
cisco
Cisco live!
July 10–14, 2016 · Las Vegas, NV
Your Time Is Now

Best Practices for Configuring Cisco Wireless LAN Controllers

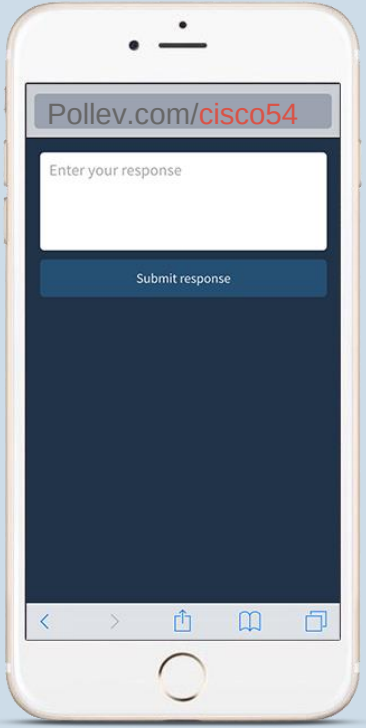
Aparajita Sood

Technical Marketing Engineer

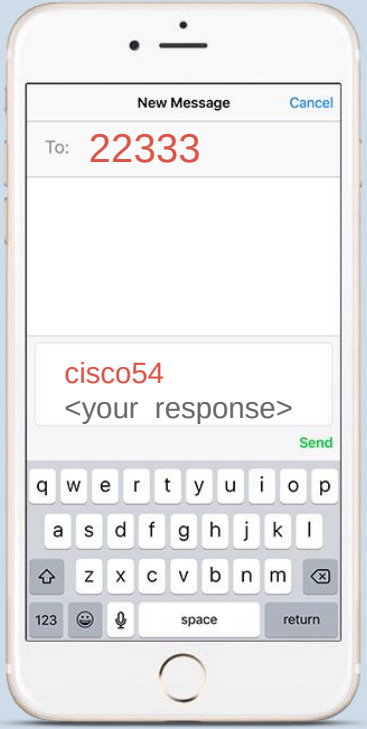
BRKEWN-2670

Cisco live!

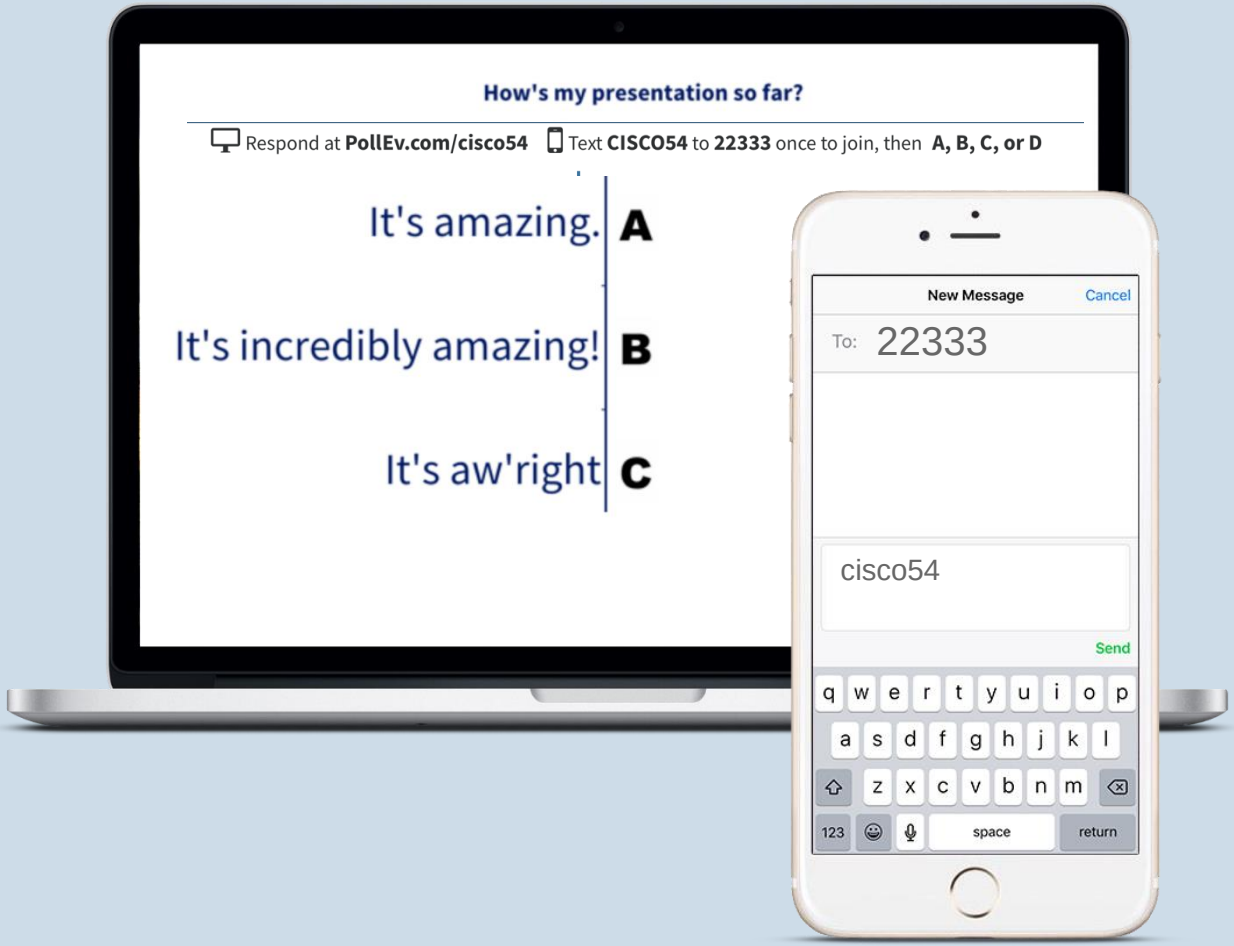
Participating with Poll Everywhere

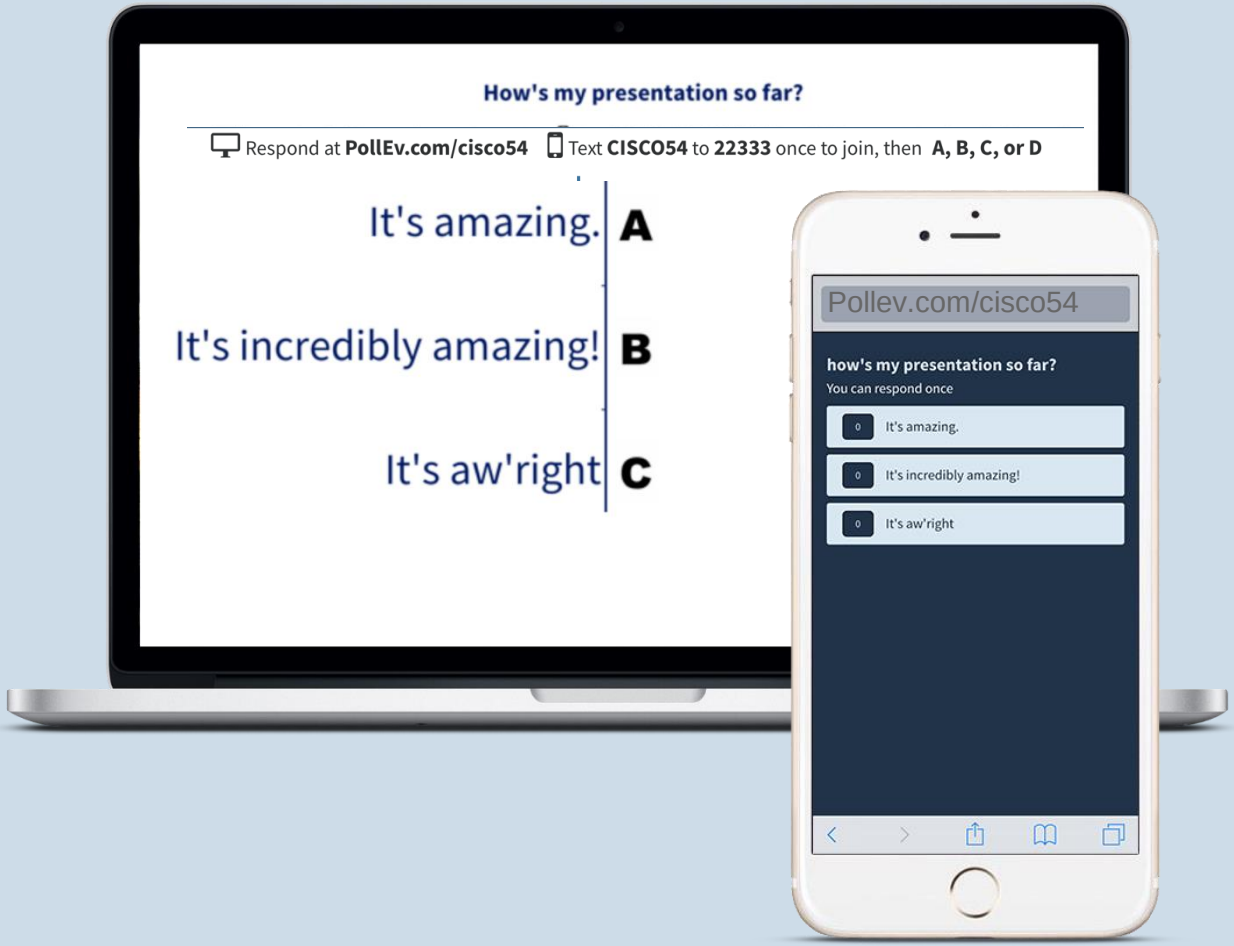


Web voting



Text voting


How's my presentation so far?
Respond at PollEv.com/cisco54
Text CISCO54 to 22333 once to join, then A, B, C, or D
It's amazing.
A
It's incredibly amazing!
B
It's aw'right
C
New Message
Cancel
To:
22333
cisco54
Send
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
123
space
return


How's my presentation so far?
Respond at PollEv.com/cisco54
Text CISCO54 to 22333 once to join, then A, B, C, or D
It's amazing. A
It's incredibly amazing! B
It's aw'right C
Pollev.com/cisco54
how's my presentation so far?
You can respond once
0 It's amazing.
0 It's incredibly amazing!
0 It's aw'right

Your poll will show here

1

Install the app from
pollev.com/app

2

Make sure you are in
Slide Show mode

Still not working? Get help at pollev.com/app/help
or
Open poll in your web browser

Your poll will show here

1

Install the app from
pollev.com/app

2

Make sure you are in
Slide Show mode

Still not working? Get help at pollev.com/app/help
or
Open poll in your web browser

Agenda

- Network Requirements for the Digital Organization
- Self-Healing Infrastructure
- Self-Optimizing Automation and Assurance
- Self-Defending Security and Compliance
- Self-Aware Insights and Experiences

Businesses everywhere are reinventing themselves with mobility.

Creating New Priorities for Digital Organization

Transform Processes & Business Models

Innovations

Faster Time to Market

Empower Workforce Efficiency and Innovation

Increased Productivity

Better Retention

Personalize Customer/ Citizen Experience

Increased Loyalty

Greater Insight

Mobility

Mobile traffic will exceed wired traffic by 2017

IoT

IoT devices will triple by 2020

Analytics

75% of companies planning to or investing in big data

Cloud

80% of organizations will primarily use SaaS by 2018

The Network Must Evolve for Digital

Faster Innovation

Reduce Cost & Complexity

Lower Risk & Meet Compliance

Insights & Experiences

Visibility & analytics

users | devices | applications | threats

Automation & Assurance

Accelerated roll out of services

Security

Rapid threat detection and mitigation

Network Requirements for the Digital Organization

Self-Aware

Insights | Experiences

Self-Optimizing

Automation | Assurance

Self-Defending

Security | Compliance

Visibility and Analytics
Driving change through insight

Speed and Simplicity
Innovating beyond the standard

Threat Defense
Protecting the business and users

Self-Healing Infrastructure

Infra Software | Highly Available

Always on, Always ready

Infra Software | Highly Available

Infrastructure Best Practices

User-First Lifecycle

The Bigger Picture

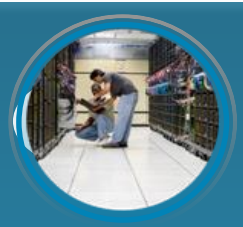
Plan

Design Phase

Design Guides

- Mobility Design Guides
- Data Sheets
- RF Planner
- Site Survey

Deploy



Day 0 – Provision

Express Setup

- Wired
- Over the Air
- Best Practices at Day 0

Operate

Day 1 – Optimize

Best Practices

- Audit Upgrades
- Config Analyzer
- Cisco Active Advisor

Manage

Day 2 – Monitor

Dashboards

- Wireless Performance Monitoring
- Real time troubleshooting

WLAN Express Setup
Easy Provisioning

WLAN Express Setup

Day 0/1 Ease of Setup

WLC
WLAN Express Setup
7.6 MR2, 8.0, 8.1

Best Practices defaults,
RF Parameter Optimization, Network Profiles

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

WLC
Upgrade Audit Workflow
8.1

Audit Page on Upgrade,
One-click Fix It,
Manual Config Option

- Identify missing best practice configuration on upgrade
- Easy one-click fix It option to turn on Best Practice Knobs
- Restore Defaults to revert configuration to default

WLCCA
Config
Analyzer

Windows Executable
"show run-config" Based
Analyzer Tool

- Simplified operational use to quickly identify and and fix problem areas
- RF Health metrics, IOS Support, Mobility Group support

CAA
Cisco
Active Advisor

Free, cloud based service
Agentless – nothing to download

- Cisco Personalized device health score
- Compare your wireless network configuration to Cisco's recommended best practices
- Automated Inventory Management and Network Scanning

Wired Express Setup

- Introduced on 2504 in 7.6 MR2, 8.0
- Extended to 5508, vWLC, 7510, 8510 in 8.1
- Extended to 5520, 8540 in 8.1 and Mobility Express in 8.1 MR

Wireless Over-The-Air (OTA) Setup

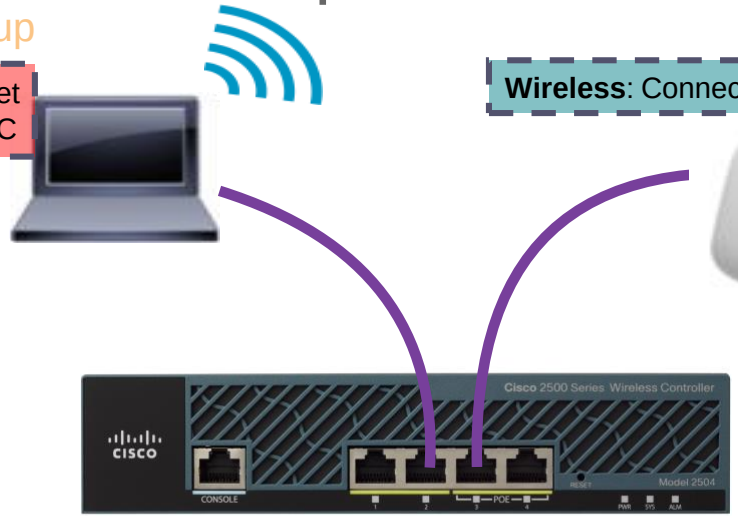
- Available in 8.1 and higher
- Supports Universal AP (UX)
- Supported on 2504 and Mobility Express

WLAN Express Setup

Day 0/1 Ease of Setup

Wired: Connect PC Ethernet cable to any port on the WLC

Wireless: Connect AP WLC port 3 or 4 (PoE)



Connect to SSID '**CiscoAirProvision**' using the key '**password**'

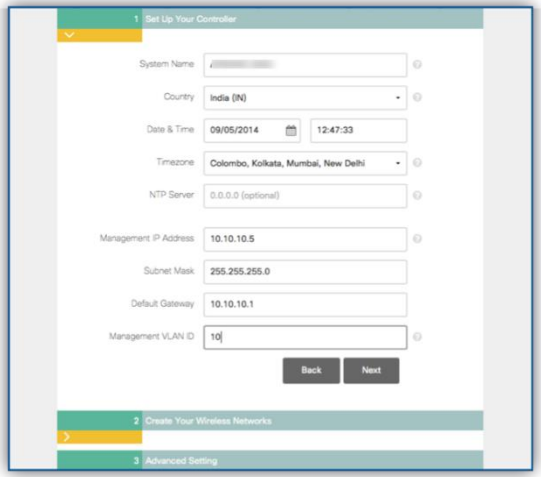
Wait for the SYS LED light to be solid

If setup is Wireless, wait for AP to power and broadcast SSID

WLAN Express Setup

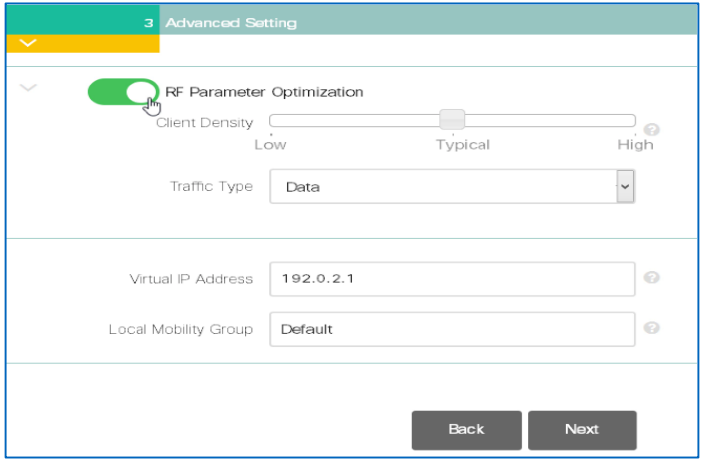
Day 0/1 Ease of Setup

Open a web browser and access *http://192.168.1.1*

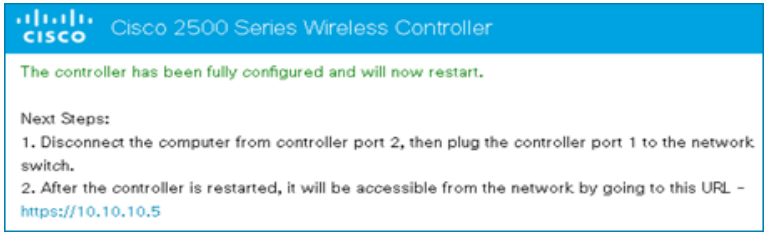


Go through a setup wizard

Enable RF Optimization



Confirm settings



WLAN Express 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

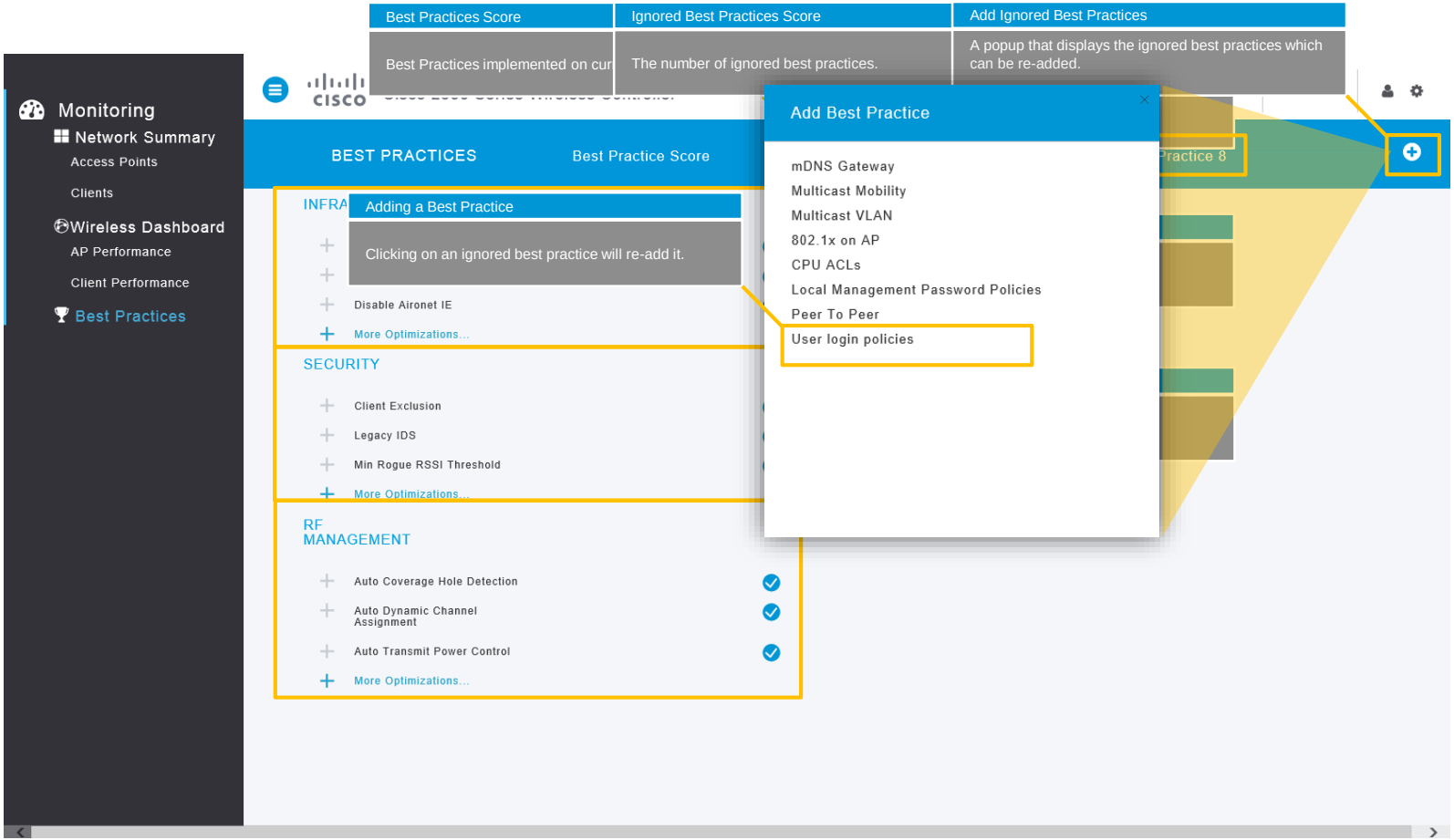
Management over Wireless disabled
Load Balancing
Rogue Threshold Enabled
Client Exclusion Enabled
FastSSID Enabled
Infra MFP
Multicast Forwarding Mode
SNMPv3 (delete default)
Mobility Name
RF Group same as Mobility Name
DHCP Required on Guest WLAN
5 GHz Channel Bonding

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

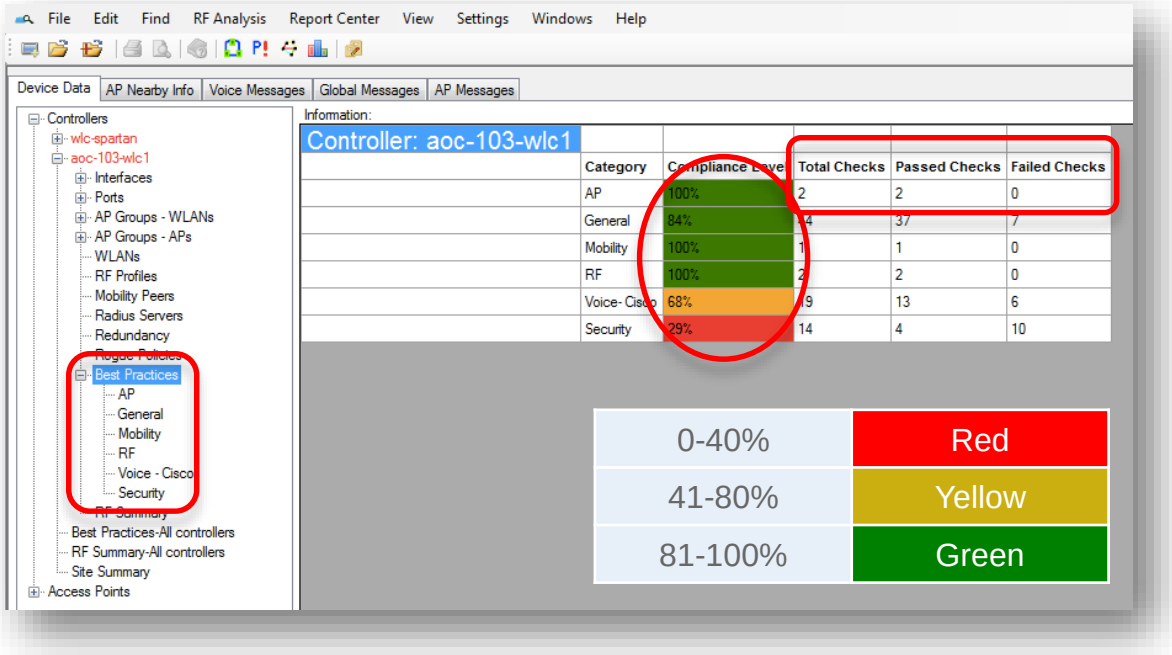
Best Practices Audit
Optimization

Best Practices Fix and Ignore Options



WLC Config Analyzer – Per Controller Compliance

- Best Practices categorized into
  - General
  - AP
  - Mobility
  - RF
  - Security
  - Voice
  - Mesh
  - Flex
- Per-Controller Compliance Level for Each category
- Total/Passed/Failed checks



Compliance Level w/ and w/o Express WLAN Setup

Information:

Controller: wlc					
	Category	Compliance Level	Total Checks	Passed Checks	Failed Checks
	AP	50%	2	1	1
	General	73%	44	32	12
	Mobility	100%	1	1	0
	RF	100%	2	2	0
	Voice- Cisco	68%	19	13	6
	Security	36%	14	2	12

7.6 MR2 without Express WLAN Setup

Information:

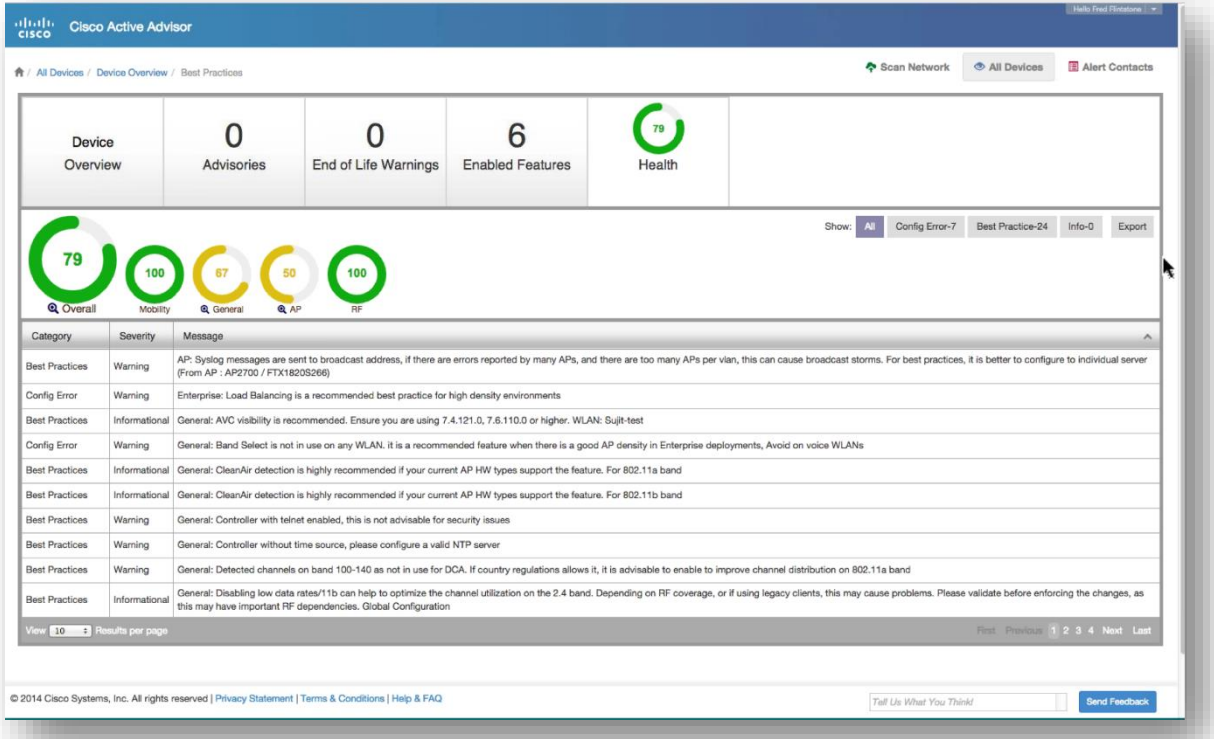
Controller: wlc-spartan					
	Category	Compliance Level	Total Checks	Passed Checks	Failed Checks
	AP	100%	2	2	0
	General	82%	44	36	8
	Mobility	100%	1	1	0
	RF	100%	2	2	0
	Voice- Cisco	79%	19	15	4
	Security	100%	14	14	0

8.1 with Express WLAN Setup

Analyze & Mitigate

- Downloadable client
- Configuration stays local
- Simplified operational use to quickly identify and and fix problem areas
- RF Health metrics, IOS Support, Mobility Group support

Cisco Active Advisor Personalized Health Score



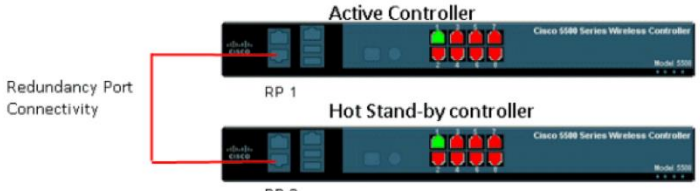
Improve

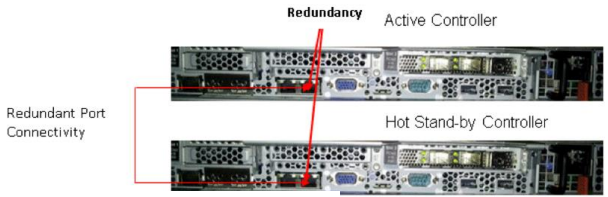
- Personalized device health score
- Free, cloud-based service
- Automatically takes an inventory of your Cisco network

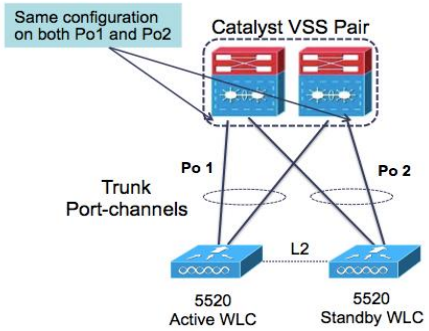
Create Cisco Active Advisor login at : https://www.ciscoactiveadvisor.com

Infrastructure: Enable High Availability (AP & Client 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



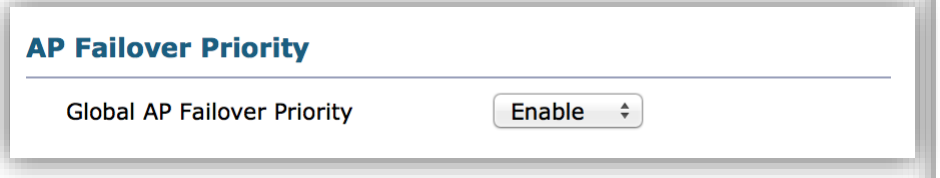


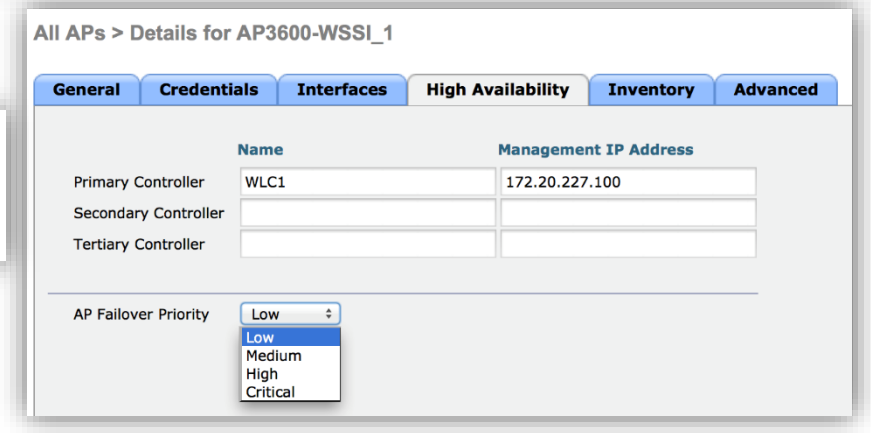


Sub-second failover and zero SSID outage

Infrastructure: Enable AP Failover Priority

- Wireless → Access Points → Global Configurations
- Wireless → Access Points → All APs->AP_NAME → High Availability





Allows certain APs to be assigned higher WLC join priorities, so they are given preference while joining a WLC

Your poll will show here

1

Install the app from
pollev.com/app

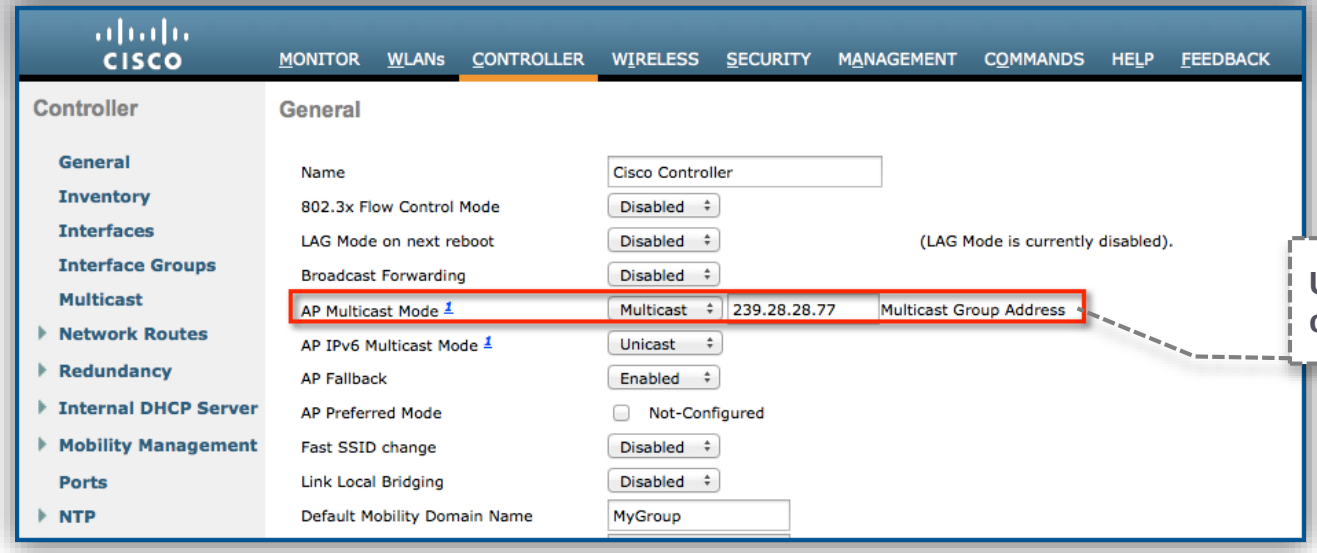
2

Make sure you are in
Slide Show mode

Still not working? Get help at pollev.com/app/help
or
Open poll in your web browser

Infrastructure: Enable AP Multicast mode

Controller → General → AP Multicast Mode



Unique across WLCs and not clashing with other protocols

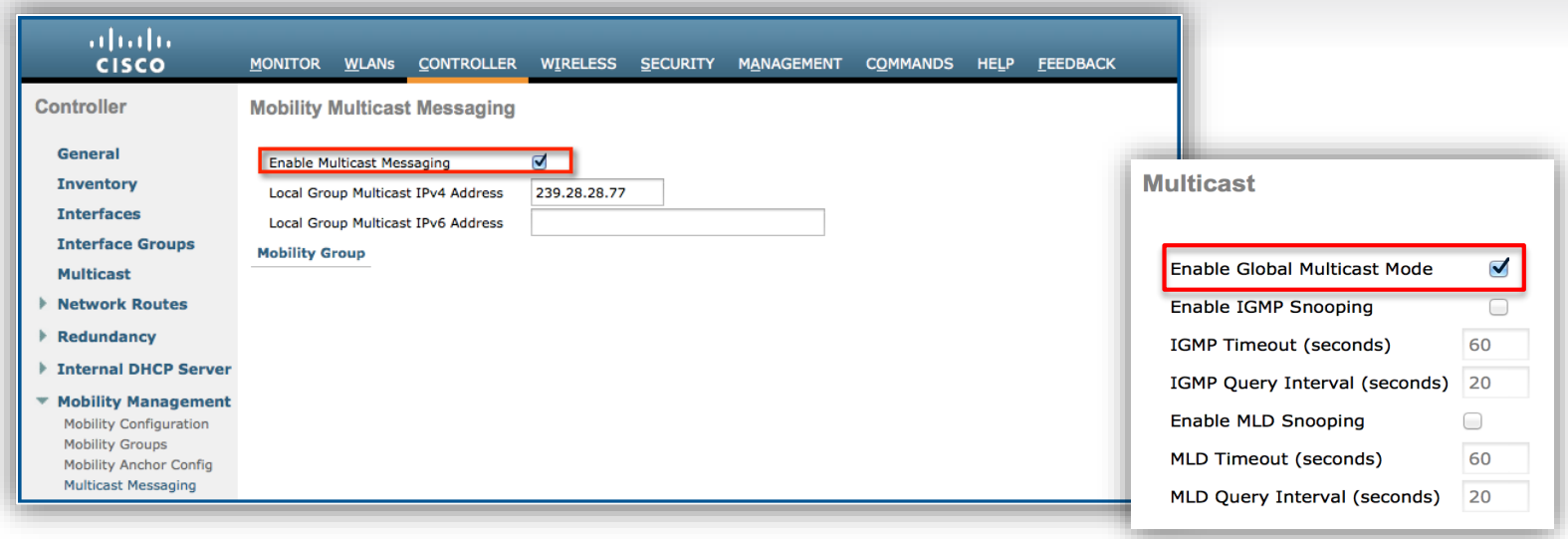
Network infrastructure must provide multicast routing between management interface subnet and AP subnet

Forward multicast traffic to Access Points instead of sending unicast messages to each individual AP

Infrastructure: Enable Multicast Messaging for mobility domains

Controller → Multicast

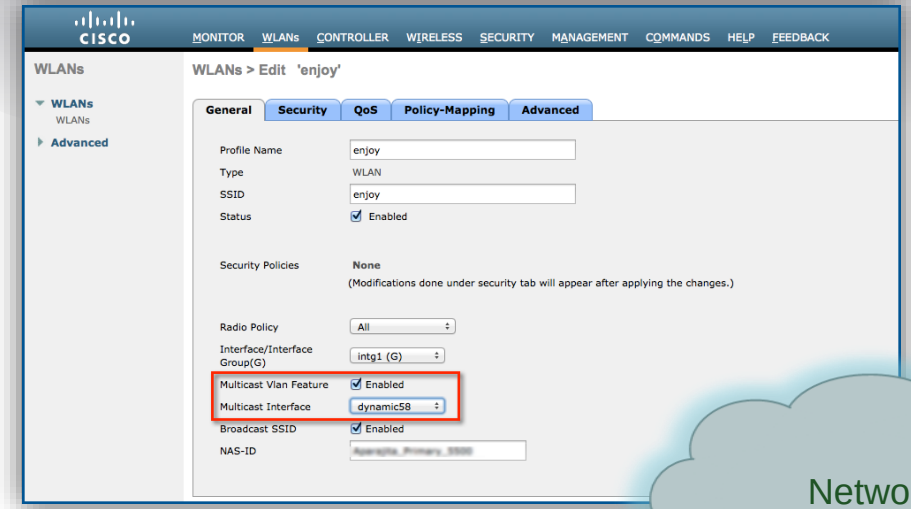
Controller → General

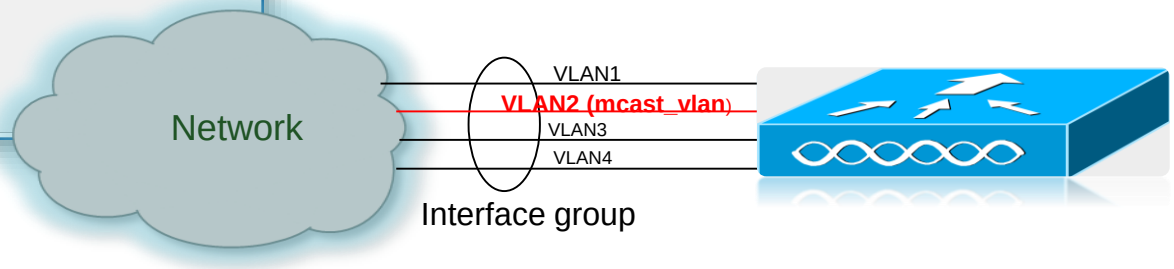


Allows clients to announce messages to all mobility peers, instead of individual WLCs, benefiting time, CPU usage, and network utilization. Multicast routing between controllers

Infrastructure: Multicast VLAN for Interface Groups

WLANs → WLAN Name → General





To limit the multicast on the air to a single copy on a predefined multicast VLAN

Your poll will show here

1

Install the app from
pollev.com/app

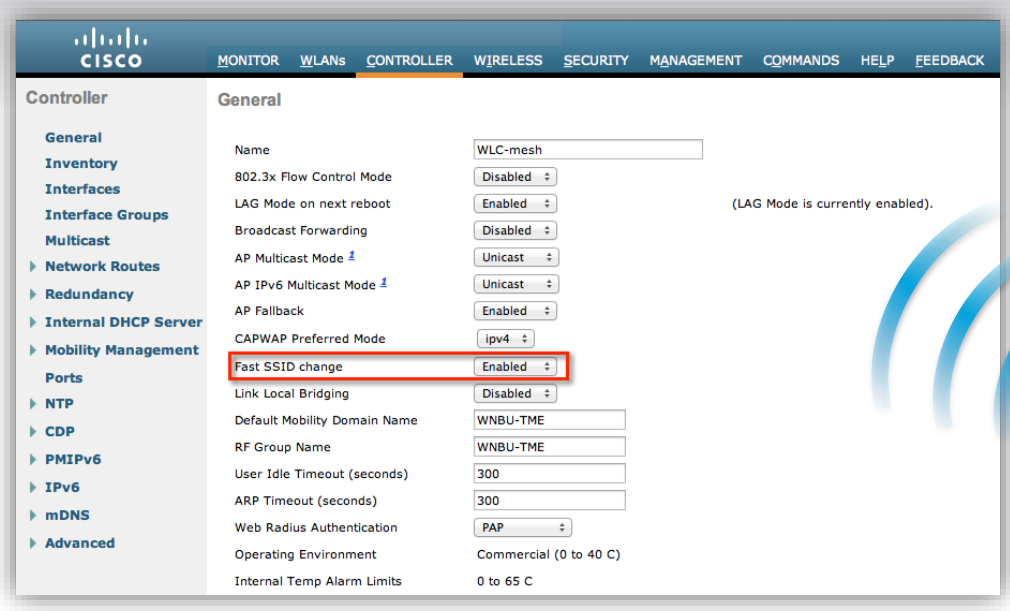
2

Make sure you are in
Slide Show mode

Still not working? Get help at pollev.com/app/help
or
Open poll in your web browser

Infrastructure: Enable Fast SSID change

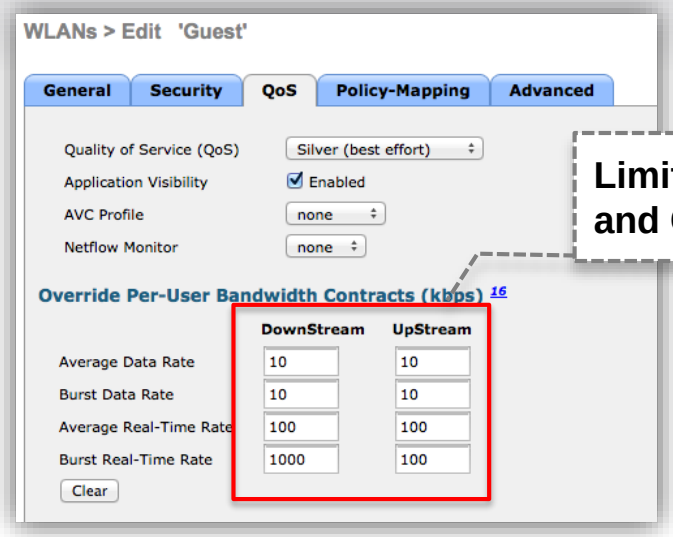
Controller → General



Allows clients to move faster between SSIDs, by not clearing the client entry

Infrastructure: Enable per-user bandwidth contract

WLANs → Edit 'WLAN_NAME' → QoS

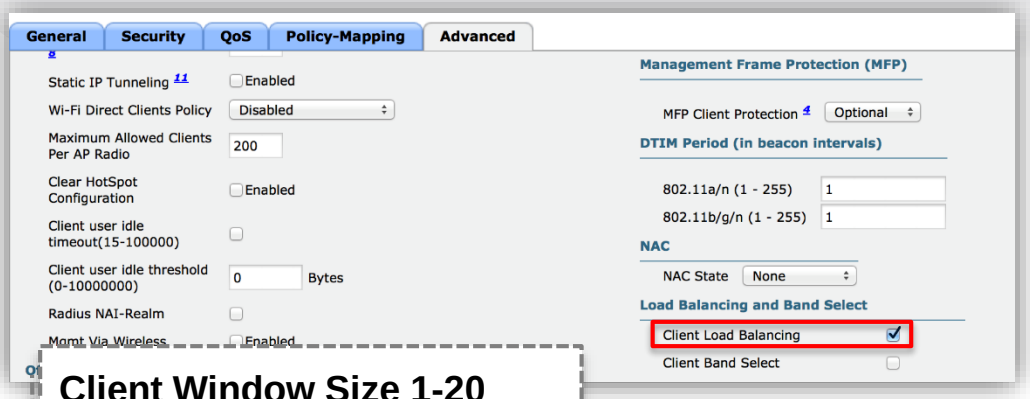


Limit data rates for Guest and Contractor accounts

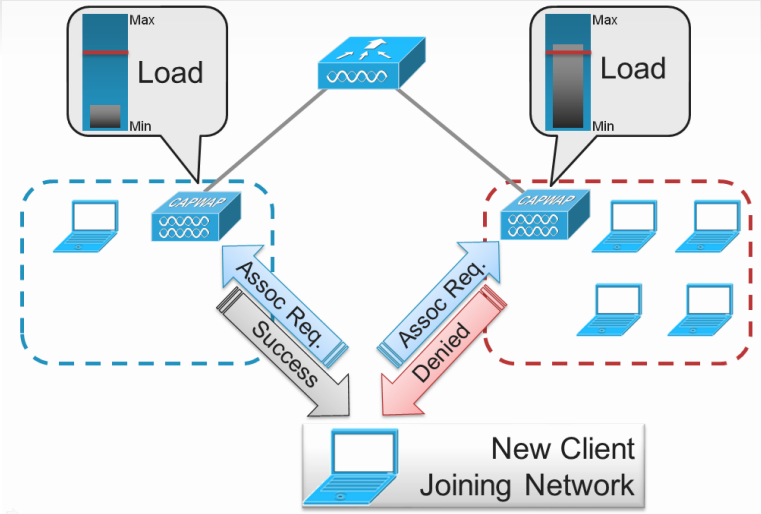
Enforces limits on non-mission critical clients

Infrastructure: Enable Client Load Balancing

WLANs → Edit “WLAN-NAME” → Advanced



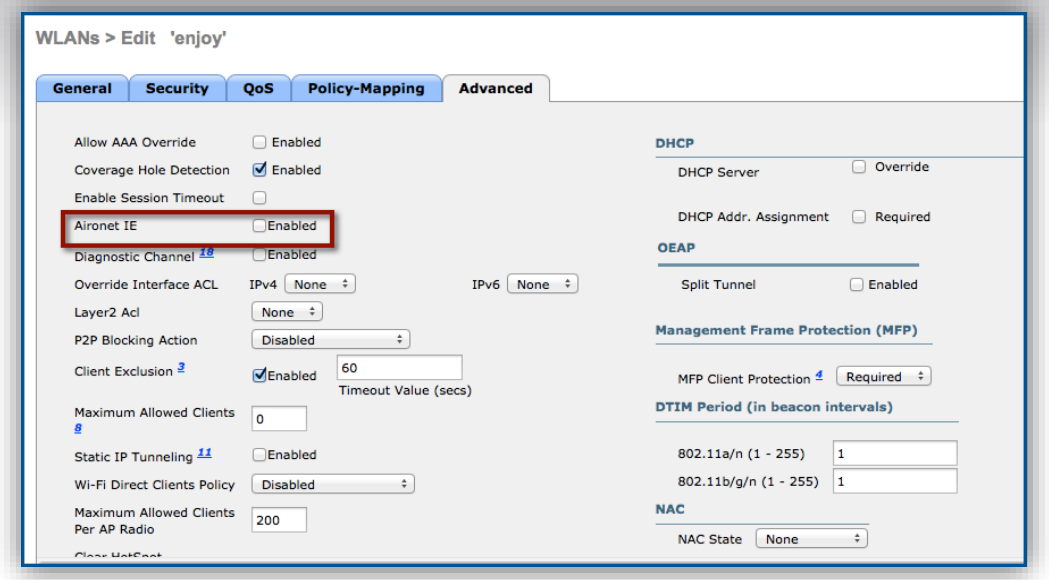
Client Window Size 1-20
Maximum Denial Count 0-10



Balances the number of clients connect to a WLAN between multiple APs
Not suitable for Voice, Low Density and single AP deployments like hotspots

Infrastructure : Disable Aironet IE

WLANs → Edit “WLAN-NAME” → Advanced

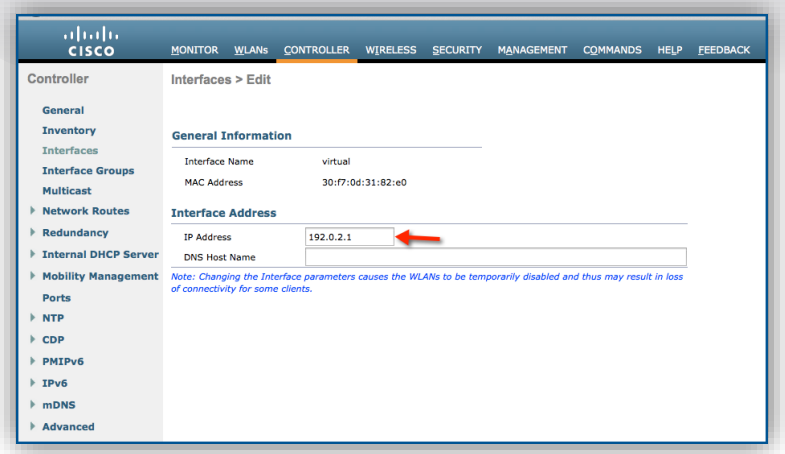


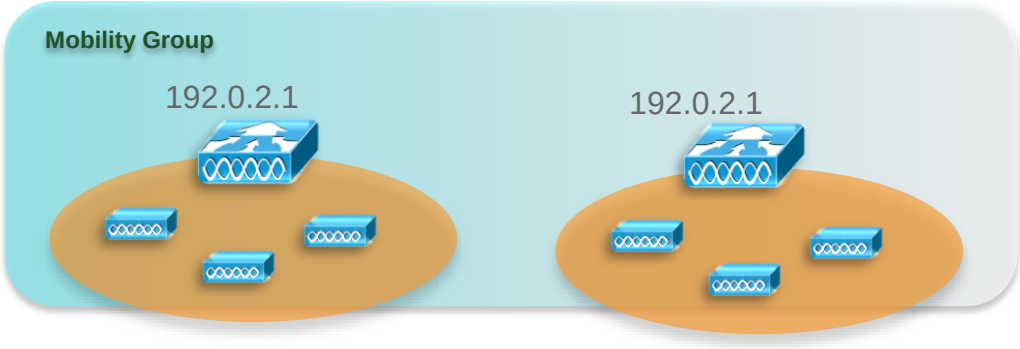
- Aironet IE 0x85 in beacons and probe responses
  - AP name, load, client count etc.
- Controller sends Aironet IEs 0x85 and 0x95 in the reassociation response if it receives Aironet IE 0x85 in the reassociation request
  - Management IP address of WLC
  - IP address of AP

Can cause compatibility issues with some types of wireless clients
Enable for WGB and Cisco voice. Optional for CCX based clients

Infrastructure: Same Virtual IP if same mobility name

Controller → Interfaces → virtual



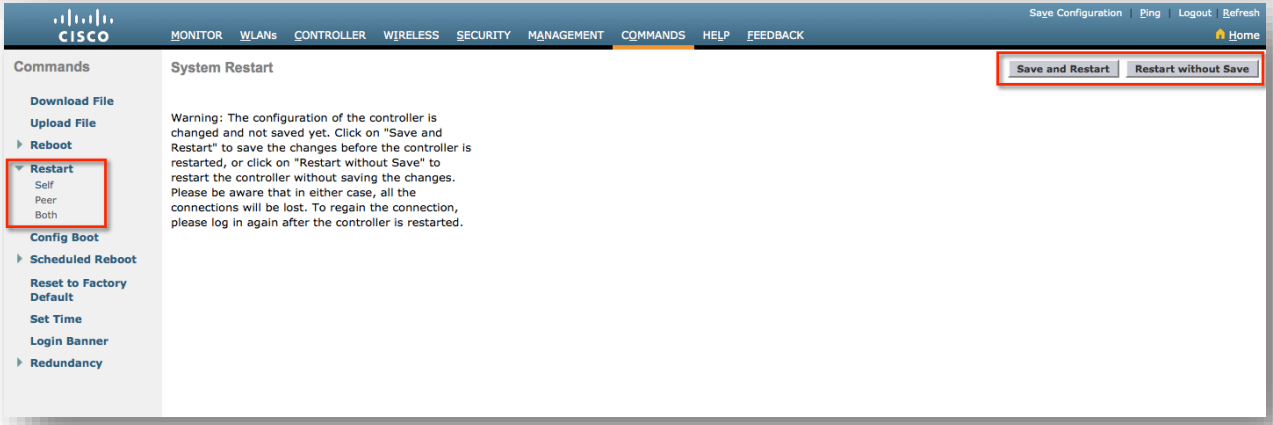


Inter-controller roaming can appear to work, but the hand-off does not complete and the client loses connectivity when DHCP renew is performed if DHCP proxy enabled

Infrastructure: Fast Restart

Commands → Restart

73% Faster



Use Cases

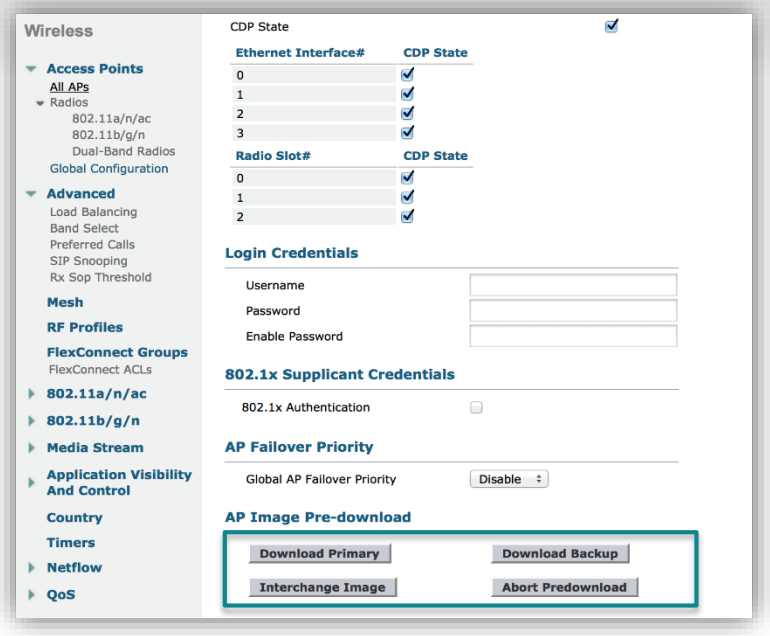
- ✓ LAG <-> no LAG
- ✓ 10 G <-> 1 G
- ✓ High Availability SSO Pairing
- ✓ Post Configuration Wizard
- ✓ Web-auth certificate installation
- ✓ Transfer Download of XML

- Supported on Cisco WLC 7510, 8510, 5520 8540 and vWLC

Process Restart to reduce network and service downtime and improve serviceability

Infrastructure: Enable Pre-image download

Wireless → Global Configurations → AP Image Pre-download



Allows for less network downtime during software updates

FlexConnect: Enable “FlexConnect AP Upgrade”

Wireless → Flexconnect Groups → Edit “Groupname” → Image Upgrade Tab

FlexConnect Groups > Edit 'RetailStore_flexgroup'

General | Local Authentication | Image Upgrade | ACL Mapping | Central DHCP | WLAN VLAN mapping

FlexConnect AP Upgrade ☑

Slave Maximum Retry Count 44

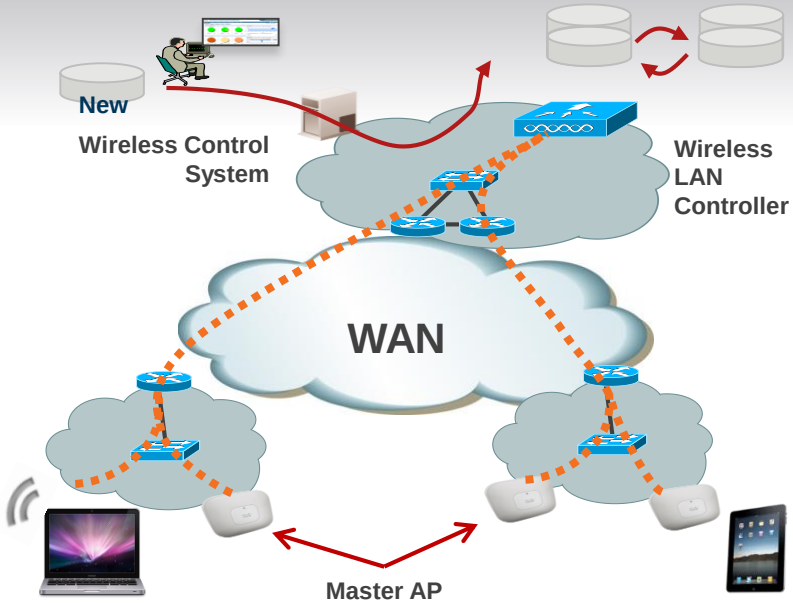
Upgrade Image Primary FlexConnect Upgrade

FlexConnect Master APs

AP Name

Add Master

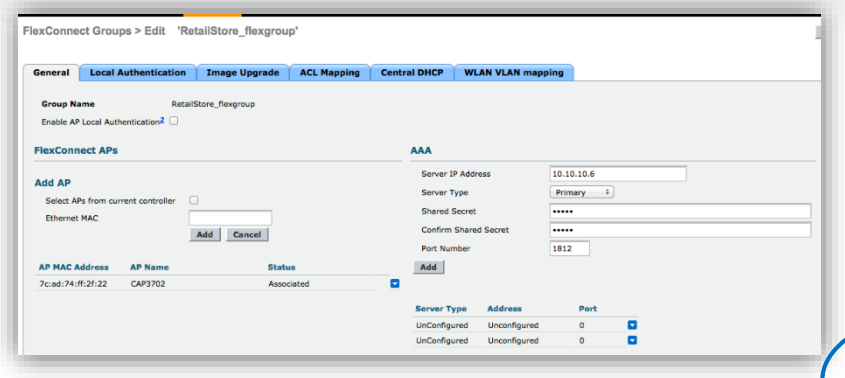
Master AP Name	AP Model	Manual
CAP3702	c3700E	no

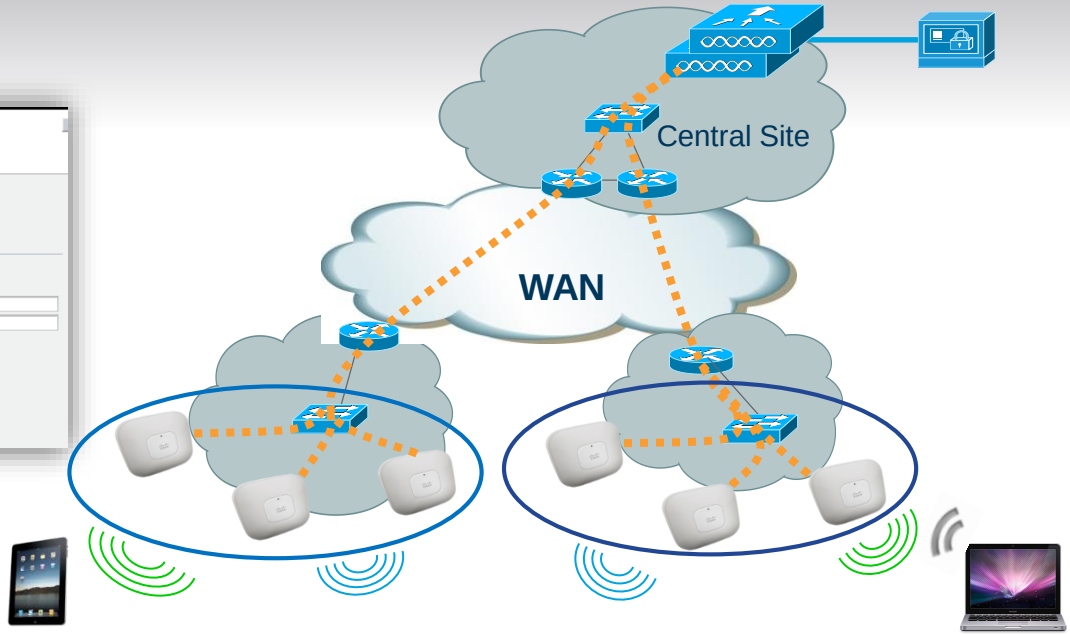


Avoids downloading multiple copies of the Access Point software over the slow WAN link to the remote site, reduces service downtime and reduces risk of download failure

FlexConnect: Enable FlexConnect Groups

Wireless → FlexConnect Groups → Edit “Groupname”





Allow users to assign specific APs to groups with set configurations, OKC/CCKM key caching for Voice, Local RADIUS server configuration, consistent WLAN mappings

Your poll will show here

1

Install the app from
pollev.com/app

2

Make sure you are in
Slide Show mode

Still not working? Get help at pollev.com/app/help
or
Open poll in your web browser

Network Requirements for the Digital Organization

Self-Aware

Insights | Experiences

Self-Optimizing

Automation | Assurance

Self-Defending

Security | Compliance

Visibility and Analytics
Driving change through insight

Speed and Simplicity
Innovating beyond the standard

Threat Defense
Protecting the business and users

Self-Healing Infrastructure

Infra Software | Highly Available

Always on, Always ready

Self-Optimizing : Automation & Assurance

Network Plug-N-Play – Simple, Secure, Scalable

Today's Process

Central Staging Facility

Ships equipment

Reseller/Partner

Network Admin

- Install OS
- Install Config
- Prime device

Installer

Site-1 Site-2 Site-3

Business Challenges

Network PnP

Direct Costs

- Shipping after Configuring device
- Travel costs for IT installer

Complexity

- Config errors
- Different products / processes

Security

- 3rd party not secure

Time/Productivity

- Manual process
- Shipping , Storage, Travel

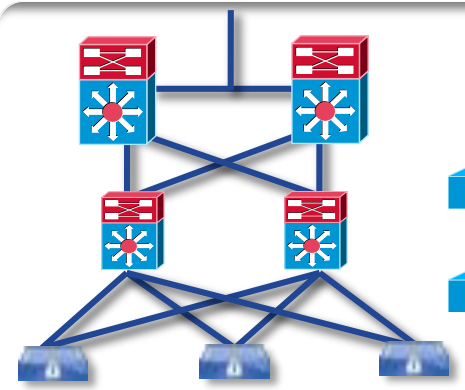
Unskilled Installer | GUI Based | Consistent for devices & PIN(Campus/Branch) | Secure | Zero-touch RMA | Greenfield & Brownfield

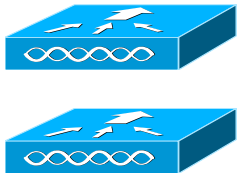
Single Site

PnP Server

Site Rule

Product ID	Serial #	Hostname	WLC IP	AP Group	AP Mode
AIR-CAP3702I-A-K9	RFD0PP2T025	Site-1-AP	WLC-1a	Site-1-Group	FlexConnect





WLC-1a

WLC-1b

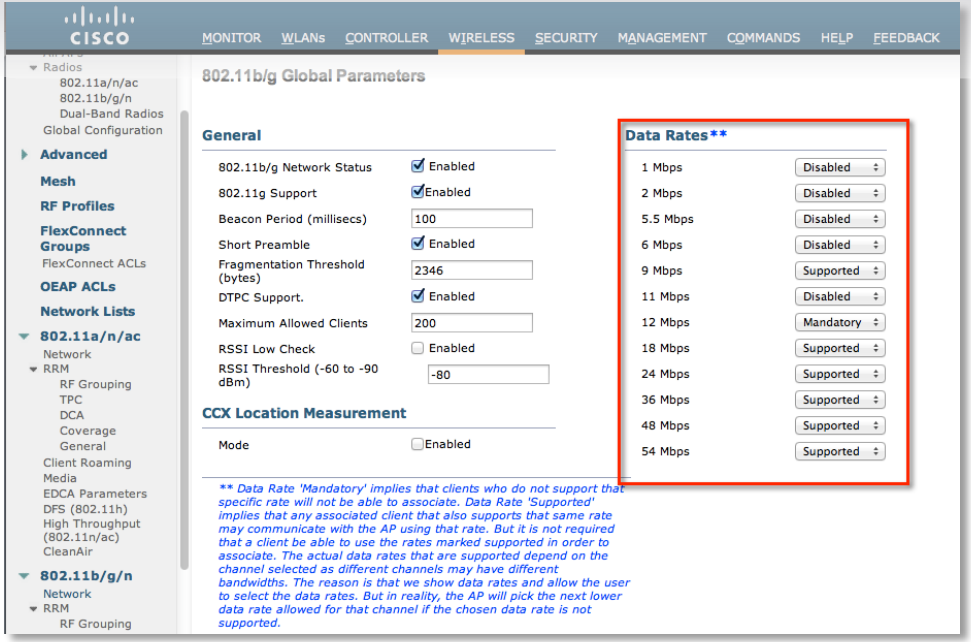
WLC IP: WLC-1a
AP Name: Site-1-AP
AP Mode: FlexConnect
AP Group: Site-1-Group

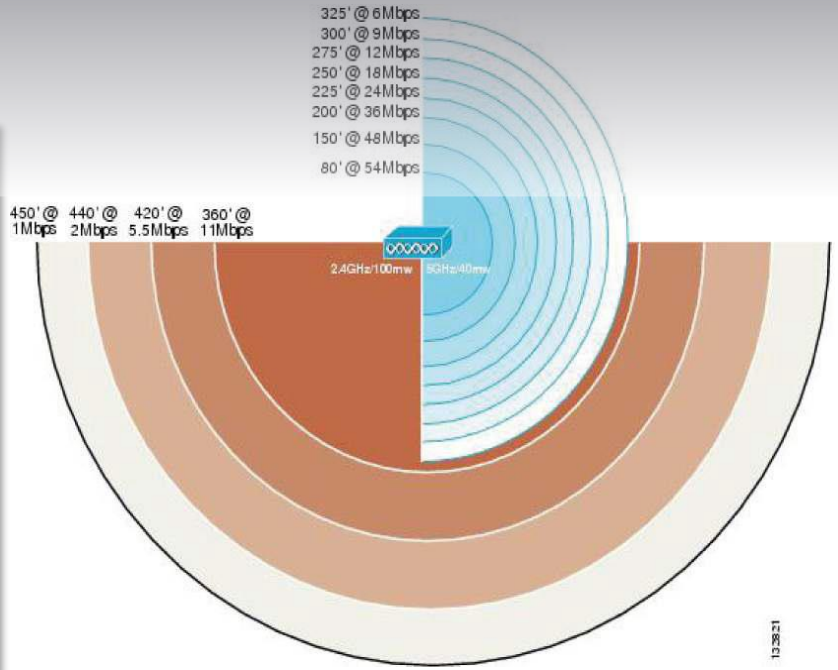
Site-1

RF & RRM Best Practices

RF & RRM: Disabling .11b Data Rates

Wireless → 802.11b/g/n → Network

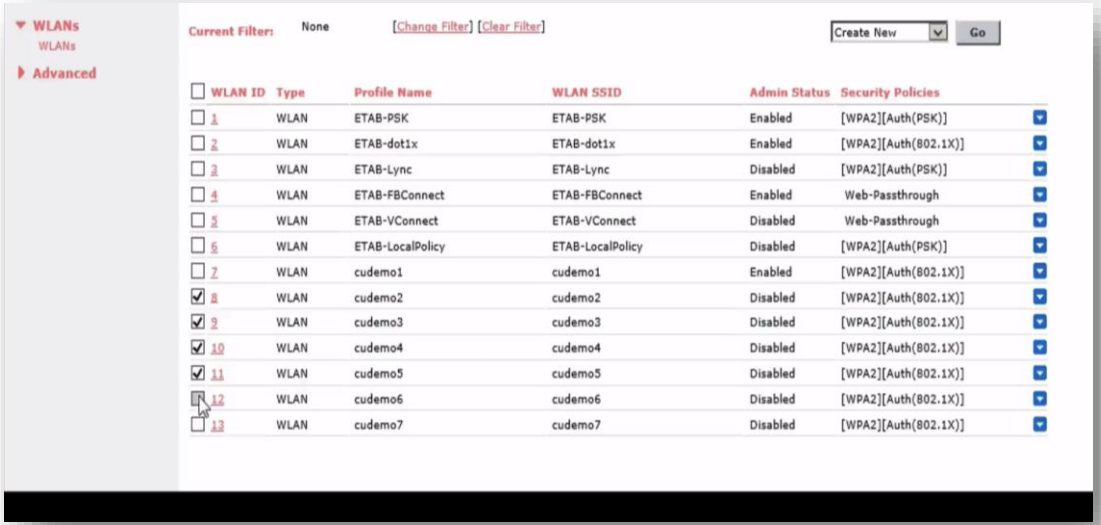




Management frames sent at lowest mandatory rate - slows down the entire cell

RF & RRM: Disabling .11b Data Rates

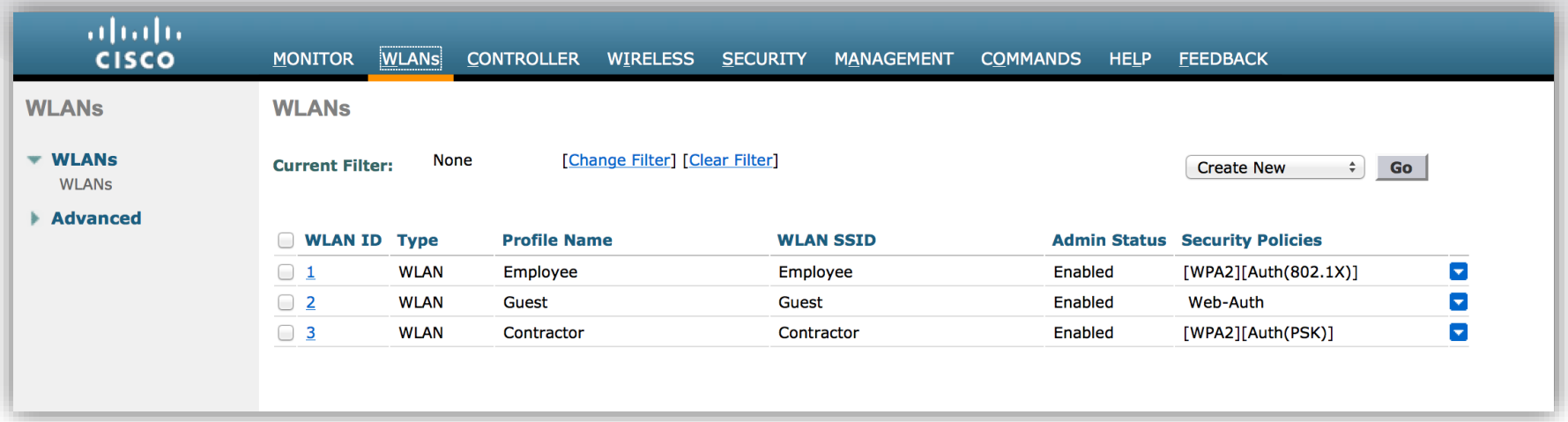
Demonstrating the impact of 802.11b data rates on Channel Utilization



1 Mbps Mandatory : Channel Utilization 67%
6 Mbps Mandatory : Channel Utilization 23%

RF & RRM: Restrict Number of WLANs below 4

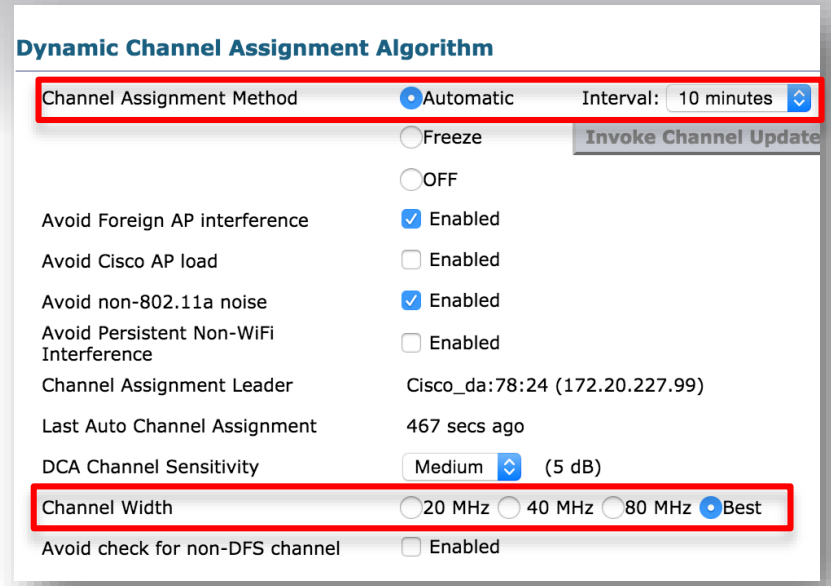
WLANs → WLANs



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

RF & RRM: Enable Channel Bonding – DBS

Wireless → 802.11a/n/ac → RRM → DCA



Select the widest Channel Width with:

- Highest Client Data Rates
- Lowest Channel Utilization per Radio
- Minimize Data Retries / CRC errors

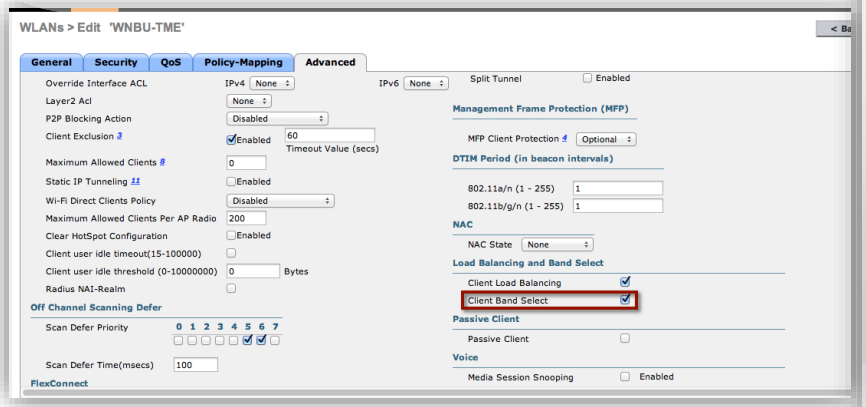
While avoiding:

- Rogue APs
- CleanAir Interferers

40/80MHz wide channels in the 5GHz space can 2x/4x the amount of user data than can be transmitted. For extreme HD deployments use 20 MHz channels to keep cell size small

RF & RRM: Enable Client Band Select

WLANs → Edit “WLAN-NAME” → Advanced



Challenge

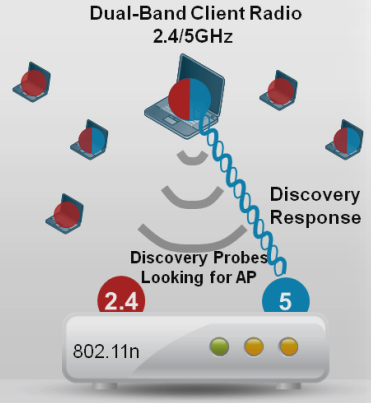
Dual-Band clients persistently connect to 2.4 GHz

- 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

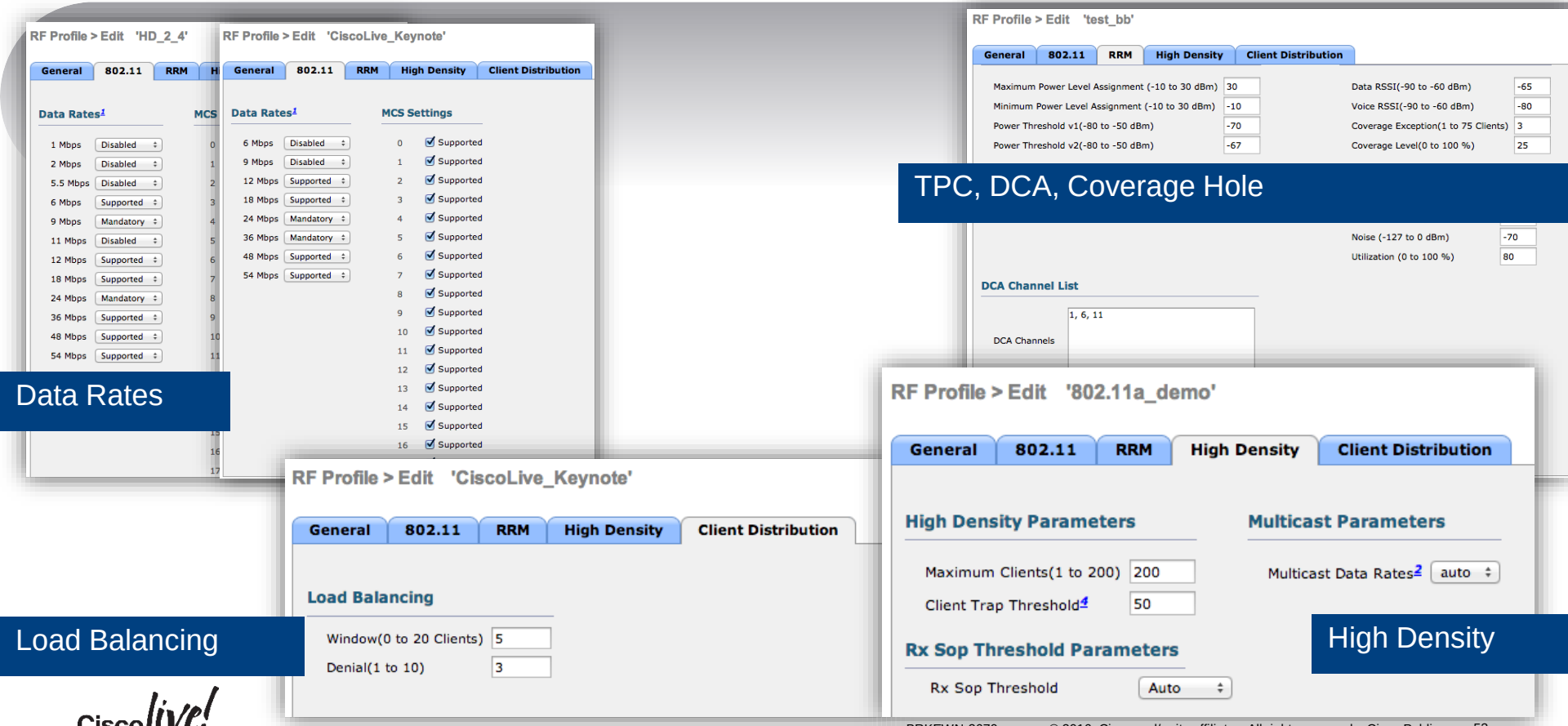
- Better usage of the higher capacity 5GHz band
- Frees up 2.4 GHz for single band clients



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

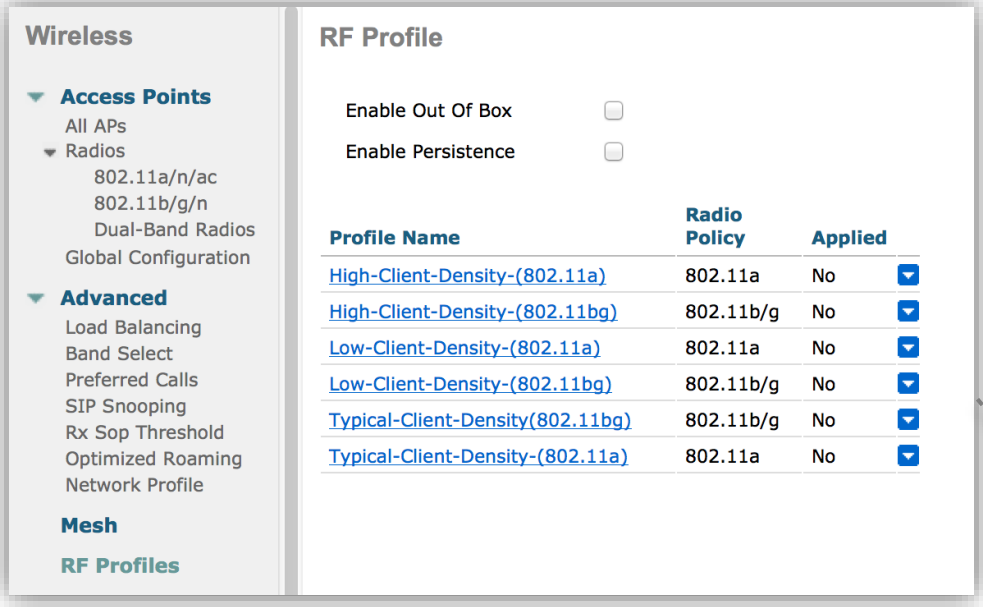
Allows dual-band clients to move to the less congested 5GHz band
Not recommended for Voice deployments

RF Profiles : Granular Control



Pre-built RF profiles

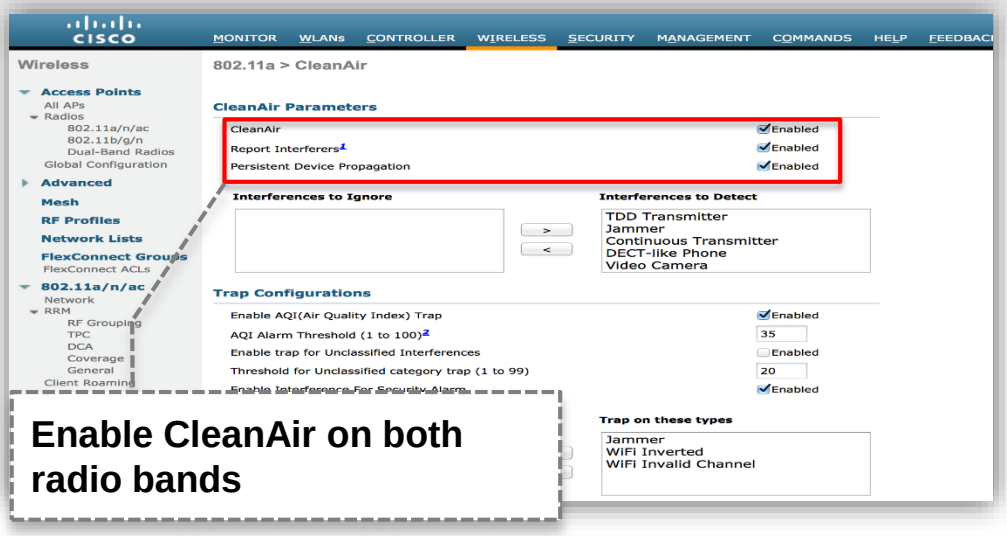
Client Density specific pre-built RF profiles for 2.4 GHz and 5GHz Bands – to be used with AP Groups



Pre-built RF profiles for use with AP Groups

RF & RRM: Enable Cisco CleanAir

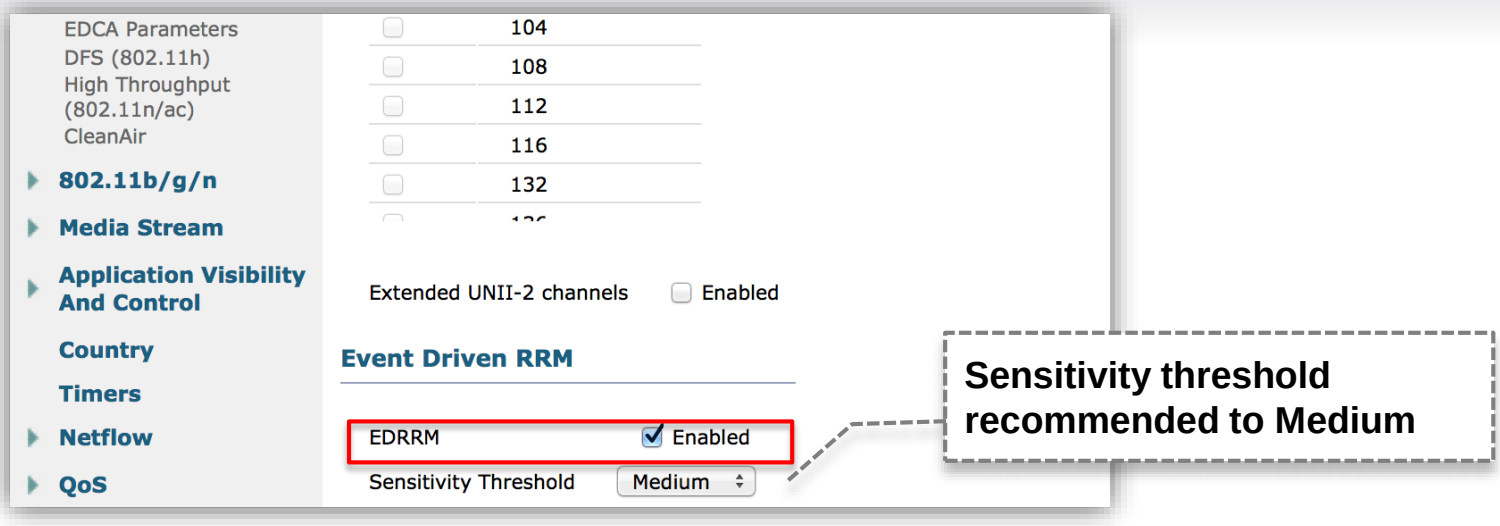
Wireless → 802.11a/n/ac or 802.11b/g/n → CleanAir



CleanAir identifies non-WIFI interferers and generates interferer and air quality reports

RF & RRM: Enable Cisco EDRRM

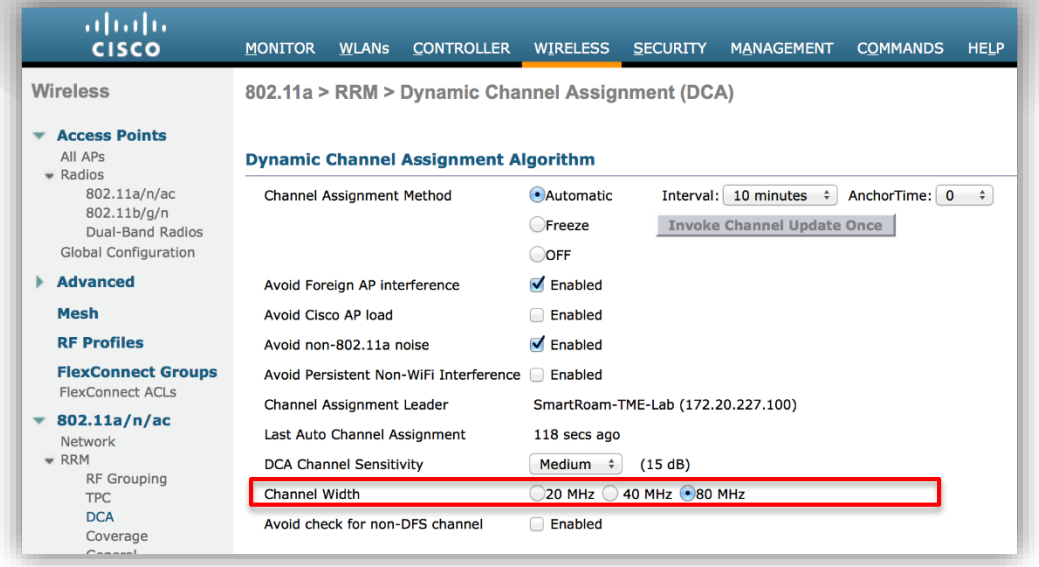
Wireless → 802.11a/n/ac or 802.11b/g/n → RRM → DCA

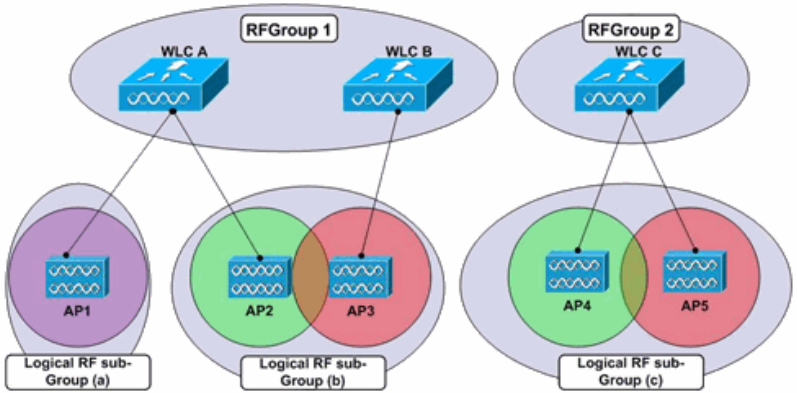


EDRRM triggers RRM to run when an access point detects a certain level of interference

RF & RRM: RF Group Leader must be an .11ac WLC (Release 7.5+) in RF Groups with mixed versions

Wireless → 802.11a/n/ac → RRM → DCA





If the RF Group Leader does not support 802.11ac (Release 7.5+), APs in the RF Group cannot select 80MHz channel widths

Your poll will show here

1

Install the app from
pollev.com/app

2

Make sure you are in
Slide Show mode

Still not working? Get help at pollev.com/app/help
or
Open poll in your web browser

Cisco And Apple
Better Together

Optimized Wi-Fi Connectivity

iOS and Cisco devices recognize each other

Roaming technologies are enabled automatically

Benefits of Optimized Wi-Fi Connectivity

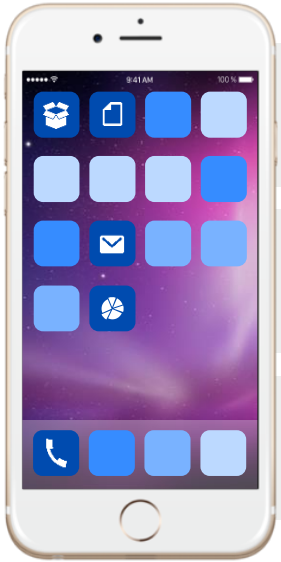
Up to 8x faster roaming and
66% more reliable Wi-Fi calling

85% fewer messages
exchanged with radius server

Automatic configuration
reducing complexity for IT

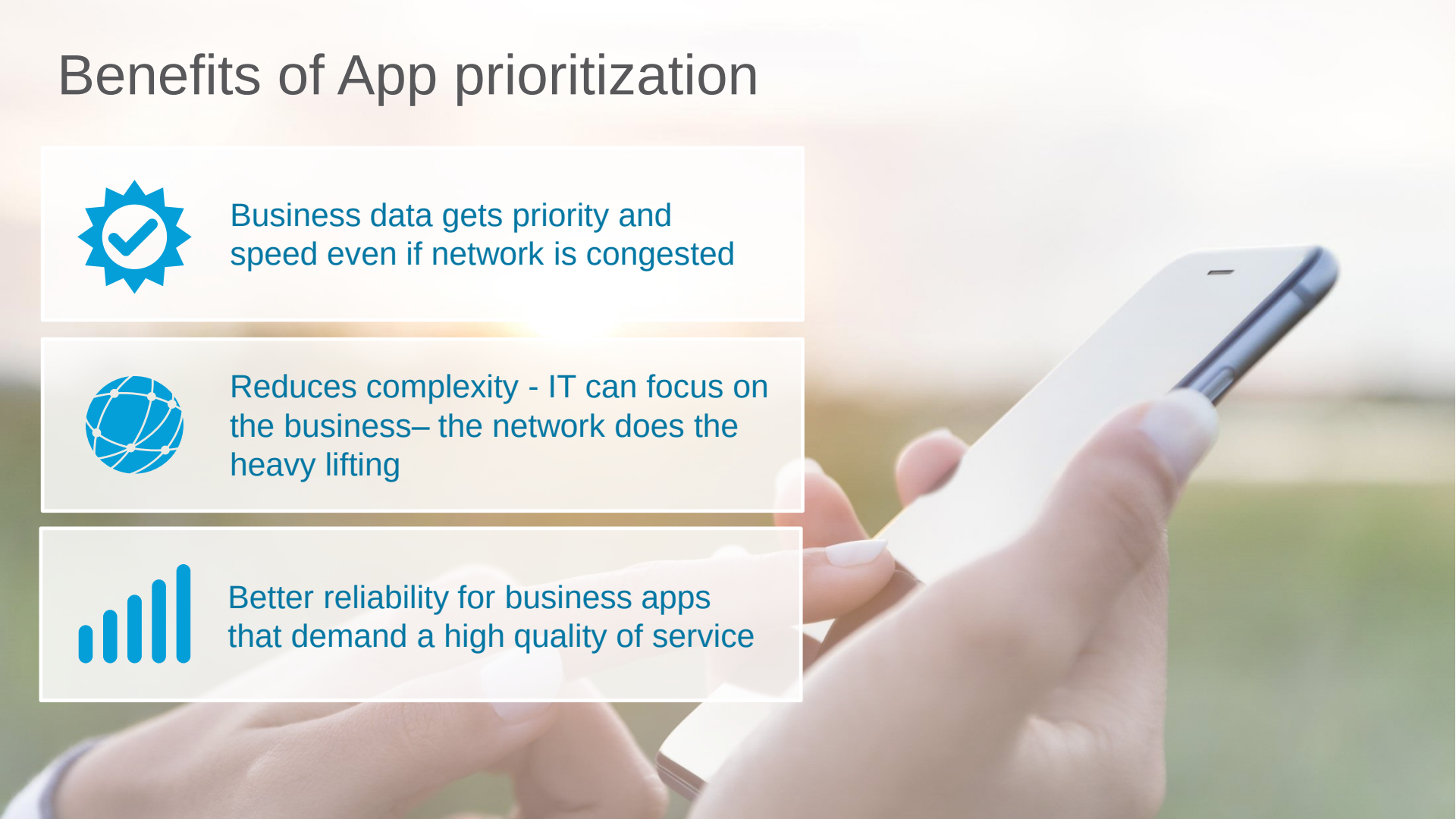
Investment protection -
Leverage existing network
design

Prioritizing Business Apps



- Prioritize business critical apps
- IT has control over which apps get priority
- Enabled using iOS configuration profiles

Benefits of App prioritization



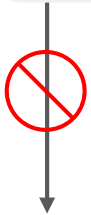
- Business data gets priority and speed even if network is congested
- Reduces complexity - IT can focus on the business– the network does the heavy lifting
- Better reliability for business apps that demand a high quality of service

Optimized Wi-Fi Connectivity

Cisco live!

Cisco and Apple Optimized Roaming

Legacy client **cannot** join the same SSID where 11r is enabled



Non-Cisco-AP

Legacy client that does not support 11r/k/v **can** join the same SSID

I recognize that you are an Apple iOS device
11r is enabled for you

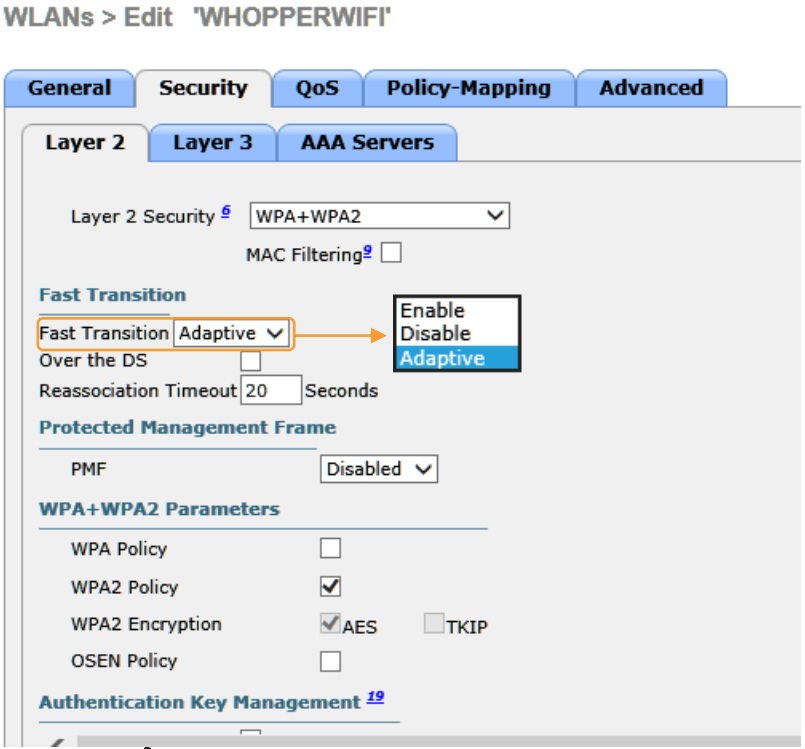
802.11k, 802.11v are on by default

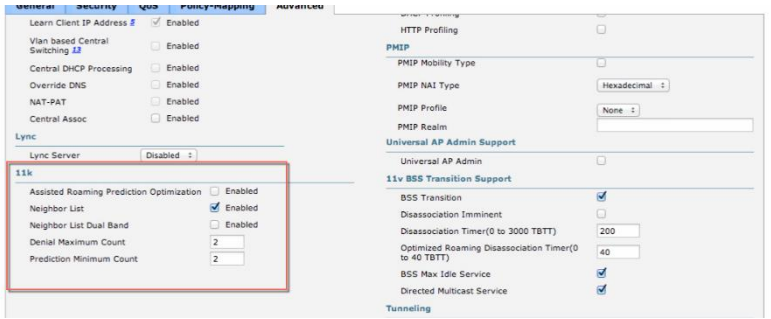
Association

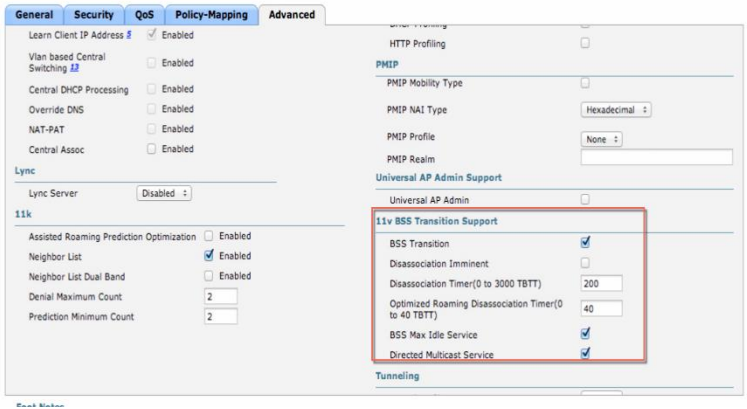
Cisco-AP

Adaptive 11r/k/v

Features enabled by default on a newly created SSID







Benefits of Optimized Wi-Fi Connectivity

66x reduction in probability of poor audio quality experience. 10x more successful end user browsing experience

86% reduction in network message load from the device during roaming

Automatic configuration reducing complexity for IT

Investment protection - Leverage existing network design

Up to 50% reduced management overhead due to fewer SSIDs

Lower battery usage

Prioritizing Business Apps: *Fast Lane*

Cisco live!

What happens Today?

Inability to prioritize business-critical real-time traffic all the way from clients to the destination

- Today IT administrators can classify traffic ONLY at the access point. this implies:
  - Inability to prioritize between the client and the AP.
  - Burden on IT administrator to manage the applications across the enterprise

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:
Minecraft = Realtime-interactive
Viber = BE

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

Supports Fast lane

Supports Fast lane

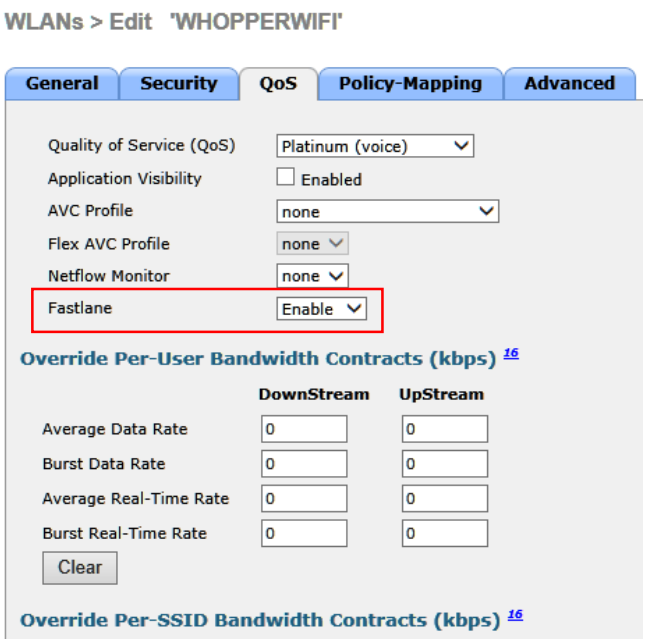
Supports Fast lane

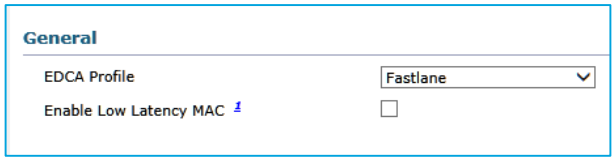
Cisco-AP

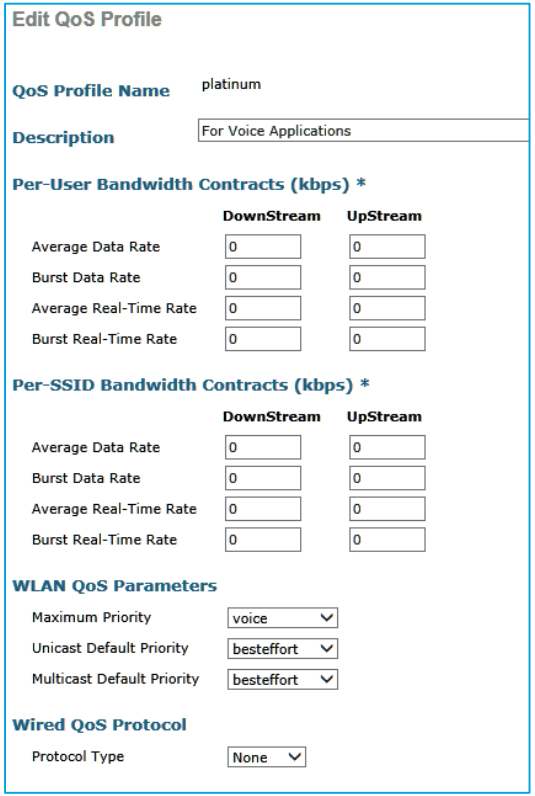
Cisco-AP

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

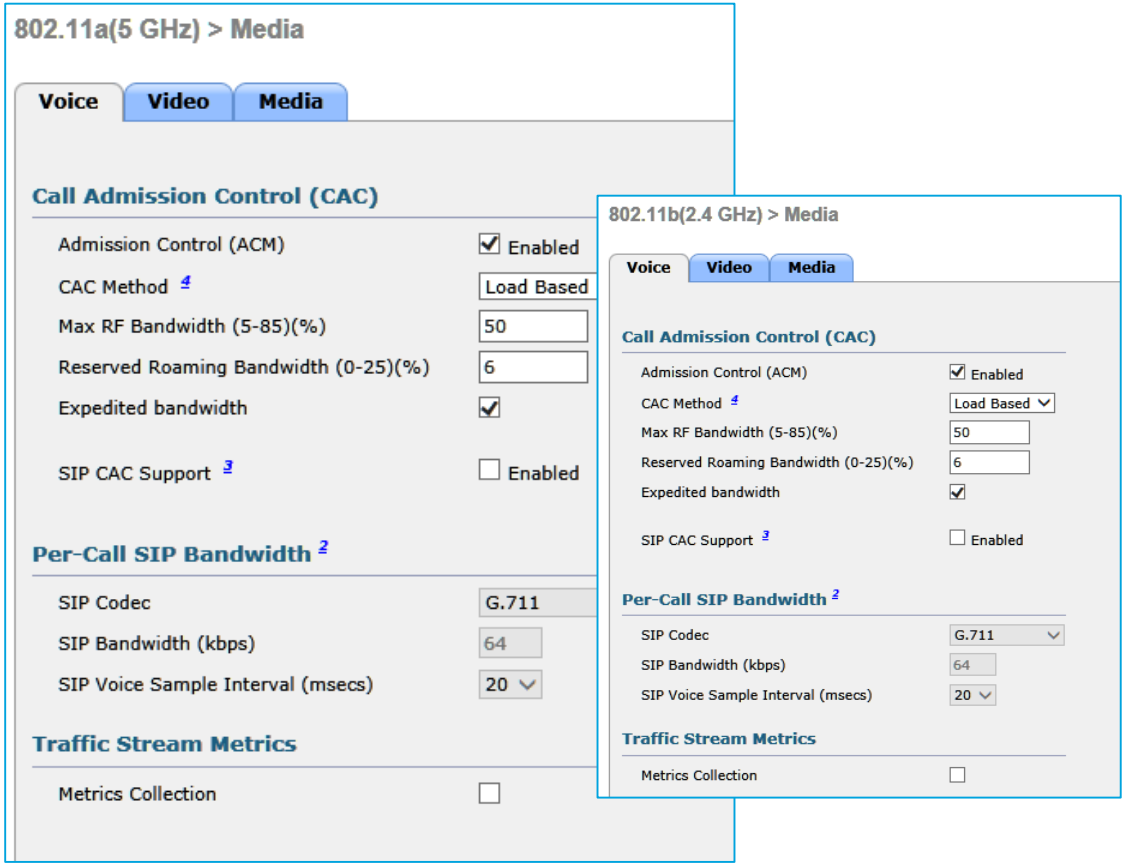






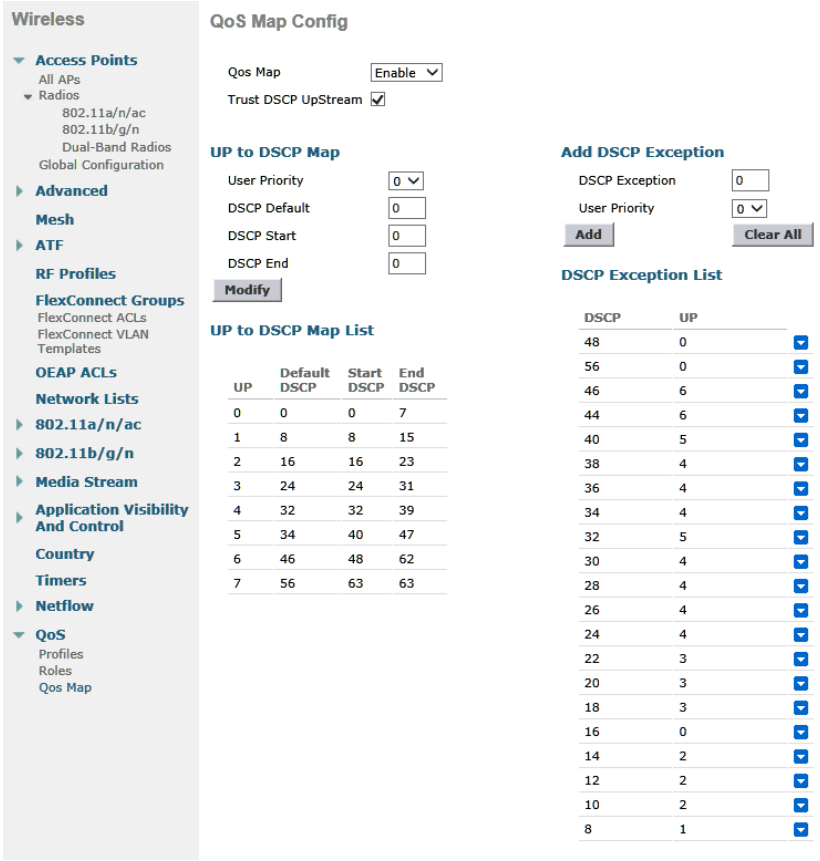
Fast Lane

- Enabling Fast Lane 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



Fast Lane

- Enabling Fast Lane 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

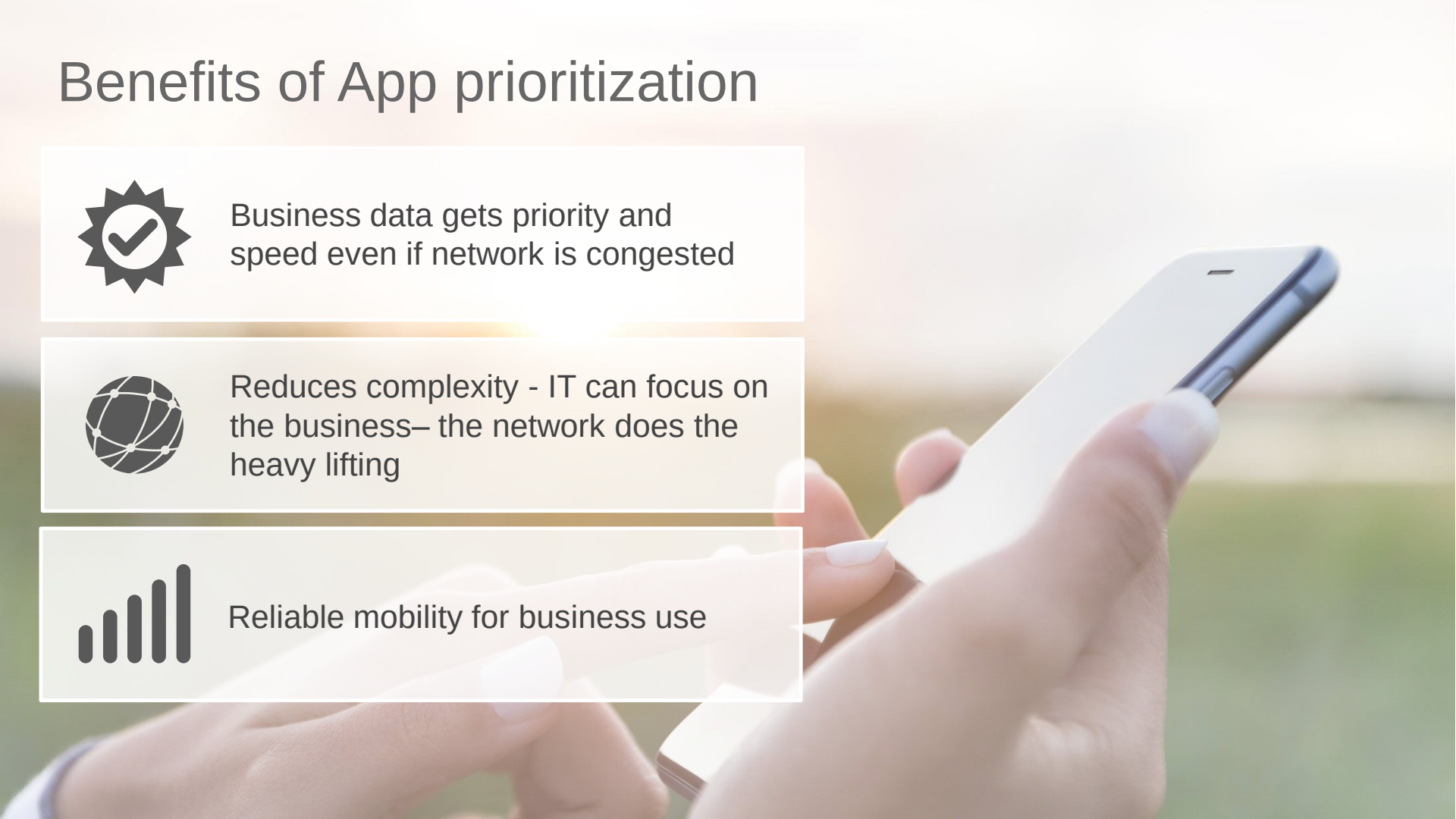


Benefits of App prioritization

Business data gets priority and speed even if network is congested

Reduces complexity - IT can focus on the business– the network does the heavy lifting

Reliable mobility for business use



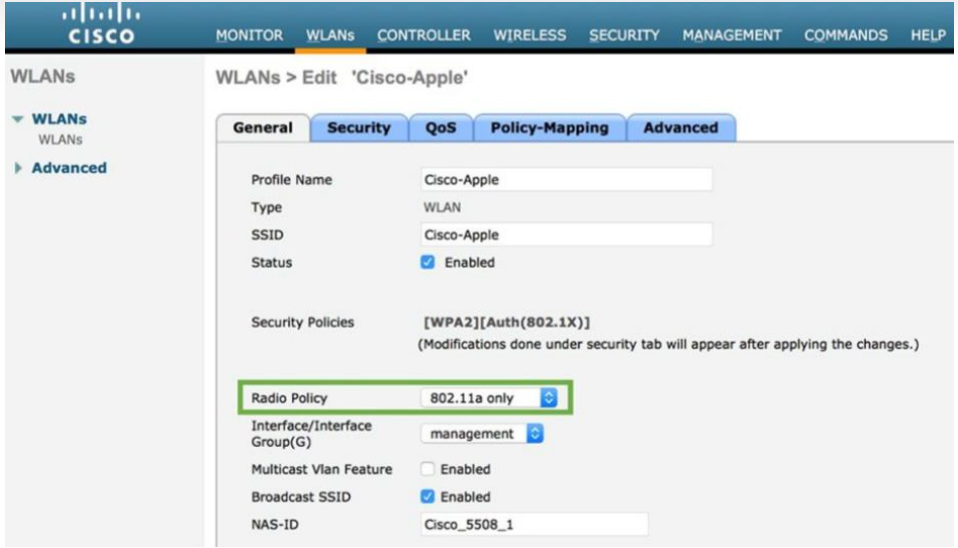
Cisco & Apple : Upgrade to Latest iOS version

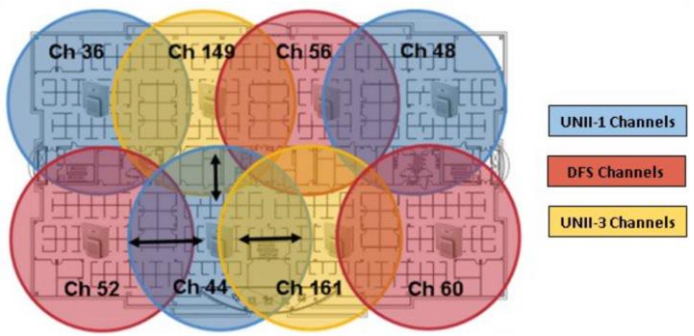
- Although many of the enterprise feature like 802.11r and 802.11k were introduced starting with Apple iOS 6.0 update, Apple recommends upgrading all the devices to the latest iOS

http://www.apple.com/ios/whats-new/

Cisco & Apple : 5 GHz Channel preferred

- Cisco recommends a 5 GHz only network and coverage design for all apple devices.





5 GHz band less affected by non-802.11 sources of interferences and more channels available

Cisco & Apple : RF design recommendations

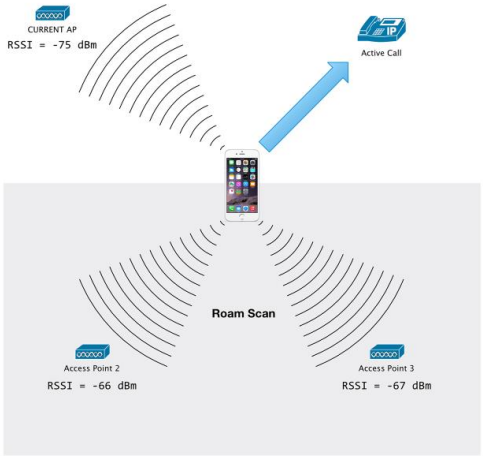
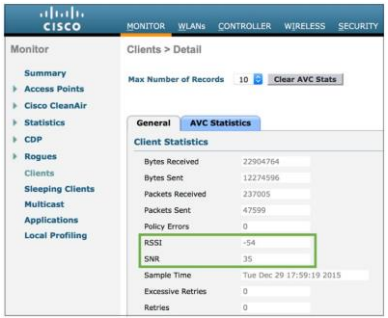


Image courtesy: https://support.apple.com/en-us/HT203068

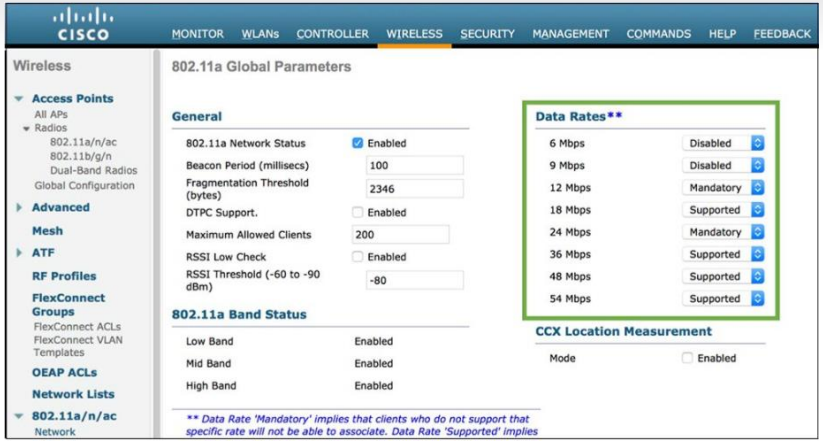
- Channel Utilization < 40%.
- Client SNR >= 25 dB.
- 802.11 retransmissions < 15%
- Packet Loss < 1%
- Jitter < 100 ms.

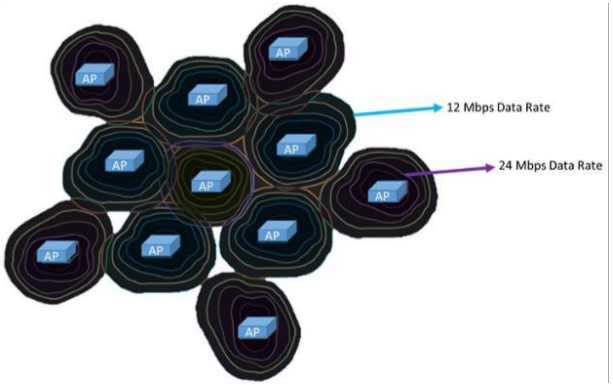


Apple client device should observe a minimum of 2 APs with an RSSI measurement of -67 dBm

Cisco & Apple : Data Rates

Wireless > 802.11a/n/ac > Network





- Cisco highly recommends leaving all MCS rates enabled

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

Network Requirements for the Digital Organization

Self-Aware

Insights | Experiences

Self-Optimizing

Automation | Assurance

Self-Defending

Security | Compliance

Visibility and Analytics
Driving change through insight

Speed and Simplicity
Innovating beyond the standard

Threat Defense
Protecting the business and users

Self-Healing Infrastructure

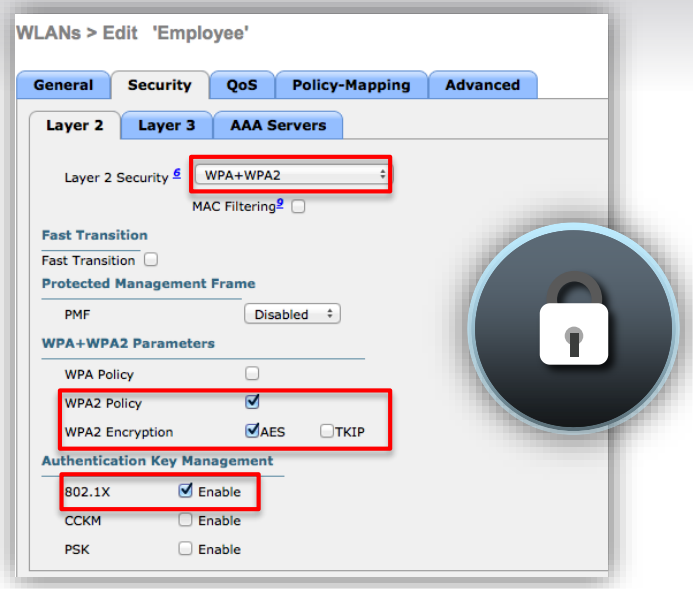
Infra Software | Highly Available

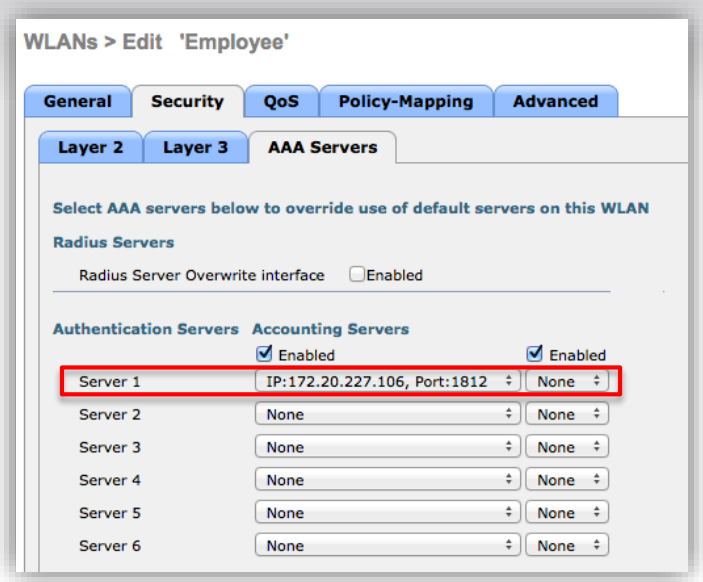
Always on, Always ready

Self-Defending : Security and Compliance

Security : Enable 802.1x authentications on WLAN

WLANs → Edit ‘WLAN_NAME’ → Security

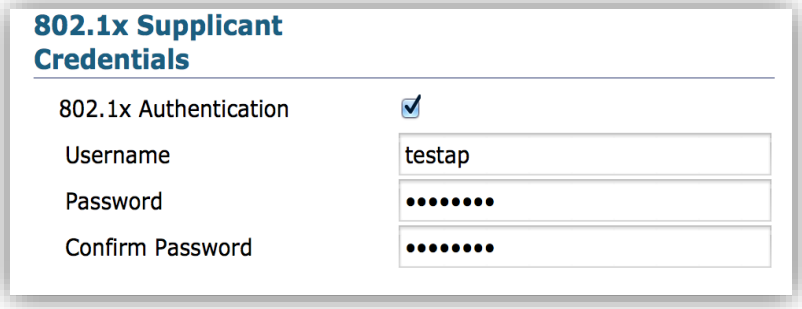




Provides greater network security on WLAN using 802.1x authentication

Security: Enable 802.1x authentications for AP

Wireless → Access Points → Global Configurations



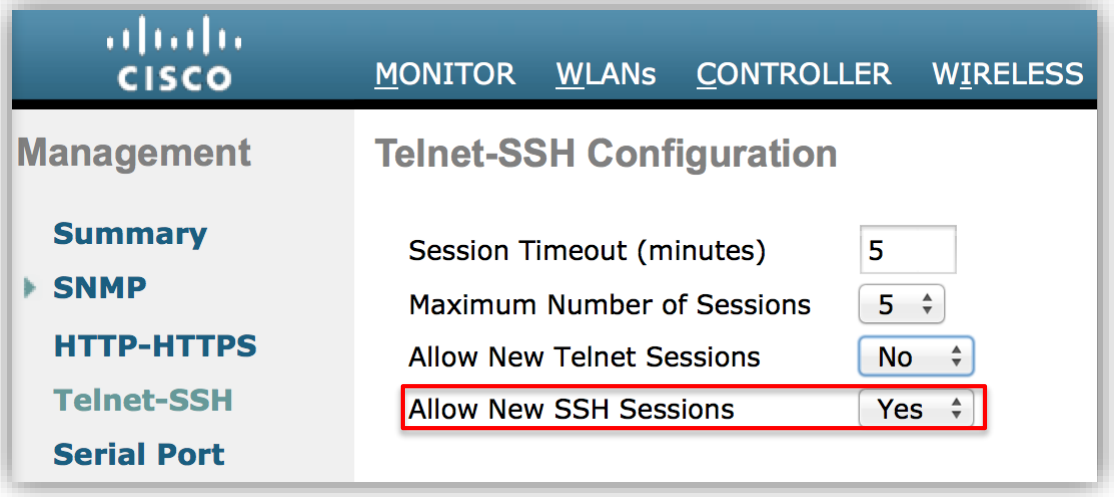

```
To enable 802.1X authentication on a switch port, on the switch CLI, enter
these commands:
Switch# configure terminal
Switch(config)# dot1x system-auth-control
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# radius-server host ip_addr auth-port 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 by enabling 802.1x on the switch port where AP is connected. Not supported for Mesh deployments

Security: Enable Secure Management Access

Management → Telnet–SSH

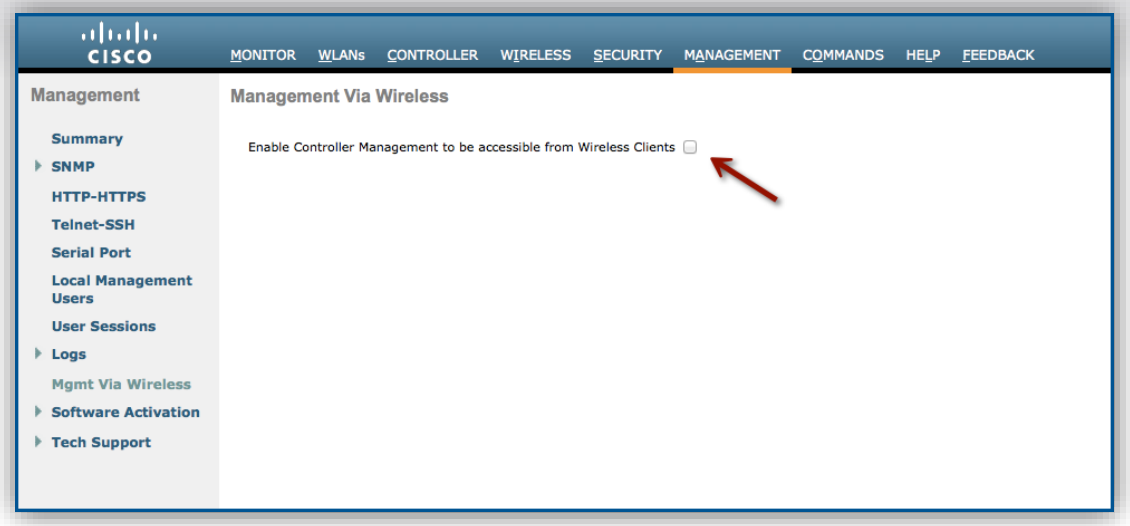
Disable Telnet and enable SSH as the default option



Provides greater security by allowing secure access and denying unencrypted access

Security: Disable Management Over Wireless

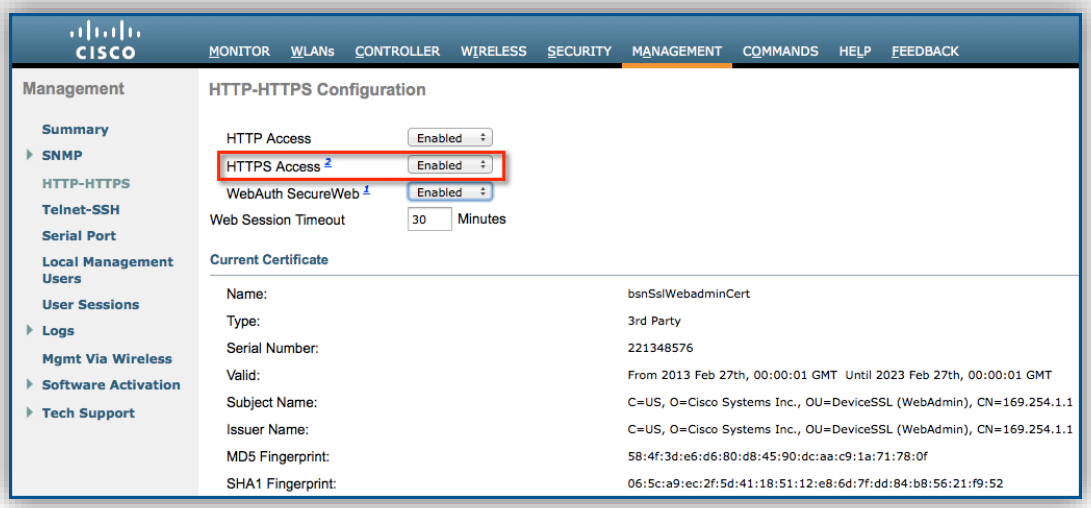
Management → Mgmt Via Wireless



Disallow management of the Controller via Wireless

Security: Secure Web Access (HTTPS)

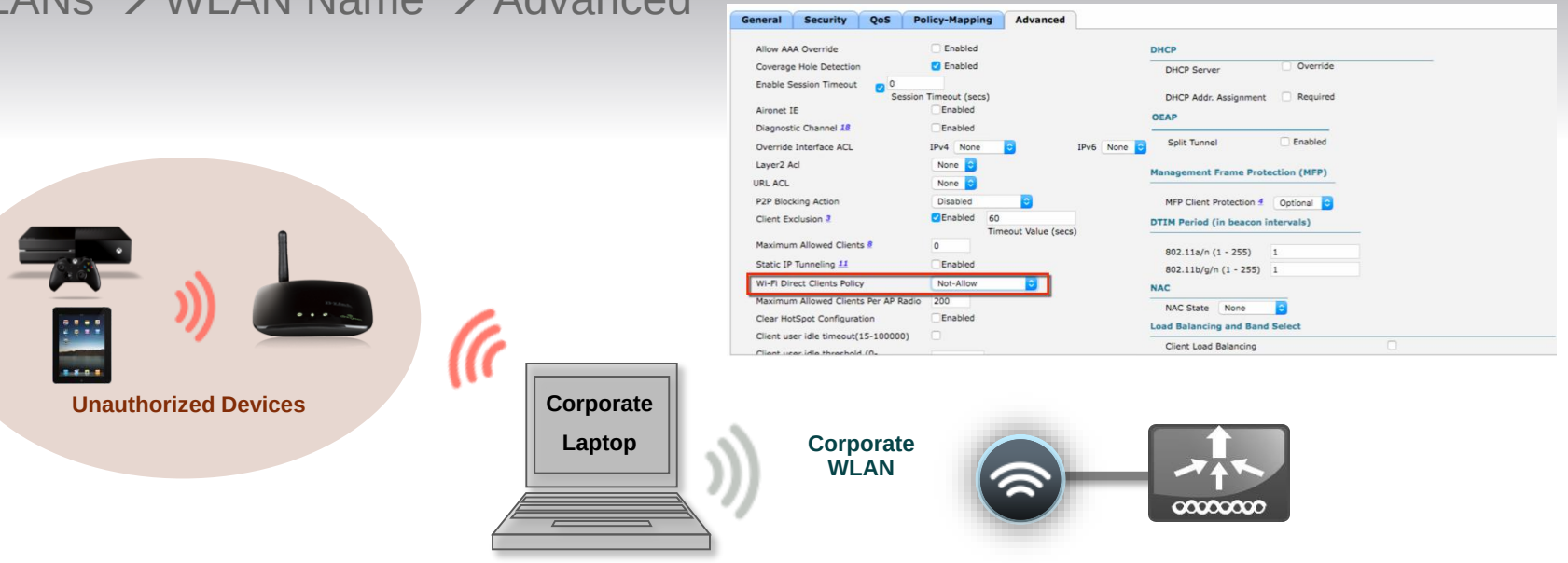
Management → HTTP-HTTPS



Provides greater security by allowing secure access

Security : Disable WiFi Direct

WLANs → WLAN Name → Advanced



Prevent security hole if the device is connected to both the infrastructure and a Personal Area Network (PAN) at the same time. Will break Android devices

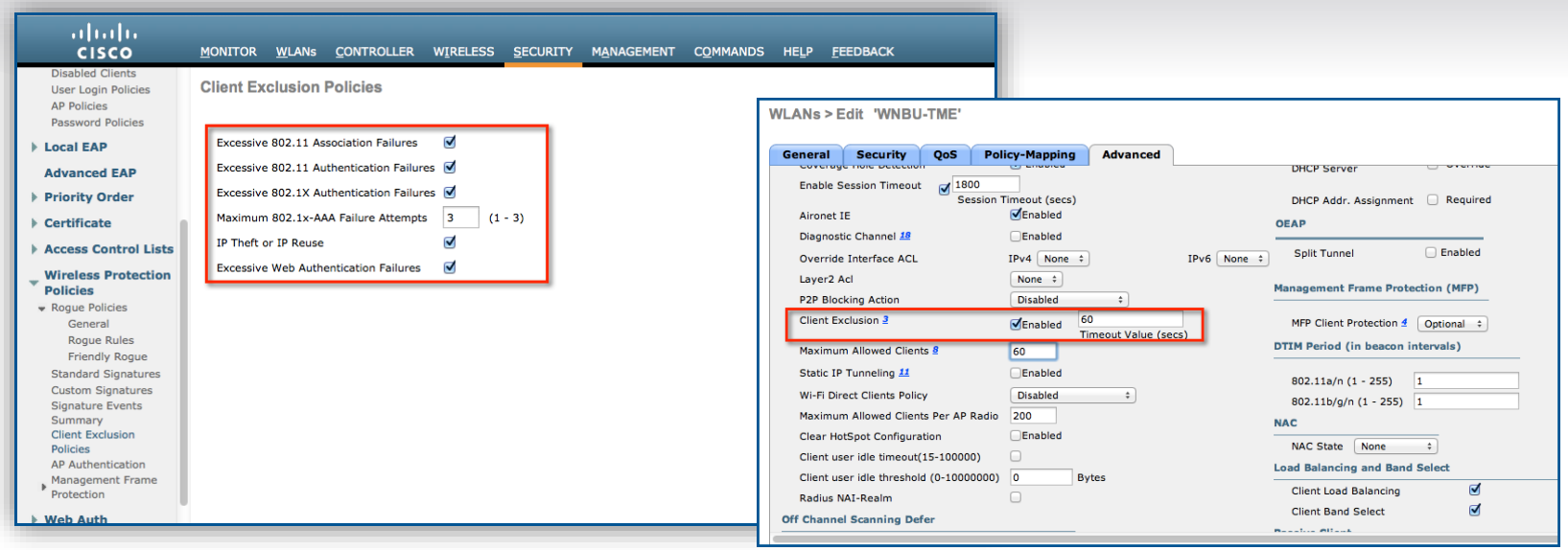
Security: Enable User Login Policies

Security → AAA → User Login Policies

Prevent login attacks by restricting the numbers the users who can use the same login credentials between 1 - 5

Security: Enable Client Exclusion Policies

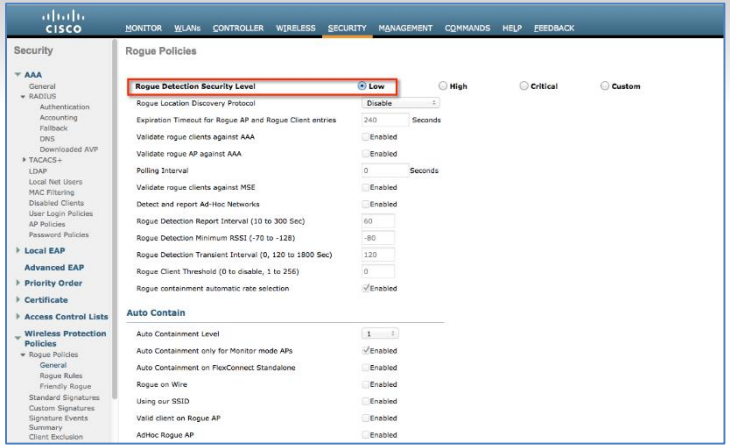
Security → Wireless Protection Policies →Client Exclusion Policies

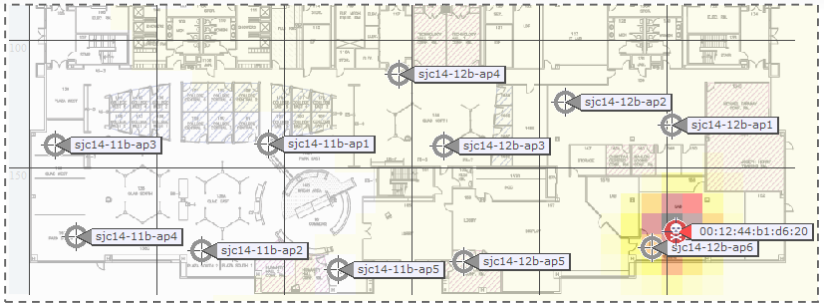


Enable exclusion policies to prevent the network from Assoc/Auth failure attacks. Disable for Voice deployments 180 seconds is the recommended default with ISE though 60 seconds is the WLC default. The reason behind this is the minimum reject interval on ISE for miss-configured supplicant detection is 5 minutes or 300 seconds

Security: Enable Rogue Policies

Security → Wireless Protection Policies → Rogue Policies → General → Low





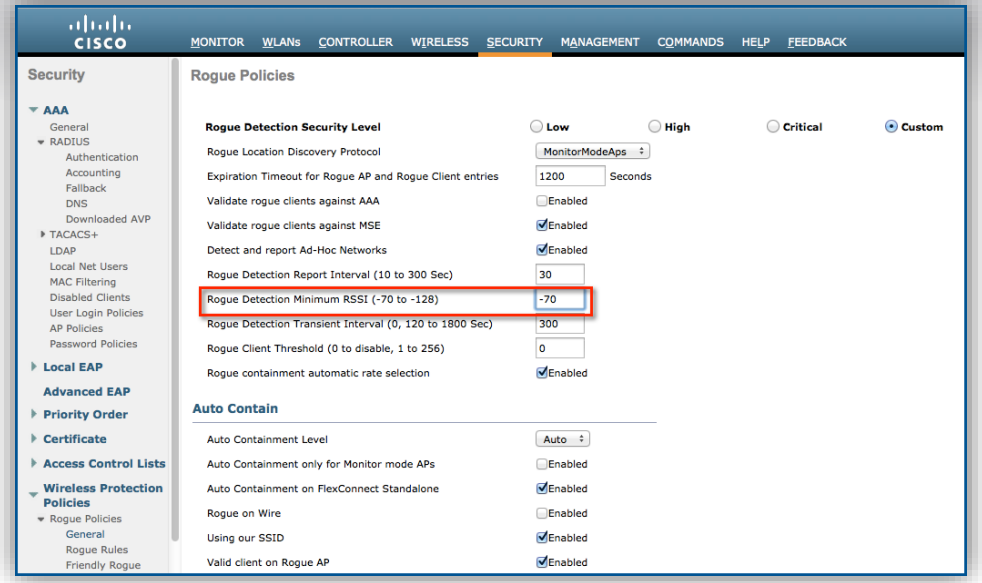
Friendly

Malicious

The Rogue Detection Security Level should be set at a minimum to “low”

Security: Set Rogue Detection RSSI

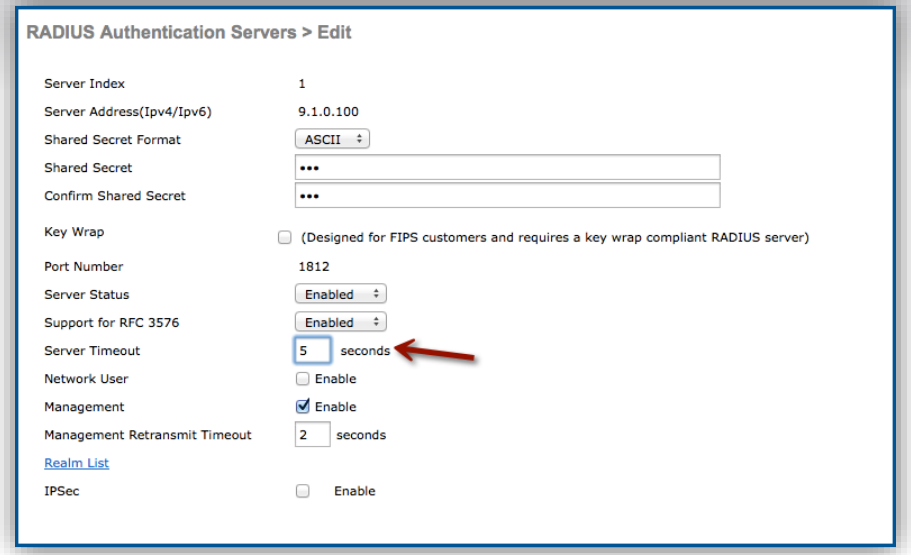
Security → Wireless Protection Policies → Rogue Policies → General



Set Rogue Detection Minimum Threshold to -70 to -75 dBm

BYOD: Radius Timeout >=5 sec

Security → AAA → RADIUS → Authentication



To prevent pre-mature failover since the default of 2 seconds is generally low for ISE as ISE relies on backend databases for user lookups and group fetches. Too high causes queue issues on WLC

BYOD : Disable Aggressive Failover

- **`config radius aggressive-failover disable`** command to disable the aggressive failover feature

- **`show radius summary`** to check the status of this feature

- Only fails over to the next AAA server if there are three consecutive clients that fail to receive a response from the RADIUS server

In some circumstances it can cause the WLC to pre-maturely mark ISE dead in times of high load and cause additional load on ISE

Your poll will show here

1

Install the app from
pollev.com/app

2

Make sure you are in
Slide Show mode

Still not working? Get help at pollev.com/app/help
or
Open poll in your web browser

Network Requirements for the Digital Organization

Self-Aware

Insights | Experiences

Self-Optimizing

Automation | Assurance

Self-Defending

Security | Compliance

Visibility and Analytics
Driving change through insight

Speed and Simplicity
Innovating beyond the standard

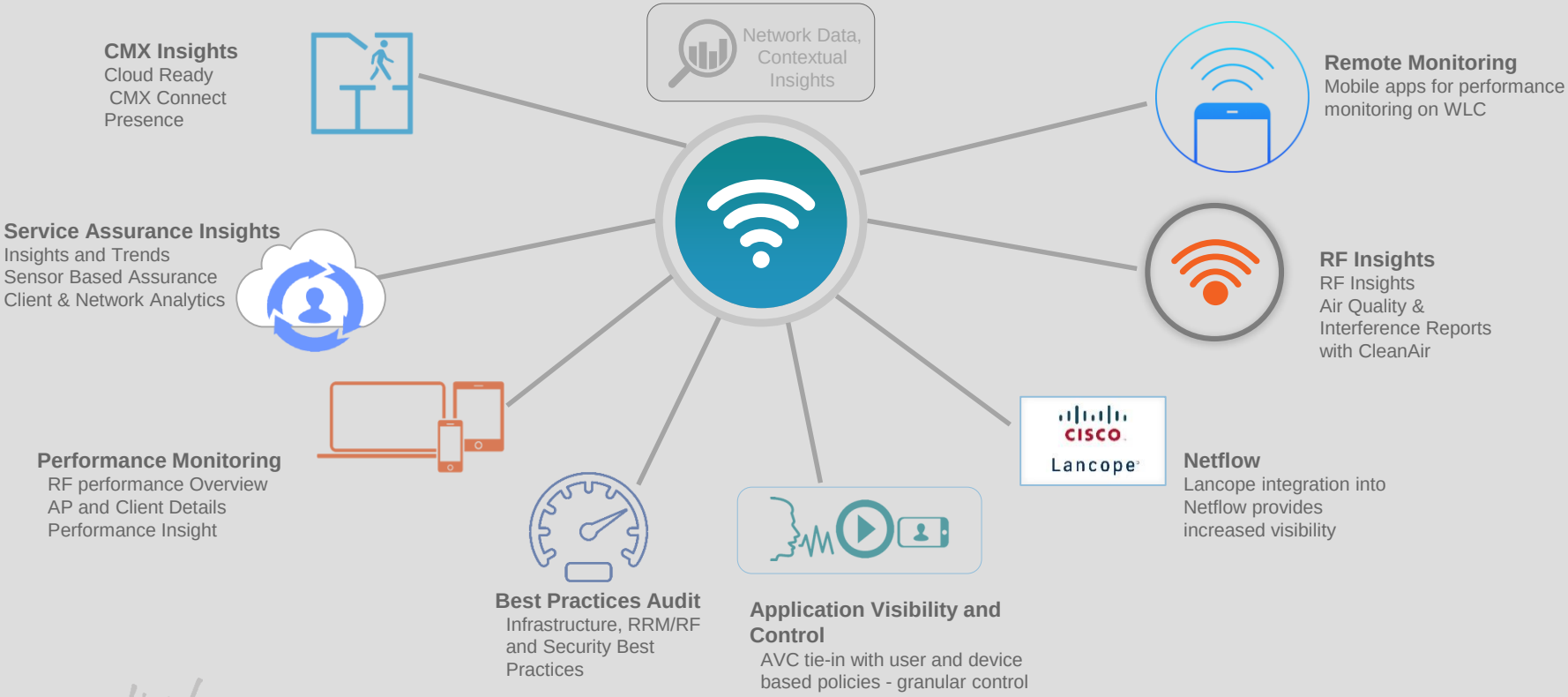
Threat Defense
Protecting the business and users

Self-Healing Infrastructure

Infra Software | Highly Available

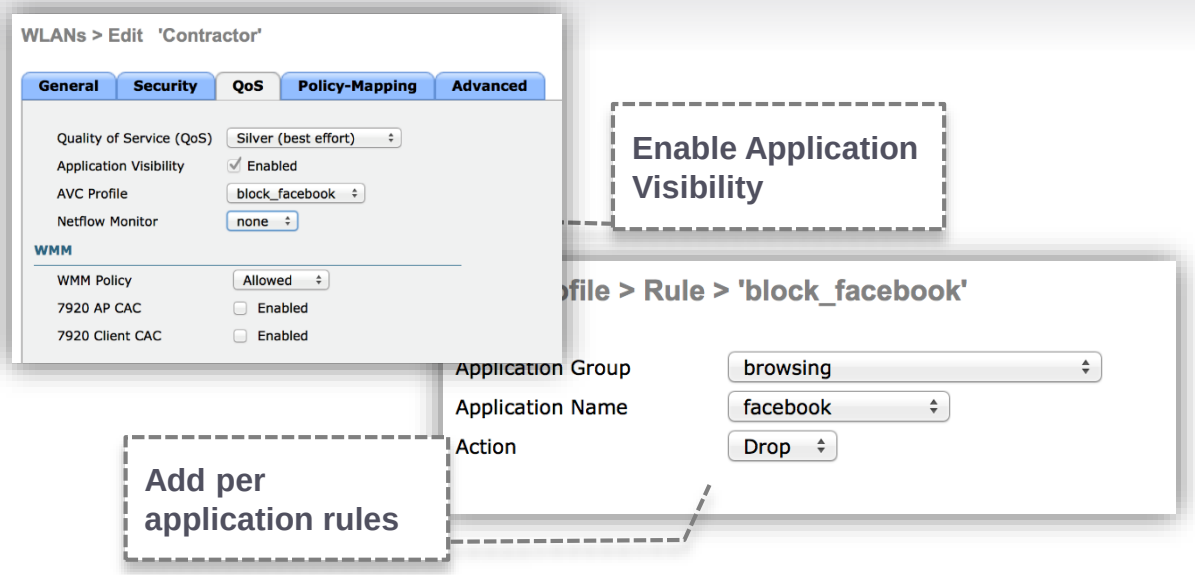
Always on, Always ready

Self-Aware : Insights and Experiences



Application Visibility : Enable AVC and Netflow

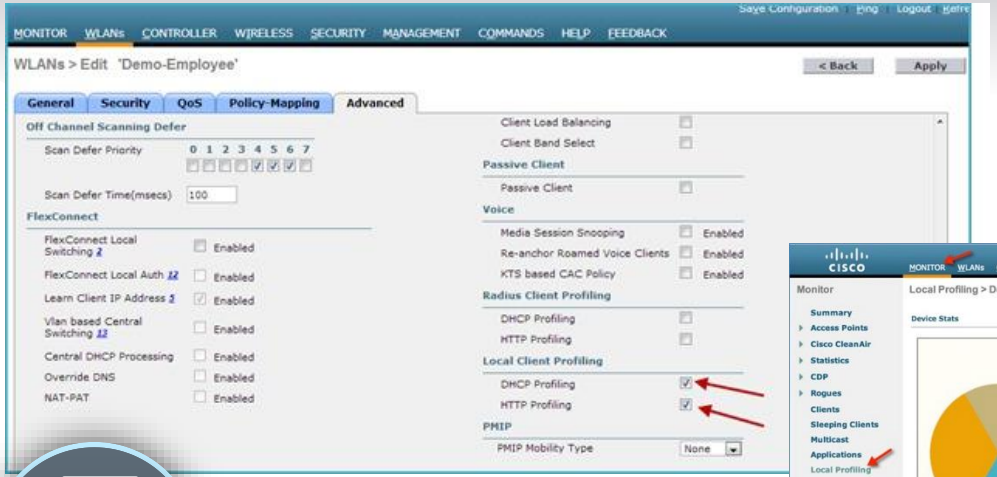
Wireless → Application Visibility and Control → AVC Profiles



Classifies applications, provides real-time analysis, and allows users to drop or mark data. Per-user, per-device granularity for control

Device Visibility : Enable Local Profiling

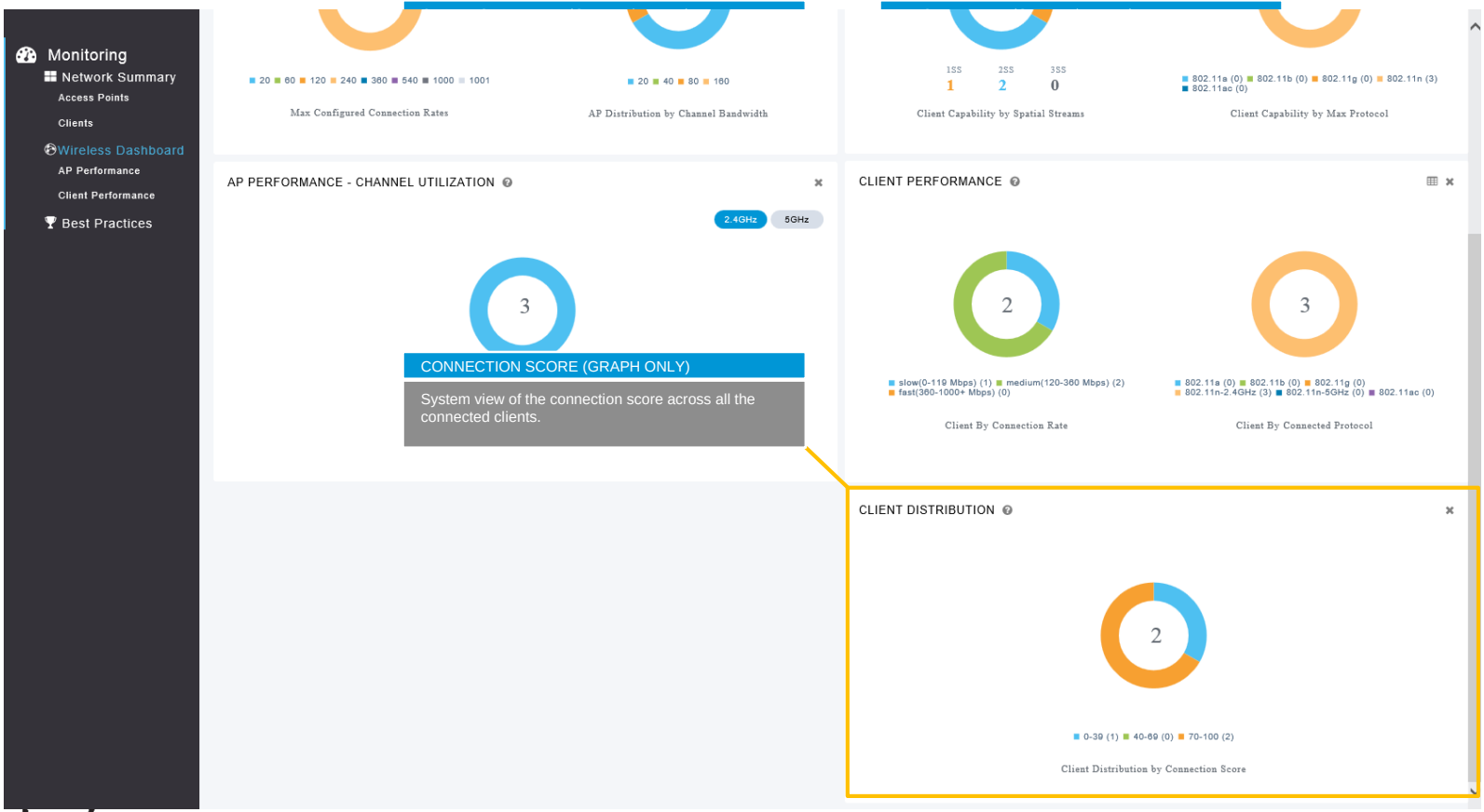
WLANs → Edit → WLAN_NAME → Advanced



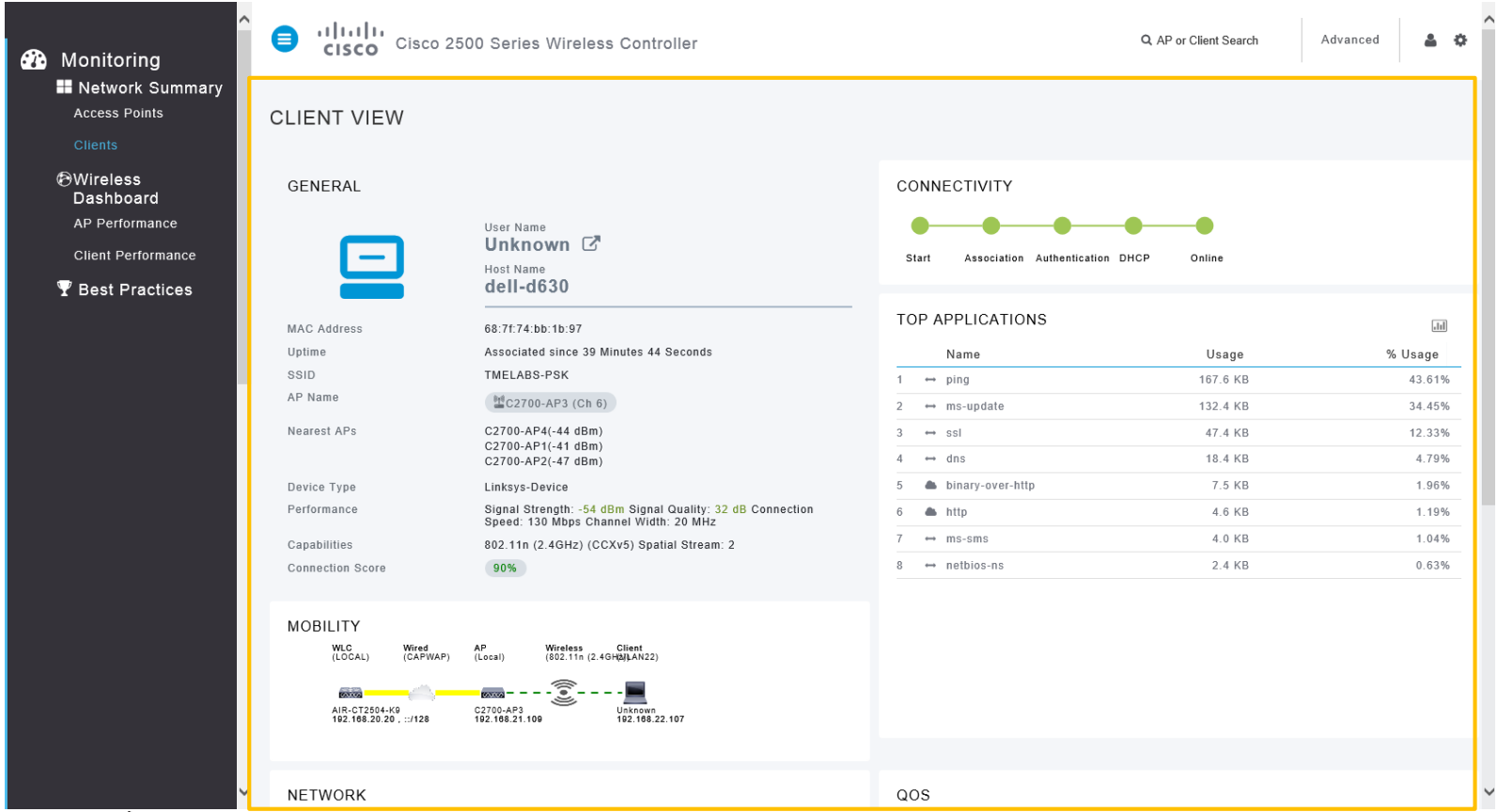
Client devices can be profiled based on their manufacturer and operating system

Monitoring Wireless Performance

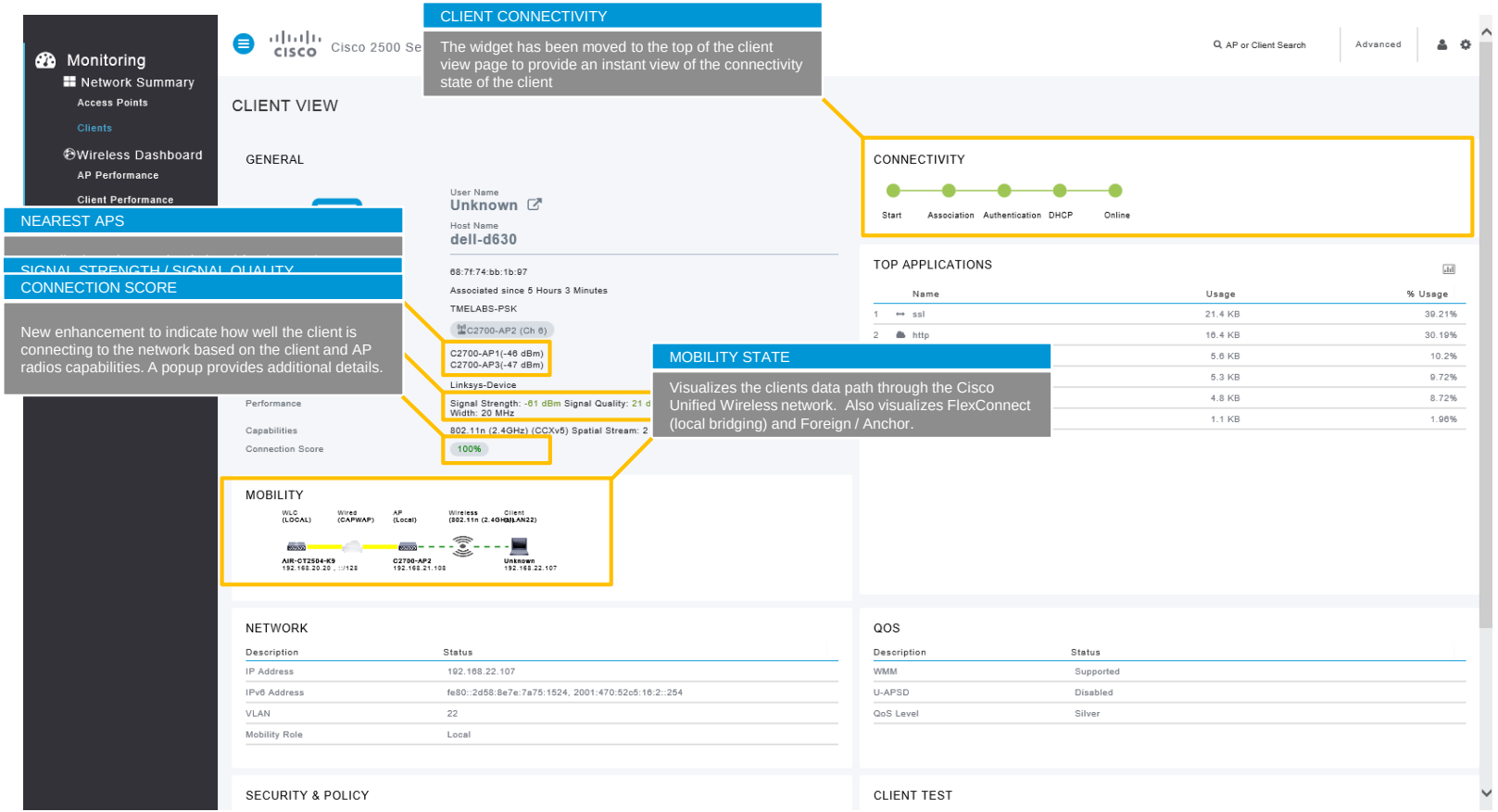
Wireless Dashboard – What does it show?



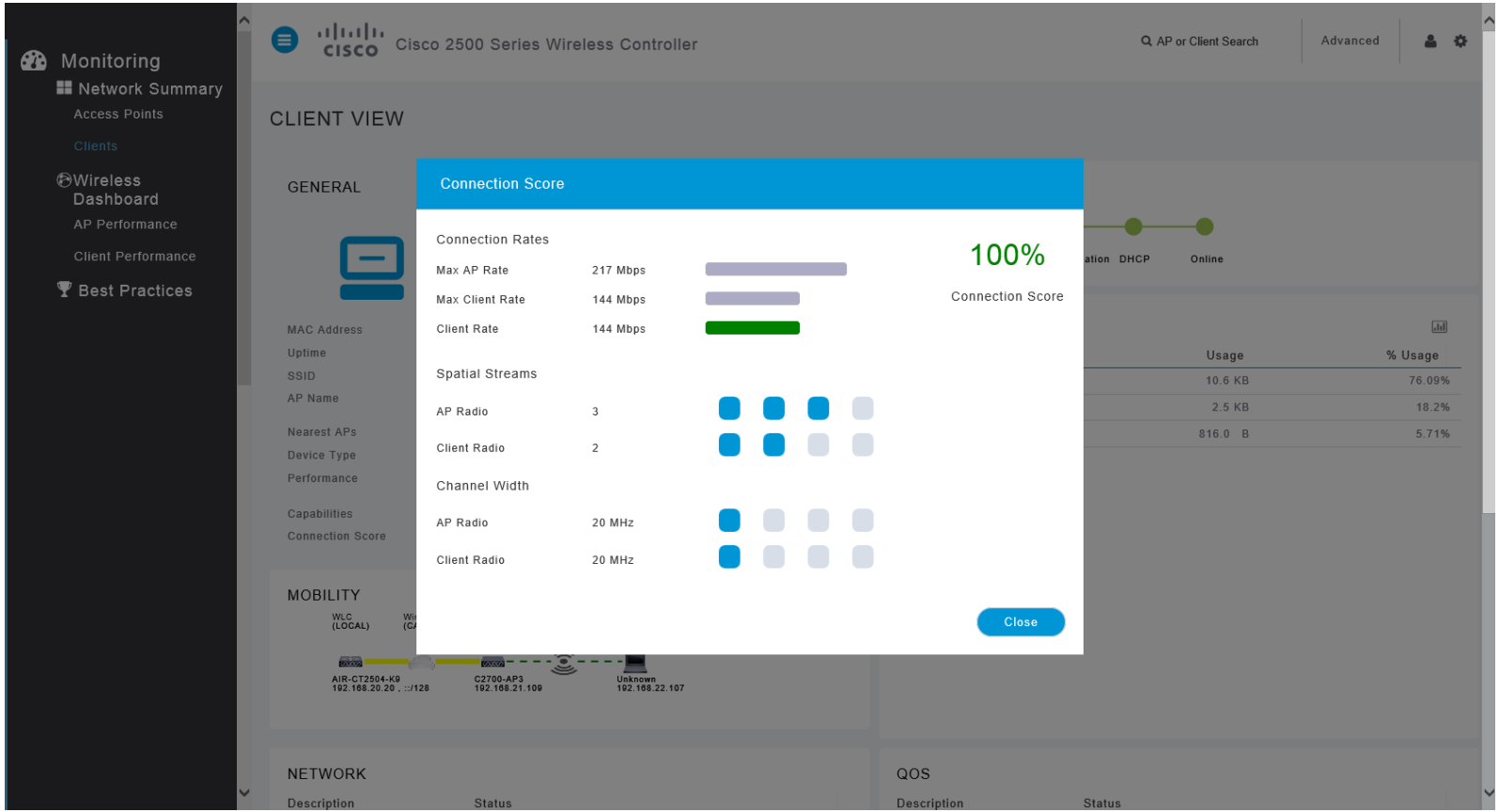
Client View – Where do I find it?



Client View – Enhancements



Connection Score – Where do I find it?



Connection Score – What does it show?

AP MAX CONFIGURED

CLIENT MAX CAPABILITY

CLIENT ACTUAL RATE

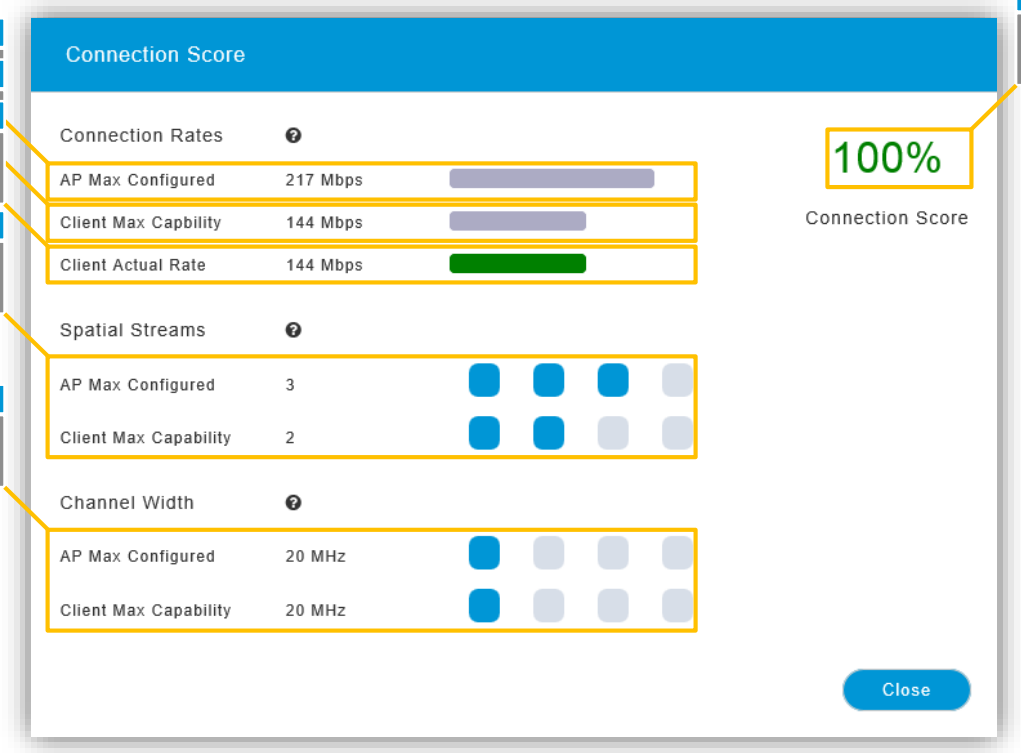
The current data rate of the client (reported by the AP).

SPATIAL STREAMS

The number of spatial streams supported by the AP radio and advertised by the client.

CHANNEL WIDTH

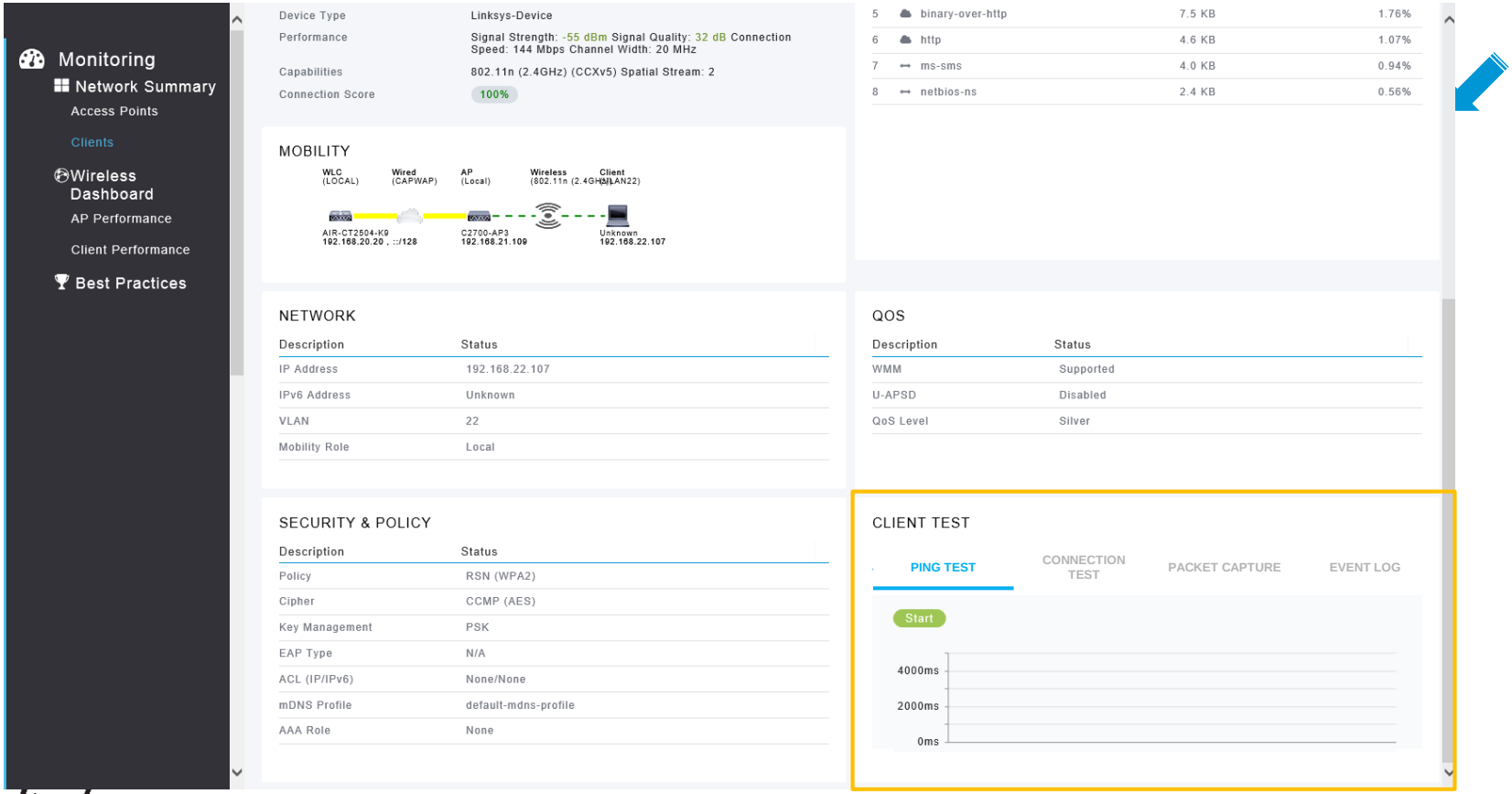
The number of spatial streams supported by the AP radio and advertised by the client.



CONNECTION SCORE

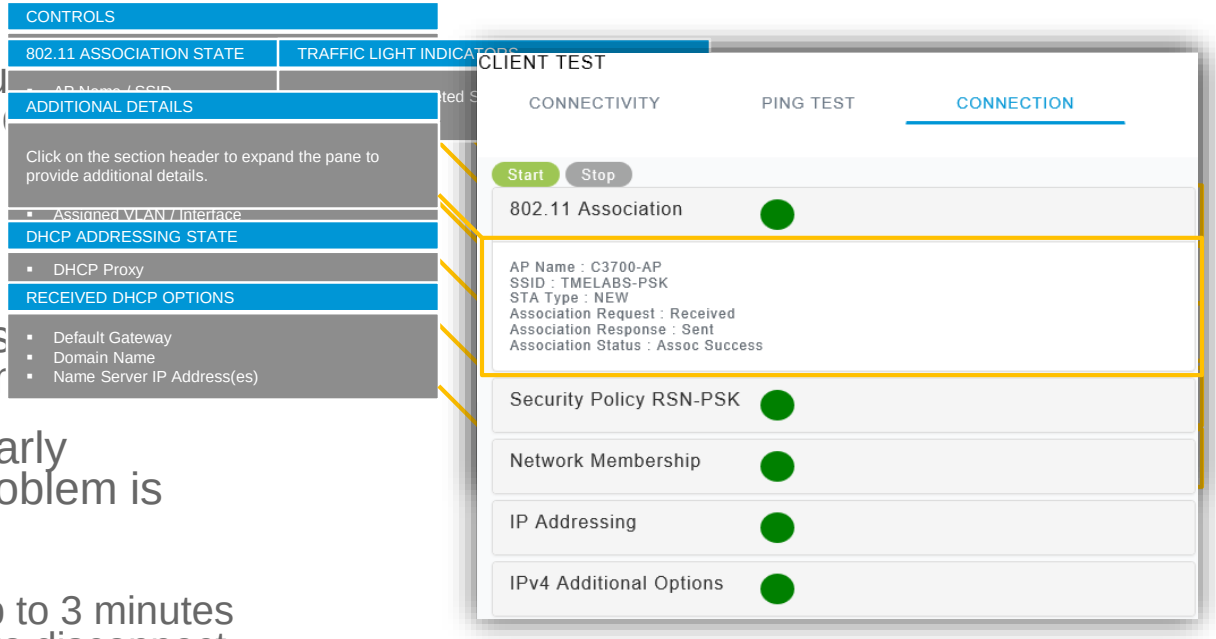
% value based on the Client Actual Rate divided by either the Client Max Capability or Max AP Configured (whichever is lower).

Client Troubleshooting – Where do I find it?



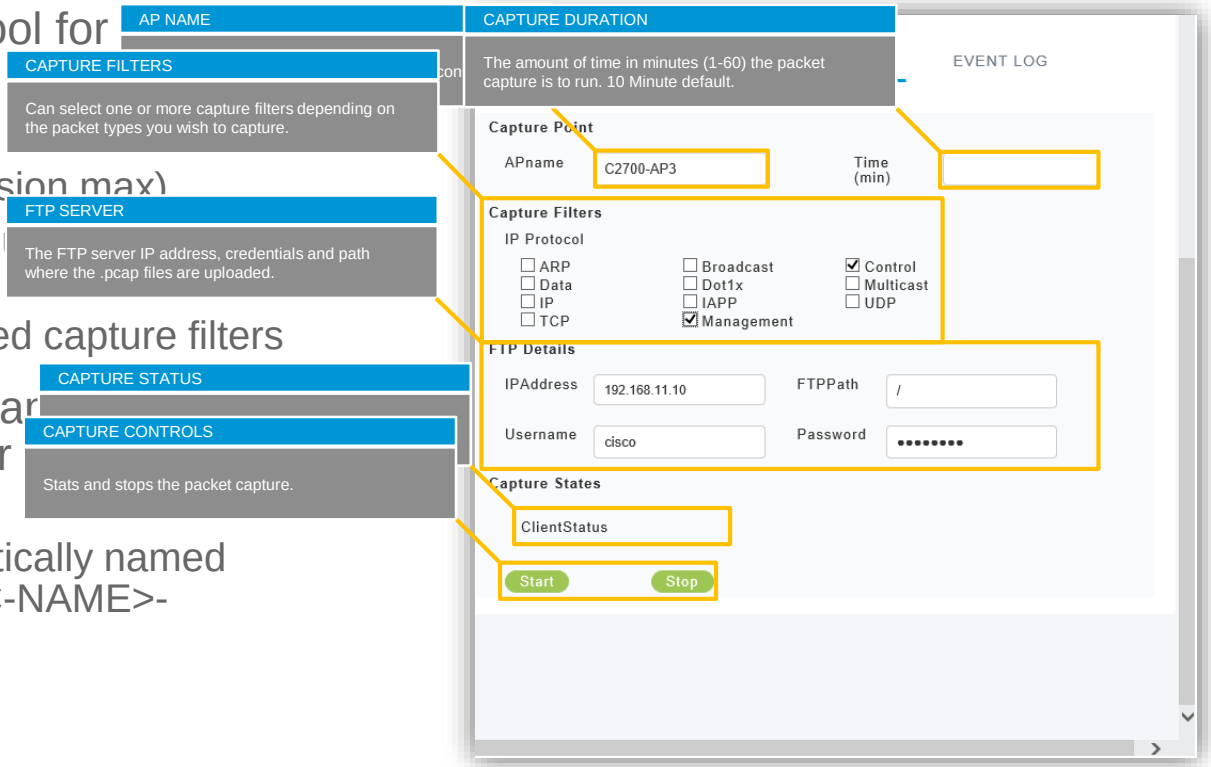
Client Troubleshooting – Connection Test

- A helpdesk level tool for qu
  client connection troublesh
  - 802.11 Phases
  - IP Addressing
  - Network Membership
- Traffic light indicators to vis
  determine where a problem
- Simple messaging that clearly communicates what the problem is
- Enabled per client
  - Once initiated will run for up to 3 minutes allowing the end-user time to disconnect and re-connect the client to the network



Client Troubleshooting – Packet Capture

- 802.11 packet capture tool for administrators and TAC
  - Previously only available
  - Enabled per client (1 session max)
  - Capture times 1 – 60 min (1 minutes)
  - 802.11 and Protocol based capture filters
- Packet captures are strea server in .pcap format for analysis
  - Capture files are automatically named using <AP-NAME><WLC-NAME>-<DATE>_<TIME>



Your poll will show here

1

Install the app from
pollev.com/app

2

Make sure you are in
Slide Show mode

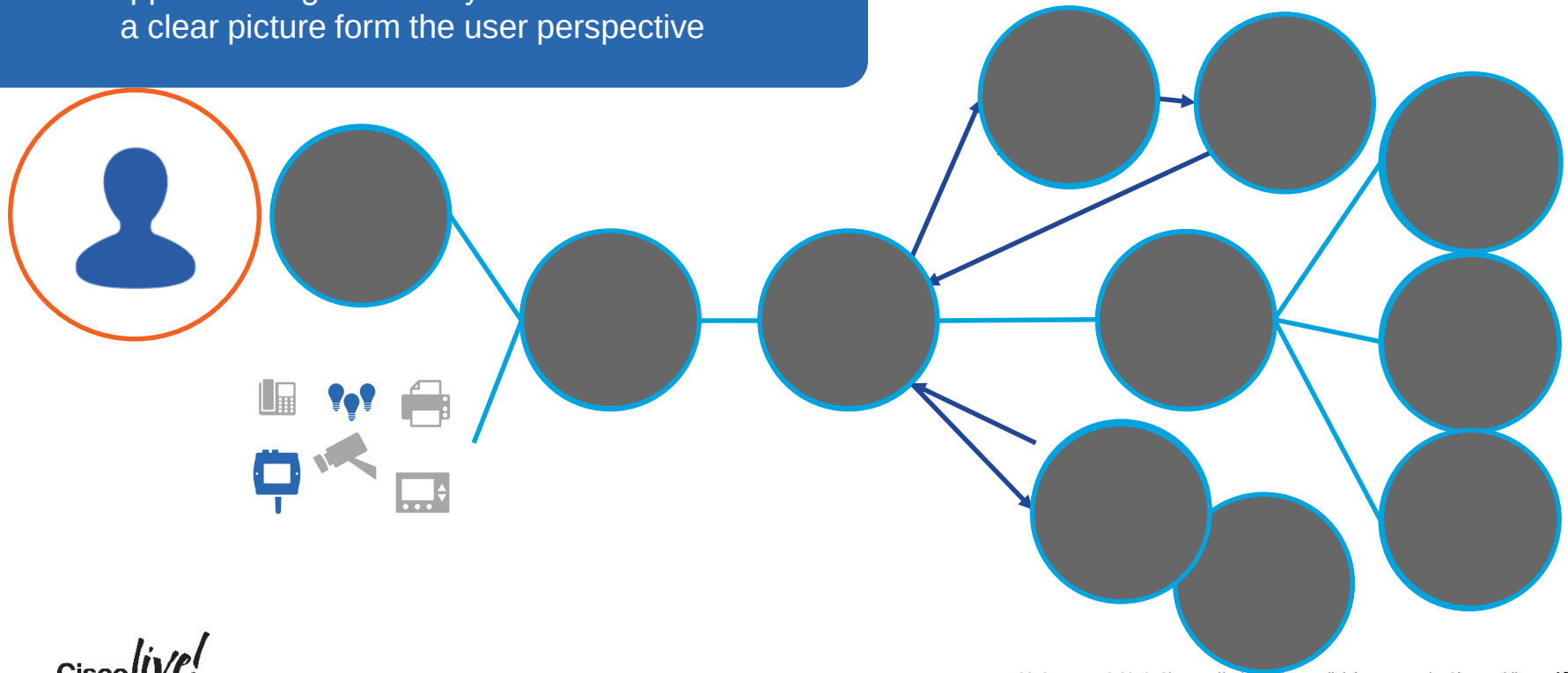
Still not working? Get help at pollev.com/app/help
or
Open poll in your web browser

Wireless Service Assurance

Client, Network, Application Insights On Cloud

Assuring Client Experience

Client-in approach: Aligns to today's workflows and delivers a clear picture form the user perspective



Your poll will show here

1

Install the app from
pollev.com/app

2

Make sure you are in
Slide Show mode

Still not working? Get help at pollev.com/app/help
or
Open poll in your web browser

Your poll will show here

1

Install the app from
pollev.com/app

2

Make sure you are in
Slide Show mode

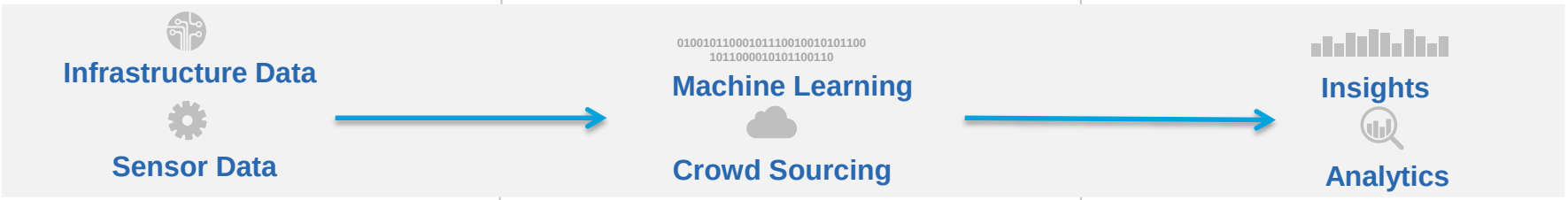
Still not working? Get help at pollev.com/app/help
or
Open poll in your web browser

Vision of Network Assurance

Surface undetected client and network anomalies

Fix real time issues and get insight into historic trends and errors

Predict Client and network issues before they occur



Automate tools to discover outliers

Root cause issues in **few Clicks**

Build **Resilient** and **Reliable** Networks

Wireless Service Assurance Use-Cases

What are we trying to solve ?

Network Health Before users come in

- Sanity Checking
- Base-lining

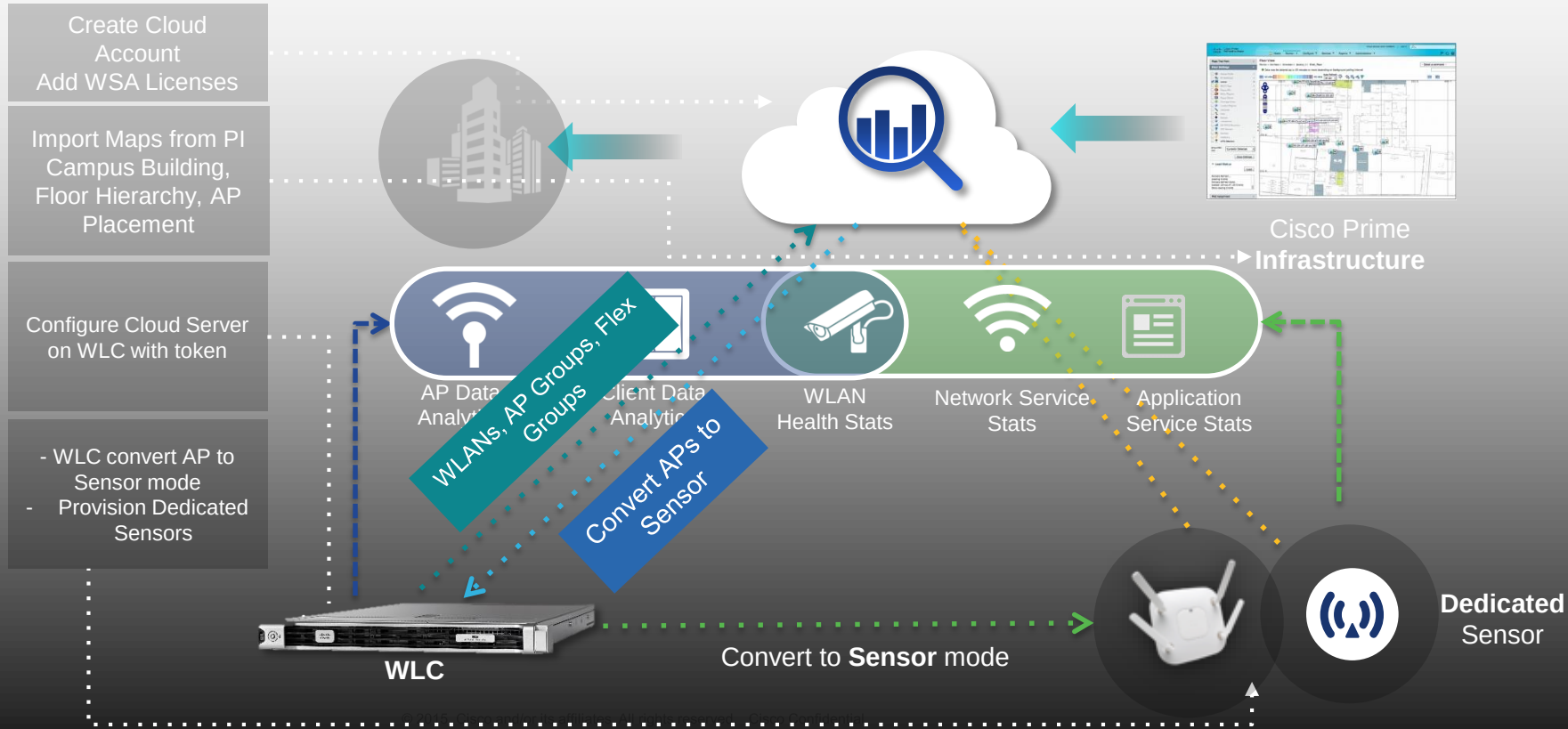
Network Health at Peak Traffic

- Proactively monitor Issues and trends
- Spot and fix issue before it causes downtime
- Quick remediation of Real-time Issues

Network Health Historically

- Analyze and troubleshoot historical events
- Retrospect and Reporting*

Wireless Service Assurance Architecture



Best Practices Recommendations

For Your Reference

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 WiFi 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

http://www.cisco.com/c/en/us/td/docs/wireless/technology/wlc/82463-wlc-config-best-practice.html

Key Takeaways

Self-Defending

Protect Business and Users with Security and Compliance

Self-Healing

Always on, Always Ready Robust Network

Self-Optimizing

Innovating Beyond the Standard with Assurance and Automation

Self-Aware

Driving Change through insight and visibility

References

- Wireless LAN Controller Best Practices

http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82463-wlc-config-best-practice.html

- Cisco & Apple Best Practices

http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-2/b_Enterprise_Best_Practices_for_Apple_Devices_on_Cisco_Wireless_LAN.html

- Mobility Design Guide 8.1

http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/Enterprise-Mobility-8-1-Design-Guide/Enterprise_Mobility_8-1_Deployment_Guide.html

- Cisco Active Advisor

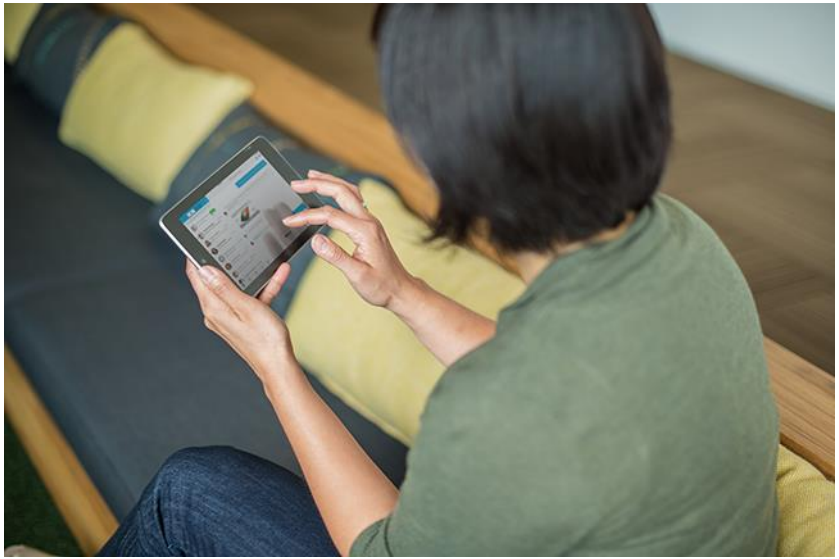
https://www.ciscoactiveadvisor.com

- Config Analyzer

https://upload.cisco.com/cgi-bin/swc/fileexg/main.cgi?CONTYPES=wlc-conf-app-dev

Complete Your Online Session Evaluation

- Give us your feedback to be entered into a Daily Survey Drawing. A daily winner will receive a $750 Amazon gift card.
- Complete your session surveys through the Cisco Live mobile app or from the Session Catalog on CiscoLive.com/us.



Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at CiscoLive.com/Online

Continue Your Education

- Demos in the Cisco campus
- Walk-in Self-Paced Labs
- Lunch & Learn
- Meet the Engineer 1:1 meetings
- Related sessions

Please join us for the Service Provider Innovation Talk featuring:

Yvette Kanouff | Senior Vice President and General Manager, SP Business

Joe Cozzolino | Senior Vice President, Cisco Services

Thursday, July 14th, 2016

11:30 am - 12:30 pm, In the Oceanside A room

What to expect from this innovation talk

- Insights on market trends and forecasts
- Preview of key technologies and capabilities
- Innovative demonstrations of the latest and greatest products
- Better understanding of how Cisco can help you succeed

Register to attend the session live now or watch the broadcast on cisco.com

Thank you


cisco
Cisco live!
July 10-14, 2016 • Las Vegas, NV