

COMPTE RENDU

Reseau - TP2 - Configuration Réseau et Analyse de Protocoles
3e année Cybersécurité - École Supérieure d'Informatique et du
Numérique (ESIN)
Collège d'Ingénierie & d'Architecture (CIA)

Étudiant : HATHOUTI Mohammed Taha
Filière : Cybersecurité
Année : 2025/2026
Enseignante : Mme.FADI
Date : 7 octobre 2025

1 Objectifs du TP

Les objectifs principaux de ce TP sont :

- Configuration d’adressage IP sur machines Linux (Ubuntu) et Windows ;
- Étude pratique des protocoles ARP et ICMP ;
- Utilisation d’outils d’analyse réseau : Wireshark ;
- Analyse comparative de différentes topologies réseau ;

2 Configuration du réseau

2.1 Architecture matérielle

Pour ce laboratoire, nous avons utilisé une configuration physique composée de :

- Une machine physique Ubuntu (Machine hôte avec adaptateur USB-C vers Ethernet) ;
- Une machine Windows 7 (Unité centrale avec port Ethernet intégré) ;
- Un câble Ethernet pour la connexion directe ;

Cette configuration remplace l’utilisation de machines virtuelles en mode ”Host only”. Contraint d’adopter cette approche en raison des difficultés rencontrées pour installer un VMware sur mon Ubuntu, j’ai finalement découvert qu’il était bien plus pratique, instructif et marquant de travailler sur de véritables machines physiques en réalisant soit même le montage offrant ainsi une expérience réseau réelle.

2.2 Questions théoriques

2.2.1 Question 1 : Équipement pour connecter trois machines physiques

Pour connecter trois machines physiques, on peut utiliser :

- **Switch** : Équipement intelligent qui transmet les trames uniquement au host concerné en utilisant les adresses MAC ;
- **Hub** : Équipement diffusant les données à tous les hosts connectés, agissant ainsi comme un Broadcast ;

2.2.2 Question 2 : Différence entre Hub et Switch

Critère	Hub	Switch
Fonctionnement	Diffuse à tous les hosts	Transmet uniquement au host concerné
Performance	Collisions fréquentes très fréquentes (vu en TP l’année dernière)	Pas de collisions
Sécurité	Faible (agissant comme un Broadcast)	Meilleure

TABLE 1 – Comparaison Hub vs Switch

2.3 Configuration IP

Nous avons choisi un réseau de **Classe C** avec l'adresse réseau **192.168.1.0/24**.

Machine	Adresse IP	Masque	Interface
Ubuntu	192.168.1.1	255.255.255.0	enx0c3796401539
Windows 7	192.168.1.2	255.255.255.0	Connexion réseau local

TABLE 2 – Plan d'adressage du réseau

2.3.1 Configuration sur Ubuntu

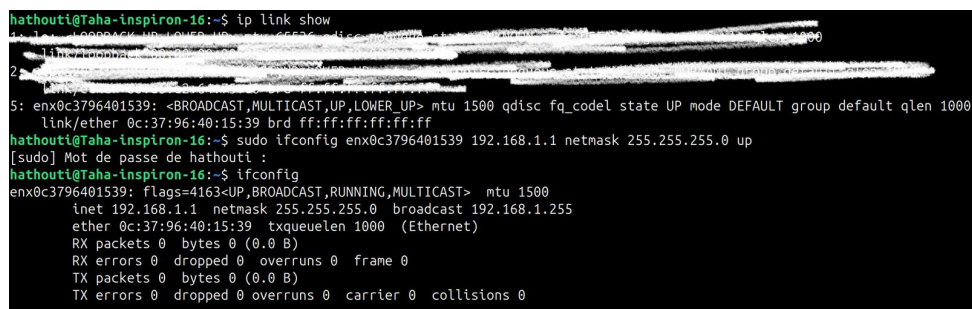
L'interface réseau utilisée est l'adaptateur USB-C Ethernet : **enx0c3796401539**.

Commande de configuration :

```
sudo ifconfig enx0c3796401539 192.168.1.1 netmask 255.255.255.0  
up
```

Vérification de la configuration :

```
ifconfig //ou ip addr show enx0c3796401539
```



```
hathouti@Taha-inspiron-16:~$ ip link show  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UP mode DEFAULT group default qlen 1000  
link/ether 00:00:00:00:00:00  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000  
link/ether 0c:37:96:40:15:39 brd ff:ff:ff:ff:ff:ff  
hathouti@Taha-inspiron-16:~$ sudo ifconfig enx0c3796401539 192.168.1.1 netmask 255.255.255.0 up  
[sudo] Mot de passe de hathouti :  
hathouti@Taha-inspiron-16:~$ ifconfig  
enx0c3796401539: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.1.1 netmask 255.255.255.0 broadcast 192.168.1.255  
    ether 0c:37:96:40:15:39 txqueuelen 1000 (Ethernet)  
    RX packets 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 0 bytes 0 (0.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

FIGURE 1 – Configuration de l'interface réseau Ubuntu

2.3.2 Configuration sur Windows 7

Commande de configuration (CMD en administrateur) :

```
netsh interface ip set address "Connexion au r seau local"  
static 192.168.1.2 255.255.255.0
```

Vérification de la configuration :

```
ipconfig
```


3.2 Manipulation de la table ARP

3.2.1 Commandes ARP utilisées

Affichage de la table ARP :

```
# Ubuntu
arp -a

# Windows
arp -a
```

Suppression des entrées ARP :

```
# Ubuntu
sudo ip -s -s neigh flush all

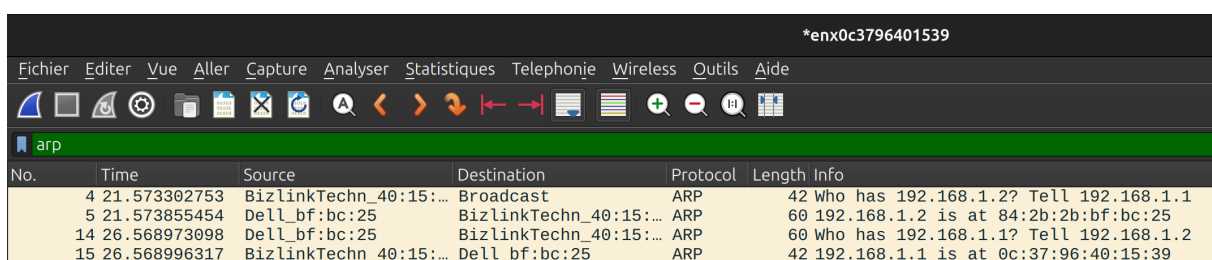
# Windows
arp -d *
```

3.3 Capture et analyse avec Wireshark

3.3.1 Procédure de capture

1. Vidage de la table ARP sur les deux machines ;
2. Lancement de Wireshark sur Ubuntu (interface `enx0c3796401539`) ;
3. Application du filtre : `arp` ;
4. Exécution d'un ping depuis Ubuntu vers Windows ;
5. Observation des paquets ARP capturés ;

3.3.2 Paquets ARP capturés



No.	Time	Source	Destination	Protocol	Length	Info
4	21.573302753	BizlinkTechn_40:15:...	Broadcast	ARP	42	Who has 192.168.1.2? Tell 192.168.1.1
5	21.573855454	Dell_bf:bc:25	BizlinkTechn_40:15:...	ARP	60	192.168.1.2 is at 84:2b:2b:bf:bc:25
14	26.568973098	Dell_bf:bc:25	BizlinkTechn_40:15:...	ARP	60	Who has 192.168.1.1? Tell 192.168.1.2
15	26.568996317	BizlinkTechn_40:15:...	Dell_bf:bc:25	ARP	42	192.168.1.1 is at 0c:37:96:40:15:39

FIGURE 4 – Capture Wireshark - Paquets ARP uniquement

Analyse des paquets observés :

— **Paquet 4 - ARP Request :**

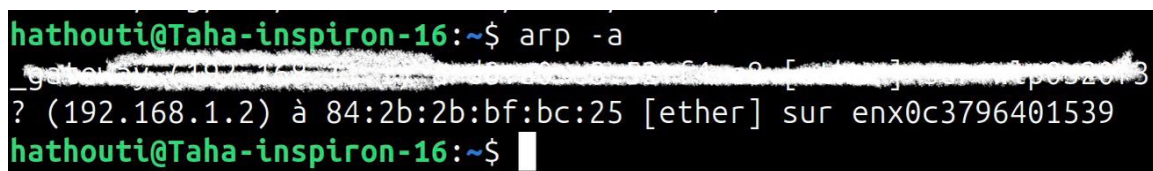
- Source : BizlinkTechn (Ubuntu - MAC : 0c :37 :96 :40 :15 :39)
- Destination : Broadcast (ff :ff :ff :ff :ff :ff)
- Message : "Who has 192.168.1.2? Tell 192.168.1.1"
- Type : Requête en broadcast (diffusée à tous)

- **Paquet 5 - ARP Reply :**
 - Source : Dell (Windows - MAC : 84 :2b :2b :bf :bc :25)
 - Destination : BizlinkTechn (Ubuntu)
 - Message : "192.168.1.2 is at 84 :2b :2b :bf :bc :25"
 - Type : Réponse en unicast (dirigée uniquement vers l'émetteur)

3.4 Tables ARP après résolution

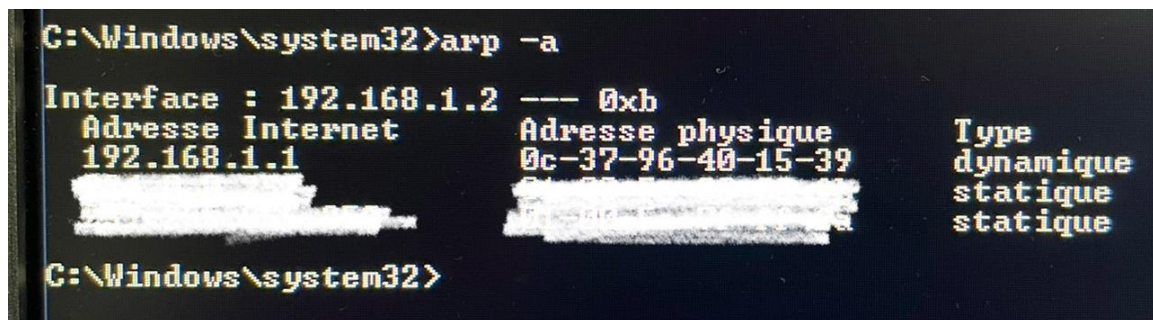
3.4.1 Table ARP sur Ubuntu

```
$ arp -a
? (192.168.1.2) at 84:2b:2b:bf:bc:25 [ether] on enx0c3796401539
```



```
hathouti@Taha-inspiron-16:~$ arp -a
? (192.168.1.2) à 84:2b:2b:bf:bc:25 [ether] sur enx0c3796401539
hathouti@Taha-inspiron-16:~$
```

FIGURE 5 – Table ARP Ubuntu après résolution



```
C:\Windows\system32>arp -a

Interface : 192.168.1.2 --- 0xb
  Adresse Internet    Adresse physique    Type
  192.168.1.1         0c-37-96-40-15-39  dynamique
  [redacted]           [redacted]          statique
  [redacted]           [redacted]          statique

C:\Windows\system32>
```

FIGURE 6 – Table ARP Windows après résolution

4 Exploration du protocole ICMP

4.1 Présentation du protocole ICMP

Le protocole ICMP (Internet Control Message Protocol) est utilisé pour :

- Tester la connectivité réseau (commande **ping**) ;
- Transmettre des messages d'erreur et de diagnostic ;
- Mesurer le temps de réponse réseau ;

Types de messages ICMP :

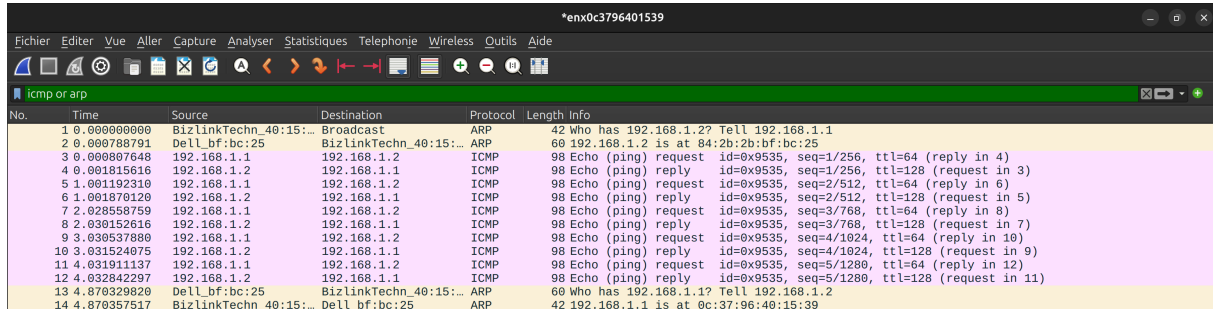
- Echo Request (requête ping)
- Echo Reply (réponse ping)

4.2 Tests de connectivité avec ping

4.2.1 Ping Ubuntu vers Windows

Commande exécutée :

```
ping -c 5 192.168.1.2
```



The image shows a Wireshark packet capture window titled '*enx0c3796401539'. The filter is 'icmp or arp'. The packet list shows 14 packets. Packets 1-2 are ARP requests and replies. Packets 3-12 are ICMP Echo (ping) requests and replies. Packets 13-14 are ARP requests and replies. The packet details pane shows the selected packet (No. 14) as an ARP request from BizlinkTechn_40:15: to Dell_bf:bc:25.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	BizlinkTechn_40:15:...	Broadcast	ARP	42	Who has 192.168.1.2? Tell 192.168.1.1
2	0.000788791	Dell_bf:bc:25	BizlinkTechn_40:15:...	ARP	60	192.168.1.2 is at 84:2b:2b:bf:bc:25
3	0.000807648	192.168.1.1	192.168.1.2	ICMP	98	Echo (ping) request id=0x9535, seq=1/256, ttl=64 (reply in 4)
4	0.001815616	192.168.1.2	192.168.1.1	ICMP	98	Echo (ping) reply id=0x9535, seq=1/256, ttl=128 (request in 3)
5	1.001192318	192.168.1.1	192.168.1.2	ICMP	98	Echo (ping) request id=0x9535, seq=2/512, ttl=64 (reply in 6)
6	1.001870120	192.168.1.2	192.168.1.1	ICMP	98	Echo (ping) reply id=0x9535, seq=2/512, ttl=128 (request in 5)
7	2.028558759	192.168.1.1	192.168.1.2	ICMP	98	Echo (ping) request id=0x9535, seq=3/768, ttl=64 (reply in 8)
8	2.030152616	192.168.1.2	192.168.1.1	ICMP	98	Echo (ping) reply id=0x9535, seq=3/768, ttl=128 (request in 7)
9	3.030537880	192.168.1.1	192.168.1.2	ICMP	98	Echo (ping) request id=0x9535, seq=4/1024, ttl=64 (reply in 10)
10	3.031524075	192.168.1.2	192.168.1.1	ICMP	98	Echo (ping) reply id=0x9535, seq=4/1024, ttl=128 (request in 9)
11	4.031911137	192.168.1.1	192.168.1.2	ICMP	98	Echo (ping) request id=0x9535, seq=5/1280, ttl=64 (reply in 12)
12	4.032842297	192.168.1.2	192.168.1.1	ICMP	98	Echo (ping) reply id=0x9535, seq=5/1280, ttl=128 (request in 11)
13	4.870329820	Dell_bf:bc:25	BizlinkTechn_40:15:...	ARP	60	Who has 192.168.1.1? Tell 192.168.1.2
14	4.870357517	BizlinkTechn_40:15:...	Dell_bf:bc:25	ARP	42	192.168.1.1 is at 0c:37:96:40:15:39

FIGURE 7 – Résultats ping depuis Ubuntu vers Windows

Résultats observés :

- 5 paquets transmis, 5 reçus (0% de perte)
- Temps de réponse : 0-2 ms (connexion directe très rapide)
- Connectivité bidirectionnelle confirmée

4.2.2 Ping Windows vers Ubuntu

Commande exécutée :

```
ping 192.168.1.1
```

4.3 Capture simultanée ARP et ICMP

4.3.1 Procédure de capture complète

1. Vidage complet des tables ARP sur les deux machines ;
2. Lancement de Wireshark avec filtre : `icmp or arp` ;
3. Exécution de `ping -c 5 192.168.1.2` depuis Ubuntu ;
4. Analyse de la séquence complète des paquets ;

4.3.2 Analyse détaillée de la séquence

Séquence observée dans Wireshark :

1. **Paquets 1-2 : Résolution ARP initiale**
 - ARP Request : "Who has 192.168.1.2?"
 - ARP Reply : "192.168.1.2 is at 84 :2b :2b :bf :bc :25"
2. **Paquets 3-12 : Échange ICMP (5 pings)**
 - Echo Request (Type 8) : seq=1/256, 2/512, 3/768, 4/1024, 5/1280
 - Echo Reply (Type 0) : Réponses correspondantes
 - Temps de réponse (TTL) : 64 pour les requêtes, 128 pour les réponses
3. **Paquets 13-14 : Échange ARP inverse (optionnel)**
 - Windows interroge Ubuntu pour mise à jour de son cache ARP

4.4 Observation importante : Cache ARP

Question du lab : Pourquoi les requêtes ARP n'apparaissent-elles pas avant chaque ping ?

Réponse : Après la première résolution ARP (paquets 1-2), l'adresse MAC du host de destination est stockée dans le cache ARP. Les pings suivants (paquets 3-12) utilisent directement cette information en cache sans nécessiter de nouvelles requêtes ARP.

Cette optimisation permet de :

- Réduire le trafic réseau ;
- Accélérer les communications ultérieures ;
- Diminuer la charge sur le réseau local ;

Le cache ARP a une durée de vie limitée, après laquelle une nouvelle résolution sera nécessaire. C'est pourquoi on remarque dans la *Figure 7* qu'après le dernier *request reply* du 5ème *ping* un nouveau paquet ARP est envoyé, cette fois-ci par le host Windows.

5 Topologies réseau avec Packet Tracer

5.1 Topologie Bus

5.1.1 Configuration

Dans une topologie bus, tous les équipements sont connectés sur un même câble (ligne de transmission).

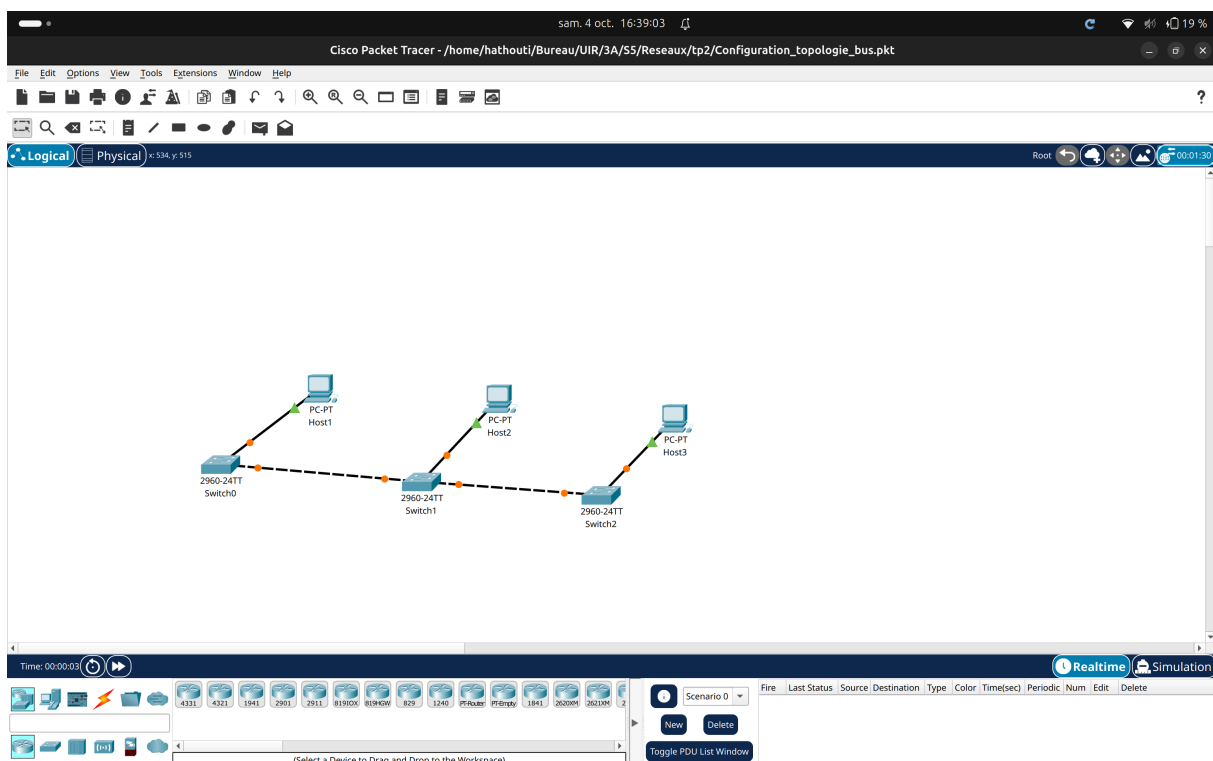


FIGURE 8 – Topologie Bus - Schéma de configuration

Configuration IP :

PC	Adresse IP
Host1	192.168.1.1
Host2	192.168.1.2
Host3	192.168.1.3

TABLE 3 – Adressage topologie Bus

5.1.2 Tests de connectivité

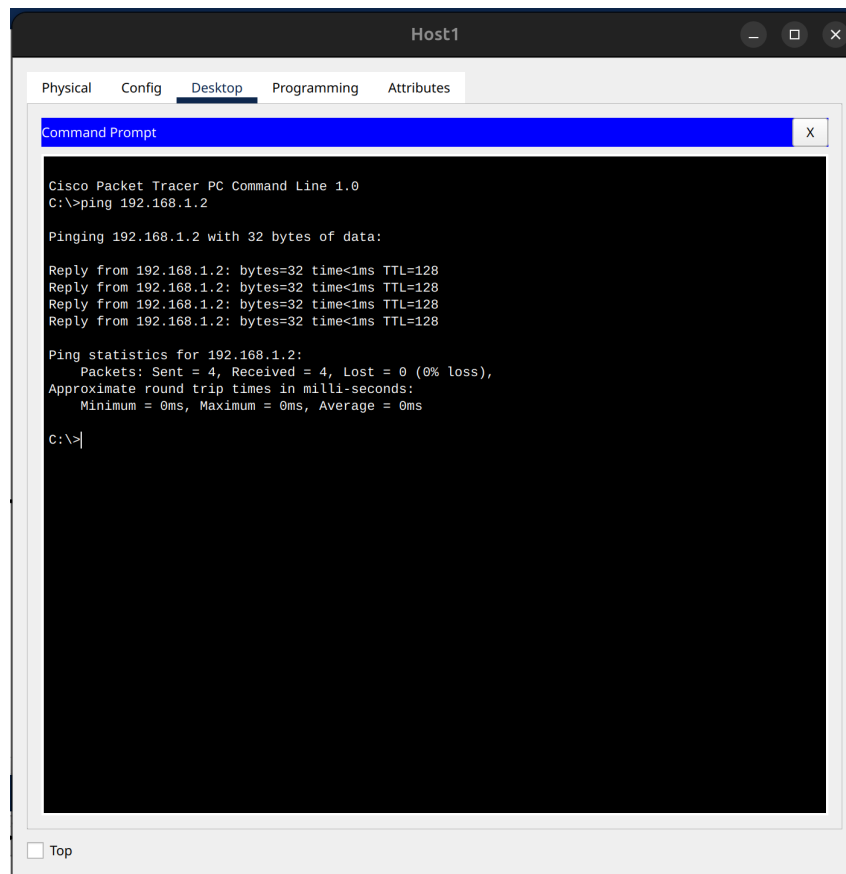


FIGURE 9 – Tests de connectivité - Topologie Bus

- Ping Host1 → Host2 : Succès (4 paquets reçus, 0% perte)
- Temps de réponse : $< 1ms$ (connexion locale)

5.1.3 Avantages et inconvénients

Avantages	Inconvénients
Installation simple et économique	Si le câble principal est coupé, tout le réseau est hors service
Peu de câblage nécessaire	Difficile d'identifier l'origine d'une panne
Facile à étendre	Collisions fréquentes sur le bus partagé

TABLE 4 – Analyse topologie Bus

5.2 Topologie Étoile (Star)

5.2.1 Configuration

Dans une topologie étoile, tous les équipements sont connectés à un Switch central.

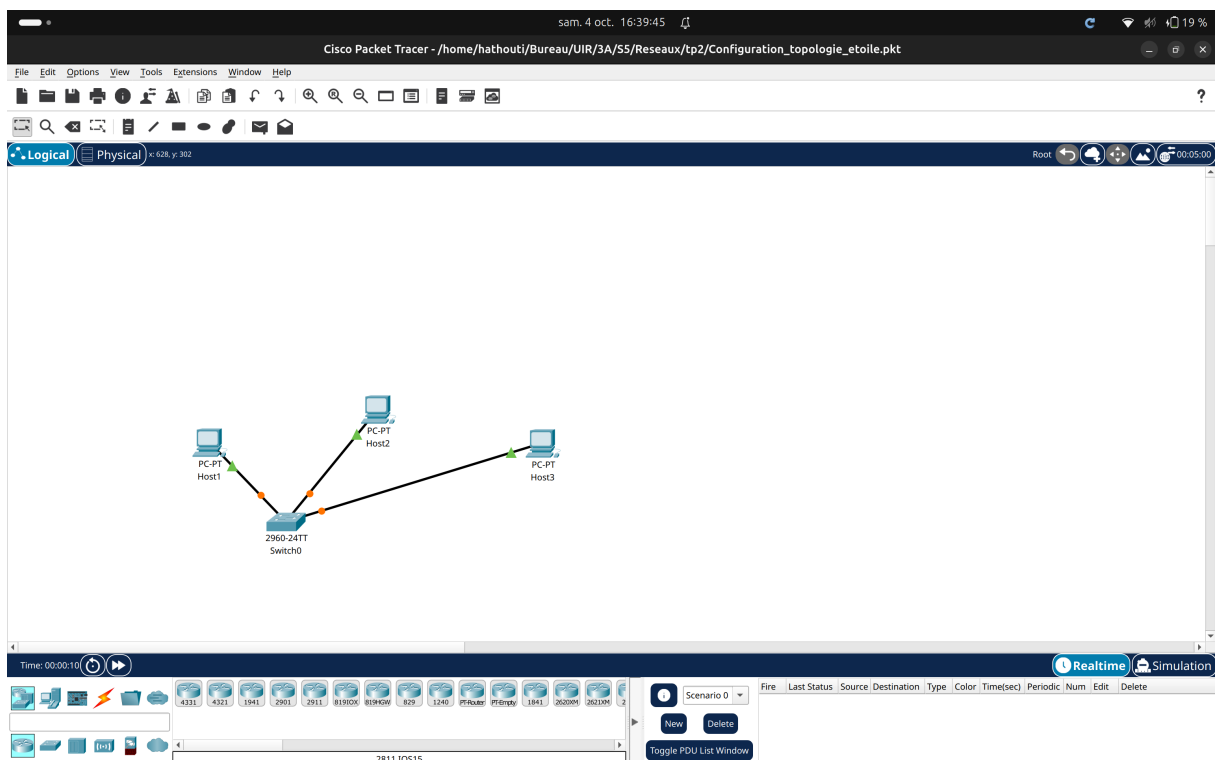


FIGURE 10 – Topologie Étoile - Schéma de configuration

Configuration IP :

PC	Adresse IP
Host1	192.168.1.1
Host2	192.168.1.2
Host3	192.168.1.3

TABLE 5 – Adressage topologie Étoile

5.2.2 Tests de connectivité

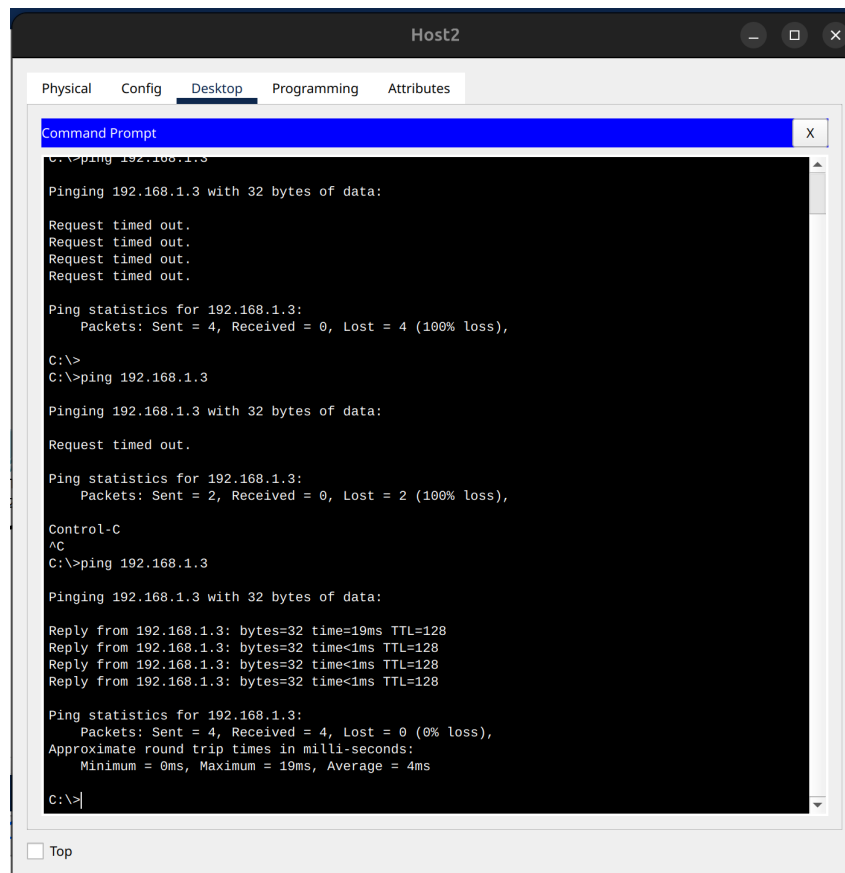


FIGURE 11 – Tests de connectivité - Topologie Étoile

- Ping Host2 → Host3 : Succès (4 paquets reçus, 0% perte)
- Temps de réponse moyen : $< 5ms$

5.2.3 Avantages et inconvénients

Avantages	Inconvénients
Panne isolée à un host	Si le Switch tombe, tout le réseau est hors service
Facile à étendre et reconfigurer	Plus de câblage nécessaire
Bonne performance (pas de collisions)	

TABLE 6 – Analyse topologie Étoile

5.3 Topologie Anneau (Ring)

5.3.1 Configuration

Dans une topologie en anneau, chaque équipement est connecté à deux voisins, formant une boucle fermée.

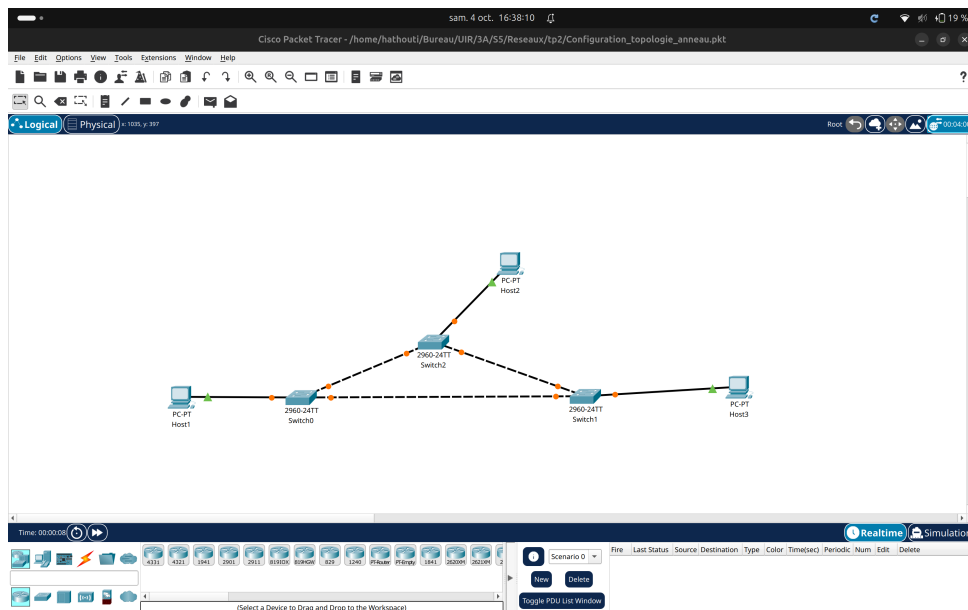


FIGURE 12 – Topologie Anneau - Schéma de configuration

Configuration IP :

PC	Adresse IP
Host1	192.168.1.1
Host2	192.168.1.2
Host3	192.168.1.3

TABLE 7 – Adressage topologie Anneau

5.3.2 Tests de connectivité

```

Host1
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Request timed out.

Ping statistics for 192.168.1.2:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),

Control-C
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
  
```

FIGURE 13 – Tests de connectivité - Topologie Anneau

- Ping Host1 → Host2 : Succès
- Ping Host2 → Host3 : Succès

5.3.3 Avantages et inconvénients

Avantages	Inconvénients
Pas de collisions	Une seule panne peut paralyser tout le réseau Difficile à reconfigurer ou étendre Dépannage complexe

TABLE 8 – Analyse topologie Anneau

5.4 Topologie Maillée (Mesh)

5.4.1 Configuration

Dans une topologie maillée complète, chaque équipement est directement connecté à tous les autres.

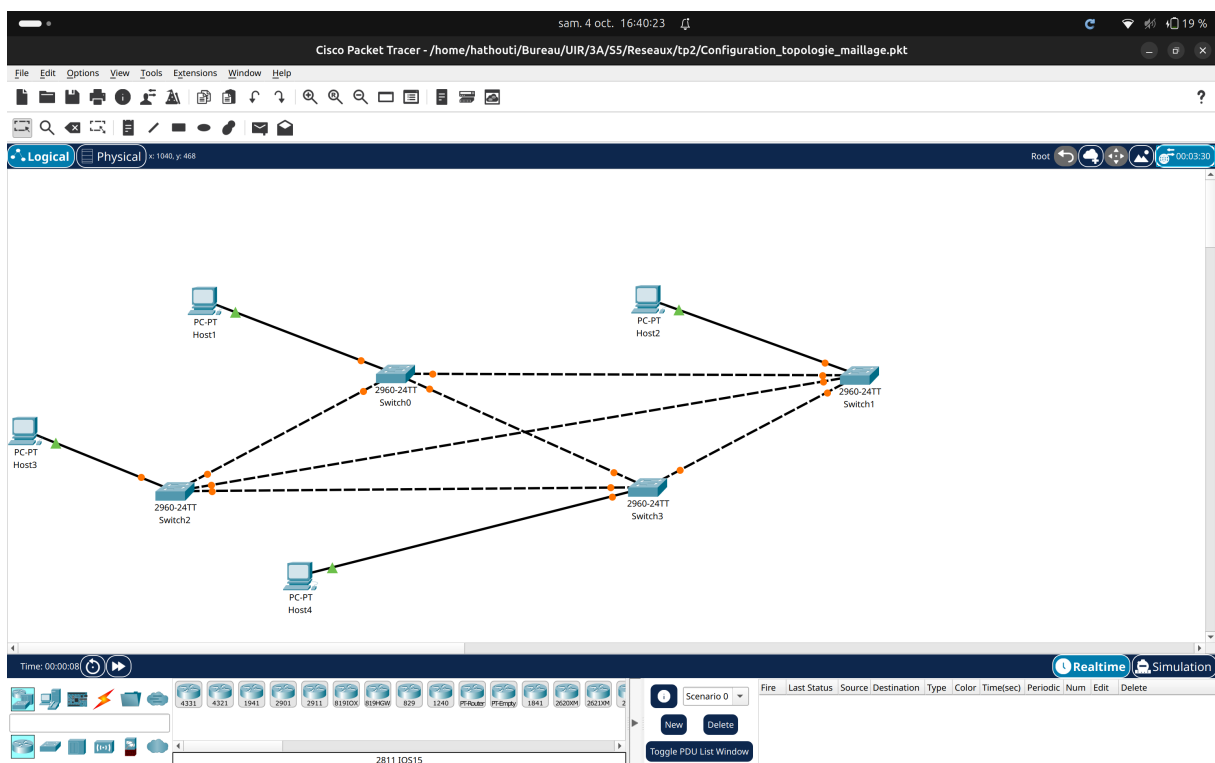


FIGURE 14 – Topologie Maillée - Schéma de configuration

Configuration IP :

PC	Adresse IP
Host1	192.168.1.1
Host2	192.168.1.2
Host3	192.168.1.3
Host4	192.168.1.4

TABLE 9 – Adressage topologie Maillée

Nombre de connexions : Pour n hosts, nombre de liens = $\frac{n(n-1)}{2}$
 Pour 3 Hosts : $\frac{3 \times 2}{2} = 3$ connexions

5.4.2 Tests de connectivité

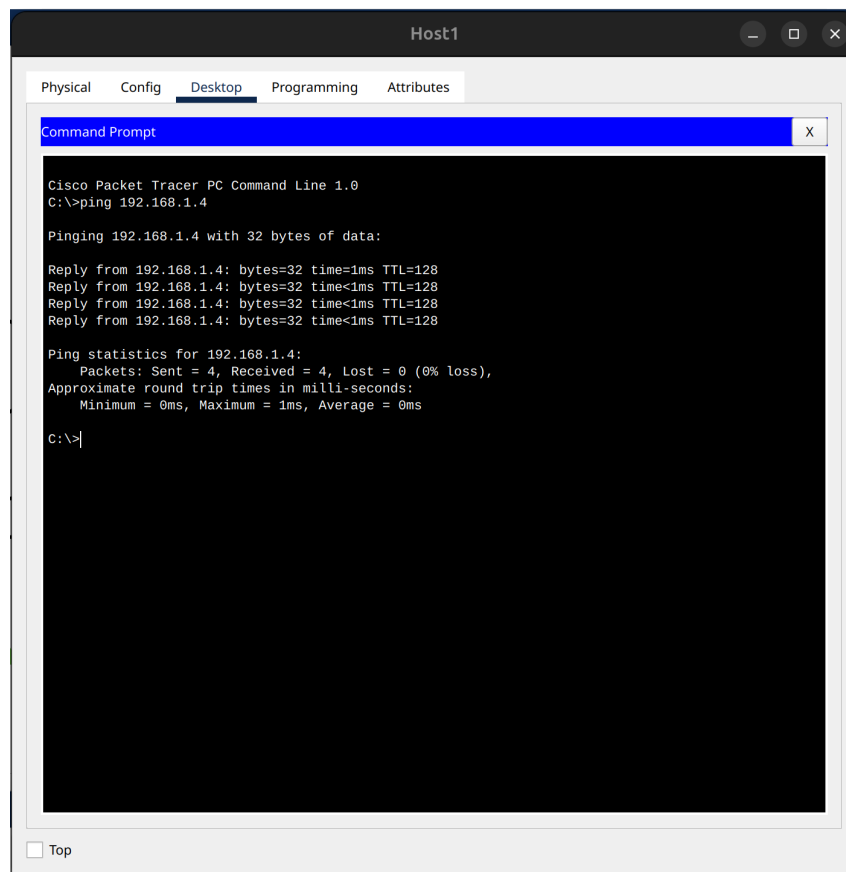


FIGURE 15 – Tests de connectivité - Topologie Maillée

— Ping Host1 → Host4 : Succès (connexion directe)

5.4.3 Avantages et inconvénients

Avantages	Inconvénients
Très haute fiabilité	Trop de câbles
Excellente performance	Complicé à configurer
Chemins alternatifs disponibles	Nombre d'interfaces réseau élevé par host ($\frac{n(n-1)}{2}$)
Tolérance aux pannes maximale	Inadapté pour les grands réseaux

TABLE 10 – Analyse topologie Maillée

6 Conclusion

Ce TP nous a permis de voir plus claire en ce qui est configuration réseau et protocoles ARP et ICMP. Les points clés retenus sont :

6.1 Compétences techniques acquises

- Configuration manuelle d'adresses IP sur Linux et Windows ;
- Maîtrise des commandes réseau (`ifconfig`, `arp`, `ping`) ;
- Utilisation d'outils d'analyse : Wireshark ;
- Compréhension du fonctionnement des protocoles ARP et ICMP ;
- Analyse comparative de différentes topologies réseau ;

6.2 Enseignements principaux

Protocole ARP :

- Essentiel pour pouvoir affecter une adresse MAC (connue) à l'adresse IP (encore pas connue de la part du host) en réseau local ;
- Le cache ARP permet d'éviter les requêtes répétées ;
- Fonctionne en broadcast (request) et unicast (reply) ;

Protocole ICMP :

- Permet de diagnostiquer le réseau (ping) ;
- Permet de tester la connectivité et mesurer les latences ;
- ARP indispensable pour une première communication car l'adresse IP ;

Topologies réseau :

- La topologie étoile est un standard très souvent utilisé dans le gaming, ou même en cours l'année dernière par le professeur de POO durant ses exams ;
- Chaque topologie répond à des besoins spécifiques ;

6.3 Difficultés rencontrées

Configuration matérielle : L'utilisation d'un adaptateur USB-C vers Ethernet a nécessité l'identification correcte de l'interface réseau (`enx0c3796401539`), très différents des interfaces Ethernet standards (`em0` ou encore `bge0`).