Chap 1 :

modele osi:

couches:

application : donnees

presentation : donnees

session : donnees

transport : segmentation et la numerotation de segments

reseau : paquet et ajouter @IP source et la

destination reseau

liaison donnees : trame @Mac source et

destinataire

physique : bit si le msg va quitter en un signal carte rx

numerique alors codage en ligne

si le msg va quitter en une onde alors la modulation (transposition de frq)

***durant l’encapsulation :***

la donnee= SDU :service data unit

l’entete de la couche= PCI :protocol control information

après le passage d’une couche= PDU :Protocol data unit

SDU(couche N)+PCI(N)=PDU(N)=SDU( couche N-1)

Chap 2 :

Pour se connecter a internet il nous fait un modem ADSL pour faire la modulation et il joue le rôle d’un commutateur

Un équipement qui possède les 7 couches il fait partie de la 7eme couche

7-Couche APP : pc, serveur TCP/IP

3-Couche RES : commutateur 3, routeur

2-Couche LIAI : pont, commutateur 2

1-Couche PHY : répéteur, concentrateur(repeteur multiports),hub

Equipement nv 1 : lorsqu’il recoit un signal il va le régénérer, on l’utilise dans le cas du signal atténué (affaiblie)

Vitesse de propagation=dist /temps de propagation

Lorsqu’il recoit un msg il le transmet/diffuse vers tout le monde et tt bêtement

\*niv phy

\*pas de gestion de collision

\*diffuse la collision(erreur)

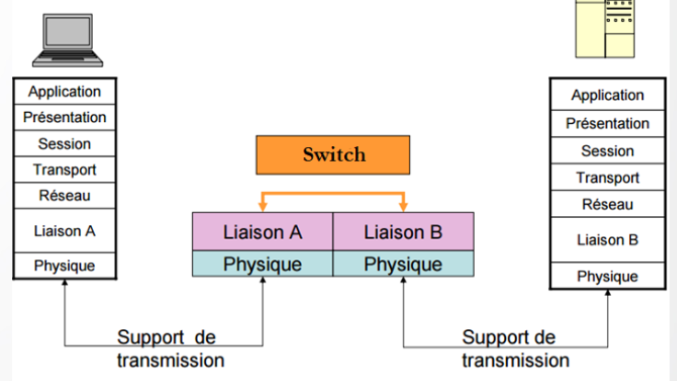
Topologie Physique: c’est l'arrangement physique des machines dans le réseau. C'est-à-dire la configuration spatiale du réseau

Topologie Logique: représente la façon dont les données transitent sur le réseau

Equipement nv 2 :

-Un commutateur est un élément actif agissant au niveau 2 du modèle OSI.

-Multiport permettant de relier plusieurs machines ou plusieurs segments (des machines en bus) d’un même réseau.

\* capable de délimiter la trame (Identification de la destination, Identification de la source) : 8o :préambule, 6o :@des,6o :@src

Par la suite le switch va réaliser une table de commutation compose de l’@mac de la machine et son nbre de port.

LES (++)

\*En cas de collision, seules les machines sur la liaison où la collision a eu lieu sont impactées.

\*Utilise des mécanismes de gestion de collision

\*niv 2 : liaison donnees

\*Aiguillage de trafic

\*Améliore l’exploitation de la bande passante

\* Dispositif actif simplement configurable

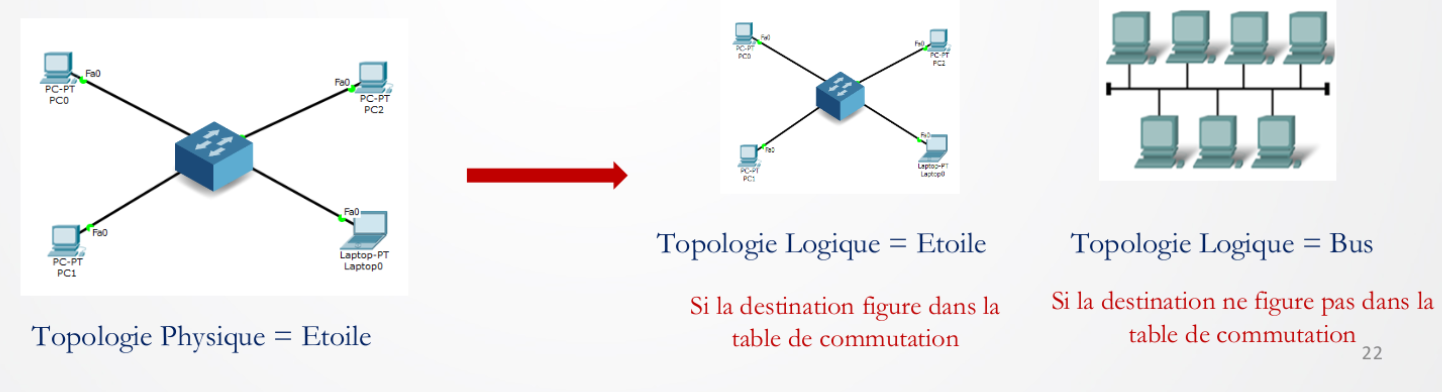
\* Permet d'augmenter la distance entre deux stations dans un réseau local

\*pas de propagation de l’erreur

LES(--)

\* Diffusion systématique des données vers tous les ports

\*Problème de sécurité : Tout le monde à l’écoute



La latence: C’est le temps que va mettre le switch à analyser la trame avant de la retransmettre.

La fiabilité: C’est probabilité de transmettre des trames non erronée.

Commutation Store and Forward

La trame entière doit être reçue avant de pouvoir être acheminée.

* Arrivée de la trame
* Stockage de la trame
* Commutation vers le port de sortie

Avantages: Traitement des erreurs, utilisation du CRC

Inconvénients: La latence est plus élevée dans le cas des grandes trames, car la trame entière est plus longue à lire.

Commutation Cut through

arrivée de la trame

* Lecture des premiers octets (début en-tête Ethernet)
* Commute la trame vers le destination en fonction de l'adresse destination .

Avantages: Temps de latence faible

Indépendant de la longueur de la trame

Inconvénients: Retransmission des erreurs

Commutation fragment-free

* Lecture des 64 premiers octets avant retransmission

Avantages: Filtre les fragments de collision avant de commencer la transmission.

Elimine les erreurs de type « Runt»

N.B : Tout fragment d’une taille supérieure à 64 octets constitue une trame valide et il est habituellement reçu sans

erreur donc acheminée avant d'avoir été entièrement reçue.

Equipement nv 3 :

Routeur : Fonctionne au niveau 3 (paquet).

Nv3 : couche reseau

Topologie physique : etoile >>> topologie logique : etoile

Domaine de collision

Nv 1 : tout le reseau local

Nv2 : chaque port du pont, Chaque port du switch

Domaine de diffusion

Tous les ports d’un Hub ou d’un pont(bridge) appartiennent au même DD

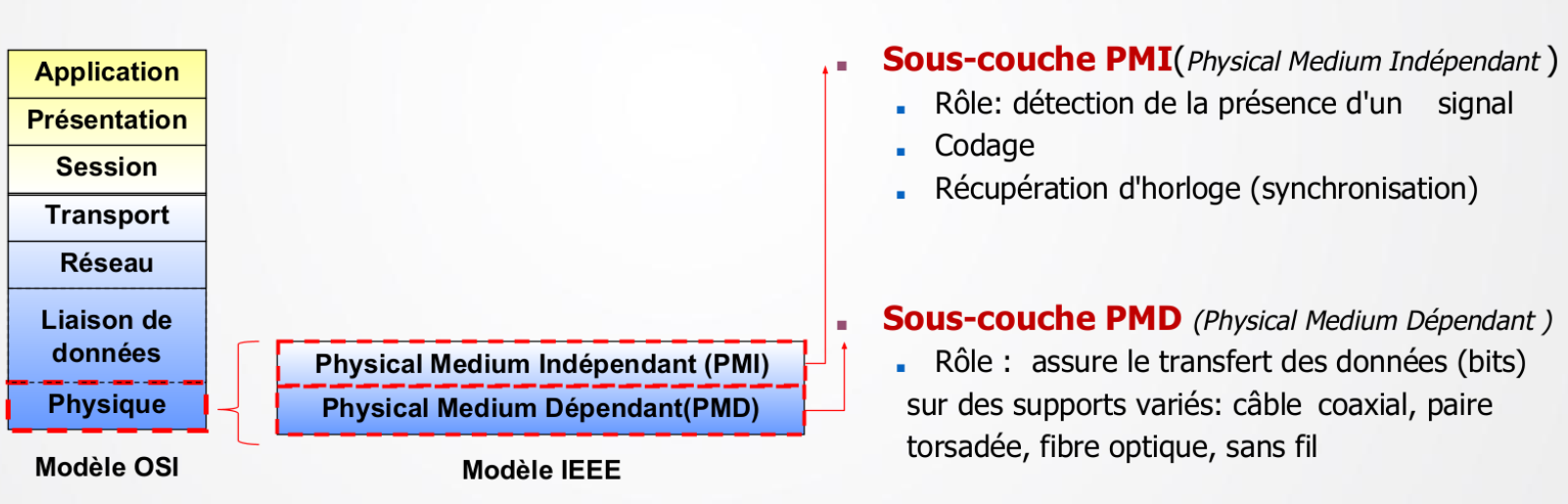
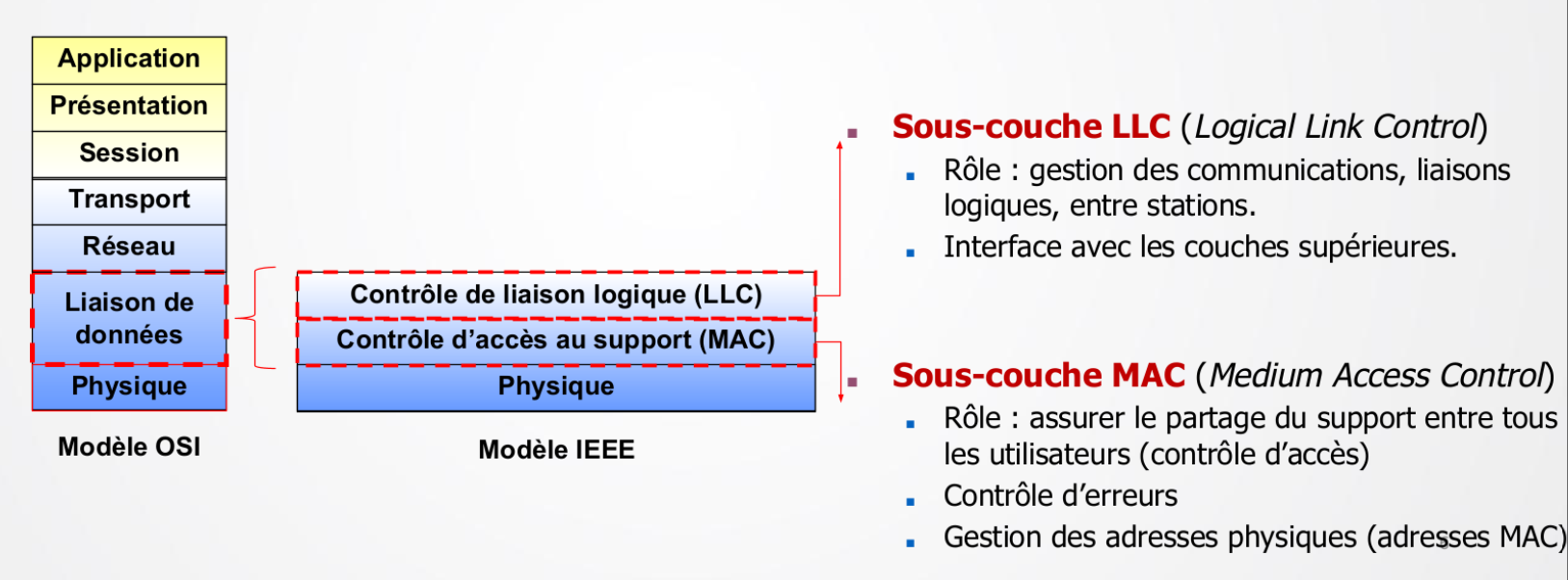
CHAPITRE 3 : ETHERNET (1500 octets)

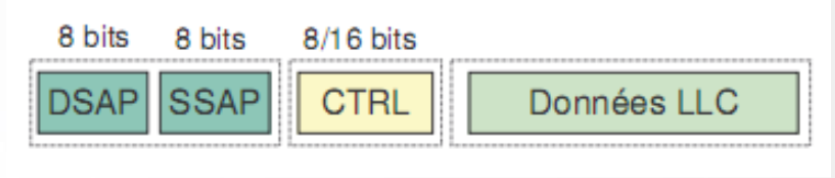
802.3 (entête 18 octets)

Lan : méthode de transmission de données opère la couche 1 & 2 du modèle OSI

1. Ethernet : Technologie de transmission d’information sur un réseau local câblé, Initialement destiné à une topologie en bus, avec une diffusion de la trame sur tout le support partagé, juste l@dest l’accepte et les autres la rejette, il trouve 2 types :

* Ethernet DIX est standard réalisé principalement par Digital, Intel et Xerox
* Ethernet 802.3 est la norme élaborée par l’organisme IEEE

1. IEEE devise la couche phy en 2 autres couches (PMI,PMD)
2. IEEE devise la couche liaison en 2 couches(LLC,MAC)

IEEE 802.3 encapsule LLC

* Format & Champs Trame LLC :

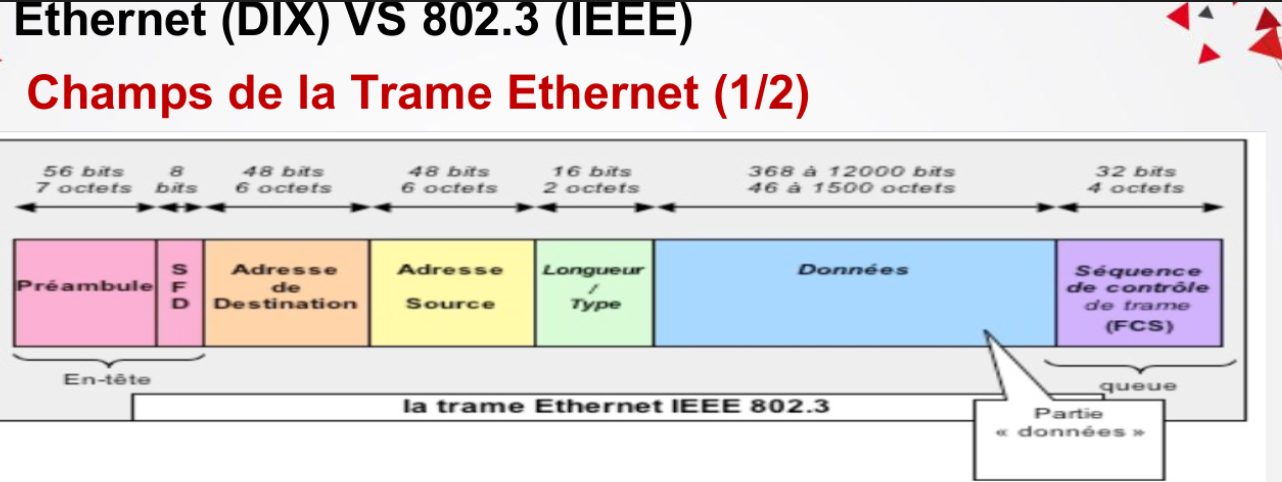
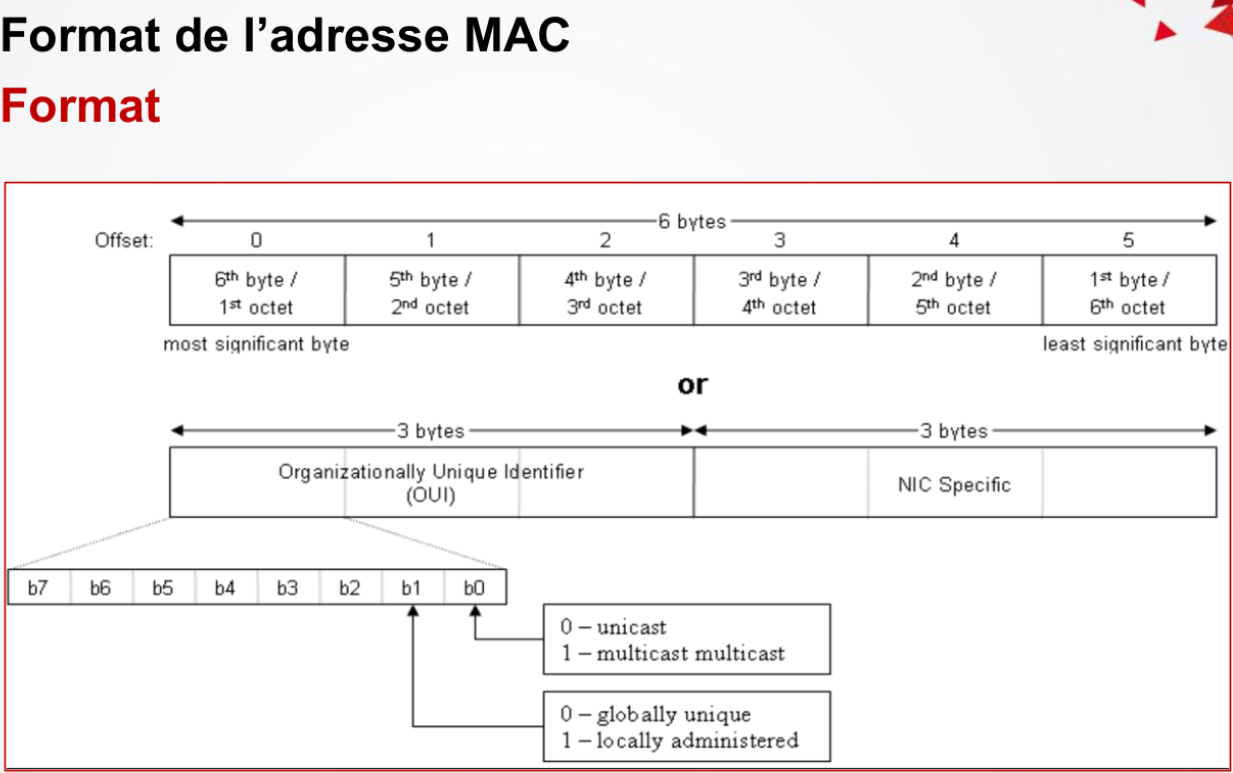
Le champ DSAP désigne le protocole de niveau supérieur (Niveau 3) à qui seront fournis les données.

* DSAP (Destination service access point) : 1 octet
* 1er bit :(individual bit=0/group bit=1)
* adresse fonctionnelle(traitement specifique)

Le champ SSAP désigne le protocole réseau qui a émis la trame LLC.

CTRL (FC : Frame Contol) : 1ou 2 octets

3 types de trames (I:Information / S:Supervision / U:non numérotées)

La sous-couche MAC : elle permet l’Encapsulation des données, Accès au support de transmission et elle depend du support utilise.

Probleme de collision

Tranche Canal TC : C’est la durée pendant laquelle il y’a un risque de collision + Détection de collision

Solution : CSMA/CD

* Méthodes d’accès dynamiques
* Listen before talking : si une station veut émettre, elle écoute le canal pour savoir s'il y a déjà une autre émission en cours (présence ou non de porteuse ). Si oui elle attend, sinon elle émet.
* La station émet pendant une durée minimale (le temps de transmssion T tr)(supérieure au temps maximal d'aller et retour du signal entre 2 stations= 2xTp), ceci afin que son émission puisse être détectée par les autres stations et donc d'éviter d'autres émissions simultanées.
* Cependant elle continue à écouter pendant son émission (au moins 2xTp) afin de vérifier que ses données n'ont pas générées une collision : Listen while talking

CHAPITRE 4 : WIFI (2300 octets)

802.11

* WLAN: wireless local area network
* MODES DE COMMU SANS FILS :



1. AD HOC

Les machines appelées « nœuds »

* chaque machine joue en même temps le rôle de client et le rôle de point d'accès.
* **services de base indépendants IBSS** ( Independant Basic Service Set), (constitué au minimum de deux stations ) est un réseau sans fil   
  restreint : le mode ad-hoc ne propose pas de   
  système de distribution capable de transmettre   
  les trames d'une station à une autre.
* **Ad hoc – Domaines d’application**
* monument historique
* Réseau de courte durée

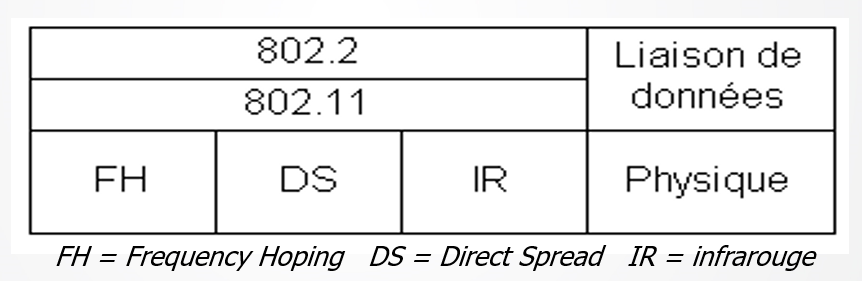
1. **Mode avec infrastructure**

* Les machines partagent la bande passante disponible.
* Fonctionne via une topologie en étoile
* L’AP (Access point), est muni d'une interface de communication sans fil pour la communication directe avec les Unités Mobiles
* **Architecture**
* **BSS (*Basic Service Set*)** =AP (point d’acces)+ Ums (les unites mobiles)
* **BSSID:** Identifiant de 6 octets pour le BSS, correspondant à l’adresse MAC du point d'accès.
* **ESS (*Extended Service Set*)** ou simplement **SSID**:

Un ensemble de services étendu reliant plusieurs BSSs par une liaison système de distribution(ethernet, wifi, cable..)

**La norme IEEE 802.11**

* **Architecture en couches:**



**Méthode d’accès CSMA/CA**

* **CSMA/CD** est non applicable pour les WLANs: Dans un

milieu sans fil, il est possible que toutes les stations ne soient pas à portée radio les unes des autres. Or, CSMA/CD se base sur le **principe que le signal se propage à toutes les stations du réseau à un instant donné.**

* Deux types d’accès au support sont normalisés:

**-PCF (Point Coordination Function)**

**-DCF (Distributed Coordination Function)**

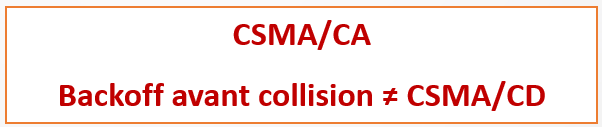
* **Problème de la station cachée:**
* **Problème de la station exposée:**
* **DCF (Distributed Coordination Function)**

Utilisé à la fois pour les communications via un AP et pour les communications directes d’UM à UM.

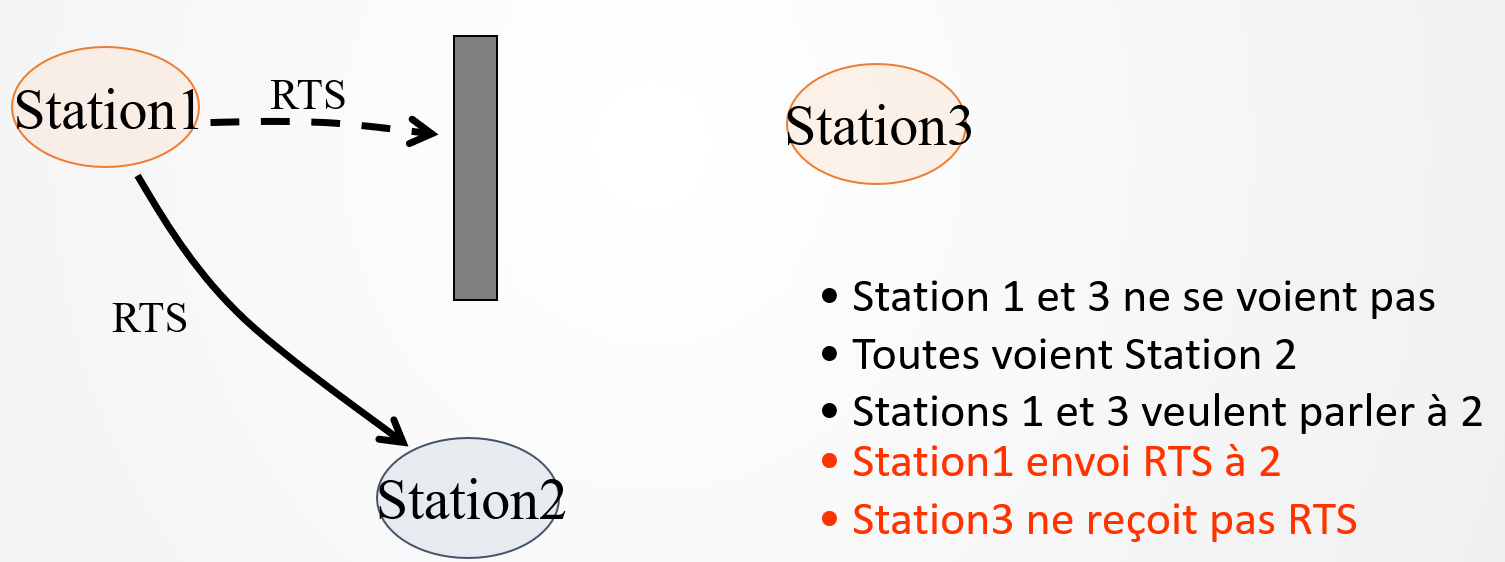
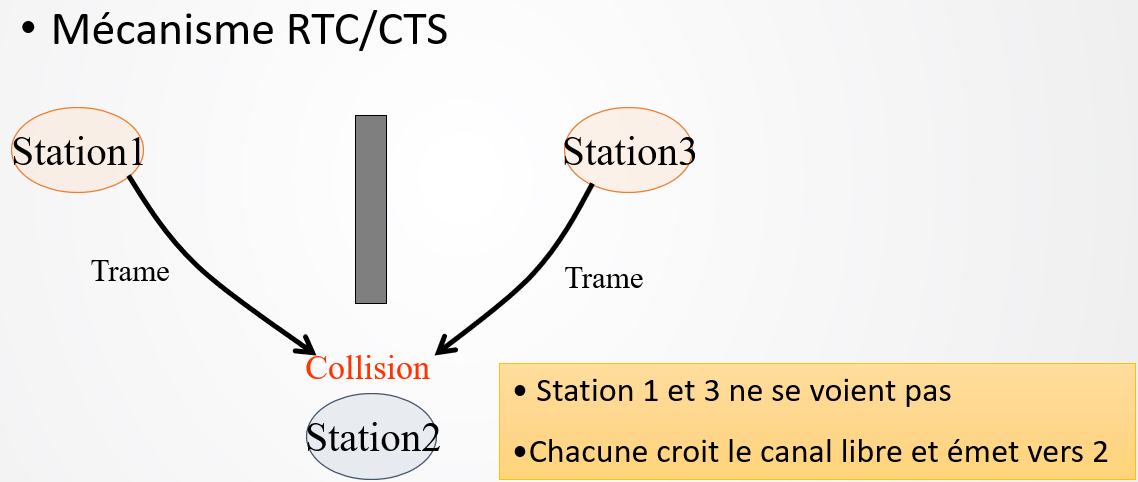
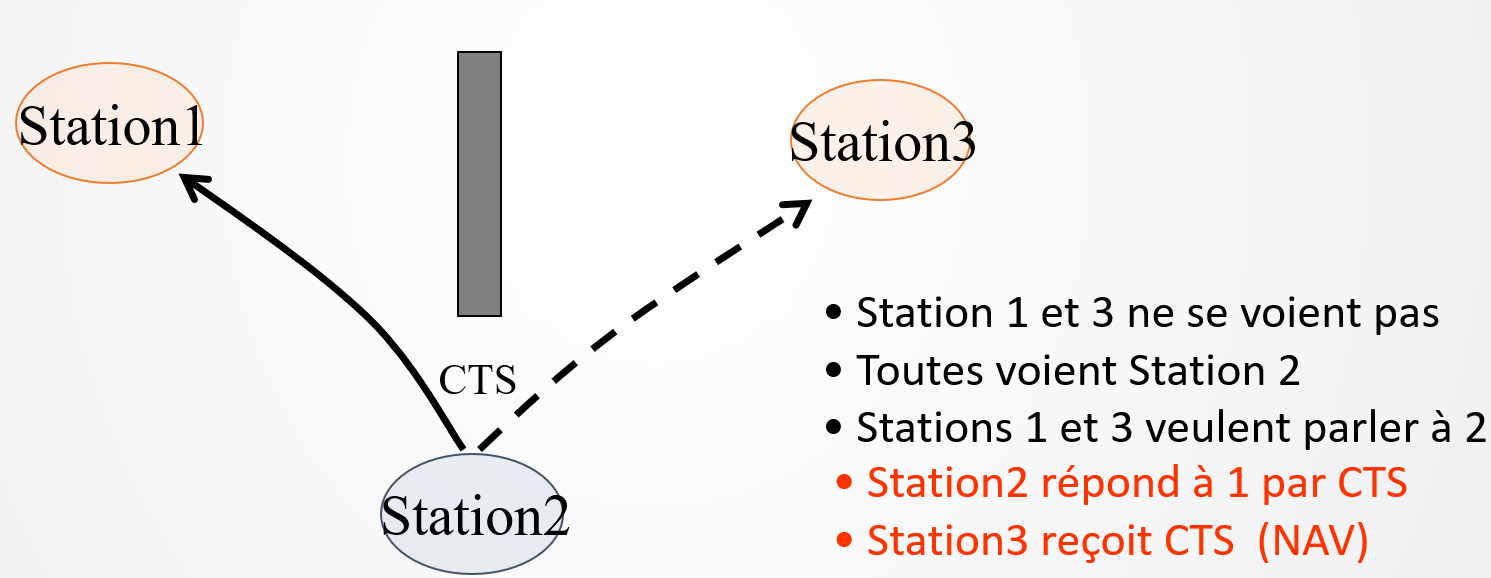
☺ Elle est mieux adaptée à un trafic déséquilibré entre les postes.

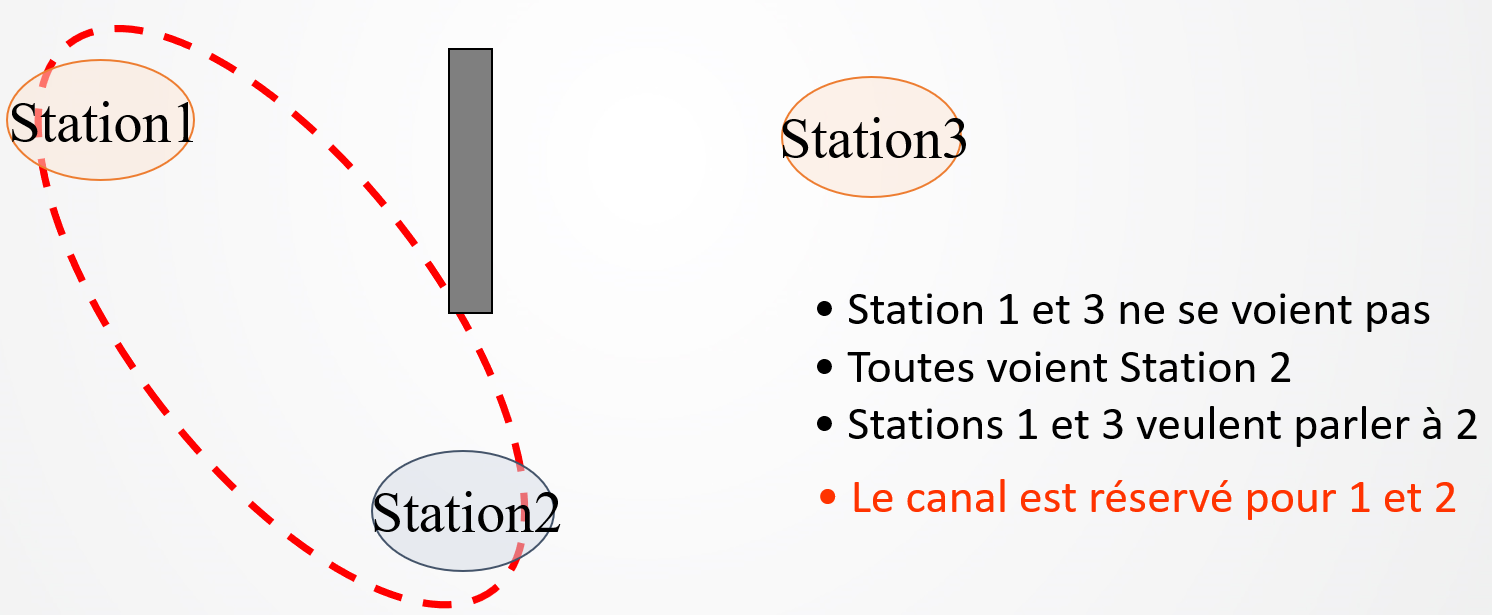
☹ Elle est moins efficace pour les trafics temps réel.

* Permet de résoudre le problème de la station cachée avec le mécanisme RTS/CTS
* **Principe CSMA/CA:**
  + le protocole couplé à une **« fiabilité »**
  + Le principe de base sont:
    - Écoute du canal
    - Attente pour un canal libre
    - La transmission différée après un **DIFS + backoff**, si le canal est occupé et pendant un **DIFS uniquement** si le canal est libre
    - Transmission data
    - En cas de collision: Aucun acquittement n’est reçu.



* Mécanisme RTC/CTS



* + Virtual Carrier Sense: VCS
    1. Le VCS consiste à « **réserver**» le support avant émission.
  + Avant de transmettre, si le support est libre:
    1. L’émetteur émet une trame RTS (@src, @dest, durée transaction = paquet)
    2. Si le support est libre, le récepteur émet un CTS
  + Toute station entendant le RTS ou le CTS déclenche son **NAV** (***Network Allocation Vector***) et se tait pendant toute la durée de la communication.
  + **!!** La probabilité de collision par une station cachée de l’émetteur est limitée à la courte durée du RTS.
  + **!!** Si données courtes, pas de RTS ni CTS.

Trame IEEE802.11

* + Il existe trois types de trame:
* Trame de contrôle
* Trame de données
* Trame de gestion

CHAPITRE 5 : COUCHE RESEAU

* Elle traite de tout ce qui concerne l‘adressage et le routage dans le réseau
  1. **Adressage** : identification des différents réseaux à interconnecter.
  2. **Routage** : découverte d'un chemin de transmission entre récepteur et émetteur, chemin qui passe par une série de machines ou de routeurs qui transmettent l'information de proche en proche (je ne vois pas la destination finale juste le prochain équipement).

**La couche réseau dans OSI est la couche internet dans TCP/IP**

Utilise principalement le protocole IP (Internet Protocol) avec ses deux versions IPv4 et IPv6

**Caractéristiques du protocole IP**

1/ sans cnx :

J’envoie le message et je quitte sans établir une cnx entre l’émetteur et le destinataire ou même connaitre s’il existe.

2/ service au mieux (best effort) :

Protocole rapide mais la probabilité qu’un paquet perd son chemin existe.

Puisque s’il va garder la fiabilité il va perdre du temps et c’est un protocole rapide.

3/ indépendant du media :

Le media : le support.

On ne peut pas deviner des le départ quel est le support utiliser pour transférer le paquet (qq soit Lan, Ethernet cuivre, fibre optique…)

Le paquet s’adapte aux types du media grâce a la fragmentation.

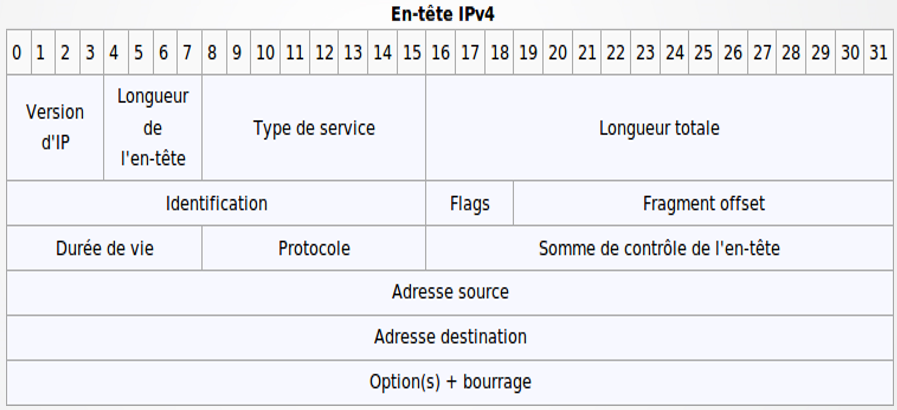
LA FRAGMENTATION :

* Le protocole IP permet au paquet de s’adapter aux diff support grâce a la fragmentation qui consiste à découper un datagramme ( la trame reçu de la couche transport en lui ajouter son entête) en plusieurs paquets **ET** de reconstituer ces paquets à la machine destinatrice.

Chaque datagramme réserve 20 octets pour l’entête de la taille maximale du datagramme

Aussi dans chaque MTU on doit enlever 20 octets réservé s a l’entête

On appelle paquet lorsqu’il quitte la couche réseau et le datagramme découpé en plusieurs paquets

*  longueur de l'en-tête en mots de 32 bits, généralement égal à 5 (pas d'option)

L’entête IP composée de 5 lignes (extensibles) chaque ligne est de taille 4 octets

2eme ligne : identification, indicateur (0, DF, MF), décalage du fragment (l’ordre).

3eme ligne : durée de vie(TTL), protocole,

4eme ligne : @ source

5eme ligne : @ dest

Composition d’@ IP

🡺Net ID : identifie le réseau

A,B,C

Nbre d’@ possibles : 3\*8=24 -> (2^24)-2.

Diff : netID,255,255,255

Reseau : netID,0,0,0

Masque : net=255, host=0,0,0

🡺Host ID : identifie la machine connectée

🡺🡺🡺 ROUTAGE 🡸🡸🡸

Sélectionner le chemin a suivre par un paquet.

L’interface du machine connectee au seg du reseau lan : @ de passerelle par defaut qui doit contenir le net id du reseau

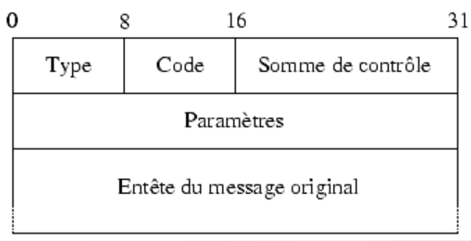
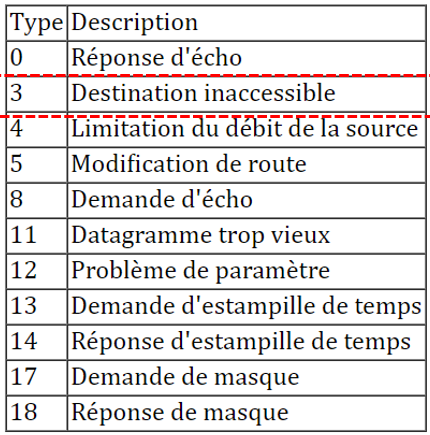
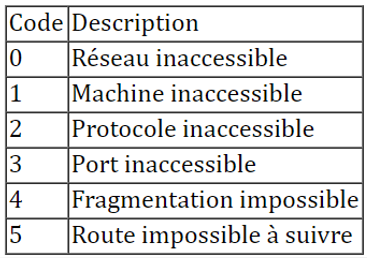
Protocole ICMP :

Informer les stations de l’état de résultat est ce que le paquet est reçu ou détruit.

L IP utilise le ICMP pour envoyer les msgs d’erreur, de supervision

ICMP utilise IP pour transporter ces messages

* + messages d’erreur, renvoyés à l’hôte source qui a émis le paquet IP en erreur.
  + messages de supervision: ICMP signale les conditions d’erreur, sans rendre IP plus fiable



Parmi les messages ICMP qui peuvent être envoyés, citons :

* Host confirmation (Confirmation de l’hôte) : envoyer un echo request. S’il est bien recu la machine dest va envoyer un echo replay pour dire qu’elle disponible
* Unreachable Destination / Service (Destination / service inaccessible) : msg permet de signaler a un hote ou machine que le service est inaccessible (w waqt’ha nshouf tableau de code bsh taarf prob bedhabt wyn)
* Time exceeded (Délai dépassé) : lorque une machine recoit un paquet avec un TTL=0 c.a.d il va le detruire. Le ICMP envoi a la mchine émettrice que le message est detuit faute de TTL.
* Route redirection (Redirection de la route) : informer l’emettrice que le paquet change de chemin.
* Source Quench (Épuisement de la source) : a l’etat de saturation c.s.d pas d’espace

ARP(@ resolution protocol)/RARP protocole

Pour envoyer un msg a un hôte, il nous faut les les @mac et @IP src et dest

Alors pour connaitre @mac du dest, la src envoie une requête ARP et tts les machines du rex vont recevoir la requete puisqu’elle ne contienne pas l’@ dest et cherche qui a l’@ IP demandee puis l’ARP va créer un table ARP