atmosphere'22 MEETUP

Streamline Operations and Enhance Protection with

Aruba Central NetConductor

aruba
a Hewlett Packard Enterprise company

Agenda

1. Problem statement: Why NetConductor?
2. Overlay Technology Review
3. Aruba NetConductor Overview
4. Aruba NetConductor Personas
5. Aruba NetConductor Demo

The Problem Statement

Customer Challenges

Lack of Visibility

- Rapid adoption of a wide variety and volume of IoT devices
- Expanding cyber attack surface leading to security blind spots

Lack of Automation

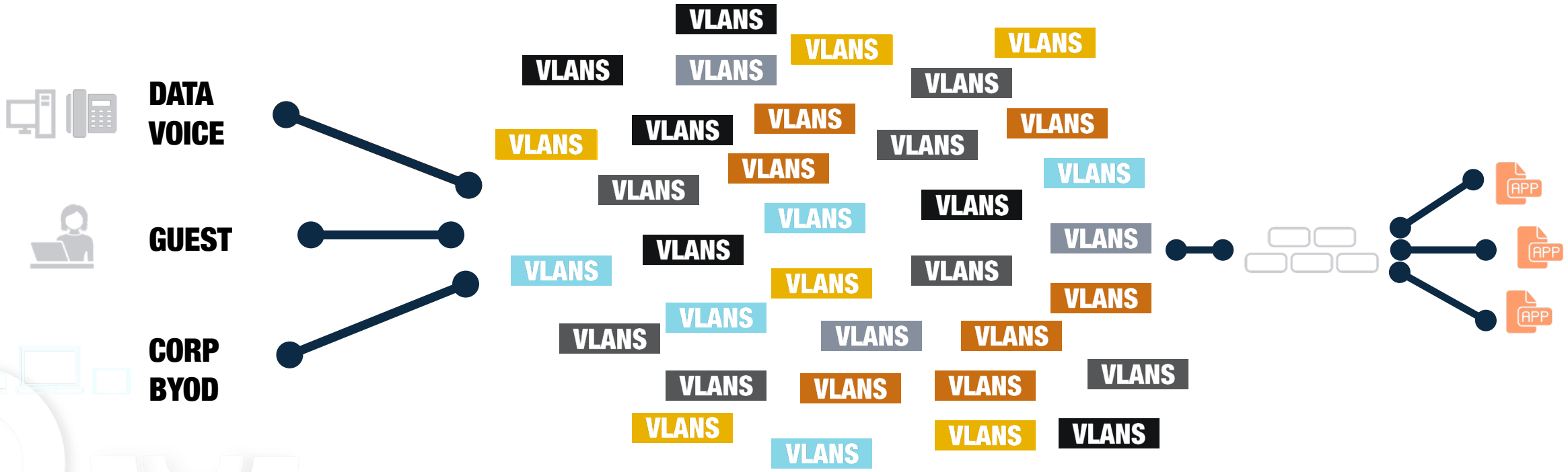
- Static VLAN-based approaches are error-prone and inadequate
- Add-move-changes require extensive reconfiguration, impacting IT productivity

Lack of Scale and Agility

- Increasingly complex networks, inconsistent user experience
- Deploying new architectures requires infrastructure rip-and-replace

“VLANs are COOL!”*

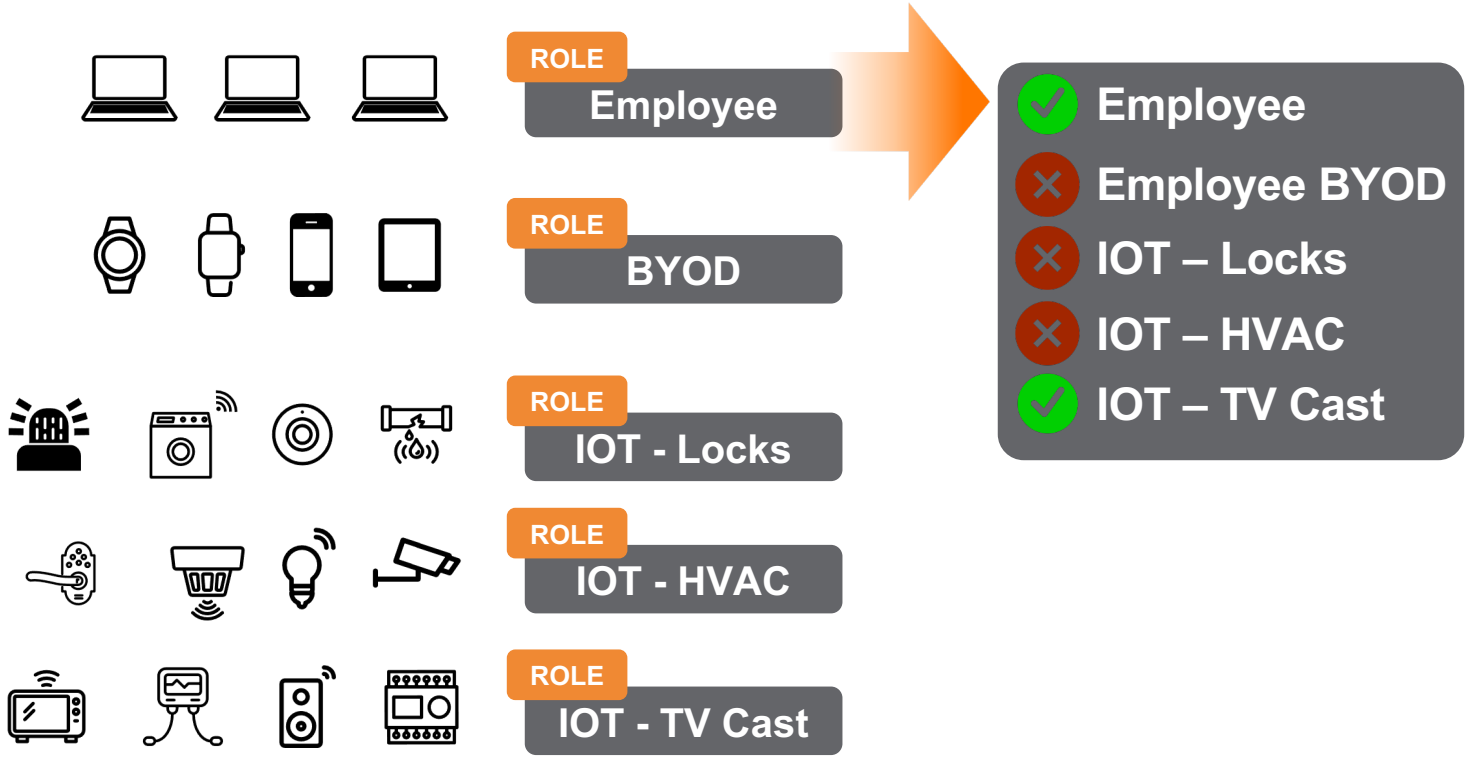
– IT Manager circa 1998*



- Complex and inefficient
- Extensive static, manual configuration
- Leads to VLAN sprawl and poor IPAM usage

If you remember nothing else…

THE ARUBA USER ROLE



DYNAMIC SEGMENTATION

Software defined approach eliminates VLAN sprawl and simplifies policy implementation

Delivers wired, wireless, and SD-WAN micro-segmentation needed for securing end-user and IoT devices

Aruba User Roles are COOL!*

– Seth Fiermonti circa 2011*

What Are User-Roles

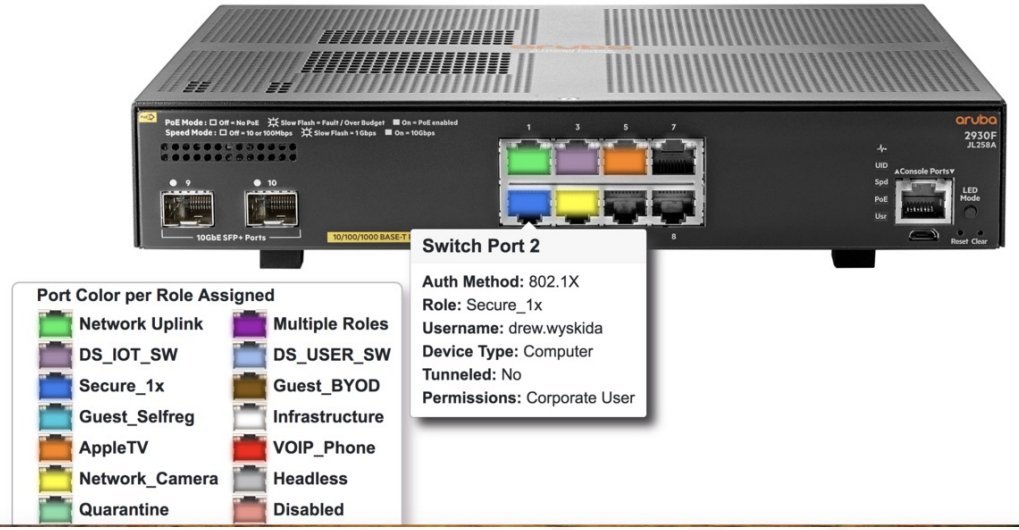
- A simple container for policy and security
  - VLAN, overlay/underlay path, QoS, Rate Limiters, MTU, POE priority, STP port settings
- *Have existed for ~20 years in Aruba products. If you're on an Aruba AP, you're using user roles!*

How to Apply User-Roles

- User-Roles are applied dynamically once a device authenticates with any AAA method.
- Can be applied with a device profile.
- Can be dynamically or statically applied.

Benefits

- Apply policy based on role configuration
- No need to preconfigure access ports - ACLs, rate limiters, QoS, etc.
- Associated to the <u>client</u> not the physical port.

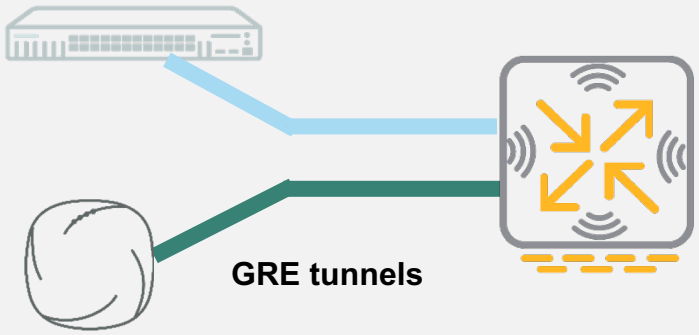



```
aaa authentication port-access dot1x authenticator
    radius server-group ClearPass
    enable

aaa authentication port-access mac-auth
    radius server-group ClearPass
    enable

interface 1/1/1-1/1/48
    aaa authentication port-access dot1x authenticator
        max-eapol-requests 1
        max-retries 1
        enable
    aaa authentication port-access mac-auth
        enable
```

Centralized or Distributed Overlays

two choices for policy enforcement

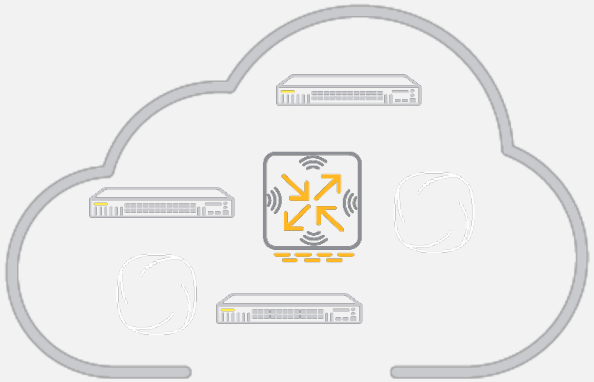
CENTRALIZED POLICY ENFORCEMENT



Enforcement Done at Gateways

User Based Tunneling with Aruba Gateways

DISTRIBUTED POLICY ENFORCEMENT



Enforcement at Ingress and Egress

Aruba Central NetConductor

- ✓ Simple and easy to deploy
- ✓ Consistent experience across wired & wireless
- ✓ Enhanced security features

- ✓ Open & multi-vendor ready
- ✓ Higher scale and performance
- ✓ Consistent operations across campus & data center

Achieving Zero Trust

Leverage existing constructs for new outcomes

Understand Traffic Flows

Custom Fingerprinting

Automatic Device Grouping

Ubiquitous and comprehensive telemetry

Visibility

Context Share

Leverage Security Partnerships

More endpoint data == better security

Bi-directional sharing from ClearPass to Security Partners

Dynamic enforcement to the network

One Role, One Network

Wired, Wireless and Remote Access

User Roles == policy

Enhance AAA with visibility

Authentication

Enforcement

Policy Enforcement Options

Centralized and/or Distributed

Policy bound to the user not the SSID/port

EVPN-VXLAN Technology Review

EVPN-VXLAN

Two separate but linked technologies

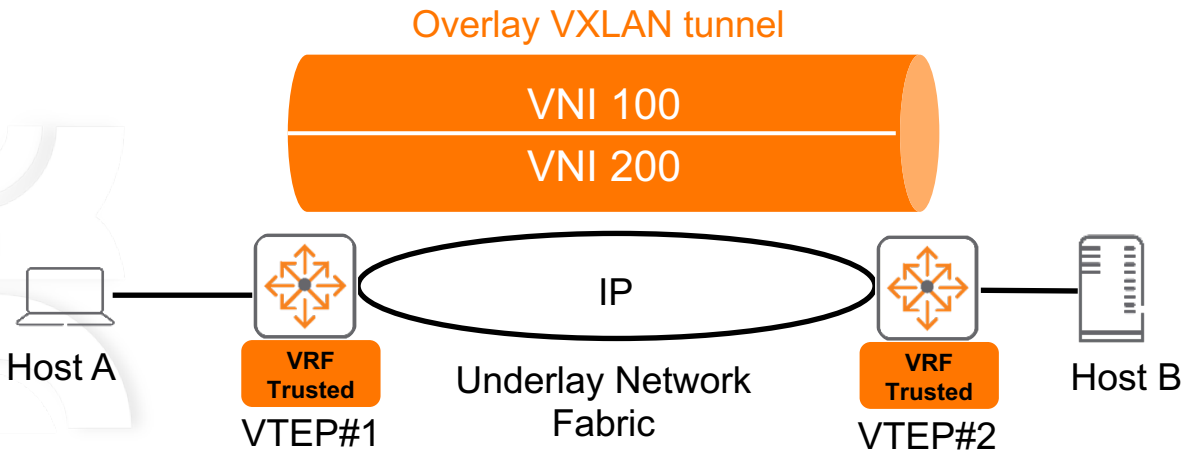
- Data plane
- Encapsulation of L2 frames in UDP packets
- Header carries VNI & GPID

EVPN-VXLAN

- Control Plane
- Uses BGP to communicate MAC reachability across a fabric
  - EVPN Type 2 messages communicate /32 route w/ MAC

VXLAN and Overlay Networking

- VXLAN encapsulation supports up to 16 million VXLAN Network Identifiers (VNIs) or virtual networks.
- VXLAN overlay tunnels should be created over a resilient routed IP underlay network fabric.
- VXLAN Tunnel End Point (VTEP) runs on switches in the fabric to terminate tunnels and enforce policy.
- A single VXLAN VTEP can support multiple VNIs.
- The collection of VNIs and VTEPs represent a virtual network overlay often referred to as an overlay "fabric".
- Routers/Switches in the IP underlay network do not need to understand VXLAN, they only need to forward IP/UDP jumbo frame traffic between VTEPs
- **It's still just a VLAN at the end of the day!**




```
interface vxlan 1
    source ip 10.10.10.53
    no shutdown
    vni 100
        vlan 100
    vni 200
        vlan 200
    vni 10011
        vrf Trusted
        routing
```

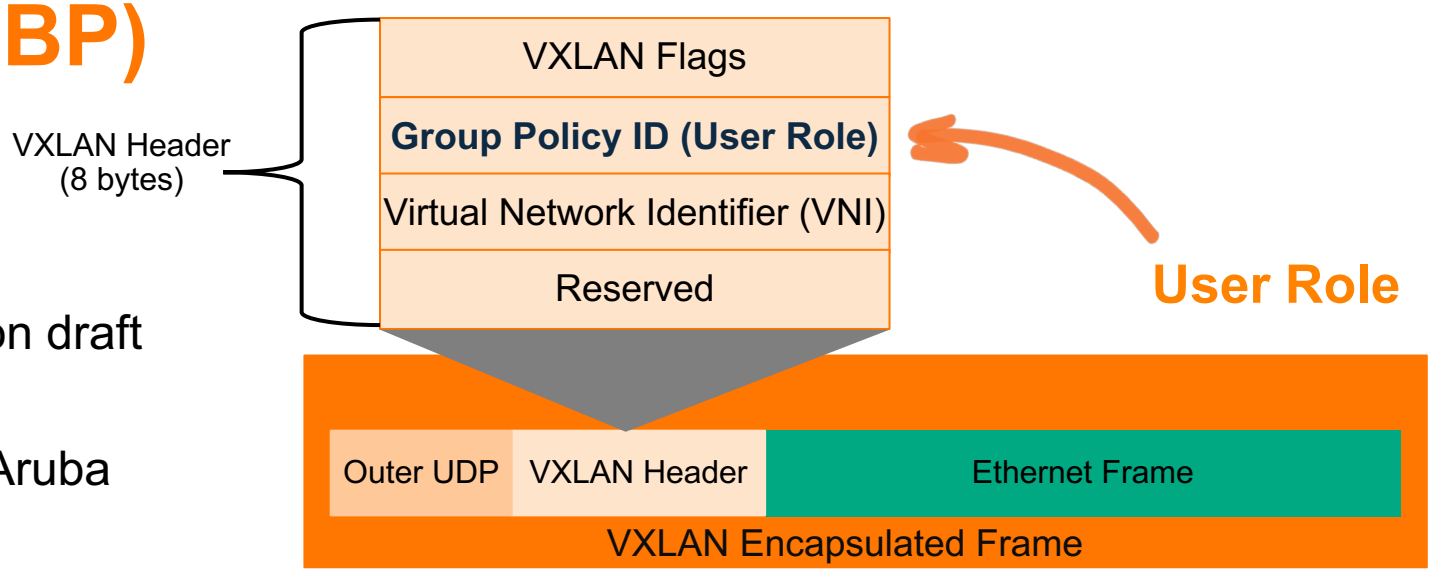
Micro-Segmentation with Group-Based Policy (GBP)

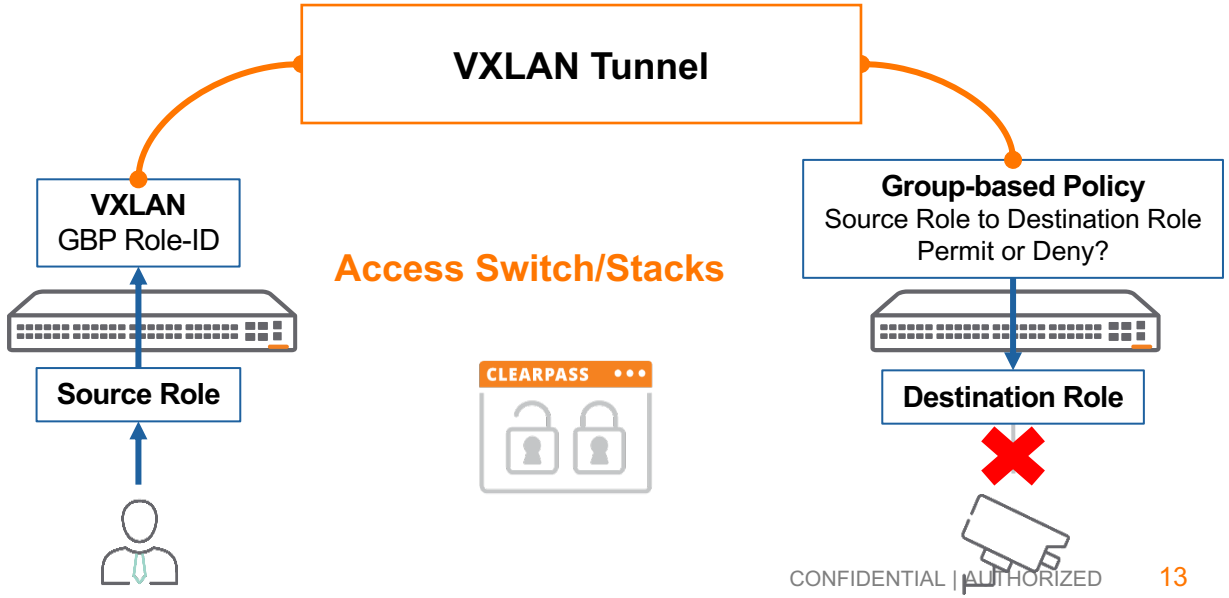
VXLAN-GBP

- Extension of the VXLAN header (based on draft IETF standard).
- Transports a GPID which is used as the Aruba ROLE-ID.
- Allows for end-to-end, role-to-role policy enforcement within an enterprise fabric.

Use Cases

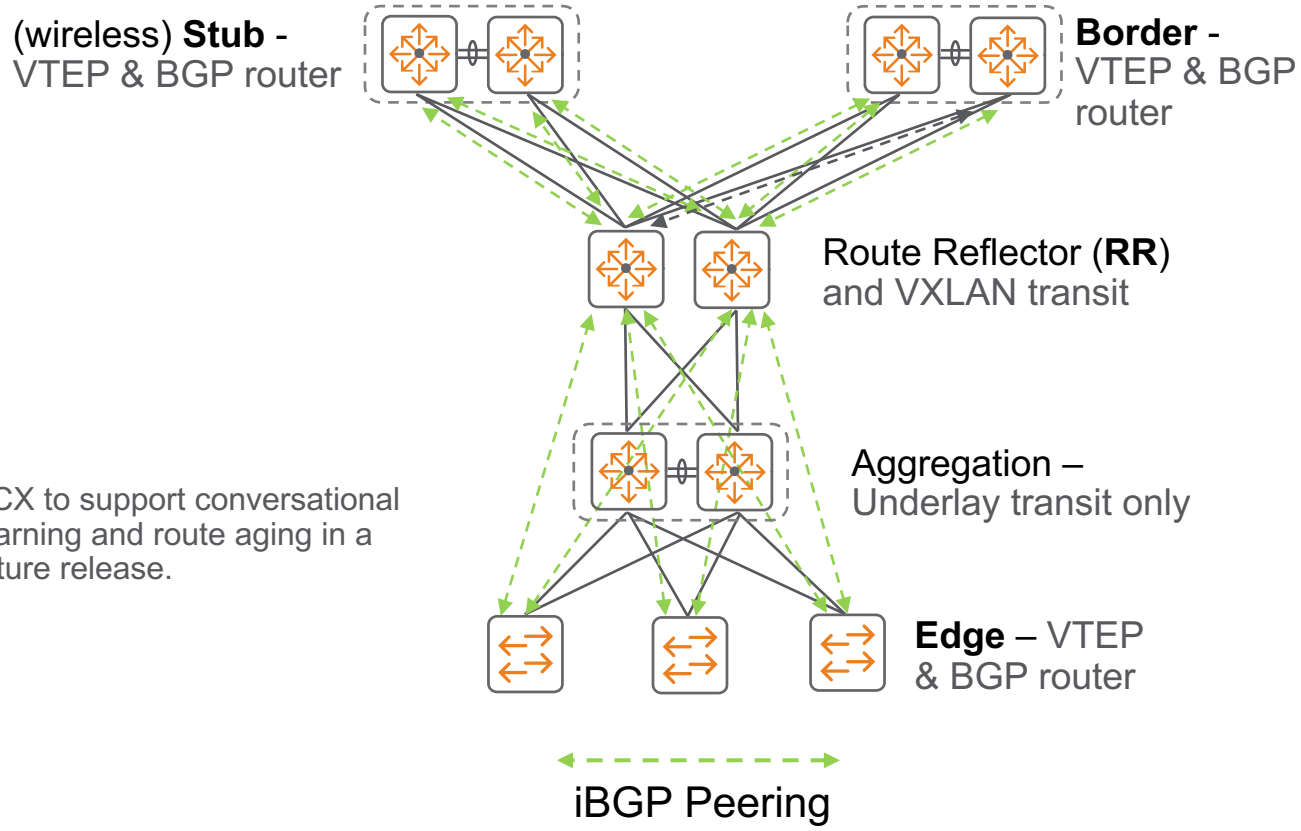
- IoT device protection
- Guest management
- Intra-VLAN/segment granular isolation between users/devices





EVPN Control Plane

- EVPN is an MP-BGP address family that communicates endpoint reachability across a fabric.
  - No flood and learn
- BGP route reflectors enable simplified configuration with fewer required peering sessions.



* CX to support conversational learning and route aging in a future release.

https://tools.ietf.org/html/rfc7432

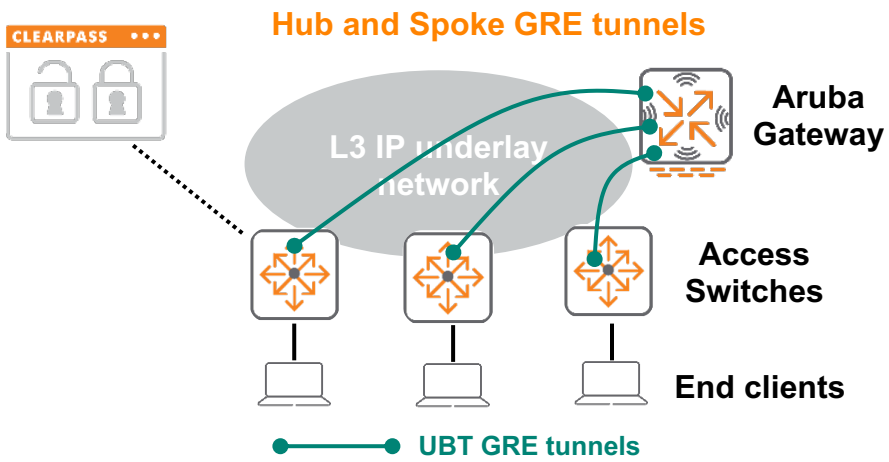
```
router bgp 65001
    bgp router-id 10.10.10.23
    neighbor Fabric01 peer-group
    neighbor Fabric01 remote-as 65001
    neighbor Fabric01 fall-over
    neighbor Fabric01 update-source loopback 0
    neighbor 10.10.10.1 peer-group Fabric01
    neighbor 10.10.10.2 peer-group Fabric01
    address-family l2vpn evpn
        neighbor 10.10.10.1 activate
        neighbor 10.10.10.1 send-community extended
        neighbor 10.10.10.2 activate
        neighbor 10.10.10.2 send-community extended
    exit-address-family
```

Why is EVPN-VXLAN important?

- VXLAN virtualizes layer 2 broadcast domains so they can be carried over layer 3 topologies.
  - VXLAN makes layer 2 more efficient and enterprise friendly, allowing broadcast domains to appear anywhere in the campus.
- VXLAN increases flexibility and reliability of segmentation and multi-tenancy in the network.
  - VXLAN-Group Based Policy (GBP) enables a group ID to be carried in the header of every frame for policy enforcement anywhere in the network.
- EVPN provides MAC reachability information in the form of /32 routes communicated over iBGP peering.
  - ARP and ND broadcasts are not propagated beyond the originating host and SVI.

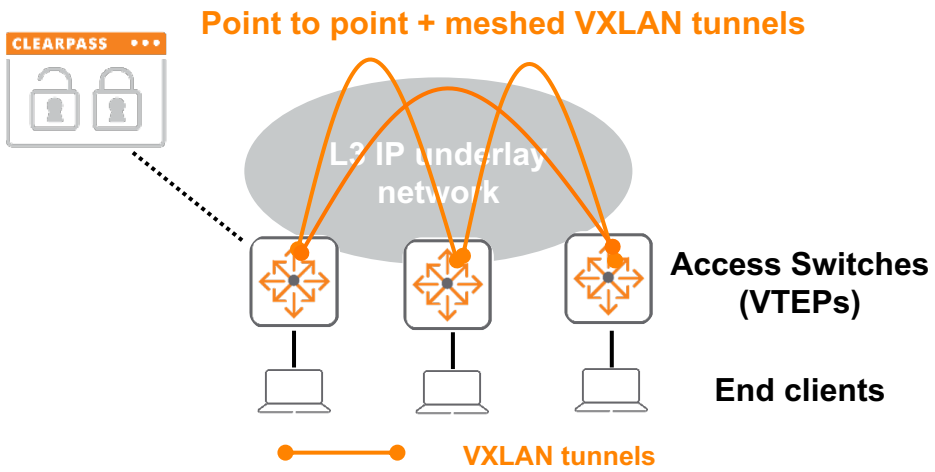
User Based Tunneling (UBT)

Expensive traffic engineering



Campus LAN VXLAN-EVPN Fabric

L2 Tunnels with a standards-based control plane



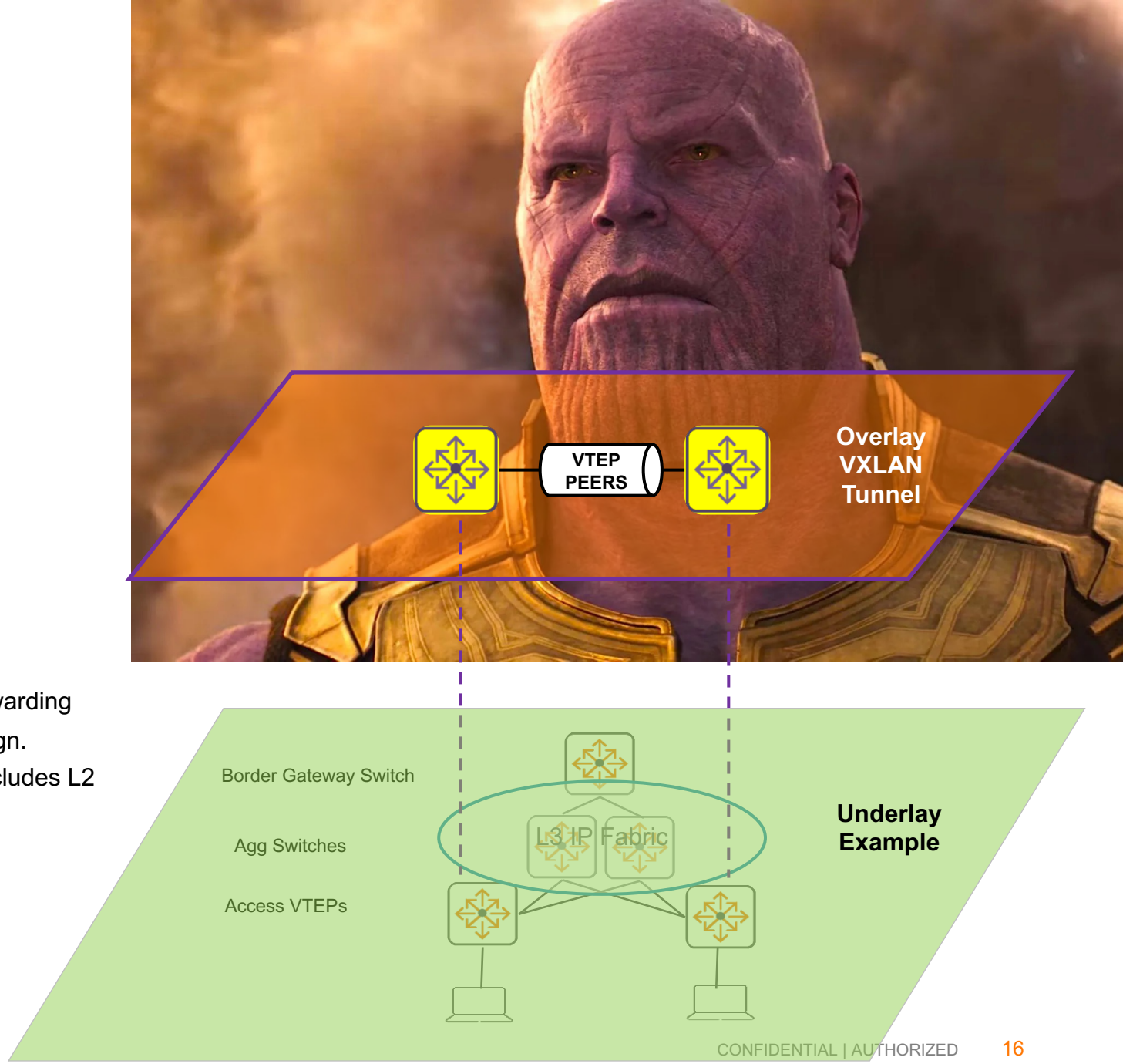
The End Game

In the Overlay

- Provisioning agility – Virtual networks segments can be created quickly/easily between VTEPs
- VXLAN leverages multiple equal cost paths in the underlay – no passive uplinks
- Host and client mobility
- Efficient data plane with broadcast and ARP traffic

In the Underlay

- A distributed/high performance, scalable and simple network
- Failure of single link/switch should not impact VXLAN tunnel forwarding
- No Spanning Tree Protocol (STP) – Due to routed underlay design.
- Loop free, multi-pathing network – VXLAN protocol inherently includes L2 loop avoidance

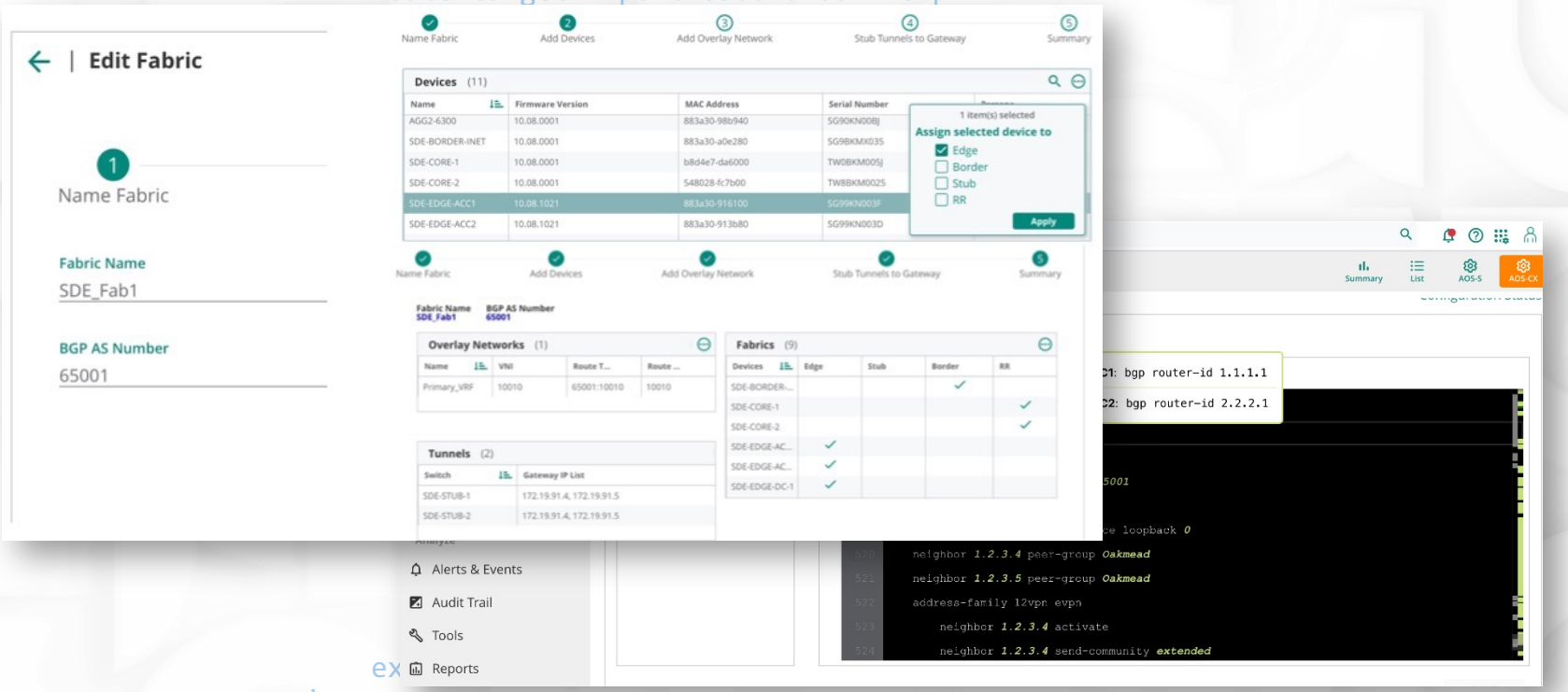


What is Aruba Central NetConductor?!

Aruba Central NetConductor

Aruba Central NetConductor (ACN) is an automation workflow which resides on Central and simplifies the deployment of an **EVPN-VXLAN fabric** on Aruba CX switching and wireless platforms and orchestrates **micro-segmentation** policies.

```
vrf Trusted
    rd 10.10.10.23:10011
    route-target export 65001:10011 evpn
    route-target import 65001:10011 evpn
```



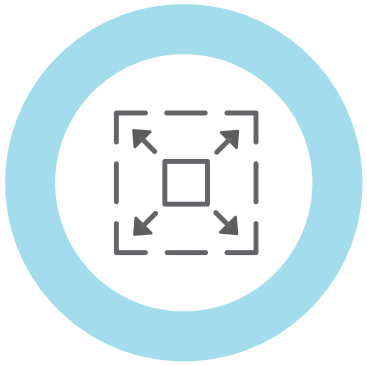

```
ex
!
vrf Trusted
    address-family ipv4 unicast
        redistribute connected
    exit-address-family
```

Aruba Central NetConductor

- ✓ Enhancement of Dynamic Segmentation for scale and performance
- ✓ Cloud-native network & security services
- ✓ Overlay-based (EVPN-VXLAN) automation with intent-based workflows
- ✓ ‘Inline’ policy enforcement by CX switches and AOS 10 gateways
- ✓ Flexible migration and investment protection

Cloud-Native Single Pane of Glass

Zero Trust & SASE Security with Role-Based Policies



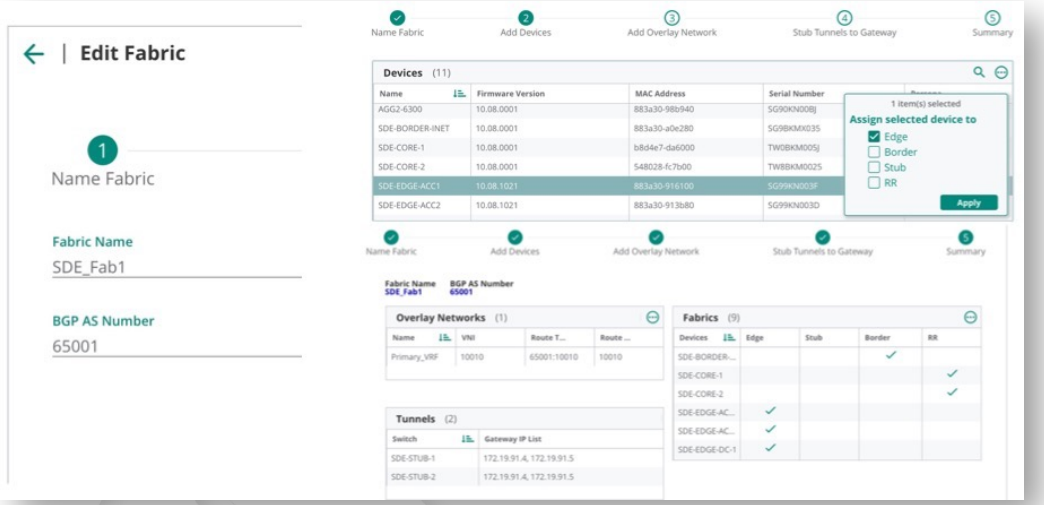
Flexible and Scalable Networks

Aruba Central NetConductor Fabric Wizard

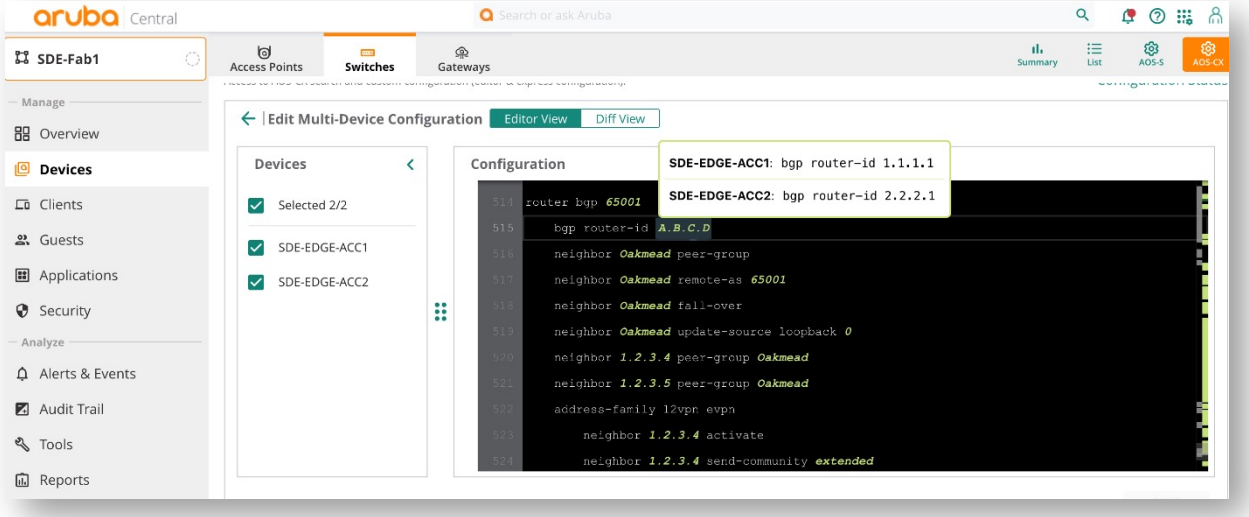
- A new Aruba Central Service.
- Graphical UI that uses assigned personas and connection topology to define VXLAN components.
- CLI is automatically generated and pushed to switches and gateways.

User Role (AOS-CX)

- Policy ID
- Ingress user policy
- Captive portal profile
- Inactivity timeout
- Reauth period
- Vlan access
- Vlan trunk
- Auth mode
- Poe priority
- MTU
- Vlan trunk allowed
- Trust mode

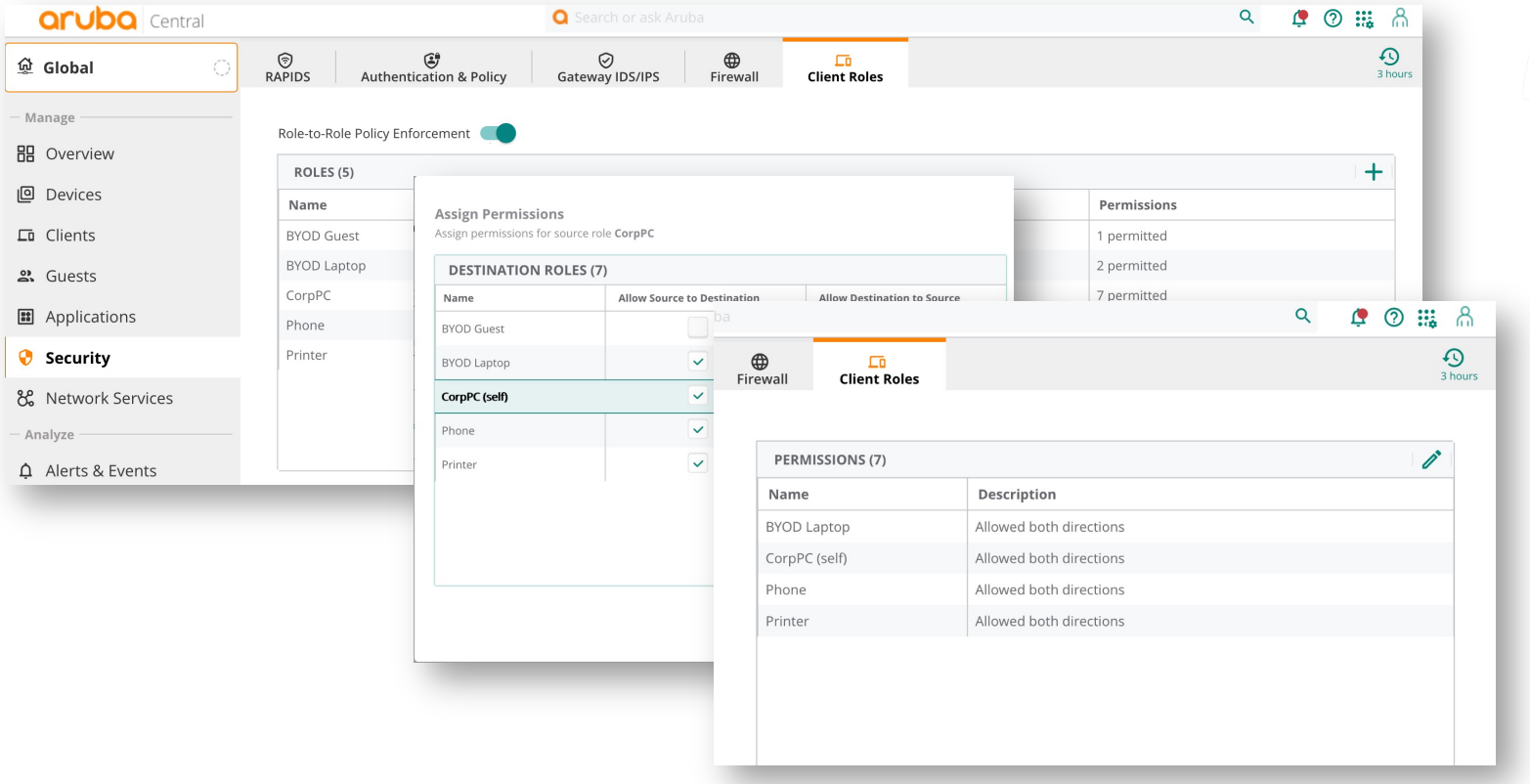


UI Driven Workflows



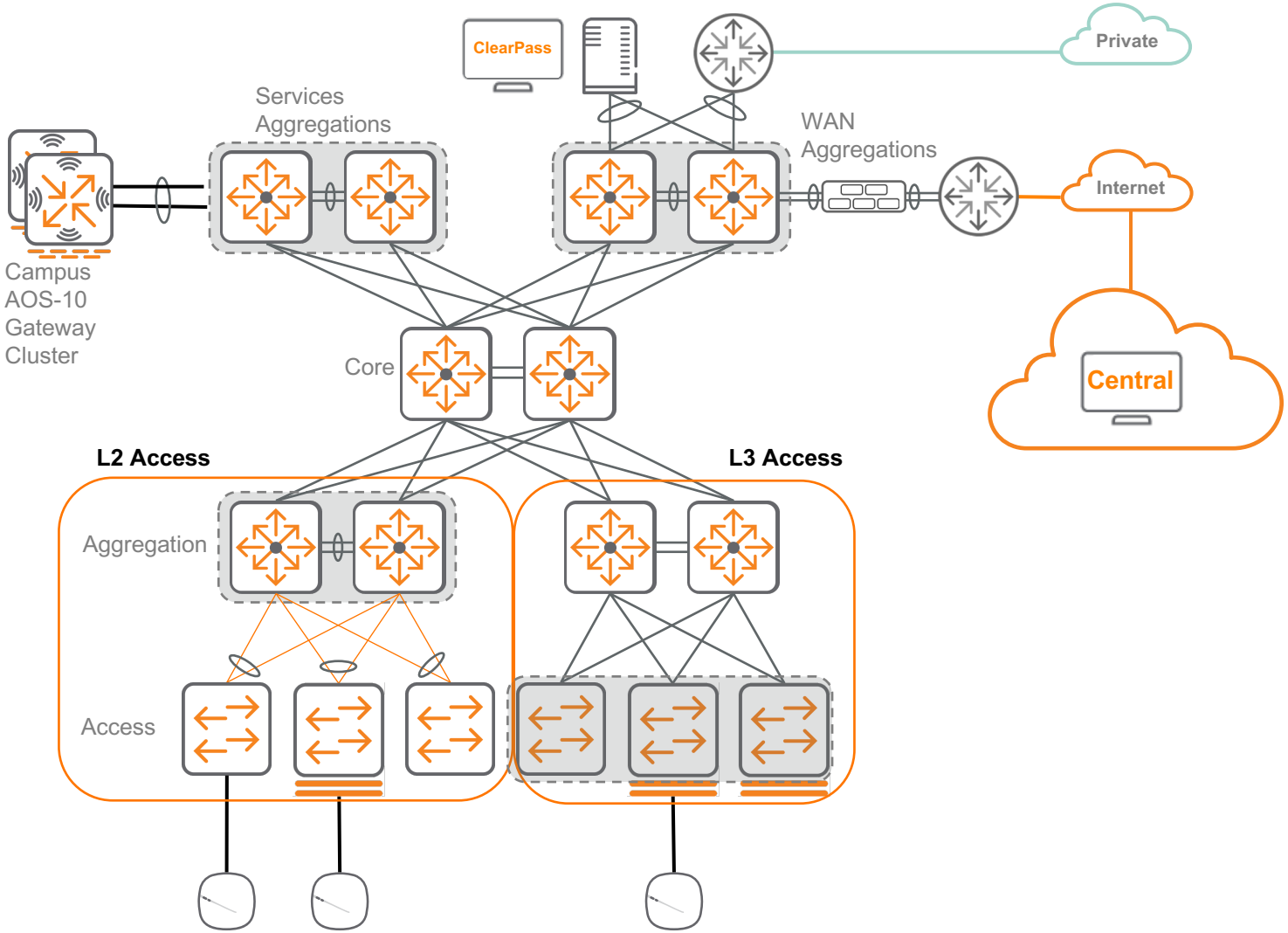
Resultant CLI Configs

Aruba Central NetConductor Policy Manager



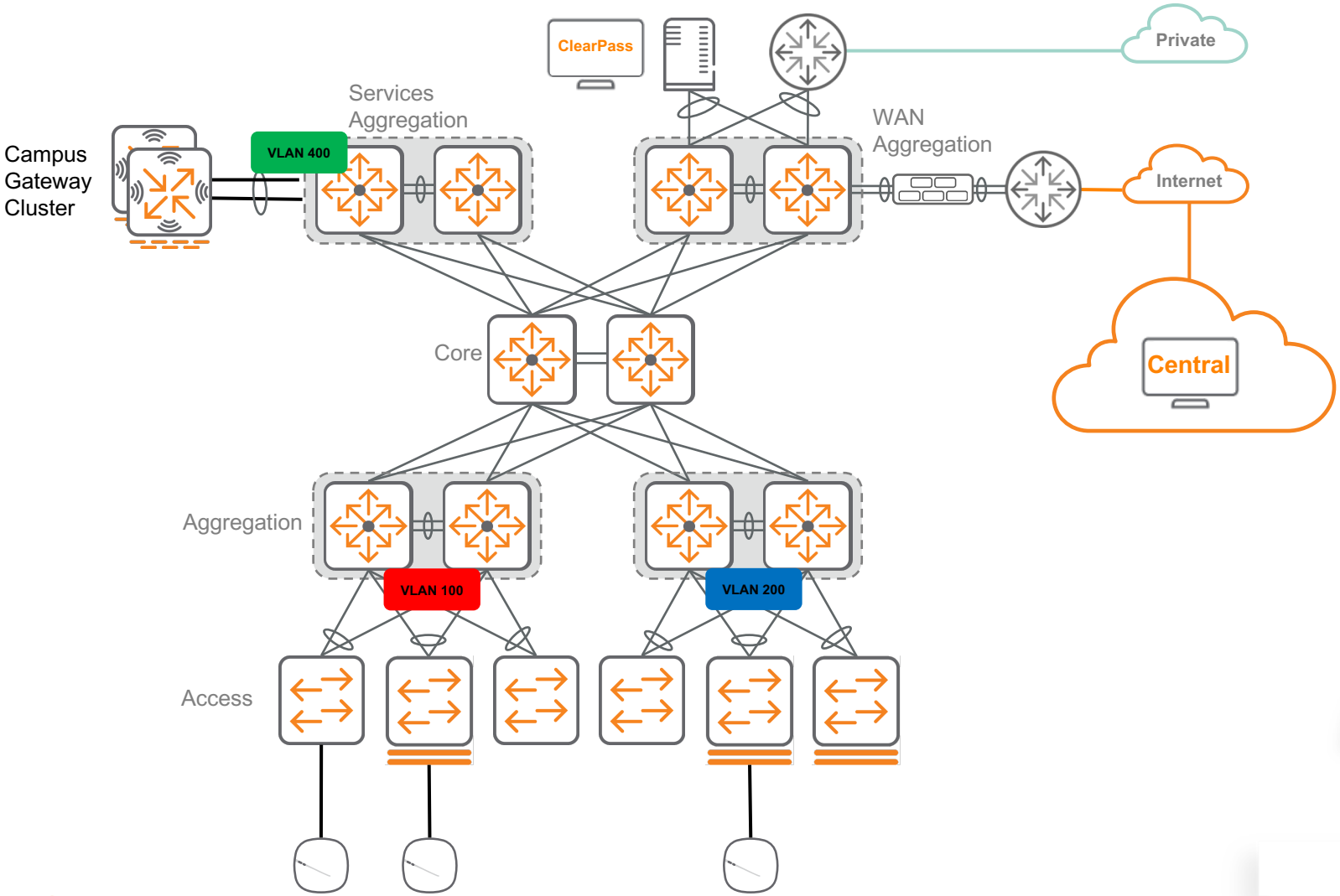
- A new Aruba Central Service.
- A simple UI to define both roles and access control policies.
- Single interface for all Role Based policies across wired, wireless and WAN.
- Can be used with or without a fabric
- Polices can be enforced across a 3rd party WAN
- … and MUCH more to come!!!

NetConductor Supports a Flexible Underlay



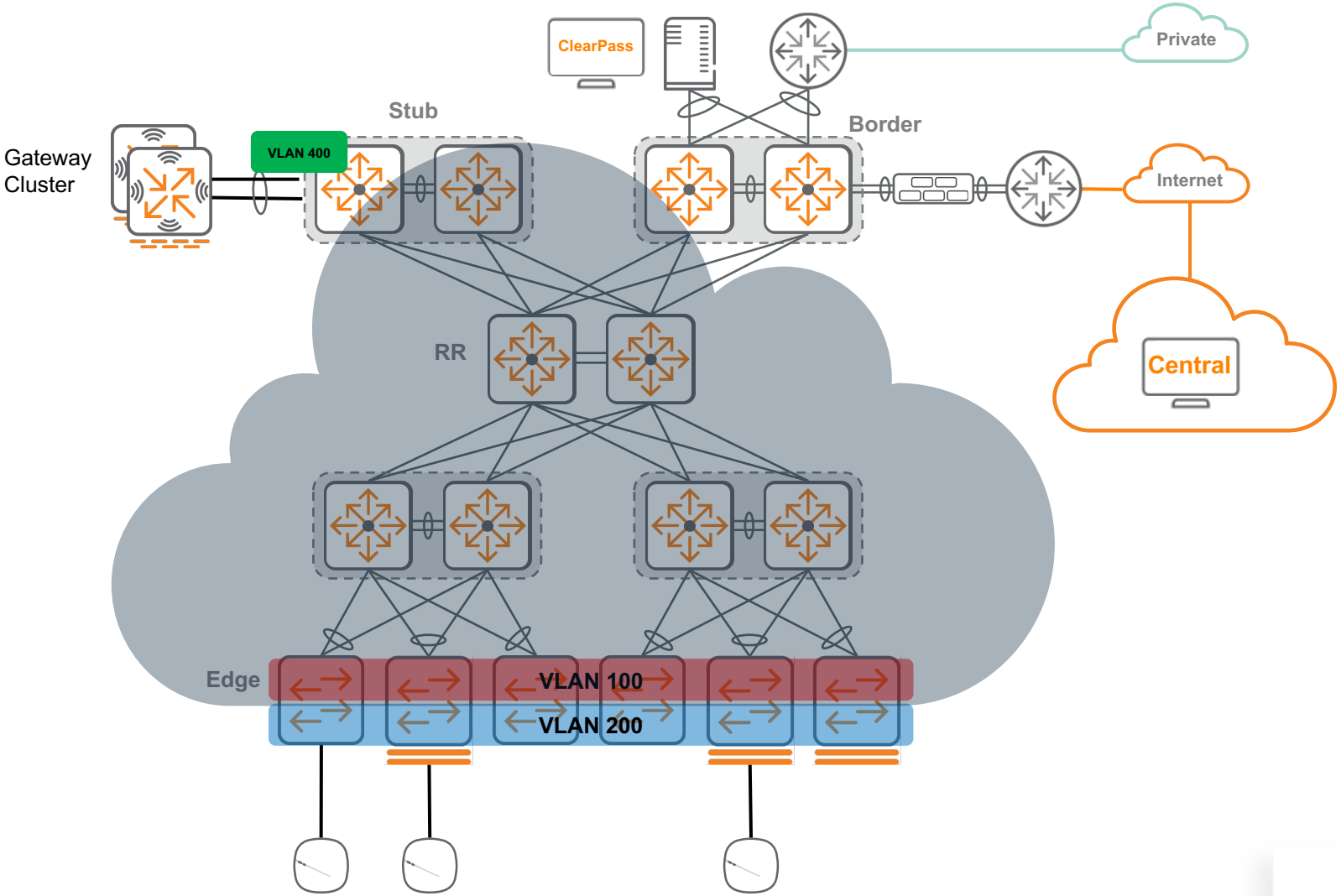
- A NetConductor fabric works with any IP underlay.
  - Use an L3 mesh and ECMP routing for maximum resiliency.
- Works with brownfield deployments.
  - Start with L2 access, migrate to L3.
- Devices participating in the overlay must have loopback reachability.
  - OSPF is necessary to the edge.
- Underlay must support Jumbo frames.

WHY use NetConductor?
Segment Design - Traditional



- VLANs are rigid and typically limited to an aggregation block.
- Granular security policy results in increasing numbers of VLANs.
- Policy is bound to the VLAN.
- VLAN quantity is limited to 4094.
- Limited options to provide L2 between access blocks.
  - IoT and other use cases require larger broadcast domains.

WHY use NetConductor?
Segment Design - Fabric

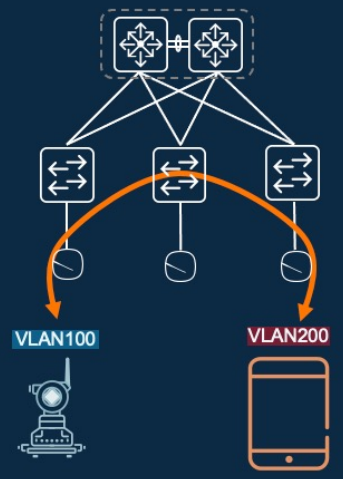


- Decouples policy from VLAN.
- L2 domains can be efficiently stretched across the underlay.
- VNI quantity is 16million.
- Simplified IP subnet Design
- Provides Active-Gateway for distributed default-gateway service.
  - Reduced latency for Inter-VLAN traffic.
  - MAC/ARP scale is distributed across Edge switches.
  - Reduced blast radius during failures or maintenance.

Aruba Makes a Fabric Better

Active Gateways

- Auto-created with overlay VLANs using ACN

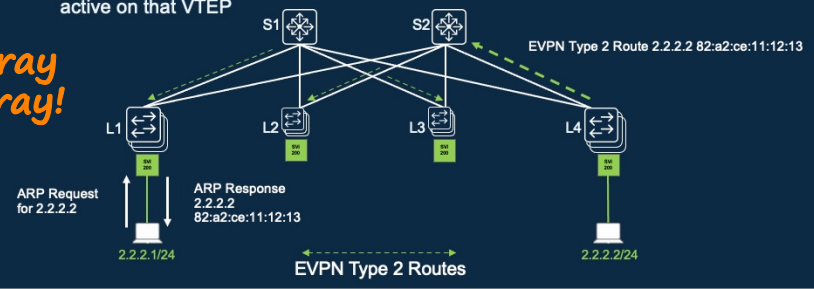


A Single-ish default gateway is so "legacy"

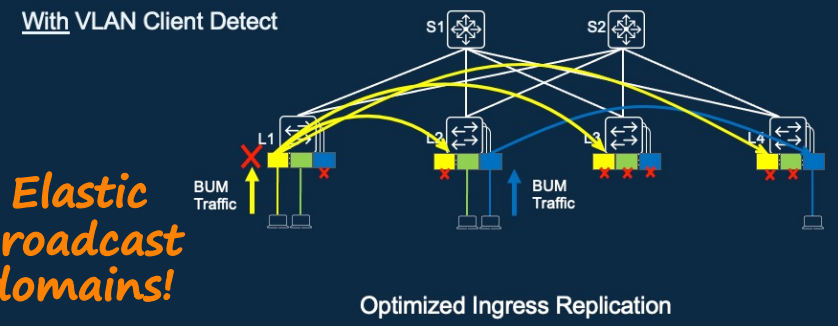
VXLAN ARP/ND Suppression

- When there is traffic from an endpoint, the source VTEP will discover the MAC/IP of the endpoint
- MAC/IP of the endpoint is shared with other VTEPs using EVPN Type 2 routes
- All VTEPs should have MAC/IP info for all endpoints in a given VLAN if that VLAN is active on that VTEP

No spray and pray!



Colorless Ports and EVPN-VXLAN Fabric

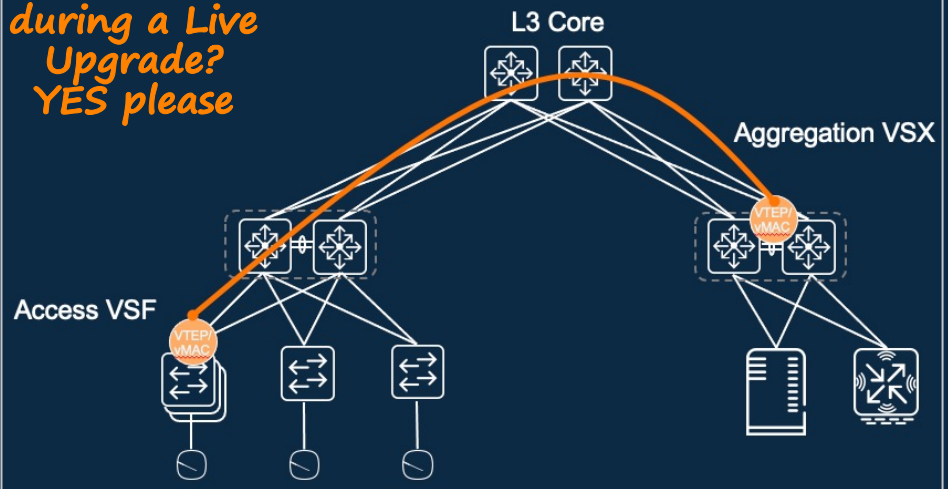


Elastic broadcast domains!

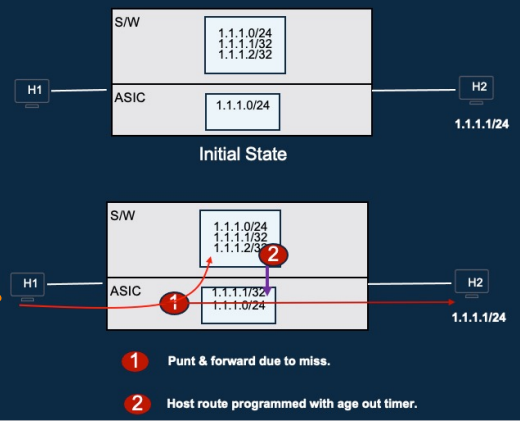
VTEP Survivability

- Virtual MAC on VSX and VSF

Overlay remains UP during a Live Upgrade? YES please



Distributed L3 Gateway FIB Optimization - Solution



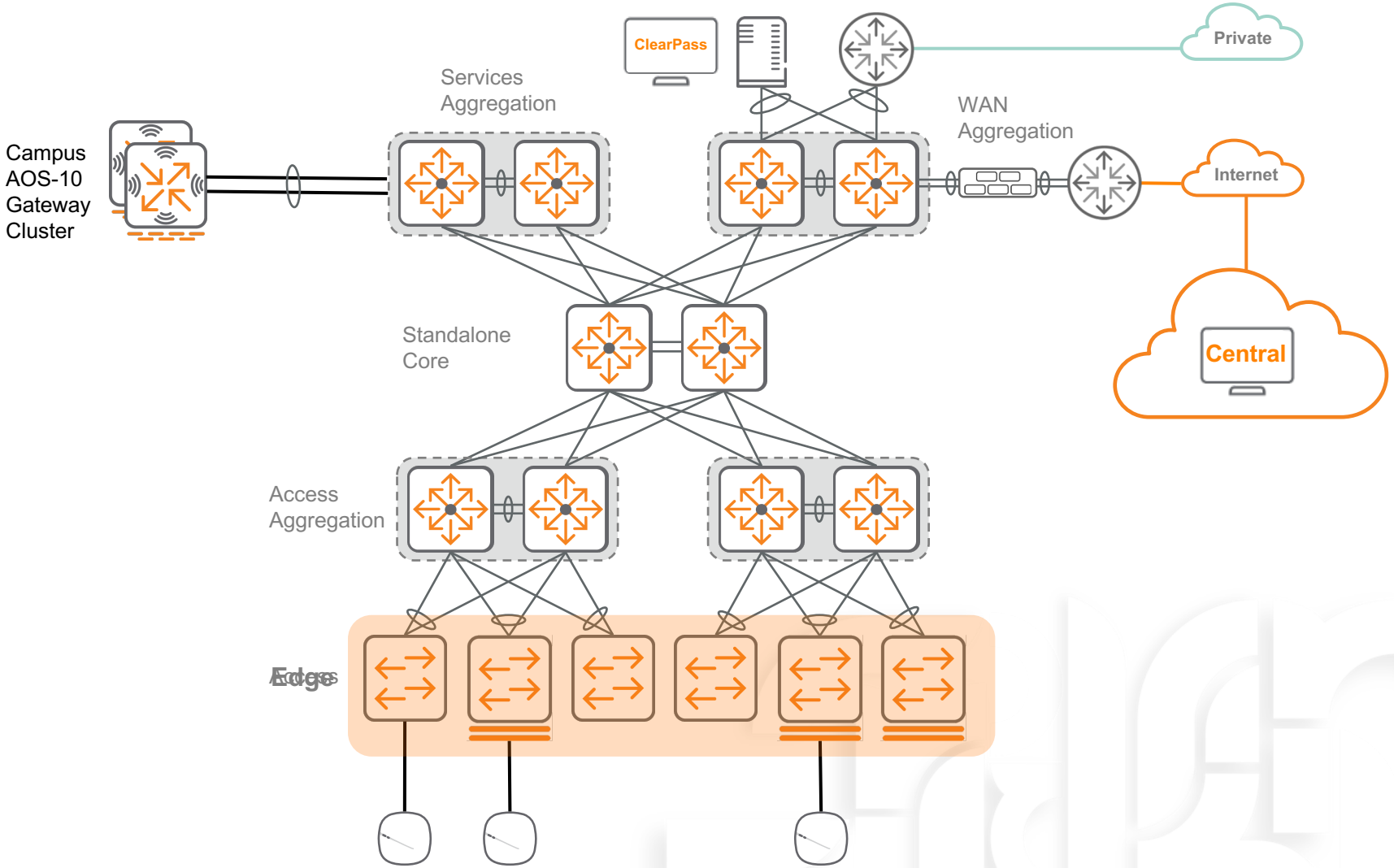
Enables Access layer platforms with lower hardware route scale to operate efficiently in large Campus fabrics

Smarter TCAM!

ACN Fabric Personas

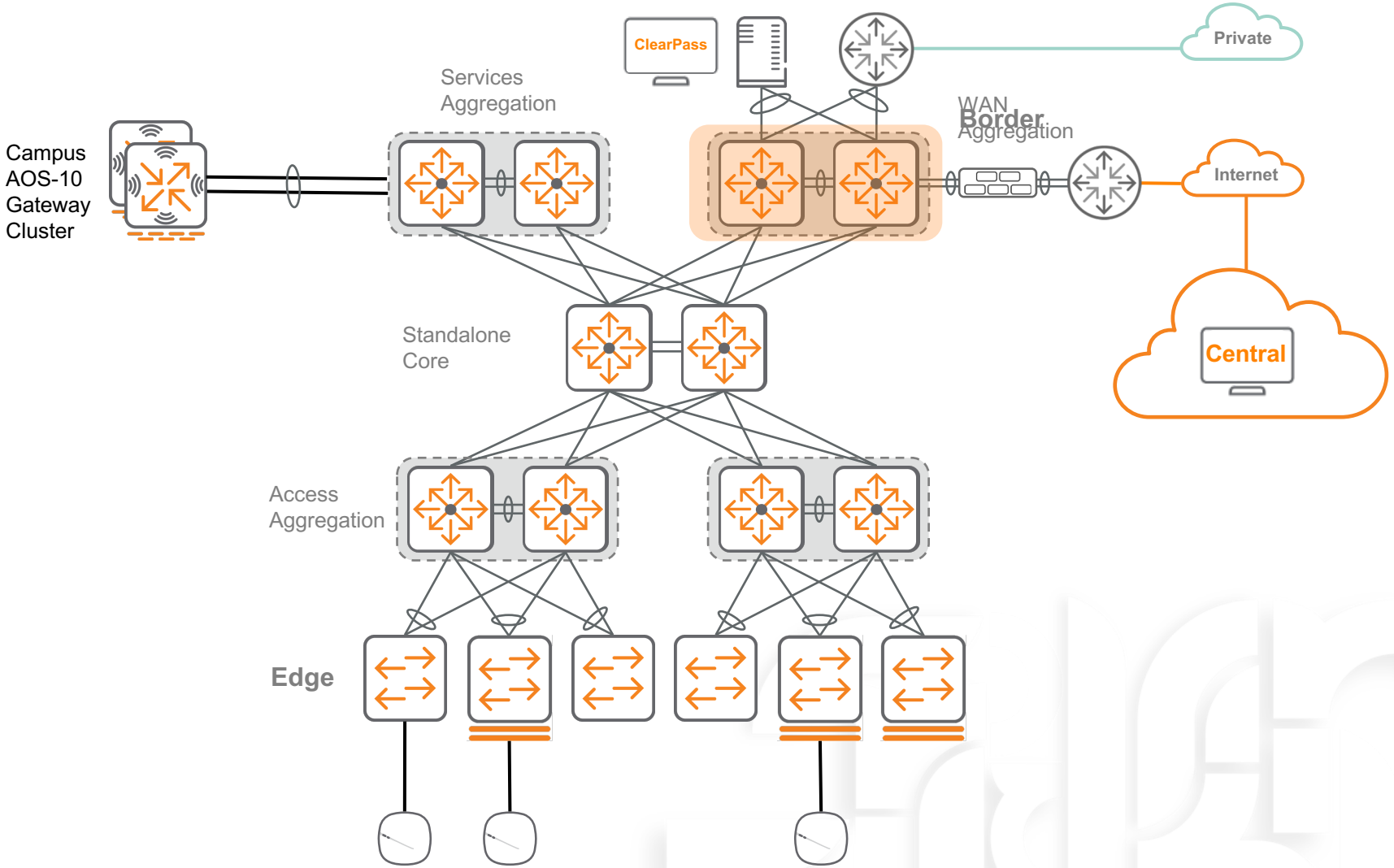
Device Personas in the Fabric

- **Edge** – connects endpoint devices into the fabric with authentication and policy enforcement.
- **Border** – connects the fabric to networks outside the fabric.
- **Stub** – enables GBP communication with a non-EVPN device in the fabric.
- **Route Reflector (RR)** – enables BGP routing across the fabric without the need for meshed peering.



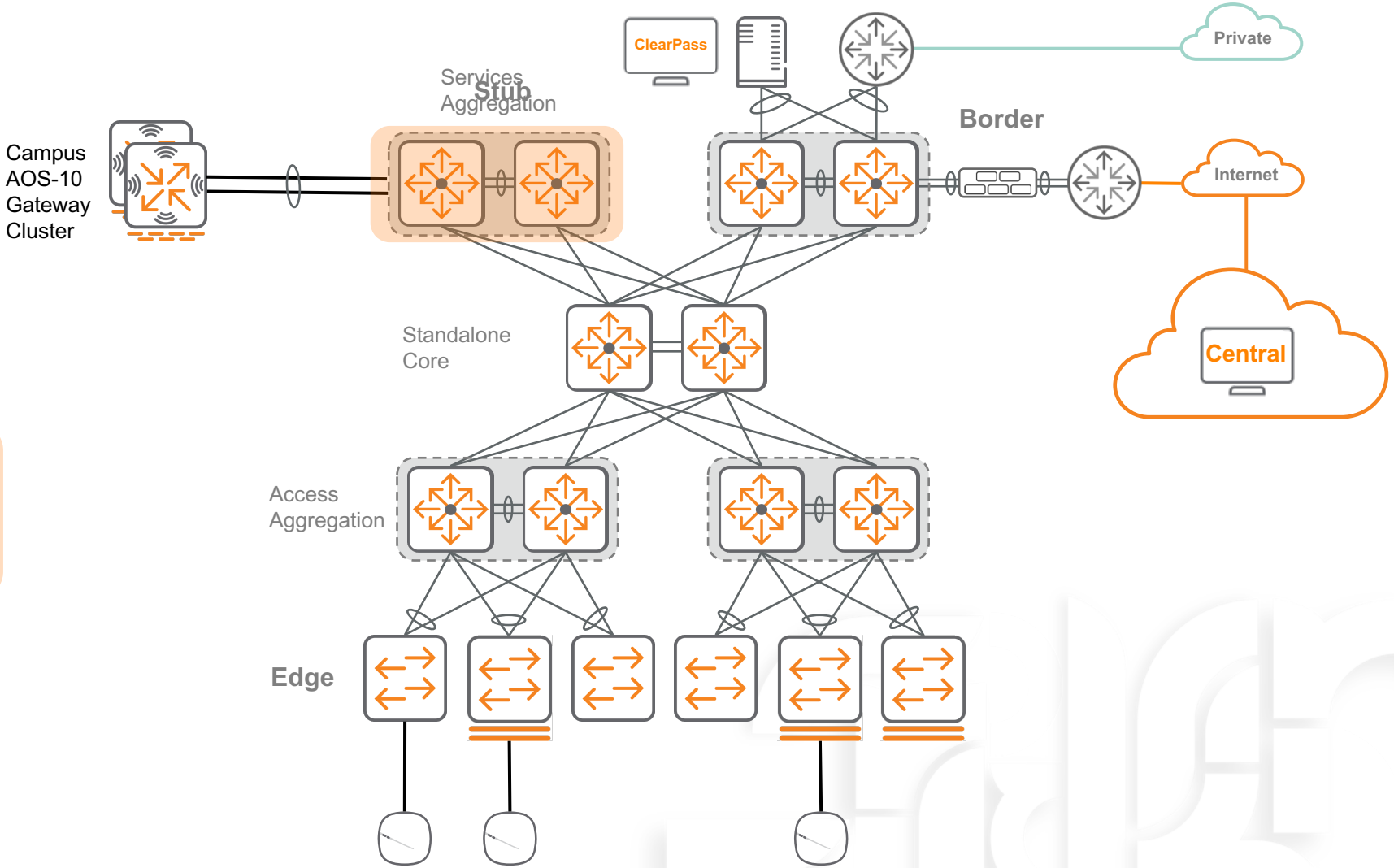
Device Personas in the Fabric

- **Edge** – connects endpoint devices into the fabric with authentication and policy enforcement.
- **Border** – connects the fabric to networks outside the fabric.
- **Stub** – enables GBP communication with a non-EVPN device in the fabric.
- **Route Reflector (RR)** – enables BGP routing across the fabric without the need for meshed peering.



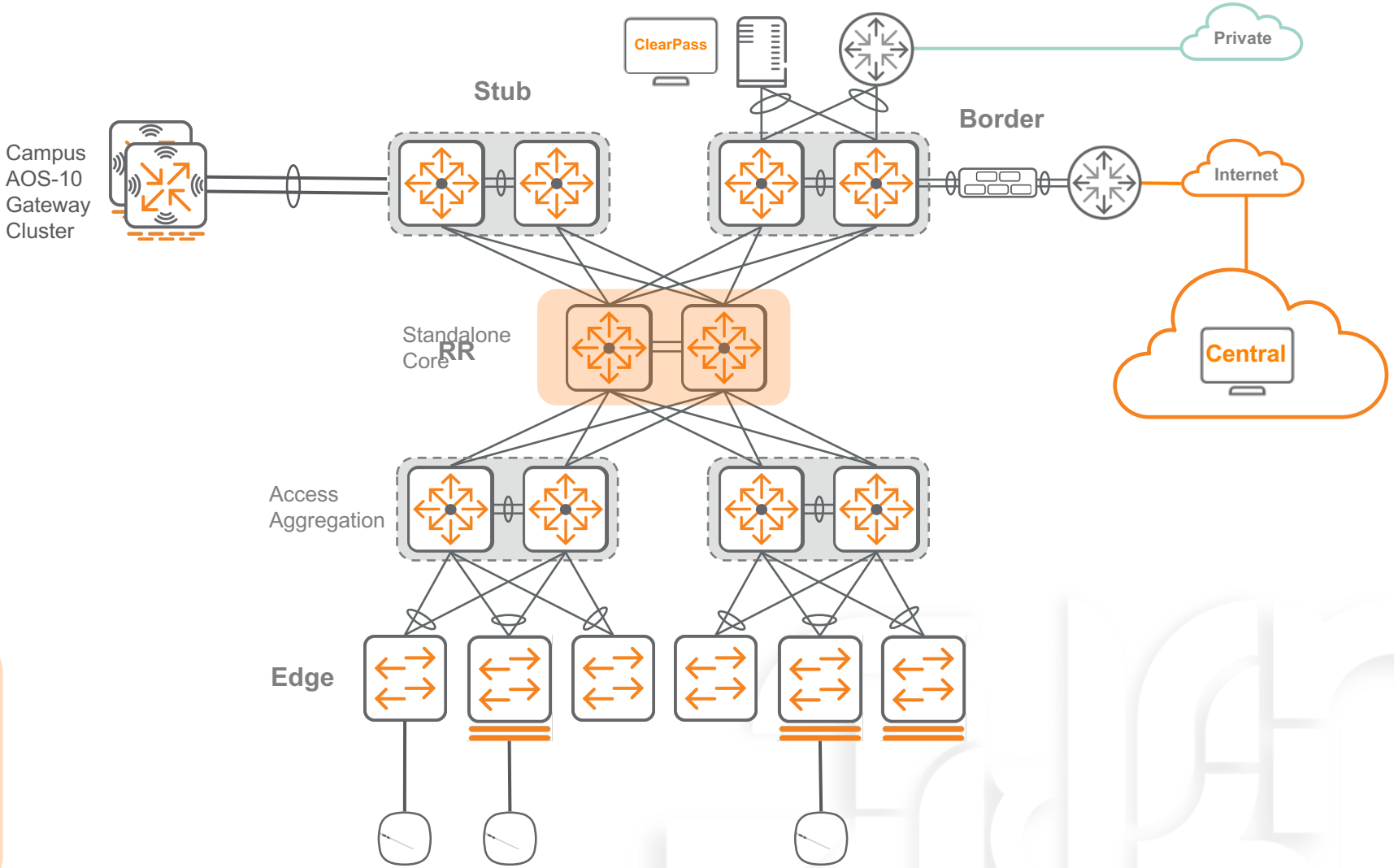
Device Personas in the Fabric

- **Edge** – connects endpoint devices into the fabric with authentication and policy enforcement.
- **Border** – connects the fabric to networks outside the fabric.
- **Stub** – enables GBP communication with a non-EVPN device in the fabric.
- **Route Reflector (RR)** – enables BGP routing across the fabric without the need for meshed peering.



Device Personas in the Fabric

- **Edge** – connects endpoint devices into the fabric with authentication and policy enforcement.
- **Border** – connects the fabric to networks outside the fabric.
- **Stub** – enables GBP communication with a non-EVPN device in the fabric.
- **Route Reflector (RR)** – enables BGP routing across the fabric without the need for meshed peering.



atmosphere'22
MEETUP

Thank you

aruba
a Hewlett Packard
Enterprise company