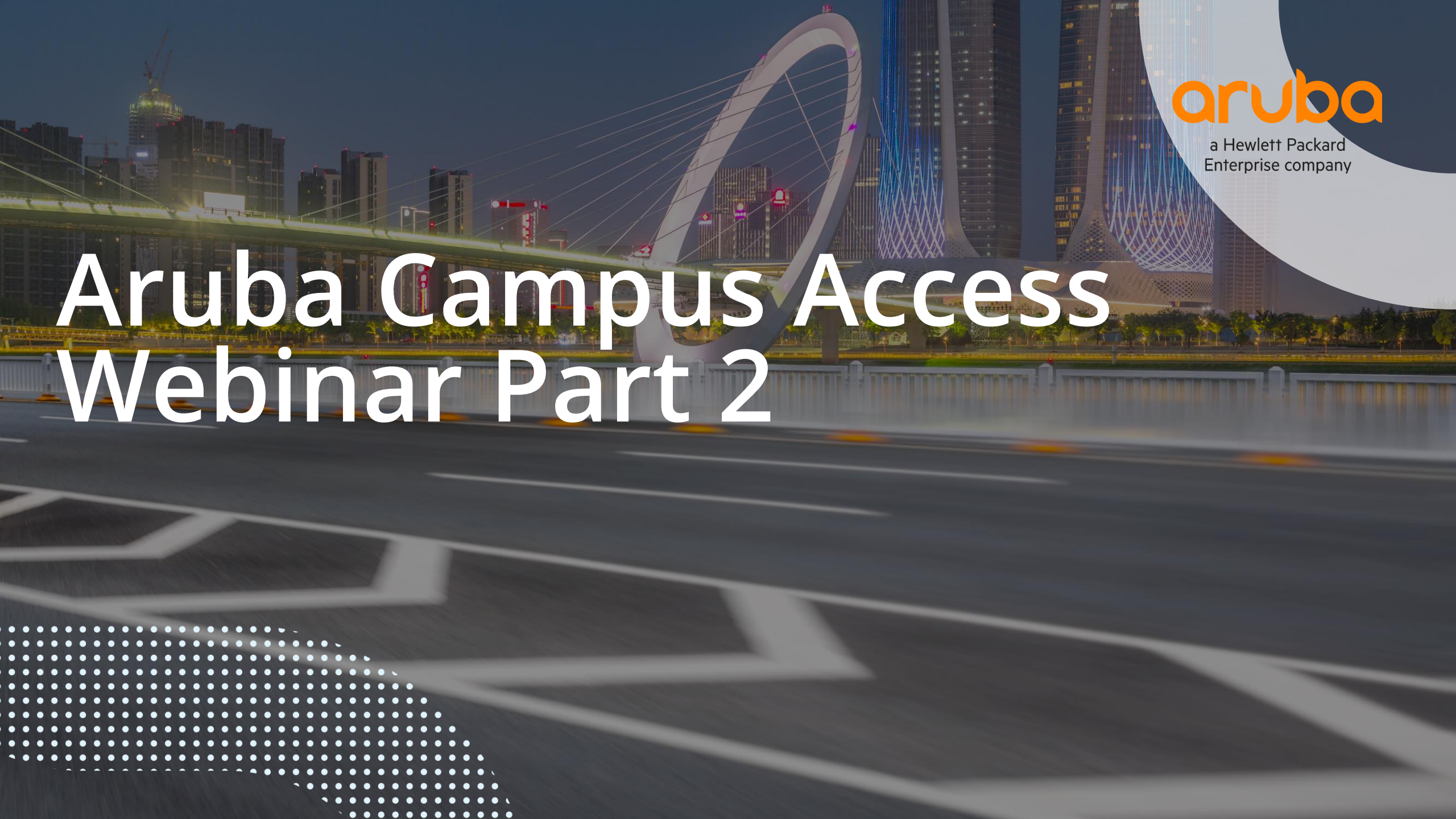


aruba
a Hewlett Packard Enterprise company

Aruba Campus Access Webinar Part 2

Aruba Campus Access Webinar

What to expect

ENGLISH | Presenter: Jacob Stelmaszczyk

PART 1: February 6th , 2023 | 9AM-11AM PST

PART 2: February 8th , 2023 | 9AM-11AM PST

- Part 1 Introduces networking fundamentals, types of networking devices, VLANs, IP routing, switch virtualization, Aruba WLAN bridge mode
- Part 2 Covers VSX, Aruba WLAN tunneled & mixed mode, 802.1X authentication, Dynamic Segmentation and VxLAN GBP

SPANISH | Presenter: Alvaro Tellez

PART 1: February 6th , 2023 | 12:00-14:00 PST

PART 2: February 8th , 2023 | 12:00-14:00 PST

Aruba VSX

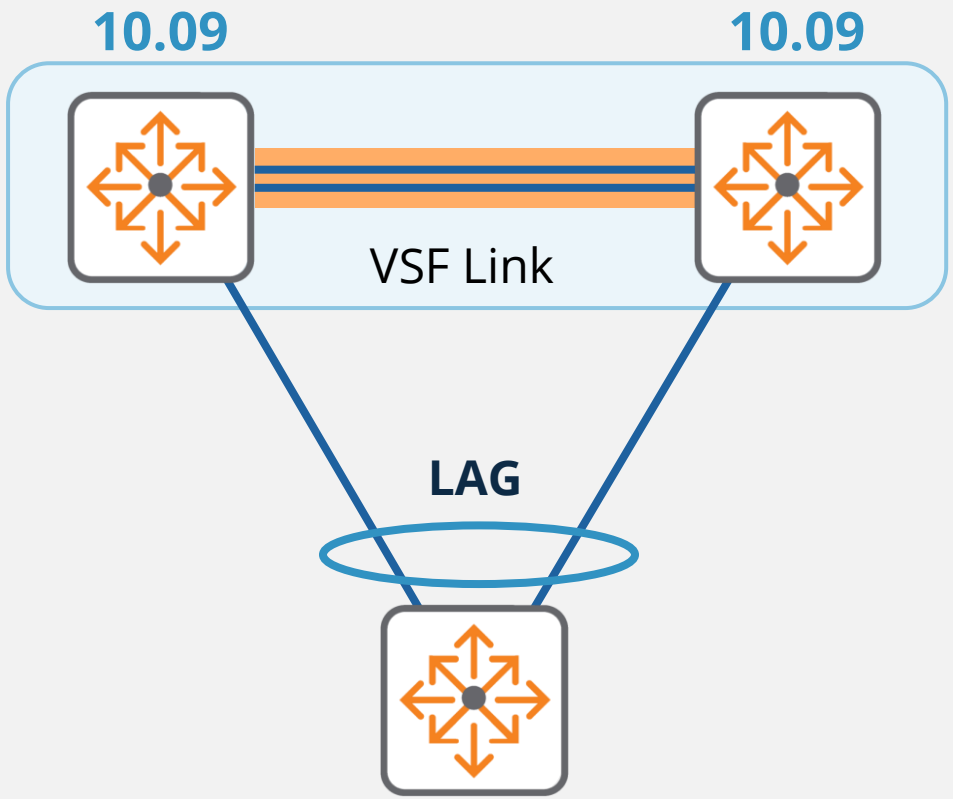
aruba
a Hewlett Packard Enterprise company

EDUCATION
SERVICES

AOS-CX Switch Virtualization: VSX vs VSF

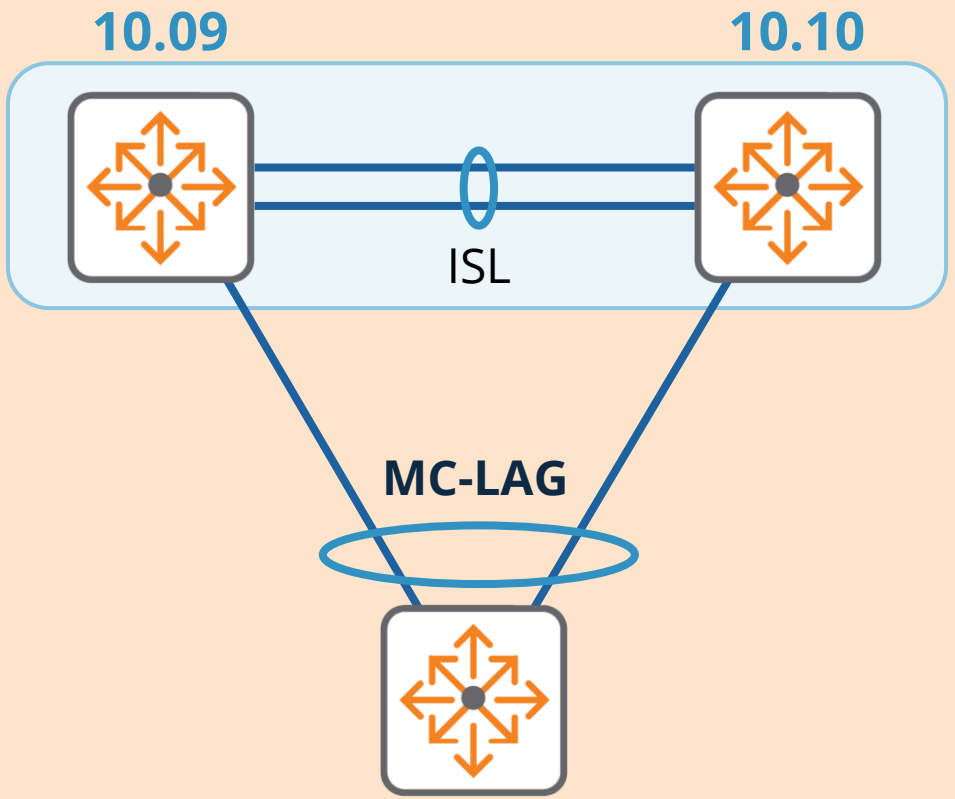
VSF

Both switches must run the same OS version
Predictable downtime during upgrade

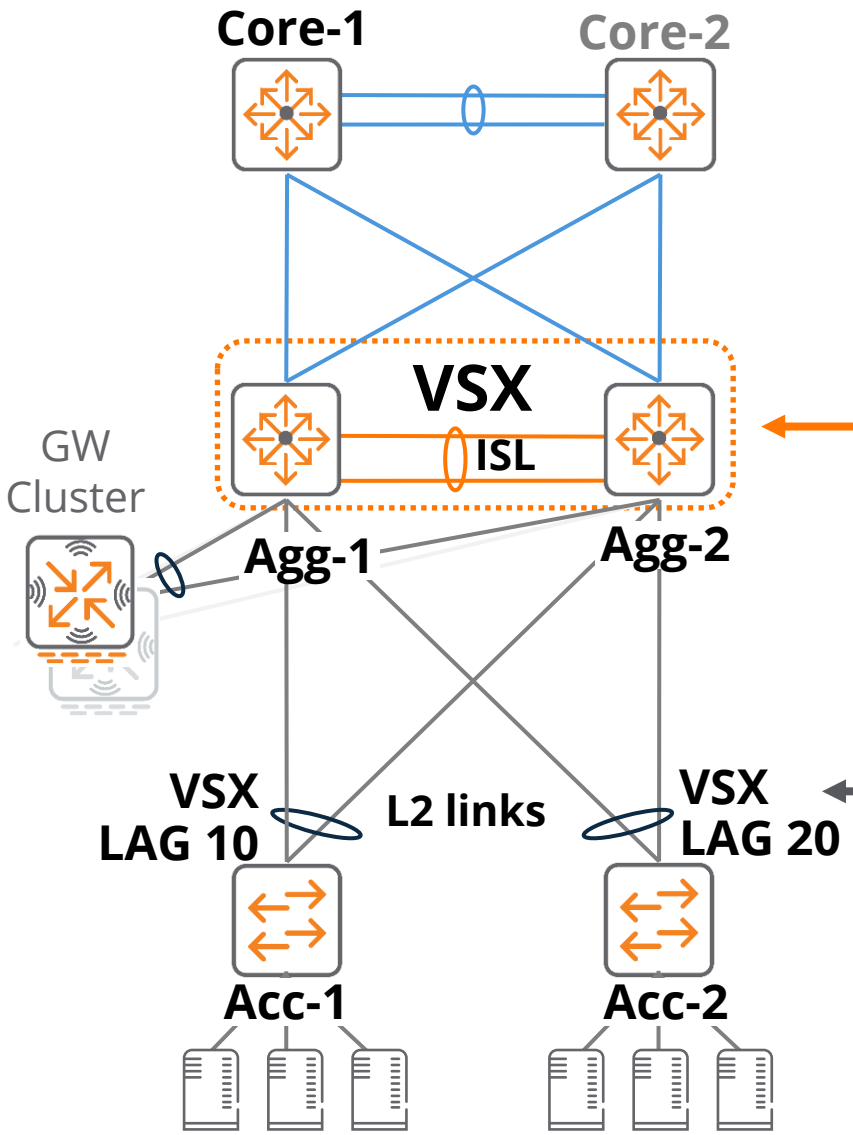


VSX

Switches can run different OS versions
No downtime during upgrade



VSX Benefits



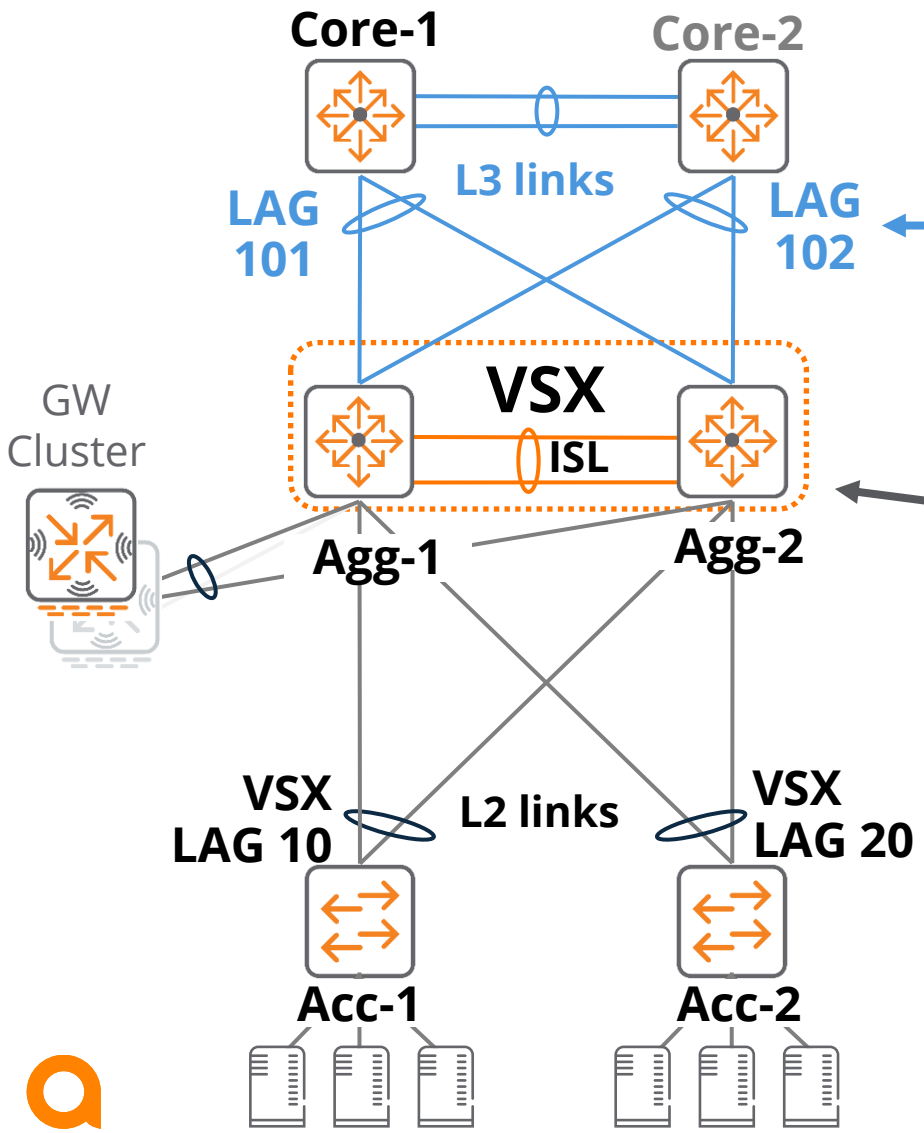
Control Plane

- Dual control plane: Better resiliency
- Unified management: Synced config, easy troubleshooting
- Independent software upgrades: Near zero downtime
- In-chassis (8400/6400) and device level redundancy

L2 distributed LAGs

- No spanning-tree requirement
- Loop-free L2 multi-pathing (active-active)
- Simple configuration
- Rapid failover

VSX Benefits: Layer 3



L3 Links

- Various options:
  - Routed only ports (ROPs)
  - L2 ports associated with dedicated SVIs
  - VSX LAGs associated with dedicated SVIs
- Unified data path: active-active L2/L3 forwarding
- L3 ECMP + L2 VSX LAG (highly fault tolerant)

Active-Active Gateway

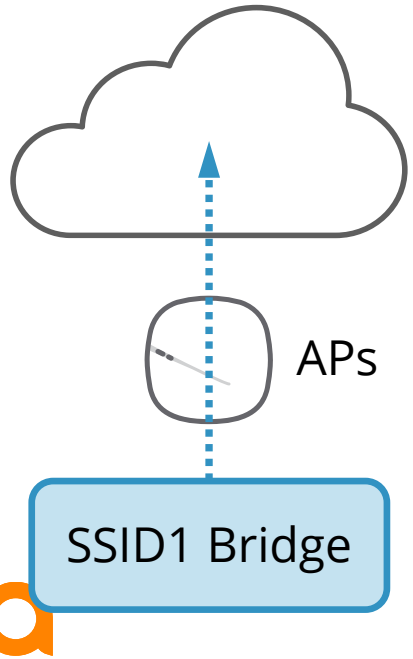
- Active-Active first hop gateway (VIP)
- No VRRP/HSRP
- Simple configuration
- No gateway protocol overhead
- DHCP relay redundancy

Aruba Gateways

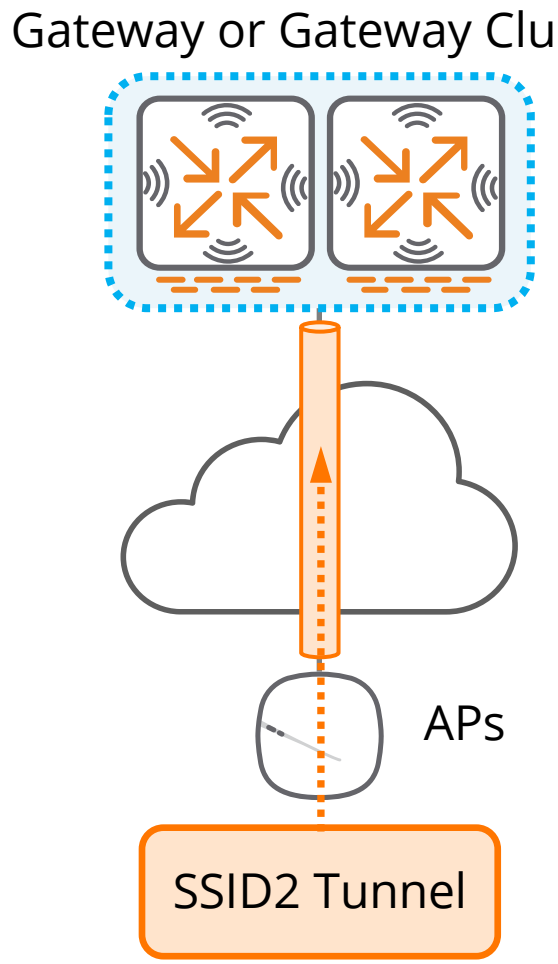
aruba
a Hewlett Packard Enterprise company
EDUCATION SERVICES

Aruba WLAN forwarding modes

Bridge

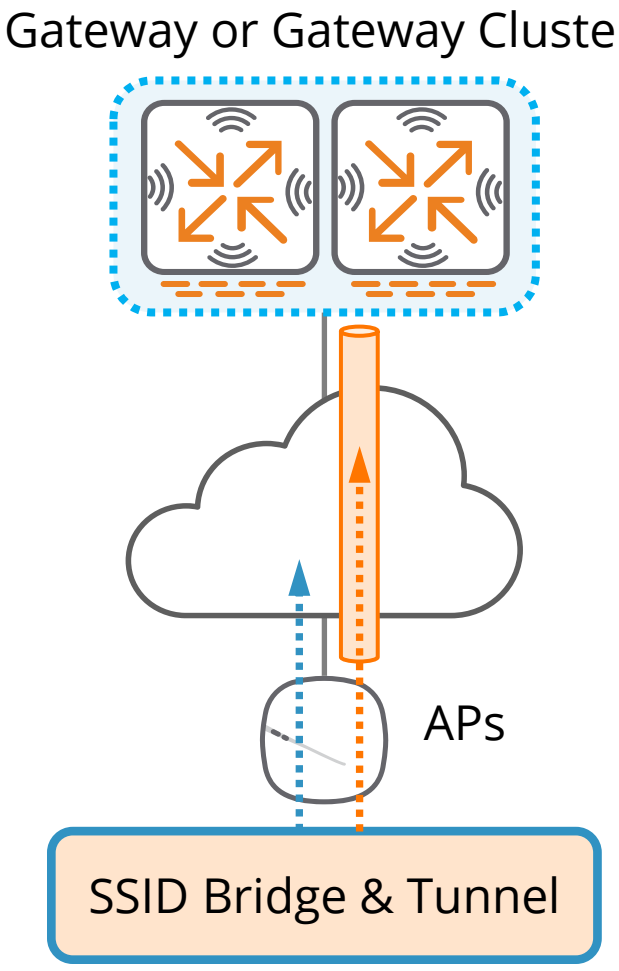


Tunnel Mode



Mixed Mode

1 SSID: Bridge & Tunnel



When to Use Gateways

More than 5000 clients

More than 500 APs

Tunneled WLANs

Network simplification

A key element in

AOS10 architecture

Dynamic segmentation

Enhanced mobility

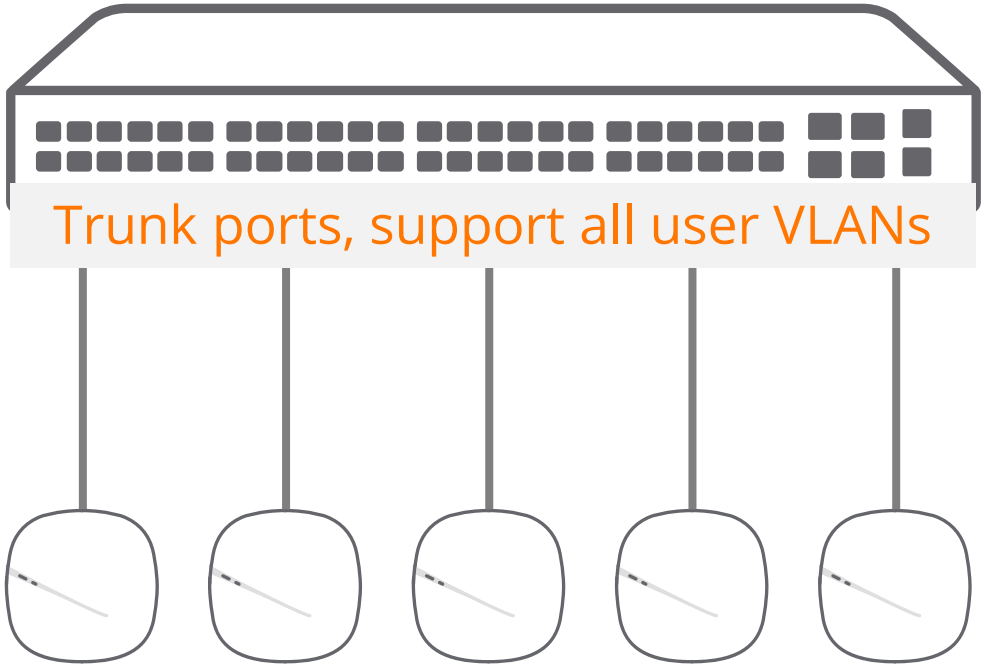
Microbranch deployments

RADIUS proxy

Network Simplification

Must likely enable user VLANs on:

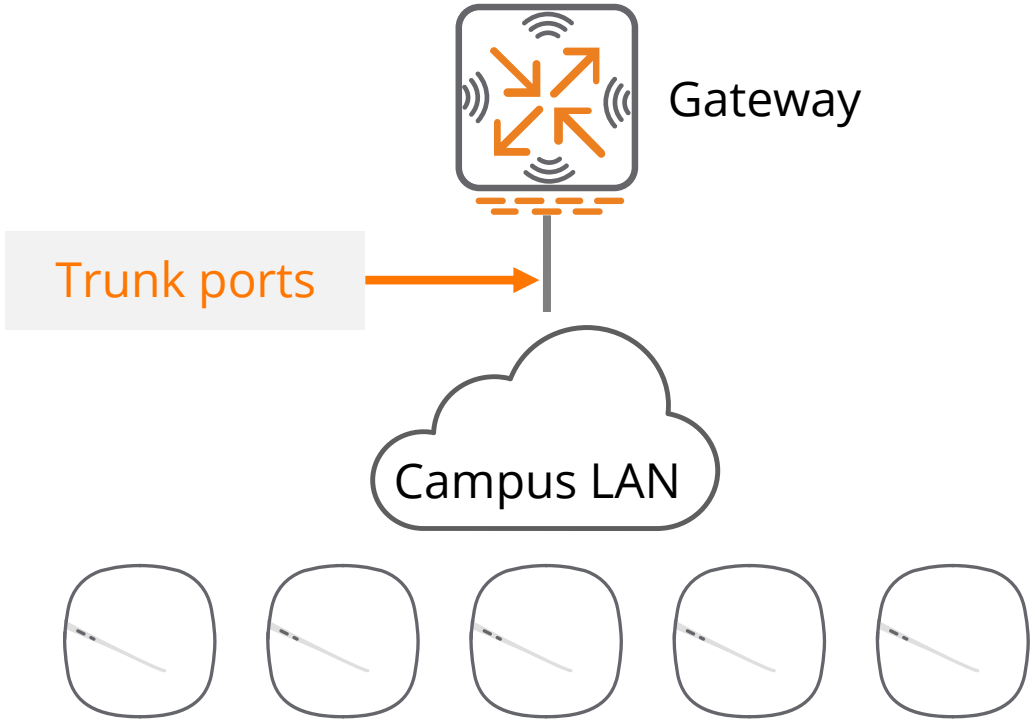
- Every AP-connected access switch
- Each AP port



User VLANs likely span entire network

Must only enable user VLANs on:

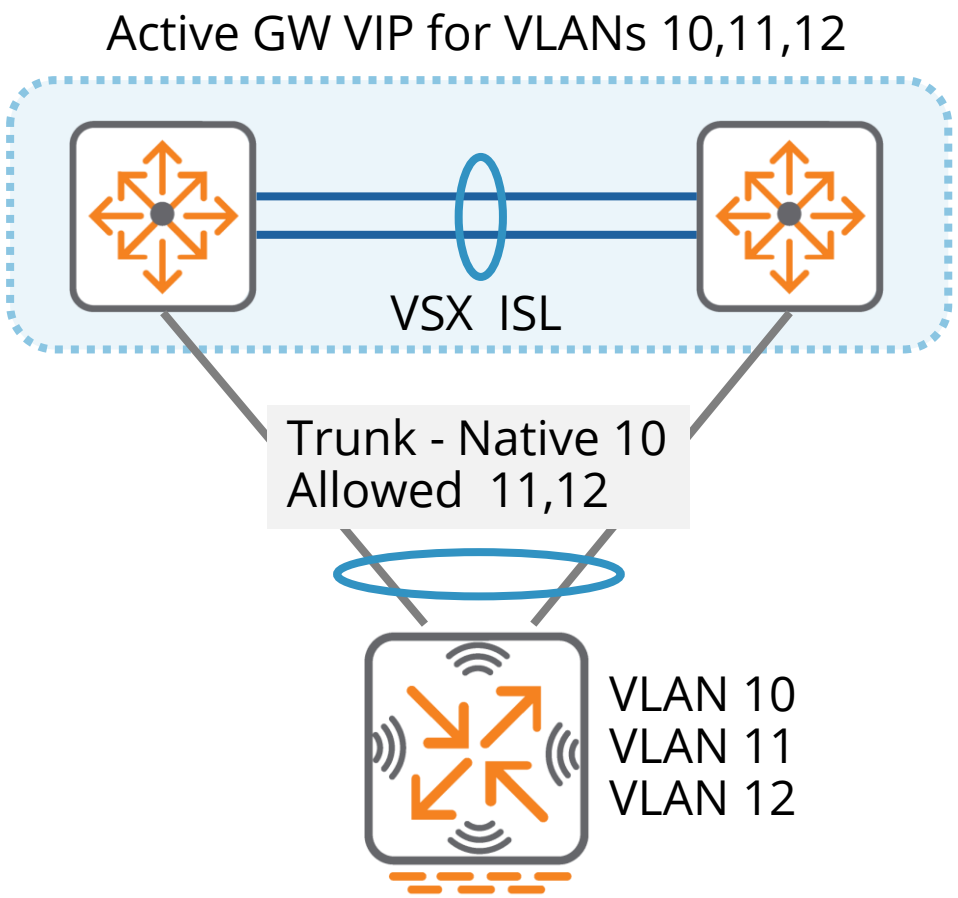
- Gateway
- Gateway ports on Core (Agg) switches



User VLANs do not span entire network

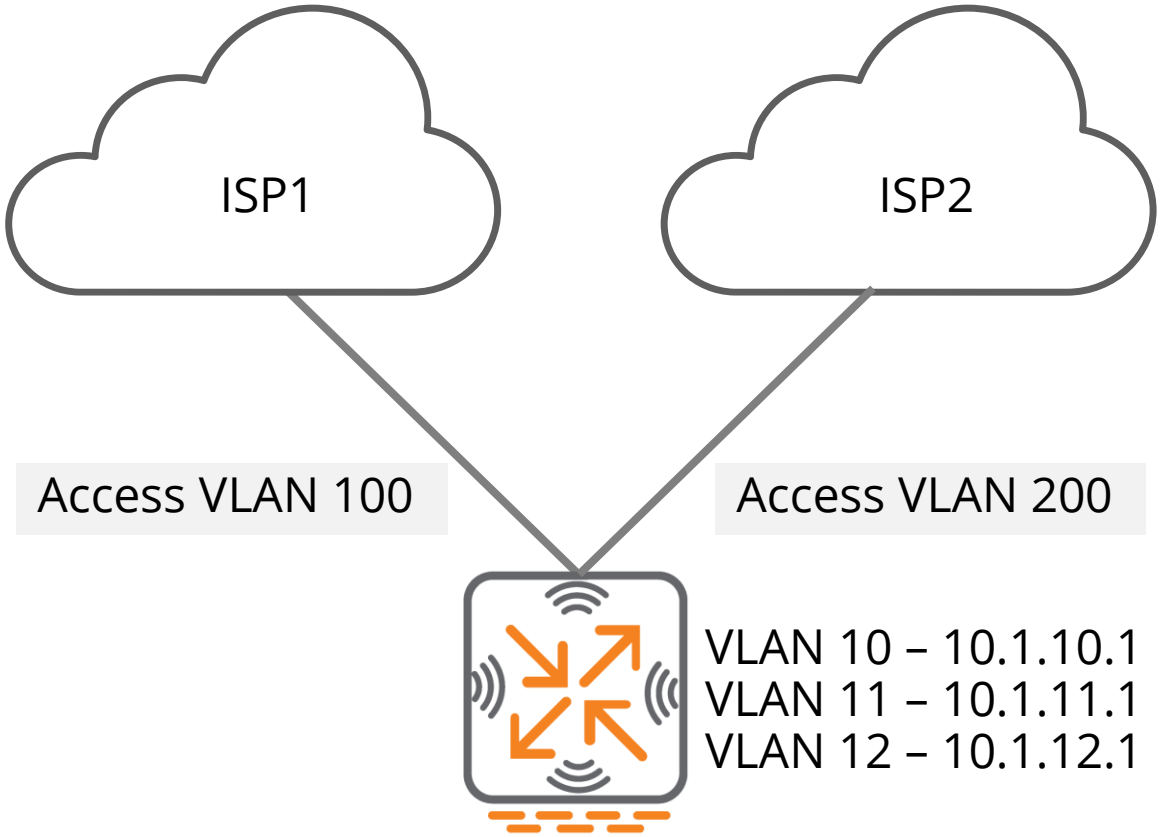
Gateway as L2 or L3 Device

Layer 2 mode



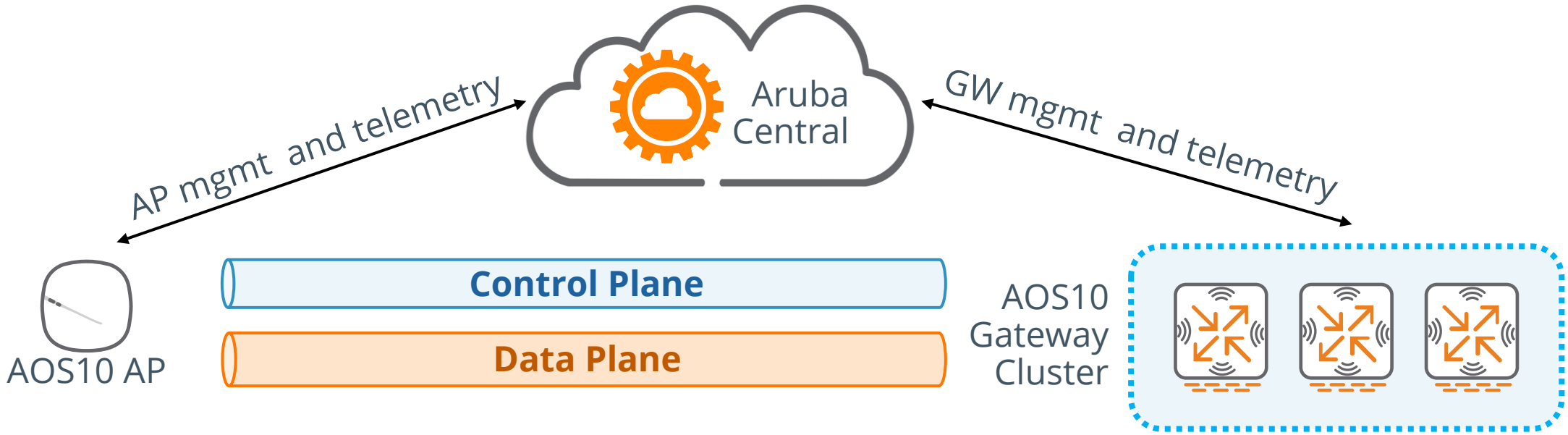
Typical for Campus deployment

Layer 3 mode



Typical for Branch gateway deployment

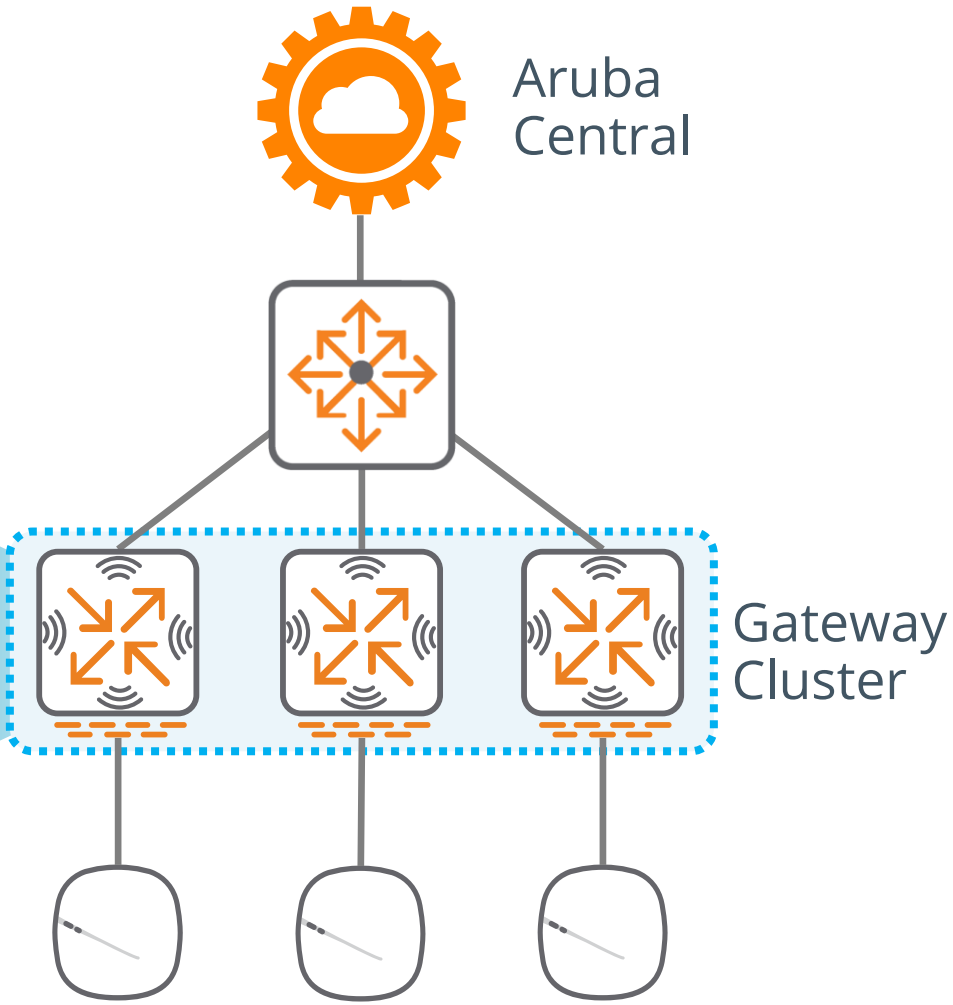
Deployment with Gateways



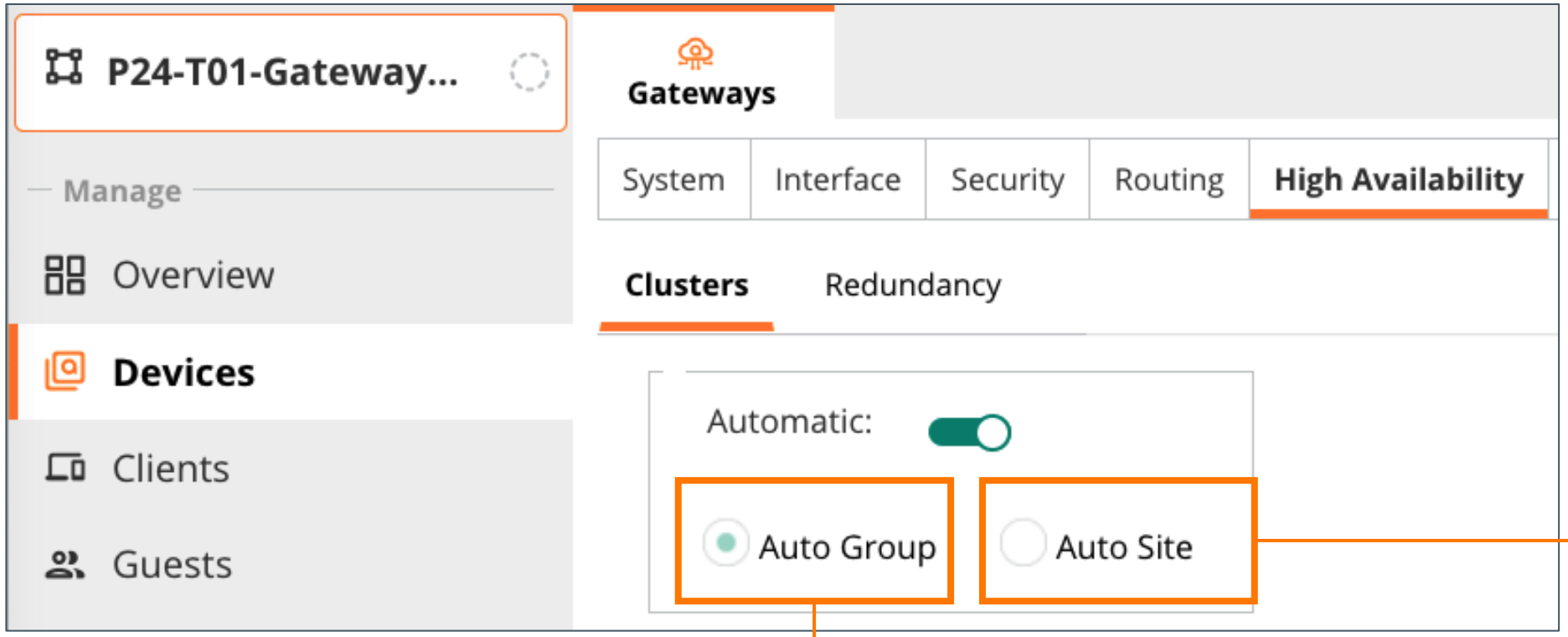
Forwarding modes	AP - Gateway Communication	Authentication and Encryption
• Tunnel mode • Mixed mode • Microbranch mode (VPNC)	• Version independent • IPsec for control plane • GRE for data plane	• AP is the authenticator • Gateway act as a RADIUS proxy • APs do encrypt/decryption

Gateway Cluster

- Seamless roaming
- Client/AP load balancing
- Hitless failover
- Client state sync
- Ease of deployment



Automatic Cluster Mode



Default

Warning

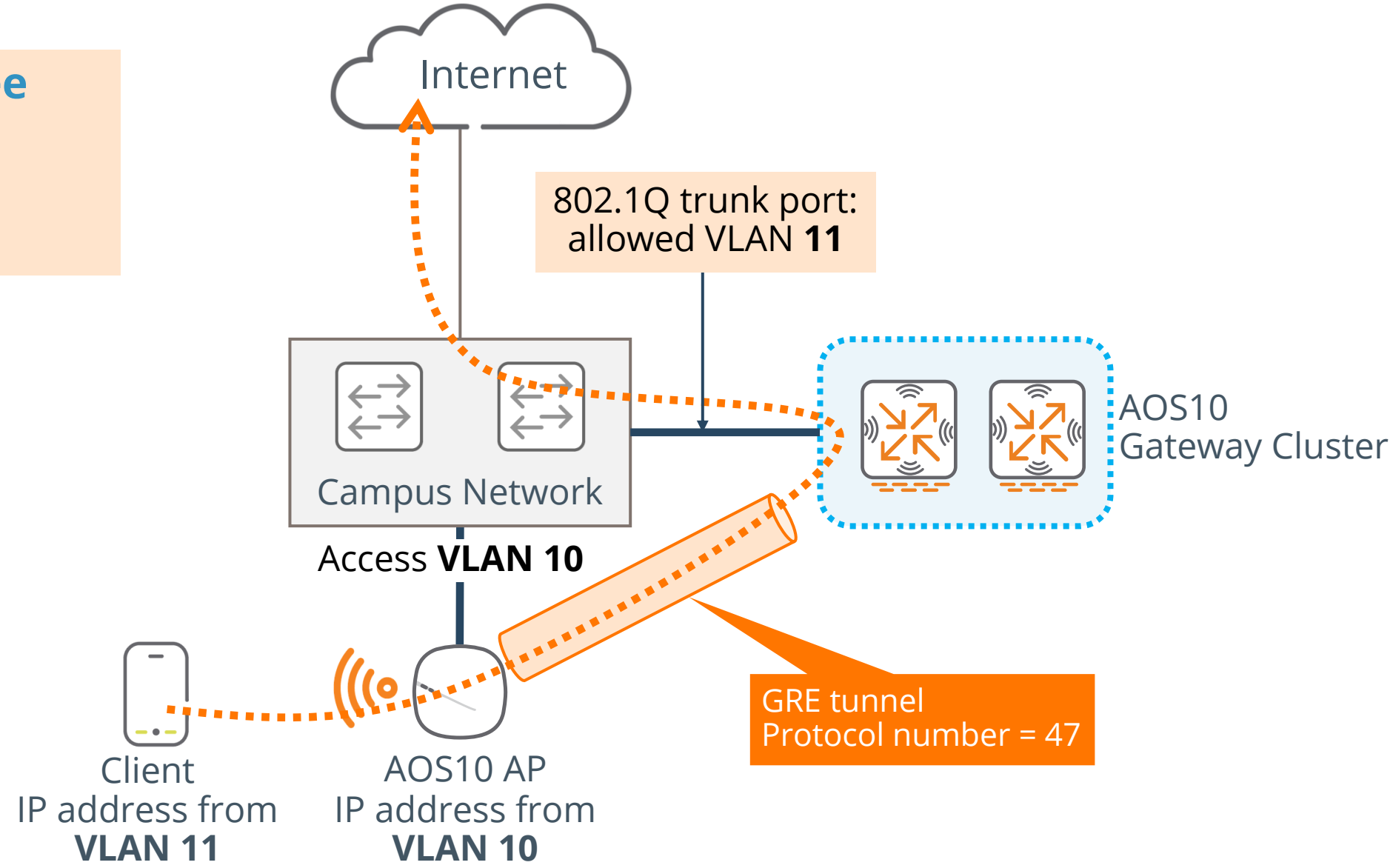
⚠ Existing auto-group clusters will be dismantled and gateways will be remapped to new site specific auto-clusters.

Do you want to save and continue?

Aruba Tunneled Mode

Tunnel Forwarding Mode

WLAN **Employee**
Tunnel Mode
802.1X
VLAN 11



AP to Gateway Connections

Control Plane

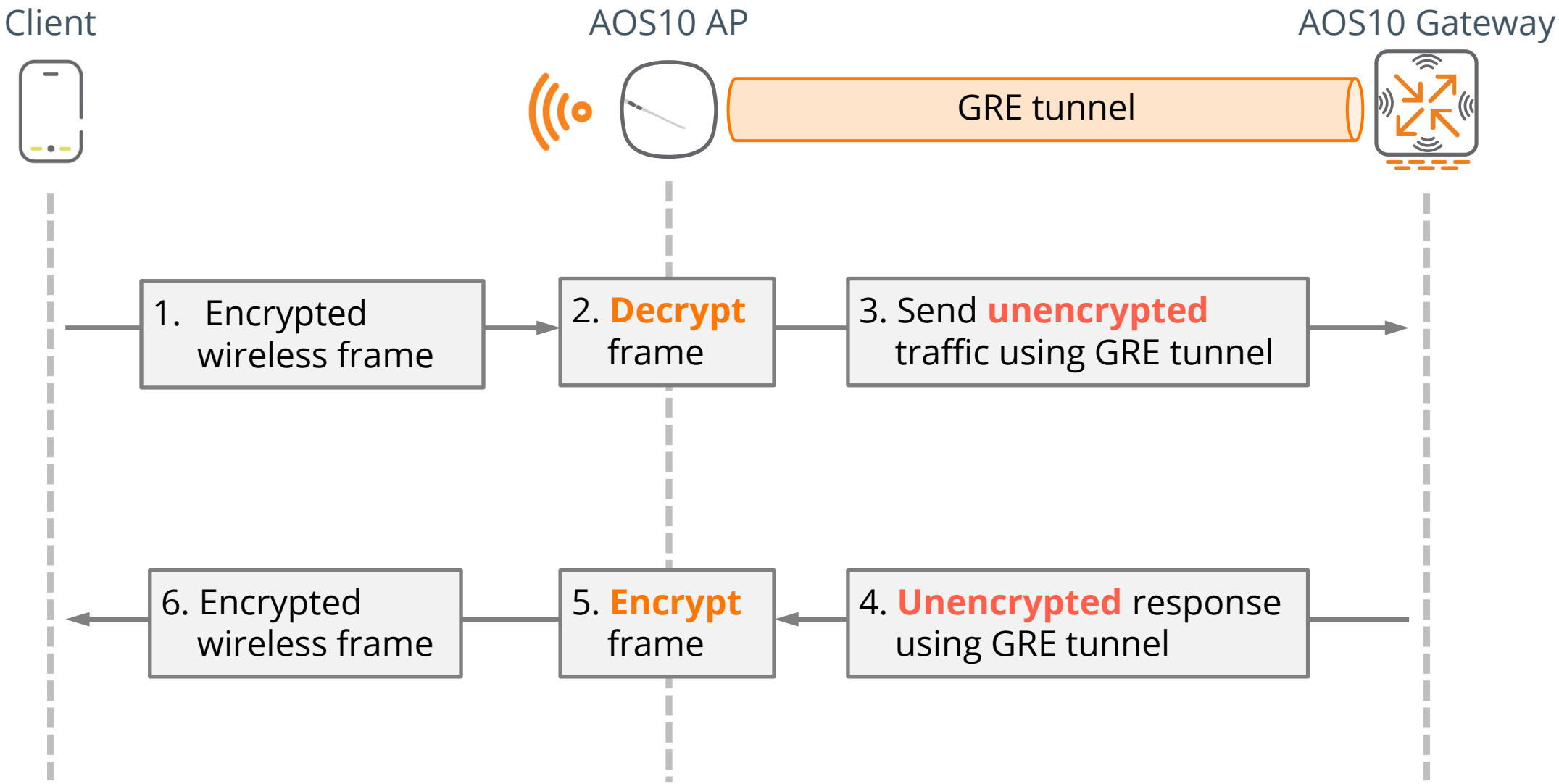
- AP-GW Heartbeats
- Cluster information
- RADIUS
- Roaming assistance
- Orchestrated tunnel

Data Plane

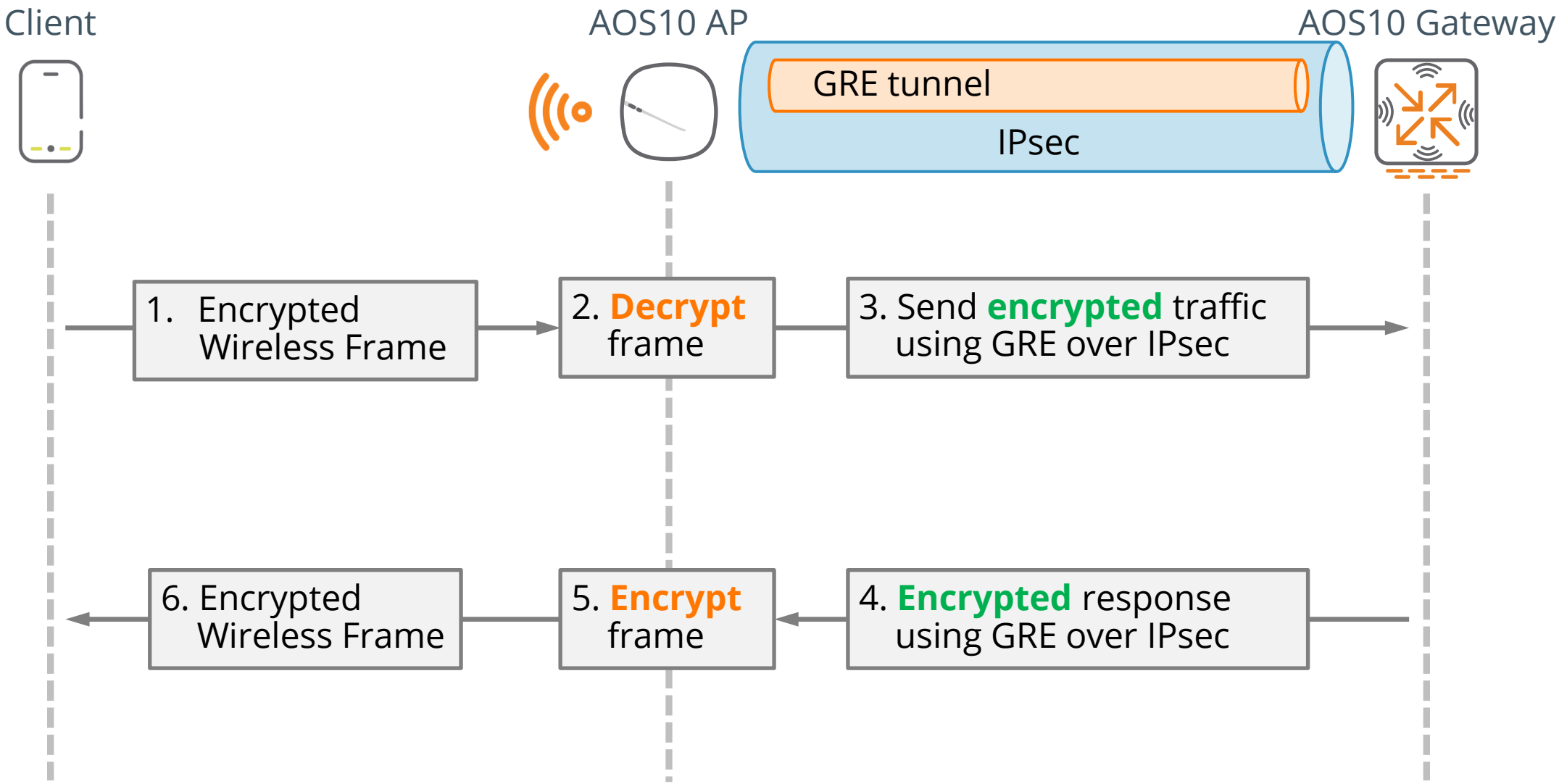
- Client's traffic
- **Single tunnel for all SSIDs**

AOS10 GRE tunnel setup different from previous AOS versions

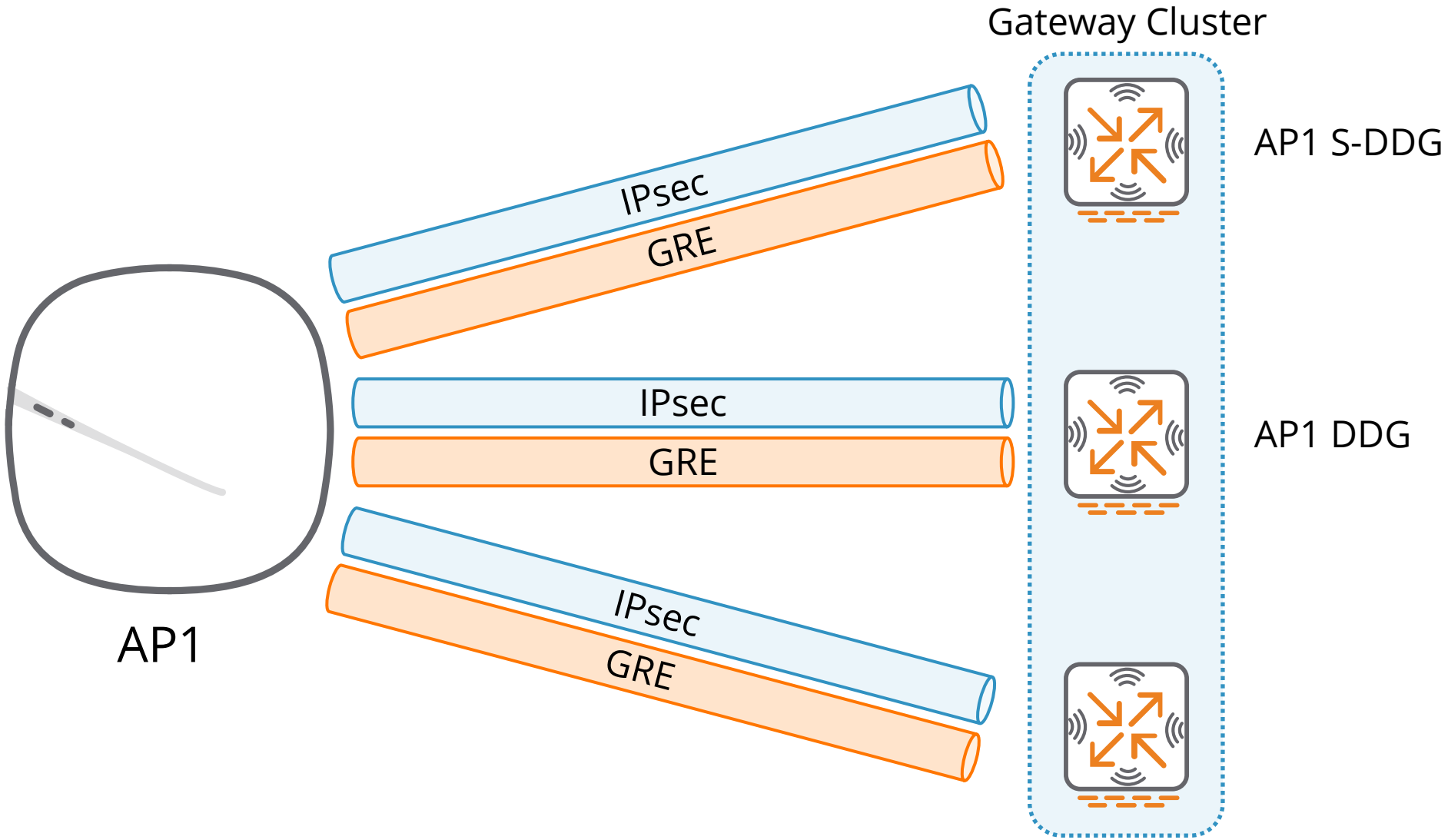
Tunnel Forwarding Mode



Data Encryption

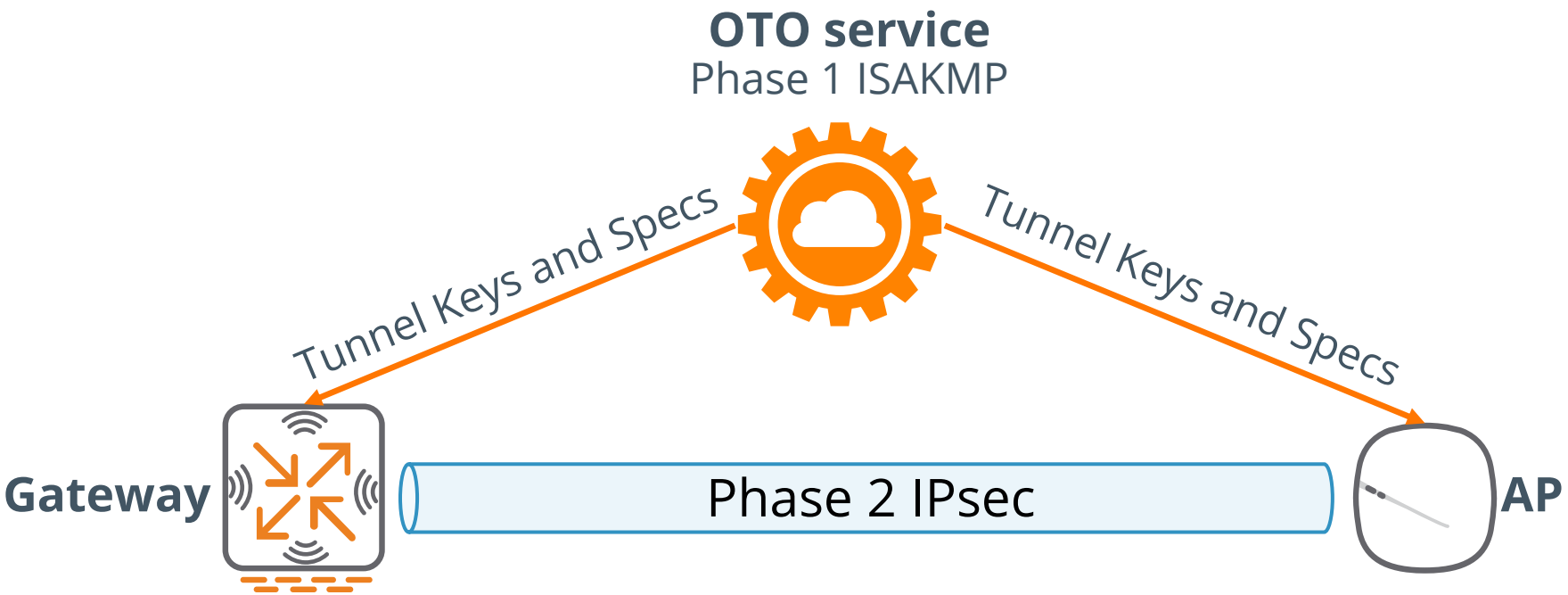


AP to Gateway Cluster Tunnels



A single IPsec & GRE tunnel to every Gateway

Overlay Tunnel Orchestrator



OTO Service

- Negotiate IPsec Phase1
- Share key material with APs and Gateways

APs and Gateways

- Negotiate IPsec Phase 2
- IPsec protect control plane communication

No controller discovery mechanism necessary

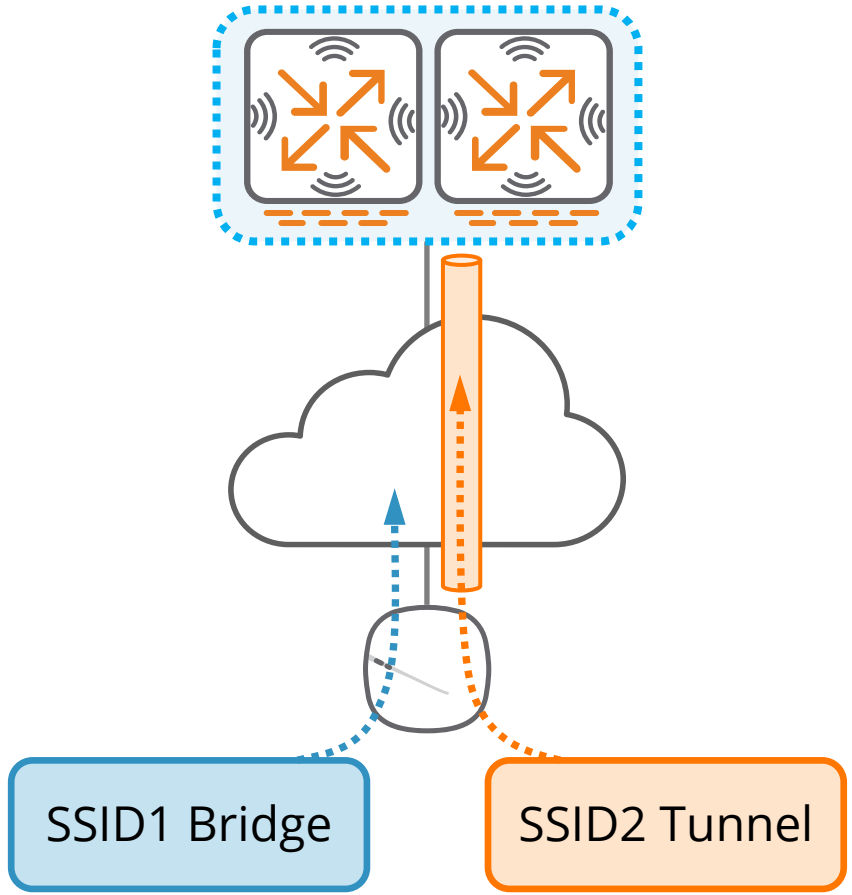
Aruba Mixed Mode

aruba
a Hewlett Packard Enterprise company
EDUCATION SERVICES

Introduction

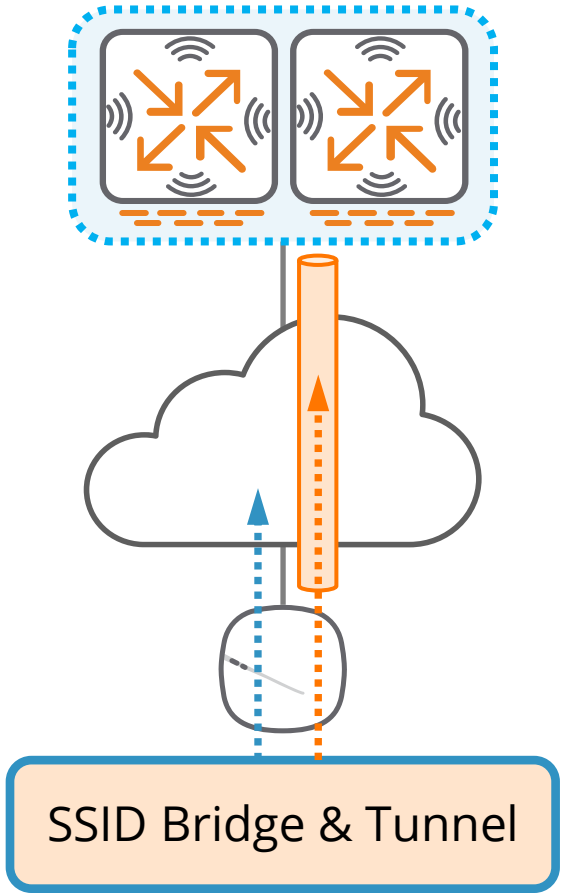
Bridge & Tunnel Mode

2 SSIDs: One Bridge, One Tunnel



Mixed Mode

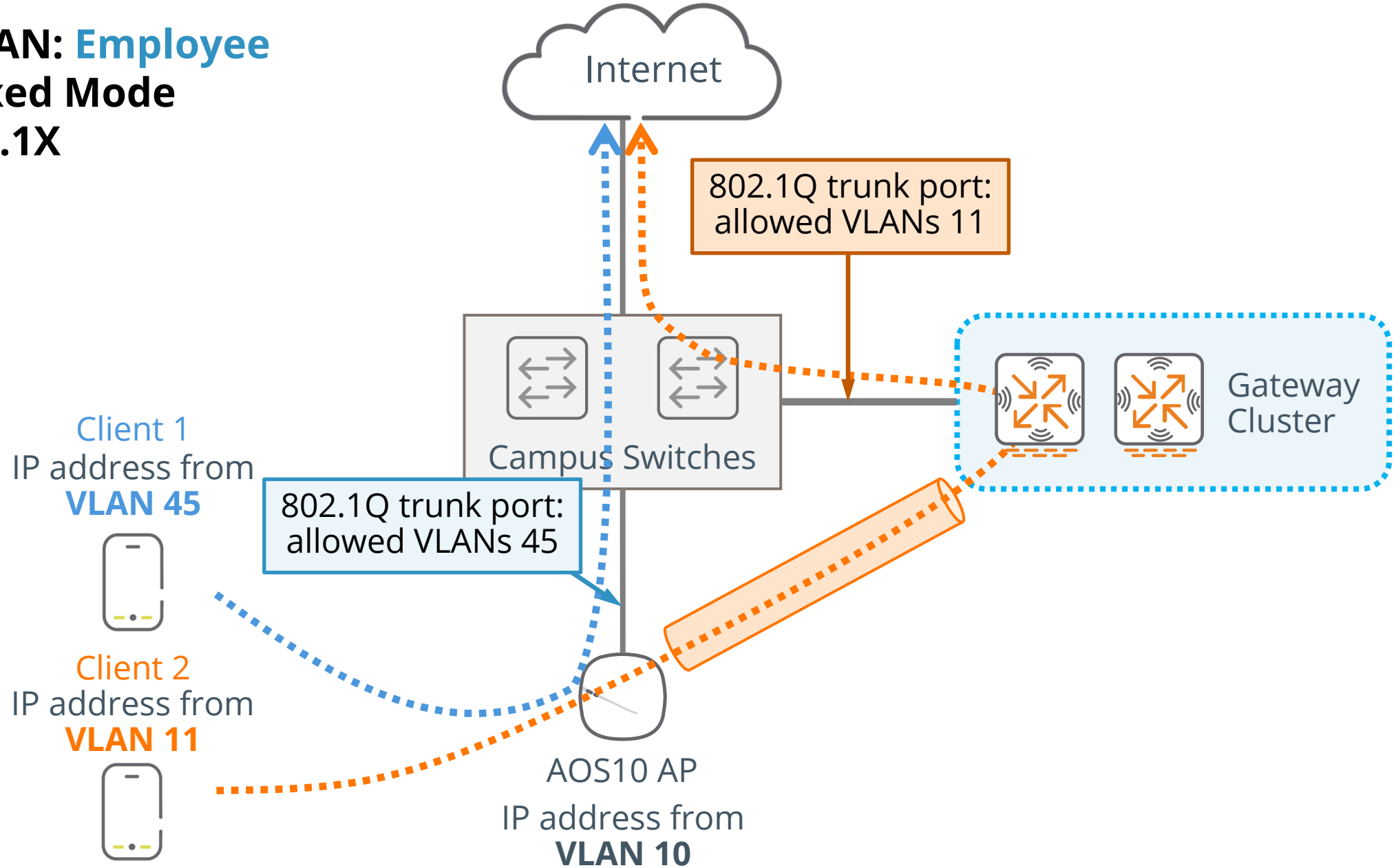
1 SSID: Bridge & Tunnel



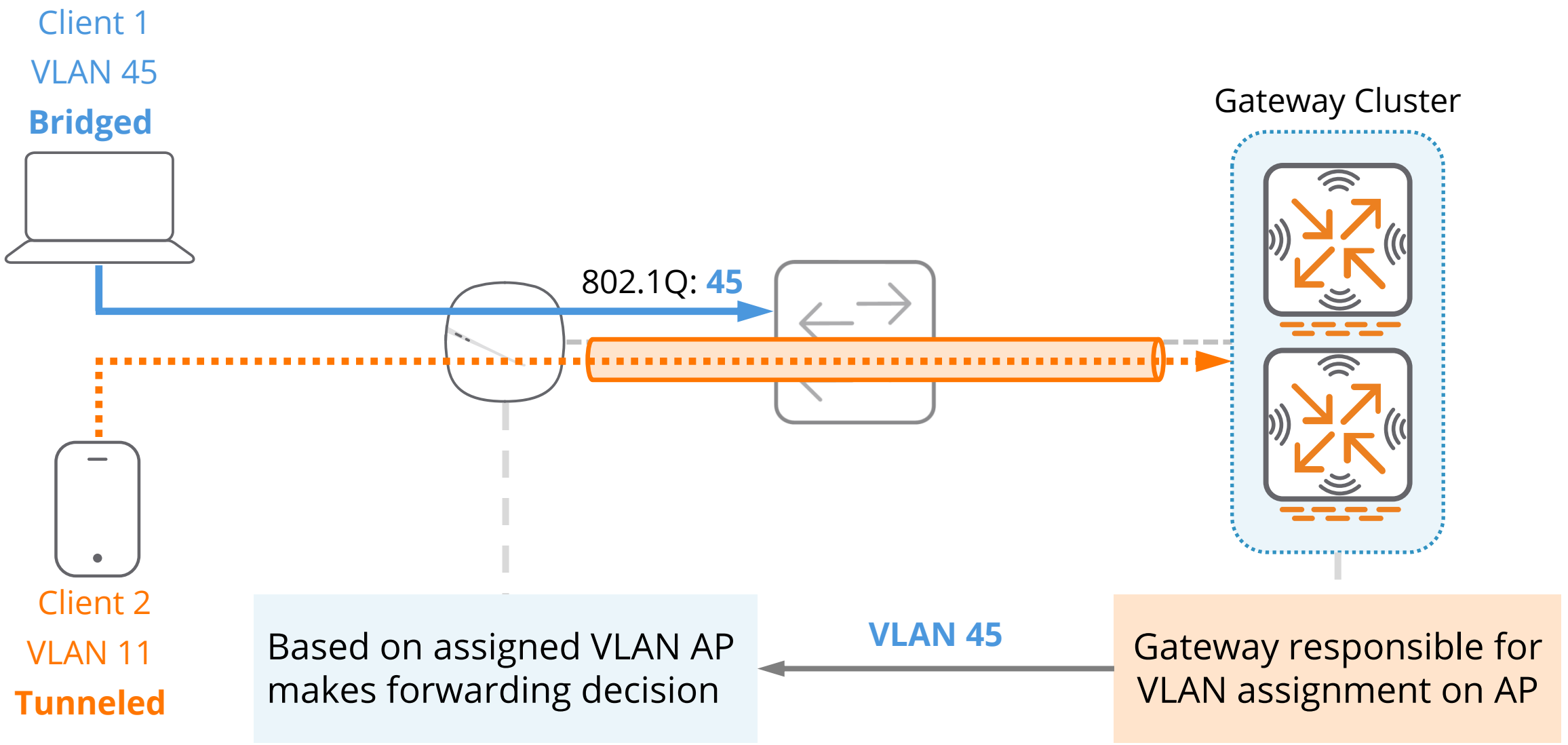
Reduced number of SSIDs in Campus

Mixed Forwarding Mode

WLAN: Employee
Mixed Mode
802.1X



Mixed Forwarding Mode Architecture



Switch must support bridged clients VLANs on AP port

Secure WLAN & 802.1X

aruba
a Hewlett Packard Enterprise company
EDUCATION SERVICES

Authentication Overview

Supplicant

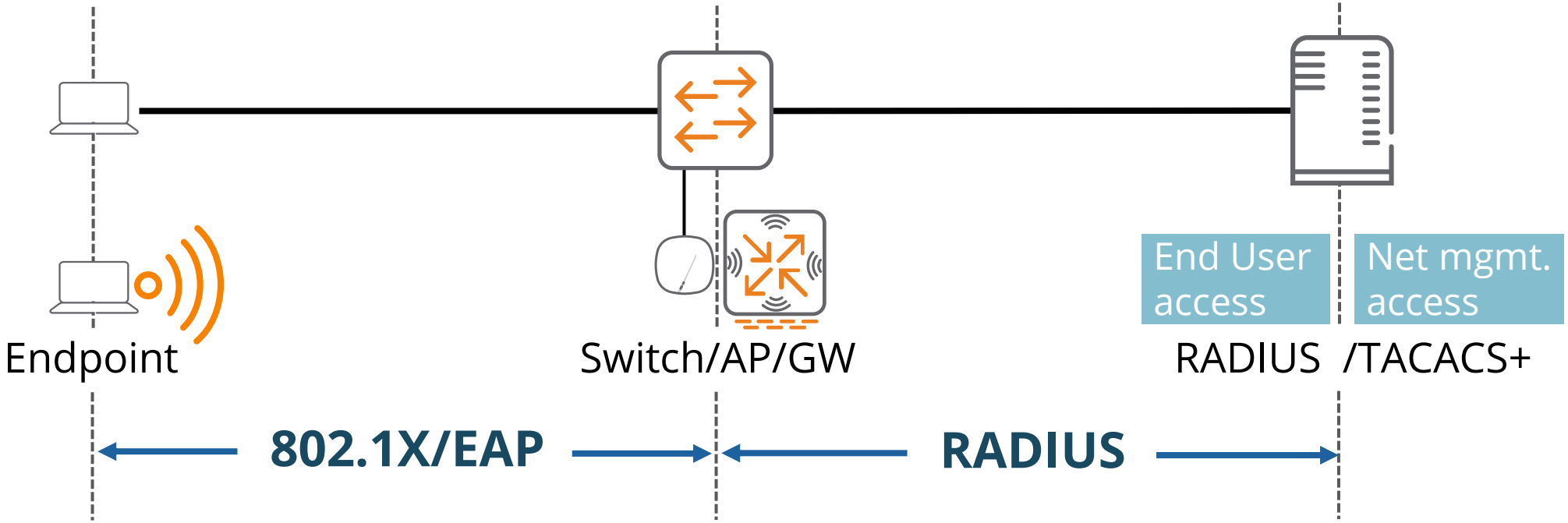
802.1X-capable client software

Authenticator

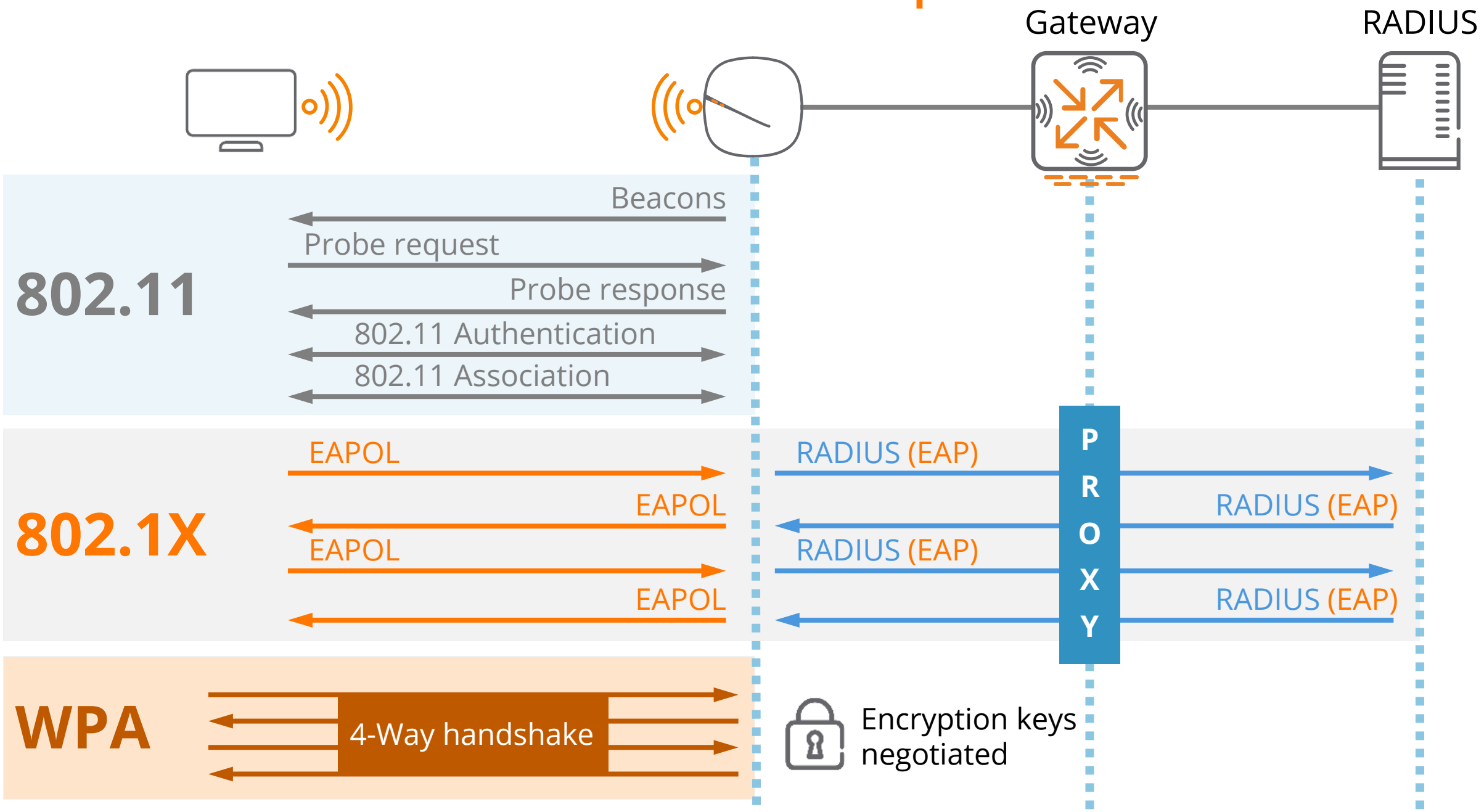
Controls initial access

Authentication Server

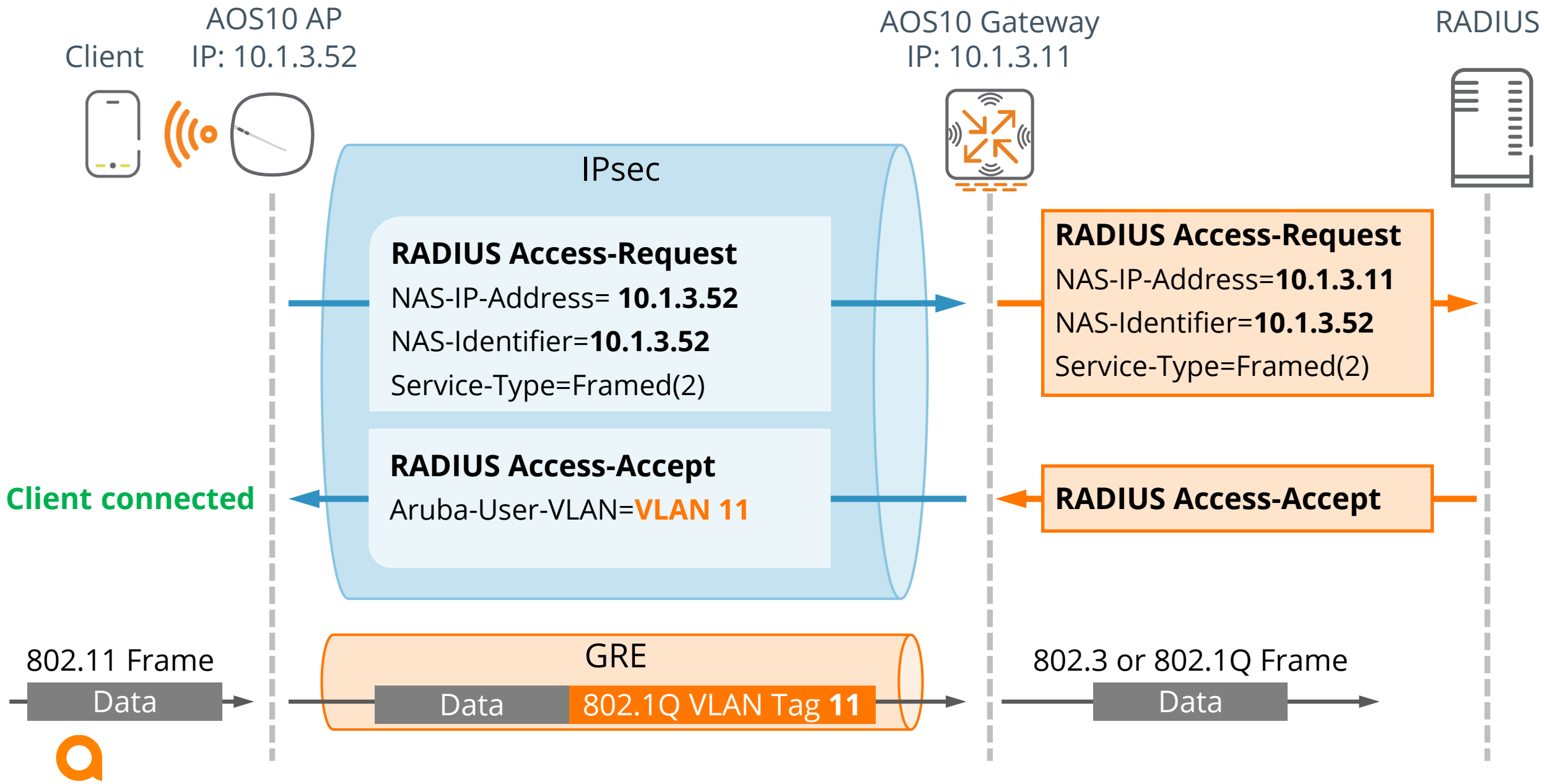
Grants / denies access



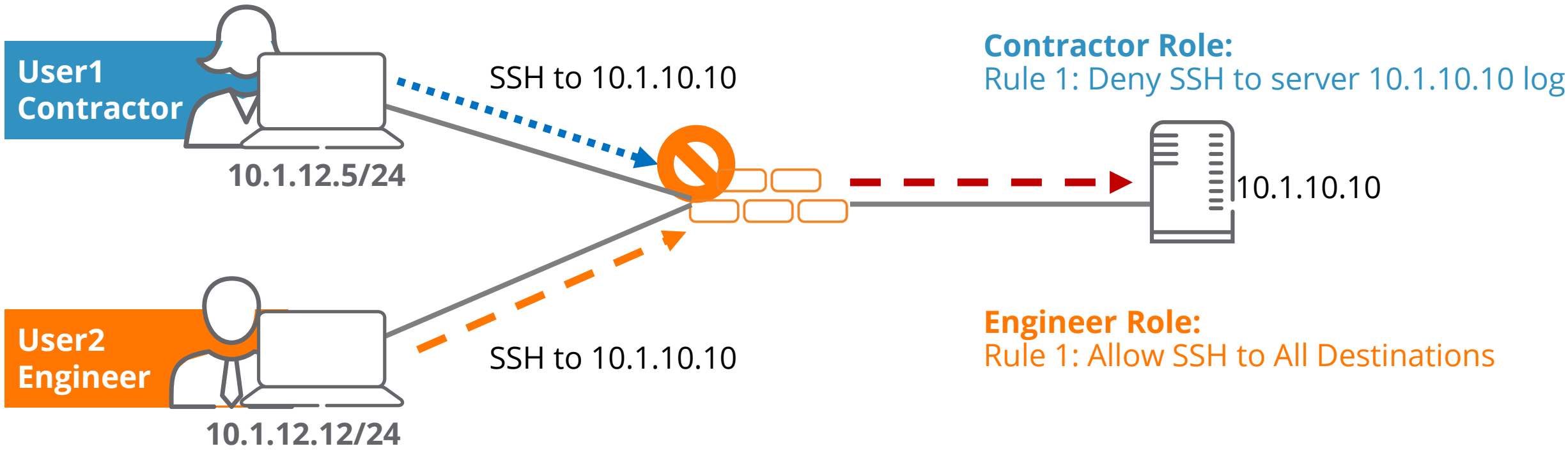
802.11 with 802.1X Connection Steps



Client Connecting to 802.1X SSID

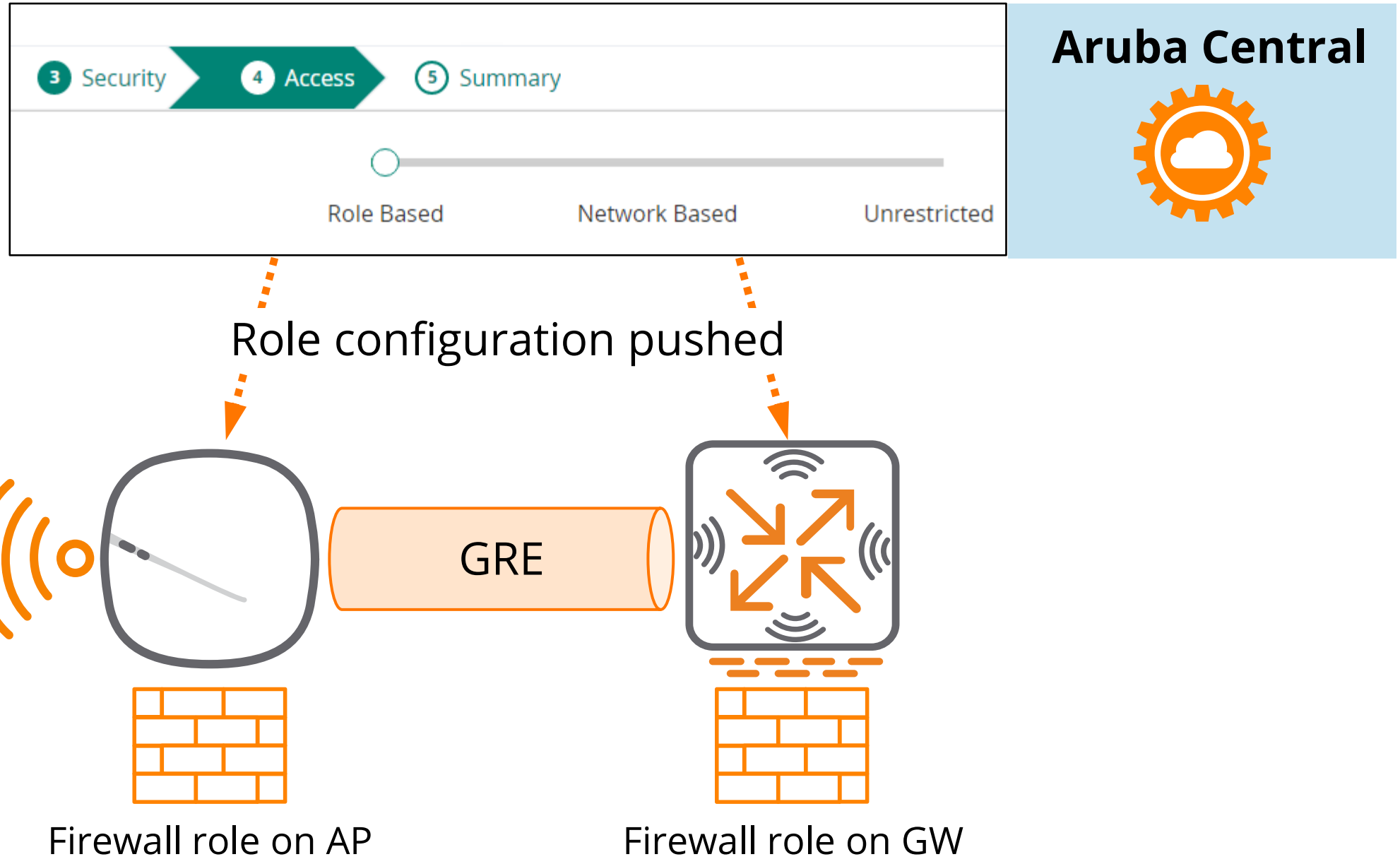


Role-Based ArubaOS Firewall



Same network subnet
Same destination and application
Different User = different handling

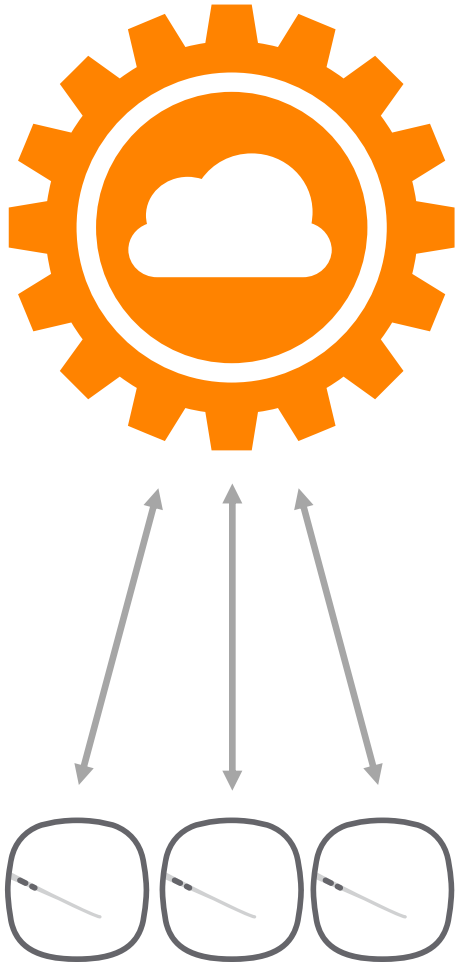
Firewall Roles in Tunneled Mode



Survivability

Aruba AOS10 Architecture: Responsibilities

Central	Management	Device config, Firmware mgmt
	Control	ClientMatch, AirMatch
	Services	Key Mgmt,AirGroup, RAPIDS, UCC
APs	Authenticator	Users and devices
	User Data	Forward, encrypt/decrypt
	Telemetry	Feed AP info to Central



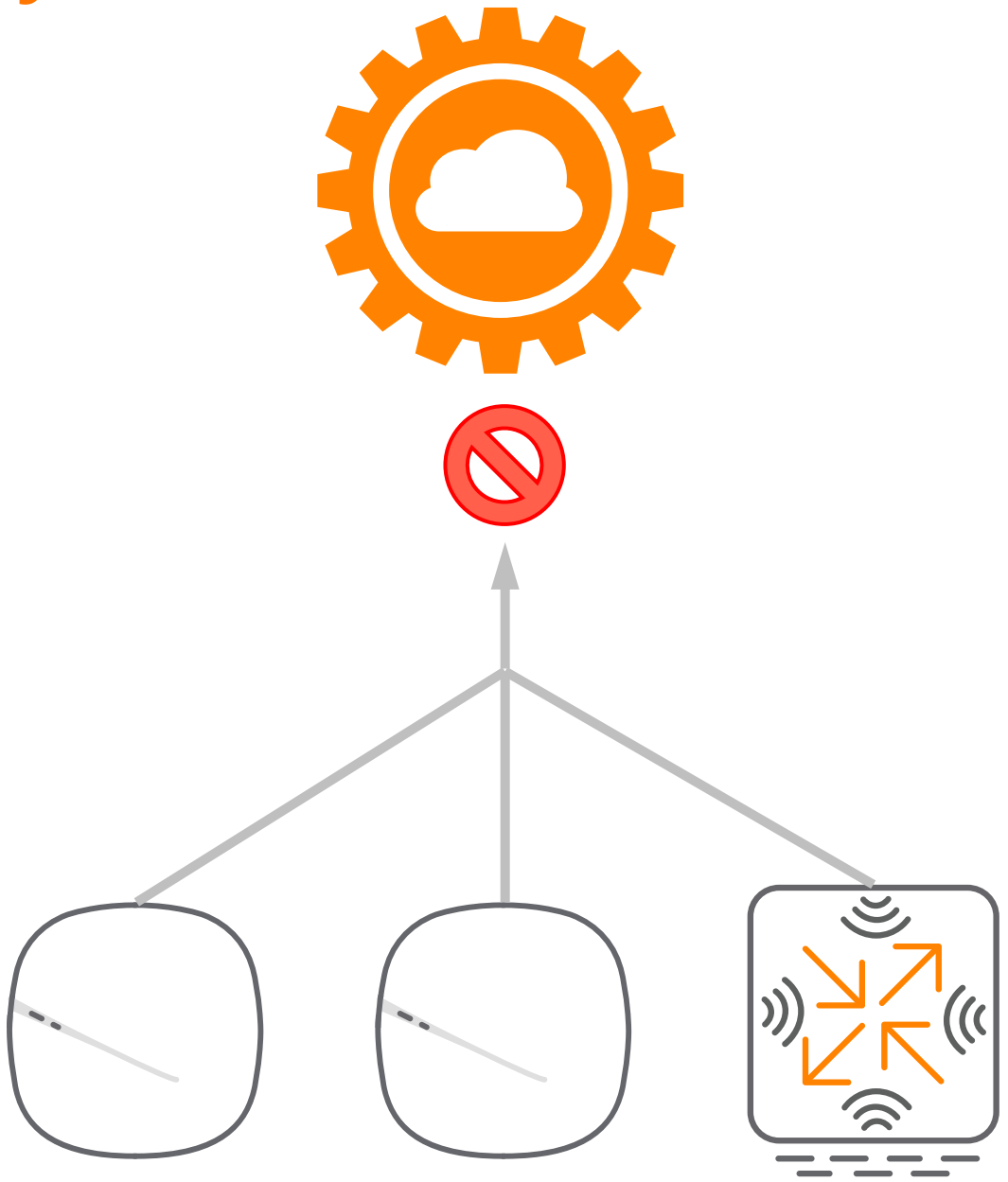
Key Management Survivability

Existing users

- Can continuously do fast roaming
- PMK or R1 keys exist for 8 hours

New users

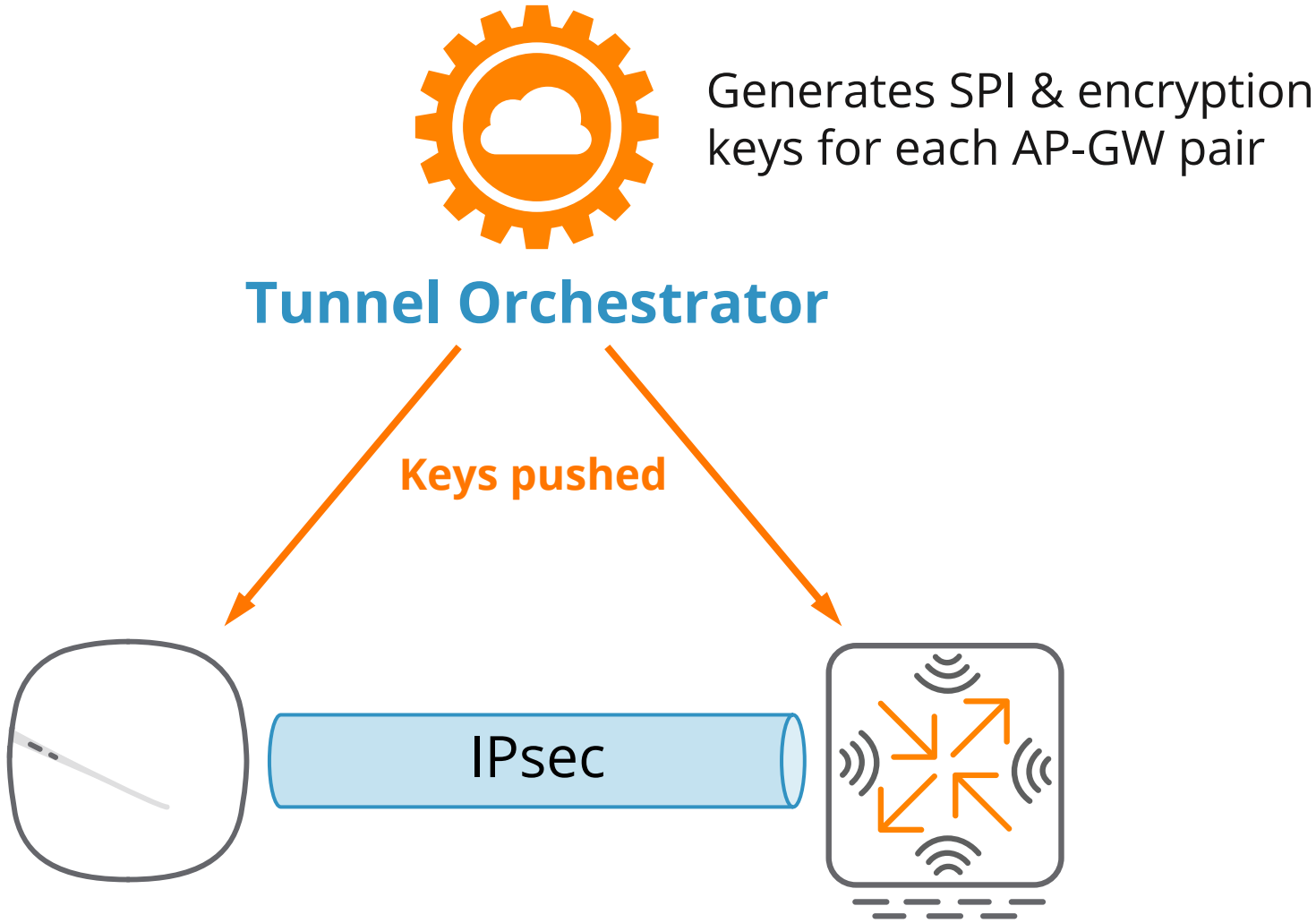
- PMK or R1 keys not shared between APs
- Must re-authenticate when roaming



Tunnels Rekeying

Keys

- Valid for 36h / AP-GW
- 12h before expiration, new keys are generated

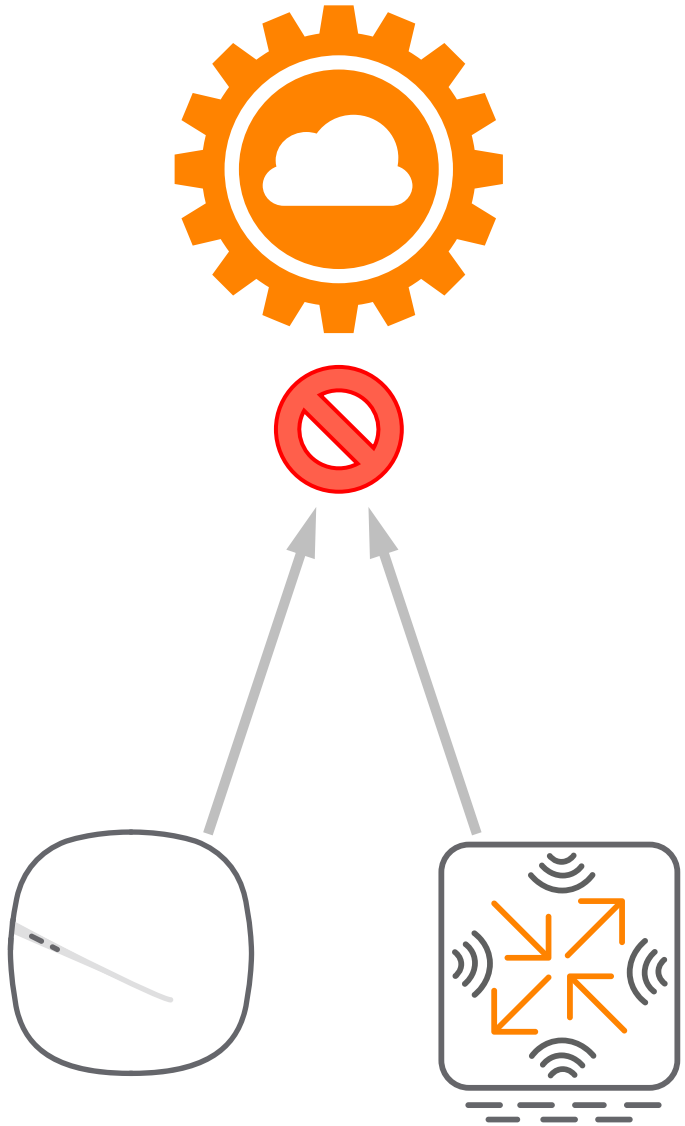


Tunnels Survivability

Initial Orchestration — Cloud is mandatory for initial tunnel orchestration

Survivability — Tunnel config from tunnel orchestrator is preserved in both AP and GW

Legacy Mode — When both AP & GW fails rekeying, AP and GW start legacy IKE process



Wired Port Access & Dynamic Segmentation

aruba
a Hewlett Packard Enterprise company
EDUCATION SERVICES

Common Authentication Methods

802.1X

- Supports bi-directional authentication
- Usernames/passwords and/or certificates
- Commonly used for employees

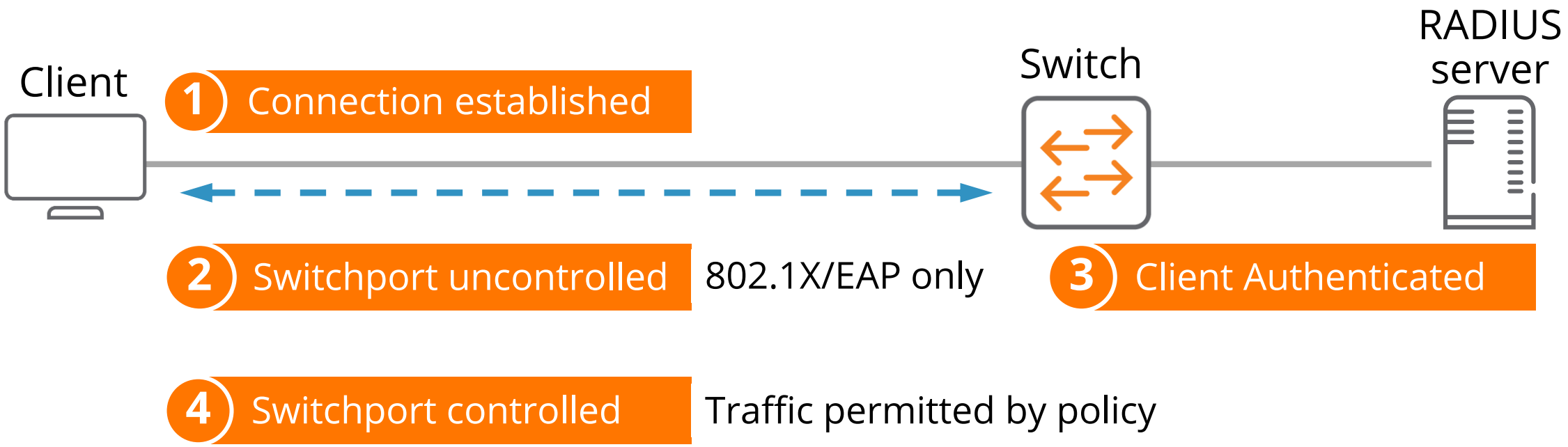
MAC Auth

- Must manage MAC address DB
- Subject to spoofing, augment with ACLs and fingerprinting
- Commonly used for non-intelligent devices, like IoT

Web Portal

- Commonly used in guest networks
- User device uses a web browser to authenticate
- Commonly used for guests

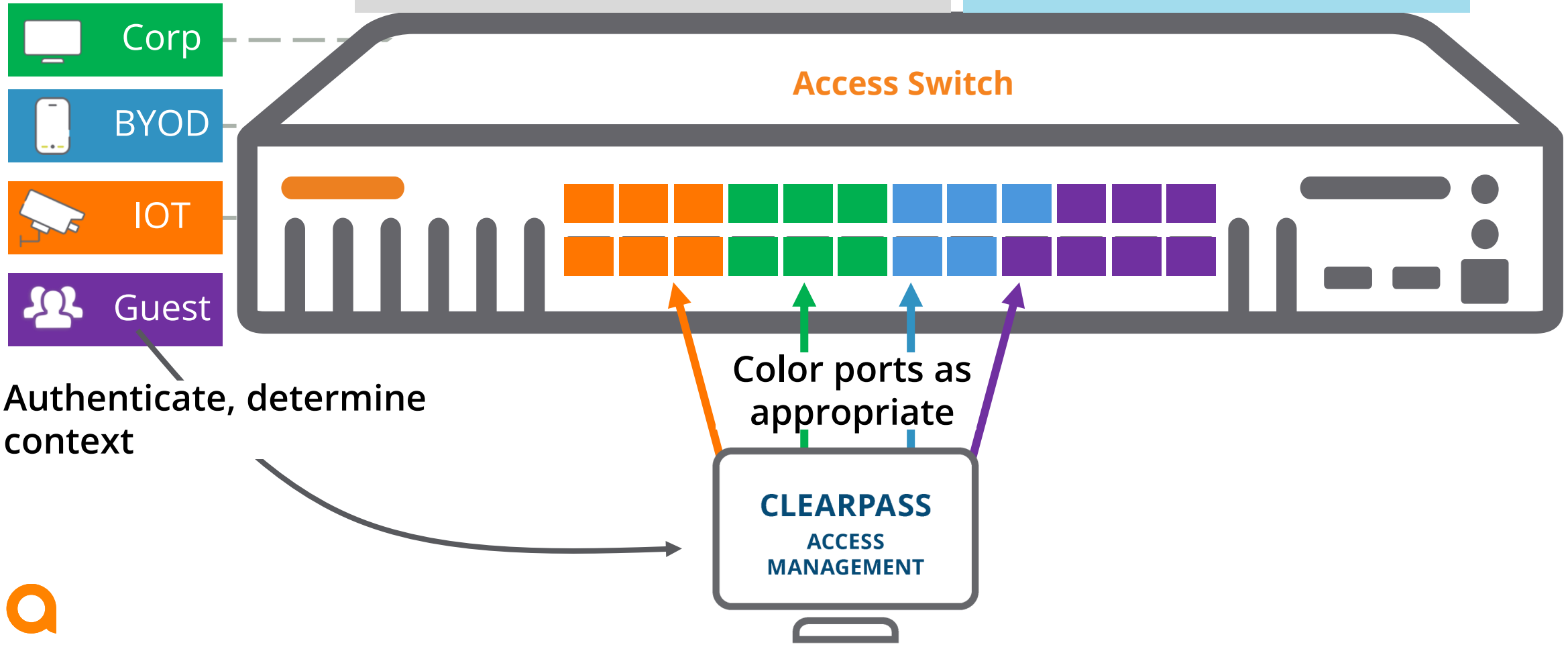
802.1X Overview



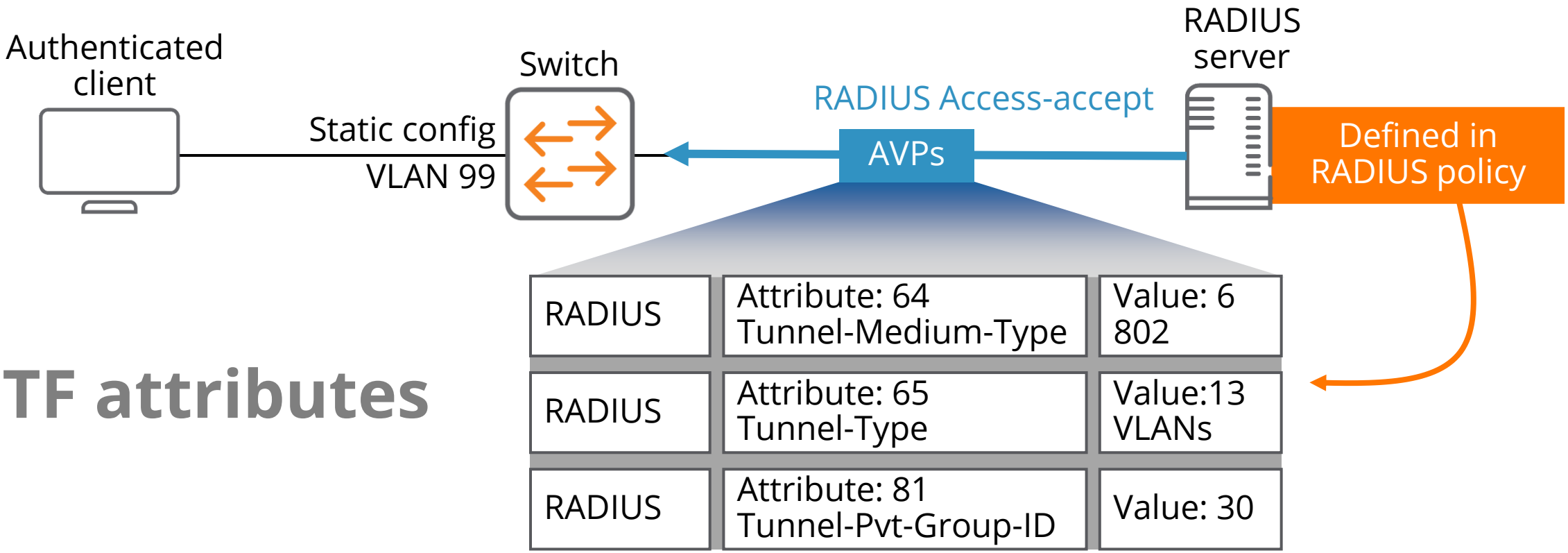
Customizing Authenticated User Access

Legacy: Manually configure ports
- VLAN, ACLs, QoS
- Tedious and error prone

Modern: Colorless ports
- Minimally configured
- Automated, easy, scalable



How the RADIUS Server Sends Dynamic Settings

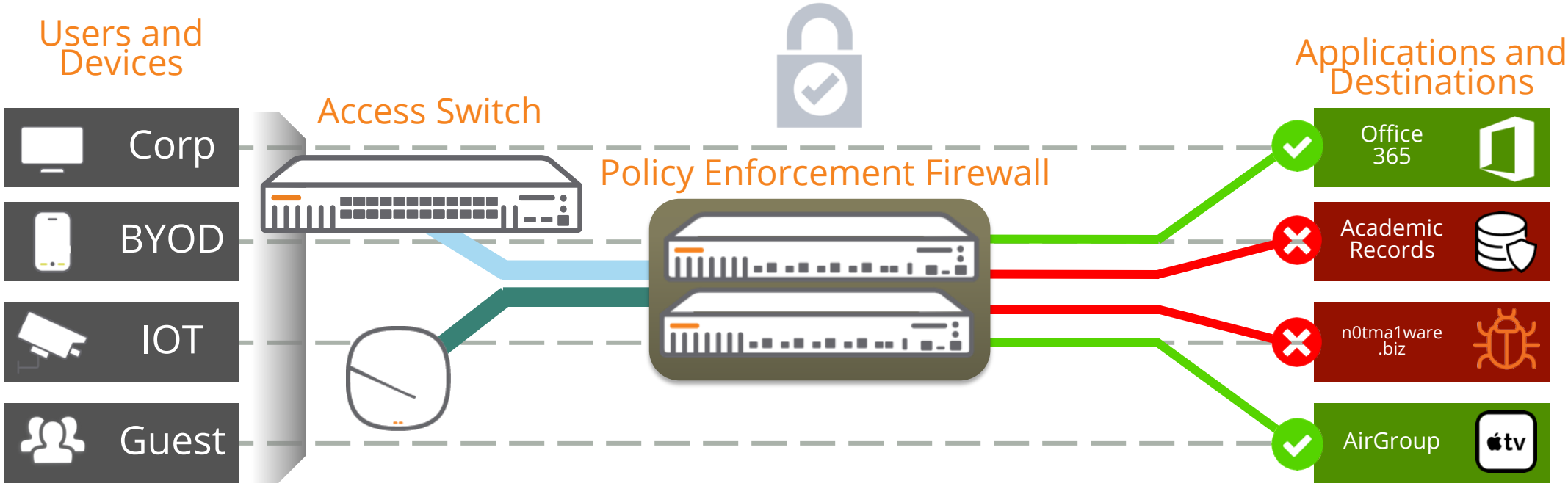


IETF attributes

Aruba VSAs

Aruba-User-Role=employee	Assign user role to a client
Aruba-Poe-Priority=0	Set port POE priority

Dynamic Segmentation



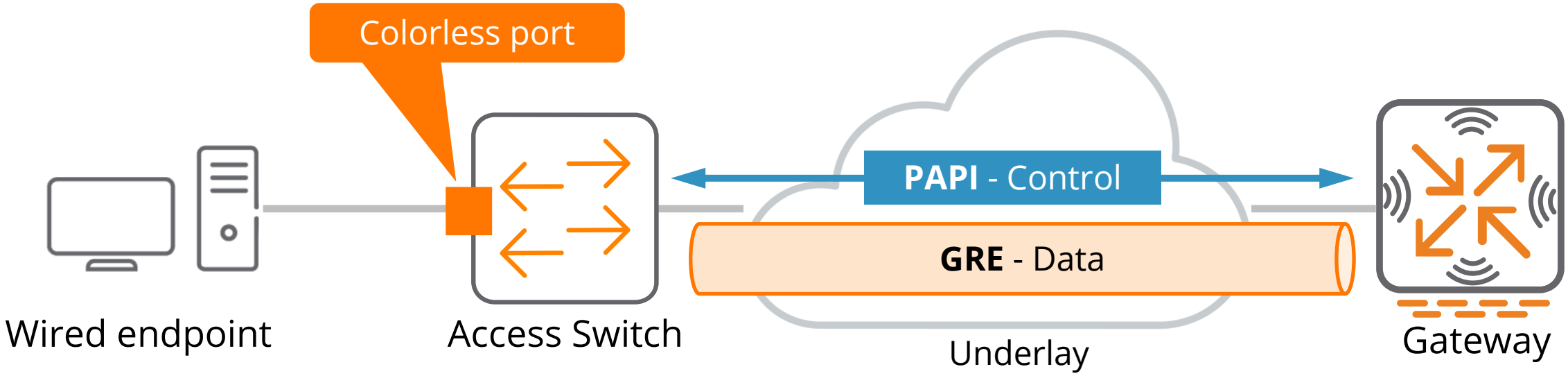
User capabilities are centrally controlled

VLANs, security, and QoS are dynamically assigned

Tighter security, fewer config / mgmt. cycles

Dynamic Segmentation Overview

- ✓ Consistent wireless and wired network security
- ✓ Centralized role-based policy enforcement
- ✓ Access to Aruba gateway security features
- ✓ Redundant gateway and cluster support



Use Cases

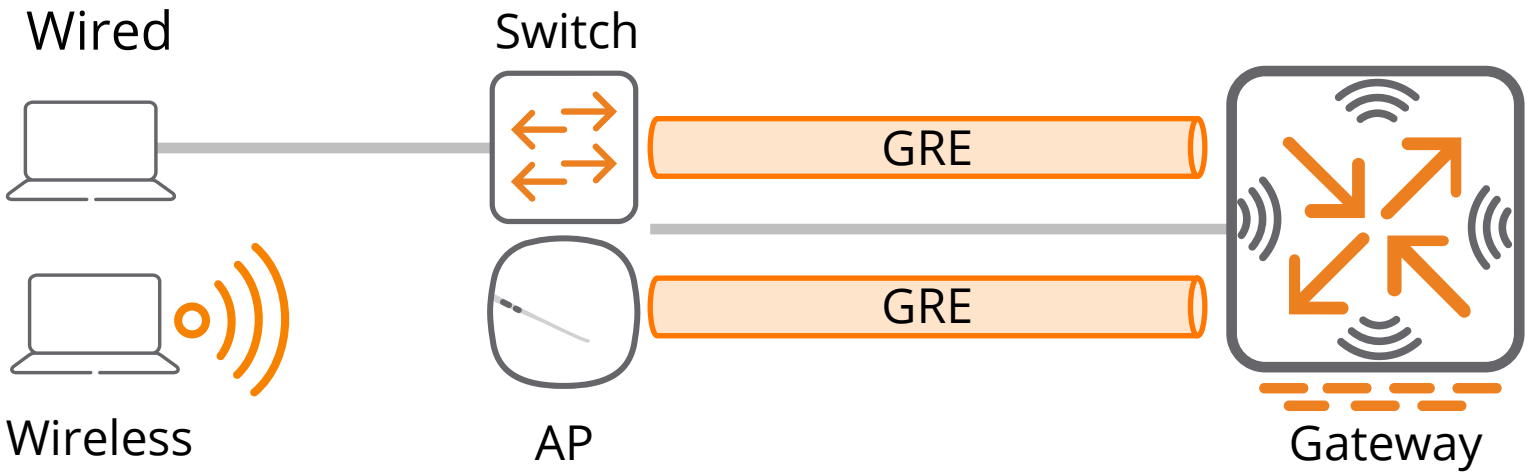
Wired/wireless traffic tunneled to Gateway

- ✓ Consistent user experience
- ✓ Centralized, role-based enforcement

RADIUS

CLEARPASS

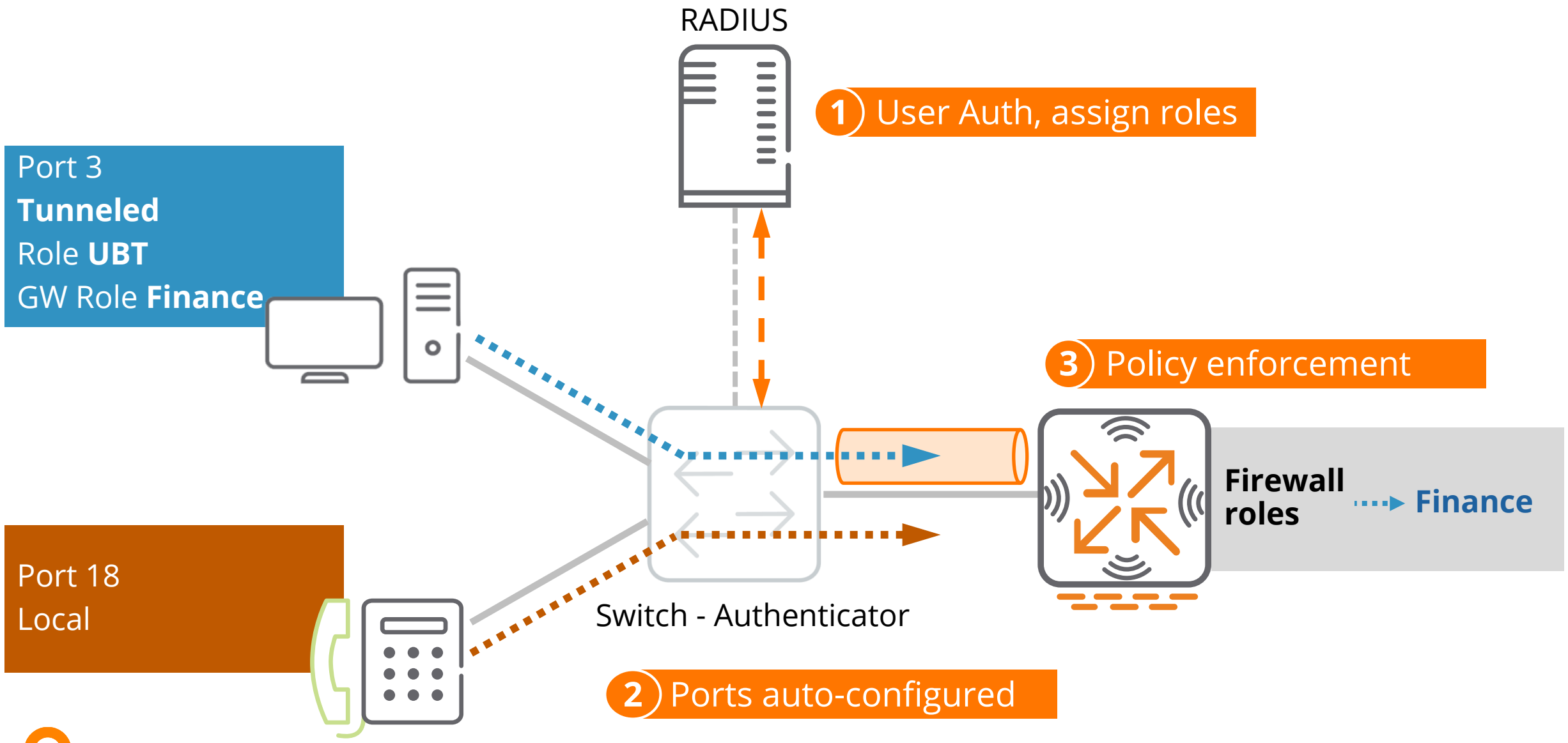
POLICY MANAGEMENT



Security features applied to wired and wireless traffic

- Stateful firewall
- Deep packet inspection
- Device fingerprinting

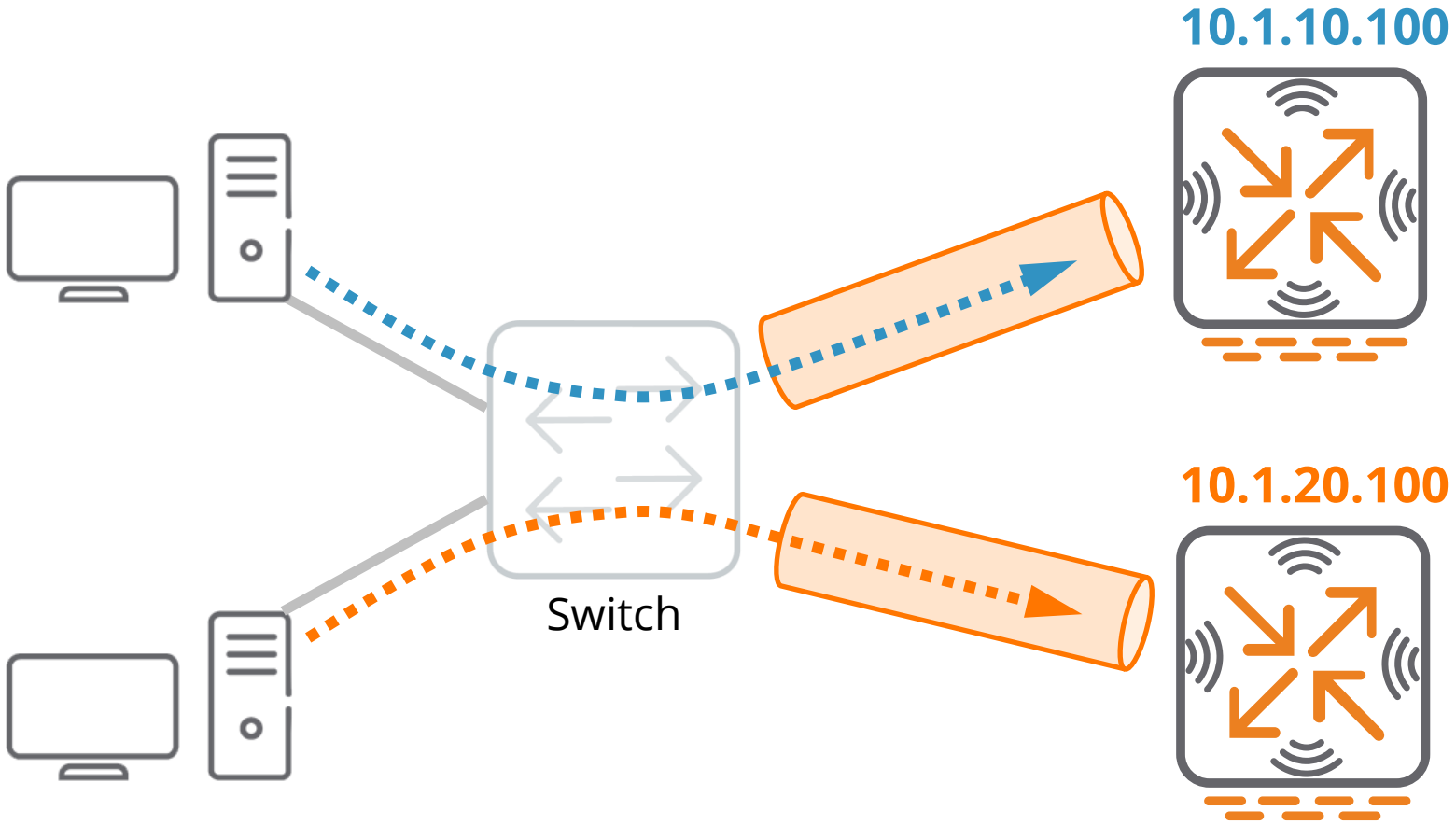
Operation Overview



UBT Zones

```
port-access role Employee
 gateway-zone zone Building1
```

```
port-access role Contractor
 gateway-zone zone Building2
```




```
ubt zone Building1
  primary-controller ip 10.1.10.100
ubt zone Building2
  primary-controller ip 10.1.20.100
```

UBT clients terminate on different Gateways

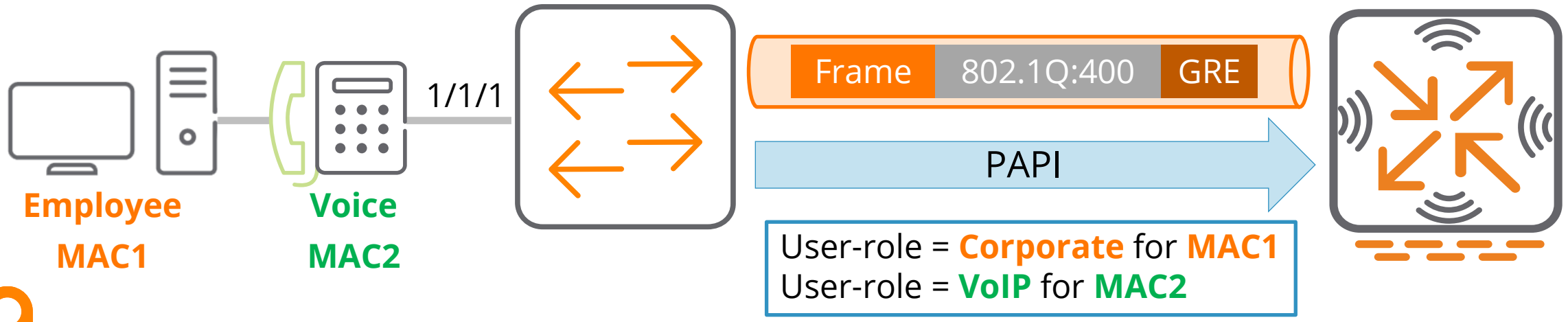
Tunneled Traffic Behavior: Multiple clients

Switch communicates gateway roles

```
ubt-client-vlan 400
port-access role Employee
 gateway-zone zone zone1 gateway-role Corporate
port-access role Voice
 gateway-zone zone zone1 gateway-role VoIP
```

Gateway applies policy and VLAN

```
User-role Corporate
  Policy 1
  Policy 2
  vlan 4000
User-role VoIP
  Policy 1
  Policy 2
  vlan 3000
```

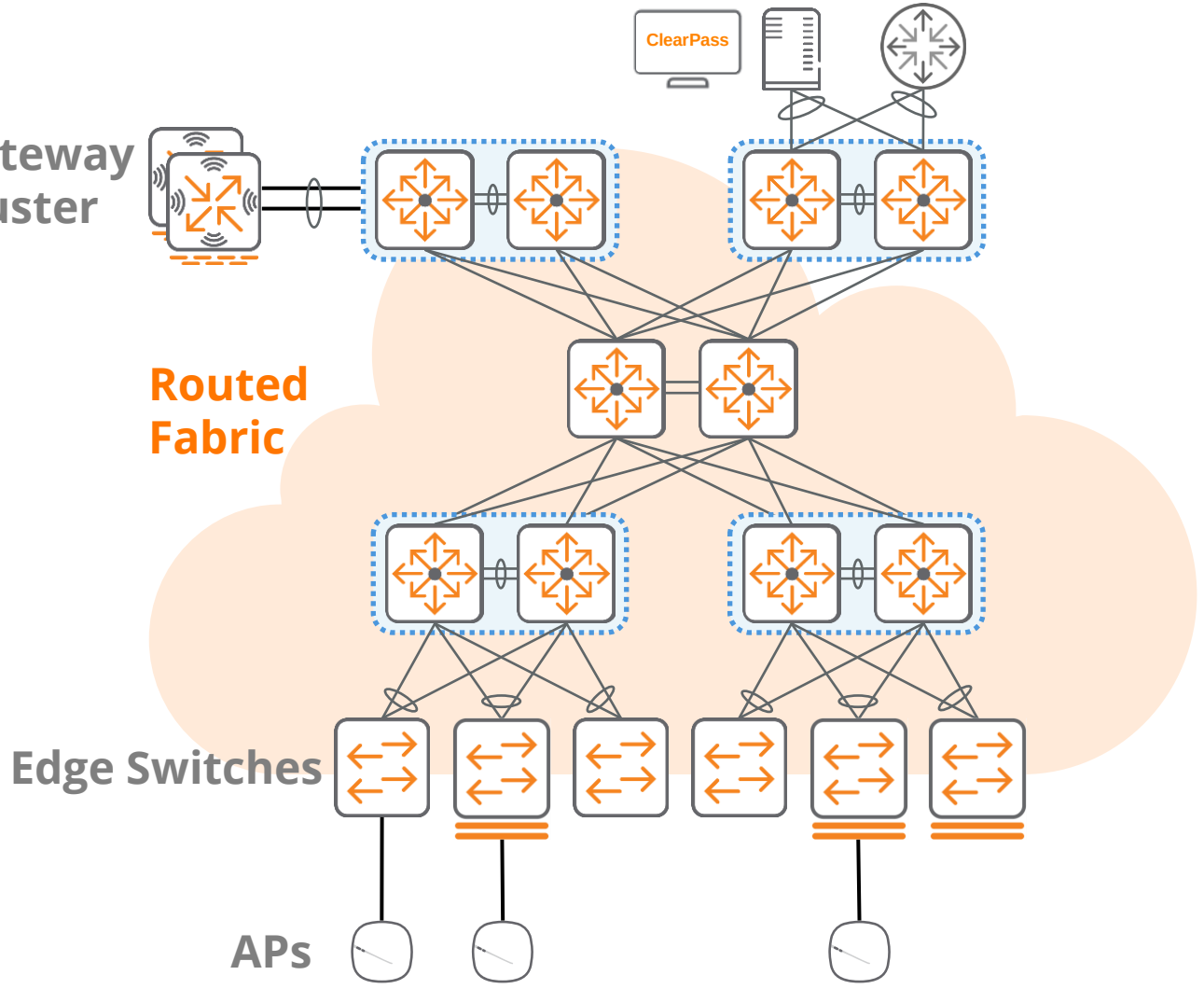


VxLAN & GBP

aruba
a Hewlett Packard Enterprise company
EDUCATION SERVICES

Distributed Overlay Architecture

- Uniform bridging & routing across a campus topology
- End-to-end segmentation using VXLAN-GBP
- Efficient layer 2 extension across layer 3 boundaries
- Transported across any IP network
- Stable, predictable IP based backbone (no STP)



VXLAN Characteristics

Usage

- Focused on data centers & Aruba Campus
- IP-based overlay technology

Overlay

- MAC in UDP (IP) format
- Runs on any IP routed infrastructure

Scaling

- Can leverage IP ECMP for load sharing
- 24-bit VXLAN ID: 16M IDs

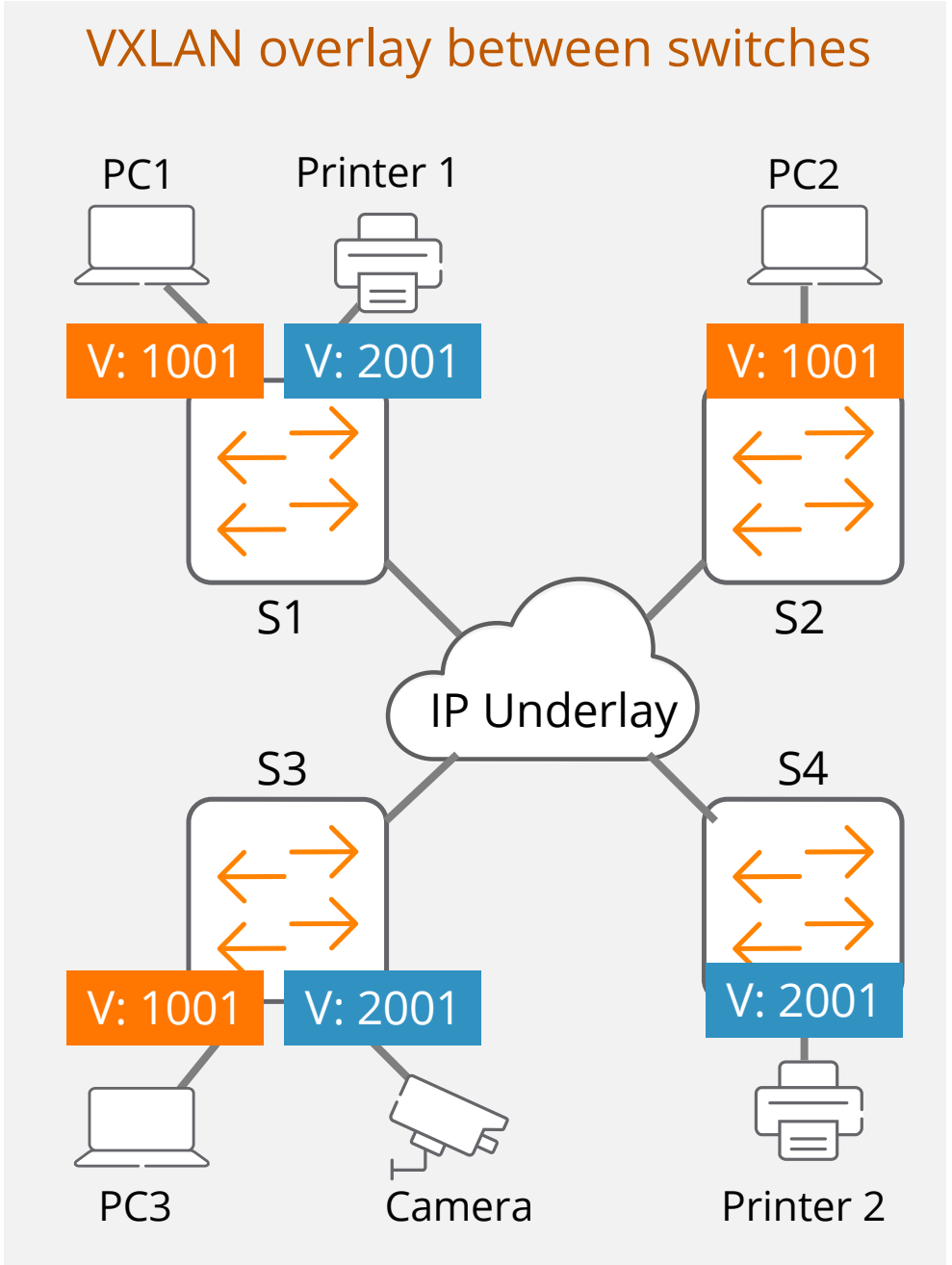
VXLAN Terminology

VXLAN

- Like classic VLAN without L3 IP Interface
- Totally isolated

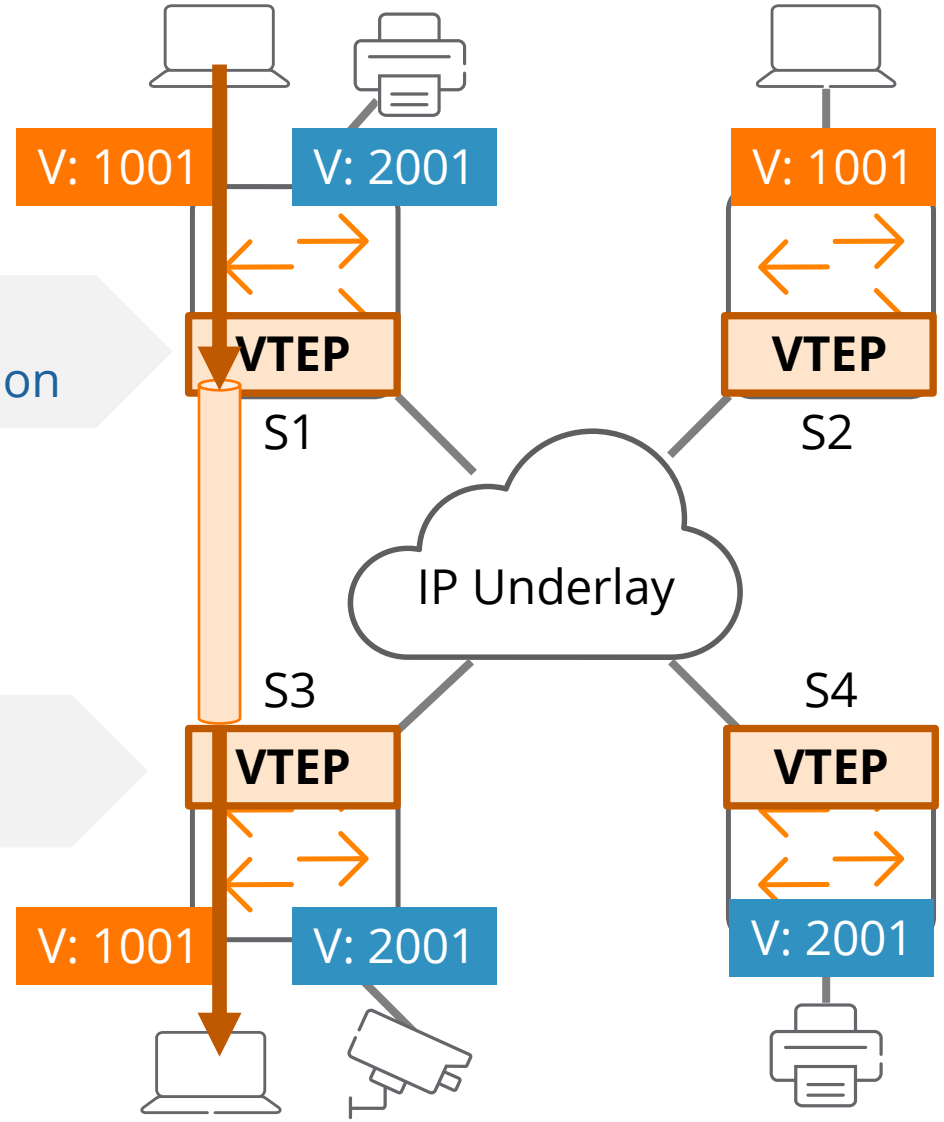
VNI

- VXLAN Network Identifier
- 24-bit value



VXLAN VTEP

- Entry or “on-ramp” into the tunnel
- Device that interacts with other VTEPs



VXLAN Packet Structure

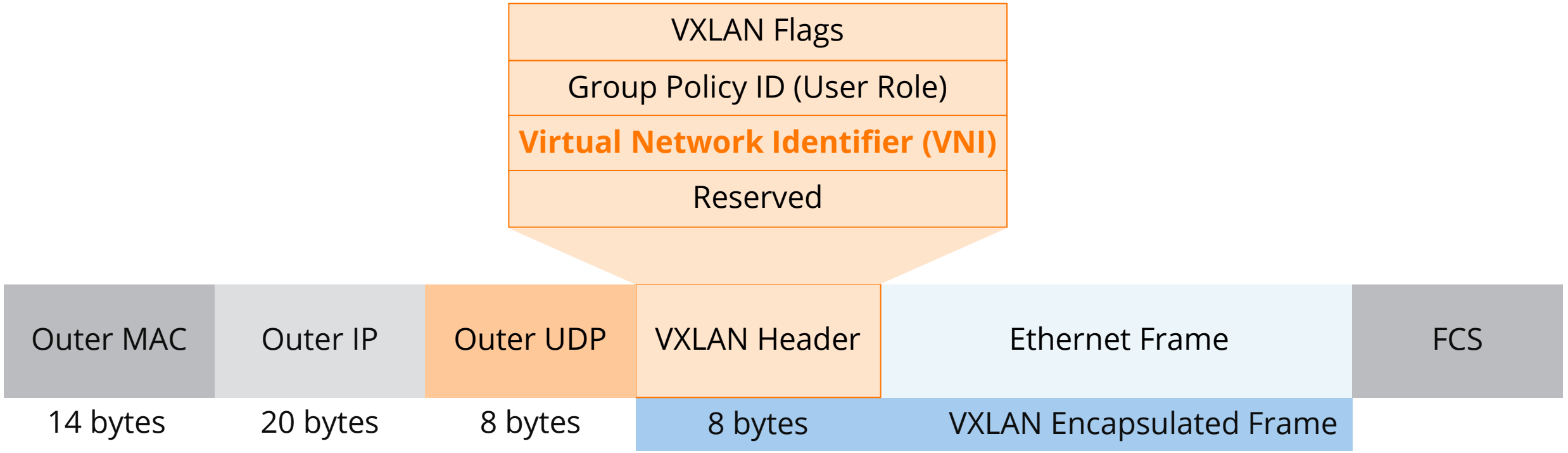
Header

- IP: 20 bytes
- UDP: 8 bytes
- **VNI: 3 Bytes (24 bits)**

50 bytes total

- 8 bytes VXLAN header
- 8 bytes UDP
- 20 bytes IP
- 14 bytes Ethernet

MTU greater than 1550 bytes

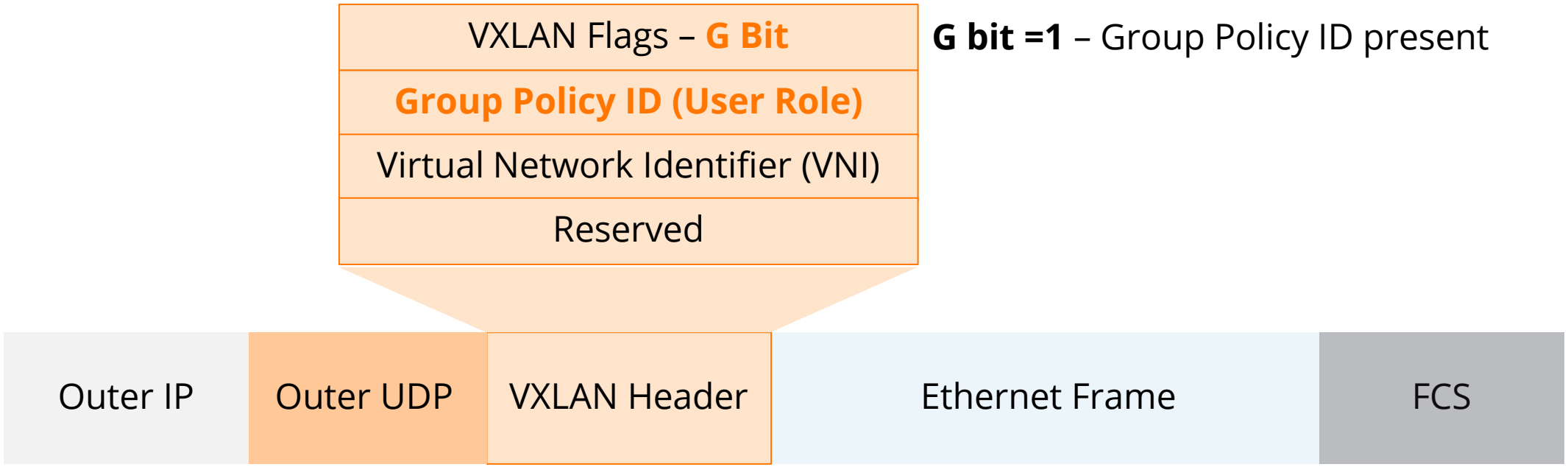


Aruba recommends enabling jumbo frames with VXLAN

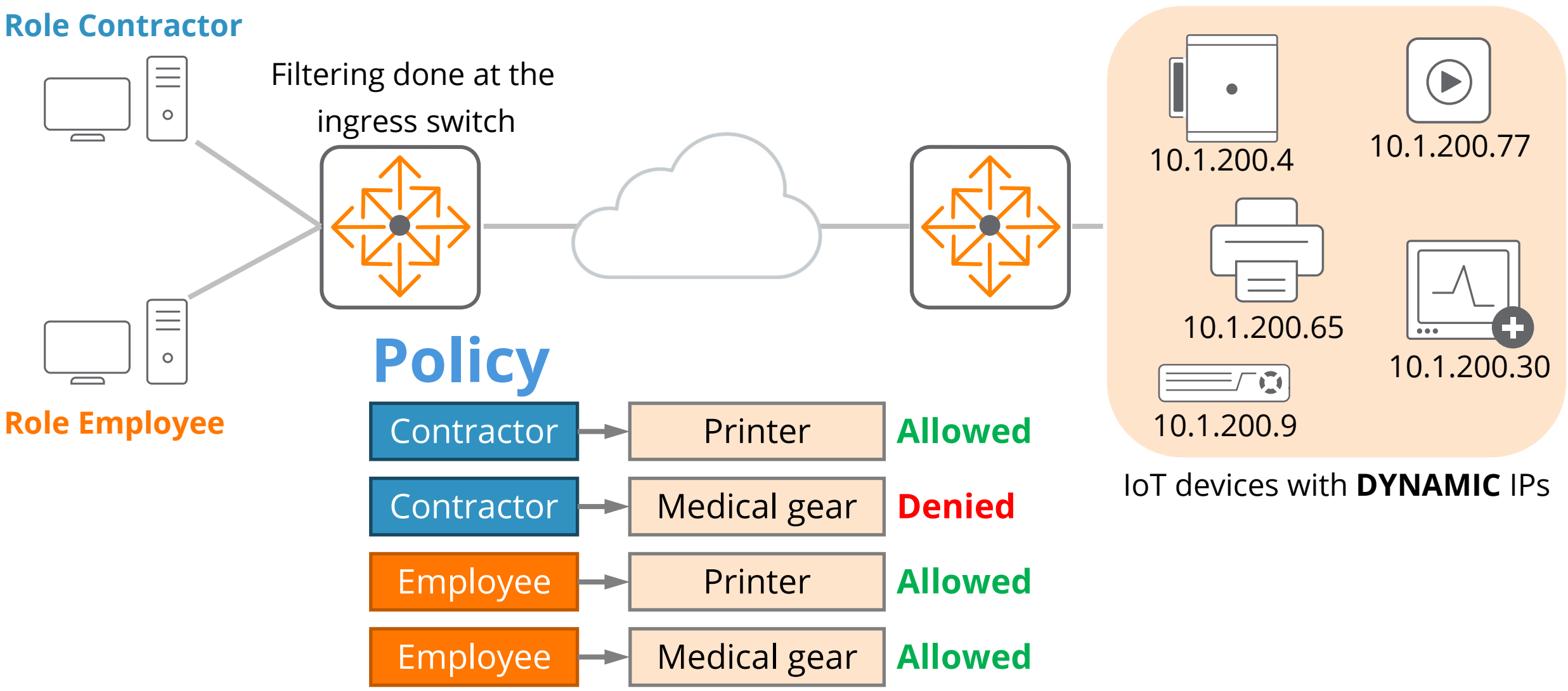
GBP Introduction

Enhances Campus VXLAN Virtual network based tunneling solution

Enables role-based policies Role based policies not tied to IP addresses



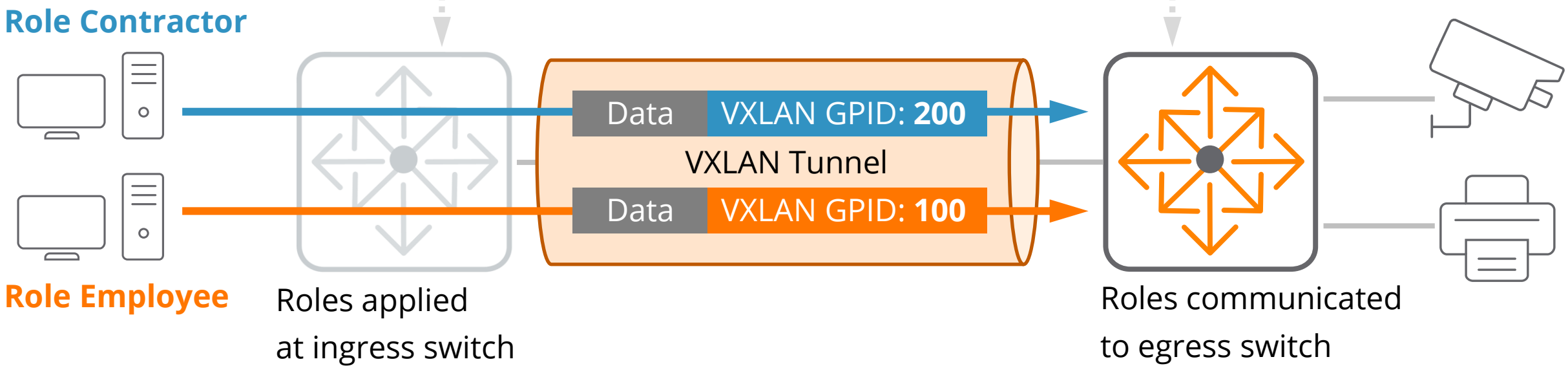
Problem with IP Based Policies



Impossible to implement with IP based policies

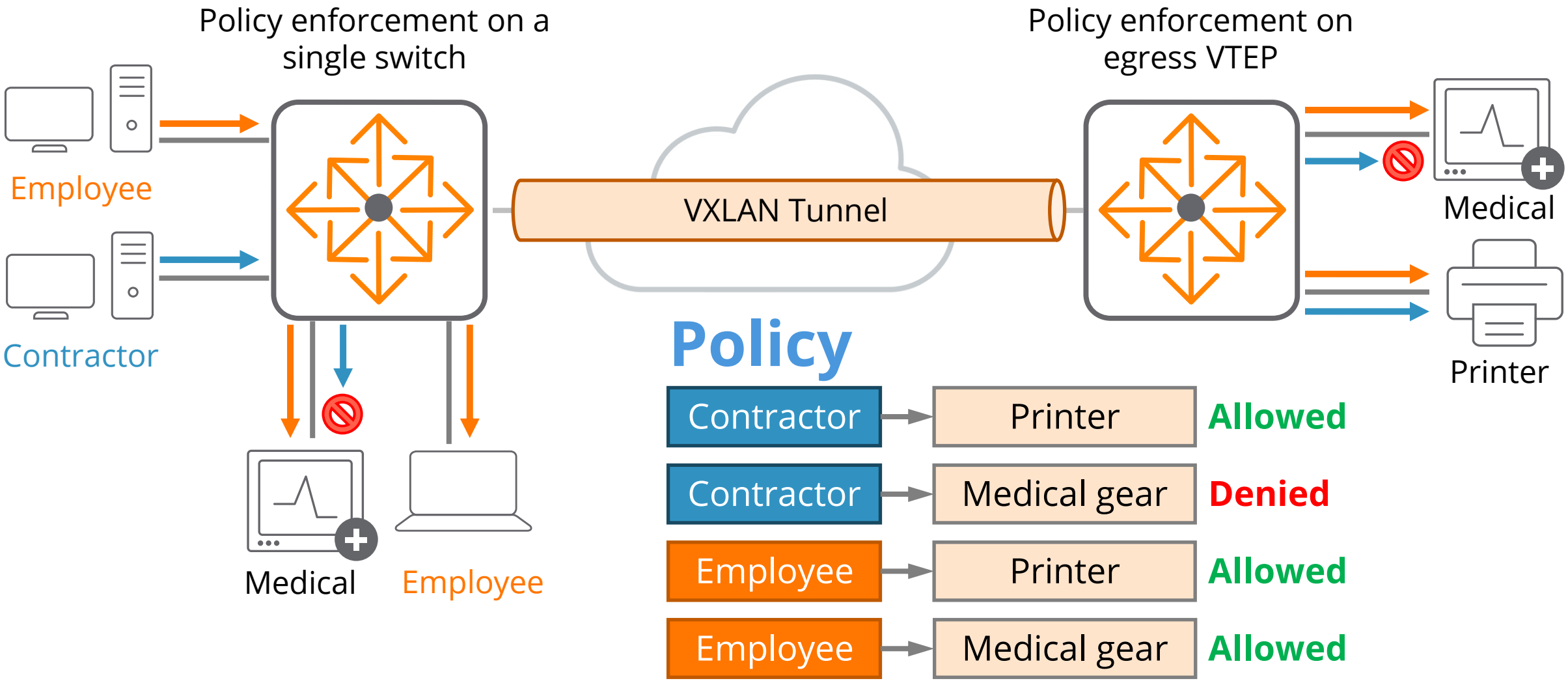
Role to Policy ID Mapping

```
gbp enable
gbp role-tag mapping Employee 100
gbp role-tag mapping Contractor 200
gbp role-tag mapping Camera 300
gbp role-tag mapping Printer 400
```



Role names are created locally on every required VTEP and mapped to Group Policy ID

Policy Enforcement: IP Independent



Clients with the same role – default **allowed**, clients with different role – default **denied**

NetConductor

Managing policies in large network can be challanging

Aruba NetConductor

Policy manager

- Defines user and device groups
- Creates the associated traffic routing and access enforcement rules for the physical network

Group policy identifier

- Carries configuration and client policy information
- Reduces configuration and security overhead
- Increases mobility and scalability.

Fabric wizard

- Simplifies the creation of the overlays
- Intuitive GUI
- Eases configuration of switches and gateways

Thank You !