

Jalon 4 :

4.1

Copie du cache Arp de chaque machine réalisé avec la commande arp -a

figure 21) cache arp de la raspberry

```
noah@noah:~$ arp -a
? (192.168.33.2) at 4c:d7:17:9f:18:78 [ether] on eth0
? (192.168.33.3) at 4c:d7:17:86:85:d9 [ether] on eth0
? (192.168.33.114) at f8:e4:3b:52:16:e7 [ether] on eth0
? (192.168.33.151) at d8:3a:dd:07:01:c1 [ether] on eth0
? (192.168.33.1) at 00:00:5e:00:01:02 [ether] on eth0
? (192.168.33.88) at 00:be:43:8c:43:12 [ether] on eth0
? (192.168.33.103) at d8:3a:dd:07:01:c1 [ether] on eth0
? (192.168.33.178) at c8:a3:62:23:ba:0b [ether] on eth0
```

figure 22) cache arp de l'ordinateur

```
root@rt:~# arp -a
? (192.168.33.79) at 00:be:43:8c:54:7a [ether] on eth0
? (192.168.33.1) at 00:00:5e:00:01:02 [ether] on eth0
? (192.168.33.114) at f8:e4:3b:52:16:e7 [ether] on eth0
? (192.168.33.49) at 18:66:da:48:90:1e [ether] on eth0
? (192.168.33.23) at 34:17:eb:9d:25:75 [ether] on eth0
? (192.168.33.227) at f8:75:a4:5b:64:3e [ether] on eth0
? (192.168.33.106) at 00:05:5d:7c:c6:4e [ether] on eth0
? (192.168.33.2) at 4c:d7:17:9f:18:78 [ether] on eth0
? (192.168.33.15) at 34:17:eb:9d:4f:1d [ether] on eth0
? (192.168.33.50) at 18:66:da:48:88:48 [ether] on eth0
? (192.168.33.37) at e4:54:e8:a5:99:c5 [ether] on eth0
? (192.168.33.215) at 00:40:8c:b6:f1:7e [ether] on eth0
? (192.168.33.85) at 00:be:43:8c:4d:f7 [ether] on eth0
? (192.168.33.3) at 4c:d7:17:86:85:d9 [ether] on eth0
? (192.168.33.29) at e4:54:e8:a5:99:61 [ether] on eth0
? (192.168.33.103) at d8:3a:dd:07:01:c1 [ether] on eth0
? (192.168.33.151) at d8:3a:dd:07:01:c1 [ether] on eth0
? (192.168.33.125) at d8:3a:dd:0c:fd:10 [ether] on eth0
? (192.168.33.78) at 00:be:43:8c:3c:a7 [ether] on eth0
? (192.168.33.39) at e4:54:e8:a5:9a:0f [ether] on eth0
? (192.168.33.74) at 00:be:43:8c:9e:e7 [ether] on eth0
```

4.2

figure 23) Copie de la capture des trames composants un ping réalisé sur wireshark

The image shows a Wireshark packet capture window titled '*eth0'. The menu bar includes: Fichier, Editer, Vue, Aller, Capture, Analyser, Statistiques, Telephonie, Wireless, Outils, Aide. The toolbar contains various icons for packet capture and analysis. The packet list pane shows a list of captured packets, with the filter 'icmp' applied. The packet details pane shows the structure of the selected packet (No. 6), which is an ICMP Echo (ping) request. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
6	0.797632967	192.168.33.88	192.168.33.125	ICMP	98	Echo (ping) request id=0x1
7	0.797898273	192.168.33.125	192.168.33.88	ICMP	98	Echo (ping) reply id=0x1
14	1.823360184	192.168.33.88	192.168.33.125	ICMP	98	Echo (ping) request id=0x1
15	1.823620143	192.168.33.125	192.168.33.88	ICMP	98	Echo (ping) reply id=0x1
19	2.847556866	192.168.33.88	192.168.33.125	ICMP	98	Echo (ping) request id=0x1
20	2.848147256	192.168.33.125	192.168.33.88	ICMP	98	Echo (ping) reply id=0x1
26	3.871363803	192.168.33.88	192.168.33.125	ICMP	98	Echo (ping) request id=0x1
27	3.871854264	192.168.33.125	192.168.33.88	ICMP	98	Echo (ping) reply id=0x1

Packet 6 details:

- ... 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 84
 - Identification: 0xc101 (49409)
- Flags: 0x4000, Don't fragment
 - Fragment offset: 0
 - Time to live: 64
 - Protocol: ICMP (1)
 - Header checksum: 0xb581 [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 192.168.33.88
 - Destination: 192.168.33.125
- Internet Control Message Protocol
 - Type: 8 (Echo (ping) request)
 - Code: 0
 - Checksum: 0xcb54 [correct]
 - [Checksum Status: Good]
 - Identifier (BE): 4966 (0x1366)
 - Identifier (LE): 26131 (0x6613)
 - Sequence number (BE): 1 (0x0001)
 - Sequence number (LE): 256 (0x0100)
 - [Response frame: 7]
 - Timestamp from icmp data: Jan 9, 2025 17:26:19.000000000 CET
 - [Timestamp from icmp data (relative): 0.069991981 seconds]
- Data (48 bytes)

Packet 6 bytes:

```

0000 d8 3a dd 0c fd 10 00 be 43 8c 43 12 08 00 45 00  .:.....C.C...E.
0010 00 54 c1 01 40 00 40 01 b5 81 c0 a8 21 58 c0 a8  .T..@..@...!X..
0020 21 7d 08 00 cb 54 13 66 00 01 ab f8 7f 67 00 00  !}...T.f....g..
0030 00 00 2e 11 01 00 00 00 00 00 10 11 12 13 14 15  .....!#$%
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  .....!#$%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,-./012345
0060 36 37 67
  
```

Wireshark status bar: wireshark_eth0_20250109172617_YV9sRs.pcapng Paquets: 44 · Affichés: 8 (18.2%) · Perdus: 0 (0.0%) · Profile: Default

4.3

Copie du résultat d'un netstat sur chacune des machines réalisé avec la commande netstat -tulnp

figure 24) netstat du raspberry

```
noah@noah:~$ netstat -tulnp
(Tous les processus ne peuvent être identifiés, les infos sur les processus
non possédés ne seront pas affichées, vous devez être root pour les voir toutes.)
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Adresse locale Adresse distante Etat PID/Programme
tcp 0 0 0.0.0.0:5900 0.0.0.0:* LISTEN -
tcp 0 0 127.0.0.1:631 0.0.0.0:* LISTEN -
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN -
tcp6 0 0 :::5900 :::* LISTEN -
tcp6 0 0 ::1:631 :::* LISTEN -
tcp6 0 0 :::22 :::* LISTEN -
tcp6 0 0 :::80 :::* LISTEN -
udp 0 0 0.0.0.0:68 0.0.0.0:* -
udp 0 0 224.0.0.251:5353 0.0.0.0:* 2281/chromium
udp 0 0 0.0.0.0:5353 0.0.0.0:* -
udp 0 0 0.0.0.0:631 0.0.0.0:* -
udp 0 0 0.0.0.0:47754 0.0.0.0:* -
udp6 0 0 :::5353 :::* -
udp6 0 0 :::40403 :::* -
udp6 0 0 :::546 :::* -
noah@noah:~$
```

figure 25) netstat de l'ordinateur

```
root@rt:~# netstat -tulnp
```

Connexions Internet actives (seulement serveurs)

Proto	Recv-Q	Send-Q	Adresse locale	Adresse distante	Etat	PID/Program name
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN	654/sshd
tcp	0	0	127.0.0.1:631	0.0.0.0:*	LISTEN	614/cupsd
tcp6	0	0	:::22	:::*	LISTEN	654/sshd
tcp6	0	0	:::1:631	:::*	LISTEN	614/cupsd
udp	0	0	0.0.0.0:68	0.0.0.0:*		626/dhclient
udp	0	0	192.168.33.88:123	0.0.0.0:*		647/ntpd
udp	0	0	127.0.0.1:123	0.0.0.0:*		647/ntpd
udp	0	0	0.0.0.0:123	0.0.0.0:*		647/ntpd
udp	0	0	0.0.0.0:631	0.0.0.0:*		662/cups-brow
udp	0	0	0.0.0.0:59866	0.0.0.0:*		629/avahi-dae
mon: r						
udp	0	0	0.0.0.0:5353	0.0.0.0:*		629/avahi-dae
mon: r						
udp6	0	0	:::55629	:::*		629/avahi-dae
mon: r						
udp6	0	0	fe80::2be:43ff:fe8c:123	:::*		647/ntpd
udp6	0	0	:::1:123	:::*		647/ntpd
udp6	0	0	:::123	:::*		647/ntpd
udp6	0	0	:::5353	:::*		629/avahi-dae
mon: r						

```
root@rt:~#
```

4.4

Procédure d'utilisation de Wireshark:

- Ouvrir Wireshark pour accéder aux interfaces réseau.
- Choisir une interface réseau (ex. Ethernet ou Wi-Fi) dans la liste.
- Cliquer sur "Start" pour capturer le trafic.
- Observer le trafic capturé en temps réel dans la fenêtre principale.
- Utiliser les filtres pour simplifier l'analyse.
- Cliquer sur un paquet pour afficher ses détails dans la fenêtre inférieure.
- Analyser les protocoles, les adresses IP, et les ports des paquets.

4.5

Copie de l'agenda hebdomadaire réactualisé.

Etat des tâches		
ID	Tâches récapitulatives	Sous tâches
<div> Non commencé En cours Terminé </div>		
	Binôme 1. SAE 12 s'initier aux réseaux informatiques : 20 heures	11
2	1 Outil de supervision: Mise en place d'un agenda hebdomadaire (1h)	1
3	2 Le PC fixe est connecté au réseau de l'IUT et il accède sur l'extérieur : (1h)	1
4	3 Rpi connecté sur le réseau de l'IUT (2h)	1
5	4 Mise en place d'un serveur web Apache sur le Rpi	1
6	5 Certification de la connexion des 2 machines sur le même réseau (2h)	1
7	6 Accès ssh établi entre le PC fixe et le Rpi(1h)	1
8	7 partage de ressources actif (3h)	1
9	8 réseau de la salle analysé (3h)	1
10	9 Infrastructure réseau de l'IUT analysé (3h)	1
11	10 Etude énergétique	1
12	11 Présentation finale: oral de 15mn en binôme	1
	Total tâches	11