



Introduction

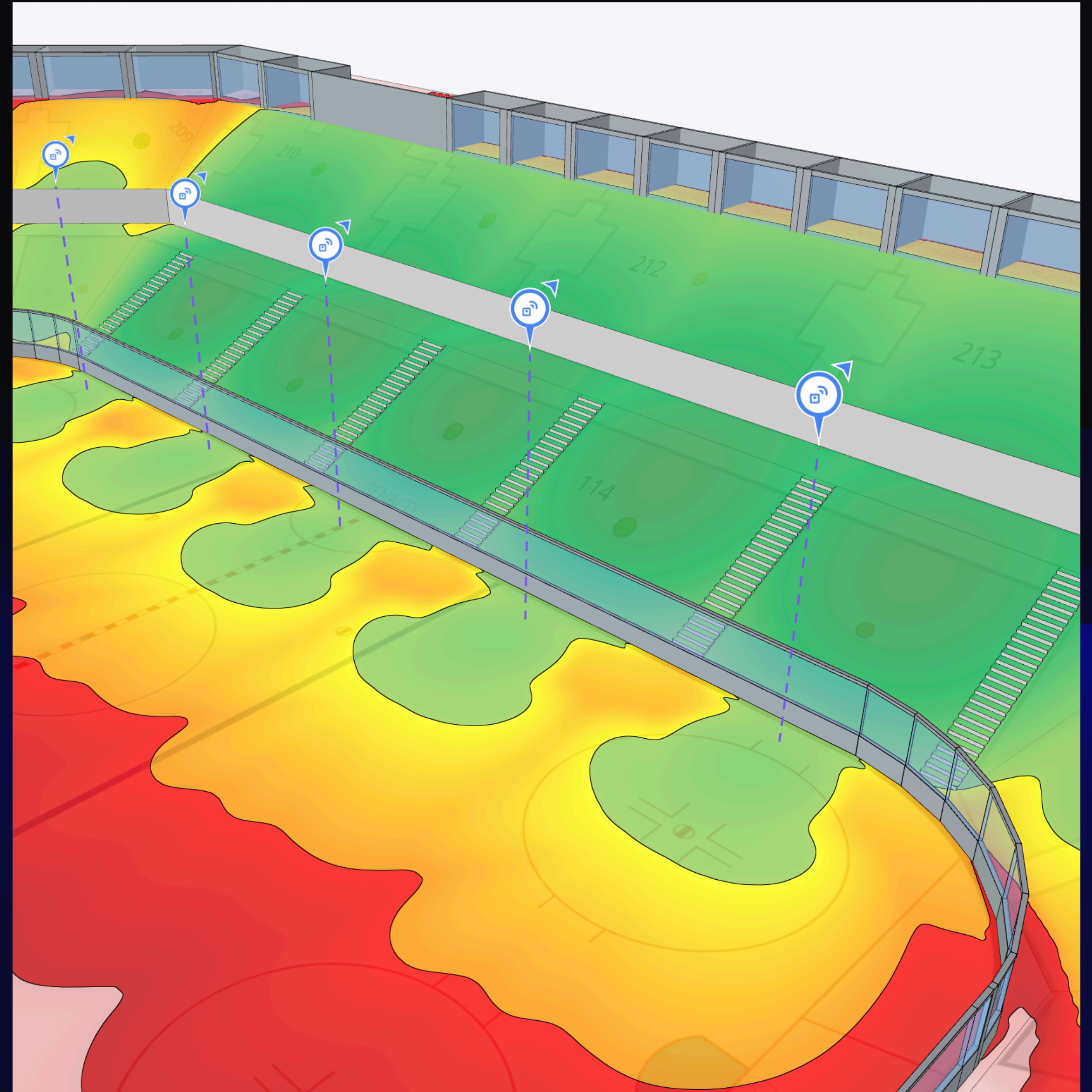
Wi-Fi 101, Part 2

Joel Crane, CWNE #233
Hamina Wireless

Agenda

Wi-Fi 101, Part 2

- BSSIDs, SSIDs, and ESSIDs
- Signal Strength
- Signal to Noise Ratio
- Data Rates
- 802.11 Frame Types
- Airtime Arbitration Process
- Roaming
- Security



BSSID

Basic Service Set Identifier

- MAC address of an AP radio
- Example: D4:20:B0:A2:EF:B7

D4:20:B0:A2:EF:B7
D4:20:B0:A2:EF:B8



SSID

Service Set Identifier

- Friendly network name
- Example: Aperture Science

Aperture Science



ESSID

Extended Service Set Identifier

- Multiple APs with the same SSID

Aperture Science



Aperture Science



Aperture Science



Signal Strength

Rule of 3's and 10's

- +3 dB: Double the signal strength
- -3 dB: Half the signal strength
- +10 dB: 10x the signal strength
- -10 dB: 10x less signal strength

Why dBm?

-60 dBm	.000001 mW
---------	------------

-70 dBm	.0000001 mW
---------	-------------

-80 dBm	.00000001 mW
---------	--------------

-90 dBm	.000000001 mW
---------	---------------

What is “Good” Signal Strength?

-30 dBm	As good as it gets
---------	--------------------

-65 dBm	Voice applications, mobile devices
---------	------------------------------------

-67 dBm	Streaming video
---------	-----------------

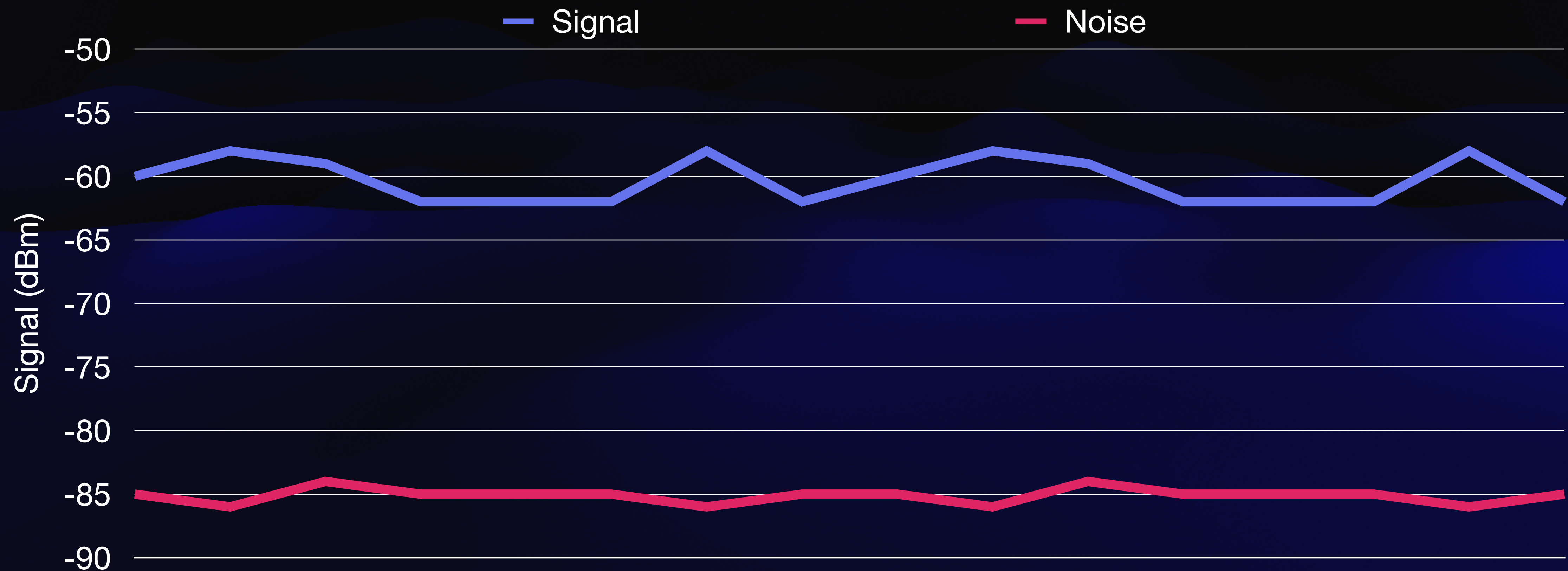
-75 dBm	Messaging, email
---------	------------------

-80 dBm	Generally unreliable
---------	----------------------

-90 dBm	Approaching or drowning in the noise floor
---------	--

SNR

Signal to Noise Ratio: How much signal is there above the background noise?



Data Rates

- 802.11b: 1, 2, 5.5, 11 Mbps
- 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
- 802.11n/ac: MCS Index
 - <https://mcsindex.com/>
- Our goal as engineers: down and to the right

MCS Index Table, Modulation and Coding Scheme Index 11n, 11ac, and 11ax																							
MCS																							
Full MCS Table (HT/VHT/HE)						MCS Table 3SS (HT/VHT/HE)						MCS Table HE		MCS Table HE (OFDM)		MCS Table HE (OFDMA)		The Math Behind it		Credit			
MCS Index		Spatial Stream	Modulation	Coding	OFDM (Prior 11ax)								OFDM (802.11ax)										
					20MHz		40MHz		80MHz		160MHz		20MHz			40MHz			80MHz				
HT	VHT	HE				0.8µs GI	0.4µs GI	0.8µs GI	0.4µs GI	0.8µs GI	0.4µs GI	0.8µs GI	0.4µs GI	0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI	
0	0	0	1	BPSK	1/2	6.5	7.2	13.5	15	29.3	32.5	58.5	65	8.6	8.1	7.3	17.2	16.3	14.6	36	34	30.6	
1	1	1	1	QPSK	1/2	13	14.4	27	30	58.5	65	117	130	17.2	16.3	14.6	34.4	32.5	29.3	72.1	68.1	61.3	
2	2	2	1	QPSK	3/4	19.5	21.7	40.5	45	87.8	97.5	175.5	195	25.8	24.4	21.9	51.6	48.8	43.9	108.1	102.1	91.9	
3	3	3	1	16-QAM	1/2	26	28.9	54	60	117	130	234	260	34.4	32.5	29.3	68.8	65	58.5	144.1	136.1	122.5	
4	4	4	1	16-QAM	3/4	39	43.3	81	90	175.5	195	351	390	51.6	48.8	43.9	103.2	97.5	87.8	216.2	204.2	183.8	
5	5	5	1	64-QAM	2/3	52	57.8	108	120	234	260	468	520	68.8	65	58.5	137.6	130	117	288.2	272.2	245	
6	6	6	1	64-QAM	3/4	58.5	65	121.5	135	263.3	292.5	526.5	585	77.4	73.1	65.8	154.9	146.3	131.6	324.3	306.3	275.6	
7	7	7	1	64-QAM	5/6	65	72.2	135	150	292.5	325	585	650	86	81.3	73.1	172.1	162.5	146.3	360.3	340.3	306.3	
	8	8	1	256-QAM	3/4	78	86.7	162	180	351	390	702	780	103.2	97.5	87.8	206.5	195	175.5	432.4	408.3	367.5	
	9	9	1	256-QAM	5/6	N/A	N/A	180	200	390	433.3	780	866.7	114.7	108.3	97.5	229.4	216.7	195	480.4	453.7	408.3	
	10	10	1	1024-QAM	3/4										129	121.9	109.7	258.1	243.8	219.4	540.4	510.4	459.4
			11	1024-QAM	5/6										143.4	135.4	121.9	286.8	270.8	243.8	600.5	567.1	510.4
8	0	0	2	BPSK	1/2	13	14.4	27	30	58.5	65	117	130	17.2	16.3	14.6	34.4	32.5	29.3	72.1	68.1	61.3	
9	1	1	2	QPSK	1/2	26	28.9	54	60	117	130	234	260	34.4	32.5	29.3	68.8	65	58.5	144.1	136.1	122.5	
10	2	2	2	QPSK	3/4	39	43.3	81	90	175.5	195	351	390	51.6	48.8	43.9	103.2	97.5	87.8	216.2	204.2	183.8	
11	3	3	2	16-QAM	1/2	52	57.8	108	120	234	260	468	520	68.8	65	58.5	137.6	130	117	288.2	272.2	245	
12	4	4	2	16-QAM	3/4	78	86.7	162	180	351	390	702	780	103.2	97.5	87.8	206.5	195	175.5	432.4	408.3	367.5	
13	5	5	2	64-QAM	2/3	104	115.6	216	240	468	520	936	1040	137.6	130	117	275.3	260	234	576.5	544.4	490	
14	6	6	2	64-QAM	3/4	117	130	243	270	526.5	585	1053	1170	154.9	146.3	131.6	309.7	292.5	263.3	648.5	612.5	551.3	
15	7	7	2	64-QAM	5/6	130	144.4	270	300	585	650	1170	1300	172.1	162.5	146.3	344.1	325	292.5	720.6	680.6	612.5	
	8	8	2	256-QAM	3/4	156	173.3	324	360	702	780	1404	1560	206.5	195	175.5	412.9	390	351	864.7	816.7	735	
	9	9	2	256-QAM	5/6	N/A	N/A	360	400	780	866.7	1560	1733.3	229.4	216.7	195	458.8	433.3	390	960.8	907.4	816.7	
	10	10	2	1024-QAM	3/4										258.1	243.8	219.4	516.2	487.5	438.8	1080.9	1020.8	918.8
			11	1024-QAM	5/6										286.8	270.8	243.8	573.5	541.7	487.5	1201	1134.3	1020.8
16	0	0	3	BPSK	1/2	19.5	21.7	40.5	45	87.8	97.5	175.5	195	25.8	24.4	21.9	51.6	48.8	43.9	108.1	102.1	91.9	
17	1	1	3	QPSK	1/2	39	43.3	81	90	175.5	195	351	390	51.6	48.8	43.9	103.2	97.5	87.8	216.2	204.2	183.8	
18	2	2	3	QPSK	3/4	58.5	65	121.5	135	263.3	292.5	526.5	585	77.4	73.1	65.8	154.9	146.3	131.6	324.3	306.3	275.6	
19	3	3	3	16-QAM	1/2	78	86.7	162	180	351	390	702	780	103.2	97.5	87.8	206.5	195	175.5	432.4	408.3	367.5	
20	4	4	3	16-QAM	3/4	117	130	243	270	526.5	585	1053	1170	154.9	146.3	131.6	309.7	292.5	263.3	648.5	612.5	551.3	
21	5	5	3	64-QAM	2/3	156	173.3	324	360	702	780	1404	1560	206.5	195	175.5	412.9	390	351	864.7	816.7	735	
22	6	6	3	64-QAM	3/4	175.5	195	364.5	405	N/A	N/A	1579.5	1755	232.3	219.4	197.4	464.6	438.8	394.9	972.8	918.8	826.9	
23	7	7	3	64-QAM	5/6	195	216.7	405	450	877.5	975	1755	1950	258.1	243.8	219.4	516.2	487.5	438.8	1080.9	1020.8	918.8	
	8	8	3	256-QAM	3/4	234	260	486	540	1053	1170	2106	2340	309.7	292.5	263.3	619.4	585	526.5	1297.1	1225	1102.5	
	9	9	3	256-QAM	5/6	260	288.9	540	600	1170	1300	N/A	N/A	344.1	325	292.5	688.2	650	585	1441.2	1361.1	1225	
	10	10	3	1024-QAM	3/4										387.1	365.6	329.1	774.3	731.3	658.1	1621.3	1531.3	1378.1
			11	1024-QAM	5/6										430.1	406.3	365.6	860.3	812.5	731.3	1801.5	1701.4	1531.3
24	0	0	4	BPSK	1/2	26	28.9	54	60	117	130	234	260	34.4	32.5	29.3	68.8	65	58.5	144.1	136.1	122.5	
25	1	1	4	QPSK	1/2	52	57.8	108	120	234	260	468	520	68.8	65	58.5	137.6	130	117	288.2	272.2	245	
26	2	2	4	QPSK	3/4	78	86.7	162	180	351	390	702	780	103.2	97.5	87.8	206.5	195	175.5	432.4	408.3	367.5	

Demo: Simulating SNR and Data Rate in Hamina

802.11 Frame Types

Management

Manages stations joining and leaving wireless networks.

- Beacon
- Probe Request
- Probe Response
- Authentication Request
- Authentication Response
- Association Request
- Association Response

Control

Controls the RF medium and ensures delivery of other frames.

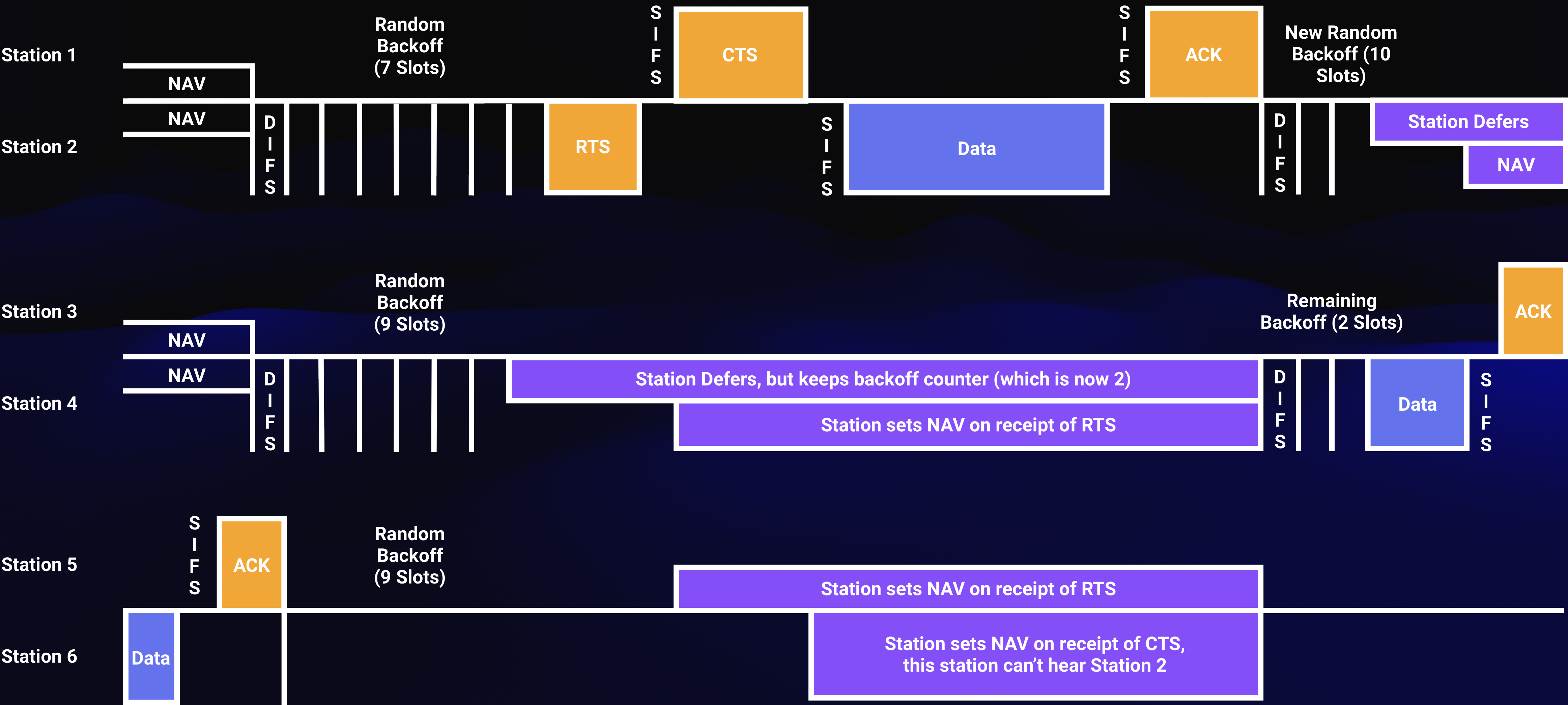
- Ack
- Block-Ack
- RTS/CTS

Data

Carries higher-level protocol data (actual network traffic).

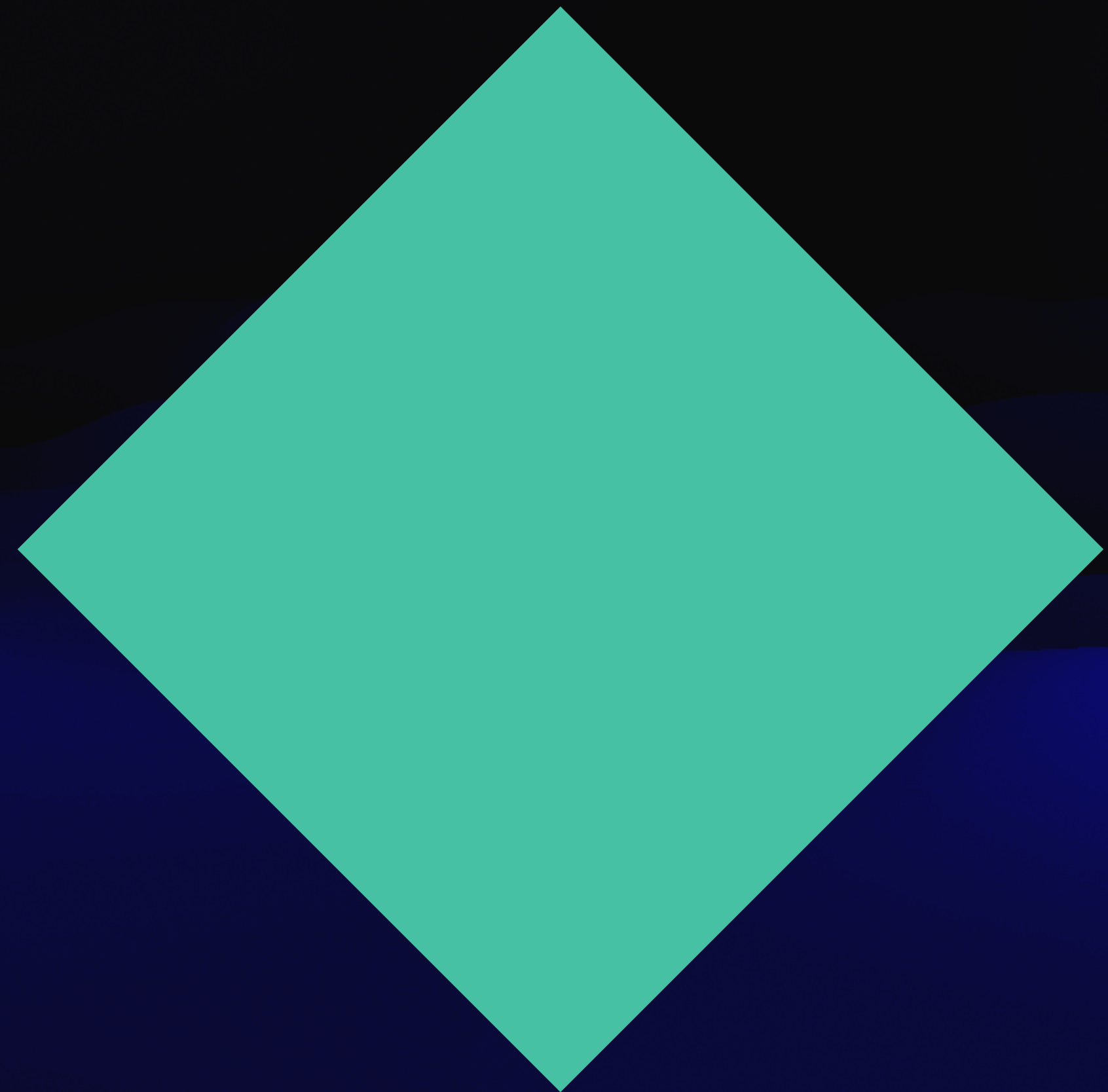
- Data
- QoS Data
- Null Data

Airtime Arbitration Process

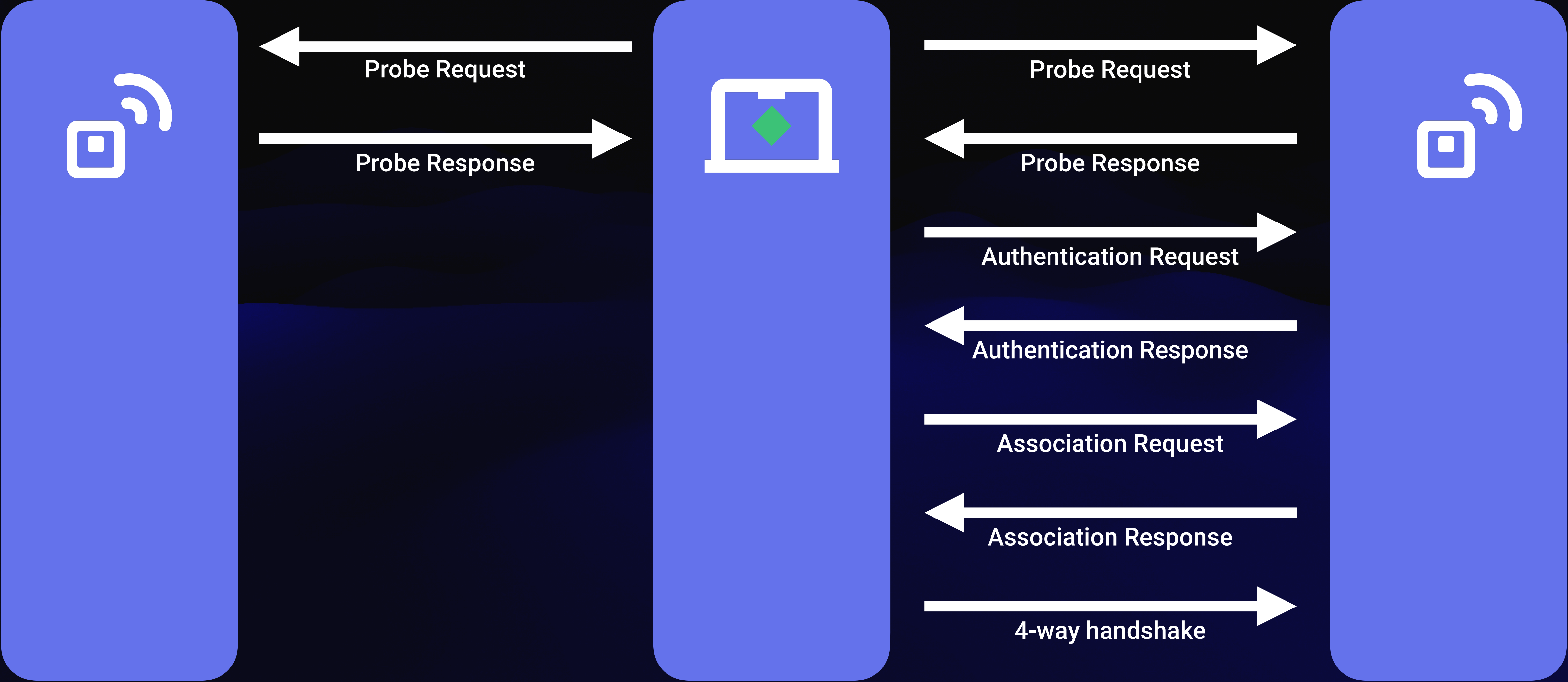


Roaming

- Client devices decide:
 - When to roam
 - How to roam
- Green Diamond
 - Represents a decision matrix
 - Concept by Keith Parsons at Wireless LAN Professionals



Client Association Process



Wi-Fi Security

Open

- Open authentication
- Unencrypted
- No built-in security
- Relies on upper-layer protocols (like HTTPS) for security

WEP

- “Wired Equivalent Privacy”
- Authentication with a hexadecimal key

WPA

- “Wi-Fi Protected Access”
- A stop-gap until WPA2 hardware rolled out
- Limited to 54 Mbps

Two variants

- WPA-Personal / WPA-PSK
 - 8-63 character pre-shared passkey
- WPA-Enterprise
 - Credentials exchanged with a RADIUS server

WPA2

- “Wi-Fi Protected Access 2”
- New cipher suite
- Required new hardware

Two variants

- WPA2-Personal / WPA2-PSK
 - 8-63 character pre-shared passkey
- WPA2-Enterprise
 - Credentials exchanged with a RADIUS server

WPA3

- “Wi-Fi Protected Access 3”

Three variants

- Enhanced Open
 - Encryption for open networks with Opportunistic Wireless Encryption (OWE)
- WPA3-Personal
- WPA3-Enterprise

What next?

- Hamina Training:
 - Hamina Certified Network Architect
 - Hamina Planning Specialist
 - Hamina Survey Specialist
 - hamina.com/training
- CWNP Program:
 - cwnp.com





Thank you!

Joel Crane, CWNE #233
Hamina Wireless

joel@hamina.com
support@hamina.com