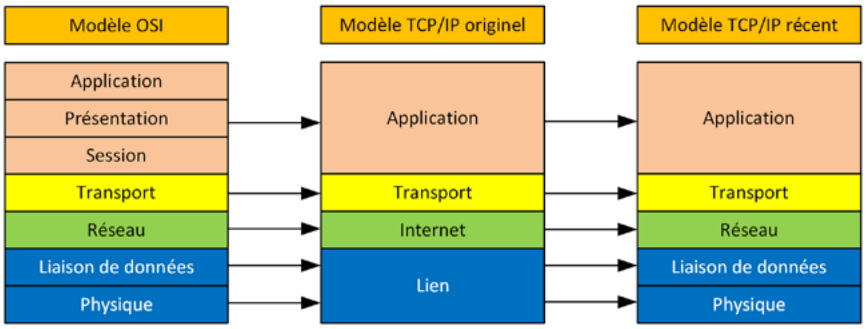
# Modèles OSI et TCP/IP

### Les fondamentaux

- Un réseau est l'ensemble des composants utilisés pour faire communiquer deux ou plusieurs ordinateurs.
- Le média de communication est utilisé pour transmettre les données de A vers B et inversement.
- Les premiers réseaux étaient propriétaires et utilisaient des protocoles propriétaires comme SNA d'IBM ou DECnet.
- À la fin des années 1990, la plupart des réseaux utilisaient le modèle TCP/IP pour communiquer, qui est une suite de protocoles libres et standards.




Points importants à retenir :

**Interaction couche similaire** : Deux équipements utilisent les mêmes règles pour échanger des données. Exemple : les routeurs utilisent des protocoles de couche 3 pour échanger leur table de routage.

**Interaction couche adjacente** : Au sein d'un équipement, le protocole d'une couche récupère la donnée de la couche supérieure (ou inférieure) puis ajoute (ou supprime) l'entête définissant ses propriétés de protocole.

Se souvenir des 5 étapes pour envoyer des données sur un réseau TCP/IP : 1/données - 2/entête TCP - 3/entête IP - 4/entête Ethernet - 5/envoi des bits.

La modélisation d'un réseau par couche a les avantages suivants : Moins complexe, interface standard, facile à comprendre, facile à développer, interopérabilité et ingénierie modulaire.

Connaitre les bases du routage IP et les modèles OSI et TCP/IP

Le modèle **Open Systems Interconnection** (**OSI**) a été défini dans les années 90 comme la première suite de protocoles de communication réseau. Il a été développé par l'**International Organization for Standardization** (**ISO**). Attention à ne pas mélanger OSI et ISO...

Le département USA de la défense a créé son propre modèle, aujourd'hui appelé **TCP/IP**. Très similaire au modèle OSI, il consolide les 3 couches hautes en une seule couche appelée "**Application**". Les deux modèles restent identiques pour les 4 couches basses. Une version originelle de TCP/IP agrégeait les 2 couches basses en une seule.

Bien que les équipements d'aujourd'hui n'utilisent pas le modèle OSI, celui-ci reste la référence.

| Couche TCP/IP | Exemple de protocoles |
|---|---|
| Application | HTTP, HTTPS, POP3, SNMP |
| Transport | TCP/UDP |
| Internet | IP, RIP, OSPF, EIGRP, BGP |
| Liaison de données | Ethernet, PPP, HDLC, Wireless |
| Physique | 802.3, 802.11, E1, STM1 |

| Ports connus | |
|---|---|
| HTTP | 80 |
| HTTPS | 443 |
| SSH | 22 |
| FTP | 21 |
| Telnet | 23 |

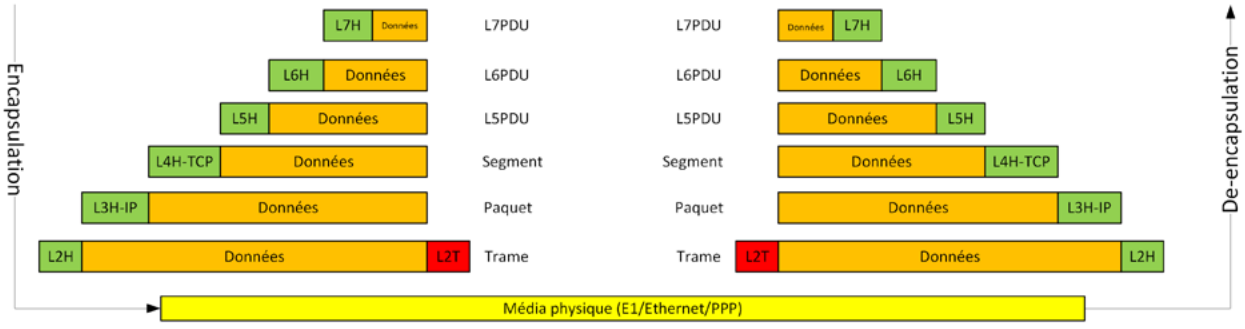
# L'encapsulation TCP/IP

Alice veut envoyer à Bob une requête HTTP GET. Quand Bob reçoit la requête HTTP GET, il répond avec un HTTP OK.

Cet exemple illustre comment la donnée est encapsulée, transmise puis décapsulée

Alice (1.1.1.1)

Bob (2.2.2.2)




Encapsulation de la donnée

Vu que l'application source ne peut pas communiquer directement avec l'application destination, la pile de protocole permet à la donnée d'être transmise de la source à la destination. Chaque donnée et entête est appelée **Protocol Data Unit** ou **PDU**. Le PDU passe chaque couche en ajoutant l'entête de la couche traversée et ainsi de suite...

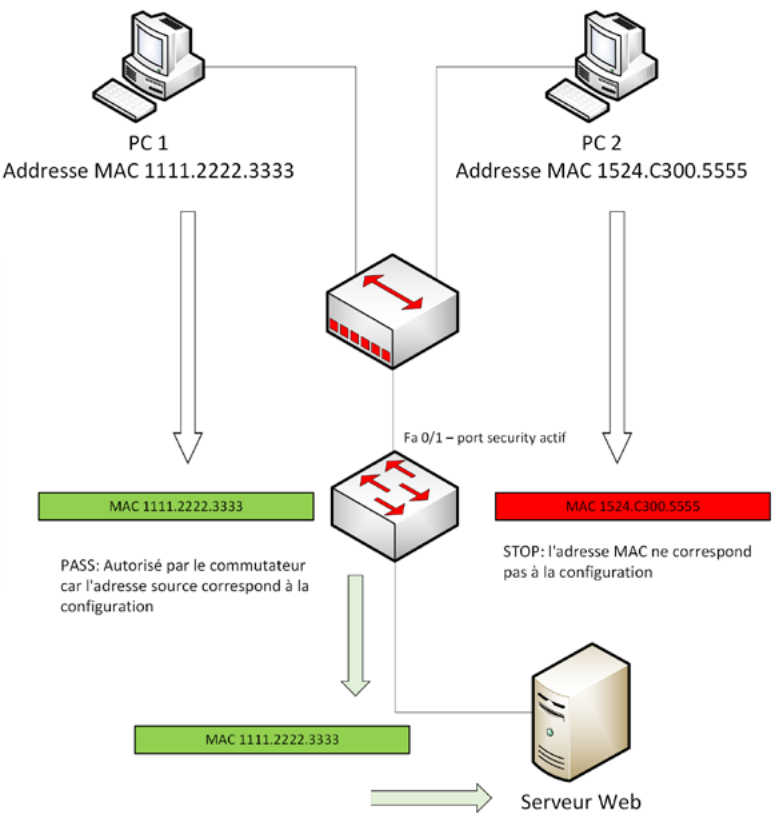
**Point important** :
- Le PDU de la couche 4 est appelé "**Segment**"
- Le PDU de la couche 3 est appelé "**Paquet**" (**Packet** en anglais)
- Le PDU de la couche 2 est appelé "**Trame**" (**Frame** en anglais)

Points importants : Étapes de l'encapsulation

1. Crée et encapsule la donnée de l'application avec l'entête de la couche **Application**.
2. Encapsule l'ensemble reçu avec l'entête de la couche **Transport**.
3. Encapsule l'ensemble reçu avec l'entête de la couche **Réseau** (IP). Cela crée un **paquet IP**.
4. Encapsule l'ensemble reçu avec l'entête de la couche **Liaison de données**. Cela crée une **trame**.
5. Envoi la trame (succession de bits 0 et 1) sur le média physique.

# Configuration des interfaces de commutation

| Options de commande de violation du port-security | Protect | Restrict | Shutdown |
|---|---|---|---|
| Infraction au trafic rejeté | oui | oui | oui |
| Envoyer une trap SMNP et un log | non | oui | oui |
| Compteur de violations augmente pour chaque trame de violation | non | oui | oui |
| Mettre l'interface en état err-disabled et jetez tout le trafic | non | non | oui |



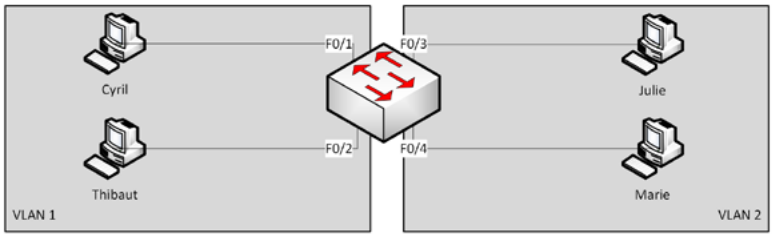

**Configuration de la sécurité des ports**

- Étape 1: Configurez l'interface comme un port d'accès (**switchport mode access**) ou Trunk (**switchport mode trunk**).
- Étape 2: Activer la sécurité du port via le commande **switchport port-security**
- Étape 3: (facultatif) Définissez le nombre d'adresses MAC autorisées à l'aide de la commande **switchport port-security maximum *number***
- Étape 4: (facultatif) Remplace l'action par défaut (shutdown) en cas de violation de sécurité: **switchport {protect | restrict | shutdown}**
- Étape 5: (facultatif) Définissez les adresses MAC source via la commande **switchport-security mac-address *mac-address***
- Étape 6: (facultatif) Configurez le commutateur à apprendre automatiquement les adresses MAC entrantes via la commande **port-security mac-address sticky**

**Configuration d'adresses MAC statiques**

```
Switch # configure terminal
Switch(config) # interface FastEthernet 0/1
Switch(Config-if) # switchport mode access
Switch(Config-if) # switchport port-security
Switch(Config-if) # switchport port-security mac-address 1111.2222.3333
Switch(Config-if) # switchport port-security mac-address 4444.5555.6666
Switch(Config-if) # exit
```

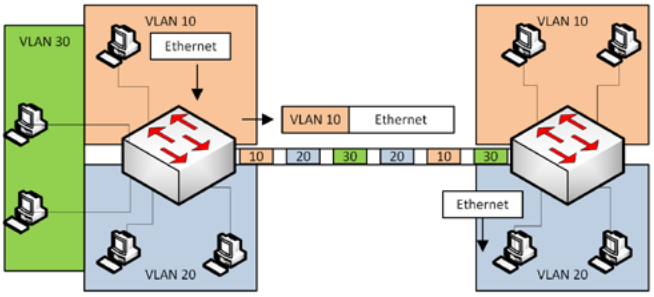
# Implémentation de réseaux virtuels Ethernet



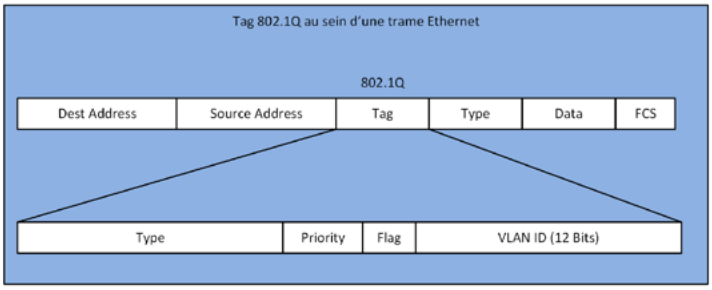

Création de deux domaines de diffusion avec un commutateur et deux VLAN

Objectifs du VLAN:

- Réduire le nombre d'équipements qui reçoivent les trames de diffusion
- Réduire le risque de sécurité en diminuant le nombre de trames que chaque équipement reçoit
- Améliorer la sécurité de certains équipements en les isolants dans un VLAN distinct
- Créer des designs plus flexibles basés sur des groupes, des départements ou autres besoins métiers
- Résoudre les problèmes plus rapidement car chaque domaine de diffusion est séparé
- Réduire le temps de calcul du protocole Spanning-Tree en limitant un VLAN à un seul commutateur d'accès




3 VLAN Trunking entre deux commutateurs

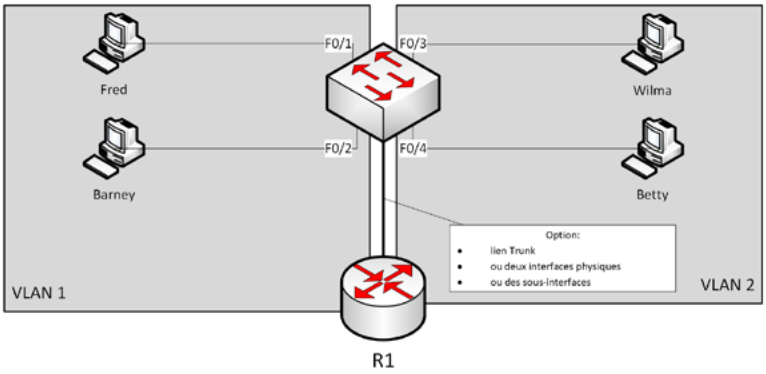



Notions importantes à savoir sur les VLANs:

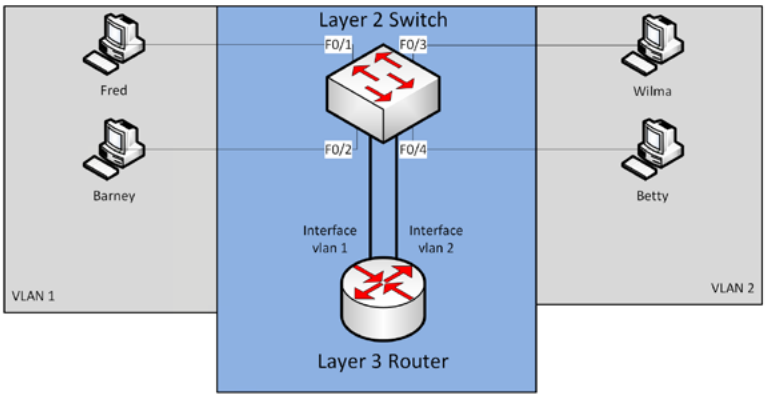
les commutateurs Cisco peuvent utiliser les VLAN 1 à 4094. Cette plage est divisée en deux sous-plages. Les VLAN 1 à 1005 sont présents sur les commutateurs anciens. Les récents commutateurs peuvent utiliser la plage d'origine et la plage qui contient les VLAN 1006 à 4094.

VLAN natif: ce VLAN, également appelé VLAN non taggé, se compose de paquets Ethernet sans tag 802.1q (étiquette) envoyés sur un réseau Ethernet. S'il y a un périphérique à l'autre extrémité qui ne comprend pas le Trunk, le commutateur peut prendre ce trafic non taggé et le placer sur le VLAN Natif.
La modification du VLAN natif sur un port ou un Trunk peut être utilisée comme mesure de sécurité ou lorsqu'un périphérique tel qu'un téléphone VoIP Cisco utilise le trafic taggé pour le trafic voix et non taggé pour les données.


# Implémentation de réseaux virtuels Ethernet


Routage entre deux VLans sur un commutateur




Routage entre deux vlans sur un commutateur de couche 3 (symbolisé par le carre bleu)

Note: 1 VLAN = 1 IP Subnet

Création de VLAN et attribution d'interfaces:

Étape 1: à partir du mode de configuration, utilisez la commande **vlan vlan-id** pour créer le VLAN. Utilisez la sous-commande **name NOM** pour nommer le VLAN (par exemple, **name *Finance***)
Étape 2: pour chaque interface qui rejoindra le vlan, utiliser la commande **switchport access vlan vlan-id** et définissez le port en mode accès avec la commande **switchport mode access**.

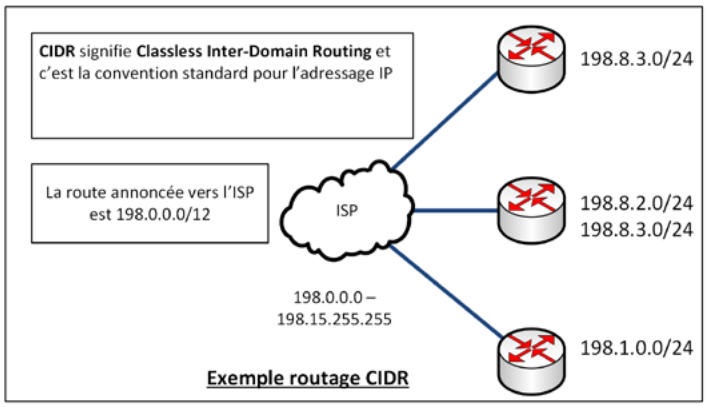
```
Switch# configure terminal
Switch(config)# vlan 2
Switch(config-vlan)# name SALES
Switch(config-vlan)# exit
Switch(config)# interface FastEthernet 0/3
Switch(config-if)# switchport access vlan 2
Switch(config-if)# switchport mode access
Switch(config-if)# exit
Switch(config)# exit
Switch# show vlan

VLAN Name                              Status    Ports
1    SALES                             active    Fa0/3

Switch#
```

Remarque: au lieu d'utiliser un routeur physique et un switch pour effectuer du routage entre VLAN, on peut utiliser des nouveaux commutateurs qui intègrent les fonctionnalités Layer-2 et Layer-3. Ces commutateurs sont appelés commutateurs multicouches et permettent à l'ingénieur réseau d'avoir une commutation Layer-2 et un routage Layer-3 dans la même boîte physique.

# Network Address Translation (NAT)

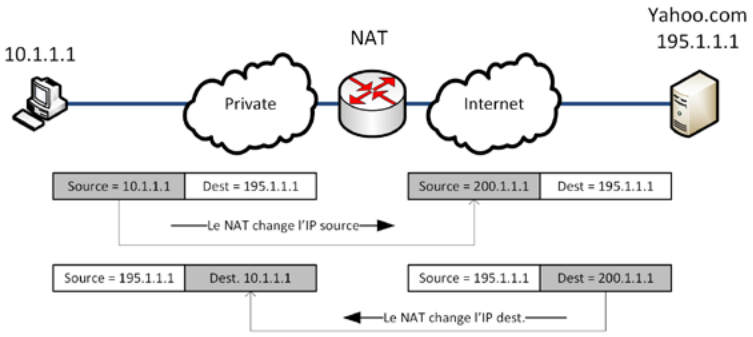



**RFC 1918 – adressage IP prive**

| Plage d'adresses IP | Classe | Networks |
|---|---|---|
| 10.0.0.0 – 10.255.255.255 | A | 1 |
| 172.16.0.0 – 172.31.255.255 | B | 16 |
| 192.168.0.0 – 192.168.255.255 | C | 256 |

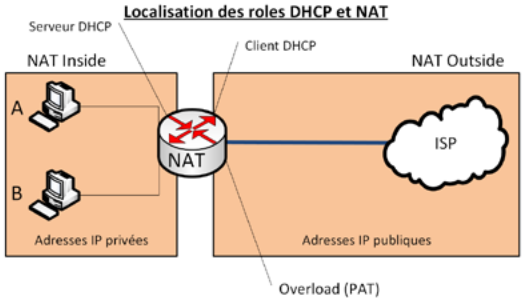
**Terminologie NAT**

| Terme | Signification |
|---|---|
| Inside local | Inside signifie le réseau interne à l'entreprise. Ce sont donc les adresses IP attribuées aux Hosts, qui sont des adresses IP privées. |
| Inside Global | Cette adresse IP est la nouvelle adresse IP NATée du Host pour aller sur Internet. Le routeur change l'adresse Inside Local par cette adresse Inside Global. C'est généralement une adresse IP publique. |
| Outside Global | Cette adresse réside dans la partie extérieur du réseau. Elle représente donc l'adresse IP de destination que le Host interne souhaite joindre. |
| Outside Local | Cette adresse est l'adresse externe du Host de destination. Généralement, elle est identique a l'adresse Outside Global. |

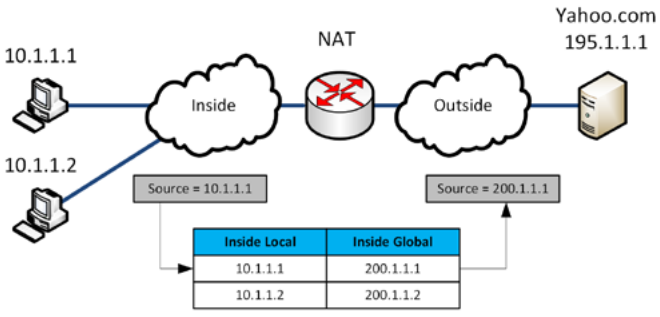



**Le NAT permet l'utilisation de l'adressage privée pour communiquer sur Internet**

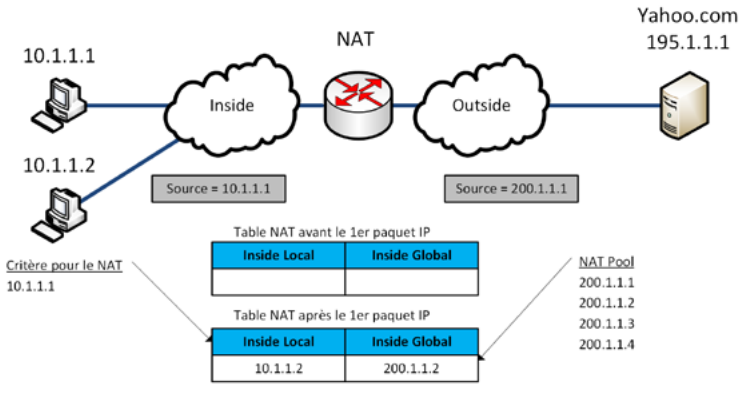
**Localisation des roles DHCP et NAT**



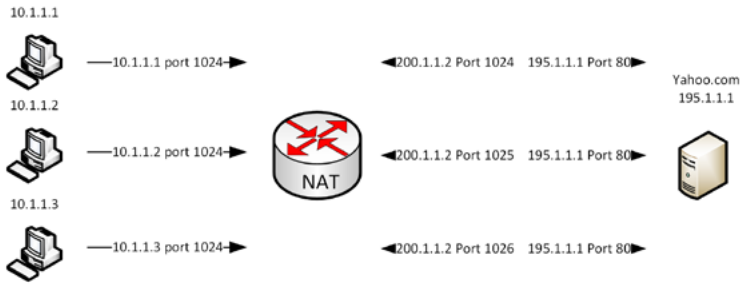

# Network Address Translation (NAT)




**Terminologie NAT statique**




**Terminologie NAT dynamique**




| Inside Local | Inside Global |
|---|---|
| 10.1.1.1: 1024 | 200.1.1.2: 1024 |
| 10.1.1.2: 1024 | 200.1.1.2: 1025 |
| 10.1.1.3: 1024 | 200.1.1.2: 1026 |

**Table de NAT dynamique avec Overloading**

**NAT Overload (PAT)**

**Exemple de translation de NAT statique**

NAT# **show ip nat translations**

| Pro | Inside global | Inside Local | Outside Local | Outside Global |
|---|---|---|---|---|
| --- | 200.1.1.1 | 10.1.1.1 | --- | --- |
| --- | 200.1.1.2 | 10.1.1.2 | --- | --- |

**Exemple de translation de NAT Overload (ou PAT)**

NAT# **show ip nat translations**

| Pro | Inside global | Inside Local | Outside Local | Outside Global |
|---|---|---|---|---|
| --- | 200.1.1.2:1024 | 10.1.1.1:1024 | 195.1.1.1:80 | 195.1.1.1:80 |
| --- | 200.1.1.2:1025 | 10.1.1.2:1024 | 195.1.1.1:80 | 195.1.1.1:80 |
| --- | 200.1.1.2:1026 | 10.1.1.3:1024 | 195.1.1.1:80 | 195.1.1.1:80 |