

```
manc2957@engs-labb27: ~  
pi@p4pi: ~  
manc2957@engs-labb27: ~  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: enp0s31f6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 50:9a:4c:02:e3:76 brd ff:ff:ff:ff:ff:ff  
    inet 10.200.17.160/22 brd 10.200.19.255 scope global dynamic noprefixroute enp0s31f6  
        valid_lft 688489sec preferred_lft 688489sec  
    inet6 fe80::4656:31:66aa:201d/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
5: enx0c37965f8a0b: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 0c:37:96:5f:8a:0b brd ff:ff:ff:ff:ff:ff  
    inet 192.168.10.1/24 brd 192.168.10.255 scope global noprefixroute enx0c37965f8a0b  
        valid_lft forever preferred_lft forever  
    inet6 fe80::b475:c20d:d0fc:7a85/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
manc2957@engs-labb27:~$
```

Local machine name is enx0c37965f8a0b.

Capturing from enx0c37965f8a0b							
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help							
Apply a display filter ... <Ctrl-/>							
No.	Time	Source	Destination	Protocol	Length	Info	
38	58.242901292	192.168.10.1	224.0.0.251	MDNS	261	Standard query	0x0000 ANY
39	58.493685028	fe80::b475:c20d:d0f...	ff02::fb	MDNS	224	Standard query	0x0000 ANY
40	58.493990694	192.168.10.1	224.0.0.251	MDNS	261	Standard query	0x0000 ANY
41	58.693853647	192.168.10.1	224.0.0.251	MDNS	243	Standard query response	0:
42	58.694042104	fe80::b475:c20d:d0f...	ff02::fb	MDNS	212	Standard query response	0:
43	59.698912521	192.168.10.1	224.0.0.251	MDNS	243	Standard query response	0:
44	59.699071692	fe80::b475:c20d:d0f...	ff02::fb	MDNS	212	Standard query response	0:
45	61.703174567	192.168.10.1	224.0.0.251	MDNS	243	Standard query response	0:
46	61.703327855	fe80::b475:c20d:d0f...	ff02::fb	MDNS	212	Standard query response	0:
<p>Frame 1: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits) on interface enx0c37965f8a0b, id</p> <p>Ethernet II, Src: BizlinkT_5f:8a:0b (0c:37:96:5f:8a:0b), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)</p> <p>Internet Protocol Version 4, Src: 192.168.10.1, Dst: 224.0.0.251</p> <p>User Datagram Protocol, Src Port: 5353, Dst Port: 5353</p> <p>Multicast Domain Name System (response)</p>							
0000	01 00 5e 00 00 fb 0c 37 96 5f 8a 0b 08 00 45 00	..A....7...E.					
0010	00 e5 52 81 40 00 ff 11 7c e1 c0 a8 0a 01 e0 00	..R.@...					
0020	00 fb 14 e9 14 e9 00 d1 ac 87 00 00 84 00 00 005.8.a.7.c					
0030	00 04 00 00 00 00 01 35 01 38 01 61 01 37 01 63	.f.0.d.d.0.2.c.5					
0040	01 66 01 30 01 64 01 64 01 30 01 32 01 63 01 35	.7.4.b.0.0.0.0.0					
0050	01 37 01 34 01 62 01 30 01 30 01 30 01 30 01 30	.0.0.0.0.0.0.0.0					
0060	01 30 01 30 01 30 01 30 01 30 01 30 01 30 01 30	.8.e.f.i.p6.arpa.					
0070	01 38 01 65 01 66 03 69 70 36 04 61 72 70 61 00x...engs-					
0080	00 0c 80 01 00 00 00 78 00 1a 12 65 6e 67 73 2d	labb27-1 27555.lo					
0090	6c 61 62 62 32 37 2d 31 32 37 35 35 35 05 6c 6f	cal...x..					
00a0	63 61 6c 00 c0 60 00 01 80 01 00 00 00 78 00 041.1 0.168.19					
00b0	c0 a8 0a 01 01 31 02 31 30 03 31 36 38 03 31 39						

Packets are being captured.

Not quite sure what they are for. It seems to be some form of standard query for small stand alone networks under the multicast DNS protocol.

Packets are quite small (around 2000 bits). Contains the name of my local machine (engs-labb27)

*enp0s31f6						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
648	16.503080763	10.200.16.26	224.0.0.251	MDNS	82	Standard query 0x0000
649	16.503248018	fe80::b0ab:a136:b77...	ff02::fb	MDNS	102	Standard query 0x0000
650	16.521097909	10.200.17.147	224.0.0.251	MDNS	143	Standard query 0x0000
651	16.529145973	10.200.16.205	255.255.255.255	UDP	65	49779 → 35891 Len=23
652	16.533428051	10.200.16.26	224.0.0.251	MDNS	82	Standard query 0x0000
653	16.533493539	fe80::b0ab:a136:b77...	ff02::fb	MDNS	102	Standard query 0x0000
654	16.534244701	10.200.16.26	224.0.0.251	MDNS	82	Standard query 0x0000
655	16.534384613	fe80::b0ab:a136:b77...	ff02::fb	MDNS	102	Standard query 0x0000
656	16.612514722	10.200.17.10	255.255.255.255	UDP	259	25536 → 25536 Len=217
657	16.632659602	10.200.16.26	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
▶ Frame 644: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface enp0s31f6, id 0						
▶ Ethernet II, Src: Dell_25:34:e6 (d8:d0:90:25:34:e6), Dst: IPv6mcast_fb (33:33:00:00:00:fb)						
▶ Internet Protocol Version 6, Src: fe80::b0ab:a136:b776:e1d5, Dst: ff02::fb						
▶ User Datagram Protocol, Src Port: 5353, Dst Port: 5353						
▶ Multicast Domain Name System (query)						
0000	33 33 00 00 00 fb d8 d0	90 25 34 e6 86 dd 60 03	33.....%4..`.			
0010	e8 d0 00 30 11 01 fe 80	00 00 00 00 00 00 b0 ab	...0.....			
0020	a1 36 b7 76 e1 d5 ff 02	00 00 00 00 00 00 00 00	.6.v.....			
0030	00 00 00 00 00 00 fb 14 e9	14 e9 00 30 a1 f6 00 00:0....			
0040	00 00 00 01 00 00 00 00	00 00 0b 5f 67 6f 6f 67_goog			
0050	6c 65 63 61 73 74 04 5f	74 63 70 05 6c 6f 63 61	lecast_ tcp loca			
0060	6c 00 00 0c 00 01		l.....			
wireshark enp0s31f6_2...3111743_FPjhlpcapng Packets: 677 · Displayed: 677 (100.0%) · Dropped: 0 (0.0%) Profile: Default						

We see a lot more packets being sent within the network.

*enp0s31f6

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
1729	31.645991424	185.125.190.18	10.200.17.160	HTTP	66	HTTP/1.0 400 Bad request
5173	82.944631721	10.200.17.160	35.232.111.17	HTTP	153	GET / HTTP/1.1
5185	83.041879571	35.232.111.17	10.200.17.160	HTTP	214	HTTP/1.1 204 No Content
19964	316.842259199	10.200.17.160	216.58.213.3	OCSP	507	Request
19982	317.056450818	216.58.213.3	10.200.17.160	OCSP	780	Response
20380	320.771611409	10.200.17.160	18.165.196.217	OCSP	499	Request
20390	320.918565936	18.165.196.217	10.200.17.160	OCSP	1071	Response
20579	322.233479268	10.200.17.160	96.17.179.201	OCSP	489	Request
20582	322.238432592	96.17.179.201	10.200.17.160	OCSP	954	Response
25430	402.933685515	10.200.17.160	35.232.111.17	HTTP	153	GET / HTTP/1.1

Frame 5185: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface enp0s31f6, id 0

Ethernet II, Src: Cisco_a2:1a:f1 (00:9a:d2:a2:1a:f1), Dst: Dell_02:e3:76 (50:9a:4c:02:e3:76)

Internet Protocol Version 4, Src: 35.232.111.17, Dst: 10.200.17.160

Transmission Control Protocol, Src Port: 80, Dst Port: 47728, Seq: 1, Ack: 88, Len: 148

Hypertext Transfer Protocol

```

0000  50 9a 4c 02 e3 76 00 9a d2 a2 1a f1 08 00 45 60  P.L.v. ....E`
0010  00 c8 a6 1c 40 00 35 06 ef 52 23 e8 6f 11 0a c8  ...@.5. R#.o...
0020  11 a0 00 50 ba 70 f5 25 c2 d9 5d 07 89 90 80 18  ...P.p.% ..]....
0030  01 f6 0c b7 00 00 01 01 08 0a 8a de a0 ae a0 2a  .....*
0040  14 f3 48 54 54 50 2f 31 2e 31 20 32 30 34 20 4e  ..HTTP/1 .1 204 N
0050  6f 20 43 6f 6e 74 65 6e 74 0d 0a 44 61 74 65 3a  o Content t..Date:
0060  20 4d 6f 6e 2c 20 31 33 20 4a 75 6e 20 32 30 32  Mon, 13 Jun 202
0070  32 20 31 30 3a 32 35 3a 35 33 20 47 4d 54 0d 0a  2 10:25: 53 GMT..
0080  53 65 72 76 65 72 3a 20 41 70 61 63 68 65 2f 32  Server: Apache/2
0090  2e 34 2e 31 38 20 28 55 62 75 6e 74 75 29 0d 0a  .4.18 (U buntu)..
00a0  58 2d 4e 65 74 77 6f 72 6b 4d 61 6e 61 67 65 72  X-Networ kManager
00b0  2d 53 74 61 74 75 73 3a 20 6f 6e 6c 69 6e 65 0d  -Status: online.

```

Hypertext Transfer Protocol: Protocol Packets: 29777 · Displayed: 12 (0.0%) Profile: Default

We can apply a display filter to only view the http packages. This will give us the packets sent by HTTP.


```
manc2957@engs-labb27: ~/CWM-ProgNets/assignment1
pi@p4pi: ~/daoxin/CWM-ProgNets/assignment1 x manc2957@engs-labb27: ~/CWM-ProgNets/assign... x
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 100 packets in total
manc2957@engs-labb27:~/CWM-ProgNets/assignment1$ python3 send.py 100 enx0c37965f8a0b 192.168.10.1 192
.168.10.2
```

We can run `python3 send.py 100 enx0c37965f8a0b 192.168.10.1 192.168.10.2` to our custom packets to the Raspberry PI.

Capturing from enx0c37965f8a0b

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
82	100.981473886	fe80::b475:c20d:d0f...	ff02::fb	MDNS	212	Standard query response 0
83	101.331689861	192.168.10.1	192.168.10.2	ADwin ...	64	
84	101.392094865	192.168.10.1	192.168.10.2	ADwin ...	64	
85	101.464688546	192.168.10.1	192.168.10.2	ADwin ...	64	
86	101.532802365	192.168.10.1	192.168.10.2	ADwin ...	64	
87	101.592808528	192.168.10.1	192.168.10.2	ADwin ...	64	
88	101.676661619	192.168.10.1	192.168.10.2	ADwin ...	64	
89	101.736514524	192.168.10.1	192.168.10.2	ADwin ...	64	
90	101.800810290	192.168.10.1	192.168.10.2	ADwin ...	64	
91	101.860638349	192.168.10.1	192.168.10.2	ADwin ...	64	
92	101.948575204	192.168.10.1	192.168.10.2	ADwin ...	64	
93	102.176083343	192.168.10.1	224.0.0.251	MDNS	243	Standard query response 0
94	102.176326843	fe80::b475:c20d:d0f...	ff02::fb	MDNS	212	Standard query response 0
95	104.370354144	192.168.10.1	224.0.0.251	MDNS	243	Standard query response 0

Frame 83: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface enx0c37965f8a0b, id 0

- Ethernet II, Src: 00:00:00_00:00:02 (00:00:00:00:00:02), Dst: 00:00:00_00:00:01 (00:00:00:00:00:01)
- Internet Protocol Version 4, Src: 192.168.10.1, Dst: 192.168.10.2
- User Datagram Protocol, Src Port: 50000, Dst Port: 1024
- ADwin configuration protocol

```

0000  00 00 00 00 00 01 00 00 00 00 02 08 00 45 00  ....E.
0010  00 32 00 01 00 00 40 11 e5 66 c0 a8 0a 01 c0 a8  .2...@.f.....
0020  0a 02 c3 50 04 00 00 1e 26 59 64 66 63 70 62 6f  ...P...&Ydfcpbo
0030  6d 6a 6f 76 6b 6c 62 69 68 68 66 72 6f 63 69 79  mjovklbi hhfrocly

```

Frame (frame), 64 bytes Packets: 110 - Displayed: 110 (100.0%) Profile: Default

We do see these packages in Wireshark.

Capturing from enx0c37965f8a0b						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
2117	639.562508618	192.168.10.2	192.168.10.1	SSH	118	Server: Encrypted packet
2118	639.562509002	192.168.10.2	192.168.10.1	SSH	102	Server: Encrypted packet
2119	639.562679565	192.168.10.1	192.168.10.2	TCP	66	46900 → 22 [ACK] Seq=1085
2120	639.616152949	192.168.10.2	192.168.10.1	ADwin ...	64	
2121	639.616153251	192.168.10.2	192.168.10.1	SSH	102	Server: Encrypted packet
2122	639.616318986	192.168.10.1	192.168.10.2	TCP	66	46900 → 22 [ACK] Seq=1085
2123	639.626515727	192.168.10.2	192.168.10.1	SSH	118	Server: Encrypted packet
2124	639.626516157	192.168.10.2	192.168.10.1	SSH	102	Server: Encrypted packet
2125	639.626685017	192.168.10.1	192.168.10.2	TCP	66	46900 → 22 [ACK] Seq=1085
2126	639.668689085	192.168.10.2	192.168.10.1	ADwin ...	64	
2127	639.668739316	192.168.10.2	192.168.10.1	SSH	102	Server: Encrypted packet
2128	639.668889619	192.168.10.1	192.168.10.2	TCP	66	46900 → 22 [ACK] Seq=1085
2129	639.679047434	192.168.10.2	192.168.10.1	SSH	118	Server: Encrypted packet
2130	639.679047870	192.168.10.2	192.168.10.1	SSH	102	Server: Encrypted packet
2131	639.679202770	192.168.10.1	192.168.10.2	TCP	66	46900 → 22 [ACK] Seq=1085
2132	639.719997404	192.168.10.2	192.168.10.1	ADwin ...	64	
2133	639.720193396	192.168.10.2	192.168.10.1	SSH	102	Server: Encrypted packet
2134	639.720352837	192.168.10.1	192.168.10.2	TCP	66	46900 → 22 [ACK] Seq=1085
2135	639.730510331	192.168.10.2	192.168.10.1	SSH	118	Server: Encrypted packet
2136	639.730510940	192.168.10.2	192.168.10.1	SSH	102	Server: Encrypted packet
2137	639.730635226	192.168.10.1	192.168.10.2	TCP	66	46900 → 22 [ACK] Seq=1085
2138	639.771991115	192.168.10.2	192.168.10.1	ADwin ...	64	
Frame 83: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface enx0c37965f8a0b, id 0						
0000	00 00 00	00 00 01 00 00	00 00 00 02 08 00 45 00E.	
0010	00 32 00	01 00 00 40 11	e5 66 c0 a8 0a 01 c0 a8	2.....@. .f.....		
0020	0a 02 c3	50 04 00 00 1e	26 59 64 66 63 70 62 6f	...P....&Ydfcpbo		
0030	6d 6a 6f	76 6b 6c 62 69	68 68 66 72 6f 63 69 79	mjovklbi hhfrociy		
Frame (frame), 64 bytes						
Packets: 2299 · Displayed: 2299 (100.0%) Profile: Default						

The packets that are being sent across in a format known as Adwin. Each packet has a size of 64 bits.

Window title: *enx0c37965f8a0b

Menu: File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Toolbar: [Icons for various network analysis functions]

Filter: !mdns and !tcp

No.	Time	Source	Destination	Protocol	Length	Info
43	50.901982854	192.168.10.2	192.168.10.1	ADwin ...	64	
44	50.953273452	192.168.10.2	192.168.10.1	ADwin ...	64	
45	51.013344864	192.168.10.2	192.168.10.1	ADwin ...	64	
46	51.065405765	192.168.10.2	192.168.10.1	ADwin ...	64	
47	51.117413924	192.168.10.2	192.168.10.1	ADwin ...	64	

Packet details for selected packet (No. 47):

- Total Length: 50
- Identification: 0x0001 (1)
- Flags: 0x0000
- Fragment offset: 0
- Time to live: 64
- Protocol: UDP (17)
- Header checksum: 0xe566 [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.10.2
- Destination: 192.168.10.1
- User Datagram Protocol, Src Port: 50000, Dst Port: 1024
 - Source Port: 50000
 - Destination Port: 1024
 - Length: 30
 - Checksum: 0x025b [unverified]
 - [Checksum Status: Unverified]
 - [Stream index: 2]
 - [Timestamps]
- ADwin configuration protocol

Hex dump:

```

0000  00 00 00 00 01 00 00 00 00 02 08 00 45 00  .....E.
0010  00 32 00 01 00 00 40 11 e5 66 c0 a8 0a 02 c0 a8  .2...@.f....
0020  0a 01 c3 50 04 00 00 1e 02 5b 70 76 62 70 70 69  .P....[pvbppi
0030  61 68 72 6a 6c 7a 77 6e 63 77 65 6a 72 63 6a 61  ahrjIzwn cwejrca

```

Status bar: User Datagram Protocol (udp), 8 bytes | Packets: 171 · Displayed: 5 (2.9%) | Profile: Default

We see that the Package is sent by UDP protocol on port 50000. We can filter out the MDNS packets with a display filter.

```
Open  send.py  Save  ~ /CWM-ProgNets/assignment1

1 #!/usr/bin/python
2
3 from scapy.all import Ether, IP, sendp, get_if_hwaddr, get_if_list, TCP, Raw, UDP
4 import sys
5 import random, string
6
7
8 def randomword(max_length):
9     length = random.randint(22, max_length)
10    return ''.join(random.choice(string.ascii_lowercase) for i in range(int(length)))
11
12 def send_random_traffic(num_packets, interface, src_ip, dst_ip):
13     dst_mac = "00:00:00:00:00:01"
14     src_mac = "00:00:00:00:00:02"
15     total_pkts = 0
16     port = 1024
17     for i in range(num_packets):
18         data = randomword(22)
19         p = Ether(dst=dst_mac,src=src_mac)/IP(dst=dst_ip,src=src_ip)
20         p = p/TCP(sport=5555, dport=port)/Raw(load=data)
21         sendp(p, iface = interface, inter = 0.01)
22         total_pkts += 1
23     print ("Sent %s packets in total" % total_pkts)
24
25 if __name__ == '__main__':
26     if len(sys.argv) < 5:
27         print("Usage: python send.py packet_num interface src_ip dst_ip")
28         sys.exit(1)
29     else:
30         num_packets = sys.argv[1]
31         interface = sys.argv[2]
32         src_ip = sys.argv[3]
33         dst_ip = sys.argv[4]
34         send_random_traffic(int(num_packets), interface, src_ip, dst_ip)
```

Python Tab Width: 8 Ln 20, Col 22 INS

We now send the packets via TCP protocol on port 5555.

Wireshark interface showing a packet capture on the interface `enx0c37965f8a0b`. The filter is `!mdns`.

No.	Time	Source	Destination	Protocol	Length	Info
15	8.019542839	192.168.10.2	192.168.10.1	TCP	76	5555 → 1024 [SYN] Seq=0 Win
16	8.067001758	192.168.10.2	192.168.10.1	TCP	76	[TCP Retransmission] 5555
17	8.118949233	192.168.10.2	192.168.10.1	TCP	76	[TCP Retransmission] 5555
18	8.174948565	192.168.10.2	192.168.10.1	TCP	76	[TCP Retransmission] 5555
19	8.234890562	192.168.10.2	192.168.10.1	TCP	76	[TCP Retransmission] 5555

Selected packet details (Packet 15):

- Transmission Control Protocol, Src Port: 5555, Dst Port: 1024, Seq: 0, Len: 22
- Source Port: 5555
- Destination Port: 1024
- [Stream index: 0]
- [TCP Segment Len: 22]
- Sequence number: 0 (relative sequence number)
- Sequence number (raw): 0
- [Next sequence number: 23 (relative sequence number)]
- Acknowledgment number: 0
- Acknowledgment number (raw): 0
- 0101 = Header Length: 20 bytes (5)
- Flags: 0x002 (SYN)
- Window size value: 8192
- [Calculated window size: 8192]
- Checksum: 0x263b [unverified]
- [Checksum Status: Unverified]
- Urgent pointer: 0
- [SEQ/ACK analysis]
- [Timestamps]

Packet bytes (hex and ASCII):

```

0000  00 00 00 00 00 01 00 00 00 00 00 02 08 00 45 00  .....E.
0010  00 3e 00 01 00 00 40 06 e5 65 c0 a8 0a 02 c0 a8  .>...@.e...
0020  0a 01 15 b3 04 00 00 00 00 00 00 00 00 00 50 02  .....P.
0030  20 00 26 3b 00 00 65 63 6b 70 75 72 64 68 77 6a  .&;.ec kpurdhwj
0040  79 61 63 62 74 79 73 62 68 70 6b 61              yacbtysb hpka

```

Summary: Multicast Domain Name System: Protocol. Packets: 375 · Displayed: 5 (1.3%) · Profile: Default

We do see the packets on Wireshark.