

Encyclopédie des Réseaux Locaux

Cours de Réseaux Locaux - S7 - ENSEEIHT

Écrit par Clément Lizé et Nicolas Lazzari
v1 - Novembre 2020

Avant-propos

Face au manque d'organisation du cours proposé ce semestre, les auteurs proposent dans ce document des notes les plus organisées possible du cours de Réseaux Locaux. Un énorme travail a été nécessaire pour son élaboration, et les notes présentées ne sont pas exhaustives. Nous vous invitons à utiliser le sommaire interactif de Google docs (Affichage → Afficher le plan du document) pour naviguer et comprendre le contexte des notes. Bonne lecture !

Sommaire

Avant-propos	2
Sommaire	3
Introduction aux Réseaux Locaux	6
1: Objectifs	6
2 : En bref : les méthodes d'accès	6
A - Méthode par interrogation polling	6
B - Méthode de partage sur requête TDMA	7
C - Méthode à jeton	7
D - Méthode à collision	7
a. Aloha	7
b. CSMA/CD	7
c. CSMA/CA	8
3: Classification des méthodes d'accès	8
A - Partage statique	8
B - Partage dynamique	8
a. Partage dynamique centralisé	8
b. Partage dynamique décentralisé / distribué	9
Chapitre 1 : Architecture et Standardisation	10
1 : Architecture réseau local	10
A - LLC (Logical Link Control)	10
B - MAC (Medium Access Control)	11
C - Physique	11
2 : Standardisation des Réseaux Locaux	12
A - Standardisation	12
B - Adressage MAC	12
a. Format	13
b. Portée	13
c. Complément	13
C - Couche LLC	14
a. Format PDU	15
b. Service LLC1	15
Chapitre 2 : Commutation et VLAN Ethernet	16
1 : Architectures Ethernet et formats de trames	16
A - Informations de la couche physique	16
B - Couche MAC	17

2 : Segmentation Switch et Apprentissage	18
A - Principe du bridge	18
B - Table dynamique du bridge	18
C - Switch VS Hub	18
3 : VLAN	19
A - Bases du VLAN	19
B - Administration des VLAN	20
a - Configuration VTP	20
b - Configuration VMPS	20
C - Communications inter-VLAN	20
Chapitre 3 : Arbre recouvrant : STP, RSTP, MSTP	21
1 : Problèmes et solution au routage par apprentissage	21
A - Principe de l'algo de Spanning Tree	21
B - Routage par apprentissage	24
2 : Protocoles de STP	25
A - Protocole d'arbre recouvrant	25
B - VLAN et Arbre recouvrant	27
3 : Autres routages-Alternative à l'apprentissage	27
A - Routage par la source (ou par noeud)	27
a. Principe de l'apprentissage	27
b. Principe du relayage	28
Chapitre 4 : Fonctionnement d'un lien Ethernet	29
1 : Support, débit et contrôle	29
A - Eléments de base	29
a. Support, débit et transmission	29
b. Contrôle de flux	30
c. Autonegotiation	31
B - Amélioration de performances	33
a. Augmentation des longueurs de trames	33
b. Agrégation	33
c. Consommation d'énergie	34
2 : Résumé des couches	34
Chapitre 5 : WiFi	35
1 : Eléments de base	35
A - Caractéristiques d'une transmission	35
a. Bandes : 2,4Ghz ou 5Ghz	35
b. Modulation et constellations	36
c. Diffusion MIMO	36

B - Les architectures réseau	37
2 : Gestion de l'accès au support	38
A - DCF (Collision Avoidance)	38
a. Principe	38
b. Problème de la station cachée	39
B - PCF (polling)	40
3 : Améliorations au niveau MAC	40
A - Économie d'énergie	40
B - Qualité des services (WMM)	40
a. EDCA : priorités	41
b- HCCA : accès contrôlé	41

Introduction aux Réseaux Locaux

1: Objectifs

Étude des problèmes de **performance** et **efficacité**, étude des méthodes de **segmentation & virtualisation**.

Objectifs du cours :

- Comprendre une architecture réseau local
- Connaître le fonctionnement de la virtualisation de LAN
- Connaître les algorithmes de pontage
- Compétences en administration de technologie Ethernet, WiFi

2 : En bref : les méthodes d'accès

Méthode d'accès = allocation des ressources pour par exemple :

- économiser des supports filaires
- partager un support sans fil

Procédé : **définir un ordre d'émission** (ordonnancement, scheduling)

Ici la ressource = temps d'émission

On va étudier 4 méthodes :

- A. Méthode par interrogation polling
- B. Méthode de partage sur requête TDMA
- C. Méthode à jeton
- D. Méthode à collision

A - Méthode par interrogation polling

Station "chef", donne la parole aux stations (cyclique)

Exemple connu : le **polling** (liaison de données HDLC)

- 1 : le "chef" demande si la station veut parler
- 2 : la station parle, puis indique qu'elle a fini
- 3 : le "chef" demande à la station suivante

B - Méthode de partage sur requête TDMA

Station demande au “chef” donne une **quantité de parole**

Quantité = temps ou fréquence

Station envoie une requête de ressources

Exemple : Pt d'Accès Wifi alloue du temps aux appareils

C - Méthode à jeton

La station qui **possède le jeton** a le droit d'émettre

Analogie à un micro dans un amphi

Utilisée sur des topologies de boucle réseau local token ring

D - Méthode à collision

Aucune synchronisation → risque de collisions

3 méthodes principales :

- a. Aloha
- b. CSMA/CS
- c. CSMA/CA

a. Aloha

Station émet sans contrainte

Si collision → retransmission

b. CSMA/CD

Écoute du support :

si libre → la station transmet

si occupé → attente de libération puis émission

Si collision (Collision Detection)

→ arrêt émission + retransmission après attente aléatoire

c. CSMA/CA

Écoute du support :

si libre → la station transmet

si occupé → attente de libération + attente aléatoire puis émission

Si collision (non réception de ACK)

→ arrêt émission + retransmission après attente aléatoire

3: Classification des méthodes d'accès

2 classifications :

Statiques ≠ **dynamiques**

Centralisées ≠ **décentralisées** (ou distribuées)

A - Partage statique

Pas besoin de méthodes d'accès

Station émet si elle a des ressources dédiées

Exemple : Wifi ; ligne réseau téléphonique

Avantages :

- **simplicité** : pas d'algo avant d'émettre, pas d'échange d'infos
- **qualité de service** : émission à délai garanti (on sait quand une station veut transmettre, et combien de temps ça prend)
- efficace pour besoins d'émission constants

Inconvénients :

- **gaspillage de ressources** : bande passante peut être non utilisée
- **passage à l'échelle difficile** : ajouter un user ⇒ changer le partage

B - Partage dynamique

a. Partage dynamique centralisé

Machine "chef" (**point central**) décide qui peut émettre et quand

2 options :

- Interrogation par le point central : "veux-tu émettre ?"
- Requête au point central : "je veux émettre"

Avantages méthode par interrogation :

- **efficacité** : ressource donnée à ceux qui ont besoin
- contrôle des temps d'émission

Inconvénients méthode par interrogation :

- **pas simple** : il faut interroger, indiquer la fin de l'échange
- **efficacité** : interrogation stations qui n'ont rien à émettre → perte de temps
- **passage à l'échelle** : ajouter un user ⇒ augmenter le temps d'interrogation

b. Partage dynamique décentralisé / distribué

Pas de chef → chaque machine détermine son ordre d'émission

Exemple : méthodes à jeton, méthodes aléatoires

Avantages :

- **passage à l'échelle** : sans problème

Inconvénients :

- **qualité de service** : comment être sûr d'avoir une quantité de ressources ?

2 options :

- Méthodes **déterministes** : ordonnancement des machines → sans collisions
→ garantie de transfert
- Méthodes **probabilistes** : pas d'ordonnancement → avec collisions → sans
garantie de transfert

Chapitre 1 : Architecture et Standardisation

1 : Architecture réseau local

But : Définir un modèle générique indépendant de la technologie.

Architecture = **service rendu** par une fonction, ses **paramètres** et **unités échangées**.

Architecture → modéliser un réseau en définissant un certain nombre de niveaux et leurs rôles.

3 termes : **Entité, Service, Niveau**

- Entité effectue un service (ex : entité TCP réalise un transfert fiable d'info)
- Entité de niveau N va rendre un service de niveau N+1

Modélisation modulaire et mécanisme d'encapsulation

→ module modifié ⇒ ne change pas les modules qui "l'entourent".

Permet de modifier facilement le réseau.

Fonctionnement entités d'un niveau = décrit par **standards**

Favoriser le multiplexage = le plus de personnes possible qui transmettent sur le support, entrelacement des temps de paroles

Architecture IEEE : 3 niveaux pour favoriser le multiplexage sur le support:

- A - LLC (Logical Link Control)
- B - MAC (Medium Access Control)
- C - Physique

A - LLC (Logical Link Control)

But → demander les informations à transmettre (ex: protocole IP ou X25)

S'occupe du multiplexage et contrôle du lien entre deux entités

Réseau local identifie le protocole émetteur/récepteur grâce au **SAP** (Service Access Point)

SAP ⇒ faire la différence entre IP et X25.

En charge du contrôle

Si besoin → contrôle important → fiabiliser le transfert.

Plusieurs services définis

Chaque service ⇒ entité d'un certain type (1,2,...)

B - MAC (Medium Access Control)

But → Obtenir le **droit d'accès**

Récupère l'info du niveau sup (LLC) et la transmet quand il peut sur le niveau inférieur (physique)

Délivre une trame : avec des limitations, des adresses MAC

Contient champ détecteur d'erreur + autres champs selon protocole émetteur (ex: Ethernet, WiFi ...)

C - Physique

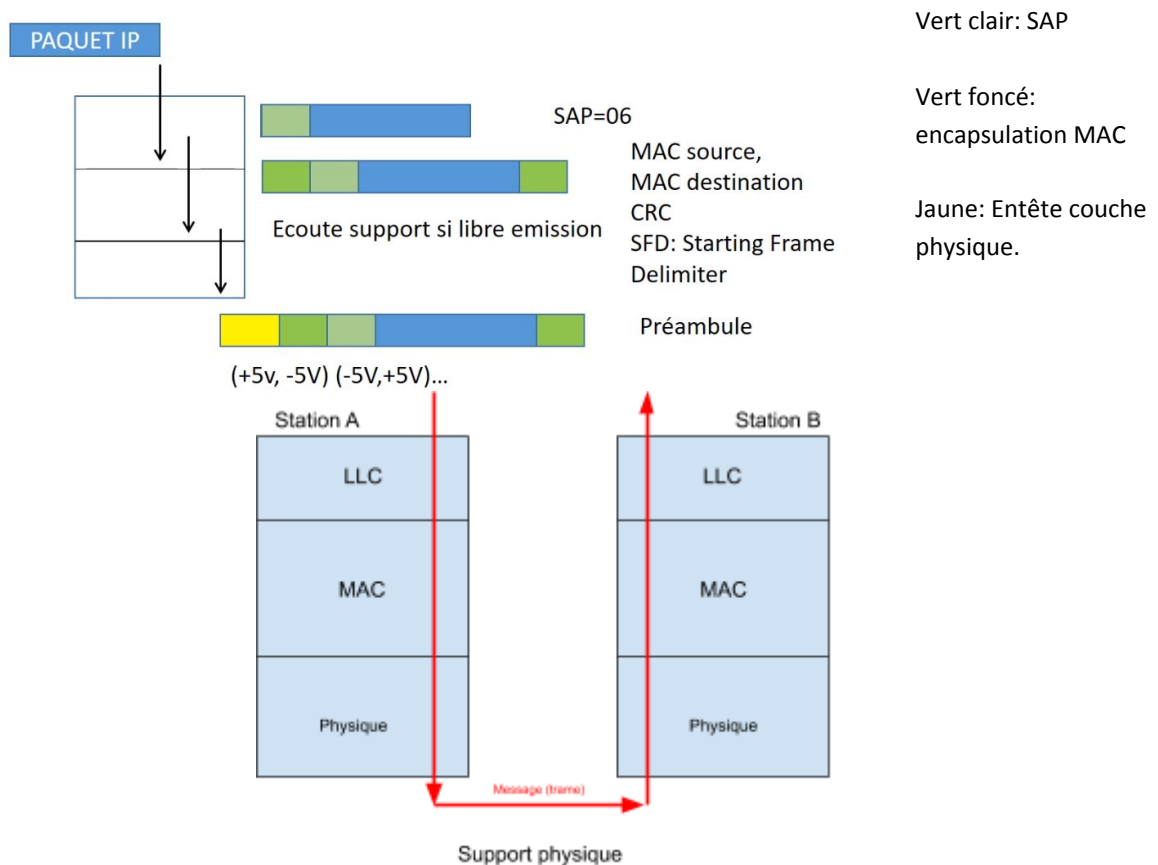
But → Transmettre sur le support (optique, air, cuivre) les trames de niveau MAC

Définir les codages (binaire, symboles...)

Séquence de synchronisation pour comprendre les symboles (avant la communication)

Différentes connectiques (RJ45, Optique, Radio...)

Illustration :



Utilisation d'éléments intermédiaires (routeur, bridge...) qui ne modifient pas le comportement des éléments terminaux (ordinateurs...)

→ Architecture est dite pontée.

3 types d'éléments intermédiaires :

- **Répéteurs** : Raccordement **niveau physique** (diffuse le signal au niveau 1)
- **Ponts** : Raccordements **niveau MAC** (relaye les trames au niveau 2)
- **Routeurs** : Raccordements entre **plusieurs réseaux** (au niveau 3)

2 : Standardisation des Réseaux Locaux

Intérêt de normalisation : assurer la **compatibilité** entre les produits de différents constructeurs

A - Standardisation

Réseau locaux : IEEE en charge de standardisation (comité 802) ⇒ standards nommés 802.X

- 802.1 : Architecture générale des réseaux locaux
- 802.2 : Échange de trame LLC
- 802.3 : Fonctionnement CSMA/CD sur bus (historique)
- 802.5 : Fonctionnement Token Ring
- 802.3z/3bs : Augmentation de la bande passante

Evolution de la standardisation :

- Disparition (802.4/5)
- Apparition pour suivre les évolution technologiques (802.3z/bs, WLAN/WPAN/WRAN)

2 niveaux de standards :

- Spécifique : définit 1 protocole sur 1 topologie
ex : produit Ethernet 802.3, produit WiFi 802.11
- Généraux : Valable pour tout les LAN
ex : 802.1

B - Adressage MAC

Protocoles MAC échangent des trames avec 2 adresses MAC (source/destinataire(s))
Adresses MAC notées sur 12 symboles hexadécimaux
Appelée Physical address ou Hardware address

a. Format

6 octets (0 -> 5)

1er bit : I/G (0 = Individuelle/1 = Groupe)

2è bit : U/L (0 = Universelle/1 = Administrée localement)

Universelle : Mondialement unique

3 premiers octets Identifiant Unique d'Organisation (OUI)

Même constructeur \Rightarrow champs OUI identique

Possible (maintenant) d'avoir un champ OUI de 20 voir 12 bits

3 octets suivant numérotation des composants de communication par l'organisation

b. Portée

Unicast : cible 1 seule destination (I/G = 0)

Multicast : cible plusieurs destinataire (I/G = 1)

Broadcast : tous les éléments du réseau (6 octets = 1)

\Rightarrow Définition d'un réseau local : groupe de machine pouvant recevoir un message broadcast par adresse MAC

c. Complément

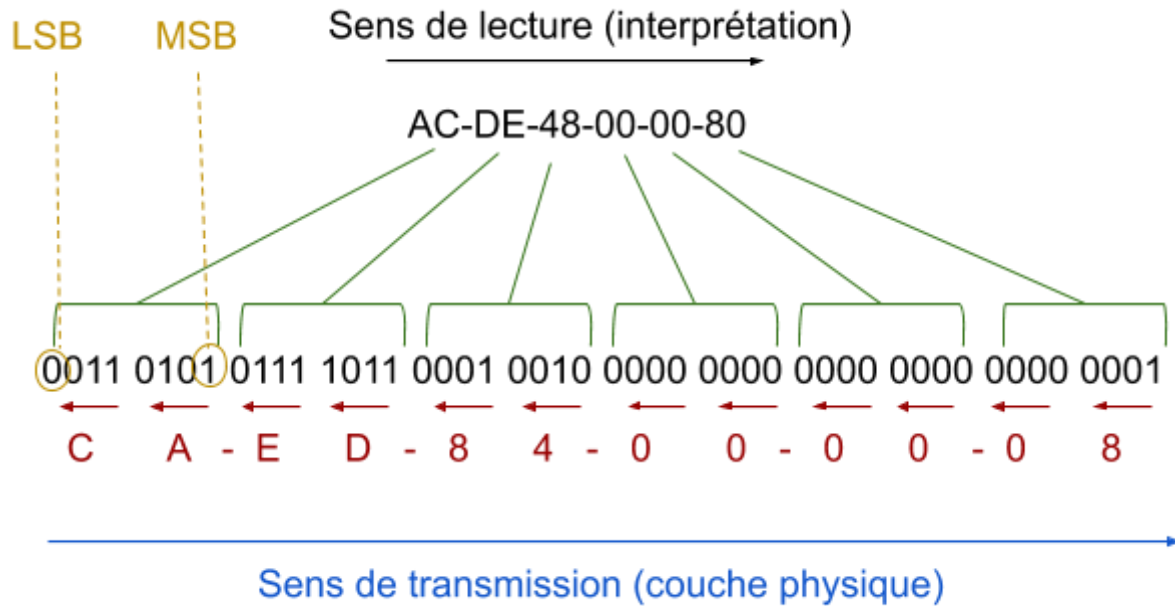
Adresse MAC \neq Adresse IP :

Adresse MAC dans le réseau local alors que Adresse IP de routeurs en routeurs

Adresse IP indépendant de la technologie, Adresse MAC changent à chaque réseau local

Trame de diffusion (Adresse de destination = FFFFFFFF) ne se propage pas au niveau IP (à travers les routeurs)

Attention à la transmission sur le support, les bits de chaque octet sont inversés



En rouge : comment c'est lu et interprété
par les couches supérieures

C - Couche LLC

802.2 : Échange de trame entre deux station d'un réseau local

3 types de **services** offert :

T1 : non fiable, ans connexion, sans acquittement (aucun contrôle)

T2 : fiable, orienté connexion (contrôle de la fiabilité avec mise en place de la connexion, numérotation des messages, acquittement)

T3 : sans connexion avec acquittement (contrôle sur l'arrivée pas la qualité)

ex : T1 : UDP / T2 : TCP / T3 : service intermédiaire

a. Format PDU

Les échanges vont être fait au moyen de PDU (Protocol Data Unite)

Format = identique quelque soit le service :

8 bits adresse DSAP (Destination Service Access Point)

8 bits adresse SSAP (Source Service Access Point)

8/16 bits contrôle

M*8 bits information (M entier)

Les champs SAP :

Identifient le protocole qui demande le service d'échange.

ex en hexa: 42 spanning tree (ponts transparents)

06 IP

AA si le protocole est identifié à un autre niveau

Champ contrôle :

1 octet déterminant le jeu d'instruction (trame de signalisation, trames numérotées ou non, numéro si oui ...)

b. Service LLC1

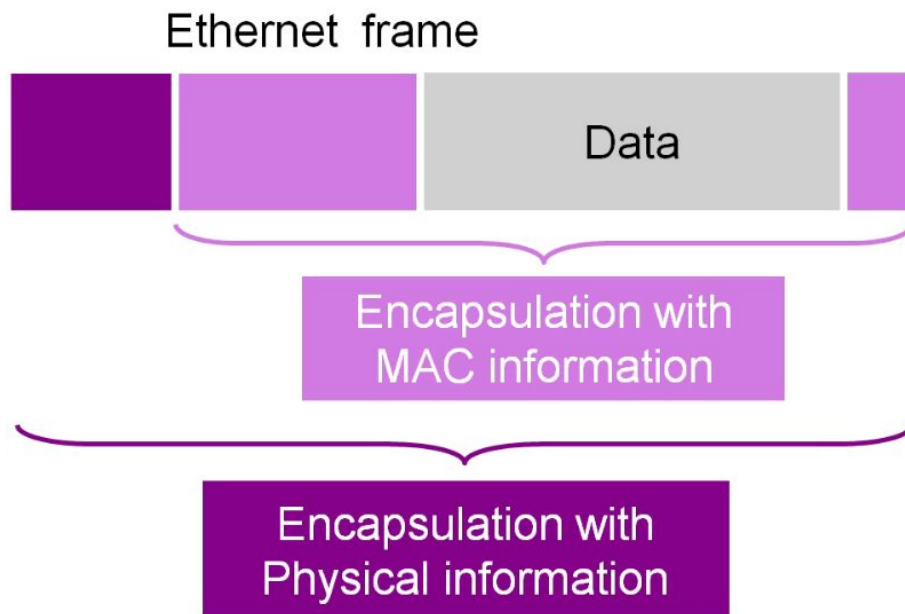
Utilisé dans les réseau locaux (échange entre ponts)

Envoie des trames non numérotées \Rightarrow code en hexa = 03

Chapitre 2 : Commutation et VLAN Ethernet

1 : Architectures Ethernet et formats de trames

Données encapsulées → info couche MAC, puis couche physique



A - Informations de la couche physique



Dans l'ordre :

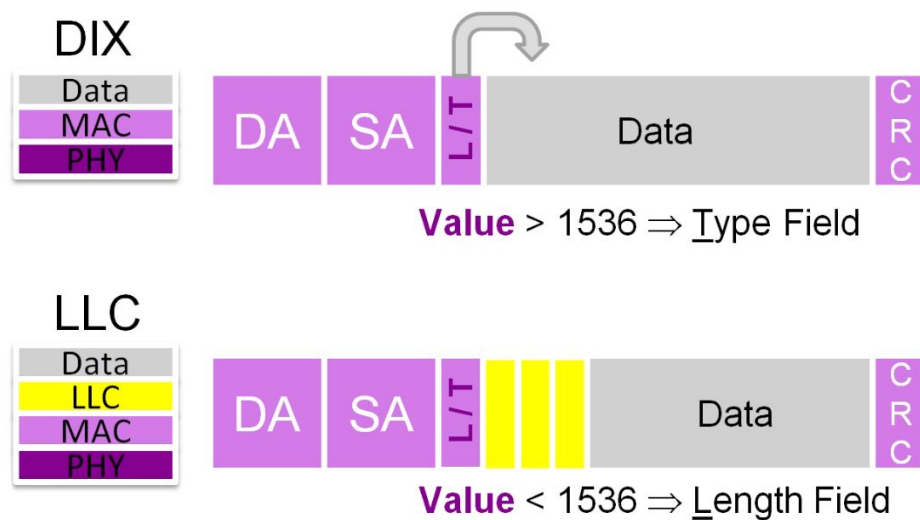
- 7 octets de Préambule → **synchronisation émetteur/récepteur** : 101010.....10 pour 10Mbps, symboles J et K pour 100Mbps...
- 1 octet de **Start-of-Frame Delimiter** → 10101011, signale au récepteur le début de la trame MAC.

B - Couche MAC

- 6 octets : adresse destination
- 6 octets : adresse source
- 2 octets : champ **L/T** (longueur/type)
- Données
- Champ de **padding** → **bourrage** ajouté car CSMA/CD impose une taille minimale de trame Ethernet (64 octets) → infos **inutiles**
- 4 octets : redondance → vérifie que la trame est **correcte, sans erreur de transmission**

Limitations de taille : 64B < trame Ethernet < 1500B

Champ LLC → différencie 2 architectures Ethernet : **DIX (sans LLC) ≠ IEEE (avec LLC)** → Différence dans l'encapsulation des données



En fonction des 3B du LLC : encapsulation SNAP

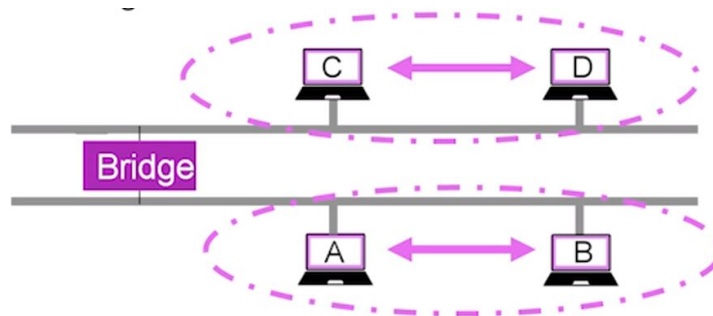
→ Champ T (type)



2 : Segmentation Switch et Apprentissage

Problématique : connecter au même réseau local des réseaux physiquement éloignés

A - Principe du bridge



Objectif d'un pont = relayer des trames entre 2 LAN

Mise en oeuvre :

- Écoute du LAN
- Décision de relayer ou non sur l'autre LAN
- LAN ont des formats MAC différents ? → adaptation des trames (ex: Wifi et Eth)

B - Table dynamique du bridge

Message passe dans le bridge → **Adresse source** ajoutée à la table ainsi que son **port associé**

Si adresse de destination dans la table → relayage vers son port associé

Sinon → Relayage sur tous les ports (sauf celui d'entrée)

Time To Leave = défini à l'entrée d'une adresse dans la table, reset à chaque passage d'une trame qui a la même adresse source

C - Switch VS Hub

Switch = pont → Trame relayée en fonction de la table dynamique

Hub = répéteur → Trame relayée sur tous les ports

3 : VLAN

A - Bases du VLAN

Portée du broadcast \Rightarrow différencier LAN et VLAN :

LAN Physique \rightarrow toutes les machines reliées physiquement

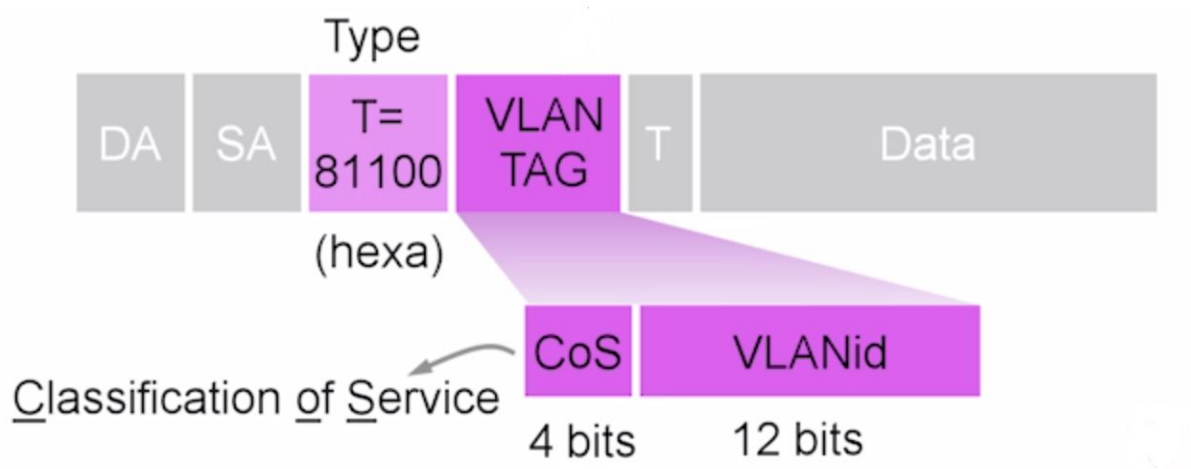
LAN Virtuel \rightarrow machines reliées physiquement **qui suivent certaines règles logicielles**

Politiques de règles logicielles :

- Par ports (problème si on déplace une machine)
- Par adresses
- Par applications (ex: VoIP sur un certain VLAN)

Fonctionnement basé sur les tables de relayage MAC \rightarrow **1 table par VLAN**

Câble multi-VLAN ? \rightarrow Modification de la trame Ethernet



CoS \rightarrow permet de définir une priorité par ex.

Avantages du VLAN :

- **Meilleure performance** \rightarrow broadcast limité
- **Flexibilité** car config logicielle
- **Sécurité** car VLAN ne communiquent pas entre eux

B - Administration des VLAN

2 étapes :

- Création (nom, id)
- Configuration (association de stations à des VLAN)
→ Admin. standard IEEE ou outils des constructeurs

2 modes de créations de VLAN sur un modèle client-serveur :

- a - **VTP** (VLAN Trunking Protocol)
- b - **VMPS**

a - Configuration VTP

Définir la configuration sur un switch serveur

Switch client branché → hérite des infos du VLAN

Config manuelle des ports sur chaque switch (serveur et client)

b - Configuration VMPS

Définir sur le switch serveur les **règles d'assignation** VLAN → dépendent de l'adresse MAC

Nouvel appareil sur switch client ? → interrogation du switch serveur → configuration du port sur un VLAN

C - Communications inter-VLAN

Interconnexion de 2 VLAN → **routeur qui appartient aux 2 VLAN**

Problème : interconnexion grand nombre de VLAN → Beaucoup d'interfaces routeur
→ Solution : **interfaces virtuelles**

Interface virtuelle :

Port physique multi-VLAN → les trames doivent indiquer dans quel VLAN elles se situent (= marquage de trames)

Changement de marquage lors d'un changement de VLAN

Chapitre 3 : Arbre recouvrant : STP, RSTP, MSTP

Réseau Internet = ensemble de switch qui relayent les trames grâce à un algo d'apprentissage

1 : Problèmes et solution au routage par apprentissage

Problèmes :

Solution contre les pannes : redondance

⇒ problème pour l'algo, le réseau ne fonctionne plus (instabilité, surcharge)

Solutions :

Désactiver le cycle en invalidant la transmission sur certains ports

Physiquement → architecture cyclique

Virtuellement → on ignore des ponts pour ne pas avoir de cycle → protocole d'arbre recouvrant (STP)

A - Principe de l'algo de Spanning Tree

Identification des ports et des ponts, et du coût (longueur du chemin) d'un port d'un pont. (coût du port 1 = 1 ⇒ émission d'une trame coûte 1)

Algo ST plusieurs étapes :

Etape 1 :

Choix du **pont racine** (pont de + petit id)

Etape 2 :

Détermination du coût d'un chemin d'un pont à la racine

Etape 3 :

Chaque pont : **port racine** (port le + proche de la racine, si égalité le plus petit id)
toujours actif

Etape 4 :

Détermination des ports de **relayage** :

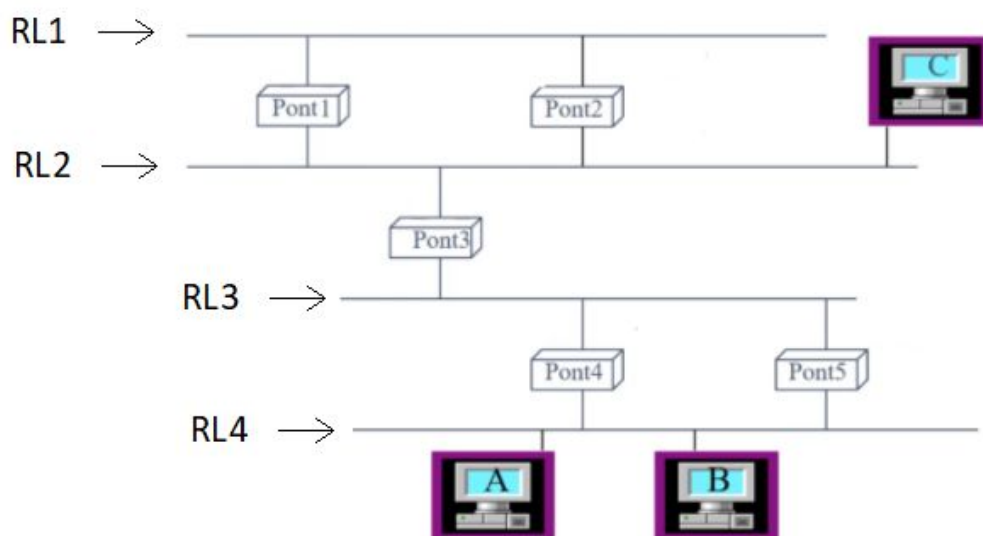
Port **racine** toujours en **relayage**

Si plusieurs ponts raccordés sur le même RL → un seul pont relaye par son port dit port **désigné**

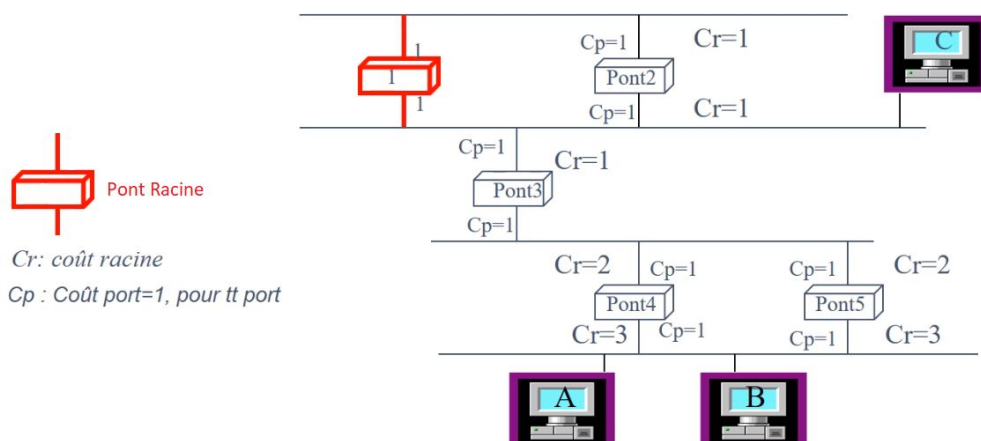
Désactivation des autres

Exemple :

Plan de base :

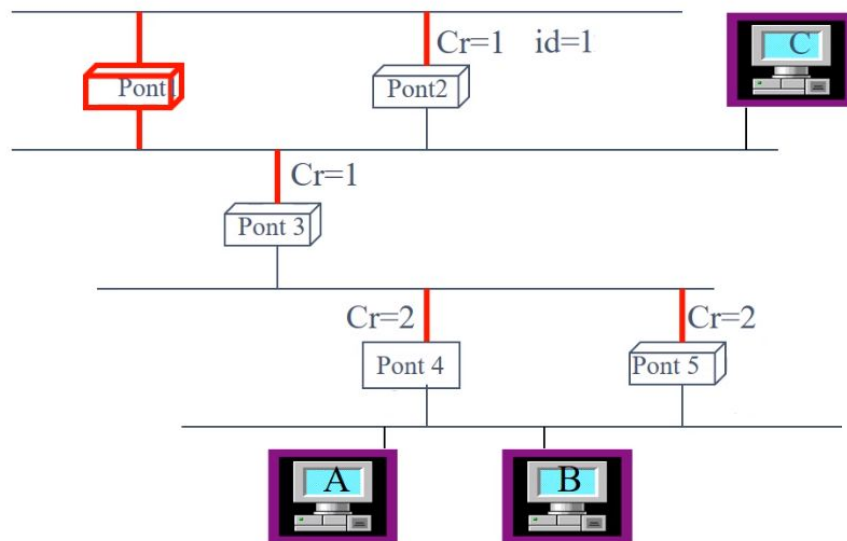


Etapes 1 et 2:



Etape 3:

Pour le pont 2 on choisit le port “en haut” car son id est plus faible

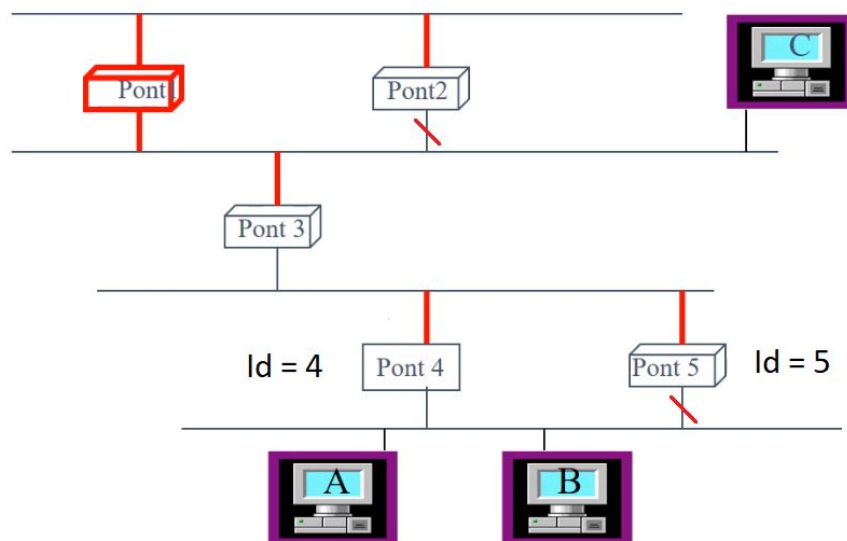


Etape 4 :

On ne bloque pas les ports racine.

On bloque les ports des ponts 2 et 5 :

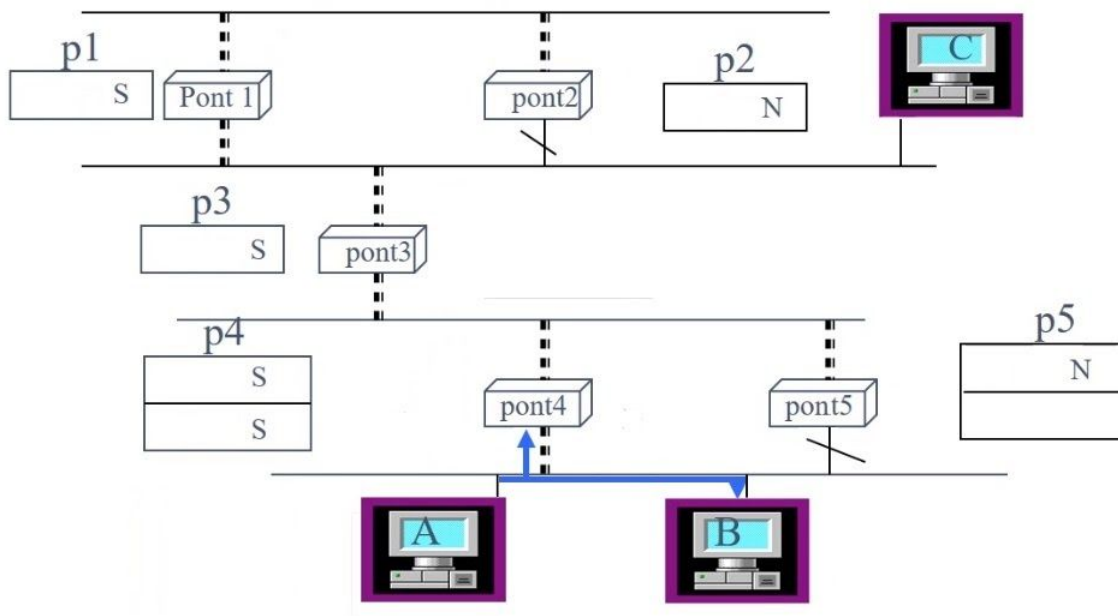
Pont 2/5 \Leftrightarrow Pont 1/4 mais plus grand Id



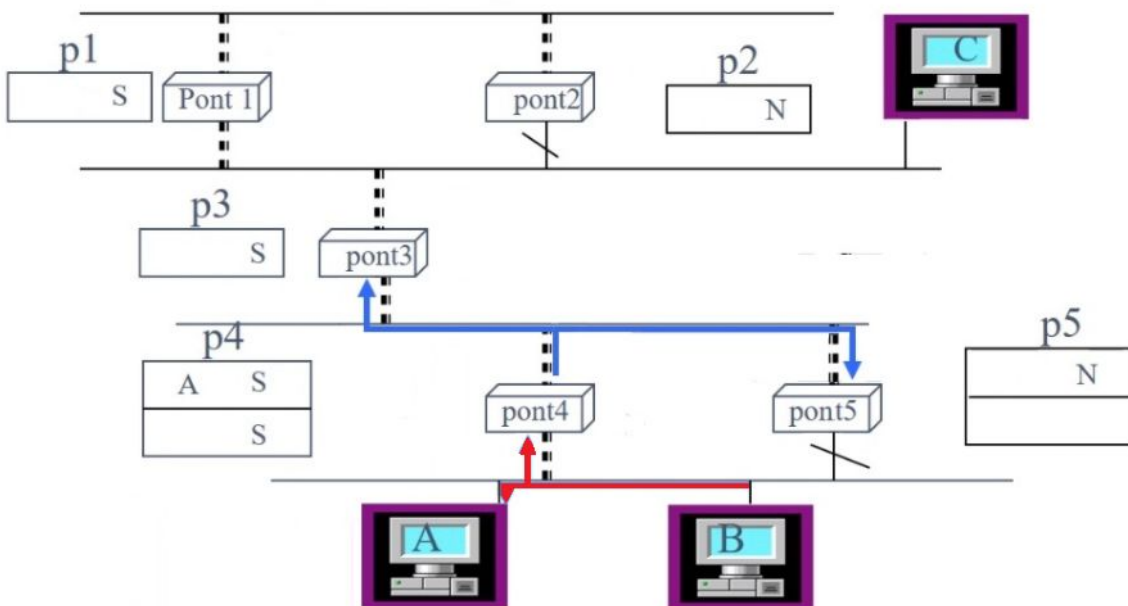
B - Routage par apprentissage

Exemple : sur un réseau vierge (le protocole STP a été appliqué) la machine A envoie un message à B.

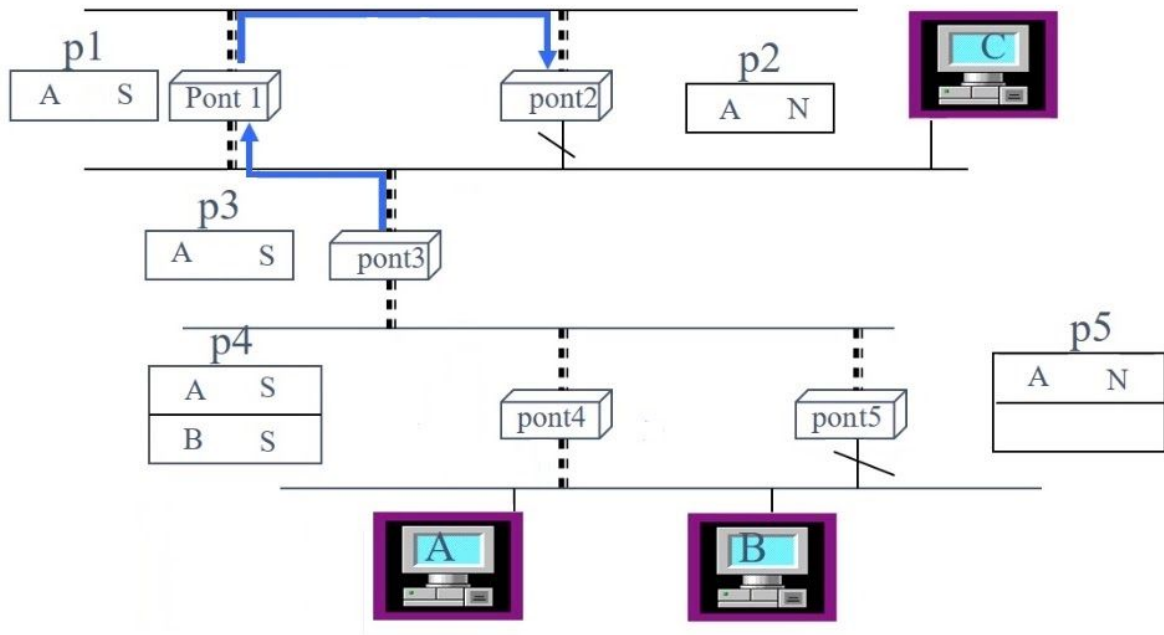
t0 :



t1 :



Le pont 4 enregistre B mais ne le transmet pas car B communique avec A et le pont 4 connaît A. L'algorithme continue et finit de notifier les autres ponts :



2 : Protocoles de STP

A - Protocole d'arbre recouvrant

Mise en place d'un arbre recouvrant : protocole (SPT, RSTP, MSTP) envoie des trames **BPDU** (Bridge Protocol Data Unit) à une adresse de groupe standard, celle des ponts (01 80 C2 00 00 00) (norme 802.1d--.Q)

BPDU échangées au niveau LLC via un service de transfert de trames LLC1

SAP de BPDU = 42

3 Infos dans BPDU :

Id racine (Ir)

Coût du chemin à la racine (Cr)

Id du port (Ibd)

BPDU1 meilleure que BPDU2 :

$ldr1 < ldr2$

$ldr1 = ldr2$ et $cr1 < cr2$

$ldr1 = ldr2$ et $cr1 = cr2$ et $lbd1 < lbd2$

Echange de BPDU :

Au début :

Chaque ponts envoie une BPDU aux autres disant je suis racine et distance = 0

Chaque ports reçoit BPDU des voisins

Pendant (cycliquement) :

Construction de la meilleure BPDU grâce à celles reçues

Mémorisation du port qui reçoit la meilleure BPDU (port racine)

Emission de la meilleure BPDU

Les ports non racine recevant une meilleure BPDU sont bloqués (WTF)

RSTP = RapidSTP établit un arbre + vite et accélère le rétablissement en cas de panne (convergence)

Donne des rôles aux ports désactivés (Alternate(racine) et Backup(désigné))

Détection de panne : 3 BPDU non reçus

Accélération de convergence -> **Pendant** + changement des rôles des ports

Ajout d'un lien :

Utilisateur (edge) -> port mis en relayage

Non edge -> **Début**

B - VLAN et Arbre recouvrant

Problème : isolation de VLAN

Solutions :

Créer un arbre par VLAN (PSTP vieux)

Regrouper des VLAN sur un même arbre (MSTP nouveaux)

3 : Autres routages-Alternative à l'apprentissage

A - Routage par la source (ou par noeud)

Recherche destination par diffusion

Relayage des informations sur le chemin

a. Principe de l'apprentissage

Station qui veut émettre vérifie sa table de routage, si AdrrDest non trouvée -> déclenche recherche

Recherche :

Pont recevant trame de recherche s'inscrit sur la trame (ne relaie que si Id et réseau non présent -> pas de problème de cycle)

Station destinataire : reçoit +ieur trames, choisit une route, renvoie la réponse

Source apprend également les routes

Autres possibilités pour l'apprentissage :

Recherche envoyée sur l'arbre STP

Destination envoie réponses à tout le monde

Source choisit la route

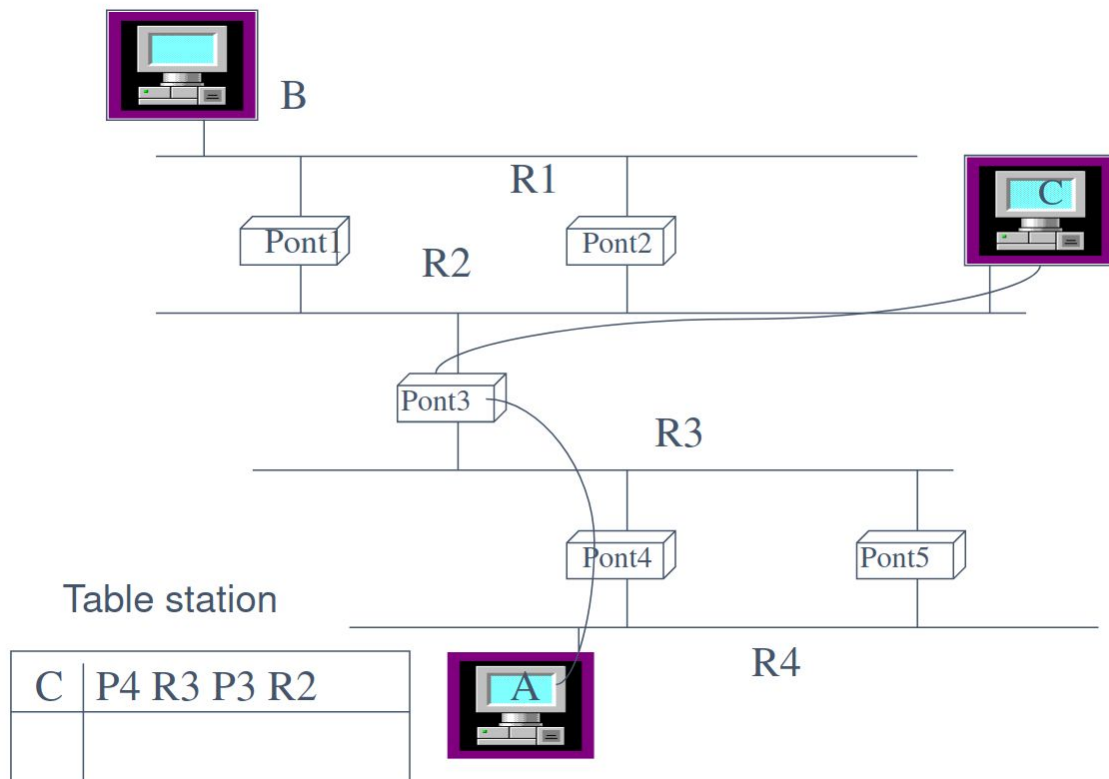
b. Principe du relayage

Champ chemin dans trame MAC

Route déterminée avant émission

Séquence de numéro de pont et de réseaux

Quand pont reçoit trame, il relaie à la suivante si existante sinon détruit



Chapitre 4 : Fonctionnement d'un lien Ethernet

1 : Support, débit et contrôle

A - Eléments de base

a. Support, débit et transmission

Possibilité d'éthernet d'évoluer :

Pas de changement au niveau MAC

Définition de nouvelle norme de transmission (Codage de symbole)

Nouvelle technologie (fibre optique)

Définir différents usage (=> nouvelles fonctions)

Support Connecteur RJ45 :

8 broches numérotées

4 paires colorées (P1 bleu, P2 orange, P3 verte, P4 marron)

Standard RJ-45 (T568B)								
Configuration des deux connecteurs pour un câble de réseau 100 mbps								
Pin	1	2	3	4	5	6	7	8
Couleur	blanc		blanc		blanc		blanc	
	orange	orange	vert	bleu	bleu	vert	brun	brun
Configuration du deuxième connecteur si "cross link" (T568A)								
Pin	1	2	3	4	5	6	7	8
Couleur	blanc		blanc		blanc		blanc	
	vert	vert	orange	bleu	bleu	orange	brun	brun

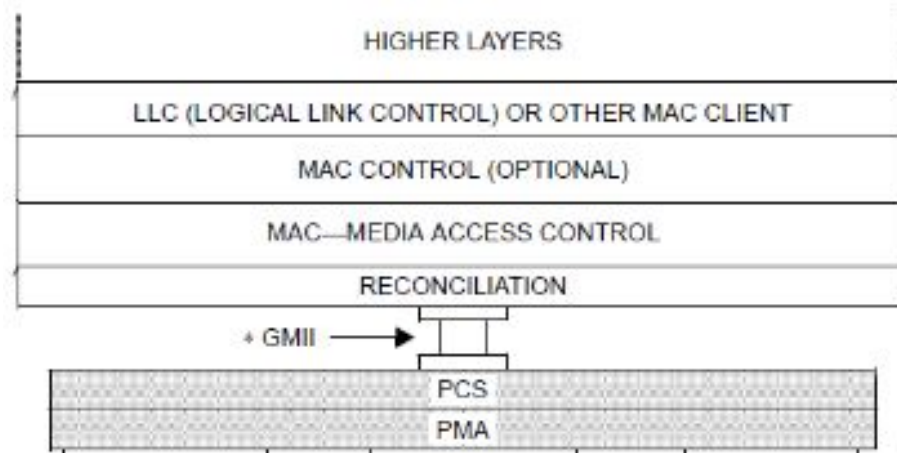
Fonction de transmission :

RS sous niveau de sous niveau de réconciliation, fournit la signalisation physique à la couche MAC : collision, signal présent, données reçues...

MII /GII: bus d'interface pour 'MAU' externes

PCS : sous niveau de codage (4B/5B, 8B/6T..)

PMA : mise en symboles transmissibles, gestion de la ligne



b. Contrôle de flux

Ethernet de base = half duplex mais évolution => full duplex

De configuration partagée (même support) → dédiée (1 station = 1 support)

Permet Full duplex sans CSMA/CD, mais problème de congestion

⇒ **contrôle de flux**

Trame de contrôle de flux :

Trame pause contenant durée de pause

Gérée par nouveau niveau MAC-c (control) (entre LLC et MAC)

Champ type 8808 et MCO = 0001

c. Autonegotiation

Plusieurs versions d'ethernet (évolution) => **fonction auto négociation**

Fonction d'auto-négociation :

Pour que 2 équipements communiquent entre eux (même débit et même fonctionnalité (half/full duplex))

Utilise des signalisation physique pour que les équipements se mettent d'accord (échange de **pulse**(elec) et mot de codes(optique))

Echange de pulse :

2 type de pulse

NLP : (Normal Link Pulse)

Pulses de Test (histo 10Mbps)

Transfert de données en codage manchester

Entre les données, vide : attente d'un fonctionnement correct

FLP : (Fast Link Pulse) aussi appelé Burst

Pulses rapide (100Mbps) pour négociation

Contient 33 pulse

Pulse impair horloge, Pulse pair information

Pulse pair : present => data = 1 absent => data = 0

Format de données FLP :

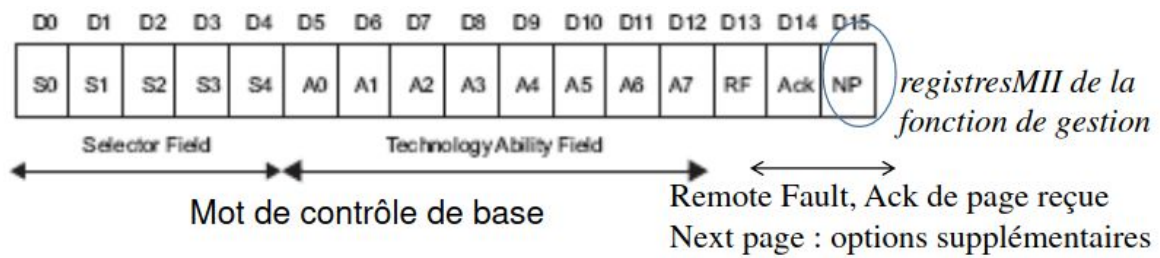
Les données transmises forment des mots registres octets

Le champ sélecteur d'un mot de code définit un réseau

Le champ Technology Ability Field définit :

La technologie physique 'PMA'

Le fonctionnement du contrôle de flux



Les pulses -> faire un choix selon priorités :

Plus grand débit possible :

- 10GBASE-T full duplex
- 1000BASE-T full duplex
- 1000BASE-T
- 100BASE-T2 full duplex
- 100BASE-TX full duplex
- 100BASE-T2
- 100BASE-T4
- 100BASE-TX
- 10BASE-T full duplex
- 10BASE-T

full duplex > half duplex

Protocole d'autonegociation :

Émission cyclique du mot de contrôle

Réception de 3 mots consécutifs identiques (hors ACK) => positionné ack et émettre

Autonegociation Ethernet optique :

Au niveau PCS

Pas d'utilisation FLB mais mots de codes

Mot de registre similaire à celui transmis via les FLP

B - Amélioration de performances

a. Augmentation des longueurs de trames

Augmentation de la taille min et max :
pour augmenter la distance et les encapsulation
-> Pb de compatibilité

min :

version 1Gps partagée modifie :
la taille 64 minimale -> 512 octets
temps inter trame 96bits -> 96 octets

Solution :

Ajout d'un champ optionnel pour compléter les trames
Groupement de trame

max :

Jumbo frame , trames géantes de 9000 octets

b. Agrégation

Plusieurs liens entre machines :

Améliore la robustesse/la fiabilité du réseau
Augmente aussi la puissance si utilisé en parallèle et non en backup

Utilisation :

Un serveur multcartes sur un switch
Raccordements inter switch

Principe d'émission sur une agrégation :

1 conversation/communication = 1 lien (éviter déséquilibrage)
Répartition des conversations selon le constructeur

Regroupement de port :

Agrégation gérée par une sous couche LACP (Link Aggregation Control Protocol) entre LLC et MAC-c

Ports \in à une agrégation doivent avoir :

mm débit

mm utilisation (full/half duplex)

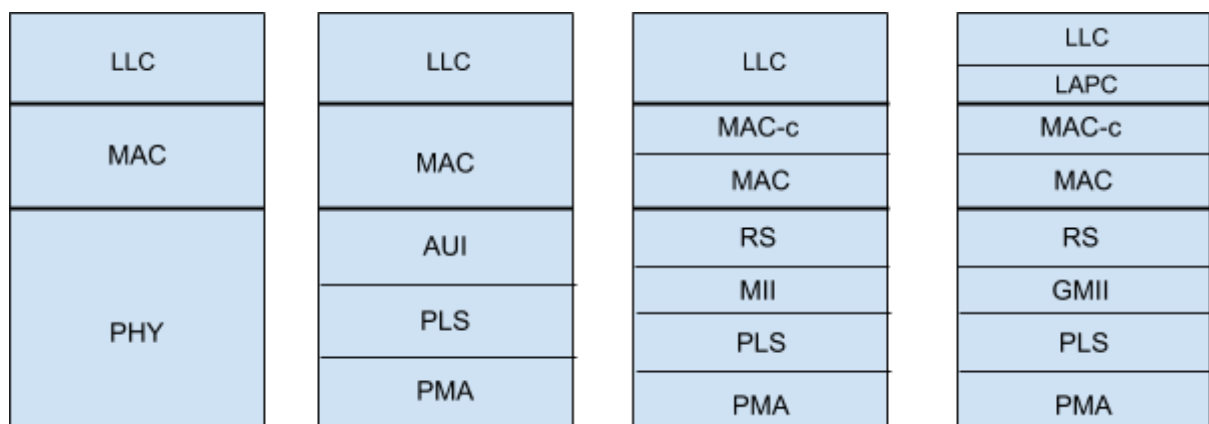
mm VLAN/priorité

Champ type 8809

c. Consommation d'énergie

Définition d'un mode basse consommation d'énergie quand on émet pas.

2 : Résumé des couches



Evolution de couches dans le temps

Chapitre 5 : WiFi

1 : Éléments de base

Wifi = nom pour produits certifiés **802.11**

Support partagé (ondes radios) → nécessité de **méthodes d'accès**

Plusieurs couches physiques, une seule couche MAC

→ couches physiques adaptées environnement (indoor/outdoor) ou au service (VoIP..)

Version la plus récente : **802.11ax**

A - Caractéristiques d'une transmission

a. Bandes : 2,4Ghz ou 5Ghz

Bandes "libres" → très utilisées (2,4Ghz très encombrée)

Problème de compatibilité (communication équipement 2,4 - équipement 5 impossible)

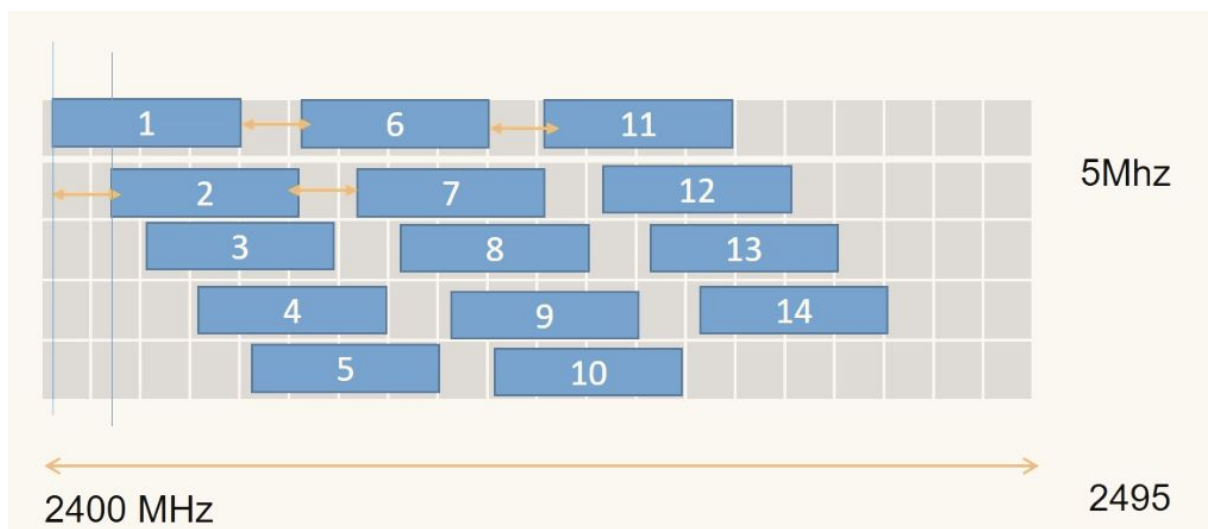
→ Solution : pontage : réseau disponible sur les 2 bandes

Bande 2,4Ghz:

Divisée en 14 canaux de largeur 22MHz, espacés de 5MHz

Canaux avec recouvrement → limité à 3 par point d'accès

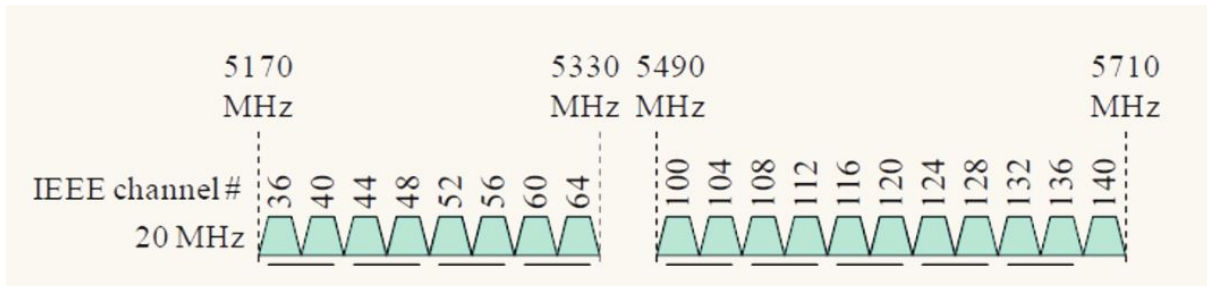
Canaux disponibles = décidé par pays ou continents (France → 1, 6 et 11)



Bande 5Ghz :

2 sous-bandes, canaux de 20MHz

Utilisation de 1 canal ou 2+ canaux adjacents



b. Modulation et constellations

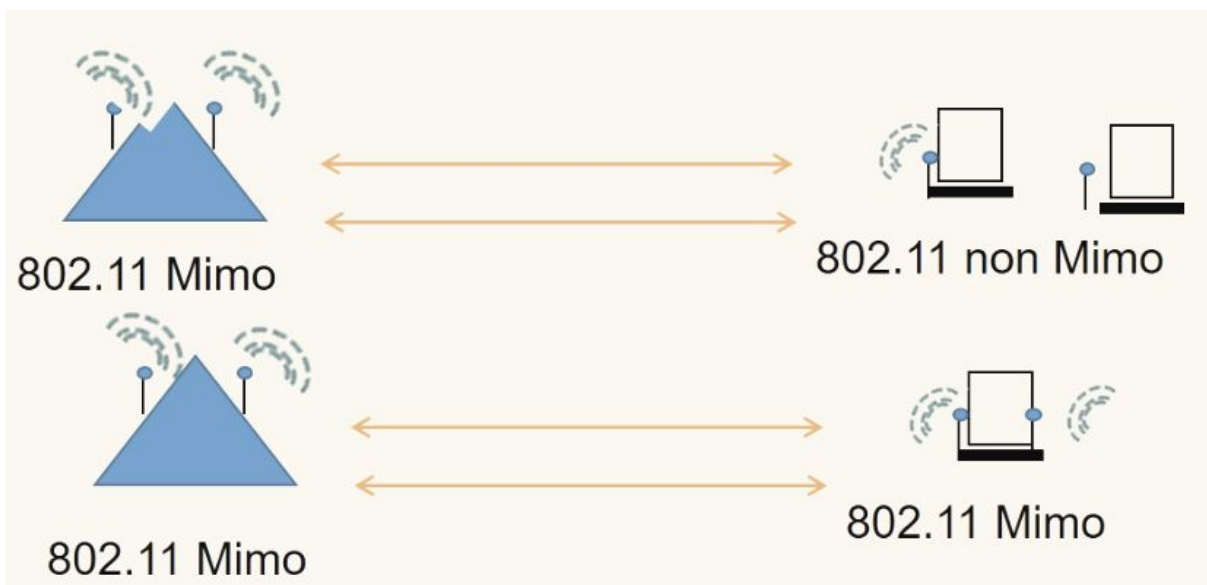
cf télécom

c. Diffusion MIMO

MIMO = Multiple Input Multiple Output

Principe → diffuser sur 2 flux

Si un seul destinataire → Single User MIMO

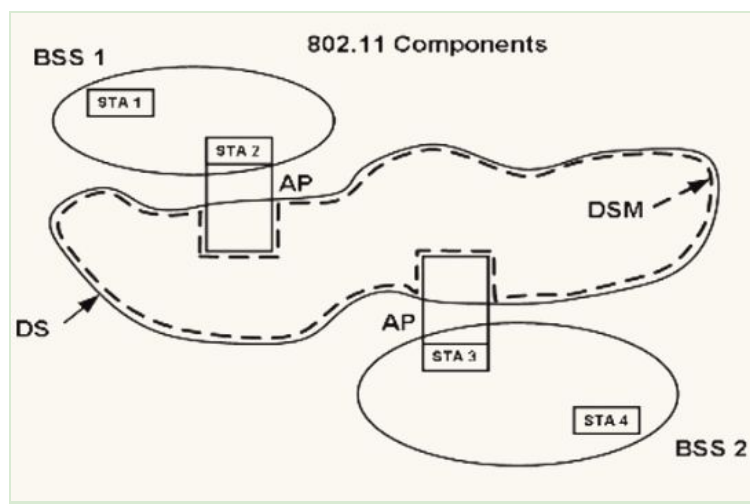


B - Les architectures réseau

Déf : Cellule = ensemble de terminaux à portée

Vocab :

- AP : Point d'Accès
- STA : station
- BSS (Basic Service Set) = AP et les stations situés dans sa zone de couverture
- BSA (Basic Service Area) = Domaine de couverture d'un AP dans un BSS
- DS (Distribution System) = Système qui connecte des BSS entre eux
- DSM (Distribution System Medium) = Moyen physique pour connexion à l'AP



2 modes d'architecture:

- Cellule sans infrastructure : terminaux reliés directement = **mode adhoc**
- Cellule avec infrastructure : terminaux en mode point d'accès (AP)

Réseau = ensemble de cellules → routage avec pont/routeur entre 2 AP

Architecture en 3 phases :

1 - Découverte de l'AP

Configuration préalable de l'AP (SSID, canaux, auth, ...)

2 modes de découverte :

- passive : AP émet des trames **Beacon** → indique son SSID, adresse, ..
- active : STA émet des trames **Probe request** → demander l'accès aux réseaux qui l'entourent. Réception de **Probe response**

2 - Association

- Choix de l'AP
- STA Demande à AP → obtention d'un **AID** (id d'association)
- Association acceptée → demande d'adresse IP (DHCP)
- Mise en oeuvre : routage, sécurité, ...

Si auth échoue → trafic bloqué sur le port (en wifi : port ↔ AID)

3 - Transmission de données : utilisation de différentes méthodes d'accès

2 : Gestion de l'accès au support

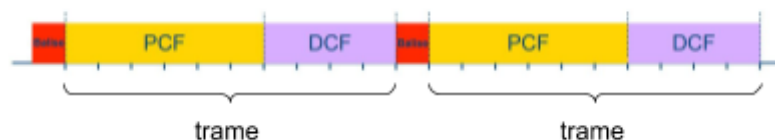
Wifi implante 2 méthodes d'accès : **DCF** (basé sur [CSMA/CA](#)) et **PCF**.

En mode adhoc → seulement DCF

En mode infrastructure → seulement DCF **OU** DCF et PCF en même temps

But de cette partie → expliquer ces 2 méthodes

Exemples de trames en mode infrastructure (AP-STA) :



A - DCF (Collision Avoidance)

a. Principe

Basé sur le CSMA/CA → éviter les collisions

Trames séparées par **SIFS** (Short Interframe Space)

STA veut émettre → écoute du support

Si libre pendant **DIFS** (DCF Interframe Space) → émission d'un **RTS** (Request To Send)

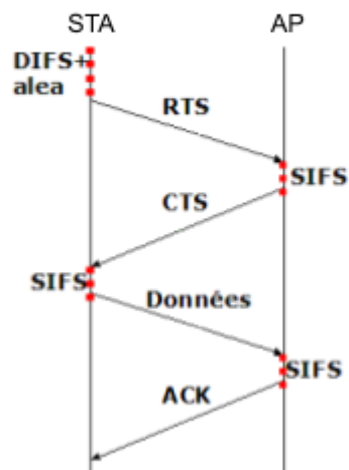
Si réception d'un **CTS** (Clear To Send) → envoi des données

Si occupé ou non réception du CTS → attente de disponibilité support + retard (backoff) avant de transmettre (cf [CSMA/CA](#))

Après émission → attente ACK

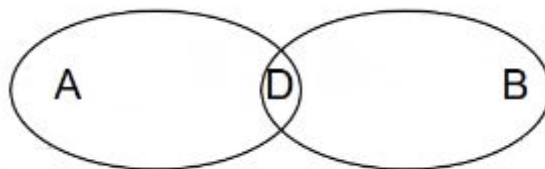
ACK non reçu → retransmission

Exemple : transmission DCF



b. Problème de la station cachée

Exemple :



STA A et STA B ne s'entendent pas → peuvent croire que le support est libre → peuvent émettre en même temps → collisions

Solution : RTS et CTS → AP et STA préviennent tout le monde de l'émission → les autres attendent → pas de collisions

B - PCF (polling)

Basé sur un mécanisme de polling → interrogation des stations, chacune son tour
(cf [Méthode par interrogation \(polling\)](#))

3 : Améliorations au niveau MAC

But → favoriser certains services (ex: multimédia)

A - Économie d'énergie

Objectif → mettre les stations en sommeil quand il n'y a pas de trafic

Mise en oeuvre: (ex: station A envoie des données à B)

- l'AP stocke le trafic à destination de B
- l'AP indique périodiquement si trafic en attente
- B dort et se réveille cycliquement → vérifie si trafic en attente
- si oui : l'AP lui donne les données stockés

l'AP indique si trafic en attente → trames **Beacon**

Amélioration : **APSD** (Automatic Power Safe Delivery)

- Sans APSD (mode non ordonné) → l'AP envoie les données en attente **après demande de la STA**
- Avec APSD (mode ordonné) → l'AP **impose le temps de sommeil** → envoie les données en attente sans prévenir

B - Qualité des services (WMM)

WMM = Wifi MultiMedia

Besoins : transmettre certaines infos plus vite que d'autres ; garanties de délai

Solutions : mécanisme de priorité ; limiter les autorisations d'émettre

Extension de DCF et PCF dans la couche MAC :

- **EDCA** (Enhanced Distributed Channel Access) → priorités
- **HCCA** (HCF Controlled Channel Access) → limitation des autorisations

a. EDCA : priorités

4 classes de priorités : **AC** (Access Category)

8 niveaux de priorités

Priority	UP (Same as 802.1D user priority)	802.1D designation	AC	Designation (informative)
Lowest ↓ Highest	1	BK	AC_BK	Background
	2	—	AC_BK	Background
	0	BE	AC_BE	Best Effort
	3	EE	AC_BE	Best Effort
	4	CL	AC_VI	Video
	5	VI	AC_VI	Video
	6	VO	AC_VO	Voice
	7	NC	AC_VO	Voice

3 types de priorités (chaque classe a des valeurs différentes pour chaque type) :

- Priorité d'accès au support
- Priorité de retransmission (en cas de collision)
- Priorité en quantité de données transmises

b- HCCA : accès contrôlé

TxOP (Transmit Opportunity) = nombre de trames qu'une STA peut transmettre après avoir reçu un CTS (autorisation de l'AP, voir [Problème de la station cachée](#))

HCCA inspiré du polling PCF (voir [PCF \(polling\)](#))

Principe : l'AP alloue des TxOP à chaque station