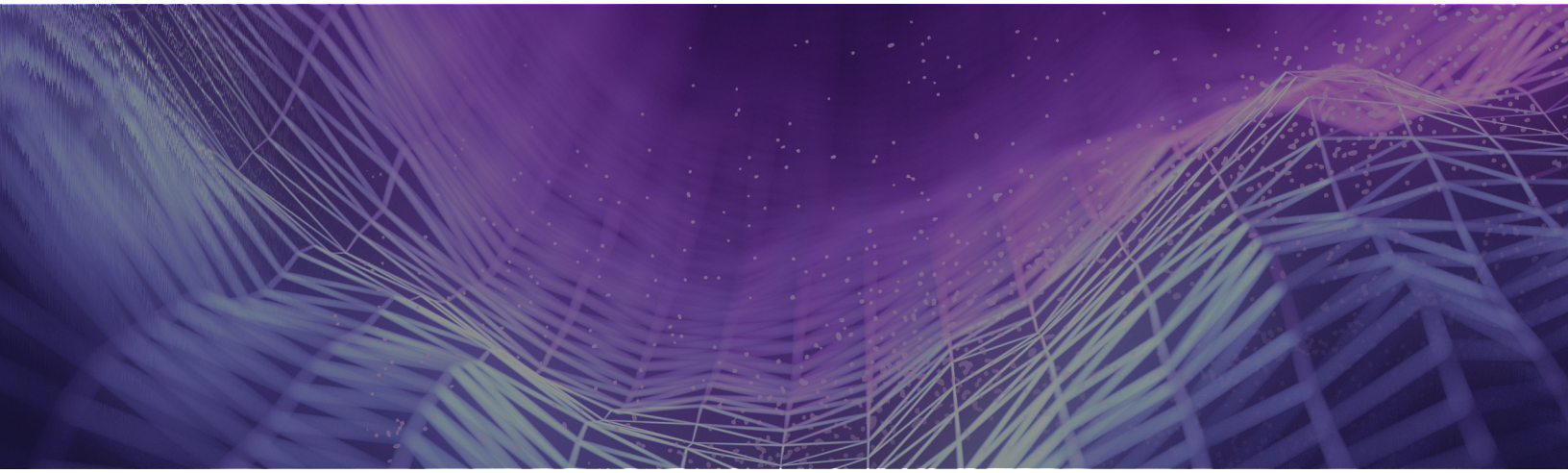


Extending Fabric Connect to the Campus Wiring Closet with Extreme's Fabric Edge Solution

Executive Summary

Enterprise networking requirements have evolved over the past decades, but the basic way networks are being built and operated has largely remained the same.

Driven primarily by IoT, network security through segmentation has become important to ensure that only the devices which are allowed to communicate with each other can do so, while remaining isolated from the rest of the IT environment.

With traditional networking solutions, the connectivity services (VLANs for Layer 2 and IP subnets, VRFs for Layer 3 separation), as well as the physical infrastructure have been tightly coupled. Since connectivity service configuration was locked into the infrastructure, network changes have been complex to implement and have required extensive planning prior to implementation. Network changes typically required long maintenance windows.

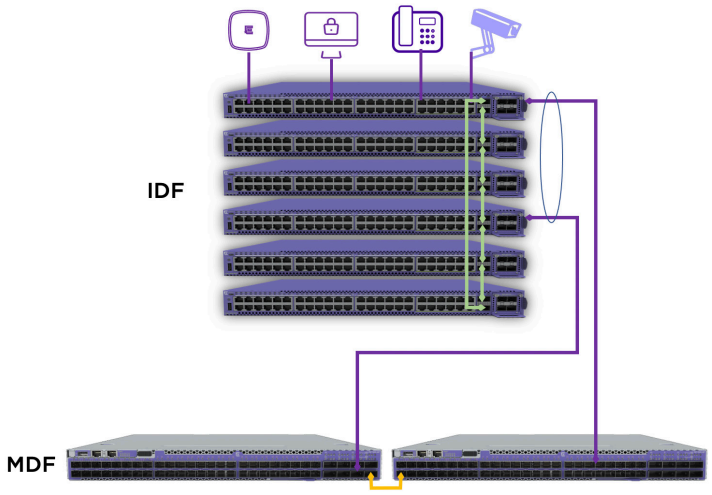
With today's fabric-based solutions, the infrastructure layer and the service layer are logically separate from each other and are only loosely coupled at the service access layer. As a result, services can be deployed independent of the physical topology of the underlying infrastructure.

This enables provider-like connectivity service provisioning and enables automation of service deployments, thus building the foundation for heavily segmented logical networks as required for networks where IoT devices are fast becoming ubiquitous.

Today's Edge Switching Architecture

Enterprise networks these days typically have a two to four tier architecture where tiers are added based on the size and physical distribution of the network. A building typically consists of MDFs and IDFs. MDF is the Main Distribution Frame a.k.a building core/distribution layer and the IDF is the Intermediate Distribution Frame a.k.a floor access switching layer.

MDF to IDF interconnections are typically built using a triangle architecture with two MDF switches clustered together to form a multi-link aggregation group (MLAG a.k.a SMLT) and the IDF connected with a link-aggregation group to the MDF switch pair for redundancy. Most Enterprise networks try to avoid the use of Spanning Tree as the main topology protocol as it has shown to be too unreliable and inefficient for building robust edge networks.



Within the IDF, switches are typically stacked providing a single point of management of all ports in the IDF reducing the number of elements to be managed in a network. User IP subnets typically span multiple IDFs, so it is very common to keep them as Layer 2 switches i.e. configure VLANs only on IDFs and provide default gateway routing functionality at the MDF layer.

This approach of building edge networks has been and is very successfully deployed world-wide, but it has its drawbacks because of the use of multiple technologies between edge and core to provide an end-to-end network solution, resulting in increased operational efforts.

Extreme's New Fabric to the Edge Approach

A novel approach to providing a consistent end-to-end network is enabled with today's fabric technologies. Fabric-based solutions for networks allow endpoint only provisioning, thus significantly reducing the amount of configuration required on network devices. By reducing the configuration requirements at the edge, even with a large number of edge switches, operation and maintenance efforts are reduced greatly.

Extreme's Fabric Edge solution reduces the number of network protocols by replacing the multi-chassis link aggregation protocol, the VLAN signaling protocol as well as the stacking protocol with a single fabric protocol that is also used in the core of the network (IS-IS).

The result is an end-to-end fabric that provides a single operational model from Data center to Core to Campus-Edge, with the option to expand it even to the Branch.

To top it off, deployment simplification through automation is also implicitly provided, reducing network deployment times significantly.

Fabric-Based Edge Switch Architecture

Design Goals

The design goal of extending fabric to the Campus-Edge (IDF) is to simplify all operational aspects of a network solution from initial deployment, to network expansions and daily operations.

This is achieved by removing as many protocol state-machines as possible by consolidating the network functions into a single fabric protocol streamlining core and edge operations. Importantly, there shall not be any different operational behavior from the end-user connectivity perspective.

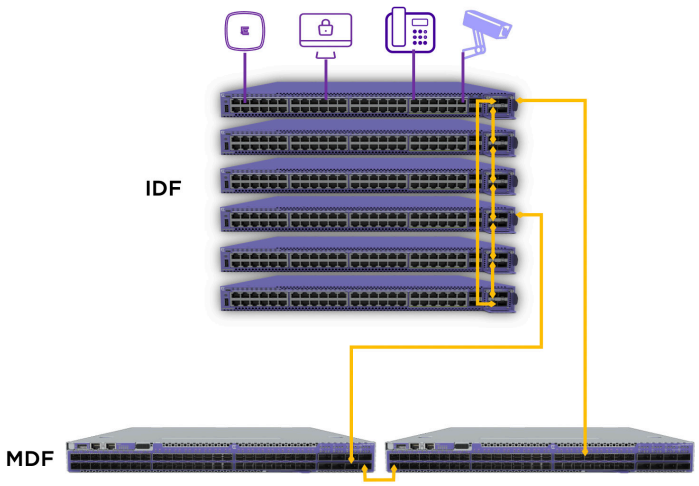
Additional focus has been put on implicit automation of the fabric solution, reducing the need for network operators to explicitly configure and automate the infrastructure.

Fabric Edge Architecture

A fabric edge solution expands the fabric from the core and aggregation (MDF) layer of the network to the access (IDF) switching layer. Instead of stacked IDF switches, the IDF switches remain standalone switches that are individually managed. Switch stacking was originally invented to reduce the configuration effort at the network edge allowing network operators to apply network configurations such as VLAN IDs once at the network edge (stack) and then add user ports to it on demand.

With Fabric to the Edge, there is no stacking and each switch is managed individually. However, by minimizing the amount of edge configuration required, we can make the fabric edge far simpler to manage than traditional stacked architectures. Today, many networks rely on zero-trust approaches where end-users and end-devices are authenticated by a centralized Network Access Control solution before they are allowed onto the network. With this approach not only is host authentication employed, but also end-device service mapping provided by having the VLAN, service ID and a user policy (filters) applied through Network Access Control (NAC), using EAPoL or MAC based authentication.

This approach removes the need for pre-configuration of VLANs or filters on edge switches, as they are dynamically applied based on the authentication results. By removing the necessity for preconfiguring VLANs and user-based filters on edge switches, baseline configurations are reduced significantly. For networks that don't use network access control and thus require manual per port configuration, simplification can be achieved by deploying flexible port templates that can be applied to a bulk of ports simultaneously from the management tools.



For infrastructure links such as uplinks as well as intra-IDF links, further reduction of edge configuration is achieved, by employing Zero-touch-fabric, which automatically establishes fabric connectivity among devices within an IDF, as well as towards the MDF, since there is no need to configure stacking or uplinks to the aggregation layer anymore.

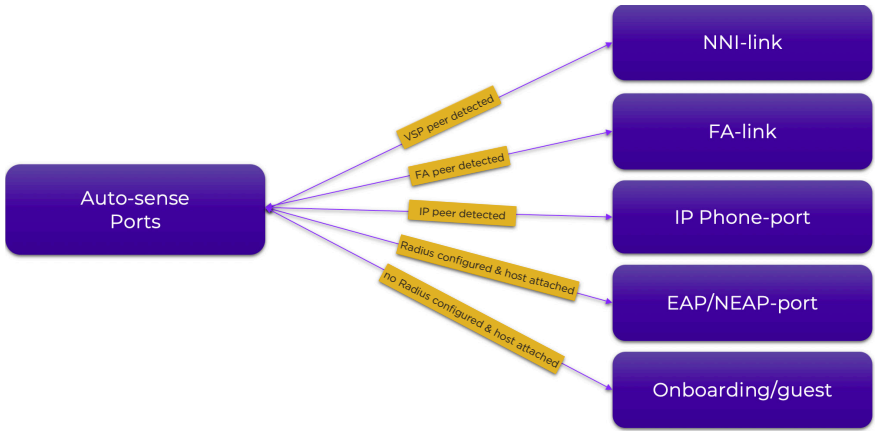
This edge automation is enabled by a new port functionality where a port state can change based on sensing what is connected to it. This functionality is called port auto-sense.

Zero-touch-fabric leverages the auto-sense port functionality to detect whether a fabric switch is connected to another fabric capable switch. If detected, the fabric is automatically expanded to the connected device, signaling and negotiating all relevant fabric configuration parameters across the fabric link, enabling a plug and play deployment model.

In addition to fabric link detection, auto-sense port functionality is also used to dynamically detect fabric-attach (FA) capable devices such as EXOS and ERS switches, Access Points or third-party FA capable devices enabling automated service signaling directly from the FA device.

Auto-sense ports can also detect whether they are connected to IP Phones or hosts with or without 802.1X login procedures.

Plug and Play Enabled by Auto-Sense Ports



This elaborate auto-sense port state-machine reduces the need for edge switch configurations dramatically, thus simplifying IDF deployments significantly.

An additional important element of this zero-touch deployment solution is the automated onboarding service creation. The fabric automatically creates an isolated connection for each onboarding device towards the network management segment where devices can reach the DHCP, Radius and network management servers. This onboarding-service ensures secure reachability to the management tools for all connected network devices as well as end-devices. End-devices remain in an isolated guest segment until they are assigned to a specific user segment.

What Can be Expected From a Fabric Edge Solution?

Fabric capable switches can be deployed in a plug and play manner with factory default settings i.e. no configuration. The switches will form a new fabric automatically or can connect to an existing fabric that is auto-sense capable, get an IP address from a DHCP server and onboard to the management servers such as XIQ and XIQ-SE/XMC automatically for further provisioning.

Switch ports on those devices will accept any device into a guest/onboarding segment ensuring a touchless onboarding for any connected end-device.

Once the switches are onboarded and RADIUS server reachability information and credentials are deployed, the network is fully EAP/NEAP enabled without any further configuration required providing a seamless deployment experience.

In summary, the Extreme Fabric Solution provides and end-to-end networking solution that significantly reduces operational complexities, while at the same time providing all the necessary segmentation capabilities hardening the network for today's ever growing IoT demands.