

Chapitre V

Réseaux locaux



But du chapitre

- Connaître la situation des normes LANs dans la hiérarchie OSI (LLC, MAC)
- Connaître les méthodes d'accès aux médias
 - Savoir expliquer en détail le mécanisme CSMA
 - Savoir expliquer en détail le fonctionnement du protocole MAC des réseaux Ethernet
- Connaître les différentes variantes d'Ethernet ainsi que leurs supports physiques et les contraintes respectives
- Connaître les méthodes d'interconnexion de réseaux locaux (ponts)
- Connaître les différentes normes de réseaux locaux sans fil

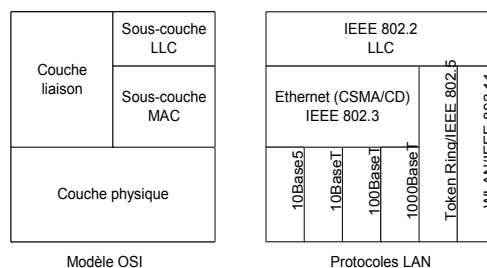
Réseaux locaux (LANs)

- LAN: Local Area Network
 - Réseaux d'entreprise
 - Connectent les stations, PC, imprimantes et serveurs d'une entreprise
 - Taille jusqu'à quelques kilomètres
- Particularités
 - **Multipoint**:
 - Le multicast / broadcast est une fonction essentielle du réseau
 - **Taux d'erreur** bit en ligne très faible ($\sim 10^{-10}$)
 - distance faible entre les stations
 - correction d'erreur non nécessaire
 - **Haut débit**
 - Quelques Mb/s jusqu'à quelques Gb/s

Les protocoles LAN

- Protocoles des **couches liaison** et **physique** spécifiques pour tenir compte des particularités des LANs
 - Définis dans le cadre du projet 802 de l'IEEE
- Division de la couche 2 en deux sous-couches:

- LLC (Logical link control):
 - Fonctions de contrôle indépendantes de la technologie sous-jacente
- MAC (Medium Access Control):
 - Gestion de l'accès au média physique
 - Dépend du médium physique



Projet 802 de l'IEEE

Groupe 802.1 : Protocoles de couches supérieures dans les réseaux locaux

- Architecture de réseaux 802 LAN/MAN et leur interconnexion
- Norme **802.1D** : ponts LAN (Interconnexion de réseaux LAN)
- Norme **802.1Q** : réseaux LAN virtuels.
 - Comprend la norme **802.1p** (classes de trafic et priorités dans les réseaux LAN)

Groupe 802.2 : LLC

Groupe 802.3 : Ethernet

- Développement de normes pour les réseaux LAN utilisant CSMA/CD.
- Norme **802.3** : Ethernet (**10 Mb/s Ethernet**, **FastEthernet**, **Gigabit-Ethernet** et **10Gb/s Ethernet**)

Groupe 802.5 : Token Ring

Groupe 802.11 : Réseaux locaux sans fil

- Norme **802.11a** : Réseaux sans fil jusqu'à 54 Mb/s dans la bande de 5 GHz
- Norme **802.11b** : Réseaux sans fil jusqu'à 11 Mb/s dans la bande de 2.4 GHz
- Norme **802.11e** : Qualité de service dans les réseaux 802.11
- Norme **802.11i** : Sécurité
- Norme **802.11g** : Extension de 802.11b pour un débit de 54Mb/s

Groupe 802.12 : Demand Priority

- Norme **802.12a** : 100VG-AnyLAN

Groupe 802.15 : Réseaux PAN (Personal Area Networks) sans fil

- Norme **802.15.1** : Bluetooth
- Norme **802.15.3** : UWB
- Norme **802.15.4** : Zigbee

Sous-couche LLC (Logical Link Control)

- Sous-couche supérieure de la couche liaison
- Effectue les tâches qui sont indépendantes de la technologie sous-jacente
 - Fonctions de la couche liaison selon OSI:

Liaison

LLC

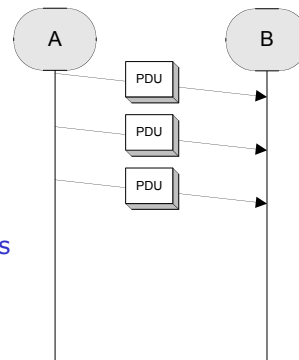
- Transformation du moyen physique de transmission en une **liaison exempte d'erreurs** de transmission
- Transmission de trames et **d'acquittements** entre deux nœuds adjacents
- **Contrôle d'erreurs et retransmission**
- **Élimination** de trames dupliquées
- **Contrôle de la vitesse** d'émission

MAC

- Contrôle **d'accès au médium physique**
- **Structurer le flot de bits** de la couche 1 en trames

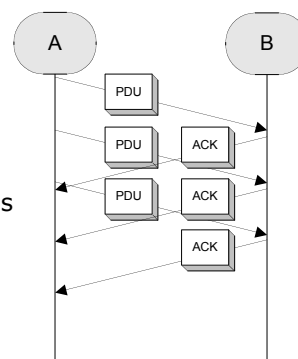
Norme LLC 1 (*unacknowledged connectionless service*)

- Souvent appelé LLC
- Utilisée dans les réseaux Ethernet
- Tient compte du faible taux d'erreur du support physique
 - Transmission de blocs isolés **sans connexion**
 - Sans acquittement
 - Sans **contrôle de l'ordre** des trames
 - Format de la trame permet de **détecter des erreurs bit**
 - Suppression de trames erronées
 - Retransmission initiée par les couches supérieures



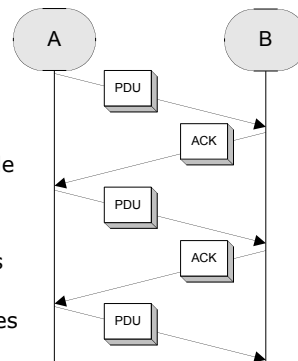
Norme LLC 2 (*connection mode service*)

- Service **orienté connexion**
 - Utilisation d'acquittements
 - Retransmission de trames erronées
 - Élimination de trames dupliquées
 - Contrôle de l'ordre des trames
- Service fiable réalisé à la couche 2 au lieu des couches supérieures comme dans LLC 1



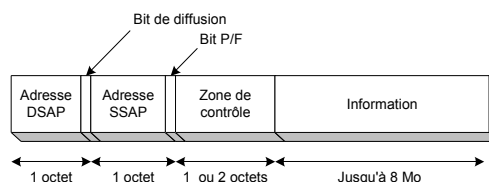
Norme LLC 3 (*acknowledged connectionless service*)

- Service **sans connexion**
- Utilisation **d'acquittement**
- **contrôle de flux**: « envoyer et attendre » (*stop and go*):
 - Transmission d'une trame après la réception de l'acquittement de la trame précédente
- Utilisée dans les **réseaux industriels**
 - L'ordinateur central transmet des informations aux équipements périphériques
 - Mémoire limitée des équipements périphériques



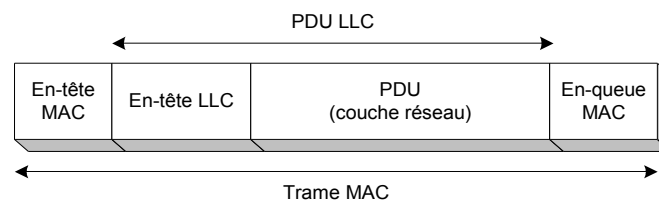
Format d'une PDU LLC

- Utilisé par les trois normes LLC
- **Adresse DSAP** (*Destination Service Access Point*) et **SSAP** (*Source Service Access Point*)
 - Identifient le type de données transmises
- **Bit de diffusion**: Indique s'il s'agit d'une adresse DSAP individuelle ou multipoint
- **Bit P/F**: PDU de commande ou de réponse
- Utilisation du **champ de contrôle** dépend de la norme LLC utilisée



Encapsulation d'une PDU LLC

- Une PDU LLC est encapsulée dans une trame MAC



Sous-couche MAC (Medium Access Control)

- Très important dans les réseaux LAN
- Fonctions principales
 - Structurer le flot de bits de la couche 1 en trames
 - Ajout d'en-têtes et d'en-queues avec des séquences de bits spécifiques
 - Contrôle d'accès au médium physique
 - Souvent par diffusion sur un réseau multipoint
 - Déterminer qui a le droit d'émettre sur un médium partagé
- Utilisent généralement LLC 1

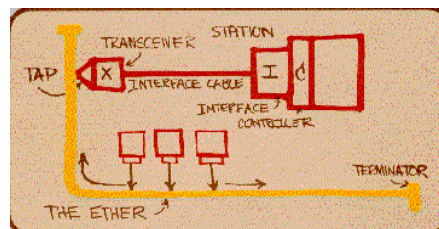
Méthodes de partage d'un canal

- **Partage statique**
 - chaque station dispose en **permanence** de l'accès à une **partie** du canal
 - **sans interférence** avec les communications échangées par les autres stations
 - **Multiplexage fréquentiel**
 - **Multiplexage temporel**
 - Mal adapté au **trafic irrégulier**
- **Partage dynamique**
 - Allocation du canal selon les **besoins des stations**
 - Partage par **élection**
 - Allocation du canal aux stations **à tour de rôle**
 - Utilisé dans **Token Ring**
 - Partage par **contention**
 - Une station peut initier une transmission à tout moment
 - Procédure de **résolution de collisions** de transmissions
 - Utilisé dans **Ethernet**

Exercices 2,3

Ethernet

- Initialement conçu par Xerox sur un **canal partagé**
 - Éther: substance impalpable, imaginée au XVIII^e siècle pour expliquer la propagation des ondes électromagnétiques
 - Proposé comme standard par DEC, Xerox et Intel
 - Normalisé en 1981 comme **IEEE 802.3** et en 1989 comme **ISO 8802-3**
- Deux variantes **incompatibles**
 - Ethernet-II
 - IEEE 802.3
- **La technologie LAN la plus importante**

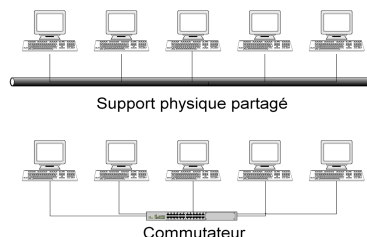


5. Réseaux locaux

15

Modes partagé et commutés

- Mode partagé
 - Possibilité de **collisions**
 - **Mauvaises performances** en cas de charge élevée
 - Temps de transmission **non-déterministe**
 - **Contraintes de la taille** maximale du réseau
- Mode commuté
 - Chaque terminal est directement connecté à un commutateur (*switch*)
 - Transmission full-duplex
 - **Sans collisions**
 - Débit de transmission **dédié**
 - Temps de transmission **déterministe**
 - Transmission half-duplex
 - Collisions entre terminal et switch sont possibles
 - Nécessité de mémoriser les trames dans le switch → **contrôle de flux**
 - **Plus cher**

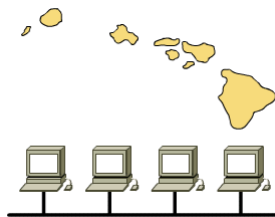


5. Réseaux locaux

16

Méthodes d'accès à médium partagé

- Origine: Protocole **ALOHA**
 - Développé dans les années 1970 par l'Université de Hawaï
 - Permettait la connexion des différentes îles
 - Support physique partagé: canal radio



Protocole ALOHA

- Une station peut envoyer des données **à tout moment** sans vérifier si le canal est libre
- Des **collisions** de transmission rendent les signaux indéchiffrables
- Une station attend **l'acquittement** pendant un délai déterminé
- **Retransmission** des données perdues après un **délai aléatoire**
 - Évite que les même stations entrent à nouveau en collision

Performances du protocole ALOHA

- Hypothèses
 - Nombre très grand d'utilisateurs qui génèrent des trames avec une fréquence totale λ_{gen} constante (selon un processus de Poisson)
 - Durée moyenne de transmission d'une trame: τ
 - Canal de transmission exempt d'erreurs de transmission
 - Temps de propagation du signal négligeable
 - Trafic offert A : Toutes les tentatives de transmission (y compris les collisions et les retransmissions)
 - Trafic écoulé Y : Trafic transmis avec succès
- Nous cherchons la relation entre A et Y

Trafic

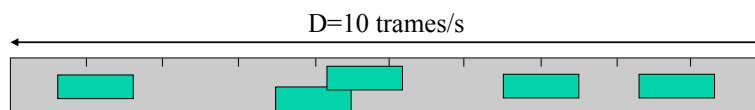
- Trafic offert: $A = \lambda_{\text{tot}} \cdot \tau$
 - Durée moyenne de transmission d'une trame: $\tau = l/D$
 - Longueur moyenne d'une trame: l (bits)
 - Débit de transmission: D (bits/s)
 - Fréquence de transmission de trames: $\lambda_{\text{tot}} = \lambda_{\text{gen}} + \lambda_{\text{retr}}$
 - Fréquence de génération de trames par les utilisateurs: λ_{gen}
 - Fréquence des retransmissions: λ_{retr}
- Trafic écoulé: $Y = \lambda_{\text{reçu}} \cdot \tau$
 - Fréquence de trames reçues correctement: $\lambda_{\text{reçu}}$
- Probabilité de transmission d'une trame sans collision: P_0
 - $\lambda_{\text{reçu}} = P_0 \cdot \lambda_{\text{tot}}$ et

$$Y = P_0 \cdot A$$

Exemple

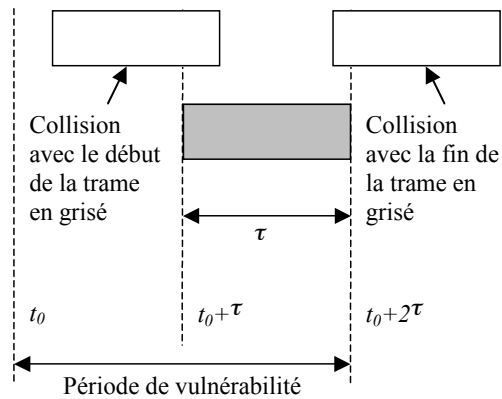
- Longueur moyenne d'une trame: $l = 1500$ octets = 12000 bits
- Débit de transmission: $D = 10$ Mb/s
- ⇒ **Durée de transmission** $\tau = 1,2$ ms
- Fréquence de génération de trames: $\lambda_{gen} = 400$ s⁻¹
- Fréquence de retransmissions de trames: $\lambda_{retr} = 50$ s⁻¹
- ⇒ **Fréquence de tentatives de transmission:** $\lambda_{tot} = 450$ s⁻¹
- ⇒ **Trafic offert** $A = 450$ s⁻¹ · 1,2 ms = 0.54 Erlang

Exemple 2



- $D = 10$ trames/s
- $\tau = 1/10$ s
- $A = 5/10 = 0.5$ E
- $P_0 = 3/5$
- $Y = 3/10 = 0.3$ E

Période de vulnérabilité d'une trame



Modèle mathématique

- Nous cherchons la probabilité de transmission sans collision: P_0
- Probabilité que k trames soient générées pendant un intervalle de temps t :

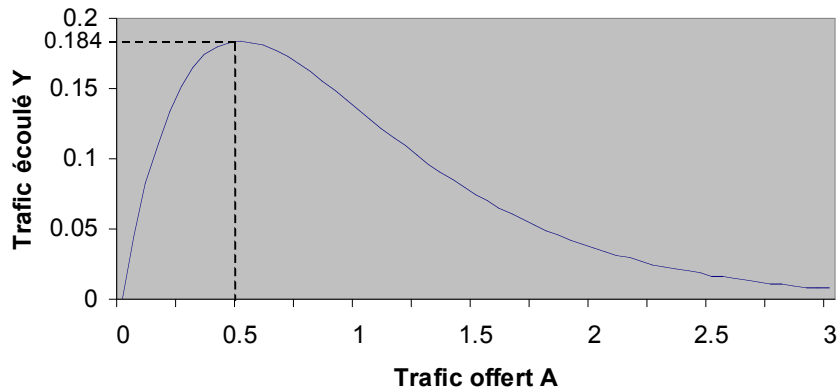
Distribution de Poisson $\Pr(k) = \frac{(\lambda t)^k e^{-\lambda t}}{k!}$

- Alors $P_0 = \frac{(2A)^0 e^{-2A}}{0!} = e^{-2A}$

- Et finalement $Y = A \cdot P_0 = A \cdot e^{-2A}$

Résultats

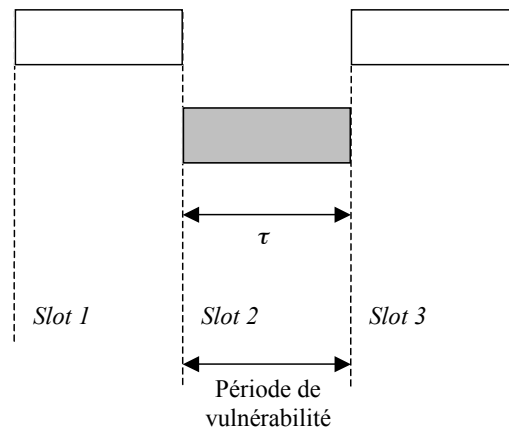
ALOHA



Amélioration: ALOHA discrétisé

- Division du temps en intervalles répétitifs (*slots*)
→ *slotted ALOHA*
 - Les slots ont une durée constante: durée d'une trame
- Début d'une émission seulement au début d'un slot
- Nécessite une *synchronisation* entre les stations
- Effets:
 - Dans le cas d'une collision, les trames se chevauchent complètement et non seulement en partie
 - Diminution de la période de vulnérabilité

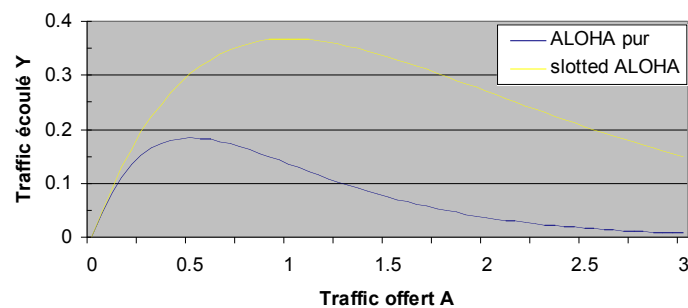
Période de vulnérabilité dans ALOHA discrétisé



Résultats

- Période de vulnérabilité: τ
- Trafic écoulé: $\gamma_{\text{slotted}} = A \cdot e^{-A}$

ALOHA



Performances d'Aloha discrétisé

- Utilisation optimale du canal
 - Occupation utile maximale du canal (= trafic écoule Y) 36.8 % (= 0.368 E)
 - Occupation du canal par les collisions: 26.4 % des slots
 - Occupation optimale du canal 63.2 % (= 0.632 E)
- Canal non-utilisé: 36.8 % des slots
- L'occupation du canal peut être augmentée en augmentant le trafic
 - Croissance exponentiellement le nombre de collisions
 - Diminution de trafic écoulé

Délai moyen de transmission

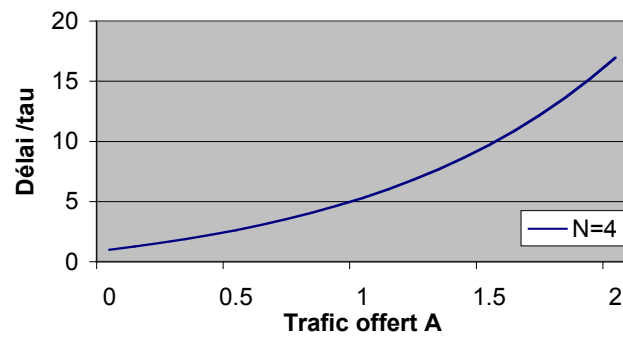
- Probabilité d'une trame de ne pas subir une collision: $P_0 = e^{-A}$
- Probabilité d'une trame de subir une collision: $1 - P_0 = 1 - e^{-A}$
- Probabilité de nécessiter k transmissions: $P_k = e^{-A} (1 - e^{-A})^{k-1}$
- Nombre moyen de transmission d'une trame:

$$E = \sum_{k=1}^{\infty} k P_k = \sum_{k=1}^{\infty} k e^{-A} (1 - e^{-A})^{k-1} = e^A$$

- Délai aléatoire entre retransmissions: $(1 \dots N) \cdot \tau$
- Délai moyen entre retransmissions: $\frac{N+1}{2} \tau$
- Délai moyen de transmission d'une trame:

$$D = (e^A - 1) \frac{N+1}{2} \tau + \tau$$

Aloha discrétisé: Délai moyen de transmission



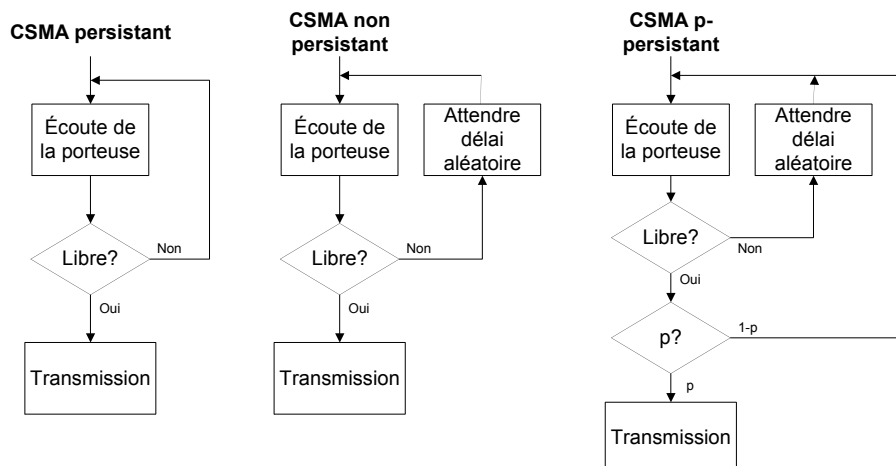
- Exemple
 - Trafic offert: $A = 1 \text{ E}$
 - Délai moyen de transmission: $D = 5.2 \tau$

Exercice 1

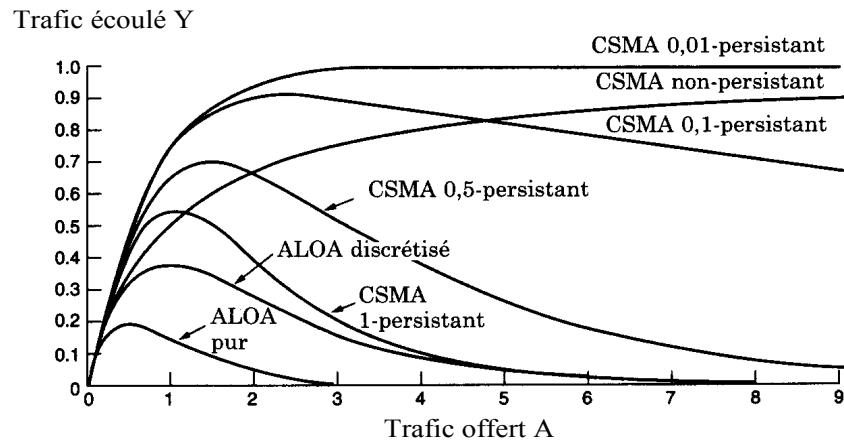
Méthode CSMA

- Dans ALOHA, l'émetteur initie la transmission sans vérifier si le canal est libre
- Le câble **permet d'écouter** si le canal partagé est libre
- Protocole amélioré:
Carrier Sense Multiple Access (CSMA)
- Collisions toujours possibles à cause du délai de propagation

Variantes de CSMA



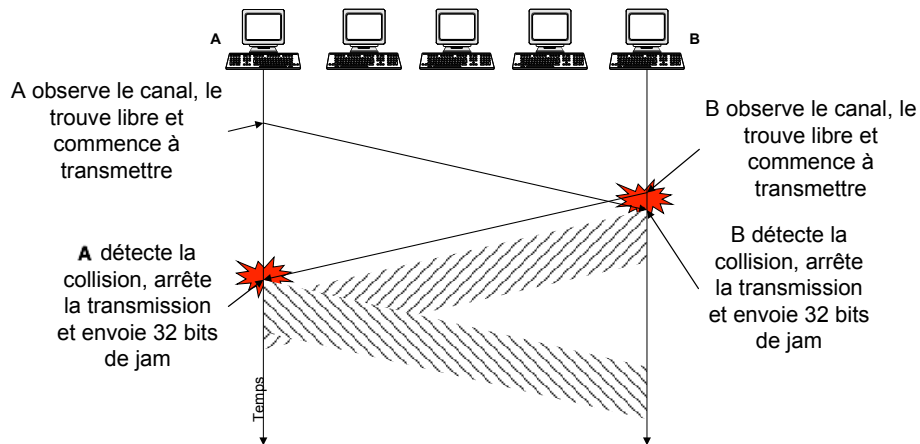
Performances de CSMA



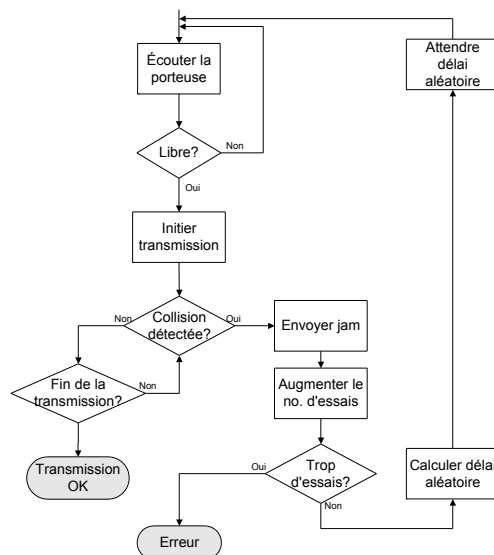
La sous-couche MAC Ethernet

- Le câble comme médium partagé permet
 - de vérifier si le canal est libre
 - de détecter une collision
 - L'émetteur écoute le canal même pendant sa transmission
 - Une collision se manifeste par une différence entre le signal transmis et le signal vu sur le canal
- Algorithme CSMA/CD:
 - Carrier Sense Multiple Access and Collision Detect
 - Les émetteurs peuvent arrêter très tôt une transmission en collision

Exemple d'une collision

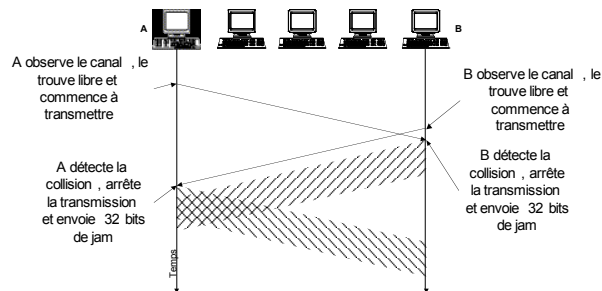


Algorithme CSMA/CD



Paramètres d'IEEE 802.3

- Certains paramètres doivent être définis pour pouvoir détecter correctement les collisions
 - Temps de propagation aller-retour maximal: 51,2 μ s
 - Taille minimale d'une trame: 512 bits
 - Longueur du signal jam: 32 bits



5. Réseaux locaux

39

Calcul du délai aléatoire entre retransmissions

- Après une collision, l'émetteur attend un délai aléatoire avant de retransmettre
 - Diminue la probabilité d'une nouvelle collision des mêmes trames
- « **Truncated Binary Exponential Backoff** »
 - Après n collisions:

$\text{Délai de retransmission} = r \cdot 51.2 \mu\text{s}$
 $\text{Nombre aléatoire } r \text{ avec } 0 \leq r \leq 2^m - 1$
 $m = \min(n, 10)$
 - Exemple:
 - 1^{ère} retransmission: $r = 0$ ou 1
 - 2^{ème} retransmission: $r = 0, \dots, 3$
 - 3^{ème} retransmission: $r = 0, \dots, 7$
 - 10^{ème} retransmission: $r = 0, \dots, 1023$
 - 11^{ème} retransmission: $r = 0, \dots, 1023$

➤ **Augmentation exponentielle du délai entre retransmissions**

5. Réseaux locaux

40

Performances de CSMA/CD

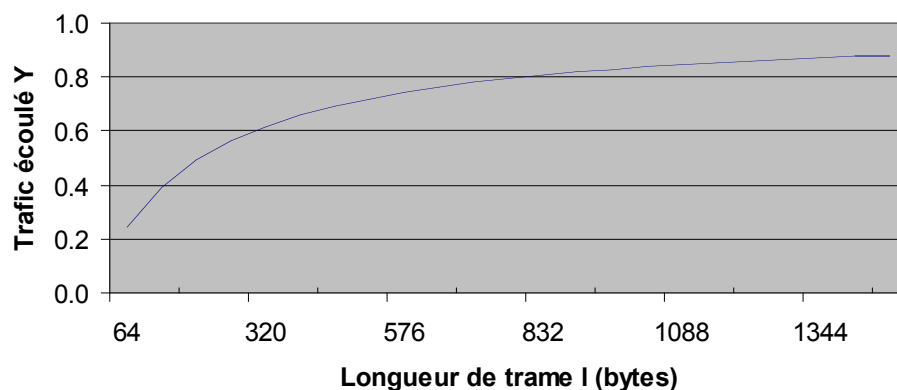
- Modèle simple basé sur l'hypothèse d'un **trafic poissonnien** ($\Rightarrow$ **modèle optimiste**)
 - Modèles tenant compte d'un trafic réaliste sont trop complexes
- **Limite optimiste** au trafic écoulé:

$$Y = \frac{1}{1 + \alpha \frac{B}{l} RTT}$$

- B : Débit nominal de transmission du réseau (p.ex. $B=10$ Mb/s)
- l : taille moyenne des trames, y compris toutes les entêtes
- RTT : Temps aller-retour maximal du réseau (*Round-Trip-Time*) ($RTT \leq 51.2 \mu s$)
- α : **constante empirique**
 - valeur pessimiste: $\alpha=3,1$,
 - valeur réaliste: $\alpha=2,5$

Résultats

- $B = 10$ Mb/s
- $RTT = 51,2 \mu s$
- $\alpha = 2,5$

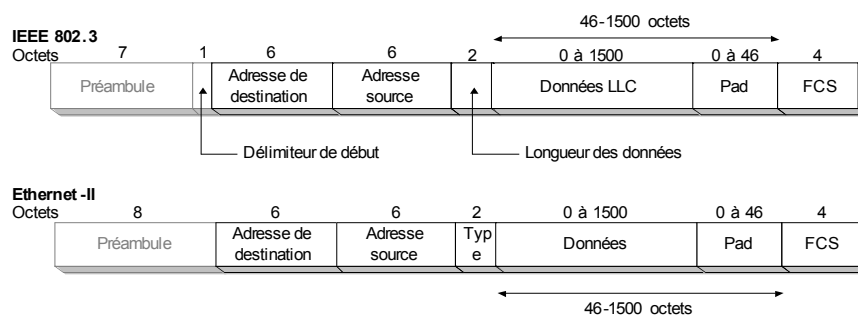


Exercices 6,7,8

- A faire ensemble: Exercice 33

Formats de trame Ethernet-II/802.3

- Padding pour obtenir la taille minimale de trame
- Longueur des données (802.3) ≤ 1500 , Type (Ethernet) > 1500
- FCS: code polynomial (CRC) sur tous les champs sauf préambule et délimiteur
- Préambule/préambule+délimiteur : 7 octets 10101010, dernier octet 10101011



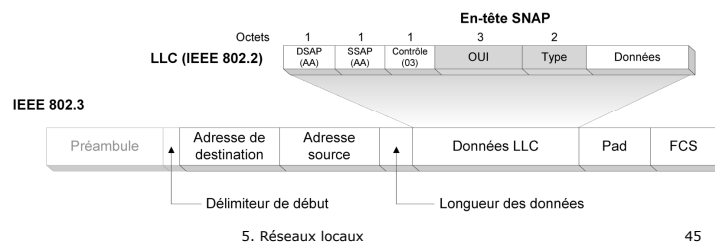
IP sur Ethernet

- Presque toutes les cartes réseau utilisent Ethernet-II pour la transmission de datagrammes IP
- Le champ 'Type' de la trame contient la valeur 0800 hex pour indiquer un datagramme IP

Ethernet-II



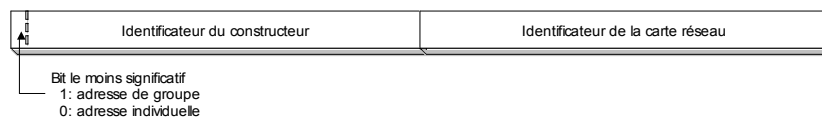
- IP sur IEEE 802.3: Encapsulation SNAP (SNAP/LLC/802.3)



45

Adresses MAC

- Adresse physique d'une carte réseau
 - **Unique** : Toutes les cartes de réseaux ont une adresse différente
 - **Fixe** : configurée dans la mémoire ROM de la carte
- Longueur: 48 bits
 - 3 premiers octets : Identification du constructeur (définie par l'IEEE)
 - 00-00-0C-xx-xx-xx: Cisco
 - 08-00-20-xx-xx-xx: Sun
 - 08-00-09-xx-xx-xx: HP
 - 3 derniers octets : Identification de la carte (gérée par le constructeur)
 - Bit le moins significatif du premier octet: Indique une adresse de groupe



5. Réseaux locaux

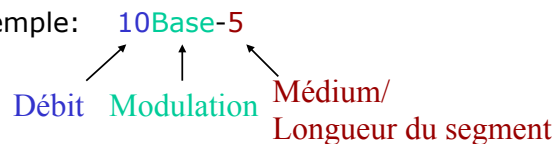
46

Adresses de groupe

- **Broadcast (diffusion)**
 - Adresse FF-FF-FF-FF-FF-FF
 - Les cartes réseau écoutent cette adresse et les stations doivent traiter les trames reçues
 - Commutateurs et ponts : transmettent une trame reçue sur tous les ports
 - Applications
 - **ARP** : conversion adresses IP --> MAC)
- **Multicast**
 - 1^{er} bit transmis de l'adresse vaut 1 (1^{er} octet de l'adresse est impair)
 - Exemple : 09-00-2B-00-00-0E
 - Une station doit configurer la carte réseau d'écouter une adresse multicast
 - Applications :
 - Configuration automatique de l'acheminement dans un LAN (**Spanning Tree Protocol**)
 - Tous les ponts font partie d'un groupe multicast

Types de réseau Ethernet

- La norme 802.3 définit toute **une famille de technologies** basées sur CSMA/CD
- Premiers réseaux Ethernet:
 - 10 Mb/s sur un câble coaxial comme médium partagé
- Évolution de la norme:
 - Technologies plus performantes (100 Mb/s, 1 Gb/s, ...)
- Noms des technologies
 - Exemple: **10Base-5**

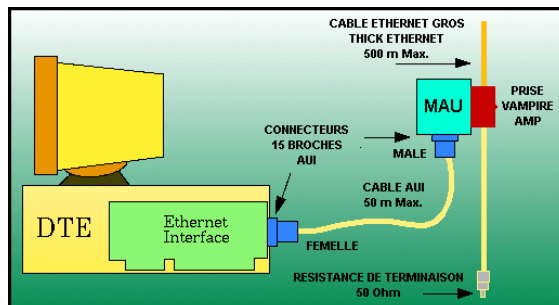


Types d'Ethernet

Type	Débit	Codage	Longueur max. d'un segment	Média	Topologie
10Base-5	10 Mb/s	Bande de base	500 m	Câble coax. épais	Bus
10Base-2	10 Mb/s	Bande de base	185 m	Câble coax. fin	Bus
10Base-T	10 Mb/s	Bande de base	100 m	UTP cat. 3, 2 paires	Étoile
100Base-TX	100 Mb/s	Bande de base	100 m	UTP cat. 5, 2 paires	Étoile
100Base-FX	100 Mb/s	Bande de base	2000 m	2 fibres multimodes	Étoile
1000Base-T	1 Gb/s	Bande de base	100 m	UTP cat. 5 e, 4 paires	Étoile
1000Base-X (plusieurs normes)	1 Gb/s	Bande de base	275-5000 m	2 fibres optiques	Étoile

10Base-5 (*Thicknet*)

- Premier mode défini et utilisé
 - Configuration en bus sur un câble coaxial partagé
 - Débit de transmission : 10 Mb/s



Transceiver (MAU)

- Circuit électronique pour la transmission et réception
- Détection de collisions
- Câble AUI (*Attachment Unit Interface*)
 - Relié à la carte réseau
 - Câble de 5 paires torsadées
 - Long. max. 50 m

Segment 10Base-5

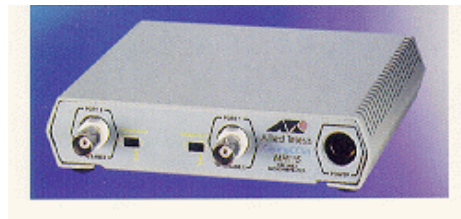
- **Segment**: câble partagé auquel les stations sont connectées
 - Câble coaxial
 - Diamètre: 1 cm
 - Impédance caractéristique: 50 ohms
 - Terminaisons de 50 ohms des deux bouts, dont une mise à terre
 - Coefficient de vélocité : 0,77
 - **Longueur maximale** d'un segment : **500 m**
 - Distance des stations: multiples de 2,5 m
 - **Nombre maximal** de stations par segment : **100 stations**

Utilisation de 10Base-5

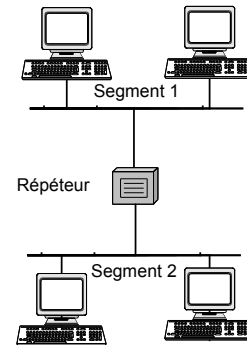
- **Inconvénients majeurs**
 - Rigidité, diamètre et coût du câble
- **Pratiquement plus utilisé**
- **Emploi est réservé aux sites**
 - nécessitant un **segment long** ou
 - une bonne protection contre les **interférences électromagnétiques**

Répéteurs

- Interconnectent plusieurs segments pour
 - couvrir des distances plus longues que 500 m
 - connecter plus de 100 stations dans un LAN



5. Réseaux locaux



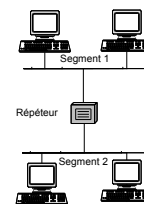
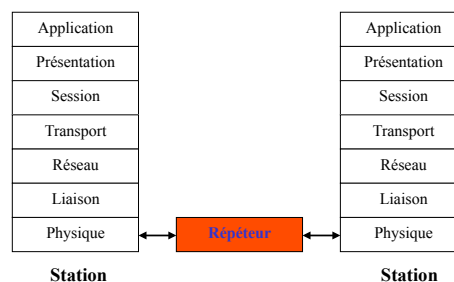
Fonctions d'un répéteur

Travaille au niveau de la couche 1

- Transmet bit par bit sans décoder les trames
- Régénère le signal
 - Transmission sur une distance plus élevée

Gestion de collisions

1. Collisions causées par d'autres éléments du réseau:
 - Propage la collision reçue vers les autres segments
2. Collisions causées par le répéteur
 - Arrête la transmission et envoie le signal jam
 - Ne ré-émet pas la trame



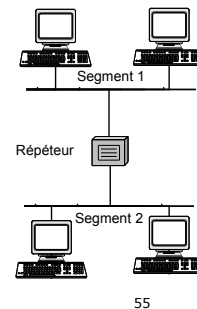
5. Réseaux locaux

Domaine de collision

Domaine de collision :

Ensemble des stations et systèmes intermédiaires d'un LAN dont les transmissions peuvent entrer en collision

- Exemples
 - Un seul segment 10Base-5
 - Plusieurs segments interconnectés par un répéteur
- Un répéteur élargit le domaine de collision



Taille maximum d'un LAN

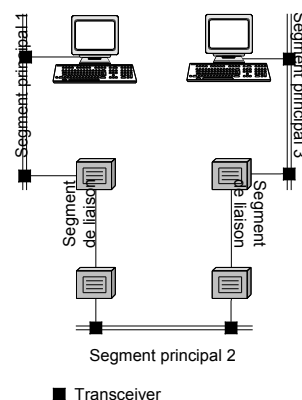
Norme:

- Délai de propagation aller-retour $\leq 51,2 \mu s$
- Temps de propagation sur les segments et à travers les répéteurs sont définis dans la norme

- Règle 5-4-3-2-1

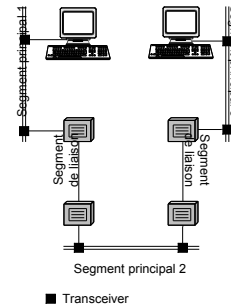
Un chemin traverse au maximum :

- 5 segments et
- 4 répéteurs
- dont 3 segments principaux (avec stations)
- et 2 segments de liaison
 - Sans stations
 - Paires torsadées ou fibres
- Résultat: 1 domaine de collision



Longueur du chemin maximum

3 segments principaux (500 m chacun)	1500 m
2 segments de liaison	1000 m
6 câbles AUI pour la connexion aux segments principaux (50 m chacun)	300 m
Distance maximum	2800 m

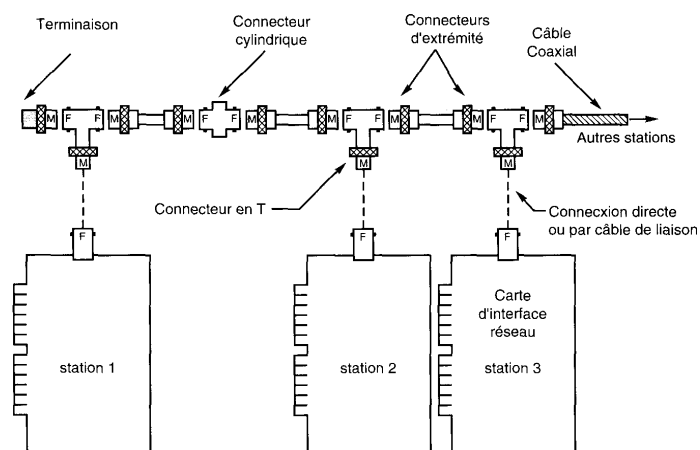


Exercice 34

10Base-2

- Aussi appelé **Thinnet** ou **Cheapnet**
- Utilise un câble coaxial moins encombrant et plus souple (RG-58)
 - Débit de transmission: 10 Mb/s
 - Diamètre du câble: 0,48 cm
 - Impédance caractéristique: 50 ohms
 - Coefficient de vélocité: 0,65
 - Longueur maximale d'un segment: 185 m
 - Nombre maximal de stations par segment: 30

Éléments d'un réseau 10Base-2

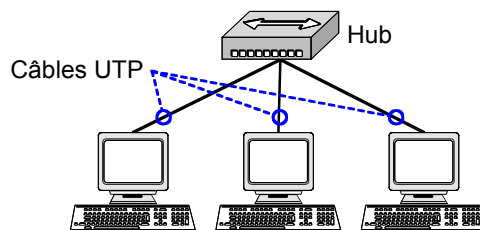


Interconnexion de segments 10Base-2

- Même règle que pour 10Base-5 (5-4-3-2-1)
- Interconnexion de segments 10Base-5 et 10Base-2 possible
- Résumé des paramètres
 - Longueur maximale d'un segment: 185 m
 - Nombre maximal de stations par segment: 30
 - Nombre total de stations dans un LAN: 1024
 - Distance minimale entre deux stations: 0,5 m

10Base-T

- Configuration en étoile
 - Problème des réseaux en bus: localisation de ruptures, ...
 - Nœud central: hub
 - Câbles à paires torsadées
 - Possibilité d'utiliser le câblage existant dans les bâtiments
- Configuration la plus répandue actuellement



Câbles 10Base-T

- Spécifications

Paramètre	
Média physique	Câble à paires torsadées
Impédance caractéristique	100 ohms
Coefficient de vélocité	0,585
Débit de transmission	10 Mb/s
Longueur maximale d'un segment	100 m
Nombre de stations par segment	2

- La norme n'exige pas un type de câble précis mais permet l'utilisation de différents types

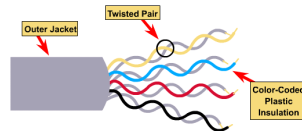
Câbles à paires torsadées

- Paire torsadée:
 - deux conducteurs en cuivre, isolés l'un de l'autre,
 - enroulés de façon hélicoïdale
 - **Avantage**: meilleure protection électromagnétique
- Câble à paires torsadées:
 - Comprend plusieurs paires torsadées
 - Avec écran ou non

Types de câbles torsadés

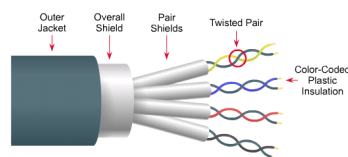
UTP (Unshielded Twisted Pair)

- Comprend 4 paires torsadées non écrantées
- Longueur jusqu'à 100 m
- **Avantages**: moins cher et plus flexible
- Différentes catégories:
 - Cat. 3: jusqu'à 10 Mb/s
 - Cat. 5: jusqu'à 100 Mb/s
 - Cat. 5e, 6, 7a: Gigabit-Ethernet (1-100 Gb/s)



STP (Shielded Twisted Pair)

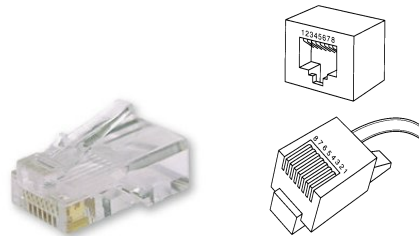
- Paires individuelles et câble complet sont écrantés
- Longueur jusqu'à 100 m
- Atténuation plus faible
- **Inconvénient**: cher et difficile à installer (mise à terre)



Connecteur RJ-45

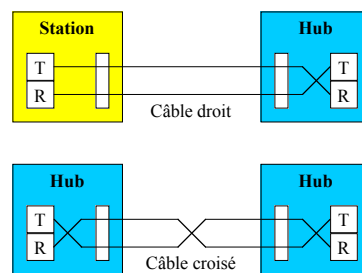
- Raccordement normalisé pour 10Base-T
 - Seulement deux paires (émission et réception) du câble sont utilisées
 - Raccorde directement les cartes réseaux (avec les transceivers intégrés dans les cartes)

Broche	Signal
1	Transmission +
2	Transmission -
3	Réception +
4	Non utilisé en 10Base-T
5	Non utilisé en 10Base-T
6	Réception -
7	Non utilisé en 10Base-T
8	Non utilisé en 10Base-T



Croisement

- La paire d'émission de la source doit être la paire de réception du destinataire
 - Croisement des paires nécessaire
- Les hubs effectuent souvent un **croisement interne** au niveau des ports
- **Pour la connexion direct hub-hub, PC-PC: câble croisé**



5. Réseaux locaux

67

Hubs

- Réseaux 10Base-T :
 - câblage en étoile
 - mais une **topologie logique en bus**
 - Hub: bus logique
- Hub = **répéteur multi-port**
 - Travaille au niveau de la **couche physique** (niveau des bits)
 - Reçoit, contrôle et **régénère** les signaux reçus sur chaque port



5. Réseaux locaux

68

Exercices 9,10,11

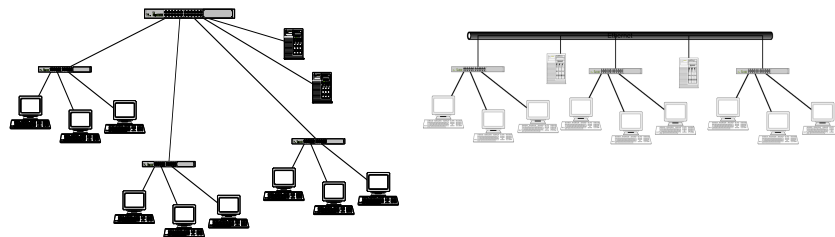
Fonctions avancées

Auto-partition:

- Permet d'isoler des segments défectueux
 - Arrêt de toute transmission d'un segment en faute vers les autres ports
 - Trafic des autres ports continu à être envoyé sur le segment défectueux
- Segment est considéré défectueux
 - Après 30 collisions consécutives
 - Lors d'une collision permanente
- Cause classique d'un segment défectueux:
 - Oubli de la terminaison de 50 ohms lors de l'installation d'un segment coaxial

Interconnexion de hubs (10Base-T)

- Pour augmenter le nombre de ports
- Pour relier des stations distantes
- Même règle que dans 10Base-5 et 10Base-2:
 - Au maximum **4 répéteurs/hubs** entre deux stations
 - **Distance maximale** avec des segments 10Base-T: **500 m**
 - Pour couvrir des distances plus grandes:
Segment **10Base-5** comme épine dorsale



5. Réseaux locaux

71

FastEthernet

- Débit de transmission: 100 Mb/s
- Couche MAC similaire à Ethernet à 10 Mb/s
 - Même format de trame
 - CSMA/CD comme méthode d'accès
 - **Seule modification**: réduction de la **durée de transmission d'un bit**

- Conséquences:

Paramètre	
Délai aller-retour maximal	512 temps bit (= 5.12 µs)
Longueur du signal jam	32 bits
Interframe gap	0,96 µs
Taille minimale d'une trame	64 octets

➤ **Diamètre maximum d'un domaine de collision: 200 m**
(10Base-5 > 2km)

- **Bonne compatibilité**
 - au niveau logiciel des stations
 - et matériel (p.ex. hubs avec ports 10 Mb/s et 100 Mb/s)

5. Réseaux locaux

72

Normes FastEthernet

100Base-TX (1995)

- Utilise deux paires torsadées d'un câble UTP cat. 5

100Base-FX

- Requiert deux fibres optiques multimodes

100Base-T4 (1995)

- Requiert quatre paires d'un câble UTP cat. 3, 4 ou 5
- Ne permet pas la transmission full-duplex

100Base-T2 (1997)

- Utilise deux paires torsadées d'un câble UTP cat. 3

- Pas de support de câbles coaxiaux
- Seulement 100Base-TX et 100Base-FX sont utilisées

100Base-TX et 100Base-FX

- 100Base-TX
 - Similaire aux réseaux 10Base-T
 - Câblage en étoile (UTP cat. 5!) avec un hub/switch comme nœud central
 - Longueur maximale d'un segment: 100 m
- 100Base-FX
 - Utilise un câble à deux fibres optiques multimodes
 - Le croisement est effectué au niveau du câble
 - Longueur maximale d'un segment: 400 m
 - Connecteurs:



Connecteur duplex SC



Connecteur MIC

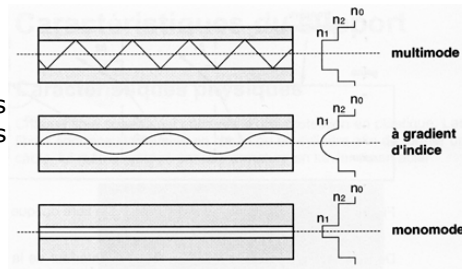


Connecteur ST

Types de fibres optiques

Fibre multimode

- Diamètre épais (62,5 ou 50 μm)
- Le signal se propage avec plusieurs 'angles' (modes) différents
- L'interférence entre les modes limite la distance de transmission (dispersion modale)



Fibre monomode

- Diamètre plus petit (10 μm)
- Un seul mode est possible
- Très bonnes caractéristiques de transmission
- Plus chère

Interconnexion de segments FastEthernet

- Répéteur/hub FastEthernet :
 - Peut interconnecter des segments 100Base-TX avec 100Base-FX
 - Au maximum deux répéteurs dans un chemin
 - Règle 5-4-3-2-1 n'est plus valable

Configurations maximales

Configuration	100Base-TX	100Base-FX
Longueur maximale d'un segment	100 m	412 m
Réseaux avec un répéteur	200 m	320 m
Réseaux avec deux répéteurs	205 m	228 m

Gigabit-Ethernet

Sur cuivre

1000Base-T (802.3ab)

- Dernière norme Gigabit
- Utilise 4 paires UTP 5e
- Longueur max. d'un segment: **100 m**
- **Full duplex, plus de Hubs!**

1000Base-CX

- Sur câble STP spécial
- Principalement pour le 'patching' entre deux switches dans une armoire
- Longueur max d'un segment: **25 m**

Sur fibre optique

1000Base-LX ($\lambda=1300$ nm)

- Sur une paire de fibres (multimode ou monomode)
- Longueur max d'un segment :
 - Half Duplex: 316 m
 - FD sur fibre **multimode**: 550 m
 - FD sur fibre **monomode**: 5000 m

1000Base-SX ($\lambda=850$ nm)

- Sur une paire de fibres **multimodes**
 - Moins cher que 1000Base-LX
- Longueur max d'un segment :
 - Half Duplex: 316 m
 - FD, fibre **multimode**, 62,5 μ m: 275 m
 - FD, fibre **multimode**, 50 μ m :500 m

Standards industriels (sans norme officielle)

- 1000Base-ZX ($\lambda=850$ nm)
 - Sur fibres optiques monomodes
 - Longueurs maximum d'un segment (full duplex!)
 - Sur fibre monomode, 10 μ m: 70 km
 - Sur fibre monomode, 8 μ m: 100 km
 - Distance minimum:
 - Avec atténuateur: 10 km
 - Sans atténuateur: 40 km
- 1000Base-LH
 - Similaire à 1000Base-LX, mais jusqu'à 10 km sur fibre monomode

CSMA/CD dans Gigabit-Ethernet

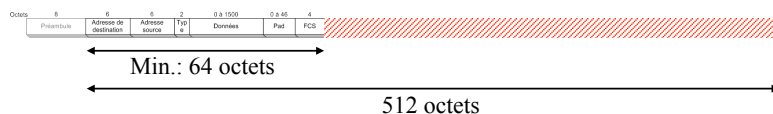
- La norme exige qu'un commutateur Gigabit-Ethernet soit capable de travailler en half-duplex
 - Utilisation de CSMA/CD
- Problème en half-duplex :

Débit	10 Mb/s	100 Mb/s	1000 Mb/s
Délai aller retour max.	51,2 µs	5,12 µs	512 ns
Étendue max.	2800 m	200 m	20 m ?

- Solutions:
 - ~~Ne pas utiliser CSMA/CD (half-duplex)~~
 - ~~Agrandir la trame avec du padding plus long~~
 - Prolonger la durée de transmission d'une trame courte

Carrier extension (Half Duplex)

- Ajout d'octets de bourrage à la fin d'une trame courte



- Durée de transmission minimum d'une trame $\approx 4 \mu s$ (512 octets)
- Étendue maximale du réseau similaire à FastEthernet
- Exemple du débit de transmission en half duplex:
 - Charge utile de la trame : 60 octets (Voix sur IP)
 - FastEthernet: $100 \text{ Mb/s} * 60 \text{ octets} / 86 \text{ octets} = 69 \text{ Mb/s}$
 - Gigabit-Ethernet: $1 \text{ Gb/s} * 60 \text{ octets} / 520 \text{ octets} = 117 \text{ Mb/s}$

Interconnexion de réseaux locaux

- A l'aide de ponts et commutateurs
 - Évitent les problèmes de l'interconnexion par des hubs

Pont:

- Souvent réalisé en logiciel
- Peu de ports (normalement 2)
- Lent

Commutateur

- Réalisé en hardware
- Beaucoup de ports

Exercices 26,27

Types de ponts

- L'IEEE a défini deux types de ponts
 - Pont transparent
 - Utilisé dans des réseaux Ethernet
 - Pont à routage par la source
 - Utilisé dans des réseaux Token Ring
- Ces deux types de ponts sont **incompatibles**
 - Les ponts d'un LAN doivent être du même type
- Interconnexion d'Ethernet avec Token Ring
 - Ponts « mixed media »

Fonctions principales des ponts

- Acheminer une trame reçue vers le ou les ports de sortie
 - Une trame est normalement transmise sur un seul port, vers le destinataire
 - Destinataire inconnu: **diffusion** sur tous les ports
- Filtrage du trafic
 - Diminution la charge du réseau
 - Augmente la sécurité
- Séparation des domaines de collision

Ponts transparents

Transparence

- Le pont doit fonctionner sans aucune configuration ou modification du réseau

Fonctions principales

1. Apprentissage dynamique de la table de commutation

Adresse MAC	Port de sortie
00-00-0C-E1-F2-03	2
06-20-EE-02-3A-02	1
03-03-35-AC-54-01	1

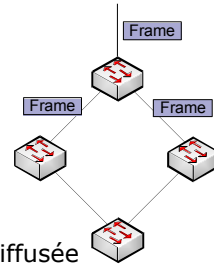
2. Résolution automatique de **boucles** dans la topologie
 - Protocole de l'« **arbre recouvrant** »

Acheminement et filtrage des trames

- Hub:
 - Une trame reçue est diffusée sur tous les ports
- Pont / switch
 - **Apprentissage** des stations atteignables sur chaque port
 - *Filtering Database*: Adresse MAC destinataire → Port de sortie
 - Une entrée apprise est valable pendant **5 min** (par défaut)
 - Destinataire inconnu: **diffusion** sur tous les ports
- Diminue la charge du réseau
- Augmente la sécurité
- Mais les trames de broadcast se propagent à travers le LAN entier
 - Un seul domaine de broadcast

Spanning-Tree Protocol (Arbre recouvrant)

- Ethernet ne fonctionne que dans une topologie en arborescence
- Une topologie avec boucles peut dupliquer des trames
 - Une trame vers un destinataire inconnu est diffusée sur le réseau entier
 - La trame peut revenir au pont/switch qui l'a diffusée
 - Boucle de transmission infinie
- Mais: une topologie avec boucles augmente la **fiabilité** du LAN
- Solution:
 - Créer une topologie physique **avec redondance**
 - Spanning Tree Protocol pour désactiver dynamiquement certains ports



Protocole de l'Arbre Recouvrant (« *Spanning tree* »)

- Construction d'une **topologie virtuelle**
 - Il existe exactement un chemin entre chaque paire de réseaux
 - **Sans boucles**
 - Tous les réseaux peuvent être **atteints**
- Construite à partir de la topologie réelle en **désactivant certains ports**

Construction de l'arbre recouvrant

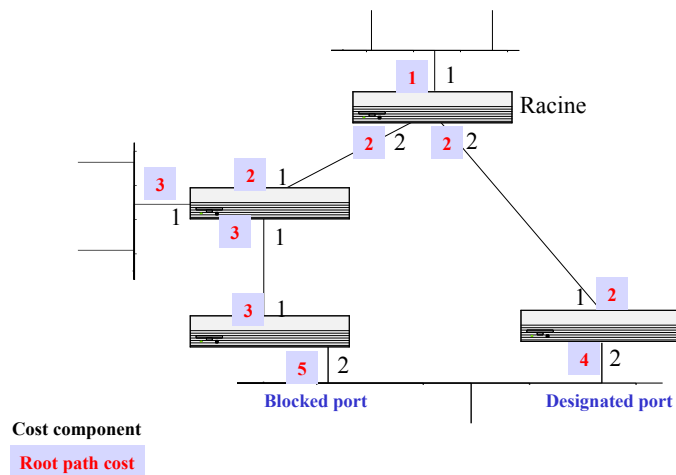
1. Élection de la racine de l'arbre
 - Initialement tous les switches émettent des trames BPDU (message 'Hello') contenant l'identificateur de la machine
 - Le switch avec le plus petit identificateur (adresse MAC + priorité) devient la racine
 - Seule la racine continue à émettre des BPDU (toutes les 2s)
2. Pour chaque switch: sélection d'un port racine
 - Port racine : Port avec la distance la plus petite vers la racine
3. Pour chaque LAN: sélection d'un **port désigné**
 - Port désigné: port attaché à un segment qui offre le chemin le plus court entre le LAN et la racine
 - Les autres ports attachés à un LAN sont désactivés

Sélection d'un port racine / désigné

Algorithme:

- Chaque port a un 'coût partiel' (*cost component*) assigné
- Les BPDU indiquent le coût total du chemin parcouru
- Un pont transmet une BPDU reçue sur les ports de sortie
 - Additionne le coût partiel au coût du chemin
→ **Coût du port vers la racine**
- Le port avec le coût le plus petit devient port racine
- Un port ayant un coût x doit être désactivé quand une BPDU avec un coût total inférieur est reçu sur ce port
 - Seul le port désigné reste actif sur le LAN

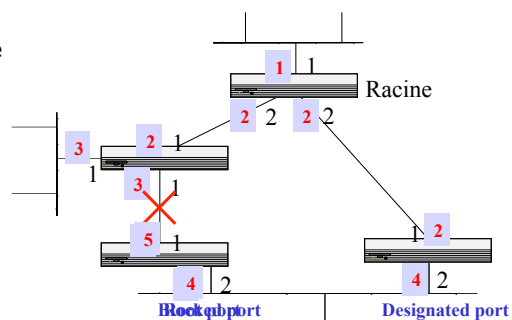
Exemple



Panne d'un lien

- Les coûts appris sont valables pendant un certain temps (p.ex. 20s)
- Ils doivent périodiquement être renouvelés par des BPDUs
- Après une panne d'un lien, l'état des ports (bloqué/actif) peut changer
- Un message « **Annonce de changement de topologie** » informe les switches de mettre à jour leur table de filtrage
- En général, la reconfiguration prend env. 30s

– Le protocole « **Rapid Spanning Tree** » (802.1w) permet une convergence en moins d'une seconde



Exercices 48,49,50

Ponts à routage par la source

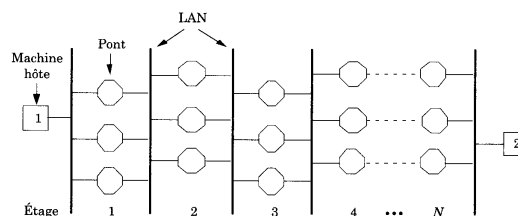
- Les ponts transparents sont faciles à installer mais n'utilisent pas toute la capacité du réseau (→ports désactivés)
- Les tenants de **Token Ring** ont opté pour un autre type de pont
 - Pont de routage à la source
- **Routage par la source**
 - La source indique le chemin complet à suivre par la trame
 - Les ponts intermédiaires lisent le chemin et acheminent la trame

Découverte de la route

1. La source X envoie en diffusion une trame « **Découverte de chemin** »
2. Les ponts intermédiaires **inscrivent leur nom** dans la route parcourue et diffuse la trame sur tous les ports de sortie
3. Le destinataire Y reçoit plusieurs trames et retourne chacune à la source X en utilisant la route indiquée dans la trame (routage par la source)
4. La source reçoit une trame de réponse pour **chaque route possible**
 - Peut choisir la « meilleure » route
 - La source mémorise les routes apprises

Avantages et inconvénients

- **Avantages**
 - L'algorithme trouve la meilleure route
 - La transmission de trames peut être répartie sur plusieurs routes
- **Inconvénient**
 - Explosion combinatoire des trames de découverte du chemin

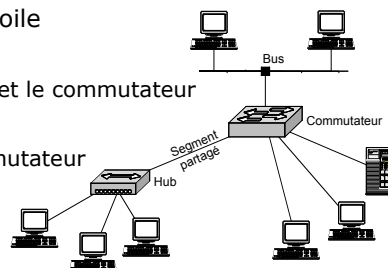


Interconnexion de LANs hétérogènes

- Exemple
 - Interconnexion d'Ethernet avec Token Ring
- Des ponts « **mixed media** » existent
- Les incompatibilités des technologies rendent impossible une interconnexion parfaite
 - Exemple: Longueur maximale de trames
 - Ethernet 1500 octets
 - Token Ring > 5000 octets
 - Une partie de la fonctionnalité des LANs est sacrifiée
- **Meilleure solution:**
Interconnexion par des routeurs (niveau 3)

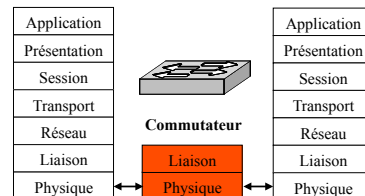
Ethernet commuté

- Ethernet partagé:
 - **Bande passante est partagée** entre toutes les stations du domaine de collision
 - FastEthernet (100 Mb/s) avec 1024 stations
 - > 100 kb/s par station en moyenne
- Ethernet commuté
 - Topologie physique **et logique** en étoile
 - Port based switching:
 - Lien point à point entre une station et le commutateur
 - Segment based switching:
 - Segment partagé connecté au commutateur



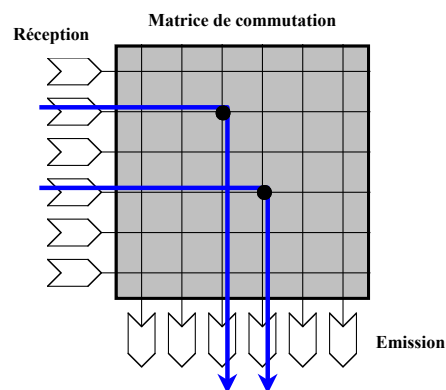
Commutateur (switch)

- Travaille au niveau de la **couche liaison** (niveau trames)
- Fonction principale:
 - **Acheminer** un trame reçue vers le ou les ports de sortie
- Différences par rapport à un hub
 - Interprète l'en-tête des trames
 - Implémente une topologie logique en étoile
 - Traite plusieurs trames simultanément
- **Sépare les domaines de collision**



Commutation

- Port:
 - composé d'un récepteur et d'un émetteur
 - Connecté à une **matrice de commutation**
- Les ports sont **indépendants** l'un de l'autre
 - Plusieurs trames peuvent être commuté simultanément
 - Pas de collisions entre les trames de différents ports
- **Chaque port représente un domaine de collision**



Techniques de commutation: *Store and forward*

- Technique
 1. Réception de la trame complète
 2. Analyse et contrôle d'erreurs
 3. Commutation vers le port de sortie
- Avantages
 - Adapté aux configurations asymétriques (10/100 Mb/s)
 - Trames incorrectes sont filtrées
- Inconvénients
 - Temps de latence élevé
 - Nécessite une mémoire tampon de grande taille

Techniques de commutation: *Cut-through switching*

- Technique
 1. Le commutateur attend les premiers octets de l'en-tête
 2. Décodage de l'adresse du destinataire
 3. Réception et transmission de la trame **au même temps**
- Avantages
 - Temps de latence très court et constant
 - Mémoire tampon faible
- Inconvénients
 - Contrôle d'erreurs n'est pas possible
 - Ne permet pas de conversion de la vitesse

Techniques de commutation: *Adaptive error free*

- Combine store and forward avec cut-through
 - Le commutateur travaille en mode cut-through
 - Le contrôle d'erreurs est effectué pour chaque trame
 - Ne permet pas de filtrer des trames incorrectes
 - Le commutateur change en mode store and forward après plusieurs erreurs consécutives

Ethernet full-duplex

- Un commutateur peut travailler en full-duplex ou half-duplex
 - Half-duplex
 - Utilise CSMA/CD
 - Une seule transmission sur un segment à chaque moment
 - Full-duplex (optionnel)
 - Transmissions simultanées dans les deux sens sur un lien point à point
 - Pas de collisions
 - Pas de retransmission
 - **Pas de CSMA/CD !**

Avantages du full-duplex

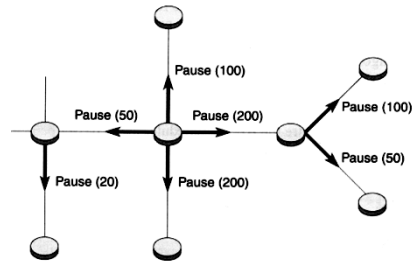
- Double la bande passante d'un lien point à point
- Pas d'attente avant d'émettre
 - Seulement l'interframe gap doit être respecté
- **Aucune limitation de la longueur d'un segment**
 - Délai aller-retour n'est plus important
 - Atténuation peut être compensée à l'aide de répéteurs

Inconvénients d'Ethernet commuté

- **Gestion d'adresses**
 - Nécessaire pour le filtrage de trames
 - Nécessite une quantité non-négligeable de mémoire
 - Peut ralentir la commutation de trames
 - Un réseau important doit être sous-divisé en réseaux logiques: **VLAN**
- **Contrôle de flux** nécessaire
 - Congestion d'un switch possible (contrairement à un hub)
 - Configuration asymétrique: 100 Mb/s --> 10 Mb/s
 - Concentration du trafic sur un port de sortie

Contrôle de flux 802.3x (en full duplex)

- Lorsqu'un port commence à être saturé, le switch peut envoyer une trame de contrôle « Pause » en amont
 - La trame « Pause » indique le temps pendant lequel le récepteur n'a plus le droit de transmettre
 - Problèmes:
 - Pas tous les switches l'implémentent complètement
 - Déconseillé si la QoS est activée



Auto-négociation

- Plusieurs modes utilisent les câbles UTP avec RJ-45 (10Base-T, 100Base-TX, 1000Base-T, Half/Full duplex)
- Connexion de deux cartes avec des modes différents est possible
- L'auto-négociation permet aux cartes réseaux d'annoncer les modes Ethernet implémentés et de configurer le mode le plus approprié que les deux cartes supportent
 - Optionnelle pour 10Base-T, 100Base-TX
 - Obligatoire pour 1000Base-T, mais uniquement pour le mode et non pas le débit
- Attention: Quelques interfaces Gigabit-Ethernet ne négocient pas le débit (ne fonctionnent pas à 10 ou 100 Mb/s)
- Signalisation est compatible avec cartes réseau sans auto-négociation

Signalisation auto-négociation

- Utilise des séquences d'impulsions de test de liens (link test pulse)
 - Rafales de 33 impulsions qui code les modes implémentés
- Une carte non-compatible les interprète comme test de lien



Mode	Priorité
1000Base-T full-duplex	9
1000Base-T half-duplex	8
100Base-T2 full-duplex	7
100Base-TX full-duplex	6
1000Base-T2 half-duplex	5
1000Base-T4 half-duplex	4
1000Base-TX half-duplex	3
10Base-T full-duplex	2
10Base-T half-duplex	1

Auto-négociation et duplex mismatch

- Lorsque deux interfaces sont connectées, elles utilisent l'auto-négociation pour déterminer
 - Le débit (10/100; 1000 Mb/s pour les interfaces multispeed)
 - Le mode (half / full duplex)
 - Le croisement des paires (Gigabit-Ethernet)
 - **Fiable et recommandée par les constructeurs**
- Problème du « Duplex mismatch » (applicable à 10/100 Mb/s)
- Une interface est manuellement mise à **x Mb/s, FD**
 - Elle ne participe pas à l'auto-négociation
 - L'autre interface va correctement détecter le débit (Parallel Detection Function)
 - **MAIS: l'autre interface se mettra en Half Duplex, comme elle ne peut pas détecter le mode !**
 - **Problèmes de performances (beaucoup de collisions)**
- Solutions
 - Utiliser l'auto-négociation (recommandée)
 - Configurer manuellement le même mode des deux côtés
 - Configuration manuelle d'un côté, mais en HALF DUPLEX

Exercices 38,39,40,41

Réseaux locaux virtuels (VLAN)

- Problèmes de l'interconnexion par les ponts et les commutateurs
 - Les ponts/commutateurs doivent connaître toutes les machines du réseau
 - Les trames de diffusion se propagent dans le réseau entier
 - Un seul « domaine de broadcast »
- Solution:
 - **VLAN**: Ensemble logique de stations dans un réseau local
 - Les différents VLAN sont isolés les uns des autres
- Avantages
 - Contrôle des trames broadcast
 - Chaque VLAN est un domaine de broadcast séparé
 - Sécurité
 - Les utilisateurs peuvent être groupés en fonction de leurs privilèges
 - La communication inter-VLAN peut être sécurisée par des routeurs et firewalls
 - Administration
 - Affectation d'un utilisateur à un groupe par configuration, sans re-câblage

Regroupement logique des stations

VLAN par port

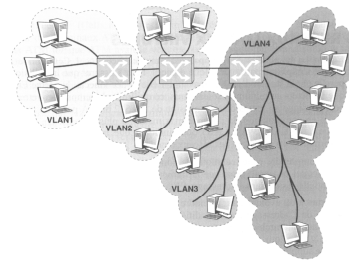
- Chaque port d'un switch est assigné à un VLAN
- Les stations connectées sur un port font partie de ce VLAN
- Simple à configurer mais peu flexible

VLAN basés sur les adresses IP

- Sur chaque switch, les VLAN sont définis à travers des listes d'adresses IP
- Déplacement de machines sans reconfiguration
- Le switch doit inspecter les en-têtes IP

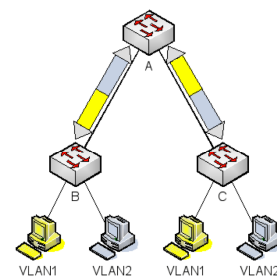
VLAN basés sur des critères arbitraires

- N'importe quel champs du paquet peut définir des VLAN
- Exemple typique: VLAN selon les adresses MAC



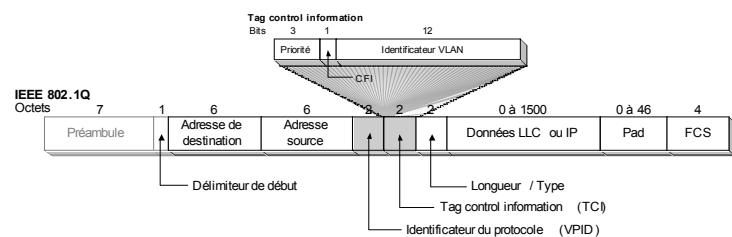
VLAN trunking

- Un VLAN peut s'étendre sur plusieurs commutateurs
- Comment savoir sur quel port il faut transmettre une trame reçue ?
 - Les liens entre commutateurs (« trunk links ») multiplexent le trafic de plusieurs VLAN
 - L'administrateur peut restreindre les VLAN sur un tronçon VLAN
 - Le commutateur d'accès marque la trame avec le VLAN d'origine lors de la transmission sur un tronçon VLAN
- Deux méthodes de **VLAN tagging**:
 - IEEE 802.1Q (Norme officielle)
 - Cisco ISL (protocole propriétaire Cisco)



VLAN tagging avec IEEE 802.1Q

- Ajout de 4 octets dans l'en-tête Ethernet/802.3
 - Utilisé uniquement entre les commutateurs, les stations typiquement ne génèrent ou reçoivent pas ces trames
 - La longueur max d'un trame passe à 1522 octets
- L'identificateur VLAN permet de distinguer jusqu'à 4096 VLAN (Cisco: souvent au maximum 1000 VLAN)



Exemple de configuration

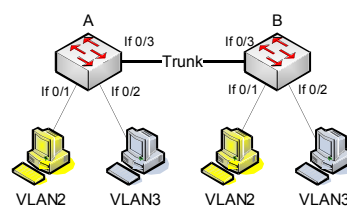
Switch A

1. Définition des deux VLAN

```
SwitchA#vlan database
SwitchA(vlan)#vlan 2 name Compta
SwitchA(vlan)#vlan 3 name Marketing
SwitchA(vlan)#exit
```

2. Configuration des ports d'accès

```
SwitchA#config terminal
SwitchA(config)#interface fastethernet 0/1
SwitchA(config-if)#switchport access vlan 2
SwitchA(config-if)#exit
SwitchA(config)#interface fastethernet 0/2
SwitchA(config-if)#switchport access vlan 3
SwitchA(config-if)#exit
```

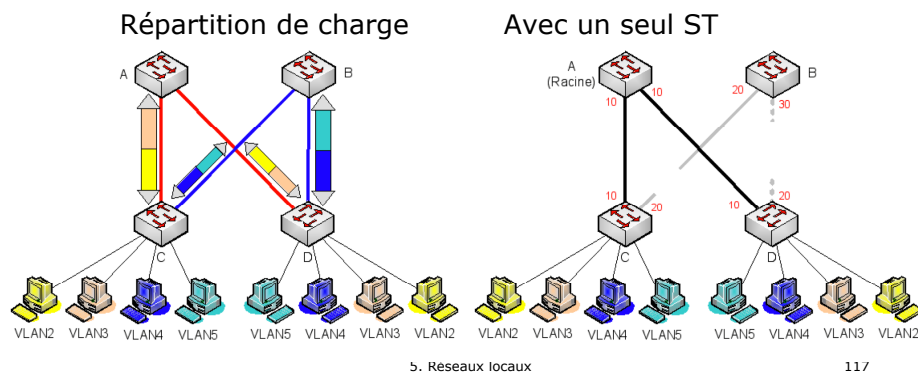


3. Configuration des ports trunk

```
SwitchA(config)#interface fastethernet 0/3
SwitchA(config-if)#switchport mode trunk
SwitchA(config-if)#switchport trunk encapsulation dot1q
SwitchA(config-if)#switchport trunk allowed vlan remove 4-1001
SwitchA(config-if)#exit
```

VLAN et Spanning Tree

- A l'origine, 802.1Q utilise le même Spanning Tree pour tous les VLAN
 - Pas de répartition de charge



Spanning Trees multiples

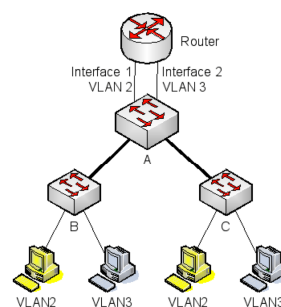
- Plusieurs solutions ont été développées pour créer des ST multiples, permettant la répartition de charge
- IEEE **MSTP** (*Multiple Spanning Tree Protocol*)
 - La méthode préconisée, si disponible
 - Permet de créer plusieurs instances de ST
 - Pour chaque instance, sur chaque switch
 - Configuration de la **priorité racine** et du **coût d'un port**
 - Un VLAN est assigné à une instance de ST
- Protocoles prioritaires Cisco
 - PVST (*Per VLAN Spanning Tree*)
 - Un ST pour chaque VLAN
 - MISTP (*Multiple Instances Spanning Tree Protocole*)

Routage entre VLAN

- Les différents VLAN sont complètement isolés au niveau des switches
 - Aucune trame ne passe directement d'un VLAN à un autre
- La communication entre VLAN nécessite un routeur
 - Un firewall peut filtrer les paquets non autorisés
 - Même niveau de sécurité que pour une connexion vers un réseau externe

Routage avec une interface par VLAN

- Le routeur a plusieurs interfaces, une par VLAN
- Les ports du switch vers le routeur sont des **ports d'accès**
 - Le switch enlève le VLAN tag avant d'envoyer une trame au routeur
 - Le switch ajoute le VLAN tag aux trames reçues du routeur
- Simple, mais trop cher s'il y a beaucoup de VLAN

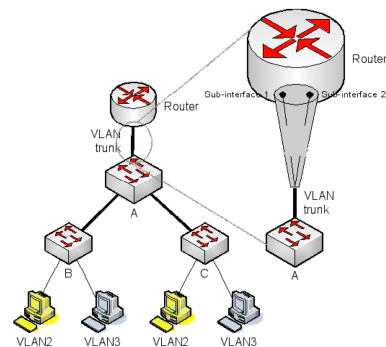


Routing avec interfaces virtuelles

- Le routeur a une seule interface physique qui est connectée à un **port trunk** du switch
- Quand le routeur reçoit une trame, il enlève le VLAN tag et effectue l'algorithme de routage normal.
 - Il trouve une **interface virtuelle** de sortie
- Chaque interface virtuelle est associée à un VLAN et marque les trames avec le VLAN correct

Exemple de configuration

```
Rtr(config)#interface fastethernet 0/1.1
Rtr(config-subif)#encapsulation dot1q 2
Rtr(config-subif)#ip address 10.1.0.1 255.255.0.0
```



Exercices 56,57

Les réseaux locaux sans fil

- En plein développement depuis quelques années
 - Réseaux d'entreprises
 - Réseaux publics (« hot spots »)
 - Aéroports et gares
 - Bistros, ...
- **Avantages**
 - Mobilité
 - Facilité de l'installation
 - Coût
- **Inconvénients et problèmes**
 - Problèmes liés à la transmission radio: Interférences, multi-trajets
 - Législation
 - Sécurité !
 - Qualité de service (débit faible, média partagé)

Normes principales

IEEE 802.11

- Réseaux « Wi-Fi » (Certification)

Norme	Débit nominal	Commentaire	Bande de fréquences
802.11	1 et 2 Mb/s	Première norme	2.4 GHz
802.11a	Jusqu'à 54 Mb/s	Incompatible avec les normes 802.11b/g	5 GHz
802.11b	1, 2, 5.5, 11 Mb/s	Deuxième génération	2.4 GHz
802.11g	Jusqu'à 54 Mb/s	Le plus populaire, compatible avec 802.11b	2.4 GHz

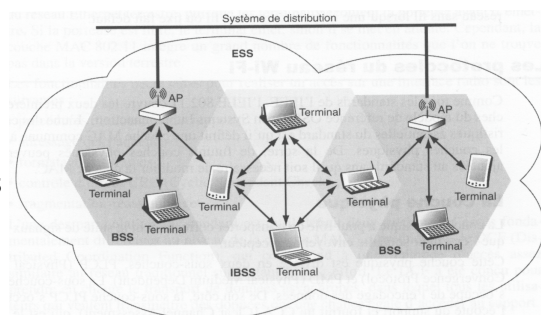
- 802.11e: Qualité de Service (finalisée en 2005?)
- 802.11f: Roaming entre AP
- 802.11i: Améliorations de sécurité (WPA)
- 802.11n: Nouvelle génération (108 – 600 Mb/s)

Principe de conception

- Puissance d'émission faible
 - durée plus longue des batteries
- Couche physique robuste
 - Réflexions multiples
 - Interférences avec d'autres émetteurs
 - Taux d'erreurs de $BER=10^{-4}$ ($BER=10^{-10}$ sur fibres optiques)
- Possibilité d'utiliser la technologie au niveau global
- Transparence envers les applications existantes
- Sécurité acceptable

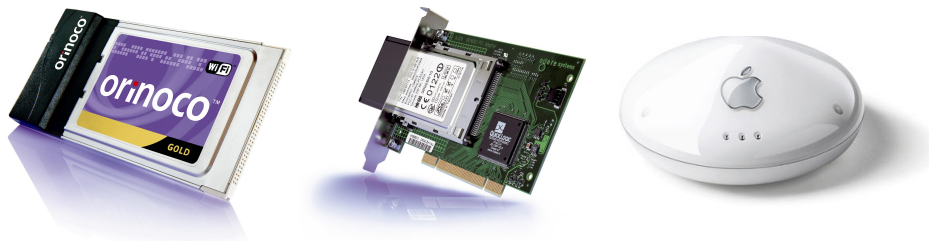
Structure des réseaux WLAN

- Mode **infrastructure**
 - Transmissions (normalement) par l'intermédiaire d'un AP
 - Interconnexion des BSS par un système de distribution
- Mode **ad-hoc**
 - Transmission directe entre les stations

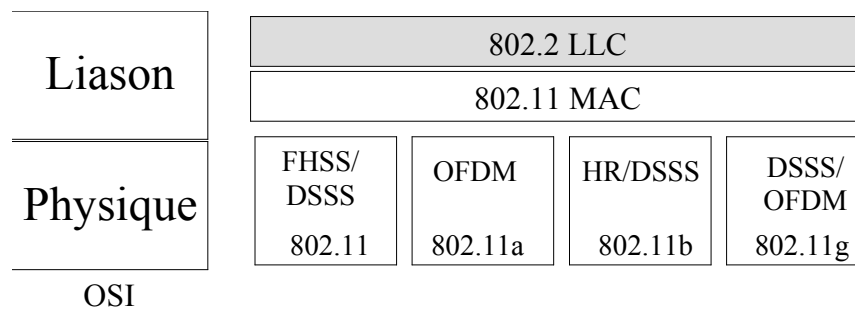


AP (Access Point) : point d'accès
BSS (Basic Service Set) : cellule de base
ESS (Extended Service Set) : ensemble des cellules de base
IBSS (Independent Basic Service Set) : cellule de base en mode ad-hoc

Équipements



IEEE 802.11 dans la hiérarchie OSI



Les couches physiques 802.11x

- Utilisent des modulations de **Spectre Étale** (*Spread Spectrum*)

Principe:

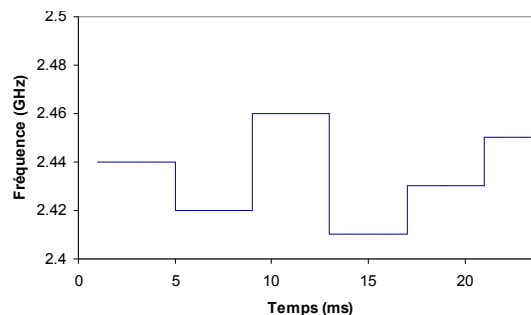
Étaler la puissance du signal sur une bande de fréquences beaucoup plus large que nécessaire

- Sacrifie de la largeur de bande
- Réduit les interférences et les effet de bruit
- Taux d'erreur plus faible

FHSS

Frequency hopping spread spectrum

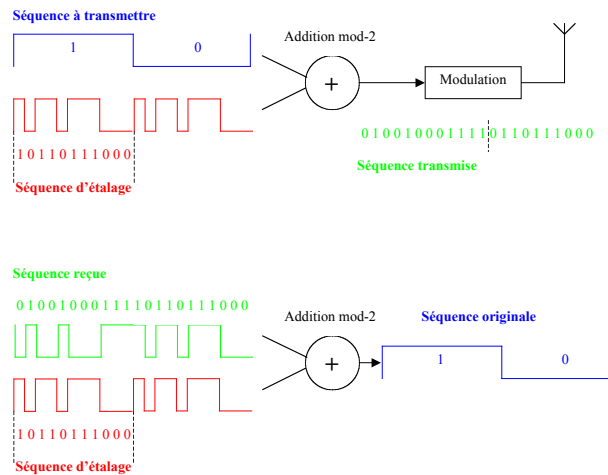
- Utilisé par 802.11 (1 ou 2 Mb/s) dans la bande 2,4-2,483 GHz
- Émetteur et récepteur changent de manière pseudo-aléatoire mais coordonnée les fréquences



DSSS

Direct Sequence Spread Spectrum

- Utilisé par 802.11b à 2,4 GHz
- Multiplication du signal avec une séquence d'étalement
- 0 → 10110111000
- 1 → 01001000111



5. Réseaux locaux

131

OFDM

Orthogonal Frequency Division Multiplexing

- Utilisé par 802.11a et 802.11g à 54 Mb/s
- Basé sur le **multiplexage fréquentiel**
- Principe
 - Utilisation de plusieurs porteuses → **sous-canaux**
 - Répartition de la séquence binaire à transmettre sur les différents sous-canaux
 - **Orthogonalité**: élimination d'interférences entre les sous-canaux

5. Réseaux locaux

132

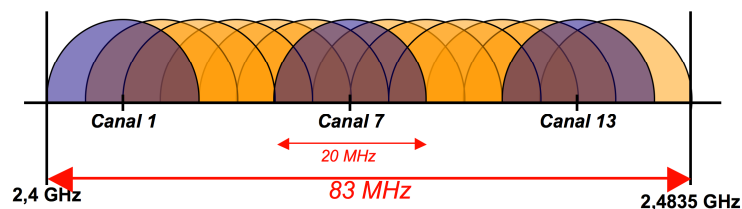
IEEE 802.11b

- « Wi-Fi » ou « Wi-Fi 2 »
- Produits disponibles depuis 2000
- Autorisée en Europe
- Zones de couverture

Débit	Portée
A l'intérieur des bâtiments	
11 Mb/s	50 m
5 Mb/s	75 m
2 Mb/s	150 m
1 Mb/s	200 m
A l'extérieur des bâtiments	
11 Mb/s	200 m
5 Mb/s	300 m
2 Mb/s	400 m
1 Mb/s	500 m

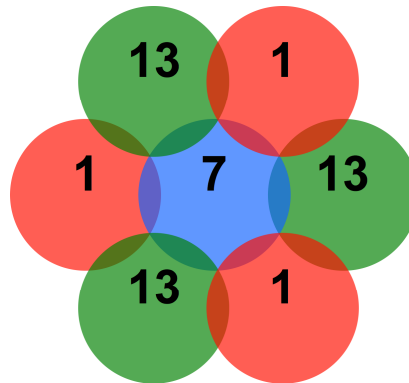
IEEE 802.11b

- Transmission dans la bande de 2,4 GHz
- DSSS comme méthode de modulation
- Largeur de bande de 83 MHz est divisé en 14 canaux de 20 MHz de largeur de bande chacun
 - Autorisés: Europe: 13, US: 11, France: 4, Espagne: 2
- Une cellule peut utiliser jusqu'à 3 canaux simultanément (en Europe !)



Réutilisation des canaux

- Zone de couverture de chaque cellule limitée
- Réutilisation des fréquences sans interférences



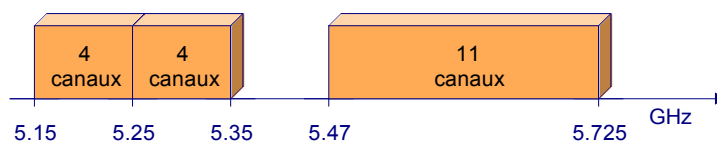
Exercices 62,66,67

IEEE 802.11g

- Remplace IEEE 802.11b dans la bande de 2,4 GHz
- Débit jusqu'à 54 Mb/s
- OFDM comme modulation
- Compatible avec 802.11b
- Portée supérieure à 802.11a

IEEE 802.11a (Wi-Fi 5)

- Débit à la couche physique jusqu'à 54 Mb/s
 - Débit dépend fortement de la distance
- Transmission dans la bande de 5 GHz
 - 19 canaux complètement séparés en Europe
- OFDM comme méthode de modulation
- Incompatible avec 802.11b/g



IEEE 802.11n

- Norme disponible depuis 9.**2009**
- Débit théorique: **300 Mb/s**. En pratique: 100 Mb/s sur 100 m.
- Technologie MIMO et OFDM
- Bande des 2.4 GHz ou **des 5 GHz**

Choix de la bonne norme

Norme	Caractéristiques	Avantages	Inconvénients
802.11b	• Débit jusqu'à 11 Mb/s • Bande de 2.4 GHz • 3 canaux séparés	• Utilisée par la plupart des équipements • Prix faible • Bonne portée	• Débit faible • Interférence avec d'autres équipements dans la bande de 2.4 GHz • Peu de canaux utilisables simultanément
802.11g	• Débit jusqu'à 54 Mb/s • Bande de 2.4 GHz • 3 canaux séparés	• Bonne portée • Compatible avec 802.11b • Débit élevé • Prix moyen	• Interférence avec d'autres équipements dans la bande de 2.4 GHz • Peu de canaux utilisables simultanément
802.11a	• Débit jusqu'à 54 Mb/s • Bande de 5 GHz • 19 canaux séparés	• Pas d'interférences avec d'autres équipements • Débit élevé • Beaucoup de canaux utilisables simultanément	• Portée plus faible • Coût plus élevé • Incompatible avec 802.11b

MAC 802.11

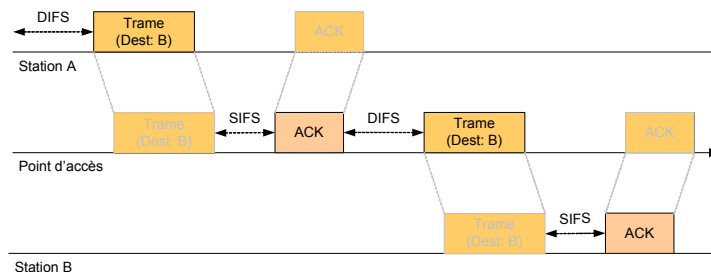
- Deux modes sont définis
 - DCF (Fonction de Coordination Distribuée)
 - Basée sur CSMA avec des extensions
 1. CSMA/CA: Carrier Sense Multiple Acces / Collision avoidance
 2. Réservation du canal avec RTS / CTS
 - Collisions possibles
 - Appropriée à la transmission de données (sans QoS)
 - PCF (Fonction de Coordination Centralisée)
 - Basée sur l'interrogation périodique des stations par l'AP
 - Sans collisions
 - Appropriée au services temps réel
 - Utilisable seulement en mode infrastructure



Méthode CSMA

- Canal radio: détection de collision difficile
 - CSMA/CD n'est pas utilisable
- Principe de CSMA dans 802.11
 - Une station écoute le canal avant de transmettre
 - Si le canal est libre pendant un temps DIFS: transmission
 - Si le canal est occupé: remettre transmission à plus tard
 - Durée d'occupation est signalée dans les trames
 - Chaque trame doit être acquittée après chaque transmission
 - Intervalle SIFS (< DIFS) entre la réception de la trame et l'acquittement)

Exemple



Transmission A -> AP -> B

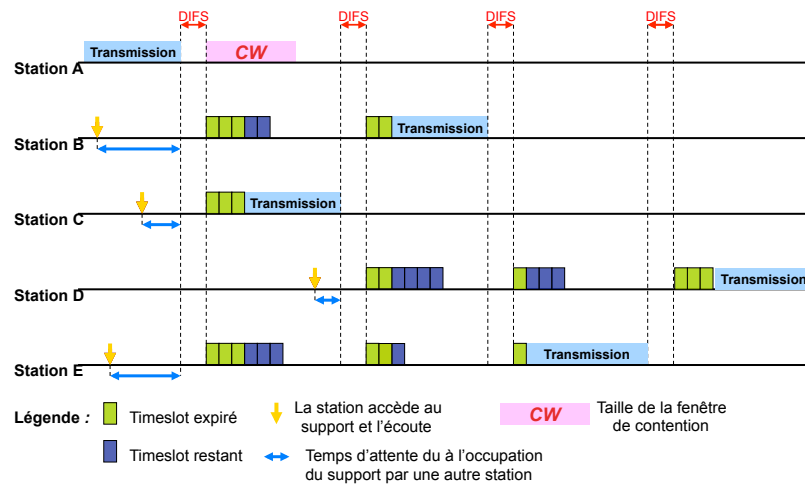
- Chaque trajet est acquitté
- Le point d'accès n'a pas de priorité
 - Il est possible qu'une autre station gagne accès au canal avant lui
 - Dans ce cas, le point d'accès va transmettre la trame plus tard

Évitement de collisions

- Défaut de CSMA:
 - Lorsque plusieurs stations attendent la libération du canal, il y aura forcément une collision
- CSMA/CA (*Collision avoidance*)
 - Après avoir vu le canal vide pendant DIFS, une station doit encore attendre un délai aléatoire avant de transmettre
 - Le délai aléatoire est calculé comme

$$d = \text{TimeSlot} * \text{Random}(0, \text{CW})$$
 - CW: Contention Window
 - $\text{CW}_{\min} = 31$, $\text{CW}_{\max} = 1023$
 - Double après chaque collision
 - La station décrémente le délai aléatoire seulement quand le canal est libre

Exemple: Collision Avoidance



Collision avoidance

- Similaire au backoff exponentiel d'Ethernet
- Mais: il est utilisé
 - quand le canal est occupé lors de l'écoute
 - après une transmission réussie
 - après chaque retransmission
- Résultat
 - Évite les collisions quand le canal se libère
 - Empêche une station de monopoliser le canal
 - Toutes les stations ont la même priorité d'accéder le canal
 - Pas de qualité de service

Débit effectif

- Le débit effectif d'une transmission est inférieur au débit de la couche physique (11 Mb/s ou 54 Mb/s) à cause des en-têtes des trames et des délais d'attente lors des transmissions (DIFS, Backoff, acquittements).

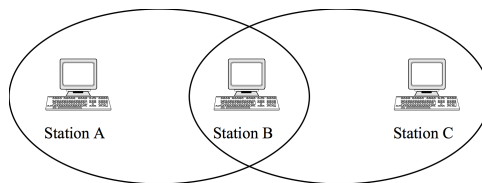
Débits effectifs pour un datagramme IP

Standard	Maximum PHY data rate	Max. effective throughput	
		64B packet	1500B packet
802.11b	11 Mb/s	0.8 Mb/s	7.1 Mb/s
802.11g/a	54 Mb/s	1.3 Mb/s	20 Mb/s

Exercice 83

Faiblesses

- Collisions toujours possibles
 1. Deux stations atteignent simultanément
 $\text{Temporisateur}_{\text{Back-off}} = 0$
 2. Problème de la station cachée
- **Réservation du canal peut**
 - Éviter le problème de la station cachée
 - Réduire la durée de collisions



La réservation avec RTS et CTS

Message RTS (*request-to-send*):

- Bref message envoyé par la source pour indiquer l'intention d'émettre

Message CTS (*clear-to-send*):

- Bref message envoyé par la destination comme réponse au message RTS
- Reçu par tous les nœuds dans la couverture du récepteur
- Indique la durée de la 'réservation'

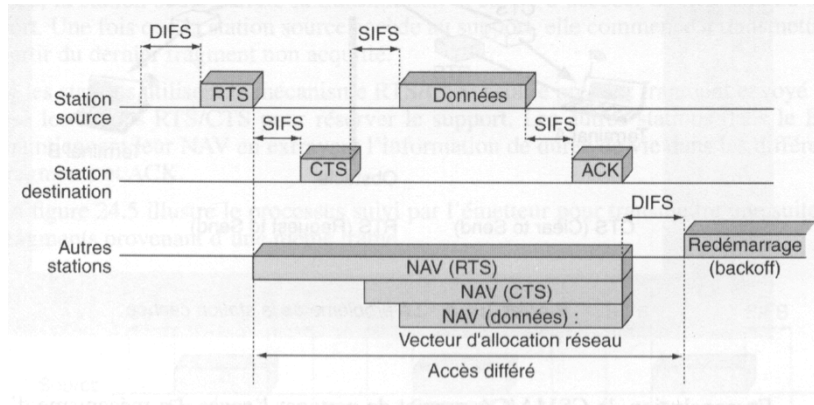
⇒ Réception de RTS:

Silence pendant la transmission de CTS+trame suivante

⇒ Réception de CTS:

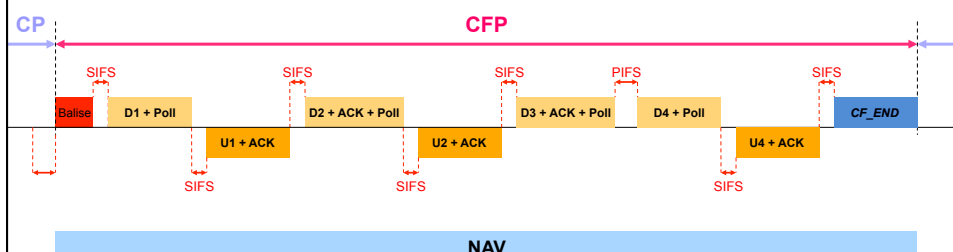
Silence pendant la transmission suivante

Exemple: RTS et CTS



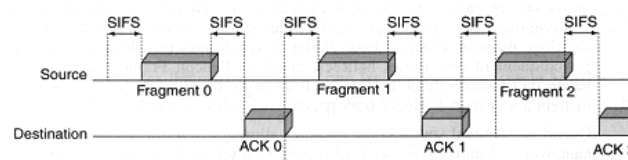
Méthode PCF

- Permet la transmission de données temps réel
- Principe
 - L'AP gagne accès au canal
 - L'AP interroge à tour de rôle toutes les stations



Fragmentation de trames

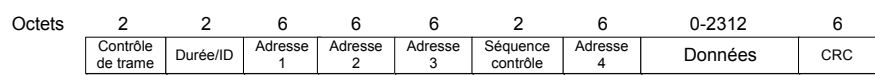
- Découpage d'une trame longue en plusieurs fragments
 - Diminue les données à retransmettre en cas d'erreur bit
- Principe
 - Les fragments sont transmis de manière séquentielle
 - Le support est libéré
 - après la transmission de tous les fragments ou
 - après une erreur de transmission d'un fragment
 - Après une erreur
 - La station regagne l'accès au canal
 - Retransmission à partir de la trame perdue



5. Réseaux locaux

153

Format de trame 802.11

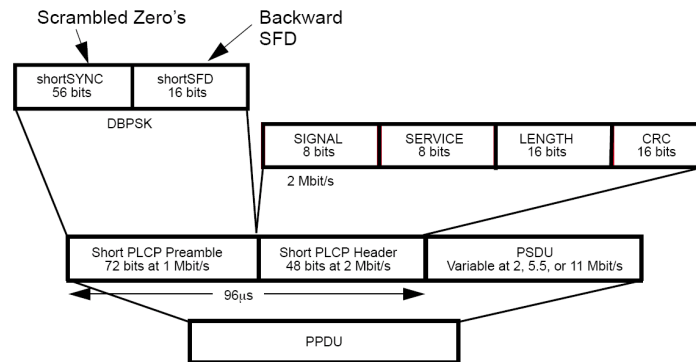


- Durée: contient le NAV de l'échange
- Adresses
 - 1: Destinataire (intermédiaire ou finale)
 - 2: Source (intermédiaire ou originale)
 - 3, 4: Varient selon la trame
- Données: jusqu'à 2312 octets

5. Réseaux locaux

154

Encapsulation des données MAC



- La couche physique ajoute également un en-tête
 - Préambule: 72 bits transmis à 1 Mb/s
 - En-tête PLCP: 48 bits transmis à 2 Mb/s

Exercice 70,83

Sécurité dans 802.11

- Le support de transmission est partagé
- Portée de la transmission non maîtrisée
- Problèmes potentiels
 - Utilisation non autorisée du réseau
 - Écoute clandestine des transmissions
 - Accès non protégé par des firewalls
- Solutions
 - Cryptage
 - Authentification des utilisateurs

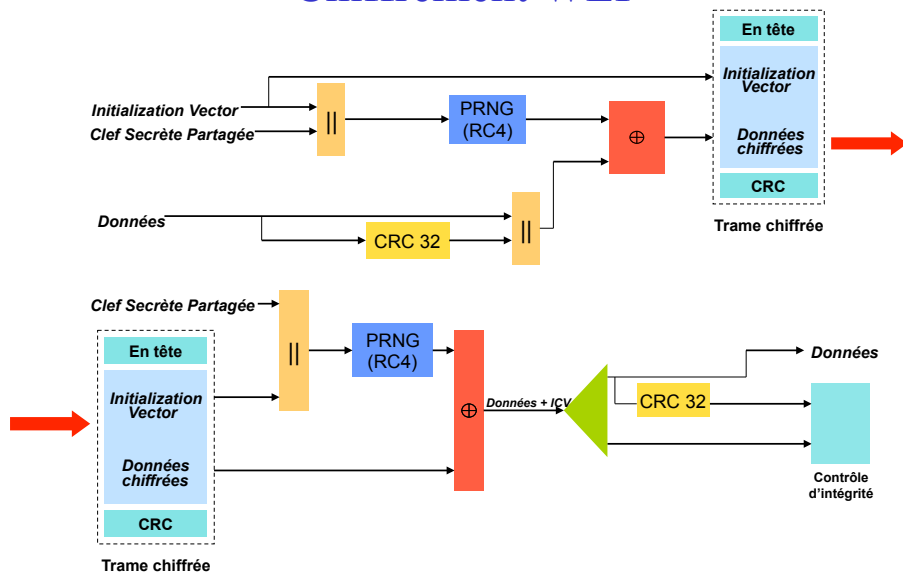
Protocole de sécurité original: WEP *Wired Equivalent Privacy*

- Objectif:
 - Utilisation simple !
 - Effort d'une intrusion similaire à un réseau sur câble
- Développé par de non-spécialistes en comité fermé
- Résultat:
- Problèmes majeurs :
 - Authentification faible: usurpation d'identité
 - Chiffrement faible: décryptage des données, récupération de la clé secrète.
 - Contrôle d'intégrité faible: modification, injection, reroutage des données

Cryptage dans WEP

- Utilise une **clé secrète partagée** (40 ou 104 bits), connue à la station et à l'AP
 - Interception de trames cryptées avec la même clé permettrait de deviner facilement le contenu
- Clé est concaténée avec un **Vecteur d'Initialisation** (IV) qui change pour chaque trame
- La clé résultante est utilisée pour générer un flot d'octets pseudo-aléatoires
- **XOR** du message et du flot d'octets produit le message crypté

Chiffrement WEP



Faibles de sécurité de WEP

Récupération de la clé secrète

- Le vecteur d'initialisation représente les premiers octets de la clé RC4
- Si l'on connaît les premiers octets de la clé RC4, on peut trouver le prochain octet à partir du premier octet de la séquence générée par RC4 (**IV faibles**)
- Algorithme utilisé par Aircsnort et WEPCrack

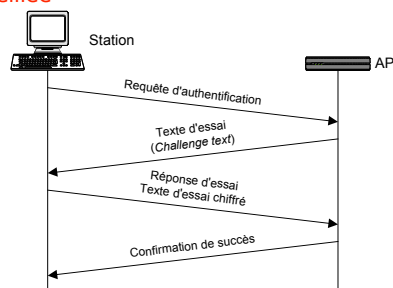
Modification clandestine du message crypté

- Le code CRC, prévu pour l'intégrité du message, est linéaire
- Si l'intrus modifie le message crypté, il peut calculer un CRC correct, sans savoir déchiffrer le message

Et beaucoup d'autres...

Authentification

- Deux possibilités
 1. *Open system authentication*
 - Aucune authentification explicite
 2. Authentification à l'aide de la clé secrète partagée (*Shared Key*)
 - **Déconseillée**



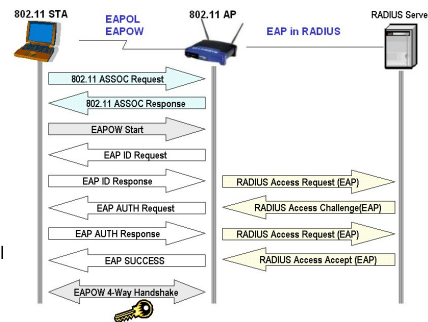
Améliorations de la sécurité WLAN

WEP+

- Solution ad-hoc des constructeurs (modification des drivers)
- Ne pas utiliser des IV faibles

802.1X

- Utiliser un serveur RADIUS pour authentifier chaque utilisateur
- L'accès au réseau reste bloqué jusqu'à l'authentification correcte
- Authentification par un mot de passe, un certificat, une smart-card, ...
- Création d'une clé de cryptage par session



Améliorations de la sécurité WLAN

WPA (Wi-Fi protected Access) (2003)

- Solution intermédiaire jusqu'à l'approbation de la norme 802.11i
- Sûre !
 - Authentification 802.1X
 - Home-networks sans serveur RADIUS
 - Authentification à l'aide d'un mot de passe (*Pre-Shared Keys*, PSK)
 - Nouveau protocole de chiffrement: TKIP (*Temporal Key Integrity Prot.*)
 - Clé de cryptage sur 128 bits
 - Une clé par utilisateur et par session
 - Distribution automatique des clés
 - Contrôle d'intégrité
 - Protocole MIC (Message Integrity Code, aka Michael) au lieu de CRC

Améliorations de la sécurité WLAN

Norme 802.11i (WPA2) (Juin 2004)

- **Compatible avec la législation internationale**
- **Produits seront compatibles avec WPA**
 - Remplace TKIP avec AES
 - Nécessite plus de puissance de calcul
 - Changement de hardware nécessaire

Conseils de sécurité

A la maison

- Utiliser WEP (mieux que rien)
- Utiliser WPA avec mot de passe partagé, si disponible

Au bureau

- Utiliser WPA/WPA2 avec un serveur d'authentification RADIUS si disponible, sinon
- Considérer le WLAN comme un réseau externe
 - Utiliser un VPN sur le WLAN
 - Protéger le réseau interne par un firewall

Exercice 87

HiperLAN 2

- Prévu comme technologie européenne
 - **Haut débit**: 54 Mb/s dans la bande de 5 GHz
 - Transmission **orientée connexion**
 - **Qualité de service** ->Transmission temps-réel
 - **Sécurité**
 - Authentification et cryptage basés sur DES ou 3-DES
 - **Itinérance** entre cellules possible
- Conception semble supérieure à 802.11 **MAIS**
 - Pas de soutien des grands fournisseurs américains
 - Soutien des fournisseurs européens diminue
 - **Avenir incertain pour HiperLAN**

802.16: WirelessMAN

- Organisation de certification: **WiMAX**
- Fournit un accès réseau sans fil à large bande
 - Alternative à ADSL / Câblemodem
 - Vise principalement des utilisateurs fixes !
 - L'utilisation mobile sera considérée dans les normes futures
 - N'est pas optimisé quant à la consommation d'énergie

État actuel

- Les premières normes sont approuvées
- Les premiers produits sont disponibles aux US
- L'Europe (la Suisse) va allouer des fréquences en 2005 (Swisscom a rendu sa bande en 2008)
- Quelques fréquences nécessiteront une licence de l'OFCOM

Comparaison WLAN - WMAN

	802.11	802.16
Utilisation principale	Ordinateurs mobiles	Ordinateurs fixes ou nomadiques
Portée	< 100 m	Typiquement 3 – 10 km
Nombre d'utilisateurs	< 10	Des centaines de récepteurs, avec un nombre illimité d'utilisateurs
Débit	Jusqu'à 54 Mb/s	Jusqu'à 100 Mb/s
Support de QoS	802.11e	QoS intégrée dans la couche MAC. Approprié pour la transmission multimédia
Prix d'un récepteur	< CHF 100	

Les différentes normes WiMAX

	802.16	802.16a	802.16e
Approbation	Déc. 2001	Janv. 2003	2005
Fréquences	10 – 66 GHz	2 – 11 GHz	2 – 6 GHz
Transmission	Visibilité directe (Line-of-Sight)	Sans visibilité directe (Non-Line-of-Sight)	Sans visibilité directe (Non-Line-of-Sight)
Débits	32 – 134 Mb/s dans un canal de 28 MHz	Jusqu'à 75 Mb/s dans un canal de 20 MHz	Jusqu'à 15 Mb/s dans un canal de 5 MHz
Portée typique	2 – 5 km	7 – 10 km (max. 70 km)	2 – 5 km
Utilisation	Fixe	Fixe	Mobile