

MOOC Réseaux Locaux

Le réseau local Wi-Fi (Wi-Fi)

Objectifs généraux du Wi-Fi

Objectifs

Cette leçon a pour but de présenter les objectifs de Wi-Fi et ses principales évolutions.

Prérequis

Connaissances élémentaires des réseaux locaux.

Connaissances

Principales évolutions de Wi-Fi.

Compétences

Différencier et expliquer les principales évolutions de Wi-Fi.

Évaluation des connaissances

Description des évolutions de Wi-Fi.

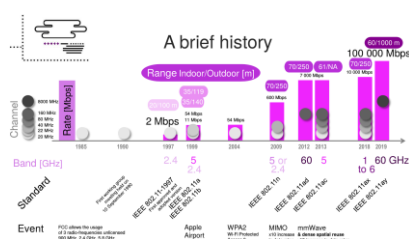
Évaluation des compétences

Analyser les évolutions de Wi-Fi.

 <p>Wi-Fi Introduction</p> <p>Riadh DHAOU</p>	<p>Pendant cette semaine, nous nous intéresserons à la technologie phare des réseaux locaux sans-fil : le Wi-fi. Cet acronyme désignant en fait le terme anglais Wireless Fidelity.</p>
 <p>Objectives</p> <ul style="list-style-type: none"> History of Wi-Fi, the main Wireless Local Area Network Evolution of standardization IEEE 802.11 	<p>Aujourd'hui, cette technologie est largement utilisée dans les réseaux d'entreprise, pour des applications domotiques, dans les transports, dans les gares et aéroports.</p> <p>Les objectifs de cette séance sont d'une part de s'arrêter aux principales étapes de l'histoire des réseaux locaux sans fil Wi-Fi et d'autre part de passer en revue les principales évolutions des standards associés émanant des travaux des groupes de standardisation de l'IEEE 802.11.</p>
 <p>Wireless Fidelity (Wi-Fi)</p> 	<p>Qu'est-ce qu'un réseau Wi-Fi ? De quoi est-il composé ? Et qu'est-ce qui le distingue de réseau Ethernet, que vous avez eu l'occasion de voir la semaine dernière?</p> <p>Un réseau Wi-Fi permet de relier, par ondes radio, plusieurs équipements informatiques (ordinateur, tablette, etc.) au sein d'un réseau informatique afin de permettre la transmission de données entre eux.</p> <p>La communication peut être directe entre terminaux ou bien via un point d'accès.</p> <p>Comme vous le voyez sur ce schéma, le point d'accès constitue le plus souvent une passerelle entre le réseau sans fil et un réseau filaire.</p> <p>Grace à la nature du support utilisé, le Wi-Fi procure une liberté de mobilité aux usagers et permet de s'affranchir ainsi des contraintes liés au câblage.</p>
 <p>Wireless Fidelity (Wi-Fi)</p> <ul style="list-style-type: none"> 1 MAC layer Many physical layers 2.4GHz, 60GHz, infrared... Li-Fi (Light-Fidelity) Unlicensed bands Limited range <ul style="list-style-type: none"> 10s meters indoor 100s meters outdoor 	<p>L'une des caractéristiques essentielles des standards Wi-Fi est qu'elles définissent une couche MAC commune à toutes les couches physiques utilisées, et qui sont assez diverses et variées.</p> <p>En effet, le Wi-Fi exploite des bandes de fréquences variées. Les bandes centimétriques (autour des 2.4 GHz), aussi les bandes millimétriques exploitées le plus récemment autour des 60GHz ou encore des communications en infra-rouges. Le Wi-Fi se distingue de technologies concurrentes comme le LiFi qui utilise la partie visible du spectre électromagnétique pour communiquer.</p> <p>L'utilisation des bandes radio est régie par des organismes</p>

propres à chaque pays. Pour éviter qu'une licence ne soit demandée pour chaque type de réseau Wi-Fi, les couches radios utilisent des fréquences situées dans des bandes dites sans-licence. Il s'agit de bandes libres qui ne nécessitent pas d'autorisation d'un organisme de régulation, mais pour lesquelles une limitation de puissance maximale d'émission est imposée.

Vu la limitation de puissance autorisée (de la dizaine à la centaine de milliwatts) la portée de transmission des équipements, et à fortiori le rayon couvert par le point d'accès, est limitée (de quelques dizaines de mètres en indoor à quelques centaines de mètres à l'extérieur).



L'histoire des réseaux Wi-Fi est marquée principalement par une évolution de la couche physique :

Dès la libération, par l'autorité de régulation des télécoms américaine (la Federal Communications Commission) en 1985, des bandes de fréquences des 900 MHz, 2.4 GHz et 5.8 GHz, dites bandes ISM, et qui peuvent être utilisées dans un espace réduit pour des applications industrielles, scientifiques et médicales, la course à l'exploitation de ces bandes sans licence a été engagée. L'organisme de standardisation IEEE s'est emparé de la création de standards de communication pour des réseaux locaux sans-fil en créant le groupe 802.11 en 1990 (on parle alors de WLAN ou Wireless Local Area Network). 7 ans plus tard le premier standard IEEE 802.11 legacy a été finalisé.

Plusieurs concurrents existaient à l'époque, nous pouvons citer à titre d'exemple le standard HiperLAN de l'ETSI.

Mais les standards IEEE se sont rapidement imposés.

Les premiers standards, 802.11b et plus tard le 11g puis 11n exploitaient la bande 2.4 GHz. Mais très vite, la bande des 5GHz a également été exploitée par les versions a, n et ac. Les ressources radio disponibles sont plus abondantes dans les bandes à fréquences plus élevées. Néanmoins, celles-ci sont plus sensibles aux atténuations (dues aux obstacles ou à la pluie).

Même si la bande ISM est reconnue par les principaux organismes de réglementation (le FCC aux états unis, l'ETSI en Europe ou l'ARCEP en France), sa largeur varie selon les pays. Par exemple, en Europe, la sous-bande des 900MHz est exploitée par le GSM. Des efforts d'harmonisation ont été conduits et de nouvelles sous-bandes sont libérées

progressivement.

En plus des problèmes de réglementation, cette bande est utilisée par de nombreux standards, à part le Wi-Fi, comme le Bluetooth ou Zigbee ce qui provoque d'importants conflits de fréquences et crée des interférences et une dégradation de la qualité des communications. Les organismes de réglementation s'efforcent de libérer de nouvelles bandes de fréquences pour pallier la pénurie de ressources radio et prévoir la densification des WLANs. C'est ainsi que les bandes autour des 60GHz sont désormais utilisées.

Remarquons que les canaux en fréquence utilisés sont de plus en plus larges et varient de la vingtaine de MHz, dans les tous premiers standards, jusqu'à 8GHz pour le 11ay, exploitant la bande millimétrique dont la sortie est prévue pour l'année 2019.

Les utilisations de canaux plus larges, accompagnés de l'exploitation de techniques de transmission avancées, ont permis d'accroître les débits physiques crêtes, qui seront partagées entre les utilisateurs de la même cellule et qui sont passées de 2Mbps dans les toutes premières versions jusqu'à l'ordre de quelques dizaines de Gbps proposées dans les versions en cours de standardisation.

Autre remarque, les lettres qui suivent le 802.11 n'ont aucune signification chronologique, mais elles permettent de désigner les amendements apportés au standard 802.11 émanant des multiples groupes de standardisation. La preuve, 11b culminant à 11Mbps et 11a allant à 54 Mbps sont parus en même temps en septembre 1999.

Notons ici, deux points :

Le premier, est que la technique au niveau physique du 11b est une technique d'étalement de spectre. Alors que les standards 11a et plus récents ont adopté une technique aux performances supérieures l'OFDM (Orthogonal Frequency Division Multiplexing). Technique qui était réservée aux systèmes de transmission de données en continue tels que DVB (Digital Video Broadcasting) ou ADSL (Asymmetric Digital Subscriber Line). Vous verrez plus en détail ces techniques pendant la prochaine leçon.

Le deuxième point est relatif à la mise en disponibilité d'équipements Wi-Fi. Le premier équipement Wi-Fi ayant un

prix raisonnable pour être exploité par le grand public a été introduit par Steve Jobs en juillet 1999. Il s'agit de Apple Airport introduit avec l'Ibook.

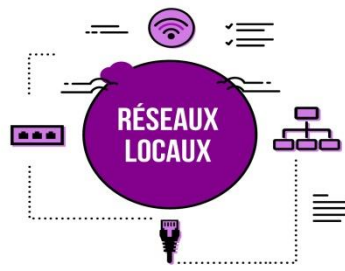
Ces amendements sont regroupés dans des documents de références qui sont estampillés par leur année d'apparition par exemple le dernier en date est le standard 802.11-2012.

Cette histoire riche est marquée également par des évolutions technologiques :

- Soit au niveau de la couche physique : par exemple liés à l'utilisation de plusieurs antennes en émission ou en réception. Technique dite Multiple-Input Multiple-Output (ou MIMO). Intégrée dans les équipements Wi-Fi récents dès l'amendement 11n.
- Soit aux niveaux plus élevés, comme pour introduire des éléments liés à la sécurité : principalement l'amendement 11i qui a introduit en 2004 l'authentification par contrôle d'accès au port et le chiffrement des données.

Le terme Wi-Fi est apparu assez tard, il est parfois accompagné par d'un qualificatif comme le Wi-Fi 5 par exemple pour 11a opérant dans la bande des 5GHz, Wi-Fi MIMO pour 11n ou encore Wi-Fi Protected Access (ou WPA2) pour le 11i.

Si aujourd'hui les équipements embarquant les cartes Wi-Fi a, b ou g sont en cours d'extinction, il n'en reste pas moins que les standards 802.11 se doivent d'être rétro-compatibles. Un équipement conforme à 802.11n doit pouvoir communiquer avec un point d'accès 802.11 b ou g.



MOOC Réseaux Locaux

Le réseau local Wi-Fi

La couche MAC de Wi-Fi

Objectifs

Cette leçon a pour but de décrire la couche MAC de Wi-Fi. Elle s'intéresse en particulier aux différentes méthodes d'accès, à la gestion de la qualité de service (QoS) ainsi qu'aux trames utilisées dans ce contexte.

Prérequis

Connaissance de base de Wi-Fi : les trames, la couche physique.

Connaissances

Les principaux éléments de la couche MAC de Wi-Fi.

Compétences




Distinguer les différentes méthodes de partage de support de Wi-Fi. Identifier les trames utilisées pour la gestion de la couche MAC.

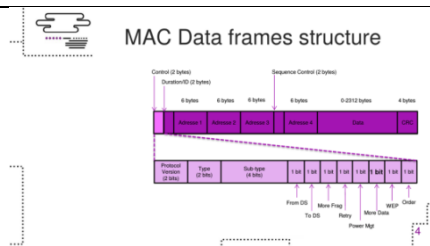
Évaluation des connaissances

Décrire les principales composantes de la couche MAC de Wi-Fi.

Évaluation des compétences

Analyser un scénario d'échange de trame de gestion de la couche MAC.

 <p>Wi-Fi 802.11 MAC Layer</p> <p>Riadh DHAOU</p>	<p>Cette séance est dédiée à la couche d'accès du Wi-Fi spécifiée dans le standard 802.11.</p>
 <p>Objectives</p> <ul style="list-style-type: none"> o Medium Access Control (MAC) o MAC frames structure o QoS o Power saving mode 	<p>Comment le Wi-Fi contrôle-t-il l'accès au médium ? Et comment permet-il de différencier les services pour des applications assez variées ? Pour que vous puissiez comprendre le fonctionnement, nous allons vous donner une idée sur les différents types de trames Wi-Fi et la structuration associée.</p> <p>Nous allons, par la suite, discuter les méthodes d'accès utilisées en s'intéressant particulièrement à la gestion de la QoS</p> <p>Enfin, nous savons que les équipements mobiles sont alimentés sur batterie ; ce qui pose un problème pour la gestion de l'économie de l'énergie. Comment le Wi-Fi traite-t-il ce problème ?</p>
 <p>Frames types</p> <ul style="list-style-type: none"> o Management frames <ul style="list-style-type: none"> • Beacons • Probe Requests/Responses • Authentication • Association o Control frames <ul style="list-style-type: none"> • RTS/CTS, ACK o Data frames 	<p>Pour commencer, trois principaux types de trames sont utilisés dans la norme 802.11.</p> <p>D'abord, les trames de gestion, transmises comme des trames de données afin d'échanger des informations de gestion. Parmi elles des trames balise (beacon), des trames Probe Request / Response et enfin des trames utilisées pour l'authentification et pour l'association. (Toutes ces trames de gestion ne sont pas délivrées aux couches supérieures).</p> <p>Ensuite des trames de contrôle, utilisées pour contrôler l'accès au média partagé et qui contribuent au bon acheminement des trames de données.</p> <p>Par exemple : les trames RTS/CTS, utilisées respectivement pour prémunir des problèmes de station cachée et de station exposée. En annonçant la durée pendant laquelle le canal sera occupé et donc inutilisable par les voisins potentiels de l'émetteur et du récepteur. Enfin les trames d'ACK qui permettent de confirmer la réception de la trame de donnée.</p> <p>Enfin, nous trouvons les trames de données, qui contiennent les informations utiles.</p>



Voyons plus en détail la structuration de ce dernier type de trames:

La trame MAC est composée d'un premier champ de contrôle de la trame.

D'un champs à double signification Durée/ID. Selon le type de la trame, ce champ peut avoir deux sens différents : pour les trames de polling en mode d'économie d'énergie, c'est l'identifiant de la station. Pour les autres trames, c'est la valeur de la durée de vie pendant laquelle le canal sera occupé.

De quatre champs d'adresses. Chaque adresse est sur 48 bits (même format qu'une adresse Ethernet).

D'un champ Contrôle de séquence. Utilisé pour spécifier l'ordre des fragments d'une trame fragmentée.

D'une charge utile qui peut aller jusqu'à 2312 octets

Et, enfin, d'un champ CRC, pour le contrôle d'erreur, sur 32 bits.

Le champ de contrôle est composé : D'une Version de protocole. D'un Type et d'un sous-type.


Et d'un ensemble de flags. Nous trouvons ici les bits : ToDS et From DS (Pour indiquer que la trame est envoyée vers le système de distribution ou si elle vient du DS. Selon les valeurs de ces bits, la signification des 4 champs adresses change. En effet, les deux premières adresses représentent respectivement l'adresse de la station destination, et de la station source.




L'adresse 3 est l'adresse de la station source originale (si le flag from DS du champ de contrôle est à 1)

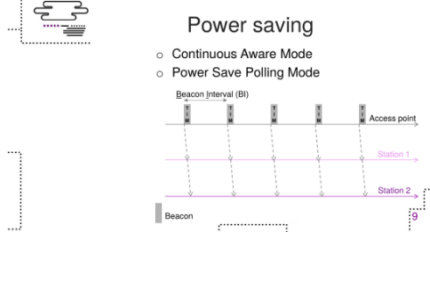
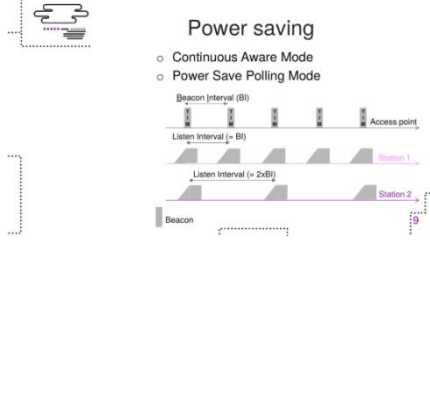
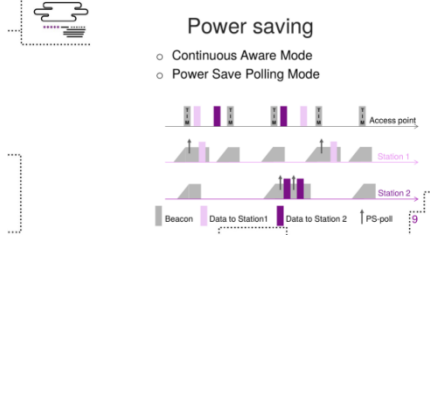
Cette adresse 3 est l'adresse du terminal de destination (si le flag from DS du champs de contrôle est à 0 et le flag to DS est à 1)

Et enfin l' Adresse 4 est utilisée lorsqu'une trame est transmise d'un point d'accès à un autre à travers le système de distribution. Lesbits To DS et From DS sont alors tous les deux à 1, et il faut renseigner à la fois la source et le destinataire.

Le bit More Fragments est mis à 1 lorsque d'autres fragments

	<p>suivent le fragment en cours. Le bit Retry indique que la transmission du fragment, ou de la trame, en cours est une retransmission d'un fragment ou d'une trame précédemment transmise. Ainsi, la station destination peut reconnaître les doublons, ce qui peut arriver lorsqu'un ACK se perd. Le bit Power Management est utilisé pour la gestion de l'énergie. Il indique que la station passe en mode d'économie d'énergie juste après la fin de la transmission de la trame en cours. Grâce à ce bit, les stations peuvent changer de mode de fonctionnement, passant du mode veille au mode actif, ou inversement.</p> <p>Le bit More Data est également utilisé pour la gestion de l'énergie. Il est utilisé par l'AP pour indiquer que des trames sont stockées pour une station. La station peut demander à recevoir les autres trames ou bien, grâce à cette information, passer en mode actif.</p>
 <p>Medium Access Control</p> <ul style="list-style-type: none"> ○ Two methods to Share the medium <ul style="list-style-type: none"> ○ DCF (Distributed Coordination Function) <ul style="list-style-type: none"> ○ Random access based on CSMA/CA ○ Uses contention backoff algorithm ○ Designed for a best-effort service ○ Supports asynchronous transmissions ○ PCF (Point Coordination Function) <ul style="list-style-type: none"> ○ Contention free based ○ Uses a centralized based priority ○ Designed for time-bounded multimedia services ○ Supports synchronous transmissions 	<p>Pour partager le Média le standard 802.11 définit deux méthodes d'accès : la première est distribuée, la deuxième est centralisée.</p> <p>La première méthode est DCF (ou Distributed Coordination Function) Utilisable dans toutes les stations, en mode ad-hoc ou avec infrastructure. Elle utilise CSMA/CA avec le recours à un algorithme de backoff exponentiel pour retarder les retransmissions en cas de contention. Cette méthode est conçue pour des services de type best-effort typiquement pour le support de transmissions asynchrones.</p> <p>La deuxième méthode est PCF (ou Point Coordination Function) conçue pour être utilisée dans un point de coordination central donc uniquement dans les points d'accès, Le PA contrôle l'accès au média (par interrogation des stations). C'est une méthode sans contention et qui donne la liberté au PA de gérer des priorités de façon centralisée. Mais cette méthode reste peu implémentée même si elle a été conçue pour des services multimédias typiquement des transmissions synchrones.</p>

 <h3>Medium Access Control</h3> <ul style="list-style-type: none"> Limitations of the medium access <ul style="list-style-type: none"> DCF (Distributed Coordination Function) <ul style="list-style-type: none"> Does not provide QoS guarantees Does not support real-time applications Designed for equal priorities Does not differentiate the frames for different user priorities PCF (Point Coordination Function) <ul style="list-style-type: none"> Poor QoS performance Uses a simple round-robin algorithm, which cannot handle the various QoS requirements Transmission time of the polled stations is unknown 	<p>Ceci dit, les deux méthodes présentent des faiblesses. En effet, ni l'une ni l'autre ne permettent de donner des garanties d'accès aux ressources. Vu qu'on ne met pas de contrôle d'accès et que le nombre de stations qui sont susceptibles de transmettre peut varier dans le temps.</p> <p>La première méthode DCF ne fournit pas de garanties de QoS. Ne supporte pas les applications temps réel et n'est pas conçue pour gérer des priorités. En effet, si un utilisateur a des trames avec différents niveaux de priorités à émettre, cette méthode ne permet aucune différenciation de service.</p> <p>La deuxième méthode non plus ne permet pas de donner de garanties. Même si le point d'accès se charge de donner aux différentes stations des opportunités de communication, le niveau de performance de la qualité de service est assez médiocre.</p> <p>Cette méthode utilise un simple algorithme de round-robin qui ne peut gérer des niveaux de QoS variés. De plus, le temps de transmission des stations scrutées n'est pas connu à l'avance : il peut dépendre de la qualité de transmission.</p>
 <h3>Quality of Service</h3> <ul style="list-style-type: none"> Capacity to provide resource assurance in the network Mandatory for services such as VoIP or live video 	<p>La qualité de service sur un réseau permet aux utilisateurs de s'assurer que des informations envoyées arriveront dans un laps de temps maîtrisé. Cet élément est indispensable lorsqu'il s'agit d'utiliser des services comme la voix sur IP ou la vidéo live. Une des principales fonctions de la qualité de service est de rendre prioritaires certains paquets de données. Par exemple, une trame contenant de la voix a la priorité sur une trame contenant un fichier qu'un utilisateur est en train de télécharger d'Internet (et qui pourra patienter quelques millisecondes). Nous avons vu, le système PCF permet d'instaurer des priorités puisque le point d'accès gère l'accès au support. Par contre, il n'assure pas complètement la qualité de service.</p>
 <h3>Hybrid Coordination Function</h3> <ul style="list-style-type: none"> Two methods for medium access <ul style="list-style-type: none"> EDCF (Enhanced Distributed Coordination Function) <ul style="list-style-type: none"> Contention based channel Access Provide service differentiation Classify the traffic into 8 different classes Each station has 4 access categories to provide service differentiation HCCA (Hybrid Controlled Channel Access) <ul style="list-style-type: none"> Operates in CFP and CP Provides guaranteed services with a much higher probability than EDCA Combines the advantages of PCF and DCF Coordinates the traffic in any fashion (not just round-robin) 	<ul style="list-style-type: none"> La norme 802.11e a ajouté deux nouvelles méthodes d'accès : EDCF (Extended DCF) et HCF (Hybrid Coordination Function), en remplacement de DCF et PCF. EDCF pour Enhanced Distributed Coordination Function est une méthode à accès aléatoire avec différenciation de service. Comme vous le voyez sur le schéma on va classer le trafic en 8 classes de trafic qui vont être mappées sur 4 files avec quatre niveaux de priorités différentes. Donc 4 files avec des paramètres de backoff qui vont être spécifiques à

	<p>chaque file.</p> <p>La deuxième méthode Hybrid Controlled Channel accès (HCCA), comme son nom l'indique est une méthode hybride qui combine les avantages de PCF et de DCF. Elle opère à la fois en mode avec contention et en mode sans contention. Elle permet de donner de meilleures garanties que la méthode précédente, mais par contre les garanties ne sont pas absolues.</p>
 <p>Power saving</p> <ul style="list-style-type: none"> Continuous Aware Mode Power Save Polling Mode 	<p>Pour utiliser au mieux les batteries des stations mobiles, le standard définit deux modes d'économie d'énergie : le premier est le mode de fonctionnement par défaut. La station est tout le temps allumée et écoute constamment le support. Il ne s'agit donc pas d'un mode d'économie d'énergie.</p> <p>Le second, est bien un mode d'économie d'énergie.</p>
 <p>Power saving</p> <ul style="list-style-type: none"> Continuous Aware Mode Power Save Polling Mode 	<p>Dans ce mode, le point d'accès tient à jour un enregistrement de toutes les stations qui sont en mode d'économie d'énergie et stocke toutes les données qui leur sont adressées. Ces données sont stockées dans un élément appelé TIM (Traffic Information Map).</p> <p>Comme expliqué précédemment, les stations d'un BSS sont toutes synchronisées. Cette synchronisation, qui s'effectue par le biais de trames balises, permet d'établir le mécanisme d'économie d'énergie.</p>
 <p>Power saving</p> <ul style="list-style-type: none"> Continuous Aware Mode Power Save Polling Mode 	<p>Les stations en veille s'activent à des périodes de temps régulières pour recevoir une trame balise contenant le TIM envoyé en broadcast par le point d'accès. Entre les trames balises, les stations retournent en mode veille. Du fait de la synchronisation, toutes les stations partagent le même intervalle de temps pour recevoir les TIM et s'activent de la sorte toutes au même moment pour les recevoir.</p> <p>Les TIM indiquent aux stations si elles ont ou non des données stockées dans le point d'accès. Lorsqu'une station s'active pour recevoir un TIM et qu'elle s'aperçoit que le point d'accès contient des données qui lui sont destinées, elle lui envoie une trame de requête (PS-POLL) pour mettre en place le transfert de données.</p> <p>Une fois le transfert terminé, la station retourne en mode veille jusqu'à la réception du prochain TIM.</p>



To summarize

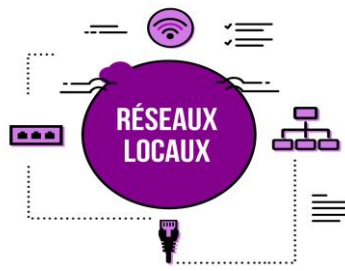
- Probability based QoS
- No guarantee
- Wi-Fi evolution

Pour finir, que devons-nous retenir?

Le Wi-Fi utilise un mécanisme d'accès aléatoire.

La gestion de la QoS est fondée sur une différenciation selon des niveaux de priorités sur la base de temps d'attente et taille maximale de fenêtre de contention différenciés, de plus en plus grands pour les classes de trafic de faible priorité. L'ensemble des mécanismes d'accès ne donne aucune garantie de disposer d'opportunité de communication.

Enfin le niveau accès du Wi-Fi évolue, pour aller plus loin vous pouvez vous intéresser aux derniers amendements qui gèrent des réseaux Wi-Fi plus denses.



MOOC Réseaux Locaux

Le réseau local Wi-Fi

La couche radio

Objectifs

Cette leçon a pour but de présenter les techniques les plus marquantes utilisées dans la couche physique de Wi-Fi.

Prérequis

Bonne connaissance des réseaux locaux. Notions de transmission et modulation.

Connaissances

Principales variantes de la couche physique de Wi-Fi.

Compétences




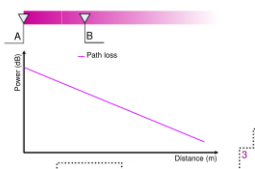
Analyser les principales solutions de la couche physique de Wi-Fi.

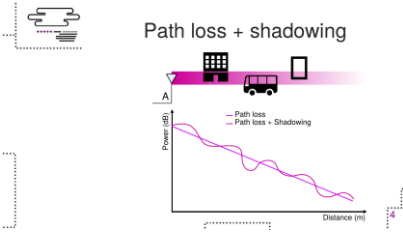
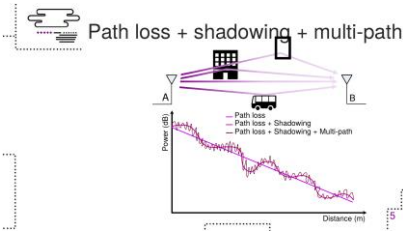
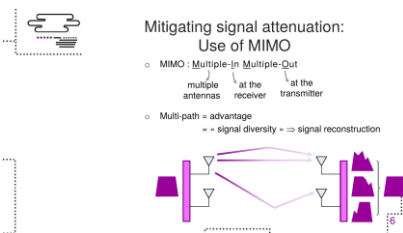
Évaluation des connaissances

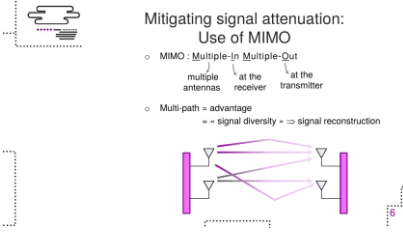
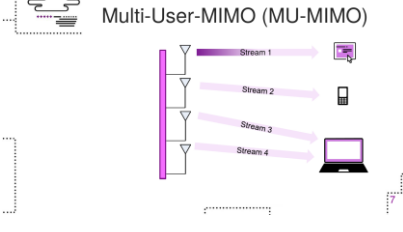
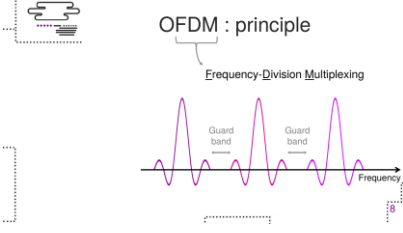
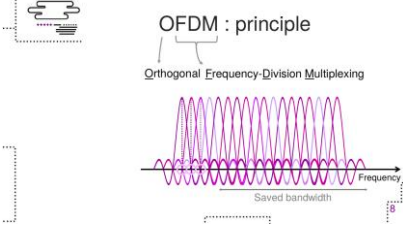
Description de la couche physique de Wi-Fi.



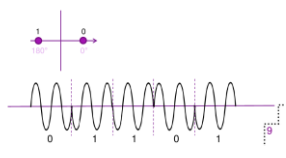

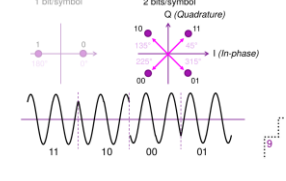

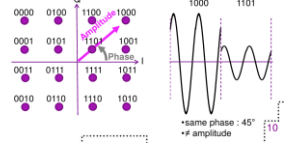
Évaluation des compétences


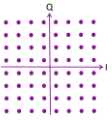
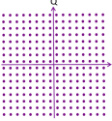

Analyse de la couche physique de Wi-Fi.

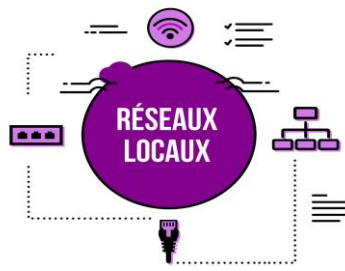
 <p>Wi-Fi Wi-Fi physical layer</p> <p>Naouel Ben Salem Grati</p>	<p>Dans cette leçon, nous allons décrire le fonctionnement de la couche physique de Wi-Fi.</p> <p>Il est à noter que depuis 20 ans qu'il existe, le Wi-Fi a évolué pour s'adapter aux besoins des utilisateurs et ceci principalement à travers l'amélioration des techniques utilisées au niveau de sa couche physique.</p> <p>Nous ne pouvons malheureusement pas décrire toutes ces techniques mais nous allons présenter quelques solutions innovantes utilisées dans les versions les plus récentes de Wi-Fi.</p>
 <p>Objectives</p> <ul style="list-style-type: none"> ○ Signal attenuation mitigation ○ Frequency band optimization ○ Modulation techniques <p>bitrates</p>	<p>Nous allons d'abord décrire le phénomène d'atténuation du signal dont toutes les transmissions sans fils souffrent et expliquer comment les nouvelles versions de Wi-Fi arrivent à contourner ce problème.</p> <p>Nous allons ensuite expliquer comment, à travers l'utilisation optimisée de la bande de fréquence et l'implémentation de techniques de modulation efficace, il est possible pour la couche physique de Wi-Fi d'offrir de débits de plus en plus importants.</p> <p>Nous commençons d'abord par décrire le phénomène l'atténuation du signal.</p>
 <p>Signal attenuation: path loss</p> 	<p>Quand une station A émet un signal, ce signal se propage et s'atténue avec la distance.</p> <p>Ce phénomène s'appelle affaiblissement de parcours ou "path loss" en anglais et il est illustré sur cette courbe où on représente la puissance du signal en fonction de la distance.</p> <p>Si la station réceptrice B est assez proche de A, elle va recevoir un signal de bonne qualité et donc comprendre le message que A lui a envoyé.</p> <p>Si B s'éloigne de A le signal reçu s'affaiblira de plus en plus jusqu'à ce que B ne puisse plus l'interpréter convenablement ou qu'il ne puisse même plus le recevoir.</p>

 <p>Path loss + shadowing</p>	<p>A ce phénomène d'affaiblissement de parcours vient s'ajouter le phénomène de "fading" qui est dû à la présence d'obstacles.</p> <p>La première conséquence de la présence d'obstacles est ce qu'on appelle en anglais le "shadow fading" ou le "shadowing".</p> <p>Les obstacles entre la source et la destination créent des zones d'ombre qui affectent la propagation normale du signal et créent donc des fluctuations d'un endroit à un autre.</p> <p>Le "shadowing" va donc faire que l'atténuation effective du signal ne soit pas aussi régulière que la courbe précédente l'indiquait mais qu'elle ressemblera plutôt à ce qui est indiqué dans cette nouvelle courbe.</p>
 <p>Path loss + shadowing + multi-path</p>	<p>La présence de ces obstacles va avoir un second effet qui est l'effet des chemins multiples ou "multi-path".</p> <p>En effet, quand il rencontre un obstacle le signal va être dévié et la destination va finir par recevoir plusieurs versions de ce signal qui sont plus ou moins atténuées et avec un léger décalage.</p> <p>Ceci ajoutera à l'atténuation du signal et fera que notre courbe ressemblera en pratique à cette nouvelle courbe. Ces deux derniers phénomènes le "shadowing" et le "multi-path" doivent être spécialement pris en compte lorsqu'on monte en fréquence quand on utilise la bande de fréquences de 5 giga hertz ou celle des 60 giga hertz par exemple parce que même les obstacles les plus petits vont avoir un effet sur la qualité de la communication.</p> <p>Il est donc clair que la couche physique de Wi-Fi doit faire en sorte de réduire l'effet de l'atténuation du signal lors des transmissions mais, en fait, Wi-Fi va faire plus que ça en exploitant ce phénomène et en transformant ainsi une faiblesse potentielle en une force.</p>
 <p>Mitigating signal attenuation: Use of MIMO</p> <ul style="list-style-type: none"> ◦ MIMO : Multiple-In Multiple-Out ◦ Multi-path = advantage ◦ = signal diversity => signal reconstruction 	<p>Et ce à travers l'utilisation de la technique MIMO (Multiple In Multiple Out).</p> <p>Cette technique se base sur l'existence de plusieurs antennes à la source et à la destination et elle considère que le phénomène de "multi-path" est un atout vu qu'il offre ce qu'on appelle une diversité du signal, c'est-à-dire, qui va permettre à la destination de recevoir plusieurs versions du même signal, et même si ces</p>

	<p>différentes versions sont atténuées, l'atténuation ne va pas être la même d'un signal à un autre ; il sera donc possible pour la destination de combiner ces versions pour reconstituer le signal d'origine envoyé par la source.</p>
	<p>MIMO permet aussi d'utiliser ces antennes multiples pour envoyer plusieurs flux en parallèle permettant ainsi d'augmenter la capacité de liens de communication entre la source et la destination.</p> <p>Dans la version mono utilisateur de MIMO qui est représentée ici, on n'a qu'une destination pour les flux de la source.</p>
	<p>Mais il est aussi possible d'avoir de flux destinés à plusieurs clients dans ce cas on parle de MIMO multi utilisateur.</p> <p>Pour expliquer comment la couche physique de Wi-Fi optimise l'utilisation de la bande de fréquence, nous allons expliquer le principe de base d'une des techniques de transmission les plus utilisés dans Wi-Fi qui est l'OFDM (Orthogonal Frequency-Division Multiplexing).</p>
	<p>Cette méthode se base sur le principe du multiplexage par répartition de fréquences FDM qui divise l'espace de fréquences disponibles en sous bandes de fréquence appelées sous porteuses qui sont utilisés pour envoyer les flux de données en simultané.</p> <p>Pour éviter les interférences, ces sous porteuses ne doivent pas être collées les unes aux autres mais devraient être séparées d'une étroite bande de fréquence appelée "guard band". Ceci réduit de façon très importante l'espace de fréquences qu'on peut utiliser pour transférer les informations des utilisateurs.</p>
	<p>OFDM vient résoudre ce problème en utilisant ce qu'on appelle de fréquences orthogonales. Le principe de base est expliqué dans cette figure: bien que ces trois sous porteuses soient partiellement recouvrantes, on remarque que les pics des signaux envoyés sur chacune de ces sous porteuses correspondent à des fréquences où les signaux des sous porteuses avoisinantes s'annulent. On peut ainsi optimiser l'utilisation de la bande passante et envoyer plus de données à la fois augmentant ainsi les débits effectifs.</p>

 <h3>Objectives</h3> <ul style="list-style-type: none"> Signal attenuation mitigation <ul style="list-style-type: none"> MIMO Frequency band optimization <ul style="list-style-type: none"> OFDM Modulation techniques <ul style="list-style-type: none"> PSK QAM <p>↑ bitrates</p>	<p>L'utilisation de MIMO et d'OFDM permettent d'augmenter les débits dans Wi-Fi mais ce ne sont pas les seuls mécanismes prévus pour cela.</p> <p>En effet, les techniques de modulation utilisées par la couche physique de Wi-Fi qui sont PSK et QAM sont destinées à optimiser l'envoi des données et permettent donc d'améliorer les vitesses de transmission.</p>
 <h3>Modulation: Phase Shift Keying (PSK)</h3> <p>Binary PSK (BPSK) 1 bits/symbol</p> 	<p>Dans la version basique de PSK, qui est le PSK binaire (BPSK), et qui est représenté dans cet exemple, on peut utiliser un signal de face 0 degré pour représenter un 0, et un signal de 180 degrés pour représenter 1, cela donne donc la forme suivante au message : 0-1-1-0-1.</p> <p>Dans le PSK binaire il s'agit donc de faire varier la phase de 180 degrés ce qui nous permet de coder un bit par symbole, on a donc un 0 ou un 1.</p>
 <h3>Modulation: Phase Shift Keying (PSK)</h3> <p>Binary PSK (BPSK) 1 bits/symbol Quadrature PSK (QPSK) 2 bits/symbol</p> 	<p>Si on veut coder deux bits par symbole on doit donc passer au PSK en quadrature (QPSK) où il ne s'agit plus de faire varier la phase de 180 degrés mais plutôt de la faire varier de 90 degrés. Comme indiqué dans cet exemple pour représenter les bits 1-1 on envoie un signal de phase 45 degrés 1-0 va donc correspondre à un chiffre de 90 degrés et donc à une phase de 135 degrés et ainsi de suite.</p> <p>Donc même si on ne change rien au niveau de la bande passante il est possible de doubler les débits rien qu'en utilisant en QPSK au lieu de BPSK parce que chaque symbole représente désormais deux bits au lieu d'un seul.</p>
 <h3>Quadrature Amplitude and phase Modulation (QAM)</h3> <p>16-QAM 4 bits/symbol</p>  <p>*same phase : 45° *r amplitude</p>	<p>On peut faire encore mieux avec la technique QAM (« Quadrature Amplitude and phase Modulation ») qui joue sur les variations aussi bien de la phase que de l'amplitude du signal ce qui permet de coder plus de bits par symbole.</p> <p>Cet exemple présente la technique 16-QAM qui permet de coder 4 bits par symbole.</p> <p>On peut voir par exemple que les bits 1-1-0-1 et 1-0-0-0 ont la même phase qui est de 45 degrés mais pas la même amplitude, 1-0-0-0 va donc être codé avec un signal de phase 45 degrés et de forte amplitude alors que 1-1-0-1 va être codé avec un signal toujours de 45 degrés mais de faible amplitude.</p>

 <p>Quadrature Amplitude and phase Modulation (QAM)</p> <div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> <p>64-QAM 6 bits/symbol</p>  </div> <div style="text-align: center;"> <p>256-QAM 8 bits/symbol</p>  </div> </div>	<p>Le même principe peut être appliqué pour mettre en œuvre les techniques 64-QAM et 256-QAM qui permettent de coder, respectivement, 6 et 8 bits par symbole.</p>
 <p>Summary</p> <ul style="list-style-type: none"> ○ Mitigation of the effects of signal attenuation <ul style="list-style-type: none"> • MIMO ○ Frequency band optimization <ul style="list-style-type: none"> • OFDM ○ Increasing bitrates: modulation techniques <ul style="list-style-type: none"> • PSK • QAM 	<p>Dans cette leçon nous avons expliqué le phénomène d'atténuation du signal et expliqué comment la technique MIMO l'exploite ; nous avons ensuite expliqué comment le principe d'OFDM permet d'optimiser l'utilisation de la bande de fréquence ; enfin, nous avons présenté les techniques de modulation PSK et QAM et illustré comment ces techniques sont utilisées pour augmenter les débits.</p>



MOOC Réseaux Locaux

Le réseau local Wi-Fi

La méthode d'accès CSMA/CA

Objectifs

Cette leçon a pour but de décrire et justifier le fonctionnement de la méthode d'accès de Wi-Fi.

Prérequis

Connaissance des réseaux locaux, de la notion de méthode d'accès. Connaissance de base de Wi-Fi.

Connaissances

Principes et fonctionnement de la méthode d'accès CSMA/CA.

Compétences




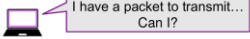

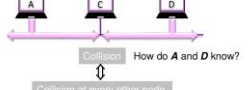

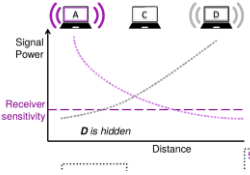
Comprendre le fonctionnement de la méthode d'accès CSMA/CA.

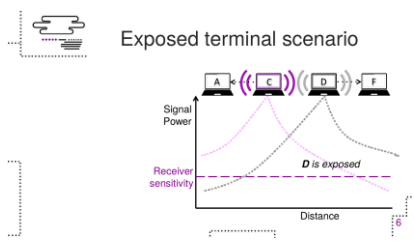
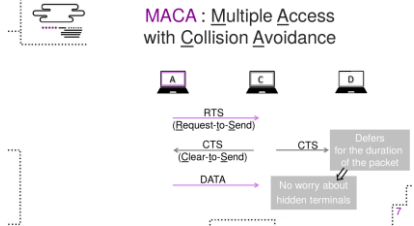
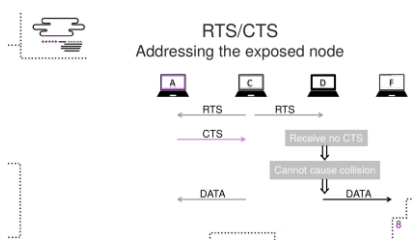
Évaluation des connaissances

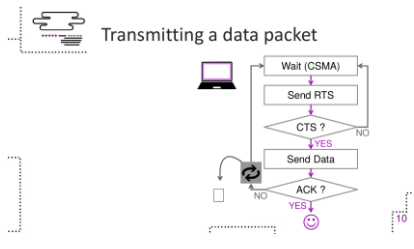
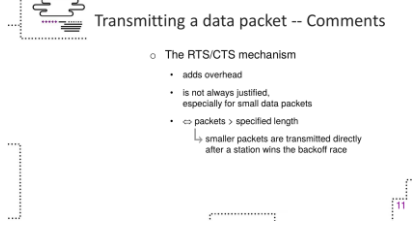
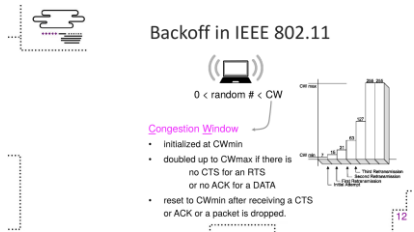
Décrire la méthode CSMA/CA.

Évaluation des compétences

Analyser sur un scénario le fonctionnement de la méthode CSMA/CA.

 <p>Wi-Fi Wi-Fi MAC layer</p> <p>Gentian JAKLLARI</p>	<p>Cette leçon est consacrée à la couche MAC du Wi-Fi.</p>
 <p>Objectives</p> <ul style="list-style-type: none"> How the wireless medium changes the channel access problem? Hidden/exposed terminal problem How problems are addressed by Wi-Fi standard (IEEE 802.11)? 	<p>Et elle a trois objectifs :</p> <ul style="list-style-type: none"> Comprendre comment le lien radio impacte la couche MAC Comprendre le problème du terminal caché et celui du terminal exposé Comprendre la solution retenue par le standard du Wi-Fi
 <p>Sharing a common medium</p>  <p>Ethernet \Rightarrow CSMA/CD congestion at the receiver = congestion at the transmitter (Just have to wait a little)</p>	<p>Quand il s'agit de partager un support commun, la question pour un nœud est de savoir s'il peut émettre.</p> <p>La couche MAC d'Ethernet a résolu cette question en utilisant le protocole CSMA/CD. Cependant, ce protocole suppose que la congestion au récepteur est exactement la même que la congestion à l'émetteur (il suffit juste d'attendre un peu).</p>
 <p>Sharing a wired medium</p>  <p>Collision How do A and D know? Collision at every other node</p> <ul style="list-style-type: none"> Signal power levels: everywhere almost the same Avoid detect collisions: relying on what it is receiving (CSMA/CD) 	<p>Considérons un réseau Ethernet simple avec 3 nœuds : une collision se produit en C ; comment A et B le savent-ils ?</p> <p>Il y a une collision au niveau du récepteur C si, et seulement si, il y a une collision sur chaque autre nœud.</p> <p>Pourquoi ? Parce que les niveaux de puissance du signal sont presque partout les mêmes.</p> <p>Un émetteur peut éviter et / ou détecter des collisions en se fondant simplement sur ce qu'il reçoit.</p>
 <p>Sharing a wireless medium Hidden terminal scenario</p>  <p>Signal Power Receiver sensitivity Distance D is hidden</p>	<p>Considérons les mêmes stations qui utilisent maintenant les communications sans fil .</p> <p>Comme vous pouvez voir sur l'image, les niveaux de puissance du signal ne sont pas partout les mêmes en raison du «pathloss» C peut recevoir A et D mais A ne peut pas recevoir D. Au moment où le signal de D (la courbe verte sur l'image) atteint A, il est trop faible pour être décodé.</p> <p>Si A écoute le support pendant que D transmet il ne détecte</p>

	<p>rien et il finit par transmettre, ce qui est la mauvaise décision. On dit que D est caché pour A.</p>
<p>Exposed terminal scenario</p> 	<p>Considérons maintenant un scénario avec quatre stations</p> <p>Si C et D transmettent au même moment à A et à F, respectivement, il n'y aura pas de collisions. Pourquoi? Plaçons nous sur la station A (et c'est pareille pour F): En apparence, A reçoit deux signaux, celui de C et celui de D. Sauf que le signal de D est très faible et au-dessous du seuil de sensibilité de A et n'empêche pas A de décoder le signal de C.</p> <p>Cependant, si la station C commence à émettre en premier, le protocole CSMA empêcherait D d'émettre, vu que le signal de C est au-dessus du seuil de sensibilité quand il atteint D, même si cela n'aurait pas provoqué une collision.</p> <p>On dit que D est "exposé" à C.</p>
<p>MACA : Multiple Access with Collision Avoidance</p> 	<p>Nous présentons maintenant MACA, un protocole conçu pour aborder les limites de la CSMA et qui consiste à envoyer des paquets courts pour éviter des collisions.</p> <p>Dans cet exemple, A souhaite envoyer un paquet à C. Avant de transmettre le paquet de données, il transmet un paquet court RTS</p> <p>C répond avec un CTS.</p> <p>D reçoit le CTS et, donc, retarde sa transmission.</p> <p>Enfin, A transmet le paquet de données à C sans collision.</p>
<p>RTS/CTS Addressing the exposed node</p> 	<p>MACA évite aussi le problème de terminal exposé. Dans cet exemple, C souhaite envoyer un paquet à A. Avant de transmettre le paquet de données, il transmet un RTS à A.</p> <p>A répond avec un CTS.</p> <p>D reçoit le RTS mais pas le CTS, il ne peut pas causer une collision, il est donc libre de transmettre au nœud F.</p>
<p>IEEE 802.11 MAC</p> <ul style="list-style-type: none"> CSMA + MACA ⇒ CSMA/CA <ul style="list-style-type: none"> CSMA before transmitting an RTS ARQ: Automatic Repeat reQuest <ul style="list-style-type: none"> The recipient of data packet sends an ACK to the sender It's necessary because of the high channel errors 	<p>La norme IEEE a finalement décidé de faire un compromis et de combiner CSMA avec MACA</p> <p>Les nœuds écoutent le support avant d'utiliser les paquets RTS/CTS.</p> <p>De plus, pour améliorer la fiabilité, elle a inclus un protocole ARQ.</p>

 <p>Transmitting a data packet</p>	<p>Pour transmettre un paquet de données, une station doit d'abord attendre que le canal soit libre, puis utiliser la procédure du « Backoff » pour gagner le droit de transmettre. Une fois qu'il a acquis le droit de transmettre, il envoie un RTS au récepteur. S'il reçoit un CTS, il envoie directement le paquet de données. Sinon il faudra tout recommencer</p> <p>Enfin, la réception d'un acquittement conclut la transmission du paquet. En cas d'échec, cette procédure est répétée un nombre limité de fois. Le paquet est abandonné si malgré les répétitions la station n'a pas reçu d'acquittement.</p>
 <p>Transmitting a data packet -- Comments</p> <ul style="list-style-type: none"> o The RTS/CTS mechanism <ul style="list-style-type: none"> • adds overhead • is not always justified, especially for small data packets • packets > specified length <ul style="list-style-type: none"> ↳ smaller packets are transmitted directly after a station wins the backoff race 	<p>Il faut dire que le mécanisme RTS / CTS ajoute du surcoût et n'est pas toujours justifié, en particulier pour les petits paquets de données. C'est pourquoi la norme a introduit un attribut qui permet de configurer une station afin d'utiliser le RTS/CTS uniquement pour les paquets plus grands qu'une longueur spécifiée. Les paquets plus petits sont transmis directement après qu'une station gagne la course du « backoff ». Dans ce cas nous faisons du CSMA pur.</p>
 <p>Backoff in IEEE 802.11</p> <p>$0 < \text{random \#} < \text{CW}$</p> <p>Congestion Window</p> <ul style="list-style-type: none"> • initialized at CWmin • doubled up to CWmax if there is no CTS for an RTS or no ACK for a DATA • reset to CWmin after receiving a CTS or ACK or a packet is dropped. 	<p>La procédure du « backoff » que nous venons d'invoquer est très similaire à celle utilisée par Ethernet. En particulier, une station sélectionne un nombre aléatoire entre 0 et une valeur donnée, que nous appelons la fenêtre de congestion, et elle effectue un décompte jusqu'à 0. Le moment où la valeur atteint 0, la station transmet.</p> <p>Bien évidemment, la valeur de la fenêtre de congestion est cruciale. Si la valeur est très petite, il y a de bonnes chances que plusieurs stations sélectionnent la même valeur de « backoff ». Si elle est trop grande, on risque de sous-utiliser le canal. Le problème est que, dans un système distribué, on ne sait jamais combien de stations veulent transmettre. Par conséquent, on utilise une procédure simple.</p> <p>La fenêtre de congestion est initialisée à une valeur minimale et elle est doublé jusqu'à la valeur maximale s'il n'y a pas de CTS pour un RTS ou s'il n'y a pas d'ACK pour un paquet de données. Elle est remise à la valeur minimale après avoir reçu un CTS ou un ACK ou lorsque un paquet est abandonné</p>



Summary

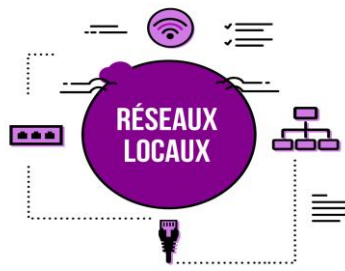
- The nature of the wireless channel makes the MAC problem fundamentally different
 - Hidden/Exposed terminal problem
- RTS/CTS exchange can help address the hidden terminal problem
- IEEE 802.11 CSMA/CA: combination of CSMA with RTS/CTS



Pour conclure, nous avons vu comment la nature du lien radio rend le partage du support fondamentalement différent. Elle introduit, en particulier, le problème du terminal caché et celui du terminal exposé.

Nous avons également vu en quoi l'échange de paquets RTS / CTS peut aider à résoudre le problème du terminal caché et celui du terminal exposé.

Finalement, nous avons observé que la norme IEEE 802.11 a décidé de faire un compromis et de combiner CSMA avec MACA.



MOOC Réseaux Locaux

Le réseau local Wi-Fi

Les modes de communication

Objectifs

Cette leçon a pour but de présenter les modes de communication de Wi-Fi.

Prérequis

Connaissance des réseaux locaux, notions de Wi-Fi.

Connaissances

Les différents modes de communication de Wi-Fi.

Compétences







Faire la différence entre les modes Ad Hoc et avec infrastructure.

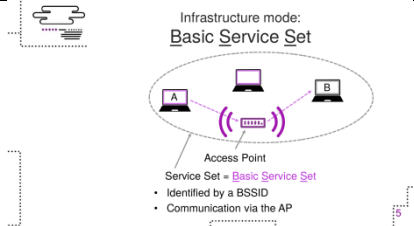
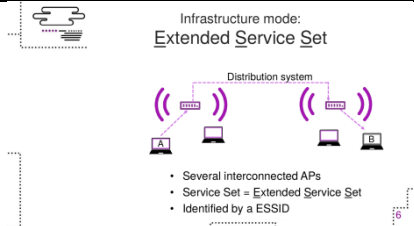
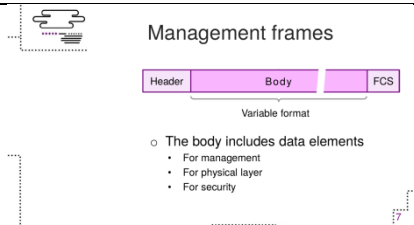
Évaluation des connaissances






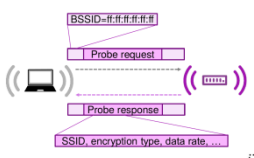

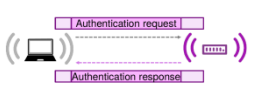

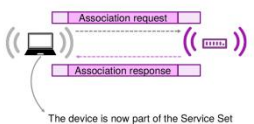


Décrire le fonctionnement des modes de communication de Wi-Fi.


Évaluation des compétences

Analyser les différences entre les modes de communication de Wi-Fi.

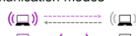


 <p>Wi-Fi <i>Communication modes</i></p> <p>Emmanuel Chaput</p>	<p>Cette leçon est consacrée aux modes de communication de Wi-Fi.</p> <p>Quels en sont les objectifs ?</p>
 <p>Objectives</p> <ul style="list-style-type: none"> o Wi-Fi communication modes o Basic mechanisms 	<p>Il s'agit de vous présenter les différents modes de communication de Wi-Fi et de vous expliquer les principes de base de leur fonctionnement.</p>
 <p>Wi-Fi modes</p> <ul style="list-style-type: none"> o Ad Hoc mode  <ul style="list-style-type: none"> • Direct communications • Simple and efficient for host to host communications o Infrastructure mode <ul style="list-style-type: none"> • Most widely used  	<p>Lorsque des machines équipées de Wi-Fi veulent communiquer, le premier réflexe que l'on peut avoir c'est de les faire communiquer directement entre elles comme sur la figure que vous voyez ici.</p> <p>Ce mode de fonctionnement existe dans Wi-Fi : c'est le mode « Ad Hoc ». Il est très simple et relativement efficace lorsqu'il s'agit de faire communiquer des machines deux à deux entre elles.</p> <p>En revanche, le mode le plus généralement utilisé est le mode infrastructure dans lequel on utilise un équipement supplémentaire : « l'access point » ou point d'accès, qui aura pour but d'organiser les communications et de fournir des services supplémentaires.</p> <p>L'ensemble des machines qui communiquent entre elles dans un même réseau est appelé un « service set » et il est décrit par un identifiant qualifié de SSID.</p>
 <p>What is an <u>A</u>ccess <u>P</u>oint ?</p> <ul style="list-style-type: none"> o Specific device <ul style="list-style-type: none"> • Communicates with all devices • Can provide services o Can communicate with other APs o Can communicate with a router <ul style="list-style-type: none"> • Thus providing Internet access 	<p>Qu'est-ce que c'est qu'un point d'accès ? C'est un équipement spécifique, tel que celui-ci par exemple, qui va communiquer avec toutes les machines et leur fournir un certain nombre de services.</p> <p>Il va pouvoir lui-même communiquer également avec d'autres points d'accès voire avec des routeurs de sorte à permettre de fournir un accès Internet par exemple.</p> <p>Il est même généralement implanté dans le même équipement tel que celui-ci avec un routeur, un commutateur Ethernet ou d'autres types de fonctionnalités.</p>



 <p>Infrastructure mode: Basic Service Set</p> <ul style="list-style-type: none"> • Identified by a BSSID • Communication via the AP 	<p>Dans sa version la plus simple, le mode infrastructure est constitué d'un point d'accès et d'un ensemble de machines. Elles font donc partie d'un service set qualifié de BSS pour « Basic Service Set » et caractérisé par un BSSID qui est défini par le point d'accès. Les machines communiquent au travers de ce point d'accès. Cela signifie que lorsque la machine A souhaite envoyer une trame à destination de la machine B, elle envoie cette trame au point d'accès (et ce au travers de la méthode d'accès CSMA/CA) et le point d'accès, à son tour, envoie la trame à destination de la machine B (à nouveau au travers de la méthode d'accès CSMA/CA).</p>
 <p>Infrastructure mode: Extended Service Set</p> <ul style="list-style-type: none"> • Several interconnected APs • Service Set = Extended Service Set • Identified by a ESSID 	<p>Il est possible d'étendre géographiquement un tel service set en interconnectant, au travers d'un système de distribution, plusieurs points d'accès.</p> <p>Le fonctionnement reste le même : lorsque la machine A souhaite envoyer une trame à destination de la machine B, elle l'envoie d'abord à son point d'accès, qui la fait suivre, au travers du système de distribution au point d'accès qui dessert la machine finale. Ce dernier transmet, bien entendu la trame à sa destinatrice.</p> <p>Ici vous remarquerez que le réseau s'appelle cette fois-ci un ESS, un « Extended Service Set », caractérisé, évidemment, par un ESSID. ESSID qui, attention, bien entendu, doit être commun à tous les points d'accès faisant partie de ce même ESS.</p>
 <p>Management frames</p> <ul style="list-style-type: none"> ○ The body includes data elements <ul style="list-style-type: none"> • For management • For physical layer • For security 	<p>Pour faire fonctionner tout cela, il y a besoin de signalisation, et des trames spécifiques ont donc été définies pour cela. Les trames de gestion, ou « management frames », ont une structure, présentée ici, qui est relativement classique, avec un entête, un enqueue et un contenu.</p> <p>Ce contenu a une géométrie variable car différents type d'information peuvent être véhiculés. Nous allons ici nous intéresser aux trames de gestion qui vont servir à gérer les service sets. Mais des trames peuvent également servir à la gestion de la couche physique (quel type de modulation va être utilisé, quel débit va être accessible) ou encore à la sécurité.</p>

 <p>Infrastructure mode: beacon frames</p>  <ul style="list-style-type: none"> o Sent on a regular basis by the AP o Contains SSID o Contains SS specifications <p>10</p>	<p>Comment est-ce qu'un point d'accès va identifier un réseau de façon à le rendre connu, public, pour des machines arrivantes ? Il va régulièrement envoyer des trames de management : des trames de « beacon ». Il va envoyer ces trames sur la base de une trame toutes les 100ms environ. Dans ces trames, il y aura un certain nombre d'informations permettant de décrire le service set et l'ensemble des caractéristiques de ce service set.</p>
 <p>Joining a network</p>  <ul style="list-style-type: none"> o Probe the network o Authenticate with the AP o Associate to the network <p>10</p>	<p>Comment, maintenant, une station qui veut rejoindre un réseau, va procéder ? Lorsqu'elle va arriver, elle va passer par un certain nombre d'étapes. Elle va d'abord sonder le réseau, puis elle va s'authentifier auprès du point d'accès pour enfin s'associer au réseau.</p>
 <p>Probe the network</p>  <p>10</p>	<p>Comment se déroule la phase de scrutation du réseau ? La station va envoyer des trames « Probe request » afin de demander à découvrir des réseaux. À ces trames, les points d'accès vont pouvoir répondre en transmettant une trame « Probe Response ». Je dis bien les points d'accès car plusieurs de ces points d'accès peuvent être à portée de la machine et peuvent lui envoyer des trames « Probe Response ». À elle de choisir, en fonction des caractéristiques des réseaux qui lui sont proposés (en fonction par exemple de la puissance qu'elle reçoit) elle va choisir un de ces point d'accès.</p>
 <p>Authenticate with the AP</p>  <ul style="list-style-type: none"> o More complex (and safer) procedures can be implemented <p>11</p>	<p>Elle va ensuite passer à une phase d'authentification. Là encore, un mécanisme relativement simple à la base : elle va envoyer une trame de requête et le point d'accès va lui répondre au travers d'une trame de réponse d'authentification. Des procédures plus complexes peuvent être mises en œuvre. Nous n'en parlerons évidemment pas ici.</p>
 <p>Associate the network</p>  <p>12</p>	<p>Enfin la station va pouvoir s'associer au réseau. Elle va pour cela envoyer une trame d'association à laquelle, encore une fois, le point d'accès va répondre. À partir de là, la station peut communiquer, elle fait partie du service set.</p>
 <p>Ad Hoc mode</p>  <ul style="list-style-type: none"> o Direct communications o Independent BSS <ul style="list-style-type: none"> • Identified by a IBSSID <p>13</p>	<p>Dans le mode Ad Hoc les choses sont sensiblement différentes, bien sûr, puisqu'il n'y a pas de point d'accès. Toutes les machines vont pouvoir communiquer directement entre elles sur la seule base de l'identifiant du réseau. On parle ici de IBSSID pour « Independent Basic Service Set Identifier ».</p>

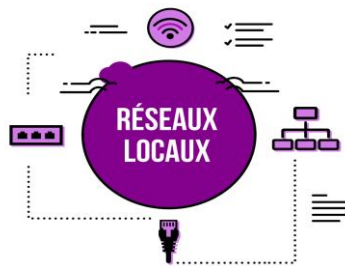


Summary

- Several communication modes
 - Ad Hoc 
 - Infrastructure 
- Description of the management
 - Specific frames



Qu'avons-nous dit dans cette leçon ? Nous avons présenté les différents modes de communication de Wi-Fi : le mode Ad Hoc et le mode avec infrastructure et nous avons présenté simplement leur fonctionnement élémentaire au travers des trames de gestion.



MOOC Réseaux Locaux

Le réseau local Wi-Fi

La sécurité dans Wi-Fi

Objectifs

Cette leçon a pour but de présenter les mécanismes de base de sécurisation du réseau local Wi-Fi.

Prérequis

Bonne connaissance des réseaux locaux.

Connaissances

Principaux enjeux et principales méthodes de sécurisation des réseaux locaux sans fils.

Compétences






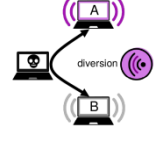

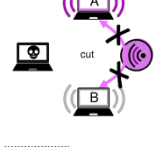

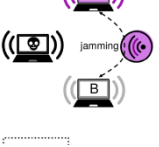

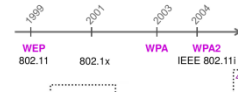
Analyser la sécurité d'un réseau local sans fil.


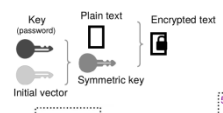

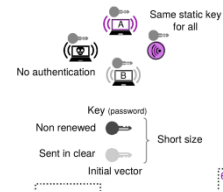

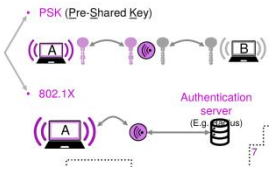
Évaluation des connaissances

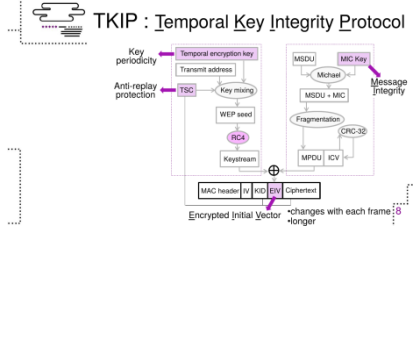
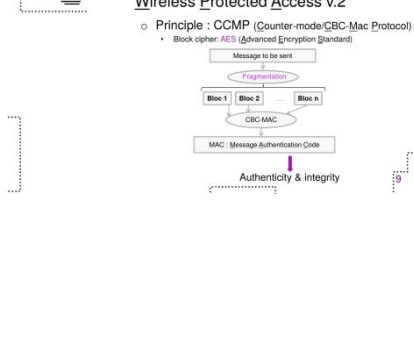
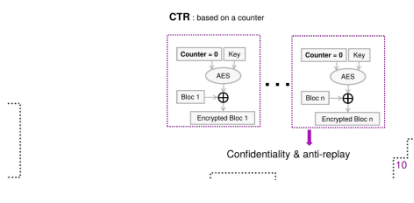
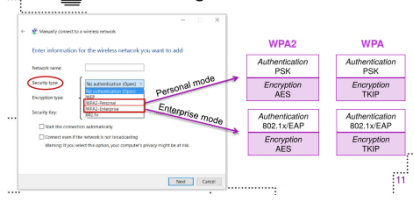
Décrire les principes de la sécurisation de Wi-Fi.


Évaluation des compétences

Donner les principaux éléments de sécurité de Wi-Fi.

 <p>Wi-Fi Wi-Fi security</p> <p>Samiha Ayed</p>	<p>Dans cette vidéo, j'aborde avec vous la sécurité des réseaux Wi-Fi : quelles sont les vulnérabilités associées à ces réseaux, les solutions proposées ainsi que leurs limites ?</p>
 <p>Objectives</p> <ul style="list-style-type: none"> What vulnerabilities? What solutions? Within what limits? 	<p>En plus des problèmes de sécurité des réseaux filaires, les réseaux sans fils rajoutent encore des vulnérabilités à cause de leur utilisation des ondes radios qui peuvent être captées par tout le monde. Il suffit juste qu'une machine entre dans la portée d'un point d'accès.</p>
 <p>Vulnerabilities of Wi-Fi</p> 	<p>Si une machine malveillante entre dans la zone de propagation, elle peut présenter plusieurs risques si le réseau n'est pas sécurisé.</p> <p>Le premier risque est l'interception de données, consistant à écouter passivement les transmissions.</p>
 <p>Vulnerabilities of Wi-Fi</p> 	<ul style="list-style-type: none"> L'attaquant peut même détourner les connexions pour que toutes les communications passent par lui.
 <p>Vulnerabilities of Wi-Fi</p> 	<p>Une attaque de déni de service peut également rendre le réseau inutilisable en envoyant des commandes factices et en coupant les communications entre les différentes machines.</p>
 <p>Vulnerabilities of Wi-Fi</p> 	<p>Un dernier exemple de ces risques est le brouillage des transmissions consistant à émettre des signaux radio pour produire des interférences et ainsi perturber le fonctionnement du réseau.</p>
 <p>Security in Wi-Fi networks</p> <p>Authentication authorised users only</p> <p>Encryption secure communication</p> 	<p>Pour remédier à ces risques, et assurer la sécurité des réseaux Wi-Fi, plusieurs travaux ont eu lieu. Ces travaux se basent sur</p> <ul style="list-style-type: none"> des mécanismes d'authentification pour limiter les accès au réseau Wi-Fi ; des mécanismes de chiffrement pour crypter les communications.

	<p>Le résultat de ces travaux a donné naissance à trois mécanismes de sécurité</p> <ul style="list-style-type: none"> le WEP, apparu en 1999, est la première tentative qui a essayé de sécuriser la norme 802.11. Ce protocole n'a pas beaucoup résisté et a été rapidement craqué. Des outils open source existent sur internet pour casser l'algorithme en quelques secondes. Vues ses failles, le WEP a été remplacé par le WPA qui respecte la majorité de la norme IEEE 802.11i et a été prévu comme une solution intermédiaire en attendant que la norme IEEE 802.11i soit terminée. En 2004, il y a eu la sortie officielle de la norme IEEE 802.11i dédiée à la sécurité du Wi-Fi et présentant le WPA2.
<p> WEP : Wired Equivalent Privacy</p> <p>o Principe :</p> <ul style="list-style-type: none"> RC4 encryption \Rightarrow privacy CRC (Cyclic Redundancy Check) \Rightarrow message integrity 	<p>Le WPA et le WPA2 ont bénéficié de l'apparition de la norme d'authentification 802.1x. Si on regarde un peu plus en détail les spécificités de ces trois mécanismes, on trouve que le WEP se base principalement sur l'algorithme de chiffrement par flot RC4, connu pour sa simplicité, pour crypter les communications et assurer leur confidentialité. Il se base également sur le CRC, qui est le champ de contrôle de redondance cyclique pour assurer l'intégrité des messages.</p> <p>Le WEP utilise une clef de chiffrement (qui est votre mot de passe) à laquelle est concaténé un vecteur d'initialisation formant ainsi la clef symétrique WEP. Une opération logique XOR est, par la suite, appliquée entre la clef WEP générée et le message à chiffrer pour produire le message crypté.</p>
<p> WEP : limits</p> 	<p>La grande faiblesse du protocole WEP provient de la taille et de la gestion de ces clefs. En fait, la même clef WEP est utilisée par le point d'accès et toutes les stations se connectant à ce point d'accès. De plus, le WEP n'assure aucune authentification : il considère qu'il suffit à un utilisateur qui rejoint le réseau de prouver sa possession de la clef partagée, même s'il l'a obtenue frauduleusement pour qu'il soit authentifié.</p> <p>En outre, lors de la création de la clef WEP, la clef de chiffrement n'est pas renouvelée. Le vecteur d'initialisation est envoyé en clair et leurs tailles respectives sont considérées petites.</p>
<p> WPA / WPA2 authentication methods</p> 	<p>Pour remédier à ces failles, WPA et WPA2 ont introduit l'utilisation de deux méthodes d'authentification</p> <ul style="list-style-type: none"> La première est l'authentification par la clef symétrique, qui est un secret partagé entre la station et le point d'accès. La deuxième méthode, c'est l'authentification 802.1x. Dans ce cas, le point d'accès sert de relai entre la station

 <p>TKIP : Temporal Key Integrity Protocol</p>	<p>et un serveur d'authentification comme RADIUS.</p> <p>Concernant les méthodes de chiffrement, le WPA utilise le protocole TKIP qui se base, comme le WEP, sur l'algorithme RC4. Le WPA élimine les failles du WEP en changeant périodiquement la clef. Il renforce l'intégrité des messages en ajoutant un code d'intégrité de message. Il assure une protection contre les attaques par rejeu en définissant un compteur de séquence sur les paquets. Finalement, il agit sur le vecteur d'initialisation qui change avec chaque trame, a une taille plus importante, et il est envoyé crypté.</p>
 <p>WPA2 Wireless Protected Access v.2</p> <ul style="list-style-type: none"> Principe : CCMP (Counter-mode/CBC-Mac Protocol) Block cipher: AES (Advanced Encryption Standard) 	<p>Le WPA2 peut également implanter le protocole TKIP pour rester compatible avec les anciens équipements. Il implante essentiellement le protocole CCMP. Avec ce protocole, WPA2 a ramené une grande innovation en se basant sur le chiffrement symétrique par bloc au lieu du chiffrement par flot. Il a donc remplacé le RC4 par l'AES qui est beaucoup plus robuste. Tous les équipements conçus à partir de 2006 supportent le WPA2/AES. L'algorithme CBC-Mac est appliqué sur les différents blocs d'un message pour générer un code d'authenticité qui assure l'intégrité des messages.</p>
 <p>WPA2 Wireless Protected Access v.2</p> <p>CTR : based on a counter</p>	<p>L'algorithme CTR est utilisé pour crypter ces différents blocs. La protection anti rejeu est assurée par l'utilisation d'un compteur.</p>
 <p>Configuration modes</p>	<p>La combinaison de ces mécanismes d'authentification et de chiffrement a donné lieu aux deux modes de configuration que vous pouvez rencontrer lors de la configuration d'un réseau Wi-Fi.</p> <p>Je prends ici l'exemple de configuration en utilisant Windows. Comme vous pouvez le voir, vous avez l'option WPA2 personnel et WPA2 entreprise. Il est conseillé de choisir le mode personnel si vous configurez un réseau domestique. Cette configuration se base sur le TKIP et l'authentification par clef partagée. Le mode entreprise, conseillé pour les utilisations professionnelles, assure un chiffrement AES et une authentification 802.1x.</p> <p>Le WPA propose également ces deux modes de configuration.</p>

 <p>Conclusion</p> <p>✗ WEP</p> <p>✓ WPA2 with AES = The more secure</p> <p>Recommendations: Use IPSec Use VPN</p>	<p>Pour conclure, vous devez retenir que le</p> <ul style="list-style-type: none"> • WEP est à éviter, même s'il est encore proposé dans les configurations des réseaux ; • le WPA2 avec l'algorithme AES reste le protocole le plus sûr ; • si jamais vous avez des besoins critiques en sécurité, sachez que vous pouvez accompagner le protocole WPA2 par l'utilisation de IPSec ou encore l'utilisation de VPN (réseaux privés virtuels).
---	--