UNITECH
TIC-HAITI-BRH

DEVOIR DE RESEAU

JUDITH SOULAMITE NOUHO NOUTAT

Marie France Logea DORCIN
logeadorcinmf@gmail.com

Compte rendu-Travaux pratiques WIRESHARK

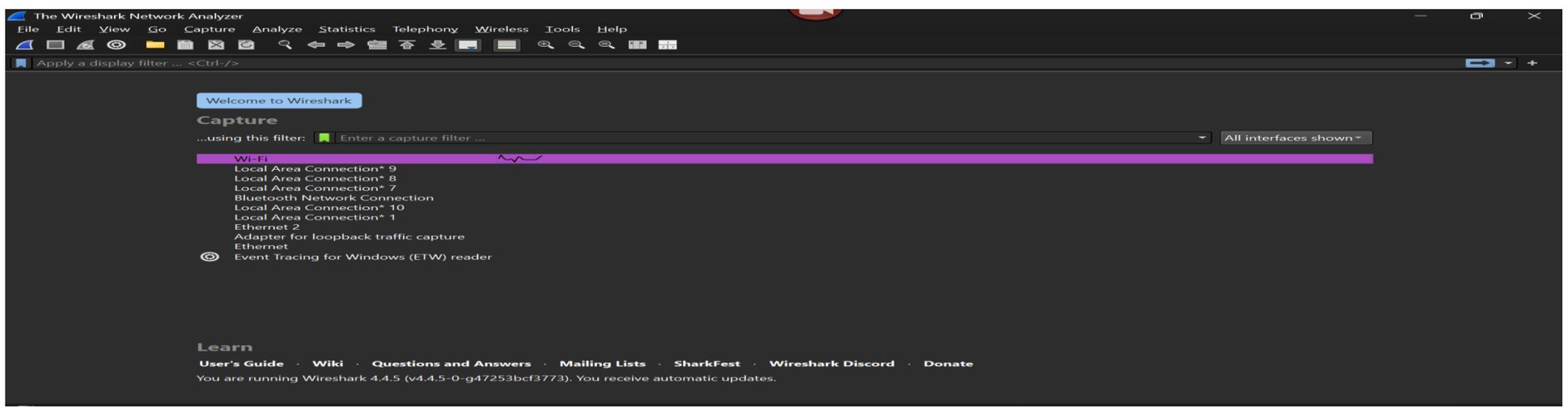
Pour ce TP, j'ai utilisé Wireshark, un analyseur de protocoles. Wireshark est en fait un outil essentiel pour les professionnels des réseaux qui permet de capturer et d'examiner en détail le trafic réseau. J'ai compris que son principal avantage est sa capacité à capturer chaque unité de données (PDU) qui circule sur le réseau et à les décoder selon les normes établies.
J'ai téléchargé et installé la version 4.4.5 de Wireshark pour Windows 64-bit.

2eme partie : Capture et analyse des données ICMP locales avec Wireshark
Pour cette partie, j'ai commencé par récupérer les informations de mon interface réseau. J'ai ouvert une invite de commande et j'ai exécuté la commande ipconfig /all qui m'a permis de voir mon adresse IP (192.168.1.158) ainsi que mon adresse MAC. Après j'ai effectué un test de ping vers l'adresse IP (192.168.1.102), qui correspond à mon deuxième ordinateur sur le réseau local.

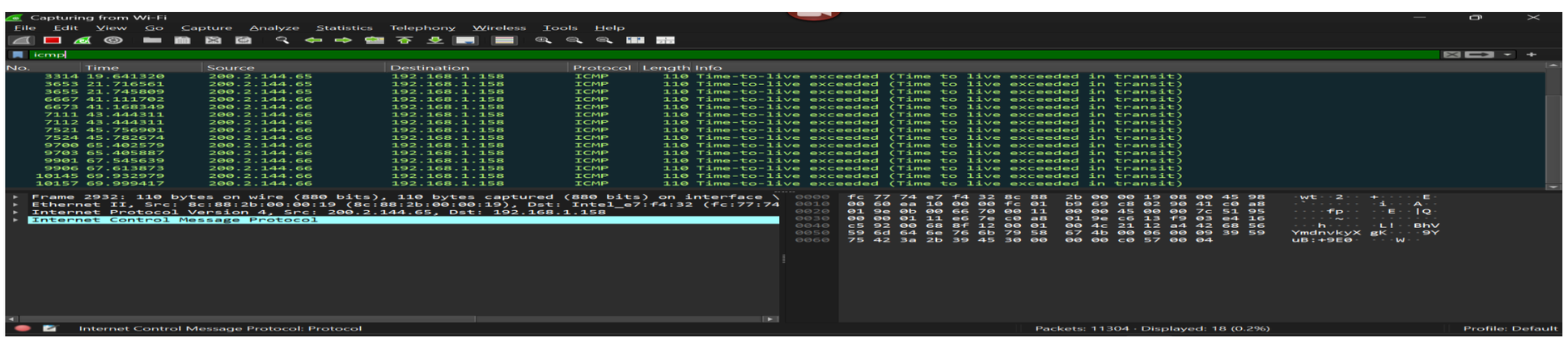
```
C:\Users\DELL>ping 192.168.1.102

Pinging 192.168.1.102 with 32 bytes of data:
Reply from 192.168.1.102: bytes=32 time=268ms TTL=128
Reply from 192.168.1.102: bytes=32 time=12ms TTL=128
Reply from 192.168.1.102: bytes=32 time=12ms TTL=128
Reply from 192.168.1.102: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 268ms, Average = 73ms
```

```
C:\Users\Marie-France>ping 192.168.1.158

Pinging 192.168.1.158 with 32 bytes of data:
Reply from 192.168.1.158: bytes=32 time=10ms TTL=128
Reply from 192.168.1.158: bytes=32 time=2ms TTL=128
Reply from 192.168.1.158: bytes=32 time=2ms TTL=128
Reply from 192.168.1.158: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.1.158:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 10ms, Average = 4ms
```

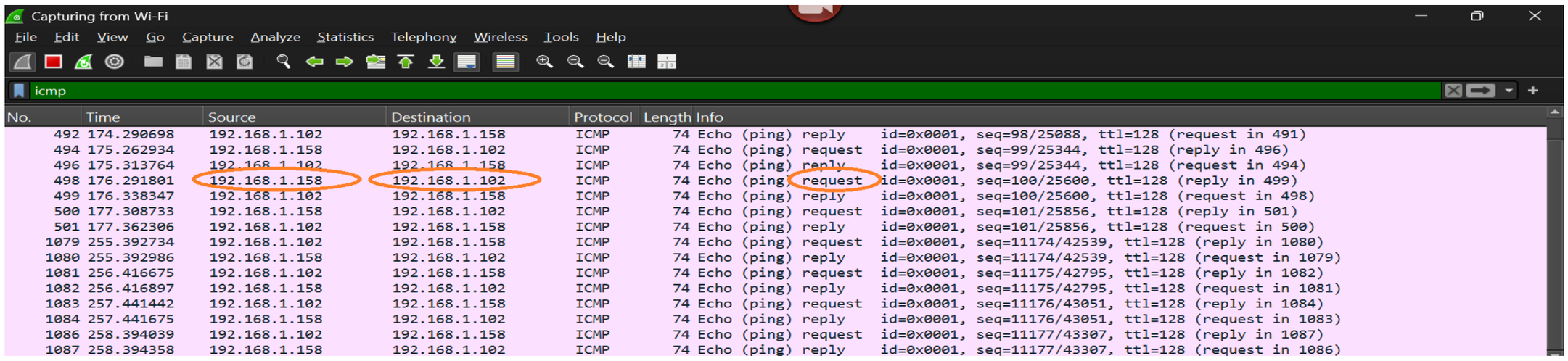
Etape 2 : Démarrage de Wireshark et capture des données
J'ai démarré le logiciel Wireshark en double-cliquant sur son icône. Une fois l'interface ouverte, j'ai sélectionné l'interface réseau utilisée par mon ordinateur pour se connecter au réseau local. Dans mon cas, il s'agissait de l'interface Wi-Fi.



Examinons les données capturées.
Pour cette partie, j'ai lancé une nouvelle capture sur l'interface Wi-Fi, puis j'ai utilisé le filtre icmp pour afficher uniquement les paquets ICMP.



Remarque sur la source et la destination
Dans les trames ICMP capturées, je remarque que l'adresse IP source est 192.168.1.158, ce qui correspond à mon ordinateur. L'adresse IP de destination est 192.168.1.102, qui est celle de mon second PC. Cela signifie que c'est moi qui ai envoyé la requête ping (Echo Request) vers cet autre ordinateur. Lorsque je reçois une réponse (Echo Reply), les rôles s'inversent la source devient 192.168.1.102 (le second PC) et la destination 192.168.1.158 (mon PC).



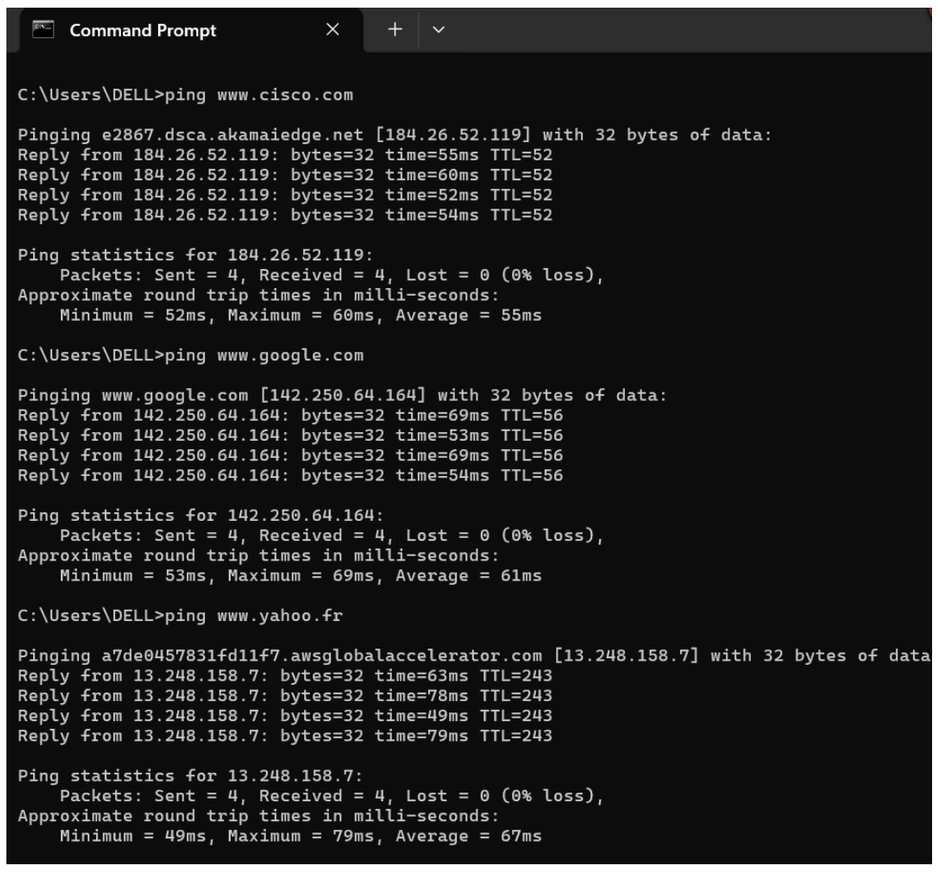
No.	Time	Source	Destination	Protocol	Length	Info
492	174.290698	192.168.1.102	192.168.1.158	ICMP	74	Echo (ping) reply id=0x0001, seq=98/25088, ttl=128 (request in 491)
494	175.262934	192.168.1.158	192.168.1.102	ICMP	74	Echo (ping) request id=0x0001, seq=99/25344, ttl=128 (reply in 496)
496	175.313764	192.168.1.102	192.168.1.158	ICMP	74	Echo (ping) reply id=0x0001, seq=99/25344, ttl=128 (request in 494)
498	176.291801	192.168.1.158	192.168.1.102	ICMP	74	Echo (ping) request id=0x0001, seq=100/25600, ttl=128 (reply in 499)
499	176.338347	192.168.1.102	192.168.1.158	ICMP	74	Echo (ping) reply id=0x0001, seq=100/25600, ttl=128 (request in 498)
500	177.308733	192.168.1.158	192.168.1.102	ICMP	74	Echo (ping) request id=0x0001, seq=101/25856, ttl=128 (reply in 501)
501	177.362306	192.168.1.102	192.168.1.158	ICMP	74	Echo (ping) reply id=0x0001, seq=101/25856, ttl=128 (request in 500)
1079	255.392734	192.168.1.102	192.168.1.158	ICMP	74	Echo (ping) request id=0x0001, seq=11174/42539, ttl=128 (reply in 1080)
1080	255.392986	192.168.1.158	192.168.1.102	ICMP	74	Echo (ping) reply id=0x0001, seq=11174/42539, ttl=128 (request in 1079)
1081	256.416675	192.168.1.102	192.168.1.158	ICMP	74	Echo (ping) request id=0x0001, seq=11175/42795, ttl=128 (reply in 1082)
1082	256.416897	192.168.1.158	192.168.1.102	ICMP	74	Echo (ping) reply id=0x0001, seq=11175/42795, ttl=128 (request in 1081)
1083	257.441442	192.168.1.102	192.168.1.158	ICMP	74	Echo (ping) request id=0x0001, seq=11176/43051, ttl=128 (reply in 1084)
1084	257.441675	192.168.1.158	192.168.1.102	ICMP	74	Echo (ping) reply id=0x0001, seq=11176/43051, ttl=128 (request in 1083)
1086	258.394039	192.168.1.102	192.168.1.158	ICMP	74	Echo (ping) request id=0x0001, seq=11177/43307, ttl=128 (reply in 1087)
1087	258.394358	192.168.1.158	192.168.1.102	ICMP	74	Echo (ping) reply id=0x0001, seq=11177/43307, ttl=128 (request in 1086)

L'adresse MAC de la source correspond-elle à l'interface de votre ordinateur ?
R- OUI, l'adresse MAC de la source affichée dans Wireshark correspond bien à celle de l'interface réseau de mon ordinateur, que j'ai vérifiée à l'aide de la commande ipconfig /all.

L'adresse MAC de la destination dans Wireshark correspond-elle à l'adresse MAC du membre de votre équipe ? R- OUI

Comment votre ordinateur obtient-il l'adresse MAC de l'ordinateur de destination des requêtes ping ? R- Mon ordinateur utilise le protocole ARP pour découvrir l'adresse MAC de l'ordinateur de mon ami (192.168.1.102) avant d'envoyer les paquets ICMP. Il envoie une requête sur le réseau local, et l'ordinateur ciblé répond avec son adresse MAC. Mon ordinateur peut alors transmettre les données à la bonne destination.

3eme partie : Ping aux trois URL de sites Web



Examen et analyse des données à partir des hôtes distants.

- IP :184.26.52.119 MAC : 8c :88 :2b :00 :00 :19
- IP :142.250.64.164 MAC : 8c :88 :2b :00 :00 :19
- IP : 13.248.158.7 MAC : 8c :88 :2b :00 :00 :19

Remarque : J'ai remarqué que je n'ai pas pu ping www.yahoo.com comme indiqué dans le document, car le site ne répondait pas. En revanche, ping www.yahoo.fr a très bien fonctionné, ce qui m'a permis de continuer l'analyse sans problème.

Quel élément important tirez-vous de ces informations ?
R- L'élément important que je retiens est que, lors d'une communication avec un hôte distant, l'adresse MAC de destination affichée dans Wireshark n'est pas celle du serveur distant, mais celle du dispositif local qui assure la liaison entre mon ordinateur et Internet.

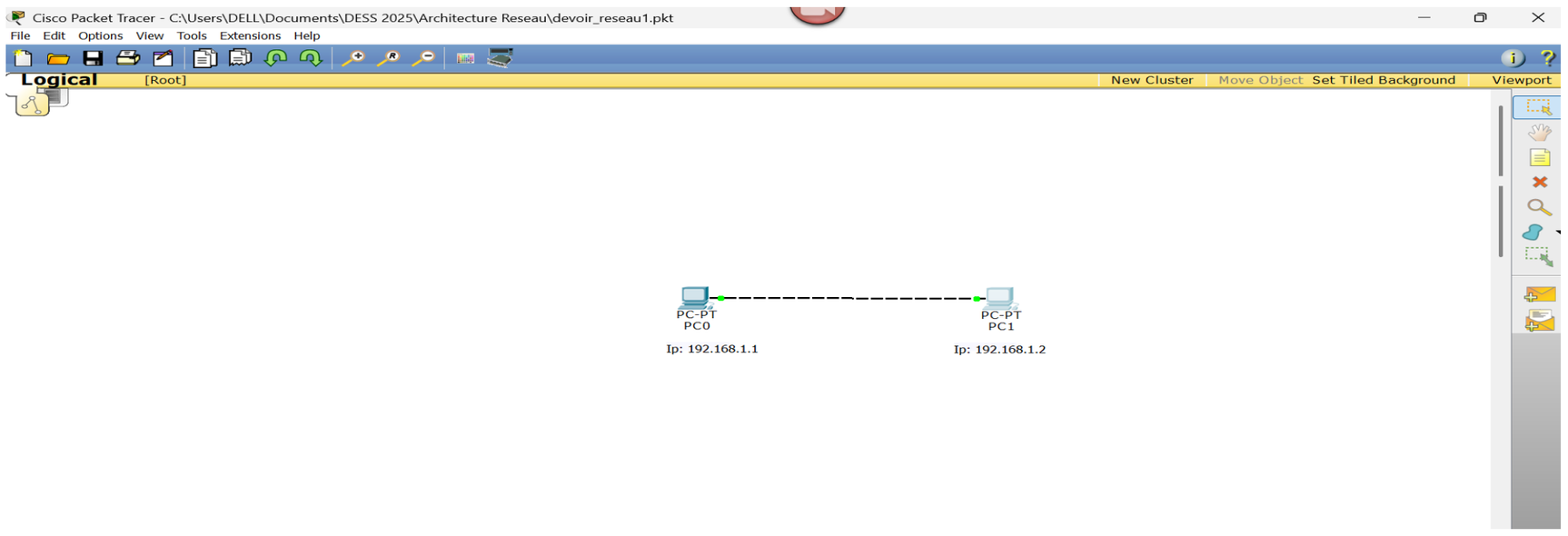
En quoi ces informations diffèrent-elles des informations de requêtes ping locales que vous avez reçues dans la deuxième partie ?
R- Dans les requêtes ping locales, l'adresse MAC de destination affichée dans Wireshark est réellement celle de l'ordinateur ciblé, car les deux machines se trouvent sur le même réseau local (LAN).

Pourquoi Wireshark affiche-t-il l'adresse MAC réelle des hôtes locaux, mais pas l'adresse MAC réelle des hôtes distants ?
R- Parce que sur un réseau Wi-Fi, comme sur un réseau local câblé, mon ordinateur connaît uniquement l'adresse MAC du point d'accès local.
Pour les hôtes distants, les paquets passent par Internet et traversent plusieurs routeurs. Mon ordinateur ne voit donc pas l'adresse MAC du serveur distant, mais seulement celle du prochain saut local.

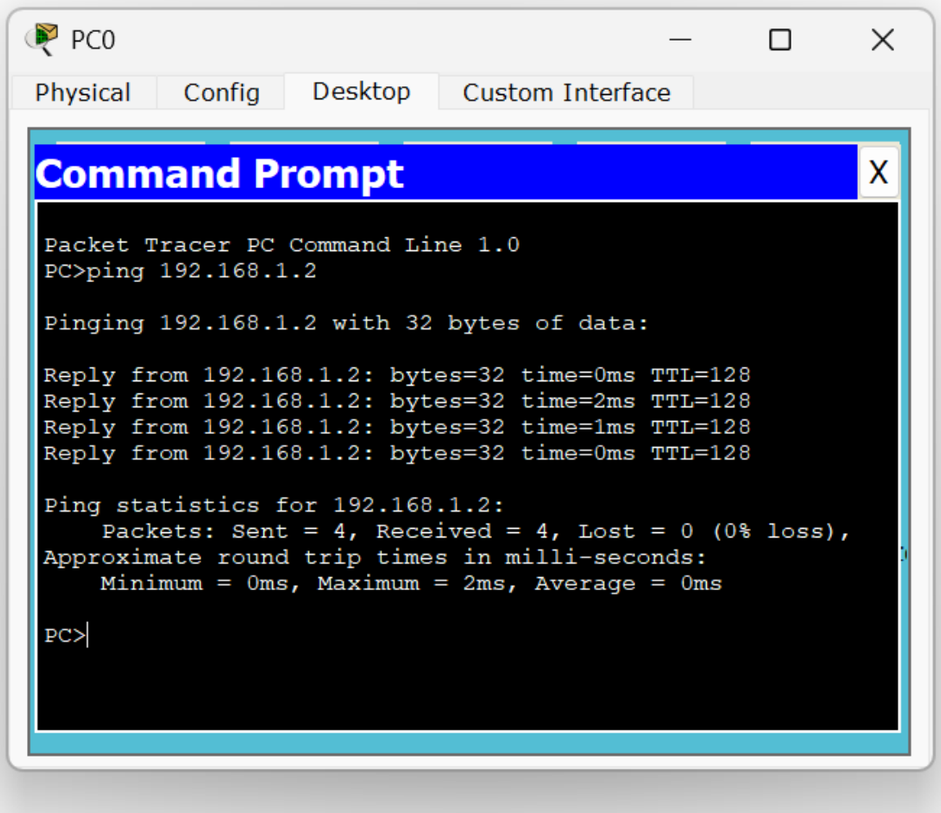
Compte rendu-Travaux pratiques Packet Tracer
Simulation d'un Réseau avec Packet Tracer

Dans ce TP, j'ai configuré un réseau simple dans Packet Tracer en reliant deux PC par un câble croisé. L'objectif était de leur attribuer une adresse IP et de tester la communication entre eux.
-Matériel et Outils Utilisés
-Logiciel : Cisco Packet Tracer 6.0.1
-Équipements réseau : 2 PC-PT, câble croisé

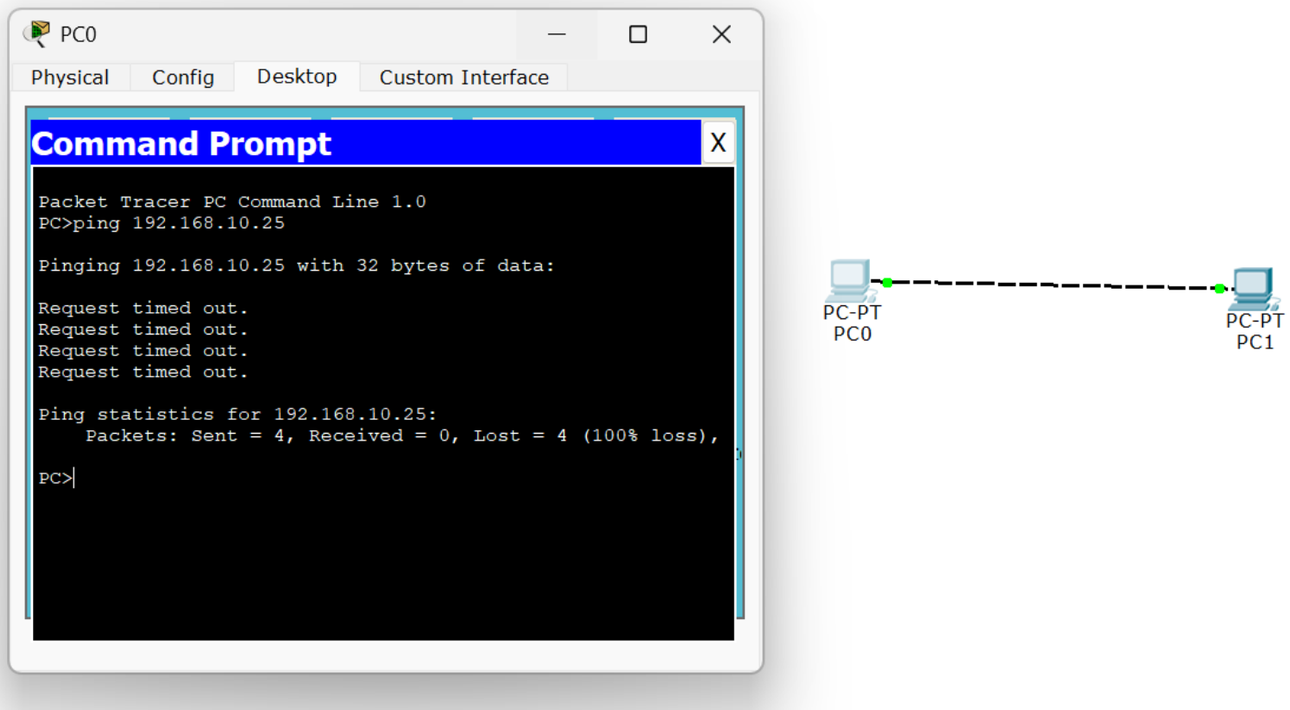
J'ai conçu le réseau de la manière suivante
PC0 (192.168.1.1) connecté à **PC1** (192.168.1.2) via un câble croisé.



J'ai effectué un test de connectivité en utilisant la commande ping depuis PC0 vers PC1. Voici la capture d'écran du résultat :

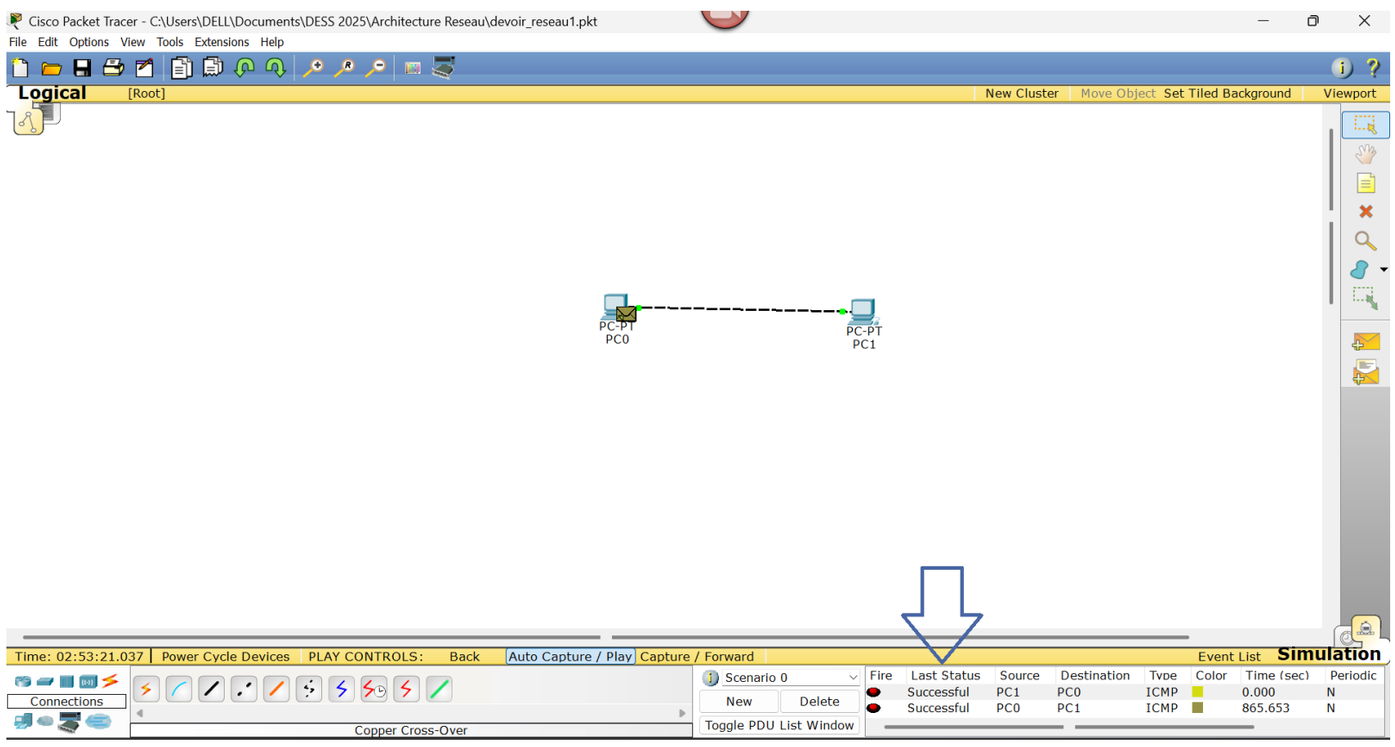


j'ai vérifié le comportement du réseau face à une adresse IP qui n'existe pas dans le réseau local



Utilisation du mode Simulation

J’ai activé le mode Simulation dans Packet Tracer afin observer les échanges de paquets entre mes deux ordinateurs. Depuis PC0, j’ai envoyé une requête ping vers PC1 (192.168.1.2). En simulation, j’ai pu remarquer l’envoi et la réponse à l’aide de paquets ICMP sous forme d’enveloppes.



Les résultats montrent qu’un paquet ICMP envoyé de PC0 à PC1 Source : PC0, Destination : PC1. Un paquet ICMP de réponse retourné par PC1 vers PC0. Les deux paquets ont le statut Successful. Le protocole utilisé est bien ICMP. Cette simulation m’a permis de visualiser le fonctionnement détaillé de ces commandes et de suivre chaque étape du trajet des paquets réseau, ce qui renforce ma compréhension.