Bryan Ward

Apples to Apples

And Other

AN ANALYSIS OF THE EFFECTS OF MDNS TRAFFIC ON A CAMPUS WLAN

^

What is mDNS?

Name resolution without a central server

- RFC 6762 “Multicast DNS”
- A way of “running the AppleTalk Name Binding Protocol over IP”
- Reserved multicast addresses 224.0.0.251 and ff0x::fb (commonly ff02::fb)
- UDP Port 5353
- DNS Service Discovery (DNS-SD, RFC 6763) rides on top of mDNS

IANA says:

“Addresses between 224.0.0.0 and 224.0.0.255… Multicast routers should not forward any multicast datagram with destination addresses in this range, regardless of its TTL.”

TTL should therefore be set to **1** to avoid forwarding

This is not explicitly defined.

TTL	Scope
0	Restricted to the same host. Won't be output by any interface.
1	Restricted to the same subnet. **Won't be forwarded by a router.**
<32	Restricted to the same site, organization or department.
<64	Restricted to the same region.
<128	Restricted to the same continent.
≤255	Unrestricted in scope. Global.

https://tldp.org/HOWTO/Multicast-HOWTO-2.html

"Packets with an address in this range are **local in scope** and **always should be transmitted with a Time To Live (TTL) of 1** so that they go no farther than the local subnet."

–Cisco
(https://www.cisco.com/c/dam/en/us/support/docs/ip/ip-multicast/ipmlt_wp.pdf)

"Packets with addresses in the range 224.0.0.0- 224.0.0.255 are sent with the **TTL field set to one**, and, therefore, the **scope** of the corresponding groups is **limited to the local network**."

–Ixia
(https://support.ixiacom.com/sites/default/files/resources/whitepaper/multicast.pdf)

TTL	Scope
0	Restricted to the same host. Won't be output by any interface.
1	Restricted to the same subnet. Won't be forwarded by a router.
<32	Restricted to the same site, organization or department.
<64	Restricted to the same region.
<128	Restricted to the same continent.
≤255	Unrestricted in scope. Global.

https://tldp.org/HOWTO/Multicast-HOWTO-2.html

Branch Sites

Watch out for:

- Spanned Layer 2 over a WAN circuit
- Routing multicast back to the main network
- APs tunnelling CAPWAP back to a controller

Jim Vajda: “**37% of the packets** on this busy WAN circuit were mDNS queries!”

https://framebyframewifi.net/2018/01/15/beware-of-mdns-floods-from-buggy-android-clients/

Wireless **LOCAL AREA** Network

Each multicast frame is seen over the air twice

or more…

Once when first sent from the STA to the AP

And again when retransmitted by the AP

Each AP connected to the same DS will retransmit the frame

Site with 20 APs, you see frame over the air 21 times total

It’s Like Fireworks

Multicast to Unicast

Some systems forward multicast frames as unicast to each associated STA

Multicast to Unicast

APs should participate in IGMP snooping and update the snooping tables as STAs roam

Not all do

Multicast to Unicast may be required with
STAs bridging into different VLANs on the DS

Otherwise, multicast traffic from all VLANs on the DS
will be sent to all STAs, not just from the VLAN the STA is bridged to

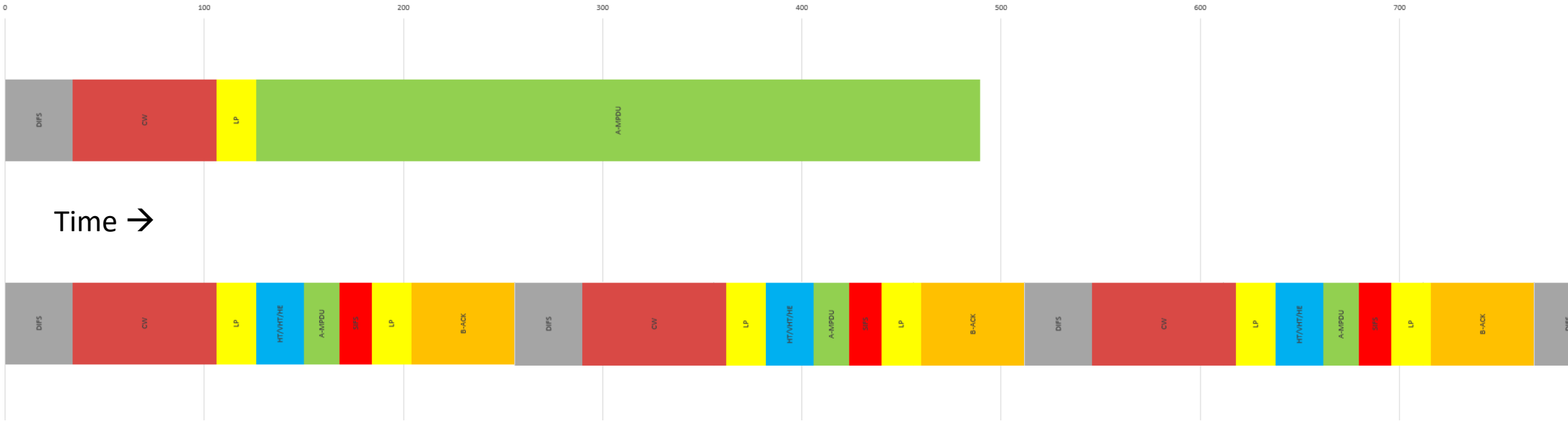
Like a Lawn Sprinkler

		Scenario 1 **Multicast**	Scenario 2 **Unicast**
AIFS/DIFS		DIFS	DIFS
AIFSN		2	2
Contention Window		8	8
Data Rate Control frames		6 mb/s	6 mb/s
modulation		BPSK 1/2	BPSK 1/2
bits pr subcarrier		1	1
coding value		0.5	0.5
PHY		20MHz OFDM (nonHT)	20MHz VHT
data subcarriers		48	52
Modulation and Coding		mcs0, BPSK 1/2 (or 6mbs for nonHT)	mcs7, 64-QAM 5/6
bits pr subcarrier		1	6
coding value		0.50	0.83
Spatial streams		1	2
Guard Interval		0.4	0.4
Speed Rate A-MPDUs		6.7	144.4
RTS, bytes		20	20
Symbols RTS		8	8
CTS, bytes		14	14
symbols CTS		6	6
ACK/B-ACK, bytes		34	34
symbols ACK		13	13
A-MPDU, bytes		300	300
databits to send		2422	2422
databits pr symbol		24	520
symbols A-MPDU		101	5
Protection on/off		0	0
		Durations scenario 1	**Durations scenario 2**
DIFS/AIFS	DIFS	34	34
Random backoff timer/CW	CW	72	72
Legacy preamble	LP		
RTS	RTS		
SIFS	SIFS		
Legacy preamble	LP		
CTS	CTS		
SIFS	SIFS		
Legacy preamble	LP	20	20
HT/VHT preamble	HT/VHT/HE		24
A-MPDU	A-MPDU	363.6	18
SIFS	SIFS		16
Legacy preamble	LP		20
ACK/B-ACK	B-ACK		52
Duration including DIFS&CW		489.6	256
Duration excluding DIFS&CW		383.6	150
Throughput		4.9	9.4

Airtime Calculator

https://gjermundraaen.com/thewifiairtimecalculator/

- Unicast is faster



- Unless it’s Unicast to multiple clients

In a
Reflection Amplification Attack,
the threat actor
consumes network resources
by reflecting a
high volume of network traffic
to the target.

https://www.cisa.gov/sites/default/files/publications/understanding-and-responding-to-ddos-attacks_508c.pdf

No.	Time	Source	Destination	Protocol	Length	DSCP	Info
8980	27.296323709	192.168.1.103	224.0.0.251	MDNS	329	0x00	Standard query 0x0000 ANY iPhone._rdlink._tcp.local,
8981	27.298900432	fe80::4fa:2b1:4500:f798	ff02::fb	MDNS	349	0x00	Standard query 0x0000 ANY iPhone._rdlink._tcp.local,

It gets worse:

Some devices send each mDNS message twice

One for IPv4 and again for IPv6

This is recommended by RFC 6762!

It’s not just Apple

- Amazon Echo
- Printers
- “Smart” TVs
- Android devices
- Chromecast
- Netally Etherscope

No.	Time	Source	Destination	Protocol	Length	DSCP	Info
75	50.805158	192.168.1.21	224.0.0.251	MDNS	70	0x00	Standard query 0x0000 A wpad.local, "QM" question
76	50.805619	fe80::94b6:5338:dd86:b…	ff02::fb	MDNS	90	0x00	Standard query 0x0000 A wpad.local, "QM" question
77	50.806065	192.168.1.21	224.0.0.251	MDNS	70	0x00	Standard query 0x0000 A wpad.local, "QM" question
78	50.806516	fe80::94b6:5338:dd86:b…	ff02::fb	MDNS	90	0x00	Standard query 0x0000 A wpad.local, "QM" question

WPAD

Windows is always looking for Web Proxy Auto-Discovery

Discoveries for devices/services that don’t even exist on your network

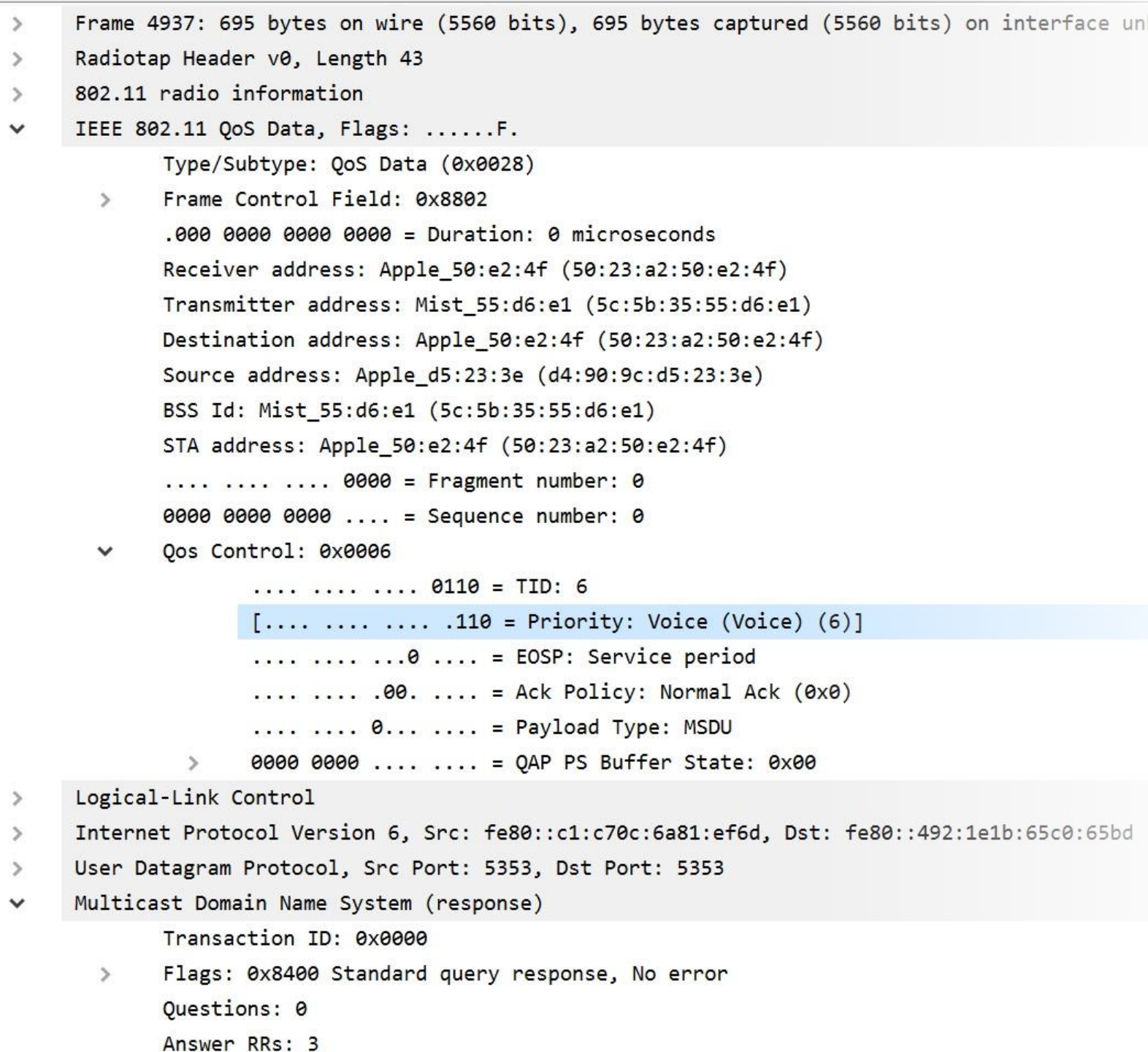
No.	Time	Source	Destination	Protocol	Length	DSCP	Info
96590	84.758911	192.168.1.150	224.0.0.251	MDNS	79	0x00	Standard query 0x0000 PTR _sengled._udp.local, "QM" question
98034	85.760471	192.168.1.150	224.0.0.251	MDNS	79	0x00	Standard query 0x0000 PTR _sengled._udp.local, "QM" question
99740	87.760902	192.168.1.150	224.0.0.251	MDNS	79	0x00	Standard query 0x0000 PTR _sengled._udp.local, "QM" question
1037…	91.764298	192.168.1.150	224.0.0.251	MDNS	79	0x00	Standard query 0x0000 PTR _sengled._udp.local, "QM" question
1130…	99.826405	192.168.1.150	224.0.0.251	MDNS	79	0x00	Standard query 0x0000 PTR _sengled._udp.local, "QM" question
1296…	115.774893	192.168.1.150	224.0.0.251	MDNS	79	0x00	Standard query 0x0000 PTR _sengled._udp.local, "QM" question

I don’t have any of these on my home network…

Home network, 24-hour period

iPhone	• 25,976 mDNS frames sent • 50% 12,988 IPv4 • 50% 12,988 IPv6
Android Phone	• 413 mDNS frames sent • 52% 213 IPv4 • 48% 200 IPv6
Amazon Echo Show	• 264 mDNS frames sent • 95% 250 IPv4 • 5% 14 IPv6
Amazon Echo Dot	• 154 mDNS frames sent • All IPv4

All devices connected for the full 24-hours



It gets more worse

QoS

Some devices mark mDNS traffic as

Voice Priority

or

Network Control

mDNS isn't the only chatty protocol

- LLMNR
- SSDP/UPnP
- Dropbox LAN Sync
- NBNS/WINS
- Sonos
- Spotify
- Printer Drivers

Paramount Pictures. (1988, January 18). Datalore. *Star Trek: The Next Generation*. episode. <https://memory-alpha.fandom.com/wiki/Lore>

Capture Rig

- 24 CPU Cores
- 512 GB RAM
- 5 TB Striped SSD Storage
- 10 Gbps Network
- 27 ERSPAN Ring Buffers

504,205,498

frames captured from the wire

DARTMOUTH ENGINEERING

408 APs, ~1500 Clients

3 Buildings

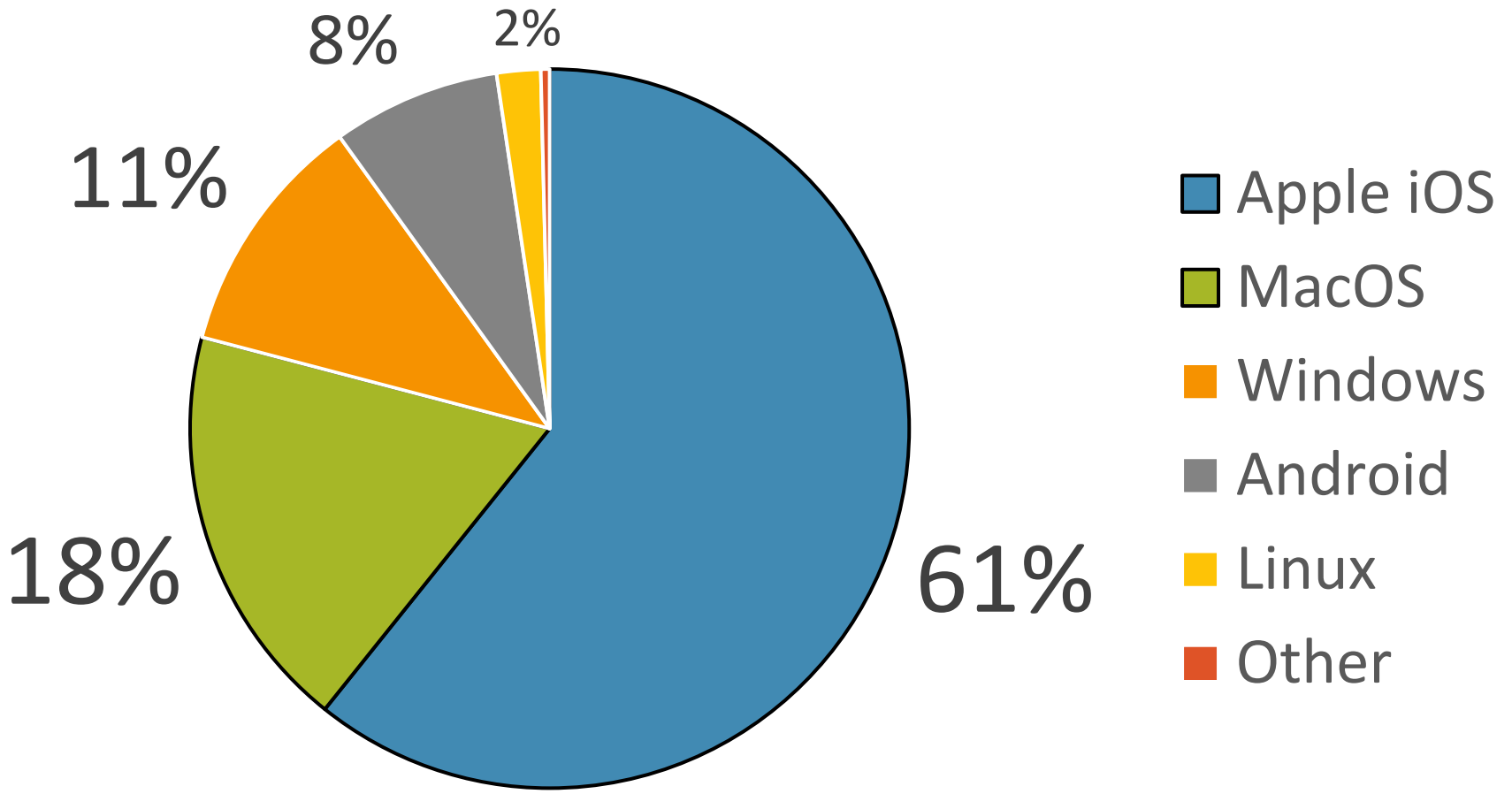
400k+ total sq. ft.

2 SSIDs

1 Hour-Long Test

12:30PM – 1:30PM

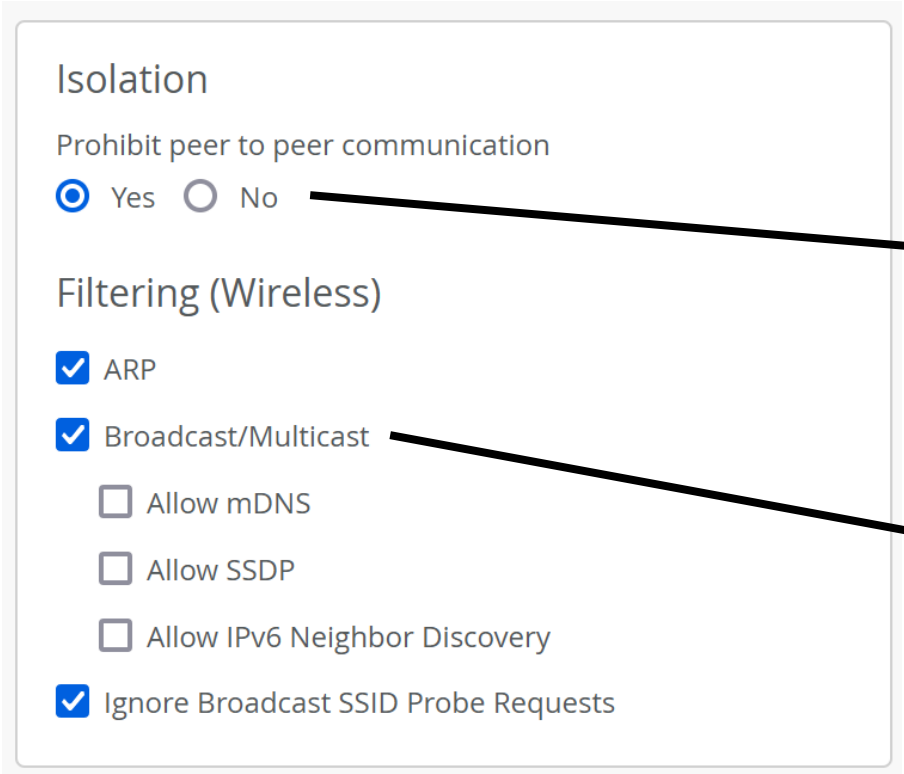
Client Distribution



What Was Changed

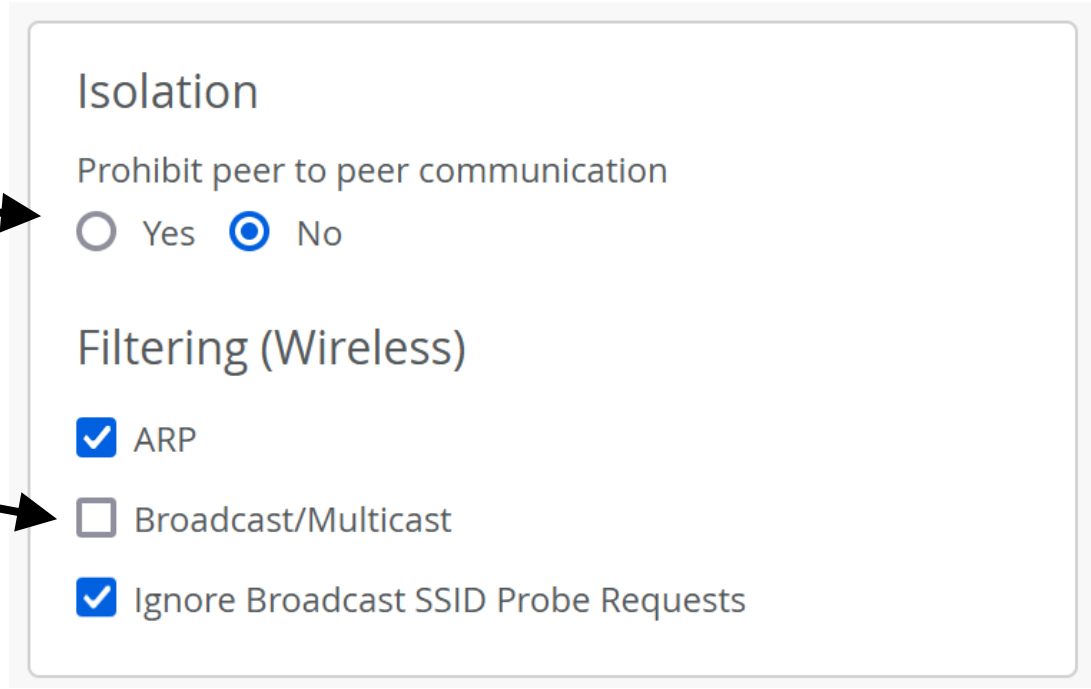
Traffic Blocked

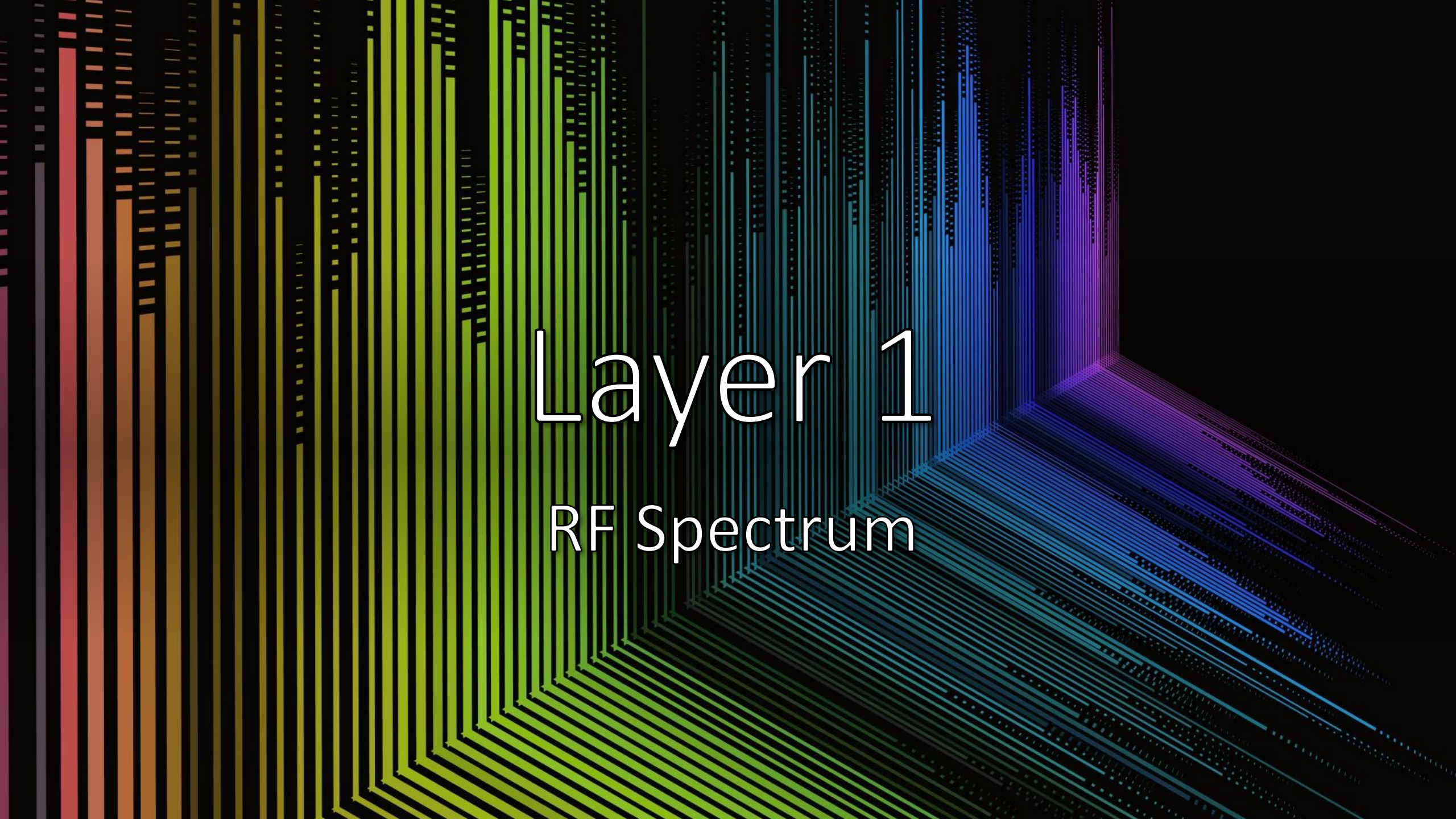
Before and After the Test



Traffic Allowed

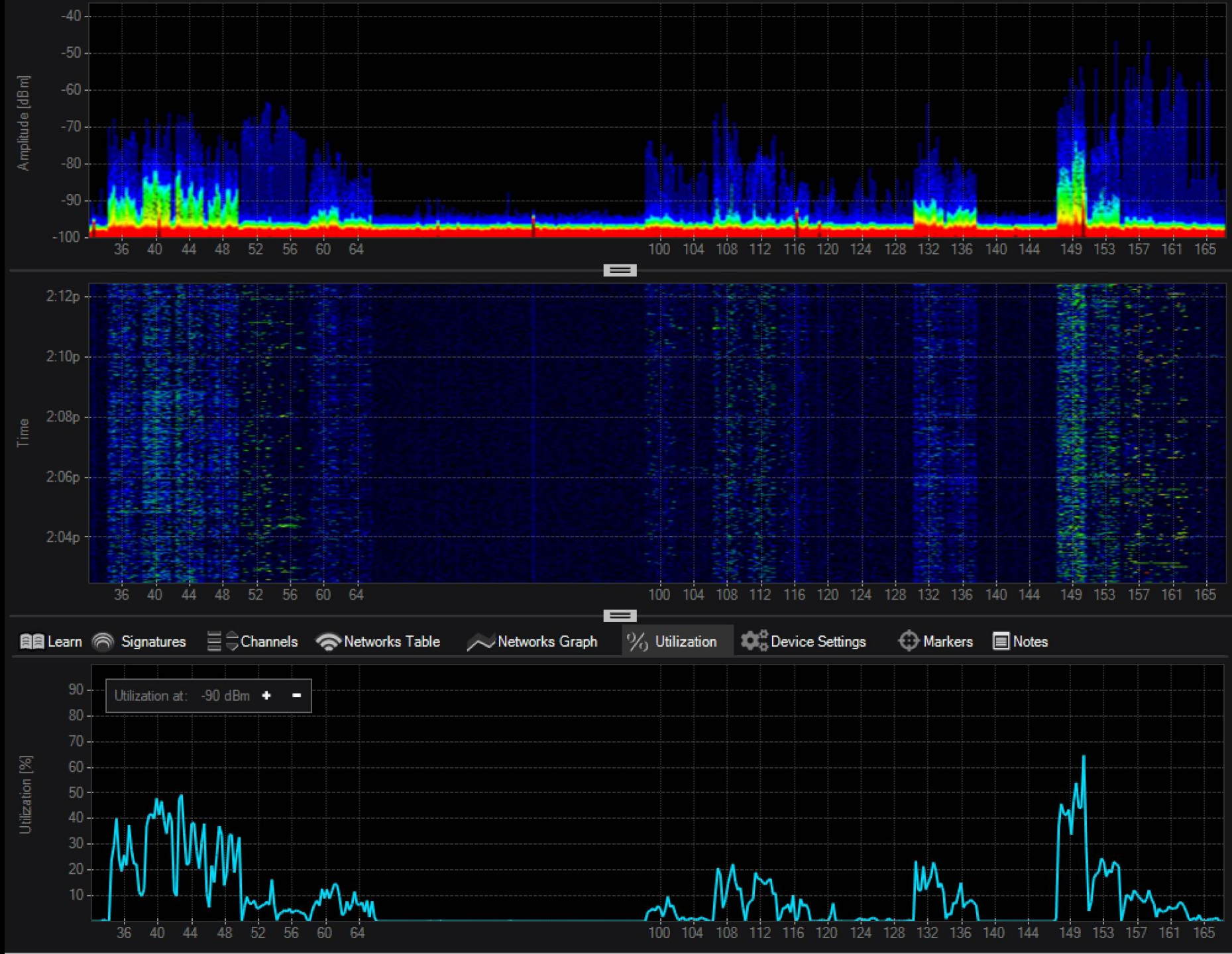
During the Test




Layer 1
RF Spectrum

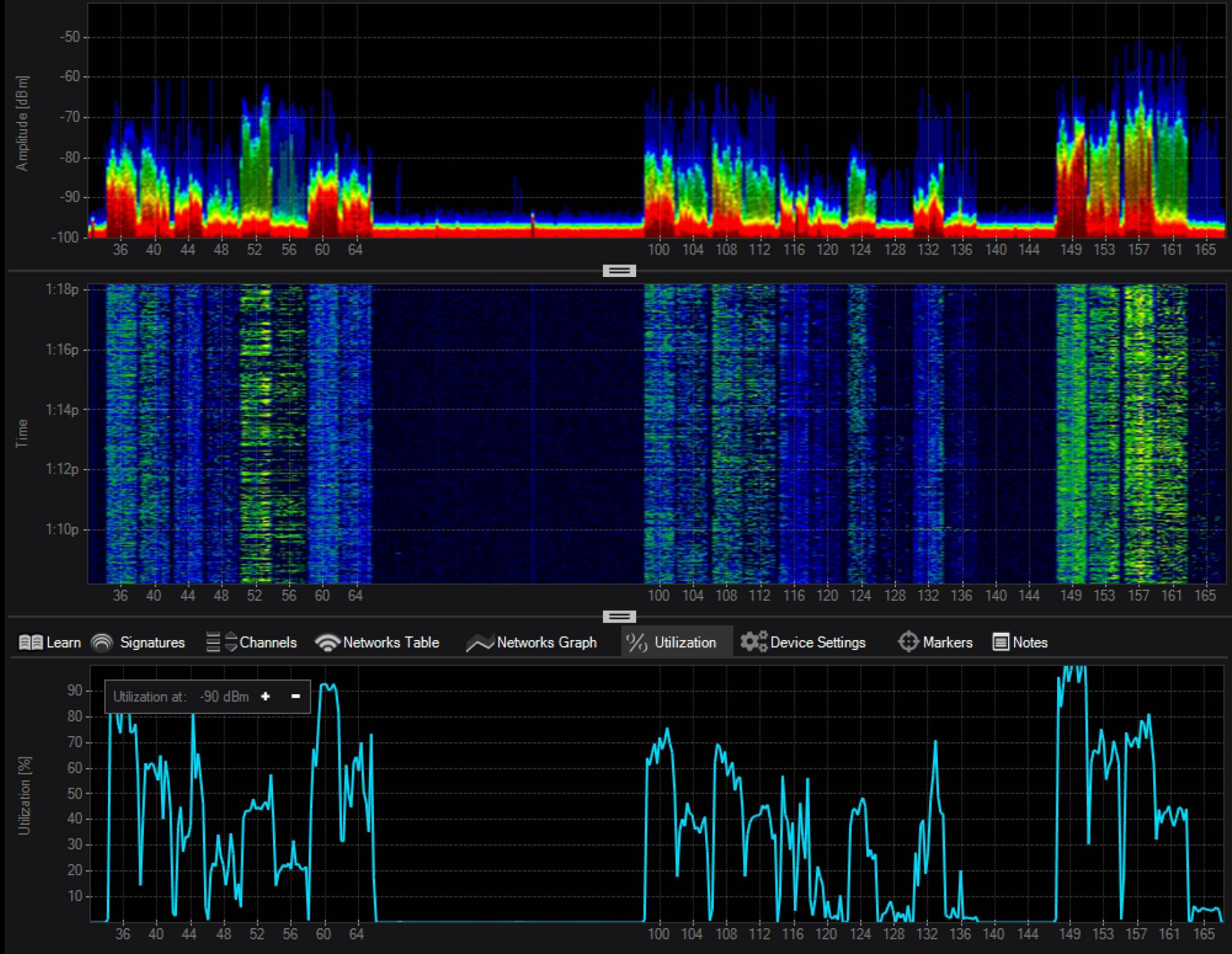
Spectrum

Traffic
Blocked

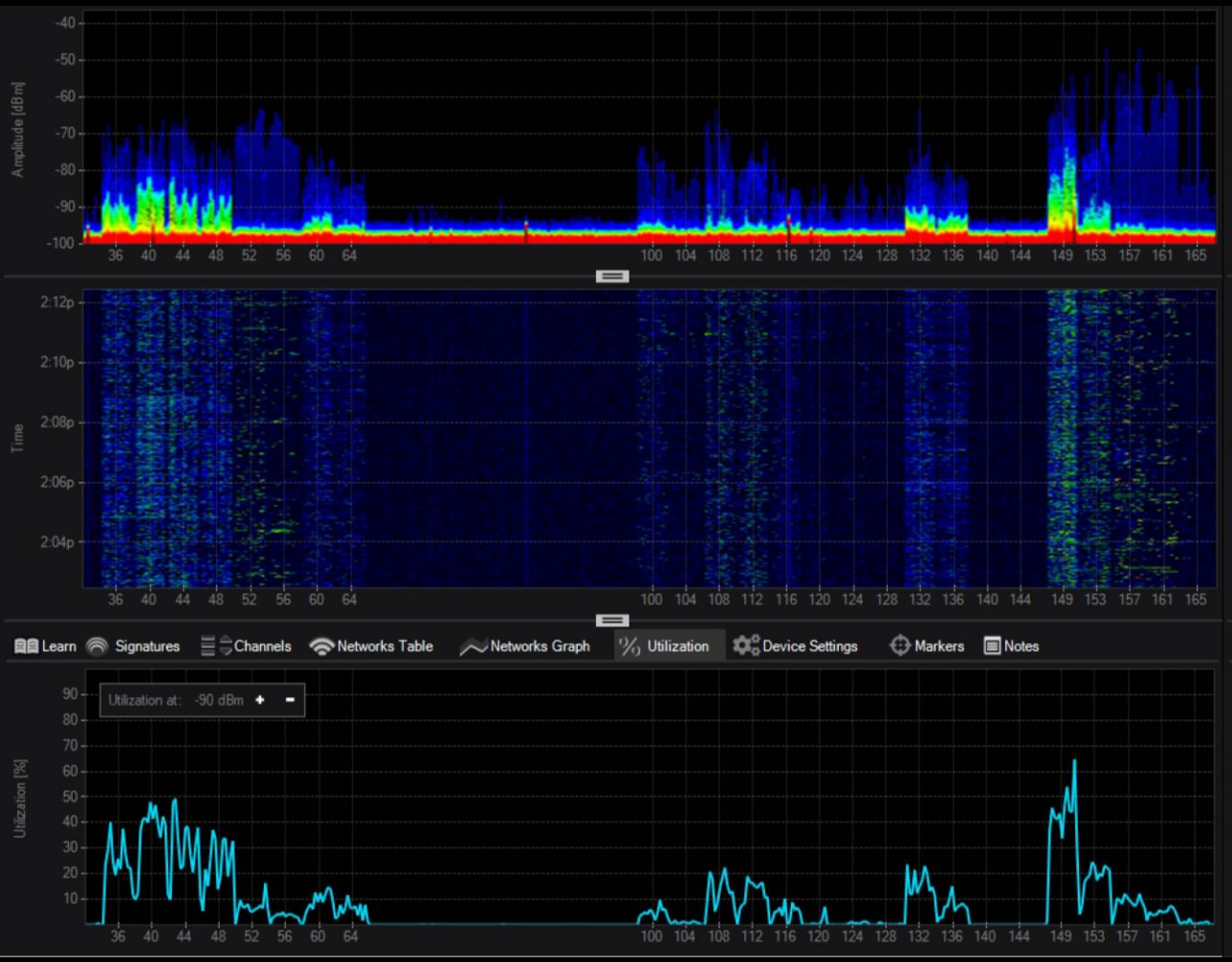


Spectrum

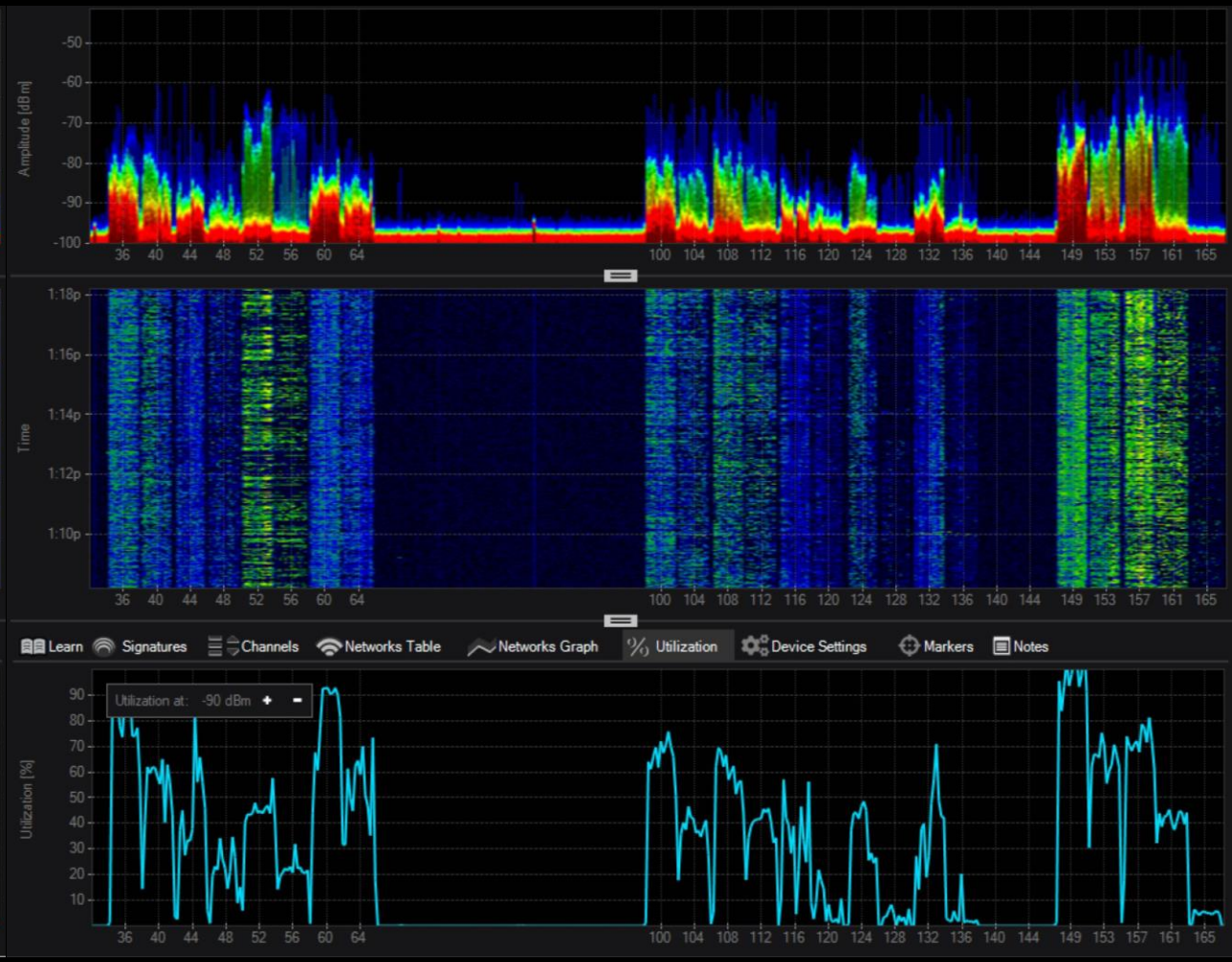
Traffic
Allowed

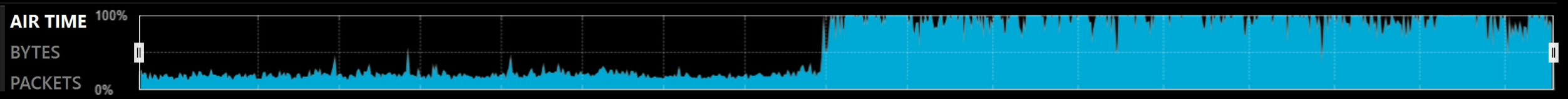


Traffic Blocked



Traffic Allowed



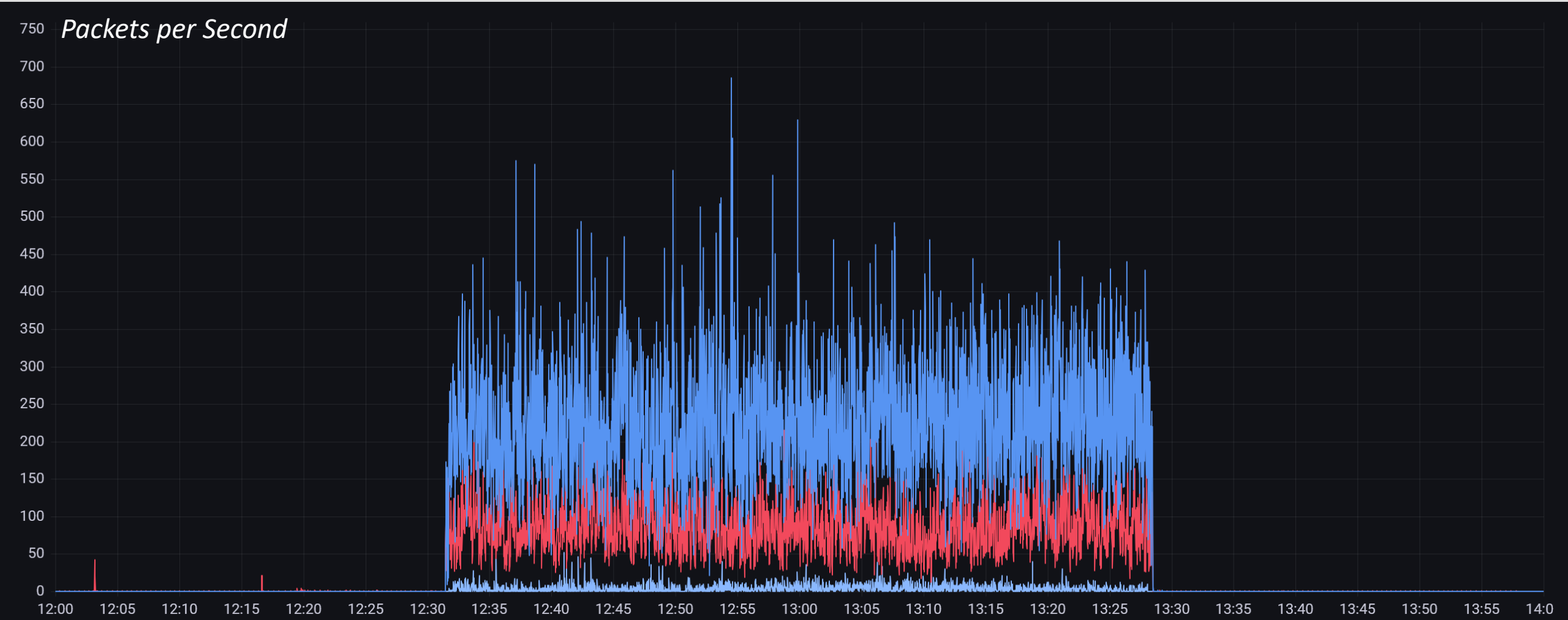


What did 500 Million Frames Show

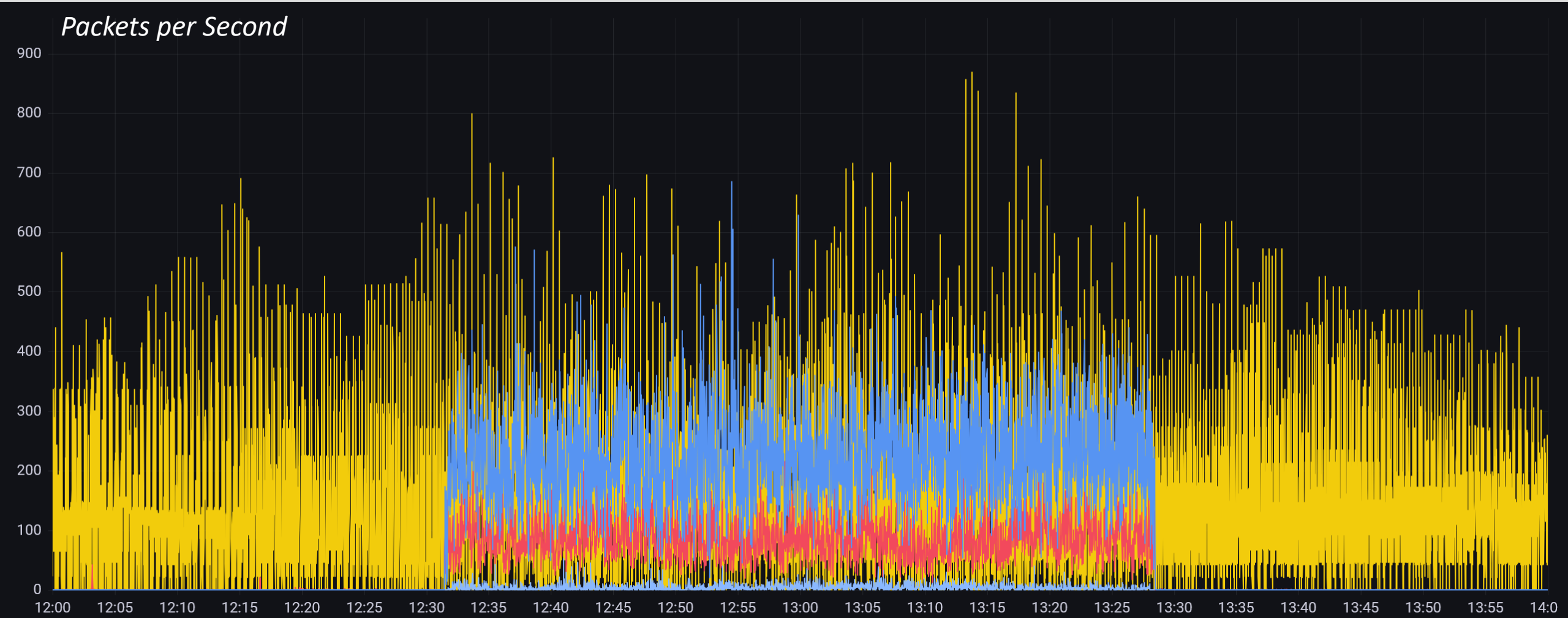
mDNS


Packets per Second
750
700
650
600
550
500
450
400
350
300
250
200
150
100
50
0
12:00
12:05
12:10
12:15
12:20
12:25
12:30
12:35
12:40
12:45
12:50
12:55
13:00
13:05
13:10
13:15
13:20
13:25
13:30
13:35
13:40
13:45
13:50
13:55
14:0

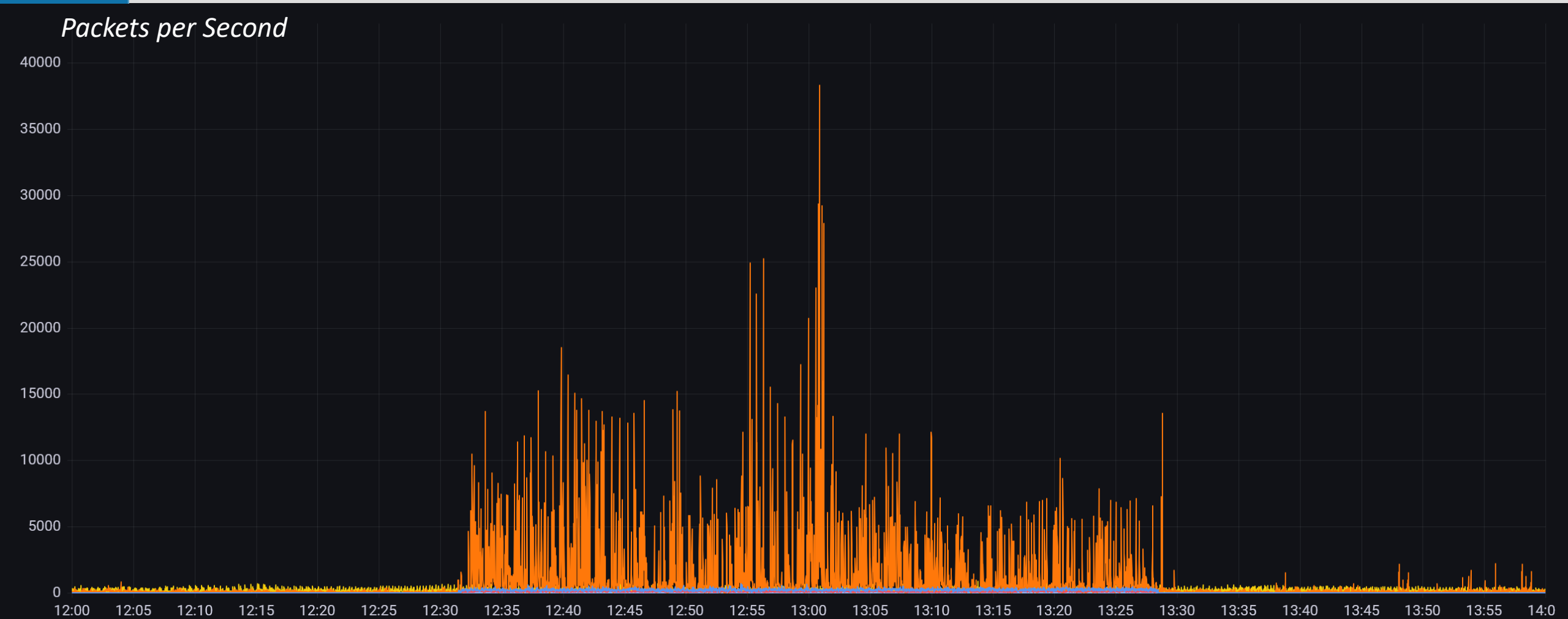
mDNS + SSDP + LLMNR



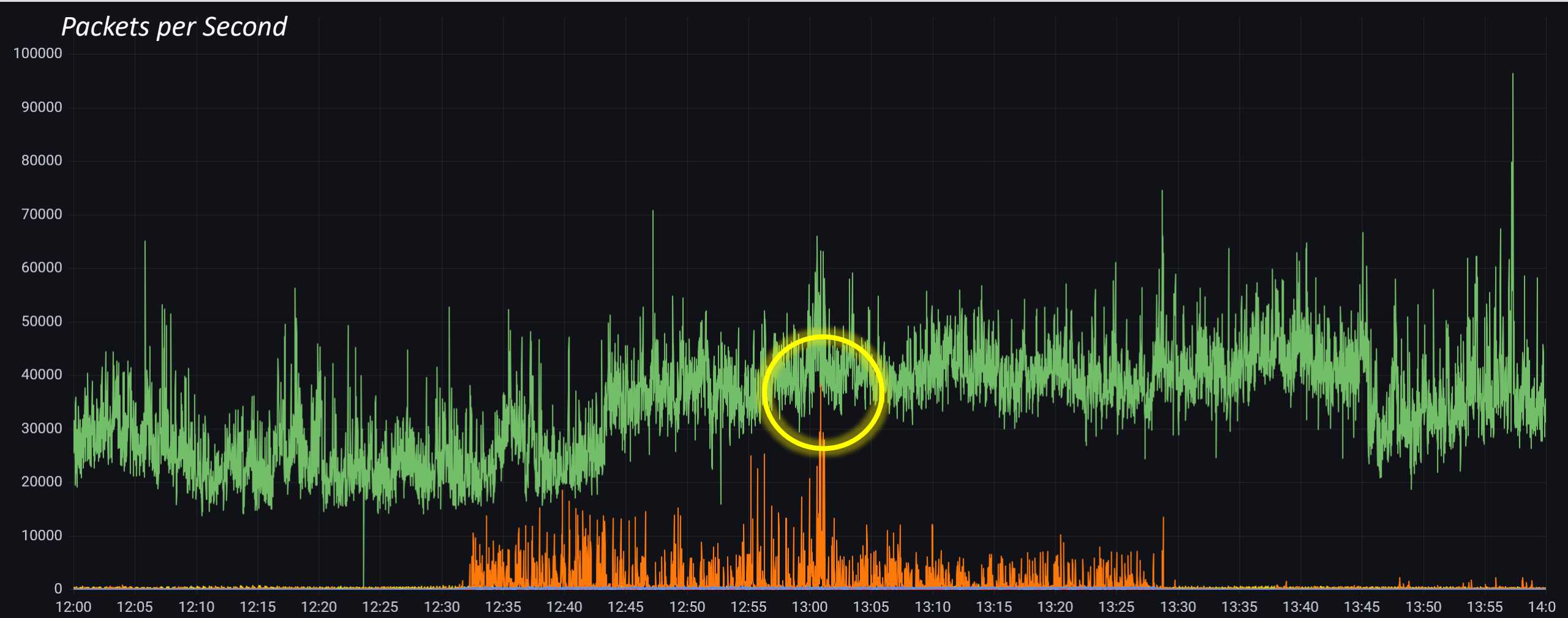
mDNS + SSDP + LLMNR + DB-LAN-Sync

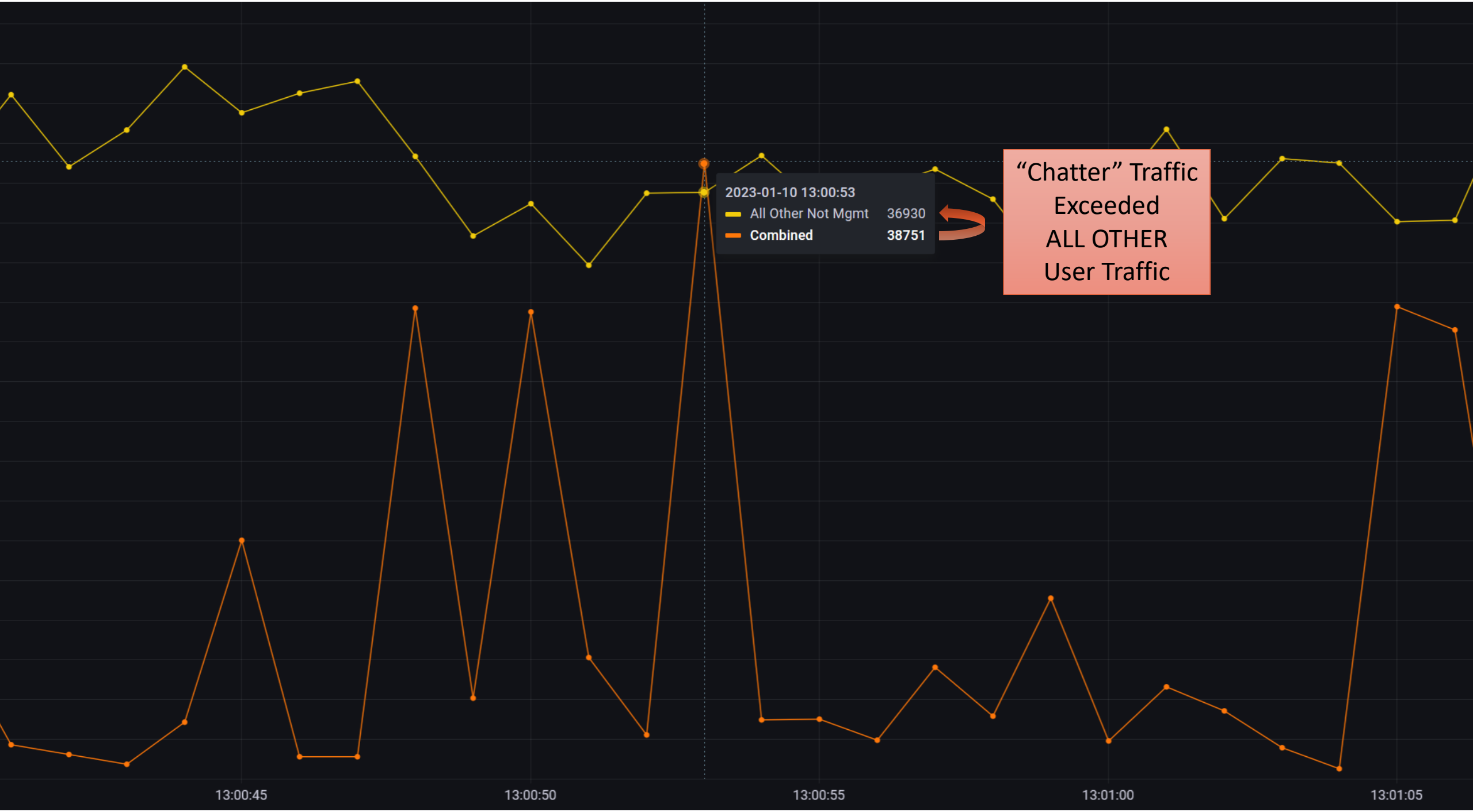


:(+ NBNS (aka. WINS)



Compared to All Other Site-Wide Traffic



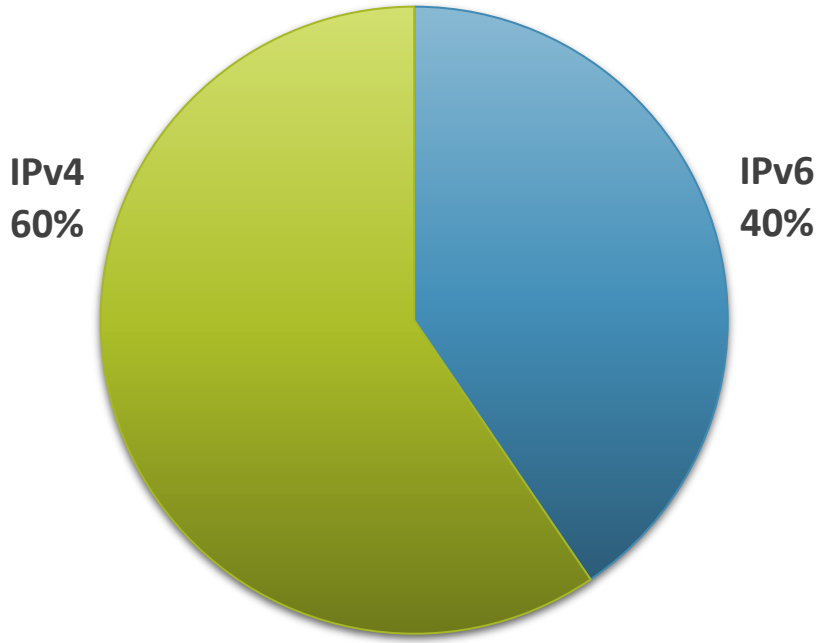

2023-01-10 13:00:53
All Other Not Mgmt 36930
Combined 38751
“Chatter” Traffic Exceeded ALL OTHER User Traffic
13:00:45
13:00:50
13:00:55
13:01:00
13:01:05

OTA Capture

Guest Network

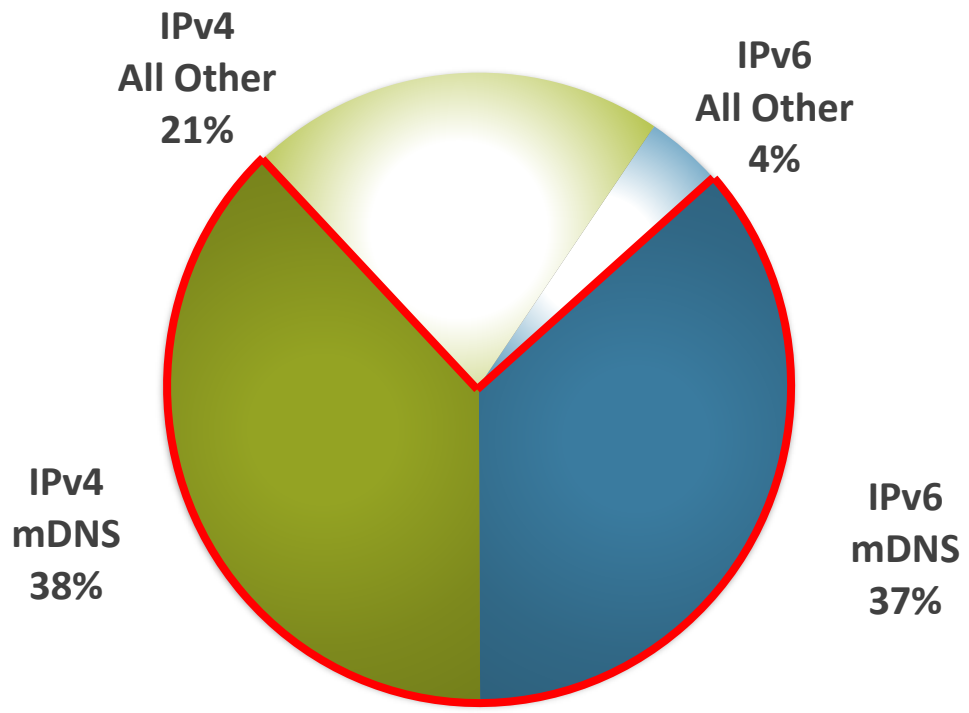
20 minutes

Protocol	Packets
Internet Protocol Version 6	18000
Internet Protocol Version 4	26453



OTA Capture
Guest Network
20 minutes

Protocol	Packets
Internet Protocol Version 6	18000
Multicast Domain Name System	16238
Internet Protocol Version 4	26453
Multicast Domain Name System	16883



mDNS accounted for
75% of ALL IP PACKETS

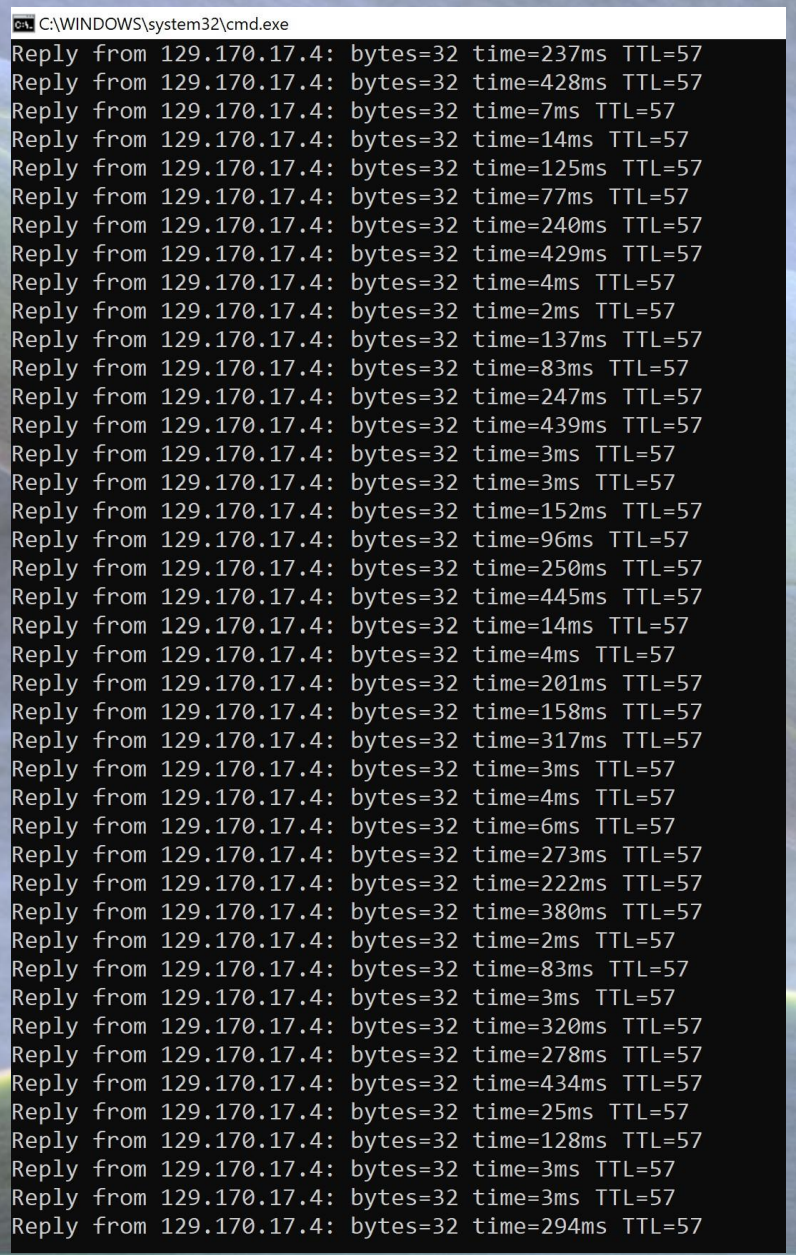
QBSS Load IE

Captured in Atrium

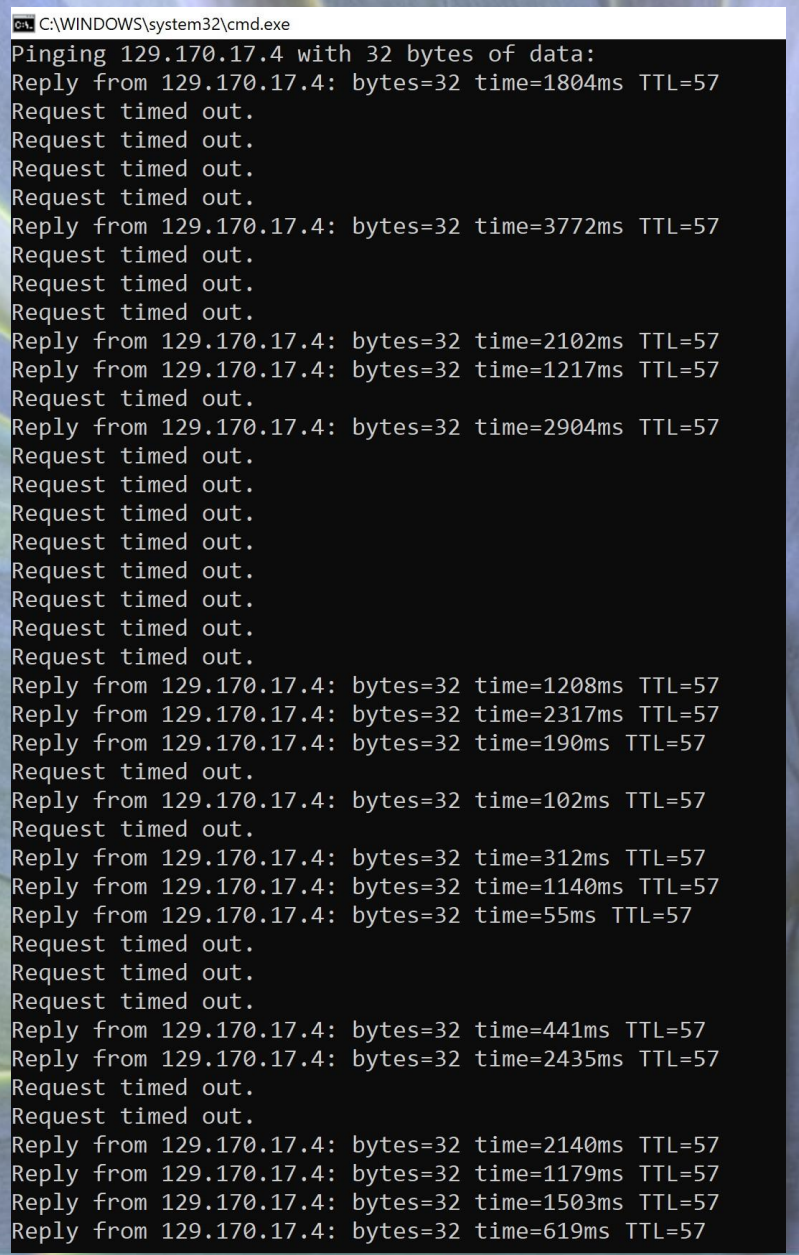
Source	Channel	Channel Utilization	Channel Util %	Station Count	Info
Mist_85:9f:f1	1	76	30%	0	Beacon frame, SN=0, FN=0, Flags=....., BI=0, SSID="eduroam"
Mist_85:96:31	6	38	15%	0	Beacon frame, SN=0, FN=0, Flags=....., BI=0, SSID="eduroam"
Mist_85:a4:13	6	25	10%	0	Beacon frame, SN=0, FN=0, Flags=....., BI=0, SSID="eduroam"
Mist_85:1d:a1	6	33	13%	0	Beacon frame, SN=0, FN=0, Flags=....., BI=0, SSID="eduroam"
Mist_85:96:31	6	18	7%	0	Beacon frame, SN=0, FN=0, Flags=....., BI=0, SSID="eduroam"
Mist_85:a4:13	6	26	10%	0	Beacon frame, SN=0, FN=0, Flags=....., BI=0, SSID="eduroam"
Mist_85:9f:33	11	101	40%	0	Beacon frame, SN=0, FN=0, Flags=....., BI=0, SSID="eduroam"
Mist_85:af:01	36	185	73%	12	Beacon frame, SN=0, FN=0, Flags=....., BI=0, SSID="eduroam"
Mist_85:93:71	100	68	27%	0	Beacon frame, SN=0, FN=0, Flags=....., BI=0, SSID="eduroam"
Mist_85:9a:f1	116	142	56%	3	Beacon frame, SN=0, FN=0, Flags=....., BI=0, SSID="eduroam"
Mist_63:4d:e3	124	114	45%	13	Beacon frame, SN=0, FN=0, Flags=....., BI=0, SSID="eduroam"
Mist_31:1b:83	124	255	100%	8	Beacon frame, SN=0, FN=0, Flags=....., BI=0, SSID="eduroam"
Mist_85:a0:93	132	125	49%	7	Beacon frame, SN=0, FN=0, Flags=....., BI=0, SSID="eduroam"
Mist_85:9f:d3	149	103	40%	3	Beacon frame, SN=0, FN=0, Flags=....., BI=0, SSID="eduroam"
Mist_85:96:11	157	105	41%	2	Beacon frame, SN=0, FN=0, Flags=....., BI=0, SSID="eduroam"
Mist_85:96:11	157	95	37%	2	Beacon frame, SN=0, FN=0, Flags=....., BI=0, SSID="eduroam"
Mist_62:ec:41	157	77	30%	1	Beacon frame, SN=0, FN=0, Flags=....., BI=0, SSID="eduroam"

Ping

Traffic Blocked



Traffic Allowed

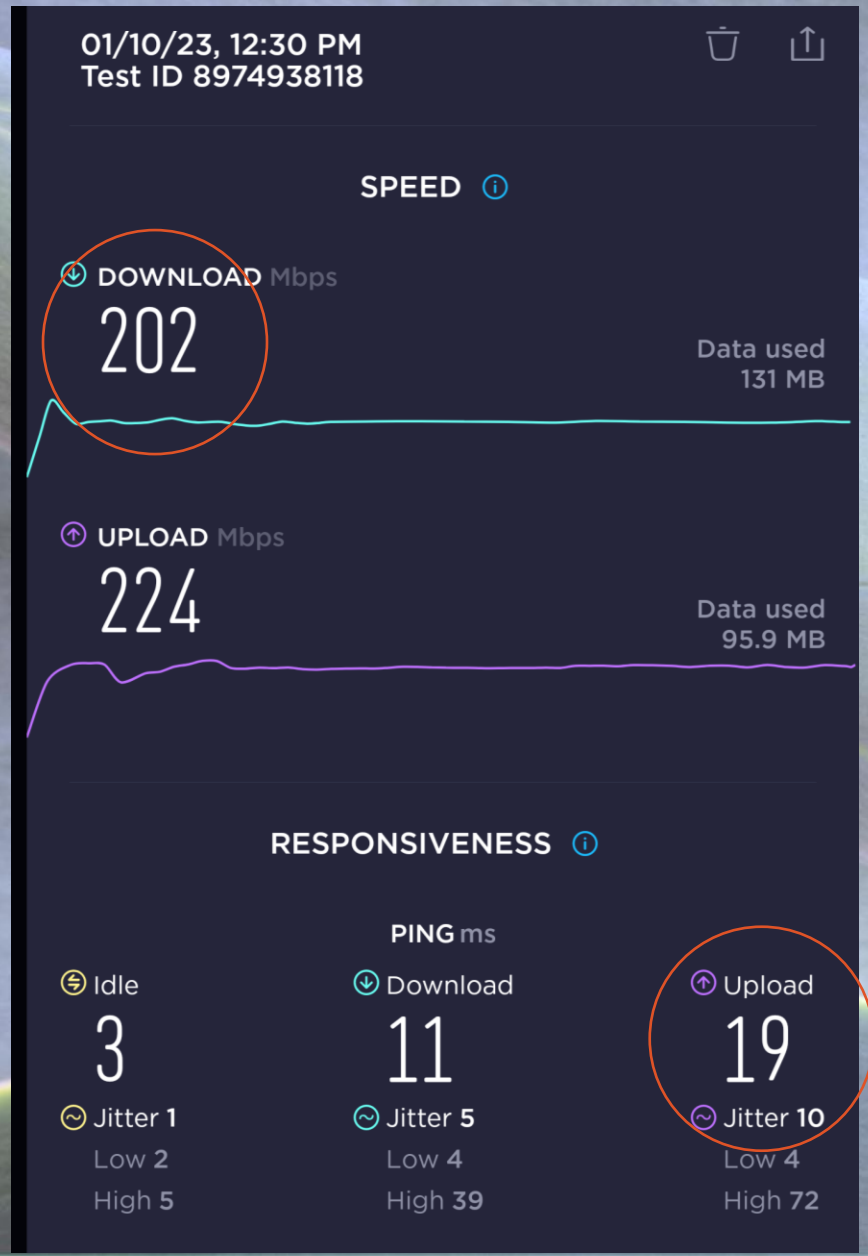


~10x more latency

154ms	1413ms
0% loss	56% loss

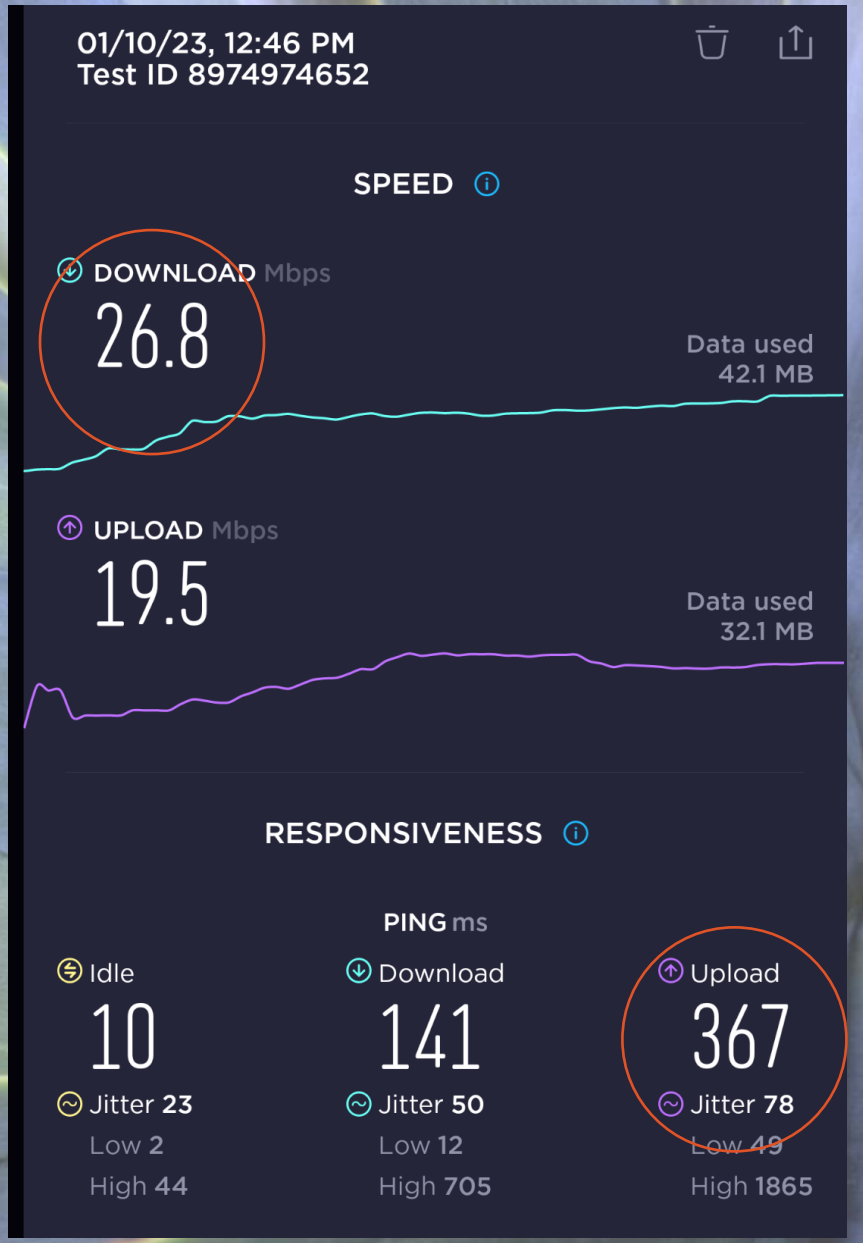
Speedtest

Traffic Blocked

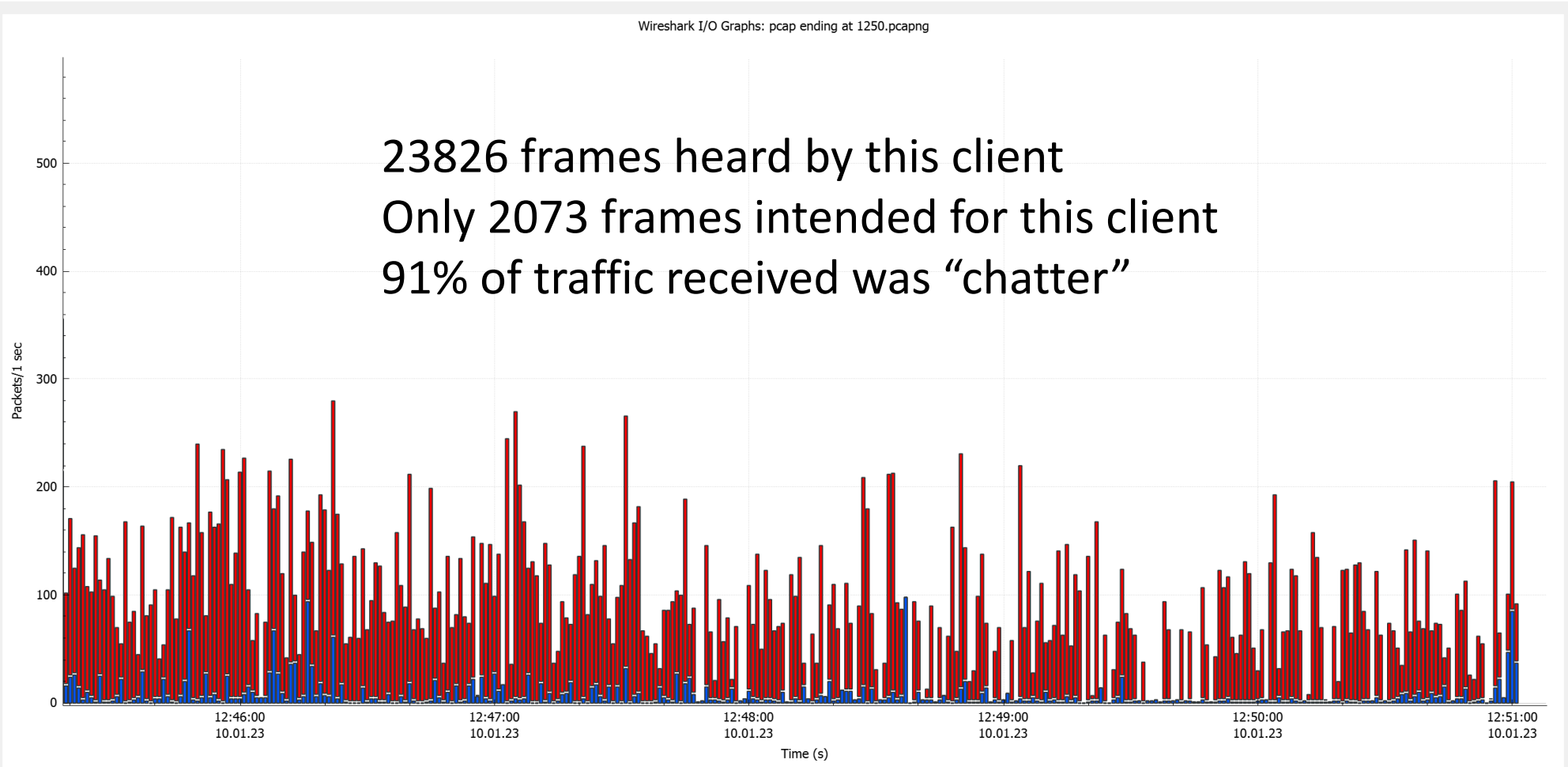


90% slower speed
17x loaded latency
8.5x more jitter

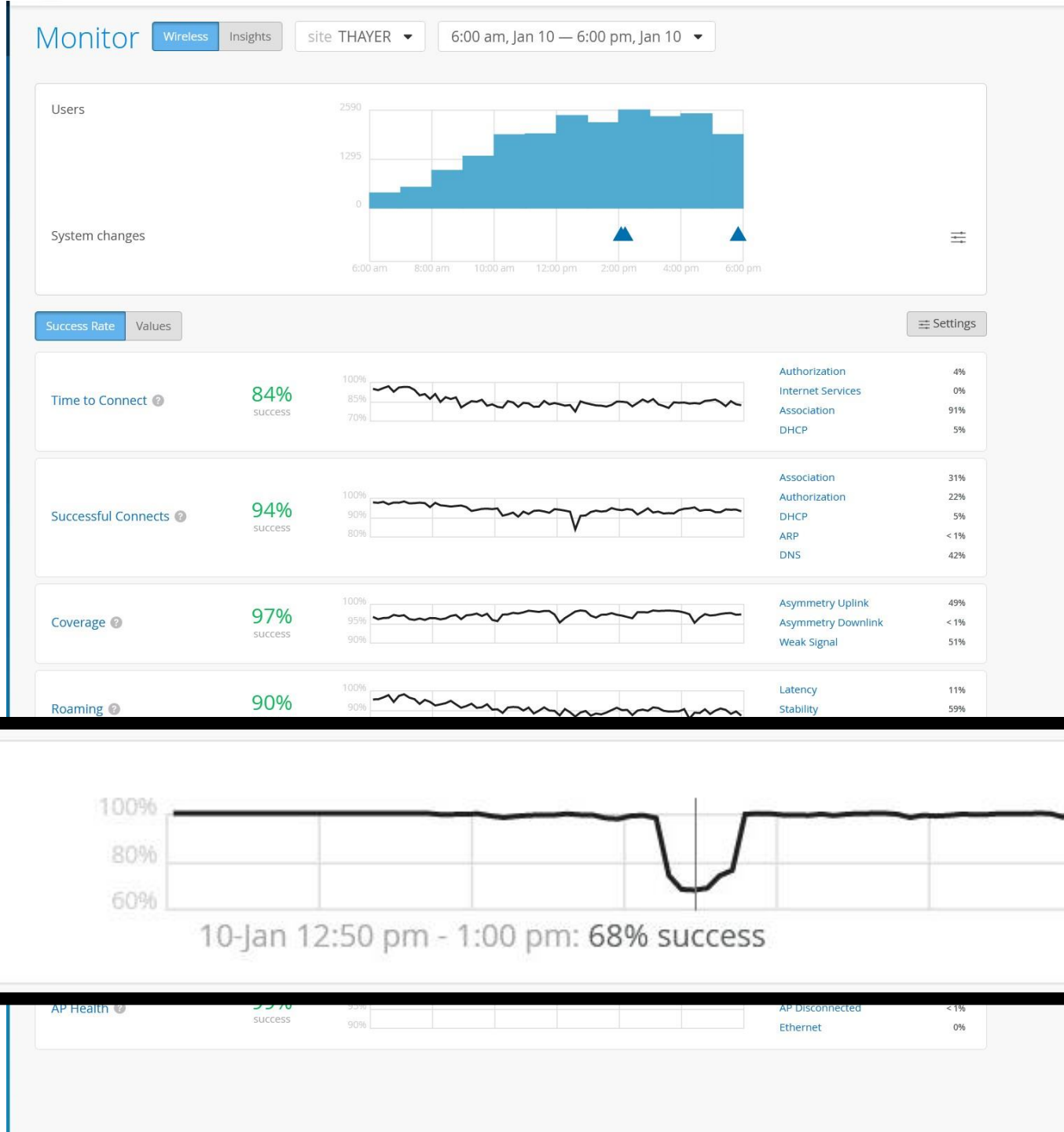
Traffic Allowed



PCAP from an associated STA



Mist SLEs


Monitor
Wireless
Insights
site THAYER
6:00 am, Jan 10 — 6:00 pm, Jan 10
Users
System changes
2590
1295
0
6:00 am
8:00 am
10:00 am
12:00 pm
2:00 pm
4:00 pm
6:00 pm
Success Rate
Values
Settings
Time to Connect
84%
success
Authorization 4%
Internet Services 0%
Association 91%
DHCP 5%
Successful Connects
94%
success
Association 31%
Authorization 22%
DHCP 5%
ARP < 1%
DNS 42%
Coverage
97%
success
Asymmetry Uplink 49%
Asymmetry Downlink < 1%
Weak Signal 51%
Roaming
90%
Latency 11%
Stability 59%
AP Health
success
AP Disconnected < 1%
Ethernet 0%

Capacity
100%
80%
60%
10-Jan 12:50 pm - 1:00 pm: 68% success

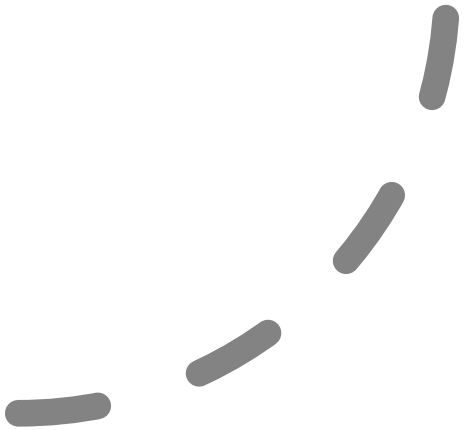
User Impact

- “We did notice effects from this test (worse than hoped/expected)…some of it was pretty impactful”
- “Sorry, having Wi-Fi trouble”
- SCP-ing a ~500MB file. About halfway in, the copy started stalling. A separate ssh connection to this same system was dropped
- RDP connection to a Windows server disconnected and reconnected constantly so the session was unusable
- Connections to various web sites were either slow or unusable during this whole window

User Impact

“I'm glad you only did an hour!

This was disruptive enough that it probably would have resulted in us bailing out if the test had run longer.”



Recommendations for Enterprise

1

Block This Traffic

2

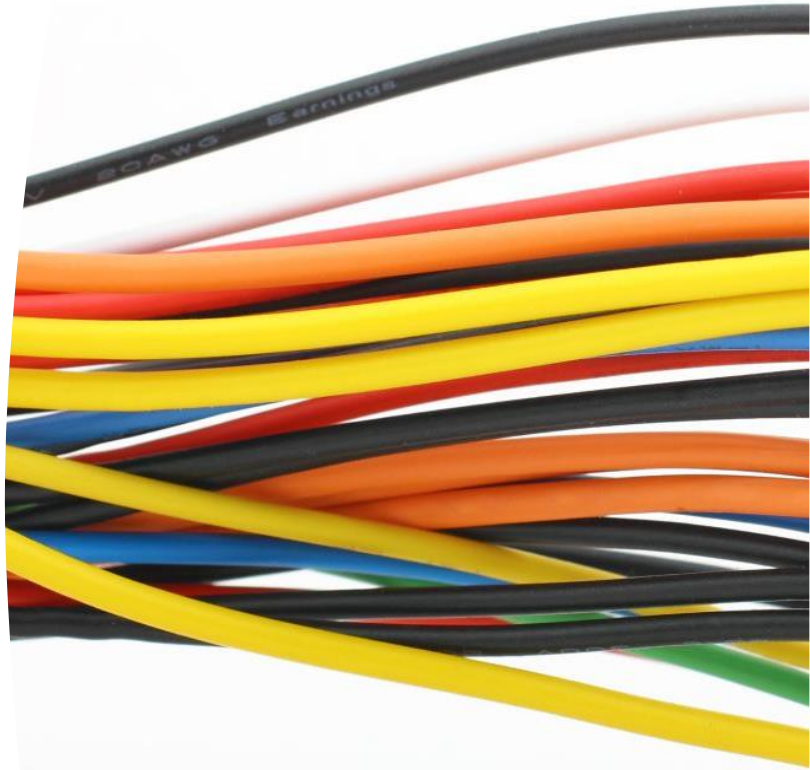
Use a Bonjour Gateway to advertise your services if needed

3

Limit scope of advertisements

Other Lessons Learned

- Wireshark has a hard-coded limit, independent of RAM
- Wireshark/TShark are single-threaded
- It’s REALLY hard to capture and analyze this amount of traffic
- **Layer 2 statistics do not accurately show the Layer 1 impact**



Thank You

Bryan Ward
Lead Network Engineer
Dartmouth College

www.BryanWard.net

@_bryan_ward_

3 Underscores