

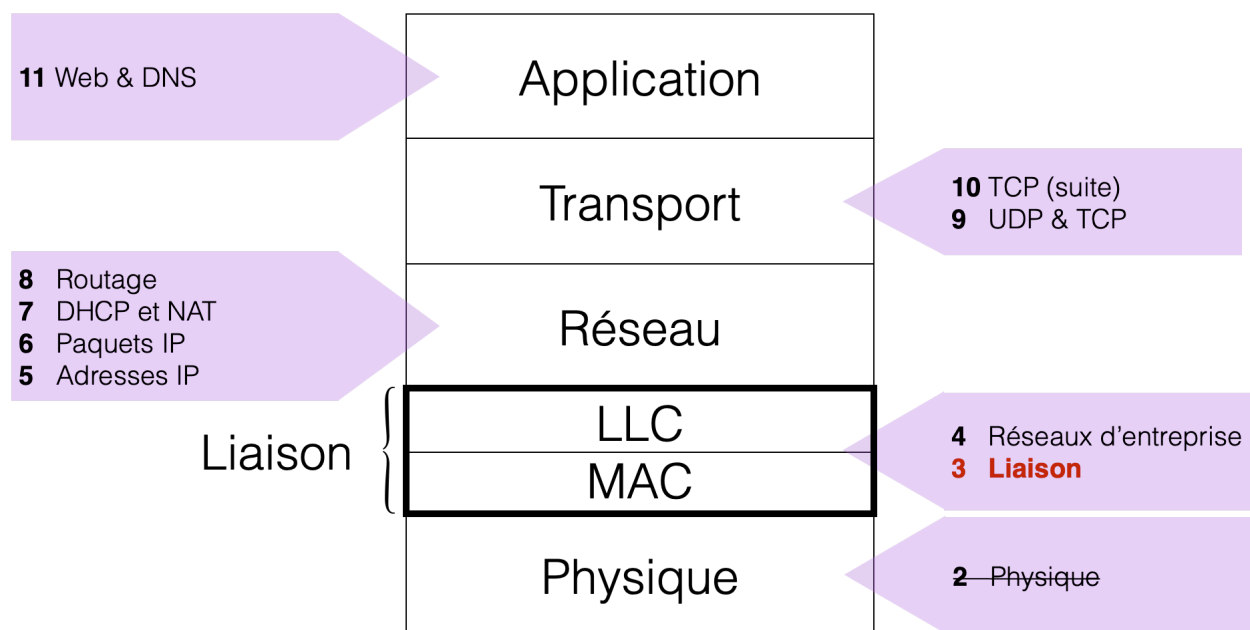
Couche Liaison de Données & Réseaux Locaux

UE LU3IN033 Réseaux
2020-2021

Prométhée Spathis
promethee.spathis@sorbonne-universite.fr



Programme de l'UE LU3IN033



Plan du cours

- Support de transmission
 - point-à-point
 - partagé (à diffusion naturelle) : bus, anneau, étoile
- Topologie
 - physique
 - logique
- Contrôle d'accès
 - accès statique
 - accès dynamique
- Normes IEEE 802
 - 802.3 et Ethernet
 - 802.11 et Wifi
- Contrôle d'erreur
 - Codes de parité : VRC et LRC
 - Codes polynomiaux : CRC

3



Méthode de contrôle d'accès

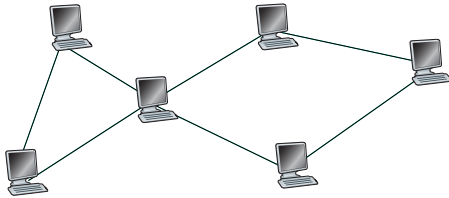
UE LU3IN033 Réseaux
2020-2021

Prométhée Spathis
promethee.spathis@sorbonne-universite.fr



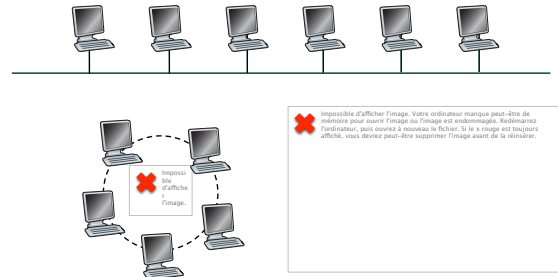
Types de réseaux

Réseaux point à point



- Chaque lien connecte :
 - deux stations
 - ces stations peuvent être des routeurs
 - elles exécutent un protocole liaison de données en mode point à point :
 - HDLC, PPP
- Topologie adaptée aux réseaux longue distance

Réseaux à diffusion naturelle



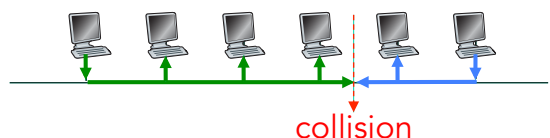
- Plusieurs stations partagent un même support de transmission
 - une trame est reçue par toutes les stations connectées au support
- Nécessitent des méthodes de contrôle d'accès au support
- Topologie adaptée aux réseaux locaux
 - Exemple : Ethernet, WiFi



7

Méthodes de contrôle d'accès

- Support de transmission partagé
 - Plusieurs stations sont connectées au même support
 - Les transmissions sont reçues par l'ensemble des stations
 - Une copie suffit à une trame pour être reçue de tous
 - Des transmissions simultanées entraînent des collisions
 - Les collisions brouillent les communications et les rendent inintelligibles



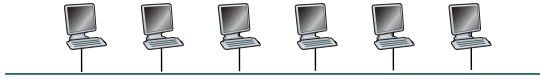
- Méthodes de contrôle d'accès
 - Algorithmes distribués pour partager le support
 - Ces algorithmes déterminent quelle station peut transmettre à un instant donné
 - Contrôler l'accès revient à partager la bande passante parmi toutes les stations (équité)

8

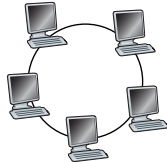


Topologies physiques courantes des réseaux locaux

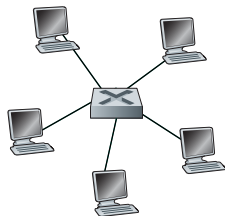
- Bus



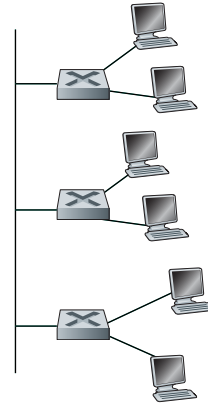
- Anneau



- Etoile



- Arbre



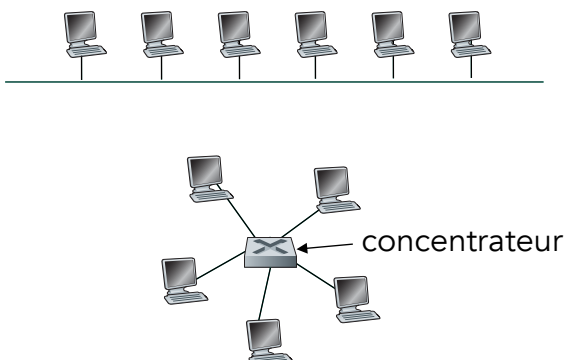
Les méthodes de contrôle d'accès sont conçues en tenant compte de la topologie logique !



9

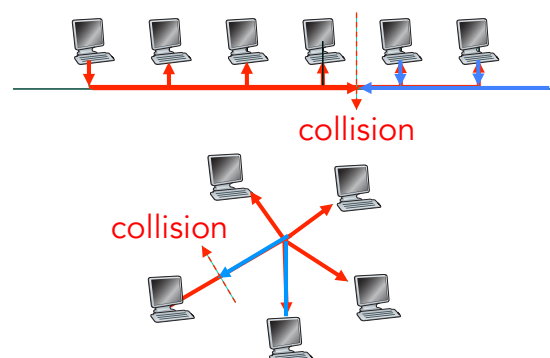
Topologie physique vs logique

Topologie physique



- La topologie physique décrit l'agencement des nœuds du réseau et les liens les reliant entre eux
 - Position des nœuds
 - Distance entre les nœuds
 - Connectivité

Topologie logique



- La topologie logique décrit les nœuds et liens qu'emprunte une trame
- Exemple : étoile vs bus
 - Si le concentrateur diffuse les données sur toutes ces interfaces :
 - La topologie logique d'une étoile est identique à celle d'un bus



10

Méthodes de contrôle d'accès

- Les méthodes de contrôle d'accès
 - Algorithmes distribués qui déterminent la (les) station(s) qui peut (peuvent) transmettre à un instant donné
 - Partage de la bande passante parmi toutes les stations du réseau
 - temps passé à transmettre vs temps passé à attendre son tour
 - problème d'équité
 - Elles prennent en compte la topologie logique (et non physique)
- Classification des méthodes de contrôle d'accès
 - accès statique
 - la bande passante est répartie de façon invariante dans le temps
 - accès dynamique
 - la bande passante est allouée à la demande

13



Classification des méthodes de contrôle d'accès

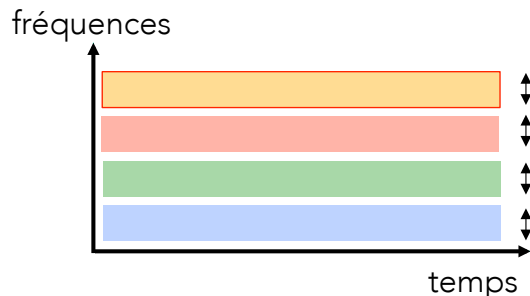
- Accès statique
 - accès multiple à répartition en fréquence
 - accès multiple à répartition dans le temps
- Accès dynamique
 - méthodes d'accès dynamique à allocation déterministe
 - le polling
 - le jeton
 - non adressé
 - adressé
 - méthodes d'accès dynamique à allocation aléatoire
 - Aloha
 - Carrier Sense Multiple Access
 - persistant, non-persistant, p-persistant
 - collision detection : 802.3 Ethernet
 - collision avoidance : 802.11 Wifi

14

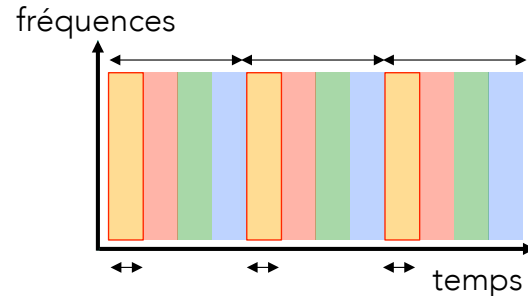


Méthodes d'accès statique

répartition en fréquence



répartition dans le temps



- La bande passante est divisée en sous-bande
 - une sous-bande allouée par station
 - toutes les stations peuvent transmettre simultanément
- Méthode peu efficace si stations inactives
- Redécoupage de la BP si ajout ou retrait de stations
- Le temps est divisé en intervalles de temps (time slots)
 - les stations émettent à tour de rôle dans le même ordre
- Méthode peu efficace si stations inactives
- Redécoupage du temps si ajout ou retrait de stations

15



Méthodes d'accès statique vs dynamique

- Les méthodes d'accès statique sont adaptées si :
 - le nombre de stations actives est :
 - réduit
 - fixe
 - connu à l'avance
 - les trafics sont prévisibles et à débits constants
- Les méthodes d'accès statique ne sont pas adaptées si :
 - le nombre de stations actives varie dans le temps
 - les stations génèrent un trafic sporadique
 - c'est le cas des réseaux informatiques (de données)
- Nécessité de méthodes qui permettent l'allocation dynamique de la bande passante
 - allocation en fonction des demandes immédiates



Méthodes d'accès dynamique

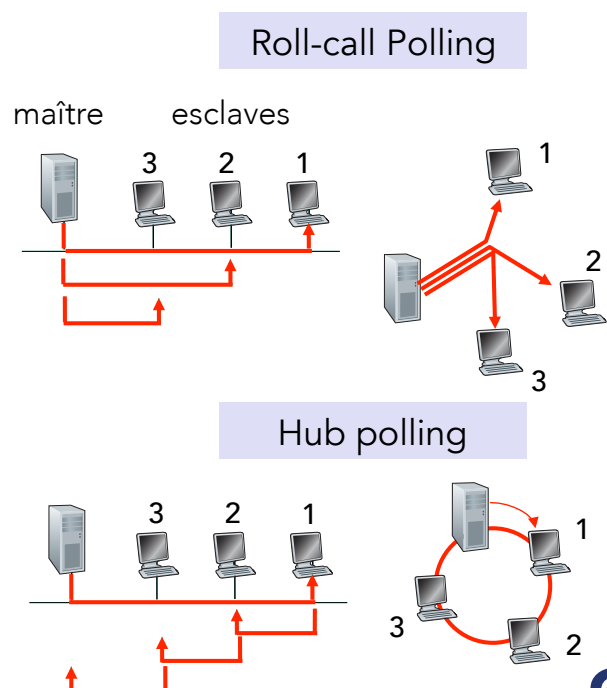
- Méthodes d'accès dynamique à allocation déterministe
 - le polling
 - non adressé
 - adressé
 - le jeton
- Méthodes d'accès dynamique à allocation aléatoire
 - Aloha
 - Carrier Sense Multiple Access

17

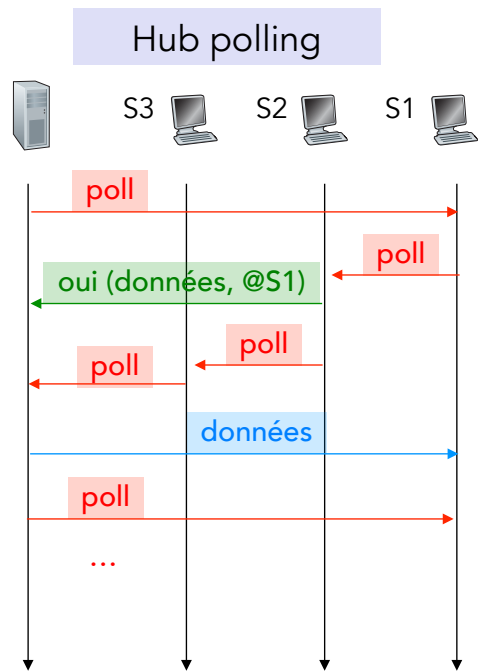
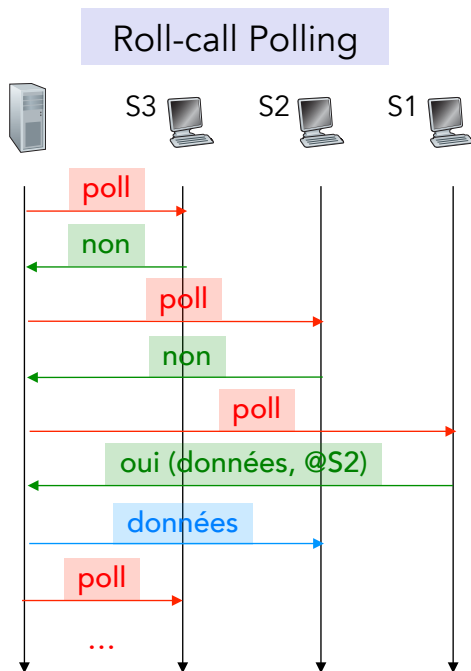


Le polling (1)

- Polling
 - Méthode centralisée :
 - Station primaire : maître
 - Stations secondaires : esclaves
 - Le maître interroge (poll) les esclaves à tour de rôle
 - Les esclaves répondent :
 - positivement avec les données à transmettre le cas échéant
 - négativement sinon
- Deux variantes du polling selon l'ordre du polling
 - Roll-call polling (Bluetooth)
 - topologie logique : étoile
 - Hub polling
 - topologie logique : anneau



Le polling (2)



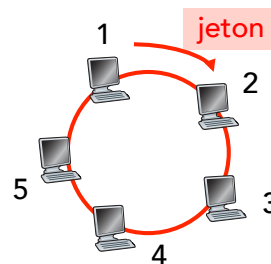
19



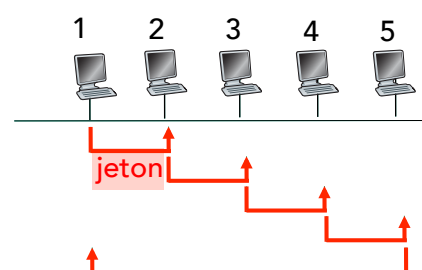
Le jeton

- Méthode distribuée
 - Pas de station maître (primaire)
- Le jeton est une trame spéciale
 - une seule copie sur le réseau
 - deux états possibles :
 - libre
 - occupé
- Topologies logiques concernées :
 - Anneau : jeton non adressé
 - sens de circulation naturel
 - Bus : jeton adressé
 - chaque station connaît
 - son prédécesseur
 - son successeur
 - le jeton est passé de successeur en successeur

Jeton non adressé

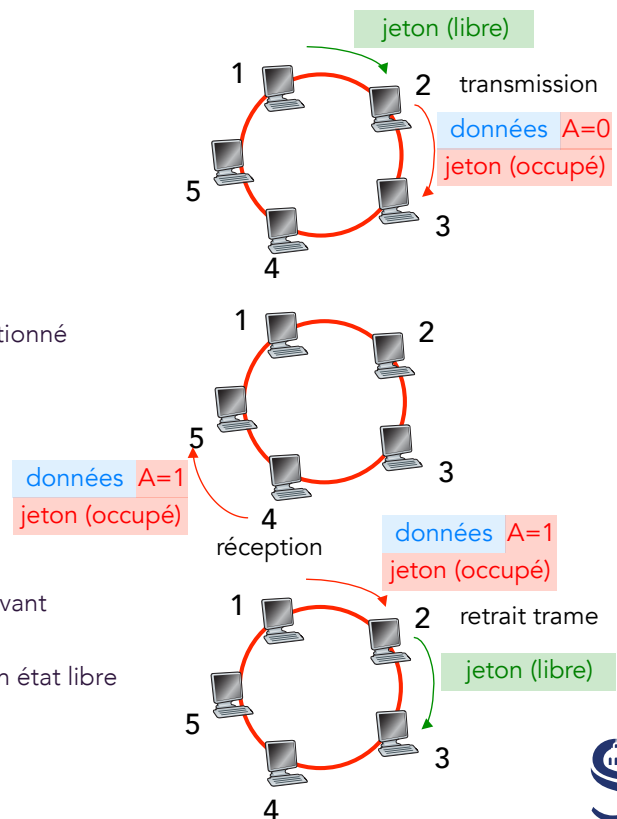


Jeton adressé

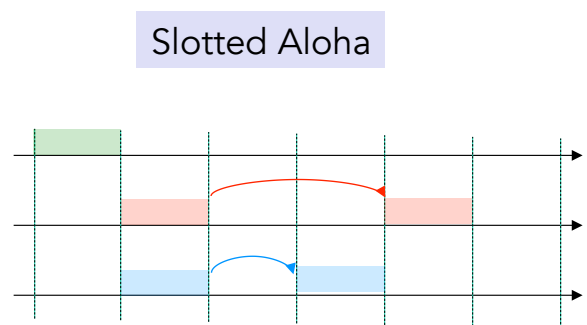
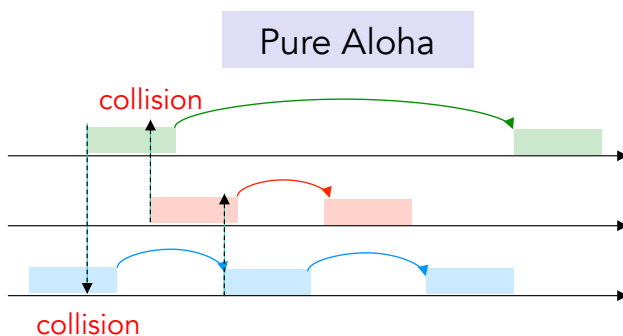


Le jeton non adressé

- Une station qui désire transmettre
 - attend de recevoir le jeton à l'état libre
 - change l'état du jeton à l'état occupé
 - accole le jeton à sa trame de données
 - les trames de données contiennent :
 - l'adresse de la source
 - l'adresse de la destination
 - un bit d'acquittement initialement non positionné
- Les stations inspectent :
 - l'état du jeton
 - si occupé :
 - si l'adresse destination est la sienne :
 - » elle prélève une copie de la trame
 - » elle change le bit d'acquittement
 - » passe la trame initiale au voisin suivant
 - si l'adresse source est la sienne :
 - » elle retire la trame et libère le jeton état libre
 - si libre :
 - elle transmet si elle le désire



Méthodes d'accès dynamique à allocation aléatoire (1)



- une station émet dès lors qu'elle le souhaite
- en cas de collision, la station réémettra sa trame au terme d'un délai **aléatoire**
- au bout de N collisions successives, la station abandonne

- Efficacité : 18%
 - rapport = nombre de transmissions en succès / nombre total de transmissions

- le temps est découpé en intervalles temps
 - durée de transmission d'une trame
- les stations ne peuvent émettre qu'en début d'intervalle

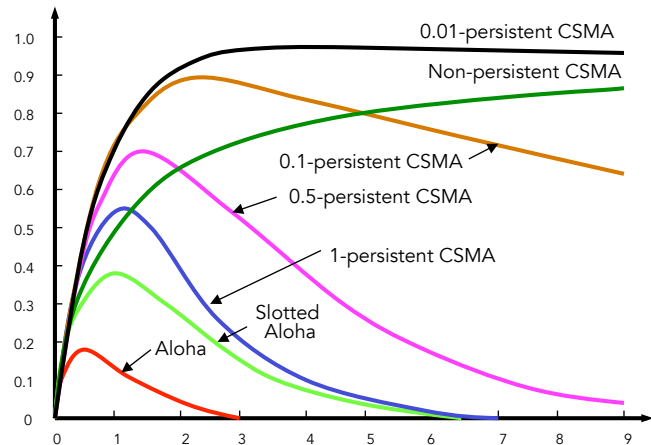
- Efficacité : 36%



Méthodes d'accès dynamique à allocation aléatoire (2)

Carrier Sense Multiple Access

- CSMA reprend le Pure Aloha
 - avec une "écoute" du canal avant d'émettre : la station n'émet que si le canal est libre
- Plusieurs variantes selon la décision prise par la station émettrice si le canal occupé :
 - CSMA persistant
 - écoute persistante du canal
 - dès qu'il devient libre, émettre
 - CSMA non persistant
 - faire une nouvelle tentative au bout d'un temps aléatoire
 - CSMA p-persistant
 - écoute persistante du canal
 - dès qu'il devient libre,
 - avec une probabilité p , émettre
 - avec une probabilité $(1-p)$, attendre un délai et aller en 1



23

Méthodes d'accès dynamique à allocation aléatoire (3)

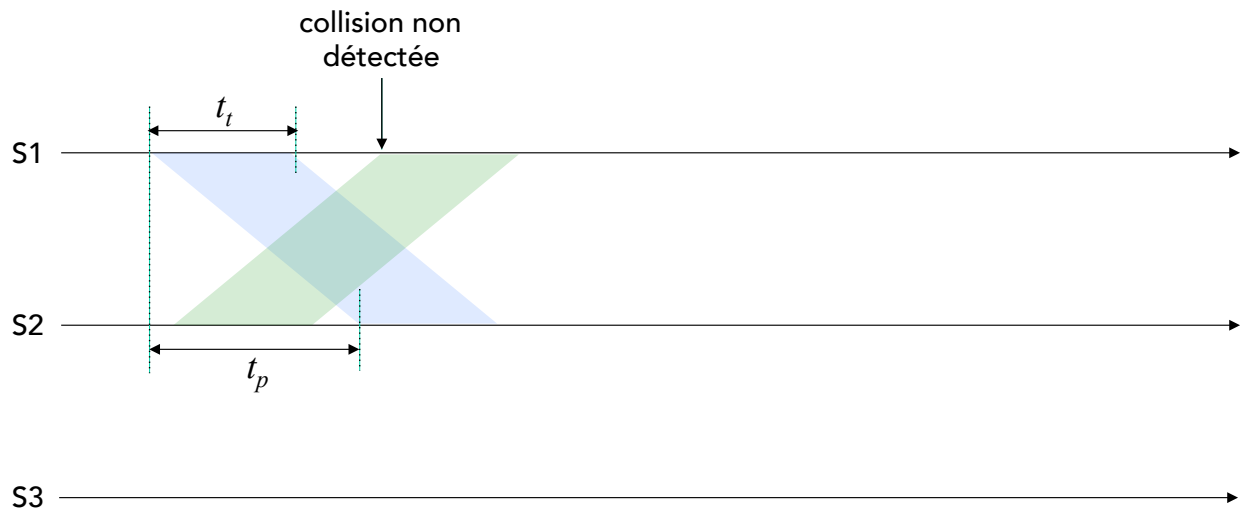
Carrier Sense Multiple Access / Collision Detection

- CSMA/CD est
 - la méthode utilisée par Ethernet
 - standardisée par la norme IEEE 802.3
- CSMA/CD reprend les principes du CSMA
 - une station qui émet, continue à écouter le canal pendant sa transmission
 - elle détecte les collisions en comparant le signal émis à celui qu'elle reçoit
 - utilisation d'un transceiver : transmitter-receiver
 - en cas de collision, chaque station impliquée déroule un algorithme de reprise
 - utilisation de temps d'attente aléatoire pour réduire les risques de nouvelles collisions



24

Détection des collisions

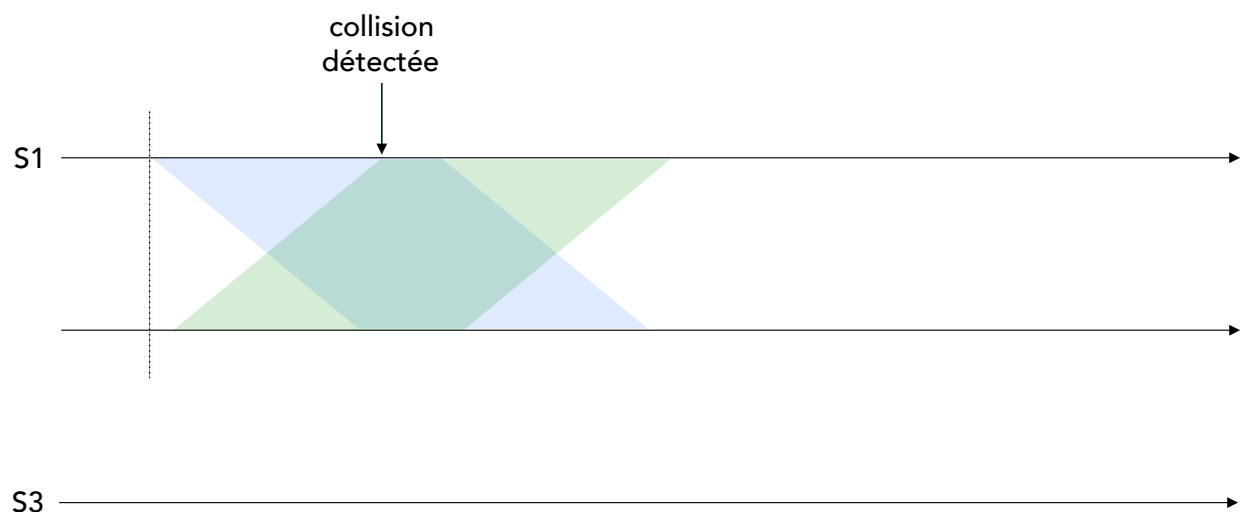


- Une collision est détectée en comparant le signal émis et le signal reçu
 - S1 et S2 terminent leur transmission avant de recevoir le signal brouillé
 - Collision non détectée

25



Détection des collisions

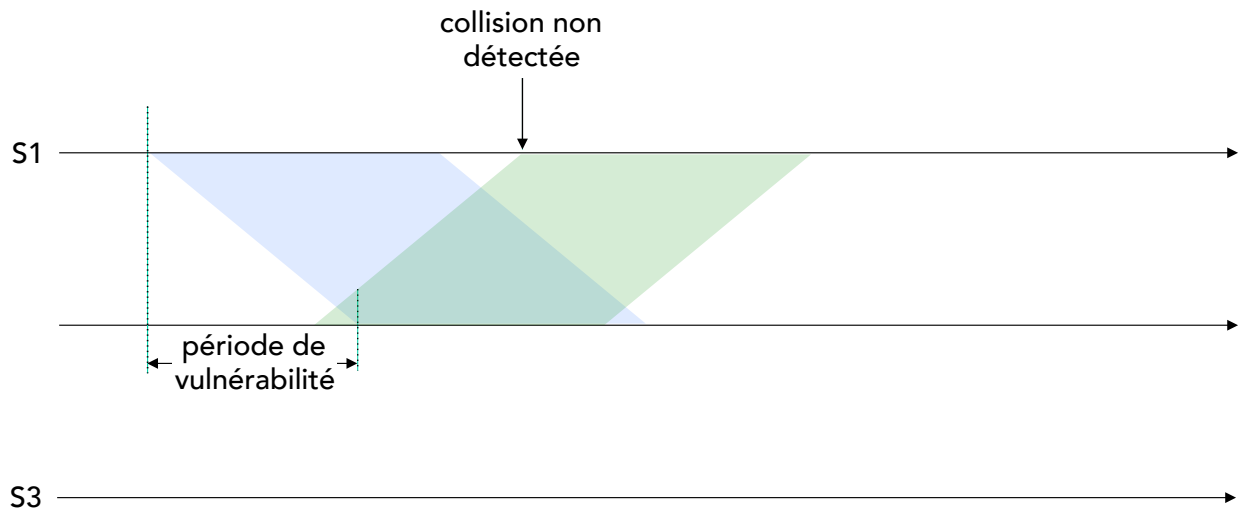


- Une collision est détectée en comparant le signal émis et le signal reçu
 - S1 et S2 doivent transmettre suffisamment longtemps pour recevoir le signal brouillé en cas de collision

26



Détection des collisions

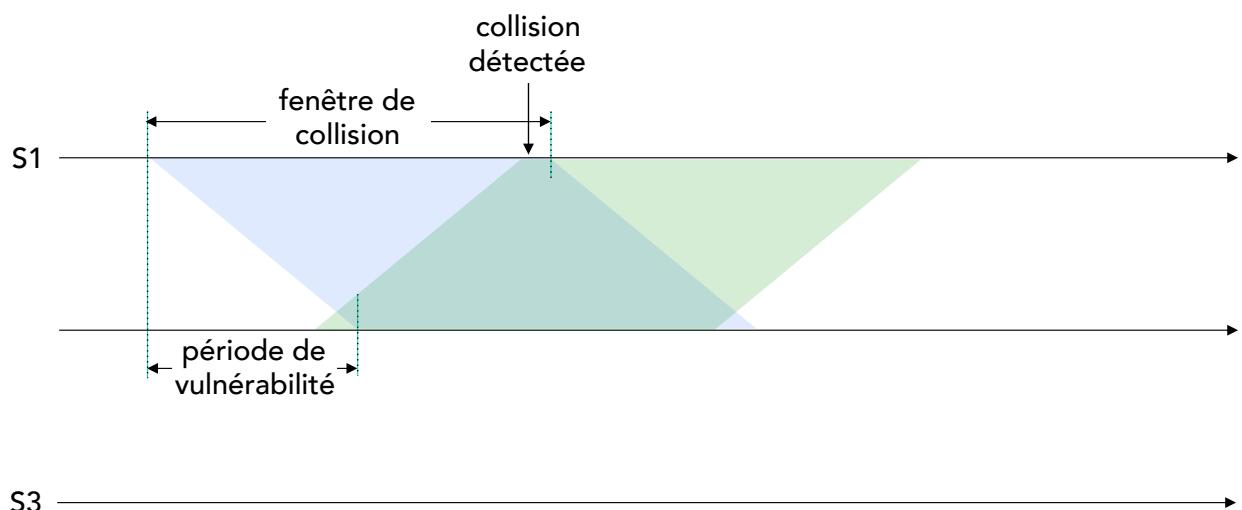


- Une collision est détectée en comparant le signal émis et le signal reçu
 - S1 et S2 doivent transmettre suffisamment longtemps pour recevoir le signal brouillé en cas de collision
 - Quelle est la durée min de transmission idéale ?

27



Détection des collisions

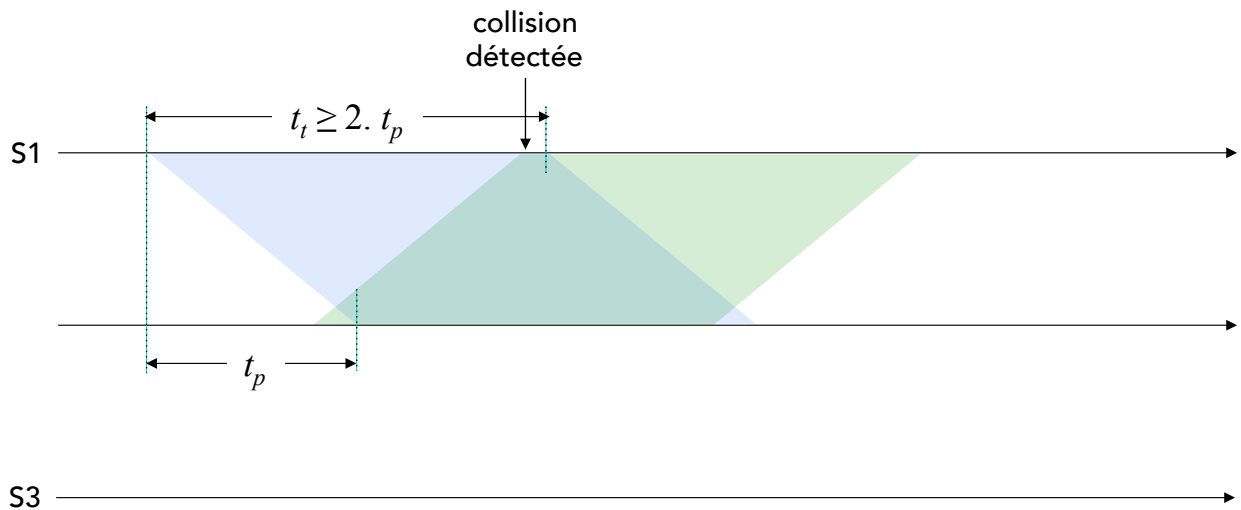


- Période de vulnérabilité (t_p)
 - Durée qui s'écoule après le début d'une transmission et durant laquelle une autre transmission entraînera une collision
 - Échec des deux transmissions

28



Détection des collisions

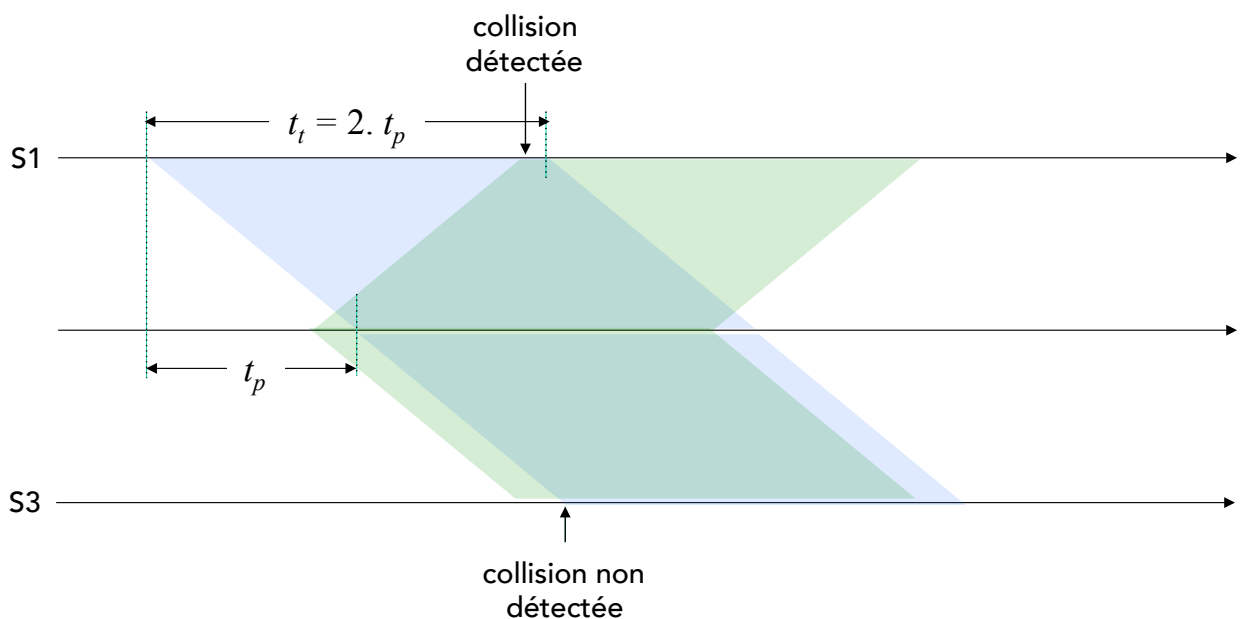


- Fenêtre de collision ($t_t \geq 2 \cdot t_p$)
 - Durée qui s'écoule entre le début d'une transmission et l'instant au delà duquel une transmission sera en succès

29



Détection des collisions

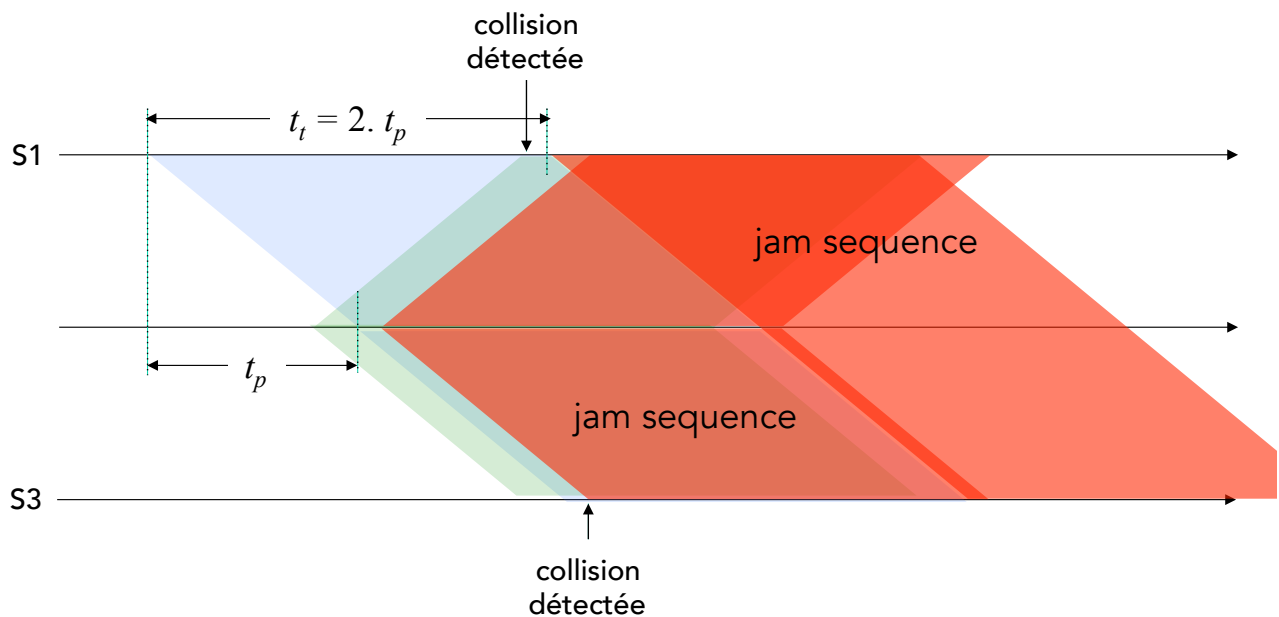


- Une collision est détectée en comparant le signal émis et le signal reçu
 - S3 ne transmet pas et ne peut donc interpréter le signal reçu comme résultant d'une collision

30



Détection des collisions



- Jam sequence
 - Signal émis afin d'informer toutes les stations (y compris celles qui n'étaient pas en transmission) d'une collision

31



CSMA/CD : définitions

- Période de vulnérabilité
 - intervalle de temps pendant lequel une station éloignée peut détecter (à tort) le canal libre et transmettre
 - égale au maximum au temps de propagation entre les 2 stations les plus éloignées sur le support
- Fenêtre de collision (time-slot)
 - délai maximum qui s'écoule avant qu'une station en cours de transmission détecte une collision
 - délai au bout duquel une station est certaine d'avoir réussi sa transmission
 - égale à deux fois le temps de propagation d'un signal sur le support
- Séquence de brouillage (jam sequence)
 - séquence de brouillage envoyée par une station dès qu'elle détecte une collision, afin d'en informer toutes les stations du réseau
- Délai inter-trame (interframe gap)
 - silence minimum entre 2 trames successives
 - permet à toutes les autres stations de transmettre à leur tour
 - partage équitable de la bande passante

32



CSMA/CD : procédures

1. Transmission d'une trame pour la première fois :
 - le support est occupée
 - attendre qu'il le devienne
 - le support est libre
 - commencer à transmettre en continuant à écouter le support
 - si collision détectée : procédure de résolution de collision (2)
 - pas de collision : remettre à 0 le compteur de retransmissions et terminer la transmission
2. Résolution de collision :
 - transmission d'un signal de brouillage (jam signal)
 - incrémenter le compteur de retransmission
 - si le nombre maximal de retransmission est atteint
 - abandon de la transmission
 - sinon
 - calculer la durée du retrait aléatoire en fonction du nombre de collisions
 - attendre pour cette durée avant d'aller à la procédure de transmission (1)

33



Retrait exponentiel

- Algorithme de calcul du délai aléatoire d'attente
 - détermine D , l'instant de retransmission d'une trame qui a subi une ou plusieurs collisions
- Calcul de l'intervalle dans lequel la valeur de D est tirée aléatoirement
 - l'intervalle croît avec n le nombre de collisions subies
 - des collisions successives indiquent que le réseau est chargée
 - éviter de mettre de l'huile sur le feu
- Lorsque n atteint 16, il y a abandon de la transmission

```
Backoff (D);  
n : nombre total de  
collisions déjà subies par  
la trame  
k = min(n, 10)  
tirage d'une variable  
aléatoire M telle que  
0 ≤ M < 2k  
D = M * time-slot  
return (D)
```

34



Normalisation IEEE des LAN

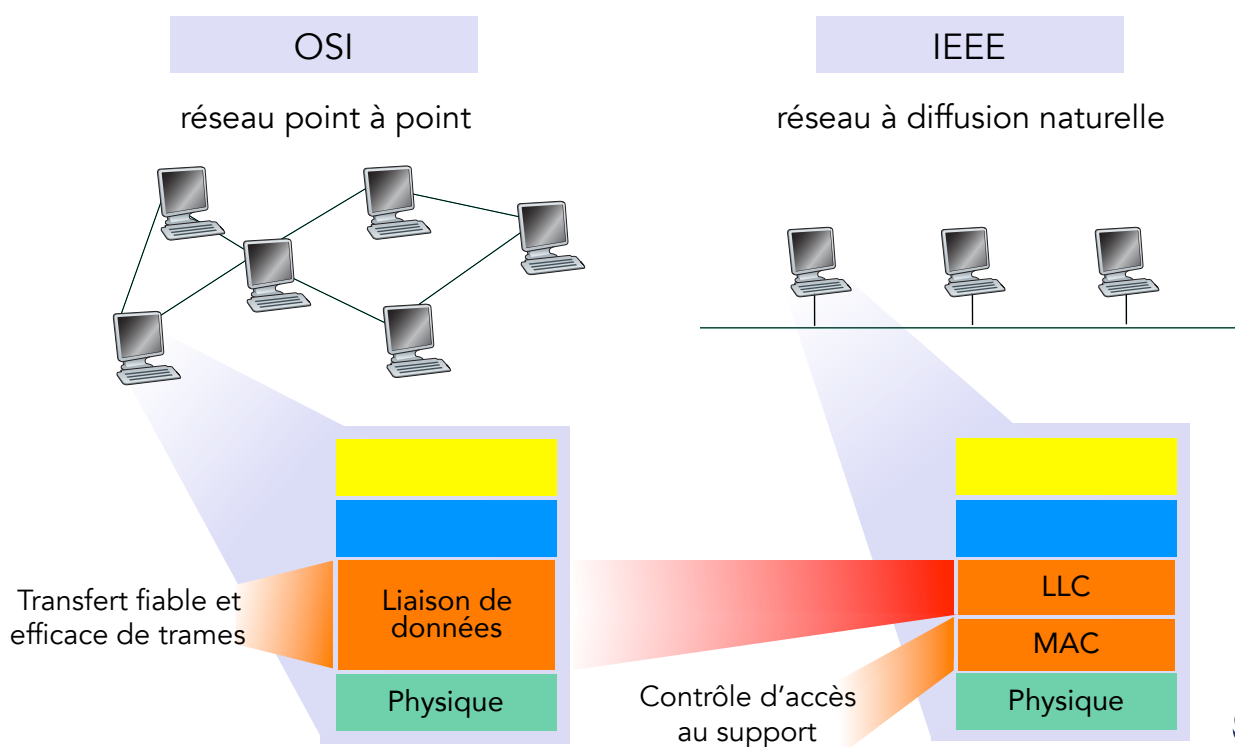
Définition IEEE d'un LAN

« A datacomm system allowing a number of **independent devices** to communicate **directly** with each other, within a **moderately sized** geographic area over a physical communications channel of **moderate data rates** »

35



OSI vs IEEE

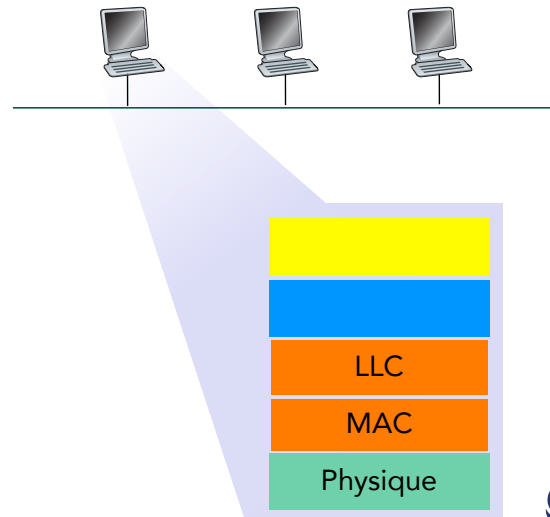


36



La couche liaison de données selon l'IEEE

- 2 sous-couches
 - LLC Logical link control
 - MAC Medium access control
- Logical Link Control
 - fournit la plupart des fonctions de la couche liaison de données
 - contrôles d'erreur et de flux
- Medium Access Control
 - définit la méthode de contrôle d'accès au support
 - évite les collisions
 - partage équitablement la BP



37



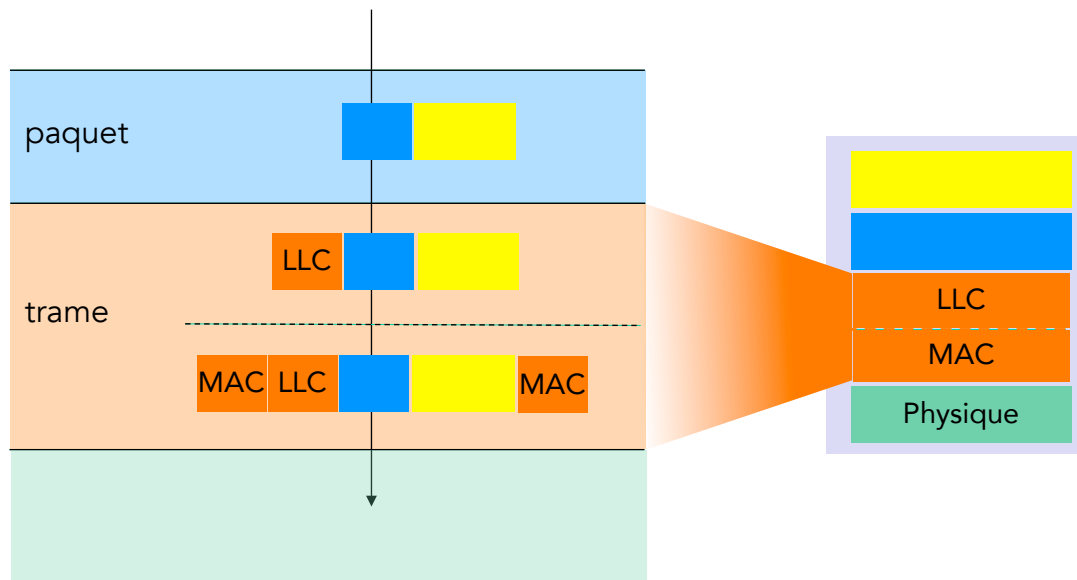
Les normes IEEE 802.*

Réseau										
LLC	802.2 LLC									
MAC	802.3 CSMA/CD			802.11 CSMA/CA (Wifi)			802.5 Token Ring		...	
PHY	802.3 (10Base5)	802.3a (10Base2)	802.3b (10BROAD36)	⋮	802.11 (DSSS/FHSS)	802.3b (HR-DSSS)	802.3g (ERP-OFDM)	⋮	⋮	

39



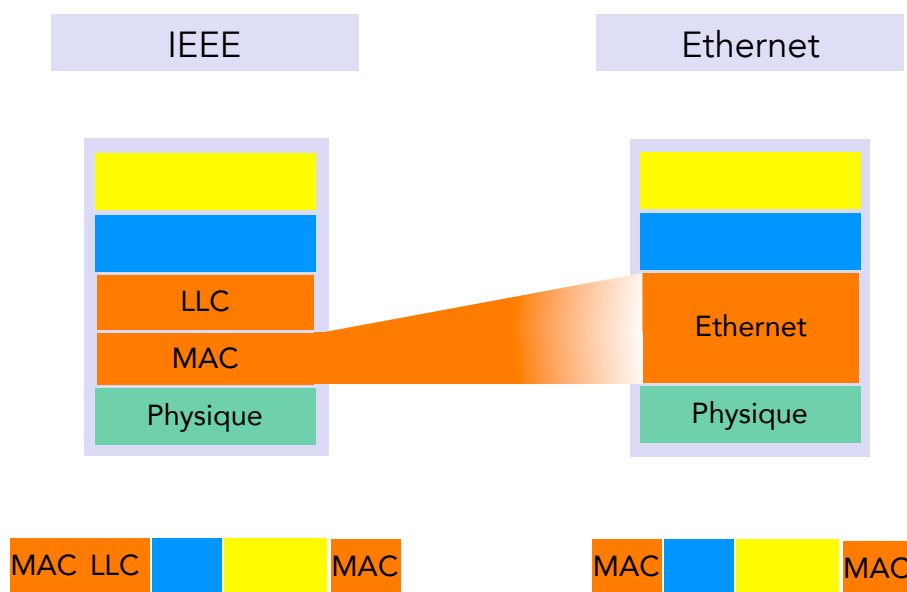
Encapsulation IEEE



40



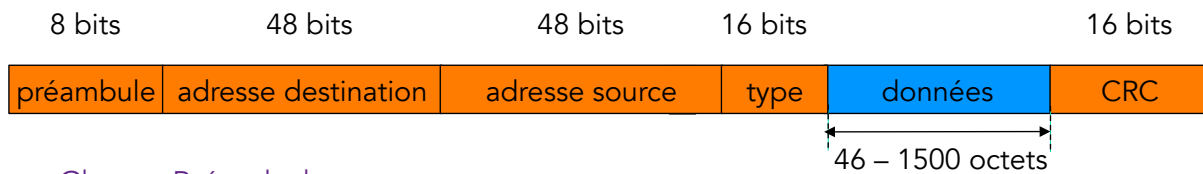
802.3 vs Ethernet



41



Trame Ethernet

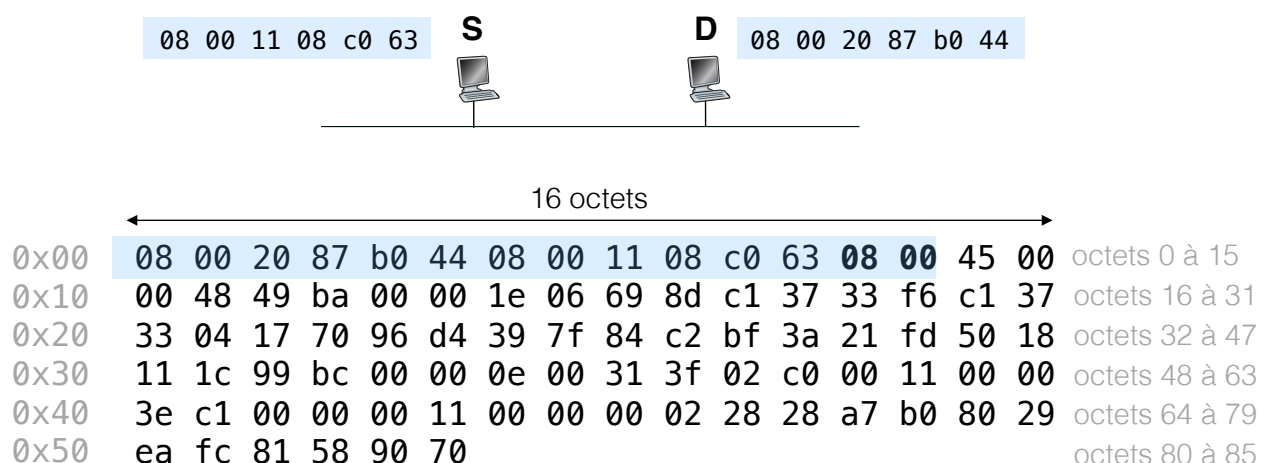


- Champ Préambule
- Champs Adresse source et destination
 - adresse MAC codée sur 48 bits (6 octets)
 - notation hexadécimale : **F0:18:98**:59:AE:32
 - les 3 premiers octets indiquent quel est le constructeur (F0:18:98 : Apple)
- Champ Type
 - paquet IPv4 : 0x0800, message ARP : 0x0806, ...
- Champ Données
 - la taille des données est comprise entre 46 et 1500 octets
 - utilisation de bits de bourrage pour compléter les données si nécessaire
- Champ CRC (Cyclic redundancy check)
 - Code générateur :

$$X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + X + 1$$



Exemple de trace

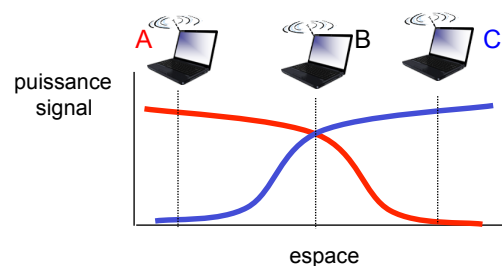


- Trame Ethernet donnée sans préambule ni CRC
- Adresse MAC destination : 08:00:20:87:B0:44
- Adresse MAC source : 08:00:11:08:C0:63
- Type : 0x0800 → entête encapsulé suivante : paquet IP



IEEE 802.11 Wireless LANs (Wi-Fi)

- 802.11 : CSMA/CA
 - CSMA : écoute du support
 - CA: évitement de collisions
- Ecouter le support :
 - pour ne pas empiéter sur une transmission en cours
- Eviter les collisions :
 - la détection des collisions est difficile voir impossible en sans fil :
 - affaiblissement du signal (fading)
 - problème du terminal caché



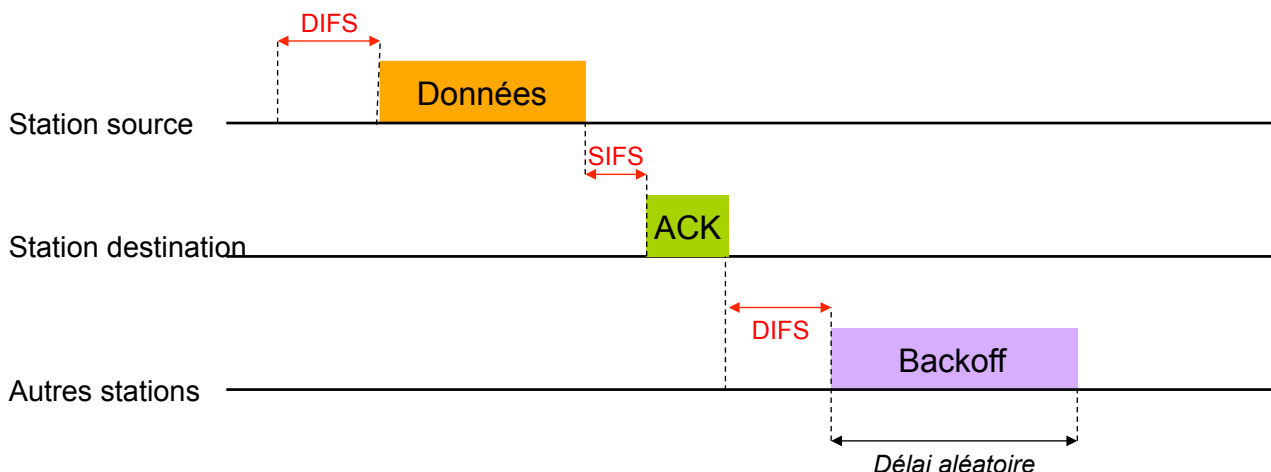
- utilisation des ACK
 - détection et retransmissions des trames en collision

44



Temporisateurs et priorités

- SIFS (Short Inter Frame Spacing) 10
 - La plus haute priorité : ACK
- DIFS (DCF, Distributed Coordination Function IFS)
 - La plus basse priorité : données



45



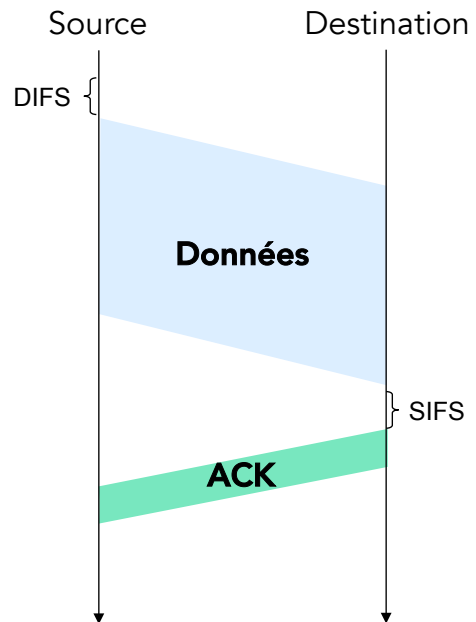
CSMA/CA

- Source 802.11

1. Si le support est libre :
 - attendre DIFS
 - envoyer la trame
 2. Si le support est ou devient occupé:
 - attendre que le support soit libre
 - démarrer un temporisateur (random backoff timer)
 - décrémenter le temporisateur uniquement lorsque le support est libre (mis en pause sinon)
 - transmettre à expiration du temporisateur
- Si pas d'ACK,
 - augmenter l'intervalle de tirage des valeurs du temporisateur

- Récepteur 802.11

- Si la trame est reçue sans erreur :
 - attendre in SIFS
 - envoyer un ACK



46



Algorithme de backoff exponentiel

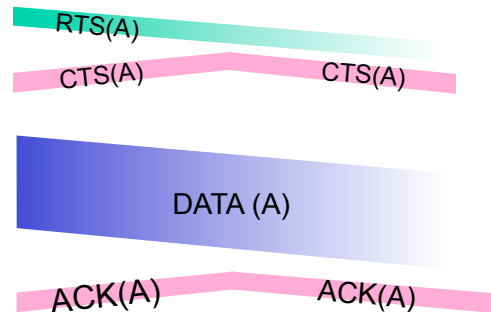
- $DAA = CW * \text{random}(0, CW) * \text{SlotTime}$
 - $\text{random}(0, CW)$ est une variable aléatoire uniforme comprise entre 0 et $CW-1$
 - CW est la taille de la fenêtre de contention,
 - $CW = [CW_{\min}, CW_{\max}]$
- Lors de la première tentative de transmission :
 - $CW = CW_{\min}$
- En cas de collision :
 - CW est doublée jusqu'à ce que CW atteigne CW_{\max} .
- Exemple wifi :
 - $\text{SlotTime} = 20 \mu s$
 - $CW_{\min} = 31$
 - $CW_{\max} = 1023$

47



Trames de réservation RTS/CTS

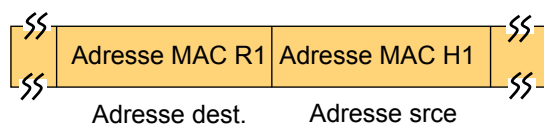
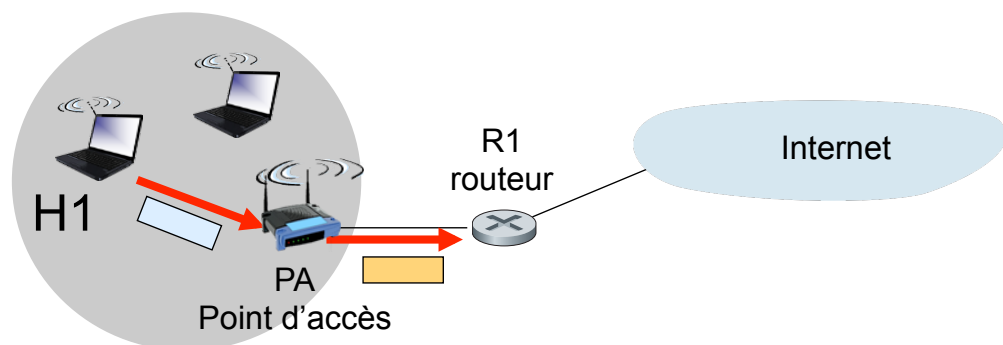
- Une source qui désire émettre des données :
 - envoie un RTS au point d'accès
 - indiquant la durée nécessaire pour transmettre ses données et l'ACK
- Le point d'accès répond :
 - après un SIFS, en broadcastant un CTS
- Après réception du CTS :
 - la source transmet ses données
 - Les autres stations diffèrent leur transmission pour la durée indiquée par le CTS



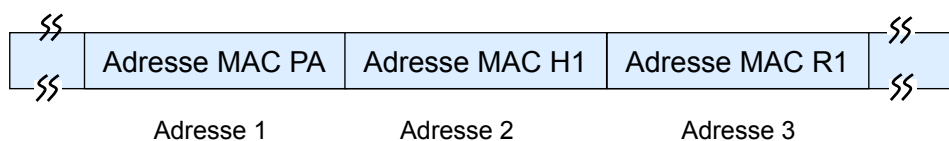
48



Trames 802.11



802.3 frame



802.11 frame



Contrôle d'erreur

UE LU3IN033 Réseaux
2020-2021

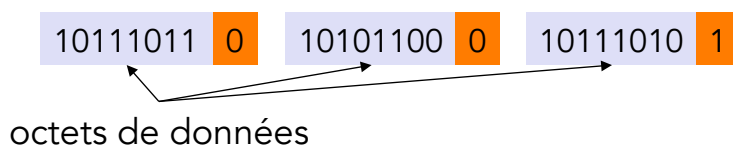
Prométhée Spathis
promethee.spathis@sorbonne-universite.fr



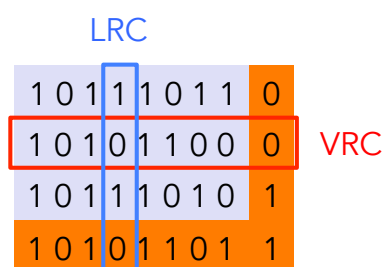
Codes de parité

- Bit de parité
 - parité paire (0) : le nombre de bits à 1 dans le message est pair
 - parité impaire (1) : les nombre de bits à 1 dans le message est impair

- VRC (Vertical redundancy checking)



- LRC (Longitudinal redundancy checking)



Codes Polynomiaux

- CRC (Cyclic redundant code)

- Le message a envoyé est converti en polynôme

$$\begin{array}{cccccccc}
 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\
 x^7 & x^6 & x^5 & x^4 & x^3 & x^2 & x^1 & x^0 \\
 M(X) = x^7 + x^5 + x^4 + x^3 + x + 1
 \end{array}$$

- Emetteur et récepteur se mettent d'accord sur $G(X)$ un polynôme générateur

Exemple : $G(X) = x^4 + x + 1$

- L'émetteur transmet :

$$T(X) = M(X).X^r + R(X) \text{ où } r \text{ est le degré de } G(X)$$

- où $R(X)$ résulte de la division polynomiale de $M(X).X^r$ par $G(X)$

$$M(X).X^r = Q(X).G(X) + R(X)$$

https://en.wikipedia.org/wiki/Cyclic_redundancy_check#Polynomial_representations_of_cyclic_redundancy_checks



$$\begin{array}{r}
 \begin{array}{c} \textcolor{red}{M(X).X^4} \\ \hline \textcolor{red}{11010110110000} \end{array}
 \quad
 \begin{array}{c} \textcolor{blue}{G(X)} \\ \hline \textcolor{blue}{10011} \end{array} \\
 \begin{array}{r}
 \textcolor{red}{11010110110000} \\
 \textcolor{blue}{10011} \downarrow \\
 \textcolor{blue}{010011} \\
 \textcolor{blue}{10011} \downarrow \\
 \textcolor{blue}{00001} \\
 \textcolor{blue}{00000} \downarrow \\
 \textcolor{blue}{00010} \\
 \textcolor{blue}{00000} \downarrow \\
 \textcolor{blue}{00101} \\
 \textcolor{blue}{00000} \downarrow \\
 \textcolor{blue}{01011} \\
 \textcolor{blue}{00000} \downarrow \\
 \textcolor{blue}{10110} \\
 \textcolor{blue}{10011} \downarrow \\
 \textcolor{blue}{01010} \\
 \textcolor{blue}{00000} \downarrow \\
 \textcolor{blue}{10100} \\
 \textcolor{blue}{10011} \downarrow \\
 \textcolor{blue}{01110} \\
 \textcolor{blue}{00000} \downarrow \\
 \textcolor{red}{R(X) = } \textcolor{red}{1110}
 \end{array}
 \end{array}$$



Codes Polynomiaux

- Message à envoyer
10111011
 $M(X) = X^7 + X^5 + X^4 + X^3 + X + 1$
- Code générateur
 $G(X) = X^4 + X + 1$
- Division polynomiale
 $M(X).X^4 = X^{13} + X^{12} + X^{10} + X^8 + X^7 + X^5 + X^4$
 $M(X).X^4 = G(X).(X^9 + X^8 + X^3 + X) + (X^3 + X^2 + X)$
- L'émetteur transmet :
 $T(X) = M(X).X^r + R(X)$
 $T(X) = X^{13} + X^{12} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^3 + X^2 + X$
1101011011110 où 1110 est le CRC
- Le récepteur reçoit $T'(X)$ fait la division polynômiale :
 $T'(X) = G(X).Q'(X) + R'(X)$
- Si $R'(X) = 0$ alors pas d'erreur !

54



Conclusion

- Les réseaux locaux utilisent des supports à diffusion naturelle
 - Toutes les stations sont connectées au même support
 - Une copie suffit pour qu'une trame soit reçue par toutes les stations
- Nécessité de contrôler l'accès au support
 - Pour éviter les collisions (contentions d'accès)
 - Pour partager la bande passante équitablement
- Les politiques d'accès dépendent de la topologie logique
 - Bus : CSMA/CD
 - Anneau : jeton non adressé, ...
- Les normes IEEE 802 ont introduit la sous-couche MAC
 - MAC Medium access control : contrôle d'accès
 - LLC Logical link control : contrôles d'erreur et de flux
- La norme 802.3 standardise le CSMA/CD et le format des trames
 - Ethernet est la version commerciale apparue avant sa normalisation par l'IEEE
- La norme 802.11 standardise le CSMA/CA utilisé par le Wifi

55

