CAPTURE DNS TRAFFIC

```
┌──(kali㉿kali)-[~]
└─$ nslookup
> www.cisco.com
Server:         192.168.50.1
Address:        192.168.50.1#53

Non-authoritative answer:
www.cisco.com   canonical name = www.cisco.com.akadns.net.
www.cisco.com.akadns.net        canonical name = wwwds.cisco.com.edgekey.net.
wwwds.cisco.com.edgekey.net     canonical name = wwwds.cisco.com.edgekey.net.globalredir.akadns.net.
wwwds.cisco.com.edgekey.net.globalredir.akadns.net      canonical name = e2867.dsca.akamaiedge.net.
Name:   e2867.dsca.akamaiedge.net
Address: 23.51.50.61
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:df:6b3::b33
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:df:692::b33
```

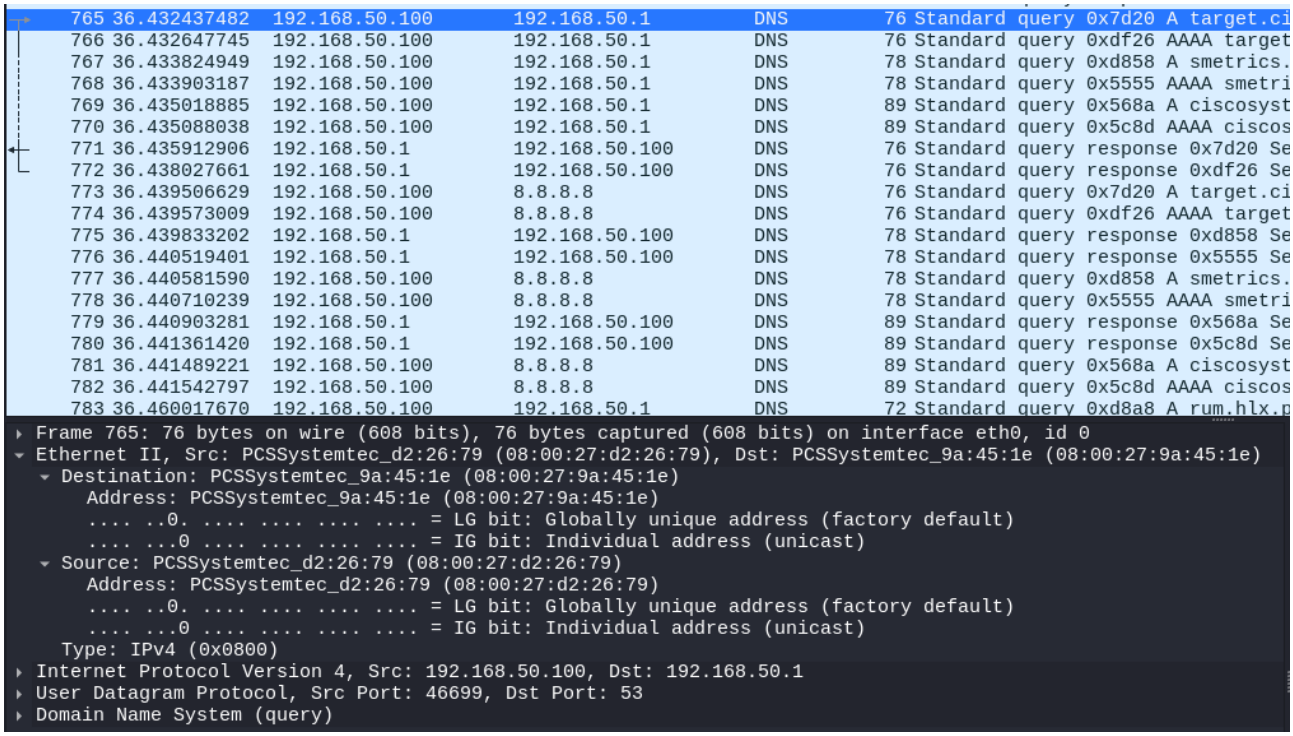
Osservo il traffico catturato nel pannello Packet List di Wireshark. Inserisco il filtro **udp.port == 53** nell'apposita barra dei filtri per visualizzare esclusivamente i pacchetti DNS.

udp.port==53

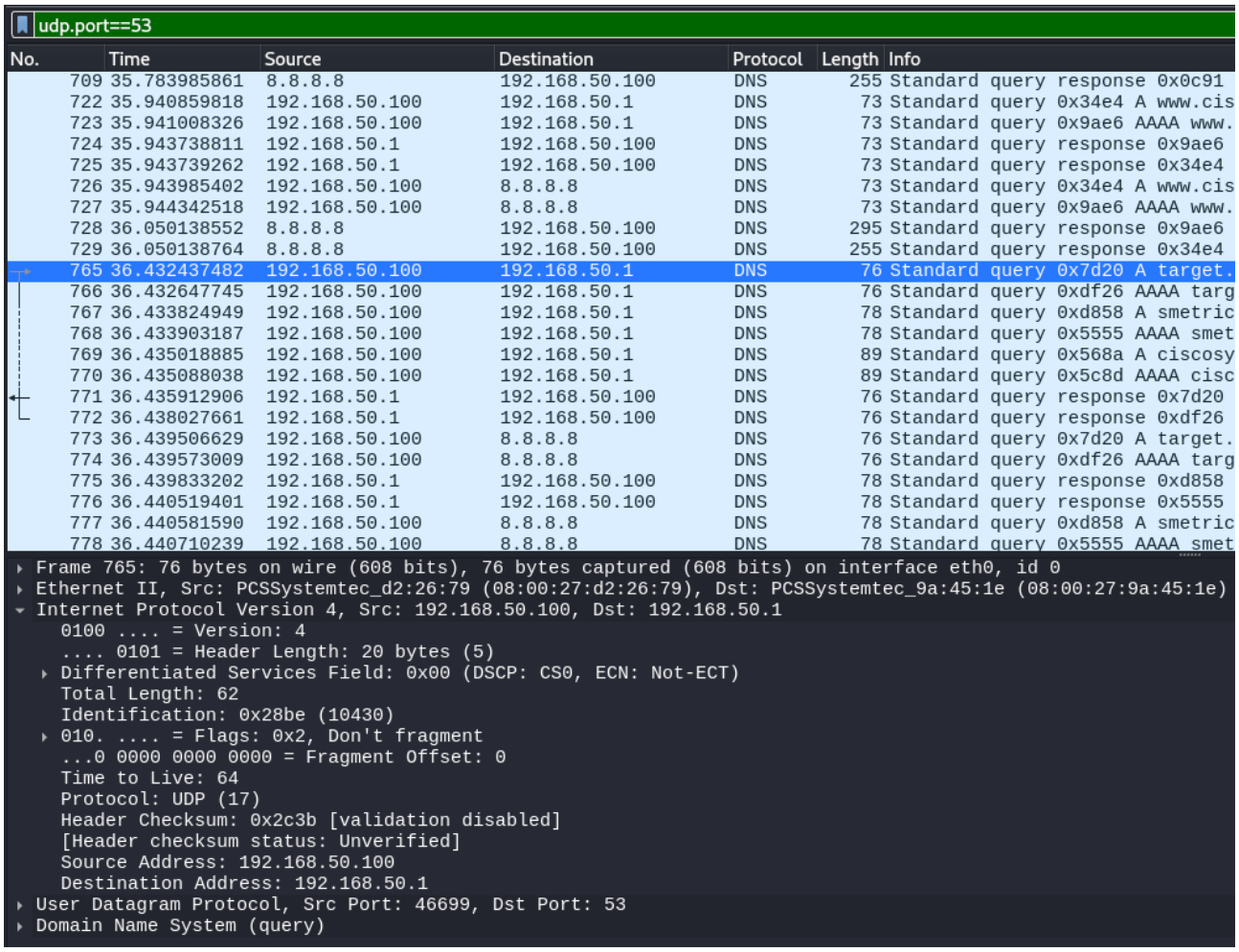
No.	Time	Source	Destination	Protocol	Length	Info
13	5.349440947	192.168.50.100	192.168.50.1	DNS	87	Standard query 0x0291 A service
14	5.349536855	192.168.50.100	192.168.50.1	DNS	87	Standard query 0xb39e AAAA serv
15	5.392883640	192.168.50.100	192.168.50.1	DNS	89	Standard query 0xefc9 A locatio
16	5.392970328	192.168.50.100	192.168.50.1	DNS	89	Standard query 0x59c5 AAAA loca
80	5.892395590	192.168.50.1	192.168.50.100	DNS	151	Standard query response 0x0291
81	6.044888672	192.168.50.1	192.168.50.100	DNS	167	Standard query response 0xefc9
82	6.054951906	192.168.50.1	192.168.50.100	DNS	168	Standard query response 0xb39e
91	6.149914511	192.168.50.1	192.168.50.100	DNS	241	Standard query response 0x59c5
120	6.253590449	192.168.50.100	192.168.50.1	DNS	76	Standard query 0x854b A aus5.mo
121	6.253692143	192.168.50.100	192.168.50.1	DNS	76	Standard query 0x684d AAAA aus5
154	7.208257084	192.168.50.1	192.168.50.100	DNS	268	Standard query response 0x684d
155	7.274083061	192.168.50.1	192.168.50.100	DNS	194	Standard query response 0x854b
176	7.387674864	192.168.50.100	192.168.50.1	DNS	77	Standard query 0x935c A ocsp.di
177	7.387751586	192.168.50.100	192.168.50.1	DNS	77	Standard query 0x6b59 AAAA ocsp
178	7.389830254	192.168.50.1	192.168.50.100	DNS	77	Standard query response 0x6b59
179	7.389830476	192.168.50.1	192.168.50.100	DNS	77	Standard query response 0x935c
180	7.389996515	192.168.50.100	8.8.8.8	DNS	77	Standard query 0x935c A ocsp.di
181	7.390053587	192.168.50.100	8.8.8.8	DNS	77	Standard query 0x6b59 AAAA ocsp
184	7.441387189	8.8.8.8	192.168.50.100	DNS	182	Standard query response 0x935c
185	7.441387211	8.8.8.8	192.168.50.100	DNS	194	Standard query response 0x6b59
226	7.791249891	192.168.50.100	192.168.50.1	DNS	79	Standard query 0x95b3 A archive
229	7.791317741	192.168.50.100	192.168.50.1	DNS	79	Standard query 0xbcb1 AAAA arch
245	7.859023767	192.168.50.1	192.168.50.100	DNS	95	Standard query response 0x95b3

```
▸ Frame 13: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface eth0, id 0
▸ Ethernet II, Src: PCSSystemtec_d2:26:79 (08:00:27:d2:26:79), Dst: PCSSystemtec_9a:45:1e (08:00:27:9a:45:1e)
▸ Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.1
▸ User Datagram Protocol, Src Port: 39875, Dst Port: 53
▸ Domain Name System (query)
```

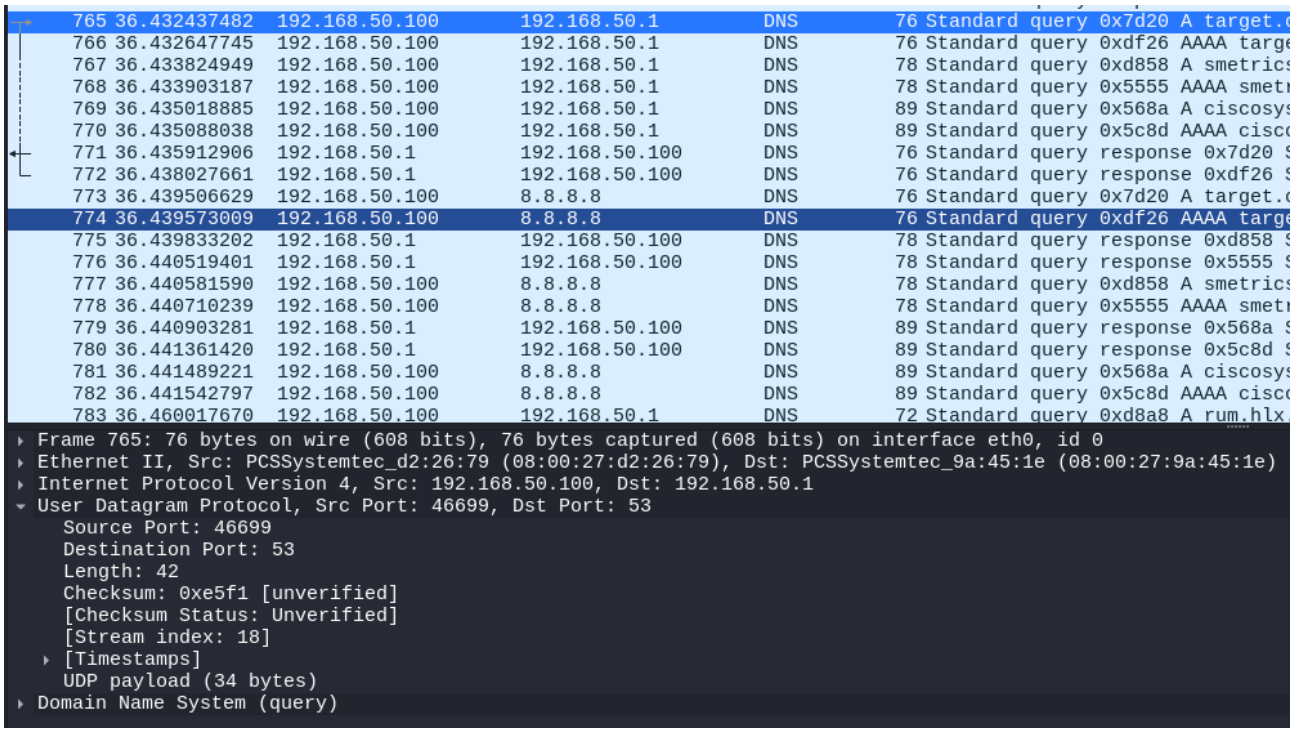
What are the source and destination MAC addresses? Which network interfaces are these MAC addresses associated with?



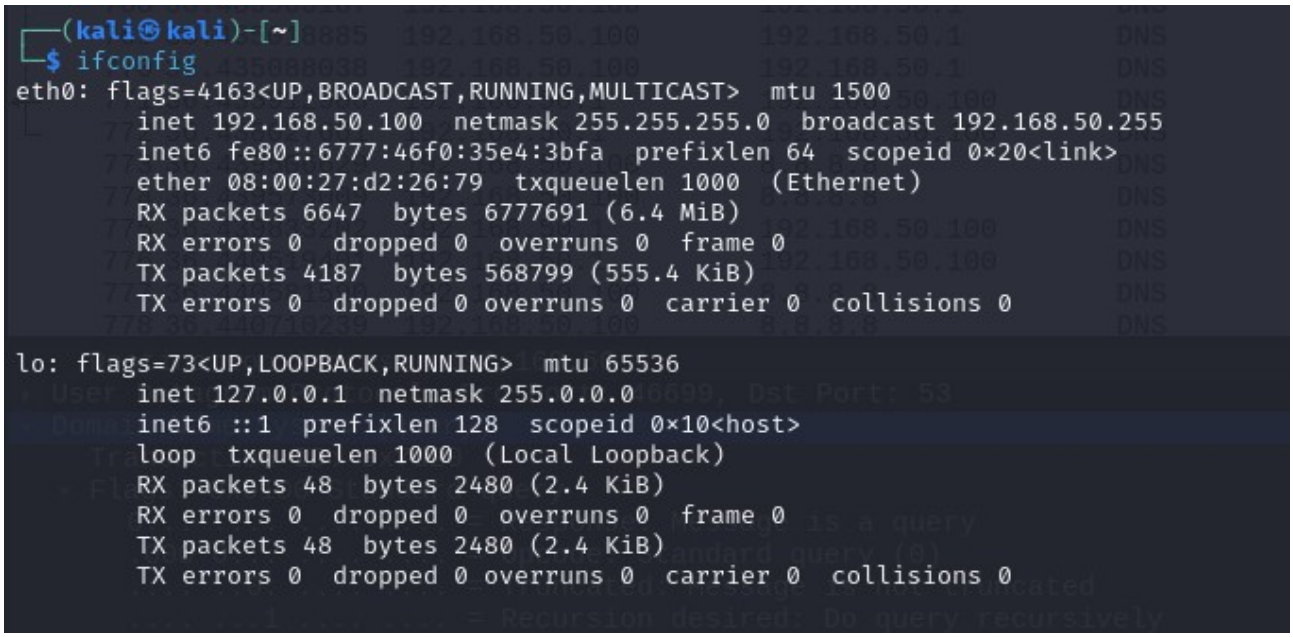
What are the source and destination IP addresses? Which network interfaces are these IP addresses associated with?



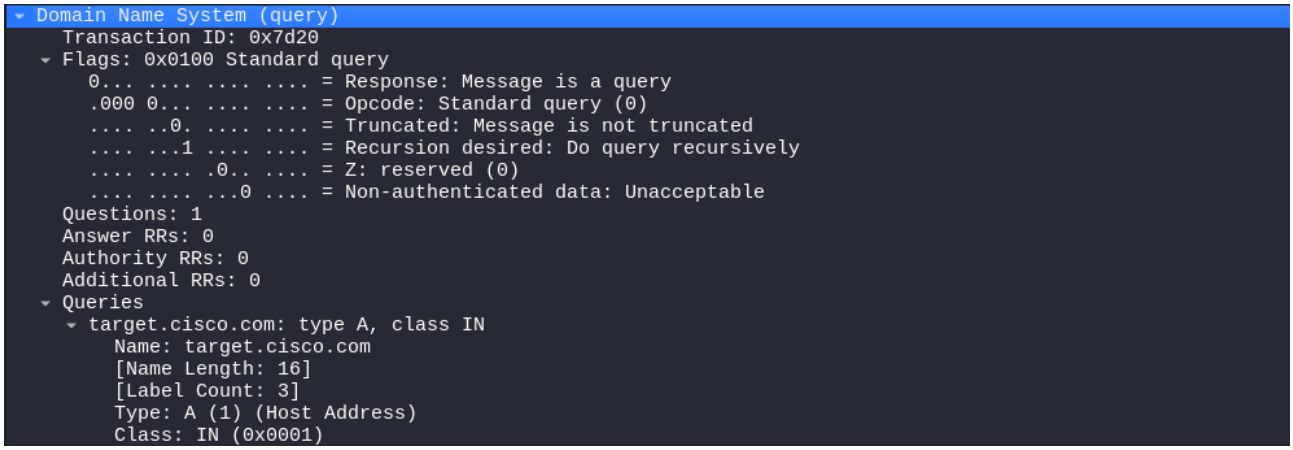
What are the source and destination ports? What is the default DNS port number?



Determine the IP and MAC address of the PC.



Expand **Domain Name System (query)** in the Packet Details pane. Then expand the **Flags** and **Queries**.



Expand **Domain Name System (response)**. Then expand the **Flags, Queries,** and **Answers.**