

Chapitre 3

Architecture en couches et technologies réseaux impactant le Wi-Fi

3-1

Version – 09/2017

Objectifs du chapitre

- ➲ Dans ce chapitre, nous allons étudier
 - La structure en couches WLAN 802.11
 - Les différentes technologies radio 802.11
 - La méthode d'accès CSMA/CA
 - Les normes :
 - 802.1D (STP),
 - 802.1q (VLAN),
 - 802.1x (et le NAP)
 - 802.3af (PoE)

3-2

Les réseaux Ethernet



Architecture en couches

La couche physique et les sous-couches

Les technologies radio 802.11...

La couche liaison de données et les sous-couches

CSMA/CA

Le protocole Spanning Tree

Les Vlan

Le 802.1X

Power over Ethernet (PoE)

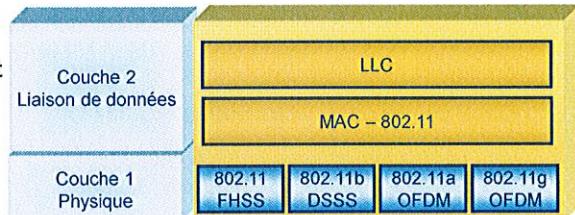
Résumé du chapitre

3-3

Les Couches 802.11

• Les standards 802.11 définissent les deux premières couches

- Couche 1 : Physique
- Couche 2 : Liaison de données



• La Couche physique

- La couche PHY définit la méthode de communication
- 802.11 dispose de différentes couches physiques
 - DSSS, utilisée par 802.11b
 - OFDM, utilisée par 802.11a et 802.11g
 - Infrarouge, spécifiée dans le standard d'origine 802.11
 - FHSS (Frequency Hopping Spread Spectrum), utilisée par le standard d'origine 802.11

• La Couche liaison de données

- Subdivisée en deux sous couches LLC et MAC
- Chaque standard 802 a une couche MAC (Media Access Control) unique
 - Commune à toutes les couches physique
 - Gère l'accès au média réseau
- MAC 802.11 gère la communication et l'accès pour les équipements sans-fil
 - Authentification
 - Secret des données (chiffrement)
 - Association à un point d'accès et transmission des messages

3-4

Les réseaux Ethernet

Architecture en couches



La couche physique et les sous-couches

Les technologies radio 802.11...

La couche liaison de données et les sous-couches

CSMA/CA

Le protocole Spanning Tree

Les Vlan

Le 802.1X

Power over Ethernet (PoE)

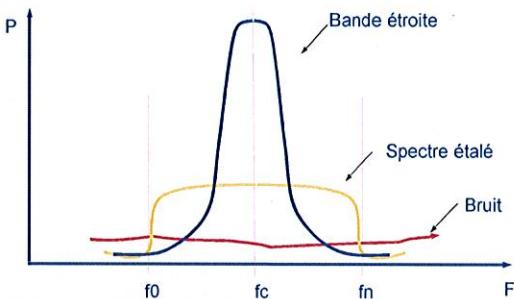
Résumé du chapitre

3-5

Technologie à étalement de spectre

Différents types de signaux

- 80% de l'énergie émise



De nombreux équipements partagent les bandes ISM, avec des interférences potentielles

L'étalement de spectre étale le signal sur tout le canal

- Permet de partager le spectre et de réduire les interférences
- A la différence des technologies traditionnelles à bande étroite (radio, TV)

L'étalement de spectre implique une technique de codage pour la transmission

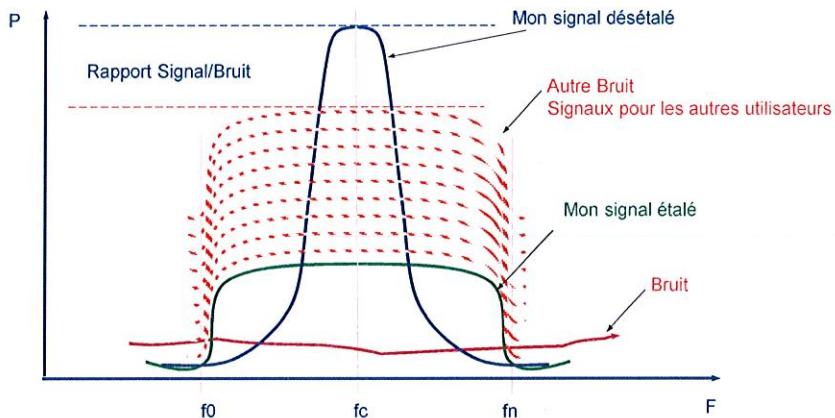
- Le signal ressemble à un bruit pour les récepteurs traditionnels à bande étroite

3-6

Technique d'étalement

• Reconnaissance des signaux

- Le signal qui m'est destiné est identique aux signaux destinés aux autres utilisateurs
- Mon code me permet de le reconnaître et le désétailler
- Le rapport Signal sur Bruit ne doit pas descendre en dessous d'un certain seuil

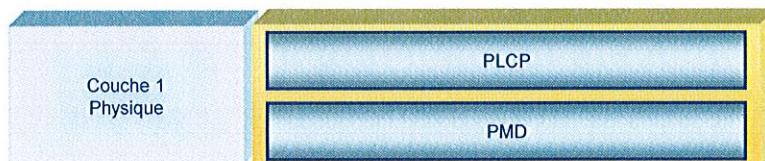


3-7

La couche physique

• La couche physique est l'interface entre la couche MAC et le support qui permet d'envoyer et de recevoir les données

- Le standard d'origine prévoit trois couches physiques
 - FHSS, DSSS et IR
- L'ajout de 802.11a et 802.11g ne modifie pas la couche MAC
- Subdivisée en deux sous-couches



- PLCP (Physical Layer Convergence Protocol) s'occupe de l'écoute du support et fournit le CCA (Clear Channel Assessment) à la couche MAC pour lui dire que le support est libre
- PMD (Physical Medium Dependent) gère l'encodage de la modulation des données

3-8

Les réseaux Ethernet

Architecture en couches

La couche physique et les sous-couches



Les technologies radio 802.11...

La couche liaison de données et les sous-couches

CSMA/CA

Le protocole Spanning Tree

Les Vlan

Le 802.1X

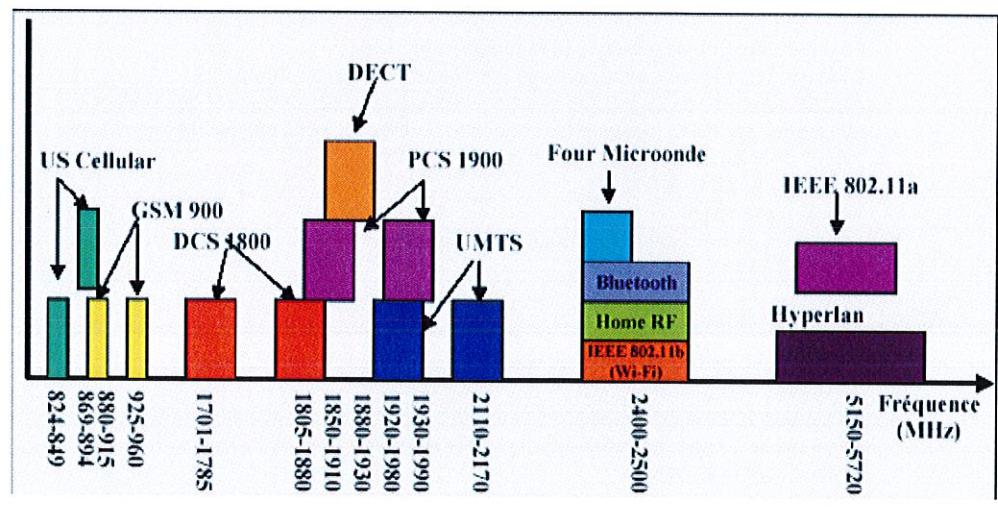
Power over Ethernet (PoE)

Résumé du chapitre

3-9

Fréquences couramment utilisées

Différents types de fréquence utilisées tous les jours

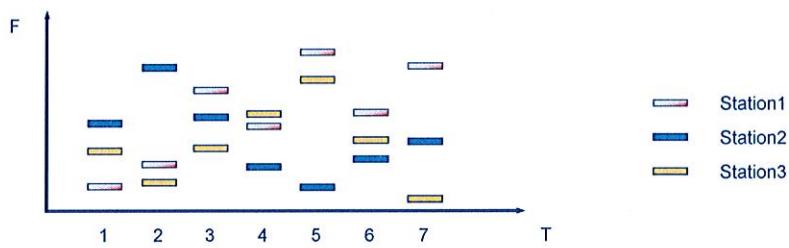


3-10

Technologie à étalement de spectre

• FHSS – Frequency Hopping Spread Spectrum – 802.11

- 79 canaux de 1 MHz
- L'émetteur et le récepteur s'accordent pour une séquence de sauts effectués sur ces 79 canaux, tous les 300 ms
- FHSS définit 3 ensembles de 26 séquences soit 78 séquences de sauts possibles
- Minimisation des collisions en cas de transmissions simultanées
- Modulation GFSK (Gaussian Frequency Phase Keying)
- Débit 1 à 2 Mb/s
- Théoriquement 26 communications simultanées (15 dans la pratique)



3-11

Fréquences 802.11b,g,a

• 802.11 ... utilisent des fréquences micro-ondes

- Utilise des bandes sans licence affectées aux domaines industriels, scientifique et médical (ISM)
 - FCC (Federal Communications Commission) aux USA
 - ETSI (European Telecommunications Standards Institute) en Europe
 - ARCEP : Autorité de Régulation des Communications Electroniques et des Postes (anciennement ART). Elle gère les conditions d'utilisations des bandes de fréquences.
 - 2,4 à 2,4835 GHz, une largeur de bande de 83,5 MHz
 - Standards 802.11b et 802.11g
 - 5,15 to 5,825 GHz
 - U-NII (Unlicensed-National Information Infrastructure)
 - Standard 802.11a

• Affectations de canaux

- Le spectre de fréquence est divisé en canaux
 - 79 canaux de 1 MHz pour 802.11
 - 14 canaux de 20 MHz sont spécifiés dans la bande ISM, pour 802.11b et 802.11g
 - 8 canaux de 20 MHz spécifiés dans la bande de 5 Ghz, pour 802.11a aux US et 19 canaux pour l'Europe
- Les numéros de canaux de la bande ISM ont été définis pour d'autres usages antérieurs au Wi-Fi

3-12

Technologie à étalement de spectre

• DSSS (Direct Sequence Spread Spectrum)

- Utilisé par les standards 802.11b (11 Mbps)
- Technique de codage CCK (Complémentary Code Keying) avec le mécanisme de modulation QPSK (Quadrature Phase Shift Keying)
- Utilise un *code d'étalement* unique
 - Chaque bit de données est représenté par une *séquence appelée chip* de 11 ou 20 bits
 - Chaque utilisateur se voit attribué une paire de codes orthogonale par rapport aux codes des voisins
- Un récepteur utilisant le code attribué par l'émetteur peut éliminer l'interférence d'autres terminaux par une fonction de corrélation

• Recouvrement de canaux

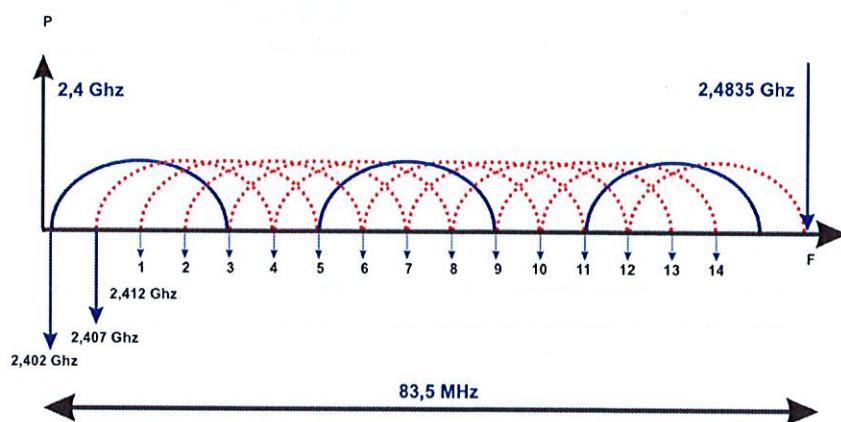
- 802.11b permet des transmissions à 11 Mbps
 - En réalité, le spectre du signal occupe une bande de + et - 10 à 15 MHz de chaque côté de la fréquence crête
 - Malheureusement, les affectations de canaux pour 802.11 n'avaient que 5 MHz d'espacement
 - En pratique, on ne peut utiliser que trois canaux à la fois
 - Par exemple les canaux 1, 7 et 13 pour éviter le recouvrement

3-13

Fréquences Wi-Fi 802.11b

• Découpage en canaux dans la bande ISM 2.4 GHz DSSS

- Etalement sur la largeur d'un canal



3-14

Fréquences radio Wi-Fi

Canaux 802.11b par pays

| N° de canal | Fréquence en GHz | Amérique du Nord | Europe | France | Japon |
|-------------|------------------|------------------|--------|--------|-------|
| 1 | 2.412 | X | X | X | X |
| 2 | 2.417 | X | X | X | X |
| 3 | 2.422 | X | X | X | X |
| 4 | 2.427 | X | X | X | X |
| 5 | 2.432 | X | X | X | X |
| 6 | 2.437 | X | X | X | X |
| 7 | 2.442 | X | X | X | X |
| 8 | 2.447 | X | X | X | X |
| 9 | 2.452 | X | X | X | X |
| 10 | 2.457 | X | X | X | X |
| 11 | 2.462 | X | X | X | X |
| 12 | 2.467 | | X | X | X |
| 13 | 2.472 | | X | X | X |
| 14 | 2.483 | | | X | X/- |

NB 1 : Jusqu'en 2007 la bande 2 400,00 à 2 446,50 MHz était partagée avec le ministère de la Défense. Depuis décembre 2003, les forces armées utilisent cette bande pour les radars de la défense anti-aérienne et pour les radars de poursuite des rampes de missiles Crotale. Le ministère s'est engagé à libérer totalement la bande ISM (Industrie, Scientifique et Médical) en 2011.

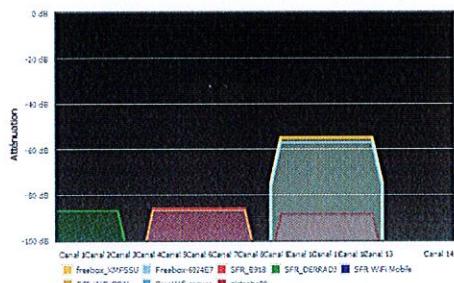
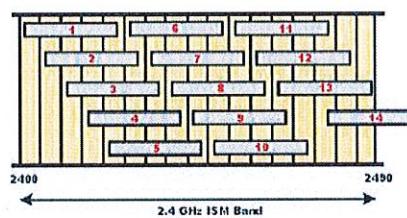
NB 2 : fin limitation de la puissance à 10mW en extérieur des canaux 8-13 en 2013

* PIRE (Puissance Isotrope Rayonnée Equivalente) < 100 mw extérieur –
EIRP en Anglais = puissance d'émission réelle du signal dans l'air : puissance de l'équipement + gain de l'antenne.

3-15

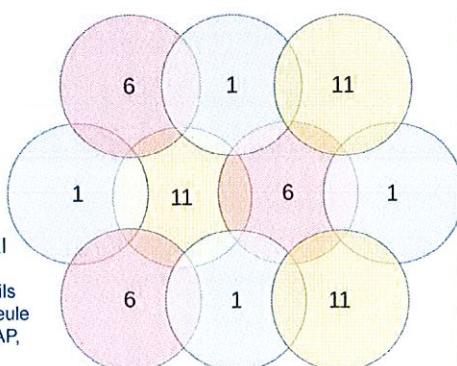
Fréquences Wi-Fi 802.11b

- Du fait du non espacement des canaux en 802.11b/g, un recouvrement est possible, amenant des perturbations



- Implémentation en « Nid d'abeilles »

- Ensemble de 3 canaux distincts
- Chaque canal ne chevauche que des canaux disjoints
- L'objectif est de disposer de la totalité du canal



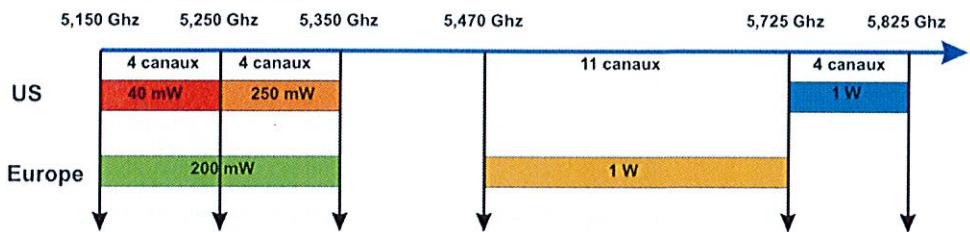
NB : On peut baisser la puissance des différents AP pour qu'ils se chevauchent qu'un petit peu, et donc rendre visible une seule AP, cela permet de bien répartir les clients sur les différents AP, avec moins de puissance radio.

3-16

Fréquences Wi-fi 5 – 802.11a

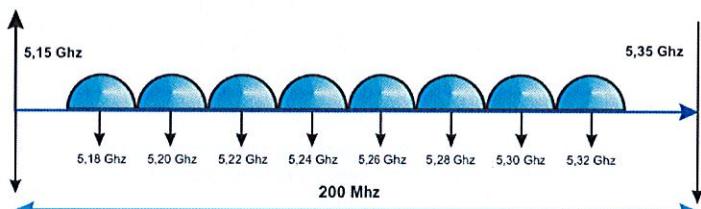
• Découpage en canaux dans la bande U-NII 5.15 GHz

- 12 canaux pour les US
- 19 canaux pour l'Europe



• Découpage en canaux dans la bande U-NII 5.15 GHz

- Les 2 premières sous-bandes U-NII 5.15-5.25 GHz et 52.5-5.35 GHz
- Puissance maximale 200 mW PIRE pour l'Europe



3-17

Fréquences radio Wi-Fi 5 (suite)

• Canaux 802.11a en France

| Bande de fréquence | Intérieur | Extérieur |
|--------------------|---|--|
| 5150-5250 MHz | 200mW | - |
| 5250-5350 MHz | 200mW si régulation, 100mW sans régulation | - |
| 5470-5725 MHz | 1W si régulation, 500mW sans régulation | 1W si régulation, 500mW sans régulation |

| Fréquences | Intérieur | Extérieur |
|---|---|--|
| UNI-1 5150 - 5250 MHz Canaux 36,40,44,48 | 200 mW (23 dB) | |
| UNI-2 5250 - 5350 MHz Canaux 52,56,60,64 | 200 mW (23 dB) Si TPC. Sinon 100mW Requiert DFS | |
| UNI-2e 5470 - 5725 MHz Canaux 100,104,108, 112,116,123,124,128, 132,138,140 | | 1W (30dB) Si TPC. Sinon 500mW Requiert DFS |
| UNI-3 5725 - 5825 MHz Canaux 149,153,157,161,165 | | 1W (30dB) |

• Canaux 802.11a aux USA

| Band | Center frequency | Channel number | Maximum power |
|--|------------------|----------------|---------------|
| U-NII low band (5150 MHz to 5250 MHz) | | | |
| | 5180 MHz | 36 | 40 mW |
| | 5200 MHz | 40 | 40 mW |
| | 5220 MHz | 44 | 40 mW |
| | 5240 MHz | 48 | 40 mW |
| U-NII medium band (5250 MHz to 5350 MHz) | | | |
| | 5260 MHz | 52 | 200 mW |
| | 5280 MHz | 56 | 200 mW |
| | 5300 MHz | 60 | 200 mW |
| | 5320 MHz | 64 | 200 mW |
| U-NII high band (for outdoor use) (5725 MHz to 5825 MHz) | | | |
| | 5745 MHz | 149 | 800 mW |
| | 5765 MHz | 153 | 800 mW |
| | 5785 MHz | 157 | 800 mW |
| | 5805 MHz | 161 | 800 mW |

<http://www.arcep.fr/index.php?id=9272#c12931>

3-18

Fréquences Wi-fi 5 – 802.11a

• Découpage canaux 802.11a par pays (exemples)

| N° de canal | Fréquence en GHz | Amérique du Nord | France | Japon |
|-------------|------------------|------------------|--------|-------|
| 36 | 5.180 | X | X * | X |
| 40 | 5.200 | X | X * | X |
| 44 | 5.220 | X | X * | X |
| 48 | 5.240 | X | X * | X |
| 52 | 5.260 | DFS | X * | DFS |
| 56 | 5.280 | DFS | X * | DFS |
| 60 | 5.300 | DFS | X * | DFS |
| 64 | 5.320 | DFS | X * | DFS |

Il résulte de la limitation sur la puissance (PIRE) que l'étendue d'un réseau constitué au moyen de la seule technologie RLAN est typiquement de quelques centaines de mètres. L'opérateur qui souhaite déployer des liaisons point à point, avec des portées non compatibles avec les limitations de puissance indiquées dans les tableaux, doit solliciter à cet effet auprès de l'Autorité une autorisation d'utilisation de fréquences dans l'une des bandes de fréquences identifiées pour cet usage.

* : Pas d'utilisation en extérieur

DFS : c'est une fonctionnalité qui permet de sélectionner une fréquence qui n'interfère pas avec certains radars (météorologiques par exemple) dans la bande de fréquence des 5 GHz

3-19

Technologie OFDM

• OFDM (Orthogonal Frequency Division Multiplexing)

- Utilisé par le standard 802.11a (54 Mbps) et 802.11g (54 Mbps)
- Divise le canal de 20 MHZ en 52 sous-canaux de 300KHz
- Les 48 premiers sous/canaux sont utilisés pour la transmission de données et les 4 derniers pour la correction d'erreurs
- Les émissions et réceptions se font dans les 48 ss/canaux de façon simultanée et sont multiplexées sur un seul canal de 20 MHz

• Wi-Fi 5 introduit un correcteur d'erreurs FEC (Forward Error Correction)

- Les données sont transmis dans les 48 ss/canaux qui utilisent une modulation appelée 64QAM (64 level Quadrature Amplitude Modulation) qui offre 1,125 Mb/s par ss/canal
- En fonction du FEC, une copie est faite sur les 4 derniers ss/canaux pour éviter une retransmission complète des données



3-20

Les réseaux Ethernet

Architecture en couches

La couche physique et les sous-couches

Les technologies radio 802.11...



La couche liaison de données et les sous-couches

CSMA/CA

Le protocole Spanning Tree

Les Vlan

Le 802.1X

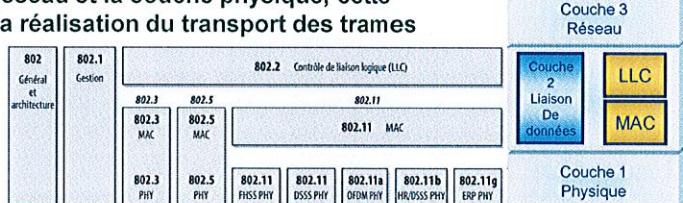
Power over Ethernet (PoE)

Résumé du chapitre

3-21

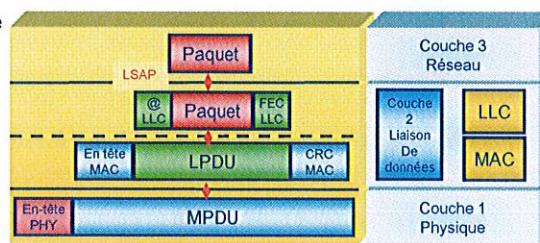
La couche liaison de données

- Située entre la couche réseau et la couche physique, cette couche a pour objectif la réalisation du transport des trames sur l'interface radio



- Deux sous couches :

- LLC (Logical Link Control) s'occupe de la structure de la trame (adresse en tête et FEC à la fin) et fournit deux fonctionnalités :
 - Contrôle de flux
 - Reprise sur erreur
- MAC (Medium Access Control) définit l'algorithme qui permet d'accéder au réseau,
 - donc permet à la carte Ethernet d'émettre sur l'interface radio sans qu'une autre carte ne le fasse en même temps
 - Évite les collisions



NB : LSAP (Logical Service Access Point) :
adressage logique pour masquer aux couches hautes les informations venant des couches basses

3-22

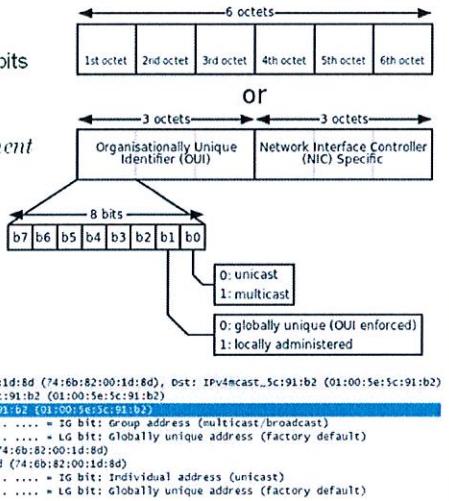
La sous-couche MAC - Structure de l'adressage IEEE

- Les LAN supportent un format commun d'adresse sur 48 bits
 - Il s'agit de l'adresse *liaison* (ou adresse de la couche *liaison*) appelée *adresse MAC*

- L'adresse est divisée en quatre champs
 - OUI (Organization Unique Identifier) sur 24(-2) bits
 - Définit le constructeur
 - Bit U/L (Universal/Local) : b1
 - Adressе définie *universellement ou localement*
 - Bit G/I (Group/Individual) : b0
 - Adressе *unicast ou multicast*
 - Numéro de série attribué par le constructeur sur 24 bits

- ## 3 types de trames

- Diffusion (broadcast) : tout à 1
 - Unicast U/L=0
 - Multicast U/L=1



3-23

Caractéristique de CSMA/CD

- ### Ethernet est un système de diffusion

- L'émetteur diffuse une trame de données sur le média
 - Chaque station reçoit la trame et décide si elle doit la traiter
 - En fonction de l'information d'adresse véhiculée dans la trame

- ## • Règles

- L'émetteur écoute avant de transmettre pour s'assurer que le médium n'est pas utilisé (*carrier sense*)
 - Toutes les stations raccordées peuvent émettre et recevoir (*multiple access*)
 - Si deux stations transmettent simultanément, les deux détectent une "collision" et attendent un temps aléatoire avant de retransmettre (*collision detection*)

- Période d'attente suivant la collision déterminée par un temporisateur aléatoire

- Les stations doivent attendre un temps aléatoire avant de retransmettre
 - Ce qui réduit la probabilité d'une nouvelle collision

3-24

Les réseaux Ethernet

Architecture en couches

La couche physique et les sous-couches

Les technologies radio 802.11...

La couche liaison de données et les sous-couches



CSMA/CA

Le protocole Spanning Tree

Les Vlan

Le 802.1X

Power over Ethernet (PoE)

Résumé du chapitre

3-25

La couche MAC 802.11

Le rôle de la couche MAC

- Similaire à la couche MAC 802.3 Ethernet (Fidélité respectée)
- Gère l'accès à un support commun partagé par plusieurs stations, chaque station doit écouter le support avant d'émettre

MAC 802.11 intègre en plus d'autres fonctionnalités

- Contrôle d'accès
- Adressage et formatage des trames
- Contrôle d'erreurs CRC
- Fragmentation et réassemblage
- QoS
- Gestion de l'énergie
- Gestion de la mobilité
- Gestion de la sécurité

Deux méthodes d'accès

- DCF (Distributed Coordination Function) : Méthode dite avec contention, les utilisateurs se disputent le droit d'émettre, donc collision. Elle s'appuie sur le protocole CSMA/CA combiné à l'algorithme de Back-off
- PCF (Point Coordination Function) : Méthode sans contention, centré sur le point d'accès qui gère les transmissions, donc pas de collision. DCF est obligatoire, PCF est optionnel et ne fonctionne qu'en mode infrastructure.

3-26

CSMA/CA

Carrier Sense Multiple Access

- L'accès pour chaque station est aléatoire, chacun doit écouter la porteuse avant d'émettre
- Ceci réduit le nombre de collisions sans les éviter

Les collisions

- Dans Ethernet CSMA/CD, chaque peut émettre et détecter les collisions, et les traitent si cela se produit
- Dans 802.11, cela n'est pas possible, la station n'est pas capable d'écouter **et** de transmettre en même temps

Collision Avoidance

- Sur un canal radio, une station qui émet n'entend pas les collisions
- CA = prévenir les collisions, la plus grande probabilité de collisions se fait au moment de l'accès au support
- Algorithme de back-off
- Mécanisme de réservation
- Trames d'acquittement

3-27

CSMA/CA

L'écoute de la porteuse

- Se fait au niveau de la couche physique avec le Physical Carrier Sense (PCS), et au niveau MAC avec le Virtual Carrier Sense (VCS)
- Le PCS permet de connaître l'état du support
 - Déetecte la présence d'autres stations
 - Analyse les trames qu'il reçoit
 - Écoute l'activité sur le support
 - Utilise le PLCP (Physical Layer Convergence Protocol)
- Le VCS réserve le support par l'intermédiaire du PCS
 - La réservation se fait par l'envoi de trame RTS/CTS (Request to Send)/Clear to Send entre l'expéditeur et le destinataire avant tout transfert
 - La réservation du support se fait en l'annonçant aux autres stations du BSS, pour s'assurer de la disponibilité du support pendant la durée de la communication
 - Les stations du BSS mettent en place un timer, le NAV (Network Allocation Vector)
 - Le calcul du NAV s'appuie sur le Duration ID de l'en-tête de la trame, qui donne la durée d'occupation du support, fonction de la taille de la trame et de la vitesse
 - VCS est optionnel, utilisé pour éviter la retransmission de trame de grandes tailles

3-28

CSMA/CA

• L'accès au support

- L'accès est contrôlé par un mécanisme d'espacement entre deux trames
- IFS (Inter Frame Spacing) = Intervalle de temps entre deux trames
- Période d'inactivité sur le support qui permet de gérer l'accès aux autres stations
- Système de « priorité »

• Quatre types d'IFS

- SIFS – (Short Inter-Frame Spacing), le plus court des IFS, **séparation des trames** au sein d'une communication (périodes d'inactivité sur le support) : durée 28µs
 - Entre data et ACK
 - Entre RTS et CTS
 - Entre les fragments d'une trame fragmentée
 - Après un polling pour une station en mode PCF
 - Permet de terminer une communication sans interruption
- PIFS – PCF IFS, (Point Coordination Function Inter-Frame Spacing) employé par l'AP pour accéder **prioritairement au médium**, par rapport aux stations : durée de 78µs
- DIFS – DCF IFS, (Distributed Coordination Function Inter-Frame Spacing) employé par une station lorsqu'elle veut **commencer une nouvelle transmission** : durée est de 128µs
- EIFS – Extended IFS, en mode DCF, lorsqu'une trame envoyée est erronée

3-29

CSMA/CA : la fenêtre de contention CW

• Fenêtre de Contention

- Contention Window (CW)
 - Correspond au **nombre** d'IT sélectionnés pour le calcul du temporisateur de back-off
 - Une valeur Minimale CW_{min} et une valeur Maximale CW_{max} définies par le standard
- Pour une première tentative, CW minimale
- Au démarrage, une station
 - Écoute le support grâce au Physical Carrier Sense
 - Si le support est libre pendant un temps DIFS
 - Transmet sa trame sans attendre le timer de back-off
 - Si le support est occupé, diffère sa transmission et attend in DIFS
 - Utilise alors le back-off pour une nouvelle tentative
- Lors du calcul du timer, plusieurs stations peuvent obtenir le même nombre
- Les Timers de ces stations vont expirer en même temps, d'où une émission simultanée possible, provoquant des collisions
- Les émetteurs n'entendent pas les collisions, mais doivent attendre un ACK de la part de chacun des destinataires, les collisions entraînent des absences d'acquittement
- Nouvelles tentatives : la taille de CW est doublée à chaque nouvelle tentative, jusqu'à CW_{max} . Ceci réduit la probabilité de collisions
- On parle de croissance exponentielle de CW : avec $CW_i = 2^{k+i-1}$
- En général, $CW_{min} = 7$, $CW_{max} = 255$

3-30

CSMA/CA

• L'algorithme de Back-off

- Déjà présent dans Ethernet 802.3
- Basé sur le calcul aléatoire d'un temporisateur gérant les retransmissions
- Dans 802.11 le temps est découpé en timeslot (Intervalle de temps)
- L'IT est plus petit que la durée minimale d'une transmission
- Correspond au temps que met une station pour détecter une transmission en cours

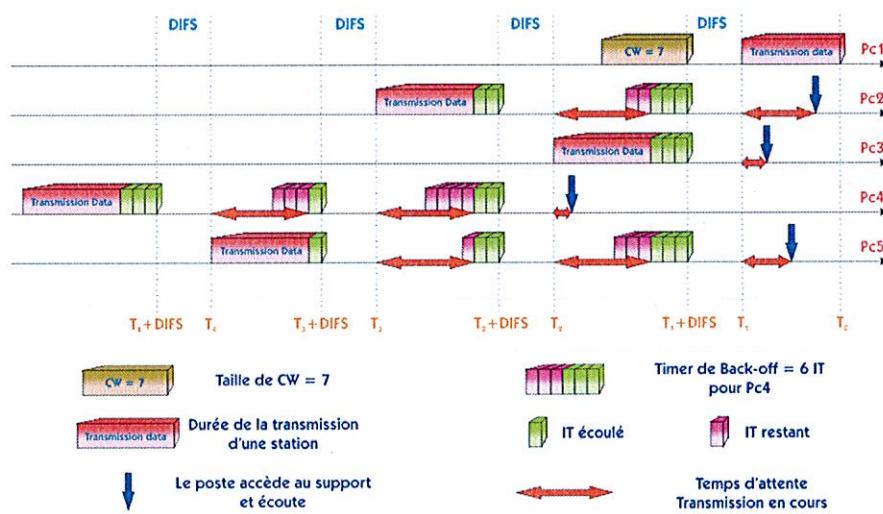
• Le temporisateur de Back-off

- Si plusieurs stations attendent de transmettre, elles utilisent toutes l'algorithme de back-off
- Le Timer est calculé par : $T_{\text{backoff}} = \text{Aléatoire}(0, \text{CW}) \times \text{IT}$
- La fonction Aléatoire(0,CW) va générer un nombre pseudo-aléatoire compris entre (0,CW) -1
- T_{backoff} est un nombre de timeslot
- Chaque station a théoriquement un T_{backoff} différent, donc chacun a la même chance d'accéder au support
- Quand le support devient libre après un DIFS, les stations décrémentent leur timer IT par IT, jusqu'à 0
- Celui qui a son timer à 0 va émettre car le support est libre. Les autres bloquent leur timer
- Une fois cette transmission terminée, les autres stations attendent le prochain DIFS et décrémentent leur timer de nouveau, jusqu'à 0, et ainsi de suite
- Les stations qui attendent ne recalculent pas de timer, car elles ont déjà attendu.
- Ces dernières ont plus de chance que celles qui commencent leur tentative

3-31

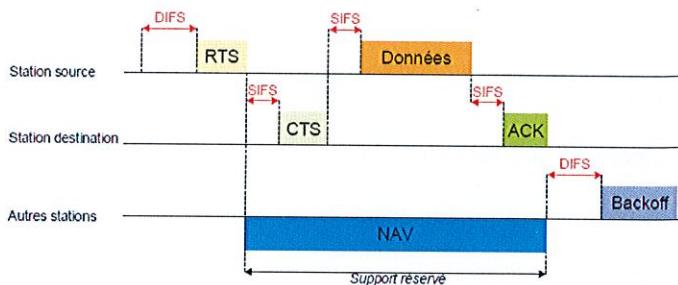
CSMA/CA Transmission avec Back-off

• Exemple d'utilisation de back-off pour 5 stations



3-32

NAV et Algorithme de backoff : résumé (1/2)



- Lorsqu'une station veut émettre des données, elle écoute le support.
- Si le support est libre pendant un DIFS, la station émet
- Si elle détecte une transmission, elle utilise un timer appelé NAV (Network Allocation Vector), lui permettant de suspendre ses transmissions. Ce NAV s'applique à toutes les stations et elles n'ont la capacité d'émettre qu'après la fin du NAV. Le NAV est calculé par rapport au champ TTL (Time To Live) des trames envoyées. Cela permet aux stations situées dans le voisinage des stations source et destination de connaître la durée du cycle complet de la transmission à venir.

3-33

NAV et Algorithme de backoff : résumé (2/2)

- **Mécanisme de réservation :** envoi de trames RTS/CTS (Request To Send/Clear To Send) entre une station source et une station destination avant tout envoi de données
- **Station qui veut émettre envoie un RTS**
Les stations du BSS entendent le RTS, lisent le champ durée du RTS et mettent à jour leur NAV
 - Station destination répond après un SIFS, en envoyant un CTS
Les autres stations lisent le champ de durée du CTS et mettent de nouveau à jour leur NAV
 - Après réception du CTS par la source, celle-ci est assurée que le support est stable et réservé pour la transmission de données
- Ces différentes stations en attente d'émission risquent de créer de collisions si on n'utilise pas une technique de gestion lorsque le support sera à nouveau libre. Ce procédé de redémarrage s'appelle l'algorithme de **backoff**, chaque station calcule un délai aléatoire compris entre 0 et 7 "time slot" (unité de temps la plus petite, variant suivant la norme physique) et décrémente ce timer dès que le support est libre. La station atteignant la valeur 0 la première pourra transmettre ses informations, les autres bloquent leur temporisateur et recommencent dès que le support est de nouveau libre. Si deux stations ont la même valeur de timer une collision se produira. Ces stations devront régénérer alors un nouveau compteur, compris cette fois entre 0 et 15. Cet algorithme permet aux stations d'accéder au support avec la même probabilité, mais sans garanti de délai. Pour chaque tentative de retransmission, le temporisateur croît de la façon suivante : $[2^2+1 * \text{randf}()] * \text{timeslot}$

3-34

Les réseaux Ethernet

Architecture en couches

La couche physique et les sous-couches

Les technologies radio 802.11...

La couche liaison de données et les sous-couches

CSMA/CA



Le protocole Spanning Tree

Les Vlan

Le 802.1X

Power over Ethernet (PoE)

Résumé du chapitre

3-35

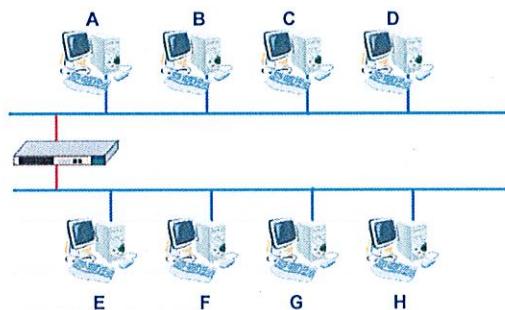
Les ponts

• Pont à auto-apprentissage

- Ecoute
- Apprend
- Laisse passer
- Ou Bloque

- ✓ Fonctionne en mode « *promiscuous* »
- ✓ Reçoit et stocke chaque trame arrivant sur un port
- ✓ Étudie le port d'émission en se basant sur le champ adresse MAC source de la trame
- ✓ Construit une table des adresses MAC connues sur chaque port
- ✓ Purgée à intervalle régulier (5 minutes par défaut)

| Port 1 | Port 2 |
|--------|--------|
| A | E |
| B | F |
| C | G |
| D | H |



• Génération d'équipements baptisés Switch

- Ce sont des ponts plus sophistiqués
- Densité de ports plus importante – chaque port est un segment / domaine de collision
- Changement de vitesse – 10 – 100 – 1000
- Vitesse de commutation plus rapide : qq Mb/s

3-36

Le protocole STP

● Protocole inter-commutateur

- Transparent aux protocoles de plus haut niveau
 - D'où le terme *transparent spanning tree*

● Buts

- Construire une topologie logique sans bouclage
- Mise en place d'une arborescence

● Algorithme plaçant certains ports du commutateur dans le *mode passant*

- Les autres sont *bloqués*
- Fournit un seul chemin de commutation entre deux segments de LAN

● Standard international IEEE 802.1

- Développé dans le milieu des années 1980
- Mis à jour en 1998 pour inclure les commutateurs et les VLAN
 - IEEE 802.1D
 - IEEE 802.1w (RSTP) - 2001
 - IEEE 802.1s (MSTP, instance par VLAN) – totalement intégré en 2005

3-37

Aperçu du STP

● 1^{ère} étape: Élire la racine du Spanning Tree

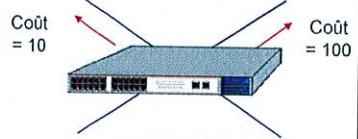
- Tous les commutateurs émettent des BPDUs pour déterminer lequel a le plus faible identificateur BID (Bridge IDentifier)
 - Il devient le commutateur racine

BPDU = Bridge Protocol Data Unit



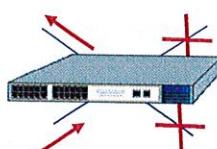
● 2^e étape : Déterminer le chemin racine

- Chaque commutateur détermine le chemin de plus faible coût vers la racine



● 3^e étape : Désactiver les chemins non racine

- Les commutateurs valident la *retransmission* sur les chemins de plus faible coût vers la racine
- Sur les chemins de coût plus élevé éloigné de la racine
 - Les autres ports sont maintenus dans l'état *bloqués*

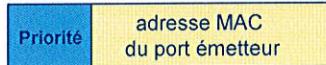


3-38

Identificateur des ponts et coût des chemins

• ID commutateur officiellement appelée BID (Bridge ID)

- Composé de 16 bits de priorité et 48 bits d'adresse MAC



• La priorité par défaut est de 32768

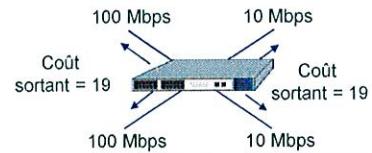
- Réduire ceci augmente la priorité

• L'équipement avec la plus basse BID devient le commutateur racine du Spanning Tree

• Chaque port du commutateur dispose d'un coût sortant associé

- Les anciens logiciels utilisaient $10^9/\text{débit}$
- Les nouvelles versions utilisent l'échelle non linéaire de l'IEEE 802.1D

• Le coût du chemin racine est l'addition des chemins à traverser entre le commutateur et la racine



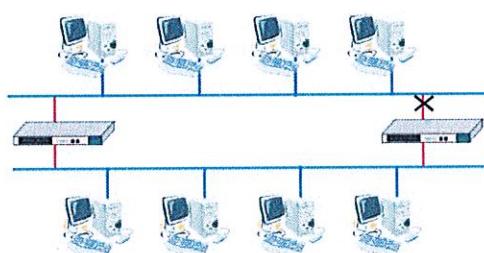
| Bandé passante | Coût |
|----------------|------|
| 10 Mbps | 100 |
| 16 Mbps | 62 |
| 45 Mbps | 39 |
| 100 Mbps | 19 |
| 155 Mbps | 14 |
| 622 Mbps | 6 |
| 1 Gbps | 4 |
| 10 Gbps | 2 |

3-39

Le STP pour le 802.11

• Redondance de chemin (Redundant Bridging)

- Possibilité de mettre en place 2 ponts afin de permettre une redondance de chemin ou d'équilibrage de charge, et coupure "logique" d'un lien via le STP.
- Sans coupure logique = création d'une "boucle".



- Pour le 802.11, principe identique; les ponts devront utiliser des canaux radios disjoints pour éviter toute interférence.



3-40

Les réseaux Ethernet

Architecture en couches

La couche physique et les sous-couches

Les technologies radio 802.11...

La couche liaison de données et les sous-couches

CSMA/CA

Le protocole Spanning Tree



Les Vlan

Le 802.1X

Power over Ethernet (PoE)

Résumé du chapitre

3-41

Concepts et avantages des VLAN

• Les VLAN identifient une *communauté d'intérêt*

- Un groupe de travail, département, ou un autre regroupement

• Ils limitent la taille du domaine de diffusion

- Réaliser des sous ensembles du domaine naturel de diffusion, appelés parfois *domaines logique de diffusion*
- Les commutateurs évitent de propager les diffusions au delà du VLAN

• Ce qui limite le risque d'exposition

- Fournit une frontière sécurisée de Niveau 2
- Contient en local la congestion et d'autres problèmes

• Les trames Inter-VLAN doivent être retransmises à un niveau plus élevé

- Avec un routeur ou le routage d'un commutateur multi-niveaux

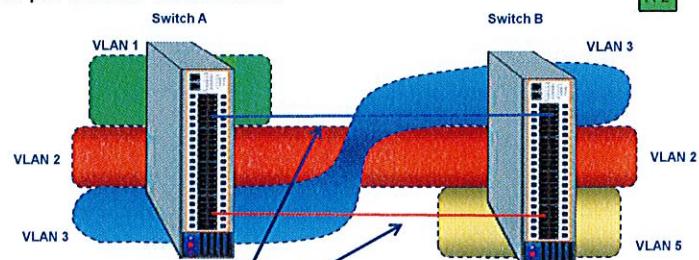
• Cinq types de VLAN

- Groupement de ports du commutateur (Appelé *static VLAN* ou *port-grouped VLAN*) (*cf ci après*)
- Groupes d'adresse MAC (Appelé *dynamic VLAN*), nécessite un serveur de configuration (*cf ci après*)
- Groupes de protocoles (par exemple, IP, NetWare, NetBIOS, AppleTalk...) : création de VLAN basés sur le types de paquet par filtrage des protocoles sur le routeur en utilisant les *access lists*
- Groupes d'adresses de Niveau 3 (essentiellement en sous réseau) : affectation d'un sous-réseau à un VLAN
- « Marquage de trame » (*trunk*) : IEEE 802.1Q

3-42

VLAN statiques

- Les VLAN statiques utilisent des groupes de port
 - Sur un seul commutateur
 - Sur de multiples commutateurs
- Le regroupement de port de VLAN est le plus facile à configurer
 - Mais ne fournit pas la flexibilité des VLAN dynamiques
- Supportés par tous les fournisseurs

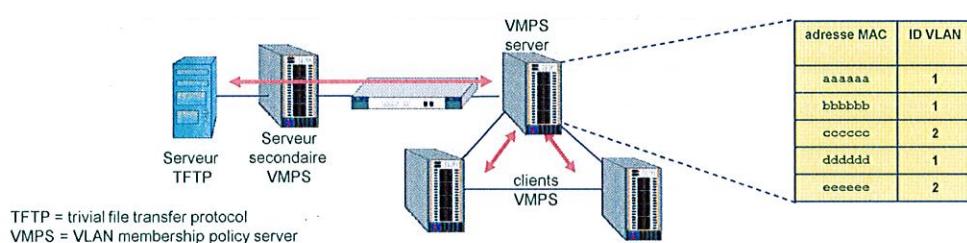


- Besoin d'un lien par VLAN pour la propagation vers d'autres switchs
 - Cela multiplie les liens inter-switch

3-43

VLAN dynamiques

- Les VLAN dynamiques utilisent les adresses MAC pour déterminer l'appartenance au VLAN
 - La configuration des commutateurs Cisco est plus compliquée qu'en statique
- Un ou plusieurs commutateurs sont configurés comme *serveurs VMPS*
 - Charge la liste des adresses MAC et de l'association VLAN depuis un serveur TFTP au démarrage
 - Ou lorsqu'un rechargement est réclamé explicitement
- Les autres commutateurs sont configurés comme *clients VMPS*
 - Consultation du serveur VMPS pour déterminer l'action de retransmission



3-44

IEEE 802.1Q: Virtual Local Area Networks

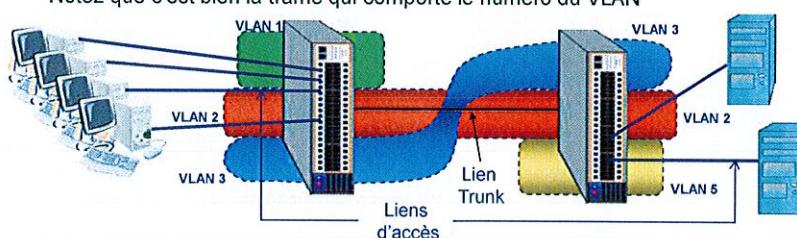
- Le standard complet définit les services VLAN, protocoles, et algorithmes
 - Utilise les propriétés des protocoles multicast définis dans l'IEEE 802.1p*
- Le Standard International stipule aussi que le domaine de commutation de Niveau 2 doit être dans le même Spanning Tree
 - Appelé parfois CST (Common Spanning Tree)
 - Supporté par la majorité des fournisseurs
 - IEEE 802.1Q stipule le mode CST
 - Ne supporte pas un Spanning Tree par VLAN
- Cisco implémente (et recommande) un Spanning Tree par VLAN
 - Appelé PVST (Per VLAN Spanning Tree)
 - Facilite la répartition de charge et d'autres règles de contrôle du trafic
- Multiple Spanning Tree Protocol (MSTP)
 - [IEEE 802.1s](#)

* IEEE 802.1p: Extension to MAC Bridge standard—"Traffic Class Expediting and Dynamic Multicast Filtering": Définit les règles pour la priorité des trames MAC et le filtrage du trafic semblable aux routeurs

3-45

Liaison inter commutateurs

- Les liaisons d'accès connectent les utilisateurs au commutateur
 - Elles sont habituellement dans un seul VLAN (VLAN par port par exemple)
- Les liaisons marquées/tagguées (trunks) connectent un commutateur aux autres commutateurs
 - Peuvent être dans différents VLAN simultanément
 - Notez que c'est bien la trame qui comporte le numéro du VLAN
- Un seul lien peut transporter le trafic de multiples VLAN
 - Solution plus évolutive (si ajout d'autres VLAN)
 - Occupe une seule paire de ports
- Fonction réservée au Fast Ethernet et Gigabit Ethernet



3-46

Marquage 802.1Q

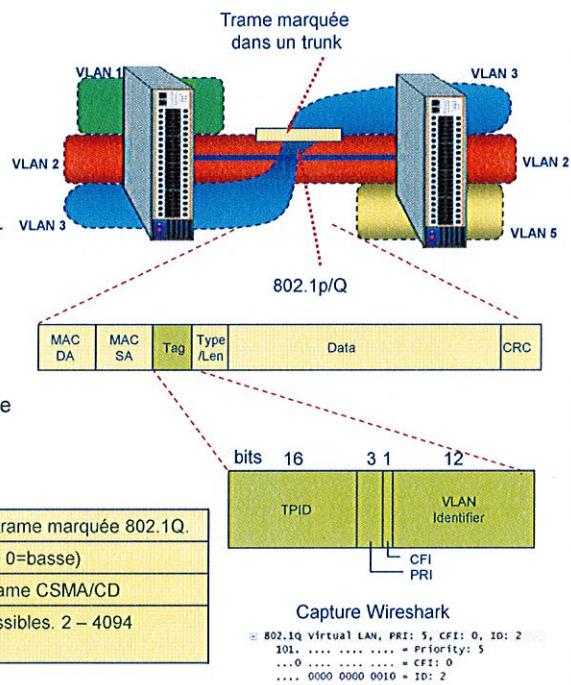
Le marquage des VLAN est nécessaire sur les liens trunk

- Les trames des utilisateurs doivent transporter l'identificateur VLAN
- Le commutateur récepteur doit savoir où retransmettre la trame

Cisco supporte 2 méthodes de marquage sur les trunks Ethernet

- Cisco ISL (InterSwitch Link)
 - Méthode de marquage propriétaire
- IEEE 802.1Q
 - Marquage standardisé Champ additionnel dans l'en-tête MAC

| | |
|---------|---|
| TPID | Identificateur de protocole : 0x8100 = trame marquée 802.1Q. |
| PRI | IEEE 802.1p champ priorité (7=haute, 0=basse) |
| CFI | Canonical Format Identificateur: 0 = trame CSMA/CD |
| VLAN ID | Identificateur VLAN 12 bits, valeurs possibles. 2 – 4094 0, 1 et 4095 sont réservées |

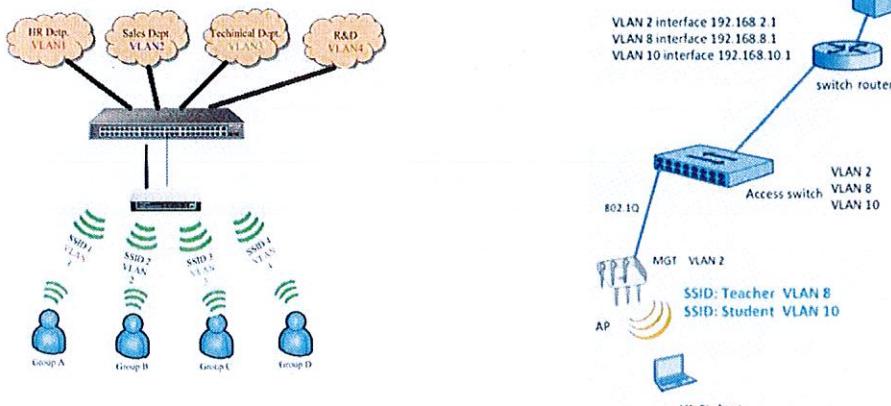


3-47

VLAN : Application aux AP

Principe

- Le VLAN est associé à un SSID, l'uplink de l'AP devient un trunk
- L'interface de management se situe dans le « native VLAN », non taggué par défaut
- Rejoindre le SSID, c'est se positionner dans le VLAN
- L'éclatement par VLAN/communication inter-VLAN se fait au moyen d'un switch/routeur
- Chaque SSID peut disposer d'une sécurité différente (téléphonie, Guest, Entreprise)
- Pas de limite (théorique) au nombre de SSID



3-48

Les réseaux Ethernet

Architecture en couches

La couche physique et les sous-couches

Les technologies radio 802.11...

La couche liaison de données et les sous-couches

CSMA/CA

Le protocole Spanning Tree

Les Vlan



Le 802.1X

Power over Ethernet (PoE)

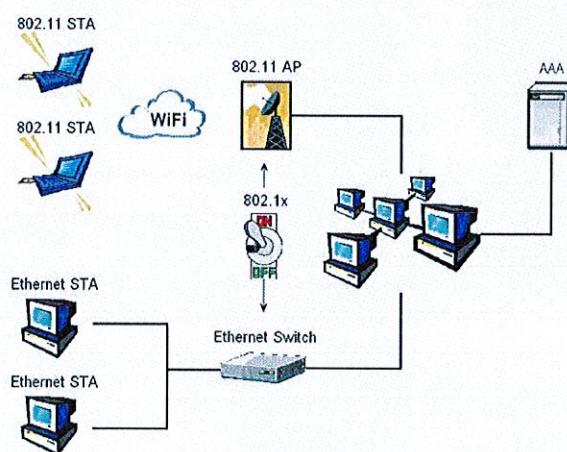
Résumé du chapitre

3-49

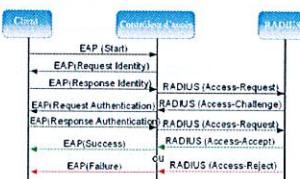
802.1X : Principe

L'accès est autorisé par le serveur d'authentification AAA

802.1x Port-Based Network Access Control



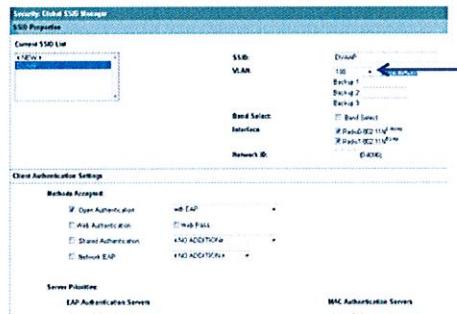
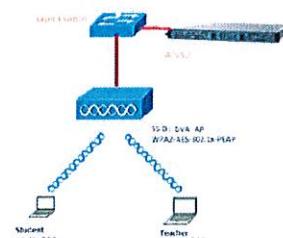
- Le contrôle se fait grâce à un élément connu de l'utilisateur/ordinateur (mot de passe, certificat)
- C'est le switch/AP qui laisse passer ou non les trames de data
- Le serveur d'authentification AAA renvoie des informations au switch ou AP, comme l'acceptation/refus et le positionnement du port dans un VLAN spécifique
- Possibilité d'avoir un VLAN « poubelle » en cas de non réponse/erreur de réponse du client



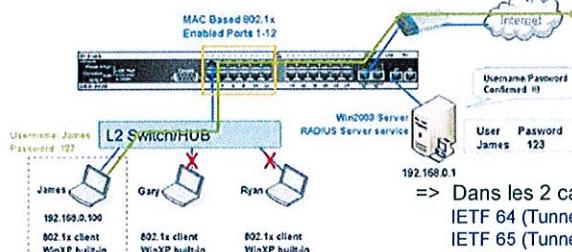
3-50

802.1X : Application aux Switchs/ AP

Sur un AP



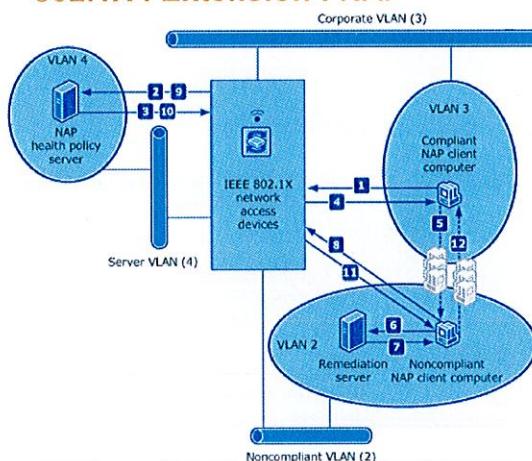
Sur un switch



=> Dans les 2 cas, le serveur RADIUS renvoie les attributs
IETF 64 (Tunnel Type) – Précise que c'est un VLAN.
IETF 65 (Tunnel Medium Type) – Positionné à 802.
IETF 81 (Tunnel Private Group ID) – Précise le VLAN ID (le n°) qui écrasera alors la valeur indiquée.

5-51

802.1X : Extension : NAP



1. The NAP client computer detects a change in its health state and sends an access request containing its health state to the network access device.
2. The network access device forwards the client's access request to the NAP health policy server for analysis.
3. The NAP health policy server evaluates the access request. The client computer is determined to be noncompliant with health requirements, so NPS instructs the network access device to place the computer on the noncompliant VLAN.
4. The network access device forwards the access response along with health remediation instructions to the client computer.
5. The network access device places the client computer on the noncompliant VLAN.
6. If required, the client computer requests updates from a remediation server.
7. The remediation server provides software updates to the client computer.
8. After its health state has been updated, the client computer sends a new access request containing its health state to the network access device.
9. The network access device forwards the client computer's access request to the NAP health policy server for analysis.
10. The NAP health policy server evaluates the access request and determines that the client computer is compliant with health requirements. The NAP health policy server instructs the network access device to place the client computer on the corporate VLAN.
11. The network access device forwards the access response to the client computer.
12. The network access device places the client computer on the corporate VLAN.

• Notez que dans ce cadre, le client se connecte toujours au même SSID, sur le même AP, les informations de changement de VLAN étant fournies par le serveur NAP/RADIUS à l'AP.

3-52

Les réseaux Ethernet

Architecture en couches

La couche physique et les sous-couches

Les technologies radio 802.11...

La couche liaison de données et les sous-couches

CSMA/CA

Le protocole Spanning Tree

Les Vlan

Le 802.1X



Power over Ethernet (PoE)

Résumé du chapitre

3-53

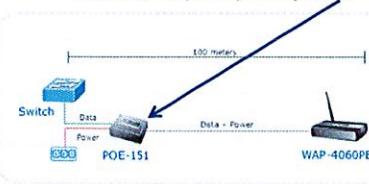
802.3af : Principe

- Objectif : permettre d'installer des appareils tels qu'une imprimante ou un téléphone dans des endroits qui sont dépourvus de prise électrique en utilisant le câble réseau.
- L'alimentation électrique par câble Ethernet (Power over Ethernet ou PoE) permet de faire passer une tension de 48 V (jusqu'à 13 watts de puissance électrique), en plus des données à 100 Mbit/s ou 1 Gbit/s (802.3af : 2003).
- Extension : IEEE 802.3at (PoE+) : Si l'équipement d'alimentation et le périphérique sont à cette norme, alors la puissance peut être entre 24 et 30W (48V).
- Précautions à prendre (rappel HSCT) :

| Effets du passage du courant alternatif | | |
|---|---|------------|
| Intensité | Perception des effets | Temps |
| 0,5 à 1 mA | seuil de perception suivant l'état de la peau | |
| 8 mA | choc au toucher, réactions brutales | |
| 10 mA | contraction des muscles des membres | 4 mn 30 |
| 20 mA | début de tétonisation de la cage thoracique | 60 s |
| 30 mA | paralysie ventilatoire | 30 s |
| 40 mA | fibrillation ventriculaire | 3 s |
| 75 mA | fibrillation ventriculaire | 1 s |
| 300 mA | paralysie ventilatoire | 110 ms |
| 500 mA | fibrillation ventriculaire | 100 ms |
| 1 000 mA | arrêt cardiaque | 25 ms |
| 2 000 mA | centre nerveux atteints | instantané |



Schéma de principe : Injecteur



Limites de tensions dangereuses

| Tension | Alternative | Continue |
|----------------|-------------|----------|
| Milieu sec | 50V | 120V |
| Milieu humide | 25V | 60V |
| Milieu mouillé | 12V | 30V |

3-54

Les réseaux Ethernet

Architecture en couches

La couche physique et les sous-couches

Les technologies radio 802.11...

La couche liaison de données et les sous-couches

CSMA/CA

Le protocole Spanning Tree

Les Vlan

Le 802.1X

Power over Ethernet (PoE)



Résumé du chapitre

3-55

Résumé du chapitre

❖ Dans ce chapitre, nous avons étudié

- La structure en couches WLAN 802.11
- Les différentes technologies radio 802.11
- La méthode d'accès CSMA/CA
- Les normes :
 - 802.1D (STP),
 - 802.1q (VLAN),
 - 802.1x (NAP)
 - 802.3af (PoE)

3-56