La sécurité dans les réseaux

ORGANISATION INTERNATIONALE DE la francophonie

cedric.foll@(education.gouv.fr|laposte.net)
Ministère de l'éducation nationale

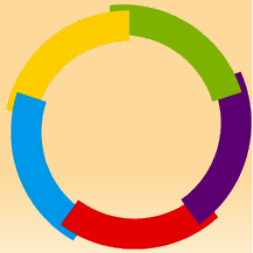
Atelier sécurité
Rabat – RALL 2007

Ce cours est inspiré par celui donné par Cedric Blancher aux RALL 2006

Une citation

« Being able to break security doesn't make you a hacker anymore than being able to hotwire cars makes you an automotive engineer. »

Eric Raymond



Plan

- La sécurité en quelques dates
- Rappels réseaux
- Faiblesses dans les réseaux
- Switchs & VLAN
- Wifi

1998...

- Janvier : perte de DNS pendant trois jours
- Février : ”fairly heavey cyber attacks... the most organized and systematic the Pentagon has seen to date”. En fait, deux gamins de 15 ans...
- Mars : crash de milliers de machines NT et Win95, début de la course aux nukes
- Lotus convaincu d’avoir introduit une backdoor dans les versions de Notes livrées au gouvernement Suédois
- 100 attaques/jour sur le Pentagone

1999...

- Janvier : USAF piratée à San Diego (par un français)
- Mars : flood des serveurs de l'OTAN par des militants serbes pour protester contre l'intervention des casques bleus en Yougoslavie (enfin, c'est ce qu'on dit)
- Avril : Acrobat Reader contient un trojan, NetBus
- Septembre : un commentaire malheureux dans les sources de NT4SP5 lance le doute : "NSA Key"...

2000...

- Le ”très” sérieux bug de l’an 2000 n’a pas eu lieu
- Déni de service distribué (DDoS) massif sur Yahoo, Amazon, Altavista, etc.
- Ver ”I Love You” : première diffusion virale massive par courrier électronique
- Microsoft se fait compromettre suite à une infection virale et voler une partie des sources de Windows XP
- 50 sites web détournés par jour

2001...

- Juillet : Dimitri Sklyarov arrêté par le FBI à la DefCon pour avoir cassé une protection Ebook de Adobe, pour violation du DMCA
- Novembre : adoption en France de la LSQ avec son volet sur la cryptographie
- Explosion de la diffusion virale via le réseau à travers des failles de serveurs : CodeRed en juillet, Nimda en octobre
- 120 sites web détournés par jour

2002...

- Décembre : obligation pour les Etats européens d’appliquer l’EUCD, équivalent européen du DMCA
- Juillet : OpenSSH contient un trojan
- 60% des piratages se font via un site HTTP dynamique

2003...

- Janvier : Slammer. 90% des machines vulnérables contaminées en 10 min, soit 350000 machines...
- Août : Blaster/Sobig
- Septembre : Valve se fait dérober une partie du code de HalfLife 2 dont la sortie sera retardée d'un an et demi
- Octobre : Verisign détenant .com et .net redirige toutes les requêtes DNS inexistante vers un de leurs sites.
- Novembre : 4 serveurs Debian sont compromis via une faille connue mais non publiée sur le noyau Linux, avec un exploit privé

2004...

- Janvier: virus MyDoom, le ver mail le plus rapide de tous les temps.
- Mai : Sasser, petit ver très médiatisé (AFP infectée)
- Juin : Akamai tombe pendant 4 jours suite à un problème de DNS
- Décembre : Santy, ver utilisant une application web populaire (PhpBB) pour assurer sa réplication

2005...

- « Fin » des mass mailing virus
- Septembre: un adolescent est condamné à 11 mois de prison pour avoir piraté le téléphone portable de Paris Hilton
- Octobre: Samy, ver XSS infectant MySpace

2006...

- Novembre: loi française reconnaissant le génocide arménien
  - Vague d'attaque sur les sites webs français
- Montée en puissance des botnet

2007...

- Storm botnet
  - Commandé par le réseau P2P Edonkey/Overnet
  - Entre 1 000 000 et 50 000 000 de zombies
  - Utilisé pour DdoS et Spam
- Les principaux pays occidentaux retouvent des trojans chinois dans les réseaux de leurs administrations.

Constatations

- CodeRed, Nimda : failles connues et patchées depuis plus d’un an. Ils tournent encore...
- Slammer : faille connue et patchée depuis plus d’un an, sur un service ne présentant pas d’application sur Internet
- Blaster : faille connue et patchée depuis 7 jours, sur un service ne présentant pas d’application sur Internet

Rappels réseaux

- Model OSI
- TCP/IP et leurs amis
- VLAN
- Wifi

LE Modèle OSI

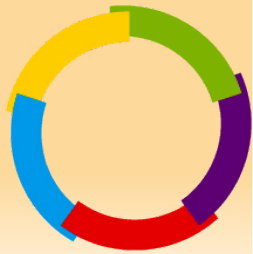
- Modèle à 7 couches
  - (7) Application
  - (6) Présentation
  - (5) Sesssion
  - (4) Transport
  - (3) Réseau
  - (2) Liaison
  - (1) Physique

Le modèle OSI

- « Quand le steack est trop cuit on ne va pas se plaindre au boucher »
  - Chaque couche est responsable de sa problématique et ne s'occupe pas de celle des autres couches.

Couche 1

- Couche physique : véhicule le signal sur le médium de communication
  - Câble coaxial
  - Paire torsadée
  - Fibre optique
  - Faisceau infrarouge
  - Faisceau hertzien
  - Faisceau laser



Couche 2

- Couche liaison, également appelée Medium Access Control (MAC) : mise en forme de l’information binaire.
- Répond à la problématique d'ordinateurs « directements connectés »
  - Ethernet
  - Token Ring
  - 802.11 (ie « wifi »)

Couche 3

- Couche réseau : trouver un chemin entre la source et la destination.
- Répond à la problématique de joindre un correspondant distant.
  - IPv4
  - IPv6
  - IPX
  - NetBEUI

Couche 4

- Couche transport : assure le transport de l’information de la source à la destination.
- Répond à la problématique d'extrémité, comment faire correspondre des services.
  - TCP
  - UDP

Couche 5

- Couche session : assure la communication entre le point de départ et le point d’arrivée
- Très peu utilisée dans le monde IP
  - FTP et ses deux connexions (commandes et données)
  - IRC et les connexions DCC
  - VoIP: H.323, SIP, ...

Couche 6

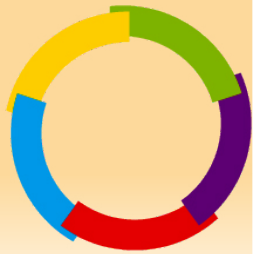
- Couche présentation : responsable de la mise en forme des données avant leur fourniture aux applications
- Peu utilisée dans le monde IP à l'exception notable de SSL/TLS

Couche 7

- Couche application : responsable de la communication entre les applications distantes impliquées dans l’échange de données
  - HTTP
  - SMTP
  - FTP

Le monde IP

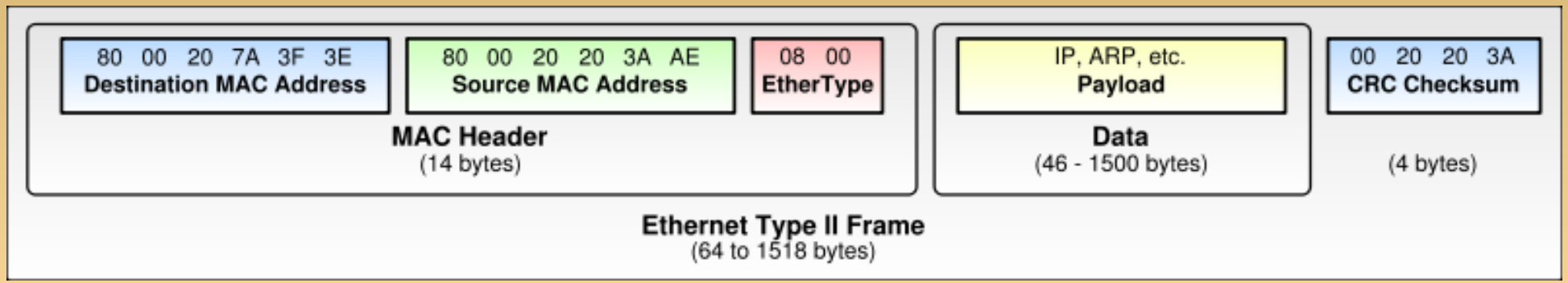
- Modèle simplifié
  - Application (couche 5/6/7) on parle de couche 7.
  - Transport (couche 4)
  - Reseau (Couche 3)
  - Physique (Couche 1/2)
- Les ingénieurs réseaux sont très friands des couches OSI et de leurs numéros (switch de niveau 3, Firewall de niveau 7, segmentation de niveau 2, switching de niveau 7, ...)



Les protocoles du monde IP

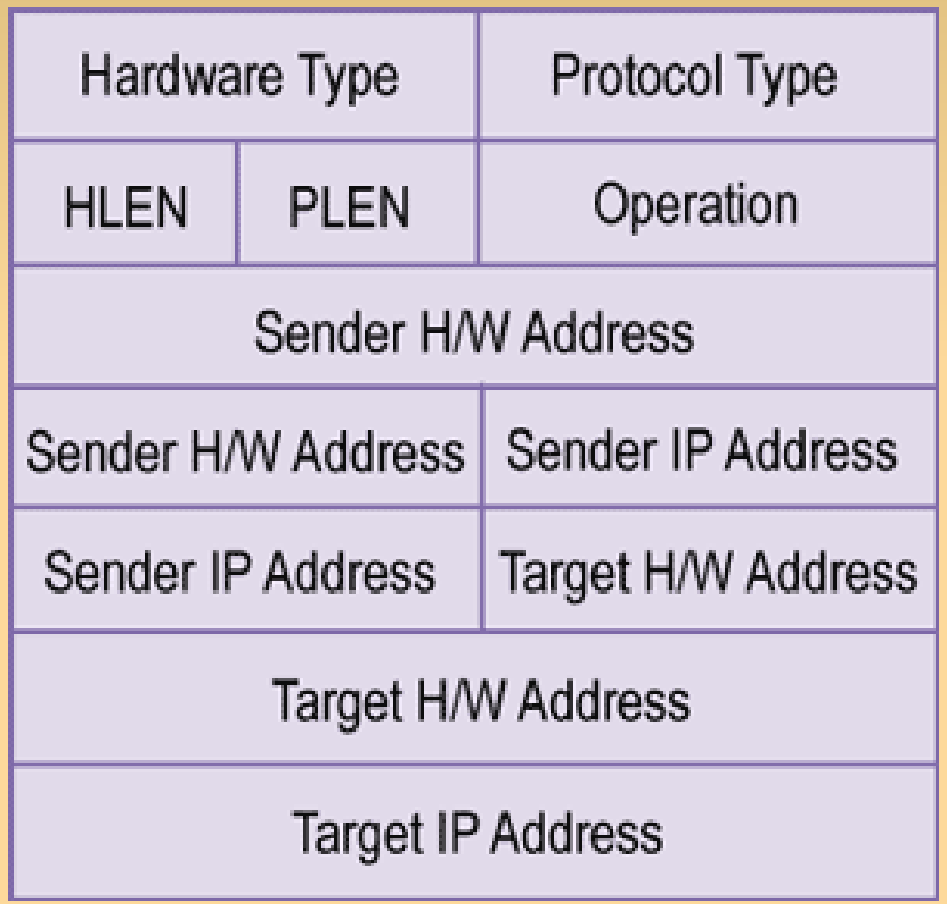
- Protocole de niveau 2: principalement Ethernet avec ARP pour le lien avec la couche 3
- Protocole de niveau 3: IP et Ipv6
- Transport: principalement TCP, UDP et ICMP (gestion des erreurs)

Ethernet



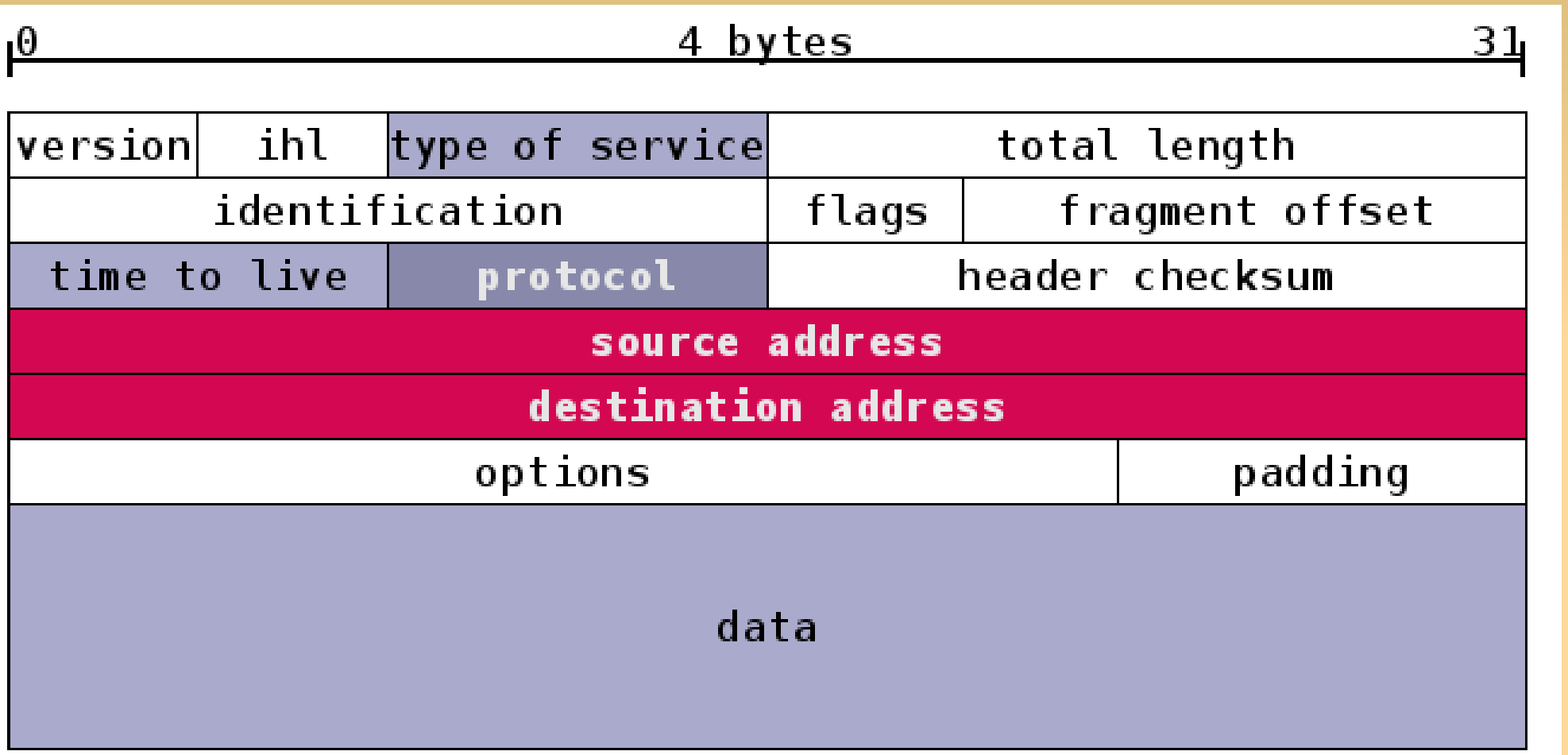
- Adresse MAC destination
- Adresse MAC source
- Type
- En fin de paquet, le CRC (checksum)
- Peut aussi contenir un tag 802.1Q (VLAN et priorité) ajoutant 4 octets

ARP, address resolution protocol

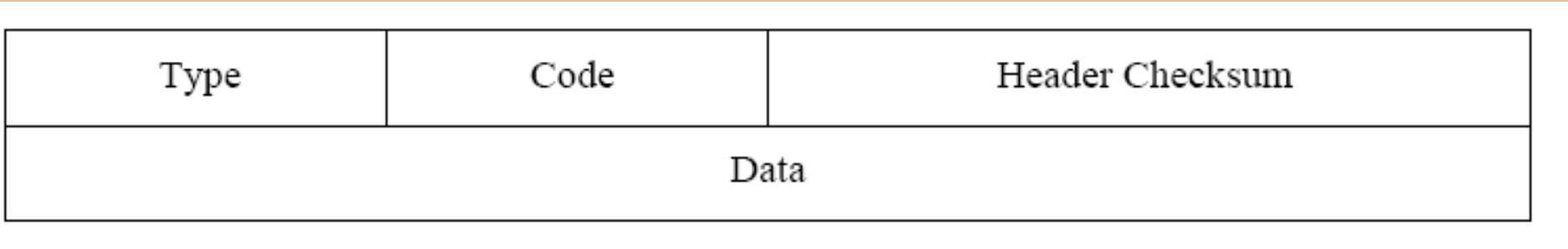


- Faire la correspondance entre MAC et IP
- Opération: 1 pour requête, 2 pour réponse

IP, Internet Protocol



ICMP, Internet control Message Protocol



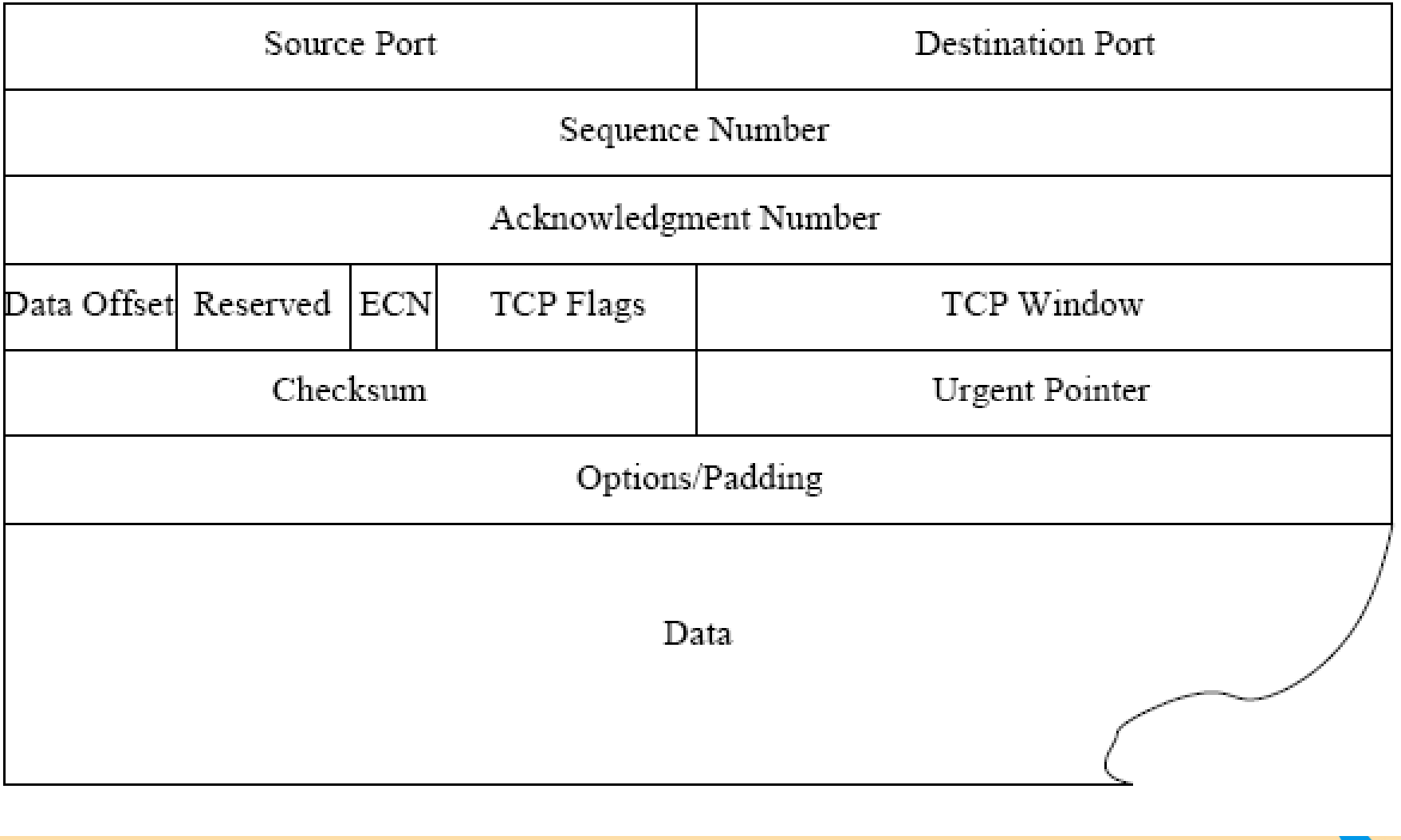
- Deux classes
  - Requête/réponse (comme ping)
  - Message d'erreur

UDP, User Datagram Protocol

Source Port	Destination Port
Length	Checksum (optional)
Data	

- Transmission de données façon bouteille à la mer (ie sans garantie sur la délivrance)

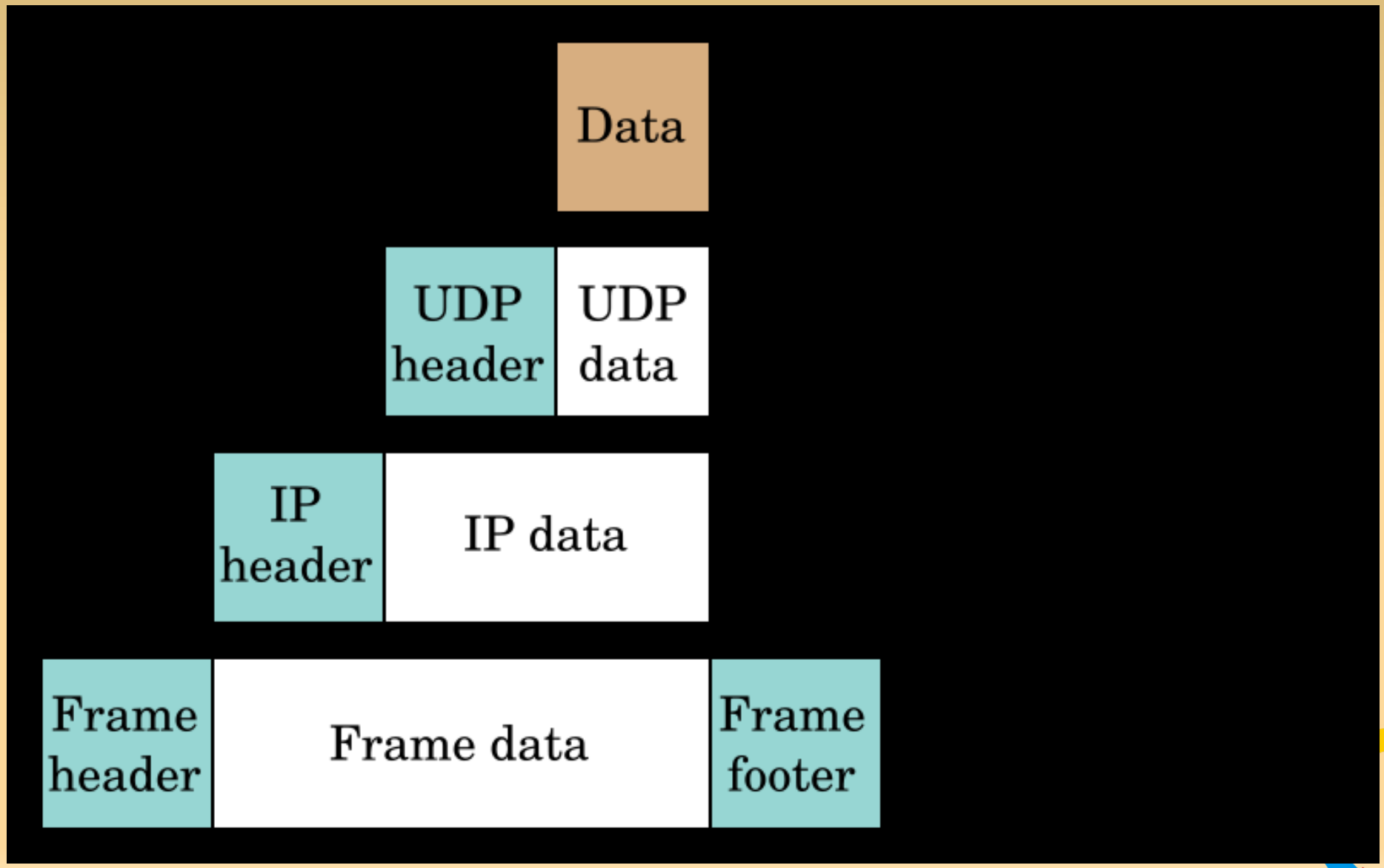
TCP, Transmission Control Protocol



TCP

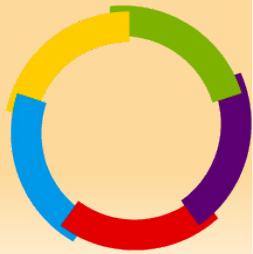
- Principes de base
  - Circuit virtuel à double sens
  - Double fenêtre coulissante en émission (séquence) et en réception (acquittement)
- Établissement (Handshake) à trois messages:
  - SYN/SYN-ACK/ACK
- Fermeture à quatre messages :
  - FIN-ACK/ACK//FIN-ACK/ACK
- Fermeture anticipée : RST-ACK

Un exemple de paquet



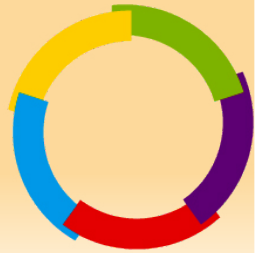
Mise en musique

- Communication dans un LAN
  - Le protocole ARP
  - Unicast et broadcast
- Communication à distance
  - Notions de routage



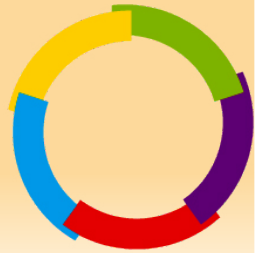
Communication dans un LAN

- La machine A veut envoyer un paquet à la machine B qui est dans le même LAN qu'elle.
  - A regarde sans sa table de routage si B est bien dans son LAN -> oui.
  - A demande à toutes les machines auxquelles elle est directement connectée qui est B (ie quelle est son adresse de niveau 2).
  - **C'est le protocole ARP qui entre en jeu.**



Communication dans un LAN (suite)

- A forge un paquet avec comme adresse destinataire de niveau 2 et de niveau 3 celle de B.
  - B voit passer un paquet avec comme adresse de niveau 2 son adresse, l'OS récupère le paquet.
  - L'IP destination est la sienne, l'OS transfère le paquet à l'application concernée.



Communication dans un LAN (tcpdump -e)

- ping 192.168.2.10
  - **Envoi d'un paquet ARP who-has (broadcast L2)**

```
22:02:38.037046 00:0e:35:7f:06:a2 > ff:ff:ff:ff:ff:ff, ethertype ARP
   (0x0806), length 42: arp who-has 192.168.2.10 tell 192.168.2.11
```

  - **Réponse ARP reply (unicast L2)**

```
22:02:38.040586 00:0c:6e:77:48:5f > 00:0e:35:7f:06:a2, ethertype ARP
   (0x0806), length 60: arp reply 192.168.2.10 is-at 00:0c:6e:77:48:5f
```

  - **Envoi d'un paquet unicast L2.**

```
22:02:38.040609 00:0e:35:7f:06:a2 > 00:0c:6e:77:48:5f, ethertype IPv4
   (0x0800), length 98: 192.168.2.11 > 192.168.2.10: ICMP echo request,
   id 19223, seq 1, length 64
```

Broadcast L3 dans un LAN

- ping -b 192.168.2.255
  - Un ping sur l'adresse IP de broadcast est traduite par un paquet à destination de l'adresse de broadcast L2.

```
22:10:57.972762 00:0e:35:7f:06:a2 > ff:ff:ff:ff:ff:ff, ethertype IPv4
   (0x0800), length 98: 192.168.2.11 > 192.168.2.255: ICMP echo request,
   id 39191, seq 1, length 64
```

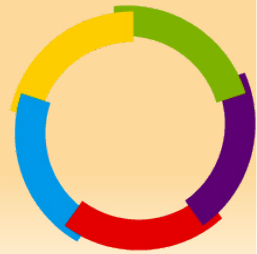
  - Ce paquet va forcer toutes les IP du LAN à faire un arp who-has pour pouvoir répondre.

```
follc@follc:~$ sudo arp -an

? (192.168.2.250) à 00:01:E3:0F:60:E8 [ether] sur eth0

? (192.168.2.1) à 00:20:78:D0:0A:02 [ether] sur eth0
```

  - **En un seul paquet on a découvert tous les hosts du LAN répondant à un ping en broadcast.**



Ping L2

- Comment découvrir si une machine est présente alors qu'elle dispose d'un firewall ?
  - Il suffit de lui demander son adresse MAC (arp who-has).
    - Peut se faire en lui envoyant un paquet IP (par exemple ping) puis en analysant notre table arp (arp -a).
    - Peut se faire en une commande via scapy:
      - arping ("192.168.2.1")

scapy

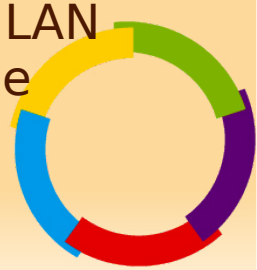
- Excellent logiciel permettant de jouer avec les couches 2/3 (et les autres).
  - **Envoi d'un paquet icmp avec MAC destination en broadcast:**

```
>>> res =
   srp(Ether(dst='ff:ff:ff:ff:ff:ff')/IP(dst='192.168.2.1')/ICMP())

>>> res[0][0][1]

<Ether  dst=00:0e:35:7f:06:a2 src=00:20:78:d0:0a:02 type=IPv4 |<IP
   version=4L ihl=5L tos=0x0 len=28 id=25271 flags= frag=0L ttl=64
   proto=ICMP chksum=0x92cd src=192.168.2.1 dst=192.168.2.11 options='' |
   <ICMP  type=echo-reply code=0 chksum=0xffff id=0x0 seq=0x0 |<Padding
   load='\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
   \x00\x00' |>>>>
```

Cela fonctionne, on peut donc communiquer avec les machines de son LAN sans connaître leur adresse MAC, il suffit d'envoyer le paquet à tout le monde (au sens de la couche 2).

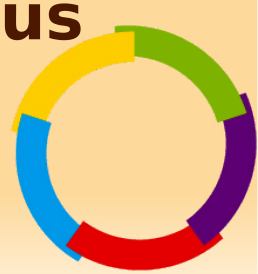


Questions
Dans un LAN

- Que se passe-t-il lorsque 2 stations ont la même MAC adresse (avec des hubs, avec des switchs)?
- Que se passe-t-il lorsque deux stations ont la même IP ?
- Cas légitimes où plusieurs IP ont la même MAC?
- Cas légitimes où plusieurs MAC ont la même IP?
- Que se passe-t-il lorsque l'on envoie des paquets avec une adresse MAC spoofée (ie ne pas changer l'adresse MAC de sa carte mais envoyer des paquets avec une adresse MAC source bidon)?

Éléments de routage

- Que se passe-t-il lorsque A veut envoyer un paquet à B qui n'est pas dans son LAN ?
  - La notion de routage apparaît, elle répond à la problématique « par où passer pour atteindre une IP distante ».
  - A consulte sa table de routage et trouve la gateway capable de transmettre le paquet.
    - **La gateway choisie est celle capable d'atteindre le LAN ayant le netmask le plus proche de B (ie la plus « spécialisée »).**



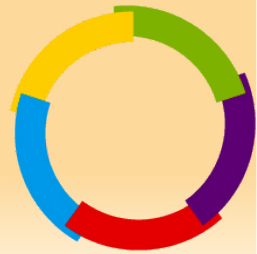
Choix de la gateway

- A: 192.168.2.10 -> B: 192.168.0.1
- Table de Routage de A:

Table de routage IP du noyau

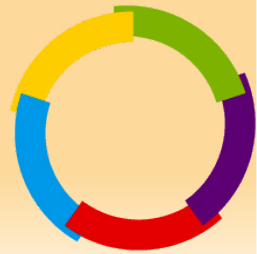
Destination	Passerelle	Genmask	Indic	Metric	Ref	Use	Iface
192.168.2.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
192.168.0.0	R1	255.255.255.0	U	0	0	0	eth0
192.168.0.0	R2	255.255.0.0	U	0	0	0	eth0
0.0.0.0	R3	0.0.0.0	UG	0	0	0	eth0

- Routes capables d'atteindre B ?
- Route choisie ?



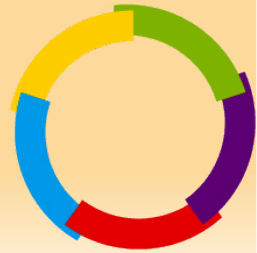
Éléments de routage

- A demande à R1 quelle est son adresse L2.
  - A forge un paquet avec comme adresse de niveau 2 R1 et comme adresse de niveau 3 B.
  - R1 voit le paquet sur sa carte réseau, il est destinataire au sens L2, le paquet est remonté à l'OS.
  - L'OS consulte la couche 3, il n'est pas destinataire au sens IP, il route le paquet.
- R1 consulte sa table de routage pour trouver comment atteindre B, etc ...



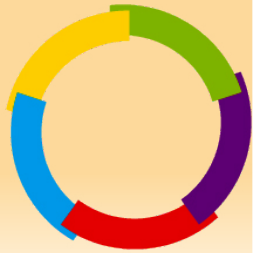
Routage

- Les tables de routage sur une machine peuvent être statiques (en général le cas sur les serveurs, postes et routeurs de petits et moyens réseaux).
- Elles peuvent être dynamiques (et s'échanger entre les routeurs).
  - **Sur Internet, eBGP.**
  - **Sur un réseau d'entreprise OSPF, RIP, iBGP, ...**
- Sous linux le routage (ie le fait de transférer un paquet lorsque l'on est destinataire au sens MAC mais pas au sens IP) se fait via:
  - **echo 1 > /proc/sys/net/ipv4/ip_forward**



Question

- Dans un réseau, les postes de travails sont configurés sans gateway et avec un netmask de 0.0.0.0. Etonnamment, tout fonctionne.
  - Qu'est ce qui se passe ?
  - Si ça marche comme ça, pourquoi s'embêter ?



Les menaces

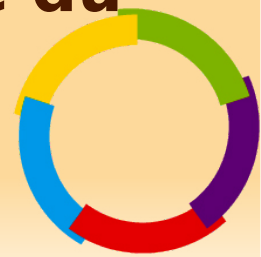
- Qu'est ce que l'on protège ?
  - La confidentialité (C)
    - Ne pas divulguer ses secrets
  - L'intégrité (I)
    - Empêcher l'altération de nos informations
  - La disponibilité (D)
    - Permettre l'accès au SI aux utilisateurs légitimes
  - Et aussi la traçabilité (T) (ou auditabilité, preuve)
    - Savoir ce qui se passe dans son SI

Attaques sur les couches

- La couche physique (couches 1/2)
- La couche réseau (couche 3)
- La couche transport (couche 4)
- La couche applicative (couches 5-7)

Couche physique

- Accès au medium de communication:
  - Filaire, hertzien, ...
- Typiquement, un pirate est dans vos locaux et a accès à une prise Ethernet de votre réseau (ou est sur le parking et accède à votre réseau en wifi).
  - Corruption possible de toutes les couches supérieures.
    - **C'est la pire des situations... la meilleure du point de vue du pirate.**



Couche physique

- Corruption des mécanismes de niveau 2
  - Usurpation d'adresse MAC (MAC spoofing)
  - MAC Flooding
  - VLAN Hoping
  - Corruption de signalisation (STP, VTP, CDP, etc.)
- La plupart des mécanismes de niveau 2 ne sont pas des mécanismes de sécurité !

Couche physique/réseau

- Attaque de ARP
  - Introduction de réponses usurpées (ARP Spoofing)
  - Corruption du cache ARP (ARP Cache Poisoning)
  - Cas typique de problème de cohérence entre les couches
- Conséquence : redirection de trafic (Graal de l’intrus)

Redirection de trafic

- Conséquences
  - Ecoute (C)
  - Détournement (C, I)
  - Modification (I)
  - Usurpation d’adresse (C, I)
  - Déni de service (D)
- Une possibilité de redirection est lourde de conséquences, quel qu'en soit le niveau

Couche réseau

- IPv4 n’apporte aucune sécurité
  - Pas d’authentification (usurpation)
  - Pas de confidentialité (écoute)
  - Pas de contrôle d’intégrité (modification)
  - Le coeur d’Internet est aisément corruptible
  - Entête compliquée, extensible via des options parfois malheureuses (source routing)

Couche réseau

- IPv6 pallie certains manque de IPv4
  - Nombre d’adresses
  - Entête plus simple de taille fixe
  - Entête extensible facilement via le champ NextHeader
  - Intégration de mécanisme de sécurité possible (IPSEC), ce mécanisme à été porté sur IPv4.

IPv6

- Beaucoup de difficultés à s'imposer
  - Les mécanismes de sécurité (IPSec) ont été backportés sur IPv4
  - Les matériels tardent à supporter IPv6 au même niveau que IPv4
  - Le principal avantage (le seul?) concerne la raréfaction des adresse IPv4.
- Mais les choses évoluent...
  - L'Asie utilise beaucoup IPv6
  - Tous les backbones des administrations US doivent être compatibles IPv6 pour 2008.

Couche transport

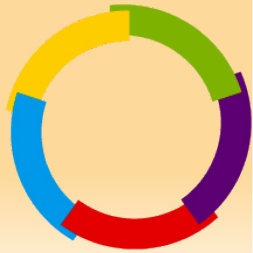
- UDP n’apporte rien
  - Aussi vulnérable qu’IP
- TCP, parce qu’il met en oeuvre un circuit virtuel, est un peu plus sûr
  - Les paquets doivent arriver
  - Les paquets sont ordonnés
  - Chaque octet de donnée est acquitté
  - Il est difficile de spoofer en aveugle
  - Il est difficile d’insérer du trafic

Couche application

- La plupart des protocoles applicatifs
  - Circulent sans authentification ou avec des authentifications en clair
  - Circulent en clair
  - Circulent sans contrôle d’intégrité
- Cependant, quelques réactions
  - Secure Socket Layer (SSL) et Transport Layer Security (TLS)
  - Protocoles sécurisés (SSH par exemple)

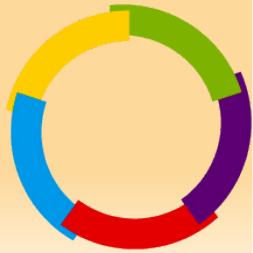
Couche application

- Les applications sont le point de traitement des données transportées sur le réseau
  - Elles sont le point de prise de l'intrus sur le système
  - Ce sont elles qui vont présenter les vulnérabilités exploitables à distance



Les VLAN

Qu'est ce que c'est ?

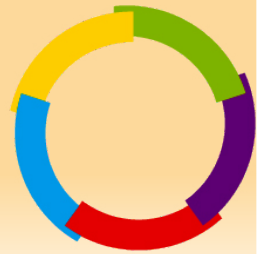


Les VLAN

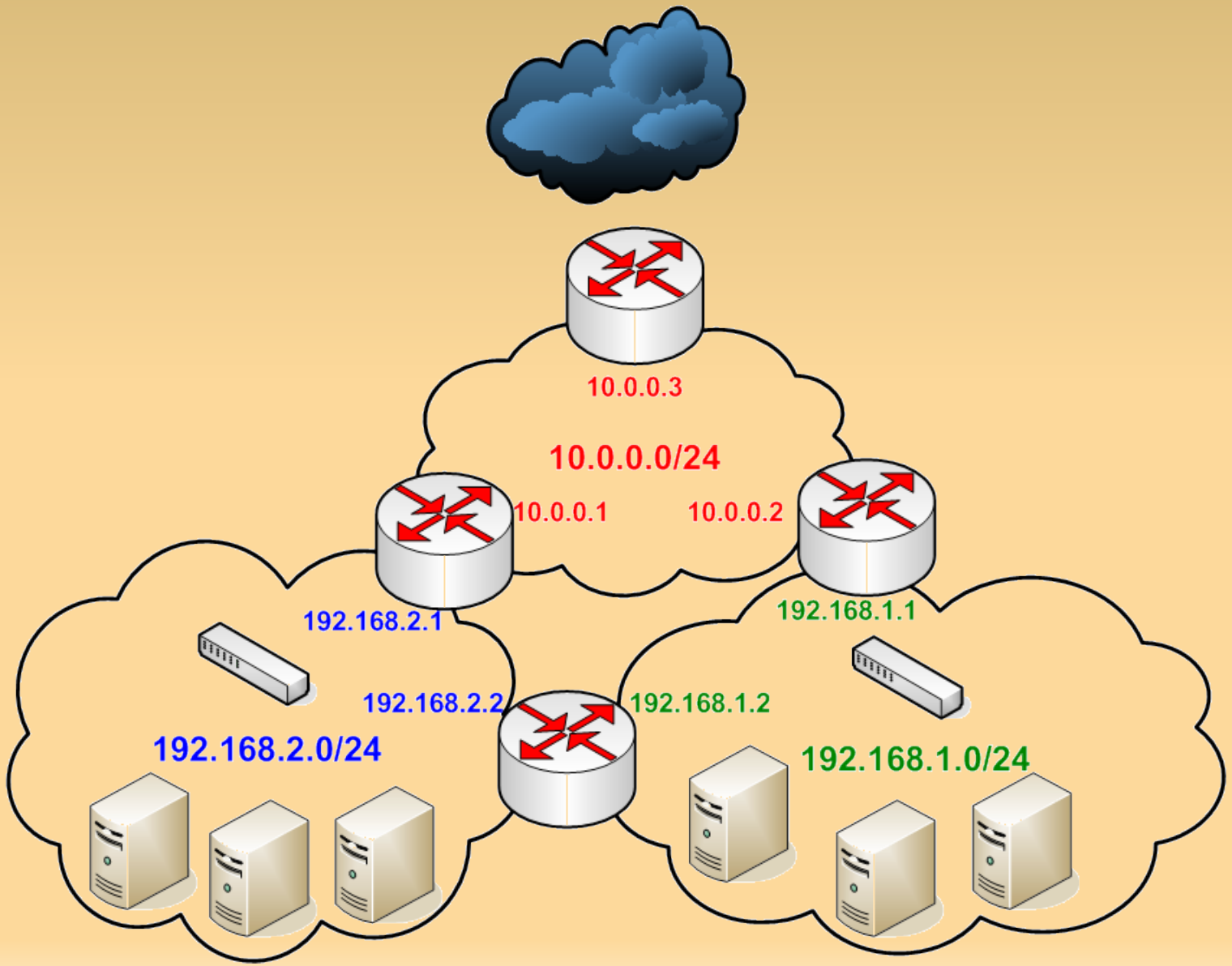
- Rappel sur les switchs
  - Équipement de niveau 2.
  - Il « connaît » pour chacun de ses ports, la liste des équipements reliés en niveau 2, c'est à dire les adresses MAC.
  - La connaissance de la liste de ces adresses MAC se fait par apprentissage au fur et à mesure des paquets .
  - Quand il reçoit un paquet, il regarde l'adresse de niveau 2 de destination (i.e. adresse MAC) et transmet le paquet sur le port où se trouve la machine avec cette adresse MAC.
  - Il n'a (théoriquement) aucune connaissance des adresses IP.

Exemple de commande sur un switch cisco

```
rrgi1#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.30.205.125      230   000b.5fe7.8180  ARPA   Vlan99
Internet  172.30.205.124        -   000b.5fe7.8a80  ARPA   Vlan99
Internet  172.30.195.116        9   0030.0589.f54c  ARPA   Vlan5
Internet  172.30.195.100        1   0006.5b26.16e0  ARPA   Vlan5
Internet  172.30.192.103        -   0800.46db.f2d3  ARPA
Internet  172.30.192.100        -   0800.46dc.7d36  ARPA
Internet  172.30.192.101        -   0800.46da.c7de  ARPA
```

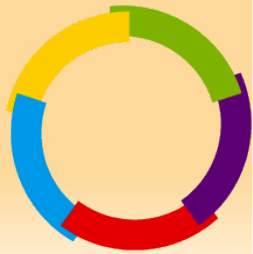


Un réseau hier



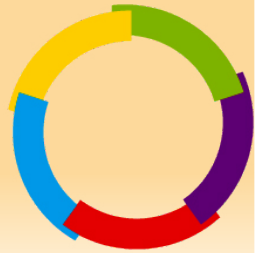
Problèmes

- Je veux placer dans la salle machine/baie du réseau 192.168.2.0/24 un serveur du réseau 192.168.1.0/24.
  - Il faut tirer un câble jusqu'au réseau 192.168.2.0/24.
  - Ou déplacer physiquement le serveur.
- Si l'on désire subneter un réseau il faut acheter un nouveau routeur s'il n'y a plus de port libre.



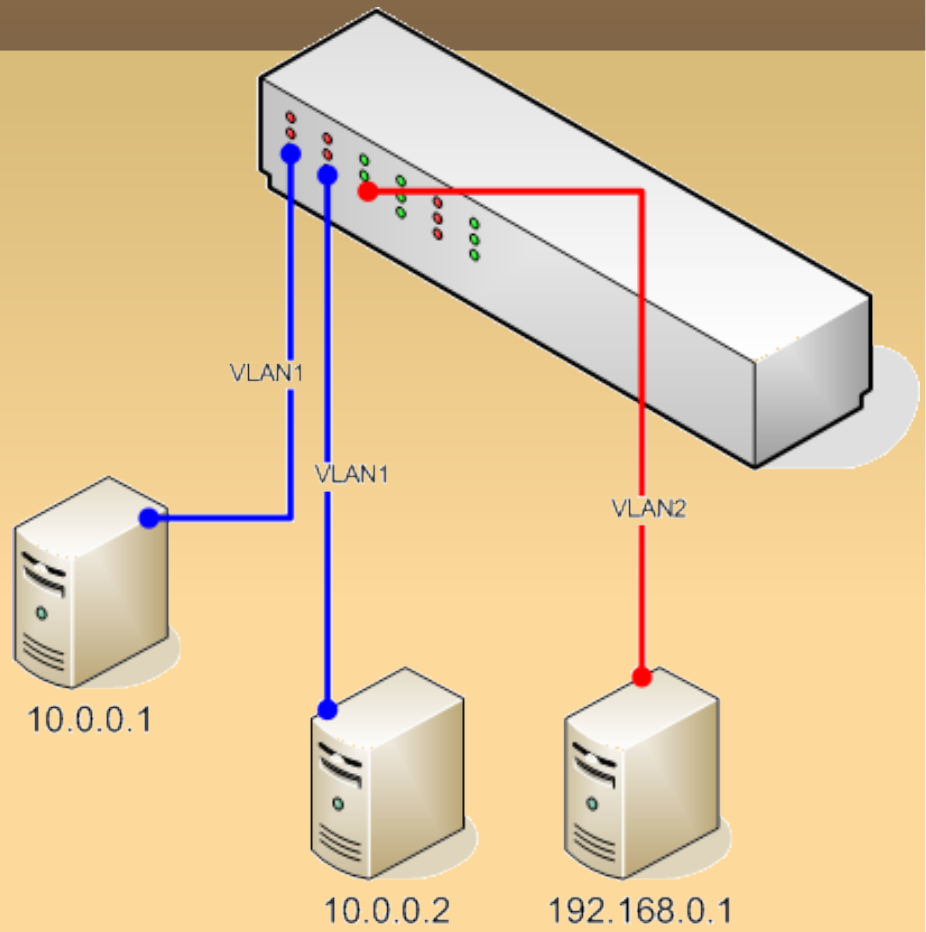
Les VLAN

- Concept:
  - Les VLAN permettent de faire coexister de manière sûre plusieurs domaines de broadcast sur un même switch.
- Buts:
  - Simplifier le brassage. « Comment changer un poste de réseau sans avoir à déplacer le poste » ?
  - Ne pas multiplier le nombre de routeurs.
  - Ne pas multiplier le nombre de ports sur les routeurs et firewalls.
  - Subneter facilement.

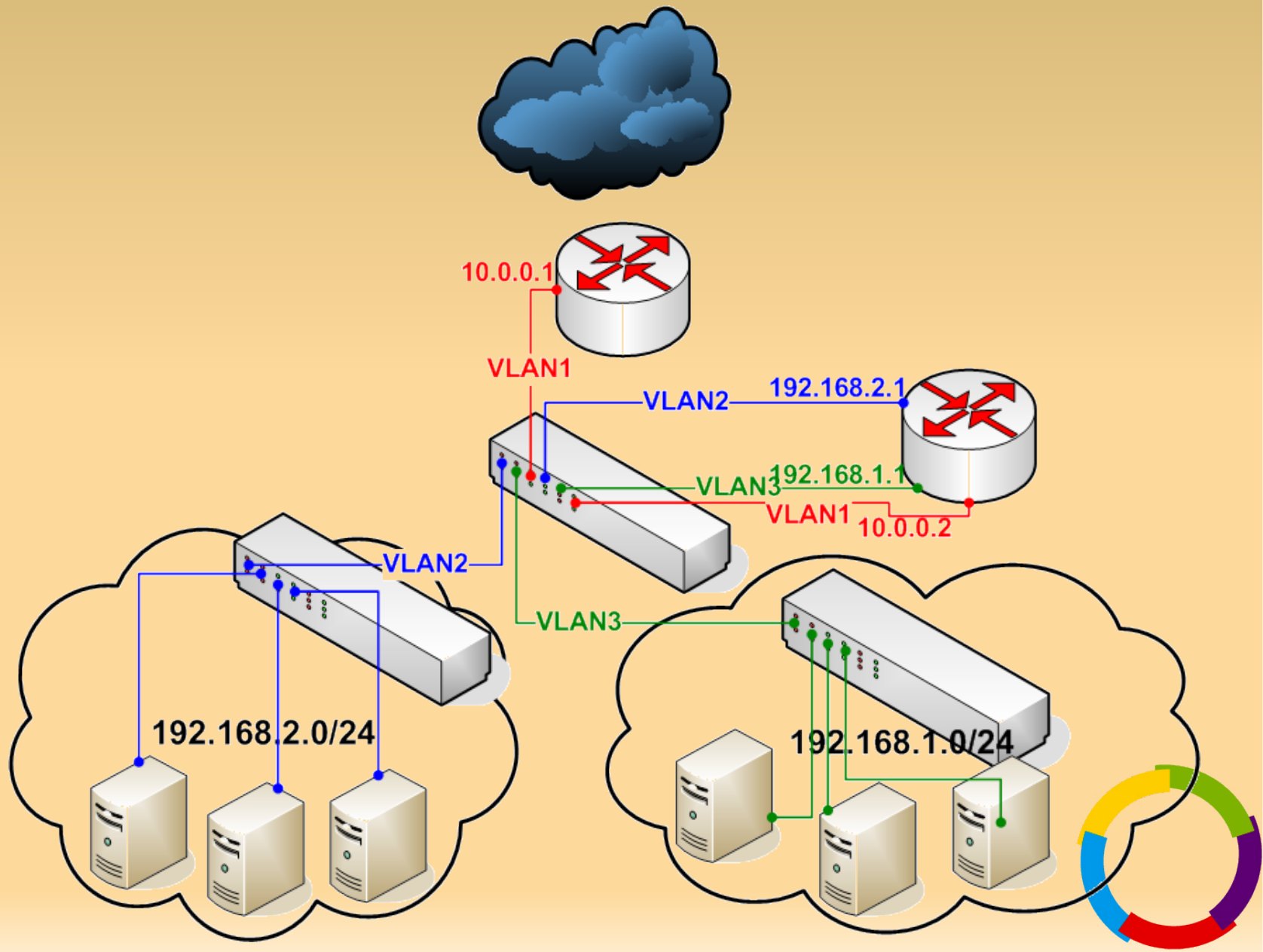


VLAN sur un switch

- Les ports 1 et 2 sont configurés en VLAN1.
- Le port 3 est configuré en VLAN2.
- 10.0.0.1 et 10.0.0.2 peuvent communiquer (ils appartiennent au même VLAN).
- Les postes sur le VLAN 100 (bleu) ne peuvent joindre ceux du VLAN 200 (rouge) (et réciproquement)



Les même réseau avec des VLAN

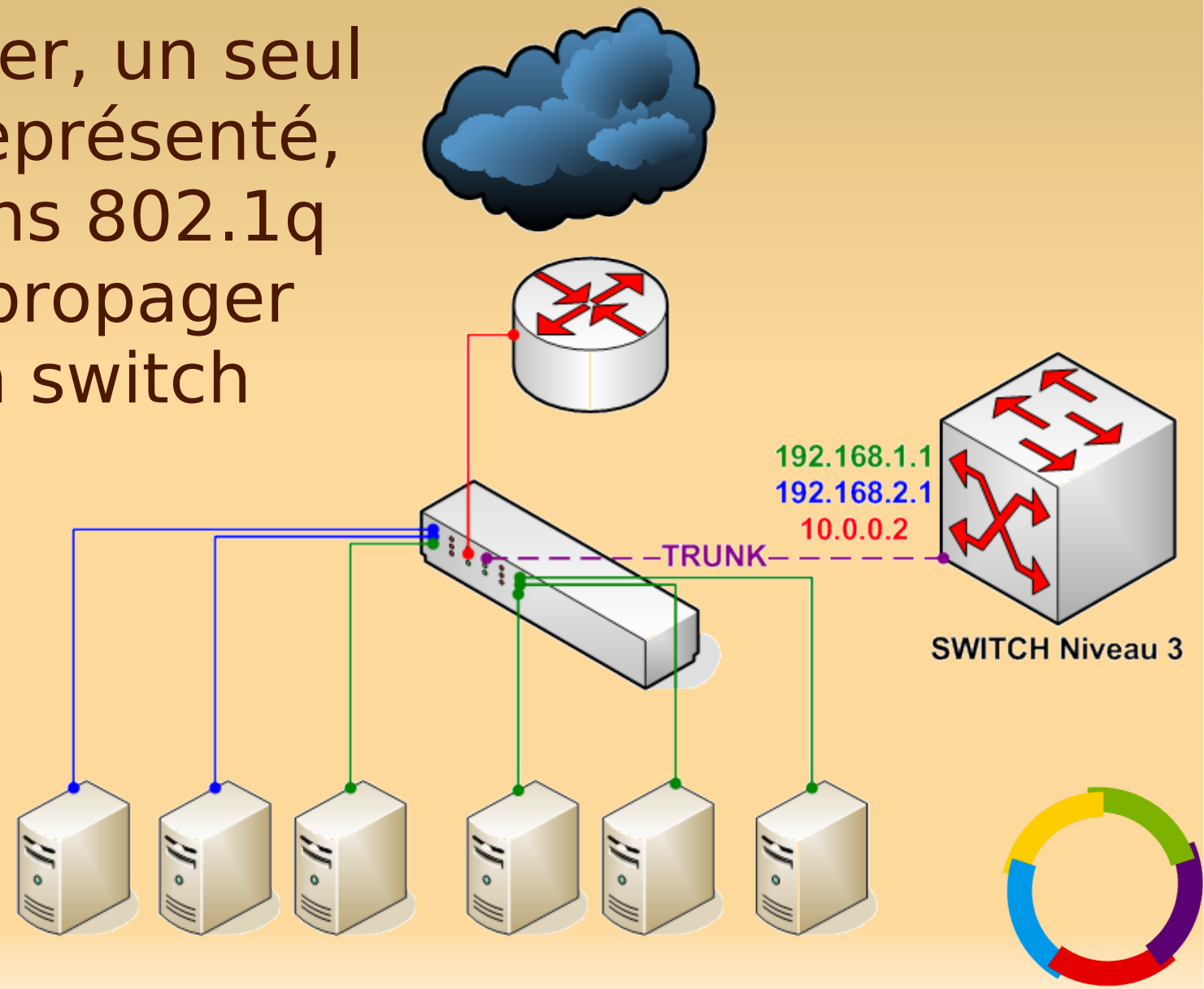


Notion de lien 802.1Q (ou TRUNK)

- Un lien 802.1q ou TRUNK (terminologie cisco) permet de faire transiter plusieurs VLAN sur un lien réseau.
- Afin de savoir à quel VLAN appartient un paquet d'un lien 802.1q, un tag est ajouté sur la couche 2.

Le même réseau avec un trunk

Pour simplifier, un seul switch est représenté, mais des liens 802.1q peuvent se propager de switch en switch



Les switchs de niveau 3

- Ils permettent de faire du routage Inter-VLAN sur les liens 802.1q.
- Ils ont des adresses IP comme des routeurs.
- La différence entre routeur et switch niveau 3 est faible.

Comment on les configure ?

- Les switchs
  - A configurer sur chaque port:
    - A quel VLAN il appartient ?
    - Si c'est un TRUNK, quels sont les VLANS propagés.
- Les switchs L3
  - Pareil et ajouter une IP par VLAN (comme sur un routeur on ajoute une IP par interface).
- Il est possible d'automatiser la propagation des VLAN vers les switchs d'extrémité grâce au protocole VTP (VLAN Trunk Protocol), protocole propriétaire cisco.

Comment ça se configure ?

- Native VLAN X
  - Sur un lien trunk, spécifie que les paquets non taggés appartiennent au VLAN X. En général c'est le VLAN 1.
- Private VLAN
  - Système permettant à deux ports d'un VLAN de ne pas pouvoir communiquer.
    - Typiquement empêche les machines d'un même LAN de se voir. Les oblige à passer par leur gateway.

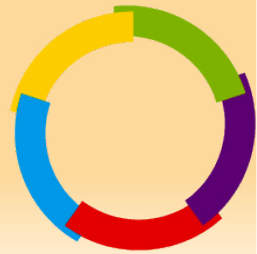
Exemple de conf sur switc cisco

- Sur ce port les paquets arrivent non taggés et appartiennent au VLAN 600.

```
interface GigabitEthernet0/1
    switchport access vlan 600
    switchport mode access
```

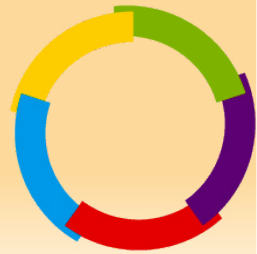
- Sur ce port les paquets sont taggés et les VLANS 600 à 610 peuvent transiter.

```
interface GigabitEthernet0/2
    switchport trunk encapsulation dot1q
    switchport trunk allowed vlan 600-610
    switchport mode trunk
```



Un réseau typique

- Les switchs en capillarité possèdent un port en mode trunk et tous les autres sont configurés avec un VLAN donné (sur lesquels sont branchés les serveurs, PC).
- Ils sont reliés directement (ou en cascade) aux switchs de niveau 3 de coeur effectuant le routage inter-VLAN.
- La redondance est assurée en doublant les liens et en créant des boucles entre les switchs
  - Le Spanning Tree Protocol (STP) est chargé d'empêcher les boucles en désactivant certains chemins.
  - SPT est l'équivalent du routage dynamique pour le niveau 2.

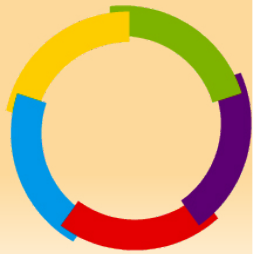


Routage inter-VLAN

- Aujourd'hui un routeur/Firewall n'a plus besoin que d'une interface s'il supporte les liens 802.1q.
  - La paquet rentre avec un tag indiquant qu'il appartient au VLAN X et ressort en indiquant qu'il appartient au VLAN Y.
- Windows et Linux supportent le routage inter-VLAN de même que la plupart des routeurs et firewalls propriétaires.

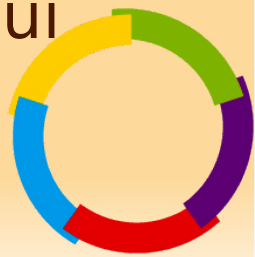
Routage inter-VLAN sous Linux

- Activer le coeur de routage:
  - # echo 1 > /proc/sys/net/ipv4/ip_forward
- Chargement du module noyau de VLAN:
  - # modprobe 8021q
- Création des VLAN 100 et VLAN 200
  - # vconfig add eth0 100
  - # vconfig add eth0 200

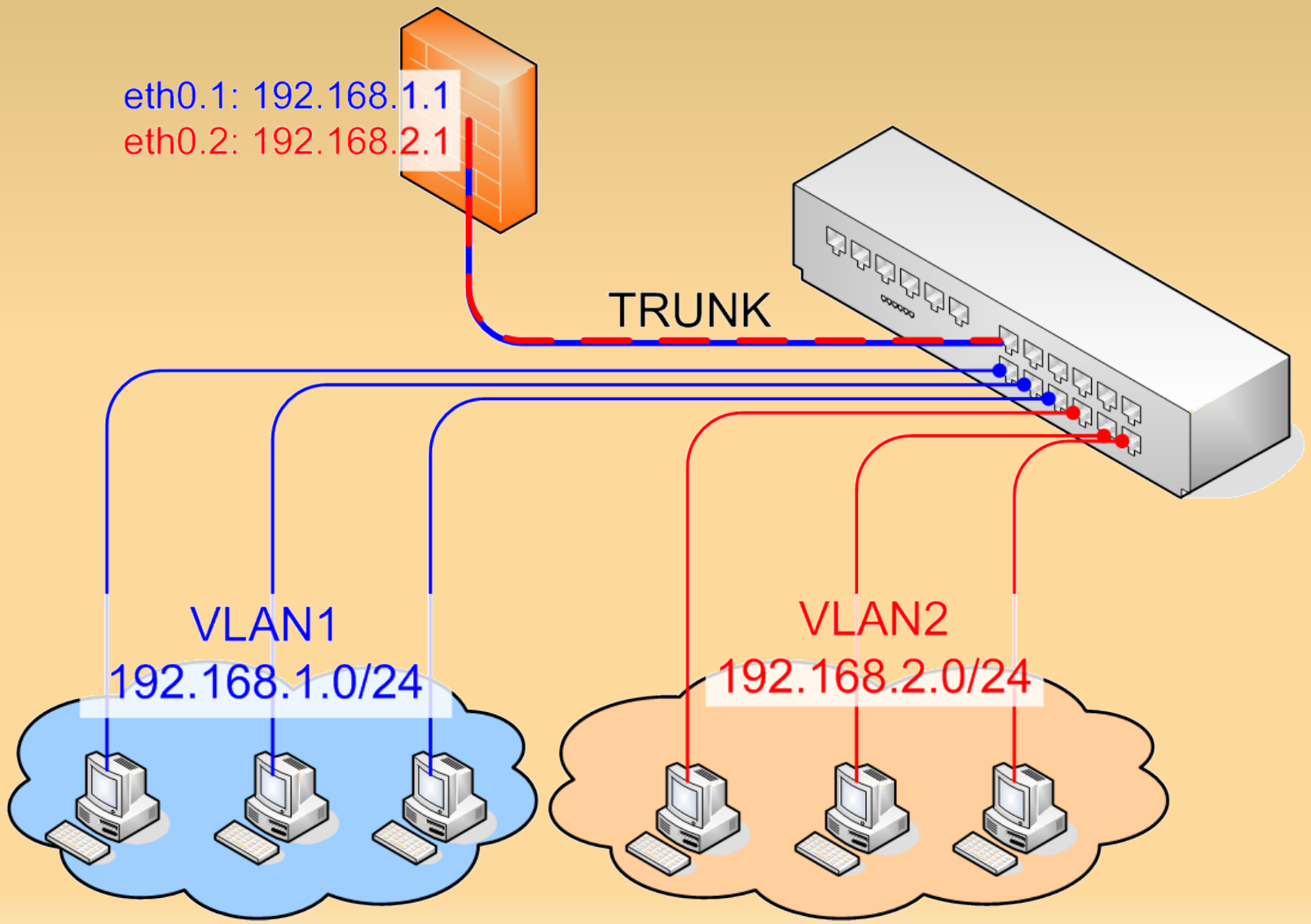


Routage inter-VLAN sous Linux

- Attribution d'adresses IP:
  - # ifconfig eth0.100 192.168.1.1
  - # ifconfig eth0.200 192.168.2.1
- Au final:
  - Sur eth0 la machine est capable de recevoir un trunk contenant les VLAN 100 et 200.
  - Elle est capable de router 192.168.1.0/24 et 192.168.2.0/24, les paquets rentrent et sortent sur la même interface mais avec un tag 802.1q différent.
  - Les paquets non taggés arrivent sur eth0, on lui attribue en général une adresse IP dédiée au management.



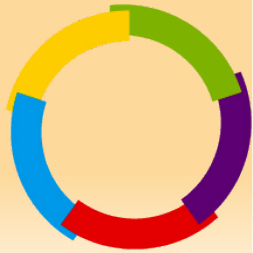
Routage inter-VLAN



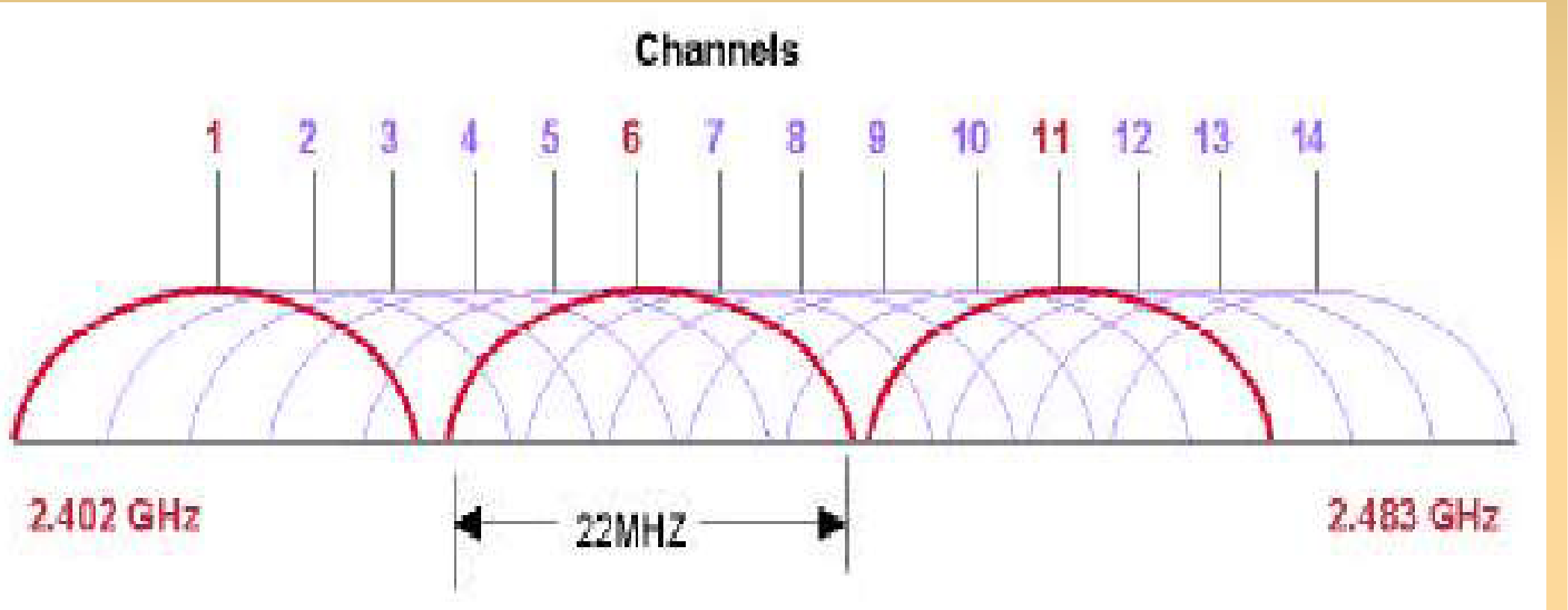
Les réseaux WLAN

Adapté d'un cours donné à l'INSA de Rouen

par Paul Tavernier
paul.tavernier@ac-rouen.fr

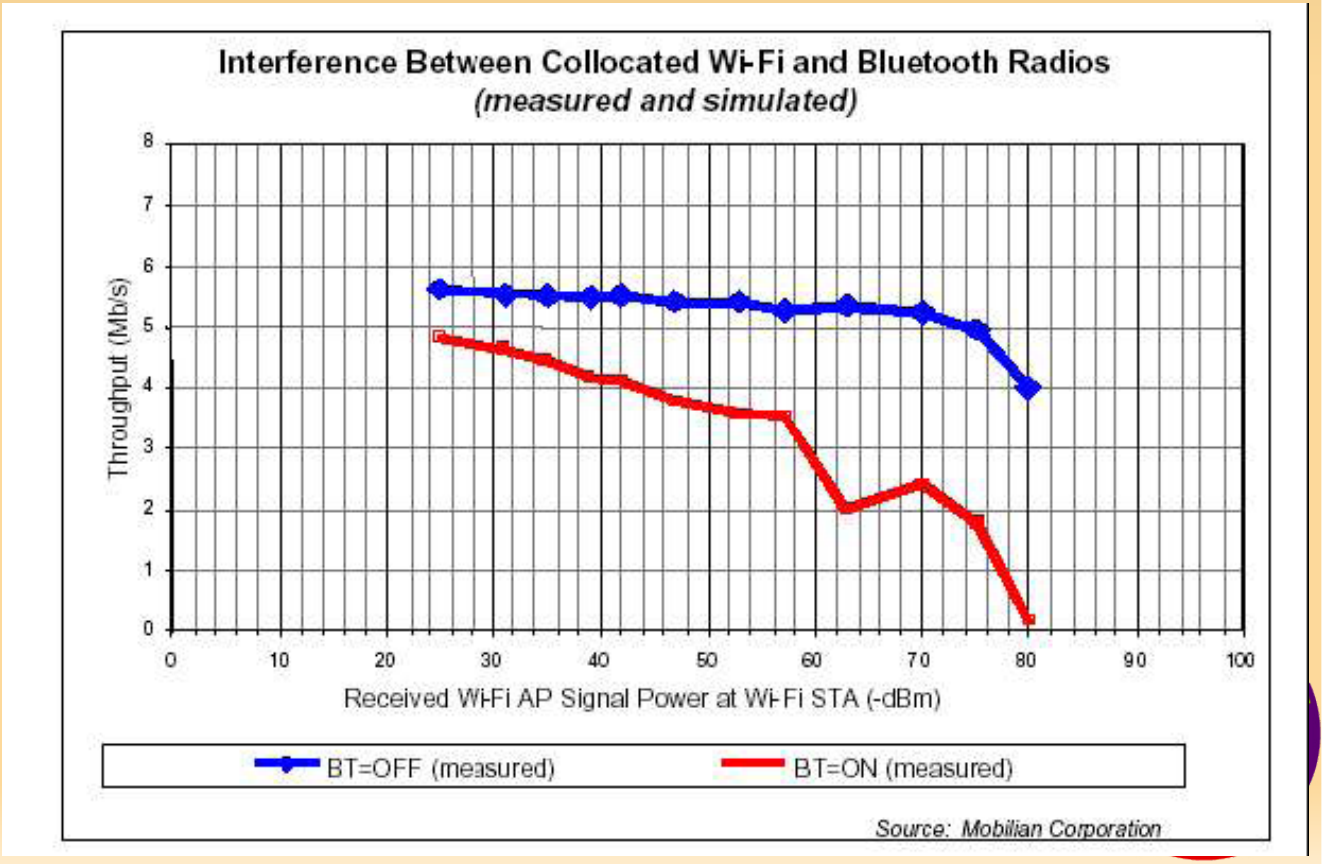


Les canaux



Interférences Wifi-BlueTooth

- En cas de coexistence, la probabilité de collision de fréquence durant une émission de trame 802.11 est comprise entre 48% et 62%
- Solution
  - Limiter l'usage de BT!



Réseaux sans-fils: WIMAX

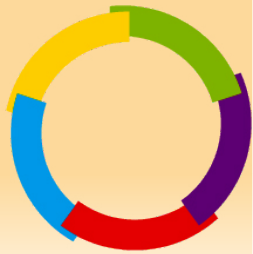
- WDSL – WiMAX (802.16)
  - Concurrent de xDSL (filaire) et du câble de télévision (CATV)
  - Débit théorique de 70 Mb/s sur 50 Km
  - Utilisation de 3 bandes de fréquence
    - 3,5 GHz, 2,5 GHz et 5,86 GHz
  - Diffusion « Point à multipoint »
  - Intégration de la puce WDSL dans les ordinateurs dès 2007 (annonce Intel du 10.12.06)
  - Intégration dans les ordinateurs de poche et les téléphones portables dès 2007
  - Ordre de prix des points d’accès
    - WI-FI: 100 €
    - WiMAX: 1 000 €
    - UMTS: plus de 10 000€

Réseaux sans-fils: 802.11

- Initialement une norme définissant un débit de 1 ou 2 Mbit/s
- Déclinée en diverses *révisions*
  - Adaptation des débits
    - 802.11a, 802.11b, 802.11g, 802.11n, ..
  - Apport de normes de sécurité
    - 802.11i, ...
  - Besoins d'interopérabilité
    - 802.11d (internationalisation), 802.11f (roaming), ...

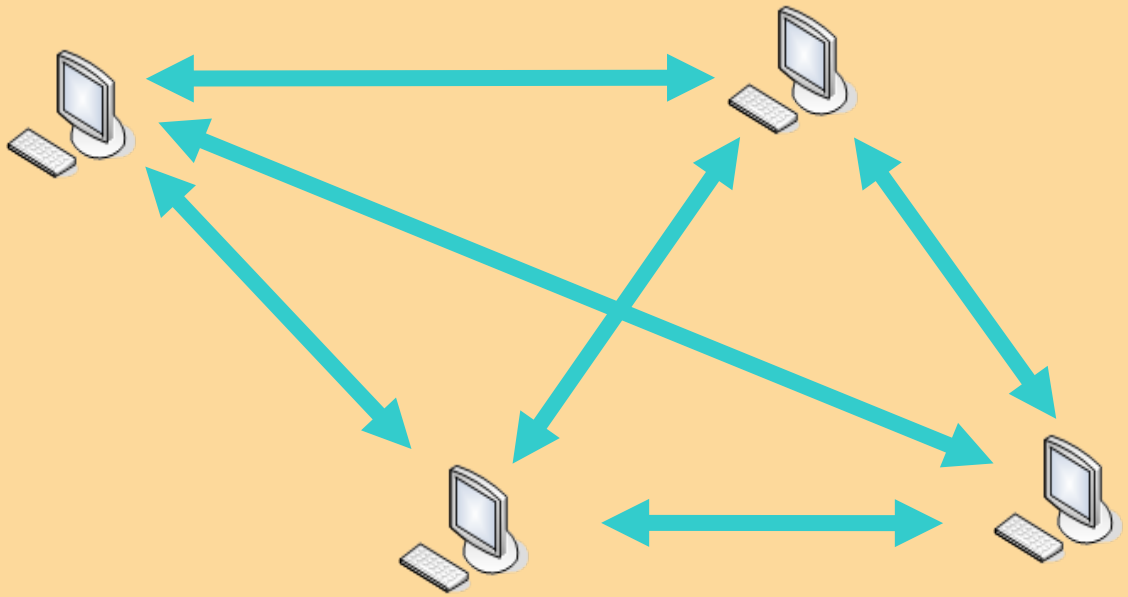
Reseaux sans-fils: 802.11

- S’attache à définir les couches basses du modèle OSI (1 et 2)
  - La couche physique (PHY)
  - La couche liaison
    - La sous-couche LLC
      - Reprend la norme LLC 802.2
      - Aiguillage des données vers la couche 3, éventuellement en mode connecté et/ou avec acquittement
    - La sous-couche MAC
      - Accès au support
      - On est proche des techniques utilisées sur Ethernet
- Une interface Ethernet 802.11 est similaire à une interface Ethernet 802.3
  - Vision identique pour les couches hautes (TCP/IP, app)
  - Adressage MAC identique
    - Les adresses MAC des bornes en plus
    - 4 adresses MAC par trame.



Réseaux sans-fils: modes de fonctionnement

- Mode "Ad-Hoc" ou réseau "point à point"
  - Mise en oeuvre simple, adapté au échanges de poste à poste
  - Permet, via la mise en œuvre de protocole de routage dynamique, de créer des réseaux mobiles *full-mesh*
    - OLSR (RFC3626)

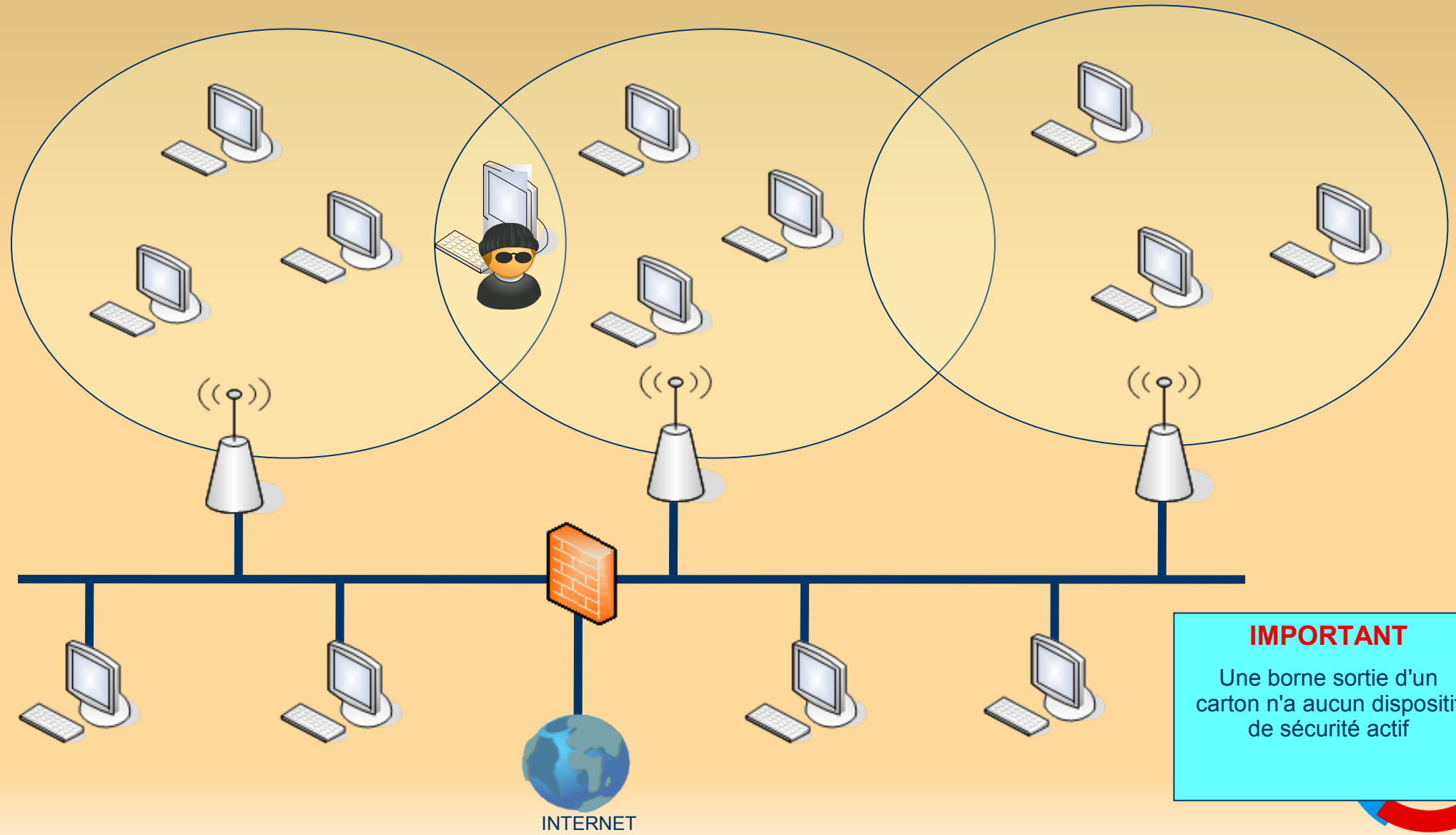


Mode dit "IBSS"

Ensemble de Services de Base Indépendant

Réseaux sans-fils: modes de fonctionnement

- Mode "**Infrastructure**": Les AP, ou *points d'accès*, deviennent les éléments VITAUX du réseau (en terme d'accès et de sécurité!)



IMPORTANT

Une borne sortie d'un carton n'a aucun dispositif de sécurité actif

Réseaux sans-fils: Mise en oeuvre

- Le beacon framing
  - Trames émises à intervalle régulier par un AP sur l'ensemble des 11 canaux
    - L'intervalle d'émission se doit d'être optimal
      - trop long: l'AP ne sera jamais détecté
      - trop court: épuisement des ressources
  - Contient (entre autres)
    - Un *timestamp*
    - Le FH (*Frequency Hopping*)
    - Le SSID
    - Le *Beacon Interval*
    - ...

Réseaux sans-fils: Mise en oeuvre

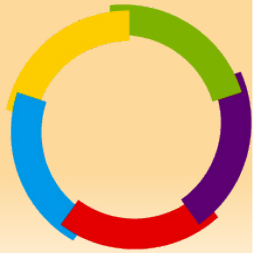
- Un client rejoint un BSS identifié par son SSID
  - Service Set Identifier
    - ESSID: L'identificateur du réseau (nom)
    - BSSID: MAC adresse de l'AP
  - Il sert d'identificateur
    - de réseau dans un contexte BSS/ESS
    - de connexion dans un contexte IBSS
  - N'est pas un dispositif de sécurité, mais d'identification.
  - Le SSID est non chiffré, mais peut être non diffusé
  - Véhiculé par les « beacon frames » de l'AP
- 2 phases sont observées
  - Association
  - Authentification

Association client-AP

- Enregistre la station auprès de l'AP
- A l'initiative de la station cliente (toujours)
- Obtention d'un AID (association identity) partagé entre chaque AP d'un ESS
- Pour cette phase, on peut faire un parallèle avec le monde Ethernet
  - ~ branchement de la RJ45 sur un switch

Authentification client-AP

- Prouver son identité afin de rejoindre un BSS/ESS
- 2 méthodes d'authentification
  - Ouverte
    - pas d'authentification
  - Partagée
    - on utilise la clé WEP pour chiffrer un défi envoyé par la borne (catastrophique!)
  - La désauthentification peut venir de l'AP ou du client.

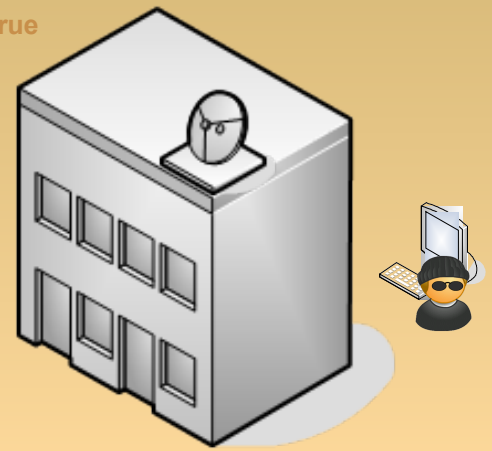


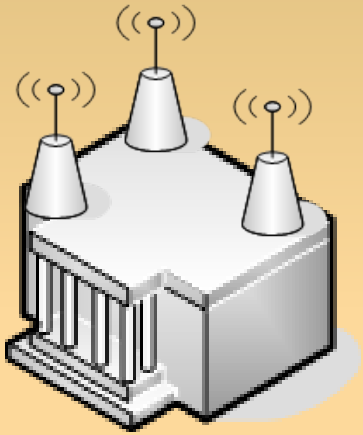
Réseaux sans-fils: Le roaming

- Permet de gérer l'itinérance au sein d'un même BSS
- Très orienté vers les nouveaux terminaux
  - PDA, Smartphones...
- Mécanisme de "préauthentification"
  - Permet à un client de s'identifier avec un autre AP sur lequel il risque de basculer
  - Les trames d'authentification générées par le client voyagent par l'intermédiaire du réseau filaire
  - Avantage: Roaming effectif
  - Inconvénient: Charge du serveur d'authentification

Réseaux sans-fils: sécurité, confidentialité...

Résidence
du coin de la rue





Entreprise X

Surf,
Ecoute,
Wardriving
WarChalking
DoS

Les réseaux d'entreprises n'auront bientôt plus de frontières délimitées et connues.

UNE SEULE (?) REPONSE
SECURISER LES POINTS D'ACCES

Réseaux sans-fils: les vulnérabilités

- Espionnage
  - Écoute passive (sniffing)
- Modification de messages
  - Contenu
  - Identifiants (MAC, IP)
    - Attaques MitM
- Déguisement
  - Masquerading
- Dénis de service (DoS)
  - Inondation de paquets De-auth/De-Assoc
  - Brouillage radio

Sécurité des réseaux informatiques

- Avec ou sans fil…
  - …Mais toujours avec au moins 2 « interlocuteurs » qui doivent se garantir mutuelle confiance
    - Authentification
    - Intégrité
    - Confidentialité
    - Non répudiation
    - Non rejeu
  - 5 **principes essentiels** qui doivent pouvoir se vérifier quelle que soit la nature du transport utilisée sur un réseau informatique
    - Cependant…aucun caractère obligatoire.
      - Dépend du contexte
      - Dépend du besoin

Un des fondements de 802.11: WEP

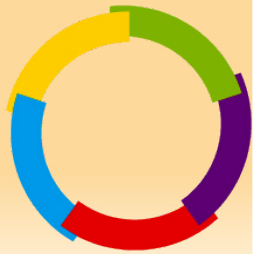
- Devait permettre en théorie de fournir un niveau de sécurité équivalent à celui d'un réseau filaire
- Implémentation catastrophique sans consultation avec les cryptologues
- Basé sur l'algorithme de chiffrement par flot (symétrique) RC4
- Intégrité des données basée sur CRC32
- Peut servir aussi pour l'authentification des stations (shared mode)
  - Comme ça, un pirate récupère le défi en clair ET le défi chiffré par simple écoute passive
  - Dans ce cas, le calcul de clé est dérivé d'une passphrase (souvent triviale, et attaquable par dictionnaire

Le cassage de clés WEP

- Attaque statistique
  - capture de 100000 IV (WEP64) à 500000 (WEP128)
  - automatisé par la suite aircrack de Christophe Devine
  - la récupération de dump réseau pouvant être très largement accélérée par injection de trafic
    - aireplay
  - extrêmement performante avec un volume d'IV raisonnable (moins d'une heure de capture)
    - environ 10" sur un Pentium 4

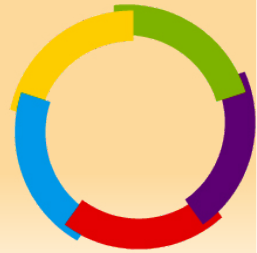
Le virage WPA/WPA2

- WEP ne garantissait plus rien dès 2001!
- WPA
  - Wireless Protected Access
  - sous forme de recommandations dans un premier temps par la Wi-Fi Alliance (ex WECA) - Avril 2003
  - palliatif à la faiblesse de WEP
  - jonction entre le monde WEP et WPA2
- WPA2
  - sous forme de norme (802.11i) à partir de juin 2004



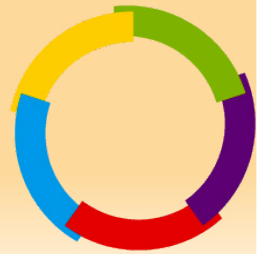
Le WPA: Wireless Protected Access - Avantages

- **Solution du WECA pour corriger les erreurs du WEP**
- **Profil de 802.11i promu par le WECA**
- **Permet de combler une partie des problèmes du WEP**
- **Utilisation du mécanisme TKIP**
  - **Changement des clefs de chiffrement de façon périodique**
    - **10ko de données échangées**
  - **Clef à 128 bits**
  - **Vecteur d'initialisation de 48bits (281 474 976 710 656 possibilités)**
  - **Impossibilité de réutiliser un même IV avec la même clef**
  - **Utilisation du MIC qui est un contrôle d'intégrité de tout le message**
  - **2 modes de fonctionnement**
    - **Mode PSK (*PreShared Key*) secret partagé**
    - **Mode à base de 802.1X pour une authentification centralisée (radius)**



Le WPA: Wireless Protected Access - Inconvénients

- **Conserve une filiation certaine avec WEP**
- **Pas de réponse à la sécurisation des réseaux multi-points Ad-Hoc (prévu dans le 802.11i)**
- **Pas de chiffrement symétrique robuste**
  - **RC4 toujours...**
- **Nécessité d'avoir des équipements capables d'évoluer de WEP vers WPA**
- **Obligation de déployer une architecture AAA dans le cas de WPA-Enterprise**

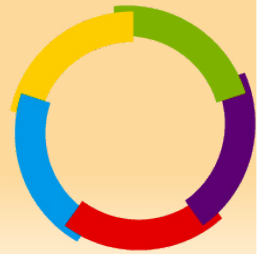


Le WPA2: vers la maturité...

- **Enfin une réponse point par point à la problématique de sécurisation d'un réseau (RSN: *Robust Security Network)***
  - **Authentification/Itinérance**
    - **le client n'est plus authentifié par un AP mais par un dispositif indépendant central au sein de l'ESS/BSS**
  - **Intégrité/Confidentialité**
    - **distribution dynamique des clefs par couple client-AP**
    - **HMAC-SHA1 (intégrité)**
    - **AES (chiffrement)**
- **(Re)Popularisation de 802.1x**
  - **EAP**
- **Ratification d'une norme: 802.11i**

Sécurité WPA2: La norme 802.11i

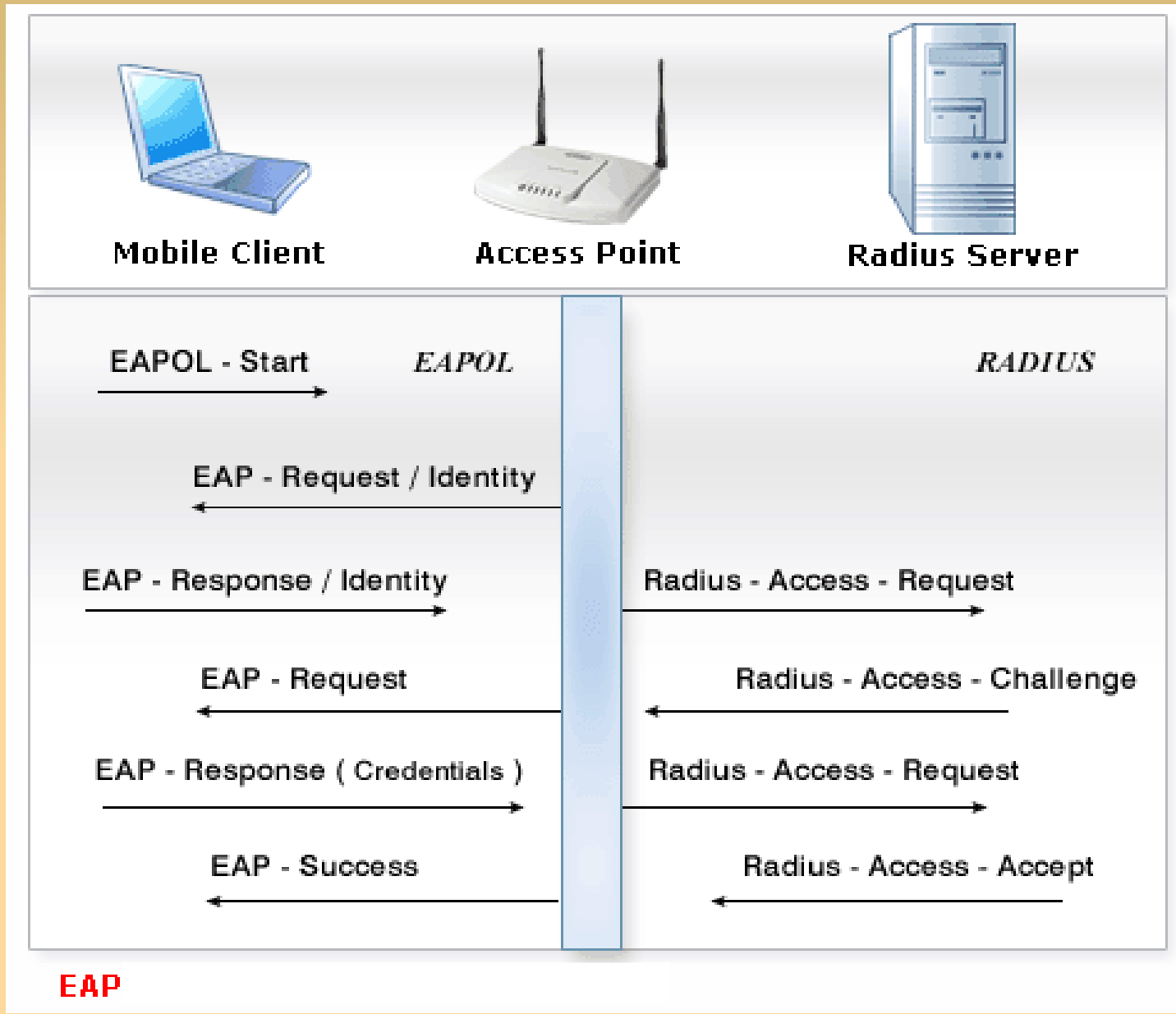
- **Phase 1: Négociation de la politique de sécurité**
  - **circule dans les *beacon frames***
- **Phase 2: Authentification 802.1x**
  - **La *Master Key* (MK) est choisie**
    - **dérivation de la PMK (PairWise Master Key)**
- **Phase 3: Echange de clés**
  - **La MK est envoyée du serveur AAA à l'AP**
  - **Quadruple poignée de main (4-Way Handshake) entre AP et client**
    - **Durant cette phase, génération de la PTK (PairWise Transient Key) et de la GTK (Group Transient Key)**
  - **La GTK est envoyée au client par l'AP**



EAP: L'implémentation de 802.1x aux WLAN

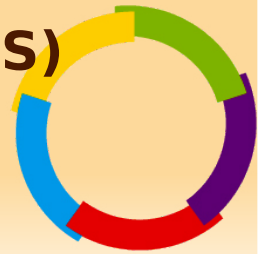
- 802.1x permet de contrôler l'accès au réseau pour tout réseau 802 (lan,wlan)
- EAP *(Extensible Authentication Protocol)*
  - pas un protocole d'authentification
  - protocole de transport de l'authentification
  - basé sur des protocoles de haut niveau (radius, couche 7)
    - Vérification de couples login/mot de passe, gestion de certificat X503, supports des cartes à puce (côté client), interface avec des annuaires...

EAP


Mobile Client
Access Point
Radius Server
EAPOL - Start
EAPOL
RADIUS
EAP - Request / Identity
EAP - Response / Identity
Radius - Access - Request
EAP - Request
Radius - Access - Challenge
EAP - Response (Credentials)
Radius - Access - Request
EAP - Success
Radius - Access - Accept
EAP

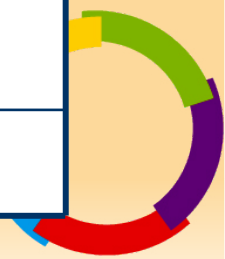
Les implémentations d'EAP

- **LEAP**
  - **Développé par Cisco**
  - **challenge/response basé sur Radius+login/mdp**
- **PEAP**
  - **Popularisé par Microsoft (~MSCHAPv2)**
  - **Utilisation d'un certificat serveur + login/pwd coté client**
- **EAP/TTLS**
  - **Version ouverte de PEAP**
  - **ne se base pas forcément sur MSCHAPv2**
- **EAP/TLS**
  - **Echange de certificats mutuels clients-serveurs**
- **EAP/SIM**
  - **authentification par carte SIM (opérateurs GSM/GPRS)**

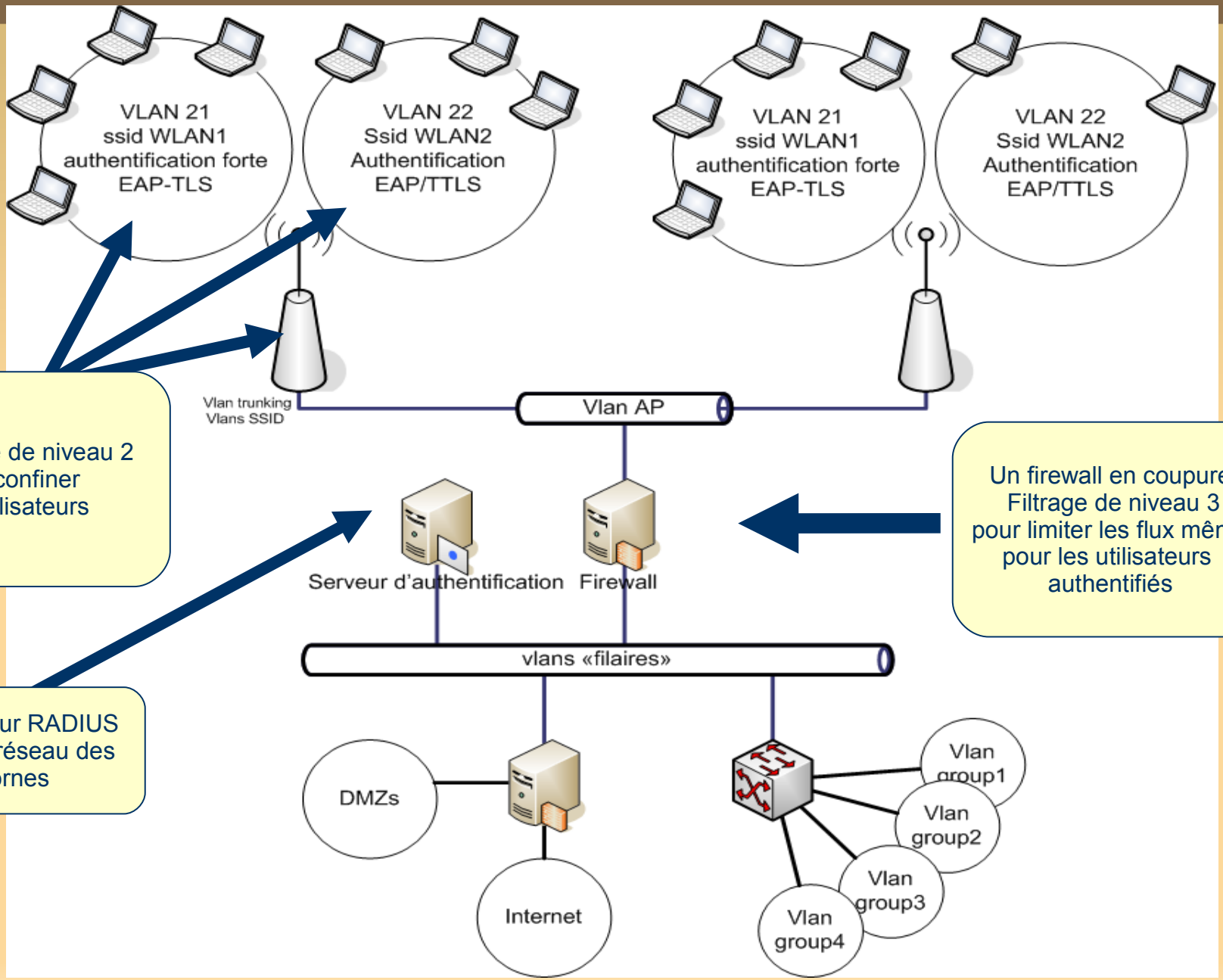


Récapitulatif: Les solutions de chiffrement

	WEP	TKIP	CCMP
chiffrement	RC4	RC4	AES
taille de clé	40/104	128 (chiff.) 64 (auth.)	128
taille IV	24	48	48
clé par paquet	Non (seul l'IV fait varier la suite chiffrante)	oui	pas nécessaire
intégrité de l'entête du paquet	non	SA+DA (MIC)	CCM
intégrité des données du paquet	CRC32	MIC	CCM
Détection du rejeu	Non	Sequencement des IV obligatoire (rejeu imp.)	Sequencement des IV obligatoire (rejeu imp.)
Gestion de clés	Aucune	802.1x	802.1x



La sécurité WLAN: Approche L2

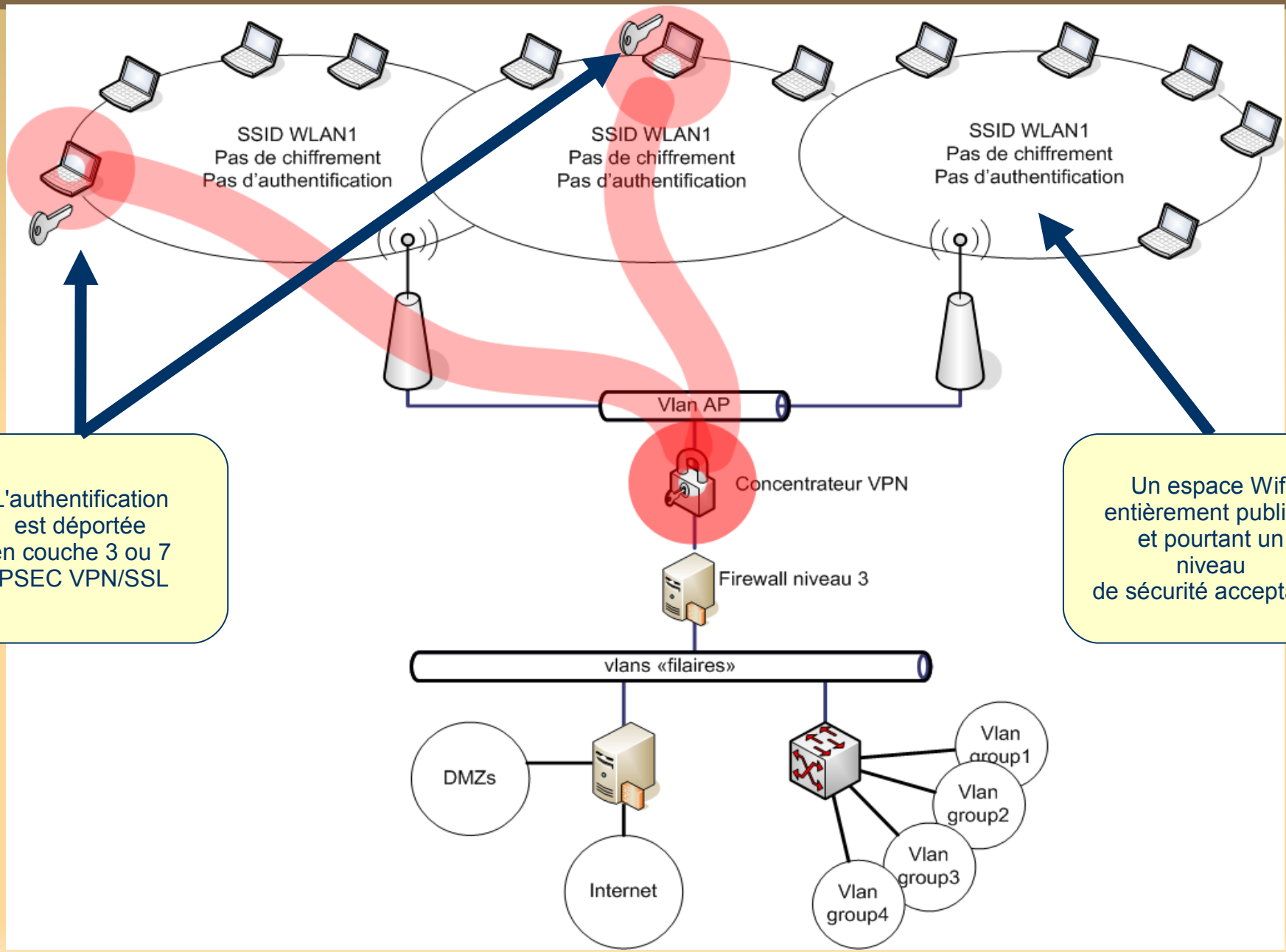


Un filtrage de niveau 2 pour confiner les utilisateurs

Un firewall en coupure Filtrage de niveau 3 pour limiter les flux même pour les utilisateurs authentifiés

Le serveur RADIUS Isolé du réseau des bornes

La sécurité WLAN: Approche L3



L'authentification est déportée en couche 3 ou 7 IPSEC VPN/SSL

Un espace Wifi entièrement public... et pourtant un niveau de sécurité acceptable

Quelle réponse "sécurité" pour les réseaux WLAN?

- **Sécurisation L2**
  - **on met en place toute la norme 802.11i, et on "blinde" en couche 2**
    - **Avantages**
      - **transparent pour les couches 3 à 7**
      - **supporté nativement sur les OS clients**
    - **Inconvénients**
      - **très contraignant**
      - **technologie jeune**
- **Sécurisation L3**
  - **On considère le nuage WLAN comme un réseau public.**
  - **On remonte la problématique de la sécurité sur la couche 3 (IPSEC)...voire 7 (VPN-SSL)**
    - **Avantages**
      - **Technologie robuste, maitrisée**
      - **"instanciable" sur les réseaux LAN ou WLAN**
    - **Inconvénients**
      - **boitiers VPN en coupure entre les AP et le réseau LAN privé filaire**
      - **lourd à déployer côté client (VPN L3)**
      - **On expose son réseau WLAN à l'extérieur des parefeux**
      - **On expose les clients aux attaques de couche 2 (arp cache poisoning)**
      -

Réseaux sans-fils: conclusion...provisoire

- **Les réseaux WiFi, ce n'est pas la panacée**
  - **aucune solution totalement satisfaisante**
    - **trop contraignante...ou trop laxiste.**
    - **Par la nature du support physique utilisé, reste très exposé aux dénis de services...**
      - **Brouillage radio!**
- **Politique de sécurité**
  - **Commencer par là...**
- **Sécuriser les points d'accès**
  - **A minima WPA-PSK pour une utilisation personnelle, WPA2 + EAP pour une utilisation industrielle.**
  - **Pas de diffusion du SSID**
  - **Ajouter un filtrage MAC pour éviter certains dénis de services**
- **Le sans fil est inéluctable!**
  - **Interdire sous prétexte d'insécurité est la pire des politiques**