Hewlett Packard
Enterprise

Dynamic segmentation mit EVPN-VXLAN

Łukasz Budzisz, Ph.D.,
ACEX #98 (ACMX, ACCX, ACDX)
SYSTEMS ENGINEER

March 2024

Hewlett Packard Enterprise

User roles and dynamic segmentation

Basic concepts

Simplify Secure Network Access For Users and Devices

TODAY

- Separate Wired and Wireless Policy
- Static Configuration of Wired LAN
- Segmentation is VLANs

SEPARATE, MANUAL

TIME CONSUMING, SECURITY RISK

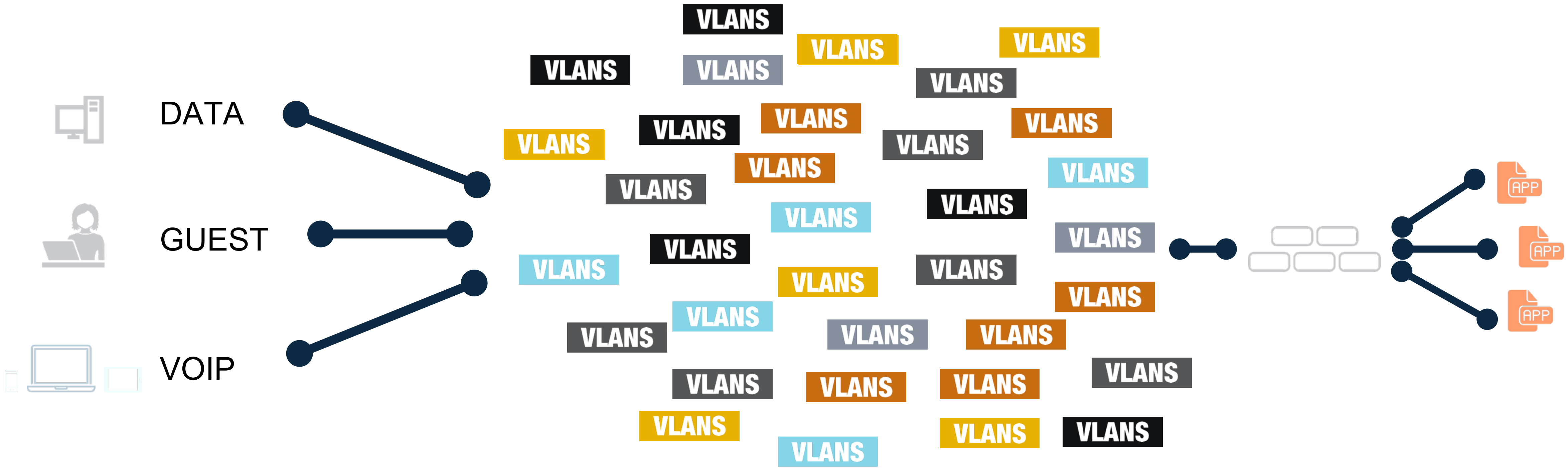
GOAL

- Unified, Role Based Policies
- Simplify Configurations
- Improve Segmentation

BETTER USER EXPERIENCE AND SECURITY POSTURE, FASTER, DYNAMIC

“VLANs are COOL!”*

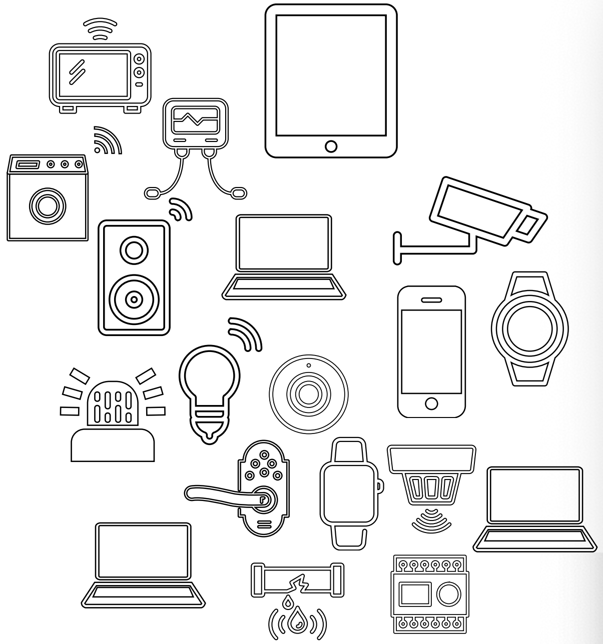
* = IT Manager back in 1998...



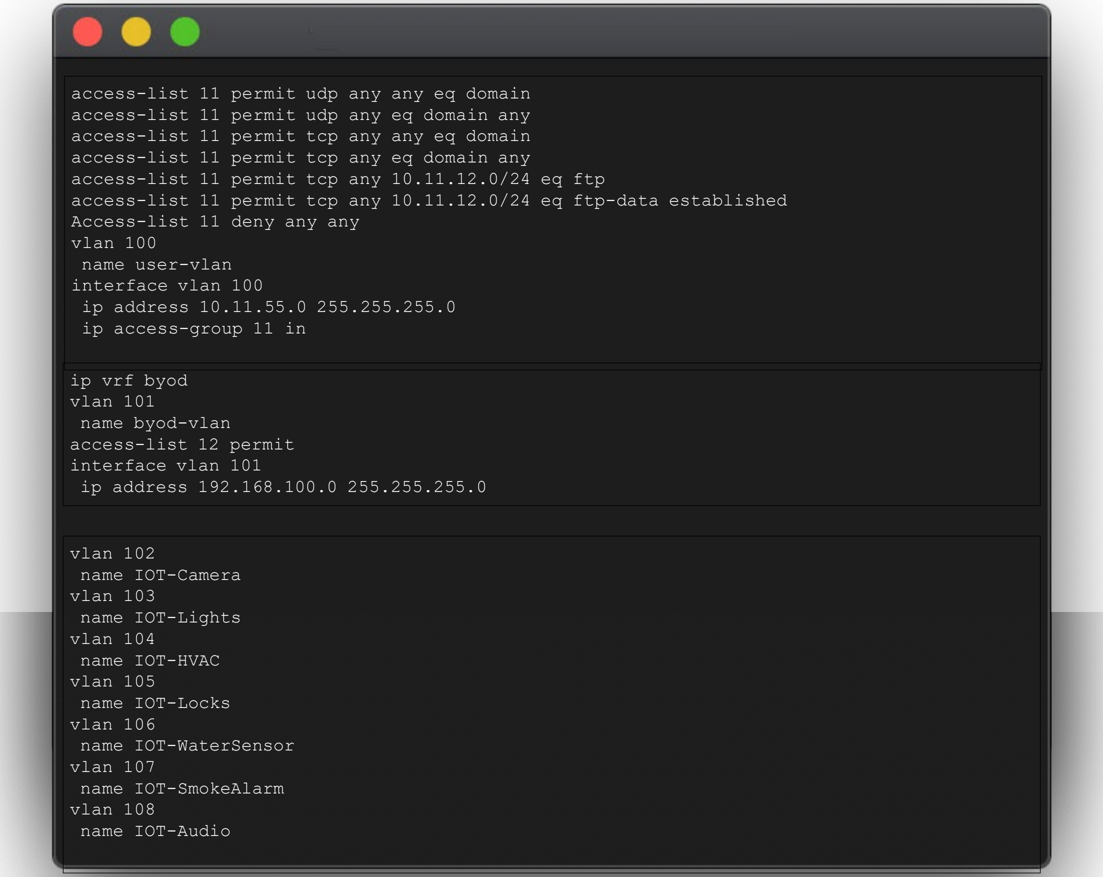
- Complex and inefficient
- Extensive static, manual configuration
- Leads to VLAN sprawl and poor IPAM usage

“LEGACY” NETWORK SEGMENTATION

(B.A.)



EMPLOYEES
BYOD
IOT



```
access-list 11 permit udp any any eq domain
access-list 11 permit udp any eq domain any
access-list 11 permit tcp any any eq domain
access-list 11 permit tcp any eq domain any
access-list 11 permit tcp any 10.11.12.0/24 eq ftp
access-list 11 permit tcp any 10.11.12.0/24 eq ftp-data established
Access-list 11 deny any any
vlan 100
 name user-vlan
interface vlan 100
 ip address 10.11.55.0 255.255.255.0
 ip access-group 11 in
```

```
ip vrf byod
vlan 101
 name byod-vlan
access-list 12 permit
interface vlan 101
 ip address 192.168.100.0 255.255.255.0
```

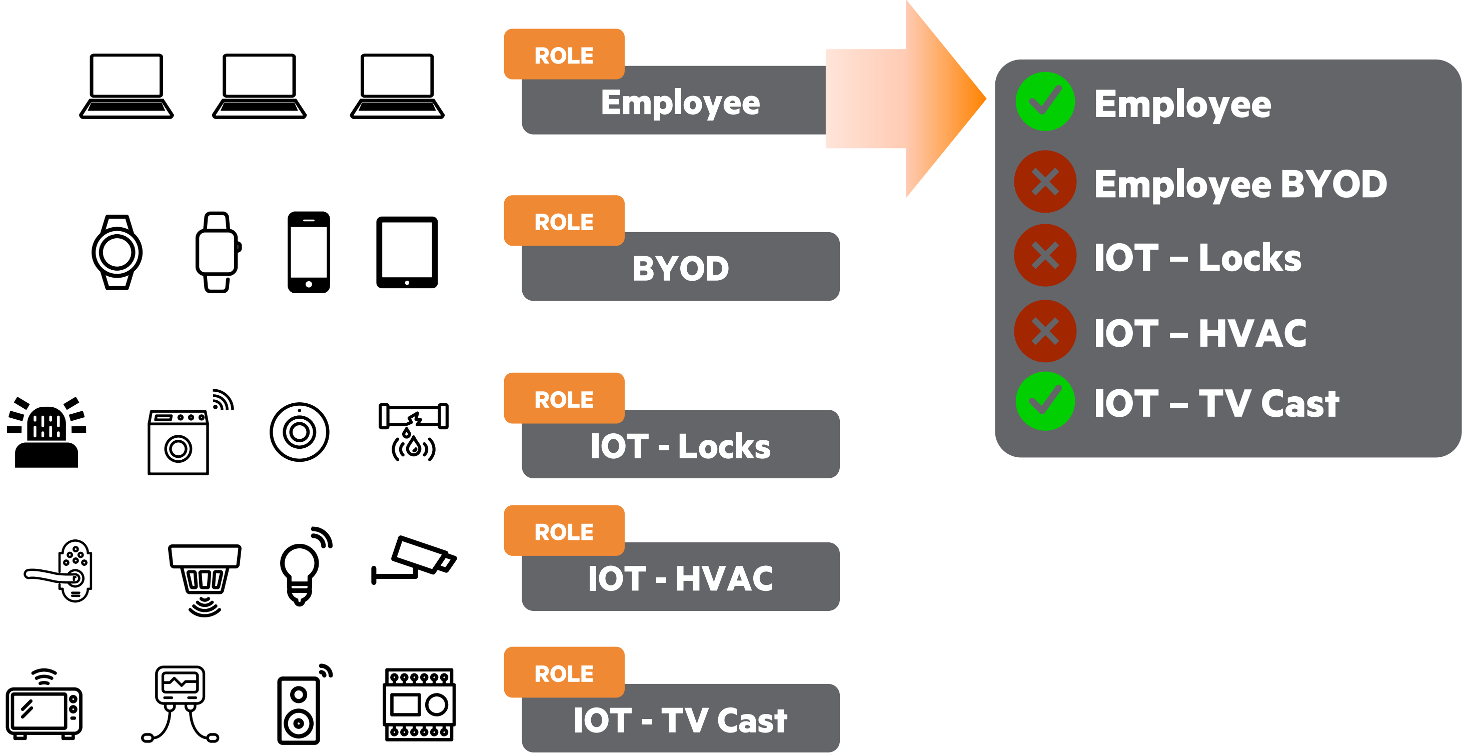
```
vlan 102
 name IOT-Camera
vlan 103
 name IOT-Lights
vlan 104
 name IOT-HVAC
vlan 105
 name IOT-Locks
vlan 106
 name IOT-WaterSensor
vlan 107
 name IOT-SmokeAlarm
vlan 108
 name IOT-Audio
```

Complex hop-by-hop segmentation configuration slows the deployment of new devices on the network

ACLs either become unmanageable or are non-existent ultimately leading back to security struggles

A ZERO TRUST FRAMEWORK

SECURES AND SIMPLIFIES



ROLE Employee

ROLE BYOD

ROLE IOT - Locks

ROLE IOT - HVAC

ROLE IOT - TV Cast

- ✓ Employee
- ✗ Employee BYOD
- ✗ IOT – Locks
- ✗ IOT – HVAC
- ✓ IOT – TV Cast

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's User Roles

What Are User-Roles

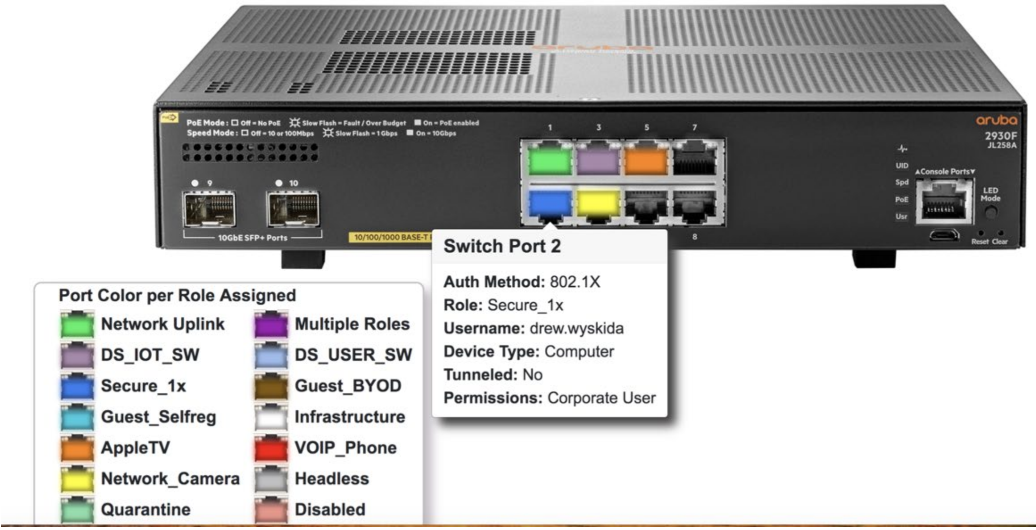
- A container for policy and security
- ***Exist for ~20 years in Aruba products!***

How to Apply User-Roles

- Applied upon authentication
  - dynamically
  - statically

Benefits

- Policy based on role configuration
- No pre-configuration needed
- Associated to the client not the physical port



Port Color per Role Assigned

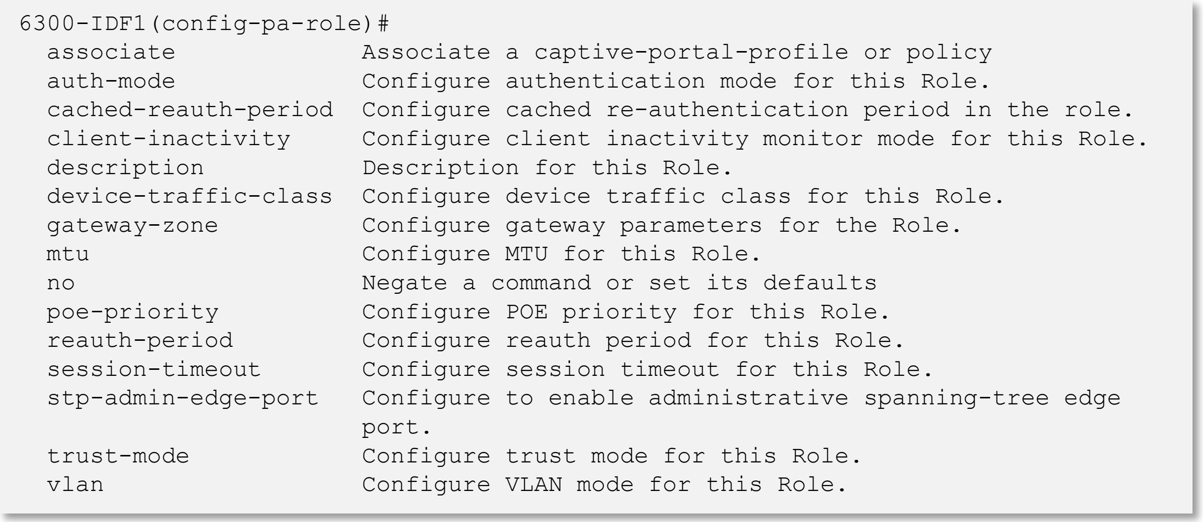
- 🟩 Network Uplink
- 🟪 DS_IOT_SW
- 🟦 Secure_1x
- 🟦 Guest_Selfreg
- 🟧 AppleTV
- 🟨 Network_Camera
- 🟩 Quarantine
- 🟪 Multiple Roles
- 🟦 DS_USER_SW
- 🟫 Guest_BYOD
- ⬜ Infrastructure
- 🟥 VOIP_Phone
- ⬜ Headless
- 🟥 Disabled

Switch Port 2

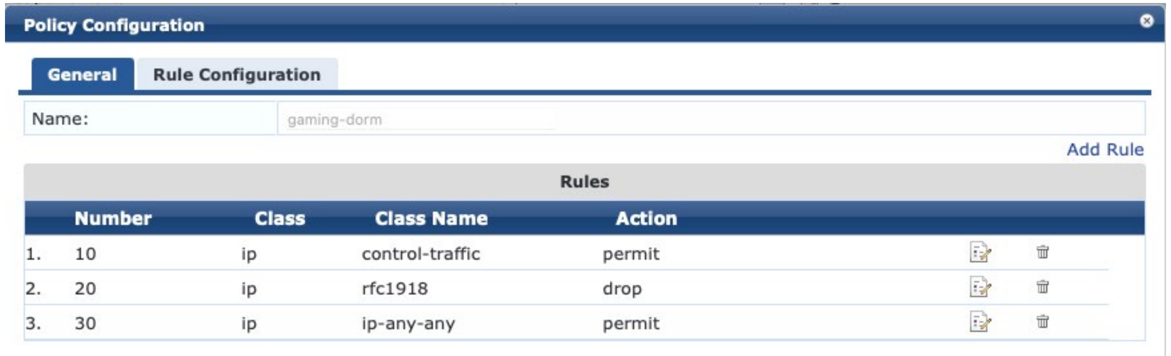
Auth Method: 802.1X
Role: Secure_1x
Username: drew.wyskida
Device Type: Computer
Tunneled: No
Permissions: Corporate User

```
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
```

Aruba Role



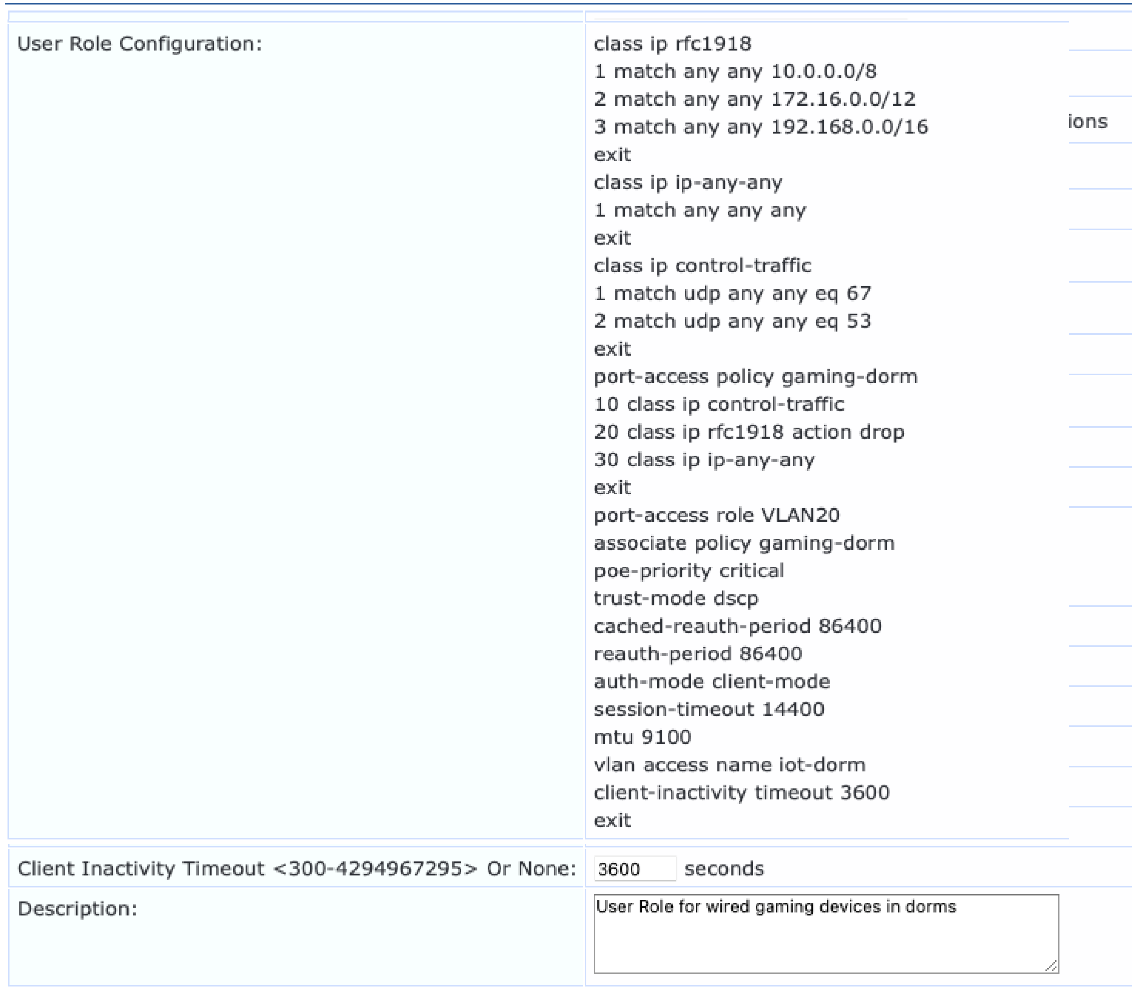
```
6300-IDF1(config-pa-role)#
  associate              Associate a captive-portal-profile or policy
  auth-mode              Configure authentication mode for this Role.
  cached-reauth-period   Configure cached re-authentication period in the role.
  client-inactivity      Configure client inactivity monitor mode for this Role.
  description            Description for this Role.
  device-traffic-class   Configure device traffic class for this Role.
  gateway-zone           Configure gateway parameters for the Role.
  mtu                    Configure MTU for this Role.
  no                     Negate a command or set its defaults
  poe-priority           Configure POE priority for this Role.
  reauth-period          Configure reauth period for this Role.
  session-timeout        Configure session timeout for this Role.
  stp-admin-edge-port    Configure to enable administrative spanning-tree edge
                         port.
  trust-mode             Configure trust mode for this Role.
  vlan                   Configure VLAN mode for this Role.
```



Name: gaming-dorm

Rules

	Number	Class	Class Name	Action
1.	10	ip	control-traffic	permit
2.	20	ip	rfc1918	drop
3.	30	ip	ip-any-any	permit



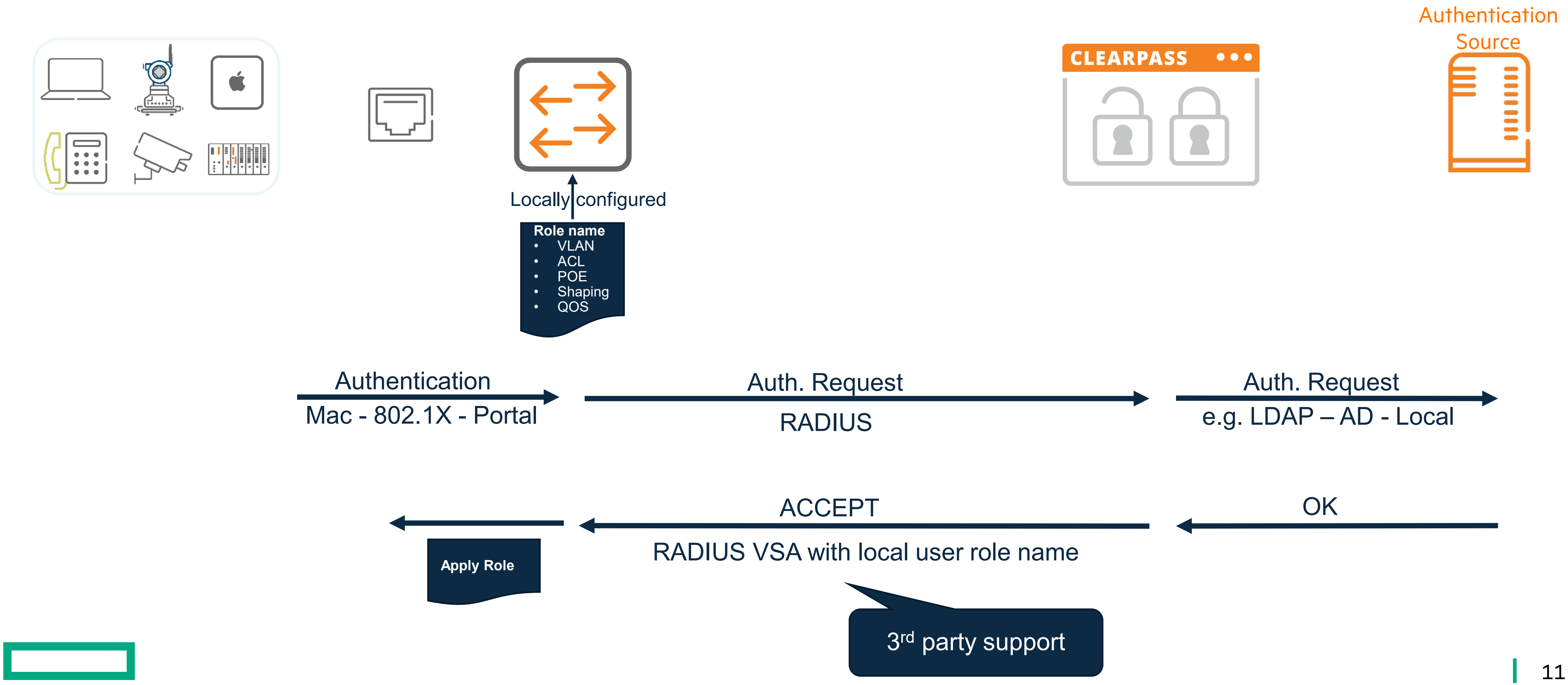
User Role Configuration:

```
class ip rfc1918
1 match any any 10.0.0.0/8
2 match any any 172.16.0.0/12
3 match any any 192.168.0.0/16
exit
class ip ip-any-any
1 match any any any
exit
class ip control-traffic
1 match udp any any eq 67
2 match udp any any eq 53
exit
port-access policy gaming-dorm
10 class ip control-traffic
20 class ip rfc1918 action drop
30 class ip ip-any-any
exit
port-access role VLAN20
associate policy gaming-dorm
poe-priority critical
trust-mode dscp
cached-reauth-period 86400
reauth-period 86400
auth-mode client-mode
session-timeout 14400
mtu 9100
vlan access name iot-dorm
client-inactivity timeout 3600
exit
```

Client Inactivity Timeout <300-4294967295> Or None: 3600 seconds

Description: User Role for wired gaming devices in dorms

Local user roles



Authentication Source

Locally configured

Role name

- VLAN
- ACL
- POE
- Shaping
- QOS

Authentication

Mac - 802.1X - Portal

Auth. Request

RADIUS

Auth. Request

e.g. LDAP – AD - Local

ACCEPT

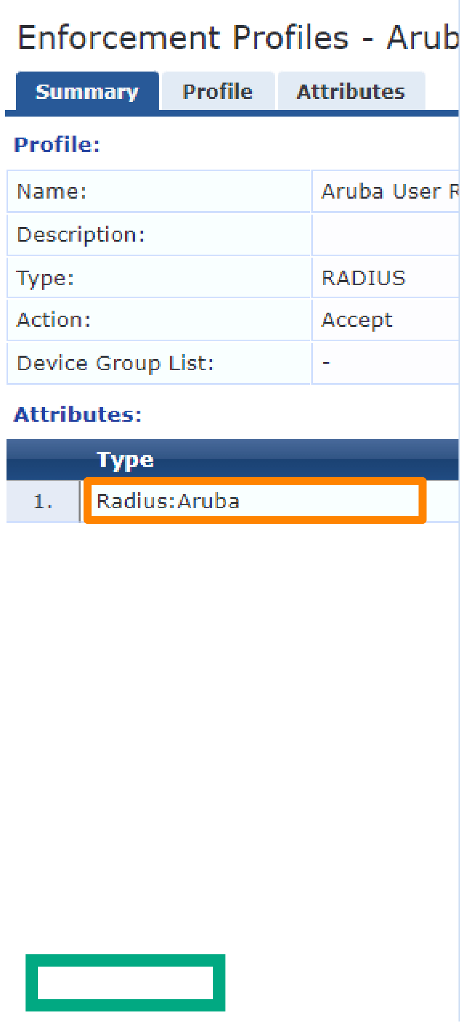
RADIUS VSA with local user role name

OK

Apply Role

3rd party support

Any Radius Server vs. ClearPass (Dow



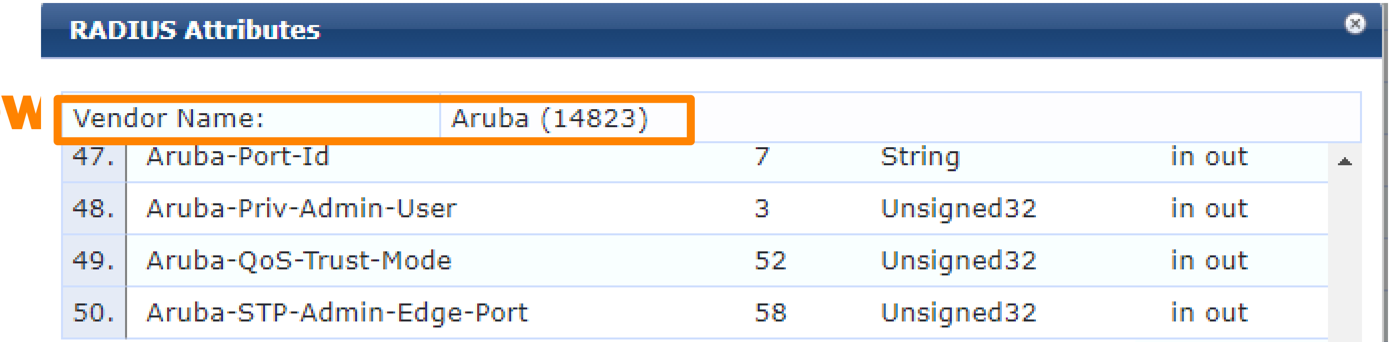
Enforcement Profiles - Arub

Profile:

Name:	Aruba User R
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

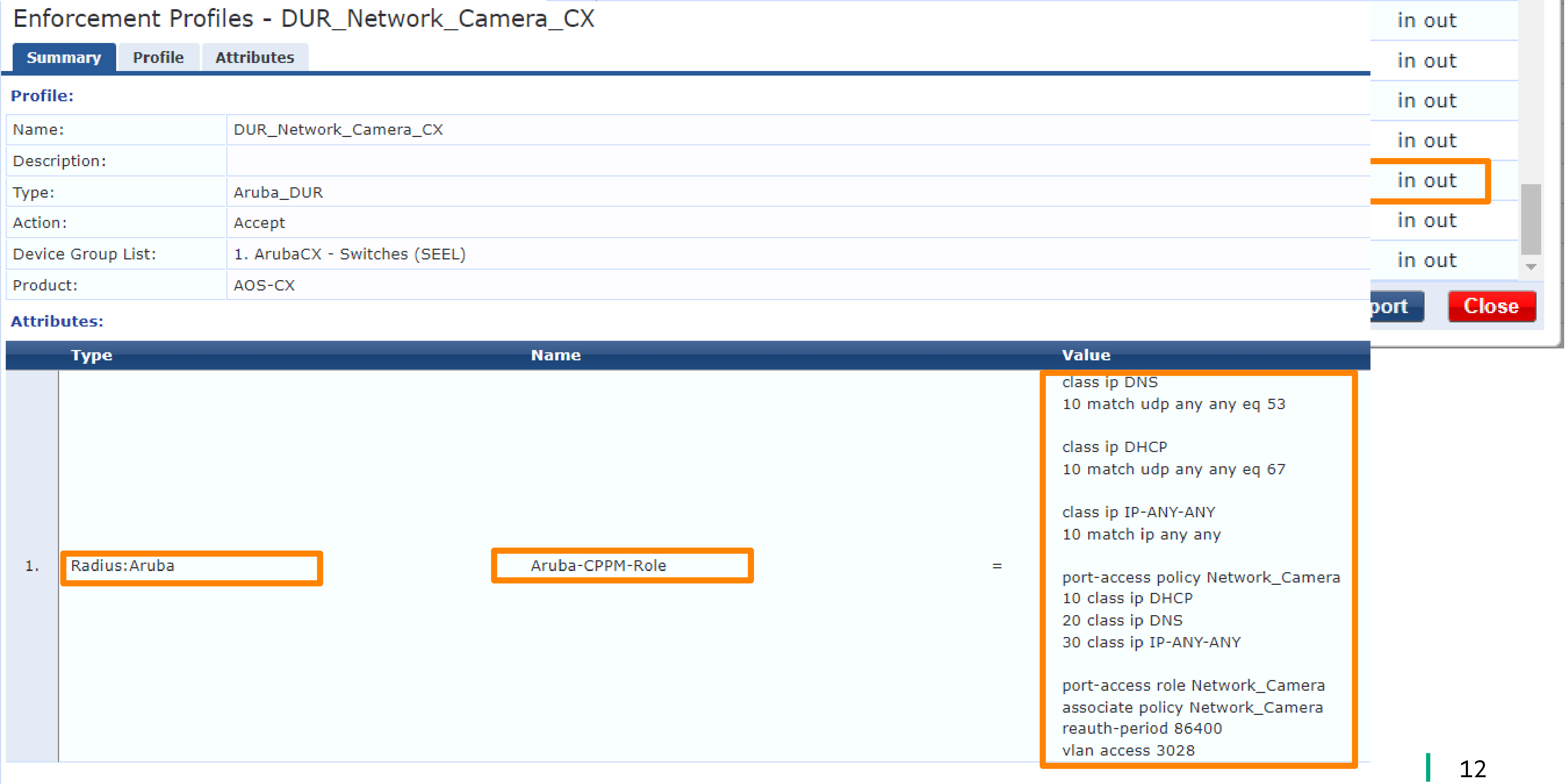
Attributes:

	Type
1.	Radius:Aruba



RADIUS Attributes

Vendor Name:	Aruba (14823)			
47.	Aruba-Port-Id	7	String	in out
48.	Aruba-Priv-Admin-User	3	Unsigned32	in out
49.	Aruba-QoS-Trust-Mode	52	Unsigned32	in out
50.	Aruba-STP-Admin-Edge-Port	58	Unsigned32	in out
				in out
				in out
				in out
				in out
				in out
				in out
				in out



Enforcement Profiles - DUR_Network_Camera_CX

Profile:

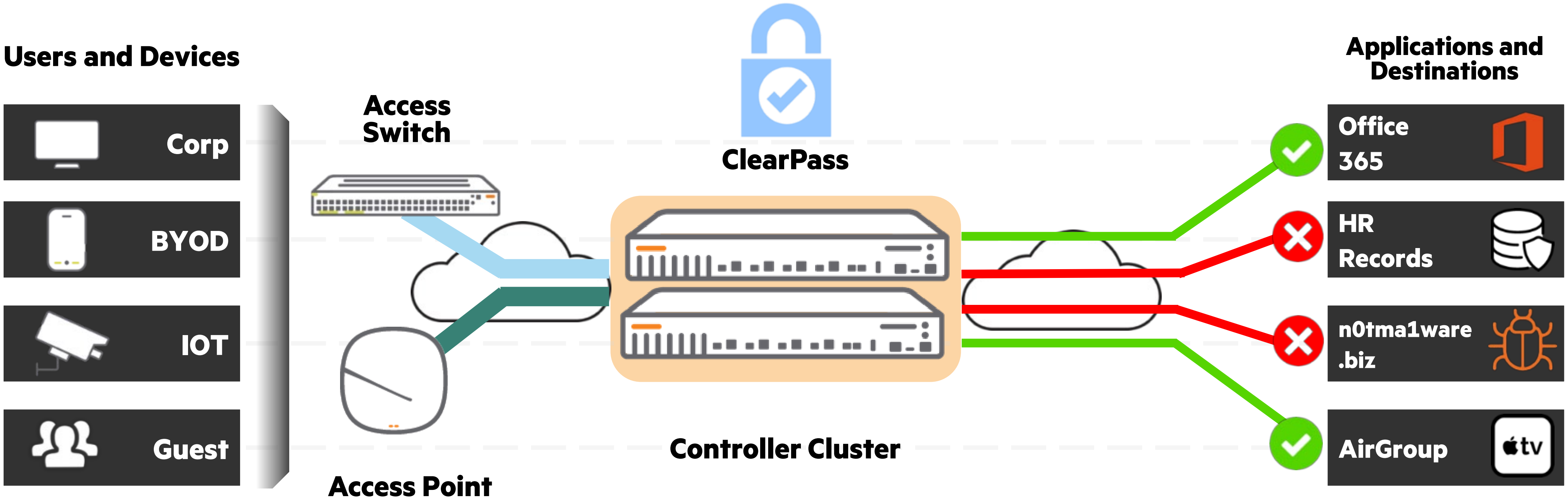
Name:	DUR_Network_Camera_CX
Description:	
Type:	Aruba_DUR
Action:	Accept
Device Group List:	1. ArubaCX - Switches (SEEL)
Product:	AOS-CX

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-CPPM-Role	=	class ip DNS 10 match udp any any eq 53 class ip DHCP 10 match udp any any eq 67 class ip IP-ANY-ANY 10 match ip any any port-access policy Network_Camera 10 class ip DHCP 20 class ip DNS 30 class ip IP-ANY-ANY port-access role Network_Camera associate policy Network_Camera reauth-period 86400 vlan access 3028

Flexible and Secure Network Segmentation

Dynamic Segmentation – what is possible today?



AUTOMATED

Save time and reduce misconfigurations

SEGMENTED

Improve traffic separation and security posture

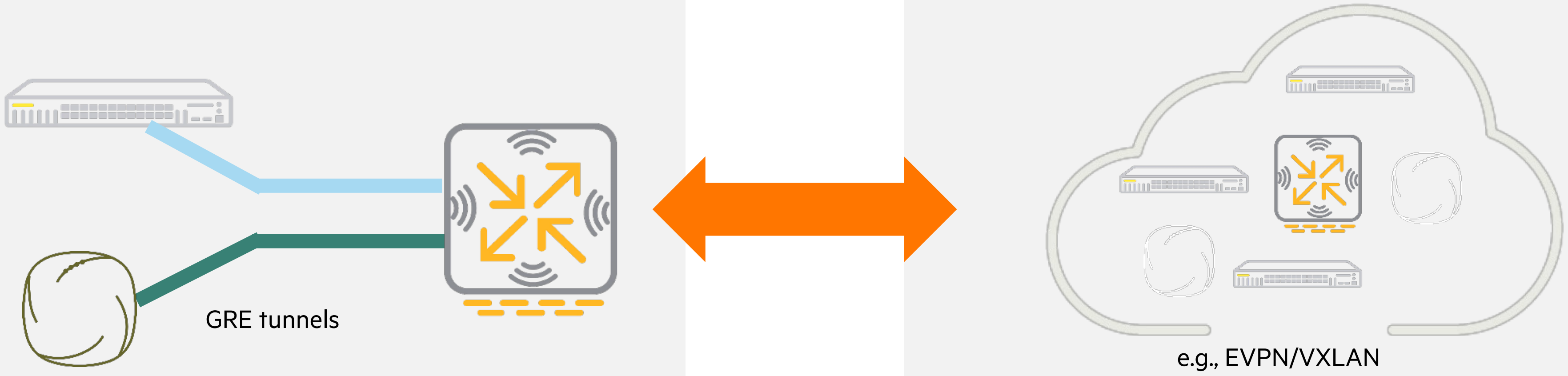
CENTRALIZED

Enhance visibility and management

Dynamic Segmentation Options

CENTRALIZED
OVERLAY ENFORCEMENT

DISTRIBUTED
OVERLAY ENFORCEMENT



Enforcement Done at Controller

ClearPass
Policy Enforcement Firewall

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

Enforcement at Ingress and Egress

Aruba Central NetConductor

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

Hewlett Packard
Enterprise

Distributed fabric

Most important concepts and advantages

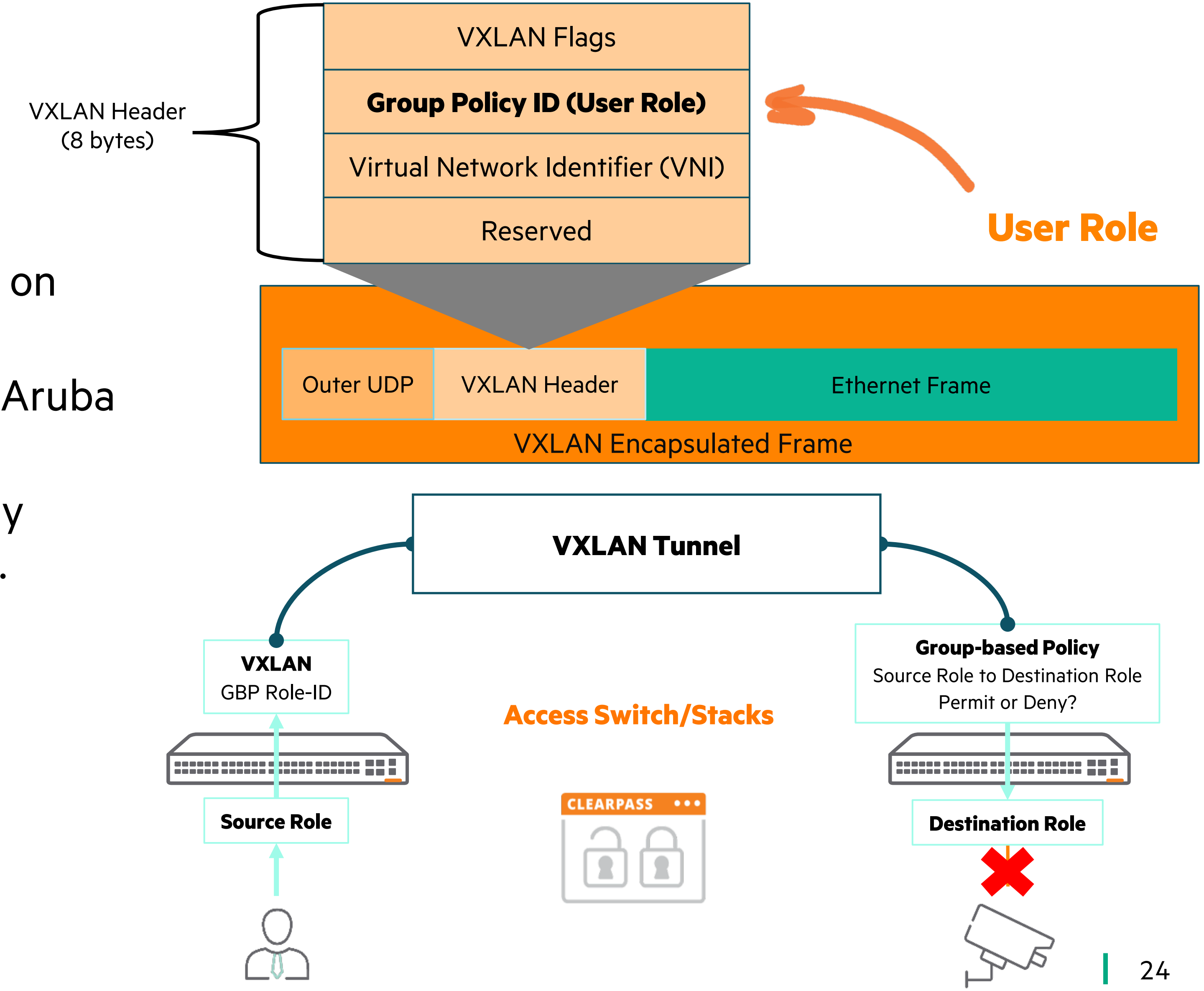
Micro-Segmentation with Group-Based Policy (GBP)

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.

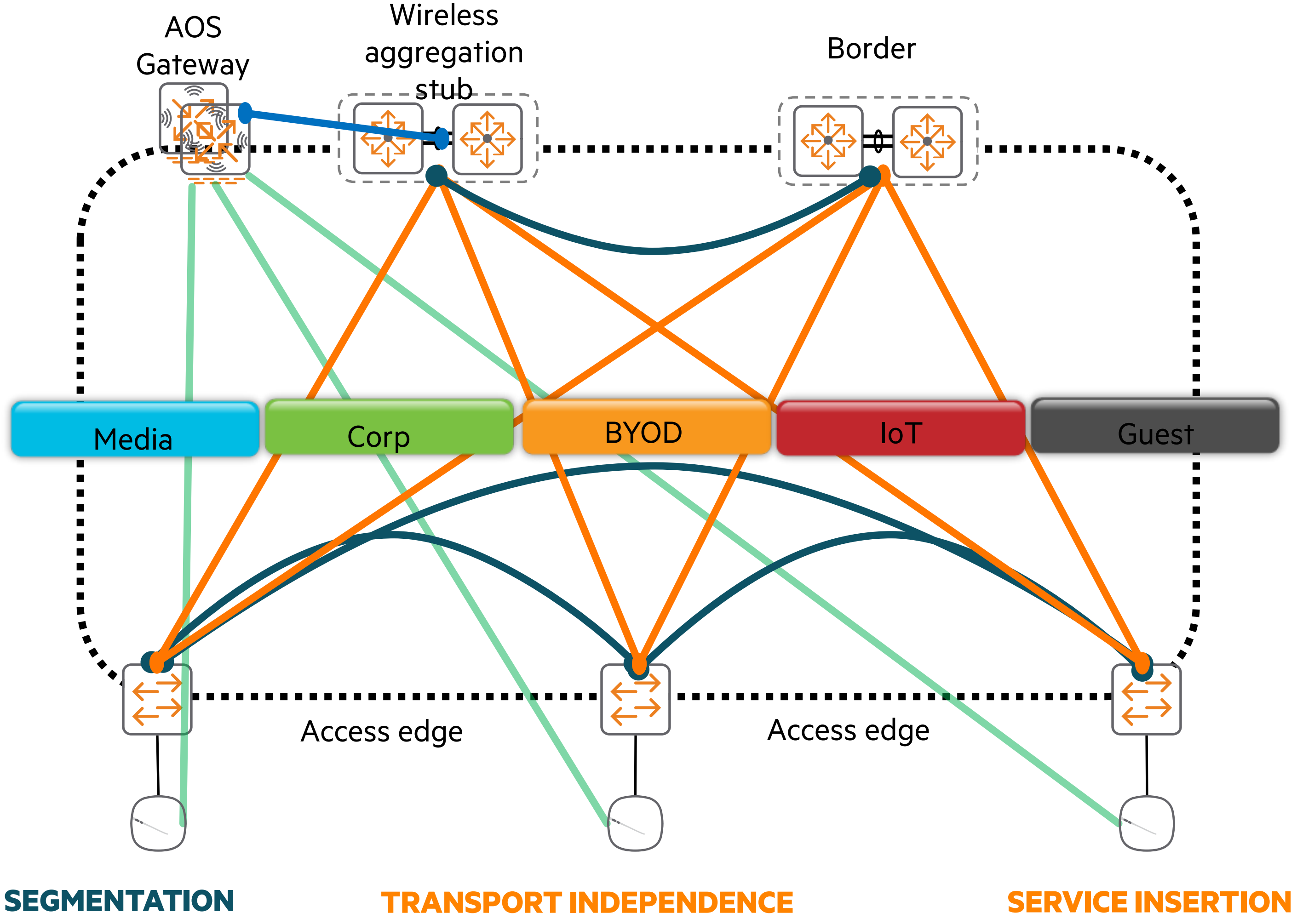
Use Cases

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



Aruba Central NetConductor

Standards based distributed overlay fabric

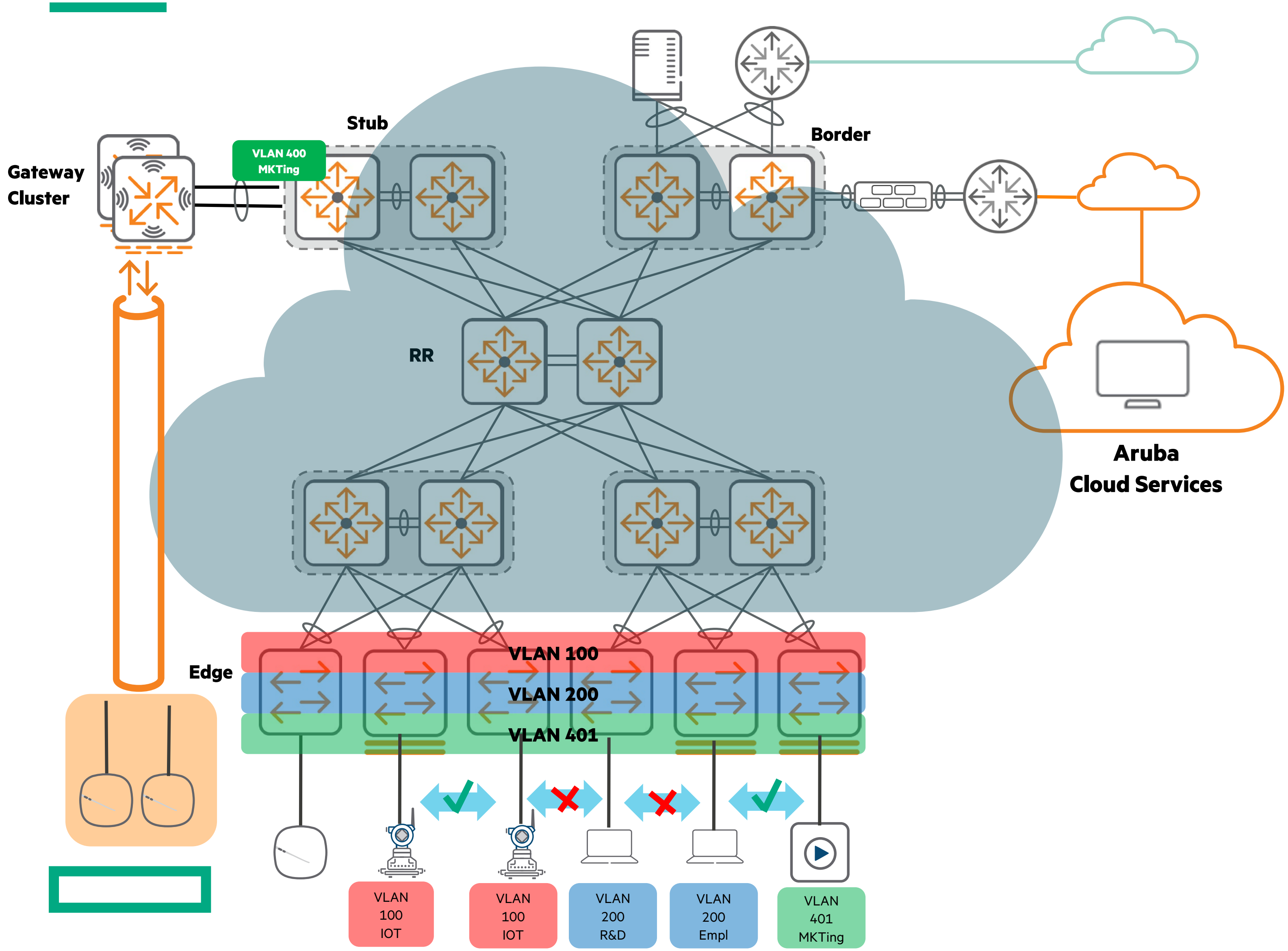


- IETF Standards based
- Multi-vendor campus deployments
- Scales from small to large fabrics
- L2/L3 services across locations
- Multi-Tenancy (VRF)
- Zero Trust Security
- Efficient multicast transport
- Low latency for East-West traffic

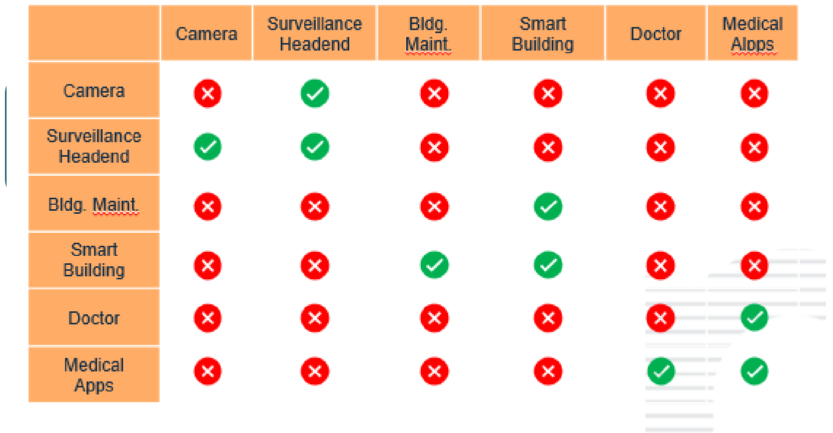
🟦 Static VXLAN-GBP Tunnels
🟧 EVPN VXLAN-GBP Tunnels
🟩 GRE Tunnels

WHY use NetConductor?

Automated Segment Design Fabric



- VLAN is not tied to security policy
- Fabric allows large L2 domain in a scalable way
- Simplified IP subnet Design
- Utilize 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



	Camera	Surveillance Headend	Bldg. Maint.	Smart Building	Doctor	Medical Alpps
Camera	✗	✓	✗	✗	✗	✗
Surveillance Headend	✓	✓	✗	✗	✗	✗
Bldg. Maint.	✗	✗	✗	✓	✗	✗
Smart Building	✗	✗	✓	✓	✗	✗
Doctor	✗	✗	✗	✗	✗	✓
Medical Apps	✗	✗	✗	✗	✓	✓

Thank you!

lukasz.budzisz@hpe.com