Protocole de niveau 2

Non filaire

Généralité et exemples

Généralités

But : Communiquer avec différents systèmes sans utiliser de liaison filaire

Plusieurs normes concurrentes :

- IrDA,
- liaison hertzienne, GSM, GPRS, UMTS, LTE , 5G …
- 802.11, 802.15, 802.16,…

Chaque norme correspond à une application bien spécifique.

WLAN : Wireless Local Area Network *a été défini par*

WECA : Wireless Ethernet Compatibility Alliance

(3com, Apple, Compaq, Dell, Lucent Technologies, Nokia, ….)

Fréquences

Bande ISM : Industriel, Scientifique et Médical

VLF	LF	MF	HF	VHF	UHF	SHF	EHF	IR

9 kHz 30 kHz 300 kHz 3 MHz 30 MHz 300 MHz 3 GHz 30 GHz 300 GHz THz

VLF : Very Low Frequencies -> navigation maritime, sonar

LF : Low Frequencies -> aéronautique, radio grandes ondes

MF : Medium Frequencies -> 500Khz et 2182 Khz = S.O.S, entre 535 et 1705 khz= Radio OM

HF : High Frequencies -> 6,7 Mhz=ISM, radio-diffusion sur onde courte

VHF : Very High frequencies ->entre 174 à 223 Mhz=radio numérique,
entre 88 et 108 Mhz=radio FM, communication satellite LEO, trafic aérien

UHF : Ultra High Frequencies -> entre 470 et 694 Mhz=télé, entre 700 et 900 Mhz=téléphonie,
trafic aérien, 1600 Mhz=GPS, communication satellite LEO et MEO,
2400 Mhz = micro-onde

SHF : Super High Frequencies-> entre 5 et 5,7 Ghz = ISM, communication satellite

EHF : Extremely High Frequencies -> recherche spatiale

Généralités (1)

Objets communicants:

• Vers 1960, Création du port RS232 pour relier **deux** systèmes , un maître, un esclave

• Evolution logique vers le sans-fil, -> **IrDA**

•Pb : permet seulement la communication entre deux systèmes

•Evolution logique vers les ondes radio, -> Bluetooth v1.0 → Bluetooth v5.0

Norme :

802.15.1 : Bluetooth v1.0 ⇒ **WPAN** : Wireless Personal Area Network

802.15.2 : Amélioration de la norme pour l'interopérabilité

802.15.3 :WPAN, haut débit : Augmentation du débit et de la portée
(> 20 Mbps et 10m, BP : 2,4 Ghz)

802.15.4 : WPAN, faible débit pour réseau ZigBee ou 6LowPan
(< 250 kb/s)

Généralités (2)

Norme 802.16 alias Wimax:

- Réseau sans fil à large Bande
- Utilisation de la technologie BWA (Broadland Wireless Access)
- Débit jusqu'à 70Mb/s sur de grandes distances (20 km), BP de 2 à 11 Ghz
- Technique MIMO (Multiple Input/Multiple Output) -> plusieurs antennes en émission et en réception

Consortium WiMax

(*Worldwide Interoperability for Microwave Access)*

Définition de la norme 802.16a, b, i, ….m

But : au départ, relier les villages ne pouvant bénéficier de l'ADSL (Boucle Local Radio), puis 802.16d pour concurrencer Wifi/3G/4G.

La norme 802.16d est considérée comme norme autorisé 4G.

Jusqu'à présent, 2 licences WiMax par région + 1 nationale

- deux choisis par l'ARCEP (auvergne : Maxtel et Bollore)
- une appartenant à Altitude Telecom (racheté par Iliad (free))

Généralité (3)

- Wimax
  - Bollore a racheté de nombreuses régions pour assurer une diffusion sur la France (une licence par région)
  - Quelques offres existèrent → concurrente de l'ADSL ou de la 4G
    - Mais très concurrencé par la fibre, et obsolète par rapport à 5G
  - Débit allant de 2 à 70 Mb/s
    - Tarif environs 40 €/mois (max 10 Go consommation)
- Fin Wimax Français
  - → bande passante rendue de 3410 à 3490 Mhz
  - Redistribution en 2026… vers la 5G

Protocole de niveau 2

Non filaire

LE WIFI

La norme 802.11

La norme **802.11** définit la couche 1 et 2 pour une liaison sans fil utilisant des ondes électromagnétiques :

- La couche physique
  - codage DSSS, FHSS, IrDA
- La couche Liaison de données
  - couche LLC et couche MAC

Cette norme permet d'avoir un débit de 1 ou 2Mb/s et elle utilise un accès au médium par compétition (méthode CSMA/CA)
(CA : Collision Avoidance)

Mais, évolution de cette norme

Wi-Fi (Wireless Fidelity)

Wi-Fi

Nom norme	Nom	Description
802.11a	Wifi 2	Débit : 54Mb/s, 8 canaux radio dans la bande de fréquence des 5 Ghz.
802.11b	Wifi 1	Débit : 11Mb/s, portée 300m, 3 canaux radio dans la bande de fréquence des 2,4 Ghz
802.11c	Pontage	Etablissement d'un pont pour la norme 802.11d
802.11d	International	Etablit les règles à respecter entre les différents pays pour transporter les données 802.11
802.11f	Roaming	Interopérabilité entre les différents points d'accès pour permettre l'itinérance (définition de l'IAPP)
802.11g	Wifi 3	Débit : 54MB/s, portée 300m, compatible avec 802.11b
802.11i	WPA2	Amélioration de la sécurité pour les normes a, b et g.
802.11n	Wifi 4	Débit max : 300 Mb/s, bande fréquence 2,4 ou 5Ghz
802.11ac	Wifi 5	Débit 1gb/s, Bande fréquence 5 Ghz
802.11ax	Wifi 6	Débit 10gb/s, Bande fréquence entre 2,4, 5 et 6 Ghz
802.11be	Wifi 7	Débit 25 gb/s, Bande fréquence entre 2,4, 5 et 6 Ghz, personne presque fixe
802.11bn	Wifi 8 (2028)	Débit 100 gb/s, Bande fréquence entre 2,4, 5 et 6 Ghz

Topologies

- **Mode Infrastructure (ou hotspot)**

  le plus courant

• Au minimum , **1 AP** + postes sans fil

BSS : Basic Service Set

- identifié par un BSSID (abrégé en SSID -> Service Set Identifier)

- **Mode Ad-Hoc**

• Aucun AP, que des postes sans fil

IBSS : Independant Basic Service Set

- identifié par un SSID

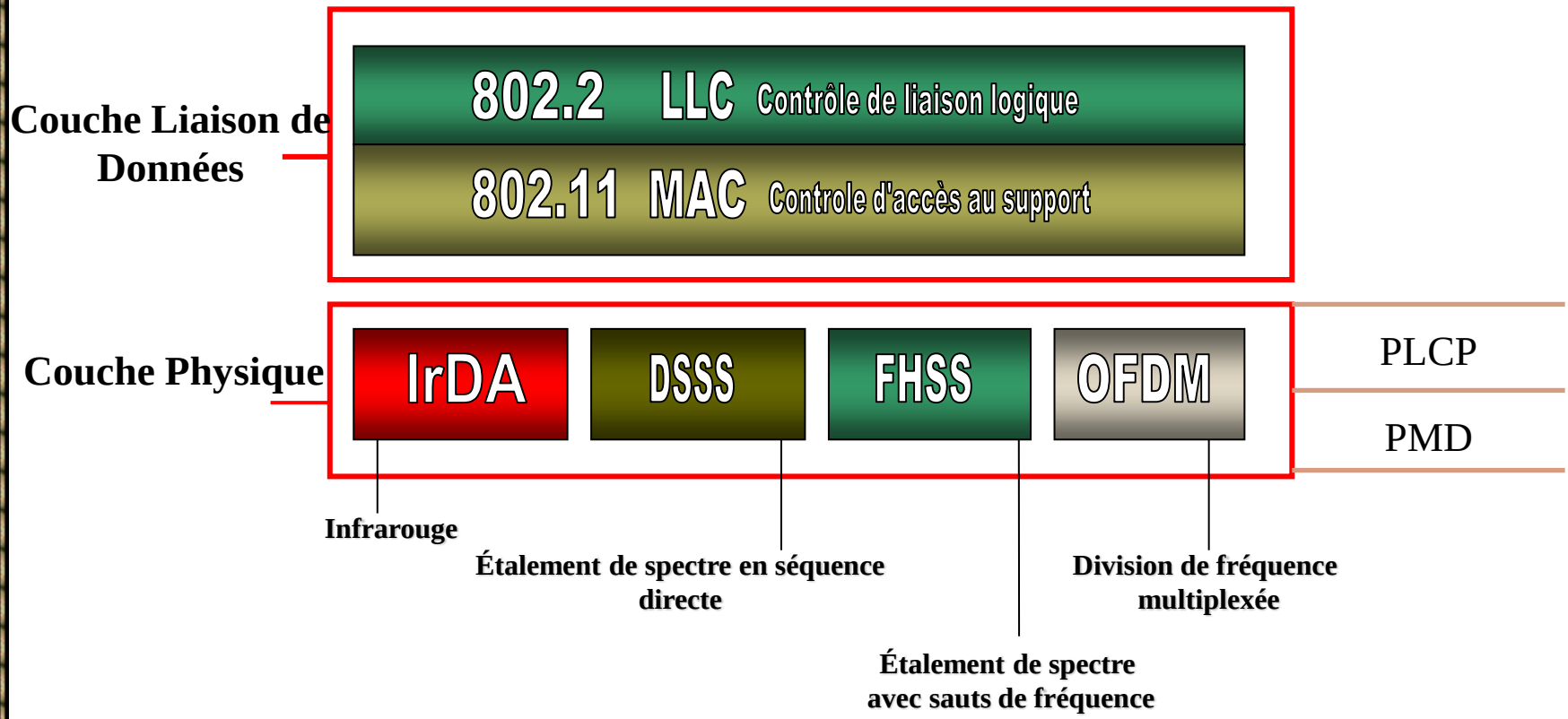
Tout le monde doit voir tout le monde
ou
Pc configuré comme routeur

Architecture en couches

- **WiFI**

PLCP : Physical Layer Convergence Procedure

PMD : Physical Medium Dependant



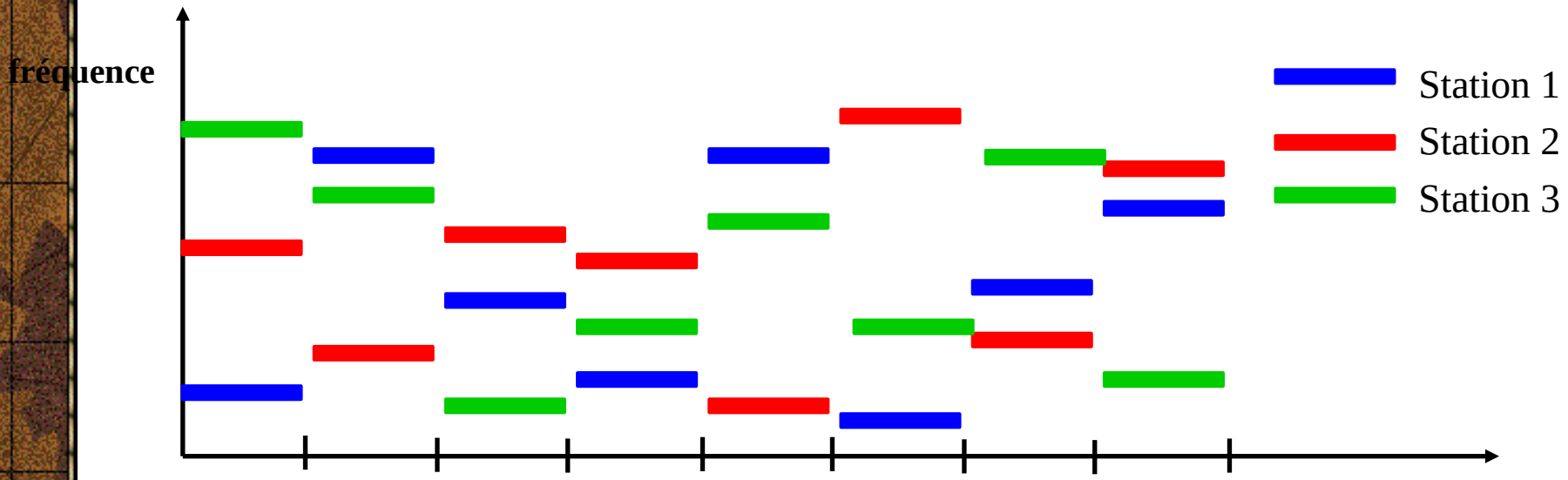
Physique -FHSS

- **FHSS : Frequency Hoping Spread Spectrum**

  • Découpage de la bande de fréquence en 79 canaux de 1 Mhz, puis transmission en utilisant une combinaison de canaux connue de toutes les stations (78 combinaisons possibles)

  • Emission sur un canal pendant 400ms, puis changement de canal,etc…

  • Bande de fréquence entre 2,4 Ghz et 2,4835 GHz



Physique - DSSS

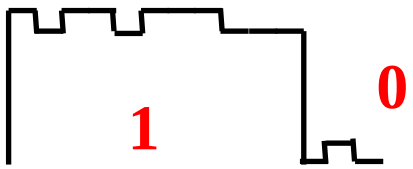
- **DSSS : Direct Sequence Spread Spectrum**
  - Découpage de la bande de fréquence en 14 canaux de 22 Mhz, mais recouvrement des canaux -> utilisation des canaux 1, 6 et 11

Canal	1	2	3	4	5	6	7
Fréquence (Ghz)	2,412	2,417	2,422	2,427	2,432	2,437	2,442
Canal	8	9	10	11	12	13	14
Fréquence (Ghz)	2,447	2,452	2,457	2,462	2,467	2,472	2,483

Pour éviter les collisions, on utilise le « chipping », c'est à dire faire une petite modulation pour faire apparaître plusieurs bits (*séquence barker* ,11 bits) lorsque l'on émet un seul bit

➡ redondance de l'information

bit 1 = 10110111000, bit 0 = 01001000111



Physique - OFDM

- **OFDM : Orthogonal Frequency Division Multiplexing**

  - Basé sur les différentes fréquences utilisées (2,4 Ghz , 5 Ghz, …)
  - Division du canal principal en sous canaux utilisés en parallèle
  - Un canal principal de x Mhz est divisé en y canaux de 300 Khz
  - Modulation différente pour chacun des canaux.

  - Très utilisé pour le 802.11a, ac
    norme a :8 canaux de 20 Mhz entre 5,15 Ghz et 5,35 Ghz
    norme ac : 8 canaux de 80 Mhz entre 5,17 Ghz et 5,83 Ghz

  Utilisation de la norme **OFDMA** (… Multiple Access) pour le 802.11ax
  Déjà présent dans la 5G

Couche liaison de données

La couche MAC

- Similaire à la couche Mac Ethernet (compatibilité)
- ***Fonctionnalité***
  - Contrôle d'accès au support
  - Contrôle d'erreur par CRC
  - Fragmentation et réassemblage
  - *Gestion de l'énergie*
  - *Gestion de la mobilité*
- ***Deux méthodes d'accès pour le 802.11a, b, g***
  - **DCF** (Distributed Coordination Function) : utilisation pour les données asynchrones, collisions possibles
  - **PCF** (Point Coordination Function) : utilisation pour les données synchrones, pas de collision.

Distributed Coordination Function

◆ DCF

• **Basé sur un accès CSMA/CA**

Pour émettre :

- On écoute le support (ondes)
- Si libre pendant un temps donné (*DIFS*, Distributed Inter Frame Space)

-> transmission d'une trame Ready To Send (RTS) contenant les informations sur le volume de données et la vitesse de transmission (optionnel)

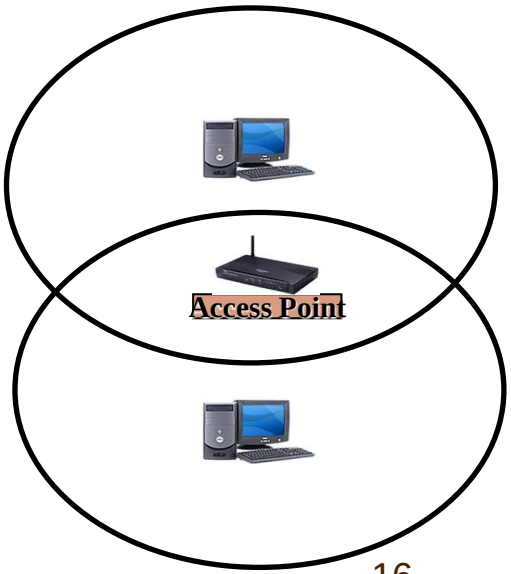
-> réception d'un Clear To Send (CTS) (optionnel)

-> envoie des données

-> récupération d'un ACK pour chaque trame

Une station qui veut émettre doit attendre la libération du support.

(NAV : Network Allocation Vector)



Un ACK pour chaque trame car

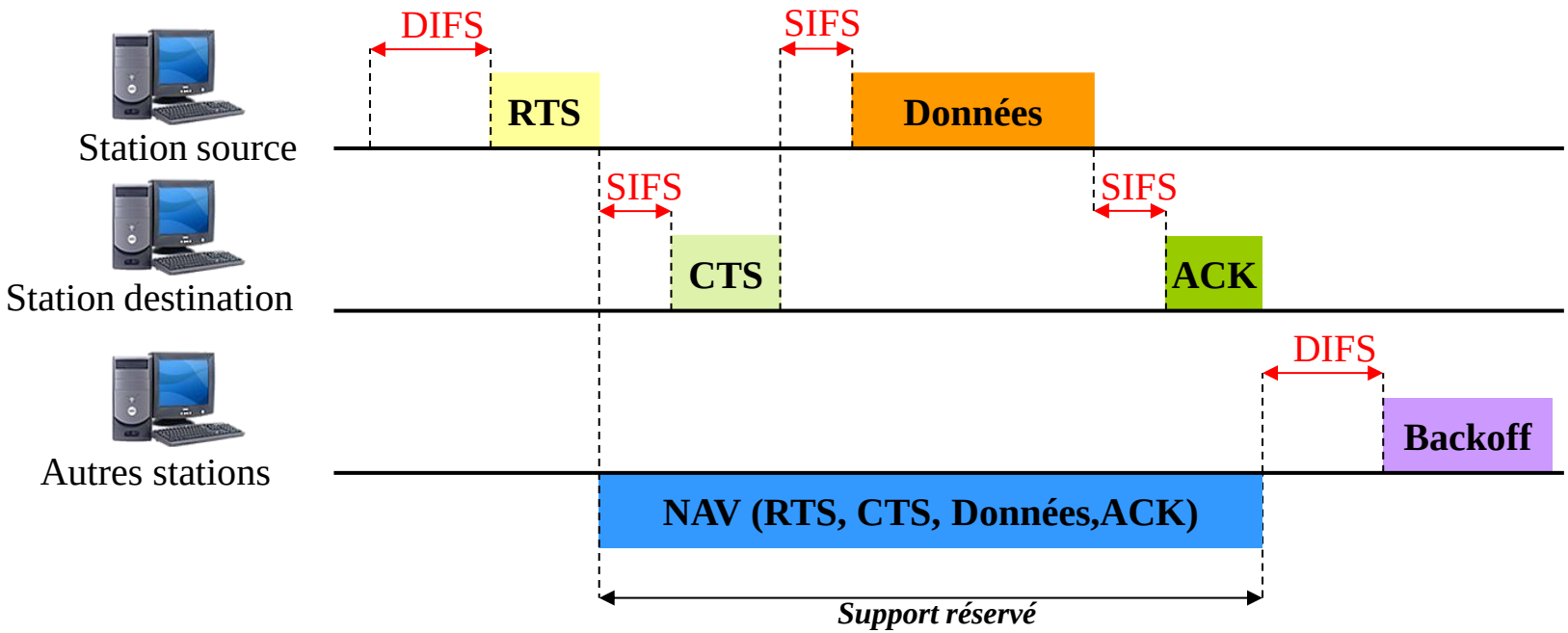
2 stations peuvent vouloir émettre en même temps sans se voir.

Distributed Coordination Function

◆ DCF

• *Exemple de dialogue*

SIFS : Short Inter Frame Space < **PIFS** : Prioritary < **DIFS** < **EIFS** (Extented)



Backoff : temps d'attente aléatoire pour que toutes les stations n'émettent pas en même temps.

Les Trames WiFI (1)

- **3 types de trames**
  - Trames de *données*
  - Trames de *contrôle* (RTS, CTS, ACK)
  - Trames de *gestion*

- **Structure d'une trame WIFI:**

PLCP : Physical Layer Convergence Procedure
-> renseigne sur la composition de la trame

Le préambule et le PLCP varie en fonction de l'interface physique utilisée
(FHSS, DSSS, IrDA, OFDM, OFDMA)

Les Trames WiFI (2)

- **Couche MAC pour les trames de données**

Contrôle de trame 2 octets	Durée/ID 2 octets	Adresse 1 6 octets	Adresse 2 6 octets	Adresse 3 6 octets	Séquence 2 octets	Adresse 4 6 octets

Corps de la trame 0 à 2312 octets	CRC 4 octets

Contrôle de trame

Version (2 bits)	Type (2 bits)	Sous-Type (4 bits)	To DS (1 bit)	From DS (1 bit)	More Frag (1 bit)	Retry (1 bit)	Power Mgt (1 bit)	More Data (1 bit)	WEP (1 bit)	Order (1 bit)

Version : actuellement, 00
Type : 3 types, plusieurs sous-types (00 : gestion, 01:contrôle, 10 : données)
To DS ou From DS : trame vers ou en provenance du système de distribution
More fragment : 1, trame fragmentée et pas dernier fragment, 0 sinon
Retry : 1 , retransmission
Power management : 1 , économie d'énergie, 0 actif
More Data : 1 si d'autres données à faire parvenir à la station
WEP : trame chiffrée ou non
order : Trame ordonnée ou non

Les Trames WiFI (3)

◆ Couche MAC pour les trames de données

Champ « *durée/ID* » : identifiant pour des trames polling de contrôle, ou durée pour calculer le NAV

Champ «*Adresse* » : même format que les adresses Mac (6 octets)

- DA : Destination Adresse : destination de la trame : individuelle ou groupe
- SA : Source Adresse : source de la trame : individuelle
- RA : Receiver Adresse : réception des données : Point d'accès récepteur
- TA : Transmitter Adresse : transmission des données : Point d'accès émetteur
- BSSID : soit adresse MAC de l'AP, soit @MAC du IBSS.

To DS	From DS	Adresse 1	Adresse 2	Adresse 3	Adresse 4	
0	0	DA	SA	BSSID	Aucune	Ad-hoc
0	1	DA	BSSID	SA	Aucune	
1	0	BSSID	SA	DA	Aucune	Normal
1	1	RA	TA	DA	SA	Entre 2 PA

Champ « *contrôle de séquence* » : numérotation des trames

Les Trames WI-FI (4)

- **Couche MAC pour les trames de contrôle**

Trame RTS

Contrôle de trame 2 octets	Durée 2 octets	RA 6 octets	TA 6 octets	FCS 2 octets

Trame CTS

Contrôle de trame 2 octets	Durée 2 octets	RA 6 octets	FCS 2 octets

Trame ACK

Contrôle de trame 2 octets	Durée 2 octets	RA 6 octets	FCS 2 octets

La Sécurité (1)

- **Les types d'attaque :**
  - Ecoute passive ou active → permet l'interception de données
  - ➡ facile à réaliser car les données sont émises dans un rayon, difficilement détectable
  - Intrusion réseau (intrusion, usurpation) par les employés, par virus,…
  - Le brouillage radio (facilement détectable, mais très efficace)
  - Les dénis de services
  - Attaque Man In the Middle via ARP spoofing, ARP poisoning…

La Sécurité (2)

Les contres mesures

- Limiter la puissance d'émission des bornes si possible
  éviter d'arroser le quartier
- Désactivation des services d'administration disponible (passwd admin) ou fermeture de port pour limiter les accès
  changement des mots de passes par défaut
- Changement de SSID par défaut (attribution d'un SSID)
  mais transmis en général par AP ou en méthode Ad-Hoc ➔ Pb
- Désactivation du Broadcast du SSID
  mais visible dans les trames lors de l'association
- Filtrer les adresses MAC : utilisation des ACL (Access LISTS) des clients RLAN au niveau des bornes d 'accès
  mais possibilité de « voler » une adresse MAC (MAC Spoofing)
- Chiffrer les données (avec un bon cryptage…)

La Sécurité (3)

Couche MAC pour la sécurité

Le cryptage

- Utiliser un chiffrement pour les données

- l ’implémentation **WEP** (Wired Equivalent Privacy) (clé sur 40 bits / 104 bits) donnée par les utilisateurs auquel est rajouté un vecteur d'initialisation (24 bits).

Fonctionnement : chiffrement RC4 en utilisant clé + vecteurs d’initialisation (IV)

message envoyé = (M.c(M)) xor RC4(IV . K)

{ c(M) = cheksum de M et K = clé
{ le RC4 donne des séquences pseudo-aléatoires

Le vecteur d'initialisation change à chaque trame envoyée, on lui rajoute 1

(assez facilement crackable si on connaît le 1er octet de M et IV)

Pb : faiblesse d’implémentation dans IV commencent à 0 puis incrémentés de 1 à chaque envoi, vecteurs faibles ….

Actuellement, quelques dizaines de minutes pour cracker clé WEP 128 bits

Si utilisation de WEP, alors codage supplémentaire : ssl, Ipsec, ssh,…

La Sécurité (4)

Couche MAC pour la sécurité

Le cryptage (suite) → utilisation de la norme 802.11i (2003)

- Utiliser la norme 802.1x (WPA : Wifi protected Access ou WPA2)

=> concerne spécifiquement l'authentification

- 3 acteurs :
  - -> le client (demandeur ou supplicant)
  - -> le point d'accès relais (NAS : Network Access Server)
  - -> le serveur d'authentification = serveur RADIUS

codage en utilisant les trames EAP : Extensible Authentication Protocol

- Pour le chiffrement : remplacement de WEP par TKIP

Temporal Key Integrity Protocol (changement de clé souvent)

(cela ne sert à rien de décrypter une clé si elle n'est plus utilisée)

WPA2 : basé sur CCMP (Counter-Mode/CBC-Mac protocol) avec utilisation du chiffrement AES (2004)

WPA3 (2018) : augmente longueur clé et négociation de départ.

Le roaming

- **But** : permettre à un appareil sans fil qui se déplace de rester connecté
  - protocole IAPP : Inter-Access Point Protocol (norme 802.11F)
    -Utilisation de 4 ou 5 trames pour changer de AP
    - Pb : aucune sécurité

Latence trop longue lors d'une authentification 802.1X

Nouvelle norme : 802.11r

Fast Basic Service Set Transition

idée : les clés de chiffrement sont mises en cache dans les AP

→ gain de temps

Mobilité dans les réseaux sans fils

Les réseaux MANET

Les réseaux mobiles Ad Hoc (1)

Définition:

Un réseau mobile ad hoc, appelé généralement **MANET** (Mobile Ad hoc NETwork), consiste en une grande population, relativement dense, d'unités mobiles qui se déplacent dans un territoire quelconque et dont le seul moyen de communication est l'utilisation des interfaces sans fil, sans l'aide d'une infrastructure préexistante ou administration centralisée.

Un réseau ad hoc peut être modéliser par un graphe G = (V,E)

où - V représente l'ensemble des nœuds et

- E l'ensemble des connections qui existent entre ces nœuds.

But : Faire communiquer deux nœuds distants en passant par un ou plusieurs intermédiaires

Application : aéroport, sécurité routière, randonnée …

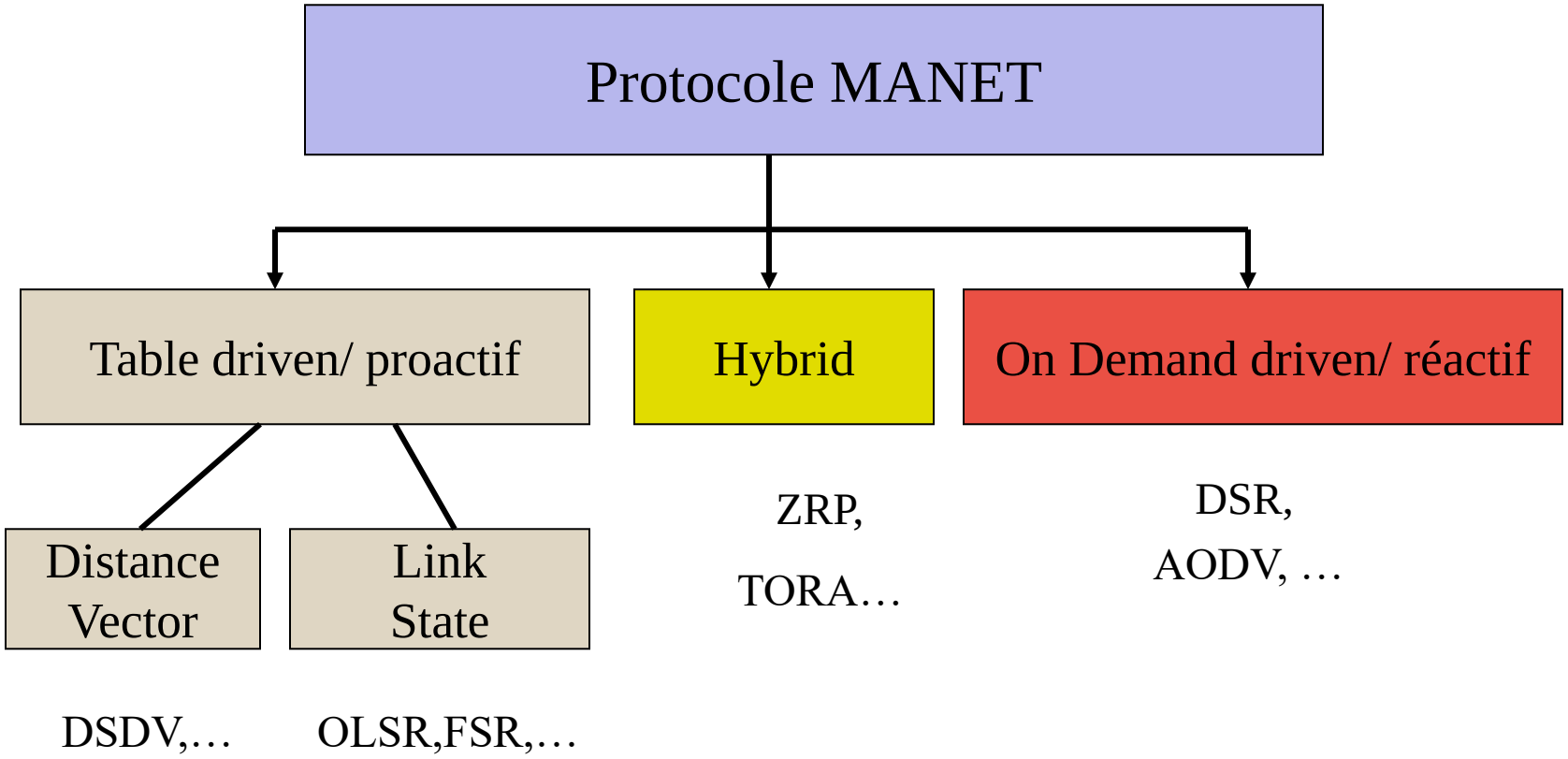
Les réseaux mobiles Ad Hoc (2)

- Caractéristiques :
  - Topologie dynamique
    - c'est le but, permettre aux ordinateurs de bouger, donc changement continu de la topologie.
    - impossible de savoir si un ordinateur sera encore joignable dans les minutes suivantes.
  - Bande passante limitée /débit limité
    - du fait du partage de la bande passante
  - Contraintes énergétiques
    - mouvement ➔ utilisation batterie…
  - Absence d'infrastructure
  - Sécurisation des données
    - problème au niveau physique (inondation, dispersion,…)

Communication dans réseaux MANET

- Objectifs :
  - Minimiser la charge réseau
    - Eviter les boucles
    - Eviter la concentration du trafic en un point
    - Eviter de surcharger les entêtes des trames ou des paquets
  - Effectuer des communications multipoints fiables
  - Assurer une route optimale
  - Optimiser le temps de latence
    - De nombreux protocoles utilisent un timer pour gérer leurs envois de données → problème si latence trop longue

Classification



Communication : *envoyer des données d'un ordinateur vers un autre ordinateur en passant par d'autres ordinateurs….*

OLSR (1)

- Optimized Link State Routing
  - Algorithme proactif
  - Basé sur un algorithme d'état de lien "optimisé"
    - Gestion des relais multipoints (MPR : MultiPoint Relay)
  - Protocole ratifié par l'IETF
    RFC 3626, 7181
  - Utilise plusieurs tables :
    - Table de voisinage
    - Table de topologie du réseau
    - Table de routage

OLSR (2)

Découverte du voisinage

- Envoie de trames HELLO périodique
- 4 sortes de lien
  - lien symétrique
  - lien asymétrique
  - lien MPR
  - lien perdu → plusieurs trames "hello" sans réponse

→ Un lien sera considéré comme fiable s'il est symétrique

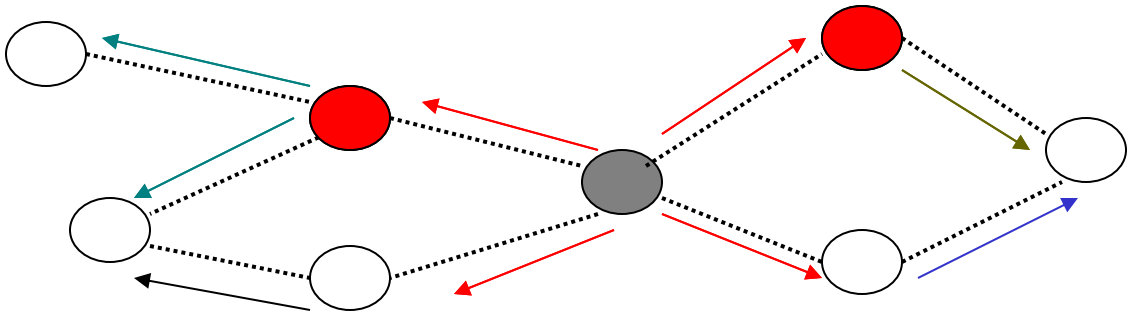
4 échanges pour avoir lien symétrique :

- A envoie une trame Hello vide (on découvre)
- B répond avec une trame Hello asymétrique (B entend A)
- A répond avec une trame Hello symétrique
- B répond avec une trame Hello symétrique

OLSR (3)

- Les relais multipoints (MPR)
  Chaque nœud envoie à tous ces voisins sa table de voisinage.
  - Permet de remplir la table de topologie
  - Permet à un nœud de connaître la liste des stations se trouvant à 2 sauts

- But des relais multipoints : minimiser le nombre de transmission pour que tous les voisins de second niveau reçoivent l'information.
  (une station peut-être visible par plusieurs nœuds)



lien symétrique

SANS MPR → 5 retransmissions

AVEC MPR → 3 retransmissions

OLSR (4)

- Table de « routage »
  (pour joindre les autres ordinateurs)
  - création identique à un algorithme d'état de lien
    - utilisation table de voisinage, bd topologique et SPF.
    - utilisation des liens stables

- Bilan
  - **Table de routage complète en permanence**
  - Trames de contrôle qui transitent sur le réseau
  - Problème énergétique possible sur certains nœuds
  - Utilisé par d'autres protocoles IOT

AODV (1)

- Ad Hoc On –Demand Distance Vector
  - Basé sur l'algorithme de Bellman-Ford
    - vecteur de distance, mais en évitant les boucles
  - Protocole normalisée par l'IETF
    RFC 3561
  - **Protocole réactif**
    - supporte l'unicast et le multicast
    - Plutôt développé pour les liens symétriques
    - 2 fonctions : la découverte des routes
      la maintenance des routes

AODV (2)

- Table de « routage »
  - Elle contient :
    - l'adresse IP de destination
    - Le nombre de sauts (de nœuds) nécessaire pour atteindre la destination
    - L'adresse IP du prochain saut
    - Le numéro de séquence qui correspond à cette destination
    - Le temps d'expiration de l'entrée de la table
    - La liste des précurseurs

Une destination D est rajoutée dans la table de routage seulement lorsque la station veut envoyer un message à D

→ temps d'expiration arrive à 0 → élimination de la destination

AODV (3)

Découverte d'une route

- **Broadcast** d'un paquet ROUTE REQUEST *(requête de route)* avec la destination D
  - Ce paquet contient :
    - un numéro de broadcast (RREQ ID)
    - l'adresse de la source (initiateur de la demande)
    - l'adresse destination
    - le n° séquence correspondant à la dernière fois que cette destination était dans la table de routage
      (si jamais, n° séquence = 0 et flag = U)
    - le n° séquence à utiliser actuellement pour le retour

Si pas de retour avant NET_TRAVERSAL_TIME, n° de broadcast est incrémenté de 1, et une RREQ est relancée

un seul n°broadcast par station (pour toutes les destinations)

AODV (4)

Réception d'une RREQ

- Si destination,
  - Vérification si (n° RREQ, id_source) n'a pas été déjà reçu
  - mise à jour de sa table de routage
    - insertion du chemin vers le destinataire
    - mise à jour du n° séquence,
    - mise à jour du temps d'expiration, …
  - Renvoie d'une Route Reply (RREP) en unicast

- Si nœud intermédiaire,
  - vérification si (n° RREQ, id_source) n'a pas été déjà reçu
  - cas 1 : Pas de route disponible vers destination D
    - Mise à jour de la table de routage pour le retour (on suppose les liens symétriques)
    - Diffusion de la demande en ajoutant 1 au nombre de saut

AODV (5)

- cas 2: route disponible vers la destination D
  - Vérification du n°séquence de l'ancienne route (stocké dans le paquet RREQ) < n° séquence de la route trouvée dans la table de routage
  - Renvoie d'une Route Reply en unicast avec le nombre de saut correspondant à la distance jusqu'à destination
  - Mise à jour de la liste des prédécesseurs pour cette destination

➡ **Mais, il faut avertir la destination qu'un nœud cherche à le joindre (car autrement table de routage incomplète)**

Bilan :

- La table de « routage » est construite au moment où le besoin est là
- Pas de trafic de contrôle
- Problème pour les protocoles ayant des timers… (TCP)
- Bonne gestion d'énergie