

Les Réseaux Informatiques

TD 1



1

Connectez-vous sur www.wooclap.com/UFSBGI

2

Vous pouvez participer

thierry.bacon@insa-rouen.fr

Les TD : Objectifs

1. Découvrir le matériel physique utilisé
2. Quel est mon réseau local et son étendue
3. Comment sortir de mon réseau local
4. Maitriser les commandes et outils pour l'analyse des couches

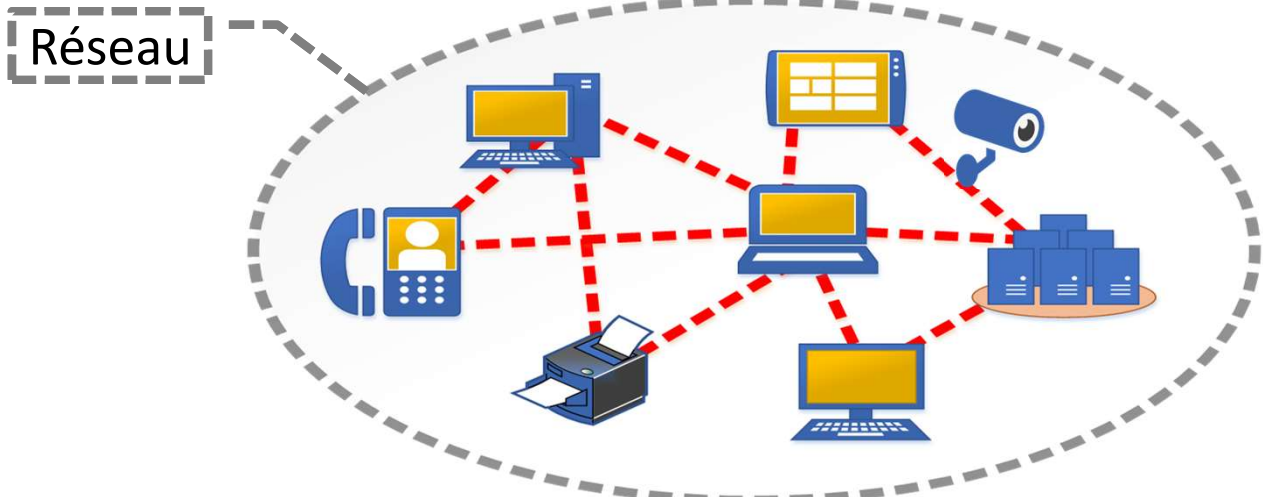


Analyse de son environnement

L'objectif du jour est d'utiliser les commandes systèmes pour comprendre notre environnement de travail réseau (carte réseau, configuration IP etc...)

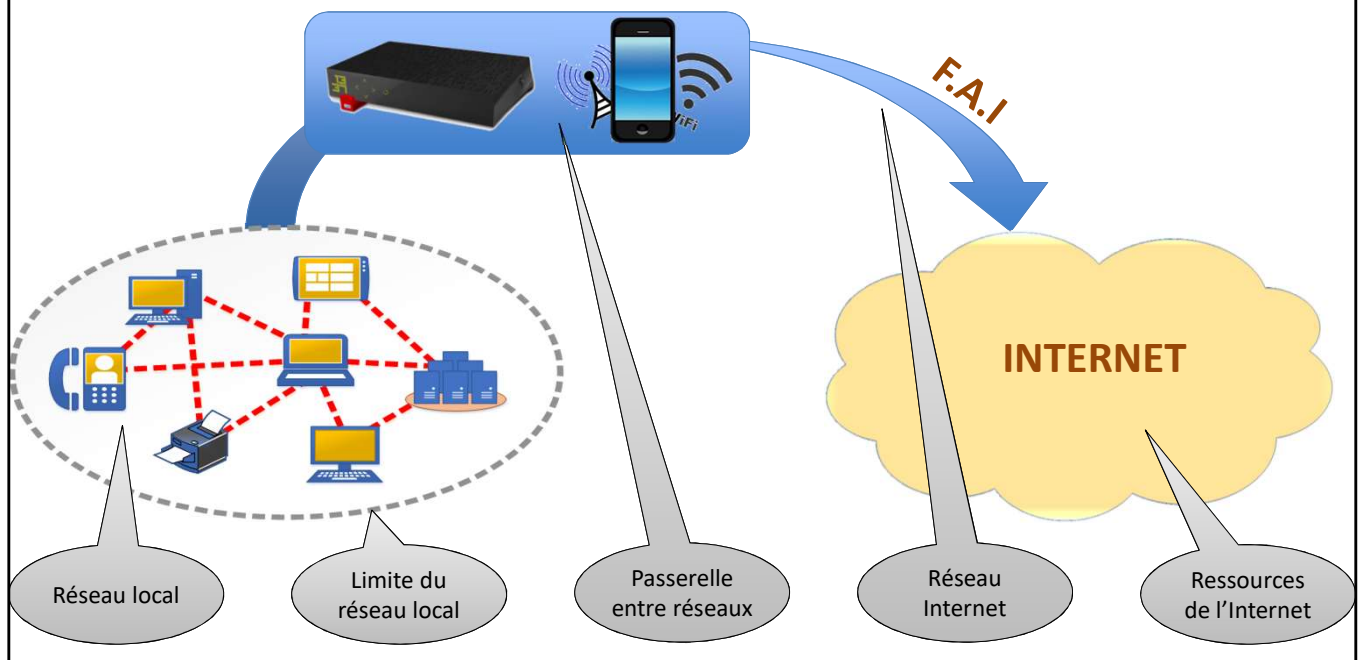
Le réseau local

- Définition d'un « Réseau Informatique »
Ensemble d'ordinateurs ou de terminaux interconnectés par des télécommunications généralement permanentes.



Rappel du cours

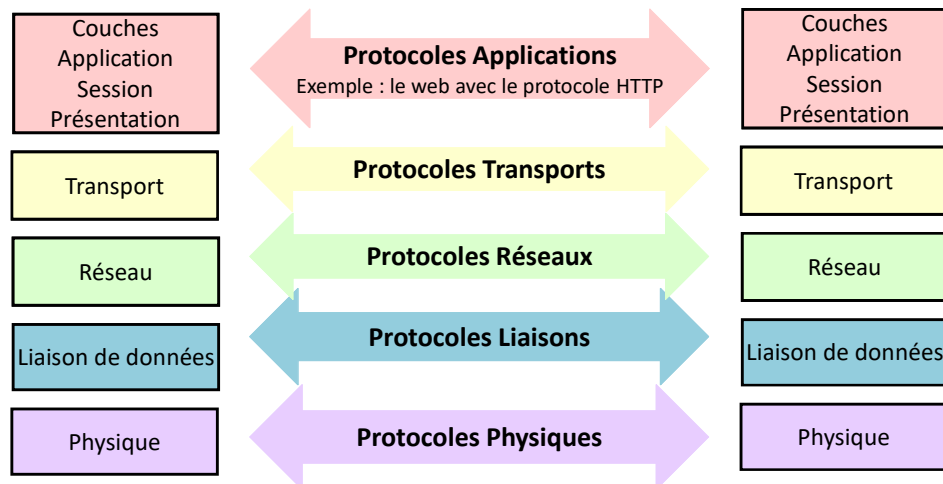
Du réseau local a l'Internet



Rappel lié au vocabulaire

Les communications du point de vue de l'INTERNET

- L'internet fonctionne suivant un **modèle en couches**, similaire au **modèle OSI**. Les éléments appartenant aux **mêmes couches** utilisent un **protocole de communication** pour s'échanger des informations.

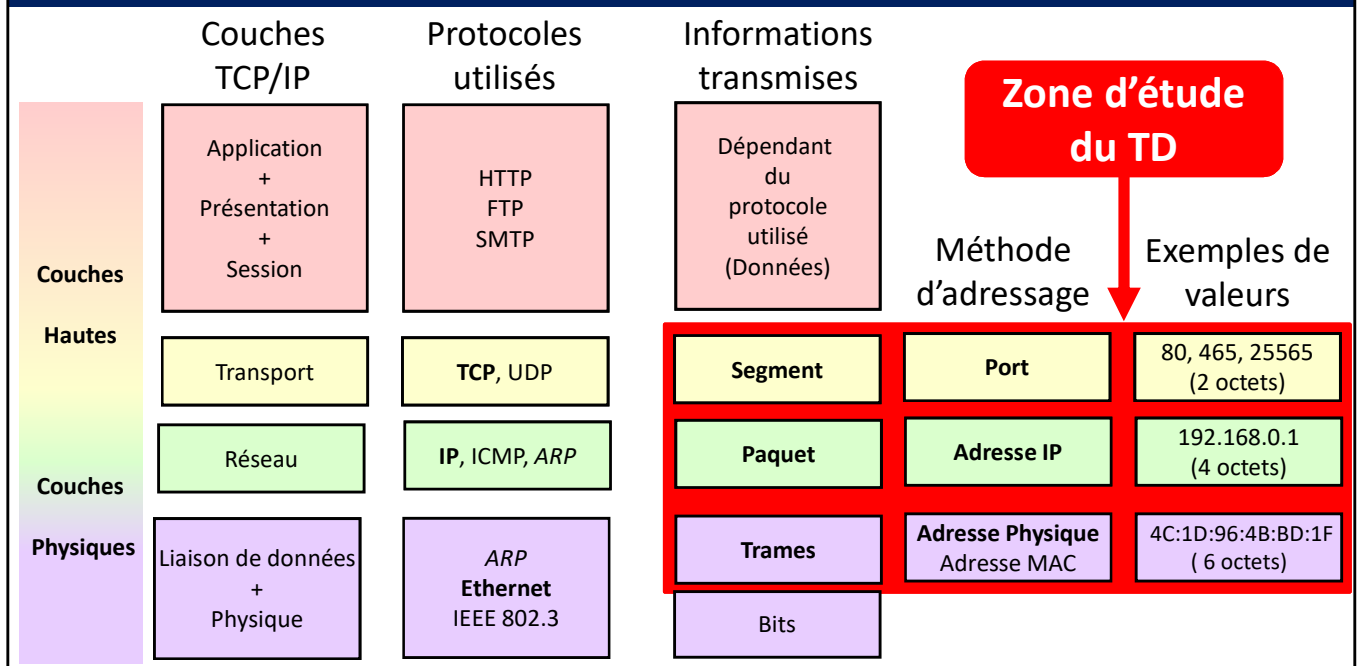


Du point de vue des couches, le dialogue se fait entre couches identiques, sans connaître le fonctionnement ou les réglages des autres couches

Pour le web, il ne semble exister que le client « Firefox » par exemple, et le site web consulté.

Si on fait une analogie de type colis, c'est comme si la commande, d'une « boîte bleue », qui serait livrée rapidement, cachait les étapes de fabrication, mise en paquet, transport par la société de livraison ainsi que les routes et camions utilisés.

Les couches et leurs vocabulaires

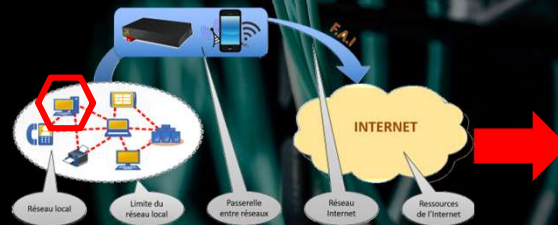


Couche transport :

- Le port 80 est le port par défaut pour le Web (HTTP), 443 pour le HTTPS
- Le port 25 est le port SMTP (Simple Mail Transfert Protocol) par défaut, le 465 est le SMTPS
- Le port 25565 est le port par défaut des serveurs Minecraft d'après Wikipédia

Analyse 1

Présence physique
d'une carte réseau
dans mon PC



Application
+
Présentation
+
Session

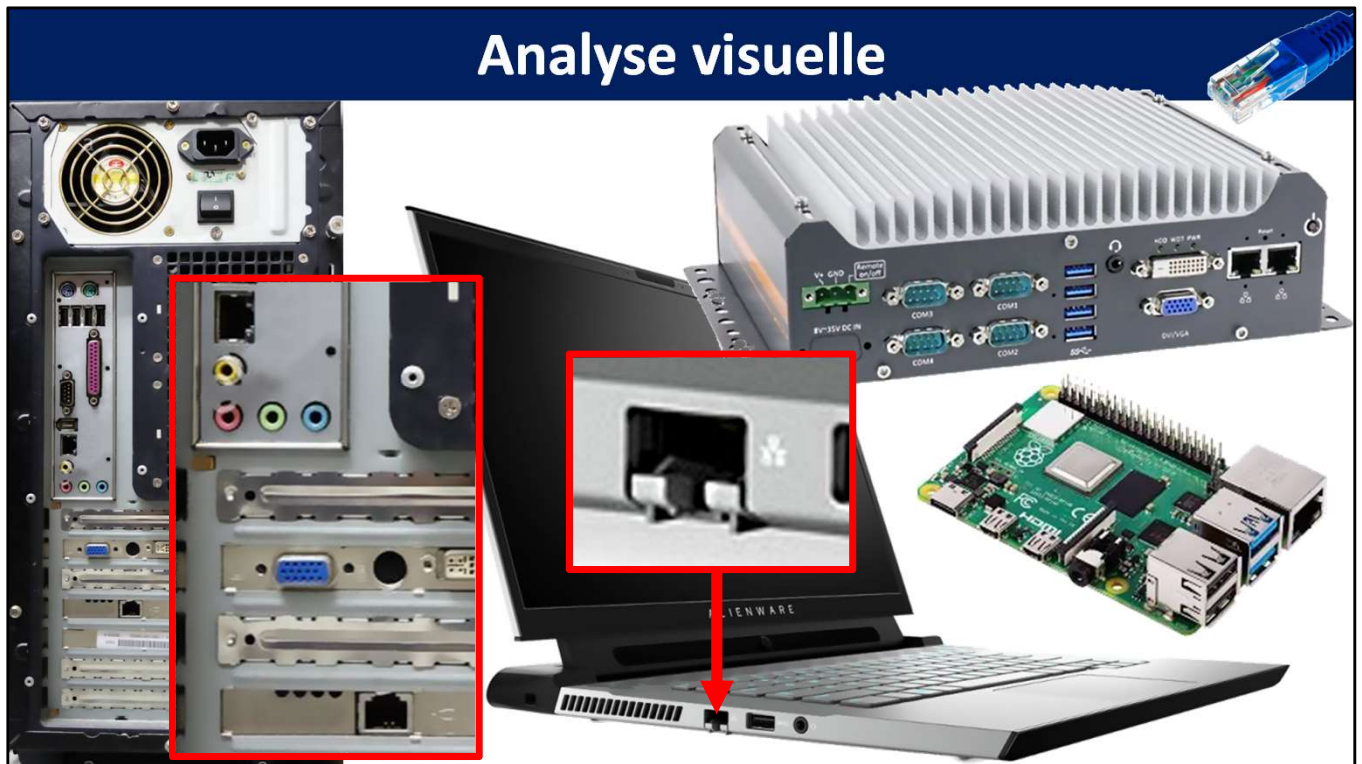
Transport

Réseau

Liaison
de données

Physique

Analyse visuelle



Recherche d'une carte réseau

Sous Linux saisir :



- **dmesg**
- **dmesg |grep -i eth**
Recherchez les mots clefs **eth**, **wlan** ou le nom du fabricant de la carte réseau (**Intel**, **Rtl...**).
- **lspci** liste les périphériques. Filtrer avec **|grep -i eth** (ou **wifi**)
- **lsusb** liste les périphériques usb

Sous Windows saisir :

- **driverquery /v** (avec un filtre possible ex : **|findstr réseau**)
Attention : complexe à analyser
- **devmgmt.msc** : Pour afficher le gestionnaire de périphériques

lspci (liste les périphériques pci du PC)

lspci |grep -i ether --color

Pour rechercher un mot clef tel qu'**ether**

L'objectif de la recherche c'est de s'assurer de la présence d'une carte réseau reconnue par l'OS.

Quel est le nom de la carte utilisé par le S.E?

Sous Linux :

- **ip a**
- **ifconfig (obsolète)**



Le nom devrait s'afficher en début de ligne, ethx, wlanx, enp0s3...

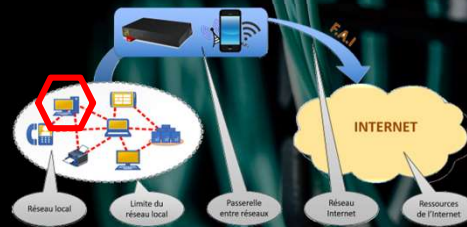
Sous Windows :

- **netsh interface ipv4 show interfaces**
filtre pour n'afficher que les interfaces connectées :
|findstr /V /C:disconnected

Le nom est généralement long : Ethernet; Wi-Fi

Analyse 2

Trouver l'adresse
physique de la carte
réseau



Application
+
Présentation
+
Session

Transport

Réseau

Liaison
de données

Physique

Quel est l'adresse physique de la carte ?

Cette adresse est utilisée pour **toutes** les communications de niveau 2.
Chaque **TRAME** contient les adresses physiques des interlocuteurs.



Elle se compose de 6 octets notés en hexadécimal.

Sous Linux :

- **ip a**
- **ifconfig (obsolète)** Chercher le nom Hwaddr ou link/ether

Sous Windows :

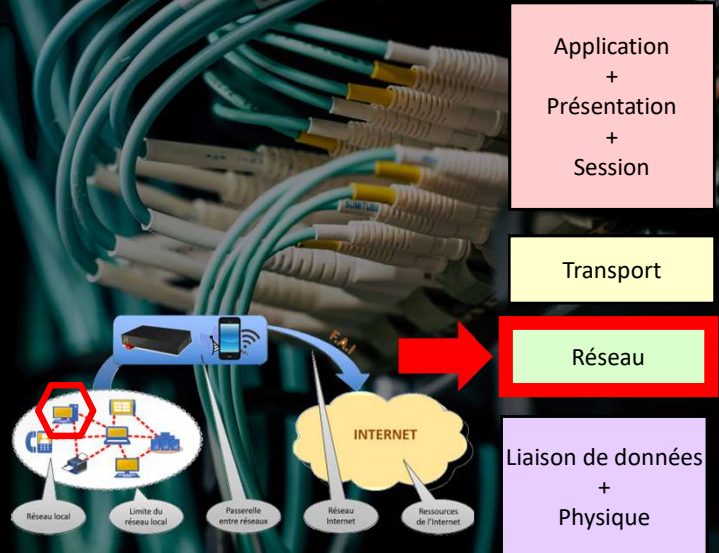
- **getmac /v /fo list**
- **Ipconfig /all**

Entre les PC du réseau local circulent des trames.

Le début de la trame contient l'adresse physique (MAC) du destinataire, ou des destinataires si la trame s'adresse à un groupe de machines.

Analyse 3

Contrôle d'une
configuration IP valide



Connaître sa configuration IP



Sous Linux :

- **ip a**
- **ifconfig (obsolète)**

Cherchez une ligne avec le mot **inet** ou **IPv4** dans la section de votre carte réseau

Sous Windows :

- **ipconfig**

Cherchez une ligne avec le mot **inet** ou **IPv4** dans la section de votre carte réseau

Note : L'adresse IPv4 se présente sous la forme de 4 octets notés xxx.xxx.xxx.xxx

Wireshark


Les outils pour mieux voir les communications et
notre environnement réseau

INSA INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
ROUEN



Les outils

■ ANALYSE DES COMMUNICATIONS:

- Wireshark (Tout OS) 
- Tcpdump (linux)

■ ANALYSE DES PORTS UTILISÉS PAR LA COUCHE TRANSPORTS

- Netstat (Tout OS)

■ ANALYSE DES HÔTES DU RÉSEAU ET DES SERVICES QU'ILS HÉBERGENT

- Nmap (tout OS)

■ ANALYSE DE LA ROUTE

- Tracert (Windows) traceroute (Linux)

Tracert -d pour ne pas résoudre les adresses IP

Wireshark

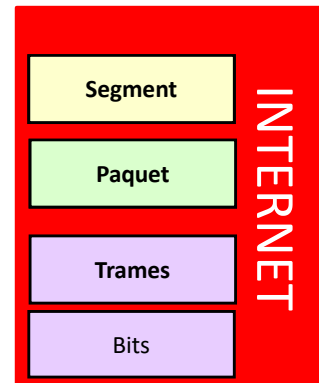


■ CE QUE PROPOSE LE LOGICIEL :

- Capture des « trames du réseau »
- Analyse en direct ou à partir d'un fichier

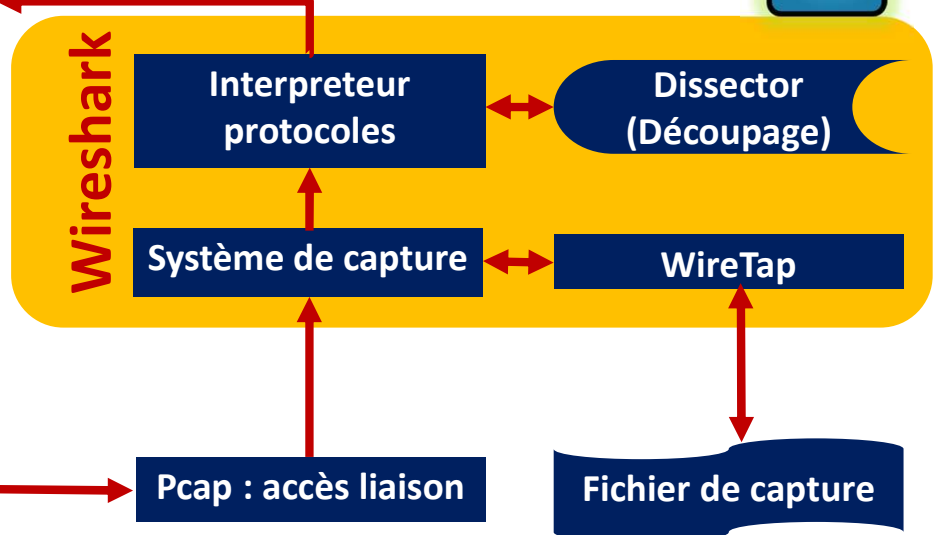
■ FONCTIONS DE WIRESHARK:

- Décrypte des centaines de protocoles
- Filtre lors de la capture ou lors de l'analyse

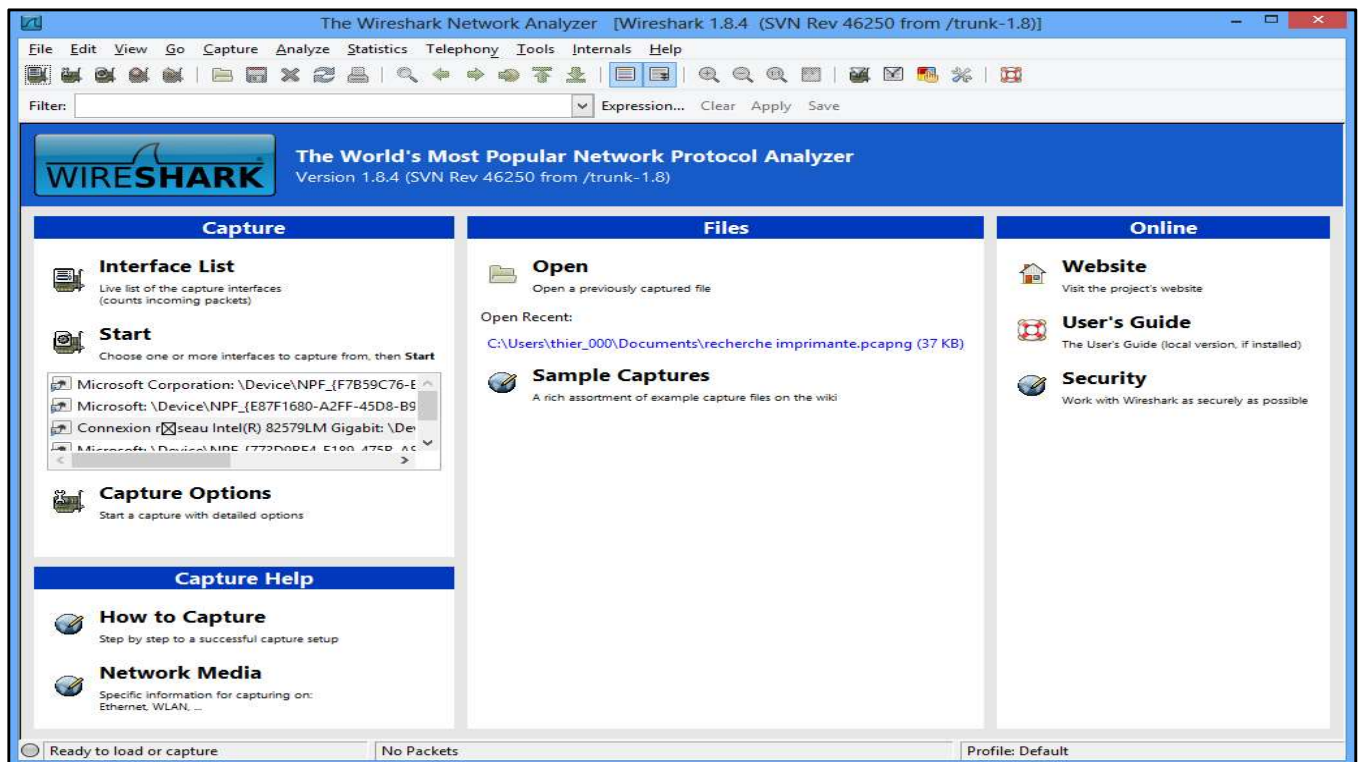


La trame est l'élément de base transmis sur le réseau Ethernet, sa taille est d'environ 1500 octets

Wireshark : fonctionnement global



Dissector : modules interne ou externe (plugins) / Pcap : accès à la couche de liaison (modif driver) avec library pour l'accès



Au démarrage, la liste des cartes réseaux s'affiche.

Attention : ce programme s'utilise avec des droits élevés sur le système (root ou administrateur)

Filtre d'affichage

Trames capturées

Détail trame couche par couche

Contenu brut de la trame

recherche imprimante.pcapng [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.0.1	239.255.0.1	UDP	211	Source port: 8375 Destination port: 9303
2	1.24816100	00:1b:11:69:a9:51	ff:ff:ff:ff:ff:ff	ARP	42	who has 192.168.0.17? (192.168.0.17)
3	4.85651900	Fe80::91e2:35a5:8b1	ff02::1:2	DHCPv6	171	solicit XID: 0xfffd6 CID: 0
4	7.90479900	192.168.0.26	192.168.0.255	NBNS	92	Name query NB WORKGROUP<id>
5	9.44085900	192.168.0.26	192.168.0.255	NBNS	92	Name query NB WORKGROUP<id>
6	9.44213900	192.168.0.26	192.168.0.255	NBNS	92	Name query NB WORKGROUP<id>
7	9.99972800	192.168.0.1	239.255.0.1	UDP	211	Source port: 8375 Destination port: 9303
8	11.4562560	68:94:23:6d:2f:24	ff:ff:ff:ff:ff:ff	ARP	42	who has 192.168.0.17? (192.168.0.17)
9	11.4889280	192.168.0.26	192.168.0.255	NBNS	92	Name query NB WORKGROUP<id>
10	11.4912320	192.168.0.26	192.168.0.255	BROWSE	225	Browser Election Request
11	12.0015670	a4:ee:57:12:81:ca	68:94:23:6d:2f:24	ARP	42	192.168.0.12 is at a4:ee:57:12:81:ca
12	12.0016040	192.168.0.19	192.168.0.12	TCP	66	49195 > 80 [SYN] Seq=14195
13	12.0035140	192.168.0.12	192.168.0.19	TCP	66	80 > 49195 [SYN, ACK] Seq=14195
14	12.0036840	192.168.0.19	192.168.0.12	TCP	54	49195 > 80 [ACK] Seq=14195

Frame 1: 211 bytes on wire (1688 bits), 211 bytes captured (1688 bits) on interface 0

Ethernet II, Src: 00:1b:11:69:a9:51 (00:1b:11:69:a9:51), Dst: 68:94:23:6d:2f:24 (68:94:23:6d:2f:24)

Internet Protocol version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 239.255.0.1 (239.255.0.1)

User Datagram Protocol, Src Port: 8375 (8375), Dst Port: 9303 (9303)

Data (169 bytes)

0000 68 94 23 6d 2f 24 00 1b 11 69 a9 51 08 00 45 00 n.#m/\$.-.i.Q..E.

0010 00 c5 3a 2a 00 00 40 11 8f 54 c0 a8 00 01 ef ff ...%..@..T.....

0020 00 01 20 b7 24 57 00 b1 a3 54 4b 41 4e 4e 4f 55 ...\$.w..TKANNOU

0030 25 4e 00 00 00 00 00 1b 11 69 a9 51 64 6c 69 %N.....i.qdTi

0040 6e 6b 72 6f 75 74 65 72 00 00 00 00 6b 63 33 nkrouter.....kc3

0050 30 32 00 00 00 00 00 00 00 00 00 00 00 00 00 02123.....

0060 00 31 32 33 00 00 00 00 00 00 00 00 00 00 00 00123.....

0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00123.....

0080 00 32 2e 33 32 00 00 00 00 31 32 33 00 00 00 00123.....

0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02123.....

00a0 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00123.....

00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00123.....

Frame (frame), 211 bytes Packets: 182 Displayed: 182 Marked: 0 Load time: 0:00.020 Profile: Default

Wireshark : Phase 2 analyse



Analyse des trames pour trouver un dialogue HTTP

- Recherche dans la colonne Infos
- Filtrer !

The image shows a Wireshark packet capture analysis. A magnifying glass highlights the 'Info' column of a packet, showing the following details:

- TCP 78 63553 → 80
- TCP 74 80 → 63553
- IGMPv2 46 Membership Report
- TCP 66 63553 → 80 [ACK]
- HTTP 414 GET / HTTP/1.1
- TCP 174 [TCP segment of a reassembled PDU]
- TCP 66 63553 → 80
- HTTP 298 HTTP/1.0 200 OK
- TCP 66 80 → 63553
- TCP 66 63553 → 80

The main packet list shows the following details for the selected packet (No. 13):

No.	Time	Source	Destination	Protocol	Length	Info
5	0.000000	IntelCor_71:02:eb	Sagecon_aa:24:42	ARP	42	Iho has 192.168.0.17 Tell 192.168.0.20
6	2.595871	Sagecon_aa:24:42	IntelCor_71:02:eb	ARP	60	192.168.0.1 is at 7c:03:d8:aa:24:42
7	3.595520	192.168.0.20	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
8	5.826790	192.168.0.5	224.0.0.251	PDNS	164	Standard query response 0x0000 TXT, cache flush
9	6.453365	192.168.0.5	192.168.0.20	TCP	78	63553 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 TSval=282429804 TSecr=0 PERM=1
10	6.453462	192.168.0.20	192.168.0.5	TCP	74	80 → 63553 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=282429804 TSecr=282429804
11	6.594026	192.168.0.20	224.0.0.251	IGMPv2	46	Membership Report group 224.0.0.251
12	6.618051	192.168.0.5	192.168.0.20	TCP	66	63553 → 80 [ACK] Seq=1 Ack=1 Win=6668 Len=0 TSval=282429501 TSecr=1207552
13	6.613434	192.168.0.5	192.168.0.20	HTTP	414	GET / HTTP/1.1
14	6.619322	192.168.0.20	192.168.0.5	TCP	174	[TCP segment of a reassembled PDU]
15	6.622455	192.168.0.5	192.168.0.20	TCP	66	63553 → 80 [ACK] Seq=349 Ack=349 Win=66500 Len=0 TSval=282429512 TSecr=1207712
16	6.626638	192.168.0.20	192.168.0.5	HTTP	298	HTTP/1.0 200 OK (text/html)
17	6.626917	192.168.0.20	192.168.0.5	TCP	66	80 → 63553 [FIN, ACK] Seq=341 Ack=349 Win=66500 Len=0 TSval=1207724 TSecr=282429512
18	6.630913	192.168.0.5	192.168.0.20	TCP	66	63553 → 80 [ACK] Seq=349 Ack=341 Win=66376 Len=0 TSval=282429519 TSecr=1207724
19	6.630914	192.168.0.5	192.168.0.20	TCP	66	63553 → 80 [FIN, ACK] Seq=349 Ack=341 Win=66600 Len=0 TSval=282429519 TSecr=1207724
20	6.630914	192.168.0.5	192.168.0.20	TCP	66	[TCP Out-of-Order] 63553 → 80 [FIN, ACK] Seq=349 Ack=342 Win=66600 Len=0 TSval=120425240 TSecr=1207724
21	8.298881	192.168.0.5	192.168.0.20	TCP	66	[TCP Spurious Retransmission] 63553 → 80 [FIN, ACK] Seq=349 Ack=342 Win=66600 Len=0 TSval=282431892 TSecr=1207724
22	8.296915	192.168.0.20	192.168.0.5	TCP	54	[TCP ZeroWindow] 80 → 63553 [ACK] Seq=342 Ack=350 Win=0 Len=0
23	8.296902	192.168.0.5	192.168.0.20	TCP	66	[TCP Out-of-Order] 63553 → 80 [ACK] Seq=350 Ack=342 Win=66600 Len=0 TSval=282431180 TSecr=1207724
24	8.626707	192.168.0.20	192.168.0.17	NDPSS	55	NDPSS Continuation Message
25	8.631619	192.168.0.17	192.168.0.20	TCP	66	445 → 49837 [ACK] Seq=1 Ack=2 Win=914 Len=0 SLE=1 SRE=2
26	9.215109	192.168.0.19	224.0.0.251	PDNS	164	Standard query response 0x0000 TXT, cache flush

The packet details pane shows the following information for the selected packet (No. 13):

- Frame 13: 414 bytes on wire (3312 bits), 414 bytes captured (3312 bits) on interface 0
- Ethernet II, Src: Apple_88:93:ab (08:23:6c:88:93:ab), Dst: IntelCor_71:02:eb (e8:b3:18:71:02:eb)
- Internet Protocol Version 4, Src: 192.168.0.5, Dst: 192.168.0.20
- Transmission Control Protocol, Src Port: 63553, Dst Port: 80, Seq: 1, Ack: 1, Len: 348
- Hypertext Transfer Protocol
- GET / HTTP/1.1

Wireshark : Phase 2 l'analyse

Simplification de l'affichage avec un filtre :

- Il ne reste que 2 lignes
- Utilisation du filtre 'HTTP'

The screenshot shows the Wireshark interface with the filter bar set to 'http'. The packet list displays two packets:

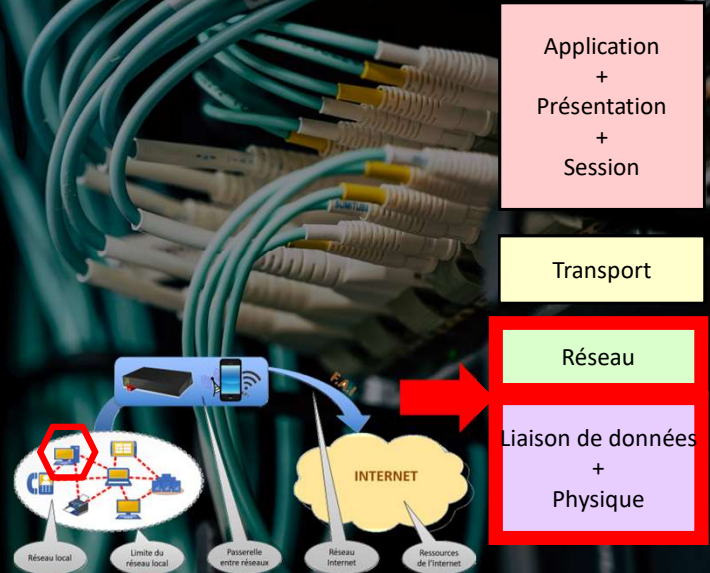
No.	Time	Source	Destination	Protocol	Length	Info
13	6.613434	192.168.0.5	192.168.0.20	HTTP	414	GET / HTTP/1.1
16	6.626638	192.168.0.20	192.168.0.5	HTTP	298	HTTP/1.0 200 OK (text/html)

The details pane for the selected packet (No. 16) shows the Hypertext Transfer Protocol section expanded, displaying the following information:


```
GET / HTTP/1.1\r\nHost: 192.168.0.20\r\nUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.78.2 (KHTML, like Gecko) Vers\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\nCache-Control: max-age=0\r\nAccept-Language: fr-fr\r\n
```

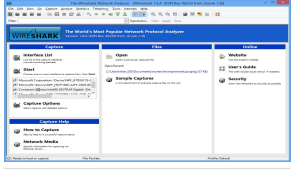
Analyse 4

Observation avec
Wireshark



Wireshark : Analyse passive

- Lancez une capture Wireshark 
- Regardez défiler les protocoles ●
- Indiquez dans le questionnaire WOOLAP celui qui vous semble revenir le plus souvent



	Protocol	Length	Info
:42		42	Who
:eb		60	192.
0		46	Memt
		164	Star
		78	6355
		74	80 →
		46	Memt
		66	6355
		414	GET
		174	[TCP
		66	6355
		298	HTTP
		66	80 →

FIN DU TD 1

