

802.11

II. Formats de trames

RÉSEAUX & TÉLÉCOMS - Cours avec 129 exercices corrigés 2è édition page 534

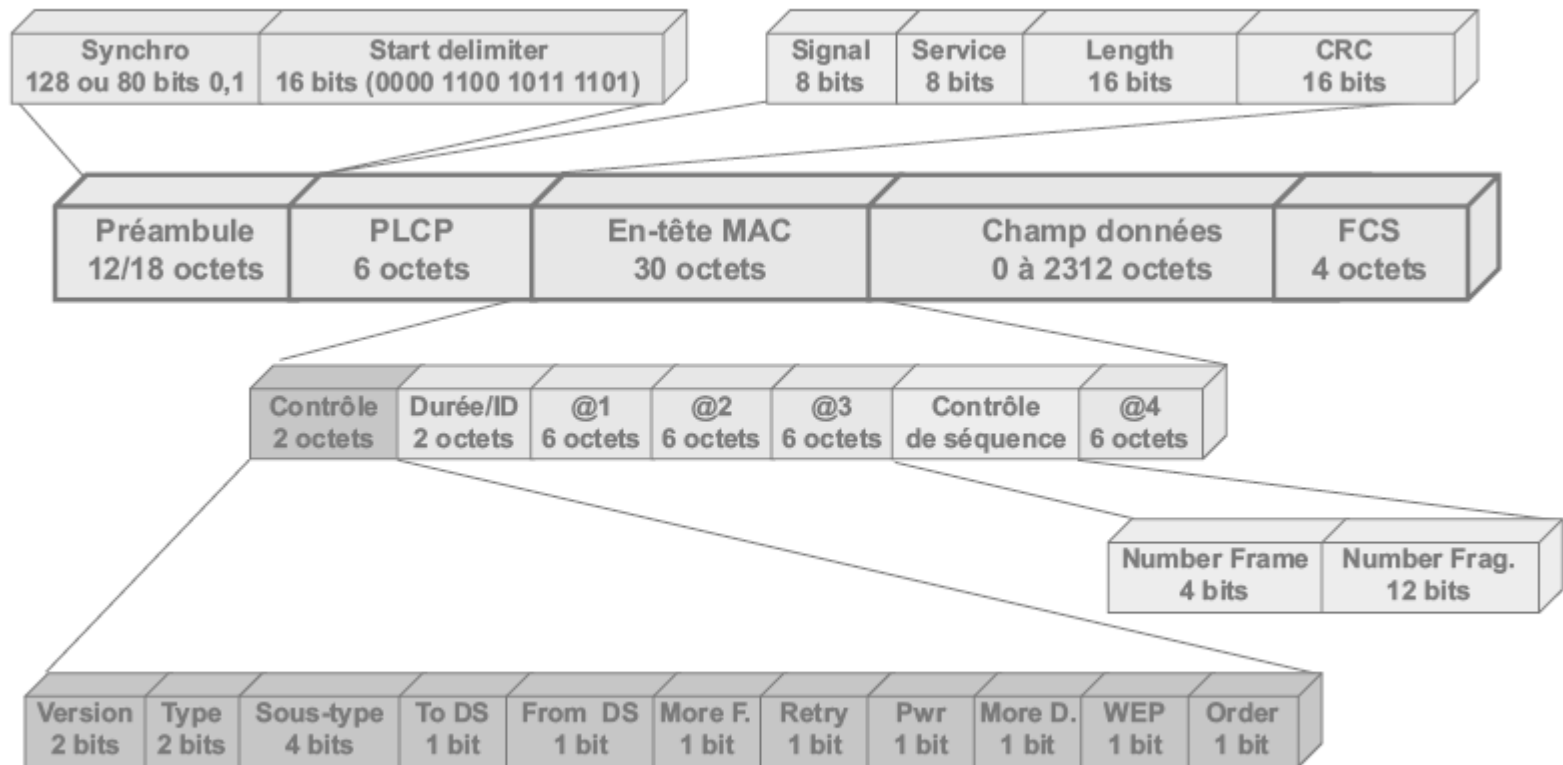
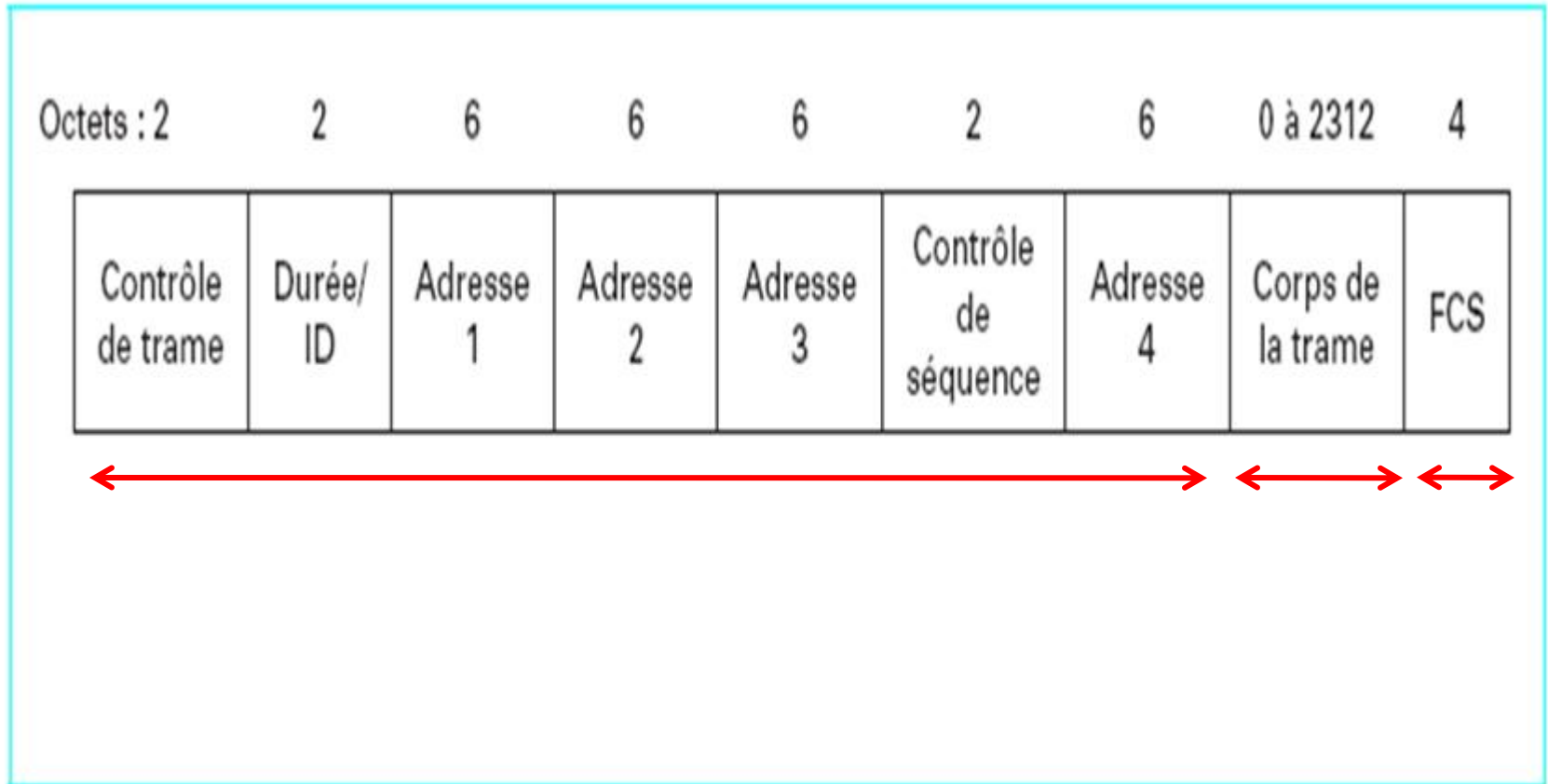


Figure 17.55 Trame MAC 802.11.

Format général d'une trame de données



En-tête MAC

- Le champ « contrôle de trame » contient des données telles que le protocole utilisé et le type de trame transmise.
- « durée/ID » il indique la durée d'utilisation du canal, et permet le positionnement du NAV (*Network Allocation Vector*). Cette valeur est dépendante du débit de la couche physique.
- Les champs « adresse » contiennent respectivement :
 - l'adresse du destinataire des données contenues dans le corps du paquet transmis ;
 - l'adresse de la source des données contenues dans le corps du paquet transmis;
 - l'adresse de la station à laquelle cette trame est envoyée (utile lorsque la trame doit transiter par des relais avant d'atteindre sa destination) ;
 - l'adresse de la station expédiant la présente trame (utile lorsque cette station est une station relais).

En-tête MAC

- Le sous-champ **Contrôle de séquence** assure la numérotation des trames émises (*Number frames*). Le second sous-champ (*Number fragment*) est utilisé par le destinataire pour assurer le réassemblage des différents fragments.

En-tête MAC

- Le champ *FCS Frame Check Sequence* contient un code détecteur d'erreur. CRC (*Cyclic Redundancy Code*) servant à la détection des erreurs de transmissions.
- *4 octets*
- **Exposé** : code détecteur d'erreurs pour la trame MAC 802.11 principe et évolution.

En-tête MAC

- Le corps de la trame contient l'LLC Protocol Data Unit (PDU)_{WS}
- Taille variable 0 à 2304 (+8 pour le WEP, ou +20 pour le TKIP, ou +16 pour l'AES)

Frame Control

Version		Type		Sous-type			
2 bits		2 bits		4 bits			
toDS	fromDS	Frag	Retry	Sleep	More	WEP	Order
1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit

Frame Control

- **Version** du 802.11 utilisée : pour l'instant, il s'agit toujours de 0.
- **Type** : type du paquet.
 1. paquet de gestion 00
 2. paquet de contrôle 01
 3. paquet de données 10
- **Sous-type**: ...
- **toDS et fromDS**: ils servent à indiquer si le paquet s'adresse au système de distribution (toDS) et s'il en provient (fromDS).

L'utilisation des champs Adresses.

Mode de fonctionnement	To Ds	From Ds	@1	@2	@3	@4
Mode ad-hoc	0	0	DA	SA	BSSID	0
Infrastructure message AP vers station	0	1	DA	AP	SA	0
Infrastructure message de la station vers l'AP	1	0	AP	SA	DA	0
Infrastructure message d'un AP vers un autre AP WDS	1	1	AP suivant	AP	DA	SA

DA (*Destination Address*) : adresse MAC Destination

SA (*Source Address*) : adresse MAC Source

AP (*Access Point*) : adresse MAC de l'AP (BSSID de la cellule)

BSSID (*Basic Service Set Identifier*)

WDS (*Wireless Distribution System*)

Frame Control

- **Frag** : indique s'il reste encore des fragments après ce paquet. 1 more fragment et 0 le dernier. Si la trame n'est pas fragmenté 0.
- **Retry** : indique est ce paquet est une nouvelle tentative d'émission d'un paquet déjà envoyé précédemment, mais qui n'a pas reçu d'ACK en réponse.
- **Sleep** : indique si la station sera en mode d'économie d'énergie (PSM) ou non, après ce paquet.

Frame Control

- **More** : en mode économie d'énergie, ce bit est positionné par le point d'accès pour indiquer qu'il dispose encore de données à transmettre après la trame en cours. Ceci évite que la station ne passe en mode sommeil après réception de la trame en cours ;

Frame Control

- **WEP** :indique si ce paquet est crypté avec WEP ou non.
- **Order** : indique que l'émetteur souhaite que ce paquet appartienne à la « classe de service strictement ordonné ». Les paquets appartenant à cette classe doivent toujours être relayés dans le même ordre qu'ils ont été reçus.

Les types de trames

- 1. les paquets de gestion (type 0) sont échangés comme des paquets de données, mais ils servent purement à la couche MAC et ne sont pas « remontés » aux couches réseaux supérieures. Ils mettent en œuvre certaines fonctions du WiFi telles que l'association, l'authentification, les balises, etc. ;**
- 2. les paquets de contrôle (type 1) sont émis, comme leur nom l'indique, pour contrôler les communications et permettre un bon partage des ondes ;**
- 3. les paquets de données (type 2) transportent les paquets fournis par les couches réseaux supérieures.**

Trames de gestion, contrôle et données

Contrôle

Gestion

Sous-type	Description
0	Requête d'association
1	Réponse d'association
2	Requête de réassociation
3	Réponse de réassociation
4	Requête de sondage
5	Réponse de sondage
6-7	Inutilisés
8	Balise
9	ATIM
10	Désassociation
11	Authentification
12	Désauthentification
13-15	Inutilisés

Sous-type	Description
0-9	Inutilisés
10	PS-Poll
11	RTS
12	CTS
13	ACK
14	CF-End
15	CF-End et CF-ACK

Donnée

Sous-type	Description
0	Données (c'est-à-dire un MPDU)
1	Données et CF-ACK
2	Données et CF-Poll
3	Données, CF-ACK et CF-Poll
4	Paquet vide (sans données)
5	CF-ACK
6	CF-Poll
7	CF-ACK et CF-Poll
8-15	Inutilisés

Trame d'acquittement

Octets : 2

2

6

4

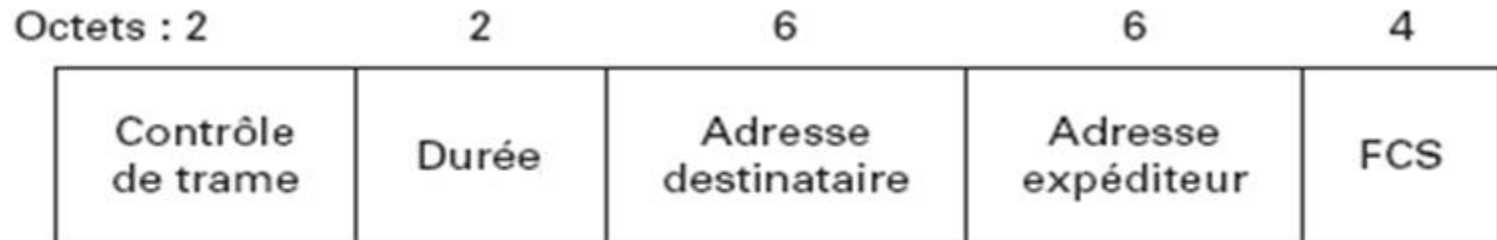
Contrôle de trame	Durée	Adresse destinataire	FCS
----------------------	-------	-------------------------	-----

Trame d'acquittement

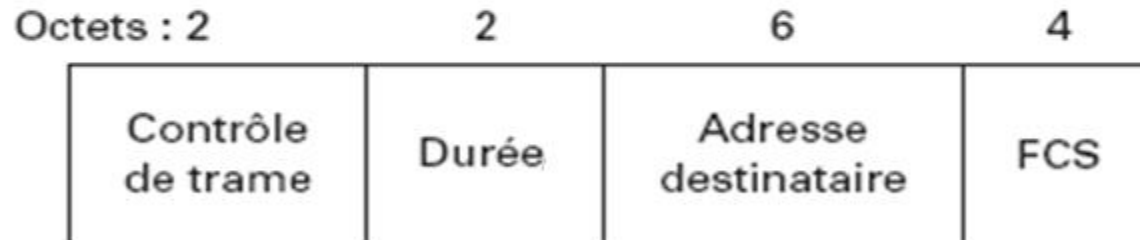
ACK-Frame

- Même champ de Contrôle du format général d'une trame 802.11.
- Dans la trame ACK, le champ **adresse destination** est la recopie du champ @2 de la trame précédente (**adresse source**).
- *FCS : détection* des erreurs de transmissions.

Trames RTS et CTS



Trame RTS



Trame CTS

Frames RTS/CTS

- Même champ de Contrôle du format général d'une trame 802.11.
- Dans la trame RTS le champ **Durée** contient en μ s la durée totale de l'échange (Données et CTS).
- Le champ Durée de la trame CTS correspond à celle annoncée par le RTS diminuée de la durée d'émission du CTS et du SIFS correspondant (Durée restante nécessaire à l'échange).
- *FCS : détection* des erreurs de transmissions.

Remarque

- En fonction des différents types de trames, tous les champs ne sont pas présents.

Exposé

- Analyseur de trafic -niveau MAC-, principe et exemples.

Référence

- ***Claude Servin***, RÉSEAUX & TÉLÉCOMS - Cours avec 129 exercices corrigés 2è édition pages: 534-436.

Homework -1-

- Value of duration filed in acknowledgment frame ?
- Use the right packet sniffer to visualize different frame type.
 - Microsoft Network Monitor.
 - WireShark
 - ...

Ce qui reste à étudier

1. Mise en place de deux architectures.
2. D'autres services de la 802.11
 1. Sécurité
 2. Gestion de l'énergie;
 3. Qos
 4. Mobilité;
 5. ...
3. Les couches physiques
4. Les versions de la 802.11
5. ...

1. Fonctionnement

- Mode Infrastructure
- Mode Ad hoc

1. Mode Infrastructure

- Dans les réseaux de type Infrastructure, chaque périphérique est relié au réseau *via* un point d'accès (AP) WiFi.
- On dit que le périphérique est le « client » et l'AP le « maître ».
- Un réseau de ce type s'appelle un *Basic Service Set (BSS)* et couvre un espace qu'on appelle une « cellule » ou *Basic Service Area (BSA)*.
- Chaque *BSS* est identifié par un nombre composé de 48 bits : c'est le BSSID.

1. Mode Infrastructure

- En mode Infrastructure, ce BSSID correspond tout simplement à l'adresse MAC du point d'accès.
- L'AP sert de **relais** entre les périphériques, mais il peut aussi servir de relais vers un réseau filaire, par exemple votre réseau d'entreprise.
- Plusieurs points d'accès peuvent être déployés pour atteindre une plus large couverture WiFi.
- Ces BSS multiples peuvent être reliés par un système de distribution (Distribution System, DS) : réseau filaire Ethernet (cas le plus fréquent), de façon à former un unique réseau sans fil étendu.

1. Mode Infrastructure

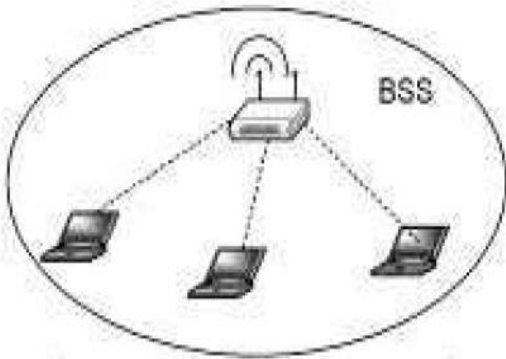
- Il est alors possible pour un utilisateur de se déplacer dans l'ensemble de la zone de couverture sans souffrir de ralentissement ou d'interruption de sa connexion.
- En cas de besoin, la liaison bascule automatiquement (c'est le ***hand-over***) vers le point d'accès offrant la meilleure connexion.

1. Mode Infrastructure

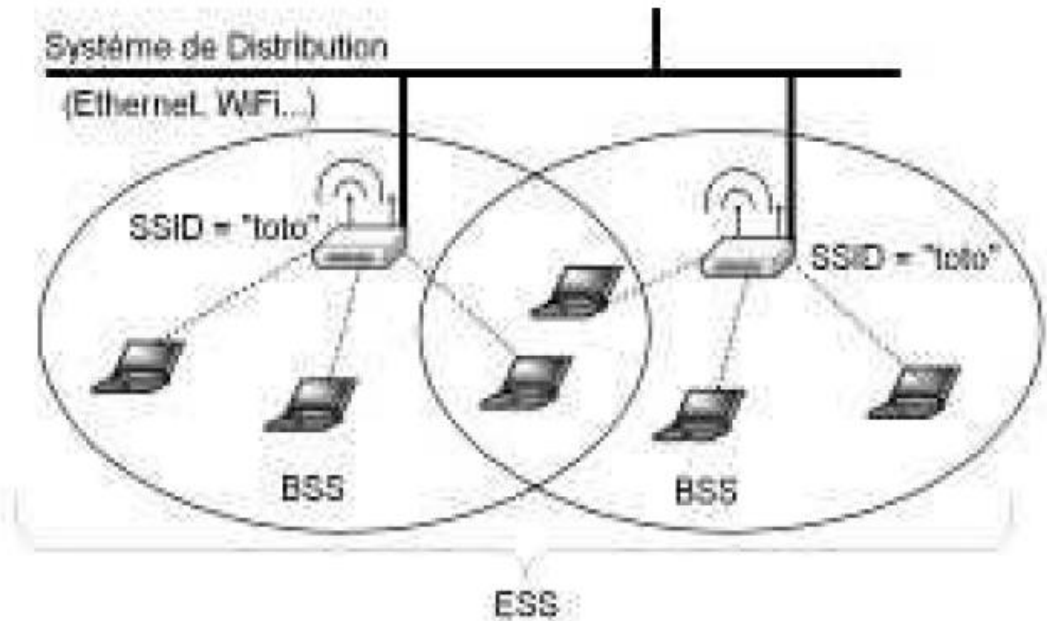
- On parle dans ce cas d'*Extended Service Set* qui couvre naturellement un espace appelé l'*Extended Service Area (ESA)*, composé de plusieurs cellules.
- Chaque ESS est identifié par un nom stocké sur 32 octets maximum qui s'appelle l'ESSID (ou simplement le SSID)

1. Mode Infrastructure

BSS



ESS



1. Le processus d'association

a. Les trames balises

1. AP sends every 100 ms a beacon frame 'trame balise'.
 - BSSID
 - débits autorisés et éventuellement le SSID
 - Le standard reste assez ouvert sur les informations diffusées dans les trames balises, ce qui permet à certains constructeurs de rajouter des informations spécifiques, comme la charge actuelle de l'AP, pour permettre aux équipements sachant interpréter ce paramètre de se connecter à l'AP le moins encombré.
 - Un Champ qui indique avec précision le temps écoulé depuis l'initialisation de l'AP.

1. Le processus d'association

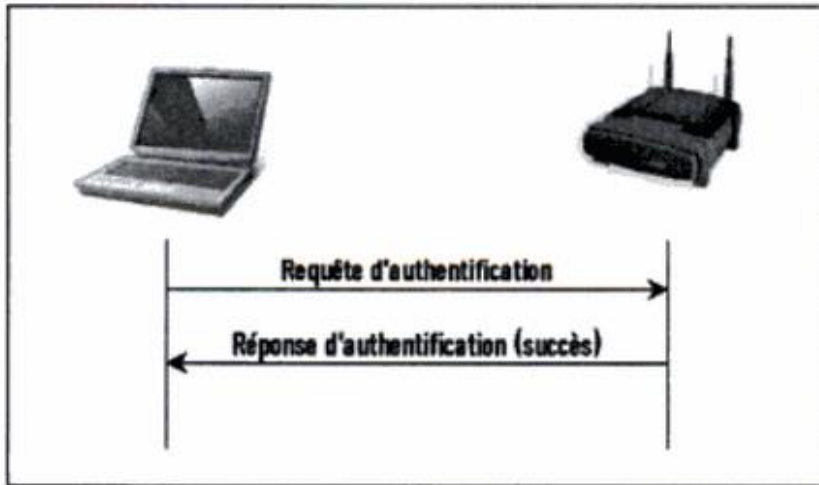
b. Détecter les réseaux présents

1. Passive : La diffusion (ou *broadcast*) du SSID dans les trames balises, l'utilisateur pourra ainsi très simplement sélectionner le SSID de son choix dans une liste.
2. Active : envoyer des requêtes de sondage (*probe requests*) contenant le SSID souhaité et les débits que le périphérique est capable de gérer.
 1. Si un point d'accès se situe à proximité et reçoit la requête, il commence par vérifier que le SSID correspond au sien et il répond avec un paquet (*probe response*) contenant à peu près la même chose que la trame balise.

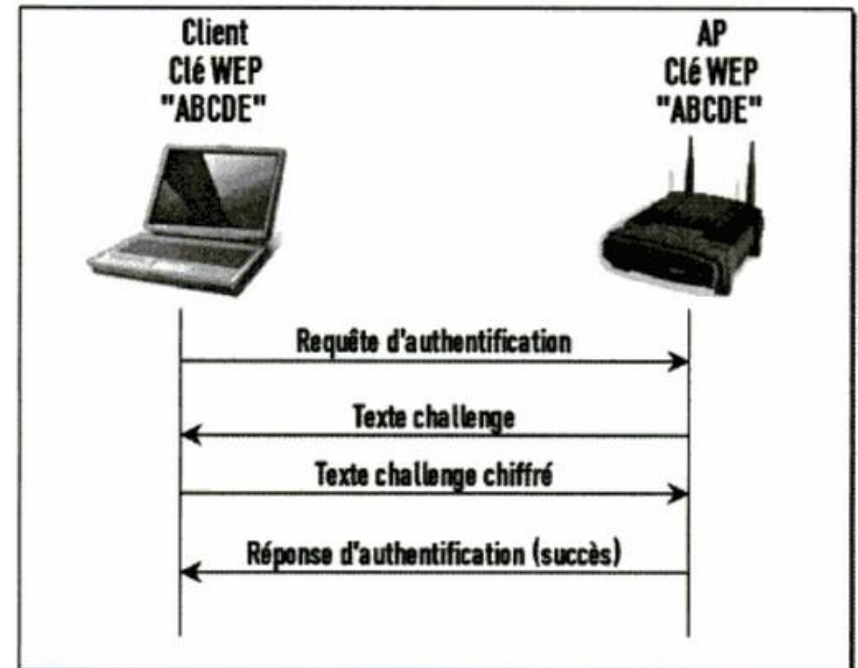
1. Le processus d'association

c. L'authentification

Authentification ouverte



Authentification WEP



2. L'authentification

- WEP présente plusieurs vulnérabilités et rapidement a été abandonné.

1. Le processus d'association

d. L'association

- Lorsque la station a bien été identifiée et que l'AP a renvoyé une réponse d'authentification positive, la station peut alors s'associer à l'AP pour avoir accès aux services du réseau.
- Pour cela, elle doit envoyer une requête d'association à l'AP. Cette requête contient entre autres la liste des débits que la station est capable de gérer.

1. Le processus d'association

d. L'association

- L'AP alloue un identifiant unique à la station (**l'identifiant d'association**), elle enregistre les informations de la requête dans sa table des associations (en mémoire), enfin elle renvoie une réponse d'association pour confirmer que l'association a bien eu lieu.
- À partir de ce moment, la station fait « officiellement » partie du réseau : tout paquet envoyé par cette station **est relayé par l'AP**.

1. Le processus d'association

e. La réassociation

- La station vérifie régulièrement (passivement ou activement) la présence d'autres AP ayant le même SSID.
- Ainsi, lorsqu'un AP s'avère plus intéressant (plus proche ou plus disponible),
 - la station envoie d'abord une requête de « désassociation » auprès de l'AP actuel suivie d'une requête de « réassociation » auprès du nouvel AP.
- La requête de réassociation indique entre autres l'identité de l'AP précédent.

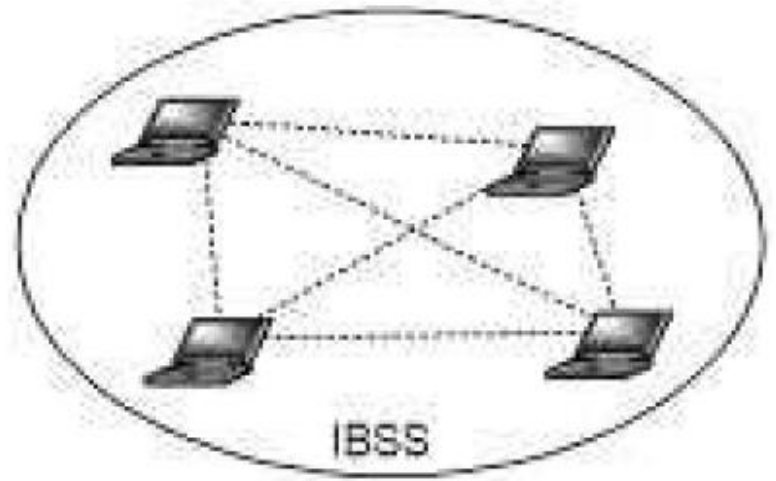
1. Le processus d'association

e. La réassociation

- Ceci permet aux deux AP de se mettre en relation au travers du système de distribution (DS) pour se transmettre des informations concernant la station et pour distribuer d'éventuels paquets en attente pour la station.
- Tout ce processus de réassociation se déroule automatiquement, de façon complètement transparente pour les couches réseaux supérieures et pour l'utilisateur : on peut ainsi changer de cellule tout en poursuivant un téléchargement, par exemple.

2. Mode ad hoc

- Dans les réseaux de type Ad Hoc, chaque périphérique communique directement avec les périphériques situés à sa portée, sans passer par un intermédiaire.

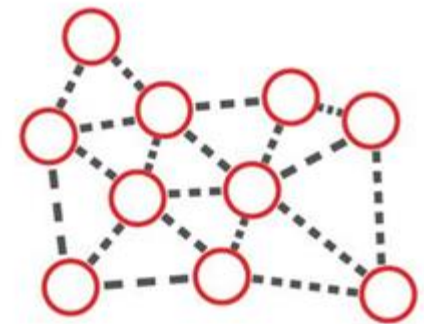


2. Mode ad hoc

1. Pour relier plusieurs ordinateurs entre eux en mode *Ad Hoc*, il faut configurer le réseau au niveau WiFi, mais aussi au niveau IP.
2. Ce mode Ad Hoc ne spécifie pas comment deux stations peuvent communiquer entre elles par l'intermédiaire d'une troisième : aucun protocole de routage n'est prévu.

2. Mode ad hoc

3. Autrement dit, le mode Ad Hoc ne permet que de parler avec ses voisins directs, et il ne permet pas, tout seul, la mise en place ce qu'on appelle un « réseau maillé » (en anglais, « *mesh network* »), *c'est-à-dire un réseau où les stations peuvent communiquer les unes avec les autres par l'intermédiaire d'autres stations.*



Mesh **Network**

Le processus d'association

- Lorsqu'une station est configurée en mode Ad Hoc, elle attend un certain temps et si elle ne détecte pas de balise, elle l'émet elle-même, à intervalles réguliers.
- Chaque station peut rejoindre le réseau.
- Chaque station peut envoyer la balise .
- Le hasard désigne donc la station qui émettra la balise, ce qui répartit naturellement cette tâche entre toutes les stations.

Homework -2-

1. Créer un réseau ad hoc et tester les concepts mentionnés dans le slide précédent.
2. Use the right packet sniffer to show frames used in association/disassociation, authentication, ... in ad hoc and infrastructure wireless networks.

Exposé

- Standard *802.11s* pour les réseaux maillés.

2. Les services de la 802.11

a. Les mécanismes de sécurité (ch4)

1. Masquer le SSID

- **Masquer le SSID** : Puisque toute requête d'authentification doit contenir le bon SSID, on voit qu'un premier niveau de sécurité pour un réseau WiFi consiste à simplement configurer les points d'accès pour qu'ils ne diffusent pas leur SSID. Si quelqu'un ne connaît pas le SSID du réseau, il ne parviendra pas à s'y associer.

les mécanismes de sécurité

2. Filtrage par adresse MAC

- Bien que cela ne soit pas officiellement dans la norme 802.11, rien n'empêche à un AP de vérifier si l'adresse MAC de la station qui cherche à s'authentifier se trouve bien dans une liste d'adresses MAC autorisées.

les mécanismes de sécurité

2. Filtrage par adresse MAC

- En effet, l'adresse MAC d'une station est présente dans toutes les trames qu'elle émet, et donc en particulier dans la requête d'authentification.
- On pourra, par exemple, n'autoriser que les adresses MAC des machines de l'entreprise.
- Ce type d'authentification peut être employé en complément d'un autre type d'authentification (WEP, WPA, WPA2...).

les mécanismes de sécurité

3. Le WEP

- Wired Equivalent Privacy : malgré son nom qui signifie littéralement « sécurité équivalente à un réseau filaire », le cryptage WEP a été « cassé » par des chercheurs qui y ont trouvé plusieurs failles.
- Il existe même des logiciels gratuits pour déchiffrer toutes les communications WEP.

les mécanismes de sécurité

4. Le 802.11i et le WPA

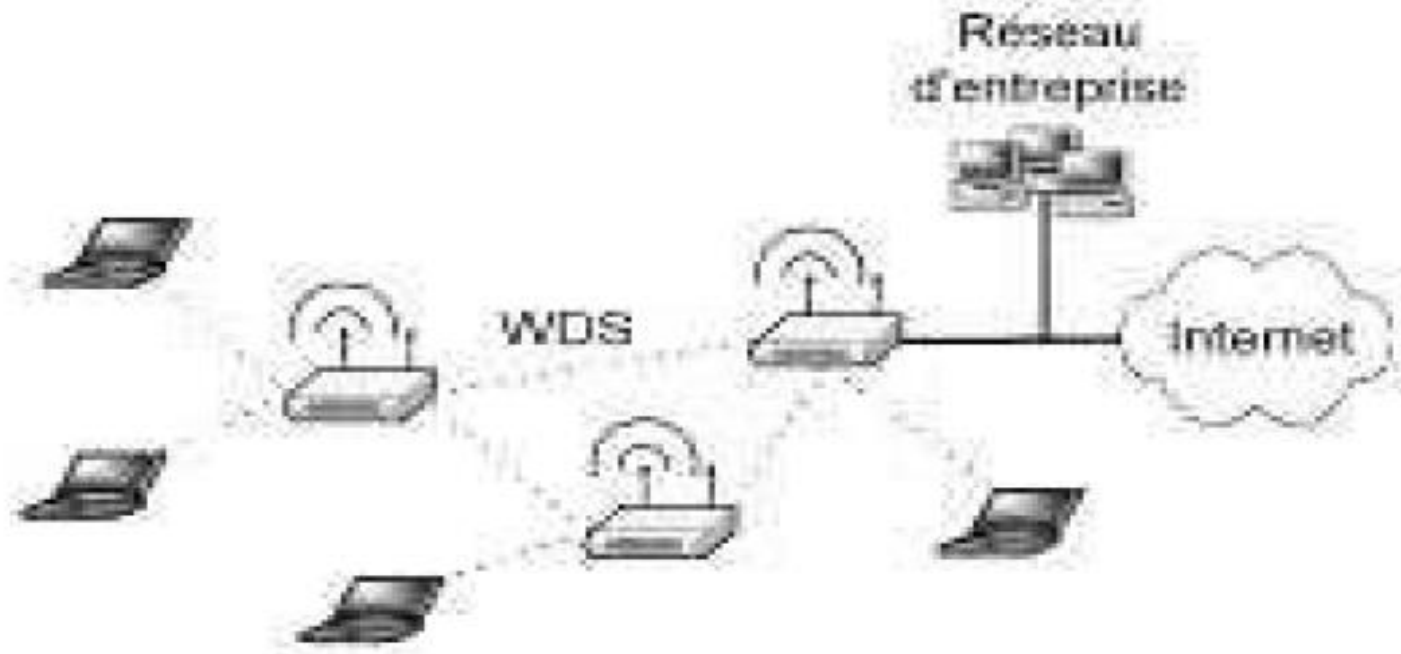
Très critiqué pour les failles de sécurité du 802.11, l'IEEE a décidé de réagir en lançant un nouveau groupe de travail : le 802.11i

- *Wireless Protected Access (WPA)*. avec une méthode de cryptage plus puissante encore : l'AES.
- WPA2.

b. MAC autres fonctions

- a. **Le contrôle d'erreur 'CRC'** : si les deux CRC calculé par le récepteur et l'émetteur sont identiques, il est très probable que le paquet ait été transmis correctement.
- b. **L'acheminement des paquets et le WDS** : Il offre la possibilité à un AP de relayer un paquet non pas directement à la station de destination, mais plutôt à un autre AP, à travers les airs. Ceci permet d'étendre la couverture du réseau sans fil avec des AP qui ne sont pas connectés au réseau filaire.

b. MAC autres fonctions



Le Wireless Distribution System (WDS)

L'acheminement des paquets et le WDS

Version		Type		Sous-type			
2 bits		2 bits		4 bits			
toDS	fromDS	Frag	Retry	Sleep	More	WEP	Order
1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit

toDS	fromDS	Mode	Cas de figure
0	0	Ad Hoc	Un paquet envoyé directement d'une station à une autre.
1	0	Infrastructure	Un paquet envoyé par une station vers un AP pour être relayé vers une autre station.
0	1	Infrastructure	Un paquet relayé par un AP vers la station de destination.
1	1	Infrastructure	Un paquet relayé par un AP vers un autre AP pour acheminer le paquet à destination (WDS).

Lecture complémentaire -1- reste des slides ...

- Gestion de l'énergie dans la 802.11 dans les deux modes avec et sans infrastructure.

b. MAC autres fonctions

c. L'économie d'énergie

- Les communications WiFi peuvent diminuer l'autonomie l'appareil de plus de 80 %.
- Pour définir une stratégie d'économie d'énergie, il faut d'abord savoir à quel moment cette énergie est consommée par un adaptateur WiFi.

L'économie d'énergie

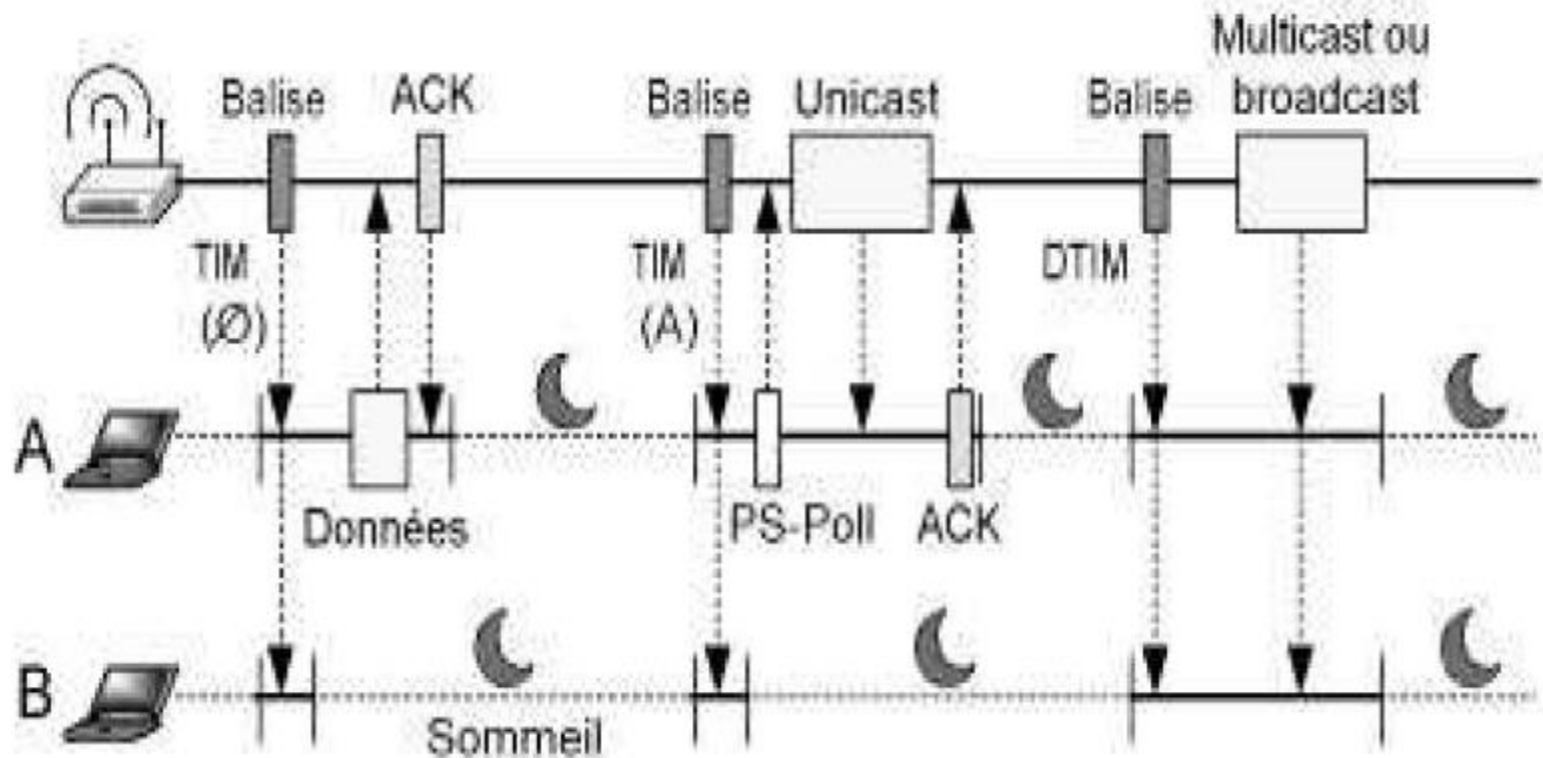
- Il en consomme le plus lorsqu'il envoie des données ;
- il en consomme un peu moins en recevant des données ;
- lorsqu'il écoute les ondes radio sans rien recevoir, il consomme presque autant que lorsqu'il reçoit un paquet ;
- il ne consomme presque rien lorsqu'il est en sommeil ;
- il ne consomme rien lorsqu'il est éteint.

Le mode d'économie d'énergie

Mode Infrastructure

- WiFi se trouvent en général dans le mode de disponibilité continue (*Continuously Available Mode ou CAM*).
- Le 802.11 définit *Power Save Polling Mode ou PSPM*, souvent noté PSM).
 - Balises :
 - *Traffic Indication Map (TIM)*
 - *Delivery TIM (DTIM)*,

Le mode d'économie d'énergie



Le mode d'économie d'énergie

- Une station WiFi configurée en mode d'économie d'énergie n'active son interface radio que de façon intermittente.
- Les paquets devant être envoyés sont placés dans une file d'attente et ne sont émis qu'au « réveil » suivant, de façon groupée.
- Dans le dernier paquet envoyé à l'AP, la station signale qu'elle va se remettre en mode d'économie d'énergie. L'AP sait alors que tout paquet adressé à cette station devra être mis dans une file d'attente jusqu'à son réveil.
- À intervalles réguliers, au sein des trames balises, l'AP envoie la liste des stations (plus exactement la liste de leurs identifiants d'association) pour lesquels il possède des paquets en attente. Ce paramètre s'appelle le *Traffic Indication Map (TIM)*.

Le mode d'économie d'énergie

- *De cette façon, au moment d'un réveil, la station n'a pas à émettre de requête pour savoir s'il y a des paquets en attente pour elle : il lui suffit d'attendre de recevoir la liste des stations concernées et de voir si elle en fait partie. Si c'est le cas, elle demande à l'AP de lui envoyer les paquets qui lui sont dus, en lui envoyant une requête *Power Save Poll (PS-Poll)*. Sinon, elle se « rendort » immédiatement.*

Le mode d'économie d'énergie

1. Le trafic broadcast et multicast que l'AP doit émettre est conservé dans une file d'attente et envoyé uniquement à certains moments précis : les stations peuvent ainsi se réveiller au bon moment pour le recevoir. Pour cela, toutes les quelques balises, l'AP envoie un TIM spécial appelé le *Delivery TIM (DTIM)*, qui indique une *durée* pendant laquelle le trafic **broadcast et multicast** sera envoyé. (par exemple, une balise sur cinq)

L'économie d'énergie en mode Ad Hoc

- Pour les communications Ad Hoc, le mécanisme est légèrement différent, mais le principe est le même : si une station est en mode d'économie d'énergie, elle se réveille à intervalles réguliers, au moment de l'émission des balises et elle écoute pendant un bref instant avant de se rendormir .Les stations sont synchronisées et toutes celles qui sont en mode d'économie d'énergie se réveillent en même temps.

L'économie d'énergie en mode Ad Hoc

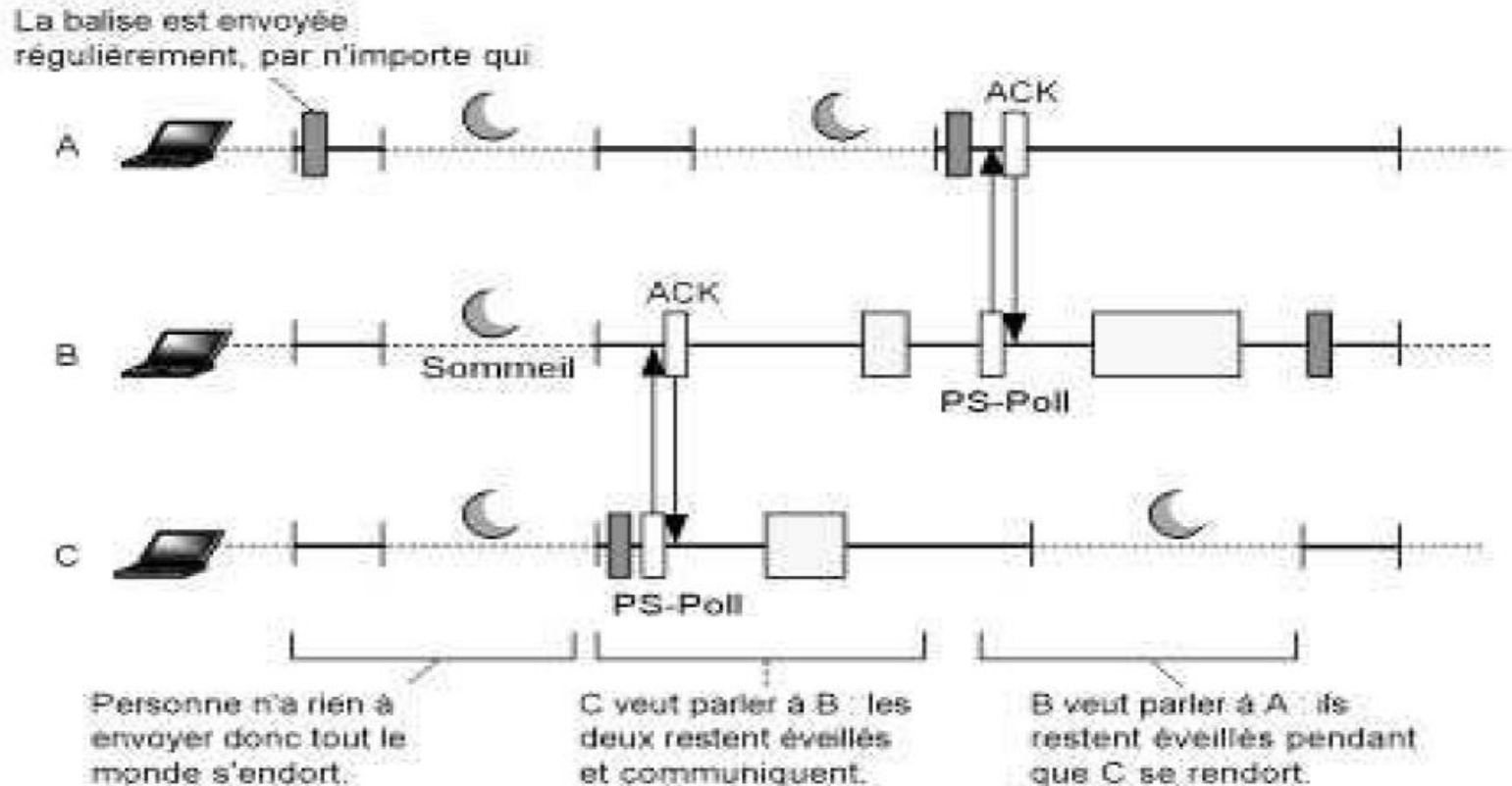


Figure 3.18 — L'économie d'énergie en mode Ad Hoc.

Économie d'énergie et QoS

- Bien que ce mécanisme permet une importante économie d'énergie et donc une plus grande autonomie (très variable selon le type du périphérique et le débit), il peut perturber légèrement la communication WiFi et empêcher toute politique de QoS pour la station qui l'utilise.

Le WMMPS

- Pour limiter cet effet négatif de l'économie d'énergie sur la qualité de service, la WiFi Alliance a défini le « *WMM-Power Save* » (ou *WMM-PS*). Il s'agit d'un ensemble de mesures techniques définies dans le standard **802.11e**, et qui ont pour objectif d'optimiser l'économie d'énergie, notamment pour les terminaux mobiles.
- Permet aux concepteurs de logiciels d'indiquer la priorité du trafic qu'ils gèrent : l'algorithme d'économie d'énergie s'adapte alors automatiquement en fonction de cette priorité. Par exemple, si une station n'a que du trafic peu prioritaire à émettre, elle restera « endormie » plus longtemps, et économisera davantage d'énergie

Home works

- Les travaux à domicile sont optionnels, mais à noter pour améliorer principalement la note de TD et éventuellement l'évaluation globale de module.
- Chaque travail doit être rédigé dans un rapport en format PDF qui porte obligatoirement le nom et prénom.
- Envoyé à : azedine.attir@univ-msila.dz
accepted only before EMD.