Újdonságok a Wifi hálózatok világából

Szepesi Zoltán
Cisco
HBONE tábor 2012 november

Topics

- Wifi standard evolution (phy layer):
  - 802.11a,b,g
  - 802.11n
  - 802.11ac and the future
- How to cope with interference: Cisco CleanAir and Clientlink technology
- Wireless security: Wireless IDS/IPS

Topics

- Wifi standard evolution (phy layer):
  - *802.11a,b,g*
  - 802.11n
  - 802.11ac and the future
- How to cope with interference: Cisco CleanAir and Clientlink technology
- Wireless security: Wireless IDS/IPS

IEEE 802.11 Family
Technology Overview

IEEE 802.11 Standard define :

- A **Physical layer**
  Radio Frequencies, Data Modulation, …
  (802.11, 802.11b, 802.11g, 802.11a, 802.11n, …)

- A **MAC layer**
  How to access the medium, how to manage the collisions, …

IEEE 802.11b

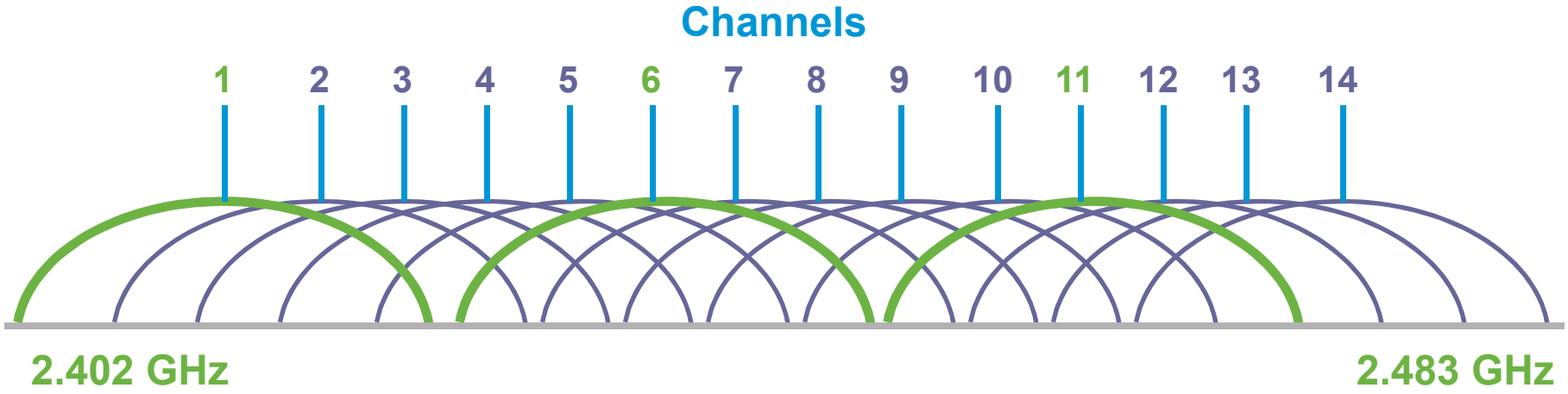
- Ratified as standard in Sept, 1999
- Uses 2.4 GHz unlicensed spectrum
- Different physical access defined (PHY)

  Direct sequence at 1, 2, 5.5, and 11 Mbps,
  Can “downshift” to lower data rates for longer range

  Frequency hopping at 1 and 2 Mbps for 2.4 Ghz (legacy)

  Infrared (obsolete)
- 11 US channels, 13 ETSI channels, 14 Japan channels
- Generally approved for worldwide use in many countries

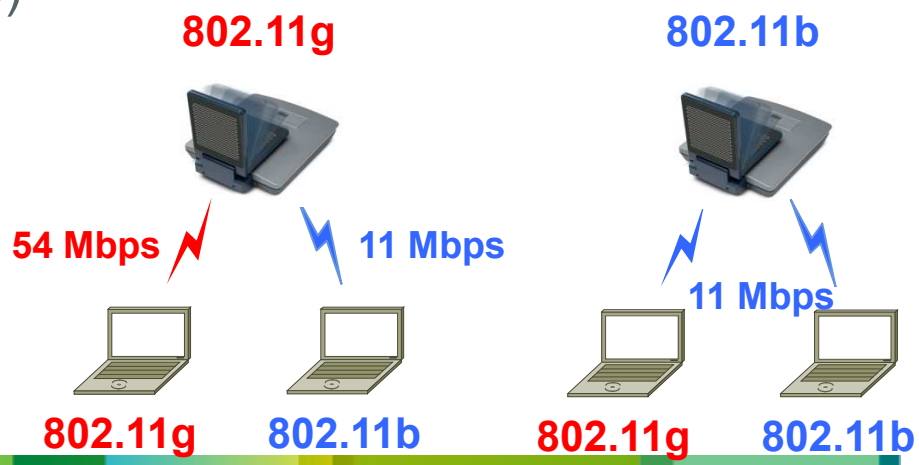
IEEE 802.11b
Direct Sequence @ 2.4 GHz



- Up to (14) 22 MHz wide channels
- 3 non-overlapping channels (1, 6, 11)
- Up to 11 Mbps data rate
- 3 access points can occupy the same space for a total of 33 Mbps aggregate throughput, but not on same radio card

IEEE 802.11g

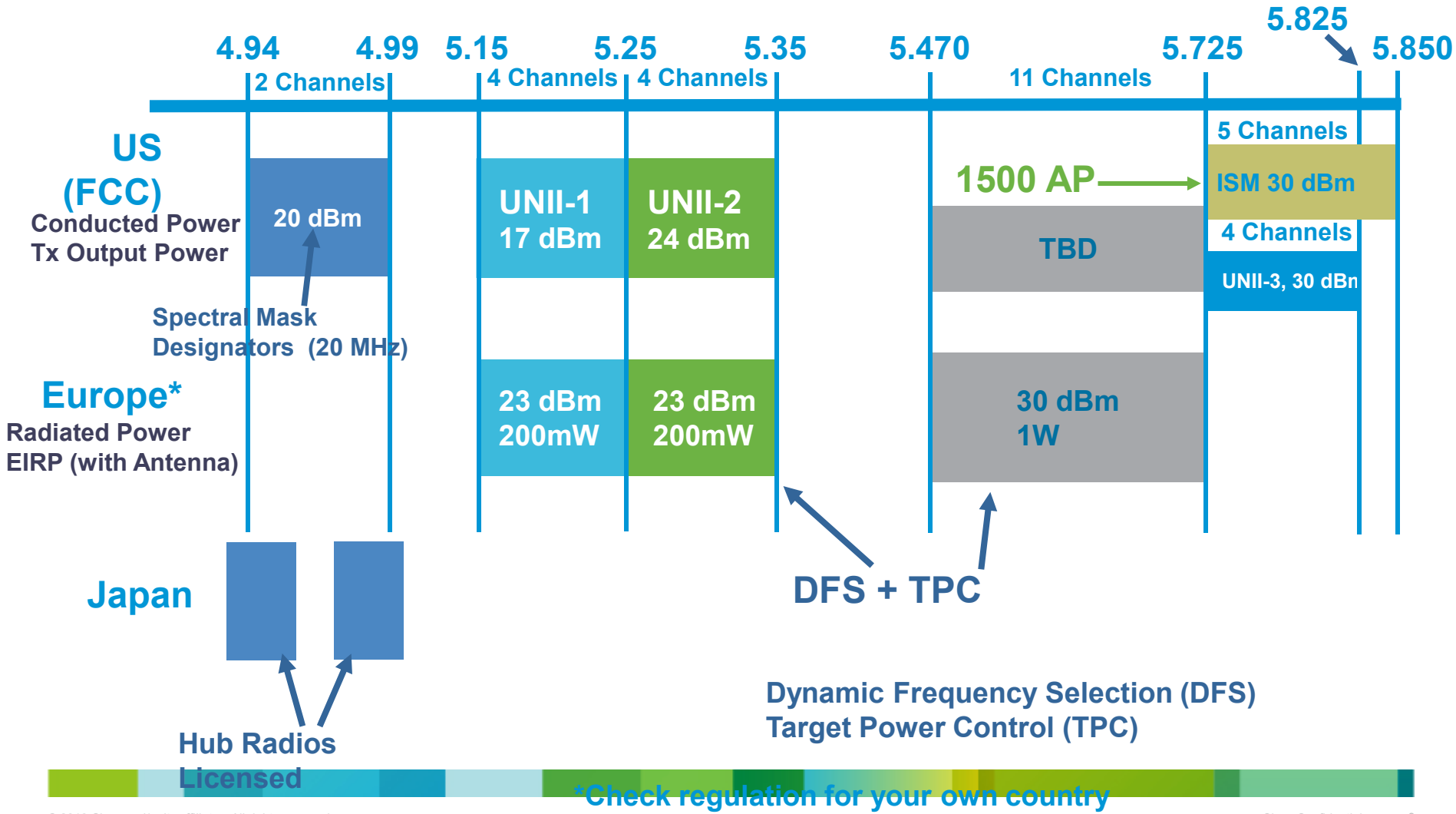
- Ratified as standard in June, 2003
- Same frequencies as IEEE 802.11b (2.4 GHz)
- Backward compatible with 802.11b
- Orthogonal Frequency Division Multiplexing (OFDM)
  - Data rates supported: 54, 48, 36, 24, 12, and 6 Mbps
- Direct sequence (802.11b backwards compatible)
  - Data rates: 1, 2, 5.5, and 11 Mbps



IEEE 802.11a

- Ratified as standard in Sept, 1999
- Orthogonal Frequency Division Multiplexing (OFDM)
  - Data rates supported: 54, 48, 36, 24, 12, and 6 Mbps
  - Can “downshift” to lower data rates for longer range
- Compliant in some countries
- 5 GHz band has more channels than 2.4 GHz band
  - 19 non-overlapping channels in ETSI Regulation Area
  - (vs. 3 channels for 2.4 GHz) for greater scalability

Current State of 5 GHz Bridging Spectrum



Topics

- Wifi standard evolution (phy layer):
  - 802.11a,b,g
  - *802.11n*
  - 802.11ac and the future
- How to cope with interference: Cisco CleanAir and Clientlink technology
- Wireless security: Wireless IDS/IPS

Extra topic (if time allows)

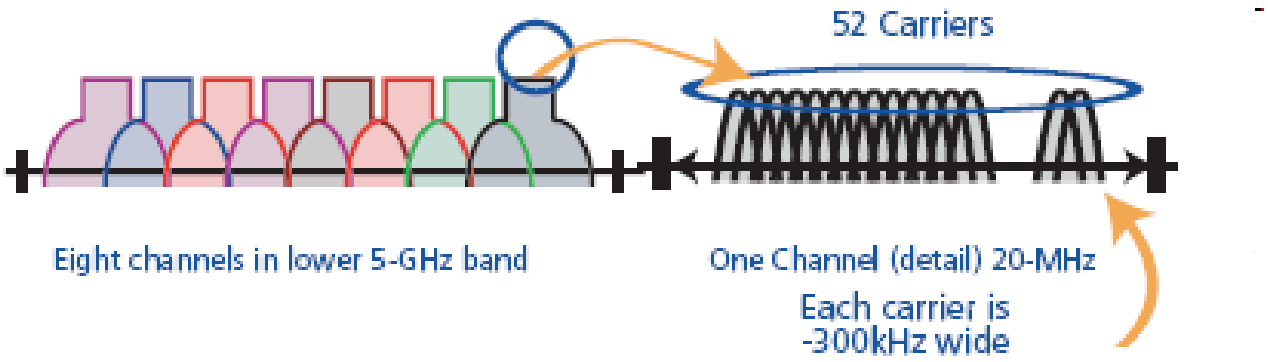
- Cisco Convereged Access

PHY Enhancement Steps

- Modified OFDM : 54 Mbps > 58.5 Mbps
- Forward Error Correction (FEC) : 58.5 Mbps > 65 Mbps
- Shorter Guard Interval (GI) : 65 Mbps > 72.2 Mbps
- Channel Bonding : 72.2 Mbps > 150 Mbps
- Spatial Multiplexing : 150 Mbps > 300 Mbps (up to 600 Mbps)

Modified OFDM : 54 Mbps > 58.5 Mbps

- The number of OFDM data sub-carriers on a 20 MHz channel is increased from 48 to 52 which improves the maximum throughput from 54 Mbps to 58.5 Mbps.

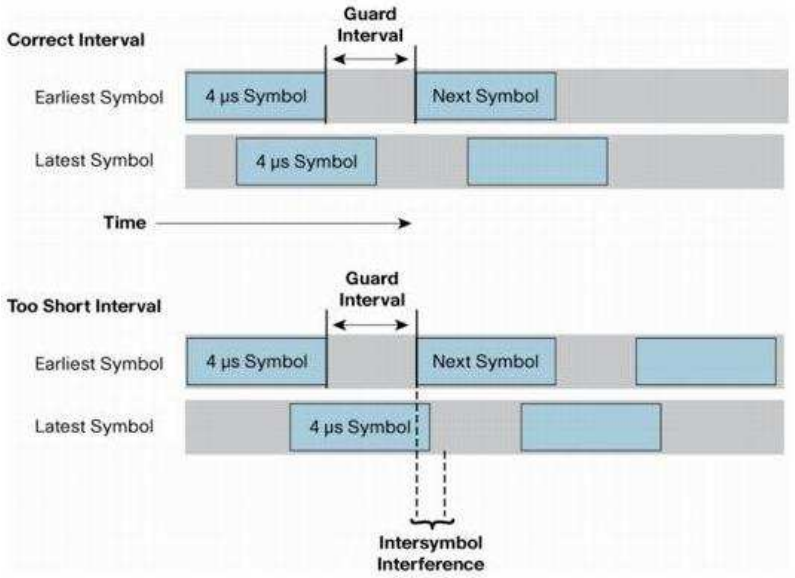


FEC : 58.5 Mbps > 65 Mbps

- FEC is a system of error control whereby the sender adds redundant data to allow the receiver to detect and correct errors.
- 3/4 coding rate is improved with 5/6 boosting the link rate from 58.5 Mbps to 65 Mbps.

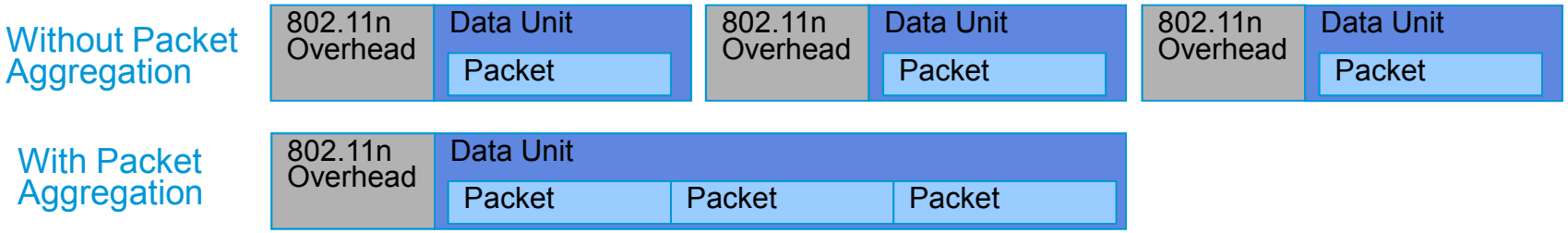
Shorter GI : 65 Mbps > 72.2 Mbps

- The guard interval is the period of time that is used to minimize OFDM intersymbol interference.
- This type of interference is caused in multipath environments when the beginning of a new symbol arrives at the receiver before the end of the last symbol is done.
- These two symbols arrive over two different paths. The "late" symbol that has not yet been completely received when the new symbol arrives traveled a longer path than the new symbol.
- The guard interval is a quiet period between symbols that provides for the arrival of late symbols over long paths. The length of the guard interval is selected for the severity of the multipath environment. 802.11a and 802.11g use 800 nanoseconds as the guard interval.



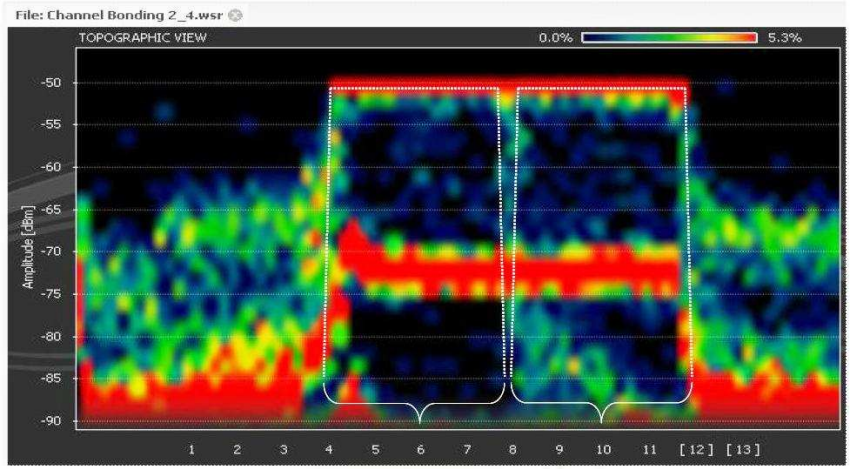
802.11n Packet Aggregation

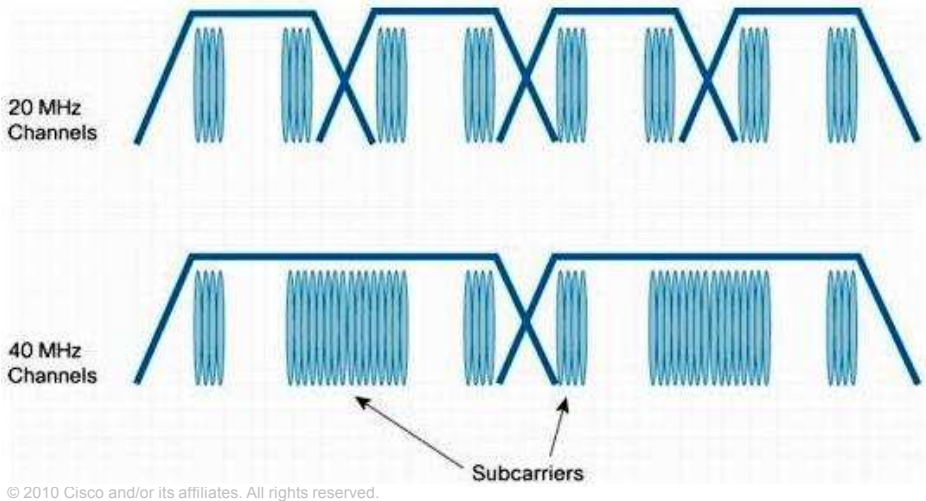
Packet Aggregation:
Combine multiple data units into one frame
Saves on 802.11n and MAC overhead



Channel Bonding : 72.2 Mbps > 150 Mbps

- Doubling channel bandwidth from 20 to 40 MHz slightly more than doubles rate from 72.2 to 150 Mbps.





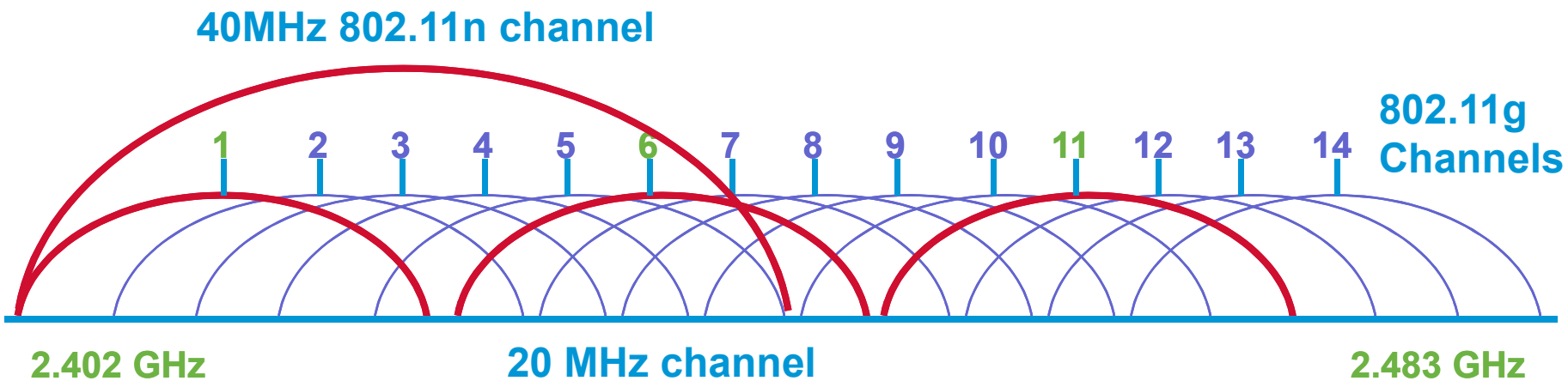
802.11n takes advantage of the fact that each 20-MHz channel has a small amount of the channel that is reserved at the top and bottom, to reduce interference in those adjacent channels.

When using 40-MHz channels, the top of the lower channel and the bottom of the upper channel don't have to be reserved to avoid interference.

These small parts of the channel can now be used to carry information.

By using the two 20-MHz channels more efficiently in this way, 802.11n achieves slightly more than doubling the data rate when moving from 20-MHz to 40-MHz channels.

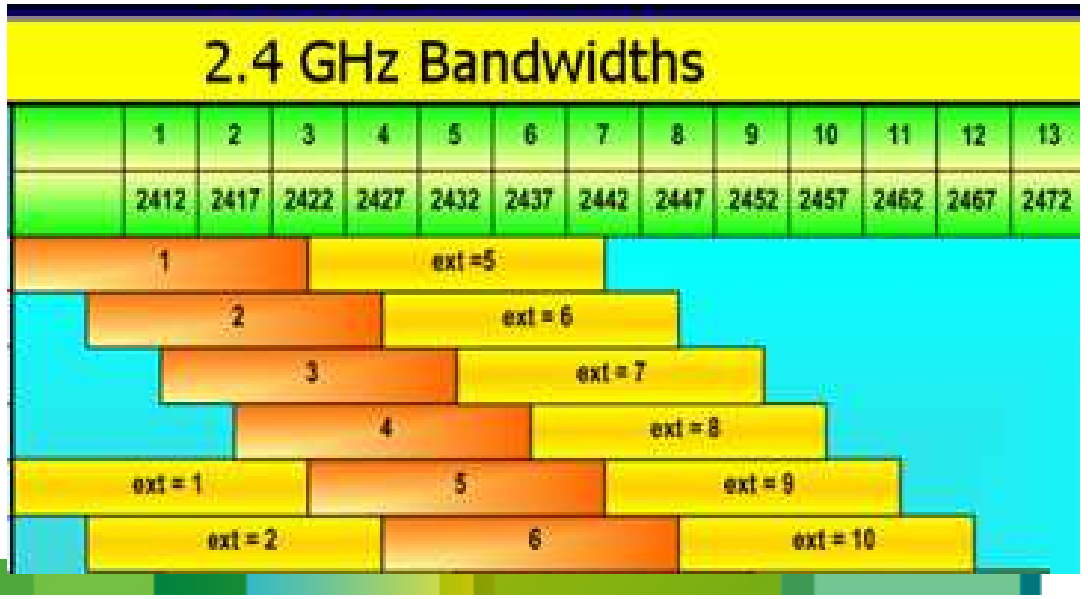
Channel Bonding in 2.4GHz



When you bond a channel you define the control channel and then the extended data channel.

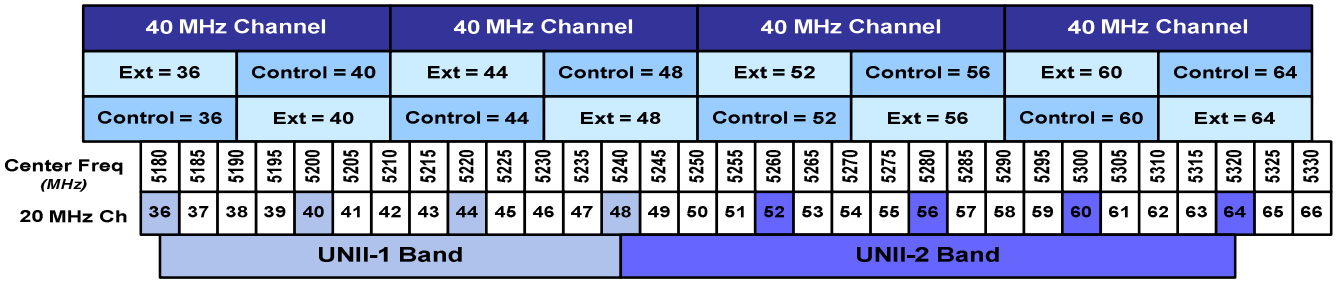
Legacy clients use only the control channel, also for data communication.

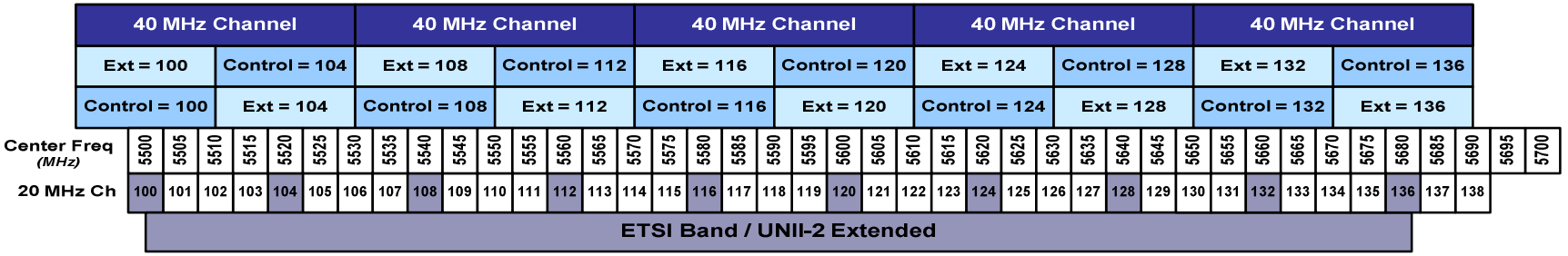
The extension channel is the bonded channel that 802.11n clients use in addition to the control channel for higher throughput, as they send data on BOTH channels.

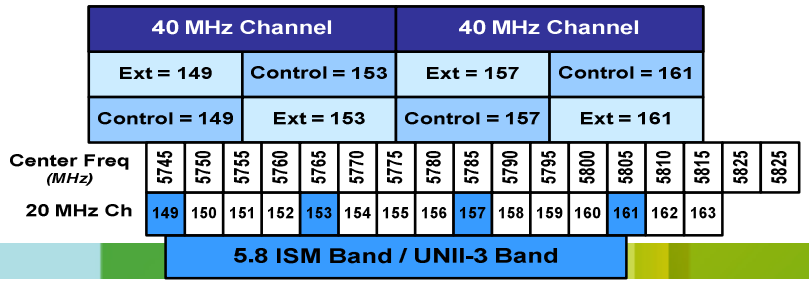


Channel Bonding in 5 GHz

5 GHz Bandwidths

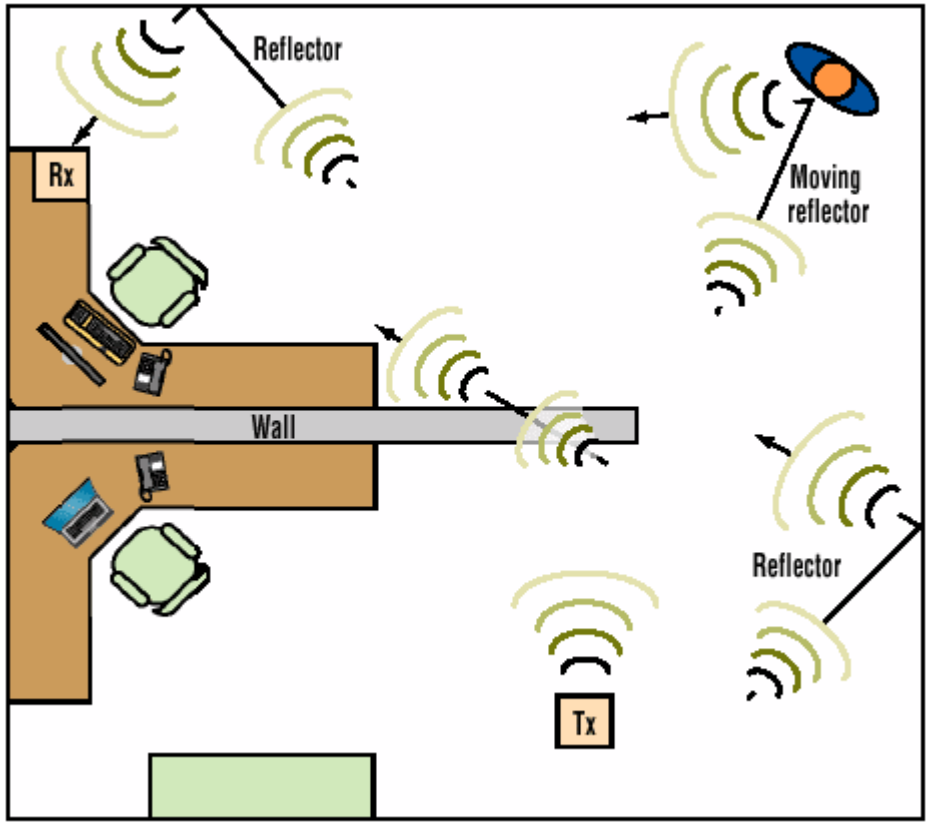






MIMO – Multi Inputs and Outputs

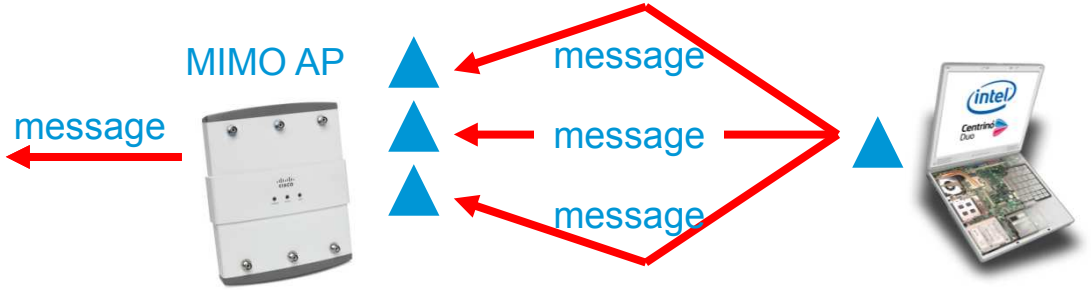
- MIMO takes advantage of multi path



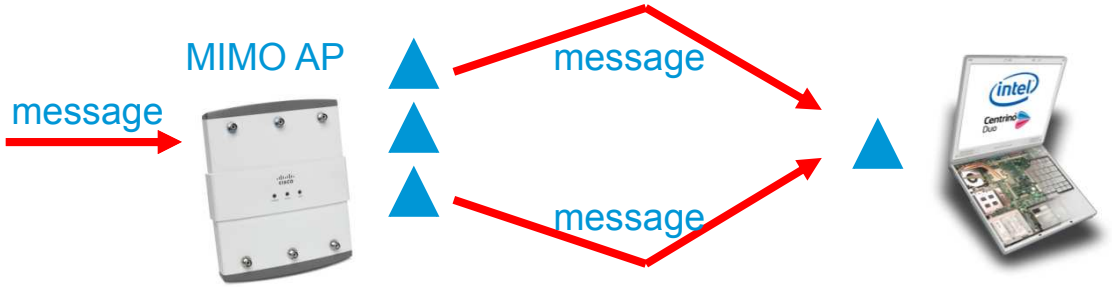
Office environment multiple paths from transmitter to receiver

MIMO Overview

Maximal Ratio Combining
- Performed by receiver
- Combines multiple received signals
- Increases receive sensitivity
- Works with non-MIMO and MIMO clients



Transmit beam forming
- Performed by transmitter
- Ensures signal received in phase
- Increases receive sensitivity
- Works with non-MIMO and MIMO clients

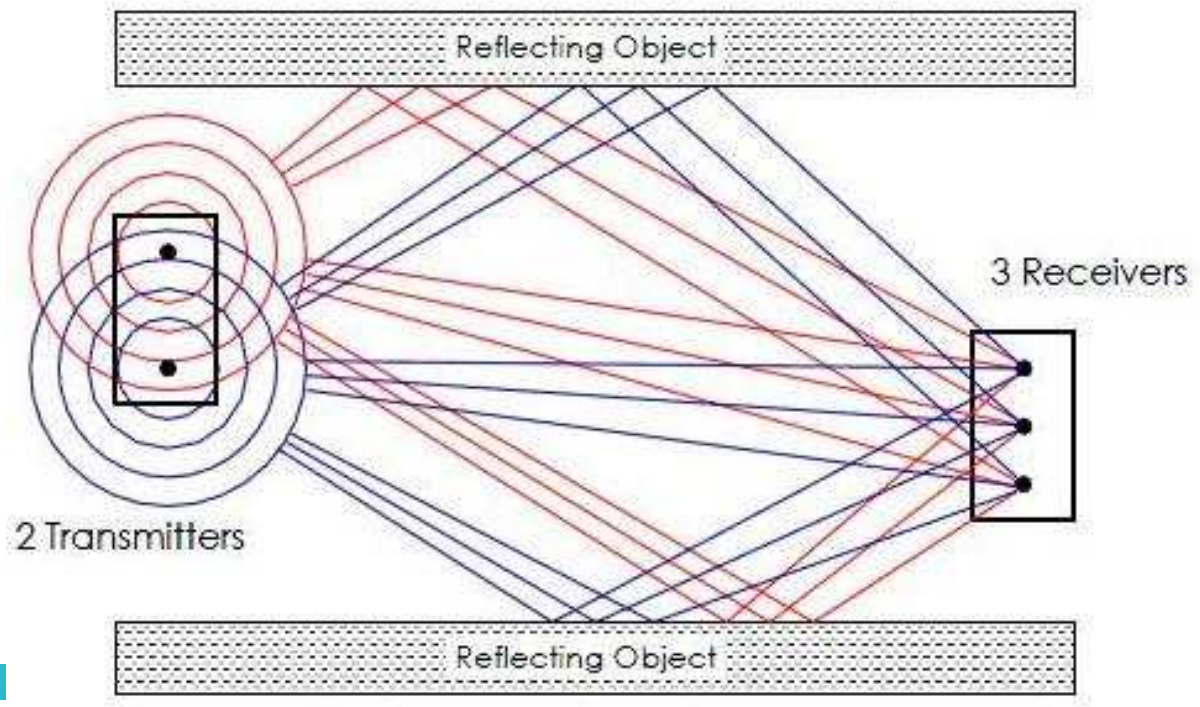


Spatial Multiplexing
- Transmitter and receiver participate
- Multiple antennas transmit concurrently on same channel
- Increases bandwidth
- Requires MIMO client

Spatial Multiplexing : 150 Mbps > 300 Mbps

Multipath (RF signal reflection between transmitter and receiver) is normally the enemy of performance, but with MIMO it is used constructively.

A signal stream is broken down into multiple signal streams, each transmitted from a different antenna. Each of these “spatial” streams arrives at the receiver with different amplitude (signal strength) and phase.



PHY Enhancements

				Signal BW =20 MHz		40 MHz	
MCS	**Coding**	**Modulation**	**Streams**	**GI = 800 nS**	**GI =400 nS**	**GI = 800 nS**	**GI =400 nS**
MCS0	1/2	BPSK	1	6.5	7.2	13.5	15
MCS1	1/2	QPSK	1	13	14.4	27	30
MCS2	3/4	QPSK	1	19.5	21.7	40.5	45
MCS3	1/2	16-QAM	1	26	28.9	54	60
MCS4	3/4	16-QAM	1	39	43.3	81	90
MCS5	2/3	64-QAM	1	52	57.8	108	120
MCS6	3/4	64-QAM	1	58.5	65	131.5	135
MCS7	5/6	64-QAM	1	65	72.2	135	150
MCS8	1/2	BPSK	2	13	14.4	27	30
MCS9	1/2	QPSK	2	26	28.9	54	60
MCS10	3/4	QPSK	2	39	43.3	81	90
MCS11	1/2	16-QAM	2	52	57.8	108	120
MCS12	3/4	16-QAM	2	78	86.7	162	180
MCS13	2/3	64-QAM	2	104	115.6	216	240
MCS14	3/4	64-QAM	2	117	130	243	270
MCS15	5/6	64-QAM	2	130	144.4	270	300
MCS16	1/2	BPSK	3	19.5	21.7	40.5	45
MCS17	1/2	QPSK	3	39	43.3	81	90
MCS18	3/4	QPSK	3	58.5	65	121.5	135
MCS19	1/2	16-QAM	3	78	86.7	162	180
MCS20	3/4	16-QAM	3	117	130	243	270
MCS21	2/3	64-QAM	3	156	173.3	324	360
MCS22	3/4	64-QAM	3	175.5	195	364.5	405
MCS23	5/6	64-QAM	3	195	216.7	405	450

Topics

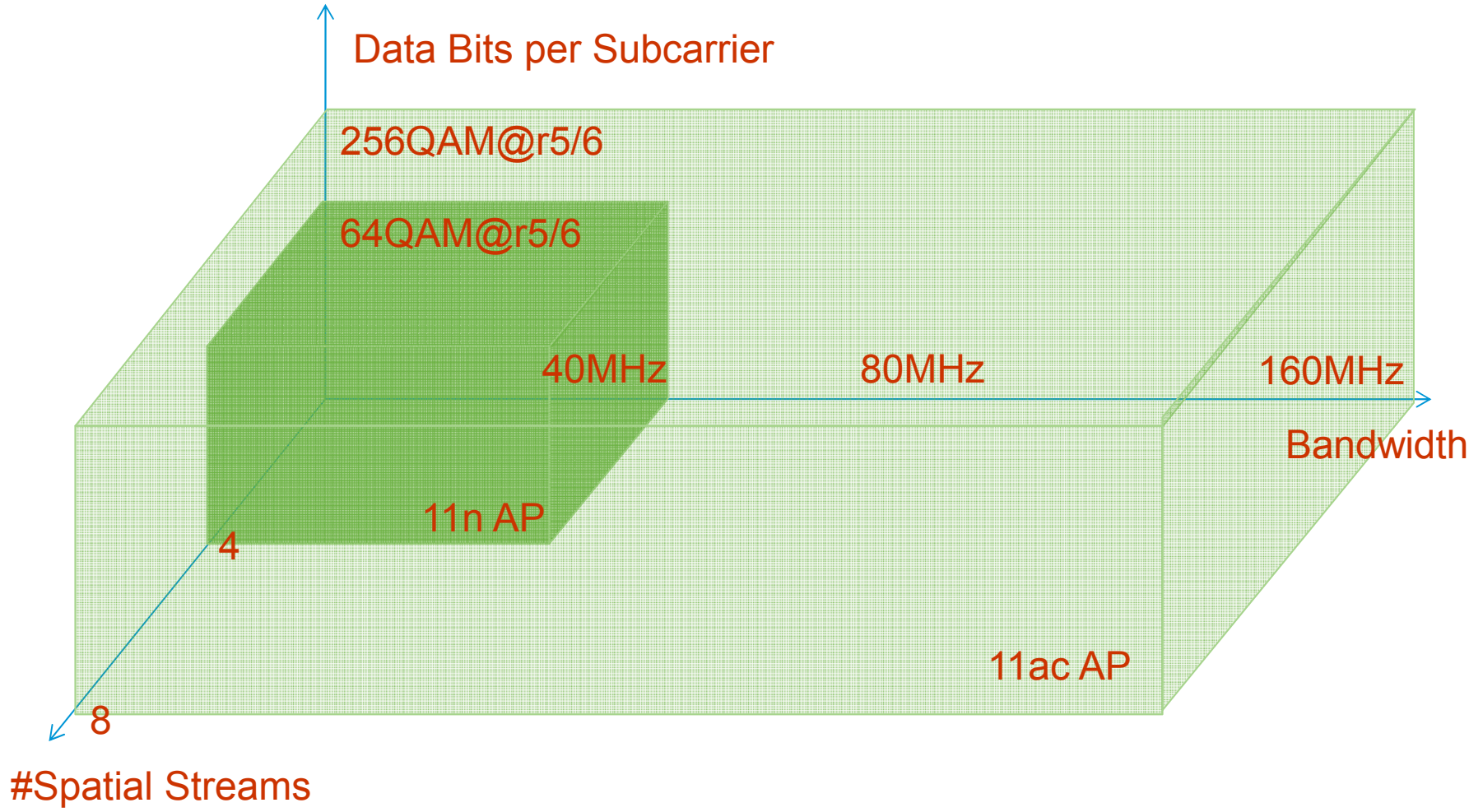
- Wifi standard evolution (phy layer):
  - 802.11a,b,g
  - 802.11n
  - *802.11ac and the future*
- How to cope with interference: Cisco CleanAir and Clientlink technology
- Wireless security: Wireless IDS/IPS

802.11ac – Extend the 11n User Experience

- Support the same use cases
  - Data/video/voice
- With similar range
  - 30-100+ ft range
- But faster, more in line with 1GigE
  - E.g. can support multiple HD video streams at range
- And maintain these benefits even for smartphones/tablets
  - With just one antenna

802.11ac Core Technology

How Can We Make11n Go Faster?



802.11ac: Important Numbers

- For battery-powered APs and clients, the yellow row is mandatory
- For wall-powered APs, the blue row is mandatory
- Gigabit rates for some plausible product configurations (orange rows)
- 11ac offers significant upside compared with 11n (white rows)

BW (MHz)	#Spat Strm	MCS (QAMr5/6)	PHY rate (Mbps)	MAC thruput (Mbps)*
40	2	64	**300**	**210**
80	1	64	**330**	**230**
80	1	256	**430**	**300**
80	2	64	**650**	**460**
80	2	256	**870**	**610**
80	3	64	**980**	**680**
80	3	256	**1300**	**910**
80	4	256	**1700**	**1200**
80	8	256	**3500**	**2400**

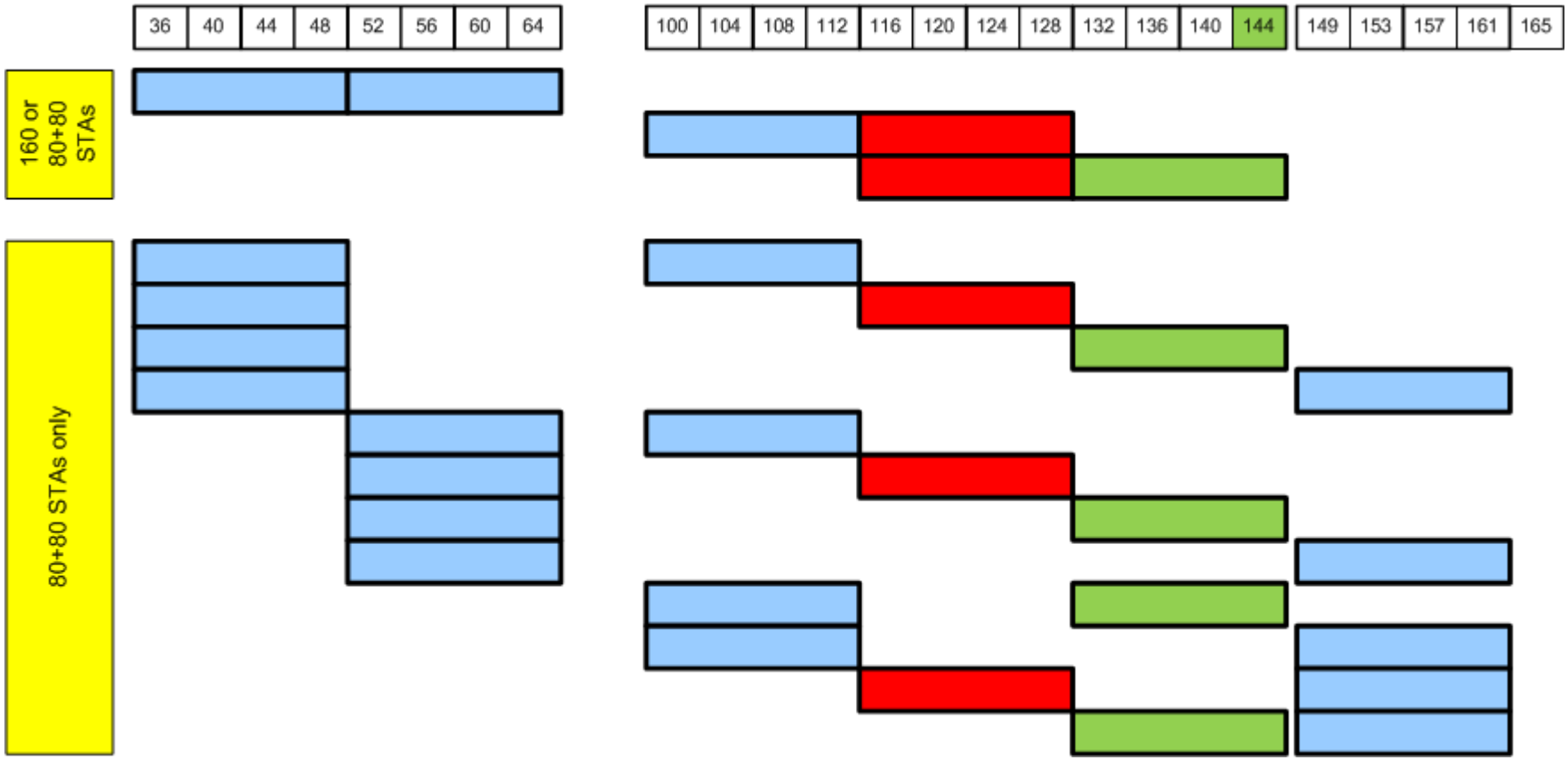
BW (MHz)	#Spat Strm	MCS (QAMr5/6)	PHY rate (Mbps)	MAC thruput (Mbps)*
40	3	64	**450**	**320**
160	1	64	**650**	**460**
160	1	256	**870**	**610**
160	2	64	**1300**	**910**
160	2	256	**1700**	**1200**
160	3	64	**2000**	**1400**
160	3	256	**2600**	**1800**
160	4	256	**3500**	**2400**
160	8	256	**6900**	**4900**

*Assuming 70% efficiency

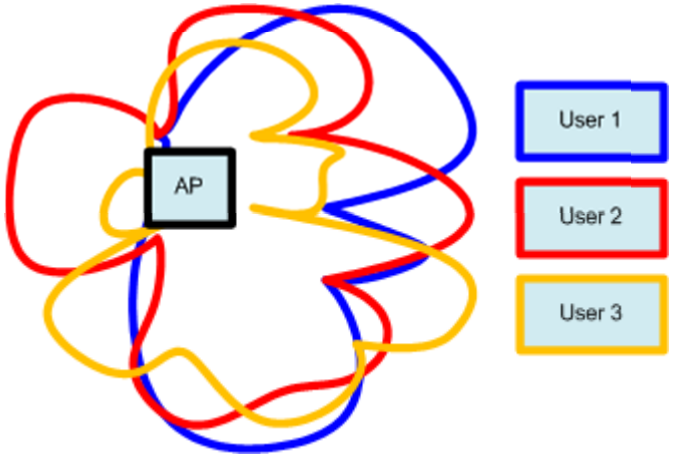
802.11ac Technology Overview

- 5 GHz only (not 2.4 GHz)
  - Although 256 QAM, VHT sounding and MU-MIMO are possible at 2.4 GHz
- 80 MHz
  - Optional 160 MHz, 80+80MHz
- Optional 256 QAM
- Up to 8 space time streams
  - 1 SS mandatory, 2 SS mandatory for non-battery powered APs at WFA
- A single interoperable (though optional) sounding mechanism for beamform training
- Optional MU-MIMO
  - Cool new technology
- RTS/CTS improvements for wider bandwidths

160 MHz and 80+80 MHz - Diagrammatically



What is MU-MIMO?



- 11n offers Single User MIMO (SU-MIMO)
- 11ac adds Multi-User MIMO (MU-MIMO)

  Instead of one frame for one receiver, there are multiple simultaneous frames for multiple receivers

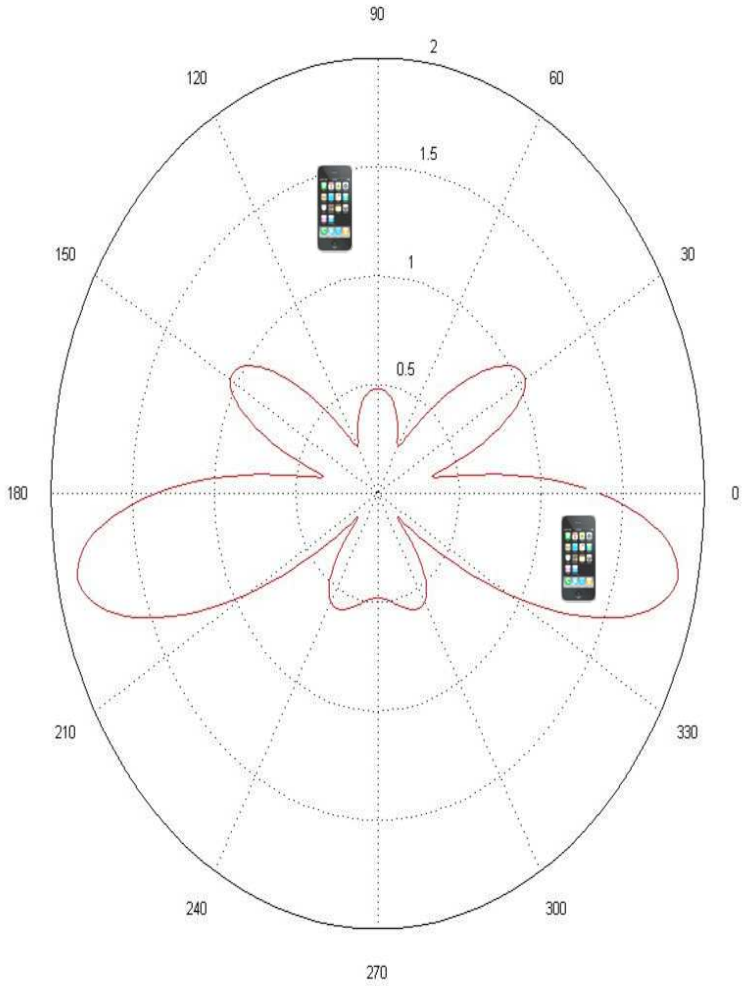
  e.g. An AP with 4 antennas can send 1 stream each to 3 smartphones, all at the same time

  This is a tricky technology: the AP must beamform 1 space-time stream to the first receiver and simultaneously null-steer that space-time streams to the two other receivers

  And simultaneously repeat this process for the two other users!

- “Switch” technology versus SU-MIMO “hub” technology

How MU-MIMO Increases Throughput over SU-MIMO



MU-MIMO

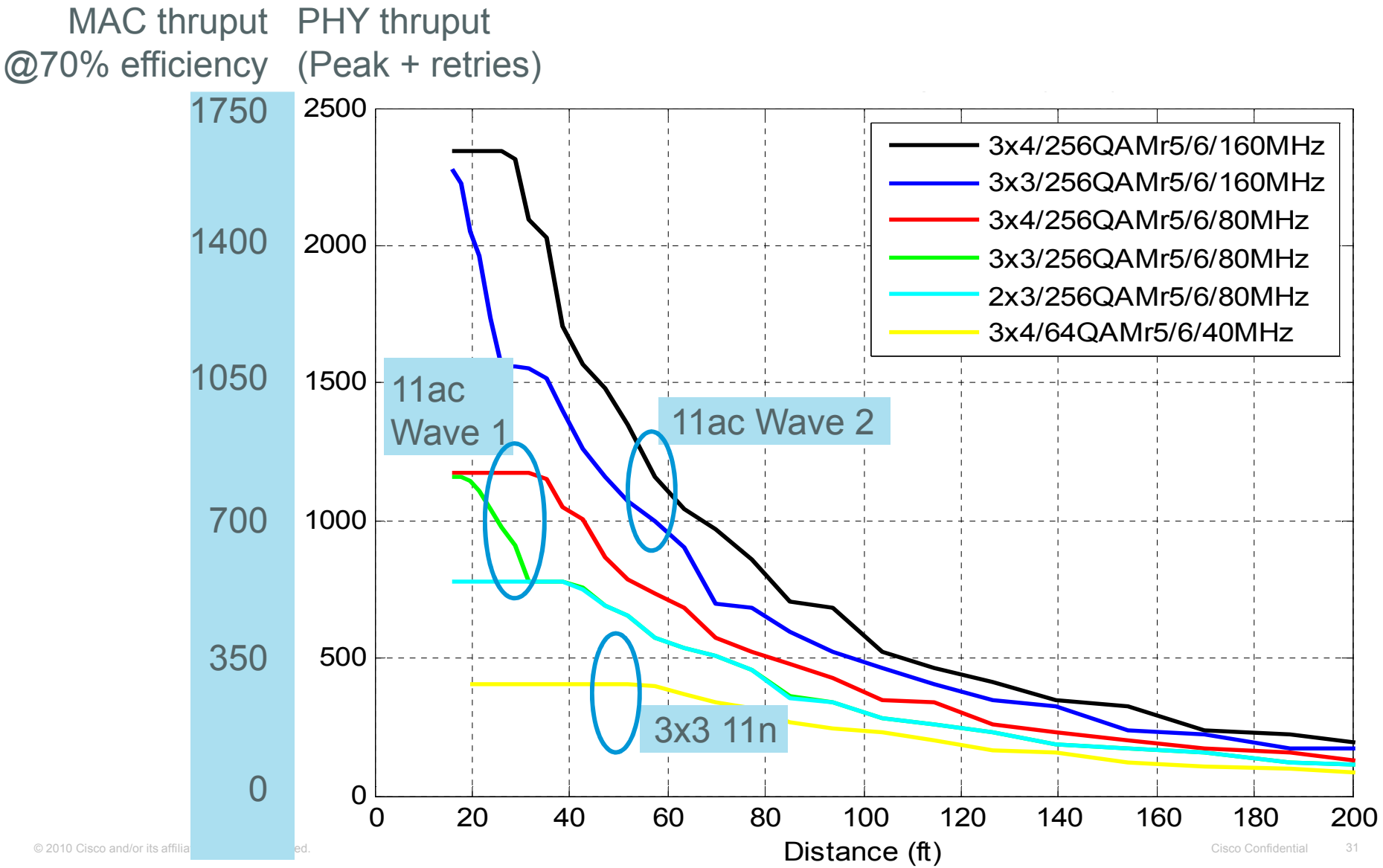
Client 2 DL Frame

Client 2 DL Frame

Client 1 DL Frame

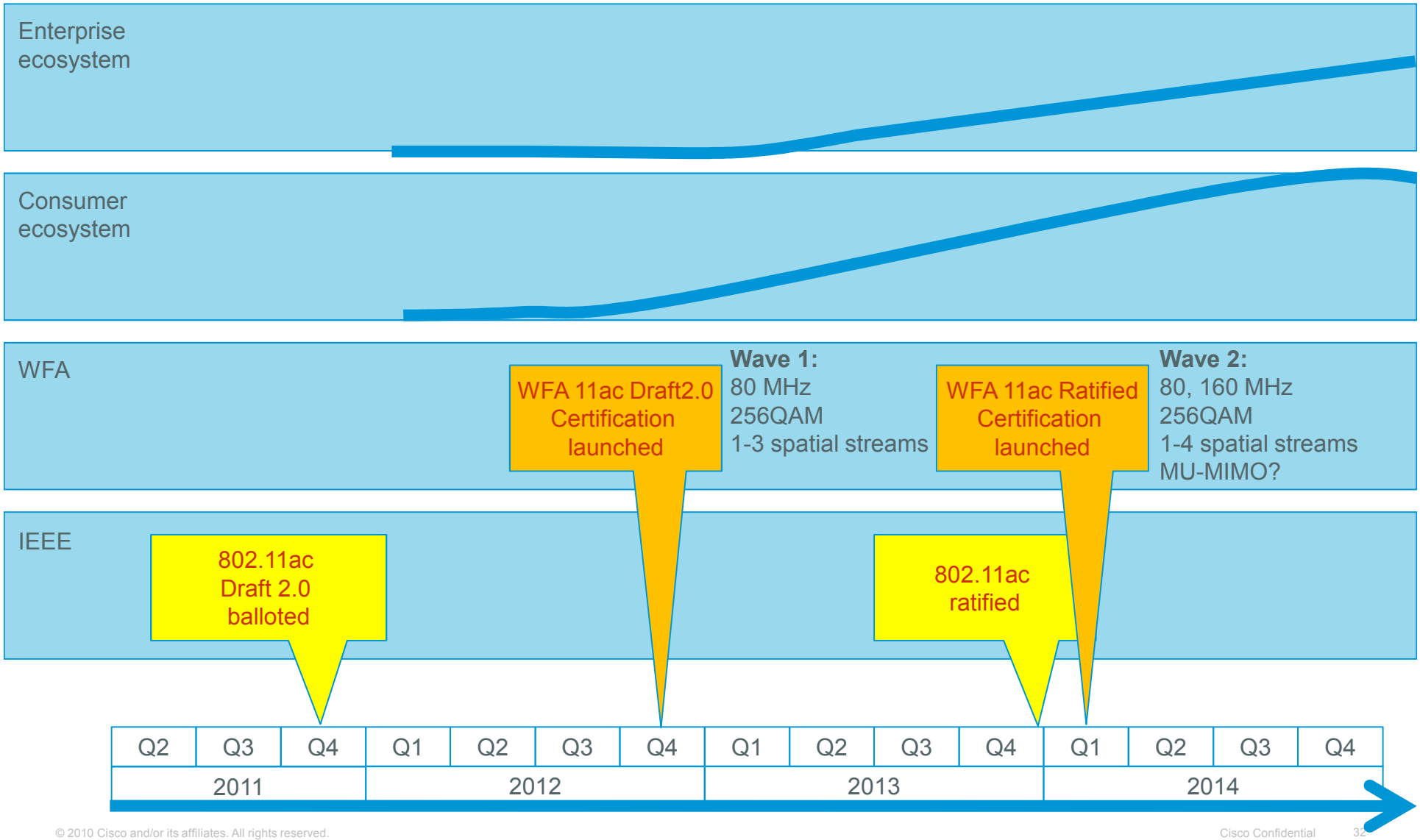
Client 1 DL Frame

Rate-at-range of 11ac significantly outperforms 11n

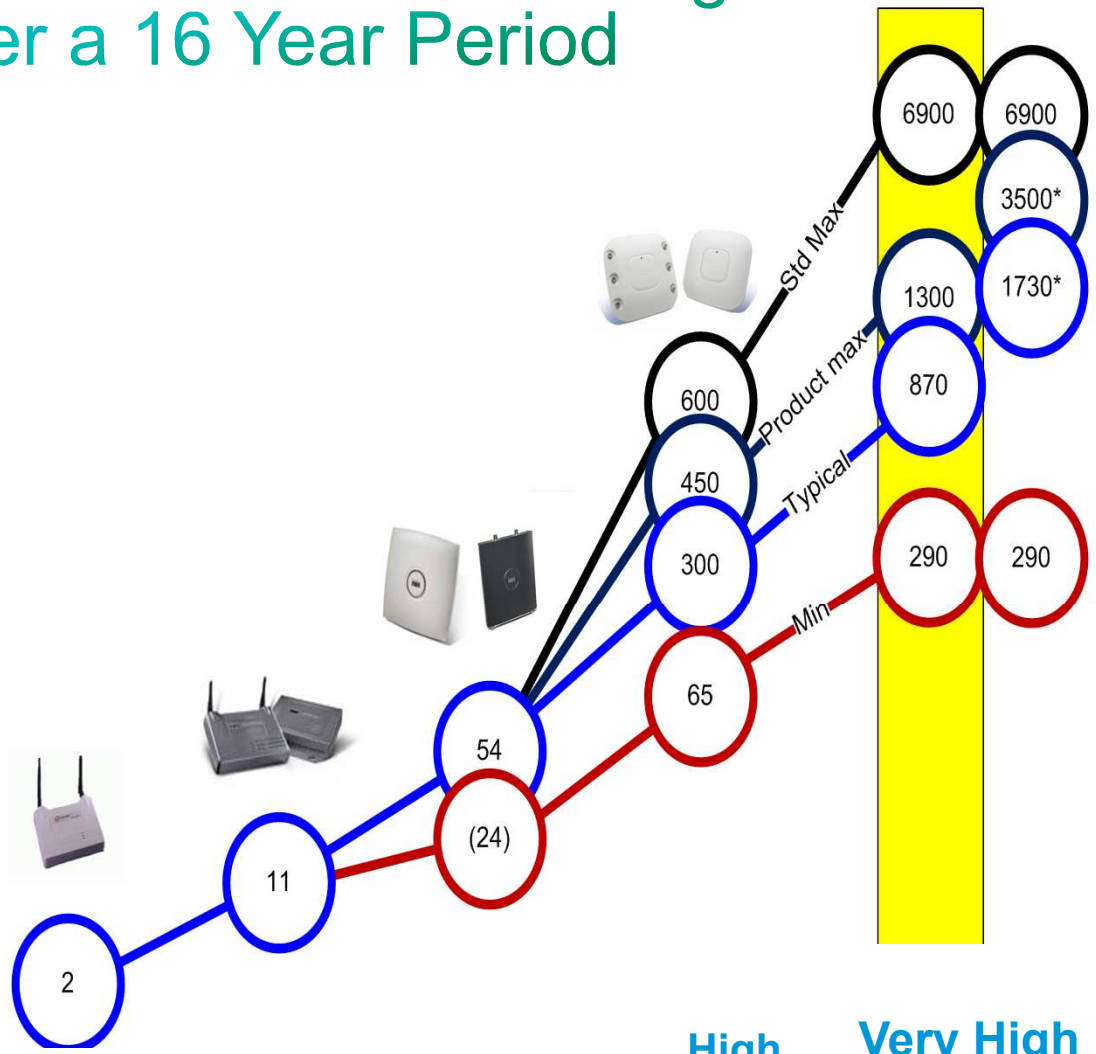


Timelines

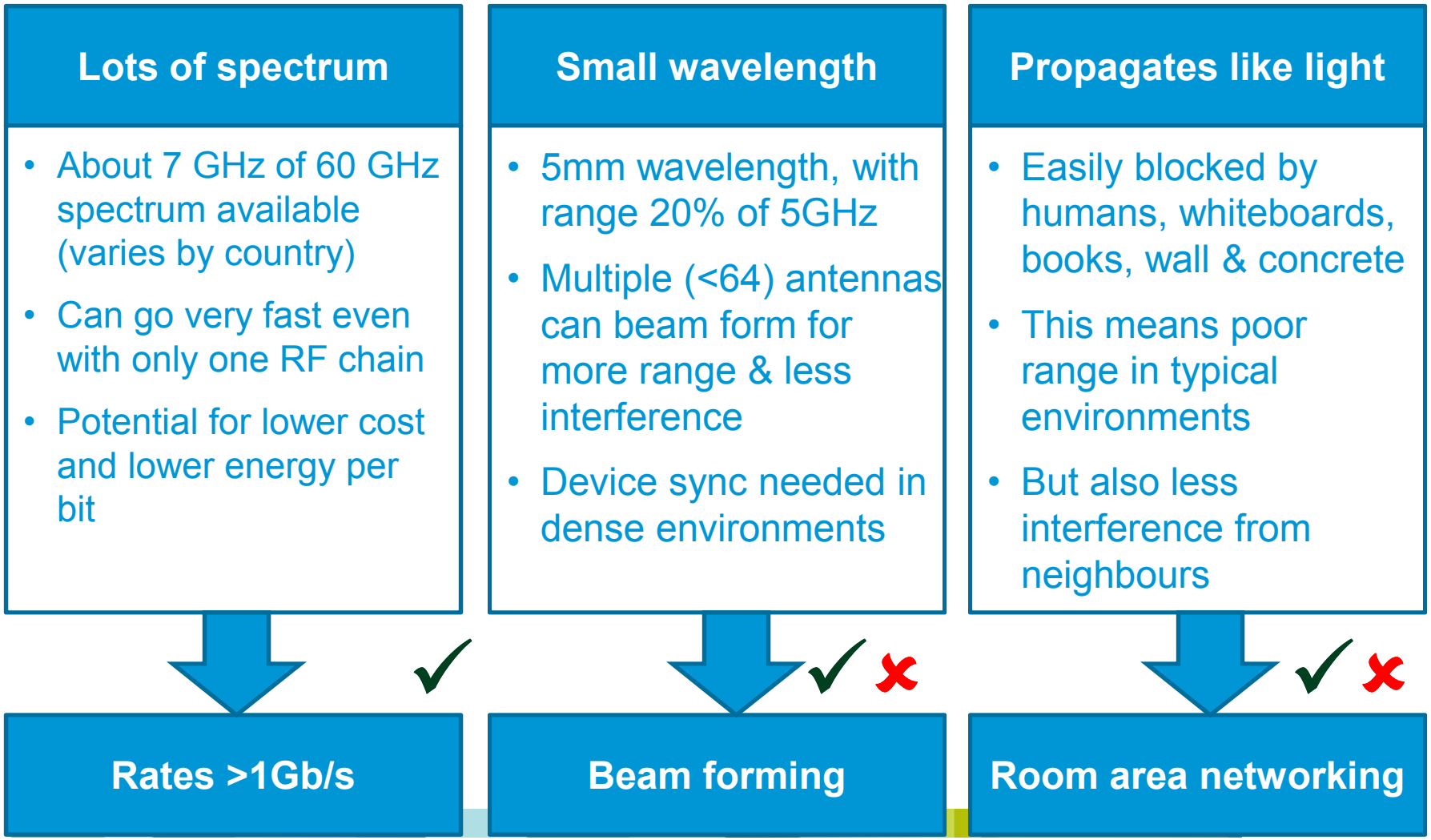
802.11ac is not a factor in the enterprise for 18-24 months



802.11ac is at the End of a Progression to Higher Rates Over a 16 Year Period



802.11ad (WiGig)



802.11ad: Important Numbers

- The yellow row is mandatory
- Multi-gigabit rates for some plausible product configurations (orange rows)

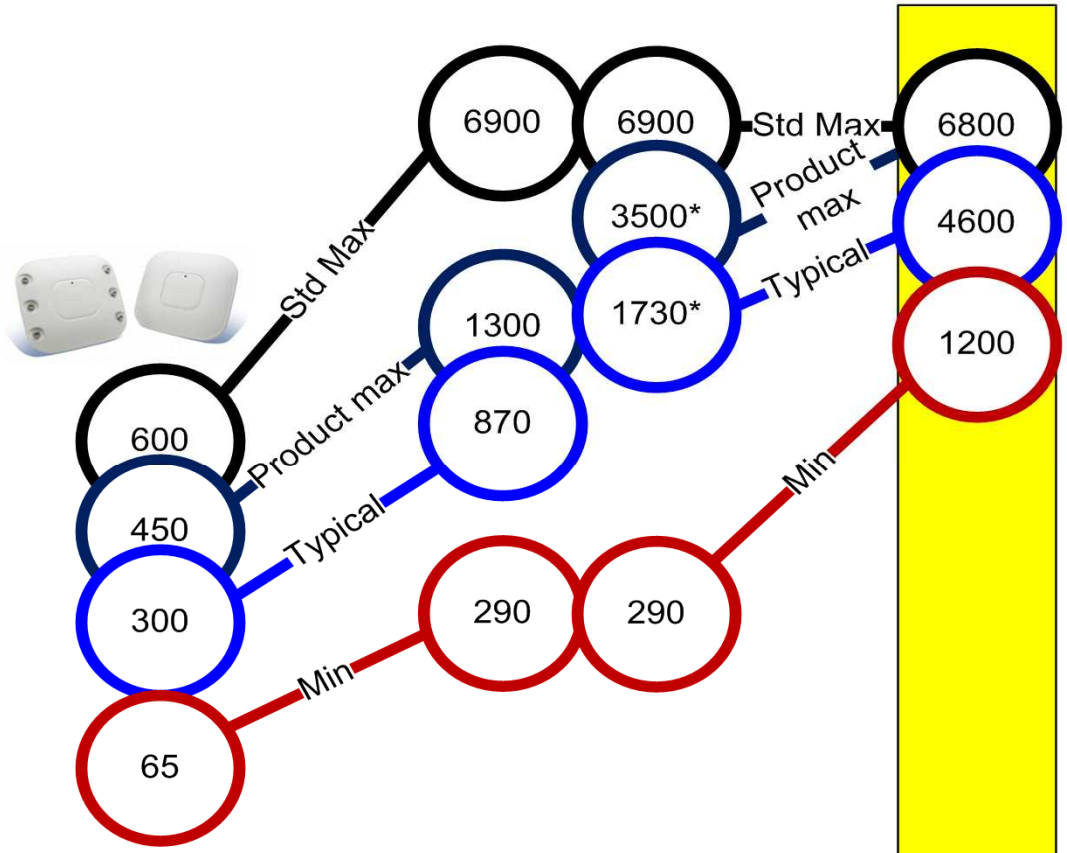
BW (MHz)	#Spat Strm	Modulation	MCS	PHY rate (Mbps)	MAC thruput (Mbps)*
2520	1	SC	BPSK-r3/4	1200	810
2520	1	OFDM	QPSK-r3/4	2100	1500
2520	1	SC	16QAM-r3/4	4600	3200
2520	1	OFDM	64QAM-r13/16	6800	4700

*Assuming 70% efficiency

Wireless Docking for Smartphones, Ultrabooks and Tablets

- Is this the work environment of the future?

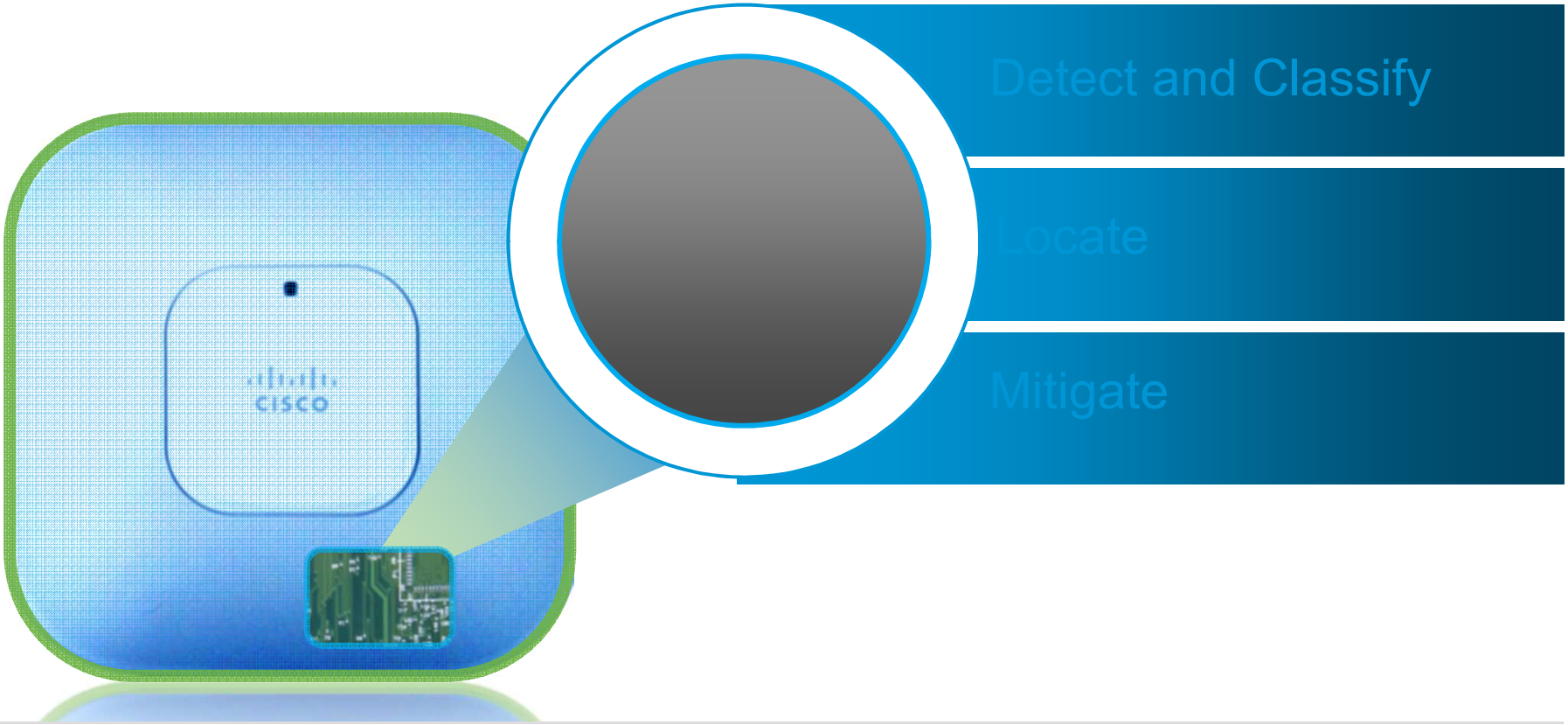
Comparing bandwidth



Topics

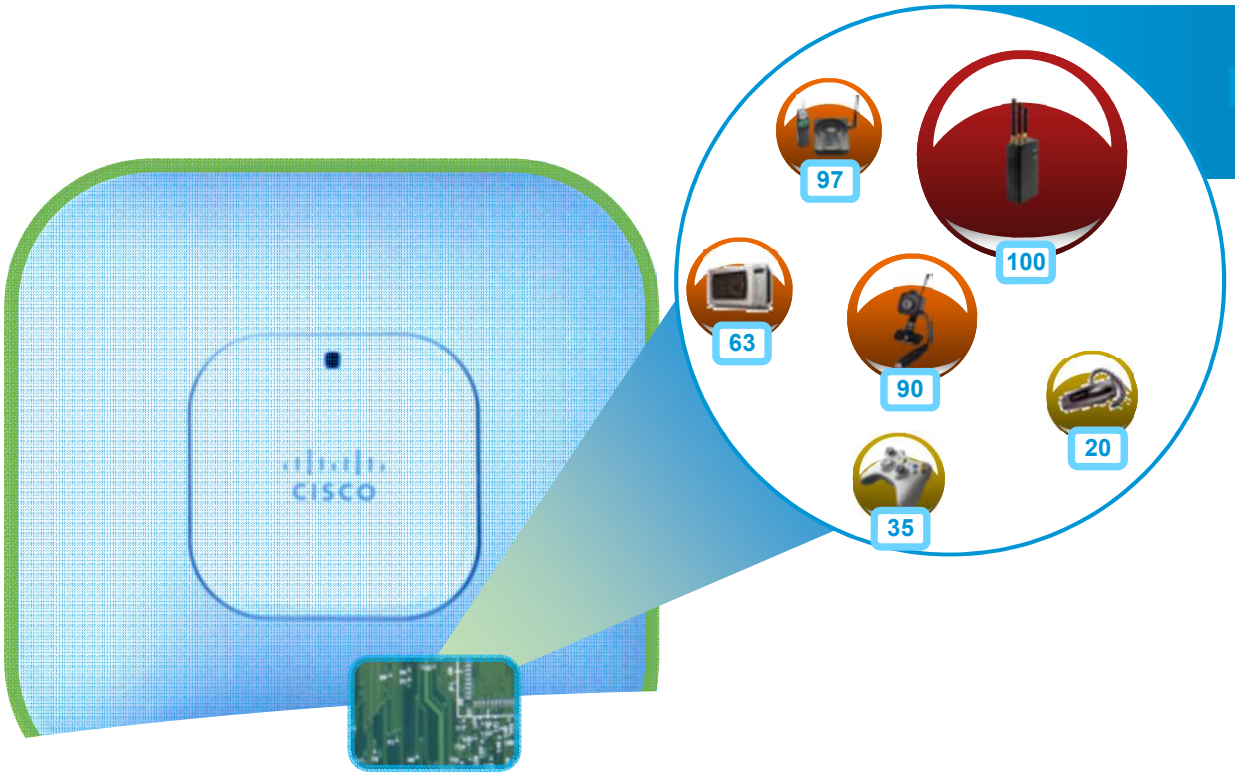
- Wifi standard evolution (phy layer):
  - 802.11a,b,g
  - 802.11n
  - 802.11ac and the future
- How to cope with interference: *Cisco CleanAir* and Clientlink technology
- Wireless security: Wireless IDS/IPS

Introducing CleanAir



A system-wide feature that uses silicon-level intelligence to automatically mitigate the impact of wireless interference, optimize network performance and reduce troubleshooting costs

Detect and classify



Detect and Classify

- Uniquely identify and track multiple interferers
- Assess unique impact to Wi-Fi performance
- Monitor AirQuality

The Impact of a Crowded Spectrum

Performance at Risk in Unprotected Networks

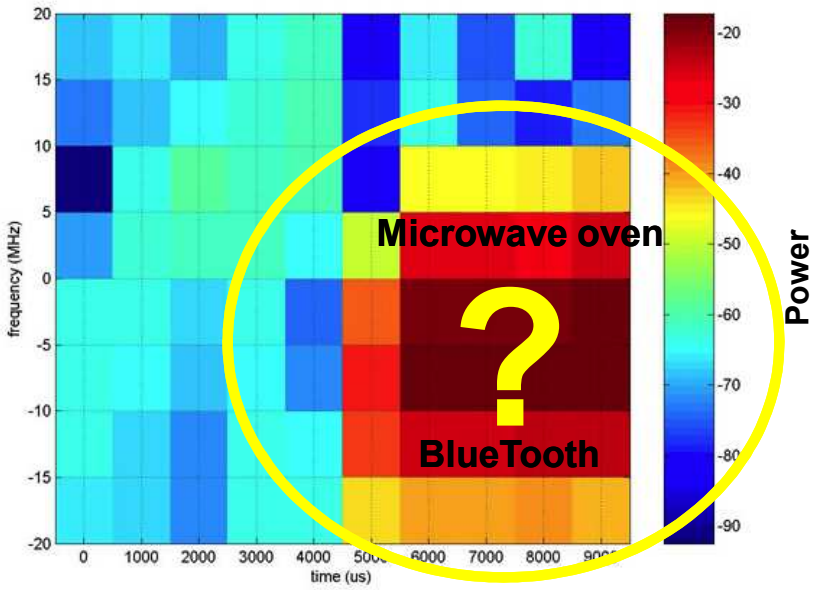
Interference Type		Throughput Reduction	
		Near (25 ft)	Far (75 ft)
2.4 or 5 GHz Cordless Phones		100%	100%
Video Camera		100%	57%
Wi-Fi (busy neighbor)		90%	75%
Microwave Oven		63%	53%
Bluetooth Headset		20%	17%
DECT Phone		18%	10%

Source: FarPoint Group

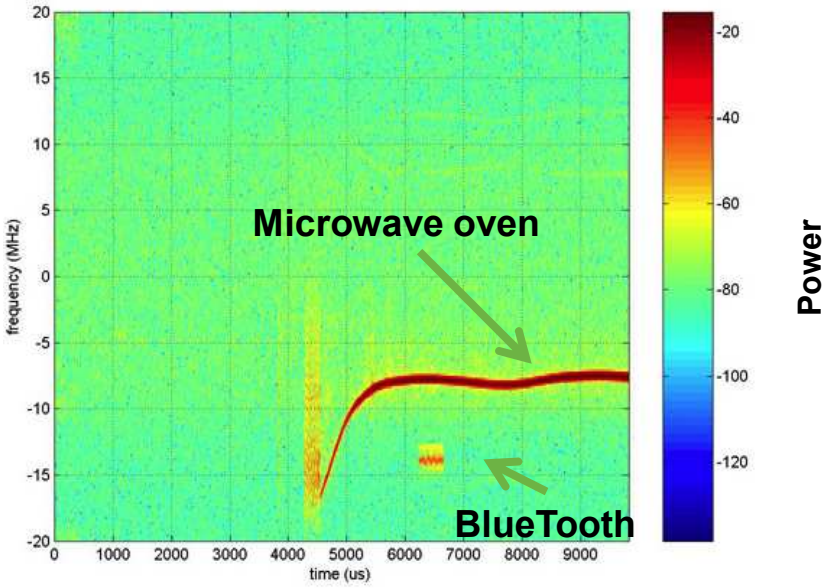
High Resolution Spectral Advantage

The Industry's ONLY in-line high-resolution spectrum analyzer

Typical Wi-Fi chipset
Spectral Resolution at 5 MHz



Cisco CleanAir Wi-Fi chipset
Spectral Resolution at 78 to 156 KHz



'Chip View Visualization' of Microwave oven and BlueTooth Interference

Supported Interferers
Cisco Unified Wireless Network 7.0 Release

- 2.4 GHz only
  - Bluetooth Link
  - Bluetooth Discovery
  - 802.11FH
  - Microwave Oven
  - Industrial wireless/802.15.4
  - Xbox
- 5 GHz only
  - Radar
  - WiMAX Mobile
  - WiMAX Fixed

- 2.4 or 5 GHz
  - Jammer
  - WiFi Inverted
  - WiFi Invalid Channel
  - Continuous Transmitter
  - Video Camera
  - SuperAG
  - Canopy
  - Other (i.e. unclassified devices)
  - TDD Transmitter
  - DECT-like Phone

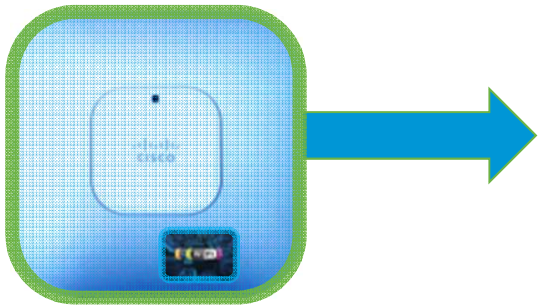
1. Classifiers are expandable over time with software upgrade.
2. All third party trademarks are the property of their respective

Definite Security Threat Devices

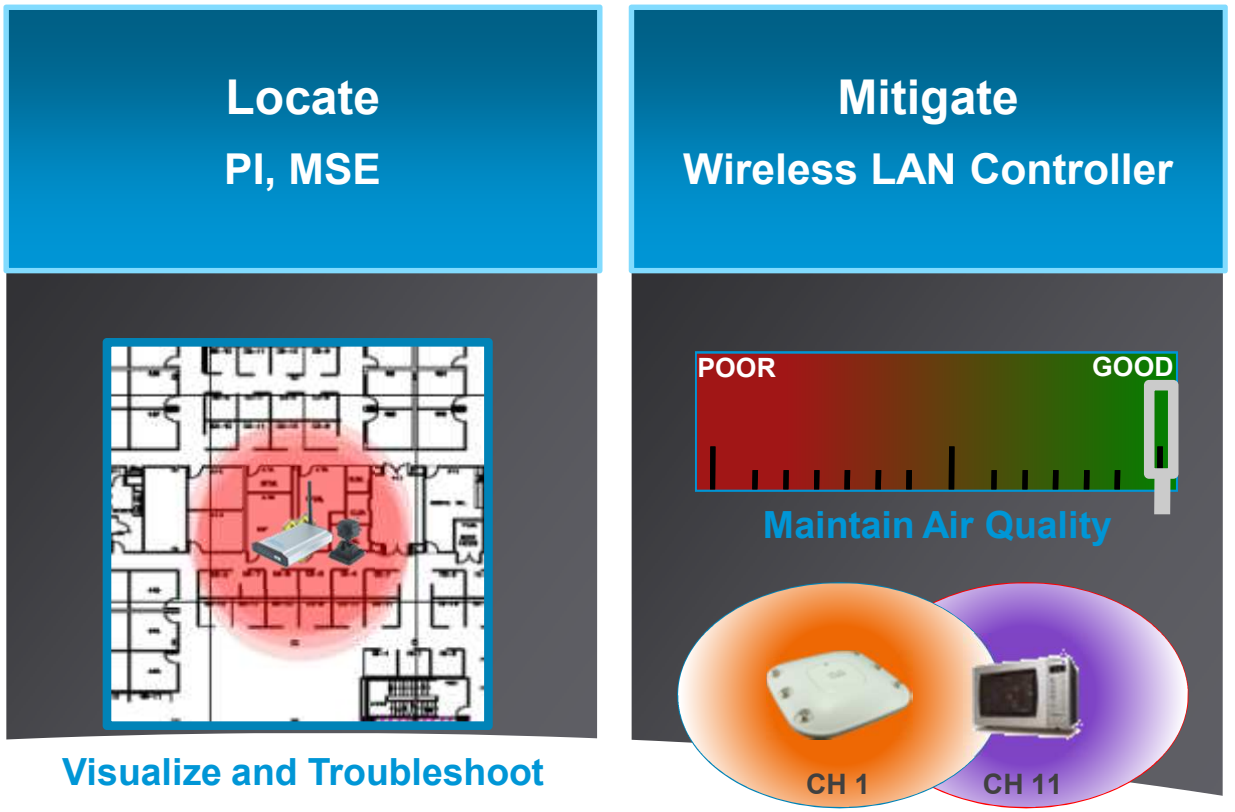
Potential Security Threat Devices

Performance Impacting Devices

Mitigation and locate



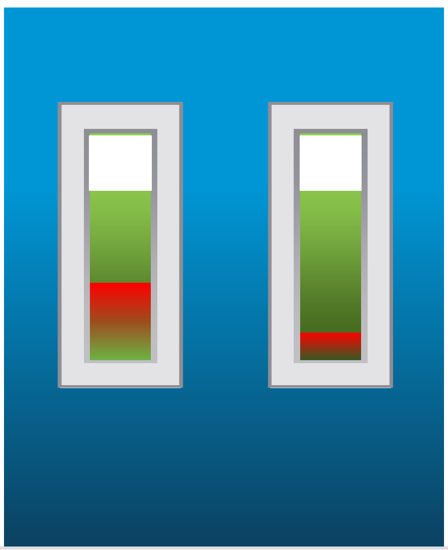
- Classification processed on Access Point
- Interference impact and data sent to WLC for real-time action
- PI and MSE store data for location, history, and troubleshooting

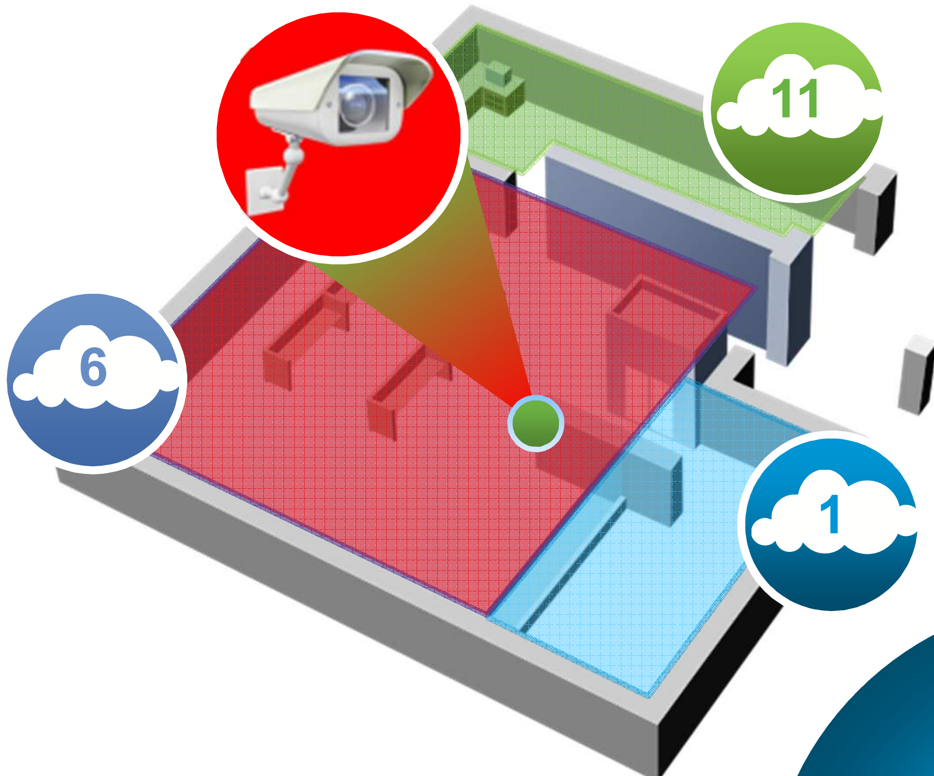


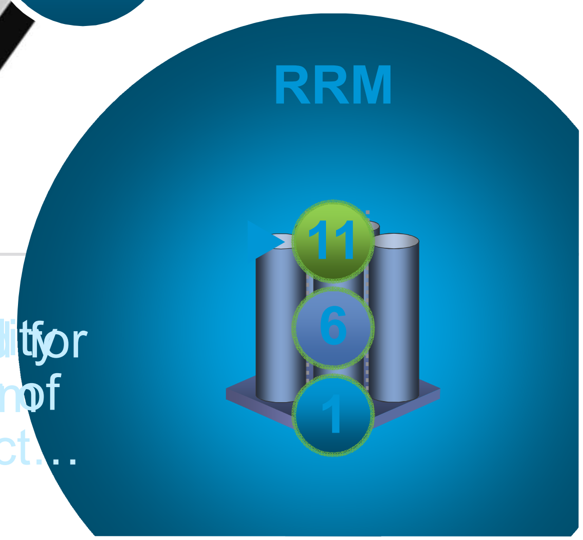
Cisco CleanAir

Cisco CleanAir Technology integrates interference information from the AP into the entire system.

Self Healing and Optimization



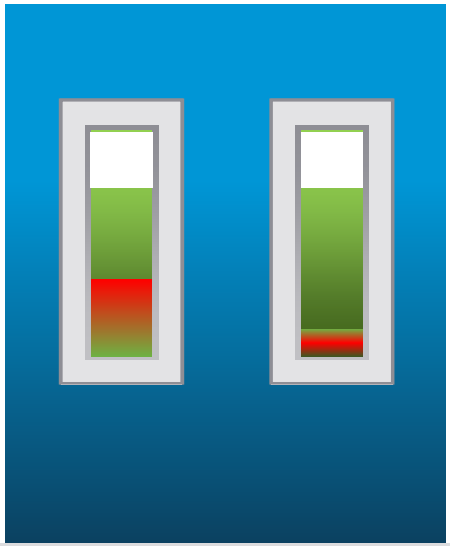


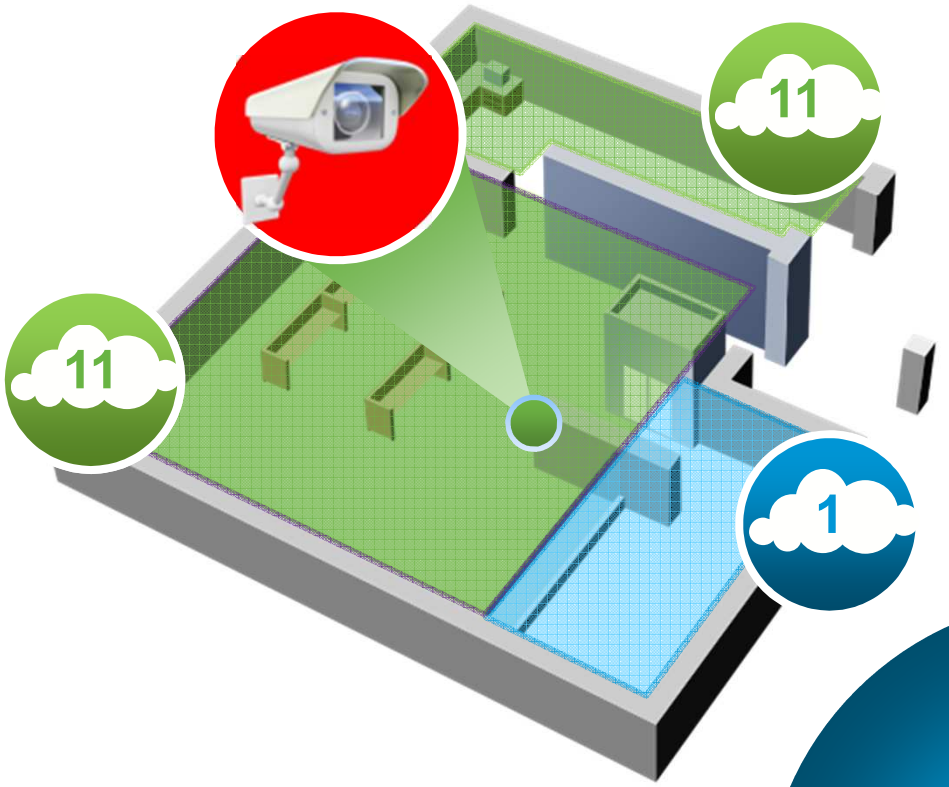


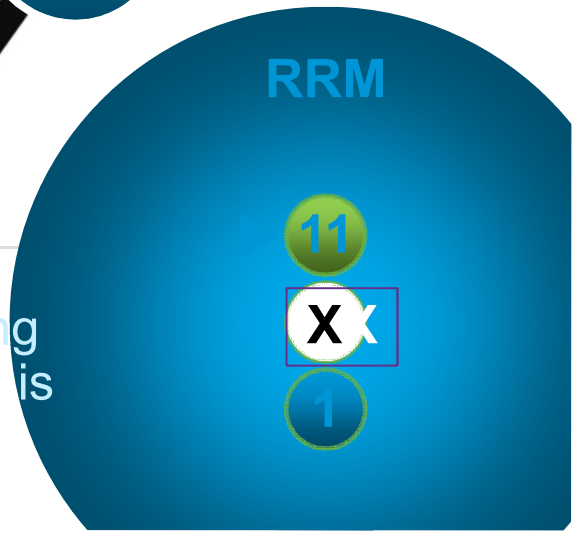
Wireless LAN Controller

channels to resolve conflict…

Self Healing and Optimization





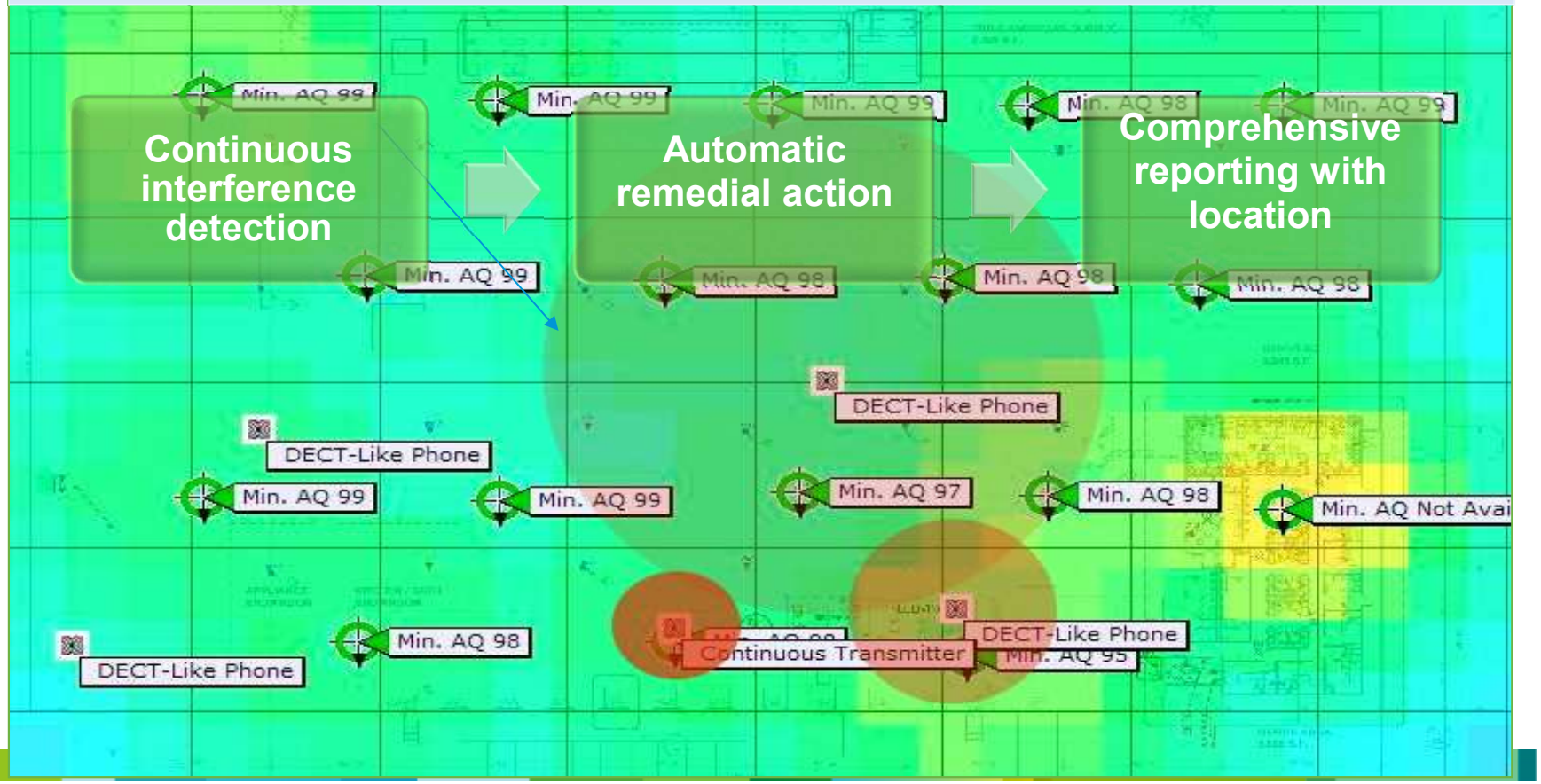


Wireless LAN Controller

Conflict resolved. Information is being
Changing to RRM Conflicting channel is
relayed to RRM.
blocked from future use.

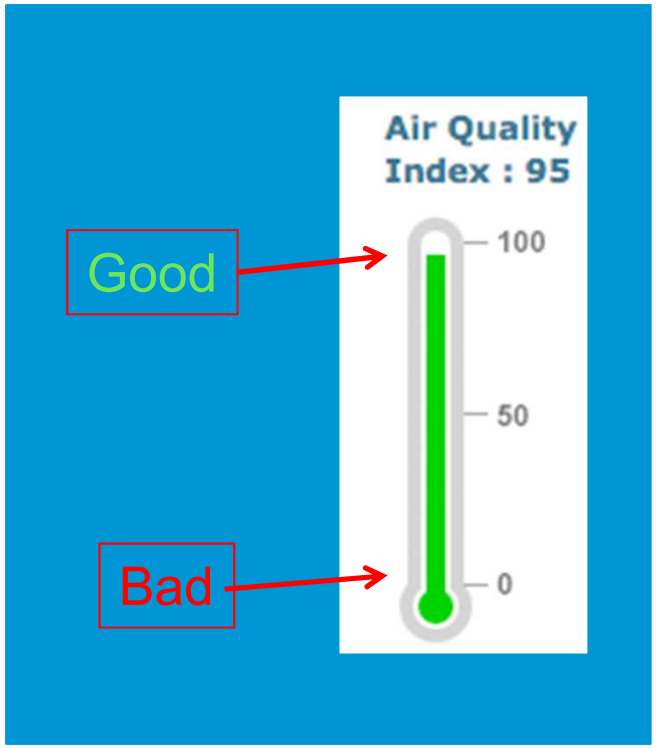
Visualize Interference

CleanAir technology provides the ability to visualize performance-impacting interference and automatically adjusts network settings and channels to avoid interference and optimize network performance.

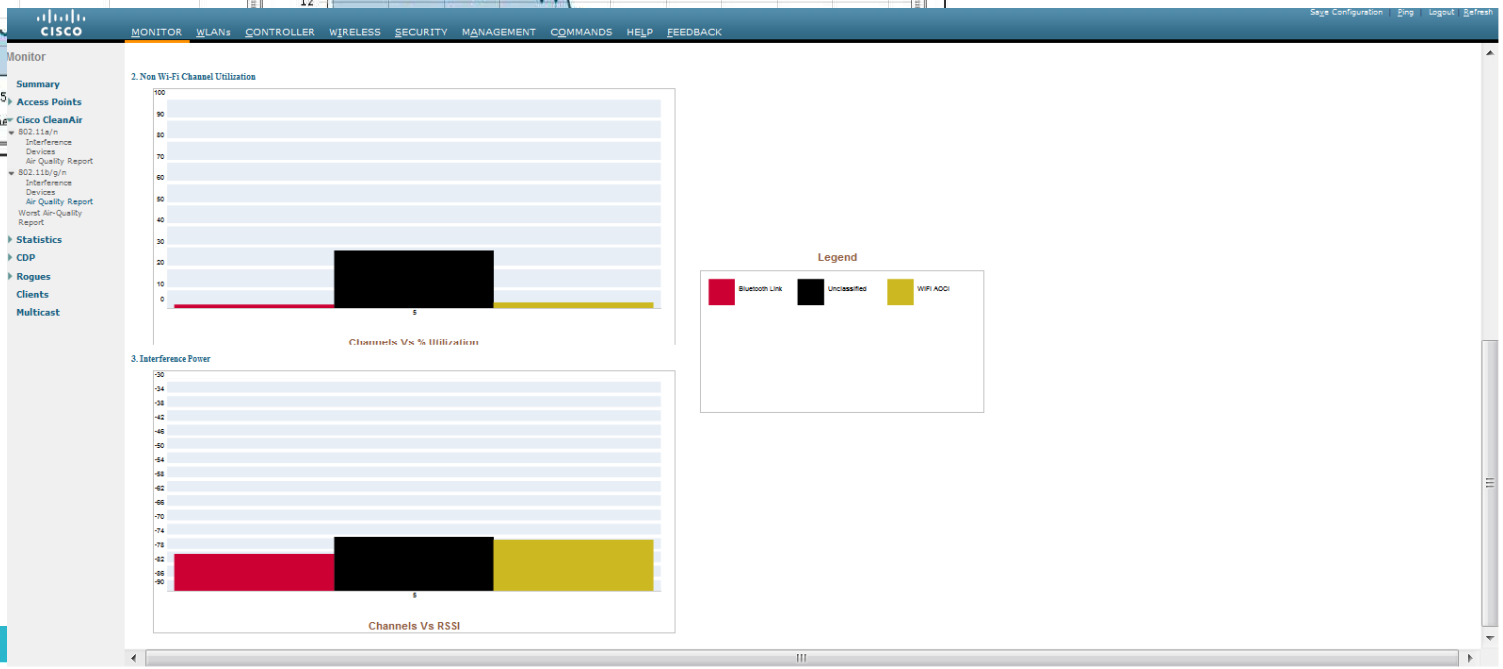


Air Quality Index - AQI

- Air Quality is a measurement of non-wifi and adjacent channel interference
- All Individual devices when Classified are assigned a Severity Value
- Air Quality is a measure of all Devices/Severities within a Radio, Floor, Building, or Campus



Graphical representation

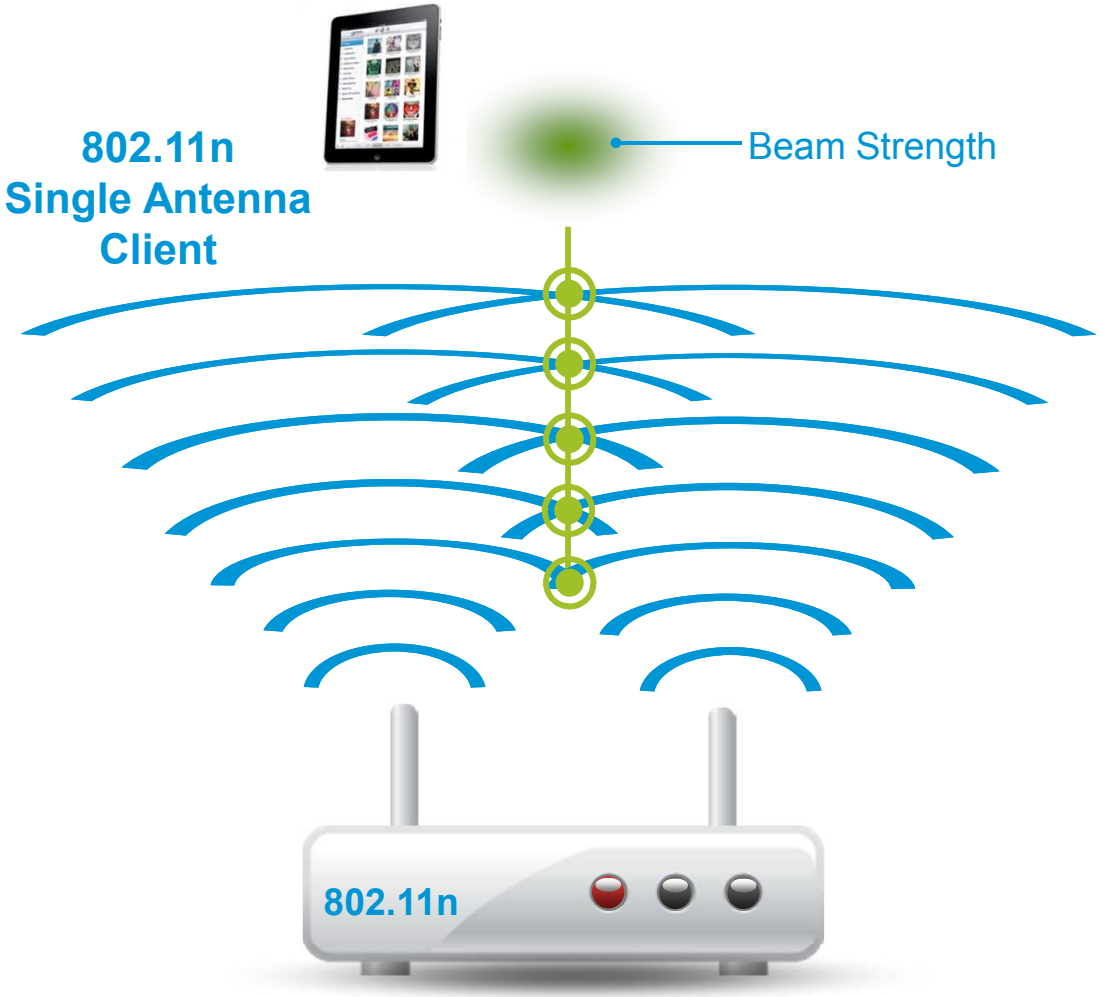


Topics

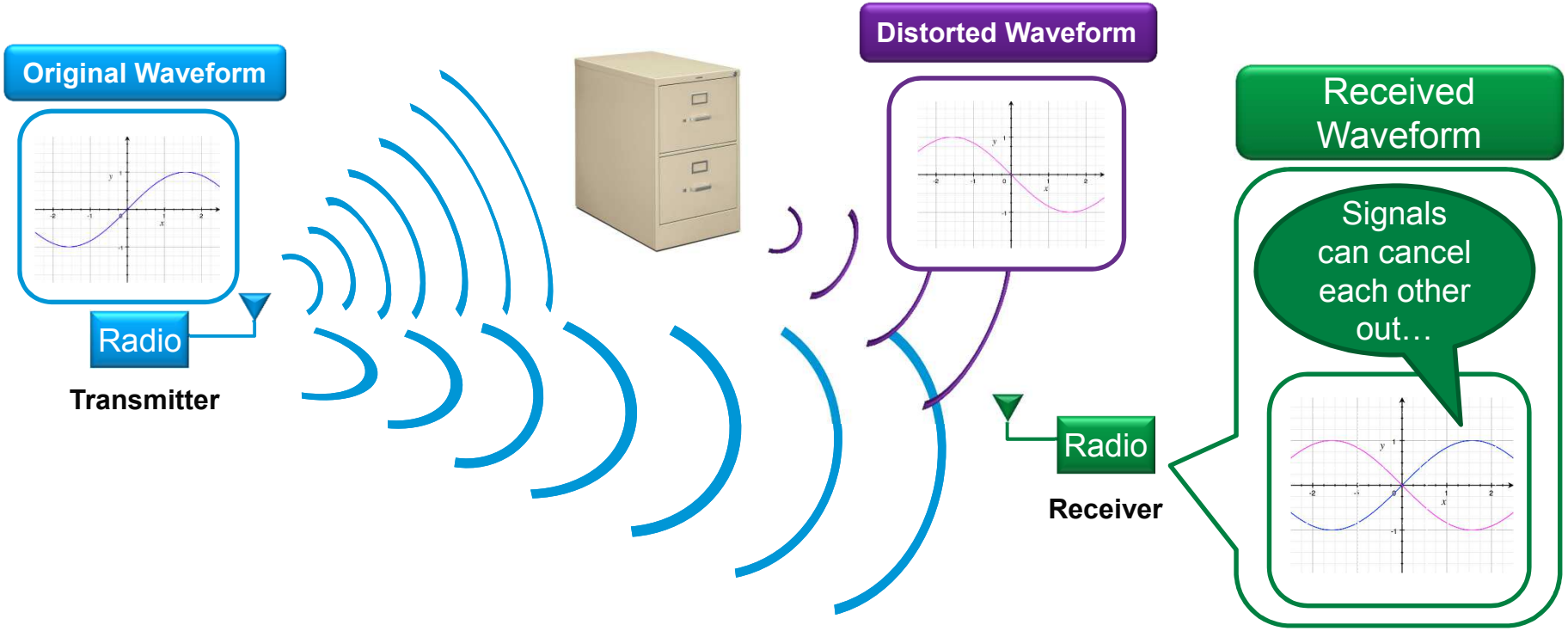
- Wifi standard evolution (phy layer):
  - 802.11a,b,g
  - 802.11n
  - 802.11ac and the future
- How to cope with interference: Cisco CleanAir and *Clientlink technology*
- Wireless security: Wireless IDS/IPS

The Connectivity Challenge

- Clients can be in hard to reach areas with a low single strength.
- Clients with a single antenna (like an iPad or Android) offer even more of a challenge since they lack diversity.
- 802.11n offers beam forming, but requires client support.



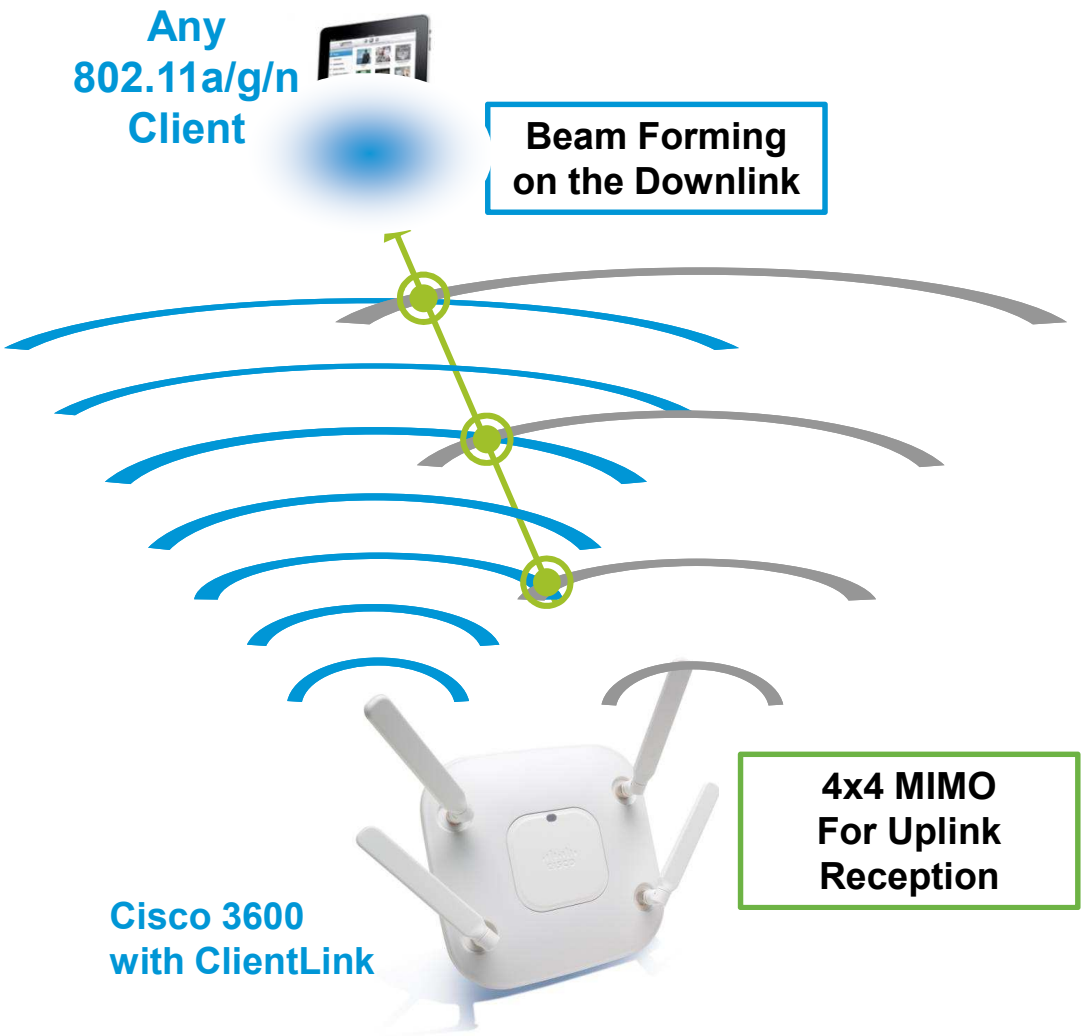
Multipath Can Lead to Distorted Waveforms and Reduced Data Rates



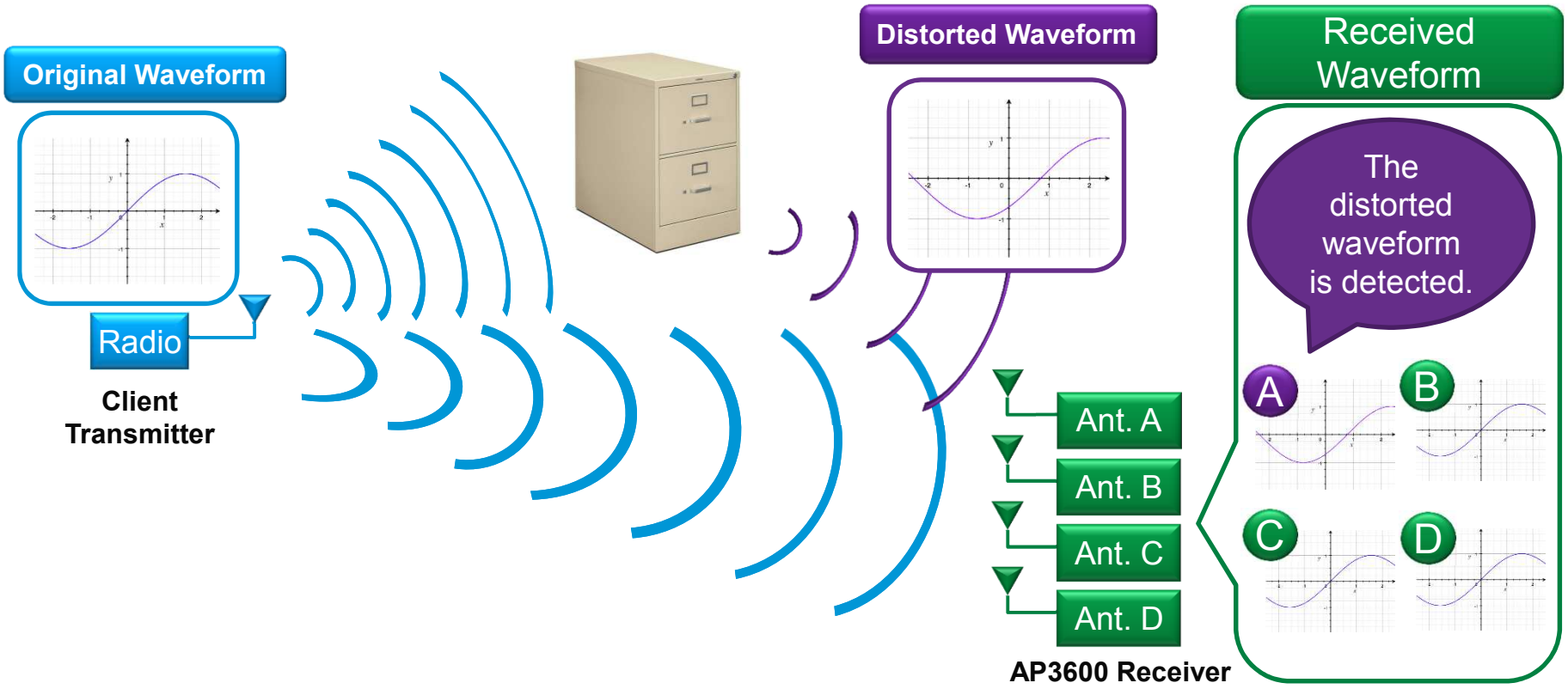
- Multipath from signal reflections can interfere with the original waveform's transmission causing it to be degraded.
- If the waveform is too degraded, the client cannot decode it and the transmitter must reduce the modulation complexity.

How Does Cisco Improve Connectivity?

- Cisco ClientLink uses four transmit antennas to increase the fidelity of the signal in the location of the client.
- Cisco ClientLink 2.0 can beam form to all 802.11a/g and 802.11n clients, whether the client is using 1, 2 or 3SSs, and requires no special client software.
- Four receivers enhances the upstream signal and updates the beam forming matrix.

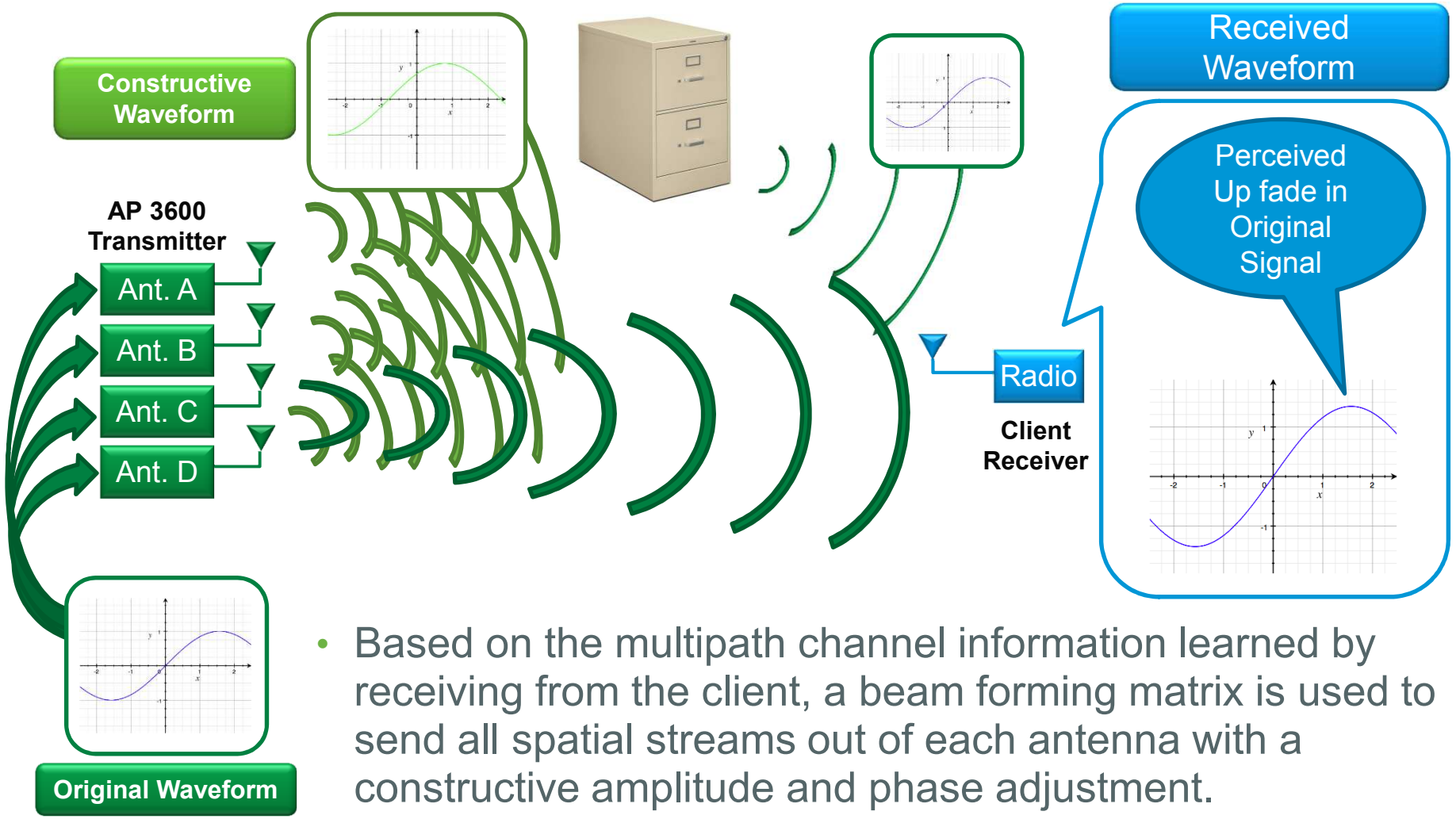


How AP Can Use Four Antennas To Hear Better



- More antennas means more view points into the RF environment.
- With more view points, the fidelity of the signal can be increased and information about the channel can be discovered for beam forming.

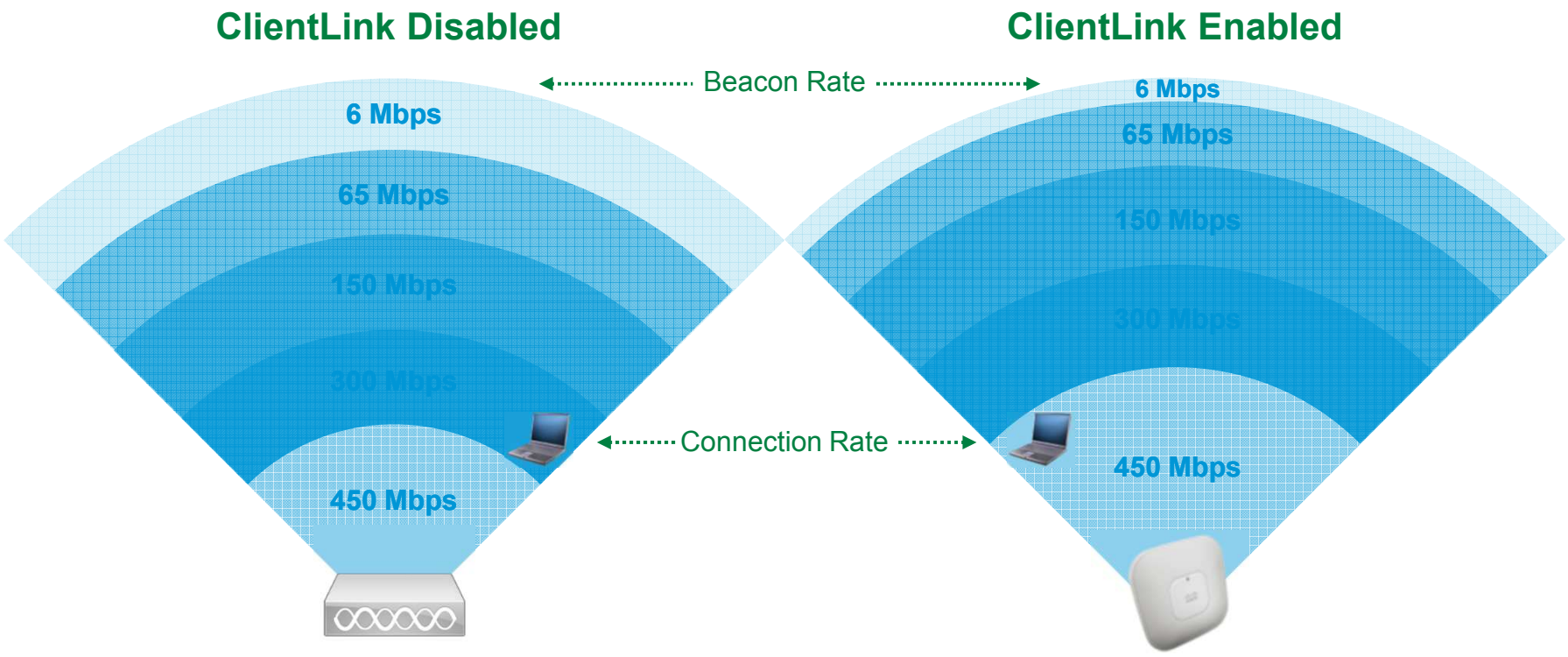
How The AP3600 Can Use Four Antennas To Beam Form



- Based on the multipath channel information learned by receiving from the client, a beam forming matrix is used to send all spatial streams out of each antenna with a constructive amplitude and phase adjustment.

Why is Cisco's ClientLink 2.0 so Unique?

Reduces Coverage Holes/Improves Both Upstream and Downstream



Cisco ClientLink 2.0—Improves Predictability and Performance

Topics

- Wifi standard evolution (phy layer):
  - 802.11a,b,g
  - 802.11n
  - 802.11ac and the future
- How to cope with interference: Cisco CleanAir and Clientlink technology
- Wireless security: *Wireless IDS/IPS*

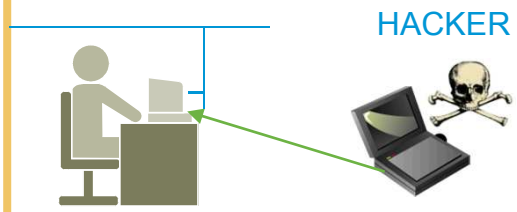
WLAN Security

Vulnerabilities and Threats

On-Wire Attacks

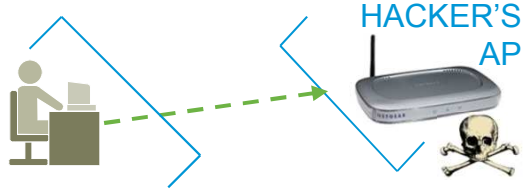
Over-the-Air Attacks

Ad-hoc Wireless Bridge



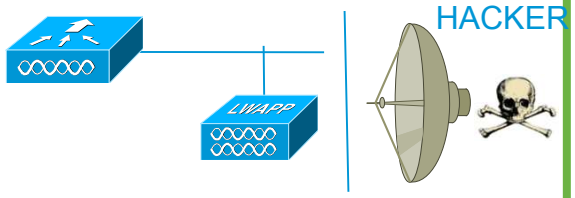
Client-to-client backdoor access

Evil Twin/Honeypot AP



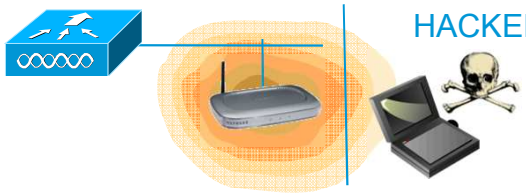
Connection to malicious AP

Reconnaissance



Seeking network vulnerabilities

Rogue Access Points

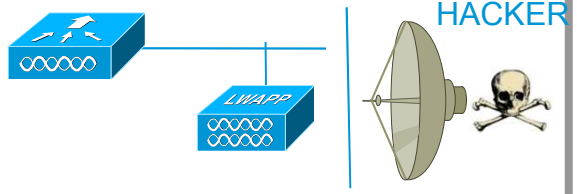


Backdoor network access

Denial of Service

Service disruption

Cracking Tools



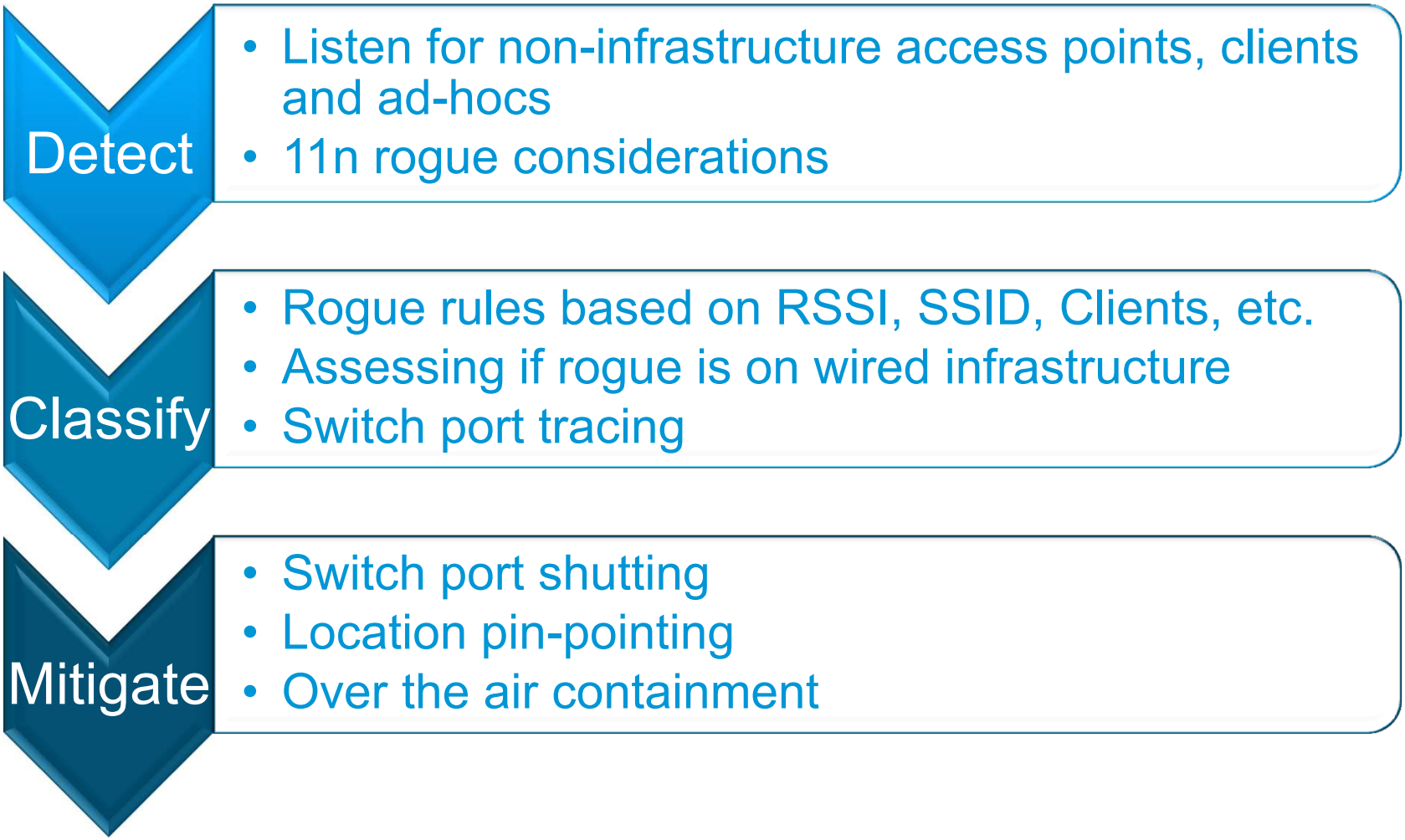
Sniffing and eavesdropping

Non-802.11 Attacks

Rogue Devices

- **What is a Rogue?**
  - Any device that's sharing your spectrum, but not managed by you
  - Majority of rogues are setup by insiders (low cost, convenience, ignorance)
- **When is a Rogue dangerous?**
  - When setup to use the same ESSID as your network (honeypot)
  - When it's detected to be on the wired network too
  - Ad-hoc rogues are arguably a big threat, too!
  - Setup by an outsider, most times, with malicious intent
- **What needs to be done?**
  - Detect
  - Classify (over-the-air, and on-the-wire)
  - Mitigate (Shutdown, Contain, etc)

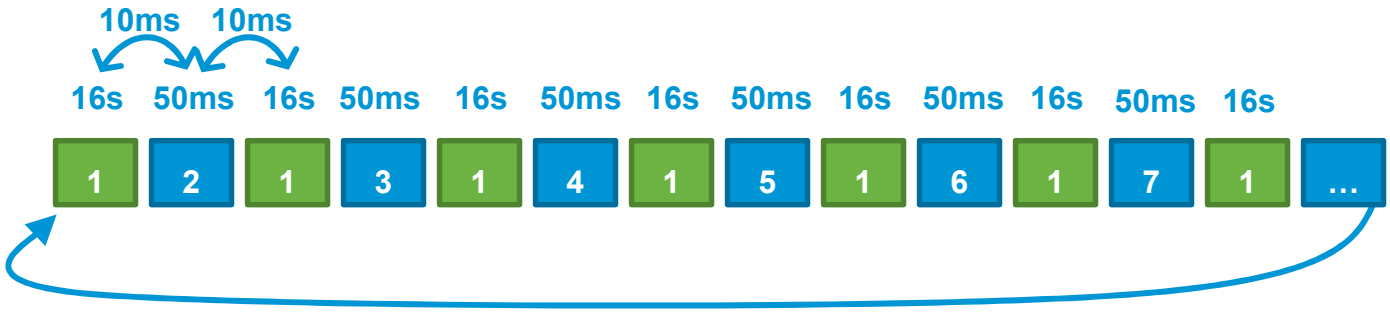
Phases of Rogue Management



RRM Channel Scanning
Local Mode AP

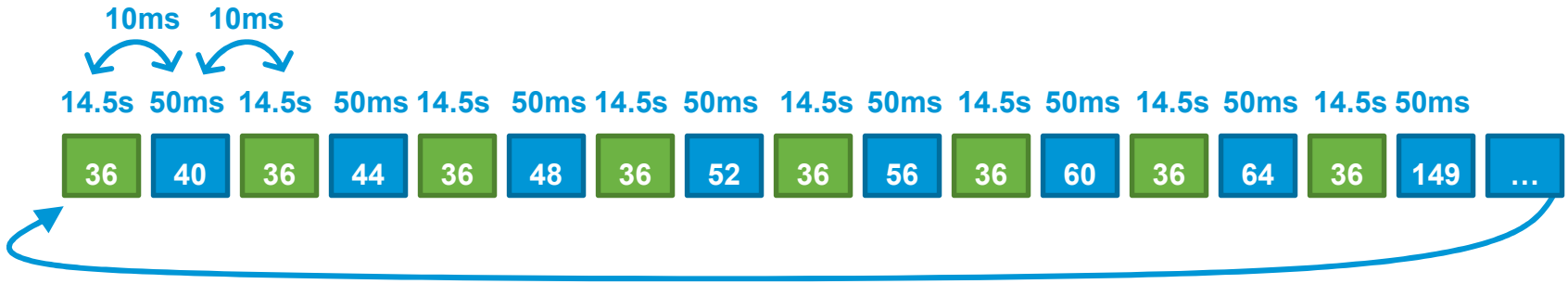
Detect

AP on channel 1 - 802.11 b/g/n – US County Channels



- Every 16s, a new channel is scanned for 50ms (180sec / 11 channels = ~16s)

AP on channel 36 - 802.11 a/n – US Country Channels (w/o UNII-2 Extended)



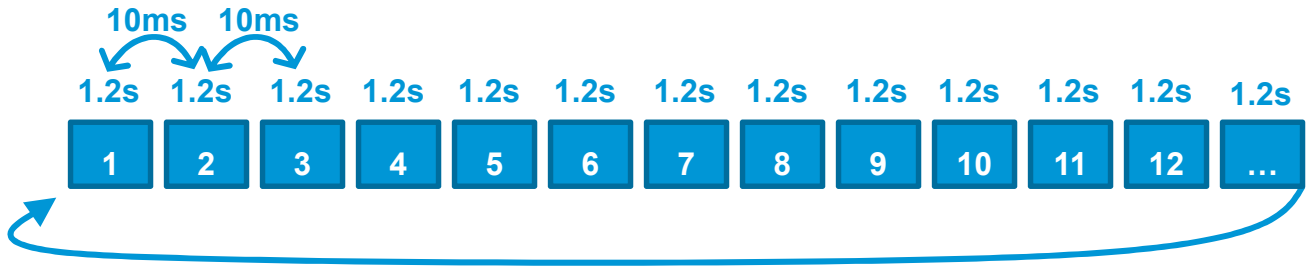
- Every 14.5s, a new channel is scanned for 50ms (180sec / 12 channels = ~14.5s)

RRM Channel Scanning

Monitor Mode AP

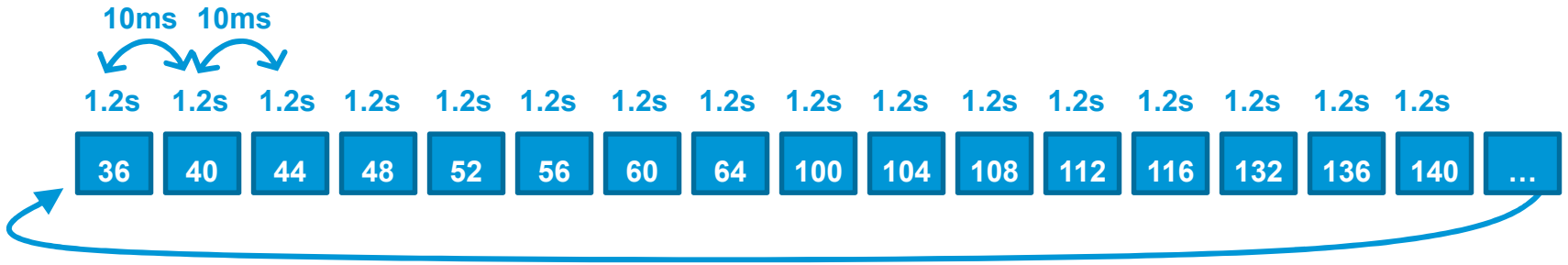
Detect

802.11b/g/n – All Channels



- Each channel is scanned a total of ~10.7s ((180s / 1.2s) / 14ch) within the 180s channel scan duration

802.11a/n – All Channels



- Each channel is scanned a total of ~6.8s ((180s / 1.2s) / 22ch) within the 180s channel scan duration

Rogue Information Available at PI and Controller

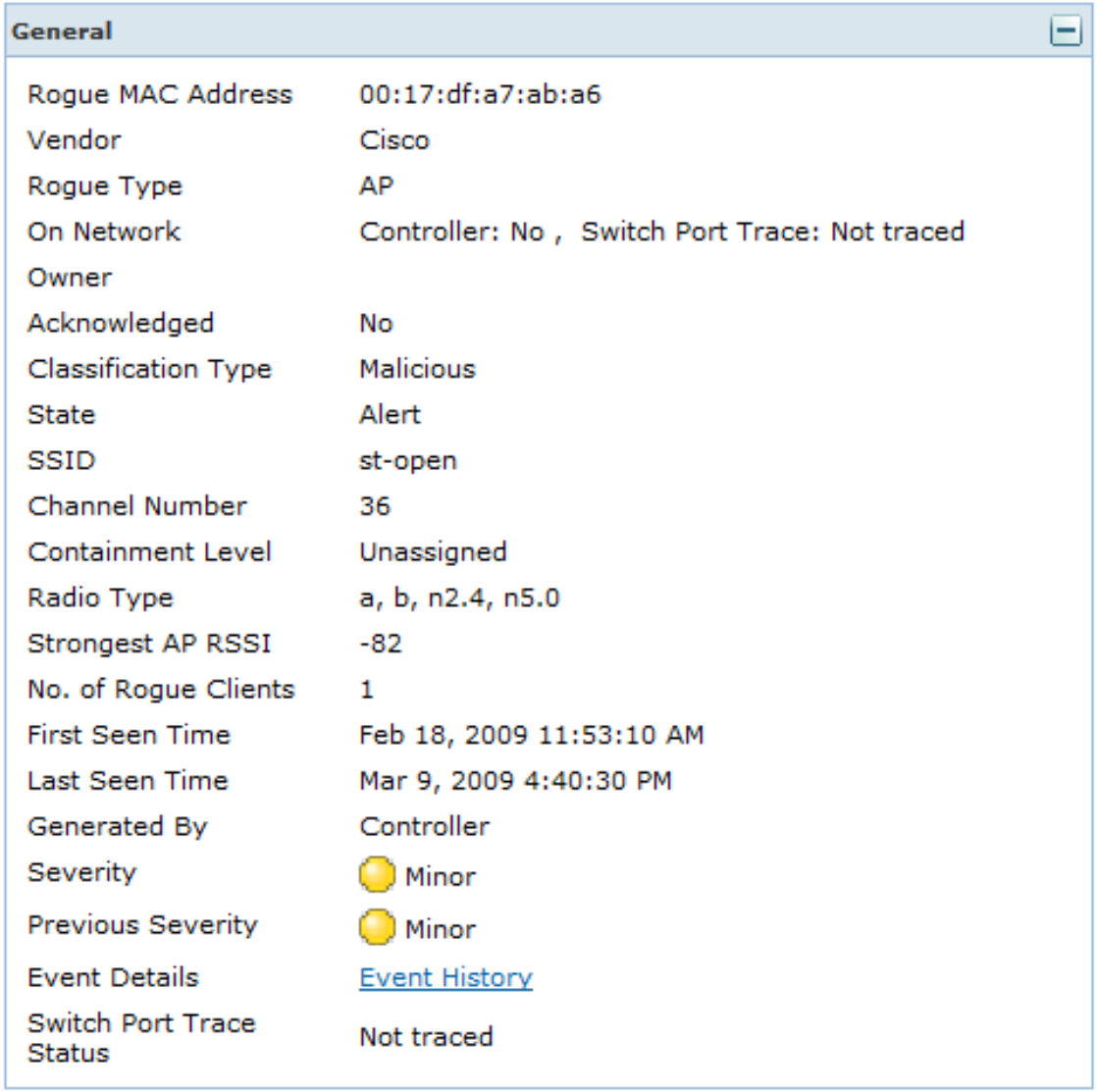
Detect

Network Name

Radio Type (11n)

# of Clients

Both Local Mode and Monitor Mode APs provide the same information regarding the rogue.



General

Rogue MAC Address	00:17:df:a7:ab:a6
Vendor	Cisco
Rogue Type	AP
On Network	Controller: No , Switch Port Trace: Not traced
Owner	
Acknowledged	No
Classification Type	Malicious
State	Alert
SSID	st-open
Channel Number	36
Containment Level	Unassigned
Radio Type	a, b, n2.4, n5.0
Strongest AP RSSI	-82
No. of Rogue Clients	1
First Seen Time	Feb 18, 2009 11:53:10 AM
Last Seen Time	Mar 9, 2009 4:40:30 PM
Generated By	Controller
Severity	Minor
Previous Severity	Minor
Event Details	Event History
Switch Port Trace Status	Not traced

Rogue APs and Clients

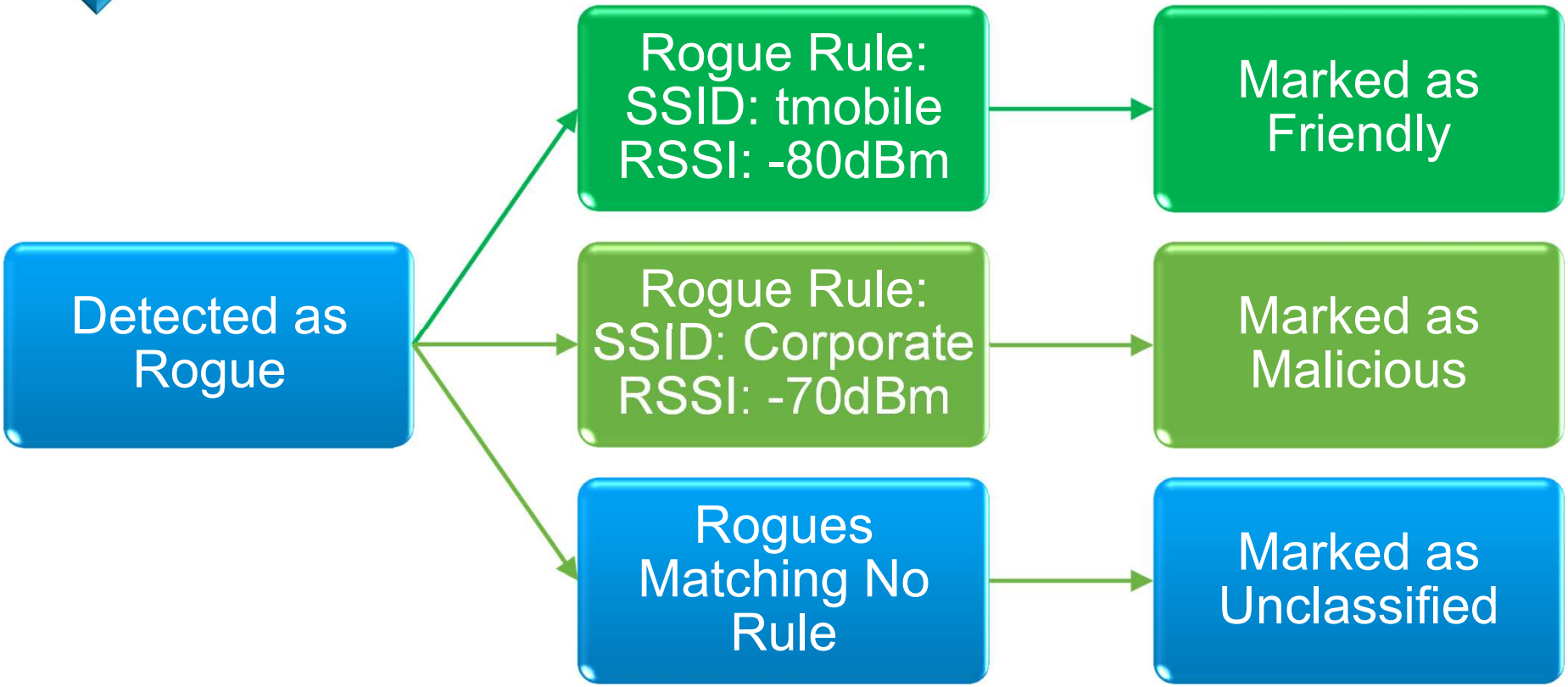
Rogue Classification Rules
Concept

- **Classification based on threat severity and mitigation action**
- **Rules tailored to customer risk model**

Lower Severity → Higher Severity

Off-Network	On-Network
Secured	Open
Foreign SSID	Our SSID
Weak RSSI	Strong RSSI
Distant location	On-site location
No clients	Attracts clients

Rogue Classification Rules
Examples

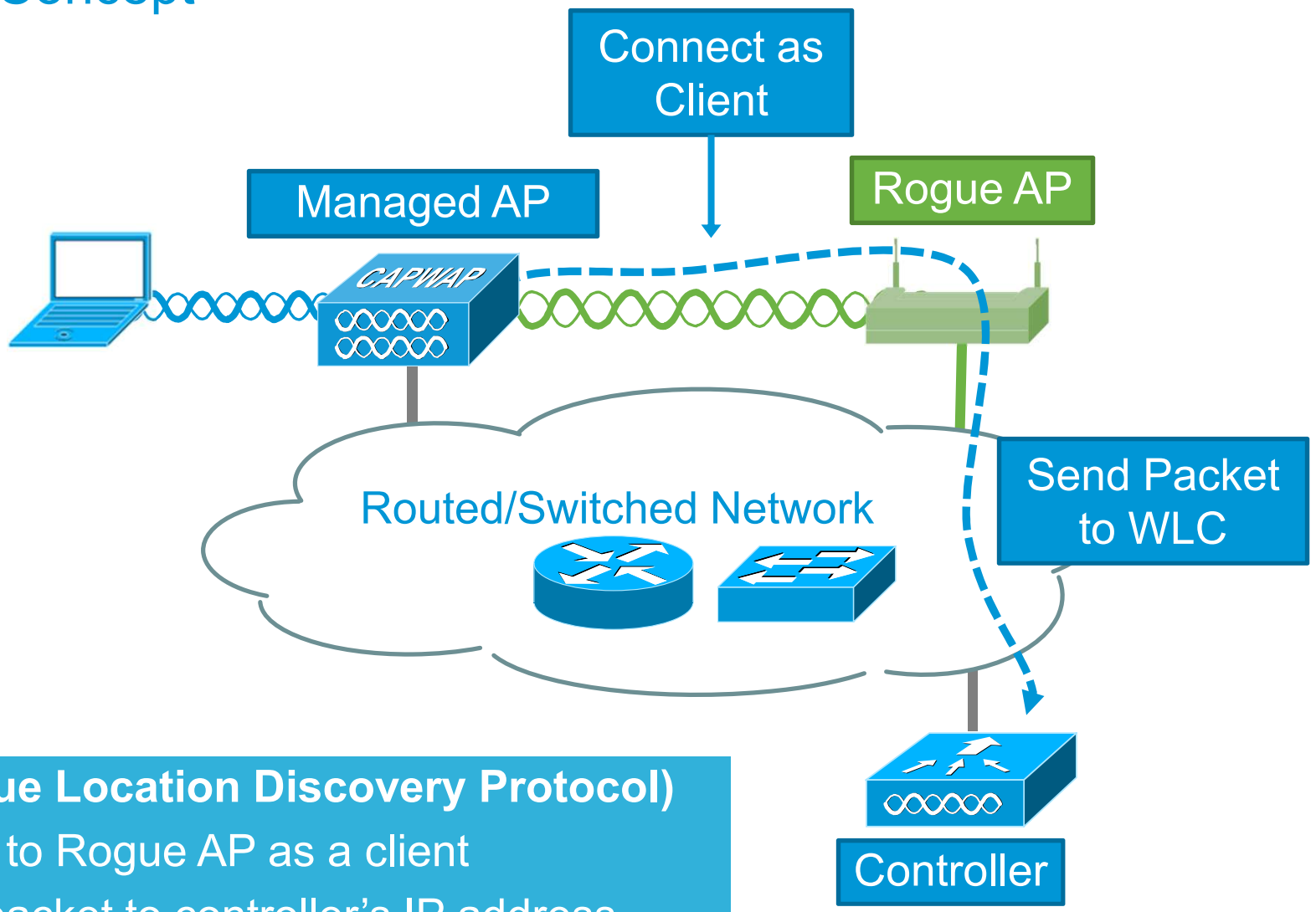


Rules are stored and executed on the Wireless LAN Controller

Classify

Rogue Location Discovery Protocol

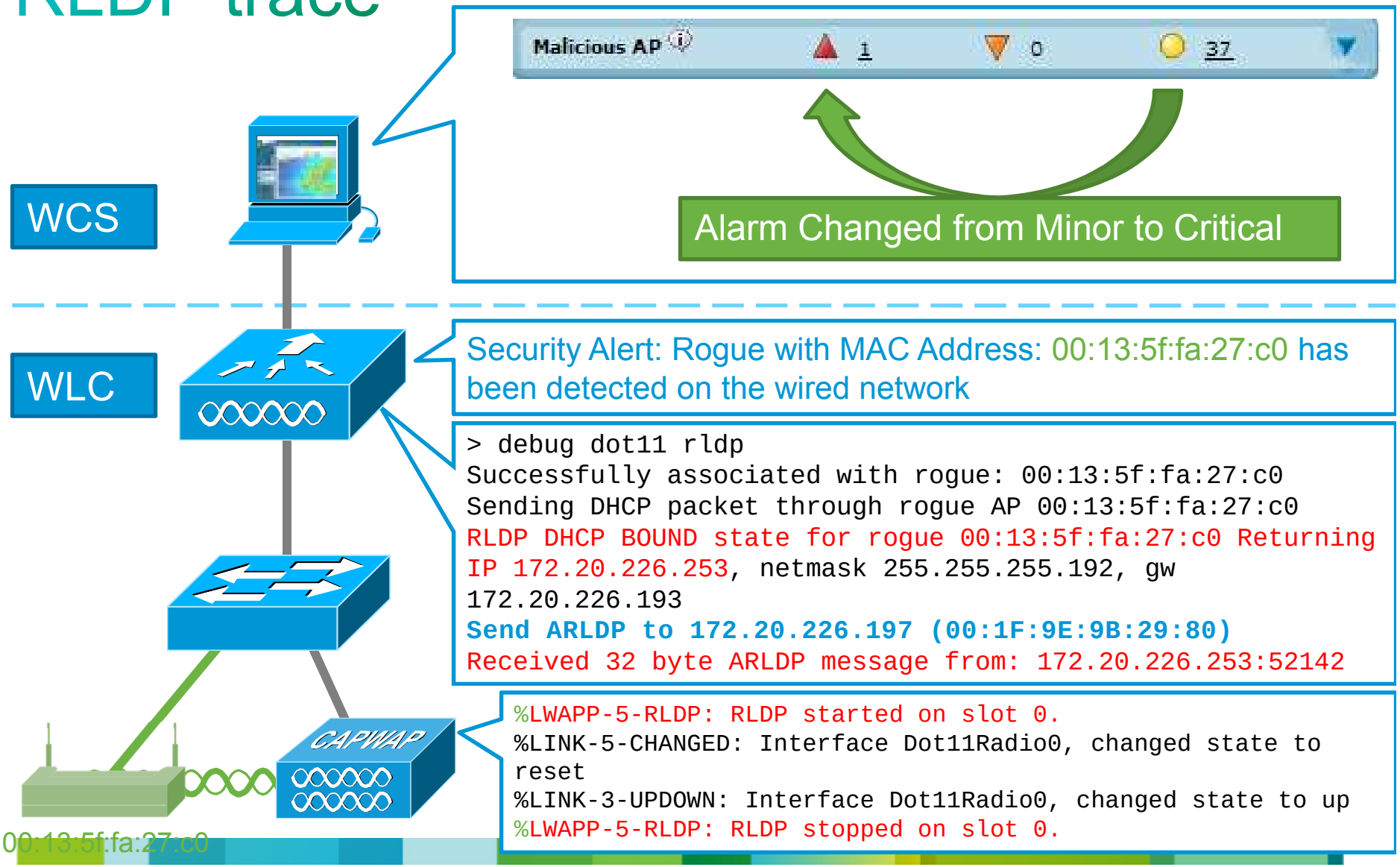
Concept



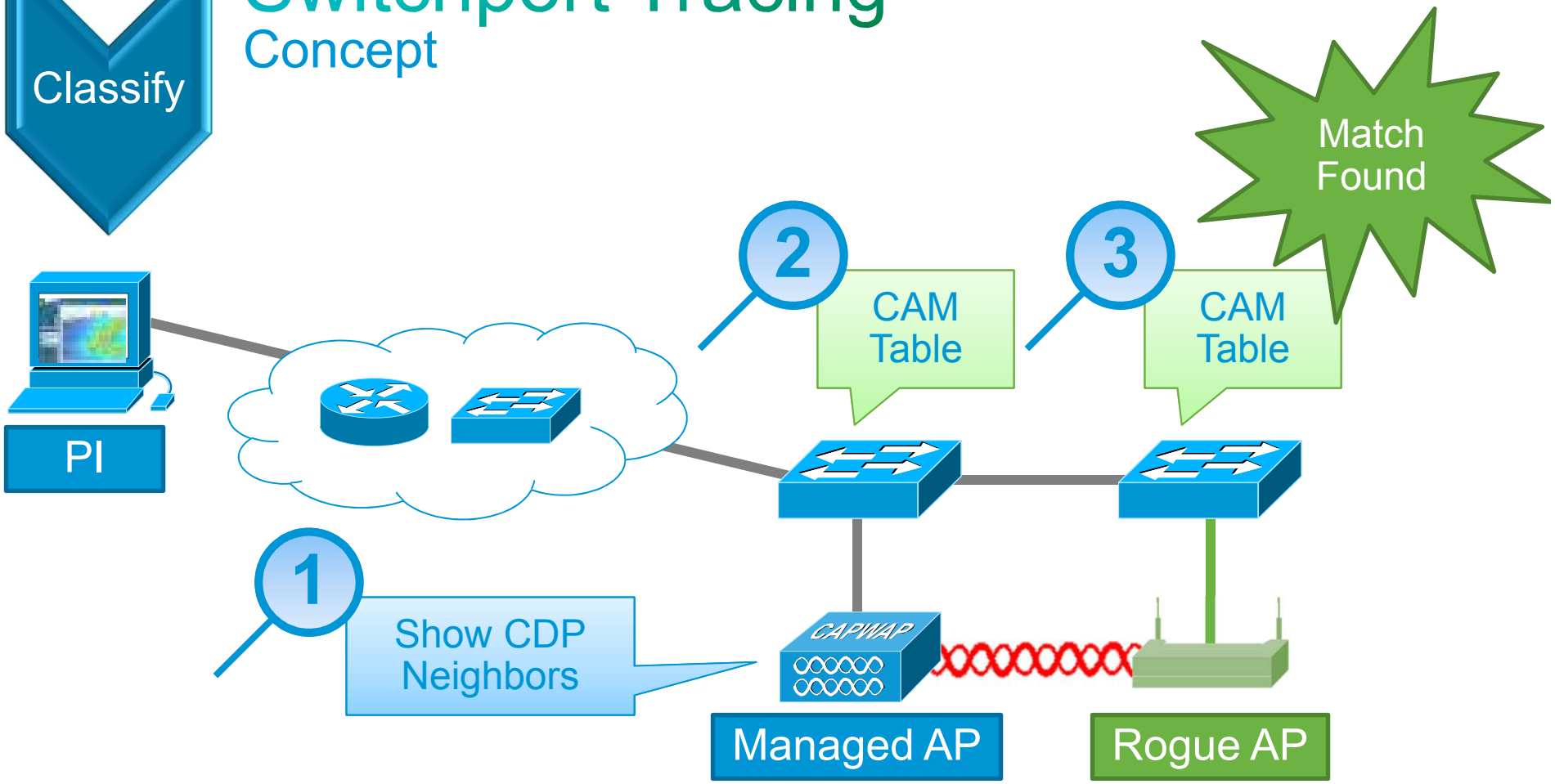
RLDP (Rogue Location Discovery Protocol)

- Connects to Rogue AP as a client
- Sends a packet to controller's IP address
- Only works with open rogue access points

RLDP trace



Switchport Tracing
Concept



PI Switchport Tracing

- Identifies CDP Neighbors of APs detecting the rogue
- Queries the switches CAM table for the rogue's MAC
- Works for rogues with security and NAT

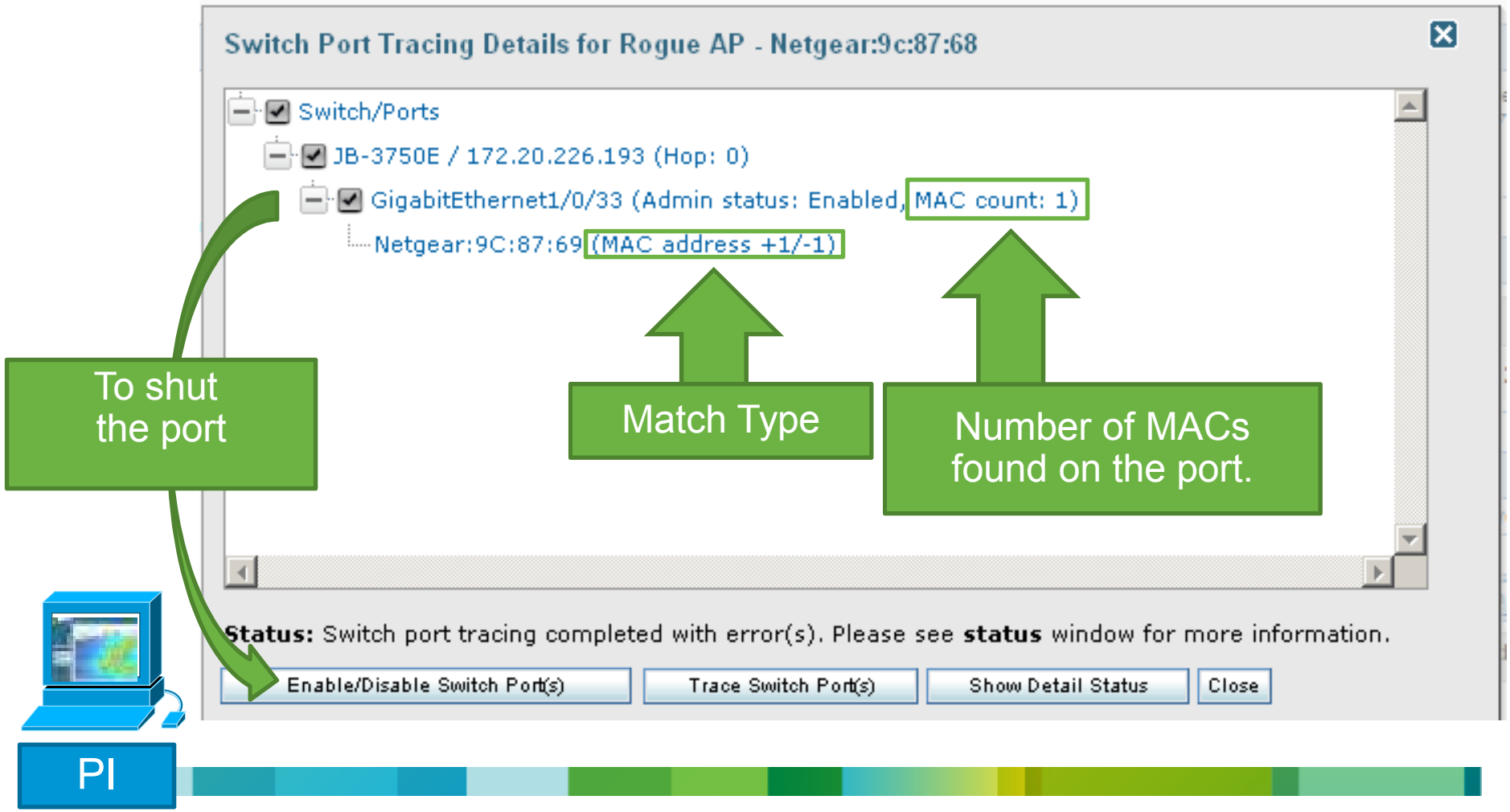
PI Switchport Tracing
Operation

Tracing is done on-demand per rogue AP.

PI

```
Switch port tracing started for rogue AP 00:09:5B:9C:87:68
Rogue AP 00:09:5B:9C:87:68 vendor is Netgear
Following MAC addresses will be searched:
00:09:5B:9C:87:68, 00:09:5B:9C:87:67, 00:09:5B:9C:87:69
Following rogue client MAC addresses will be searched:
00:21:5D:AC:D8:98
Following vendor OUIs will be searched:
00:0F:B5, 00:22:3F, 00:1F:33, 00:18:4D, 00:14:6C, 00:09:5B
Rogue AP 00:09:5B:9C:87:68 was reported by following APs: 1140-1
Reporting AP 1140-1 is connected to switch 172.20.226.193
Following are the Ethernet switches found at hop 0 172.20.226.193
Started tracing the Ethernet switch 172.20.226.193 found at hop 0
Tracing is in progress for Ethernet switch 172.20.226.193
MAC entry 00:09:5B:9C:87:69 (MAC address +1/-1) found
Ethernet Switch: 172.20.226.193, VLAN: 113, Port: GigabitEthernet1/0/33
Finished tracing all the Ethernet switches at hop 0
```

PI Switchport Tracing
Operation (Cont)



PI Switchport Tracing
Options

Classify

Configure Search Methods

Exclude Vendors from OUI Search

PI

Switch Port Trace

Administration > Settings > **Switch Port Trace**

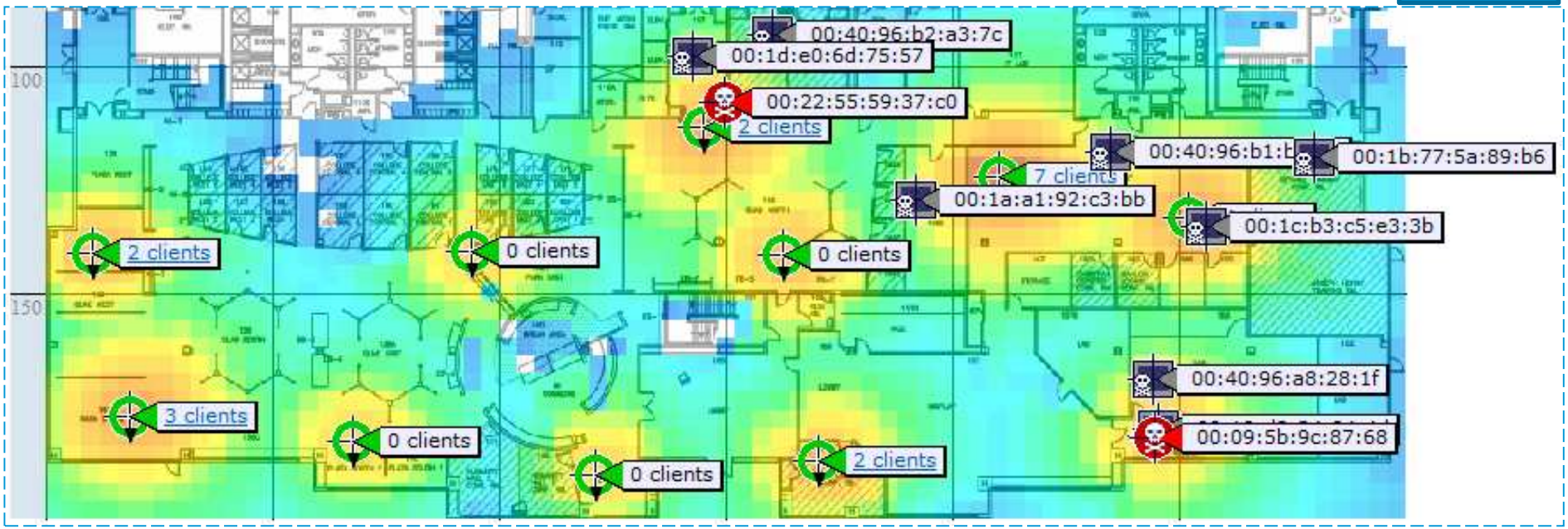
Basic Settings

Enable MAC address +1/-1 search	☑
Enable rogue client MAC address search	☑
Enable Vendor (OUI) search	☑
Exclude switch trunk ports	☑
Exclude device list	(comma separated IP address list)
Max hop count	2 (valid range: 1 - 10)
Exclude vendor list	cisco (comma separated case insensitive vendor name list)

Mitigate

Rogue Location

In real-time with PI and MSE Context-Aware

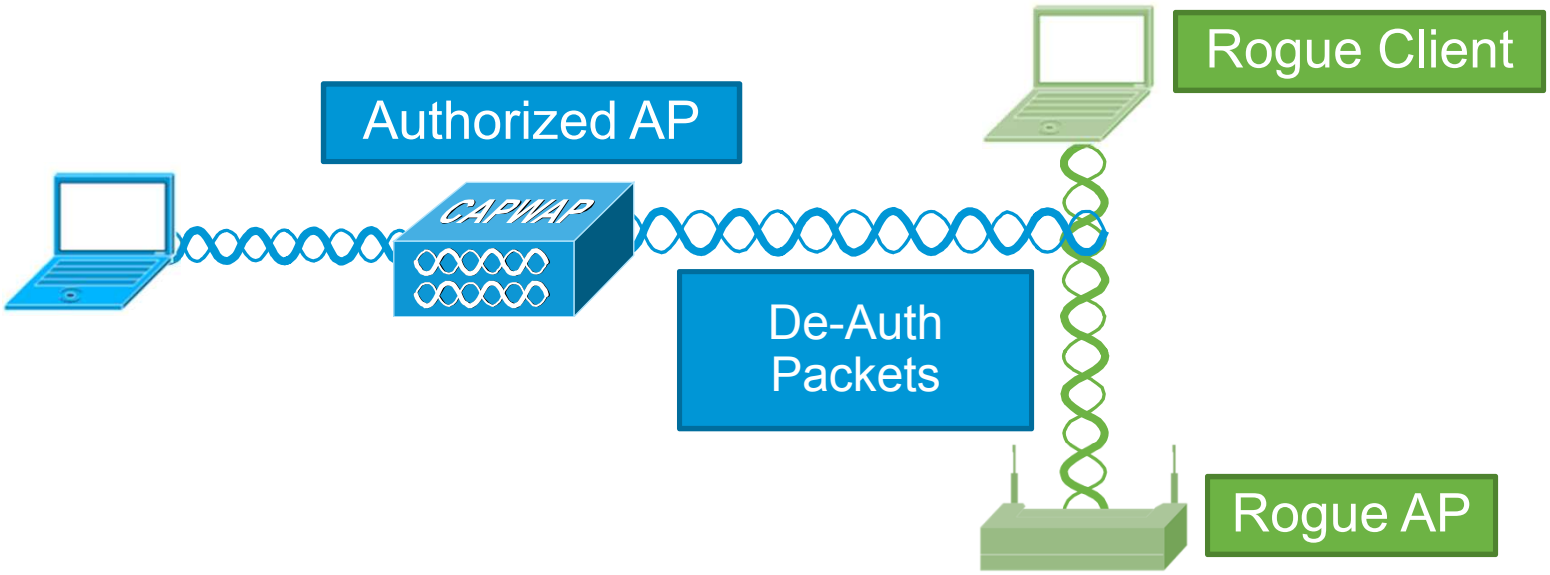


- Track of multiple rogues in real-time (up to MSE limits)
- Can track and store rogue location historically
- Provides location of rogue clients
- Provides location of rouge ad-hoc networks

Rogue APs
Rogue Adhocs
Rogue Clients

Mitigate

Rogue Containment
Concept



Rogue AP Containment

- Sends De-Authentication Packets to Client and AP
- Can use local, monitor mode or Flex APs
- Impacts client performance on managed AP

Köszönöm a figyelmet !