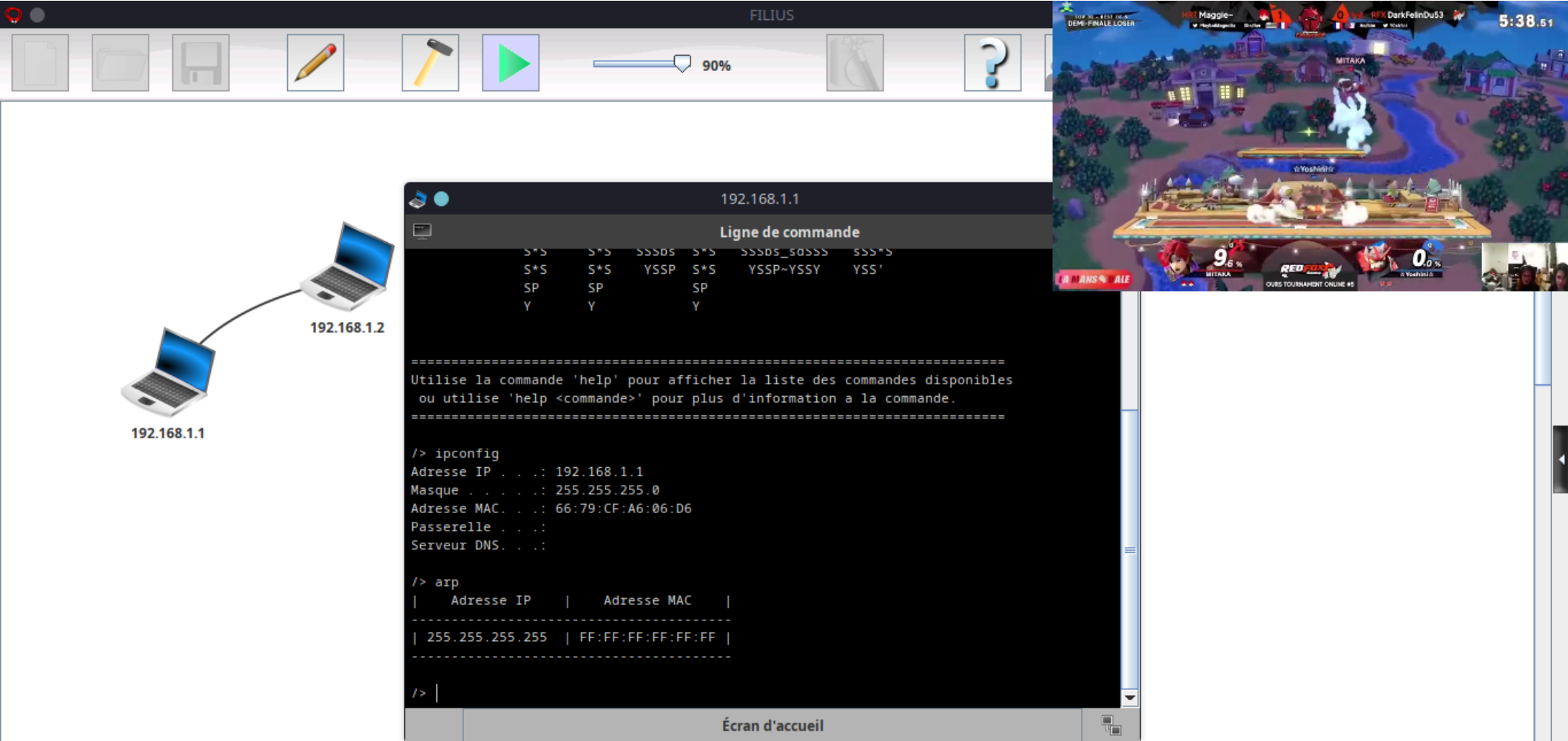


CR

table ARP

avant toute communication, et sur un reseau à 2 machines, le setup est le suivant



nous effectuons ensuite un ping depuis .1 vers .2, et constatons que l'@MAC correspondant à l'@IP de .2 est désormais dans la table ARP

```
/> arp
| Adresse IP | Adresse MAC |
|-----|-----|
| 255.255.255.255 | FF:FF:FF:FF:FF:FF |
|-----|-----|

/> ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2)
From 192.168.1.2 (192.168.1.2): icmp_seq=
From 192.168.1.2 (192.168.1.2): icmp_seq=
From 192.168.1.2 (192.168.1.2): icmp_seq=
From 192.168.1.2 (192.168.1.2): icmp_seq=
--- 192.168.1.2 Statistiques des paquets
4 paquets transmis, 4 paquets reçus, 0% p

/> arp
| Adresse IP | Adresse MAC |
|-----|-----|
| 192.168.1.2 | F9:E4:8A:13:40:1F |
| 255.255.255.255 | FF:FF:FF:FF:FF:FF |
|-----|-----|

/>
```

en examinant le trafic reseau de la machine 1, on voit:


Échanges de données

192.168.1.1 X

No.	Date	Source	Destination	Protocole	Couche	Commentaire / Détail
1	22:19:03.224	192.168.1.1	192.168.1.2	ARP	Internet	Recherche de l'adresse MAC associée à 192.168.1.2 [op=REQUEST, sender=66:79:CF:A6:06:D6 192.168.1.1, target=FF:FF:FF:FF:FF:FF 192.168.1.2]
2	22:19:03.425	192.168.1.2	192.168.1.1	ARP	Internet	L'adresse MAC est F9:E4:8A:13:40:1F [op=REPLY, sender=F9:E4:8A:13:40:1F 192.168.1.2, target=66:79:CF:A6:06:D6 192.168.1.1]
3	22:19:03.426	192.168.1.1	192.168.1.2	ICMP	Internet	ICMP Echo Request (ping), TTL: 64, Seq.-No.: 1
4	22:19:03.551	192.168.1.2	192.168.1.1	ICMP	Internet	ICMP Echo Reply (pong), TTL: 64, Seq.-No.: 1
5	22:19:04.225	192.168.1.1	192.168.1.2	ICMP	Internet	ICMP Echo Request (ping), TTL: 64, Seq.-No.: 2
6	22:19:04.348	192.168.1.2	192.168.1.1	ICMP	Internet	ICMP Echo Reply (pong), TTL: 64, Seq.-No.: 2
7	22:19:05.231	192.168.1.1	192.168.1.2	ICMP	Internet	ICMP Echo Request (ping), TTL: 64, Seq.-No.: 3
8	22:19:05.347	192.168.1.2	192.168.1.1	ICMP	Internet	ICMP Echo Reply (pong), TTL: 64, Seq.-No.: 3
9	22:19:06.222	192.168.1.1	192.168.1.2	ICMP	Internet	ICMP Echo Request (ping), TTL: 64, Seq.-No.: 4

No.: 1 / Date: 22:19:03.224

- Réseau
 - Source: 66:79:CF:A6:06:D6
 - Destination: FF:FF:FF:FF:FF:FF
 - Commentaire / Détail: 0x806
- Internet
 - Source: 192.168.1.1
 - Destination: 192.168.1.2
 - Protocole: ARP
 - Commentaire / Détail: Recherche de l'adresse MAC associée à 192.168.1.2 [op=REQUEST, sender=66:79:CF:A6:06:D6|192.168.1.1, target=FF:FF:FF:FF:FF:FF|192.168.1.2]



le paquet 1 est la machine 1 qui demande à tout le reseau (target @FF:FF:FF:FF:FF:FF) "EH QUI SAIT QUI C LE .2???"

le paquet 2 est la réponse donnant l'@MAC correspondante

un exemple sur un reseau domestique:

Time	Source	Destination	Protocol	Length	Info
15.095843560	Netgear [redacted]	Intel [redacted]	ARP	42	Who has 192.168.1.57? Tell 192.168.1.101
15.095894633	Intel [redacted]	Netgear [redacted]	ARP	42	192.168.1.57 is at 5c:5f:67:[redacted]
15.458617229	AnovFrance [redacted]	Intel [redacted]	ARP	42	Who has 192.168.1.57? Tell 192.168.1.1
15.458663558	Intel [redacted]	AnovFrance [redacted]	ARP	42	192.168.1.57 is at 5c:5f:67:[redacted]
15.810889515	Netgear [redacted]	Broadcast	ARP	42	Who has 99.86.91.14? Tell 192.168.1.101
18.151502574	MS-NLB-PhysServer [redacted]	Intel [redacted]	ARP	42	Who has 192.168.1.57? Tell 192.168.1.124
18.151512957	Intel [redacted]	MS-NLB-PhysServer [redacted]	ARP	42	192.168.1.57 is at 5c:5f:67:[redacted]


yapudjus@thickpad:~ — Konsole

New Tab Split View

```

[~] [~] arp -n
Address      HWtype  HWaddress      Flags Mask      Iface
192.168.1.75 ether    28:6f:40:      C               wlp3s0
192.168.1.124 ether    02:38:3e:      C               wlp3s0
192.168.1.132 ether    74:df:bf:      C               wlp3s0
192.168.1.101 ether    94:a6:7e:      C               wlp3s0
192.168.1.1  ether    30:7c:b2:      C               wlp3s0
192.168.1.10 ether    10:4f:a8:      C               wlp3s0

[yapudjus@thickpad] - [~] - [10005]
[~] [~] ifconfig wlp3s0
wlp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.1.57 netmask 255.255.255.0 broadcast 192.168.1.255
  
```



conclusion sur ARP

nous pouvons déduire que le protocole ARP permet de lier les @MAC[physiques] et les ports du switch sur un réseau

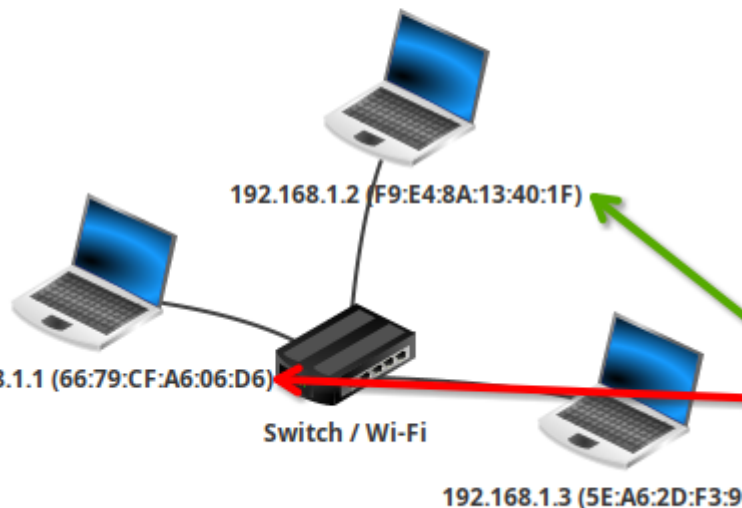
CAM/SAT

nous constatons en 1er que la table cam/sat du switch est vide

nous lançons ensuite un ping vers .2

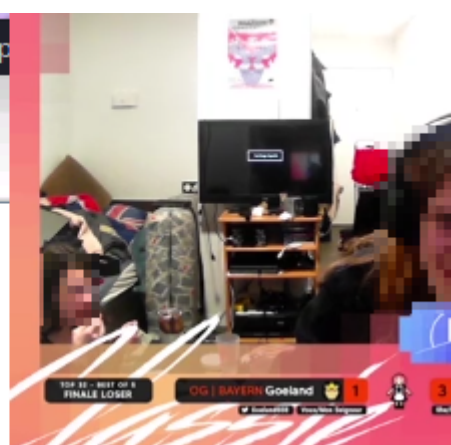
FILIUS - /home/yapudjus/Documents/cours/SIN/SIN/S7 - IoT/TP/tp

90%



Switch / Wi-Fi

MAC	Port	Dernière mise à jour
F9:E4:8A:13:40:1F	Port 2	22:50:59
66:79:CF:A6:06:D6	Port 1	22:50:59



nous pouvons constater que les appareils ayant communiqué apparaissent désormais sur la table du switch

Échanges de données

192.168.1.3 X

No.	Date	Source	Destination	Protocole	Couche	Commentaire / Détail
1	22:49:09.872	192.168.1.1	192.168.1.2	ARP	Internet	Recherche de l'adresse MAC associée à 192.168.1.2 [op=REQUEST, sender=66:79:CF:A6:06:D6]
2	22:50:56.188	192.168.1.1	192.168.1.2	ARP	Internet	Recherche de l'adresse MAC associée à 192.168.1.2 [op=REQUEST, sender=66:79:CF:A6:06:D6]

No.: 1 / Date: 22:49:09.872

Réseau

Source: 66:79:CF:A6:06:D6

Destination: FF:FF:FF:FF:FF:FF

Commentaire / Détail: 0x806

Internet


Source: 192.168.1.1

Destination: 192.168.1.2

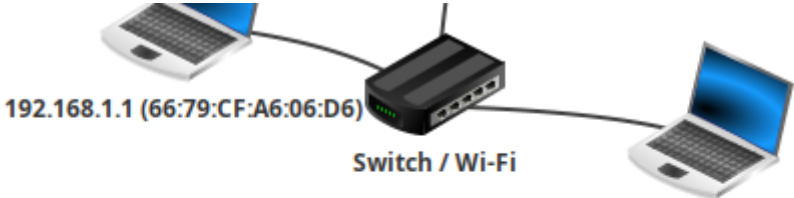
Protocole: ARP

Commentaire / Détail:

Recherche de l'adresse MAC associée à 192.168.1.2 [op=REQUEST, sender=66:79:CF:A6:06:D6|192.168.1.1, target=FF:FF:FF:FF:FF:FF|192.168.1.2]



de plus, l'appareil .3 à reçu une reqt ARP, cependant, **elle n'y a pas rep**
désormais, nous envoyons un ping vers .3, et pouvons constater que la table s'enrichie avec le port et l'@mac de la machine .3



192.168.1.1 (66:79:CF:A6:06:D6)

Switch / Wi-Fi

192.168.1.3 (5E:A6:2D:F3:90:E4)

Table SAT Switch / Wi-Fi

MAC	Port	Dernière mise à jour
F9:E4:8A:13:40:1F	Port 2	23:00:23
5E:A6:2D:F3:90:E4	Port 3	23:00:29
66:79:CF:A6:06:D6	Port 1	23:00:29

de+, .3 recoit un autre ARP req, y repondant cette fois car elle connaît l'@mac demandée (~~normal~~ c'est elle)

4	23:00:26.372	192.168.1.1	192.168.1.3	ARP	Internet	Recherche de l'adresse MAC associée à 192.168.1.3 [...]
5	23:00:26.391	192.168.1.3	192.168.1.1	ARP	Internet	L'adresse MAC est 5E:A6:2D:F3:90:E4 [op=REPLY, send...

conclusion?

la table CAM/SAT permet au switch de savoir "où est qui", afin de distribuer les paquets aux bons destinataires, et pas juste envoyer le paquet à tt le monde

Routeur et passerelle

sans configurer nôtre passerelle

depuis 192.168.0.1, les machines suivantes sont:

- 192.168.0.2 : **accessible**
- 192.168.0.3 : **accessible**
- 192.168.2.1 : non
- 192.168.2.2 : non

en conf uniquement la passerelle

depuis 192.168.0.1, les machines suivantes sont:

- 192.168.0.2 : **accessible**
- 192.168.0.3 : **accessible**
- 192.168.2.1 : non
- 192.168.2.2 : non

En configurant aussi les ordinateurs

depuis 192.168.0.1, les machines suivantes sont:

- 192.168.0.2 : **accessible**
- 192.168.0.3 : **accessible**
- 192.168.2.1 : **accessible**
- 192.168.2.2 : **accessible** en tracant la route entre .0.1 et .2.1, on voit que la passerelle sert de... bah passerelle

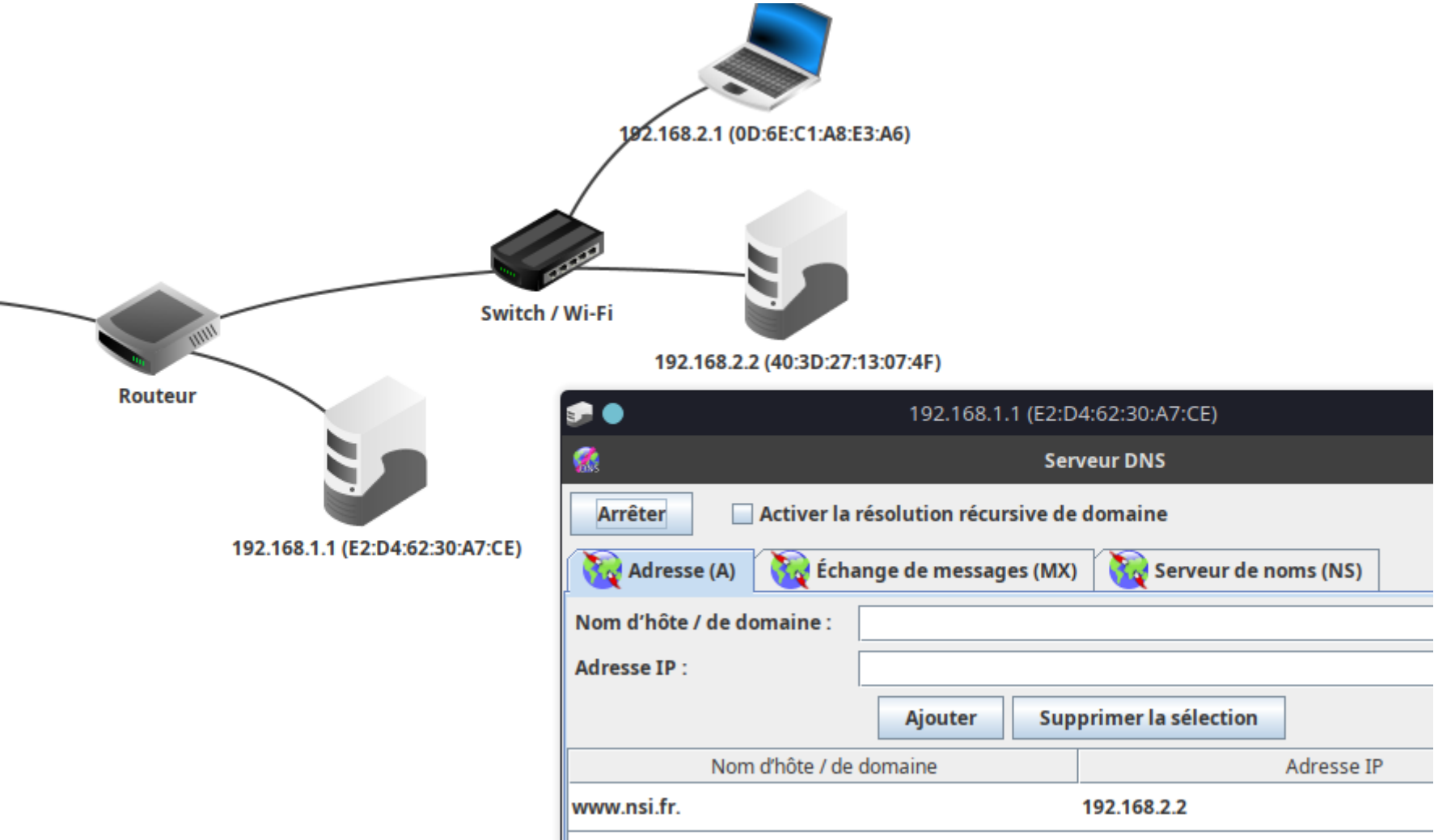
```
> traceroute 192.168.2.1
Établissement de la connexion avec 192.168.2.1 (en 20 sauts max.).
 0  192.168.0.254
 1  192.168.2.1
```

conclusion passerelle

dans ce TP, nous avons vu l'utilité des passerelles qui permettent de faire communiquer des machines de différents réseaux entre elles, en servant de... ponts (yep j'arrête la blague)

DNS

on configure un ordinateur sur le reseau comme un serveur DNS et on ajoute une entrée dans sa table de liaison



en effectuant un ping vers `www.nsi.fr` depuis .0.3, on remarque deux échanges DNS

192.168.0.3:49405	192.168.1.1:53	DNS	Application	ID=42420 QR=0 RCODE=0 QDCOUNT=1 ANCOUNT=0 NSCOUNT=0 ARCOUNT=0	www.nsi.fr. A IN
192.168.1.1:53	192.168.0.3:49405	DNS	Application	ID=42420 QR=1 RCODE=0 QDCOUNT=0 ANCOUNT=1 NSCOUNT=0 ARCOUNT=0	www.nsi.fr. A 3600 192.168.2.2

WEB

en ayant un srvweb sur .2.2 {www.nsi.fr}

Échanges de données						
No.	Date	Source	Destination	Protocole	Couche	Commentaire / Détail
1	08:52:41.349	192.168.0.3:43627	192.168.1.1:53	DNS	Application	ID=60702 QR=0 RCODE=0 QDCOUNT=1 ANCOUNT=0 NSCOUNT=0 ARCOUNT=0 www.nsi.fr. A IN
2	08:52:41.718	192.168.1.1:53	192.168.0.3:43627	DNS	Application	ID=60702 QR=1 RCODE=0 QDCOUNT=0 ANCOUNT=1 NSCOUNT=0 ARCOUNT=0 www.nsi.fr. A 3600 192.168.2.2
3	08:52:41.720	192.168.0.3:52940	192.168.2.2:80	TCP	Transport	SYN, SEQ: 8 000 000
4	08:52:42.184	192.168.2.2:80	192.168.0.3:52940	TCP	Transport	SYN, SEQ: 7 000 000, ACK: 8 000 001
5	08:52:42.191	192.168.0.3:52940	192.168.2.2:80	TCP	Transport	SEQ: 8 000 001, ACK: 7 000 001
6	08:52:42.283	192.168.0.3:52940	192.168.2.2:80	HTTP	Application	GET / HTTP/1.1 Host: www.nsi.fr
7	08:52:42.758	192.168.2.2:80	192.168.0.3:52940	TCP	Transport	SEQ: 7 000 001, ACK: 8 000 033
8	08:52:42.833	192.168.2.2:80	192.168.0.3:52940	HTTP	Application	HTTP/1.1 200 OK Content-type: text/html <html> <head> <meta charset="UTF-8"> <title>Page d...
9	08:52:42.859	192.168.0.3:52940	192.168.2.2:80	TCP	Transport	SEQ: 8 000 033, ACK: 7 000 616
10	08:52:42.932	192.168.0.3:52940	192.168.2.2:80	HTTP	Application	GET splashscreen-mini.png HTTP/1.1 Host: www.nsi.fr
11	08:52:43.401	192.168.2.2:80	192.168.0.3:52940	TCP	Transport	SEQ: 7 000 616, ACK: 8 000 085
12	08:52:43.463	192.168.2.2:80	192.168.0.3:52940	HTTP	Application	HTTP/1.1 200 OK Content-type: image/png iVBORw0KGgoAAAANSUHEUgAAAIAAAABgCAYAAADVenpJAAAAAXNSR0IArs4c...
13	08:52:43.471	192.168.0.3:52940	192.168.2.2:80	TCP	Transport	SEQ: 8 000 085, ACK: 7 002 076
14	08:52:43.945	192.168.2.2:80	192.168.0.3:52940	HTTP	Application	J285HmH0qGH4aXrASU0R1BnxDMAWb58uasHZSk0TKR8 8kGKILIJ89squ0ZSQu2knnpHfNqgdRAApFIENvIVXQAbYQeAA3JqfwK5...
15	08:52:43.952	192.168.0.3:52940	192.168.2.2:80	TCP	Transport	SEQ: 8 000 085, ACK: 7 003 536
16	08:52:44.421	192.168.2.2:80	192.168.0.3:52940	HTTP	Application	SsqATIZhcoDx90PpgCn0GF/t4Wem0x1DEbnZEcvi+EF6yD Z0aXLX86TagAKKTSSdo/JGVctEAiBeUhJXn/554ZFT1kAet1RFW0n2...
17	08:52:44.424	192.168.0.3:52940	192.168.2.2:80	TCP	Transport	SEQ: 8 000 085, ACK: 7 004 996
18	08:52:44.893	192.168.2.2:80	192.168.0.3:52940	HTTP	Application	Mb9u2rWM+kgCQcCEEewEKLbc85vM+kQAZAKG3Pvfcc248j94N gwnkgZU/ffp0x2iAgHgXAJACRx11VPpeQhgTRrk5A6AiVmNVj4v...
19	08:52:44.921	192.168.0.3:52940	192.168.2.2:80	TCP	Transport	SEQ: 8 000 085, ACK: 7 006 456
20	08:52:45.379	192.168.2.2:80	192.168.0.3:52940	HTTP	Application	cK4FHWZZnSvmW50hH1rdMT9a/TvN9hy/3v4+eImV9Jtju3W+14Lm 16WkQmsbPfmkgCgmUAYmTJpsh2x32HW6IqjrX279m5r1iOP...
21	08:52:45.383	192.168.0.3:52940	192.168.2.2:80	TCP	Transport	SEQ: 8 000 085, ACK: 7 007 916
22	08:52:45.859	192.168.2.2:80	192.168.0.3:52940	HTTP	Application	V0yHM6E6aAaAzJugRbHm1ia1njxo3t2G0PdSd8YTiSgQ0l/ocvZSqi GXRr0CoibgBA44DeGpWHKBgagICvYbPRAuYyNMJBHijGQ...
23	08:52:45.868	192.168.0.3:52940	192.168.2.2:80	TCP	Transport	SEQ: 8 000 085, ACK: 7 009 054
24	08:52:45.956	192.168.0.3:52940	192.168.2.2:80	TCP	Transport	FIN, SEQ: 8 000 085

les paquets sont les suivants:

- 1&2: resolution du domaine via le dns
- 6: requete de la page parent du site (/)
- 8: reponse du site et retour de la page parent (/)
- 10&{12,14,16,18,20,22}: requete et reponse de l'image du site

http vs https

en http, on voit que tout est transmi en clair, par exemple (en local):

```

Transmission Control Protocol, Src Port: 38162, Dst Port: 8989, Seq: 1, Ack: 1, Len: 1754
Hypertext Transfer Protocol
  GET /signalr/messages?access_token=[REDACTED] HTTP/1.1\r\n
  Host: 127.0.0.1:8989\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:122.0) Gecko/20100101 Firefox/122.0\r\n
  Accept: */*\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate, br\r\n
  Sec-WebSocket-Version: 13\r\n
  Origin: http://127.0.0.1:8989\r\n
  Sec-WebSocket-Extensions: permessage-deflate\r\n
  Sec-WebSocket-Key: g9P[REDACTED]\r\n
  Authorization: Basic e[REDACTED]:4MA==\r\n
  Credentials: yapudjus:[REDACTED]
  Connection: keep-alive, Upgrade\r\n
  [truncated]Cookie: connect.sid=[REDACTED]; Jackett=[REDACTED]
  Sec-Fetch-Dest: empty\r\n
  Sec-Fetch-Mode: websocket\r\n
  Sec-Fetch-Site: same-origin\r\n
  Pragma: no-cache\r\n

```

tandis qu'en https, en prenant l'exemple de parcoursup, aucun trafic n'est lisible

ip.addr==193.54.151.206

No.	Time	Source	Destination	Protocol	Length	Info
3329...	142.870737083	192.168.1.73	193.54.151.206	TCP	76	44500 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2543453157 TSecr=0 WS=128
3329...	142.902132806	193.54.151.206	192.168.1.73	TCP	76	443 → 44500 [SYN, ACK] Seq=0 Ack=1 Win=14160 Len=0 MSS=1416 WS=1 SACK_PERM TSval=2623510151 TSecr=25434531...
3329...	142.902158530	192.168.1.73	193.54.151.206	TCP	68	44500 → 443 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=2543453188 TSecr=2623510151
3329...	142.906927476	192.168.1.73	193.54.151.206	TLSv1.2	420	Client Hello (SNI=authentication.parcoursup.fr)
3329...	142.933683653	193.54.151.206	192.168.1.73	TCP	68	443 → 44500 [ACK] Seq=1 Ack=353 Win=14512 Len=0 TSval=2623510187 TSecr=2543453193
3329...	142.940367635	193.54.151.206	192.168.1.73	TLSv1.2	6150	Server Hello, Certificate, Server Key Exchange, Server Hello Done
3329...	142.940390401	192.168.1.73	193.54.151.206	TCP	68	44500 → 443 [ACK] Seq=353 Ack=6083 Win=31872 Len=0 TSval=2543453227 TSecr=2623510193
3329...	142.941859831	192.168.1.73	193.54.151.206	TLSv1.2	194	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
3329...	142.969265225	193.54.151.206	192.168.1.73	TCP	68	443 → 44500 [ACK] Seq=6083 Ack=479 Win=14638 Len=0 TSval=2623510222 TSecr=2543453228
3329...	142.969265429	193.54.151.206	192.168.1.73	TLSv1.2	119	Change Cipher Spec, Encrypted Handshake Message
3329...	142.979502365	192.168.1.73	193.54.151.206	TLSv1.2	842	Application Data
3329...	142.979952614	192.168.1.73	193.54.151.206	TLSv1.2	267	Application Data
3330...	143.006787565	193.54.151.206	192.168.1.73	TCP	68	443 → 44500 [ACK] Seq=6134 Ack=1452 Win=15611 Len=0 TSval=2623510259 TSecr=2543453266
3330...	143.083141225	193.54.151.206	192.168.1.73	TCP	81	443 → 44500 [ACK] Seq=6134 Ack=1452 Win=15611 Len=13 TSval=2623510336 TSecr=2543453266 [TCP segment of a r...
3330...	143.083142499	193.54.151.206	192.168.1.73	TLSv1.2	1953	Application Data
3330...	143.083193232	192.168.1.73	193.54.151.206	TCP	68	44500 → 443 [ACK] Seq=1452 Ack=8032 Win=31872 Len=0 TSval=2543453369 TSecr=2623510336
3330...	143.252464460	192.168.1.73	193.54.151.206	TLSv1.2	714	Application Data
3330...	143.279021177	193.54.151.206	192.168.1.73	TCP	68	443 → 44500 [ACK] Seq=8032 Ack=2098 Win=16257 Len=0 TSval=2623510532 TSecr=2543453539
3330...	143.301770926	193.54.151.206	192.168.1.73	TCP	81	443 → 44500 [ACK] Seq=8032 Ack=2098 Win=16257 Len=13 TSval=2623510555 TSecr=2543453539 [TCP segment of a r...
3330...	143.301771132	193.54.151.206	192.168.1.73	TLSv1.2	1996	Application Data
3330...	143.301795133	192.168.1.73	193.54.151.206	TCP	68	44500 → 443 [ACK] Seq=2098 Ack=9973 Win=31872 Len=0 TSval=2543453588 TSecr=2623510555
4090...	163.305468152	193.54.151.206	192.168.1.73	TCP	68	443 → 44500 [FIN, ACK] Seq=9973 Ack=2098 Win=16257 Len=0 TSval=2623530555 TSecr=2543453588
4090...	163.305972877	192.168.1.73	193.54.151.206	TCP	68	44500 → 443 [FIN, ACK] Seq=2098 Ack=9974 Win=31872 Len=0 TSval=2543473592 TSecr=2623530555
4091...	163.333888765	193.54.151.206	192.168.1.73	TCP	68	443 → 44500 [ACK] Seq=9974 Ack=2099 Win=16257 Len=0 TSval=2623530586 TSecr=2543473592

[Next Sequence Number: 353 (relative sequence number)]
Acknowledgment Number: 6083 (relative ack number)
Acknowledgment number (raw): 1658437910
1000 = Header Length: 32 bytes (8)
Flags: 0x010 (ACK)
Window: 249
[Calculated window size: 31872]
[Window size scaling factor: 128]
Checksum: 0x8b8f [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[Timestamps]
[SEQ/ACK analysis]

0000 00 04 00 01 00 06 5c 5f 67 3c 64 1e 4a dd 08 00 \ g<d .J ...
0010 45 00 00 34 a9 4c 40 00 40 06 76 81 c0 a8 01 49 E..4.L@. @.v....I
0020 c1 36 97 ce ad d4 01 bb 7d 64 af 83 62 d9 c1 16 .6..... }d..b...
0030 80 10 00 f9 8b 8f 00 00 01 01 08 0a 97 9a 04 2b +
0040 9c 5f 96 b1 _..

Source or Destination Address: IPv4 addressPackets: 514008 · Displayed: 719 (0.1%)Profile: Default

cependant, ce système est (difficilement) contournable par une attaque par mitm, ainsi qu'un contournement de certificat ou une injection de certificat auprès du client, nous donnant accès au trafic

Double authmitmprox

127.0.0.1:8081/#/flows/07714e27-4aac-482c-a391-629eba3feacd/request

FileStartOptionsFlow

ReplayDuplicateRevertDeleteMarkExportResumeAbort

Flow ModificationExportInterception

Path	Method	Status	Size	Time	Request	Response	Connection	Timing
https://dossier.parcoursup.fr/Candidat/authentification?redir...	GET	302		0 40ms	GET https://dossier.parcoursup.fr/Candidat/authorize?redirect=compte	HTTP/1.1		
https://dossier.parcoursup.fr/Candidat/authorize?redirect=c...	GET	302		0 41ms	Host: dossier.parcoursup.fr			
https://authentification.parcoursup.fr/Authentification/oa...	GET	302		0 46ms	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:122.0) Gecko/20100101 Firefox/122.0			
https://dossier.parcoursup.fr/Candidat/callback?code=1esxm...	GET	302		0 128ms	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8			
https://dossier.parcoursup.fr/Candidat/authentification?ACTI...	GET	302		0 58ms	Accept-Language: en-US,en;q=0.5			
https://dossier.parcoursup.fr/Candidat/candidatures.liste	GET	302		0 43ms	Accept-Encoding: gzip, deflate, br			
https://dossier.parcoursup.fr/Candidat/doubleAuthenticati...	GET	200	23.9kb	51ms	Referer: https://dossier.parcoursup.fr/Candidat/authentification?mode=connecter			
https://ressource.parcoursup.fr/js/jquery/jquery-3.4.1.min.js	GET	404	196b	48ms	Connection: keep-alive			
https://ressource.parcoursup.fr/js/jquery/jquery-3.4.1.min.js	GET	404	196b	!	Cookie: JSESSIONID= cookiePsup=!			
https://ressource.parcoursup.fr/css/dsfr/dist/icons/system/a...	GET	200	120b	43ms	atinternet=true;			
https://ressource.parcoursup.fr/css/dsfr/dist/icons/business...	GET	200	288b	49ms	atuserid=%7B%2			
https://ressource.parcoursup.fr/css/dsfr/dist/icons/user/acc...	GET	200	462b	75ms	bbbb-454b-9bb7			
https://ressource.parcoursup.fr/css/dsfr/dist/icons/system/l...	GET	200	219b	77ms	Upgrade-Insecure-Requests: 1			
https://ressource.parcoursup.fr/css/dsfr/dist/fonts/Mariann...	GET	200	43.2kb	116ms	Sec-Fetch-Dest: document			

*:8080mitmproxy 10.2.2

(ici, le certificat d'autorité unique à mon proxy d'ecoute a été ajoutté en confiance sur firefox, seulement sur un conteneur d'ecoute)

conclusion http,s

l'usage du protocole https est à privilégier car il permet une "sécurité" dans l'echange de données, tandis qu'une communication http classique est visible de tous, cependant, d'autres mesures sécurité sont à prendre, comme les classiques "ne pas cliquer sur tout les liens", "ne pas entrer ses info partout" et "retaper le lien à la main pour éviter des remplacements de lettres (ex: remplacer le a de amazon.fr avec un symbole russe ressemblant à un a)"