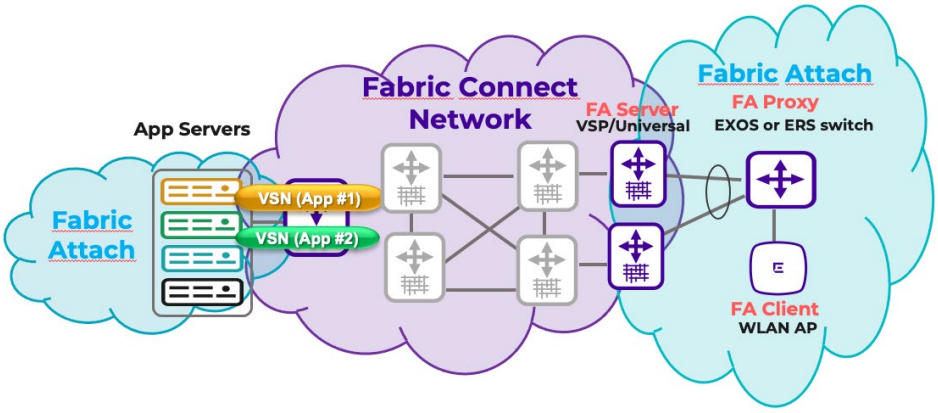

Figure 2.4 – Fabric Attach ready network solution example

As users or devices connect, VLANs are dynamically created, port memberships dynamically changed and virtual service attachment is established. The process of user or device connection to a service is ubiquitous regardless if the user or device is wired or wireless.

Full automation is achieved via a centralized RADIUS server with policy enforcement – such as Extreme Control. Extreme Control/RADIUS provides the capability to signal Fabric Attach functions to an FA enabled switch to provision a local VLAN and map the VLAN to a Fabric Connect service thus enabling the user or device to communicate with the application(s) visible within that service.

If required, configuration can also be manually provisioned directly on FA enabled network elements such as FA Server or FA Proxy switches, and FA Clients that support the FA Assignment TLV.

Figure 2.5 illustrates an example of a wired and Wi-Fi user attaching to one service, plus a wired IP camera attaching to a video surveillance service. The example includes Extreme Control which is used to authenticate users and devices and signal the FA Proxy which service the user or device is to connect to. The ExtremeCampus Controller is used to provision services on WLAN AP39xx and WLAN WiNG series Access Points. The ExtremeCampus Controller can operate independently or in conjunction with Extreme Control for full centralized authentication, policy and service attachment.

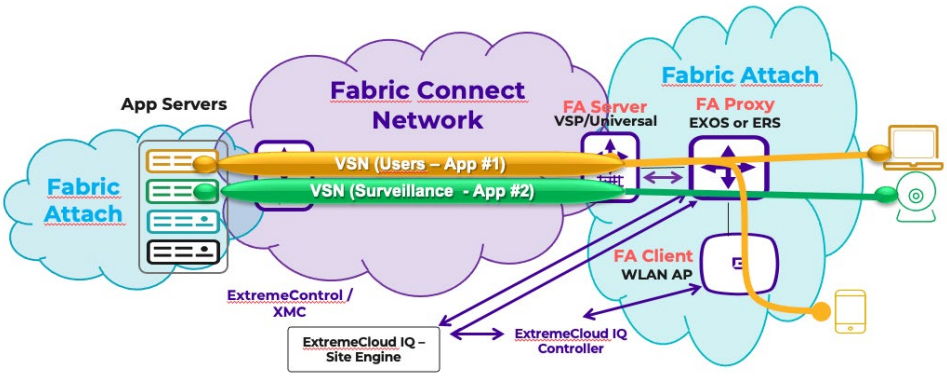

Figure 2.5 – Fabric Attach Service Extension example

2.2.2 Extending Management with Fabric Attach

Fabric Attach can also provide dynamic attachment of FA Elements to a designated management VLAN or management service. The FA Server can be configured to advertise the management VLAN for FA Proxy switches and FA Client devices to use for management plane communication within a management domain. The presence of the management VLAN ID in the FA Element TLV enables a zero-touch function where the FA Proxy or FA Client automatically determines the link tagging mode and the VLAN in which to send DHCP requests for IP management address assignment to the device. This is particularly beneficial for FA Clients that are VLAN aware bridges – such as WLAN AP's and Ethernet Switches.

Figure 2.6 illustrates how a network management service is extended to an FA Proxy and to FA Client devices. The purple arrows depict the direction of the management VLAN ID advertisement from the FA Server switch to downstream FA elements. Extreme FA Clients, such as WLAN AP's and ISW switches use the advertised FA management VLAN to automatically connect their management plane to the network management service.

Figure 2.6 – Fabric Attach Auto Management VLAN Extension

2.2.3 Fabric Attach Zero Touch

Fabric Attach Zero Touch is a configuration option supported on VSP, ERS and EXOS switches (as of 31.3) that enables automated service attachment without the presence of a RADIUS server. The FA Zero Touch feature provide a means of automatically detecting specific FA Client devices and connecting each one to the service that has been pre-configured for that device type. This means the FA Client device can be connected to any switch port, and once detected, FA is triggered locally to create the VLAN, change the port VID assignment and map the VLAN to virtual service for the port the device is connected to.

The following example shows an IP video surveillance camera or FA Client being connected to an Extreme switch. The IP camera and the switch has been configured

to create a VLAN and I-SID for that IP camera. As soon as the Fabric Attach enabled switch sees that specific camera, FA is triggered to create VLAN, update the port VLAN membership and map it to the video surveillance virtual service.

Figure 2.7 – Fabric Attach Zero Touch Functions

Other zero touch functions can be enabled with FA Client detection such as setting port QoS, FA Client trust, and automatic management VLAN assignment.

When the FA Client device is disconnected, all port settings are restored to their previous configuration which provides additional security so that ports do not remain "open" for other devices or users to connected to.

3. Fabric Attach with RADIUS Auth

3.1 Extreme Control/RADIUS

Extreme Control provides centralized authentication and policy control functions for users and devices connecting to the network. At the edge of the network, switches and WLAN AP's provide 802.1X EAP or MAC (Non-EAP) port-based authentication in concert with the central RADIUS server. Whether it is a user PC running an EAP supplicant, or an IoT device MAC address, Extreme Control processes the authentication request and signals back to the switch or AP if the user/device has been authenticated.

The authentication response from Extreme Control can also contain RADIUS FA return Vendor Specific Attributes (VSAs) which can configure and set FA functions. These RADIUS FA attributes trigger Fabric Attach to dynamically create VLAN(s), change port memberships and map the VLAN(s) to virtual service I-SID(s) based on the profile of the user or device ensuring they are each connected to their rightful service.

Figure 3.1 illustrates a user and an IoT device connecting to two different switches using EAP and MAC authentication respectively with each device connected to its appropriate service. The purple arrows signify the authentication signaling while the red arrow signifies FA service assignment requests up to the FA Server for Fabric Connect service attachment.

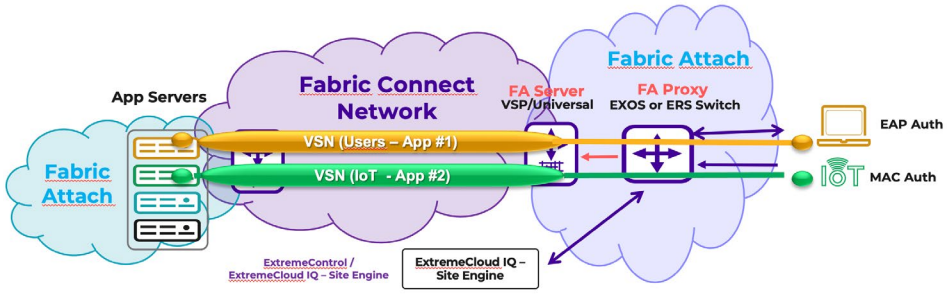

Figure 3.1 – Fabric Attach with RADIUS Authentication

4. Third Party FA Clients

A number of vendors have partnered with Extreme Networks and implemented Fabric Attach Client capability on their products. This enables these third-party products to leverage FA's automatic detection, configuration and network service attachment.

Fabric Attach Client devices can connect to FA Server or FA Proxy switches (reference figures 2.1 and 2.3). When the FA Client is an Ethernet bridge, such as a WLAN Access Point or an Ethernet switch, these devices typically support users and IoT devices. WIFI APs and wired switches usually support 802.1X/EAP or MAC based authentication for users or IoT devices. FA Clients that support RADIUS FA Vendor Specific Attributes (VSAs) have the capability to dynamically create VLANs locally, change port assignment and then signal FA assignments upstream to map a VLAN to a Fabric Connect I-SID to fully automate network access.

Below is a table that lists the current third-party vendors products that support FA Client functionality and the major capabilities within the Client. These are currently split into two broad device categories; Industrial Ethernet switches and Video Surveillance cameras.

Industrial Ethernet switches

Brand	Model(s)	Element TLV	Assignment TLV	RADIUS FA VSAs - 802.1X	Auto Mgmt VLAN (FA mgmt VID)
Hirschmann	HiOS switches (RSP20/25/30/35)	Yes	Yes	Yes	Yes
MicroSens	Industrial Eth and FTTO Microswitches	Yes	Yes	Yes	Yes
Nexans	LAN Active FTTO switches	Yes	Yes	No	No

Video Surveillance IP Cameras

Brand	Model(s)	Element TLV	Assignment TLV	RADIUS FA VSAs - 802.1X	Auto Mgmt VLAN (FA mgmt VID)
Axis	Mid/high end models – requires ACAP*	Yes	Yes	N/A	N/A
Pelco	• Mid/high end models: Sarix, SarixPro. • Spectra Enh, Esprit Enh, Optera, Exsite Enh – 2.11.1.7 • Pro2 (IBP224, IMP, IXP) – 1.16.37 • Enh2 (IME329, IXE, etc.) – 6.4.0.4	Yes	No	N/A	N/A
iPRO	Refer to the following link: iPRO Models	Yes	Yes	N/A	N/A

*Axis ACAP = Applications Capabilities firmware module. Mid to high end Axis cameras require an ACAP file to be loaded on the camera that supports FA Client capabilities.

Video Surveillance cameras fall into the network device category of an end-station. They are a terminating end device without any downstream stations and typically not VLAN aware. Because of this, RADIUS FA VSAs and automatic FA management VID creation are not applicable.

5. Summary

The key benefit of Fabric Attach is not only the automatic and dynamic provisioning of VLAN and virtualized services within a Fabric Connect network infrastructure, but also the removal of those services when they are no longer required. This enables the creation of a secure, elastic and programmable network with services that expand and contract in step with an enterprise's needs.

Extreme Networks provides flexible options to leverage Fabric Attach's automation no matter how big the network infrastructure is by supporting automated attachment locally on a switch or via a centralized authentication mechanism using RADIUS. This enables anyone deploying Extreme Networks switches to fully automate connectivity to their network infrastructure and drastically reduce administration cost and time for adds, moves and changes.