BBQ Fabric!

Juha Lindström

Senior Systems Engineer

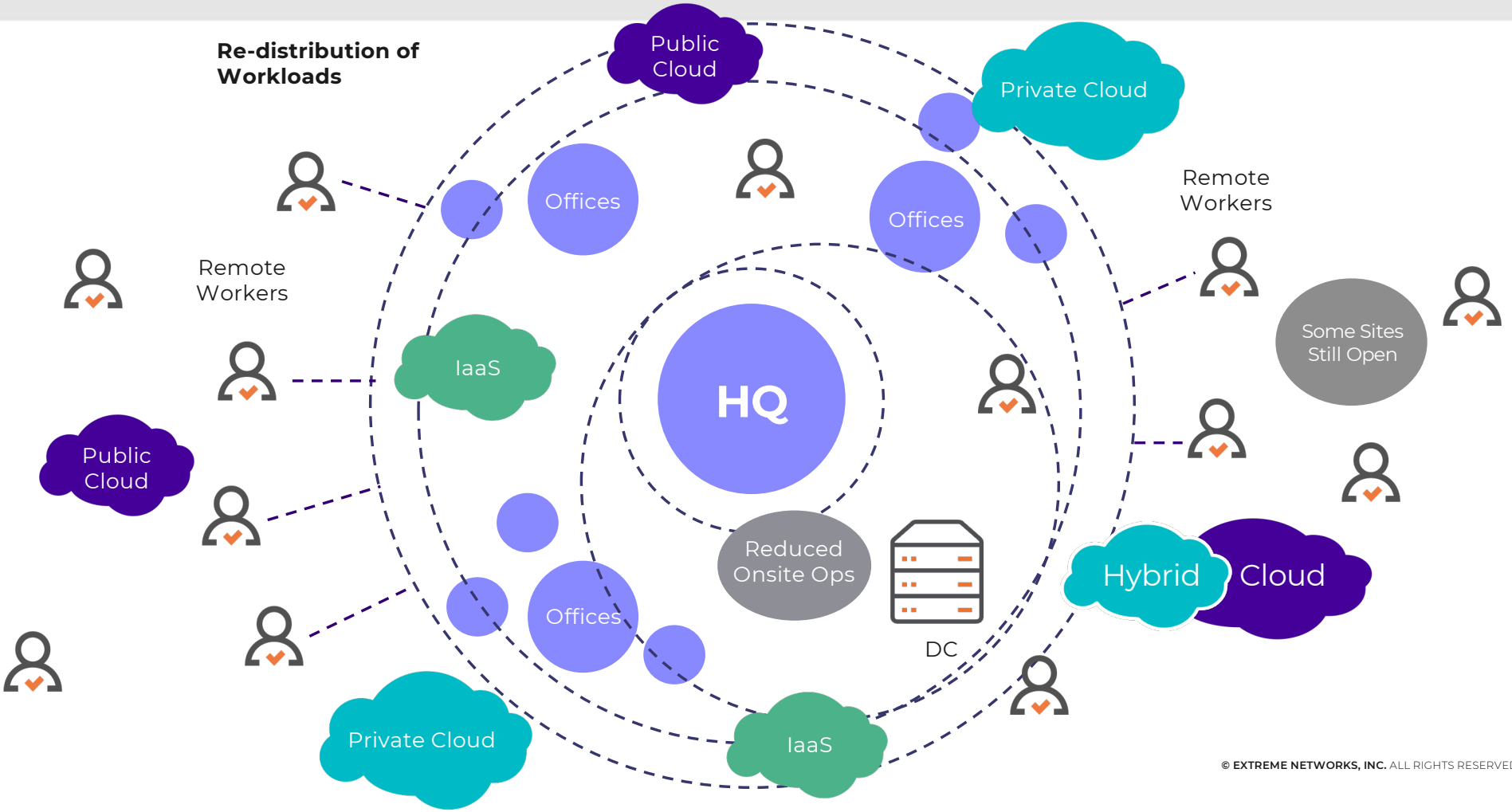
Extreme Networks, Finland & Baltics

jlindstro@extremenetworks.com

Extreme networks

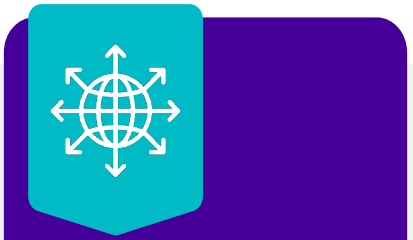
What is Perimeter Based Security?

Where is the perimeter?

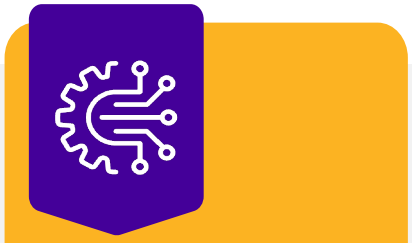


What is Zero Trust Networking?

Never Trust, Always Verify

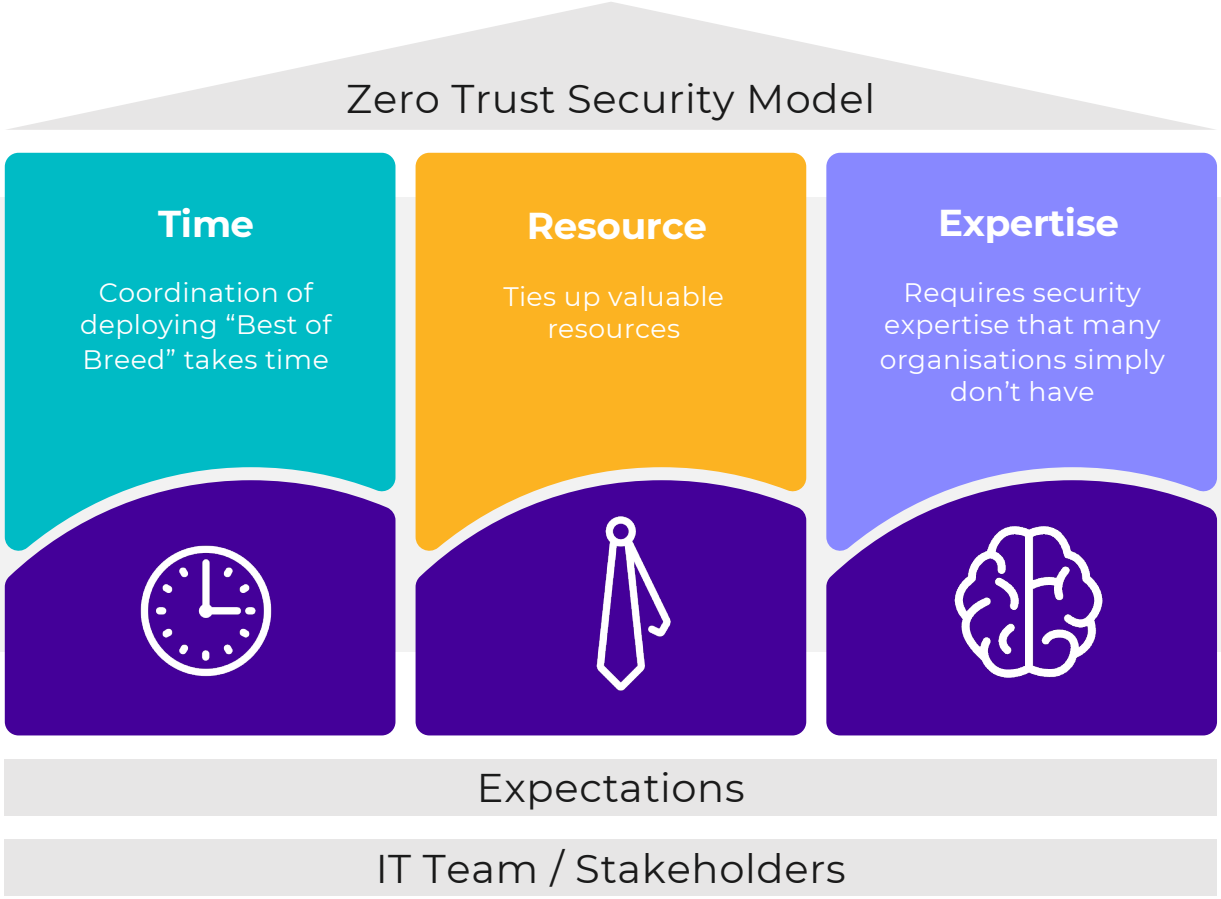


Least Privilege Access



Assume Breach

Implementing Zero Trust Networking – What it takes?



The Problem – Organizations Left Behind

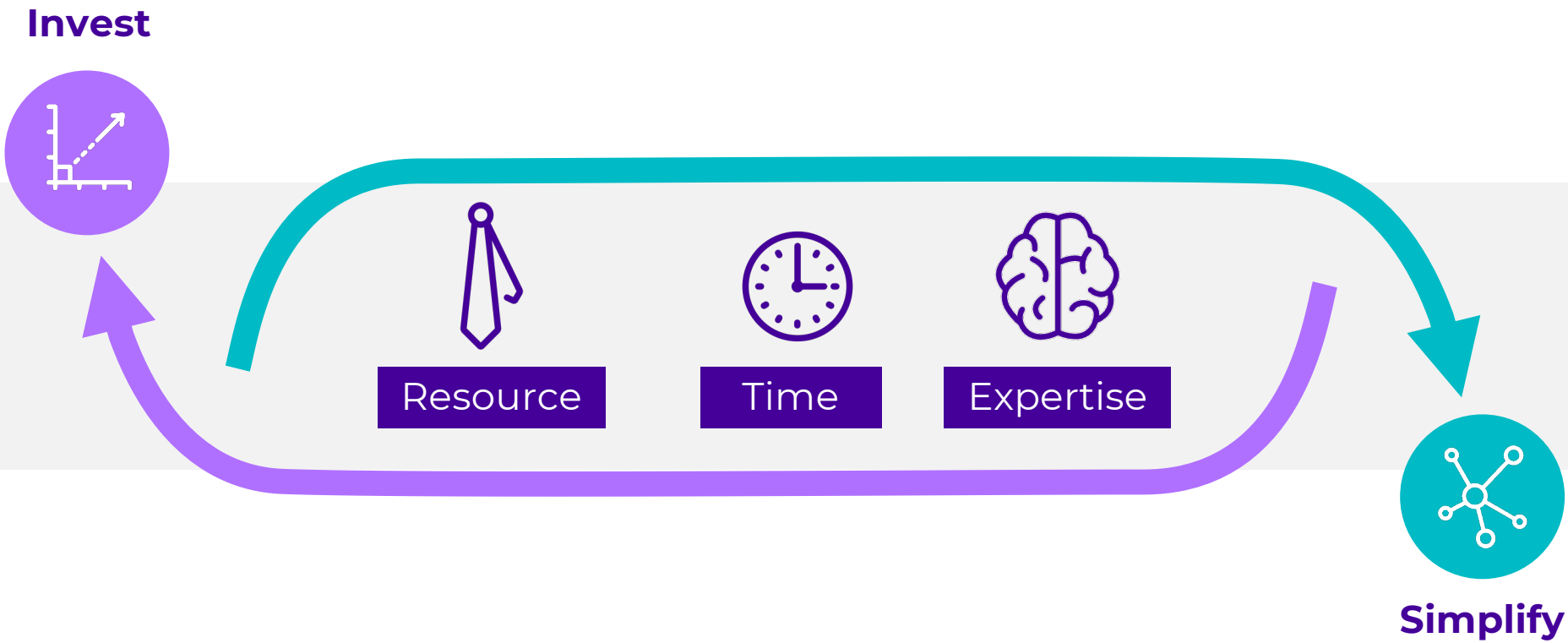
Why?

- Network managers often have security responsibilities
- Cost
- Difficult to deploy
- Difficult to manage
- Do not have the resource

Who?

- Public Sector
- SME
- Enterprise
- Retail
- Transport and Logistics

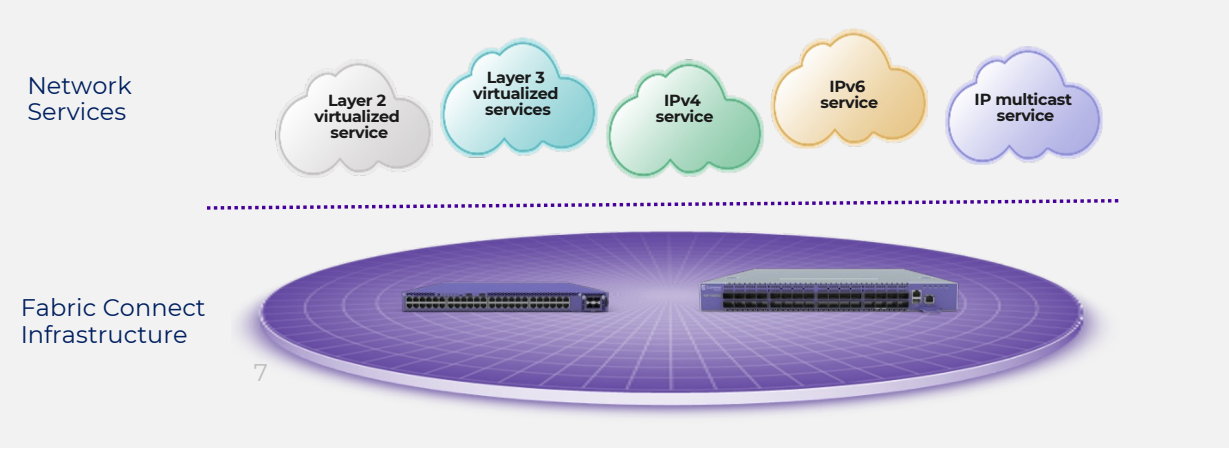
Two Approaches to Move Forward



What is Fabric Connect?

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; services operate as ships in the night

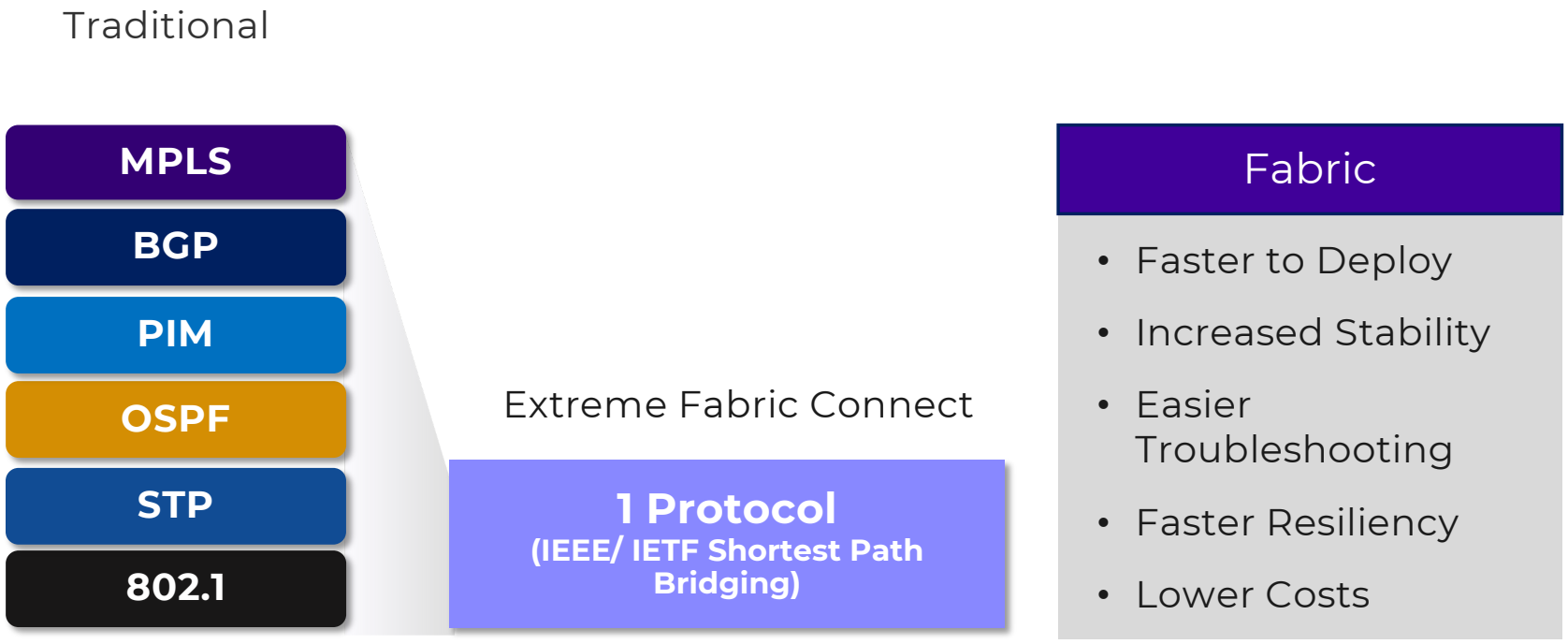


Key Technology attributes:

- Forwards traffic based on Ethernet Switched Paths
- Control plane is based on IS-IS routing
- Controllerless technology
- Highly Differentiated

Network becomes a plug and play utility

How to simplify? – Less protocols, less complexity



"When you look at Fabric Connect, you'll say, 'It can't be that easy,' but I'm telling you it works." ***- Promedica***

One Technology - Simplifies and Automates

Other Fabrics

Controller-based approach

- VXLAN
- LISP
- BGP
- PIM
- OSPF
- 802.1

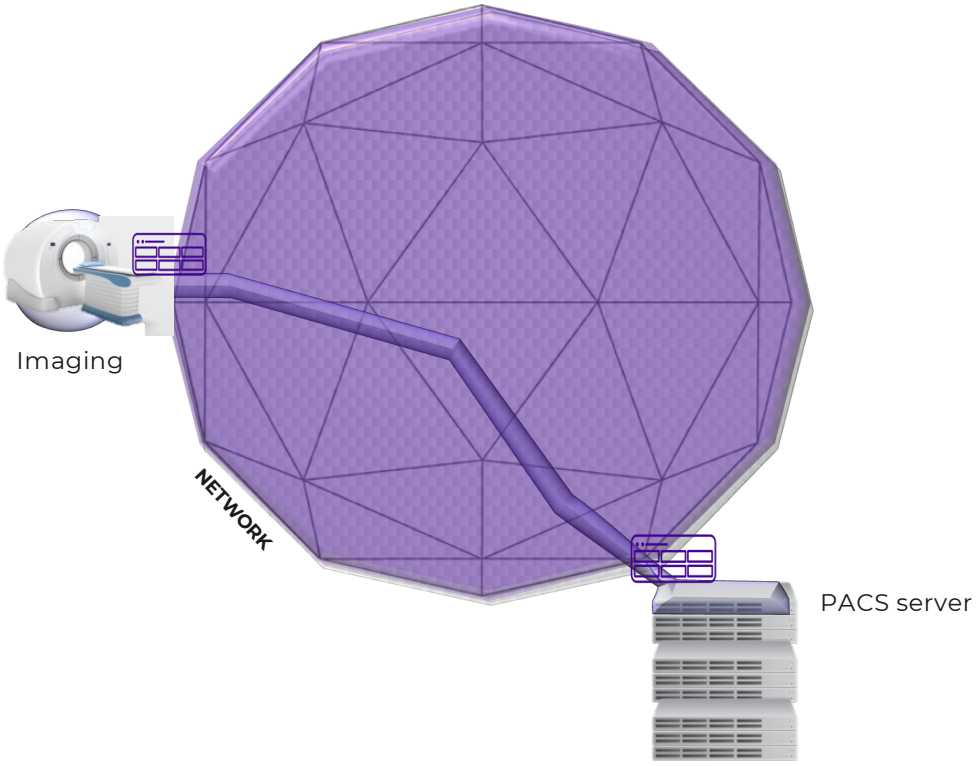
Extreme Fabric Connect

1 Protocol
(IEEE/ IETF Shortest Path Bridging)

Inherent automation

"Fabric Connect is logical – the way networks should be." - ***Norwegian State Railways***

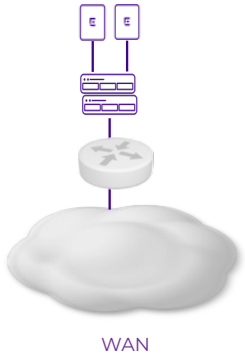
Delivers a Hands-off network aggregation / core

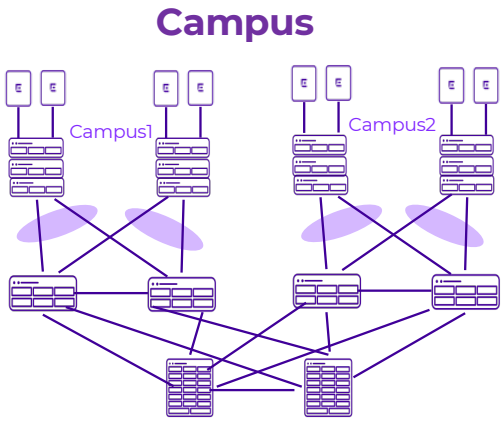


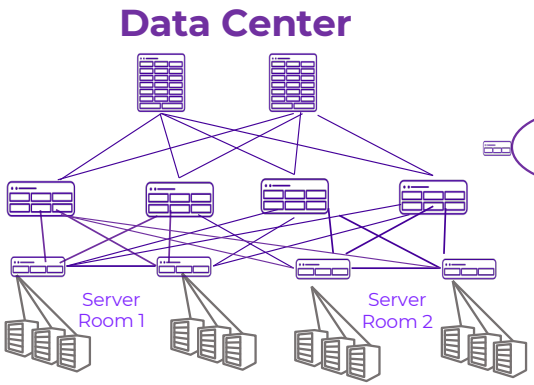
- Eliminates time consuming hop by hop provisioning
- Services are enabled by provisioning the edges only (ToR and access switches)
- Core and aggregation nodes are built out once then hands off
- Better stability, enhanced ability, reduced chance of human error

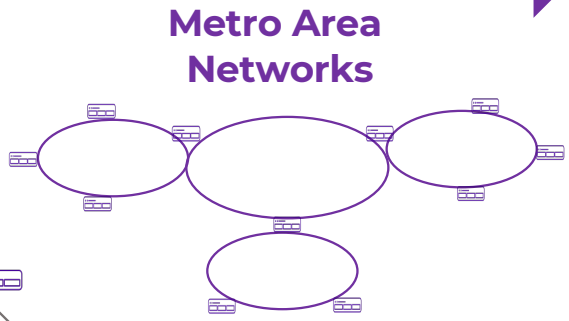
"Before Fabric Connect to extend a VLAN [Virtual Local Area Network] between the two data centers, we had to configure 36 uplinks on 17 devices, and in doing so we risked creating loops and errors. Now we don't have to configure any uplinks: we just set up the VLAN on two devices" ***– City University in London***

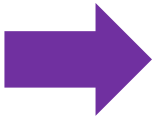
Only Fabric Technology that Extends Enterprise Wide

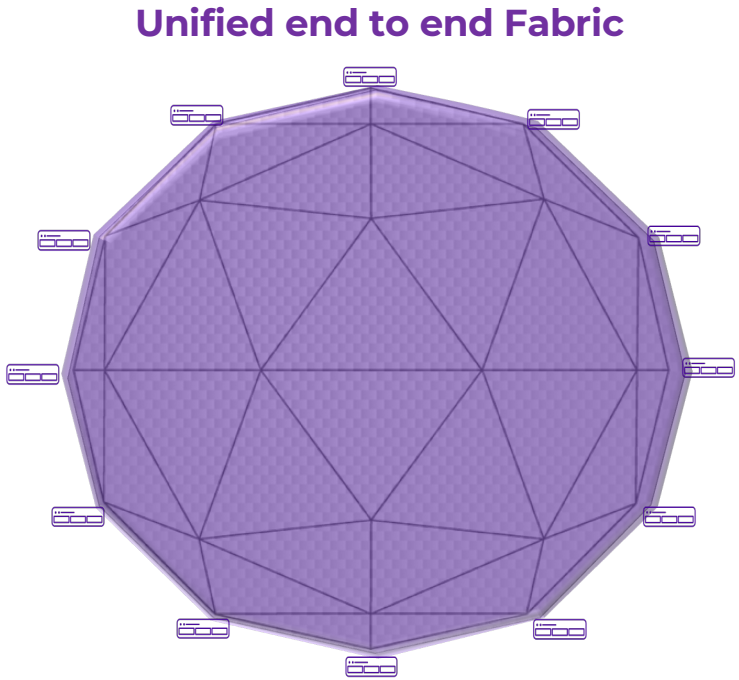






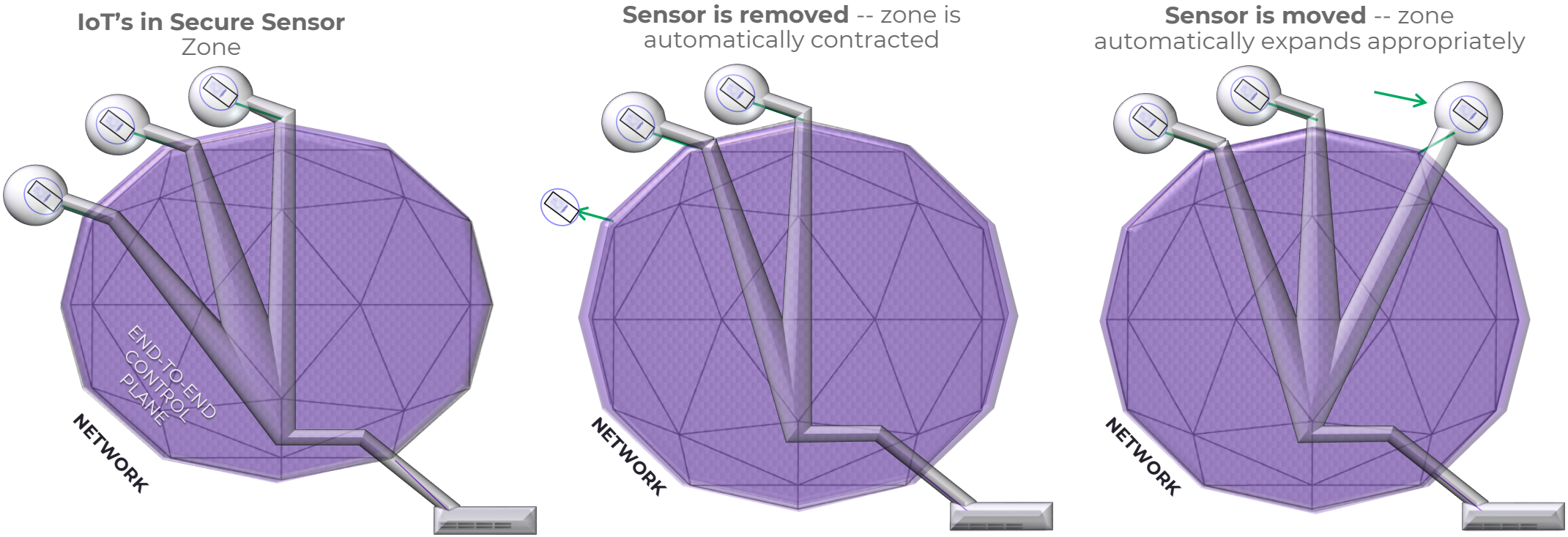






Only Fabric that provides a loop-free, redundant network across <u>any</u> physical topology

Fabric Connect and Fabric Attach = Service Elasticity

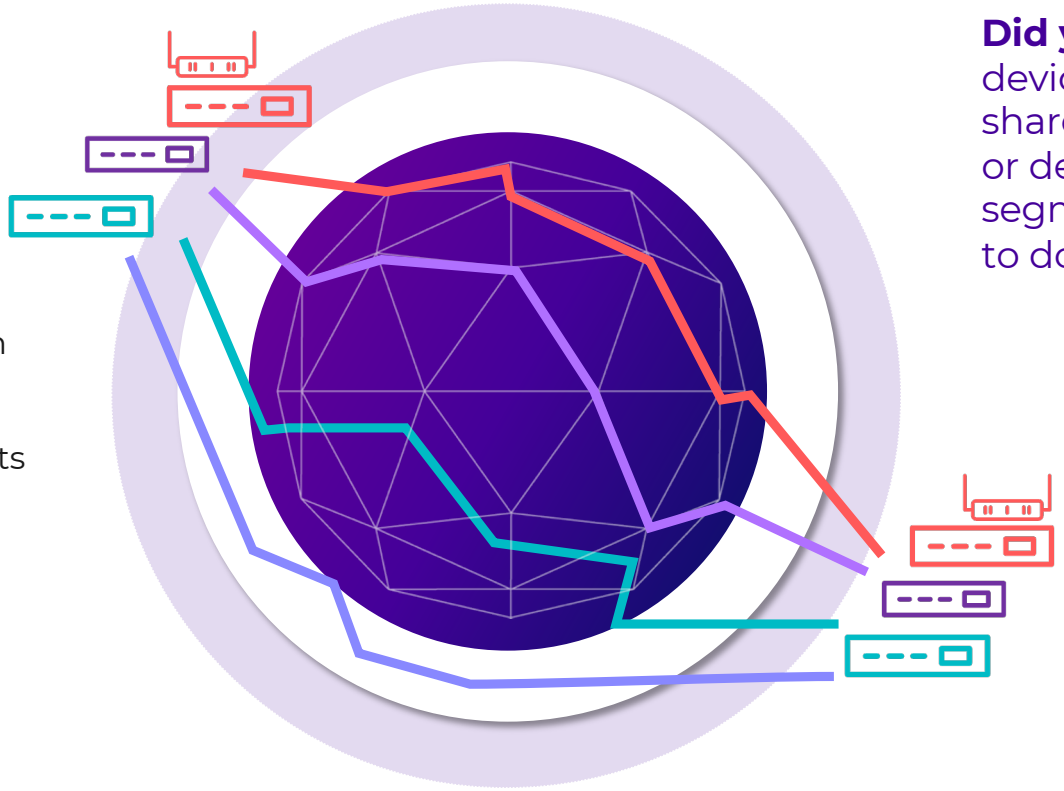


Increased agility with plug and play end points and APs without complex scripting or controllers

Where is the ZTNA? HYPER-SEGMENTATION locks down network traffic, services

Key Values:

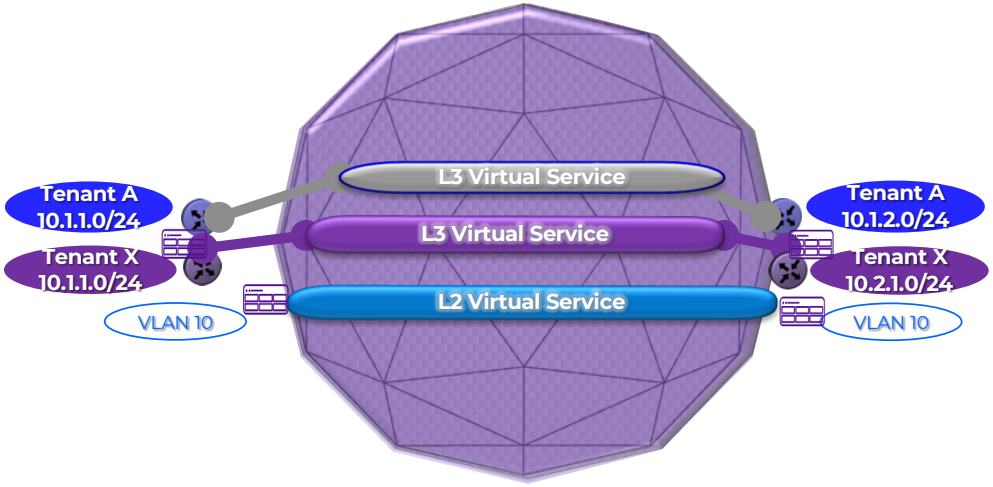
- **Isolated by design:** Segments are separate and secure
- **Provisioned at the edges:** Users and devices are hidden from the core
- **Massive scaling:** Assignments follow the user or device
- **Segments extend network-wide**
- **Control** secure segment access through policy/NAC



Did you know? A user or device in one segment can't share resources with a user or device in another segment unless configured to do so.

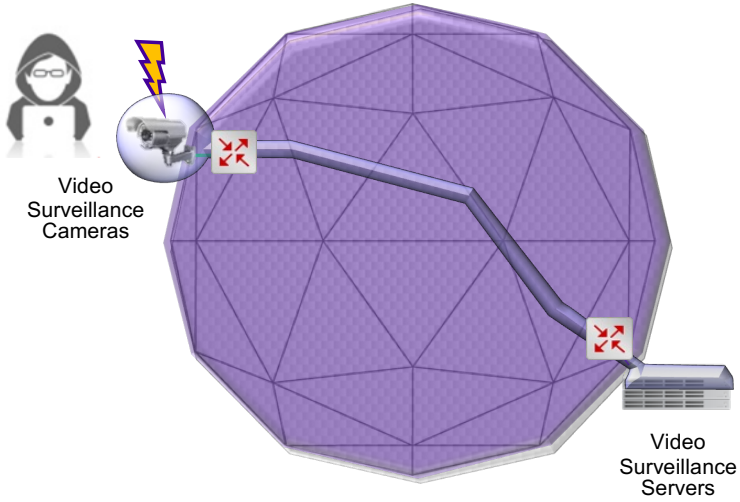
Simple, scalable segmentation within a Stealth Topology

Fabric Connect
Segmentation end to end at scale



- Complete isolation between services
- Provisioned at the edges only
- Massive scaling
- Segments extend network-wide

Fabric Connect
Forwarding based on Ethernet Switched Paths



- No IP required to forward traffic
- Network topology is therefore dark when scanned
- Breaches contained; damage minimized

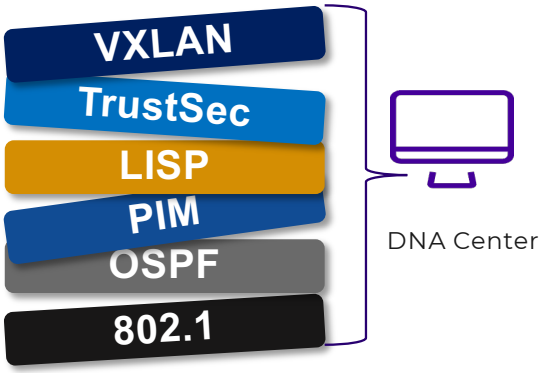
Unbreachable in multiple Hack-a-thon events

EXTREME FABRIC
Competitive View
(Cisco and HPE / Aruba)

Extreme Differentiation: Simplest Fabric Technology

Cisco Campus Fabric:

- IP Fabric (BGP/EVPN) derivative
- Many control planes
- Campus only (DC requires ACI fabric)
- Introduced in 2016



Extreme Fabric Connect:

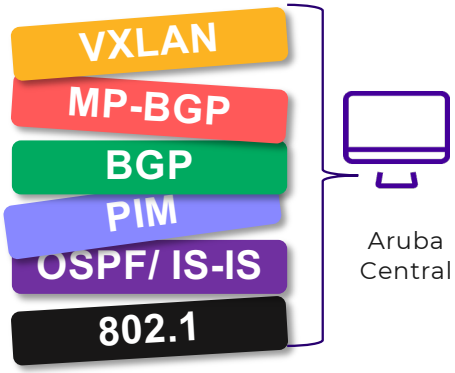
- IEEE/IETF standardized
- One control plane
- Enterprise-wide
- Mature technology (First deployments 2011 / 2012)

Benefits of single control plane

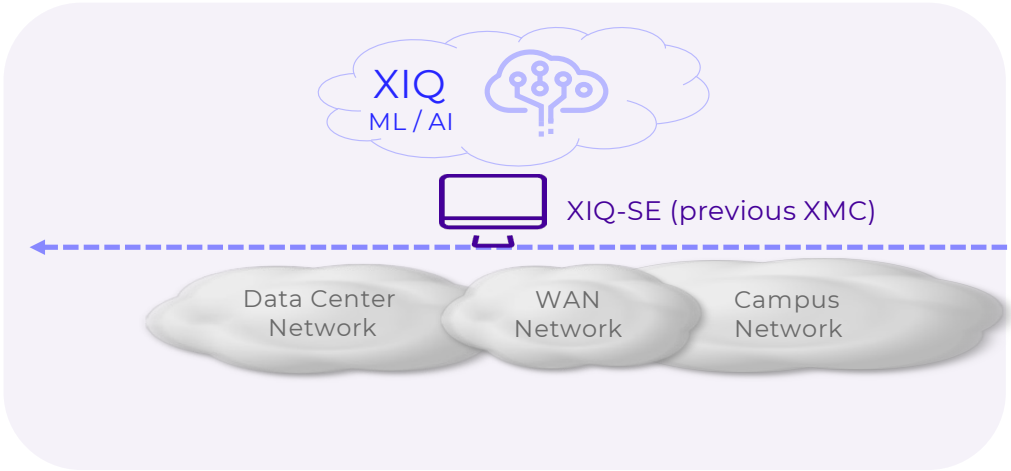
- Faster to Deploy
- Increased Stability
- Easier Troubleshooting
- Faster Resiliency

HPE / Aruba IP Fabric:

- IP Fabric (BGP/EVPN)
- Many control planes
- Converged Data Center / Campus cores
- Introduced late 2019

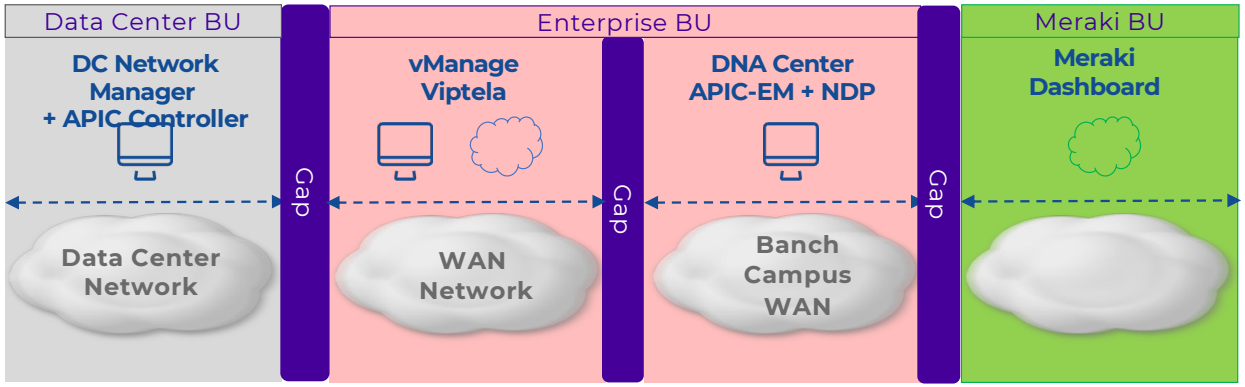


Extreme Differentiation: One Operational Model

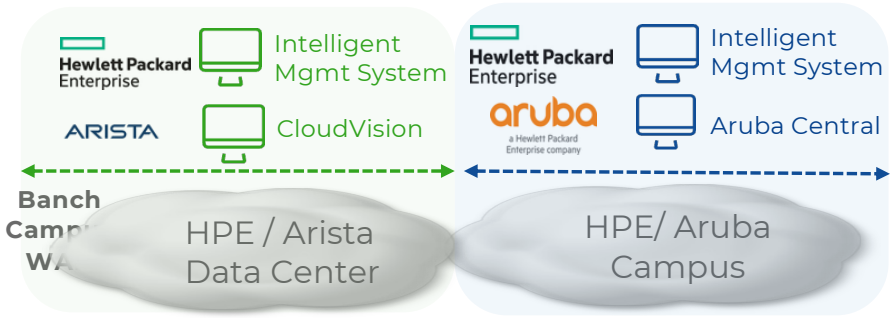


Single Operational Model:

- Wired/ wireless edge to Data Center to Cloud
- End to end view of services to simplify troubleshooting
- Simplified deployment and training
- Connectors between XMC and XIQ for manager of manager capabilities and AI/ML driven insights



Separate Operational Domains & Business Units. No Aligned Strategy

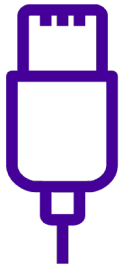


Separate operational domains; separate vendor offers

Extreme Differentiation: Unified Wired / Wireless

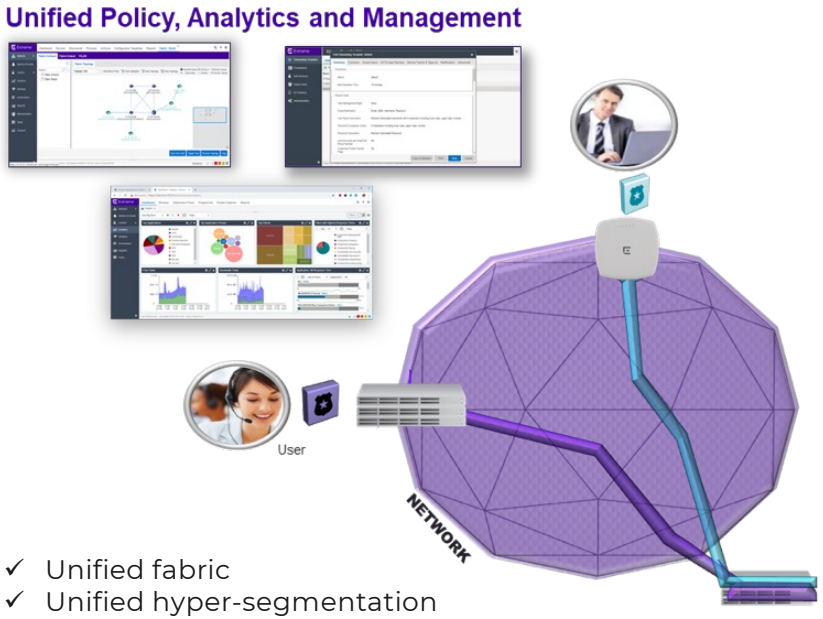
Cisco

✓ Wired centric architecture



× Complex integration between fabric and wireless controller
× Lack of WiFi 6 AP integration into Fabric
× Complex segmentation with ISE and TrustSec

Extreme



✓ Unified fabric
✓ Unified hyper-segmentation
✓ Plug and play APs and dynamic auto-attach with Fabric Attach (no scripting required)
✓ Consistent management
✓ Consistent policies
✓ Consistent analytics
✓ Seamless roaming (IP subnet extension)

HPE / Aruba

✓ Wireless centric architecture

× Lack of fabric extension to APs
× GRE tunnels for segmentation across wired and wireless (complex and lacks scale)
× Application visibility in wireless but doesn't extend to wired network

Competitive Matrix - FABRIC

	Extreme	Cisco	HPE/Aruba
Control planes required	**One:** IS-IS	**Many:** underlay and overlay	**Many:** underlay and overlay
Fabric Maturity	**Very:** Deployments started in 2011/2012	**Limited:** Introduced in 2016	**New:** on Campus core switches
Controller-based	**No:** Automation inherent in protocol. Optional use of NAC/XIQ-SE (previous XMC).	**Yes:** DNA Center (reports of inability to toggle between CLI and controller)	**No**
Extends enterprise-wide	**Yes:** one technology from Data Center to wired/wireless edge	**No:** Campus only, no extension across WAN or into Data Center	**No:** Converged campus / DC cores only
IP Multicast	**Simple:** only scalable, high performance multicast without PIM	**Complex:** PIM required in either underlay or overlay or both	**Complex**: PIM required in either underlay or overlay or both
Deployment	**Simple:** Based on customer feedback can be deployed quickly with minimal training	**Complex:** Takes 13 high-end UCS appliances for customers to fully take full advantage of DNA	**Unknown:** IP Fabric on Campus core switches is so new, deployment is unknown/ unproven
Licensing	**Simple:** Based on desired features. Perpetual or subscription	**Mandatory:** DNA licensing is mandatory for every switch/AP sold. Many ppl pay for unused features	**Standard**
Segmentation	**Simple:** inherent in fabric, edge provisioning, scalable	**Complex:** Requires TrustSec plus ISE	**Complex:** GRE tunnels / not scalable, complex (EVPN option)
Stealth topology	**Yes:** Ethernet forwarding	**No:** IP underlay	**No:** IP underlay
Operational model	**One: XIQ-SE (previous** XMC) end to end	**Many:** Data Center Network Manager / APIC controller for DC operations, DNA Center for Campus, vManage for WAN, Meraki for Cloud wired and WiFi.	**Few:** Separate Data Center and Campus operations
Analytics	**Comprehensive:** Network and application analytics end to end. Consistent across wired and wireless	**Disjointed:** Multiple tools with limited integration. Network analytics through DNA Center/ Assurance; Application analytics through AppDynamics	**Lacking:** Strong wireless analytics but Aruba's switches lacks the packet- and flow-level analytics needed for true application finger-printing.

EXTREME FABRIC Implementation considerations

How do I get started?

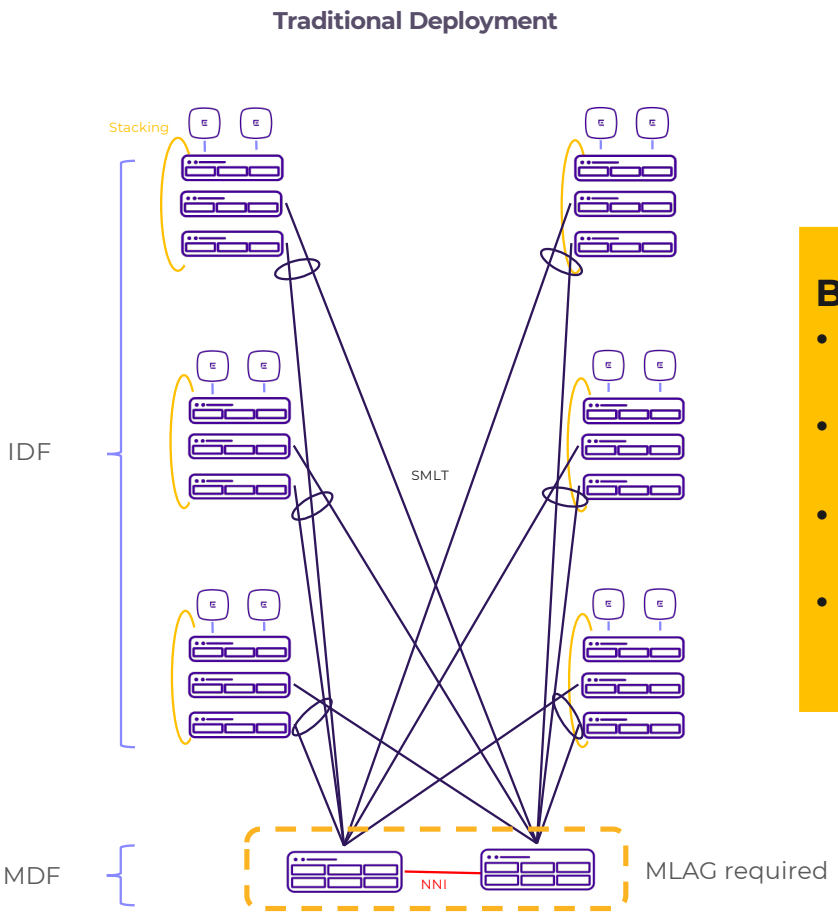
Set your goals

- How many segments do I need?
- What is the size of segments?
- Define you user groups / segments
- Define who needs access and where
- How is your current AD built?

What else?

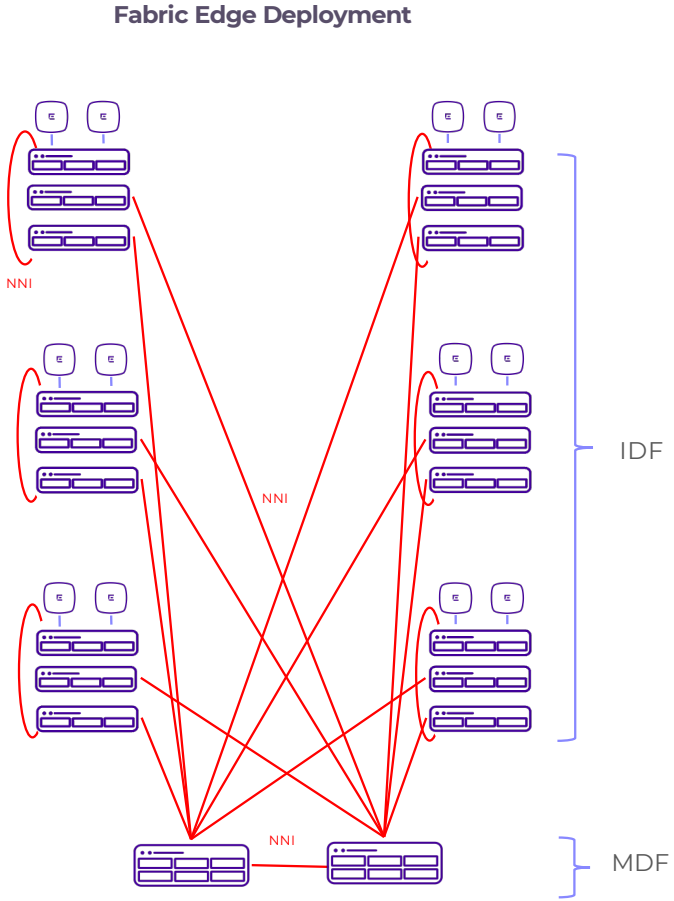
- Schedule – not everything can be done at once
- Where is your routing done?
- IP addressing – new segments, new IP's
- Build NAC policies
- Build device templates for ZTP+

Deployment Options – physical topology



Benefits:

- No edge configuration
- No more stacking
- No more MLAG in distribution
- Topology freedom



Automation Background: Understanding the Approaches

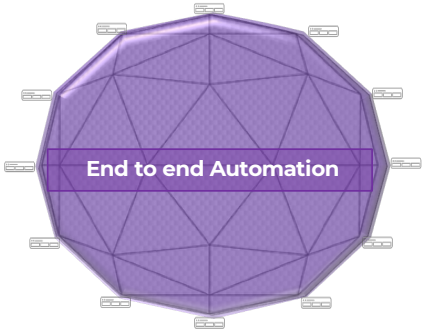
Explicit Automation

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

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

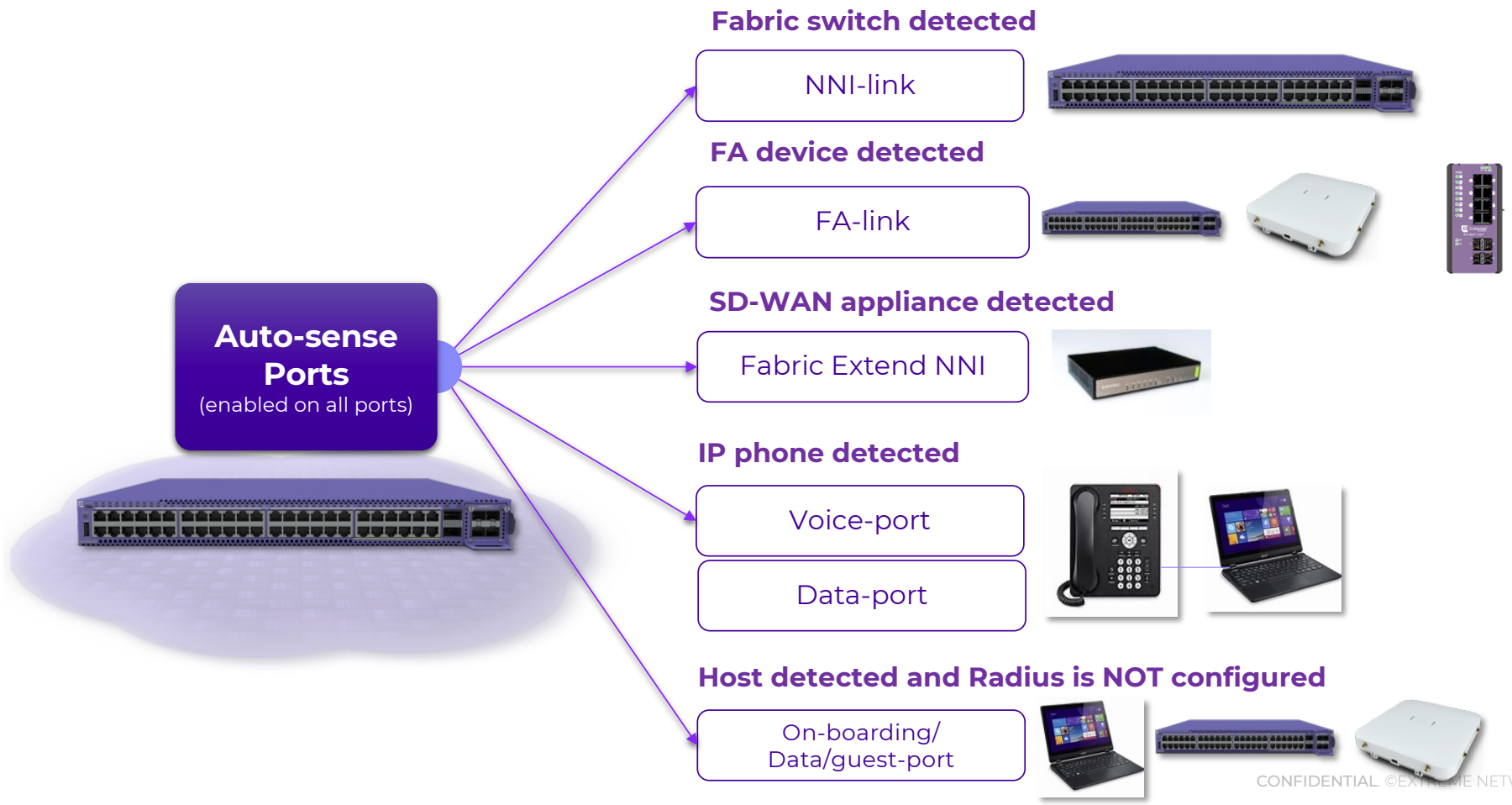
Implicit Automation

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



Example: Fabric Connect

Zero Touch Fabric - Auto-Sense Ports



What you can expect

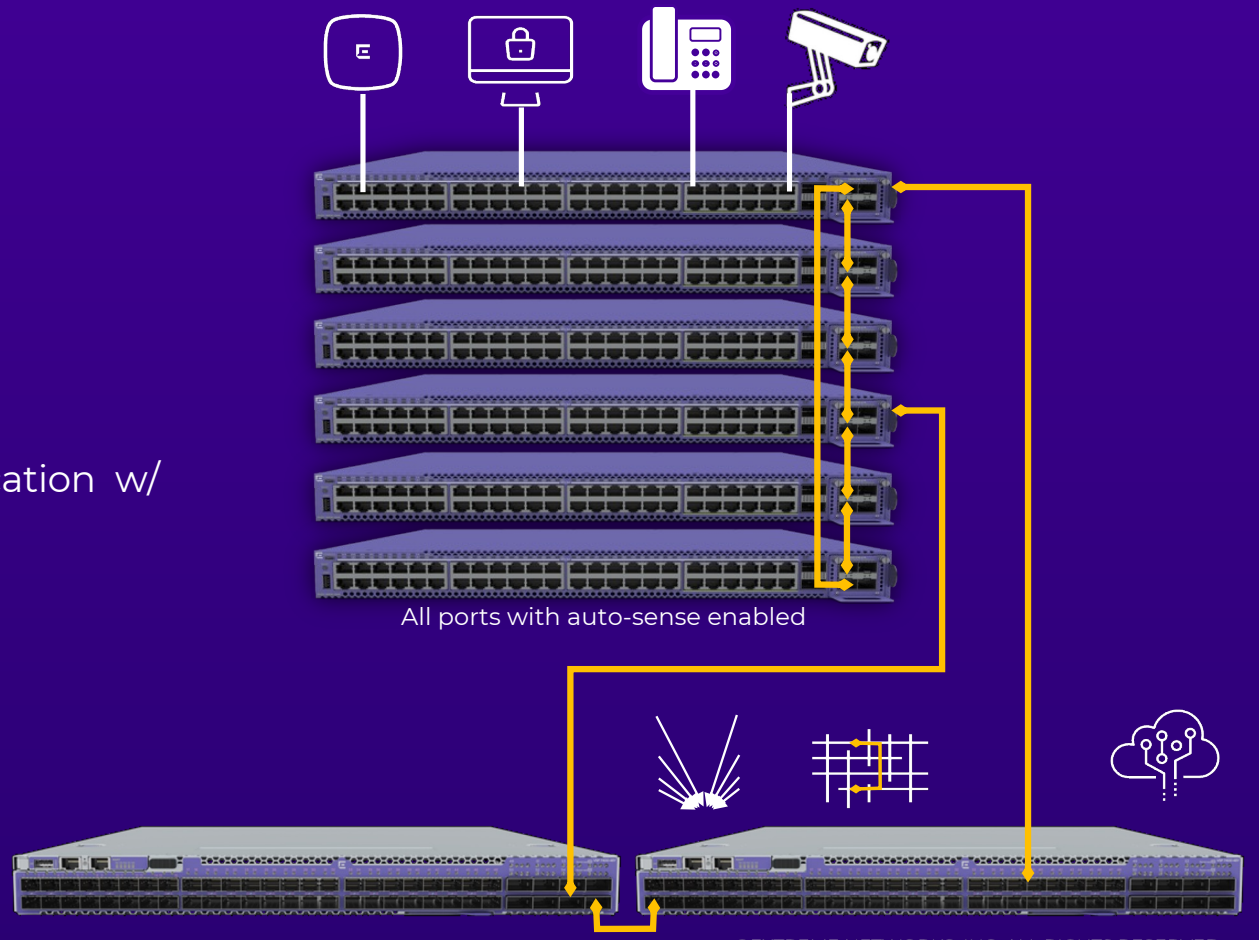
- Prerequisites:
  - Network management infrastructure with XIQ-SE or XIQ & DHCP Server
  - Existing Fabric core works as seed for new device(s) to ease Fabric onboarding with fabric ids and reachability to Network management infrastructure (VOSS 8.3+)
  - New Fabric no seed needed, built automatically

1. **Unbox new Universal Hardware switch**
2. **Connect it to network**
3. **Power up the device**
4. **Zero Touch Fabric (ZTF): Switch joins fabric**
   - **Uses implicit automation**
5. **Zero Touch Provisioning (ZTP+): Switch onboards to XIQ-SE & XIQ**
   - **Uses explicit automation**

For New Customers: True Automation; Highly Differentiated

Automation Elements:

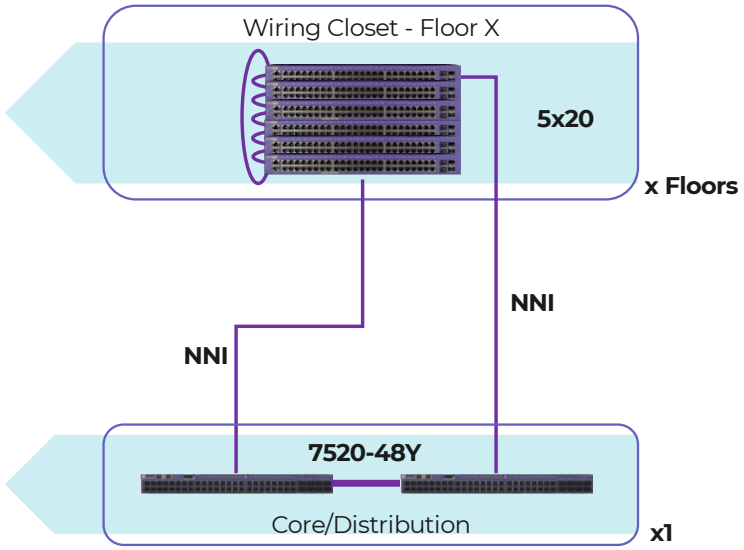
- Zero-Touch-Fabric
- Auto-Onboarding Segment
- Auto-Onboarding to XIQ-SE/EP1
- EAPoL/NEAP based User authentication w/ VLAN/VSN and Policy assignment
- Auto Fabric Attach
- Auto IP Phone Integration
- FA Zero-Touch-Client



Fabric Edge Deployment Decision Points

Fabric Edge deployment – step by step

- 100% Zero Touch Deployment



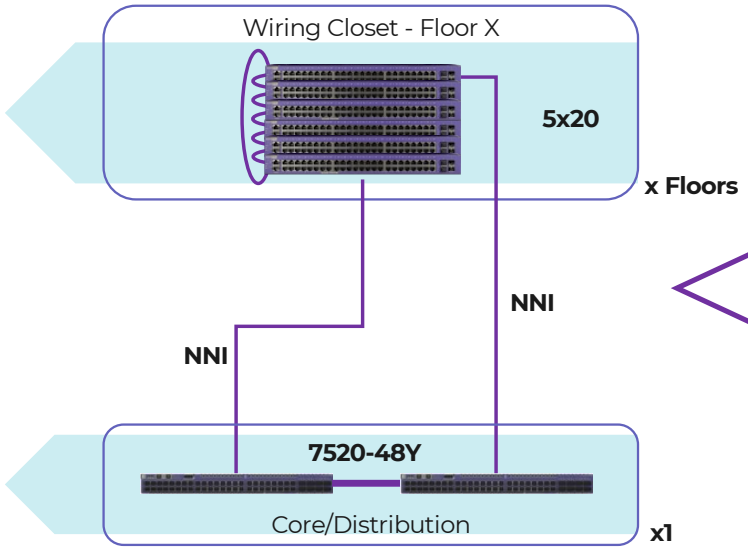
- Existing Core either upgraded to VOSS 8.3+ or green field deployed
- Some config may be required

- The real benefits of ZTF and ZTP+ are in the Fabric edge deployment
- The core does need some “seed” configuration to allow ZTF and ZTP+ to work correctly. Either the core is upgraded to VOSS 8.3 and the “seed” config added OR the core is also green field deployed
- Core “seed” config includes ISIS Area, SPBM Backbone VLANs, Nick-name server, DHCP-relay for onboarding I-SID, etc..

Fabric Edge deployment – decision point ISIS Multi-Area

- No stacking ➔ every unit counts as 1 SPB node

- Fabric core



Multi-Area ?

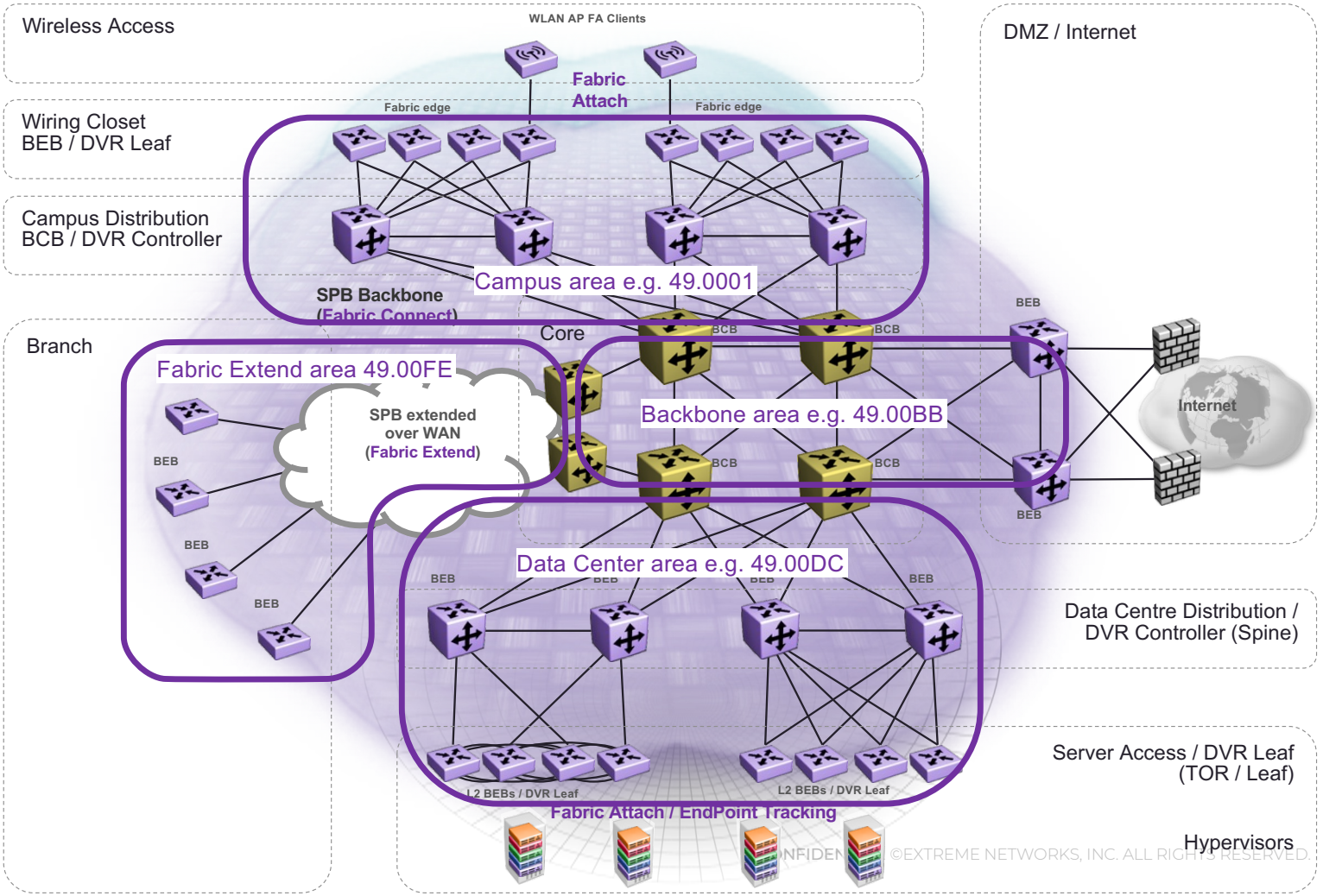
Switch Model	Max SPB nodes
VSP 8600	1200
VSP 8000	800
VSP 7400	2000
VSP 7200	800
VSP 4900	550
VSP 4450	550
XA 1400	550
7720,7520	2000
5720	1000
5520	800
5420	500/350
5320	500/350

- Scaling limit of number of SBP nodes in same area is 500 nodes
  - Can be higher on some switch models
  - Can be lower on some models (5320 & 5420)
    - Determined by spbm-node-scaling boot flag (enabled = 500; disabled = 350)
    - Values can drop even lower (150/200) if IP Multicast in use on all BEBs
  - Is determined by lowest capable switch deployed

- Deploying Fabric to the edge will have a big impact on the number of SPB nodes, as every Fabric edge unit will count for 1 SPB node
- If count of SPB nodes is close or over 500, then a Multi-Area design is required

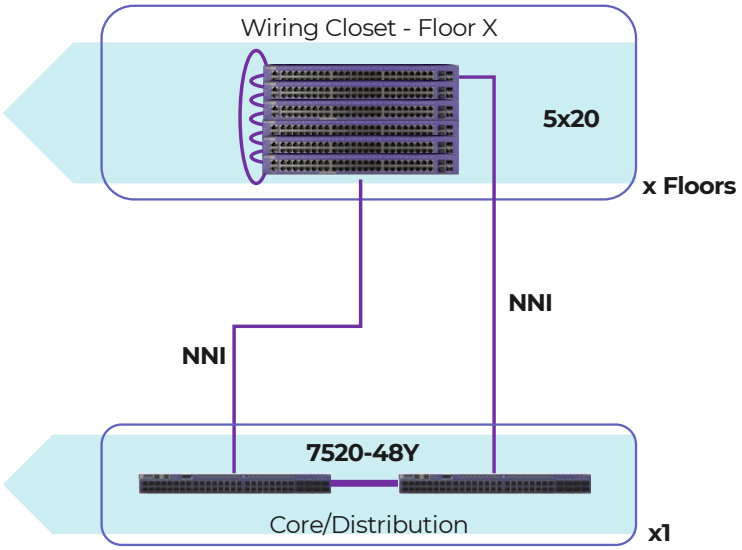
Fabric Connect Multi-Area with Campus Fabric Edge

- Each area supporting up to 500 SPB nodes
- Ability to control in which area VSN services are available
- Multi-Area support
  - VSP7400 (VOSS8.4)
  - 7720,7520, 5720,5520 (VOSS8.10)
- Diagram shows a possible sample of Multi-Area config



Fabric Edge deployment – Gateway redundancy protocol

- **DVR**: Prefer for Data Center
- Pros:
  - Optimal traffic L3 flows
  - Gateway defined on Controllers, routing happens on DVR Leaf
- Cons:
  - Overall DVR design needed to determine number of DVR Domains
  - Only Switched-UNI port/vlan config supported
  - DVR does host routing on access DVR Leaf; requires higher end models for host route scaling and lower end models (5320/4220) do not support DVR
  - Stretching a L2VSN outside of DVR domain is delicate and requires use of DVR-VRRP
  - No IPv6 support



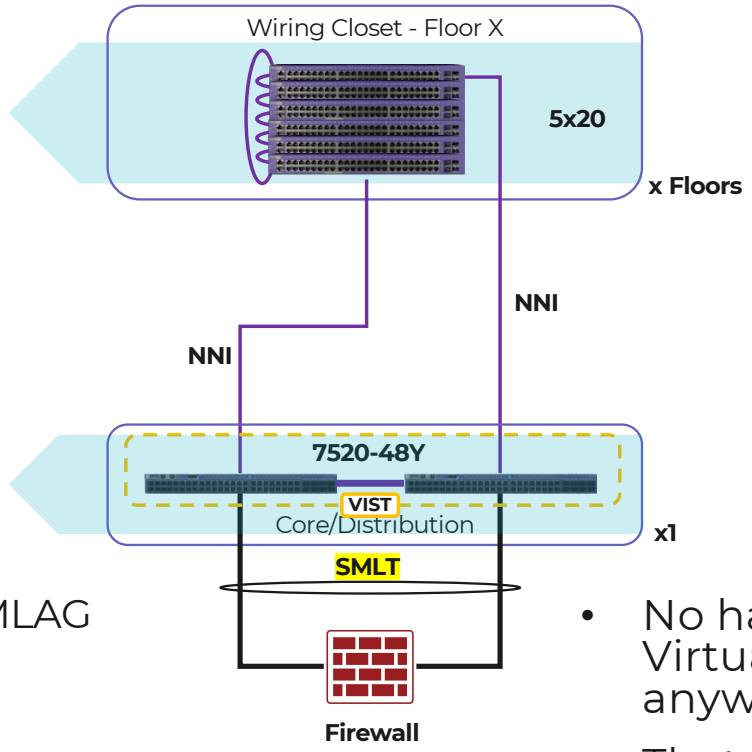
- **Anycast Gateway**: Prefer for Campus
- Pros:
  - Access switch always uses nearest Anycast Gateway
  - No IPv6 support
- Cons:
  - Access switches must have baseline 9.1 software version
  - No IPv6 support

- **VRRP**: Use where Anycast Gateway or DVR not possible
- Pros:
  - Always works
  - IPv4 & IPv6 support
- Cons:
  - Only the VRRP Master is actively IP routing traffic for the VLAN
  - Backup-Master mode will not work with fabric to the edge

Fabric Edge deployment – decision point SMLT/MLAG

- Usually, no MLAG requirements

- No MLAG requirement for supporting Fabric edge

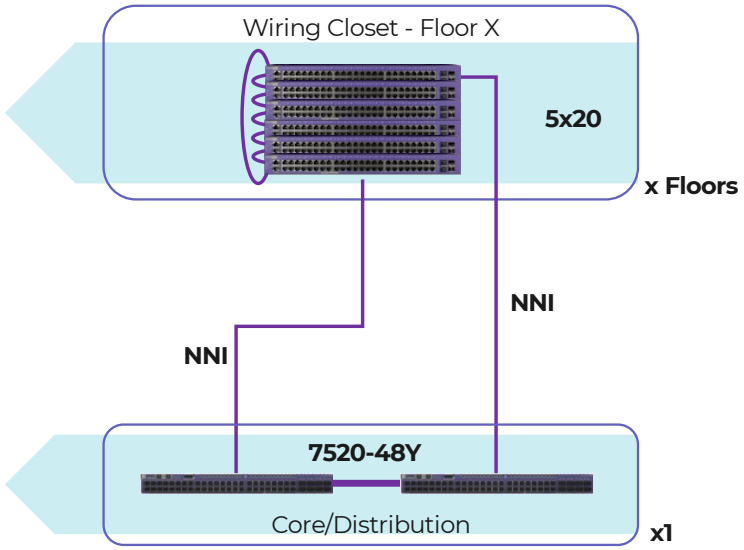


- There is no need to run MLAG (SMLT Clustering) on the Distribution/Core
- Unless there will be a requirement to SMLT connect non-fabric devices to it, such as Firewalls or legacy FA Proxy access

- No harm in provisioning a Virtual-IST on the Fabric core anyway
- That way, if an SMLT connection is required at a later date, no downtime is needed to configure a vIST

Fabric Edge deployment – decision point NAC

- Network Access Control (NAC)

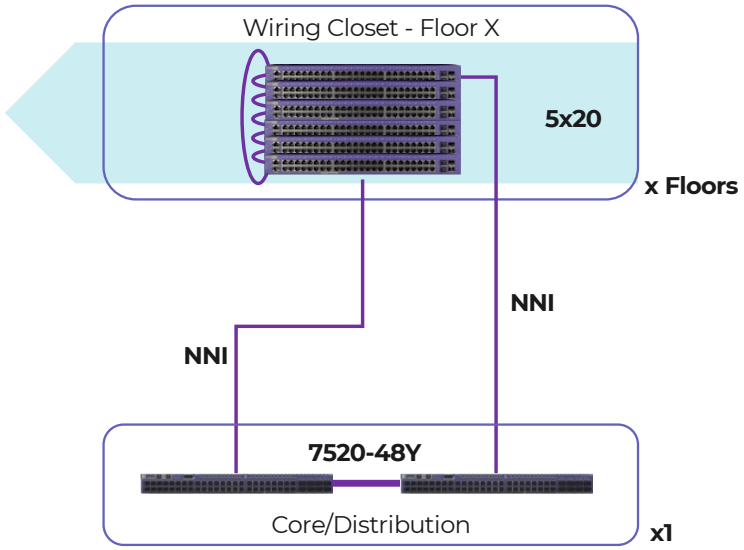


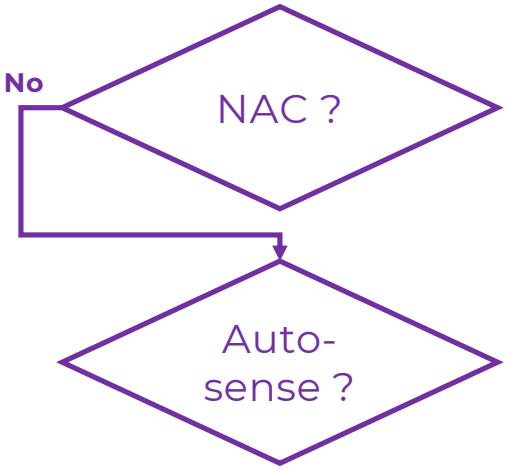
- Typically, no NAC on Core/Distribution, but it can also be enabled

- Will users and devices be EAPoL (802.1X) or MAC authenticated against a RADIUS Server (XIQ-SE/XMC Control) and their respective VLAN/I-SID assignment auto-assigned based on return RADIUS attributes ?
  - Auto-sense ports do not need any configuration to work with NAC
  - Enough to globally configure RADIUS server for EAPoL on switch and globally enable eapol
- Or will the Fabric edge access ports be statically configured with desired VLANs ?
  - Auto-sense will allow a degree of automation even in this case; for instance, certain FA client types (e.g., WLAN APs) can be placed on a desired I-SID, and a Data I-SID can be specified for user traffic, but if this needs to be different on different ports, will still require some static config

Fabric Edge without NAC – decision point Auto-Sense or not

- Access ports use auto-sense or not





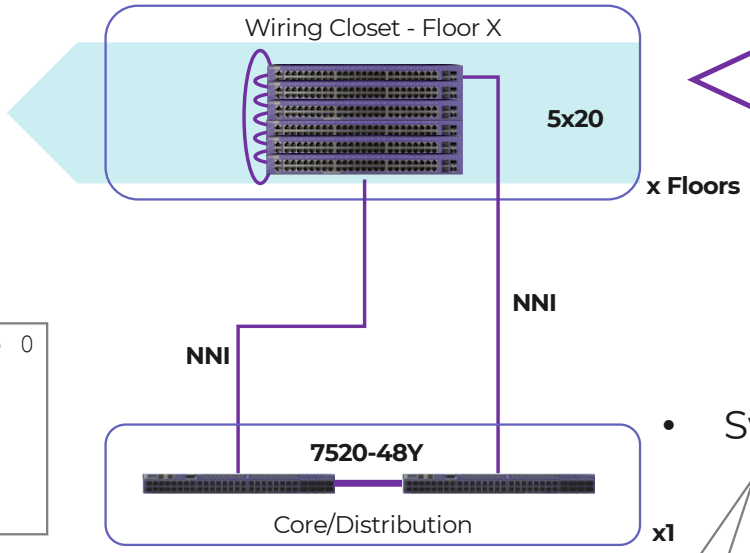

```
interface gigabitEthernet 1/x
   no auto-sense enable
exit
```

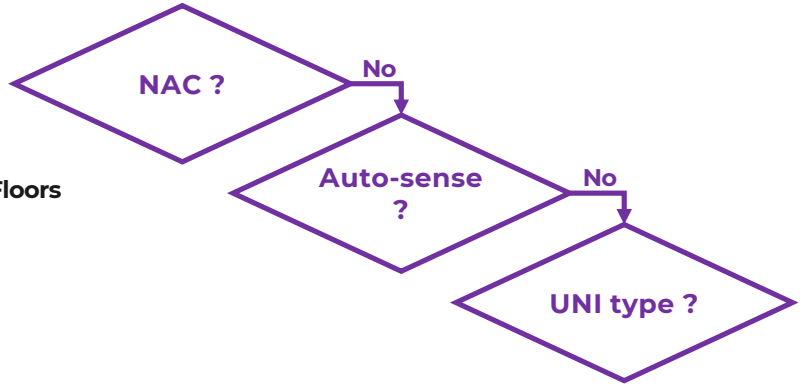
- **Auto-Sense, without NAC**
  - Fabric edge access ports have auto-sense enabled, by default
  - When onboarding the access switch, provide auto-sense global config for:
    - Data I-SID at global and/or at port level
    - Voice I-SID & optional VLAN-id (tagged access if VLAN-id provided)
    - WLAN AP mgmt I-SID
    - Video camera I-SID
    - Open vSwitch (OVS) I-SID
    - FA Proxy mgmt I-SID
  - Auto-sense port state will automatically configure the right I-SIDs based on what is connected to the port

- **No NAC, no auto-sense**
  - All config on access ports is manual and static
  - Choice of CVLAN UNI or Switched-UNI config (next slide)
  - Requires auto-sense to be disabled on access ports

Fabric Edge no NAC & no auto-sense – decision point UNI-type

- Access ports configured as CVLAN-UNI or Switched-UNI






```
vlan create 101 type port-mstprstp 0
vlan i-sid 101 20101
interface gigabitEthernet 1/5
   encapsulation dot1q
exit
vlan members add 101 1/5,1/6
```

- CVLAN UNI
  - Same VLAN syntax as used on ERS platforms
  - Supports Spanning Tree
  - Not available in DVR Leaf mode

- Switched-UNI (Flex-UNI)
  - More powerful and flexible
  - Assign ports directly to I-SIDs
  - Completely does away with VLAN id for untagged bindings
  - Configuration syntax is very different from traditional VLAN config syntax
  - No Spanning Tree support

```
i-sid 20101
   c-vid 101 port 1/5
   untagged-traffic port 1/6
exit
```

What else should I think about?

Some extra things..

- Did you harden your device configs?
  - Enable Enhanced Security mode
    - ✓ Provide role-based access levels
    - ✓ Stronger password requirements
    - ✓ Stronger rules on password length
    - ✓ Stronger rules on password complexity
    - ✓ Stronger rules on password change intervals
  - Did you update firmware?
  - Secure local admin account, just in case..
  - Add your own encryption certificates
  - Disable unencrypted mgmt. (telnet, http, old snmp..)
  - Login banners
  - AAA configuration
  - NTP
  - SSH & SNMPv3
  - Disable extra services
  - List goes on..

What about the cable? - MACsec ENCRYPTION

WHAT IS IT?

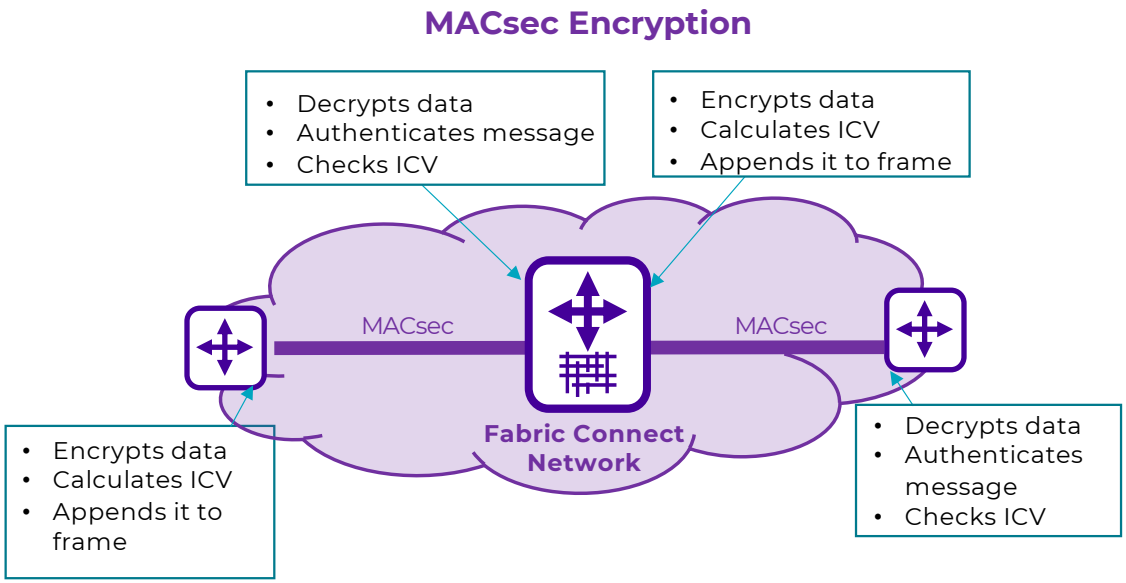
- MACsec is a hop-by-hop security capability which encrypts/ decrypts packets between connected switches or devices.

WHAT IS THE VALUE?

- Provides increased security/ data protection at the Ethernet link layer.

REQUIREMENTS:

- Requires a MACsec feature license to activate
- Supported on select platforms



Networks security begins at the foundation.

Control who and what gets on the network

Provide granular visibility to potential threats

Contain breaches and isolate hackers

Meet compliance and regulatory obligations

Manage and secure IoT

TRAIN YOUR USERS!


ADVANCE
WITH US™