



Cisco *live!*

January 29 - February 2, 2018 · Barcelona

BRKEWN-2670

Wireless Best Practices for Next-gen Workspace

Aparajita Sood, Technical Marketing Engineer
apsood@cisco.com

Cisco Spark

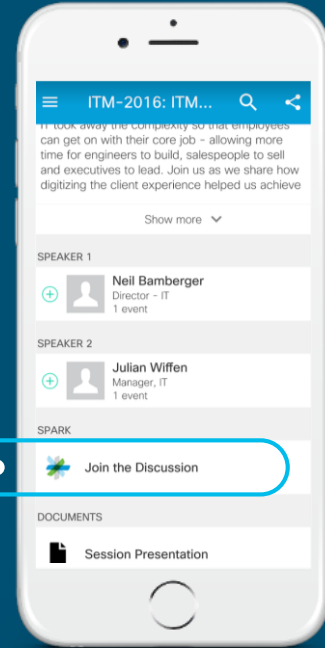


Questions?

Use Cisco Spark to communicate with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space

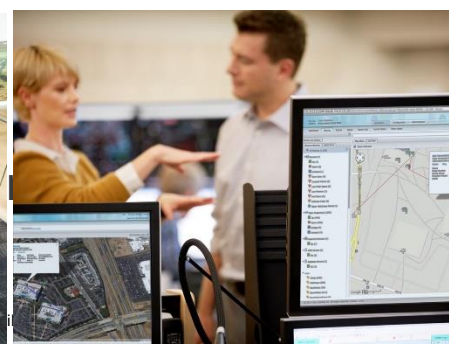


cs.co/cislivebot#BRKEWN-2670



Work Styles Have Evolved Work anytime from anywhere

“Work is a thing you do, not a place you go to”



Agenda



- Designing for Performance and Resiliency
- Provisioning with Best Practices
- **Optimizing** RF and Security
- Analytics and Visibility



Deployment Lifecycle

The Bigger Picture



Next-Gen Office Design Goals

Designing for RF Coverage and Performance

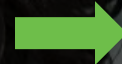
Media Access: Wi-Fi Networks are not Deterministic! (like a teacher in a class)



More devices in cell



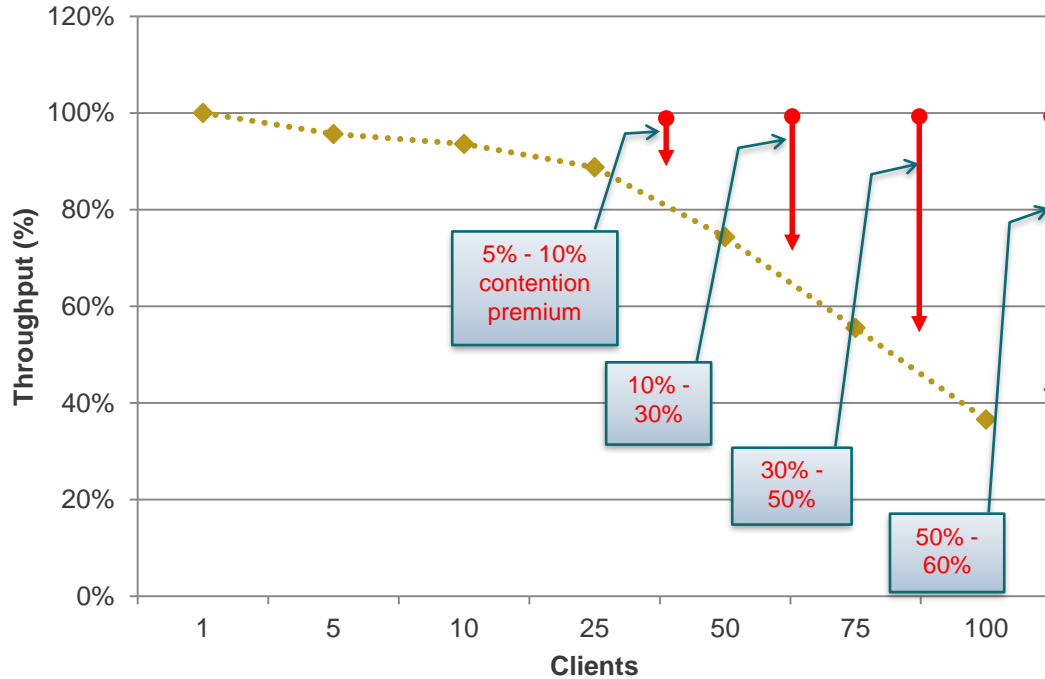
Greater contention



Increased risk of collisions

How Much Does Contention Affect Performance

The Breaking Point Depends on How Many Clients You Have

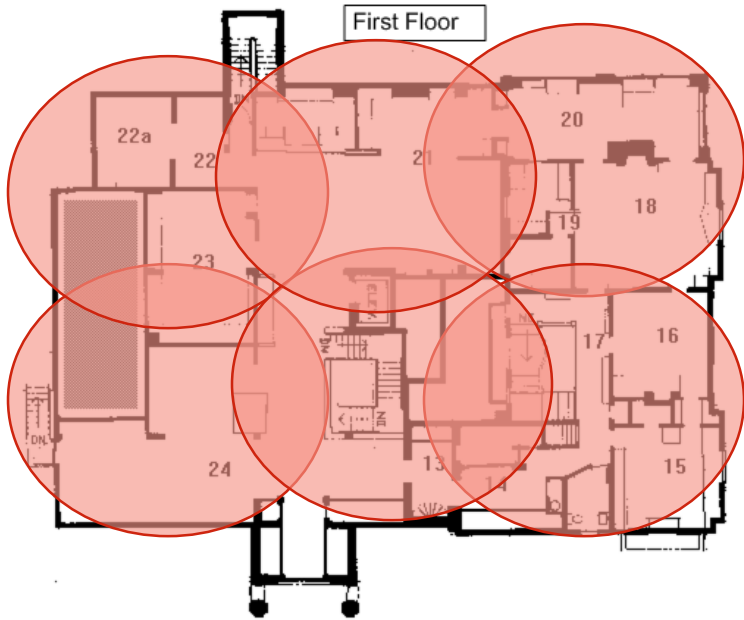


As more clients associate and transmit, WLAN contention increases for all clients.

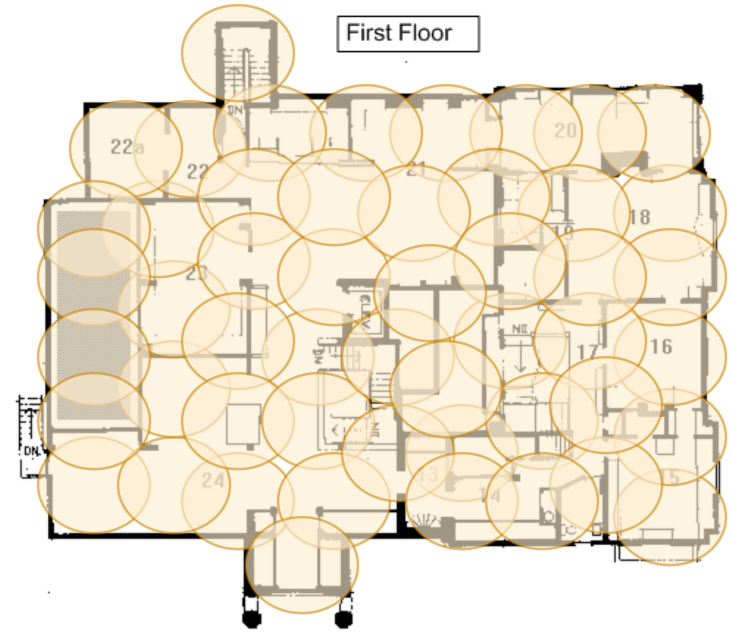


Retry attempts increase and each station spends more and more time in the “waiting and listening” state, driving down performance

Design for Density, not Coverage



3.2 Mbps cell edge



72.5 Mbps cell edge

People only use one real time application at a time

1. Check the bandwidth of each expected applications in your network
2. Multiply by number of users of that application in the cell:

This is the bandwidth you need at the edge of the cell

Application – By Use Case	Throughput – Nominal Case
Web - Casual	500 Kbps
Web - Instructional	1 Mbps
Audio - Casual	100 Kbps
Audio - instructional	1 Mbps
Video - Casual	1 Mbps
Video - Instructional	2-4 Mbps
Printing	1 Mbps
File Sharing - Casual	1 Mbps
File Sharing - Instructional	2-8 Mbps
Online Testing	2-4 Mbps
Device Backups	10-50 Mbps

An Example – Identifying the BW Needs in a Cell

- Skype 4 Business / Lync (Up and Down):

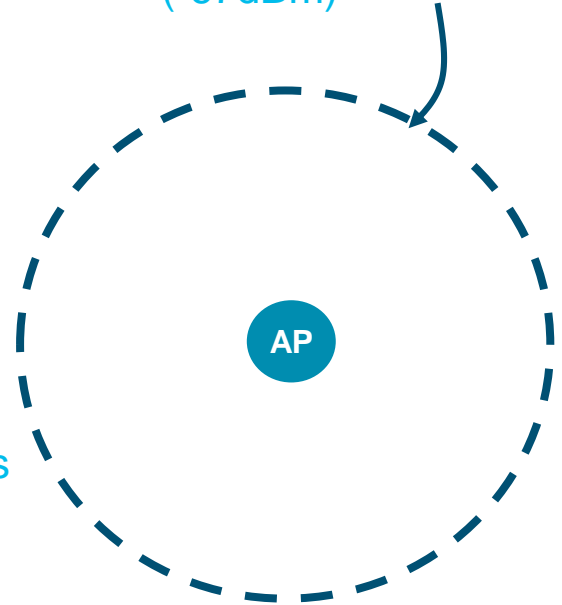
Call type	Audio	Audio HD	Video	Video HD
Typical Bandwidth	51Kbps	86Kbps	190kbps	2.5 Mbps

- A few other examples:
 - Jabber audio (G.711) ~100 kbps, Jabber video (HQ) ~750 kbps
 - Facetime (video, iPhone 4S): 400 Kbps, (audio) 32 kbps
 - Viber, Skype (video) 130 kbps, (audio) 30 kbps
 - Netflix (video), from 600 kbps (low quality) to 10 Mbps (3D HD), average 2.2 Mbps

Real Life Example

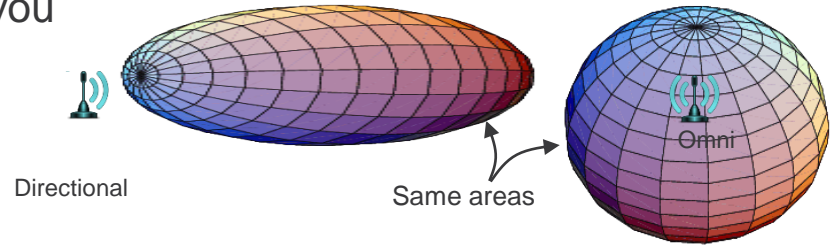
- Density studies show active 12 users / cell on average
 - Expected 2 HD video calls (Skype type)
 - 5 audio calls
 - Other users may browse
- Let's do the math:
 - 2 HD video calls = $2.5 \text{ Mbps} \times 2 \times 2 \text{ ways} = 10 \text{ Mbps}$
 - 5 audio calls... mmm what application?
 - Maybe SfB $51 \text{ kbps} \times 5 \times 2 \text{ ways} = 510 \text{ kbps}$
 - Others are browsing (5 people) = $250 \text{ kbps} / \text{user} = 1.2 \text{ Mbps}$
 - Total = **~12 Mbps needed**

I need ~12 Mbps throughput everywhere in the cell
... therefore I need it here (-67dBm)



Cell Shape and Cell Size

- Your cell shape depends on the antenna you use:
 - Directional
 - Omnidirectional
- The cell size depends on 3 parameters:
 1. The AP power level
 2. The protocol you use (802.11a/b/g/n/ac)
 3. The Data rates you allow



Higher Power Does not Always Mean Better Signal

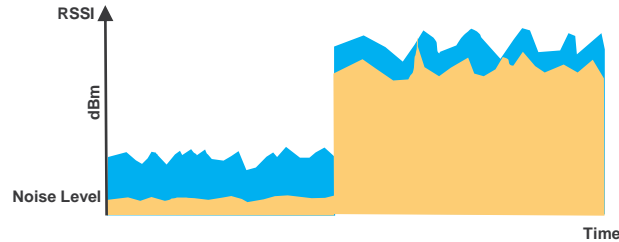
Is it better now?



Blah blah blah



You are a bit quiet




¿MOU
¿now?
¿MOU

Aim for:

- Noise level ≤ -92 dBm
- RSSI ≥ 67 dBm
- $\rightarrow 25$ dB or better SNR
- Channel Utilization under 50%.

- What's the right power ? In short: **half your worst client max power**
 - E.g. you design for 5 GHz, worst client max is at 11 dBm, set your AP power to 8 dBm



A modern office hallway with a woman in a grey top and black pants walking towards the camera, and another woman in a grey top and black skirt walking away. A man is visible in the background. The hallway has a green perforated wall on the left and a dark floor with a red stripe. The ceiling has recessed lights.

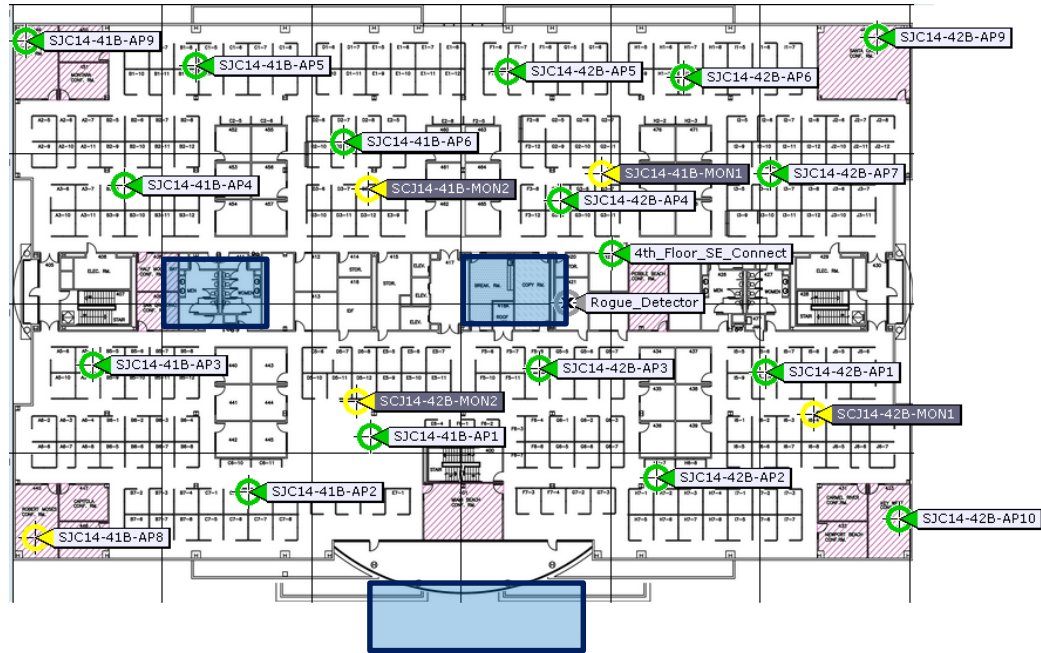
Next-Gen Office Design Goals

Design your Roaming Path

Where do You Need Coverage?

- Talk to end-users. Think what they will need and when, look for roaming paths

Bathroom?
Elevator?
Stairs?



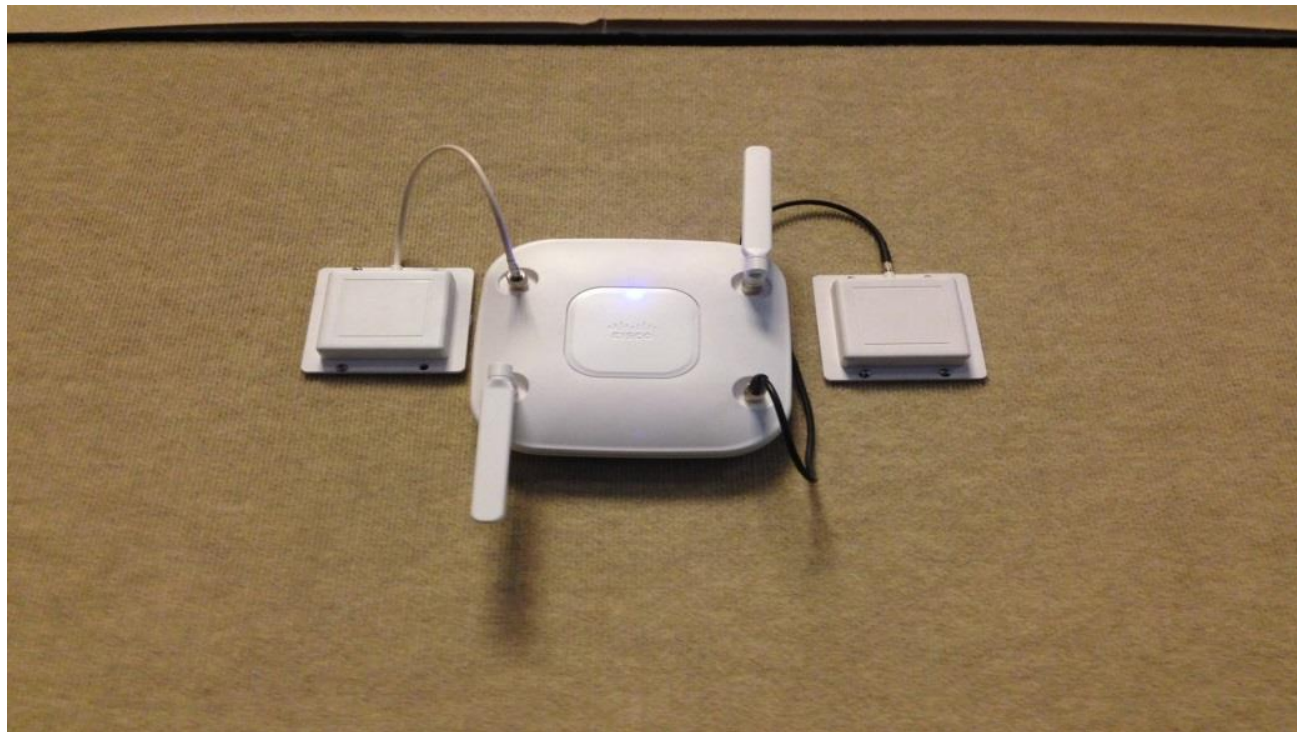
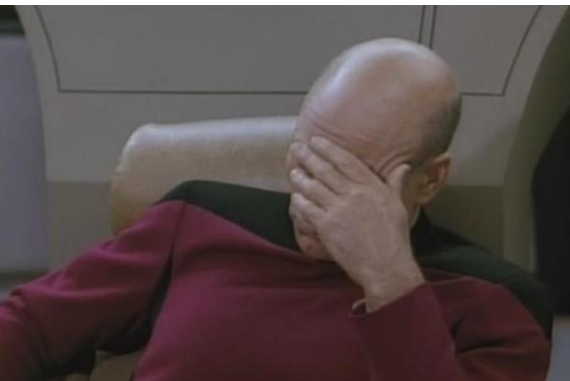
Outdoor
Smoking
Area?

Follow AP Placement Guidelines

- Mount APs so that antennas are vertical (we use vertical polarization)
- Avoid metallic objects that can affect the signal to your clients

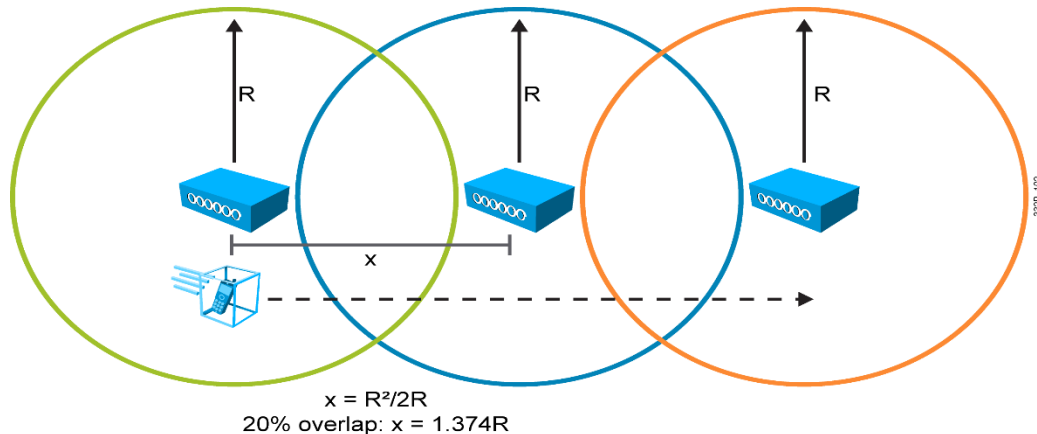


Really..? When RF cluelessness becomes art...



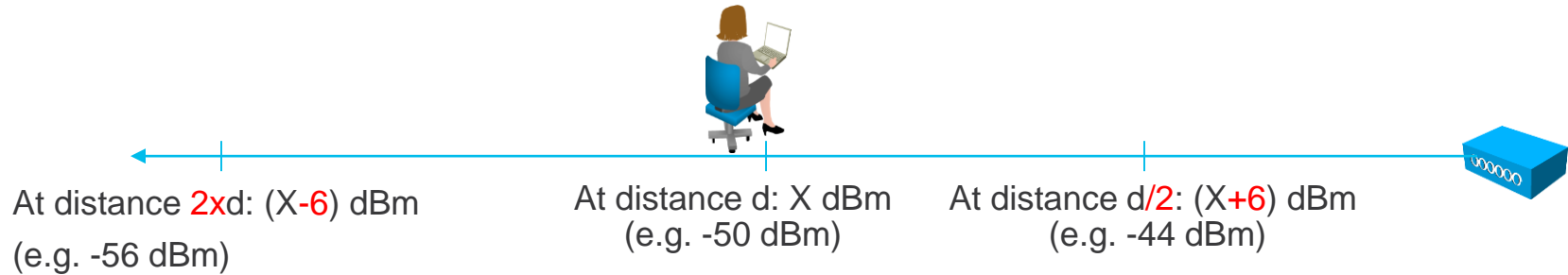
Rates and Cell Overlap

- Cell overlap is designed so that when a VoWLAN device gets to the -67 dBm area, it is already in good range of another access point.
- 20-percent overlap between cells is recommended
- How much is that? Use the -75 dBm rule if you are not sure.



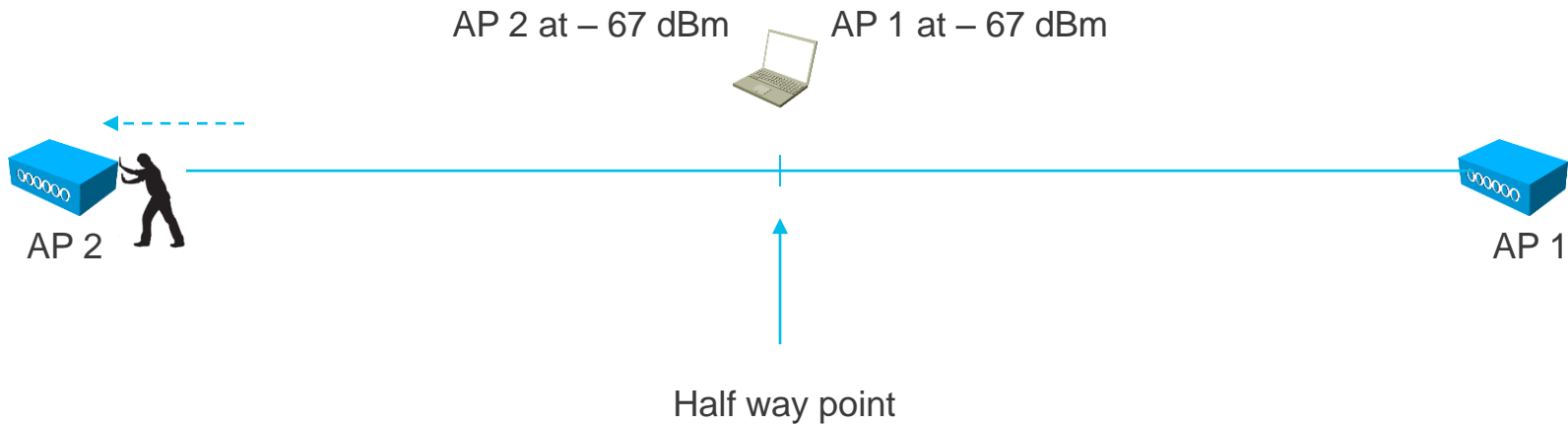
The -75 dBm Rule

- First trick to know:
 - Twice the distance = -6 dB
 - Half the distance = + 6dB



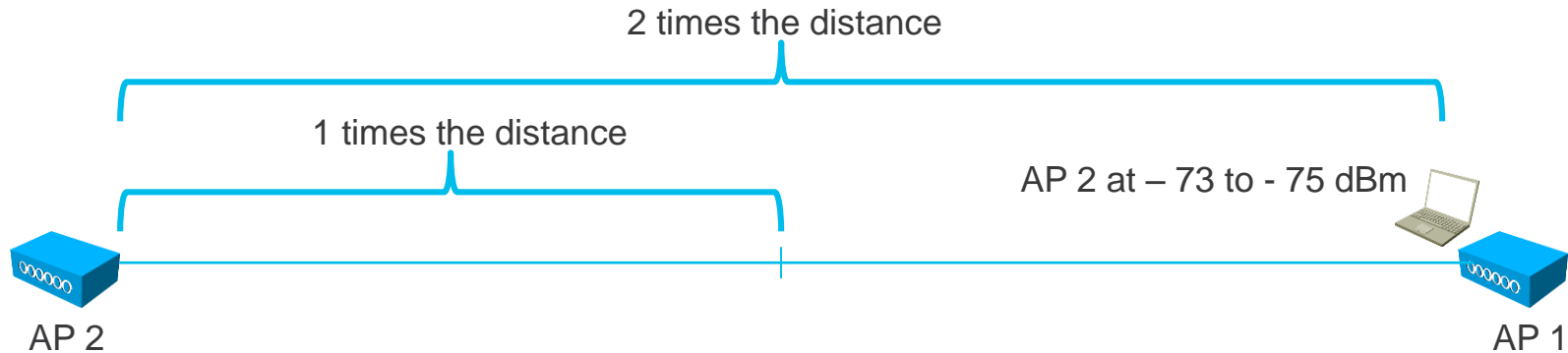
The -75 dBm Rule

- So if you stand at the “-67 dBm border”...
 - Move away from AP 1 until you get - 67 dBm
 - Then pull AP 2 in the other direction until you also hear it at - 67 dBm



The -75 dBm Rule

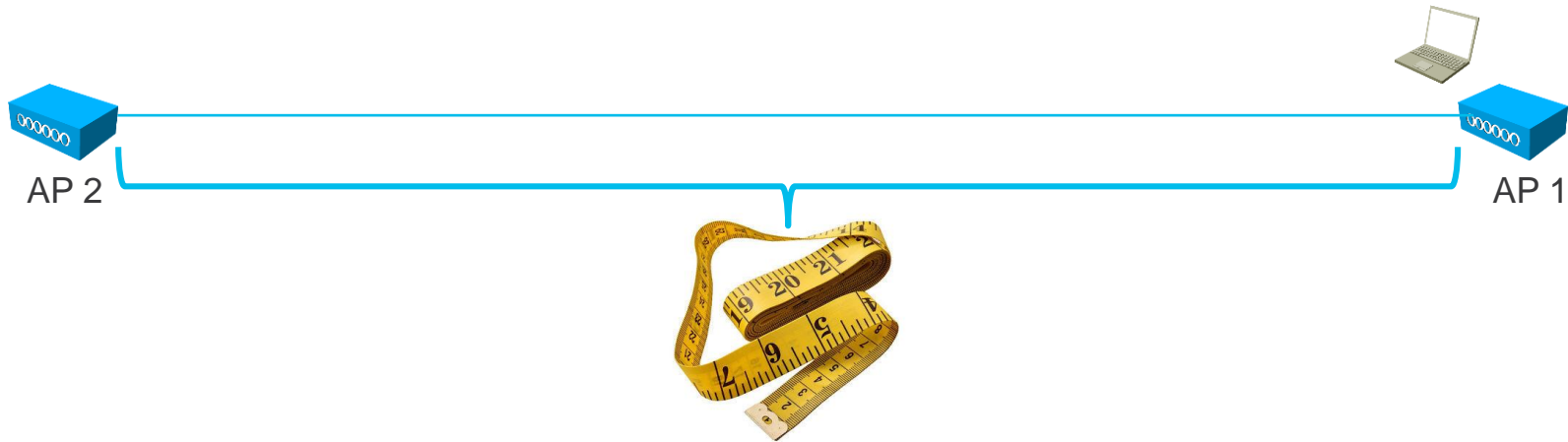
- Go back to AP 1
 - AP2 should be at “- 67 - 6” = -73 dBm. Add 2-3dB loss if there is a plaster wall -> - 75 dBm



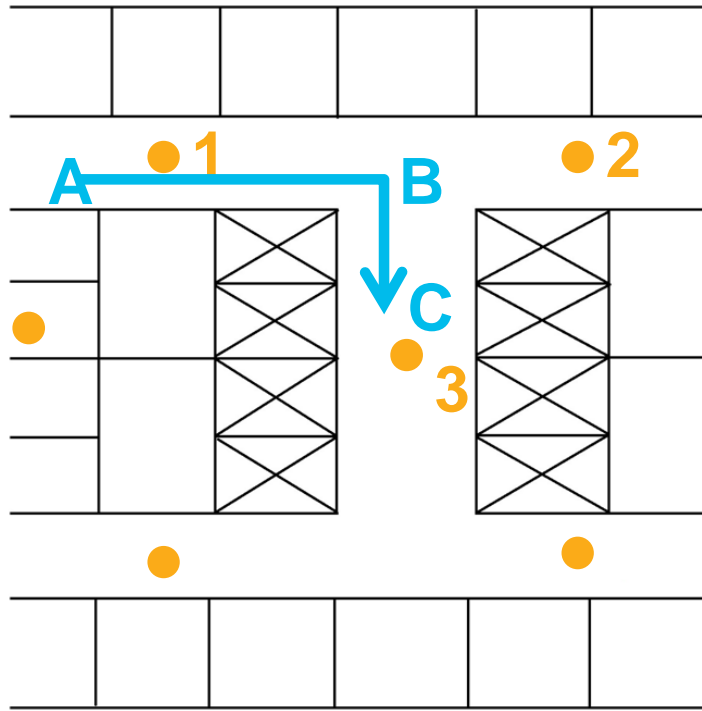
The -75 dBm Rule

- Measure
 - This is your average AP to AP distance

AP 2 at - 72 to - 75 dBm

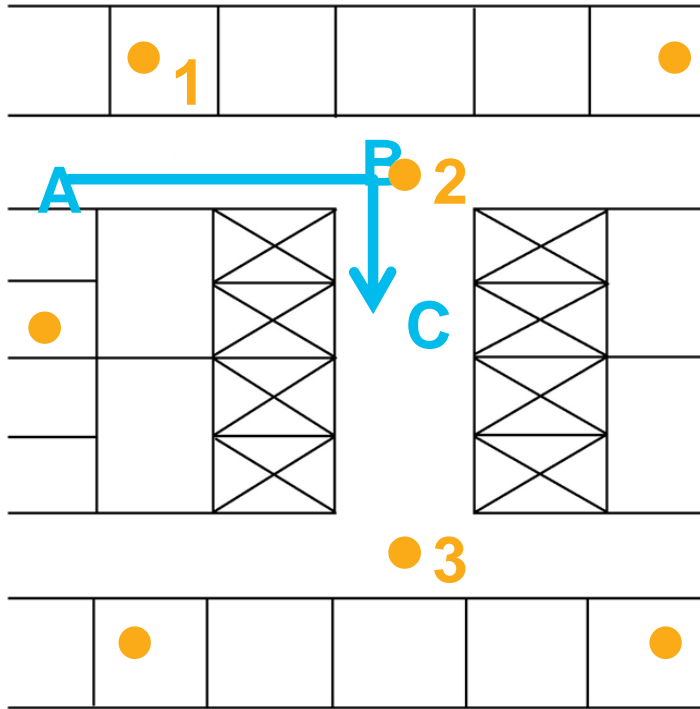


Strategically Position Your Transition APs



- At “A” the phone is connected to AP 1
- At “B” the phone has AP 2 in the neighbor list, AP 3 has not yet been scanned due to the RF shadow caused by the elevator bank
- At “C” the phone needs to roam, but AP 2 is the only AP in the neighbor list
- The phone then needs to rescan and connect to AP 3
 - 200 B frame @ 54 Mbps is sent in 3.7 μ s
 - 200 B frame @ 24 Mbps is sent in 8.3 μ s
 - Rate shifting from 54 Mbps to 24 Mbps can waste 1100 μ s

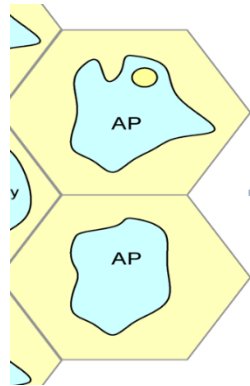
Strategically Position Your Transition APs



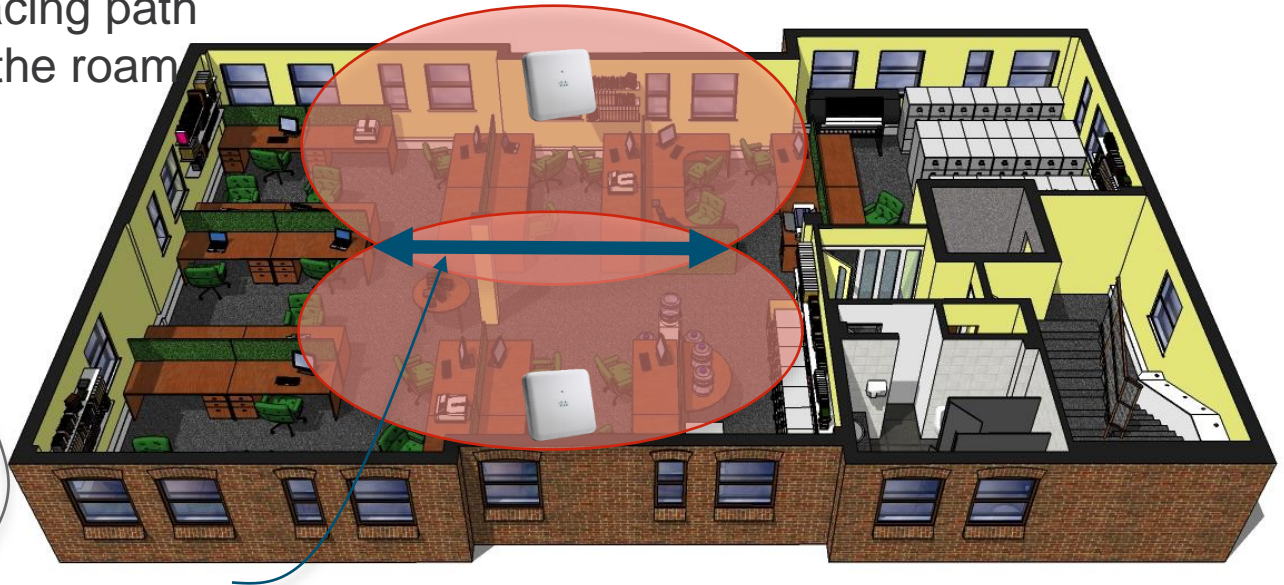
- At point A the phone is connected to AP 1
- At point B the phone has AP 2 in the neighbor list as it was able to scan it while moving down the hall
- At point C the phone needs to roam and successfully selects AP 2
- The phone has sufficient time to scan for AP 3 ahead of time

Avoid Ping Pong Zones

Ping Pong zone recipe:
Set overlap along pacing path
Let user head force the roam



Client stays here



“Pacing back and forth” zone

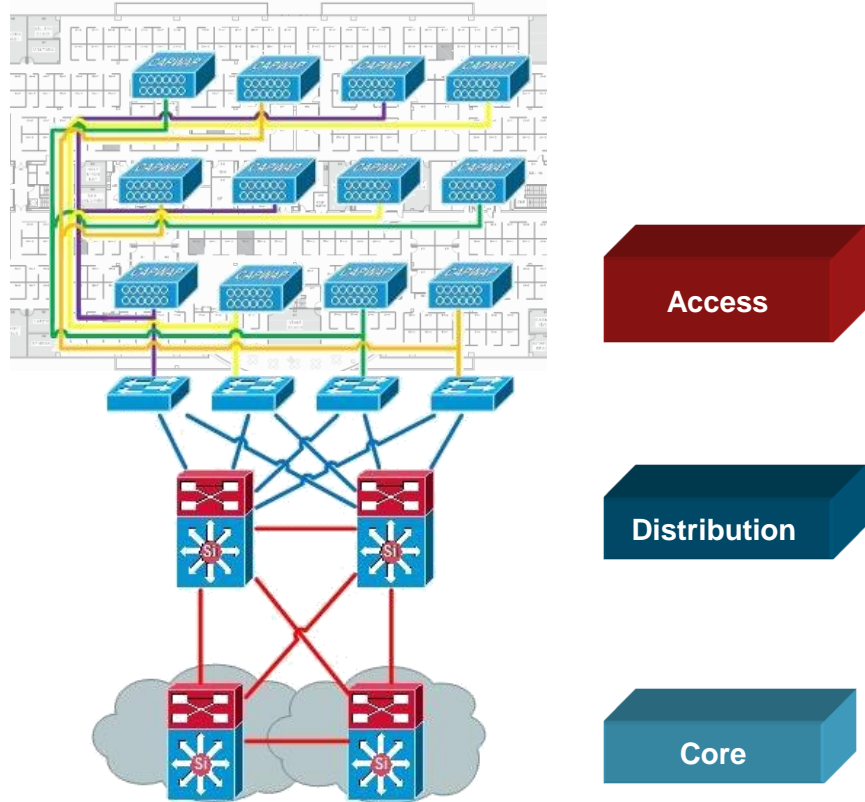
Next-Gen Office Design Goals

Always on, Always Ready

Network Resiliency

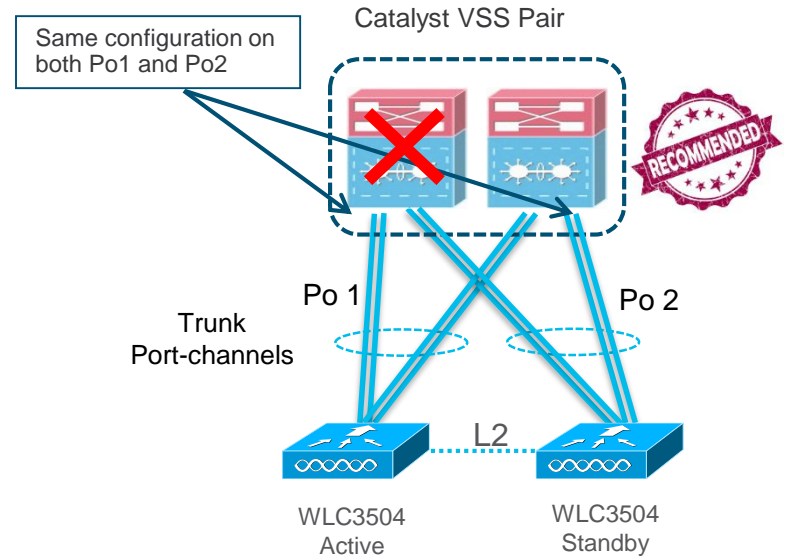
Highly Available Design

Create redundancy throughout the access layer by homing APs into different switches



High Availability SSO

A direct physical connection between Active and Standby Redundant Ports or Layer 2 connectivity is required to provide stateful redundancy within or across datacenters




Sub-second failover and zero SSID outage

Deployment Lifecycle

The Bigger Picture





Next-Gen Wireless Office Goal:


Easy Setup with Best Practices

WLAN Express Setup

w/ Best Practice Defaults

AVC Visibility
mDNS Snooping
New MDNS Profile for printer, http
Local Profiling
Band Select
DHCP Proxy
Secure Web access
Virtual IP 192.0.2.1
RRM-DCA Auto
RRM-TPC Auto
CleanAir Enabled
EDRRM Enabled
Channel Width 40 MHz
Aironet IE Disabled

Management over Wireless disabled
Load Balancing
Rogue Threshold Enabled
Client Exclusion Enabled
FastSSID Enabled
Infra MFP
Multicast Forwarding Mode
SNMPv3 (delete default)
Mobility Name
RF Group same as Mobility Name
DHCP Required on Guest WLAN
5 GHz Channel Bonding



Save Time & Money

- Optimum starting point at Day 0/1 network setup
- RF parameter setting ease of use
- Enhanced performance, security, resiliency with best practice recommendations turned

Checklist



Yes



No

Best Practices Audit

The screenshot displays the Cisco 2500 Series Wireless Controller interface. The left sidebar contains navigation options: Monitoring, Network Summary, Clients, Wireless Dashboard, and Best Practices. The main content area is titled 'BEST PRACTICES' and shows a 'Best Practice Score' of 31/31 and 'Ignored Best Practice 8'. The practices are organized into three categories: Infrastructure, Security, and RF Management. Each category lists several practices, all of which are marked as compliant with a blue checkmark icon.

BEST PRACTICES		Best Practice Score	31/31	Ignored Best Practice 8
INFRASTRUCTURE				
+ AVC Visibility			✓	
+ Band Select			✓	
+ Disable Aironet IE			✓	
+ More Optimizations...				
SECURITY				
+ Client Exclusion			✓	
+ Legacy IDS			✓	
+ Min Rogue RSSI Threshold			✓	
+ More Optimizations...				
RF MANAGEMENT				
+ Auto Coverage Hole Detection			✓	
+ Auto Dynamic Channel Assignment			✓	
+ Auto Transmit Power Control			✓	
+ More Optimizations...				

Best Practices Audit

The screenshot displays the Cisco 2500 Series Wireless Controller interface for a Best Practices Audit. The left sidebar contains navigation options: Monitoring, Network Summary, Access Points, Clients, Wireless Dashboard, AP Performance, Client Performance, and Best Practices. The main content area is titled 'BEST PRACTICES' and shows a 'Best Practice Score' section. It lists various best practices under categories: INFRA, SECURITY, and RF MANAGEMENT. A callout box titled 'Adding a Best Practice' points to a '+' icon, stating 'Clicking on an ignored best practice will re-add it.' Another callout box titled 'Add Ignored Best Practices' points to a '+' icon in the top right, stating 'A popup that displays the ignored best practices which can be re-added.' A third callout box titled 'Add Best Practice' points to a '+' icon in the top right, displaying a list of best practices: mDNS Gateway, Multicast Mobility, Multicast VLAN, 802.1x on AP, CPU ACLs, Local Management Password Policies, Peer To Peer, and User login policies. The 'User login policies' item is highlighted with a yellow box. The interface also shows a 'Practice 8' label and a '+' icon in the top right corner.

Monitoring

- Network Summary
- Access Points
- Clients
- Wireless Dashboard
- AP Performance
- Client Performance
- Best Practices

CISCO Cisco 2500 Series Wireless Controller

BEST PRACTICES Best Practice Score

INFRA

- Adding a Best Practice
- Clicking on an ignored best practice will re-add it.
- Disable Aironet IE
- More Optimizations...

SECURITY

- Client Exclusion
- Legacy IDS
- Min Rogue RSSI Threshold
- More Optimizations...

RF MANAGEMENT

- Auto Coverage Hole Detection
- Auto Dynamic Channel Assignment
- Auto Transmit Power Control
- More Optimizations...

Add Ignored Best Practices

A popup that displays the ignored best practices which can be re-added.

Add Best Practice

- mDNS Gateway
- Multicast Mobility
- Multicast VLAN
- 802.1x on AP
- CPU ACLs
- Local Management Password Policies
- Peer To Peer
- User login policies

Practice 8

Cisco and Apple Best Practices



APPLE DEVICES

- + WLAN Configuration
- + 5GHz Enabled
- + 5GHz Mandatory Rates
- + 5GHz EDCA Fastlane
- + 5GHz MCS Rates
- + QOS Trust DSCP
- + QOS Platinum Profile
- + mDNS or Bonjour
- + Optimized Roaming Disabled
- Less Optimizations...

http://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/technotes/8-3/Optimizing_WiFi_Connectivity_and_Prioritizing_Business_Apps.pdf
http://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/technotes/8-3/Enterprise_Best_Practices_for_Apple_Devices_on_Cisco_Wireless_LAN.pdf

Monitoring

Network Summary

Access Points

Clients

Rogues

Access Points

Auto Transmit Power Control

+ More Optimizations...

APPLE DEVICES

WLAN Configuration

None of the Active WLANs are compliant with Cisco Apple Best Practices

Benefits : Allows the user to identify if the WLAN is configured

Detailed Best Practices



WLAN Profile	Security	QoS	Advanced	Configuration
Demo-Mobility2	✗	✗	✗	Manual Configuration
	Security	QoS	Advanced	
	<ul style="list-style-type: none">✓ Fast Transition should be Enabled or Adaptive✓ FT PSK has to be enabled✓ FT 802.1X has to be enabled✓ Layer 3 Security has to be None✗ Over the DS has to be disabled	<ul style="list-style-type: none">✓ Fastlane should be enabled✓ QoS has to be Platinum (Voice)✓ AVC Profile has to be enabled and AUTOQOS-AVCPROFILE applied✗ WMM Policy should be required	<ul style="list-style-type: none">✓ 11k Neighbor List or Dual Band should be enabled✓ 11v BSS Transition should be enabled✓ WLAN Radio Policy has to be ALL or 802.11a or 802.11a/g✗ mDNS Snooping should be enabled	

ISE RADIUS



Monitoring

Network Summary

Access Points

Clients

Rogues

Access Points

+ Auto Dynamic Channel Assignment

+ Auto Transmit Power Control

+ More Optimizations...

APPLE DEVICES

+ WLAN Configuration

+ 5GHz Enabled

Detailed Best Practices



WLAN Profile



Security

Advanced

Configuration



Demo-Mobility2



Manual Configuration

Security

Advanced

- ✓ Interim Update in AAA Server should be enabled
- ✓ Interim Interval in AAA Server should be 0 Second

- ✓ Session Timeout should be enabled
- ✗ Session Timeout should be greater than or equal to 7200 Seconds
- ✗ Client Exclusion has to be enabled
- ✗ Client Exclusion value has to be set to 180 Seconds
- ✗ Client user idle timeout should be enabled
- ✗ Client user idle timeout should not be greater than 3600 Seconds



10

items per page

Access Point Provisioning with PnP

PID	Serial #	Hostname	WLC IP address	AP Mode	Flex Group name
AIR-CAP3702I-A-K9		AP-Store1-1	192.168.15.1	FlexConnect	FlexGrp1



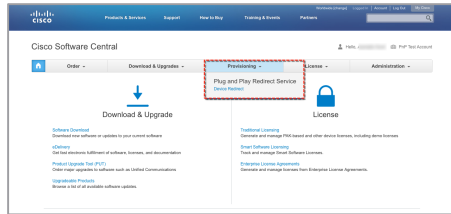
PnP Server



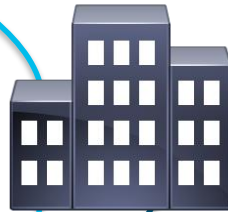
Day 0

Network Admin

Network Admin pre provisions APs in PnP server.



Cisco Public Cloud



WLC IP (Prim/Sec/Ter)
AP Name
AP Mode (Flex)
AP Group Name
Flex Group Name



Installer

- Places AP in appropriate Group
- Apply relevant configs to AP

- Mount and cable devices
- Power-on

* Resources required for PnP:
64 Gb RAM, 500 Gb Storage
Scale: 10,000 devices

Deployment Lifecycle

The Bigger Picture




Next-Gen Wireless Office Goal:

Self-Optimizing RF Network



RF Optimized Connectivity

- Enabled by Dual 5GHz
- Adjust Radio Bands to Better Serve the Environment


5GHz
Serving




5.24GHz
Serving

Self-Optimizing RF network



XOR Radio
FRA



Client Link 4.0



Optimized Roaming
RX-SOP



RRM, DCA, TPC, CHDM



Event Driven
RRM



Off-Channel
Scanning




Cisco CleanAir®



HDX Turbo
Performance




Load Balancing
Band Select

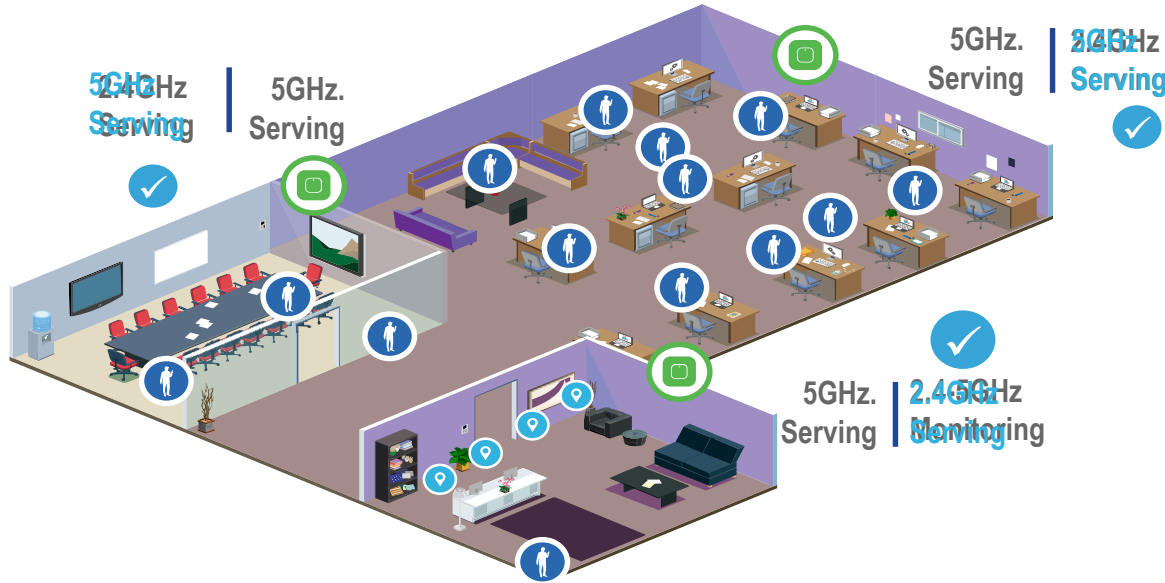


Flex DFS
DBS



RF Profiles

XOR Radio and FRA



- ✓ FRA-auto (default value) or Manual
- ✓ Auto 2.4 -> 5GHz or Monitor Mode
- ✓ Transition to 2.4 GHz if coverage drops

AP Name	Radio Slot#	Base Radio MAC	Coverage Overlap Factor	Suggested Mode	Operational Status	Load Profile	Radio Role	Noise Profile	Interference Profile	Coverage Profile	CleanAir Admin Status
802.11a/n/ac 802.11b/g/n Cisco CleanAir											
Statistics											
CDP											
Rogues											
Clients											
Sleeping Clients											

Radio Role Assignment

Auto Manual

Client Serving Monitor

Band: 2.4 GHz

RF Channel Assignment

Current Channel: 1 *
 Channel Width: 20 MHz
 Assignment Method: Global
 Custom

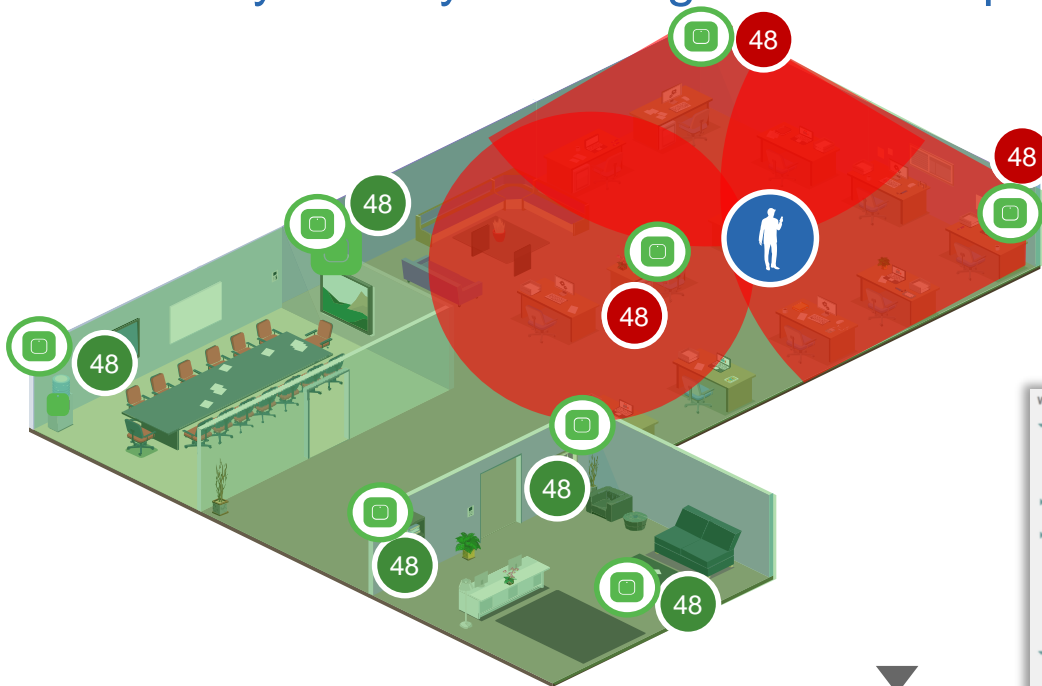
Tx Power Level Assignment

Current Tx Power Level: 1
 Assignment Method: Global
 Custom



Optimize Wi-Fi with CleanAir

Quickly Identify and Mitigate Wi-Fi Impacting Interference



- ✓ Interference on 20/40/80/160 MHz
- ✓ Air Quality and Interference by AP/radio on WLC
- ✓ AQ Threshold trap and Interference Device trap (per radio)
- ✓ CleanAir-enabled RRM



Channel 48

BRKEWN-2670

Network Air Quality and Interference Location with PI 3.1.x and MSE 8.0.

The screenshot shows the configuration for CleanAir and Event Driven RRM. The CleanAir Parameters section includes:

- CleanAir: Enabled
- Report Interferers: Enabled
- Persistent Device Propagation: Enabled

The Interferences to Detect section includes:

- TDD Transmitter
- Jammer
- Continuous Transmitter
- Video Camera

The Trap Configurations section includes:

- Enable AQI(Air Quality Index) Trap:
- AQI Alarm Threshold (1 to 100):
- Enable trap for Unclassified Interference:
- Threshold for Unclassified category trap:
- Enable Interference For Security Alarm:

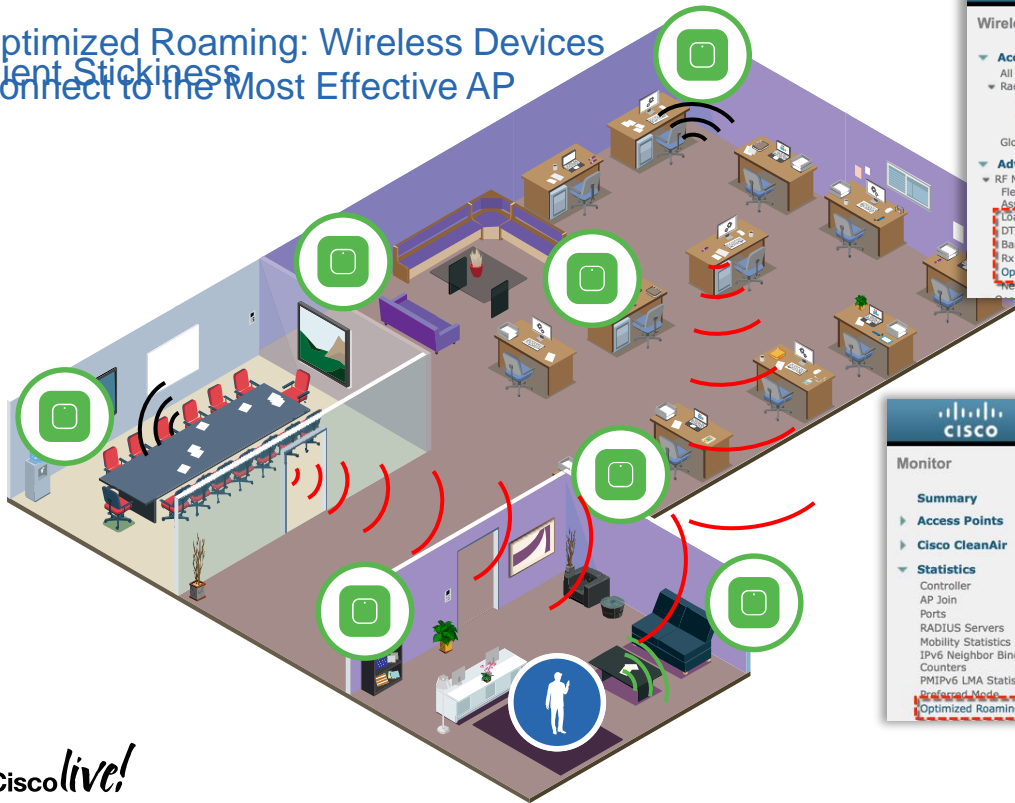
The Event Driven RRM section includes:

- EDRRM: Enabled
- Sensitivity Threshold:
- Rogue Contribution: Enabled
- Rogue Duty-Cycle:

Better Support for Users on the Move

Optimized Roaming

Optimized Roaming: Wireless Devices
Client Stickiness
Connect to the Most Effective AP



Wireless

- Access Points
 - All APs
 - Radios
 - 802.11a/n/ac
 - 802.11b/g/n
 - Dual-Band Radios
 - Global Configuration
- Advanced
 - RF Management
 - Flexible Radio Assignment
 - Load Balancing
 - DTLS
 - Band Select
 - Rx Sop Threshold
 - Optimized Roaming

Optimized Roaming

802.11a

- Optimized Roaming Mode: Enable
- Optimized Roaming Interval: 90 sec
- Optimized Roaming Data Rate Threshold: Disable

802.11b

- Optimized Roaming Mode: Disable

1. CHDM configuration can be done in Wireless--> RF Profile
2. Disable 802.11a / 802.11b network before changing Opti...

Monitor

- Summary
- Access Points
- Cisco CleanAir
- Statistics
 - Controller
 - AP Join
 - Ports
 - RADIUS Servers
 - Mobility Statistics
 - IPv6 Neighbor Bind
 - Counters
 - PMIPv6 LMA Statistics
 - Preferred Mode
 - Optimized Roaming

Optimized Roaming Statistics

802.11a Optimized Roaming Stats

- Optimized Roaming Disassociations: 0
- Optimized Roaming Rejections: 0

802.11b Optimized Roaming Stats

- Optimized Roaming Disassociations: 0
- Optimized Roaming Rejections: 0

CISCO

MONITOR WLANs CONTROLLER WIRELESS SECURITY

802.11a > RRM > Coverage

General


- Enable Coverage Hole Detection:

Coverage Threshold

- Data RSSI (-40 to -90 dBm): -75
- Voice RSSI (-40 to -90 dBm): 0
- Mesh
 - Min Packet Count per AP (1 to 200): 0
- ATF
 - Coverage exception level per AP (0 to 100 %): 25
- RF Profiles
 - FlexConnect Groups
 - FlexConnect ACLs: 50
 - FlexConnect VLAN Templates: 50
 - OEAP ACLs
 - Data Packet Count (1 to 255 packets): 100
 - Voice Packet Percentage (1 to 100 %): 50
 - Data Packet Percentage (1 to 100 %): 50

Better Client Connectivity

RXSOP, Load Balancing, Band Select



Wireless

- Access Points
 - All APs
 - Radios
 - 802.11a/n/ac
 - 802.11b/g/n
 - Dual-Band Radios
 - Global Configuration
- Advanced
 - RF Management
 - Flexible Radio Assignment
 - Load Balancing
 - DTLS
 - Band Select
 - Rx Sop Threshold
 - Optimized Roaming
 - Network Profile

Band Select ✓

Probe Cycle Count	2
Scan Cycle Period Threshold (1-1000 milliseconds)	200
Age Out Suppression (10-200 seconds)	20
Age Out Dual Band (10-300 seconds)	60
Acceptable Client RSSI (dBm)	-80
Acceptable Client Mid RSSI (dBm)	-80


* Band Select is configurable per WLAN.

Challenge

- Dual-Band clients persistently connect to 2.4 GHz
- 2.4GHz may have 802.11b/g clients causing contention
- 2.4GHz is prone to interference

Solution

- BandSelect directs clients to 5 GHz optimizing RF usage
- Better usage of the higher capacity 5GHz band
- Frees up 2.4 GHz for single band clients



Optimized RF Utilization by Moving 5 GHz Capable Client Out of the Congested 2.4 GHz Channels

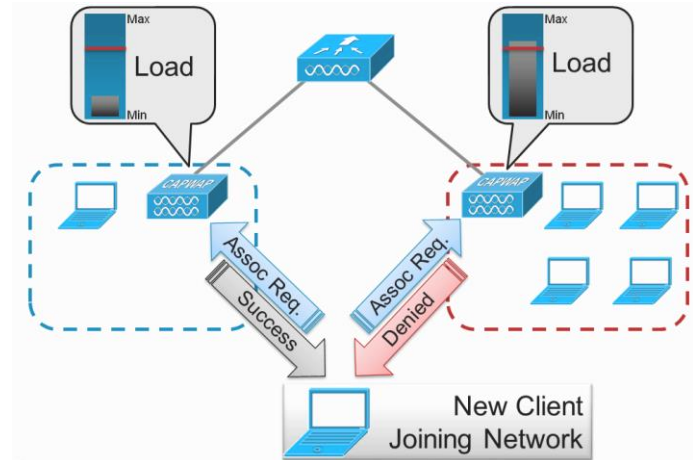
Load Balancing ✓

Client Window Size	5
Maximum Denial Count	3

Load Balancing Statistics

Total Denied Client Count	0
Total Denial Message Sent	0
Exceeded Denial Max Limit Count	0
None 5G Candidate Count	0
None 2.4G Candidate Count	0

* Load Balancing is configurable per WLAN.



Fine-tuning HDX with RF Profiles

- ✓ Pre-canned RF Profiles
- ✓ Client Distribution
- ✓ Data Rates
- ✓ DCA, TPC, CHDM
- ✓ Profile Threshold for Traps
- ✓ High Density Features

Wireless

Access Points

Radios

- 802.11a/n/ac
- 802.11b/g/n
- Dual-Band Radios

Global Configuration

Advanced

- Load Balancing
- Band Select
- Preferred Calls
- SIP Snooping
- Rx Sop Threshold

RF Profile > Edit 'HD_2_4'

RF Profile

Enable Out Of Box

Enable Persistence

Profile Name	Radio Policy	Applied
High-Client-Density-(802.11a)	802.11a	No <input checked="" type="checkbox"/>
High-Client-Density-(802.11bg)	802.11b/g	No <input checked="" type="checkbox"/>
Low-Client-Density-(802.11a)	802.11a	No <input checked="" type="checkbox"/>
Client-Density(802.11bg)	802.11b/g	No <input checked="" type="checkbox"/>
Client-Density(802.11a)	802.11a	No <input checked="" type="checkbox"/>

RF Profile > Edit 'test_bb'

General 802.11 RRM High Density Client Distribution

Maximum Power Level Assignment (-10 to 30 dBm) 30

Minimum Power Level Assignment (-10 to 30 dBm) -10

Power Threshold v1(-60 to -50 dBm) -70

Power Threshold v2(-60 to -50 dBm) -67

DCA

Avoid AP Foreign AP Interference Enabled

DCA Channel List

DCA Channels

Select Channel

1

2

3

4

RF Profile > Edit '802.11a_demo'

General 802.11 RRM High Density Client Distribution

High Density Parameters

Maximum Clients(1 to 200) 200

Client Trap Threshold 50

Rx Sop Threshold Parameters

Rx Sop Threshold Auto

Multicast Parameters

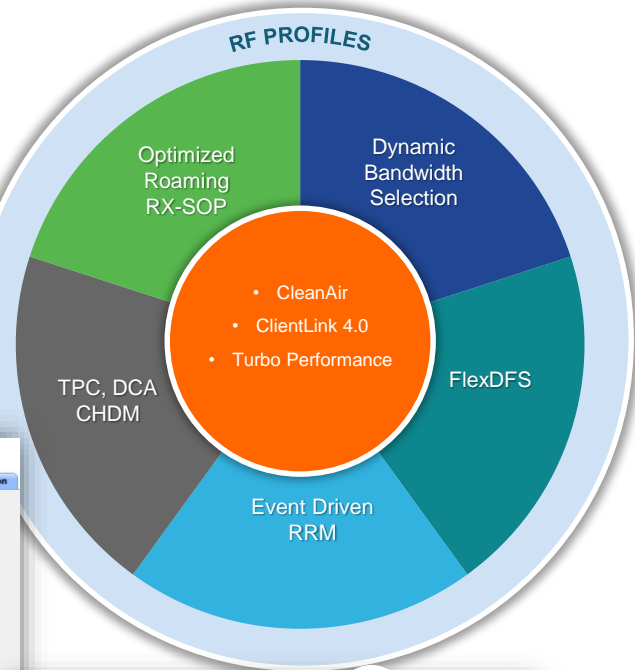
Multicast Data Rates 2 auto

RF Profile > Edit 'CiscoLive_Keynote'

General 802.11 RRM High Density Client Distribution

Data Rates

6 Mbps	Disabled	0	<input checked="" type="checkbox"/> Supported
9 Mbps	Disabled	1	<input checked="" type="checkbox"/> Supported
12 Mbps	Supported	2	<input checked="" type="checkbox"/> Supported
18 Mbps	Supported	3	<input checked="" type="checkbox"/> Supported
24 Mbps	Mandatory	4	<input checked="" type="checkbox"/> Supported
36 Mbps	Mandatory	5	<input checked="" type="checkbox"/> Supported
48 Mbps	Supported	6	<input checked="" type="checkbox"/> Supported
54 Mbps	Supported	7	<input checked="" type="checkbox"/> Supported
		8	<input checked="" type="checkbox"/> Supported
		9	<input checked="" type="checkbox"/> Supported
		10	<input checked="" type="checkbox"/> Supported
		11	<input checked="" type="checkbox"/> Supported
		12	<input checked="" type="checkbox"/> Supported
		13	<input checked="" type="checkbox"/> Supported
		14	<input checked="" type="checkbox"/> Supported
		15	<input checked="" type="checkbox"/> Supported
		16	<input checked="" type="checkbox"/> Supported
		17	<input checked="" type="checkbox"/> Supported



RF Profile > Edit 'CiscoLive_Keynote'

General 802.11 RRM High Density Client Distribution

Load Balancing

Window(0 to 20 Clients) 5

Denial(1 to 10) 3

RF & RRM: Disable lower .11b Data Rates, Limit SSIDs

Wireless → 802.11b/g/n → Network

802.11b/g Global Parameters

General

- 802.11b/g Network Status: Enabled
- 802.11g Support: Enabled
- Beacon Period (milliseconds):
- Short Preamble: Enabled
- Fragmentation Threshold (bytes):
- DTPC Support: Enabled
- Maximum Allowed Clients:
- RSSI Low Check: Enabled
- RSSI Threshold (-60 to -90 dBm):

CCX Location Measurement

Mode: Enabled

Data Rates**

1 Mbps	Disabled
2 Mbps	Disabled
5.5 Mbps	Disabled
6 Mbps	Disabled
9 Mbps	Supported
11 Mbps	Disabled
12 Mbps	Mandatory
18 Mbps	Supported
24 Mbps	Supported
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	Supported

** Data Rate 'Mandatory' implies that clients who do not support that specific rate will not be able to associate. Data Rate 'Supported' implies that any associated client that also supports that same rate may communicate with the AP using that rate. But it is not required that a client be able to use the rates marked supported in order to associate. The actual data rates that are supported depend on the channel selected as different channels may have different bandwidths. The reason is that we show data rates and allow the user to select the data rates. But in reality, the AP will pick the next lower data rate allowed for that channel if the chosen data rate is not supported.

Each SSID needs a separate probe response and beaconing, the more SSIDs the less RF space available for real data traffic

Management frames sent at lowest mandatory rate - slows down the entire cell

RF design recommendations

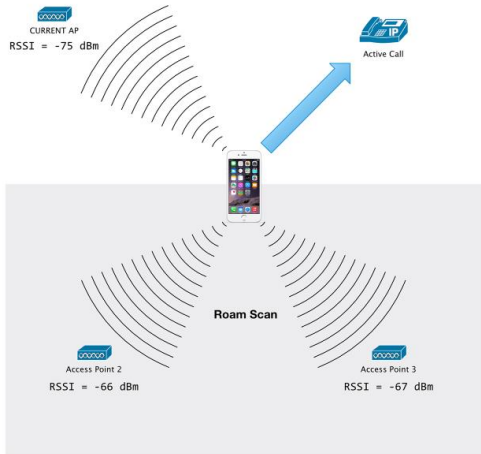


Image courtesy: <https://support.apple.com/en-us/HT203068>

- Channel Utilization < 40%.
- Client SNR \geq 25 dB.
- 802.11 retransmissions < 15%
- Packet Loss < 1%
- Jitter < 100 ms.



Apple client device should observe a minimum of 2 APs with an RSSI measurement of -67 dBm

Standard Density Data Rates

Wireless > 802.11a/n/ac > Network

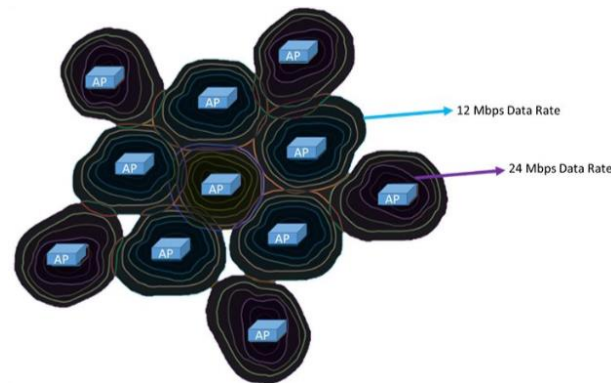
- Channel Utilization < 40%.
- Client SNR >= 25 dB.
- 802.11 retransmissions < 15%
- Packet Loss < 1%
- Jitter < 100 ms.

802.11a Global Parameters	
General	
802.11a Network Status	<input checked="" type="checkbox"/> Enabled
Beacon Period (milliseconds)	100
Fragmentation Threshold (bytes)	2346
DTPC Support.	<input type="checkbox"/> Enabled
Maximum Allowed Clients	200
RSSI Low Check	<input type="checkbox"/> Enabled
RSSI Threshold (-60 to -90 dBm)	-80
802.11a Band Status	
Low Band	Enabled
Mid Band	Enabled
High Band	Enabled

Data Rates**	
6 Mbps	Disabled
9 Mbps	Disabled
12 Mbps	Mandatory
18 Mbps	Supported
24 Mbps	Mandatory
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	Supported

CCX Location Measurement
Mode Enabled

** Data Rate 'Mandatory' implies that clients who do not support that specific rate will not be able to associate. Data Rate 'Supported' implies

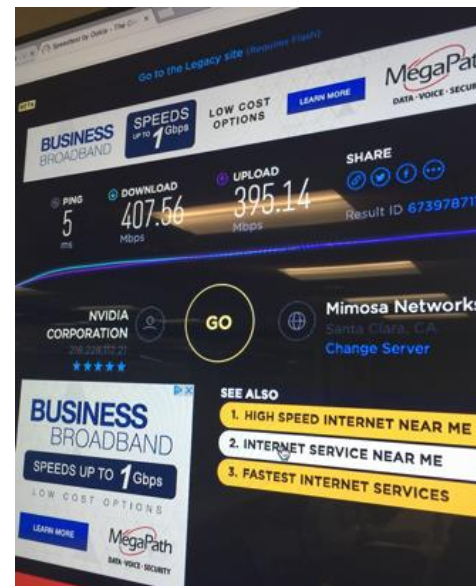
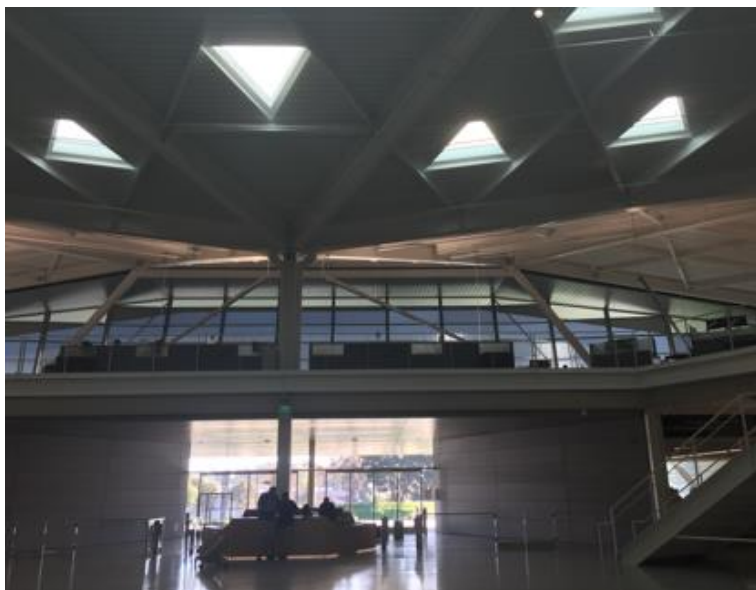


- Cisco highly recommends leaving all MCS rates enabled

Minimum data rate of 12Mbps and 24 Mbps as the mandatory rates 6 Mbps as the lowest mandatory rate, if coverage marginal

Endeavour @NVIDIA, Santa Clara

- 4K Video @100 Mbps, all day every day



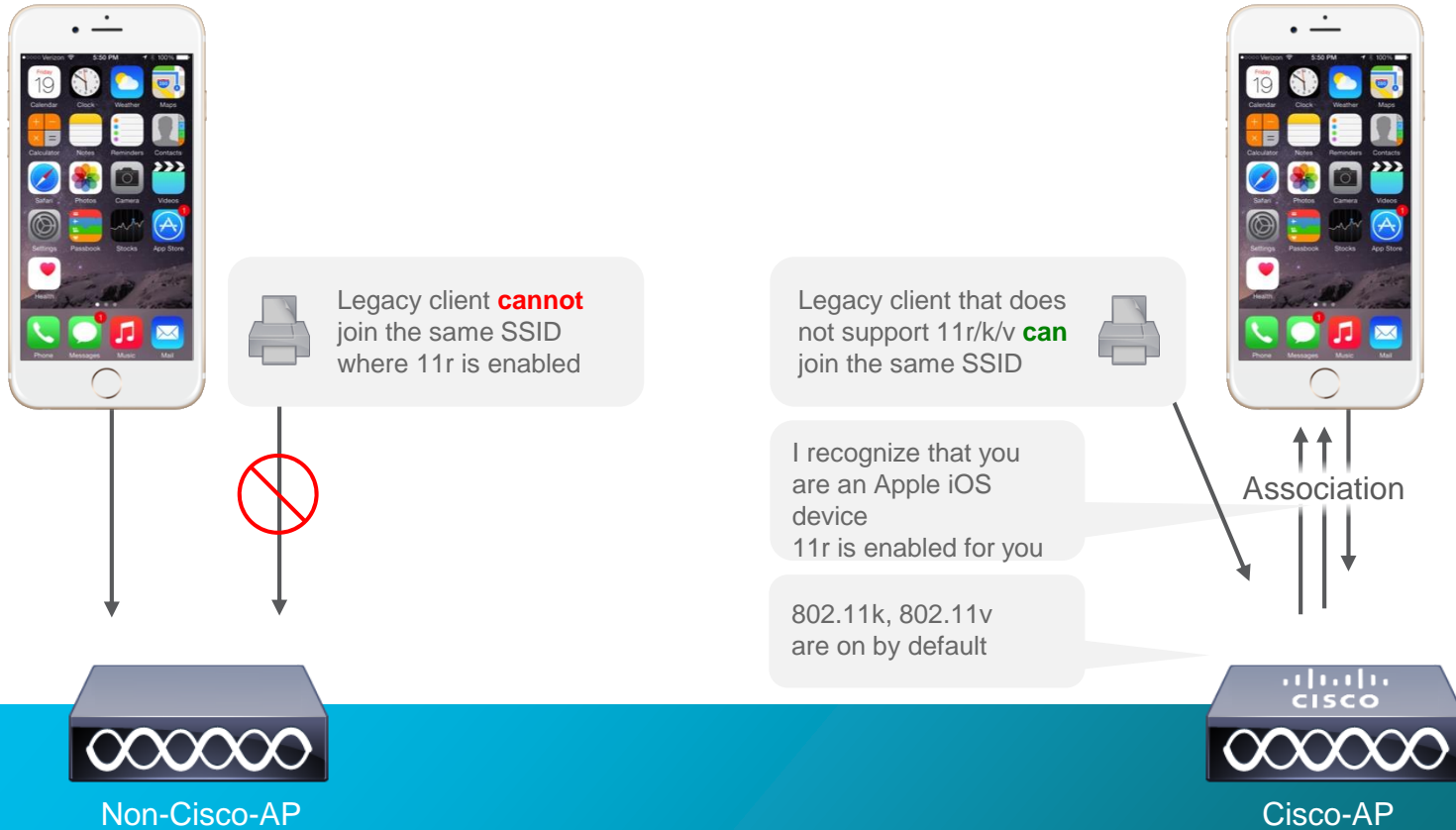
- 560 AP3800s across 500,000 sq feet
- 2 WLC8540s in HA
- All APs connect to CAT 4500 series switches with mGig and UPOE

Live speed test in one of the conference rooms during our visit DL: 407Mbps, UL: 395Mbps

Next-Gen Wireless Office Goal:

Seamless connectivity

Cisco and Apple Optimized Roaming



Adaptive 11r/k/v

Features enabled by default on a newly created SSID

WLANs > Edit 'WHOPPERWIFI'

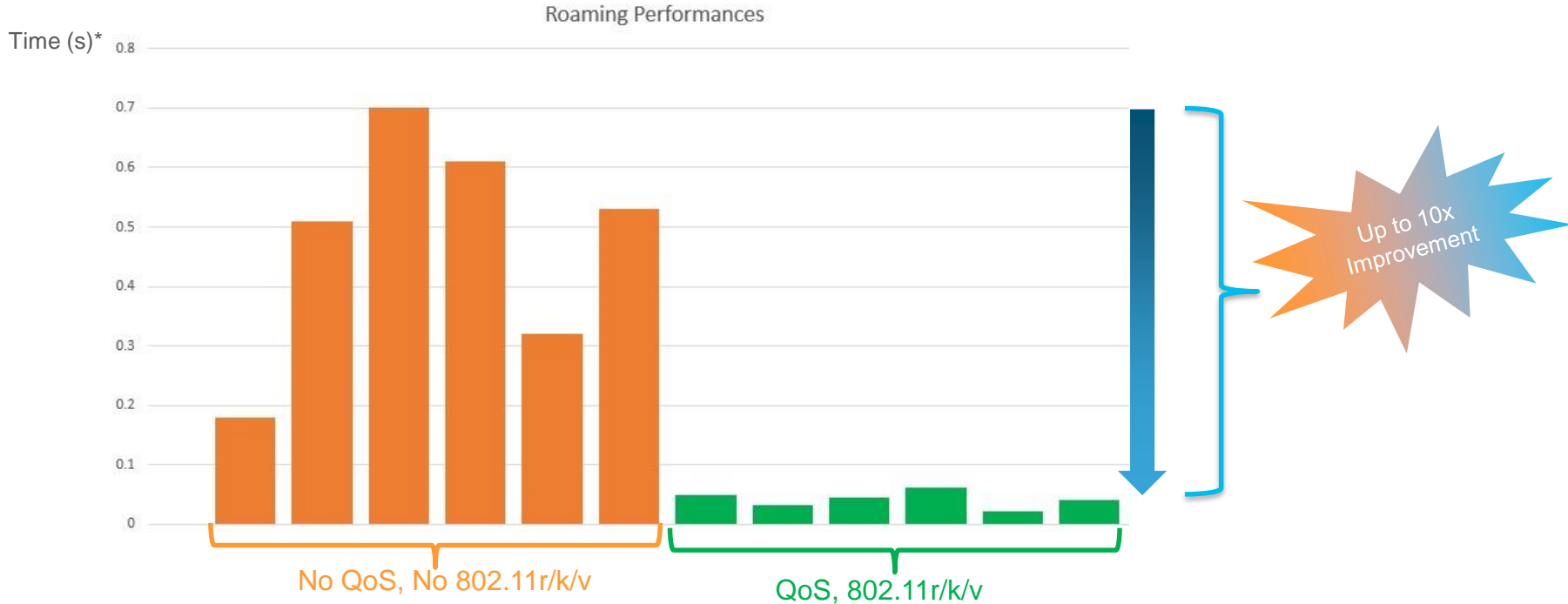
The screenshot shows the configuration page for a WLAN. The 'General' tab is selected. Under 'Layer 2 Security', 'WPA+WPA2' is selected. 'Fast Transition' is set to 'Adaptive'. A callout box highlights the 'Adaptive' option in the dropdown menu. 'Protected Management Frame' is set to 'Disabled'. Under 'WPA+WPA2 Parameters', 'WPA2 Policy' and 'WPA2 Encryption' (AES) are checked.

This screenshot shows the 'Advanced' tab of the configuration page. The '11k' section has 'Assisted Roaming Prediction Optimization', 'Neighbor List', and 'Neighbor List Dual Band' checked. The '11v BSS Transition Support' section has 'BSS Transition', 'BSS Max Idle Service', and 'Directed Multicast Service' checked.

This screenshot is similar to the previous one but highlights the '11v BSS Transition Support' section with a red box, showing that 'BSS Transition', 'BSS Max Idle Service', and 'Directed Multicast Service' are all checked.

Roaming Performance :

10x Better end-user Browsing and App Experience



*Time Interval between last packet on previous AP, and first packet on next AP



Next-Gen Wireless Office Goal:

Prioritize business-critical Apps

Fast Lane enables network administrator to prioritize applications per your environment

Supports Fast lane

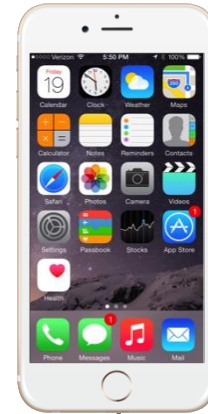


Admin can provision Apple IOS device with a QoS profile*
Applications in whitelist get QoS marking**
Other applications get BE/BK

My profile for this environment:
Webex = Realtime-interactive
Viber = BE

My profile for this environment:
Webex = BE
Viber = Voice

Supports Fast lane



Supports Fast lane



Cisco-AP

Supports Fast lane



Cisco-AP

Fast Lane

- Enabling Fast Lane:
- Sets the WLAN for Platinum
- Sets WMM to Required
- Platinum profile sets Max Priority to voice (UP 6), non-WMM and multicast to BE, 802.1p disabled, bandwidth contracts disabled
- EDCA profile is set to Fast Lane

WLANs > Edit 'WHOPPERWIFI'

General **Security** **QoS** **Policy-Mapping** **Advanced**

Quality of Service (QoS)

Application Visibility Enabled

AVC Profile

Flex AVC Profile

Netflow Monitor

Fastlane

Override Per-User Bandwidth Contracts (kbps) ¹⁶

	DownStream	UpStream
Average Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Average Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>

Override Per-SSID Bandwidth Contracts (kbps) ¹⁶

General

EDCA Profile

Enable Low Latency MAC ⁴

Edit QoS Profile

QoS Profile Name platinum

Description

Per-User Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Average Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>

Per-SSID Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Average Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>

WLAN QoS Parameters

Maximum Priority

Unicast Default Priority

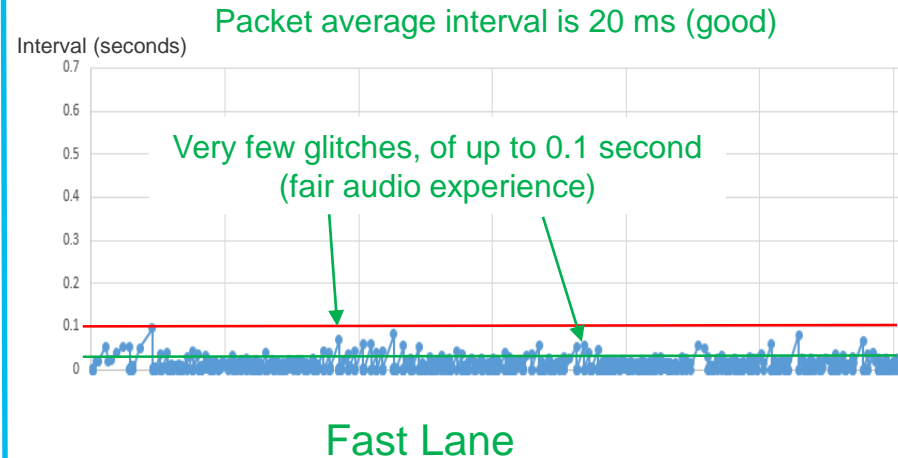
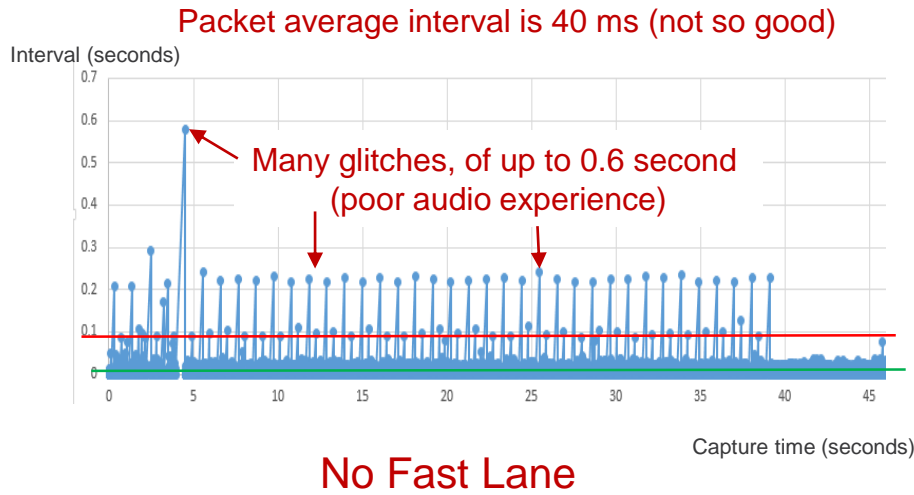
Multicast Default Priority

Wired QoS Protocol

Protocol Type

Fast Lane delivers a reliable voice experience even in a congested environment

- In a congested environment, one voice packet is sent every 20 ms
- We measure the actual interval between voice packets in the upstream direction



Cisco Apple Analytics Release 8.5

Cisco Apple Wireless Features Journey

AireOS 8.3, 8.3 MR1
iOS 10.0+

Phase 1

Roaming Optimizations

- **Adaptive 802.11r:** Fast Transition is enabled automatically for iOS 10 clients
- **Auto 802.11k/v:** 11k/v are enabled by default and optimized to provide 'best next AP'

Cisco Apple Phase 2 : iOS Analytics

1. Beacon Reporting to the Access Point by iOS Client
2. Enhanced Dis-Association Reason to the Access Point by iOS Client
3. iOS Version information to the Access Point by iOS Client

[Video demo : https://youtu.be/1XCqV0Pux_s](https://youtu.be/1XCqV0Pux_s)

How does the client see the Network

How does the client see the network ?

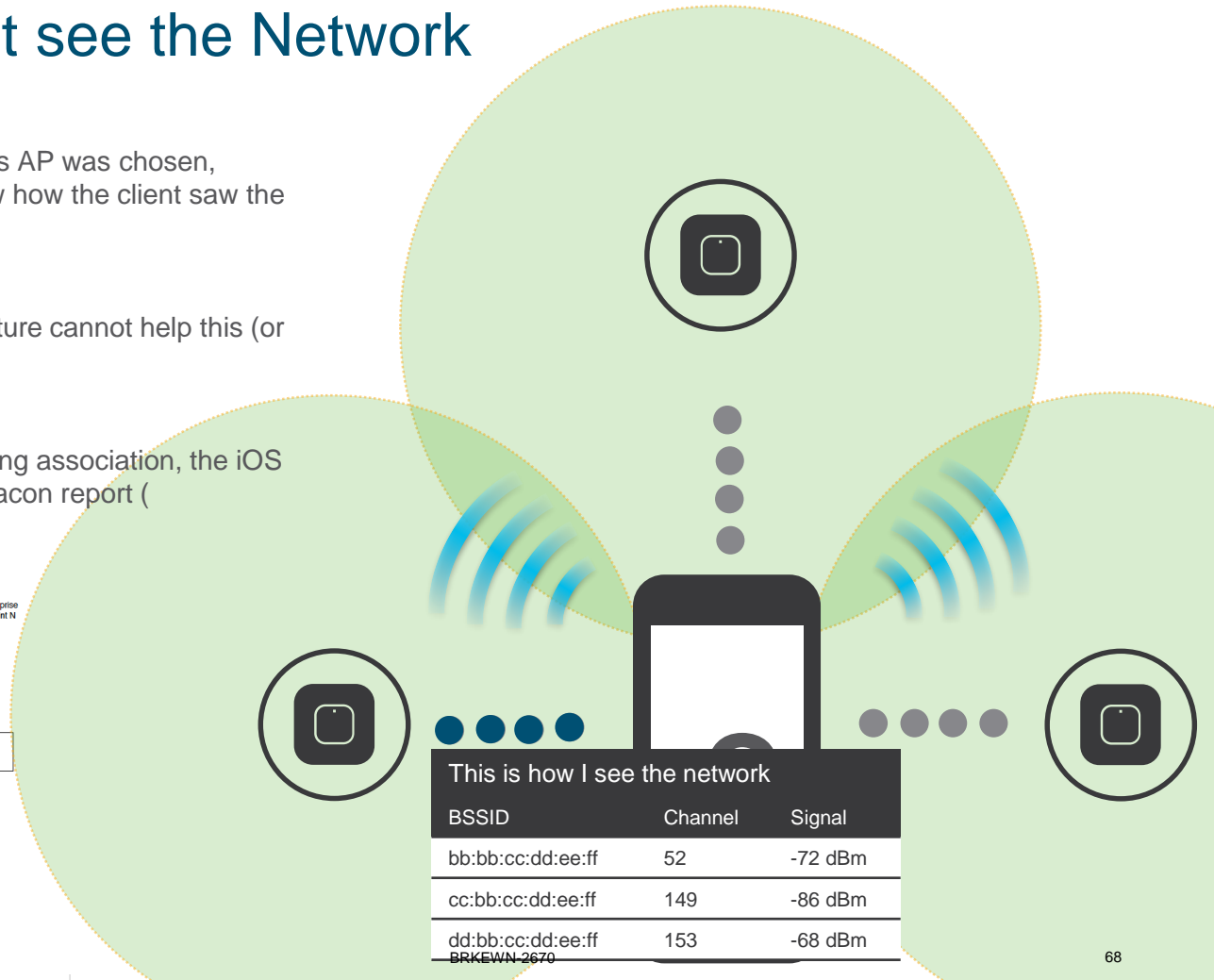
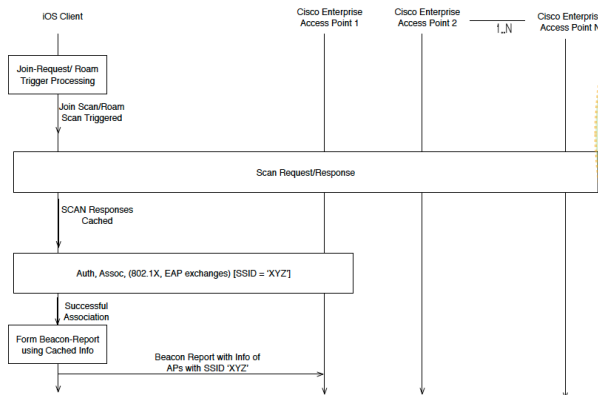
The infrastructure does not know why this AP was chosen, because the infrastructure does not know how the client saw the network

Why is this a problem?

Because without that view, the infrastructure cannot help this (or other) client find the “best AP”

How do Cisco and Apple solve this?

Right after successful key-exchange during association, the iOS 11 device sends to its AP an 802.11k beacon report (Unsolicited mode)



Where can I see this Scan report on WLC ?

Client detail page in the controller UI as Client Scan Report

How can we use this neighbor map ?

- To draw a super-accurate RF map of the floor, and help other clients roam
- When a new client enters the cell, and asks for a neighbor map, we can tailor the map to this client location!
- When another client needs to roam, we can suggest the best AP, seen from where the client sits!

The screenshot shows the 'CLIENT VIEW' page for an iPhone7 client. The 'GENERAL' section displays client details: User Name (Unknown), Host Name (iPhoneSeven), MAC Address (d4:61:9d:9a:af:a0), SSID (11reapt), AP Name (11reapt_1 (Ch 52)), Nearest APs (corisco_1 (-62 dBm), 3700(-70 dBm)), Device Type (iPhone7,1), OS Version (11.0), Previous AP (58:ac:78:df:84:28), Last Disassociation Reason (User triggered disassociation), Performance (Signal Strength: -60 dBm, Signal Quality: 25 dB, Connection Speed: 400 Mbps, Channel Width: 40 MHz), Capabilities (802.11ac (5GHz) Spatial Stream: 2), Cisco Compatible (Not Supported), and Connection Score (85%). The 'CONNECTIVITY' section shows a flow from Start to Association to Authentication to DHCP to Online. The 'TOP APPLICATIONS' section lists: ping (88.9 KB), apple-services (331.3 KB), dns (95.6 KB), icmp (59.4 KB), icloud (42.2 KB), iTunes (14.9 KB), alt-web-services (12.8 KB), and ntp (10.9 KB). The 'CLIENT SCAN REPORT' table is shown below.

Mac Address	RSSI	Channel
58:ac:78:df:84:22	-50	54
d8:b1:90:4a:51:a2	-60	38
a0:ec:f9:6d:17:82	-54	38
a0:ec:f9:6d:17:86	-64	11
58:ac:78:df:84:28	-42	1

This is how I see the network

BSSID	Channel	Signal
bb:bb:cc:dd:ee:ff	52	-72 dBm
cc:bb:cc:dd:ee:ff	149	-86 dBm
dd:bb:cc:dd:ee:ff	153	-68 dBm

How does the Network see the device

How does the network see the device ?

Usually as an iPad or iPhone with DHCP and HTTP Device profiling

When is this not enough?

When we need to analyze device model and OS specific behaviors in the network

How do Cisco and Apple solve this?

After association, the iOS 11 client also tells us about itself. We can correlate platform, OS to behavior at different points of time and space

Where can I see this on WLC ?

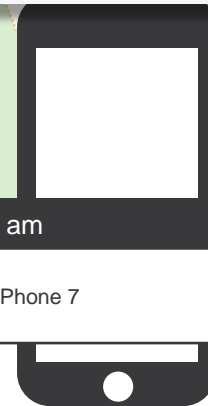
Client summary and client detail page

The screenshot shows the Cisco 5500 Series Wireless Controller interface. The main section is titled 'CLIENT VIEW' and contains a 'GENERAL' tab. The client information is as follows:

- User Name: Unknown
- Host Name: iPhoneSeven
- MAC Address: d4:61:9d:9a:af:e0
- Uptime: Associated since 1 Minute 47 Seconds
- SSID: 11radapt
- AP Name: User_1 (Ch 52)
- Nearest APs: corsica_1(-62 dBm), corsica_70(-68 dBm)
- Device Type: iPhone9,1
- OS Version: 11.0
- Previous AP: 58:ac:78:df:84:20
- Last disassociation reason: User triggered disassociation
- Performance: Signal Strength: -50 dBm, Signal Quality: 25 dB, Connection Speed: 400 Mbps, Channel Width: 40 MHz
- Capabilities: 802.11ac (5GHz) Spatial Stream: 2
- Cisco Compatible: Not Supported
- Connection Score: 55%

On the right side, there is a 'CONNECTIVITY' diagram showing a sequence of steps: Start, Association, Authentication, DHCP, and Online. Below that is a 'TOP APPLICATIONS' table:

Name	Usage
1 ping	88.9 KB
2 apple-services	331.3 KB
3 dns	95.6 KB
4 icmp	59.4 KB
5 loaded	42.2 KB
6 itunes	14.9 KB
7 att-web-services	12.8 KB
8 ntp	19.9 KB



This is who I am

I am iOS 11.0, iPhone 7

Why did the Client go away ?

Do we know why client disassociated ?

When a client roams or disconnects, it sends a disassociation message. The AP does not always know why... bad signal? Something else?

Why is this a problem?

Without knowing why a client is gone, we cannot help other clients in the same location (is this location okay? Is there a better AP there? Is there incompatibility in config at this location?)

How do Cisco and Apple solve this?

The Apple device sends a proprietary reason code

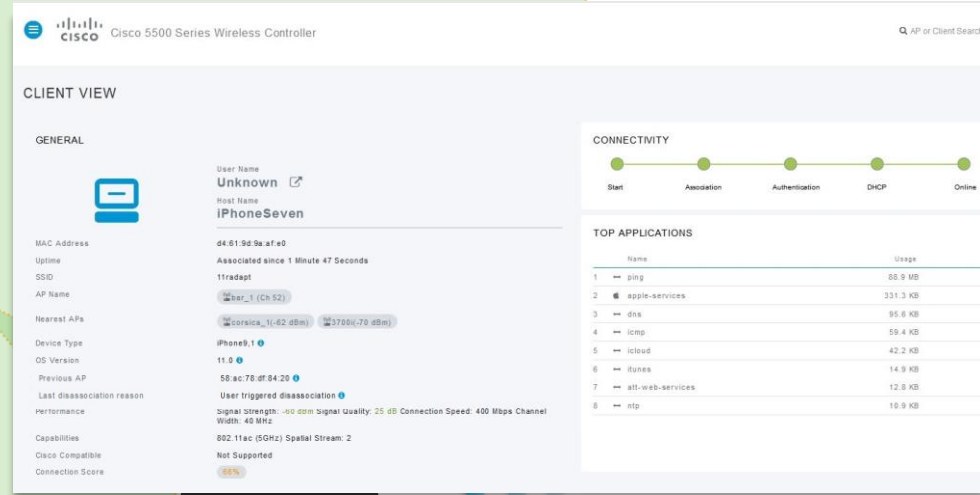


Why did the Client go away ?

Where can I see this Reason code on WLC ?
Client detail page in the controller UI

How can we use this Reason Code ?

- Help other clients in the same location if there is an RF issue
- Collect data to understand patterns (where clients go, etc)



The screenshot shows the Cisco 5500 Series Wireless Controller interface. The main section is titled "CLIENT VIEW" and is divided into "GENERAL" and "CONNECTIVITY" tabs. The "GENERAL" tab is active, displaying the following information:

- User Name:** Unknown
- Host Name:** iPhoneSeven
- MAC Address:** d4:61:9d:9a:af:e0
- Uptime:** Associated since 1 Minute 47 Seconds
- SSID:** 11radapt
- AP Name:** cor_1 (Ch 52)
- Nearest APs:** cor_1 (-62 dBm), 3706 (-70 dBm)
- Device Type:** iPhone9,1
- OS Version:** 11.0
- Previous AP:** 58:ac:78:0f:04:29
- Last disassociation reason:** User triggered disassociation
- Performance:** Signal strength: -60 dBm, Signal Quality: 25 dB, Connection Speed: 400 Mbps, Channel Width: 40 MHz
- Capabilities:** 802.11ac (5GHz) Spatial Stream: 2
- Cisco Compatible:** Not Supported
- Connection Score:** 85%

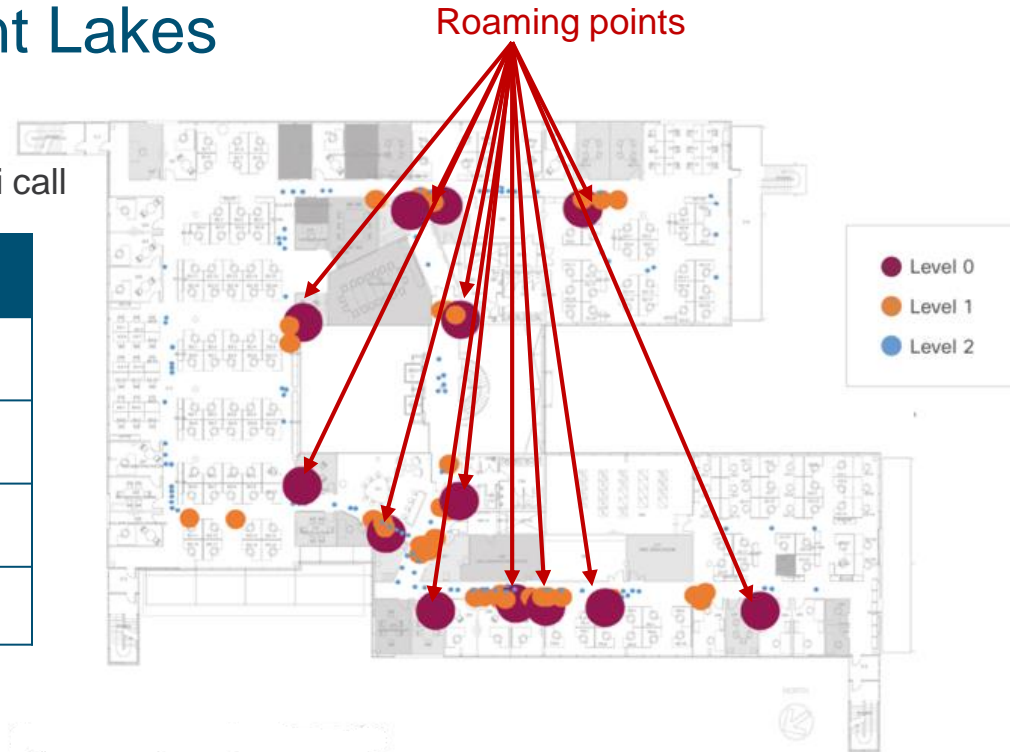
The "CONNECTIVITY" tab shows a progress bar with stages: Start, Association, Authentication, DHCP, and Online. The "TOP APPLICATIONS" section lists the following:

Name	Usage
ping	88.9 MB
apple-services	331.3 KB
dns	95.6 KB
icmp	59.4 KB
icloud	42.2 KB
itunes	14.9 KB
atl-web-services	12.8 KB
ntp	10.9 KB

An Example – Cisco Bedford Lakes

Support requests – Wi-Fi issues during Video VoWi call

Incident level	(Before upgrade) Count over 1 week
Level 0 (productivity Crusher) - Call disconnected -	13
Level 1 (Productivity Inhibitor) - Audio & video gaps -	36
Level 2 (Minor Annoyance) - Audi glitch or light pixelization-	131
Total	180



1. Determine coverage gaps
2. If coverage is satisfactory, look at SW config

An Example – Cisco Bedfont Lakes

Support requests – Wi-Fi issues during Video VoWi call

Incident level	(Before upgrade) Count over 1 week	(After upgrade) Count over 1 week	Change (%)
Level 0 (productivity Crusher) - Call disconnected -	13	0	- 100%
Level 1 (Productivity Inhibitor) - Audio & video gaps -	36	8	- 78%
Level 2 (Minor Annoyance) - Audi glitch or light pixelization-	131	96	- 27%
Total	180	104	-42 %

Security and Threat Mitigation

- User segmentation and end to end policy enforcement
- Secure BYOD and guest access
- Detection and mitigation of Rogues and interferers

Security and Threat Mitigation



802.1x
WPA2/AES



TKIP Encryption



P2P
Blocking



MAC Auth



MFP, 802.11w



Rogue Detection



awIPS, ELM



TrustSec
SGT, SXP



AAA Override
VLAN, ACL, QoS



Local Policy w/
QoS and AVC



BYOD
NAC RADIUS



Client Exclusion

Lower Risk



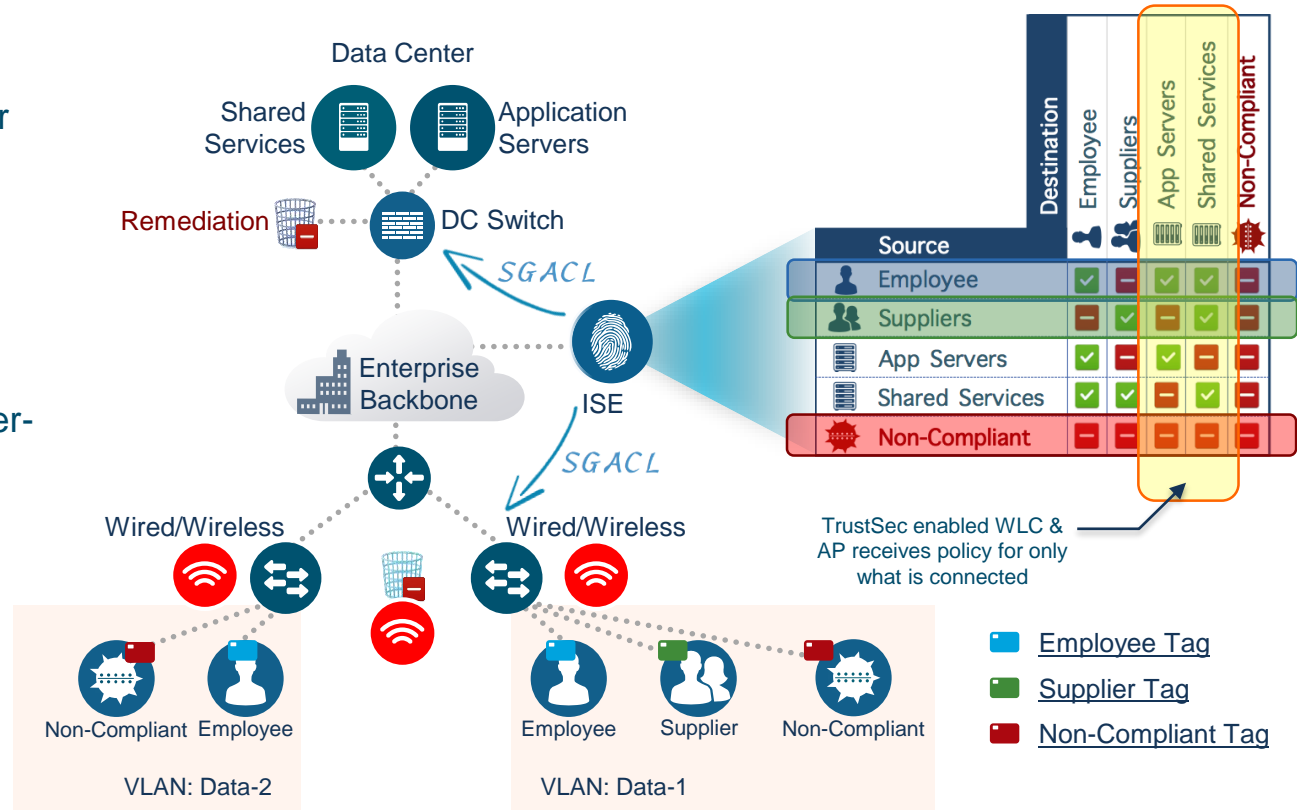
Next-Gen Wireless Office Goal:

Simplified Security

Simplified and Consistent Access governed by TrustSec

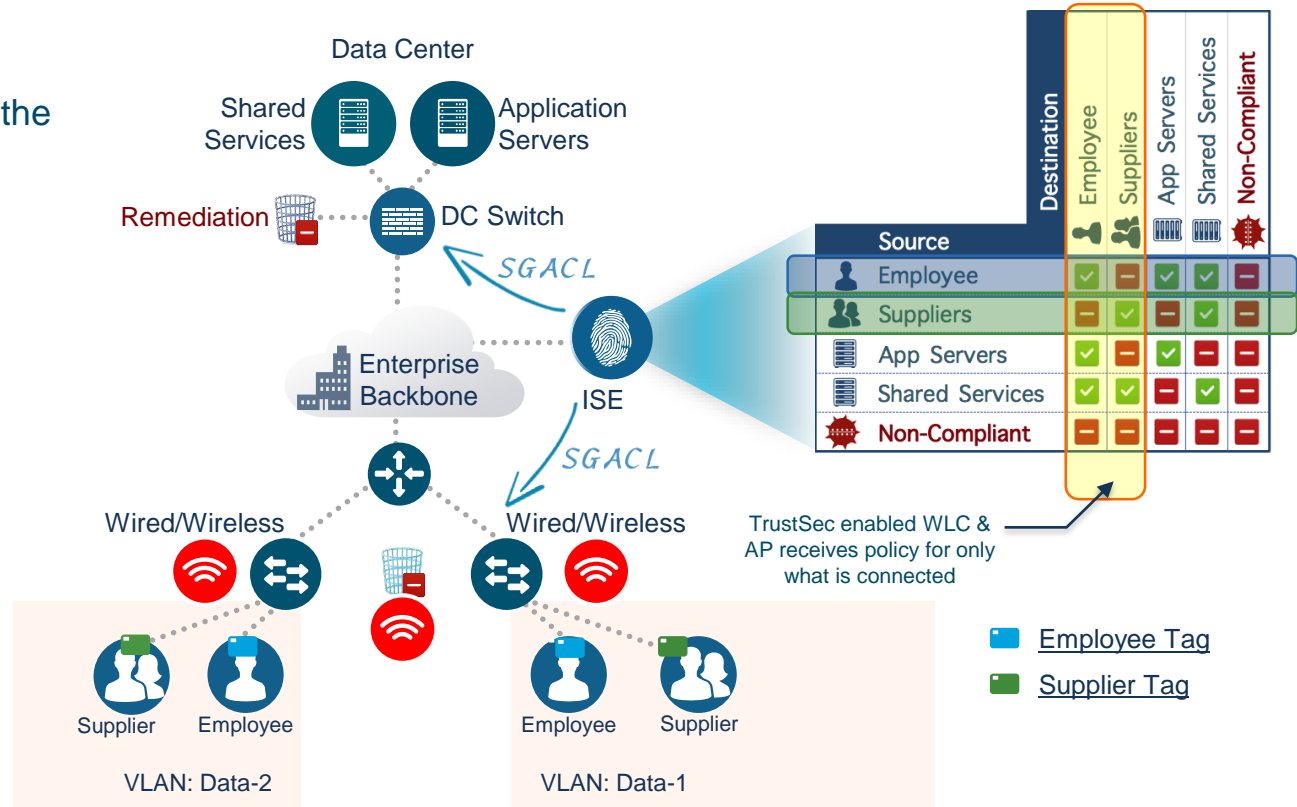
Regardless of topology or location, policy (Security Group Tag) stays with users, devices, and servers

TrustSec simplifies ACL management for intra/inter-VLAN traffic



Role Based Segmentation governed by TrustSec

Access control based on the Role of the user








Next-Gen Wireless Office Goal:

Mitigate Rogues and Intrusion

Cisco Adaptive wIPS with AP3800/2800

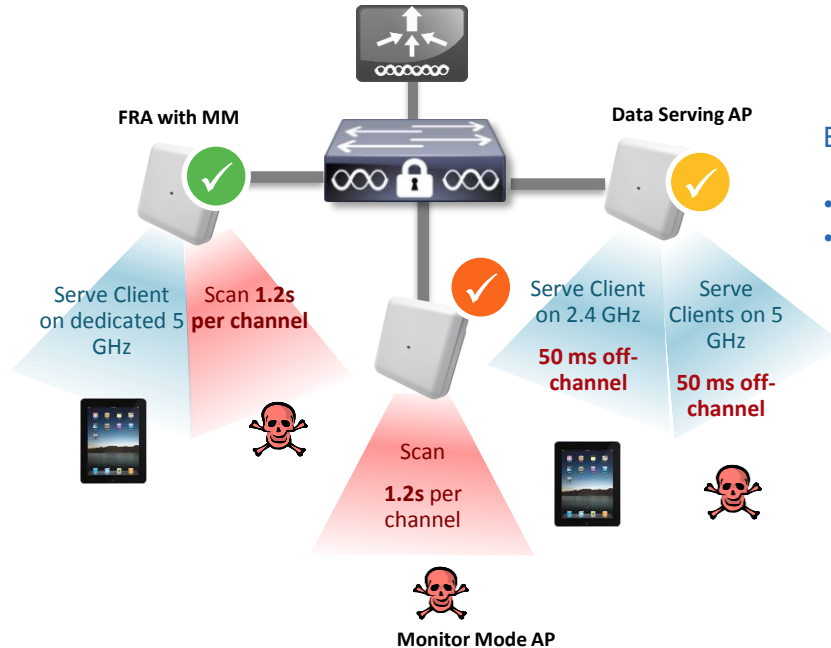
Maintains Capacity and Avoids Interference

	Good 	Better 	Best 
Features	ELM	Monitor Mode AP	ELM with FRA Monitor Mode
Deployment Density	Per AP	1 in 5 APs	1 radio per 5 APs
Client Serving with Security Monitoring	Y	N	Y
wIPS Security Monitoring	50 ms off-channel scan on selected channels on 2.4 and 5 GHz	7 x 24 All Channels on 2.4GHz and 5GHz	7 x 24 All Channels on 2.4GHz and 5GHz
CleanAir Spectrum Intelligence	7 x 24 on client serving channel	7 x 24 All Channels on 2.4GHz and 5GHz	7 x 24 All Channels on 2.4GHz and 5GHz



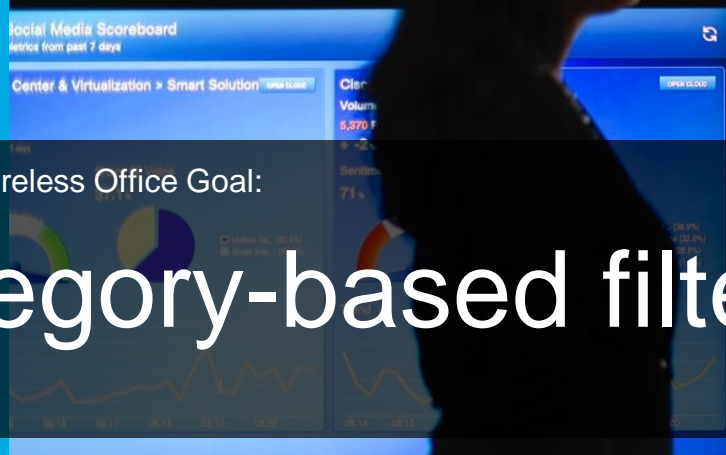
Rogue Detection and Mitigation

- ✓ **Rogue Classification and Containment**
 - Rogue Rules
 - Manual Classification – Friendly/Malicious
 - Manual and Auto Containment
- ✓ **CleanAir with Rogue AP Types**
 - Wi-Fi Invalid Channel
 - Wi-Fi Inverted
- ✓ **Rogue Location**
 - Real-time with PI, MSE, CleanAir
 - Location of Rogue APs and Clients, Ad-hoc Rogue, Non-Wi-Fi interferers



Best Practice Recommendation:

- Set Rogue Detection Security Level to “low”
- Set Detection threshold to ≤ -75 dB



Cisco NetWorking Academy Social M

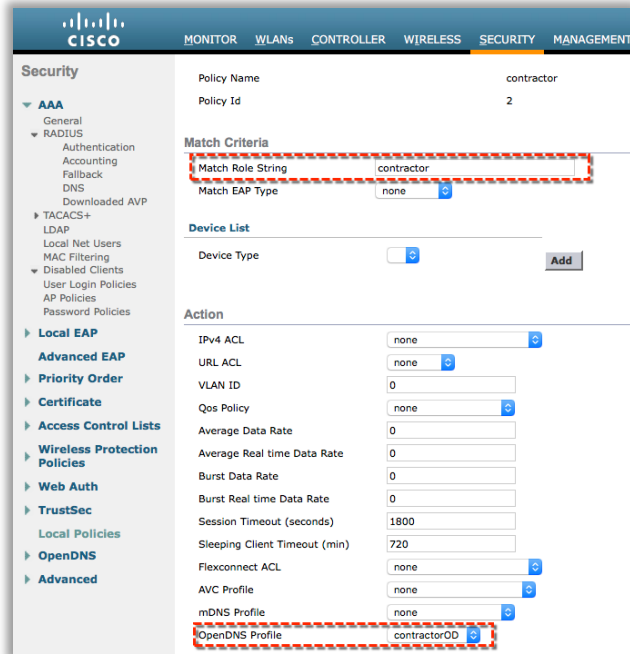
- What
 - Use the social media platform to address students questions
 - Encourage peer-to-peer support
 - Monitor results and satisfaction
- How
 - Use the social media platform of choice
 - Media is available and tag
 - Agents to pick up
- Why
 - Encourage participation for better learning approach
 - Maximize social media investment
- Benefits
 - Reduced
 - Enabled

Next-Gen Wireless Office Goal:

Category-based filtering

Role Based Cisco Umbrella Policy

Cisco Umbrella Profile Mapping in Local Policy



Security

Policy Name: contractor
Policy Id: 2

Match Criteria

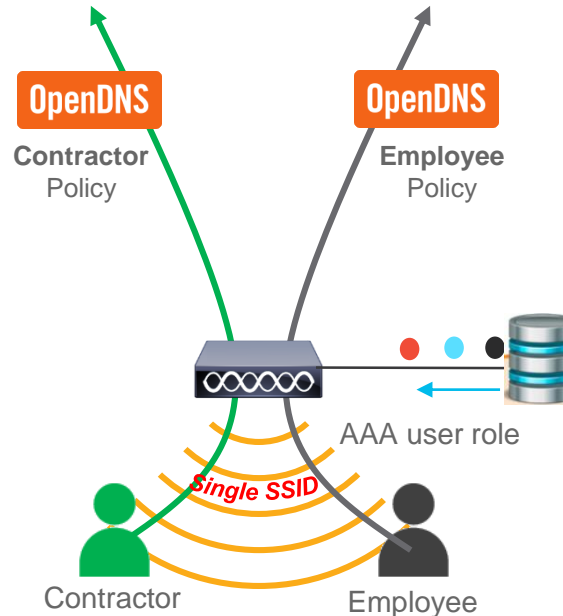
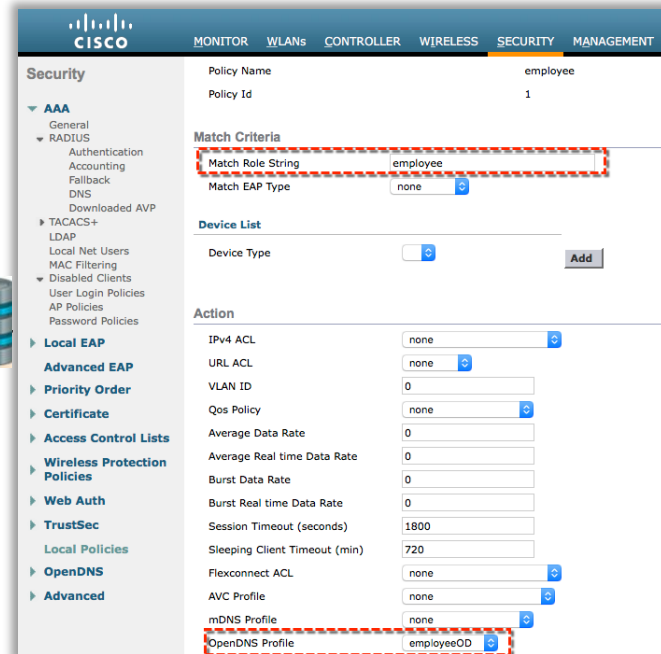
Match Role String: contractor
Match EAP Type: none

Device List

Device Type: [none] [Add]

Action

IPv4 ACL: none
URL ACL: none
VLAN ID: 0
Qos Policy: none
Average Data Rate: 0
Average Real time Data Rate: 0
Burst Data Rate: 0
Burst Real time Data Rate: 0
Session Timeout (seconds): 1800
Sleeping Client Timeout (min): 720
Flexconnect ACL: none
AVC Profile: none
mDNS Profile: none
OpenDNS Profile: contractorOD

Security

Policy Name: employee
Policy Id: 1

Match Criteria

Match Role String: employee
Match EAP Type: none

Device List

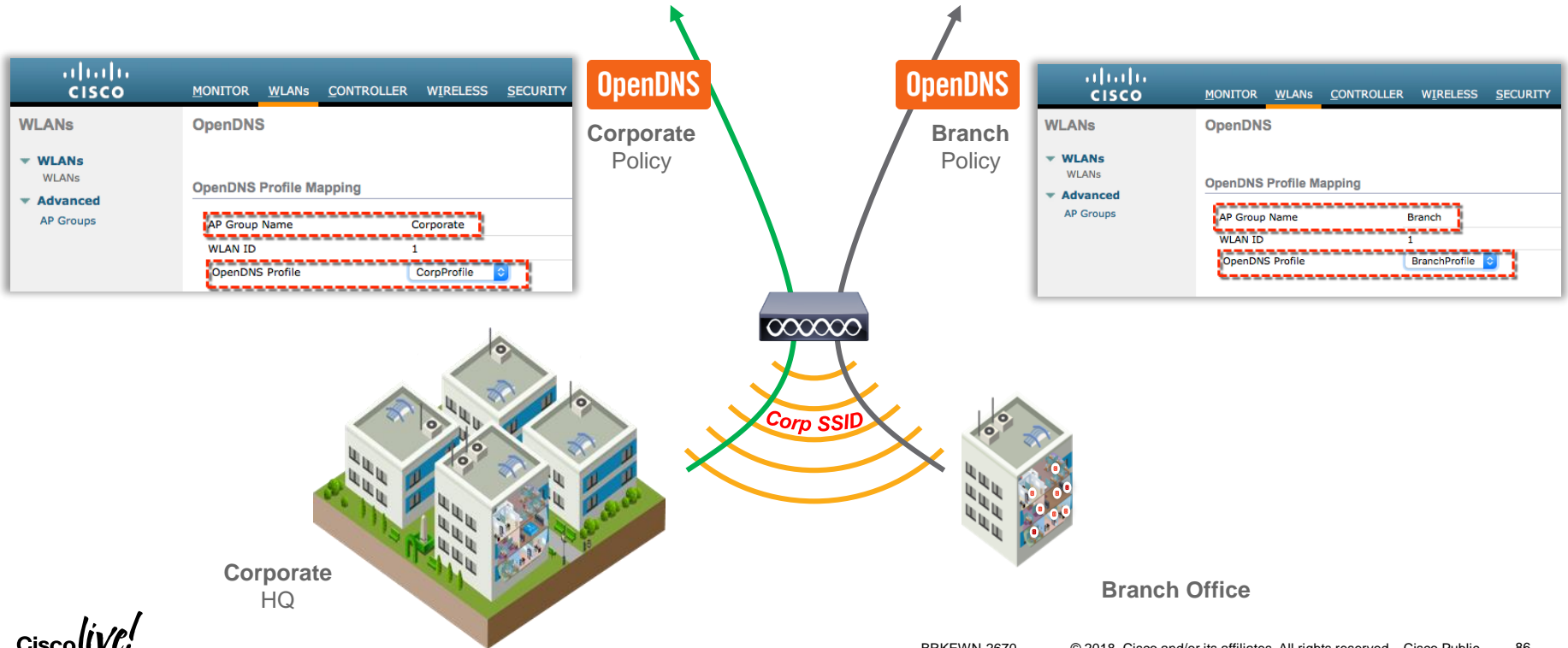
Device Type: [none] [Add]

Action

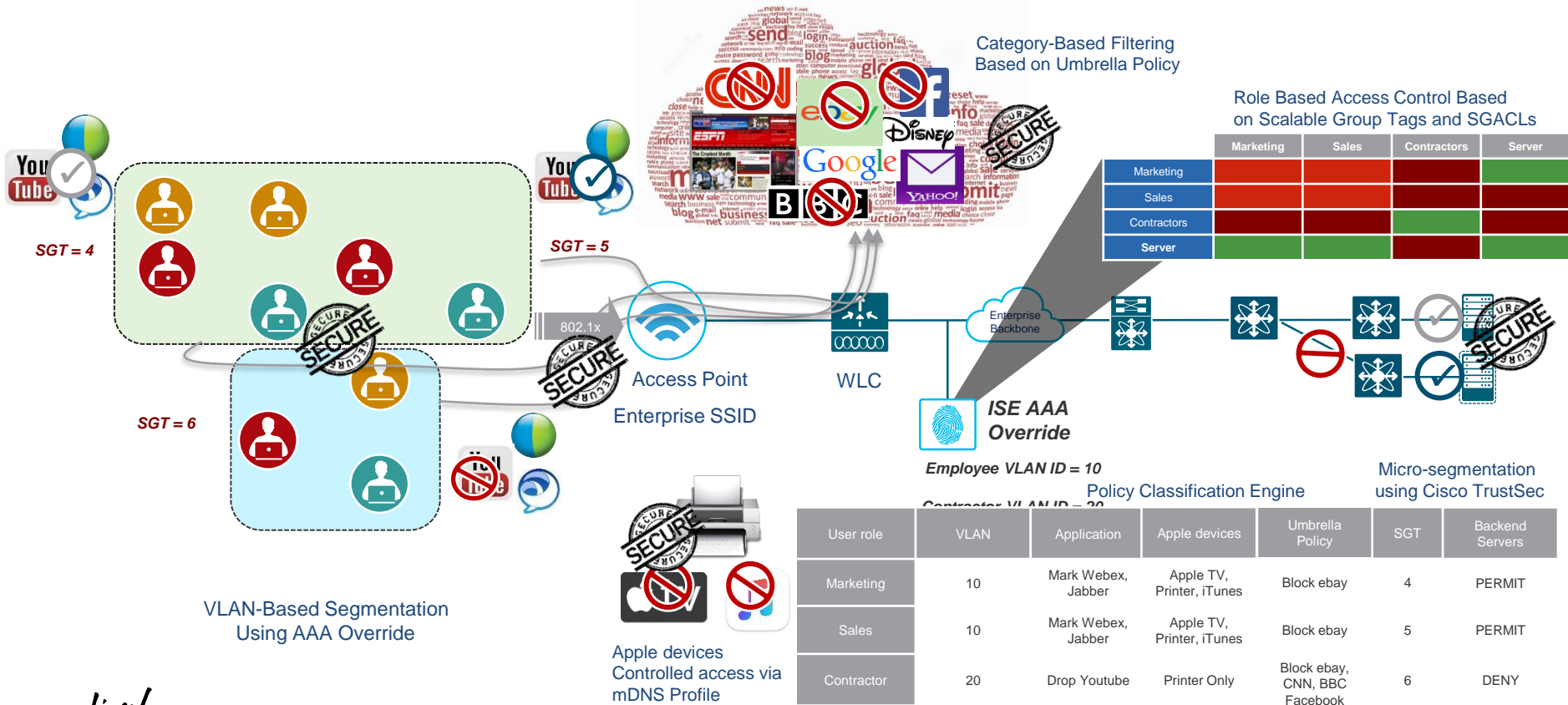
IPv4 ACL: none
URL ACL: none
VLAN ID: 0
Qos Policy: none
Average Data Rate: 0
Average Real time Data Rate: 0
Burst Data Rate: 0
Burst Real time Data Rate: 0
Session Timeout (seconds): 1800
Sleeping Client Timeout (min): 720
Flexconnect ACL: none
AVC Profile: none
mDNS Profile: none
OpenDNS Profile: employeeOD

Location Based Cisco Umbrella Policy

Cisco Umbrella Profile Mapping in AP Group



Enterprise SSID Security and Segmentation



Challenges for Enterprises: Advanced security encryption across all devices



Increased demand for IoT devices



Identity security without 802.1x



Simple Operations
High Scale
Cost Effective

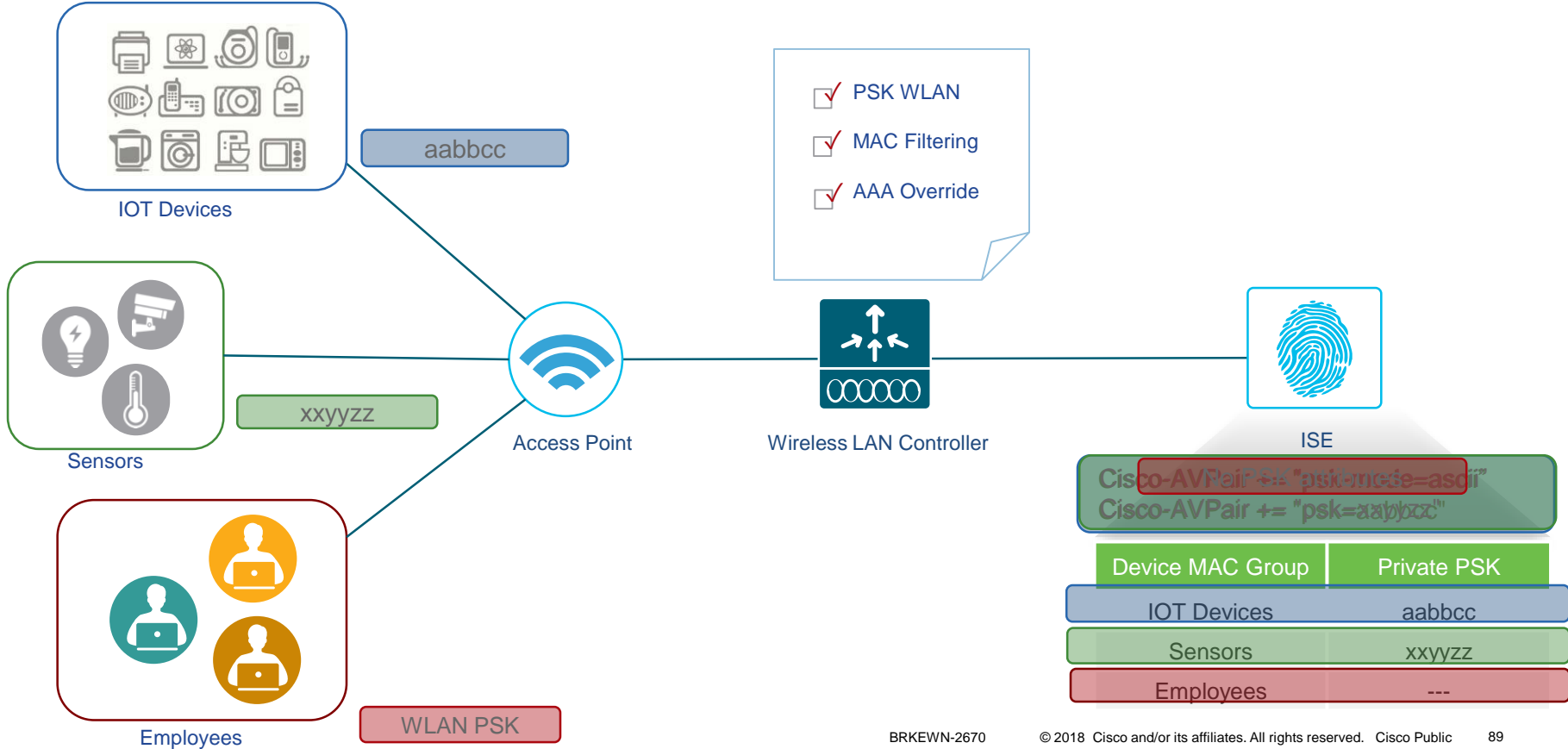
Keys Solution Asks:

Private PSK with RADIUS integration; Per client AAA override (VLAN / ACL, QoS etc)

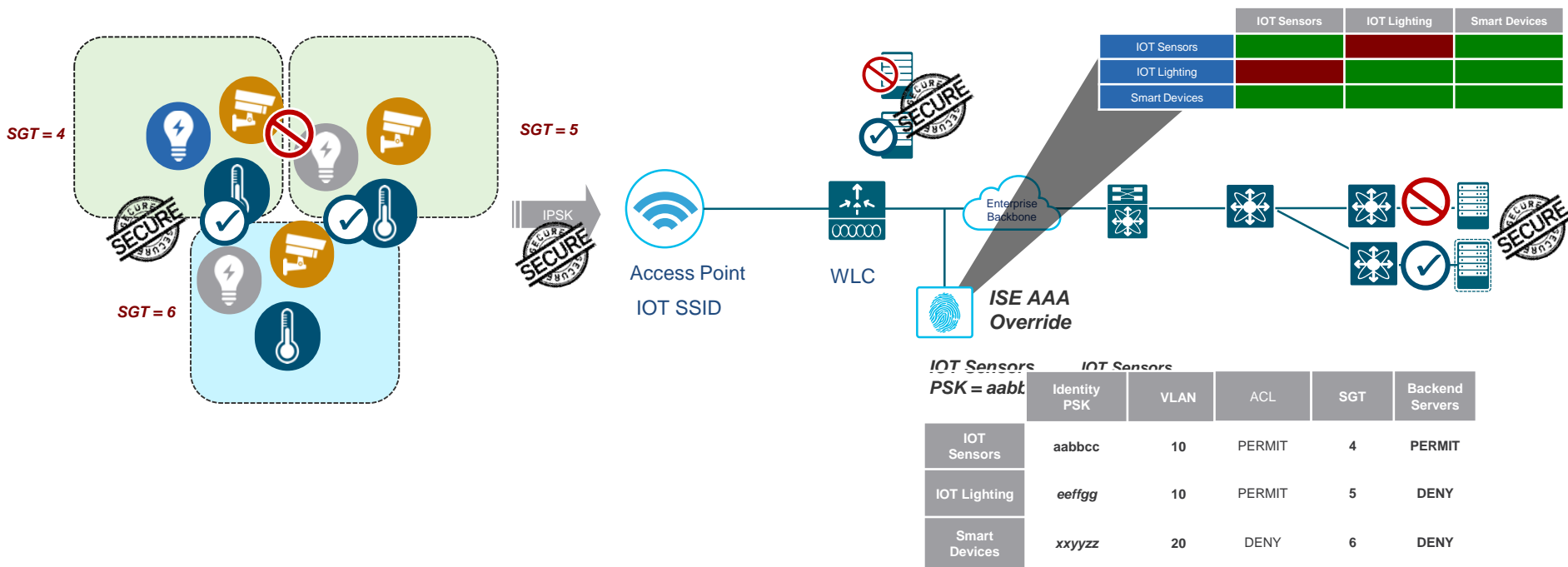
Cisco Advantage:

Highly scalable identity PSK solution designed for a large multi controller network

Identity PSK



IOT SSID Security and Segmentation



How Not to do #hotel #WiFi #Security

WiFi Internet Access

Search WiFi connections, access strongest signal, 5G (preferred), security key as per password

	WiFi Access	Password
Ground Floor	OceanHotelG	OceanHotelG
First Floor	OceanHotel1	OceanHotel1
Second Floor	OceanHotel2	OceanHotel2
Third Floor	OceanHotel3	OceanHotel3
Fourth Floor	OceanHotel3	OceanHotel3

Due to some dead spots other WiFi Networks available:

	WiFi Access	Password
1 st / 2 nd floor	NetGear 14	oddflemingo952
3 rd / 4 th floor	NetGear 91	basickayak276
3 rd / 4 th Floor	NetGear 54	quietflower966

Some devices connect to internet using the above only while others may need further log on information as follows:

Should, Additional log on information required popup - click

= Big4N: ID & Password

Or enter address into web browser <http://10.10.0.1>

= Big4N: ID & Password

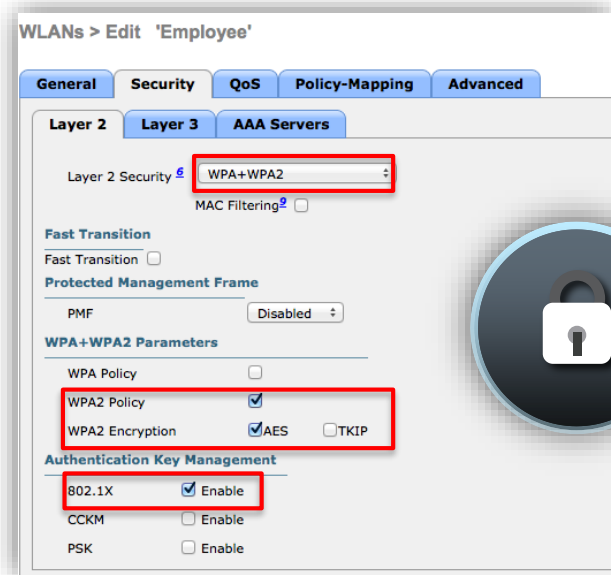
Please contact Reception (dial 9) to provide ID & Password

Should you only receive a weak WiFi signal, please contact reception for assistance.

Source: <https://badfi.com/bad-fi/>

Security Best Practice: Enable 802.1x auth on WLAN and AP

WLANs → Edit 'WLAN_NAME' → Security



The screenshot shows the 'WLANs > Edit 'Employee'' configuration page. The 'Security' tab is selected. Under 'Layer 2 Security', 'WPA+WPA2' is selected. Under 'WPA+WPA2 Parameters', 'WPA2 Policy' is checked, and 'WPA2 Encryption' is set to 'AES'. Under 'Authentication Key Management', '802.1X' is checked and set to 'Enable'. A padlock icon is overlaid on the right side of the screenshot.

Wireless → Access Points → Global Configurations

802.1x Supplicant Credentials

802.1x Authentication

Username

testap

Password

••••••••

Confirm Password

••••••••

To enable 802.1X authentication on a switch port, on the switch CLI, enter these commands:

```
Switch# configure terminal
Switch(config)# dot1x system-auth-control
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# radius-server host ip_addr auth-port port acct-port port
key key
Switch(config)# interface fastethernet2/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
```

Provides greater network security on WLAN using 802.1x authentication

Deployment Lifecycle

The Bigger Picture





Introducing DNA Center

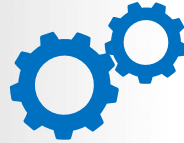
Realizing vision of the intent-powered intuitive network



Policy

Translate business intent
into network policy

Decouple Policy from
Network Topology



Automation

Reduce manual operations
and cost associated with
human errors

Industry Best-Practices
Configuration and Policy
Compliance

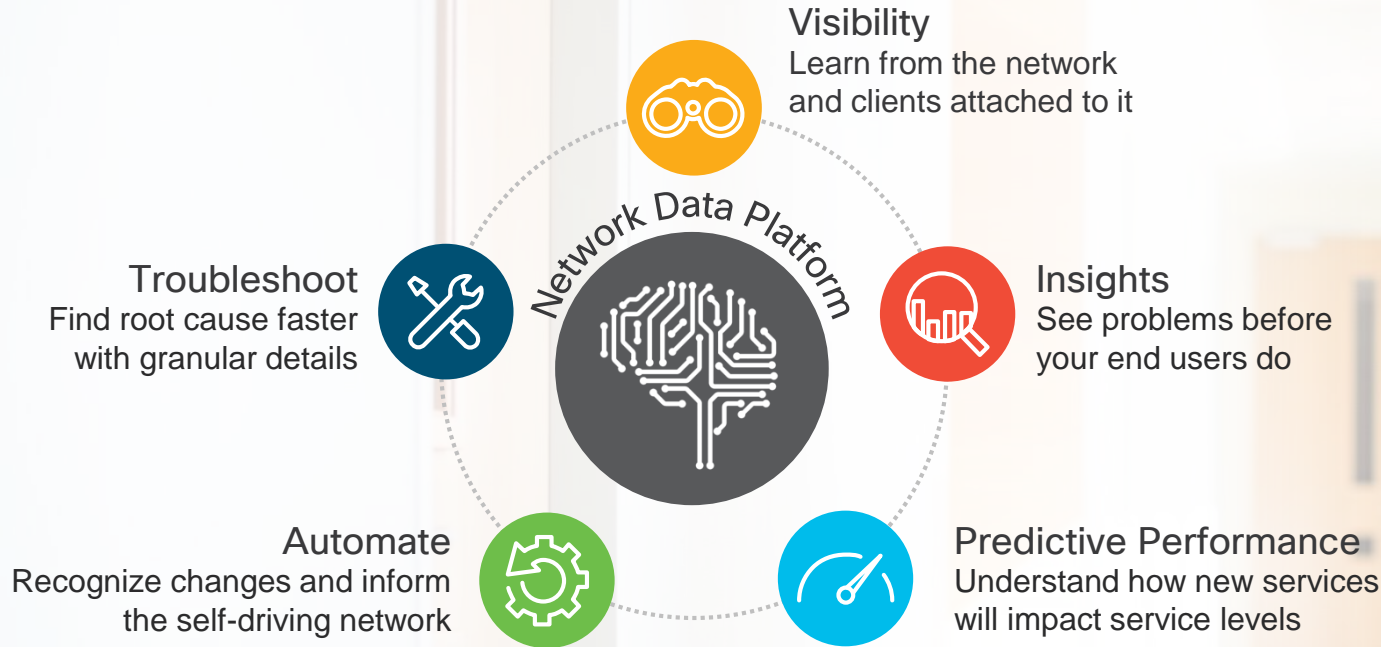


Assurance and
Analytics

Use context to turn data into
intelligence

Proactive Issue
Identification and
Resolution

Assurance: Predict Issues Before They Happen



Industry's First Self-Predicting Network Analytics Platform

Wireless Sensors Proactively Assess Performance

Test your network with existing APs at any time

➤ On-Boarding Tests

- 802.11 Association
- 802.11 Authentication & Key Exchange
- IP Addressing DHCP (IPv4)

➤ Network tests

- DNS (IPv4)
- RADIUS (IPv4)
- First Hop Router/Default gateway (IPv4)
- Intranet Host
- External Host (IPv4)

➤ Application tests

- Email: POP3, IMAP, Outlook Web Access (IPv4)
- File Transfer: FTP (IPv4)
- Web: HTTP & HTTPS (IPv4)



Flexible Radio Assignment Algorithm intelligently identifies excessive radios and seamlessly converts those into Sensor mode without client impact

Wireless Sensor Support

Flexible Radio as Sensor (2800/3800)



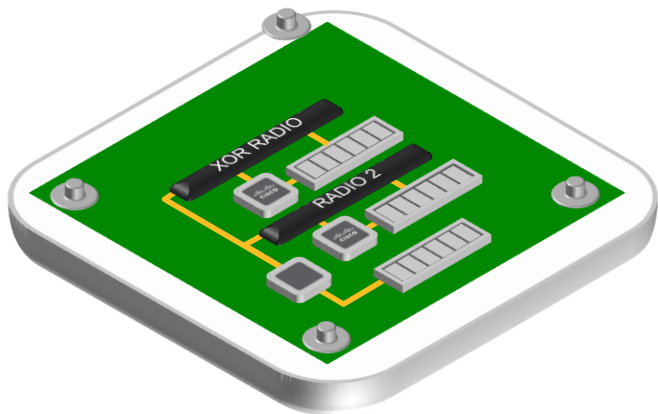
Dual 5 GHz Flexible Radios

Software defined radios automatically adjust to dual 5GHz



Purpose-built Hardware for Analytics

Flexible radios can provide simultaneous in-line monitoring to DNA for analytics and insights while serving clients (future)



- 5GHz.
- 2.4GHz.
- Sensor (Client Testing)

XOR RADIO

Dedicated AP as Sensor

1815/1830/1850 AP



1815



1830/1850

1800s dedicated sensor



- 2x2 with 2 spatial streams
- Multiple powering options:
 - PoE Power
 - USB Type “C” power
 - Direct AC Power Plug
- Integrated BLE

- BRKEWN-3033: DNA Assurance – deep dive
 - Wednesday Jan 31, 4:30pm – 6:00pm with Jerome Henry
- BRKEWN-2032: DNA Assurance: bring intelligence to your WLAN issues
 - Tuesday Jan 30, 4.30 pm with Jeremy Cohoe





Workspace Analytics

Making Buildings Smarter



Workspace Optimization
Lower Real-estate costs



Cisco Portfolio for Next-Gen Wireless Workspace

DNA ready Wireless Controller Portfolio

Large Enterprise

Mid-size Enterprise

Small Network

Mobility Express
50 APs/1000 Clients AP 18xx
100 AP/2000 Clients: AP2/3K



Cisco 3504
150 APs
3000 Clients
4 Gbps



Cisco 5520
1500 APs
20,000 Clients
20 Gbps



Cisco vWLC
3000 APs
32000 Clients
Flexconnect mode



Cisco 8540
6000 APs
64,000 clients
40 Gbps



Up to 100 APs

Up to 3000 APs

Up to 6000 APs

Designed to be DNA Ready

Industry's Most Comprehensive Indoor AP Portfolio:

Enterprise Class			Mission Critical	Best in Class
1815	1830	1850	2800	3800
				
<p>Indoor / High-powered Indoor Wall Plate / Teleworker</p> <ul style="list-style-type: none">2x2:2SS 80 MHz867 Mbps PerformanceTx Beam FormingIntegrated BLE Gateway¹Max Transmit Power (dBm) per local regulations²3 GE Local Ports, including 1 PoE out³Local ports 802.1x ready³USB 2.0⁴	<ul style="list-style-type: none">3x3:2SS 80MHz867 Mbps PerformanceTx Beam Forming1 GE Port UplinkUSB 2.0	<ul style="list-style-type: none">4x4:3SS 80MHz1.7 Gbps PerformanceInternal or External AntennaTx Beam Forming2 GE Ports UplinkUSB 2.0	<ul style="list-style-type: none">4x4:3SS 160 MHz5 Gbps Performance2.4 and 5GHz or Dual 5GHz2 GE Ports UplinkCleanAir and ClientLinkInternal or External AntennaSmart Antenna ConnectorUSB 2.0	<ul style="list-style-type: none">4x4:3SS 160 MHz5 Gbps Performance2.4 and 5GHz or Dual 5GHz2 GE Ports Uplink or 1 GE + 1 mGig (5G)CleanAir and ClientLinkStadiumVisionInternal or External AntennaSmart Antenna ConnectorUSB 2.0Investment Proof Modularity

DNA Ready | RF Excellence | CMX | Centralized, FlexConnect or Mobility Express

Dual 5 GHz | Flexible Radio | HDX

Future Proof

Designed to be DNA Ready

Industry's Most Comprehensive Outdoor AP Portfolio:

1540



- 802.11ac Wave 2, MU-MIMO
- 2x2:2, 80MHz, 867 Mbps
- Ultra low profile
- Internal antenna only
- PoE (802.3af) power
- Centralized, FlexConnect, Mesh and Mobility Express

1560



- 802.11ac Wave 2, MU-MIMO
- 3x3:3, 80MHz, 1.3Gbps (I)
- 2x2:2, 80MHz, 867Mbps (E/D)
- Internal or External antenna model (I/E)
- Internal directional antenna model (D)
- SFP
- Flexible Antenna Ports
- CleanAir and ClientLink
- Centralized, FlexConnect, Mesh and Mobility Express

1570



- 802.11ac Wave 1
- 4x4:3 80 MHz; 1.3 Gbps
- External antenna model (EAC)
- Cable Modem model (IC/EC)
- SFP/GPS
- PoE Out 802.3at (Ext Ant. only)
- Flexible Antenna Ports
- CleanAir and ClientLink
- Modularity (Ext Ant. only)
- Centralized, FlexConnect and Mesh
- Cable Modem Version Only (IC/EC)
- DOCSIS 3.0, 24x8
- Internal or External antenna

DNA Ready | RF Excellence | CMX

Learning Resources



Best Practices Summary



BEST PRACTICES (AireOS)

INFRASTRUCTURE

- Enable High Availability (AP and Client SSO)
- Enable AP Failover Priority
- Enable AP Multicast Mode
- Enable Multicast VLAN
- Enable Pre-image download
- Enable AVC
- Enable NetFlow
- Enable Local Profiling (DHCP and HTTP)
- Enable NTP
- Modify the AP Re-transmit Parameters
- Enable FastSSID change
- Enable Per-user BW contracts
- Enable Multicast Mobility
- Enable Client Load balancing
- Disable Aironet IE
- FlexConnect Groups and Smart AP Upgrade

MESH

- Set Bridge Group Name
- Set Preferred Parent
- Multiple Root APs in each BGN
- Set Backhaul rate to "Auto"
- Set Backhaul Channel Width to 40/80 MHz
- Backhaul Link SNR > 25 dBm
- Avoid DFS channels for Backhaul
- External RADIUS server for Mesh MAC Authentication
- Enable IDS
- Enable EAP Mesh Security Mode

SECURITY

- Enable 802.1x and WPA/WPA2 on WLAN
- Enable 802.1x authentication for AP
- Change advance EAP timers
- Enable SSH and disable telnet
- Disable Management Over Wireless
- Disable Wi-Fi Direct
- Peer-to-peer blocking
- Secure Web Access (HTTPS)
- Enable User Policies
- Enable Client exclusion policies
- Enable rogue policies and Rogue Detection RSSI
- Strong password Policies
- Enable IDS
- BYOD Timers

WIRELESS / RF

- Disable 802.11b data rates
- Restrict number of WLAN below 4
- Enable channel bonding – 40 or 80 MHz
- Enable BandSelect
- Use RF Profiles and AP Groups
- Enable RRM (DCA & TPC) to be auto
- Enable Auto-RF group leader selection
- Enable Cisco CleanAir and EDRRM
- Enable Noise & Rogue Monitoring on all channels
- Enable DFS channels
- Avoid Cisco AP Load



VoD Links

- Cisco CMX Solution <https://www.youtube.com/watch?v=KQRb8vfU0qM>
- CMX Hyperlocation vs RSSI Demo <https://www.youtube.com/watch?v=6ls7EHbSK4A>
- Cisco Dual 5GHz Wi-Fi <https://www.youtube.com/watch?v=mbpjiETvDXc>
- Cisco Aironet AP-3800 RF Excellence <https://www.youtube.com/watch?v=dBpGsTKeyNM&t=64s>
- Digital Network Architecture with Wave2 with 802.11ac <https://www.youtube.com/watch?v=ySjN13hPhXY&t=2s>
- Cisco Aironet Series – Flexible Radio Assignment https://www.youtube.com/watch?v=K_-BykT_YIM
- TechWiseTV: Apple and Cisco: Fast-Tracking the Mobile Enterprise <https://www.youtube.com/watch?v=bh8rEvrzm7Y&feature=youtu.be>
- Prioritized Business Apps <https://www.youtube.com/watch?v=z0EOKNxL964&feature=youtu.be>
- Apple and Cisco: Three Solutions Coming Together <https://www.youtube.com/watch?v=7MgsDkf55wQ&feature=youtu.be>
- Wi-Fi Optimized Feature <https://www.youtube.com/watch?v=xgPfxAoJoQ&feature=youtu.be>
- Fastlane App Demo <https://www.youtube.com/watch?v=N1QMUcv3aRQ>
- Cisco APIC-EM Wireless PnP Demo https://www.youtube.com/watch?v=_9P2-bU66PU
- Cisco Aironet Plug and Play Cloud Redirection <https://www.youtube.com/watch?v=W7fBZ6xfSxw>
- Wireless LAN Controller Dashboard Review <https://www.youtube.com/watch?v=af09T1BaafRI&feature=youtu.be>
- Cisco Wireless Mobile App <https://www.youtube.com/watch?v=HyvZ4mbVAWs>
- WLC Advanced UI Client Troubleshooting https://www.youtube.com/watch?v=dZVxl6jOx_Q
- ISE Simplified Wireless Setup <https://www.youtube.com/watch?v=A3F2DrFu7Lo&feature=youtu.be>
- Cisco Wireless TrustSec Demo <https://www.youtube.com/watch?v=A3F2DrFu7Lo&feature=youtu.be>
- Cisco Wireless Netflow Lancope Integration Demo <https://www.youtube.com/watch?v=TUWYkrt94CQ>
- Cisco Umbrella Integration with WLC <https://www.youtube.com/watch?v=cMdX8sBBYG4>

[Click - https://www.youtube.com/user/CiscoWLAN/](https://www.youtube.com/user/CiscoWLAN/)

Cisco Wireless LAN Documentation

INSTALLATION GUIDES

- 5520 WLC
- 8540 WLC
- AP1570
- AP1810 OE
- AP1810W Wall Plate
- AP1850
- AP2700/3700
- AP2800/3800
- AP702W
- APIC-EM Wireless AP PnP
- Flex7500 WLC
- Mesh APs
- Mobility Express
- Smart Licensing
- Univ. AP Regulatory Domain
- Virtual WLC

RADIO CONFIGURATION

- 802.11r BSS Fast Transition
- Adaptive wIPS
- ATF Ph 1 & 2
- CleanAir
- CMX FastLocate
- High Density
- Rogue Management
- RRM RF Grouping Algorithm
- RRM White Paper

ENCRYPTION

- BYOD for FlexConnect
- BYOD with ISE
- Security Integration

CLIENT ADDRESSING

- Bi-Directional Rate Limiting
- Flex AP-EoGRE Tunnel Gtwy
- IPv6
- Jabber
- Jabber and UCM
- Microsoft Lync
- Passpoint Configuration
- Real-Time Traffic Over WLAN
- VideoStream
- Vocera IP Phone in WLAN
- VoWLAN Troubleshooting



POLICY ENGINE

- AVC
- Bonjour
- Chromecast
- Device Classification
- Domain Filtering
- mDNS Gateway w/Chromecast
- Wireless Device Profiling & Policy Classification

BEST PRACTICES

- Apple Devices
- Enterprise Mobility Design Guide
- High Availability (SSO)
- HyperLocation
- iPhone 6 Roaming
- N+1 High Availability
- WLAN Express
- WLC Configuration Best Practices

Continue Your Education

BRKEWN-2003	Optimize your WLANs for Iphones (and welcome other mobile devices too)	01/30/2018	Hall 8.0, Session Room 112	16:45:00
BRKEWN-2010	Design and Deployment of Enterprise WLANs	01/30/2018	Hall 8.0, Session Room 101	14:15:00
BRKEWN-2017	Understanding RF Fundamentals and the Radio Design for 11ac Wireless Networks	01/30/2018	Hall 8.0, Session Room 107	11:15:00
BRKEWN-2019	7 Ways to Fail as a Wireless Expert	01/30/2018	Hall 8.0, Session Room 132	11:15:00
BRKEWN-2033	A Cloud-based Machine Learning / Analytics architecture for DNA (wireless/wired) Assurance	01/31/2018	Hall 8.0, Session Room 137	16:30:00
BRKEWN-3014	Best practices to deploy high-availability in Wireless LAN Architectures	01/31/2018	Hall 8.0, Session Room 112	14:30:00
BRKEWN-2012	Design and Use Cases of a location enabled Wi-Fi network supported by Connected Mobile Experiences (CMX)	02/01/2018	Hall 8.0, Session Room 106	14:30:00
BRKEWN-3010	Improve Enterprise WLAN Spectrum Quality with Cisco's advanced RF capacities (RRM, CleanAir, ClientLink, etc)	02/01/2018	Hall 8.0, Session Room 101	09:00:00
BRKEWN-2005	Securely Designing Your Wireless LAN for Threat Mitigation, Policy and BYOD	02/01/2018	Hall 8.0, Session Room 139	11:30:00

Cisco Spark

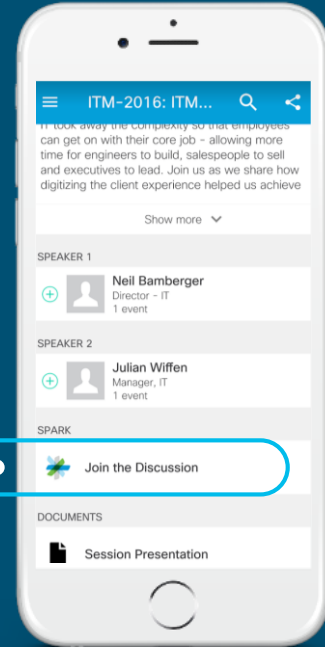


Questions?

Use Cisco Spark to communicate with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space



cs.co/cislivebot#BRKEWN-2670

- Please complete your Online Session Evaluations after each session
- Complete 4 Session Evaluations & the Overall Conference Evaluation (available from Thursday) to receive your Cisco Live T-shirt
- All surveys can be completed via the Cisco Live Mobile App or the Communication Stations

Don't forget: Cisco Live sessions will be available for viewing on-demand after the event at www.ciscolive.com/global/on-demand-library/.

Complete Your Online Session Evaluation



Continue Your Education

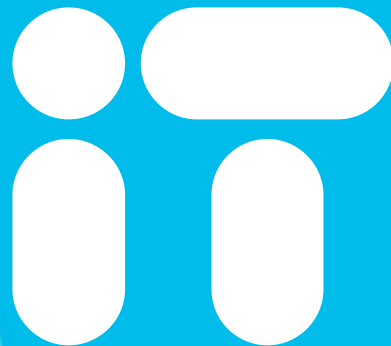
- Demos in the Cisco campus
- Walk-in Self-Paced Labs
- Tech Circle
- Meet the Engineer 1:1 meetings
- Related sessions



Thank you



You're



Cisco *live!*

Supplementary Material

Configurations and Setup Instructions

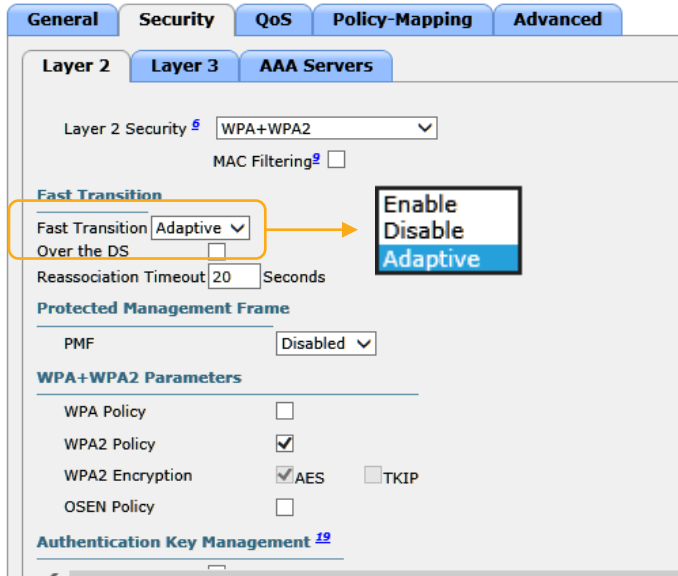
Optimized WiFi Connectivity Configuration

Adaptive 11r

Feature enabled by default on a newly created SSID

- Even if 802.11r is not enabled on the WLAN, it is enabled for the WLAN for the Apple IOS 10 devices (adaptive 11r) by default:

WLANs > Edit 'WHOPPERWIFI'



```
Show wlan 3
```

```
.../...
```

```
Security
```

```
802.11 Authentication:..... Open System
```

```
FT Support..... Adaptive
```

Adaptive 11r

- Adaptive 11r means that the WLAN security is set to WPA2 (NOT to static 802.11r, no need for “hybrid” mode either):

The screenshot shows the 'Layer 2' configuration page for WLAN security. The 'Layer 2 Security' dropdown is set to 'WPA+WPA2'. Below it, 'MAC Filtering' is disabled. The 'Fast Transition' section is highlighted with an orange box, showing 'Fast Transition' set to 'Adaptive' and 'Over the DS' disabled. 'Reassociation Timeout' is set to 20 seconds. 'Protected Management Frame' (PMF) is set to 'Disabled'. The 'WPA+WPA2 Parameters' section shows 'WPA2 Policy' checked, 'WPA2 Encryption' set to 'AES', and 'TKIP' disabled. 'Authentication Key Management' is also visible at the bottom.

The screenshot shows the 'WPA+WPA2 Parameters' and 'Authentication Key Management' sections. Under 'WPA+WPA2 Parameters', 'WPA Policy' is disabled, 'WPA2 Policy' is checked, 'WPA2 Encryption' is set to 'AES' (with 'TKIP' disabled), and 'OSEN Policy' is disabled. Under 'Authentication Key Management', '802.1X', 'CCKM', and 'PSK' are all enabled. 'FT 802.1X' and 'FT PSK' are both disabled, with this section highlighted by an orange box. 'PSK Format' is set to 'ASCII' and 'WPA gtk-randomize State' is set to 'Disable'.

11k Configuration

- Feature enabled by default on a newly created SSID
- Dual band neighbor list selectively enable for Apple devices that supportive Adaptive capability

The screenshot displays the configuration page for SSID 11k, divided into two main sections: General and Advanced. The General section includes options for Learn Client IP Address, Vlan based Central Switching, Central DHCP Processing, Override DNS, NAT-PAT, and Central Assoc, all of which are currently disabled. The Lync section shows the Lync Server is disabled. The 11k section, highlighted with a red box, contains the following settings:

Setting	Value
Assisted Roaming Prediction Optimization	<input type="checkbox"/> Enabled
Neighbor List	<input checked="" type="checkbox"/> Enabled
Neighbor List Dual Band	<input type="checkbox"/> Enabled
Denial Maximum Count	2
Prediction Minimum Count	2

The Advanced section includes settings for HTTP Profiling, PMIP (Mobility Type, NAI Type, Profile, Realm), Universal AP Admin Support, 11v BSS Transition Support (BSS Transition, Disassociation Imminent, Disassociation Timer, Optimized Roaming Disassociation Timer, BSS Max Idle Service, Directed Multicast Service), and Tunneling.

11v Configuration

- 802.11v features are enabled by default on a newly created SSID

The screenshot shows a configuration page with tabs for General, Security, QoS, Policy-Mapping, and Advanced. The Advanced tab is selected. Under the '11k' section, 'Assisted Roaming Prediction Optimization' is disabled, while 'Neighbor List', 'Neighbor List Dual Band', 'Denial Maximum Count' (set to 2), and 'Prediction Minimum Count' (set to 2) are enabled. The '11v BSS Transition Support' section is highlighted with a red box and contains the following settings:

Feature	Value
BSS Transition	<input checked="" type="checkbox"/>
Disassociation Imminent	<input type="checkbox"/>
Disassociation Timer(0 to 3000 TBTT)	200
Optimized Roaming Disassociation Timer(0 to 40 TBTT)	40
BSS Max Idle Service	<input checked="" type="checkbox"/>
Directed Multicast Service	<input checked="" type="checkbox"/>

FastLane Feature Configuration

Fast lane on WLC

- Enabled from the QoS tab of WLAN configuration
- Enabling the first WLAN for Fastlane also enables AutoQoS (best QoS config) globally
- Application Visibility is semi-independent

WLANs > Edit 'WHOPPERWIFI'

The screenshot shows the configuration page for a WLAN named 'WHOPPERWIFI'. The 'QoS' tab is selected, and the 'Fastlane' option is set to 'Enable'. A warning dialog box is displayed, indicating that applying the configuration will temporarily disable all WLANs and networks. The dialog box contains the following text: 'Warning: If you continue and apply the WLAN configuration, this command will temporarily disable all WLANs and networks. Active WLANs and networks will be re-enabled automatically after the configuration completes. This command will also override the file named AUTOQOS-AVC-PROFILE, if it exists, and will apply it to the WLAN, if Application Visibility is enabled. Are you sure that you want to continue?' The dialog box has 'OK' and 'Cancel' buttons.

Fast lane

- Enabling Fastlane:
- Configures best QoS globally
- Sets the WLAN for Platinum
- Sets WMM to Required
- (Notice AV is still disabled)

General
Security
QoS
Policy-Mapping
Advanced

Quality of Service (QoS) Platinum (voice) ▾

Application Visibility Enabled

AVC Profile none ▾

Flex AVC Profile none ▾

Netflow Monitor none ▾

Fastlane Enable ▾

Override Per-User Bandwidth Contracts (kbps) ¹⁶

	DownStream	UpStream
Average Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Average Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>

Override Per-SSID Bandwidth Contracts (kbps) ¹⁶

Fast lane

- Enabling Fastlane enables best QoS config globally:
- Platinum profile sets Max Priority to voice (UP 6), non-WMM and multicast to BE, 802.1p disabled, bandwidth contracts disabled
- EDCA profile is set to Fastlane

General

EDCA Profile

Enable Low Latency MAC

Edit QoS Profile

QoS Profile Name

Description

Per-User Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Average Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>

Per-SSID Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Average Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>

WLAN QoS Parameters

Maximum Priority

Unicast Default Priority

Multicast Default Priority

Wired QoS Protocol

Protocol Type

Fast lane

- Enabling Fastlane enables best QoS config globally:
- ACM is enabled on both bands (load-based), with max RF bandwidth 50% and roaming bandwidth to 6%
- Expedited bandwidth is enabled

The image displays two screenshots of Cisco configuration pages for Media settings on different frequency bands. The top screenshot is for 802.11a(5 GHz) and the bottom is for 802.11b(2.4 GHz). Both pages show the 'Media' tab selected, with 'Call Admission Control (CAC)' and 'Per-Call SIP Bandwidth' sections visible. The 'Metrics Collection' checkbox is unchecked in both.

802.11a(5 GHz) > Media

Call Admission Control (CAC)

- Admission Control (ACM) Enabled
- CAC Method [?](#) Load Based
- Max RF Bandwidth (5-85)(%) 50
- Reserved Roaming Bandwidth (0-25)(%) 6
- Expedited bandwidth
- SIP CAC Support [?](#) Enabled

Per-Call SIP Bandwidth [?](#)

- SIP Codec G.711
- SIP Bandwidth (kbps) 64
- SIP Voice Sample Interval (msecs) 20

Traffic Stream Metrics

- Metrics Collection

802.11b(2.4 GHz) > Media

Call Admission Control (CAC)

- Admission Control (ACM) Enabled
- CAC Method [?](#) Load Based
- Max RF Bandwidth (5-85)(%) 50
- Reserved Roaming Bandwidth (0-25)(%) 6
- Expedited bandwidth
- SIP CAC Support [?](#) Enabled

Per-Call SIP Bandwidth [?](#)

- SIP Codec G.711
- SIP Bandwidth (kbps) 64
- SIP Voice Sample Interval (msecs) 20

Traffic Stream Metrics

- Metrics Collection

Fast lane

- Enabling Fastlane enables best QoS config globally:
- DSCP is trusted upstream (instead of UP)
- DSCP to UP map is configured as per IETF recommendations (“well-known” DSCP values mapped to IETF-recommended values, “unexpected” DSCP values mapped to BE

Wireless

- ▼ **Access Points**
 - All APs
 - ▼ Radios
 - 802.11a/n/ac
 - 802.11b/g/n
 - Dual-Band Radios
 - Global Configuration
- ▶ **Advanced**
- Mesh**
- ▶ **ATF**
- RF Profiles**
- FlexConnect Groups**
 - FlexConnect ACLs
 - FlexConnect VLAN Templates
- OEAP ACLs**
- Network Lists**
- ▶ **802.11a/n/ac**
- ▶ **802.11b/g/n**
- ▶ **Media Stream**
- ▶ **Application Visibility And Control**
- Country**
- Timers**
- ▶ **Netflow**
- ▼ **QoS**
 - Profiles
 - Roles
 - Qos Map

QoS Map Config

Qos Map ▼

Trust DSCP UpStream

UP to DSCP Map

User Priority ▼

DSCP Default

DSCP Start

DSCP End

Modify

UP to DSCP Map List

UP	Default DSCP	Start DSCP	End DSCP
0	0	0	7
1	8	8	15
2	16	16	23
3	24	24	31
4	32	32	39
5	34	40	47
6	46	48	62
7	56	63	63

Add DSCP Exception

DSCP Exception

User Priority ▼

Add **Clear All**

DSCP Exception List

DSCP	UP	
48	0	▼
56	0	▼
46	6	▼
44	6	▼
40	5	▼
38	4	▼
36	4	▼
34	4	▼
32	5	▼
30	4	▼
28	4	▼
26	4	▼
24	4	▼
22	3	▼
20	3	▼
18	3	▼
16	0	▼
14	2	▼
12	2	▼
10	2	▼
8	1	▼

Fast lane

- When Fastlane is enabled on a WLAN, enabling AV automatically applies the AUTOQOS-AVC-PROFILE

WLANs > Edit 'WHOPPERWIFI'

General Security QoS Policy-Mapping Advanced

Quality of Service (QoS) Platinum (voice) ▾

Application Visibility Enabled

AVC Profile none ▾

Flex AVC Profile none ▾

Netflow Monitor none ▾

Fastlane Enable ▾

Override Per-User Bandwidth Contracts (kbps)

	DownStream	UpStream
Average Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Average Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>

Clear

Override Per-SSID Bandwidth Contracts (kbps)

WLANs > Edit 'WHOPPERWIFI'

General Security QoS Policy-Mapping Advanced

Quality of Service (QoS) Platinum (voice) ▾

Application Visibility Enabled

AVC Profile AUTOQOS-AVC-PROFILE ▾

Flex AVC Profile none ▾

Netflow Monitor none ▾

Fastlane Enable ▾

Override Per-User Bandwidth Contracts (kbps) ¹⁶

	DownStream	UpStream
Average Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Average Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>

Clear

Override Per-SSID Bandwidth Contracts (kbps) ¹⁶

Fast lane

- As long as Fastlane is enabled, you cannot (and should not) change the AVC Profile (you can disable/enable AV, but not change the AVC profile)

WLANs > Edit 'WHOPPERWIFI'

General Security QoS Policy-Mapping Advanced

Quality of Service (QoS)

Application Visibility Enabled

AVC Profile

Flex AVC Profile


Netflow Monitor

Fastlane

Override Per-User Bandwidth Contracts (kbps)

	DownStream	UpStream
Average Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Average Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>

Message from webpage

 Fastlane is enabled. Need to disable the Fastlane before doing configuration change in AVC Profile

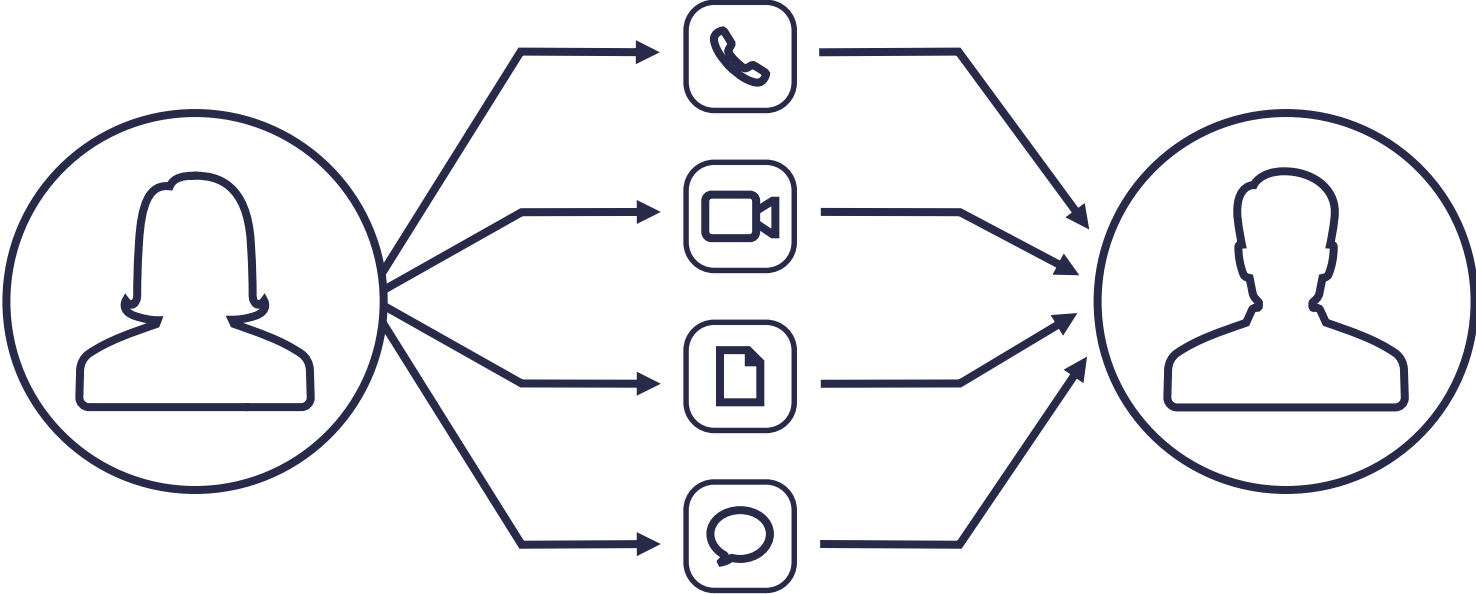
OK

Cisco Apple Partnership

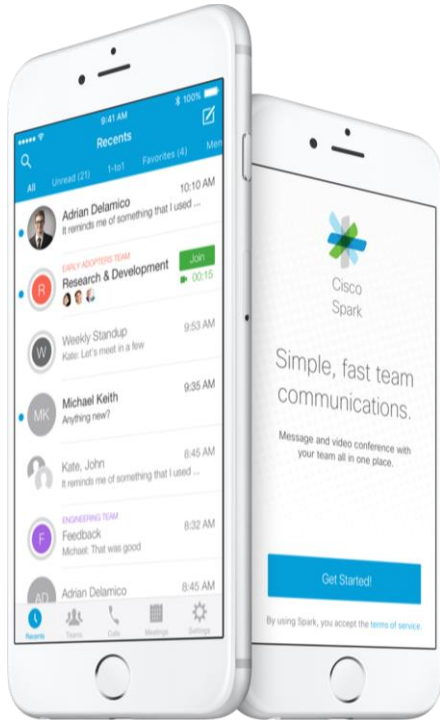
Spark Collaboration

Additional Information

Many Ways to Communicate



Seamless Collaboration with Cisco Spark



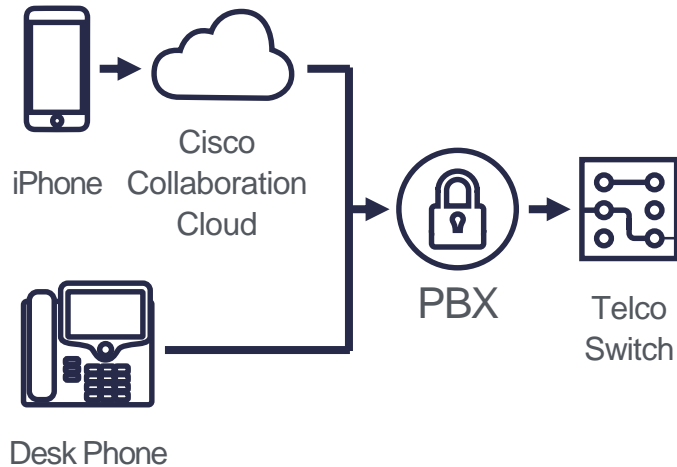
- Meet anywhere and everywhere
- Always-on, secure team messaging and file sharing
- Integrated business phone with
- HD voice and video calling

Native Voice Experience

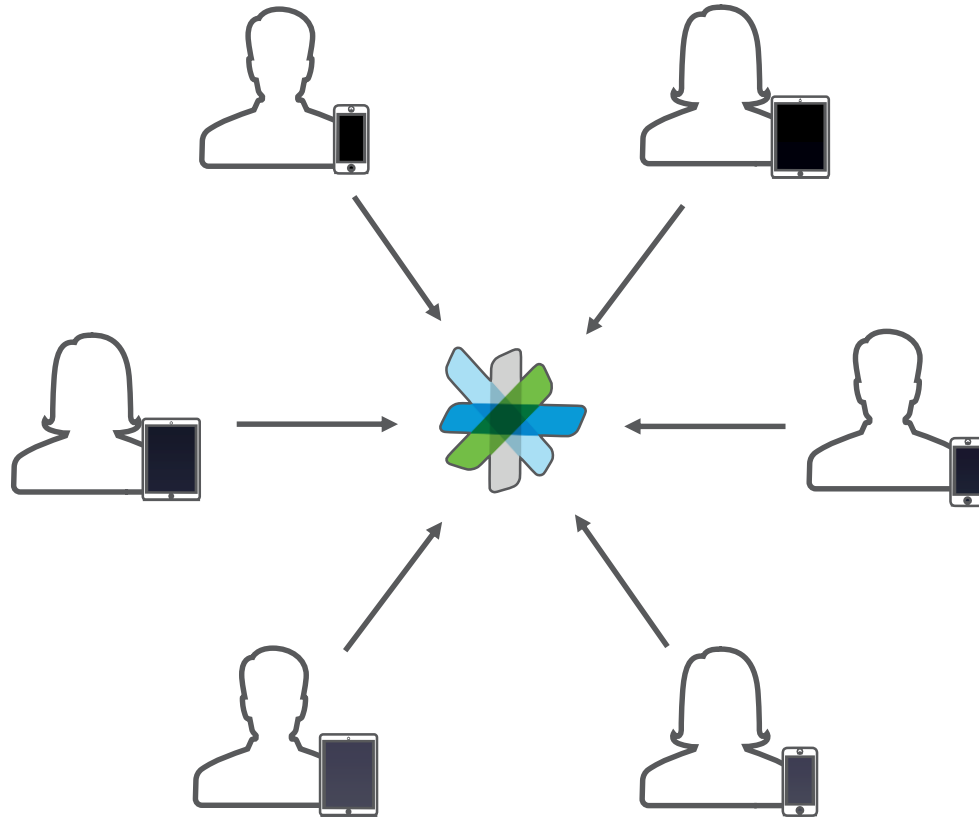


- New framework for integrated calling over IP
- Answer calls from the Lock screen
- Make voice or video calls from Contacts, Favorites, and Recents
- Make calls with Siri
- Switch seamlessly between VoIP and cellular calls
- Use connected headsets and accessories

Enterprise Voice Integration



- Users never miss a call
- Reliable, high-quality calling with reduced costs
- Improved compliance for calls made through the corporate PBX
- Accelerated user onboarding



Benefits of Voice and Collaboration

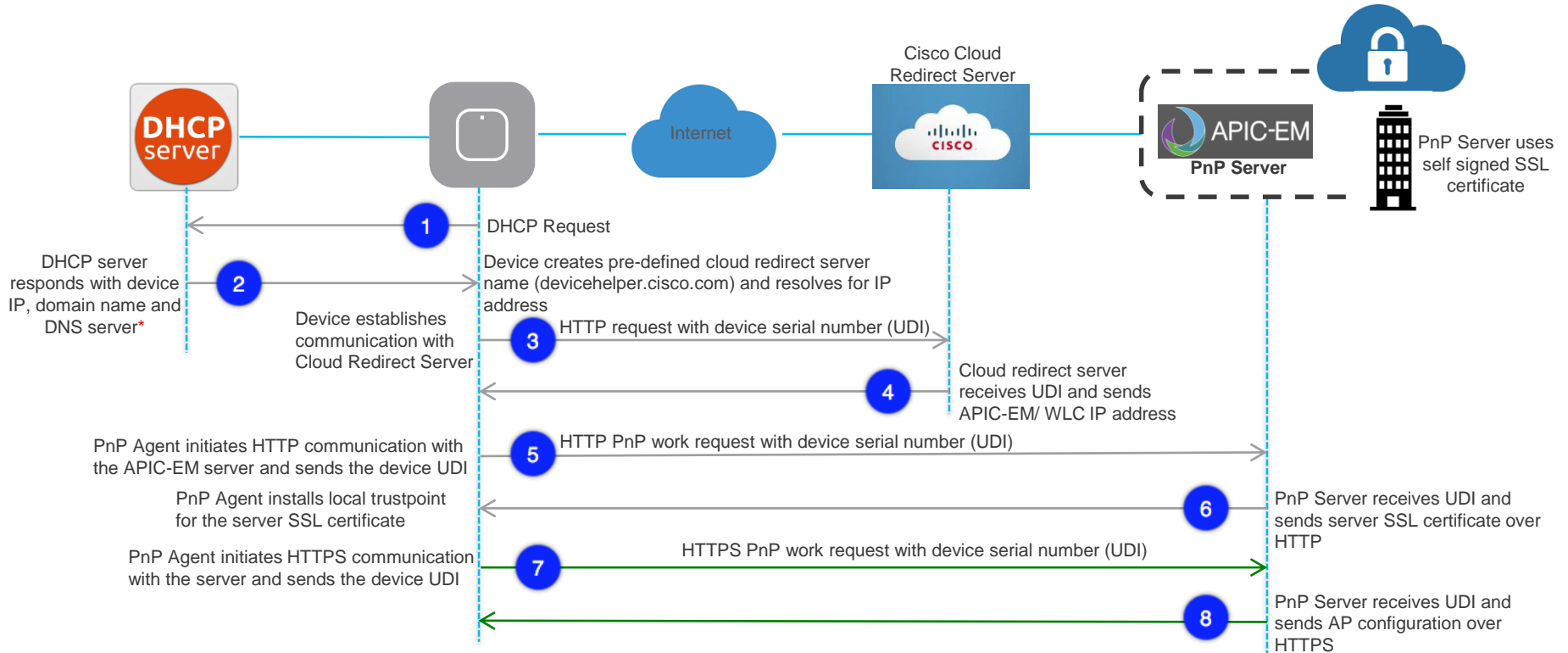


- Intuitive native user experience
- Extend existing investments to iOS devices and reduce calling costs
- Integrate into your existing telephony systems
- Expand collaboration tools beyond voice

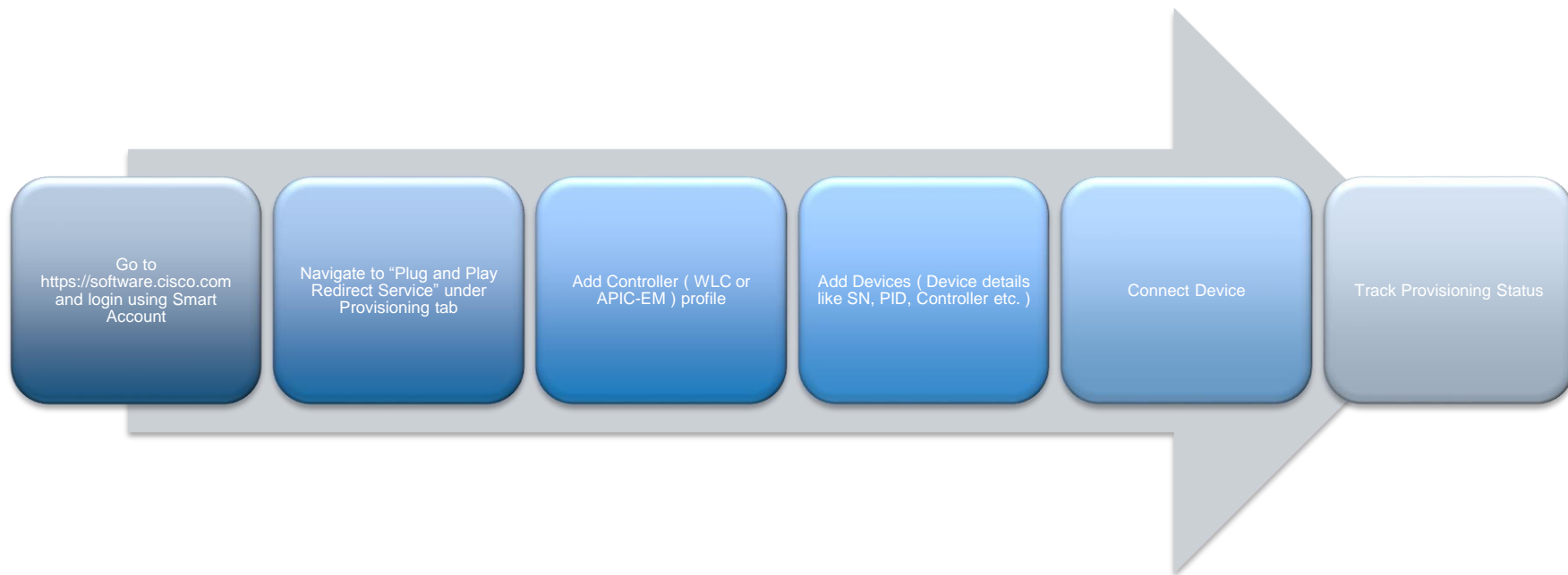
Network PnP with Public Cloud Redirect Setup Steps

Network PnP support Workflow

Cisco Cloud Redirect



Cisco Cloud Redirect Workflow



Cisco Software Central

Hello, [User] PnP Test Account

- [Home](#)
- [Order](#)
- [Download & Upgrades](#)
- [Provisioning](#)**
- [License](#)
- [Administration](#)

Download & Upgrade

Software Download

Download new software or updates to your current software

eDelivery

Get fast electronic fulfillment of software, licenses, and documentation

License

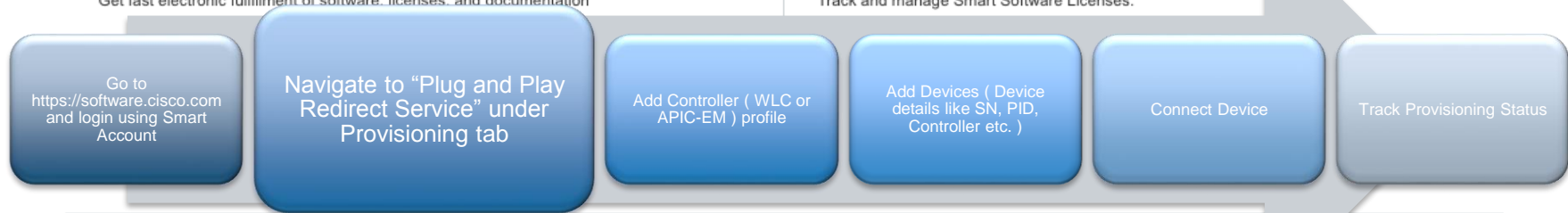
Traditional Licensing

Generate and manage PAK-based and other device licenses, including demo licenses

Smart Software Licensing

Track and manage Smart Software Licenses.

Plug and Play Redirect Service
[Device Redirect](#)



Setting Up Controller Profile

Cisco Software Central > Device Redirect

Device Redirect

Devices | Controller Profiles

Virtual Account: DEF

Add Profile...

Add Controller Profile

STEP 1

Profile Type

Conditional Steps

Choose the type of Profile to be created:

Controller Type:

APIC - EM
APIC - EM
WLC

Next

Go to <https://software.cisco.com> and login using Smart Account

Navigate to "Plug and Play Redirect Service" under Provisioning tab

Add Controller (WLC or APIC-EM) profile

Add Devices (Device details like SN, PID, Controller etc.)

Connect Device

Track Provisioning Status

Add Controller Profile

Add Controller (WLC or APIC-EM) profile

STEP 1 ✓

STEP 2

STEP 3

STEP 4

Add Controller Profile

STEP 1 ✓

Profile Type

STEP 2 ✓

Name and Controller Address

STEP 3

Review

STEP 4

Confirmation

Review the following options to make sure they are correct before you Submit the changes.

Add Controller Profile

STEP 1 ✓

Profile Type

STEP 2 ✓

Name and Controller Address

STEP 3 ✓

Review

STEP 4

Confirmation

✓ The controller profile "REMOTE_WLC" was successfully created.

Done

Setting Up Device Profile – Access Points

Cisco Software Central > Device Redirect

Hello, Trithanh Nguyen PnP Test Account

[Feedback](#) [Support](#) [Help](#)

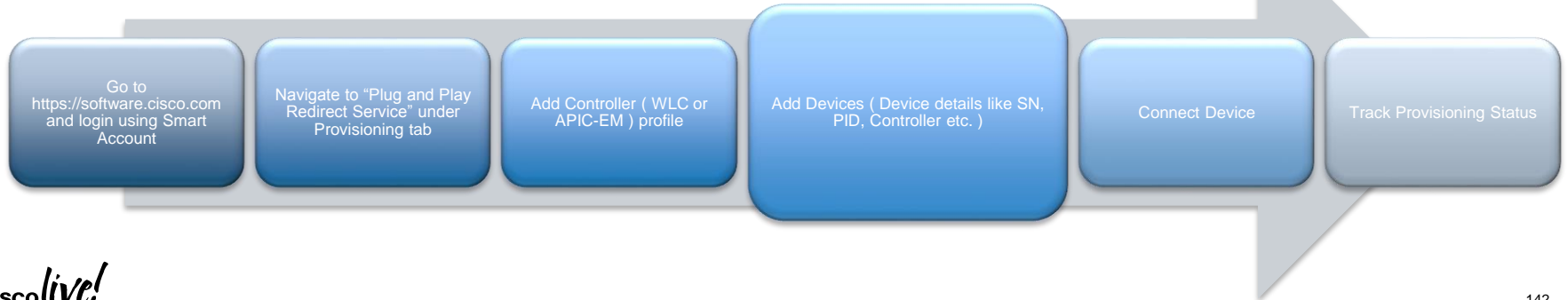
Device Redirect

Devices Controller Profiles

Virtual Account: **DEFAULT** ▾

[Add Profile...](#) [Edit...](#) [Delete](#) [Make Default](#) [Show Log](#)

<input type="checkbox"/>	Profile Name	Controller Type	Default	Description	Used By
<input type="checkbox"/>	REMOTE_WLC	WLC			0



Add Devices



STEP **1**
Identify Devices

STEP **2**
Validate

STEP **3**
Confirm

Add Devices (Device details like SN, PID, Controller etc.)

Add Devices



STEP **1** ✓

STEP **2** ✓

STEP **3**

Add Devices



STEP **1** ✓
Identify Devices

STEP **2** ✓
Validate

STEP **3** ✓
Confirm



Attempted to add 1 device(s).
1 device(s) have been added.
0 device(s) have errors and were not added.

It may take a few minutes for the new devices to show up in the Devices table. Please wait a minute or two and refresh the page as needed.

Done

APIC - Enterprise Module

Status | Sites | Image Management | Image Management | Unclaimed Devices

Site: Site1

Load Create Clone Delete

Deploy devices that Do not Support Cisco PnP Protocol (Unsecure)

Specify additional site information

Serial Number * Device Name * Product ID Add Rule Refresh

Serial Number	Device Name	Product ID	Config	Bootstrap	Image	Device Certificate	Details	Status	Delete
FTX1630GH7D	ap1	AIR-CAP	FTP1630GH7D-2.txt					PENDING	

10 Displaying 1 to 1 of 1 device First Previous 1 Next Last

Page loaded in 141ms

I wish this page would..

AP Pending to connect to APIC-EM server

APIC - Enterprise Module

Status | Sites | Image Management | Image Management | Unclaimed Devices

Site: Site1

Load Create Clone Delete

Deploy devices that Do not Support Cisco PnP Protocol (Unsecure)

Specify additional site information

Serial Number * Device Name * Product ID Add Rule Refresh

Serial Number	Device Name	Product ID	Config	Bootstrap	Image	Device Certificate	Details	Status	Delete
FTX1630GH7D	ap1	AIR-CAP	FTP1630GH7D-2.txt					PROVISIONED	

10 Displaying 1 to 1 of 1 device First Previous 1 Next Last

Page loaded in 141ms

I wish this page would..

AP Provisioned through APIC-EM server

Track Access Points on Controller

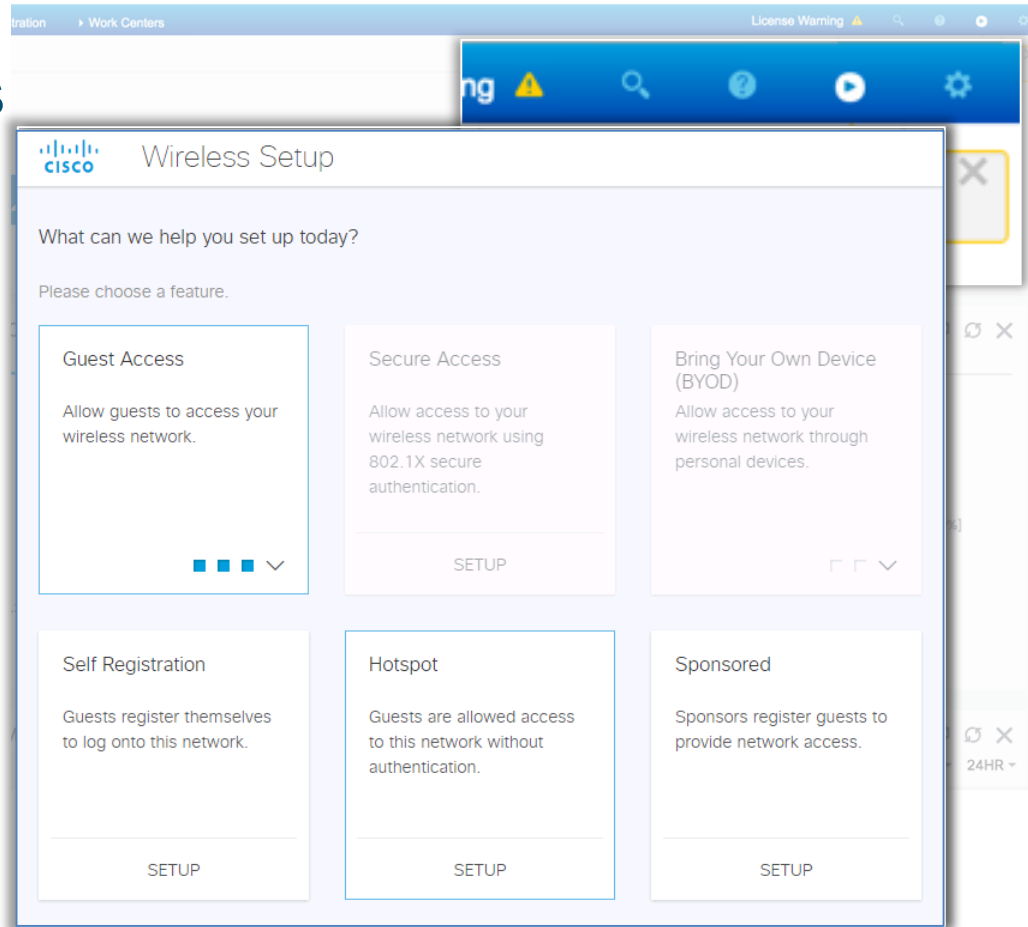
The screenshot shows the Cisco Wireless Controller interface. The top navigation bar includes tabs for MONITOR, WLANs, CONTROLLER, WIRELESS (selected), SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar shows the 'Wireless' section with a tree view for 'Access Points' (All APs, Radios) and other configuration options. The main content area is titled 'All APs' and shows a 'Current Filter' of 'None' with links to '[Change Filter]' and '[Clear Filter]'. Below this, it indicates 'Number of APs' as 2. A table lists the APs:

AP Name	IP Address(Ipv4/Ipv6)	AP Model	AP MAC
APfc5b_3963_1b68	10.10.10.184	AIR-CAP3702I-A-K9	fc:5b:39:63:1b:68
AP1832	10.10.10.108	AIR-AP1832I-B-K9	38:ed:18:ca:47:68

ISE 2.2 Xenia

Simplified Guest Workflow Configuration

Secure Guest in Few Steps



Easy Guest Hotspot Setup

Step 1 : Register the wireless LAN Controller

SETUP | HOTSPOT

1 Wireless LAN Controller

Register a Wireless LAN Controller.

WLC IP ADDRESS

2 10.1.100.61

3 USERNAME

admin

4 PASSWORD

SHARED SECRET

Register

Click **Register** and you should see a card for the WLC IP address.

SETUP | HOTSPOT

1 Wireless LAN Controller

Choose or register a Wireless LAN Controller.

2 REGISTER

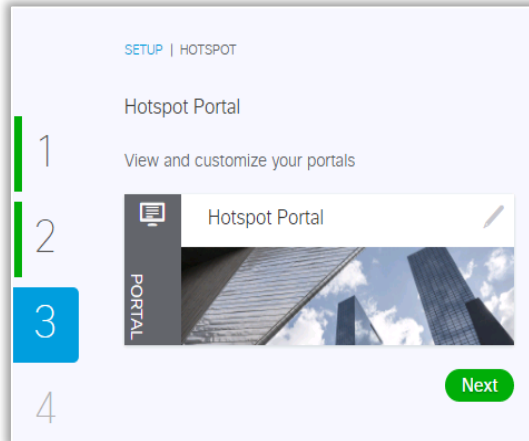
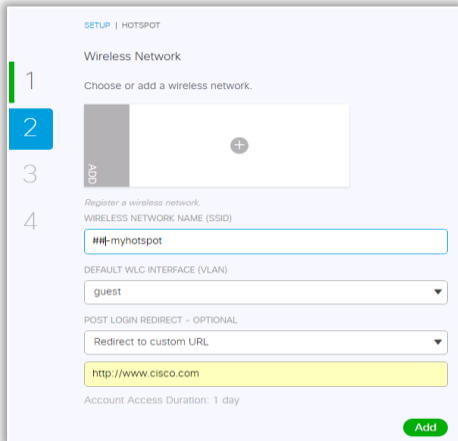
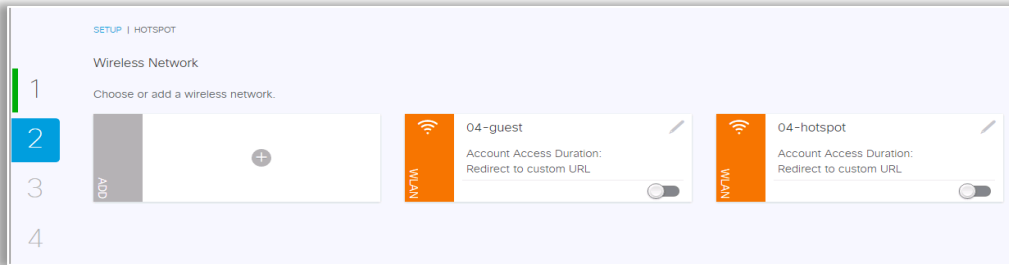
3 WLC

04-vWLC

IP address: 10.1.100.61

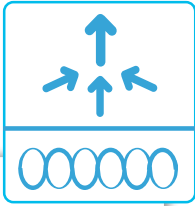
4 Next

Easy Guest Hotspot Setup



- Step 2 : Wizard shows any existing that could be used
- Or new WLANs can be created.
- Step 3 : Create and Customize Portal

Zero Touch WLC Config - Reference



Xenia automates WLC configuration without GUI or CLI, a significant time savings.

- **WLAN**
- **AAA Override**
- **Radius/ISE NAC**
- **RADIUS Servers**
- **CoA Enabled**
- **ACL (Pre-Auth)**

WLANs > Edit 'd-hotpot'

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security None

MAC Filtering

OEAP

Split Tunnel Enabled

Management Frame Protection (MFP)

MFP Client Protection Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1

802.11b/g/n (1 - 255) 1

NAC

NAC State ISE NAC

Access Control Lists

Enable Counters

Name

ACL_WEBAUTH_REDIRECT

WLANs > Edit 'd-hotpot'

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Select AAA servers below to override use of default servers on this WLAN

RADIUS Servers

RADIUS Server Overwrite interface Enabled

Authentication Servers

Accounting Servers

Server 1 IP:192.168.201.231, Port:1812 IP:192.168.201.231, Port:1813

Server 2 None None

A single workflow to achieve 100+ manual setup steps



Zero Touch ISE Config - Reference

ISE configuration is automated.

- **ISE Auth Policies**
- **Auth Profiles**
- **NAD Client**
- **Custom Portal**
- **Active Directory**

The screenshot displays the ISE configuration interface with several key components highlighted:

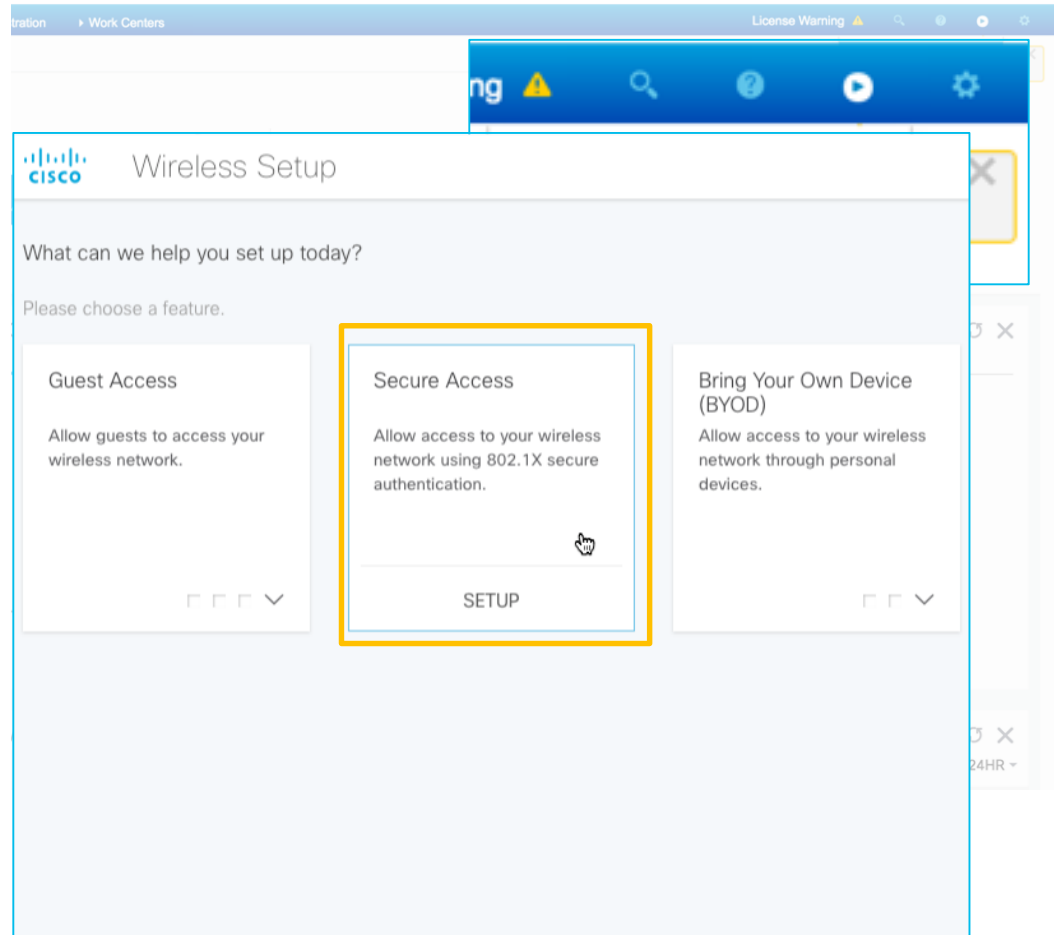
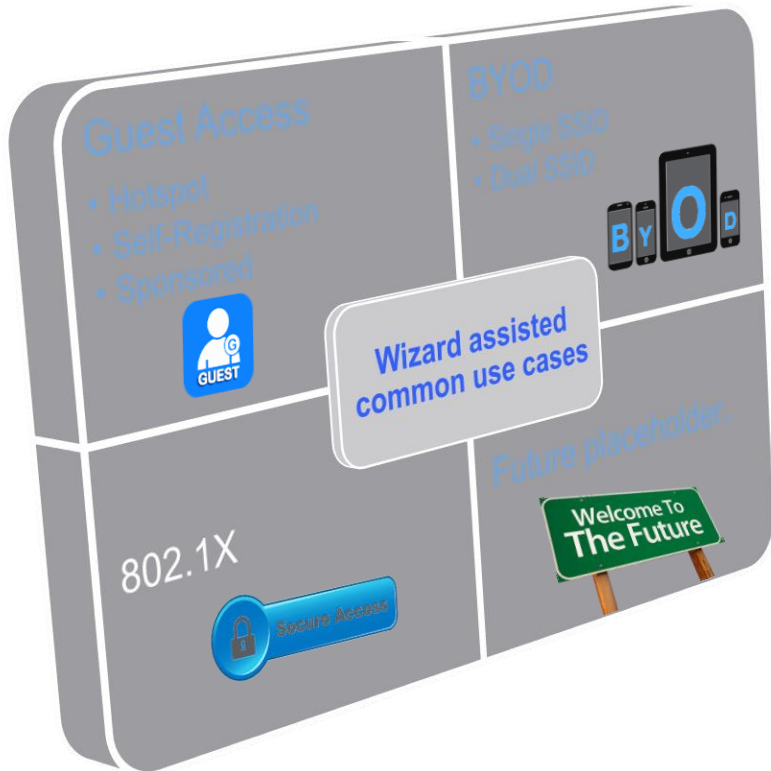
- Standard Authorization Profiles:** A table listing profiles such as 'test1231_Dot1xProfile', 'WS_1byod-240_BYOD Portal_Profile', and 'WS_1self-240_Self Registration Portal_GuestProfile'. A red box highlights the bottom two rows.
- Network Devices:** A table listing devices like 'NAD_192.168...' with IP/Mask and Profile Name columns. A red box highlights the first row.
- Authorization Policy:** A table listing rules such as 'Wireless Black List Default', 'Profiled Cisco IP Phones', and 'WS_d-hotspot_Hotspot Portal_GuestAccessPolicy'. A red box highlights the 'WS_d-hotspot_Hotspot Portal_RedirectPolicy' row.
- Guest Portals:** A section showing pre-defined portal types like 'Self-Registered Guest Portal (default)', 'Sponsored Guest Portal (default)', and 'WS_1self-240_Self Registration Portal'. A red box highlights the 'WS_1self-240_Self Registration Portal' entry.

Minimize user complexity and errors while maximizing time savings

ISE 2.2 Xenia

Simplified 802.1x Workflow Configuration

Secure Wireless in Few Steps



Secure Wireless in Few Steps

1

Choose or register a Wireless LAN Controller.

2/10 WLCs created

REGISTER

+

WLC

vWLC2

IP address: 10.10.20.22

WLC

WLC-5520

IP address: 10.10.40.10

2

3

Register a Wireless LAN Controller.

WLC IP ADDRESS

USERNAME

PASSWORD

SHARED SECRET

Register

4

SETUP | SECURE ACCESS

Wireless Network

Choose or add a wireless network. The wireless network you select will remain disabled until the end of your setup where you can 'Go Live.' 1/10 WLANs created

ADD

+

WLAN

My8021X

Register a wireless network.

WIRELESS NETWORK NAME (SSID)

DEFAULT WLC INTERFACE (VLAN)

management
▼

Add

1

2

3

4

SETUP | SECURE ACCESS

Active Directory

Choose or join an Active Directory (AD).

1/10 ADs created

1

2

3

NIOS

AD

Corporate AD

Domain: demo.local

4

ACTIVE DIRECTORY DOMAIN

domain.com

USERNAME

PASSWORD

Join



SETUP | SECURE ACCESS

You're All Set

Everything is set and ready to go. Wondering what configuration changes were made in ISE and on the Wireless Controller? [See for yourself.](#)

1

2

3

4



vWLC2

IP address: 10.10.20.22



My8021X



Corporate AD

Domain: demo.local

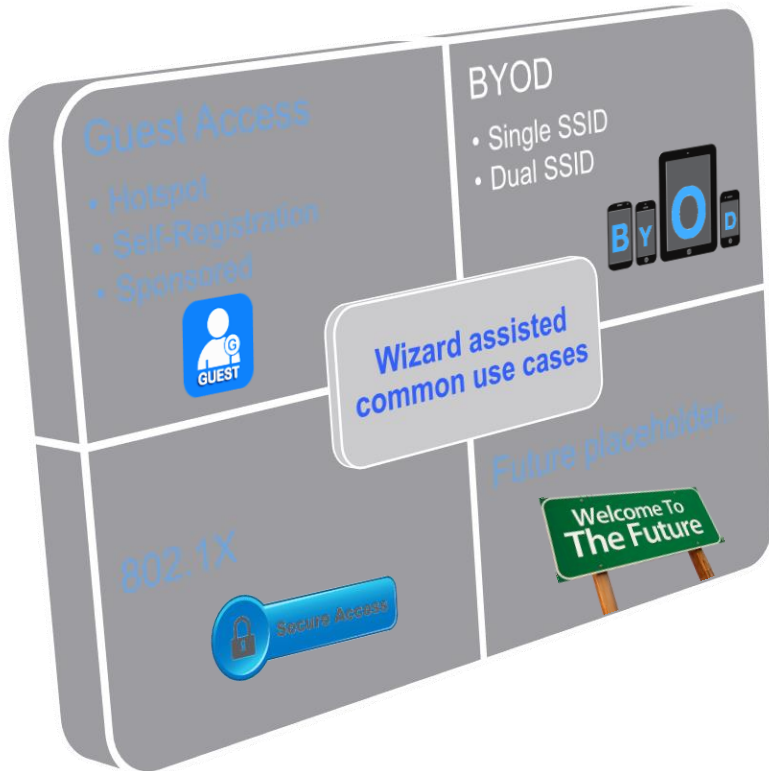


Go Live

ISE 2.2 Xenia

Simplified BYOD Workflow Configuration

Secure BYOD in Few Steps



Work Centers License Warning

Wireless Setup

What can we help you set up today?

Please choose a feature.

- Guest Access**
Allow guests to access your wireless network.
- Secure Access**
Allow access to your wireless network using 802.1X secure authentication.
- Bring Your Own Device (BYOD)**
Allow access to your wireless network through personal devices.
- Single SSID**
One SSID for onboarding and network connection.
- Dual SSID**
One SSID for onboarding and another SSID for network connection.

BYOD x 2

Secure BYOD in Few Steps



SETUP | BYOD SINGLE SSID

Wireless LAN Controller

Choose or register a Wireless LAN Controller.

2/10 WLCs created

1

2

3

4

5

REGISTER

+

WLC

WLC2

IP address: 10.10.20.22

WLC

WLC-5520

IP address: 10.10.40.10

Commit



SETUP | BYOD SINGLE SSID

Wireless Network

Choose or add a wireless network. The wireless network you select will remain disabled until the end of your setup where you can 'Go Live.' 1/10 WLANs created

- 1
- 2
- 3
- 4
- 5

ADD

+

WLAN

My8021X

Commit

SETUP | BYOD SINGLE SSID

Active Directory

Choose or join an Active Directory (AD).

1/10 ADs created

1

2

3

NIOF

+

AD

Corporate AD

Domain: demo.local

4 OVERRIDE DEFAULT VLAN SETTINGS - OPTIONAL

This will override the default WLC interface selected in the previous step.

1/2 overrides created

Type to filter and select employee groups

management ▼

[Add More Secure Employee Groups](#)

Commit

SETUP | BYOD SINGLE SSID

Customize Your BYOD Portals

Any visual customizations made in BYOD Portal will also be applied to the My Devices Portal.



Interested in creating a friendly URL for your My Devices Portal?

1. Create a custom URL, also known as a fully qualified domain name (FQDN).

2. To use your custom URL, update your DNS to ensure it resolves to your ISE IP addresses:

[Next](#)




SETUP | BYOD SINGLE SSID

You're All Set

Everything is set and ready to go. Wondering what configuration changes were made in ISE and on the Wireless Controller? [See for yourself.](#)


- 1
- 2
- 3
- 4
- 5




vWLC2
IP address: 10.10.20.22



My8021X



Corporate AD
Domain: demo.local



BYOD Portal



TEST PORTAL



My Devices Portal



LIVE PORTAL

Go Live

Wireless TrustSec Configuration



Wireless TrustSec – How to Setup



Basic infrastructure setup – Certificates, Active Directory integration, etc.



Create **Security Group Tags** to be used in the network



Setup **Network Device Admission Control** - NDAC



Define Authentication and **Authorization policies** for Users and Devices



Configure **SGACL & Egress Policies**

Security Group Tags in ISE




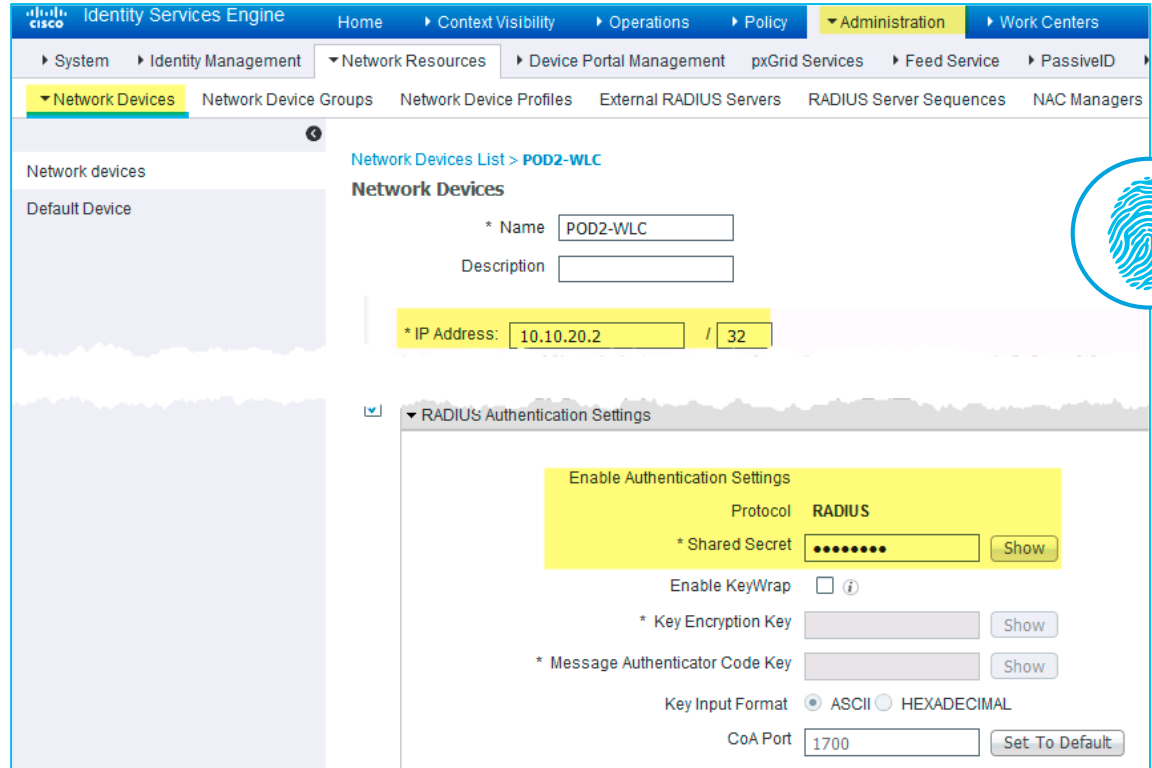
Define SGTs under 'Components' section in **TrustSec Work Center** (ISE 2.0 and above)

The screenshot displays the Cisco Identity Services Engine (ISE) interface, specifically the TrustSec Work Center. The navigation menu includes Home, Operations, Policy, Guest Access, Administration, and Work Centers. The 'TrustSec' section is expanded to show Overview, Authentication Policy, Authorization Policy, Components, Policy, SXP, Reports, and Settings. The 'Components' section is selected, and the 'Security Groups' page is displayed. The page title is 'Security Groups' and it includes a link for Policy Export: 'For Policy Export go to Administration > System > Backup & Restore > Policy Export Page'. The main content area shows a table of Security Groups with columns for Icon, Name, SGT (Dec / Hex), and Description. The table lists several groups, including Contractors, Employee_BYOD, Employee_FullAccess, Mail_Servers, PCI_Devices, TrustSec_Infra_SGT, Unknown, Unregist_Dev_SGT, and Web_Servers. A red box highlights the table content.

Icon	Name	SGT (Dec / Hex)	Description
<input type="checkbox"/>	Contractors	30/001E	Contractors User Group
<input type="checkbox"/>	Employee_BYOD	20/0014	Employees with Personal Assets
<input type="checkbox"/>	Employee_FullAccess	10/000A	Employees with Corporate Assets
<input type="checkbox"/>	Mail_Servers	120/0078	Email Servers
<input type="checkbox"/>	PCI_Devices	100/0064	Point-of-Sales (POS) terminals and PCI Servers
<input type="checkbox"/>	TrustSec_Infra_SGT	2/0002	Network Device SGT
<input type="checkbox"/>	Unknown	0/0000	Unknown Security Group
<input type="checkbox"/>	Unregist_Dev_SGT	255/00FF	Unregistered BYOD Devices
<input type="checkbox"/>	Web_Servers	110/006E	Web Servers

Define WLC in the 'Network Devices'

- The Network Devices, e.g. Wireless controllers, needs to be defined here. 



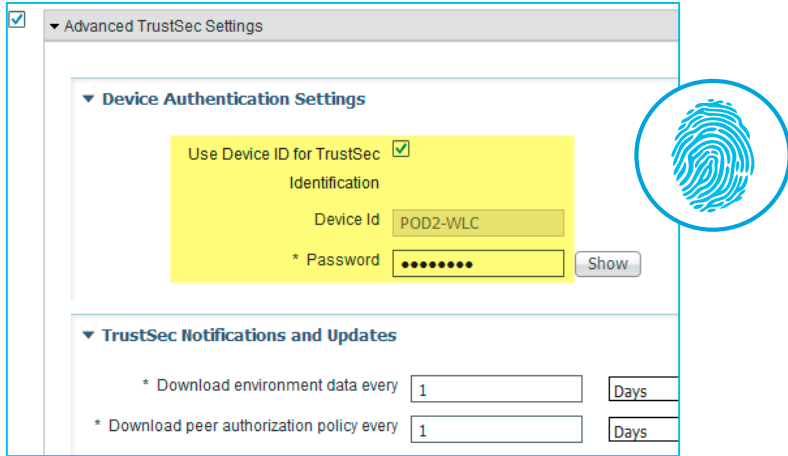
The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The breadcrumb navigation path is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Network Resources > Device Portal Management > pxGrid Services > Feed Service > PassiveID > Network Devices. The 'Network Devices' section is active, showing a list of devices with 'POD2-WLC' selected. The configuration form for 'POD2-WLC' includes the following fields:

- * Name:
- Description:
- * IP Address: /
- RADIUS Authentication Settings
 - Enable Authentication Settings:
 - Protocol: **RADIUS**
 - * Shared Secret:
 - Enable KeyWrap:
 - * Key Encryption Key:
 - * Message Authenticator Code Key:
 - Key Input Format: ASCII HEXADECIMAL
 - CoA Port:



Configure parameters for TrustSec

- In addition to RADIUS secret, check 'Advanced Trustsec Settings' and 'Use Device ID for Trustsec', then type device password.



Advanced TrustSec Settings

Device Authentication Settings

Use Device ID for TrustSec

Identification

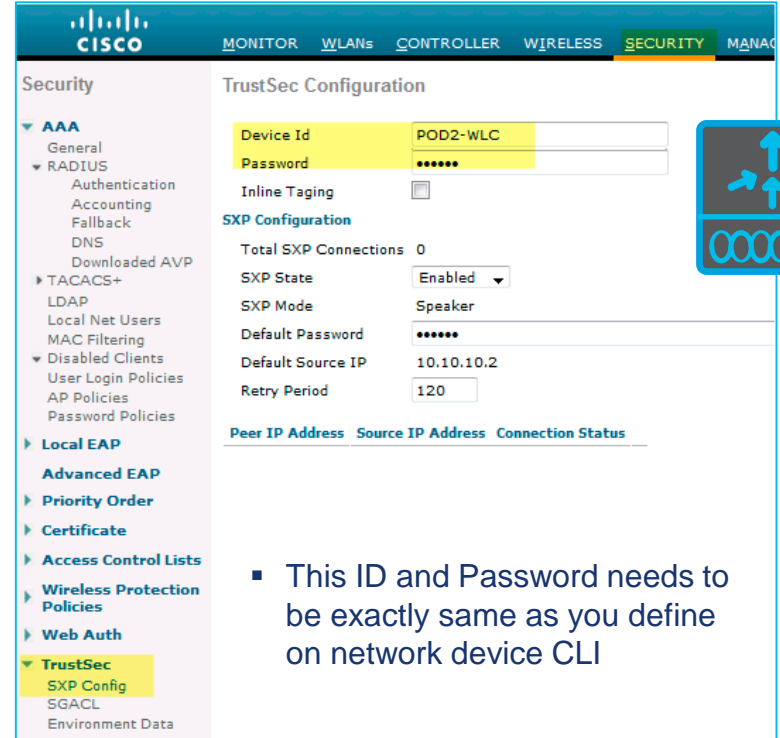
Device Id: POD2-WLC

* Password: [masked]

TrustSec Notifications and Updates

* Download environment data every: 1 Days

* Download peer authorization policy every: 1 Days



Security

TrustSec Configuration

Device Id: POD2-WLC

Password: [masked]

Inline Tagging:

SXP Configuration

Total SXP Connections: 0

SXP State: Enabled

SXP Mode: Speaker

Default Password: [masked]

Default Source IP: 10.10.10.2

Retry Period: 120

Peer IP Address | Source IP Address | Connection Status

Advanced EAP

Priority Order

Certificate

Access Control Lists

Wireless Protection Policies

Web Auth

TrustSec

SXP Config

SGACL

Environment Data

- This ID and Password needs to be exactly same as you define on network device CLI

Define authorization policies for Users and Devices



802.1X / MAB / Web
Authentication policy
to assign SGTs to the
Users and Devices



The screenshot shows the Cisco Identity Services Engine (ISE) web interface for configuring an Authorization Policy. The breadcrumb navigation is: Home > Operations > Policy > Guest Access > Administration. The main menu includes Authentication, Authorization, Profiling, Posture, Client Provisioning, and Policy Elements. The 'Authorization Policy' section is active, with a description: 'Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page'. A dropdown menu is set to 'First Matched Rule Applies'. Under 'Exceptions (0)', there is a 'Standard' section with a table of rules:

Status	Rule Name	Conditions (identity groups and other conditions)
<input checked="" type="checkbox"/>	Employee Access	if Any and AD_Group_Employee AND Wired...
<input checked="" type="checkbox"/>	Default	if no matches, then DenyAccess

At the bottom are 'Save' and 'Reset' buttons. On the right, a 'Security Group' list is visible, containing: Contractors, Employee_BYOD, Employee_FullAccess, Mail_Servers, PCI_Devices, TrustSec_Infra_SGT, Unknown, Unregist_Dev_SGT, and Web_Servers. A red box highlights the 'Employee_BYOD' through 'Web_Servers' items. Below the list is a 'Select an item' dropdown menu.

Configure Security Group ACLs

Configure SGACLs first to be referenced under the Egress policy later



The screenshot shows the Cisco Identity Services Engine (ISE) configuration page for Security Group ACLs. The breadcrumb navigation is: Home > Operations > Policy > Guest Access > Administration > Work Centers > TrustSec > Components > Policy. The left sidebar contains a tree view with 'Security Groups', 'Security Group ACLs', 'Network Devices', and 'Trustsec AAA Servers'. The main content area is titled 'Security Group ACLs' and shows the configuration for 'Permit_Email_Traffic'. The configuration includes:

- Name: Permit_Email_Traffic
- Description: Access control policy to permit Email service
- IP Version: Agnostic (selected)
- Security Group ACL content:

```
permit tcp dst eq 110
permit tcp dst eq 143
permit tcp dst eq 25
permit tcp dst eq 465
permit tcp dst eq 585
permit tcp dst eq 993
permit tcp dst eq 995
deny all log
```

A blue circular fingerprint icon is overlaid on the right side of the configuration area.

Configure parameters for TrustSec

- In addition to RADIUS secret, check 'Advanced Trustsec Settings' and 'Use Device ID for TrustSec', then type device password.

Advanced TrustSec Settings

▼ Device Authentication Settings

Use Device ID for TrustSec

Identification

Device Id

* Password

▼ TrustSec Notifications and Updates

* Download environment data every

* Download peer authorization policy every

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGE

Security

▼ AAA

General

▼ RADIUS

Authentication

Accounting

Fallback

DNS

Downloaded AVP

▶ TACACS+

LDAP

Local Net Users

MAC Filtering

▼ Disabled Clients

User Login Policies

AP Policies

Password Policies

▶ Local EAP

Advanced EAP

▶ Priority Order

▶ Certificate

▶ Access Control Lists

▶ Wireless Protection Policies

▶ Web Auth

▼ TrustSec

SXP Config

SGACL

Environment Data

TrustSec Configuration

Device Id

Password

Inline Tagging

SXP Configuration

Total SXP Connections 0

SXP State

SXP Mode

Default Password

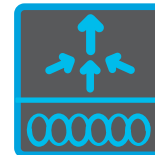
Default Source IP

Retry Period

Peer IP Address Source IP Address Connection Status

- This ID and Password needs to be exactly same as you define on network device CLI

TrustSec WLAN Configuration



General Security QoS Policy-Mapping **Advanced**

Layer 2 Layer 3 **AAA Servers**

Select AAA servers below to override use of default servers on this WLAN

RADIUS Servers

RADIUS Server Overwrite interface Enabled
Apply Cisco ISE Default Settings Enabled

Authentication Servers **Accounting Servers**

Server	IP:Port	IP:Port
Server 1	<input checked="" type="checkbox"/> Enabled IP:10.10.105.20, Port:1812	<input checked="" type="checkbox"/> Enabled IP:10.10.105.20, Port:1813
Server 2	None	None

General Security QoS Policy-Mapping **Advanced**

Allow AAA Override Enabled

Coverage Hole Detection Enabled

Enable Session Timeout 1800
Session Timeout (secs)

Aironet IE Enabled

Diagnostic Channel Enabled

Override Interface ACL IPv4 IPv6

Layer2 Acl

URL ACL

P2P Blocking Action

Client Exclusion Enabled 60
Timeout Value (secs)

Maximum Allowed Clients

Static IP Tunneling Enabled

DHCP

DHCP Server Override

DHCP Addr. Assignment Required

OEAP

Split Tunnel Enabled

Management Frame Protection (MFP)

MFP Client Protection

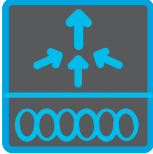
DTIM Period (in beacon intervals)

802.11a/n (1 - 255)	<input type="text" value="1"/>
802.11b/g/n (1 - 255)	<input type="text" value="1"/>

NAC

NAC State

TrustSec Policy Downloaded on WLC



CISCO MONITOR WLANs CONTROLLER WIRELESS **SECURITY** MANAGEMENT COMMANDS HELP FEEDBACK

Security

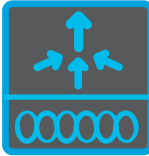
- AAA
 - General
 - RADIUS
 - Authentication
 - Accounting
 - Fallback
 - DNS
 - Downloaded AVP
 - TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
 - Disabled Clients
 - User Login Policies
 - AP Policies
 - Password Policies
 - Local EAP
 - Advanced EAP
 - Priority Order
 - Certificate
 - Access Control Lists
 - Wireless Protection Policies
 - Web Auth
 - TrustSec**
 - General
 - SXP Config
 - Policy

SGT-TAG List Entries 1 - 2 of 2

Total SGT Authorization Policy count 2

SGT	Generation Id	Policy Download Status	Number of clients with this SGT	Reference count APs	Refresh Period(seconds)	Time Remaining to Refresh(seconds)	Number of RBACLs for DGT
4	02	Success	1	1	86400	84357	2
5	02	Success	1	1	86400	84740	1

SG-ACL enforcement



MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Home

All APs > Details for AP58ac.78de.8ae8

< Back Apply

General Credentials Interfaces High Availability Inventory **Advanced**

Regulatory Domains 802.11bg:-A 802.11a:-B
Country Code US (United States)
Cisco Discovery Protocol
AP Group Name default-group
Statistics Timer 30
Data Encryption
Rogue Detection
Telnet Global Config
SSH Global Config
TCP Adjust MSS (IPv4: 536 - 1363, IPv6: 1220 - 1331)
LED State Enable
LED Flash State 0 (1-3600)seconds Indefinite Disable

Hyperlocation Configuration
Enable Hyperlocation Global Config
Link Latency
Enable Link Latency
AP Image Download
Perform a primary image pre-download on this AP
Perform a backup image pre-download on this AP
Perform an interchange of both the images on this AP
Perform an abort of predownload on this AP

Power Over Ethernet Settings
Pre-standby Power
AP Core Download
AP Core Settings
AP Retransmission
AP Retransmission
VLAN Tagging
VLAN Tagging
mDNS Configuration
mDNS Configuration
VLAN Settings
AP Virtual
Override
Trusted Security
TrustSec

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Wireless

All APs > AP58ac.78de.8ae8 > Trusted Security

AP Name AP58ac.78de.8ae8
Base Radio MAC cc:16:7e:30:47:d0

Trusted Security

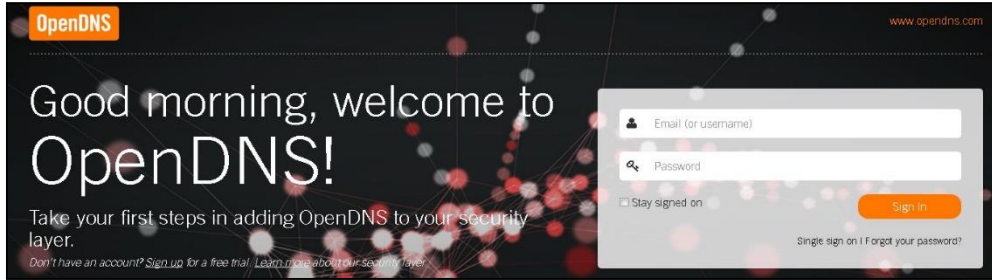
Sgac1 Enforcement

1. Inline tagging is supported in only Flex mode AP (Applicable to 11ac AP)
2. SXPv4(Listener/Speaker/Both) is supported in Flex, Flex+bridge AP (Applicable to 11ac AP)

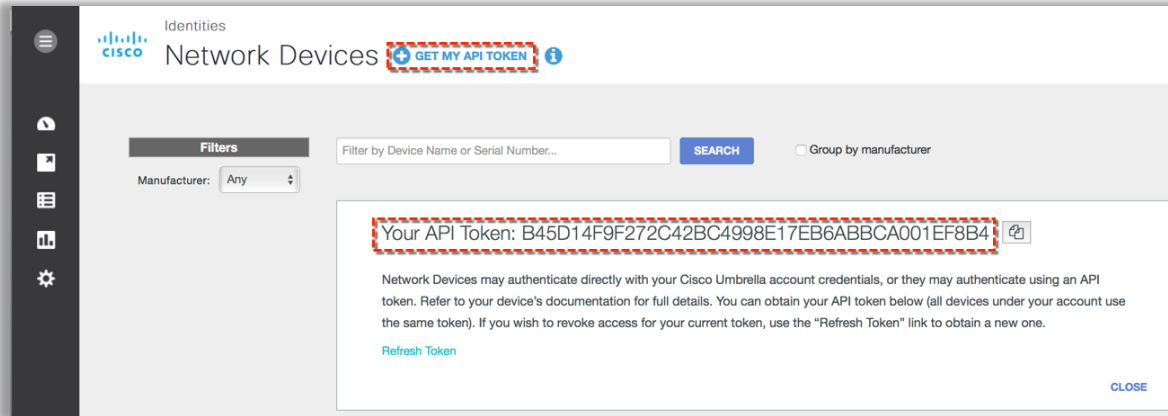
Access Points
All APs
Radios
802.11a/n/ac
802.11b/g/n
Dual-Band Radios
Global Configuration
Advanced
Mesh
ATF
RF Profiles
FlexConnect Groups
FlexConnect ACLs
FlexConnect VLAN
Templates
QoS ACLs

OpenDNS configuration and setup

OpenDNS – Account Setup



Create an OpenDNS account with active subscription license.



Obtain API-Token from dashboard to be used on WLC

OpenDNS - Profile Creation on WLC

Configure OpenDNS

Configure API Token

Create Profiles

Map Profile to WLAN/AP Group/Local Policy

Enable OpenDNS on WLC
Security > OpenDNS

OpenDNS

Global Configuration

OpenDNS Global Status



OpenDns-APIToken

B45D14F9F272C42BC4998E17EB6ABBCA001EF8B4

Create two profiles – for employee and contractor roles

Profile

Profile Name

Add

[Profile Mapped Summary](#)

Profile Name

Opendns-Identity

WLC-5520_employeeOD

Not Applicable

WLC-5520_contractorOD

Not Applicable

Category Based Filtering on OpenDNS

Cisco Umbrella

Cisco Systems

Overview

Identities >

Policies >

Policy List

POLICY COMPONENTS

- Destination Lists
- Content Categories
- Security Settings

BLOCK PAGE SETTINGS

- Block Page Appearance
- Bypass Users
- Bypass Codes
- Root Certificate

Reporting >

Settings >

1 contractorPolicy

Impacting 3 Identities | Category Setting contractorCategory | Security Setting Default Settings

1. Select Identities | 2. Select Policy Settings | 3. Select Block Page Settings | 4. Set Policy Details

Category setting to enforce: contractorCategory

Security setting to enforce: Default Settings

Destination lists to enforce: Select from existing destination list

- Global Block List
- Global Allow List

DELETE POLICY

2 EmployeePolicy

1. Select Identities

Category setting to enforce: employeeCategory

Security setting to enforce: Default Settings

Destination lists to enforce: Select from existing destination list

- Global Block List
- Global Allow List

Edit Category Setting

High
Blocks adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters.

Moderate
Blocks all adult-related websites and illegal activity.

Low
Blocks pornography.

None

Custom

<input type="checkbox"/>	Academic Fraud
<input checked="" type="checkbox"/>	Adult Themes
<input checked="" type="checkbox"/>	Adware
<input type="checkbox"/>	Alcohol
<input type="checkbox"/>	Anime/Manga/Webcomic
<input type="checkbox"/>	Auctions
<input type="checkbox"/>	Automotive
<input type="checkbox"/>	Blogs
<input type="checkbox"/>	Business Categories

add new destination list

<input checked="" type="checkbox"/>	block	⊕
<input checked="" type="checkbox"/>	allow	⊕

REVIEW | NEXT | SAVE

Category Setting contractorCategory | Security Setting Default Settings

4. Set Policy Details

add new destination list

<input checked="" type="checkbox"/>	block	⊕
<input checked="" type="checkbox"/>	allow	⊕

SAVE

Support

OpenDNS Reporting – Security Overview



Cisco Umbrella

Cisco Systems

Reporting

Security Overview

Activity Search

REPORTS

Security Activity

Cloud Services

Total Requests

Activity Volume

Top Domains

Top Categories

Top Identities

My Reports

Exported Reports

Scheduled Reports

Admin Audit Log

Reporting

Security Overview



LAST 30 DAYS

Security

Reporting

Activity Search



Activity Search - All Identities - All Destinations - All IPs - All Responses - Nov. 04, 2016 12:00AM - Nov. 05, 2016 12:00AM (UTC-07:00 Change time zone) - All Categories - 2 Security Categories

Filters

Filter by Identity:

Select an identity...

Filter by Destination:

Enter a Domain or IP

Filter by Source IP:

Enter an Internal or External IP

Include all traffic

Filter by Response:

All Responses

Filter by date:

Custom Date Range...

From: To:

Nov. 4, 2016 Nov. 5, 2016

12:00am 12:00am

Date	Time	Destination	Record	Category	Identity	External IP	Internal IP
Nov. 04, 2...	6:35:44 AM	nytimes.com	A	Malware	Unidentified L...	64.103.25...	N/A
Nov. 04, 2...	6:35:44 AM	nytimes.com	A	Malware	Unidentified L...	64.103.25...	N/A
Nov. 04, 2...	6:35:43 AM	nytimes.com	A	Malware	Unidentified L...	64.103.25...	N/A
Nov. 04, 2...	2:14:20 AM	ccn.com	A	Malware	Unidentified L...	64.103.25...	N/A

- ✓ Visualize security activity in real time with aggregated reports.
- ✓ Schedule and get reports to your inbox.
- ✓ Pinpoint infected device or user targeted by advanced attacks to reduce time to remediation

OpenDNS Reporting – Activity Search



Activity Search - All Identities - All Destinations - All IPs - Include all traffic - Blocked - Last 7 Days (UTC-08:00 Change time zone) - All Categories - All Security Categories

Filters

Filter by Identity:
Select an identity...

Filter by Destination:
Enter a Domain or IP

Filter by Source IP:
Enter an Internal or External IP

Include all traffic

Filter by Response:
Blocked

Filter by date:
Last 7 Days

Filter by Categories: CHOOSE

Filter by Security Categories: CHOOSE

RUN REPORT

Date	Time		Destination	Record	Category	Identity	External IP	Internal IP
Nov. 22, 2016	4:53:56 PM	🚫	mobile.brill.com	A	Adware, Software/Techno...	WLC-5520_empl...	128.107.234.4	N/A
Nov. 22, 2016	4:53:56 PM	🚫	espn.go.com	A	Games, News/Media, Tel...	WLC-5520_empl...	128.107.234.4	N/A
Nov. 22, 2016	1:45:37 PM	🚫	geo-um.brill.com	A	Adware, Software/Techno...	WLC-5520_empl...	128.107.234.4	N/A
Nov. 22, 2016	1:45:14 PM	🚫	geo-um.brill.com	A	Adware, Software/Techno...	WLC-5520_empl...	128.107.234.4	N/A
Nov. 22, 2016	1:45:12 PM	🚫	xp.apple.com	A	Movies, Software/Technol...	WLC-5520_empl...	128.107.234.4	N/A
Nov. 22, 2016	1:45:12 PM	🚫	client-api.tunes.apple.com	A	Movies, Software/Technol...	WLC-5520_empl...	128.107.234.4	N/A
Nov. 22, 2016	1:45:04 PM	🚫	ebay.com	A	Auctions, Ecommerce/Sh...	WLC-5520_empl...	128.107.234.4	N/A
Nov. 22, 2016	1:43:46 PM	🚫	espn.go.com	A	Games, News/Media, Tel...	WLC-5520_empl...	128.107.234.4	N/A
Nov. 22, 2016	1:43:34 PM	🚫	www.disney.com	A	Games, Television, Travel	WLC-5520_empl...	128.107.234.4	N/A
Nov. 22, 2016	1:43:30 PM	🚫	porn.com	A	Adult Themes, Nudity, Po...	WLC-5520_empl...	128.107.234.4	N/A
Nov. 22, 2016	1:43:23 PM	🚫	play.google.com	A	Ecommerce/Shopping, G...	WLC-5520_empl...	128.107.234.4	N/A
Nov. 22, 2016	1:43:22 PM	🚫	itunes.apple.com	A	Movies, Software/Technol...	WLC-5520_empl...	128.107.234.4	N/A
Nov. 22, 2016	1:42:13 PM	🚫	www.icloud.com	A	File Storage, Software/Te...	WLC-5520_contr...	128.107.234.4	N/A
Nov. 22, 2016	1:42:03 PM	🚫	l.co	A	URL Shortener	WLC-5520_contr...	128.107.234.4	N/A
Nov. 22, 2016	1:42:03 PM	🚫	analytics.twitter.com	A	Social Networking	WLC-5520_contr...	128.107.234.4	N/A
Nov. 22, 2016	1:42:03 PM	🚫	connect.facebook.net	A	Social Networking	WLC-5520_contr...	128.107.234.4	N/A
Nov. 22, 2016	1:41:41 PM	🚫	itunes.apple.com	A	Movies, Software/Technol...	WLC-5520_contr...	128.107.234.4	N/A
Nov. 22, 2016	1:41:41 PM	🚫	connect.facebook.net	A	Social Networking	WLC-5520_contr...	128.107.234.4	N/A
Nov. 22, 2016	1:41:26 PM	🚫	www.disney.com	A	Games, Television, Travel	WLC-5520_contr...	128.107.234.4	N/A
Nov. 22, 2016	1:41:09 PM	🚫	timesofindia.indiatimes.com	A	News/Media	WLC-5520_contr...	128.107.234.4	N/A
Nov. 22, 2016	1:41:06 PM	🚫	ping.chartbeat.net	A	Ecommerce/Shopping, B...	WLC-5520_contr...	128.107.234.4	N/A
Nov. 22, 2016	1:41:04 PM	🚫	storage.cloud.kargo.com	A	News/Media	WLC-5520_contr...	128.107.234.4	N/A
Nov. 22, 2016	1:40:58 PM	🚫	connect.facebook.net	A	Social Networking	WLC-5520_contr...	128.107.234.4	N/A
Nov. 22, 2016	1:40:48 PM	🚫	sync.adaptv.advertising.com	A	Video Sharing, Business ...	WLC-5520_contr...	128.107.234.4	N/A

- ✓ Activity Search Filter by Response for Blocked, Allowed, Proxy
- ✓ Filter by time – Last 24 hours, today, yesterday, last 7 days, last 30 days
- ✓ Detail on activity eg. Which OpenDNS policy blocked sites

Detailed Reporting Options



Cisco Umbrella

Cisco Systems

Overview

Identities

Policies

Reporting

Security Overview

Activity Search

REPORTS

- Security Activity
- Cloud Services
- Total Requests
- Activity Volume
- Top Domains
- Top Categories
- Top Identities

My Reports

Exported Reports

Scheduled Reports

Admin Audit Log

Settings

Support

Setup Guide

Reporting / Reports

Total Requests

AI AI

Total Requests - All Identities - Last 24 hours (UTC-08:00 [Change time zone](#))

Filters

Filter by identity:

Select an identity...

Filter by date:

Last 24 Hours

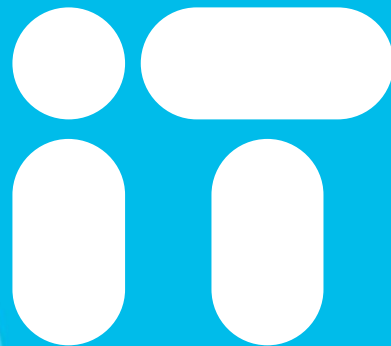
RUN REPORT

Time	Total Requests
11/21 1:00:00	0
11/21 2:00:00	0
11/21 2:22:00	0
11/22 0:00:00	0
11/22 0:02:00	0
11/22 0:04:00	0
11/22 0:06:00	0
11/22 0:08:00	0
11/22 10:00	0
11/22 12:00	900
11/22 14:00	0
11/22 16:00	0

- ✓ Reports for Cloud Services, Top Request, Activity Volume, Top Domains, Top Categories, Top Identities
- ✓ Service Details including % Allowed, % Blocked, First Seen, Last Seen, Identities, number of requests to a particular Cloud Service



You're



Cisco *live!*