

Les Réseaux TD

1



2



www.wooclap.com/BXFPDS

Réglage Wireshark : L'affichage des adresses MAC

- Si Wireshark n'affiche pas les adresses mac complètes

2

The image shows two screenshots of the Wireshark interface. The top screenshot, labeled 'AVANT' (Before), shows the packet list with source MAC addresses truncated to 4 octets (e.g., IntelCor_3a:ac:0f). The bottom screenshot, labeled 'APRES' (After), shows the same packet list with full 6-octet MAC addresses (e.g., 4c:1d:96:3a:ac:0f). A red arrow points from the 'AVANT' state to the 'APRES' state. The 'View' menu is open in the 'APRES' state, showing the 'Name Resolution' submenu, which is also open, highlighting the 'Editer Nom Résolu' option.

AVANT

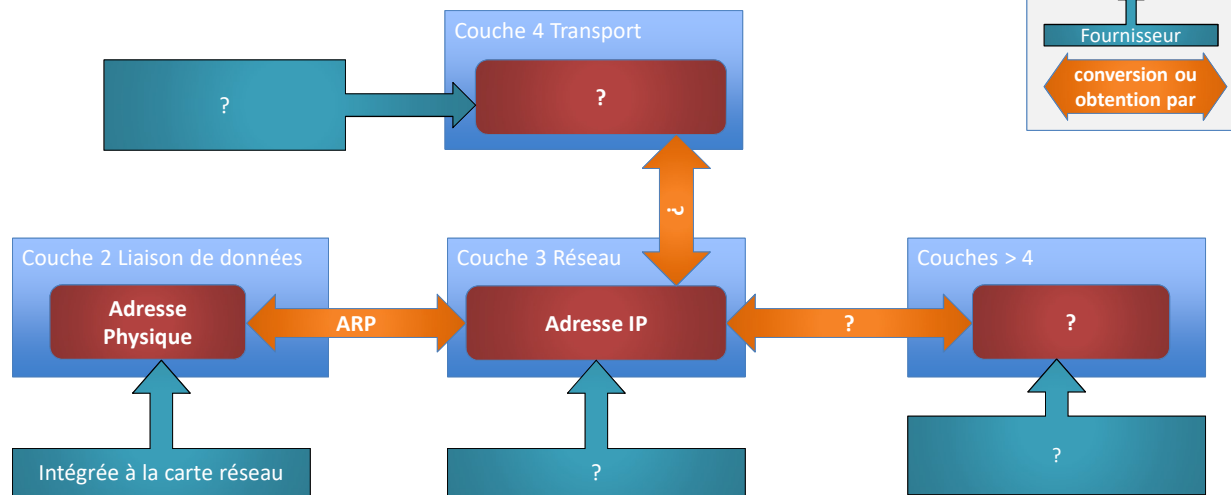
APRES

View menu path: View > Name Resolution > Editer Nom Résolu

Une adresse MAC comporte 6 octets. Les 3 premiers désignent le fabricant.
C'est le OUI (Organizationally Unique Identifier).
C'est l'organisme IEEE (Institute of Electrical and Electronics Engineers) qui gère ces références.

Repérage et protocoles dans la famille TCP/IP

Synthèse de la communication entre couches



Etat de nos connaissances actuelles.

Les TD : Déjà vu

5

Depuis le premier TD nous connaissons :

- La ou les interfaces réseaux utilisées par notre ordinateur
- L'adresse Physique (MAC) de la carte principale
- L'adresse IP cette carte
- Utilisation de Wireshark



Les TD : à voir aujourd'hui

6

Aujourd'hui nous souhaitons découvrir :

- Notre masque de réseau
- Avons-nous une passerelle ?
- D'où proviennent ces informations ?



Les outils à utiliser

7

A INSTALLER :

- Wireshark : <https://www.wireshark.org/#download>
- NMAP : <https://nmap.org/download.html>

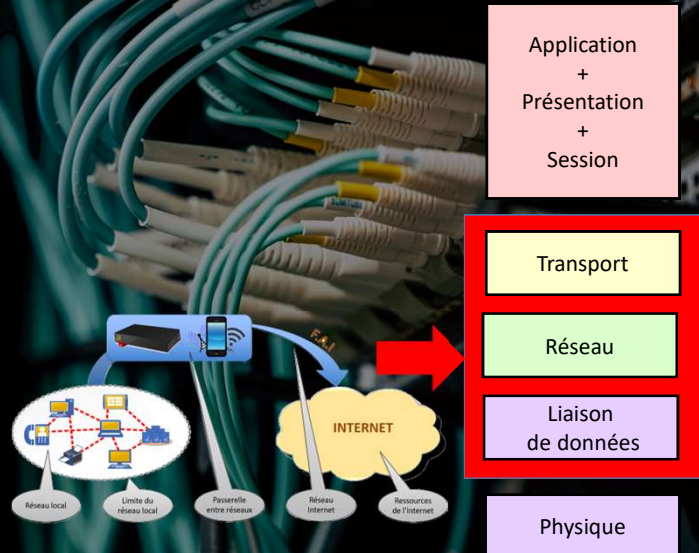


- CONNEXION AU WIFI DU TD
- Connectez-vous sur le **TdReseauGm3**
- Mot de passe **TdReseauGm3**



Analyse

Retour sur le TD 1



Rappel du TD 1

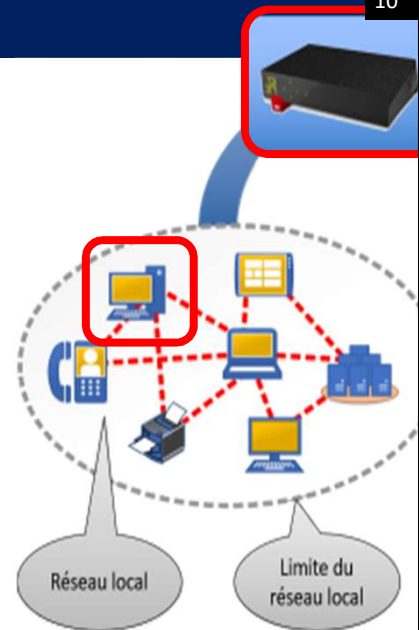
10

Noter vos informations réseaux principales :

- Nom de l'interface réseau utilisée
- Adresse MAC
- Adresse IP



- Sous Linux :
ip a
- Sous Windows :
ipconfig /all




Analyse 5

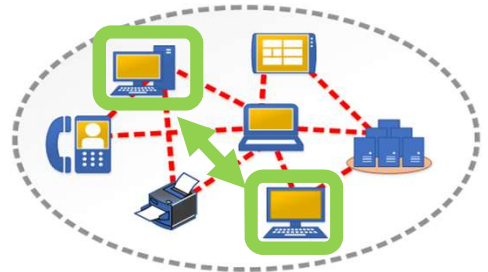
Test de connectivité



Tester la présence d'un hôte du réseau local

Sous Linux & Windows :

- Lancer une nouvelle capture Wireshark 
- Faire un **ping** sur une adresse IP connue par exemple l'IP du PC voisin.
Exemple : **ping 172.18.24.78 -c 4**
Stopper la capture après quelques ping
- Recherchez dans Wireshark les trames liées au ping pour connaître les protocoles utilisés.
Note : cherchez l'IP de destination

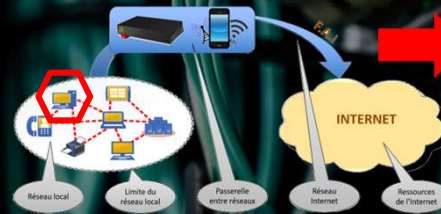


Sous Windows il y a 4 ping puis arrêt, sous Linux, le ping ne stoppe pas, il faut faire un Ctrl+C

Il est aussi possible de limiter à 4 ping avec l'option -c Ex: ping 127.0.0.1 -c 4

Analyse 5

Visualiser le lien entre
adresse physique et
adresse IP



Application
+
Présentation
+
Session

Transport

Réseau

Liaison de données
+
Physique

Le protocole ARP : Address Resolution Protocol

- Dans un réseau de type Internet, les communications utilisent une adresse IP (Internet Protocol)
- ARP permet de faire la correspondance entre une adresse physique (couche 2) et une adresse IP (couche 3)
- L'adresse physique est constante et unique pour une carte réseau
- L'adresse IP est dynamique et change en fonction du réseau local ou du temps.

**J'interdis l'entrée des
trames qui n'ont pas
mon adresse physique**



Voir les adresses en mémoire

Sous Linux :

- **arp**
- **arp -n** (Affiche les adresses IP au lieu des noms)

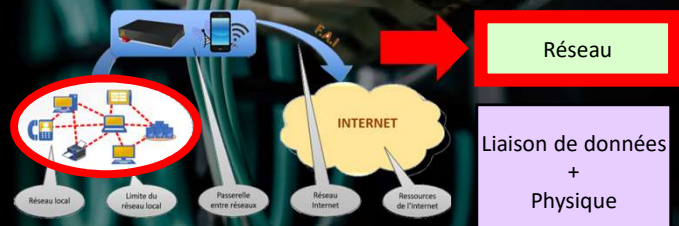
Sous Windows :

- **arp -a**
- **arp -d *** (Efface la table ARP)

Note : S'il y a plusieurs cartes réseaux, chaque cache est affiché séparément.

Analyse

Ou sont les limites de
notre réseau local ?



Les limites du réseau local : le masque

18

Sous Linux :

- **ip a** (Chercher un /x derrière l'adresse IP. Ex : /16 ou /24)
- **ifconfig -n** (Chercher le mot 'netmask'. Ex : 255.255.255.0)

Sous Windows :

- **ipconfig /all** (Chercher la ligne 'Masque de sous réseau')

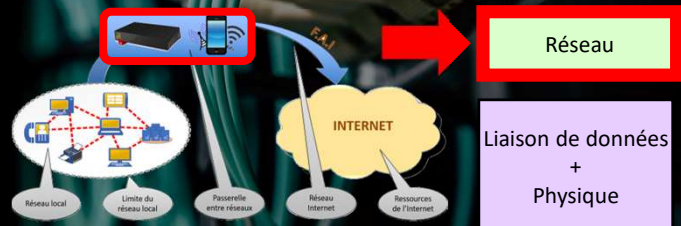
Note : Le masque peut s'écrire de différentes façons.

Sur 4 octets, comme une adresse IP, ou en notation CIDR avec un /x ou x est la longueur du masque en bits

Classless Inter Domain Routing (routage sans classes entre domaines).

Analyse

Un moyen de sortir du réseau local ?



La machine pour sortir : la passerelle

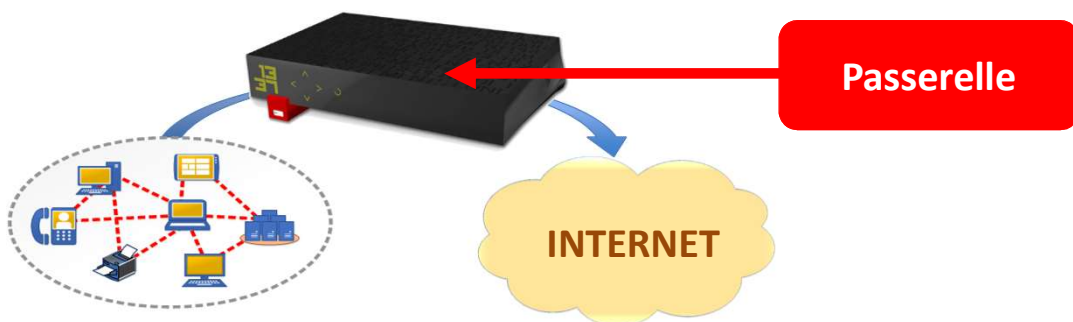
21

Sous Linux :

- **ip route show** (Chercher 'default via' suivi de l'IP de la passerelle)

Sous Windows :

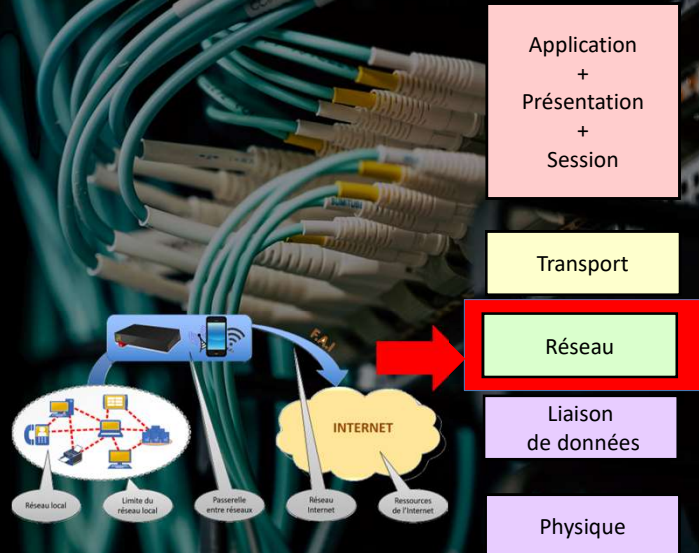
- **ipconfig /all** (Chercher la ligne 'Passerelle par défaut')



La « route » est aussi visible avec la commande linux « route » ou windows « route print »

Analyse

Notre réseau IP



Notre réseau IP

24

Ajouter ces nouvelles informations :

- Masque de réseau, les 2 notations (255.0.0.0) et CIDR (/8)
- Adresse réseau (10.0.0.0) :
- Adresse de broadcast :



- Sous Linux :
ip a
ip route show
- Sous Windows :
ipconfig /all

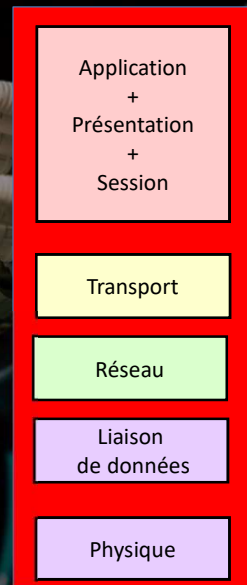


Aide pour le calcul de masque et des adresses :

<https://cric.grenoble.cnrs.fr/Administrateurs/Outils/CalculMasque>

Analyses Wireshark

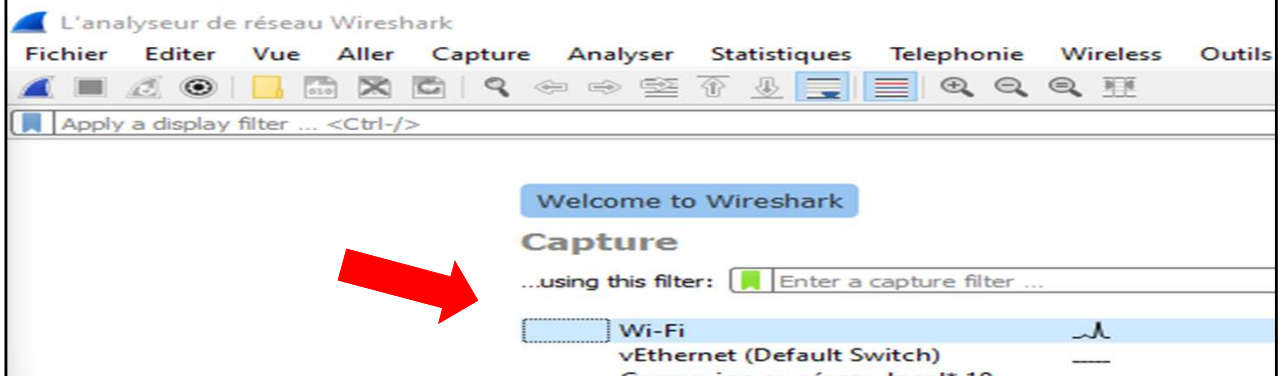
- D'où provient mon adresse IP ?
- Trois étapes :
 - 1 - préparation
 - 2 - capture
 - 3 - analyse



Préparation avant capture

27

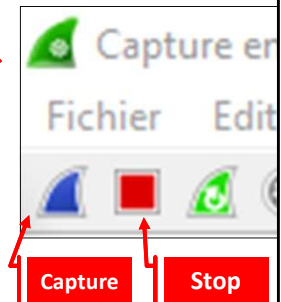
- Ouvrir un terminal avec des droits élevés (ou faire des sudo si besoin)
- Ouvrir Wireshark avec des droits élevés (sudo / Ouvrir en administrateur)
- Repérer votre carte réseau dans Wireshark
- ATTENDRE AVANT DE CAPTURER



Capturer le renouvellement d'une adresse IP

29

1. Dans Wireshark, capturer le trafic réseau
2. Dans le terminal, saisir :
 - Linux : **dhclient** 'Nom de votre carte réseau'
Exemple **dhclient enp0s3**
 - Windows :
ipconfig /release && ipconfig /renew
3. STOPPER la capture et indiquer dans Wooclap que c'est fait



Linux : dhclient demande au serveur DHCP de donner une adresse IP à la carte réseau spécifiée

Windows : ipconfig /release efface la configuration reçue du DHCP, ipconfig /renew demande une nouvelle configuration

En WiFi, il est aussi possible de se déconnecter, lancer la capture et connecter au réseau

Attention, si le fournisseur n'est pas sur le réseau local, les informations viendront de la passerelle.

Analyser la capture Wireshark

31

Dans Wireshark, analyser la capture pour retrouver :

- Les trames liées au renouvellement d'adresse IP
- Le protocole ou les protocoles utilisés
- Les éventuelles informations supplémentaires fournies
(Il faut chercher dans la bonne couche de la trame dans Wireshark 😊)
- L'adresse IP du serveur

Le nombre de trames affichées

Filtre : bootp



Linux : dhclient demande au serveur DHCP de donner une adresse IP à la carte réseau spécifiée

Windows : ipconfig /release efface la configuration reçue du DHCP, ipconfig /renew demande une nouvelle configuration

En WiFi, il est aussi possible de se déconnecter, lancer la capture et connecter au réseau

Attention, si le fournisseur n'est pas sur le réseau local, les informations viendront de la passerelle.

L'offre du DHCP Dynamic Host Configuration Protocol

32

No.	Time	Source	Destination	Protocol	Length	Info
4	0.642682	192.168.1.254	192.168.1.24	DHCP	342	DHCP Offer
5	0.643336	0.0.0.0	255.255.255.255	DHCP	360	DHCP Request
6	0.650228	192.168.1.254	192.168.1.24	DHCP	354	DHCP ACK


```
> Frame 4: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device
> Ethernet II, Src: Sagemcom_00:b8:4c (78:65:59:00:b8:4c), Dst: IntelCor_3a:ac:0f (4c:1d:96:3
> Internet Protocol Version 4, Src: 192.168.1.254, Dst: 192.168.1.24
> User Datagram Protocol, Src Port: 67, Dst Port: 68
  Dynamic Host Configuration Protocol (Offer)
    Message Type: Boot Reply (2)
    Hardware Type: Ethernet (10801)
    > Option: (53) DHCP Message Type (Offer)
    > Option: (54) DHCP Server Identifier (192.168.1.254)
    > Option: (51) IP Address Lease Time
    > Option: (58) Renewal Time Value
    > Option: (59) Rebinding Time Value
    > Option: (28) Broadcast Address (192.168.1.255)
    > Option: (6) Domain Name Server
    > Option: (15) Domain Name
    > Option: (3) Router
    > Option: (1) Subnet Mask (255.255.255.0)
    > Option: (255) End
    Padding: 000000
```

Fournisseur → Option: (54) DHCP Server Identifier (192.168.1.254)

Durée → Option: (51) IP Address Lease Time

Domaine → Option: (15) Domain Name

Passerelle → Option: (3) Router

Masque → Option: (1) Subnet Mask (255.255.255.0)

Offre IP → Option: (53) DHCP Message Type (Offer)

Un serveur DHCP répond en proposant adresse IP, masque, durée de bail
Il utilise le protocole de transport UDP avec les ports 67 et 68

FIN DU TD 2

