

# Technologies de l'information



**Cours:**

**Sécurité des systèmes  
informatiques**

Séance # 8

Préparé par: Blaise Arbouet

**DESS**



# Contenu de la séance

Principes fondamentaux des réseaux: Modèle OSI

Sécurité du réseau (Pare-feu, VPN et systèmes de détection/prévention des intrusions (IDS/IPS)

Problèmes de sécurité sans fil

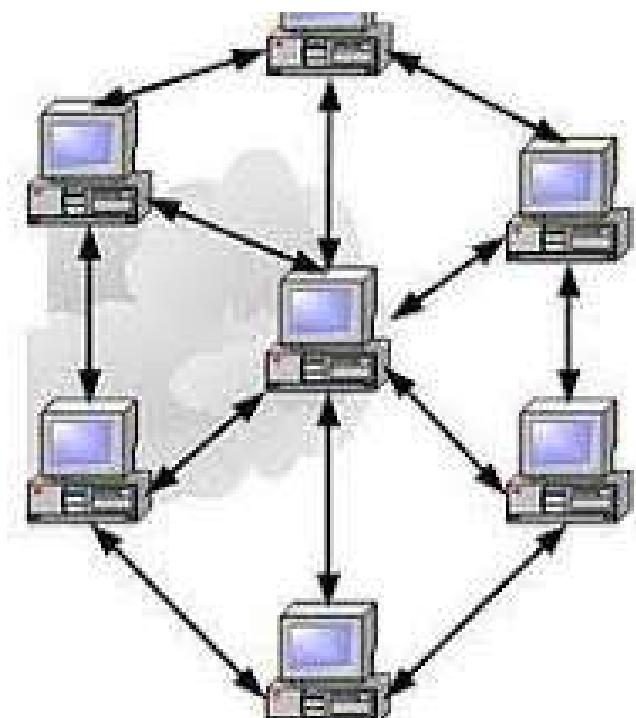
# Réseaux informatiques

---

« Un réseau informatique est un ensemble d'équipements reliés entre eux pour échanger des informations. (...)

On appelle nœud l'extrémité d'une connexion, qui peut être une intersection de plusieurs connexions ou équipements (un ordinateur, un routeur, un commutateur). »

Le réseau et son infrastructure, sont supportés par du câblage, les câbles permettent de relier physiquement les équipements. Interconnectés, ils auront des protocoles pour définir les services... Les réseaux filaires Ethernet respectent les normes (10baseT, 100baseT, 1000baseT, 10GbaseT). Parmi les protocoles, il y a des protocoles de communication qui permettent les transferts et les échangent de flux de données entre les équipements du réseau.



# Types de réseaux

---

1- Le découpage géographique des réseaux nous présente les grandes familles de réseaux comme ceci :

---

LAN : réseau local (Local area network)

---

MAN : réseau métropolitain (Metropolitan area network)

---

WAN : réseau étendu (Wide area network)

---

WLAN: Wireless LAN

---

Etc..

---

2- Le découpage fonctionnel, lui, nous présente les réseaux selon leurs services et leurs fonctions :

---

Réseau intranet : réseau interne à une entreprise;

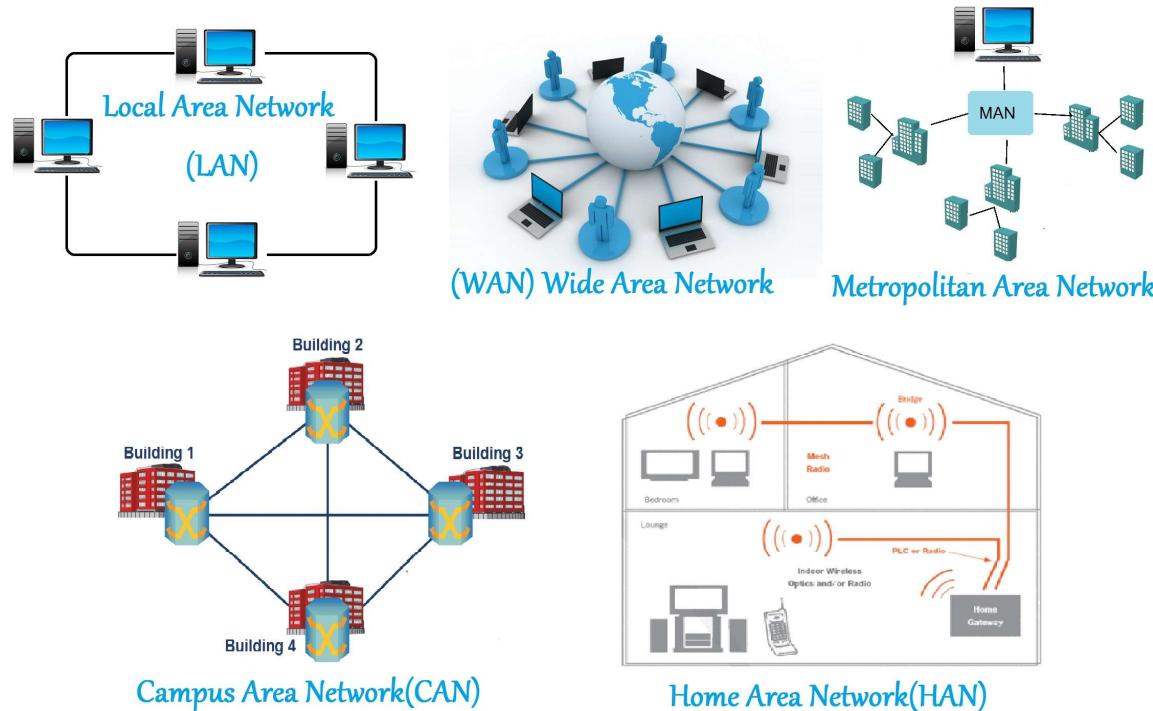
---

Réseau extranet : réseau externe d'une entreprise;

---

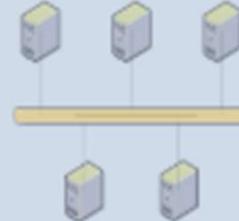
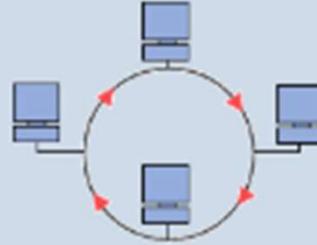
Réseau Internet : réseau interconnecté.

# Types de réseaux



## Types de réseaux (suite)

3- Le découpage peut aussi nous présenter les réseaux dans un découpage topologique :

Réseau en étoile	Réseau en bus	Réseau en anneau
 <p>Pc reliés à une « switch »</p>	 <p>Pc reliés par une ligne « en bus »</p>	 <p>Pc reliés à un répartiteur</p>

# Modèle OSI

« Le modèle OSI (de l'anglais Open Systems Interconnection) est un standard de communication, en réseau, de tous les systèmes informatiques. C'est un modèle de communications entre ordinateurs proposé par l'ISO (Organisation internationale de normalisation) qui décrit les fonctionnalités nécessaires à la communication et l'organisation de ces fonctions. »

Le modèle OSI a été créé en 1971 mais c'est seulement en 1984 qu'il deviendra une norme ISO. Ce « Modèle basique de référence pour l'interconnexion des systèmes ouverts (OSI) » a été sur planté par un autre modèle celui du TCP/IP. On verra ce modèle plus tard.

# Modèle OSI (suite)

Le modèle OSI c'est : En premier lieu, une architecture en plusieurs couches qui sont définies et délimitées par des notions de services, protocoles et interfaces:

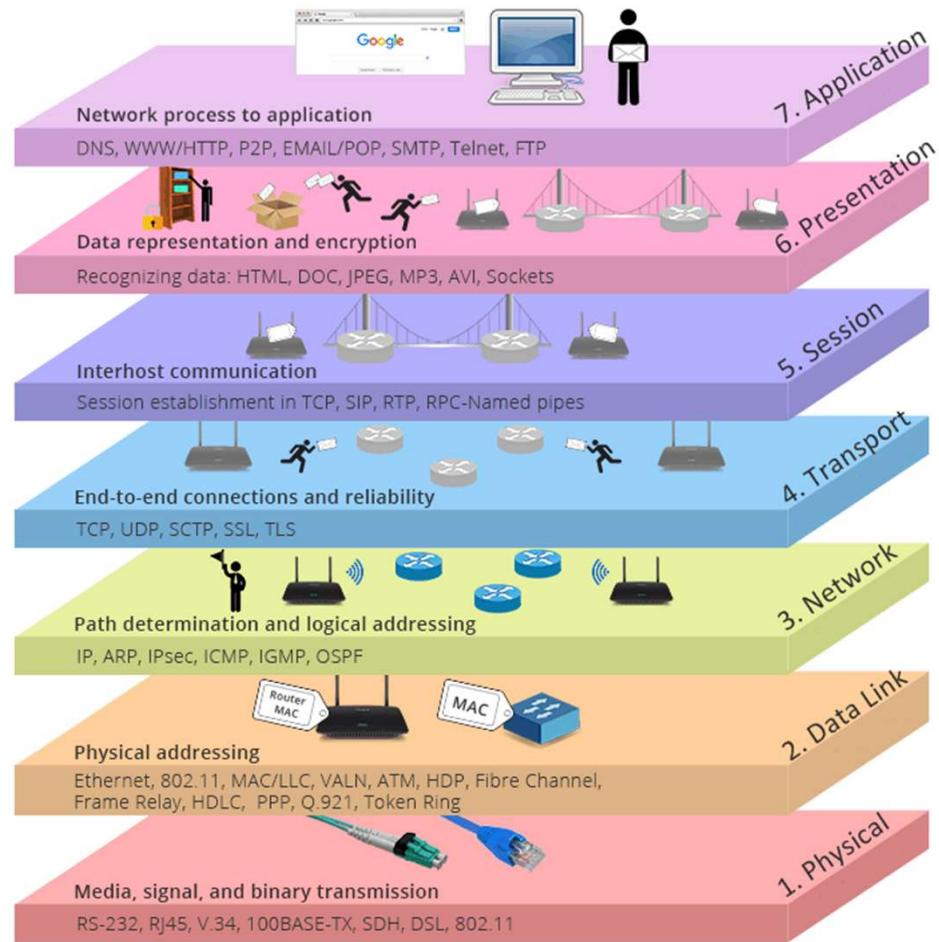
Un service : description de fonctions;

Un protocole : ensemble de messages/règles d'échange qui réalise le service;

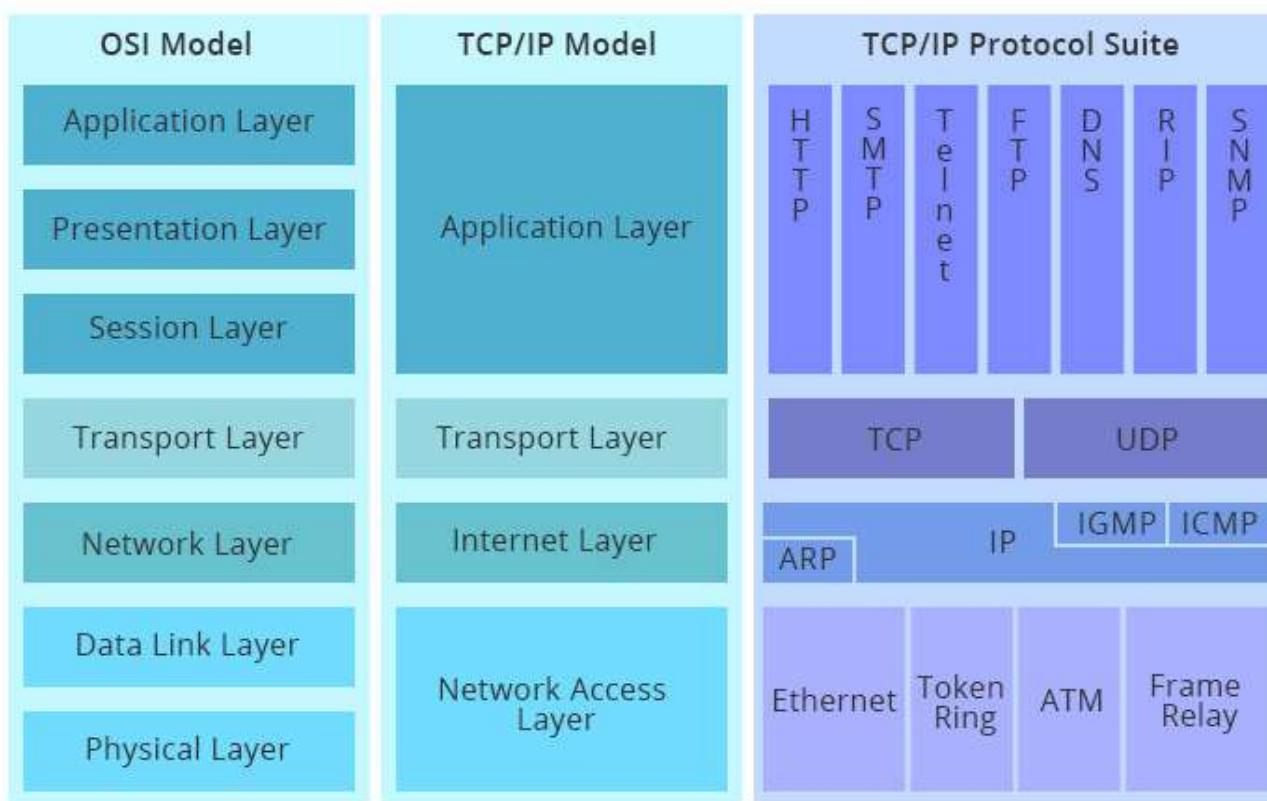
Une interface : moyen pour utiliser un programme.

Chaque couche à son rôle et ses responsabilités. Elles ont toutes un travail à faire. Chacune des couches a des standards et des protocoles définis.

# Couches du modèle OSI



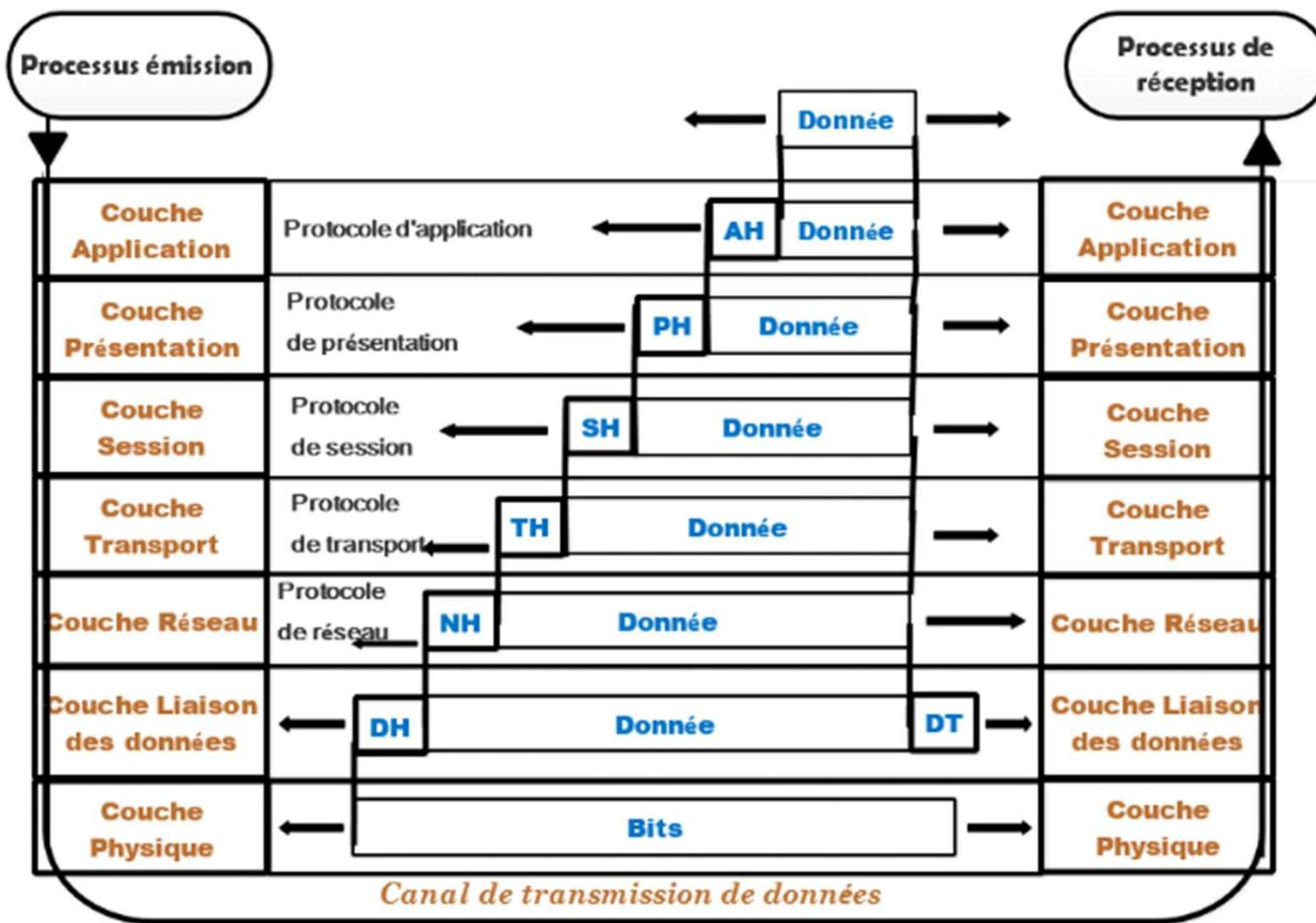
# OSI vs TCP/IP



# LE MODÈLE OSI

LE MODÈLE OSI PEUT ÊTRE CONSIDÉRÉ COMME UN LANGAGE UNIVERSEL POUR LES RÉSEAUX INFORMATIQUES. IL EST BASÉ SUR LE CONCEPT CONSISTANT À DIVISER UN SYSTÈME DE COMMUNICATION EN SEPT COUCHES ABSTRAITES, EMPILÉES LES UNES SUR LES AUTRES.

7		<b>COUCHE APPLICATION</b>	<i>Point de contact avec les services réseaux</i>		<b>DONNÉES</b>	TELNET, FTP, HTTP, SMTP, ETC.
6		<b>COUCHE PRÉSENTATION</b>	<i>Préparation des données pour la présentation (formatage, chiffrement, encodage etc.)</i>		<b>DONNÉES</b>	HTML, DOC, MP3, JPEG, ETC.
5		<b>COUCHE SESSION</b>	<i>Organisation de la session de communication (points de contrôle, etc.)</i>		<b>DONNÉES</b>	SIP, RTP, ETC.
4		<b>COUCHE TRANSPORT</b>	<i>Coordination du transfert des segments (numéro de port, contrôle réception, etc.)</i>		<b>SEGMENTS</b>	TCP, UDP, SSL, TLS, ETC.
3		<b>COUCHE RÉSEAU</b>	<i>Routage des paquets entre les noeuds d'un réseau</i>		<b>PAQUETS</b>	IP, ARP, ETC.
2		<b>COUCHE LIAISON</b>	<i>Assure le transfert des trames de noeud à noeud</i>		<b>TRAMES</b>	ETHERNET, PPP, ETC.
1		<b>COUCHE PHYSIQUE</b>	<i>Transmission des bits</i>		<b>BITS</b>	MULTIPLEXING, MODULATION, ETC.



Couche (couches basses et matérielles)	donnée	description	protocoles
3 réseau (network)	Paquets	<p>Le routage de l'information vers les réseaux et sur le réseau local entre les devices</p> <p>Matériel informatique : routeurs (transfert in/out du réseau)</p>	IP, ICMP, IPX...
2 liaison (data link)	Trames (série de bits, en-tête)	<p>Va établir et décider comment le transfert sera fait après la couche physique.</p> <p>Matériel informatique : les cartes réseau, « switch » (permet l'accès au réseau à plusieurs devices)</p>	802.3, 802.5, Ethernet...
1 physique (physical)	Bits (0-1)	C'est le transfert de données à travers le matériel informatique : concentrateur, câble RJ-45, etc.	100BaseT, 1000BaseT...

couche (couches hautes)	donnée	description	protocoles
7 application (application)	Données	Création des paquets et des messages, accès aux diverses bases de données. C'est la couche la plus près des utilisateurs. Cette couche implémente plusieurs protocoles pour activer les communications sur le réseau local et sur Internet	FTP, HTTP, POP3, SMTP...
6 présentation (présentation)	Données	S'assure de la traduction des formats de données lors de l'envoi (send) vers le receveur (receiver).	Protocoles présentation, de compression et de chiffrement, ASCII...
5 session (session)	Données	Responsable de la gestion des dialogues entre les ordinateurs. C'est l'établissement, la terminaison et la synchronisation de la session du SE sur le réseau (logon, logoff)	Protocole d'entrée et de sortie (logon/logoff), netbios, RPC...
4 transport (transport)	Segment (message) Datagram-me	Facilite le transfert et la transmission entre les hôtes, gestion des messages des couches 1 à 3	TCP, UDP...

v · m	Couches du modèle OSI	[masquer]
<b>7. Application</b>	AMQP · BGP · DHCP · DNS · FTP · FTPS · SFTP · FXP · Gemini · Gopher · H.323 · HTTP · HTTPS · IMAP · IPP · IRC · LDAP · LMTP · MODBUS · MQTT · NFS · NNTP · POP · RDP · RTSP · SILC · SIMPLE · SIP · SMB-CIFS · SMTP · SNMP · SOAP · SSH · TCAP · Telnet · TFTP · VoIP · WebDAV · XMPP	
<b>6. Présentation</b>	AFP · ASCII · ASN.1 · HTML · MIME · NCP · TDI · TLS · TLV · Unicode · UUCP · Vidéotex · XDR · XML	
<b>5. Session</b>	AppleTalk · DTLS · NetBIOS · RPC · RSerPool · SOCKS	
<b>4. Transport</b>	DCCP · QUIC · RSVP · RTP · SCTP · SPX · TCP · UDP	
<b>3. Réseau</b>	ARP · Babel · BOOTP · CLNP · ICMP · IGMP · IPv4 · IPv6 · IPX · IS-IS · NetBEUI · NDP · RIP · EIGRP · OSPF · RARP · X.25	
<b>2. Liaison</b>	Anneau à jeton (token ring) · Anneau à jeton adressé (Token Bus) · ARINC 429 · AFDX · ATM · Bitnet · CAN · Ethernet · FDDI · Frame Relay · HDLC · I <sup>2</sup> C · IEEE 802.3ad (LACP) · IEEE 802.1aq (SPB) · LLC · LocalTalk · MIL-STD-1553 · PPP · STP · Wi-Fi · X.21	
<b>1. Physique</b>	4B5B · ADSL · BHDn · Bluetooth · Câble coaxial · Codage bipolaire · CSMA/CA · CSMA/CD · DSSS · E-carrier · EIA-232 · EIA-422 · EIA-449 · EIA-485 · FHSS · HomeRF · IEEE 1394 (FireWire) · IrDA · ISDN · Manchester · Manchester différentiel · Miller · MLT-3 · NRZ · NRZI · NRZM · Paire torsadée · PDH · SDH · SDSL · SONET · SPI · T-carrier · USB · VDSL · VDSL2 · V.21-V.23 · V.42-V.90 · Wireless USB · 10BASE-T · 10BASE2 · 10BASE5 · 100BASE-TX · 1000BASE-T	

# Pour découvrir plus

---

## Modèle OSI

- <https://www.youtube.com/watch?v=YG57te3jqE8>
- Environ 7 minutes

## Protocoles

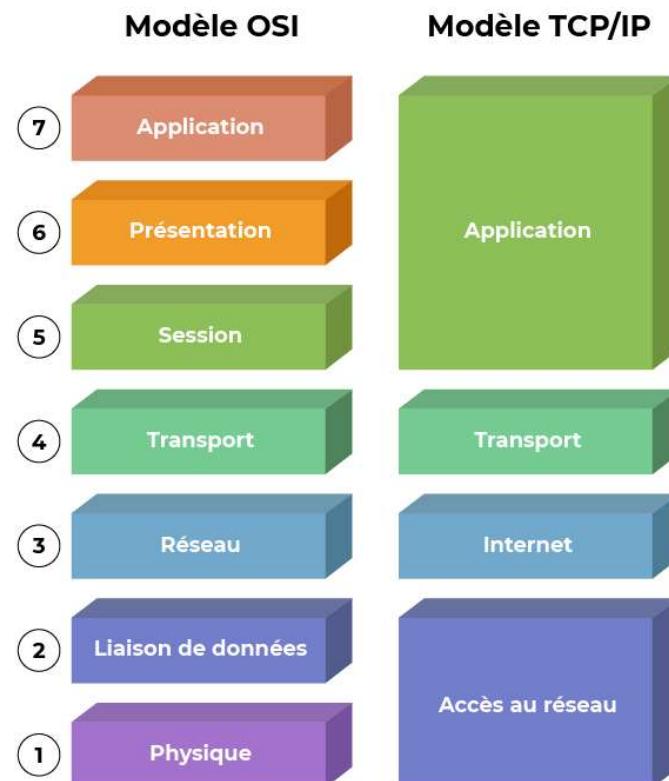
<https://www.youtube.com/watch?v=Ds7TvEvM9z4>

- Environ 6 minutes

## Vous écoutez après si vous voulez :

<https://www.youtube.com/watch?v=nigYvhsDrd4>

- Environ 14 minutes



# Protocole IP de la (couche réseau)

IP (Internet Protocol) : un protocole développé au début des années 80, c'est un protocole qui permet la communication entre les ordinateurs. C'est une adresse/numéro d'identification qui est attribué à un appareil connecté/branché à un réseau local ou Internet.

Une adresse IP est à la base du système d'acheminement des messages sur le réseau Internet. **La version 4 est actuellement utilisée et la version 6 est utilisée depuis peu, nous sommes en manque d'adresses IP v4.** Son identification est : quatre nombres entre 0-255 séparés par des « . »

# Classe d'adresses IP

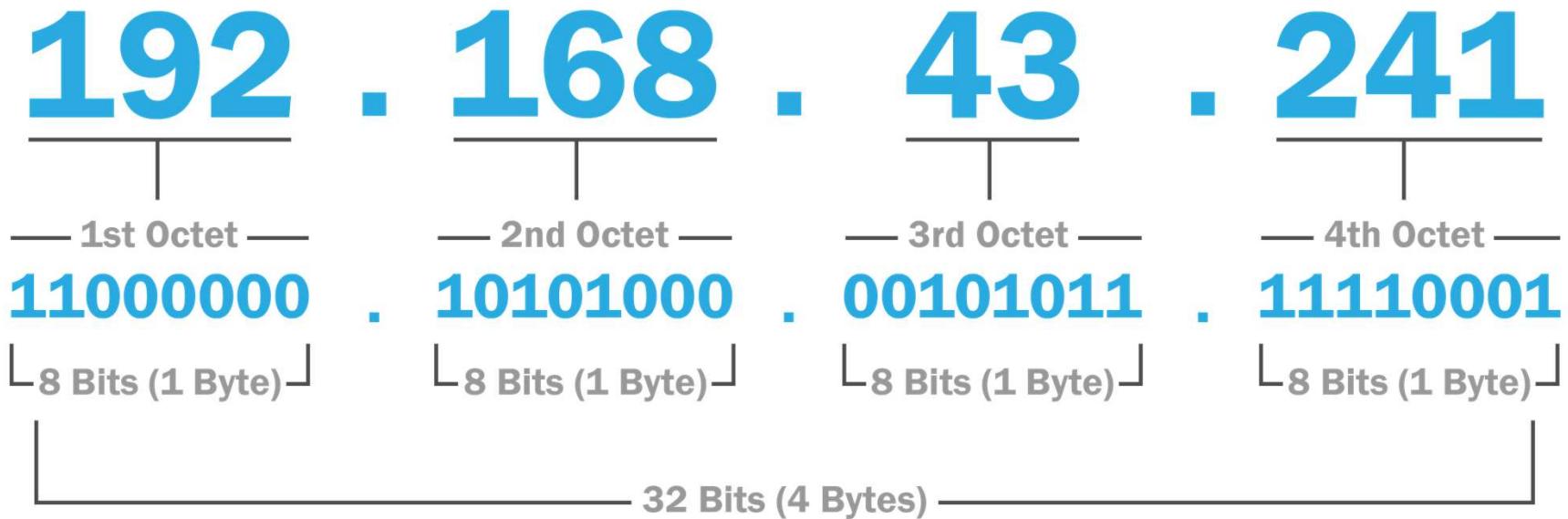
Classes d'IP	Plage d'IP	Masque de sous-réseau*
	0.0.0.0	Réserve, route par défaut
Classe A	1.0.0.0 à 127.255.255.255 adresses privées et publiques 10.0.0.0 à 10.255.255.255 privées	255.0.0.0
	127.0.0.1	Test sur votre réseau local, localhost
Classe B	128.0.0.0 à 191.255.255.255 adresses privées et publiques 172.16.0.0 à 172.31.255.255 privées	255.255.0.0
Classe C	192.0.0.0 à 223.255.255.255 adresses privées et publiques 192.168.1.0 à 192.168.255.255 privées	255.255.255.0
Classe D	224.0.0.0 à 239.255.255.255	Multicast (diffusion entre émetteur et récepteur)
Classe E	240.0.0.0 à 255.255.255.255	Réserve IETF

## Adresses IP privées

- Non routable

Classe	Plage d'adresse IP privée
A	10.0.0.0 - 10.255.255.255
B	172.16.0.0 - 172.31.255.255
C	192.168.0.0 - 192.168.255.255

# **IPv4 Address Format**



# IPv6 address

**2001 : 0DC8 : E004 : 0001 : 0000 : 0000 : 0000 : F00A**



16 bits : 16 bits



**128 Bits**

# IP (Internet Protocol) & sous-réseau

Si ça vous tente, vous pourrez écouter plus tard :

<https://www.youtube.com/watch?v=RnpSaDSSjR4>

Environ 22 minutes



# Protocole ARP (couche réseau)

ARP (« Address Resolution Protocol ») : ce protocole traduit une adresse du protocole de la couche réseau (adresse IP) en une adresse (physique) MAC (media access control). Il est à la bordure de la couche réseau (3) et liaison (2).

Exemple d'une adresse MAC :  
**00:45:00:a1:2b:cc**



# Trouver sa MAC

Invite de commandes

```
Microsoft Windows [version 10.0.19043.1526]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Utilisateur> ipconfig /all
```

C:\Users\Utilisateur>ipconfig

C:\Users\Utilisateur>getmac

Adresse physique	Nom du transport
00-FF-06-BC-DD-A7	Support déconnecté
50-7B-9D-9E-EC-C8	Support déconnecté
E0-94-67-E8-29-FC	N/A
0A-00-27-00-00-22	N/A
0A-00-27-00-00-04	N/A

dave@howtogeek:~\$ ip addr

[root@aimsit ~]# ifconfig

# Trouver sa MAC (suite)

Pour retrouver le OUI (organizationally unique identifier) de votre MAC :

- <https://aruljohn.com/mac.pl>
- [https://en.wikipedia.org/wiki/Organizationally\\_unique\\_identifier](https://en.wikipedia.org/wiki/Organizationally_unique_identifier) &
- [https://fr.wikipedia.org/wiki/Organizationally\\_Unique\\_Identifier](https://fr.wikipedia.org/wiki/Organizationally_Unique_Identifier)

Standard :

- <https://standards.ieee.org/products-services/regauth/index.html>

Liste des manufacturiers de MAC :

- <http://standards-oui.ieee.org/oui.txt>

Identifier  
votre MAC et  
identifier son  
OUI



aruljohn.com

Home

Blog

Bible

Code

MAC Address lookup

## MAC Address and OUI Lookup

This program displays the name of the company that manufactured your network card. You can also do a reverse lookup and find the MAC addresses registered by a company. You can [generate random MAC addresses](#).

Last Updated: 27 April 2025

MAC addresses: 54291

Vendors: 32471

**Lookup single MAC Address**

Multiple MAC Addresses

ENTER MAC ADDRESS OR OUI

lookup MAC address

# Pourquoi avoir besoin d'un adresse MAC?



La commande ARP est souvent utilisée par les administrateurs de réseau, mais aussi les « white hat » et les pirates : arp : affiche toutes les entrées des machines sur le réseau.



arp -a : affiche les entrées dans la cache ARP;



arp -a « IP » : affiche l'entrée d'une adresse IP spécifiée.

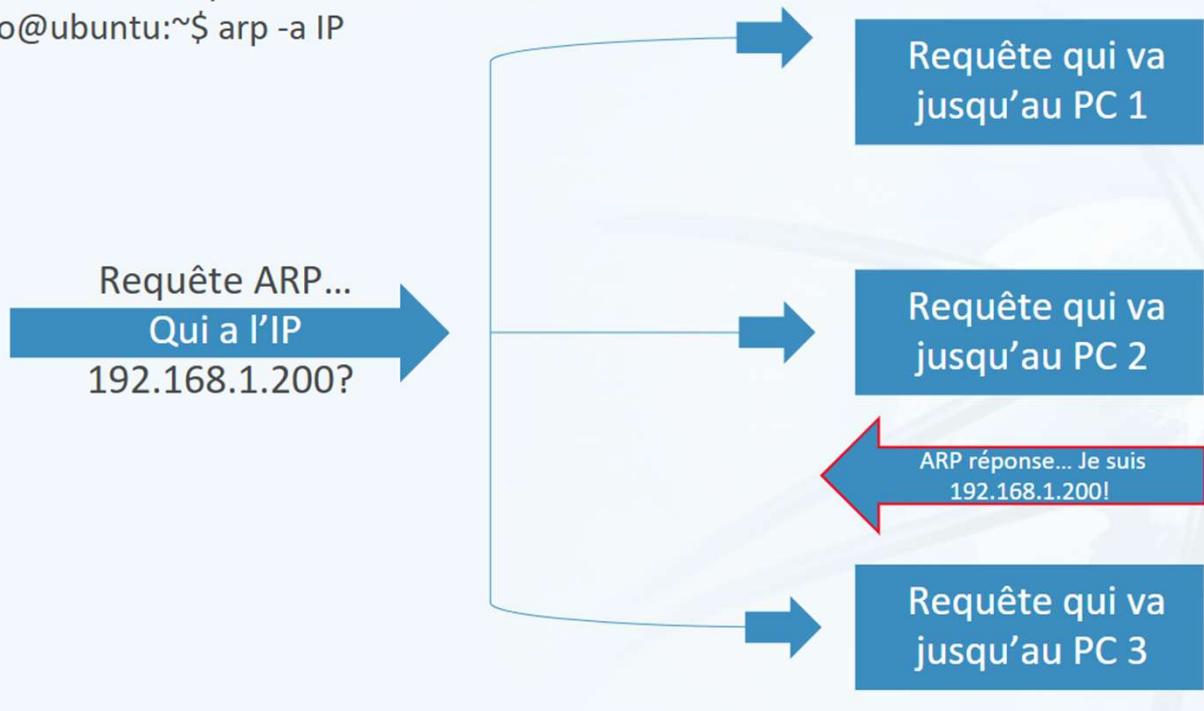


arp-v: affiche les entrées ARP actuelles en mode détaillé.

# Comment cela fonctionne?

La requête est envoyée sur le réseau local:

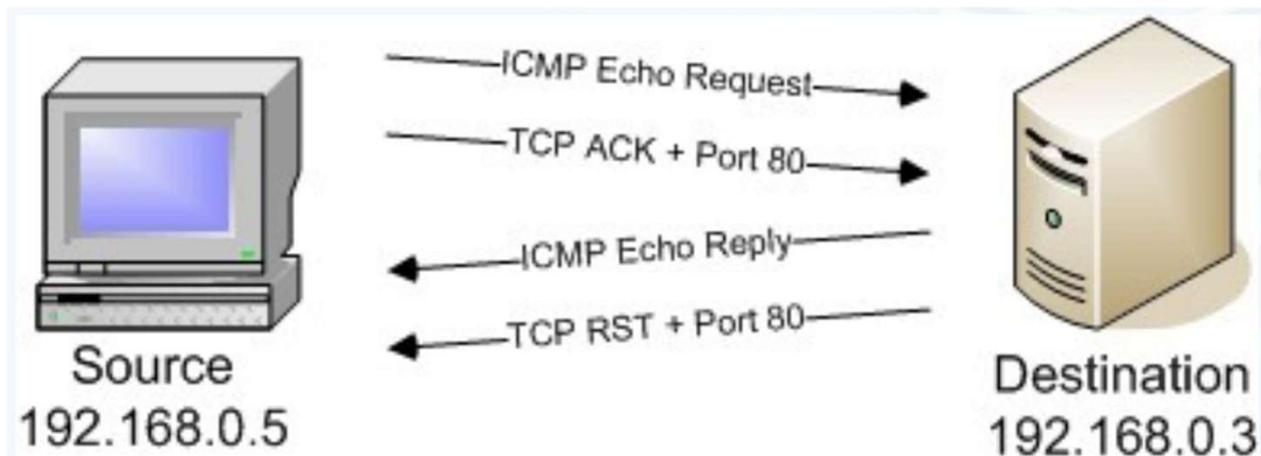
cybinfo@ubuntu:~\$ arp -a IP



# Protocole ICMP (couche réseau)

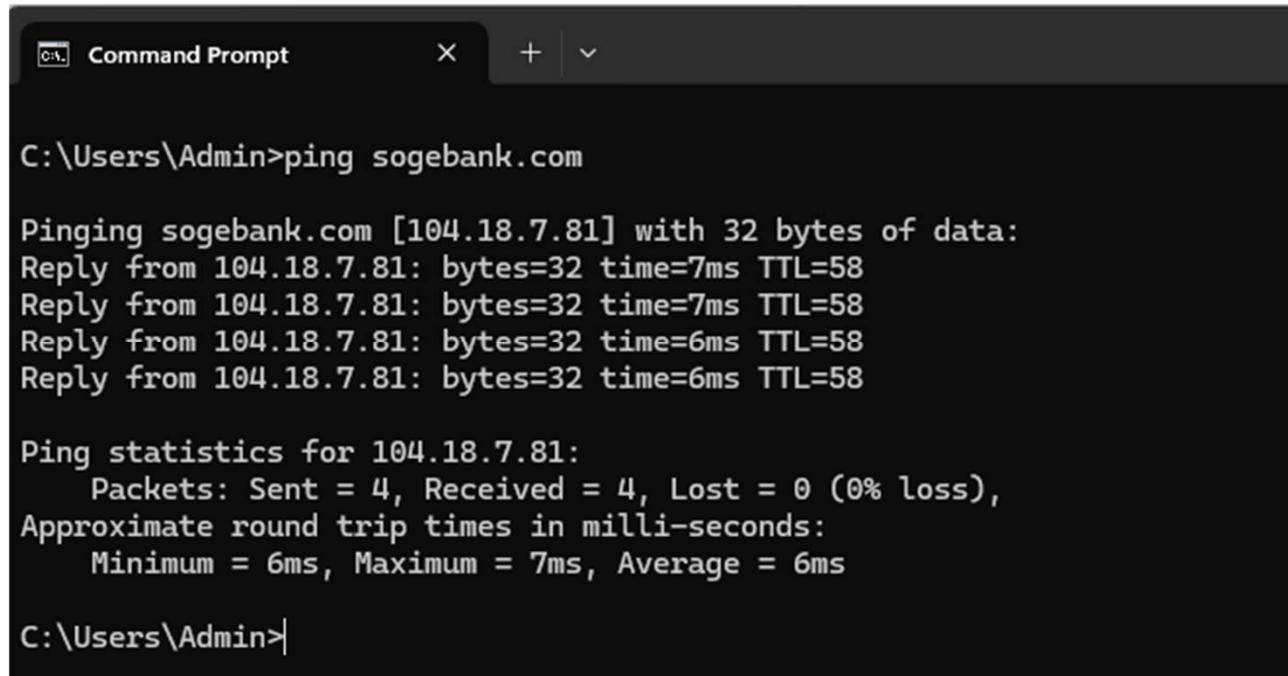
ICMP (Internet Control Message Protocol) : un protocole très important. Il véhicule les messages de contrôle et les messages d'erreur. RFC792. Les messages de contrôle sont envoyés quand la destination cause problèmes : non rejoignable, réseau congestionné, délais d'attendre.

La commande « **ping** » permet à un administrateur réseau, un pirate ou un « white hat » de vérifier si l'ordinateur à distance est connecté ou pas. Cette commande envoie des requêtes et c'est le protocole ICMP qui est en fonction. Il y a 18 types différents de messages d'erreur ou de succès.



# Commande PING

La commande ping est celle utilisée pour connaître l'état d'une machine, cette commande utilise le protocole ICMP : ping IP : indique si le poste est branché ou non (son état)



```
C:\Users\Admin>ping sagebank.com

Pinging sagebank.com [104.18.7.81] with 32 bytes of data:
Reply from 104.18.7.81: bytes=32 time=7ms TTL=58
Reply from 104.18.7.81: bytes=32 time=7ms TTL=58
Reply from 104.18.7.81: bytes=32 time=6ms TTL=58
Reply from 104.18.7.81: bytes=32 time=6ms TTL=58

Ping statistics for 104.18.7.81:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 7ms, Average = 6ms

C:\Users\Admin>
```

# Protocole TCP (couches 5-7)

TCP (Transmission Control Protocol) : est le protocole de transport sur un réseau et sur Internet. Transport vers les couches 5-7.  
RFC793.

TCP découpe le flux de données que les applications transmettent. TCP découpe ce flux en segments. Ce protocole a été développé en 1973 et a été rapidement adopté en 1983 comme modèle TCP/IP.

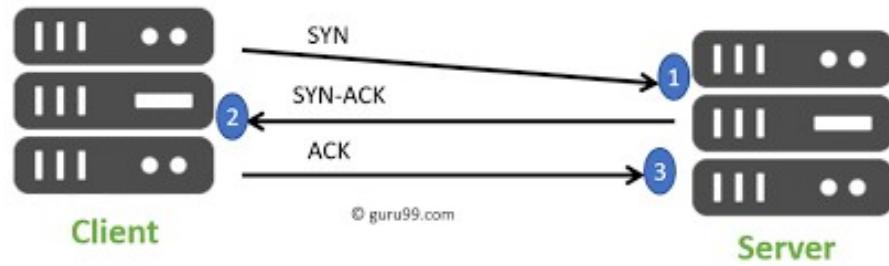
Une session TCP a trois étapes :

- L'établissement de la connexion;
- Les transferts de données;
- La fin de la connexion.

# Protocole TCP (suite)

Plusieurs ports utilisent le protocole TCP  
(FTP, SSH, Telnet, SMTP, HTTP, POP3).

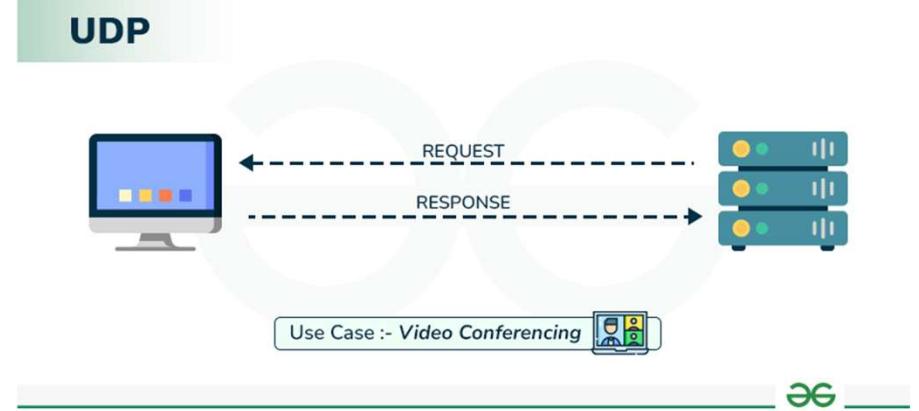
Plusieurs outils de piratage et de tests de sécurité utilisent le protocole TCP pour balayer ou tester une machine distante. Par exemple, l'outil NMAP a plusieurs arguments et options pour tester une session TCP.



# Protocole UDP

UDP (User Datagram Protocol) : est un protocole important. Ce protocole permet la transmission de données entre deux machines. Comme il n'a pas de procédure de connexion comme le TCP, il n'attend pas que l'autre machine lui donne le « OK » (« handshaking »), donc aucune négociation. Il ne peut donc pas garantir que les données sont rendues au bon endroit. Pas de vérifications d'erreurs. RFC768.

- Plusieurs ports utilisent le protocole UDP (DHCP, DNS, SNMP, TFTP, les jeux en réseau, le vidéo en « streaming »....).



# Protocole RTP

RTP (Real-Time Transport Protocol) : est un protocole de communication qui permet le transport des données lors de communication VoIP (téléphone IP) en combinaison avec un autre protocole SIP, vidéo conférence ou lors de l'écoute de vidéo en « streaming ».

Lors d'une enquête informatique, on peut utiliser la surveillance sur le réseau (technique de capture du trafic) pour enregistrer les conversations de type « téléphonique » (VoIP, SIP...) et pouvoir les écouter lors de l'analyse de la capture.

Wireshark est un excellent outil pour ça.

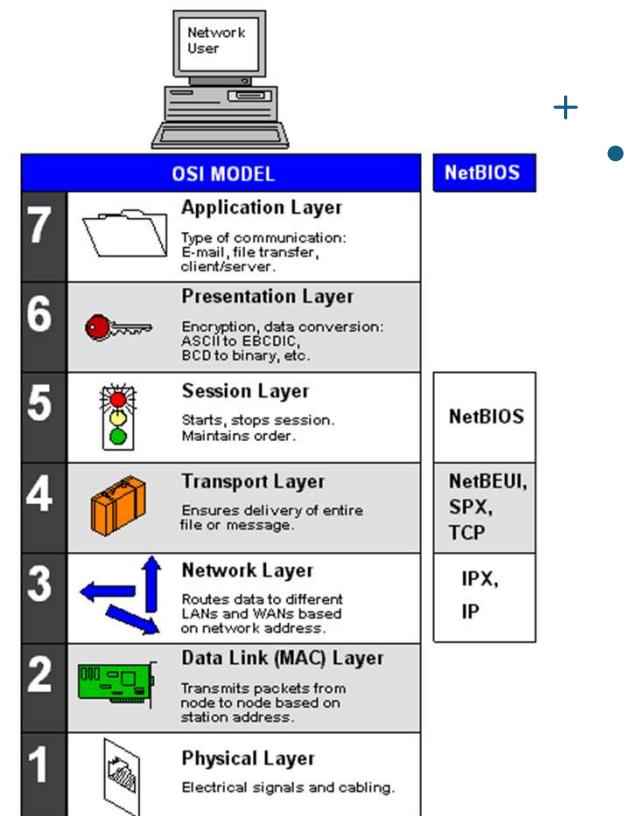


# Netbios (couche Session)

Netbios c'est un système de nommage et une interface développée par Microsoft qui permet d'établir des sessions entre les ordinateurs en réseau. Donc ce n'est pas un protocole.

Netbios va utiliser trois ports différents sur le réseau :

- Protocole UDP port 137 Name service;
- Protocole UDP port 138 Datagram service;
- Protocole UDP port 139 Session service.



# Quelques commandes

Les commandes utilisées lors de l'étape d'énumération sur le réseau (par un attaquant ou par un « white hat »):

**nbtstat -a adresse\_ip:** affiche la table de noms de la machine à distance

**nmbllookup -A adresse\_ip:** affiche la table de noms de la machine à distance



The screenshot shows a Windows Command Prompt window with the title 'Command Prompt'. The command entered is 'C:\>nbtstat -A 172.16.212.133'. The output displays the NetBIOS Remote Machine Name Table for the Local Area Connection 2 interface, which has an IP address of 172.16.212.128 and a scope ID of []. The table lists several entries, all of which are registered and have a status of 'Registered'. The entries include 'METASPLOITABLE' (with three different MAC addresses), 'MSBROWSE', and 'WORKGROUP' (with two different MAC addresses). At the bottom of the output, it shows the MAC Address as 00-00-00-00-00-00.

Name	Type	Status
METASPLOITABLE <00>	UNIQUE	Registered
METASPLOITABLE <03>	UNIQUE	Registered
METASPLOITABLE <20>	UNIQUE	Registered
__MSBROWSE__.<01>	GROUP	Registered
WORKGROUP <00>	GROUP	Registered
WORKGROUP <1D>	UNIQUE	Registered
WORKGROUP <1E>	GROUP	Registered

MAC Address = 00-00-00-00-00-00

C:\>\_

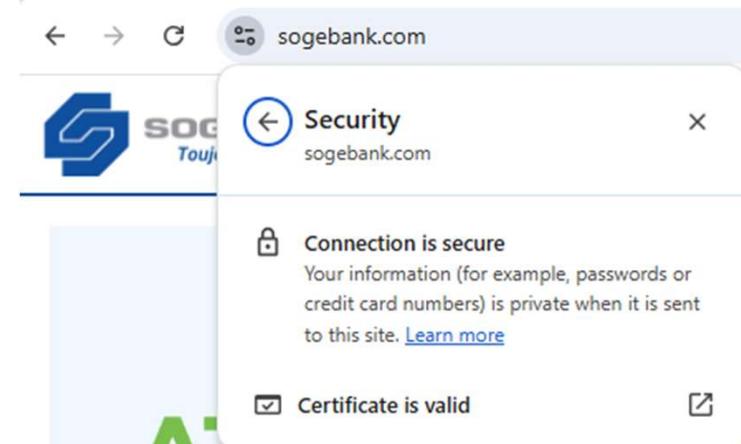
# Protocole TLS (entre application et transport)

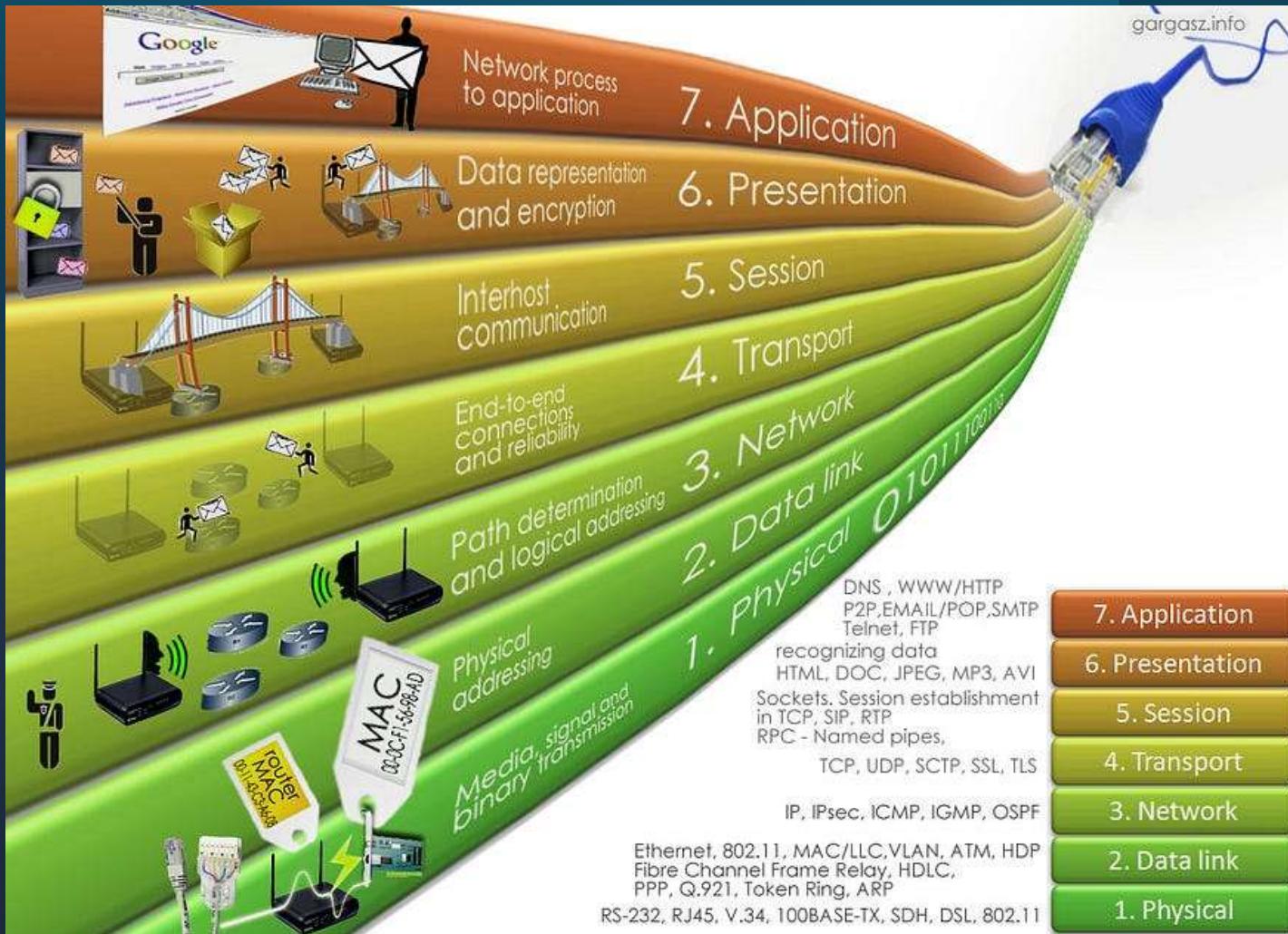
TLS (Transport Layer Security) & SSL (Secure Sockets Layer) : protocoles pour sécuriser et chiffrer les échanges sur Internet. SSL est l'ancienne version, maintenant c'est TLS (depuis 2018 TLS 1.3). Ses objectifs :

- Intégrité des données échangées;
- Confidentialité des données qui sont échangées entre deux machines;
- Authentification au serveur;

Les ports vulnérables de la couche Application (7) peuvent tous être sécurisés par TLS/SSL, voici des exemples :

- POP3 110 – POP3 SSL 995
- SMTP 25 – SMTP SSL 465
- HTTP 80 – HTTPS 443
- FTP 21 – FTPS 990





# Les ports réseau

Un port est une passerelle virtuelle utilisée par un service, un processus ou une application spécifique de votre ordinateur pour communiquer sur le réseau. Chaque port se voit attribuer un numéro unique, permettant de diriger différents types de trafic vers le logiciel approprié.

Par exemple, votre messagerie électronique peut utiliser un port, tandis que votre navigation web en utilise un autre. Associé à une adresse IP, un numéro de port crée une adresse de socket complète, permettant un routage précis des données vers et depuis votre ordinateur sur le réseau.

# Plages de ports



Ports connus/système (0-1023) : Les ports connus ou systèmes, compris entre 0 et 1023, sont réservés aux services courants et largement utilisés. Ils sont uniquement utilisés par les processus système, les systèmes d'exploitation et les applications par défaut. Ces ports réseau courants incluent HTTP (80), HTTPS (443), SMTP (25) et SSH (22).



Ports enregistrés (1024-49151) : Ces ports sont utilisés par des applications ou services moins courants, mais qui nécessitent néanmoins des ports spécifiques pour fonctionner correctement. Parmi les numéros de port importants de cette plage, on trouve : Remote Desktop Protocol (3389), Xbox LIVE et Jeux pour Windows (3074) et IBM Lotus Notes/Domino (1352).



Ports dynamiques/privés (49152-65535) : Ces ports sont utilisés pour les connexions temporaires ou de courte durée et ne sont pas attribués à des services spécifiques. Ils sont souvent utilisés comme ports sources pour les connexions sortantes et peuvent être utilisés par n'importe quel processus.



## Well-known TCP/UDP ports

Port	Protocol	Service	Port	Protocol	Service
Created by <a href="#">@dan_nanni</a> on Instagram					
20	TCP	FTP/data	443	TCP	HTTP over SSL
21	TCP	FTP/control	464	TCP/UDP	Kerberos
22	TCP	SSH	465	TCP	SMTP over SSL/TLS (SMTPS)
23	TCP	Telnet	500	UDP	IPsec/IKE
25	TCP	SMTP	513	TCP	Rlogin
53	TCP/UDP	DNS	514	UDP	Syslog
67	UDP	DHCP/server	515	TCP	lpd/lpr
68	UDP	DHCP/client	520	UDP	UDP
69	UDP	TFTP	546	TCP/UDP	DHCPv6/client
80	TCP	HTTP	547	TCP/UDP	DHCPv6/server
110	TCP	POP3	563	TCP/UDP	NNTP over SSL/TLS (NNTPS)
119	TCP	NNTP	587	TCP	SMTP/submission
123	UDP	NTP	636	TCP/UDP	LDAP over SSL/TLS (LDAPS)
137	UDP	NetBIOS/name	691	TCP	Microsoft Exchange
138	UDP	NetBIOS/datagram	860	TCP	iSCSI
139	TCP	NETBIOS/session	873	TCP	Rsync
143	TCP	IMAP	902	TCP/UDP	VMware Server
161	UDP	SNMP/agent	989	TCP	FTP over SSL/TLS for data
162	UDP	SNMP/manager	990	TCP	FTP over SSL/TLS for control
179	TCP	BGP	992	TCP/UDP	Telnet over SSL/TLS
201	TCP/UDP	Appletalk	993	TCP	IMAP over SSL/TLS (IMAPS)
389	TCP/UDP	LDAP	995	TCP/UDP	POP3 over SSL/TLS (POP3S)

# Les différentes attaques reliées aux 7 couches

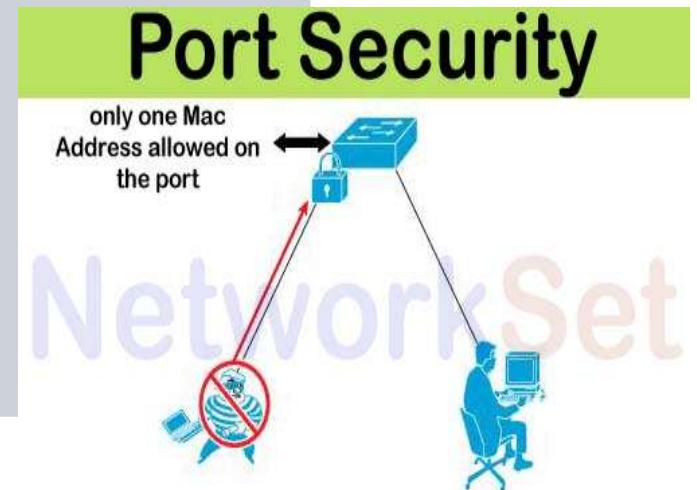
Les différentes couches du modèle OSI... et attaques reliées à celles-ci.

<https://www.cisa.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf>



<b>couche</b>	<b>protocoles</b>	<b>Exemples d'attaques</b>	<b>Potentiel impact de l'attaque</b>	<b>Exemples de contre-mesures</b>
1 Physique	100BaseT, 1000BaseT...	Destruction physique Obstruction Manipulation Mauvaise fonction	Bande passante et connections limitées, perte d'équipement	Contrôle d'accès Audits de sécurité Verrouillage/Barrière

couche	protocoles	Exemples d'attaques	Potentiel impact de l'attaque	Exemples de contre-mesures
<b>2 Liaison</b>	802.3, 802.5, Ethernet...	<p>Si la couche 2 est compromise, toutes les autres couches du haut le seront aussi.</p> <p>Saturer la Table ARP/MAC d'une « switch » pour l'attaquer.</p> <p>MAC flooding : Inondation</p> <p>Mac spoofing : Un pirate se fait passer pour un autre . Donc sa MAC n'est pas la sienne mais celle d'une autre machine sur le réseau.</p>	Perturbation du flux de données de l'expéditeur au destinataire à travers tous les ports	<ul style="list-style-type: none"> <li>• Limiter les adresses MAC dans la « switch »</li> <li>• Sécurité des Ports</li> <li>• Certains IDS (Intrusion detection system) peuvent détecter un comportement ARP anormal</li> </ul>

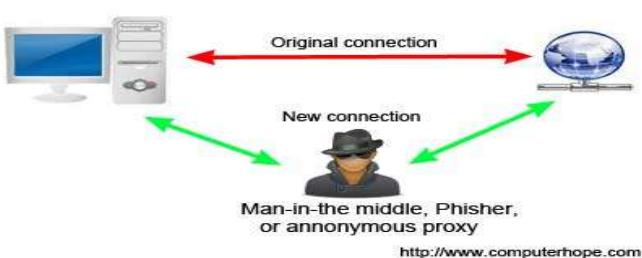


[https://en.wikipedia.org/wiki/MAC\\_spoofing](https://en.wikipedia.org/wiki/MAC_spoofing)

[https://fr.wikipedia.org/wiki/Saturation\\_de\\_la\\_table\\_d%27apprentissage](https://fr.wikipedia.org/wiki/Saturation_de_la_table_d%27apprentissage)

couche	protocoles	Exemples d'attaques	Potentiel impact de l'attaque	Exemples de contre-mesures
3 Réseau	IP, ICMP, ARP...	<p>Un pirate envoie plusieurs requêtes ICMP (echo Request) en faisant la commande ping. ICMP/Ping flooding</p> <p>Le pirate détourne les communications entre une machine et une « switch ». ARP spoofing / ARP poisoning</p> <p>Interception de paquets pendant la transmission. MITM packet sniffing</p> <p>Un pirate se fait passer pour un autre . Donc son IP n'est pas la sienne mais celle d'une autre machine sur le réseau. IP spoofing</p>	Peut affecter le réseau, la bande passante et imposer « un overload » sur le pare-feu	<ul style="list-style-type: none"> <li>Activer la limite du trafic ICMP</li> <li>Outils de détection sur le réseau</li> <li>Entrer chaque adresse MAC dans les entrées (tables ARP) des équipements comme les « switch ».</li> <li>Inspection : validation des paquets ARP</li> <li>Installer IPSEC : protocole pour sécuriser les communications IP par l'authentification et le chiffrement de chaque paquet IP d'une session de communication</li> <li>Règles de pare-feu (firewall)</li> </ul>

### Man-in-the-middle attack



[https://fr.wikipedia.org/wiki/Usurpation\\_d%27adresse\\_IP](https://fr.wikipedia.org/wiki/Usurpation_d%27adresse_IP)  
[https://fr.wikipedia.org/wiki/Ping\\_flood](https://fr.wikipedia.org/wiki/Ping_flood)  
[https://fr.wikipedia.org/wiki/ARP\\_poisoning](https://fr.wikipedia.org/wiki/ARP_poisoning)  
[https://fr.wikipedia.org/wiki/Attaque\\_de\\_l%27homme\\_du\\_milieu](https://fr.wikipedia.org/wiki/Attaque_de_l%27homme_du_milieu)

couche	protocoles	Exemples d'attaques	Potentiel impact de l'attaque	Exemples de contre-mesures
4 Transport	TCP, UDP...	<p>Déni de service et Déni de Service Distribué DDoS/DoS</p> <p>Le pirate envoie plusieurs requêtes SYN à une machine pour la saturer. SYN flood</p> <p>Le pirate fait une attaque « Distributed Reflection Denial of Service », attaque réfléchie ou par rebond DRDoS</p> <p>Réseau d'ordinateurs compromis contrôlés par un « C&amp;C » (serveur criminel: Command &amp; Control) Botnet</p>	La bande passante et la connexion seront limitées et perte d'équipement	<ul style="list-style-type: none"> <li>• Filtrage de paquets</li> <li>• Profilage d'activités : surveiller l'augmentation des activités malicieuses sur le réseau</li> <li>• Déetecter, isoler le trafic malicieux</li> <li>• Outil Anti-DoS</li> <li>• WAF (Pare-feu application comme CloudFlare)</li> </ul>

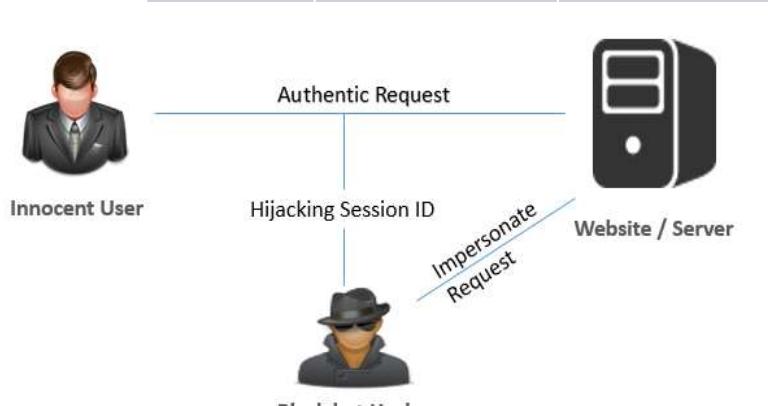
[https://fr.wikipedia.org/wiki/Attaque\\_par\\_d%C3%A9ni\\_de\\_service](https://fr.wikipedia.org/wiki/Attaque_par_d%C3%A9ni_de_service)

[https://en.wikipedia.org/wiki/Denial-of-service\\_attack#Reflected\\_2F\\_spoofed\\_attack](https://en.wikipedia.org/wiki/Denial-of-service_attack#Reflected_2F_spoofed_attack)

[https://fr.wikipedia.org/wiki/SYN\\_flood](https://fr.wikipedia.org/wiki/SYN_flood)

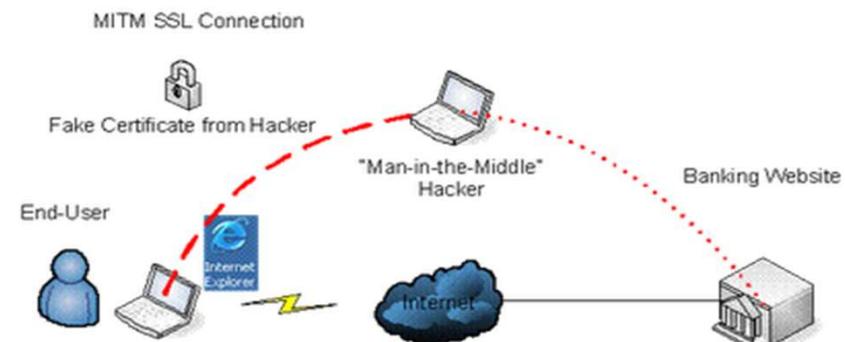
<https://fr.wikipedia.org/wiki/Botnet>

couche	protocoles	Exemple d'attaques	Potentiel impact de l'attaque	Exemples de contre-mesures
5 Session	Protocole d'entrée et de sortie (logon/logoff), netbios, RPC...	<p>Un pirate fait l'énumération sur le réseau NetBios</p> <p>Un pirate fait du « Hijacking » de la session Windows.</p>	<p>Reconnaissance sur le réseau (pré-attaque)</p> <p>Vol de session, vol de fichier cookie</p> <p>Il a un accès non autorisé à un ordinateur qui n'est pas le sien</p>	<ul style="list-style-type: none"> <li>• Limiter les informations de versions sur les serveurs</li> <li>• Authentification à double facteur</li> <li>• Limiter le temps de session</li> </ul>



<https://resources.infosecinstitute.com/process-scanning-and-enumeration/>  
[https://en.wikipedia.org/wiki/Session\\_hijacking](https://en.wikipedia.org/wiki/Session_hijacking)

couche	protocoles	Exemples d'attaques	Potentiel impact de l'attaque	Exemples de contre-mesures
6 Présentation	Protocoles présentation, de compression et de chiffrement, ASCII...	MITM SSL  Virus, vers, trojans...  Malformation de requêtes SSL  Tunnel HTTP	Les systèmes peuvent arrêter d'accepter les connexions SSL	Surveillance du trafic  Passer de SSL vers TLS  Anti-virus sur le serveur de courrier, anti-spam, anti-malwares...



<http://techgenix.com/understanding-man-in-the-middle-attacks-arp-part4/>

Fig 2. MITM InSecure SSL Connection

couche	protocoles	Exemples d'attaques	Potentiel impact de l'attaque	Exemples de contre-mesures
7 Application	FTP, HTTP, POP3, SMTP...	<p>« Sniffing » de session</p> <p>Faillle de sécurité d'un site web permettant d'injecter du contenu dans une page web vulnérable : diriger les utilisateurs vers un site d'hameçonnage...</p> <p>Cross-site scripting (XSS)</p> <p>Trojan infectant un navigateur, infecte sa sécurité et peut modifier le contenu de la page web</p> <p>MIT-Browser</p> <p>Données insérées dans la cache DNS, le DNS retourne une mauvaise IP</p> <p>DNS spoofing/DNS cache poisoning</p>	<p>Prendre le contrôle d'une session HTTP en obtenant un ID de session</p> <p>Diverses attaques sur l'applications web (formulaire)</p>	<p>Filtrage et Surveillance (IDS...)</p> <p>Pare-feu applicatif (WAF)</p> <p>Bloquer les requêtes DNS provenant d'un serveur externe</p> <p>Déployer le protocole de sécurité DNSSEC (Domain Name System Security Extensions )</p> <p>Input validation : validation des informations entrées dans un formulaire</p>

[https://en.wikipedia.org/wiki/Session\\_hijacking](https://en.wikipedia.org/wiki/Session_hijacking)  
[https://fr.wikipedia.org/wiki/Cross-site\\_scripting](https://fr.wikipedia.org/wiki/Cross-site_scripting)  
<https://en.wikipedia.org/wiki/Man-in-the-browser>  
[https://en.wikipedia.org/wiki/DNS\\_spoofing](https://en.wikipedia.org/wiki/DNS_spoofing)  
<https://cybersecuritynews-com.cdn.ampproject.org/c/s/cybersecuritynews.com/injection-attacks/?amp>



## Ces comportements à éliminer permettront d'augmenter la sécurité...

Issue	Solution	Notes
Telnet, rlogin	OpenSSH or ssh (Secure Shell)	It sends encrypted data and makes it difficult for attacker to send the correctly encrypted data if session is hijacked
FTP	sFTP	It reduces the chances of successful hijacking
HTTP	SSL (Secure Socket Layer)	It reduces the chances of successful hijacking
IP	IPSec	It prevents hijacking by securing IP communications
Any Remote Connection	VPN	Implementing encrypted VPN such as PPTP, L2PT, IPSec, etc. for remote connection prevents session hijacking
SMB (Server Message Block)	SMB signing	It improves the security of the SMB protocol and reduces the chances of session hijacking
Hub Network	Switch Network	It mitigates the risk of ARP spoofing and other session hijacking attacks

# Sécurisation du réseau

## Vulnérabilités sur le réseau et sur l'infrastructure :

Une vulnérabilité sur le réseau peut être un défaut d'un équipement (matériel – logique), un défaut de configuration d'un équipement (matériel – logique) ou un processus de l'organisation.

Les vulnérabilités sur le réseau sont diverses et viennent en différentes formes :

- Programme malveillant
- Ingénierie sociale
- Mises à jour non appliquées
- Mauvaises configurations du pare-feu ou d'un système d'exploitation
- Shadow IT (système, application, service... installé sans autorisation de la haute direction TI)

Une vulnérabilité peut être exploitée et peut résulter en une attaque de rançongiciel, déni de service, etc.

Exploitation des vulnérabilités sur le réseau ?:

- Reconnaissance, balayages et énumération sur le réseau
- Exploitation, intrusion et escalade des priviléges

# Sécurisation du réseau (suite)

Une analyse sur notre réseau est un processus pour découvrir, identifier et analyser les défauts de sécurité sur le réseau. Failles et « trous » de sécurité qui pourraient être une porte d'entrée pour les pirates ou acteurs malveillants seront découverts et devront être corrigés.

Ces vérifications doivent être faite continuellement :

- Fréquence : quotidienne – hebdo – mensuelle
- Outils : « open-source » ou commerciaux
- Techniques : Analyses de vulnérabilités – Test d'intrusion
- Résultats : Rapports – Corrections – Mitigation

# **Plusieurs défenses à mettre en place sur le réseau**

Plusieurs défenses à mettre en place sur le réseau en premier lieu.

## **1) Solutions de « gouvernance » :**

- Politique de sécurité
- Classification des actifs informationnels et Analyses de risques
- Directives, Normes, Cadre de gestion, etc.
- Évaluation des risques, menaces et vulnérabilités

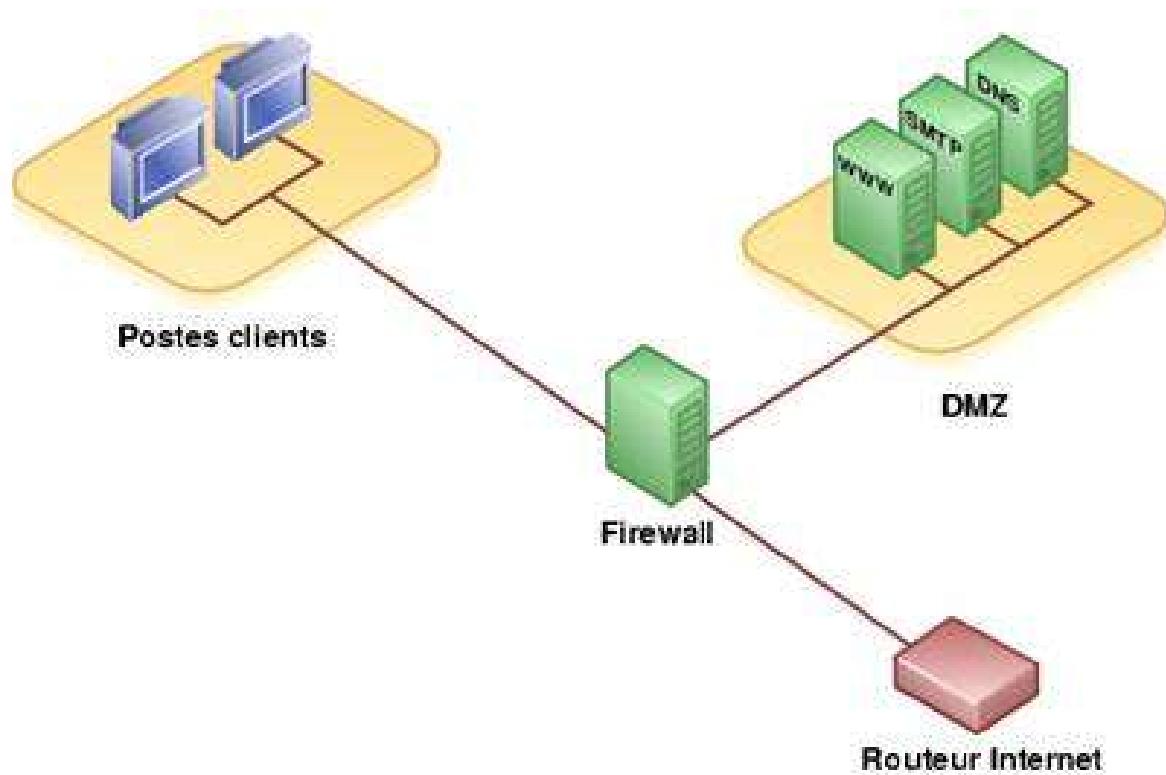
# Plusieurs défenses à mettre en place sur le réseau

## 2) Solution « technique » :

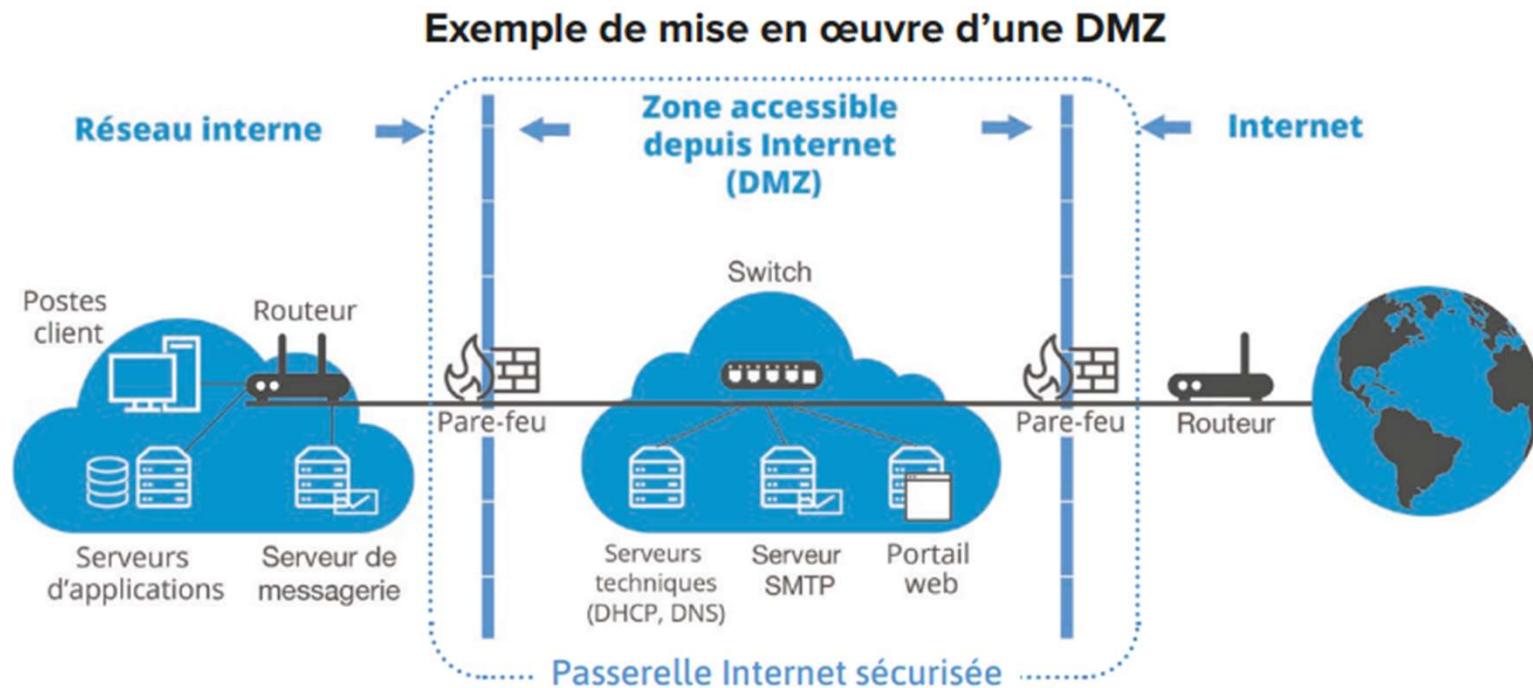
La segmentation du réseau :

- Diviser le réseau en plusieurs sous-réseaux pour améliorer la performance mais aussi la sécurité
- Intégrer une DMZ (zone démilitarisée)

Exemple de défenses à mettre en place



# Sécurité via une zone DMZ



# Plusieurs défenses à mettre en place sur le réseau

## 3) Solutions « technologiques » :

- Pare-feu : système qui protège le réseau des intrusions externes. Il filtre les paquets qui entrent (externe) et sortent (interne) du réseau. Il fonctionne avec des règles qui sont prédéfinies :
  - Autoriser ce trafic (allow)
  - Bloquer ce trafic (deny)
  - Refuser ce trafic (drop)

Note: Cela fait partie de 2 approaches fondamentales: Blacklist et Whitelist

# Types de parefeu

## **1) Filtres de paquets (sans état ou Stateless)**

Si un paquet correspond aux règles du filtre, celui-ci l'ignore ou l'accepte.

## **2) Filtres « avec état ou Statefull**

Il conserve un enregistrement de toutes les connexions qui le traversent et peut déterminer si un paquet est le début d'une nouvelle connexion, une partie d'une connexion existante ou un paquet invalide.

## **3) Couche applicative**

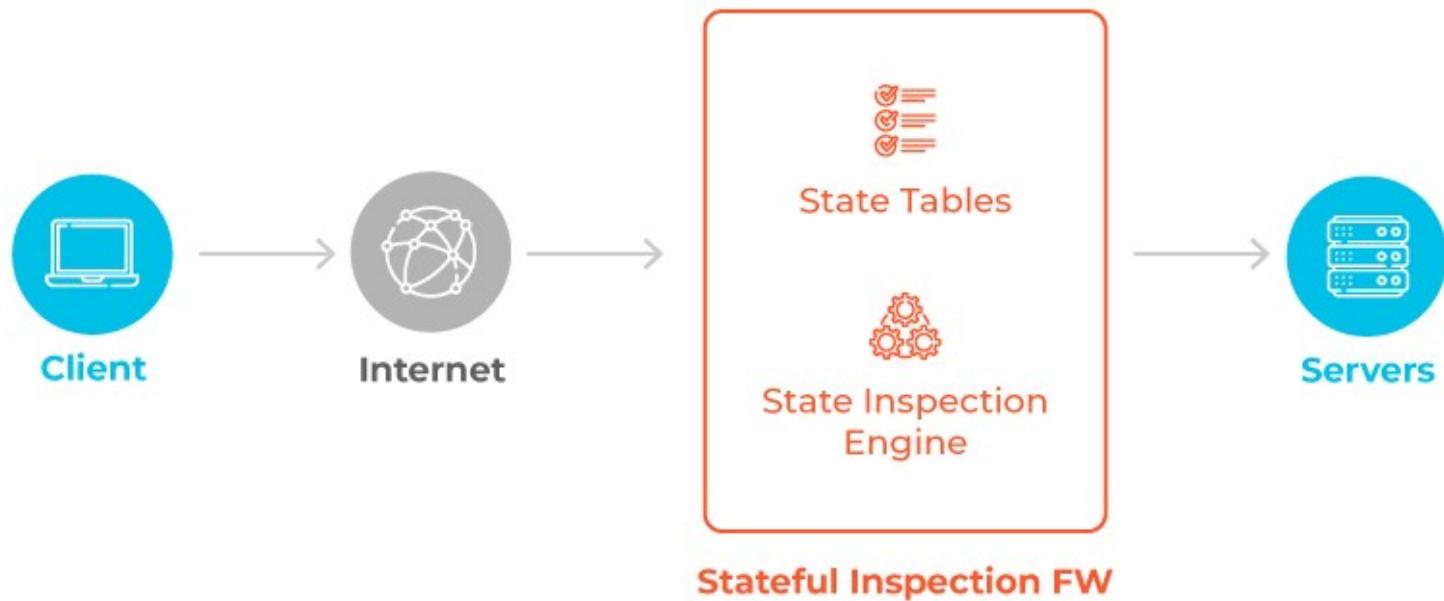
Il fonctionne comme un proxy et peut « comprendre » certaines applications et protocoles. Il peut inspecter le contenu du trafic et bloquer ce qu'il considère comme inapproprié (par exemple, sites web, virus, vulnérabilités, etc.).

## Packet Filtering Firewall



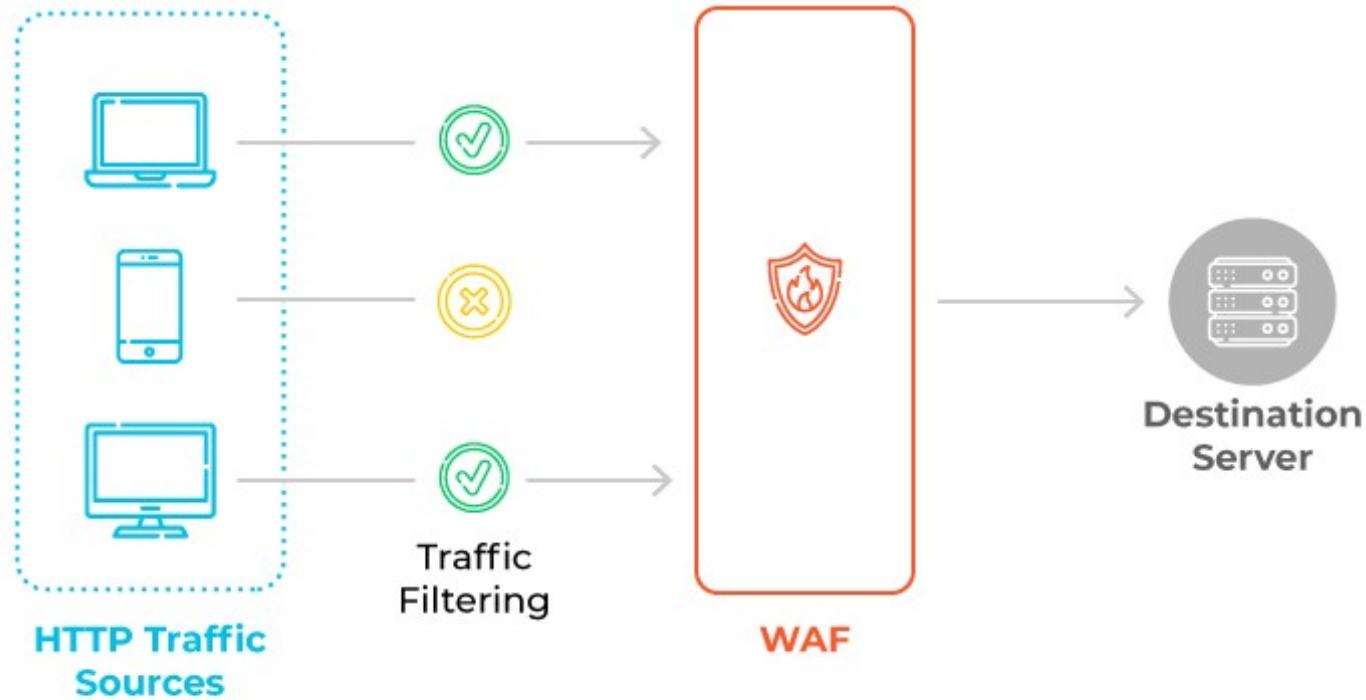
<https://www.paloaltonetworks.ca/cyberpedia/types-of-firewalls>

## Stateful Inspection Firewall



<https://www.paloaltonetworks.ca/cyberpedia/types-of-firewalls>

## Web Application Firewall



<https://www.paloaltonetworks.ca/cyberpedia/types-of-firewalls>

# Plusieurs défenses à mettre en place sur le réseau

## 2) Solutions « technologiques » : IDS/IPS

**Détection d'intrusion:** Identification par signatures d'intrusion et signalement des activités d'intrusion.

**Prévention des intrusions:** Processus de détection des activités d'intrusion et de gestion des actions réactives automatiques sur l'ensemble du réseau.

- Les diverses familles de systèmes de détection et de prévention des intrusions (alerte):
  - NIDS : Network Based Intrusion Detection System – Surveille la sécurité du réseau
  - HIDS : HostBased Intrusion Detection System – Surveille la sécurité des hôtes (serveurs)
  - IDS : Intrusion Detection System – Surveille la sécurité du réseau et des hôtes
  - HIPS : Host-based Intrusion Prevention System – Surveille les postes de travail
  - NIPS : Network Intrusion Prevention System – Surveille le trafic réseau
  - WIPS : Wireless Intrusion Prevention System – Surveille le réseau WIFI
  - KIPS : Kernel Intrusion Prevention System – Surveille le noyau d'un hôte

Divers outils de détection d'intrusion :

Snort

OSSEC

Alienvault OSSIM (Open Source Security Information Management)

Sguil

Suricata

Bro



Security Onion includes Elasticsearch, Logstash, Kibana, Suricata, Zeek (formerly known as Bro), Wazuh, Stenographer, TheHive, Cortex, CyberChef, NetworkMiner, and many other security tools.

Si vous voulez vous amuser... installer SecurityOnion (VM).

Basé sur Ubuntu/CentOS, ce système contient :

Snort, Suricata, Bro, OSSEC, Sguil, Squert, ELSA, Xplico, NetworkMiner, Wireshark, etc.

<https://securityonion.net/>

<https://docs.securityonion.net/en/2.3/>

<https://github.com/Security-Onion-Solutions/securityonion>



# VPN (réseau privé virtuel)

Un VPN permet de connecter en toute sécurité deux réseaux privés reliés par le biais d'Internet. Des ordinateurs distants peuvent ainsi fonctionner de la même manière que s'ils appartenaient à un même réseau local sécurisé.

## **Avantages:**

- Vous pouvez accéder aux ordinateurs de votre entreprise depuis votre domicile comme si vous étiez sur votre lieu de travail.
- Il est impossible pour une personne extérieure d'intercepter ou de perturber les données passant par le tunnel VPN.
- Si un logiciel client VPN est installé sur votre ordinateur portable, vous pouvez interagir avec votre entreprise, où que vous soyez dans le monde.



# VPN (réseau privé virtuel)

## Inconvénients

- La configuration est plus complexe que les méthodes moins sécurisées. Connecter à différents produits peut devenir problématique.
  - Aussi étrange que cela puisse paraître, l'entreprise dont vous rejoignez le réseau peut vous demander d'appliquer ses politiques sur vos ordinateurs personnels.
-



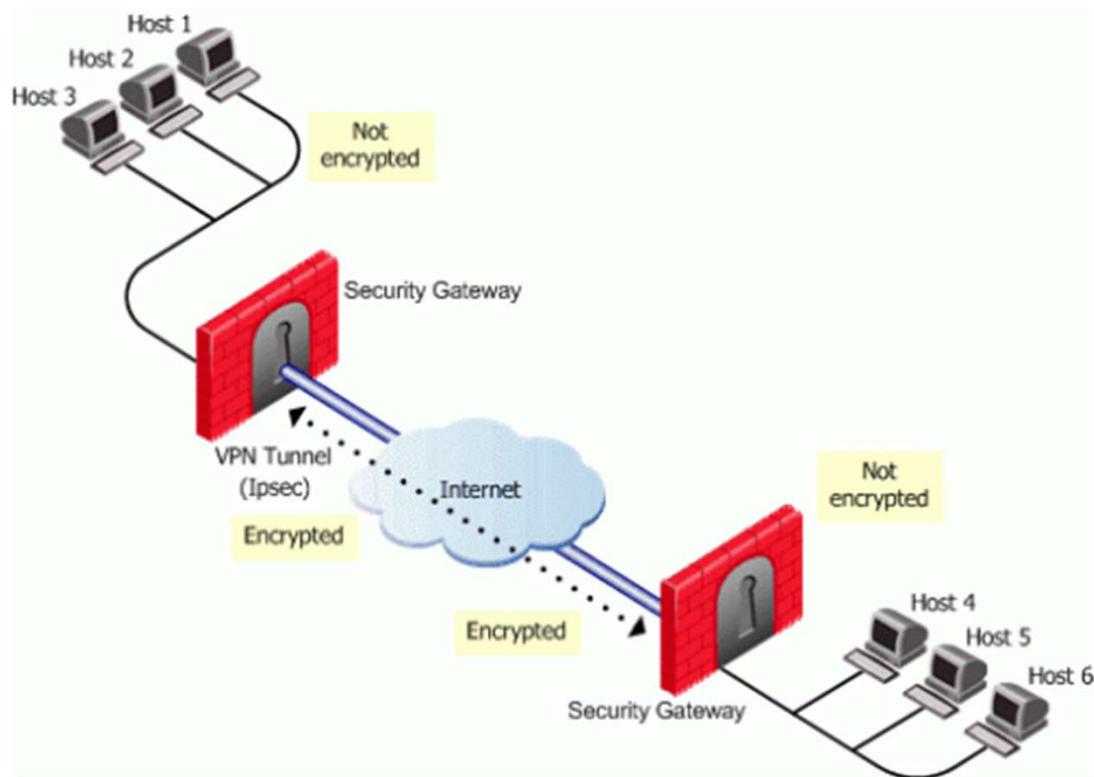
# Types de VPN

Un VPN garantit la confidentialité, l'intégrité et l'authentification des données, même en cas de transmission sur un réseau non fiable.

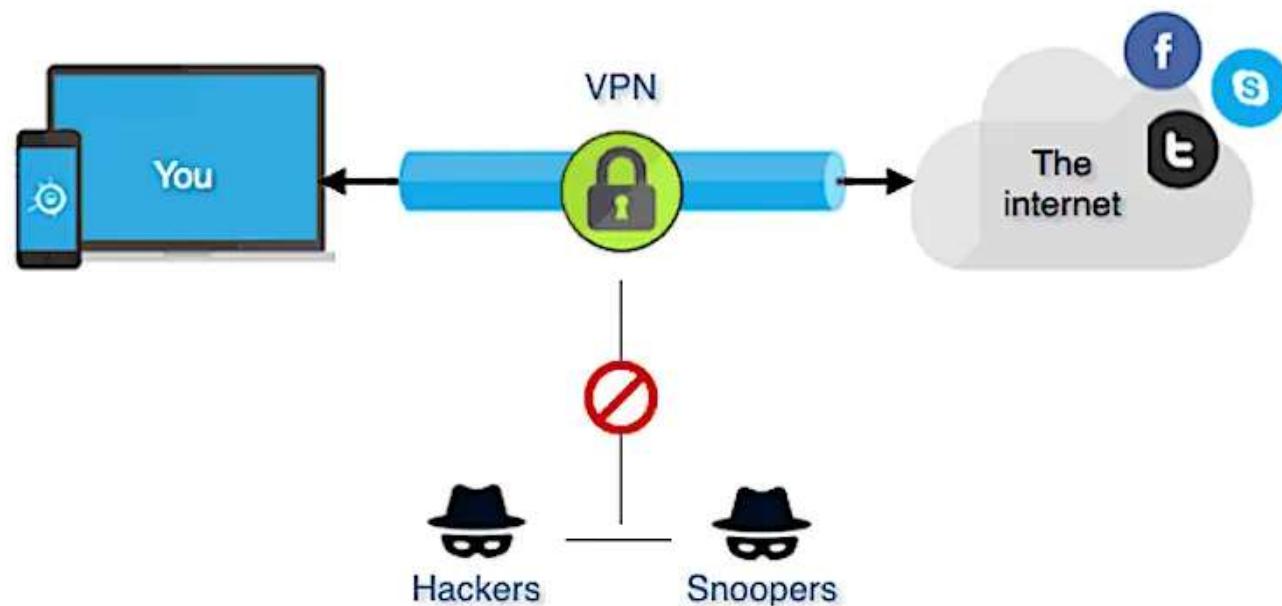
Il existe deux principaux types de VPN :

- les VPN d'accès à distance permettant aux clients autorisés d'accéder à un réseau privé appelé intranet. Les clients installent un logiciel client VPN sur leurs machines.
- les VPN de site à site sont conçues pour fournir une passerelle sécurisée entre deux ou plusieurs réseaux physiquement distants.

# Exemples de VPN

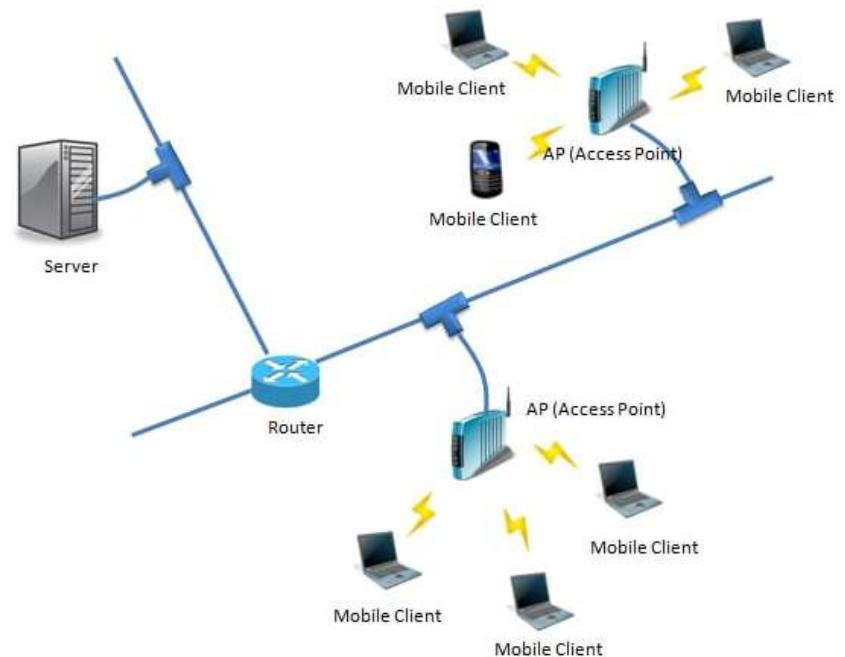


## Navigation anonyme



# Réseau WLAN

Un réseau local sans fil (WLAN) est un groupe d'ordinateurs ou d'autres appareils colocalisés qui forment un réseau basé sur des transmissions radio (plutôt que sur des connexions filaires).

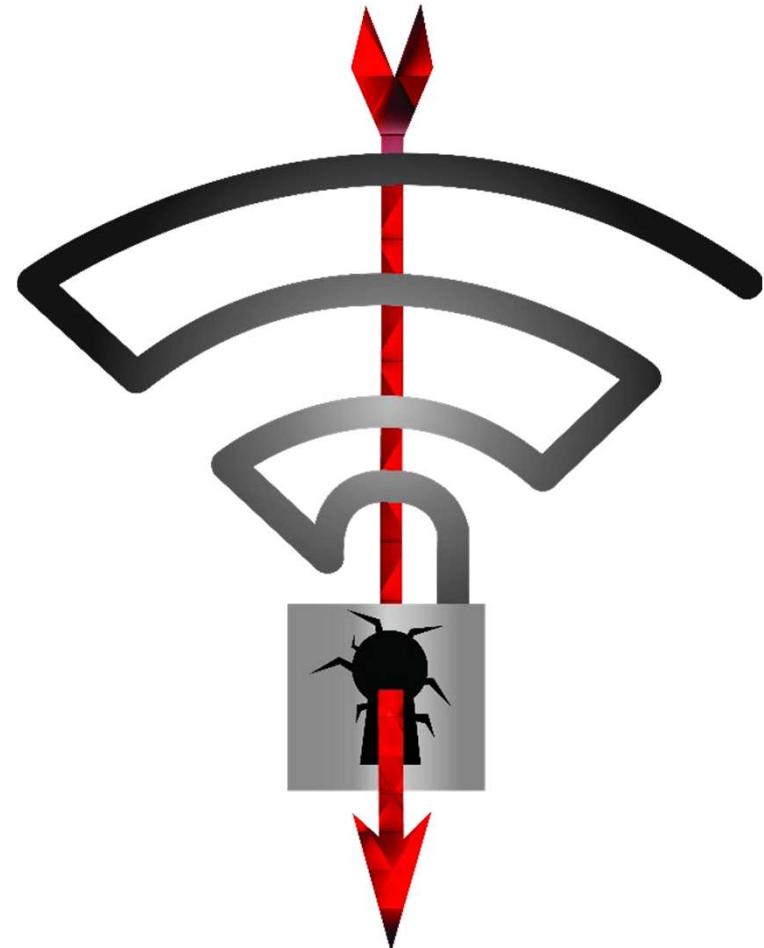


Wireless LAN

# Vulnérabilités Réseau sans-fil

WLAN : Flexibilité, rentabilité et facilité d'installation

- Utilisation des radiofréquences:  
Difficulté à contenir les signaux
- Vulnérabilités des normes de sécurité
- Une configuration simple implique souvent une configuration réseau inadéquate pour un accès sécurisé.



# Standards de sécurité

WEP (Wired Equivalent Privacy)

- Créé en 1999 par la norme IEEE 802.11b
- Offre le même niveau de confidentialité qu'un réseau local filaire
- Les clés 40/104 bits sont statiques et l'IV est court
- Pas de gestion efficace des clés
- Algorithme de chiffrement (RC4) : failles connues
- Cible facile pour la cryptanalyse
- Ne devrait pas être utilisé dans les réseaux WLAN actuels



## Standard de sans-fil: WPA (wifi preected access)

Développé en 2004 par 802.11i pour résoudre les problèmes liés au WEP

Utilise le protocole TKIP 48 bits

Ajoute une protection d'intégrité

Modes entreprise et personnel

Le mode entreprise utilise EAP et 802.1x pour le contrôle d'accès et l'authentification

Rétrocompatible avec les anciens appareils utilisant le WEP

Utilise toujours le protocole RC4

Vulnérabilité aux attaques par dictionnaire, par force brute et par déni de service



## Standard de sans-fil: WPA2

Successeur du WPA, ratifié par l'IEEE 11i en 2004

Norme de sécurité la plus sécurisée disponible

Remplacez RC4 et TKIP par AES et CCMP pour le chiffrement et l'authentification

Itinérance plus fluide

Vulnérabilité toujours présente

# WPA 2 mode enterprise vs mode personnel



- Existe en WPA et WPA2
- Mêmes algorithmes de chiffrement
- Méthode d'authentification différente
- Mode entreprise : 802.1x, conçu pour les organisations
- Mode personnel : clés pré-partagées, conçu pour un usage domestique

## Standard WPA3 (Wi-Fi Protected Access 3)

---

Sécurité avancée au-delà de WPA2

Protection renforcée contre les pirates informatiques

Authentification utilisateur améliorée

Remplace les versions précédentes qui utilisaient une clé pré-partagée

Cryptage 256 bits



# Attaques aux réseau sans-fil

---

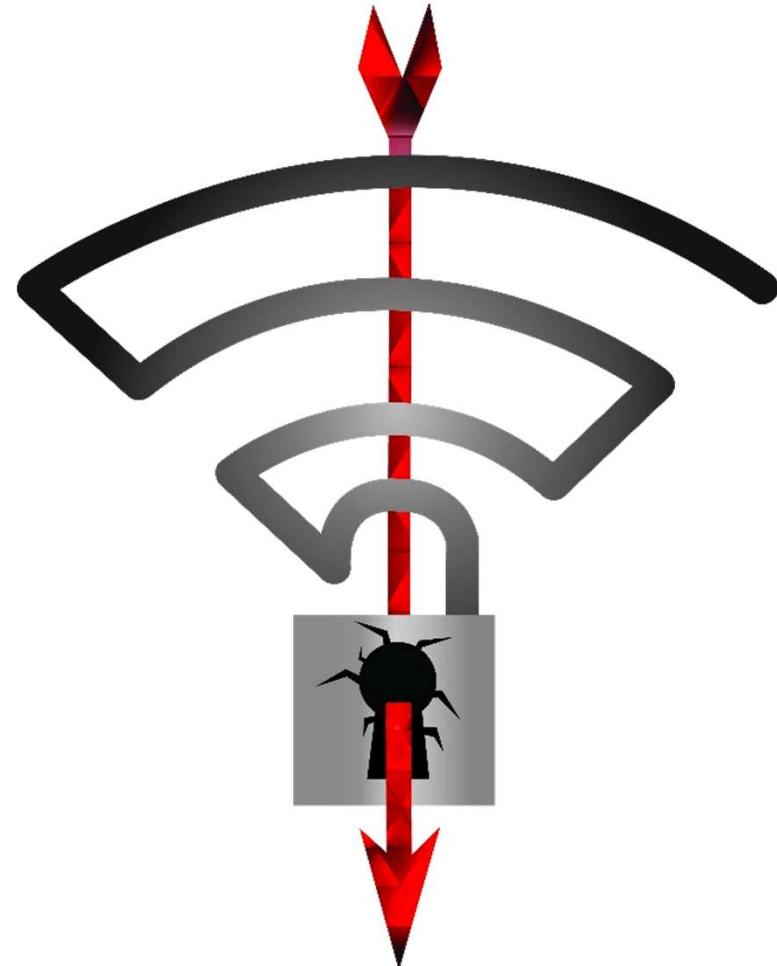
Attaque passive

Analyse du trafic

Attaque active

Accès non autorisé

Point d'accès malveillant



# Attaques liées aux CID

Confidentialité	Contrôle réseau I	Intégrité	Authentification	Disponibilité
Traffic analysis Eavesdropping Man-in-the-Middle attack Evil Twin AP	War driving Rogue access point MAC address spoofing Unauthorized access	Session hijacking Reply attack 802.11 frame injection attack 802.11 data replay attack 802.11 data deletion	Dictionary & brute force <ul style="list-style-type: none"><li>• Shared key guessing</li><li>• PSK cracking</li><li>• Application login theft</li><li>• Etc.</li></ul>	DoS/ Queensland DoS RF Jamming 802.11 beacon flood 802.11 association flood 802.11 de-authentication Fake SSID EAPOL flood AP theft

# Voici quelques méthodes pour prévenir les attaques sans fil :

Désactiver les fonctionnalités réseau inutilisées ;

Ne pas diffuser votre SSID ;

Modifier le mot de passe par défaut et le sécuriser avec un mot de passe fort ;

Chiffrer vos communications sans fil ;

Filtrer les adresses MAC autorisées à se connecter à votre routeur.

# Références

- <https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-threatsaurusaz.pdf?la=de-DE.pdf>
- <https://www.sans.org/media/critical-security-controls/CSC-5.pdf>
- <https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf>
- [http://www.cil.cnrs.fr/CIL/IMG/pdf/Glossaire\\_securite\\_informatique.pdf](http://www.cil.cnrs.fr/CIL/IMG/pdf/Glossaire_securite_informatique.pdf)
- <https://securityinabox.org/fr>
- [https://fr.wikipedia.org/wiki/ARP\\_poisoning](https://fr.wikipedia.org/wiki/ARP_poisoning)
- [https://fr.wikipedia.org/wiki/Ping\\_flood](https://fr.wikipedia.org/wiki/Ping_flood)
- <https://fr.wikipedia.org/wiki/Botnet>

# Références (suite)

- [https://fr.wikipedia.org/wiki/Cross-site\\_scripting](https://fr.wikipedia.org/wiki/Cross-site_scripting)
- [https://fr.wikipedia.org/wiki/Usurpation\\_d%27adresse\\_IP](https://fr.wikipedia.org/wiki/Usurpation_d%27adresse_IP)
- [https://en.wikipedia.org/wiki/MAC\\_spoofing](https://en.wikipedia.org/wiki/MAC_spoofing)
- <https://www.us-cert.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf>
- [https://www.owasp.org/index.php/Input\\_Validation\\_Cheat\\_Sheet](https://www.owasp.org/index.php/Input_Validation_Cheat_Sheet)
- <https://www.giac.org/paper/gsec/2868/osi-defense-in-depth-increase-application-security/104841>
- <https://www.blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switches.pdf>
- [https://fr.wikipedia.org/wiki/Saturation\\_de\\_la\\_table\\_d%27apprentissage](https://fr.wikipedia.org/wiki/Saturation_de_la_table_d%27apprentissage)

# Références (fin)

- <https://www.pandasecurity.com/en/mediacenter/wpa-vs-wpa2/>
- <https://purplesec.us/learn/wireless-network-attack/>
- <https://www.securew2.com/blog/what-is-wep-security>
- <https://www.cisa.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf>
- <https://kb.netgear.com/fr/22359/Qu-est-ce-qu-un-VPN-r%C3%A9seau-priv%C3%A9-virtuel-1479991135130?language=fr>
- <https://www.formip.com/pages/blog/adresses-publiques-et-privees>
- <https://blog.netwrix.com/common-ports>