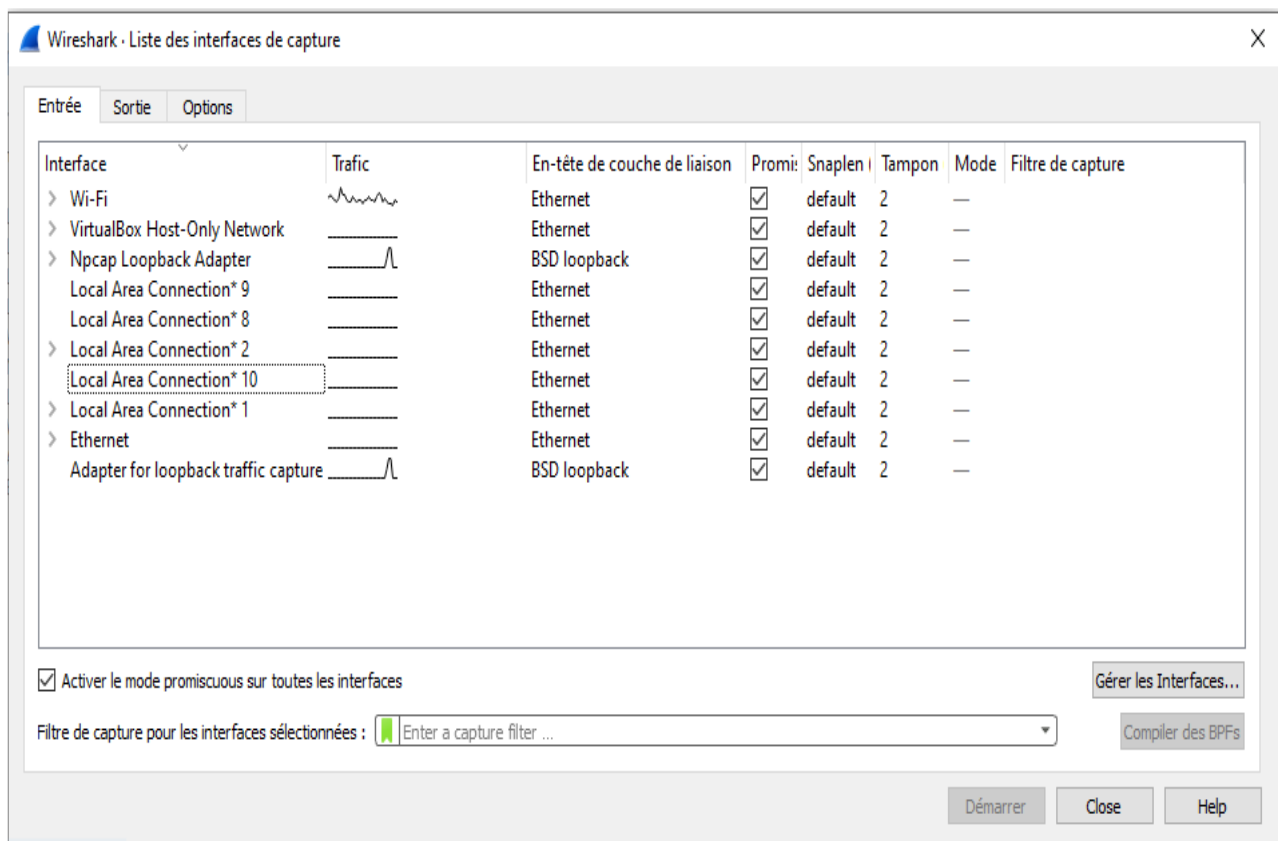


Administration Réseaux et Systèmes

TP N° 1 : Simulateur Wireshark

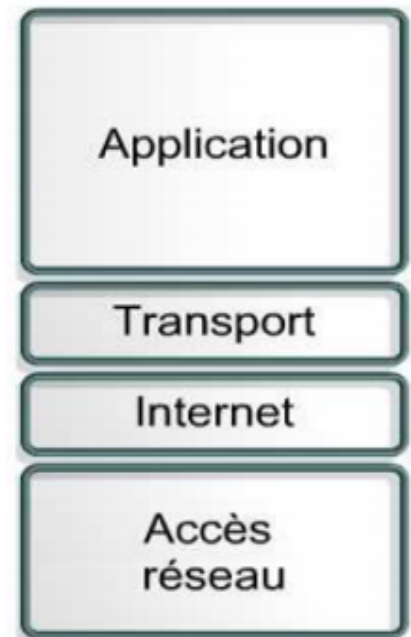
1. _____
2. _____
3. Lancer Wireshark et sélectionner Capture/ Interfaces...



4. Pourquoi on appelle TCP/IP une pile ? indiquez brièvement les fonctionnalités de chaque couche.

Le modèle TCP/IP comporte les quatre couches suivantes :

- La couche application
- La couche transport
- La couche Internet
- La couche d'accès au réseau



⇒ On appelle TCP/IP une pile parce qu'il empile plusieurs couches dans une seule couche

Couche Accès réseau :

Objectif :

Cette couche réalise l'interconnexion des réseaux (hétérogènes) distants sans connexion.

Son rôle est de **permettre l'injection de paquets dans n'importe quel réseau** et l'acheminement des ces paquets indépendamment les uns des autres jusqu'à destination.

Unité d'échanges : **Trame**

Couche Internet:

Objectif :

Réalise l'interconnexion des réseaux hétérogènes distants

permettre l'injection de paquets dans n'importe quel réseau et acheminement de ces paquets indépendamment les uns des autres jusqu'à destination

Gère le routage des paquets au travers des réseaux empruntés

Unité d'échanges : **Datagramme**

Les protocoles :

- IP : Internet Protocol
- ICMP : Internet Control and Error Message Protocol
- ARP : Address Resolution Protocol
- RARP : Reverse Address Resolution Protocol

L'Architecture du modèle TCP/IP

Couche Transport :

Objectif :

Même rôle que la couche Transport du modèle OSI

Transport correct de messages de manière fiable et de bout en bout entre l'émetteur et le récepteur.

Unité d'échanges : Paquet.

Les protocoles :

➤ TCP : Transmission Control Protocol

- Protocole à remise garantie, orienté connexion, qui permet un acheminement sans erreur des messages.

➤ UDP : User Datagram Protocol

- Plus simple que TCP mais non fiable (remise non garantie)
- Plus rapide que TCP

Couche Application :

Objectif :

La couche application fournit les protocoles et les fonctions nécessaires pour les applications clients. Il existe un nombre important de services fournis par la couche d'application.

Unité d'échanges : Message.

Quelques protocoles :

➤ FTP : File Transfer Protocol

➤ SMTP : Simple Mail Transfer Protocol

➤ TFTP : Trivial File Transfer Protocol

➤ DHCP : Dynamic Host Configuration Protocol

➤ http : pour le web

5. Donner les couches et les rôles des protocoles réseau que vous connaissez indiqués dans la fenêtre affichée.

▣ **IP** (**Internet Protocol**) : permet l'élaboration et le transport des datagrammes **IP** (les paquets de données), sans toutefois en assurer la « livraison ».

▣ **ICMP** (**Internet Control Message Protocol**) : permet le contrôle des erreurs de transmission.

▣ **IGMP** (**Internet Group Management Protocol**) : permet à des routeurs IP de déterminer de façon dynamique les groupes multicast qui disposent de clients dans un sous-réseau.

▣ **ARP** (**Adresse Résolution Protocol**) : permet de connaître l'adresse physique d'une carte réseau correspondant à une adresse IP

6. Sélectionner un exemple d'un paquet et analyser en détails ses divers champs

The image shows a Wireshark packet capture analysis of an ARP request. The packet list shows a single packet (No. 1582) at time 8.802590, source zte_e0:15:c4, destination Broadcast, protocol ARP, length 42 bytes. The packet details pane shows the following structure:

- Frame 1582: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{D1031D2A-00FD-4927-8B91-3FD8EFC71B04}, id 0
 - Interface id: 0 (\Device\NPF_{D1031D2A-00FD-4927-8B91-3FD8EFC71B04})
 - Interface name: \Device\NPF_{D1031D2A-00FD-4927-8B91-3FD8EFC71B04}
 - Interface description: Wi-Fi
 - Encapsulation type: Ethernet (1)
 - Arrival Time: Mar 26, 2020 00:21:31.268090000 Morocco Daylight Time
 - [Time shift for this packet: 0.000000000 seconds]
 - Epoch Time: 1585178491.268090000 seconds
 - [Time delta from previous captured frame: 0.015355000 seconds]
 - [Time delta from previous displayed frame: 0.000000000 seconds]
 - [Time since reference or first frame: 8.802590000 seconds]
 - Frame Number: 1582
 - Frame Length: 42 bytes (336 bits)
 - Capture Length: 42 bytes (336 bits)
 - [Frame is marked: False]
 - [Frame is ignored: False]
 - [Protocols in frame: eth:ethertype:arp]
 - [Coloring Rule Name: ARP]
 - [Coloring Rule String: arp]
 - Ethernet II, Src: zte_e0:15:c4 (60:14:66:e0:15:c4), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 - > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 - > Source: zte_e0:15:c4 (60:14:66:e0:15:c4)
 - Type: ARP (0x0806)
 - Address Resolution Protocol (request)
 - Hardware type: Ethernet (1)
 - Protocol type: IPv4 (0x0800)
 - Hardware size: 6
 - Protocol size: 4
 - Opcode: request (1)
 - Sender MAC address: zte_e0:15:c4 (60:14:66:e0:15:c4)
 - Sender IP address: 192.168.0.1
 - Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```

0000  ff ff ff ff ff ff 60 14 66 e0 15 c4 08 06 00 01  ..... f...
0010  08 00 06 04 00 01 bc e2 65 4a 7e 9f c0 a8 00 a0  ..... eJ~...
0020  00 00 00 00 00 00 c0 a8 00 01  ..... ..
  
```

Hardware type (arp.hw.type), 2 byte(s) | Paquets: 26056 · Affichés: 21

7. Sélectionner 3 paquets et visualiser leur contenu en hexadécimale. Calculer leurs équivalents binaires.

The image shows a Wireshark packet capture analysis of an ARP request. The packet list shows a single packet (No. 10) at time 5.287521, source HuaweiTe_4a:7e:9f, destination Broadcast, protocol ARP, length 42 bytes. The packet details pane shows the following structure:

- Frame 10: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{D1031D2A-00FD-4927-8B91-3FD8EFC71B04}, id 0
 - Ethernet II, Src: HuaweiTe_4a:7e:9f (bc:e2:65:4a:7e:9f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 - > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 - > Source: HuaweiTe_4a:7e:9f (bc:e2:65:4a:7e:9f)
 - Address: HuaweiTe_4a:7e:9f (bc:e2:65:4a:7e:9f)
 -0. = LG bit: Globally unique address (factory default)
 -0. = IG bit: Individual address (unicast)
 - Type: ARP (0x0806)
 - Address Resolution Protocol (request)

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```

0000  ff ff ff ff ff ff bc e2 65 4a 7e 9f 08 06 00 01  ..... eJ~...
0010  08 00 06 04 00 01 bc e2 65 4a 7e 9f c0 a8 00 a0  ..... eJ~...
0020  00 00 00 00 00 00 c0 a8 00 01  ..... ..
  
```

(bc e2 65 4a 7e 9f) =

(1011110011100010011001010100101001111110100111110000100000000110)2

8. Indiquer le rôle joué par Adresse MAC. Peut-on avoir plusieurs ordinateurs avec une même adresse MAC ?

☐ Le MAC (*Media Access Control*) : Est un identifiant physique d'une seule machine, et on ne peut pas avoir la même adresse MAC dans plusieurs machines.

9. Quels sont les protocoles supportés par les paquets : 14, 23, 101 et 134.

```
14    18.129305    5.45.58.214    192.168.0.178    HTTP    115 HTTP/1.1 200 OK
```

⇒ HTTP (HyperText Transfer Protocol) : protocole de communication client-serveur.

```
23    24.969501    192.168.0.178    157.240.21.52    TCP    54 50499 → 443 [ACK] Seq=93 Ack=469 Win=255 Len=0
```

```
101   60.288832    52.157.234.37    192.168.0.178    TCP    54 443 → 50521 [ACK] Seq=6193 Ack=3877 Win=524800 Len=0
```

⇒ TCP (Transmission Control Protocol) : protocole de transport fiable, en mode connecté

```
134   93.351357    IntelCor_96:1f:13    zte_e0:15:c4    ARP    42 192.168.0.178 is at e0:94:67:96:1f:13
```

⇒ ARP (**A**dresse **R**ésolution **P**rotocol) : utilisé pour traduire une adresse de **protocole** de couche réseau (typiquement une adresse IPv4) en une adresse de **protocole** de couche de liaison (typiquement une adresse MAC).

Wireshark fournit deux possibilités de filtrage : l'une au moment de la capture et l'autre au moment de l'affichage.

10. Quelle est la différence entre les deux en faisant des tests

☐ **Au moment de capture** on bloque les autres ports et on prendra le seul Protocole sélectionné

☐ **Au moment d'affichage** on prendra tous les protocoles après on va sélectionner un seul pour afficher

11. Retrouver un paquet ARP. Indiquer la correspondance entre une adresse IP et une adresse MAC pour deux machines.

```
134   93.351357    IntelCor_96:1f:13    zte_e0:15:c4    ARP    42 192.168.0.178 is at e0:94:67:96:1f:13
```

12. Interpréter le champ Destination pour un paquet ARP

134	93.351357	IntelCor_96:1f:13	zte_e0:15:c4	ARP	42	192.168.0.178 is at e0:94:67:96:1f:13
Frame 134: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{D1031D2A-00FD-4927-8891-3FD8EFC71B04}, id 0						
Ethernet II, Src: IntelCor_96:1f:13 (e0:94:67:96:1f:13), Dst: zte_e0:15:c4 (60:14:66:e0:15:c4)						
Destination: zte_e0:15:c4 (60:14:66:e0:15:c4)						
Address: zte_e0:15:c4 (60:14:66:e0:15:c4)						
.... ..0. = LG bit: Globally unique address (factory default)						
.... ..0 = IG bit: Individual address (unicast)						
Source: IntelCor_96:1f:13 (e0:94:67:96:1f:13)						
Address: IntelCor_96:1f:13 (e0:94:67:96:1f:13)						
.... ..0. = LG bit: Globally unique address (factory default)						
.... ..0 = IG bit: Individual address (unicast)						
Type: ARP (0x0806)						

13. Réaliser les filtres pour : IP, TCP, UDP, HTTP, ICMP et DHCP. Décrivez leurs caractéristiques et leurs champs.

IP (Internet Protocol) c'est un Protocol de la couche 3 (réseau) permettant un service d'adressage unique pour l'ensemble des terminaux connectés

TCP (Transmission Control Protocol) : c'est un Protocol de la couche 4 (transport) protocole de transport fiable, en mode connecté.

tcp						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	157.240.21.52	192.168.0.178	TLSv1.2	148	Application Data
2	0.041104	192.168.0.178	157.240.21.52	TCP	54	50499 → 443 [ACK] Seq=1 Ack=95 Win=257 Len=0
Frame 2: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{D1031D2A-00FD-4927-8891-3FD8EFC71B04}, id 0						
Ethernet II, Src: IntelCor_96:1f:13 (e0:94:67:96:1f:13), Dst: zte_e0:15:c4 (60:14:66:e0:15:c4)						
Destination: zte_e0:15:c4 (60:14:66:e0:15:c4)						
Address: zte_e0:15:c4 (60:14:66:e0:15:c4)						
.... ..0. = LG bit: Globally unique address (factory default)						
.... ..0 = IG bit: Individual address (unicast)						
Source: IntelCor_96:1f:13 (e0:94:67:96:1f:13)						
Address: IntelCor_96:1f:13 (e0:94:67:96:1f:13)						
.... ..0. = LG bit: Globally unique address (factory default)						
.... ..0 = IG bit: Individual address (unicast)						
Type: IPv4 (0x0800)						

UDP (User Datagram Protocol) : un des principaux protocoles de télécommunication utilisés par Internet. Il fait partie de la couche transport du modèle OSI, quatrième couche

Mode déconnecté

14. Analyser le champ Continuation Data pour un paquet TCP.

No.	Time	Source	Destination	Protocol	Length	Info
2	0.041104	192.168.0.178	157.240.21.52	TCP	54	50499 → 443 [ACK] Seq=1 Ack=95 Win=257 Len=0

```
> Frame 2: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{D1031D2A-00FD-4927-8891-3FD8EFC71B04}, id 0
```

```
> Ethernet II, Src: IntelCor_96:1f:13 (e0:94:67:96:1f:13), Dst: zte e0:15:c4 (60:14:66:e0:15:c4)
```

> Internet Protocol Version 4, Src: 192.168.0.178, Dst: 157.240.21.52

▼ Transmission Control Protocol, Src Port: 50499, Dst Port: 443, Seq: 1, Ack: 95, Len: 0

Source Port: 50499

Destination Port: 443

```
[Stream index: 0]
```

[TCP Segment Len: 0]

Sequence number: 1 (relative sequence number)

Sequence number (raw): 2706913932

```
[Next sequence number: 1 (relative sequence number)]
```

Acknowledgment number: 95 (relative ack number)

Acknowledgment number (raw): 560801764

0101 = Header Length: 20 bytes (5)

```
> Flags: 0x010 (ACK)
```

```
Window size value: 257
```

```
[Calculated window size: 257]
```

```
[Window size scaling factor: -1 (unknown)]
```

```
Checksum: 0x4e20 [unverified]
```

```
[Checksum Status: Unverified]
```

```
Urgent pointer: 0
```

- ▼ [SEQ/ACK analysis]

[This is an ACK to the segment in frame: 1]

```
[The RTT to ACK the segment was: 0.041104000 seconds]
```

▼ [Timestamps]

```
[Time since first frame in this TCP stream: 0.041104000 seconds]
```

```
[Time since previous frame in this TCP stream: 0.041104000 seconds]
```