




*TOMORROW
starts here.*

Cisco *live!*



Design and Deployment of Wireless LANs for Voice and Video

BRKEWN-2000

Matt Fowler

Consulting Systems Engineer

#clmel

Cisco *live!*

Agenda

- Determine Voice/Video Requirements
 - What kind of wireless design is needed?
- Build the Cell
 - Efficient and fast for a variety of mobile applications
- Improve for QoS
 - Prioritise traffic that cannot wait
- Fine Tune for the Specific Device
 - Help applications that need priority, but don't
- What will **NOT** be covered
 - Collaboration Manager configurations, Voice protocols comparison, Voice Gateways...



A nighttime photograph of a city street. In the foreground, there are long, curved light trails from cars, primarily in shades of yellow and orange. In the middle ground, a pedestrian bridge with blue lighting spans across the street. In the background, there are several tall buildings with lit windows and some flags on poles. The overall scene is illuminated by city lights.

Determine Application Requirements

Build the Cell, Improve for QoS and Fine Tune for the Specific Device

How Much Bandwidth Is Required?

- Often Less than You May Think
- It is most likely that you won't be supporting just one application
- Design for the highest bandwidth demand that you intend to support
 - What you need is the minimum acceptable throughput that the application will require
 - Most users use only ONE high performance demanding application at a time
- Multiply this number by the number of devices that you need to support
- This is the aggregate bandwidth you will require in your space

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 is Required?

- 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.

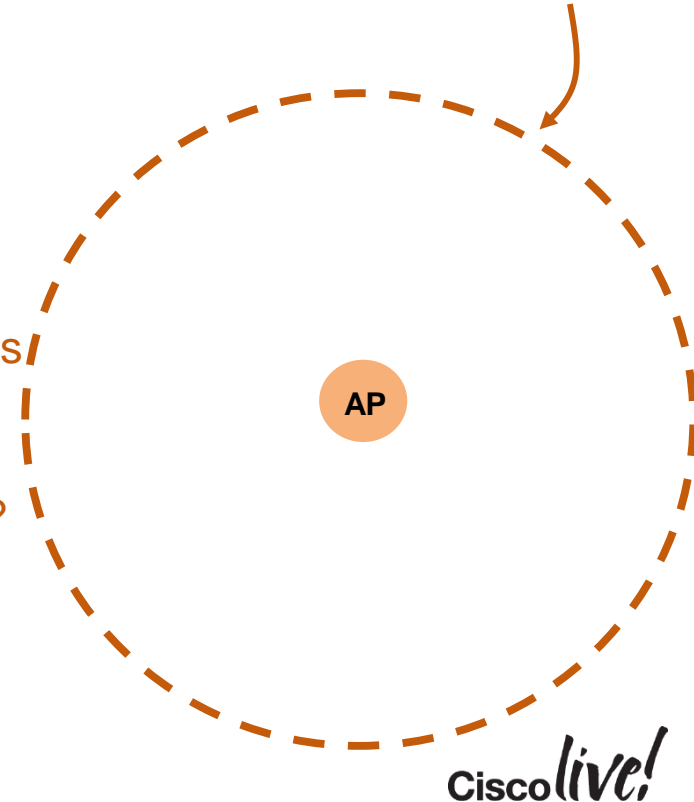
Cisco *live!*

Real Life Example?

Medical Centre

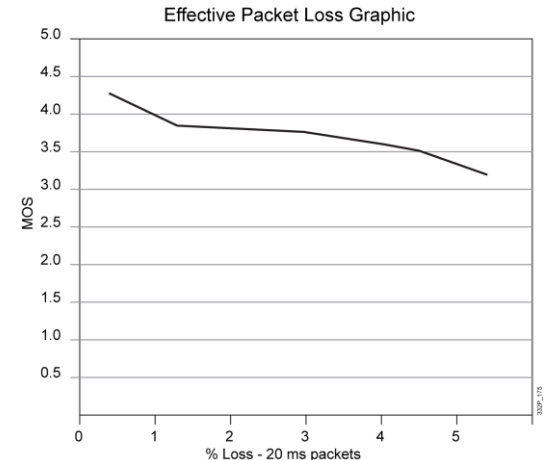
- Density studies show 12 users / cell on average
 - Expected 2 HD video calls (Skype type)
 - 5 audio calls
 - All users may browse
- Let's do the maths:
 - 2 HD video calls = $1.2 \text{ Mbps} \times 2 \times 2 \text{ ways} = 4.8 \text{ Mbps}$
 - 5 audio calls... mmm what application?
 - Skype too? $30 \text{ kbps} \times 5 \times 2 \text{ ways} = 600 \text{ kbps}$
 - Others are browsing (5 people)... $250 \text{ kbps /person?}$
 - Total = **6.65 Mbps needed**
Of course browsing requires more than voice
But should I design for browsing?

I need 6.65 Mbps throughput everywhere in the cell
- > therefore I need it here



VoIP Requirements

- VoIP carries voice sound with UDP and Real Time Protocol (RTP), voice control traffic uses Real Time Control Protocol (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 Error Rate (PER) $\leq 1\%$
 - As low jitter as possible, less than 100ms
 - Retries should be $< 20\%$
 - When these values are exceeded, MOS reduces
 - Your mission is to keep MOS high



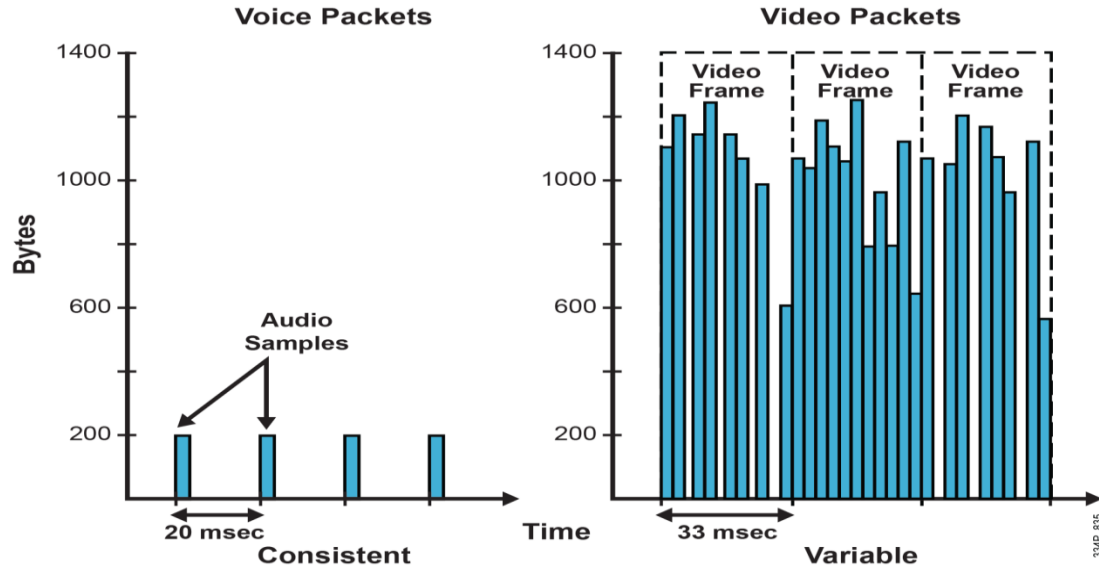
VoIP Requirements

- 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
 - Jitter should be less than 30 ms



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

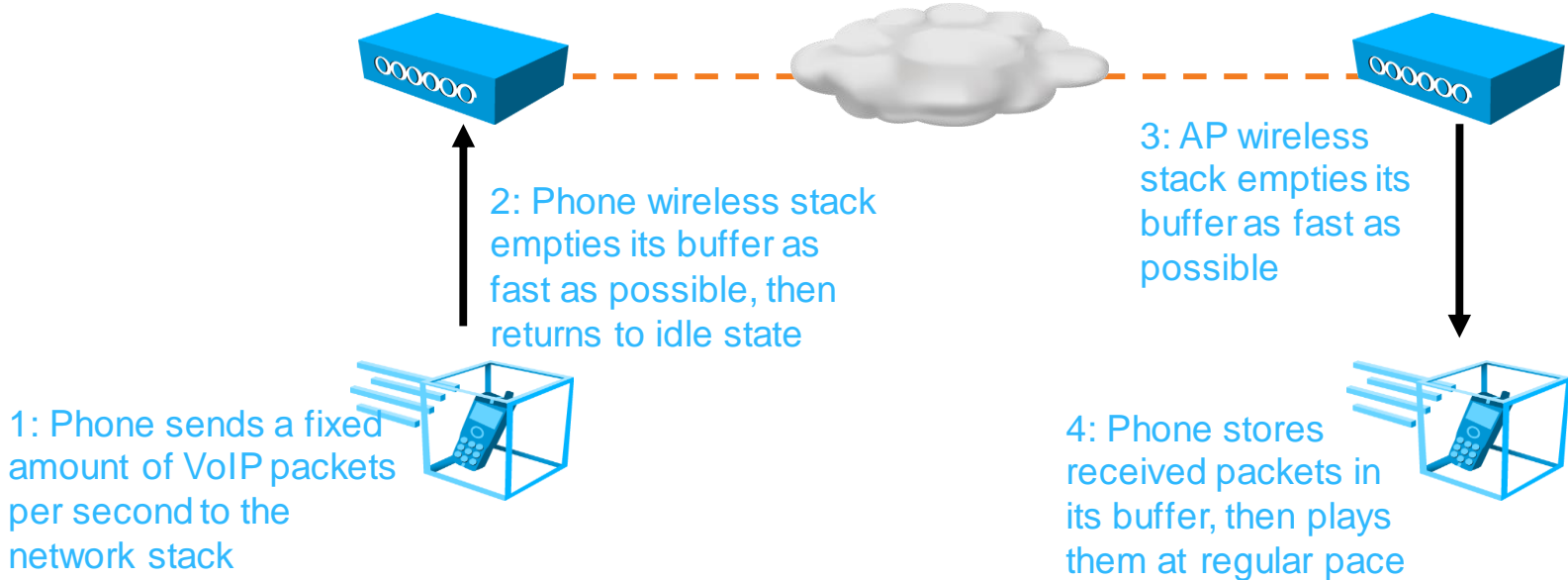


A long-exposure photograph of a city street at night. The foreground is dominated by vibrant, multi-colored light trails from moving vehicles, creating a sense of motion and energy. In the background, modern city buildings are illuminated with various lights, and a pedestrian bridge spans across the street. The overall scene is a dynamic urban environment.

Building the Cell

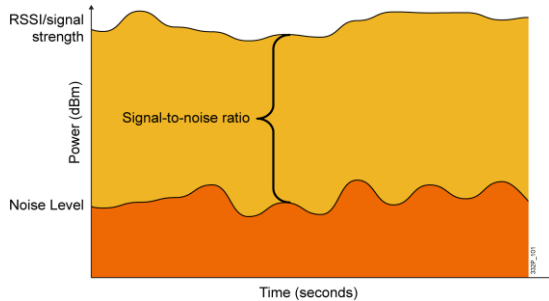
VoIP (and Video!) over Wireless Data Flow

- 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...



Is it better now?



Blah blah blah



You are a bit quiet

now?
now?

Assuming 10% PER

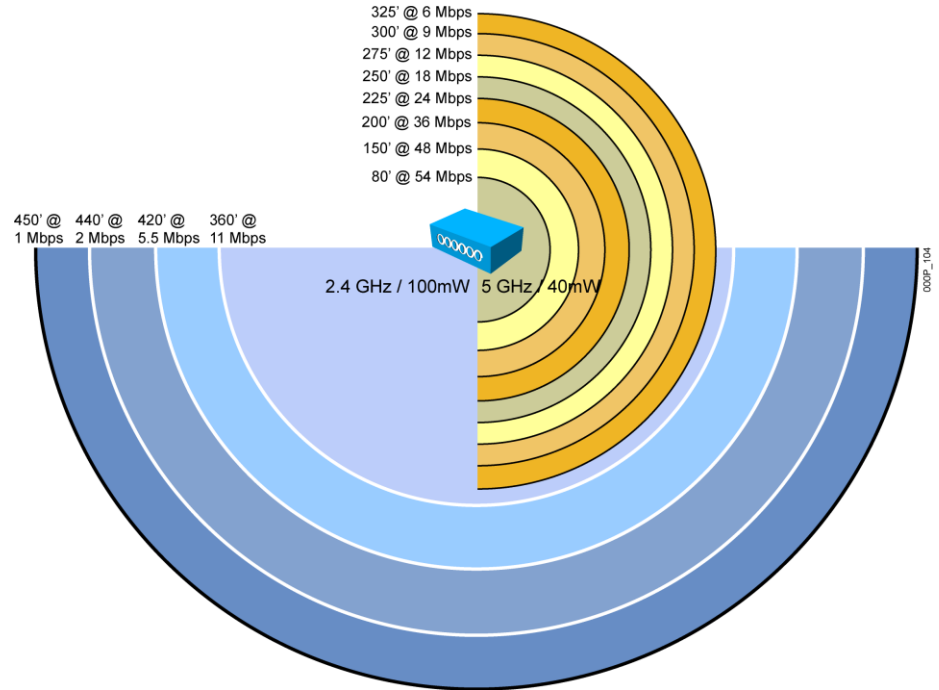
Speed	Required SNR	AP Sensitivity
1	0	-91
2	3	-91
5.5	6	-91
6	2	-87
11	9	-88
12	6	-86
24	11	-85
36	13	-85
48	17	-78
54	19	-77

This for data, for voice, add 25 dB to SNR

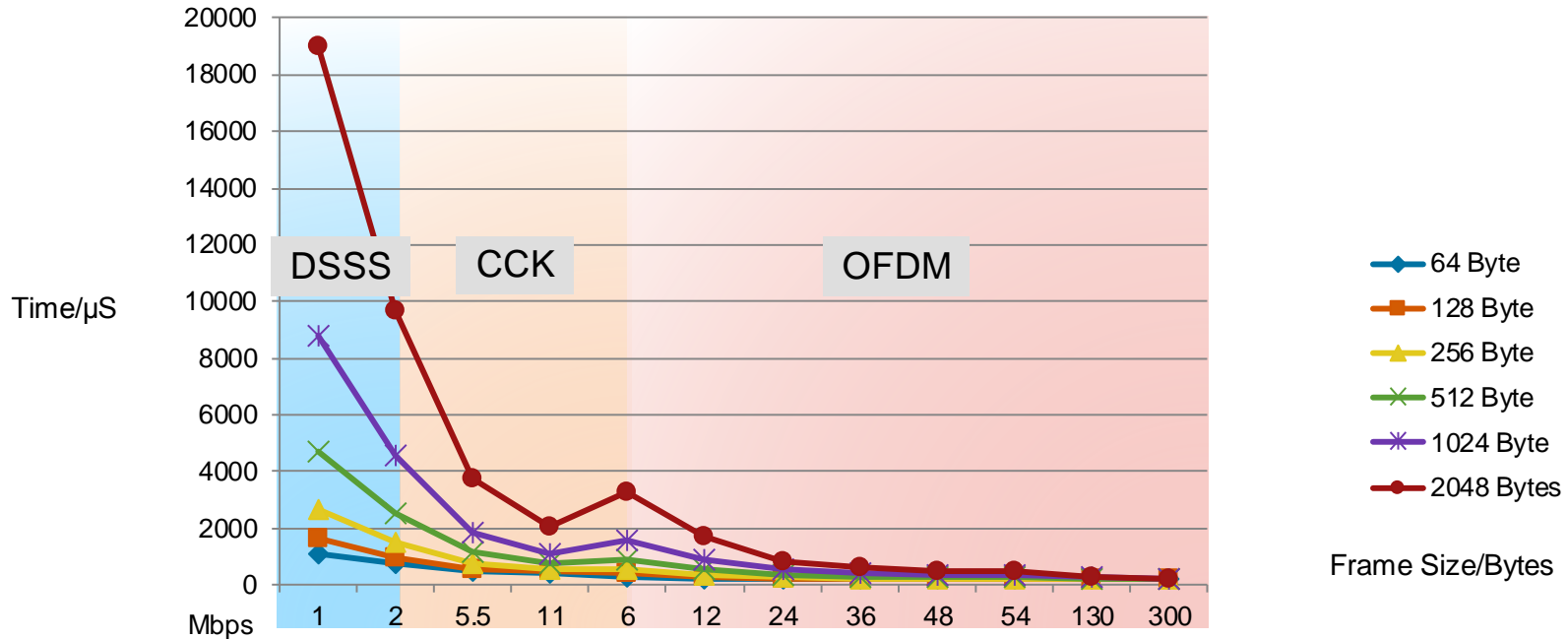
Cisco *live!*

Cell Size – Depends on Protocol and Rates

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



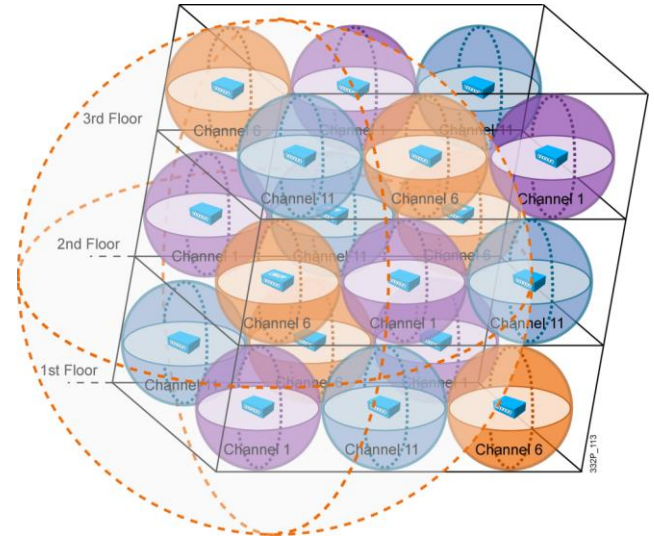
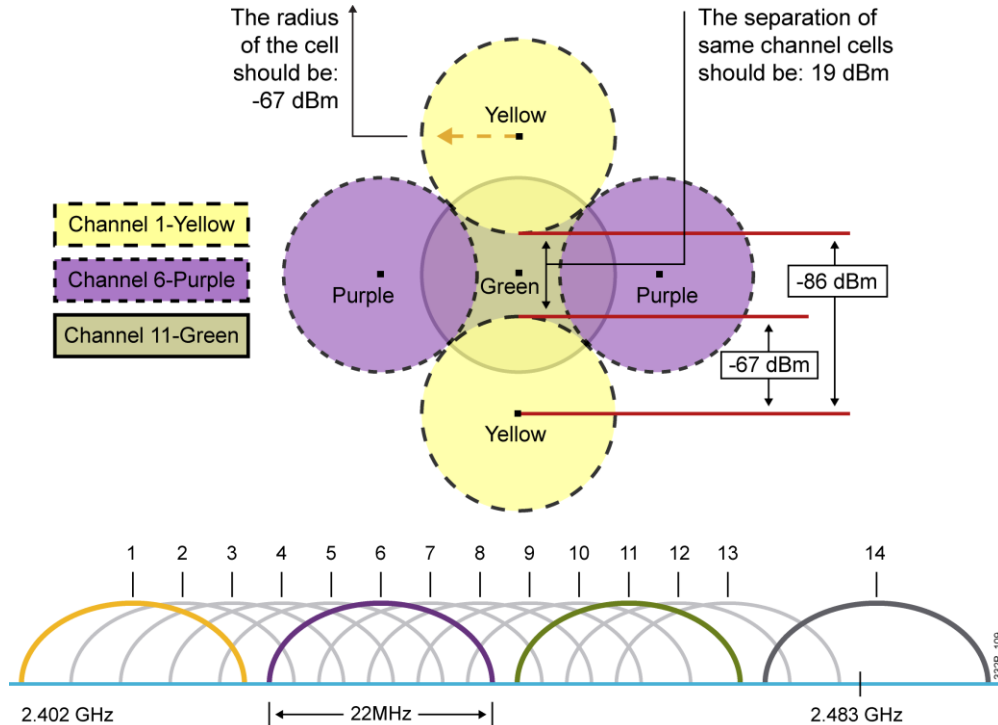
Moving Away From the AP Degrades Performances



Spectrum is a Shared Finite Resource

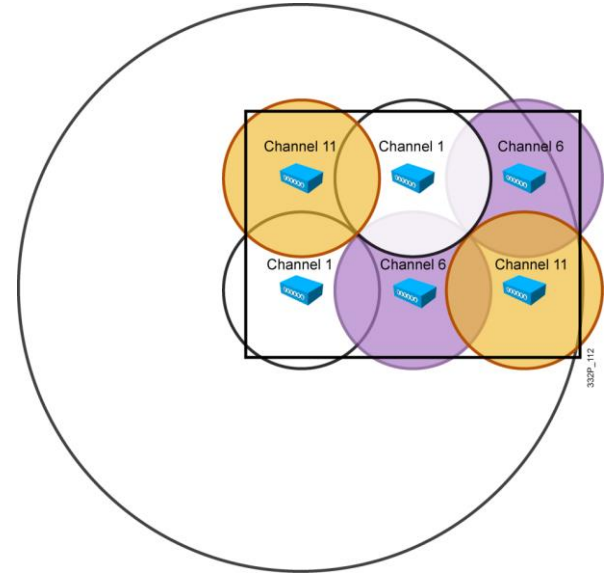
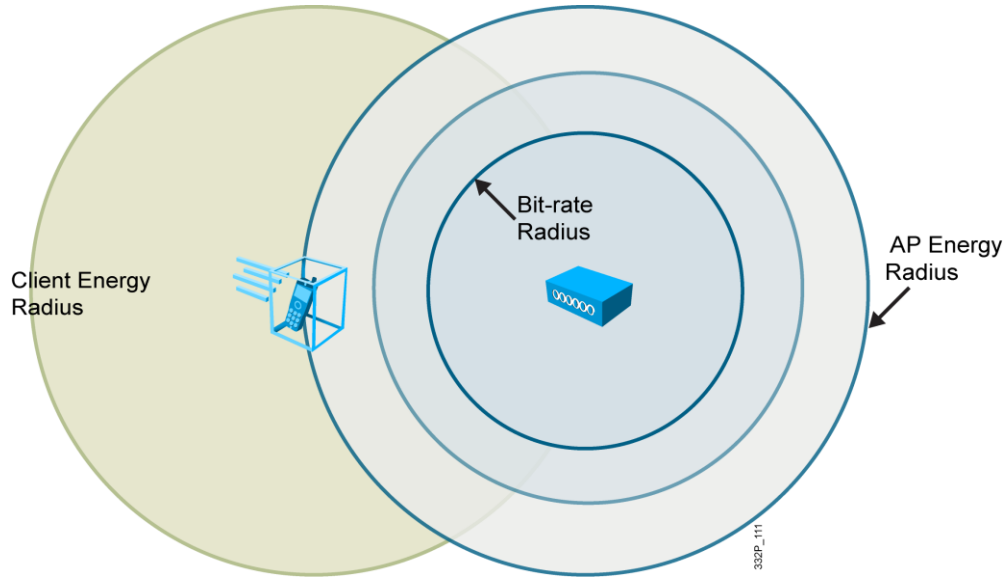
2.4-GHz Network Design

- 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...

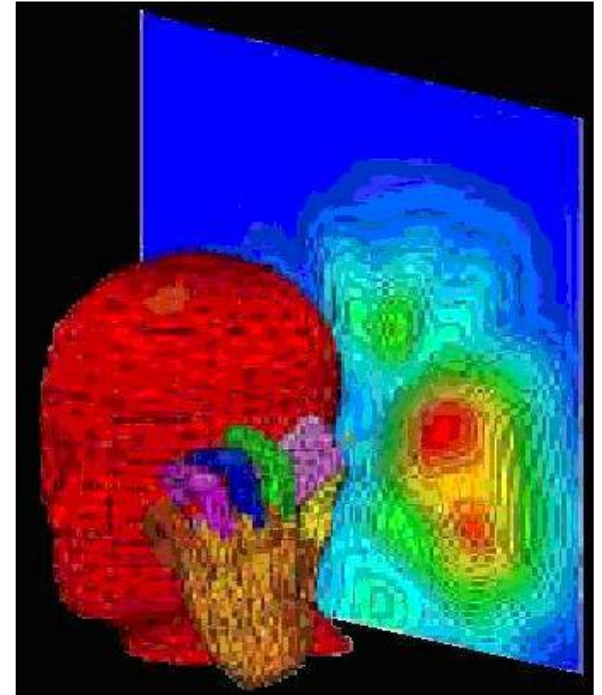


Channel Coverage Sizing Recommendations

- Coverage must be designed for your 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 the 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 Coverage Cell Sizes equals:
 1. More cells in a given coverage area
 2. More cells equals more call with better voice and video quality

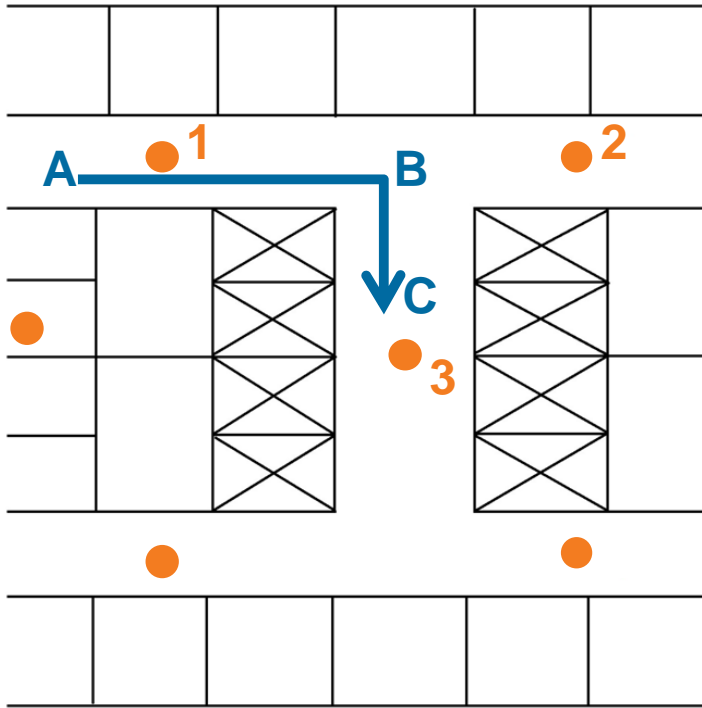
Signal Attenuation

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



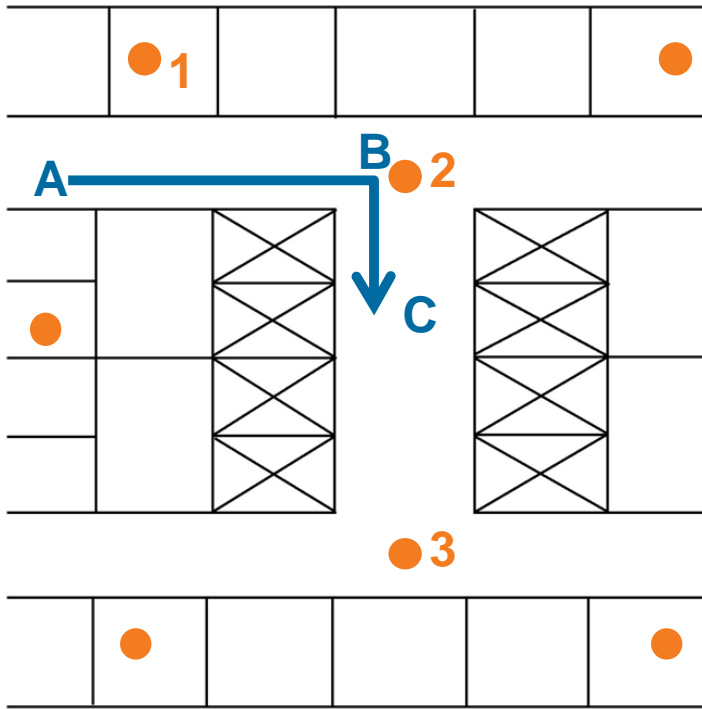
Cisco *live!*

VoWiFi Rate Shifting



- 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 μ s
 - 200 B frame @ 24 Mbps is sent in 8.3 μ s
 - Rate shifting from 54 Mbps to 24 Mbps can waste 1100 μ s

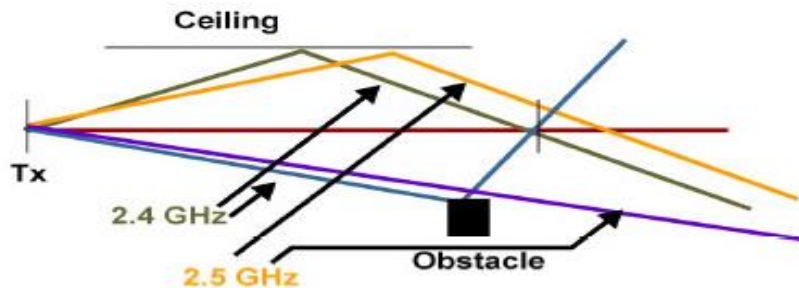
VoWiFi Rate Shifting



- 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

RF Design – Don't Do Anything Stupid

- Highly reflective environments
- Multipath distortion/fade is a consideration
- Legacy SISO technologies (802.11a/b/g) are most prone
- 802.11n/ac 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

- Site Survey
- Site Survey
- Site Survey
- **Site Survey!**



Verify coverage after deployment

Mmm...

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

Data Rates**

1 Mbps	Disabled ▾
2 Mbps	Disabled ▾
5.5 Mbps	Disabled ▾
6 Mbps	Disabled ▾
9 Mbps	Disabled ▾
11 Mbps	Disabled ▾
12 Mbps	Supported ▾
18 Mbps	Supported ▾
24 Mbps	Mandatory ▾
36 Mbps	Supported ▾
48 Mbps	Supported ▾
54 Mbps	Mandatory ▾

BAD EXAMPLE! (good example in 2 slides)

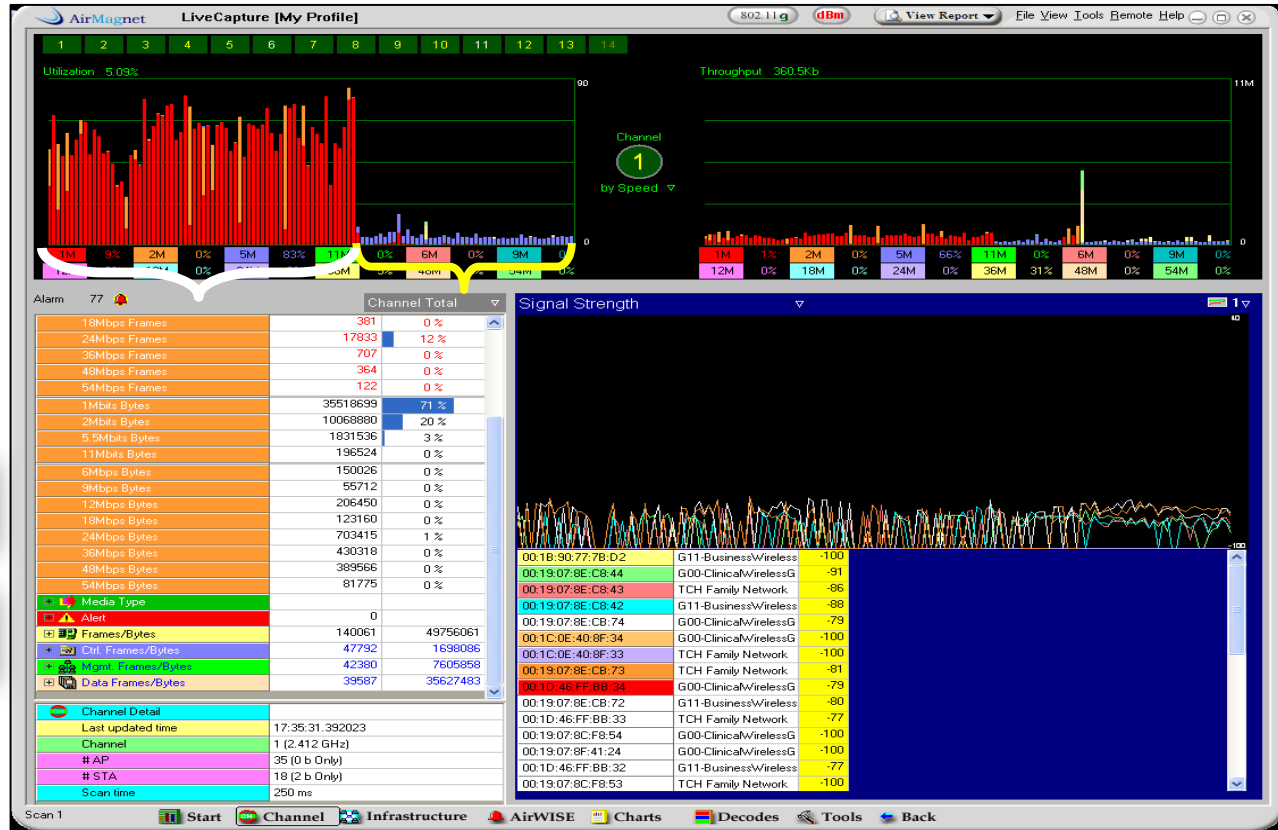
“bad” if you overlap at 12 Mbps

Cisco *live!*

Channel Utilisation - What Made the Difference?

60% Before

5% After



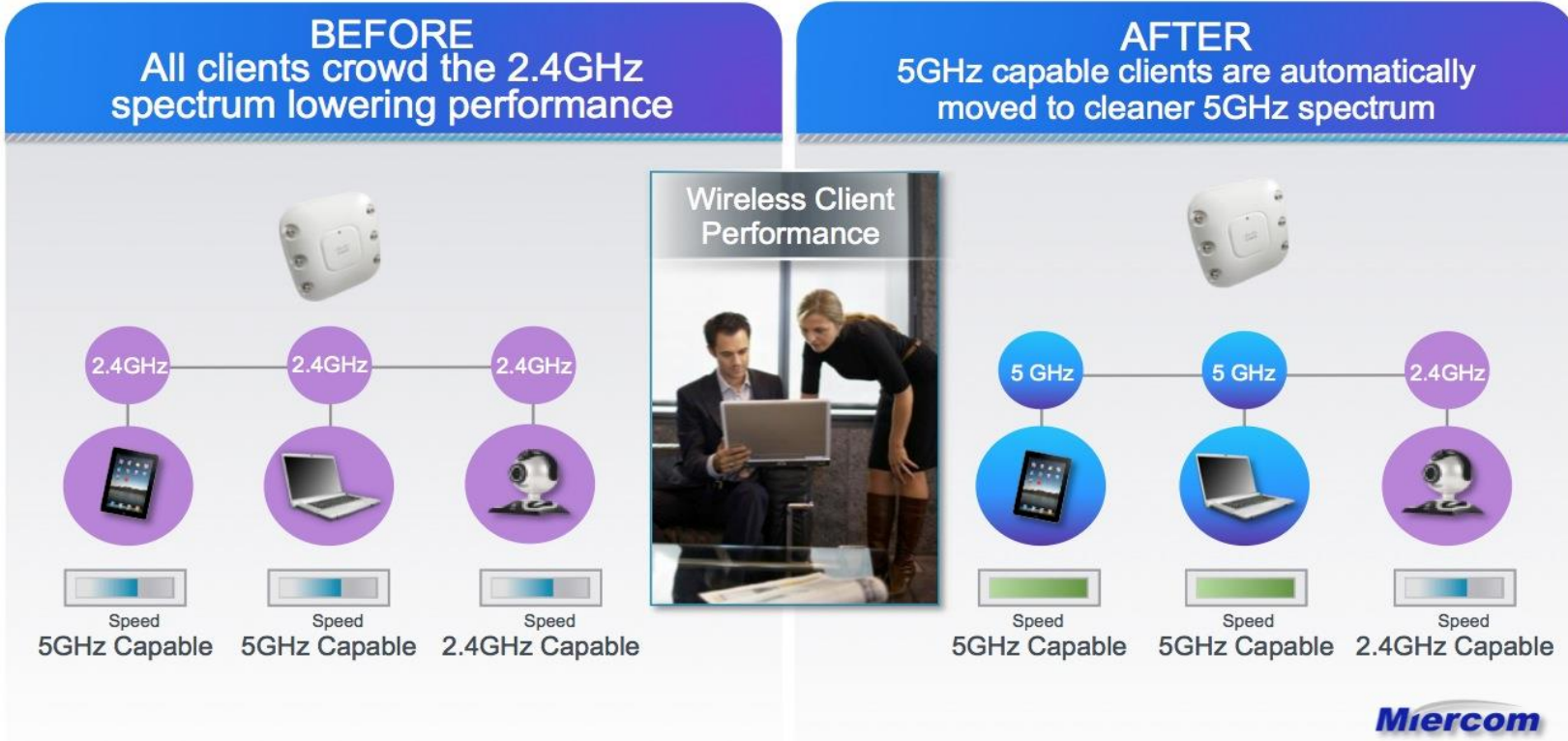
Channel Design – Use the Tools

- 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
 - ClientLink to provide better throughput for 802.11a/g/n clients

Data Rates**	
1 Mbps	Disabled
2 Mbps	Disabled
5.5 Mbps	Disabled
6 Mbps	Disabled
9 Mbps	Disabled
11 Mbps	Disabled
12 Mbps	Mandatory
18 Mbps	Supported
24 Mbps	Supported
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	Supported

Cisco BandSelect Technology

- Automatic Band Steering and Selection For 5GHz Capable Devices



Configuring Band Select

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

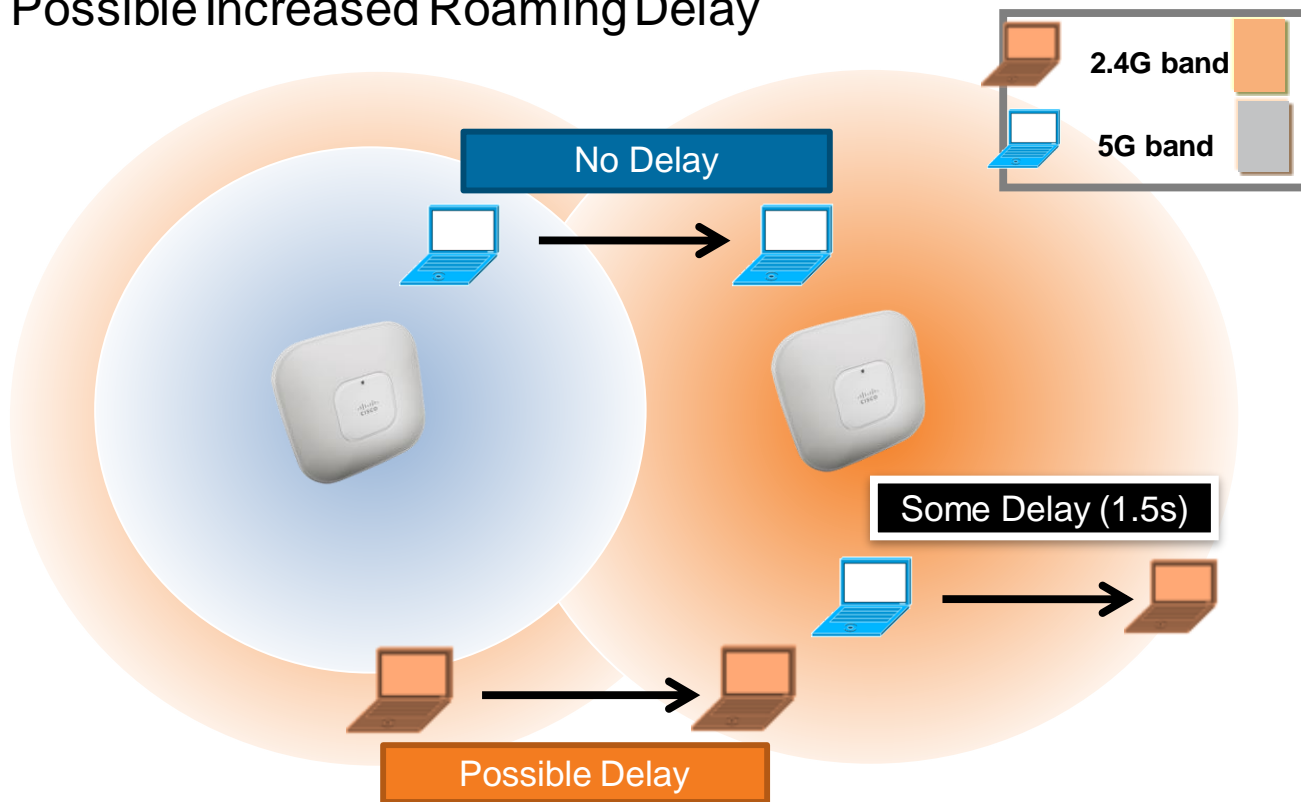
WLANs > Edit 'Open31'

The screenshot shows the configuration page for a WLAN named 'Open31'. The 'Policy-Mapping' tab is selected. The 'Client Band Select' checkbox is highlighted with a red circle. Other settings include:

- P2P Blocking Action: Disabled
- Client Exclusion: Enabled, Timeout Value (secs): 60
- Maximum Allowed Clients: 0
- Static IP Tunneling: Disabled
- Wi-Fi Direct Clients Policy: Disabled
- Maximum Allowed Clients Per AP Radio: 200
- Clear HotSpot Configuration: Enabled
- Client user idle timeout (15-100000): 300 Seconds
- Client user idle threshold (0-10000000): 0 Bytes
- Off Channel Scanning Defer: Scan Defer Priority (0-7) with checkboxes for 0-7, and Scan Defer Time(msecs): 100
- Management Frame Protection (MFP): MFP Client Protection: Optional
- DTIM Period (in beacon intervals): 802.11a/n (1 - 255): 1, 802.11b/g/n (1 - 255): 1
- NAC: NAC State: None
- Load Balancing and Band Select: Client Load Balancing: Disabled, Client Band Select: Disabled (highlighted)
- Passive Client: Passive Client: Disabled

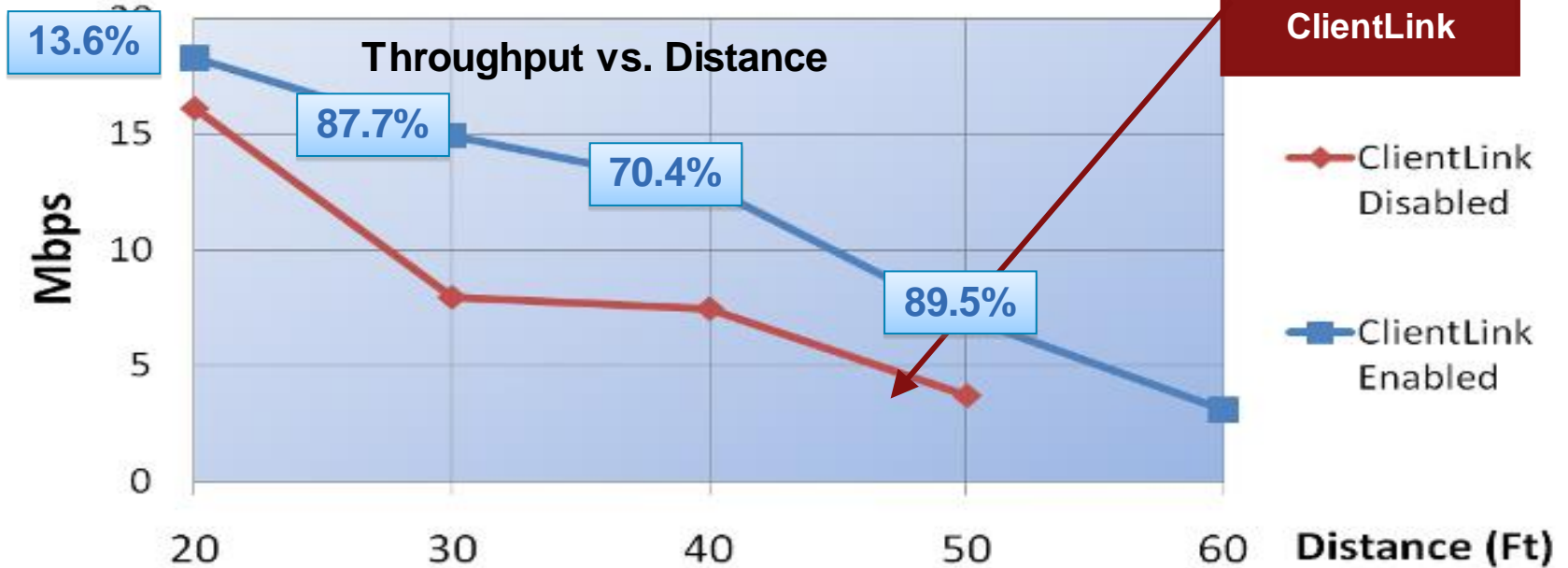
BandSelect – Test Before Full Deployment

- Caveat – Possible Increased Roaming Delay



Cisco ClientLink 3.0

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

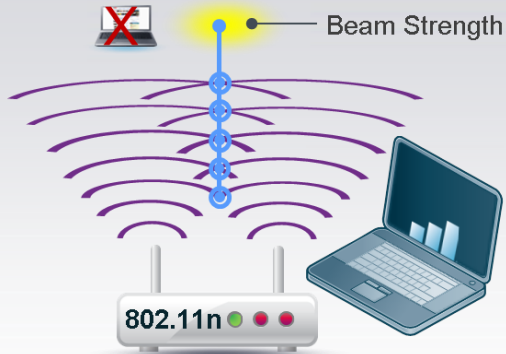


Cisco's ClientLink Technologies

Advanced Beam Forming Technologies Improve Wireless Client Performance

BEFORE

Beam not directed towards clients
resulting in inconsistent performance



Wireless Client
Performance

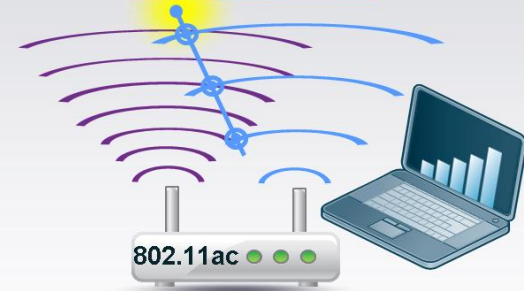


AFTER

Beam directed towards client resulting in
consistent experience and better performance

802.11a/g (ClientLink)
802.11a/g/n (ClientLink 2.0)
802.11ac (ClientLink 3.0)

Beam Forming



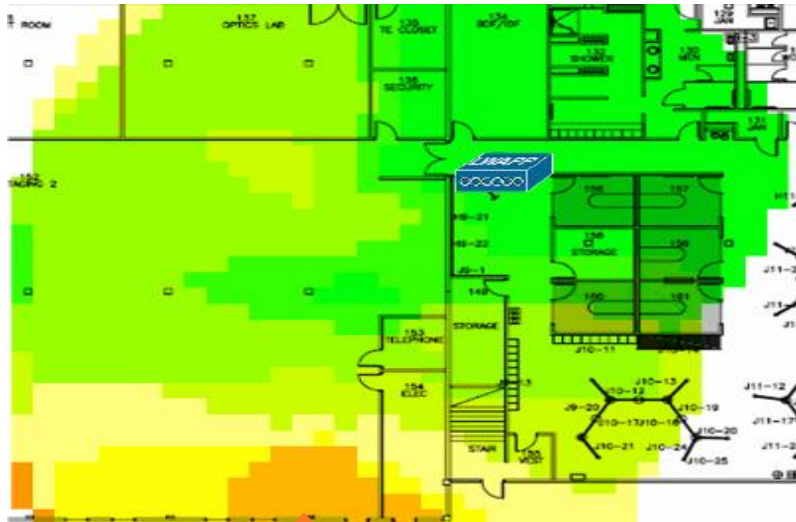
Cisco ClientLink—Improves Predictability and Performance

Client Link: Reduced Coverage Holes

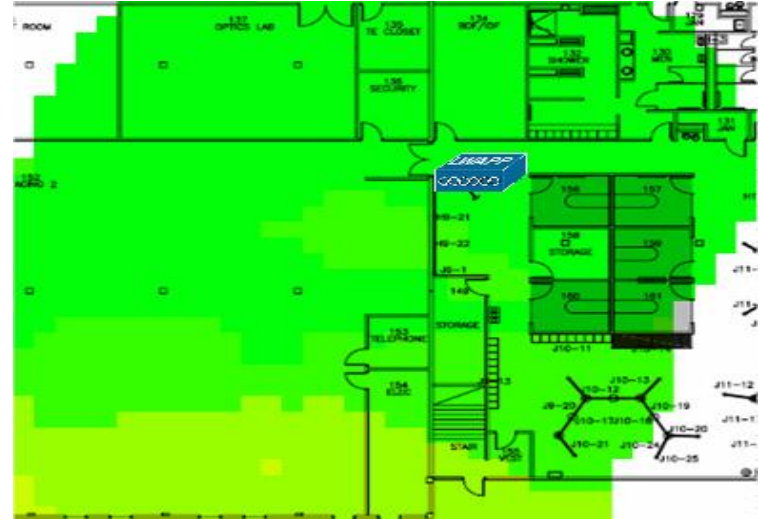
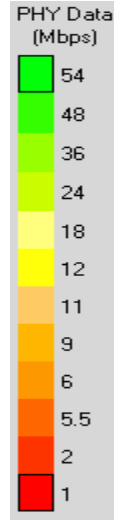
Higher PHY Data Rates

• **ClientLink Disabled**

• **ClientLink Enabled**



Lower Data Rates

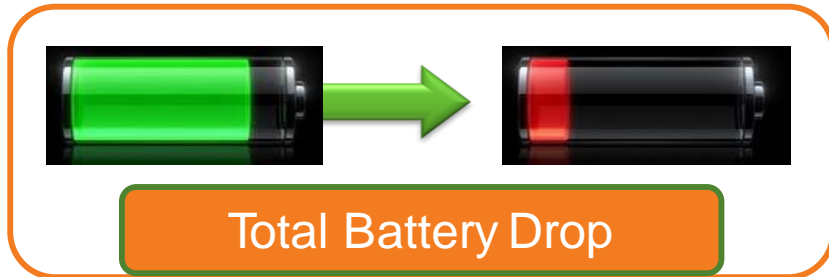
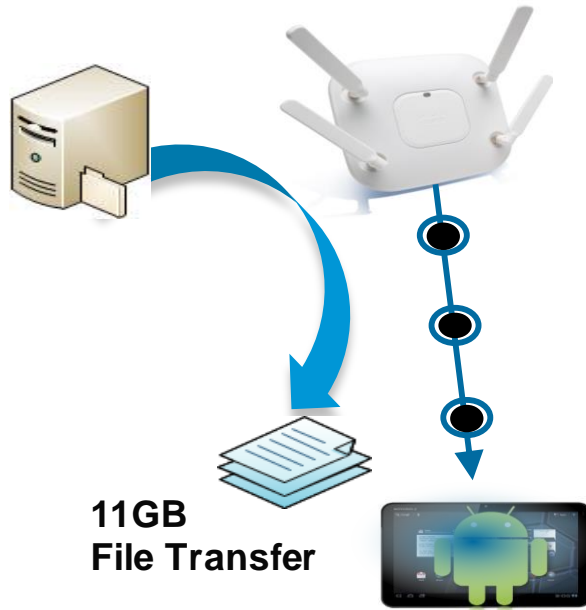


Higher Data Rates

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.





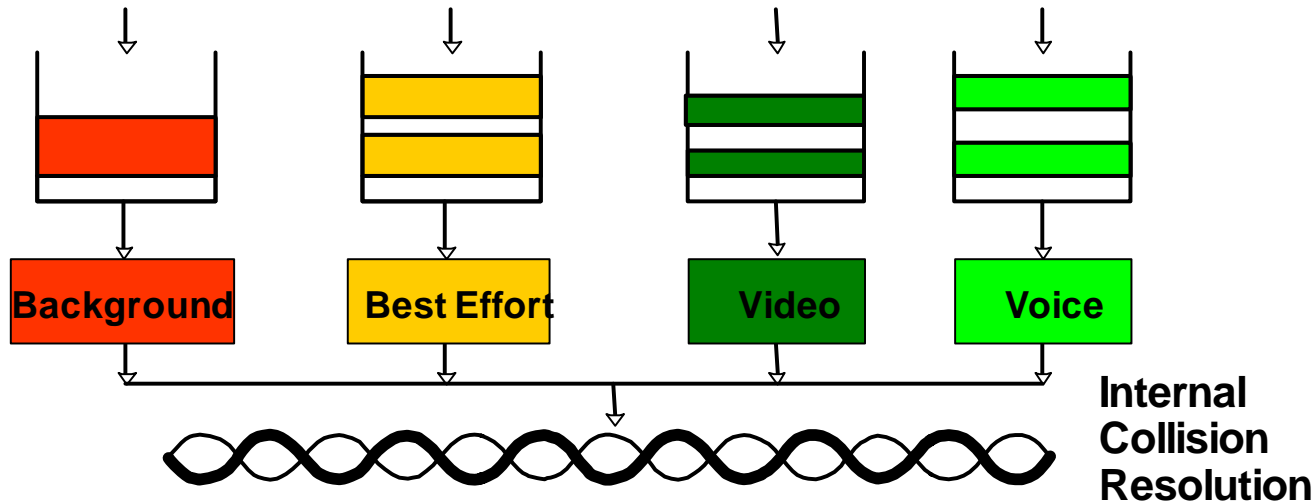
Improve for QoS

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

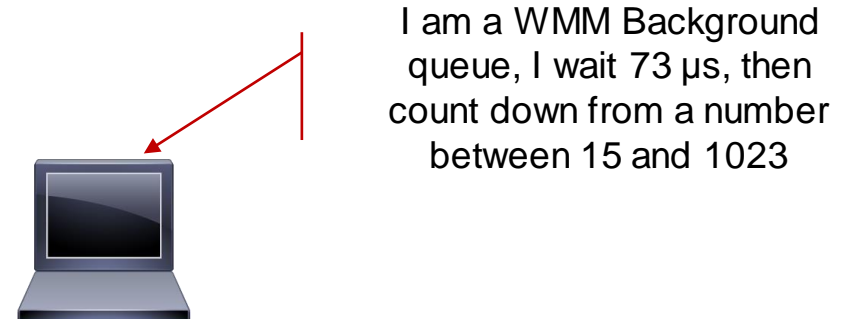
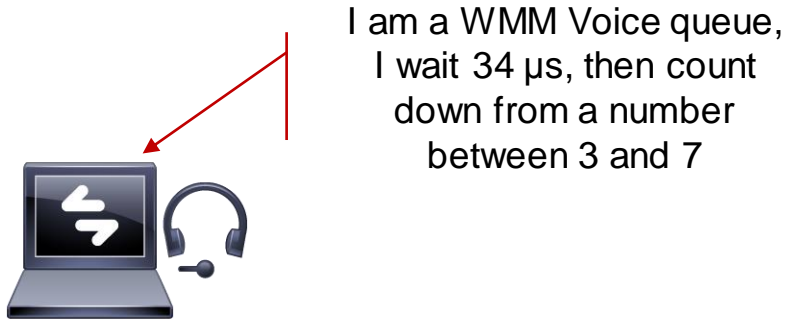
802.11e / WMM Media Access Classifications

- Separates traffic types into 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

- When you want to send a frame, you need to wait a silence (with QoS, AIFS, Arbitrated 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

- Good Countdown recipe with WMM:
- **1. Pick your queue, this will give you your initial AIFS Number**
 - Default AIFSN is different for Voice (2), Video (2), Best Effort (3) and Background (7)
- **2. Then, you need 2 other ingredients:**
 - The **band** where you operate – this is because the recipe incorporates the Short Interframe Space (SIFS), shortest possible silence
 - SIFS = 10 μ s for 2.4 GHz, 16 μ s for 5 GHz
 - The **slot time**, tempo at which you count: 9 μ s for 802.11.a/gn (802.11b has a longer one)
- **3. Then add the ingredients together!**
 - The time you wait before counting down is:
AIFS = SIFS + AIFSN x Slot Time
- **4. Then, pick up a number between CwMin and CwMax (you usually pick up CwMin the first time you try), and wait that on top of the AIFS**

AIFS, CW... Okay, it's complicated

- Example!

- You are a nice shiny phone using AC_VO in 5 GHz

- You pick 2 as your AIFSN, you know that SIFS is 16 μ s in 5 GHz, and slot time is 9 μ s for 802.11ag
- Your AIFS is: $AIFS = SIFS + AIFSN \times Slot\ Time = 16 + (2 \times 9) = 34 \mu$ s
- Suppose you pick CwMin, you count down 3 slots
- As a slot time for 802.11ag is 9 μ s, that's 27 μ s
- So you wait: 34μ s + 27 μ s = 61 μ s then you send

- Another one? You are a data device in 2.4 GHz:

- You wait: 10 μ s + 3 x 9 μ s (->AIFS=37 μ s), then 15 x 9 μ s, total: 172 μ s then you send

AC	AIFSN	Default values (Configurable)				Resulting total wait time (μ s)			
		AIFS (2.4 GHz)	AIFS (5 GHz)	CwMin	CwMax	2.4 GHz min	2.4 GHz max	5 GHz min	5 GHz max
VO	2	28	34	3	7	55	91	61	97
VI	2	28	34	7	15	91	163	97	169
BE	3	37	43	15	1023	172	9244	178	9250
BK	7	73	79	15	1023	208	9280	214	9286

$$AIFS = SIFS + AIFSN \times Slot\ Time$$

SIFS = 10 μ s for 2.4 GHz, 16 μ s for 5 GHz

Slot time = 9 μ s for 802.11ag

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 (or units of 32 μ s) and covers the time you take to send, regardless of the data rate you use and the size of your frame

In beacons 

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



"If you gain access to the medium you can send: for up to 1.504 ms for voice, 3.008 ms for video, or 1 frame only if you send BE or BK traffic"

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

```
⊕ IEEE 802.11 Beacon frame, Flags: .....C
⊖ IEEE 802.11 wireless LAN management frame
  ⊕ WME QoS Info: 0x80
    Reserved: 00
  ⊕ Ac Parameters ACI 0 (Best Effort), ACM no , AIFSN 3, ECwmin 4 ,ECwmax 10, TXOP 0
  ⊕ Ac Parameters ACI 1 (Background), ACM no , AIFSN 7, ECwmin 4 ,ECwmax 10, TXOP 0
  ⊕ Ac Parameters ACI 2 (Video), ACM no , AIFSN 2, ECwmin 3 ,ECwmax 4, TXOP 94
  ⊕ Ac Parameters ACI 3 (Voice), ACM no , AIFSN 2, ECwmin 2 ,ECwmax 3, TXOP 47
```

Cisco live!

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

Bytes	1	1	2	1	2
	Element ID (11)	Length (5)	Station Count	Channel utilization	Available Admission Capacity

332P_357

How many stations in the cell

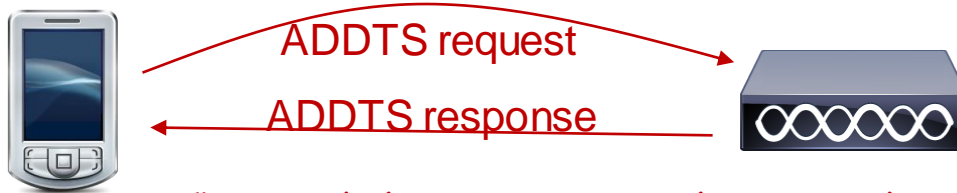
Percentage of time the channel was seen as busy by the AP

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

Setting QoS for the AP-WLC Part and Defaults

- Wireless > QoS > Profiles > Edit

Edit QoS Profile

QoS Profile Name

platinum

Description

For Voice Applications

WLAN QoS Parameters

Maximum Priority

voice

Unicast Default Priority

voice

Multicast Default Priority

voice

Wired QoS Protocol

Protocol Type

802.1p

802.1p Tag

5

besteffort
background
video
voice

None
802.1p

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

Cisco live!

Optimising WMM

- Wireless > 802.11a | 802.11bg > EDCA Parameters



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	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	12	6	10	0
BK	12	8	10	0

ACM

- Wireless > 802.11a | 802.11bg > Media

Same options now exist for Video

802.11a(5 GHz) > Media

Voice **Video** Media

Call Admission Control (CAC)

Admission Control (ACM) Enabled

CAC Method [4](#)

Load Based

Static

Load Based

Max RF Bandwidth (5-85)(%)

75

Reserved Roaming Bandwidth (0-25)(%)

6

Expedited bandwidth

When this is Enabled, VO devices should use ADDTS/TSPEC

For bandwidth calculation:
Only takes cell clients traffic
Includes all 802.11 activity on the channel

Taken out of Max RF Bandwidth value

Allows CCXv5 clients to exceed Max RF Bandwidth for emergency calls

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	FO: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	FO: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 0xFFFF]

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 Period
.....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 Video 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
227	A4:67:06:7C:BA:D7	192.168.0.2	192.168.0.10	Cisco:FC:3B:10	RTP Dynamic

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 0xFFFF0]
QoS Control Field:	%0000000000000101 [24-25] ----- AP PS Buffer State: 0 0..... A-MSDU: Not Present00..... Ack: Normal Acknowledge0..... EOSP: Not End of Triggered Service Period0101 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	TCP

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:	3611	[22-23] Mask 0xFFFF
Frag Number:	0	[24 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 Video 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

Source: A4:67:06:7C:BA:D7 [10-15]
Destination: F0:CB:A1:5F:BE:6A [16-21]
Seg Number: 3721 [22-23 Mask 0xFFFF0]
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: 1375 [36-37]
Identifier: 31655 [38-39]
Fragmentation Flags: %000 [40 Mask 0xE0]

What are we missing?

- If you are an operating system 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?



Fine Tune for the Specific Device

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

– E.g. target Facetime

802.11a(5 GHz) > Media

Voice Video Media

Call Admission Control (CAC)

Admission Control (ACM) Enabled

CAC Method [f](#) Static ▾

Max RF Bandwidth (5-85)(%) 0

Reserved Roaming Bandwidth (0-25)(%) 0

SIP CAC Support [f](#) Enabled

802.11a(5 GHz) > Media

Voice Video Media

Call Admission Control (CAC)

Admission Control (ACM) Enabled

CAC Method [f](#) Static ▾

Max RF Bandwidth (5-85)(%) 75

Reserved Roaming Bandwidth (0-25)(%) 6

Expedited bandwidth

SIP CAC Support [f](#) Enabled

Per-Call SIP Bandwidth [z](#)

SIP Codec G.711 User Defined

SIP Bandwidth (kbps) 64 G.711

SIP Voice Sample Interval (msecs) 20 ▾ G.729

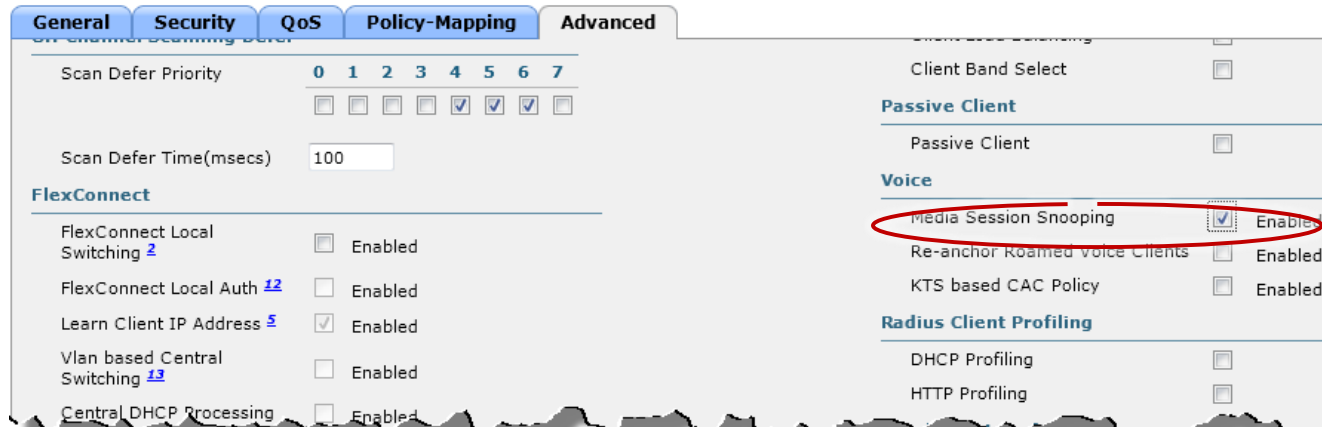
Maximum Possible Voice Calls 0

Maximum Possible Roaming Reserved Calls 0

If Your Traffic is Targeted

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

WLANs > Edit 'Open31'



The screenshot shows the configuration page for WLAN 'Open31' with the 'Policy-Mapping' tab selected. The 'Media Session Snooping' checkbox is checked and circled in red.

Section	Configuration Item	Value/Status
General	Scan Defer Priority	0 1 2 3 4 5 6 7 <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>
	Scan Defer Time(msecs)	100
FlexConnect	FlexConnect Local Switching	<input type="checkbox"/> Enabled
	FlexConnect Local Auth	<input type="checkbox"/> Enabled
	Learn Client IP Address	<input checked="" type="checkbox"/> Enabled
	Vlan based Central Switching	<input type="checkbox"/> Enabled
	Central DHCP Processing	<input type="checkbox"/> Enabled
Client Band Select	Client Band Select	<input type="checkbox"/>
	Passive Client	<input type="checkbox"/>
Voice	Media Session Snooping	<input checked="" type="checkbox"/> Enabled
	Re-anchor Roamed voice Clients	<input type="checkbox"/> Enabled
	KTS based CAC Policy	<input type="checkbox"/> Enabled
Radius Client Profiling	DHCP Profiling	<input type="checkbox"/>
	HTTP Profiling	<input type="checkbox"/>

SIP Audio, SIP Video (e.g 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:

```
Session Initiation Protocol
Status-Line: SIP/2.0 200 OK
Message Header
Via: SIP/2.0/UDP 10.142.57.139:16402;brancPo\212w4bk5134351a145c7415
To: "1010" <sip:user@10.78.78.253:16402>;tag=879704656
From: "1009" <sip:user@10.142.57.139:16402>;tag=649104684
Call-ID: 34e0ceea-5bb6-11y1-ab17-9aedbfc04012@10-142-57-Y39
\222@Seq: 1 INVITE
Contact: <sip:user@10.78.78.253:16402>;isfocus
User-Agent: Viceroy 1.5.0/GK
Content-type: application/sdp
```

Apple (outgoing call)

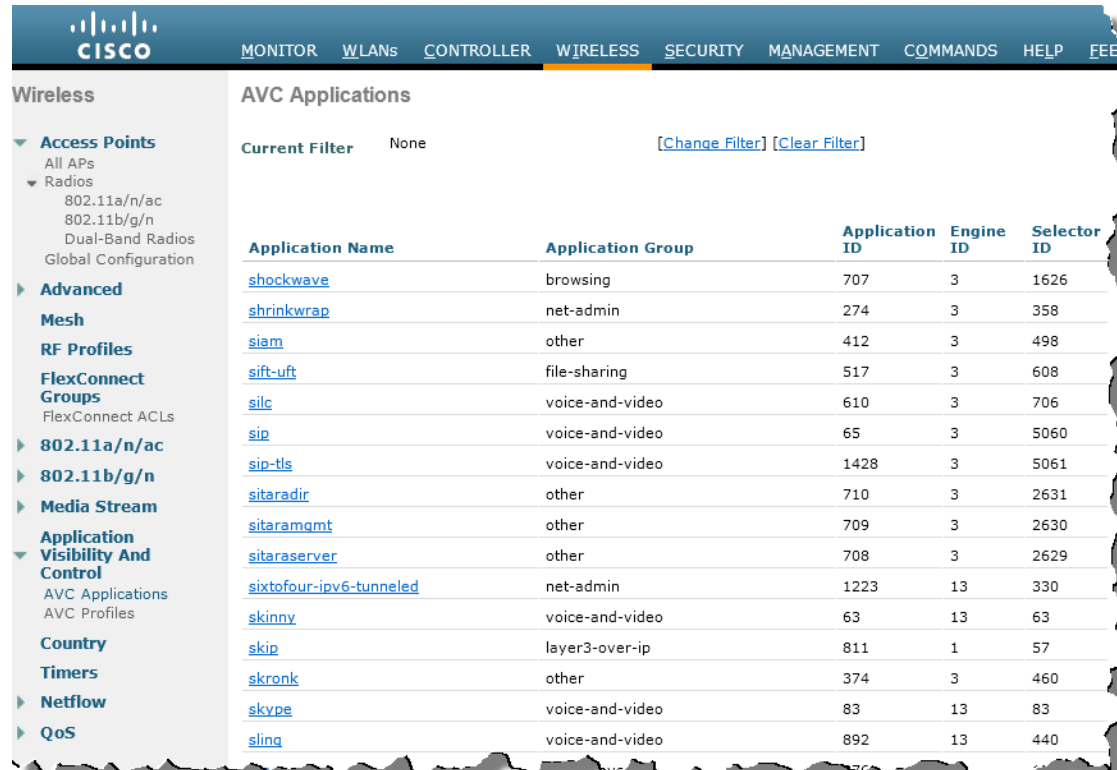
Can't tell (incoming call from CUCM), use ports

```
Session Initiation Protocol
Request-Line: INVITE sip:f302a196-3214-412e-a87b-df181bb0136c@9.11.99.101:47500;transport=tcp SIP/2.0
Message Header
Via: SIP/2.0/TCP 9.1.0.112:5060;branch=z9hg4bk6549071867
From: <sip:2086@9.1.0.112>;tag=158-d37011b0-81bc-48d9-a1a7-b0a8098c7dbf-21073507
To: <sip:2085@9.1.0.112>
Date: wed, 08 Feb 2012 04:02:14 GMT
Call-ID: ada92c80-f311f3c6-2e-70000109@9.1.0.112
Supported: timer,resource-priority,replaces
Min-SE: 1800
User-Agent: Cisco-CUCM8.6
Transmission Control Protocol, Src Port: sip (5060), Dst Port: 47500 (47500), Seq: 1, Ack: 1, Len: 982
```


If you have Several Traffic Types to Target:

Use Application Visibility and Control

- Internal application recognition engine based on NBAR
- More than 1000 applications recognised, including Netflix, Skype, MS Lync audio, MS Lync video viber, ventrilo, etc.



The screenshot shows the Cisco Wireless AVC Applications page. The left sidebar contains a navigation menu with categories like Access Points, Radios, Advanced, Mesh, RF Profiles, FlexConnect Groups, 802.11a/n/ac, 802.11b/g/n, Media Stream, Application Visibility And Control, Country, Timers, Netflow, and QoS. The main content area displays a table of applications with the following columns: Application Name, Application Group, Application ID, Engine ID, and Selector ID. The current filter is set to 'None'.

Application Name	Application Group	Application ID	Engine ID	Selector ID
shockwave	browsing	707	3	1626
shrinkwrap	net-admin	274	3	358
siam	other	412	3	498
sift-uft	file-sharing	517	3	608
silc	voice-and-video	610	3	706
sip	voice-and-video	65	3	5060
sip-tls	voice-and-video	1428	3	5061
sitaradir	other	710	3	2631
sitaramgmt	other	709	3	2630
sitaraserver	other	708	3	2629
sixtofour-ipv6-tunneled	net-admin	1223	13	330
skinny	voice-and-video	63	13	63
skip	layer3-over-ip	811	1	57
skronk	other	374	3	460
skype	voice-and-video	83	13	83
sling	voice-and-video	892	13	440

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

AVC Profile > Rule > 'help_untagged_mobile_apps'

Application Group: voice-and-video

Application Name: skype

Action: Mark

Dscp (0 to 63): Platinum(voice)

AVC Profile > Edit 'help_untagged_apps'

Application Name	Application Group Name	Action	DSCP	
skype	voice-and-video	mark	46	<input checked="" type="checkbox"/>
youtube	voice-and-video	mark	34	<input checked="" type="checkbox"/>
http	browsing	mark	0	<input checked="" type="checkbox"/>

- 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:

WLANs > Edit 'Open31'

General Security QoS **Policy-Mapping** Advanced

Quality of Service (QoS) Platinum (voice) ▾

Application Visibility Enabled

AVC Profile help_untagged_mobile_apps ▾

Netflow Monitor none ▾

WMM

WMM Policy Allowed ▾

Top Applications

Application Name		Packet Count	Byte Count
youtube	(U)	5855	535032
	(D)	9608	14489305
ssl	(U)	377	66319
	(D)	320	315143
google-services	(U)	72	15000
	(D)	72	53810
skype	(U)	20	2984
	(D)	19	1507
dns	(U)	9	1018
	(D)	0	1526

4. Watch your traffic:

```
Continuation of non-HTTP traffic 15.4200600 74.125.7.241 172.31.255.101 HTTP
[+] Frame 11204: 1556 bytes on wire (12448 bits), 1556 bytes captured (12448 bits) on interface 0
[+] Radiotap Header v0, Length 26
[+] IEEE 802.11 QoS Data, Flags: .....F.C
[+] Logical-Link Control
[+] Internet Protocol Version 4, Src: 74.125.7.241 (74.125.7.241), Dst: 172.31.255.101 (172.31.255.101)
    Version: 4
    Header length: 20 bytes
    [+] Differentiated Services Field: 0x28 (DSCP 0x22: Assured Forwarding 41; ECN: 0x00: Not-ECT (Not ECN-Capable))
    Total Length: 1492
```

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

Edit QoS Profile

QoS Profile Name platinum

Description

Per-User Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Average Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>

Per-SSID Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Average Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>

Wireless > QoS > Profiles > Edit

Bandwidth Control – per User

- You can also control upstream and downstream bandwidth consumption:

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

WLANs > Edit 'New'

General Security QoS Policy-Mapping Advanced

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

	DownStream	UpStream
Average Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Average Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>

Clear

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

	DownStream	UpStream
Average Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Average Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>

Clear

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

MONITOR WLANs CONTROLLER WIRELESS

Edit QoS Role data rates

QoS Role Name

quests

Per-User Bandwidth Contracts (kbps) *

Average Data Rate

Burst Data Rate

Average Real-Time Rate

Burst Real-Time Rate

Security > Local Net User > New

MONITOR WLANs CONTROLLER WIRELESS SECURITY

Local Net Users > New

User Name

Password

Confirm Password

Guest User

Lifetime (seconds)

Guest User Role

Role

Bandwidth Control – per Device Type

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

How to identify that device

Policy > Edit

Policy Name iPads
Policy Id 1

Match Criteria

Match Role String
Match EAP Type EAP-TLS
Device Type **Android**
Android
Apple-Device
Apple-MacBook
Apple-iPad
Apple-iPhone
Apple-iPod
Aruba-Device
Avaya-De

Device List

Close to 100 types on WLC

What policy to apply

Action

IPv4 ACL none
VLAN ID 0
Qos Policy none
Session Timeout (seconds) 1800
Sleeping Client Timeout (hours) 12

Active Hours

Day Mon
Start Time Hours Mins
End Time Hours Mins
Add

Day

Start Time

End Time

Cisco *live!*

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:

WLANs > Edit 'BYOD'

General Security QoS **Policy-Mapping** Advanced

Priority Index (1-16)

Local Classification Policy

Priority Index

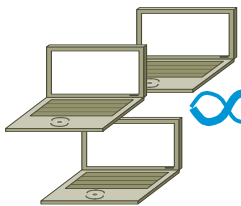
Priority Index	Policy Name
1	Ipad-policy
2	Windows_policy

Set the index.

Pick the policy, then click Add

- Each policy can group several devices

Video Multicast Delivery Challenges

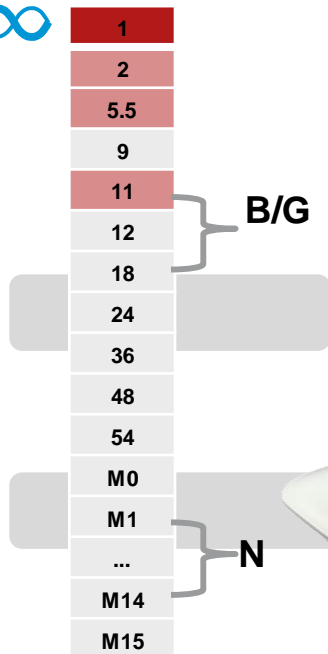


Video Impact

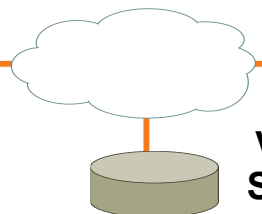
Choppy, Unreliable Video

- Video streaming does not utilise 802.11 n/ac 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

802.11 Data Rates



Access Point



Video Server

Default 802.11B/G mandatory data rates

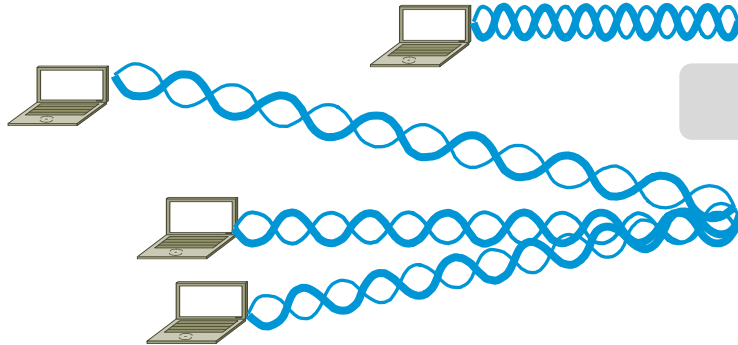
Technical Challenges

- 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.

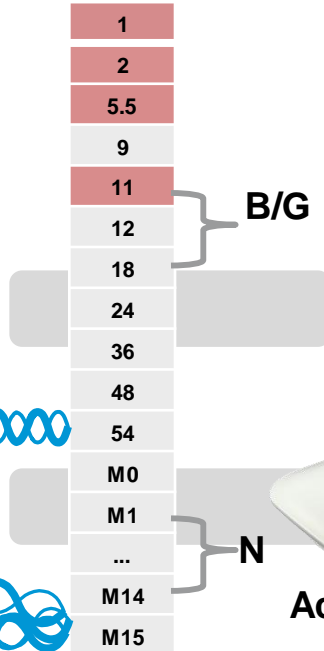
Video Multicast Delivery Solution - VideoStream

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

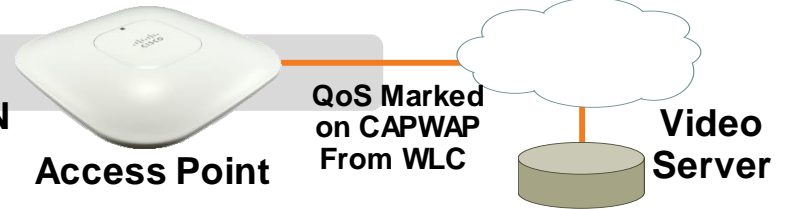


802.11 Data Rates



Technical Solution

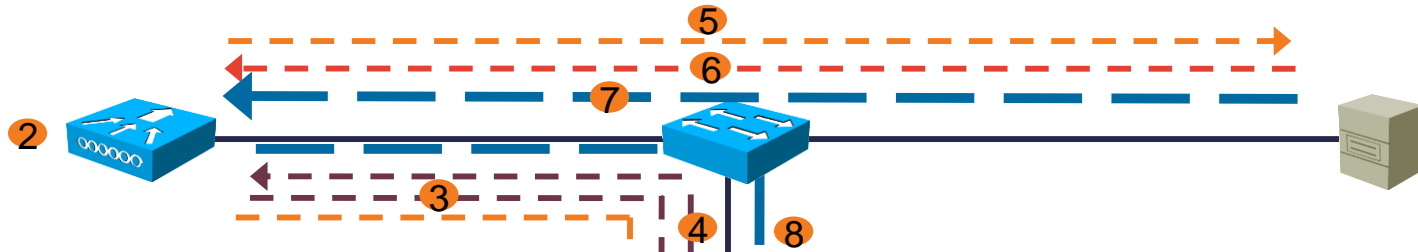
- IGMP state monitored for each client. We only send video to clients requesting it
- Multicast packets replicated at AP and sent to **individual clients at their data rate**
- Resource Reservation Control (RRC) is used to prevent channel oversubscription. Works in conjunction with Voice CAC
- Stream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



Default 802.11B/G mandatory data rates

Cisco *live!*

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

The screenshot shows the Cisco VideoStream configuration interface. The top navigation bar includes 'MONITOR', 'WLANS', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', and 'COMM'. The left sidebar lists various configuration categories: 'Wireless', 'Access Points', 'Advanced', 'Mesh', 'RF Profiles', 'FlexConnect Groups', 'FlexConnect ACLs', '802.11a/n/ac', '802.11b/g/n', 'Media Stream' (with sub-items 'General' and 'Streams'), and 'Application Visibility And Control'. The main content area is titled 'Media Stream > New' and contains several input fields: 'Stream Name' (MyCorpvideo), 'Multicast Destination Start IP Address(ipv4/ipv6)' (239.1.1.1), 'Multicast Destination End IP Address(ipv4/ipv6)' (239.1.1.2), and 'Maximum Expected Bandwidth(1 to 35000 Kbps)' (500). Below these is the 'Resource Reservation Control(RRC) Parameters' section, which includes a dropdown for 'Select from predefined templates' (currently showing 'Select'), 'Average Packet Size (100-1500 bytes)' (1200), 'RRC Periodic update' (checked), 'RRC Priority (1-8)' (1), and 'Traffic Profile Violation' (best-effort). A dropdown menu is open over the 'Select from predefined templates' field, listing options: 'Very Coarse(below 300 Kbps)', 'Coarse(below 500 Kbps)', 'Ordinary(below 750 Kbps)', 'Low(below 1 Mbps)', 'Medium(below 3 Mbps)', and 'High(below 5 Mbps)'.

Media Stream >General

Multicast Direct feature Enabled

Session Message Config

Session announcement State Enabled

Session announcement URL

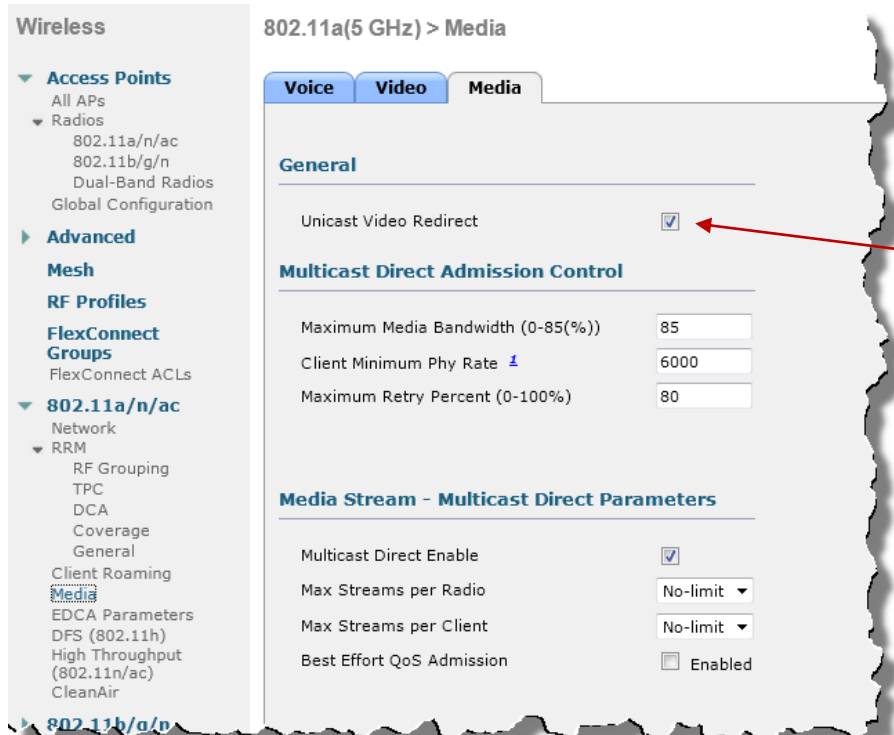
Announcement Email

Announcement Phone

Announcement Note

Cisco VideoStream - Configuration

Fine tune Video BW consumption



Wireless

802.11a(5 GHz) > Media

Access Points

Radios

802.11a/n/ac

802.11b/g/n

Dual-Band Radios

Global Configuration

Advanced

Mesh

RF Profiles

FlexConnect Groups

FlexConnect ACLs

802.11a/n/ac

Network

RRM

RF Grouping

TPC

DCA

Coverage

General

Client Roaming

Media

EDCA Parameters

DFS (802.11h)

High Throughput (802.11n/ac)

CleanAir

802.11b/g/n

Voice Video Media

General

Unicast Video Redirect

Multicast Direct Admission Control

Maximum Media Bandwidth (0-85(%) 85

Client Minimum Phy Rate 6000

Maximum Retry Percent (0-100%) 80

Media Stream - Multicast Direct Parameters

Multicast Direct Enable

Max Streams per Radio No-limit

Max Streams per Client No-limit

Best Effort QoS Admission Enabled

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

Where are We Now?

- We have:
 - ✓ Cell built based on device types and density (AP power level matches client power, settings tested)
 - ✓ Good overlap and roaming optimisation (20% overlap, -65 dBm at edge, roaming configuration optimised)
 - ✓ QoS for wireless and wired traffic (end to end)
 - ✓ EDCA optimised for voice/video (Right TXOPs, right WMM profiles)
 - ✓ CAC (to block excessive flows and guarantee ongoing calls quality)
 - ✓ AVC (to mark and filter traffic)
 - ✓ VideoStream (to optimise video delivery)
- No network is perfect, but this checklist should help you make sure that your wireless network is optimised for mobile applications



Q & A

Complete Your Online Session Evaluation

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

Complete your Overall Event Survey and 5 Session Evaluations.

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

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



Learn online with Cisco Live!

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

Cisco *live!*



Thank you.

Cisco *live!*



CISCO