AIRHEADS
COMMUNITY

aruba
a Hewlett Packard
Enterprise company

aruba
a Hewlett Packard Enterprise company

PREPARING FOR INTELLIGENT EDGE

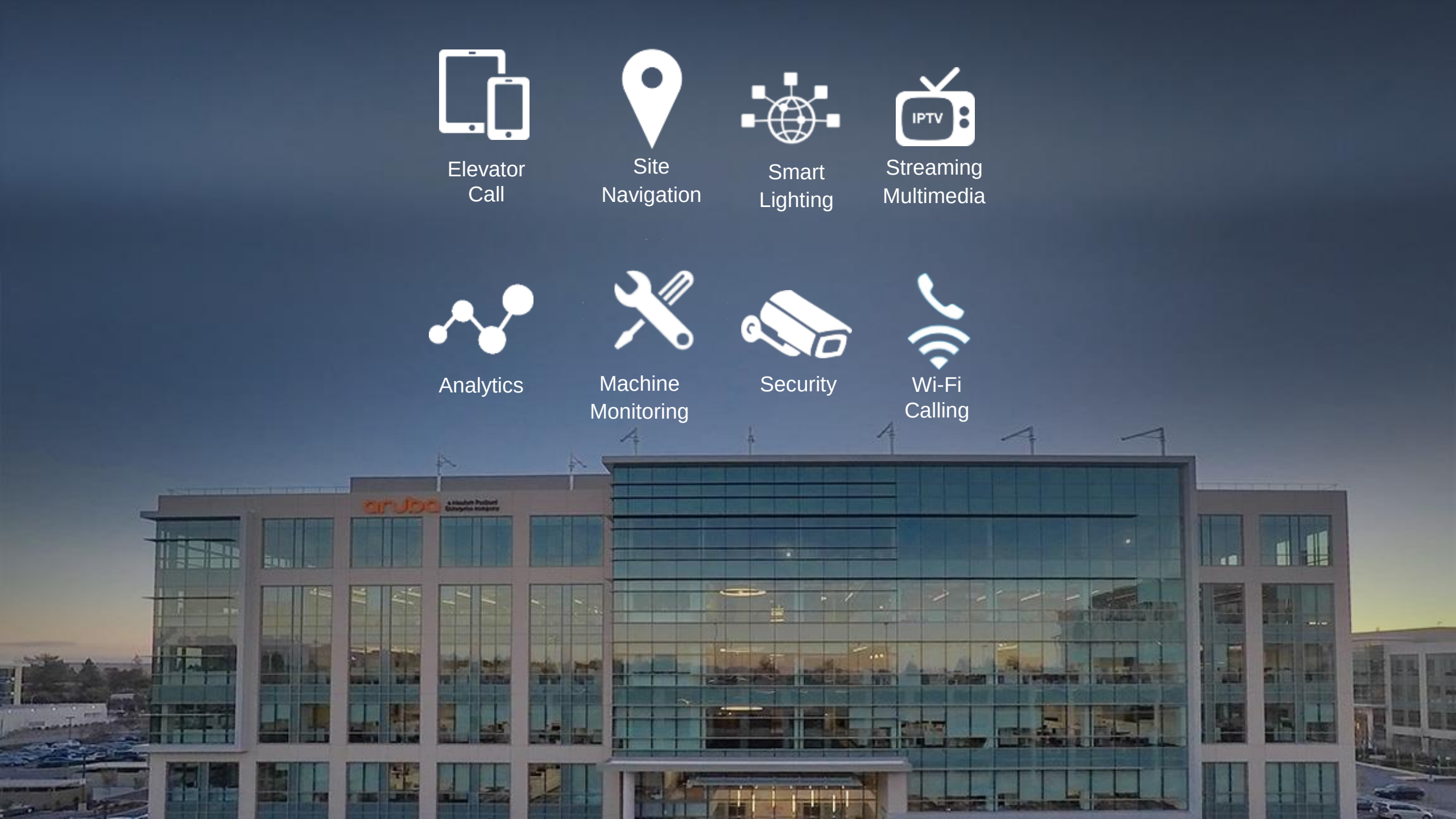
DISCOVERING IOT DEVICES IS JUST THE BEGINNING…

Vercammen@hpe.com

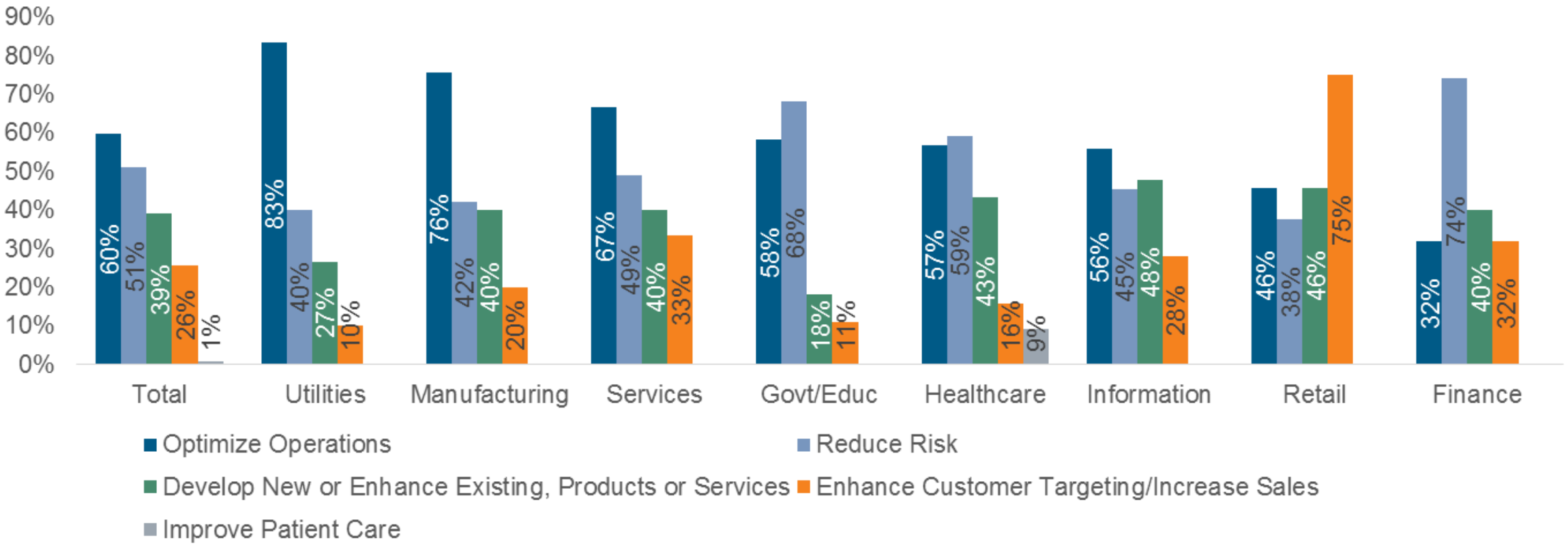
ECONOMIC DRIVERS OF SMART BUILDING IOT

- Total economic impact of IoT in 2025 is $70-140B
- Top areas include:
  - Human productivity monitoring $48-115B
  - Energy monitoring $12-21B
  - Building security $3-6B

McKinsey Global Institute, *Unlocking The Potential Of The Internet of Things*, June 2015


Elevator Call
Site Navigation
Smart Lighting
IPTV
Streaming Multimedia
Analytics
Machine Monitoring
Security
Wi-Fi Calling

THE BUSINESS REASONS FOR IOT VARY BY INDUSTRY



Source: 451 Research, Voice of the Enterprise Internet of Things (IoT) Q1 2016 [N = 590]

aruba
a Hewlett Packard Enterprise company

What are the Challenges?

Challenge #1

Real-time visibility into device behavior is essential to managing costs and enhancing user experiences, comfort, and safety

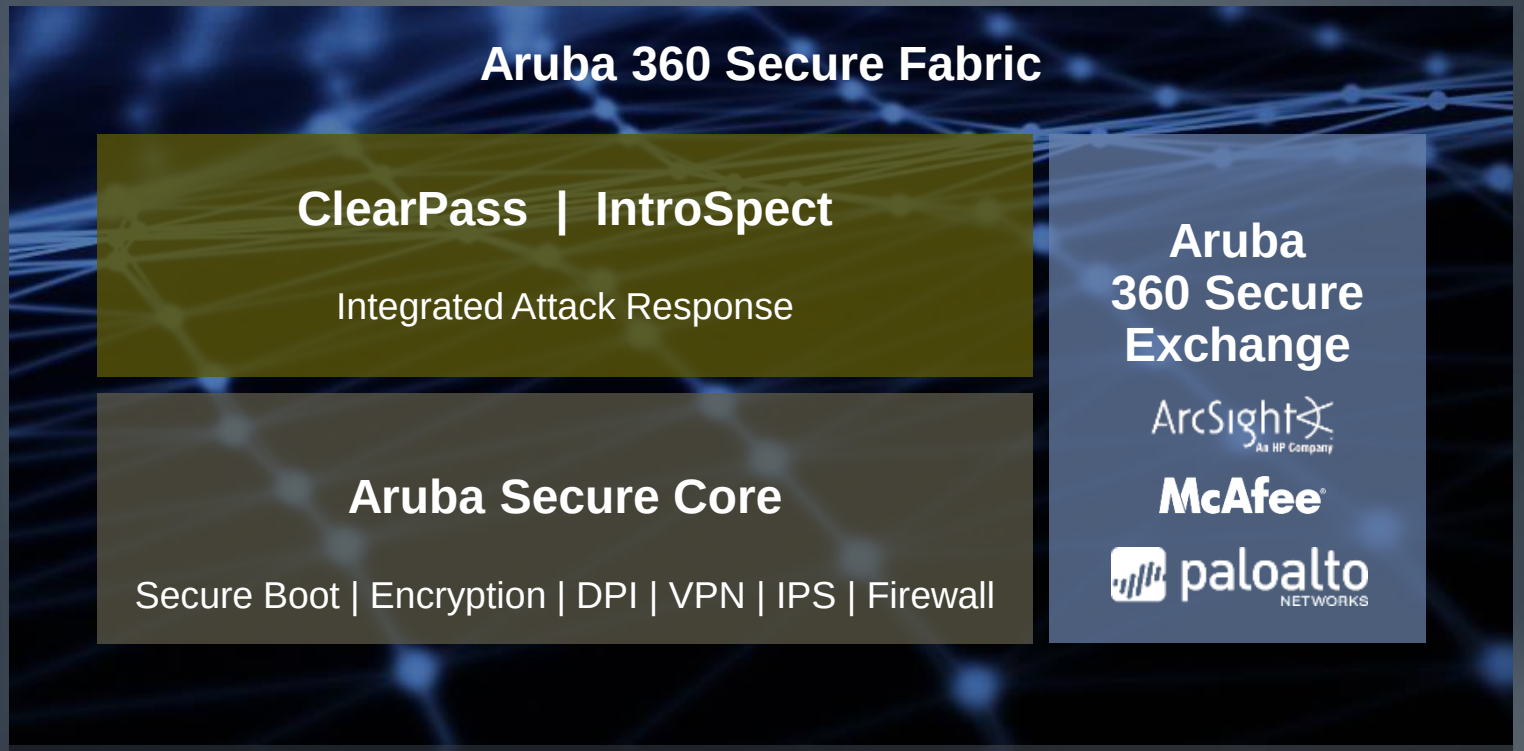
Challenge #2

Legacy IoT devices have to be supported, protected, and monitored side-by-side with the new devices using a wide variety of communications media. Even on a new network architecture.

Challenge #3

Legacy networks can't reliably support critical building and in-room IoT systems, location services, wireless sensors, mobile devices, streaming multimedia.

PROTECT
ARUBA 360 SECURE FABRIC



360^0 active cyber protection and secure access
from the edge, to the core, to the cloud—for any network

aruba
a Hewlett Packard Enterprise company

What are the steps for Innovation?

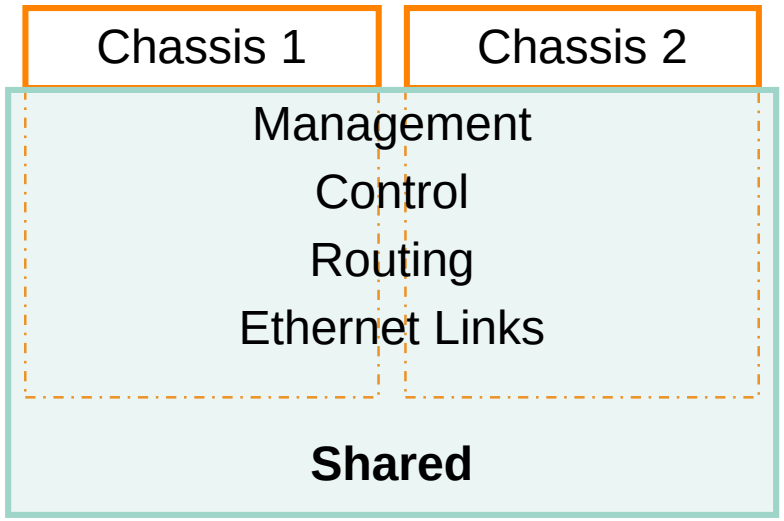
Innovation Always:

- Starts with a use case/goal
- A new technical solution is created
- Manufactures create a branding for their version

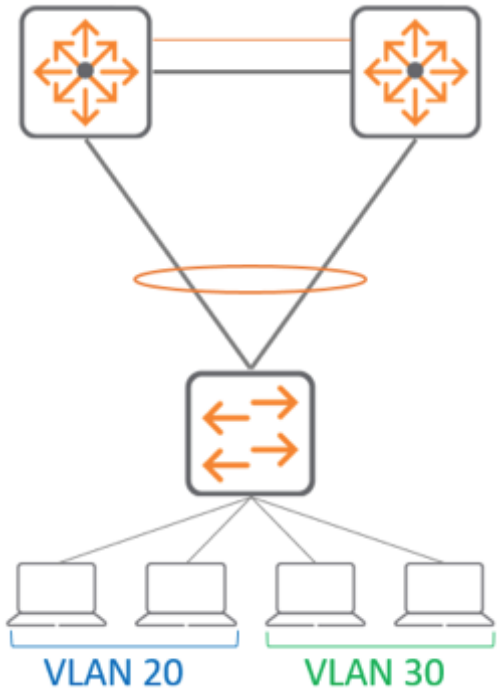
Example - Goal: How to Increase reliability of LAN

- Redundant links between network devices
- Spanning-tree
- Dual-homed Link-aggregation
  - Virtualization techniques

Virtualization Solutions Compared



VSF
IRF



aruba
a Hewlett Packard Enterprise company

What happens in the Access Layer?

Goal: Secure network access of users and devices

- Static configuration of wired access port
- Policy: ACL/QoS local significance to switch port
- Segmentation: VLAN based on topology and IP subnets

Hop-by-Hop configuration

What happens in the Access Layer?

Goal: Secure network access of users and devices

- **Radius/policy-control**
  - Network service for all device
  - Different for Wired and Wireless
- **Wired LAN**
  - Static configuration of wired access port
  - Policy: ACL/QoS local significance to switch port
  - Segmentation: VLAN based on topology and IP subnets

What is next?

What Next in the Access Layer?

Goal: Secure network access of users and devices

- **Role based Access – Wired and Wireless unified**
  - Roles tied to device or user types defines policy: VLAN, QoS, ACL, Rate-limits
  - Policy follows user/device no matter how/where they connect
  - Centralized Policy Management for Wired and Wireless
- **Simplify Access layer configuration**
  - Access port dynamically configured based on connected device
    - Remove need to statically configure access ports
    - Reduce IT staff resources for Add, Move and Changes
- **Segmentation**
  - Legacy VLAN / local-switching
  - Tunneled wired device to controller with stateful firewall/policy control

Mobile First - Dynamic Segmentation

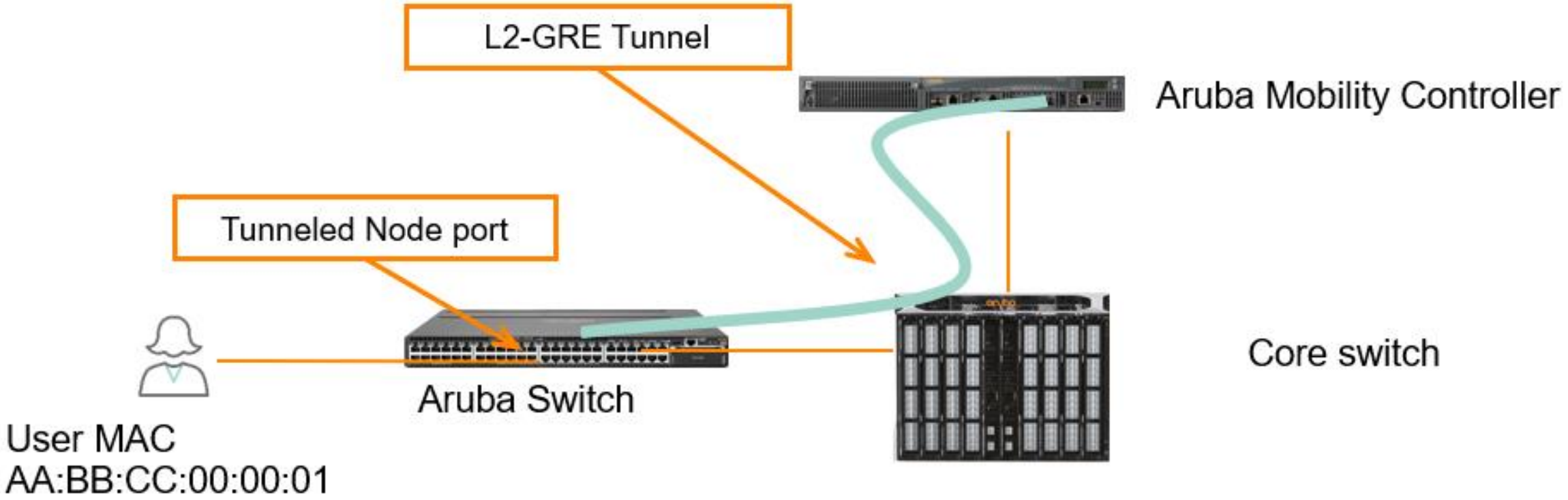
- **Simplify Access layer configuration**
  - Colorless Ports

- **Segmentation**
  - User Based Tunneling (UBT)
  - Port Based Tunneling
  - Legacy VLAN based local Switching

- **Policy control**
  - Local or Downloadable User Roles (DUR)

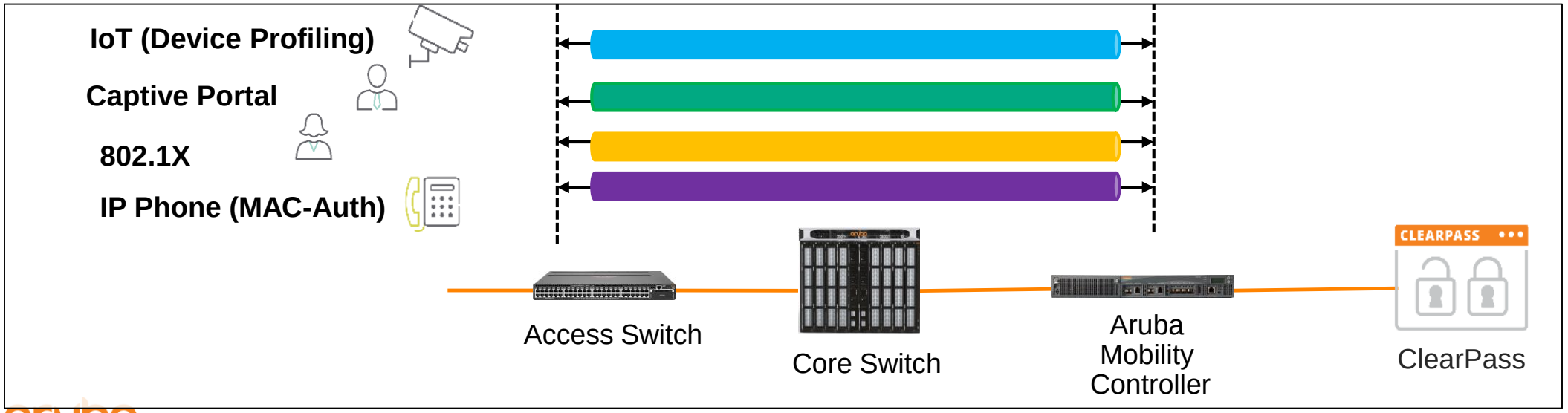
PORT-BASED TUNNELING: WHAT IS IT?

- Traffic on wired switch port is handled by a central Aruba Mobility Controller
- It's a tunnel, therefore MAC address table size relief on the intermediate devices



USER-BASED TUNNELING: WHAT IS IT?

- UBT uses the concept of a colorless access port
- It doesn't matter what you connect to the port
  - Roles and policies are assigned per device
- Authentication takes place at the access port level
  - Successful authentication enforces VLAN and ACL assignments
  - Can create a user or device-based tunnel to the Mobility Controller
  - Mobility Controller can enforce additional security
- It's a tunnel, therefore MAC address table size relief on the intermediate devices



Dynamic Segmentation – So What

Increased Flexibility and Security Wired Lan

- Roles
  - Roles follow user/devices no matter where/how they connect
    - Cameras, employee, guest, printer….
      - VLAN, QoS, ACL, Rate-Limits

- Tunneled-Node
  - Tunneled-Node + Roles enables segmentation without regard to IP subnets, I can create it is in total separated network.
  - In-line firewall

- Security
  - Downloadable User Roles provides a Single Source of Policy

Dynamic Segmentation – What should I learn?

What is the risk-factor?

- Existing/Well-known Topologies and Protocols
  - Authentication, Network-Access, Switching and Routing
- Benefits of existing IT skill sets
- Freedom to choose best-in-breed infrastructure
  - What if a new innovation comes around?

- Segmentation Local Switching **AND** Tunneled as needed
  - Can choose what data is locally-switched, and what is Tunneled.
  - Tunneled traffic, GRE: same as todays wireless traffic (Aruba CAP, CAPWAP)
- Authentication/Authorization
  - Free to choose 3rd Party Radius/ additional benefits with Aruba Clearpass*

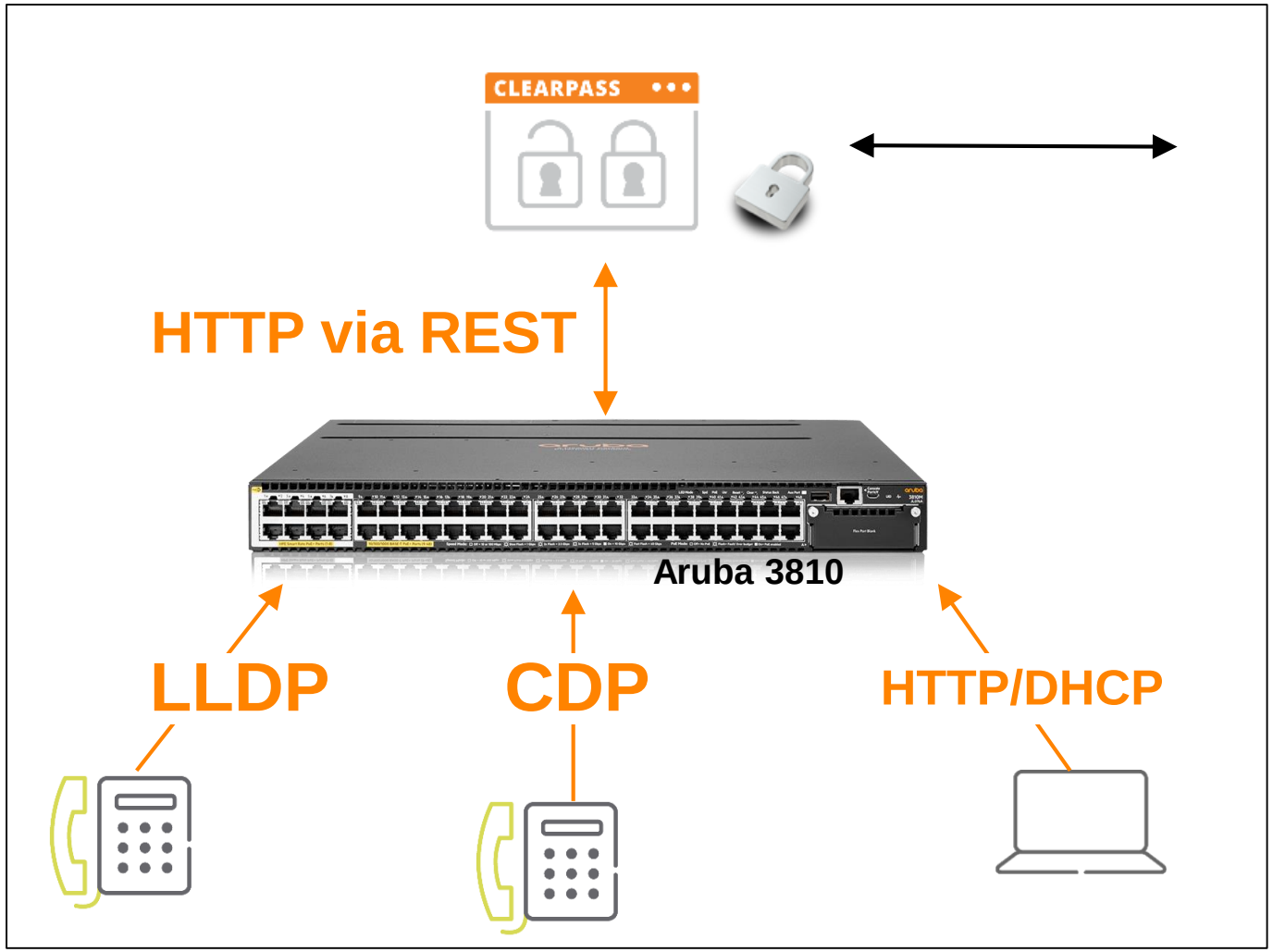
Dynamic Segmentation – What should I learn?

Controller

Switch

From controller perspective, a switch is an AP when it comes to licensing

DEVICE FINGERPRINTING: PROTOCOLS



UBEA Tools

device-fingerprinting policy

Syntax

```
device-fingerprinting policy <profile_name>

no device-fingerprinting policy <profile_name>
```

Description

Configures the device fingerprinting for profiles.

The `no` form of this command removes the device fingerprinting for profiles.

Command context

```
config
```

device-fingerprinting timer

Syntax

```
device-fingerprinting timer <time>

no device-fingerprinting timer
```

Description

Configures the timer for switch to send the client data to CPPM. The default time is 120 seconds. The time range is 60 to 300 seconds.

The `no` form of this command resets the timer to its default value.

Command context

```
config
```

Parameters

time

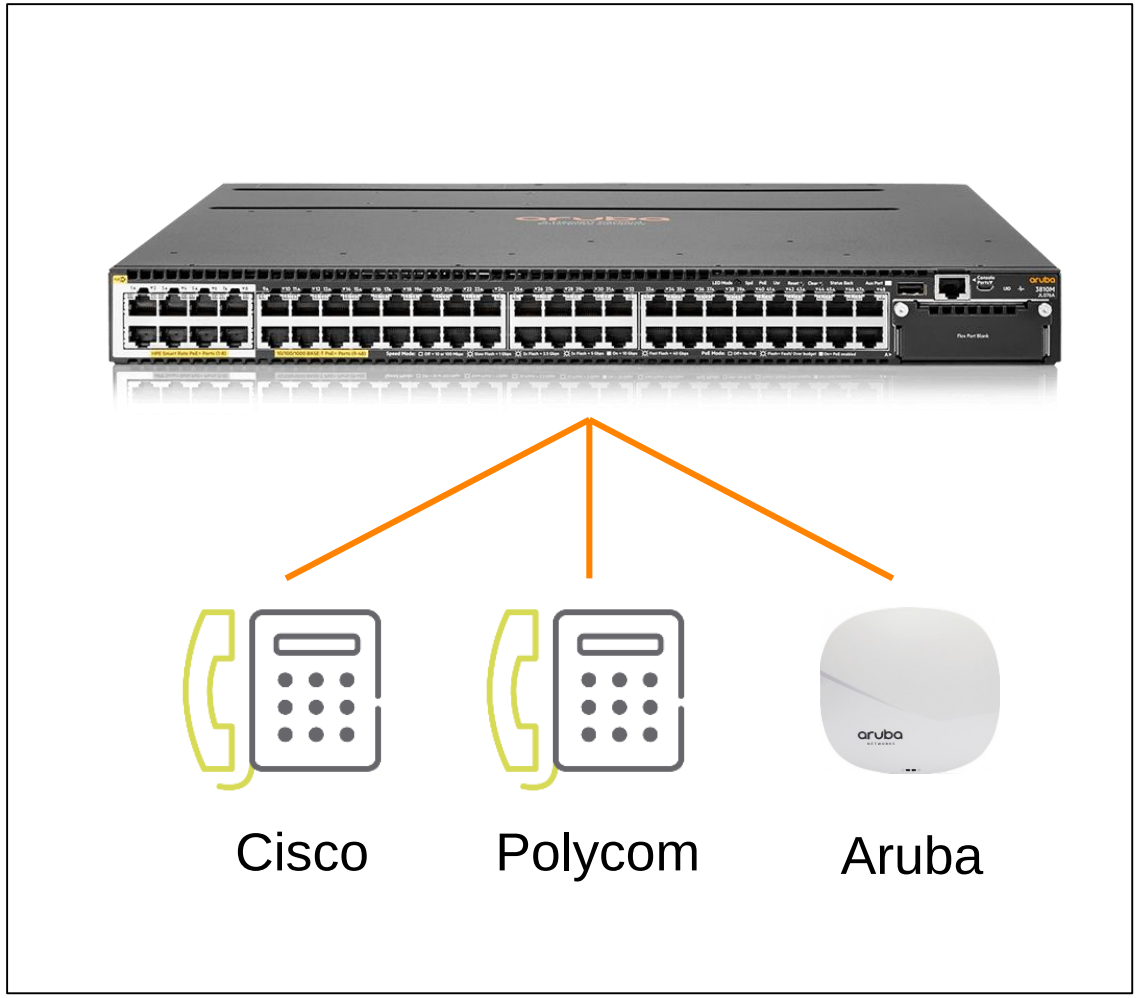
Configures the timer for switch to send the client data to CPPM. The range can be 60 to 300 seconds.

CUSTOM DEVICE PROFILES

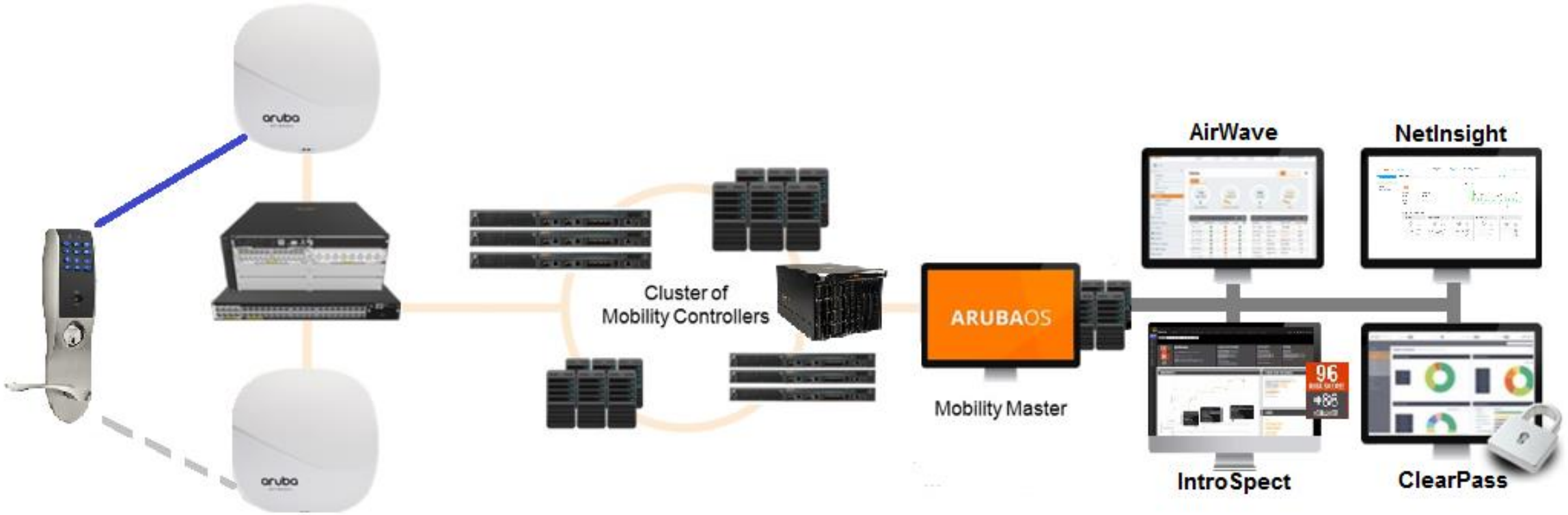
- Automatically detect device based on LLDP information received via switch port

- Device profile contains the following:
  - PoE Priority
  - PoE Power
  - VLAN Assignment (Tagged or Untagged
  - Bandwidth limit
  - Port Speed

- Can use it with Aruba Access Points as well as a custom profile for any LLDP TLV



HITLESS UPDATES



Client loads transfer to other APs prior to update/reboot

Better Together

Powering and securing the Digital Workplace

Unified Policy

- Authentication and setting policy using ClearPass Policy Manager
- User onboarding and guest access with ClearPass Policy Manager
- Simplify policy management and configuration with User Role

Consistent user experience

- Per port tunneling of all wired traffic to Mobility Controller
- Centralized policy management and enforcement
- All users have access to applications on the Controller

Wired and Wireless Management

- End-to-end management of wired and wireless networks with AirWave
- Zero Touch Provisioning for rapid deployment with AirWave
- Cloud-based management with Aruba Central

Wireless optimized

- Automatic configuration of switch port when Aruba AP is detected
- Working with IAP to contain rogue AP, add VLAN
- Set appropriate QoS of traffic from the AP

What About You

What are the use cases that you encounter?

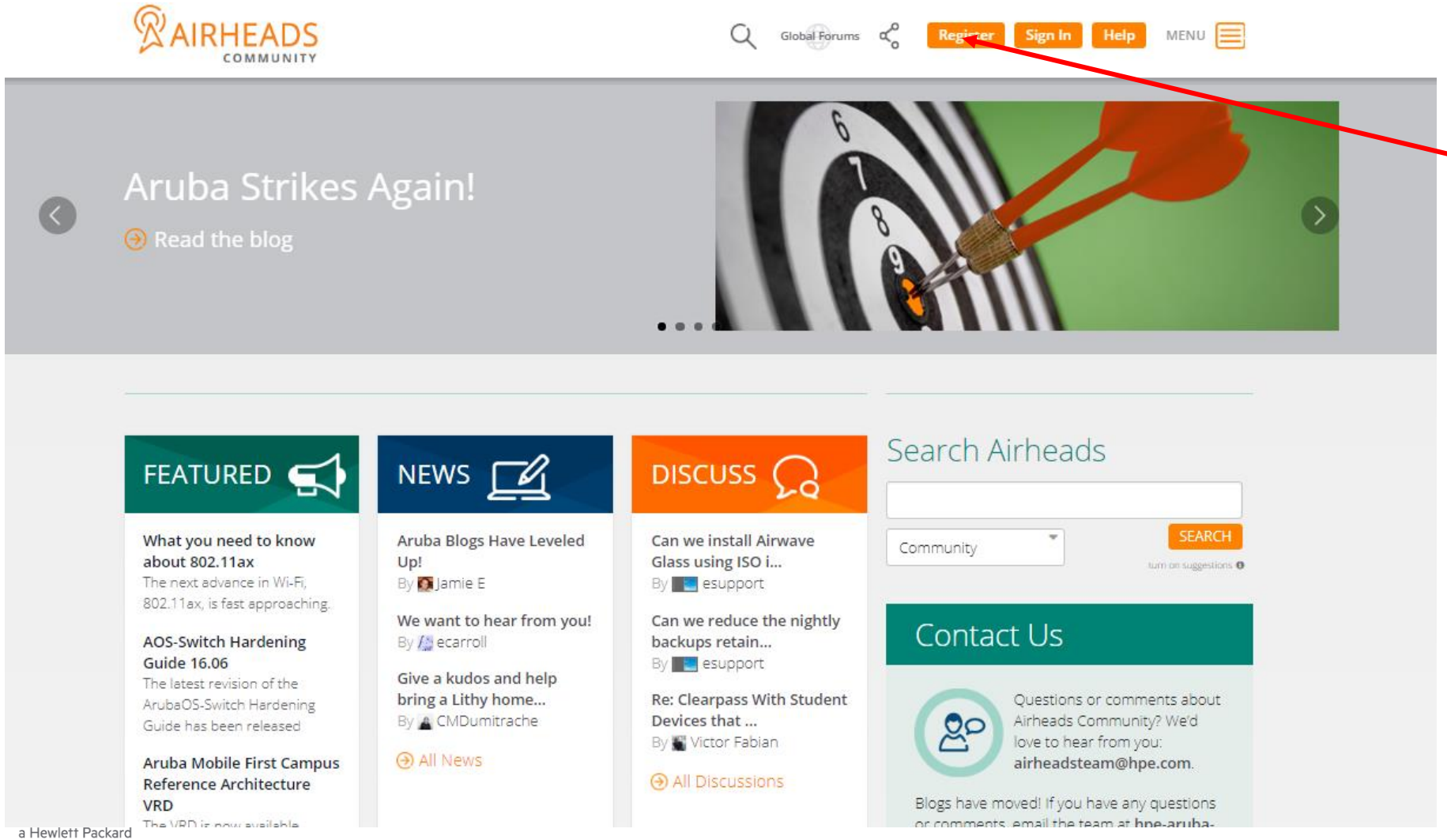
- Asset tracking
- Location services
- Monitoring

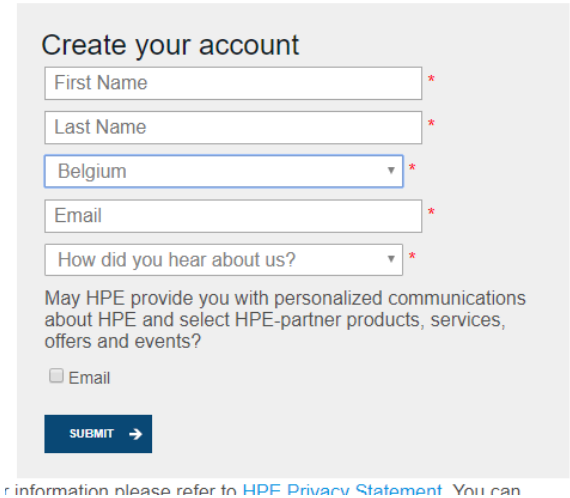
What are the protocols that you want us to interact with?

- We are known for our eco system, how should we extend it?
- BLE
- Zigbee
- Proprietary
- ….

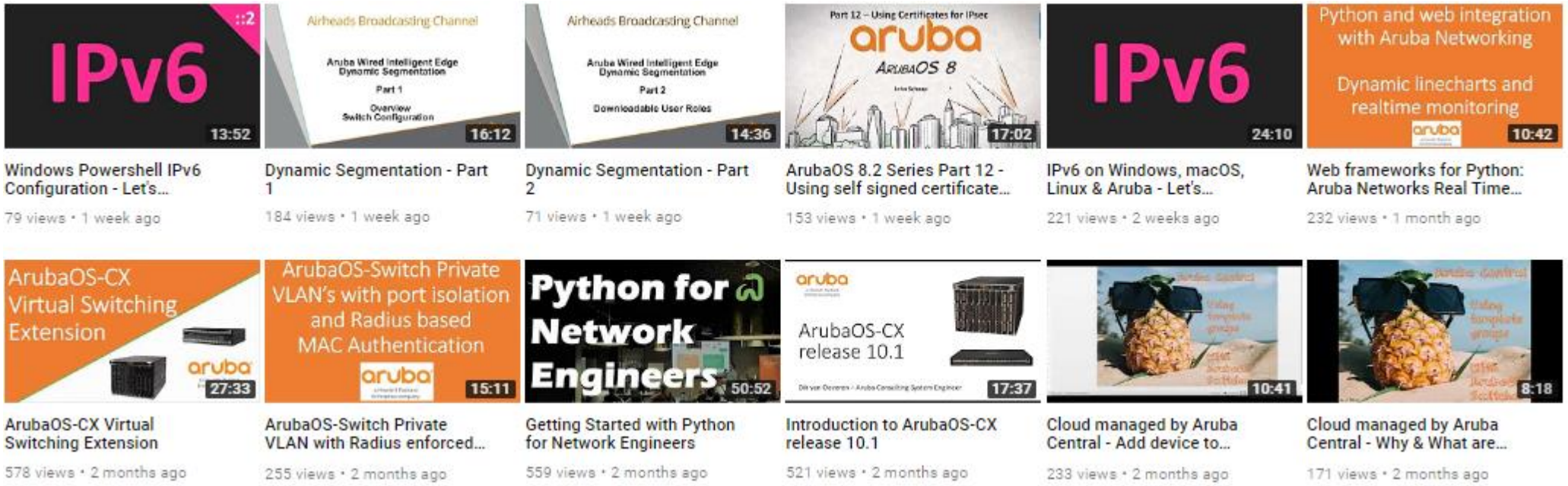
Airheads Community

community.arubanetworks.com





Airheads Broadcasting Channel



AIRHEADS COMMUNITY

THANK YOU

aruba
a Hewlett Packard Enterprise company

AIRHEADS COMMUNITY

THANK YOU

aruba
a Hewlett Packard Enterprise company

Dynamic Segmentation Scale

Controller	Maximum Supported Tunnels
7280	34816
7240 /7240XM	34816
7220	17408
7210	8704
7205	4352
7030	1088
7024	544
7010	544
7008	272
7005	272

Switch Series	Maximum Supported Tunnels
5400R – Per Switch/Stack	1024 tunnels
5400R – Per Port	32 tunnels
3810 – Per Switch/Stack	1024 tunnels
3810 – Per Port	32 tunnels
2930F/M – Per Switch/Stack	1024 tunnels
2930F/M – Per Port	32 tunnels

Port-Based Tunneling Scale

Controller	Maximum Supported Tunnels
7280	34816
7240 /7240XM	34816
7220	17408
7210	8704
7205	4352
7030	1088
7024	544
7010	544
7008	272
7005	272

Switch Series	Maximum Tunneled Ports
5400R - Standalone	up to 288 (5412R)
5400R – VSF Stack	up to 576 (2 x 5412R)
3810 - Standalone	All ports
3810 - Stack	Up to 520
2930F – Standalone	All ports
2930F – VSF Stack	Up to 208
2930M – Standalone	All ports
2930M - Stack	Up to 520
2920 – Standalone	All ports
2920 – Stack	Up to 208
3800 - Standalone	All ports
3800 - Stack	Up to 520

aruba
a Hewlett Packard Enterprise company