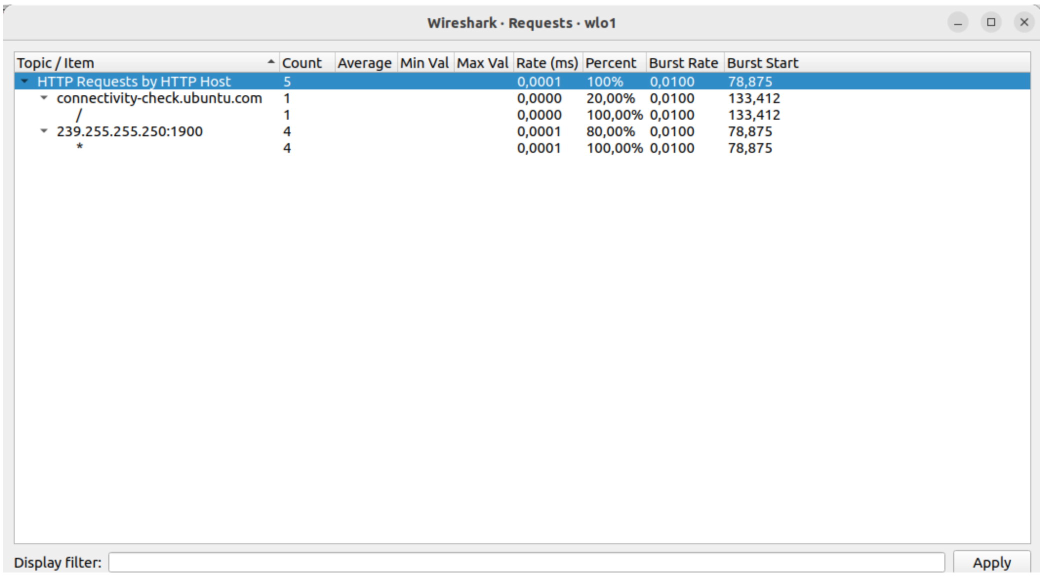
Wireshark Network Traffic Analysis Report

Introduction

This report presents an analysis of network traffic captured using Wireshark. The data includes HTTP requests, network endpoints, retransmitted packets, and TCP/UDP conversations. This analysis helps in identifying network activity patterns, potential issues, and troubleshooting network latency or retransmission errors. The insights obtained from this report can be useful for network administrators, security analysts, and IT professionals to enhance network performance and security.

HTTP Requests Analysis

- The HTTP requests captured in the network indicate communication with `connectivity-check.ubuntu.com`. This is a built-in Ubuntu feature that verifies internet connectivity by making periodic HTTP requests.
- The presence of multicast traffic to `239.255.255.250:1900` suggests that devices on the network are using SSDP (Simple Service Discovery Protocol), which is often associated with UPnP (Universal Plug and Play) services. This allows devices to automatically discover each other on the network.
- **HTTP request count:** `5` **-** A low number of HTTP requests suggests minimal browsing or automated network connectivity checks.
- The burst rate remains consistent, which indicates that network requests are evenly distributed over time, rather than being sporadic or indicative of heavy load.

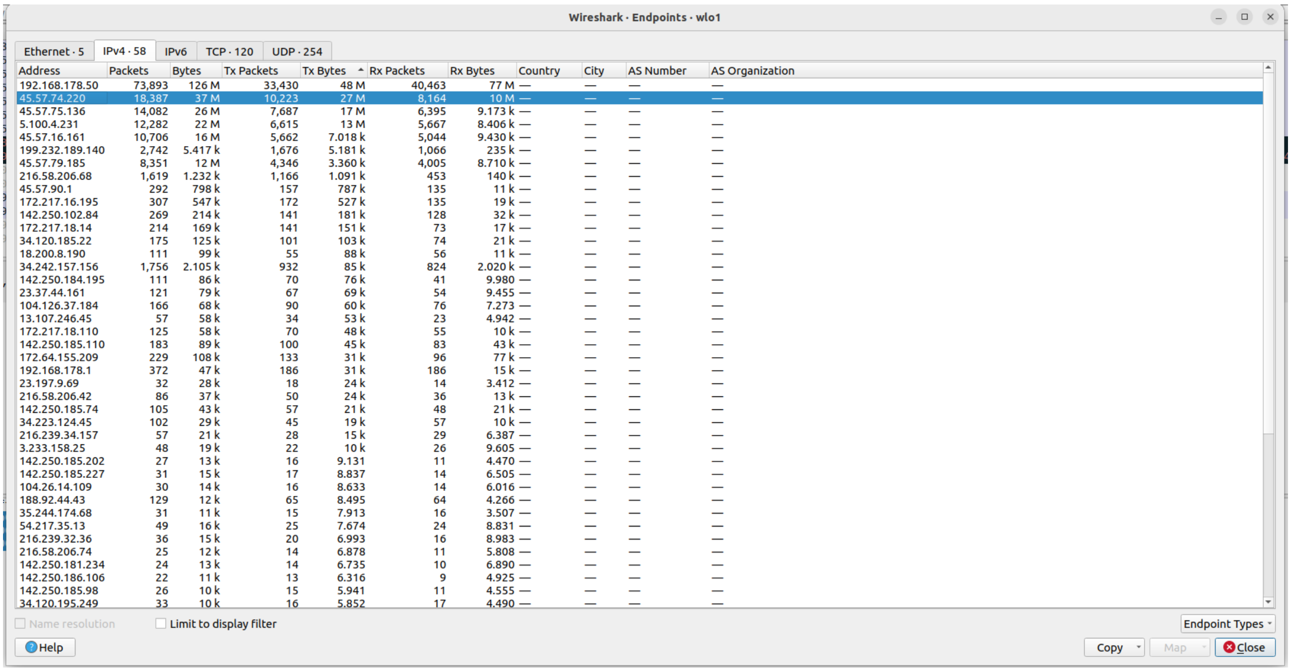


Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
HTTP Requests by HTTP Host	5				0,0001	100%	0,0100	78,875
connectivity-check.ubuntu.com	1				0,0000	20,00%	0,0100	133,412
/	1				0,0000	100,00%	0,0100	133,412
239.255.255.250:1900	4				0,0001	80,00%	0,0100	78,875
*	4				0,0001	100,00%	0,0100	78,875

Figure: HTTP Requests

IPv4 Endpoints Analysis

- The most active device in the captured packets is `192.168.178.50`, which appears to be a local machine responsible for the majority of network traffic.
- Significant communication with `45.57.74.220`, which is generating a large volume of packets and transferred bytes, suggests an ongoing connection to an external service or application.
- Other notable external connections include `5.100.4.231` and `199.232.189.140`, which could indicate access to cloud services, content delivery networks (CDNs), or other external applications.
- The dataset does not provide country or AS organization information, requiring further lookup to determine the origin and purpose of these IP addresses.

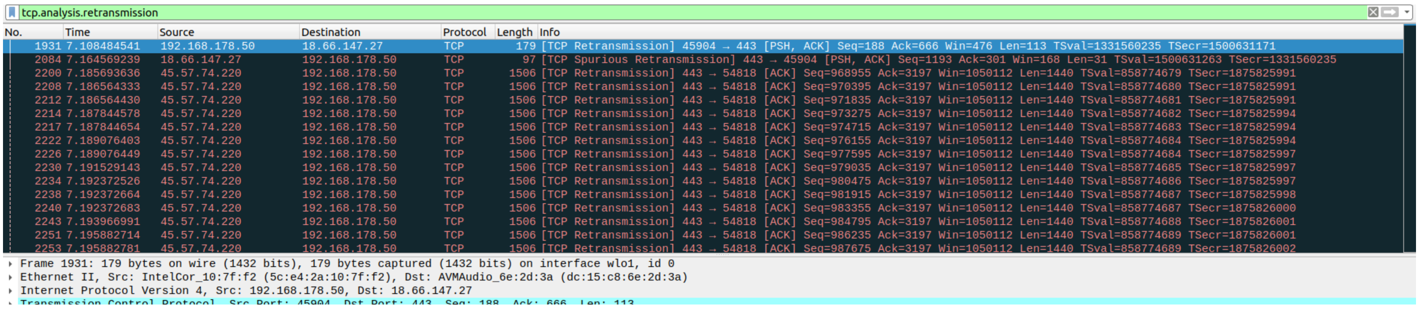


Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
192.168.178.50	73,893	126 M	33,430	48 M	40,463	77 M	—	—	—	—
45.57.74.220	18,387	37 M	10,223	27 M	8,164	10 M	—	—	—	—
45.57.75.136	14,082	26 M	7,687	17 M	6,395	9.173 k	—	—	—	—
5.100.4.231	12,282	22 M	6,615	13 M	5,667	8.406 k	—	—	—	—
45.57.16.161	10,706	16 M	5,662	7.018 k	5,044	9.430 k	—	—	—	—
199.232.189.140	2,742	5.417 k	1,676	5.181 k	1,066	235 k	—	—	—	—
45.57.79.185	8,351	12 M	4,346	3.360 k	4,005	8.710 k	—	—	—	—
216.58.206.68	1,619	1.232 k	1,166	1.091 k	453	140 k	—	—	—	—
45.57.90.1	292	798 k	157	787 k	135	11 k	—	—	—	—
172.217.16.195	307	547 k	172	527 k	135	19 k	—	—	—	—
142.250.102.84	269	214 k	141	181 k	128	32 k	—	—	—	—
172.217.18.14	214	169 k	141	151 k	73	17 k	—	—	—	—
34.120.185.22	175	125 k	101	103 k	74	21 k	—	—	—	—
18.200.8.190	111	99 k	55	88 k	56	11 k	—	—	—	—
34.242.157.156	1,756	2.105 k	932	85 k	824	2.020 k	—	—	—	—
142.250.184.195	111	86 k	70	76 k	41	9.980	—	—	—	—
23.37.44.161	121	79 k	67	69 k	54	9.455	—	—	—	—
104.126.37.184	166	68 k	90	60 k	76	7.273	—	—	—	—
13.107.246.45	57	58 k	34	53 k	23	4.942	—	—	—	—
172.217.18.110	125	58 k	70	48 k	55	10 k	—	—	—	—
142.250.185.110	183	89 k	100	45 k	83	43 k	—	—	—	—
172.64.155.209	229	108 k	133	31 k	96	77 k	—	—	—	—
192.168.178.1	372	47 k	186	31 k	186	15 k	—	—	—	—
23.197.9.69	32	28 k	18	24 k	14	3.412	—	—	—	—
216.58.206.42	86	37 k	50	24 k	36	13 k	—	—	—	—
142.250.185.74	105	43 k	57	21 k	48	21 k	—	—	—	—
34.223.124.45	102	29 k	45	19 k	57	10 k	—	—	—	—
216.239.34.157	57	21 k	28	15 k	29	6.387	—	—	—	—
3.233.158.25	48	19 k	22	10 k	26	9.605	—	—	—	—
142.250.185.202	27	13 k	16	9.131	11	4.470	—	—	—	—
142.250.185.227	31	15 k	17	8.837	14	6.505	—	—	—	—
104.26.14.109	30	14 k	16	8.633	14	6.016	—	—	—	—
188.92.44.43	129	12 k	65	8.495	64	4.266	—	—	—	—
35.244.174.68	31	11 k	15	7.913	16	3.507	—	—	—	—
54.217.35.13	49	16 k	25	7.674	24	8.831	—	—	—	—
216.239.32.36	36	15 k	20	6.993	16	8.983	—	—	—	—
216.58.206.74	25	12 k	14	6.878	11	5.808	—	—	—	—
142.250.181.234	24	13 k	14	6.735	10	6.890	—	—	—	—
142.250.186.106	22	11 k	13	6.316	9	4.925	—	—	—	—
142.250.185.98	26	10 k	15	5.941	11	4.555	—	—	—	—
34.120.195.249	33	10 k	16	5.852	17	4.490	—	—	—	—

Figure: IPV4 Conversations

TCP Retransmission Analysis

- Several **TCP retransmissions** have been detected, which may indicate network issues such as:
    1. **Packet loss**: This can occur due to weak WiFi signals, congestion, or misconfigured network settings.
    2. **Network congestion**: If the network is overloaded, packets may be delayed or dropped, leading to retransmissions.
    3. **Latency issues**: High latency can cause repeated transmission attempts before successful acknowledgment.
- The retransmissions involve port **`443`**, which suggests that HTTPS traffic is experiencing issues. This can be due to unstable internet connections or slow server responses.
- The communication between **`192.168.178.50`** and **`18.66.147.27`** repeatedly shows retransmissions, indicating a problem in reaching that external host, possibly due to server unresponsiveness or packet loss.



tcp.analysis.retransmission

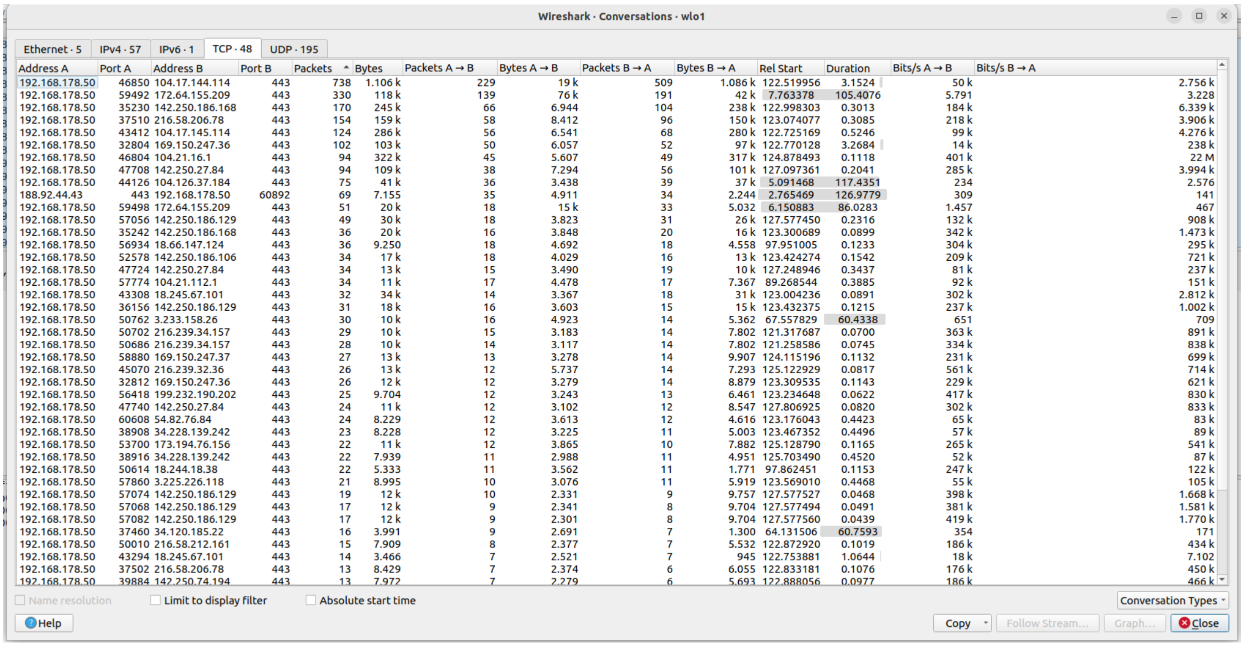
No.	Time	Source	Destination	Protocol	Length	Info
1931	7.108484541	192.168.178.50	18.66.147.27	TCP	179	[TCP Retransmission] 45904 → 443 [PSH, ACK] Seq=188 Ack=666 Win=476 Len=113 TSval=1331560235 TSecr=1500631171
2084	7.164569239	18.66.147.27	192.168.178.50	TCP	97	[TCP Spurious Retransmission] 443 → 45904 [PSH, ACK] Seq=1193 Ack=301 Win=168 Len=31 TSval=1500631263 TSecr=1331560235
2200	7.185693636	45.57.74.220	192.168.178.50	TCP	1506	[TCP Retransmission] 443 → 54818 [ACK] Seq=968955 Ack=3197 Win=1050112 Len=1440 TSval=858774679 TSecr=1875825991
2208	7.186564333	45.57.74.220	192.168.178.50	TCP	1506	[TCP Retransmission] 443 → 54818 [ACK] Seq=970395 Ack=3197 Win=1050112 Len=1440 TSval=858774680 TSecr=1875825991
2212	7.186564430	45.57.74.220	192.168.178.50	TCP	1506	[TCP Retransmission] 443 → 54818 [ACK] Seq=971835 Ack=3197 Win=1050112 Len=1440 TSval=858774681 TSecr=1875825991
2214	7.187844578	45.57.74.220	192.168.178.50	TCP	1506	[TCP Retransmission] 443 → 54818 [ACK] Seq=973275 Ack=3197 Win=1050112 Len=1440 TSval=858774682 TSecr=1875825994
2217	7.187844654	45.57.74.220	192.168.178.50	TCP	1506	[TCP Retransmission] 443 → 54818 [ACK] Seq=974715 Ack=3197 Win=1050112 Len=1440 TSval=858774683 TSecr=1875825994
2222	7.189076403	45.57.74.220	192.168.178.50	TCP	1506	[TCP Retransmission] 443 → 54818 [ACK] Seq=976155 Ack=3197 Win=1050112 Len=1440 TSval=858774684 TSecr=1875825994
2226	7.189076449	45.57.74.220	192.168.178.50	TCP	1506	[TCP Retransmission] 443 → 54818 [ACK] Seq=977595 Ack=3197 Win=1050112 Len=1440 TSval=858774684 TSecr=1875825997
2230	7.191529143	45.57.74.220	192.168.178.50	TCP	1506	[TCP Retransmission] 443 → 54818 [ACK] Seq=979035 Ack=3197 Win=1050112 Len=1440 TSval=858774685 TSecr=1875825997
2234	7.192372526	45.57.74.220	192.168.178.50	TCP	1506	[TCP Retransmission] 443 → 54818 [ACK] Seq=980475 Ack=3197 Win=1050112 Len=1440 TSval=858774686 TSecr=1875825997
2238	7.192372664	45.57.74.220	192.168.178.50	TCP	1506	[TCP Retransmission] 443 → 54818 [ACK] Seq=981915 Ack=3197 Win=1050112 Len=1440 TSval=858774687 TSecr=1875825998
2240	7.192372683	45.57.74.220	192.168.178.50	TCP	1506	[TCP Retransmission] 443 → 54818 [ACK] Seq=983355 Ack=3197 Win=1050112 Len=1440 TSval=858774687 TSecr=1875826000
2243	7.193966991	45.57.74.220	192.168.178.50	TCP	1506	[TCP Retransmission] 443 → 54818 [ACK] Seq=984795 Ack=3197 Win=1050112 Len=1440 TSval=858774688 TSecr=1875826001
2251	7.195882714	45.57.74.220	192.168.178.50	TCP	1506	[TCP Retransmission] 443 → 54818 [ACK] Seq=986235 Ack=3197 Win=1050112 Len=1440 TSval=858774689 TSecr=1875826001
2253	7.195882781	45.57.74.220	192.168.178.50	TCP	1506	[TCP Retransmission] 443 → 54818 [ACK] Seq=987675 Ack=3197 Win=1050112 Len=1440 TSval=858774689 TSecr=1875826002

```
▸ Frame 1931: 179 bytes on wire (1432 bits), 179 bytes captured (1432 bits) on interface wlo1, id 0
▸ Ethernet II, Src: IntelCor_10:7f:f2 (5c:e4:2a:10:7f:f2), Dst: AVMAudio_6e:2d:3a (dc:15:c8:6e:2d:3a)
▸ Internet Protocol Version 4, Src: 192.168.178.50, Dst: 18.66.147.27
▸ Transmission Control Protocol, Src Port: 45904, Dst Port: 443, Seq: 188, Ack: 666, Len: 113
```

Figure: Retransmitted Packets

TCP Conversations Analysis

- TCP conversations reveal the most active network communications between source and destination IPs.
- The predominant use of port **443** (HTTPS) suggests that the captured traffic primarily consists of secure web browsing, API calls, or encrypted application traffic.
- The **most significant traffic exchange** is between **192.168.178.50** and **104.17.144.114**, a Cloudflare-owned IP, likely serving as a content delivery network (CDN) for a website or web servic
- Other notable external connections include a variety of IPs associated with cloud services, likely indicating online browsing, software updates, or API interactions.
- The byte transfer statistics help in understanding which connections are using the most bandwidth, aiding in identifying potential bottlenecks or unusual data usage.



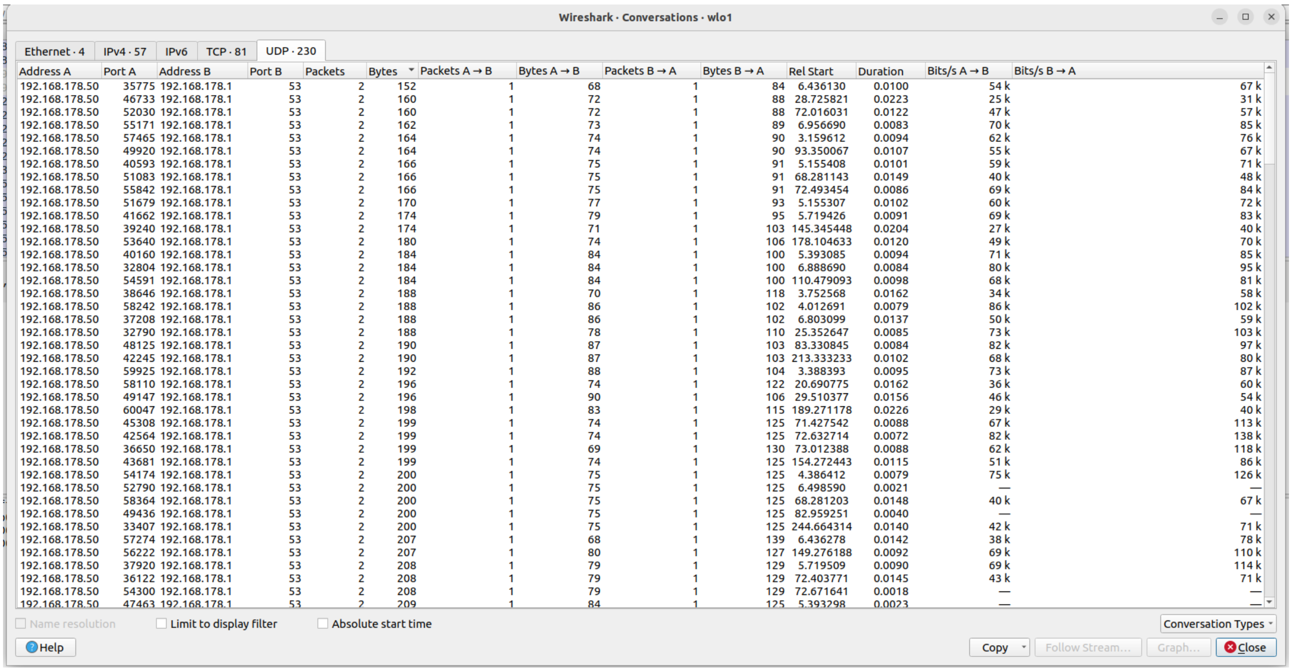
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.178.50	46850	104.17.144.114	443	738	1.106 k	229	19 k	509	1.086 k	122.519956	3.1524	50 k	2.756 k
192.168.178.50	59492	172.64.155.209	443	330	118 k	139	76 k	191	42 k	7.763378	105.4076	5.791	3.228
192.168.178.50	35230	142.250.186.168	443	170	245 k	66	6.944	104	238 k	122.998303	0.3013	184 k	6.339 k
192.168.178.50	37510	216.58.206.78	443	154	159 k	58	8.412	96	150 k	123.074077	0.3085	218 k	3.906 k
192.168.178.50	43412	104.17.145.114	443	124	286 k	56	6.541	68	280 k	122.725169	0.5246	99 k	4.276 k
192.168.178.50	32804	169.150.247.36	443	102	103 k	50	6.057	52	97 k	122.770128	3.2684	14 k	238 k
192.168.178.50	46804	104.21.16.1	443	94	322 k	45	5.607	49	317 k	124.878493	0.1118	401 k	22 M
192.168.178.50	47708	142.250.27.84	443	94	109 k	38	7.294	56	101 k	127.097361	0.2041	285 k	3.994 k
192.168.178.50	44126	104.126.37.184	443	75	41 k	36	3.438	39	37 k	5.091468	117.4351	234	2.576
188.92.44.43	443	192.168.178.50	60892	69	7.155	35	4.911	34	2.244	2.765469	126.9779	309	141
192.168.178.50	59498	172.64.155.209	443	51	20 k	18	15 k	33	5.032	6.150883	86.0283	1.457	467
192.168.178.50	57056	142.250.186.129	443	49	30 k	18	3.823	31	26 k	127.577450	0.2316	132 k	908 k
192.168.178.50	35242	142.250.186.168	443	36	20 k	16	3.848	20	16 k	123.300689	0.0899	342 k	1.473 k
192.168.178.50	56934	18.66.147.124	443	36	9.250	18	4.692	18	4.558	97.951005	0.1233	304 k	295 k
192.168.178.50	52578	142.250.186.106	443	34	17 k	18	4.029	16	13 k	123.424274	0.1542	209 k	721 k
192.168.178.50	47724	142.250.27.84	443	34	13 k	15	3.490	19	10 k	127.248946	0.3437	81 k	237 k
192.168.178.50	57774	104.21.112.1	443	34	11 k	17	4.478	17	7.367	89.268544	0.3885	92 k	151 k
192.168.178.50	43308	18.245.67.101	443	32	34 k	14	3.367	18	31 k	123.004236	0.0891	302 k	2.812 k
192.168.178.50	36156	142.250.186.129	443	31	18 k	16	3.603	15	15 k	123.432375	0.1215	237 k	1.002 k
192.168.178.50	50762	3.233.158.26	443	30	10 k	16	4.923	14	5.362	67.557829	60.4338	651	709
192.168.178.50	50702	216.239.34.157	443	29	10 k	15	3.183	14	7.802	121.317687	0.0700	363 k	891 k
192.168.178.50	50686	216.239.34.157	443	28	10 k	14	3.117	14	7.802	121.258586	0.0745	334 k	838 k
192.168.178.50	58880	169.150.247.37	443	27	13 k	13	3.278	14	9.907	124.115196	0.1132	231 k	699 k
192.168.178.50	45070	216.239.32.36	443	26	13 k	12	5.737	14	7.293	125.122929	0.0817	561 k	714 k
192.168.178.50	32812	169.150.247.36	443	26	12 k	12	3.279	14	8.879	123.309535	0.1143	229 k	621 k
192.168.178.50	56418	199.232.190.202	443	25	9.704	12	3.243	13	6.461	123.234648	0.0622	417 k	830 k
192.168.178.50	47740	142.250.27.84	443	24	11 k	12	3.102	12	8.547	127.806925	0.0820	302 k	833 k
192.168.178.50	60608	54.82.76.84	443	24	8.229	12	3.613	12	4.616	123.176043	0.4423	65 k	83 k
192.168.178.50	38908	34.228.139.242	443	23	8.228	12	3.225	11	5.003	123.467352	0.4496	57 k	89 k
192.168.178.50	53700	173.194.76.156	443	22	11 k	12	3.865	10	7.882	125.128790	0.1165	265 k	541 k
192.168.178.50	38916	34.228.139.242	443	22	7.939	11	2.988	11	4.951	125.703490	0.4520	52 k	87 k
192.168.178.50	50614	18.244.18.38	443	22	5.333	11	3.562	11	1.771	97.862451	0.1153	247 k	122 k
192.168.178.50	57860	3.225.226.118	443	21	8.995	10	3.076	11	5.919	123.569010	0.4468	55 k	105 k
192.168.178.50	57074	142.250.186.129	443	19	12 k	10	2.331	9	9.757	127.577527	0.0468	398 k	1.668 k
192.168.178.50	57068	142.250.186.129	443	17	12 k	9	2.341	8	9.704	127.577494	0.0491	381 k	1.581 k
192.168.178.50	57082	142.250.186.129	443	17	12 k	9	2.301	8	9.704	127.577560	0.0439	419 k	1.770 k
192.168.178.50	37460	34.120.185.22	443	16	3.991	9	2.691	7	1.300	64.131506	60.7593	354	171
192.168.178.50	50010	216.58.212.161	443	15	7.909	8	2.377	7	5.532	122.872920	0.1019	186 k	434 k
192.168.178.50	43294	18.245.67.101	443	14	3.466	7	2.521	7	945	122.753881	1.0644	18 k	7.102
192.168.178.50	37502	216.58.206.78	443	13	8.429	7	2.374	6	6.055	122.833181	0.1076	176 k	450 k
192.168.178.50	39884	142.250.74.194	443	13	7.972	7	2.279	6	5.693	122.888056	0.0977	186 k	466 k

☐ Name resolution ☐ Limit to display filter ☐ Absolute start time

Figure: TCP Conversations

UDP Conversations Analysis

- UDP traffic is mainly centered around port 53, indicating a large number of DNS queries being processed.
- The communication between `192.168.178.50` and `192.168.178.1` suggests that the local router is acting as the DNS resolver for this machine, handling domain name resolution requests.
- The relatively small packet sizes are characteristic of DNS queries and responses, ensuring efficient name resolution.
- A high number of DNS queries suggests that various applications are actively resolving domain names, which can be typical behavior for an internet-connected device.
- Monitoring the frequency and destinations of DNS queries can help detect potential security issues, such as malware performing command-and-control lookups or excessive tracking requests.



Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.178.50	35775	192.168.178.1	53	2	152	1	68	1	84	6.436130	0.0100	54 k	67 k
192.168.178.50	46733	192.168.178.1	53	2	160	1	72	1	88	28.725821	0.0223	25 k	31 k
192.168.178.50	52030	192.168.178.1	53	2	160	1	72	1	88	72.016031	0.0122	47 k	57 k
192.168.178.50	55171	192.168.178.1	53	2	162	1	73	1	89	6.956690	0.0083	70 k	85 k
192.168.178.50	57465	192.168.178.1	53	2	164	1	74	1	90	3.159612	0.0094	62 k	76 k
192.168.178.50	49920	192.168.178.1	53	2	164	1	74	1	90	93.350067	0.0107	55 k	67 k
192.168.178.50	40593	192.168.178.1	53	2	166	1	75	1	91	5.155408	0.0101	59 k	71 k
192.168.178.50	51083	192.168.178.1	53	2	166	1	75	1	91	68.281143	0.0149	40 k	48 k
192.168.178.50	55842	192.168.178.1	53	2	166	1	75	1	91	72.493454	0.0086	69 k	84 k
192.168.178.50	51679	192.168.178.1	53	2	170	1	77	1	93	5.155307	0.0102	60 k	72 k
192.168.178.50	41662	192.168.178.1	53	2	174	1	79	1	95	5.719426	0.0091	69 k	83 k
192.168.178.50	39240	192.168.178.1	53	2	174	1	71	1	103	145.345448	0.0204	27 k	40 k
192.168.178.50	53640	192.168.178.1	53	2	180	1	74	1	106	178.104633	0.0120	49 k	70 k
192.168.178.50	40160	192.168.178.1	53	2	184	1	84	1	100	5.393085	0.0094	71 k	85 k
192.168.178.50	32804	192.168.178.1	53	2	184	1	84	1	100	6.888690	0.0084	80 k	95 k
192.168.178.50	54591	192.168.178.1	53	2	184	1	84	1	100	110.479093	0.0098	68 k	81 k
192.168.178.50	38646	192.168.178.1	53	2	188	1	70	1	118	3.752568	0.0162	34 k	58 k
192.168.178.50	58242	192.168.178.1	53	2	188	1	86	1	102	4.012691	0.0079	86 k	102 k
192.168.178.50	37208	192.168.178.1	53	2	188	1	86	1	102	6.803099	0.0137	50 k	59 k
192.168.178.50	32790	192.168.178.1	53	2	188	1	78	1	110	25.352647	0.0085	73 k	103 k
192.168.178.50	48125	192.168.178.1	53	2	190	1	87	1	103	83.330845	0.0084	82 k	97 k
192.168.178.50	42245	192.168.178.1	53	2	190	1	87	1	103	213.333233	0.0102	68 k	80 k
192.168.178.50	59925	192.168.178.1	53	2	192	1	88	1	104	3.388393	0.0095	73 k	87 k
192.168.178.50	58110	192.168.178.1	53	2	196	1	74	1	122	20.690775	0.0162	36 k	60 k
192.168.178.50	49147	192.168.178.1	53	2	196	1	90	1	106	29.510377	0.0156	46 k	54 k
192.168.178.50	60047	192.168.178.1	53	2	198	1	83	1	115	189.271178	0.0226	29 k	40 k
192.168.178.50	45308	192.168.178.1	53	2	199	1	74	1	125	71.427542	0.0088	67 k	113 k
192.168.178.50	42564	192.168.178.1	53	2	199	1	74	1	125	72.632714	0.0072	82 k	138 k
192.168.178.50	36650	192.168.178.1	53	2	199	1	69	1	130	73.012388	0.0088	62 k	118 k
192.168.178.50	43681	192.168.178.1	53	2	199	1	74	1	125	154.272443	0.0115	51 k	86 k
192.168.178.50	54174	192.168.178.1	53	2	200	1	75	1	125	4.386412	0.0079	75 k	126 k
192.168.178.50	52790	192.168.178.1	53	2	200	1	75	1	125	6.498590	0.0021	—	—
192.168.178.50	58364	192.168.178.1	53	2	200	1	75	1	125	68.281203	0.0148	40 k	67 k
192.168.178.50	49436	192.168.178.1	53	2	200	1	75	1	125	82.959251	0.0040	—	—
192.168.178.50	33407	192.168.178.1	53	2	200	1	75	1	125	244.664314	0.0140	42 k	71 k
192.168.178.50	57274	192.168.178.1	53	2	207	1	68	1	139	6.436278	0.0142	38 k	78 k
192.168.178.50	56222	192.168.178.1	53	2	207	1	80	1	127	149.276188	0.0092	69 k	110 k
192.168.178.50	37920	192.168.178.1	53	2	208	1	79	1	129	5.719509	0.0090	69 k	114 k
192.168.178.50	36122	192.168.178.1	53	2	208	1	79	1	129	72.403771	0.0145	43 k	71 k
192.168.178.50	54300	192.168.178.1	53	2	208	1	79	1	129	72.671641	0.0018	—	—
192.168.178.50	47463	192.168.178.1	53	2	209	1	84	1	125	5.393298	0.0023	—	—

☐ Name resolution ☐ Limit to display filter ☐ Absolute start time

Figure: UDP Conversations

Conclusions and Recommendations

- **TCP Retransmissions:** The high rate of retransmissions on HTTPS traffic suggests potential issues. To mitigate this:
    - Perform a ping test to check for packet loss.
    - Use traceroute to analyze where network delays might be occurring.
    - Verify router and firewall settings to ensure they are not causing packet drops.
- **Frequent HTTP Requests:** The Ubuntu connectivity check is a normal process, but if occurring too frequently, it may indicate an unstable internet connection. Consider checking system settings to adjust the frequency of these requests.
- **High Traffic to Specific IPs:** Connections to `45.57.74.220` and `104.17.144.114` should be verified. If they are associated with cloud services or CDN providers, the traffic is likely legitimate. However, if the purpose of these IPs is unclear, further investigation is advised.
- **DNS Queries Monitoring:** Excessive DNS queries might indicate an application that aggressively resolves domain names or a potential security threat. Monitoring DNS logs and using tools like nslookup or dig can help investigate unusual domain resolution patterns.

By analyzing these network traffic patterns, administrators can optimize performance, detect security threats, and ensure the network is functioning efficiently.