

Esercitazioni 1–6 - Analisi di Rete

Esercizio 1

1. Che tipo di protocollo di livello Data-link è utilizzato? Come fa Wireshark a capirlo?
Utilizza il protocollo Ethernet. Wireshark lo capisce perché nel pacchetto è presente il campo *EtherType*.
2. Disegnare la PDU di livello Data-link indicando il valore dei vari campi.

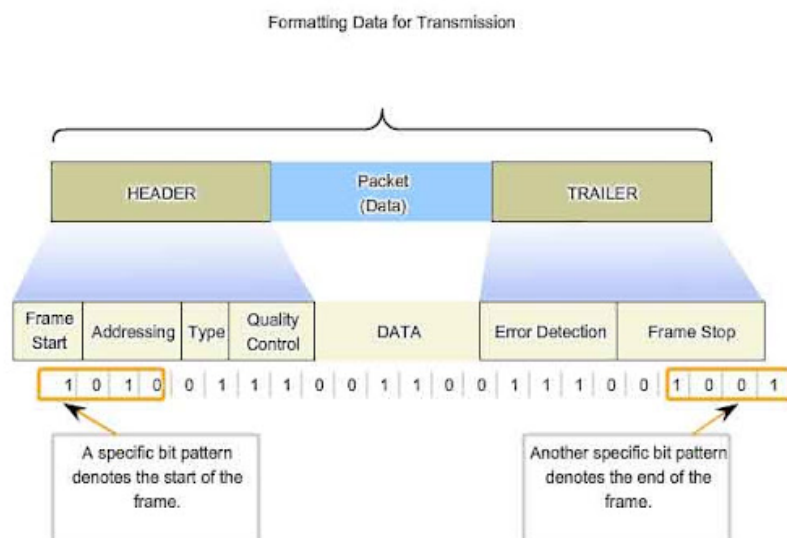
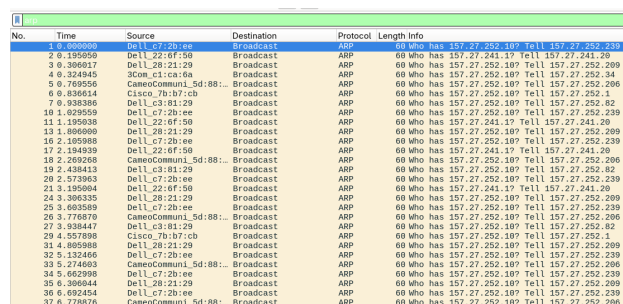


Figure 1: PDU Data-link

3. Qual è il MAC sorgente? Di che tipo è: unicast o broadcast?
Il MAC sorgente è 00:e0:81:24:dd:64 ed è di tipo *unicast*.

4. Qual è il MAC destinazione? Di che tipo è: unicast o broadcast?
Il MAC destinazione è `ff:ff:ff:ff:ff:ff` ed è di tipo *broadcast*.
5. Che tipo di protocollo di livello Network è utilizzato? Come fa Wireshark a capirlo?
Viene utilizzato il protocollo IPv4. Wireshark lo capisce leggendo il campo *Type* nell'header Data-link.
6. Qual è la lunghezza dell'header IP?
La lunghezza dell'header IP è di 20 byte.
7. Quali sono gli indirizzi IP sorgente e destinazione?
IP sorgente: 157.27.252.223
IP destinazione: 157.27.252.255
8. Che tipo di protocollo di livello trasporto è contenuto in IP? Come fa Wireshark a capirlo?
Viene usato il protocollo UDP. Wireshark lo capisce leggendo il campo *Protocol* nell'header IP.
9. Quali sono le porte sorgente e destinazione a livello trasporto?
Porta sorgente: 631
Porta destinazione: 631
10. Creare un filtro per visualizzare solo i pacchetti che hanno ARP come protocollo.
arp



No.	Time	Source	Destination	Protocol	Length	Info
16	0.000000	Dell_c7:2b:ee	Broadcast	ARP	68	68 Who has 157.27.252.10? Tell 157.27.252.239
2	0.195056	Dell_c7:2b:ee	Broadcast	ARP	68	68 Who has 157.27.252.10? Tell 157.27.252.239
3	0.306817	Dell_c7:2b:ee	Broadcast	ARP	68	68 Who has 157.27.252.10? Tell 157.27.252.239
4	0.324845	Com_c1:ca:9a	Broadcast	ARP	68	68 Who has 157.27.252.10? Tell 157.27.252.239
5	0.769556	CanoeCommuni_Sd:88::	Broadcast	ARP	68	68 Who has 157.27.252.10? Tell 157.27.252.239
6	0.836614	Cisco_7b:b7:cb	Broadcast	ARP	68	68 Who has 157.27.252.10? Tell 157.27.252.239
7	0.838386	Dell_c3:81:29	Broadcast	ARP	68	68 Who has 157.27.252.10? Tell 157.27.252.239
18	1.829559	Dell_c7:2b:ee	Broadcast	ARP	68	68 Who has 157.27.252.10? Tell 157.27.252.239
11	1.190038	Dell_c7:2b:ee	Broadcast	ARP	68	68 Who has 157.27.252.10? Tell 157.27.252.239
13	1.866080	Dell_c7:2b:ee	Broadcast	ARP	68	68 Who has 157.27.252.10? Tell 157.27.252.239
16	2.105988	Dell_c7:2b:ee	Broadcast	ARP	68	68 Who has 157.27.252.10? Tell 157.27.252.239
17	2.194539	Dell_c7:2b:ee	Broadcast	ARP	68	68 Who has 157.27.252.10? Tell 157.27.252.239
18	2.269268	CanoeCommuni_Sd:88::	Broadcast	ARP	68	68 Who has 157.27.252.10? Tell 157.27.252.239
19	2.438413	Dell_c3:81:29	Broadcast	ARP	68	68 Who has 157.27.252.10? Tell 157.27.252.239
20	2.573963	Dell_c7:2b:ee	Broadcast	ARP	68	68 Who has 157.27.252.10? Tell 157.27.252.239
21	3.195864	Dell_c7:2b:ee	Broadcast	ARP	68	68 Who has 157.27.252.10? Tell 157.27.252.239
24	3.306335	Dell_c7:2b:ee	Broadcast	ARP	68	68 Who has 157.27.252.10? Tell 157.27.252.239
25	3.603589	Dell_c7:2b:ee	Broadcast	ARP	68	68 Who has 157.27.252.10? Tell 157.27.252.239
26	3.776870	CanoeCommuni_Sd:88::	Broadcast	ARP	68	68 Who has 157.27.252.10? Tell 157.27.252.239
27	3.938447	Dell_c3:81:29	Broadcast	ARP	68	68 Who has 157.27.252.10? Tell 157.27.252.239
29	4.257899	Cisco_7b:b7:cb	Broadcast	ARP	68	68 Who has 157.27.252.10? Tell 157.27.252.239
31	4.805988	Dell_c7:2b:ee	Broadcast	ARP	68	68 Who has 157.27.252.10? Tell 157.27.252.239
32	5.132466	Dell_c7:2b:ee	Broadcast	ARP	68	68 Who has 157.27.252.10? Tell 157.27.252.239
33	5.174803	CanoeCommuni_Sd:88::	Broadcast	ARP	68	68 Who has 157.27.252.10? Tell 157.27.252.239
34	5.662998	Dell_c7:2b:ee	Broadcast	ARP	68	68 Who has 157.27.252.10? Tell 157.27.252.239
35	6.306844	Dell_c7:2b:ee	Broadcast	ARP	68	68 Who has 157.27.252.10? Tell 157.27.252.239
36	6.892454	Dell_c7:2b:ee	Broadcast	ARP	68	68 Who has 157.27.252.10? Tell 157.27.252.239
37	6.778876	CanoeCommuni_Sd:88::	Broadcast	ARP	68	68 Who has 157.27.252.10? Tell 157.27.252.239

Figure 2: Filtro ARP

11. Dopo aver applicato il filtro precedente qual è la percentuale di pacchetti che rimangono visualizzati rispetto al totale?
63% (173 pacchetti su 272)

12. Creare un filtro per visualizzare solo i pacchetti che hanno destinazione MAC 00:01:e6:57:4b:e0.
eth.dst == 00:01:e6:57:4b:e0

No.	Time	Source	Destination	Protocol	Length	Info
12	4.855885	157.27.252.10	157.27.252.25	SNMP	120	get-request 1.3.6.1.2.1.25.3.2.1.5.1.1.3.6.1.
251	58.339782	HewlettPacka_57:4b::	Broadcast	ARP	68	Who has 157.27.252.10? Tell 157.27.252.25
254	59.332916	HewlettPacka_57:4b::	Broadcast	ARP	68	Who has 157.27.252.10? Tell 157.27.252.25

Figure 3: Filtro destinazione MAC specifico

13. Dopo aver applicato il filtro precedente qual è la percentuale di pacchetti che rimangono visualizzati rispetto al totale?
0.4% (1 pacchetto su 272)
14. Creare un filtro per visualizzare solo i pacchetti che hanno destinazione MAC broadcast.
eth.dst == ff:ff:ff:ff:ff:ff

No.	Time	Source	Destination	Protocol	Length	Info
1	0.889880	Dell_c7:2b:ee	Broadcast	ARP	68	Who has 157.27.252.10? Tell 157.27.252.239
2	0.195958	Dell_c7:2b:ee	Broadcast	ARP	68	Who has 157.27.241.1? Tell 157.27.241.20
3	0.398817	Dell_c7:2b:ee	Broadcast	ARP	68	Who has 157.27.252.10? Tell 157.27.252.209
4	0.524845	3Com_c1:ca:6a	Broadcast	ARP	68	Who has 157.27.252.10? Tell 157.27.252.34
5	0.769556	CiscoCommu_5d:88::	Broadcast	ARP	68	Who has 157.27.252.10? Tell 157.27.252.206
6	0.836614	Cisco_7b:b7:cb	Broadcast	ARP	68	Who has 157.27.252.10? Tell 157.27.252.1
7	0.938386	Dell_c3:81:29	Broadcast	ARP	68	Who has 157.27.252.10? Tell 157.27.252.82
8	0.958388	157.27.252.223	157.27.252.255	CUPS	227	ipp://157.27.252.223/printers/DESKJET-970N
9	1.028599	Dell_c7:2b:ee	Broadcast	ARP	68	Who has 157.27.252.10? Tell 157.27.252.239
11	1.150338	Dell_c2:61:f5:0	Broadcast	ARP	68	Who has 157.27.241.1? Tell 157.27.241.20
12	1.869680	Dell_c7:2b:ee	Broadcast	ARP	68	Who has 157.27.252.10? Tell 157.27.252.239
15	1.958655	157.27.252.223	157.27.252.255	CUPS	275	ipp://157.27.252.223/printers/HP-LaserJet
16	2.189588	Dell_c7:2b:ee	Broadcast	ARP	68	Who has 157.27.252.10? Tell 157.27.252.239
17	2.194539	Dell_c7:2b:ee	Broadcast	ARP	68	Who has 157.27.241.1? Tell 157.27.241.20
18	2.269268	CiscoCommu_5d:88::	Broadcast	ARP	68	Who has 157.27.252.10? Tell 157.27.252.206
19	2.438413	Dell_c3:81:29	Broadcast	ARP	68	Who has 157.27.252.10? Tell 157.27.252.82
20	2.573963	Dell_c7:2b:ee	Broadcast	ARP	68	Who has 157.27.252.10? Tell 157.27.252.239
21	3.195884	Dell_c7:2b:ee	Broadcast	ARP	68	Who has 157.27.241.1? Tell 157.27.241.20
24	3.386335	Dell_c7:2b:ee	Broadcast	ARP	68	Who has 157.27.252.10? Tell 157.27.252.209
25	3.693589	Dell_c7:2b:ee	Broadcast	ARP	68	Who has 157.27.252.10? Tell 157.27.252.239
26	3.776878	CiscoCommu_5d:88::	Broadcast	ARP	68	Who has 157.27.252.10? Tell 157.27.252.206
27	3.938447	Dell_c3:81:29	Broadcast	ARP	68	Who has 157.27.252.10? Tell 157.27.252.82
28	4.327452	157.27.252.91	157.27.252.255	BROWSER	243	Host Announcement NP19976AA, Workstation, Ser
29	4.557898	Cisco_7b:b7:cb	Broadcast	ARP	68	Who has 157.27.252.10? Tell 157.27.252.1
31	4.889588	Dell_c7:2b:ee	Broadcast	ARP	68	Who has 157.27.252.10? Tell 157.27.252.209
32	5.132466	Dell_c7:2b:ee	Broadcast	ARP	68	Who has 157.27.252.10? Tell 157.27.252.239
33	5.274883	CiscoCommu_5d:88::	Broadcast	ARP	68	Who has 157.27.252.10? Tell 157.27.252.206
34	5.662898	Dell_c7:2b:ee	Broadcast	ARP	68	Who has 157.27.252.10? Tell 157.27.252.239

Figure 4: Filtro MAC broadcast

15. Dopo aver applicato il filtro precedente qual è la percentuale di pacchetti che rimangono visualizzati rispetto al totale? Sono molti? Perché?
83.8% (228 pacchetti su 272). Sono molti perché ci sono state molte assegnazioni IP tramite protocollo ARP.

Esercizio 2

1. Colorare di rosso tutti i pacchetti che contengono UDP e di verde tutti i pacchetti che contengono TCP.

2	8.000000	157.27.252.202	157.27.19.18	DNS	73 Standard query 0x9097 / www.politico.it
3	8.000021	157.27.19.18	157.27.252.202	TCP	254 Standard query response 0x9097 / www.politico.it CHAME www01.politico.it A 150.152.73.1 NS text=
4	8.000024	157.27.252.202	150.152.73.1	TCP	Seq=689888888 [ACK] Seq=689888888 Win=0 SACK Permitted SACK Permitted TSval=764888 TSercr=MS-64
5	8.000024	157.27.252.202	150.152.73.1	TCP	42 800 - 36986 [ACK] Seq=689888888 Win=0 SACK Permitted SACK Permitted TSval=764888 TSercr=MS-64
6	8.002344	157.27.252.202	139.192.73.1	TCP	50 36988 - 80 [ACK] Seq=689888888 Win=0 SACK Permitted SACK Permitted TSval=764888 TSercr=MS-64
7	8.002345	157.27.252.202	139.192.73.1	TCP	154 0 - 36986 [ACK] Seq=689888888 Win=0 SACK Permitted SACK Permitted TSval=764888 TSercr=MS-64
8	8.002423	150.152.73.1	157.27.252.202	TCP	60 0 - 36986 [ACK] Seq=689888888 Win=65155 Len=0
9	8.002423	150.152.73.1	157.27.252.202	TCP	60 0 [TCP RST] Seq=689888888 Win=0 SACK Permitted SACK Permitted TSval=764888 TSercr=MS-64
10	8.002435	150.152.73.1	157.27.252.202	TCP	80 0 [TCP RST] Seq=689888888 Win=0 SACK Permitted SACK Permitted TSval=764888 TSercr=MS-64
11	8.002488	150.152.73.1	157.27.252.202	TCP	154 0 - 36986 [ACK] Seq=689888888 Win=65155 Len=0
12	8.002488	150.152.73.1	157.27.252.202	TCP	1514 0 - 36986 [PSH, ACK] Seq=689888888 Win=65155 Len=1460 [TCP PDU reasssembled in 84]
13	8.002492	157.27.252.202	139.192.73.1	TCP	50 36988 - 80 [ACK] Seq=689888888 Win=780 Len=0
14	8.002497	157.27.252.202	139.192.73.1	TCP	1514 0 - 36986 [ACK] Seq=689888888 Win=780 Len=0
15	8.002497	157.27.252.202	139.192.73.1	TCP	50 36988 - 80 [ACK] Seq=689888888 Win=1080 Len=0
16	8.002497	157.27.252.202	139.192.73.1	TCP	154 36988 - 80 [ACK] Seq=689888888 Win=1080 Len=0
17	8.002497	157.27.252.202	139.192.73.1	TCP	1514 0 - 36986 [PSH, ACK] Seq=689888888 Win=65155 Len=1460 [TCP PDU reasssembled in 84]
18	8.002497	157.27.252.202	139.192.73.1	TCP	50 36988 - 80 [ACK] Seq=689888888 Win=1080 Len=0
19	8.002497	157.27.252.202	139.192.73.1	TCP	1514 0 - 36986 [ACK] Seq=689888888 Win=65155 Len=1460 [TCP PDU reasssembled in 84]
20	8.002497	157.27.252.202	139.192.73.1	TCP	50 36988 - 80 [ACK] Seq=689888888 Win=1080 Len=0
21	8.002497	157.27.252.202	139.192.73.1	TCP	1514 0 - 36986 [ACK] Seq=689888888 Win=65155 Len=1460 [TCP PDU reasssembled in 84]
22	8.002497	157.27.252.202	139.192.73.1	TCP	50 36988 - 80 [ACK] Seq=689888888 Win=1080 Len=0
23	8.002497	157.27.252.202	139.192.73.1	TCP	1514 0 - 36986 [ACK] Seq=689888888 Win=65155 Len=1460 [TCP PDU reasssembled in 84]
24	8.002497	157.27.252.202	139.192.73.1	TCP	50 36988 - 80 [ACK] Seq=689888888 Win=1080 Len=0
25	8.002497	157.27.252.202	139.192.73.1	TCP	1514 0 - 36986 [ACK] Seq=689888888 Win=65155 Len=1460 [TCP PDU reasssembled in 84]
26	8.002497	157.27.252.202	139.192.73.1	TCP	50 36988 - 80 [ACK] Seq=689888888 Win=1080 Len=0
27	8.002497	157.27.252.202	139.192.73.1	TCP	1514 0 - 36986 [ACK] Seq=689888888 Win=65155 Len=1460 [TCP PDU reasssembled in 84]
28	8.002497	157.27.252.202	139.192.73.1	TCP	50 36988 - 80 [ACK] Seq=689888888 Win=1080 Len=0
29	8.002497	157.27.252.202	139.192.73.1	TCP	1514 0 - 36986 [ACK] Seq=689888888 Win=65155 Len=1460 [TCP PDU reasssembled in 84]
30	8.002497	157.27.252.202	139.192.73.1	TCP	50 36988 - 80 [ACK] Seq=689888888 Win=1080 Len=0
31	8.002497	157.27.252.202	139.192.73.1	TCP	1514 0 - 36986 [ACK] Seq=689888888 Win=65155 Len=1460 [TCP PDU reasssembled in 84]
32	8.002497	157.27.252.202	139.192.73.1	TCP	50 36988 - 80 [ACK] Seq=689888888 Win=1080 Len=0
33	8.002497	157.27.252.202	139.192.73.1	TCP	1514 0 - 36986 [ACK] Seq=689888888 Win=65155 Len=1460 [TCP PDU reasssembled in 84]
34	8.002497	157.27.252.202	139.192.73.1	TCP	50 36988 - 80 [ACK] Seq=689888888 Win=1080 Len=0
35	8.002497	157.27.252.202	139.192.73.1	TCP	1514 0 - 36986 [ACK] Seq=689888888 Win=65155 Len=1460 [TCP PDU reasssembled in 84]

2. Cosa contengono i primi due pacchetti della sessione di cattura?

- IP sorgente: 157.27.252.202
- IP destinazione: 157.27.10.10
- Trasporto: UDP
- Applicazione: DNS (www.polito.it)

- IP sorgente: 157.27.10.10
- IP destinazione: 157.27.252.202
- Trasporto: UDP
- Applicazione: DNS (web01.polito.it → 130.192.73.1)

- IP sorgente: 157.27.252.202
- IP destinazione: 130.192.73.1
- Trasporto: TCP
- Applicazione: risposta alla ricerca DNS

- IP sorgente: 157.27.252.202
- IP destinazione: 130.192.73.1

- Trasporto: TCP
 - Applicazione: HTTP
 - I tre pacchetti precedenti sono il Three Way Handshake (flag SEQ e ACK).
5. **Filtro per pacchetti TCP (inclusi HTTP), numero pacchetti:**
807 su 823
6. **Filtro per pacchetti TCP (esclusi HTTP), numero pacchetti e percentuale:**
673 su 823 (81,8%). Sono i pacchetti TCP di handshake; se DNS usasse TCP, sarebbero stati generati 6 pacchetti in più, rallentando.
7. **Seguire lo stream TCP: cosa si può leggere?**
Si possono leggere le varie richieste HTTP GET.

Esercizio 3

1. **Protocolli di livello Applicazione per trasporto:**
UDP: DNS
TCP: HTTP, FTP, SSH
2. **Analisi di diversi stream TCP:**

[illegible]

Figure 6: Esempio di stream TCP

- 3. Differenza FTP vs SSH:**
Sì, la differenza è che SSH è criptato.

Esercizio 4

1. **Numero richieste ping e risposte:**
22 su 3215
2. **IP sorgente e destinazione delle richieste ICMP e intestatari:**
IP sorgente: 157.27.143.46
IP destinazione: 216.58.211.196 (www.google.com)
3. **RTT medio e variazione (google vs gateway):**
RTT gateway: 0.028 ms
RTT Google: 5.75 ms
Il gateway mostra RTT minore essendo interno alla rete locale.

Esercizio 5

1. **Interfacce dei router attraversati:**

```
ProgESicurezzaReti_2025/wireshark-analisi-rete [? main]
> traceroute www.google.com
traceroute to www.google.com (2a00:1450:4002:414::2004), 30 hops max, 80 byte packets
 1 2001:760:2204:223::1 (2001:760:2204:223::1) 6.924 ms 6.807 ms 6.774 ms
 2 2001:760:2204:f610::1 (2001:760:2204:f610::1) 6.463 ms 6.627 ms 6.598 ms
 3 ru-univr-l1-r11-vr00.vr00.garr.net (2001:760:ffff:124::18) 6.651 ms 6.622 ms 6.593 ms
 4 r11-vr00-rs1-mi01.mi01.garr.net (2001:760:ffff:ffbb:181:163) 6.483 ms 6.453 ms 6.425 ms
 5 rs1-mi01-rs1-mi02.mi02.garr.net (2001:760:ffff:ffaa:180:158) 6.537 ms 6.507 ms 6.478 ms
 6 2001:a860:1:1::1ea6 (2001:a860:1:1::1ea6) 6.476 ms 2001:a860:1:1::28a0 (2001:a860:1:1::28a0) 5.790 ms 5.662 ms
 7 2001:a860:0:1::81f3 (2001:a860:0:1::81f3) 5.739 ms 2a00:1450:813b::1 (2a00:1450:813b::1) 5.731 ms 2a00:1450:8041::1 (2a00:1450:8041::1) 10.306 ms
 8 2001:a860:0:1::1798 (2001:a860:0:1::1798) 10.266 ms mil07sl7-in-x04.1e100.net (2a00:1450:4002:414::2004) 9.296 ms 2001:a860:0:1::61b8 (2001:a860:0:1::61b8) 10.163 ms
```

Figure 7: Output del traceroute

2. **Organizzazioni intestatarie degli IP:**
Vedi annotazioni nel tracciato (fig. traceroute).

Esercizio 6

1. **Interfacce attive, IP e netmask:**

```
ProgESicurezzaReti_2025/wireshark-analisi-rete [? main][?]
> ip -brief addr

```

		UNKNOWN	127.0.0.1/8	::1/128
vlp0a28f3	ip		157.27.161.67/19	2001:760:2204:223:d2:0:ffff:a167/128
br-35fe03aa2712	vxlan		172.20.0.1/16	
br-4a036a1c0706	vxlan		172.18.0.1/16	
br-6063ccac19009	vlan		172.19.0.1/16	
bracke08	vlan		172.17.0.1/16	

Figure 8: Interfacce attive sul PC

2. IP di `www.univr.it`:

Ricavato tramite `nslookup` o comando equivalente (vedi fig. interfacce).