#### ..|...|.. cisco



### Your Time Is Now

# Best Practices for Configuring Cisco Wireless LAN Controllers

Aparajita Sood Technical Marketing Engineer BRKEWN-2670



# **Participating with Poll Everywhere**







# Your poll will show here



Install the app from <u>pollev.com/app</u> 2

Make sure you are in Slide Show mode

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



Cisco((VC)

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Your poll will show here



Install the app from <u>pollev.com/app</u> 2

Make sure you are in Slide Show mode

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



Cisco((VC)

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

#### 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

S

Innovations Faster Time to Market Empower Workforce Efficiency and Innovation

....

Increased Productivity Better Retention Personalize Customer/ Citizen Experience

> Increased Loyalty Greater Insight

#### Mobility

0

Mobile traffic will exceed wired traffic by 2017

#### loT

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



### Network Requirements for the Digital Organization



Infra Software | Highly Available Always on, Always ready



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# Infra Software | Highly Available



# **Infrastructure Best Practices**

Cisco

# **User-First Lifecycle**

#### The Bigger Picture



# WLAN Express Setup Easy Provisioning



# WLAN Express Setup

Day 0/1 Ease of Setup







# WLAN Express Setup

#### Day 0/1 Ease of Setup

Open a web browser and access http://192.168.1.1



Country	India (IN)	• 0
Date & Time	09/05/2014 🛗 12:47:33	
Timezone	Colombo, Kolkata, Mumbai, New Delhi	• 0
NTP Server	0.0.0.0 (optional)	0
Management IP Address	10.10.10.5	0
Subnet Mask	255.255.255.0	
Default Gateway	10.10.10.1	
Management VLAN ID	10	0
	Back Next	

#### Go through a setup wizard

#### **Enable RF Optimization**

3 Advanced Se	tting
RF Parameter	Optimization
Client Density	
L	ow Typical High
Traffic Type	Data
Virtual IP Address	192.0.2.1
Local Mobility Group	Default
	Back Next

#### **Confirm settings**

#### cisco Cisco 2500 Series Wireless Controller

The controller has been fully configured and will now restart.

#### Next Steps:

1. Disconnect the computer from controller port 2, then plug the controller port 1 to the network switch.

2. After the controller is restarted, it will be accessible from the network by going to this URL –  $\rm https://10.10.10.5$ 

# 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
RE Group same as Mobility Name
DHCP Required on Guest WI AN
5 GHz Channel Bonding
o onz onanner 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

20

# 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

ce Data AP Nearby Info Voice Messages Global Messages AP Messages					
Controllers Information:		1		1	
Controller: aoc-103	-wlc1				
	Category	Compliance Love	Total Checks	Passed Checks	Failed Checks
	AP	100%	2	2	0
🕀 AP Groups - WLANs	General	84%	4	37	7
AP Groups - APs	Mobility	100%	1	1	0
WLANS	RF	100%	2	2	0
- Mobility Peers	Voice Cierce	C0%		- 12	6
Radius Servers	Voice- ciso	00%	1.5	13	10
Redundancy	Security	29%	14	4	10
Best Practices - AP					
General Mobility RF		0-40%		Red	
Security		41-80%		Yello	w
Best Practices-All controllers RF Summary-All controllers Site Summary		81-100%		Gree	n

Ciscolive,

#### 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	Expres	s WLA



#### 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

Ciscolive

# **Cisco Active Advisor Personalized Health Score**

ululu Cisco	Active Advi	isor				Halts Fred Flotatore		
All Devices / D	evice Overview	/ Best Practices				Scan Network 👁 All Devices 🖪 Alert Contacts		
Devie Overv	ew	0 Advisories	0 End of Life Warnings	6 Enabled Features	(79) Health			
(79 Q Overall		General Q A	P (100 RF			Show: At Config Error-7 Best Practice-24 Info-0 Export	•	Improve
Category	Severity	Message AP: Syslog messages are si	ent to broadcast address, if there an	e errors reported by many APs, a	nd there are too many APs per vi	an, this can cause broadcast storms. For best practices, it is better to configure to individual server		
Config Error	Warning	(From AP : AP2700 / FTX18	20S266)	high density environments				
Best Practices	Informational	General: AVC visibility is rec	commended. Ensure you are using 7	.4.121.0, 7.6.110.0 or higher. WL	AN: Sujit-test			
Config Error	Warning	General: Band Select is not	in use on any WLAN. it is a recomm	ended feature when there is a go	od AP density in Enterprise deple	pyments, Avoid on voice WLANs		Personalized device
Best Practices	Informational	General: CleanAir detection	is highly recommended if your curre	ent AP HW types support the feat	ure. For 802.11a band			health score
Best Practices	Informational	General: CleanAir detection	is highly recommended if your curre	int AP HW types support the feat	ure. For 802.11b band			Free cloud beend
Best Practices	Warning	General: Controller with teln	et enabled, this is not advisable for	security issues				Free, cloud-based
Best Practices	Warning	General: Controller without	time source, please configure a valid	I NTP server				service
Best Practices	warning	General: Detected channels	rates/11b cap belp to optimize the	channel utilization on the 2.4 ban	i it, it is advisable to enable to im	prove channel distribution on suz.11a band		Automatically takes an
Best Practices	Informational	this may have important RF	dependencies. Global Configuration	1				
View 10 + F	esults per page					First Previous 1 2 3 4 Next Last		network
© 2014 Cisco System	s, Inc. All rights	reserved   Privacy Statement	Terms & Conditions   Help & FAQ			Tall Us What You Think! Send Feedback		

#### 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  $\rightarrow$  Access Points  $\rightarrow$  Global Configurations
- Wireless → Access Points → All APs->AP\_NAME → High Availability

General       Credentials       Interfaces       High Availability       Inventory       Advanced         Image: Secondary Controller       Name       Management IP Address         Primary Controller       WLC1       172.20.227.100         Secondary Controller       Enable       Tertiary Controller         AP Failover Priority       Low +		AI	II APs > D	etails for	AP3600	0-WSSI_1				
Enable     Name     Management IP Address       Primary Controller     WLC1     172.20.227.100       Secondary Controller     Enable     Enable			General	Credenti	als I	interfaces	High Ava	ilability	Inventory	Advanced
Enable   Primary Controller VIC1 172.20.227.100  Secondary Controller Tertiary Controller AP Failover Priority Low			D.i.e.		Name		,	Managemer	nt IP Address	
AP Failover Priority	riority Enable +		Primary C Secondary	ontroller y Controller	WLC1			172.20.227	.100	
AP Failover Priority		-11	Tertiary C	ontroller						
		-	AP Failove	er Priority	Low	¢				
					Critical					

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

# Your poll will show here



Install the app from <u>pollev.com/app</u> 2

Make sure you are in Slide Show mode

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



Cisco((VC)

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

### Infrastructure: Enable AP Multicast mode

#### Controller $\rightarrow$ General $\rightarrow$ AP Multicast Mode

 cısco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTROLLER	WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	
Controller	General		
General Inventory	Name	Cisco Controller	
Interfaces Interface Groups	LAG Mode on next reboot	Disabled   (LAG Mode is currently disabled).	
Multicast	AP Multicast Mode 1	Multicast + 239.28.28.77 Multicast Group Address	Clashing with other protoco
Redundancy	AP IPv6 Multicast Mode <del>1</del> AP Fallback	Unicast ‡ Enabled ‡	
Internal DHCP Server	AP Preferred Mode	Not-Configured	
<ul> <li>Mobility Management</li> <li>Ports</li> </ul>	Fast SSID change Link Local Bridging	Disabled Disabled Disabled	
▶ NTP	Default Mobility Domain Name	MyGroup	

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 $\rightarrow$ Multicast

#### Controller $\rightarrow$ General

Controller Mobility Multicast Messaging   General   Inventory   Inventory   Local Group Multicast IPv4 Address   239.28.28.77   Local Group Multicast IPv6 Address   Multicast   Multicast   Multicast   Multicast   Multicast   Multicast   Multicast   Internace   Groups   Multicast   Multicast <t< th=""><th>uluili. cisco</th><th>MONITOR WLANS CONTROLLER WIRELESS</th><th>Security Management Commands</th><th>HELP FEEDBACK</th><th></th></t<>	uluili. cisco	MONITOR WLANS CONTROLLER WIRELESS	Security Management Commands	HELP FEEDBACK	
General   Inventory   Local Group Multicast IPv4 Address   Interfaces   Local Group Multicast IPv6 Address   Local Group Multicast IPv6 Address   Multicast   Multicast   Multicast   Network Routes   Redundancy   Internal DHCP Server	Controller	Mobility Multicast Messaging			
Interface Groups       Mobility Group         Multicast       Enable Global Multicast Mode         Network Routes       Enable IGMP Snooping         Redundancy       IGMP Timeout (seconds)       60         Internal DHCP Server       IGMP Ouery Interval (seconds)       20	General Inventory Interfaces	Enable Multicast Messaging Local Group Multicast IPv4 Address 239.28.28.77 Local Group Multicast IPv6 Address		Multicast	
Network Routes     Enable IGMP Snooping       Redundancy     IGMP Timeout (seconds)       Internal DHCP Server     IGMP Ouery Interval (seconds)	Interface Groups Multicast	Mobility Group		Enable Global M	lulticast Mode 🛛 🗹
Internal DHCP Server  IGMP Ouery Interval (seconds) 20	<ul> <li>Network Routes</li> <li>Redundancy</li> </ul>			Enable IGMP Sr	seconds) 60
T Mobility Management	Internal DHCP Server			IGMP Query Int	erval (seconds) 20
Mobility Configuration Enable MLD Snooping	Mobility Management				
Mobility Anchor Config     MLD Timeout (seconds)     60       Multicast Messaging     MUD Query Interval (seconds)     20	<ul> <li>Mobility Management Mobility Configuration Mobility Groups</li> </ul>			Enable MLD Sno	ooping

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

uhuhu cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> O	NTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs • wlans	WLANs > Edit 'enjoy	Cos Policy-Mapping Advanced
VLANs Advanced	Profile Name Type SSID Status Security Policies Radio Policy Interface/Interface Group(G) Multicast Vian Feature Multicast Interface Broadcast SSID NAS-ID	

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

# Your poll will show here



Install the app from <u>pollev.com/app</u> 2

Make sure you are in Slide Show mode

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



Cisco((VC)

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

### Infrastructure: Enable Fast SSID change

#### Controller $\rightarrow$ General

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



### Infrastructure: Enable per-user bandwidth contract

#### WLANs $\rightarrow$ Edit 'WLAN\_NAME' $\rightarrow$ QoS

WLANs > Edit 'Gues General Security	Qos Polic	y-Mapping	Advanced
Quality of Service (QoS) Application Visibility AVC Profile Netflow Monitor	Silver (best Enabled none + none +	t effort) ÷	Limit data rates for Guest and Contractor accounts
Override Per-User Ba	ndwidth Contr DownStream	acts (kbps) UpStream	<u>•</u>
Average Data Rate	10	10	
Burst Data Rate	10	10	
Average Real-Time Rate	100	100	
Burst Real-Time Rate	1000	100	

Enforces limits on non-mission critical clients

# Infrastructure: Enable Client Load Balancing

#### WLANs $\rightarrow$ Edit "WLAN-NAME" $\rightarrow$ Advanced

ral Security QoS Policy-Mapping Advanced		Max
atic IP Tunneling 11	Management Frame Protection (MFP)	Load Load
Wi-Fi Direct Clients Policy Disabled +	MFP Client Protection <sup>4</sup> Optional ¢	
Maximum Allowed Clients Per AP Radio 200	DTIM Period (in beacon intervals)	
Clear HotSpot Denabled Enabled	802.11a/n (1 - 255) 1	
Client user idle	802.11b/g/n (1 - 255) 1	
Client user idle threshold 0 Bytes	NAC State None +	Ten and
Radius NAI-Realm	Load Balancing and Band Select	
Iomt Via Wireless Enabled	Client Load Balancing	0110 CA? Past 200
Client Window Size 1-20		
Maximum Denial Count 0-10		New Clien
		Joining Network

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 $\rightarrow$ Edit "WLAN-NAME" $\rightarrow$ Advanced

Nerral       Security       QoS       Policy-Mapping       Advanced         Allow AAA Override       Enabled       DHCP         Coverage Hole Detection       Image: Enabled       DHCP Server       Over         Enable Session Timeout       Image: Enabled       DHCP Addr. Assignment       Requiption         Diagnostic Channel 18       Enabled       DHCP Addr. Assignment       Requiption         Diagnostic Channel 18       Enabled       OEAP       OEAP         Doverride Interface ACL       IPv4 None ‡       IPv6 None ‡       Split Tunnel       Enabled         Layer2 Acl       None ‡       IPv6 None ‡       Split Tunnel       Enabled       Management Frame Protection (MFP         Client Exclusion 3       Image: Enabled       MFP Client Protection 4       Required         Maximum Allowed Clients       0       8       802.11a/n (1 - 255)       1         Static IP Tunneling 11       Enabled       802.11a/n (1 - 255)       1       802.11b/g/n (1 - 255)       1         Wi-Fi Direct Clients Policy       Disabled ‡       NAC       NAC	Ns > Edit 'enjoy'		
Allow AAA Override       Enabled       DHCP         Coverage Hole Detection       Image: Enabled       DHCP Server       Over         Enable Session Timeout       Image: Enabled       DHCP Addr. Assignment       Required         Diagnostic Channel       Image: Enabled       Image: Enabled       Image: Enabled       Image: Enabled         Override Interface ACL       IPv4       None ‡       IPv6       None ‡       Split Tunnel       Enabled         Disabled       ‡       Image: Enabled	neral Security	QoS Policy-Mapping Advanced	
Coverage Hole Detection	Allow AAA Override	Enabled	DHCP
Enable Session Timeout       DHCP Addr. AssignmentRequired         Aironet IE       Enabled         Diagnostic Channel 12       Enabled         Override Interface ACL       IPv4 None ‡       IPv6 None ‡       Split Tunnel       Enabled         Layer2 Acl       None ‡       IPv6 None ‡       Split Tunnel       Enabled         P2P Blocking Action       Disabled ‡       Management Frame Protection (MFP         Client Exclusion 2       Imagement Frame Protection 4       Required         Maximum Allowed Clients 3       0       DTIM Period (in beacon intervals)         Static IP Tunneling 11       Enabled ‡       802.11a/n (1 - 255)       1         Wi-Fi Direct Clients Policy       Disabled ‡       NAC	Coverage Hole Detection	Second Enabled	DHCP Server Override
Override Interface ACL     IPv4     None ‡     IPv6     None ‡     Split Tunnel     Enabled       Layer2 Acl     None ‡     IPv6     None ‡     Management Frame Protection (MF       P2P Blocking Action     Disabled ‡     Management Frame Protection (MF       Client Exclusion ‡     Imeout Value (secs)     MFP Client Protection ‡     Required       Maximum Allowed Clients §     0     Static IP Tunneling ±1     Enabled     802.11a/n (1 - 255)     1       Wi-Fi Direct Clients Policy     Disabled ‡     NAC     NAC	Enable Session Timeout Aironet IE	Enabled	DHCP Addr. Assignment   Required  OEAP
Layer2 Acl     None ÷       P2P Blocking Action     Disabled ÷       Client Exclusion <sup>2</sup> Image: Client Protection for the protectin for the protection for the protection for the protecti	Override Interface ACL	IPv4 None + IPv6 None +	Split Tunnel 🗌 Enabled
Client Exclusion 2     Enabled     60     MFP Client Protection 4     Required       Maximum Allowed Clients 2     0     DTIM Period (in beacon intervals)     0       Static IP Tunneling 11     Enabled     802.11a/n (1 - 255)     1       Wi-Fi Direct Clients Policy     Disabled     \$02.11b/g/n (1 - 255)     1       Maximum Allowed Clients     NAC	Layer2 Acl P2P Blocking Action	None + Disabled +	Management Frame Protection (MFP)
Maximum Allowed Clients     0     DTIM Period (in beacon intervals)       g     Static IP Tunneling 11     Enabled     802.11a/n (1 - 255)       Wi-Fi Direct Clients Policy     Disabled ‡     802.11b/g/n (1 - 255)     1       Maximum Allowed Clients     NAC     NAC	Client Exclusion <sup>3</sup>	€Enabled G0 Timeout Value (secs)	MFP Client Protection 4 Required +
Static IP Tunneling 11         Enabled         802.11a/n (1 - 255)         1           Wi-Fi Direct Clients Policy         Disabled ÷         802.11b/g/n (1 - 255)         1	Maximum Allowed Clients	0	DTIM Period (in beacon intervals)
Wi-Fi Direct Clients Policy     Disabled     \$     802.11b/g/n (1 - 255)     1	Static IP Tunneling 11	Enabled	802.11a/n (1 - 255) 1
Maximum Allowed Clients NAC	Wi-Fi Direct Clients Policy	Disabled +	802.11b/g/n (1 - 255) 1
Per AP Radio NAC State None +	Maximum Allowed Clients Per AP Radio	200	NAC State None +

- 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 $\rightarrow$ Interfaces $\rightarrow$ 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 $\rightarrow$ Restart

ululu cisco	MONITOR WLANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK		Sa <u>v</u> e Configuratior	a   <u>P</u> ing   Logout   <u>R</u> efresh	
Commands	System Restart	_	-	_	_		-	-		Save and Restart	Restart without Save	
Download File Upload File Restort Self Peer Both Config Boot Scheduled Reboot Reset to Factory Default Set Time	Warning: The conf changed and not s Restart" to save th restarted, or click- restart the controll Please be aware th connections will be please log in again	guration of the c aved yet. Click o e changes befor n "Restart witho e without saving at in either case lost. To regain t after the contro	controller is n "Save and e the controller out Save" to g the changes. , all the che connection, ller is restarted	is I.								
Login Banner		_		_				_	_	_	_	

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

#### 73% Faster

sh	ι	Jse Cases
	~	LAG <-> no LAG
l	~	10 G <-> 1 G
l	~	High Availability SSO Pairing
l	~	Post Configuration Wizard
	~	Web-auth certificate installation

Transfer Download of XML

Process Restart to reduce network and service downtime and improve serviceability

#### Infrastructure: Enable Pre-image download

#### Wireless $\rightarrow$ Global Configurations $\rightarrow$ AP Image Pre-download

Vireless	CDP State		✓
	Ethernet Interface#	CDP State	
Access Points	0		
All APs	1		
802.11a/n/ac	2		
802.11b/g/n	3		
Dual-Band Radios	Radio Slot#	CDP State	
Global Configuration	0	<b>I</b>	
Advanced	1		
Load Balancing	2		
Band Select Preferred Calls SIP Snooping	Login Credentials		
RX Sop Threshold	Username		
Mesh	Password		
RF Profiles	Enable Password		
FlexConnect Groups FlexConnect ACLs	802.1x Supplicant Cr	edentials	
802.11a/n/ac			
802.11b/g/n	802.1x Authentication		
Media Stream	<b>AP Failover Priority</b>		
Application Visibility And Control	Global AP Failover Prior	ity	Disable 🗧
Country	AP Image Pre-downl	oad	
Timers		1	
Netflow	Download Primary		Download Backup
0.05	Interchange Image	2	Abort Predownload

Allows for less network downtime during software updates

## FlexConnect: Enable "FlexConnect AP Upgrade"

Wireless  $\rightarrow$  Flexconnect Groups  $\rightarrow$  Edit "Groupname"  $\rightarrow$  Image Upgrade Tab

FlexConnect Groups > Edi	t 'RetailStore_flexgrou	up'			New
General Local Authentic	ation Image Upgrade	ACL Mapping	Central DHCP	WLAN VLAN mapping	Wireless Control
FlexConnect AP Upgrade 🥑 Slave Maximum Retry Count Upgrade Image	44 Primary ÷ FlexC	onnect Upgrade			System LAN Controller
FlexConnect Master APs         AP Name         Add Master					WAN
Master AP Name	AP Model	Manual			
CAP3702	c3700E	no			Macter AP

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 $\rightarrow$ FlexConnect Groups $\rightarrow$ 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

Ciscoll

### Your poll will show here



Install the app from <u>pollev.com/app</u> 2

Make sure you are in Slide Show mode

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



Cisco((VC)

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

#### Network Requirements for the Digital Organization



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

### Self-Optimizing : Automation & Assurance



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

#### Today's Process







Site-1

Ciscolive!

## **RF & RRM Best Practices**

Ciscoliv

#### RF & RRM: Disabling .11b Data Rates

Wireles	ss → 802.11b/g/n →	Network	325'@ 6Mbps 300'@ 9Mbps 275'@ 12Mbps 250'@ 18Mbps 225'@ 24Mbps 200'@ 36Mbps
CISCO * Radios 802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration Advanced Mesh RF Profiles FlexConnect ACLs OEAP ACLs Network Lists * 802.11a/n/ac Network Lists * 802.11a/n/ac Network RF Grouping TPC DCA Coverage General Client Roaming Media EDCA Parameters DFS (802.11h) High Throughput (802.11h/ac) CleanAir * 802.11b/g/n Network * RRM RF Grouping	MONITOR       WLANS       CONTROLLER       WIRELESS       SECURIT         802.11b/g       Global Parameters         602.11b/g       Global Parameters         802.11b/g       Network Status       Image: Status         802.11b/g       Network Status       Image: Status         802.11b/g       Network Status       Image: Status         802.11g       Support       Image: Status         9       Status       Image: Status         9       Status       Image: Status         9       DTPC Support:       Image: Status         9       Image: Status       Image: Status         9       Ima	Y     MANAGEMENT     COMMANDS     HELP     EEDBACK         Data Rates**       1     Mbps     Disabled ÷       2     Mbps     Disabled ÷       5     5.5     Mbps     Disabled ÷       9     Mbps     Disabled ÷       9     Mbps     Disabled ÷       11     Mbps     Disabled ÷       12     Mbps     Mandatory ÷       18     Mbps     Supported ÷       24     Mbps     Supported ÷       36     Mps     Supported ÷       48     Mbps     Supported ÷       54     Mbps     Supported ÷       54     Mbps     Supported ÷       54     Mbps     Supported ÷       54     Mbps     Supported ÷	80'@ 54Mbps 100 @ 440'@ 420'@ 360'@ 2.4GHz100me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40me BH:40m

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

	WLAN WLAN	ETAB-PSK	ETAB-PSK	Enabled	[WPA2][Auth(PSK)]	
	WLAN	ETAB-PSK	ETAB-PSK	Enabled	[WPA2][Auth(PSK)]	<b>•</b>
2	WLAN	PTAD data				_
		ETAB-dotix	ETAB-dot1x	Enabled	[WPA2][Auth(802.1X)]	•
2	WLAN	ETAB-Lync	ETAB-Lync	Disabled	[WPA2][Auth(PSK)]	
4	WLAN	ETAB-FBConnect	ETAB-FBConnect	Enabled	Web-Passthrough	
5	WLAN	ETAB-VConnect	ETAB-VConnect	Disabled	Web-Passthrough	
6	WLAN	ETAB-LocalPolicy	ETAB-LocalPolicy	Disabled	[WPA2][Auth(PSK)]	
<b>Z</b>	WLAN	cudemo1	cudemo1	Enabled	[WPA2][Auth(802.1X)]	
2	WLAN	cudemo2	cudemo2	Disabled	[WPA2][Auth(802.1X)]	
2	WLAN	cudemo3	cudemo3	Disabled	[WPA2][Auth(802.1X)]	
10	WLAN	cudemo4	cudemo4	Disabled	[WPA2][Auth(802.1X)]	
11	WLAN	cudemo5	cudemo5	Disabled	[WPA2][Auth(802.1X)]	
12	WLAN	cudemo6	cudemo6	Disabled	[WPA2][Auth(802.1X)]	
13	WLAN	cudemo7	cudemo7	Disabled	[WPA2][Auth(802.1X)]	

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

### RF & RRM: Restrict Number of WLANs below 4

WLANs → WLANs

CISCO	MONITOR	<u>WLANs</u> <u>C</u> C	ONTROLLER W <u>I</u> RELESS	<u>S</u> ECURITY M <u>A</u> NAGEMENT	C <u>o</u> mmands he <u>l</u> p	<u>F</u> EEDBACK			
WLANs	WLANs								
• WLANs WLANs	Current Filte	er: None	[Change Filter] [Cl	ear Filter]		Create New			
Advanced UKLAN ID Type Profile Name WLAN SSID Admin Status Security Policies									
	<u>1</u>	WLAN	Employee	Employee	Enabled	[WPA2][Auth(802.1X)]			
	<u>2</u>	WLAN	Guest	Guest	Enabled	Web-Auth			
	<u>3</u>	WLAN	Contractor	Contractor	Enabled	[WPA2][Auth(PSK)]			

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 $\rightarrow$ 802.11a/n/ac $\rightarrow$ RRM $\rightarrow$ DCA

#### Channel Assignment Method Automatic Interval: 10 minutes **Invoke Channel Update** Freeze OFF Avoid Foreign AP interference Enabled Avoid Cisco AP load Enabled Avoid non-802,11a noise Enabled Avoid Persistent Non-WiFi Enabled Interference Channel Assignment Leader Cisco\_da:78:24 (172.20.227.99) Last Auto Channel Assignment 467 secs ago DCA Channel Sensitivity Medium ᅌ (5 dB) Channel Width 20 MHz 40 MHz 80 MHz Best Enabled Avoid check for non-DFS channel

#### Dynamic Channel Assignment Algorithm

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 $\rightarrow$ Edit "WLAN-NAME" $\rightarrow$ Advanced

	Challenge	
MLANs > Edit         'WNBU-TME' <th><ul> <li>Dual-Band clients persistently connect to 2.4 GHz</li> <li>2.4GHz may have 802.11b/g clients causing contention</li> <li>2.4GHz is prone to interference</li> </ul></th> <th>Dual-Band Client Radio 2.4/5GHz</th>	<ul> <li>Dual-Band clients persistently connect to 2.4 GHz</li> <li>2.4GHz may have 802.11b/g clients causing contention</li> <li>2.4GHz is prone to interference</li> </ul>	Dual-Band Client Radio 2.4/5GHz
Client Exclusion ?         @Enabled         60         MPP Client Protection # Optional : Timeout Value (secs)         Optional :           Maximum Allowed Clients #         0         DTIM Period (in beacon intervals)           Static IP Tunneling #1         Enabled         802.11a/n (1 - 255)         1	Solution	Discovery
Wi-Fi Direct Clients Policy     Disabled     B02.11b/g/n (1 - 255)       Maximum Allowed Clients Per AP Radio     200       Clear HotSpot Configuration     Enabled       Client user idle timeout[15:100000)     NAC State       Client user idle timeout[15:1000000     Load Balancing and Band Select	BandSelect directs clients to 5 GHz optimizing RF usage	Discovery Probes
Client Load Balancing  Client  Cli	<ul> <li>Better usage of the higher capacity 5GHz band</li> <li>Frees up 2.4 GHz for single band clients</li> </ul>	<b>2.4 5</b> 802.11n <b>9 9</b>
Scan Defer Time(msecs) 100 Voice FlexConnect Enabled	Optimized RF Utilization by Mo Client Out of the Congested	oving 5 GHz Capable 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**

			RF Profile > Edit	test_bb'			
RF Profile > Edit 'HD_2_4' RF Profi	nie > Edit "Ciscolive_Reynote"		General 802.11	RRM Hig	Density Client Distrib	ution	
General 802.11 RRM H Genera	al 802.11 RRM High Density Client Distribution				enent bisting		
			Maximum Power Leve	I Assignment (-10 to	30 dBm) 30	Data RSSI(-90 to -60 dBm)	-65
Data Rates <sup>1</sup> MCS Data R	Rates <sup>1</sup> MCS Settings		Minimum Power Leve	Assignment (-10 to	30 dBm) -10	Voice RSSI(-90 to -60 dBm)	-80
			Power Threshold v1(-	80 to -50 dBm)	-70	Coverage Exception(1 to 75 Cl	ients) 3
1 Mbps Disabled ÷ 0 6 Mbp	as Disabled		Power Threshold v2(-	80 to -50 dBm)	-67	Coverage Level(0 to 100 %)	25
5.5 Mbns Disabled + 2 12 Mb	pps Supported ÷ 2 € Supported			ovoroc			
6 Mbps Supported ÷ 3 18 Mb	pps Supported   3 Supported		TPC, DCA, C	overaç			
9 Mbps Mandatory ‡ 4 24 Mb	Mandatory 🗧 4 🗹 Supported						
11 Mbps Disabled + 5 36 Mb	Dps Mandatory  \$ 5 Supported					Noise (-127 to 0 dBm)	-70
12 Mbps Supported ‡ 6 48 Mb	ops Supported ÷ 6 Supported					Utilization (0 to 100 %)	80
18 Mbps Supported ÷ 7 54 Mb	ops Supported ÷ 7 Supported		DCA Channel List				
24 Mbps Mandatory \$ 8	9 Supported			11			
36 Mbps Supported ÷ 9	10 Supported		1, 0	, 11			
54 Mbps Supported + 11	11 Supported		DCA Channels				
	12 🗹 Supported						
Data Rates	13 Supported	RF	Profile > Edit '8	)2.11a_de	emo'		
	14 Supported						
15	15 Supported						
16	10 8 144		Seneral 802.11	RKM	High Density	Client Distributio	n
17	RF Profile > Edit 'CiscoLive_Keynot	/					
	General 802.11 RRM High D	nsity Client Distribution	ligh Density Param	eters	Multicas	st Parameters	
							_
			Maximum Clients(1 to	200) 200	Multica	st Data Rates <sup>2</sup> auto	\$
	Load Balancing		Client Tree Three held	50			_
			Client Trap Threshold	50			
Load Balancing	Window(0 to 20 Clients) 5		. Con Threehold D			High Density	V
g	Denial(1 to 10)	ĸ	x Sop Threshold P	rameters			
			Rx Sop Threshold	Aut	<b>*</b>		
listol							
Cisco(( <i>VCi</i>		Bł	RKEWN-2670 © 201	6 Cisco and/or	its affiliates. All rights res	served. Cisco Public 53	3

#### 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	RF Profile				
Access Points	Enable Out Of Box				
Radios 802.11a/n/ac	Enable Persistence				
802.11b/g/n Dual-Band Radios	Profile Name	Radio Policy	Applied		
Global Conliguration	High-Client-Density-(802.11a)	802.11a	No	-	
Advanced	High-Client-Density-(802.11bg)	802.11b/g	No	-	
Band Select	Low-Client-Density-(802.11a)	802.11a	No	-	
Preferred Calls	Low-Client-Density-(802.11bg)	802.11b/g	No		
SIP Snooping	Typical-Client-Density(802.11bg)	802.11b/g	No		i Dro built PE profiles
Optimized Roaming Network Profile	Typical-Client-Density-(802.11a)	802.11a	No		use with AP Groups
Mesh					 
<b>RF Profiles</b>					

#### RF & RRM: Enable Cisco CleanAir

#### Wireless $\rightarrow$ 802.11a/n/ac or 802.11b/g/n $\rightarrow$ CleanAir

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

### RF & RRM: Enable Cisco EDRRM

Wireless  $\rightarrow$  802.11a/n/ac or 802.11b/g/n  $\rightarrow$  RRM  $\rightarrow$  DCA

	EDCA Parameters	1	.04					
	DFS (802.11h)	1	.08					
	(802.11n/ac)	1	.12					
	CleanAir	1	.16					
•	802.11b/g/n	1	.32					
×	Media Stream		26					
×	Application Visibility And Control	Extended UNII-	2 channels	Enabled				
	Country	Event Driven	RRM		Í	<b>C</b> omolitius		
	Timers					Sensitivi	ty threshold	- 1
×	Netflow	EDRRM		Enabled		recomm	ended to Mediun	<u>ו</u>
•	QoS	Sensitivity Thre	eshold Med	dium 🗘 🥤				

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 $\rightarrow$ 802.11a/n/ac $\rightarrow$ RRM $\rightarrow$ DCA

،،۱،،۱۰، cısco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTROLLI	ER WIRELESS SECURITY MANAGEMENT COMMANDS HELP				
Wireless	802.11a > RRM > Dynamic Channel Assignment (DCA)					
Access Points     All APs     Padies	Dynamic Channel Assignment Algorithm					
802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration	Channel Assignment Method	Automatic Interval: 10 minutes      AnchorTime: 0      Freeze Invoke Channel Update Once     OFF				
Advanced	Avoid Foreign AP interference	Senabled				
Mesh	Avoid Cisco AP load	Enabled				
<b>RF Profiles</b>	Avoid non-802.11a noise	C Enabled				
FlexConnect Groups	Avoid Persistent Non-WiFi Interference 🔲 Enabled					
FlexConnect ACLs	Channel Assignment Leader SmartRoam-TME-Lab (172.20.227.100)					
802.11a/n/ac Network	Last Auto Channel Assignment	118 secs ago				
▼ RRM	DCA Channel Sensitivity	Medium				
RF Grouping TPC	Channel Width	◯20 MHz ◯ 40 MHz ●80 MHz				
DCA Coverage	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

### Your poll will show here



Install the app from <u>pollev.com/app</u> 2

Make sure you are in Slide Show mode

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



Cisco((VC)

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

# 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







Cisco

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

### **Cisco and Apple Optimized Roaming**



**Cisco-AP** 

#### Adaptive 11r/k/v

#### Features enabled by default on a newly created SSID

#### WLANs > Edit 'WHOPPERWIFI'

	Security	QoS	Policy	Mapping	Advanced
Layer 2	Layer 3	AAA Se	ervers		
Layer 2	Security <sup>6</sup> W	/PA+WPA2 C Filtering <sup>9</sup>		~	
Fast Transi Fast Transi Over the D Reassociati Protected	tion Adaptive S	Seconds	Enabl Disab Adapt	e le ive	
PMF		Disab	led 🗸		
WPA+WP	A2 Parameter	s			
	licy				
WPA Po					
WPA Po WPA2 P	olicy	$\checkmark$			
WPA Po WPA2 F WPA2 E	Policy Encryption	✓ ✓ AES	г	KIP	
WPA Po WPA2 P WPA2 E OSEN P	olicy incryption olicy	✓ ▲AES	; 🔲 т	KIP	

General Security	Qua	Poncy-mapping	Muvanceu		
Learn Client IP Address 2	<b>√</b> E	nabled		HTTP Profiling	
Vian based Central	0.6	nabled		PMIP	
Central DHCP Procession	0.	nabled		PMIP Mobility Type	0
Override DNS	0.	nabled		PMIP NAL Type	Hexadecimal ‡
NAT-PAT	0.6	nabled			
Central Assoc	0.	nabled		PMIP Profile	None :
ync				PMIP Realm	
Lync Server	Disabl	ed :		Universal AP Admin	
1k				11v BSS Transition Support	
Assisted Roaming Predicti	on Optin	nization 🗌 Enabled		BSS Transition	Ø
Neighbor List		🗹 Enabled		Disassociation Imminent	0
Neighbor List Dual Band		Enabled		Disassociation Timer(0 to 3000 TBTT)	200
Denial Maximum Count Prediction Minimum Count		2		Optimized Roaming Disassociation Timer(0 to 40 TBTT)	40
		-		BSS Max Idle Service	<b>e</b>
				Directed Multicast Service	2
				Tunneling	
General Security Learn Client IP Address 2	QoS ✓ E	Policy-Mapping nabled	Advanced		0
Vian bacad Control				HTTP Profiling	O.
Switching 12	E	nabled		PMIP	
Central DHCP Processing	0 E	nabled		PMIP Mobility Type	0
Override DNS	🗌 E	nabled		PMIP NAI Type	Hexadecimal +
NAT-PAT	0 6	nabled		PMIP Profile	(New A)
Central Assoc	() E	nabled			None +
Lync				PMIP Realm	
Lync Server	Disabl	ા કો		Universal AP Admin Support	
Lyne Server	013401			Universal AP Admin	
LIK				11v BSS Transition Support	
Assisted Roaming Predicti	on Optin	nization 🗌 Enabled		BSS Transition	2
Neighbor List		Enabled		Disassociation Imminent	0
Neighbor List Dual Band		Enabled		Disassociation Timer(0 to 3000 TBTT)	200
Denial Maximum Count		2		Optimized Roaming Disassociation Timer(0	
Prediction Minimum Count		2		to 40 TBTT)	40
				BSS Max Idle Service	1

Fast Natas

Directed Multicast Service

### **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

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

## 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

Supports Fast lane



QoS Profile | Voice QoS Trust | AutoQoS | Better EDCA

## Fast Lane

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

#### WLANs > Edit 'WHOPPERWIFI' Edit QoS Profile Policy-Mapping General Security OoS Advanced platinum **OoS Profile Name** Quality of Service (QoS) Platinum (voice) ~ Application Visibility Enabled For Voice Applications Description AVC Profile $\sim$ none Per-User Bandwidth Contracts (kbps) \* Flex AVC Profile none 🗸 DownStream Netflow Monitor none 🗸 Average Data Rate 0 Fastlane Enable 🗸 Burst Data Rate 0 Average Real-Time Rate 0 Override Per-User Bandwidth Contracts (kbps) 16 Burst Real-Time Rate ln DownStream UpStream Average Data Rate 0 0 Per-SSID Bandwidth Contracts (kbps) \* Burst Data Rate 0 0 DownStream Average Data Rate 0 Average Real-Time Rate 0 0 Burst Data Rate 0 Burst Real-Time Rate 0 0 Average Real-Time Rate 0 Clear Burst Real-Time Rate lo. Override Per-SSID Bandwidth Contracts (kbps) 16 WLAN QoS Parameters Maximum Priority

		Plaximum Phoney	Voice
		Unicast Default Priority	besteffort V
General		Multicast Default Priority	besteffort V
EDCA Profile	Fastlane 🗸	Wired QoS Protocol	
Enable Low Latency MAC <sup>1</sup>		Protocol Type	None 🗸

UpStream

UpStream

0

0

0

0

0

0

### 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

pice Video Media			
ll Admission Control (CAC)		802.11b(2.4 GHz) > Media	
Admission Control (ACM)	✓ Enabled		
CAC Method 4	Load Based	Voice Video Media	
Max RF Bandwidth (5-85)(%)	50	Call Admission Control (CAC)	
Reserved Roaming Bandwidth (0-25)(%)	6	Admission Control (ACM)	✓ Enabled
Expedited bandwidth	<b>~</b>	CAC Method 4	Load Based 🗸
SIP CAC Support <sup>3</sup>	Enabled	Max RF Bandwidth (5-85)(%) Reserved Roaming Bandwidth (0-25)(%) Expedited bandwidth	50 6 🖌
r-Call SIP Bandwidth <sup>2</sup>		SIP CAC Support <sup>2</sup>	Enabled
SIP Codec	G.711	Per-Call SIP Bandwidth <sup>2</sup>	
SIP Bandwidth (kbps)	64	SIP Codec	G.711 V
SIP Voice Sample Interval (msecs)	20 🗸	SIP Bandwidth (kbps)	64
		SIP Voice Sample Interval (msecs)	20 🗸
affic Stream Metrics		Traffic Stream Metrics	
Metrics Collection		Metrics Collection	


# 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 ("wellknown" DSCP values mapped to IETFrecommended values, "unexpected" DSCP values mapped to BE

W	ireless	Qo	)S Ma	ap Confi	g				
•	Access Points All APs Radios 802.11a/n/ac 802.11b/g/n Dual-Band Radios	1	Qos Ma Frust D	scp UpStr	En eam 🔽	able 🗸	Add DSCP	Exception	
	Global Configuration		leer Dr	ioritu		0.14	DECD Even	ntion	
•	Advanced		JSELFI			0 🗸	DSCP EXCe	ption	
	Mesh	L	JSCP L	Default		0	User Priori	ty	0 🗸
•	ATF	1	DSCP 5	Start		0	Add		Clear All
	RF Profiles	[	DSCP E	Ind		0	DSCP Exce	ption List	t
	FlexConnect Groups	٣	lodify				DSCP	IIP	
	FlexConnect VLAN Templates	UP	to D	SCP Map	List		48	0	
	OEAP ACLs			Default	Start	End	56	0	
	Network Lists	-	UP	DSCP	DSCP	DSCP	46	6	
	802.11a/n/ac		0	0	0	7	44	6	
	802.11b/a/n		1	8	8	15	40	5	
1	Modia Stream		2	16	16	23	38	4	
			3	24	24	31	36	4	
•	Application visibility And Control		4	32	32	39	34	4	
	Country		5	34	40	4/	32	5	
	Timers		7	40	40 63	63	30	4	
	Netflow		<i>,</i>	50	05	05	28	4	
_	0.05						20	4	<b>_</b>
	Profiles						27	3	
	Roles						20	3	
	Qos Map						18	3	
							16	0	
							14	2	
							12	2	
								-	_

1

## **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

Ciscolive

### 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%</li>
- Jitter < 100 ms.</li>

cisco		WLANS CO	ONTROLLER	WIRELESS	SECURITY		
Monitor	Clients > D	ietail					
Summary Access Points Cisco CleanAir	Max Number of Records 10 Clear AVC Stats						
Statistics	General	AVC Stat	istics				
+ CDP	Client Statistics						
Rogues	Bytes Rec	eived	22904764 12274596 237005				
Clients	Bytes Ser	nt i					
Sleeping Clients	Packets R	eceived					
Multicast Applications Local Profiling	Packets S	ent	47599				
	Policy Err	ors	0 -54 35				
	RSSI						
	SNR						
	Sample T	ime	Tue Dec 29 17:59:19 2015				
	Excessive	Retries	0				
	Retries		0				

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

Cisco

### Cisco & Apple : Data Rates

### Wireless > 802.11a/n/ac > Network

cisco	MONITOR WLANS CONTR	OLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK
Vireless	802.11a Global Paramete	ers					
Access Points	General			Data Rates*	•	_	
802.11a/n/ac	802.11a Network Status	🕑 Enabled		6 Mbps	Dis	abled	
802.11b/g/n Dual-Band Radios	Beacon Period (millisecs)	100		9 Mbps	Dis	abled	0
Global Configuration	Fragmentation Threshold	2346		12 Mbps	Ma	ndatory	
Advanced	DTPC Support.	Enabled		18 Mbps	Su	pported	0
Mesh	Maximum Allowed Clients	200		24 Mbps	Ma	ndatory	
ATF	RSSI Low Check	Enabled		36 Mbps	Su	pported	0
RF Profiles	RSSI Threshold (-60 to -90	-80		48 Mbps	Su	pported	0
FlexConnect Groups	802.11a Band Status			54 Mbps	Su	pported	
FlexConnect ACLs	Low Band	Enabled		CCX Location	n Measuremer	nt	
Templates	Mid Band	Enabled		Mode	0 6	nabled	
OEAP ACLs	Hiu Banu	Enabled					
Network Lists	High Band	Enabled					
802.11a/n/ac	** Data Rate 'Mandatory' impl specific rate will not be able to	ies that clients who do r	ot support the	at			



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

Cisco

### Network Requirements for the Digital Organization



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# Self-Defending : Security and Compliance



# Security : Enable 802.1x authentications on WLAN

### WLANs $\rightarrow$ Edit 'WLAN\_NAME' $\rightarrow$ Security

'LANs > Edit 'Employee'	WLANs > Edit 'Employee'
General Security QoS Policy-Mapping Advanced	General Security QoS Policy-Mapping Advanced
Layer 2 Layer 3 AAA Servers	Layer 2 Layer 3 AAA Servers
Layer 2 Security <sup>g</sup> WPA+WPA2 MAC Filtering <sup>g</sup>	Select AAA servers below to override use of default servers on this WI
Fast Transition	Radius Servers
Fast Transition	Radius Server Overwrite interface Enabled
Fast Transition  Protected Management Frame	Radius Server Overwrite interface Enabled
Fast Transition  Protected Management Frame PMF Disabled  WPA+WPA2 Parameters	Radius Server Overwrite interface       Enabled         Authentication Servers       Accounting Servers         ✓       Enabled
Fast Transition  Protected Management Frame PMF Disabled  WPA+WPA2 Parameters WPA Policy	Radius Server Overwrite interface       Enabled         Authentication Servers       ✓ Enabled         ✓ Enabled       ✓ Enabled         Server 1       IP:172.20.227.106, Port:1812 ‡ None ‡
Fast Transition  Protected Management Frame PMF Disabled  WPA+WPA2 Parameters WPA Policy  WPA2 Policy	Radius Server Overwrite interface       Enabled         Authentication Servers       Image: Comparison of the server
Fast Transition □ Protected Management Frame PMF Disabled   WPA + WPA2 Parameters WPA Policy  WPA2 Policy  WPA2 Encryption   ✓AES TKIP	Radius Server Overwrite interface       Enabled         Authentication Servers       Image: Comparison of the server
Fast Transition □ Protected Management Frame PMF Disabled ÷ WPA Policy □ WPA2 Policy □ WPA2 Policy □ WPA2 Encryption □ Authentication Key Management	Radius Server Overwrite interface       Enabled         Authentication Servers       ✓ Enabled         ✓ Enabled       ✓ Enabled         Server 1       IP:172.20.227.106, Port:1812 ‡         Server 2       None         Server 3       None         Server 4       None
Fast Transition Protected Management Frame PMF Disabled ‡ WPA Policy WPA2 Policy WPA2 Policy WPA2 Encryption AES TKIP Authentication Key Management B02.1X C Enable	Radius Server Overwrite interface       Enabled         Authentication Servers       Image: Comparison of the server server server server 1         Server 1       IP:172.20.227.106, Port:1812 + None + Server

Provides greater network security on WLAN using 802.1x authentication

# Security: Enable 802.1x authentications for AP

### Wireless $\rightarrow$ Access Points $\rightarrow$ Global Configurations

802.1x Supplicant Credentials		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)# app now-model
802.1x Authentication		Switch(config)# aaa new-model Switch(config)# aaa authentication dot1x default group radius
Username	testap	Switch(config)# radius-server host ip_addr auth-port port acct-port port key key
Password	•••••	Switch(config)# interface fastethernet2/1 Switch(config-if)# switchport mode access
Confirm Password	•••••	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

			_	5
net-SS	H Confi	guration		
Session Timeout (minutes)5Maximum Number of Sessions5 \$				
Allow New Telnet SessionsNo ‡Allow New SSH SessionsYes ‡				
	net-SS ession Ti aximum Ilow New Ilow New	net-SSH Confi ession Timeout (mi aximum Number of llow New Telnet Se llow New SSH Sess	net-SSH Configuration ession Timeout (minutes) aximum Number of Sessions llow New Telnet Sessions llow New SSH Sessions	net-SSH Configurationession Timeout (minutes)5aximum Number of Sessions5 \$llow New Telnet SessionsNo \$llow New SSH SessionsYes \$

Provides greater security by allowing secure access and denying unencrypted access

# Security: Disable Management Over Wireless

### Management → Mgmt Via Wireless

،، ،،، ،، cısco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Management	Managem	nent Via	Wireless						
Summary SNMP HTTP-HTTPS Telnet-SSH Serial Port Local Management Users User Sessions	Enable Co	Enable Controller Management to be accessible from Wireless Clients							
<ul> <li>Logs</li> <li>Mgmt Via Wireless</li> <li>Software Activation</li> <li>Tech Support</li> </ul>									

### Disallow management of the Controller via Wireless

Cisco

# Security: Secure Web Access (HTTPS)

### Management → HTTP-HTTPS

 cısco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	
Management Summary SNMP HTTP-HTTPS Telnet-SSH Serial Port Local Management Users	HTTP-HTTPS Configuration HTTP Access Enabled : HTTPS Access <sup>2</sup> Enabled : WebAuth SecureWeb <sup>1</sup> Enabled : Web Session Timeout 30 Minutes Current Certificate	
User Sessions Logs Mgmt Via Wireless Software Activation Tech Support	Name:         bsnSslWebadminCert           Type:         3rd Party           Serial Number:         221348576           Valid:         From 2013 Feb 27th, 00:00:01 GMT Until 2023 Feb 27th, 00:00:01           Subject Name:         C=US, 0=Clisco Systems Inc., 0U=DeviceSSL (WebAdmin), CN=169           Issuer Name:         C=US, 0=Clisco Systems Inc., 0U=DeviceSSL (WebAdmin), CN=169           MD5 Fingerprint:         S8:4f:3d:e6id6:80: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	GMT 9.254.1.1 9.254.1.1

### Provides greater security by allowing secure access

Ciscolivel

## Security : Disable WiFi Direct



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 $\rightarrow$ AAA $\rightarrow$ User Login Policies

 cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MAN	AGEMENT
Security	User Policies	
<ul> <li>AAA</li> <li>General</li> <li>RADIUS</li> <li>Authentication</li> <li>Accounting</li> <li>Fallback</li> </ul>	Max Concurrent Logins for a user name <sup>1</sup> 5	
DNS Downloaded AVP TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients	1. When using 802.1X security make sure max-login-ignore-identity-respor	Range is between 0 – 8. Zero indicates no limit

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 $\rightarrow$ Wireless Protection Policies $\rightarrow$ Client Exclusion Policies

Disabled Clients AP Policies Password Policies       Client Exclusion Policies         Advanced EAP       Kccssive 802.11 Authentication Failures I         Priority Order       Excessive 802.11 Authentication Failures I         Certificate       Maximum 802.1x-AAA Failure Attempts 3 (1 - 3)         Policies Policies Certificate       IP Thef or IP Reuse         Wireless Protection Policies General Rogue Rules Friendly Rogue Standard Signatures       IP visity Order         Standard Signatures Curtom Standard       Maximum Allowed Clients # Standard Signatures       General Standard Signatures	, , <b>  , , ,   , ,</b> , , , , , , , , , , , , , , , , ,	itor <u>w</u> lans <u>c</u> ontroller w <u>i</u> reless <u>s</u> ecurity m <u>a</u> n	AGEMENT C <u>O</u> MMANDS HE <u>L</u> I	P <u>F</u> EEDBACK		
Signature Events     Wi-Fi Direct Clients Policy     Disabid     200     802.11b/g/n (1 - 255)     1       Signature Events     Maximum Allowed Clients Per AP Radio     200     NAC     NAC       Client Exclusion     Cliert User Idle timeout(15-100000)     Insabid     NAC     Insabid       Policies     Client user Idle timeout(15-100000)     Insabid     NAC State     Nac       Management Frame Protection     Client user Idle timeshold (0-10000000)     Insabid     Insabid     Client Lade Balancing and Band Select       Veh Auth     Off Channel Scanning Defer     Client Lade Slancing     Insabid	Disabled Clients User Login Policies AP Policies Password Policies Client Advanced EAP Priority Order Certificate Access Control Lists Certificate Access Control Lists Wireless Protection Policies General Rogue Policies General Rogue Rules Friendly Rogue Standard Signatures Signature Events Summary Client Exclusion Policies AP Authentication Management Frame Protection	nt Exclusion Policies	WLAN Gen Ei A D D O O L L R C C C C M S S W M C C C C C C C C C C C C C C C C C C	Ns > Edit 'WNBU-TME' teral Security QoS Po inable Session Timeout Aironet IE Digenostic Channel 18 Override Interface ACL ayer2 Acl 22P Blocking Action Client Exclusion 3 Haximum Allowed Clients 8 Static IP Tunneling 11 Wi-Fi Direct Clients Policy Maximum Allowed Clients Per AP Radio Clear HotSpot Configuration Client user idle timeout(15-100000) Client user idle threshold (0-10000000) Radius NAI-Realm	Iicy-Mapping Advanced Timeut (sees) ✓Enabled IPv4 None 2 IPv6 None 2 Disabled 2 ✓Enabled 3 ✓Enabled 2 Enabled 2 Enabled 2 Enabled 2 Enabled 2 Enabled 2 Enabled 3 Enabled 3	DHCP Server Control DHCP Addr. Assignment Required OEAP Split Tunnel Enabled Management Frame Protection (MFP) MFP Client Protection f Optional : DTIM Period (in beacon intervals) 802.11a/n (1 - 255) 1 802.11a/n (1 - 255) 1 NAC NAC State None : Load Balancing and Band Select Client Load Balancing C

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 $\rightarrow$ Wireless Protection Policies $\rightarrow$ Rogue Policies $\rightarrow$ General $\rightarrow$ Low

cisco	MONITOR WLANS CONTROLLER WIRELESS SECU	RITY MANA	GEMENT COMMANI	S HELP	EEEDBACK	
Security	Rogue Policies					
- AAA	-					
General	Rogue Detection Security Level	Low	🔾 High	0	Critical	Custom
▼ RADIUS Authentication	Rogue Location Discovery Protocol	Disable	\$			
Accounting	Expiration Timeout for Rogue AP and Rogue Client entries	240	Seconds			
DNS	Validate rogue clients against AAA	Enabled				
Downloaded AVP	Validate rogue AP against AAA	Enabled				
LDAP	Polling Interval	0	Seconds			
Local Net Users MAC Elitering	Validate rogue clients against MSE	Enabled				
Disabled Clients	Detect and report Ad-Hoc Networks	Enabled				
User Login Policies AP Policies	Rogue Detection Report Interval (10 to 300 Sec)	60				
Password Policies	Rogue Detection Minimum RSSI (-70 to -128)	-80				
Local EAP	Rogue Detection Transient Interval (0, 120 to 1800 Sec)	120				
Advanced EAP	Rogue Client Threshold (0 to disable, 1 to 256)	0				
Priority Order	Rogue containment automatic rate selection	Finabled				
Certificate						
Access Control Lists	Auto Contain					
Wireless Protection	Auto Containment Level	1				
Rogue Policies	Auto Containment only for Monitor mode APs	Enabled				
General Rocker Roder	Auto Containment on FlexConnect Standalone	Enabled				
Friendly Rogue	Rogue on Wire	Enabled				
Standard Signatures	Using our SSID	Enabled				
Signature Events	Valid client on Rogue AP	Enabled				
Clinet Evolution	AdHoc Roque AP	Enabled				





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

0.0

Friendly

# Security: Set Rogue Detection RSSI

### Security $\rightarrow$ Wireless Protection Policies $\rightarrow$ Rogue Policies $\rightarrow$ General

 cısco	MONITOR WLANS CONTROLLER WIRELESS SECU	RITY MANAGEMENT COMMANDS HELP FEEDBACK
Security	Rogue Policies	
<ul> <li>AAA</li> <li>General</li> <li>RADIUS</li> <li>Authentication</li> <li>Accounting</li> </ul>	Rogue Detection Security Level Rogue Location Discovery Protocol Expiration Timeout for Rogue AP and Rogue Client entries	Low High Critical Custom MonitorModeAps : 1200 Seconds
Fallback DNS Downloaded AVP	Validate rogue clients against AAA Validate roque clients against MSE	□Enabled
TACACS+     LDAP     Local Net Users	Detect and report Ad-Hoc Networks Rogue Detection Report Interval (10 to 300 Sec)	€ Enabled
MAC Filtering Disabled Clients User Login Policies	Rogue Detection Minimum RSSI (-70 to -128) Rogue Detection Transient Interval (0, 120 to 1800 Sec)	-70
Password Policies	Rogue Client Threshold (0 to disable, 1 to 256)	0
Advanced EAP	Rogue containment automatic rate selection Auto Contain	✓Enabled
Certificate	Auto Containment Level	Auto 🗘
Access Control Lists     Wireless Protection	Auto Containment only for Monitor mode APs	Enabled
Policies     Rogue Policies	Rogue on Wire	Enabled
General Rogue Rules Friendly Roque	Using our SSID Valid client on Roque AP	✓Enabled ✓Enabled

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

### BYOD: Radius Timeout >=5 sec

### Security $\rightarrow$ AAA $\rightarrow$ RADIUS $\rightarrow$ Authentication

RADIUS Authentication Serve	rs > Edit
Server Index	1
Server Address(Ipv4/Ipv6)	9.1.0.100
Shared Secret Format	ASCII ÷
Shared Secret	•••
Confirm Shared Secret	•••
Key Wrap	<ul> <li>(Designed for FIPS customers and requires a key wrap compliant RADIUS server)</li> </ul>
Port Number	1812
Server Status	Enabled +
Support for RFC 3576	Enabled +
Server Timeout	5 seconds
Network User	Enable
Management	✓ Enable
Management Retransmit Timeout	2 seconds
Realm List	
IPSec	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** : 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



Install the app from <u>pollev.com/app</u> 2

Make sure you are in Slide Show mode

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



Cisco((VC)

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

### Network Requirements for the Digital Organization



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# Self-Aware : Insights and Experiences



# Application Visibility : Enable AVC and Netflow

### Wireless $\rightarrow$ Application Visibility and Control $\rightarrow$ AVC Profiles

WLANs > Edit       'Contractor'         General       Security       QoS       Policy-Mapping         Quality of Service (QoS)       Silver (best effort) ÷       Application Visibility       € Enabled         AVC Profile       block_facebook ÷       Netflow Monitor       none ‡	Advanced Enable Application Visibility	Citrix Merosoft Lync
WMM Policy Allowed ‡ 7920 AP CAC Enabled 7920 Client CAC Enabled		
	Application Group browsing \$	0
	Application Name facebook +	
Add per application rules	Action Drop ÷	No.

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

### Device Visibility : Enable Local Profiling WLANs $\rightarrow$ Edit $\rightarrow$ WLAN NAME $\rightarrow$ Advanced Save Configuration | Eng | Logout | Ke MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK WLANs > Edit 'Demo-Employee' < Back Apply General Security 005 Policy-Mapping Advanced Client Load Balancing **Off Channel Scanning Defer** Client Band Select Scan Defer Priority 01234567 Passive Client Passive Client 12 Scan Defer Time(msecs) 100 Volce FlexConnect Media Session Snooping E Enabled FlexConnect Local Enabled Enabled Switching 2 Re-anchor Roamed Voice Clients CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK KTS based CAC Policy Enabled FlexConnect Local Auth 12 Enabled Monitor Local Profiling > Device Stats Learn Client IP Address 2 **Radius Client Profiling** Enabled Summary **DHCP** Profiling **Device Stats** Manufacturer Stats Vlan based Central Enabled Access Points Switching 12 17 HTTP Profiling Cisco CleanAl Central DHCP Processing Enabled Local Client Profiling > Statistics Override DNS Enabled CDP DHCP Profiling Rogues NAT-PAT Enabled **HTTP Profiling** Clients PHIP Sleeping Clients Anole-Device/ 33,33% 1 Multicast. PMIP Mobility Type None w Apple-Device( 66.67% ) Apple-iPad( 33.33% ) Applications Macintosh-Workstation( 33.33%) OS\_X-Workstation( 33.33% ) Local Profiling Device Type (46) Count Manufacture (%) Apple-Device 33.33 66.67 Anole-Device Apple-iPad 33.33 Macintosh-Workstatio 33.33 OS X-Workst

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?



Ciscolive;

### **Client View – Enhancements**



Ciscolive,

### Connection Score – Where do I find it?

Monitoring     ■ Network Summary		sco 2500 Series Wi	reless Controll	ler			Q AF	<sup>2</sup> or Client Search	Advanced	4	•
Access Points	CLIENT VIEW										
Clients											
∕∂Wireless Dashboard	GENERAL	Connection Score									
AP Performance		Connection Rates									
Client Performance		Max AP Rate	217 Mbps			100%	ation DHCP	Online			
🖞 Best Practices		Max Client Rate	144 Mbps			Connection Score					
	MAC Address	Client Rate	144 Mbps							.iii	
	Uptime	Spatial Streams						Usage		% Usage	
	AP Name	opatial otreams			_			10.6 KB		76.09%	
	Nearest APs	AP Radio	3					2.5 KB		18.2%	
	Device Type	Client Radio	2					010.0 D		J.7 176	
	Performance	Channel Width									
	Capabilities Connection Score	AP Radio	20 MHz								
		Client Radio	20 MHz								
	MOBILITY										
	WLC With (LOCAL) (C/					Close					
			<b>_</b>								
	AIR-GT2504-K9 192.168.20.20 ; ::/	C2700-AP3 192.108.21.109	Unknown 192.168.22.10	7							
	NETWORK					008					
	Description	Status				Description	Status				~

Ciscolive,

### Connection Score – What does it show?

			CONNECTION SCORE
AP MAX CONFIGURED	Connection Score		% value based on the Client Actual Rate divided by either the Client Max Capability or Max AP Configured
CLIENT MAX CAPABILITY			(whichever is lower).
CLIENT ACTUAL RATE	Connection Rates	4000/	
The current data rate of the client (reported by the AP).	AP Max Configured 217 Mbps	100%	
SPATIAL STREAMS	Client Max Capbility 144 Mbps	Connection Score	
The number of spatial streams supported by the AP radio and advertised by the client.	Client Actual Rate 144 Mbps		
	Spatial Streams 🛛 🕑		
CHANNEL WIDTH	AP Max Configured 3		
The number of spatial streams supported by the AP radio and advertised by the client.	Client Max Capability 2		
	Channel Width 🛛 🕑		
	AP Max Configured 20 MHz		
	Client Max Capability 20 MHz		
		Close	



## Client Troubleshooting – Where do I find it?

### Monitoring Network Summary Access Points

Wireless Dashboard AP Performance

Client Performance

### P Best Practices

Performa	nce		Signal Str Speed: 14	ength: - <mark>55 dB</mark> 4 Mbps Chan	m Signal Quality: 32 Inel Width: 20 MHz	dB Connection
Capabiliti	es		802.11n (2	2.4GHz) (CC)	(v5) Spatial Stream:	2
Connectio	on Score		100%			
MOBILI	ΤY					
W (L	IC .OCAL)	Wired A (CAPWAP) (	(P Local)	Wireless (802.11n (2.4G	Client H(2)(LAN22)	
	<b>1</b>	0			-	
A 11	IR-CT2504-K9 92.168.20.20.	.::/128 1	2700-AP3 92.168.21.109		Unknown 192.168.22.107	

Linksys-Device

5	binary-over-http	7.5 KB	1.76%
6	📥 http	4.6 KB	1.07%
7	⇔ ms-sms	4.0 KB	0.94%
8	↔ netbios-ns	2.4 KB	0.56%

### NETWORK

Device Type

Description	Status
IP Address	192.168.22.107
IPv6 Address	Unknown
VLAN	22
Mobility Role	Local

Description	Status	
WMM	Supported	
U-APSD	Disabled	
QoS Level	Silver	

### SECURITY & POLICY

Description	Status	
Policy	RSN (WPA2)	
Cipher	CCMP (AES)	
Key Management	PSK	
EAP Type	N/A	
ACL (IP/IPv6)	None/None	
mDNS Profile	default-mdns-profile	
AAA Role	None	

CLIENT TEST			
PING TEST	CONNECTION TEST	PACKET CAPTURE	EVENT LOG
Start			
4000ms			
2000ms			
0ms			

### Ciscoll

# Client Troubleshooting – Connection Test

DHC

- A helpdesk level tool for que
   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

ROLS							
ASSOCIATION STATE	TRAFFIC LIGHT IND	CATCHENT TEST			-		
Neme ( SCID IONAL DETAILS	te		PING TEST	CONNECTION			
n the section header to expa	and the pane to	Start Stop					
signed VLAN / Interface ADDRESSING STATE		802.11 Association	•				
CP Proxy VED DHCP OPTIONS		AP Name : C3700-AP SSID : TMELABS-PSK STA Type : NEW	AP Name : C3700-AP SSID : TMELABS-PSK STA Type : NEW				
iault Gateway main Name		Association Request : Rece Association Response : Sen Association Status : Assoc	ived 1t Success				
me Server IP Address(es)		Security Policy RSN-I	PSK				
mic		Network Membership	•				
		IP Addressing	•				
minutes		IPv4 Additional Optio	ns 🔴				

# Client Troubleshooting – Packet Capture



# Your poll will show here



Install the app from <u>pollev.com/app</u> 2

Make sure you are in Slide Show mode

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



Cisco((VC)

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Wireless Service Assurance Client, Network, Application Insights On Cloud

Cisco
#### Assuring Client Experience

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

Ciscolive!

### Your poll will show here



Install the app from <u>pollev.com/app</u> 2

Make sure you are in Slide Show mode

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



Cisco((VC)

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

### Your poll will show here



Install the app from <u>pollev.com/app</u> 2

Make sure you are in Slide Show mode

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



Cisco((VC)

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

#### Vision of Network Assurance



#### 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



letwork Health Historically

- Analyze and troubleshoot
   historical events
- Retrospect and Reporting\*



# Wireless Service Assurance Architecture



#### **Best Practices Recommendations**



**INFRASTRUCTURE** 

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

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

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

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

ECURITY

S

# Key Takeaways



Ciscolive

### 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 <u>CiscoLive.com/us</u>.



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 14<sup>th</sup>, 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



#### ıılıılıı cısco

