Cisco Expo 2008

Voice over WLAN

Design and Deployment - Piotr Chomczyk

What are we talking about today…

1. Introduction
   - Trends & drivers
2. VoWLAN – what do we need
   - RF Design
   - QoS over the air
   - Roaming
   - Security
3. VoWLAN – what do we have
   - WLC & WCS – tools and recomendations
   - Cisco 7921G / 7925G

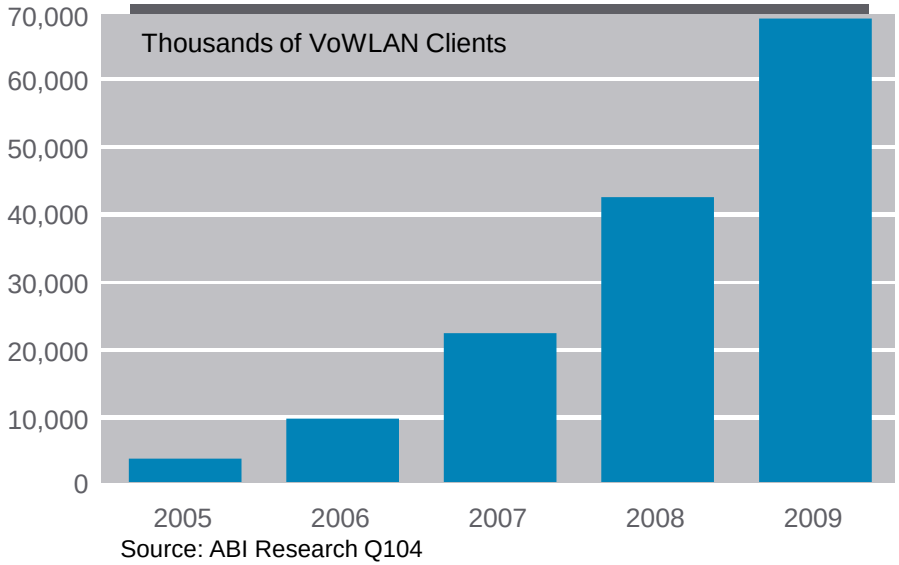
What are we NOT talking about today…

1. RF / 802.11 / Security – basics
2. Cisco Unified Wireless Architecture
3. CCX
4. Underlying „wired” campus infrastructure

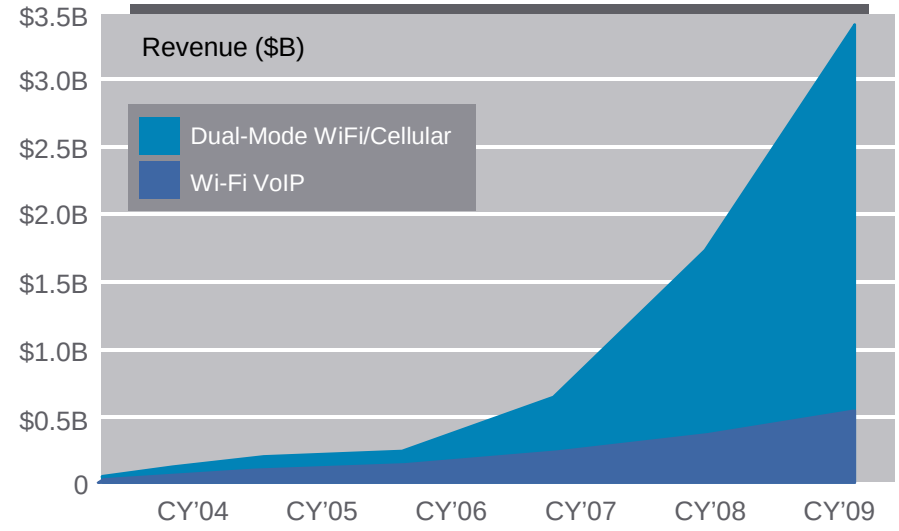
Voice over WLAN

Introduction

Voice over WLAN Drivers



Source: ABI Research Q104



Source: Infonetics Research (July 2005)

1. Mobile Workers, Virtual Teams
2. WLANs: Data → Voice
3. Cellular: Voice → Data
4. Converged Wi-Fi/Cellular Handset
5. Interoperable Standards
6. Advanced voice features
7. Affordability
8. Single number reach

Voice over WLAN

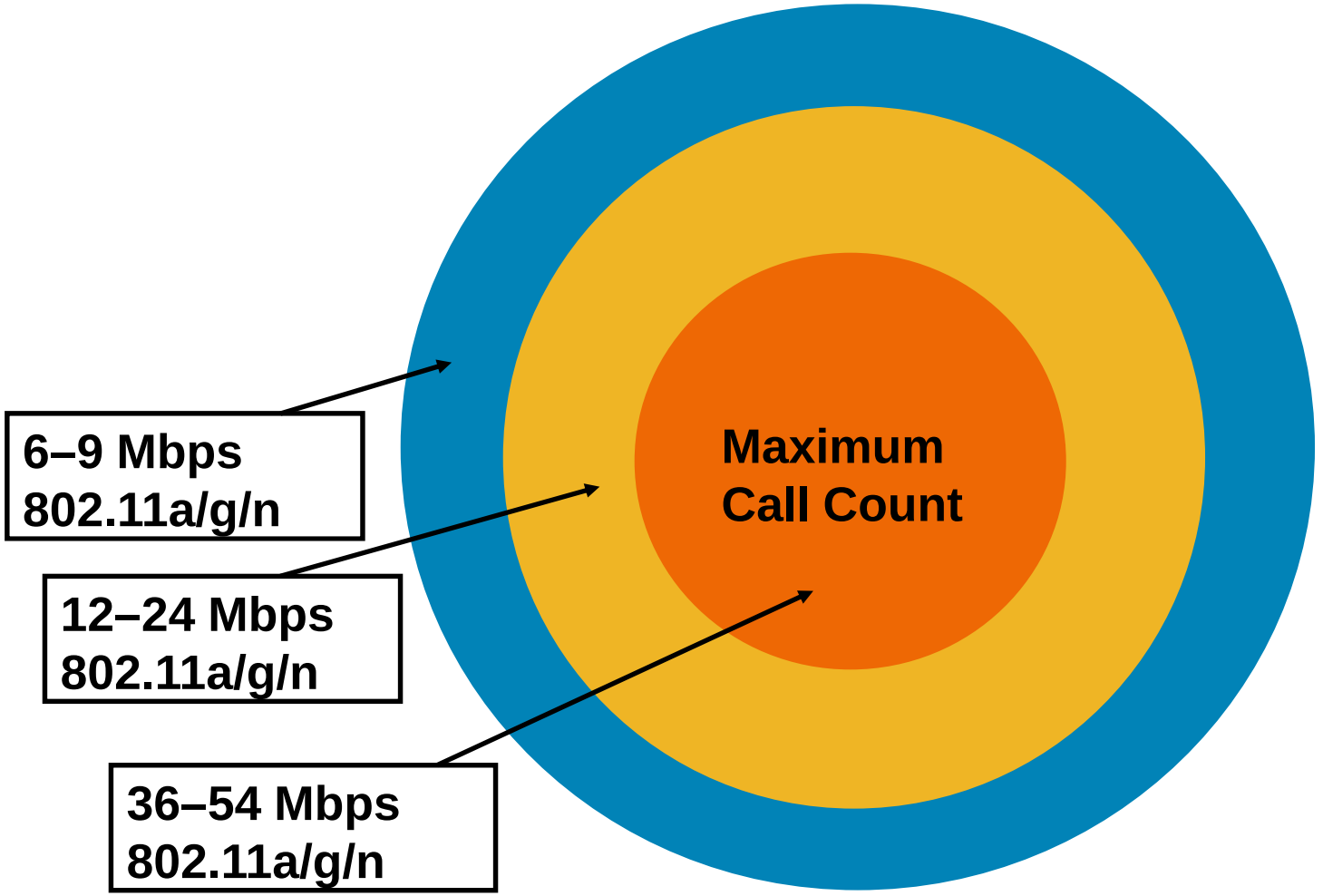
RF Design

WLAN Coverage Considerations

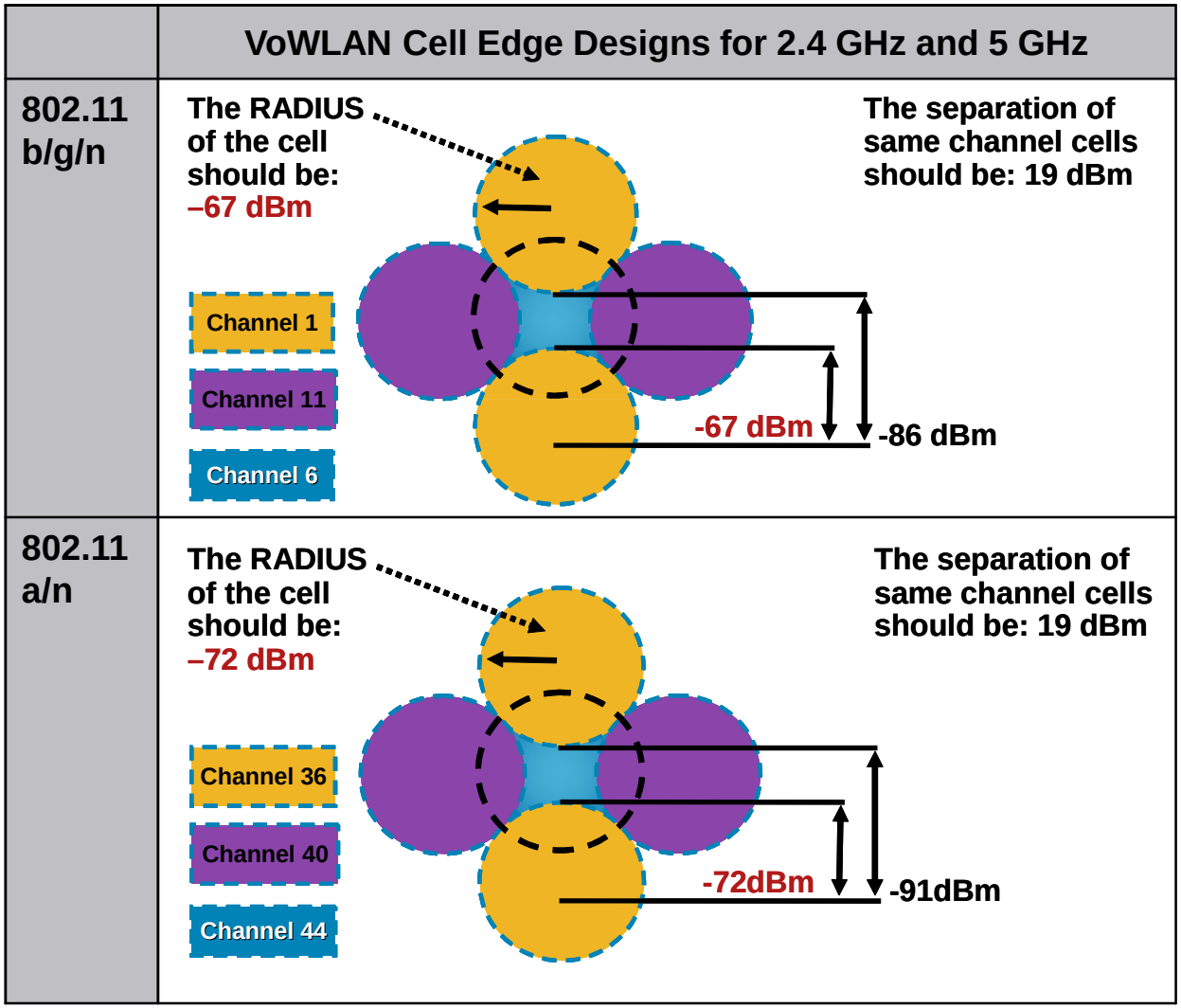
1. The AP coverage design needs to be done to match the performance of the clients and the applications they run
2. Determine the RF coverage of all the clients that are going to be used in the WLAN
   - Use data sheets to find the clients antenna gain
   - Use data sheets to find data rates and receiver sensitivity
   - Use data sheets to find channels and transmit powers
3. Determine what other applications and clients share the WLAN
4. Determine what interferers share the WLAN

Data Rate: Cell Size

Call Count Comparisons



Ideal Cell Size and Channel Separation



Capacity

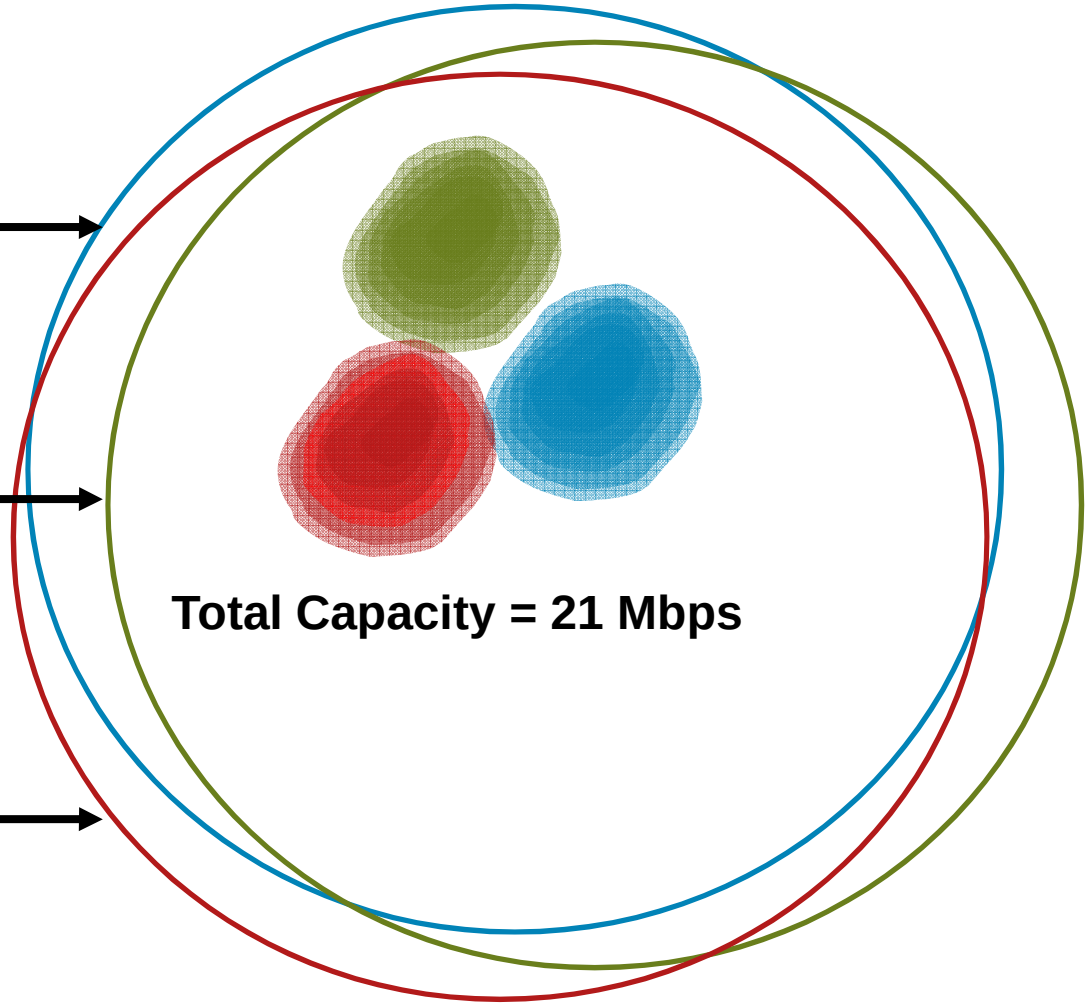
1. Capacity is throughput multiplied by available, non-overlapping channels
   - 802.11b and 802.11g operate in the same band, use the same three channels
     - Any 802.11g capacity increase is from throughput alone
2. 802.11a currently provides 12 channels in much of the world today, 23 channels in most of the world in 2005
   - While throughput might be similar to 802.11g, channels are not, neither then is capacity
3. In theory, access points set to non-overlapping channels may be co-located to provide all available capacity in a single coverage area
   - More commonly, it's an expression of total throughput across a network or facility

802.11b Scalability

Blue = 11 Mbps Data Rate, 7 Mbps Throughput

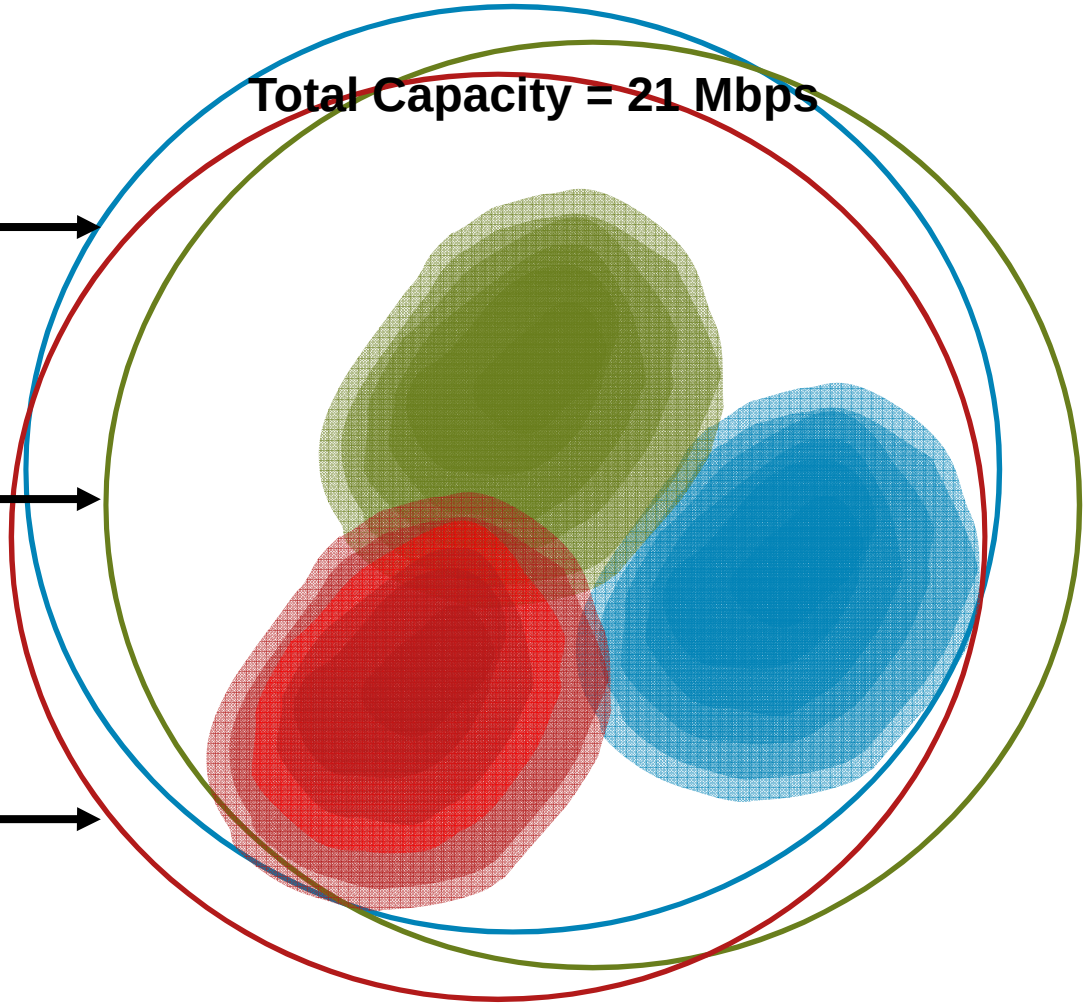
Green = 11 Mbps Data Rate, 7 Mbps Throughput

Red = 11 Mbps Data Rate, 7 Mbps Throughput



What If We Added Three More APs to This Coverage Area?

802.11b Scalability



Blue = 11 Mbps Data Rate, 7 Mbps Throughput

Green = 11 Mbps Data Rate, 7 Mbps Throughput

Red = 11 Mbps Data Rate, 7 Mbps Throughput

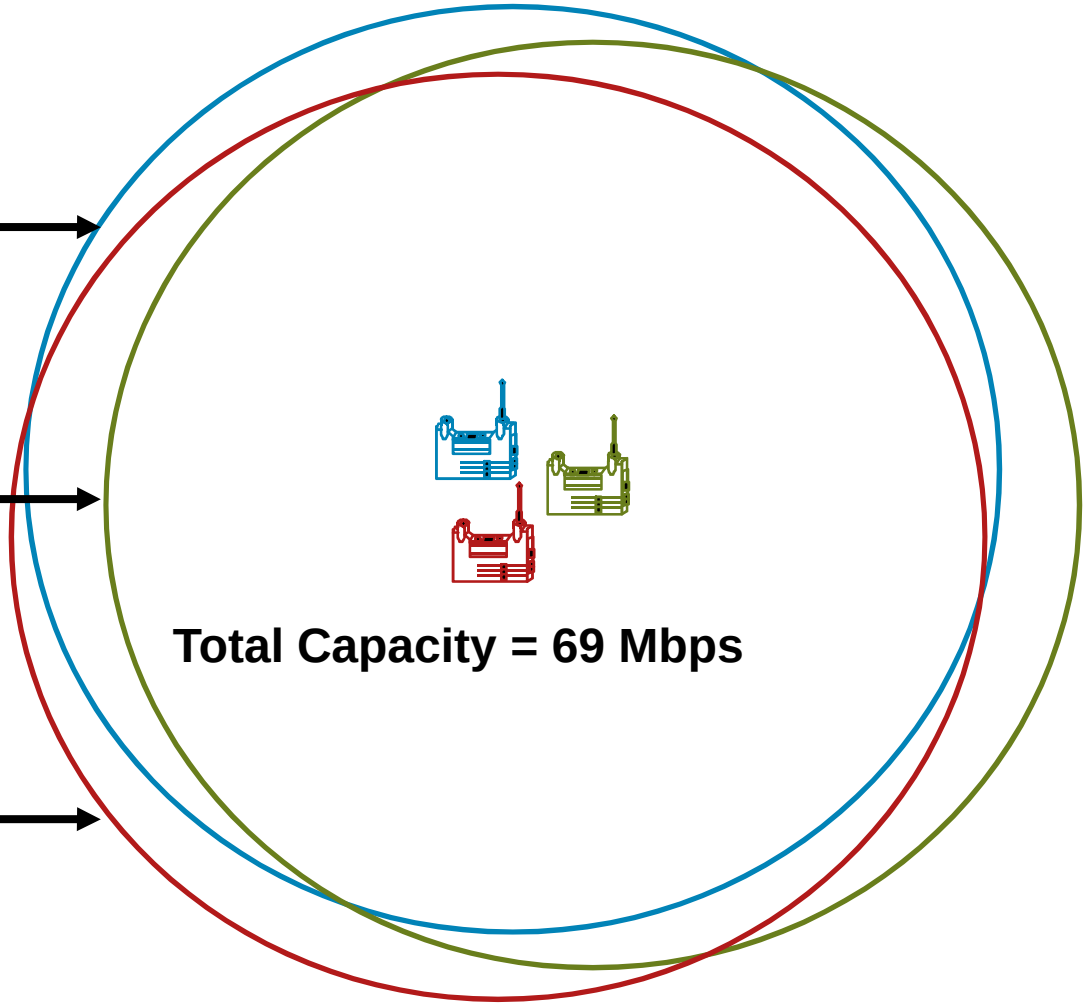
What If We Added Three More APs to This Coverage Area?

802.11g Scalability

Blue = 54 Mbps
Data Rate, 23 Mbps
Throughput

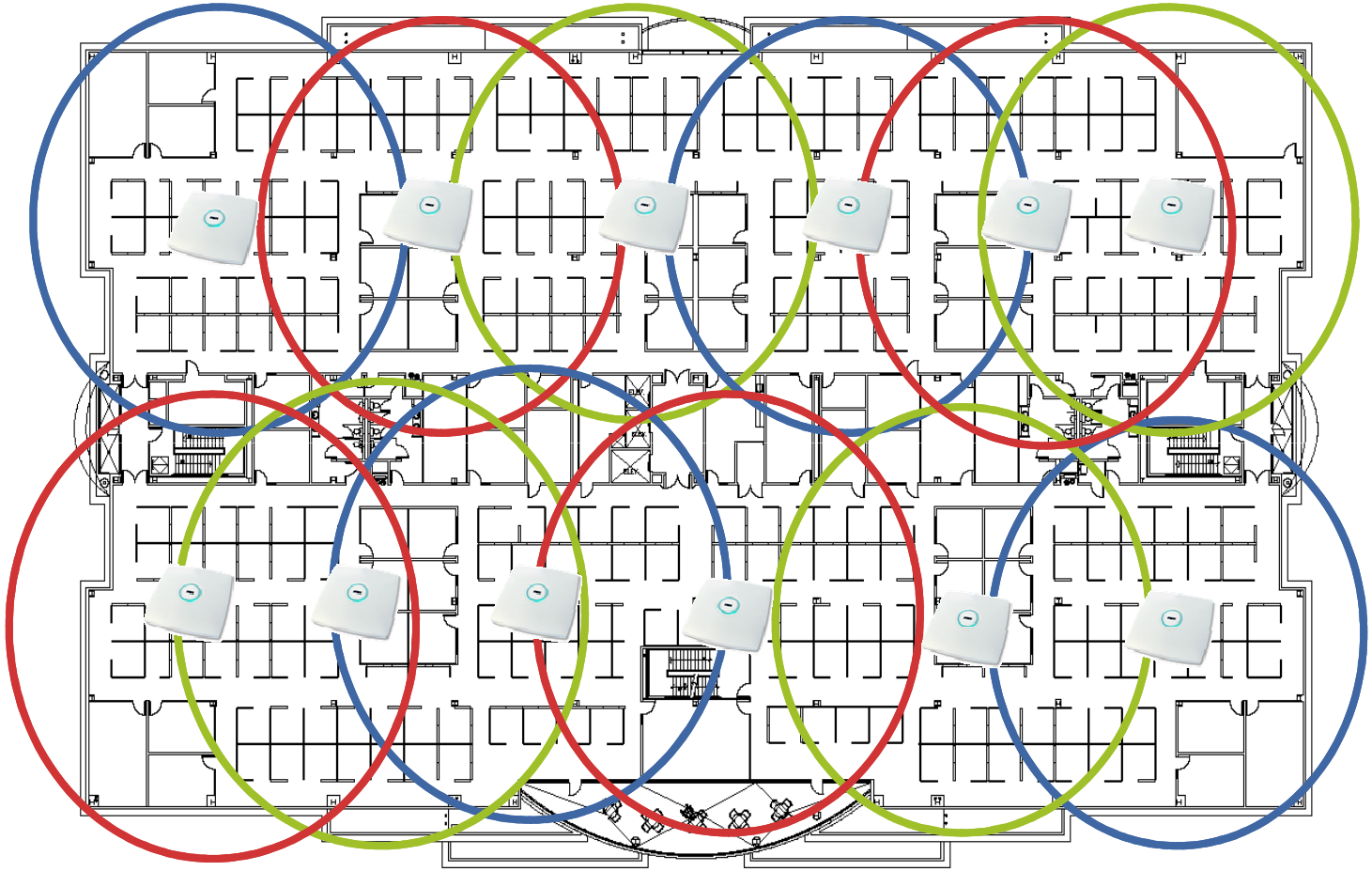
Green = 54 Mbps
Data Rate, 23 Mbps
Throughput

Red = 54 Mbps
Data Rate, 23 Mbps
Throughput



High Density Cells

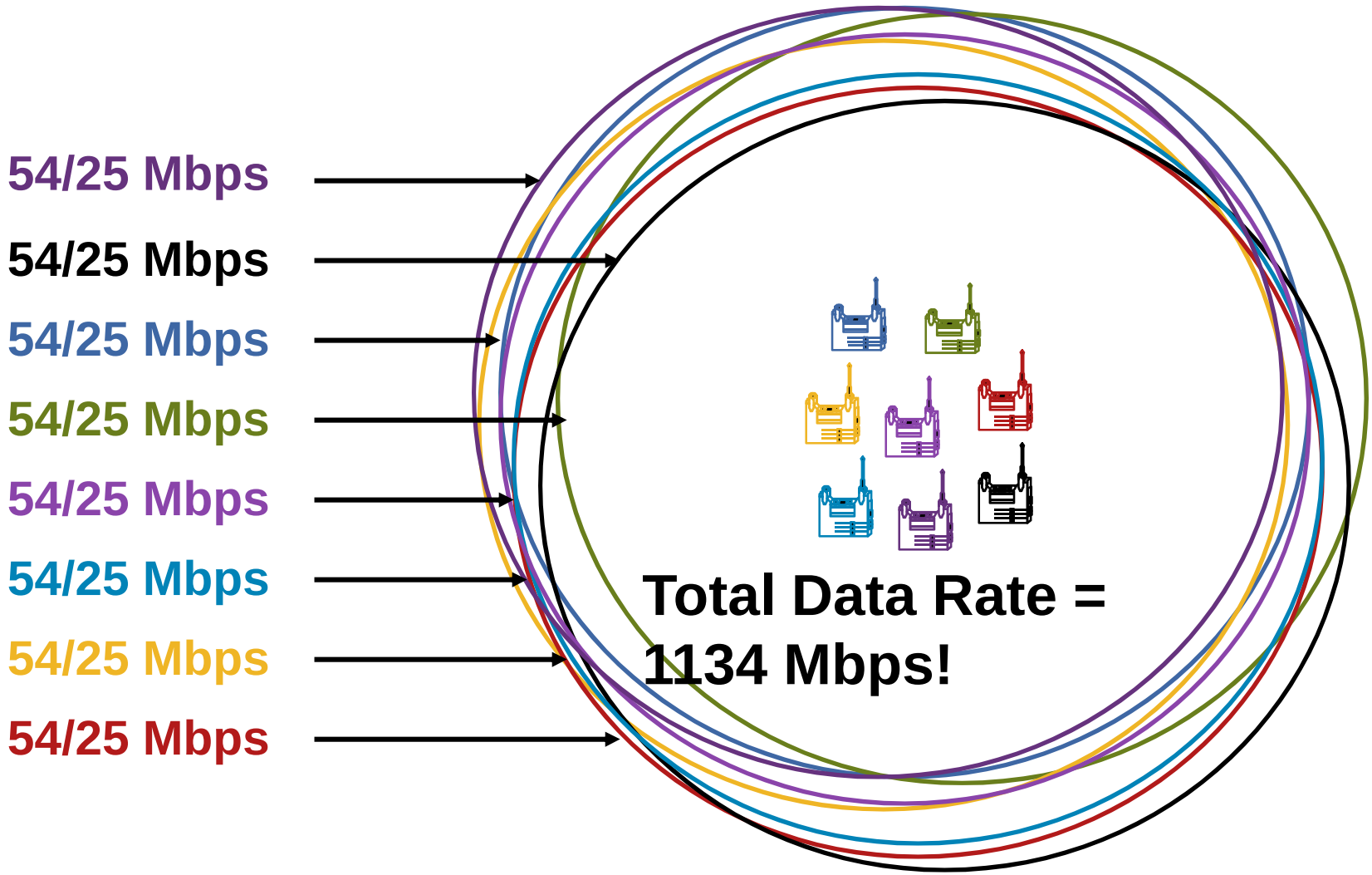
Higher Number of Available Calls in a Given Office Space



In a Floor Space This Small with This Many 2.4 GHz APs Data Rates and Transmit Powers Would Have to Be Managed to Achieve > 20 802.11b Calls per Channel

802.11a Scalability:

ETSI – up to 19 Channels

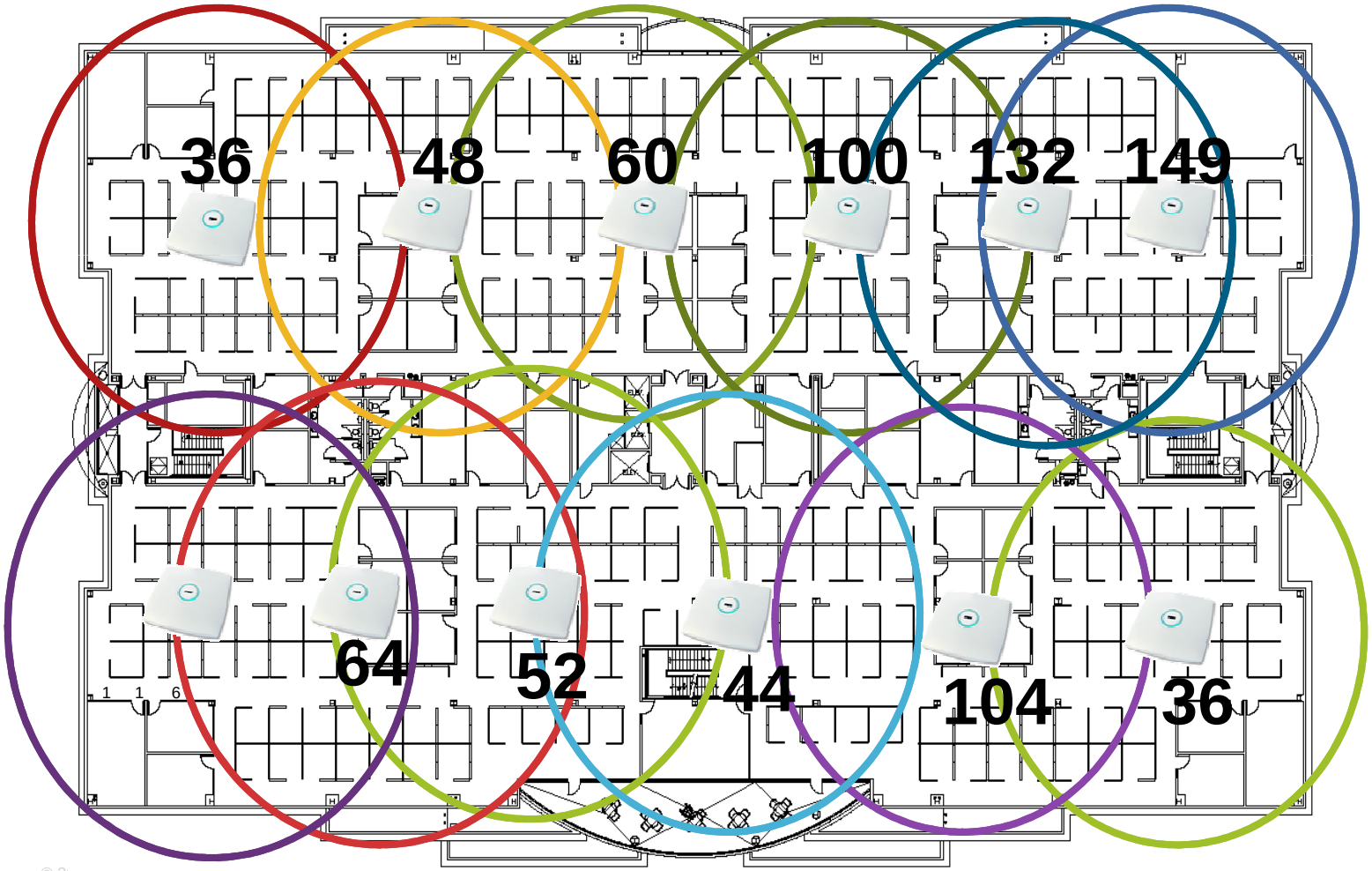


What about 11n? Nine Bonded Channels

High Density Deployment

High Density 5 GHz Office Deployment

1. 5 GHz does not have the overlap or collision domain issues of 2.4 GHz; 12 APs on one floor



Aggregate and Per-User Throughput

1. 802.11, like Ethernet, is a shared medium
2. Aggregate throughput is the total bandwidth shared by all users in a cell
3. Generally, the larger the cell, the more users in the cell
   - Greater per user throughput means smaller cells and more access points for a given area
4. How many users per access point?
   - What's the aggregate throughput of the access point?
   - On average, what amount of per user throughput do you want to provide?

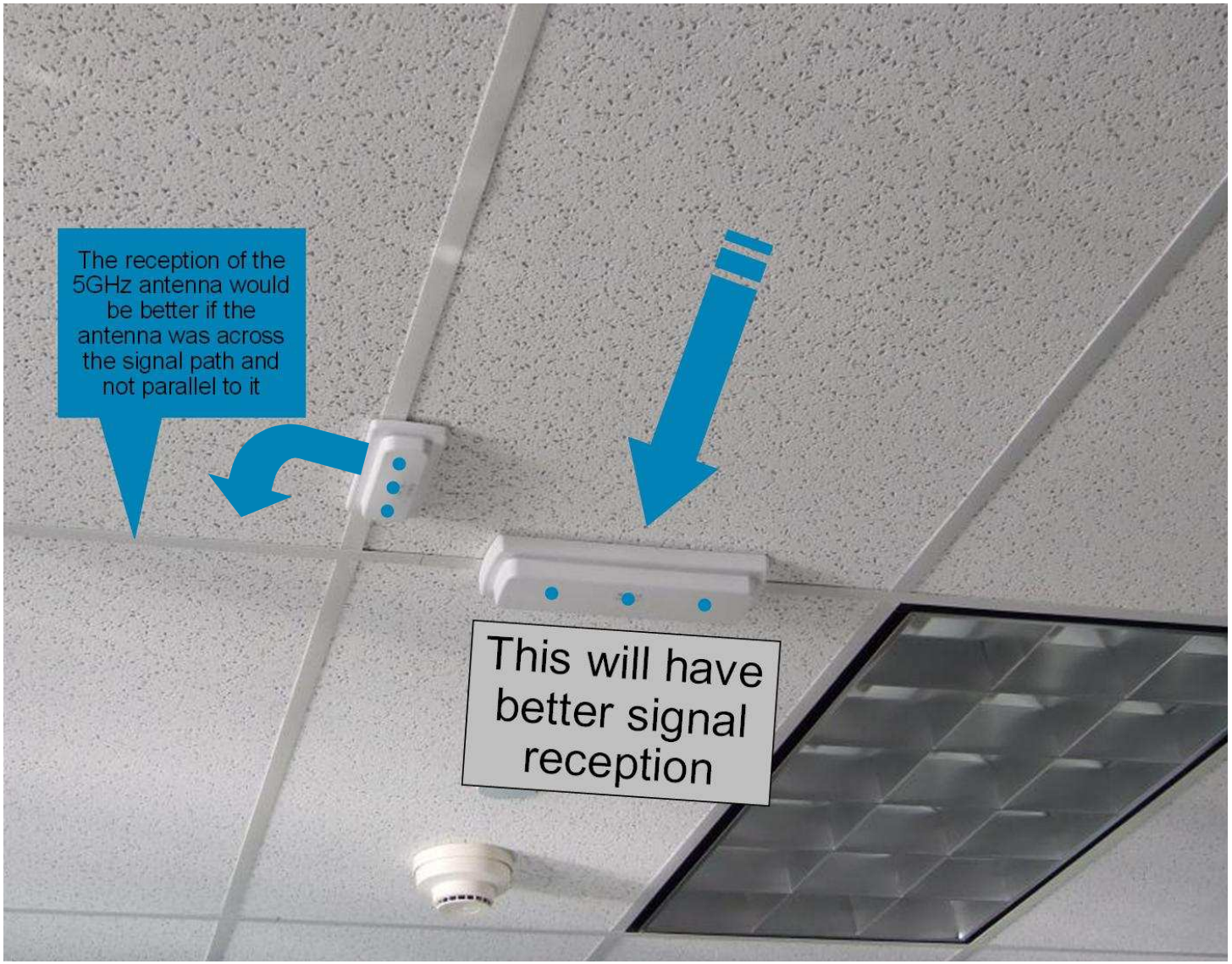
Per-User Throughput Samples

Technology	Data Rate (Mbps)	Aggregate Throughput (Mbps)	Example User Count	Average per User Throughput
802.11b	11	6	10	600 Kbps
802.11b	11	6	20	300 Kbps
802.11b	11	6	30	200 Kbps
802.11g	54	14	10	1.4 Mbps
802.11g	54	14	20	700 Kbps
802.11g	54	14	30	467 Kbps
802.11a	54	25	10	2.5 Mbps
802.11a	54	25	20	1.25 Mbps
802.11a	54	25	30	833 Kbps

Recommendations

1. Only with 5GHz can the number of APs start to align with the WLAN capacity –for voice and data.
   - The more non-overlapping channels the better
2. 2.4GHz APs may only add coverage not capacity –in many deployments
3. Ovoid supporting lower bit rates than needed by the -67dBm boundary
   - This will increase capacity, and reduce co-channel interference
4. There is a critical mass of a/b/g adaptors new deployments should be planned and designed around the 5GHz spectrum
   - Co-channel interference is the subprime mortgage of your WLAN
5. Place antennas the right way.

802.11n Antenna Placement



Voice over WLAN

Quality of Service

Quality of Service (QoS) Overview

1. Ensures packets receive the proper QoS handling end-to-end
2. Makes sure packet will maintain QoS information as it traverses network
3. Policing of 802.11e UP/802.1p and IP DSCP values ensures end-points conform to network QoS policies
4. Uses Cisco's AVVID packet marking mappings and IEEE mappings as appropriate
5. Supported on all shipping controllers
6. Supported on Cisco Aironet® 1000, 1130, 1200, 1230, 1240, 1250 and 1500 Series lightweight access points
7. Support for Cisco 7920/7921 as well as many 3rd party voice products

Wi-Fi Multimedia (WMM)

1. What is WMM?

   It is a supplement to 802.11 MAC layer

   Allows Diff-Serv QoS by creating four priority queues, called Access Categories

   The access categories access the channel using a protocol called EDCA (Enhanced Distributed Channel Access), an enhancement of the existing DCF (Distributed Coordination Function)

2. What does WMM add?

   Uplink frames are marked with 802.1d CoS

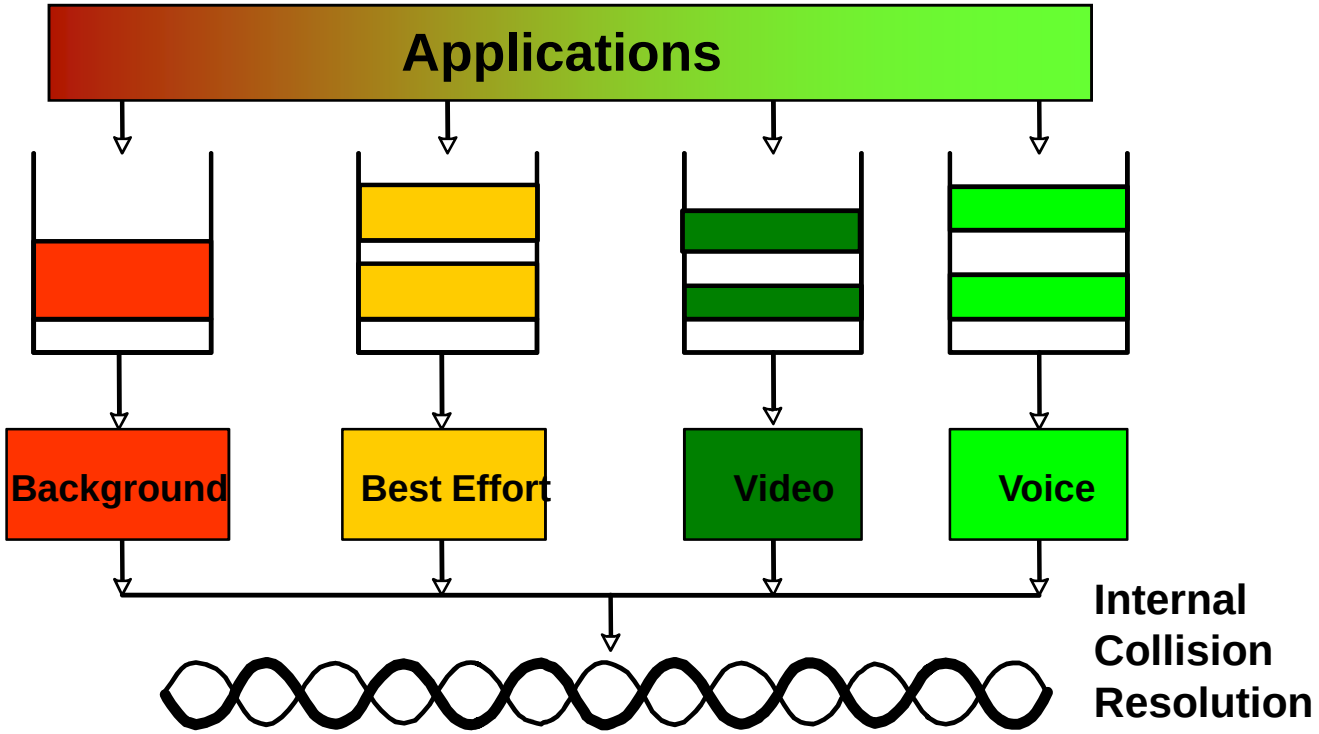
   Prioritized access for uplink traffic

   Admission Control Mandatory (ACM) flag allows uplink access categories to be enabled/disabled

   Contention-free packet bursting within the TXOP Limit (Transmission Control: Transmission Opportunity)

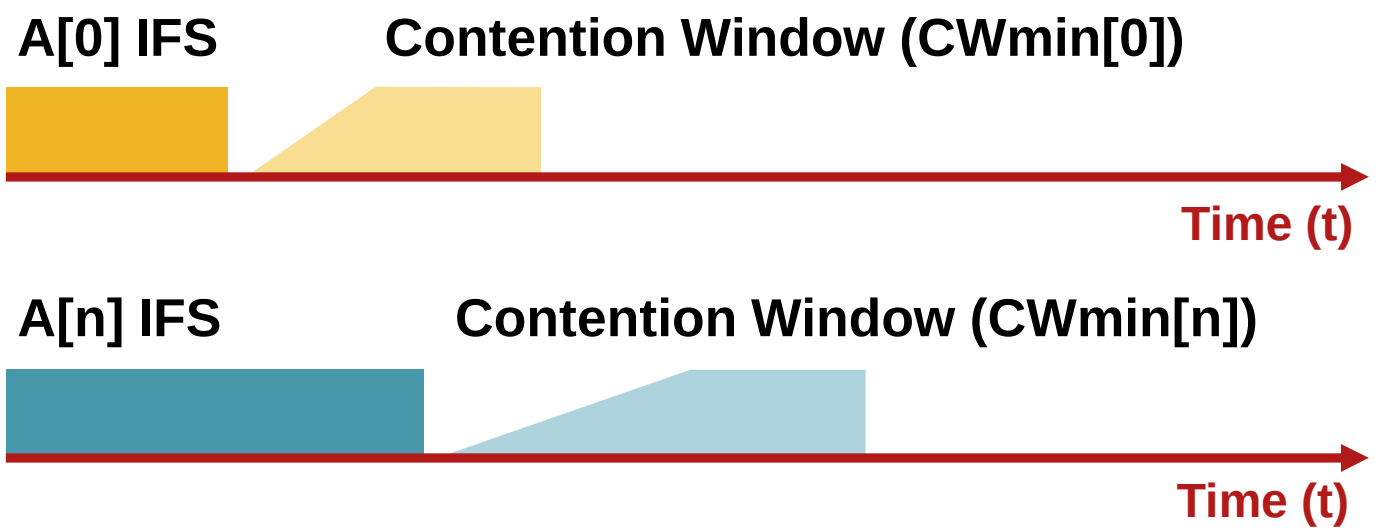
Classification

1. WMM Access separates traffic types in to 4 categories
2. Background, Best Effort, Video, Voice
3. These all compete for the channel with different delay and random back off characteristics



IEEE 802.11e — EDCA

Enhanced Distributed Channel Access



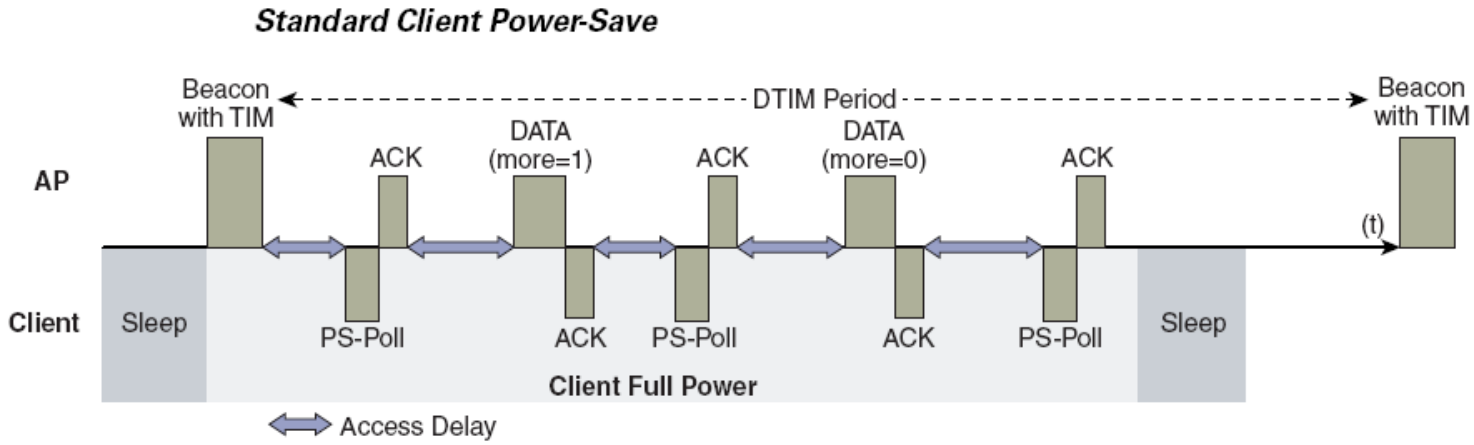
1. Superset of DCF
2. EDCA allows high priority traffic first access to the media, by altering the IFS, and the random back-off

   Transmission Operation (TXOP) is given to the lowest QoS Station (QSTA)
3. QSTAs with the same Access Category (AC) have the same back-off time

IEEE 802.11e WMM Access Categories

Access Category	Description	802.1d Tags
WMM Voice Priority	Highest Priority (Multiple Calls, Low Latency and Toll Voice Quality)	7, 6
WMM Video Priority	Traffic Other Than Data	5, 4
WMM Best Effort Priority	Legacy Devices or Applications That Lack QoS Capabilities	0, 3
WMM Background Priority	Low Priority Traffic (File Transfers, Printing)	2, 1

U-APSD

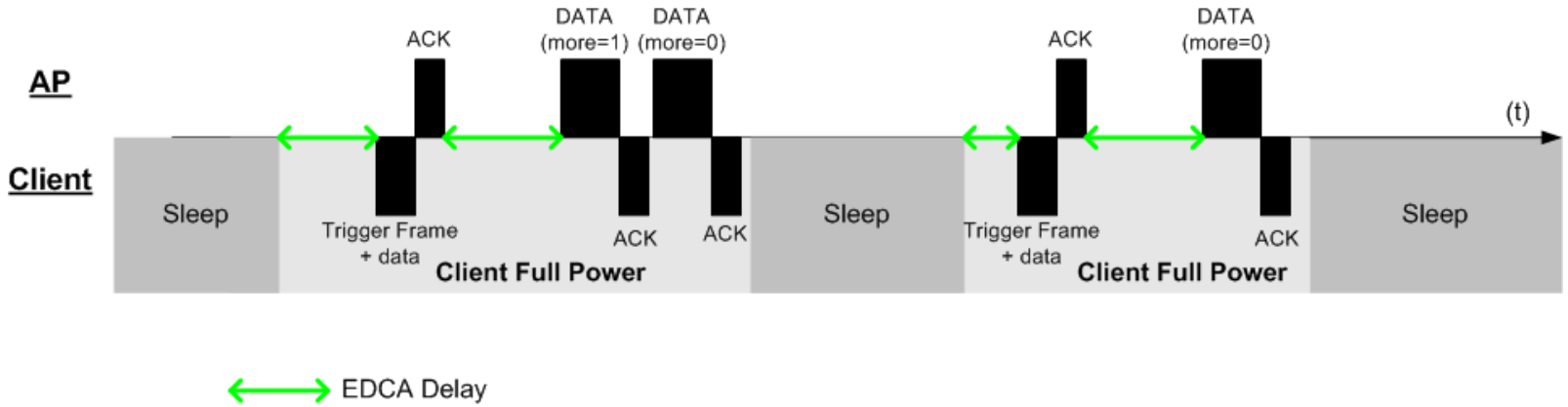


1. AKA WMM-Power Save

   Client receives buffered frames when it transmits, rather than polling for buffered frames

2. Increased Power Saving

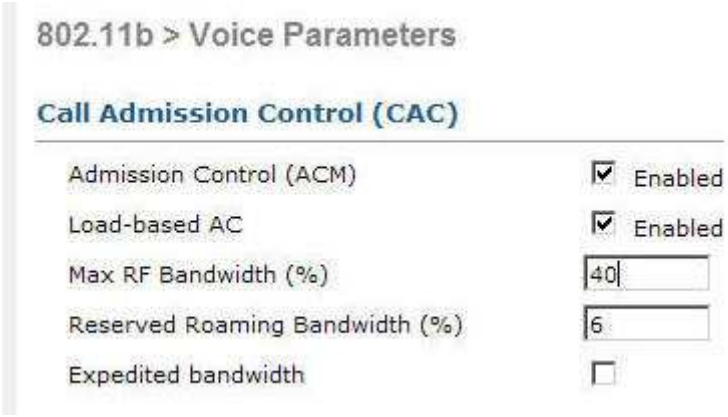
3. Increased Call capacity



WMM Performance Features

	WMM	WMM w/ Unscheduled Power-Save Delivery (UPSD) and Traffic Specification (TSPEC)
Packet Prioritization	Yes	Yes
Timed Delivery	No	Yes
Admission Control	No	Yes
Battery Life and Call Capacity	Good	Better

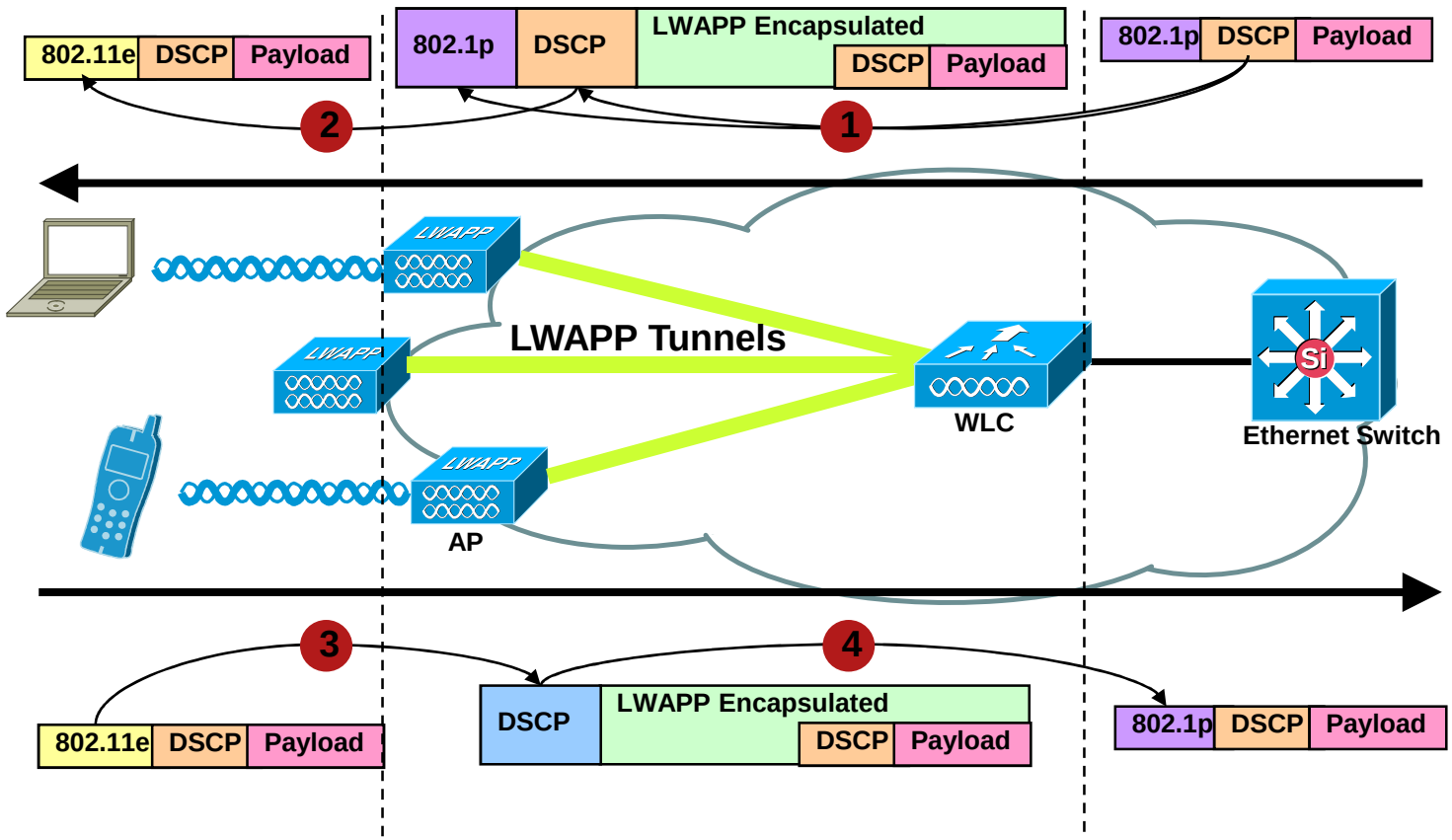
TSpec CAC



1. Load-based AC should be enabled
2. Default Maximum RF bandwidth will be too high in many cases
3. 40% is most likely to be more appropriate

   The percentages consumed depends on the client bit rates

LWAPP QoS



1. Ensures that packets receive the proper QoS handling from end to end
2. Policing of 802.11e UP / 802.1p and IP DSCP values ensures that wireless endpoints conform to network QoS policies

Voice over WLAN

Roaming

Why Client Stations Roam

1. Common reasons for roam -
   - Maximum data retry count exceeded
   - Low receive signal strength (RSSI)
   - Low Signal to Noise Ratio (SNR)
   - Proprietary load balancing scheme

Choosing a new AP to roam to

Channel Scanning

1. Active Scan - Probe each channel
2. Passive Scan - listen on each channel

3. Background scanning - build up roam information proactively
4. On-roam scanning - Scan each channel when roam required

Evaluating potential roam destinations

Evaluate the following attributes to choose an AP to roam to;

1. Receive Signal Strength Indicator RSSI
2. Signal to Noise Ration SNR
3. Number of clients on the AP
4. Transmit and receive bandwidth being used by the AP
5. RF channel load information from Beacon and probe-responses
6. others...

Cisco Compatible Client Extensions

Roam Parameter Enhancements

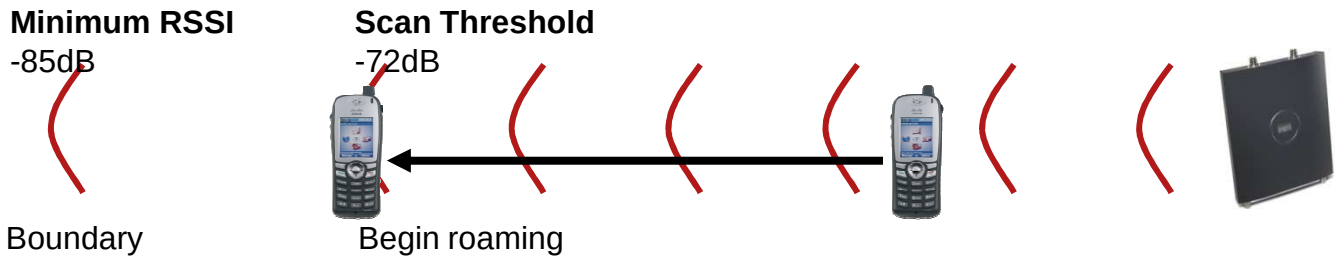
1. Parameters defined on controller that Influence roaming decisions for CCX clients

   Scan threshold (default -72DB) - the minimum RSSI value below which the client should attempt to roam

   Transition time (default -5 seconds) - the maximum time in which a roam must be completed

   Minimum RSSI field (default -85dB) - A value for the minimum received signal strength indicator (RSSI) required for the client to associate to, or stay associated with, an access point.

   Hysteresis (default -2dB) - A value to indicate how much greater the signal strength of a neighboring access point must be in order for the client to roam to it.



Cisco Compatible Extensions

Channel Scanning Enhancements

1. Access point assisted roaming
2. Enhanced neighbor list
3. Enhanced neighbor list request (E2E)
4. Directed roam request

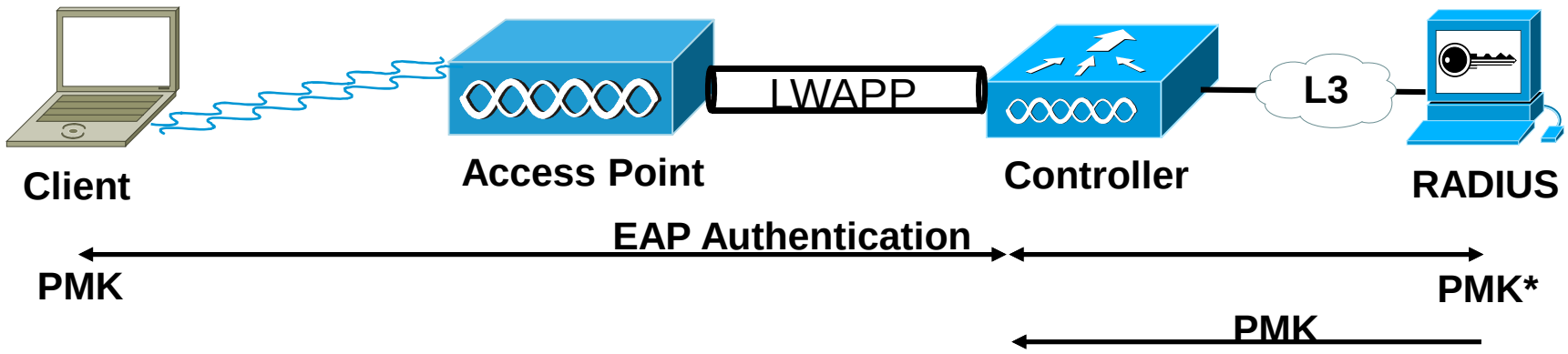
Re-authenticating to the new AP

Authentication Types

1. **Open Authentication** - This is null authentication - any client is permitted to access the WLAN
2. **WEP Shared Key (WEP)** - Static WEP requires sender and receiver to have the same pre-provisioned key in order to decode messages from each other
3. **WPA-Personal and WPA2-Personal** - A shared key, which is not the encryption key, is configured on both the WLAN and the WLAN client, and this key is used in the WPA 4-way handshake to generation and per session encryption key
4. **802.1X/EAP Authentication** - used in Wi-Fi Protected Access (WPA-Enterprise) or WPA2-Enterprise

Fast Secure Roaming – CCKM

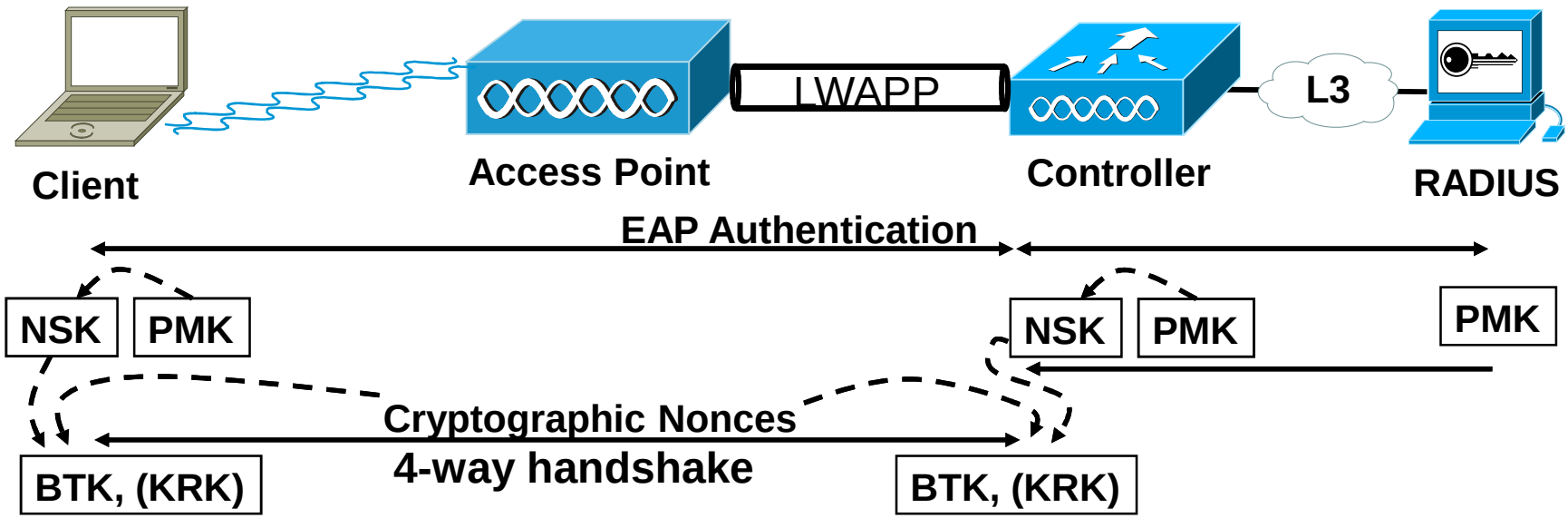
Initial Authentication (1 of 4)



1. The Network Session Key (NSK) is derived after EAP authentication, and is sent from the RADIUS server to the Controller

Fast Secure Roaming – CCKM

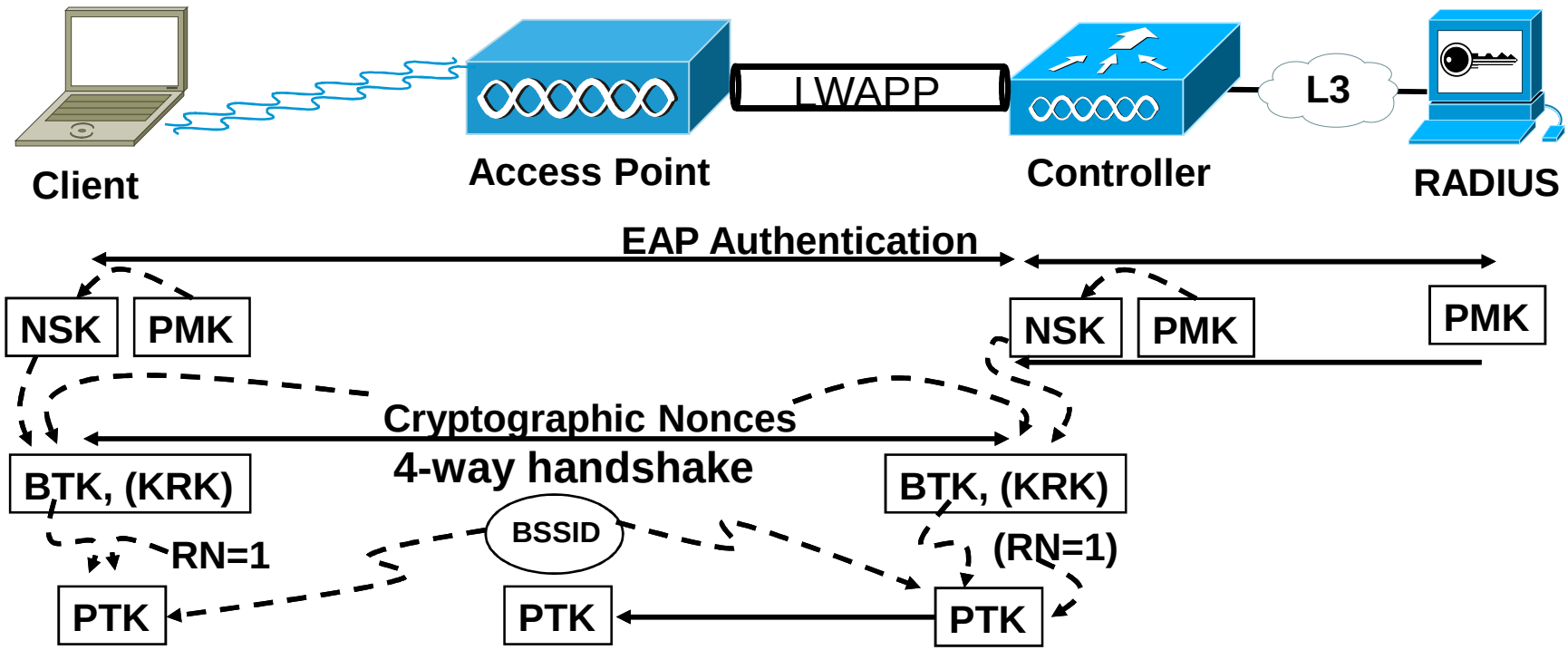
Initial Authentication (2 of 4)



1. The client and the Controller exchange nonces (random numbers), and combine the nonces with the NSK to create a Base Transient Key (BTK) and a Key Request Key (KRK)

Fast Secure Roaming – CCKM

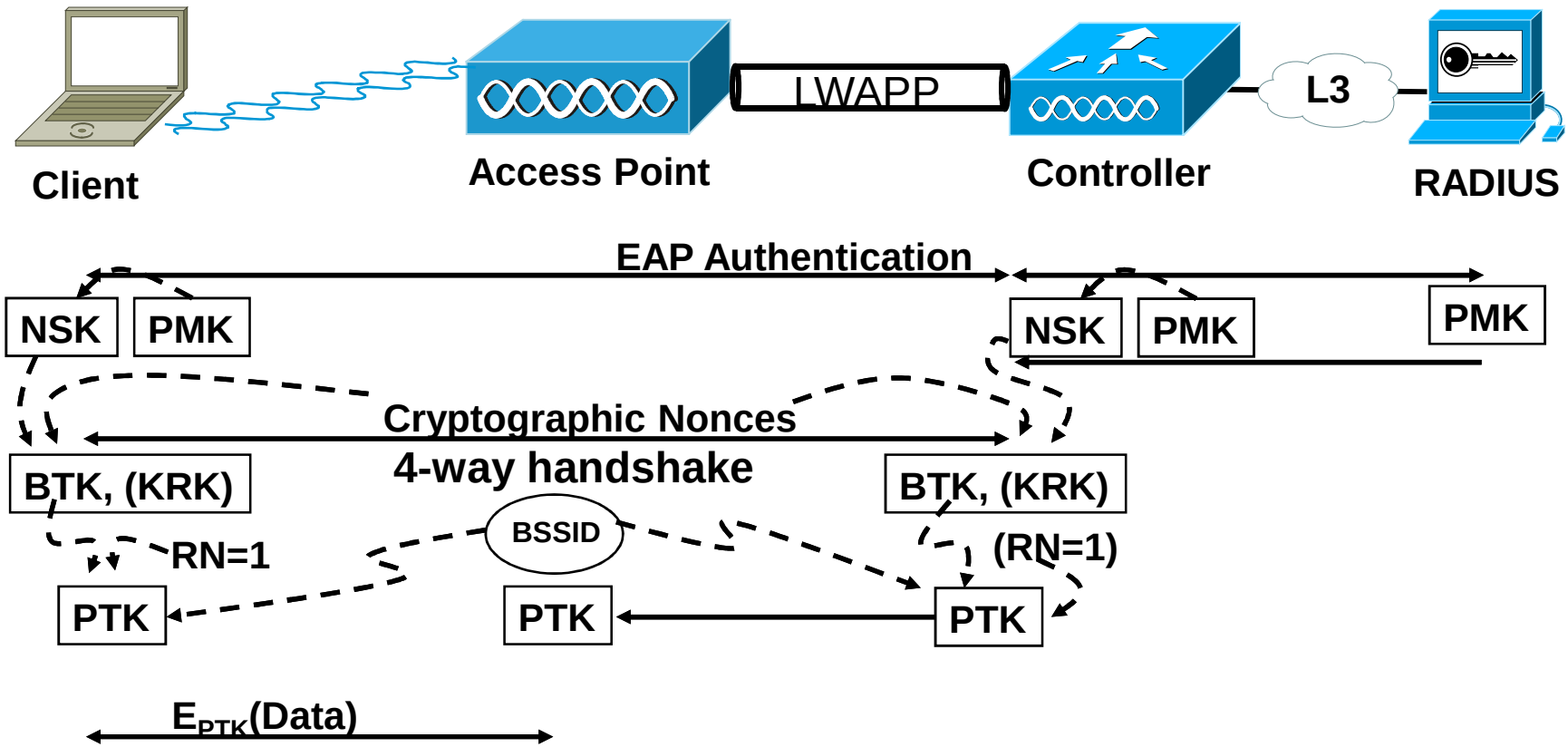
Initial Authentication (3 of 4)



1. Both the client and the Controller hash the BTK, RN, and BSSID to derive a Pairwise Transient Key (PTK). The controller then forwards the PTK to the AP over the LWAPP tunnel.

Fast Secure Roaming – CCKM

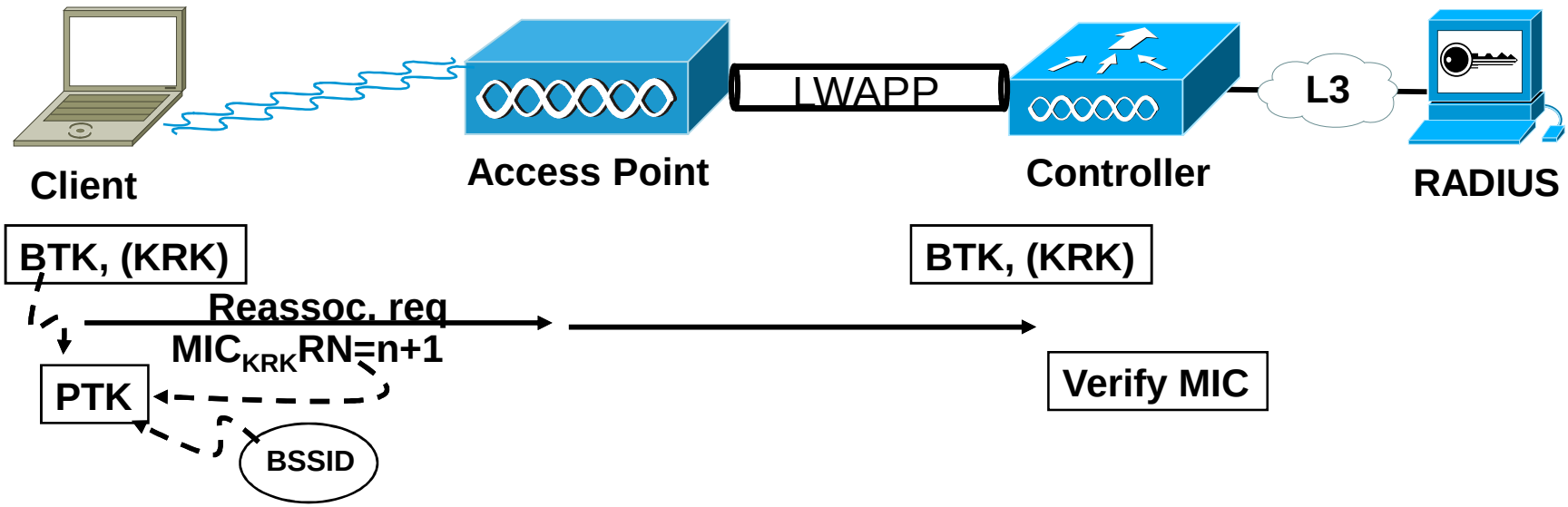
Initial Authentication (4 of 4)



1. The Client and AP communicate using the PTK

Fast Secure Roaming – CCKM

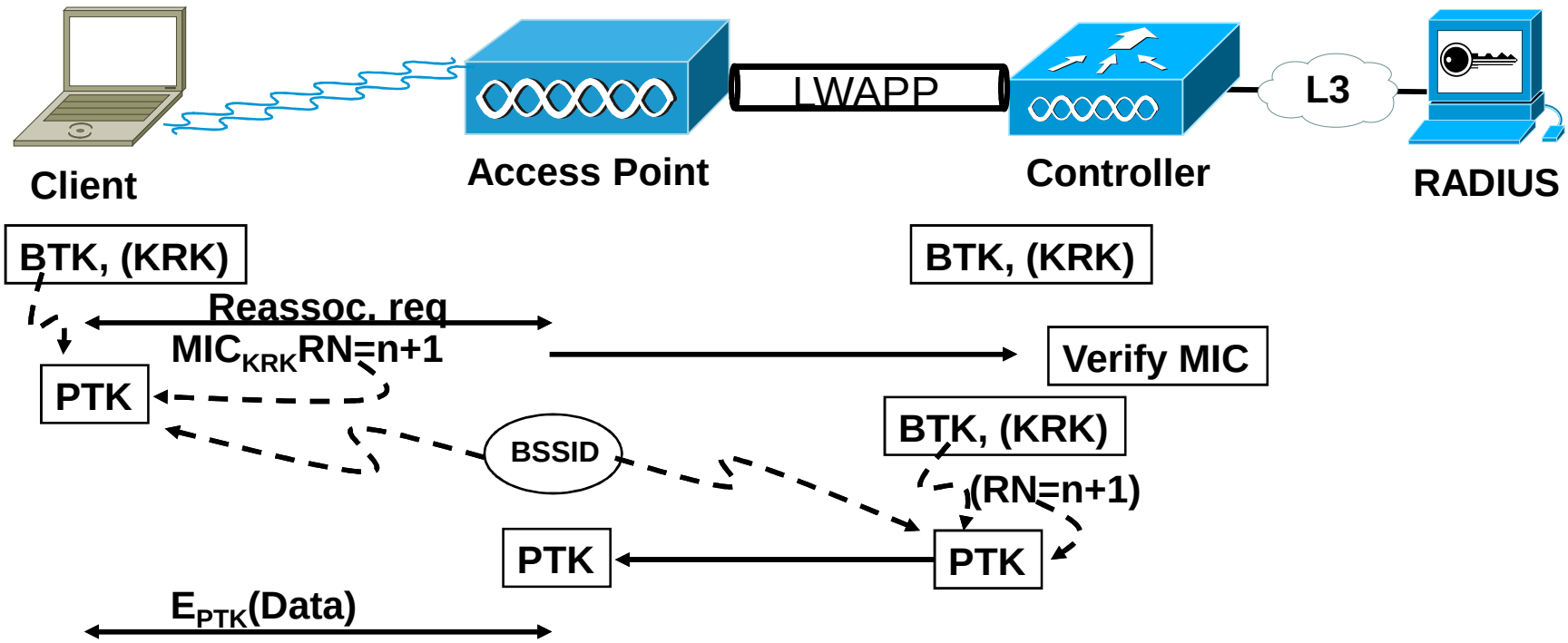
Roam (1 of 2)



1. The Client sends a reassociate-request with the next sequential rekey-number
2. The reassociate request is forwarded to the controller and the MIC is validated

Fast Secure Roaming – CCKM

Roam (2 of 2)



1. The controller calculates the next PTK, and forwards it to the AP
2. The Client and the AP can now communicate using the PTK

Fast Roaming with Proactive Key Caching (PKC)

1. WPA2 extension
2. PMK is cached in controllers
3. Client sends PMK-ID with association-request
4. Client and controller perform WPA 4-way handshake based on the PMK
5. A new, unique PTK is derived

Infrastructure impacts of client roaming

1. When a client originally associates, the controller creates an entry for each client in mobility database - noting what AP client is associated to
2. When client roams within same controller; update the entry to note the new AP
3. When client roams to a new controller mobility announcements between the controllers are used to build a tunnel for the client to/from the original controller

Voice over WLAN

Security

VoWLAN Security Recommendations

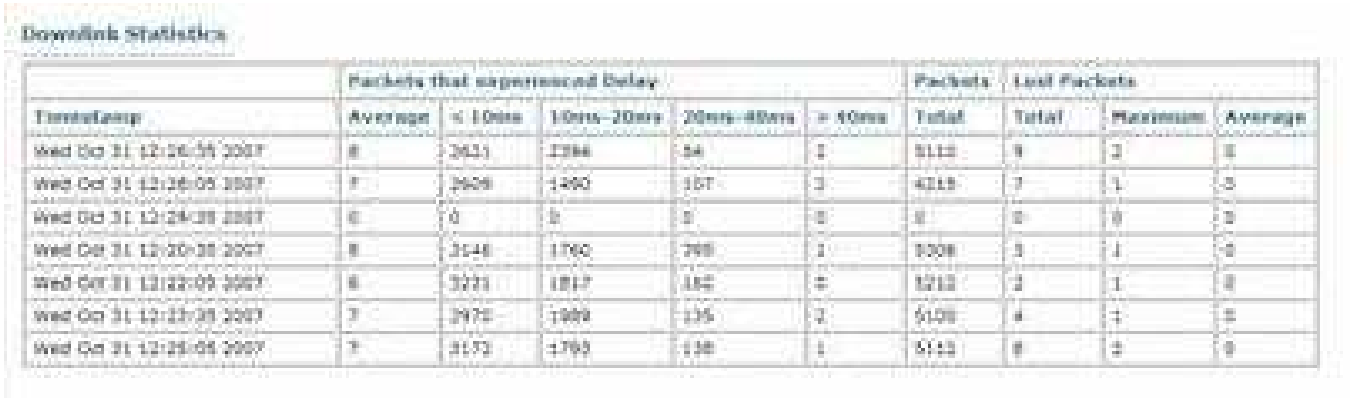
1. 802.1x/EAP Authentication is recommended
2. EAP-FAST is the recommended supplicant
3. WPA or WPA2 are recommended.
4. WEP is not recommended
5. LEAP can be used with a suitable strong password
6. WPA-PSK, and WPA2-PSK can also be used with suitable strong passwords

Voice over WLAN

WLC & WCS will help

WLC Tools (1)

1. The WLC provides many statistics to assist in generally troubleshooting
2. AP delay and Packet loss statistics are particularly useful when investigating VoWLAN call quality issues.
3. The WCS also provides historical and client reports on the same topic

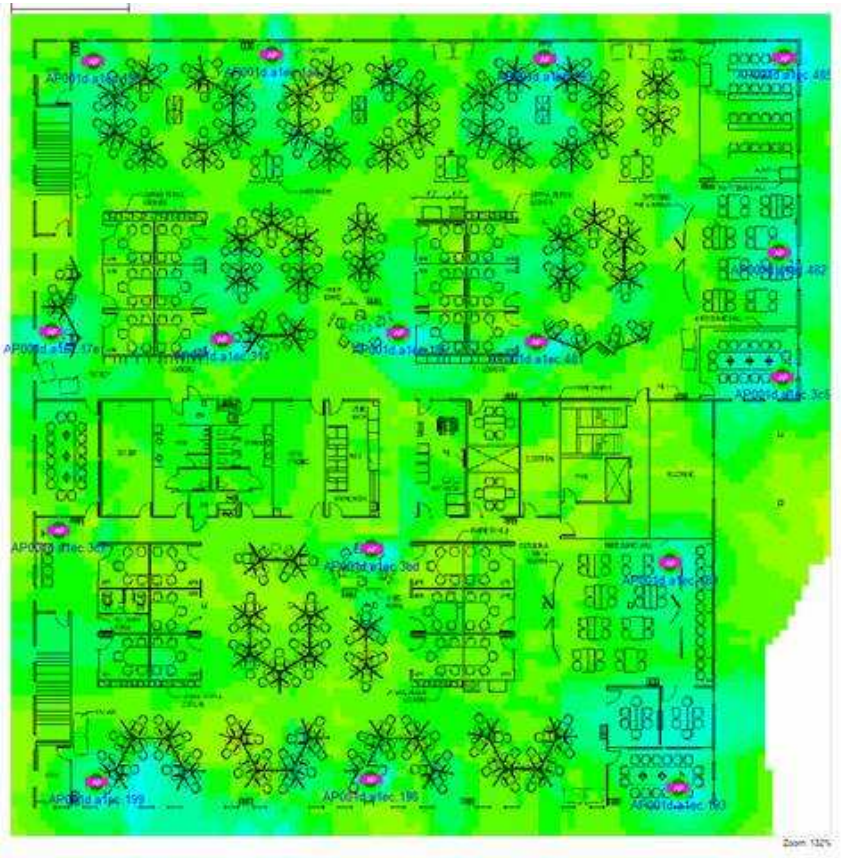

Downlink Statistics

	Packets that experienced Delay					Packets	Lost Packets		
TimeStamp	Average	< 10ms	10ms–20ms	20ms–40ms	> 40ms	Total	Total	Maximum	Average
Wed Oct 31 12:26:35 2007	8	3631	2284	84	2	6110	9	3	0
Wed Oct 31 12:26:05 2007	7	3609	1490	107	3	4219	7	1	0
Wed Oct 31 12:24:35 2007	0	0	0	0	0	0	0	0	0
Wed Oct 31 12:20:35 2007	8	3148	1700	288	2	5008	5	1	0
Wed Oct 31 12:22:05 2007	8	3221	1817	184	4	5213	2	1	0
Wed Oct 31 12:23:35 2007	7	3470	1989	135	2	5100	4	1	0
Wed Oct 31 12:25:05 2007	7	3172	1793	138	1	5143	6	3	0

WLC Tools (2)

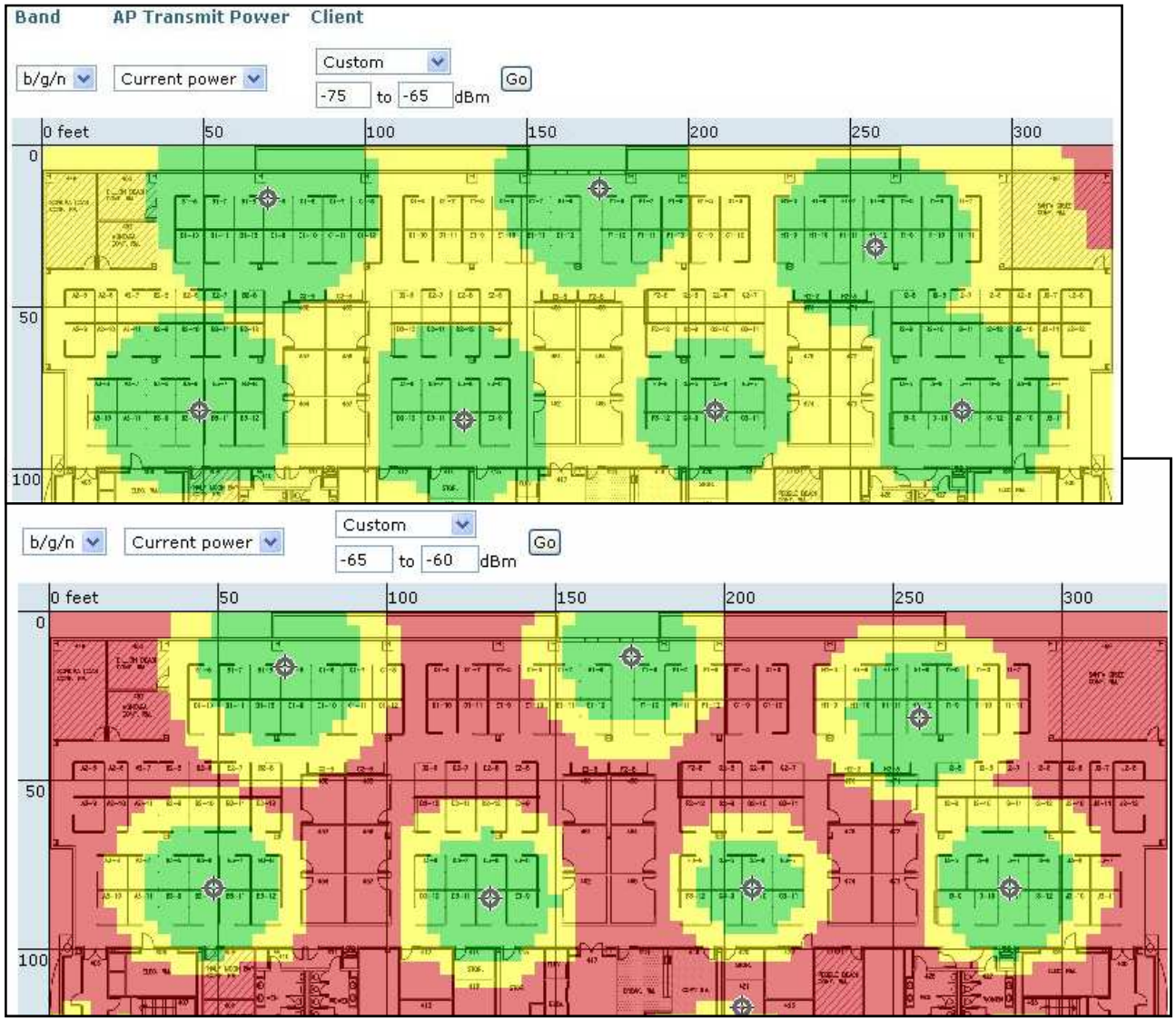
1. The WLC radio statistics provide a summary of the overall RF environment seen by an AP
2. This can be helpful in determining the root cause of packet loss and delay in the network

Site Survey



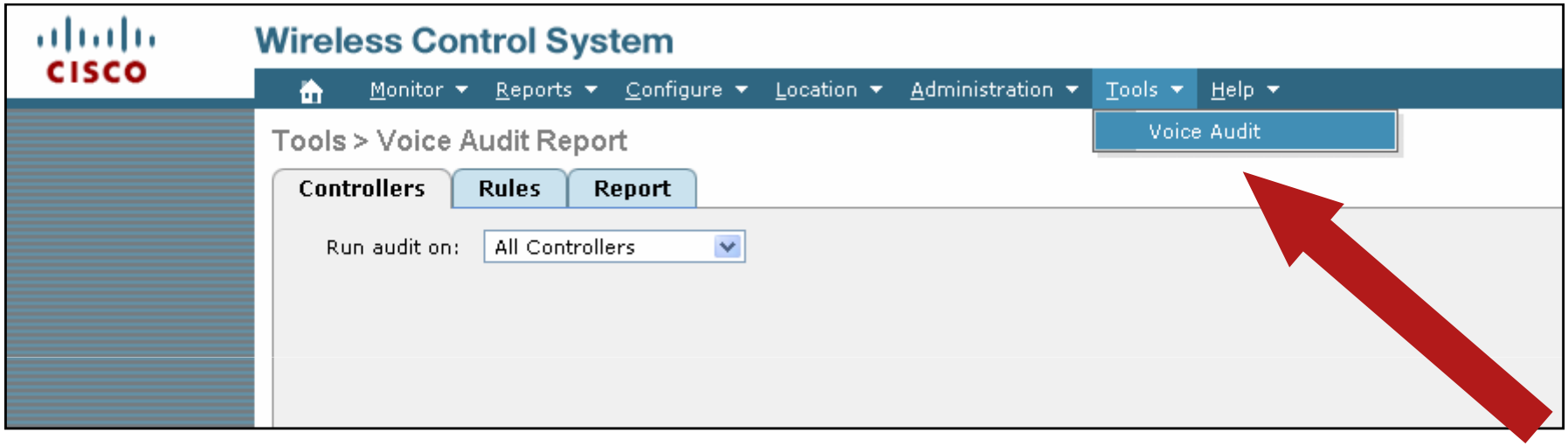
1. Coverage, overlap, and signal strength are key to a successful VoWLAN deployment
2. A survey of the VoWLAN deployment should be performed post install to determine that the project goals have been met
3. Third party tools such as Airmagnet Survey are useful for this purpose

Comparison -75/-65 to -65/-60



This Mapping Was Done Solely on Default Which Is Signal Prorogation Formula

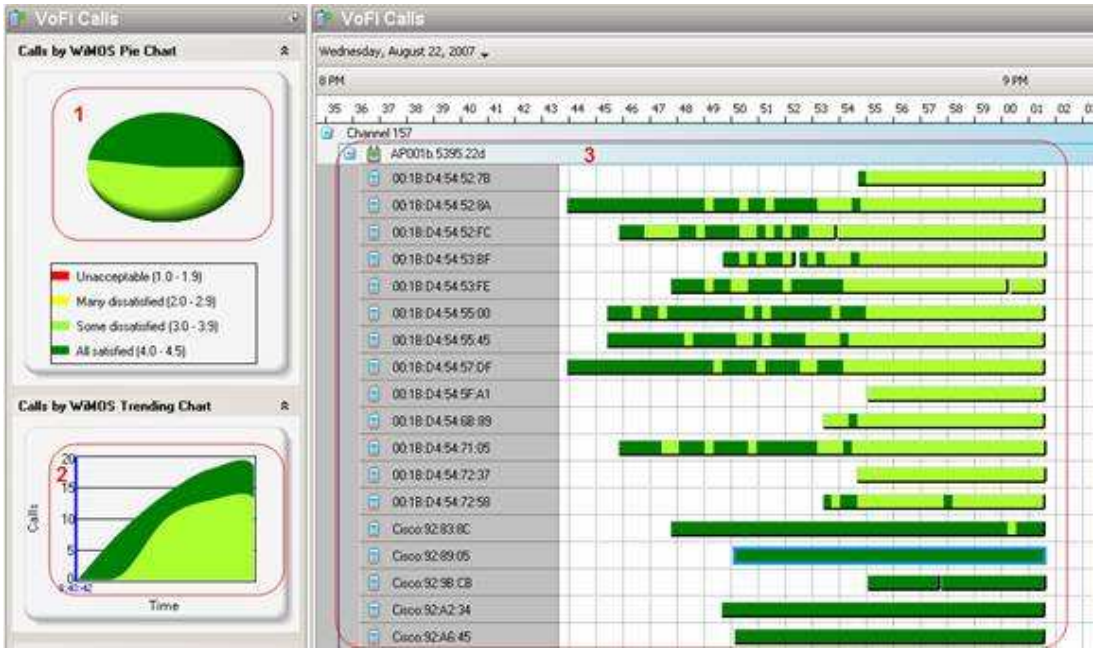
WCS VoWLAN Audit Tool



1. The user will choose:
   - The controllers to be audited
   - The rules of the audit
   - And how the audit is reported
2. The audit will be able to run the configuration checks on controllers running the following versions: 4.1.x, 4.2.x, and 5.x.x

More Troubleshooting Tools

1. The are a number of tools available for VoWLAN analysis, including sniffer tools using Wireshark or Omnipeak
2. The Airmagnet VoFI Analyzer provides useful feedback on VoWLAN MoS scores over time



Voice over WLAN

Cisco Unified IP Phone 7921/7925 Implementation Guidance

7921G Overview

1. 802.11a/b/g
2. 2 in (5 cm) color display with 176 x 220 pixel resolution
3. Dedicated Volume and Mute buttons
4. Application button supports PTT via XML
5. Two softkey buttons
6. Speakerphone
7. Diversity antenna (5GHz band only)
8. Ringing, message waiting, and charging LED
9. 5-way navigation key
10. Separate ringer and speaker
    Louder ring volume
11. Vibrate alert
12. Backlit keypad and display
13. Headset connector 2.5mm (4-conductor/tri-band)
14. USB 1.1 connector

7925G Overview

1. IP54

   Dust protected; dust deposits are permitted, but their volume must not affect the function of the unit

   Splashing protected; Spray water from all directions, (limited ingress permitted)

2. Bluetooth 2.0

   Bluetooth/WLAN Coexistence

3. Battery Life

   Standard Battery (1100 mAh) -Up to 180 hours standby OR up to 9.5 hours talk time

   Extended Battery (1400 mAh) - Up to 240 hours standby OR up to 13 hours talk time

   - Proxy ARP IE from CCX v4 is required to get maximum battery life
   - If using 5 GHz, there is a 1 hour reduction in talk time
   - Coexistence with use of 802.11b/g and Bluetooth can decrease on call battery life up to 40-50%

4. Improved Durability

   5 ft (1.5 m) drop to concrete w/o carry case

   Silicon carry case manufactured by zCover can help durability www.zcover.com

Security protocols supported

Wi-Fi Protected Access (WPA) Versions 1 and 2; Personal and Enterprise are supported by the 7921

Authentication

- Lightweight Extensible Authentication Protocol (LEAP) Authentication
- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)
- WEP/WPA/WPA2 Shared Key

Encryption

- Wired Equivalent Privacy (WEP)
- Temporal Key Integrity Protocol (TKIP)
- Advanced Encryption Standard (AES)

Fast roaming protocol

- Cisco Centralized Key Management (CCKM)
- (CCKM is supported with TKIP/WPA only; AES/WPA2 is not supported)

Behavior in presence of 2.4Ghz 802.11b/g and 5gHz

If the Cisco 7921 is enabled for both 802.11b/g and 802.11a, and If the Cisco 7921 receives beacons on both of these frequency bands for the voice SSID

On Cisco 7921 Initial association

1. If the default Auto-RSSI is enabled, the phone will associate to the radio (and therefore frequency band) it hears with the strongest Receive Signal Strength Indicator (RSSI).
2. If Auto-b/g or Auto-a is enabled, the phone will associate to the frequency band specified, and will fall back to the non-specified frequency band only if the specified is unavailable
3. 802.11-b/g or 802.11-a is enabled, the phone will only associate to the frequency band specified.

On Cisco 7921 Roam

1. Once the phone has associated to an AP on a particular frequency band, it will only scan for and roam to, APs on the same frequency band.

792xG – Design Recommendations

1. Use single band for Voice WLAN
2. QoS
   - Platinium queue
   - Require WMM*
   - WMM / QBSS / ECDS / U-APSD – ON by default

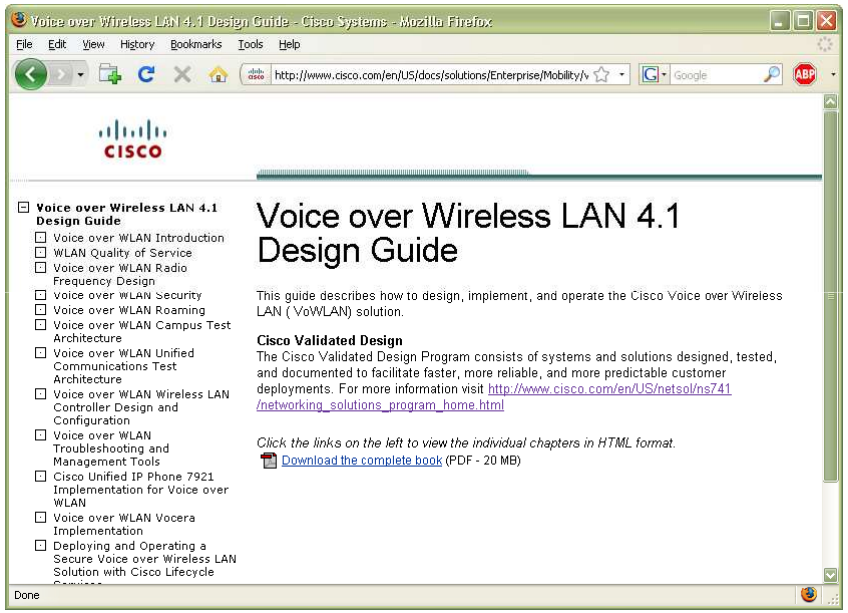
) Not in case of mixed-in 7920

Voice over WLAN

And that's about it…

For more information

1. www.cisco.com/go/cvd



Cisco Voice over WLAN – Cisco Validated Design

Cisco Networkers Barcelona
26 – 29. Januar 2009.
registrujte se!

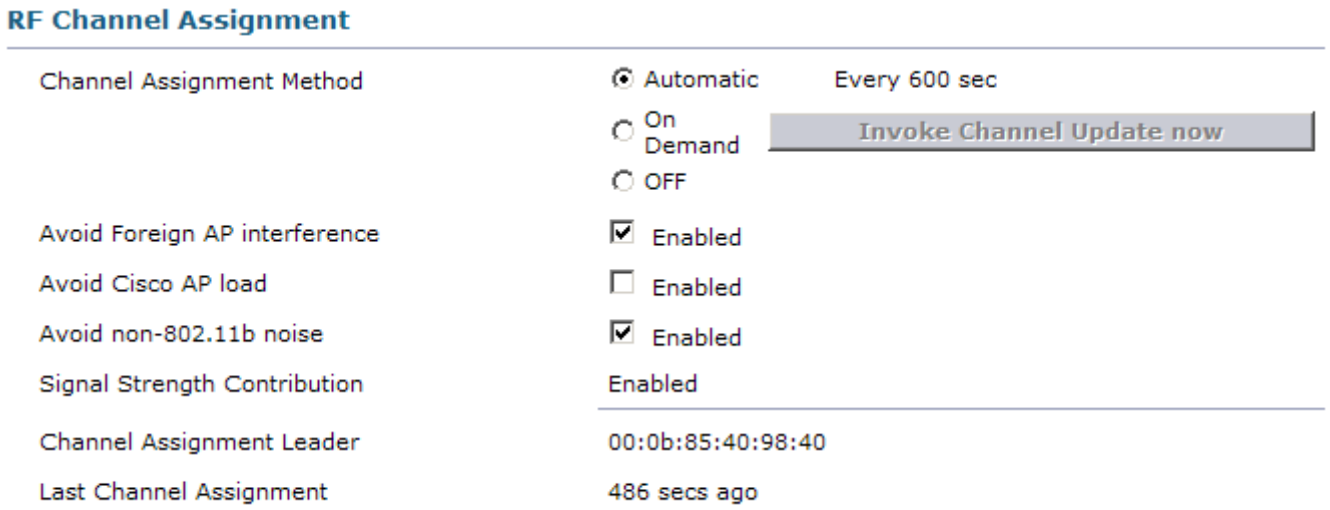
Cisco Networkers
2009
January 26-29 Barcelona, Spain

http://www.cisco.com/web/europe/cisco-networkers/2009/index.html

Voice over WLAN

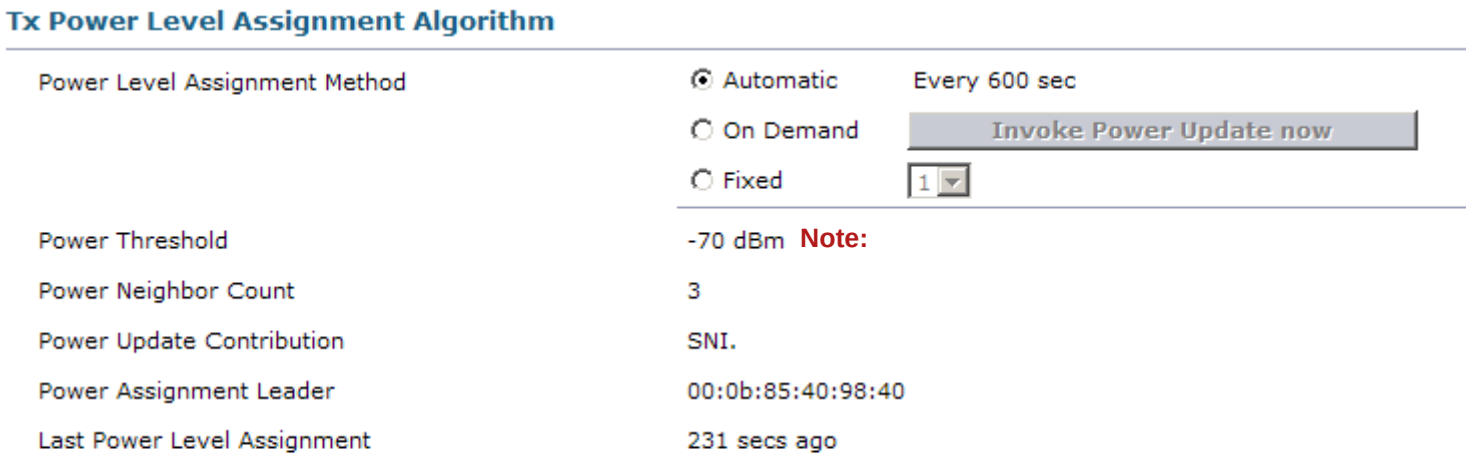
Tools & Configuration Slides

DCA



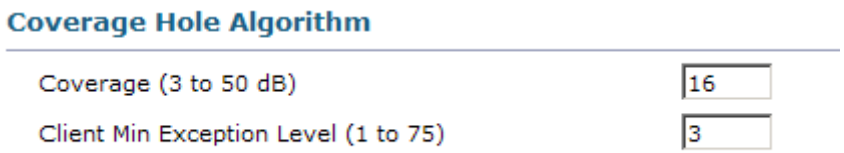
1. You get to choose the channels used by DCA
2. The default settings should meet most peoples need
   - Trying to avoid Cisco AP load is not recommended
3. You get to choose when DCA runs
4. A typical environment shouldn't see DCA change channels often

Tx Power Level Assignment



1. TPC Algorithm
   - Determine if there's a third neighbor, and if that third neighbor is above the transmit power control threshold
   - Determine the transmit power: **Tx_Max for given AP + (Tx power control thresh – RSSI of 3rd highest neighbor above the threshold)**
   - Compare calculation from step two with the current Tx power level and verify if it exceeds the TPC hysteresis.
     a. If Tx power needs to be turned down,: ***TPC hysteresis*** of atleast 6dBm must be met. ***OR***
     b. If Tx power needs to be increased: ***TPC hysteresis*** of 3dBm must be met.
2. Lets do some examples

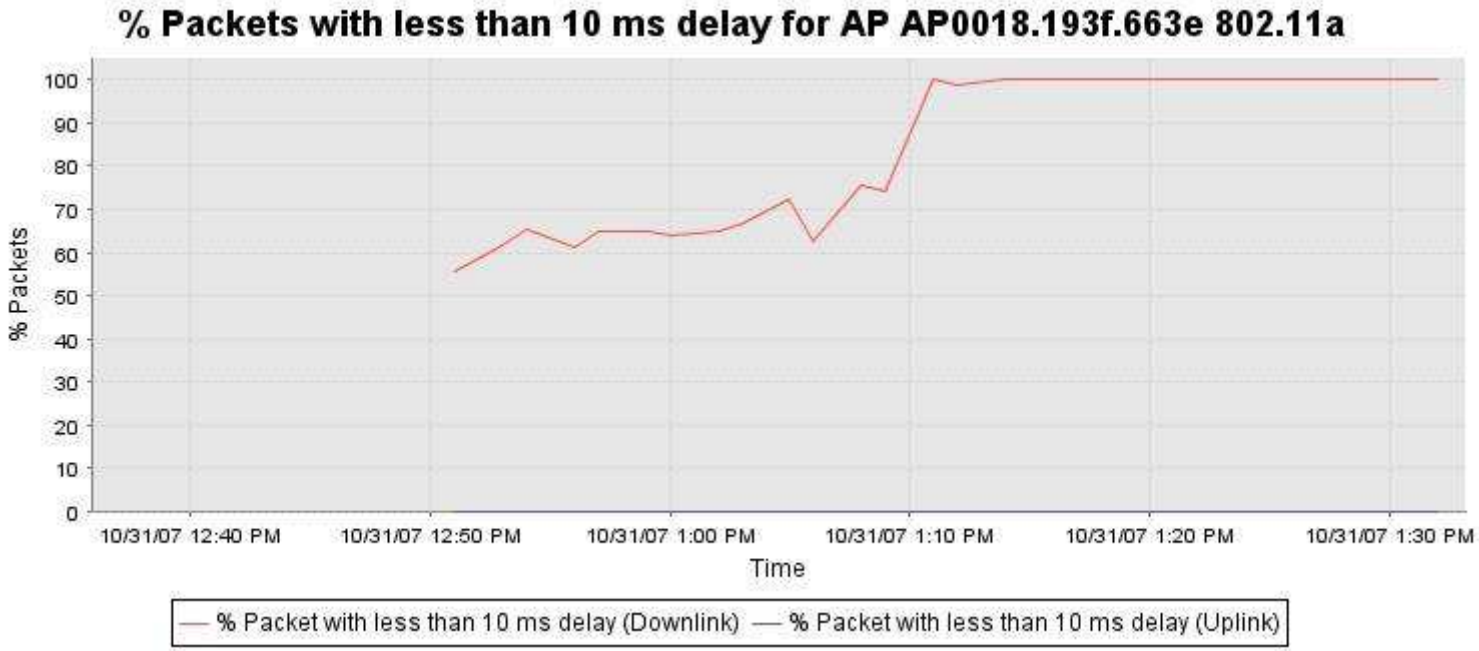
Hole Coverage



1. Hole Coverage is a nice feature
2. But it doesn't provide HA
   - Unpredictable trigger time
   - Unpredictable coverage of the hole

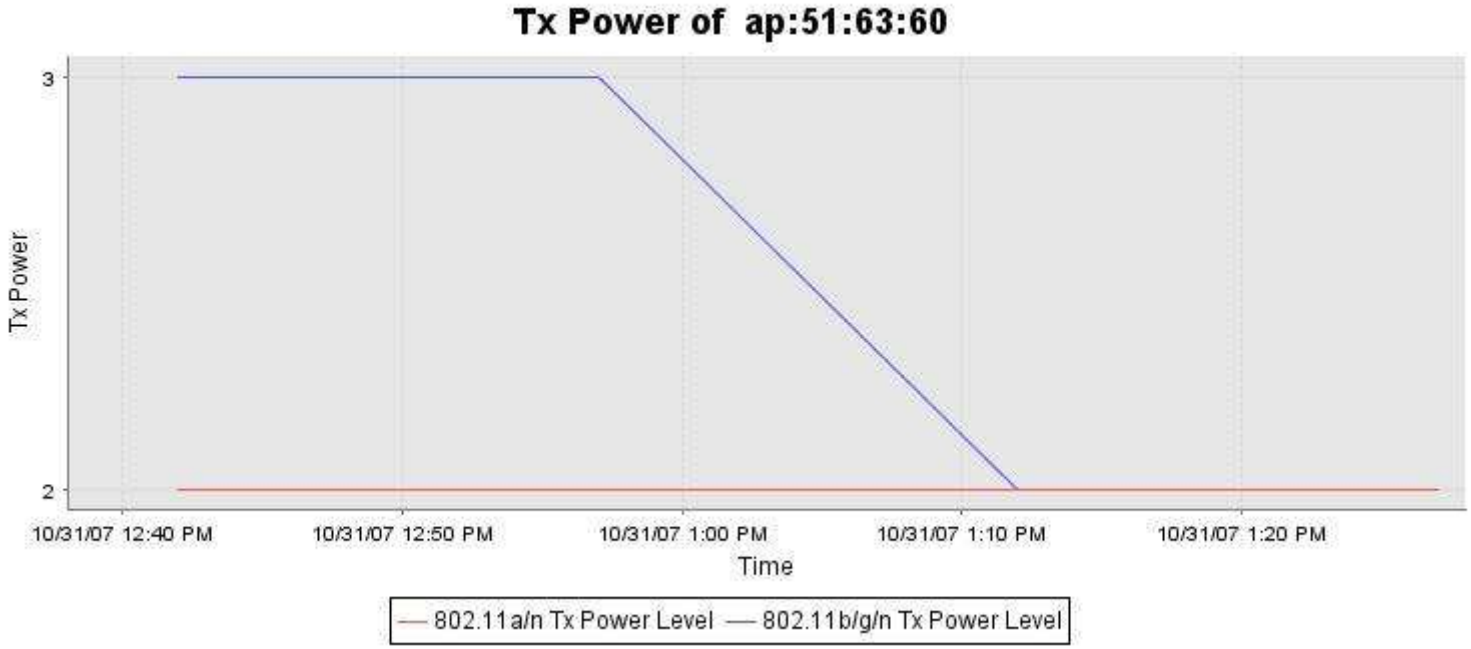
WCS -Traffic Steam Metrics

1. The WCS provides historical reports of traffic stream metrics
2. This are useful in correlating user issues with network issues, and alerting to capacity issues



WCS- Power and Channel Reports

1. The WCS reports give a picture of the AP power and channel changes over time.
2. The reports give a picture of the overall WLAN environment



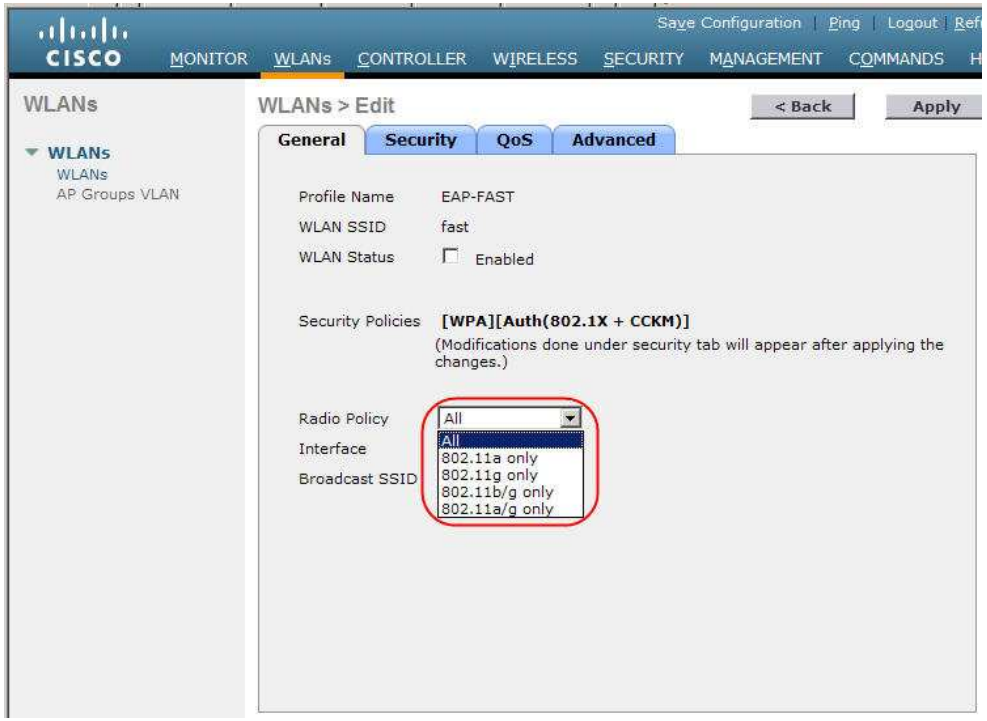
WCS Hole Coverage Alarms

Hole coverage alarms require action:

1. An radio is out of service?
2. Clients are not roaming correctly?
3. Users are operating in areas not covered by the site survey?

Controller RF Configuration

1. Recommended way to limit the 7921 operation to a single frequency band (I.E. 802.11a or 802.11b/g) is to leave the phones at their default setting, and to configure the WLAN on the controller (or WCS) to operate on a single frequency band.



QoS Configuration

The Cisco 7921 supports the following QoS related protocols and standards;

1. 802.11e/Wi-Fi Multimedia (WMM)
2. Traffic Specification (TSPEC)
3. Enhanced Distributed Channel Access (EDCA)
4. QoS Basic Service Set (QBSS)
5. Unscheduled automatic power-save delivery (U-APSD)
6. Power save mode

All of these features are enabled by default on the phone and will be used if enabled on the AP to which the phone associates. The QoS chapter of this document provides more detail on each of these.

Controller QoS configuration

1. Assign **Platinum** QoS policy to the voice VLAN
2. If only WMM capable voice handsets such as the 7921 are to be deployed, the the WMM Policy drop-down box should be set to **Required**
3. If there will be a mix of 7921 and non WMM capable devices such as the 7920, then the WMM policy should be set to **Optional**