aruba NETWORKS

atmosphere 2015
HOW TOMORROW MOVES

ARUBA WLANS 101 AND DESIGN FUNDAMENTALS

Tim Cappalli

March 2015

About Me

- **Sr. Mobility Solutions Architect**
  Wireless Practice Lead
- **Boston, MA**
- **Airheads Community: cappalli**
- **Favorite product? ClearPass**

@tcappy0707

about.me/timcappalli

CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Agenda

- **Mobility controller architecture**
- **Aruba Instant architecture**
- **RAP-NG / IAP-VPN**
- **Management platforms**
  - Aruba Central
  - AirWave
- **Discussion & Questions**

CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Deployment types

- **Mobility Controller: Master-local**
- **Mobility Controller: All masters**
- **Instant**
- **Instant: RAP-NG**
- **Hybrid! (all of the above, mix and match)**

CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Mobility Controller Architecture

Mobility Controller Family

7200 SERIES

256 APs
4,096 IPSec

512 APs
16,384 IPSec

1,024 APs
24,576 IPSec

2,048 APs
32,768 IPSec

CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Mobility Controller Family

CLOUD SERVICES CONTROLLERS

16 APs
Can be powered via PoE

64 APs

32 APs
10 PoE+

CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

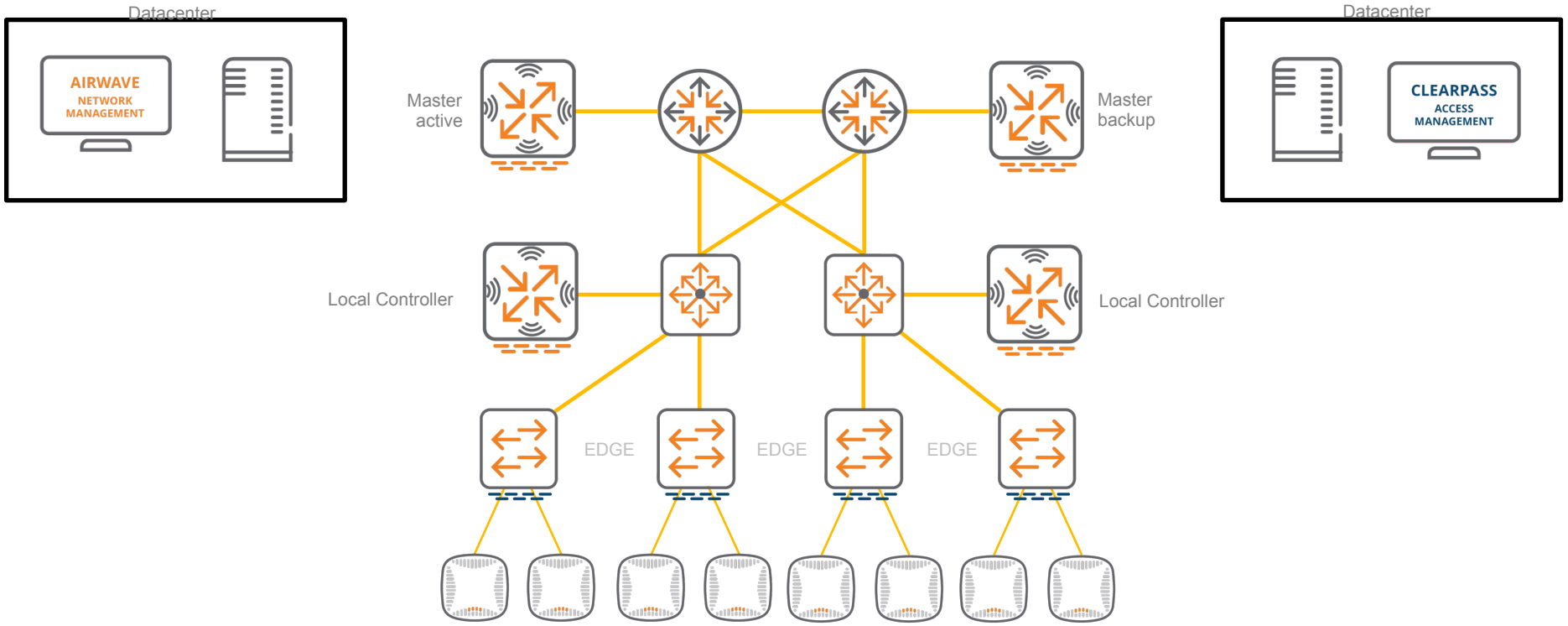
Mobility Controller Family

CLOUD SERVICES CONTROLLERS

32 APs, 24 PoE+, 2x10G

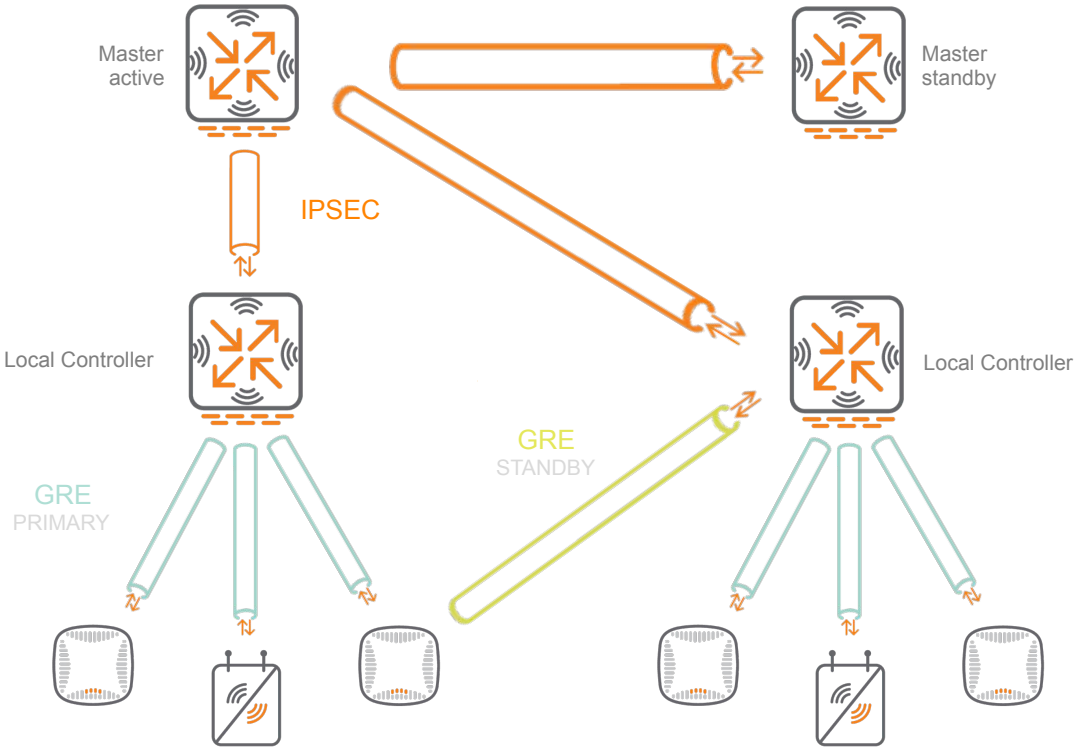
CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Campus physical topology



CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

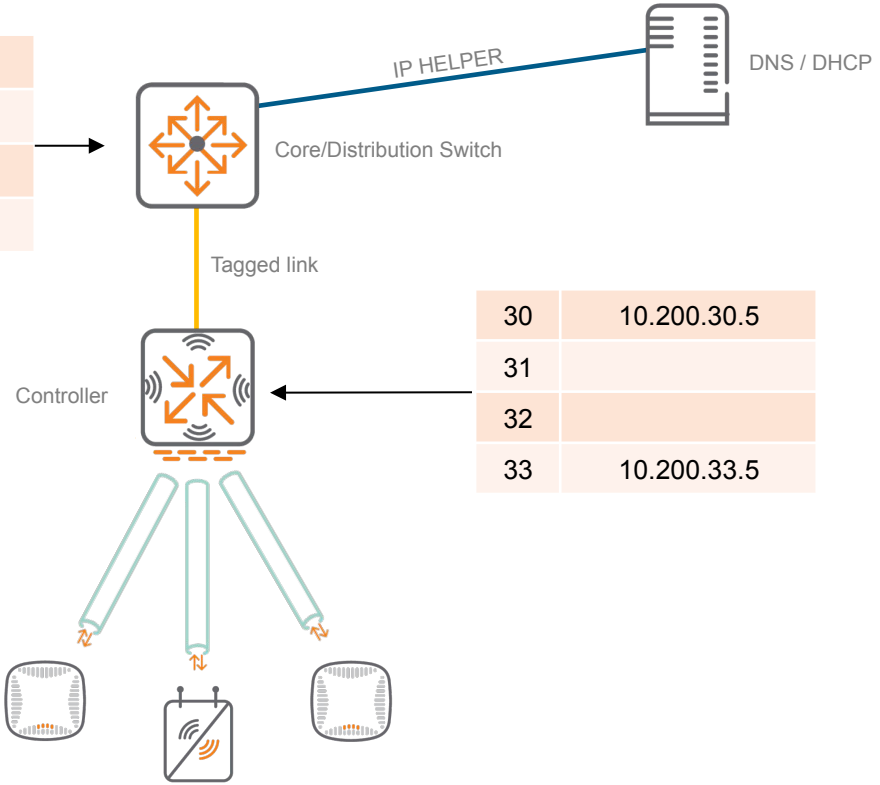
Campus logical topology



CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

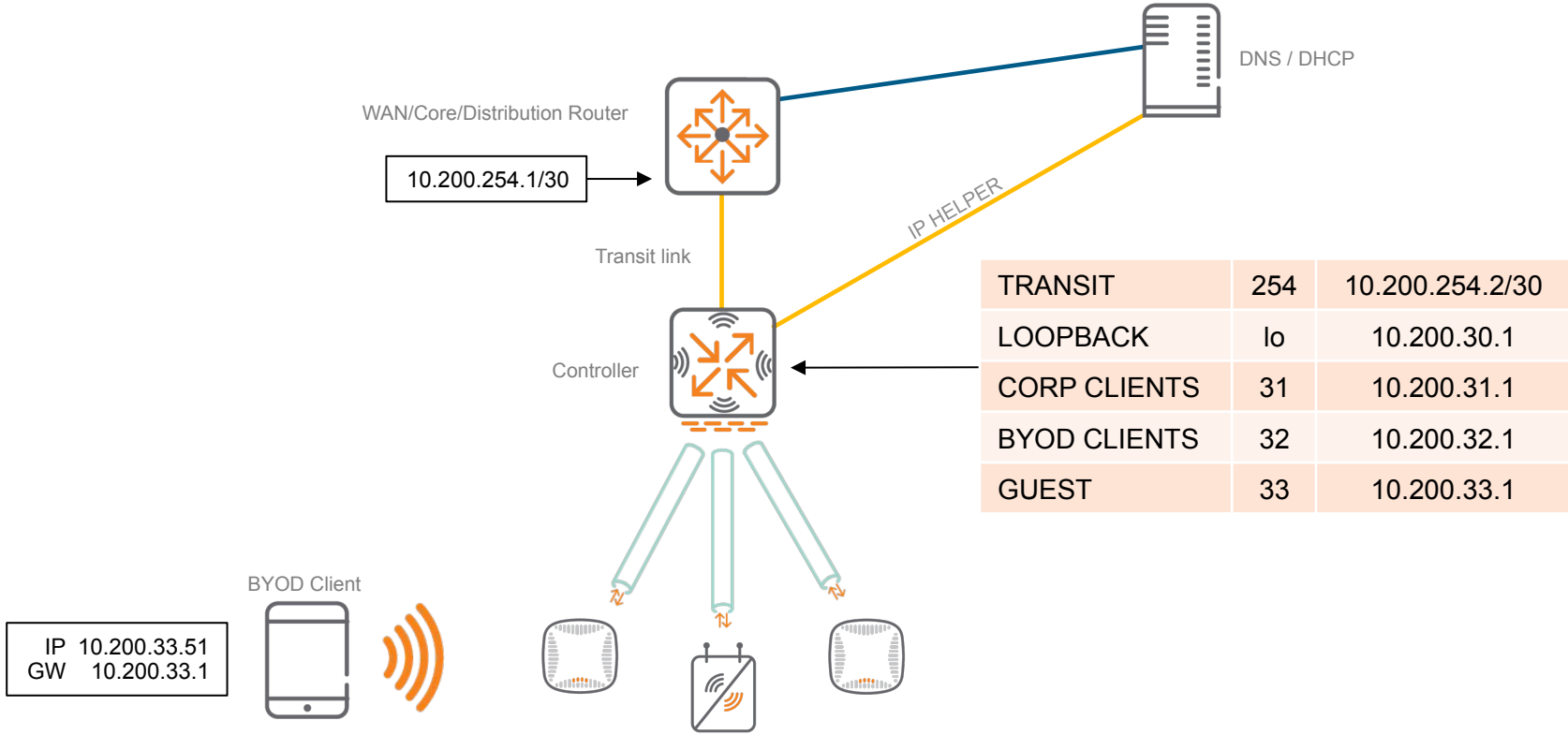
L2 Deployment

MGMT	30	10.200.30.1
CORP CLIENTS	31	10.200.31.1
BYOD CLIENTS	32	10.200.32.1
GUEST	33	10.200.33.1



CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

L3 Deployment



TRANSIT	254	10.200.254.2/30
LOOPBACK	lo	10.200.30.1
CORP CLIENTS	31	10.200.31.1
BYOD CLIENTS	32	10.200.32.1
GUEST	33	10.200.33.1

CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Master controller responsibilities

- **Policy configuration**
- **Wireless security (WIPS / RFProtect)**
- **AP white lists (CAPs w/ CPsec and RAPs)**
- **Initial AP configuration**
- **Authentication and roles**

CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Local controller responsibilities

- **AP and session termination**
  - Terminates AP tunnels
  - User traffic processed and forwarded
- **RFProtect enforcement and blacklisting**
- **ARM**
- **Mobility**
- **QoS**

CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Controller scaling

- **Controller scaling table (VRD)**
- **The important numbers**
  - AP capacity
  - User/device capacity << important!
  - Tunnel capacity
- **WMS scaling for master controller**
  - Master controller may need to be larger than the locals depending on the environment

CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Controller scaling

- **Platform**
  - 7000 series (7005/7010/7024/7030) should only be used as local controllers*
  - 7200 series should be master for multiple 7000 locals
- **Failover capacity**

CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Campus Forwarding Modes

- **Tunnel**
- **Bridge**
- **Decrypt-tunnel**

- **Configured per virtual-ap and per ethernet interface**
- **Choose based on network topology and requirements**

CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Tunnel

- All traffic is tunneled back to controller
- User VLANs live in controller
- Wired network is a high-speed overlay network
- User traffic passes through stateful firewall and deep packet inspection engine (*on 7 series controllers)

CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Bridge

- User traffic bridged out to local network
- User VLANs live in edge network
- Authentication traffic tunneled to controller
- Control plane security (cpsec) required
- Captive portal authentication is not supported

CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

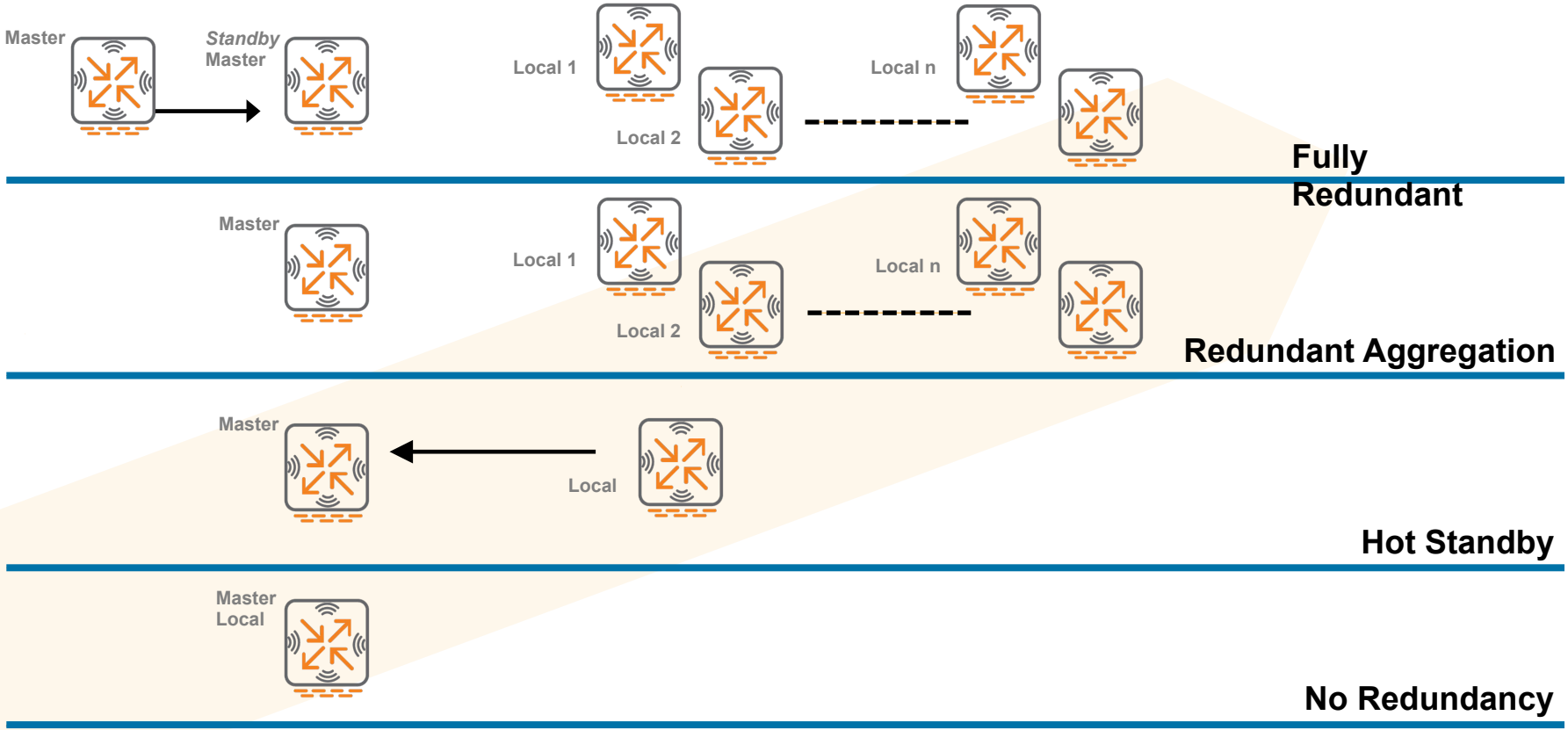
Decrypt-tunnel (d-tunnel)

- User VLANs live in controller
- AP decrypts traffic and strips 802.11 headers
- AP adds 802.3 headers and frame is encapsulated in GRE tunnel to controller
- Controller applies firewall policies to traffic
- Solves double-encryption issues when using a VPN
- Control plane security (cpsec) required

CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

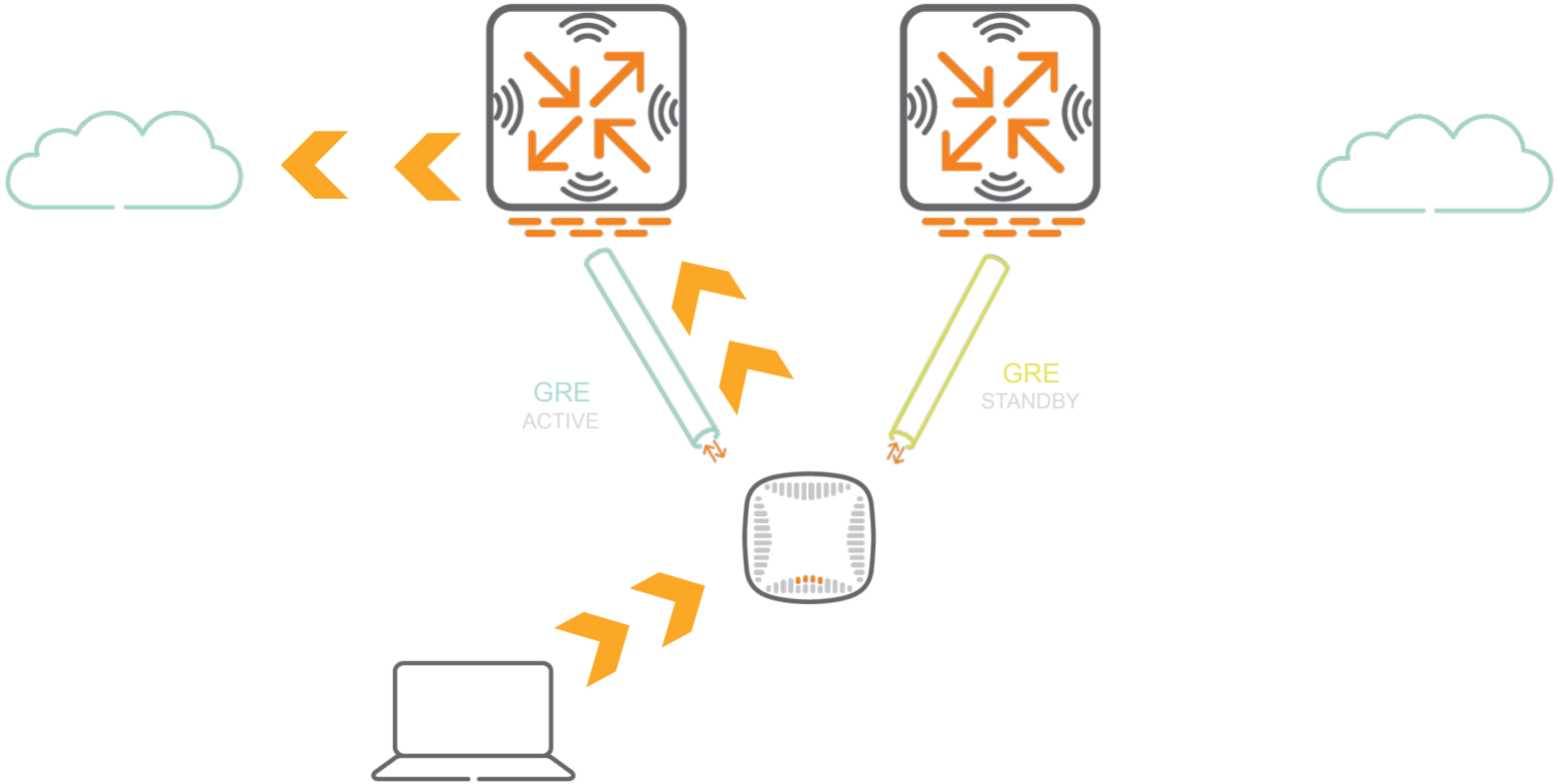
Campus Redundancy

Master-Local Redundancy



CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

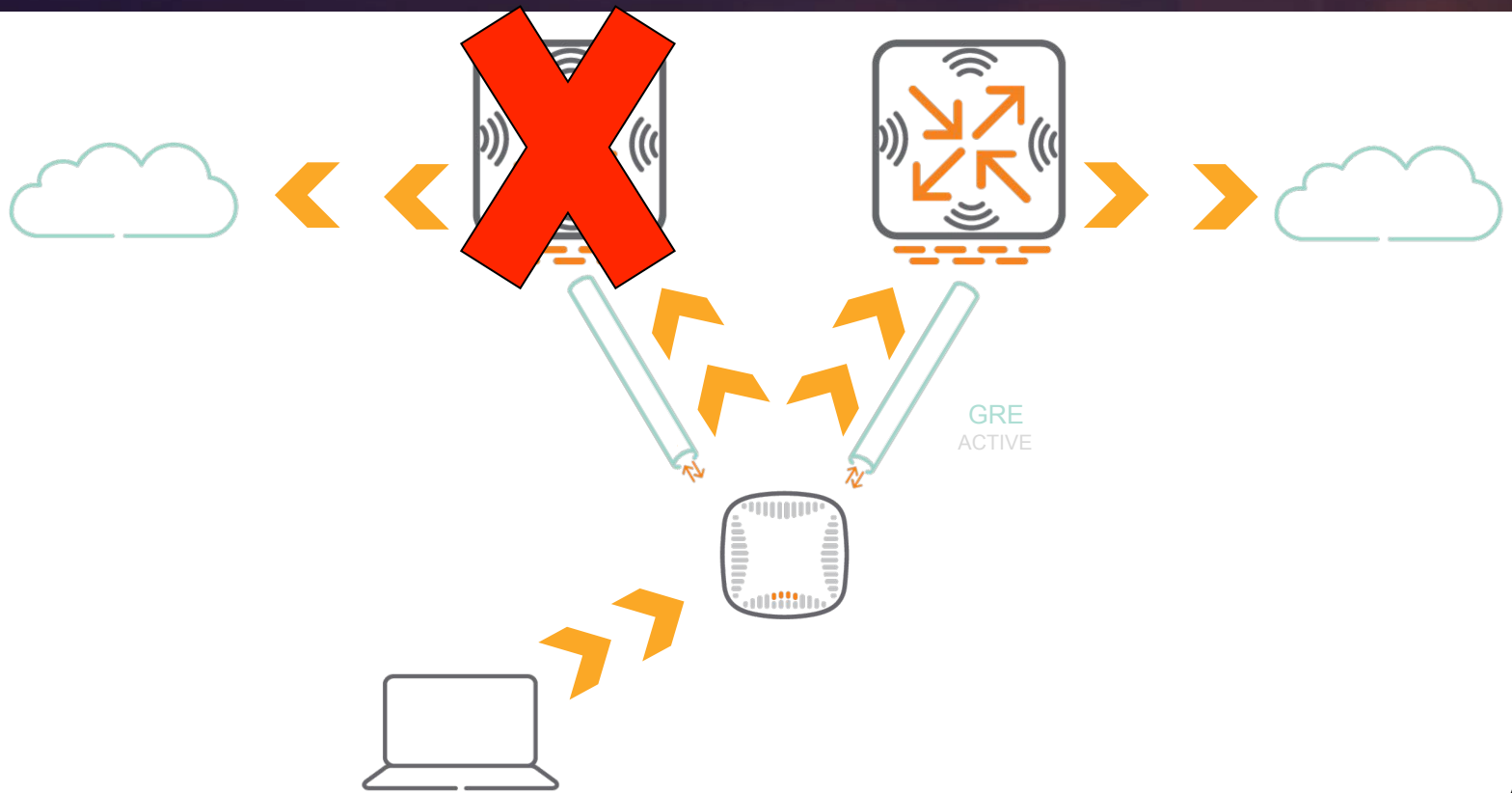
HA: AP Fast Failover



AOS 6.3+

CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

HA: AP Fast Failover



AOS 6.3+

CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

AP FF: Controller Roles

- **DUAL:** Primary for some APs, standby for others
- **ACTIVE**: Controller does not terminate standby tunnels for other controllers
- **STANDBY**: Controller only terminates standby tunnels

CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

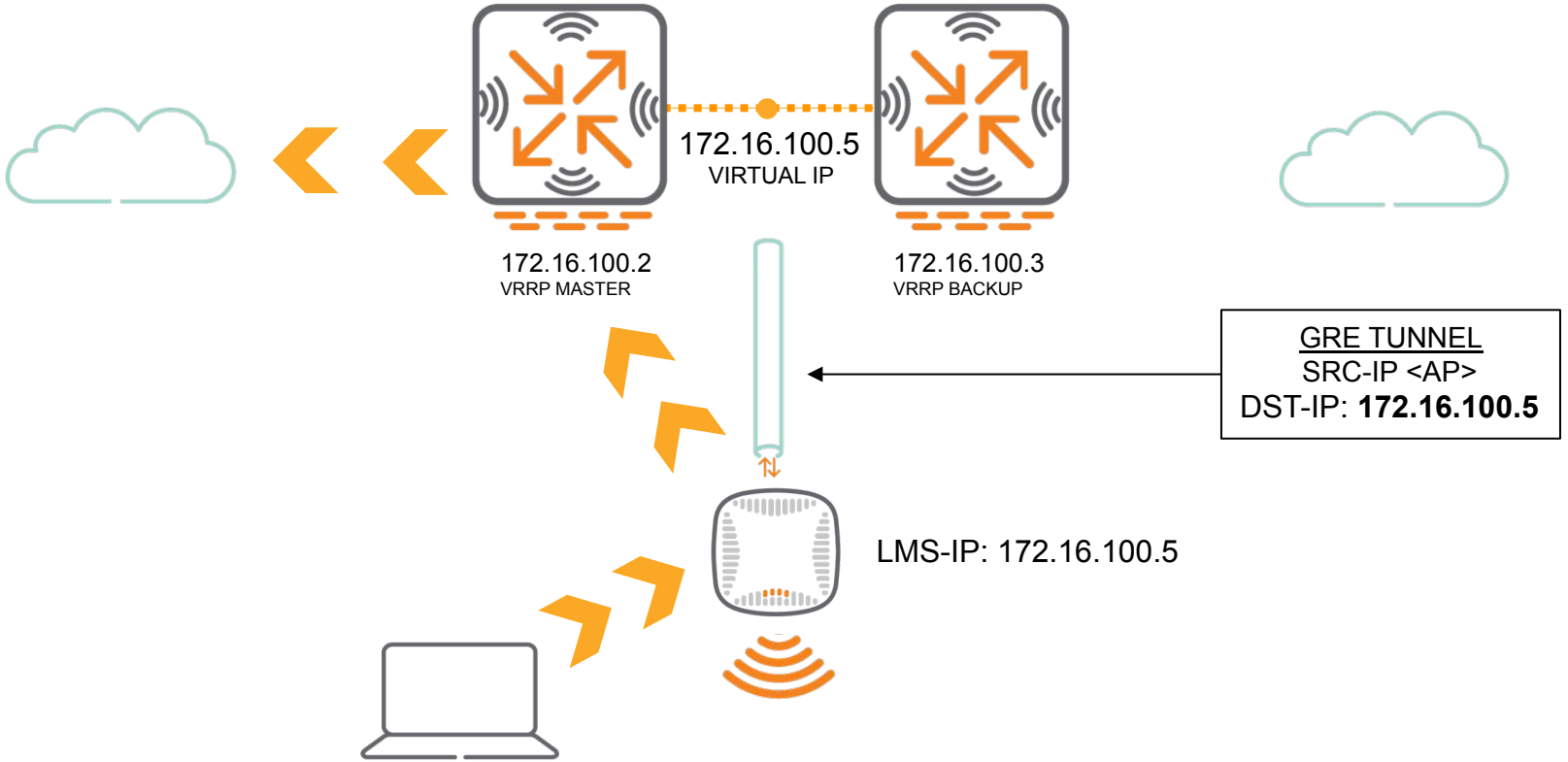
AP FF: N+1 Oversubscription

Controller Platform	Ratio	Max GRE tunnels
7000-series (70-05/10/24/30)	1:1	--
7210	4:1	16K
7220	4:1	32K
7240	4:1	64K
M3 & 3600	2:1	16K

AOS 6.**4**+

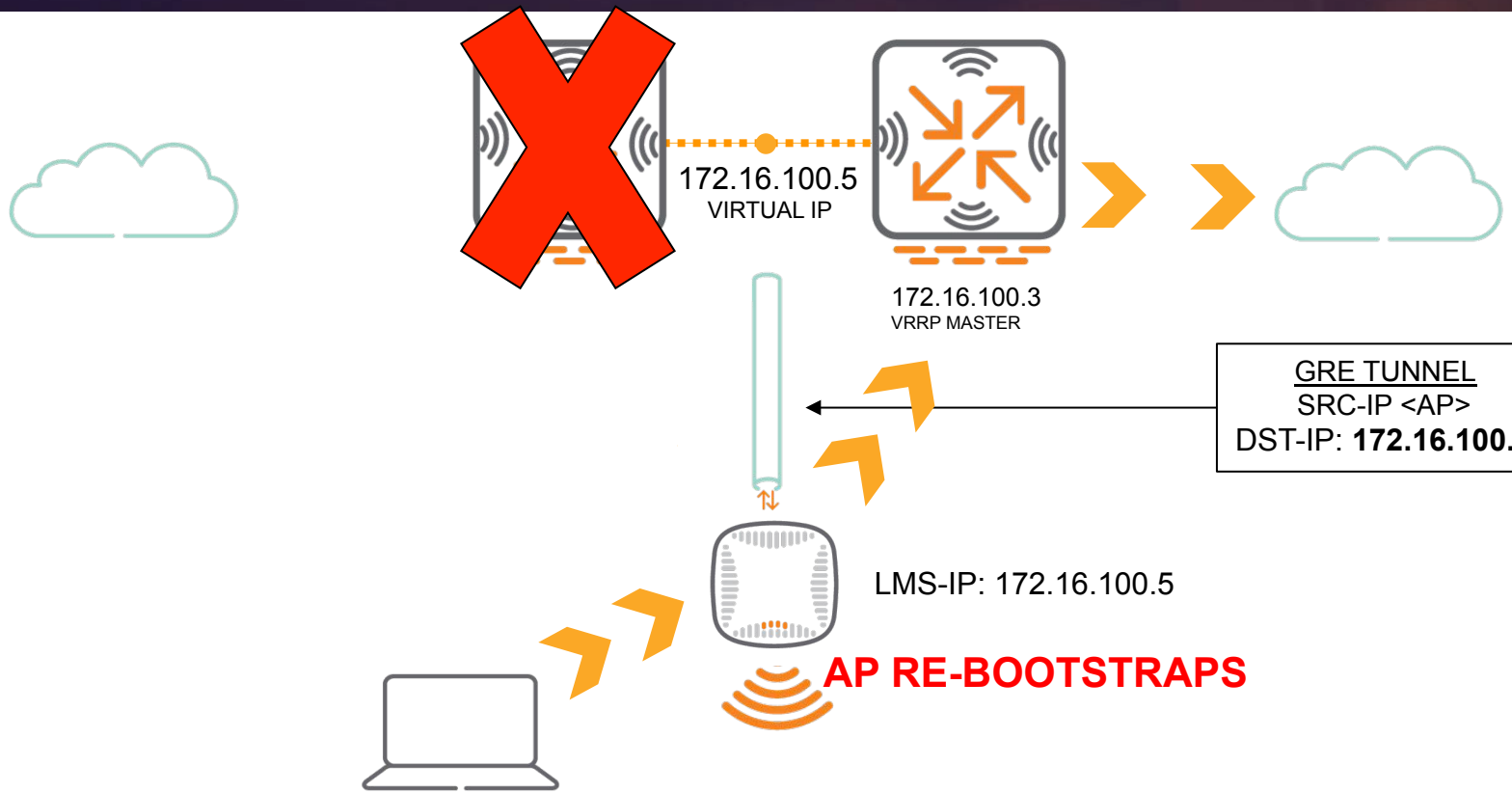
CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

VRRP Failover (L2)



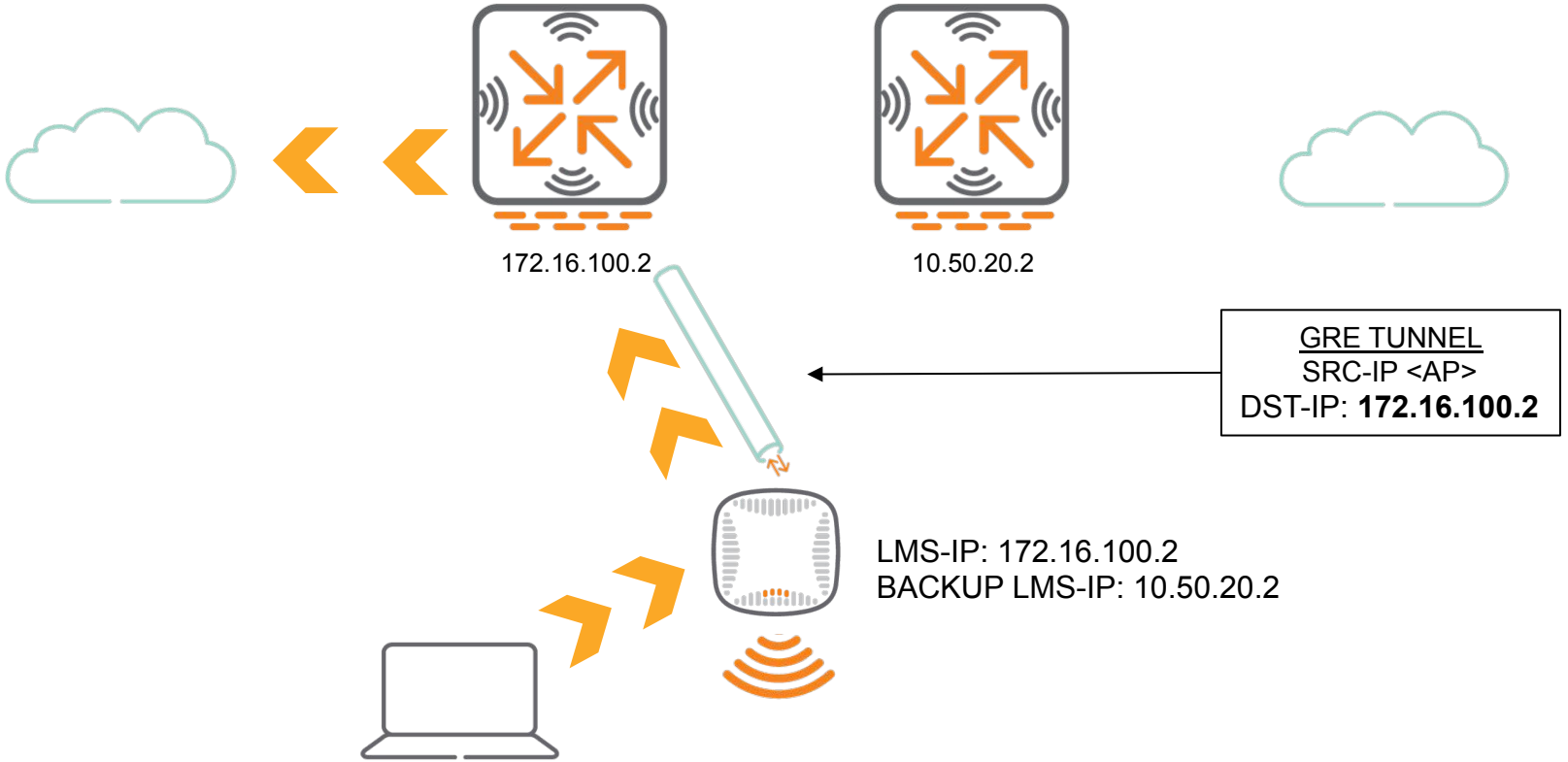
CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

VRRP Failover (L2)



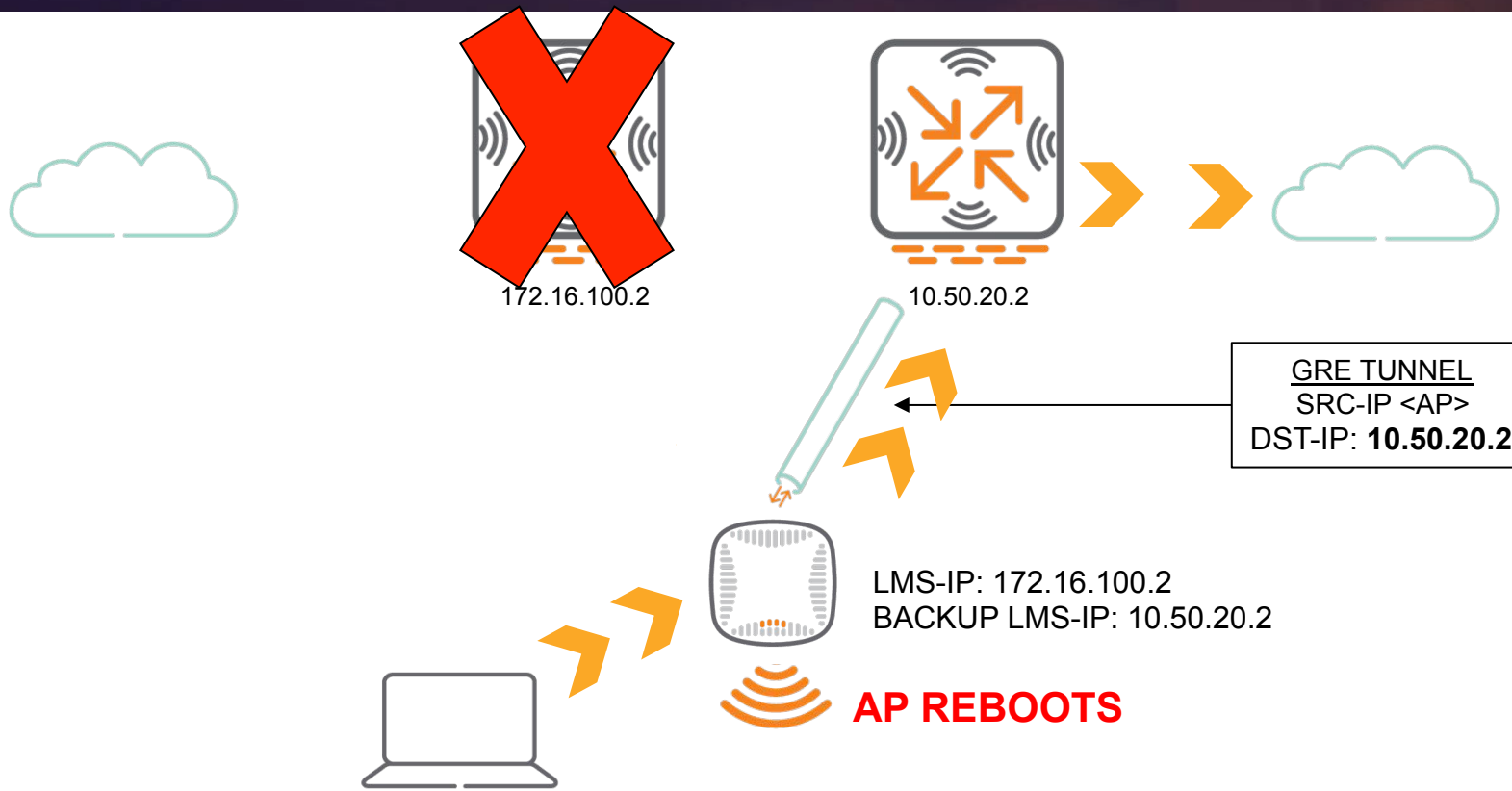
CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Backup-LMS (L3)



CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Backup-LMS (L3)



CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Remote AP (RAP)

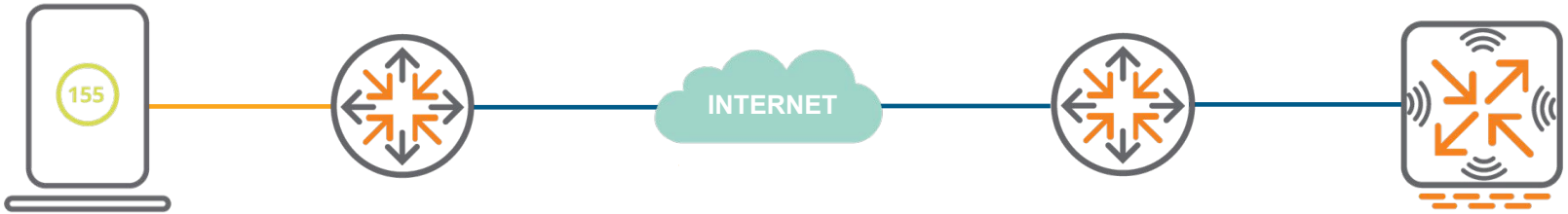
CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Remote AP (RAP)

- Purpose-built RAPs and campus APs
- Certificate-based provisioning
- Secure wired and wireless remote access
- RAPs are Instant out of the box
- Aruba Activate

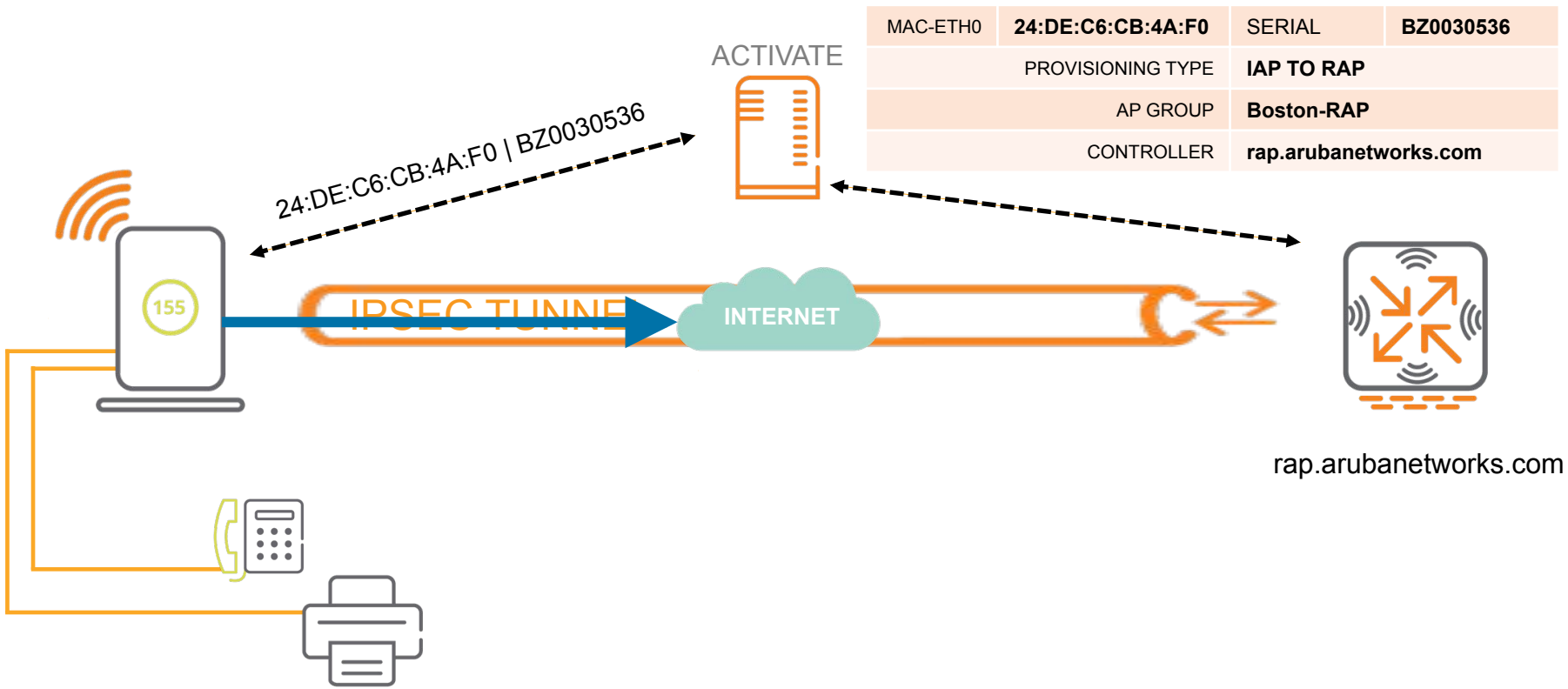
CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Remote AP



CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Remote AP - Logical



MAC-ETH0	**24:DE:C6:CB:4A:F0**	SERIAL	**BZ0030536**
PROVISIONING TYPE	**IAP TO RAP**		
AP GROUP	**Boston-RAP**		
CONTROLLER	**rap.arubanetworks.com**		

CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

RAP Forwarding Modes

- **Tunnel**
- **Bridge**
- **Decrypt-tunnel**
- **Split-tunnel**

CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Split-tunnel

- Tunnels certain traffic back to controller via IPSec tunnel (defined in user roles)
- Allows non-corporate traffic to be bridged out locally saving bandwidth.
- RAP handles encryption, decryption and firewall enforcement locally

CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Limitations

- **Roaming**
- **ARM features**
- **Requires controller licenses**
- **Limited visibility**

CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Aruba Instant Architecture

Aruba Instant Overview

- **AP model begins with the letter I**
  - IAP-225, IAP-215, IAP-205, etc
- **Instant APs can be converted to controller-based APs**
- **No feature licensing with local management**
- **Manage locally, via AirWave, or Aruba Central (cloud)**
- **Dynamic provisioning via Aruba Activate (free)**

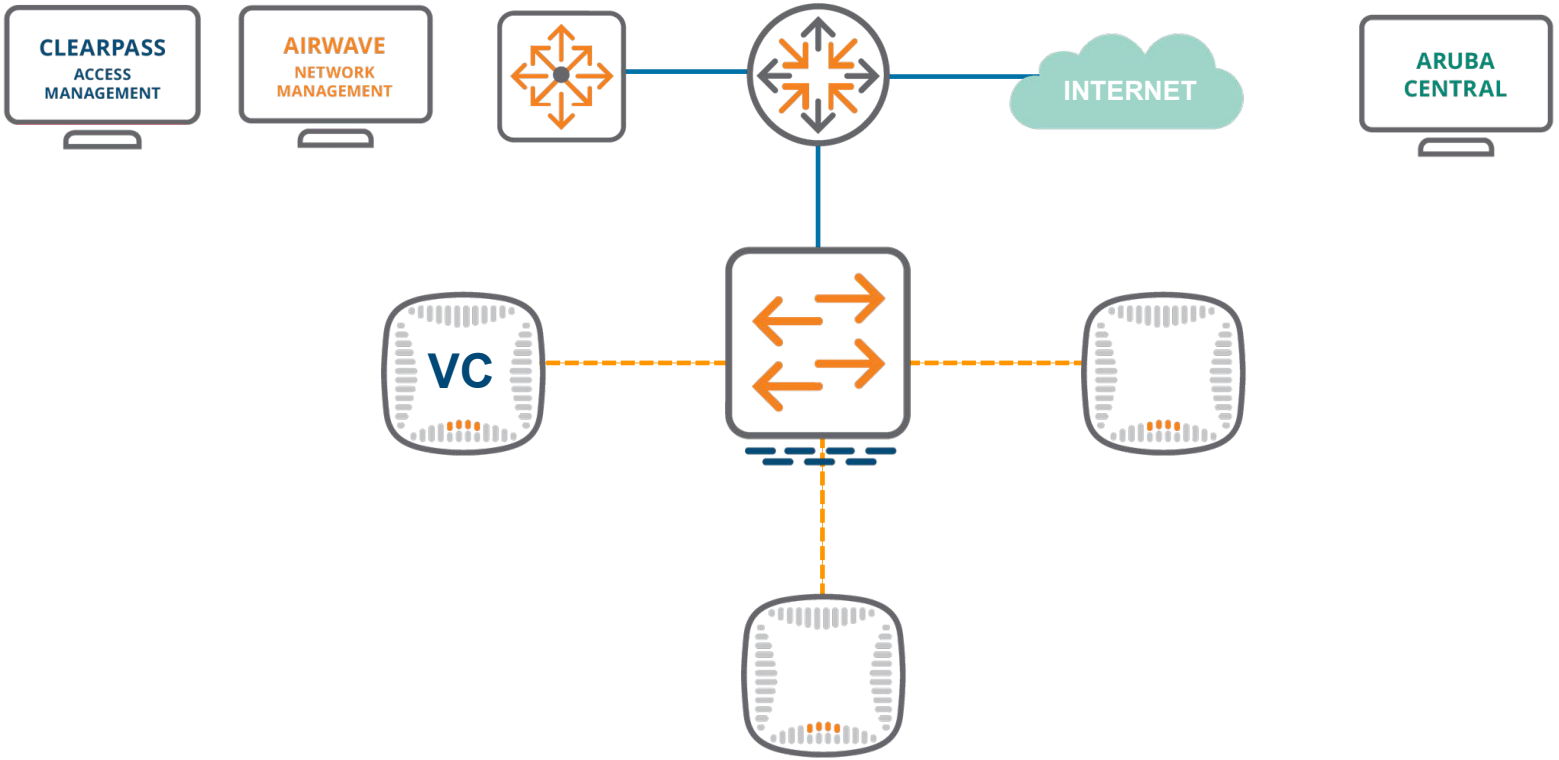
CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Aruba Instant Overview - Technical

- Cooperate locally at L2
- Multiple uplink options (Ethernet, 4G/LTE, WiFi)
- ARM, ClientMatch, AppRF, AirGroup, L3 Mobility
- IAP-VPN/RAP-NG for distributed environments

CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Instant topology



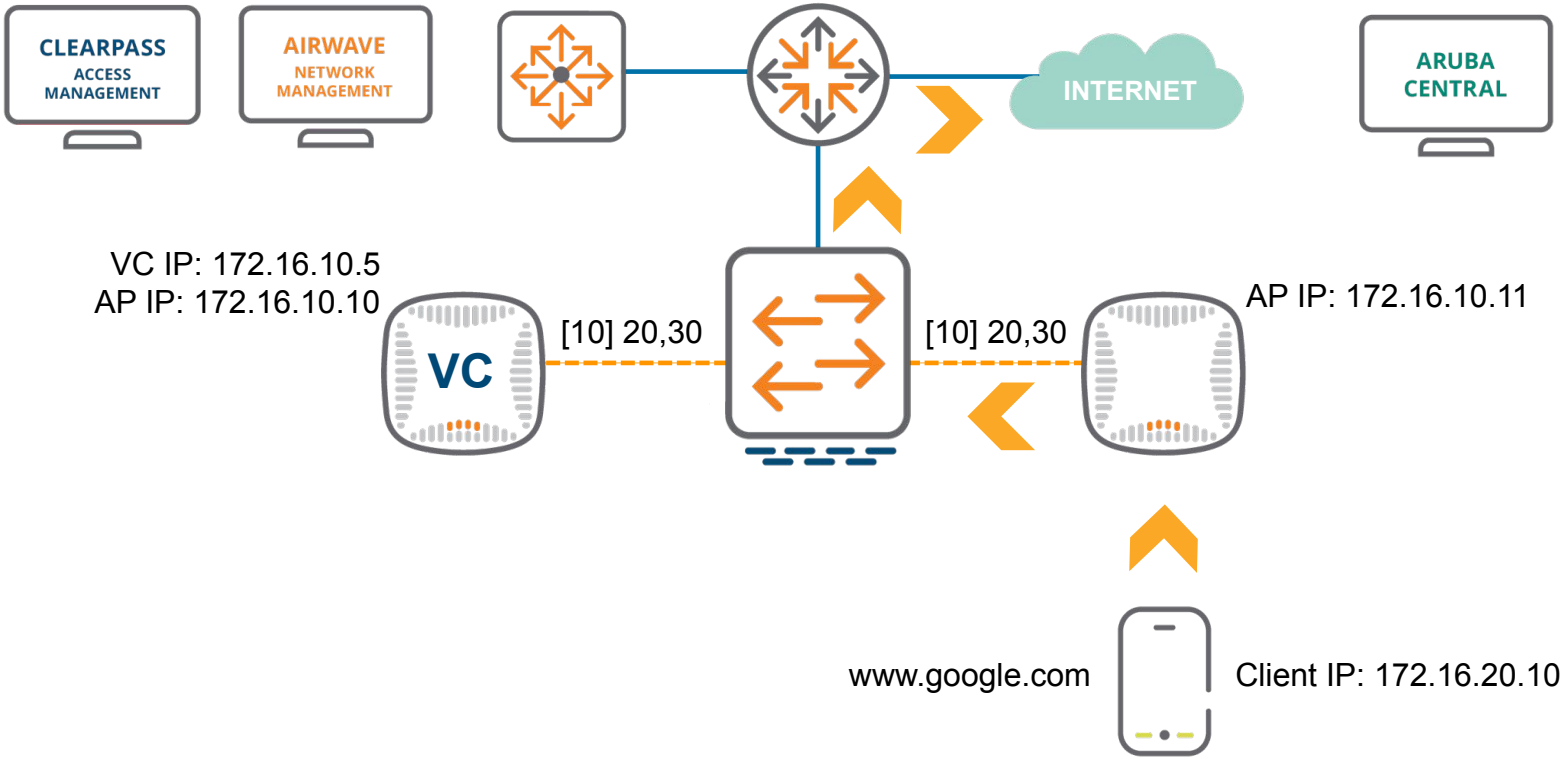
CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Instant traffic flow

- **Traffic destined for tunnels goes through VC**
- **NAT'd traffic (guest) goes through VC**
- **Regular user traffic firewalled, processed and switched out at AP**

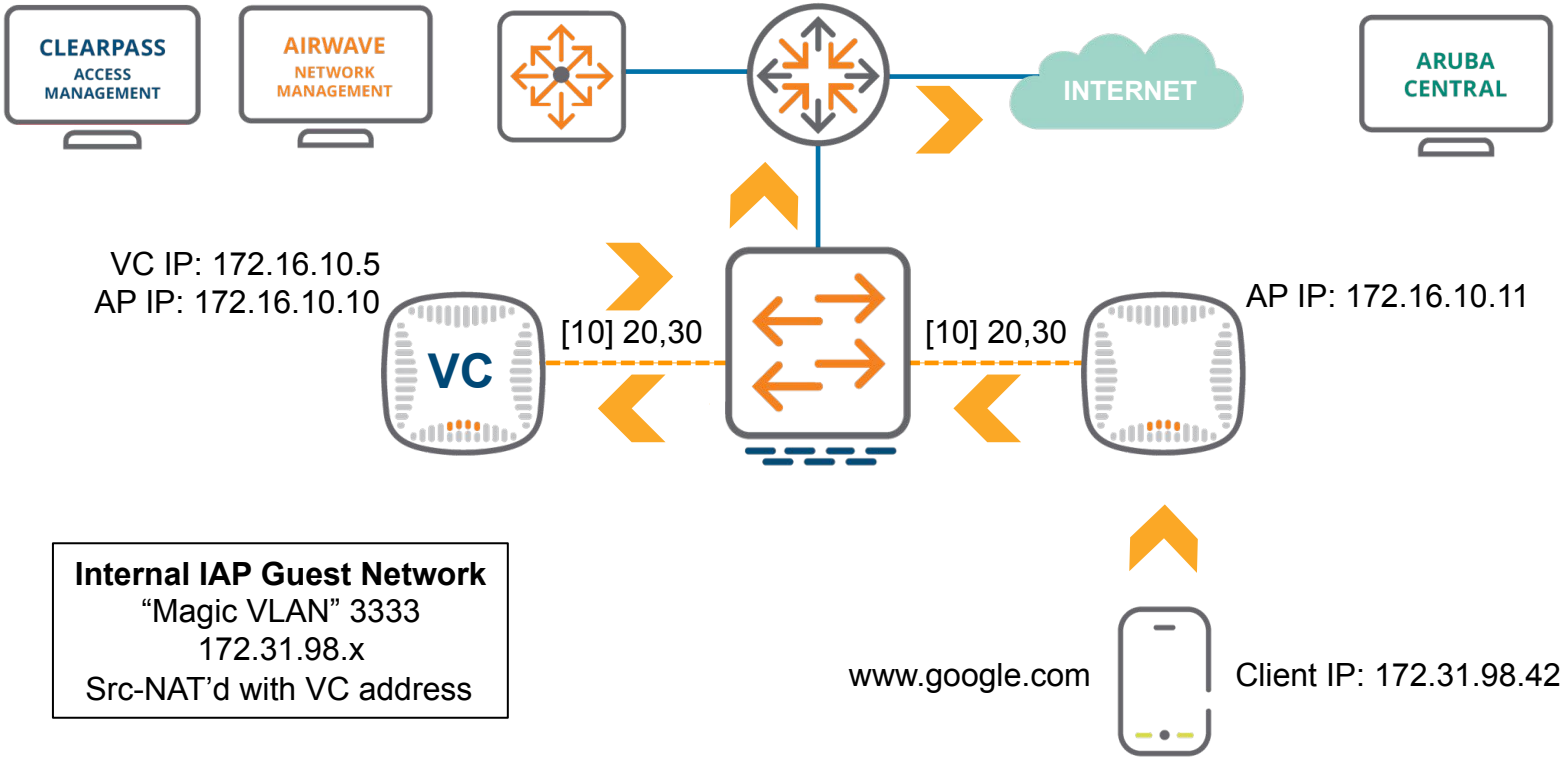
CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Instant traffic flow



CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

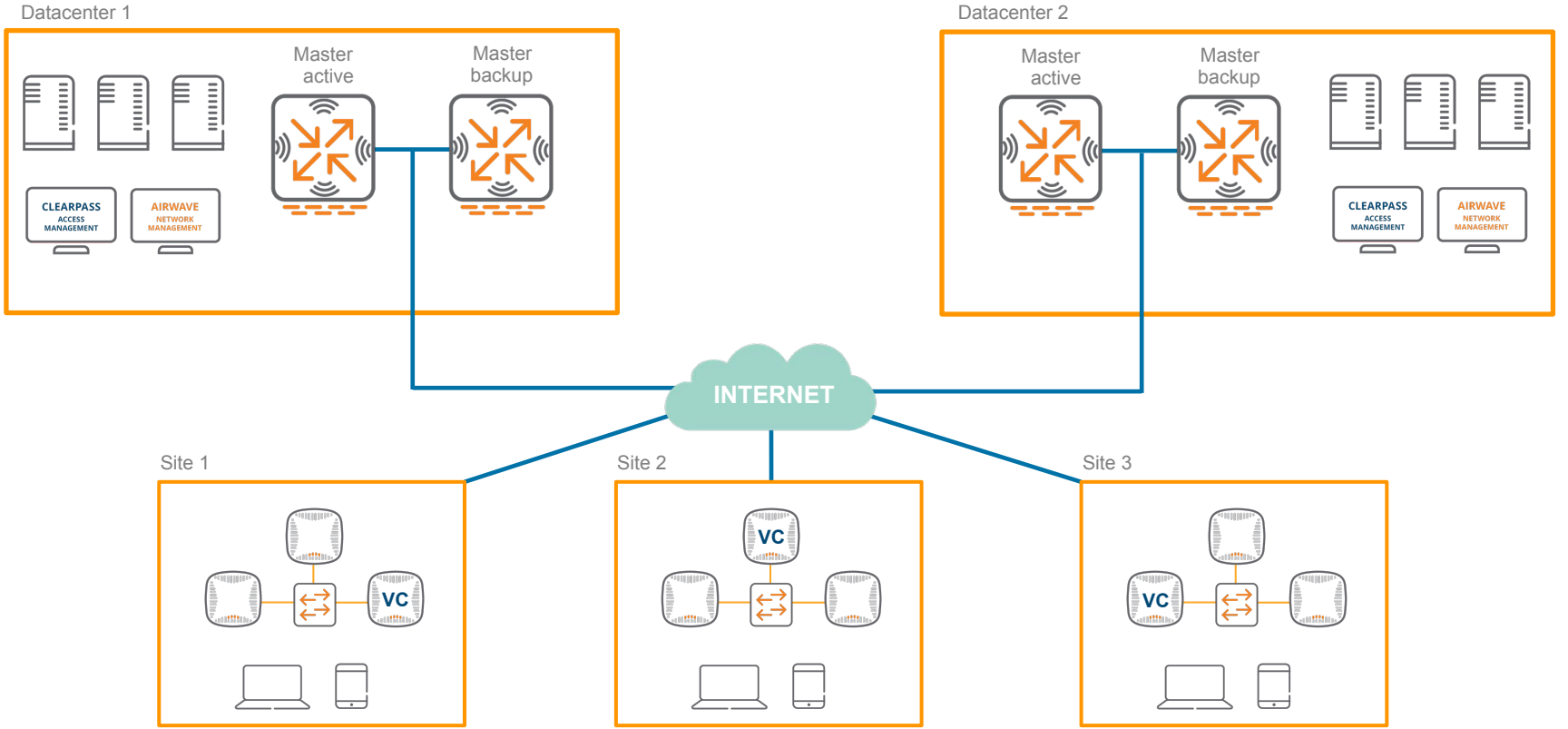
Instant traffic flow – Guest/NAT



CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

RAP-NG / IAP-VPN

RAP-NG / IAP-VPN Topology



CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Benefits

- **Local RF coordination**
- **Roaming**
- **Isolated broadcast domains for each cluster**
- **Authentication survivability**
- **MAS integration**

CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

DHCP modes

- **Local**
- **Centralized L2**
- **Distributed L2**
- **Centralized L3**
- **Distributed L3**

CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

DHCP modes

DHCP MODE	SUBNET	DHCP	CLIENT GW	CORP TRAFFIC	LCL/INTERNET
Local	Local	Master AP	Master AP	Src-NAT IPSec tunnel	Src-NAT Master AP IP
Centralized L2	CORP	Datacenter	Datacenter	Tagged & switched to datacenter via tunnel	Src-NAT Master AP IP
Distributed L2	CORP	Master AP	Datacenter	Tagged & switched to datacenter via tunnel	Src-NAT Master AP IP
Centralized L3	CORP	Datacenter	Master AP	Routed to datacenter inside IPSec tunnel	Src-NAT Master AP IP
Distributed L3	CORP	Master AP	Master AP	Routed to datacenter inside IPSec tunnel	Src-NAT Master AP IP

CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

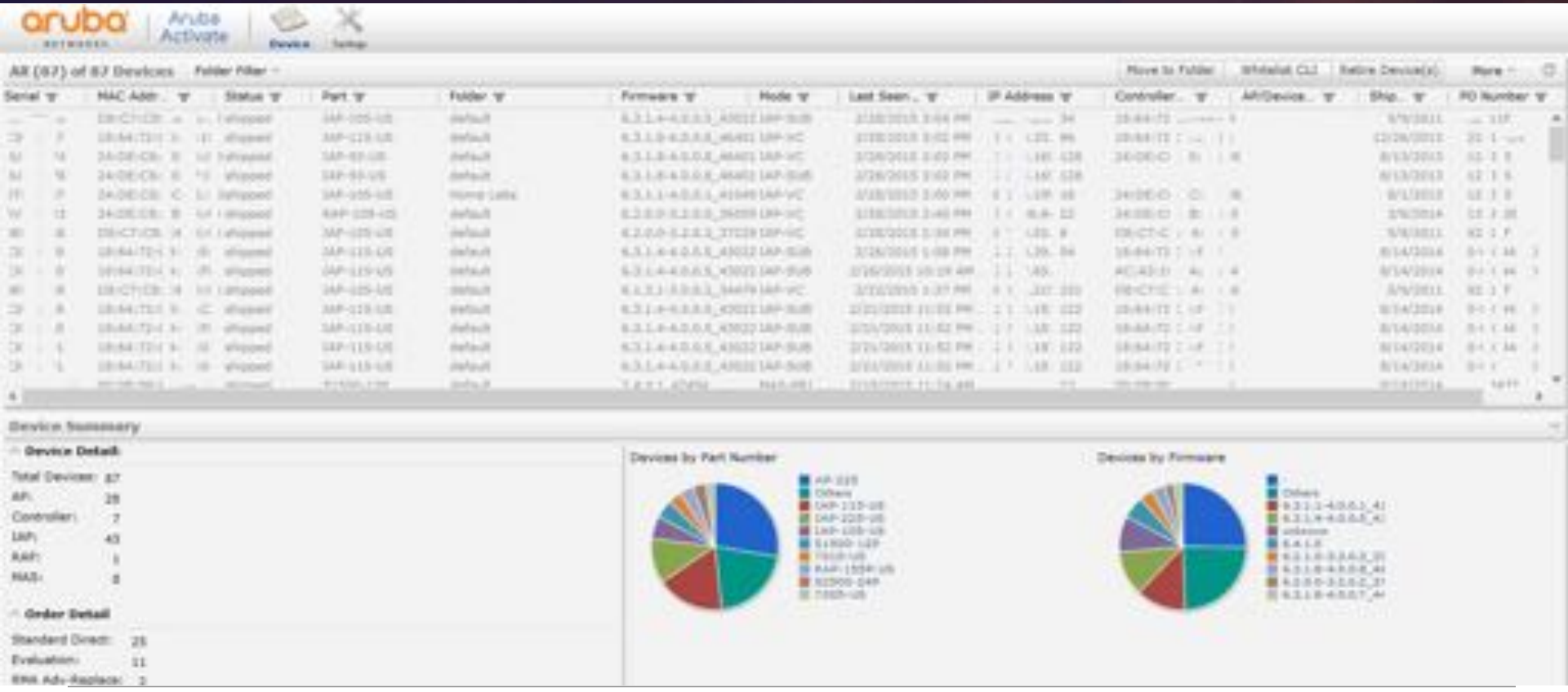
RAP-NG/IAP-VPN licensing

- **For basic VPN connectivity (single role), a single PEFNG license is required**
- **To use different roles for individual IAP clusters, the PEFV license is required for each controller**

CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Aruba Activate

Aruba Activate



CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Aruba Activate

CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

MANAGEMENT

Aruba Central

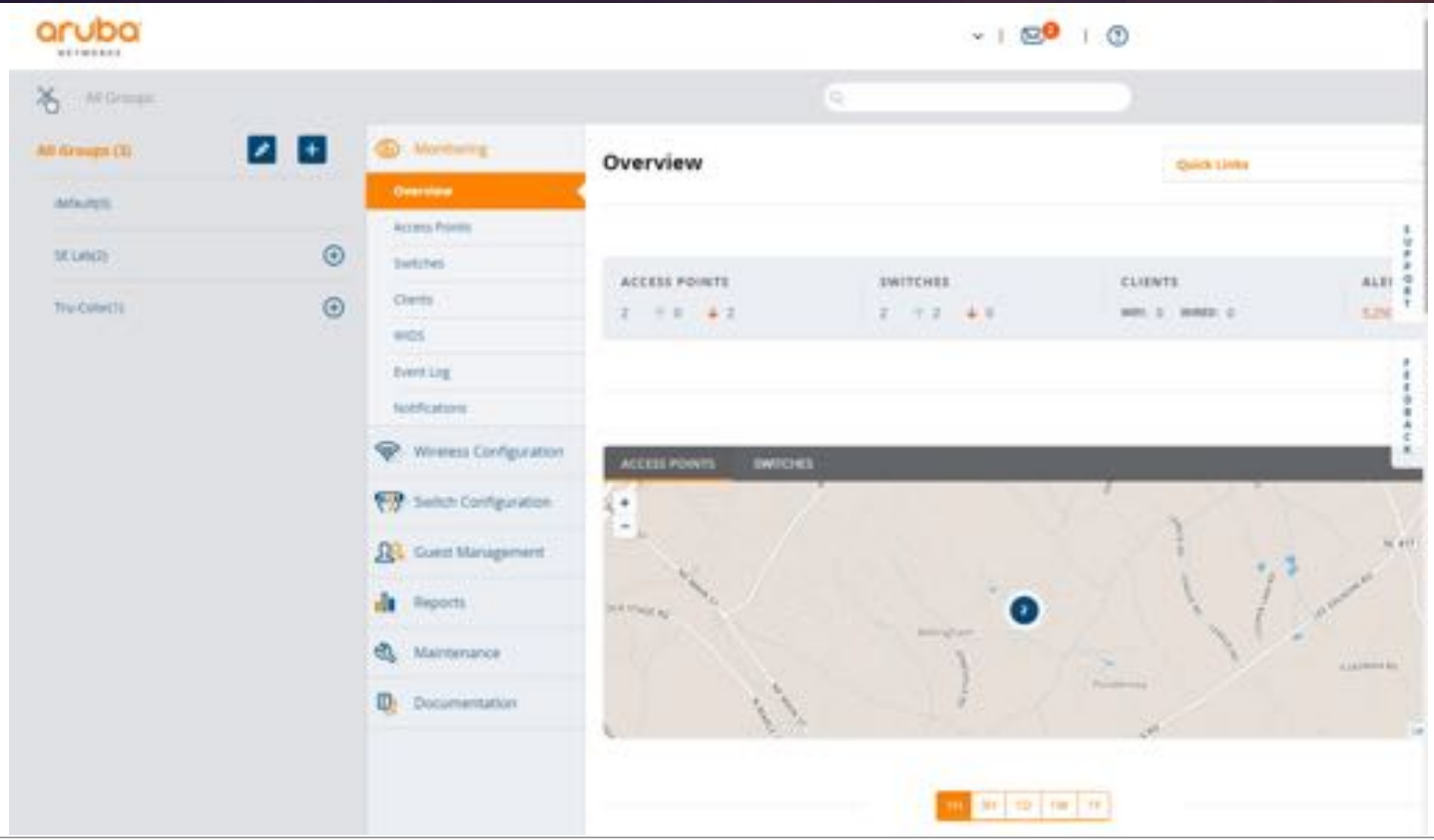
Aruba Central Overview

- **Cloud management for Instant and MAS**
- **ZTP with Aruba Activate**
- **Firmware management**
- **Reporting**
- **Responsive UI (adaptive to any display)***
- **AppRF management and visibility***
- **Cloud captive portal w/ social***

* Central 2.0 – Coming Soon

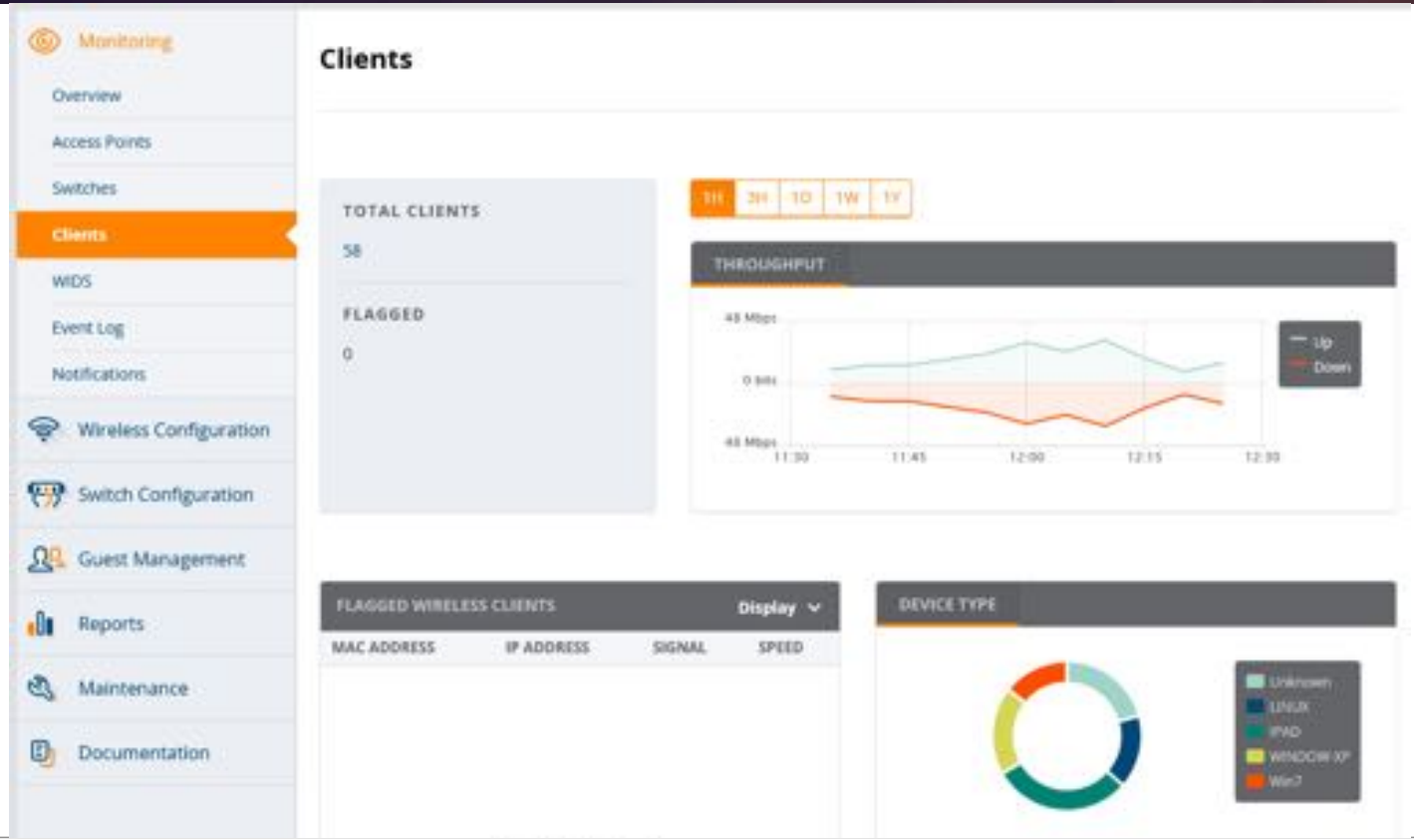
CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Aruba Central



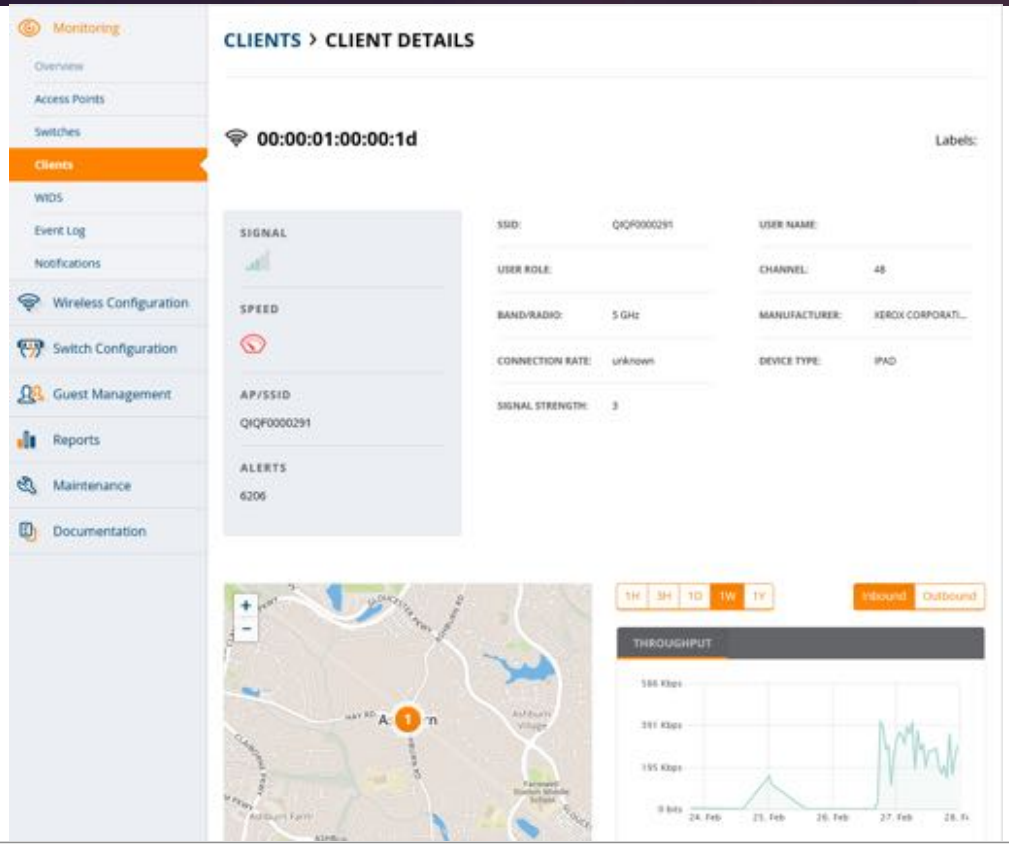
CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Aruba Central



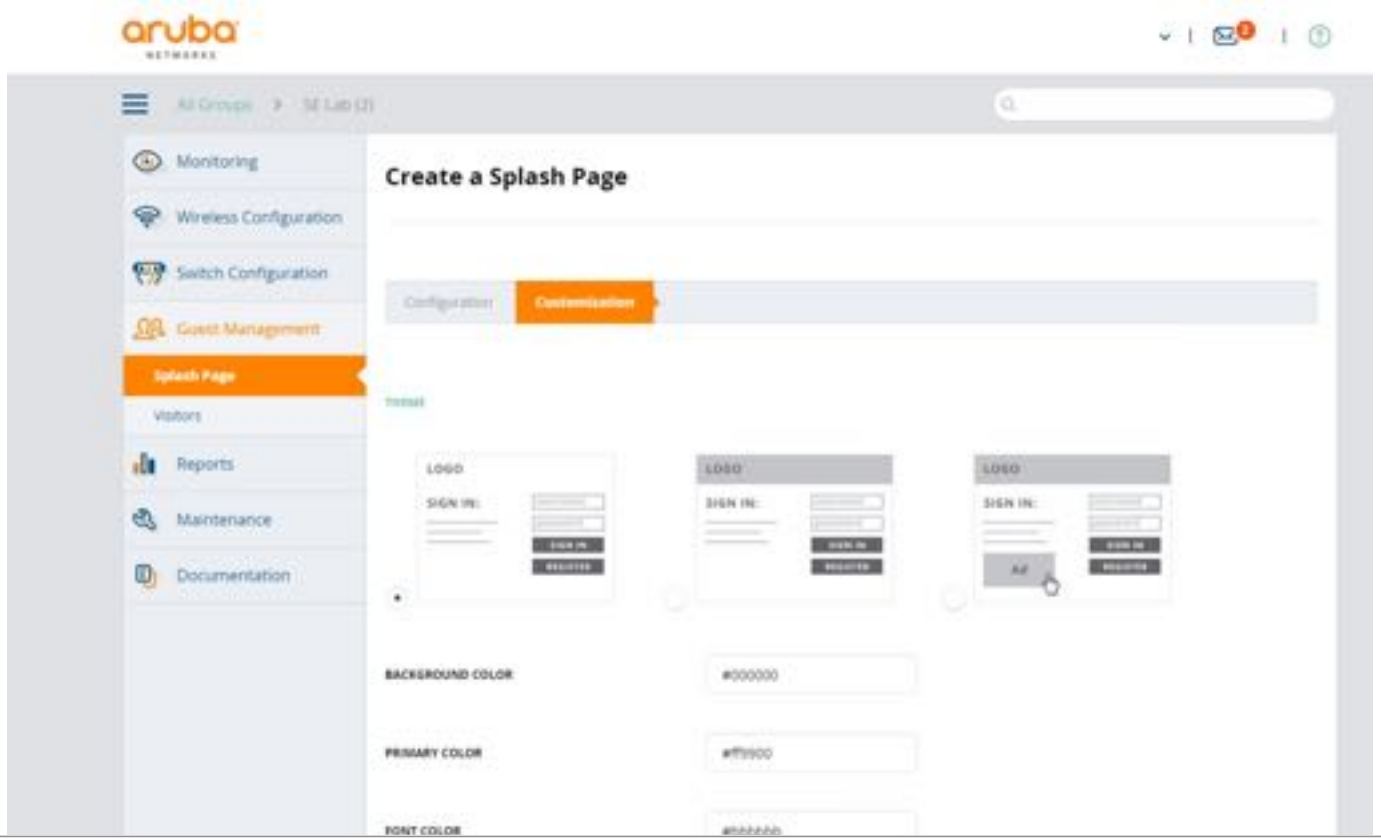
CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Aruba Central



CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Aruba Central



CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

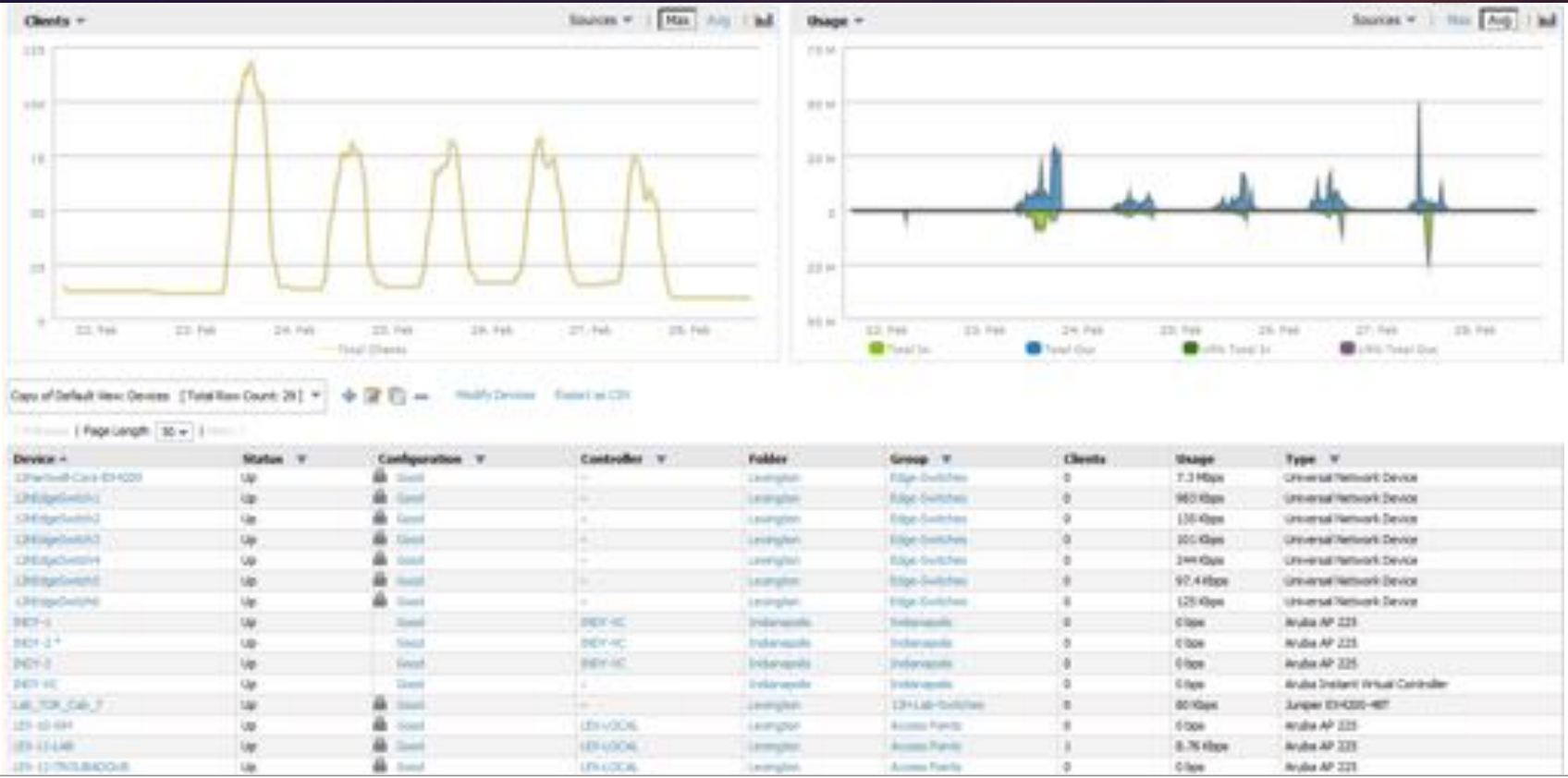
AirWave

AirWave Overview

- On-premise solution (VM or physical)
- Management, monitoring and reporting of Aruba controllers, Instant clusters, and MAS
- Multi-vendor
- In a hybrid controller-Instant environment, AirWave recommended
- Single pane of glass

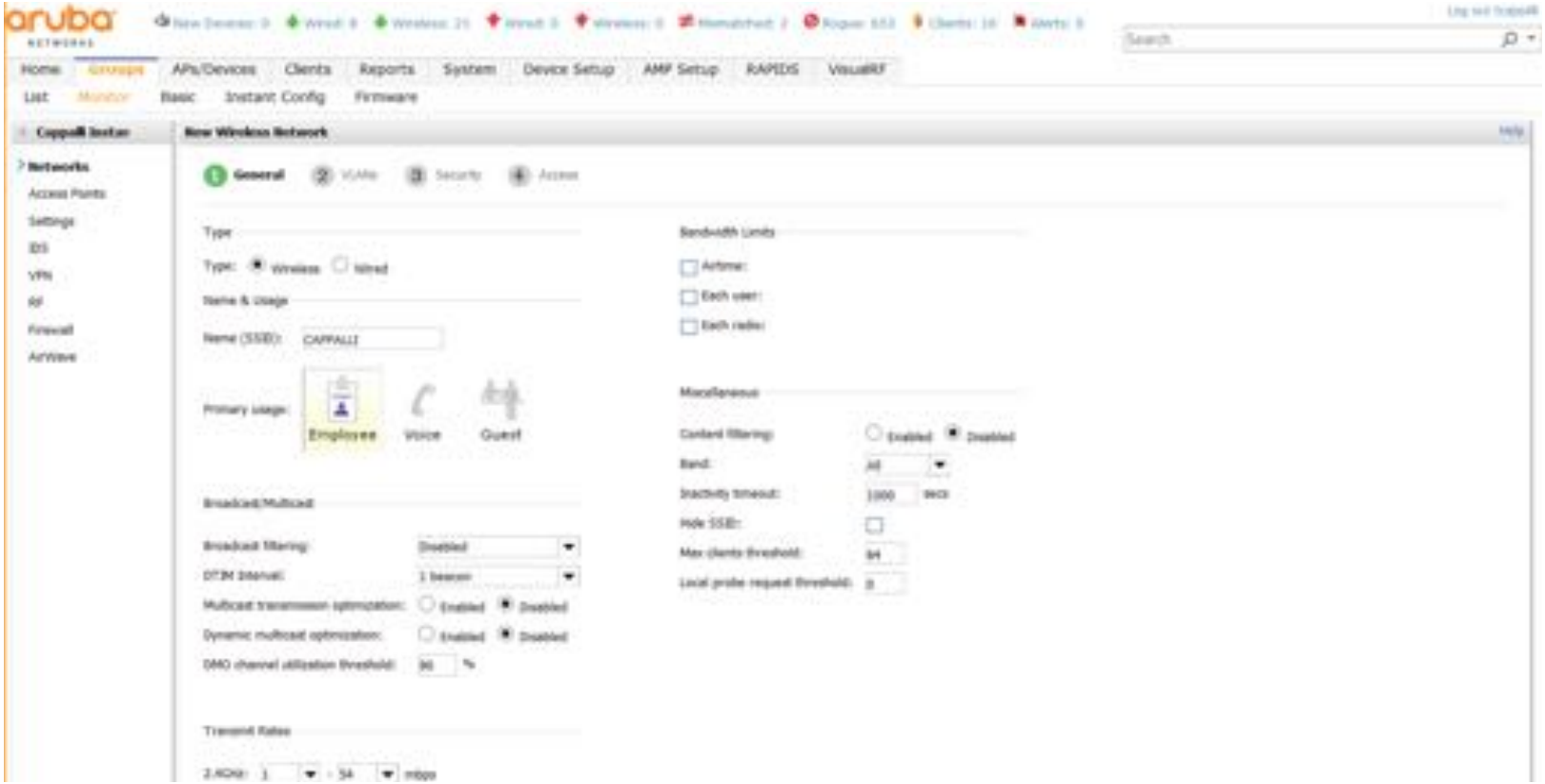
CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Single pane of glass



CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

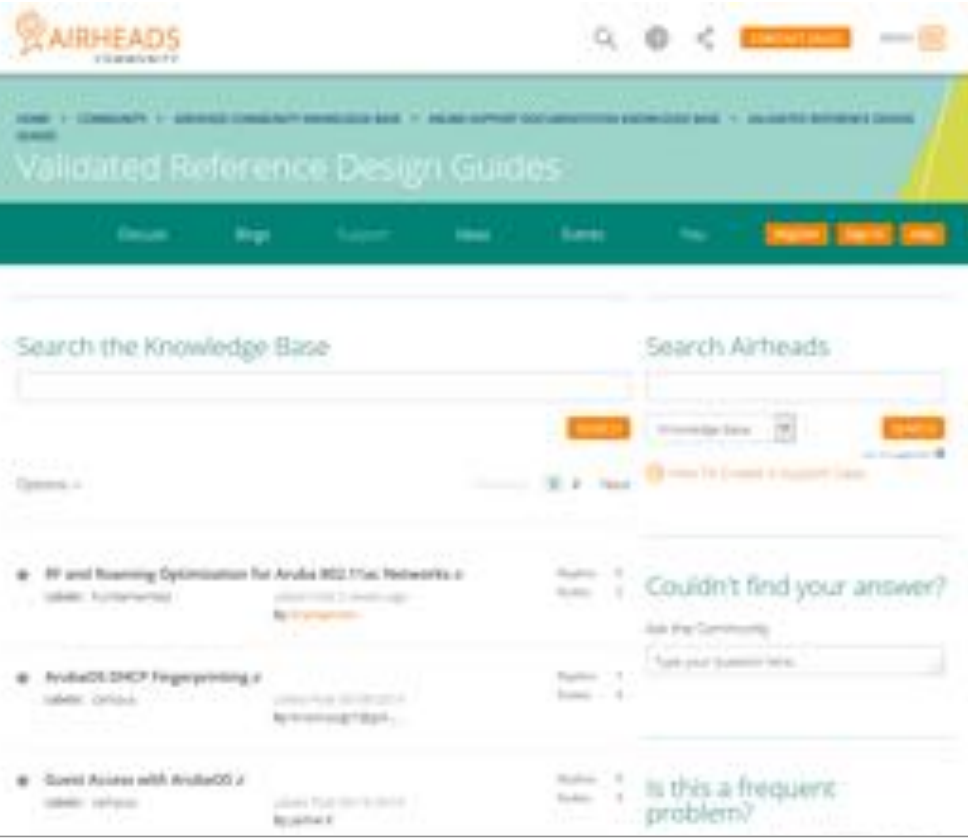
Instant GUI config



CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Discussion & Questions

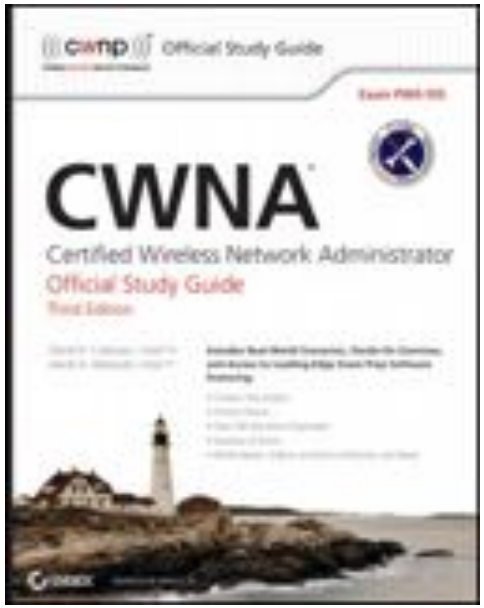
arubanetworks.com/vrd

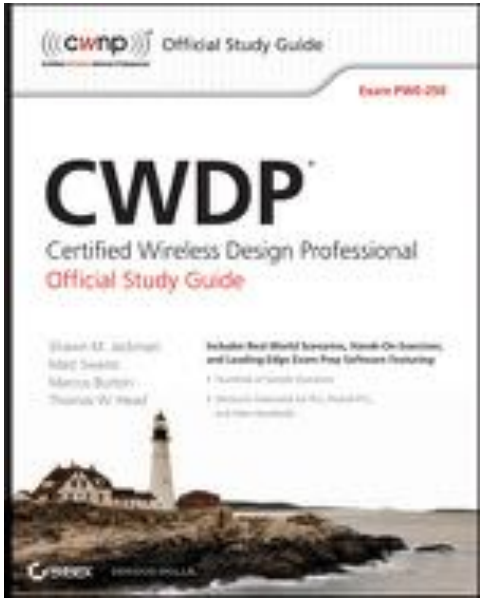


CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

Other resources

In-depth Wireless Architecture
cwnp.com





CONFIDENTIAL © Copyright 2015. Aruba Networks, Inc. All rights reserved

THANK YOU

atmosphere2015
HOW TOMORROW MOVES