Secure Switching

Metin SÖNMEZ
Systems Engineer
metin.sonmez@hpe.com
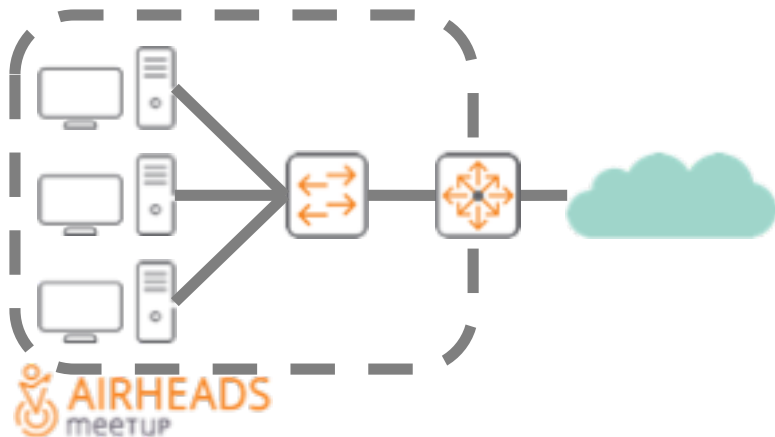
29.06.2018

#ArubaAirheads

EDGE NETWORK ARCHITECTURE EVOLUTION

Past

Networks were mostly static, connected devices homogeneous

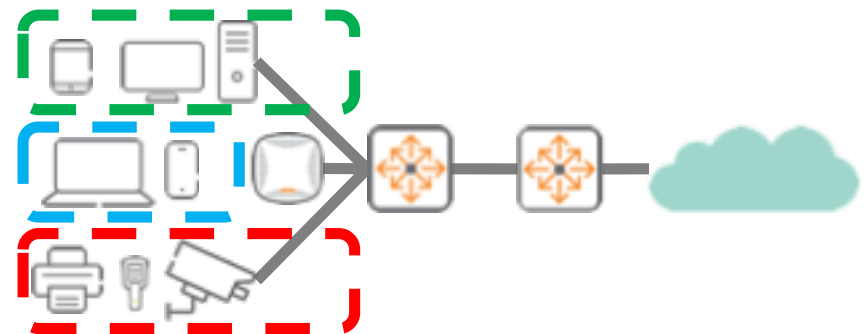Topology and policy were converged, enforced with VLANs and ACLs

Policy was simple

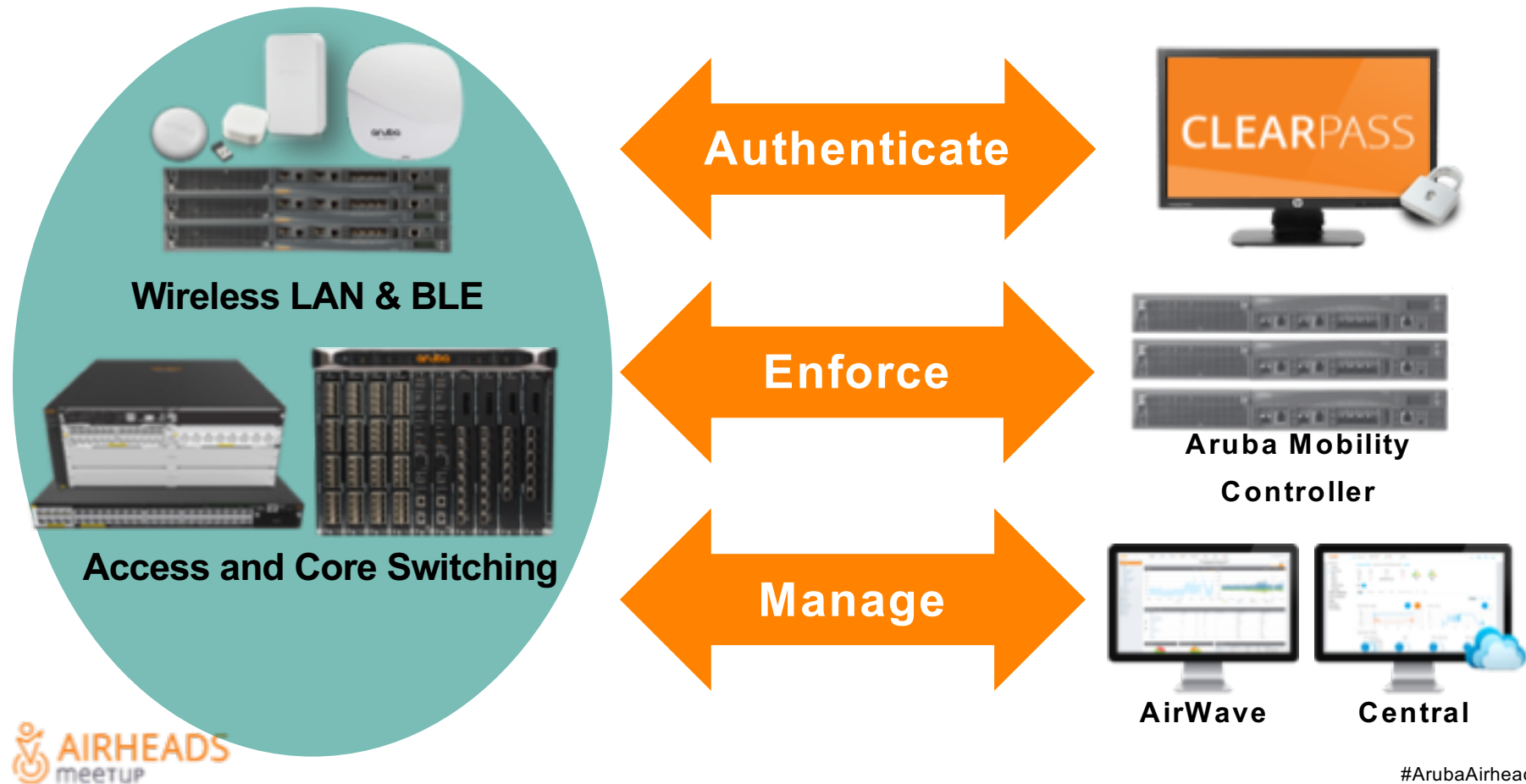**Present**

Broad range of device types on network
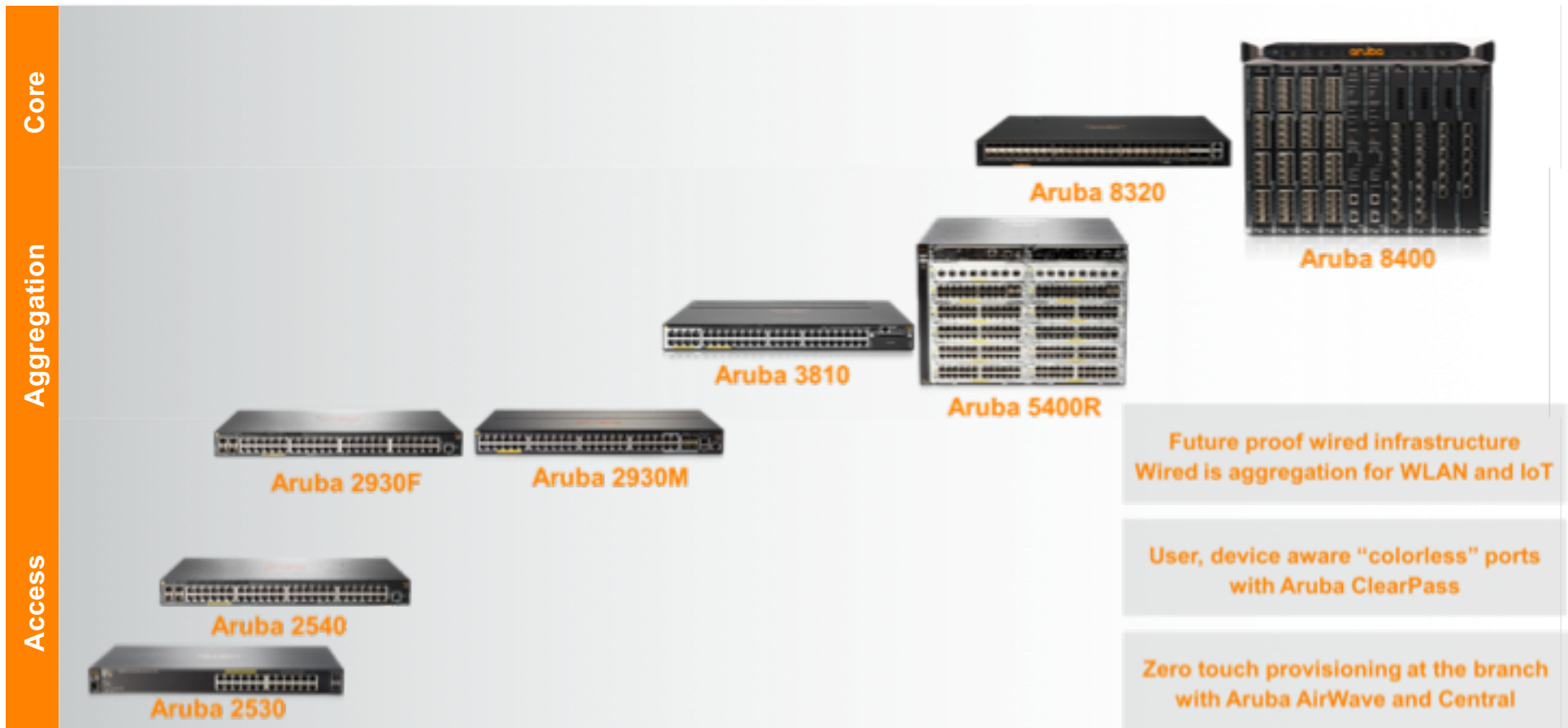
Devices are mobile, no longer static

Policy is more complicated

Tying policy to VLANs and subnets is difficult to manage and expensive

Aruba Mobile First Solution is Better Together

Wireless LAN & BLE

Access and Core Switching

Authenticate

Enforce

Manage

CLEARPASS

Aruba Mobility

Controller

AirWave   **Central**

Build a network foundation for tomorrow

Core

Aggregation

Access

Aruba 8320

Aruba 8400

Aruba 3810

Aruba 5400R

Aruba 2930F

Aruba 2930M

Aruba 2540

Aruba 2530

Future proof wired infrastructure
Wired is aggregation for WLAN and IoT

User, device aware "colorless" ports
with Aruba ClearPass

Zero touch provisioning at the branch
with Aruba AirWave and Central

HOME

Aruba Campus Switching Differentiators
Complete campus core to edge portfolio

Automated and Simple	Secure and Unified	Flexible Single View

Zero Touch Provisioning

Auto-config for VLAN, QoS, PoE priority

Full, open **REST APIs**

Aruba **Network Analytics Engine** at the core

Dynamic Segmentation secures with Aruba Controllers, Services and ClearPass

Unified Policy with Unique Aruba ClearPass Integration with User Role and Captive Portal

Multi-vendor Aruba AirWave for config., mgmt. and monitoring

Cloud-based Aruba Central for single view of WLAN and switching

Flexible management choice with same hardware

Industry leading TCO with no software licensing

AIRHEADS
meetup

Per-port Dynamic Segmentation

Tunneled Node

- Extends the AP-controller tunneling scheme to the access switches

Per-port tunnels

- GRE tunnels from each port transport all traffic to/from "tunneled" interfaces


Policy enforcement

GRE

- Traffic from other interfaces is forwarded normally by the switch

- Management and control traffic is NOT tunneled

Products

- 5400R switch series with v2 and v3 modules
- 3810 switch series

- 3800 switch series
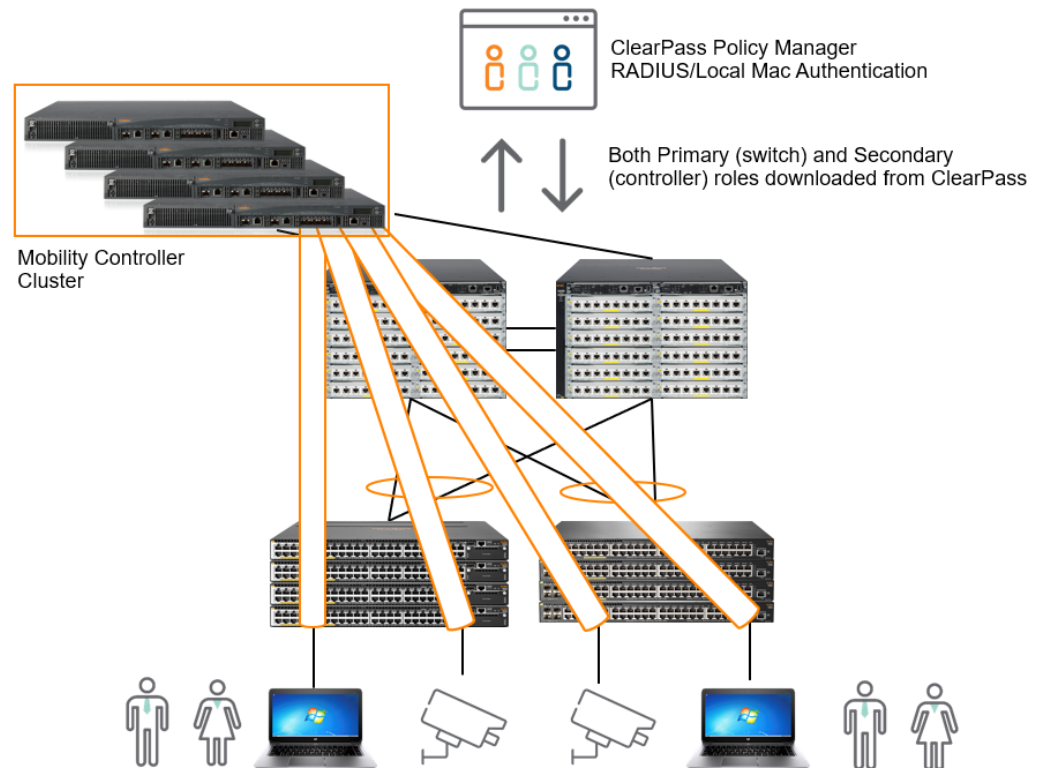- 2930F/M switch series
- 2920 switch series

Per-user Dynamic Segmentation

- Secured and flexible control of access layer

  - With ClearPass or switch configuration, only traffic from a specific user/device role is sent to the mobility controller
  - Policies (e.g., QoS, ACL, rate-limit) can be enforced at Tunneled Node ports or at the controller

- Access to Controller's applications

  - Users can access Controller's applications such as stateful firewall and AppRF

- Higher availability and scalability

  - Load balance to multiple controllers for high scalability
  - Stateful failover to standby management module for high availability

- Support on 5400R/v3, 3810M, and 2930F/M. Requires AOS 8.1 or later in the controllers

ClearPass Policy Manager
RADIUS/Local Mac Authentication

Mobility Controller
Cluster
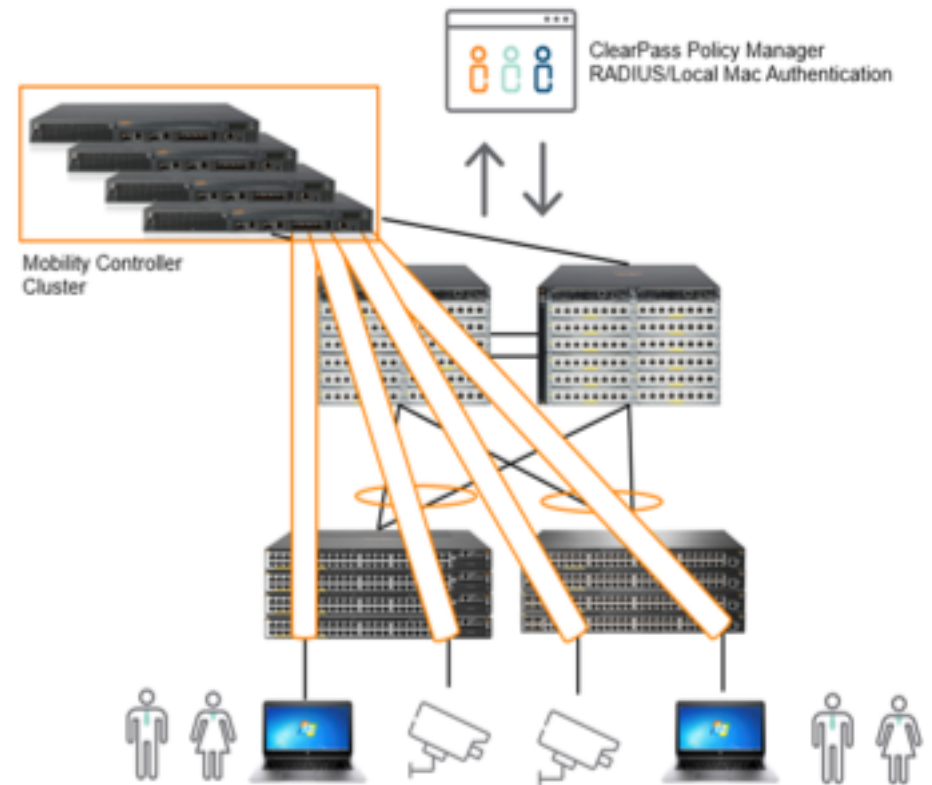
# Per-user Dynamic Segmentation/Downloadable User Role Enhancement

- Primary User Role (Switch)
  - Assigns VLAN to Users/Devices
  - Can assign policy local to switch based on User Role definition
  - Downloaded from ClearPass in 16.04
  - Initializes user tunnels with "tunneled-node-server-redirect" command which contains secondary role information
- Secondary Role (Controller)
  - Assigns firewall and user policy at controller level
  - Manually entered in 16.04
  - Downloaded from ClearPass with 16.05
- Must Have:
  - ArubaOS-Switch 16.05 (5400R/3810M/2930)
  - ArubaOS 8.3+
  - ClearPass Policy Manager 6.7

ClearPass Policy Manager
RADIUS/Local Mac Authentication

Both Primary (switch) and Secondary (controller) roles downloaded from ClearPass

Mobility Controller Cluster
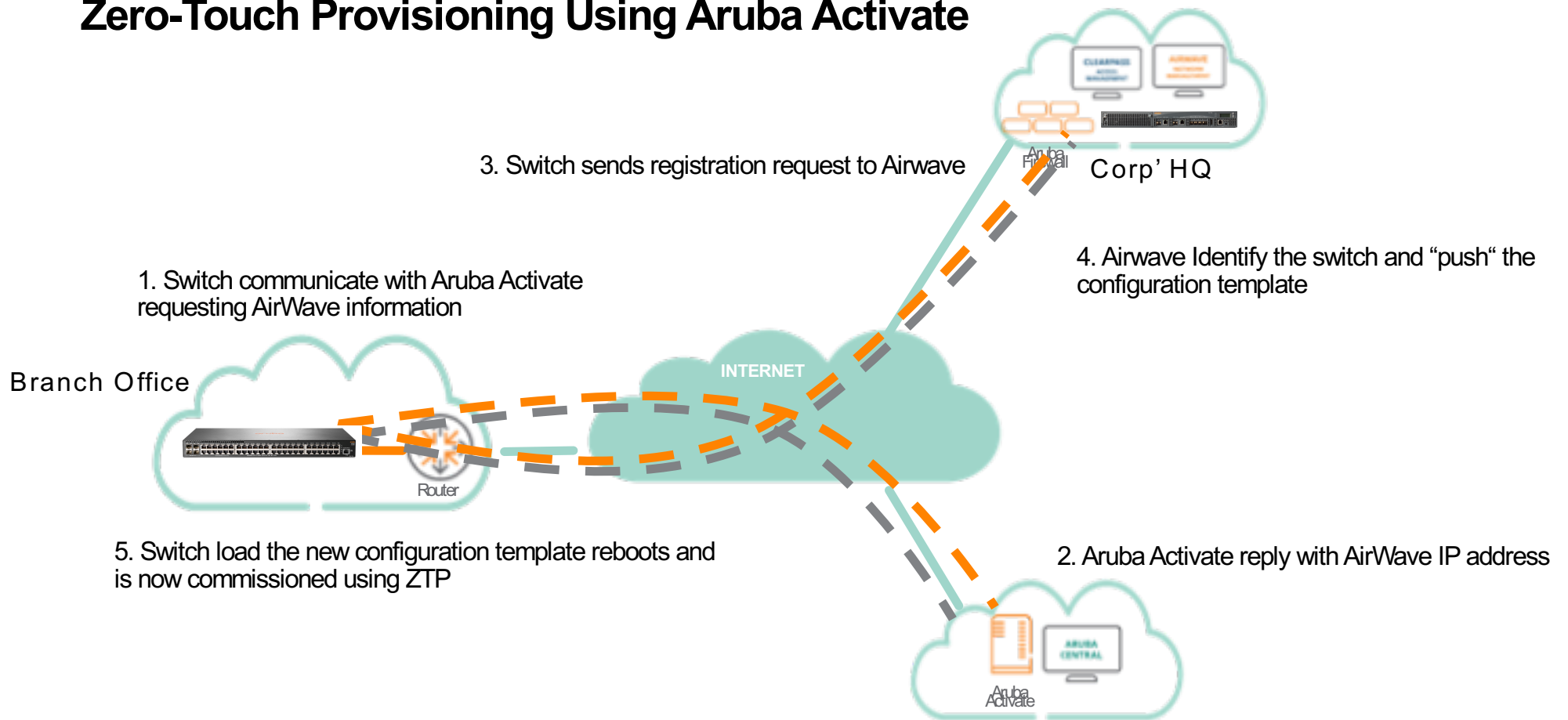
Downloadable User Roles

- **Single point of policy management for the entire network**
  - User Role can be dynamically assigned by ClearPass at the time of authentication

- **No need for policy configuration on switches**
  - Centralized policy configuration improves ease of deployment

- **Builds on top of the already-supported local User Roles**
  - Every user/device is assigned a User Role which is downloaded from ClearPass

- **User Role policies include QoS, VLAN, ACL, Rate Limits**
  - All policy-related switch configuration can be tied to a user role and configured only on ClearPass

- **Consistent wired/wireless policy management**
  - Same as WLAN AP, simplify policy configuration and managementv
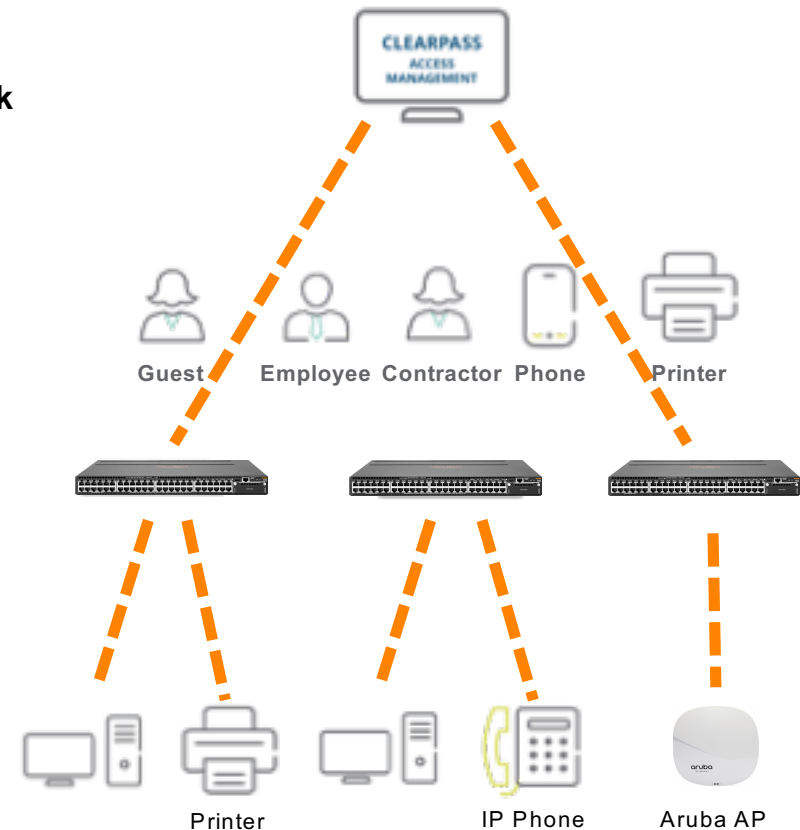
Differences between PPTN and PUTN

Feature Details	Per Port Tunneled Node	Per User Tunneled Node
User Traffic	All Traffic on the 'Tunneled' interface will be forwarded to the controller	User traffic only forwarded to controller, if Switch finds the 'redirect' attribute in the user-role
User Auth	User Authentication done at the controller. Controller decides the user-role for the wired users	User Authentication done by the Switch. Switch will send user-role information to the controller.
Modes supported	Standalone, MD (non-cluster) mode	Standalone, MD (non-cluster), cluster
VMC Support	No VMC Support	No VMC Support
Switch Support	2920,3800,3810,5400R,2930M,2930F	2930F,2930M,5400R,3810
AOS-S Version	16.02	16.04

HOME

Zero-Touch Provisioning Using Aruba Activate

3. Switch sends registration request to Airwave

Aruba
Firewall   Corp' HQ

4. Airwave Identify the switch and "push" the configuration template

1. Switch communicate with Aruba Activate requesting AirWave information

Branch Office

INTERNET

Router

5. Switch load the new configuration template reboots and is now commissioned using ZTP

2. Aruba Activate reply with AirWave IP address

Aruba
Activate

What is Aruba Activate?

Inventory Management – ZTP Auto Configuration Tool

Zero Touch – Auto configuration

HOME
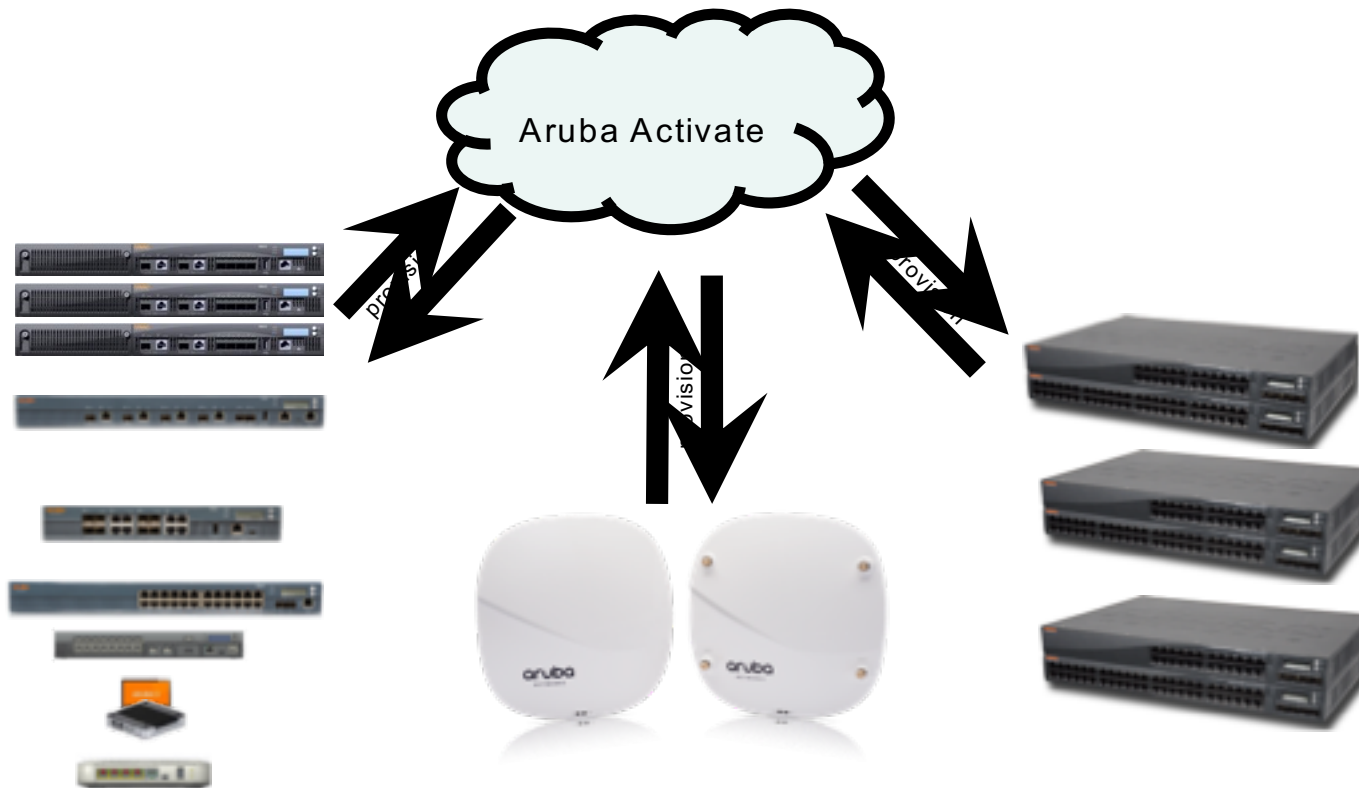
Aruba 2530 and 2540 Switch Series

Aruba 2530

Aruba 2540

- **Entry level Layer 2/2+ access switches** optimized for mobile users that are easy to deploy and manage; Robust feature set with ACLs, sFlow, and IPv6

- **Right size deployment** with choice of 8, 24, 48 port 10/100 and Gigabit switches

- **AirWave and ClearPass** Policy Manager integration

- Ready for the software defined network with **REST APIs**

- **Energy savings** with Energy Efficient Ethernet, quiet fan-less models and low power mode settings

- **2530**: Fast Ethernet and Gig

- **2540**: Convenient built-in 10GbE uplinks and static/RIP

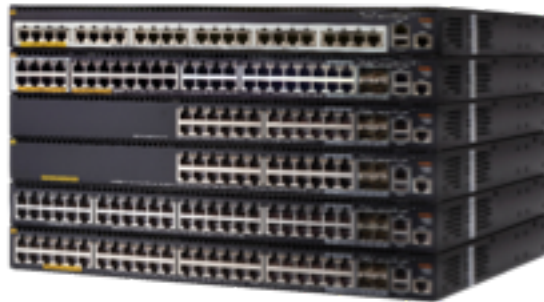| **Cloud manageable with Aruba Central**	**Up to 370W PoE+ for IoT, APs and cameras**	**Zero Touch Provisioning**

Aruba 2930F and 2930M Switch Series

Aruba 2930F

Aruba 2930M

- **Powerful Layer 3 access switches** optimized for digital workplace with enterprise features - static, RIP and Access OSPF routing, ACLs, sFlow, IPv6. No software licensing required

- **Zero Touch Deployment**

- **AirWave and ClearPass** Policy Manager integration

- **Scalable and resilient** stacking

- Ready for the software defined network with **REST APIs**

- **2930M**: Smart Rate, modular uplinks (10/40GbE) and power

- **2930F**: Fixed 1/10GbE uplinks, up to 740W fixed PoE+

| **Cloud manageable with Aruba Central** | **Smart Rate multi-gig** **Future proof with more speed** | **Up to 1440W PoE+ power** **for IoT, APs and cameras** |

Aruba 3810 and 5400R Switch Series

Aruba 3810M

Aruba 5400R

- **High performance advanced Layer 3 switches** ideal for wireless aggregation with low latency and fast 10/40GbE uplinks
- **Scalable** and resilient stacking
- **Redundant and resilient** with hot swappable power, redundant mgmt.
- **AirWave and ClearPass** Policy Manager integration
- Ready for the software defined network with **REST APIs**
- **Smart Rate** for future proof high speed multi-gigabit capacity
- **3810**: Hot swappable modular power, modular uplinks
- **5400R**: High resiliency with modular chassis with redundant management and power. Flexible connectivity modules

Cloud manageable with Aruba Central	Full 30W PoE on all ports for IoT, APs and cameras	Fast 10GbE and 40GbE uplinks for more capacity

Aruba 5400r Line Card Options

SmartRate

Aruba 20-port 10/100/1000BASE-T PoE+/4p 1/2.5/5/10GBASE-T PoE+ MACsec

Features: Combo Gig-T and HPE Smart Rate 1,2.5,5,10GT, PoE+, MACsec, Full Line Rate[1]

Aruba 8-port 1/2.5/5/10GBASE-T PoE+ MACsec

Features: HPE Smart Rate 1,2.5,5,10GT, PoE+, MACsec, Full Line Rate[1]

40GB Options

Aruba 20-port 10/100/1000BASE-T PoE+ MACsec/1-port 40GbE QSFP+

Features: Combo Gig-T and 40GbE QSFP+, PoE+, MACsec, Full Line Rate[1]

Aruba 2-port 40GbE QSFP+

Features: 40GbE QSFP+, Full Line Rate[1]

1/10GB PoE+ Options

Aruba 24-port 10/100/1000BASE-T PoE+ MACsec v3 zl2 Module (J9986A)

Features: Gig-T, PoE+, MACsec, Full Line Rate[1]

Aruba 20-port 10/100/1000BASE-T PoE+/4-port 1G/10GbE SFP+ MACsec v3 zl2 Module (J9990A)

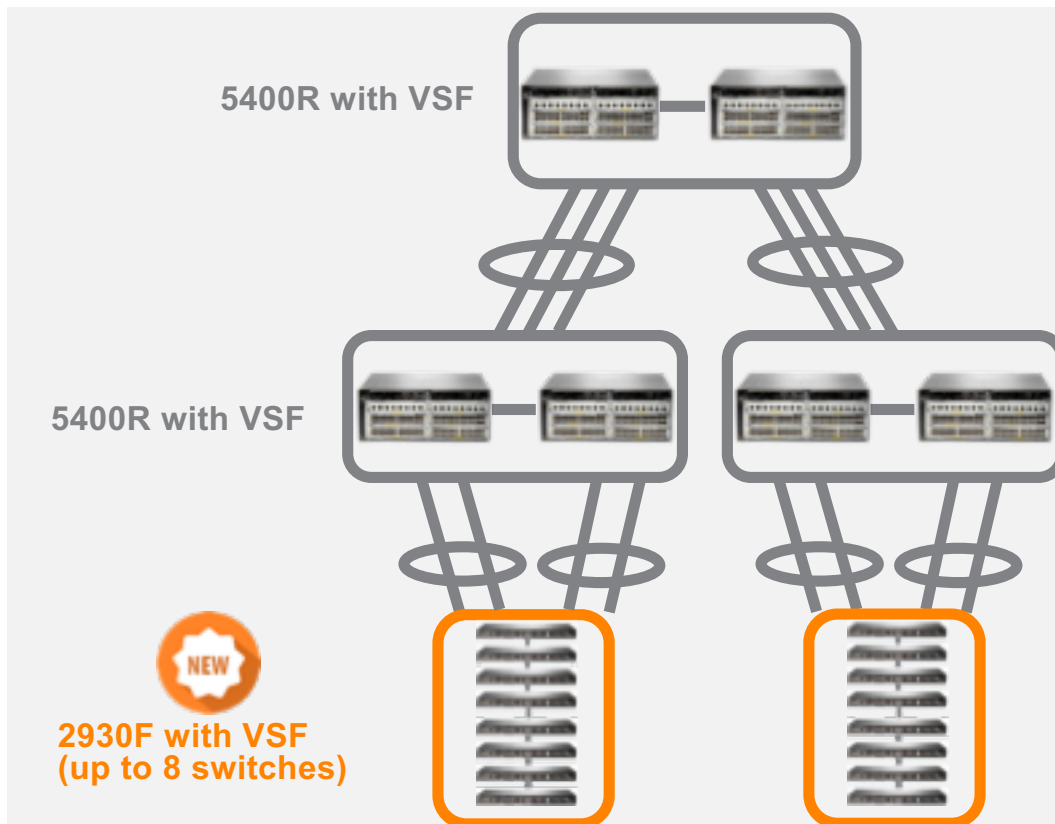**Features:** Gig-T, 10GbE, PoE+, MACsec, Full Line Rate[1]

Aruba 12-port 10/100/1000BASE-T PoE+/12-port 1GbE SFP MACsec v3 zl2 Module (J9989A)

Features: Combo Gig-T and SFP, PoE+, MACsec, Full Line Rate[1]

AIRHEADS
meetup

HOME

#ArubaAirheads 16

More scalability with 8 member Aruba 2930F VSF stack

5400R with VSF

5400R with VSF

NEW

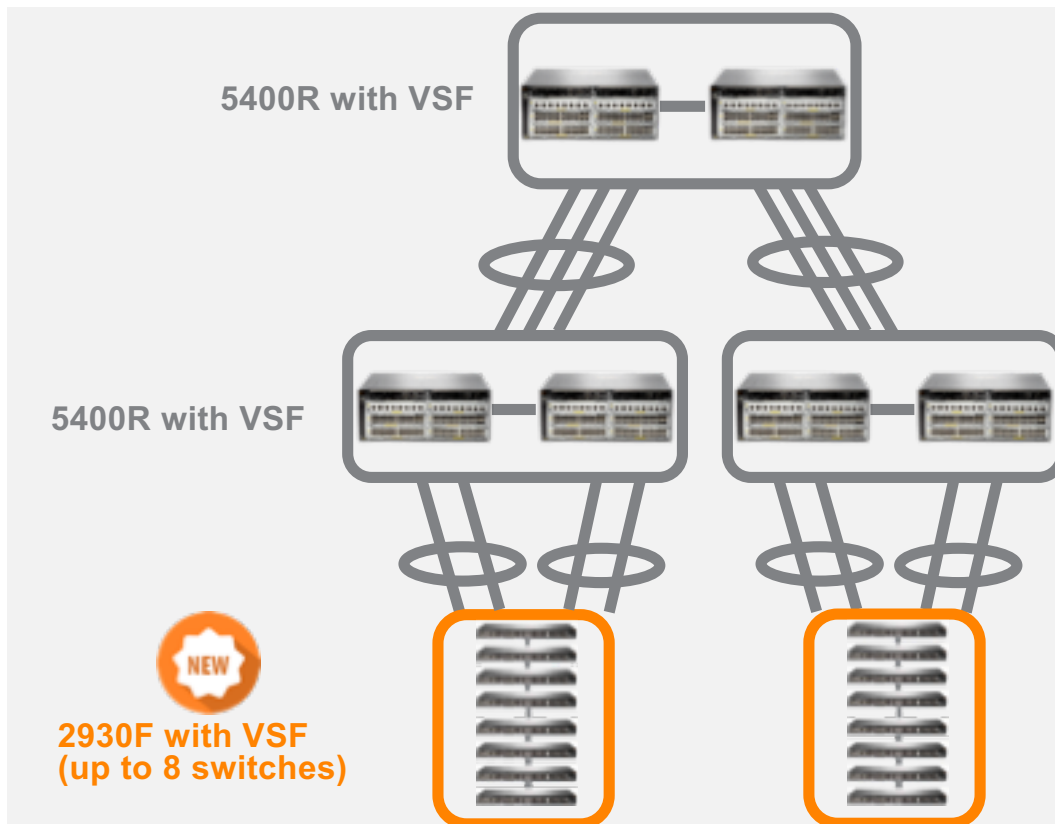**2930F with VSF
(up to 8 switches)**

Benefits
- **Simplify network operations**
- **Scalable performance**
- **Increases resiliency**

VSF on Aruba 5400R and 2930F
- Aruba 5400R – up to 2 members
- Aruba 2930F – up to 8 members
  - Mix and match of 2930F models

8 member 2930F stacking with mix and match requires ArubaOS-Switch 16.06

More scalability with 8 member Aruba 2930F VSF stack

5400R with VSF

5400R with VSF

NEW

**2930F with VSF
(up to 8 switches)**

Benefits
- **Simplify network operations**
- **Scalable performance**
- **Increases resiliency**

VSF on Aruba 5400R and 2930F
- Aruba 5400R – up to 2 members
- Aruba 2930F – up to 8 members
  - Mix and match of 2930F models

8 member 2930F stacking with mix and match requires ArubaOS-Switch 16.06

# HTTP Proxy Support for Zero Touch Provisioning

Central

Cloud-based
wired + wireless access
network management

- Addresses frequent enterprise concern of using Aruba Central because most enterprises do not allow network infrastructure devices to be available on the Internet due to security concerns. In case any switch or AP needs to talk to the internet, they will have to go via a HTTP proxy.

- Support for this basic use case and also provide a mechanism by which the switches can know the right proxy to use as part of the ZTP workflow.

Aruba Central Support for Stacking
5400R (VSF) and 2930M (Backplane)

Aruba Central

5400R with
VSF Stacking
(2 switches)

2930M with
Backplane Stacking
(up to 10 switches)
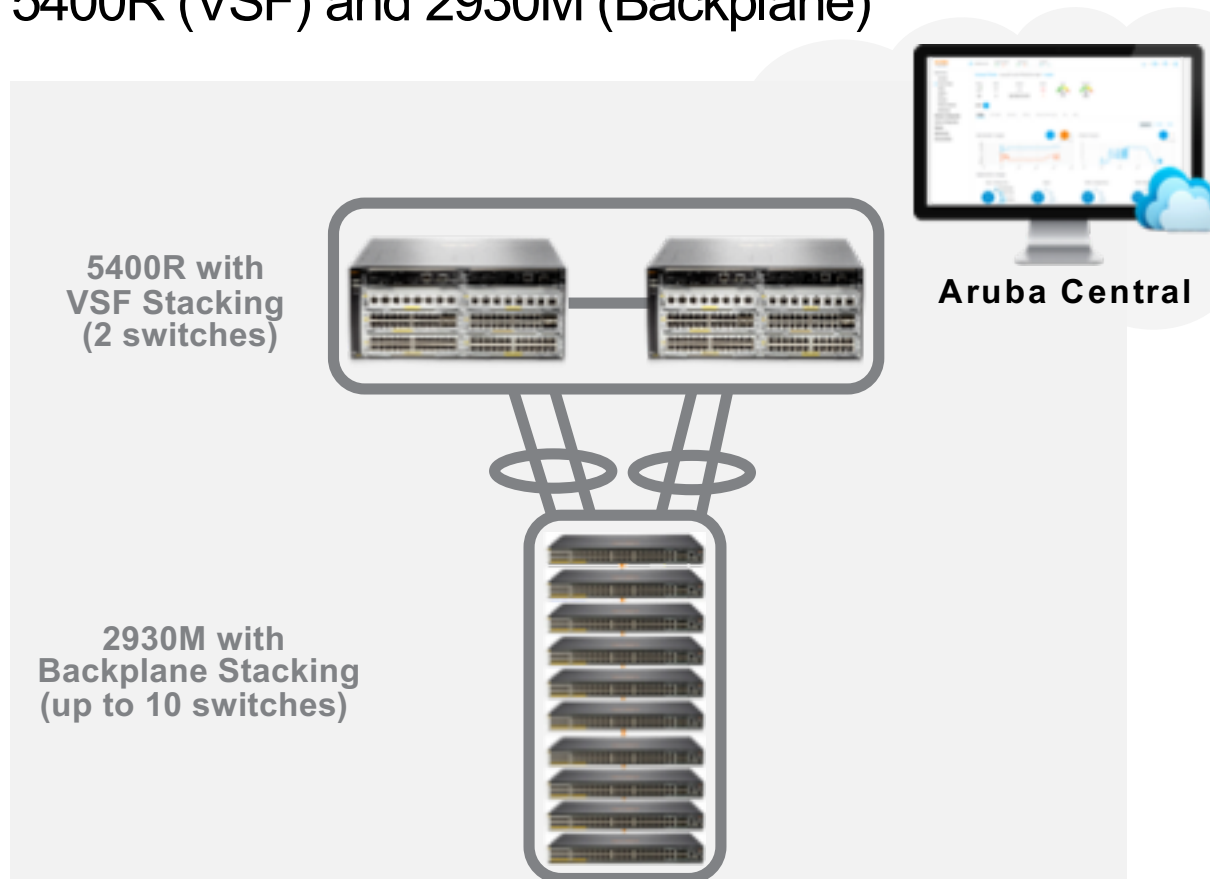
Benefits
Simplified management for common use case at branch offices
- No longer have to manage the switches individually

Requires ArubaOS-Switch 16.06

INDUSTRY LEADING WARRANTY AND NO SOFTWARE LICENSING

CAMPUS ACCESS SWITCHES

Hardware Warranty
Original Owner Lifetime
Replacements
NBD Shipment
Software Updates
Posted Releases
Phone Support
(Best Effort, Product Conformance)
24x7 for 90 Days
8x5 for Lifetime

CAMPUS CORE SWITCHES

Hardware Warranty
5 year
Replacements
10 day shipment
Software Updates
Posted Releases
Phone Support
(Best Effort, Product Conformance)
8x5 for 90 days

hpe.com/networking/warrantysummary

THANK YOU

#ArubaAirheads