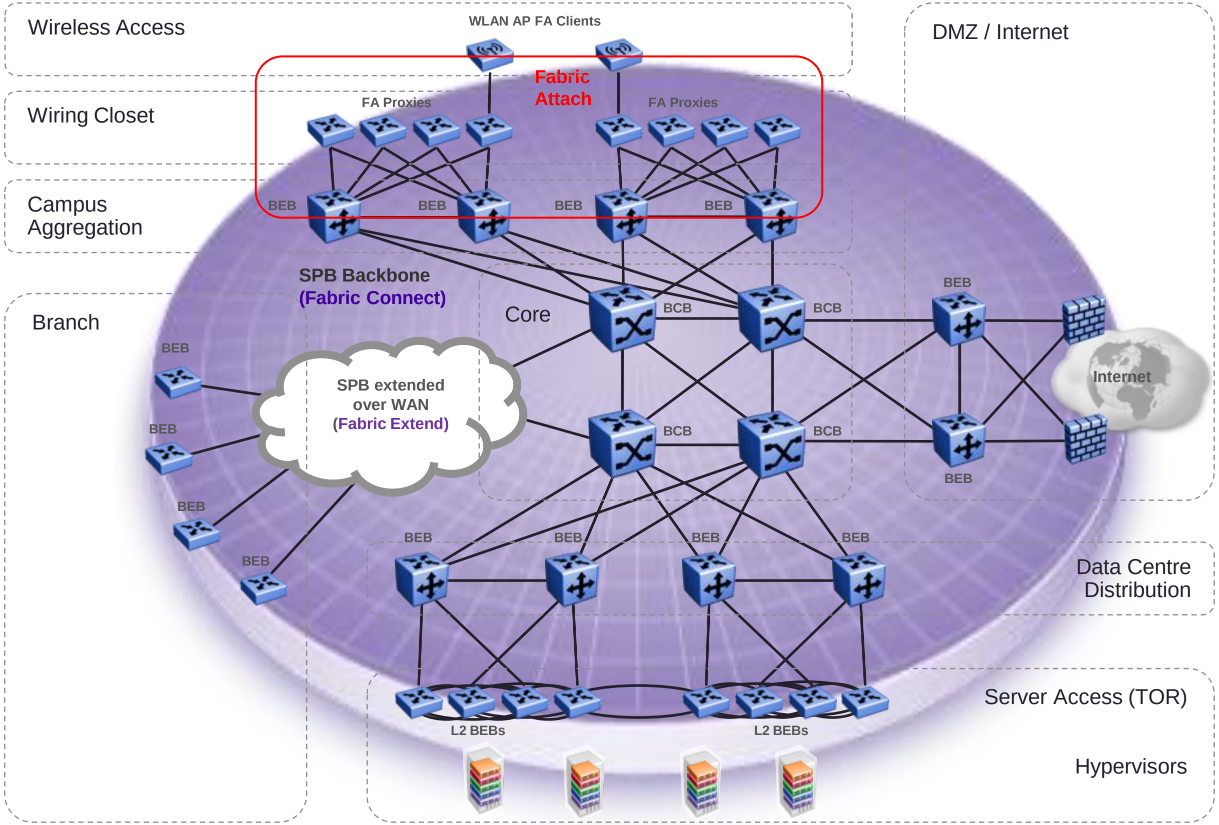
Fabric Attach

Ludovico Stevens / Scott Fincher
January 2021

Extreme™
Customer-Driven Networking

Introducing the Automated Campus

Where does Fabric Attach fit in the Automated Campus Solution?



What is Fabric Attach

- Extreme Fabric Attach allows non-SPB devices to connect to Fabric Connect or legacy networks providing automated configuration.
- It delivers flexibility by automating network service provisioning, attachment and control without complex scripting or programming of legacy protocols.
- Fabric Attach solutions provide huge Opex cost savings in IT adds moves and changes alone.
- The entire network becomes a truly elastic resource where services only exist while users or devices are connected and accessing business applications.
  - Highly flexible; Location of user or device is irrelevant. The same services can be automatically provisioned where-ever the user or device connects to the network.
  - Inherently secure; No switch port configuration exists if nothing is attached to the network, & no residual configuration remains when a user or device disconnects.

What is Fabric Attach cont.

- Fabric Attach is about connecting users and devices to the right applications, and automating that function over the entire network.
  - Fabric Attach provides network service provisioning & configuration of VLANs and SPB Virtual Services for users, devices & VM's attaching to the network.
- Fabric Attach is a draft IEEE standard - Auto Attach (802.1Qcj).
- There are two Fabric Attach deployment options:

  1/ Fabric Attach with an SPB Fabric Connect Core
  - End-to-end automated network configuration and service provisioning.

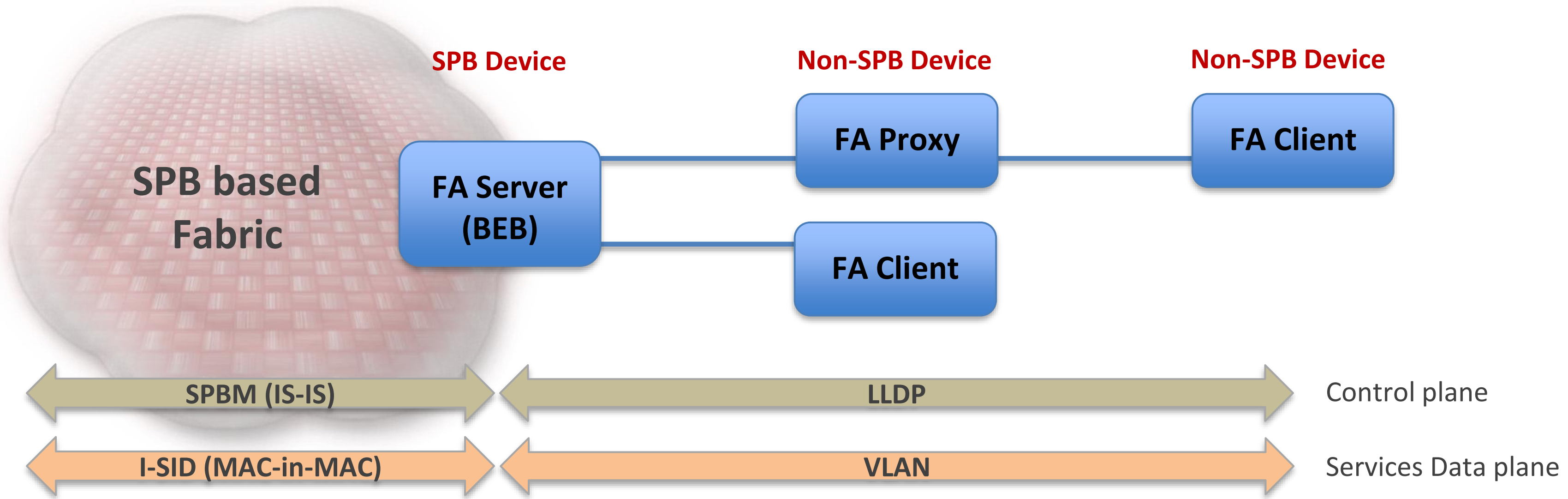
  2/ Fabric Attach with a Legacy Core
  - Network automation at the access layer only, enabling a gradual migration to an Extreme SPB based Fabric Connect network core.

Fabric Attach – General Notes

- Fabric Attach **only configures VLAN to Layer 2 VSN (I-SID) mappings** for an SPB Fabric.
  - SPB L3 VSNs and Multicast Virtualization for L2/L3 must be pre-configured manually at the BEB running FA Server if FA is used to connect access layer devices to services (which will be to an existing VLAN attached to a VRF for L3 VSNs).
- FA Proxy switches **only support C-VLAN UNIs.** (FA does not support Switched UNI or Transparent UNI)
- FA can signal at **most 94 VLAN/I-SIDs**, so an FA Proxy switch will never be able to support more than 94 FA VLANs
  - But additional VLANs can be always configured statically (requires VOSS 8.1.1.0 or later which enabled flex-uni bindings on fa ports)
- FA Server switches use Switched UNI for attachment of downstream VLANs to I-SIDs on the BEB node.
  - The **FA Server downstream link to an FA Proxy will always be a Q-Tagged link**.
  - VSP switches DO NOT create a local VLAN associated with the FA VLAN.
- On VSP FA Server: the FA service is by default globally enabled but disabled on the switch ports.
- On ERS FA Proxy: the FA service is by default globally enabled and port enabled
- On XOS FA Proxy: the FA service is by default globally enabled (there is no port level enable/disable of FA)
- FA Standalone Proxy mode is DISABLED by default and needs activating
  - On ERS explicitly set the mode and define the uplink ports; on XOS simply set the uplink ports
- FA services can be manually or automatically provisioned.
  - **Manual** = **CLI or Web Admin** configuration of VLAN/I-SID mapping on the FA Proxy switch.
  - **Automatic** = **Policy-driven** based on authentication of end user (EAP) or device (Non-EAP) by Extreme Control and Identity Engines where the server sends VLAN/I-SID mapping based on policy.

Fabric Attach - Element Model

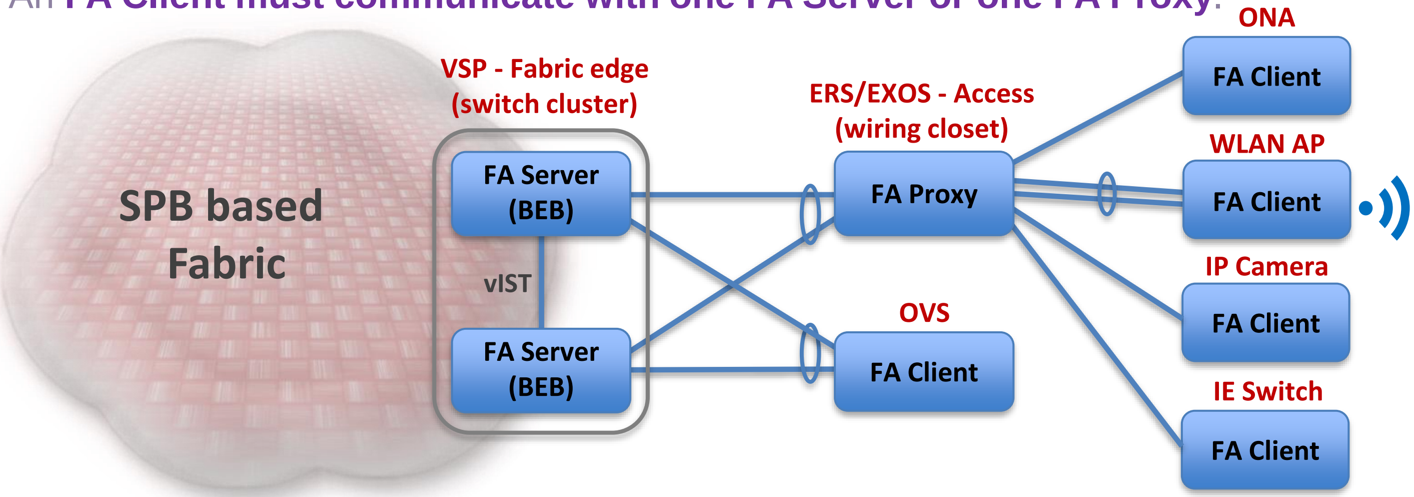
- **Fabric Attach Elements are FA agent roles in devices**
  - Below are all the **FA Elements required to create a Fabric Attach solution** with the supported Element interconnections (tiers).
  - Use this FA architectural model when designing FA solutions end to end with an SPB Fabric Core.



The two signaling planes are shown to illustrate which parts of the network are controlled by which protocols and what the "services" are delivered on. IE: Non-SPB/fabric devices only support VLANs for services.

Fabric Attach – Element connection rules

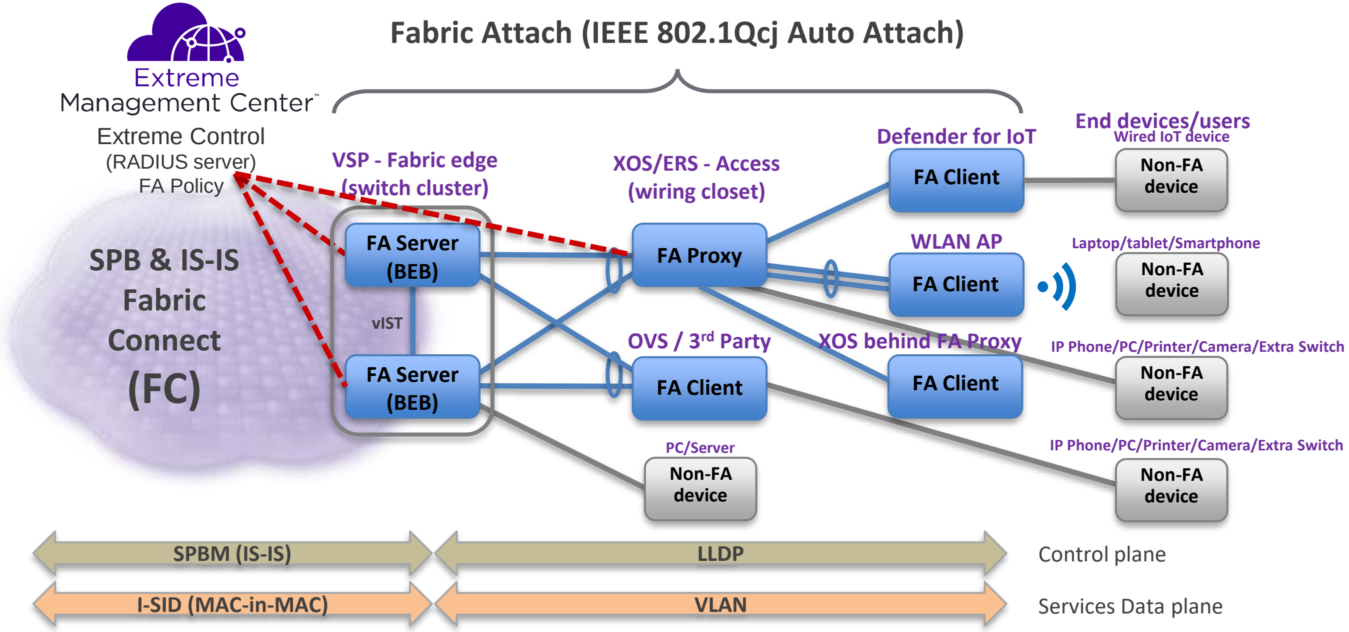
- **Supported FA Element inter-connections**
  - Basic premise: each **FA element interconnection must be a single logical link**.
  - **FA Servers** must be a single entity and **can support multiple FA Proxy or FA Client devices** (SMLT/vIST cluster is supported on VSP/VOSS).
  - An **FA Proxy must communicate with one FA Server**. (Switch Cluster seen as one FA Server to downstream FA Proxy switches or FA Client devices. Static LAG or LACP supported. FA Proxy switch chaining is not supported.
  - An **FA Client must communicate with one FA Server or one FA Proxy**.



MLT LAG or LACP links between any FA element is supported, as long as each interconnection is a single logical link.
Switch clustered FA Servers are only supported on VSP platforms.

Fabric Attach solution – Elements

- FA Proxy & FA Clients are only concerned about attaching to the Fabric Service (I-SID)
  - Fabric Attach attaches users to L2VSN I-SIDs only
- They have no need for ISIS to calculate a shortest path, as they all have a single logical uplink into the Fabric (stub connected)



Extreme Management Center™

Extreme Control (RADIUS server) FA Policy

Fabric Attach (IEEE 802.1Qcj Auto Attach)

SPB & IS-IS Fabric Connect (FC)

VSP - Fabric edge (switch cluster)

FA Server (BEB)

vIST

FA Server (BEB)

XOS/ERS - Access (wiring closet)

FA Proxy

OVS / 3rd Party

FA Client

PC/Server

Non-FA device

Defender for IoT

FA Client

WLAN AP

FA Client

XOS behind FA Proxy

FA Client

End devices/users

Wired IoT device

Non-FA device

Laptop/tablet/Smartphone

Non-FA device

IP Phone/PC/Printer/Camera/Extra Switch

Non-FA device

IP Phone/PC/Printer/Camera/Extra Switch

Non-FA device

SPBM (IS-IS) | LLDP | Control plane

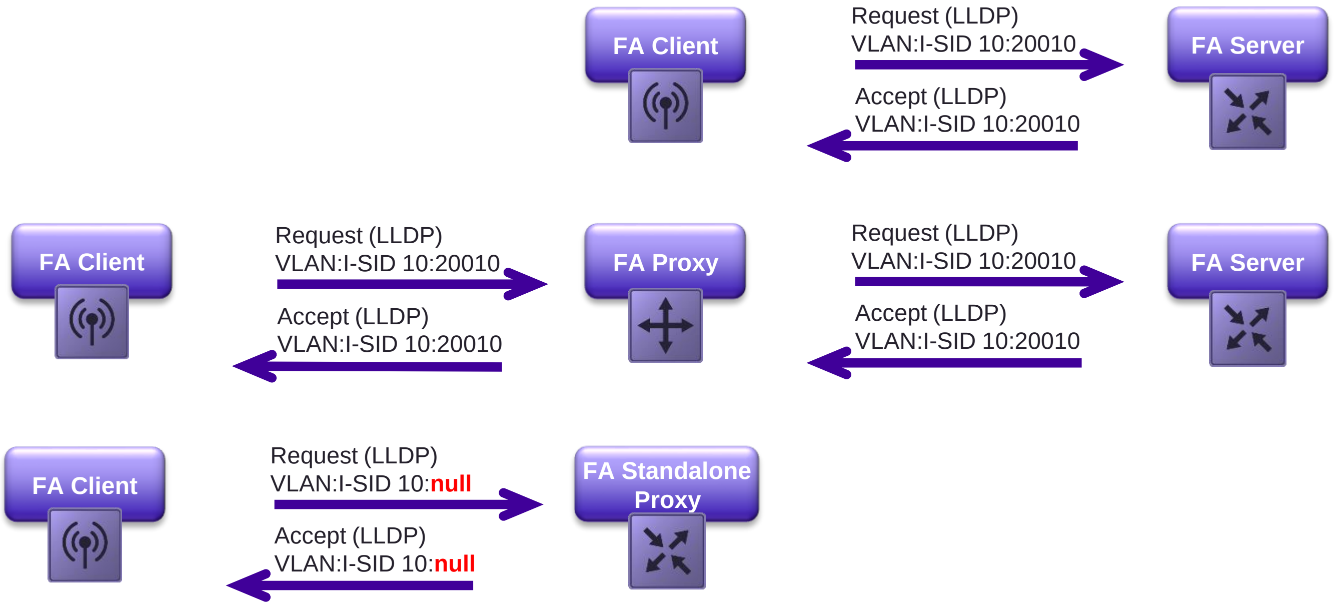
I-SID (MAC-in-MAC) | VLAN | Services Data plane

ROLE	VSP9000	VSP8600	VSP8400 VSP8200 VSP7400 VSP7200 VSP4900	5520 5420 (VOSS)	VSP4450 VSP4850	XA1400	ERS5900 ERS4900	ERS4800	ERS3600 ERS3500	XOS	ISW	Extreme Wireless Identify	Extreme Wing	Extreme Wireless AeroHive	Defender IoT	3rd Party (OVS)
FA Server standalone	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	n/a	n/a	n/a	n/a	n/a
FA Server with vIST	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	n/a	n/a	n/a	n/a	n/a
FA Proxy	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	n/a	n/a	n/a	n/a	n/a
FA Standalone Proxy	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	n/a	n/a	n/a	n/a	n/a
FA Client	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	✓	✓	✓	✓	✗	✓	✓

Extreme Fabric Attach Elements

- **FA Server**: An SPB capable switch at the Fabric Connect edge that can create fabric services requested by non-SPB devices.
- **FA Proxy**: A non-SPB switch (wiring closet) with attached users & end devices or network attached devices with an FA Client. An FA Proxy creates VLAN services & passes requests to the FA Server.
- **FA Client:** A non-SPB network attached device connected to an FA Proxy or FA Server. FA Clients can request VLAN & Fabric services. An XOS switch connected behind an FA Proxy will automatically drop down to FA Client mode.
- **FA Standalone Proxy:** A non-SPB switch (wiring closet) with directly attached users & end devices, plus network attached devices with an FA Client. FA Standalone Proxies are used with legacy core networks.
- **FA Policy Server:** Extreme Control server, when used in FA solutions, fully automates the provisioning of services based on centralized authorization / authentication policy of an end-user or device.

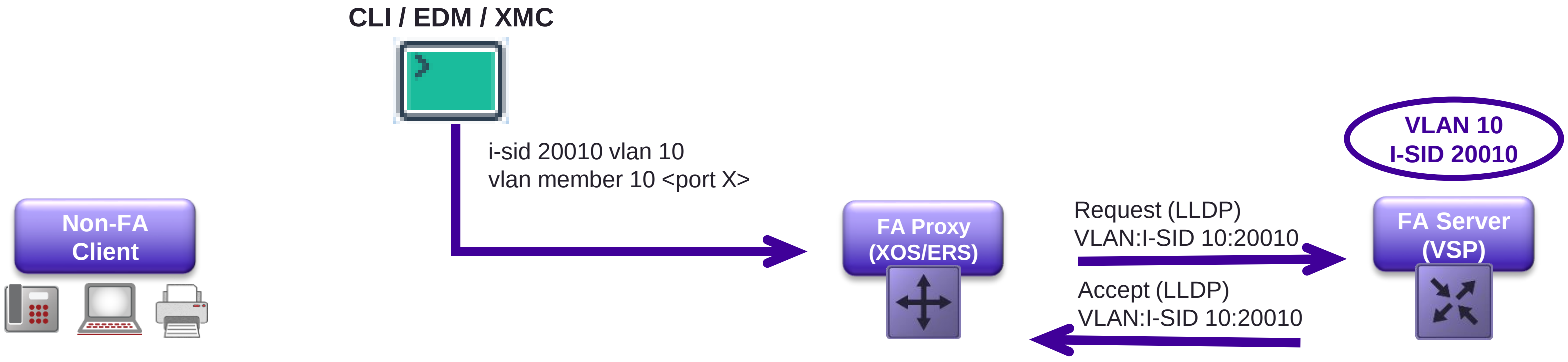
Fabric Attach possible deployment models



- FA Standalone Proxy is a mode where the FA Proxy switch operates without the presence of an FA Server. This mode is only useful in situations where the wiring closet access switch is deployed in a non-fabric architecture or in cases where the distribution layer is not capable of providing the FA Server functionality
  - ISW does not accept 0 I-SIDs so will not work with ERS Standalone-Proxy which requires 0 I-SID
  - Will work with an XOS Standalone-Proxy which simply ignores the I-SID value requested

Manual FA VLAN/I-SID Service signalling from FA Proxy/Client

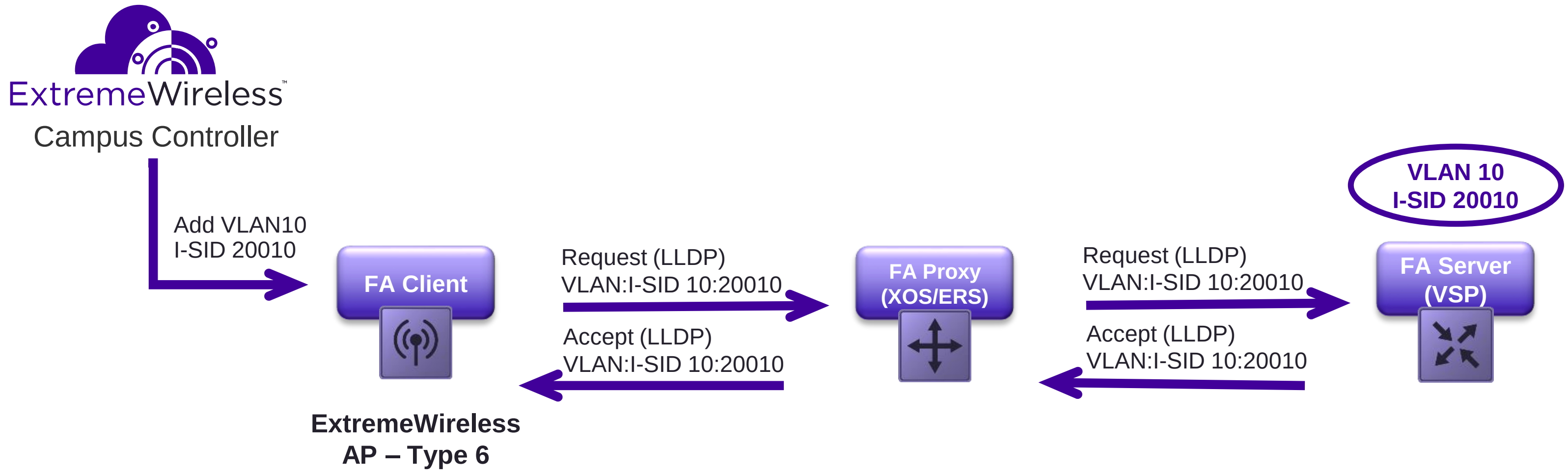
via configuration



- FA Proxy (acting as FA Client) can be configured for VLAN & I-SID (just as if it was an SPB BEB)
  - This will then trigger FA Signalling for the requested binding back to the FA Server
  - It takes 2-3 seconds for the FA signalling to complete
- Then the VLAN can be configured on any access port of the FA Proxy
  - This step can only happen after FA signalling has completed and the request accepted
- NOTE: On ERS, if scripting the CLI commands care needs to be taken to only execute the 2nd command once the FA signalling for the 1st command has succeeded
- NOTE: On XOS the CLI commands would be:
  - `create vlan 10`
  - `configure vlan 10 add isid 20010`

FA Proxy(Client) switch	ERS5900	ERS4900	ERS4800	ERS3600	ERS3500	XOS	ISW
Manual I-SID config	✓	✓	✓	✓	✓	✓	✓

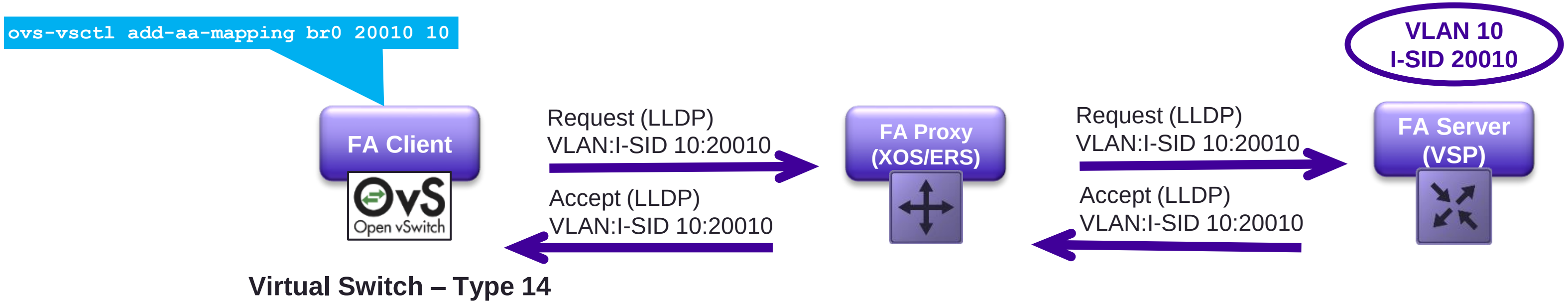
FA VLAN/I-SID Service signalling from WLAN AP FA Client



- VLANs required on the AP (for SSID mapping) are automatically provisioned by the Wireless Management
- FA Client AP then signals these back to the FA Server to gain access to them
- Supported on ExtremeWireless and ExtremeWireless Wing
- This function can only be supported by an FA Proxy (hence not the ISW)

FA Proxy switch	ERS5900	ERS4900	ERS4800	ERS3600	ERS3500	XOS	ISW
Proxy VLAN/I-SID signalling	✓	✓	✓	✓	✓	✓	✗

FA VLAN/I-SID Service signalling from generic FA Client

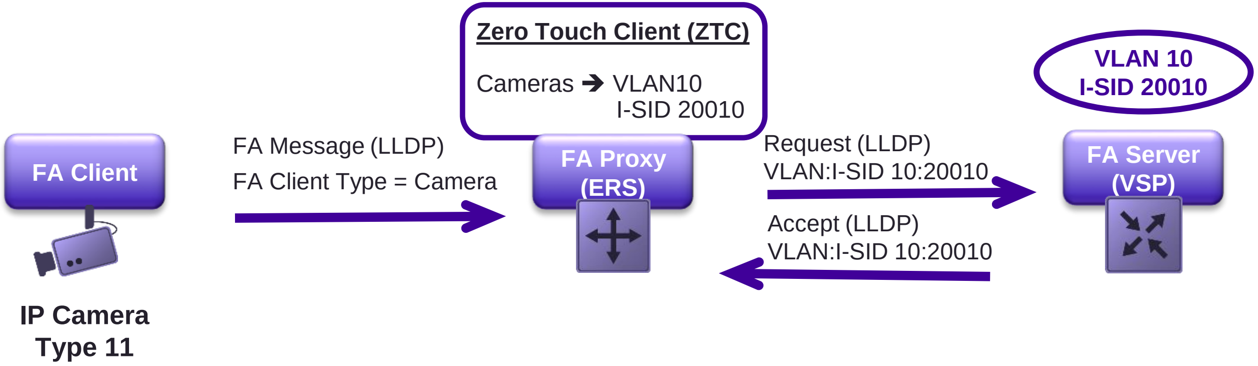


```
ovs-vsctl add-aa-mapping br0 20010 10
```

- Open vSwitch (OVS) supports Auto-Attach since release 2.4
- OVS FA Client needs to obtain information about what Service to Request via independent configuration
- OVS Auto Attach Client based device has to be manually configured to request Services
  - OVS can be deployed in KVM and Microsoft HyperV

FA Proxy switch	ERS5900	ERS4900	ERS4800	ERS3600	ERS3500	XOS	ISW
Proxy VLAN/I-SID signalling	✓	✓	✓	✓	✓	✓	✗

Fabric Attach Zero-Touch-Client



Zero Touch Client (ZTC)

Cameras ➔ VLAN10
I-SID 20010

VLAN 10
I-SID 20010

FA Client

FA Message (LLDP)
FA Client Type = Camera

FA Proxy (ERS)

Request (LLDP)
VLAN:I-SID 10:20010

Accept (LLDP)
VLAN:I-SID 10:20010

FA Server (VSP)

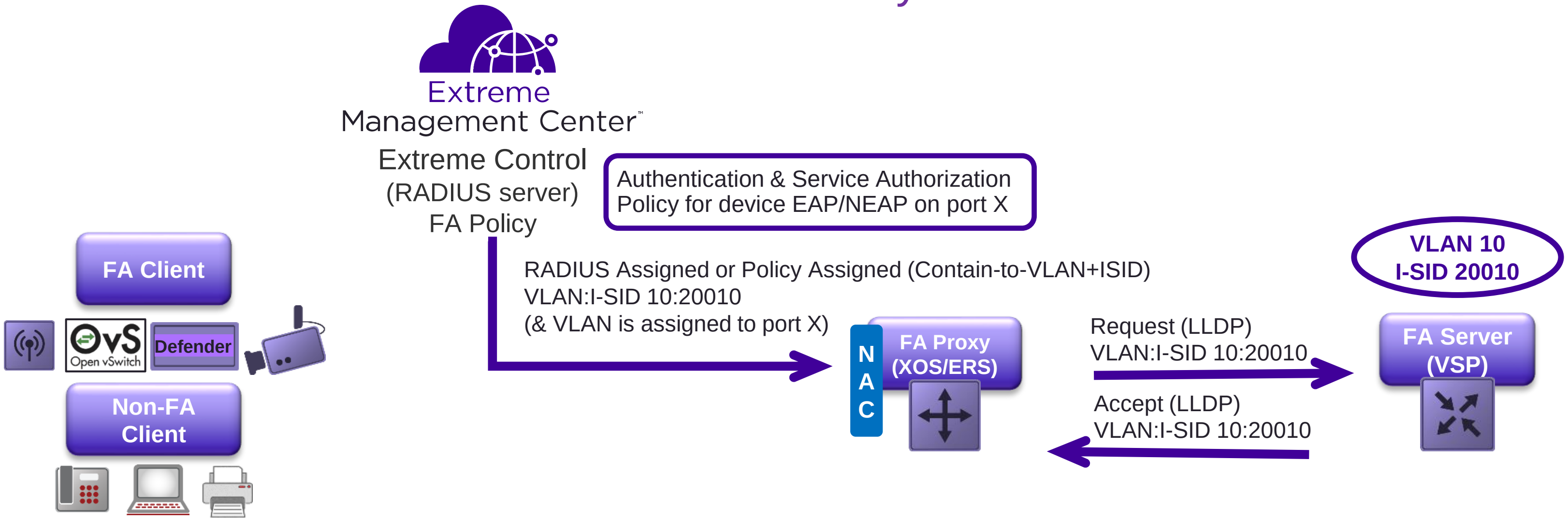
IP Camera
Type 11

- FA access switch is pre-configured with FA ZTC policies
- If an FA client is detected it is assigned to the FA VLAN/I-SID
- Useful on non-VLAN aware devices which simply need an untagged connection
- Supported on XOS as of 31.3

FA Proxy switch	VOSS/VSP8600	XA1400	ERS5900	ERS4900	ERS4800	ERS3600	ERS3500	XOS	ISW
Zero-Touch-Client (ZTC)	✓	✗	✓	✓	✓	✓	✗	✓	✗

FA VLAN/I-SID Service signalling from FA Proxy

via RADIUS outbound attributes –or– XOS Policy enforcement



Extreme Management Center™

Extreme Control
(RADIUS server)
FA Policy

Authentication & Service Authorization
Policy for device EAP/NEAP on port X

RADIUS Assigned or Policy Assigned (Contain-to-VLAN+ISID)
VLAN:I-SID 10:20010
(& VLAN is assigned to port X)

VLAN 10
I-SID 20010

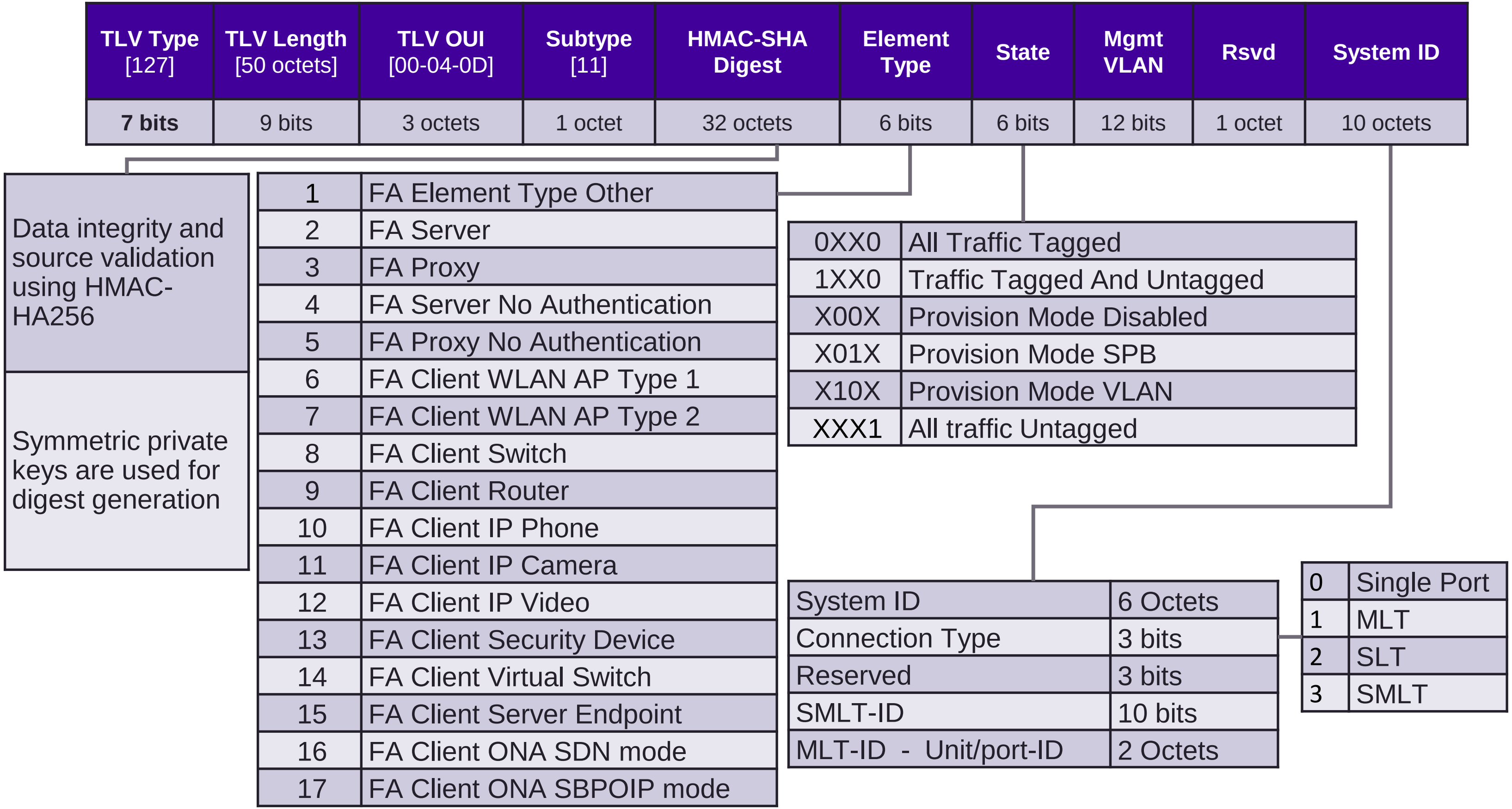
Request (LLDP)
VLAN:I-SID 10:20010

Accept (LLDP)
VLAN:I-SID 10:20010

- FA Proxy can configure EAP/NEAP enabled ports via RADIUS assigned bindings
  - This will then trigger FA Signalling for the requested binding back to the FA Server
  - And the VLAN is then assigned on the EAP Supplicant port

FA Proxy(Client) switch	ERS5900	ERS4900	ERS4800	ERS3600	ERS3500	XOS	ISW
802.1X EAP (netlogin)	✓	✓	✓	✓	✓	✓	✓
MAC-based auth (NEAP)	✓	✓	✓	✓	✓	✓	✓

Fabric Attach LLDP element signalling TLV



TLV Type [127]	TLV Length [50 octets]	TLV OUI [00-04-0D]	Subtype [11]	HMAC-SHA Digest	Element Type	State	Mgmt VLAN	Rsvd	System ID
7 bits	9 bits	3 octets	1 octet	32 octets	6 bits	6 bits	12 bits	1 octet	10 octets

Data integrity and source validation using HMAC-HA256

Symmetric private keys are used for digest generation

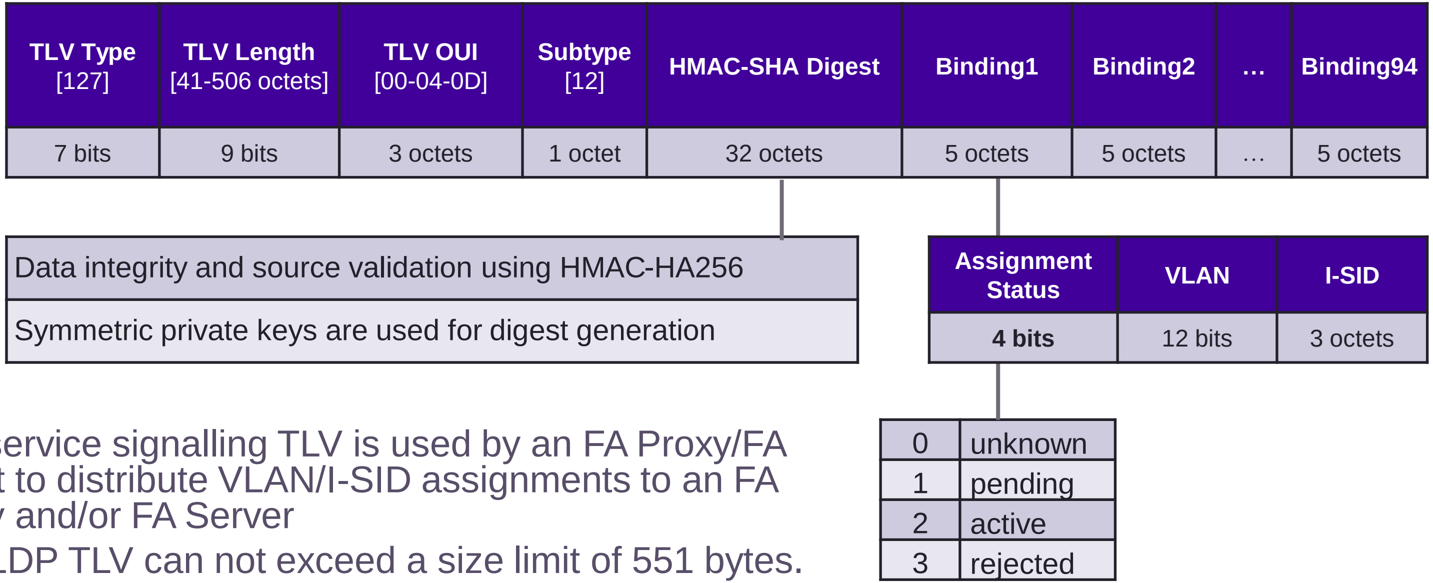
1	FA Element Type Other
2	FA Server
3	FA Proxy
4	FA Server No Authentication
5	FA Proxy No Authentication
6	FA Client WLAN AP Type 1
7	FA Client WLAN AP Type 2
8	FA Client Switch
9	FA Client Router
10	FA Client IP Phone
11	FA Client IP Camera
12	FA Client IP Video
13	FA Client Security Device
14	FA Client Virtual Switch
15	FA Client Server Endpoint
16	FA Client ONA SDN mode
17	FA Client ONA SBPOIP mode

0XX0	All Traffic Tagged
1XX0	Traffic Tagged And Untagged
X00X	Provision Mode Disabled
X01X	Provision Mode SPB
X10X	Provision Mode VLAN
XXX1	All traffic Untagged

System ID	6 Octets
Connection Type	3 bits
Reserved	3 bits
SMLT-ID	10 bits
MLT-ID - Unit/port-ID	2 Octets

0	Single Port
1	MLT
2	SLT
3	SMLT

Fabric Attach LLDP service signalling TLV



TLV Type [127]	TLV Length [41-506 octets]	TLV OUI [00-04-0D]	Subtype [12]	HMAC-SHA Digest	Binding1	Binding2	…	Binding94
7 bits	9 bits	3 octets	1 octet	32 octets	5 octets	5 octets	…	5 octets

Data integrity and source validation using HMAC-HA256
Symmetric private keys are used for digest generation

Assignment Status	VLAN	I-SID
4 bits	12 bits	3 octets

0	unknown
1	pending
2	active
3	rejected

- The service signalling TLV is used by an FA Proxy/FA Client to distribute VLAN/I-SID assignments to an FA Proxy and/or FA Server
- An LLDP TLV can not exceed a size limit of 551 bytes.
  - Maximum 94 VLAN/I-SID assignments in an LLDPDU
  - This limit determines the maximum number of VLAN/I-SIDs that an FA Proxy device can request from its FA Server

Fabric Attach support

- FC = Fabric Connect (SPBM)
- FA = Fabric Attach
- TOR = Top of Rack
- SMLT = Split Multi-Link Trunk (MC-LAG)

Product	Distribution Layer			Wiring Closet		End Device
	FA Server (SPBM mode)	FA Server (VLAN mode)	FA Server (VXLAN mode)	FA Proxy	FA Proxy Standalone	FA Client
VSP8600 (6.3)	✓ (with SMLT support)	✗	✗	n/a	n/a	n/a
VOSS (8.0): 5520, 5420, VSP8x00,VSP7x00,VSP4x00	✓ (with SMLT support)	✗	✗	n/a	n/a	n/a
VOSS: XA1400	✗	✗	✗	n/a	n/a	n/a
Summit XOS (30.1)	✗	✗	✓	✓	✓	✓
ERS4900/5900 (7.6)	✓	✓	✗	✓	✓	n/a
ERS4800 (5.12)	✓	✓	✗	✓	✓	n/a
ERS3600 (6.2)	✗	✗	✗	✓	✓	n/a
ERS3500 (5.3)	✗	✗	✗	✓	✓	n/a
S & K Series	✗	✗	✗	✗	✗	n/a
ISW	✗	✗	✗	✗	✗	✓
Extreme Wireless (10.41)	n/a	n/a	n/a	n/a	n/a	✓
Extreme WING (5.9.2)	n/a	n/a	n/a	n/a	n/a	✓
WLAN9100 (8.4)	n/a	n/a	n/a	n/a	n/a	✓
Defender for IoT	n/a	n/a	n/a	n/a	n/a	✓

- Ideal FA deployment model
  - Distribution Layer = SPBM FA Server with SMLT support
  - Wiring Closet Stackable switch = FA Proxy
  - WLAN AP / Defender for IoT = FA Client
- IP Fabric (EVPN/VXLAN) Deployment model (not covered)

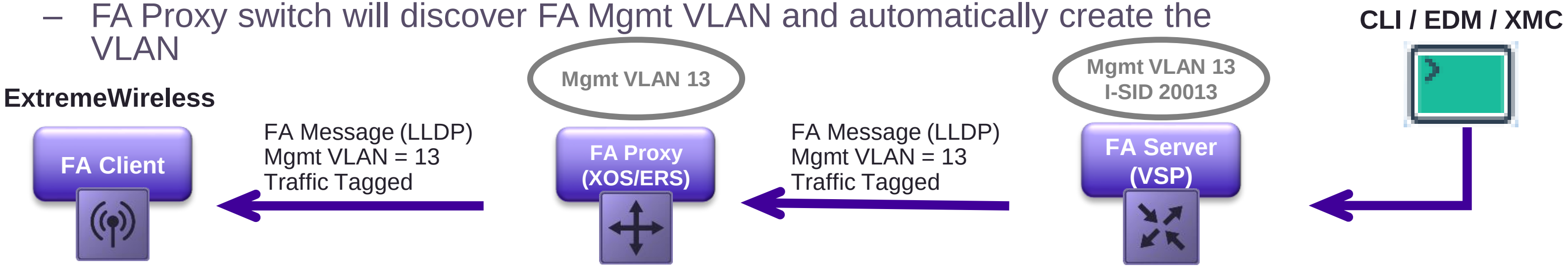
- Deployment model when core does not support Fabric Connect
  - When distribution layer not SPB capable
  - Or when distribution layer not FA Server capable
- FA Server in VLAN mode
  - Historical and no longer promoted as part of Fabric Attach solution

FA mgmt VLAN and Zero-Touch

FA Auto Attach / Zero Touch (ZT) – Mgmt VLAN

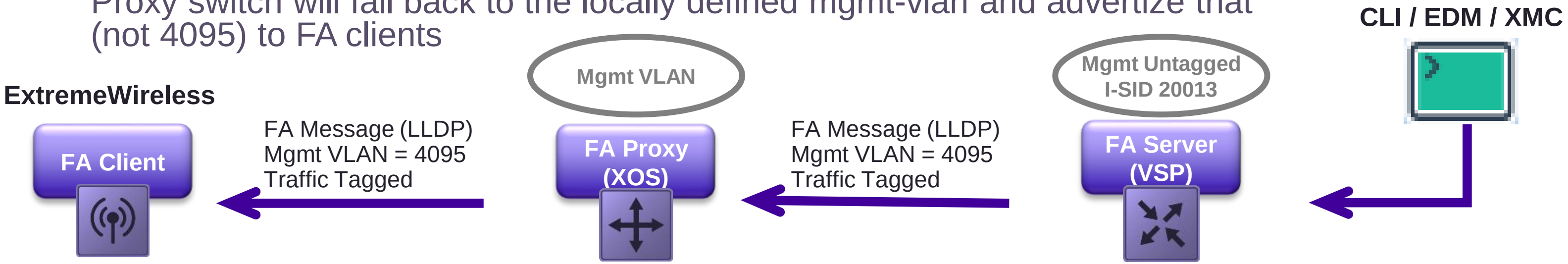
- Onboarding of FA Clients and FA Proxies
  - FA Proxy switch will discover FA Mgmt VLAN and automatically create the VLAN

```
interface X
  fa
  fa management i-sid 20013 c-vid 13
  fa enable
exit
```



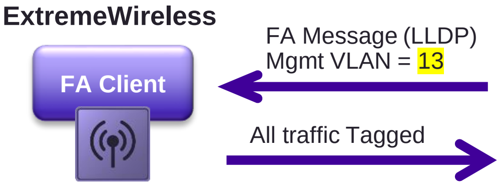
- If no c-vid was specified on VOSS FA Server, then Mgmt VLAN is untagged and advertised as 4095
  - NOTE: This mode can only work with an XOS FA Proxy switch. An ERS FA Proxy switch will fall back to the locally defined mgmt-vlan and advertize that (not 4095) to FA clients

```
interface X
  fa
  fa management i-sid 20013
  fa enable
exit
```

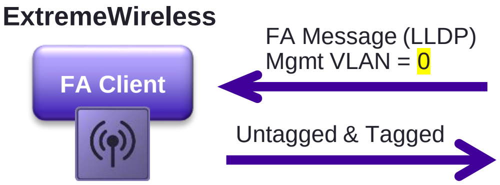


ExtremeWireless FA onboarding

- If AP sees a FA mgmt VLAN advertised
  - AP will do DHCP tagged on that VLAN
  - All mgmt traffic to/from the AP will be tagged on that VLAN
  - AP will signal its desire to send all traffic tagged
    - An ERS FA Proxy/FA Server will then automatically adapt its port to TagAll
  - The FA Mgmt VLAN needs to get plumbed, as tagged, on the ethernet port
    - NAC/Policy can do that
    - If no NAC/Policy:
      - An XOS FA Proxy will always add the FA Mgmt VLAN as tagged member
      - An ERS FA Proxy, need to activate auto-mgmt-vlan-fa-client (or auto-pvid-mode-fa-client) FA zero-touch-option



- If AP sees no FA mgmt VLAN advertised
  - AP will do DHCP untagged
    - What VLAN will be used will now depend on what untagged VLAN is defined on the ERS or XOS switch port
  - All mgmt traffic to/from the AP will be untagged
  - AP will signal its desire to send both untagged and traffic tagged
    - An ERS FA Proxy/FA Server will then automatically adapt its port to UntagPvidOnly
  - The desired AP Mgmt VLAN (which is not the FA Mgmt VLAN) needs to get plumbed, as untagged, on the ethernet port
    - NAC/Policy can do that
    - If no NAC/Policy:
      - An XOS FA Proxy, use Python script (fa-ztc.py) or use UPM
      - An ERS FA Proxy, need to configure ZTC to onboard AP onto desired VLAN:ISID

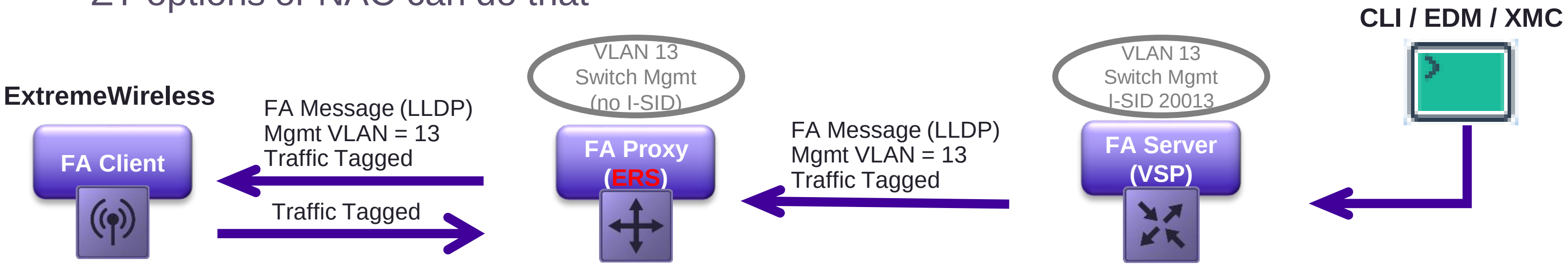


AP FA Client mgmt on FA-mgmt VLAN

ERS5900	ERS4900	ERS4800	ERS3600	ERS3500
✓	✓	✓	✓	✗

- ERS FA Proxy
  - AP mgmt VLAN will then need to be placed as tagged on the AP port
  - ZT-options or NAC can do that

```
interface X
  fa
  fa management i-sid 20013 c-vid 13
  fa enable
exit
```



CLI / EDM / XMC

ExtremeWireless

FA Client

FA Message (LLDP)
Mgmt VLAN = 13
Traffic Tagged

Traffic Tagged

VLAN 13
Switch Mgmt
(no I-SID)

FA Proxy
(ERS)

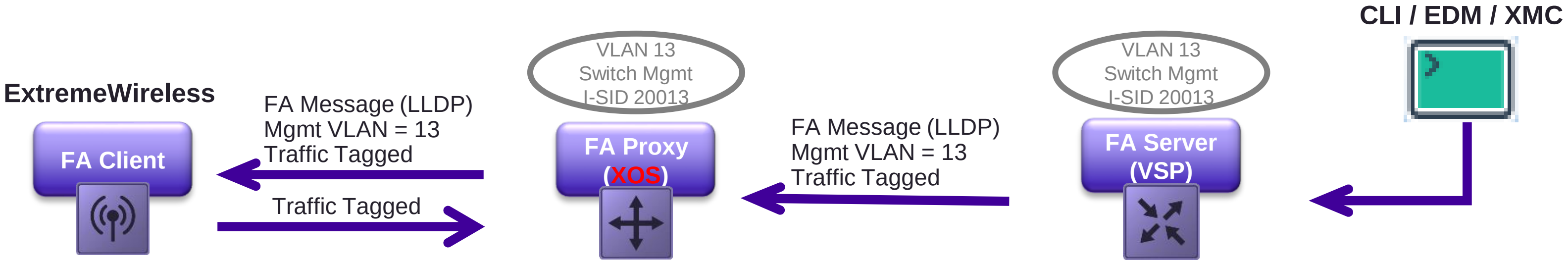
FA Message (LLDP)
Mgmt VLAN = 13
Traffic Tagged

VLAN 13
Switch Mgmt
I-SID 20013

FA Server
(VSP)

- XOS FA Proxy
  - AP mgmt VLAN will then need to be placed as tagged on the AP port
  - Without NAC, XOS does this automatically; else NAC can do it

```
interface X
  fa
  fa management i-sid 20013 c-vid 13
  fa enable
exit
```



CLI / EDM / XMC

ExtremeWireless

FA Client

FA Message (LLDP)
Mgmt VLAN = 13
Traffic Tagged

Traffic Tagged

VLAN 13
Switch Mgmt
I-SID 20013

FA Proxy
(XOS)

FA Message (LLDP)
Mgmt VLAN = 13
Traffic Tagged

VLAN 13
Switch Mgmt
I-SID 20013

FA Server
(VSP)

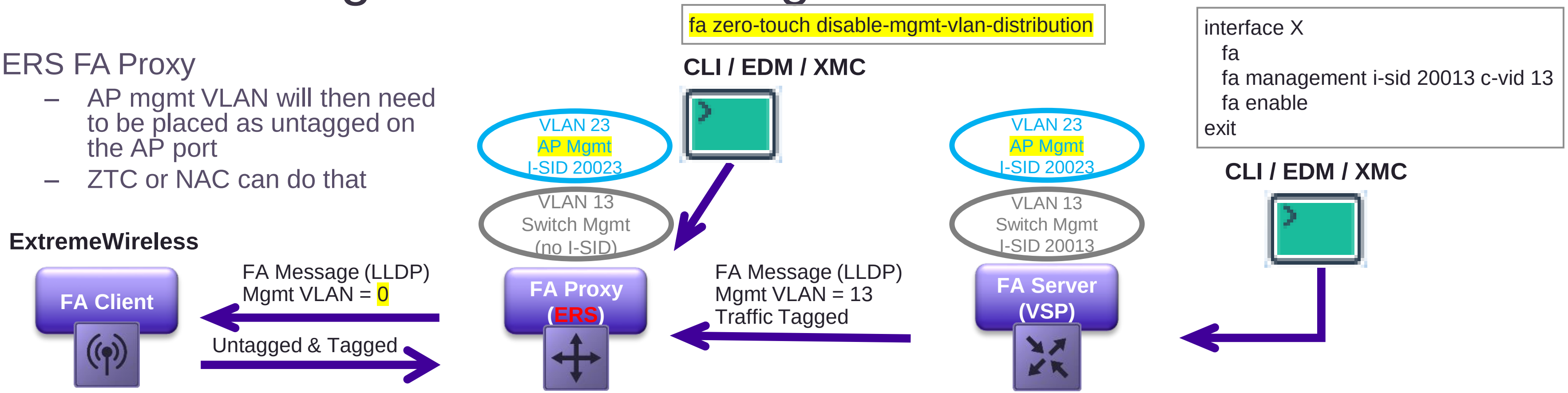
AP FA Client mgmt on non-FA-mgmt VLAN

ERS5900	ERS4900	ERS4800	ERS3600	ERS3500
✓	✓	✓	✓	✗

- ERS FA Proxy
  - AP mgmt VLAN will then need to be placed as untagged on the AP port
  - ZTC or NAC can do that

```
fa zero-touch disable-mgmt-vlan-distribution
```

```
interface X
  fa
  fa management i-sid 20013 c-vid 13
  fa enable
exit
```

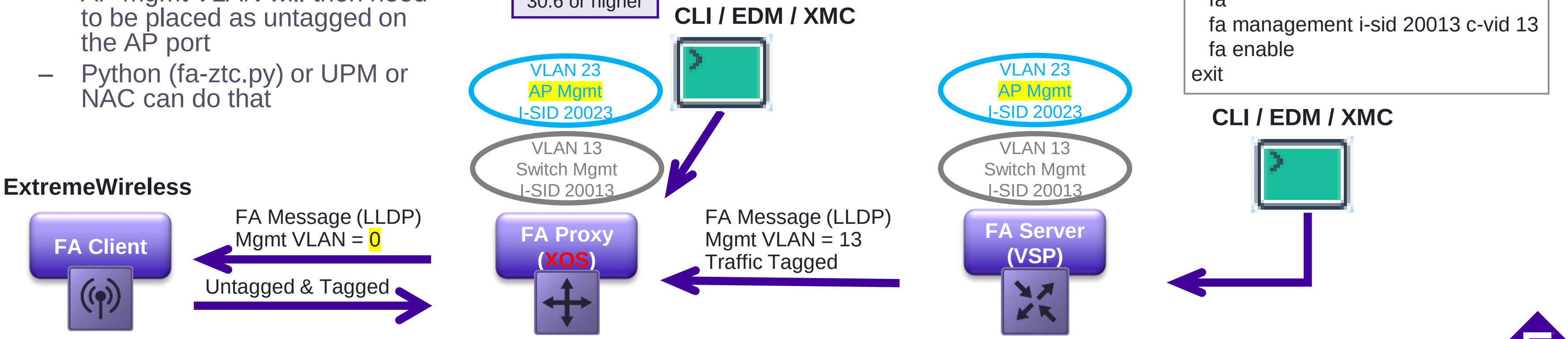


- XOS FA Proxy
  - AP mgmt VLAN will then need to be placed as untagged on the AP port
  - Python (fa-ztc.py) or UPM or NAC can do that

XOS
30.6 or higher

```
configure fabric attach management-vlan forward off
```

```
interface X
  fa
  fa management i-sid 20013 c-vid 13
  fa enable
exit
```



FA manual config to perform on FA Proxy switch

AP FA Client mgmt on FA-mgmt VLAN	With NAC	ERS	`fa zero-touch-option auto-port-mode-fa-client client-type 6`
			`fa zero-touch-option auto-trusted-mode-fa-client client-type 6`

		XOS	`<nothing>`

	Without NAC	ERS	`fa zero-touch-options auto-mgmt-vlan-fa-client client-type 6`
			`fa zero-touch-option auto-trusted-mode-fa-client client-type 6`

		XOS	`<nothing>`

AP FA Client mgmt on non-FA-mgmt VLAN	With NAC	ERS	`fa zero-touch disable-mgmt-vlan-distribution`
			`fa zero-touch-option auto-port-mode-fa-client client-type 6`
			`fa zero-touch-option auto-trusted-mode-fa-client client-type 6`

		XOS	`configure fabric attach management-vlan forward off`

	Without NAC	ERS	`fa zero-touch disable-mgmt-vlan-distribution`
			`fa zero-touch-option auto-trusted-mode-fa-client client-type 6`
			`fa zero-touch-options auto-client-attach client-type 6`
			`fa zero-touch-client standard wap-type1 vlan <vlan-id> i-sid <i-sid>`

		XOS	`configure fabric attach management-vlan forward off`
			`configure fabric attach zero-touch-client wa-type1 vlan <vlan-id> isid <i-sid> enable`

ERS FA zero-touch-options modes (notable ones)

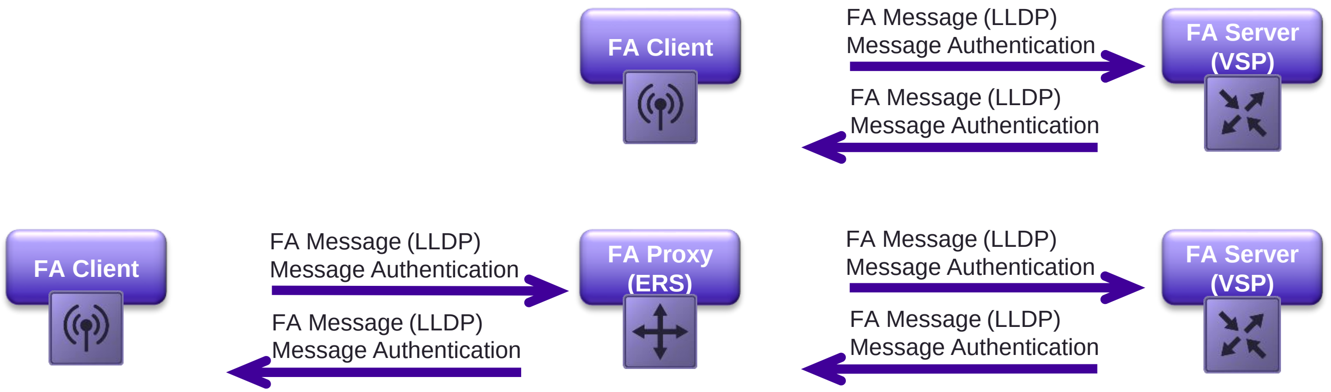
- **auto-port-mode-fa-client**: When this option is activated for certain FA Client types, whenever an FA client of that type is discovered on an access port, the access port is automatically pre-configured for EAP/NEAP in mode Multiple-Hosts-Single-Authentication (MHSA). The FA Client will thus need to authenticate against a RADIUS server using either EAPoL or RADIUS MAC-based authentication (NEAP).
- **auto-pvid-mode-fa-client**: When this option is activated for certain FA Client types, whenever an FA client of that type is discovered on an access port, the access port will be automatically assigned to the FA management VLAN. The port PVID is also set to the FA management VLAN ID. This is required in case the FA Client requested, via the FA Element TLV, both tagging and untagged traffic which would result in the FA access port being automatically configured as untagPvidOnly.
- **auto-mgmt-vlan-fa-client**: This option is almost identical to the auto-pvid-mode-fa-client option above, in that the access port will be automatically assigned to the FA management VLAN, but with the exception that the PVID on the port is not changed.
- **auto-trusted-mode-fa-client**: When this option is activated for certain FA Client types, whenever an FA client of that type is discovered on an access port, the access port will be automatically made QoS trusted.

Connecting Wireless FA Clients with NAC

Performing NAC on AP FA client ports

- NAC (dot1x and MAC netlogin) are enabled on all wiring closet access switch ports
- If an ExtremeWireless FA client is connected to a port, all of the following need to happen
  1. AP determines what mgmt VLAN to use
     - Tagged, if it sees FA mgmt VLAN announced
     - Untagged if it does not see any FA mgmt announced
  2. AP is MAC authenticated on XMC NAC
  3. AP is authorized and switch access port is opened
  4. Switch access port must be opened in MHSA / AP-aware mode
     - MHSA = Multiple Host Single Authentication
     - On ERS, this has to change before authentication (applied to port config using FA zero-touch-options)
     - On XOS, this can be done after authentication (applied with policy “AP-aware” setting)
  5. If FA mgmt VLAN is announced to AP
     - NAC must plumb the AP port with the FA mgmt VLAN/I-SID in tagged mode
  6. If FA mgmt VLAN is not announced to AP
     - NAC must plumb the AP port with the AP mgmt VLAN/I-SID in untagged mode
  7. FA signalling is authorized on the opened access port so that AP can request additional VLAN/I-SIDs based on configuration obtained from Wireless Controller

FA Message Authentication and Integrity Protection



FA Client

FA Message (LLDP)
Message Authentication

FA Server (VSP)

FA Message (LLDP)
Message Authentication

FA Client

FA Message (LLDP)
Message Authentication

FA Proxy (ERS)

FA Message (LLDP)
Message Authentication

FA Server (VSP)

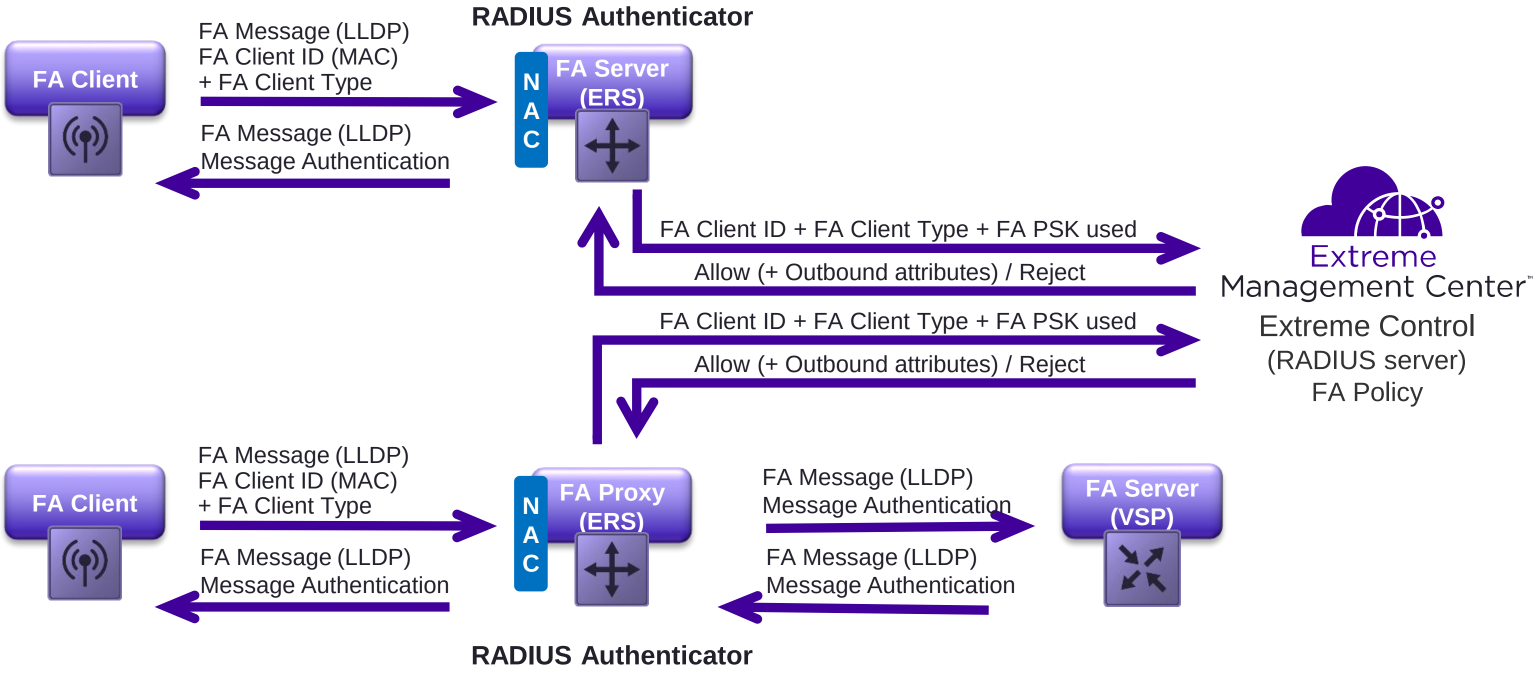
FA Message (LLDP)
Message Authentication

FA Message (LLDP)
Message Authentication

- HMAC-SHA256 algorithm is used to calculate the message authentication code (i.e., digest) involving a cryptographic hash function (SHA-256) in combination with a secret pre-configured key
- When FA message authentication is enabled, the (pre) configured FA key is used to generate a HMAC digest that is included in FA TLVs. Upon receipt, the HMAC digest is recomputed for the TLV data and compared against the digest included in the TLV. If the digests are the same, the data is valid. If not, the data is considered invalid and is “silently” ignored
- A user defined key can be configured to replace the secret pre-configured one
- On ERS4800, FA Authentication is only available with the Secure image and not with the Standard image
- Available with XOS as of 30.2 (but disabled by default); available on ISW as of 1.1.3.12

Device	VSP8600	VSP8400 VSP8200 VSP7400 VSP7200 VSP4900	5520 5420 (VOSS)	VSP4450 VSP4850	ERS5900 ERS4900	ERS4800	ERS3600	ERS3500	XOS	ISW	Extreme Wireless XCC	Extreme Wing	XIQ HiveOS	Defender IoT	3rd Party (OVS)
FA Message Authentication	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗
User configurable key	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓ (05.16.02.0020)	✗	✗	✗	✗
Support of default + custom key	✗	✗	✗	✗	✓	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗

FA Augmented NAC security for MAC based authentication



- For devices which cannot do 802.1X EAPoL (without PKI), such as video surveillance cameras, NAC deployment options are:
  - EAP-TLS : Complex, requires PKI, very secure
  - MAC based authentication (NEAP): Simple, less secure, prone to MAC spoofing

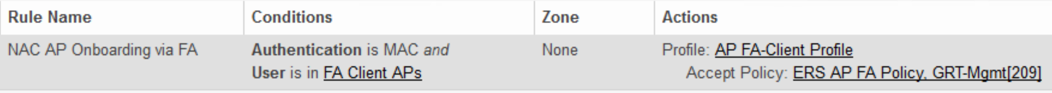
- Where the device supports FA Client and both FA Client and switch support FA message authentication, a more ideal NAC deployment option:
  - FA client with NAC authentication: Simple + more secure than MAC based authentication
  - Prevents MAC spoofing as attacker spoofing device’s MAC will not be able to provide a valid FA Client ID

FA RADIUS Attributes supported

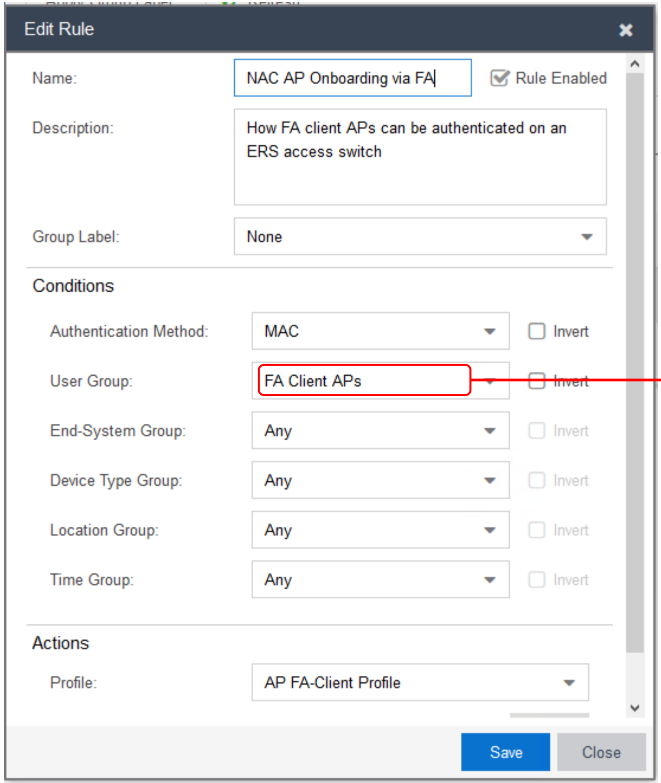
	FA RADIUS Attributes supported [Vendor id: Nortel (562)]	Attrib Id	ERS4900 /5900 (7.6)	ERS4800 (5.12)	ERS3600 (6.3)	ERS3500 (5.3)	Summit XOS (31.4)	VOSS (8.4)	VSP8600 XA1400	ISW (1.1.3.12)
IN-BOUND	**FA-Switch-Mode** *1 = FA-Server in VLAN mode; 2 = FA Server in SPBM mode; 3 = FA Proxy connected to FA Server in VLAN mode; 4 = FA Proxy connected to FA Server in SPBM mode; 5 = FA Standalone-Proxy*	180	✓ Yes	✓ Yes	✓ Yes	✓ Yes	✓ Yes	✗ No	✗ No	✓ Yes
	FA-Client-Type *FA-Client numerical type*	182	✓ Yes	✓ Yes	✓ Yes	✓ Yes	✓ Yes	✓ Yes	✗ No	✓ Yes
	FA-Client-Id *MAC address of the FA-Client device as discovered via FA signalling*	181	✓ Yes	✓ Yes	✓ Yes	✓ Yes	✓ Yes	✗ No	✗ No	✓ Yes
	FA-Client-PSK *FA Message Authentication Pre-Shared-Key in use by FA-Client* *0 = No FA Message Authentication* *10 = Default Secret Key in use & authentication failed* *11 = Default Secret Key in use & authentication succeeded* *100 = User-Defined Key in use & authentication failed* *101 = User-Defined Key in use & authentication succeeded*	183	✓ Yes	✓ Yes	✓ Yes	✗ No	✓ Yes	✗ No	✗ No	✓ Yes
OUT-BOUND	**FA-VLAN-ISID** *Attach EAP Supplicant or MAC to specified VLAN:ISID* *This attribute can be supplied multiple times with multiple VLAN:ISID bindings*	171	✓ Yes	✓ Yes	✓ Yes	✓ Yes	✓ Yes* But can use Policy instead	✓ Yes	✗ No	✓ Yes
	Extreme-NSI-Type=1 & Extreme-NSI-ID *Attach EAP Supplicant or MAC to specified ISID* *[These are Vendor ID: Extreme (1916)]*	230 231	✗ No	✗ No	✗ No	✗ No	✓ Yes*	✗ No	✗ No	✗ No
	FA-VLAN-Create *If the VLAN specified in above attribute does not locally exist, create it*	170	✓ Yes	✓ Yes	✓ Yes	✓ Yes	✗ No Policy used instead	✗ No n/a	✗ No n/a	✓ Yes
	FA-VLAN-PVID *Set the specified VLAN-id as PVID on the port*	172	✓ Yes	✓ Yes	✓ Yes	✓ Yes	✗ No Policy used instead	✗ No n/a	✗ No n/a	✓ Yes
	FA-Client-Trust *0 = Do not Trust and do not allow FA-Client initiated VLAN:ISID bindings* *1 = Trust and Allow FA-Client initiated VLAN:ISID bindings* *2 = Only allow FA-Client initiated bindings in range provided by below attribute*	184	✓ Yes	✗ No	✓ Yes	✗ No	✗ No (XOS always allows FA signalling on authorized ports)	✗ No	✗ No	✗ No
	FA-Client-Trusted-Binding *If above attributes trusts VLAN:ISID bindings from FA-Client, this attribute determines what VLAN-id:ISID-id ranges are allowed for the FA-Client*	185	✓ Yes	✗ No	✓ Yes	✗ No	✗ No (XOS always allows FA signalling on authorized ports)	✗ No	✗ No	✗ No
	FA-Service-Request *Ability to configure port-speed, BPDU-filtering, SLPP-Guard, IP-Source-Guard, DHCP-Snooping, Wake-on-Lan, Dynamic-ARP-Inspection, IGMP-Snooping*	186	✓ Yes	✓ Yes	✓ Yes	✗ No	✓ Yes (SLPP-Guard, DHCP-Snooping, DAI)	✓ Yes	✗ No	✗ No

* : On EXOS these attributes require config: configure netlogin dynamic-vlan enable

2. XMC NAC – Authenticate FA Client device on ERS/XOS access



Rule Name	Conditions	Zone	Actions
NAC AP Onboarding via FA	**Authentication** is MAC *and* **User** is in FA Client APs	None	Profile: AP FA-Client Profile Accept Policy: ERS AP FA Policy, GRT-Mgmt[209]



Name: NAC AP Onboarding via FA ☑ Rule Enabled

Description: How FA client APs can be authenticated on an ERS access switch

Group Label: None

Conditions

Authentication Method: MAC □ Invert

User Group: FA Client APs □ Invert

End-System Group: Any □ Invert

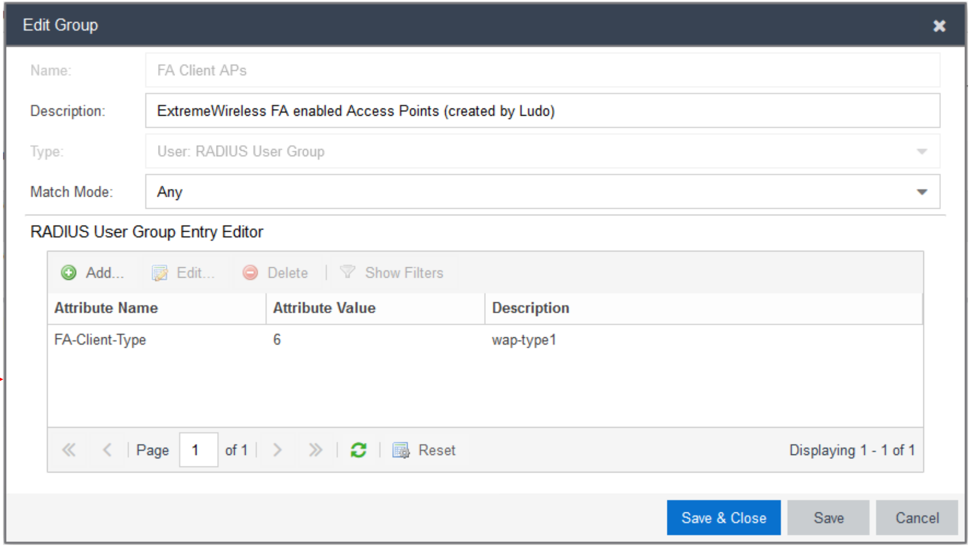
Device Type Group: Any □ Invert

Location Group: Any □ Invert

Time Group: Any □ Invert

Actions

Profile: AP FA-Client Profile



Name: FA Client APs

Description: ExtremeWireless FA enabled Access Points (created by Ludo)

Type: User: RADIUS User Group

Match Mode: Any

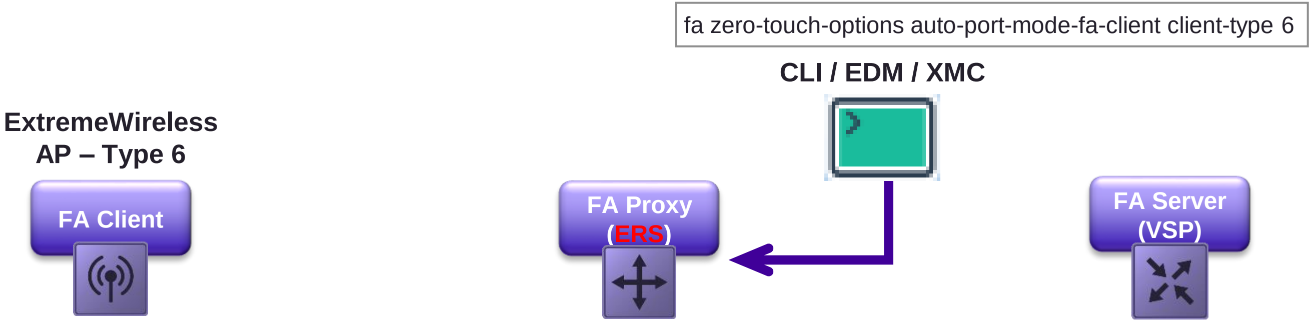
RADIUS User Group Entry Editor

Attribute Name	Attribute Value	Description
FA-Client-Type	6	wap-type1

Page 1 of 1 Reset Displaying 1 - 1 of 1

- If the FA Client and FA switch both support FA message authentication, this is a more secure way to authenticate FA clients as only clients with the correct secret key will be authorized
- Somebody spoofing the AP’s MAC won’t get in
- On XOS requires 31.1 or later

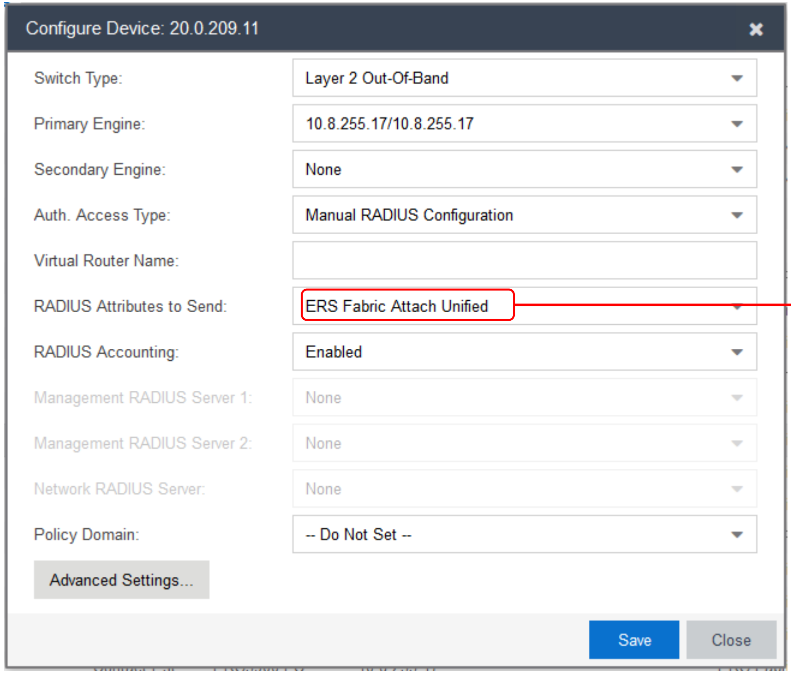
4. Automatically setting ERS port for MHSA when AP discovered



```
fa zero-touch-options auto-port-mode-fa-client client-type 6
```

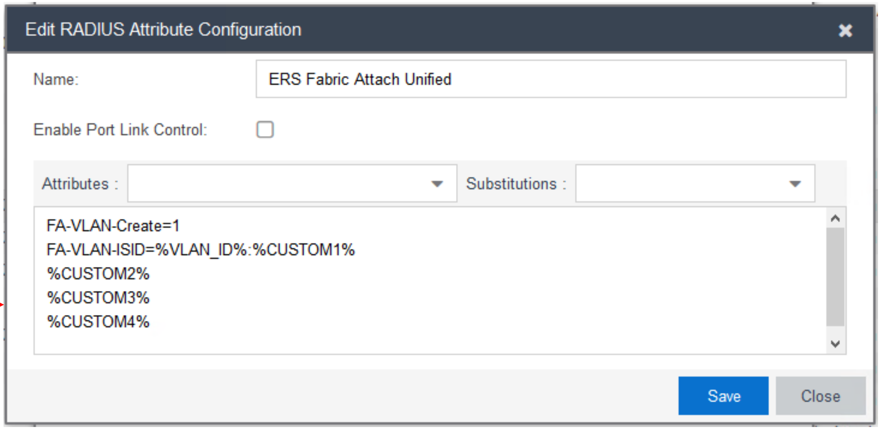
- auto-port-mode-fa-client: When this option is activated for certain FA Client types, whenever an FA client of that type is discovered on an access port, the access port is automatically pre-configured for EAP/NEAP in mode Multiple-Hosts-Single-Authentication (MHSA). The FA Client will thus need to authenticate against a RADIUS server
- This will work whether the access port is already NAC enabled or not NAC enabled at all

3. XMC NAC – ERS NAC configuration



Configure Device: 20.0.209.11

Switch Type:	Layer 2 Out-Of-Band
Primary Engine:	10.8.255.17/10.8.255.17
Secondary Engine:	None
Auth. Access Type:	Manual RADIUS Configuration
Virtual Router Name:	
RADIUS Attributes to Send:	ERS Fabric Attach Unified
RADIUS Accounting:	Enabled
Management RADIUS Server 1:	None
Management RADIUS Server 2:	None
Network RADIUS Server:	None
Policy Domain:	-- Do Not Set --



Edit RADIUS Attribute Configuration

Name: ERS Fabric Attach Unified

Enable Port Link Control: □

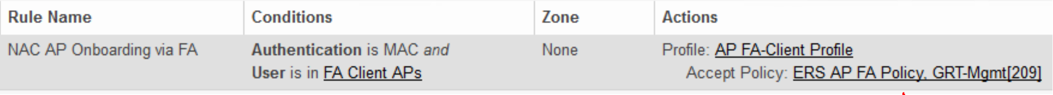
Attributes :

Substitutions :

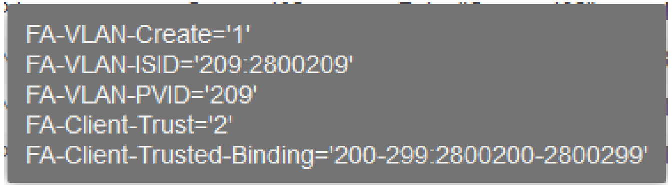
```
FA-VLAN-Create=1
FA-VLAN-ISID=%VLAN_ID%:%CUSTOM1%
%CUSTOM2%
%CUSTOM3%
%CUSTOM4%
```

- Note that we can set only 1 RADIUS attribute template per switch
- This template will be used for authorizing dot1x users, MAC based users (Custom2-4 will be null) and FA client APs (Custom2-4 will be set)

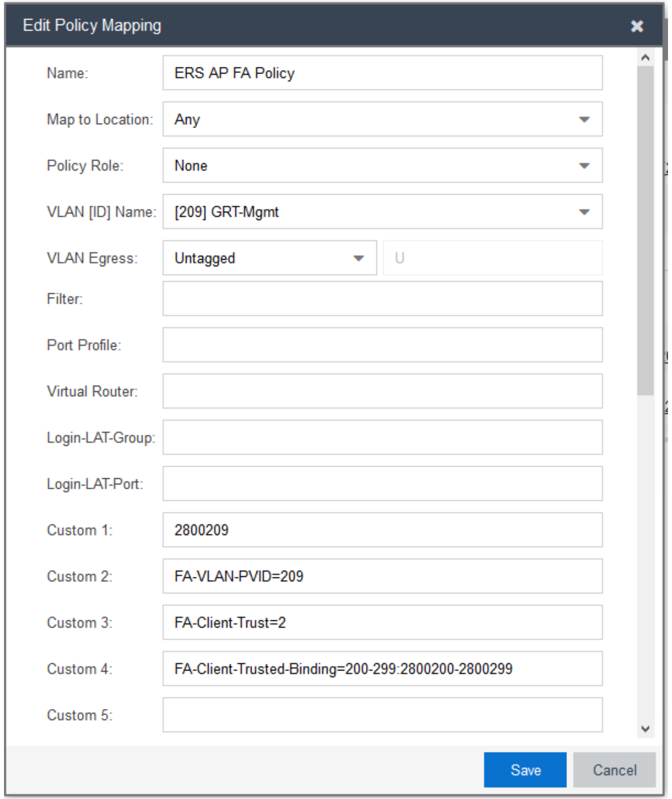
3,5,6,7. XMC NAC – ERS NAC AP FA Policy



Rule Name	Conditions	Zone	Actions
NAC AP Onboarding via FA	**Authentication** is MAC *and* **User** is in FA Client APs	None	Profile: AP FA-Client Profile Accept Policy: ERS AP FA Policy, GRT-Mgmt[209]



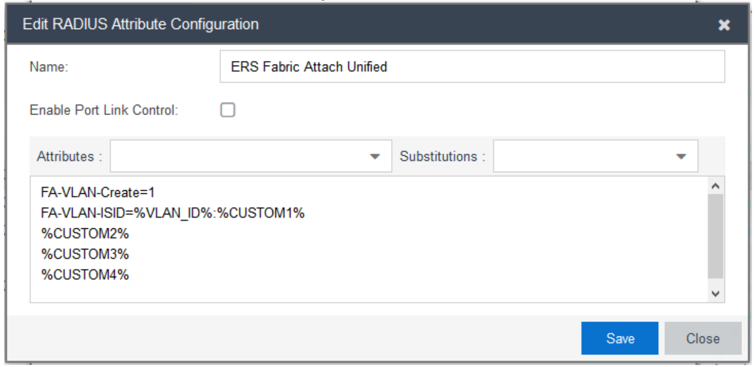
FA-VLAN-Create='1'
FA-VLAN-ISID='209:2800209'
FA-VLAN-PVID='209'
FA-Client-Trust='2'
FA-Client-Trusted-Binding='200-299:2800200-2800299'



Edit Policy Mapping

Name:	ERS AP FA Policy
Map to Location:	Any
Policy Role:	None
VLAN [ID] Name:	[209] GRT-Mgmt
VLAN Egress:	Untagged U
Filter:	
Port Profile:	
Virtual Router:	
Login-LAT-Group:	
Login-LAT-Port:	
Custom 1:	2800209
Custom 2:	FA-VLAN-PVID=209
Custom 3:	FA-Client-Trust=2
Custom 4:	FA-Client-Trusted-Binding=200-299:2800200-2800299
Custom 5:	

- This policy is used to authorize AP FA Clients on ERS access
- The above box shows an example of RADIUS attributes will be sent to ERS access switch to authorize an AP
- NOTE: We set the mgmt VLAN as PVID also; this is important if no FA mgmt VLAN is advertised to the AP, in which case the AP will do DHCP untagged and will FA signal back to ERS desire to send untagged & tagged traffic, so the ERS will automatically set the port into UntagPvidOnly, where the port PVID becomes critical!
- On ERS, the FA-Client-Trust attribute must always be set otherwise no FA signalling will be accepted on NAC port (not available on ERS4800,3600,3500)



Edit RADIUS Attribute Configuration

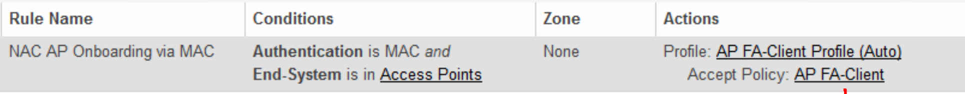
Name: ERS Fabric Attach Unified

Enable Port Link Control: □

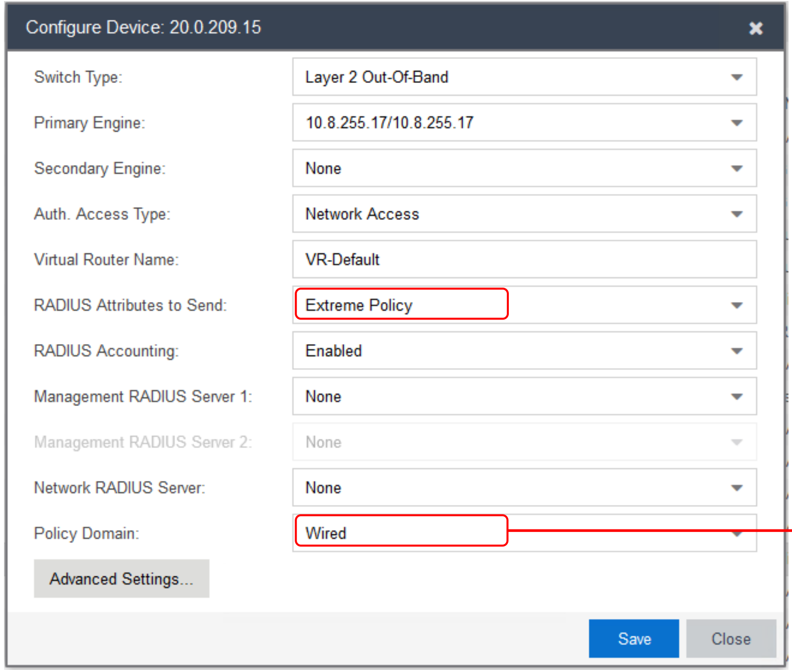
Attributes :
Substitutions :

```
FA-VLAN-Create=1
FA-VLAN-ISID=%VLAN_ID%:%CUSTOM1%
%CUSTOM2%
%CUSTOM3%
%CUSTOM4%
```

3. XMC NAC – XOS NAC configuration

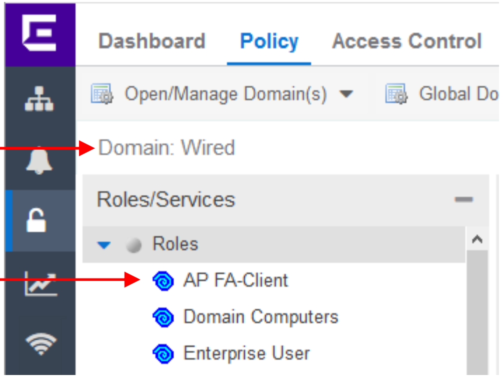


Rule Name	Conditions	Zone	Actions
NAC AP Onboarding via MAC	**Authentication** is MAC *and* **End-System** is in Access Points	None	Profile: AP FA-Client Profile (Auto) Accept Policy: AP FA-Client



Configure Device: 20.0.209.15

Switch Type:	Layer 2 Out-Of-Band
Primary Engine:	10.8.255.17/10.8.255.17
Secondary Engine:	None
Auth. Access Type:	Network Access
Virtual Router Name:	VR-Default
RADIUS Attributes to Send:	Extreme Policy
RADIUS Accounting:	Enabled
Management RADIUS Server 1:	None
Management RADIUS Server 2:	None
Network RADIUS Server:	None
Policy Domain:	Wired



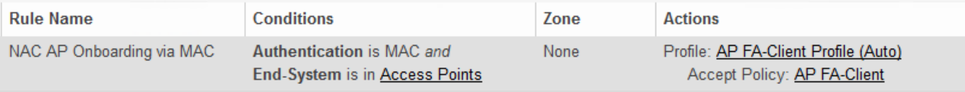
Domain: Wired

Roles/Services

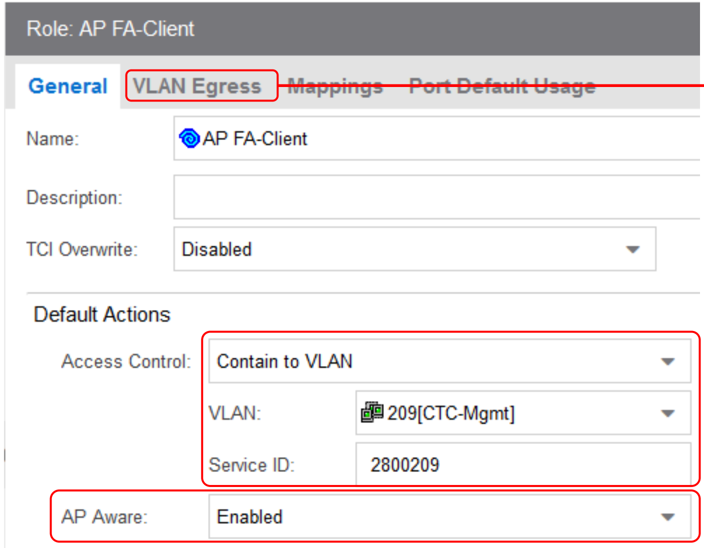
- Roles
  - AP FA-Client
  - Domain Computers
  - Enterprise User

- With XOS we have the power of policies

5,6,7. XMC NAC – XOS AP FA Policy



Rule Name	Conditions	Zone	Actions
NAC AP Onboarding via MAC	**Authentication** is MAC *and* **End-System** is in Access Points	None	Profile: AP FA-Client Profile (Auto) Accept Policy: AP FA-Client



Role: AP FA-Client

Name: AP FA-Client

Description:

TCI Overwrite: Disabled

Default Actions

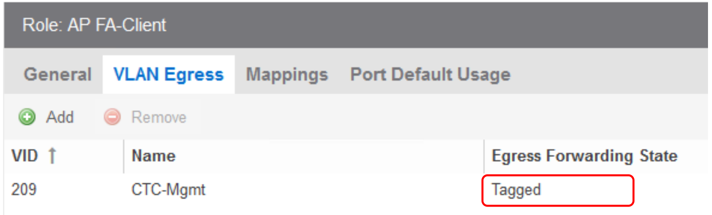
Access Control: Contain to VLAN

VLAN: 209[CTC-Mgmt]

Service ID: 2800209

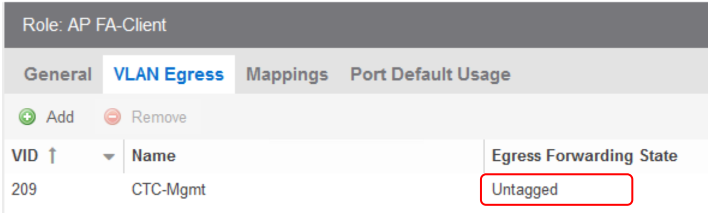
AP Aware: Enabled

- This policy is used to authorize AP FA Clients on XOS access
- If the AP is to be managed on the same switch FA mgmt VLAN, set the egress VLAN as tagged
- If the AP is to be managed on a different VLAN, set that VLAN as untagged



Role: AP FA-Client

VID	Name	Egress Forwarding State
209	CTC-Mgmt	Tagged



Role: AP FA-Client

VID	Name	Egress Forwarding State
209	CTC-Mgmt	Untagged

Summary of deployment models

Fabric Attach challenges

- Once deployed, Fabric Attach brings simplicity and automation
- ..but there is a lot of detail in deploying it, and the devil is in there..
  - Many deployment permutations exist
    - ERS or XOS (or VSP) access
      - FA Proxy access (ERS/XOS) or FA Server access (ERS/VSP)
    - Wireless APs deployed on same mgmt VLAN/subnet as access switches or on different subnet
    - NAC wired access vs Open wired Access
    - Ambition of FA is to be elastic, an access port should not need to be configured differently in order to work with an FA Client
  - Many sub-components to FA functionality, different products support different sub-sets, inconsistent implementations in some cases
    - Zero-touch-options, Zero-Touch-Client, FA mgmt VLAN, FA RADIUS attributes, interaction with NAC

Device icons used in these slides

- Non-FA-Client device
  - PC, Phone, Printer, etc..

- Untagged FA-Client
  - Devices which only need to be part of 1 VLAN/VSN
  - and do not signal any FA VLAN:ISID bindings
  - e.g. Video Surveillance cameras (AXIS, Pelco)

- Tagged FA-Client
  - Devices which will need to connect into multiple VLAN/VSNs
  - and will use FA VLAN:ISID Signalling
  - e.g. ExtremeWireless & Wing APs, Defender for IoT

Extreme Campus Controller

- Controller
  - Extreme Campus Controller (XCC) for any ExtremeWireless APs & Defender for IoT
  - Also Wing Controller, for Wing designs

Extreme Control

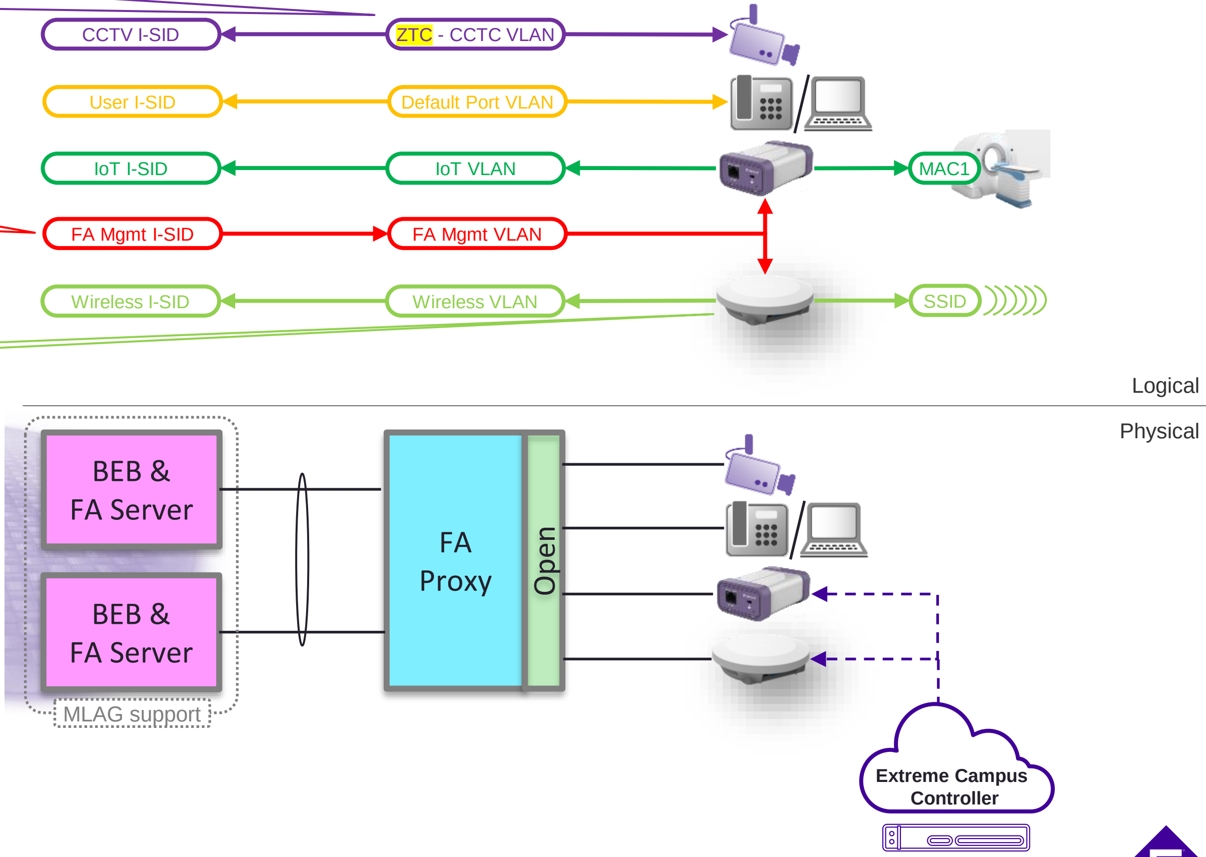
- XMC Control

Interpretation of VLAN arrows used in these slides

FA Zero-Touch-Config profiles are defined on access switch and use FA signalling back towards FA Server

FA Mgmt VLAN is defined on FA Server and advertised to attached FA Proxy/Clients

FA Signalling initiated by FA Client device

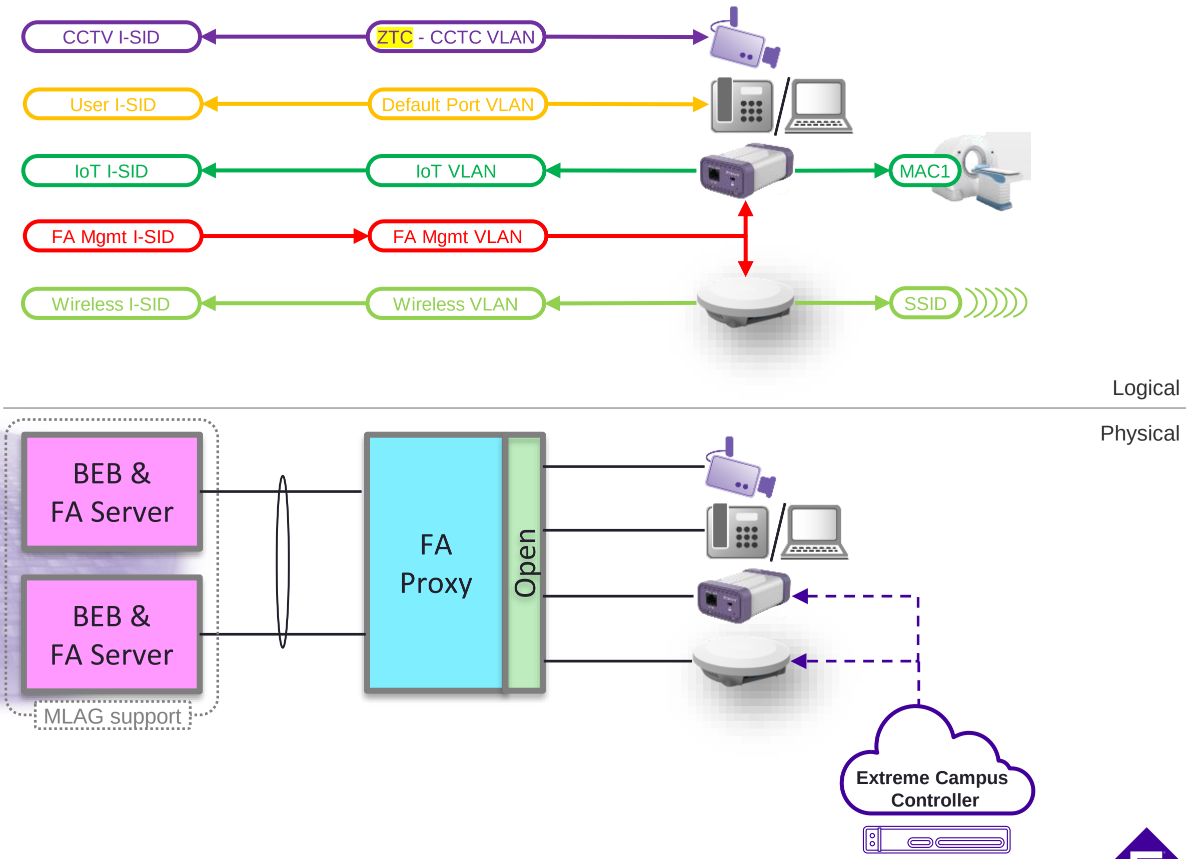


- Arrows indicate in which direction a VLAN/I-SID was provisioned/signalled

Wired access Open – AP & switch mgmt in same VLAN

	Category	FA Proxy		Comments
1	Untagged FA Client VSN based on FA Client type	XOS	✓	Use FA Zero-Touch-Client (ZTC)
		ERS	✓*	Use FA Zero-Touch-Client (ZTC)
2	Non-FA-Client device assigned to default port VLAN	XOS	✓	
		ERS	✓	
3	WAP/Defender FA Client mgmt on FA mgmt VLAN	XOS	✓	XOS automatically tags FA mgmt VLAN on ports where an FA Client detected
		ERS	✓	ERS must be configured with FA zero-touch-option auto-mgmt-vlan-fa-client
4	FA Proxy access switch obtains mgmt VLAN from FA Server	XOS	✓	
		ERS	✓	
5	Same config for all wired access ports	XOS	✓	
		ERS	✓	

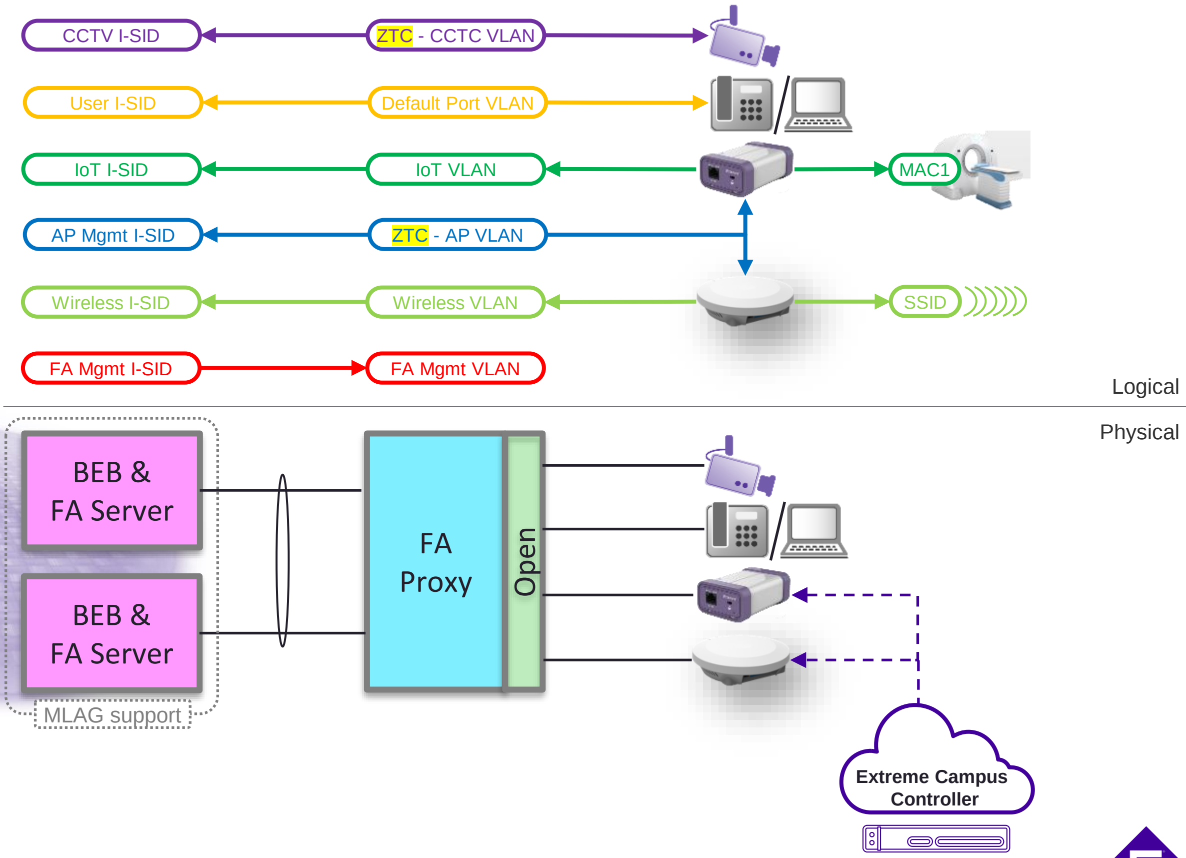
* Not on ERS3500



Wired access Open – AP & switch mgmt in separate VLANs

	Category	FA Proxy		Comments
1	Untagged FA Client VSN based on FA Client type	XOS	✓	Use FA Zero-Touch-Client (ZTC)
		ERS	✓*	Use FA Zero-Touch-Client (ZTC)
2	Non-FA-Client device assigned to default port VLAN	XOS	✓	
		ERS	✓	
3a	Do not advertise FA mgmt VLAN to FA Client	XOS	✓	configure fabric attach management-vlan forward off
		ERS	✓*	Set FA disable-mgmt-vlan-distribution
3b	WAP/Defender FA Client mgmt VSN different from FA mgmt VLAN	XOS	✓	Use FA Zero-Touch-Client (ZTC)
		ERS	✓*	Use FA Zero-Touch-Client (ZTC)
4	FA Proxy access switch obtains mgmt VLAN from FA Server	XOS	✓	
		ERS	✓	
5	Same config for all wired access ports	XOS	✓	(if using Python script for ZTC)
		ERS	✓	

* Not on ERS3500

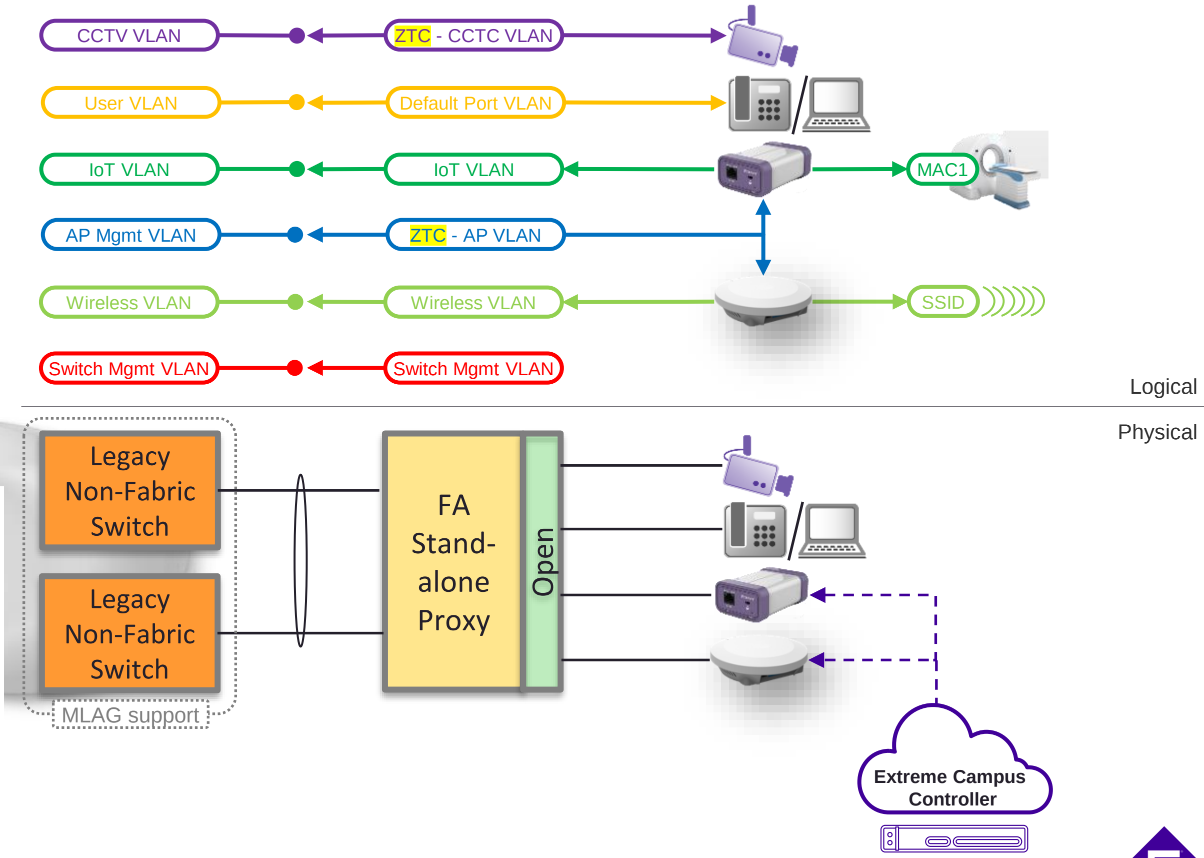


Non-Fabric/Legacy Core - Wired access Open

	Category	FA Standalone Proxy		Comments
1	Untagged FA Client VLAN based on FA Client type	XOS	✓	Use FA Zero-Touch-Client (ZTC)
		ERS	✓*	Use FA Zero-Touch-Client (ZTC)
2	Non-FA-Client device assigned to default port VLAN	XOS	✓	
		ERS	✓	
3a	Do not advertise FA mgmt VLAN to FA Client	XOS	✓	None advertised in FA Standalone Proxy mode
		ERS	✓	Set FA disable-mgmt-vlan-distribution
3b	WAP/Defender FA Client mgmt VLAN different from FA mgmt VLAN	XOS	✓	Use FA Zero-Touch-Client (ZTC)
		ERS	✓*	Use FA Zero-Touch-Client (ZTC)
5	Same config for all wired access ports	XOS	✓	(if using Python script for ZTC)
		ERS	✓	

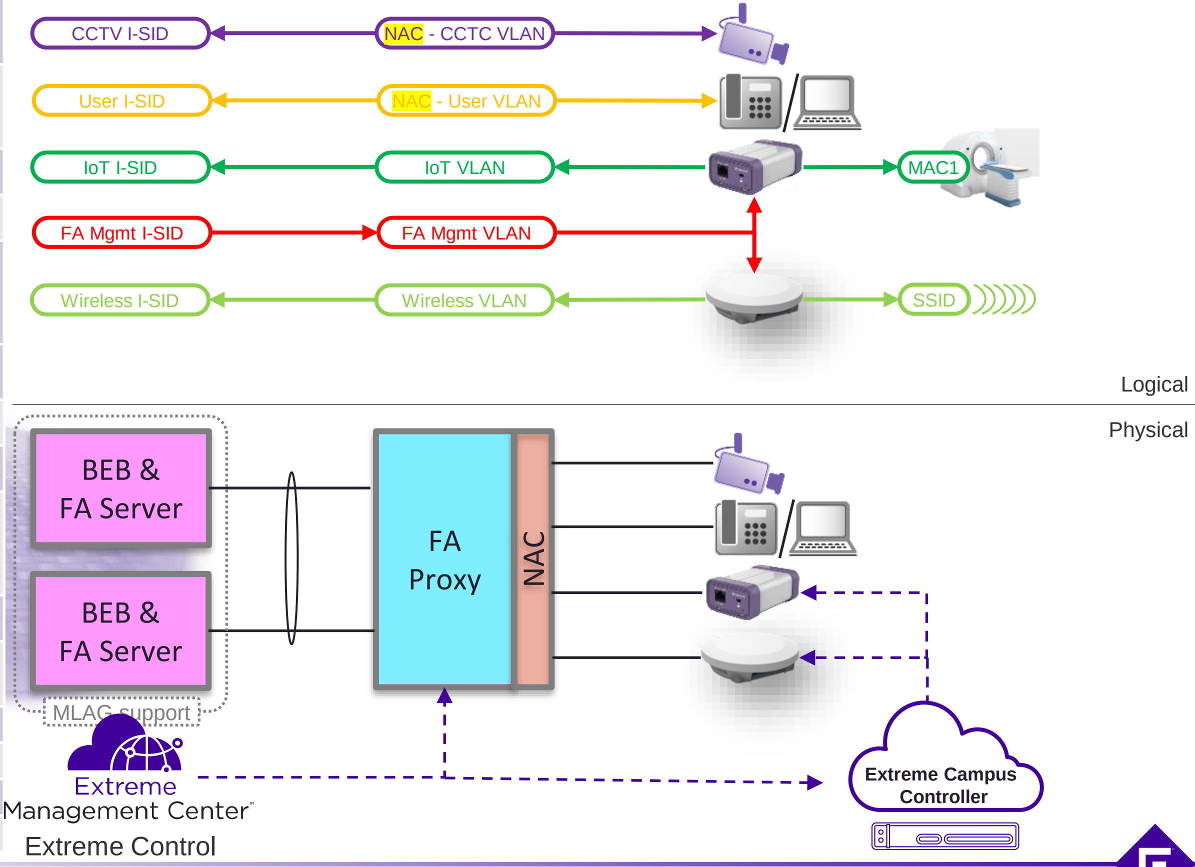
* Not on ERS3500

- On ERS in FA Standalone Proxy mode there is still a concept of FA mgmt VLAN, but this is now simply whatever ERS VLAN is set as the mgmt-vlan
- On XOS in FA Standalone Proxy mode there is no FA mgmt VLAN
  - A CLI command “`configure fabric attach management-vlan`” exists, but does not currently work



NAC Wired access – AP & switch mgmt in same VLAN

	Category	FA Proxy		Comments
1	Untagged FA Client VSN via NAC	XOS	✓	Authenticate based on inbound RADIUS attribute FA-Client-Type and use NAC + Policy with Contain to VLAN/ISID
		ERS	✓	Authenticate based on inbound RADIUS attribute FA-Client-Type and use outbound RADIUS FA-VLAN-ISID
2	Non-FA-Client VSN via NAC	XOS	✓	Use NAC + Policy with Contain to VLAN/ISID
		ERS	✓	Use NAC outbound RADIUS FA-VLAN-ISID
3b	NAC Authenticate WAP/Defender FA Client based on FA Client inbound RADIUS attributes	XOS	✓	ERS NAC rule match on inbound RADIUS attribute Fabric-Attach-Client-Type = 6 (wap-type1)
		ERS	✓	
3c	WAP/Defender FA Client mgmt on FA mgmt VLAN	XOS	✓	Use policy with Contain to FA mgmt VLAN/ISID + Egress VLAN Tagged
		ERS	✓	Use NAC outbound RADIUS FA-VLAN-ISID set to FA mgmt VLAN
3d	WAP/Defender FA Client NAC open port as Multiple Host Single Authentication (MHSA)	XOS	✓	Assign policy with "AP aware" (auth-override)
		ERS	✓	ERS must be configured with FA zero-touch-option auto-port-mode-fa-client which will enable MHSA mode on ports where FA Client detected
3e	WAP/Defender FA Client allow FA signalling on NAC port	XOS	✓	XOS always allows FA signalling on authorized NAC ports
		ERS	✓*	NAC must return RADIUS outbound attribute FA-Client-Trust and optional FA-Client-Trusted-Binding
4	FA Proxy access switch obtains mgmt VLAN from FA Server	XOS	✓	
		ERS	✓	
5	Same config for all wired access ports	XOS	✓	
		ERS	✓	

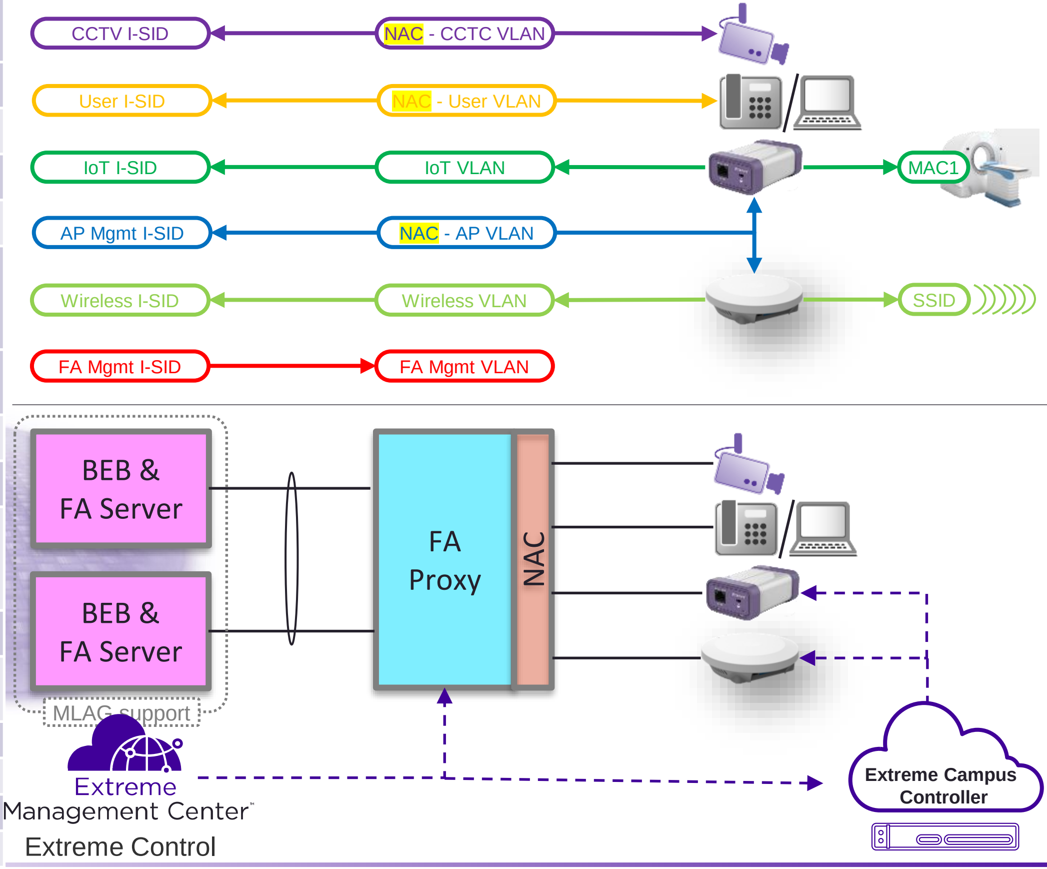


CCTV I-SID
NAC - CCTC VLAN
User I-SID
NAC - User VLAN
IoT I-SID
IoT VLAN
MAC1
FA Mgmt I-SID
FA Mgmt VLAN
Wireless I-SID
Wireless VLAN
SSID
Logical
Physical
BEB & FA Server
BEB & FA Server
MLAG support
FA Proxy
NAC
Extreme Management Center
Extreme Control
Extreme Campus Controller

* Not on ERS4800, ERS3500

NAC Wired access – AP & switch mgmt in separate VLANs

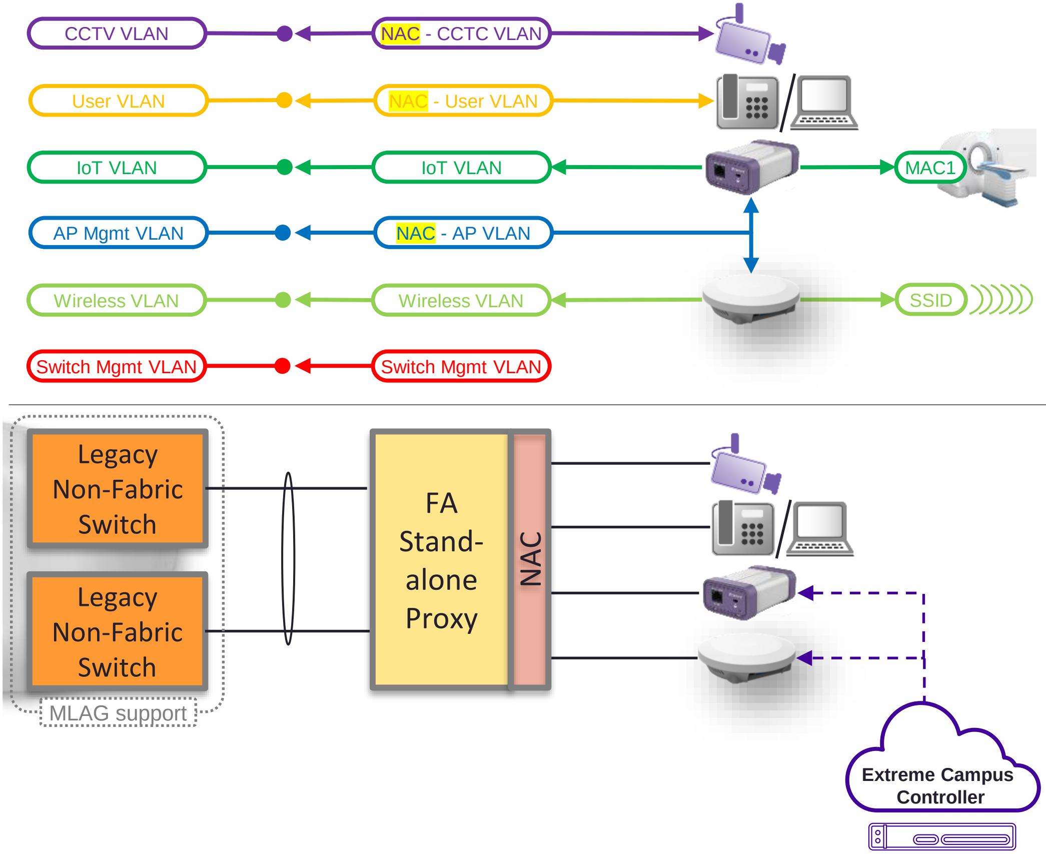
	Category	FA Proxy		Comments
1	Untagged FA Client VSN via NAC	XOS	✓	Authenticate based on inbound RADIUS attribute FA-Client-Type
		ERS	✓	
2	Non-FA-Client VSN via NAC	XOS	✓	Use NAC + Policy with Contain to VLAN/ISID
		ERS	✓	Use NAC outbound RADIUS FA-VLAN-ISID
3a	Do not advertise FA mgmt VLAN to FA Client	XOS	✓	configure fabric attach management-vlan forward off
		ERS	✓	Set FA disable-mgmt-vlan-distribution
3b	NAC Authenticate WAP/Defender FA Client based on FA Client inbound RADIUS attributes	XOS	✓	ERS NAC rule match on inbound RADIUS attribute Fabric-Attach-Client-Type = 6 (wap-type1)
		ERS	✓	
3c	WAP/Defender FA Client mgmt VSN different from FA mgmt VLAN	XOS	✓	Use policy with Contain to VLAN/ISID + Egress VLAN Untagged
		ERS	✓	Use NAC outbound RADIUS FA-VLAN-ISID
3d	WAP/Defender FA Client NAC open port as Multiple Host Single Authentication (MHSA)	XOS	✓	Assign policy with “AP aware” (auth-override)
		ERS	✓	ERS must be configured with FA zero-touch-option auto-port-mode-fa-client which will enable MHSA mode on ports where FA Client detected
3e	WAP/Defender FA Client allow FA signalling on NAC port	XOS	✓	XOS always allows FA signalling on authorized NAC ports
		ERS	✓*	NAC must return RADIUS outbound attribute FA-Client-Trust and optional FA-Client-Trusted-Binding
4	FA Proxy access switch obtains mgmt VLAN from FA Server	XOS	✓	
		ERS	✓	
5	Same config for all wired access ports	XOS	✓	
		ERS	✓	



* Not on ERS4800, ERS3500

Non-Fabric/Legacy Core - NAC Wired access

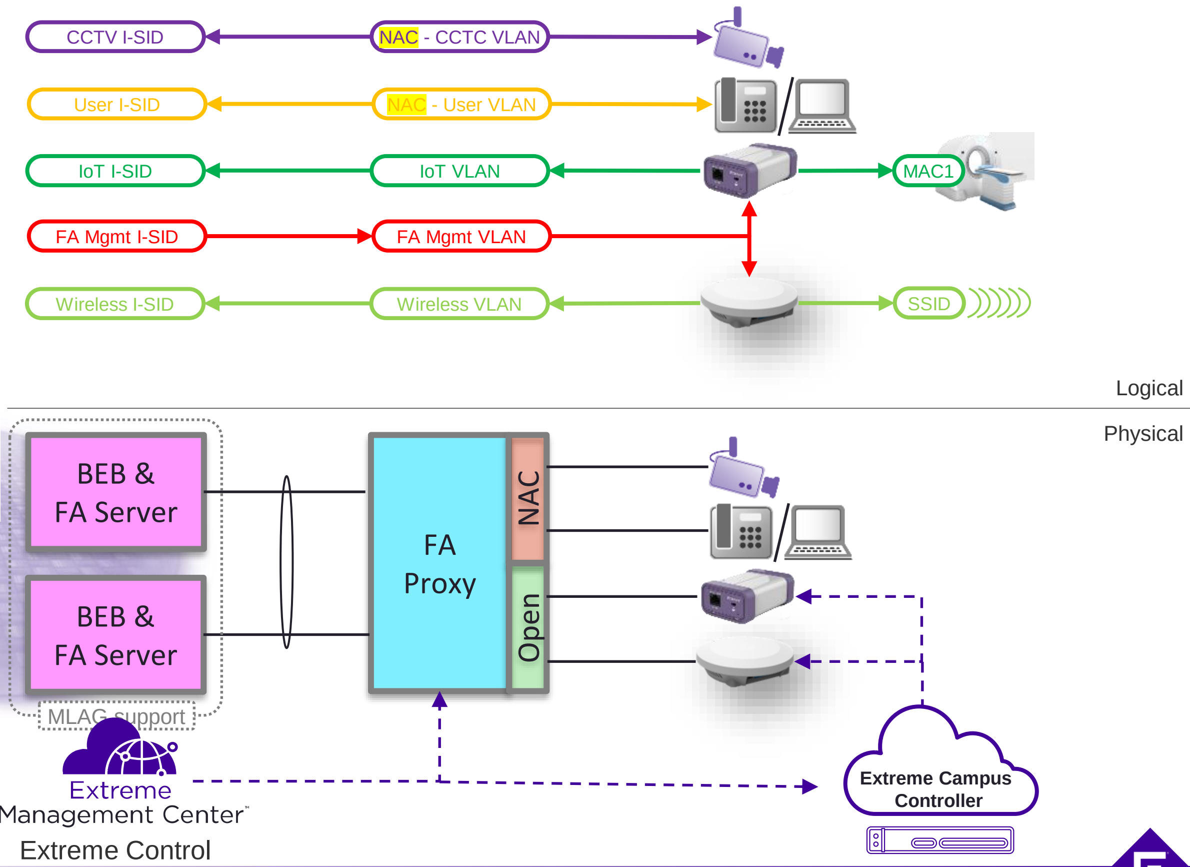
	Category	FA Standalone Proxy		Comments
1	Untagged FA Client VLAN via NAC	XOS	✓	Authenticate based on inbound RADIUS attribute FA-Client-Type
		ERS	✓	
2	Non-FA-Client VLAN via NAC	XOS	✓	Use NAC + Policy with Contain to VLAN
		ERS	✓	Use NAC outbound RADIUS FA-VLAN-ISID (with ISID=0)
3a	Do not advertise FA mgmt VLAN to FA Client	XOS	✓	None advertised in FA Standalone Proxy mode
		ERS	✓	Set FA disable-mgmt-vlan-distribution
3b	NAC Authenticate WAP/Defender FA Client based on FA Client inbound RADIUS attributes	XOS	✓	ERS NAC rule match on inbound RADIUS attribute Fabric-Attach-Client-Type = 6 (wap-type1)
		ERS	✓	
3c	WAP/Defender FA Client mgmt VLAN different from Switch mgmt VLAN	XOS	✓	Use policy with Contain to VLAN + Egress VLAN Untagged
		ERS	✓	Use NAC outbound RADIUS FA-VLAN-ISID (with ISID = 0)
3d	WAP/Defender FA Client NAC open port as Multiple Host Single Authentication (MHSA)	XOS	✓	Assign policy with “AP aware” (auth-override)
		ERS	✓	ERS must be configured with FA zero-touch-option auto-port-mode-fa-client which will enable MHSA mode on ports where FA Client detected
3e	WAP/Defender FA Client allow FA signalling on NAC port	XOS	✓	XOS always allows FA signalling on authorized NAC ports
		ERS	✓*	NAC must return RADIUS outbound attribute FA-Client-Trust and optional FA-Client-Trusted-Binding
5	Same config for all wired access ports	XOS	✓	
		ERS	✓	



* Not on ERS4800, ERS3500

Hybrid NAC/Open access – AP & switch mgmt in same VLAN

	Category	FA Proxy		Comments
1	Untagged FA Client VSN via NAC	XOS	✓	Authenticate based on inbound RADIUS attribute FA-Client-Type and use NAC + Policy with Contain to VLAN/ISID
		ERS	✓	Authenticate based on inbound RADIUS attribute FA-Client-Type and use outbound RADIUS FA-VLAN-ISID
2	Non-FA-Client VSN via NAC	XOS	✓	Use NAC + Policy with Contain to VLAN/ISID
		ERS	✓	Use NAC outbound RADIUS FA-VLAN-ISID
3	WAP/Defender FA Client mgmt on FA mgmt VLAN	XOS	✓	XOS automatically tags FA mgmt VLAN on ports where an FA Client detected
		ERS	✓	ERS must be configured with FA zero-touch-option auto-mgmt-vlan-fa-client
4	FA Proxy access switch obtains mgmt VLAN from FA Server	XOS	✓	
		ERS	✓	
5	Same config for all wired access ports	XOS	✗	By definition we have a different port config for WAP/Defender FA Clients
		ERS	✗	



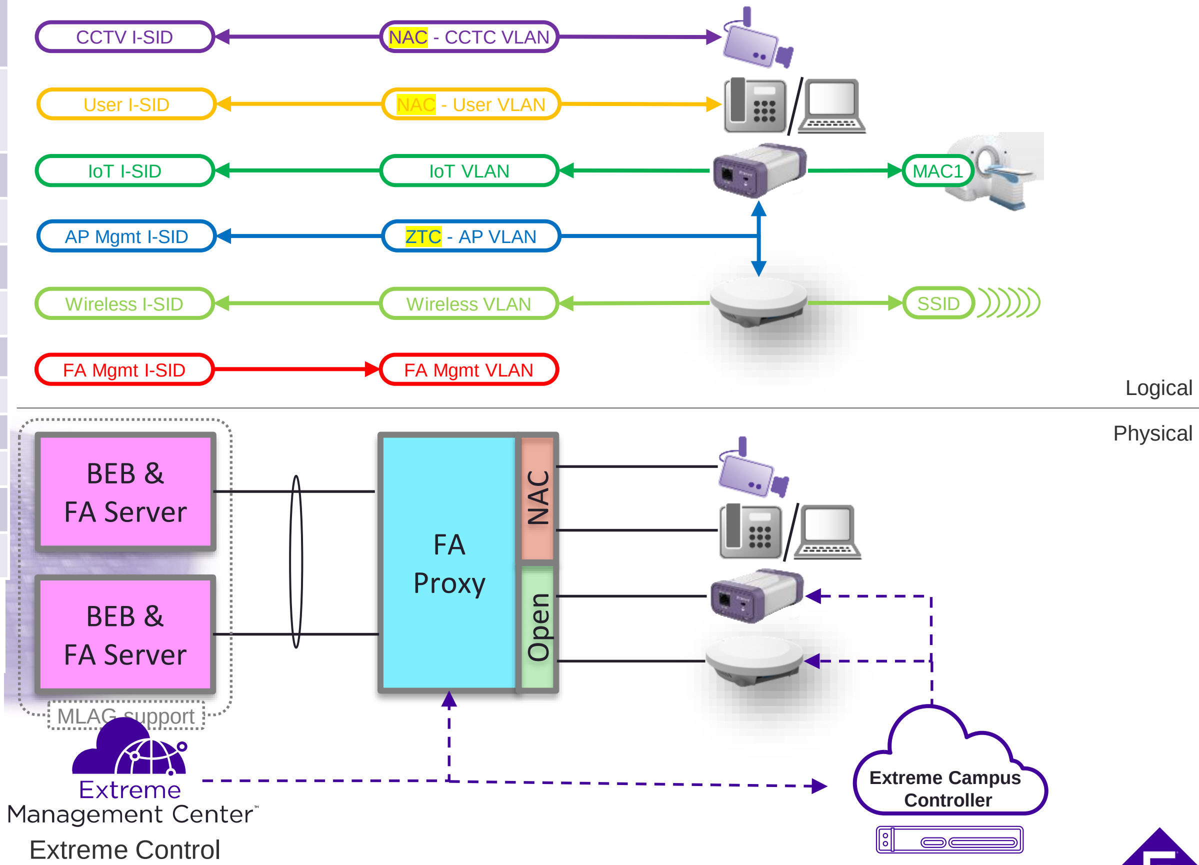
- Tempting, to avoid NAC complications with WAP/Defender FA Client devices, but..
- Defeats elasticity goal of FA as requires a different port config for some FA Clients
- Defeats doing NAC in the 1st place!

Hybrid NAC/Open access – AP & switch mgmt in separate VLANs

	Category	FA Proxy		Comments
1	Untagged FA Client VSN via NAC	XOS	✓	Authenticate based on inbound RADIUS attribute FA-Client-Type and use NAC + Policy with Contain to VLAN/ISID
		ERS	✓	Authenticate based on inbound RADIUS attribute FA-Client-Type and use outbound RADIUS FA-VLAN-ISID
2	Non-FA-Client VSN via NAC	XOS	✓	Use NAC + Policy with Contain to VLAN/ISID
		ERS	✓	Use NAC outbound RADIUS FA-VLAN-ISID
3a	Do not advertise FA mgmt VLAN to FA Client	XOS	✓	configure fabric attach management-vlan forward off
		ERS	✓	Set FA disable-mgmt-vlan-distribution
3b	WAP/Defender FA Client mgmt VSN different from FA mgmt VLAN	XOS	✓	Use FA Zero-Touch-Client (ZTC)
		ERS	✓*	Use FA Zero-Touch-Client (ZTC)
4	FA Proxy access switch obtains mgmt VLAN from FA Server	XOS	✓	
		ERS	✓	
5	Same config for all wired access ports	XOS	✗	By definition we have a different port config for WAP/Defender FA Clients
		ERS	✗	By definition we have a different port config for WAP/Defender FA Clients

* Not on ERS3500

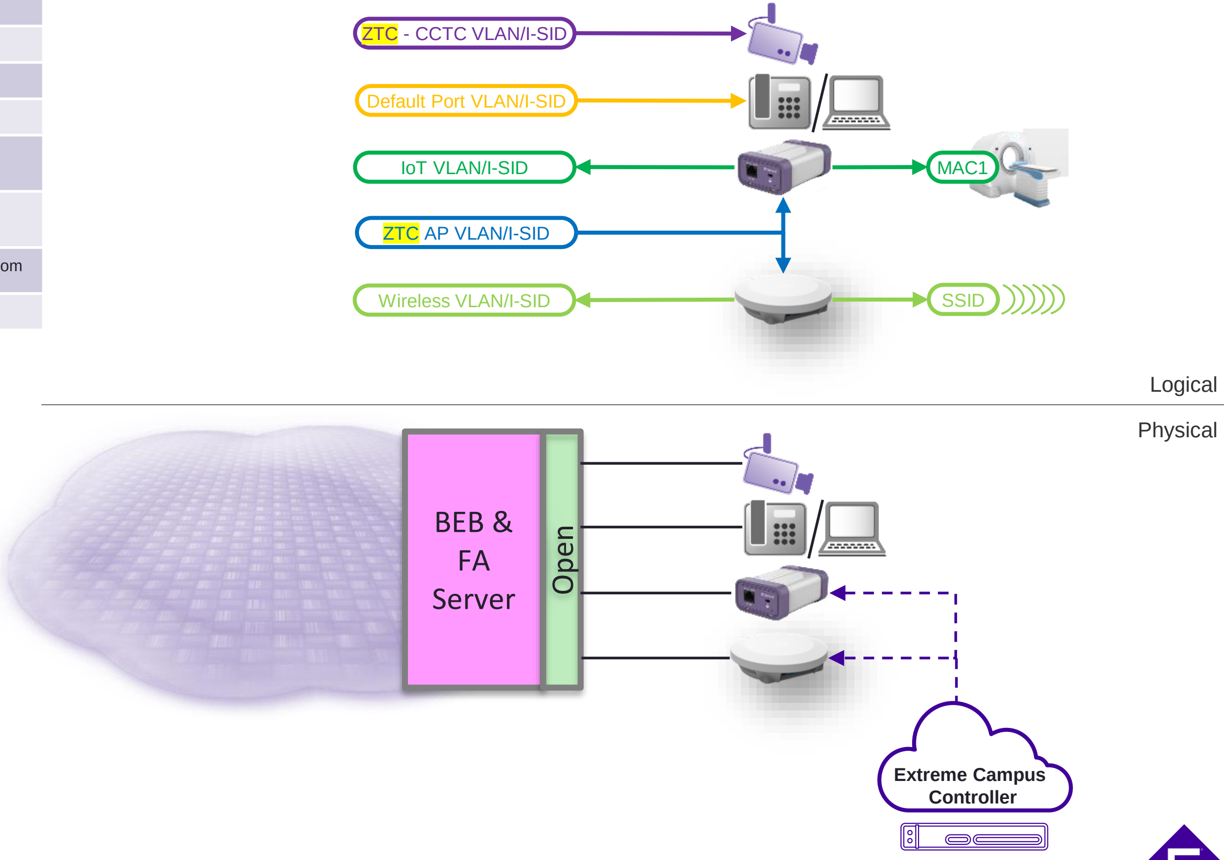
- Tempting, to avoid NAC complications with WAP/Defender FA Client devices, but..
- Defeats elasticity goal of FA as requires a different port config for some FA Clients
- Defeats doing NAC in the 1st place!



Wired access Open – Fabric Connect edge

	Category	FA Server		Comments
1	Untagged FA Client VSN based on FA Client type	VSP	✓	Use FA Zero-Touch-Client (ZTC). But port must be FA enabled
		ERS*	✓	Use FA Zero-Touch-Client (ZTC)
2	Non-FA-Client device assigned to default port VLAN	VSP	✓	But port must not be FA enabled
		ERS*	✓	
3	WAP/Defender FA Client mgmt on AP mgmt VLAN	VSP	✓	Use FA Zero-Touch-Client (ZTC). But port must be FA enabled
		ERS*	✓	Set FA disable-mgmt-vlan-distribution
5	Same config for all wired access ports	VSP	✗	1&3 require different port config from 2
		ERS*	✓	

* Not ERS3500, ERS3600 (as no FC support)



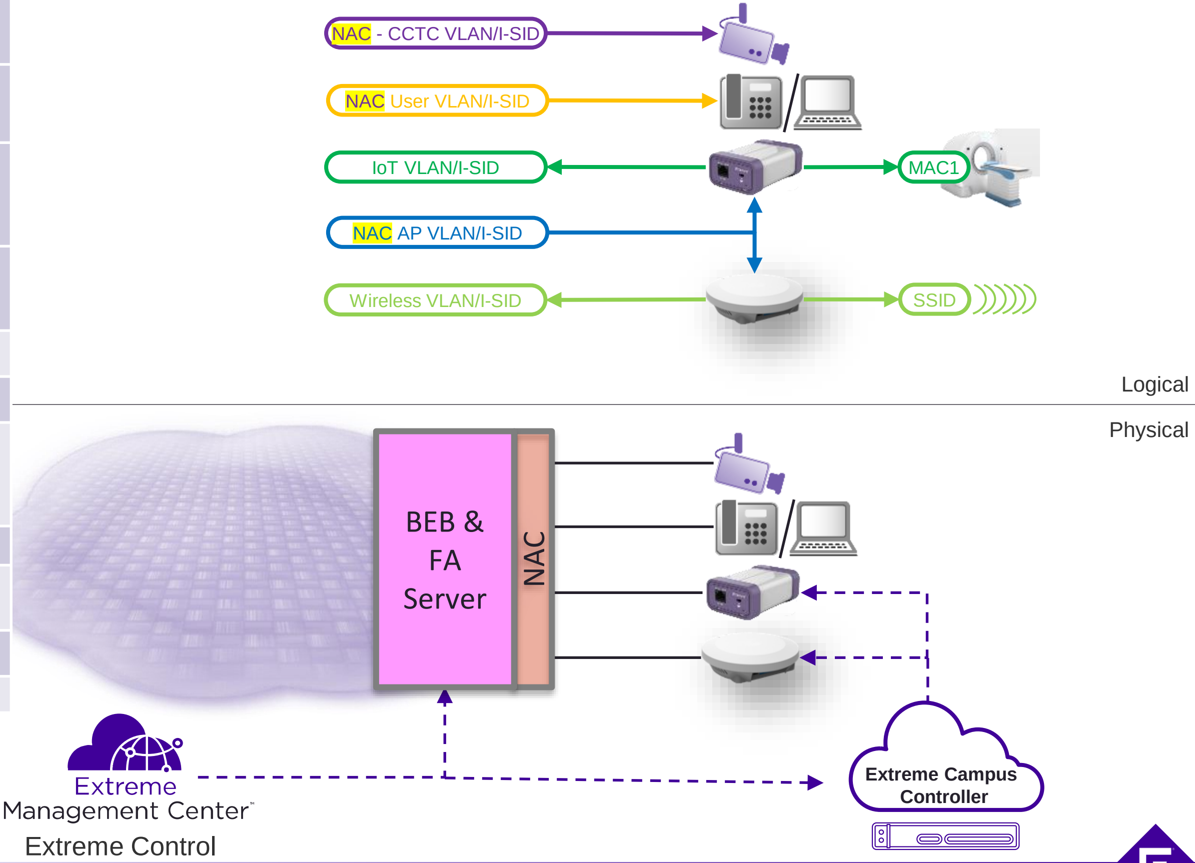
- Less common deployment scenario
- ..but will be needed once VOSS supports extended edge (VPEX)

NAC Wired access – Fabric Connect edge

	Category	FA Server		Comments
1	Untagged FA Client VSN via NAC	VSP	✓	Authenticate based on inbound RADIUS attribute FA-Client-Type and use outbound RADIUS FA-VLAN-ISID
		ERS*	✓	
2	Non-FA-Client VSN via NAC	VSP	✓	Use NAC outbound RADIUS FA-VLAN-ISID
		ERS*	✓	
3b	NAC Authenticate WAP/Defender FA Client based on FA Client inbound RADIUS attributes	VSP	✓	ERS NAC rule match on inbound RADIUS attribute Fabric-Attach-Client-Type = 6 (wap-type1)
		ERS*	✓	
3c	WAP/Defender FA Client mgmt on AP mgmt VLAN	VSP	✓	Use NAC outbound RADIUS FA-VLAN-ISID set to FA mgmt VLAN Requires disabling auto-sense to set FA mgmt VLAN on port
		ERS*	✓	Use NAC outbound RADIUS FA-VLAN-ISID set to FA mgmt VLAN
3d	WAP/Defender FA Client NAC open port as Multiple Host Single Authentication (MHSA)	VSP	✓	Use NAC outbound Extreme-Dynamic-MHSA=1 attribute
		ERS*	✓	ERS must be configured with FA zero-touch-option auto-port-mode-fa-client which will enable MHSA mode on ports where FA Client detected
3e	WAP/Defender FA Client allow FA signalling on NAC port	VSP	✓	Supported with auto-sense
		ERS*	✓*	NAC must return RADIUS outbound attribute FA-Client-Trust and optional FA-Client-Trusted-Binding
5	Same config for all wired access ports	VSP	✓	Normally yes with auto-sense (except 3c)
		ERS*	✓	

* Not ERS3500, ERS3600 (as no FC support)

* Not on ERS4800



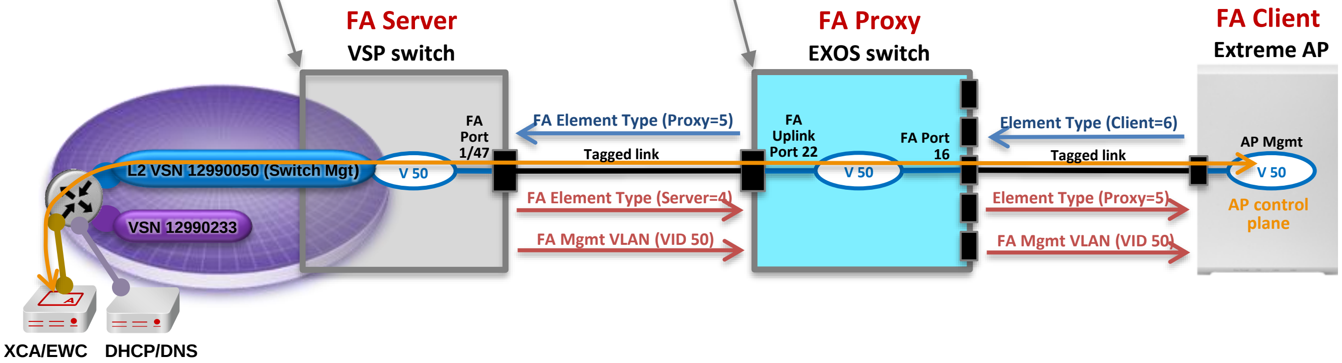
Behind the curtains for Fabric Attach

1A: EXOS and AP with FA - Tagged Mgmt

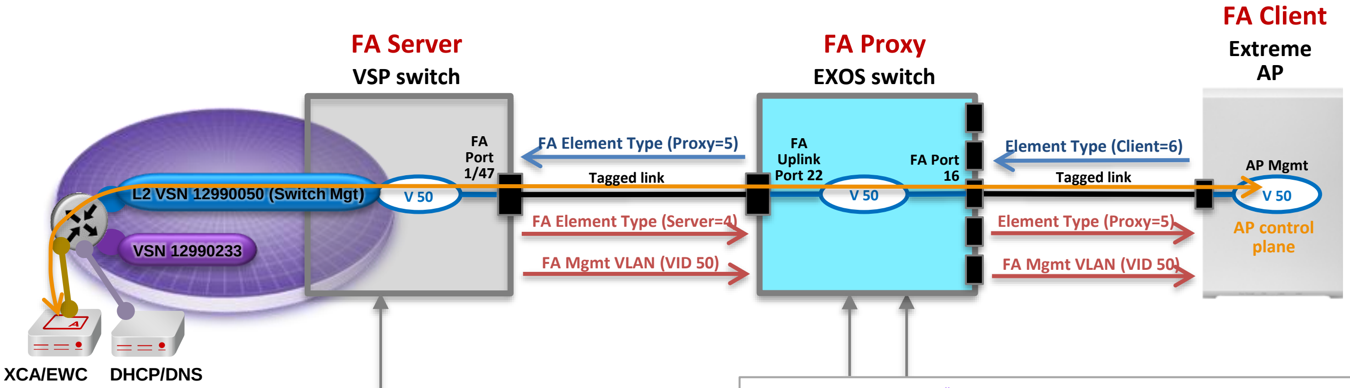
- **FA Server, FA Proxy and FA Client discover each other via LLDP Element TLVs.**
  - Disable FA message authentication on FA Server *(important ! EXOS will support Pre-shared key in 30.2).*
- **FA Management VLAN 50 advertised to FA Proxy from FA Server**
  - FA Proxy creates VLAN 50, tags uplinks, and adds port members
- **FA Proxy advertises FA Management VLAN to FA Client AP** (in the FA Element TLV).
  - AP triggered to use tagged management and sends DHCP request tagged using mgmt VID.
- **FA Proxy detects FA Client AP & adds port membership to VID 50.**
  - Switch port tagging mode set to **Mix** (default - Untagged and Tagged).
- **AP sends DHCP discover tagged to FA Proxy**
- **AP gets IP address/DNS information and connects to ECA**

```
VSP-FA-Server:
(config)# interface gig 1/47
(config-if)# fa management i-sid 12990050 c-vid 50
(config-if)# fa enable
(config-if)# no fa message authentication
```

```
X450-G2-24p-10GE4:
Nothing to configure (unless in-band
management of switch is required)
```



1A: EXOS and AP with FA - Tagged Mgmt - Verify Operations



```
X450-G2-24p-10GE4: # show fabric attach elements
Fabric Attach Mode: Proxy
                                                     Mgmt     Auto
System Id                     Port    Type           VLAN Tag Provision
----------------------------- ------- -------------- ---- --- ------------
---
d8-84-66-8b-ea-22-00-00-00-00 16    WAP Type 1       50   Mix Disabled
92-00-72-43-00-ff-30-30-00-30 22    Server (No Auth) 50   Mix Disabled
```

```
VSP-FA-Server:1# show fa elements

================================================================
                        Fabric Attach Discovery Elements
================================================================
                         MGMT                                            ELEM ASGN
PORT   TYPE              VLAN STATE  SYSTEM ID                           AUTH AUTH
--------------------------------------------------------------------------------
--
1/47   proxyNoAuth       50   T / D  02:04:96:9e:a6:c0:00:01:00:32      NA   NA
```

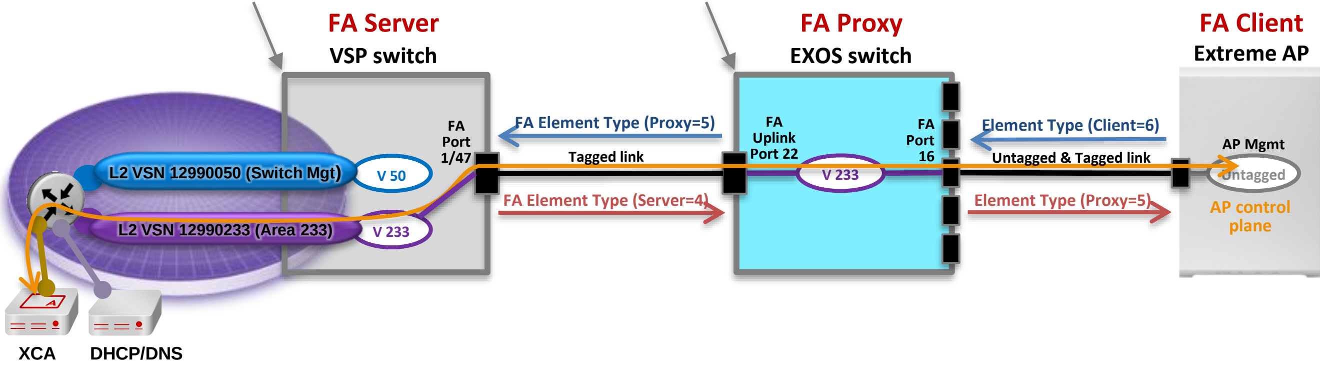
```
X450-G2-24p-10GE4: # show vlan
-----------------------------------------------------------------------------------------------
-
Name            VID  Protocol Addr       Flags                               Proto  Ports  Virtual
                                                                                    Active router
                                                                                    /Total
-----------------------------------------------------------------------------------------------
-
Default         1    --------------------------------T--------------    ANY    1 /20  VR-
Default
Mgmt            4095 -----------------------------------------------    ANY    1 /1   VR-Mgmt
SYS_VLAN_0050   50   ---------------------------------------d--------   ANY    2 /2   VR-
Default
-----------------------------------------------------------------------------------------------
-
```

1B: EXOS and AP with FA - Untagged Mgmt

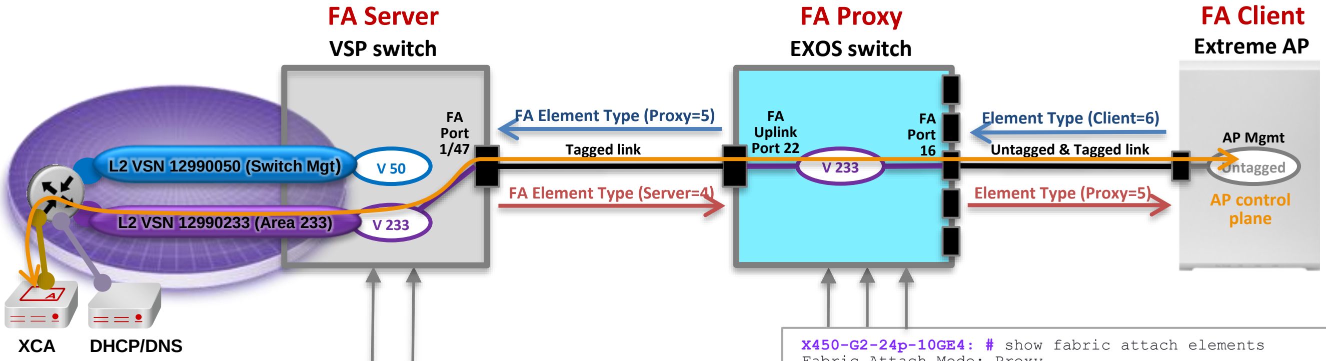
- **FA Server, FA Proxy and FA Client discover each other via LLDP Element TLVs.**
  - Disable FA message authentication on FA Server *(important ! EXOS will support Pre-shared key in 30.2).*
- **For AP management, configure a static VLAN/I-SID mapping on EXOS switch.**
  - VLAN/I-SID mapping is signaled upstream to FA server.
- **Add AP port to VLAN.**
- **FA Proxy sends AP an FA mgmt VID of "0", triggering AP to use untagged mgmt.**
  - Switch port tagging mode updated to **Mix** (default - Untagged and Tagged).
- **AP sends DHCP discover untagged to FA Proxy.**
- **AP gets IP address/DNS information and connects to ECA.**

```
VSP-FA-Server:
(config)# interface gig 1/47
(config-if)# fa enable
(config-if)# no fa message authentication
```

```
X450-G2-24p-10GE4:
# create vlan 233
# configure vlan 233 add port 16
# configure vlan 233 add isid 12990233
```



1B: EXOS and AP with FA - Untagged Mgmt – Verify Operations



```
VSP-FA-Server:#show fa elements

==================================================================================
                        Fabric Attach Discovery Elements
==================================================================================
                         MGMT                                         ELEM ASGN
PORT    TYPE             VLAN STATE   SYSTEM ID                       AUTH AUTH
----------------------------------------------------------------------------------
1/47    proxyNoAuth       0    T / D  02:04:96:9e:a6:c0:00:01:00:32   NA   NA
```

```
VSP-FA-Server:#show fa assignment

===============================================================================
                        Fabric Attach Assignment Map
===============================================================================
Interface  I-SID      Vlan       State      Origin
-------------------------------------------------------------------------------
1/47       12990233   233        active     proxy
```

```
X450-G2-24p-10GE4: # show fabric attach elements
Fabric Attach Mode: Proxy
                                                        Mgmt     Auto
System Id                      Port    Type             VLAN Tag Provision
------------------------------ ------- ---------------- ---- --- -----------
---
d8-84-66-8b-ea-22-00-00-00-00 16      WAP Type 1       None Mix Disabled
92-00-72-43-00-ff-30-30-00-30 22      Server (No Auth) None Mix Disabled
```

```
X450-G2-24p-10GE4: # show vlan
Untagged ports auto-move: Inform
-----------------------------------------------------------------------------------------------
-
Name            VID  Protocol Addr       Flags                         Proto  Ports  Virtual
                                                                              Active router
                                                                              /Total
-----------------------------------------------------------------------------------------------
-
Default         1    --------------------------------T--------------  ANY    1 /20 VR-Default
Mgmt            4095 ------------------------------------------------  ANY    1 /1   VR-Mgmt
VLAN_0233       233  ------------------------------------------------  ANY    2 /2   VR-
Default
                                                                              ----------------
```

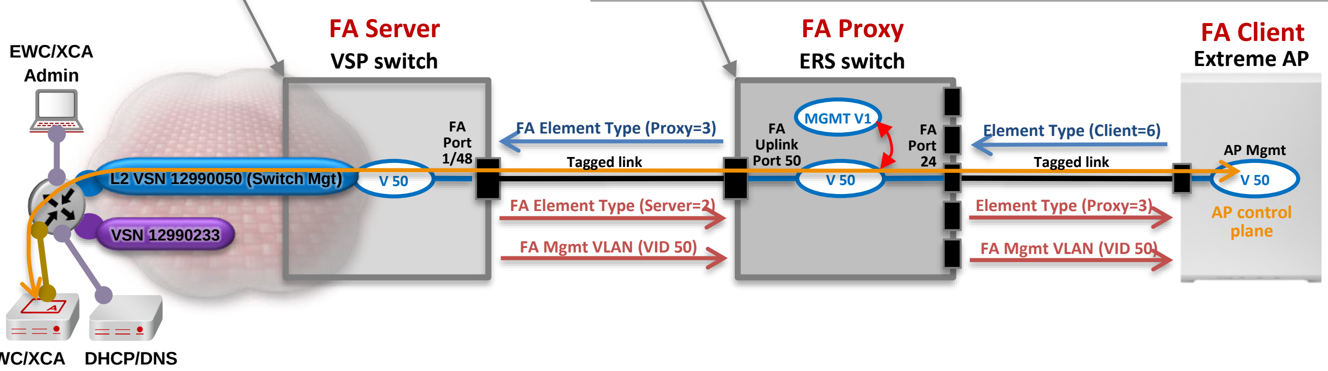
```
X450-G2-24p-10GE4: # show vlan fabric attach assignments
Fabric Attach Mode: Proxy
Port     VLAN  VLAN Name                         Type     ISID/NSI  Status
-------  ----  --------------------------------  -------  --------  -------
-
           233  VLAN_0233                         Static   12990233  Active
```

2A: ERS and AP with FA - Tagged Mgmt

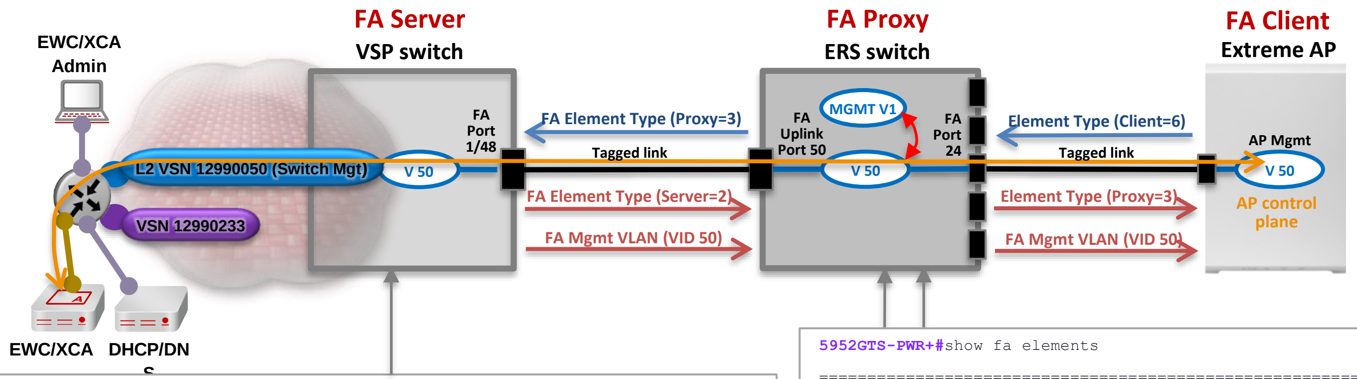
- **FA Server, FA Proxy and FA Client discover each other via LLDP element TLVs.**
- **FA Management VLAN 50 advertised to FA Proxy from FA Server.**
    - FA Proxy creates VLAN 50, makes it the Management VLAN, tags uplinks.
- **FA Proxy advertises FA Management VLAN to FA Client AP** (in the FA Element TLV).
    - AP triggered to use tagged management and sends DHCP request tagged using mgmt VID.
- **FA Client AP advertises Element type 6, FA Proxy detects & adds port membership to VID 50.**
    - Switch port tagging mode updated to **TagAll**.
- **AP sends DHCP discover tagged to FA Proxy.**
- **AP gets IP address/DNS information and connects to XCA/EWC.**

```
VSP4850GTS-PWR+:
(config)# interface gig 1/48
(config-if)# fa management i-sid 12990050 c-vid 50
(config-if)# fa enable
```

```
ERS5952GTSPWR+:
(config)# fa zero-touch-option auto-trusted-mode-fa-client client-type 6
(config)# fa zero-touch-option auto-pvid-mode-fa-client client-type 6
**existing switch Mgmt VLAN will dynamically change to FA mgmt VID**
```



2A: ERS and AP with FA - Tagged Mgmt – Verify Operations



```
VSP-FA-Server:#show fa elements

==================================================================================
                        Fabric Attach Discovery Elements
==================================================================================
                         MGMT                                        ELEM ASGN
PORT    TYPE             VLAN STATE   SYSTEM ID                      AUTH AUTH
----------------------------------------------------------------------------------
1/48    proxy             50    T / S   02:04:96:9e:a6:c0:00:01:00:32    AP    AP
```

```
5952GTS-PWR+#show fa elements

================================================================================
                       Fabric Attach Discovered Elements
================================================================================
UNIT/                      MGMT                                          ELEM ASGN
PORT    TYPE               VLAN  STATE   SYSTEM ID                       AUTH AUTH
--------------------------------------------------------------------------------
1/24    Client             0     T / D   d8:84:66:8b:ea:22:00:00:00:00    AP   AP
1/50    Server             50    T / S   92:00:72:43:00:ff:30:30:00:30    AP   AP

================================================================================
                      Fabric Attach Authentication Detail
================================================================================
UNIT/                                         ELEM OPER             ASGN OPER
PORT    EXPANDED TYPE                         AUTH STATUS           AUTH STATUS
--------------------------------------------------------------------------------
1/24    wap-type1                             successAuth           successAuth
1/50    Server (Auth)                         successAuth           successAuth
```

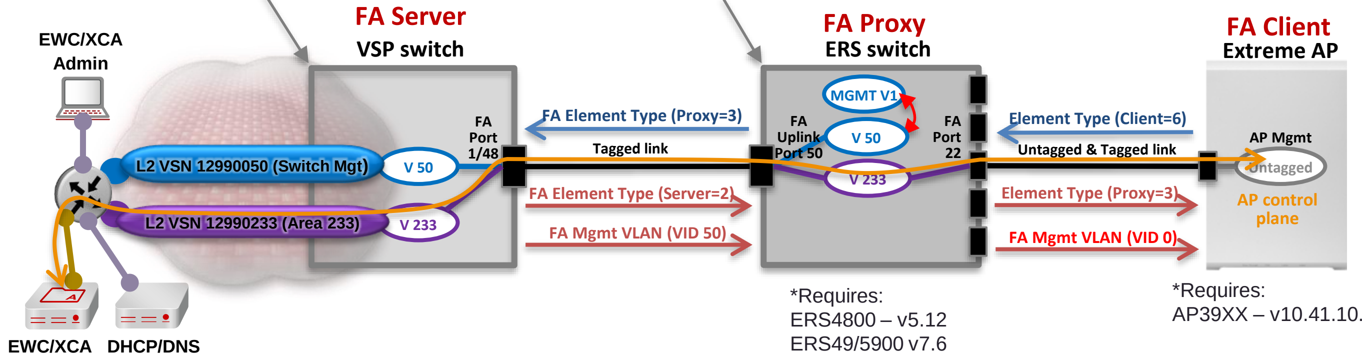
```
5952GTS-PWR+#show vlan interface info 24
      Filter     Filter
     Untagged Unregistered
Port  Frames     Frames      PVID PRI    Tagging      Name
---- -------- ------------ ---- --- ------------- ----------------
24   No         Yes          50    0    TagAll        Port 24
```

2B: ERS and AP with FA - Untagged Mgmt

- **FA Server, FA Proxy and FA Client discover each other via LLDP Element TLVs.**
- **FA Management VLAN 50 is advertised to FA Proxy from FA Server.**
  - FA Proxy makes VLAN 50 the management VLAN for switch management (linked to I-SID at FA Server).
- **For untagged AP management, configure FA Zero Touch Auto Client Attach on FA Proxy.**
  - Disable FA Management VLAN distribution
- **FA Proxy sends AP an FA mgmt VID of "0", triggering AP to use untagged mgmt.**
- **FA Client AP advertises Element type 6, FA Proxy detects & updates PVID and maps I-SID/VLAN.**
  - Switch port tagging mode updated to **UntagPvidOnly** (this = Untagged and Tagged / Mix).
- **AP sends DHCP discover untagged to FA Proxy.**
- **AP gets IP address/DNS information and connects to XCA/EWC.**

```
VSP4850GTS-PWR+:
(config)# interface gig 1/48
(config-if)# fa management i-sid 12990050 c-vid 50
(config-if)# fa enable
```

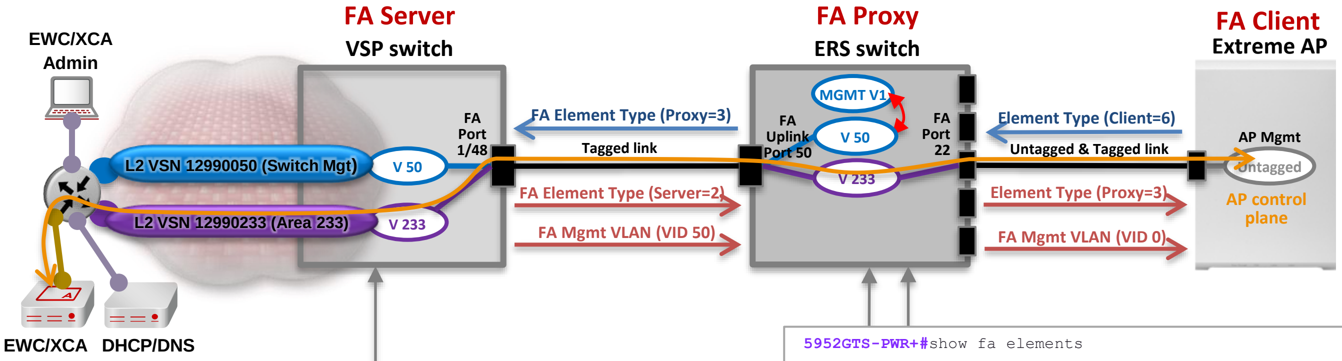
```
ERS5952GTSPWR+:
(config)# fa zero-touch disable-mgmt-vlan-distribution
(config)# fa zero-touch-option auto-client-attach client-type 6
(config)# fa zero-touch-option standard wap-type1 vlan 233 i-sid 12990233 pri 5
**existing switch Mgmt VLAN will still dynamically change to FA mgmt VID**
```



*Requires:
ERS4800 – v5.12
ERS49/5900 v7.6

*Requires:
AP39XX – v10.41.10.0016

2B: ERS and AP with FA - Untagged Mgmt – Verify Operations



```
VSP-FA-Server:#show fa elements

================================================================================
                       Fabric Attach Discovery Elements
================================================================================
                        MGMT                                 ELEM ASGN
PORT   TYPE             VLAN STATE  SYSTEM ID                AUTH AUTH
--------------------------------------------------------------------------------
1/48   proxy            50    T / S  02:04:96:9e:a6:c0:00:01:00:32   AP   AP
```

```
5952GTS-PWR+#show vlan
Id   Name                 Type    Protocol        PID    Active IVL/SVL Mgmt
---- -------------------- ------- --------------- ------ ------ ------- ----
1    VLAN #1              Port    none            0x0000 Yes    IVL     No
         Port members 29-52
50   VLAN #50             Port    none            0x0000 Yes    IVL     Yes
         Port Members 50
233  AP3912 EWC VID       Port    none            0x0000 Yes    IVL     No
         Port Members 22,50
Total VLANs: 3
```

```
5952GTS-PWR+#show fa elements

================================================================================
                       Fabric Attach Discovered Elements
================================================================================
UNIT/                       MGMT                                          ELEM ASGN
PORT    TYPE                VLAN  STATE  SYSTEM ID                        AUTH AUTH
--------------------------------------------------------------------------------
1/22    Client              0     T / D  d8:84:66:8b:ea:22:00:00:00:00     AP   AP
1/50    Server              50    T / S  92:00:72:43:00:ff:30:30:00:30     AP   AP

================================================================================
                      Fabric Attach Authentication Detail
================================================================================
UNIT/                                       ELEM OPER            ASGN OPER
PORT   EXPANDED TYPE                        AUTH STATUS          AUTH STATUS
--------------------------------------------------------------------------------
1/22   wap-type1                            successAuth          successAuth
1/50   Server (Auth)                        successAuth          successAuth
```

```
5952GTS-PWR+#show vlan interface info 22
      Filter     Filter
     Untagged Unregistered
Port  Frames     Frames    PVID PRI    Tagging     Name
---- -------- ------------ ---- --- ------------- ----------------
22   No       Yes          233  5   UntagPvidOnly Port 22
```

Extreme™

Customer-Driven Networking

WWW.EXTREMENETWORKS.COM