# Extreme Fabric Connect
A Unified Fabric That Ties One Network Together

Highlights

- Provide a unified solution that extends to any location -- whether data center, campus, SD-WAN, or branch—independent of topology.

- Deliver virtualized services across your entire infrastructure, including wired, wireless, SD-WAN, IoT and even 3rd-party devices

- Simplify your network with self-forming, automated processes that speed deployment and eliminate manual operations

- Segment and protect your network with a stealth design that blocks lateral movement and prevents network breaches

- Deploy a proven solution based on IEEE /IETF standard technology with thousands of installed networks
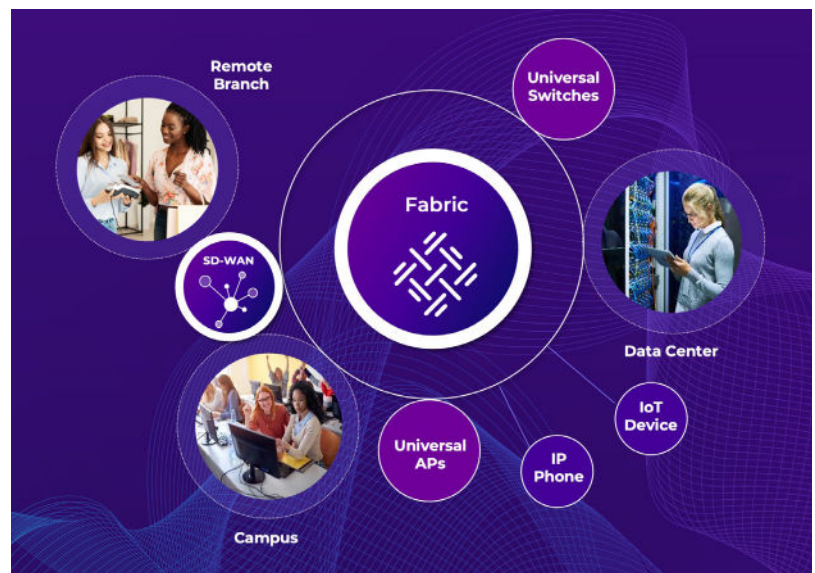
A New Way to Build Networks

With Extreme Fabric, organizations can say goodbye to the complex and inflexible networks of the past with a unified, automated, and secure network that enables you to be more responsive to your organization's needs, reduce operations costs, and increase your ability to innovate.

Unlike legacy network designs that are labor-intensive and complex to operate, Extreme Fabric is a standards-based, network abstraction technology that enables multiple, discrete, and secure virtual networks to run seamlessly over your network infrastructure – independent of topology. These virtualized networks are inherently secure, with automated provisioning that minimizes manual configuration and the risk of network errors.

Extreme Fabric Design Approach:

Extreme Fabric securely interconnects network locations and devices via secure virtual services (or segments) that can extend across SD-WAN, remote branch sites, campus, and the data center (see Figure 1). This is done by delivering a fabric solution that incorporates the following design principles:

- **Unified** – providing a comprehensive solution that can connect any location, device, and/or service in the network

- **Automated** – with auto-forming, auto-sensing, and auto-connection capabilities that streamline network operations and deployment

- **Secure** - in a framework that securely separates network services and that inherently protects against network breaches

Components Making Up Extreme's Fabric Solution:

Fabric Connect is the core component of the Extreme Fabric solution based on Shortest Path Bridging (IEEE 802.1Q) and IS-IS routing protocols. It provides virtualized network services that connect users and devices across the network infrastructure.

Fabric Attach is a software-based feature that delivers automation and time-to-service enhancements to Extreme and 3rd-party devices. It effectively automates device connection to the Fabric Connect environment, enabling endpoints, such as Extreme wireless access points, to be quickly mapped to the appropriate virtualized fabric service.

Fabric Extend allows you to connect islands of fabrics into a single fabric over a public or private WAN infrastructure and can also run in conjunction with the Extreme SD-WAN solution.
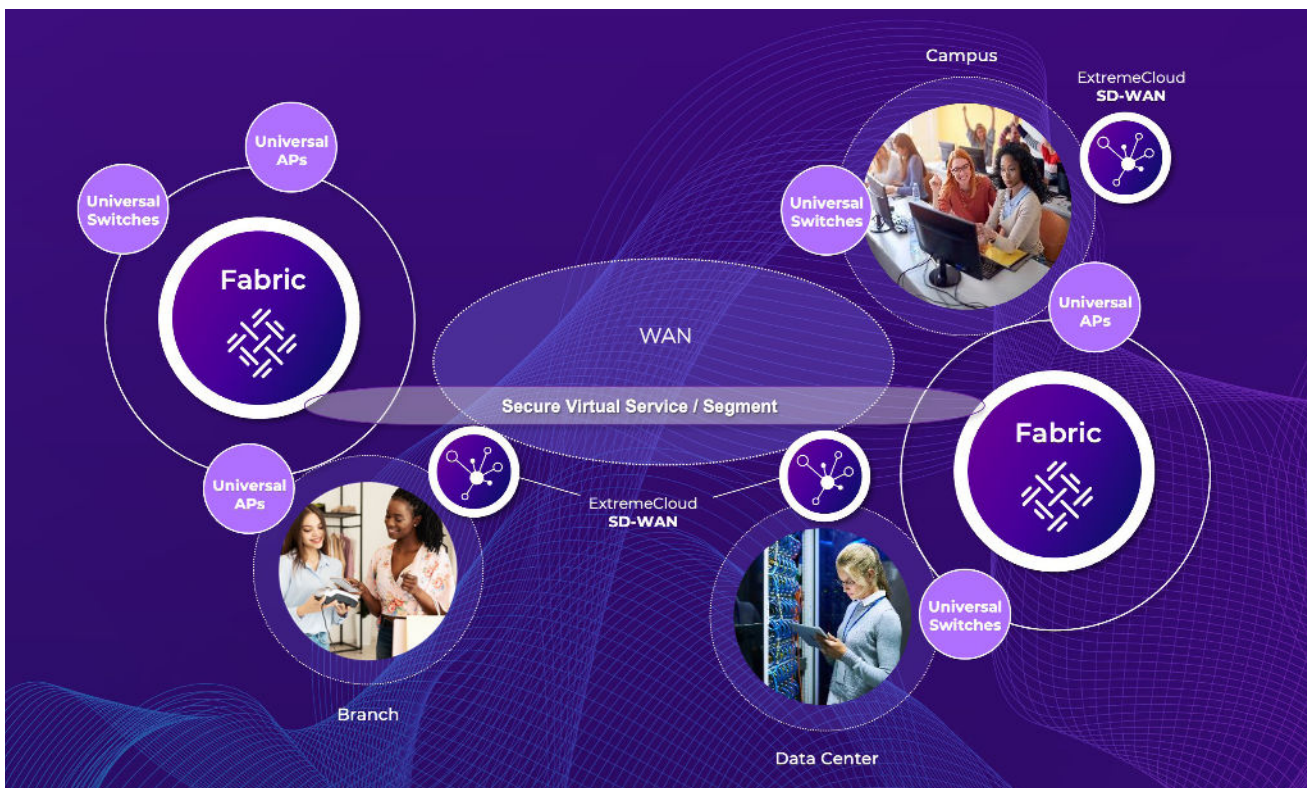

Figure 1. Extreme Fabric creates secure end-to-end virtual segments that operate across both your LAN and WAN infrastructure

A Complete Unified Fabric

Extreme's industry-leading fabric is a self-forming and self-provisioning solution that has been installed in thousands of customer networks.

Fabric Connect is automatically included with all of Extreme's Universal and VSP Switches. This means that when you buy one of these switches, you immediately get all the benefits of Extreme Fabric Connect.

These include:

- Zero-touch onboarding and auto-sensing to simplify switch and fabric deployment. The switches identify what they are connected to, and they snap to attention.
- The full suite of Fabric services, including the ability to forward Layer 2, Layer 3 (routed), and even advanced multicast services over the fabric.
- The ability to support and deploy 10s of thousands of switches across a single fabric infrastructure

Inherent Automation

Extreme Fabric provides a self-forming, auto-sensing approach to deploying fabric across wired and wireless devices on the network.

Once deployed, Fabric configuration and provisioning happen at the edges, which connects services for faster time to service and simplified operations. Changes made at the edge are propagated throughout the network dynamically.

Since set up and changes are only made at the source and destination edges:

- The core is built once and then it's "hands off".
- This automation provides better stability for the network

Zero-touch onboarding and auto-sensing of Extreme switches and Extreme access points (APs) further speed

fabric deployment.

Secure Network Services

Extreme Fabric features hyper-segmentation to secure network traffic services. This is more effective than VLANs because segments scale across an entire fabric and they're more secure.

Users, devices, and services can be bundled into segments or zones where only that traffic is provisioned and managed.

The built-in security of Fabric using hyper-segmentation also limits the risks related to the edge and/or IoT devices compromising the network. Dynamic role-based policies protect and assign appropriate network access at the wired/wireless edge. MACsec-based encryption is also available across the portfolio.

Platform Support

Fabric Connect services are supported natively on the following hardware platforms: 5320, 5420, 5520, 5720, 7520, and 7720 Series platforms running the Fabric Engine OS.

VSP 4900, VSP 7200, VSP 7400, VSP 8400, and ExtremeAccess Platform 1400 Series platforms running the VSP Operating System (VOSS).

Summary

Extreme uniquely offers a Unified Fabric that securely ties all the components of your network together - all based on industry-standard IP and Ethernet technology.

Extreme Fabric can be deployed across any type of network environment, whether the data center, campus, or branch office. It also can deliver services across a wide

variety of devices, whether switches, APs or even 3rd party products. It can even be extended across the Internet/ WAN to provide unified services to remote locations.

Extreme Fabric delivers:
- A Unified solution that is highly scalable and can extend across multiple locations and device types
- An Automated approach that allows for faster deployment, easier troubleshooting, and increased resiliency
- And a Secure framework built into the virtualization layer that reduces risk

Extreme networks