

Collection Formation Réseau Cisco CCNA

LAN SWITCHING

Technologie Ethernet et Commutation

François-Emmanuel Goffinet

Formateur IT

Version 16.01

Objectifs ICND1/ICND2

- Décrire les caractéristiques physiques et de liaison de donnée d'Ethernet.
- Identifier les caractéristiques de base d'un support physique utilisé par la technologie Ethernet.
- Décrire la fonction MAC du protocole Ethernet.
- Expliquer l'importance de l'adressage de couche 2 en terme d'opérations et de performances dans les transmissions.
- Décrire les champs des différents types de trames Ethernet
- Dénombrer les avantages de la commutation.
- Expliquer le processus ARP/ND.
- Accessoirement, expliquer les enjeux de la commutation LAN en citant les notions de
 - "câblage structuré", "tempête de diffusion", "spanning-tree", "empoisonnement de cache ARP", "sécurité sur les ports" et de "technologies VLAN".

Sommaire

1. Modèles en couches et standards Ethernet
2. Câblages, connecteurs, NIC
3. MAC CSMA/CD
4. Adressage et tramage
5. Commutation et commutateurs
6. Architectures LAN commutées (Cisco Systems)
7. Résolution d'adresses
8. Sécurités L1, L2, L3, L7
9. Exercices pratiques

1. Modèles en couches et standard Ethernet

Ethernet et Commutation

Objectifs

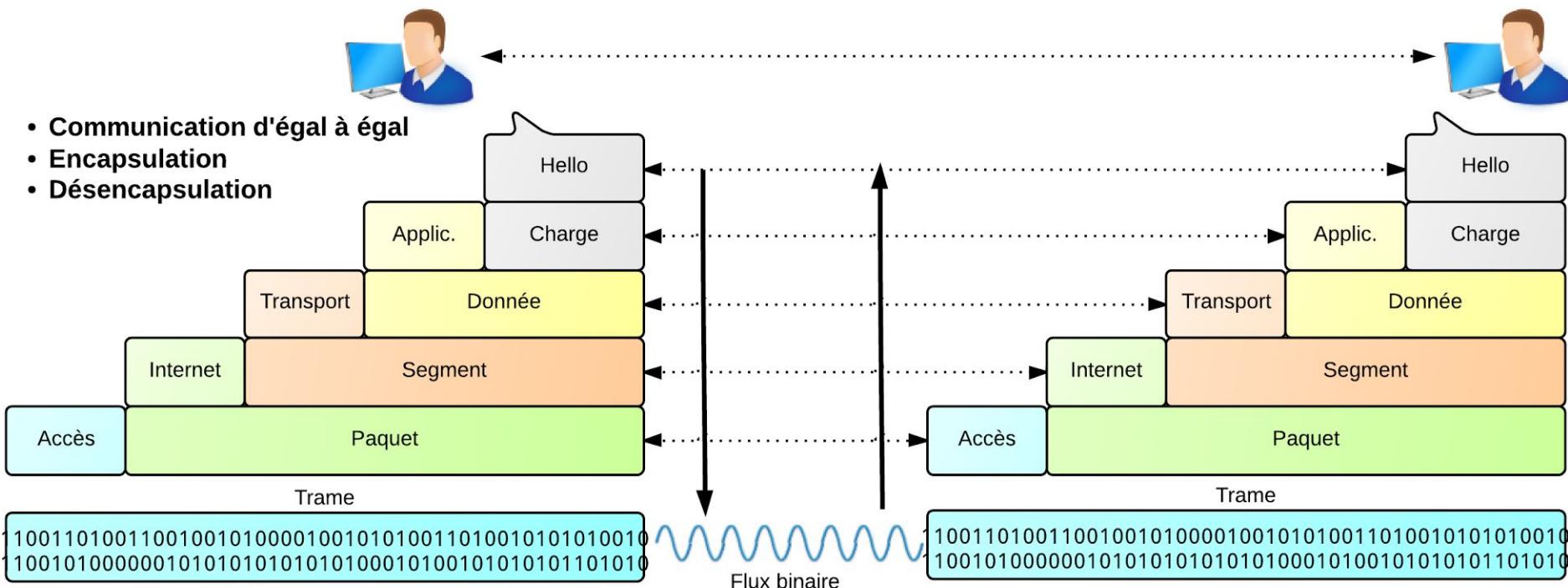
- Déterminer les modes de transmission.
- Caractériser la technologie Ethernet
- Positionner les standards Ethernet parmi les protocoles OSI, IEEE 802 et TCP/IP.
- Distinguer les notions de topologie physique et de topologie logique.
- Décrire la commutation comme une innovation.
- Distinguer technologies LAN, MAN et WAN
- Comparer les couches 1 et 2 du modèle OSI
- Distinguer les sous-couche PHY, MAC et LLC
- Distinguer les différentes normes Ethernet et leur caractéristiques

Rappels modèles OSI et TCP/IP

	Modèle OSI	Périphérique / Description	Modèle TCP/IP
7	Application	 Services applicatifs au plus proche des utilisateurs	
6	Présentation	 Encode, chiffre, compresse les données utiles	Application
5	Session	 Etablit des sessions entre des applications	
4	Transport	 Etablit, maintien et termine des sessions entre des périphériques terminaux	Transport
3	Réseau	 Adresse les interfaces globalement et détermine les meilleurs chemins à travers un inter-réseau	Internet
2	Liaison de Données	 Adresse localement les interfaces, livre les informations localement, méthode MAC	
1	Physique	 Encodage du signal, câblage et connecteurs, spécifications physiques	Accès au Réseau

Processus de communication

Chaque couche ajoute une information fonctionnelle au message original. A la réception, l'hôte examine chaque couche et prend une décision quant à ce trafic.



Modèle TCP/IP détaillé

Application

- Elle est la couche de communication qui s'interface avec les utilisateurs.
- S'exécute sur les machines hôtes terminales.

Transport

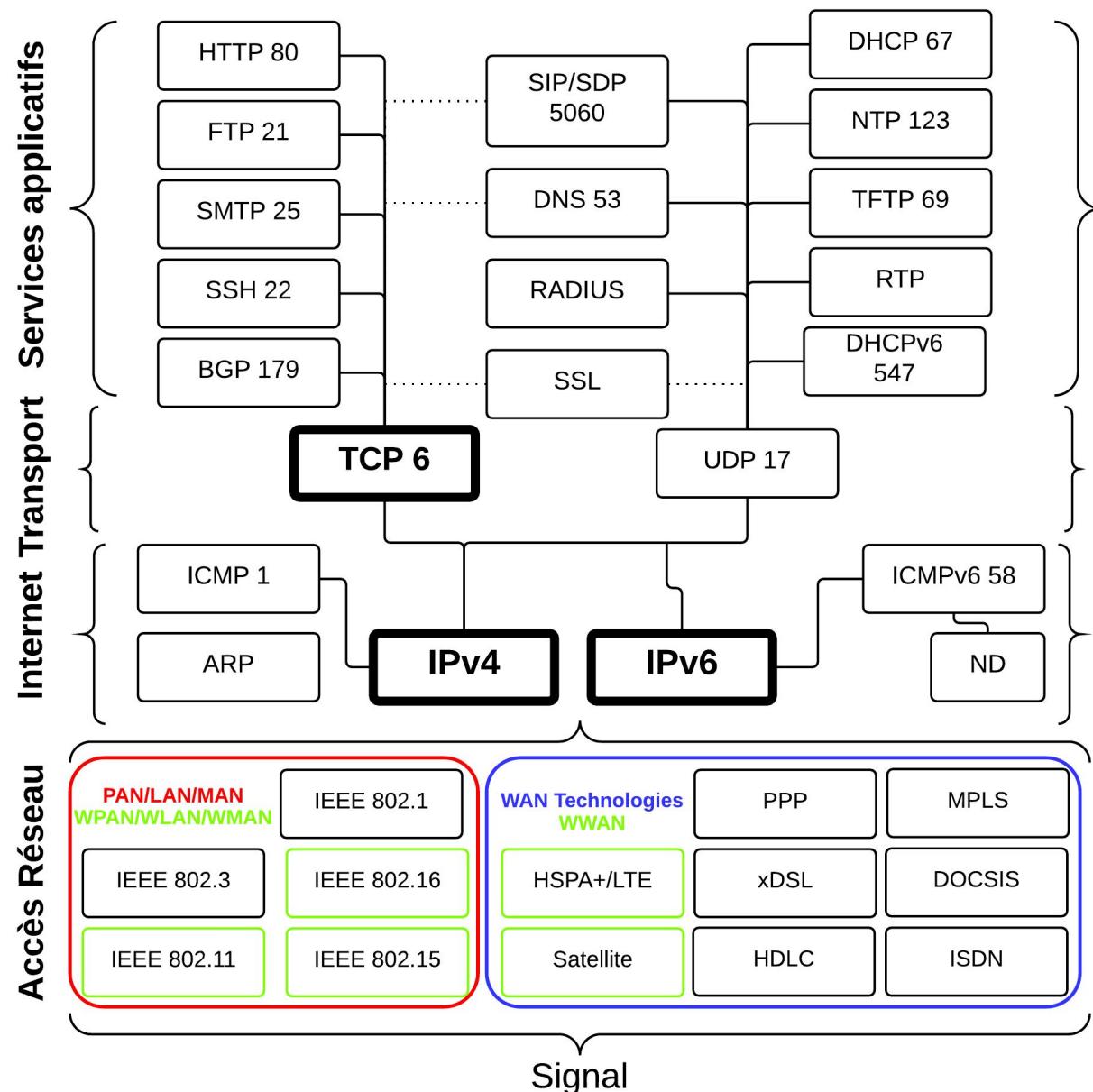
- Elle est responsable du dialogue entre les hôtes terminaux d'une communication.
- Les applications utiliseront TCP pour un transport fiable et UDP sans ce service.
- Les routeurs NAT et les pare-feu opèrent un filtrage au niveau de la couche transport.

Internet

- Elle permet de déterminer les meilleurs chemins à travers les réseaux
- Identifie globalement les interfaces
- Les routeurs transfèrent le trafic IP qui ne leur est pas destiné.

Accès réseau

- Elle organise le flux binaire
- identifie physiquement les interfaces
- Elle règle la méthode d'accès au support
- Elle place le flux binaire sur les support physique
- Commutateurs, câbles, NIC,



PDU

Chaque contenu encapsulé par une couche est une unité de donnée (Data Unit) qui prend un nom (**PDU**), **Protocol Data Unit** :

- Couche Application : **Donnée**
- Couche Transport : **Segment**
- Couche Internet : **Paquet ou Datagramme**
- Couche Accès : **Trame et Bit**

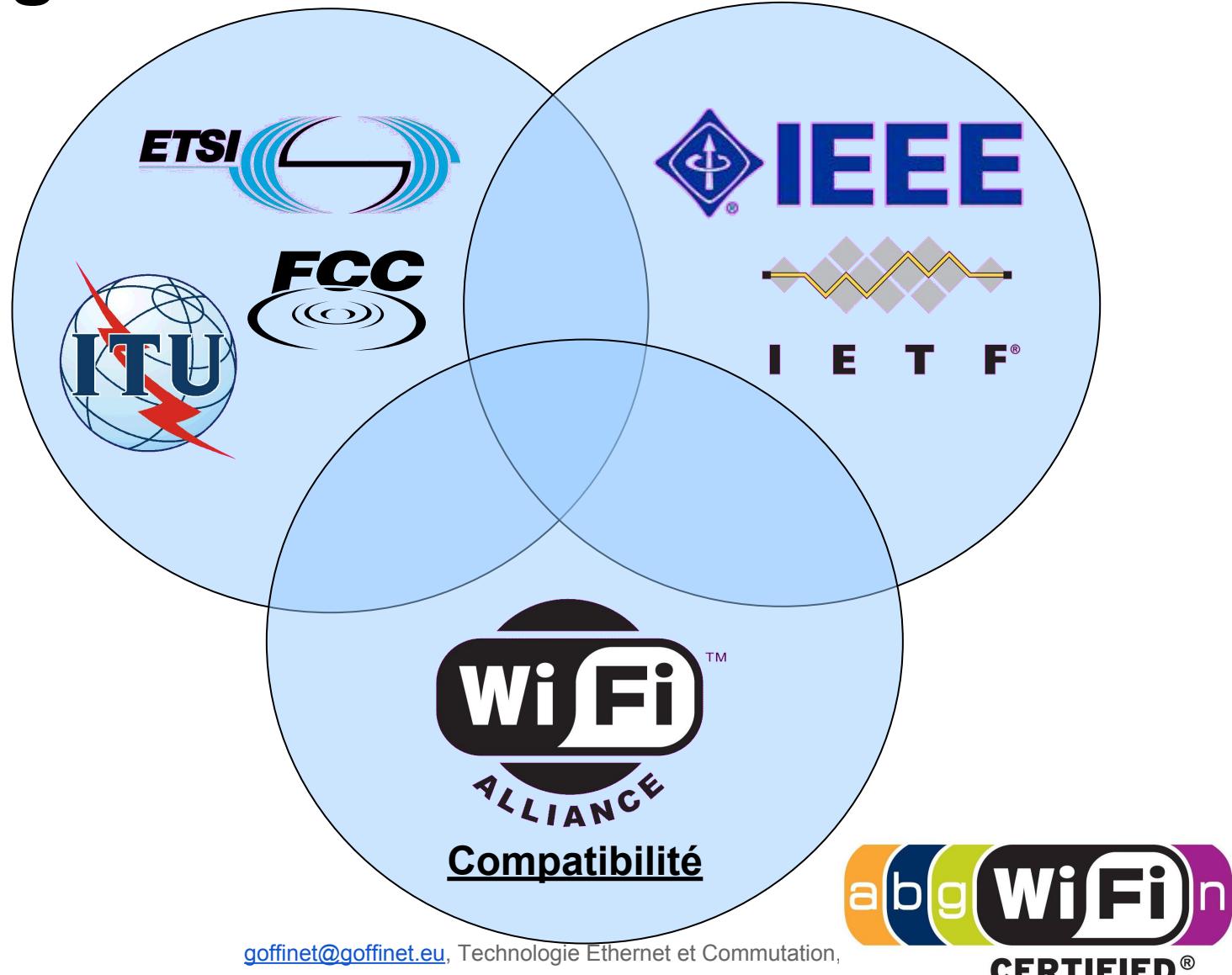
Le signal binaire contient des trames contenant des paquets contenant des segments contenant des données

Adressage et identifiants

Les machines et leurs interfaces disposent d'identifiants au niveau de chaque couche :

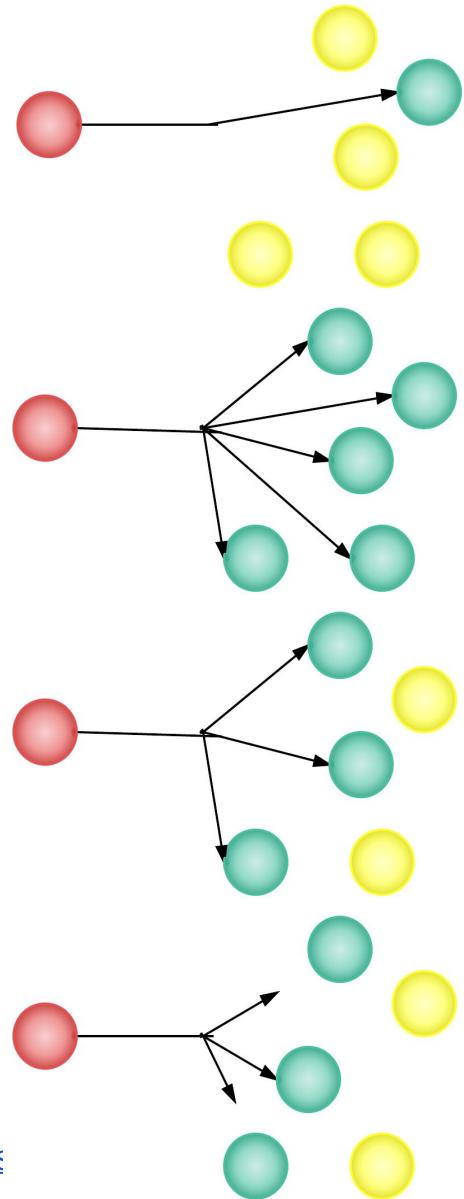
- Couche Application : **Nom de domaine**
par exemple : www.goffinet.eu
- Couche Transport : **Port TCP ou UDP**
par exemple : TCP80
- Couche Internet : **Adresse IPv4 et/ou IPv6**
par exemple : 192.168.150.252/24 ou 2001:db8::1/64
- Couche Accès : **adresse physique (MAC)**
par exemple une adresse MAC 802 : 70:56:81:bf:7c:37

Organisations de standardisation



Modes de livraison

- Unicast : à destination d'une seule interface.
- Broadcast : à destination de toutes les interfaces
- Multicast : à destination d'un ensemble (un groupe) d'interfaces
- Anycast : à destination de l'interface la plus proche



Introduction à Ethernet

Ethernet est actuellement la technologie LAN L2 dominante :

- Diversité des supports : Cuivre (paire torsadée) et Fibre
- Interopérable (vers IP, vers les protocoles IEEE 802)
- Stabilité des infrastructures (supports) / Evolutivité de la technologie (services)
- Bon marché
- Facilité de déploiement
- Fiabilité assurée par l'infrastructure et par la commutation

Caractéristiques techniques d'Ethernet

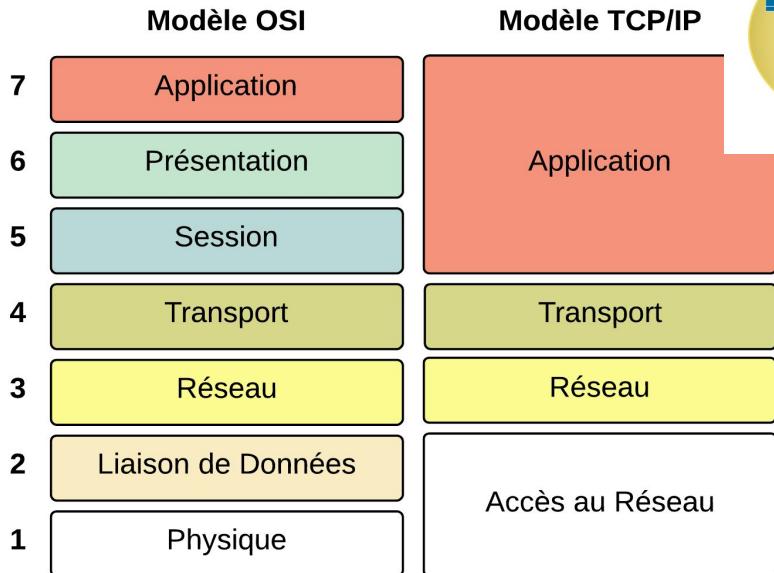
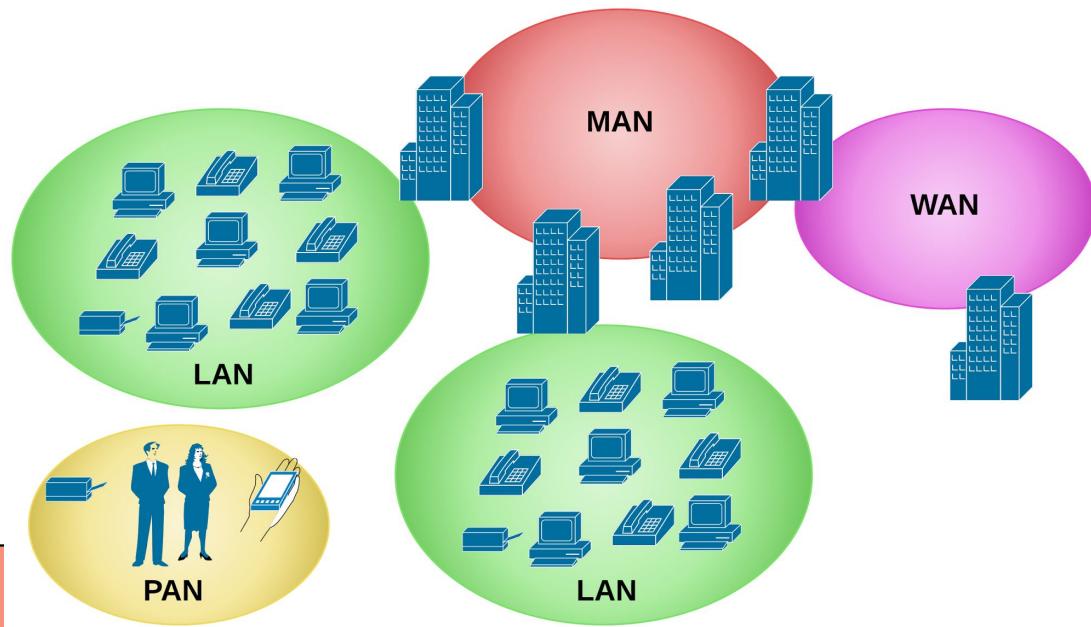
- Une technologie d'accès LAN et MAN
- Standardisé IEEE 802.3
- Aidé par IEEE 802.1 (Bridging) et IEEE 802.2 (LLC).
- de couche Liaison de données (L2) MAC : CSMA/CD
- et de couche Physique (L1)
- réputée non fiable (sans messages de fiabilité)
- non orientée connexion (pas d'établissement d'un canal préalable à la communication)

Technologie LAN et MAN

Ethernet est une technologie LAN (de réseau local).

Elle est une technologie MAN (à l'échelle d'un campus ou d'une ville).

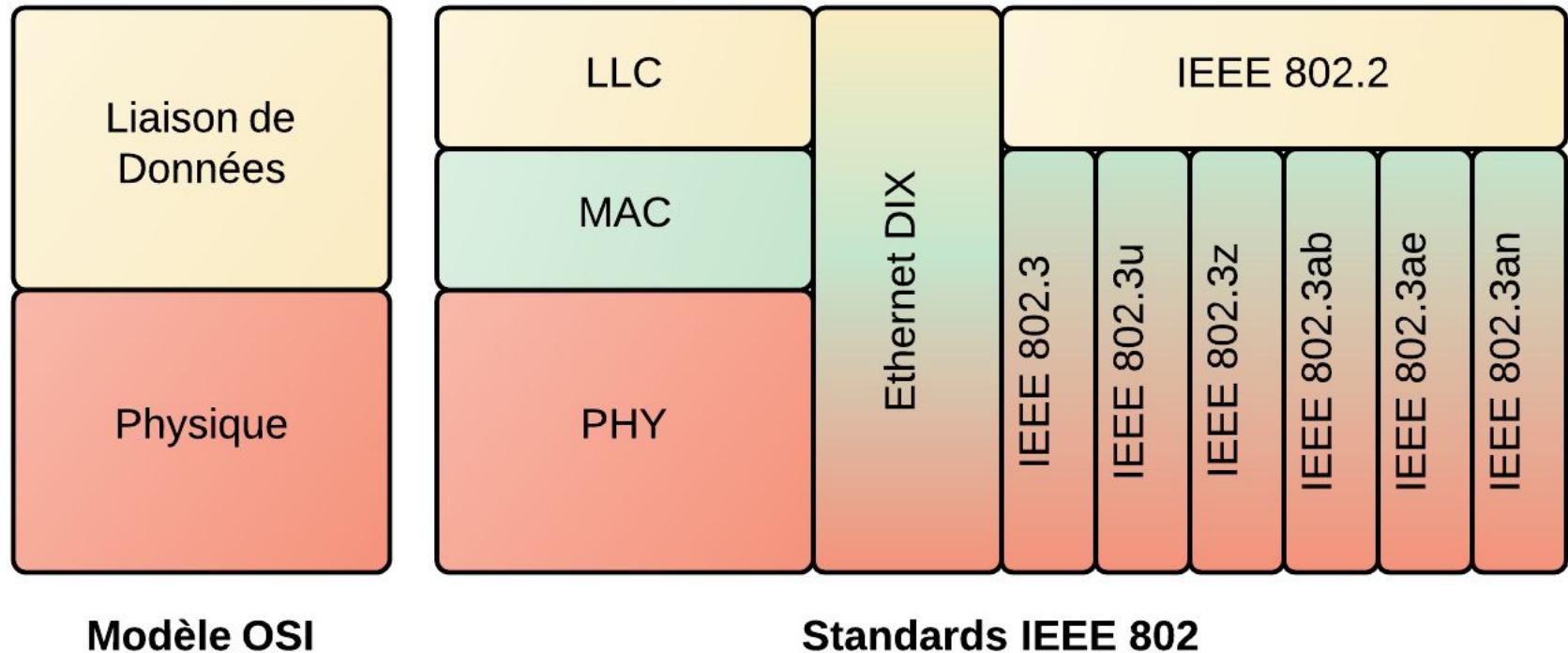
Elle peut être utilisée dans un WAN (à l'échelle du globe).



La nature PAN, LAN, MAN, WAN est une manière de qualifier une technologie d'accès selon :

- **la portée**
- **et la vitesse.**

Standard Ethernet/Modèle OSI

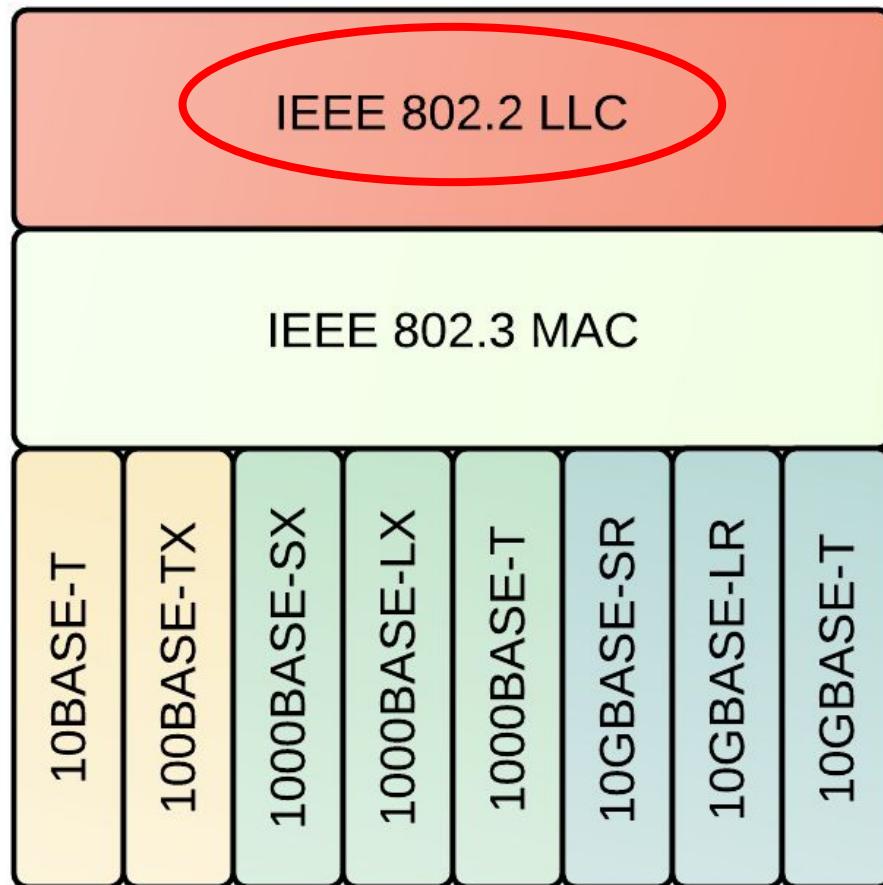


Le standard IEEE 802.3 couvre les deux basses couches du modèle OSI : PHY et MAC. LLC IEEE 802.2

Comparaison couche 1 / couche 2

Couche 1	Couche 2
Ne peut pas communiquer avec les couches supérieures	Se connecte aux couches supérieures grâce à LLC (Logical Link Control)
Ne peut pas identifier les périphériques	Utilise un adressage physique, non hiérarchique, non routable pour identifier les périphériques.
Ne reconnaît qu'un flux binaire	Utilise des trames pour organiser les données
Ne peut pas déterminer la source d'une transmission quand plusieurs périphériques transmettent	Utilise le protocole MAC pour identifier les sources des transmissions

Sous-couche LLC

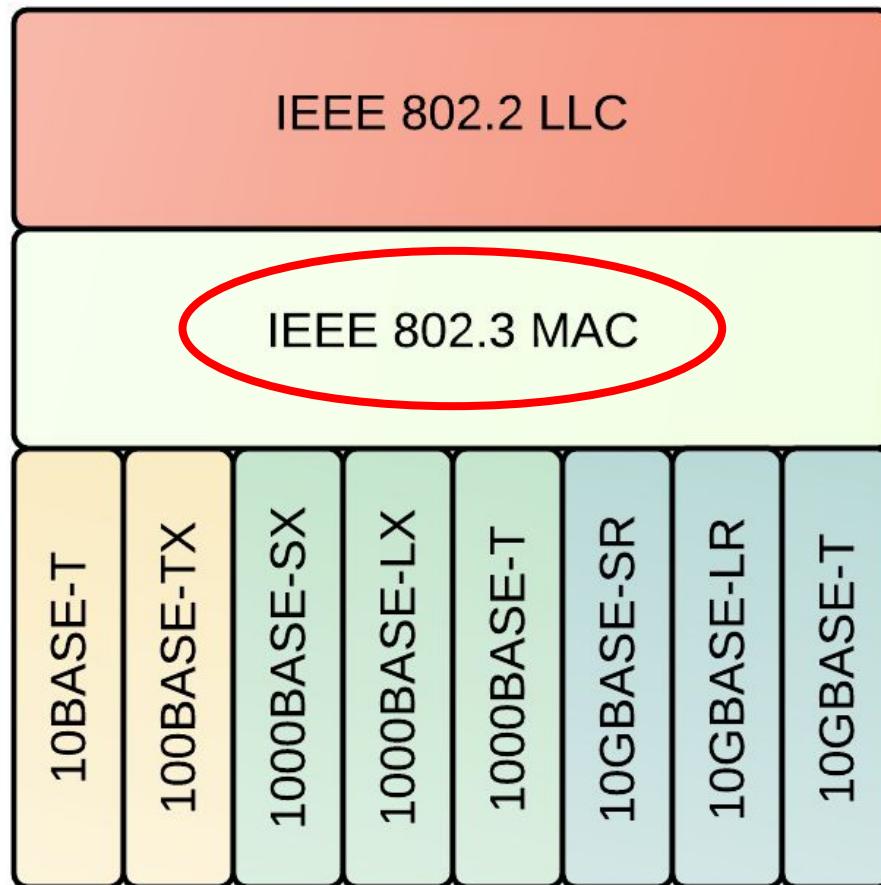


Logic Link Control –
se connecte aux
couches supérieures.

En ajoutant un champ
type, il identifie le
protocole de couche
supérieure.

Indépendant de la
couche physique

Sous-couche MAC



Media Access Control – encapsule les données.

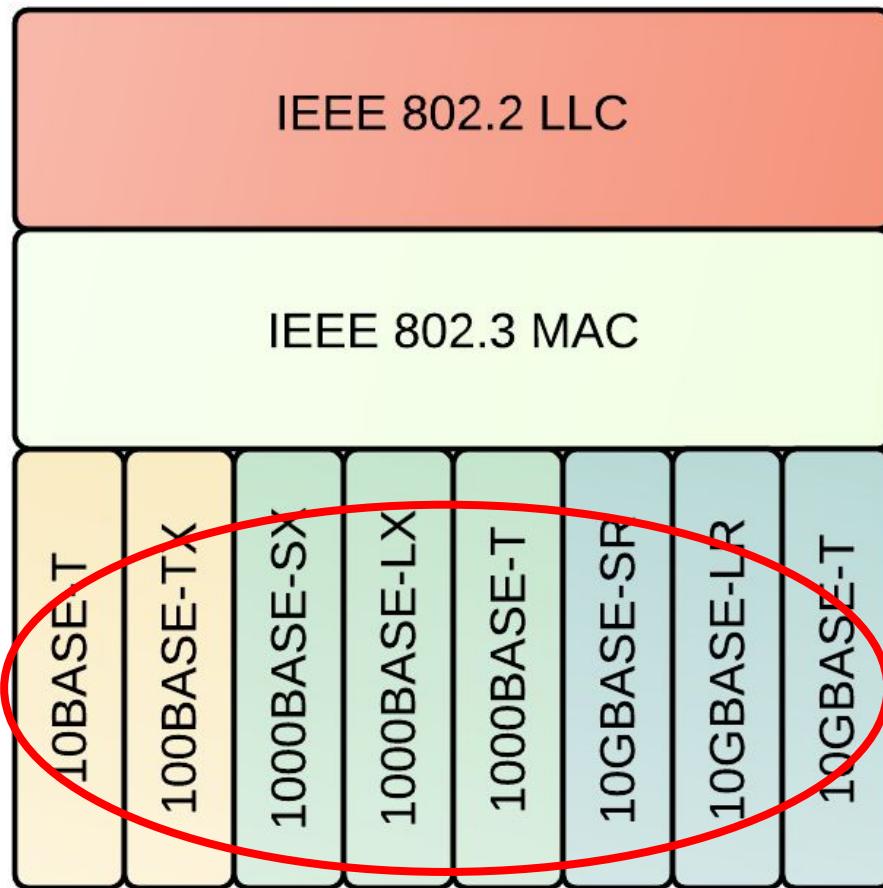
- Délimite les trames
- Adressse les périphériques
- Détecte les erreurs

Media Access Control – contrôle l'accès au support.

- Détermine le placement sur le support
- Reprise sur erreur sur le support

Sous-couches physiques

Implémentation physique d'Ethernet



La couche physique d'Ethernet est décomposée en différentes sous-couches PHY qui assurent l'interopérabilité des supports physiques, des connecteurs, s'occupe des bandes de fréquences ...

Synthèse des normes Ethernet

Nom commercial	Vitesse	Dénomination physique	Standard	Support, longueur
Ethernet	10 Mbps	10BASE-T	IEEE 802.3	Cuivre, 100 m
Fast Ethernet	100 Mbps	100BASE-TX	IEEE 802.3u	Cuivre, 100 m
Gigabit Ethernet	1 Gbps	1000BASE-SX, 1000BASE-LX	IEEE 802.3z	Fibre, 550 m, 5 Km
Gigabit Ethernet	1 Gbps	1000BASE-T	IEEE 802.3ab	Cuivre, 100 m
10Gigabit Ethernet	10 Gbps	10GBASE-SR, 10GBASE-LR	IEEE 802.3ae	Fibre, 300 m, 25 Km
10Gigabit Ethernet	10 Gbps	10GBASE-T	IEEE 802.3an	Cuivre, 100 m

Matériel et transfert de trafic

Prise de décision quant au transfert du trafic sur le bon port de sortie :

- **Routeur**

En fonction de l'adresse IP de destination du paquet
On parle de **routage (IP routing)**.

- **Commutateur (switch)**

En fonction de l'adresse MAC destination de la trame
On parle de **commutation (LAN switching)**

- **Concentrateur (Hub)**

Propage le signal par tous ses ports

2. Câblages, connecteurs, NIC

Ethernet et Commutation

Objectifs

- Concevoir et diagnostiquer un câble UTP
- Interconnecter les périphériques du réseau avec les câbles appropriés
- Distinguer les différents type de connecteurs et de câbles Fibre Optique
- Choisir des connexions fibre 10GE

Câblage à paires torsadées

1 Les types de blindages

- 1.1 Paire torsadée non blindée
- 1.2 Paire torsadée écrantée
- 1.3 Paire torsadée blindée
- 1.4 Paire torsadée écrantée et blindée
- 1.5 Paire torsadée super blindée
- 1.6 Table de récapitulative avec les nouvelles dénominations (norme ISO/IEC 11801)

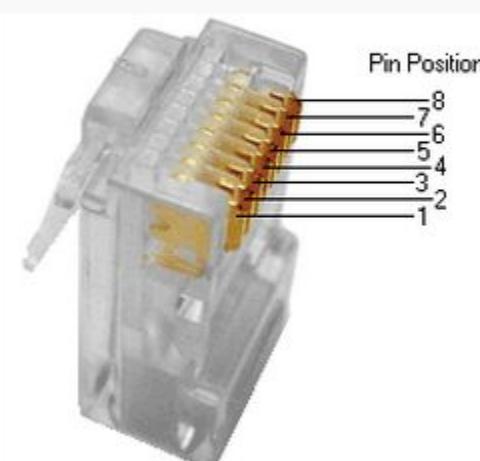
2 Les catégories de câbles

- 2.3 Catégorie 3
- 2.5 Catégorie 5
- 2.6 Catégorie 5e / classe D
- 2.7 Catégorie 6 / classe E
- 2.8 Catégorie 6a / classe Ea
- 2.10 Catégorie 7a / classe Fa

TIA/EIA 568

Connecteur RJ-45

Pin	T568A Pair	T568B Pair	1000BASE-T Signal ID	Wire	T568A Color	T568B Color	Pins on plug face (socket is reversed)
1	3	2	DA+	tip	white/green stripe	white/orange stripe	
2	3	2	DA-	ring	green solid	orange solid	
3	2	3	DB+	tip	white/orange stripe	white/green stripe	
4	1	1	DC+	ring	blue solid	blue solid	
5	1	1	DC-	tip	white/blue stripe	white/blue stripe	
6	2	3	DB-	ring	orange solid	green solid	
7	4	4	DD+	tip	white/brown stripe	white/brown stripe	
8	4	4	DD-	ring	brown solid	brown solid	

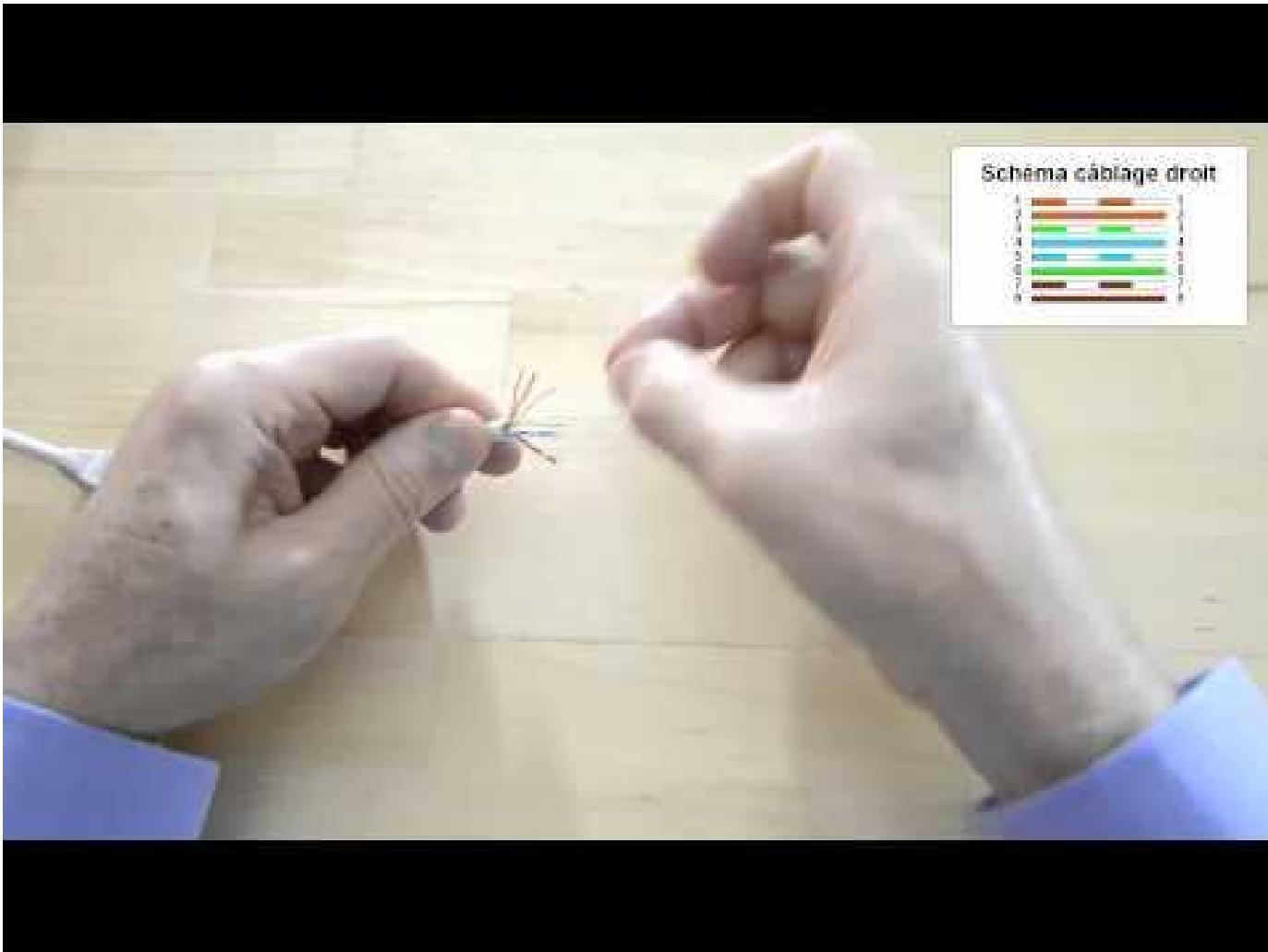


The diagram shows a perspective view of an RJ-45 connector. Eight gold-colored pins are visible on the right side. Lines extend from each pin to a numerical label indicating its position: 1, 2, 3, 4, 5, 6, 7, and 8. The pins are arranged in two rows of four, with the top row being the inner pins (1, 2, 3, 4) and the bottom row being the outer pins (5, 6, 7, 8).

Pin Position

8
7
6
5
4
3
2
1

Réalisation de câble UTP droit



Prise murale Ethernet



Diagnostic physique

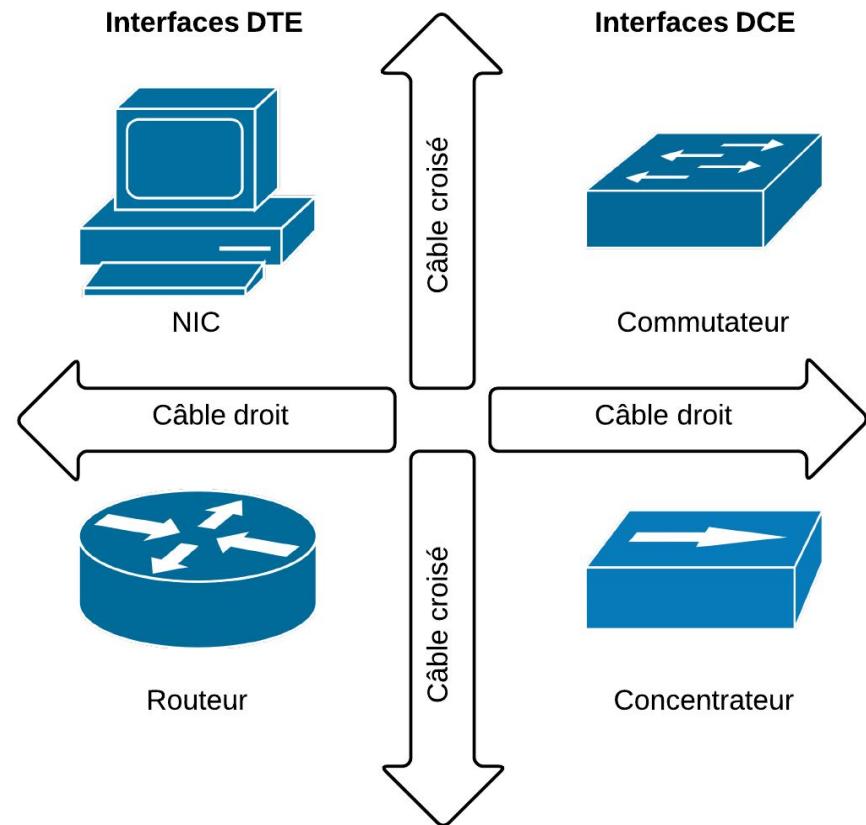
- Erreurs et certification de câblage.
- Câblage structuré

DCE/DTE

Les **commutateurs** (switches) et **concentrateurs** (hubs) sont identifiés comme ayant des interfaces **DCE** (Data Connexion Equipment) alors que les **stations terminales** et les **routeurs** sont des périphériques **DTE** (Data Terminal Equipment).

Les **équipements identiques** DTE/DTE ou DCE/DCE se connectent avec un **câble croisé** (qui croise les paires d'émission et de réception).

Les **équipements de type différent** se connectent avec un **câble droit** car la position émission réception sur leur interface est déjà inversée.



Vitesse et mode

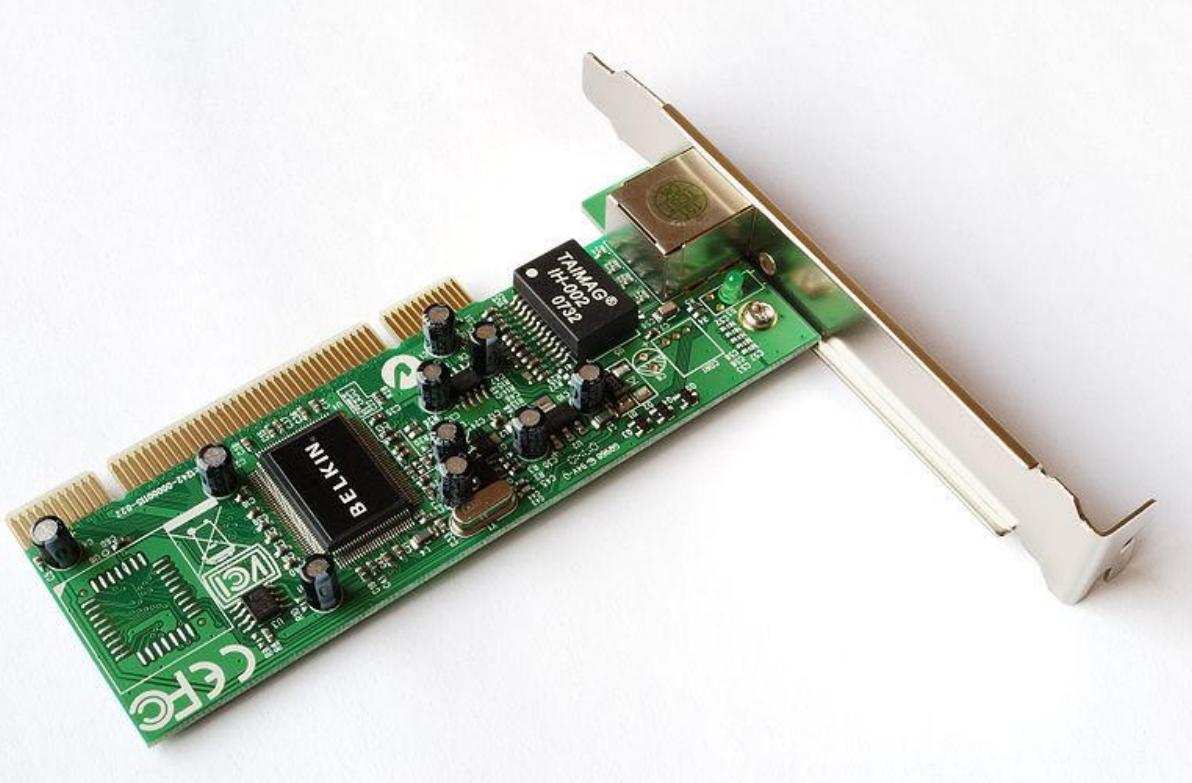
La vitesse entre interfaces est fixée par négociation (impulsion PHY) pour déterminer le mode Half/Full Duplex et la vitesse sur des valeurs compatibles.

L'auto-négociation est activée par défaut. Si on fixe ces paramètres, ils doivent être identiques de part et d'autre.

La [fonction auto-MDIX](#) reconnaît automatiquement le type de câble utilisé.

Network Interface Card

Une carte d'interface réseau (NIC) est un matériel de couche 1 et 2.



Technologies Fibre Optique

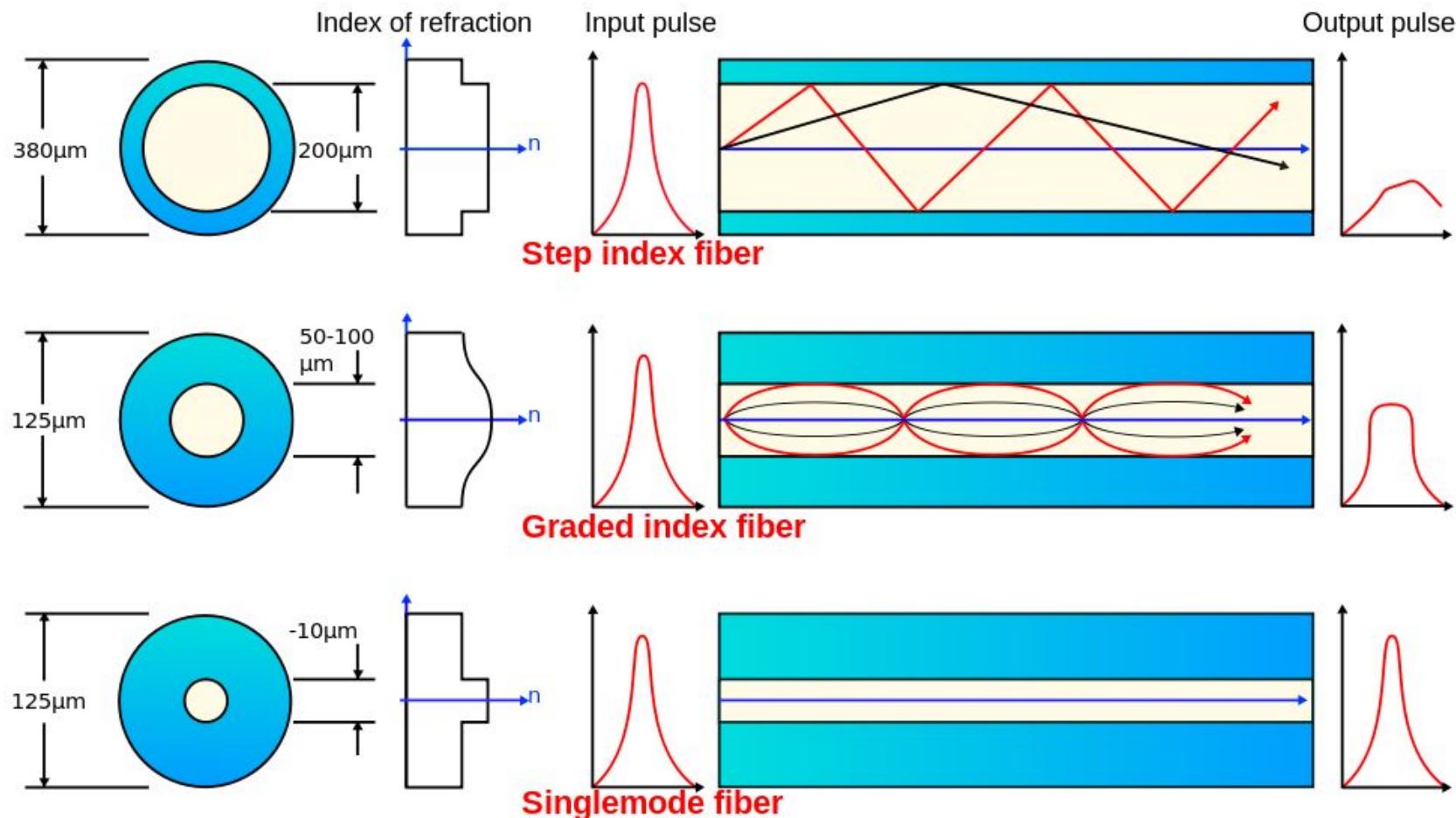
La fibre multimode

Les rayons lumineux peuvent suivre des trajets différents suivant l'angle de réfraction. Les rayons peuvent donc arriver au bout de la ligne à des instants différents, d'une certaine dispersion du signal. Elles sont généralement utilisées pour de courtes distances, elles ont pour émetteur une diode électroluminescente et des performances d'environ 1 gigabits/Km. La fibre multimode est généralement utilisée pour de courte distance (de l'ordre de la centaine de mètre). Elle est la plus employée pour les réseaux privés.

La fibre monomode

Les rayons suivent un seul chemin. Elle a le coeur si fin (de l'ordre de la longueur d'onde du signal transmis) que le chemin de propagation des différents modes est pratiquement direct. La dispersion du signal est quasiment nulle, le signal est donc très peu déformé. Ses performances sont d'environ 100 gigabits/km, l'indice de réfraction peut être constant ou décroissant. Cette fibre est utilisée essentiellement pour les sites à distance. Le petit diamètre du coeur nécessite une grande puissance d'émission, donc des diodes au laser qui sont relativement onéreuses (ce qui rend la fibre monomode plus chère que la fibre multimode). Du fait de ses débits très importants, mais de son coût élevé, cette fibre est utilisée essentiellement pour les sites à grande distance et très grande distance.

Technologies Fibre Optique



Connecteurs Fibre Optique



FC connector



E2000 connector



ESCON connector



LC connector (duplex)



LuxCis connector



MIC (FDDI) connector



MPO connector



MT-RJ connector



SC connector



SC connector (duplex)



SMA 905 connectors



ST connector



TOSI INK connector

3. Méthode d'accès MAC CSMA/CD

Ethernet et Commutation

Objectifs

- Distinguer les notions de topologie physique et de topologie logique
- Distinguer les différentes méthodes d'accès au support (MAC)
- Caractériser la méthode MAC d'Ethernet
- Expliquer le fonctionnement de CSMA/CD
- Expliquer la notion de délai dans le fonctionnement d'Ethernet

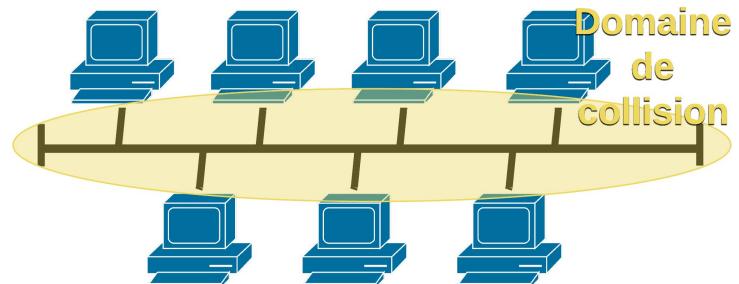
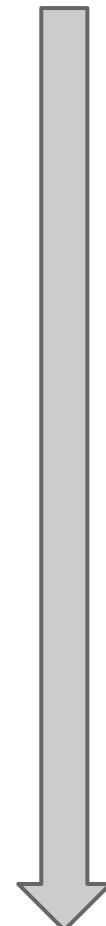
Méthode d'accès MAC

La topologie logique est la méthode d'accès (MAC) au support physique. On distingue :

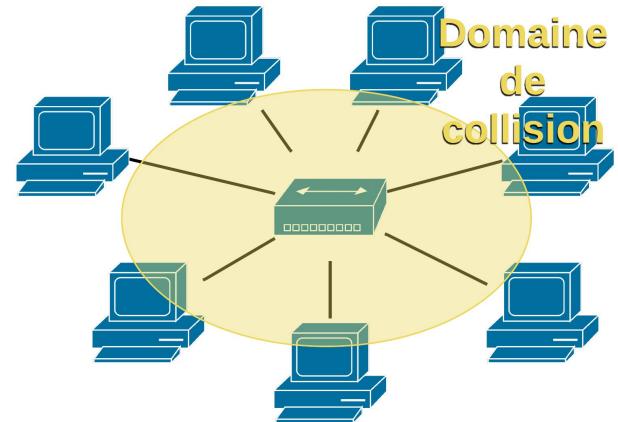
- Les méthodes stochastiques, premier arrivé premier servi (Ethernet, Wi-Fi).
- Les méthodes déterministes, par passage de jeton, contrôlé (Token-Ring).

Topologie physique et topologie logique

- Topologie physique et logique en bus : coaxial
- Topologie physique en étoile et topologie logique en bus : paire torsadée (8 fils).
- supports cuivres et fibre
- vitesse >100Mb/s
- Aujourd'hui 10Gb/s sur cuivre/fibre



Topologie Physique	Topologie logique	Technologie
Bus	Bus	10Base5 10Base2



Topologie Physique	Topologie logique	Technologie
Etoile	Bus	10BaseT 100BaseT

Révolution de la commutation

- Les commutateurs ont révolutionné les LANs grâce à un **transfert rapide et dédié**.
- L'infrastructure (le matériel) prend en charge la fiabilité, la gestion, le transfert rapide du trafic ...
- Le protocole interface physiquement (PHY) et assure la livraison du trafic sur le support (MAC)



Topologie Physique	Topologie logique	Technologie
Etoile Hiérarchique Maillée	Commutée Segmentée	10/100/1000BASE-TX 1000BASE-SX/LX 10GBASE-T/SR/LR/LRM

CSMA/CD

La méthode d'accès MAC est appelée :

Carrier Sense Multiple Access with Collision Detection
(CSMA/CD) :

- Principe premier arrivé premier servi.
- Si le canal est libre, la station place son trafic.
- Si ce n'est pas le cas, elle attend.
- Le protocole se propose de gérer les collisions.
- Pas de fonction de fiabilité (ACK), pas de fonctions de gestions d'erreur, de contrôle de flux, etc.
- **CSMA/CD = Ethernet Legacy (10BASE2, 10BASE5, 10BASE-T)**

Principe CSMA (Carrier Sense Multiple Access)

1. Une interface qui tente de placer une trame écoute le support.
2. En cas de porteuse, elle retarde le placement de la trame.
3. En l'absence de porteuse (support libre), elle attend encore quelques instants (96 Bit Time) et commence à placer le trafic.
4. Elle va rester attentive à d'éventuelles collisions pendant un certain délai appelé le "slot time" (512 Bit Time).
5. Après expiration de ce délai, l'interface n'est plus attentive à d'éventuelles collisions. Elle considère le canal acquis. Elle continue à émettre sans plus rien attendre (pas de ACK).
6. Sur un media partagé, quelle que soit la topologie physique, toutes les interfaces reçoivent ce trafic. Elles examinent toutes l'en-tête Ethernet du trafic reçu, ce qui suscite de la charge en CPU et en bande passante.
7. Seule l'interface qui reconnaît son adresse MAC dans le champ destination livre la trame à la couche supérieure.

Gestion des collisions

Sur un support partagé, une collision peut survenir lorsque deux ou plusieurs interfaces tentent de placer une trame en même temps alors qu'elles ont constaté un support libre (absence de porteuse).

Parce qu'il faut un certain délai pour qu'une trame arrive d'une extrémité à l'autre du support, l'interface émettrice va rester attentive pendant ce temps à d'éventuelles collisions. Les standards 802.3 définissent précisément ce temps. Il est appelé le slot time. Jusqu'en 100 Mbps, il s'agit du temps de placement de 512 bits ou 64 octets.

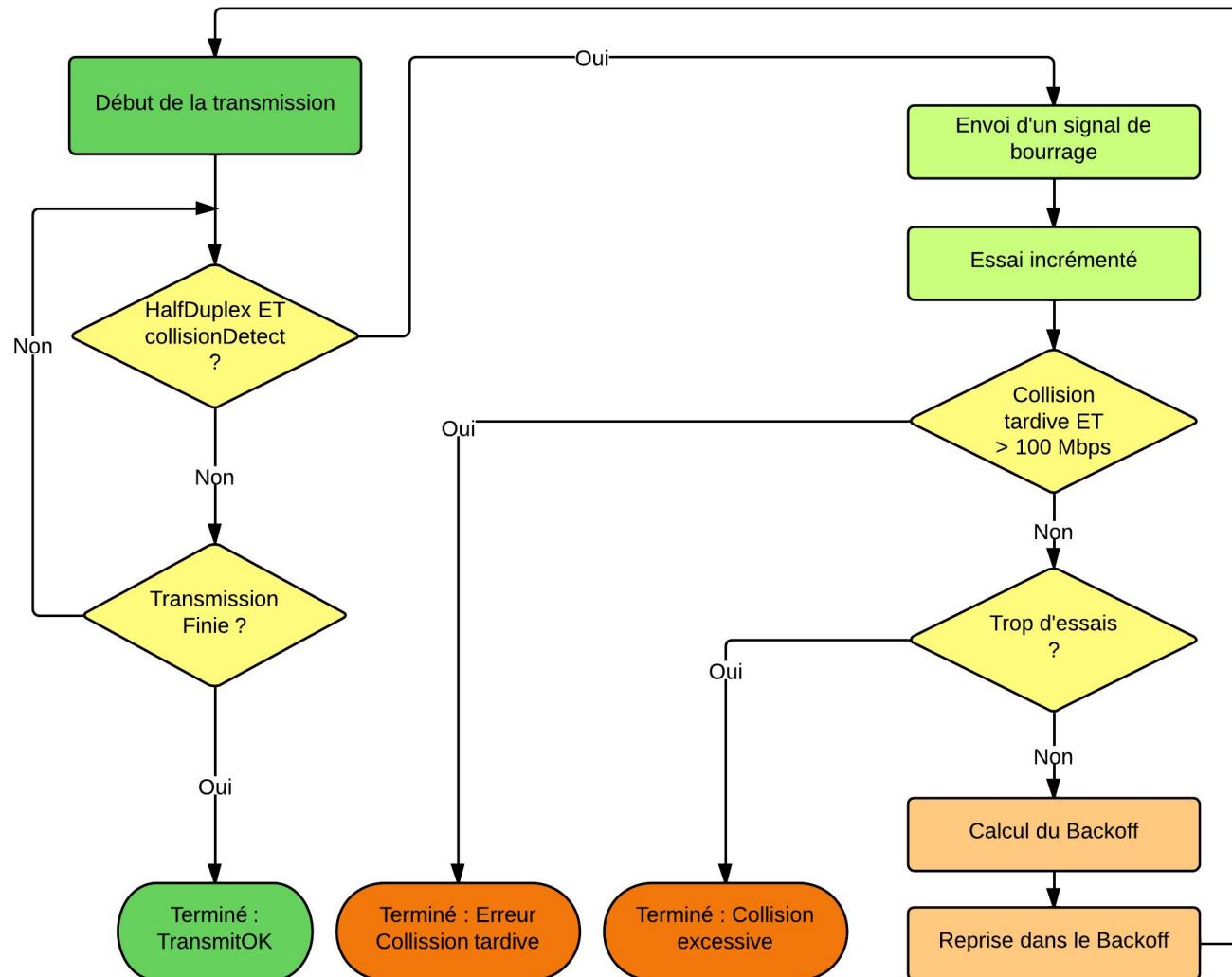
1. En cas de collision, les stations impliquées la renforcent en envoyant un signal de bourrage afin de que toutes les interfaces du réseau l'entende.
2. Elles attendent alors de reprendre la procédure de placement de la trame dans un délai aléatoire. C'est ce qu'on appelle le mécanisme de Backoff prévu par le protocole.
 - a. Précisément, les stations impliquées reprennent aléatoirement dans une fourchette variant de 0 à un multiple du slot time.

Le support partagé par du matériel de couche 1 (Hub, concentrateur, câble en bus) est appelé domaine de collision. La bande passante est partagée dans un domaine de collision.

Délais

Les délais dans la technologie Ethernet dépendant de la qualité de l'infrastructure : on comprendra comment est déterminé la taille maximale d'un segment Ethernet seulement avec une répétition de signal ou un câblage incorrect.

Algorithme CSMA/CD



4. Adressage et tramage

Ethernet et Commutation

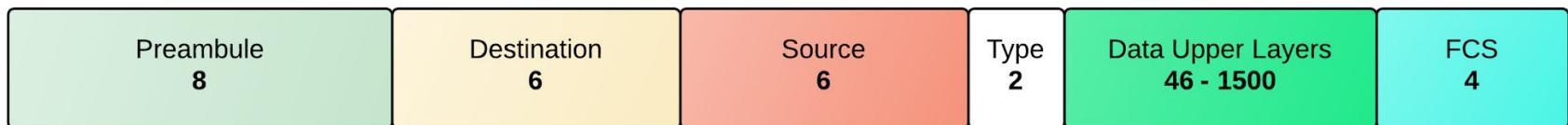
Objectifs

- Distinguer les différentes trames Ethernet
- Dénombrer, citer et expliquer les différents champs d'une trame Ethernet/IEEE 802.3
- Définir et caractériser l'adresse MAC IEEE 802
- Expliquer le processus d'encapsulation et de désencapsulation à travers un inter-réseau.

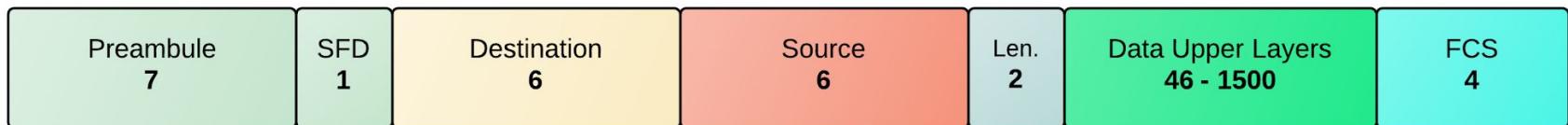
Format des trames Ethernet

- 3 formats de trames DIX et IEEE 802.3 :

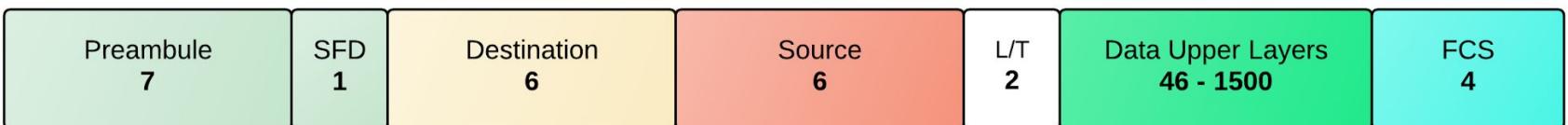
DIX



IEEE 802.3 original



IEEE 802.3 révisé



Ethertype

Valeurs du champ "Type" :

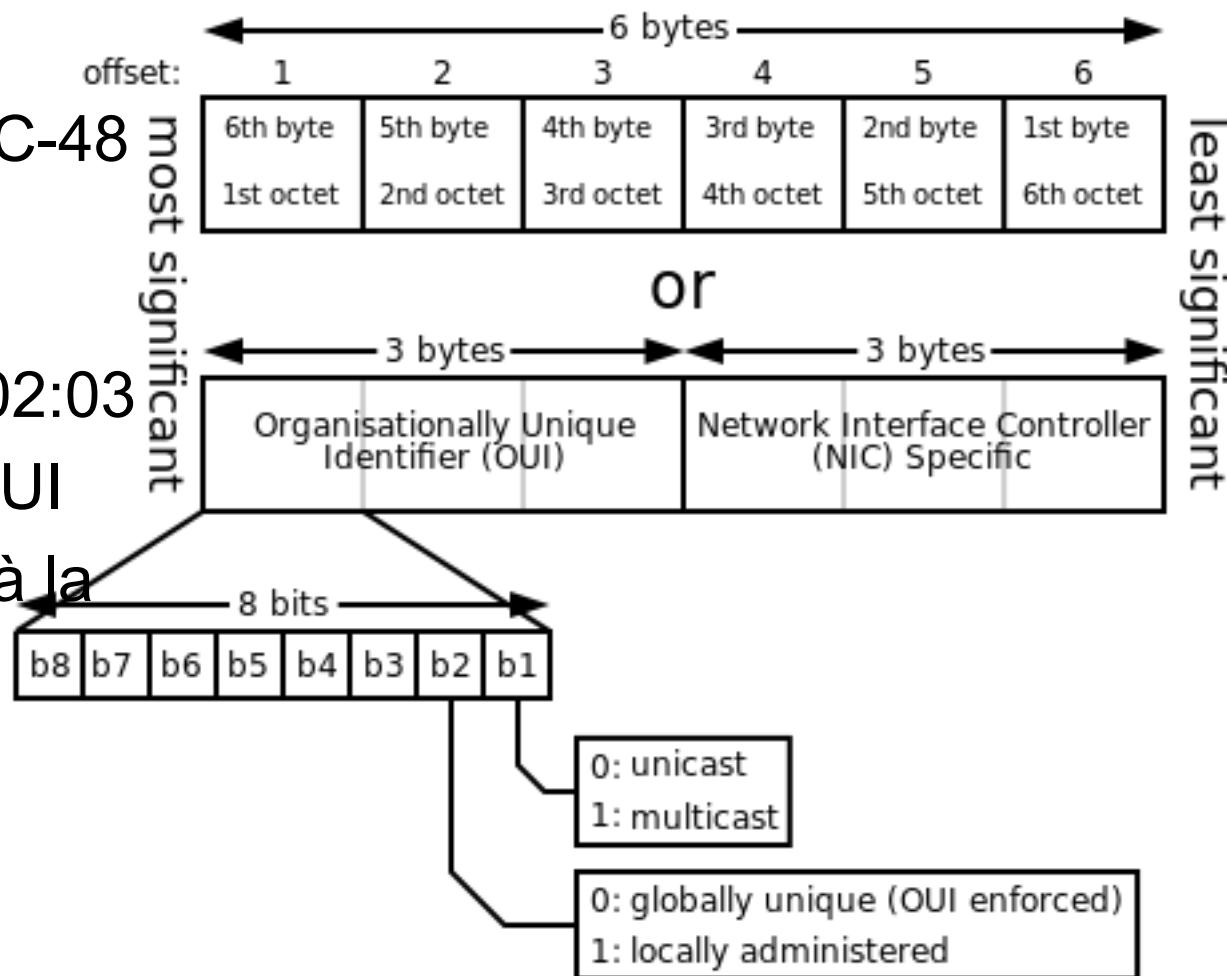
- 0x0800 Internet Protocol version 4 (IPv4)
- 0x0806 Address Resolution Protocol (ARP)
- 0x8100 VLAN-tagged frame (IEEE 802.1Q)
- 0x86DD Internet Protocol Version 6 (IPv6)
- 0x8847 MPLS unicast
- 0x8848 MPLS multicast
- 0x8863 PPPoE Discovery Stage
- 0x8864 PPPoE Session Stage
- 0x8870 Jumbo Frames
- 0x888E EAP over LAN (IEEE 802.1X)
- 0x9100 Q-in-Q

Adressage IEEE 802

- L'adresse MAC IEEE 802 permet de distinguer les périphériques qui communiquent sur le réseau **local**
- Elle sert uniquement à livrer le trafic **localement**
- Elle est censée être unique
- Ce n'est pas un adressage hiérarchique et non routable (comme IP)
- Est fondée dans les cartes réseau, mais peut être émulée.

Adressage de couche 2

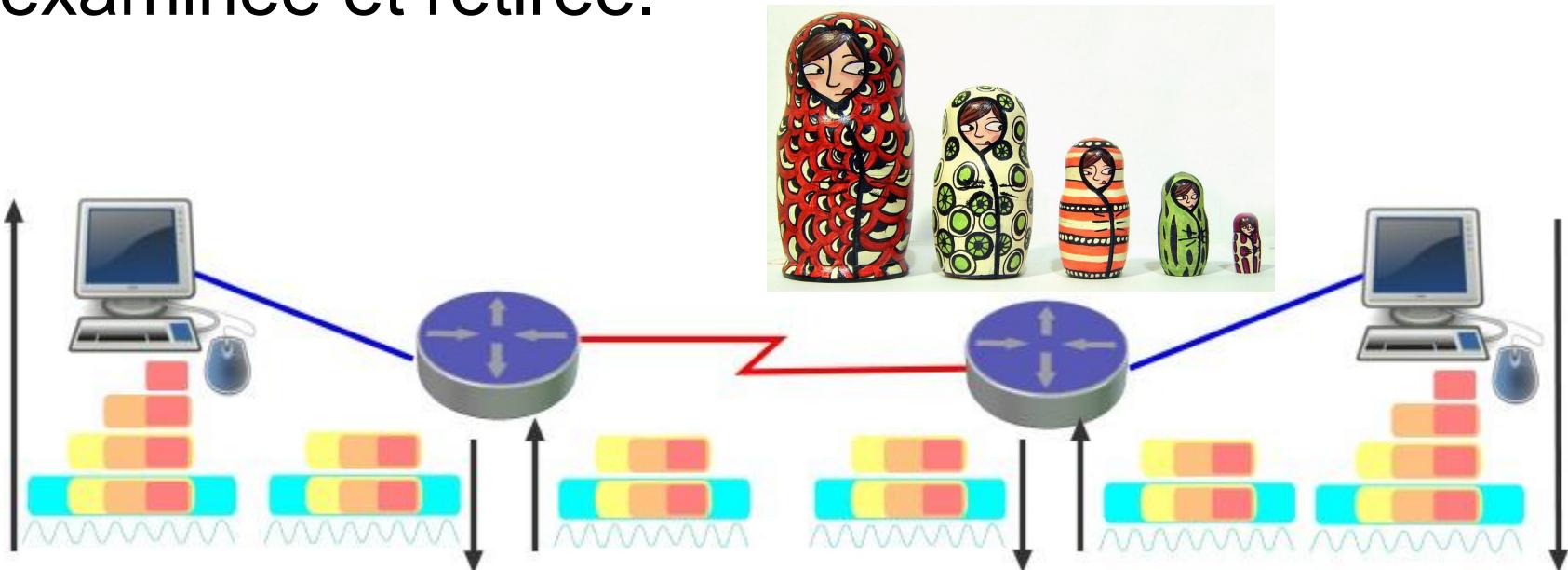
- Adressage MAC-48 IEEE 802
- 48 bits
- AA:BB:CC:01:02:03
- 24 bits pour l'OUI
- 24 bits laissés à la discrédition des fabricants



Encapsulation et désencapsulation

Chaque couche ajoute des informations fonctionnelles et utiles à la transmission.

A la réception, chacune de ces informations est examinée et retirée.



Activités

- Capture et interprétation de trames Ethernet.
- Comment modifier l'adresse MAC d'une interface ?
- Consultation et interprétation des tables ARP, CAM, de routage
- A quelle couche du modèle TCP/IP se situe le protocole ARP ?

Conclusion

- Protocole de couche liaison de données (L2) et de couche physique (L1)
- Non orienté-connexion
- Non fiable
- Méthode d'accès libérale, stochastique, "premier arrivé, premier servi" = topologie logique
- Support à accès partagé = bande passante et trafic partagé

5. Commutation et Commutateurs

Ethernet et Commutation

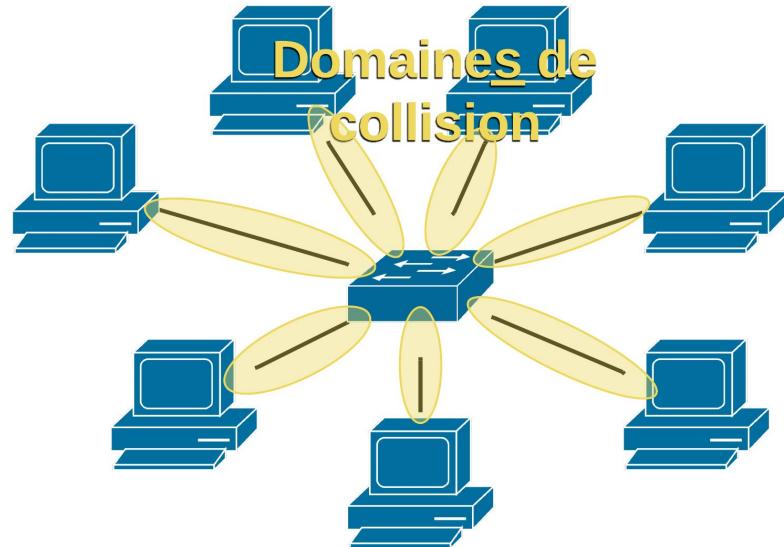
Objectifs du chapitre 5

- Expliquer le processus de *transfert de trame* dans un réseau commuté.
- Différencier différentes méthodes de commutation.
- Comparer un *domaine de collision* à un *domaine de diffusion*.

Principe de la commutation

- Grâce à une table de commutation apprise par écoute, le commutateur identifie un port à une adresse et transfert le trafic sur base de ce critère.
- Lorsqu'il ne connaît pas le port pour une destination (unicast inconnu, broadcast, multicast), il transfert ce trafic par tous les ports sauf le port d'origine.

Port de commutateur	Adresse MAC apprise
F0/1	00:00:00:00:00:01
F0/2	00:00:00:00:00:02
F0/3	00:00:00:00:00:03
F0/4	00:00:00:00:00:04

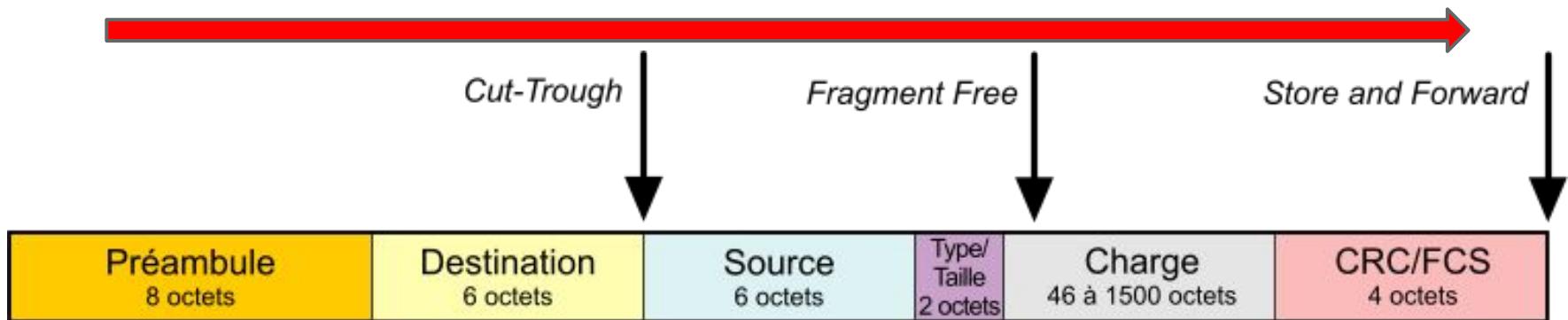


Topologie Physique	Topologie logique	Technologie
Etoile Hiérarchique Maillée	Commutée Segmentée	10/100/1000BASE-TX 1000BASE-SX/LX 10GBASE-T/SR/LR/LRM

Méthode de commutation

Moment auquel le commutateur transfère le trafic vers un port de sortie :

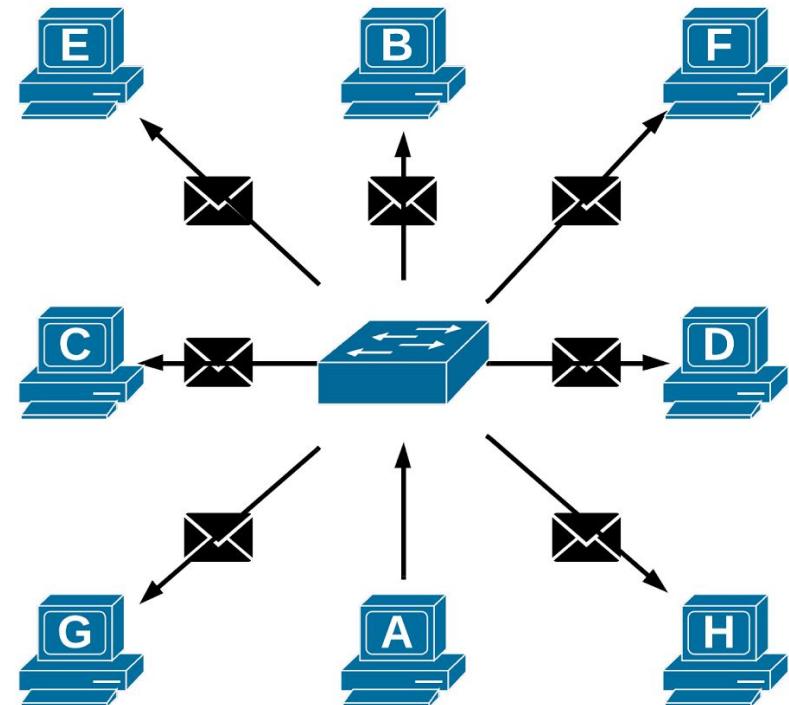
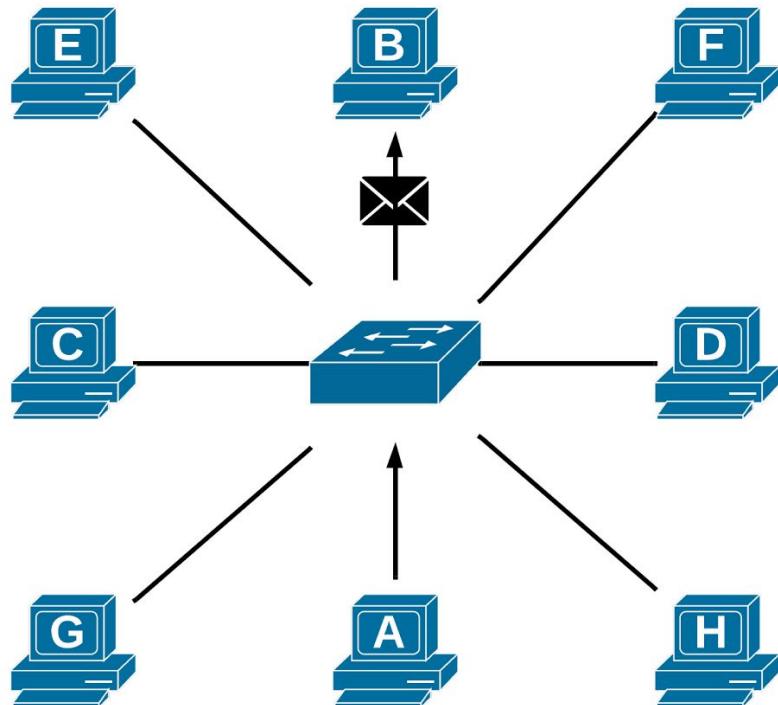
Lenteur



Le commutateur dispose de puces (ASIC) qui prennent les décisions de transfert et de mémoires tampon dédiées

Domaine de diffusion/collision

- Un domaine de collision par port de commutateur.
- Un commutateur étend un domaine de diffusion.
- Un routeur filtre et connecte des domaines de diffusion.



L'hôte A émet du trafic *unicast* à destination de B

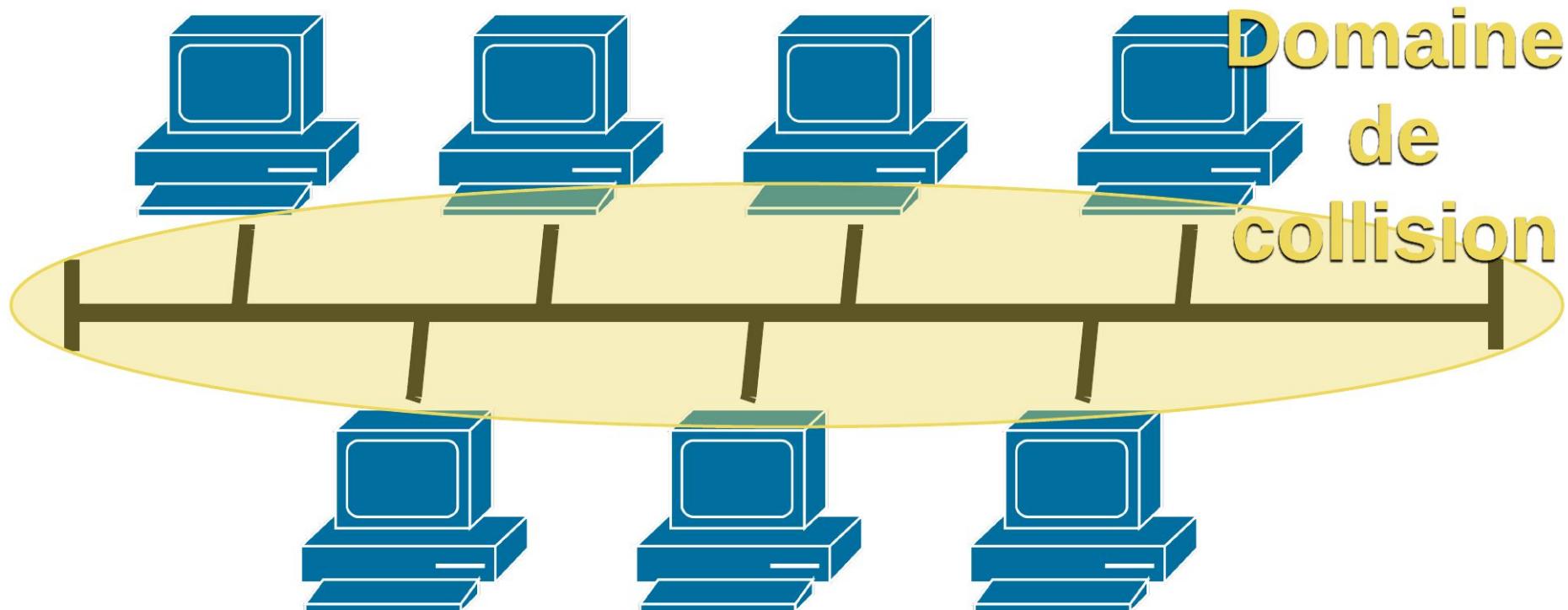
L'hôte A émet du trafic *broadcast ou multicast*

Half-duplex/Full-Duplex

La microsegmentation (un port de commutateur = une poste de travail) va offrir :

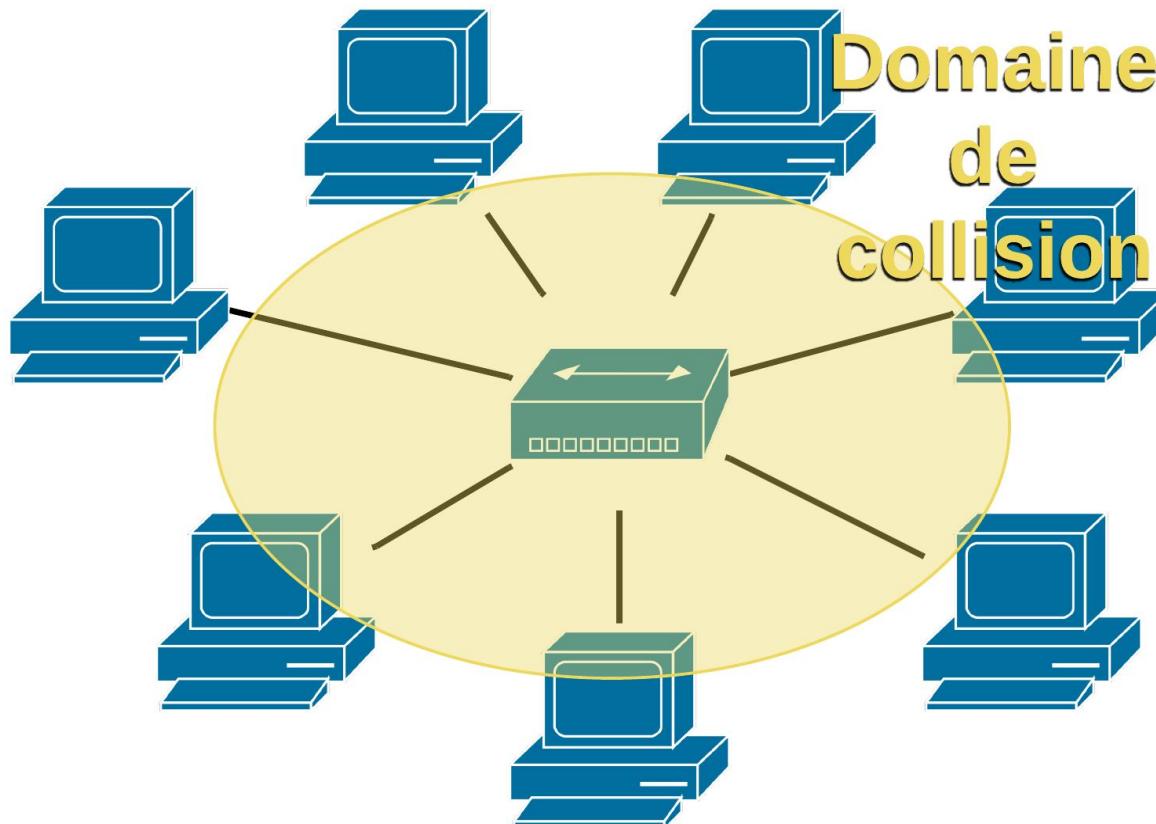
- Un domaine sans collision sur chaque port
- La bande passante dédiée sur chaque port
- Des transmissions en **full-duplex** (un canal pour l'émission et un autre pour la réception)

Domaine de collision



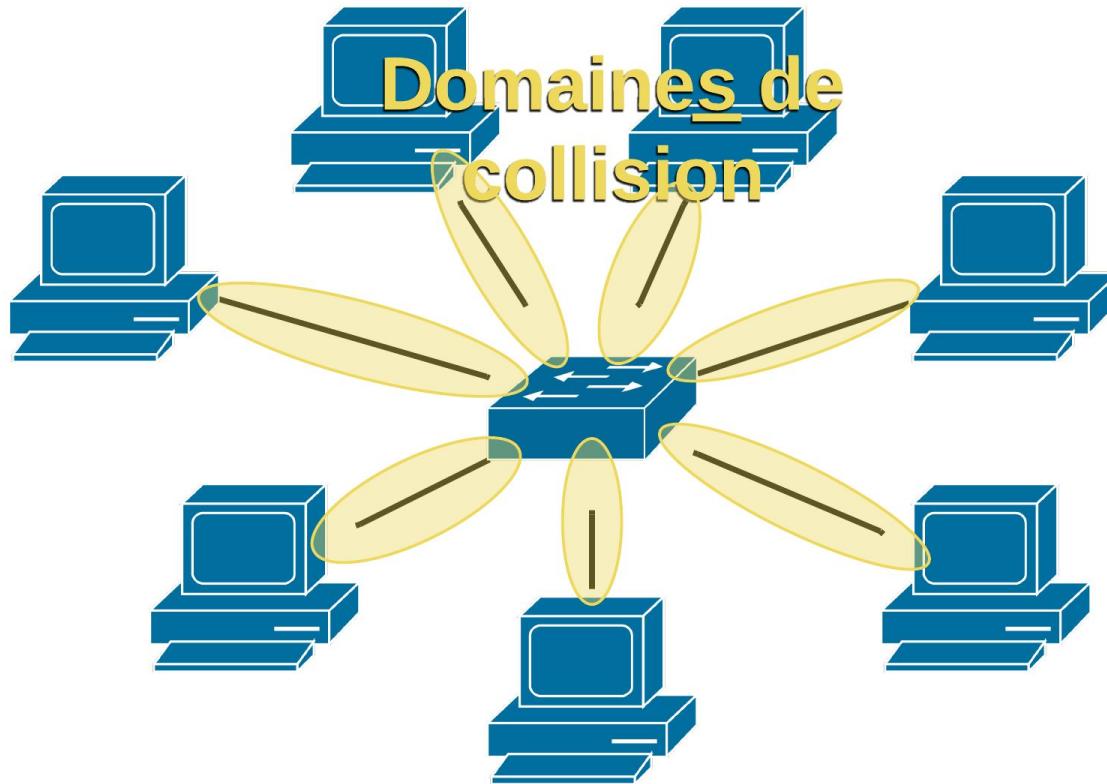
Topologie Physique	Topologie logique	Technologie
Bus	Bus	10Base5 10Base2

Domaine de collision



Topologie Physique	Topologie logique	Technologie
Etoile	Bus	10BaseT 100BaseT

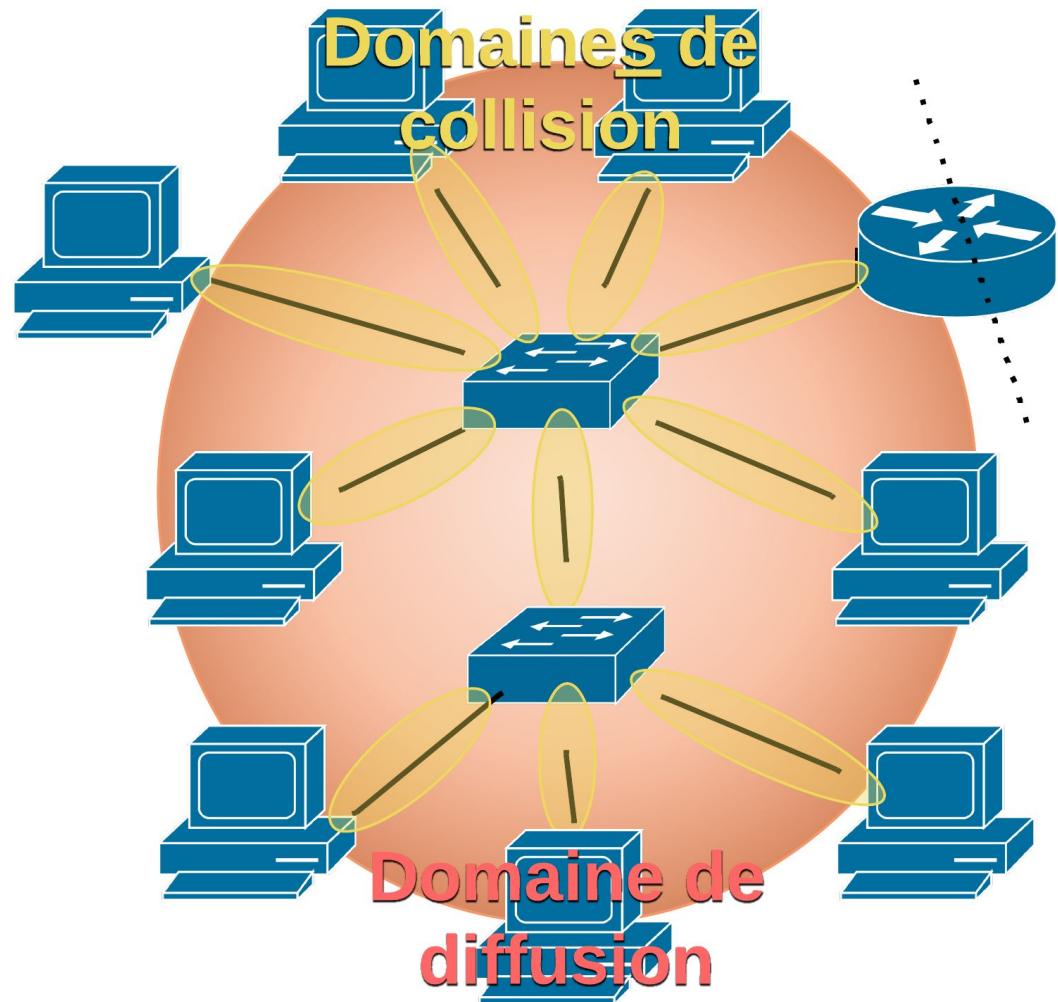
Domaine de collision



Topologie Physique	Topologie logique	Technologie
Etoile Hiérarchique Maillée	Commutée Segmentée	10/100/1000BASE-TX 1000BASE-SX/LX 10GBASE-T/SR/LR/LRM

Domaine de diffusion (Broadcast)

- Les commutateurs ne filtrent pas le trafic de diffusion (broadcast)
- Si deux commutateurs sont interconnectés, ils étendent le domaine de diffusion.
- Un routeur filtre le trafic de diffusion.



Eviter la congestion du réseau

Les commutateurs évitent et améliorent les performances du réseau en matière de congestion

- En facilitant la séparation des LANs en différents domaines de collision.
- En fournissant une communication Full-Duplex entre des périphériques
- En prenant avantage sur la haute densité des ports
- En mettant les grandes trames dans des mémoires temporaires (Buffering)
- En employant des ports à vitesse élevée
- En prenant avantage de leur capacité de transfert rapide (Hardware)
- En profitant du coût marginal peu élevé du port

6. Architectures LAN

(Cisco Systems)

Objectifs

- Décrire la *convergence* des données, de la voix et de la vidéo dans le contexte des *réseaux commutés*.
- Décrire un réseau commuté dans le contexte de petites et moyennes entreprises.
- Identifier les différents acteurs du marché.
- Choisir des commutateurs dans une architecture du réseau.

Des Réseaux de plus en plus complexes

- Notre monde digital change
- L'information doit être accessible de partout dans le monde
- Les Réseaux doivent être *fiables* et *très disponibles*.



Eléments d'un réseau convergent

- La collaboration est une nécessité
- Pour assurer la collaboration, les réseaux emploient des solutions convergentes.
- Des services de données comme des systèmes vocaux, des téléphones IP, des passerelles vocales, le support de la vidéo et des conférences.
- Le contrôle d'appels, la messagerie vocale, la mobilité et un réceptionniste automatique sont des fonctionnalités communes.

Avantages d'un réseau convergent

Les avantages d'un réseau convergent :

- Divers types de trafic; un seul réseau à gérer.
- Bénéfices substantiels par rapport à des réseaux voix, vidéos, données séparés.
- Il s'intègre à la gestion IT.



Borderless Switched Networks

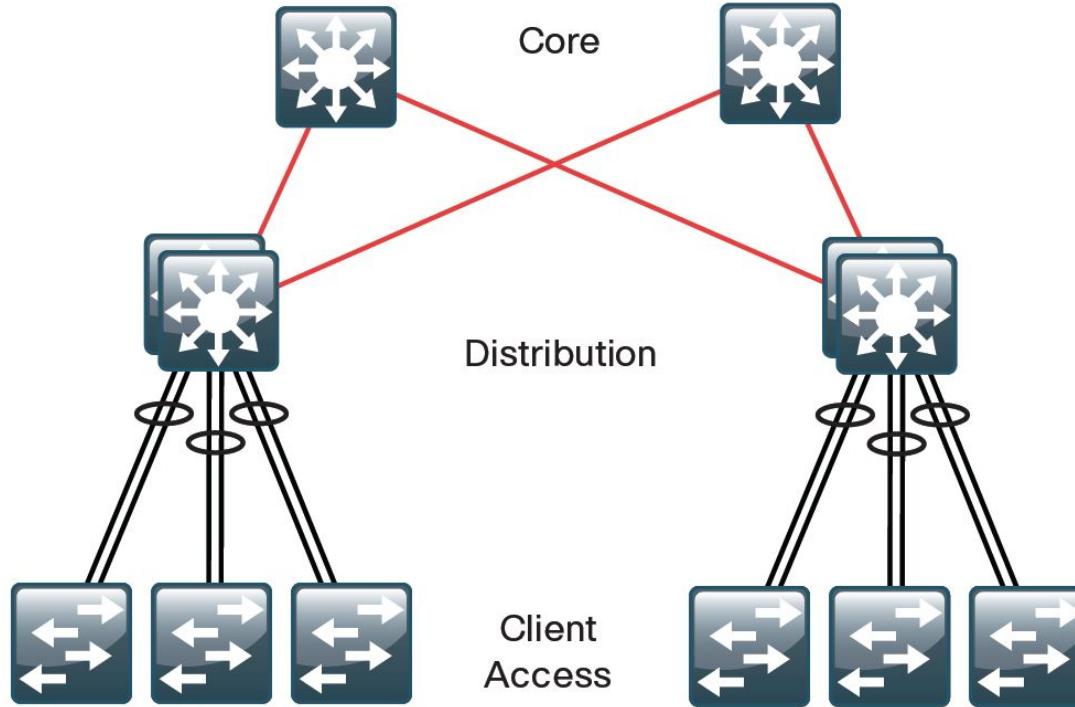
- *Cisco Borderless Network* est une architecture réseau qui permet aux organisations de connecter n'importe qui, de n'importe où, à n'importe quel moment à partir de n'importe quel périphérique de manière sécurisée, fiable et transparente.
- Elle a été conçue répondre aux défis IT et économiques comme le support des réseaux unifiés et les changements des méthodes de travail.

Architecture commutée sans frontière

Cette architecture “Borderless switched network” est construite autour des principes :

- **Hiérarchie** : comme niveaux fonctionnels, core/distribution/access
- **Modularité** : supporte facilement la croissance et les changements. Faire évoluer le réseau est facilité par l'ajout de nouveaux modules au lieu redessiner entièrement l'architecture du réseau.
- **Résilience** : une haute-disponibilité (HA) proche des 100 % de uptime.
- **Flexibilité** : les changements dans l'entreprise peuvent être adaptés au réseau rapidement selon les besoins.

Modèle hiérarchique à trois couches

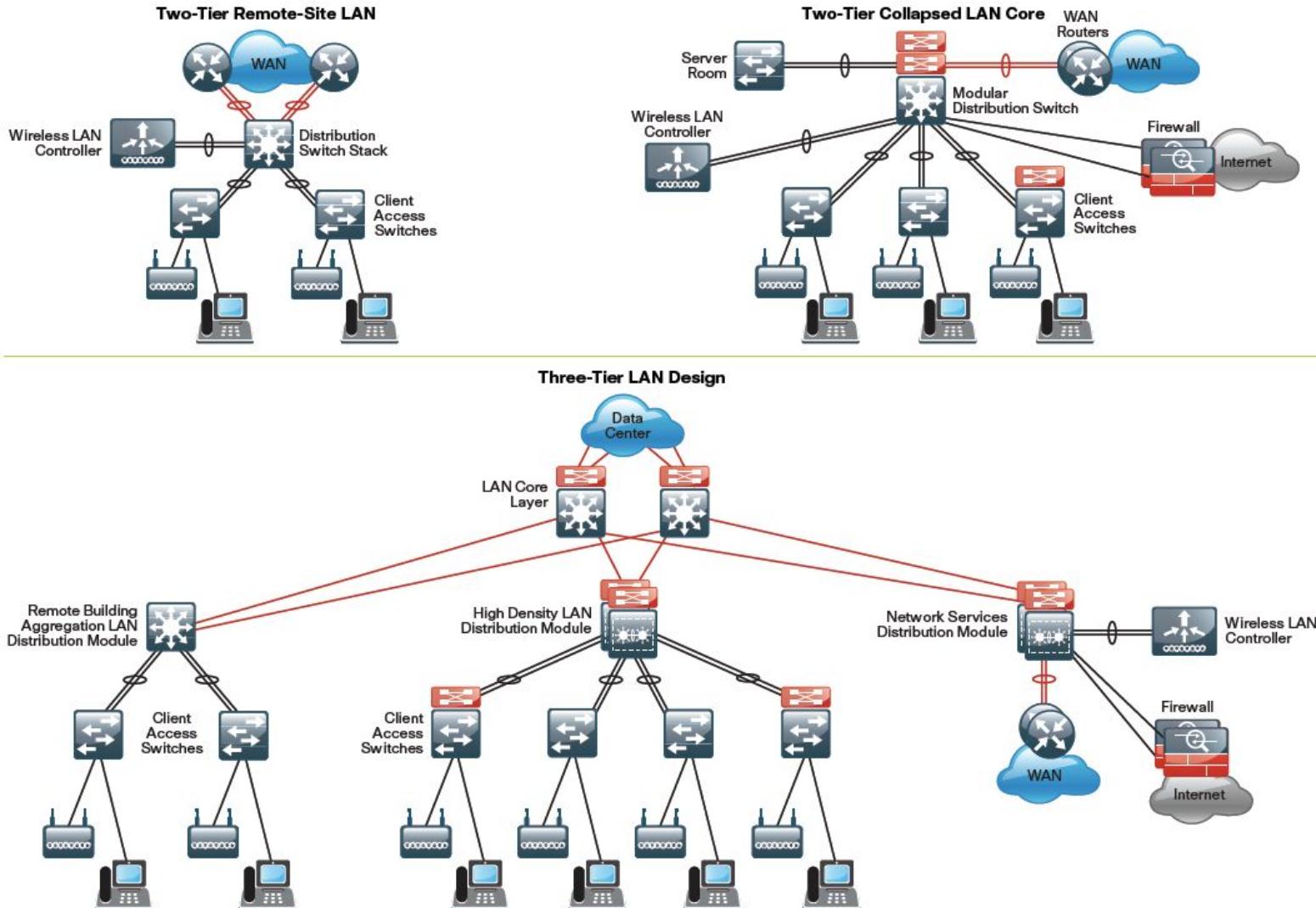


Core : Backbone haute vitesse pour transférer rapidement les paquets. Fournit de la haute disponibilité et s'adapte rapidement aux changements.

Distribution : Aggrège les connexions des locaux techniques. Utilise des commutateurs pour segmenter et organiser le SI en groupes, profils utilisateurs et isoler les problèmes.

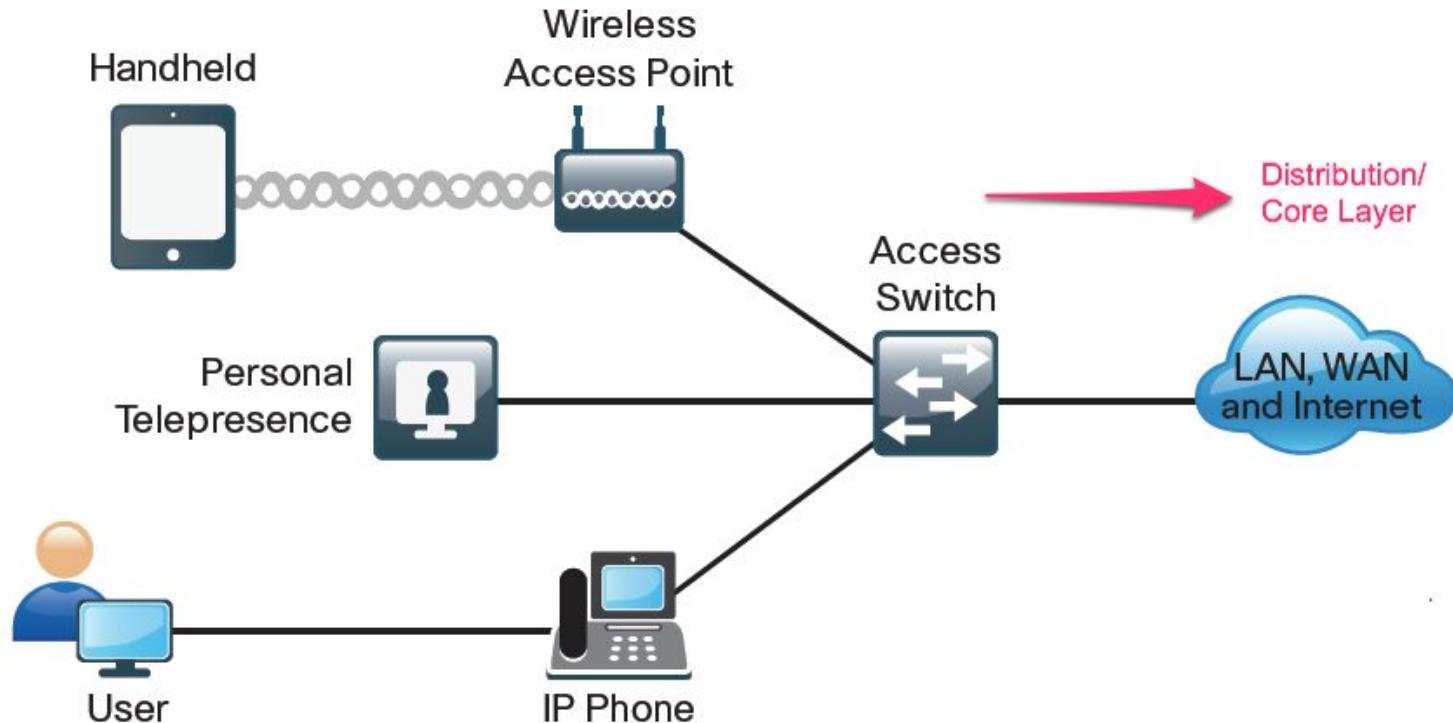
Access : Permet aux utilisateurs d'accéder aux périphériques du réseau.

Modèle hiérarchique adapté aux besoins



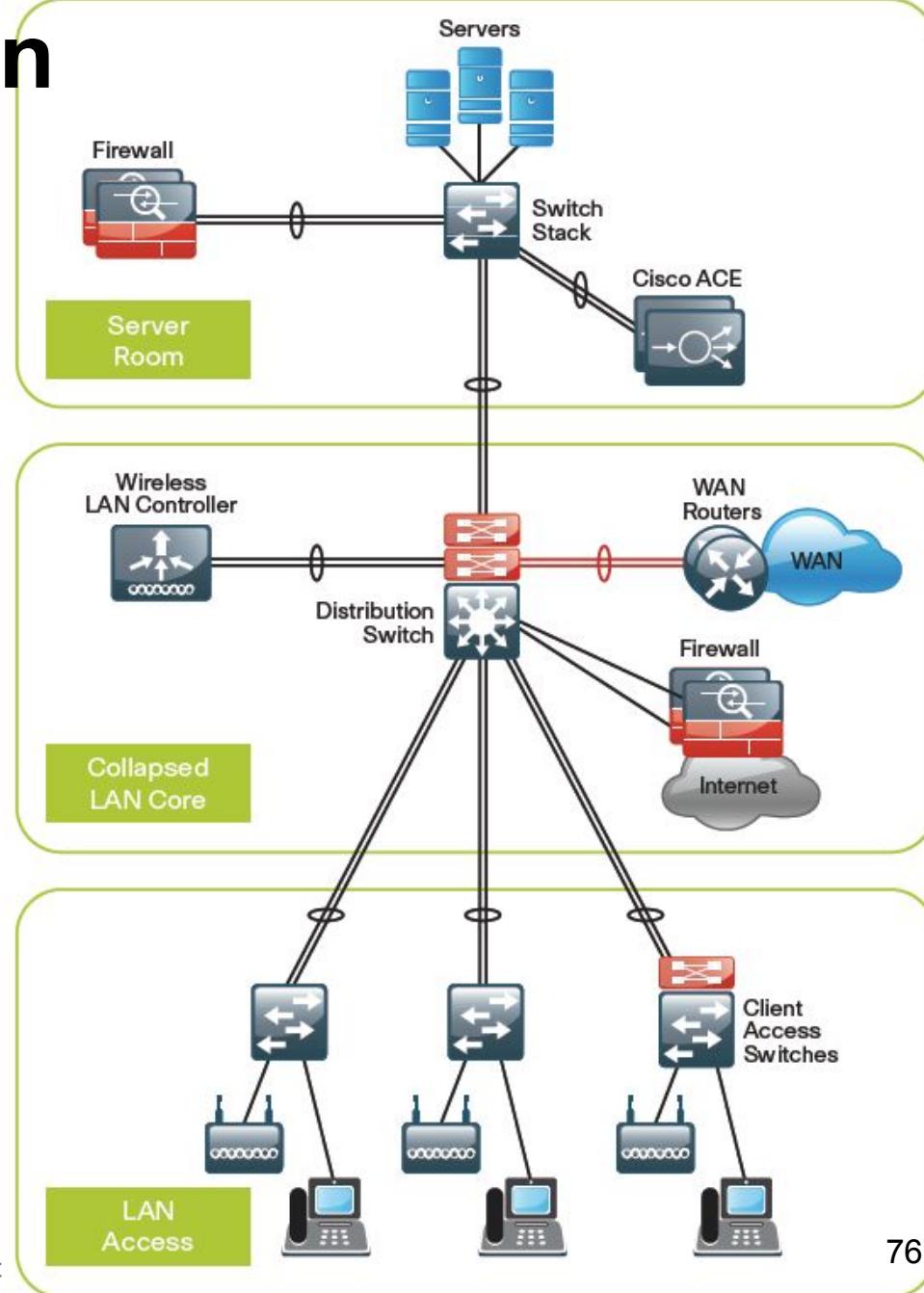
Couche Access

- **Haute Disponibilité** – alimentation redondante et support des *First Hop Redundancy Protocols (FHRP)*.
- **Convergence** – fournit de l'*inline Power over Ethernet (PoE)* pour les téléphones IP et les points d'accès sans fil
- **Security** – comprend d'office les fonctionnalités *port security*, *DHCP snooping*, *Dynamic ARP inspection*, *IP source guard*.



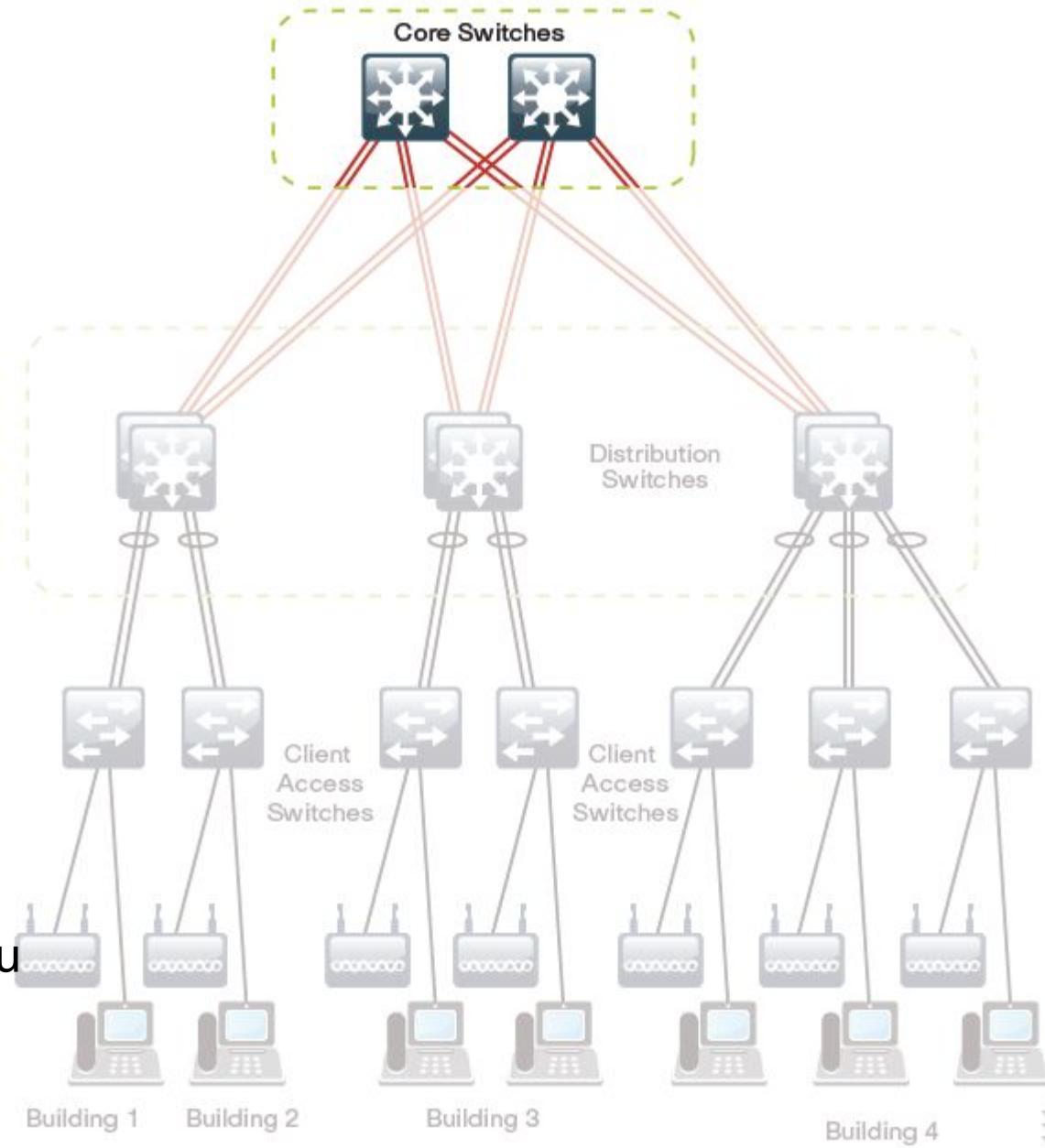
Couche Distribution

- Haute disponibilité, *fast path recovery*, répartition de charge, QoS, et sécurité
- *Route summarization* et manipulation de paquets
- Point de redistribution entre des domaines de routage
- Filtrage de paquets et politiques de routage.
- Termine les VLANs
- *First Hop Redundancy Protocol (HSRP, VRRP, GLBP)*.



Couche Core

- Agrège le trafic des commutateurs de distribution
- Implémente des protocoles et des technologies évolutives et de la répartition de charge
- Commutation High-speed de niveau 3 avec du 10-Gigabit Ethernet.
- Utilise de la redondance de niveau 3



Evolution des rôles des commutateurs

Le rôle des commutateurs a évolué :

- Un LAN commuté permet plus de flexibilité dans la gestion du trafic et des services.
- Un LAN commuté supporte des fonctionnalités comme
 - la qualité de service,
 - des services de sécurité supplémentaires
 - le support des réseaux sans fil et des services de mobilité
 - le support de la téléphonie IP
 - ...

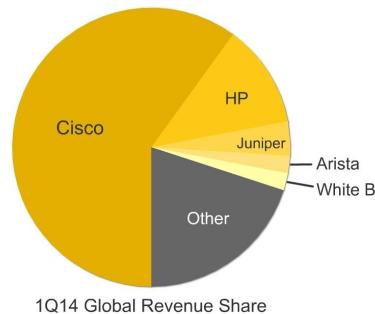
Wired and Wireless LAN access Infrastructure 2015



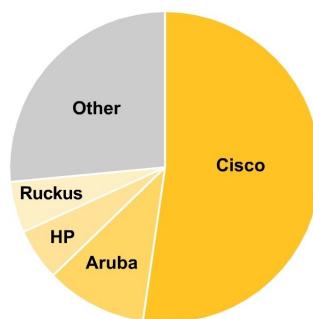
Marché de la commutation 2012

Cisco, HP, Juniper, les autres ...

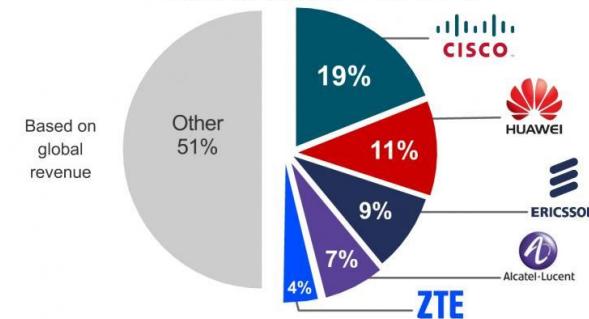
Top Ethernet Switch Vendors in 1Q14



Top 4 Wireless LAN Equipment Vendors by 1Q13 Global Revenue Share



Top 5 Telecom and Datacom Network Equipment and Software Vendors in the World

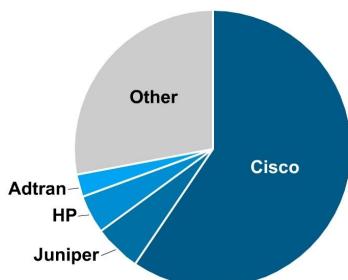


© Infonetics Research, *Ethernet Switches: Worldwide, Regional, China, and Quarterly Market Share, Size, and Forecasts*, May 2014

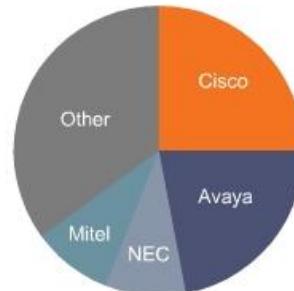
© Infonetics Research, *Wireless LAN Equipment and WiFi Phones Quarterly Market Share, Size, and Forecasts*, May 2013

© Infonetics Research, *Total Telecom and Datacom Network Equipment and Software Pivot: Annual Market Share, Size, and Forecasts*, July 2014

Top 4 Enterprise Router Equipment Vendors by 2Q13 Global Revenue Share



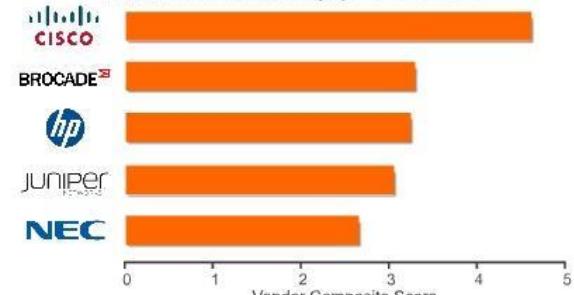
Top 4 Enterprise PBX and UC Voice Equipment Vendors by Global Revenue Share in 3Q14



© Infonetics Research, *Enterprise Routers Quarterly Market Share, Size, and Forecasts*, August 2013

© Infonetics Research, *Enterprise Unified Communications and Voice Equipment Quarterly Market Share, Size, and Forecasts*, November 2014

Overall Scores for the Top 5 Enterprise Networking and Communication Equipment Vendors



© Infonetics Research, *Enterprise Networking and Communication Equipment Vendor Scorecard*, July 2014

Lab 6 : Choisir son commutateur

- Fonctionnalités Access/Distribution/Core
- Fonctionnalités L2 / L3
- Type d'interface/technologies
- Contraintes physiques
- Nombre d'interfaces
- Conformité protocolaire
- Form Factor : Fixed ports, Modular, Stackable
- Gestion, facilités, loyauté
- Prix
- Garantie/support

Catalogues :

- [Cisco Switch Guide \(PDF\)](#)
- [HP Switches](#)

7. Résolution d'adresses

Ethernet et commutation

Objectifs

- Définir et caractériser les principes de la résolution d'adresse en IPv4 et de la découverte de voisinage en IPv6
- Caractériser le trafic ARP et ND NS/NA
- Lire les tables des caches ARP/ND des périphériques Cisco, Windows, Linux

Principe

La résolution d'adresse est utile dans les réseaux IP pour obtenir l'adresse physique à laquelle une adresse IP correspond. On peut obtenir le cache arp avec :

arp -a

Ce processus permet à l'hôte émetteur de trouver l'adresse de livraison physique du trafic.

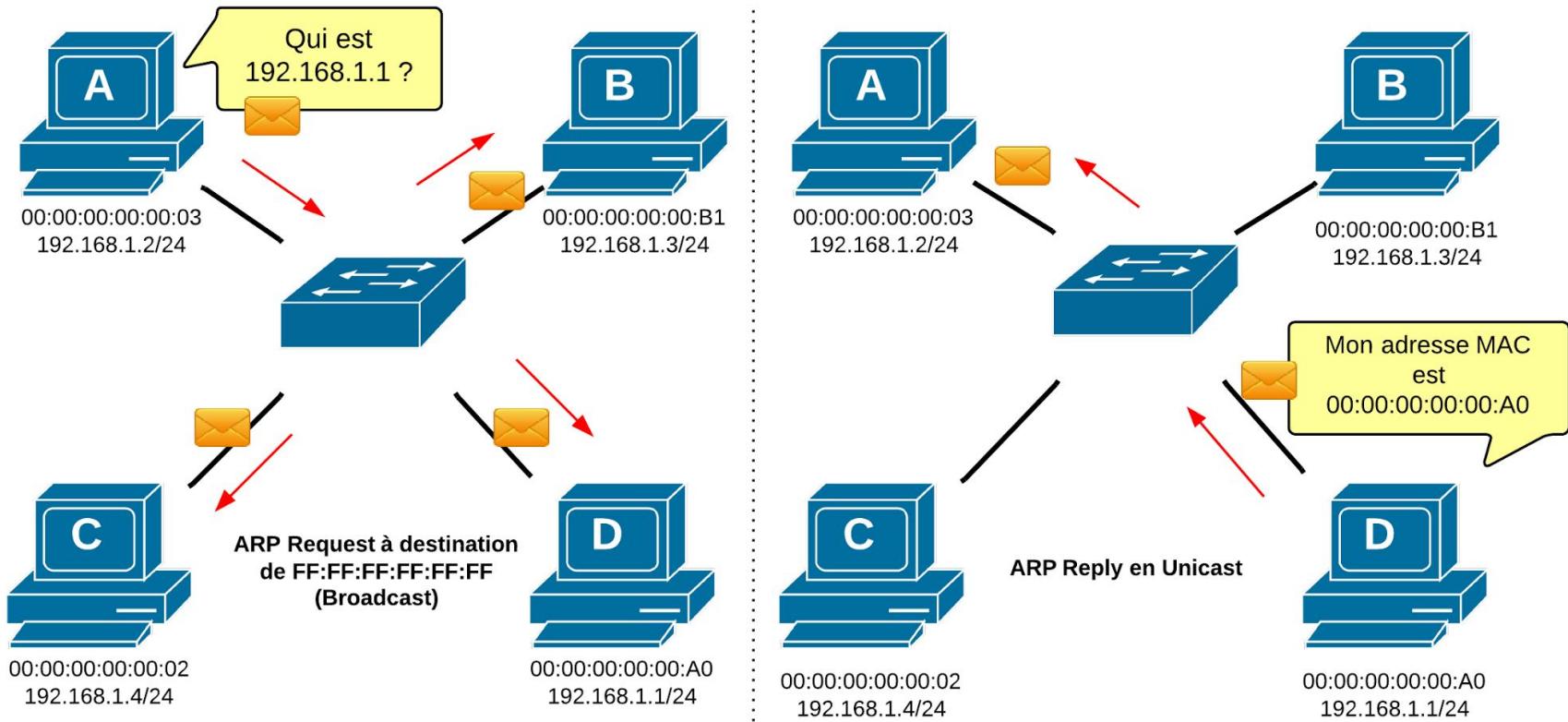
Il permet à l'hôte d'encapsuler le trafic au niveau de la couche Accès Réseau (Liaison de données) en y ajoutant l'adresse MAC du destinataire

Address Resolution Protocol

- ARP est le protocole de résolution d'adresse utilisé par IPv4.
- Il est directement encapsulé par la couche 2.
- Il est donc indépendant d'IP.
- Il est formalisé par le [RFC 826](#).

Résolution d'adresses en IPv4

Ce trafic émane en broadcast et se termine en Unicast.

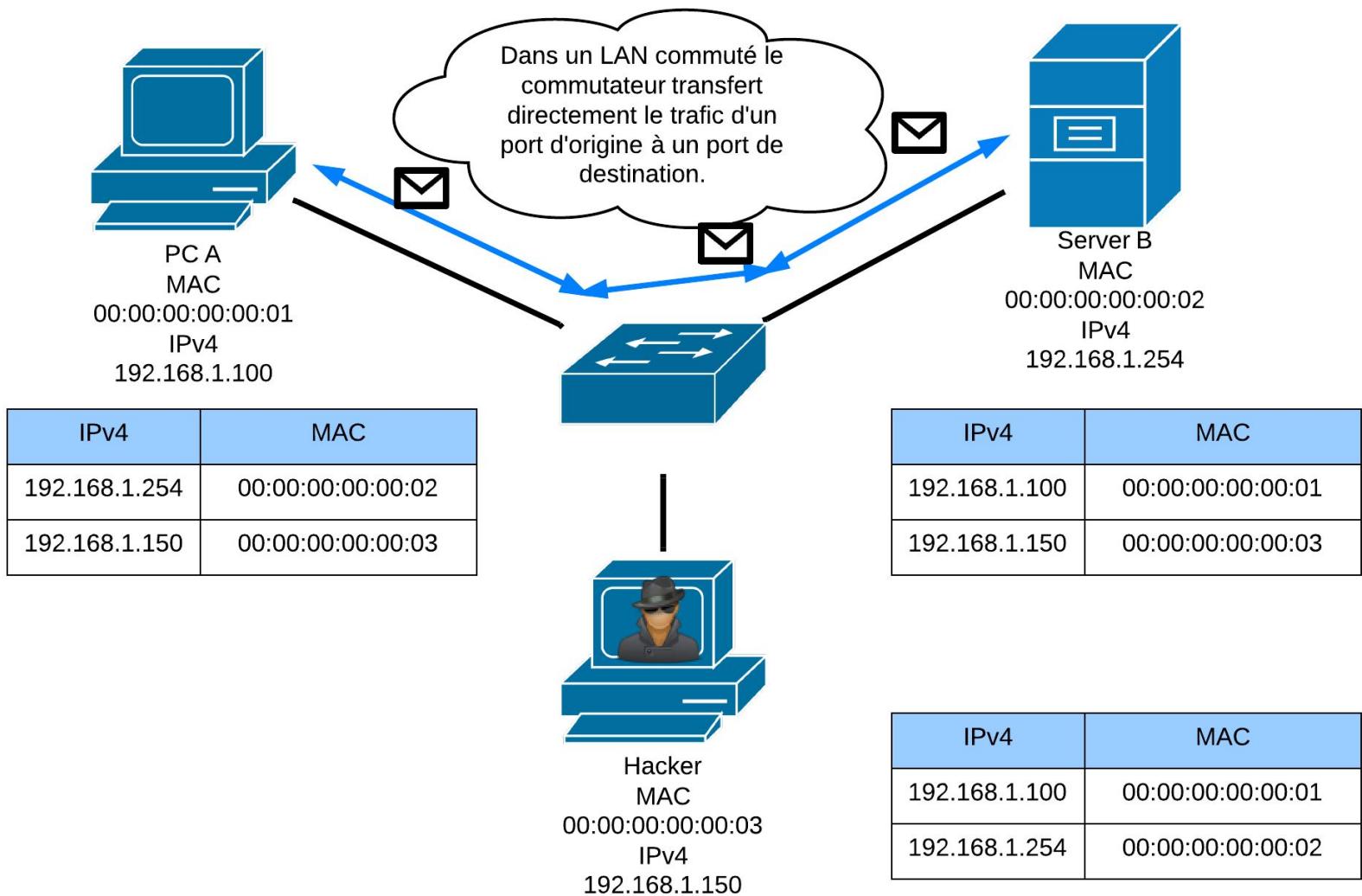


<http://www.cloudshark.org/captures/96a2bb5fe747?filter=arp>

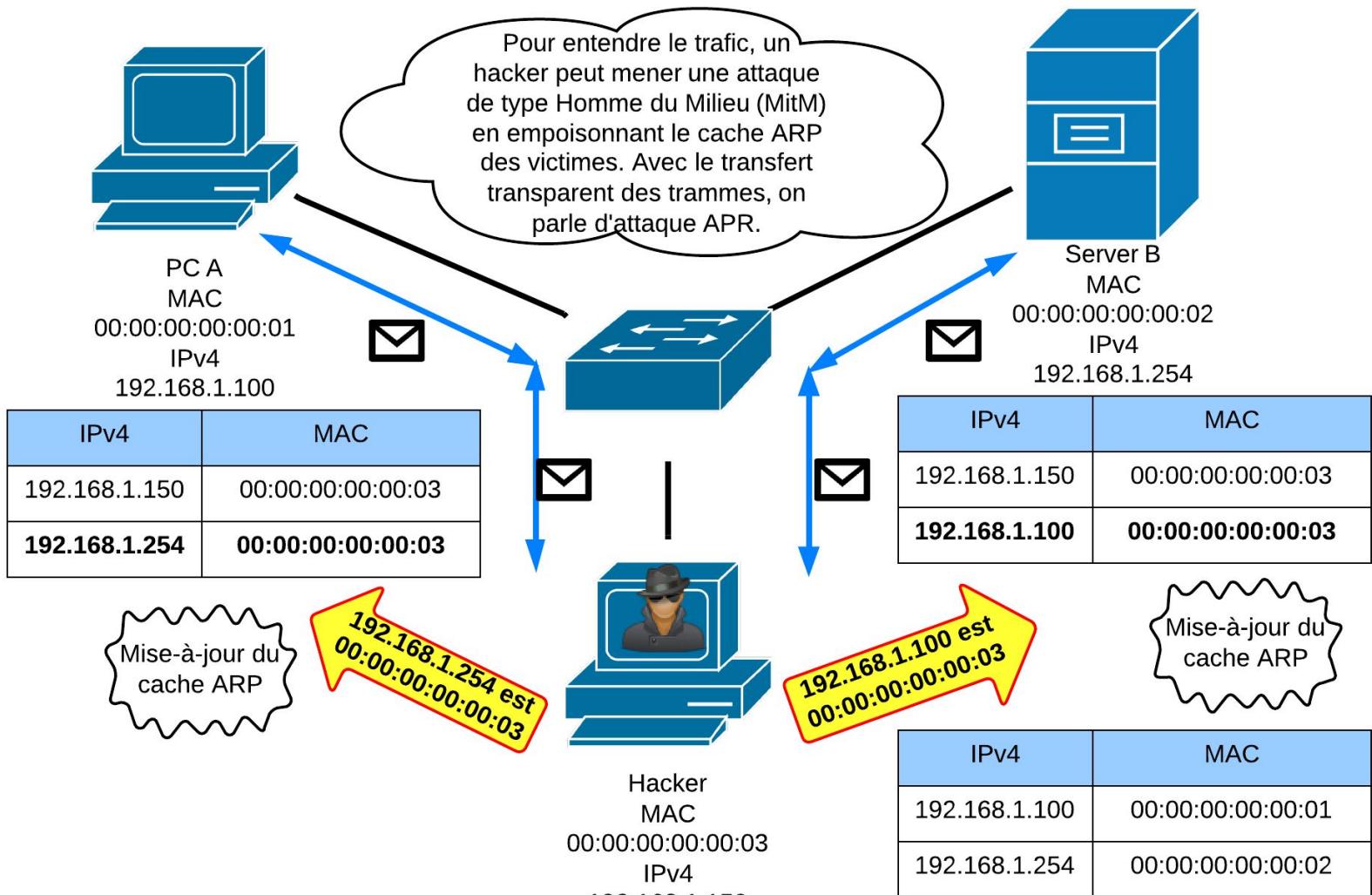
Variantes ARP

- **ARP Probe**
- **Gratuitous ARP** : annonces sans état
- **Inverse ARP** : obtenir l'IP à partir l'adresse L2 (Frame-Relay)
- **Reverse ARP** : attribution d'adresse IP
- **Proxy ARP** : mandataire ARP (routeur), fonction que l'on conseille de désactiver.

Processus ARP



Empoisonnement de cache ARP

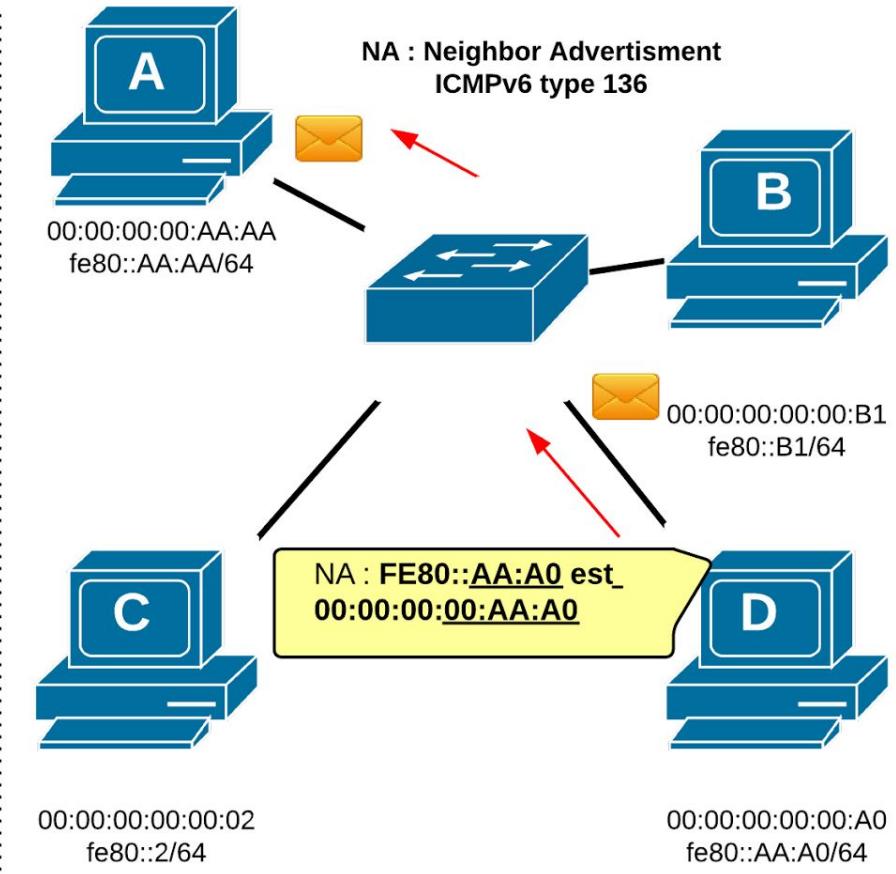
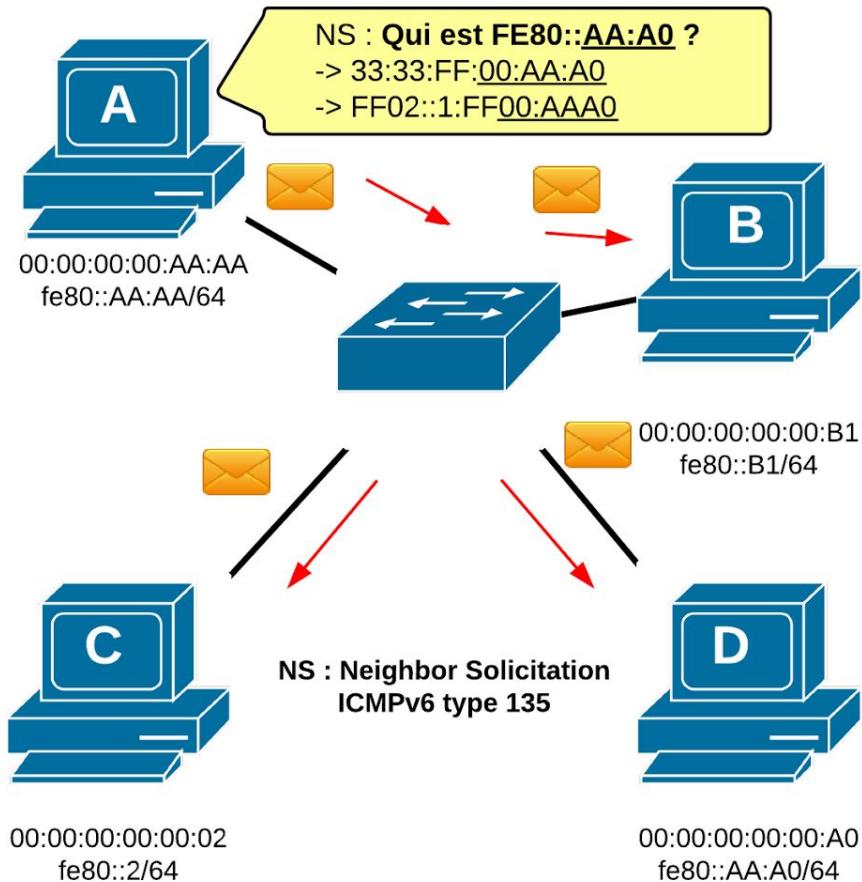


Neighbor Discovery

- En IPv6, l'usage d'ARP disparaît (comme celui du broadcast).
- C'est ND (Neighbor Discovery) qui reprend cette fonction.
- ND est encapsulé dans des paquets ICMPv6 eux-mêmes encapsulés dans de l'IPv6.
- En ce sens, pour cette fonction, IPv6 se suffit à lui-même, contrairement à IPv4.
- Comme pour ARP, ND embarque d'autres fonctions (NUD, DAD, SLAAC, validité des adresses) et d'autres messages d'un type nouveau (RA/RS).

Découverte de voisinage (IPv6)

1. NS en Solicited-Node Multicast (voir dia suivante)
2. NA en Unicast ou All-nodes Multicast (FF02::1)



Adresse Solicited-Node Multicast

Au lieu d'utiliser du broadcast pour joindre un hôte dont on ne connaît pas l'adresse physique, IPv6 propose d'utiliser une adresse Multicast inspirée de cette adresse.

Une adresse IPv6 *Solicited-Node multicast* est créée en prenant les 24 derniers bits de l'adresse IPv6 connue (unicast) et en lui ajoutant le préfixe **ff02:0:0:0:0:1:ff00::/104**

Un hôte doit joindre une adresse *Solicited-Node multicast* pour chaque adresses unicast ou anycast configurée.

Par exemple

- fc00::1/64 sera joint par ff02::1:ff00:1.
- fe80::2aa:ff:fe**28:9c5a** sera joint par ff02::1:**ff28:9c5a**.

L'adresse MAC correspondante prendra le 33:33:FF suivant des 24 derniers bits de l'adresse IPv6 demandée.

- ff02::1:ff00:1 correspond à 33:33:FF:**00:00:01**
- fe80::2aa:ff:fe**28:9c5a** correspond à 33:33:FF:**28:9C:5A**

Lab 7 : Diagnostic ARP/ND

1. Table ARP et table de voisinage (sous Windows)

- arp -a
- netsh interface ipv6 show neighbors

2. Voyez les inscriptions aux groupes multicast

- netsh interface ipv6 show joins

3. Captures SLAAC, trafic DAD, trafic NUD :

<https://www.cloudshark.org/captures/f8773b94180f>

8. Sécurités L1, L2, L3, L7

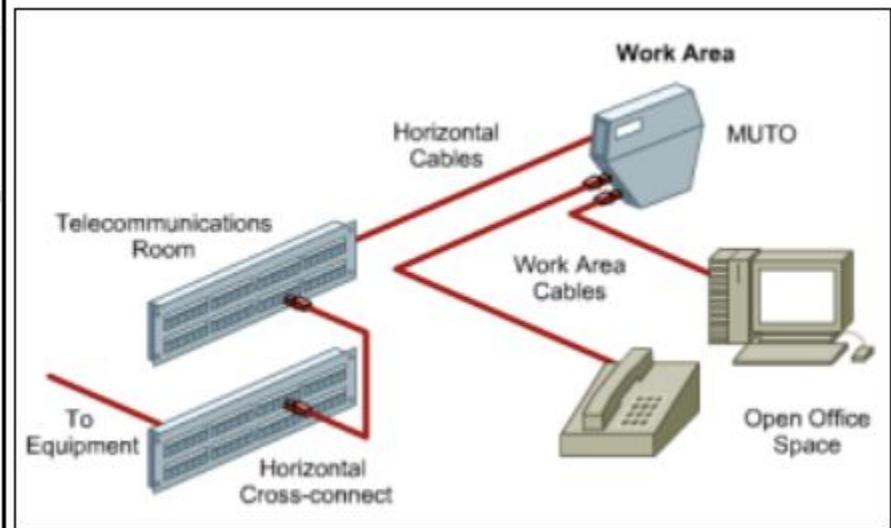
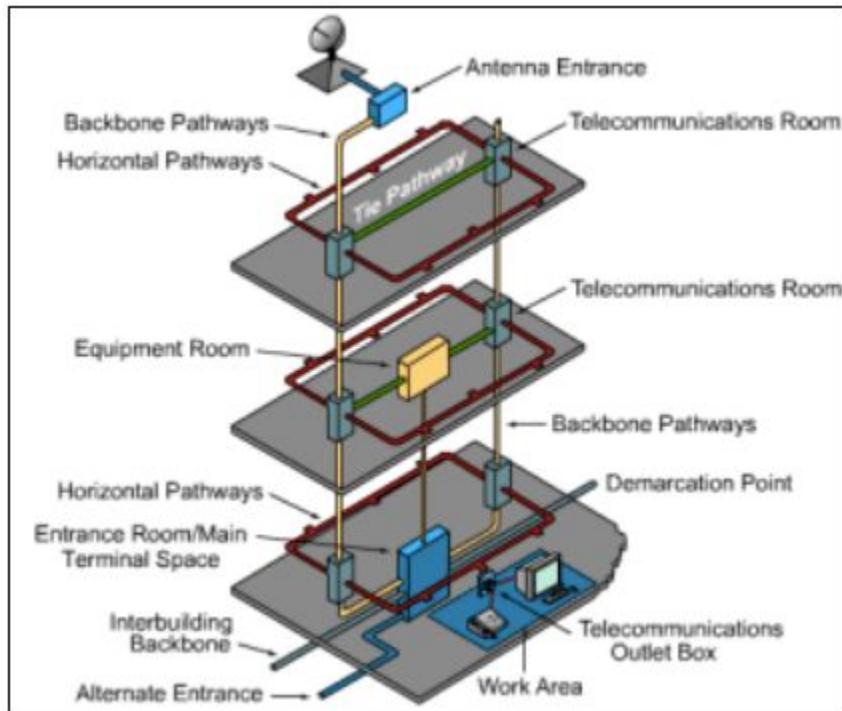
Objectifs

Ouvrir la discussion sur les sujets suivants :

- Le câblage structuré
- Les tempêtes de broadcast et STP, ses variantes
- Solutions de disponibilité Etherchannel, HSRP, Routage dynamique
- VLANs
- Sécurité sur les ports
- Protocoles Cisco et autres
- Cisco IPv6 First Hop Security

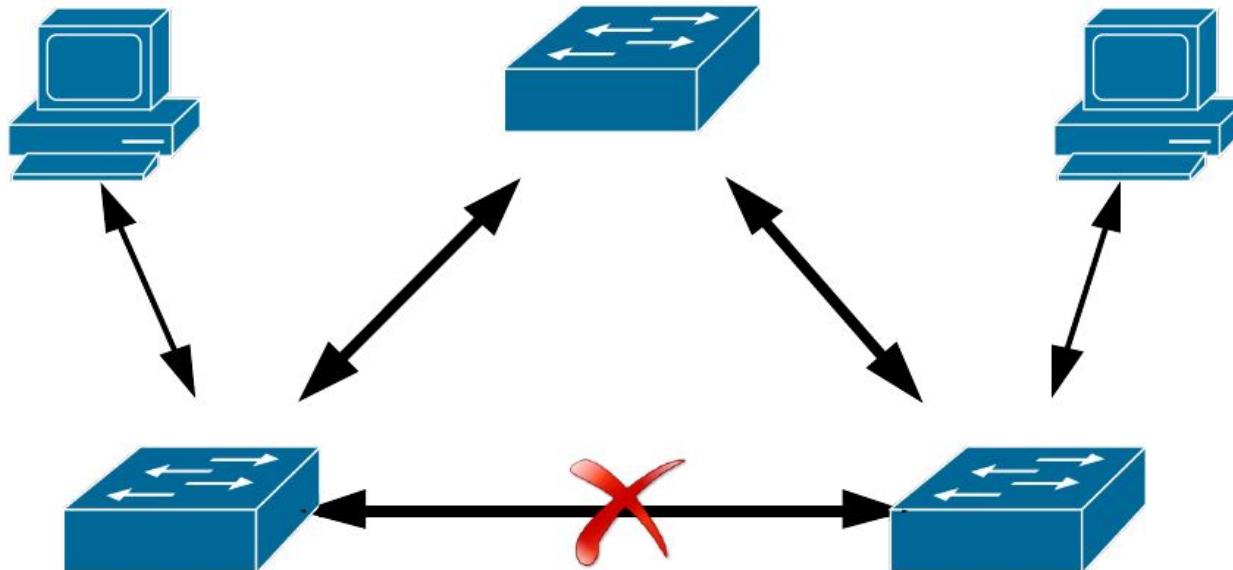
Câblage structuré

<http://softnews.unblog.fr/files/2009/07/ccna1csfr.pdf>



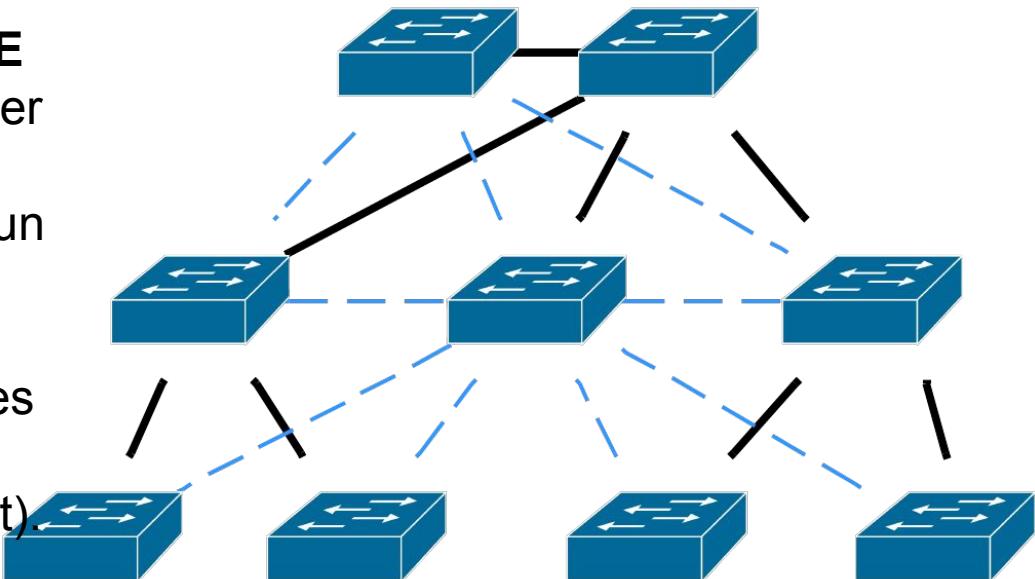
Tempêtes de broadcast

- Les boucles physiques apportent la redondance à l'infrastructure
- Dans un réseau bouclé, le trafic de diffusion sort par tous les ports sauf celui d'origine de manière indéfinie. En effet, les trames Ethernet n'ont pas de durée de vie.
- La solution est : couper la boucle = débrancher le câble



Spanning-Tree

- Spanning-Tree est un protocole L2 formalisé **IEEE 802.1D** qui permet de garder une topologie physique redondante tout en créant un chemin logique unique.
- Spanning-Tree envoie régulièrement des annonces (BPDUs) pour élire un commutateur principal (root).
- En fonction de cette information, les commutateurs "coupent" des ports et une topologie de transfert à chemin unique converge (de quelques secondes à 50 secondes selon les versions).



Variantes STP

Spanning-Tree (STP)	IEEE 802.1D
PVST+	STP Cisco
Rapid Spanning-Tree (RSTP)	IEEE 802.1w
PVRST+	RSTP Cisco
MIST	IEEE 802.1s

Disponibilité

Couche	Protocole/Solutions	Délais de reprise
L2	Rapid Spanning Tree	Quelques secondes
L2	Etherchannel	Plus ou moins 1 seconde pour rediriger le trafic sur un lien alternatif
L3	First Hop Redundancy Protocols comme HSRP, VRRP, GLBP	10 secondes par défaut (Cisco) mais le constructeur conseille 1s hello time, 3s Hold Time
L3	Protocoles de routage	En dessous de la seconde avec OSPF ou EIGRP bien configurés au niveau des compteurs

Sécurité sur les ports

Sur du matériel Cisco on peut configurer la sécurité sur les ports :

- MAC autorisées sur un port (nombre)
- Une action en cas de violation (protect, restrict, shutdown).
- Apprentissage statique ou dynamique (sticky).

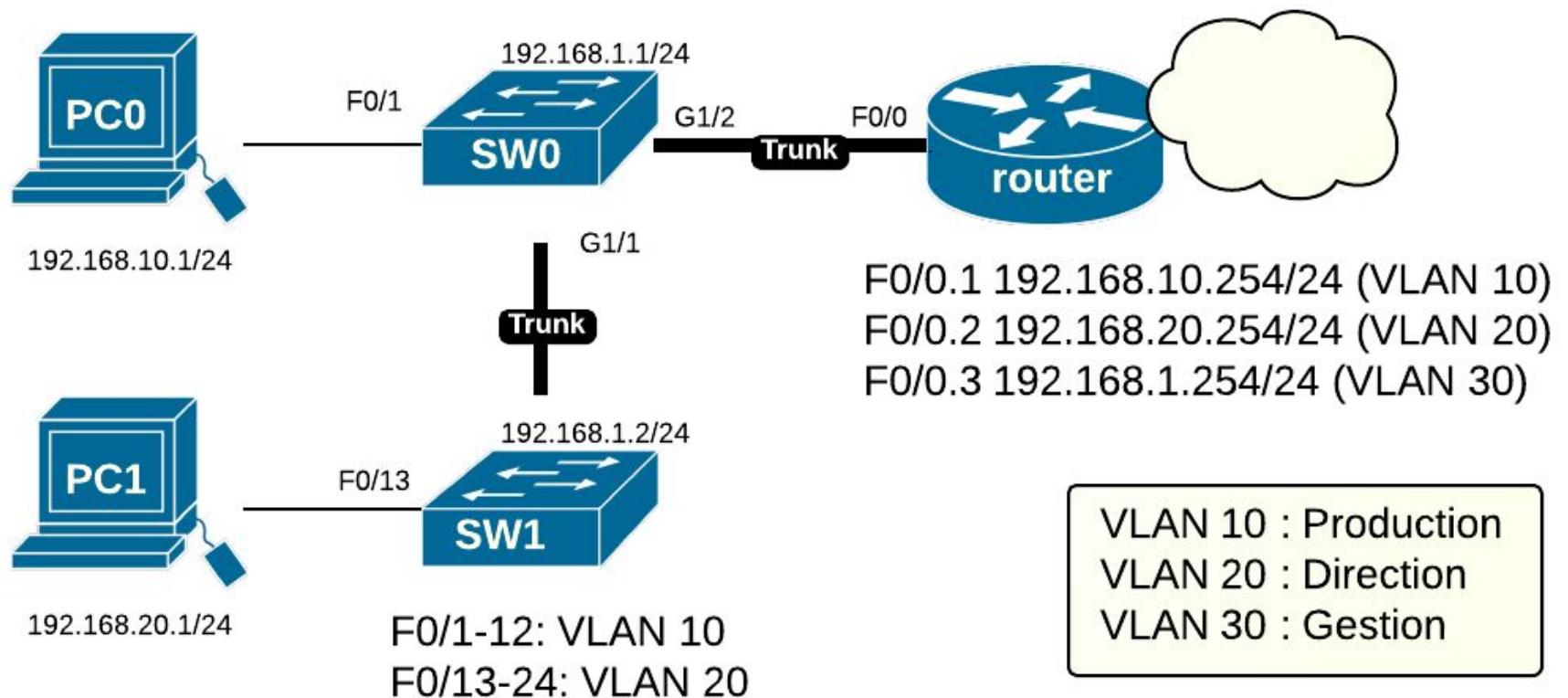
Technologie VLAN

Les technologies VLANs *virtualisent* un LAN.

La virtualisation d'un LAN consiste en la **séparation entre**, d'une part, **l'infrastructure physique** et, d'autre part, **les services de couche 2** « liaison de données » fournis par les commutateurs.

Soit une seule infrastructure physique supporte plusieurs LAN distincts.

Topologie VLAN de base



VLANs

La technologie VLAN (LAN virtuel) permet de :

- gérer et maintenir plusieurs LANs (séparés par du routage)
- sur une seule et même infrastructure physique commutée
- un VLAN = un commutateur virtuel sur plusieurs commutateurs physiques
- un VLAN = un domaine de diffusion

Avantages/Inconvénients VLANs

Pros :

- Flexibilité : allocation dynamique des utilisateurs dans un réseau indépendamment de l'emplacement
- Indépendance L1
- Facilité de gestion
- Performances : diminution de la taille des domaines de collision
- Sécurité
- Coût

Cons :

- Infrastructure/Hardware
- Compétences

Protocoles Cisco et autres

- On trouvera ici des captures de protocoles de gestion CDP, VTP, DTP, STP
- Protocole de voisinage : Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP) IEEE 802.1AB
- Agrégation de liens : Etherchannel, Link Aggregation Control Protocol (LACP)
- Unidirectional Link Detection (UDLD)
- Gestion des VLANs : VLAN Trunking Protocol (VTP), Dynamic Trunking Protocol (DTP), Multiple VLAN Registration Protocol (MVRP) IEEE 802.1ak
- Redondance de passerelle : HSRP, GLBP, VRRP, CARP
- Alimentation par le câble : PoE IEEE 802.1af

Cisco IPv6 First Hop Security

A database table of IPv6 neighbors connected to the switch is created from information sources such as Neighbor Discovery (ND) protocol snooping. This database, or binding, table is used by various IPv6 guard features (such as IPv6 ND Inspection, per-port address limit, IPv6 device tracking) to validate the link-layer address (LLA), the IPv4 or IPv6 address, and prefix binding of the neighbors to prevent spoofing and redirect attacks.

IPv6 ND Inspection learns and secures bindings for stateless autoconfiguration addresses in layer 2 neighbor tables. IPv6 ND inspection analyzes neighbor discovery messages in order to build a trusted binding table database, and IPv6 neighbor discovery messages that do not conform are dropped.

Router advertisements (RAs) are used by routers to announce themselves on the link. IPv6 RA Guard analyzes these RAs and can filter out bogus ones sent by unauthorized routers.

The per-port address limit feature enables an operator to specify a maximum number of IPv6 addresses allowed on a port of the switch. This function is achieved by filtering out ND messages sourced with addresses beyond the per-port address limit.

IPv6 Device Tracking provides IPv6 host liveness tracking so that a neighbor table can be immediately updated when an IPv6 host disappears.

The Secure Neighbor Discovery for Cisco IOS Software feature is designed to counter the threats of the ND protocol. Secure neighbor discovery (SeND) defines a set of neighbor discovery options and two neighbor discovery messages. SeND also defines a new autoconfiguration mechanism to establish address ownership. The IPv6 PACL feature adds IPv6 port-based ACL support.

9. Activités pratiques

Laboratoires

Activités pratiques

- **Connectique TIA/EIA 568B**
- Cahier des charges pour une infrastructure commutée (choisir son commutateur et ses interfaces)
- **Interprétation des différentes tables**
 - ARP (Cisco, Linux, Windows)
 - CAM (Cisco)
 - Routage (Cisco, Linux, Windows)
- ***arp-scan, arping, arpwatch/ndpmon*** avec [Kali](#) sous VMWare ou VirtualBox
- **Capture Wireshark**
- Configuration LAN PME
- **Implémentation ARP Poisoning** ([Cain](#), Ettercap, Yersinia, scapy, dnsniff)
http://hakipedia.com/index.php/Category:Network_Security
- Configuration de la sécurité sur les ports en contre-mesure
- Manipulation du commutateur Linux *brctl*
- *OpenVswitch*

Quiz Technologie Ethernet et Commutation

<http://cisco.goffinet.org/quiz/quiz-technologie-etherne-t-et-commutation>

Technologie Ethernet et Commutation (public)

10 Questions

15 Minutes

Quiz portant sur la présentation Technologie Ethernet et commutation. 10 questions en 15 minutes.

Au sommaire : Leçon 1 : Modèles en couches et standards•Leçon 2 : Câblages, connecteurs, NIC•Leçon 3 : MAC CSMA/CD•Leçon 4 : Adressage et tramage•Leçon 5 : Commutation et commutateurs•Leçon 6 : Architectures LAN commutées (Cisco Systems)•Leçon 7 : Résolution d'adresses•Leçon 8 : Sécurités L1, L2, L3, L7

Démarrer

Présentations ICND1/ICND2 sur la commutation LAN

- Technologie Ethernet et commutation
- Prise en main d'un commutateur Cisco®
- Technologies VLANs
- Lab VLANs
- Spanning-Tree et Etherchannel
- Lab VLANs+STP+Etherchannel
- Diagnostic sur le LAN
- Sécurités sur le LAN

Droits

Technologie Ethernet et Commutation de goffinet@goffinet.eu est mis à disposition selon les termes de la [licence Creative Commons Attribution - Partage dans les Mêmes Conditions 4.0 International](#)