

Wireshark Network Capture Analysis

Executive Summary

This Wireshark capture shows 205 packets over approximately 230 seconds of network activity on a 192.168.1.0/24 subnet. The traffic includes router announcements, ICMP ping tests, DNS resolution, and multicast communications.

Network Topology Identified

- **Router/Gateway:** 192.168.1.1 (MAC: 8c:13:e2:0f:c5:5b, NetlinkIct device)
- **Host :** 192.168.1.5 (PCSSystemtec device, MAC: xx:xx:xx:59:0d:34)
- **DNS Server:** 218.248.112.65
- **External Target:** 142.251.220.110 (Google server)

Detailed Analysis Steps

Step 1: Router Activity (Primary Traffic Pattern)

Packets: 1, 4-11, 14, 29, 34, 39-50, 54-71, 76-94, 98-106, 119-130, 133-153, 157-176, 178-198, 201-204

Pattern: Router broadcasts every ~5 seconds

- **Protocol 0x0ffa frames:** Unknown proprietary protocol (likely router keepalive/status)
- **ARP Announcements:** Router announces its IP every 10 seconds
- **Purpose:** Network presence maintenance and connectivity verification

Step 2: DNS Resolution Sequence

Packets: 19-26 (Time: 22.395-22.439 seconds)

Process:

1. **Query A record:** 192.168.1.5 → DNS server for google.com
2. **Query AAAA record:** 192.168.1.5 → DNS server for google.com (IPv6)
3. **A response:** google.com = 142.251.220.110
4. **AAAA response:** google.com = 2404:6800:4007:82f::200e
5. **Reverse DNS:** PTR query for 142.251.220.110
6. **PTR response:** hkg07s52-in-f14.1e100.net

Step 3: ICMP Ping Test

Packets: 23-24, 27-28, 31-32, 35-36

Sequence:

- Source: 192.168.1.5 → Destination: 142.251.220.110 (Google)
- 4 ping requests with responses

- RTT measurements: ~17-18ms consistently
- All packets successful (TTL: 64 outbound, 117 inbound)

Step 4: ARP Resolution

Packets: 37-38 (Time: 27.509-27.511 seconds)

Process:

1. **ARP Request:** "Who has 192.168.1.1? Tell 192.168.1.5"
2. **ARP Reply:** "192.168.1.1 is at 8c:13:e2:0f:c5:5b"

Step 5: IGMP Multicast Management

Regular IGMP Queries: Packets 12, 51, 73, 96, 131, 154, 177, 199

- Router sends membership queries every 30 seconds
- Destination: 224.0.0.1 (All Systems multicast)

IGMP Reports: Various packets from 192.168.1.3

- Joins multicast groups:
 - 224.0.0.251 (mDNS)
 - 224.0.0.252 (Link-Local Multicast Name Resolution)
 - 239.255.255.250 (UPnP)
 - 239.255.102.18 (Unknown application-specific)

Step 6: mDNS Service Discovery

Packets: 107-118 (Time: 117.309-118.071 seconds)

Activity:

- computer announces "_dosvc._tcp.local" service
- Service runs on port 7680
- Both IPv4 and IPv6 announcements
- Cache flush operations for service updates

Key Observations

Traffic Volume Analysis

- **Router broadcasts:** ~70% of total traffic
- **Multicast/IGMP:** ~15% of traffic
- **Application traffic:** ~15% (DNS, ICMP, mDNS)

Security Considerations

- No encrypted traffic observed

- Clear text DNS queries
- Router using unknown protocol (0xffff)
- Multiple multicast groups active

Performance Metrics

- **Ping latency:** Consistent 17-18ms to Google
- **DNS resolution:** Sub-50ms response times
- **Network stability:** Regular router announcements indicate stable infrastructure

Protocol Distribution

- **Unknown (0xffff):** 135 packets (66%)
- **ARP:** 26 packets (13%)
- **IGMP:** 21 packets (10%)
- **ICMP:** 8 packets (4%)
- **DNS:** 8 packets (4%)
- **mDNS:** 12 packets (6%)

Recommendations

1. **Monitor unknown protocol:** Investigate 0xffff protocol purpose
2. **DNS security:** Consider DNS over HTTPS/TLS implementation
3. **Multicast optimization:** Review necessary multicast groups
4. **Traffic analysis:** Set up continuous monitoring for baseline establishment

The image displays a Wireshark packet capture analysis of a TCP connection. The packet list shows a sequence of packets including application data, SYN, ACK, and TLS handshake messages. The packet details pane shows the structure of a TLS Client Hello message. The packet bytes pane shows the raw hex and ASCII data.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|--|
| 112 | 0.995973 | 20.195.84.16 | 192.168.1.3 | TLSv1.2 | 158 | Application Data |
| 113 | 1.040349 | 192.168.1.3 | 20.195.84.16 | TCP | 54 | 15793 → 443 [ACK] Seq=1 Ack=105 Win=253 Len=0 |
| 114 | 1.554059 | 192.168.1.3 | 172.64.155.209 | TCP | 55 | 15844 → 443 [ACK] Seq=1 Ack=1 Win=250 Len=1 |
| 115 | 1.568572 | 172.64.155.209 | 192.168.1.3 | TCP | 66 | 443 → 15844 [ACK] Seq=1 Ack=2 Win=16 Len=0 SLE=1 SRE=2 |
| 119 | 3.093667 | 192.168.1.3 | 20.195.84.16 | TLSv1.2 | 82 | Application Data |
| 121 | 3.142816 | 20.195.84.16 | 192.168.1.3 | TCP | 60 | 443 → 15793 [ACK] Seq=105 Ack=29 Win=501 Len=0 |
| 123 | 4.456737 | 142.250.67.42 | 192.168.1.3 | TLSv1.2 | 139 | Application Data |
| 124 | 4.504356 | 192.168.1.3 | 142.250.67.42 | TCP | 54 | 15839 → 443 [ACK] Seq=1 Ack=86 Win=255 Len=0 |
| 129 | 6.312551 | 192.168.1.3 | 20.44.239.154 | TCP | 66 | 16007 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM |
| 130 | 6.362573 | 20.44.239.154 | 192.168.1.3 | TCP | 66 | 443 → 16007 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM |
| 131 | 6.362859 | 192.168.1.3 | 20.44.239.154 | TCP | 54 | 16007 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0 |
| 132 | 6.368733 | 192.168.1.3 | 20.44.239.154 | TLSv1.2 | 268 | Client Hello (SNL=settings-win.data.microsoft.com) |
| 133 | 6.418965 | 20.44.239.154 | 192.168.1.3 | TCP | 1506 | 443 → 16007 [ACK] Seq=1 Ack=215 Win=4194560 Len=1452 [TCP PDU reassembled in 135] |
| 134 | 6.418965 | 20.44.239.154 | 192.168.1.3 | TCP | 1506 | 443 → 16007 [ACK] Seq=1453 Ack=215 Win=4194560 Len=1452 [TCP PDU reassembled in 135] |
| 135 | 6.419319 | 20.44.239.154 | 192.168.1.3 | TLSv1.2 | 908 | Server Hello, Certificate, Server Key Exchange, Server Hello Done |
| 136 | 6.419742 | 192.168.1.3 | 20.44.239.154 | TCP | 54 | 16007 → 443 [ACK] Seq=215 Ack=3759 Win=65280 Len=0 |
| 137 | 6.452265 | 20.195.84.16 | 192.168.1.3 | TLSv1.2 | 81 | Application Data |
| 138 | 6.460005 | 192.168.1.3 | 20.44.239.154 | TLSv1.2 | 212 | Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message |
| 139 | 6.499517 | 192.168.1.3 | 20.195.84.16 | TCP | 54 | 15793 → 443 [ACK] Seq=29 Ack=132 Win=253 Len=0 |

Frame 112: 158 bytes on wire (1264 bits), 158 bytes captured (1264 bits) on interface \Device\NPF_{5A18...} Ethernet II, Src: NetlinkTct_0fc5:5b (8c:13:e2:0f:c5:5b), Dst: RealtekSemic_36:0b:20 (00:e0:14:c3:36:0b:20) Internet Protocol Version 4, Src: 20.195.84.16, Dst: 192.168.1.3 Transmission Control Protocol, Src Port: 443, Dst Port: 15793, Seq: 1, Ack: 1, Len: 104 Transport Layer Security

0000 00 e0 4c 36 0b 20 8c 13 e2 0f c5 5b 08 00 45 00 ...L6.....[:E:..
0010 00 90 38 c7 40 00 30 06 a7 22 14 c3 54 10 c0 a8 ...8@0..".T...
0020 01 03 01 bb 3d b1 0f e1 59 90 a1 29 d0 a5 50 18Y...[:P..
0030 01 f5 84 48 00 00 17 03 03 00 63 4a 8b 17 43 55 ...H.....[:CU..
0040 69 65 3a 20 9d 6f 22 b5 45 7c 25 3b b5 46 bc f4 ...o"o"[:F%:F..
0050 49 70 64 09 19 0b 54 88 2f d9 87 34 72 59 21 99 ...Ipd...T /-drV..
0060 d4 d0 d5 60 83 ca 6b 50 0c 75 d6 48 7b 30 cb e6 ...-..kP..u.H(..
0070 e8 45 22 39 57 57 61 dd 09 93 3c d0 b4 e4 1c 81 ...E"9Wah...<....
0080 49 00 a3 2d fd 5b a6 86 6f 1a 2a ed c3 20 4f d5 ...I...[:o:*...O..
0090 f2 d0 a5 3d 83 85 c8 6b dd d3 9b 08 b9 9dk.....

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|-------------|-----------------|----------|--------|--|
| 648 | 48.350738 | 192.168.1.3 | 218.248.112.65 | ICMP | 152 | Destination unreachable (Port unreachable) |
| 651 | 49.618464 | 192.168.1.3 | 218.248.112.165 | ICMP | 194 | Destination unreachable (Port unreachable) |
| 796 | 50.316231 | 192.168.1.3 | 218.248.112.165 | ICMP | 240 | Destination unreachable (Port unreachable) |

> Frame 648: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits) on interface \Device\NPF_{5A18F...}

> Ethernet II, Src: RealtekSemic_36:0b:20 (00:e0:4c:36:0b:20), Dst: NetlinkKic_0f:c5:5b (8c:13:e2:0f:c5:5b)

> Internet Protocol Version 4, Src: 192.168.1.3, Dst: 218.248.112.65

> Internet Control Message Protocol

0000 8c 13 e2 0f c5 5b 00 e0 4c 36 0b 20 08 00 45 00 ...[...L6...E-...

0010 00 8a 6b 07 00 00 80 01 00 00 c0 a8 01 03 da f8 ...k...

0020 70 41 03 03 0a 4e 00 00 00 45 00 00 6e 0c 07 ...pA...N... ..E...

0030 40 00 fb 11 66 92 da f8 70 41 c0 a8 01 03 00 35 ...@...f... ..pA... ..S...

0040 e4 96 00 5a db 59 e1 81 80 00 01 00 03 00 00 ...-Z...Y...

0050 00 00 03 77 77 77 08 7a 65 6e 61 72 6d 6f 72 03 ...www...z... ..enarmon...

0060 63 6f 6d 00 00 01 00 01 c0 0c 00 01 00 01 00 00 ...com...

0070 01 2c 00 04 ac 43 45 3e c0 0c 00 01 00 01 00 00 ...p... ..CE>

0080 01 2c 00 04 68 1a 08 94 c0 0c 00 01 00 01 00 00 ...p...

0090 01 2c 00 04 68 1a 09 94 ...p...

Internet Control Message Protocol: Protocol

Packets: 5758 - Displayed: 3 (0.1%)

Profile: Default

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|-------------------------------|-----------------|----------|--------|--|
| 101 | 0.197319 | 172.217.194.84 | 192.168.1.3 | QUIC | 1288 | Protected Payload (KP0) |
| 102 | 0.197319 | 172.217.194.84 | 192.168.1.3 | QUIC | 415 | Protected Payload (KP0) |
| 103 | 0.197319 | 172.217.194.84 | 192.168.1.3 | QUIC | 76 | Protected Payload (KP0) |
| 104 | 0.197319 | 172.217.194.84 | 192.168.1.3 | QUIC | 65 | Protected Payload (KP0) |
| 105 | 0.197989 | 192.168.1.3 | 172.217.194.84 | QUIC | 77 | Protected Payload (KP0), DCID=ea958e17e307c070 |
| 106 | 0.198251 | 192.168.1.3 | 172.217.194.84 | QUIC | 73 | Protected Payload (KP0), DCID=ea958e17e307c070 |
| 107 | 0.200260 | 142.251.221.174 | 192.168.1.3 | QUIC | 666 | Protected Payload (KP0) |
| 108 | 0.203004 | 142.251.221.174 | 192.168.1.3 | QUIC | 308 | Protected Payload (KP0) |
| 109 | 0.203383 | 192.168.1.3 | 142.251.221.174 | QUIC | 79 | Protected Payload (KP0), DCID=e33abac826f710f5 |
| 110 | 0.217824 | 142.251.221.174 | 192.168.1.3 | QUIC | 65 | Protected Payload (KP0) |
| 111 | 0.269052 | 172.217.194.84 | 192.168.1.3 | QUIC | 66 | Protected Payload (KP0) |
| 127 | 6.298653 | 192.168.1.3 | 218.248.112.165 | DNS | 91 | Standard query 0x1fe3 A settings-win.data.microsoft.com |
| 128 | 6.305848 | 218.248.112.165 | 192.168.1.3 | DNS | 227 | Standard query response 0x1fe3 A settings-win.data.microsoft.com CNAME atm-settingsfe-prod-geo2.trafficmanager.net CNAME settingsfe-prod-geo2.trafficmanager.net |
| 173 | 14.620214 | 192.168.1.4 | 224.0.0.251 | MDNS | 567 | Standard query response 0x0000 PTR, cache flush Android.local PTR, cache flush Android.local TXT, cache flush PTR_mi-connect_uci |
| 174 | 14.620214 | fe80::e4d5:2eff:fe3::ff02::fb | ff02::fb | MDNS | 587 | Standard query response 0x0000 PTR, cache flush Android.local PTR, cache flush Android.local TXT, cache flush PTR_mi-connect_uci |
| 209 | 24.302479 | 192.168.1.3 | 218.248.112.65 | DNS | 77 | Standard query 0xfafa A edgeapi.slack.com |
| 210 | 24.303246 | 192.168.1.3 | 218.248.112.65 | DNS | 77 | Standard query 0x0b9e HTTPS edgeapi.slack.com |
| 214 | 24.315659 | 218.248.112.65 | 192.168.1.3 | DNS | 109 | Standard query response 0xfafa A edgeapi.slack.com A 65.1.97.76 A 13.235.226.255 |
| 215 | 24.315659 | 218.248.112.65 | 192.168.1.3 | DNS | 142 | Standard query response 0x0b9e HTTPS edgeapi.slack.com SOA dns1.p01.nsonline.net |

> Frame 111: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{5A18F...}

> Ethernet II, Src: NetlinkKic_0f:c5:5b (8c:13:e2:0f:c5:5b), Dst: RealtekSemic_36:0b:20 (00:e0:4c:36:0b:20)

> Internet Protocol Version 4, Src: 172.217.194.84, Dst: 192.168.1.3

> User Datagram Protocol, Src Port: 443, Dst Port: 55378

> QUIC IETF

0000 00 e0 4c 36 0b 20 8c 13 e2 0f c5 5b 00 00 45 00 ...L6... ..[...E-...

0010 00 34 00 00 00 00 3b 11 0e 60 ac d9 c2 54 c0 a8 ...4...@... ..T...

0020 01 03 01 bb d8 52 00 20 eb bd 57 6e 96 55 c1 dc ...-...R... ..W... ..U...

0030 b2 d4 8f 5d 54 a9 a4 7f d2 68 82 3d a1 e4 f3 60 ...-...T... ..h...

0040 34 21 ...4!...

User Datagram Protocol: Protocol

Packets: 5758 - Displayed: 1728 (30.0%)

Profile: Default