Cisco Canada Plus

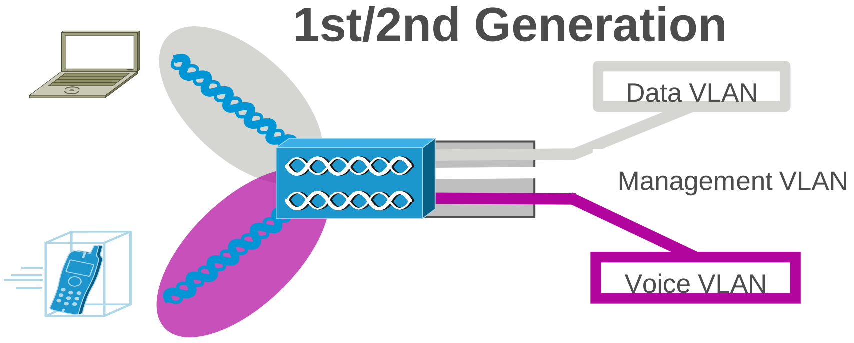
Design, Deployment and Management of Unified WLAN

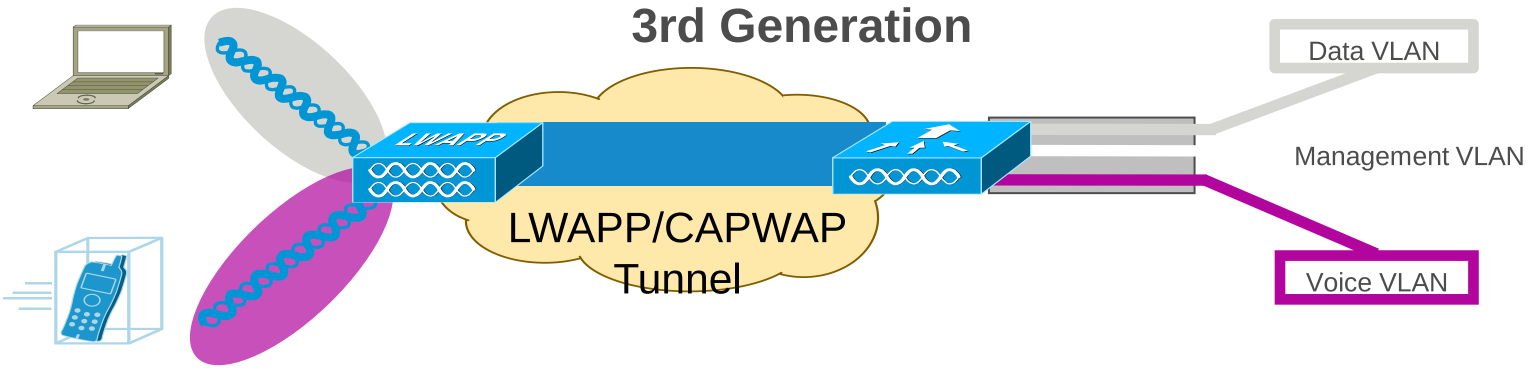
cisco

Understanding WLAN Controllers

1st/2nd Generation vs. 3rd Generation Approach

- 1st/2nd generation: APs act as 802.1Q translational bridge, putting client traffic on local VLANs
- 3rd generation: Controller bridges client traffic centrally

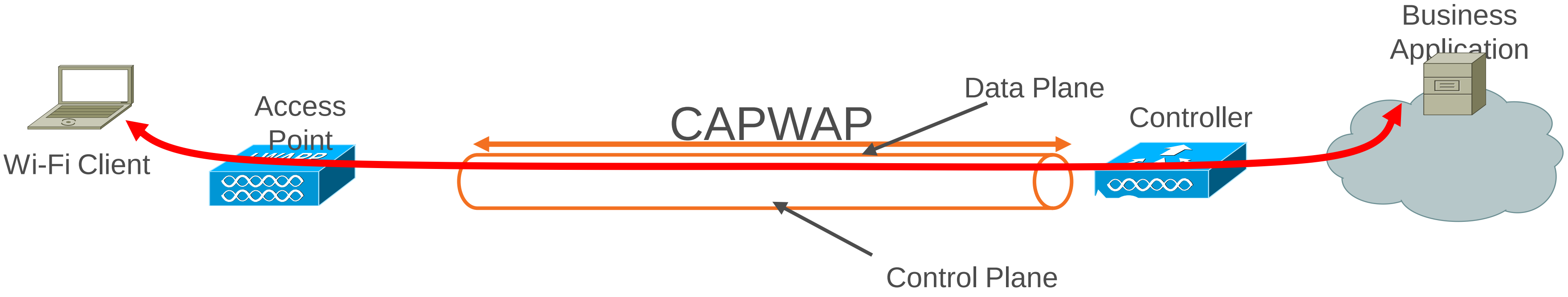




Centralized Wireless LAN Architecture

What Is CAPWAP?

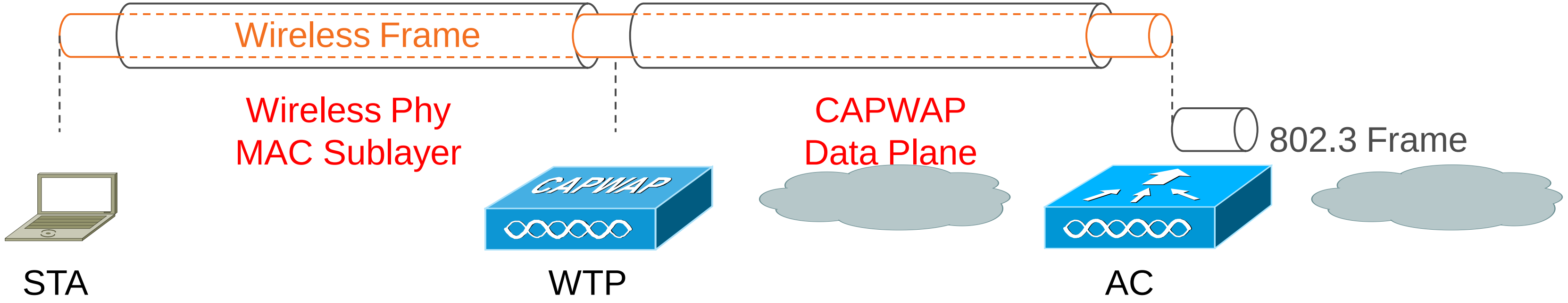
- CAPWAP: Control and Provisioning of Wireless Access Points
- Used between APs and WLAN controller and based on LWAPP
- CAPWAP carries control and data traffic between the two
  - Control plane is DTLS encrypted
  - Data plane is DTLS encrypted (optional)
- LWAPP-enabled access points can discover and join a CAPWAP controller, and conversion to a CAPWAP controller is seamless



CAPWAP Modes

- The CAPWAP protocol supports two modes of operation
  - Split MAC (centralized mode)
  - Local MAC (FlexConnect/H-REAP)

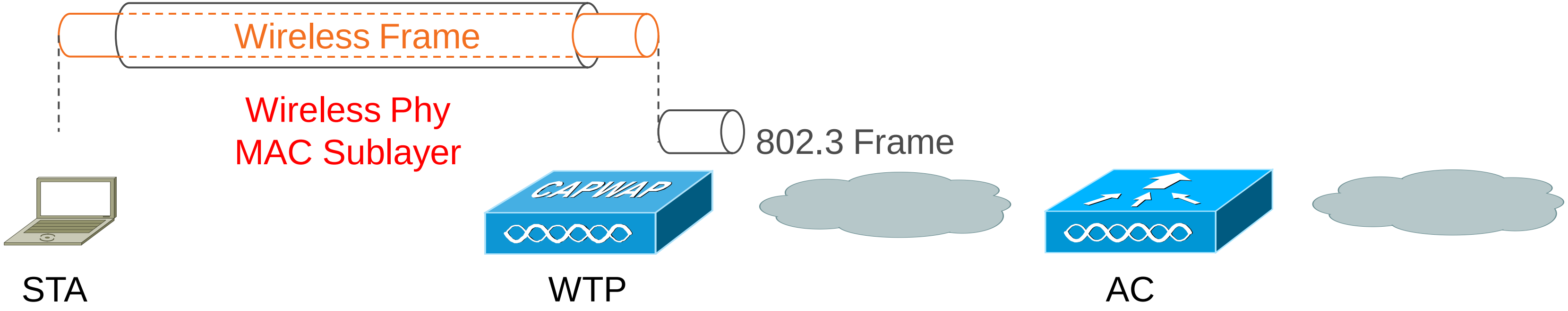
- Split MAC



CAPWAP Modes

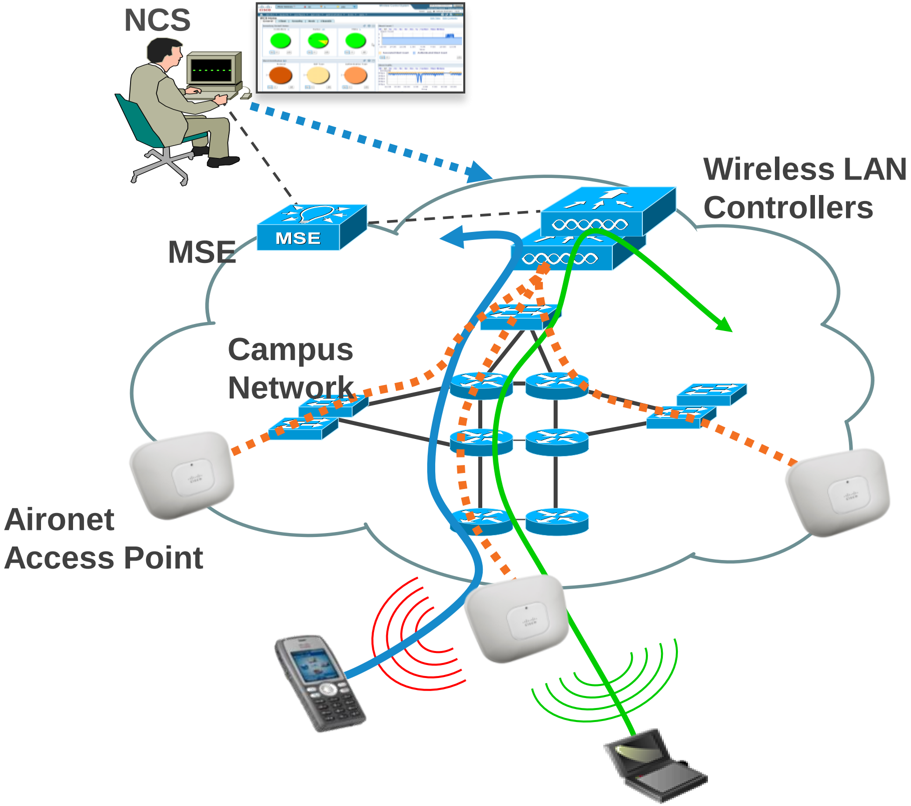
- The CAPWAP protocol supports two modes of operation
  - Split MAC (centralized mode)
  - Local MAC (FlexConnect/H-REAP)

- Locally bridged



Cisco Unified Wireless Principles

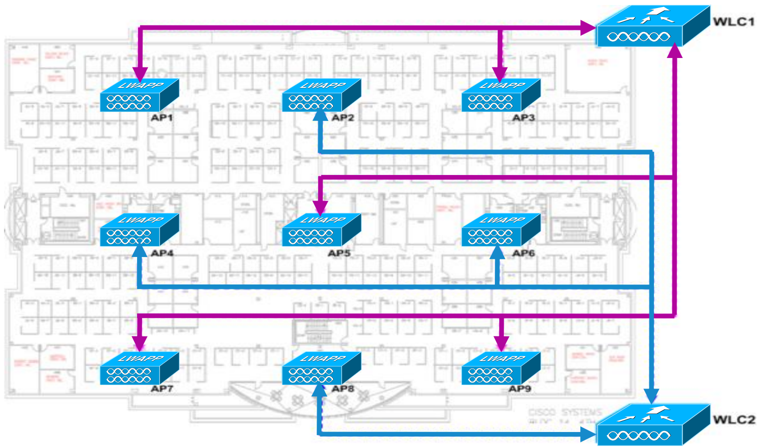
- Components
  - Wireless LAN controllers
  - Aironet access points
  - Management System (NCS)
  - Mobility Service Engine (MSE)
- Principles
  - AP must have CAPWAP connectivity with WLC
  - Configuration downloaded to AP by WLC
  - All Wi-Fi traffic is forwarded to the WLC



Controller Redundancy

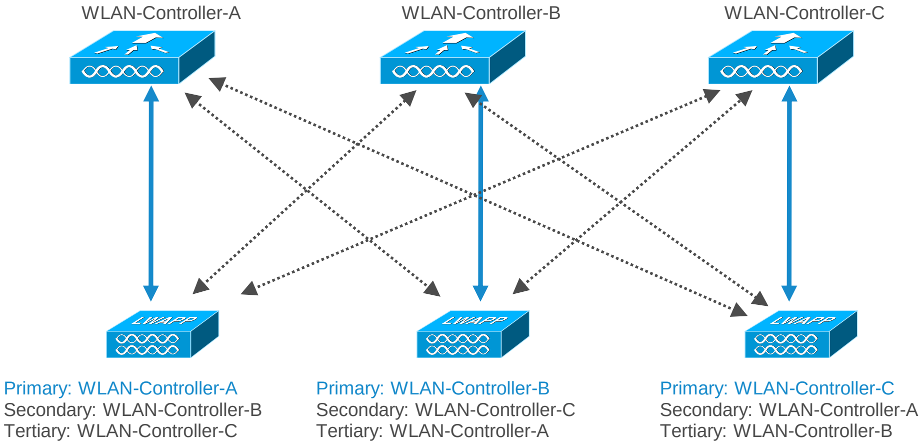
Dynamic

- Rely on CAPWAP to load-balance APs across controllers and populate APs with backup controllers
- Results in dynamic “salt-and-pepper” design
- Pros
  - Easy to deploy and configure—less upfront work
  - APs dynamically load-balance (though never perfectly)
- Cons
  - More intercontroller roaming
  - Bigger operational challenges due to unpredictability
  - No “fallback” option in the event of controller failure
- Cisco’s general recommendation is:
  Only for Layer 2 roaming
- Use deterministic redundancy instead of dynamic redundancy



Controller Redundancy

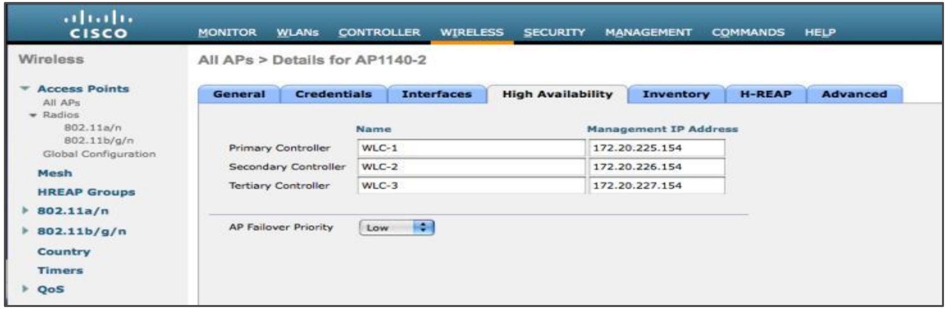
Deterministic



Primary: WLAN-Controller-A
Secondary: WLAN-Controller-B
Tertiary: WLAN-Controller-C

Primary: WLAN-Controller-B
Secondary: WLAN-Controller-C
Tertiary: WLAN-Controller-A

Primary: WLAN-Controller-C
Secondary: WLAN-Controller-A
Tertiary: WLAN-Controller-B



All APs > Details for AP1140-2

	Name	Management IP Address
Primary Controller	WLC-1	172.20.225.154
Secondary Controller	WLC-2	172.20.226.154
Tertiary Controller	WLC-3	172.20.227.154

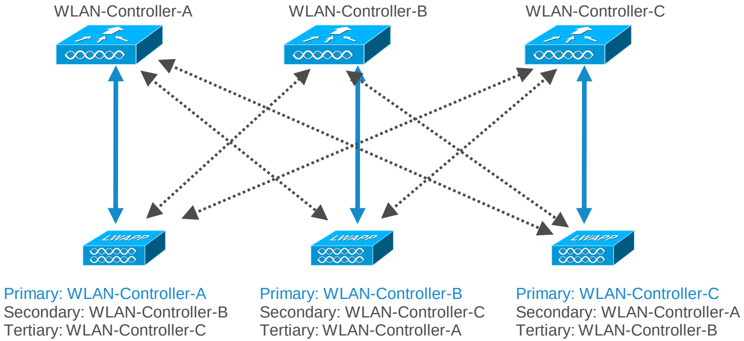
AP Failover Priority: Low

- Administrator statically assigns APs a primary, secondary, and/or tertiary controller
  - Assigned from controller interface (per AP) or WCS (template-based)
- Pros
  - Predictability—easier operational management
  - More flexible and powerful redundancy design options
  - “Fallback” option in the case of failover
- Con
  - More upfront planning and configuration
- This is Cisco’s recommended best practice

Controller Redundancy

Architecture Resiliency

Resiliency



WLAN-Controller-A

WLAN-Controller-B

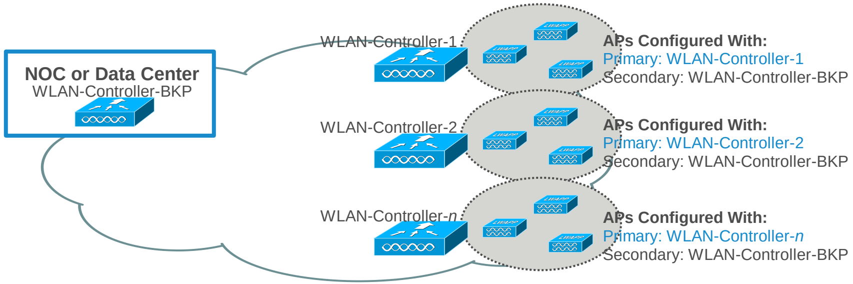
WLAN-Controller-C

Primary: WLAN-Controller-A
Secondary: WLAN-Controller-B
Tertiary: WLAN-Controller-C

Primary: WLAN-Controller-B
Secondary: WLAN-Controller-C
Tertiary: WLAN-Controller-A

Primary: WLAN-Controller-C
Secondary: WLAN-Controller-A
Tertiary: WLAN-Controller-B

N:1 Redundancy



NOC or Data Center
WLAN-Controller-BKP

WLAN-Controller-1

APs Configured With:
Primary: WLAN-Controller-1
Secondary: WLAN-Controller-BKP

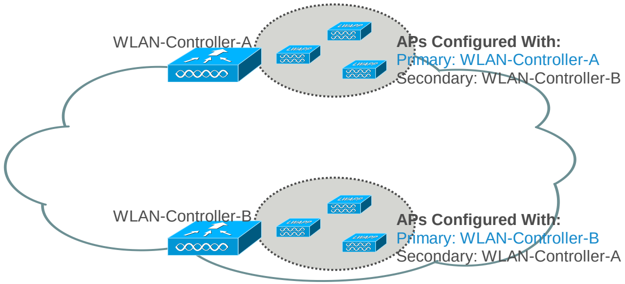
WLAN-Controller-2

APs Configured With:
Primary: WLAN-Controller-2
Secondary: WLAN-Controller-BKP

WLAN-Controller-*n*

APs Configured With:
Primary: WLAN-Controller-*n*
Secondary: WLAN-Controller-BKP

N:N Redundancy



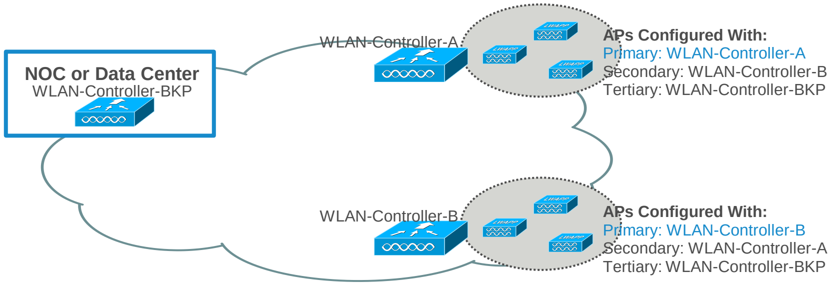
WLAN-Controller-A

APs Configured With:
Primary: WLAN-Controller-A
Secondary: WLAN-Controller-B

WLAN-Controller-B

APs Configured With:
Primary: WLAN-Controller-B
Secondary: WLAN-Controller-A

N:N:1 Redundancy



NOC or Data Center
WLAN-Controller-BKP

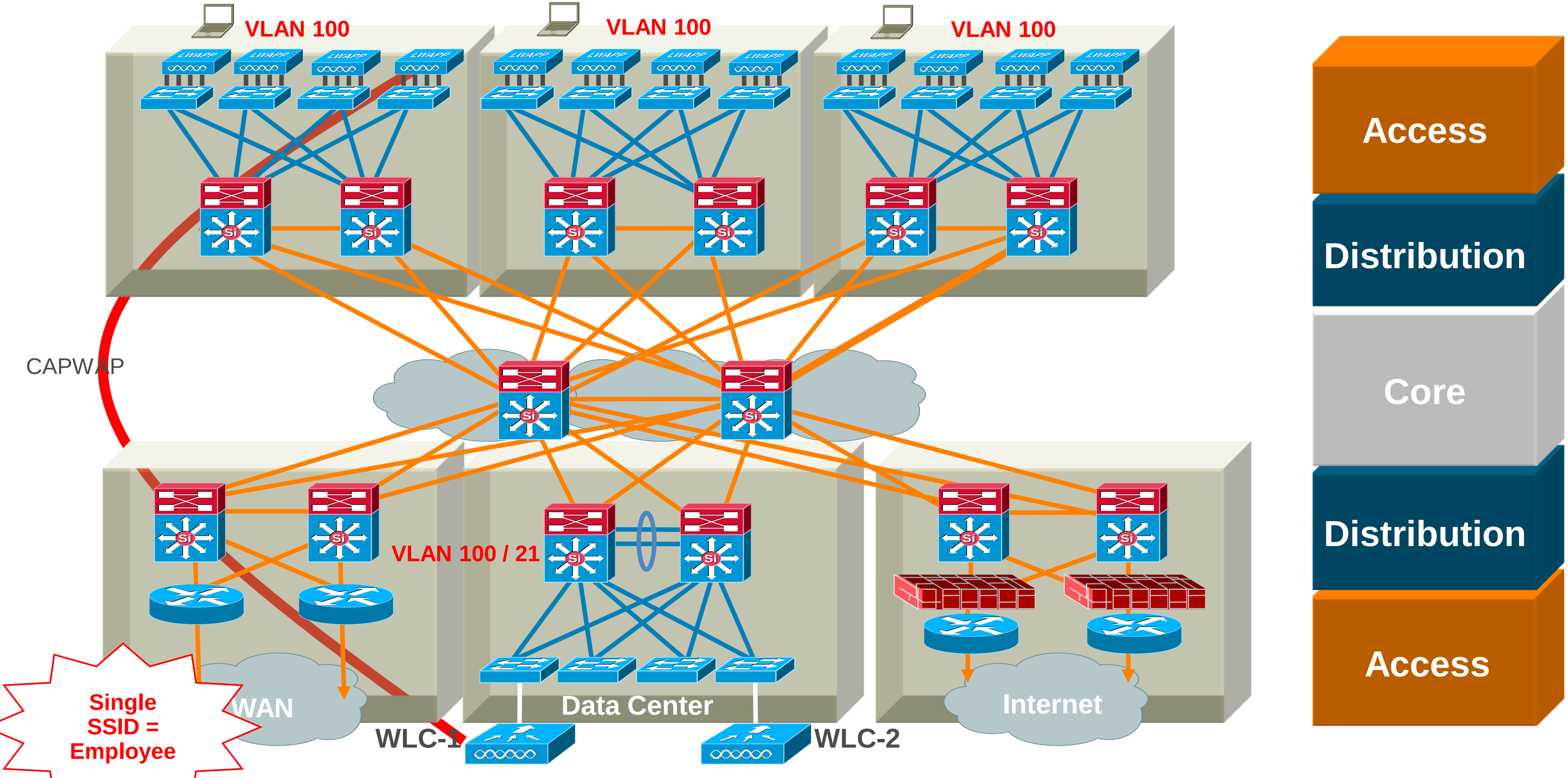
WLAN-Controller-A

APs Configured With:
Primary: WLAN-Controller-A
Secondary: WLAN-Controller-B
Tertiary: WLAN-Controller-BKP

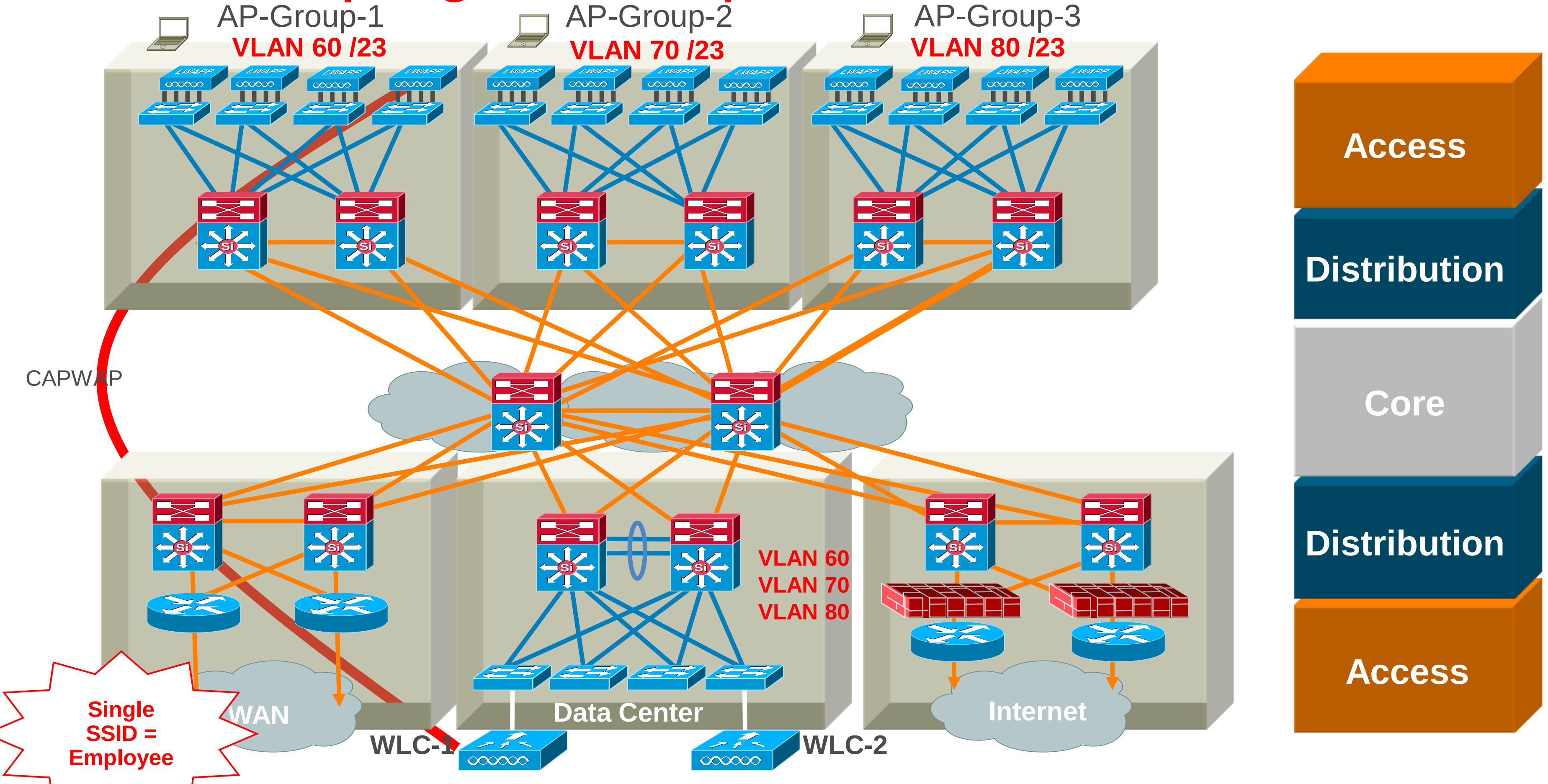
WLAN-Controller-B

APs Configured With:
Primary: WLAN-Controller-B
Secondary: WLAN-Controller-A
Tertiary: WLAN-Controller-BKP

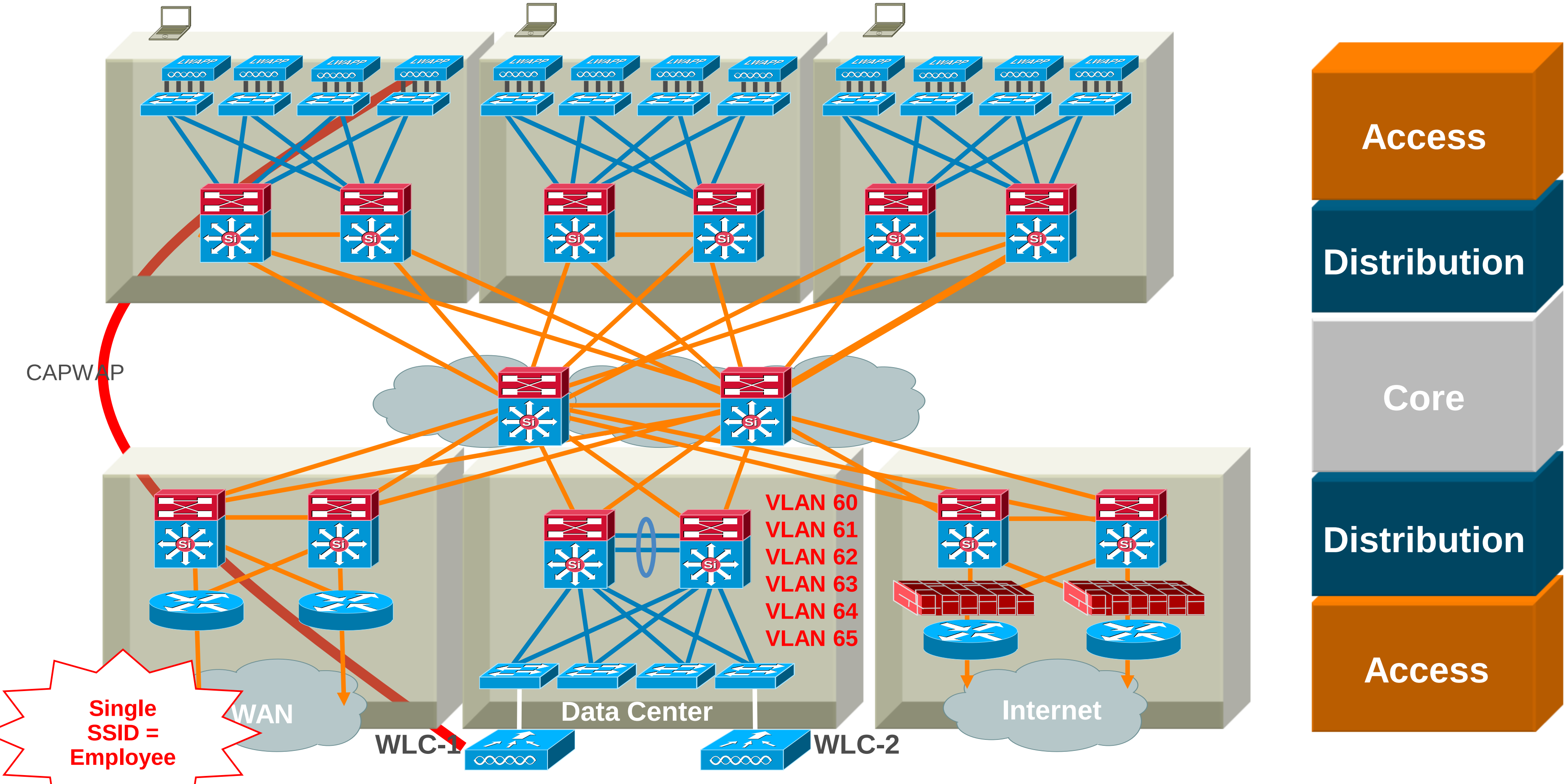
AP-Grouping in Campus



AP-Grouping in Campus

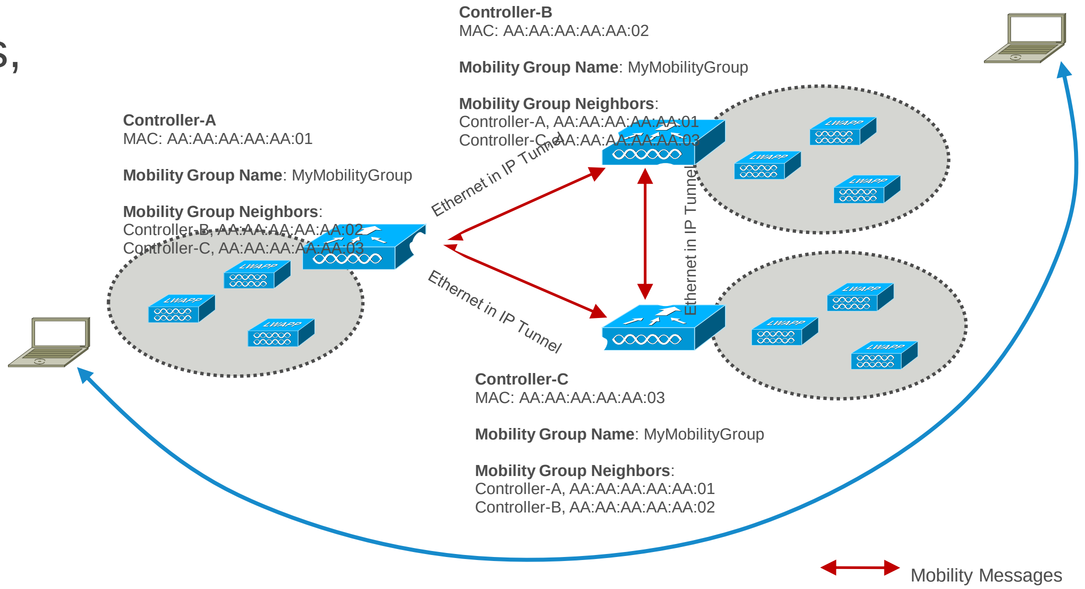


Interface-Grouping in Campus



Scaling the Architecture with Mobility Groups

- Mobility Group allows controllers to peer with each other to support seamless roaming across controller boundaries
- APs learn the IPs of the other members of the mobility group after the LWAPP Join process
- Support for up to 24 controllers, 24,000 APs per mobility group
- Mobility messages exchanged between controllers (Multicast)
- Data tunneled between controllers in EtherIP (RFC 3378)



Controller-B
MAC: AA:AA:AA:AA:AA:02

Mobility Group Name: MyMobilityGroup

Mobility Group Neighbors:
Controller-A, AA:AA:AA:AA:AA:01
Controller-C, AA:AA:AA:AA:AA:03

Controller-A
MAC: AA:AA:AA:AA:AA:01

Mobility Group Name: MyMobilityGroup

Mobility Group Neighbors:
Controller-B, AA:AA:AA:AA:AA:02
Controller-C, AA:AA:AA:AA:AA:03

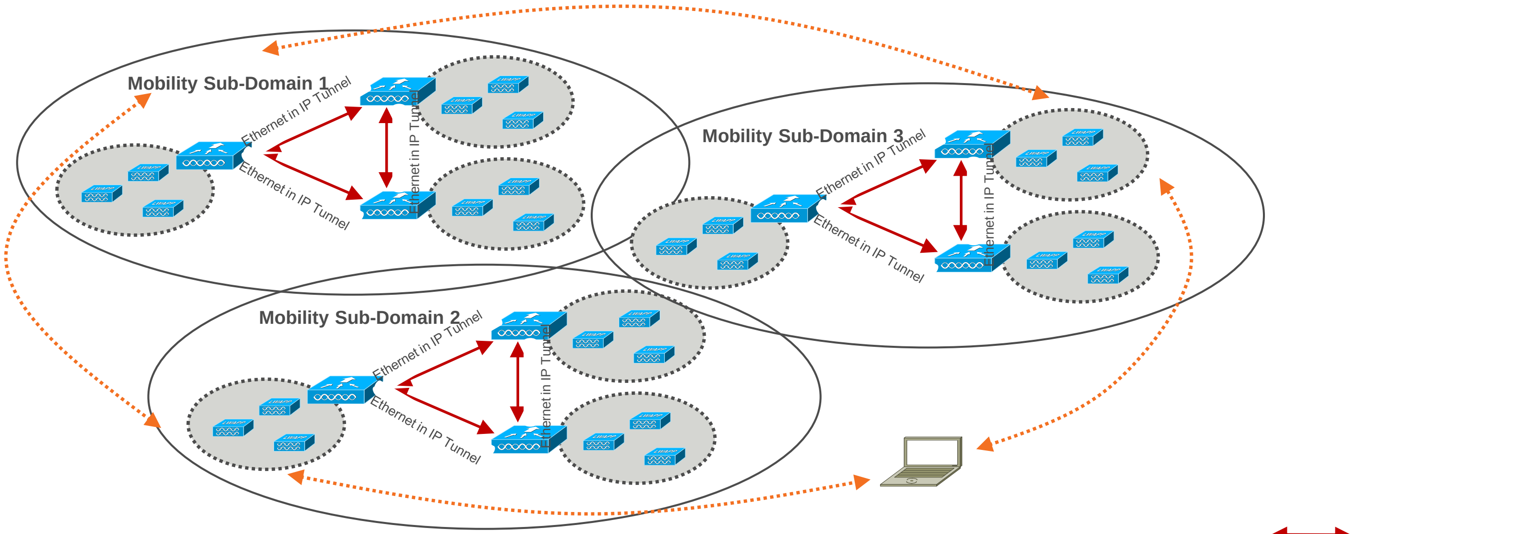
Controller-C
MAC: AA:AA:AA:AA:AA:03

Mobility Group Name: MyMobilityGroup

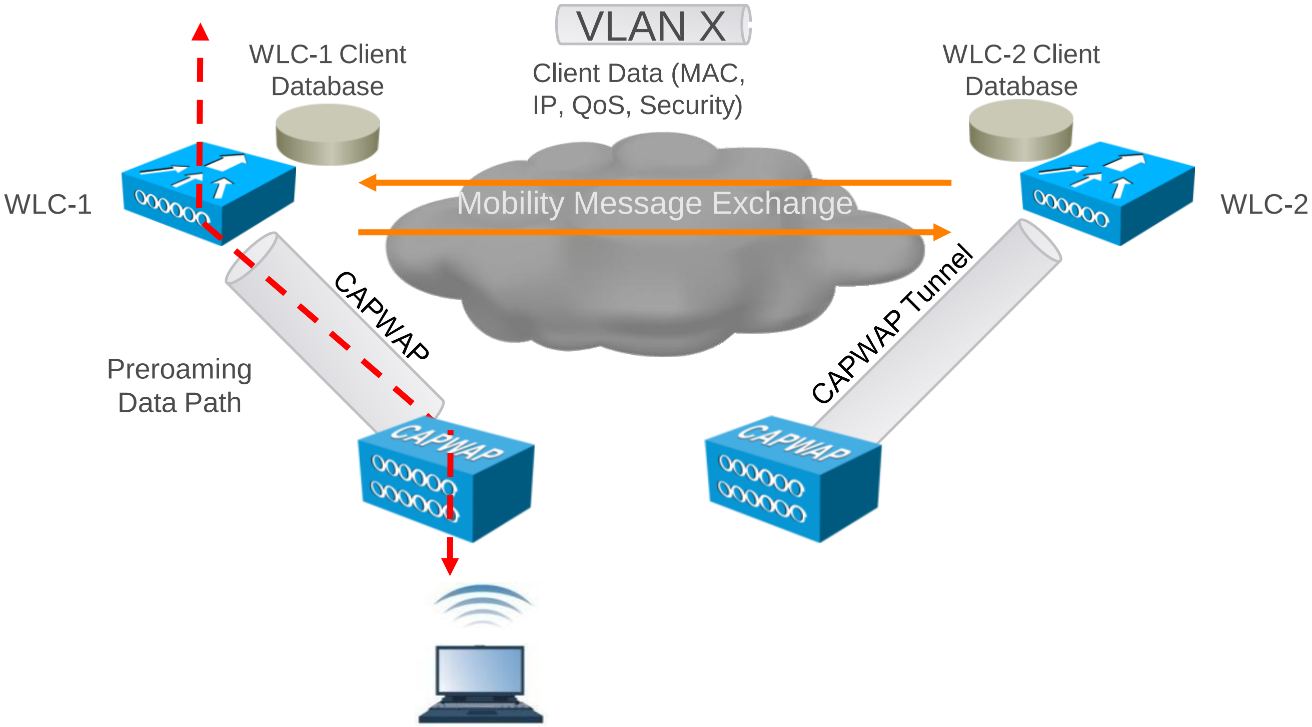
Mobility Group Neighbors:
Controller-A, AA:AA:AA:AA:AA:01
Controller-B, AA:AA:AA:AA:AA:02

Increased Mobility Scalability

- Roaming is supported across three mobility groups (3 * 24 = 72 controllers)
- With Inter Release Controller Mobility (IRCM) roaming is supported between 4.2.207 and 6.0.188 and 7.0



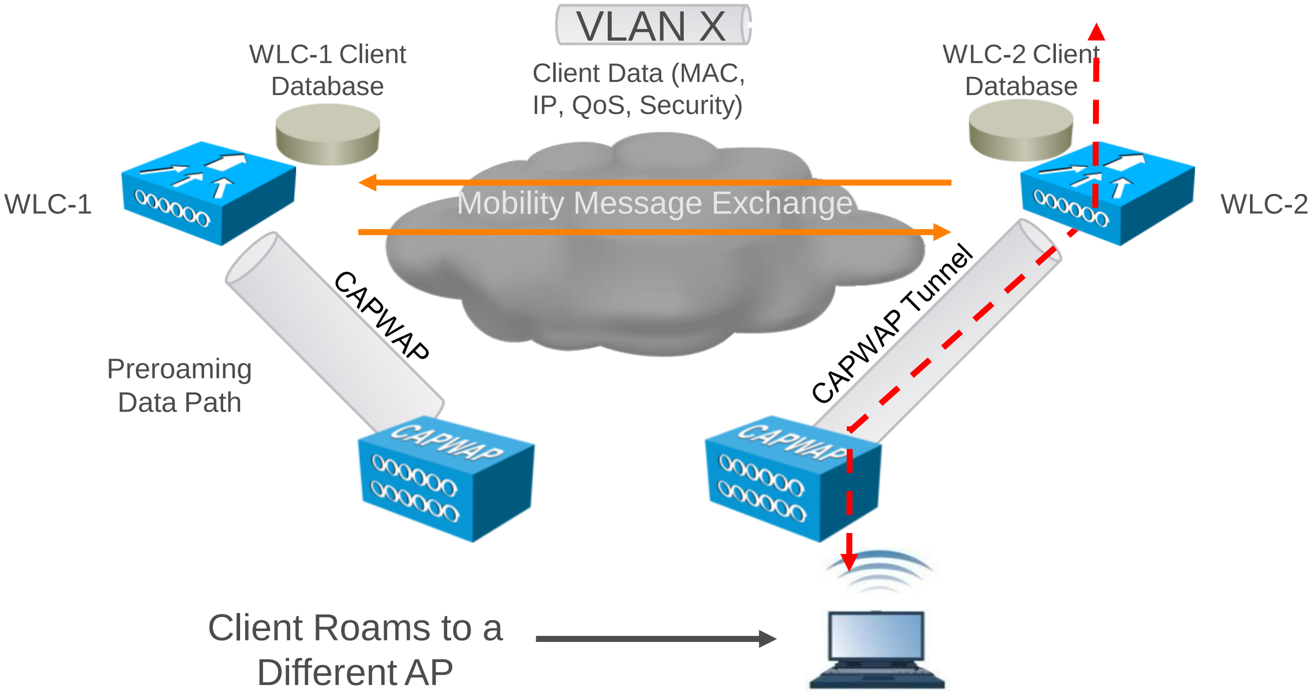
Inter-Controller Roaming:
Layer 2



- Inter-Controller roam happens when a client moves association between APs joined to different controller
- Client must be re-authenticated and new security session established

Inter-Controller Roaming:

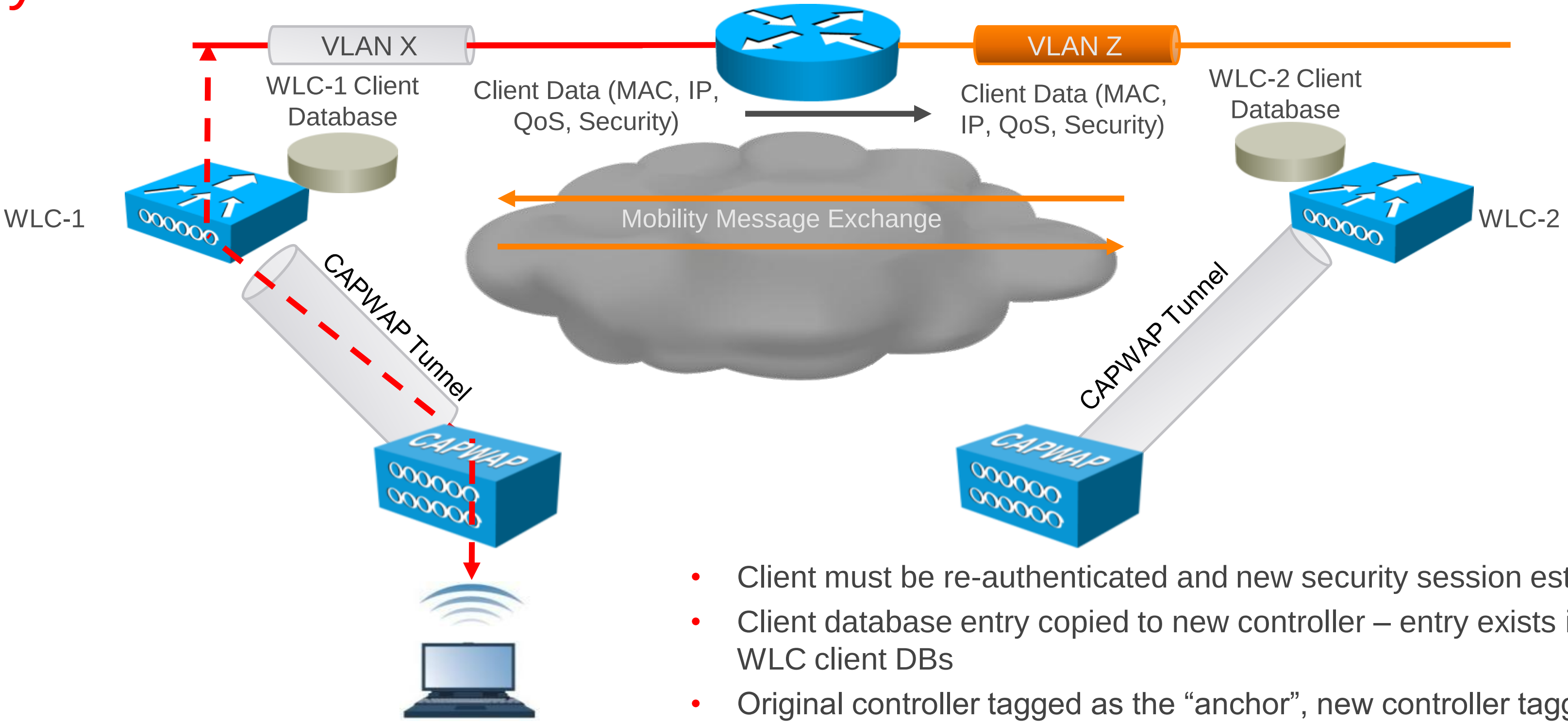
Layer 2



- Client database entry with new AP and appropriate security context
- No IP address refresh needed

Inter-Controller Roaming:

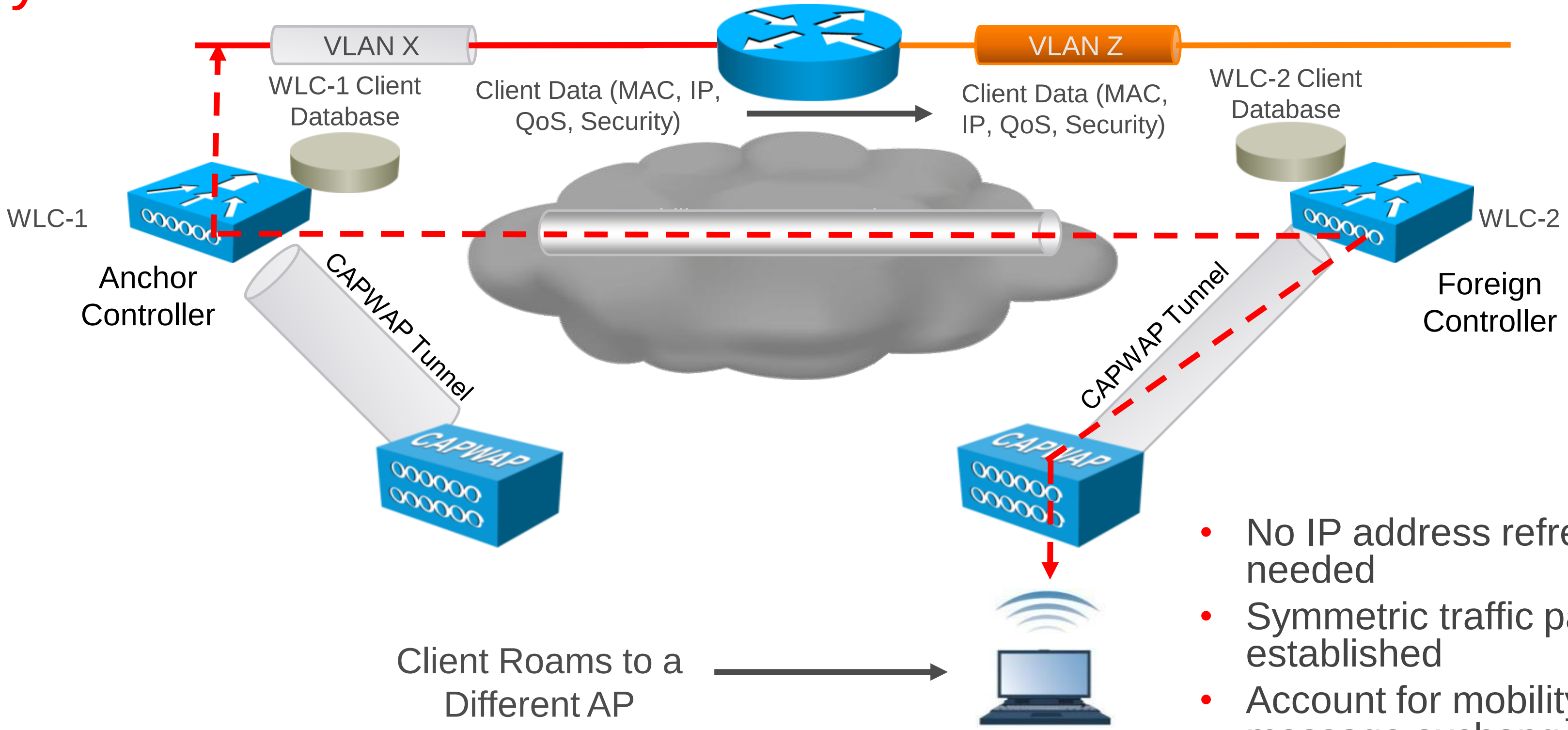
Layer 3



- Client must be re-authenticated and new security session established
- Client database entry copied to new controller – entry exists in both WLC client DBs
- Original controller tagged as the “anchor”, new controller tagged as the “foreign”
- WLCs must be in same mobility group or domain

Inter-Controller Roaming:

Layer 3



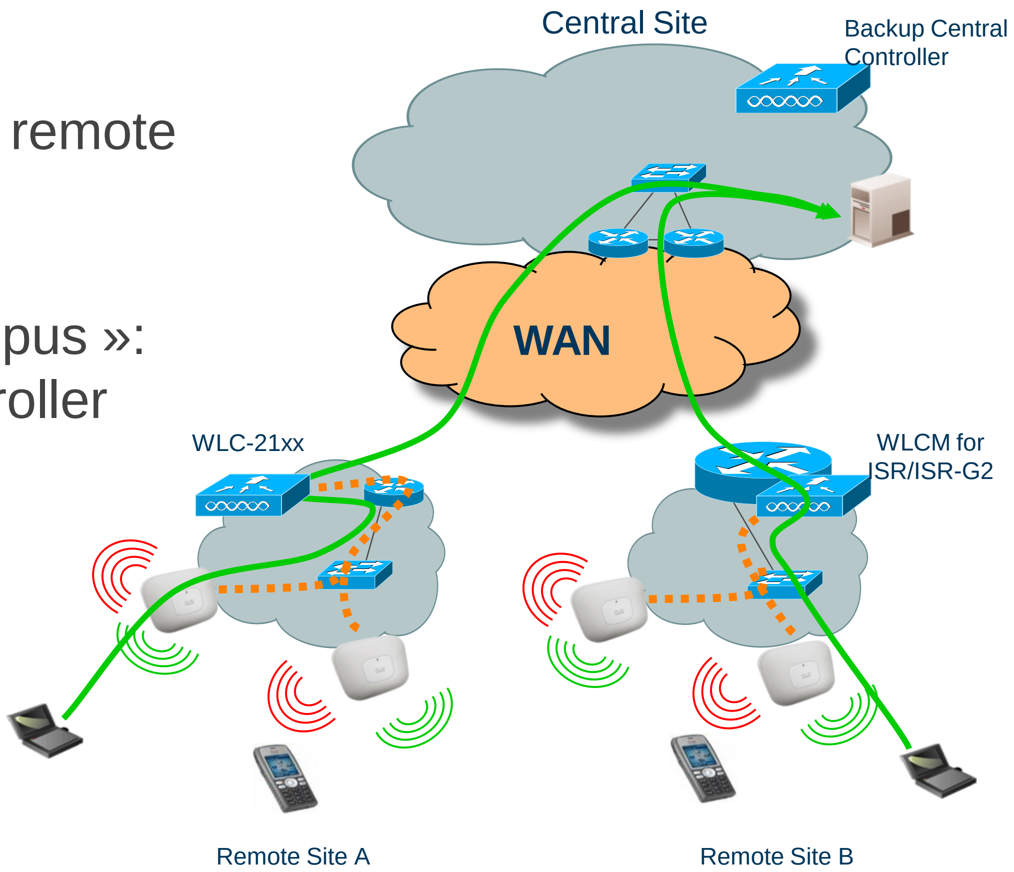
- No IP address refresh needed
- Symmetric traffic path established
- Account for mobility message exchange in network design

Designing a Mobility Group/Domain Design Considerations

- Less roaming is better – clients and apps are happier
- L3 roaming & fast roaming clients consume client DB slots on multiple controllers – consider “worst case” scenarios in designing roaming domain size
- Leverage natural roaming domain boundaries
- Mobility Message transport selection: multicast vs. unicast
- Make sure the right ports and protocols are allowed

Branch Designs Using Remote Controllers

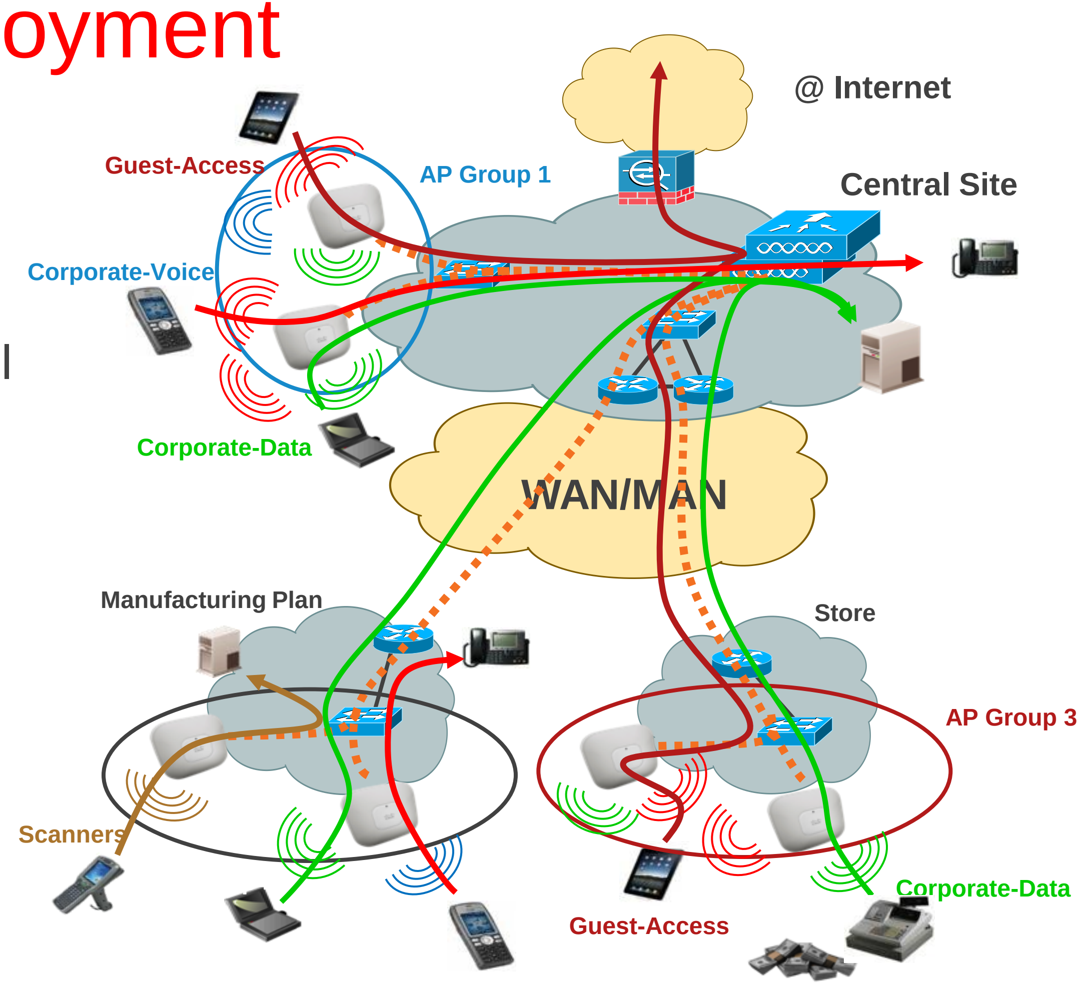
- Branches can also have local remote controllers
- Small form factors WLC are available to have « small campus »: WLC-2504 or Integrated controller modules in ISR/ISR-G2
- High Availability design with central backup controller is supported. WAN limitations may apply.



Branch Office Deployment FlexConnect

- Hybrid Remote Edge Access Point architecture (H-REAP)
- Single management and control point
- Data Traffic Switching
  - Centralized traffic

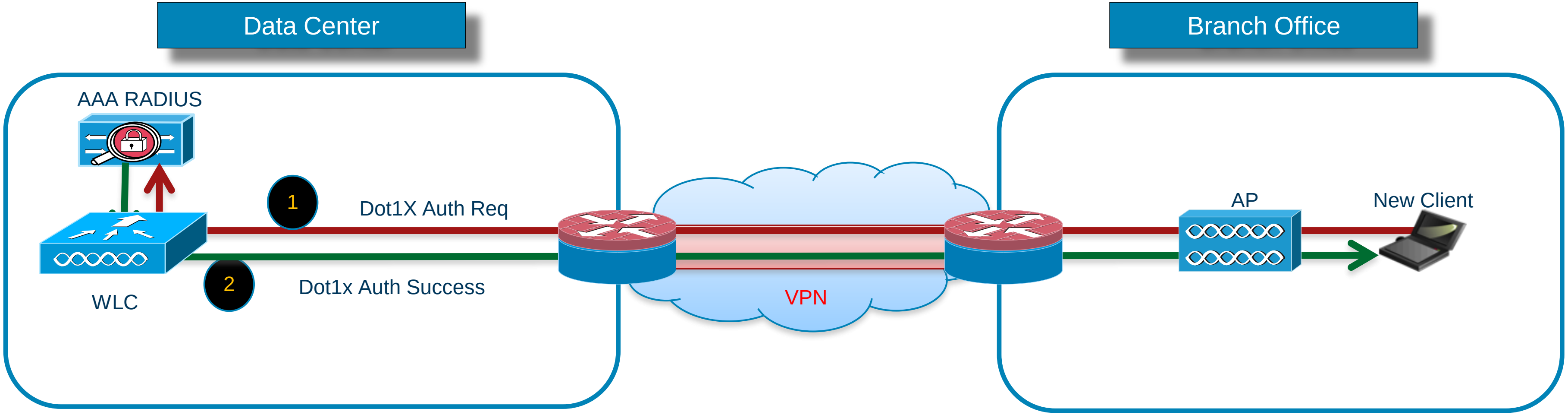
    or
  - Local traffic
- Traffic Switching is configured per AP and per WLAN (SSID)



FlexConnect – Advanced Services

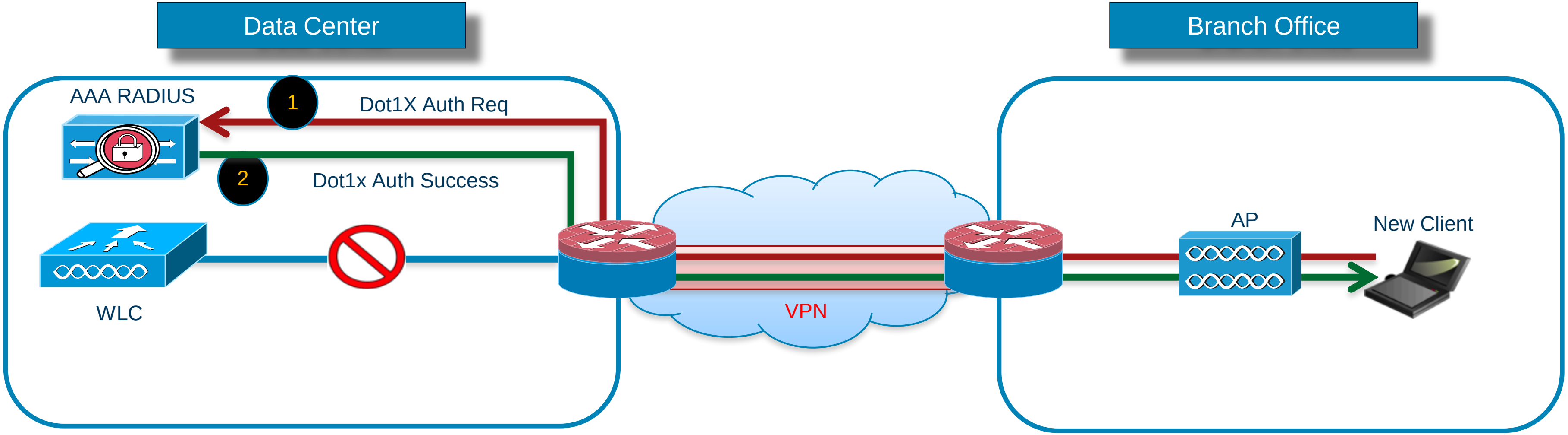
- High Availability – WAN Survivability
  - FlexConnect AP provides wireless access and services to clients when the connection to the primary WLC fails
- Local Authentication
  - Allows for the authentication capability to exist directly at the AP in FlexConnect instead of the WLC
- Fast roaming in remote branches
- Dynamic VLAN assignment
- Scalability
  - Number of FlexConnect groups: 500 (7500s) and 100 (5500s)
  - APs per Group: 50 (7500s) and 25 (5500s)

FlexConnect – WLC Authenticator



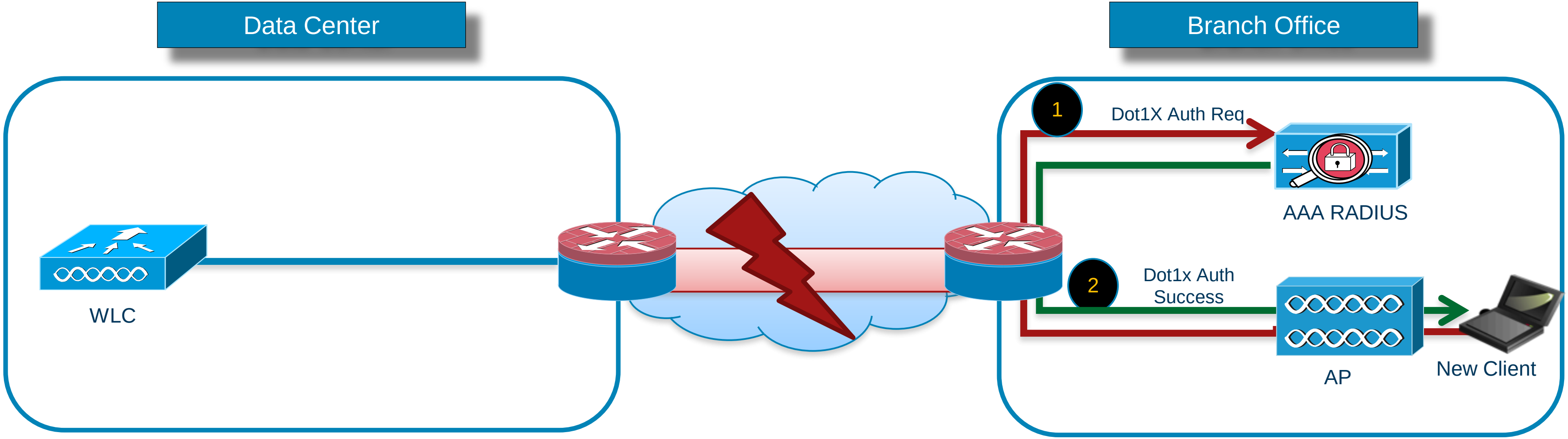
- All the client authentication requests travels through Central Controller
- If Controller is not reachable, then no clients can authenticate

FlexConnect – AP Authenticator



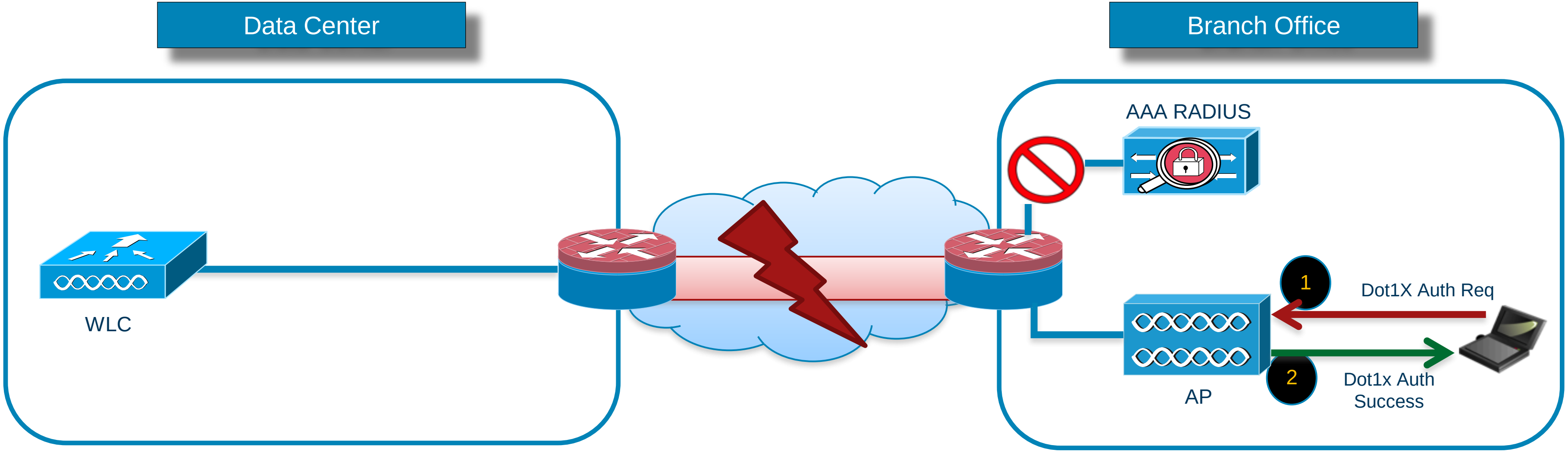
- All the client authentication requests travels straight from AP to RADIUS Server.
- If Controller is not reachable, clients can still continue to authenticate and access network services.

FlexConnect – AP Authenticator



- All the client authentication requests travels straight from AP to Local Branch RADIUS Server.
- If WAN link is down, clients can still continue to authenticate and access network services.

Local Authentication – AP as EAP Server

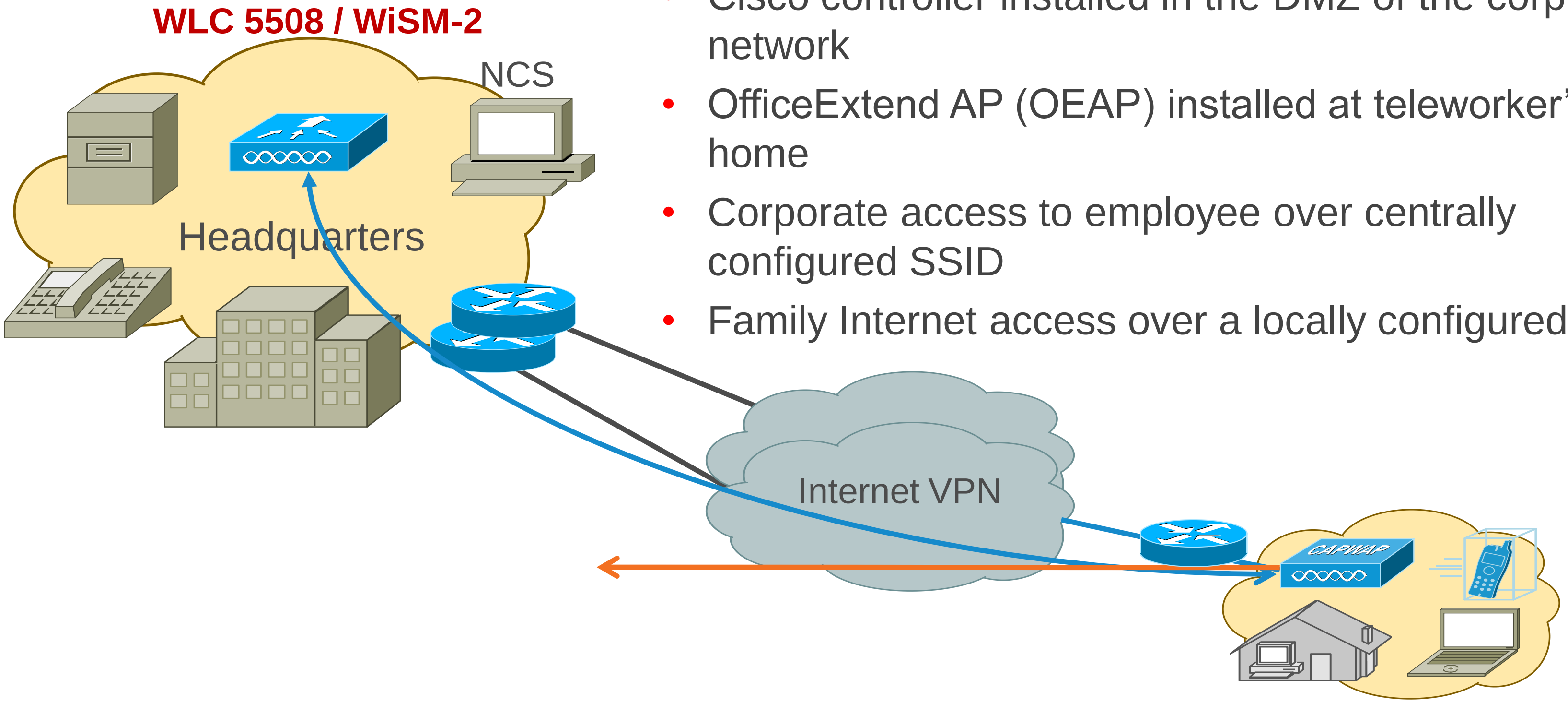


- All the client authenticated directly by the AP.
- If WAN link & Local Backup RADIUS Server is down clients can still continue to authenticate and access network services.

H-REAP Design Considerations

- Some WAN limitations apply
  - RTT must be below 300 ms data (100 ms voice)
  - Minimum 500 bytes WAN MTU (with maximum four fragmented packets)
- Some features are not available in standalone mode or in local switching mode
  - See full list in « H-REAP Feature Matrix »

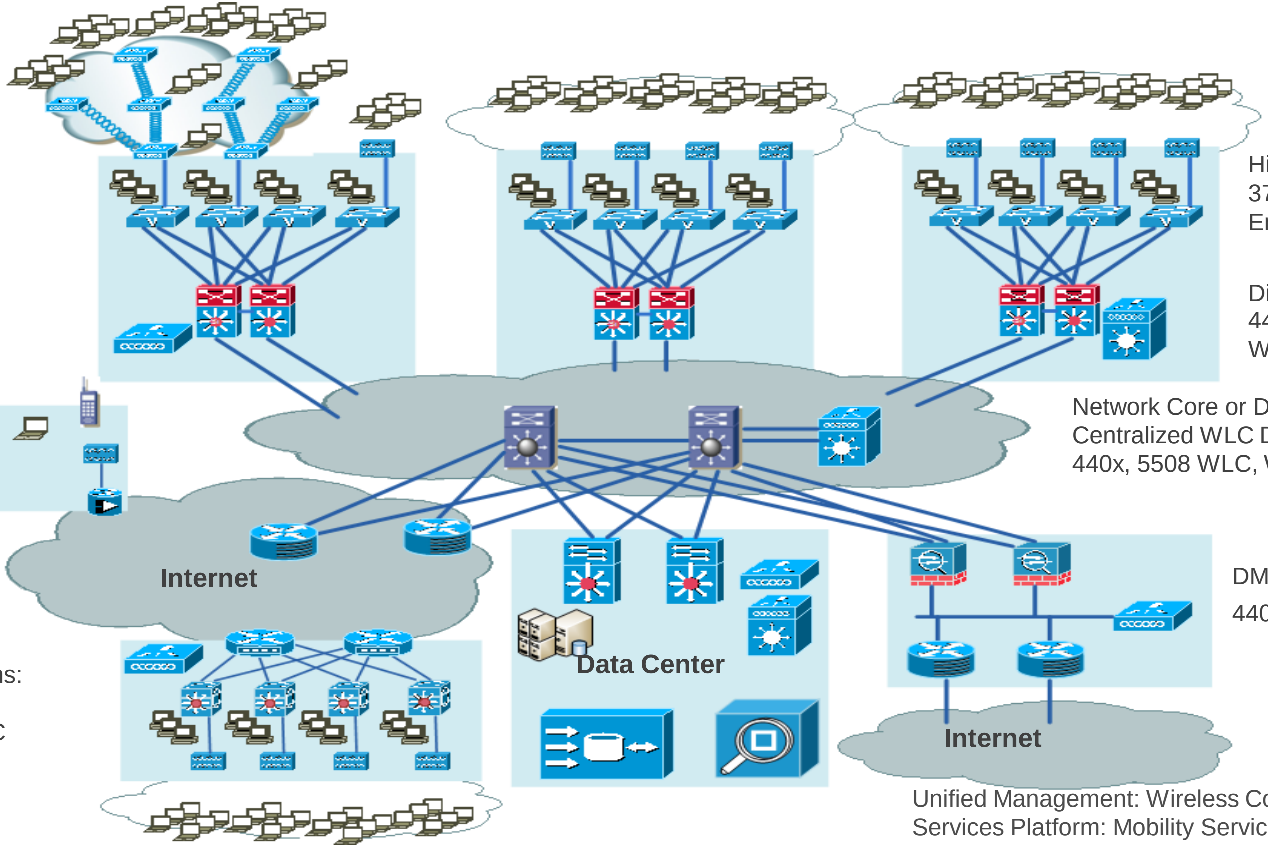
Home Office Design – OEAP



- Cisco controller installed in the DMZ of the corporate network
- OfficeExtend AP (OEAP) installed at teleworker’s home
- Corporate access to employee over centrally configured SSID
- Family Internet access over a locally configured SSID

Cisco Unified Wireless Network

Flexible, Resilient, Scalable Architecture



Unified
Outdoor/Indoor
Access

Access
Network

Distribution
Network

Teleworker/S
OHO

OfficeExtend AP

Branch Office

Unified WLC Options:
5508, 440x, 210x
3750G Unified WLC
WLCM Module
Hybrid REAP
Standalone AP

Highly Distributed Design
3750G Unified WLC
Enterprise Hybrid REAP

Distributed WLC Design
440x, 5508 WLC,
WiSM Unified WLC

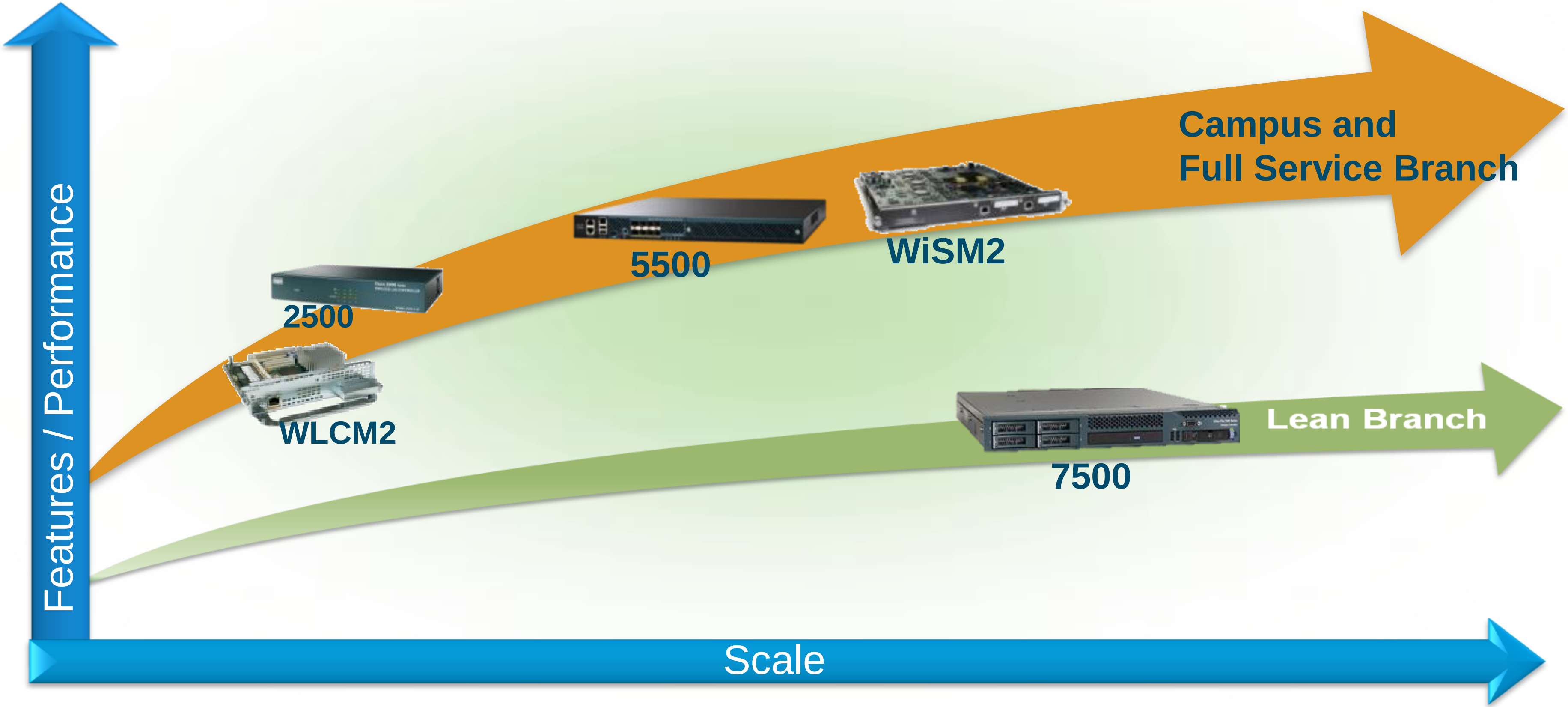
Network Core or Data Center
Centralized WLC Design
440x, 5508 WLC, WiSM Unified WLC

DMZ Guest Controller

440x, 5508 WLC

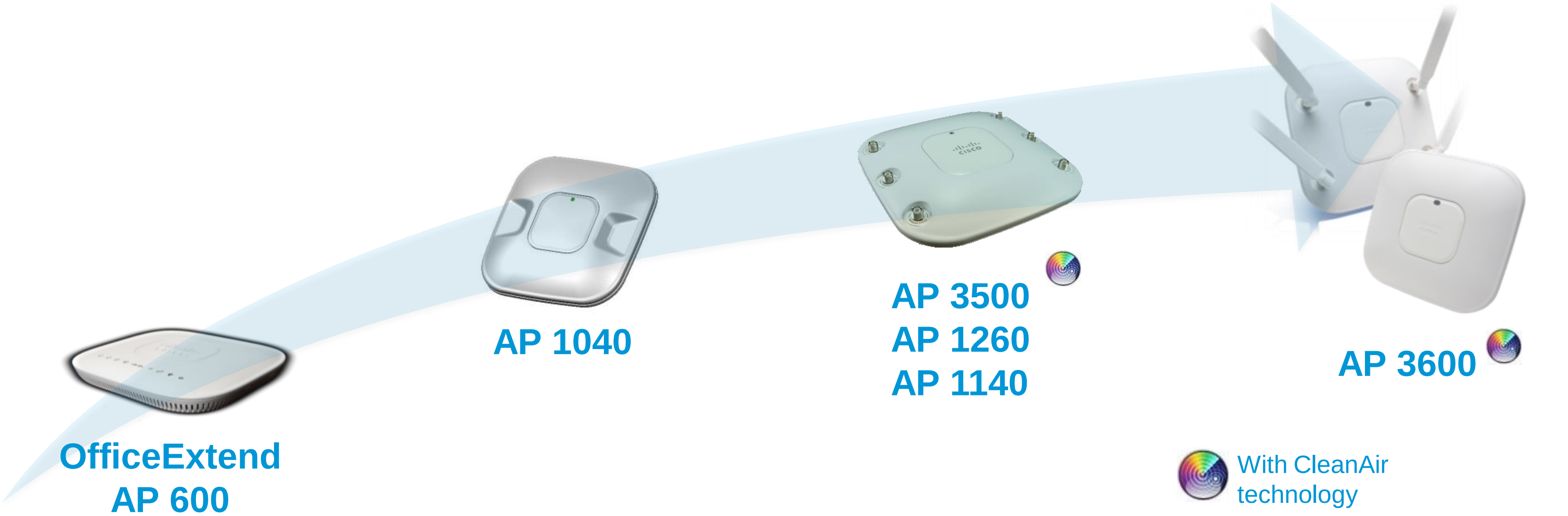
Unified Management: Wireless Control System
Services Platform: Mobility Services Engine

Cisco WLAN Controller Portfolio



Cisco Aironet 802.11n Access Points

Teleworker | *Business-Ready* | *Mission Critical* | *Best in Class Mission Critical*



OfficeExtend
AP 600

AP 1040

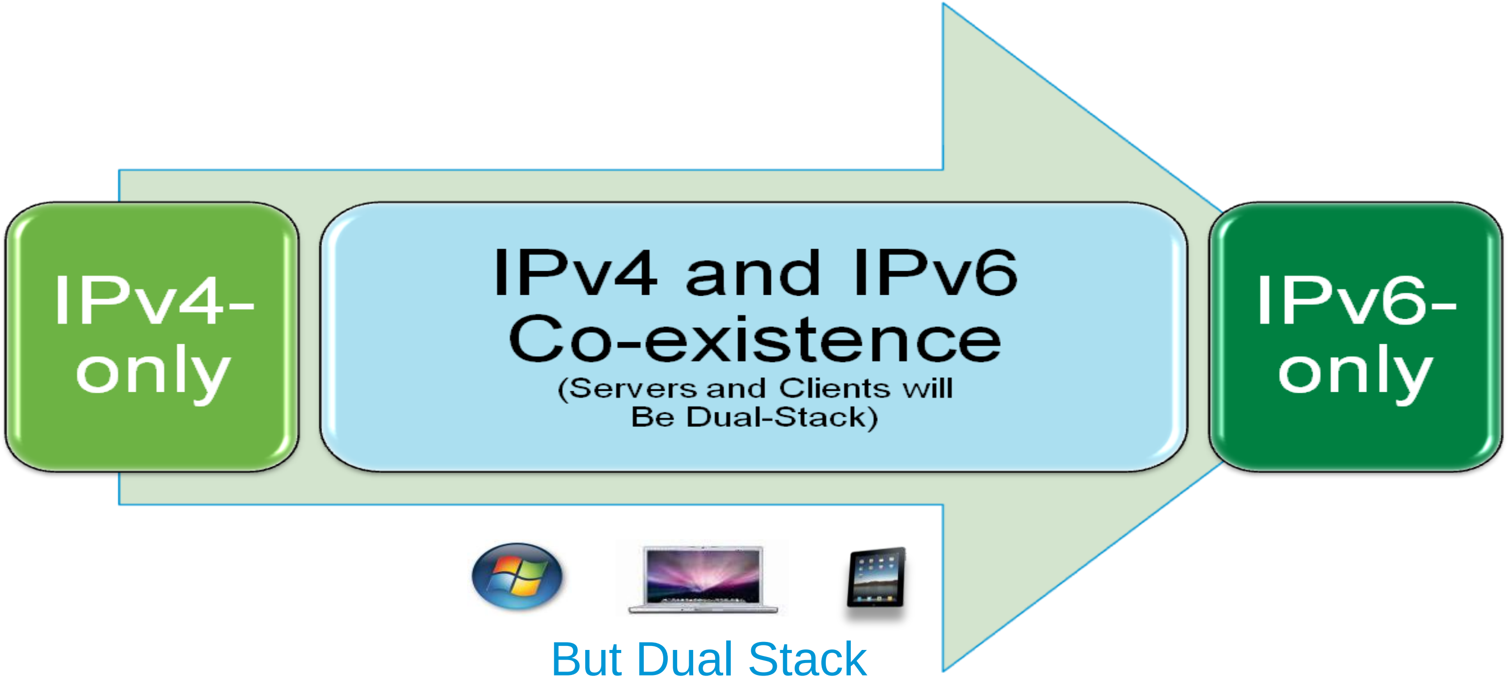
AP 3500 ●
AP 1260
AP 1140

AP 3600 ●

● With CleanAir technology

802.11n WiFi

IPv6 Will Be a Phased Implementation



IPv4-only

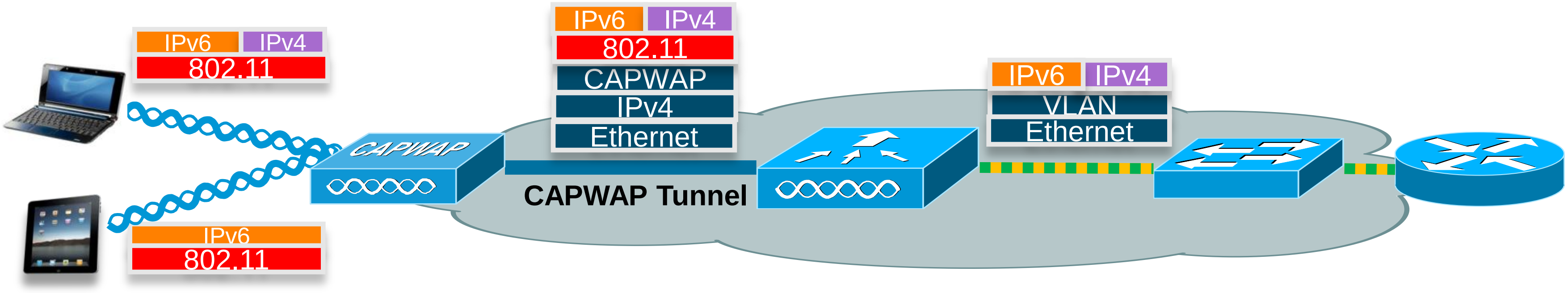
IPv4 and IPv6 Co-existence

(Servers and Clients will Be Dual-Stack)

IPv6-only

But Dual Stack Clients Are Here Now…

Wireless IPv6 Client Support



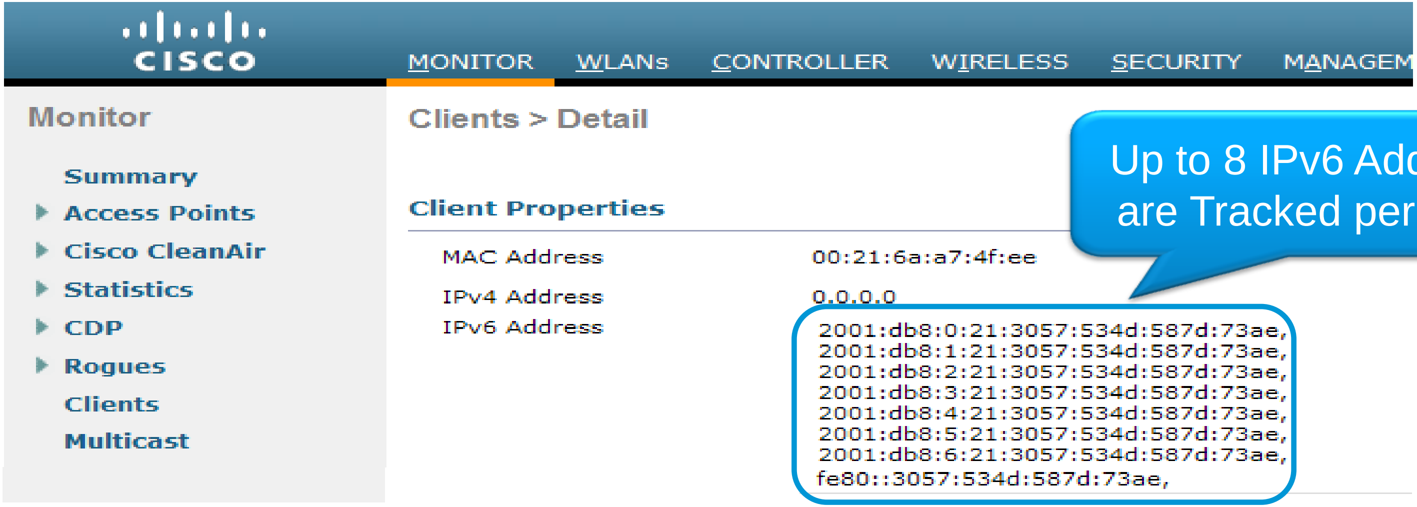
- Supports IPv4, Dual Stack and Native IPv6 clients on single WLAN simultaneously.
- Supports the following IPv6 address assignment for wireless clients:

  IPv6 Stateless Autoconfiguration [SLAAC]

  Stateless, Stateful DHCPv6

  Static IPv6 configuration
- Supports up to 8 IPv6 addresses per client.
- Clients will be able to pass traffic once IPv4 and/or IPv6 address assignment is completed after successful authentication.

Many IPv6 Addresses Per Client



Clients > Detail

Client Properties

```
MAC Address      00:21:6a:a7:4f:ee
IPv4 Address     0.0.0.0
IPv6 Address     2001:db8:0:21:3057:534d:587d:73ae,
                 2001:db8:1:21:3057:534d:587d:73ae,
                 2001:db8:2:21:3057:534d:587d:73ae,
                 2001:db8:3:21:3057:534d:587d:73ae,
                 2001:db8:4:21:3057:534d:587d:73ae,
                 2001:db8:5:21:3057:534d:587d:73ae,
                 2001:db8:6:21:3057:534d:587d:73ae,
                 fe80::3057:534d:587d:73ae,
```

Up to 8 IPv6 Addresses are Tracked per Client.

- Support for many IPv6 addresses per client is necessary because:
  - Clients can have multiple address types per interface
  - Clients can be assigned addresses via multiple methods such as SLAAC and DHCPv6
  - Most clients automatically generate a temporary address in addition to assigned addresses.

Complete IPv6 Support

- First Hop Security & Optimization
  - DHCPv6 Server Guard
  - Router Advertisement (RA) Guard
  - IPv6 Source Guard
  - Neighbor Solicitation (NS) Suppression
  - Router Advertisement (RA) Throttling
- Layer 2 & 3 Roaming
- IPv6 ACL support
- QoS support
- Guest access support
- Multicast to Unicast conversion at the AP
- FlexConnect

Beyond BYOD

Secure, Customized Experience per User, per Device

Joining "Guest Network"...

Settings — Wi-Fi Networks

Wi-Fi: ON

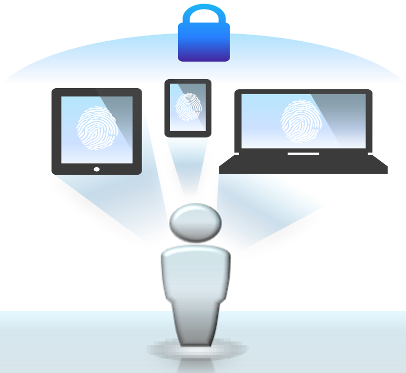
Choose a Network...

Network

✓ Guest Network

Other...

Ask to Join Networks: OFF



Device Onboarding and Guest Access

Unified Policy

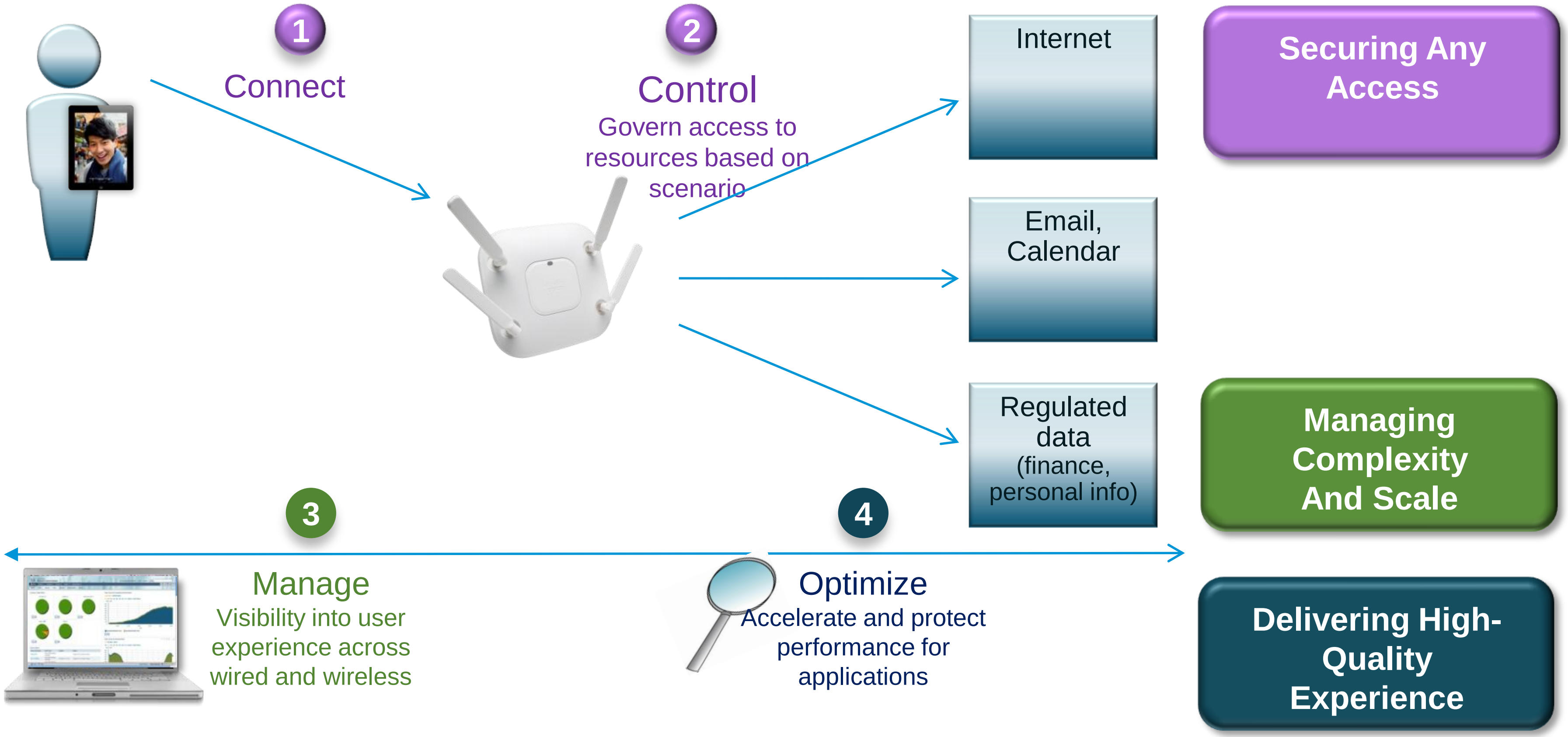
Uncompromised User Experience

Simplified IT experience

BYOD

Beyond BYOD

Cisco BYOD+



1 Connect

2 Control

Govern access to resources based on scenario

Internet

Email, Calendar

Regulated data (finance, personal info)

Securing Any Access

3 Manage

Visibility into user experience across wired and wireless

4 Optimize

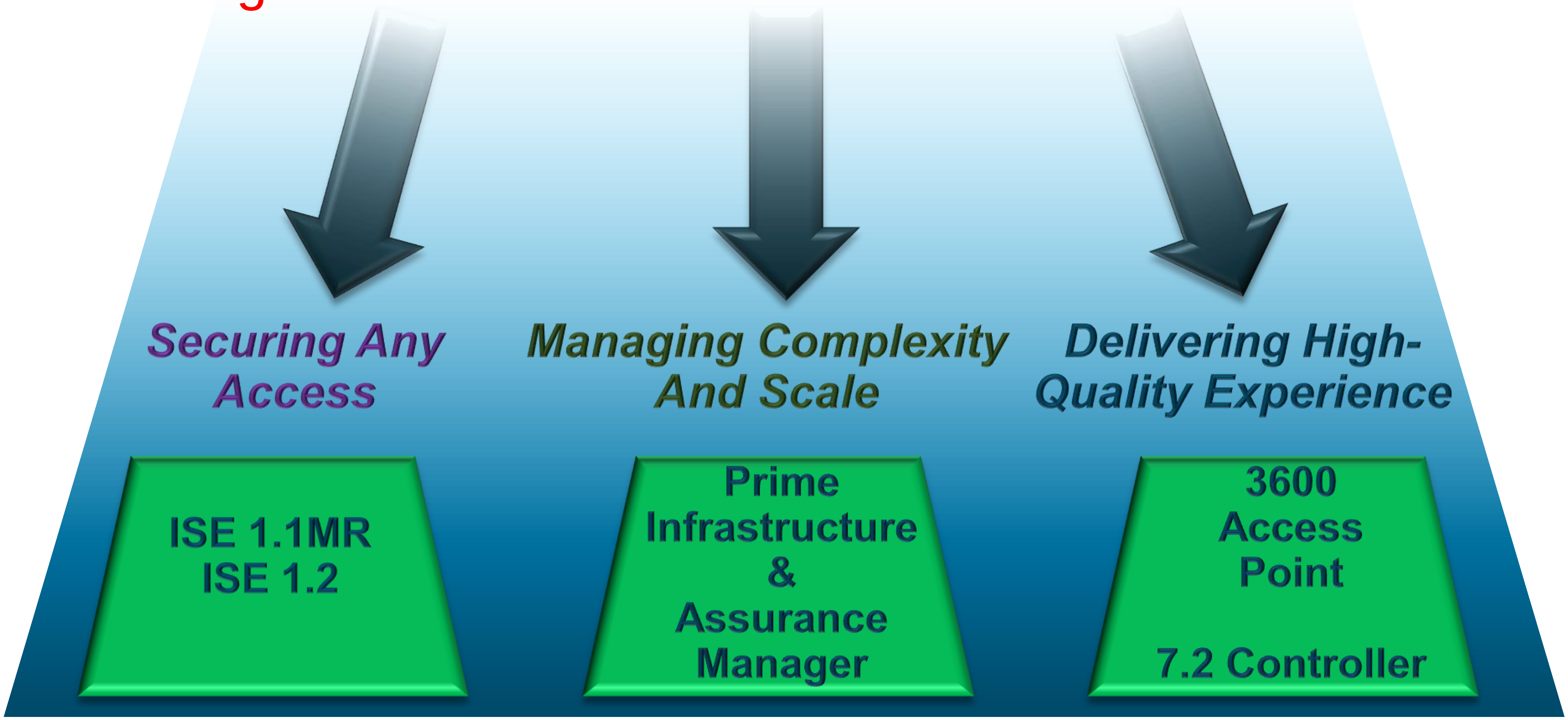
Accelerate and protect performance for applications

Managing Complexity And Scale

Delivering High-Quality Experience

Cisco BYOD+

IT Challenges to Mobile Freedom



Securing Any Access

Managing Complexity And Scale

Delivering High-Quality Experience

ISE 1.1MR
ISE 1.2

Prime Infrastructure & Assurance Manager

3600 Access Point

7.2 Controller

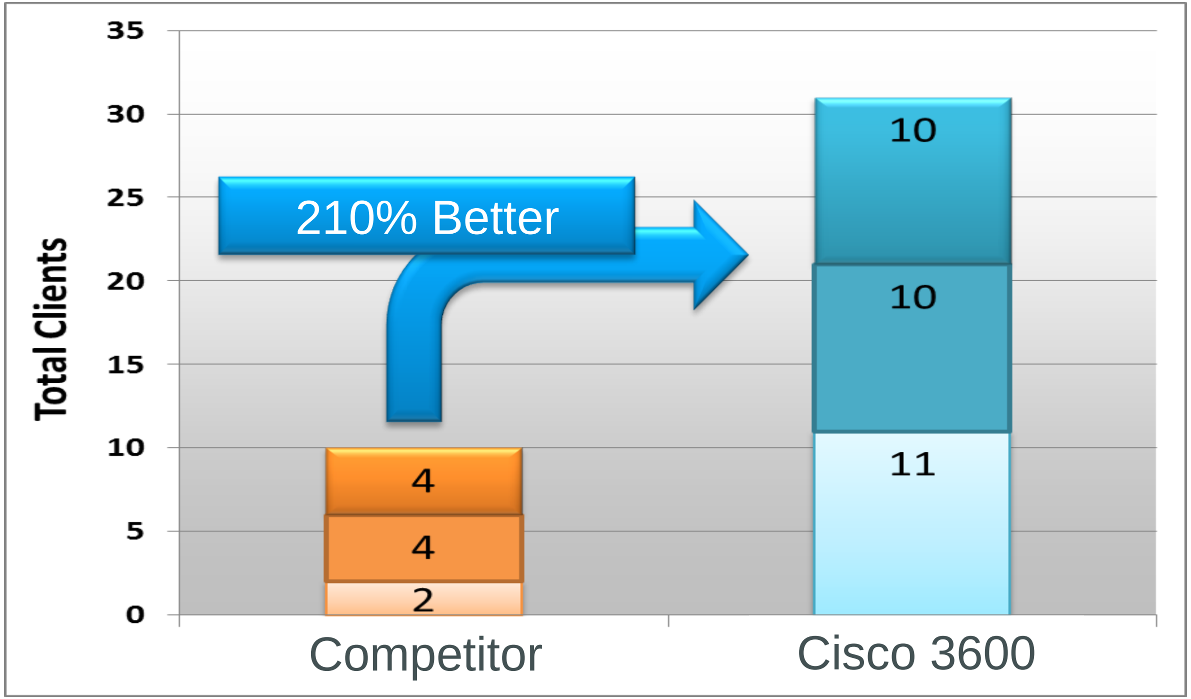
3600 Access Point

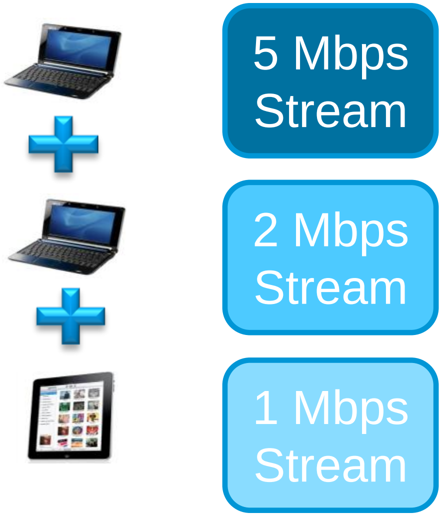
Industry's only 4x4: 3 spatial stream access point

- Deliver 30% more performance
- Deliver mission critical reliability with CleanAir
- Boost client performance with ClientLink 2.0
- Add-on modules with the Modular architecture

Triple-Stream Video Capacity

Miercom PERFORMANCE VERIFIED





5 Mbps Stream

2 Mbps Stream

1 Mbps Stream

With a mix of all types of video clients using multicast and unicast TCP video (AirVideo), Cisco delivers 3x the performance.

Cisco Identity Services Engine – ISE

Consolidated Contextual Information

Real-Time Awareness
Track Active Users and Devices

Integrated Device Profiling & Posture Assessment

Profiling of wired and wireless devices
Integrated and built into ISE policy

Consistent Policy for Device Categories

Guest Lifecycle Management

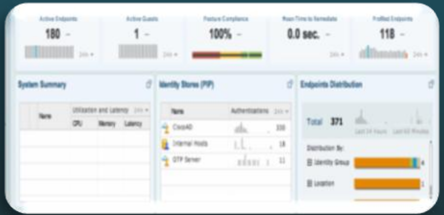
Provide Guest Access in a seamless, secure manner

Simplified Role-Based Access

SGT	Public	Private
Staff	Permit	Permit
Guest	Permit	Deny

Keep Existing Logical Design
Manage Security Group Access

System-wide Visibility



Active Endpoints 180
Active Guests 1
Posture Compliance 100%
Mean Time to Remediate 0.0 sec.
Profiled Endpoints 118

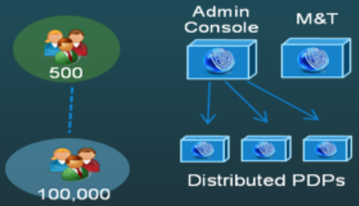
System Summary
Name | Utilization and Latency | CPU | Memory | Latency

Identity Stores (PIP)
Name | Authentications
CiscoAD 330
Internal Hosts 18
OTP Server 11

Endpoints Distribution
Total 371
Last 24 Hours
Last 60 Minutes
Distribution By:
Identity Group
Location

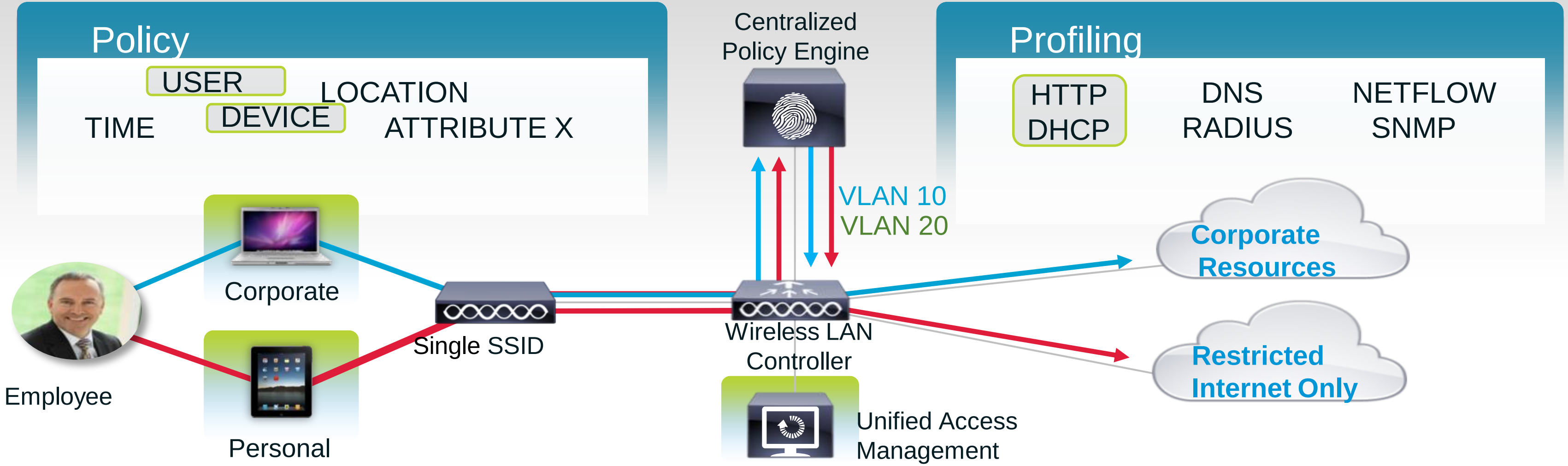
Troubleshoot and Monitoring
Consolidated Data

Scales to meet organizations needs



Scalable Architecture
Innovative Licensing

Cisco's Borderless - Unified Policy Management



District Issued Device

1. 802.1x EAP User Authentication
2. Profiling to identify device
3. Policy decision
4. Policy enforce to “VLAN 10” on same SSID
5. Full access granted
6. Full device visibility

PERSONAL Device

1. 802.1x EAP User Authentication
2. Profiling to identify device
3. Policy decision
4. Policy enforce to “VLAN 10 or 20” on same SSID
5. Full or Restricted access granted
6. Full device visibility

On-Boarding (1.1MR June 12)

Supplicant profile provisioning on supported platforms (iOS, Android, Windows, OS X)

Self / Sponsor registration portals for users and devices

Certificate provisioning as registry authority (RA) adding username and device ID to cert (integrates with existing corp CA/PKI)

Secure access (single SSID, certificate based differentiation of service)

User initiated control their devices (designate “Lost” -> black-listing, re-instate device, etc)

MDM Integration (ISE 1.2 Fall 2012)

airwatch™ MobileIron® Good ZENPRISE

On Prem MDM Device Registration - non registered clients redirected to MDM registration page

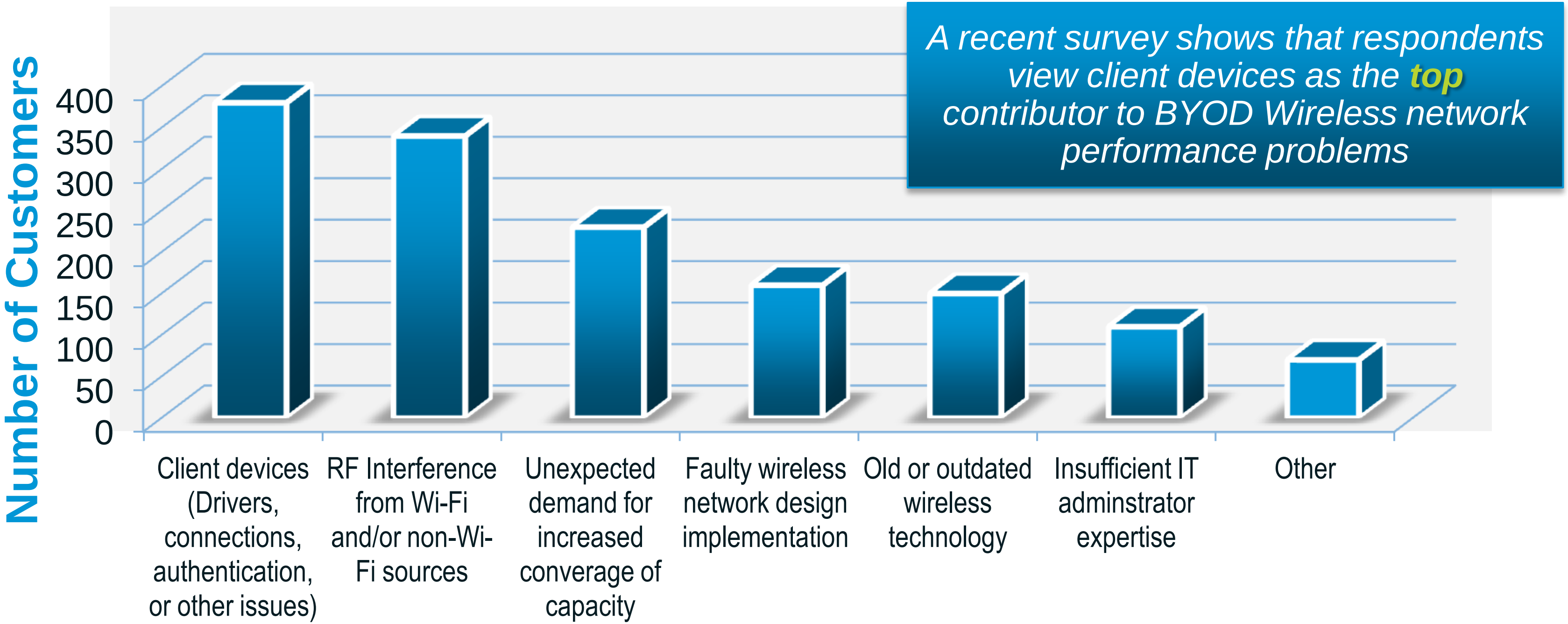
Restricted Access - non compliant clients will be given restricted access based on MDM posture state

Augment Endpoint Data - Update data from endpoint which cannot be gathered by profiling

Ability initiate device action from ISE - eg: device stolen -> need to wipe data on client (Stretch).

Cisco's Unified Network Management

Top BYOD Wireless Issues

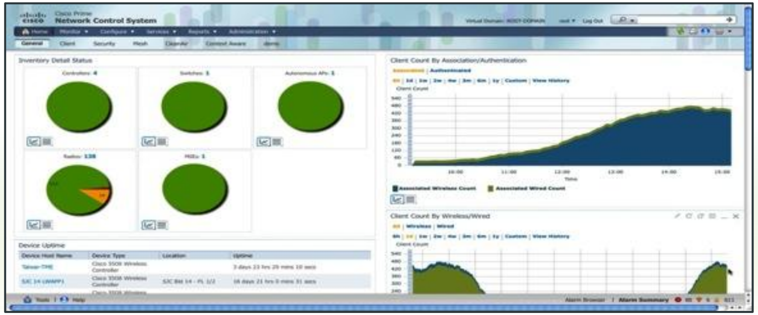


A recent survey shows that respondents view client devices as the ***top*** *contributor to BYOD Wireless network performance problems*

Cisco Prime Network Control System

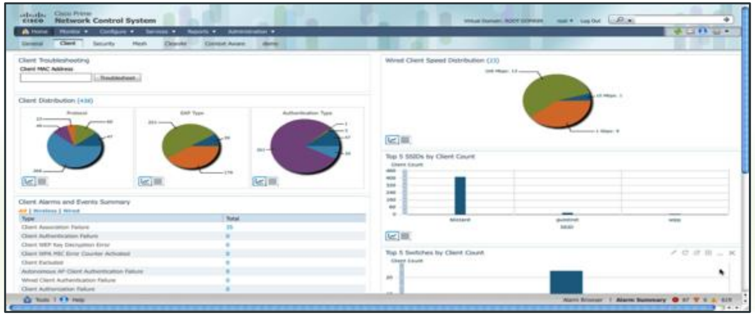
Converged Access Management for Wired and Wireless Networks

High-Level View of Key Metrics with Contextual Drill-Down to Detailed Data



Device Uptime

Device Host Name	Device Type	Location	Uptime
Taiwan-TME	Cisco 3508 Wireless Controller		3 days 23 hrs 29 mins 10 secs
SJC 14 (WAPP)	Cisco 5508 Wireless Controller	SJC Bld 14 - FL 1/2	16 days 21 hrs 0 mins 31 secs



Client Alarms and Events Summary

All | Wireless | Wired

Type	Total
Client Association Failure	35
Client Authentication Failure	0
Client WEP Key Decryption Error	0
Client WPA MIC Error Counter Activated	0
Client Excluded	0
Autonomous AP Client Authentication Failure	0
Wired Client Authentication Failure	0
Client Authorization Failure	0

- Flexible platform: Accommodates new and experienced IT administrators
- Simple, intuitive user interface: Eliminates complexity
- User-defined customization: Display the most relevant information

Integrated Access Infrastructure Visibility

- Wired and wireless discovery and inventory

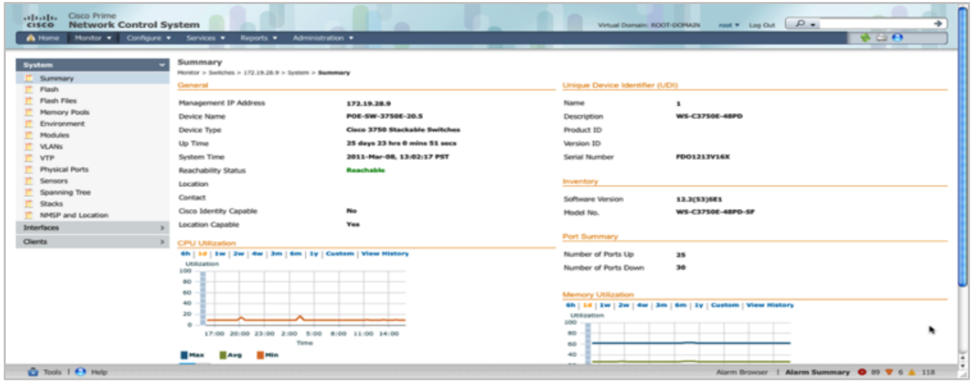
  Add/detect infrastructure devices such as switches, WLAN controllers, and access points

- Comprehensive access infrastructure reporting

  View the access infrastructure as a whole

- Stolen asset notification

  Track when devices presumed stolen come back online



Summary

Monitor > Switches > 172.19.28.9 > System > Summary

General

Management IP Address	172.19.28.9
Device Name	POE-SW-3750E-20.5
Device Type	Cisco 3750 Stackable Switches
Up Time	25 days 23 hrs 0 mins 51 secs
System Time	2011-Mar-08, 13:02:17 PST
Reachability Status	Reachable
Location	
Contact	
Cisco Identity Capable	No
Location Capable	Yes

CPU Utilization

Unique Device Identifier (UDI)

Name	1
Description	WS-C3750E-48PD
Product ID	
Version ID	
Serial Number	FDO1213V16X

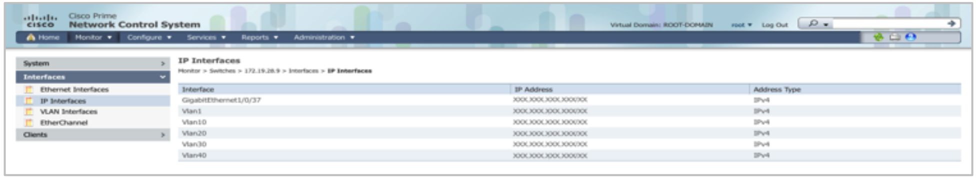
Inventory

Software Version	12.2(53)SE1
Model No.	WS-C3750E-48PD-SF

Port Summary

Number of Ports Up	25
Number of Ports Down	30

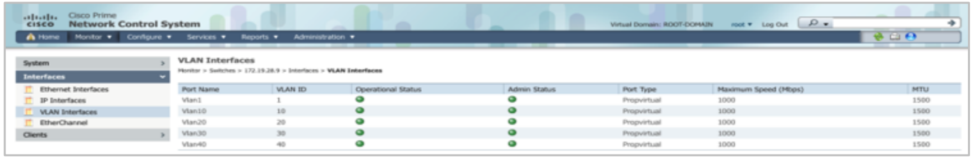
Memory Utilization



IP Interfaces

Monitor > Switches > 172.19.28.9 > Interfaces > IP Interfaces

Interface	IP Address	Address Type
GigabitEthernet1/0/37	XXX.XXX.XXX.XXX/XX	IPv4
Vlan1	XXX.XXX.XXX.XXX/XX	IPv4
Vlan10	XXX.XXX.XXX.XXX/XX	IPv4
Vlan20	XXX.XXX.XXX.XXX/XX	IPv4
Vlan30	XXX.XXX.XXX.XXX/XX	IPv4
Vlan40	XXX.XXX.XXX.XXX/XX	IPv4



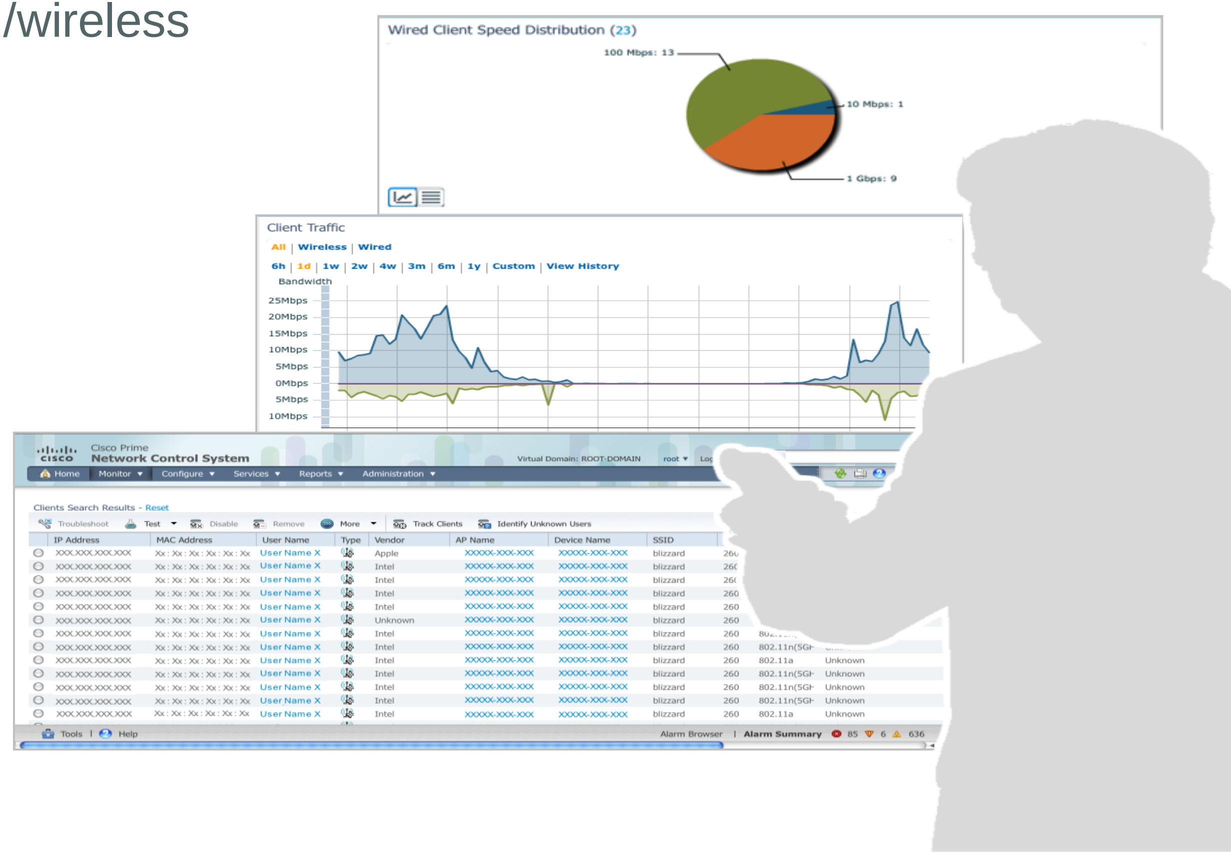
VLAN Interfaces

Monitor > Switches > 172.19.28.9 > Interfaces > VLAN Interfaces

Port Name	VLAN ID	Operational Status	Admin Status	Port Type	Maximum Speed (Mbps)	MTU
Vlan1	1	●	●	Propvirtual	1000	1500
Vlan10	10	●	●	Propvirtual	1000	1500
Vlan20	20	●	●	Propvirtual	1000	1500
Vlan30	30	●	●	Propvirtual	1000	1500
Vlan40	40	●	●	Propvirtual	1000	1500

Unified User and Endpoint Services

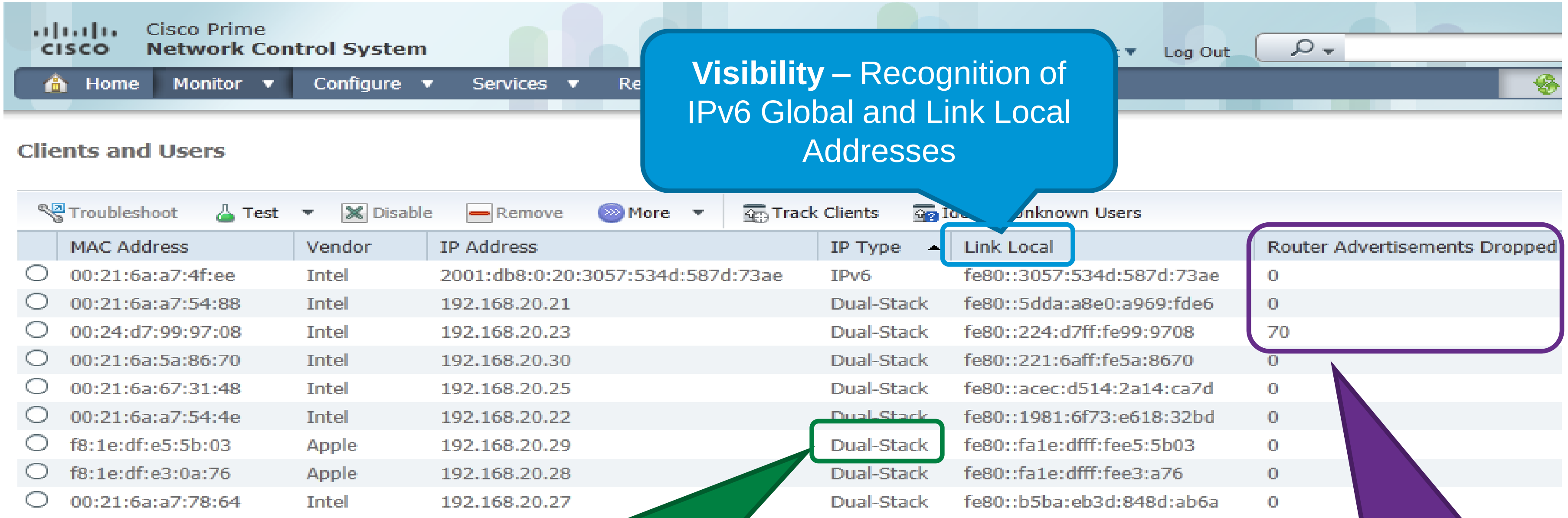
- Correlated and focused wired/wireless client visibility
    - Client health metrics
    - Client posture and profile
    - Client troubleshooting
    - Client reporting
    - Unknown device ID input
- Clear view of the end user landscape
    - Who is connecting
    - Using which device
    - Are they authorized



Clients Search Results - Reset

	IP Address	MAC Address	User Name	Type	Vendor	AP Name	Device Name	SSID			
○	XXX.XXX.XXX.XXX	Xx : Xx : Xx : Xx : Xx : Xx	User Name X		Apple	XXXXX-XXX-XXX	XXXXX-XXX-XXX	blizzard	26		
○	XXX.XXX.XXX.XXX	Xx : Xx : Xx : Xx : Xx : Xx	User Name X		Intel	XXXXX-XXX-XXX	XXXXX-XXX-XXX	blizzard	26		
○	XXX.XXX.XXX.XXX	Xx : Xx : Xx : Xx : Xx : Xx	User Name X		Intel	XXXXX-XXX-XXX	XXXXX-XXX-XXX	blizzard	26		
○	XXX.XXX.XXX.XXX	Xx : Xx : Xx : Xx : Xx : Xx	User Name X		Intel	XXXXX-XXX-XXX	XXXXX-XXX-XXX	blizzard	260		
○	XXX.XXX.XXX.XXX	Xx : Xx : Xx : Xx : Xx : Xx	User Name X		Intel	XXXXX-XXX-XXX	XXXXX-XXX-XXX	blizzard	260		
○	XXX.XXX.XXX.XXX	Xx : Xx : Xx : Xx : Xx : Xx	User Name X		Unknown	XXXXX-XXX-XXX	XXXXX-XXX-XXX	blizzard	260		
○	XXX.XXX.XXX.XXX	Xx : Xx : Xx : Xx : Xx : Xx	User Name X		Intel	XXXXX-XXX-XXX	XXXXX-XXX-XXX	blizzard	260	802.1	
○	XXX.XXX.XXX.XXX	Xx : Xx : Xx : Xx : Xx : Xx	User Name X		Intel	XXXXX-XXX-XXX	XXXXX-XXX-XXX	blizzard	260	802.11n(5GH	
○	XXX.XXX.XXX.XXX	Xx : Xx : Xx : Xx : Xx : Xx	User Name X		Intel	XXXXX-XXX-XXX	XXXXX-XXX-XXX	blizzard	260	802.11a	Unknown
○	XXX.XXX.XXX.XXX	Xx : Xx : Xx : Xx : Xx : Xx	User Name X		Intel	XXXXX-XXX-XXX	XXXXX-XXX-XXX	blizzard	260	802.11n(5GH	Unknown
○	XXX.XXX.XXX.XXX	Xx : Xx : Xx : Xx : Xx : Xx	User Name X		Intel	XXXXX-XXX-XXX	XXXXX-XXX-XXX	blizzard	260	802.11n(5GH	Unknown
○	XXX.XXX.XXX.XXX	Xx : Xx : Xx : Xx : Xx : Xx	User Name X		Intel	XXXXX-XXX-XXX	XXXXX-XXX-XXX	blizzard	260	802.11n(5GH	Unknown
○	XXX.XXX.XXX.XXX	Xx : Xx : Xx : Xx : Xx : Xx	User Name X		Intel	XXXXX-XXX-XXX	XXXXX-XXX-XXX	blizzard	260	802.11a	Unknown

Cisco NCS Comprehensive Visibility



Clients and Users

MAC Address	Vendor	IP Address	IP Type	Link Local	Router Advertisements Dropped
00:21:6a:a7:4f:ee	Intel	2001:db8:0:20:3057:534d:587d:73ae	IPv6	fe80::3057:534d:587d:73ae	0
00:21:6a:a7:54:88	Intel	192.168.20.21	Dual-Stack	fe80::5dda:a8e0:a969:fde6	0
00:24:d7:99:97:08	Intel	192.168.20.23	Dual-Stack	fe80::224:d7ff:fe99:9708	70
00:21:6a:5a:86:70	Intel	192.168.20.30	Dual-Stack	fe80::221:6aff:fe5a:8670	0
00:21:6a:67:31:48	Intel	192.168.20.25	Dual-Stack	fe80::acec:d514:2a14:ca7d	0
00:21:6a:a7:54:4e	Intel	192.168.20.22	Dual-Stack	fe80::1981:6f73:e618:32bd	0
f8:1e:df:e5:5b:03	Apple	192.168.20.29	Dual-Stack	fe80::fa1e:dfff:fee5:5b03	0
f8:1e:df:e3:0a:76	Apple	192.168.20.28	Dual-Stack	fe80::fa1e:dfff:fee3:a76	0
00:21:6a:a7:78:64	Intel	192.168.20.27	Dual-Stack	fe80::b5ba:eb3d:848d:ab6a	0

Visibility – Recognition of IPv6 Global and Link Local Addresses

Insight – Identification of IPv4, Dual-Stack or IPv6-Only Client Types

Security – Identification of Clients Acting as IPv6 Routers

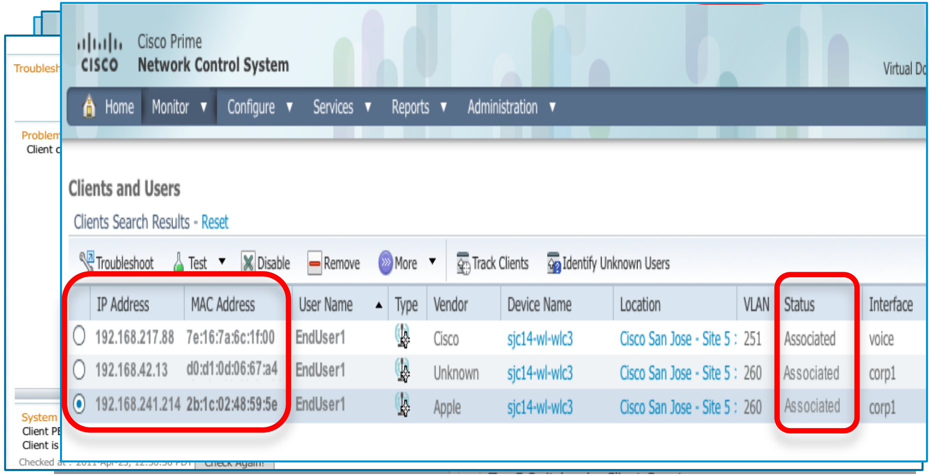
Troubleshoot Wired and Wireless Access

Using Cisco Prime for Converged Client Devices

USE CASE: User calls in to help center because they cannot get access to financial data on the network. IT determines if they are authorized to access this area.

1. Search on user name
2. Identify wired and wireless devices associated with the user
3. Display associated and disassociated devices
4. Use automated client troubleshooting workflow to resolve the issue
5.

Cisco Prime Network Control System (NCS)



Clients and Users

Clients Search Results - Reset

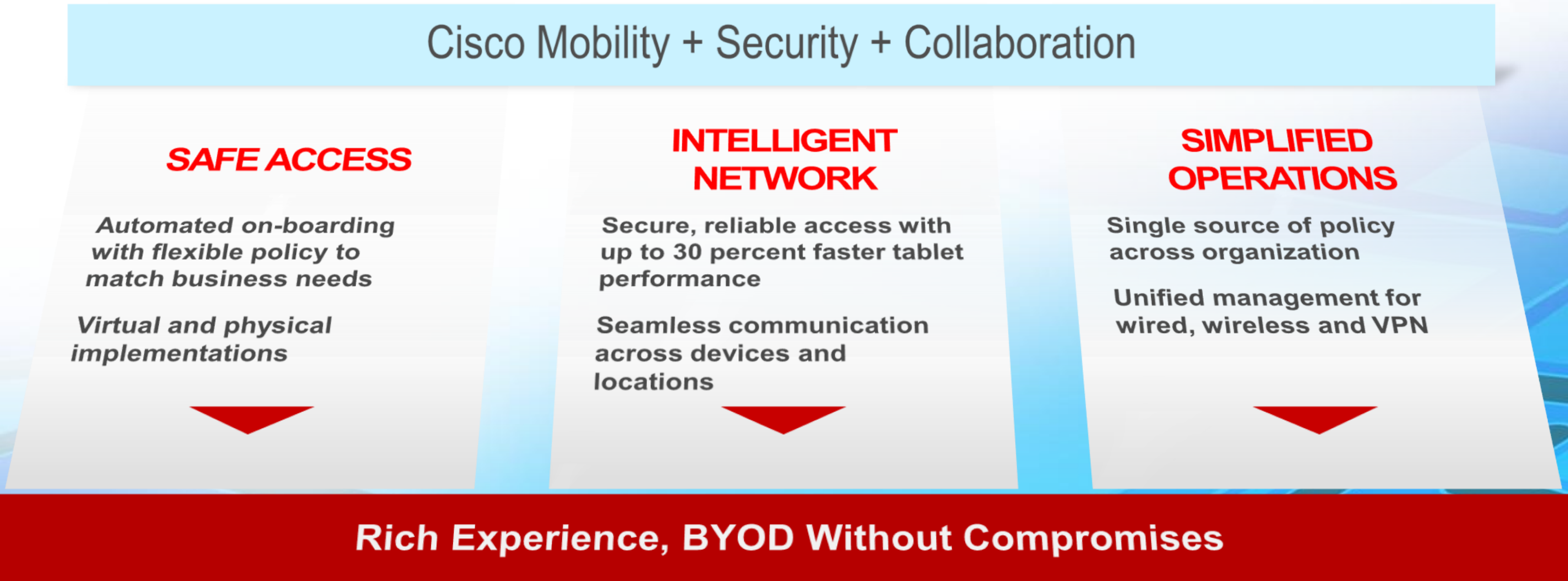
	IP Address	MAC Address	User Name ▲	Type	Vendor	Device Name	Location	VLAN	Status	Interface
○	192.168.217.88	7e:16:7a:6c:1f:00	EndUser1		Cisco	sjc14-wl-wlc3	Cisco San Jose - Site 5 :	251	Associated	voice
○	192.168.42.13	d0:d1:0d:06:67:a4	EndUser1		Unknown	sjc14-wl-wlc3	Cisco San Jose - Site 5 :	260	Associated	corp1
●	192.168.241.214	2b:1c:02:48:59:5e	EndUser1		Apple	sjc14-wl-wlc3	Cisco San Jose - Site 5 :	260	Associated	corp1

✓ *Troubleshoot user and access issues based on identity*

✓ *Speed resolution with intuitive guided workflows*

The Cisco Advantage

A Better Mobility Experience for Users and IT



Cisco Mobility + Security + Collaboration

SAFE ACCESS

Automated on-boarding with flexible policy to match business needs

Virtual and physical implementations

INTELLIGENT NETWORK

Secure, reliable access with up to 30 percent faster tablet performance

Seamless communication across devices and locations

SIMPLIFIED OPERATIONS

Single source of policy across organization

Unified management for wired, wireless and VPN

Rich Experience, BYOD Without Compromises

Q&A

Cisco Canada Plus

We value your feedback.

Please be sure to complete the Evaluation Form for this session.

Access today’s presentations at cisco.com/ca/plus

Follow @CiscoCanada and join the #CiscoPlusCA conversation