
TOMORROW starts here.
cisco
Cisco live!

Design and Deployment of Wireless LANs for Mobile Applications

BRKEWN-2000

Henry Chou

Consulting Systems Engineer

Cisco live!

About Henry Chou …

- Henry is my legal name, but not my first name
- Consulting Systems Engineer, Northern California, Enterprise West (US)
- CCIE #10315
- Co-authored; “CCNA Cisco Certified Network Associate Wireless Study Guide (Exam 640-721)”,
- Work and family

Agenda

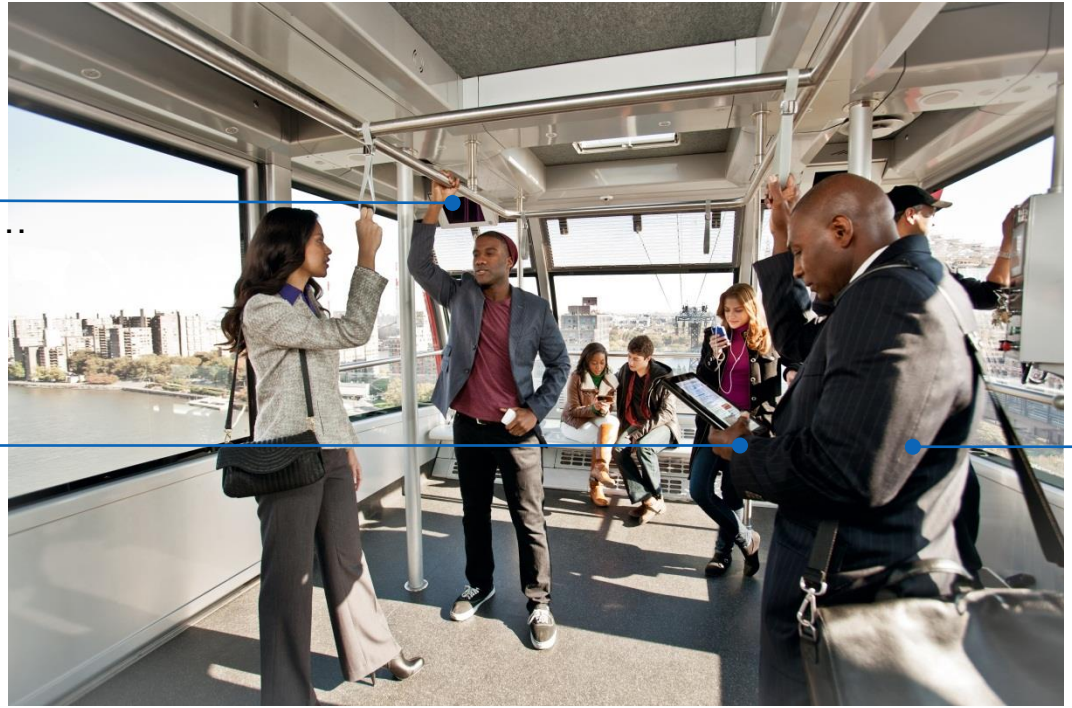
- Determine Applications Requirements
  - wireless device specs and mobile application needs
- Build the Cell
  - Efficient and fast for mobile applications
- Improve for QoS
  - Prioritise traffic that cannot wait
- Fine tune for mobile applications
  - Help applications that need priority, but do not say so
  - Roaming and more roaming
- What will NOT be covered
  - Collaboration Manager configurations, Voice protocols comparison, Voice Gateways…

Design Steps

Determine Application Requirements

- Build the cell
- Improve for QoS
- Fine Tune for Mobile apps

Welcome to Your New World



Everything uses Wi-Fi…
Everything?

Far Reaching Wi-Fi

I get Wi-Fi from
almost everywhere

More Applications

Everyone uses Wi-Fi…
for almost everything

Mobile Applications – Design Considerations

- Application demands are increasing in Wi-Fi medium
  - Use the same wireless device to browse the Internet, stream video, or place a call… so design is about the device, but also the application on the device.
  - Real time applications (voice, video) are intolerant to losses and delays, and sometimes require high throughput
  - Users have high expectations of wireless, if it works at my house, it should work everywhere
- Wireless is still a shared Half Duplex medium and requires efficient spectrum use.
  - Design your network for the most demanding applications
  - Understand 802.11 protocol
  - Understand physical coverage
  - Understand nature of mobile applications

How Much Bandwidth Is Required?

Often Less than You May Think

- Most likely you support more than one application
- Design for the highest bandwidth demand
  - What is the minimum acceptable throughput for the application
  - Most users use only ONE high performance demanding application at a time
  - Multiply this by the number of devices
  - This is the aggregate bandwidth required for the cell

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

How Much Bandwidth do They Need?

It all depends on how you use them!

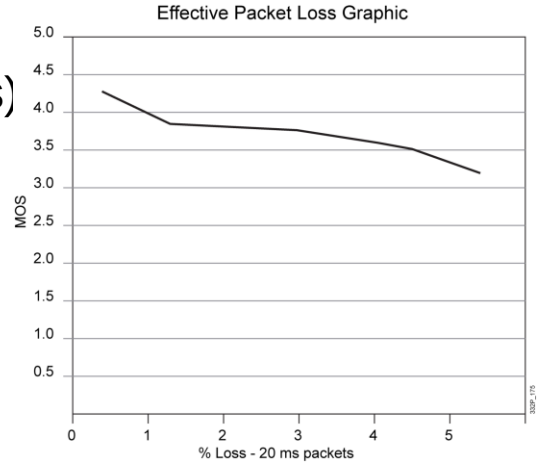
- Example, Skype (Up/Down):

Call type	Audio	Video/screen share	Video HD	Group Video (5 people)
Typical Bandwidth	30Kbps/30kbps	130kbps/130kbps	1.2 Mbps/1.2 Mbps	130 kbps/2 Mbps

- Now that you get the picture, a few other examples:
  - Fring (video): 135 kbps,
  - Facetime (video, iPhone 4S): 400 Kbps, (audio) 32 kbps
  - Viber (video) 120 kbps, (audio) 30 kbps
  - Skype/Viber/other chat: around 850 to 1000 bytes (6.8 to 8 kb) per 500 character message
  - Netflix (video), from 600 kbps (low quality) to 10 Mbps (3D HD), average 2.2 Mbps
  - This bandwidth consumption is one way, you need to double for 2-way conversations

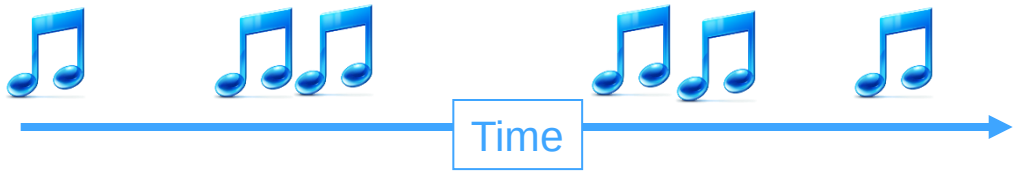
VoIP Requirements

- VoIP carries voice with UDP and RTP, voice control traffic uses RTCP
  - Voice sound is converted to digital packets using codecs
  - Resulting packet size ranges from 8 to 64 bytes per packet (+40 bytes L4/L3 headers, +L2 header)
- Voice has very strict requirements as an “application”
  - Packet loss < 1% (i.e., lost packets / total received packets)
  - Packet Error Rate (PER) <=1%
  - As low jitter as possible <100ms
  - Channel Utilisation levels should be < 50%
  - Retries should be < 20%
  - When these values are exceeded, MOS suffers
  - Goal is to keep MOS high



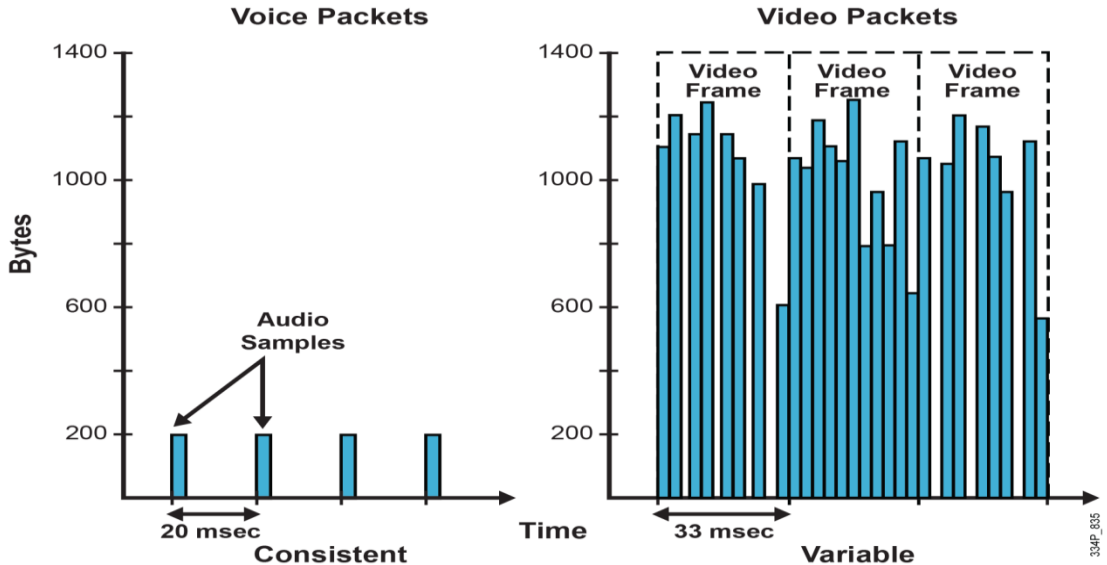
VoIP Requirements

- Voice audio quality perception varies:
  - Depends on the codec selected
  - Depends on the percentage of lost packets, delay and jitter
  - Delay is the end-to-end travel time of each packet, target for the local 802.11 cell is less than 30 ms, and 150 ms end to end
  - Long delays create disturbing silences and conversation overlaps
  - Excessively delayed packets may be dropped at the receiving end
  - Jitter is the variation of delay between packets
  - High jitter generates audio quality issues (clicks, metallic audio or silences)



Video Applications

- Video uses video and audio codecs
  - Some codecs are built for real time exchange, some for streaming
  - Video algorithms refresh entire images when large changes occur
  - The changes generate traffic bursts



Design Steps

Determine Application Requirements

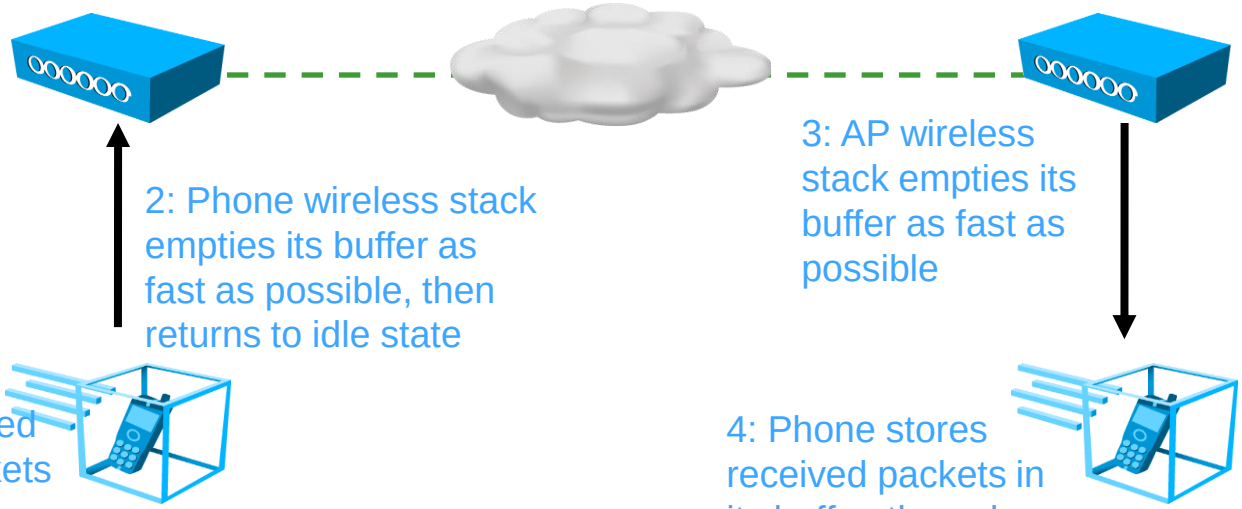
Building the Cell

Improve for QoS

Fine Tune for Mobile apps

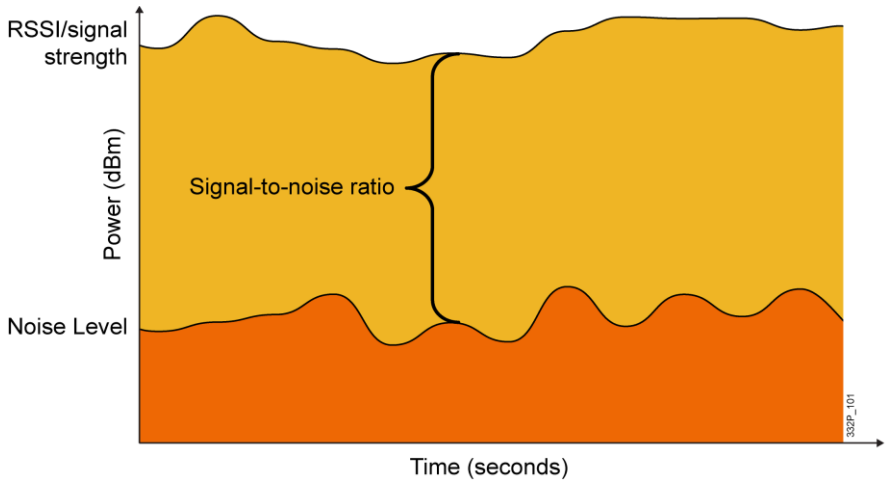
VoIP (and Video!) over Wireless Data Flow

– VoIP packet rate (e.g. 50 packets/second) is not wireless transmission rate (0.03 milliseconds per packet at 54 Mbps)



Cell Size – Depends on Protocol and Rates

- Higher power does not always mean higher SNR…

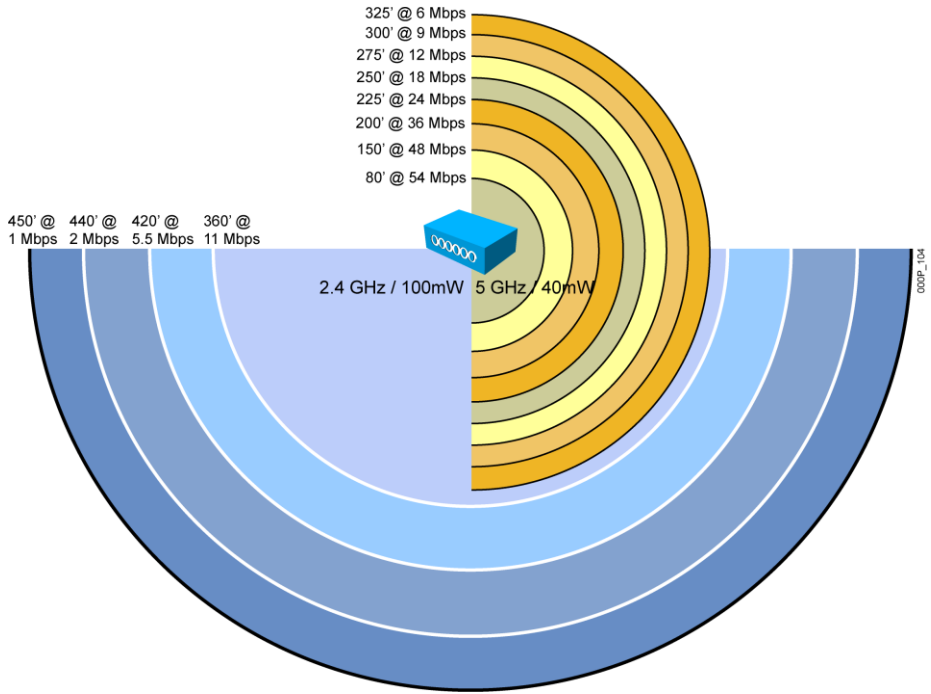


Assuming 10% PER

Speed	Required SNR	AP Sensitivity
1	0	-91
2	3	-91
5.5	6	-91
6	2	-87
11	9	-88
12	6	-86
24	11	-85
36	13	-85
48	17	-78
54	19	-77

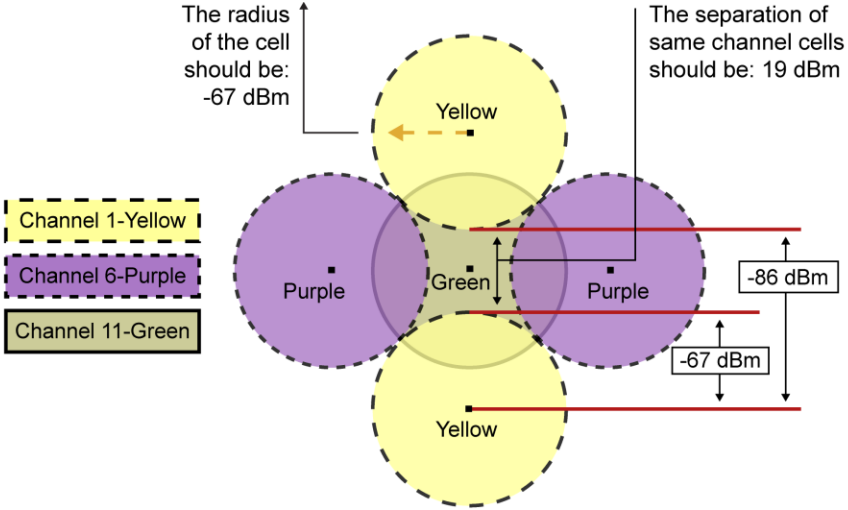
Cell Size – Depends on Protocol and Rates

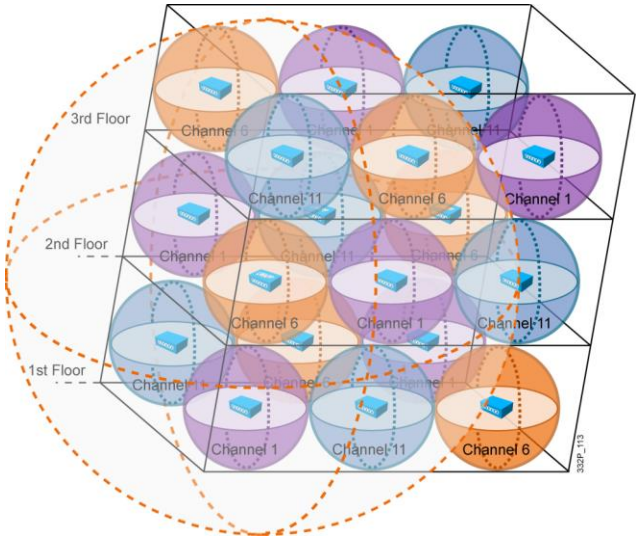
- Data rates decrease with the increase of distance from radio
- Individual throughput (performance) varies with number of users
- Performance degrades with radio interference from other sources
- Critical design goal is to achieve high data rate at cell boundary
  - High signal AND low noise



2.4-GHz Network Design

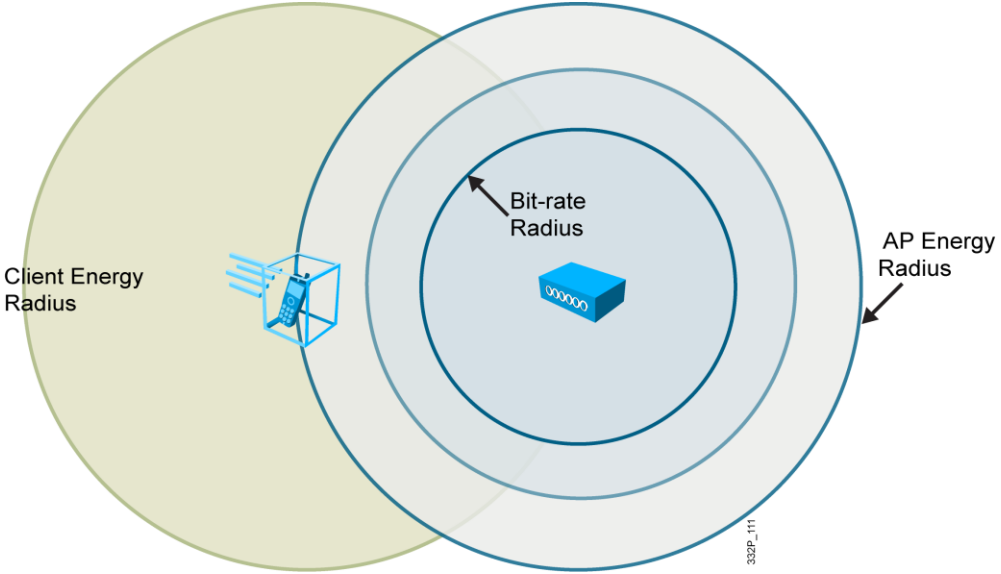
- Conclusion: try to design small cells, with clever overlap…

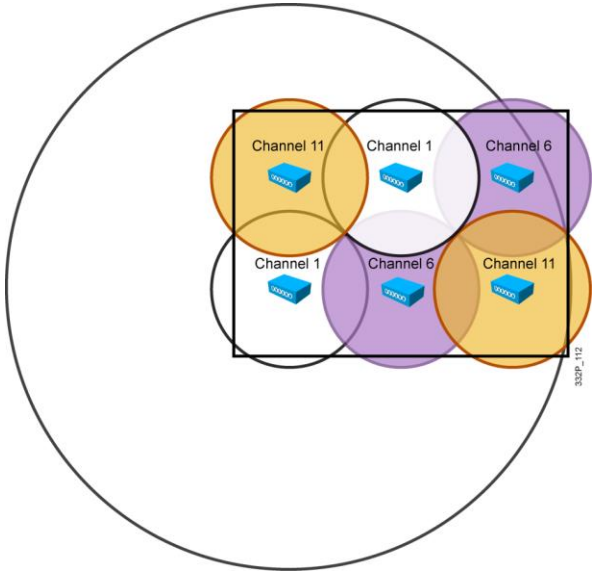




2.4-GHz Network Design

- The cell useful size is different from the AP footprint… And clients do not make it easier…





Some Performance Examples

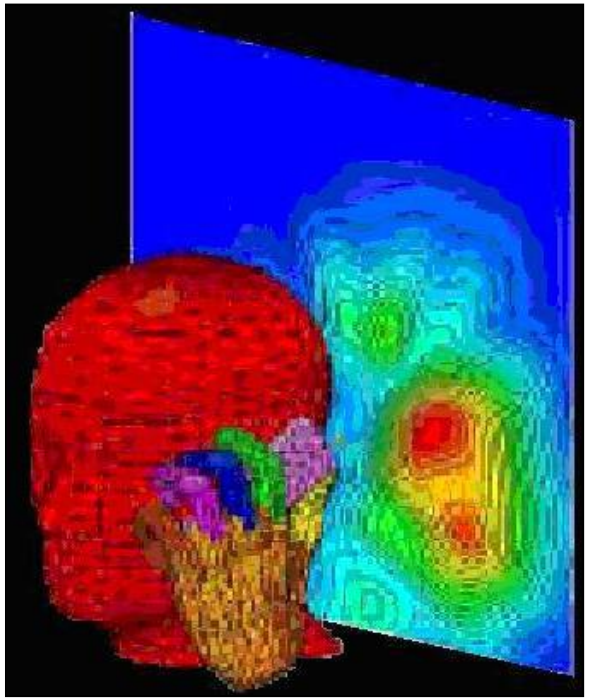
	iPad	iPhone-4	Moto-Xoom	Galaxy S2	Galaxy Tab
					
Measured - best	-33 dBm	-39 dBm	-34 dBm	-31 dBm	-33 dBm
Pathloss	46 dB	46 dB	46 dB	46 dB	46 dB
RSSI	13 dBm	7 dBm	12 dBm	15 dBm	13 dBm

Channel Coverage Sizing Recommendations

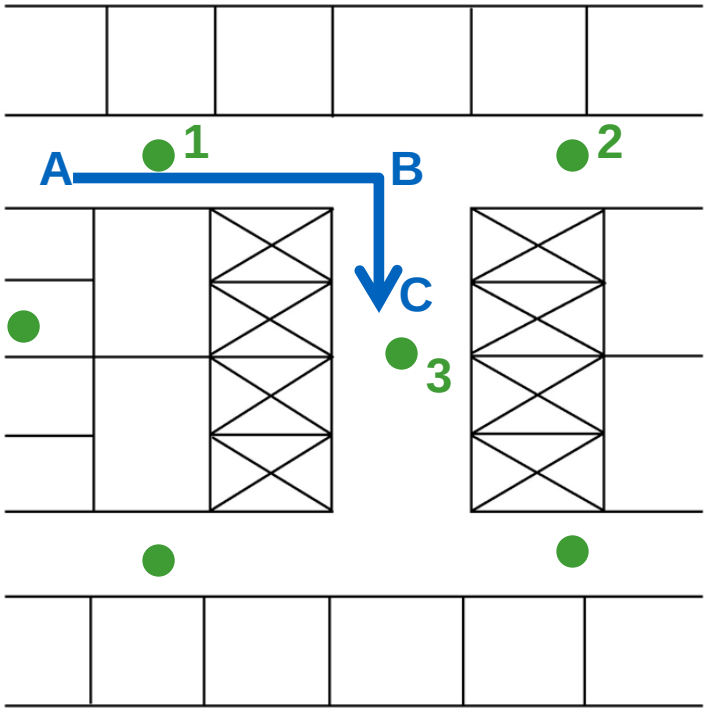
- Coverage must be designed for client devices
- Not all clients are created equal !!!
  1. Live call test with the actual client to determine its coverage
- Removing legacy DSSS data rates and slower OFDM data rates from WLC configuration equals:
  1. Less Co-Channel Interference
  2. Better throughput in the cell
  3. More usage of ClientLink and MRC
  4. Smaller coverage cells
- Smaller cell sizes equals:
  1. More cells in a given coverage area
  2. More cells equals more call with better voice and video quality

Signal Attenuation

Object in Signal Path	Signal Attenuation Through Object
Plasterboard wall	3 dB
Glass wall with metal frame	6 dB
Cinderblock wall	4 dB
Office window	3 dB
Metal door	6 dB
Metal door in brick wall	12 dB
Phone and head position	3 - 6 dB

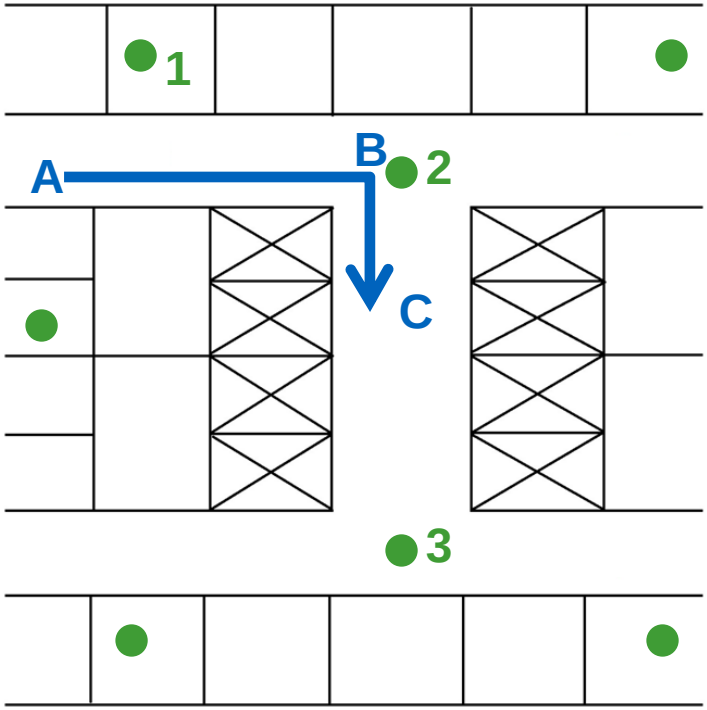


VoWiFi Rate Shifting and AP Placement



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

VoWiFi Rate Shifting and AP Placement



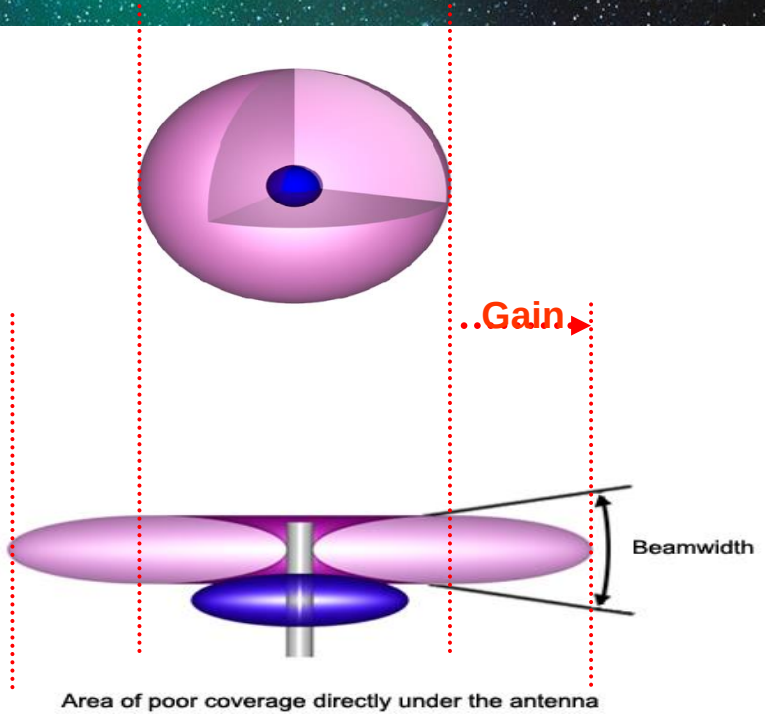
- At point A the phone is connected to AP 1
- At point B the phone has AP 2 in the neighbour list as it was able to scan it while moving down the hall
- At point C the phone needs to roam and successfully selects AP 2
- The phone has sufficient time to scan for AP 3 ahead of time

Antenna Theory and Antenna Gain

- A theoretical isotropic antenna has a perfect 360º vertical and horizontal beamwidth (it puts the i in dBi)
- This is a reference for all antennas
- Gain is equal in all directions
- The reception of good signals and interference is the same in all directions

High Gain Omni-Directional Antenna:

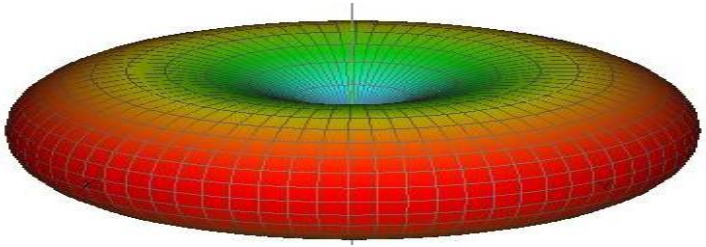
- More coverage area on the horizontal elevation
- Energy level directly above or below the antenna will become lower



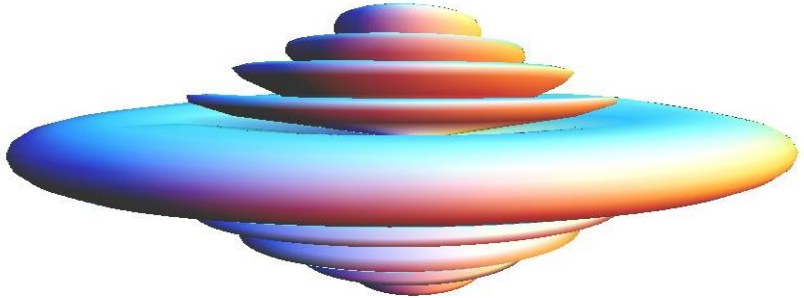
There Is No Increase in Transmitted Energy with the Higher Gain

Radiation Pattern and Environment

- Radiation patterns provided by vendors are lab values
  - Do not take into account environmental impact
- Example: dipole antenna in lab environment (left), and positioned below a metallic plate (right)
- Position the antenna carefully to obtain a radiation pattern similar to the example provided by the vendor



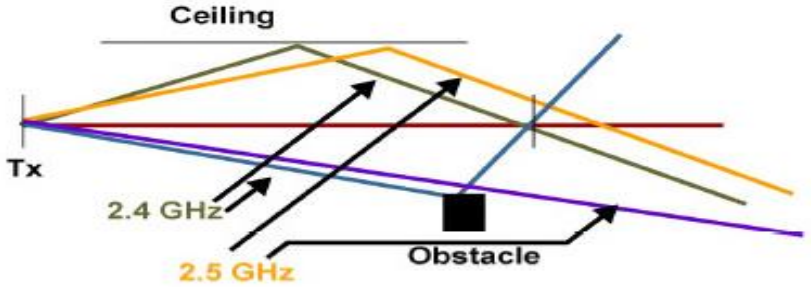
Dipole antenna
Default radiation pattern



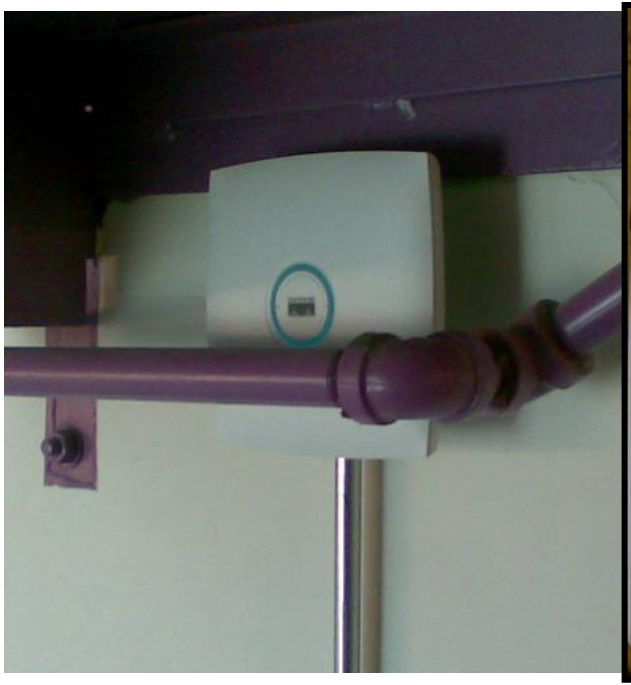
Dipole antenna
Radiation pattern when close to I-beam

RF Design – Don’t Do Anything Stupid

- Highly reflective environments
- Multipath distortion/fade is a consideration
- Legacy SISO technologies (802.11a/b/g) are
- 802.11n improvements with MIMO
- Devices are susceptible
- Things that reflect RF
  - Irregular metal surfaces
  - Large glass enclosures/walls
  - Lots of polished stone



RF Design – More Bad Examples

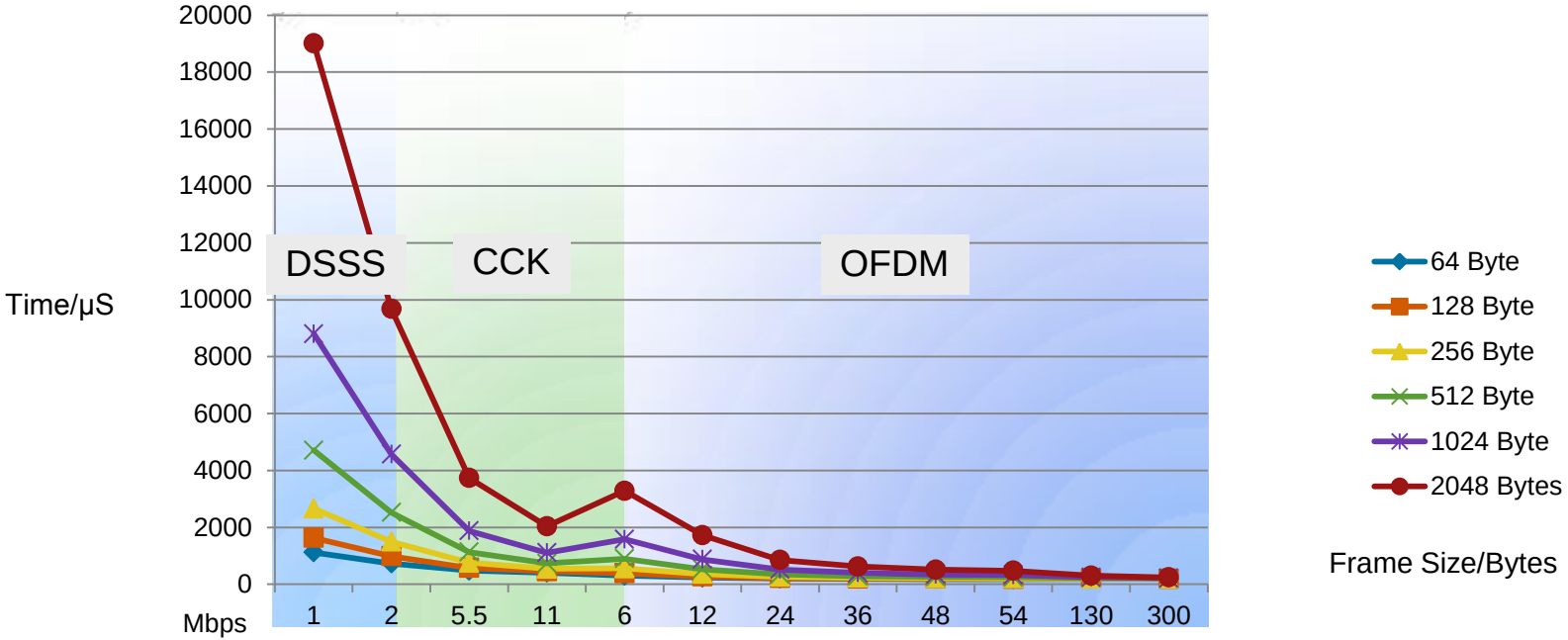


Mount horizontally… and not behind a metallic pipe

A little ICE to keep the packets cool

Mmm…

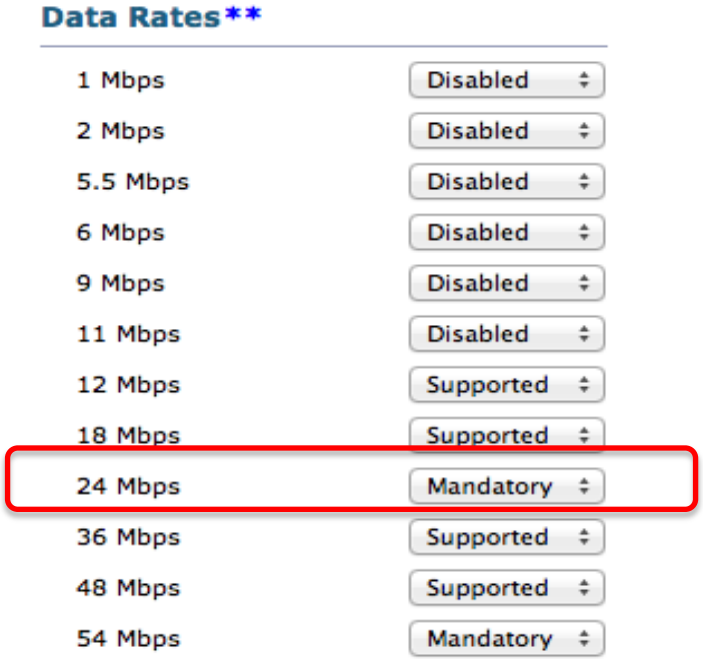
Wireless is Shared Medium



Spectrum is a Shared Finite Resource

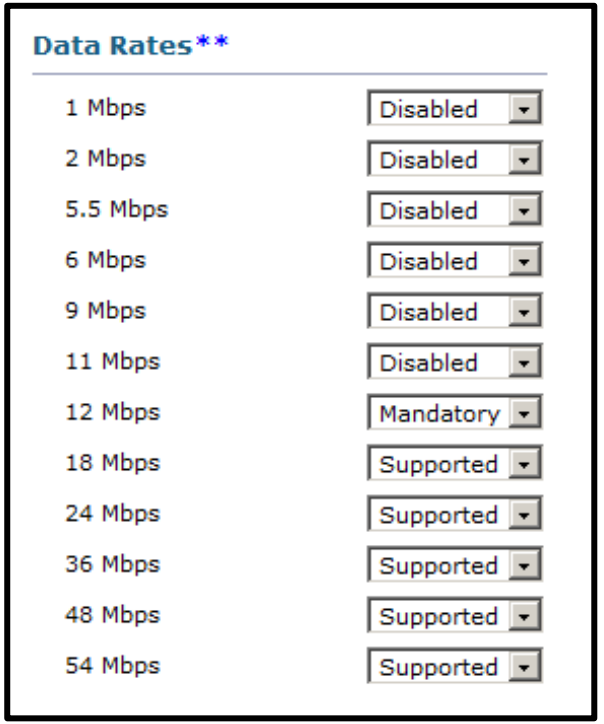
Every SSID Counts!

- Each SSID requires a separate Beacon
- Each SSID will advertise at the minimum mandatory data rate
- Disabled – not available to a client
- Supported – available to an associated client
- Mandatory – Client must support in order to associate
- Lowest mandatory rate is beacon rate
- Highest mandatory rate is default Mcast rate



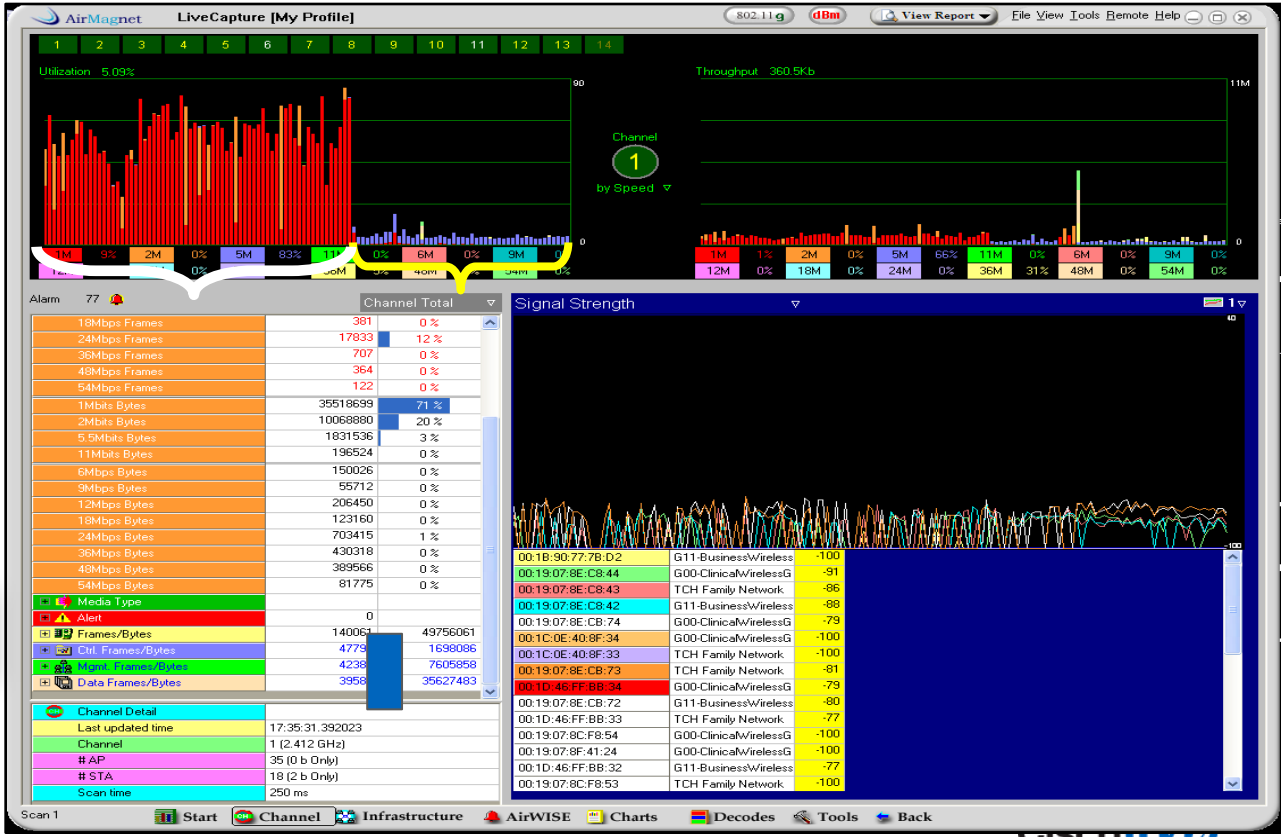
Channel Design – Use the Tools

- Disable low, unused rates (802.11b)
- Let RRM control channel and power levels
- If you can, use 3600/3700 APs, with ClientLink and BandSelect:
  - BandSelect to push 5 GHz-able to the 5 GHz band
    - Take advantage of 4-21 non-overlapping channels
  - ClientLink to provide better throughput for 802.11a/g/n/ac clients



Channel Utilisation— What Made the Difference?

5% After

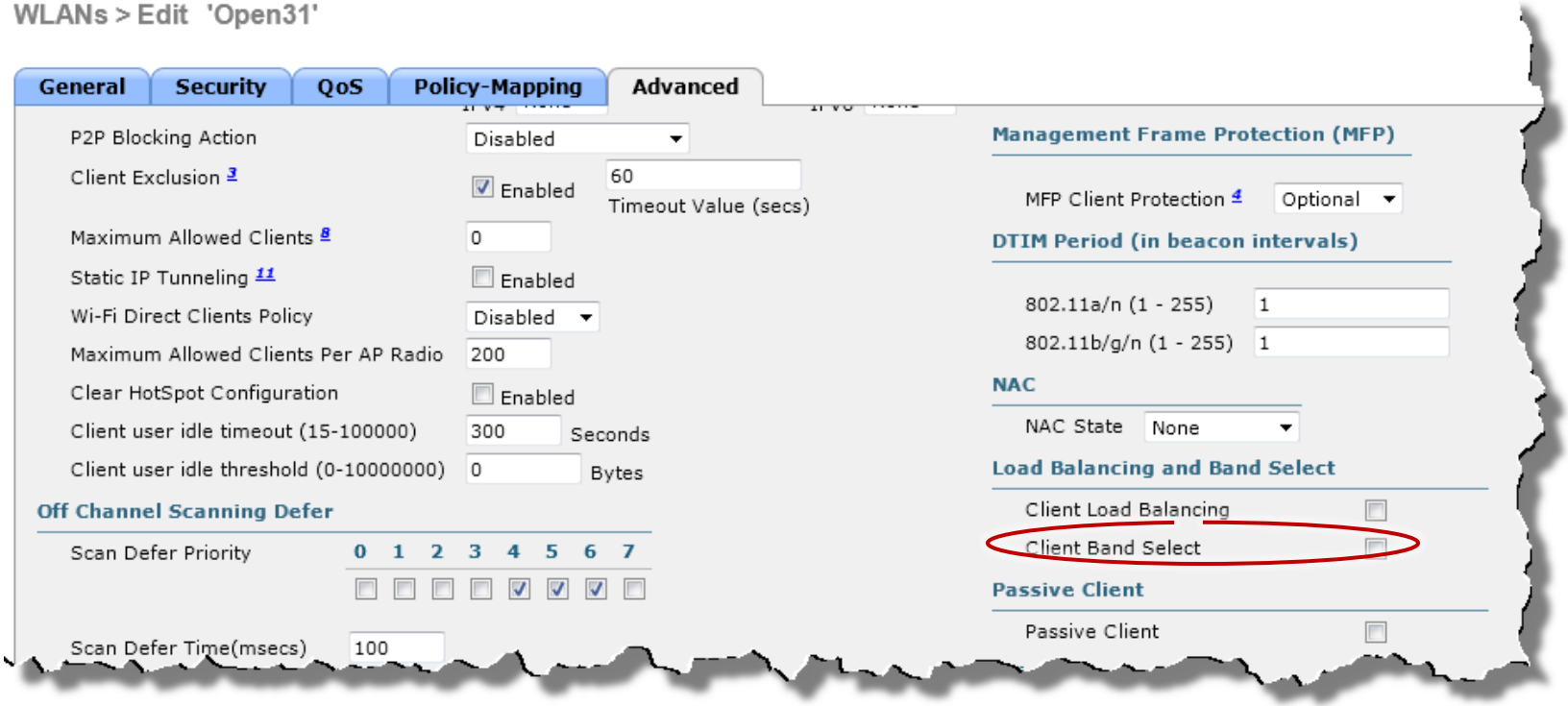


Cisco BandSelect Technology

- Automatic Band Steering and Selection For 5GHz Capable Devices

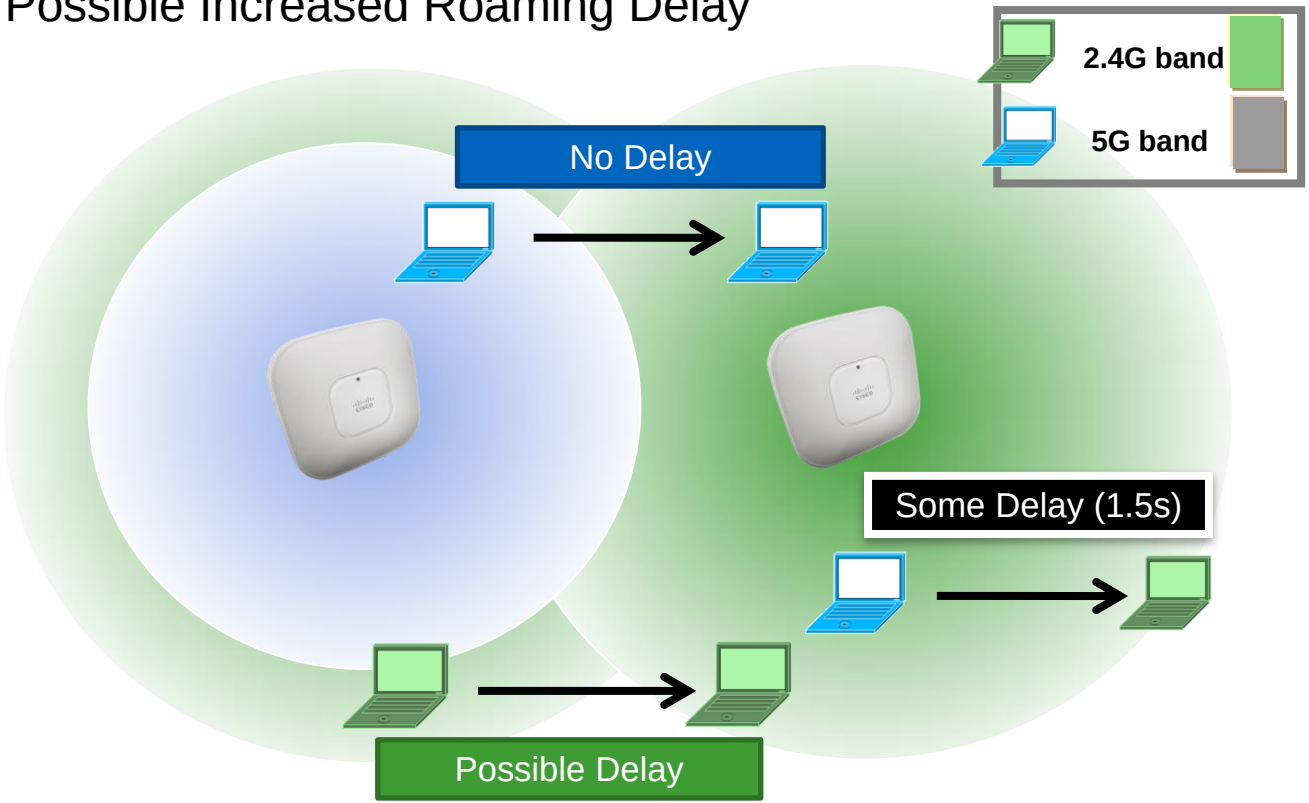
Configuring Band Select

- Enabled on a per WLAN basis (disabled by default)



BandSelect – Test Before Full Deployment

- Caveat – Possible Increased Roaming Delay

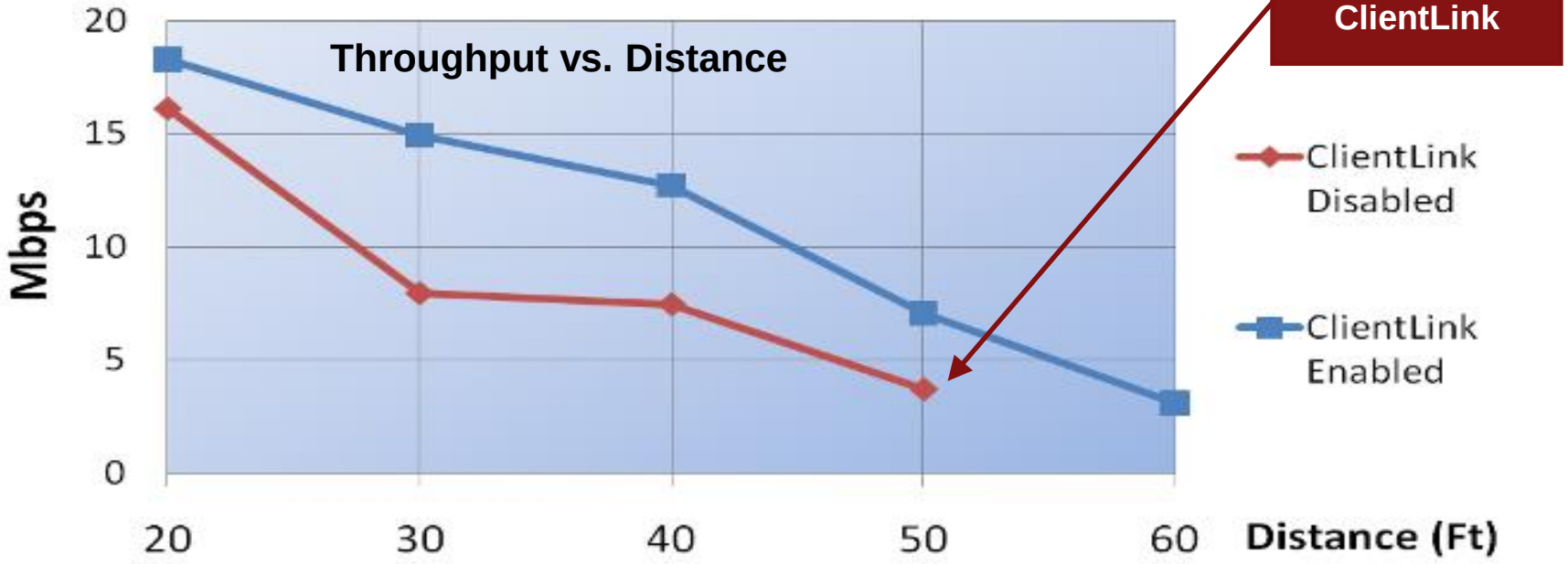


Cisco ClientLink Technology

- Advanced Beam Forming Technology

Cisco ClientLink 2.0 and 3.0

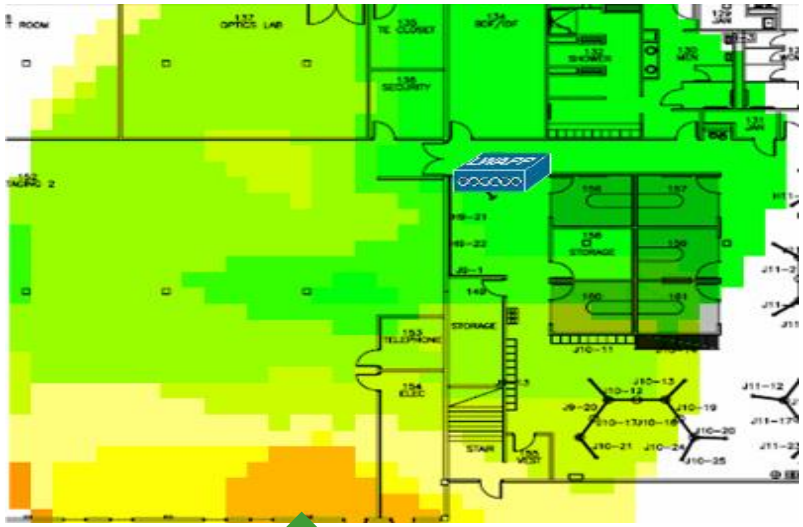
- Implicit Beam Forming, Up to **65%** Increase in Throughput
- No client config needed



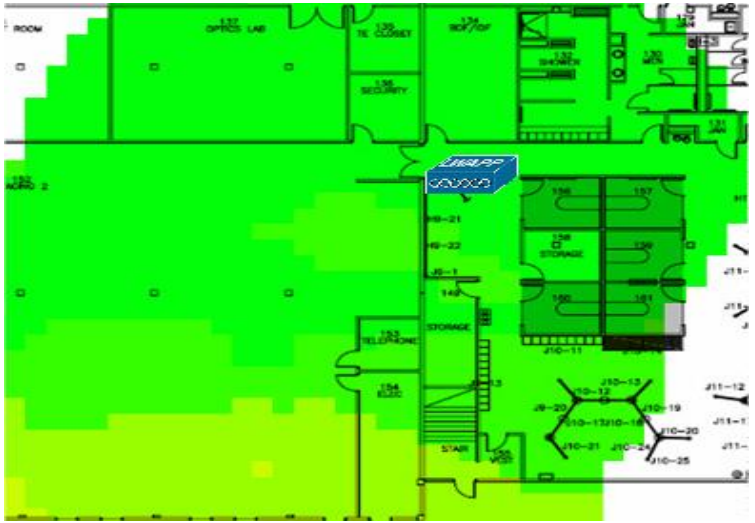
Client Link: Reduced Coverage Holes

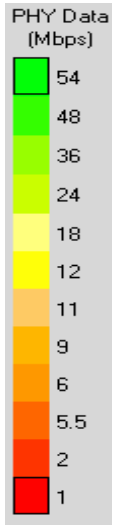
Higher PHY Data Rates

- ClientLink Disabled



- ClientLink Enabled





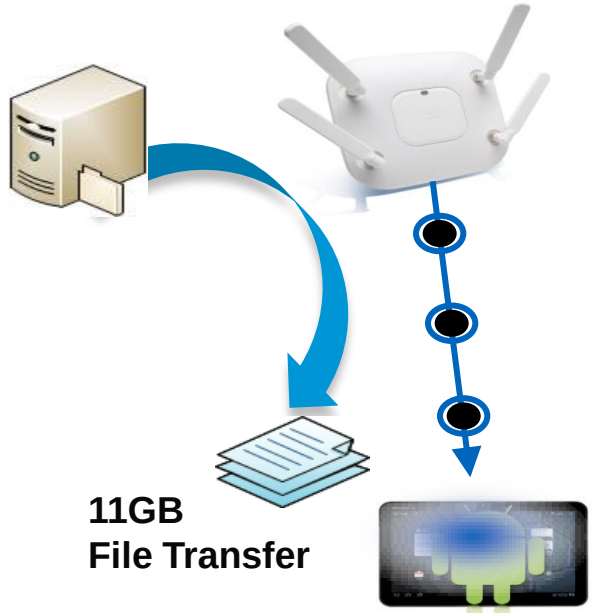
Lower Data Rates

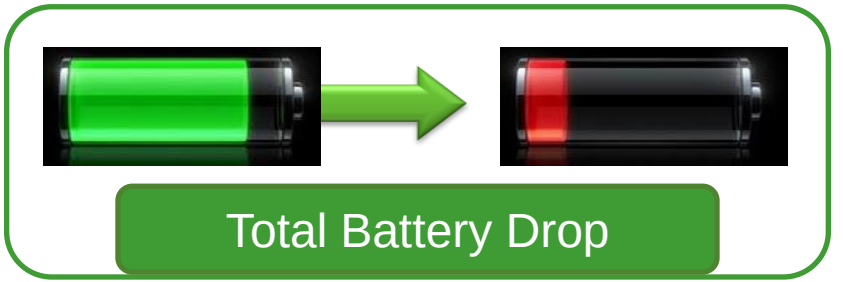
Higher Data Rates

Source: Miercom; AirMagnet/Fluke Iperf Survey

ClientLink: Battery Life Improvement

- 30ft Distance from Access Point to Motorola Xoom
- Download a file via FTP till complete and observe battery drop.





Tips on RF Design

- Every site is unique, do not assume two installations would be the same
- Think of AP coverage area as a “reading light” you want to illuminate where the devices will be.
- Use appropriated equipment for the need: 1140/3500i/3600i/3700i for carpeted areas, 1260/3500e/3600e/3700e for specific application, *antenna orientations*
- Avoid using internal antennas AP in vertical placements. RF planning is more difficult
- Validate that coverage is as expected *after installation*

Design Steps

802.11e and Wi-Fi Multimedia (WMM)

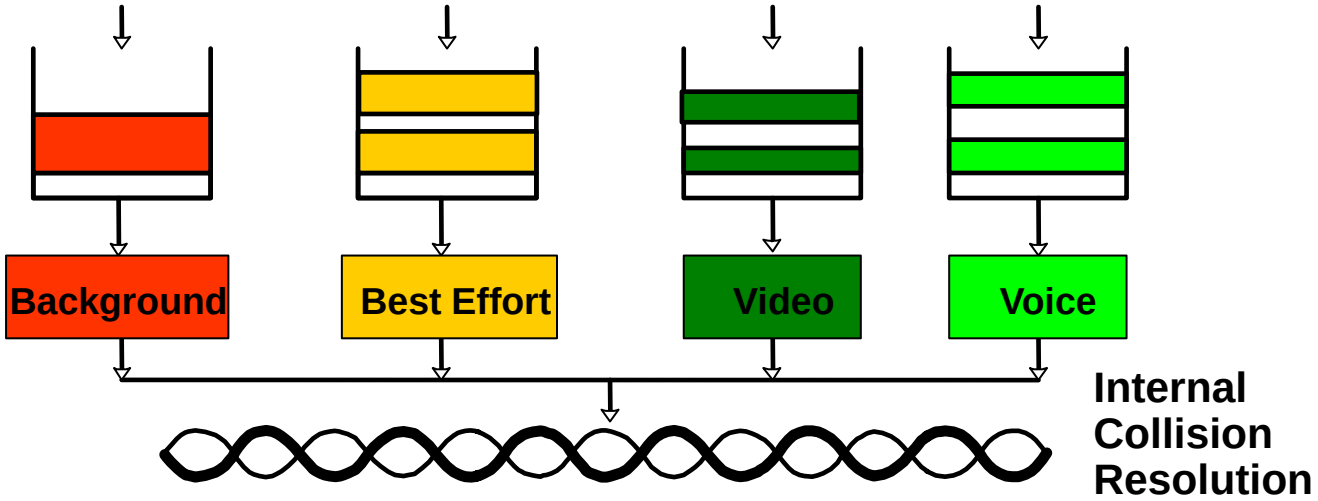
- 802.11e was ratified in 2005 to create QoS for 802.11.
- 802.11e introduces "EDCA" (Enhanced Distributed Channel Access, a framework to prioritise frames while still keeping the distributed behaviour of 802.11)
- APs are HC (Hybrid Coordinators), and cells are QBSS (QoS Basic Service Sets)
- Creates 8 UP (User Priorities, AKA Traffic Categories, TC) to set frame priority levels
- Allows Admission Control Mandatory (ACM) flag allows uplink traffic to be controlled
- Contention-free packet bursting within the TXOP Limit (Transmission Control: Transmission Opportunity)
- WMM is a Wi-Fi Alliance certification on partial implementation of 802.11e
- Ensures compatibility between vendors implementing the same 802.11e features
- Eight traffic categories (TCs) become four queues (Access Categories, AC)

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

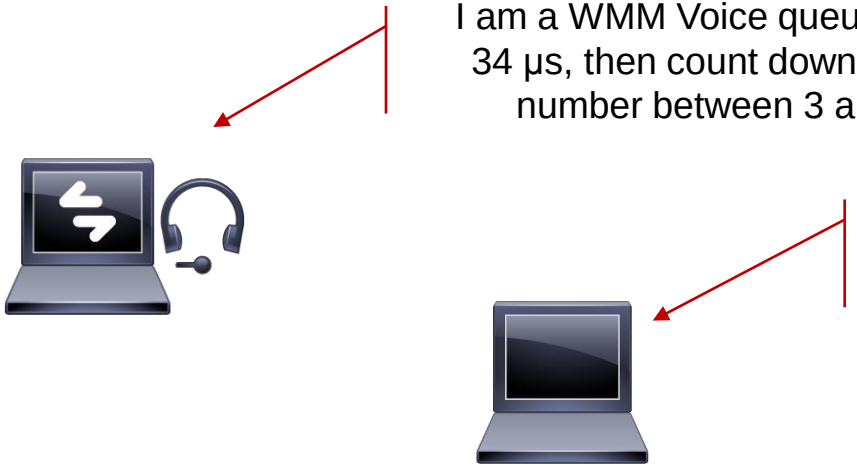
802.11e / WMM Media Access Classifications

- Separates traffic types in to 4 QoS access categories (AC)
- Background, Best Effort, Video, Voice
- These 4 ACs also have unique delay and random back off characteristics for accessing the RF channel (EDCA)



802.11e / WMM Media Priority

- To send a frame, wait a silence (IFS, Interframe Space), then count down from a random number (CW, Contention window) to zero
- WMM trick to prioritise traffic: higher priority queues wait a shorter silence (called the AIFSN, Arbitrated Interframe Space Number), and pick up a random value in a smaller number range



AIFS, CW… Okay, it's complicated

- Arbitration inter-frame spacing (AIFS) prioritises one AC over the other by shortening or expanding the time a wireless node wait before transmit.
- AIFSN is different for Voice (2), Video (2), Best Effort (3) and Background (7)
- Short slot time = 9 µs (for 802.11a/g/n, 802.11b has a longer one)
- SIFS = 10 µs for 2.4 GHz, 16 µs for 5 GHz
- The time you wait before counting down is:

  AIFS = SIFS + AIFSN x Slot Time

Example:
Voice in 802.11an: 16 + (2 x 9) = 34 µs
Bckd with 802.11gn: 10 + (7x9) = 73 µs

- Then, pick a number between CwMin and CwMax (usually start with CwMin)

AC	AIFSN	AIFS (2.4 GHz)	AIFS (5 GHz)	CwMin	CwMax
VO	2	28	34	3	7
VI	2	28	34	7	15
BE	3	37	43	15	1023
BK	7	73	79	15	1023

TXOP

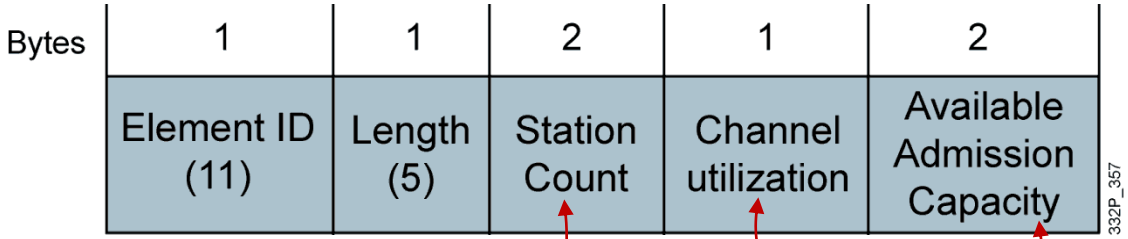
- IFS, ACK and other overheads waste time
- 802.11e/WMM allows you to send more than one frame, when you can access the medium
- The AP sets a TXOP value to tell you for how long you can send in a row
  - This is set in ms, the time you take to send, regardless of the data rate you use and the size of your frame

AC	TXOP (in ms)
VO	1.504
VI	3.008
BE	0
BK	0

0 means that you can send only one frame at a time

QBSS IE

- Sent by WMM APs in beacons and probe responses
- Helps clients decide which AP to associate or roam to
- No real interaction between client and AP



How many stations in the cell

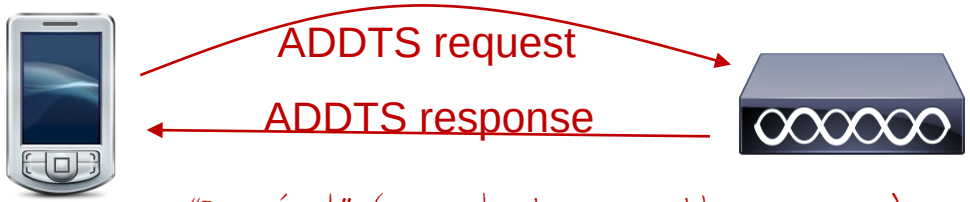
Percentage of time the channel was seen as busy by the AP

How many slots are still available for stations using ACM

Last Brick, TSPEC

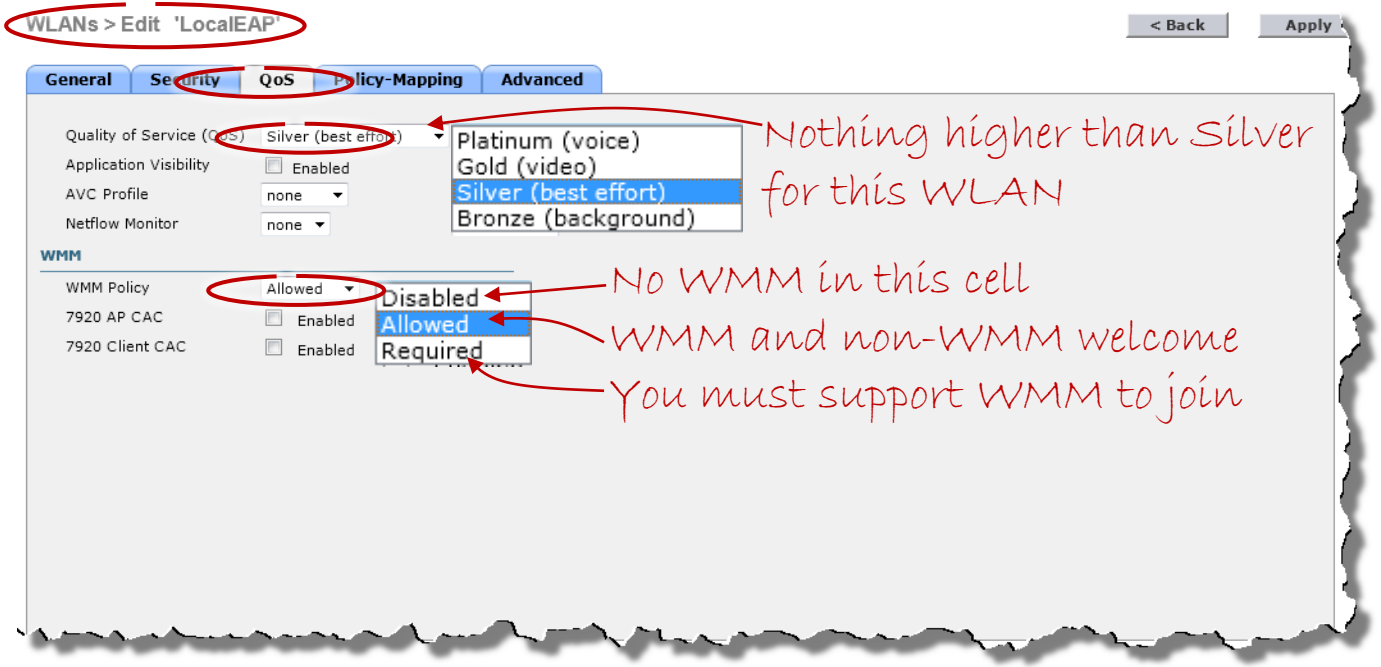
- 802.11e/WMM allows Access Control Mandatory for some queues
- When ACM is on, clients are supposed to ask for permission before sending new traffic flow

I need to place a call, this is my traffic specification (packet size, rate up and down, etc.



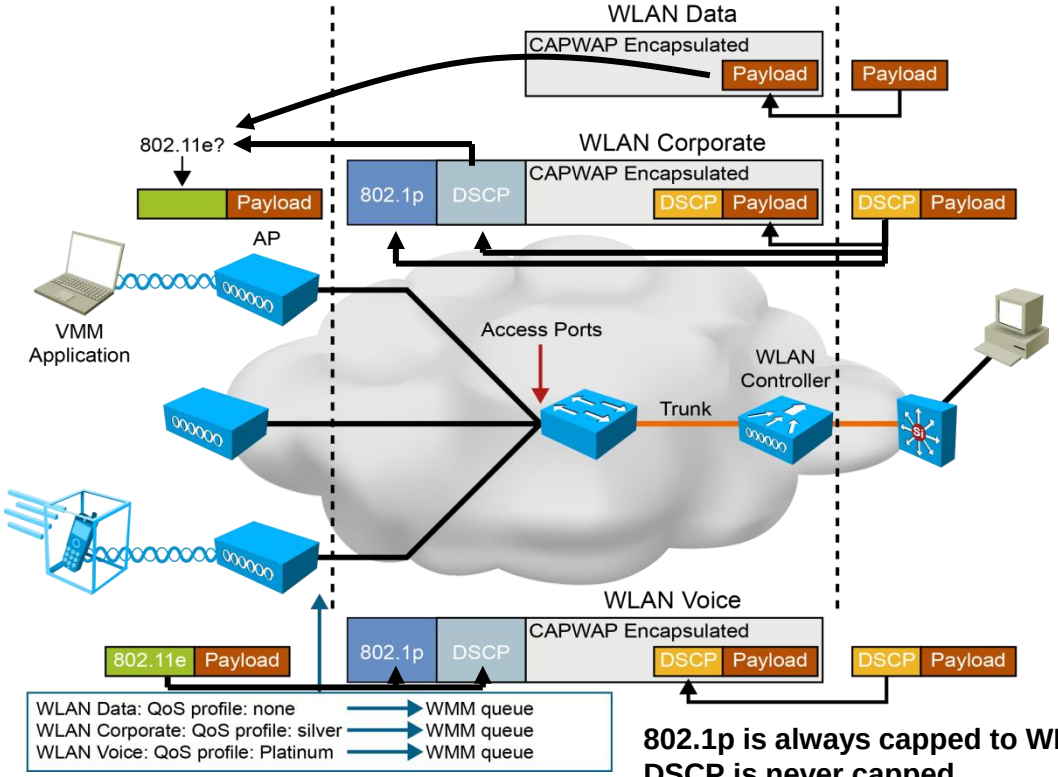
"Denied" (maybe try another queue)
Or "Accepted", your traffic is deduced from my available bandwidth

Assigning a QoS Profile to a WLAN



- QoS profile is the highest QoS level allowed in and to the cell
- If you want 802.11n/802.11ac speeds, allow/require WMM!

802.11e Traffic Priority



802.1p is always capped to WLAN QoS profile, DSCP is never capped

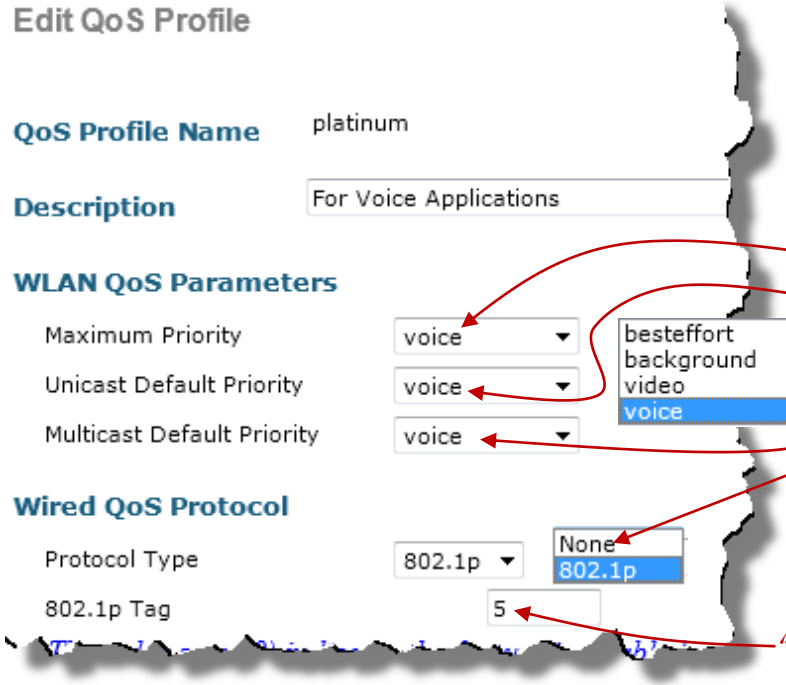
Untagged wired traffic is sent which 802.11e QoS?

QoS Packet AVVID Mappings

AVVID 802.1p UP-Based Traffic Type	AVVID IP DSCP	AVVID 802.1p UP	IEEE 802.11e UP
Reserved (Network Control)	56	7	7
Reserved	48	6	
Voice	46 (EF)	5	6
Video	34 (AF41)	4	5
Voice Control	24 (CS3)	3	4
Gold Background	18 (AF 21)	2	2
Silver Background	10 (AF 11)	1	1
Best Effort	0 (BE)	0	0, 3

Setting QoS for the AP-WLC Part and Defaults

- Wireless > QoS > Profiles > Edit



Max allowed Queue for tagged traffic

Queue for untagged traffic

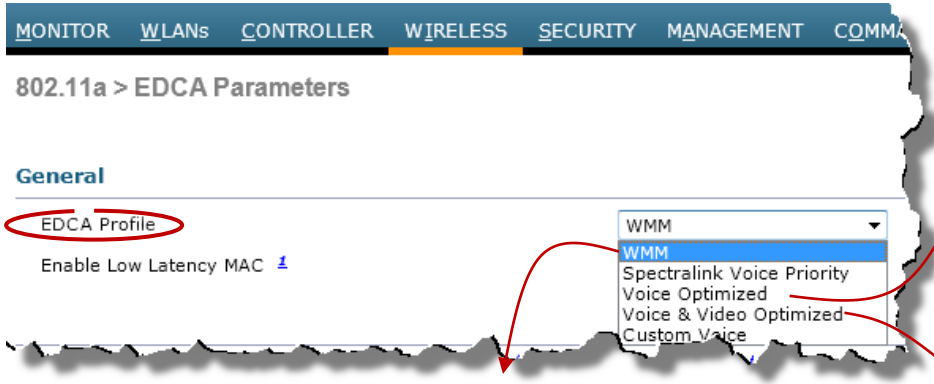
Queue for multicast traffic

Default is None -> traffic is not tagged between WLC and AP (not a good idea if you need QoS)

"Platinum" 802.1p tag between WLC-AP

Optimising WMM

- Wireless > 802.11a | 802.11bg > EDCA Parameters



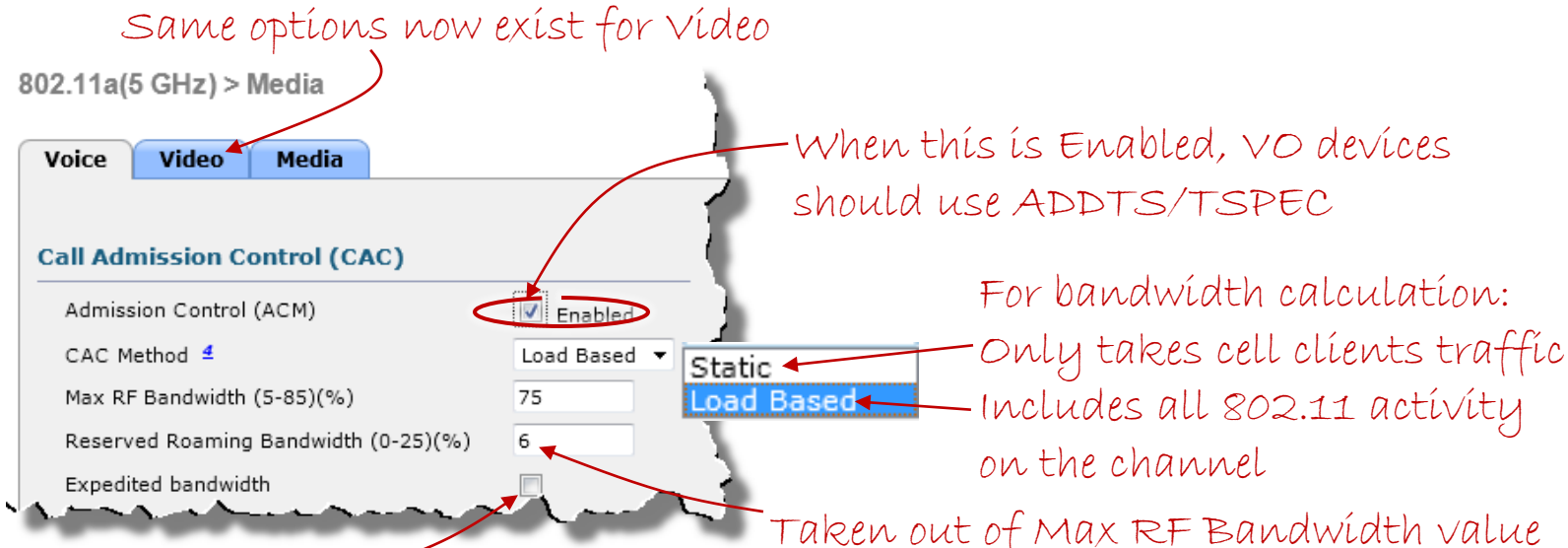
AC	AIFSN	CwMin	CwMax	TXOP
VO	2	2	3	47
VI	2	3	4	94
BE	3	4	10	0
BK	7	4	10	0

AC	AIFSN	CwMin	CwMax	TXOP
VO	2	2	4	0
VI	5	3	5	0
BE	5	6	10	0
BK	12	8	10	0

AC	AIFSN	CwMin	CwMax	TXOP
VO	2	2	4	0
VI	5	3	5	0
BE	12	6	10	0
BK	12	8	10	0

ACM

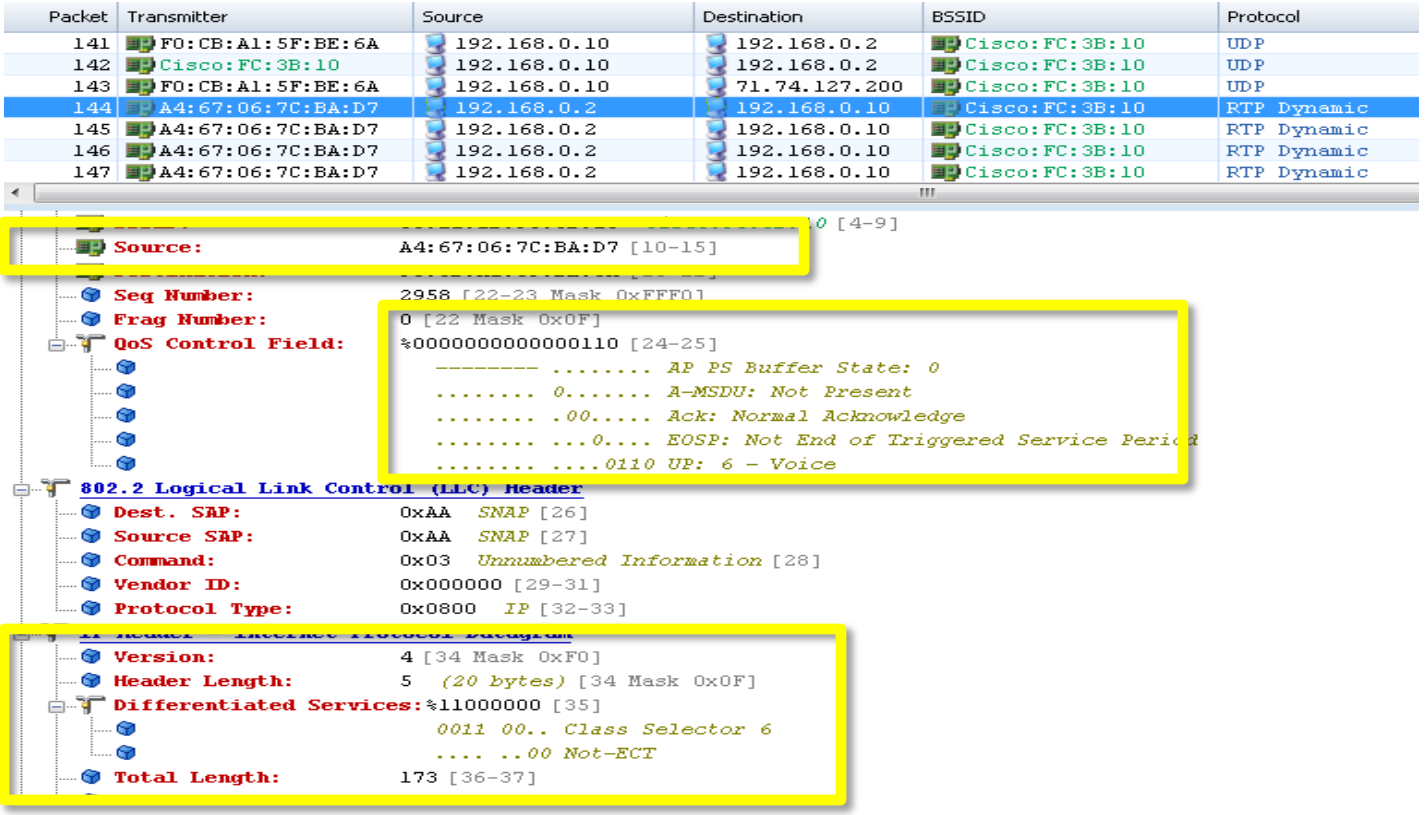
- Wireless > 802.11a | 802.11bg > Media



Where are We now?

- We have:
  - ✓ QoS Profile tagging all traffic, between WLC-AP and to the cell
  - ✓ QoS profile applied to the WLAN
  - ✓ EDCA optimised for voice/video
  - ✓ CAC to block excessive flows and guarantee ongoing calls quality
- Let' see if we are ready…

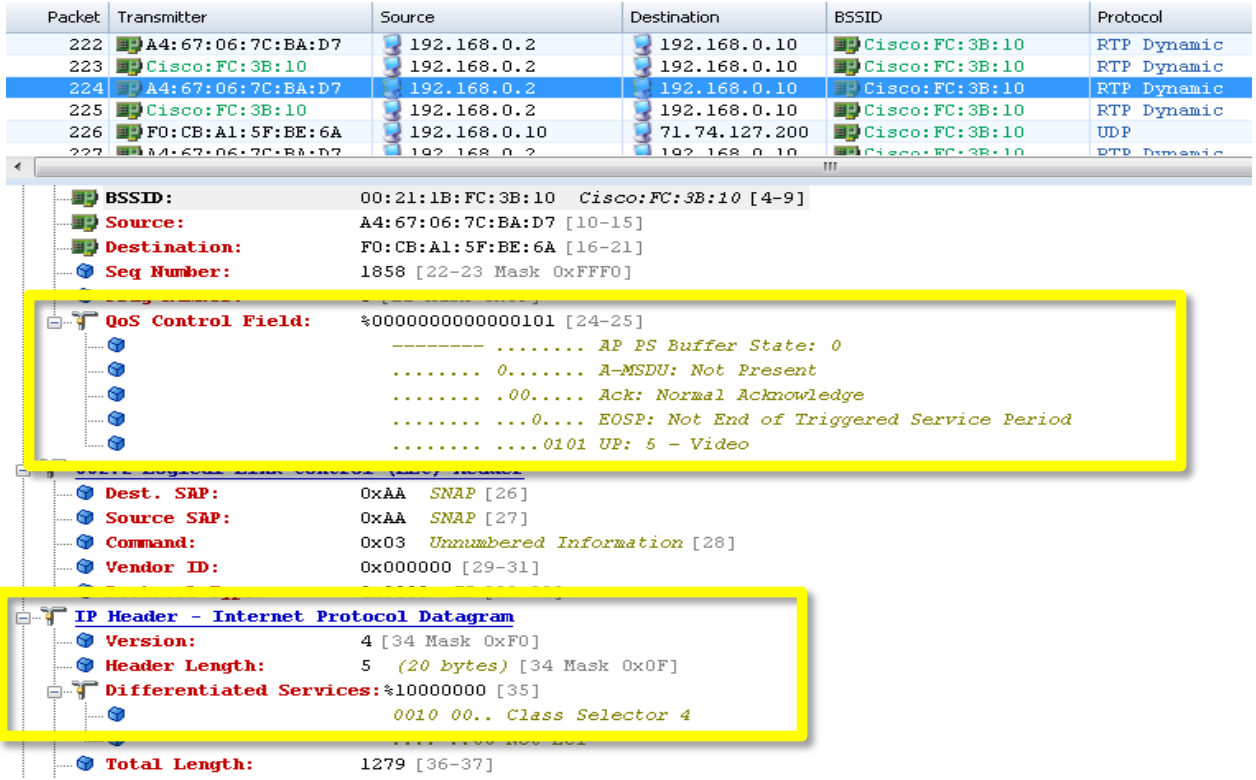
FaceTime Voice Packet: iPad



Packet	Transmitter	Source	Destination	BSSID	Protocol
141	F0:CB:A1:5F:BE:6A	192.168.0.10	192.168.0.2	Cisco:FC:3B:10	UDP
142	Cisco:FC:3B:10	192.168.0.10	192.168.0.2	Cisco:FC:3B:10	UDP
143	F0:CB:A1:5F:BE:6A	192.168.0.10	71.74.127.200	Cisco:FC:3B:10	UDP
144	A4:67:06:7C:BA:D7	192.168.0.2	192.168.0.10	Cisco:FC:3B:10	RTP Dynamic
145	A4:67:06:7C:BA:D7	192.168.0.2	192.168.0.10	Cisco:FC:3B:10	RTP Dynamic
146	A4:67:06:7C:BA:D7	192.168.0.2	192.168.0.10	Cisco:FC:3B:10	RTP Dynamic
147	A4:67:06:7C:BA:D7	192.168.0.2	192.168.0.10	Cisco:FC:3B:10	RTP Dynamic

```
Source:                 A4:67:06:7C:BA:D7 [10-15]
Seq Number:             2958 [22-23 Mask 0xFFF0]
Frag Number:            0 [22 Mask 0x0F]
QoS Control Field:      %0000000000000110 [24-25]
                          -------- ........ AP PS Buffer State: 0
                          ........ 0....... A-MSDU: Not Present
                          ........ .00..... Ack: Normal Acknowledge
                          ........ ...0.... EOSP: Not End of Triggered Service Peri
                          ........ ....0110 UP: 6 - Voice
802.2 Logical Link Control (LLC) Header
Dest. SAP:              0xAA  SNAP [26]
Source SAP:             0xAA  SNAP [27]
Command:                0x03  Unnumbered Information [28]
Vendor ID:              0x000000 [29-31]
Protocol Type:          0x0800  IP [32-33]
Version:                4 [34 Mask 0xF0]
Header Length:          5  (20 bytes) [34 Mask 0x0F]
Differentiated Services:%11000000 [35]
                          0011 00.. Class Selector 6
                          .... ..00 Not-ECT
Total Length:           173 [36-37]
```

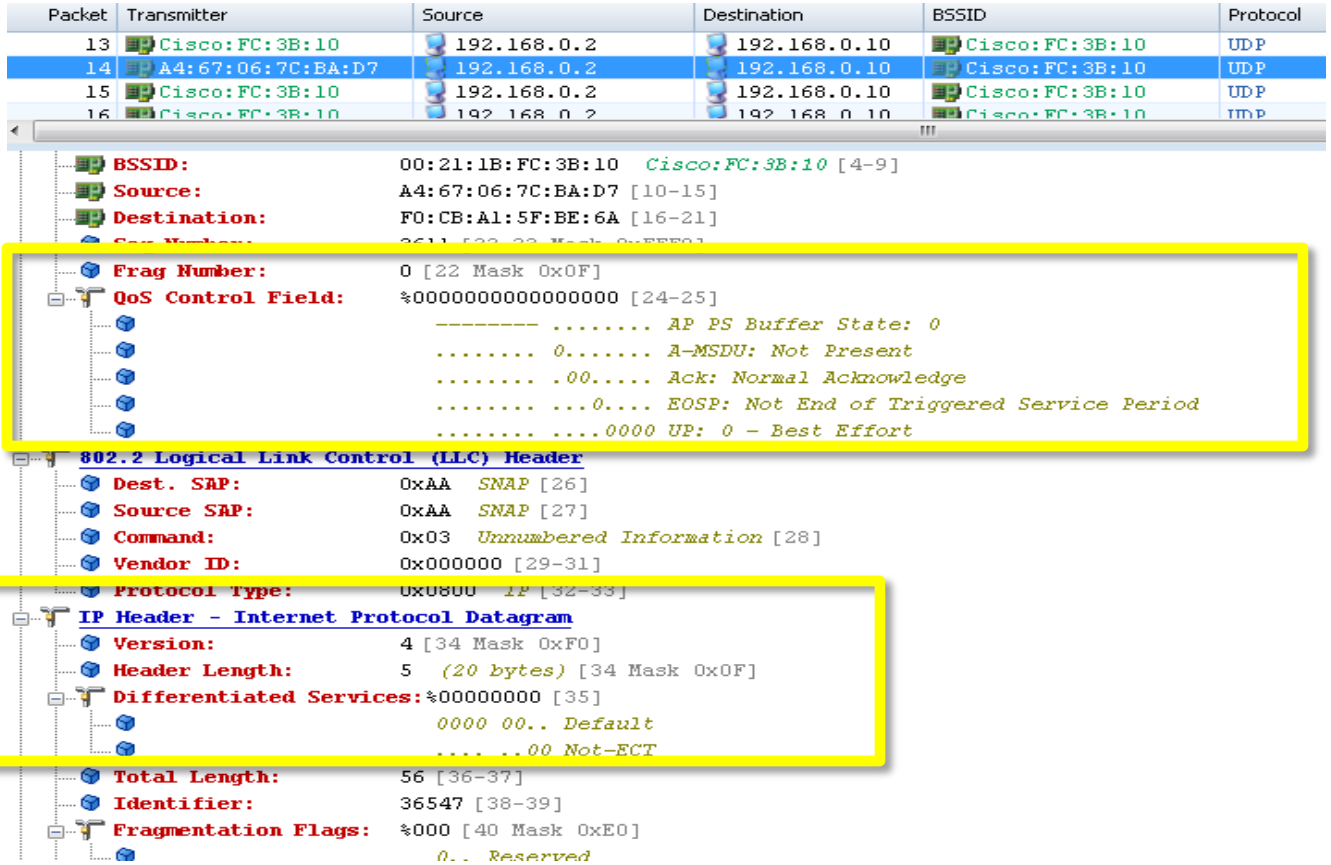
FaceTime Voice Packet: iPad



Packet	Transmitter	Source	Destination	BSSID	Protocol
222	A4:67:06:7C:BA:D7	192.168.0.2	192.168.0.10	Cisco:FC:3B:10	RTP Dynamic
223	Cisco:FC:3B:10	192.168.0.2	192.168.0.10	Cisco:FC:3B:10	RTP Dynamic
224	A4:67:06:7C:BA:D7	192.168.0.2	192.168.0.10	Cisco:FC:3B:10	RTP Dynamic
225	Cisco:FC:3B:10	192.168.0.2	192.168.0.10	Cisco:FC:3B:10	RTP Dynamic
226	F0:CB:A1:5F:BE:6A	192.168.0.10	71.74.127.200	Cisco:FC:3B:10	UDP

```
BSSID:                  00:21:1B:FC:3B:10  Cisco:FC:3B:10 [4-9]
Source:                 A4:67:06:7C:BA:D7 [10-15]
Destination:            F0:CB:A1:5F:BE:6A [16-21]
Seq Number:             1858 [22-23 Mask 0xFFF0]
QoS Control Field:      %0000000000000101 [24-25]
                        -------- ........ AP PS Buffer State: 0
                        ........ 0....... A-MSDU: Not Present
                        ........ .00..... Ack: Normal Acknowledge
                        ........ ...0.... EOSP: Not End of Triggered Service Period
                        ........ ....0101 UP: 5 - Video
Dest. SAP:              0xAA  SNAP [26]
Source SAP:             0xAA  SNAP [27]
Command:                0x03  Unnumbered Information [28]
Vendor ID:              0x000000 [29-31]
IP Header - Internet Protocol Datagram
Version:                4 [34 Mask 0xF0]
Header Length:          5  (20 bytes) [34 Mask 0x0F]
Differentiated Services:%10000000 [35]
                        0010 00.. Class Selector 4
Total Length:           1279 [36-37]
```

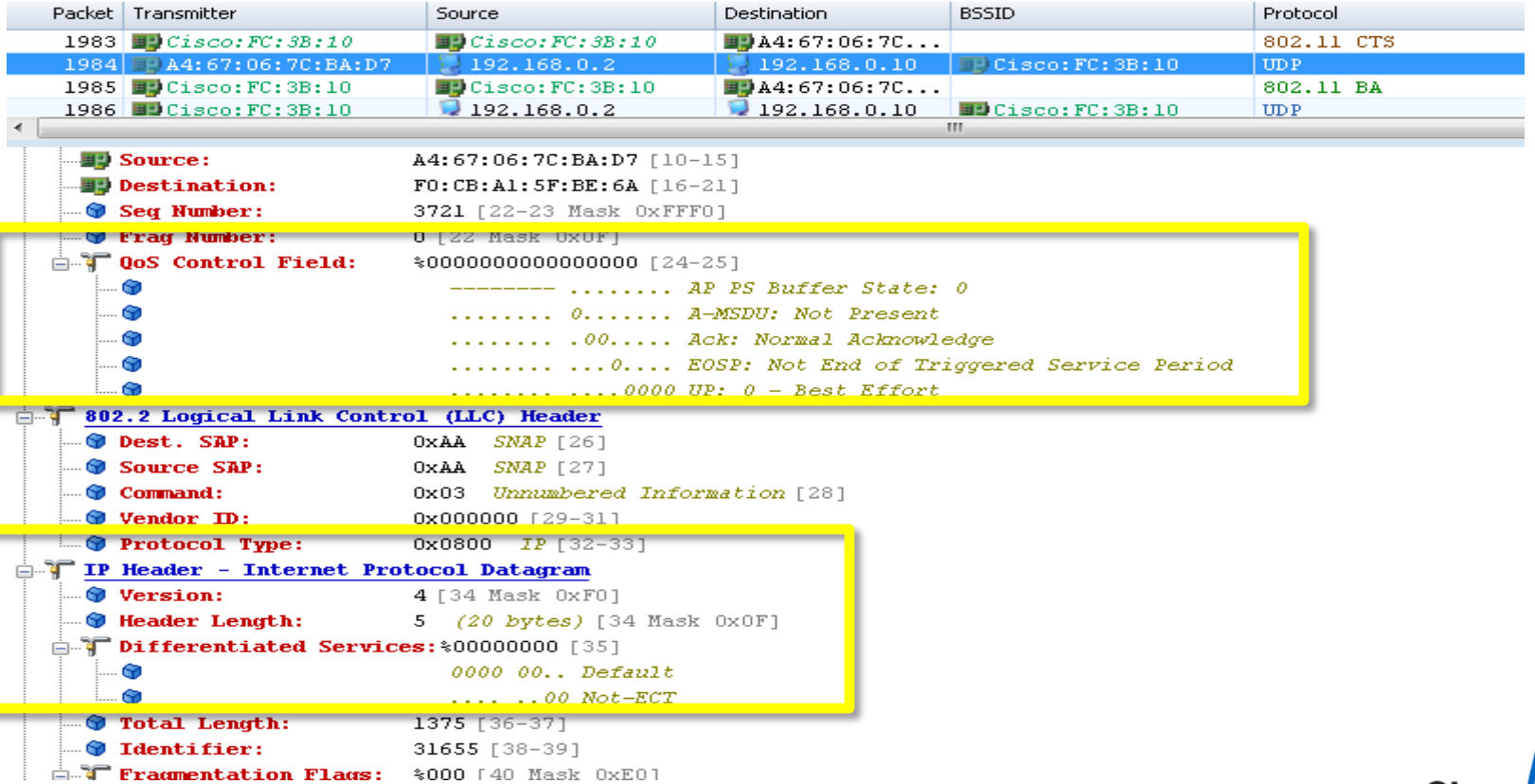
Skype Voice Packet – iPad



Packet	Transmitter	Source	Destination	BSSID	Protocol
13	Cisco:FC:3B:10	192.168.0.2	192.168.0.10	Cisco:FC:3B:10	UDP
14	A4:67:06:7C:BA:D7	192.168.0.2	192.168.0.10	Cisco:FC:3B:10	UDP
15	Cisco:FC:3B:10	192.168.0.2	192.168.0.10	Cisco:FC:3B:10	UDP
16	Cisco:FC:3B:10	192.168.0.2	192.168.0.10	Cisco:FC:3B:10	UDP

```
BSSID:                    00:21:1B:FC:3B:10  Cisco:FC:3B:10 [4-9]
Source:                   A4:67:06:7C:BA:D7 [10-15]
Destination:              F0:CB:A1:5F:BE:6A [16-21]
Frag Number:              0 [22 Mask 0x0F]
QoS Control Field:        %0000000000000000 [24-25]
                          --------  ........  AP PS Buffer State: 0
                          ........  0.......  A-MSDU: Not Present
                          ........  .00.....  Ack: Normal Acknowledge
                          ........  ...0....  EOSP: Not End of Triggered Service Period
                          ........  ....0000  UP: 0 - Best Effort
802.2 Logical Link Control (LLC) Header
Dest. SAP:                0xAA  SNAP [26]
Source SAP:               0xAA  SNAP [27]
Command:                  0x03  Unnumbered Information [28]
Vendor ID:                0x000000 [29-31]
Protocol Type:            0x0800  IP [32-33]
IP Header - Internet Protocol Datagram
Version:                  4 [34 Mask 0xF0]
Header Length:            5  (20 bytes) [34 Mask 0x0F]
Differentiated Services:  %00000000 [35]
                          0000 00..  Default
                          .... ..00  Not-ECT
Total Length:             56 [36-37]
Identifier:               36547 [38-39]
Fragmentation Flags:      %000 [40 Mask 0xE0]
                          0..  Reserved
```

Skype Voice Packet – iPad

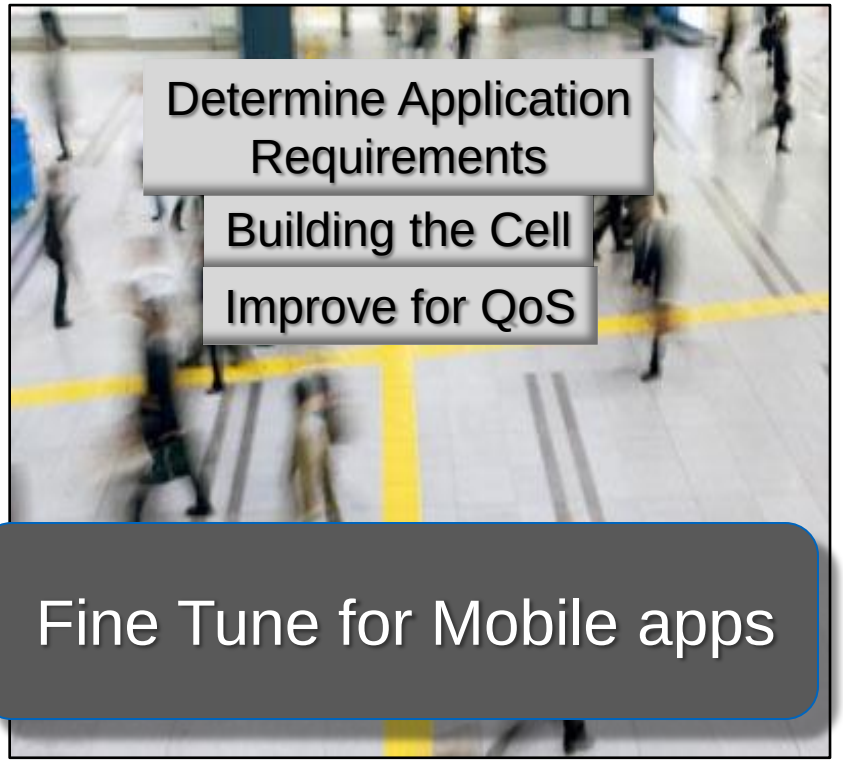


Packet	Transmitter	Source	Destination	BSSID	Protocol
1983	Cisco:FC:3B:10	Cisco:FC:3B:10	A4:67:06:7C...		802.11 CTS
1984	A4:67:06:7C:BA:D7	192.168.0.2	192.168.0.10	Cisco:FC:3B:10	UDP
1985	Cisco:FC:3B:10	Cisco:FC:3B:10	A4:67:06:7C...		802.11 BA
1986	Cisco:FC:3B:10	192.168.0.2	192.168.0.10	Cisco:FC:3B:10	UDP

What are we missing?

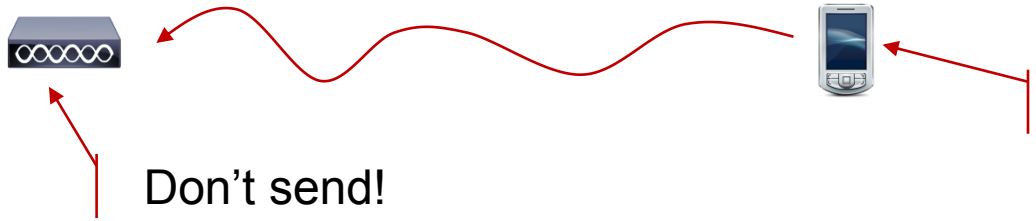
- If you are an OS vendor, which application would you allow to get higher priority than the others? What are the risks?
- From the wireless infrastructure side, the conclusion is that we should enable QoS… but can't trust that all applications on all devices will use proper marking.
- So… what else can we do to improve traffic quality for our mobile applications?

Design Steps



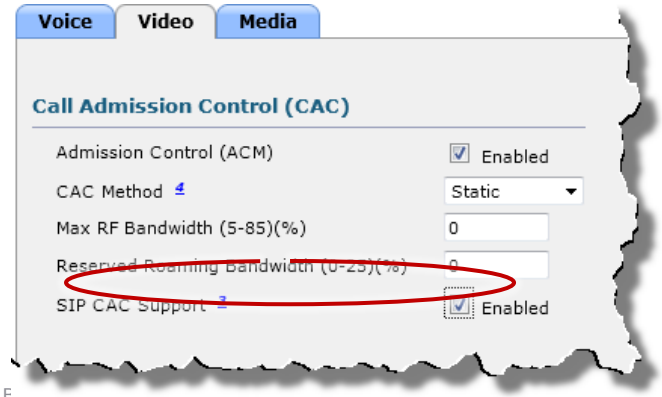
Let's Think the Problem in Terms of Directions

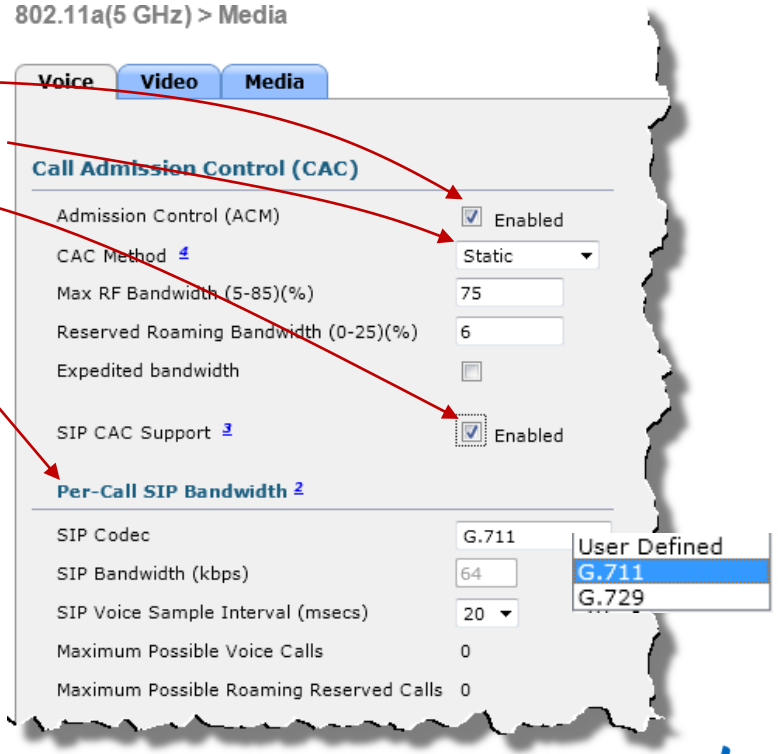
- In a standard cell, 70% of traffic is downstream (from AP to client)
- 30% is upstream
- We can definitely control downstream, especially as 802.11n/ac stations are necessarily WMM
- Can we control the upstream? Not directly, but we may have an indirect way of controlling it…



If your Traffic is Targeted

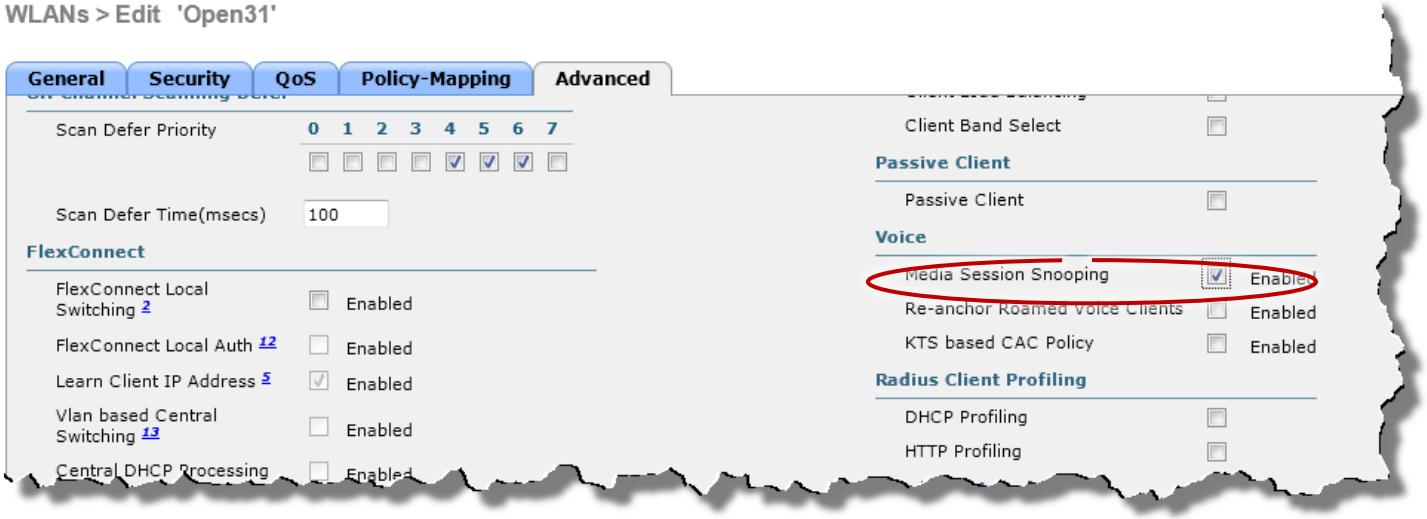
- For example, you want to prioritise SIP:
  1. Enable ACM
  2. Make sure to use Static (not Load-based)
  3. Check SIP CAC Support
  4. Determine the expected SIP specs
- You can also prioritise SIP VIDEO
  - Target is Jabber or Facetime





If your Traffic is Targeted

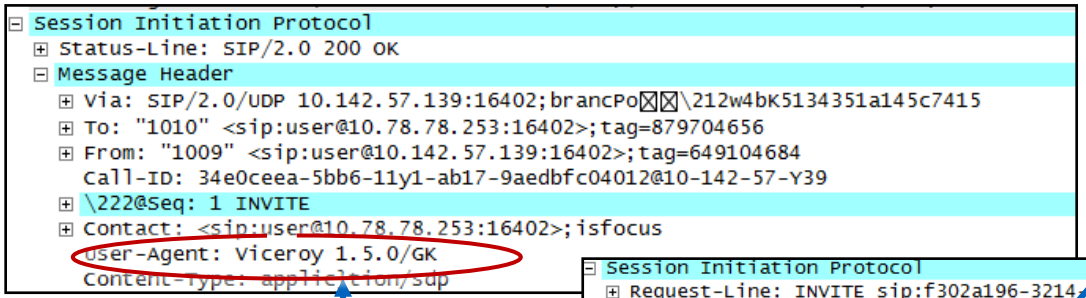
- For example, you want to prioritise SIP:
  5. Enable SIP support on the WLAN:



SIP Audio, SIP Video (Jabber, Facetime)

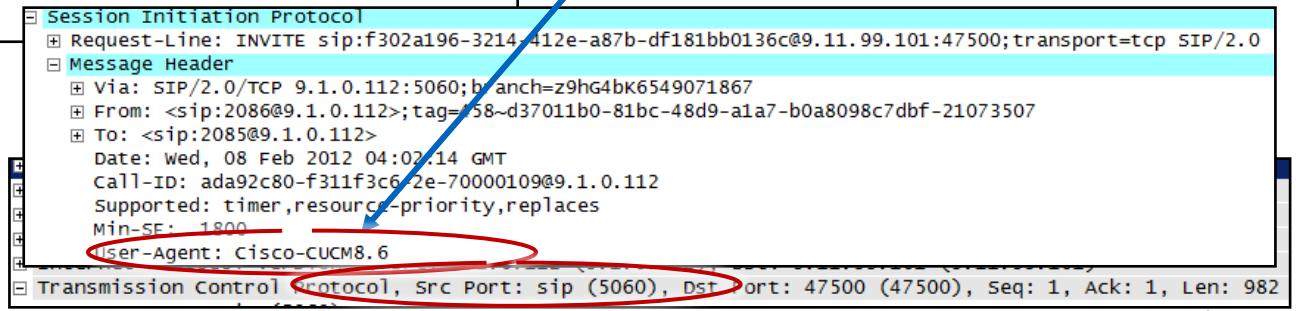
How do they do it?:

- The AP uses the port (SIP audio or video), and also use the User-agent field (video) to further identify the SIP type:



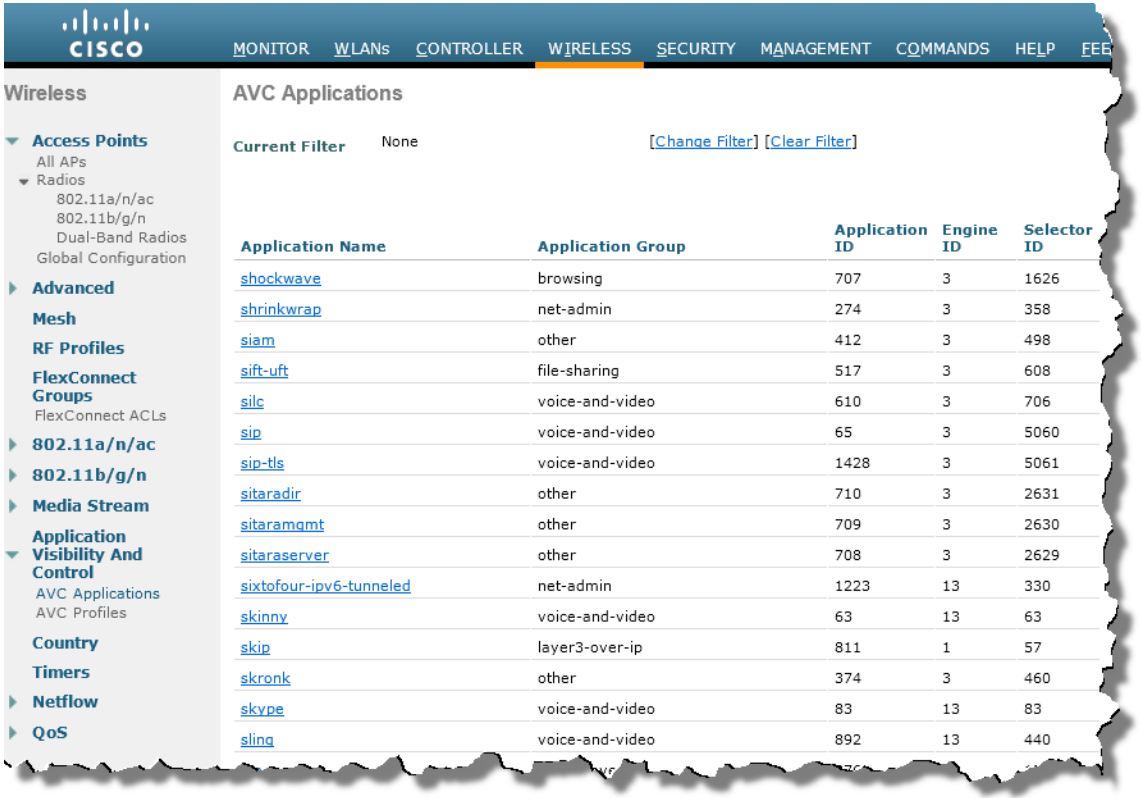
Apple (outgoing call)

Can't tell (incoming call from CUCM), use ports



If you have Several Traffic Types to Target: Use Application Visibility and Control

- Internal application recognition engine based on NBAR2
- More than 1000 applications recognised, including Netflix, Skype, Lync audio, Lync video viber, ventrilo, etc.
- Protocol Pack 6.3 breaks out Jabber audio, video, control, im, … etc.

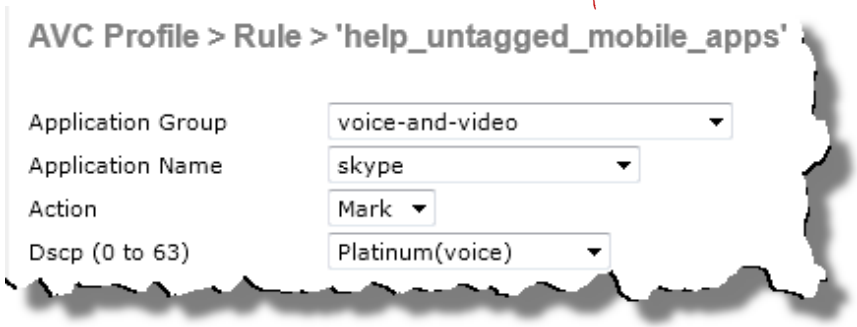


Application Visibility and Control

- With AVC, you can create rules to mark untagged applications (but also to permit or deny some application traffic!):

1. Create a new policy
2. Add rules, including what application to recognise, and what to do with it:

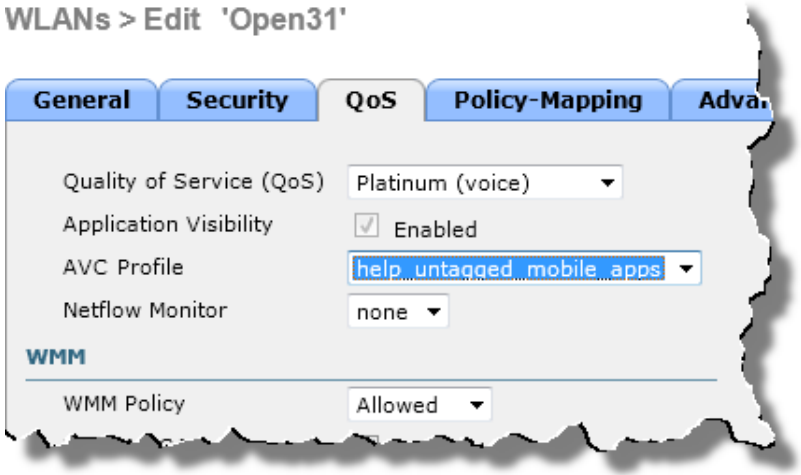
Wireless > AVC > AVC Profiles > New

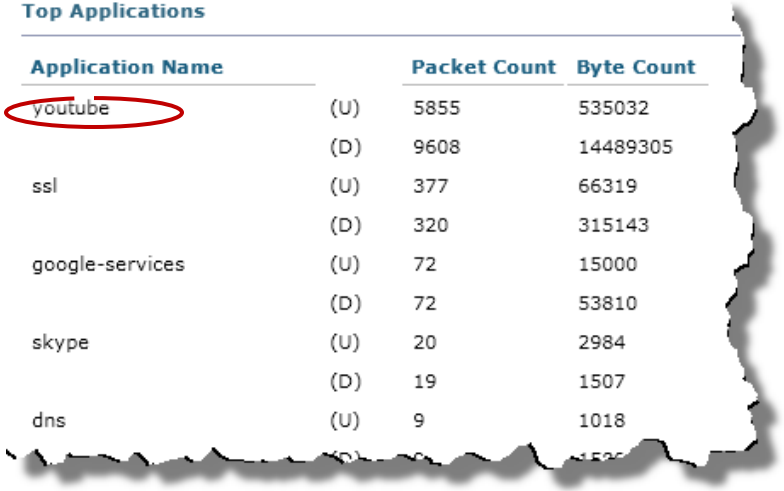


- Marking application will help prioritisation between AP and WLC, and from AP to the cell

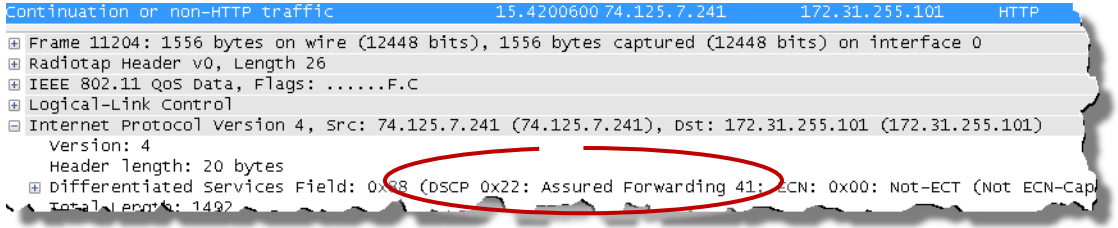
Application Visibility and Control

3. Apply your policy to the WLAN:





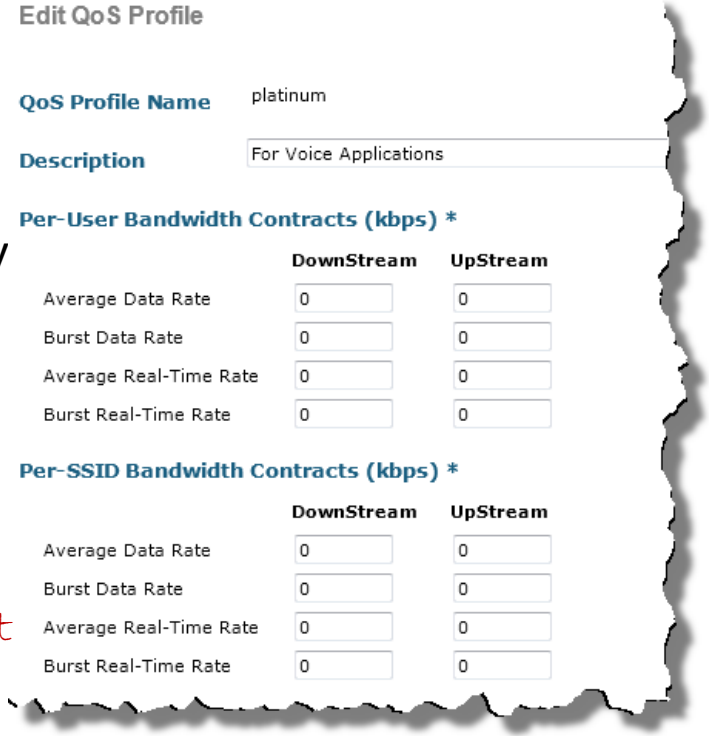
4. Watch your traffic:



Bandwidth Control – per User

- You can also control upstream and downstream bandwidth consumption:

- For each QoS profile, per user or per SSID
- The limitation will apply to each WLAN to which you apply the QoS profile

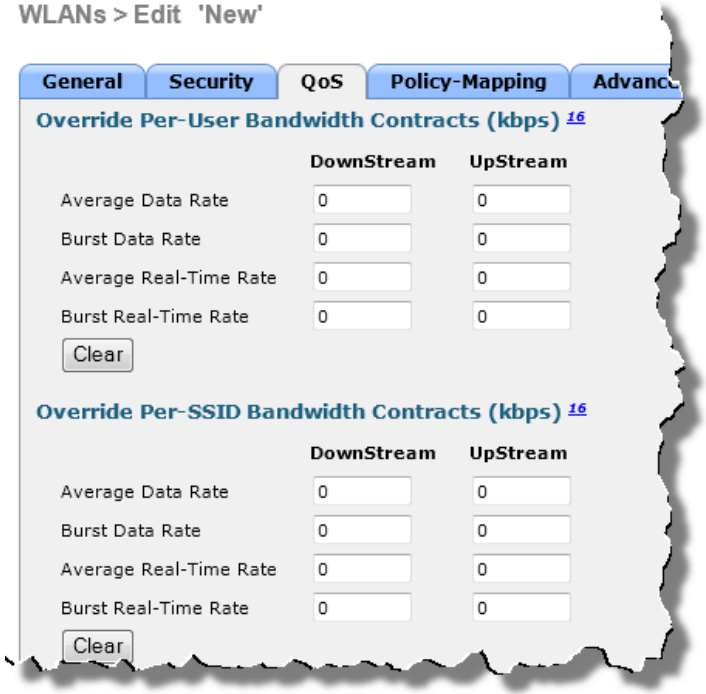


Wireless > QoS > Profiles > Edit

Bandwidth Control – per User

- You can also control upstream and downstream bandwidth consumption:

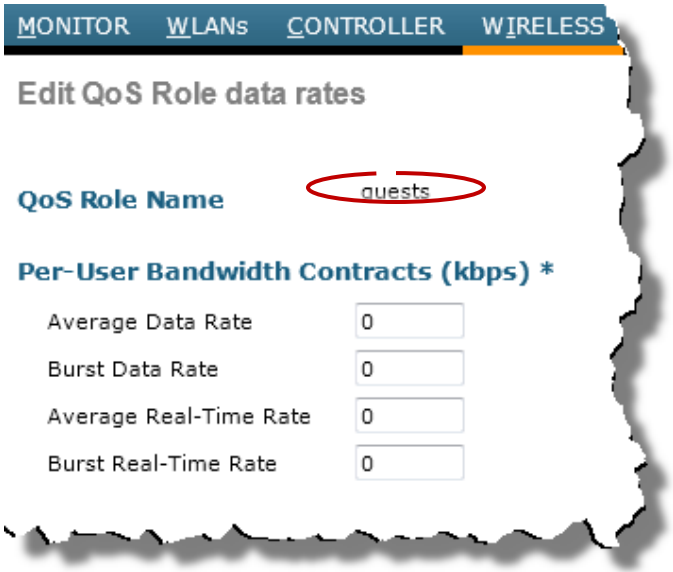
- But if QoS profile is not right for one WLAN, you can override for that WLAN!



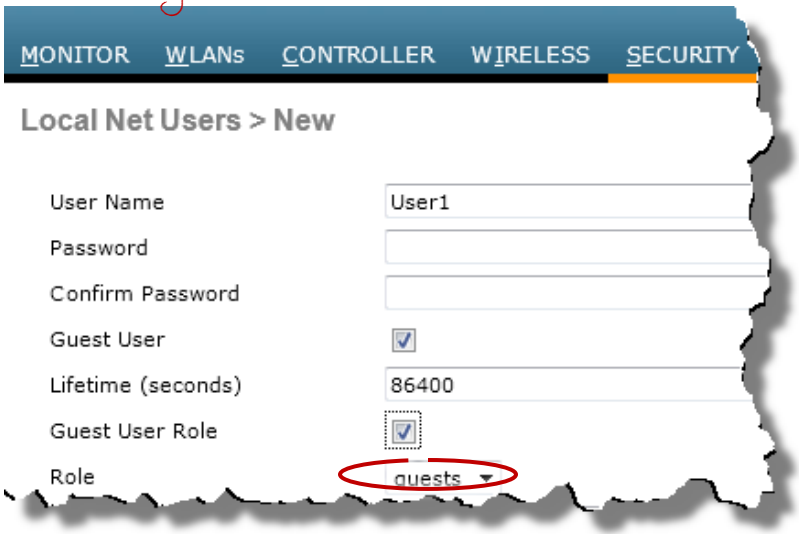
Bandwidth Control – per User

- You can also control upstream and downstream bandwidth consumption:
- There is even a specific bandwidth control for Webauth WLAN users (guests)

Wireless > QoS > Role > New



Security > Local Net User > New

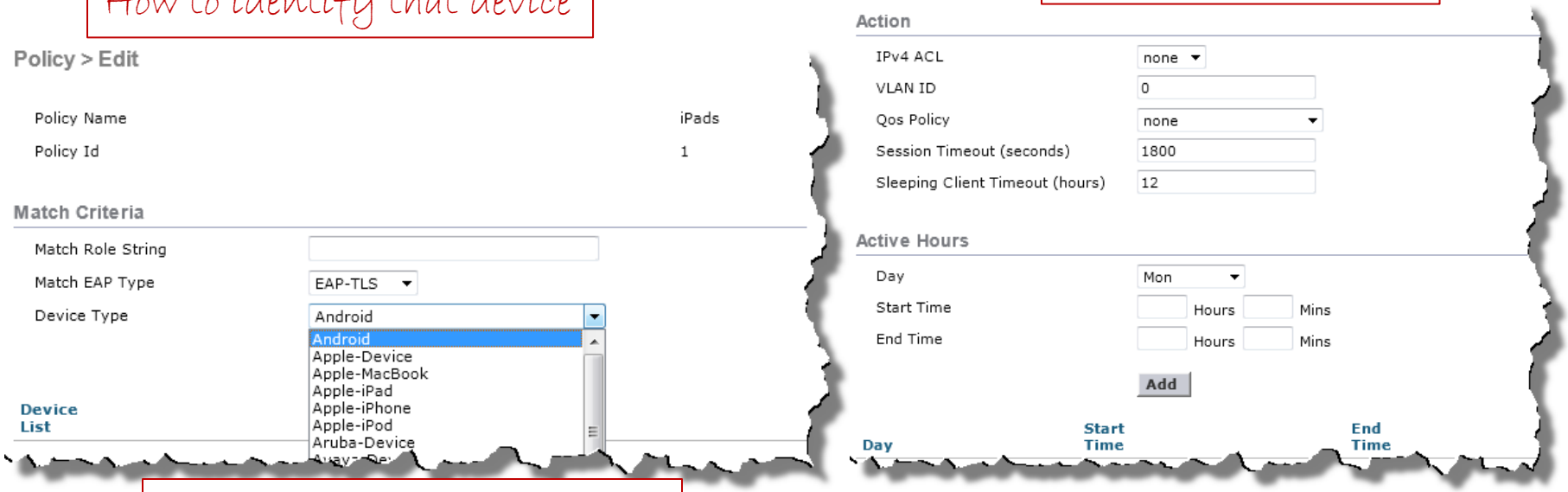


Bandwidth Control – per Device Type

- You can also identify connecting devices, from the WLC or though Cisco ISE, and create a policy based on what they are:

How to identify that device

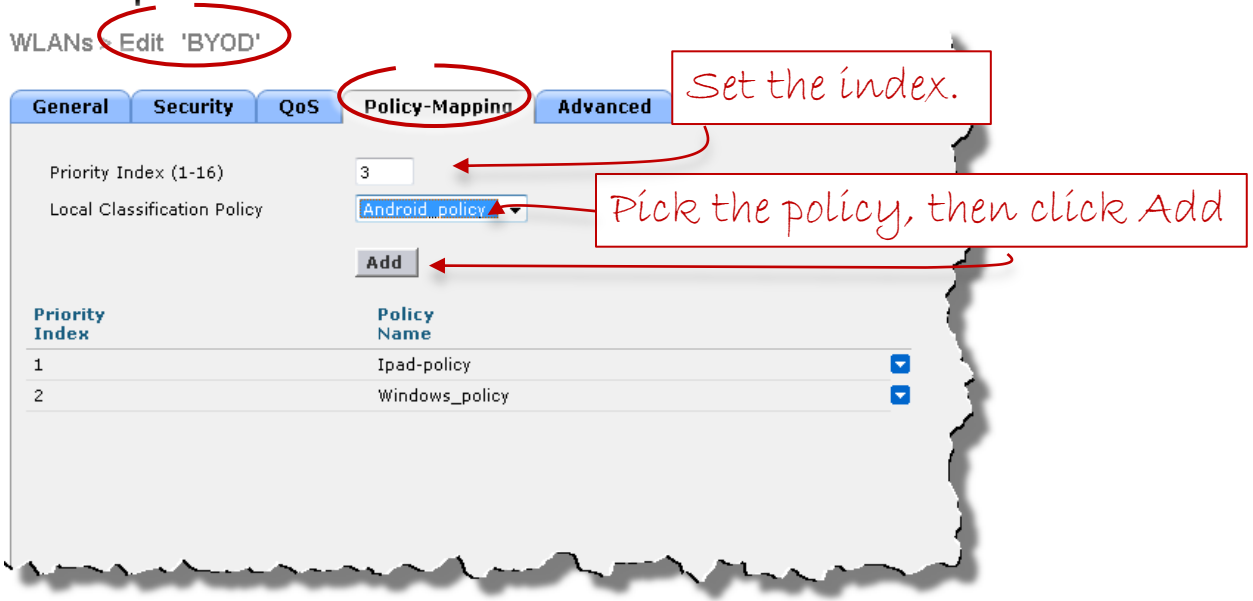
What policy to apply



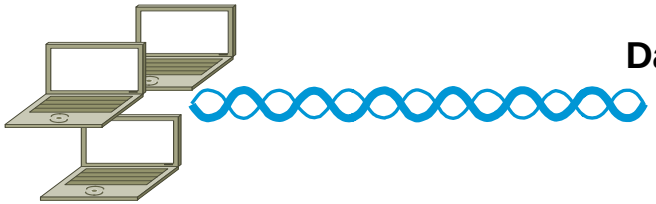
Close to 100 types on WLC

Configuring Policies

- You can then apply the policies to the WLANs, in the order you want them to be applied, up to 16 policies per WLAN:
- Each policy can group several devices



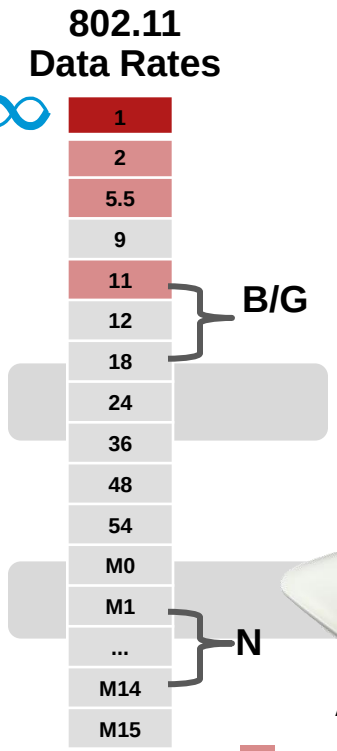
Video Multicast Delivery Challenges



Video Impact

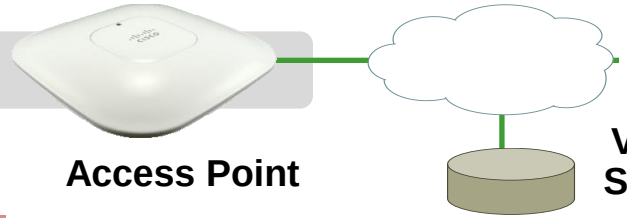
Choppy, Unreliable Video

- Video streaming does not utilise 802.11 N High Throughput data rates
- Heavy utilisation of channel due to high rate of slower packets
- Video delivery is not reliable causing poor Quality of Experience



Technical Challenges

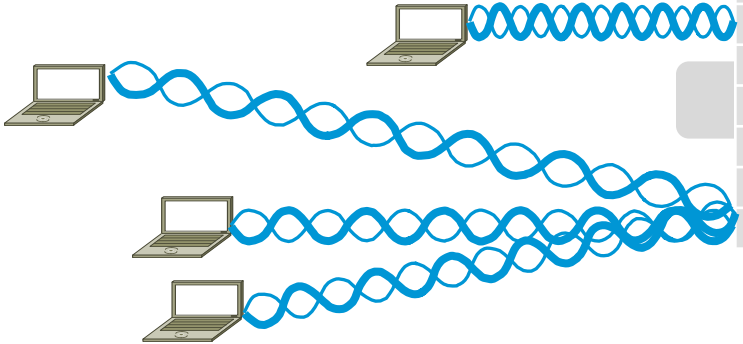
- Multicast packets (UDP) are sent as broadcast packets over the air per 802.11 standard
- Broadcast packets do not use error correction: “fire and forget”
- Broadcast packets are sent at highest basic/mandatory data rate.

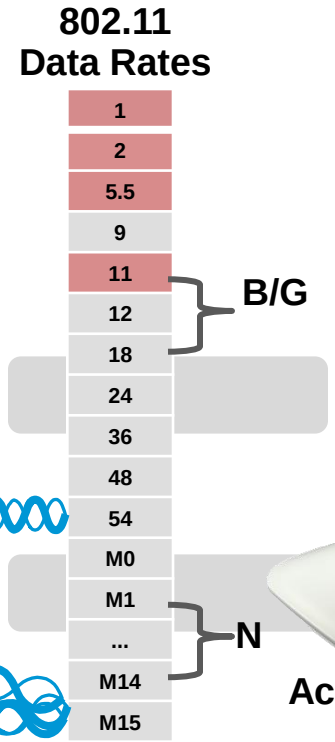


Video Multicast Delivery Solution - VideoStream

Video Impact

- Smooth, Reliable Video delivered to multiple clients
- Quality of Video protected in varying channel load conditions
- Prevents video flooding
- Prioritises Business Video over other video



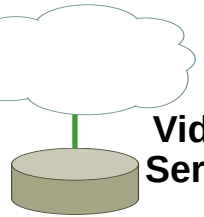


Technical Solution

- IGMP state monitored for each client. We only send video to clients requesting it
- Multicast packets replicated at AP and sent to individual clients at their data rate
- Resource Reservation Control (RRC) is used to prevent channel oversubscription. Works in conjunction with Voice CAC
- Stream Prioritisation ensures important videos take precedence over others
- SAP/SNMP error message created when Channel Subscription is violated

Access Point

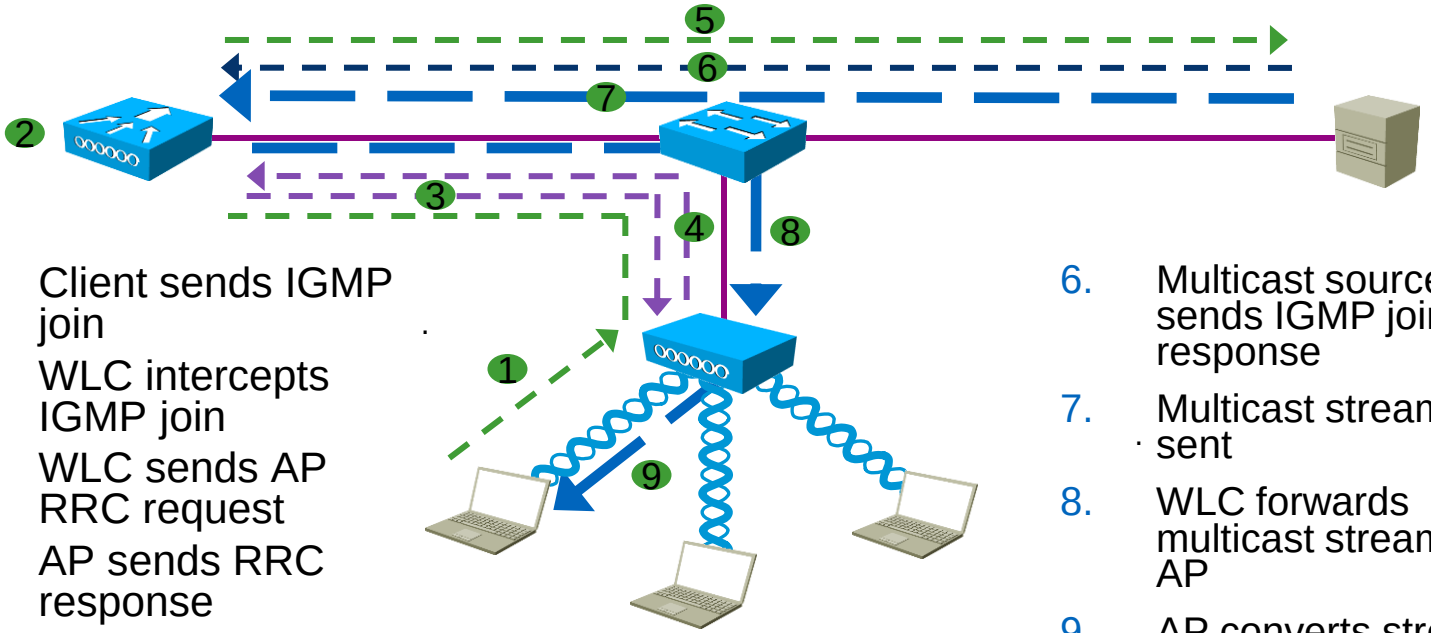
QoS Marked on CAPWAP From WLC



Video Server

Default 802.11B/G mandatory data rates

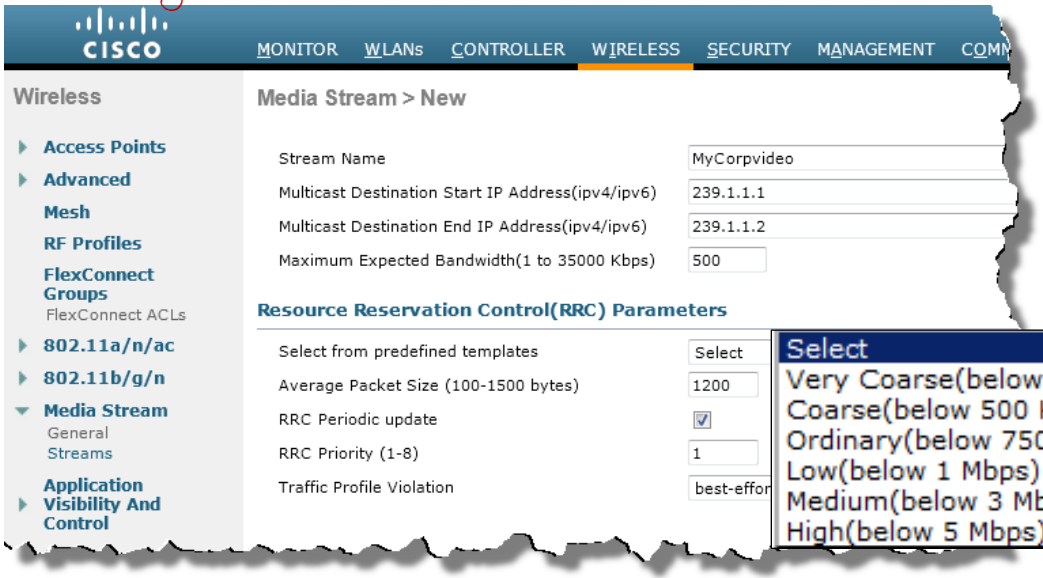
Cisco VideoStream - How Does it Work?



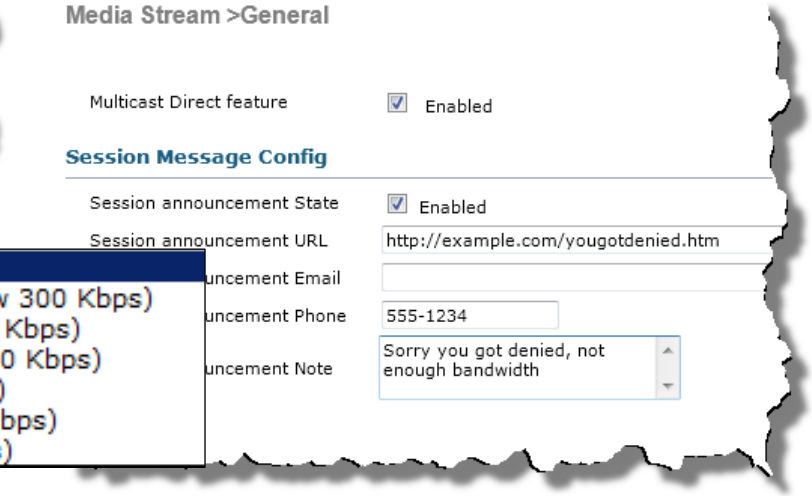
1. Client sends IGMP join
2. WLC intercepts IGMP join
3. WLC sends AP RRC request
4. AP sends RRC response
5. WLC forwards join request
6. Multicast source sends IGMP join response
7. Multicast stream sent
8. WLC forwards multicast stream to AP
9. AP converts stream to unicast and delivers to client

Cisco VideoStream - Configuration

Create your streams

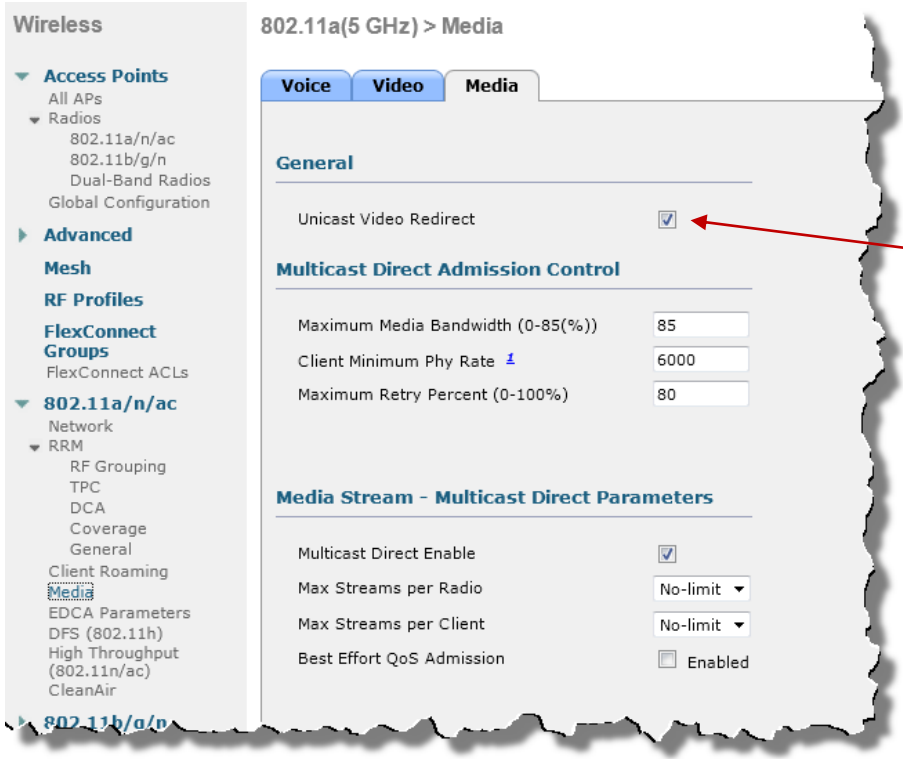


What do you tell your users if you deny a stream



Cisco VideoStream - Configuration

Fine tune Video BW consumption



- Do not forget to enable VideoStream:
- Globally (Wireless > Media Stream > General > Multicast Direct)
- Or per band

Roaming in 802.11 and Challenges

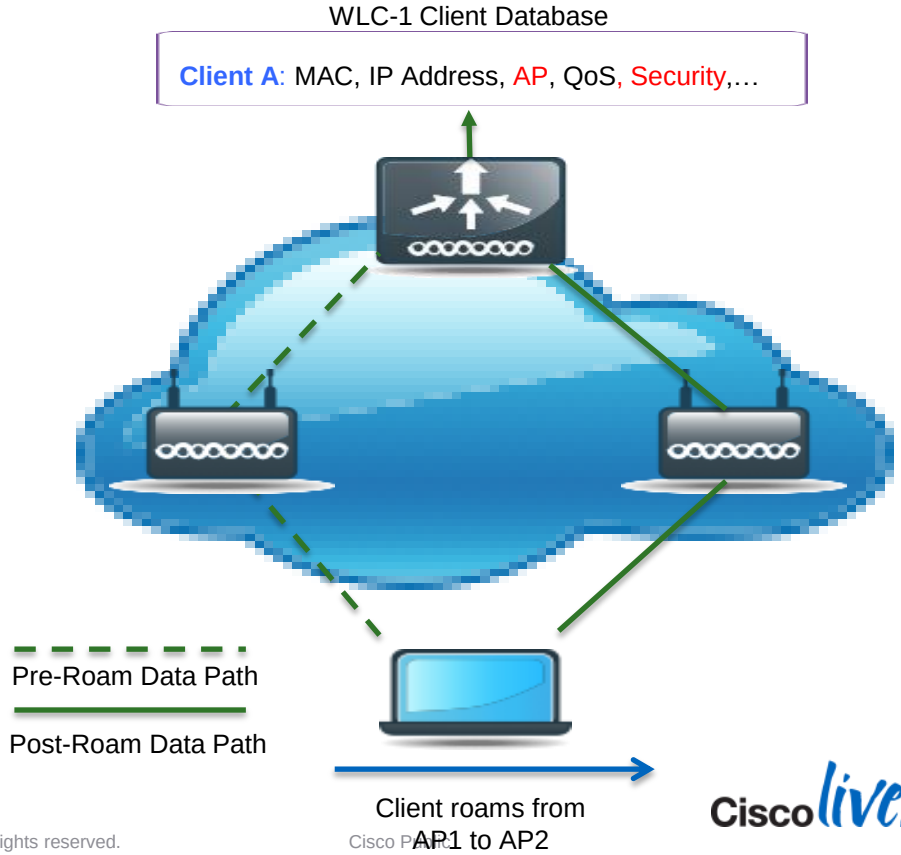
- Moving association from one AP to another with minimum disruption to service
- Meeting the roaming requirements for applications (e.g. 20-50 milliseconds for voice applications).
- Application should not restart due to IP address changes or IP stack reset.
- Authenticate the roaming client on the new AP within ‘roaming deadline.’
- Apply same authorisation policies (e.g. AAA, QoS, VLAN, ACL)

How Long Does an STA Roam Take?

- Time it takes for:
  - Probe for and select a new AP +
  - Client to disassociate +
  - 802.11 Association +
  - 802.1X/EAP Authentication +
  - Rekeying +
  - IP address (re) acquisition
- All this can be on the order of seconds…

Roaming: Intra-Controller

- Intra-controller roam happens when a STA moves association between APs joined to the same controller
- Client must be re-authenticated and new security session established
- Controller updates client database entry with new AP and appropriate security context
- No IP address refresh needed



Cisco Centralised Key Management (CCKM)

- Cisco introduced CCKM in CCXv2 (pre-802.11i)
- In highly controlled test environments, CCKM roam times consistently measure in 5-8 ms!
- CCKM is most widely implemented in ASDs (e.g., VoWLAN devices)
- WLCs must be in the same mobility group
- CCX-based laptops may not fully support CCKM – depends on supplicant capabilities

PMKID Caching

- Optional component of 802.11i specification
- PMK Security Association (PMKSA) is stored by authenticator
- PMKSA includes:
  - PMKID

    HMAC-SHA1-128 (PMK || BSSID || STA Mac)

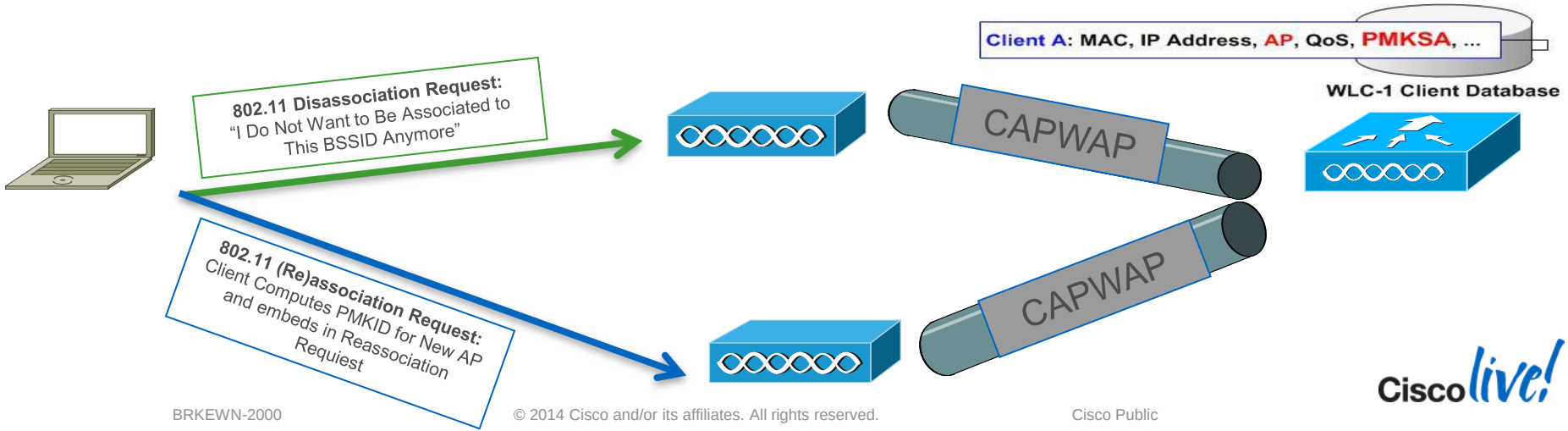
  - Lifetime
  - PMK (32 bytes)
  - BSSID (6 bytes)
  - Client's MAC (6 bytes)
  - AKM (Authentication and Key Management)

OKC/PKC

- Requires client/supplicant support
- Supported in Windows since XP SP2, but NOT in any Apple devices
- Many ASDs support OKC/PKC
- Check on client support for TKIP vs. CCMP
- Enabled by default on WLCs with WPAv2
- Requires WLCs to be in the same mobility group
- Important design note: pre-positioning of roaming clients consumes spots in client DB
- In *highly controlled test environments*, OKC/PKC roam times consistently measure in 10-20 ms

Opportunistic/Proactive Key Caching (OKC/PKC)

1. WLC extracts PMKID from 802.11 (Re)association request
2. WLC computes the new PMKID based on the PMKSA and other information it knows (BSSID, Client MAC)
3. WLC compares values – if a match, full 802.1X/EAP authentication is skipped and WLC & client go directly to the 4-way handshake, and updates PMKSA in client DB
4. If they don't match, WLC sends the STA an EAP-Identity Request to initiate full 802.1X/EAP Authentication



PMKID (Sticky Key) Caching

- Roaming client needs to do full authentication on each new AP
- Client should keep the PMKSA associated with all APs. Memory usage on small client can be costly.
- up to 8 APs will be supported
- Support for Local Mode for AP's ONLY

CLI ONLY:

config wlan security wpa wpa2 pkc-cache enable/disable <wlan-id>

Example:

(5500) >config wlan security wpa wpa2 pkc-cache enable 3

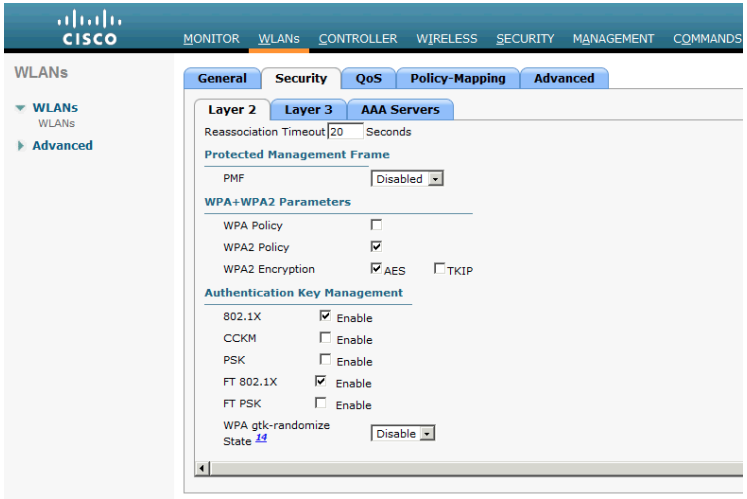
802.11r

- 802.11r is a ratified IEEE standard, based in large part on CCKM
- 802.11r: “Fast (Basic Service Set) BSS Transition”
- Cisco WLCs have implemented 802.11r in 7.2.110.0 and FlexConnect AP in 7.3
- In *highly controlled test environments*, 802.11r roam times are comparable to CCKM times
- Low adoption rate
- Required for WiFi Voice-Enterprise certification
- Your mileage may vary

802.11r Configuration

- config wlan security **ft** [enable | disable] <wlan-id>
- config wlan security **ft reassociation-timeout** <seconds> <wlan-id>
- config wlan security **ft over-the-ds** <enable/disable> <wlan-id>
- config wlan security wpa akm **ft-psk** [enable | disable] <wlan-id>
- config wlan security wpa akm **ft-802.1X** [enable | disable] <wlan-id>

WLANs > <WLAN id> >
Security > Layer 2



Assisted Roaming - 802.11k

- Client devices can optimise roaming performance and put TX radio to sleep as much as possible to reduce battery usage
  - 802.11k client requests a neighbour report containing information about known neighbour APs that are candidates for a service set transition
  - 802.11k neighbour list reduces the need for active and passive scanning to optimise their channel scanning, roaming, and battery usage
  - CCX neighbour list is not optimised; 802.11k neighbour list is optimised for each client
- Client optimised neighbour list based on WLC RRM neighbour table
  - This provides an Assisted Roaming feature based on the optimised neighbour list
  - Supported on 802.11n indoor AP and single controller support
  - Cisco implementation based on RRM neighbour list update
  - Partial 802.11k implementation with neighbour list that shows BSSID and RSSI of neighbour radios

Assisted Roaming for non-11k Clients

- Assisted Roaming utilises 802.11k generated neighbour list capabilities to optimise roaming for non-11k clients
  - A “prediction” neighbour list can be generated for each client without the client sending an 11k neighbour list request
  - When enabled on a WLAN; after each successful client association/re-association the same neighbour list optimisation on the non-11k client to generate the neighbour list and store the list in the client MSCB entry
    - Clients at different locations should have a slightly different list since the client probes are seen with different RSSI values by different neighbours
    - As clients usually probe before any association or re-association, this list will be constructed with the most updated probe data and should predict the next AP the client is likely to roam to
- WLC discourages clients from roaming to less desirable neighbours by denying association if association request to an AP does not match entries on the stored prediction neighbour list
  - CCX status code 0xCC will be sent the client for “Association denied due to non-optimised association”

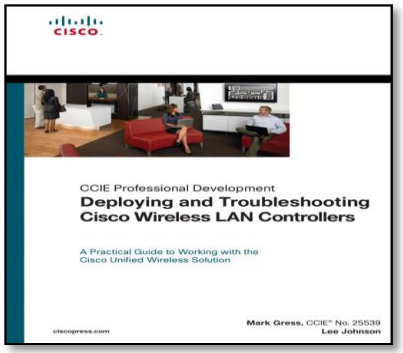
802.11k Configuration

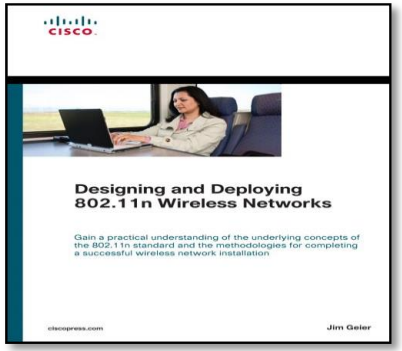
- config wlan assisted-roaming neighbor-list [enable | disable] <wlan-id>
- config assisted-roaming floor bias <dB>
- config wlan assisted-roaming dual-list [enable | disable] <wlan-id>
- config wlan assisted-roaming prediction [enable | disable] <wlan-id>
- config wlan assisted-roaming prediction minimum <1-6>
- config wlan assisted-roaming denial maximum <1-10>

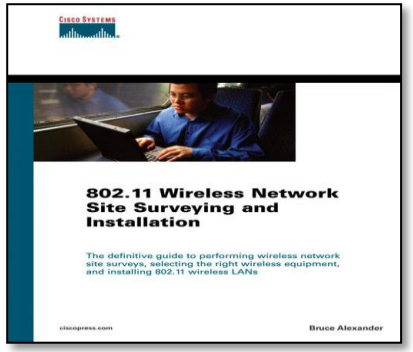
Where Are We Now?

- We have:
  - ✓ Cell built based on device types and density
  - ✓ Good overlap and roaming optimisation
  - ✓ QoS for wireless and wired traffic
  - ✓ EDCA optimised for voice/video
  - ✓ CAC to block excessive flows and guarantee ongoing calls quality
  - ✓ AVC to mark and filter traffic
  - ✓ VideoStream to optimise video delivery
  - ✓ Fast and Secure and Optimised Roaming with 802.11r and 802.11k
- No network is perfect, but our network is optimised for mobile applications

Recommended Reading










Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 March 12:00pm - 2:00pm

Learn online with Cisco Live!

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


CISCO
TM