



*TOMORROW
starts here.*

Cisco *live!*



Best Practices for Configuring Cisco Wireless LAN Controllers

BRKEWN-2670

Aparajita Sood

Technical Marketing Engineer, Enterprise Networking

#clmel

Cisco *live!*

Agenda

- What is Best Practices?
- Best Practice Check Points
- WLAN Express Setup
- User-First Dashboard View
- Upgrade Audit Workflow Compliance
- WLC Config Analyser
- Cisco Active Advisor
- Best Practice Recommendations
 - Infrastructure, RRM & RF, Security & BYOD, FlexConnect, Mesh



Best Practice Check Points

Best Practice Check Points

Measuring Compliance

WLC

WLAN Express
Setup

7.6 MR2, 8.0, 8.1

**Best Practices defaults,
RF Parameter Optimisation,
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 time

WLC

Upgrade Audit
Workflow

8.1

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

- Compliance metric and reporting natively on WLC
- 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
Analyser

**Windows Executable
“show run-config” Based
Analyser Tool**

- Downloadable client
- Configuration stays local
- 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
Agentless – nothing to
download**

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

Cisco *live!*

Cisco Wireless LAN Controller Configuration Best Practices

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

Cisco 5500 Series Wireless Controllers

Cisco Wireless LAN Controller Configuration Best Practices

HOME
SUPPORT
PRODUCT SUPPORT
WIRELESS
CISCO 5500 SERIES WIRELESS CONTROLLERS
DESIGN
DESIGN TECHNOTES

Cisco Wireless LAN Controller Configuration Best Practices

Table of Contents

- [Cisco Wireless LAN Controller \(WLC\) Configuration Best Practices](#)
- [Introduction](#)
- [Prerequisites](#)
- [Requirements](#)
- [Components Used](#)
- [Best Practices](#)
- [Network Design](#)
 - [Use PortFast on AP Connected Switch Ports](#)
 - [Interfaces: Source \(DHCP, SNMP, RADIUS, Multicast, and so on\)](#)
 - [Recommended SwitchPort Modes and VLAN Pruning](#)
- [Network Connectivity](#)
 - [Use TAG Tagging for Management Interface](#)
 - [Use Multicast Forwarding Mode](#)
 - [Disable Internal DHCP](#)
- [Security](#)
 - [Disable Local EAP](#)
 - [WPA2 + 802.1X WLAN](#)
 - [Identity Design Tip - Use AAA Override](#)
 - [Use Faster RADIUS Timeout](#)
 - [EAP Identity Request Timeout](#)
 - [EAPoL Key Timeout and Max Retries](#)
 - [EAP Request Timeout and Max Retries](#)
 - [CCM TimeStamp Validation](#)
 - [TACACS+ Management Timeout](#)
 - [Enable Infrastructure and Client Management Frame Protection \(MFP\)](#)
 - [Enable 802.11e Support](#)
 - [Change SNMPv3 Default User](#)
 - [Enable Network Time Protocol \(NTP\)](#)
 - [Enable 802.11r Fast Transition](#)
 - [DHCP Required Option](#)
- [Rogue Management](#)
 - [Rogue Detection](#)
 - [Min-RSSI](#)
 - [Rogue Rules](#)
 - [WIFI Direct](#)
 - [Channels Scanning for Rogue](#)
 - [Transient Rogue Interval](#)
 - [Enable Ad-hoc Rogue Detection](#)
 - [Enable Rogue Clients AAA Validation](#)
 - [Enable Rogue Clients MSE Validation](#)
- [Wireless/RF](#)
 - [Disable Low Data Rates](#)
 - [Lower the Number of SSIDs](#)
 - [Enable Band Selection](#)
 - [Channel Widths](#)
- [Application Visibility and Control \(AVC\)](#)
 - [Enable 802.11k for Optimal Roaming](#)

Document View Count



A long-exposure photograph of a city street at night. The foreground is filled with vibrant, multi-colored light trails from moving vehicles, creating a sense of motion. In the background, a modern pedestrian bridge with blue lighting spans the street. Tall buildings with illuminated windows and storefronts line the street, and several flags are visible on the left side.

WLAN Express Setup

WLAN Express Setup

Express Setup Phase 1.0

- Release 7.6MR2 and 8.0
- WLAN express setup on 2504 only
- Some best practice features enabled as part of WLAN express setup
- Monitoring Dashboard – Top Access Points, Top Application, Top Client Devices etc.

Express Setup Phase 2.0



- Release 8.1
- Extended to 5508, 7510, 8510, vWLC, WiSM2*
- New Best Practice defaults introduced
- Pre-built Network and RF Profiles
- RF Dashboard – Access Point Performance, Client Performance charts

*WiSM2 does not support WLAN express setup and best practice defaults

Day0/Day1 Setup Best Practices

2504 WLC Best Practice defaults Extended to all WLCs



For Your
Reference

New
in 8.1

Feature	7.6 MR2, 8.0 (2504)	8.1
AVC Visibility	Yes	Yes(2504 only)
mDNS Snooping	Yes	Yes
New MDNS Profile for printer, http	Yes	Yes
Local Profiling	Yes	Yes
Band Select	Yes	Yes
DHCP Proxy	Yes	Yes
Secure Web access	Yes	Yes
Virtual IP 192.0.2.1	Yes	Yes (configurable)
RRM-DCA Auto	Yes	Yes
RRM-TPC Auto	Yes	Yes
CleanAir Enabled	Yes	Yes
EDRRM Enabled	Yes	Yes
Channel Width 40 MHz	Yes	Yes
Aironet IE Disabled	Yes	Yes
Management over Wireless	Yes	No



Day0/Day1 Setup Best Practices

New Default Best Practices



Feature	7.6 MR2, 8.0 (2504)	8.1
2.4 Low Data Rates Disabled	No	Yes (High, typical Density)
Load Balancing	No	Yes (High Density)
Rogue Threshold Enabled	No	Yes
Client Exclusion Enabled	No	Yes
FastSSID Enabled	No	Yes
Infra MFP	No	Yes
Multicast Forwarding Mode	No	Yes
SNMPv3 (delete default)	No	Yes
Mobility Name	No	Yes (configurable)
RF Group same as Mobility Name	No	Yes
DHCP Required on Guest WLAN	No	Yes
5 GHz Channel Bonding	No	Yes

WLAN Express Setup

Cisco 2500 Series Wireless Controller

7.6 MR2, 8.0

1 Set Up Your Controller

System Name: APSOC
Country: India (IN)
Date & Time: 09/05/2015
Timezone: Colombo
NTP Server: 0.0.0.0
Management IP Address: 10.10.10.1
Subnet Mask: 255.255.255.0
Default Gateway: 10.10.10.1
Management VLAN ID: 10

7.6 MR2, 8.0

2 Create Your Wireless Networks

☒ Employee Network

Network Name: enjoy
Security: WPA2 Personal
Pass Phrase:
Confirm Pass Phrase:
VLAN: Management VLAN
DHCP Server Address: 10.10.10.1

☒ Guest Network

Back Next

8.1

3 Advanced Setting

☒ RF Parameter Optimization

Deployment Type: Low Density Typical High Density
Traffic Type: Data

Virtual IP Address: 192.0.2.1
Local Mobility Group: Default
Service Port Interface: Manually
Service Port IP Address: 0.0.0.0
Service Port Netmask: 0.0.0.0

Back Next

New in 8.1

Network Profiles GUI

Sets pre-defined RF parameters depending on “Client” Density and Traffic Type

The screenshot displays the 'Network Profile' configuration page in the Cisco Wireless GUI. On the left, a sidebar menu under 'Wireless' includes 'Access Points', 'Radios', and 'Advanced'. The 'Network Profile' option is highlighted with a red box. The main content area, titled 'Network Profile', contains three settings: 'RF Parameter Optimization' (checked), 'Client Density' (set to 'Typical'), and 'Traffic Type' (set to 'Data'). Two callout boxes provide additional context: one for 'Client Density' listing 'High', 'Typical', and 'Low' options, and another for 'Traffic Type' listing 'Data', 'Data and Voice', and 'Voice' options.

Wireless

- Access Points
 - All APs
- 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
 - Optimized Roaming
 - Network Profile**

Network Profile

- RF Parameter Optimization ☒
- Client Density **Typical**
- Traffic Type **Data**

Client Density : High, Typical, Low

Traffic Type : Data, Data and Voice



Pre-built RF Profiles

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

Wireless

▼ Access Points

All APs

▼ 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

Optimized Roaming

Network Profile

Mesh

RF Profiles

RF Profile

Enable Out Of Box☐

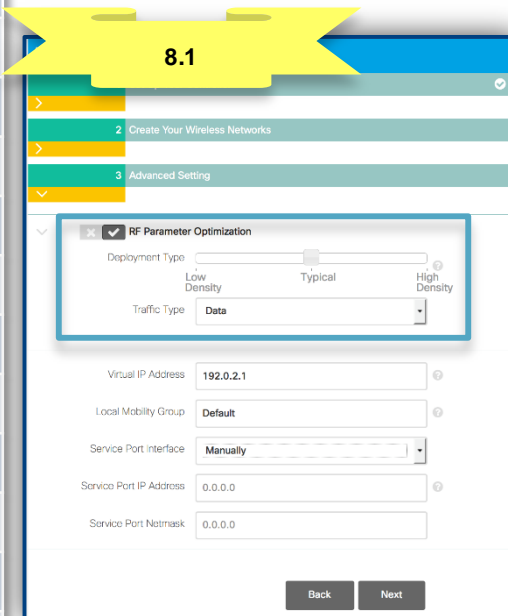

Enable Persistence☐

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"/>
Low-Client-Density-(802.11bg)	802.11b/g	No <input checked="" type="checkbox"/>
Typical-Client-Density(802.11bg)	802.11b/g	No <input checked="" type="checkbox"/>
Typical-Client-Density-(802.11a)	802.11a	No <input checked="" type="checkbox"/>

Pre-built RF profiles for use with AP Groups

WLAN Express Setup Best Practices

Best Practice Knobs	Best Practice Knobs
AVC Visibility	2.4 Low Data Rates Disabled
mDNS Snooping	Load Balancing
New MDNS Profile for printer, http	Rogue Threshold Enabled
Local Profiling	Client Exclusion Enabled
Band Select	FastSSID Enabled
DHCP Proxy	Infra MFP
Secure Web access	Multicast Forwarding Mode
Virtual IP 192.0.2.1	SNMPv3 (delete default)
RRM-DCA Auto	Mobility Name
RRM-TPC Auto	RF Group same as Mobility Name
CleanAir Enabled	DHCP Required on Guest WLAN
EDRRM Enabled	5 GHz Channel Bonding
Channel Width 40 MHz	
Aironet IE Disabled	
Management over Wireless	

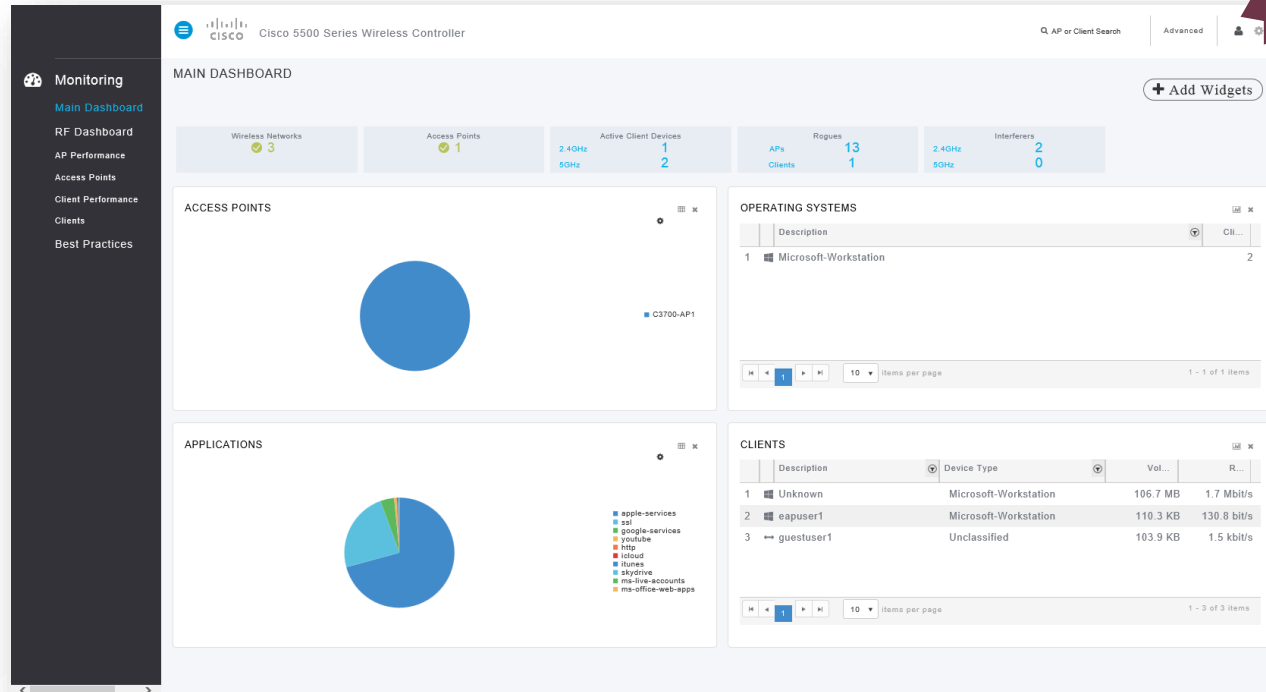
Save Time & Money

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

A long-exposure photograph of a city street at night. The foreground is filled with vibrant, multi-colored light trails from moving vehicles, creating a sense of motion. In the background, a pedestrian bridge spans the street, and modern buildings with lit windows and signage line the street. The overall scene is a dynamic urban environment.

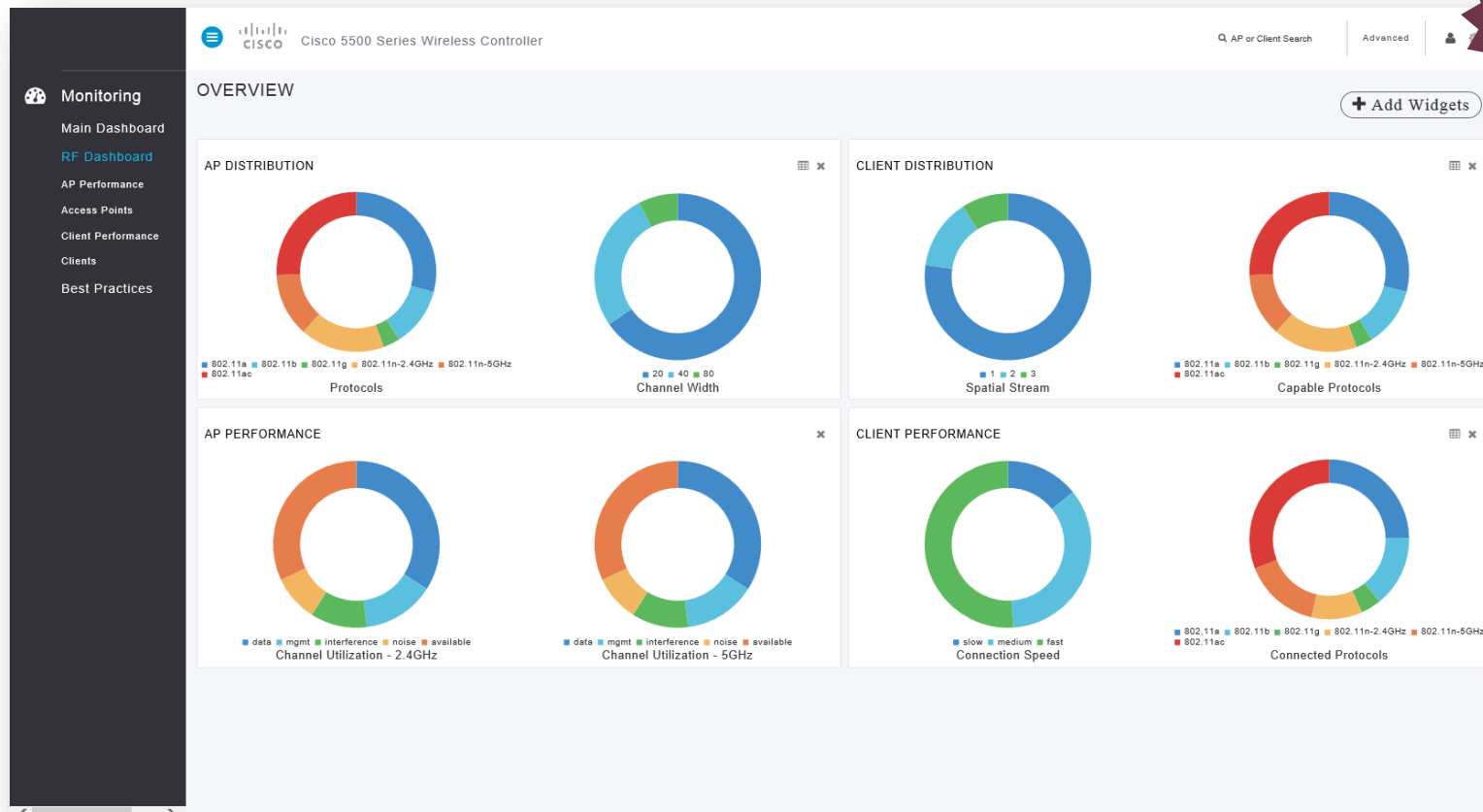
User-First Dashboard View

Monitoring Dashboard

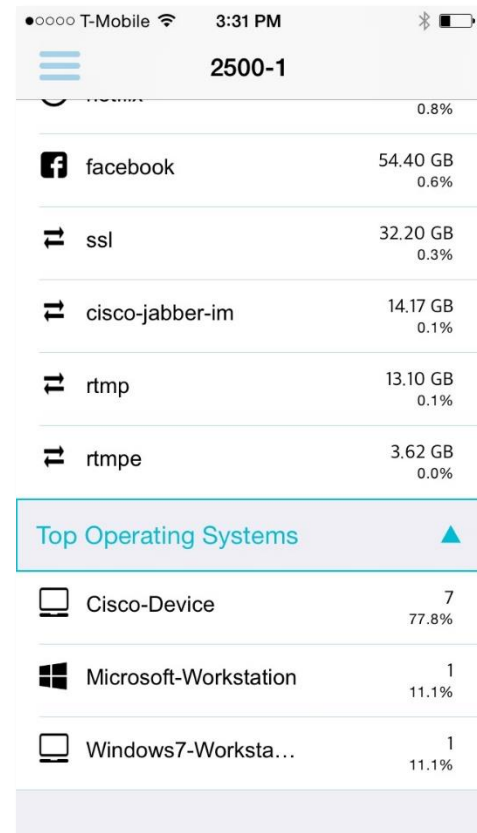
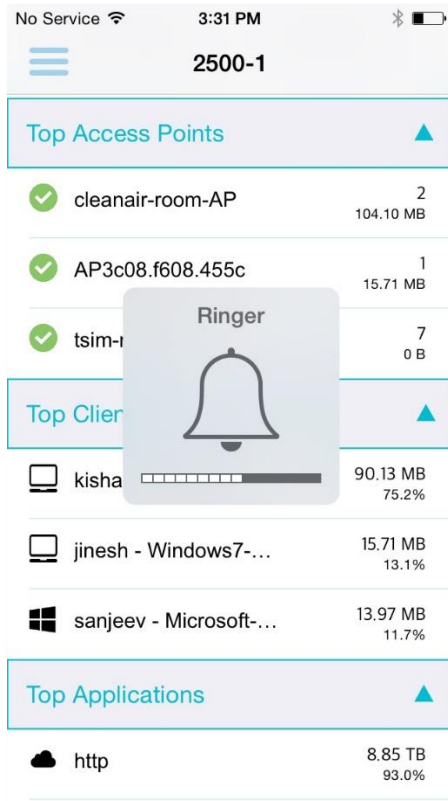
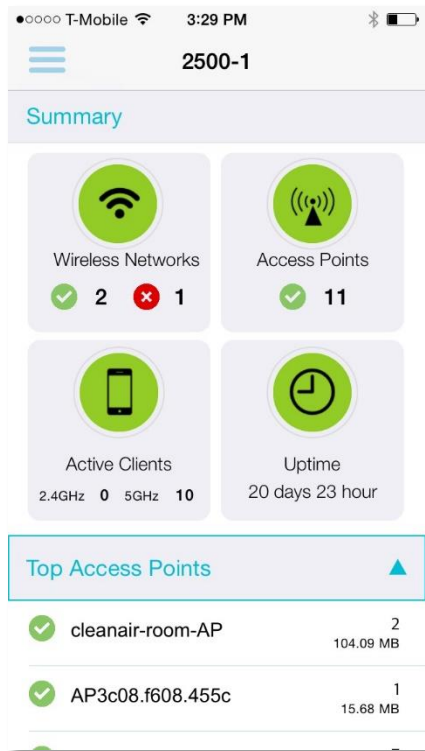


- Wireless Networks
- Access Points
- Active Clients
- Routers
- Interferers
- Top Access Points
- Top Applications
- Top Operating Systems
- Top Client Devices

RF Dashboard



Monitoring Dashboard App



A long-exposure photograph of a city street at night. The foreground is filled with vibrant, multi-colored light trails from moving vehicles, creating a sense of motion. In the background, a modern pedestrian bridge with blue lighting spans the street. Tall buildings with illuminated windows and storefronts line the street, and several flags are visible on the left side.

Upgrade Audit Work Flow

WLC Upgrade Audit Workflow

Best Practices Level of Compliance 12/29

Infrastructure

- AVC Visibility ☑
Application Visibility is enabled on all WLANs.
Benefits: Classification of applications, real time analysis of user data.
[Learn More...](#) Fix it Now Restore Default
- + Load Balancing ☑
- Local Profiling ○
Local Profiling or Radius Profiling is not enabled on WLANs.
Benefits: Local Profiling provides better visibility in the network, allowing controller to display statistics that are based on per-user or per-device end points.
[Learn More...](#) Fix it Now Restore Default

[+ More Optimizations...](#)

Security

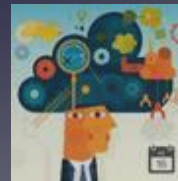
- + WLAN with 802.1X ○
- + Rogue Policies ○
- + Min Rogue RSSI Threshold ○

[+ More Optimizations...](#)

RF Management

- + High SSID Counts ☑
- + Client Bandselect ○
- + 40MHz Channel Width ○

[+ More Optimizations...](#)



Audit Upgrades

- Compliance metric and reporting natively on WLC
- 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

A long-exposure photograph of a city street at night. The foreground is filled with vibrant, multi-colored light trails from moving vehicles, creating a sense of motion. In the background, a pedestrian bridge spans the street, and tall buildings with lit windows and signage line the street. The overall scene is a dynamic urban environment.

WLC Config Analyser

WLC Config Analyser – Incorporating Best Practices

- Simplify operational use to quickly target and mitigate problem areas.
- Drive adoption of best practices and feature implementation.
- Strengthen customers security, network health and configuration robustness.
- Effectively, show customer trend, with measurable improvement of metrics over time.



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

<https://supportforums.cisco.com/document/7711/wlc-config-analyzer>

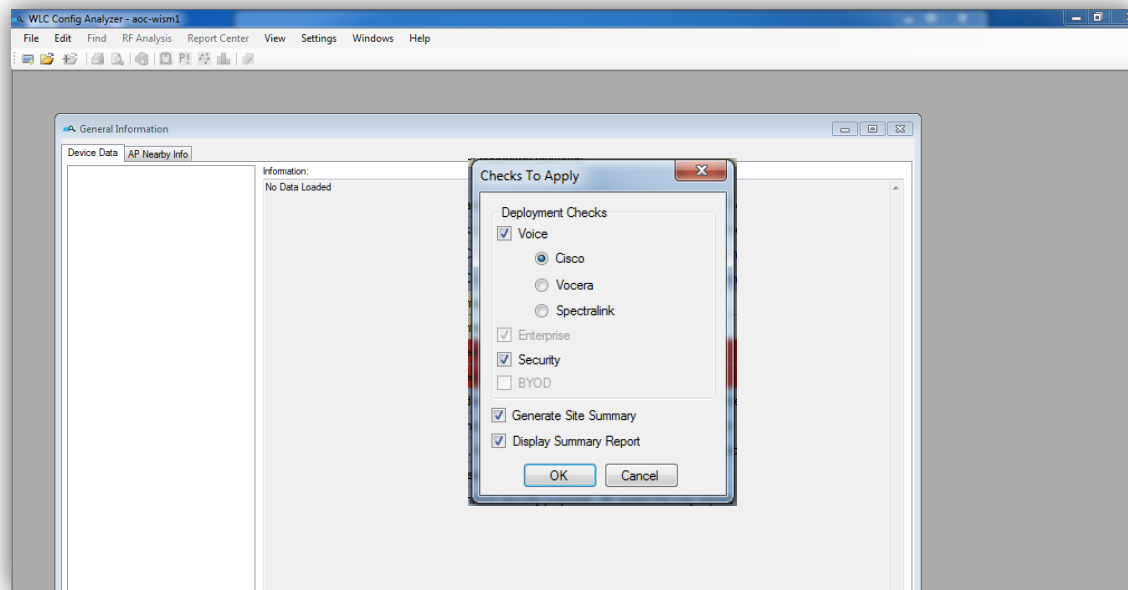
WLC Config Analyser – Deployment types



Addressing BP and features based on deployment

- Voice
- Security
- Flex
- Mesh
- Enterprise*
- BYOD*

*Coming Soon !



WLC Config Analyser – Per Controller Compliance

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

Device Data | AP Nearby Info | Voice Messages | Global Messages | AP Messages

Information:

Controller: aoc-103-wlc1

Category	Compliance Level	Total Checks	Passed Checks	Failed Checks
AP	100%	2	2	0
General	84%	44	37	7
Mobility	100%	1	1	0
RF	100%	2	2	0
Voice - Cisco	68%	9	13	6
Security	29%	14	4	10

Left Pane Tree:

- Controllers
 - wlc-spartan
 - aoc-103-wlc1
 - Interfaces
 - Ports
 - AP Groups - WLANs
 - AP Groups - APs
 - WLANs
 - RF Profiles
 - Mobility Peers
 - Radius Servers
 - Redundancy
 - RF Policies
 - Best Practices
 - AP
 - General
 - Mobility
 - RF
 - Voice - Cisco
 - Security
 - RF Summary
 - Best Practices - All controllers
 - RF Summary - All controllers
 - Site Summary
 - Access Points

0-40%	Red
41-80%	Yellow
81-100%	Green

WLC Config Analyser – Best Practices Detail

- Individual Best Practice knob compliance (Yes/ No)

Compliant	ID	Description
Yes	40001	Voice: 802.11a network has AutoRF in automatic for Power Assignment, not recommended un
Yes	40002	Voice: 802.11b network has AutoRF in automatic for Power Assignment, not recommended un
Yes	40003	Voice: 802.11a network has AutoRF in automatic for Channel Assignment, not recommended,
Yes	40004	Voice: 802.11b network has AutoRF in automatic for Channel Assignment, not recommended,
Yes	40005	Voice: 802.11a Coverage Threshold
Yes	40006	Voice: 802.11b Coverage Threshold
Yes	40012	Voice: Low data rates (1 and 2 mbps) must be disabled for voice, check in 802.11b Network C
No	40024	Voice: 802.11a Coverage Min Clients
No	40025	Voice: 802.11b Coverage Min Clients
Yes	40026	Voice: 802.11a TX Power Threshold
Yes	40027	Voice: 802.11b TX Power Threshold
No	40028	Voice: Low data rates (6 and 9 mbps) should be disabled for voice, check in 802.11a Network
Yes	40029	Voice: Session timeout should be either disabled (zero) or high, to avoid voice disruptions durin
Yes	40035	Voice: AP does not have antenna diversity enabled. It is recommended to use diversity in all v
No	40038	Voice: Traffic Stream Metrics collection is disabled. It is recommended, although not mandatory
No	40043	Voice: DCA interval is recommended to be high, to prevent channel changes during working h
No	40048	Voice: Percentage of clients with low SNR detected, it may be indication of poor RF coverage
Yes	40049	Voice: If your RF coverage is adequate, it is advisable to use 11a band for voice deployments
Yes	40050	Voice: DTPC should be enabled to help adjust TX power in client to match AP and prevent ha

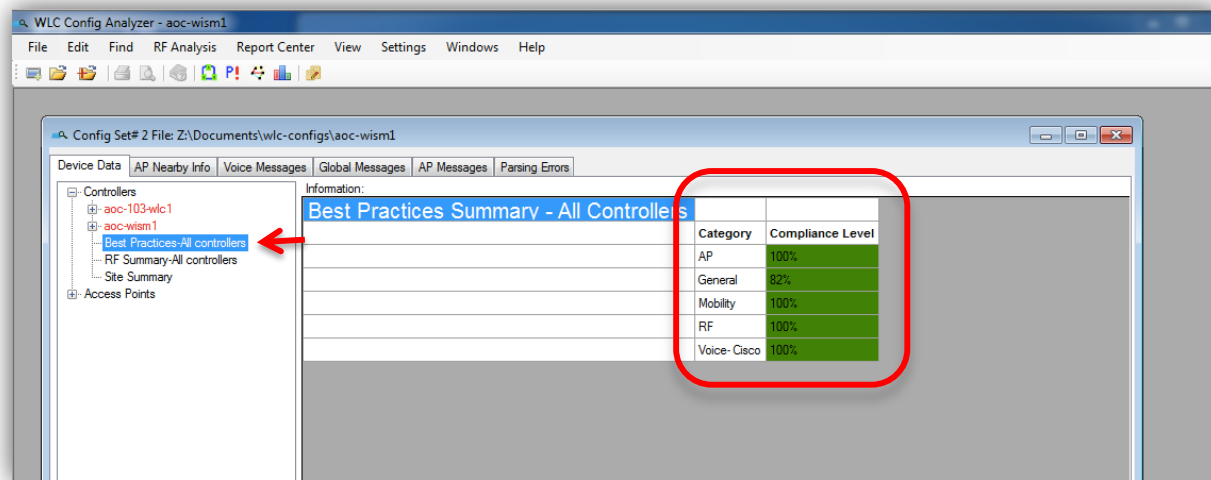
Compliance Level: 68%

Overall Compliance per category

0-40%	Red
41-80%	Yellow
81-100%	Green

WLC Config Analyser – All Controllers

- Best Practices Compliance across controllers in the same Config Set #
- Average across controllers for each category



WLC Config Analyser – Site Summary Messages

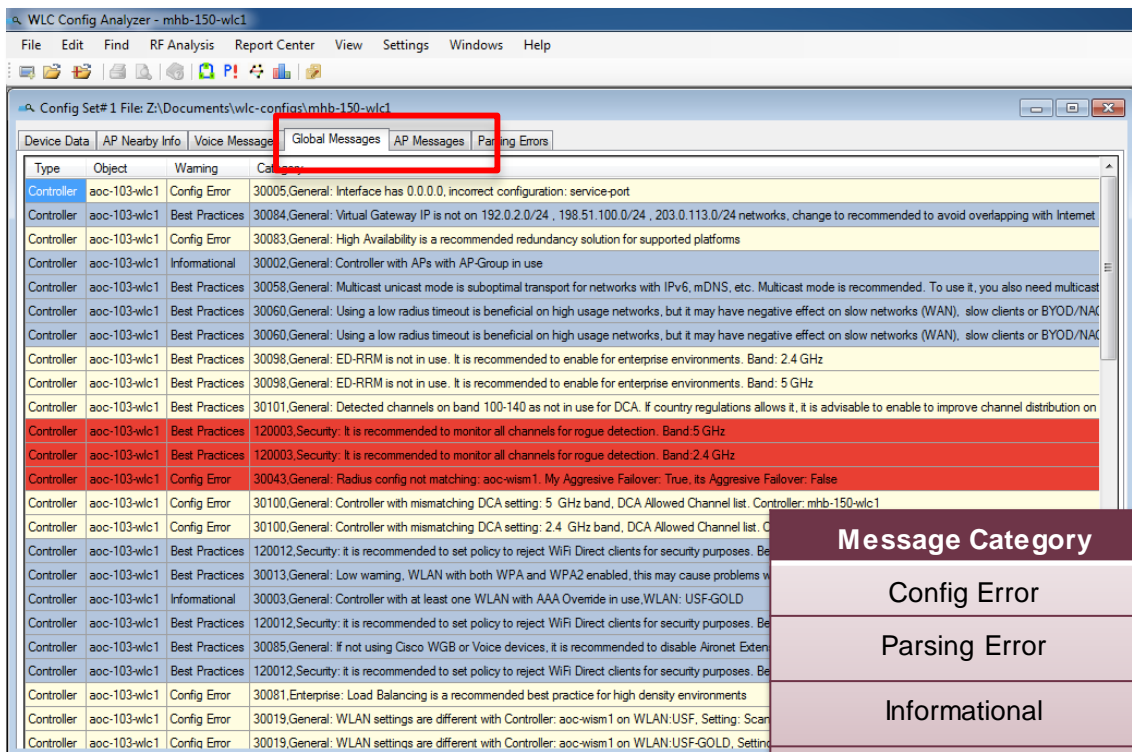
- Best Practices is NOT Config Errors or Design decisions
- It is - “Works without but works much better with”
- Verbose BP messages under Global Messages and AP Messages

The screenshot shows the WLC Config Analyzer - aoc-wism1 application. The left pane displays a tree view of configuration elements, with 'Site Summary' selected under 'Access Points'. The right pane shows the 'Site Summary' information, including a table of message counts and a list of devices.

Site Summary	
Total Messages	
Best Practices:	79
Informational:	294
Config Errors:	30
Parsing Errors:	4
Devices:	
Parsed Controllers:	2
Total APs:	623

A dashed box highlights the 'Best Practices' row in the table, with a callout box pointing to it that says 'Best practice messages'.

WLC Config Analyser – Global Messages & AP Messages



Message Severity	Color Coding
Error (Critical)	Red
Warning (Highly Recommended)	Light Yellow
Informational (Good to Have)	Light Blue

Message Category	Meaning
Config Error	Bad Configuration
Parsing Error	Error on File Processing
Informational	Informational messages
Best Practices	Compliance Checks

Config Analyser Best Practice Compliance with 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

A long-exposure photograph of a city street at night. The background shows a multi-lane road with a pedestrian bridge and modern buildings with lit windows. The foreground is dominated by vibrant, curved light trails from car headlights and taillights in shades of yellow, orange, and red. A semi-transparent dark banner is overlaid across the middle of the image, containing the text.

Cisco Active Advisor

Improve User Experience Through Automatic Discovery of Cisco Wireless Products and Health Score Calculation

Why use Cisco Active Advisor?

Dimension Data Network Barometer Report, June 2014*

51% Of All Network Devices are
Now Aging or Obsolete

Most Networks are **NOT** Ready for
Enterprise Mobility Trends

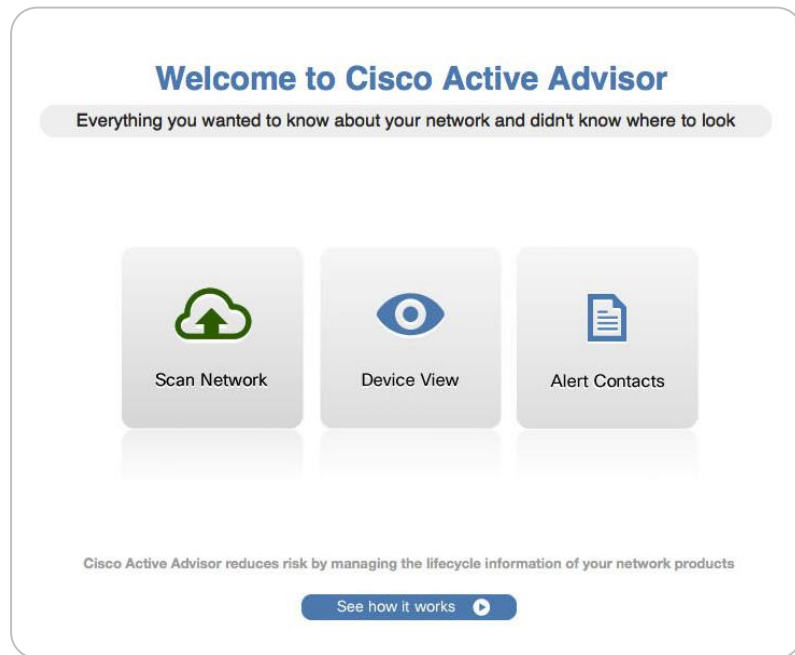
#1 Recommendation from the report:
**Have an accurate
inventory of your network**

**Plan the steps from your
'as-is' state to your 'to-be'
state**


*<http://www.dimensiondata.com/Global/Global-Microsites/NetworkBarometer/Pages/Home.aspx> (Requires Registration)


Introducing Cisco Active Advisor

- Free, cloud based service
- Agentless – nothing to download
- It provides customers:
 - Security Advisories (PSIRTs)
 - End-of-life & End-of-support dates
 - Warranty & service contract status
 - **Personalised device health score**
- Accessible at:
www.CiscoActiveAdvisor.com




CAA Device Scanner

 Cisco Active Advisor


 / Scan Network


Device Credentials

IP Address Range to Explore

172.20.224.154 


 to


172.20.224.156 




[Add More](#)

Device Login Credentials

admin 

..... 



[Add More](#)

Provide Cisco Active Advisor with the Login/Password credentials for network devices to retrieve more detailed device information.

Scan My Network

Enable CDP Discovery 

CDP Discovery Level

3  

Connection Timeout

20  

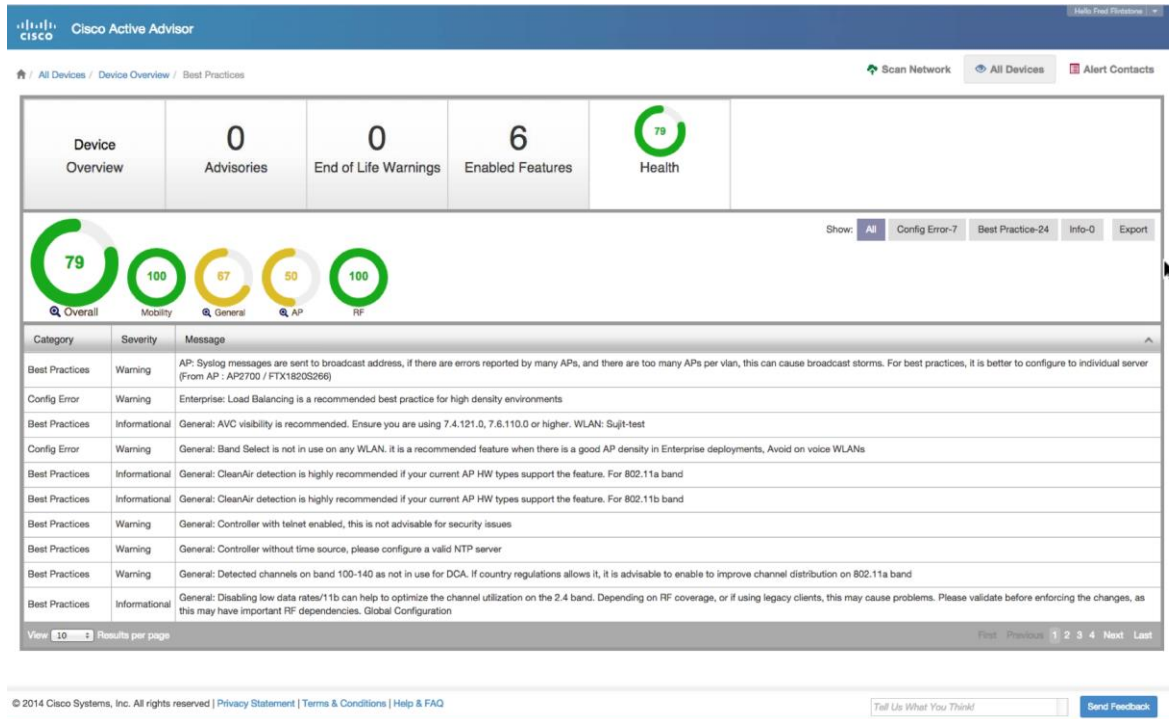
Connection Retry

0  

Enable Debug 

Upload Immediately After Scan 

CAA Device Health Score



Improve

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

A long-exposure photograph of a city street at night. The foreground is filled with vibrant, multi-colored light trails from moving vehicles, creating a sense of motion. In the background, a modern pedestrian bridge with blue lighting spans the street. Tall buildings with illuminated windows and storefronts line the street, and several flags are visible on the left side.

Best Practices Recommendations

Best Practices Recommendations



For Your
Reference

BEST PRACTICES (Airos)

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

A long-exposure photograph of a city street at night. The foreground is filled with vibrant, multi-colored light trails from moving vehicles, creating a sense of motion. In the background, a modern pedestrian bridge with blue lighting spans the street. Tall buildings with illuminated windows and storefronts line the street, and several flags are visible on poles to the left.

Infrastructure Best Practices

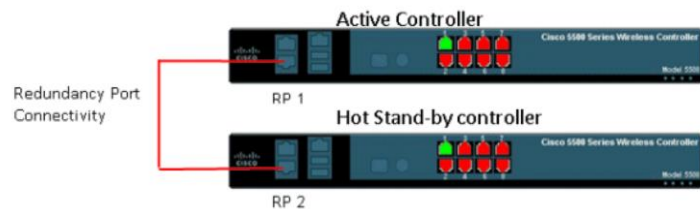
Infrastructure Best Practices

INFRASTRUCTURE

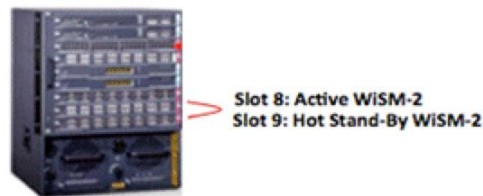
- Enable High Availability (AP and Client SSO)
- Enable AP Failover Priority
- Enable AP Multicast Mode
- Enable Multicast VLAN
- Enable Pre-image download
- Enable AVC
- Enable NetFlow
- Enable Local Profiling (DHCP and HTTP)
- Enable NTP
- Modify the AP Re-transmit Parameters
- Enable FastSSID change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

Infrastructure: Enable High Availability (AP & Client SSO)

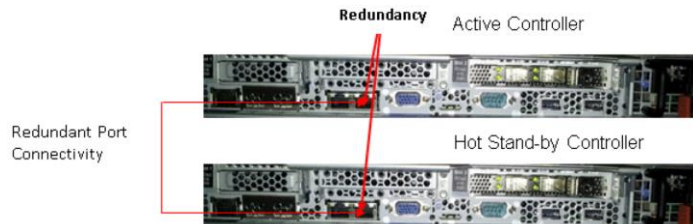
A direct physical connection between Active and Standby Redundant Ports or Layer 2 connectivity is required to provide stateful redundancy within or across data centres



Single Chassis HA Setup



Multi Chassis VSS Setup



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

AP Failover Priority

Global AP Failover Priority

Enable

All APs > Details for AP3600-WSSI_1

General

Credentials

Interfaces

High Availability

Inventory

Advanced

Name

Management IP Address

Primary Controller

WLC1

172.20.227.100

Secondary Controller

Tertiary Controller

AP Failover Priority

Low

Low

Medium

High

Critical

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

Infrastructure: Enable AP Multicast Mode

Controller → General → AP Multicast Mode

The screenshot shows the Cisco Controller configuration interface. The 'General' tab is selected, and the 'AP Multicast Mode' is configured. The 'AP Multicast Mode' is set to 'Multicast' with a group address of '239.28.28.77'. A red box highlights this row, and a dashed line points to a callout box.

Configuration Item	Value
Name	Cisco Controller
802.3x Flow Control Mode	Disabled
LAG Mode on next reboot	Disabled
Broadcast Forwarding	Disabled
AP Multicast Mode	Multicast
Multicast Group Address	239.28.28.77
AP IPv6 Multicast Mode	Unicast
AP Failback	Enabled
AP Preferred Mode	Not-Configured
Fast SSID change	Disabled
Link Local Bridging	Disabled
Default Mobility Domain Name	MyGroup

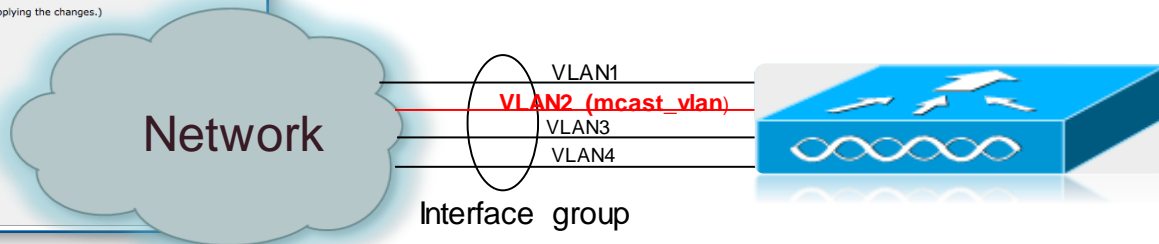
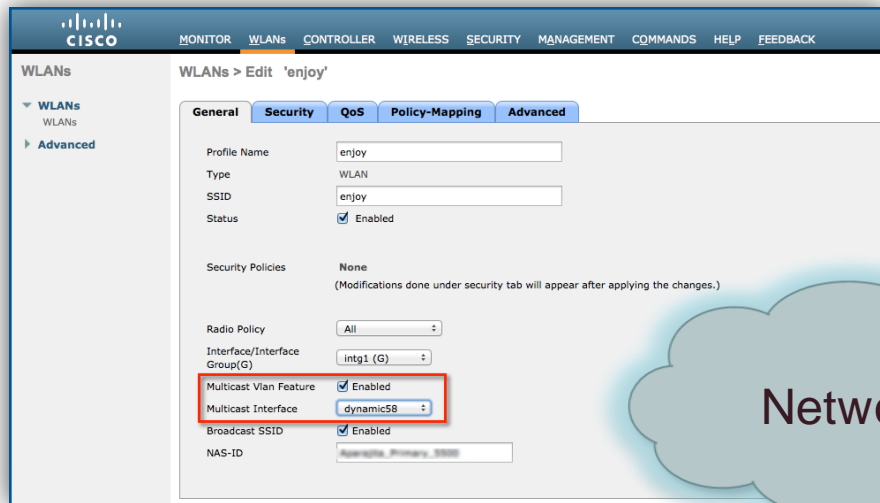
Unique across WLCs and not clashing with other protocols

Network infrastructure must provide multicast routing between the management interface subnet and the AP sub-network.

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

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

Infrastructure: Enable Pre-image Download

Wireless → Global Configurations → AP Image Pre-download

The screenshot displays the Cisco Wireless configuration page. On the left is a navigation tree with categories like Access Points, Radios, Advanced, Mesh, RF Profiles, FlexConnect Groups, and various protocols. The main content area is titled 'Wireless' and contains several sections: 'CDP State' with tables for Ethernet interfaces and radio slots, 'Login Credentials' with input fields for username, password, and enable password, '802.1x Supplicant Credentials' with an authentication checkbox, 'AP Failover Priority' with a dropdown menu, and 'AP Image Pre-download' which is highlighted with a blue box. This highlighted section contains four buttons: 'Download Primary', 'Download Backup', 'Interchange Image', and 'Abort Predownload'.

Ethernet Interface#	CDP State
0	<input checked="" type="checkbox"/>
1	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>
3	<input checked="" type="checkbox"/>

Radio Slot#	CDP State
0	<input checked="" type="checkbox"/>
1	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>

AP Image Pre-download

Allows for less network downtime during software updates

Infrastructure: Enable AVC

Wireless → Application Visibility and Control → AVC Profiles

WLANS > Edit 'Contractor'

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

Quality of Service (QoS) Silver (best effort) ▾

Application Visibility ☒ Enabled

AVC Profile block_facebook ▾

Netflow Monitor none ▾

WMM

WMM Policy Allowed ▾

7920 AP CAC ☐ Enabled

7920 Client CAC ☐ Enabled

Enable Application
Visibility

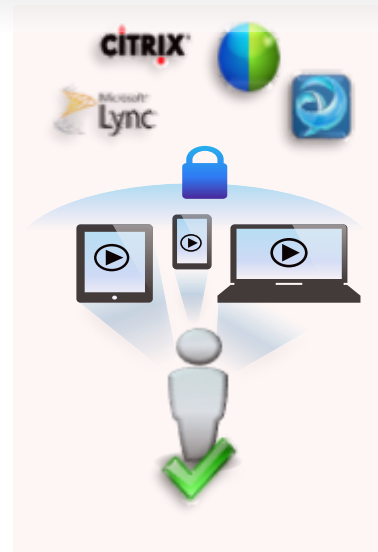
Profile > Rule > 'block_facebook'

Application Group browsing ▾

Application Name facebook ▾

Action Drop ▾

Add per
application rules



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

Infrastructure: Enable NetFlow in your WLC

Wireless → Netflow → Exporter → Create 'New'

Exporter Create

Exporter Name

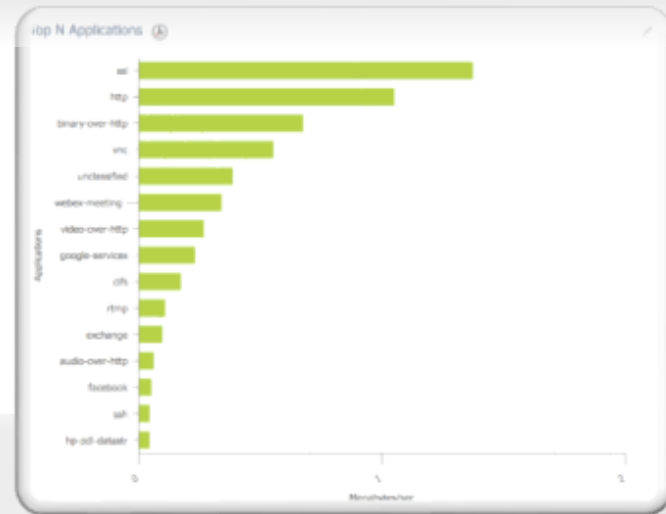
Exporter Ip

Port Number

Wireless → Netflow → Monitor → New

Netflow Monitor > New

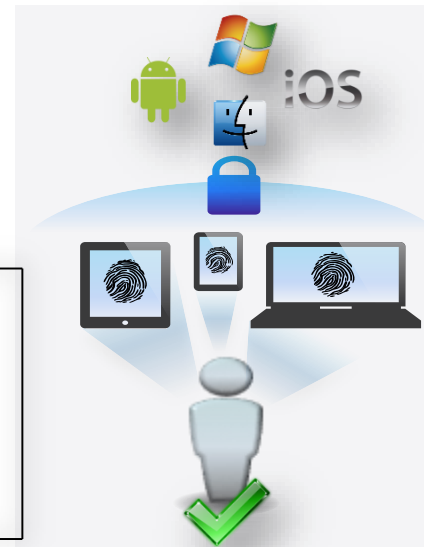
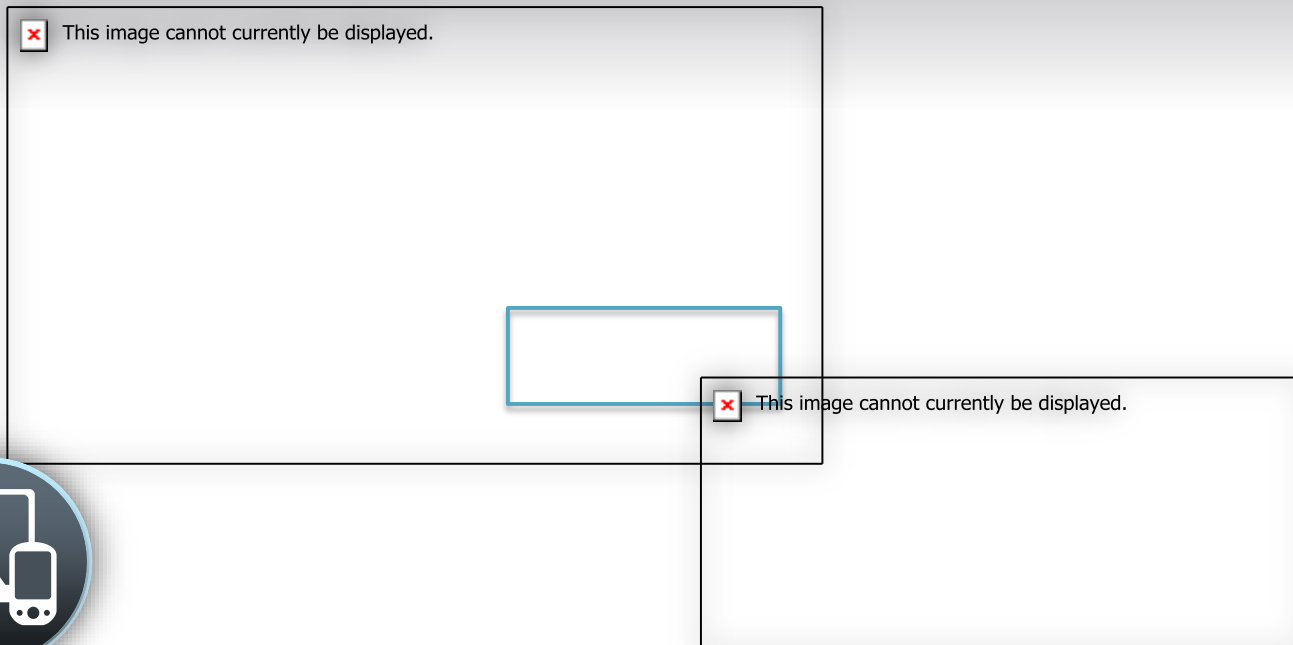
Monitor Name



Netflow export to Cisco Prime or third party network management tool

Infrastructure: Enable Local Profiling

WLANs → Edit → WLAN_NAME → Advanced



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

Infrastructure: Enable NTP

Controller → NTP → Keys

Controller → NTP → Server

NTP Keys > New

Key Index	1
Checksum	md5
Key Format	ASCII ▾
Key

If NTP requires authentication, first add key

NTP Servers > Edit

Server Index	1
Server Address	172.20.227.101
Enable NTP Authentication	<input checked="" type="checkbox"/>
Key Index	1

Synchronises the time among all devices on the network including Access Point and Controller as we have X.509 certificates installed in AP and WLC, Context-aware and location services, MFP, Debugging

Infrastructure: Modify the AP Re-transmit Parameters

Wireless → Access Points → Global Configuration

The screenshot shows the 'Global Configuration' page for an Access Point. The 'General' tab is selected. Under 'CDP', the 'CDP State' is checked. The 'High Availability' section contains various settings for heartbeat and failover. The 'TCP MSS' section is also visible. The 'AP Retransmit Config Parameters' section is highlighted with a red box, showing the 'AP Retransmit Count' set to 5 and the 'AP Retransmit Interval' set to 3 seconds. Two callout boxes provide additional context: one for the 'Number of times the AP will try to join the WLC (3-8)' and another for the 'Number of seconds to wait before rejoining (2-5sec)'.

Ethernet Interface#	CDP State
0	<input checked="" type="checkbox"/>
1	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>
3	<input checked="" type="checkbox"/>

Radio Slot#	CDP State
0	<input checked="" type="checkbox"/>
1	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>

High Availability

AP Heartbeat Timeout(1-30): 30

Local Mode AP Fast Heartbeat Timer State: Disable

FlexConnect Mode AP Fast Heartbeat Timer State: Disable

AP Primary Discovery Timeout(30 to 3600): 120

AP Primed Join Timeout(120 - 43200 seconds): 0

Back-up Primary Controller IP Address(Ipv4/Ipv6):

Back-up Primary Controller name:

Back-up Secondary Controller IP Address(Ipv4/Ipv6):

Back-up Secondary Controller name:

TCP MSS

Global TCP Adjust MSS (IPv4: 536 - 1363, IPv6: 1220 - 1331):

AP Retransmit Config Parameters

AP Retransmit Count	5	<input checked="" type="checkbox"/>
AP Retransmit Interval	3	<input checked="" type="checkbox"/>

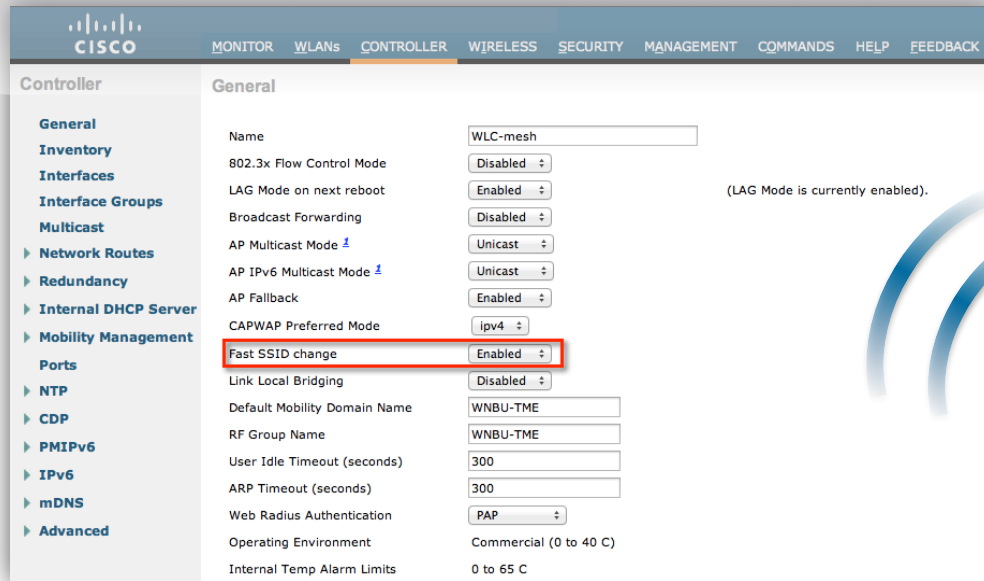
Number of times the AP will try to join the WLC (3-8)

Number of seconds to wait before rejoining (2-5sec)

Allows user to customise the way APs attempt to join a WLC.
Increase count and interval for larger latency links like FlexConnect and satellite links

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

WLANs > Edit 'Guest'

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

Quality of Service (QoS)

Application Visibility ☒ Enabled

AVC Profile

Netflow Monitor

Override Per-User Bandwidth Contracts (kbps) [16](#)

	DownStream	UpStream
Average Data Rate	<input type="text" value="10"/>	<input type="text" value="10"/>
Burst Data Rate	<input type="text" value="10"/>	<input type="text" value="10"/>
Average Real-Time Rate	<input type="text" value="100"/>	<input type="text" value="100"/>
Burst Real-Time Rate	<input type="text" value="1000"/>	<input type="text" value="100"/>

Limit data rates for Guest and Contractor accounts



Enforces limits on non-mission critical clients

Infrastructure: Enable Multicast Mobility for Mobility Domains

Controller → General

Controller → Multicast

The screenshot shows the Cisco Controller configuration interface. The top navigation bar includes links for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar lists various configuration categories under the 'Controller' heading, including General, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Redundancy, Internal DHCP Server, and Mobility Management. The 'Mobility Management' section is expanded, showing sub-items like Mobility Configuration, Mobility Groups, Mobility Anchor Config, and Multicast Messaging. The main content area is titled 'Mobility Multicast Messaging' and contains the following settings:

- Enable Multicast Messaging:** A checkbox that is checked and highlighted with a red rectangle.
- Local Group Multicast IPv4 Address:** A text field containing the value '239.28.28.77'.
- Local Group Multicast IPv6 Address:** An empty text field.
- Mobility Group:** A link to the Mobility Group configuration page.

The screenshot shows the 'Multicast' configuration page. It contains the following settings:

- Enable Global Multicast Mode:** A checkbox that is checked and highlighted with a red rectangle.
- Enable IGMP Snooping:** An unchecked checkbox.
- IGMP Timeout (seconds):** A text field containing the value '60'.
- IGMP Query Interval (seconds):** A text field containing the value '20'.
- Enable MLD Snooping:** An unchecked checkbox.
- MLD Timeout (seconds):** A text field containing the value '60'.
- MLD Query Interval (seconds):** A text field containing the value '20'.

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

Infrastructure: Enable Client Load Balancing

WLANs → Edit “WLAN-NAME” → Advanced

The screenshot shows the 'Advanced' configuration tab for a WLAN. The 'Client Load Balancing' checkbox is checked and highlighted with a red box. A dashed box highlights the 'Client Window Size 1-20' and 'Maximum Denial Count 0-10' settings.

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

Static IP Tunneling ☐ Enabled

Wi-Fi Direct Clients Policy

Maximum Allowed Clients Per AP Radio

Clear HotSpot Configuration ☐ Enabled

Client user idle timeout(15-100000) ☐

Client user idle threshold (0-10000000) Bytes

Radius NAI-Realm ☐

Management Frame Protection (MFP)

MFP Client Protection

DTIM Period (in beacon intervals)

802.11a/n (1 - 255)

802.11b/g/n (1 - 255)

NAC

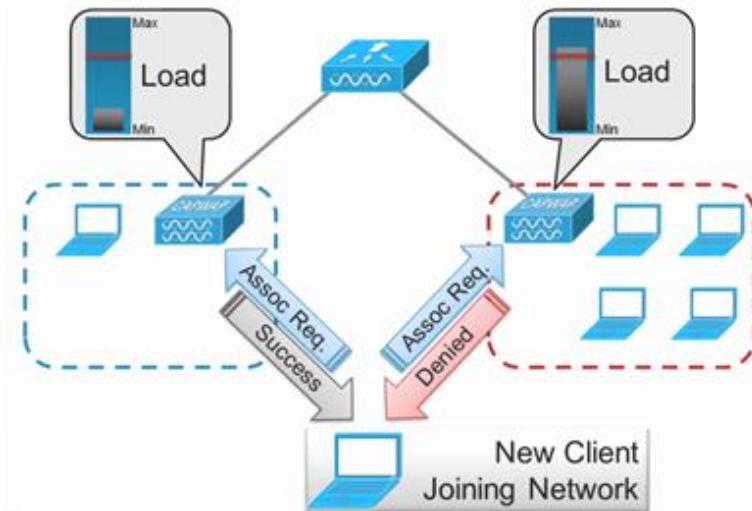
NAC State

Load Balancing and Band Select

Client Load Balancing ☒

Client Band Select ☐

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

WLANs > Edit 'enjoy'

General Security QoS Policy-Mapping **Advanced**

Allow AAA Override ☐ Enabled

Coverage Hole Detection ☒ Enabled

Enable Session Timeout ☐

Aironet IE ☐ Enabled

Diagnostic Channel [18](#) ☐ Enabled

Override Interface ACL IPv4 IPv6

Layer2 Acl

P2P Blocking Action

Client Exclusion [2](#) ☒ Enabled Timeout Value (secs)

Maximum Allowed Clients [3](#)

Static IP Tunneling [11](#) ☐ Enabled

Wi-Fi Direct Clients Policy

Maximum Allowed Clients Per AP Radio

Class of Service

DHCP

DHCP Server ☐ Override

DHCP Addr. Assignment ☐ Required

OEAP

Split Tunnel ☐ Enabled

Management Frame Protection (MFP)

MFP Client Protection [4](#)

DTIM Period (in beacon intervals)

802.11a/n (1 - 255)

802.11b/g/n (1 - 255)

NAC

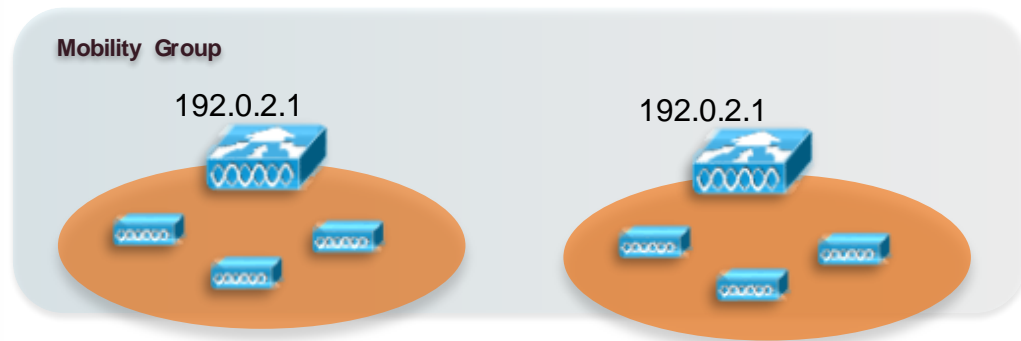
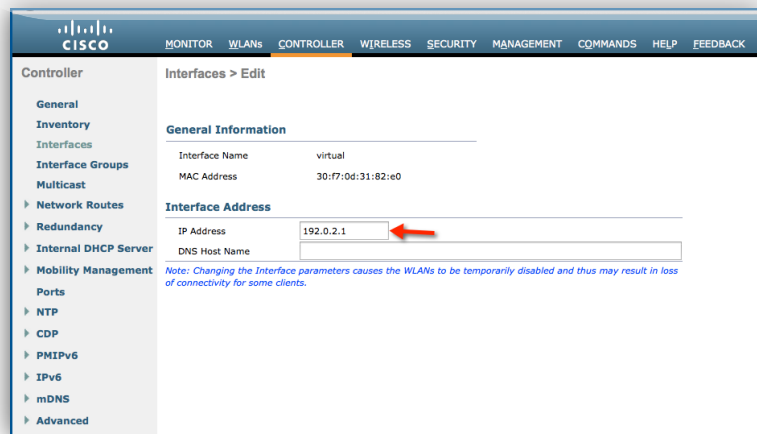
NAC State

- 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

A long-exposure photograph of a city street at night. The foreground is filled with vibrant, multi-colored light trails from moving vehicles, creating a sense of motion. In the background, a modern pedestrian bridge with blue lighting spans the street. Tall buildings with illuminated windows and storefronts line the street, and several flags are visible on the left side.

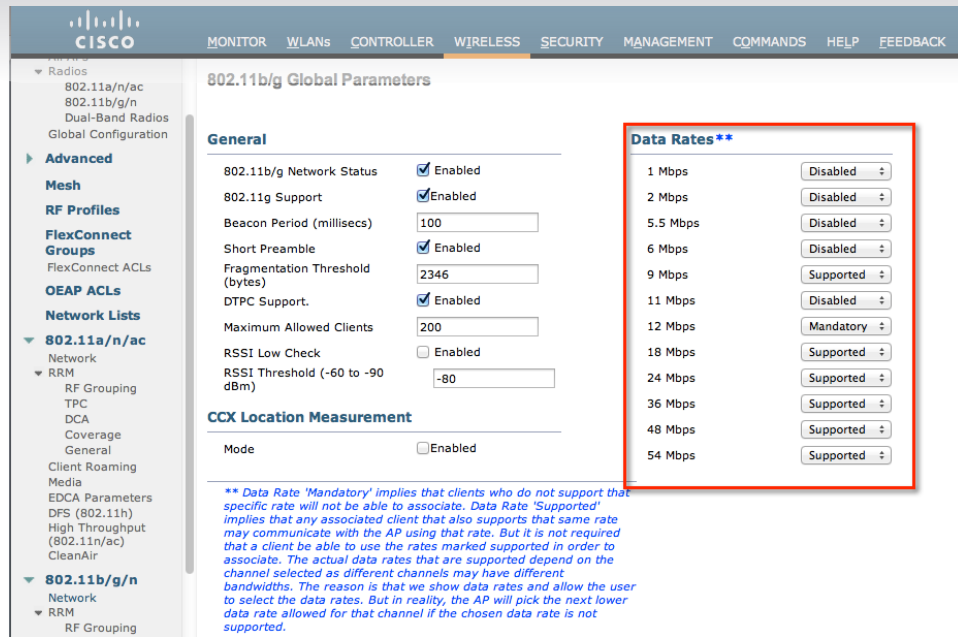
RF and RRM Best Practices

RF and RRM Best Practices

BEST PRACTICES (AiOS)	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	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
	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	WIRELESS / RF	Disable 802.11b data rates Restrict number of WLAN below 3 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

RF and RRM: Disabling .11b Data Rates

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): 100
- Short Preamble: ☒ Enabled
- Fragmentation Threshold (bytes): 2346
- DTPC Support: ☒ Enabled
- Maximum Allowed Clients: 200
- RSSI Low Check: ☐ Enabled
- RSSI Threshold (-60 to -90 dBm): -80

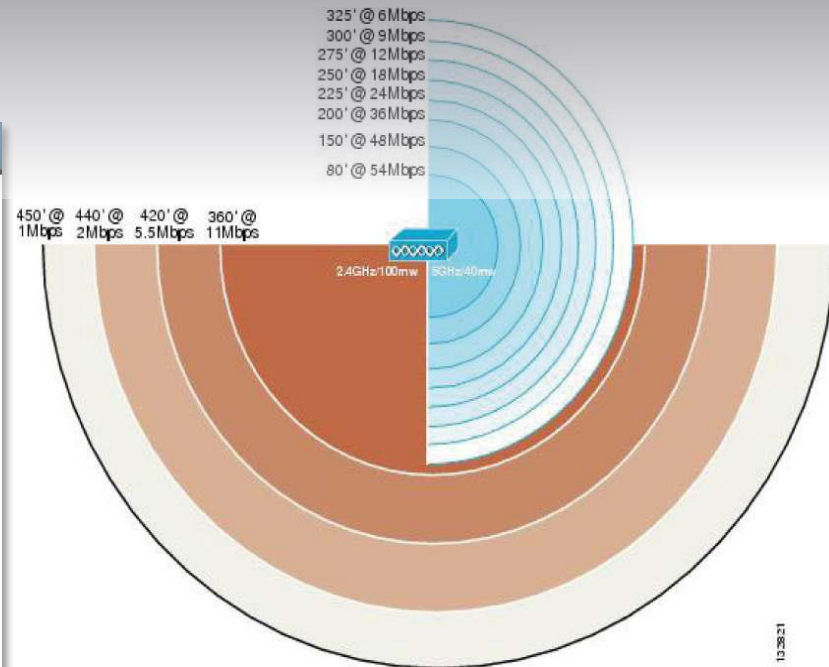
CCX Location Measurement

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.



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

RF and RRM: Disabling .11b Data Rates

Demonstrating the impact of 802.11b data rates on Channel Utilisation



<input type="checkbox"/>	WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies	
<input type="checkbox"/>	1	WLAN	ETAB-PSK	ETAB-PSK	Enabled	[WPA2][Auth(PSK)]	▼
<input type="checkbox"/>	2	WLAN	ETAB-dot1x	ETAB-dot1x	Enabled	[WPA2][Auth(802.1X)]	▼
<input type="checkbox"/>	3	WLAN	ETAB-Lync	ETAB-Lync	Disabled	[WPA2][Auth(PSK)]	▼
<input type="checkbox"/>	4	WLAN	ETAB-FBConnect	ETAB-FBConnect	Enabled	Web-Passthrough	▼
<input type="checkbox"/>	5	WLAN	ETAB-VConnect	ETAB-VConnect	Disabled	Web-Passthrough	▼
<input type="checkbox"/>	6	WLAN	ETAB-LocalPolicy	ETAB-LocalPolicy	Disabled	[WPA2][Auth(PSK)]	▼
<input type="checkbox"/>	7	WLAN	cudemo1	cudemo1	Enabled	[WPA2][Auth(802.1X)]	▼
<input checked="" type="checkbox"/>	8	WLAN	cudemo2	cudemo2	Disabled	[WPA2][Auth(802.1X)]	▼
<input checked="" type="checkbox"/>	9	WLAN	cudemo3	cudemo3	Disabled	[WPA2][Auth(802.1X)]	▼
<input checked="" type="checkbox"/>	10	WLAN	cudemo4	cudemo4	Disabled	[WPA2][Auth(802.1X)]	▼
<input checked="" type="checkbox"/>	11	WLAN	cudemo5	cudemo5	Disabled	[WPA2][Auth(802.1X)]	▼
<input checked="" type="checkbox"/>	12	WLAN	cudemo6	cudemo6	Disabled	[WPA2][Auth(802.1X)]	▼
<input type="checkbox"/>	13	WLAN	cudemo7	cudemo7	Disabled	[WPA2][Auth(802.1X)]	▼

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

<https://cisco.app.box.com/s/rzn20idytdq2zedxigcei>

RF and RRM: Restrict Number of WLANs Below 4

WLANs → WLANs



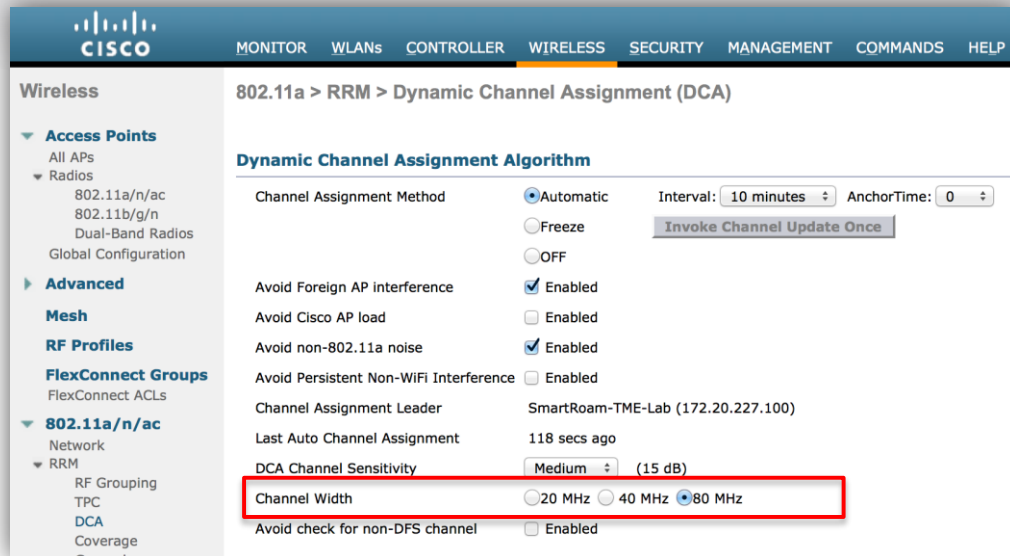
The screenshot shows the Cisco WLAN configuration page. The top navigation bar includes links for MONITOR, WLANs (highlighted), CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar shows a tree view with 'WLANs' expanded. The main content area is titled 'WLANs' and includes a 'Current Filter: None' section with links for '[Change Filter]' and '[Clear Filter]'. There is a 'Create New' button and a 'Go' button. Below this is a table with the following columns: WLAN ID, Type, Profile Name, WLAN SSID, Admin Status, and Security Policies. The table contains three entries:

<input type="checkbox"/>	WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies	
<input type="checkbox"/>	1	WLAN	Employee	Employee	Enabled	[WPA2][Auth(802.1X)]	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2	WLAN	Guest	Guest	Enabled	Web-Auth	<input checked="" type="checkbox"/>
<input type="checkbox"/>	3	WLAN	Contractor	Contractor	Enabled	[WPA2][Auth(PSK)]	<input checked="" type="checkbox"/>

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

RF and RRM: Enable Channel Bonding - 40 or 80 MHz

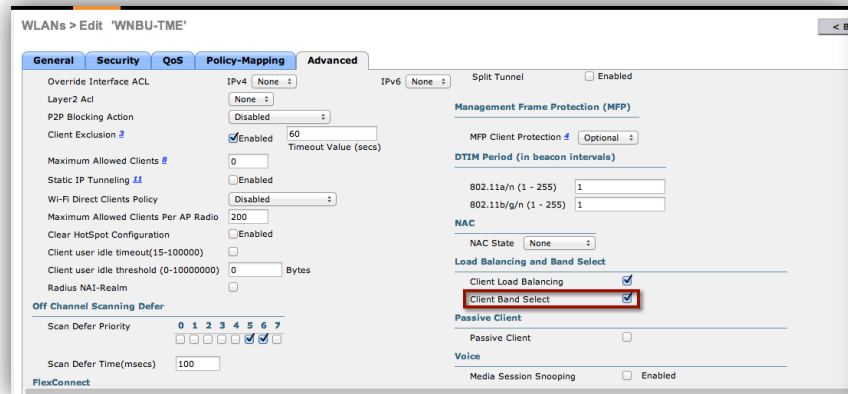
Wireless → 802.11a/n/ac → RRM → DCA



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 and 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 and RRM: RF Profiles

- RF Profiles work in Conjunction with AP Groups (beginning in release 7.2)
 - You can create separate RF profiles for both 2.4 and 5 GHz
 - 1 profile for each band (802.11a/802.11b) can be assigned to an AP group
-
- Today
 - 802.11 data rates
 - TPC Power Threshold and Min max Power settings
 - DCA
 - Coverage hole algorithm settings
 - High Density – HDX configurations RX_SOP, Client Limit, Mcast data rate
 - Client Distribution

More granular control of the RF network

RF Profiles: Granular Control

RF Profile > Edit 'HD_2_4'

General 802.11 RRM High Density Client Distribution

Data Rates¹ MCS

1 Mbps	Disabled	0
2 Mbps	Disabled	1
5.5 Mbps	Disabled	2
6 Mbps	Supported	3
9 Mbps	Mandatory	4
11 Mbps	Disabled	5
12 Mbps	Supported	6
18 Mbps	Supported	7
24 Mbps	Mandatory	8
36 Mbps	Supported	9
48 Mbps	Supported	10
54 Mbps	Supported	11

MCS Settings

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

Data Rates

Load Balancing

RF Profile > Edit 'CiscoLive_Keynote'

General 802.11 RRM High Density Client Distribution

Load Balancing

Window(0 to 20 Clients)

Denial(1 to 10)

RF Profile > Edit 'test_bb'

General 802.11 RRM High Density Client Distribution

Maximum Power Level Assignment (-10 to 30 dBm)

Minimum Power Level Assignment (-10 to 30 dBm)

Power Threshold v1(-80 to -50 dBm)

Power Threshold v2(-80 to -50 dBm)

Data RSSI(-90 to -60 dBm)

Voice RSSI(-90 to -60 dBm)

Coverage Exception(1 to 75 Clients)

Coverage Level(0 to 100 %)

Noise (-127 to 0 dBm)

Utilization (0 to 100 %)

DCA Channel List

DCA Channels

TPC, DCA, Coverage Hole

RF Profile > Edit '802.11a_demo'

General 802.11 RRM High Density Client Distribution

High Density Parameters

Maximum Clients(1 to 200)

Client Trap Threshold⁴

Rx Sop Threshold Parameters

Rx Sop Threshold

Multicast Parameters

Multicast Data Rates²

High Density

RF and RRM: Enable Cisco EDRRM

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

The screenshot shows the configuration page for Radio Resource Management (RRM) in a Cisco wireless controller. On the left is a navigation menu with options: EDCA Parameters, DFS (802.11h), High Throughput (802.11n/ac), CleanAir, 802.11b/g/n, Media Stream, Application Visibility And Control, Country, Timers, Netflow, and QoS. The main content area has a table of channels with checkboxes for 104, 108, 112, 116, 132, and 136. Below this is a section for 'Extended UNII-2 channels' with an 'Enabled' checkbox. The 'Event Driven RRM' section is highlighted with a red box around the 'EDRRM' checkbox, which is checked and labeled 'Enabled'. Below it, the 'Sensitivity Threshold' is set to 'Medium' via a dropdown menu. A dashed line points from the 'Medium' dropdown to a callout box on the right.

<input type="checkbox"/>	104
<input type="checkbox"/>	108
<input type="checkbox"/>	112
<input type="checkbox"/>	116
<input type="checkbox"/>	132
<input type="checkbox"/>	136

Extended UNII-2 channels ☐ Enabled

Event Driven RRM

EDRRM ☒ Enabled

Sensitivity Threshold Medium ▾

Sensitivity threshold recommended to Medium

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

RF and 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

Wireless

802.11a > RRM > Dynamic Channel Assignment (DCA)

Dynamic Channel Assignment Algorithm

Channel Assignment Method: ☒ Automatic ☐ Freeze ☐ OFF

Interval: 10 minutes AnchorTime: 0

Invoke Channel Update Once

Avoid Foreign AP Interference: ☒ Enabled

Avoid Cisco AP load: ☐ Enabled

Avoid non-802.11a noise: ☒ Enabled

Avoid Persistent Non-WiFi Interference: ☐ Enabled

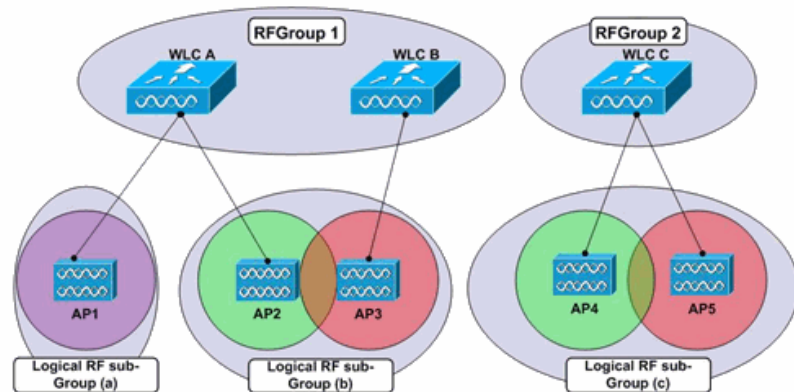
Channel Assignment Leader: SmartRoam-TME-Lab (172.20.227.100)

Last Auto Channel Assignment: 118 secs ago

DCA Channel Sensitivity: Medium (15 dB)

Channel Width: ☐ 20 MHz ☐ 40 MHz ☒ 80 MHz

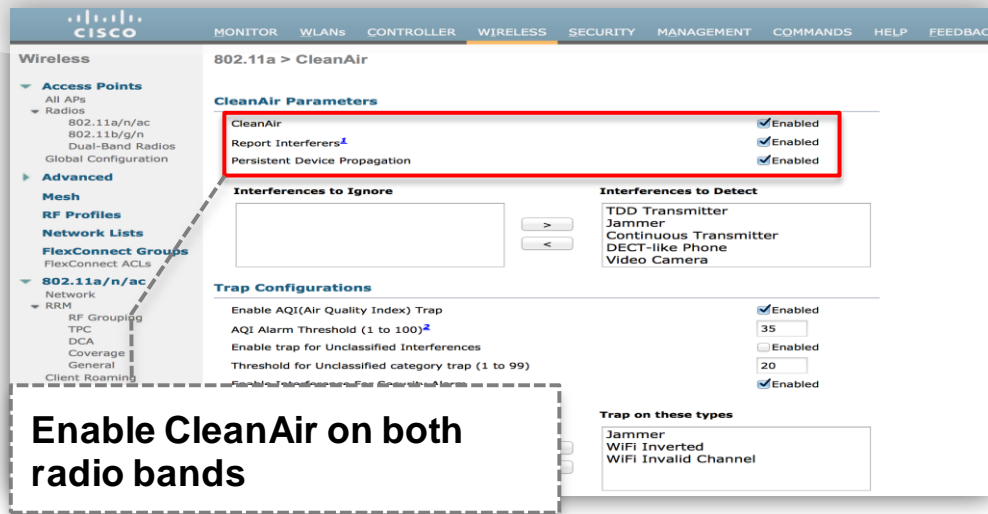
Avoid check for non-DFS channel: ☐ Enabled



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

RF and RRM: Enable Cisco CleanAir

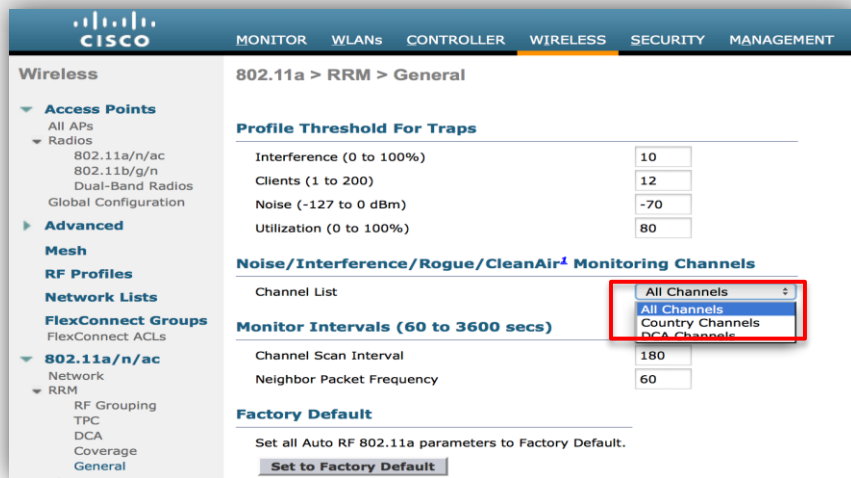
Wireless → 802.11a/n/ac or 802.11b/g/n → CleanAir



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

RF and RRM: Enable Noise and Rogue Monitoring Channels

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



Scan All Channels for security, DCA Channels for performance

RF and RRM : Avoid Cisco AP Load

Wireless → 802.11a/n/ac → RRM → DCA

Wireless → 802.11b/g/n → RRM → DCA

The screenshot shows the Cisco Wireless Configuration Manager (WCM) interface. The left sidebar contains a navigation tree with categories like Access Points, Radios, Advanced, Mesh, RF Profiles, FlexConnect Groups, OEAP ACLs, Network Lists, and 802.11a/n/ac. The main content area is titled '802.11a > RRM > Dynamic Channel Assignment (DCA)'. It features a 'Dynamic Channel Assignment Algorithm' section with various settings. The 'Channel Assignment Method' is set to 'Automatic'. The 'Interval' is '10 minutes' and 'AnchorTime' is '0'. The 'Avoid Cisco AP load' option is checked and highlighted with a red box. Other options like 'Avoid Foreign AP interference', 'Avoid non-802.11a noise', and 'Avoid Persistent Non-WiFi Interference' are also checked. The 'Channel Assignment Leader' is '5760 (9.5.56.22)' and 'Last Auto Channel Assignment' is 'N.A'. The 'DCA Channel Sensitivity' is 'High' and 'Channel Width' is '20 MHz'. The 'Avoid check for non-DFS channel' is checked. Below this is a 'DCA Channel List' table showing a list of channels: 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161.

DCA Channel List	
DCA Channels	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161

To avoid frequent changes in DCA due to varying Load conditions

A long-exposure photograph of a city street at night. The foreground is filled with vibrant, multi-colored light trails from moving vehicles, creating a sense of motion. In the background, a modern pedestrian bridge with blue lighting spans the street. Tall buildings with illuminated windows and storefronts line the street, and several flags are visible on poles to the left.

Security and BYOD Best Practices

Security and BYOD Best Practices

BEST PRACTICES (AiOS)		INFRASTRUCTURE	SECURITY
		<ul style="list-style-type: none">Enable High Availability (AP and Client SSO)Enable AP Failover PriorityEnable AP Multicast ModeEnable Multicast VLANEnable Pre-image downloadEnable AVCEnable NetFlowEnable Local Profiling (DHCP and HTTP)Enable NTPModify the AP Re-transmit ParametersEnable FastSSID changeEnable Per-user BW contractsEnable Multicast MobilityEnable Client Load balancingDisable Aironet IEFlexConnect Groups and Smart AP Upgrade	<ul style="list-style-type: none">Enable 802.1x and WPA/WPA2 on WLANEnable 802.1x authentication for APChange advance EAP timersEnable SSH and disable telnetDisable Management Over WirelessDisable WiFi DirectPeer-to-peer blockingSecure Web Access (HTTPS)Enable User PoliciesEnable Client exclusion policiesEnable rogue policies and Rogue Detection RSSIStrong password PoliciesEnable IDSBYOD Timers
		MESH	WIRELESS / RF
		<ul style="list-style-type: none">Set Bridge Group NameSet Preferred ParentMultiple Root APs in each BGNSet Backhaul rate to "Auto"Set Backhaul Channel Width to 40/80 MHzBackhaul Link SNR > 25 dBmAvoid DFS channels for BackhaulExternal RADIUS server for Mesh MAC AuthenticationEnable IDSEnable EAP Mesh Security Mode	<ul style="list-style-type: none">Disable 802.11b data ratesRestrict number of WLAN below 3Enable channel bonding – 40 or 80 MHzEnable BandSelectUse RF Profiles and AP GroupsEnable RRM (DCA & TPC) to be autoEnable Auto-RF group leader selectionEnable Cisco CleanAir and EDRRMEnable Noise &Rogue Monitoring on all channelsEnable DFS channelsAvoid Cisco AP Load

➤ BYOD Timers

Security : Enable 802.1x Authentications on WLAN

WLANs → Edit 'WLAN_NAME' → Security

WLANs > Edit 'Employee'

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security 6 WPA+WPA2

MAC Filtering 2 ☐

Fast Transition

Fast Transition ☐

Protected Management Frame

PMF Disabled

WPA+WPA2 Parameters

WPA Policy ☐

WPA2 Policy ☒


WPA2 Encryption ☒ AES ☐ TKIP

Authentication Key Management

802.1X ☒ Enable

CCKM ☐ Enable

PSK ☐ Enable



WLANs > Edit 'Employee'

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

	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
Server 1	IP:172.20.227.106, Port:1812	None
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

Provides greater network security on WLAN using 802.1x authentication

Security: Enable 802.1x Authentications for AP

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:

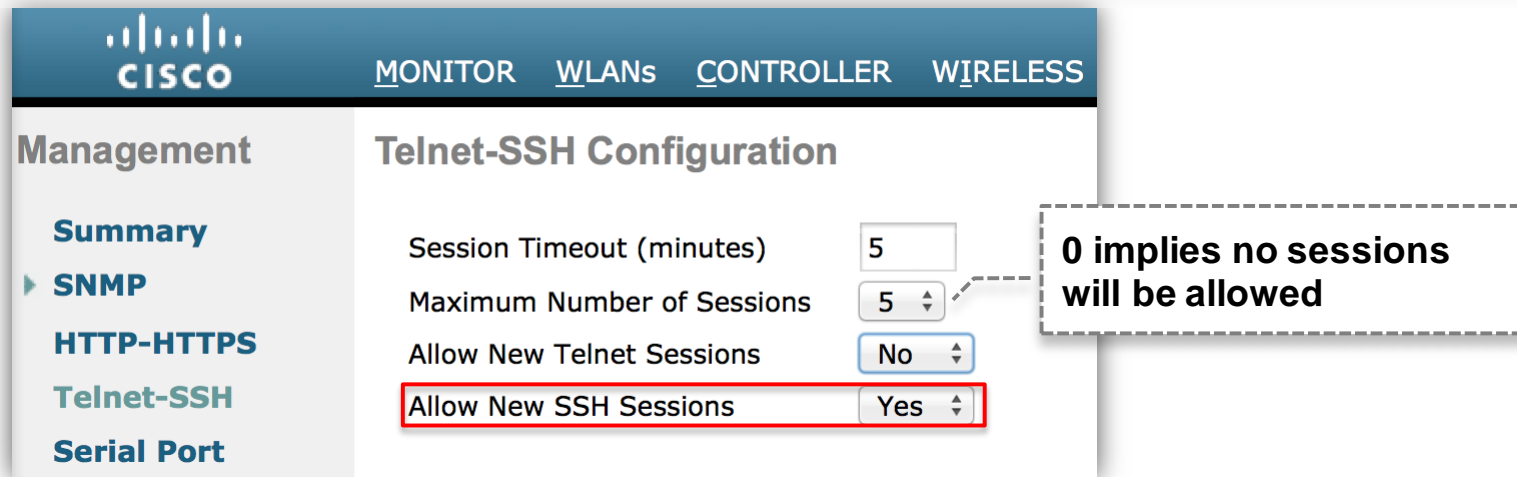
```
Switch# configure terminal
Switch(config)# dot1x system-auth-control
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# radius-server host ip_addr auth-port port acct-port port
key key
Switch(config)# interface fastethernet2/1
Switch(config-if)#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

Provides greater network security by enabling 802.1x on the switch port where AP is connected. Not supported for Mesh deployments

Security: Enable SSH and Disable Telnet

Management → Telnet–SSH

Disable Telnet and enable SSH as the default option



The image shows a screenshot of the Cisco Management Console interface. The top navigation bar includes the Cisco logo and tabs for MONITOR, WLANs, CONTROLLER, and WIRELESS. The left sidebar shows the Management menu with options: Summary, SNMP, HTTP-HTTPS, Telnet-SSH (highlighted), and Serial Port. The main content area is titled 'Telnet-SSH Configuration' and contains the following settings:

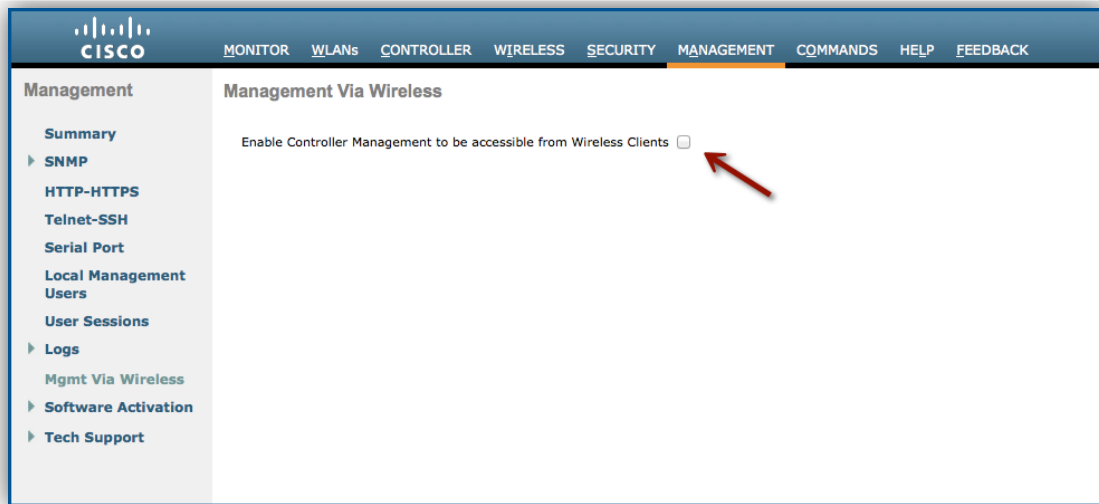
Session Timeout (minutes)	5
Maximum Number of Sessions	5
Allow New Telnet Sessions	No
Allow New SSH Sessions	Yes

A red rectangle highlights the 'Allow New SSH Sessions' setting. A dashed box callout points to the 'Maximum Number of Sessions' field with the text: **0 implies no sessions will be allowed**.

Provides greater security by allowing secure access and denying unencrypted access

Security: Disable Management Over Wireless

Management → Mgmt Via Wireless



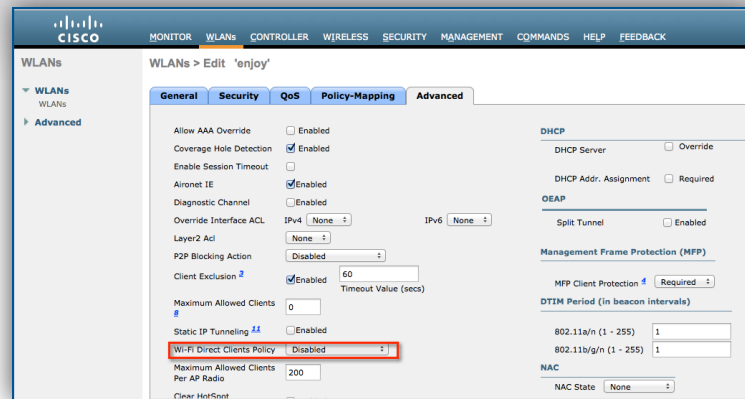
Disallow management of the Controller via Wireless

Security: Disable WiFi Direct

WLANs → WLAN Name → Advanced



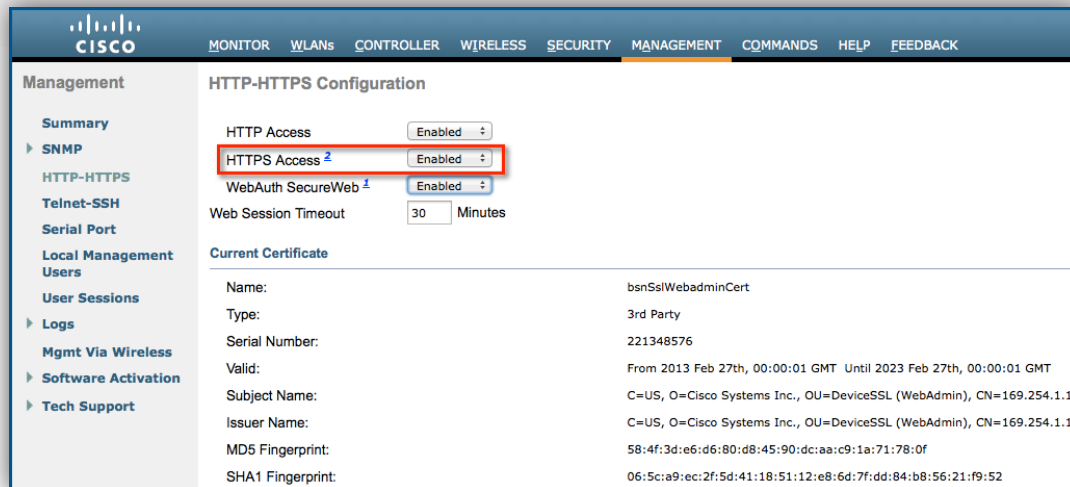
Corporate WLAN



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: Secure Web Access (HTTPS)

Management → HTTP-HTTPS



The screenshot displays the Cisco Management interface with the 'MANAGEMENT' tab selected. The left sidebar shows a navigation menu with 'HTTP-HTTPS' highlighted. The main content area is titled 'HTTP-HTTPS Configuration' and contains the following settings:

- HTTP Access: Enabled
- HTTPS Access: Enabled (highlighted with a red box)
- WebAuth SecureWeb: Enabled
- Web Session Timeout: 30 Minutes

Below the configuration settings is a section for the 'Current Certificate' with the following details:

Current Certificate	
Name:	bsnSslWebadminCert
Type:	3rd Party
Serial Number:	221348576
Valid:	From 2013 Feb 27th, 00:00:01 GMT Until 2023 Feb 27th, 00:00:01 GMT
Subject Name:	C=US, O=Cisco Systems Inc., OU=DeviceSSL (WebAdmin), CN=169.254.1.1
Issuer Name:	C=US, O=Cisco Systems Inc., OU=DeviceSSL (WebAdmin), CN=169.254.1.1
MD5 Fingerprint:	58:4f:3d:e6:d6:80:d8:45:90:dc:aa:c9:1a:71:78:0f
SHA1 Fingerprint:	06:5c:a9:ec:2f:5d:41:18:51:12:e8:6d:7f:dd:84:b8:56:21:f9:52

Provides greater security by allowing secure access

Security: Enable Client Exclusion Policies

Security → Wireless Protection Policies → Client Exclusion Policies

The image displays two screenshots from the Cisco Wireless LAN Controller (WLC) configuration interface.

Left Screenshot: Client Exclusion Policies

The left sidebar shows the navigation menu with 'Wireless Protection Policies' expanded. The main panel, titled 'Client Exclusion Policies', lists several policies with checkboxes:

- Excessive 802.11 Association Failures ☒
- Excessive 802.11 Authentication Failures ☒
- Excessive 802.1X Authentication Failures ☒
- Maximum 802.1x-AAA Failure Attempts (1 - 3)
- IP Theft or IP Reuse ☒
- Excessive Web Authentication Failures ☒

Right Screenshot: WLANs > Edit 'WNBU-TME'

The right screenshot shows the configuration for a specific WLAN. The 'Security' tab is selected. Under the 'Client Exclusion' section, the following settings are visible:

- Client Exclusion ☒ Enabled
- Timeout Value (secs)
- Maximum Allowed Clients

Other visible settings include 'Enable Session Timeout' (checked, 1800 secs), 'Session Timeout (secs)' (checked, Enabled), 'Override Interface ACL' (IPv4: None, IPv6: None), 'Layer2 Acl' (None), 'P2P Blocking Action' (Disabled), 'Static IP Tunneling' (disabled), 'Wi-Fi Direct Clients Policy' (Disabled), 'Maximum Allowed Clients Per AP Radio' (200), 'Clear HotSpot Configuration' (disabled), 'Client user idle timeout(15-1000000)' (0), 'Client user idle threshold (0-10000000)' (0 Bytes), and 'Radius NAI-Realm' (disabled).

Enable exclusion policies to prevent the network from Assoc/Auth failure attacks.
Disable for Voice deployments

Security: Enable Rogue Policies

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

Rogue Policies

Rogue Detection Security Level ☐ Low ☒ High ☐ Critical ☐ Custom

Rogue Location Discovery Protocol ☐ MonitorModeAps

Expiration Timeout for Rogue AP and Rogue Client entries 1200 Seconds

Validate rogue clients against AAA ☐ Enabled

Validate rogue clients against MSE ☒ Enabled

Detect and report Ad-Hoc Networks ☒ Enabled

Rogue Detection Report Interval (10 to 300 Sec) 30

Rogue Detection Minimum RSSI (-70 to -128) -128

Rogue Detection Transient Interval (0, 120 to 1800 Sec) 300

Rogue Client Threshold (0 to disable, 1 to 256) 0

Rogue containment automatic rate selection ☒ Enabled

Auto Contain

Auto Containment Level ☐ Auto

Auto Containment only for Monitor mode APs ☐ Enabled

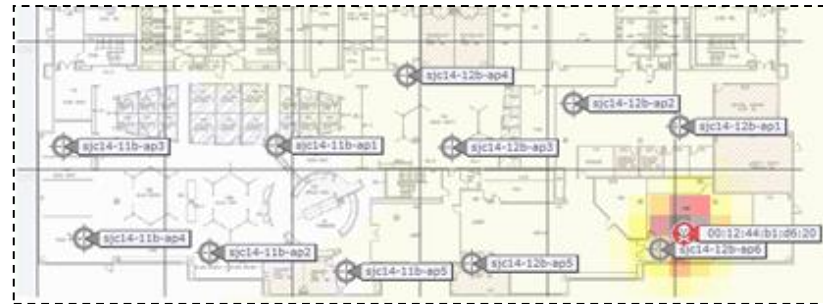
Auto Containment on FlexConnect Standalone ☒ Enabled

Rogue on Wire ☐ Enabled

Using our SSID ☒ Enabled

Valid client on Rogue AP ☒ Enabled

AdHoc Rogue AP ☐ Enabled



Friendly

Malicious



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

BYOD: Radius Timeout >=5 sec

Security → AAA → RADIUS → Authentication

RADIUS Authentication Servers > Edit

Server Index	1
Server Address(Ipv4/Ipv6)	9.1.0.100
Shared Secret Format	ASCII
Shared Secret	***
Confirm Shared Secret	***
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	5 seconds
Network User	<input type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
Management Retransmit Timeout	2 seconds
Realm List	
IPSec	<input type="checkbox"/> Enable

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: Client Idle Timeout

WLANs → WLAN Name → Advanced

WLANs > Edit 'enjoy'

General Security QoS Policy-Mapping Advanced

Client user idle timeout(15-1000000) ☒ 3600 Timeout Value (secs)

Client user idle threshold (0-100000000) Bytes

Radius NAI-Realm ☐

Off Channel Scanning Defer

Scan Defer Priority ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☒ 4 ☒ 5 ☒ 6 ☐ 7

Scan Defer Time(msecs)

MFP Client Protection ☒ Required

DTIM Period (in beacon intervals)

802.11a/n (1 - 255)

802.11b/g/n (1 - 255)

NAC

NAC State

Load Balancing and Band Select

Client Load Balancing ☒

Client Band Select ☒

Passive Client

Passive Client ☐

Voice

Media Session Snooping ☐ Enabled

Re-anchor Roamed Voice Clients ☐ Enabled

KTS based CAC Policy ☐ Enabled

Radius Client Profile

CISCO

MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Controller

Name

802.3x Flow Control Mode

LAG Mode on next reboot (LAG Mode is currently disabled).

Broadcast Forwarding

AP Multicast Mode

AP IPv6 Multicast Mode

AP Fallback


CAPWAP Preferred Mode

Fast SSID change

Link Local Bridging

Default Mobility Domain Name

RF Group Name

User Idle Timeout (seconds) 

ARP Timeout (seconds)

Web Radius Authentication

Operating Environment

Internal Temp Alarm Limits

WebAuth Proxy Redirection Mode

WebAuth Proxy Redirection Port

Maximum Allowed APs

Global IPv6 Config

Web Color Theme

HA SKU secondary unit

Nas-Id

For networks where users stay largely within the coverage area the setting can be increased to 3600 seconds for an SSID running 802.1x or RADIUS NAC against ISE.

BYOD: Client Exclusion

WLANs → WLAN Name → Advanced

The screenshot shows the 'WLANs > Edit 'enjoy'' configuration page. The 'Advanced' tab is selected. In the 'Client Exclusion' section, the 'Client Exclusion' checkbox is checked and highlighted with a red box, and the 'Timeout Value (secs)' is set to 180. Other settings include 'Allow AAA Override' (unchecked), 'Coverage Hole Detection' (checked), 'Enable Session Timeout' (unchecked), 'Aironet IE' (unchecked), 'Diagnostic Channel' (18), 'Override Interface ACL' (IPv4: None, IPv6: None), 'Layer2 Acl' (None), 'P2P Blocking Action' (Disabled), 'Maximum Allowed Clients' (0), 'Static IP Tunneling' (unchecked), 'Wi-Fi Direct Clients Policy' (Disabled), and 'Maximum Allowed Clients Per AP Radio' (200). On the right, 'DHCP' settings show 'DHCP Server' (Override unchecked) and 'DHCP Addr. Assignment' (Required unchecked). 'OEAP' settings show 'Split Tunnel' (Enabled unchecked). 'Management Frame Protection (MFP)' settings show 'MFP Client Protection' (Required checked). 'DTIM Period (in beacon intervals)' shows '802.11a/n (1 - 255)' and '802.11b/g/n (1 - 255)' both set to 1. 'NAC' settings show 'NAC State' (None).

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

BYOD: Session Timeout

WLANs → WLAN Name → Advanced

WLANs > Edit 'enjoy'

General Security QoS Policy-Mapping Advanced

Enable Session Timeout ☒ 300
Session Timeout (secs)

Aironet IE ☐ Enabled

Diagnostic Channel ☐ Enabled

Override Interface ACL IPv4 IPv6

Layer2 Acl

P2P Blocking Action

Client Exclusion ☒ Enabled
Timeout Value (secs)

Maximum Allowed Clients

Static IP Tunneling ☐ Enabled

Wi-Fi Direct Clients Policy

Maximum Allowed Clients Per AP Radio

Clear HotSpot Configuration ☐ Enabled

Client user idle ☒ 30

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)

802.11b/g/n (1 - 255)

NAC

NAC State

Load Balancing and Band Select

Client Load Balancing ☒

Client Band Select ☒

Longer is better for AAA load up to a value of 86400 seconds for 802.1x SSIDs or 65535 seconds for open/CWASSIDs, shorter is better from security point of view.

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

A long-exposure photograph of a city street at night. The foreground is filled with vibrant, multi-colored light trails from moving vehicles, creating a sense of motion. In the background, a pedestrian bridge spans the street, and tall buildings with lit windows and signage line the street. The overall scene is a dynamic urban environment.

FlexConnect Best Practices

FlexConnect Best Practices

FLEX CONNECT

- Enable FlexConnect Groups
- CCKM/OKC Key sharing, consistent WLAN mappings
- Enable Smart AP Image Upgrade

FlexConnect: Enable FlexConnect Groups

Wireless → FlexConnect Groups → Edit “Groupname”

FlexConnect Groups > Edit 'RetailStore_flexgroup'

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

Group Name: RetailStore_flexgroup
Enable AP Local Authentication ☐

FlexConnect APs

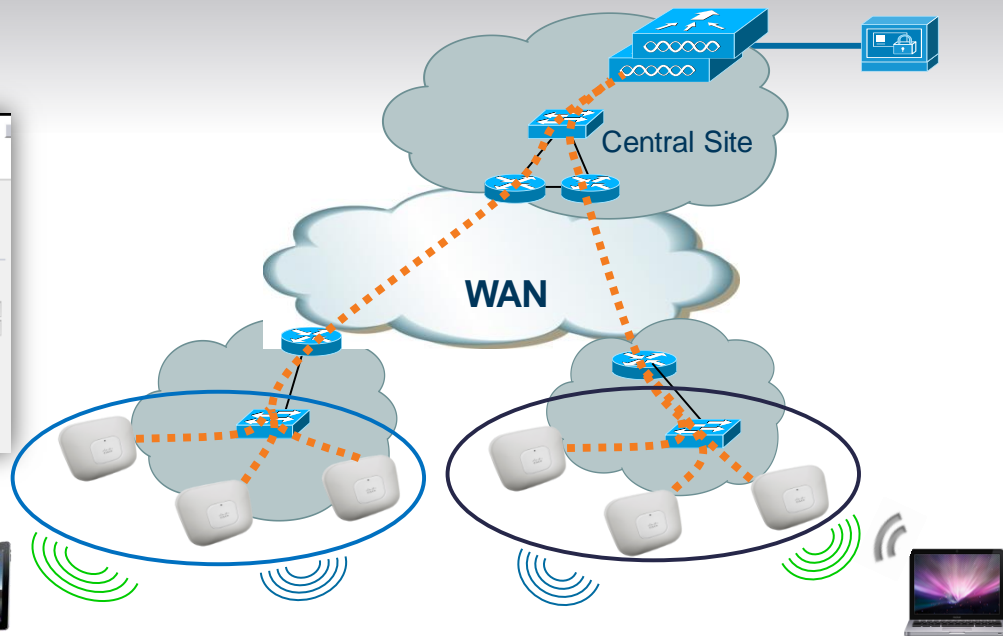
Add AP
Select APs from current controller ☐
Ethernet MAC:
Add Cancel

AP MAC Address	AP Name	Status
7c:ad:74:ff:2f:22	CAP3702	Associated

AAA

Server IP Address: 10.10.10.6
Server Type: Primary
Shared Secret: *****
Confirm Shared Secret: *****
Port Number: 1812
Add

Server Type	Address	Port
UnConfigured	UnConfigured	0
UnConfigured	UnConfigured	0



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

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 ☒

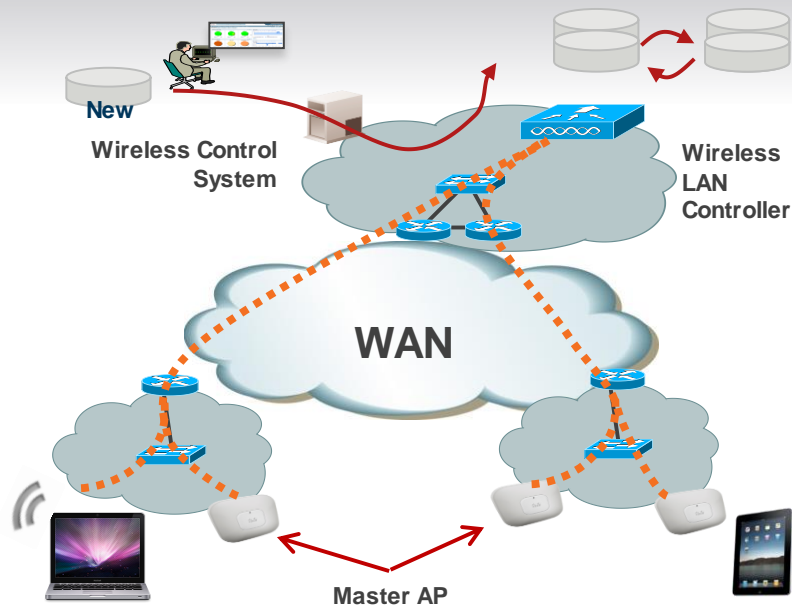
Slave Maximum Retry Count

Upgrade Image

FlexConnect Master APs

AP Name

Master AP Name	AP Model	Manual
CAP3702	c3700E	<input checked="" type="checkbox"/>



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

A long-exposure photograph of a city street at night. The foreground is filled with vibrant, multi-colored light trails from moving vehicles, creating a sense of motion. In the background, a modern pedestrian bridge with blue lighting spans the street. Tall buildings with illuminated windows and storefronts line the street, and several flags are visible on poles to the left.

Outdoor Mesh Best Practices

Mesh Best Practices

BEST PRACTICES (Airos)	INFRASTRUCTURE	
	SECURITY	
	WIRELESS / RF	
	MESH	
	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	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
	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	Disable 802.11b data rates Restrict number of WLAN below 3 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

A long-exposure photograph of a city street at night. The foreground is filled with vibrant, multi-colored light trails from moving vehicles, creating a sense of motion. In the background, a pedestrian bridge spans the street, and modern buildings with illuminated windows and signage line the street. The overall scene is a dynamic urban environment.

Key Takeaways

Best Practice Check Points

Measuring Compliance

WLC

WLAN Express
Setup
7.6 MR2, 8.0, 8.1

**Best Practices defaults,
RF Parameter Optimisation,
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**

- Compliance metric and reporting natively on WLC
- 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
Analyser

**Windows Executable
“show run-config” Based
Analyser Tool**

- Downloadable client
- Configuration stays local
- 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
Agentless – nothing to
download**

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

*Cisco*live!

Best Practices Recommendations Summary

BEST PRACTICES (Airos)

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

OUTDOOR

- 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

References

Cisco Wireless LAN Controller Configuration Best Practices

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

Enterprise Best Practices for Apple Mobile Devices on Cisco Wireless LANs

<http://www.cisco.com/en/US/docs/wireless/technology/vowlan/bestpractices/EntBP-AppMobDevs-on-Wlans.html>

Master Document Link

<http://www.cisco.com/c/en/us/support/wireless/5500-series-wireless-controllers/products-technical-reference-list.html>

A long-exposure photograph of a city street at night. The foreground is filled with vibrant, multi-colored light trails from moving vehicles, creating a sense of motion. In the background, a pedestrian bridge spans the street, and modern buildings with illuminated windows and signage line the street. The overall scene is a dynamic urban nightscape.

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2015 T-Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site
<http://showcase.genie-connect.com/clmelbourne2015>
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 March 12:00pm - 2:00pm



Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com

Cisco *live!*

Thank you.



CISCO