



#WeAreExclusive

Extreme FabricConnect

Michal Dolejší



#WeAreExclusive

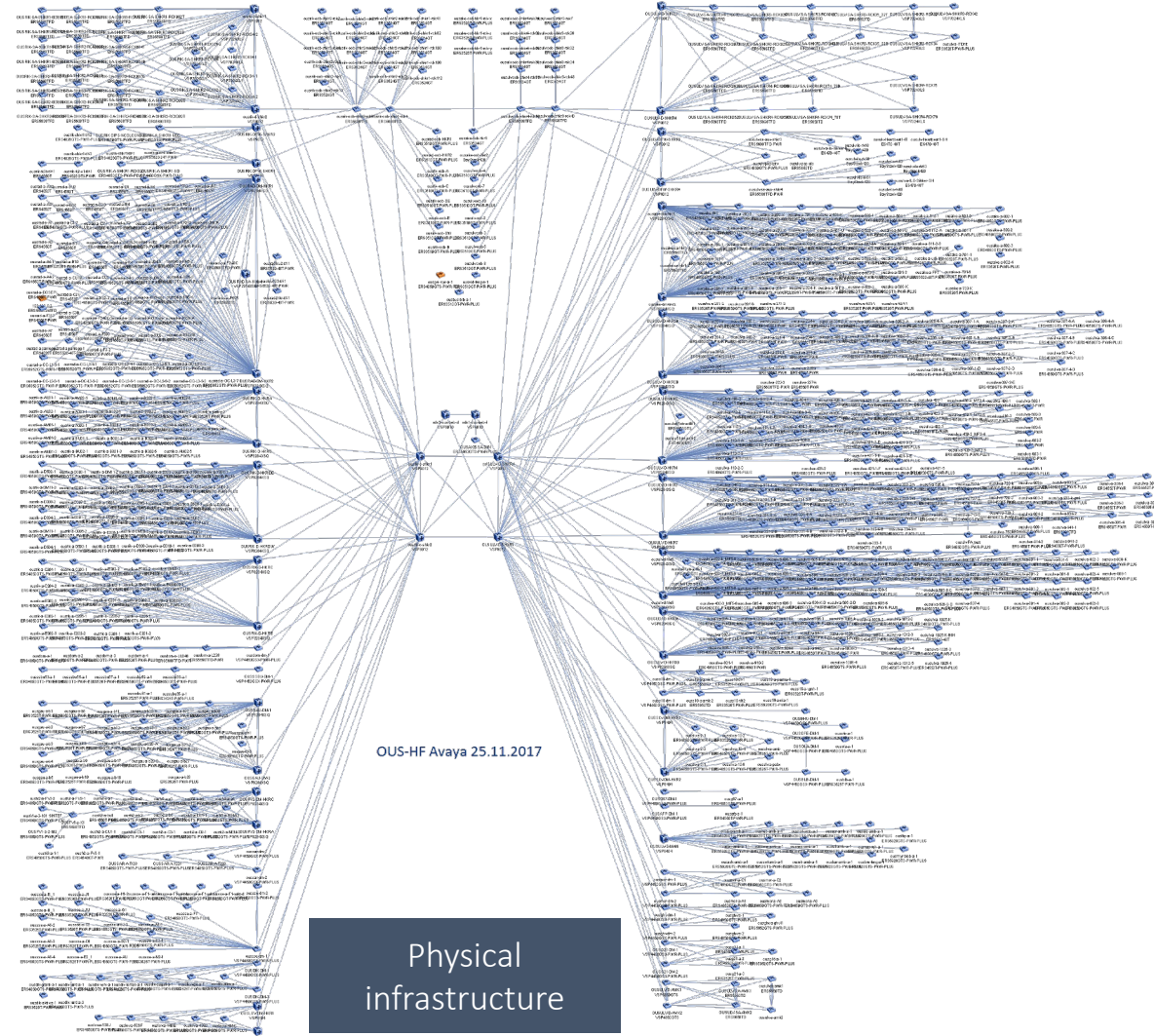
FabricConnect Introduction



Challenges in modern networks

- **Security**
- **Segmentation**
- **Orchestration**
- **Control**
- **Visibility**

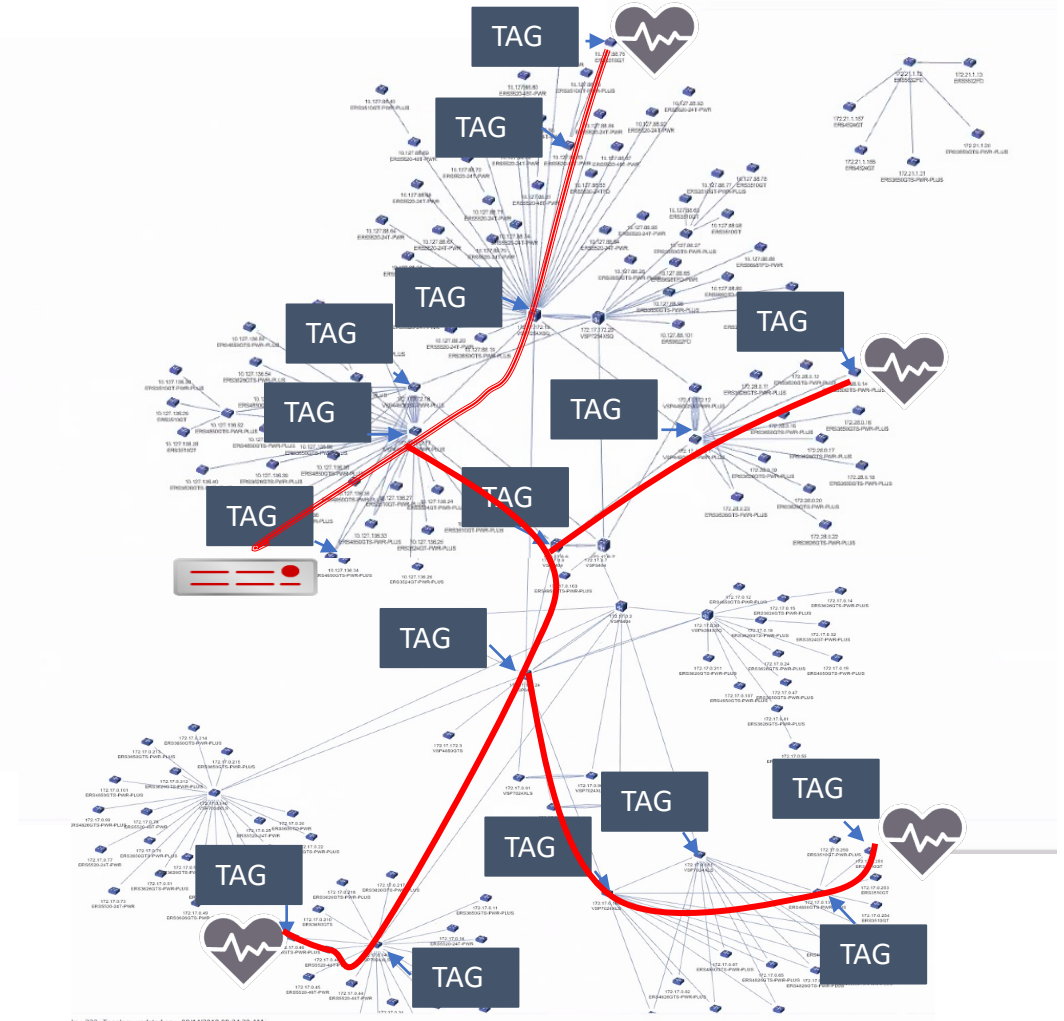
- **Operational complexity**
- **Operational cost**





The challenge of segmentation

- ▶ How to effectiently and securely extend a layer 2 segment to anywhere in the physical infrastructure?
- ▶ Is tagging the right answer?
- ▶ ...and we have not even looked at resiliency

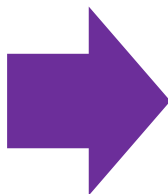
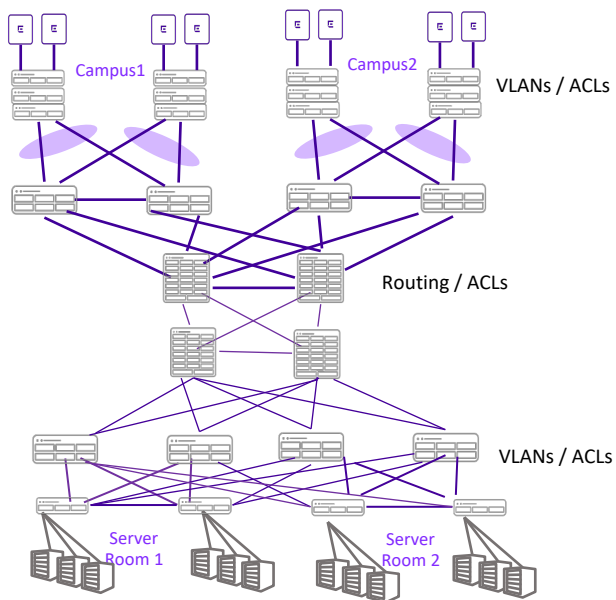




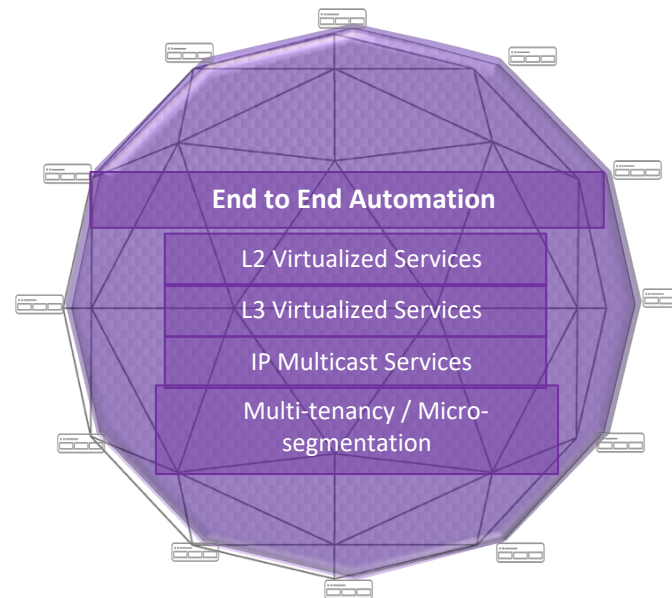
What is Fabric Connect?

➤ **A simpler way to design, deploy, manage and troubleshoot networks**

Traditional Network:
Rigid and complex



Fabric Connect:
Simple, agile, automated



Highlights

- Services abstracted from the network infrastructure
- Provisioning at the edges only
- Inherently secure
- No reconfiguration of the aggregation / core

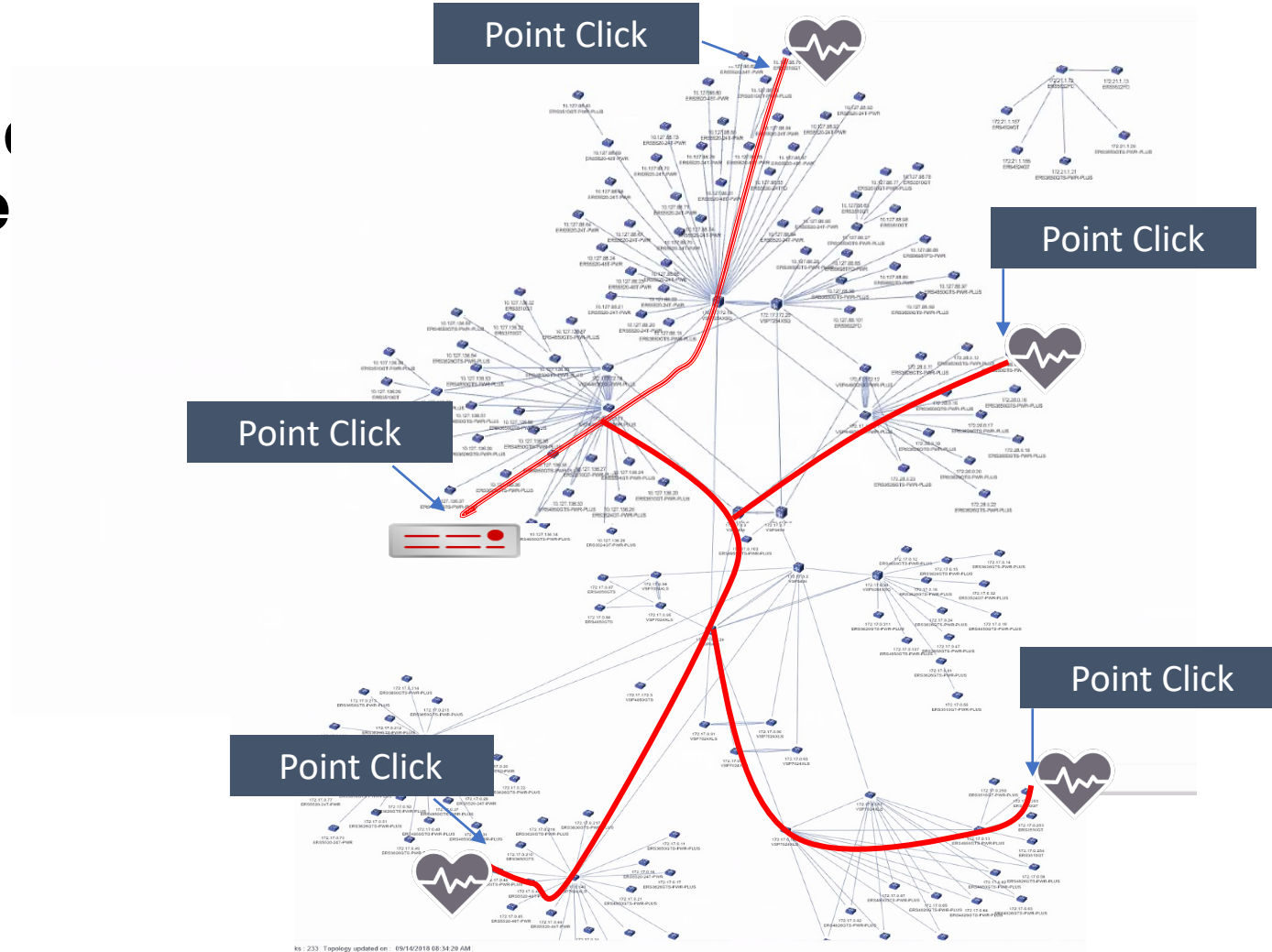


What is Fabric Connect?

➤ How to effectiently and segment to anywhere

➤ Or ...

vlan i-sid 10 20010





Fabric Connect and Key Pillars



- ▶ **Eliminates protocol stack**
 - ▶ **Acts like one „big“ fabric switch**
- ▶ **Utilizes just two standard protocols to build loop-free topologies**
 - ▶ **Simple adding/removing fabric new nodes**



Fabric Connect and Key Pillars



- ▶ **One L2 control plane protocol**
 - ▶ **Hyper-segmentation of network services**
- ▶ **Eliminates human errors in the core of the fabric**
- ▶ **L2 traffic encapsulation with optional encryption**



Fabric Connect and Key Pillars



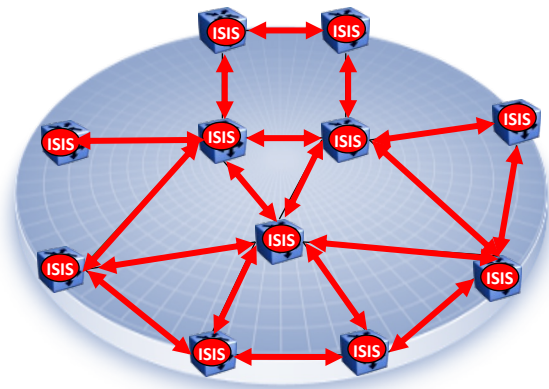
- ▶ **Automated creating and removing services at the edge**
 - ▶ **Direct integration into XIQ SE and ExtremeControl**
 - ▶ **Application telemetry for network visibility**
- ▶ **Automated VLAN provisioning with Fabric Attach standard**



What Technologies are used in the Fabric Connect

➤ Extreme Fabric Connect

- Based on IEEE 802.1aq – Shortest Path Bridging
- A link-state routing protocol capable of handling L2 and L3 traffic
- Uses ISIS as Control Plane
- Mac-in-Mac encapsulation for Data Plane
- Topology Independent
- Native support for Multicast and Virtualization
- Replaces all Legacy routing protocols + L2 redundancy and load balancing



Traditional

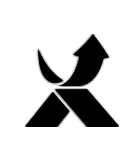
- MPLS
- BGP
- PIM
- OSPF
- VLANS
- STP
- 802.1

Extreme Fabric Connect

1 Protocol
(IEEE/ IETF Shortest Path Bridging)

Fabric Connect Benefits:

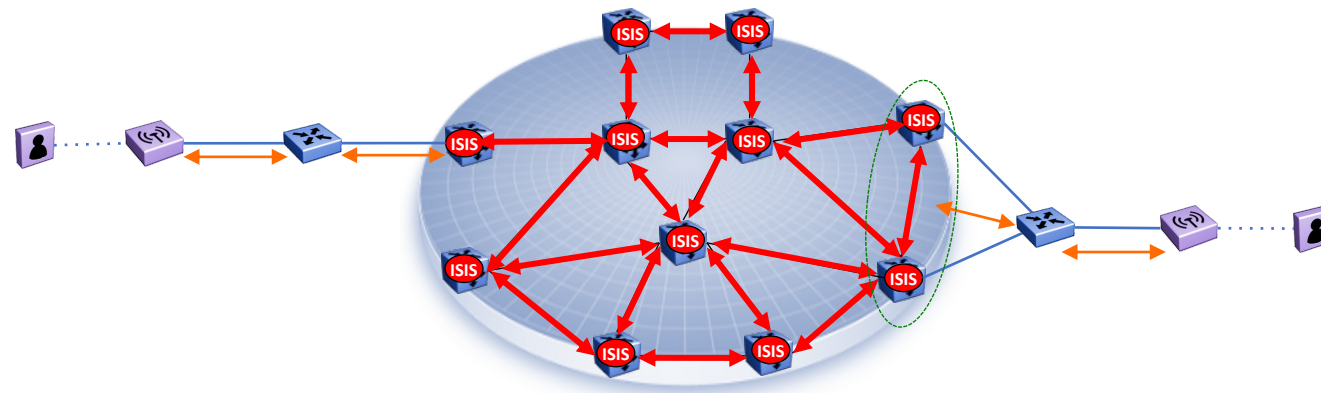
- Faster to Deploy
- Increased Stability
- Easier Troubleshooting
- Faster Resiliency
- Lower Costs



What Technologies are used in the Fabric Connect

➤ Extreme Fabric Attach (IEEE 802.1qcj)

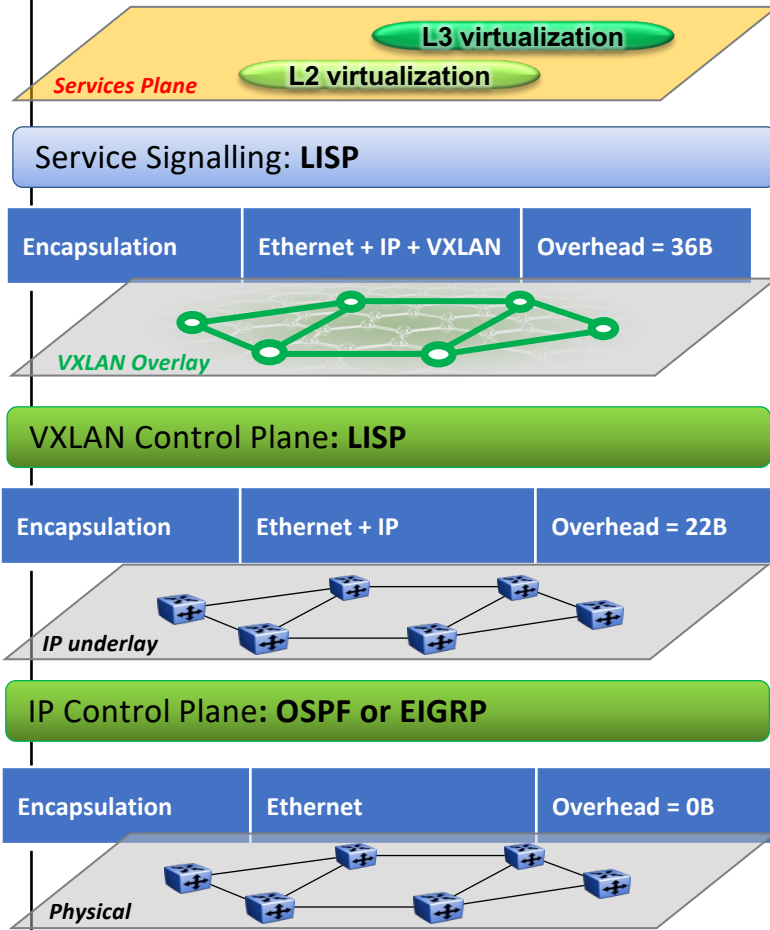
- Allows non SPB capable devices to request L2 Services from an FC network
- Uses “Automated Q-tagging” to emulate FC L2 Service
- Does not require special hardware to function
- Fabric Attach Switch can be dual attached
- Fabric Enabled Switches must in clustered in this case



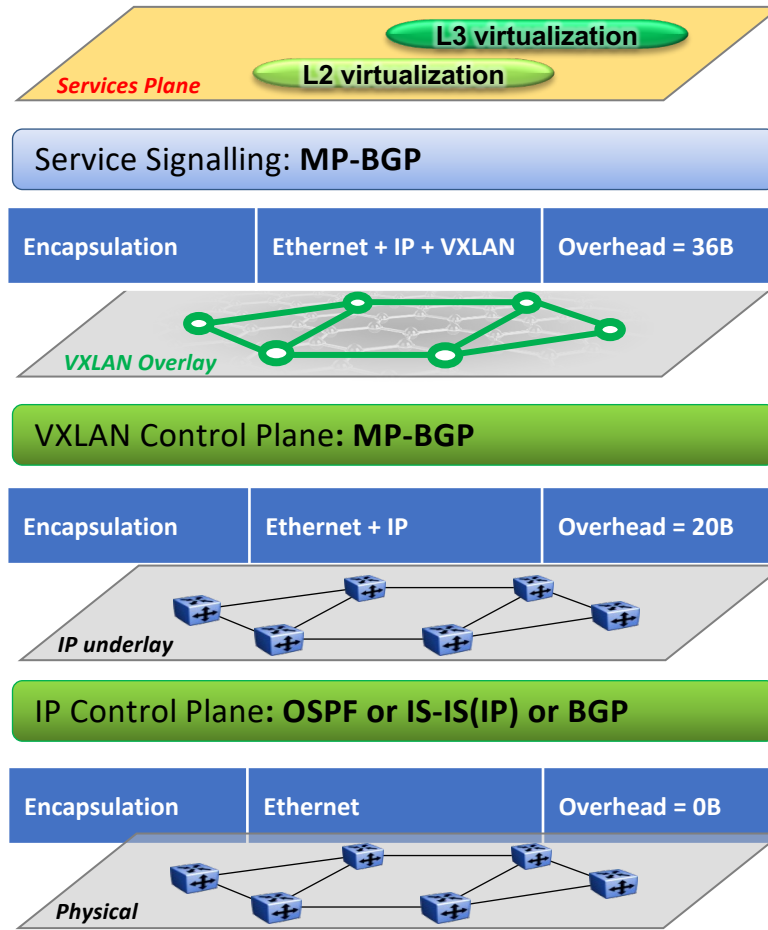


IP Fabrics vs. Fabric Connect

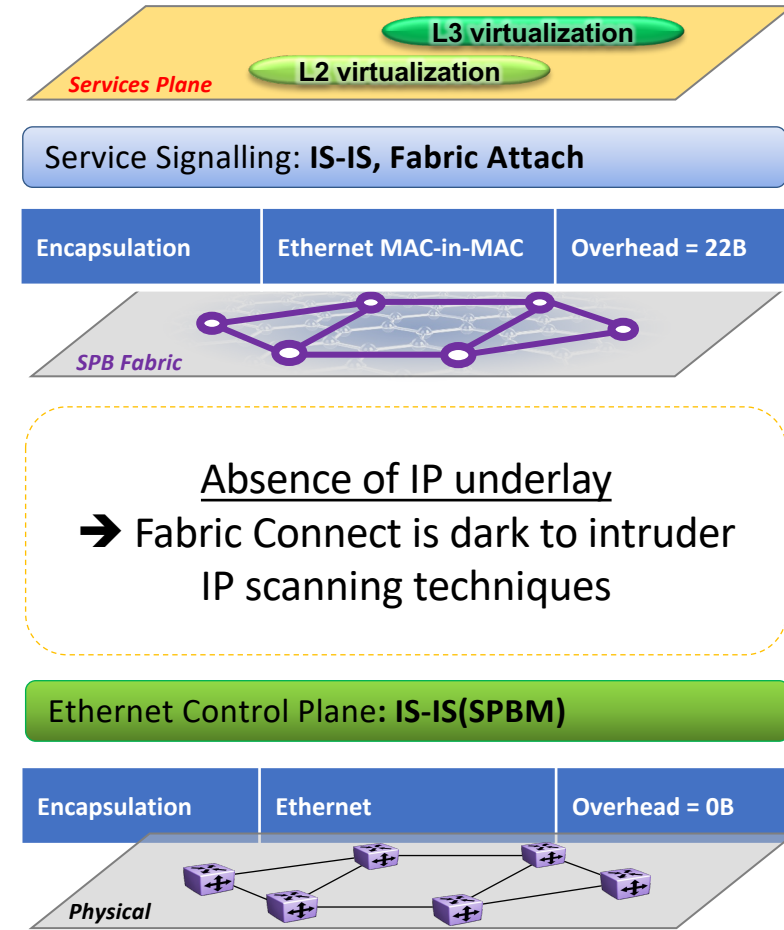
Cisco Campus Fabric



EVPN over VXLAN



Extreme Fabric Connect



Absence of IP underlay
 → Fabric Connect is dark to intruder IP scanning techniques



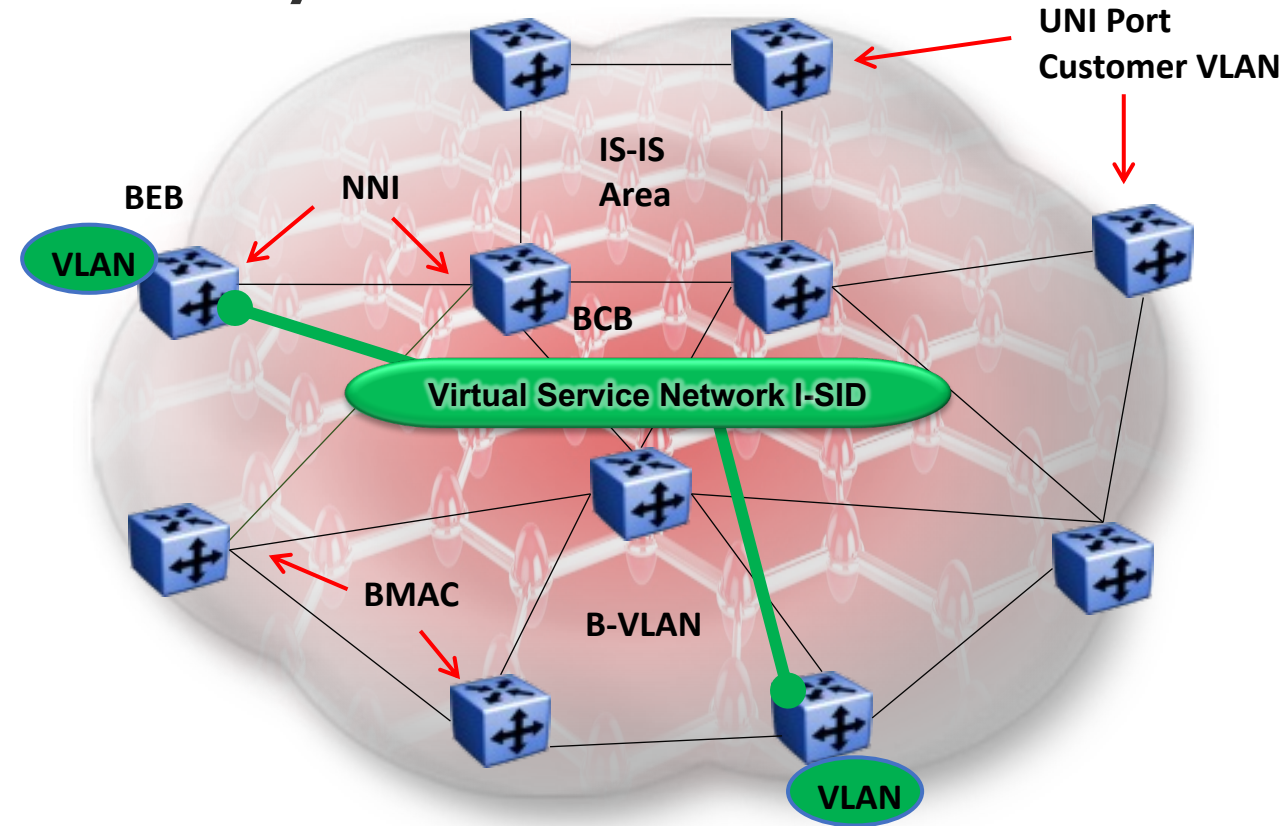
#WeAreExclusive

FabricConnect Reference Model



Fabric Connect Terminology

- **IS-IS: Intermediate System to Intermediate System**
- **BEB: Backbone Edge Bridge**
- **BCB: Backbone Core Bridge**
- **NNI: Network to Network Port**
- **UNI: User to Network Port**
- **B-VLAN: Backbone VLAN**
- **B-MAC: Backbone MAC**
- **C-VLAN: Customer VLAN**
- **VSN: Virtual Service Network**
- **I-SID: Service Identifier**



Note – only a BEB learns user MACs, BCB only learns SPB BMACs



Fabric Connect Network Services

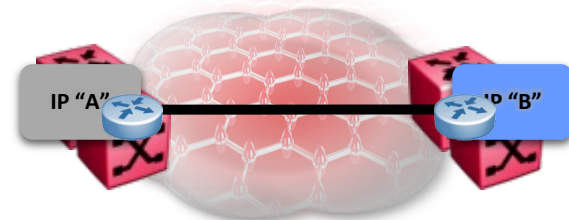
Layer 2 Virtual Service Network

Mapping of a Layer 2 VLAN into a Virtual Service Network delivering seamless Layer 2 extensions



IP Shortcuts

Native IP routing across the Virtual Service Fabric without the need for Virtual Service Networks or any additional IGP



Layer 3 Virtual Service Network

Mapping of a Layer 3 VRF into a Virtual Service Network delivering seamless Layer 3 extensions



Inter-VSN Routing

Enhancing 802.1aq by offering a policy-based Layer 3 internetworking capability of multiple Virtual Service Networks



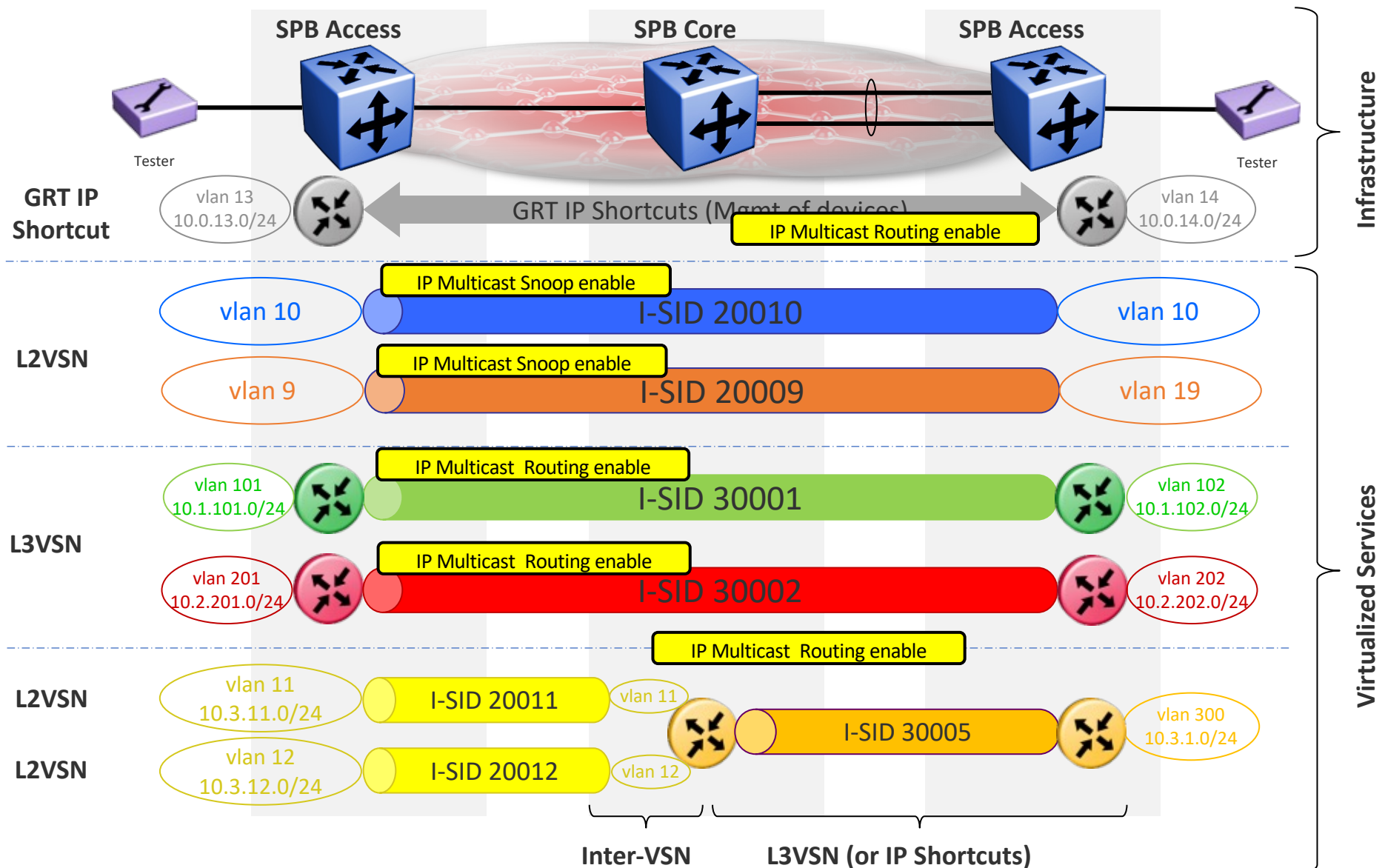
Layer 2 Virtual Service Network for IP Multicast

Mapping of a IP Multicast Group into a Virtual Service Network delivering simple Layer 2 Multicast Anywhere





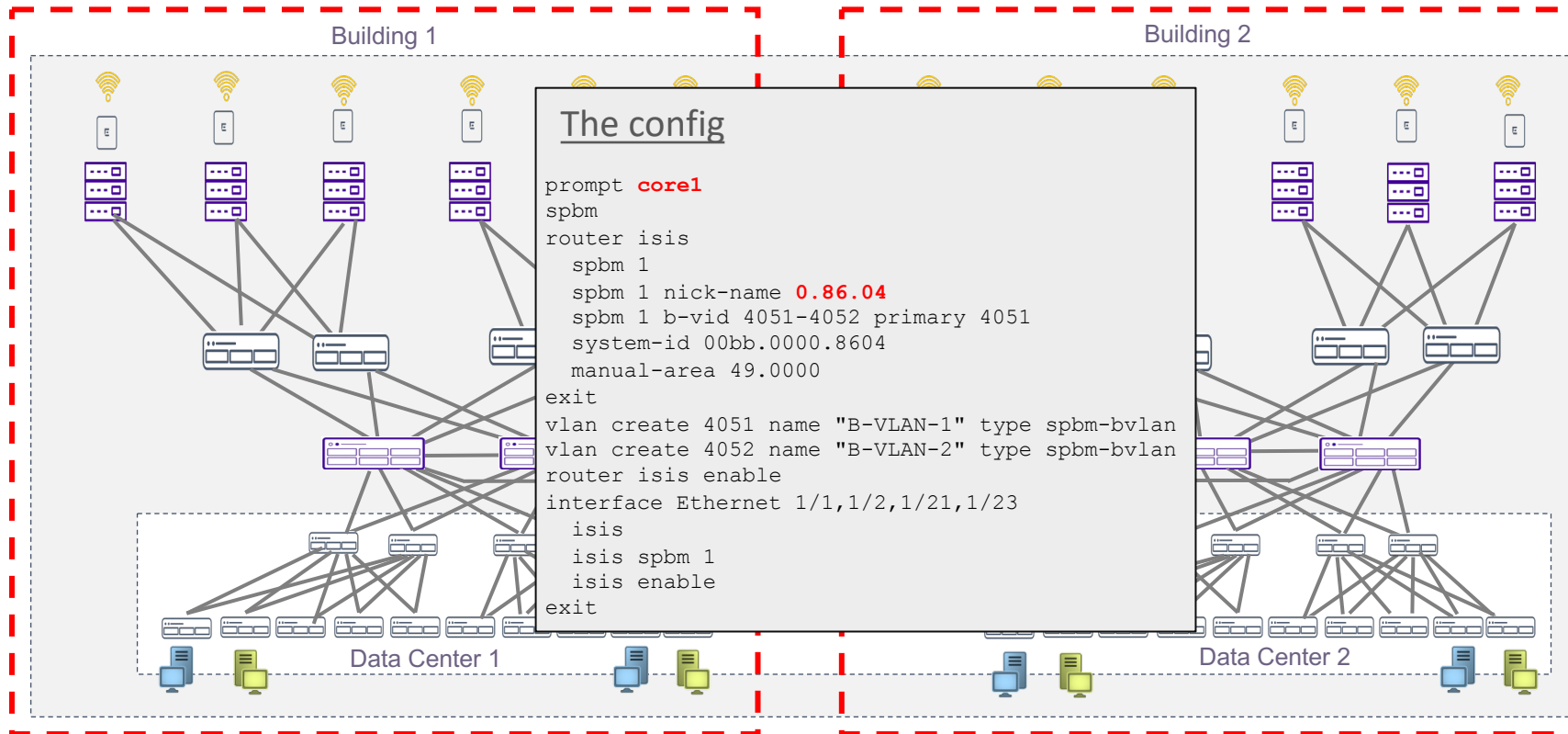
Fabric Connect Network Services



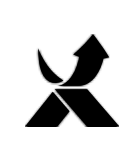


Extending the network with SPB, effortless scaling

No constraints on physical topology and wiring

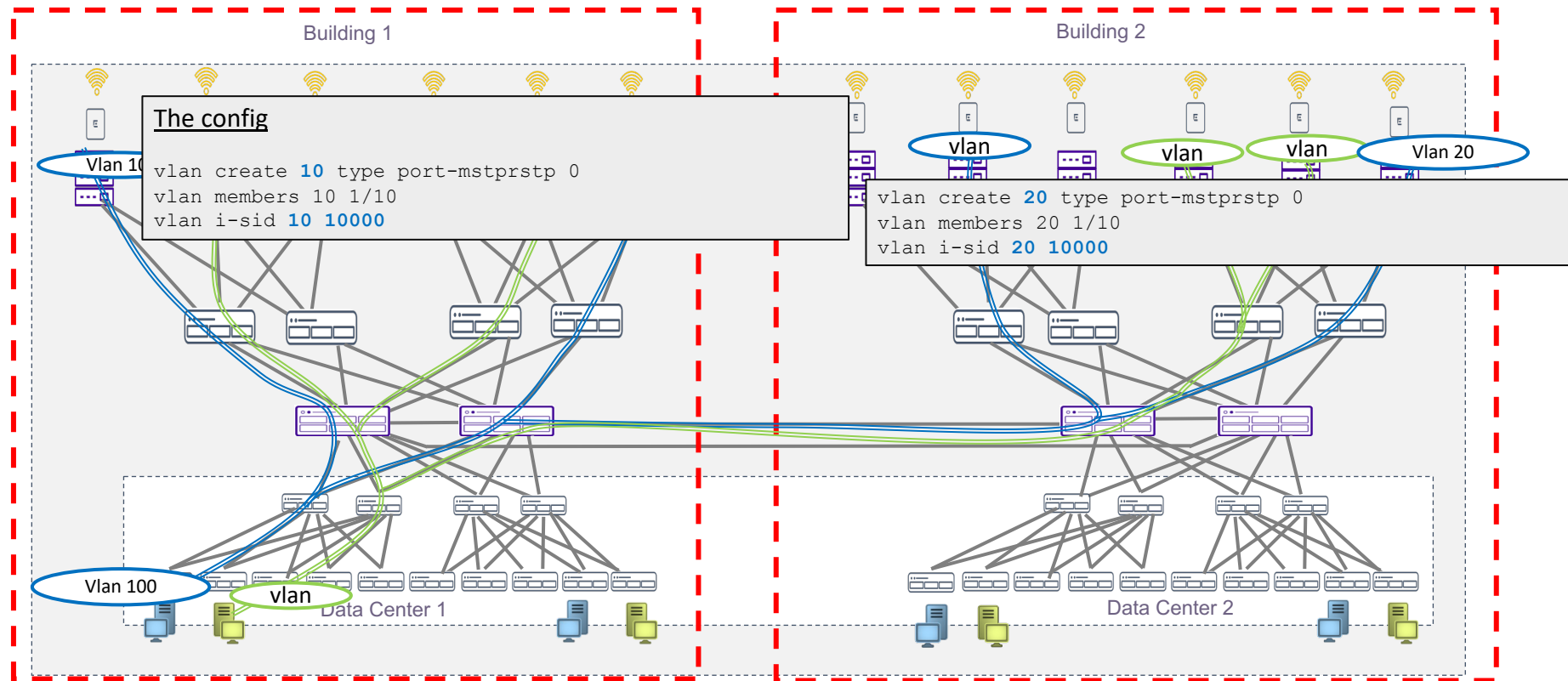


Homogenous network
Single protocol



Fabric Connect L2 services

- ▶ Flexible, effortless, no constrains - still handled by one protocol: IS-IS



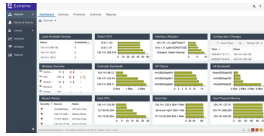


#WeAreExclusive

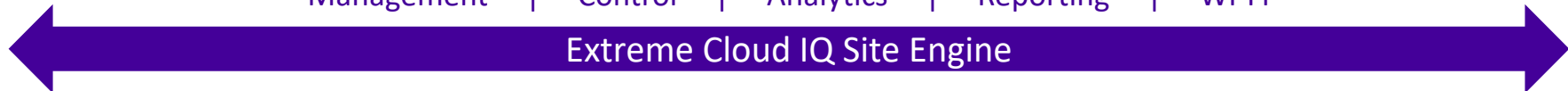
Fabric Connect Portfolio



Fabric Connect in Extreme Portfolio

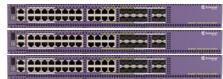


Management | Control | Analytics | Reporting | Wi-Fi



Extreme Cloud IQ Site Engine

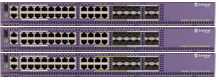
Universal series



Fabric Engine

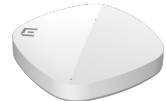
Fabric Connect

Universal series



Switch Engine

Universal/WiNG Wireless



Fabric Attach

Automated, Secure, Policy-enabled Campus Architecture



Services and Support – Ranked No. 1



Fabric Management and Explicit Automation

► ExtremeCloud IQ Site Engine (on-premise)



- Open network management system based on standards
- Configuration management, templates and Zero Touch Provisioning
- Workflow and scripting capabilities for automation



- Policy-based infrastructure, networks are no longer "anonymous"
- Automatic roll-out of applications, users, IoT devices and hyper-segments
- Key component of security at the edge of the network



- Network and application visibility
- Machine-assisted monitoring of network and application performance
- Visibility of data breaches inside the network and smart packet capture for forensics

Open API based connectors with key security infrastructure vendors and industry-leading applications



Wireless Access Layer

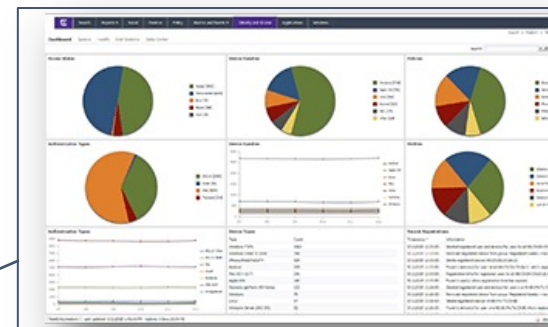
► Extreme Cloud IQ Controller (On-premise)

ExtremeCloud IQ Site Engine (on-premise management)

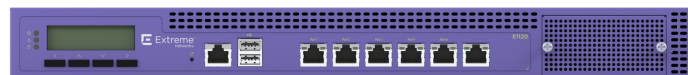
ExtremeAnalytics
Extensive Application and Analytics



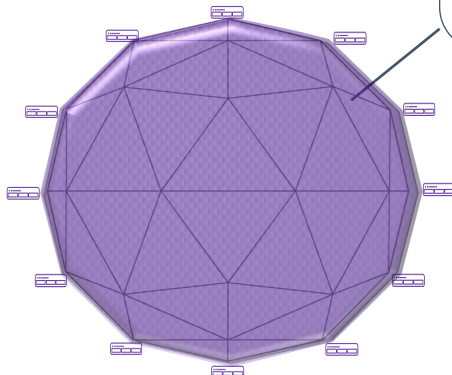
ExtremeControl
Secure BYOD and IoT Onboarding



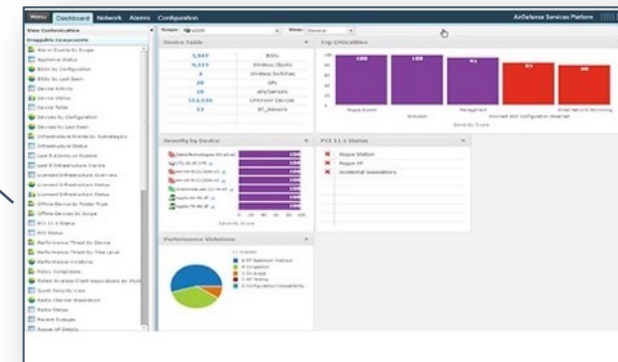
Extreme Cloud IQ Controller

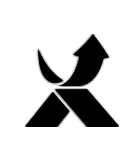


Fabric Connect
Fabric to the Wireless Edge



AirDefense
Wireless Security WIPS/WIDS





Wireless Access Layer

► Extreme Cloud IQ (public cloud)



- Removes infrastructure management and costs
- Simplicity and ease of use
- **Scalability** without compromise
- **Data privacy and protection**
- Unmatched **reliability**
- Continuous delivery of **innovations**
- **Operational savings**



#WeAreExclusive

Automation with FabricConnect



Automation Background: Understanding the Approaches

Explicit Automation

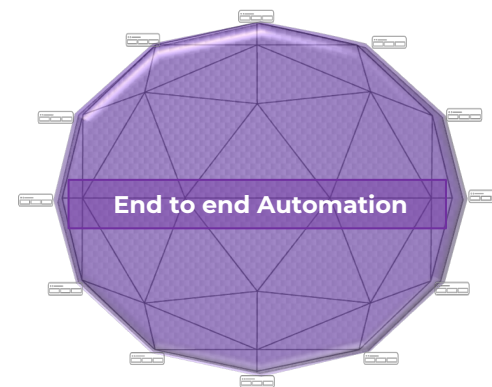
- The network operator is responsible for automation
- Config scripts externally built. Communicate to switches through APIs/ controllers



Example: XIQ-SE (XMC) Workflow Manager, Cisco DNA, Aruba NetEdit

Implicit Automation

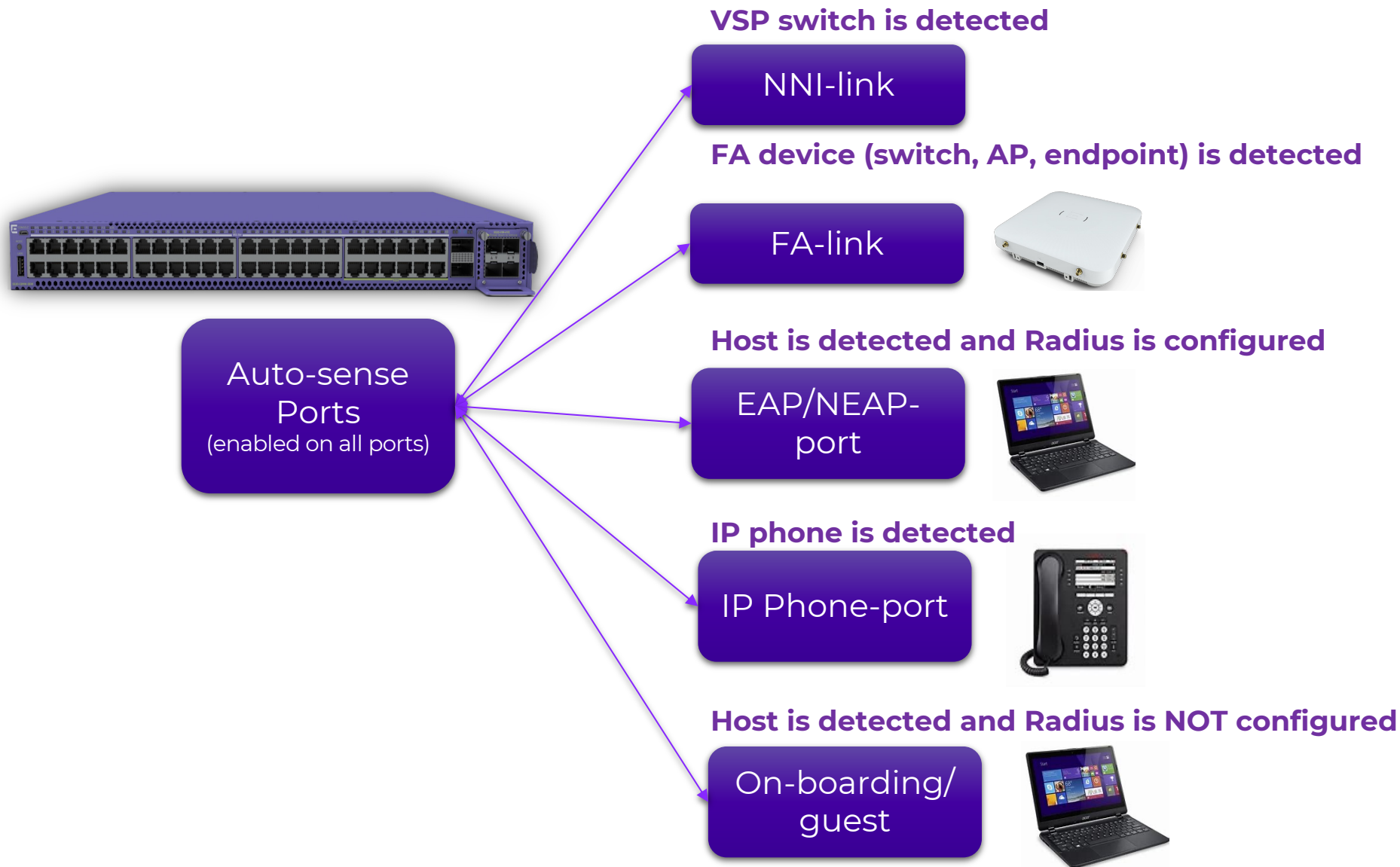
- The network takes care of automation
- No scripting/programming necessary, network protocols are used for automation



Example: Fabric Connect



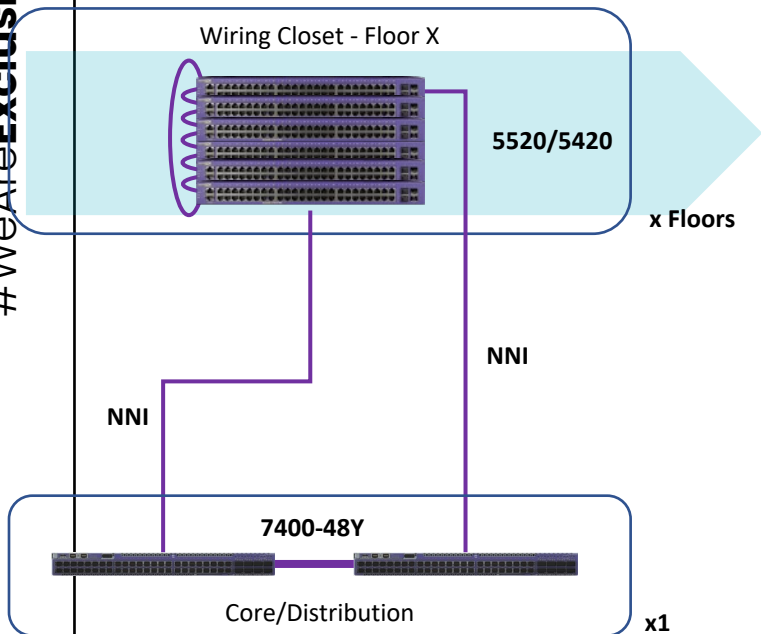
Zero Touch Fabric capabilities





Zero Touch Fabric Automation

#WeAreExclusive



- **If fully automated, the only manual config is giving the VSP edge switch a name !**

| VSP Edge functionality configuration/activation | Performed (automatically) by |
|---|---|
| Universal-hardware OS conversion EXOS → VOSS | ZTF / via ZTP+ onboarding |
| Switch System Name (including ISIS sys-name) | Network administrator, manually |
| CLI and SNMP credentials | XIQ-SE (XMC) via ZTP+ onboarding |
| SPBM enable | ZTF / Enabled in post VOSS-8.2 factory defaults |
| Global ISIS enable | ZTF / Enabled in post VOSS-8.2 factory defaults |
| ISIS Area | ZTF / Discovered from ISIS Hellos |
| SPBM Backbone VLANs | ZTF / Discovered from ISIS Hellos (else 4051 & 4052 used) |
| SPBM Nickname | ZTF / Allocated by Nickname server in existing fabric |
| SPB IP Shortcut enable (needed for mgmt clip) | Automatically enabled in DVR-Leaf mode |
| SPB IP Multicast enable (needed for multicast) | Automatically enabled in DVR-Leaf mode |
| ISIS interfaces | ZTF / Dynamically created on VSP LLDP neighbour ports |
| Fabric Attach interfaces | ZTF / Dynamically created when FA Client/Proxy detected |
| ISIS hello authentication | XIQ-SE (XMC) via site actions, "Onboard VSP" workflow |
| Fabric Attach message authentication | XIQ-SE (XMC) via site actions, "Onboard VSP" workflow |
| Voice I-SID/VLAN | XIQ-SE (XMC) via site actions, "Onboard VSP" workflow |
| DVR Leaf enable (including boot flag) | XIQ-SE (XMC) via site actions, "Onboard VSP" workflow |
| DNS Servers and Domain Name | Via initial DHCP & XIQ-SE (XMC) via ZTP+ onboarding |
| SSH/Telnet | XIQ-SE (XMC) via ZTP+ onboarding |
| Web Server HTTP/HTTPS (EDM) | XIQ-SE (XMC) via ZTP+ onboarding |
| NTP Server | XIQ-SE (XMC) via ZTP+ onboarding |
| Clock time-zone | XIQ-SE (XMC) via site actions, "Onboard VSP" workflow |
| RADIUS server & global EAPoL enable | XIQ-SE (XMC) via site actions [or "Onboard VSP" workflow] |
| Syslog & Trap receivers | XIQ-SE (XMC) via site actions |



What you can expect from Fabric switch

- 1. Unbox new Switch**
- 2. Connect it to network**
- 3. Power up the device**
- 4. Switch joins fabric**
- 5. Switch onboard to XIQ-SE**

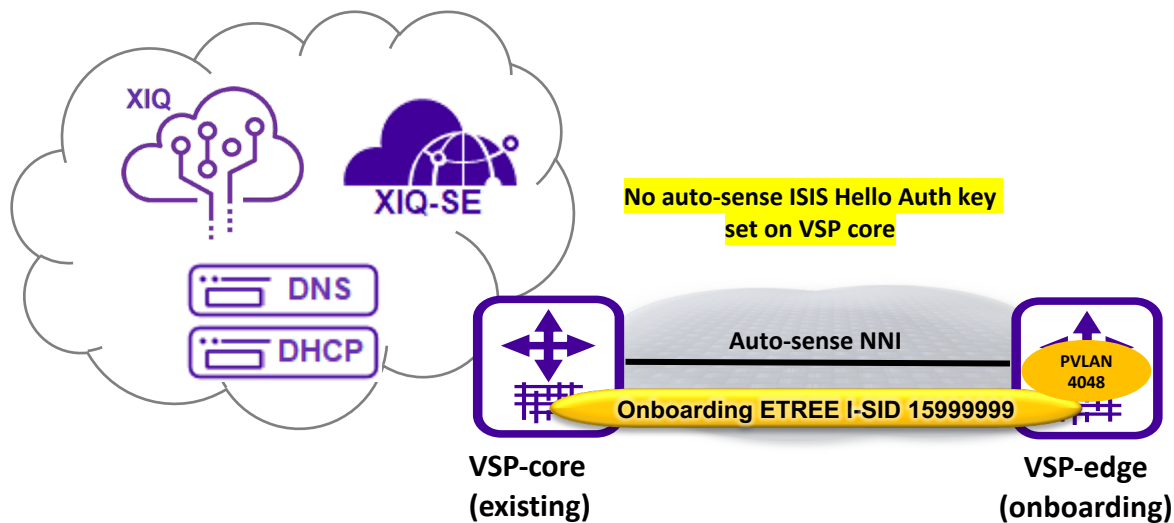
Prerequisites:

- Seed device that has nick-name server and provides reachability to Network management infrastructure
- Network management infrastructure with XIQ-SE (XMC) or XIQ & DHCP Server

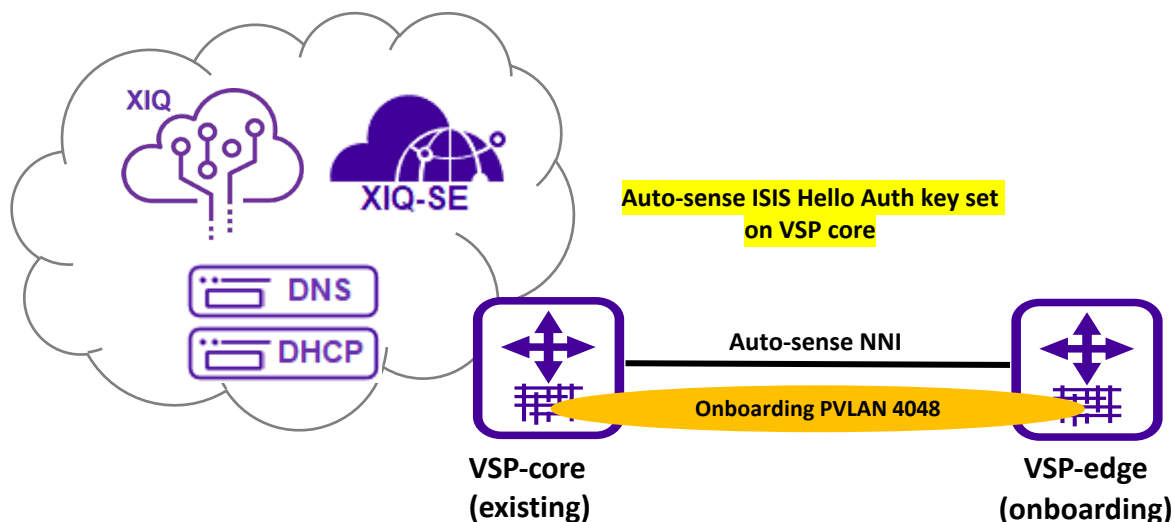




Onboarding – Security consideration



- **If no auto-sense ISIS hello auth configured on VSP core**
 - VSP edge 1st joins the fabric, then performs ZTP+ for final configuration
- **What if a rogue VSP is connected to the network ?**
 - It joins the fabric and hacker can use it to look into the fabric ISIS LSDB

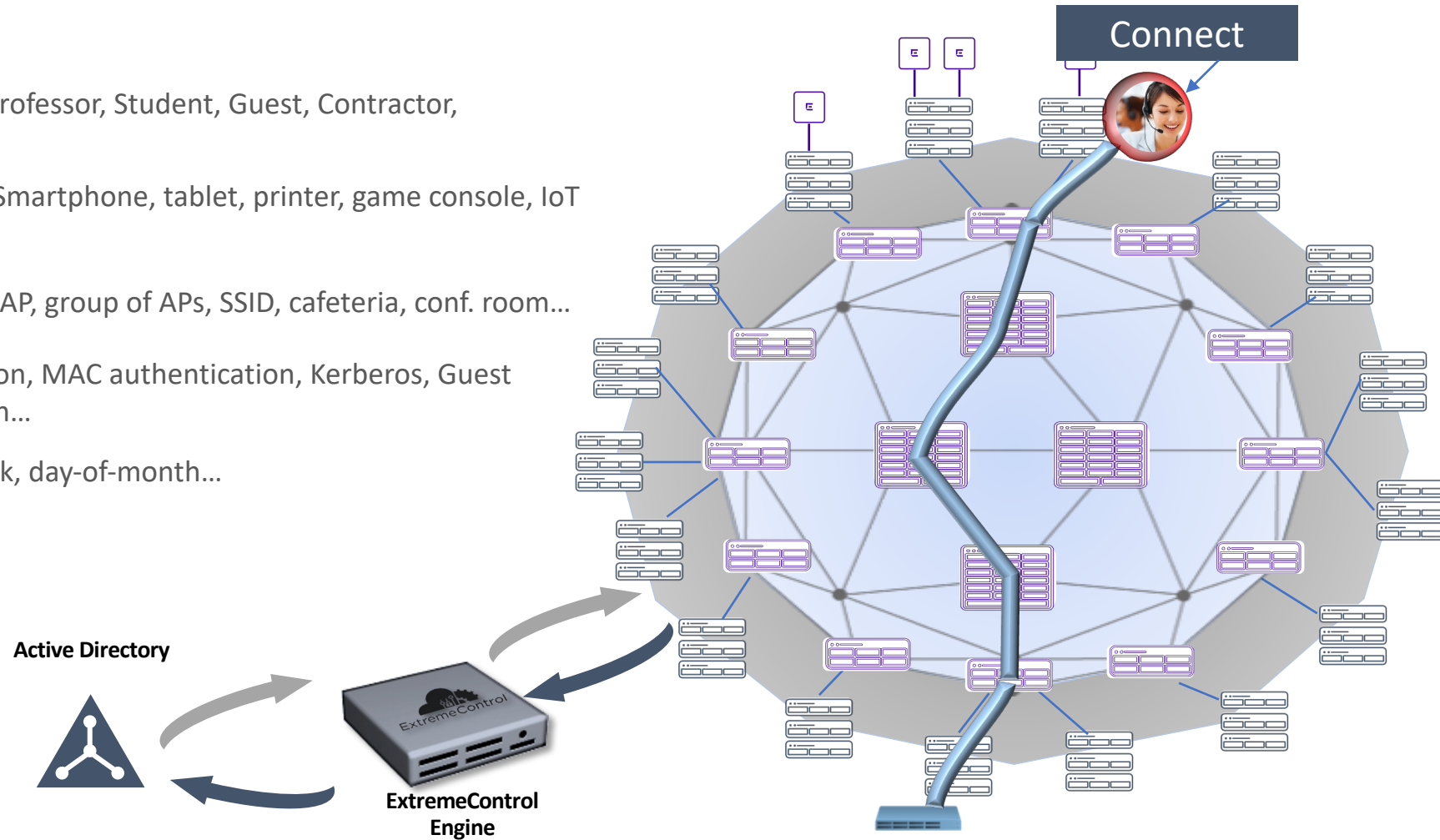


- **If auto-sense ISIS hello auth is configured on VSP core**
 - ISIS adjacency on auto-sense NNI will not come up
 - Onboarding VLAN will still be available untagged on same link
 - VSP edge 1st performs ZTP+ for final configuration, then joins the fabric once it has the auto-sense ISIS hello auth key set



Automated Edge with Fabric Connect

- Who** User role: Engineer, HR, Professor, Student, Guest, Contractor, Suppliers...
- What** Corporate laptop, BYOD, Smartphone, tablet, printer, game console, IoT Device...
- Where** Wired network, wireless, AP, group of APs, SSID, cafeteria, conf. room...
- How** 802.1X, web authentication, MAC authentication, Kerberos, Guest Management, Social Login...
- When** Time-of-Day, time-of-week, day-of-month...



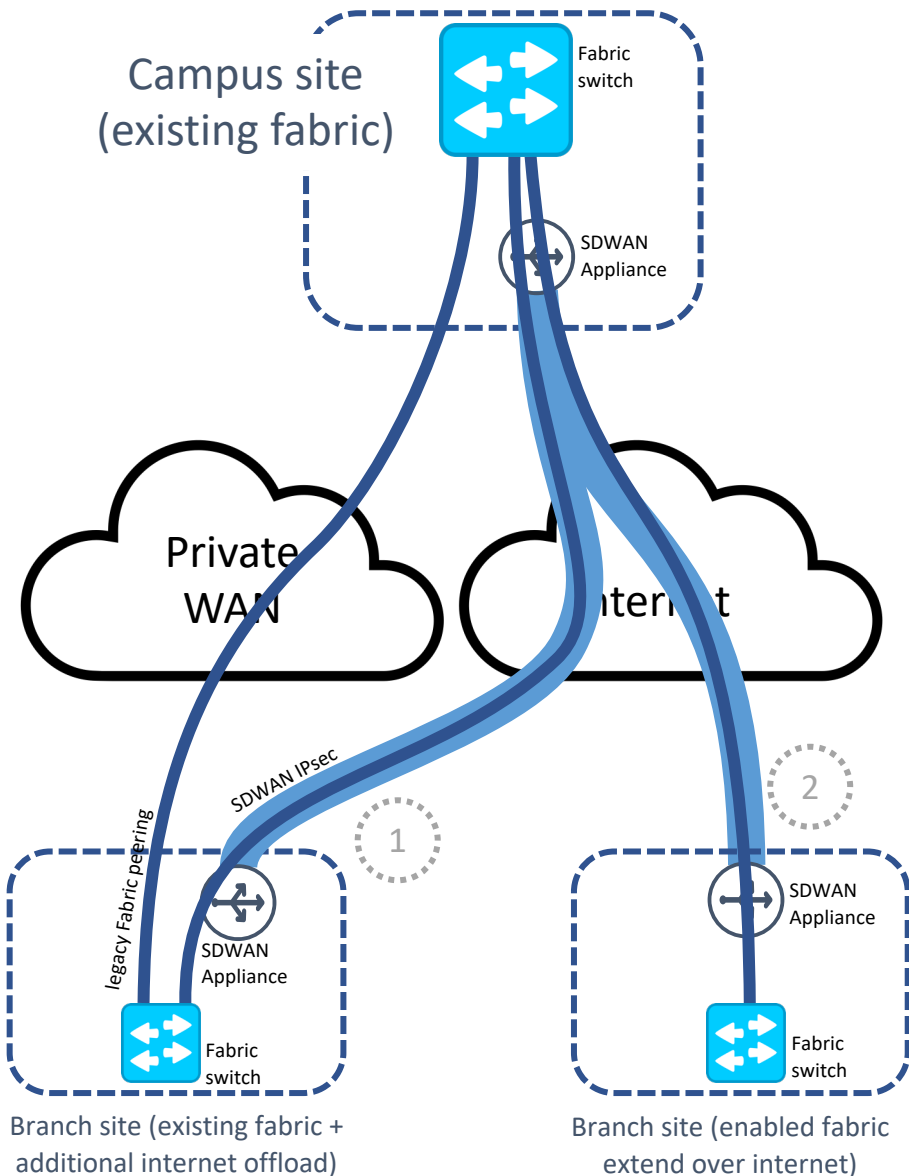


#WeAreExclusive

Integration with SD-WAN



ExtremeCloud SD-WAN integration



1

Use case 1: backup over internet for existing fabric extend

2

Use case 2: enable fabric extend over internet overlay

✓ **Included** 😊

✗ **Not included** ☹️

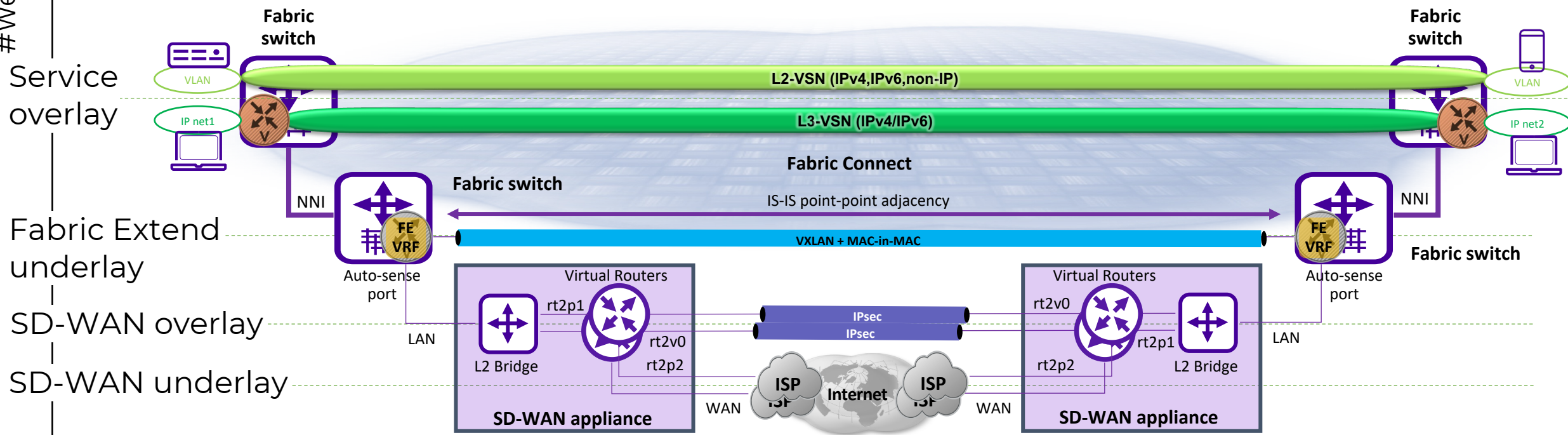
- **Full Fabric capabilities** for IPv4 networks
- **Zero Touch Fabric** configuration automation
- **Advanced application performance** (full visibility, QoS, Path Selection)

- IPv6, pure L2 networks
- Mix of Fabric and non-Fabric sites (must backhaul in campus site)
- IaaS workloads (must backhaul in campus site)
- Local Breakout
- Application performance over Private WAN links



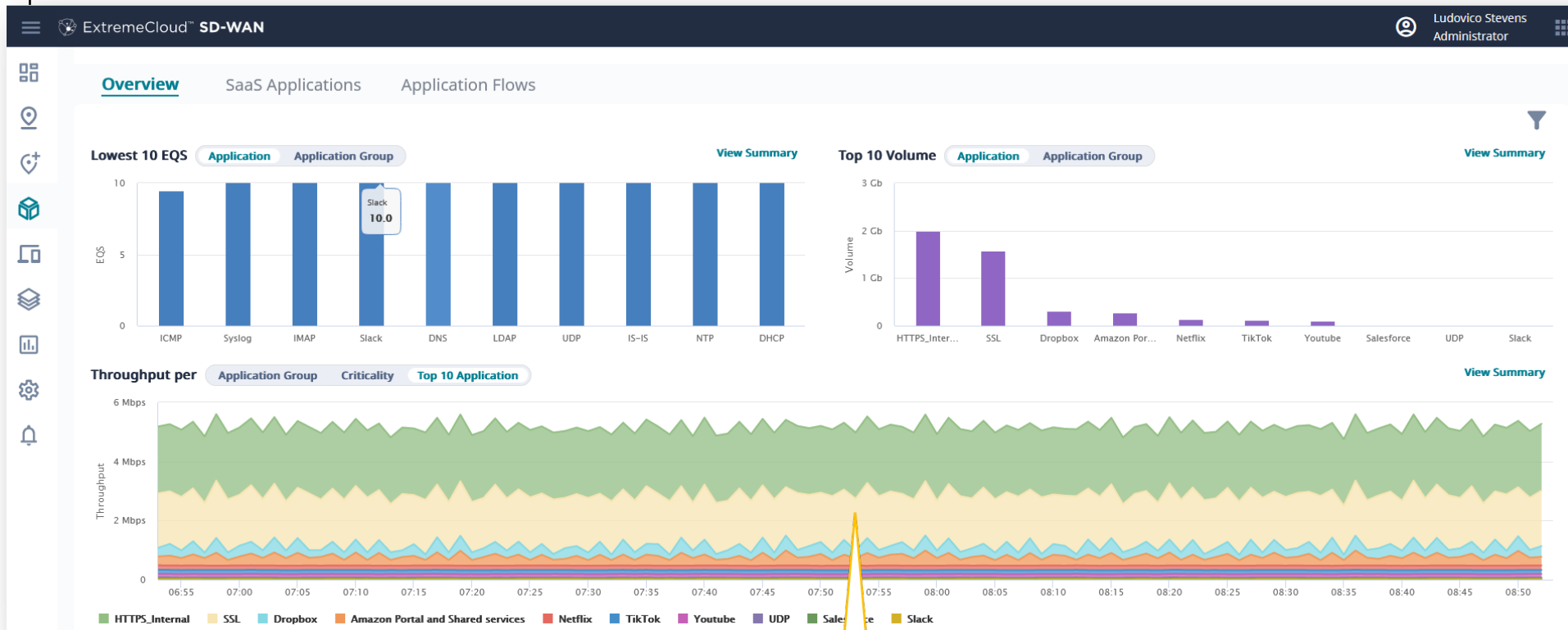
#WeAreExclusive

Know your layers in Fabric over SD-WAN

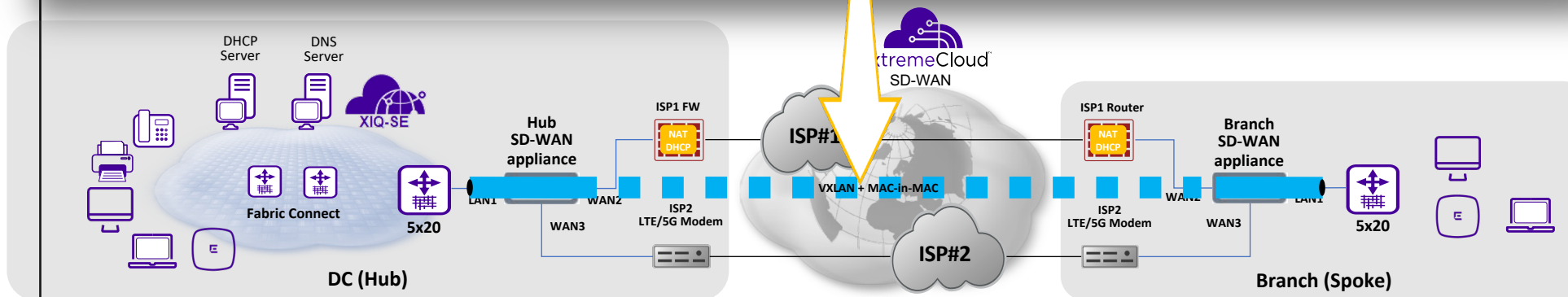




Applications crossing the SD-WAN & Fabric



- SD-WAN Deep Packet Inspection (DPI) and SaaS application visibility
- For Fabric applications running over SD-WAN
- VXLAN header is used to identify the source site and the destination site of a flow
- The VXLAN encapsulation is included in the measurement of the application throughput





Application control & DWS

- Applications are categorized in the SD-WAN into application groups with 4 criticality levels
- When WAN bandwidth becomes scarce, lower criticality applications are slowed down to ensure higher criticality applications are not impacted
- DWS determines which fabric applications should use which Internet WAN connection

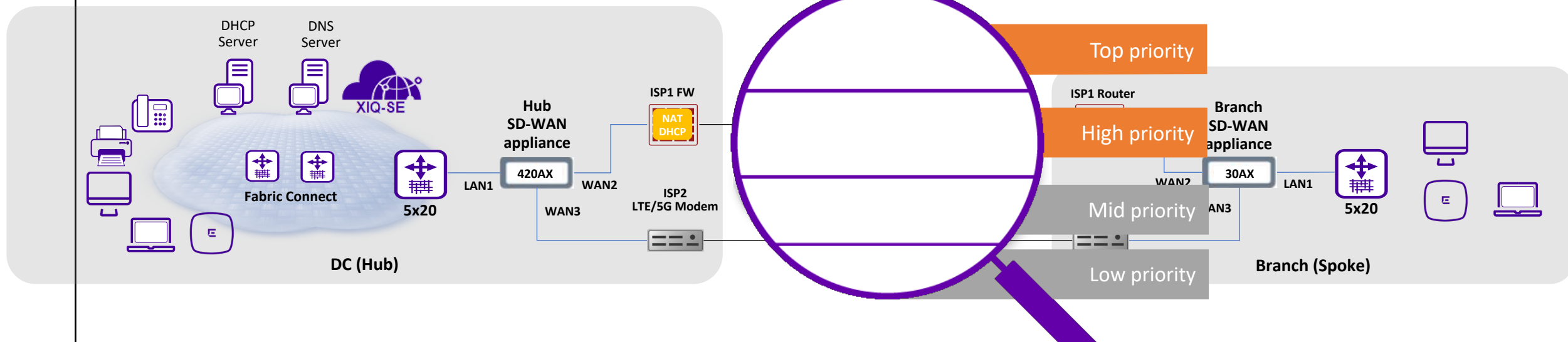
Application performance objectives defined

Top priority

High priority

Mid priority

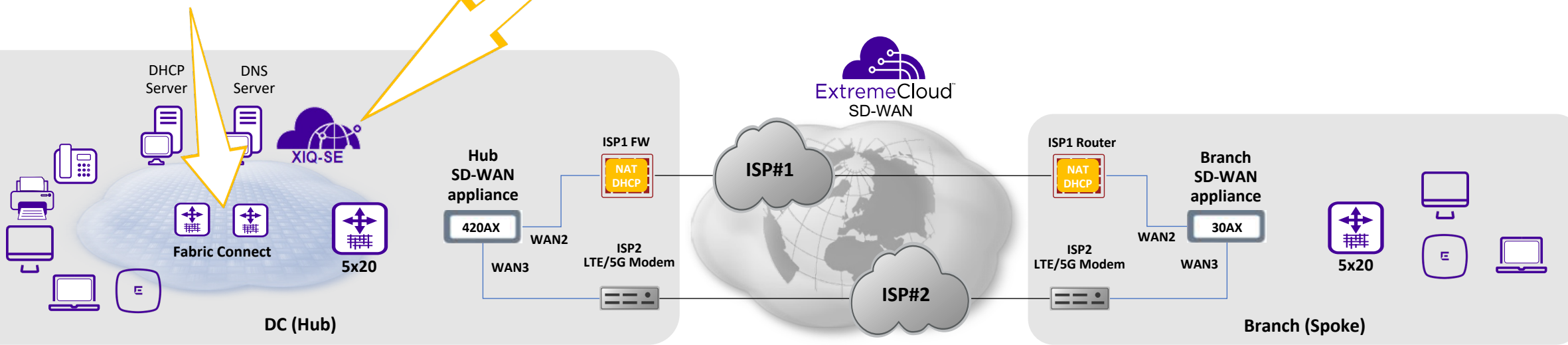
Low priority





Deployment with Zero Touch Onboarding

- Prepared head end fabric for Zero Touch Fabric
 - DHCP on Onboarding I-SID segment
- Can be done on any fabric switch in the Hub site
- Prepared XIQ-SE for ZTP+ onboarding
 - Site assignment
 - Management VLAN IP or CLIP assignment
 - Adding switch to Access Control / Policies
 - Adding switch to Analytics
 - Every other aspect of switch config



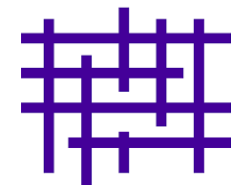


#WeAreExclusive

**Long story
short**



Extreme Fabric Connect Concept



Powerful network virtualization technology

- Based on IEEE/IETF Shortest Path Bridging
- Increases agility: services abstracted from infrastructure
- Increases security: user traffic invisible to the network core
- Increased automation: implicit and explicit

Traditional

- MPLS
- BGP
- PIM
- OSPF
- STP
- 802.1

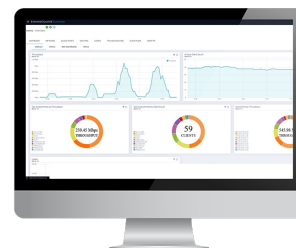
Extreme Fabric Connect

1 Protocol
(IEEE/ IETF Shortest Path Bridging)

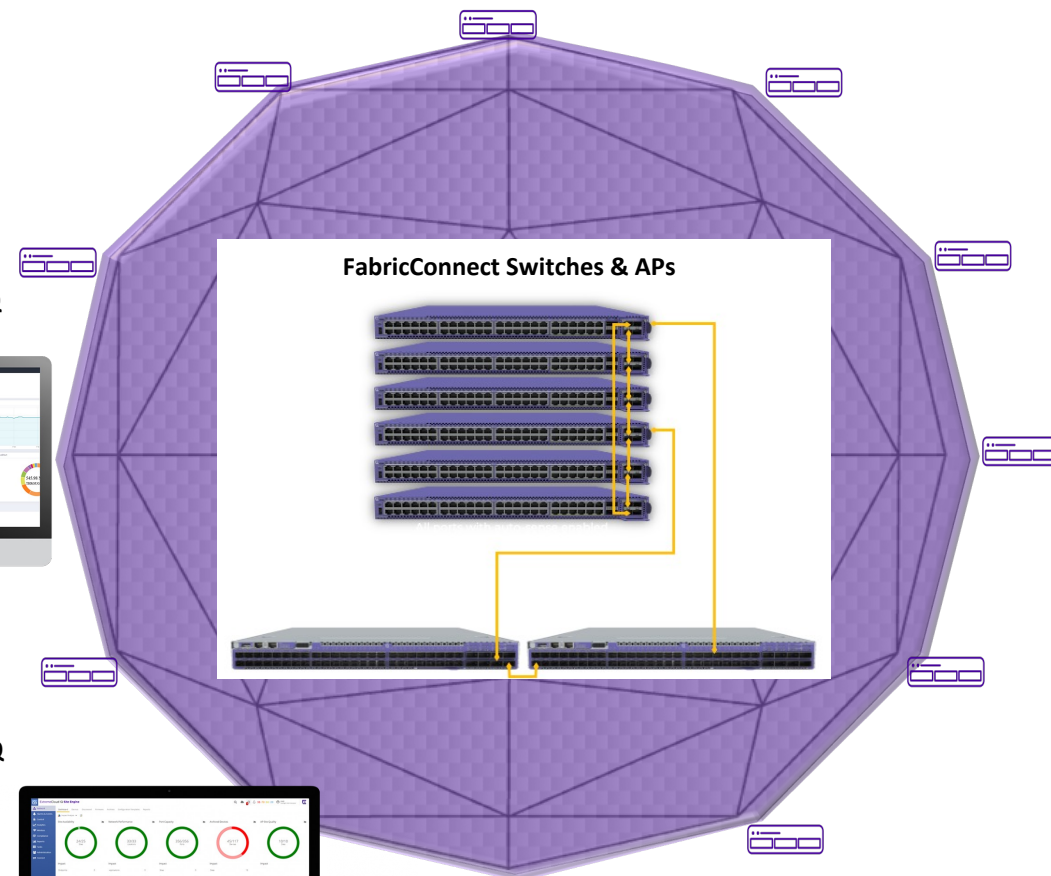
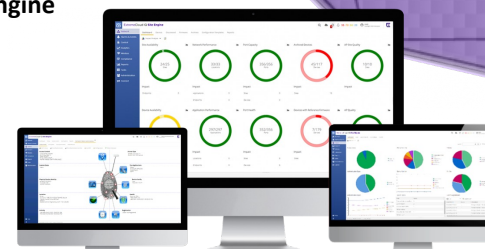
Fabric Connect Benefits:

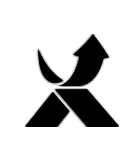
- Faster to Deploy
- Increased Stability
- Easier Troubleshooting
- Faster Resiliency
- Lower Costs

ExtremeCloud IQ Controller



ExtremeCloud IQ Site Engine





CASE STUDY: ŠKODA AUTO

ŠKODA



ŠKODA AUTO, based in Mladá Boleslav, is a leading industrial enterprise in the Czech Republic and one of the oldest carmakers in the world. Today, ŠKODA AUTO employs over 30,000 people, operating as part of the Volkswagen Group for nearly 30 years. As a result of growth and expansion, the company outgrew its network infrastructure. ŠKODA partnered with Extreme to deploy a next-generation network capable of meeting their technical requirements and providing the foundation for the business to grow.

“Extreme Fabric Connect eliminates risk of outages and disruption and provides network virtualization solution poised to drive stability and scalability.”

Technology Requirements

- Multiple networks needed to be condensed into one, Reduce costs and increase efficiency
- Continuous uptime to power staff and vehicle manufacturing
- Ease of management via automation capabilities

Solution Components

- Extreme Fabric Connect™
- ExtremeAnalytics™

Results

- Eliminated risk of unplanned outages
- Virtual networks can be created and configured in one hour instead of one day
- Time required for service outages reduced by 50%
- Mitigated financial risks associated with outages
- Multiple separated physical networks converged into one fully virtualized network, managed through a single pane of glass



#WeAreExclusive



Thank you

BeExtreme!