Corellis

Applications & Innovations TIC

Sécurité des Systèmes d'Information

Corellis

RESEAUX IP ET ADMINISTRATION RESEAUX SOUS IOS CISCO

Patrick Girard
patrick.girard@corellis.eu

Instructeur Certifié depuis Octobre 2001 – Glasgow LTS - **CCAI** (CCNA: CSCO10362533) – Copenhague 2001
CCNP 1 (**BSCI**) 7/2004; CCNP2 (**ISCWN**) 10/2009; CCNP 3 (**BCMSN**) 8/2005; CCNP4 (TSHOOT) 12/2010 – Birmingham UCE
Network Security I (**NS1**) 2/2006 – Birmingham UCE
Network Security II (**NS2**) 7/2006 - Glasgow LTS
Cisco Airespace Wireless (**CAIAM**) 3/2006 – Nice/Maidenhead/Amsterdam – Daclem
ACSE OmniSwitch R6 – 11/2006 - Brest Alcatel University

Le modèle OSI - 1/5

Open **S**ystem **I**nterconnection reference model

- Conçu par l'ISO en 1984
- Objet : créer un cadre conceptuel à la problématique d'interconnexion des réseaux
- But : favoriser l'évolution technologique en assurant l'interopérabilité sans nuire à la vitalité des acteurs
- Le moyen :
  - Différencier 7 couches indépendantes
  - Normaliser pour chaque couche l'interface avec la couche supérieure et la couche inférieure

Le modèle OSI - 2/5

- Il permet de sérier les problématiques de communication sur le réseau en éléments plus petits et plus simples;
- Il uniformise les éléments du réseau afin de faciliter le développement et le soutien multi constructeur;
- Il permet à différents types de matériel et de logiciel réseau de communiquer entre eux;
- Il empêche les changements apportés à une

Le modèle OSI - 3/5

7	Application Clients, Serveurs	Accès au service	Telnet, SMTP, SNMP, NFS, TFTP, HTTP, FTP, SSH, SMB	
6	Présentation Clients, Serveurs	Conversion de format, codage, cryptage …	ASCII, EBCDIC, jpeg, aiff, mpeg, Flash, mp3, SMB	
5	Session Clients, Serveurs	Gestion sessions, synchro., efficacité, sécurité (S, Hd, Fd)	X-Window System, RPC, Appletalk Session Protocol, NFS, SQL, NetBios	
4	Transport Clients, Serveurs	Orienté connexion, contrôle de flux & fiabilité	Segments Ports	Spx, NetBEUI TCP
3	Réseau Routeurs	Adressage, Routage, Commutation, Best Effort Del.	Paquets Adresses logiques	IP, IPX, NetBEUI
2	Liaison NIC, Pont, Switch	Gest. transmission, fiabilité, contrôle de flux, topologie rés	Trames Adresses physiques	LLC, MAC, CSMA/CD
1	Physique Répéteurs, Hubs, …	Transmission bit à bit, spécification physique du lien	01101011011101	Standards EIA/TIA…

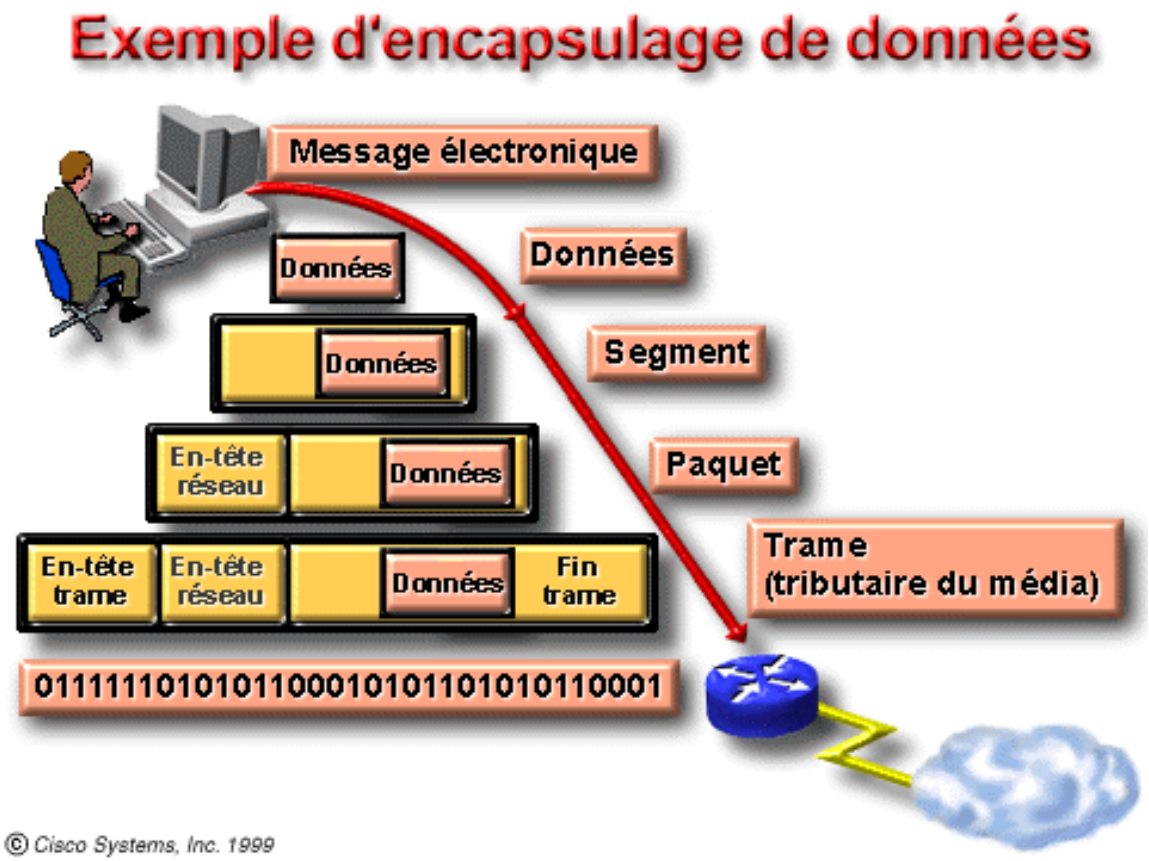
Le modèle OSI - 4/5

Communication d'égal à égal

7	Application	⟷	7	Application
6	Présentation	⟷	6	Présentation
5	Session	⟷	5	Session
4	Transport	⟷	4	Transport
3	Réseau	⟷	3	Réseau
2	Liaison	⟷	2	Liaison
1	Physique	⟷	1	Physique

Le modèle OSI - 5/5

Services de couches et datagrammes



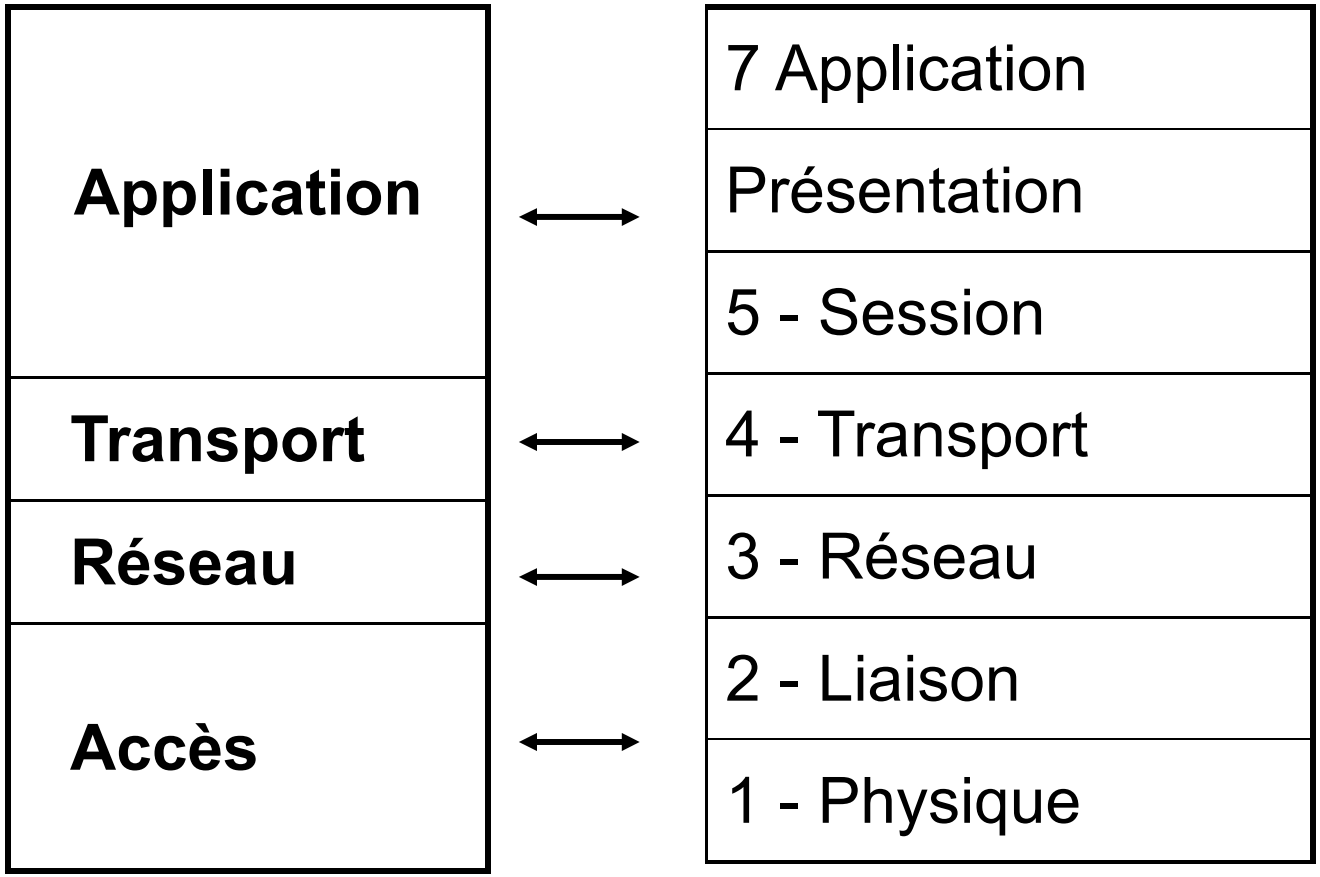
Le modèle TCP / IP – 1/2

Différences entre le modèle TCP / IP et OSI

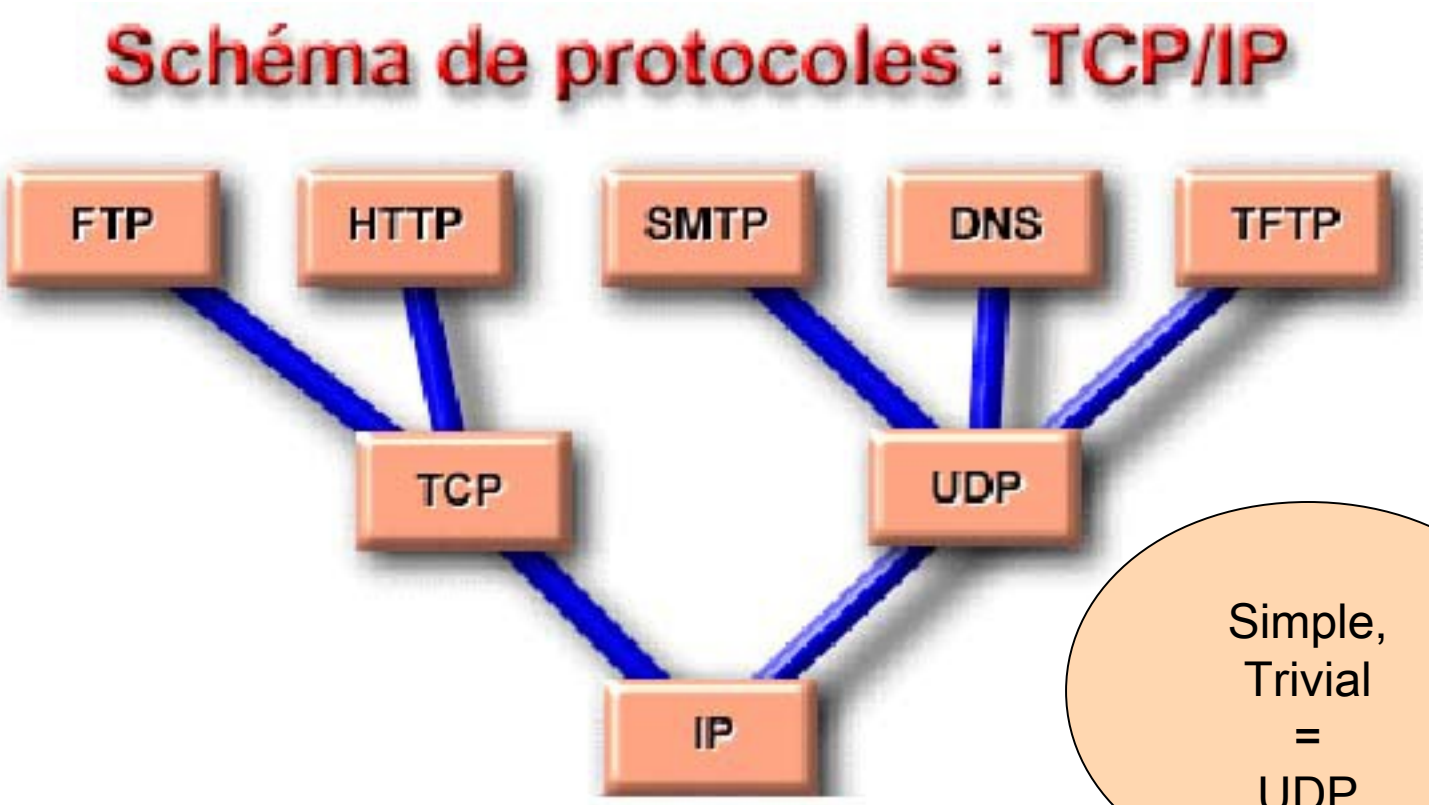
Intègre OSI 5, 6 & 7

Propose en plus un transport de service non fiable UDP

Intègre OSI 1 & 2



Le modèle TCP / IP – 2/2



Simple,
Trivial
=
UDP

La Couche Physique

- **Objet** :
  Transporter un signal entre un émetteur et un récepteur

- Moyens :
  - Choix d'un média
  - Choix d'une architecture
  - Arbitrage Coût / Fiabilité
  - Arbitrage Coût / Capacité de Transmission
  - ...

Quelques notions et acronymes…

- POP : Point of Presence
- MDF : Main distribution facility = RG ou RP
- IDF : Intermediate dist. fac. = SR ou RS
- VCC : Vertical Cross Connect (câblage vertical)
- HCC : Horizontal Cross Connect (câblage hor.)

Topologies & matériels

Topologies

- Topologie en Anneau
- Topologie en Etoile et en Etoile étendue

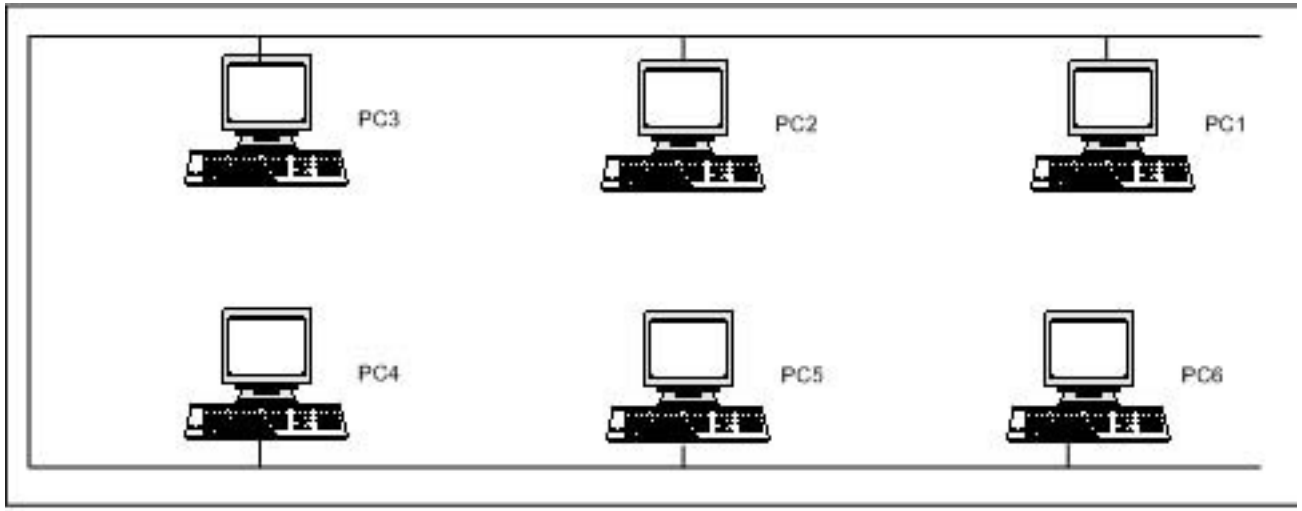
Matériels

- Câbles
- Cartes réseaux
- Répéteurs
- Répéteurs multi ports, concentrateurs, HUB

Topologie en anneau

Couche Physique

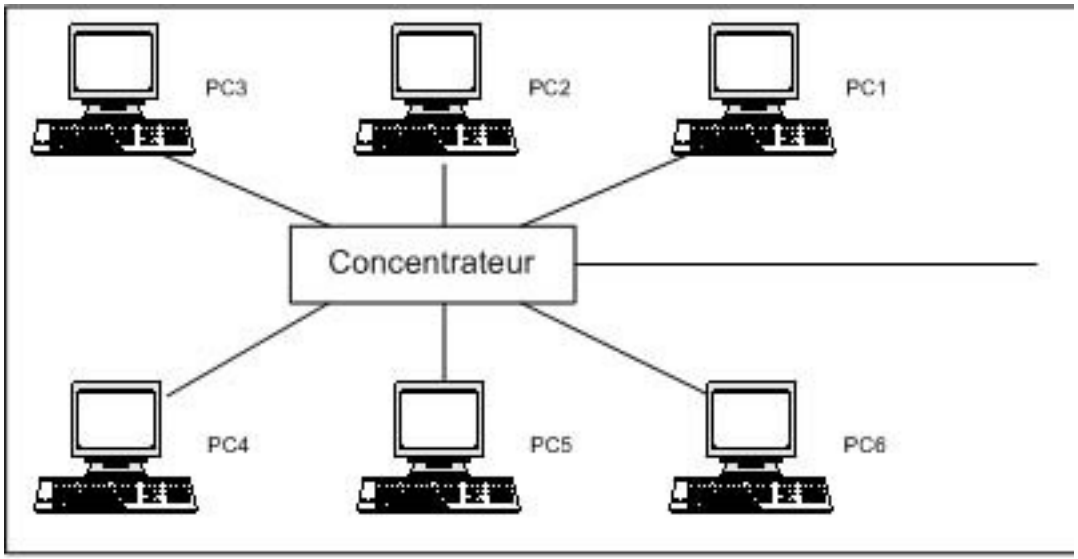
- Le signal parcoure le câble partagé en passant par PC1, PC2, … jusqu'à PC6 avant de retourner vers le reste du réseau.
- Chaque host est connecté au câble par un connecteur en T qui assure l'accès du host au média ET la continuité des signaux qui traversent le câble.
- Si le câble se coupe en un point, ou si un des connecteurs en T est défectueux, plus aucun trafic n'est possible pour tous les hosts.



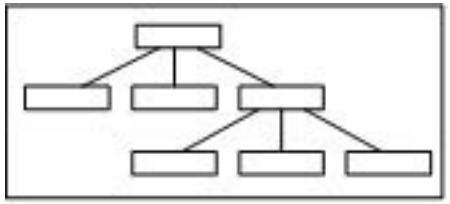
Topologie en étoile / étoile étendue

Couche Physique

- Chaque host est connecté à un appareil qui concentre la connectivité du réseau.
- Ce concentrateur permet aux hosts de partager le média.
- Une coupure de lien ou une défaillance d'un connecteur n'affecte plus qu'un seul host.
- Si le concentrateur connaît une défaillance, plus aucun trafic n'est possible..

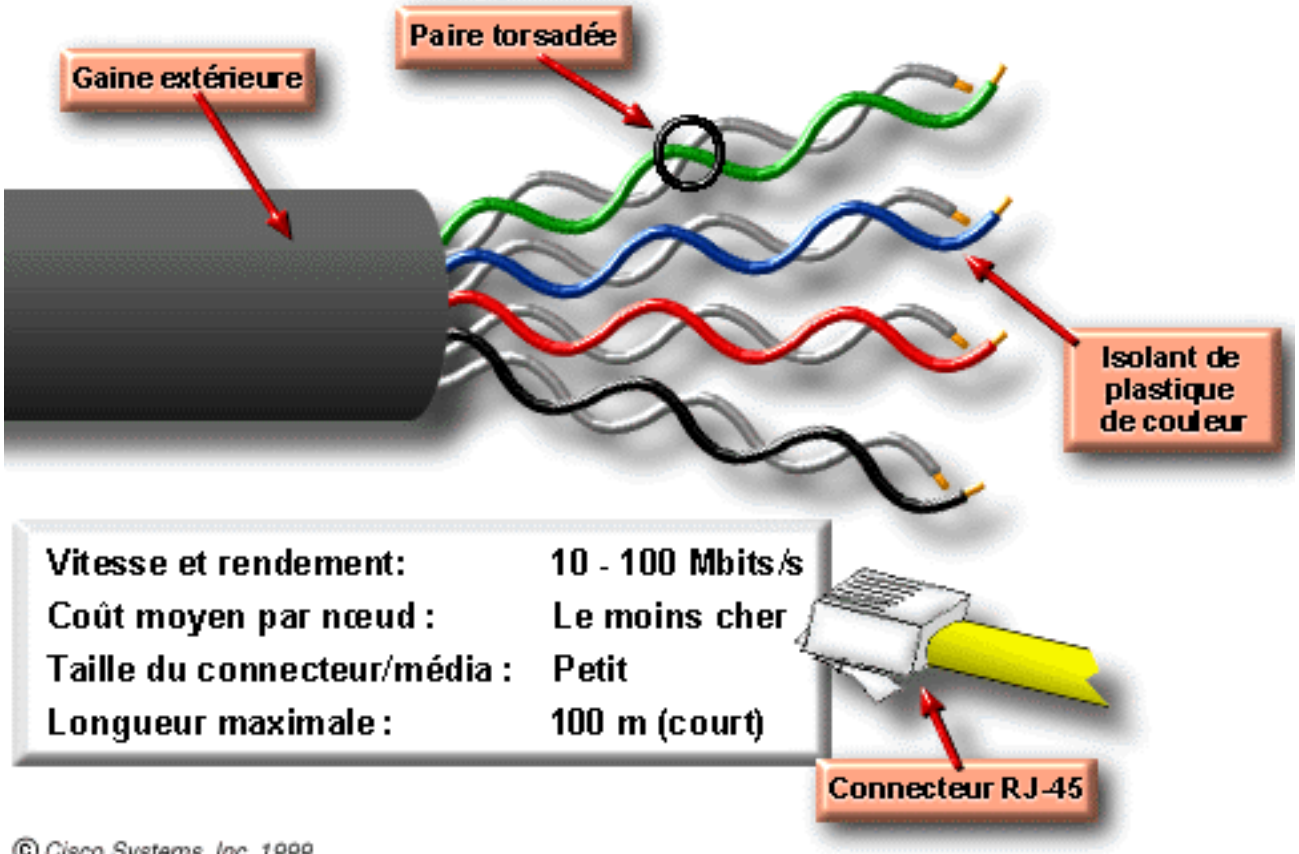


- Une topologie en étoile étendue est composée d'étoiles reliées entre elles.

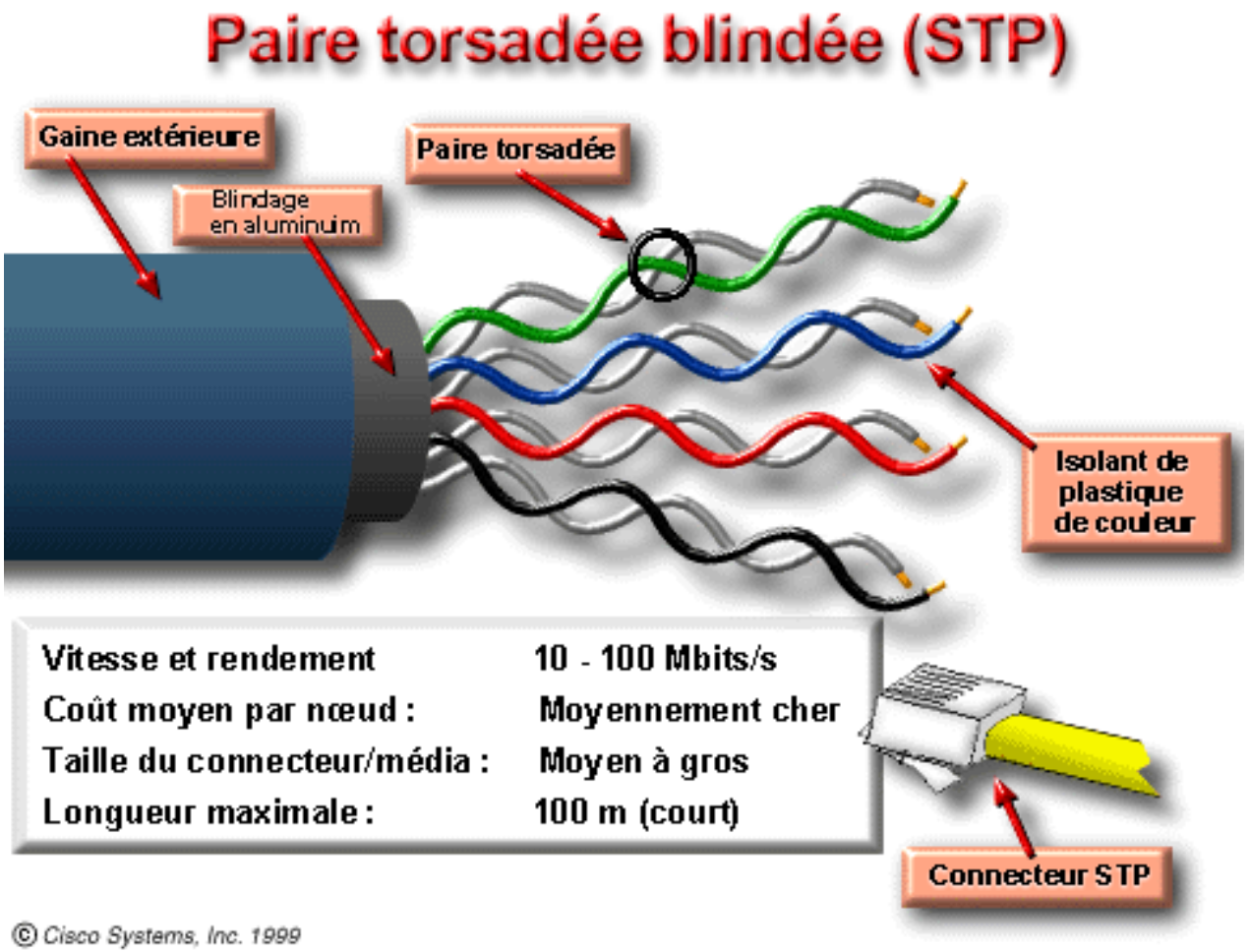


Les types de média - 1/3

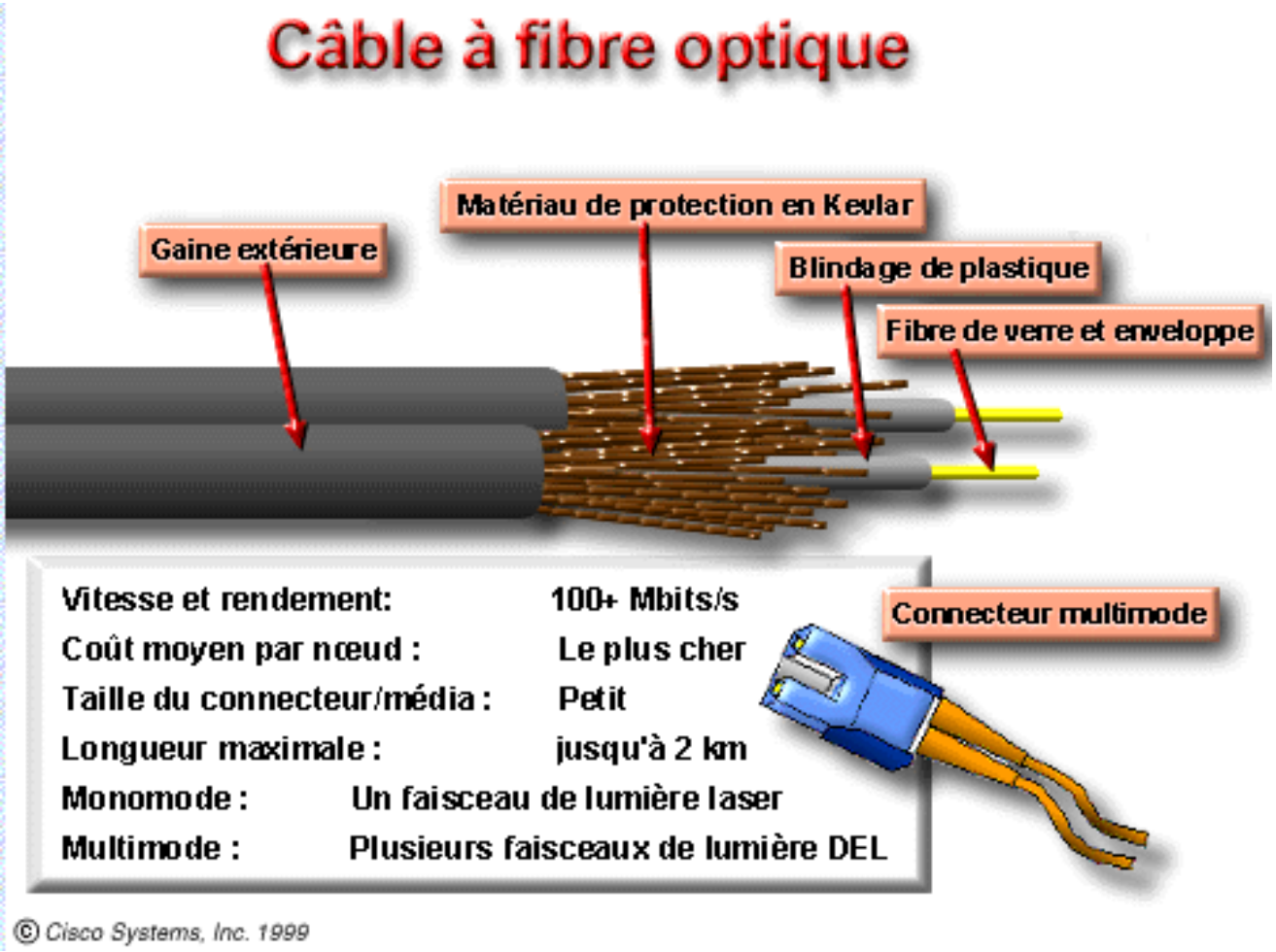
Paire torsadée non blindée (UTP)



Les types de média - 2/3

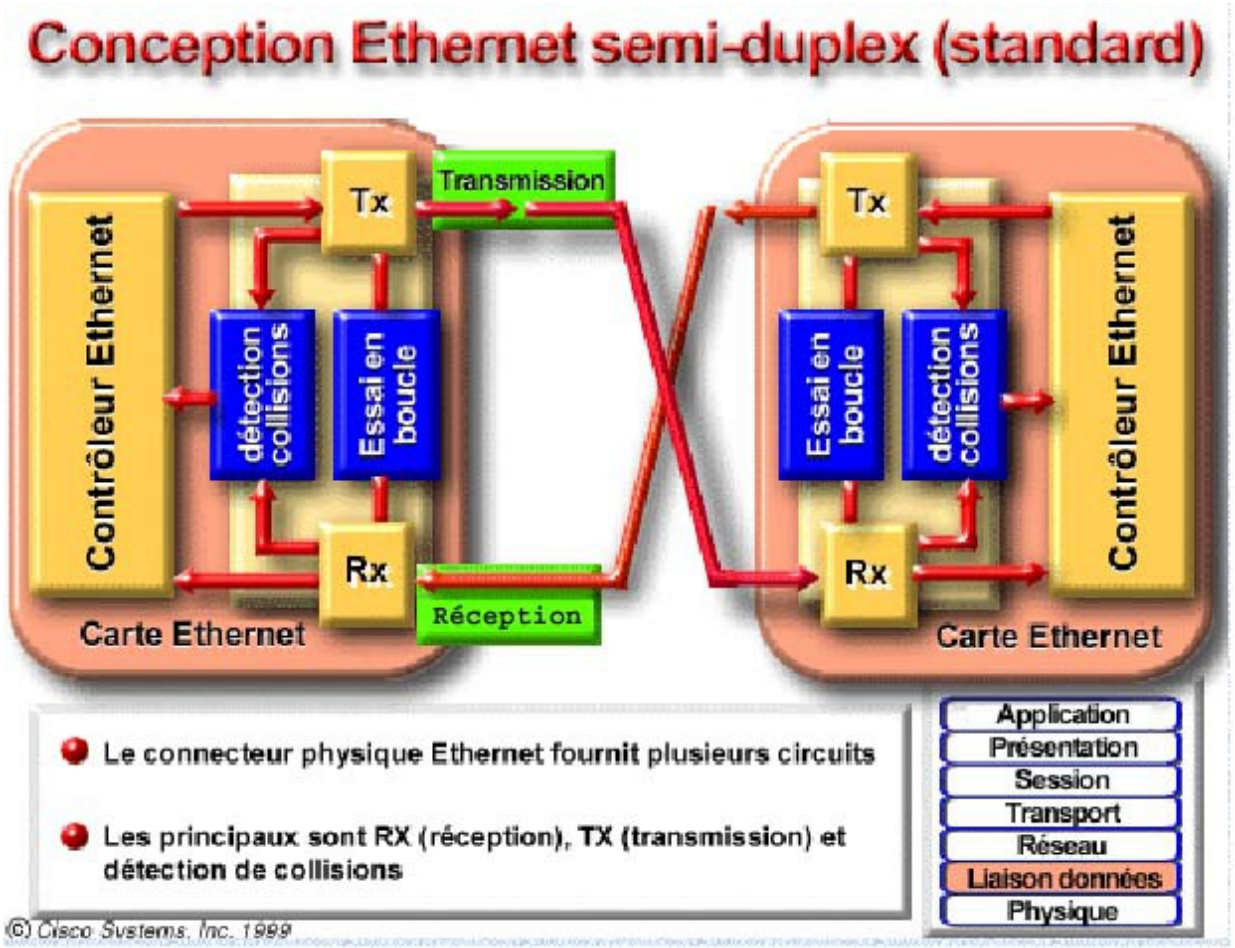


Les types de média - 3/3



Structure d'une carte NIC

- Les ports des Hubs et des Switchs croisent les circuits.
- Un câble droit relie les hosts à ces matériels.
- Pour relier deux hosts entre eux il faut un câble croisé.



Les malheurs d'un bit - 1/3

- Dispersion = étalement des impulsions dans le temps
  => problème de recouvrement de bits

  Solution : longueur/impédance, fréquences, longueur d'onde

- Gigue = désynchronisation des bits
  => problème d'ordonnancement

  Solution : synchronisation des horloges

- Latence = délais de transmission d'un bit
  Câble : 1,9 à 2,4 x 108 m/s / Hertzien 3 x 108 m/s / Fibre : 2 x 108 m/s
  + Latence des équipements du réseau

=> problème de saturation

Les malheurs d'un bit - 2/3

- Atténuation = perte de lisibilité du codage d'un bit

  Solution : distance de transmission, régénération du bit

- Réflexion = rebond et retour dans le média

  Solution : respect des normes !

- Bruit = interférence extérieures ou intérieures

  Ne peut survenir à un support optique

  Solution : respect des normes !, paire torsadée, fibre !

- COLLISION = accepter l'inévitable

Ethernet / Token Ring (digression)

Ethernet a été développé à l'origine par Xerox (1970), puis a été intégré aux travaux de l'OSI. La méthode d'accès au média (CSMA/CD) est définie dans la sous-couche MAC de OSI 2. Token Ring est une technologie déterministe arrivée trop tard sur le marché.

Ethernet est non déterministe
Token Ring est déterministe

Ethernet est simple
Token Ring est plus complexe

Le succès d'Ethernet le fait évoluer vers une technologie plus simple, plus rapide et déterministe !

L'évolution de Token Ring a conduit à une complexité de moins en moins gérable.

ALOHA !!!
a
préfiguré
Ethernet

Les malheurs d'un bit - 3/3

(délais répéteur + délais câble + délais NIC) x 2
< délai maximal entre deux hôtes

La norme prévoit une taille minimale de trame de 64 octets =>

délai maximal entre deux hôtes = (pour un débit de 10 Mb/s)

taille minimale trame * durée bit = 512 * 0.1 µs = 51,2 µs

Le délai de transmission se calcule par :

délais répéteur 2 µs (pour un débit de 10Mb/s)

délais câble 0,55 µs / 100 m

délais NIC 1 microseconde (pour un débit de 10Mb/s)

***Collision tardive* =**

collision après les 64 premiers octets de la trame

Collision tardive (digression)

1) La carte réseau émet une trame
Pendant l'émission des 64 premiers octets, si la carte réseau décèle une collision (JAM), elle arrête de transmettre…
puis réessaye de transmettre la **même** trame.

2) Si au bout de trois tentative, la trame n'a pas pu être transmise, sa transmission est abandonnée.
Ce sont alors les couches supérieures qui demanderont (éventuellement) sa réémission.

3) En cas de collision tardive, la trame réputée avoir été transmise n'est plus dans la file d'attente…. Elle sera (éventuellement) réémise à la demande des couches supérieures.

Dans ce cas, le délai passe de 100 µs à 2 à 3 secondes

Solutions : Répéteur & HUB

- Un répéteur régénère le signal électrique, ce qui permet d'étendre la longueur du brin Ethernet au-delà de la limite des 100 m.

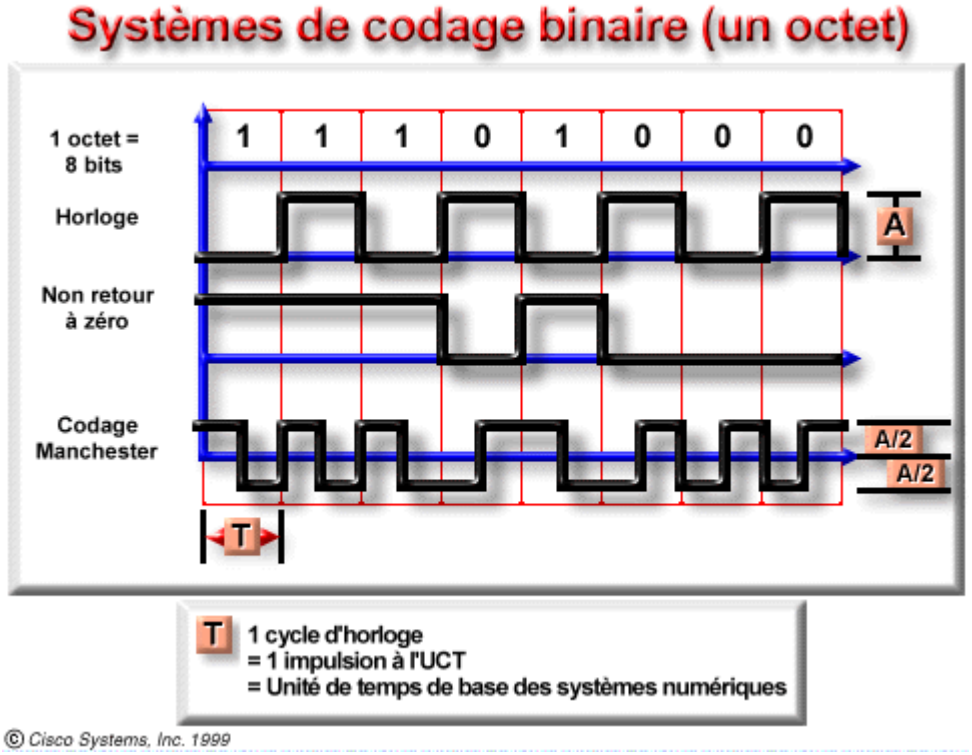
- Le HUB ou concentrateur Ethernet est un répéteur multi ports.
- Tout signal électrique entrant par un des ports est régénéré et envoyé sur tous les autres ports du HUB.
- Pour relier deux HUBS entre eux il faut un câble croisé.
- Certains HUB possèdent un « lien montant » ou UpLink qui permet de relier les HUBs par un câble droit.

Solutions : Codage

MANCHESTER

0 = transition de faible à élevé

1 = transition d'élevé à faible.



Puisque les 0 et les 1 se traduisent par une transition dans le signal, l'horloge peut être récupérée de manière efficace au niveau du récepteur.

Solutions- Normes

Couche Physique

Les normes TIA/EIA-568-A et TIA/EIA-569-A concernent

(Electronic Industries Alliance Telecommunications Industry Association)

- le câblage horizontal = média réseau de l'armoire de câblage à une zone de travail
  STP : 150 ohms à deux paires (CAT 5)

  UTP : 100 ohms à quatre paires (CAT 5)

  Fibre : deux fibres multimodes 62,5/125

  Mise à la terre et installation électrique : TIA/EIA-607

  Longueur des **câbles de raccordement** ou des cavaliers d'interconnexion **< 6 m**

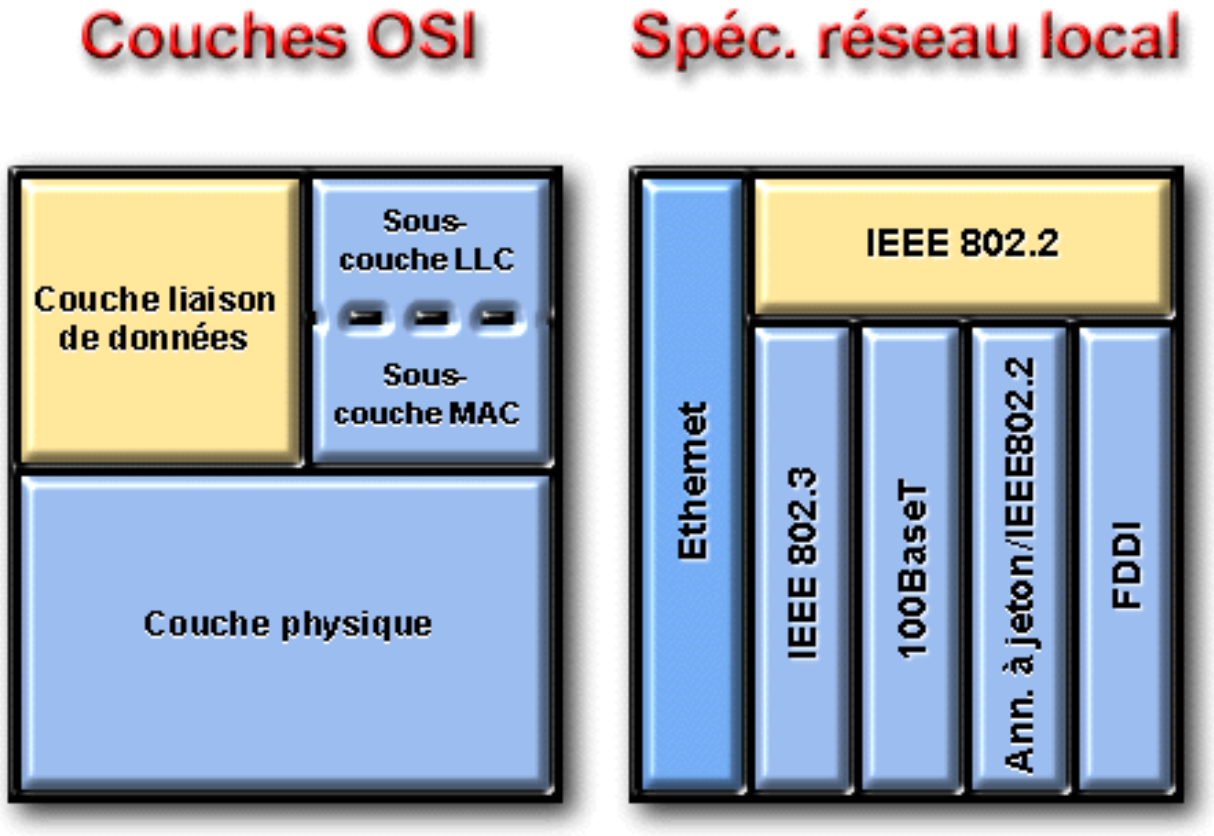
  Longueur du câble de raccordement en **zone de travail < 3 m**

  Longueur du **câblage horizontal** (ZdT, AdC) **< 90 m**
- … mais aussi : l'armoire de câblage, le câblage de backbone,

  les salles d'équipements, les zones de travail, les installations d'entrée (POP).

Solutions- Normes

Couches Physique & Liaison de Données



RFC, bureau IEEE… (digression)

- Une Request For Comment démarre le processus de normalisation
- Le bureau concerné accepte ou non la RFC et désigne éventuellement un sous-bureau

Exemple de Hiérarchie des protocoles

IEEE 802

IEEE 802.11 – Wireless Lan
- 802.11b
- 802.11g

IEEE 802.15 - Bluetooth

IEEE 802.2 - LLC

IEEE 802.3 – Ethernet
- 802.3 u - Fast Ethernet
- 802.3 x - Full Duplex

IEEE 802.4 - Token Bus

IEEE 802.5 - Token Ring

…

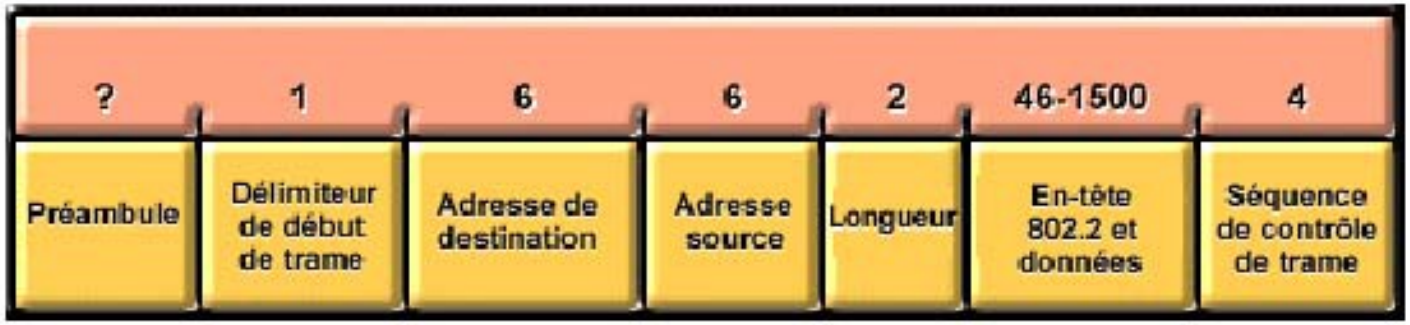
Solutions- CRC (ou FCS)

Spécifications des Trames

Structures de trame Ethernet et IEEE 802.3

Ethernet

IEEE 802.3



Trame percutée < 72 octets (7 + 1 + 6+6+2+46+4)

Solution : Règle d'or

La règle d'or des 5-4-3-2-1 (non, restez !)

Pour un réseau Ethernet en Bus : AU PLUS ...

Cinq sections du réseau, Quatre répéteurs,
Trois segments " mixtes ", Deux segments de liaison,
Dans **un** domaine de collision.

Revisitée dans les topologies en étoile

Pour un réseau Ethernet 10Mbps : AU PLUS ...

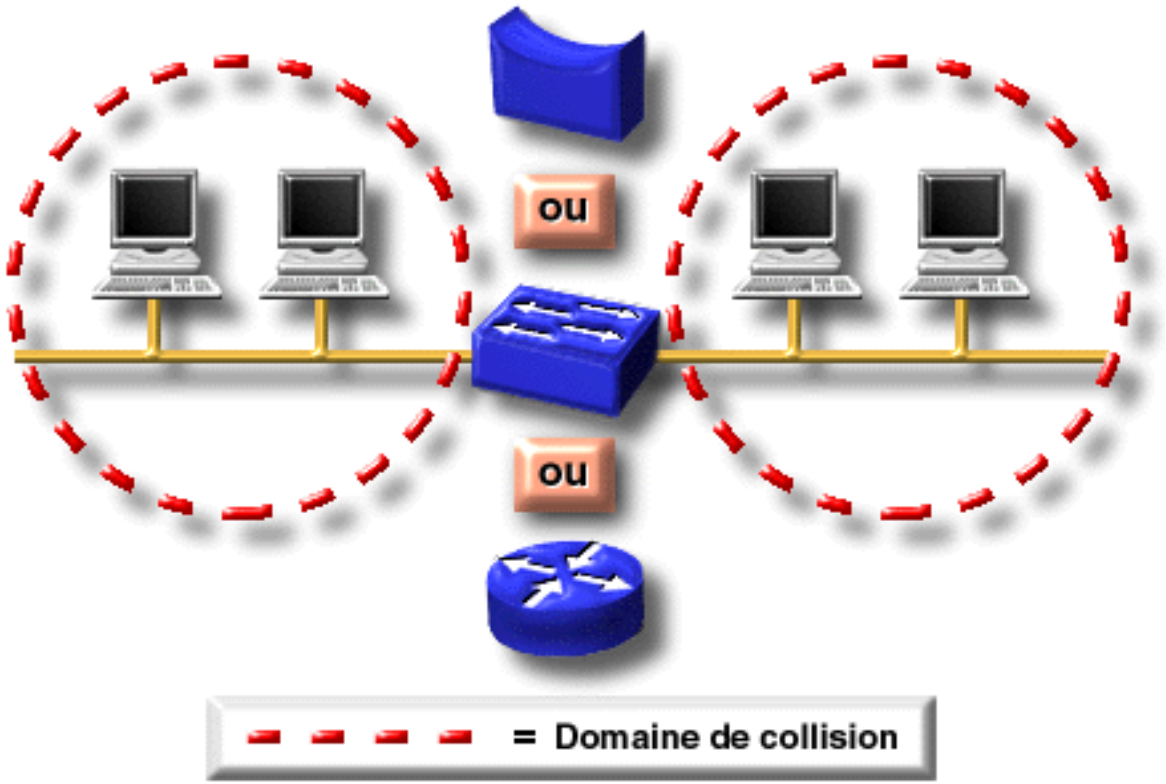
Quatre répéteurs peuvent séparer deux Hosts

Pour un réseau Fast Ethernet 100Mbps : AU PLUS ...

Deux répéteurs (Type II) peuvent séparer deux Hosts

Solution : Segmentation

Division des domaines de collision



Réduction de la taille des domaines de collision, donc augmentation de leur nombre!

Conclusion Couche Physique

Respecter les normes !

- Câblage horizontal
- Câblage vertical
- Normes électriques
- Topologie et architecture (distances)
- Règle d'or 5-4-3-2-1
- Taille des domaines de collision
- Bonne identification de la couche correspondant à chaque équipement (Transceiver, répéteur, hub)

COUCHE 2 : Liaison de Données

- **Couche MAC (Media Access Control)**

La Méthode d'Accès : CSMA / CD vient de l'algorithme radiophonique Aloha, elle est non déterministe.

La méthode d'accès d'un Toking Ring est déterministe.

- **Couche LLC (Type et utilisation)**

Type 1 : sans connexion ni acquittement point à point ou multipoint

Tous

Type 2 : connexion, acquittement, contrôle de flux, ordonnancement des trames …

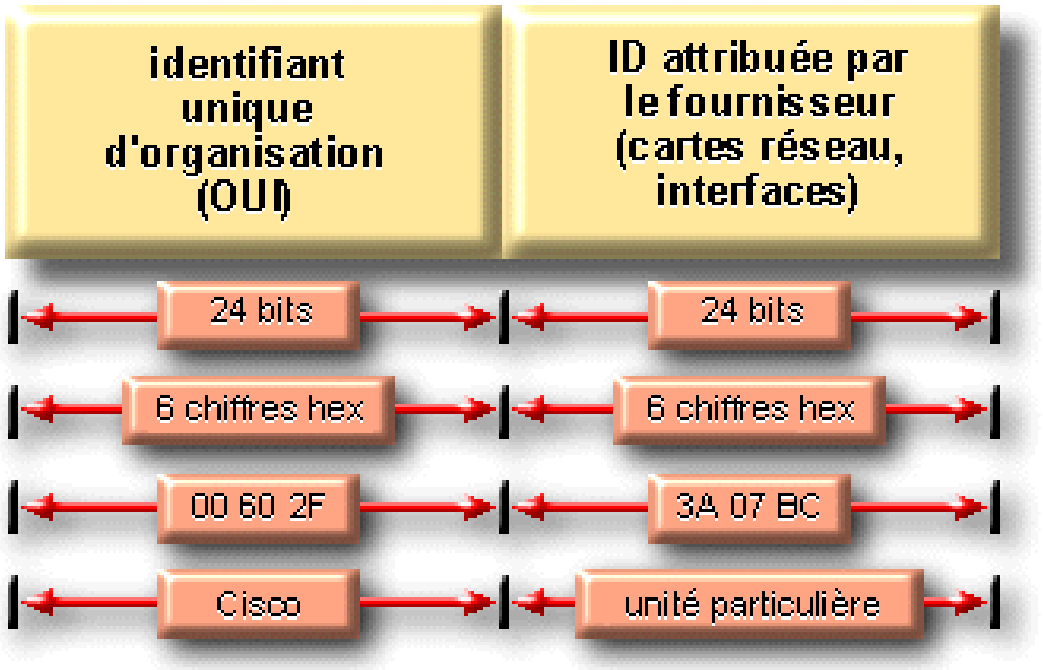
NetBios

point à point uniquement

SNA

Adressage Physique (MAC)

Structure d'adressage MAC



Adressage de niveau 2 1/2

- Les adresses MAC permettent aux hosts d'un même segment de communiquer entre eux
- Les machines de niveau 3 ou supérieur maintiennent des « Tables ARP »
- Le protocole Address Resolution Protocol permet de connaître l'adresse MAC d'un host à partir de son adresse IP
- Si cette adresse est inconnue la machine émettrice génère un broadcast ARP
- Le protocole RARP permet de retrouver l'adresse IP d'un host à partir de son adresse

Algorithme d'émission

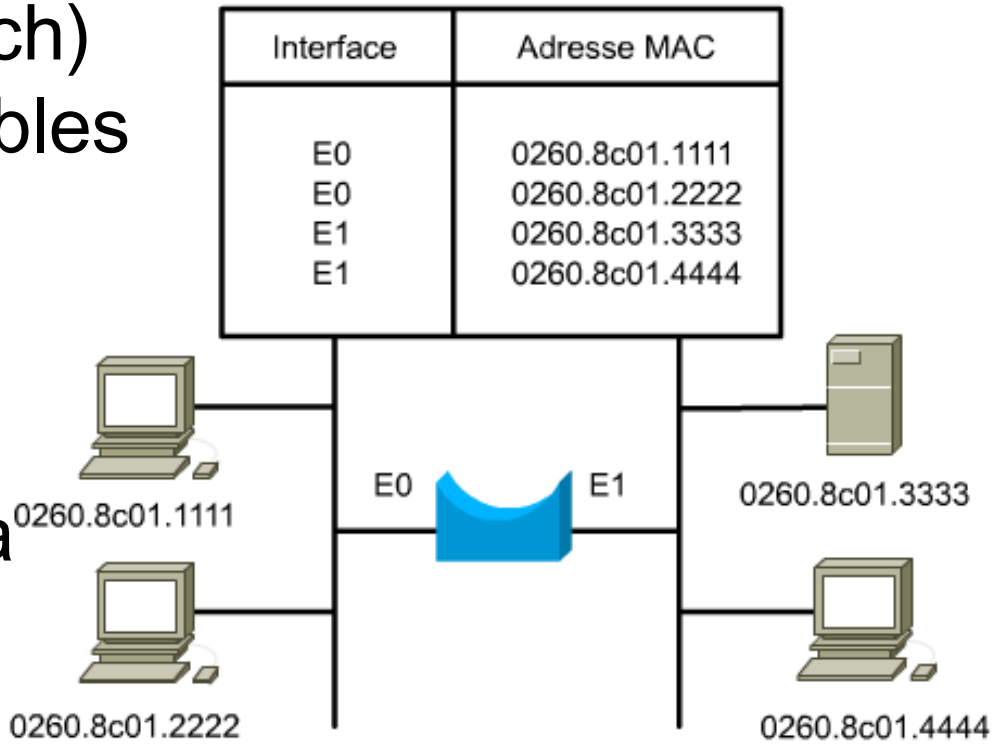
- Le destinataire est-il dans mon réseau IP ?
- Oui
  - Son adresse MAC est-elle dans ma table ARP ?
  - Oui
    - Emission de la trame vers le destinataire
  - Non
    - Emission d'un broadcast ARP pour connaître sa MAC
- Non
  - Emission d'une trame vers ma passerelle. Le paquet IP pour mon destinataire est encapsulé dans cette trame.

Adressage de niveau 2 2/2

Commutation de niveau 2

- Les ponts et donc les commutateurs (switch) maintiennent des tables de pontage (commutation)

- Ils « apprennent » la topologie du réseau



Pont / Commutateur

Ethernet

- Un pont est un matériel de couche 2 capable de désencapsuler les trames arrivantes, lire les informations de couches 2 qu'elles contiennent, puis réencapsuler en couche 2 avant de renvoyer les trames sur un port de sortie.
- Un pont peut donc, par exemple, lire des trames Ethernet et renvoyer des trames Token Ring. Il réalise ainsi une fonction d'interface entre des technologies réseaux différentes.
- Un commutateur ou switch est un pont multi

Commutateur / Switch 1 / 2

- Un commutateur concentre la connectivité et régénère le signal.
- Il permet de « segmenter » le réseau. Chaque port du commutateur est un domaine de collision distinct.
- Il peut fonctionner en modes :
- Cut through : sitôt que l'adresse MAC de destination est lue, la trame est commutée vers le bon port.
- Fragment free : identique au mode précédent, mais le commutateur lit les 64 premiers octets

Commutateur / Switch 2 / 2

- Le niveau de prix des switchs dépend de leurs fonctionnalités et du nombre de piles mémoires qui sont gérées (une pile commune, une pile par port, plusieurs piles par port avec gestion des priorités …).
- Les « hosts » connectés directement à un switch peuvent fonctionner en mode Full Duplex (le domaine de collision est réduit au host). Celui-ci peut donc émettre et recevoir en même temps sans avoir besoin d'obéir à la méthode d'accès CSMA/CD.

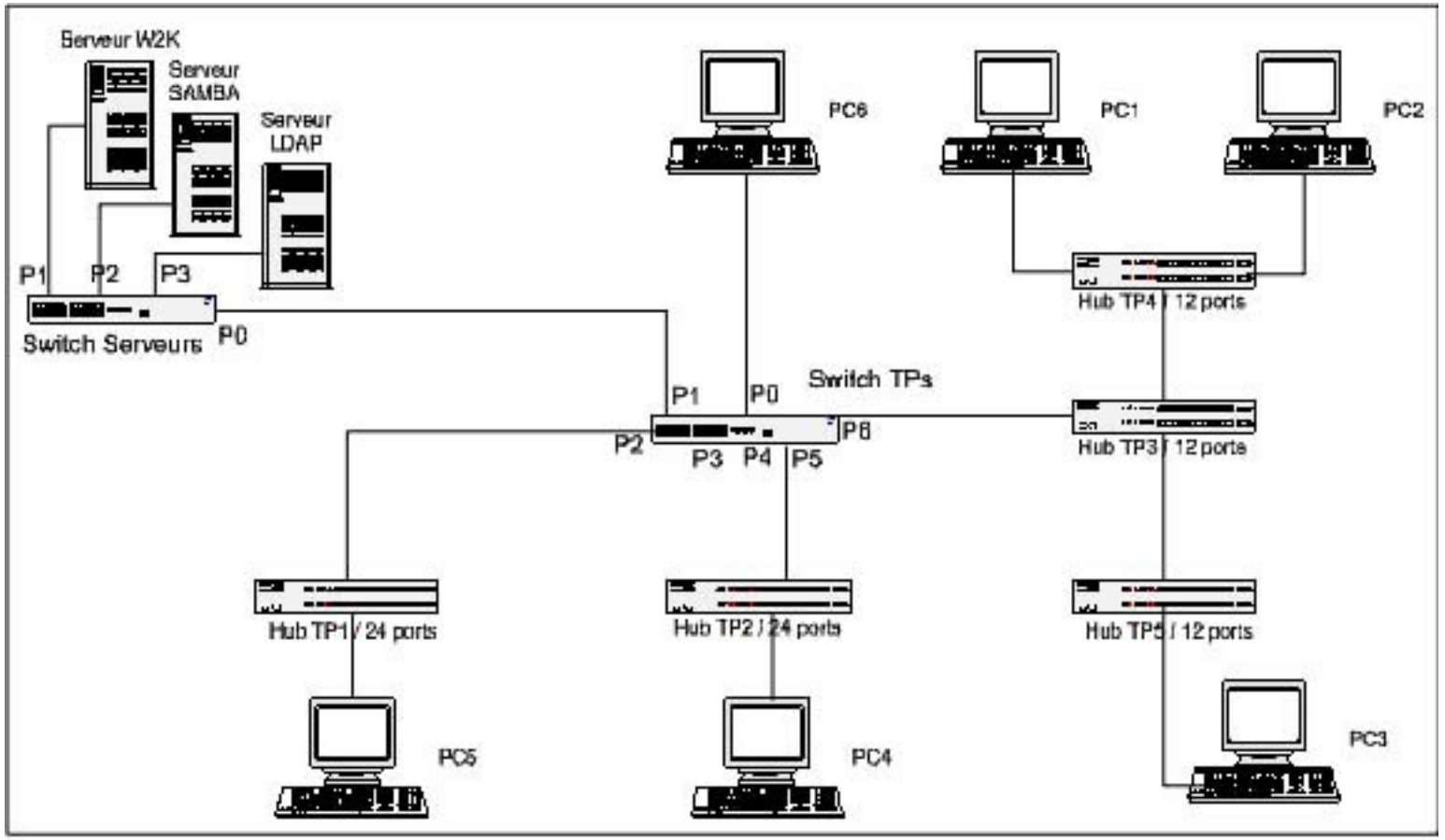
Spanning tree protocol

- Protocole qui vérifie l'absence de boucles de couche 2 => tempêtes de broadcast
- Un commutateur est élu « Root Bridge »
- Les liens vers le root sont des « root port »
- Les liens qui mènent au root sont des « designed port »
- Les autres sont « bloqués »
- Pendant le calcul le led est orange, puis passe au vert au bout d'environ 60 secondes
- Spaning tree peut être désactivé, mais attention !!!

Conclusion Couche Liaison

- Protocole phare Ethernet
- Nombreuses évolutions d'Ethernet : Fast Ethernet, Ethernet Full Duplex, Gigabit Ethernet
- Des matériels spécifiques, les commutateurs Ethernet permettent d'aboutir à un réseau sans collisions
- L'adressage de couche 2 est lié à l'adressage de couche 3 par le protocole ARP et les tables ARP maintenues par les hosts
- Les commutateurs maintiennent des tables de commutation qui apprennent la topologie du

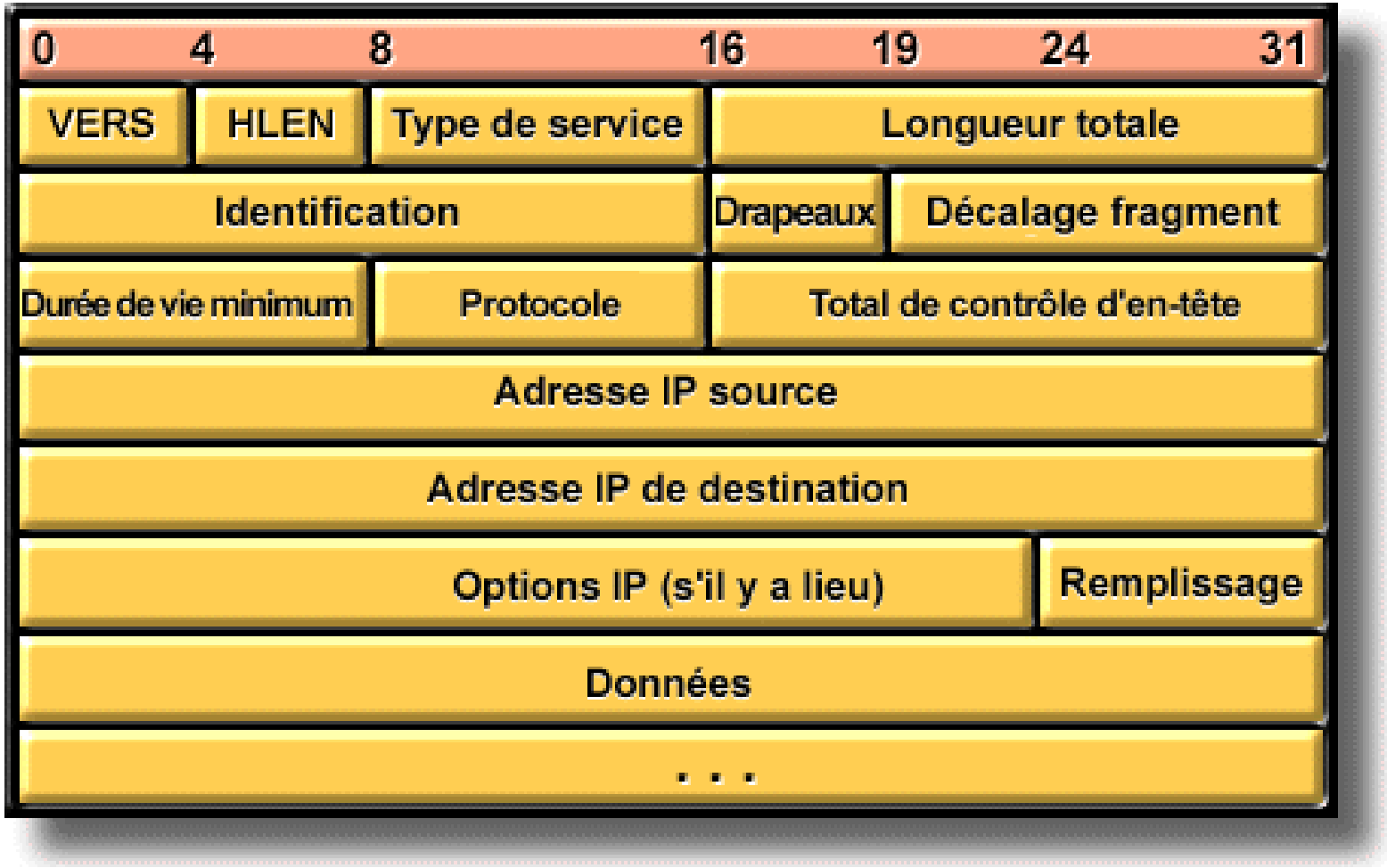
Commutation de niveau 2



COUCHE 3 : Réseau

- **Paquet**
- **Adresse de couche 3 : adresse IP**
- **Commutation de paquet – Best effort delivery**
- **Adresses publiques / adresses privées**
- **Réseaux et sous-réseaux**
- **Routeurs et routage**

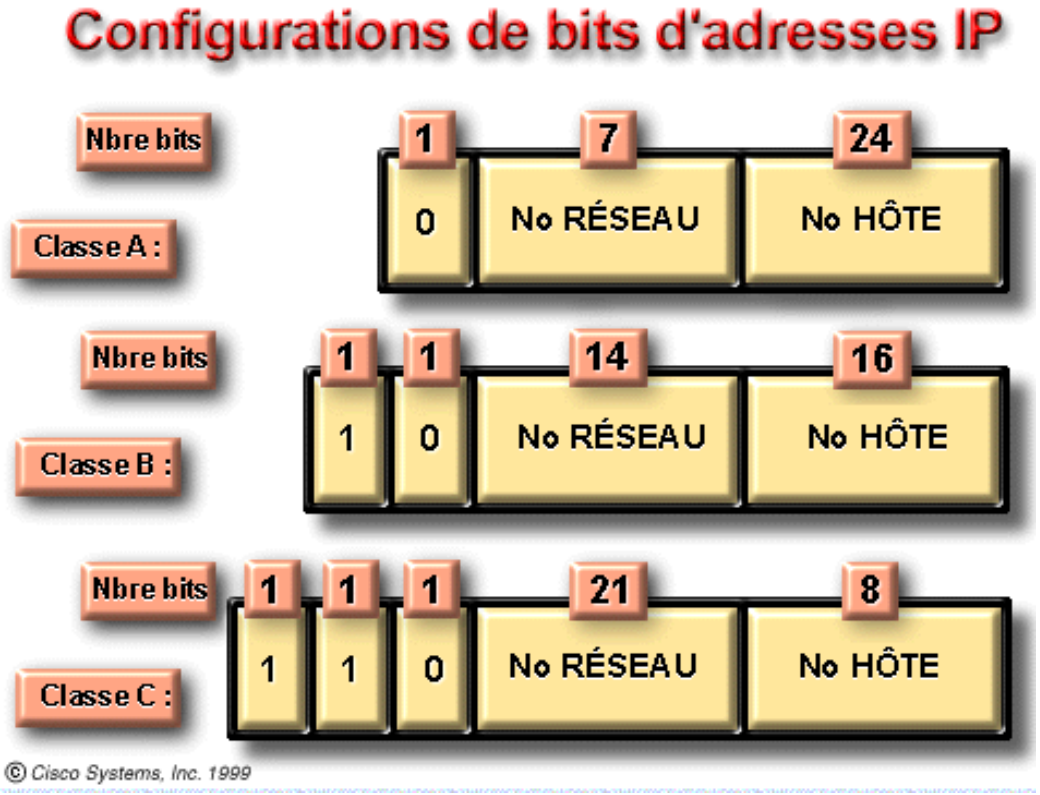
Paquet IP (1)


0
4
8
16
19
24
31
VERS
HLEN
Type de service
Longueur totale
Identification
Drapeaux
Décalage fragment
Durée de vie minimum
Protocole
Total de contrôle d'en-tête
Adresse IP source
Adresse IP de destination
Options IP (s'il y a lieu)
Remplissage
Données
. . .

Adressage de niveau 3 (1 / 3)

Adresses publiques

- Class A
  1 … 126.H.H.H
- Class B
  128 … 191.N.H.H
- Class C
  192 … 223.N.N.H
- Class D…



Adressage de niveau 3 (2 / 3)

Adresses privées – RFC 1918

- Class A 10.0.0.0 … 10.255.255.255
- Class B 172.16.0.0 … 172.31.255.255
- Class C 192.168.0.0 … 192.168.255.255

- Adresses internes à un réseau qui peuvent etre gérées par un Network Address Translation

Adressage de niveau 3 (3 / 3)

Adresse de broadcast ou adresse de diffusion

- L'adresse de broadcast d'un réseau permet de s'adresser à tous les hosts de ce réseau.
- Elle est obtenue en donnant à tous les bits de la partie host de l'adresse IP du réseau la valeur 1.
- Exemple :
- Réseau : 141.12.0.0
- Masque : 255.255.0.0
- Broadcast : 141.12.255.255
- Cette adresse ne doit jamais être attribuée à

Sous réseaux - Subnets(1/2)

- Ils servent à diminuer la taille des domaines de broadcast
- Ils sont créés par extension de la partie Network de l'adresse IP
- Cette information est associée à un masque de sous réseau (subnet mask)
- Exemple : 194.168.32.254 / 255.255.255.0 désigne :
  - le réseau 194.168.32
  - le host 254

Sous réseaux - Subnets (2/2)

- Le nombre de subnets adressables est :
  2n où n est la longueur du masque
- Deux notations :
  194.168.32.254 / 255.255.255.0
  ou 194.168.32.254 / 24
- Le nombre de hosts adressables est :
  2h-2 où h est le nombre de bits laissés pour la partie host de l'adresse

Sous réseaux - Subnets EXERCICE

- L ’adresse de l ’interface extérieure du routeur d ’accès est :
  147.94.112.129 / 26
- Déterminer :

  - le masque du sous-réseau correspondant à cette notation en format xxx.xxx.xxx.xxx
  - l ’adresse du sous-réseau qui contient cette adresse de host
  - le nombre d ’adresses valides de hosts sur ce sous-réseau
  - la première adresse de host, la dernière et l ’adresse de broadcast

Sous réseaux - Subnets - Solutions

- Réponses :

- Masque du sous-réseau : 255.255.255.192
- Adresse du sous-réseau : 147.94.112.128
- Nombre d'adresses de host valides :
  2(32-26) - 2 = 26 – 2 = 62 adresses
- Première adresse de host : 147.94.112.129
- Dernière adresse de host : 147.94.112.190
- Adresse de broadcast : 147.94.112.191

Routeur

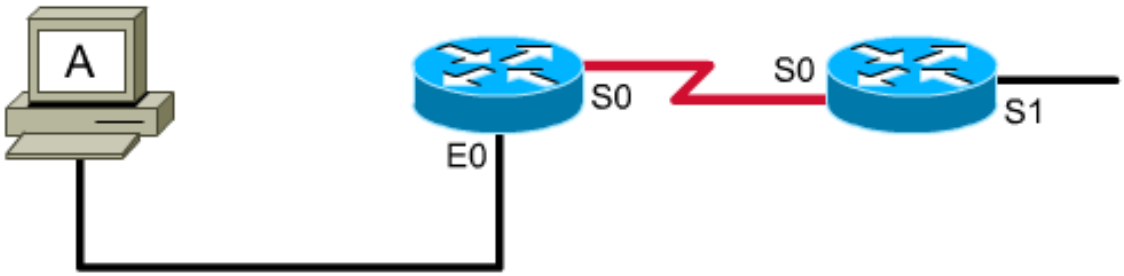
- Un routeur est un « ordinateur » spécialisé pour cette tâche, ou une machine standard configurée pour cela.
- Il comporte au moins deux interfaces. Chaque interface du routeur appartient à un réseau différent et est la passerelle du réseau qu'elle dessert.
- Le routeur désencapsule les messages jusqu'au niveau trois. Il peut donc, par exemple, connecter deux réseaux couche 2

Routeur

- Les routeurs maintiennent des tables de routage
- Ils se communiquent l'architecture logique du réseau

Table de routage IP

	Réseau de destination	Interface (Saut suiv.)
	172.16.0.0	S0
	172.18.0.0	--
	192.168.24.0	S0
Pas de corresp.	Rout. par défaut	S1



Routeur

- Les routes peuvent être définies par l'administrateur du réseau
  = routage statique

- Exemple
  ip route 169.127.0.0 255.255.0.0 interface e0

- Elles peuvent être déterminées par un échange d 'informations entre les routeurs
  = routage dynamique

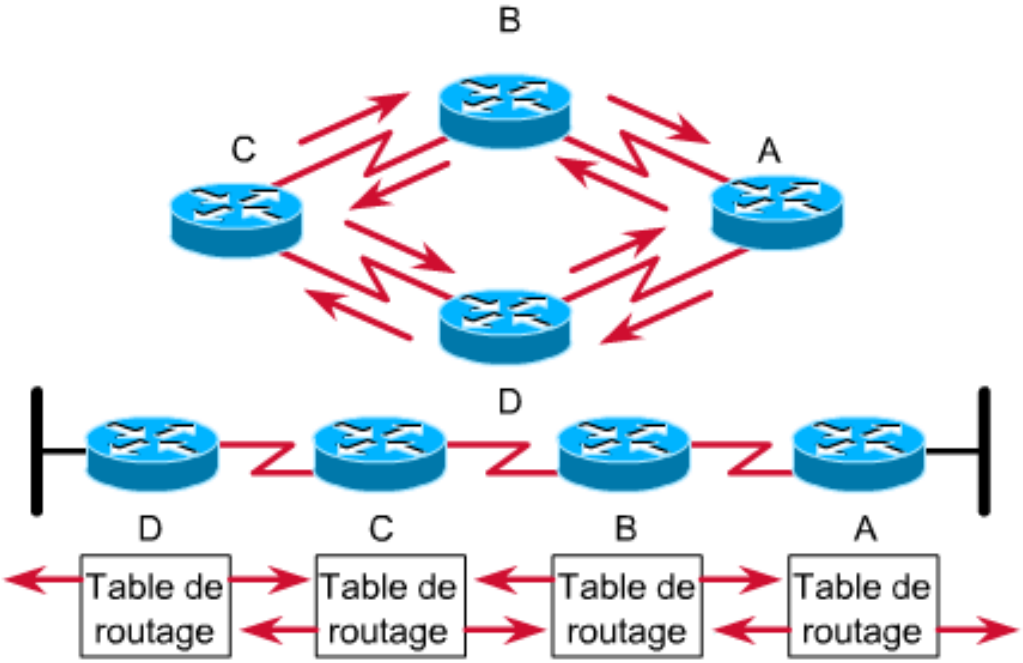
Protocoles de Routage

- Les routeurs utilisent différents protocoles plus ou moins efficaces pour déterminer les meilleures routes et s ’échanger les informations correspondantes = protocoles de routage

- Protocoles de type Vecteur de Distance
  RIP, IGRP,
- Protocoles de type Etats de Liens
  OSPF
- Protocoles hybrides

Protocoles de Routage

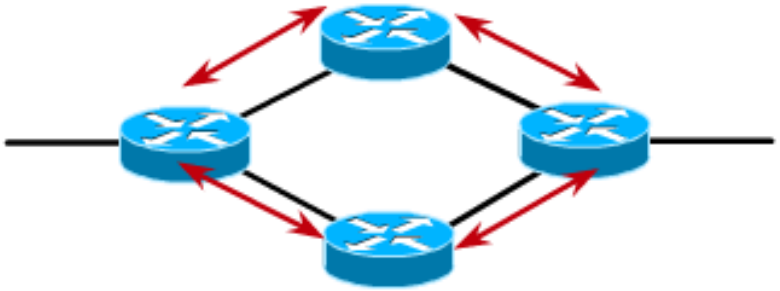
Routage à vecteur de distance



- Envoi périodique de copies de la table de routage aux routeurs voisins et addition des vecteurs de distance.

Protocoles de Routage

Notion d'état de la liaison



Paquets de mise à jour à état de liaison

Base de données topologiques

Algorithme SPF

Arbre du plus court chemin d'abord

Table de routage

- Après le flot initial, envoi de petites mises à jour déclenchées par événement à tous les autres routeurs.

Protocoles de Routage

- Vecteur de Distance

  - simples à configurer
  - échange des tables de routage
  - fréquence de mise à jour = choix administrateur - voit le réseau du point de vue des voisins - addition des vecteurs de distance

  => La convergence est lente.

- Etats de Liens

  - plus complexes => puissance de calcul
  - échange des états de liaison
  - mise à jour déclenchée par événements

Routage: configuration

- Commande network <IP> <Mask>
  - Existe pour RIP, EIGRP, OSPF, BGP
  - N'existe pas pour IS-IS
- Network : signification pour RIP, EIGRP, OSPF

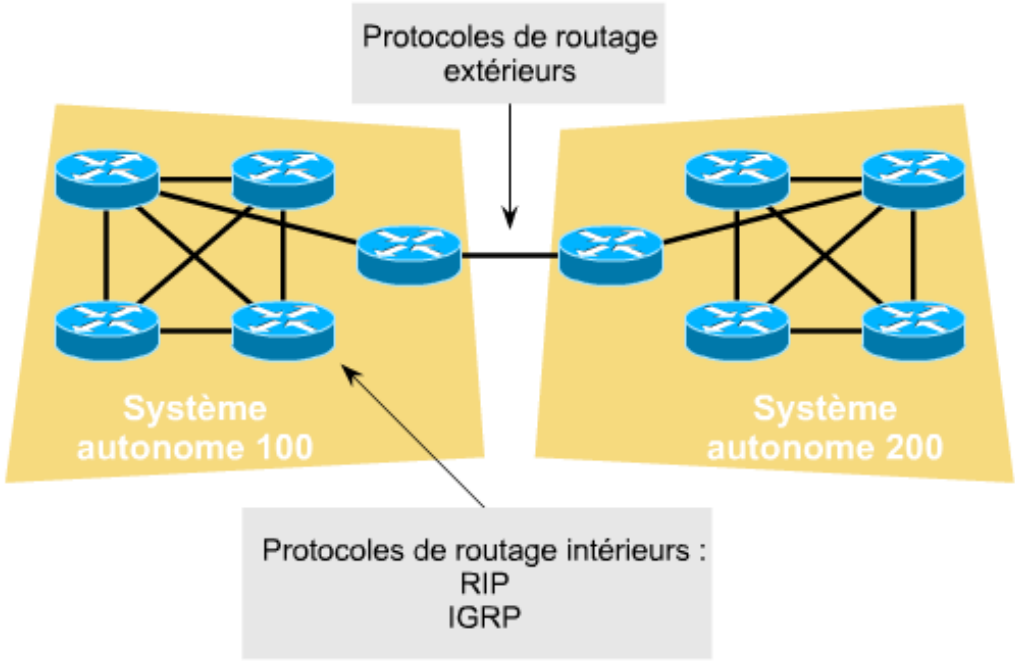
  Identifie les interfaces qui participent au protocole : c'est-à-dire toutes les interfaces dont l'adresse IP appartient au réseau défini dans network. Ces interfaces vont émettre et recevoir des paquets « hello » et définir en conséquence les routeurs voisins. Puis le routeur échangera les annonces de routage avec ces voisins.
  NB : RIP ne peut identifier que des réseaux classfull
- Network : signification pour BGP

  Identifie les réseaux qui doivent être annoncés aux autres routeurs.
  NB : la notion de voisin est totalement indépendante de l'annonce network

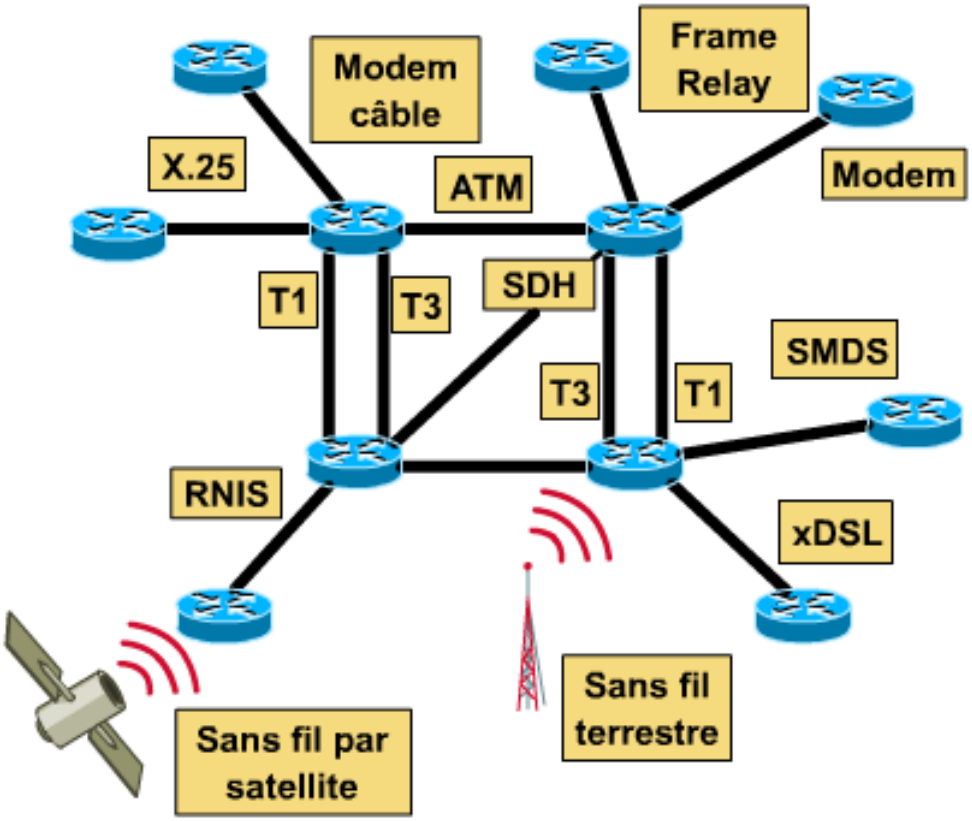
Routage intérieur, extérieur & systèmes autonomes

- Un système autonome est administré par une entité qui établit sa politique d'administration.
- Les systèmes autonomes communiquent par des protocoles extérieurs (ex : Border Gateway Protocol)

Domaines et systèmes autonomes



Liaisons WAN entre routeurs



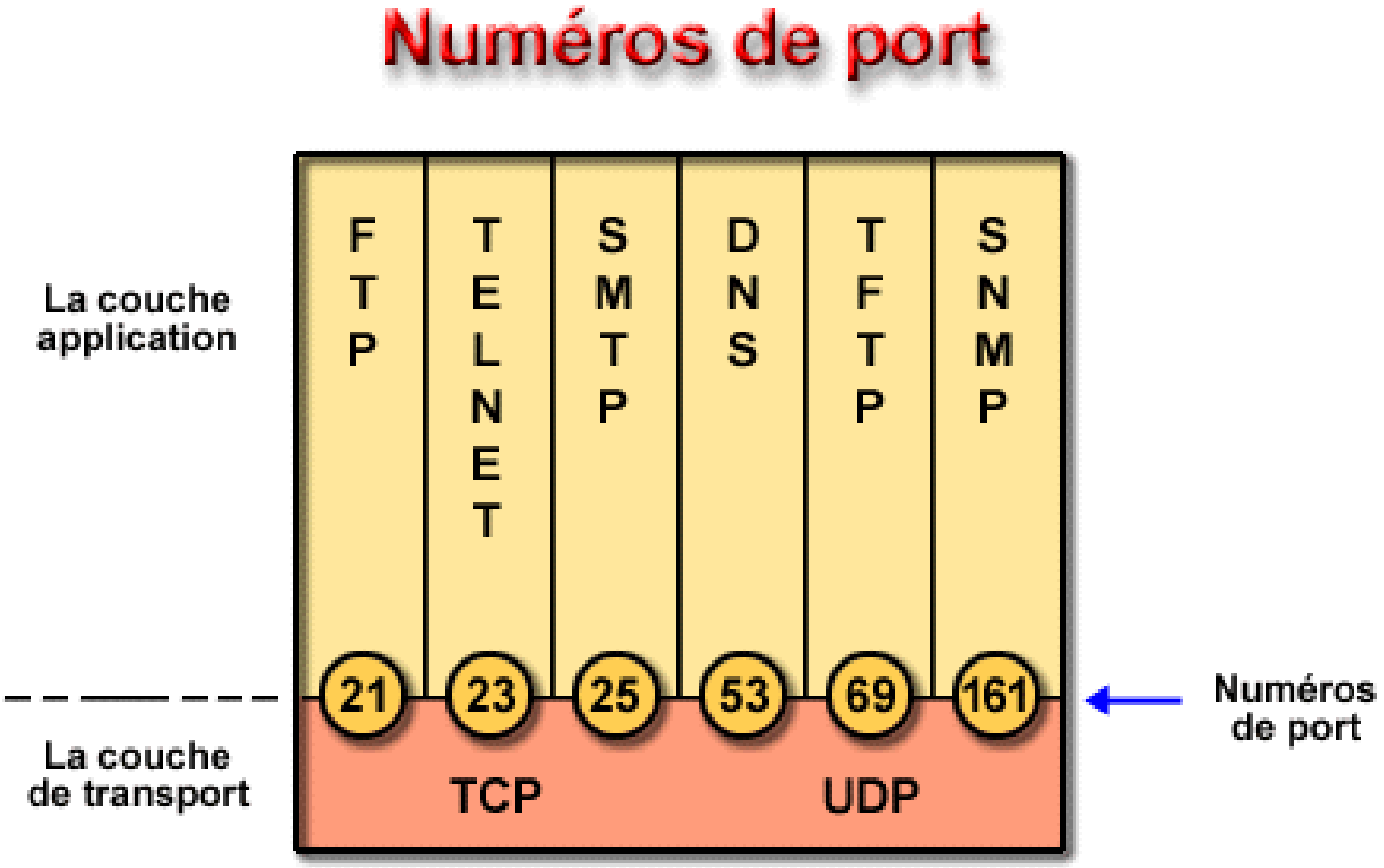
Conclusion Couche Réseau

- Gérée par les routeurs
- Chaque interface de routeur est la passerelle du domaine de broadcast qu'elle délimite
- Les routeurs sont configurés manuellement (routeurs d'extrémité) ou apprennent dynamiquement les chemins en s'échangeant des informations via les protocoles de routage
- Chaque routeur possède une route par défaut qu'il adresse quand il ne connaît pas le chemin vers la destination
- L'interconnexion mondiale est assurée par des liaisons WAN entre routeurs

COUCHE 4 : Transport

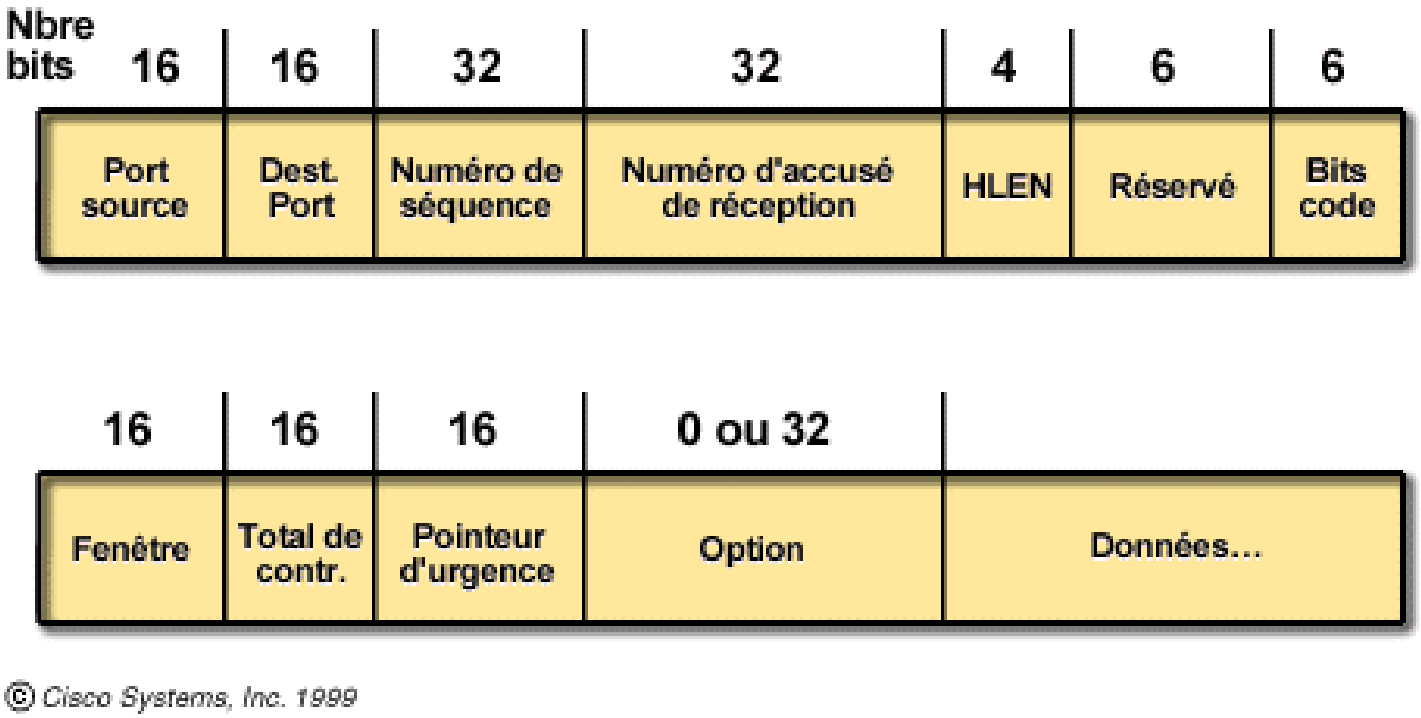
- **Segment**
- **Adresses de couche 4 : ports**
- **Structure d'un segment TCP**
- **Structure d'un segment UDP**

Adressage de niveau 4



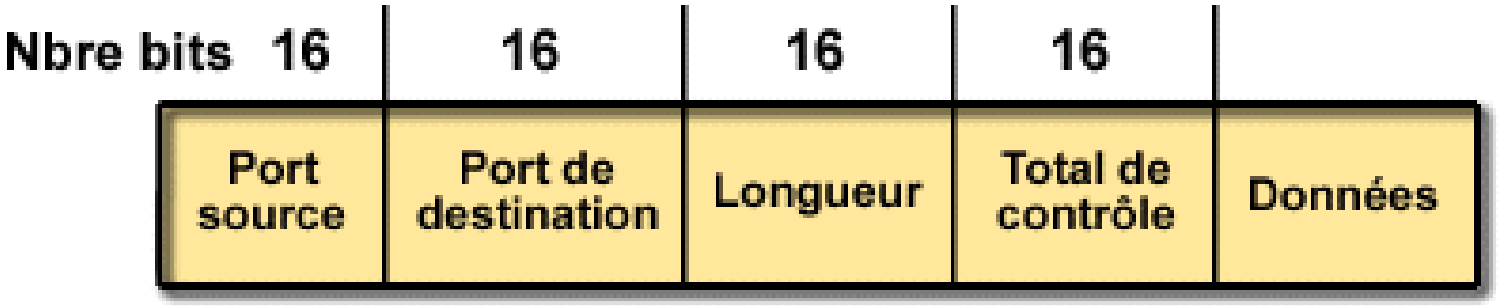
Segment TCP

Structure de segment TCP



Segment UDP

Structure de segment UDP



- Pas de champs de séquence ou d'accusé de réception

Orienté connexion / déconnecté

- Orienté connexion = téléphone
- Déconnecté = lettre postale

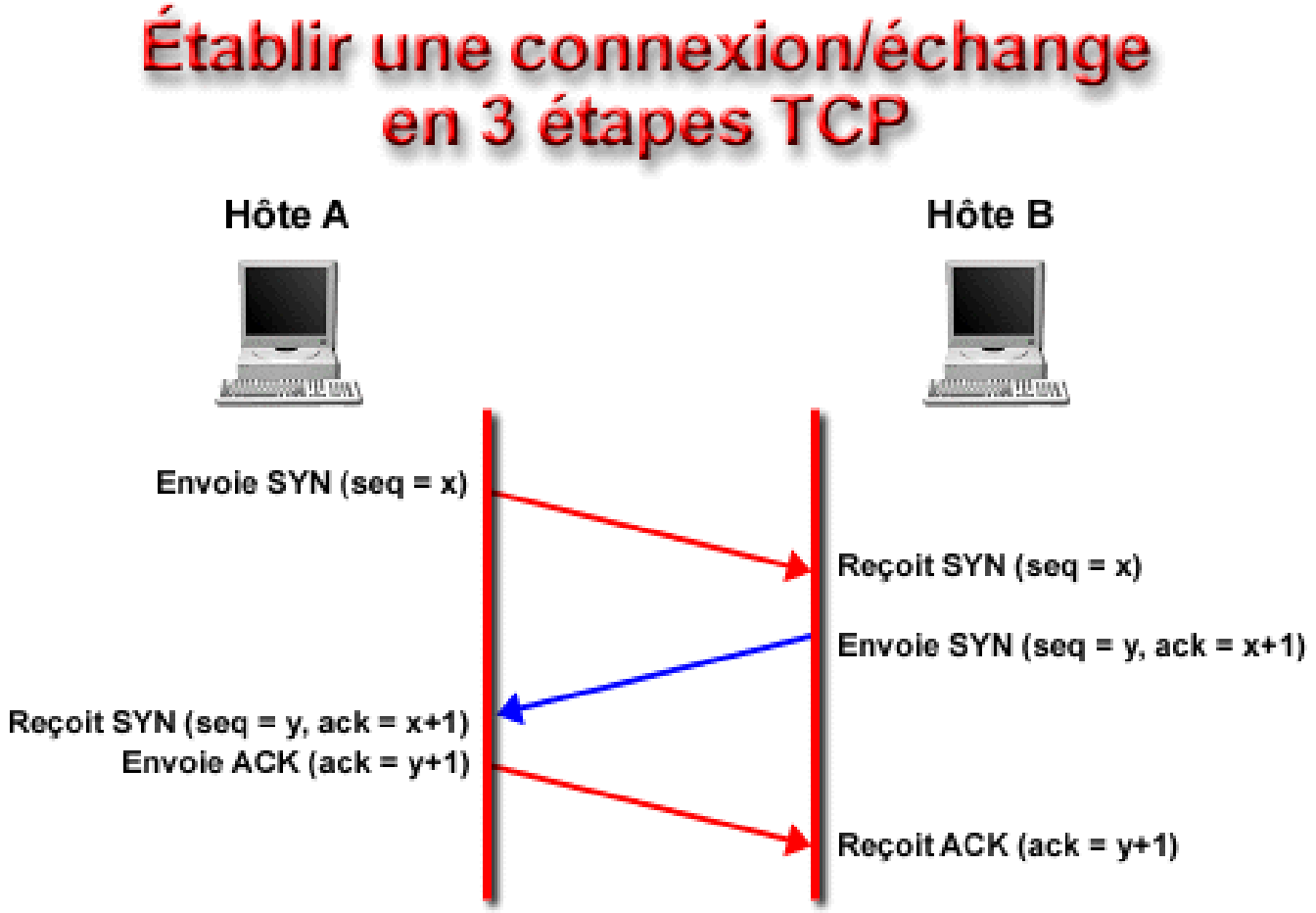
UDP : sans connexion

- *UDP = ni fenêtrage, ni accusés de réception.*
- *=> les protocoles de couche application doivent assurer la fiabilité.*
- *UDP est conçu pour les applications qui n'ont pas à assembler des séquences de segments.*
- *Voici quelques protocoles qui utilisent le protocole UDP :*
  - *protocole TFTP*
  - *protocole SNMP*
  - *protocole DHCP*

TCP : orienté connexion

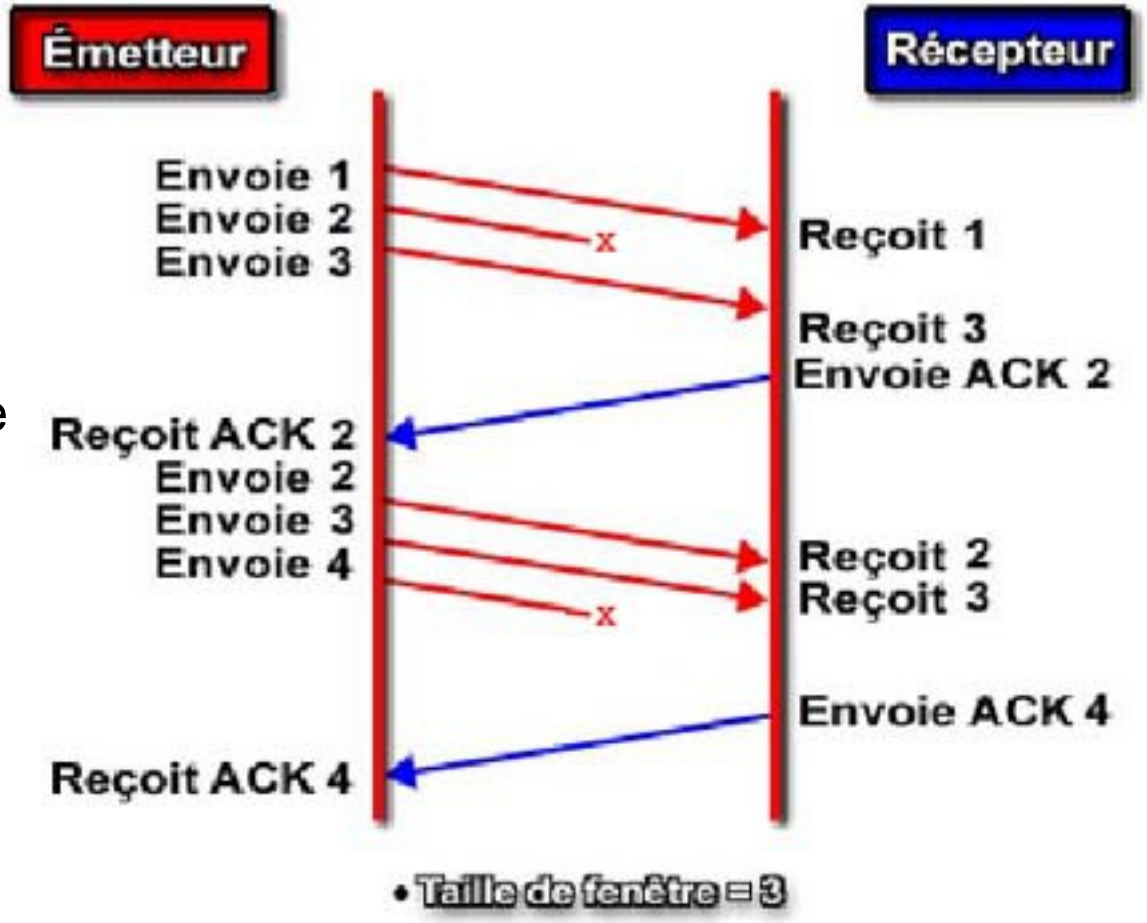
- Three way handshake
- Numérotation des segments
- Accusés de réception
- Fenêtre TCP

Three Way Handshake



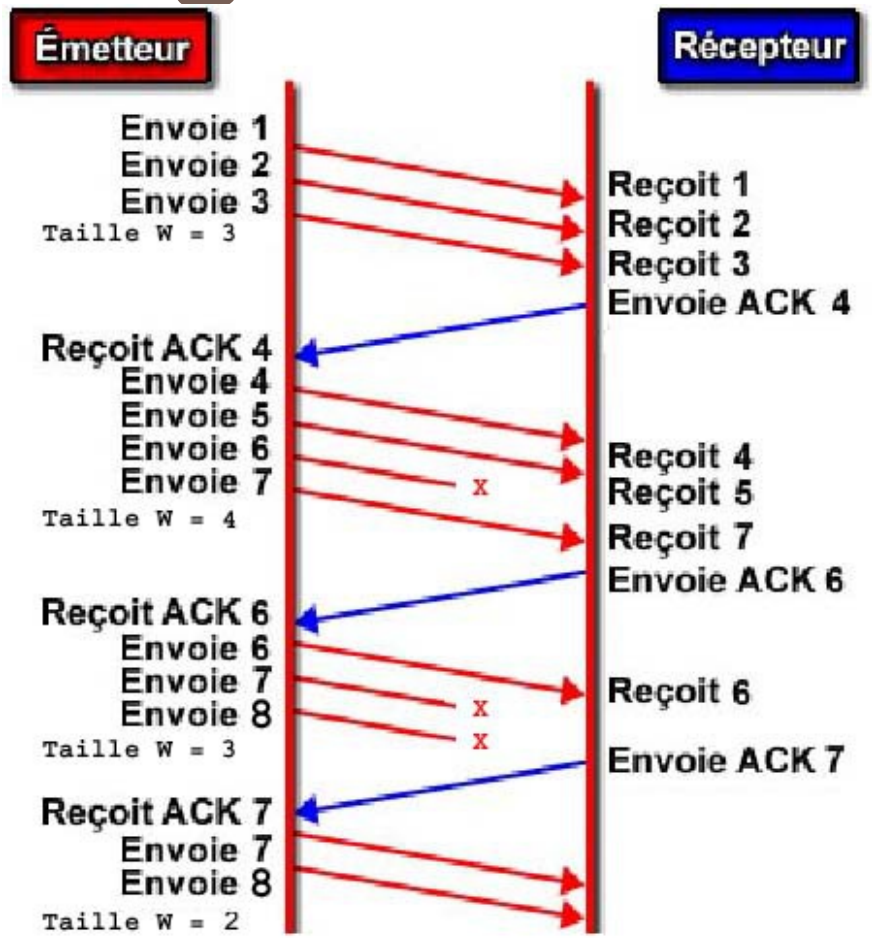
Mécanisme d'accusé réception

- L'émetteur envoie plusieurs segments numérotés.
- Ce nombre de segments est déterminé par la taille de la fenêtre TCP.
- Le récepteur renvoie un accusé de réception avec le numéro du prochain segment attendu.



Fenêtre glissante - Windowing

- Les hôtes commencent l'échange avec une taille de fenêtre par défaut.
- Ils cherchent ensuite à augmenter cette taille si la disponibilité du réseau est suffisante.
- Si les communications sont peu fiables ils diminueront la taille de la fenêtre glissante.



Algorithme d'émission

- Couple <IP/Port> = socket
- Ports parfaitement définis (Well known ports) : plage 0 à 1023
- Ports déposés (Registered ports) :

  plage1024 à 49151
- Ports Dynamiques et/ou Privés (Dynamic ports) :

  plage 49152 à 65535
- L'émetteur tire aléatoirement un numéro de port dynamique et lance un processus système

Conclusion Couche Transport

- Désignation du service demandé
- Temps réel ou très faible quantité de données : UDP
- Fiabilité, gestion de flux, données volumineuses : TCP

Architecture de réseau local

- Problématique
  - Adapter le réseau à l'organisation de l'entreprise
  - Réseaux IP = Politique spécifique du système d'Information pour un groupe défini d'utilisateurs
  - Tous les groupes n'ont pas les mêmes droits et ne disposent pas des mêmes fonctionnalités
  - => Plusieurs réseaux sur un même site
- Solution : des réseaux plus nombreux et plus petits
  - Limitation des domaines de diffusion
  - Limitation des attaques ARP
  - Politique de sécurité configurée en couche distribution

Architecture de réseau local

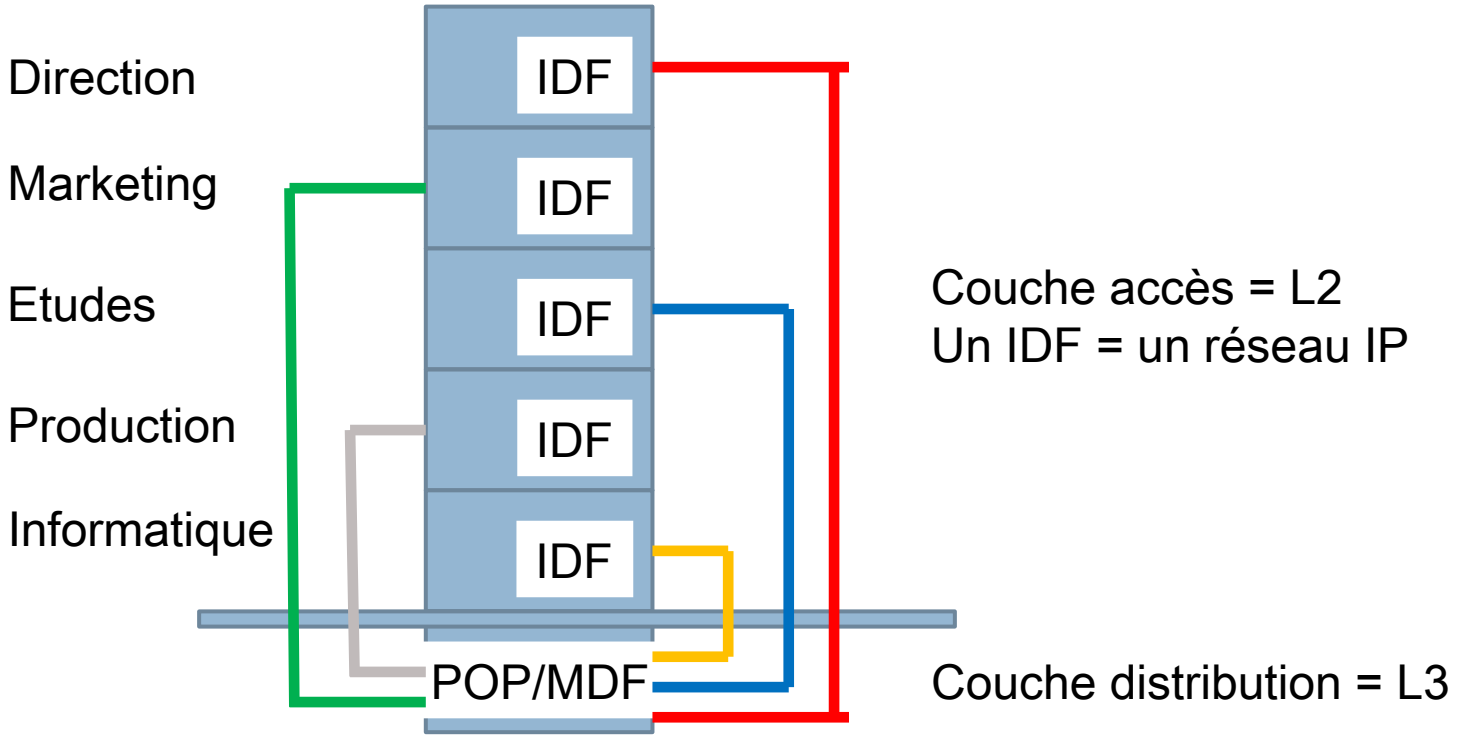
- Couche d'accès au réseau = Réseau local
  - Là où les clients se connectent
  - Hubs, commutateurs, bornes Wifi
- Couche distribution = Réseau local
  - Là où sont les passerelles (premier routeur) des différents segments de réseau
  - Là ou se configure la politique de sécurité et les contrôles de flux (QoS notamment)
- Backbone = WAN ou MAN (Réseau Métropolitain)
  - Lien au monde extérieur ou aux autres sites de l'entreprise

Architecture de réseau local

- Couche d'accès au réseau = Réseau local
  - Là où les clients se connectent
  - Hubs, commutateurs, bornes Wifi
- Couche distribution = Réseau local
  - Là où sont les passerelles (premier routeur) des différents segments de réseau
  - Là ou se configure la politique de sécurité et les contrôles de flux (QoS notamment)
- Backbone = WAN ou MAN (Réseau Métropolitain)
  - Lien au monde extérieur ou aux autres sites de l'entreprise

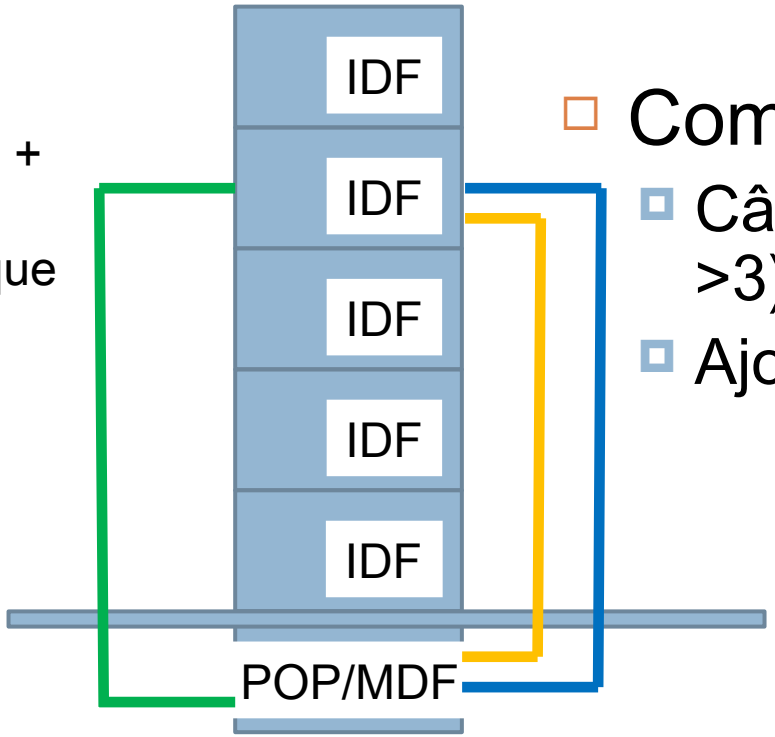
Architecture de réseau local

- Organisation de l'entreprise = chaque étage est occupé par le même groupe d'utilisateurs



Architecture de réseau local

- L'organisation de l'entreprise change => équipes pluridisciplinaires et variables



- Comment faire ?
  - Câblage vertical insuffisant (1->3)
  - Ajouter des commutateurs…

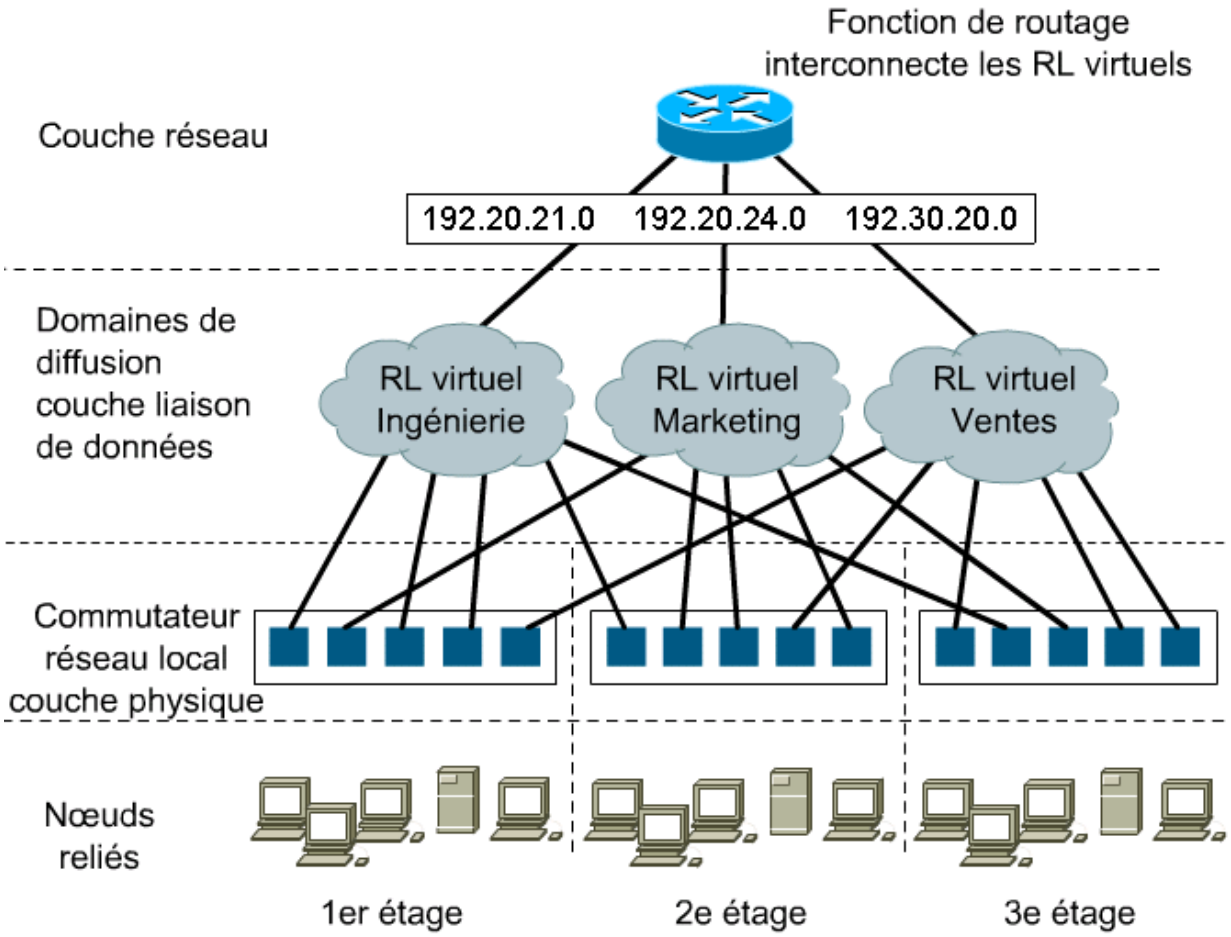
Couche accès = L2
Plusieurs réseaux IP dans un IDF

Couche distribution = L3

Segmentation en VLAN

Mise en œuvre de la sécurité LAN

- Filtrage de Trames
- Etiquetage de Trames
- Limitation des domaines de diffusion
- Filtrage entre VLANs

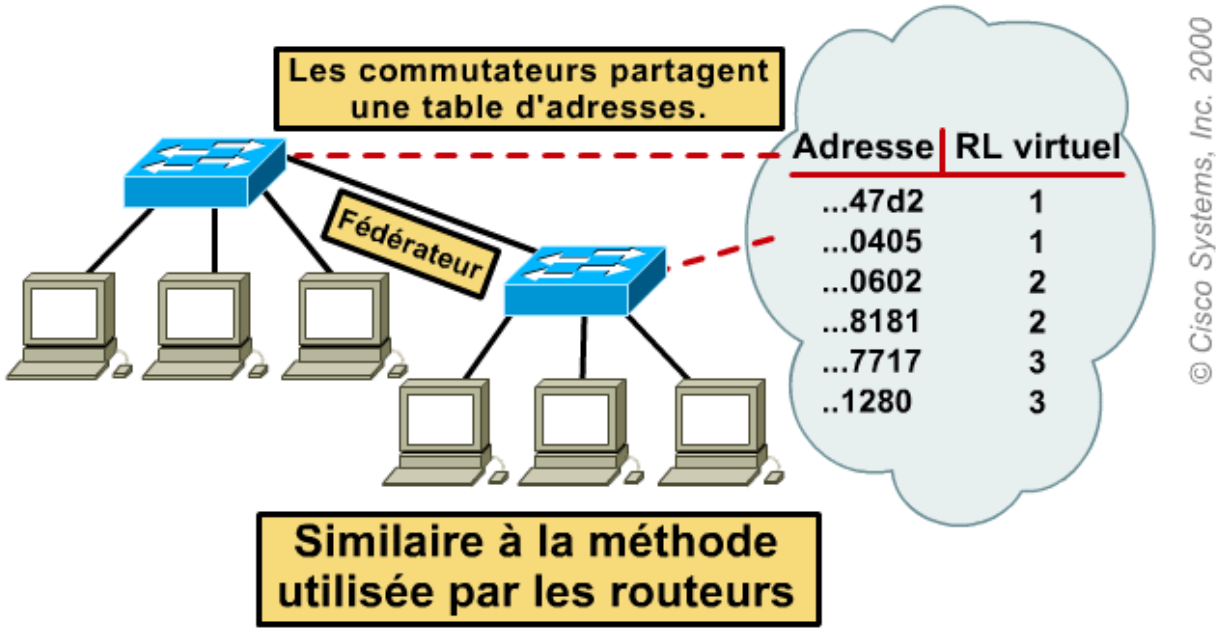


Segmentation en VLAN

- Technologie ad-hoc qui sert à interconnecter des commutateurs (backbone) supportant plusieurs VLAN (issu de Inter Switch Link de Cisco)
- Place un identificateur unique en tête de chaque trame qui entre sur le réseau fédérateur (backbone – câblage vertical)
- Retire cet identificateur de l'en-tête de trame quand elle entre dans le réseau de distribution (câblage horizontal)
- ISL a été normalisé en IEE 802.1Q

Segmentation en VLAN

Mise en œuvre de la sécurité LAN



- Une table de filtrage est élaborée pour chaque commutateur.
- Les commutateurs partagent l'information de la table d'adresses.
- Les entrées de la table sont comparées aux trames.
- Le commutateur prend la mesure appropriée.

Segmentation en VLAN

- Configuration des commutateurs L2 802.1Q
  - int range fa0/1 – 8
    switchport access vlan 10
  - int range fa0/9 – 16
    switchport access vlan 20
  - int gi0/1
    switchport mode trunk

Segmentation en VLAN

- Configuration du routeur (Port Based)
- L'interface fa0/0 du routeur est connectée sur un port vlan **10** du commutateur
  - int fa0/0
    ip address 10.10.**10**.254 255.255.255.0
- L'interface fa0/1 du routeur est connectée sur un port vlan **20** du commutateur
  - Int fa0/1
    ip address 10.10.**20**.254 255.255.255.0

Segmentation en VLAN

- Configuration du routeur (802.1Q) en mode Router-on-a-stick pour un petit nombre de clients (<30)
- L'interface physique fa0/0 du routeur est connectée sur un port trunk du commutateur
- Pas d'adresse IP sur l'interface, mais sur des sous-interfaces
  - int fa0/0.10
    encapsulation dot1q **10**

    ip address 10.10.**10**.254 255.255.255.0
  - Int fa0/0.20
    encapsulation dot1q **20**

    ip address 10.10.**20**.254 255.255.255.0

Segmentation en VLAN

- Pour un grand nombre de clients (>50) : Commutateurs couche 3
- Plus chers !
- Commutateurs 802.1Q – Exemple 24 ports Giga
- Ils possèdent un module de routage embarqué
- Les interfaces de routage (couche 3) sont virtuelles

```
interface vlan 10
        ip address 10.10.3.1 255.255.0.0
```

- Les routes sont en général statiques
  ip route 10.10.0.0 255.255.0.0 vlan 10

Intérêt : routage à la vitesse du lien (Giga) par ASICs

Segmentation en VLAN

- Configuration d'un commutateur **L3**
  - int range fa0/1 – 8
    switchport access vlan 10
  - int range fa0/9 – 16
    switchport access vlan 20
  - int gi0/1
    switchport mode trunk
  - int vlan **10**
    ip address 10.10.**10**.254 255.255.255.0
  - int vlan **20**
    ip address 10.10.**20**.254 255.255.255.0

Architectures de Réseaux

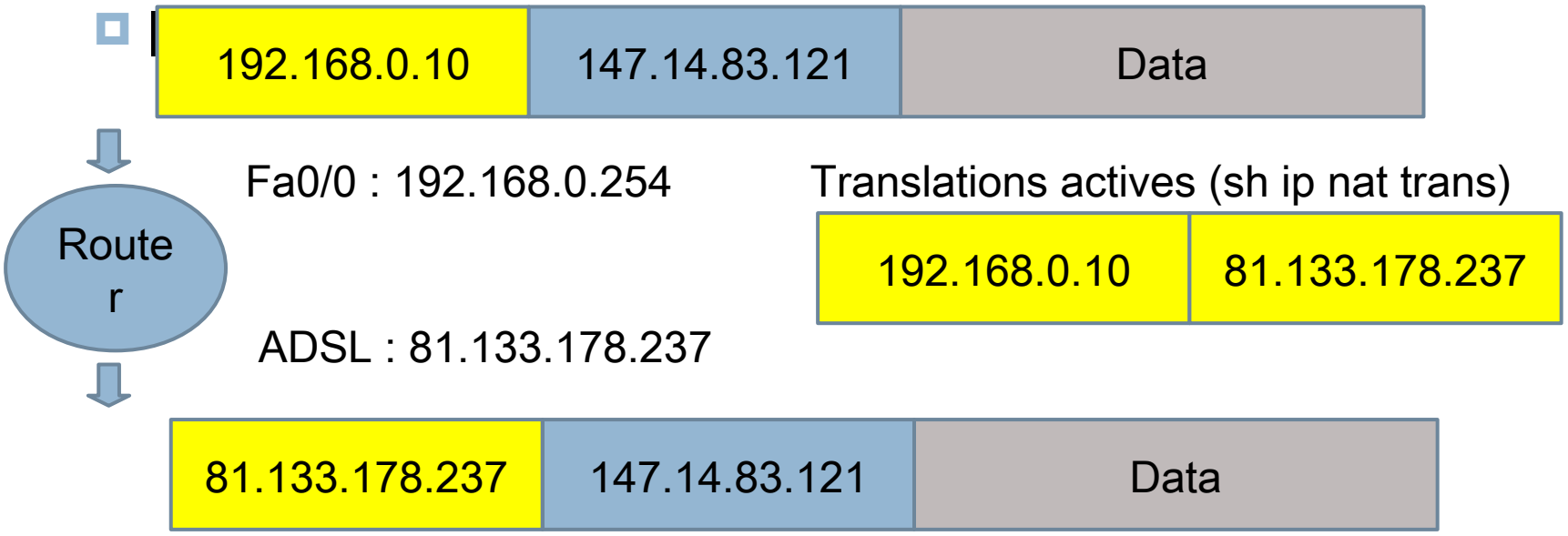
- Site unique
  - Un réseau interne, connecté à un opérateur
  - Cas de votre Box
- Plusieurs sites
  - Plusieurs sites connectés à un ou plusieurs opérateurs
  - Le réseau Internet partagé par tout le monde va permettre d'établir des liaisons entre les sites, comme s'ils étaient proches = VPN (Virtual Private Network)

Architectures de Réseaux

- Site unique
  - Adresses privées pour le réseau interne
  - Une (ou plusieurs) adresses publiques pour la connexion à Internet
- Box
  - Un réseau 192.168.0.0 / 24 sur l'interface ethernet
  - Une adresse IP publique sur l'interface ADSL
  - Les IP privées bénéficient d'une fonction de Translation d'adresse (NAT/PAT) pour les trafics sortants
    => Page suivante

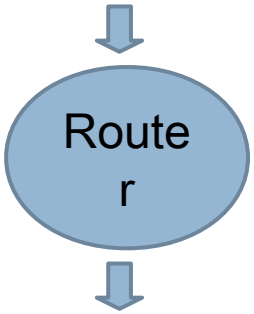
Translation d'adresse : NAT

- Network Address Translation
  - Le routeur remplace l'adresses privée interne par son IP publique : un seul PC accède à Internet en même temps
  - I



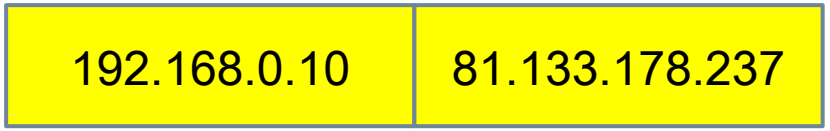
Translation d'adresse : NAT

- Network Address Translation
  - Quand la réponse arrive le routeur consulte sa table de translations actives
  - Il remplace sa propre adresse par celle du client



ADSL : 81.133.178.237

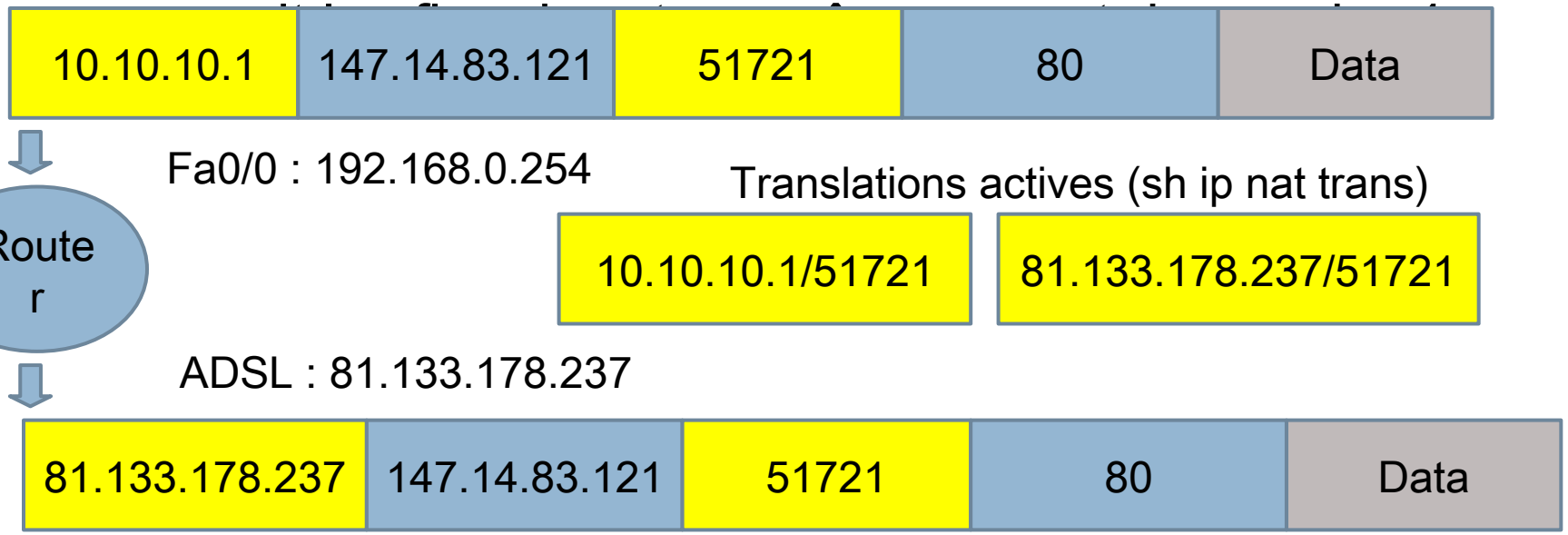
Translations actives (sh ip nat trans)



Fa0/0 : 192.168.0.254

Translation d'adresse : PAT

- Port Address Translation
  - Le routeur remplace les adresses internes par son IP publique : des milliers de PC peuvent accéder à Internet en même temps
  - Il conserve en mémoire les translations opérées et



Translation d'adresse : NAT/PAT

- Address & Port Address Translation
  - Cas d'une entreprise avec plusieurs dizaines ou centaines d'accès à Internet en même temps
  - Pour tous les flux en mode déconnecté (HTTP par exemple), le routeur opère un PAT en utilisant son IP publique externe
  - Pour les flux en mode connecté (SSH par exemple), le routeur opère un NAT en utilisant un « pool » d'adresses publiques
  - NAT STATIQUE : l'adresse privée des serveurs (serveur Web, serveur Mail) est associée de façon statique à des IP publiques référencées dans les serveurs DNS
  - Redirection de Port : en cas de pénurie d'adresses publiques c'est le port de couche 4 qui permet au routeur de diriger le trafic vers le bon serveur : par exemple port

Sécurité : Firewall

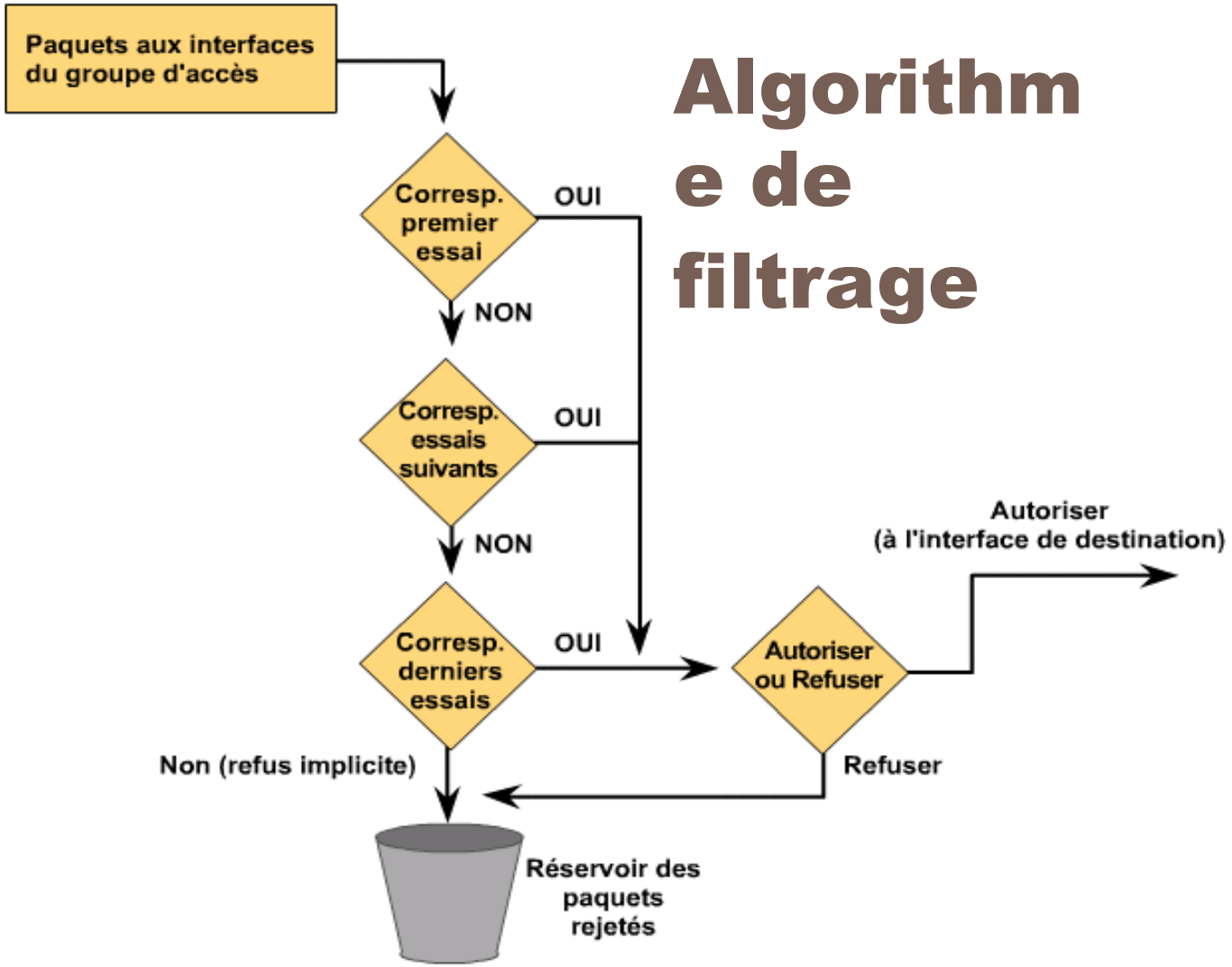
- Un Firewall est un routeur qui assure les fonctions de :
  - Routage
  - NAT/PAT
  - Filtrage d'accès (sécurité) : access list
  - Initiateur et terminateur de tunnels (GRE ou IPSEC)

Sécurité : Access list

- Liste de contrôle d'accès
  - Une ACL est une règle de filtrage définie sur une interface de routeur ou (switch L3) qui opère sur les couches 3 et 4
  - Chaque paquet entrant est comparé avec les conditions de la règle : si elles sont vérifiées, la commande associée à la règle est exécutée, sinon le paquet est comparée à l'ACL suivante. Si aucune ACL n'a « matché », le paquet est rejeté
  - Les conditions peuvent être de différents types :
    adresse source et/ou adresse destination
    port …
  - Les actions sont permit ou deny (ou log, limitation de trafic…)
  - L'ACL est appliquée à une interface et une direction : in ou out (Firewall : toujours in)

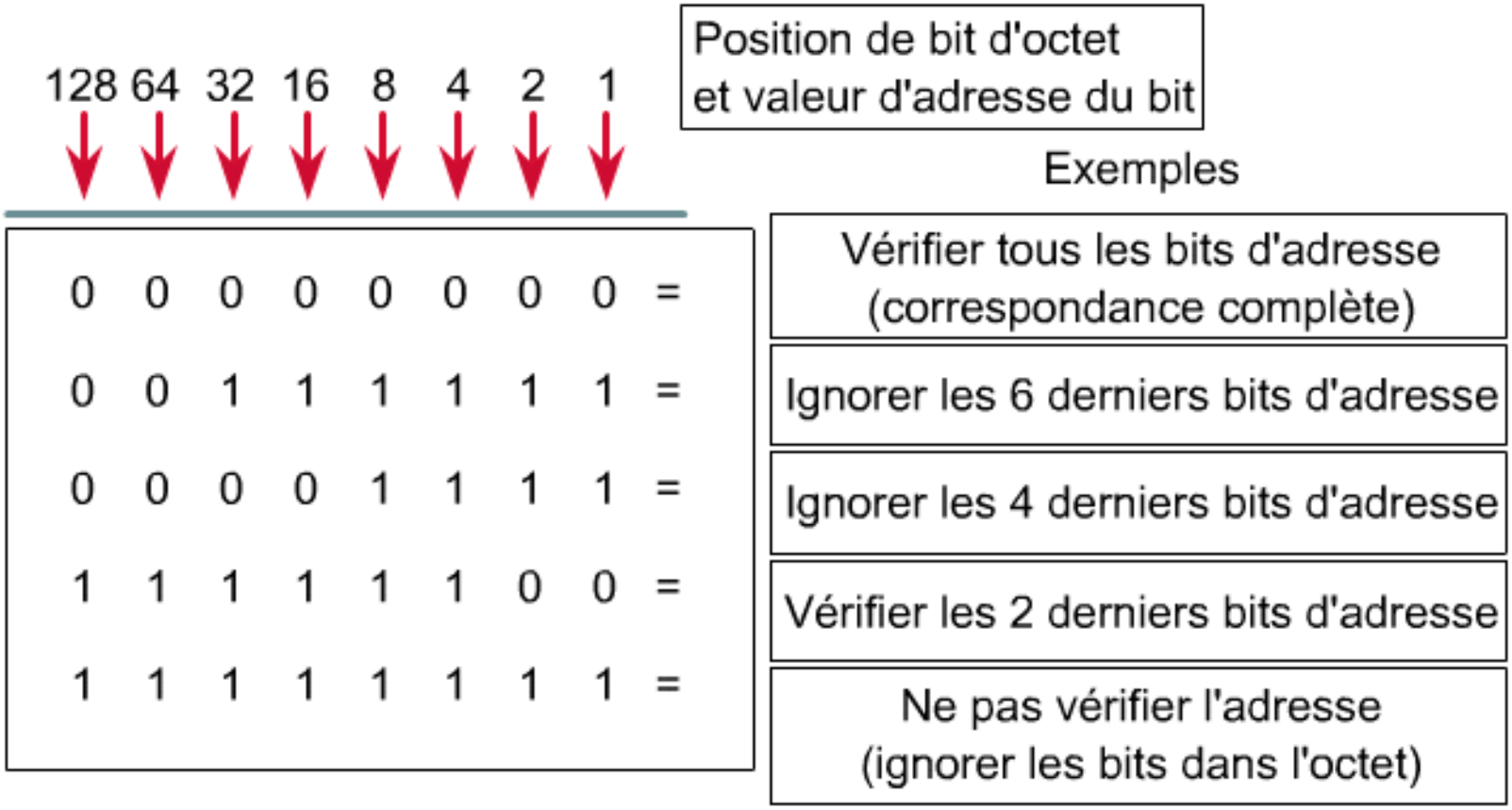
Sécurité : Access list

Algorithme de filtrage



Sécurité : Access list

Bits de Masque générique



Sécurité : Access list

Paramètre	Description
permit | deny	Indique si cette entrée autorise ou bloque l'adresse précisée.
protocole	Le protocole, tel que IP, TCP, UDP, ICMP, GRE ou IGRP.
source et destination	Identifie les adresses d'origine et de destination.
masque-source et masque-destination	Masque générique; les zéros indiquent les positions qui doivent correspondre, les uns, les positions à ignorer.
opérateur opérande	lt, gt, eq, neq (inférieur, supérieur, égal, non égal) et un numéro de port.
established	Permet au trafic TCP de passer si le paquet utilise une connexion établie (par exemple, les bits ACK sont activés).

Sécurité : Access list

- **host** 172.167.12.49 = 172.167.12.49 0.0.0.0
- **any** = 0.0.0.0 255.255.255.255
- **Permettre** l'acheminement de tout trafic du réseau d'origine 172.16.0.0 / 16 vers le réseau 81.28.234.64 / 26 et **refuser** tout autre trafic
  - ip access-list extended Exemple1
    permit ip 172.16.0.0 0.0.255.255 81.28.234.64 0.0.0.63

    "deny any any" implicite -> (deny ip 0.0.0.0 255.255.255.255 …)
  - interface ethernet 0
    ip access-group Exemple1 in
- **Refuser** un hôte particulier et **accepter** tout autre trafic
  - ip access-list extended Exemple2
    deny ip host 172.22.54.12 any
    permit ip any any

Sécurité : Access list

- **Refuser l'acheminement via E0 du trafic Telnet issu du réseau 172.16.4.0/24 et autoriser l'acheminement de tout autre trafic**
  - ip access-list extended Exemple3
    deny tcp 172.16.4.0 0.0.0.255 any eq 23

    permit ip any any
  - interface ethernet 0
    ip access-group Exemple3 in
- **Modifier cette liste de contrôle pour autoriser le trafic Telnet déjà établi**
  - ip access-list extended Exemple3Bis
    permit tcp 172.16.4.0 0.0.0.255 any eq 23 **established**

    deny tcp 172.16.4.0 0.0.0.255 any eq 23

    permit ip any any

Tunnels GRE

- **Generic Routing Encapsulation**. Permet d'établir un « tunnel » entre deux routeurs : les paquets IP sont transportés dans des paquets IP
- L'intérêt est de faire communiquer les différents sites en restant en adressage privé
- **Configuration des routeurs liés par le tunnel**
  - int tunnel 0 Configuration du routeur 1
    tunnel source fa0/1 Interface locale extérieure
    tunnel destination 81.255.255.49 IP publique de l'autre routeur
    ip address 10.1.2.1 255.255.255.252 Adresse IP du tunnel
  - int tunnel 0
    tunnel source fa0/1 Configuration du routeur 2
    tunnel destination 81.255.255.65
    ip address 10.1.2.2 255.255.255.252

Couche Application

- Après, c'est du système et de l'informatique …
- … et mon seuil d'incompétence !