



Cours 4 : le réseau local (lien)

- 4.1 Service de lien
- 4.2 Détection et correction d'erreurs
- 4.3 Protocoles à accès multiple
- 4.4 Adressage dans un réseau à diffusion
- 4.5 Ethernet
- 4.6 Sans fil

1



4.1 Service de lien

- Entre deux nœuds du réseau : les trames (paquets/datagrammes/trames)
- Mis en œuvre dans un coupleur, généralement matériel, avec ses propres processeurs (ex. Carte PMCIA)
- Offre des services comparables au transport de bout en bout (contrôle des erreurs, du flux, ...)

2

4.2 Détection et correction d'erreurs

- Au niveau bit : changement de valeur possible sur le canal physique (pas de perte car synchro à ce niveau là)
- EDC ("Error Detection and Correction") bits
- $(D + EDC) \rightarrow (D' + EDC')$: la probabilité d'erreurs non détectées n'est pas nulle : dépend de la technique utilisée et de l'overhead admissible
- Parité / Checksum / Codes cycliques

3

Parité

101011	101011
111100	101100
011101	011101
001010	001010

- EDC = 1 bit
- Nb 1 dans D+EDC pair
- Si le récepteur en compte un nombre impair, il sait qu'il y a eu au moins 1 bit erroné
- Si le nombre d'erreurs est pair, aucune erreur n'est détectée : la question est la probabilité de plusieurs erreurs dans une même trame -> problème des phénomènes de rafales
- Généralisation à 2 dimensions -> parité ligne et parité colonne -> permet de corriger 1 erreur bit (le bit qui provoque une erreur de parité à la fois sur la ligne et la colonne) et de détecter 2 erreurs bit

4

Checksum

- Internet (UDP/TCP) : les données sont traitées comme une suite d'entiers sur 16 bits et sont additionnés. Le complément à 1 de la somme forme le checksum transmis dans la trame
- Le récepteur calcule la somme des entiers reçus. Si un 0 apparaît, une erreur est détectée

```
0110011001100110
0101010101010101
1011101110111011
0000111100001111
1100101011001010
```

```
0110011001100110
0101010101010101
0000111100001111
0011010100110101
1111111111111111
```

5

"Cyclic Redondancy Check" (CRC)

- Les suites de bits sont vues comme les coefficients d'un polynôme. Les données sont transmises avec un code dépendant d'un générateur G de $r+1$ bits, $R = \text{reste de } (D \times 2^r / G)$
- On transmet $(D \times 2^r) \text{ xor } R$
- Le récepteur divise la donnée reçue par G . Si le reste est différent de 0, une erreur est détectée
- Détecte des rafales d'erreurs de moins de $r+1$ bits. Au delà la probabilité de détection est $1 - 0.5^r$

• IEEE $G =$
100000100110000010001110110110111

$D = 101110$ $G = 1001$

```
101110000 | 1001
  1010      | 101011
    1100
     1010
      011
```

6



4.3 Protocoles à accès multiple

- Canal de diffusion partagé : cable Ethernet, radio sans-fil (Wifi), satellite, ...
- Collisions : les signaux des trames se mélangent, rendant les trames inaudibles pour les différents récepteurs -> toutes les trames en collision sont perdues...
- Coordination nécessaire entre les émetteurs -> rôle du protocole d'accès :
 - Protocoles de partitionnement du canal,
 - Protocoles à accès aléatoire,
 - Protocoles tournants

7



Protocoles à partitionnement

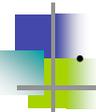
- Trois méthodes :
 - Division temporelle ("Time Division Multiplexing" TDM) : le train de bits est divisé en parts ("slots") allouées statiquement pour chaque récepteur : 123412341234. L'émetteur attend son slot. Typiquement la taille du slot permet de loger un paquet
 - > sans collision et équitable, mais débit R/N même si un seul émetteur + attente
 - Division fréquentielle ("Frequency Division Multiplexing" FDM) : la bande de fréquence est divisée en N -> fournit N sous-canaux de débit R/N : mêmes avantages et inconvénients que la technique TDM

8



- Division par code
("Code Division Multiple Acces" CDMA)

- Chaque bit émis est codé avec un mot c de longueur M
- En représentant le bit 0 par -1 , le bit de donnée d_i est transformé en la suite de bits $Z_{i,m}$ pour m de 1 à M :
$$Z_{i,m} = d_i \times c_m$$
- Le récepteur retrouve le bit de donnée par l'opération :
$$d_i = 1/M \sum_{m=1,M} Z_{i,m} \times c_m$$
- Exemple : $C = 111-11-1-1-1$
 $-1\ 1 \rightarrow -1-1-11-1111\ 111-11-1-1-1 \rightarrow -1\ 1$



- Traitement des interférences : N émetteurs

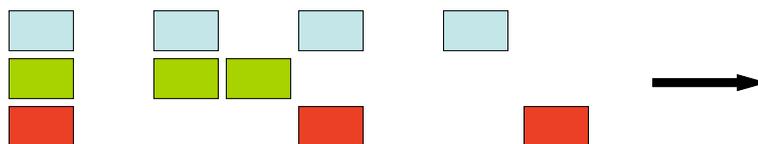
- Les valeurs de chaque émetteur s'ajoutent sur un mini-slot : $Z_{i,m}^* = \sum_{s=1,N} Z_{i,m}^s$
- Astucieusement, on peut démêler par la même formule que précédemment les valeurs à la réception si les mots de code de chaque émetteur sont bien choisis :
$$d_i = 1/M \sum_{m=1,M} Z_{i,m}^* \times c_m$$
- Outre le choix des codes, il y a aussi des difficultés pratiques dans la régulation de puissance électrique sur le canal
- Exemple : $c1 = 111-11-1-1-1$, $c2 = 1-1111-111$
 $-1\ 1 // 1\ 1 \rightarrow 0-2020022\ 20202-200 \rightarrow -1\ 1$ (récepteur 1)

Accès aléatoire

- Transmission au débit max, mais retransmission en cas de collision avec une attente aléatoire (indépendante pour chaque émetteur) -> des centaines de protocoles (Aloha/CSMA/Ethernet ...)
- Exemple le plus simple : "Slotted ALOHA"
 - Trames de L bits, débit du canal R
 - Le temps est divisé en slots de taille L/R secondes
 - Les nœuds ne transmettent qu'en début de trame. Ils sont synchronisés et connaissent donc tous le même début de trame
 - Tous les nœuds détectent une collision avant la fin du slot
 - En cas de collision, la trame est retransmise dans des slots prochains avec une probabilité p

11

Slotted ALOHA



- Performances : à charge max, N émetteurs
- Probabilité de succès pour un nœud arbitraire : $Np(1-p)^{N-1}$
- Choix du meilleur p pour N arbitrairement grand : $p = 1/e$ (0.37)
- 37% seulement du débit canal est utilisé !

12

Pure ALOHA

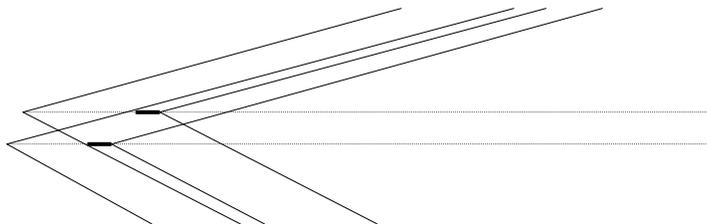
- Pas de synchronisation : l'émission n'attend pas le prochain slot libre (complètement décentralisé)
- Probabilité de succès pour un nœud arbitraire : $Np(1-p)^{2(N-1)}$, optimisé pour $p = 1/(2e)$ la moitié du cas "slotted"

13

CSMA

"Carrier Sense Multiple Access"

- Règles de politesse : "écouter avant de parler, arrêter de parler si quelqu'un d'autre prend la parole"
- Les collisions sont dues au délai de propagation
- CSMA/CD



Temps de détection et d'arrêt

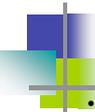
14



Protocoles tournants

- "polling" : existence d'un nœud maître qui donne la parole à tour de rôle -> délais de notification et vulnérabilité
- Passage d'un jeton de parole : vulnérabilité du jeton

15



4.4 Adressage dans un réseau à diffusion

- Il s'agit de re-construire une liaison bi-point entre nœuds connectés à un canal en diffusion
- Un coupleur possède une adresse physique (typiquement 6 octets). C'est une adresse "en dur" (ROM) unique (assuré par le constructeur qui achète des bits d'adresse, par exemple 24 fixés par l'IEEE et 24 au gré de la compagnie)
- Par opposition à l'adresse IP qui est hiérarchique et peut changer lorsque la machine se déplace
- L'adresse physique du destinataire sur le même réseau local est passée dans le message et filtrée par le destinataire. A noter aussi l'adresse de diffusion : FF-FF-FF-FF-FF-FF

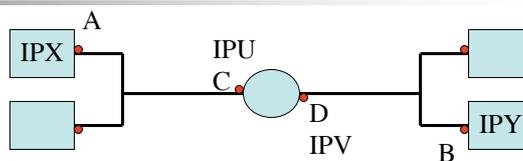
16

Protocole de résolution d'adresse (ARP)

- Le module ARP sur chaque nœud donne la correspondance adresse IP / adresse physique du coupleur
- Se trouve l'équivalent d'un DNS limité au réseau local
- Une entrée dans l'annuaire a une durée de vie limitée (typiquement 20 minutes)
- Lorsqu'une entrée n'est pas présente, le protocole de résolution est déclenché :
 - Diffusion d'une "requête ARP" sur le réseau avec les adresses IP et physique de l'émetteur et l'adresse IP du destinataire
 - Les récepteurs comparent leur adresse IP à celle du destinataire. Le nœud sélectionné renvoie à l'émetteur une "réponse ARP" avec son adresse physique. Ce qui permet à l'émetteur de mettre à jour son annuaire
- ARP est "plug-and-play" (s'adapte tout seul à un changement de l'environnement)

17

La traversée d'un routeur



- Déclenchement de l'ARP à chaque arrivée dans un nouveau réseau local
 - > ARP Request (IPX,A,IPU,FF) /* IPU routage pour IPY */
 - <- ARP Reply (IPU,C,IPX,A)
 - > Message IP (IPX,A,IPU,C,IPY)
 - > ARP Request (IPV,D,IPY,FF) /* IPV routage pour IPY */
 - <- ARP Reply (IPY,B,IPV,D)
 - > Message IP (IPV,D,IPY,B)

18

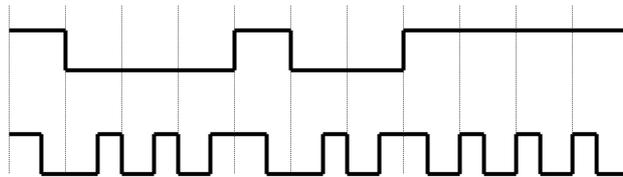
4.5 Ethernet

- Les datagrammes IP sont encapsulés dans les trames Ethernet
- Format de la trame :
Préambule / adresse dest / adresse source / type / données / CRC
 - **Données** : de 46 à 1500 octets : au delà, il faut fragmenter; en deçà il faut bourrer
 - **Adresses** : 6 octets. Le récepteur jette les trames qui ne lui sont pas destinées
 - **Type** : 2 octets. Utilisé pour multiplexer les protocoles de niveau réseau (IP/NovellIPX/AppleTalk)
 - **CRC** : 4 octets. Les trames erronées sont simplement jetées
 - **Préambule** : 8 octets = 10101010101010 ... 10101011 : sert à resynchroniser les horloges des coupleurs (dérive). Le drapeau 11 final sert à avertir que les bits suivants seront une adresse physique. La fin de la trame est simplement détectée par une absence de courant

19

Transmission en "bande de base"

- Transmission directe sur le canal sans changement de fréquence (contrairement à l'ADSL)
- Codage Manchester pour garder la synchronisation des horloges : chaque bit contient une transition en son milieu (1 → 10; 0 → 01)



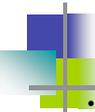
20



Ethernet CSMA/CD

- Attendre l'absence de courant + 96 bits pour transmettre
- Si détecte la présence d'un autre transmetteur, il arrête sa transmission et insère un signal d'encombrement de 48 bits. Puis il attend avant de réessayer une transmission : tire une valeur aléatoire K entre 0 et $2^{\min(n,10)}-1$ pour la n^{ième} collision et attend $K \times 512$ bits (attente exponentielle)
- Le signal d'encombrement est pour faire en sorte qu'un émetteur émette suffisamment de bits avant de s'arrêter pour cause de collision : ce qui risque de ne pas montrer suffisamment d'énergie pour la détection de collision chez les autres
- La norme Ethernet donne une limite de distance entre nœuds pour que l'algorithme d'attente exponentielle fonctionne
- Efficacité dans l'utilisation de la bande passante : $1/(1 + 5P/T)$ avec P : temps de propagation, T temps de transmission

21



Technologies

- 10Base2 (10Mbps, 200m). Cable coaxial fin linéaire sur lequel sont fixées les machines (30 max car les connexions provoquent aussi des atténuations du signal). Les cables peuvent être enchaînés à l'aide de "répéteurs" (5 segments max)
- 10BaseT et 100BaseT : "fast Ethernet". Topologie en étoile (concentrateur ou "hub"). Le concentrateur assure la diffusion en recopiant le bit en entrée sur toutes les sorties. 100BaseT utilise des paires torsadées. Le codage Manchester est remplacé par le codage 4B5B (4 bits sur 5 périodes)
- Gigabit Ethernet et 10Gbps Ethernet : même principe que BaseT. Existe aussi la notion de switch pour les communications point-a-point

22

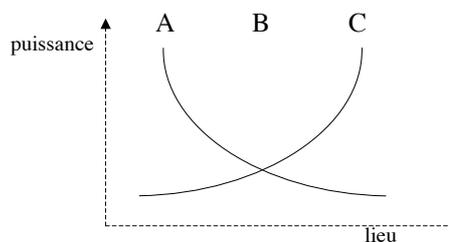
4.6 Sans fil

- IEEE 802.11 : les éléments de base d'une architecture réseau sont les cellules ("Basic Service Set"). Une cellule contient plusieurs stations sans fil et une station de base
- Une cellule peut aussi se former spontanément par proximité d'un ensemble de stations. Il n'y a pas alors de station de base spécifique -> réseaux ad-hoc
- "Media Access Control" : protocole MAC fondé sur la technique CSMA/CA (CA pour "Control Avoidance"). Le canal partagé est un canal radio (fréquence). L'écoute consiste à mesurer l'énergie sur la fréquence choisie. Si le canal est libre pendant un temps DIFS ("Distributed Inter Frame Space"), la station est autorisée à émettre. Après réception complète, le récepteur attend un temps SIFS ("Short Inter Frame Spacing") et renvoie un accusé -> il n'y a pas de détection de collision pendant la transmission comme dans Ethernet

23

Problème de la station cachée

- Une obstruction physique (montagne) entre les stations A et C peut faire qu'elles soient en interférence pour une communication avec B, mais sans s'en apercevoir : la collision n'est pas détectable
- Une autre raison peut être l'atténuation ("fading"). L'interférence en B n'est pas détectée par A ni C



24

- 
- Les trames contiennent un champ de durée de transmission pour que les autres récepteurs puissent calculer un temps minimum d'attente
 - Il y a aussi des messages courts d'allocation du canal ("Request To Send" RTS et "Clear To Send" CTS) : RTS contient la durée de transmission données+ack+SIFS. CTS est la réponse d'autorisation. Les autres entendent le RTS et CTS et s'abstiennent donc d'émettre
 - Autres facilités : synchronisation des horloges, gestion de la puissance, gestion de l'insertion et du retrait des stations...

25

Bluetooth

- 
- 2.45 Ghz dans la bande radio sans licence
 - 721 kbps ou 3 canaux voie à 64 kbps
 - 10 à 100m de portée
 - Toute une pile de protocoles en fait :
 - Protocole bande de base -> notion de réseau Bluetooth "piconet"
 - Protocole de gestion des liens (orienté connexion)
 - Protocole L2CAP : adaptation pour les niveaux supérieurs

26