

Motivations

- ▶ L'architecture physique d'un réseau de campus doit maintenant répondre à certains impératifs comme
 - ▶ L'adaptabilité aux topologies changeant rapidement
 - ▶ La redondance en cas de failles réseaux
 - ▶ L'agrandissement du réseau
 - ▶ Centralisation des servers et applications pour simplifier l'administration
 - ▶ Support de plusieurs protocoles routables et commutables
- ▶ Pour cela, suivant les fonctions du réseau, il existe principalement 2 architectures types
 - ▶ L'architecture AVVID pour une convergence voix, donnée, vidéo
 - ▶ L'architecture multi-couches

L'architecture trois couches

- ▶ Avant l'architecture réseau était composée de la manière suivante
 - ▶ Les principaux services placée au centre du réseau avec des switch niveau 2 qui assurent le transport entre les utilisateurs et les ressources
- ▶ Maintenant l'architecture réseau recommandée est en 3 couches
 - ▶ Core Layer (le coeur du réseau): fournit un backbone à haut débit
 - ▶ Distribution Layer: implémente les politiques réseaux de l'entreprise
 - ▶ Access Layer: donne aux utilisateurs l'accès aux réseaux

Core Layer

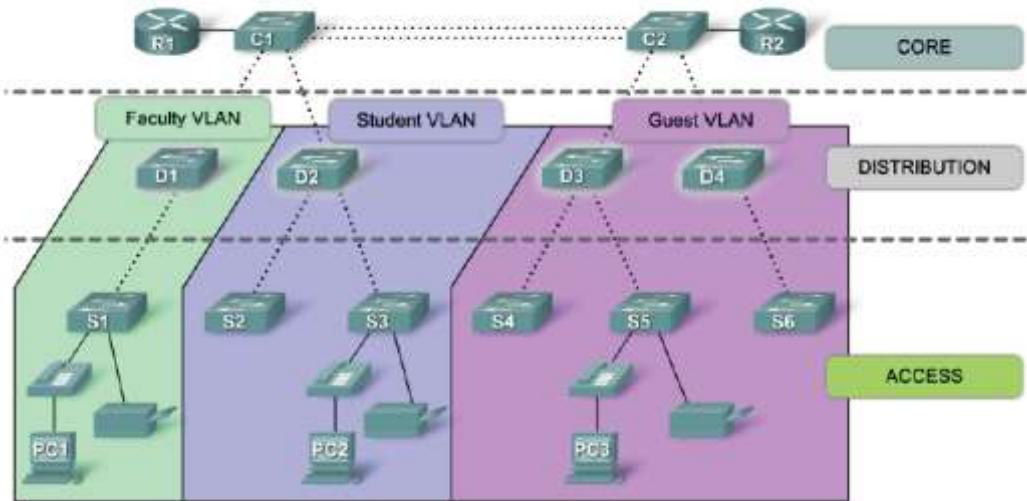
- ▶ L'objectif de cette couche est de permettre la commutation entre les différentes couches de distribution aussi vite que possible
- ▶ Généralement cette partie est assurée par de l'interconnexion de niveau 2 uniquement
- ▶ L'utilisation de services de niveau 3 n'est pas recommandée
 - ▶ Les fonctionnalités de sécurité comme le filtrage de paquets ne sont pas appliquées par cette couche
 - ▶ Même avec des switchs multi-niveaux, cela nécessite de la manipulation de paquets: ce qui ralenti le trafic réseau
 - ▶ Exception: dans le cas d'un très grand réseaux avec des équipements dans la couche distribution nécessitant une implémentation d'une commutation de niveau 3. A utiliser avec précaution !

Distribution Layer

- ▶ Cette couche se trouve entre le cœur du réseau et la couche d'accès aux réseaux
 - ▶ Interconnecter entre-eux les switchs de la couche d'accès au réseau et faire la liaison avec le cœur de réseau
- ▶ Elle doit gérer les fonctionnalités de niveau 3 et mettre en place la politique de sécurité
- ▶ Mettre en place les VLANs
- ▶ Faire le routage entre les VLANs
- ▶ Effectuer l'agrégation des routes
- ▶ Relier entre-eux les différents types de média utilisés comme FDDI, Ethernet ou Token Ring
- ▶ Comme cette couche inter-connecte le cœur de réseau à la couche d'accès, elle doit être architecturée avec de la commutation rapide de niveau 3 (ou supérieure)

Access Layer

- ▶ Sur cette couche, il est possible de mélanger des réseaux commutés (switch) et partagés (hub)
 - ▶ Définir les VLANs afin d'interdire la propagation des broadcasts et des multicasts
 - ▶ Filtrer le trafic en fonction des adresses MAC
 - ▶ Dédier de la bande passante à destination des serveurs
 - ▶ Authentifier les accès des utilisateurs au réseau
 - ▶ Cette couche est généralement composée de switchs mais éventuellement aussi de routeurs pour les accès distants (ISDN, frame relay, ...)
- Un réseau n'est pas la simple accumulation de switch et routeur !
 - Il faut l'organiser, le hiérarchiser
 - Pour simplifier son administration
 - Pour isoler rapidement les problèmes
 - Pour rendre modifiable le réseau et pour pouvoir facilement l'agrandir
 - Un réseau d'entreprise est donc découpé suivant un modèle en 3 couches
 - Access Layer
 - Distribution Layer
 - Core Layer
 - Chaque couche va avoir des fonctionnalités particulières



Rôle du la Distribution Layer

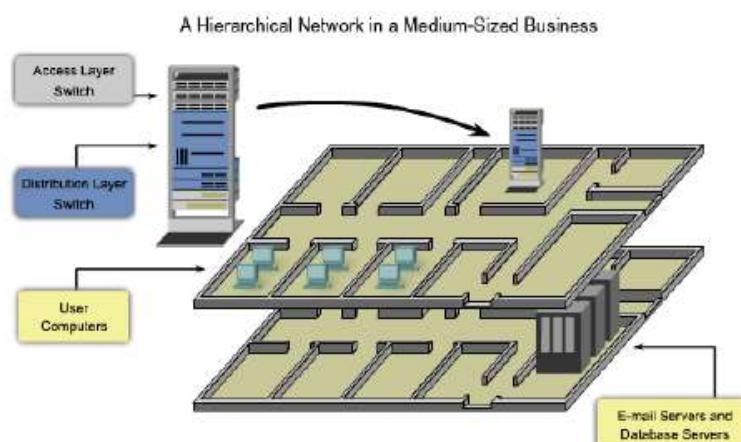
- De limiter les zones de broadcast
- Router les données entre VLAN
- Eviter certaines données de transiter vers certains VLAN

Core Layer

- C'est le backbone du réseau
- Doit transférer les données le plus rapidement possible
- Apporte la connexion à Internet ou aux autres réseaux de la société via un MAN ou WAN

Représentation physique

- Généralement, une salle de brassage par étage
- Serveur dans une salle spécialisée
- Tous les étages reliés au core layer

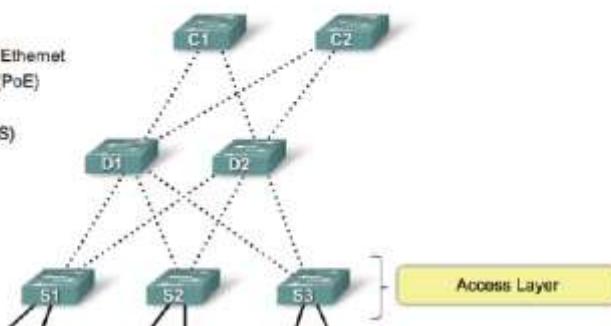


Avantages d'une architecture hiérarchique

- Scalabilité
 - Pouvoir faire des agrandissements du réseau simplement
- Redondance
 - Les services doivent être opérationnel 24/24
 - Exemple : pour la ToIP , on doit avoir une fiabilité de 99,999%, soit 5 min par an d'interruption de service. Fiabilité que nous avons en téléphonique classique
- Performance
 - Eviter des goulets d'étranglement
- Sécurité
 - Sécurisation des données et des accès au plus près de la source
- Administration simplifiée
- Maintenance facilité en raison de la modularité du réseau

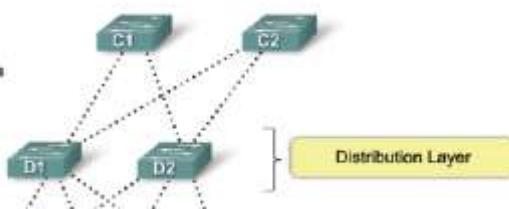
Fonctions de l'Access Layer

- Port security
- VLANs
- Fast Ethernet/Gigabit Ethernet
- Power over Ethernet (PoE)
- Link aggregation
- Quality of Service (QoS)



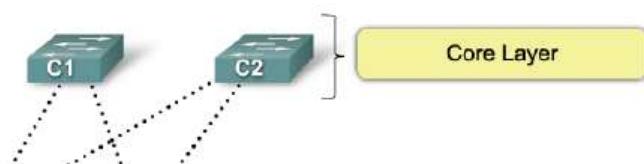
Fonction de la Distribution Layer

- Layer 3 Support
- High forwarding rate
- Gigabit Ethernet/10 Gigabit Ethernet
- Redundant components
- Security Policies/Access Control Lists
- Link Aggregation
- Quality of Service (QoS)

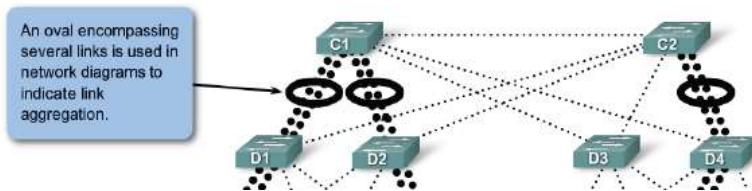


Fonctions du Core Layer

- Layer 3 Support
- Very High forwarding rate
- Gigabit Ethernet/10 Gigabit Ethernet
- Redundant components
- Link Aggregation
- Quality of Service (QoS)



- Agrégation de liens : mise en commun de plusieurs liens reliant les mêmes équipements afin d'augmenter le débit entre ces 2 équipements
 - Avec 2 liens 100 Mb/s entre 2 équipements, on peut alors créer une liaison 200 Mb/s



1) Core Layer

C'est la couche supérieure. Son rôle est simple : relier entre eux les différents segments du réseau, par exemple les sites distants, les LANs ou les étages d'une société.

Nous trouvons généralement les routeurs à ce niveau. Si l'entreprise est vraiment grande, ce modèle peut s'imbriquer : le design d'implémentation des routeurs correspond à ce modèle, mais le design du niveau 2 (modèle OSI), c'est-à-dire les switchs, reprendra la même hiérarchisation et les mêmes rôles ! On a donc un modèle Core/Distribution/Access à l'intérieur de la partie Access ou Distribution des routeurs. Le Core est aussi appelé Backbone.

2) Distribution Layer

Une fois nos routeurs/switchs de la couche Core choisis et mis en place dans notre architecture, le designer s'intéresse à la couche Distribution.

Son rôle est simple : filtrer, router, autoriser ou non les paquets... Nous sommes entre la couche Core et la couche Access, c'est-à-dire entre la partie « liaison » et la partie « utilisateurs ». Ici, on commence à diviser le réseau en segment, en ajoutant plusieurs routeurs/switchs de distribution, chacun étant connecté au Core d'un côté, et à la couche Access de l'autre.

Visualisez bien : 1 core router > plusieurs distribution routers connectés sur le même core router > encore plus de switchs access, tous connectés sur un distribution layer. C'est exactement comme un arbre généalogique

Ici aussi, selon la taille et les moyens de l'entreprise, l'architecte devra choisir entre routeur et switch. Evidemment, plus la société est grande, plus on aura besoin de routeur à ce niveau. Pour une petite entreprise, des switchs suffisent.

Ces routeurs de distribution vont s'occuper de router (envoyer sur le bon chemin, pour les néophytes) les paquets, d'y appliquer des ACLs, d'assurer la tolérance de panne, de délimiter les domaines de broadcast, etc...

Note : Bien entendu, s'il n'y a que des switchs dans notre couche distribution, ces actions seront effectuées au niveau Core puisque seule la couche Core possède des routeurs.

3) Access Layer

C'est la dernière couche de notre modèle. Son rôle est simple mais très important : connecter les périphériques « end-users » au réseau. Mais aussi, assurer la sécurité !

Ici, pas de routeur. Seuls des switchs, ou hubs parfois, sont implantés. C'est normal, me direz-vous, puisque tout le travail des routeurs est déjà effectué au niveau de la Distribution ou du Core. Résultat, on ne s'occupe que de connecter nos end-users au réseau, que ce soit en Wi-fi, Ethernet ou autre. Et si possible, on le fait de manière sécurisée, c'est-à-dire en utilisant switchport sur nos switchs, en désactivant les interfaces non utilisées, etc... (cela pourrait faire l'objet d'un prochain article, tellement il y a à dire !).

Du coup, la configuration de ce type de switch pose moins de contrainte. Pas besoin de performances particulières car chaque switch aura – au maximum – un nombre d'utilisateur égale à son nombre de port (moins 1 ou 2 pour le trunk entre Access et Distribution). De plus, les traitements restent basiques et ne demandent que peu de ressources.

Il est important de noter que chaque couche apporte ses impératifs et ses besoins, influençant le matériel mis en place ainsi que les configurations et/ou solutions.

C'est d'ailleurs la raison principale de l'existence de ce modèle : plus compliqué, au premier abord, à mettre en place, mais totalement plus efficace, rentable, réfléchi et économique sur le long terme qu'une architecture improvisée au fil du temps.

Certes, le modèle hiérarchique en trois couches est une référence que de nombreuses architectures utilisent. Il est généralement adapté aux besoins de l'entreprise.

Mais il n'est pas le seul et unique modèle. Il existe de nombreux autres modèles d'architecture, tels que le modèle « en étoile » par exemple ou encore le « Campus LAN ».

Bilan

Pour finir, 3 points à retenir :

- Ce modèle hiérarchique est une référence, il est très utilisé. Mais il faut bien entendu l'adapter aux besoins de son entreprise.
- Chaque couche – Core / Distribution / Access – implique des configurations différentes. Notamment la couche Access, qui nécessite de la part de l'administrateur certaines actions (réglage de l'état de chaque port des switches, mise en place de trunk, sécurité, etc...)
- Tous les liens (lien = liaison entre deux points, englobant le côté physique et logiciel) sont doublés/backupés dans la majorité des cas.

Et n'oubliez pas que réfléchir et choisir le mieux possible l'architecture de son réseau, c'est-à-dire le design, les plages d'IP pour les différents LANs, le nombre de LAN/VLAN et tous les autres paramètres, est primordial ! Surtout sur le long terme...

Evaluation des besoins

- Pour faire le choix d'un équipement, vous avez besoin de connaître au moins :
 - La destination des informations
 - L'ensemble des utilisateurs concernés
 - Les serveurs
 - Les serveurs de stockage
- Analyse du trafic
 - Charge CPU utilisée
 - Taux de packet perdu
 - Quantité de mémoire utilisée
 - Temps moyen de traitement
- Les outils
 - De très nombreux outils existent
 - Libre : Cacti, Nagios, Centreon, ...
 - Commerciaux : Solarwinds NetFlow, IBM Tivoli, CiscoWorks, HP OpenView

Communautés d'utilisateurs

- Localisation des communautés d'utilisateurs pour regrouper leur connexion
 - Assez souvent les utilisateurs ayant les mêmes rôles travaillent aux mêmes endroits
- Prévoir des agrandissements éventuels
- Connaître leurs usages pour placer au mieux les serveurs
 - Modèle client-serveur : les clients envoient régulièrement leur donnée vers le serveur
 - Modèle serveur à serveur : échange d'info, sauvegarde ou stockage
- Il faut donc optimiser les connexions des clients et des serveur sur les switchs afin d'« équilibrer » les bandes passantes

Les fonctionnalités

- Autres critères de choix : la densité, le débit ou l'agrégation des bandes passantes
- La densité : le nombre de port par switch : 24 ou 48 avec ou sans connecteur spécifique pour les uplink. Un chassis peut avoir jusque 1000 ports
- Le débit : quels doivent être les débits de chaque port : 100 Mb/s, 1 Gb/s ou plus ?
 - Un switch 48 ports à 1 Gb/s devra pouvoir gérer 48 Gb/s au total. En access layer, pas forcément besoin d'une telle bande passante car limitation sur l'uplink
- L'agrégation de liens : peut être une solution pour augmenter le débit entre 2 équipements

Le HUB (Concentrateur)



Cet équipement agit au niveau 1 du modèle OSI. Sa fonction est d'interconnecter plusieurs cartes d'interfaces ensembles. Ainsi, chaque signal électrique reçu est rediffusé sur tous les autres ports du HUB.

Dans le cadre d'un HUB 100Mbps, on obtient un débit partagé de 100Mbps pour l'ensemble d'équipement Ethernet raccordé.

Le commutateur (Switch)

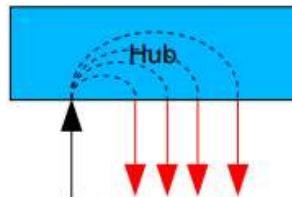
Cet équipement agit au niveau 2 du modèle OSI. Identiquement à un HUB, sa fonction est d'interconnecter plusieurs cartes d'interfaces ensembles. Cependant, lorsqu'il réceptionne une trame, il compare l'adresse MAC de destination avec sa table de correspondance. Ainsi, il ne diffuse cette trame uniquement sur le port physique concerné.

Dans le cadre d'un Switch 100Mbps, on obtient un débit dédié de 100Mbps par équipement Ethernet raccordé. les caractéristiques principales à vérifier lors de la sélection d'un Switch sont :

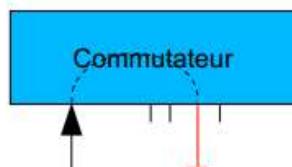
- Le nombre d'adresse MAC maximum qui peuvent être mis en mémoire
- Le nombre de paquet par seconde (PPS) que la matrice de fond de panier peut traiter

Un **hub** est un équipement « bête » :

- Il sert à réamplifier le signal d'un lien,
- Il renvoie toutes les trames reçues sur tous les ports immédiatement,
- Il peut permettre de passer d'un média à un autre. Par exemple du Cuivre vers la fibre.



Un **commutateur** est un équipement « intelligent ». Le commutateur est le centre de la topologie en étoile. A la différence du répéteur (hub), qui ne fait que répéter sur tous les ports les données qu'il reçoit, les commutateurs ont la capacité d'analyser le trafic, et ainsi de posséder une connaissance des adresses MAC (Medium Access Control) et de construire des tables de commutation.



Le commutateur possède les particularités suivantes :

- Apprendre les adresses MAC des matériels attachés à ses ports.
- N'envoie le trafic d'une adresse MAC que sur le port concerné,
- Possède une table de commutation <adresse MAC <-> port>.
- La grande majorité des commutateurs apporte des fonctionnalités supplémentaires comme éviter la formation de boucles (Spanning Tree) ou créer des réseaux virtuels (VLAN). Attention! Ces fonctionnalités ne sont pas natives aux commutateurs et peuvent ne pas exister sur les bas de gamme.

Avec un commutateur, le domaine de collision est limité à un seul port, rendant les collisions impossibles. De plus la bande passante disponible sur une interface ne sert que pour la machine connectée dessus.

Eléments d'interconnexion : pourquoi ?

- Ré-amplifier les signaux
 - Électriques - optiques
 - ↗ Augmenter la distance maximale entre 2 stations
- Connecter des réseaux différents
 - Supports : Coax, TP, FO, Radio, Hertzien, ...
 - Protocoles niveau 2 : Ethernet, FDDI, ATM, ... rieur
- « Limiter » la diffusion (Ethernet)
 - Diminuer la charge globale
 - Limiter les broadcast-multicast Ethernet (inutiles)
 - Diminuer la charge entre stations
 - Limiter la dépendance / charge des voisins
 - Objectif in fine : garantir une bande passante disponible (une qualité de service) entre 2 stations
- Limiter les problèmes de sécurité
 - Diffusion ↗ écoute possible : pas de confidentialité

- Restreindre le périmètre de la connectivité désirée
 - Extérieur ↗ Intérieur : protection contre attaques (sécurité)
 - Intérieur ↗ Extérieur : droits de connexion limités
- Segmenter le réseau :
 - Un sous-réseau / groupe d'utilisateurs : entreprises, directions, services, ...)
 - Séparer l'administration de chaque réseau
 - Créer des réseaux réseaux virtuels
 - S'affranchir de la contrainte géographique
- Pouvoir choisir des chemins différents dans le transport des données entre 2 points
 - Autoriser ou interdire d'emprunter certains réseaux ou liaisons à certains trafic

Eléments d'interconnexion : problèmes

- Eléments conçus pour répondre a des besoins :
 - Qui ont évolué au cours du temps
 - Durée de vie courte des équipements
 - Toujours mieux et moins cher
 - Rapidement à moindre coût : pragmatique
 - Chaque élément offre certaines fonctions les « prioritaires » du marché de l'époque
- ↗ Problèmes :
 - Classification, frontières sont un peu complexes
 - Terminologie imprécise (dépend du contexte)
 - Commerciaux rarement techniciens
- Attention : le choix est un compromis entre les fonctions désirées et le coût

- Répéteur (Ethernet) – Boite noire dédiée – Remise en forme, ré-amplification des signaux (électroniques ou optiques) – But augmenter la taille du réseau (au sens Ethernet) •

Exemple : distance max entre stations A - C : 500 m ? 1000 m

Eléments d'interconnexion : répéteur

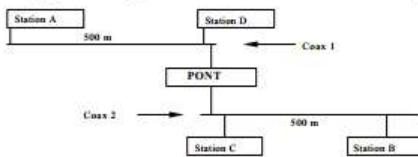
- Travaille au niveau de la couche 1
- Ne regarde pas le contenu de la trame
- Il n'a pas d'adresse Ethernet
 - Transparent pour les stations Ethernet
- Entre supports coaxiaux, TP et FO
- Avantages
 - débit 10 Mb/s
 - pas (ou très peu) d'administration
- Désavantages
 - Ne diminue pas la charge
 - Ne filtre pas les collisions
 - N'augmente pas la bande passante
 - Pas de possibilité de réseau virtuel (VLAN)

Eléments d'interconnexion : hub

- Fonction annexes :
 - Affectation d'une @ MAC (@ Eth) à chaque brin : sécurité
 - « Auto-negotiation » débit hub 10-100 (IEEE 802.3u)
 - Surveillance SNMP
- Nombre maximum sur réseau Ethernet
 - 10Base5 : 4 répéteurs
 - 10BaseT : 4 hubs
 - Distance max entre 2 stations : 500 m
 - 100BaseT : 4 hubs
 - Mais distance max entre 2 stations : 250 m
 - 1000BaseX : utilise des commutateurs
 - En cœur de réseau, pour serveurs, et même pour stations
- Utilisation actuelle
 - En « extrémité » de réseau (stations utilisateurs)
 - Remplacés par des commutateurs Ethernet
 - En cœur de réseau, pour serveurs, et même pour stations

Elts d'interconnexion : pont (Ethernet)

- Aussi appelé répéteur filtrant ou "bridge"



- Niveau de la couche 2

- Traitement : valeur @ MAC destinataire ↗ transmet ou non : trafic A-D ne va pas sur coax 2

Elts d'interconnexion : commutateur

- Commutateur – Switch Ethernet de niveau 2
 - 10, 100, 1000 Mb/s TP ou FO
- Fonction : multi-ponts, cœur d'étoile
- Commute les trames Ethernet sur un port ou un autre

• Avantages

- Augmente la distance max entre 2 stations Ethernet
 - Diminue la charge des réseaux et limite les collisions
 - Le trafic entre A et D ne va pas sur Coax 2

• Remplacés en LAN par les commutateurs

• Fonctions supplémentaires : cf commutateurs

• Ponts distants

- Ethernet – Liaison spécialisée (cuivre ou hertzienne ou laser)
 - Encore utilisés

• Mêmes fonctions et avantages que le pont + augmentation de la bande passante disponible

• Matériels - logiciel

- Chassis ou boîtier
 - Cartes : 2 ports FO, 8 ports TP ... avec débits 10, 100, 1000 Mb/s
 - Système d'exploitation
 - Configuration : telnet, client Web
 - Surveillance : SNMP

• Quelques critères de choix techniques (performances)

- Bus interne avec un débit max : 10 Gb/s
 - Vitesse de commutation nb de trames / s
 - Bande passante « annoncée » : 24 Gb/s
 - Nb d'adresses MAC mémorisable / interface

Elts d'interconnexion : commutateur

- Permet : Ethernet Full duplex (TP ou FO)
 - Emission et réception en même temps : 2x10 ou 2x100
 - « Auto-negotiation » possible (IEEE 802.3u)
- Fonctions supplémentaires
 - Auto-sensing débit (IEEE 802.3u)
 - Affectation statique d'@ MAC et filtrage au niveau 2
 - Spanning Tree : évite les boucles
 - Construction d'un arbre
 - A un instant : un seul chemin utilisé
 - Réseaux virtuels : VLAN
 - Port d'écoute qui reçoit tout le trafic des autres ports
 - Analyseur
- Limitations d'un réseau de commutateurs
 - Théoriquement pas de distance maximum
 - Broadcast et multicast diffusés partout
 - 1 seul réseau IP possible
- Très répandu :
 - Local : workgroup switch
 - Campus : complété par le routeur (plus « lent » et plus cher)
 - Remplacé par le commutateur-routeur (plus cher) quand besoin

Commutateur-routeur (IP)

- Multilayers switch
- Réunion des fonctions commutateur et routeur dans une seule « boite »
- On peut configurer certains ports en commutation, d'autres en routage
- L'équipement à tout faire
 - Mais pour le configurer il est nécessaire d'avoir défini l'architecture que l'on veut mettre en place
- Maintenant très performant avec des prix très compétitifs
 - Remplace les routeurs et les commutateurs

Caractéristiques techniques d'Ethernet

- Une technologie d'accès LAN et MAN
- Standardisé IEEE 802.3
- Aidé par IEEE 802.1 (Bridging) et IEEE 802.2 (LLC).
- de couche Liaison de données (L2) MAC : CSMA/CD
- et de couche Physique (L1)
- réputée non fiable (sans messages de fiabilité)
- non orientée connexion (pas d'établissement d'un canal préalable à la communication)

Principe CSMA (Carrier Sense Multiple Access)

1. Une interface qui tente de placer une trame écoute le support.
2. En cas de porteuse, elle tarde le placement de la trame.
3. En l'absence de porteuse (support libre), elle attend encore quelques instants (96 Bit Time) et commence à placer le trafic.
4. Elle va rester attentive à d'éventuelles collision pendant un certain délai appelé le "slot time" (512 Bit Time).
5. Après expiration de ce délai, l'interface n'est plus attentive à d'éventuelles collisions. Elle considère le canal acquis. Elle continue à émettre sans plus rien attendre (pas de ACK).
6. Sur media partagé, quelle que soit la topologie physique, toutes les interfaces reçoivent ce trafic. Elles examinent toutes l'en-tête Ethernet du trafic reçu, ce qui suscite de la charge en CPU et en bande passante.
7. Seule l'interface qui reconnaît son adresse MAC dans le champ destination livre la trame à la couche supérieure

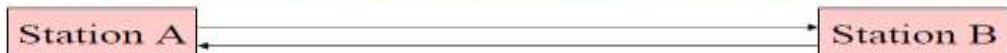
Synthèse des normes Ethernet

Nom commercial	Vitesse	Dénomination physique	Standard	Support, longueur
Ethernet	10 Mbps	10BASE-T	IEEE 802.3	Cuivre, 100 m
Fast Ethernet	100 Mbps	100BASE-TX	IEEE 802.3u	Cuivre, 100 m
Gigabit Ethernet	1000 Mbps	1000BASE-SX, 1000BASE-LX	IEEE 802.3z	Fibre, 550 m, 5 Km
Gigabit Ethernet	1000 Mbps	1000BASE-T	IEEE 802.3ab	Cuivre, 100 m
10Gigabit Ethernet	10 Gbps	10GBASE-SR, 10GBASE-LR	IEEE 802.3ae	Fibre, 300 m, 25 Km
10Gigabit Ethernet	10 Gbps	10GBASE-T	IEEE 802.3an	Cuivre, 100 m

❖ Gigabit Ethernet respecte les contraintes et objectifs suivants :

- un débit de 1 Gbit/s
- conserver le format de trame IEEE 802.3
- préserver la taille minimum et maximum des trames IEEE 802.3
- fonctionner en *half-duplex* comme en *full-duplex*
- conserver une topologie physique en étoile
- utiliser la méthode d'accès CSMA/CD
- gérer un domaine de collision dont le diamètre est égal à 200 mètres
- rester compatible avec versions précédentes FastEthernet (IEEE 802.3u) et Ethernet (IEEE 802.3).

Réseaux locaux commutés: mode bidirectionnel (' full duplex ')



- **Connexion directe entre deux stations ou entre une station et un commutateur (câblage en étoile)**
 - ▀ Une seule station connectée => **pas de partage de voie commune.**
 - ▀ Une station peut **émettre** à un instant donné vers le commutateur et **recevoir** en même temps.
 - ▀ Mode de communication **bidirectionnel simultané (full duplex)** possible.
- **Possibilité de parallélisme : débit plus important.**
- **Moins de contraintes de distance.**

Les différentes spécifications Gigabit Ethernet

- ❖ Il existe en fait deux spécifications :
 - 802.3z (juin 1998) : 1000BASE-LX, 1000BASE-SX et 1000BASE-CX (fibre optique)
 - 802.3ab (juin 1999) : 1000BASE-T (cuivre)

- ❖ Les différentes spécifications :
 - 1000BASE-LX (*Long wavelength*) : fibre optique de type monomode ou multimode (1350 nm). Distances : monomode (5000 m) et multimode (550 m).
 - 1000BASE-SX (*Short wavelength*) : fibre optique de type multimode (850 nm). Distances maximales : 220 à 550 m.
 - 1000BASE-LH (*Long Haul*) : non couverte par l'IEEE. Distances : de 10 à 40 km. Compatible avec 1000Base-LX du point de vue des connecteurs.
 - 1000BASE-CX : paires torsadées blindées (STP) d'impédance 150 ohms. Distance : limitée à 25 m (utilisation limitée aux liaisons de brassage). Utilise un codage 8B/10B NRZI.
 - 1000BASE-T (IEEE 802.3ab) : paires torsadées de Cat. 5 non blindée (UTP), cat. 6 et 7. Distance : entre 25 et 100 m. Utilise les 4 paires en parallèle et en **full-duplex** (250 Mbit/s sur chaque paire). Codage à 5 niveaux appelé PAM-5 (*Pulse Amplitude Modulation*).

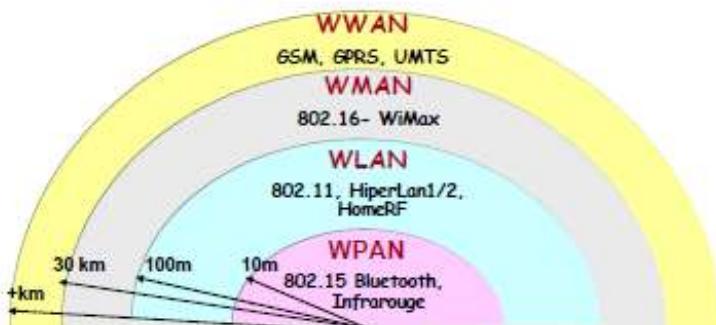
Half-duplex/Full-Duplex

La microsegmentation (un port de commutateur = une poste de travail) va offrir :

- Un domaine sans collision sur chaque port
- La bande passante dédiée sur chaque port
- Des transmissions en **full-duplex** (un canal pour l'émission et un autre pour la réception)

Les réseaux WLAN

- * Réseaux locaux sans fil (**Wireless Local Area Networks**)
- * Faire communiquer des dispositifs sans fil dans une zone de couverture moyenne



Les standards réseaux sans fils

- **WPAN :**
 - IEEE 802.15 (WiMedia)
 - IEEE 802.15.1 : Bluetooth
 - IEEE 802.15.3 : UWB (Ultra Wide Band)
 - IEEE 802.15.4 : ZigBee
 - HomeRF
- **WLAN :**
 - IEEE 802.11 (Wifi)
 - IEEE 802.11b
 - IEEE 802.11a
 - IEEE 802.11g
 - IEEE 802.11n
 - HiperLAN 1/2
- **WMAN**
 - IEEE 802.16 (WiMax)
 - IEEE 802.16a
 - IEEE 802.16b
 - IEEE 802.20 (MBWA)

► Définition

- ▶ Un réseau d'ordinateurs et de matériels sans fil qui offre les fonctionnalités des réseaux locaux LAN traditionnels (Ethernet), mais en utilisant une technologie sans fil.

► Dans la pratique

- ▶ Un WLAN permet de relier des ordinateurs portables, des machines de bureau, des assistants personnels (PDA) ou même des périphériques à une liaison haut débit (de 11 Mbit/s en 802.11b à 54 Mbit/s en 802.11a/g) sur un rayon de plusieurs dizaines de mètres en intérieur (généralement entre une vingtaine et une cinquantaine de mètres) et de centaines de mètres en extérieur (500m)

Wireless LAN (WLAN) ou WiFi

► Normes IEEE 802.11 (WiFi)

- ▶ IEEE = Institute of Electrical and Electronics Engineers
- ▶ La norme initiale 802.11 a connu de nombreuses révisions notées 802.11a, 802.11b, 802.11g pour les principales.
- ▶ Ces révisions visent essentiellement une amélioration du débit et/ou une amélioration de la sécurité.

► Wi-Fi (Wireless Fidelity)

- ▶ Un « label » commercial décerné par un groupement de constructeurs (« Wireless Ethernet Compatibility Alliance », WECA) depuis 1999, renommé « Wi-Fi Alliance » en 2003.
- ▶ Valide le respect du standard et l'inter-opérabilité entre matériels
- ▶ Souvent en avance sur la normalisation IEEE



► Dans la pratique, les 2 sont confondus

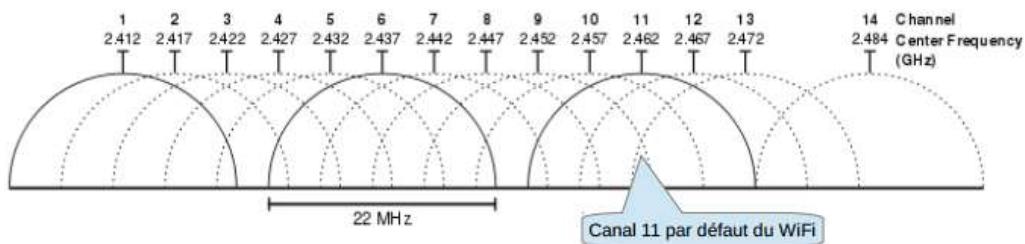
Supports de transmission du WiFi

► Infra-rouge

- Signal facilement bloqué, nécessite un espace dégagé, de faible portée, débit de seulement 4 Mbps
- Adapté aux transmissions de données entre ordinateurs et imprimante

► Fréquences radio

- Passe à travers la plupart des obstacles dans un bureau
- Bandes des 2.4Gz organisées en 14 canaux de 22Mhz de large



Débits et distance

► Technologie dépendant de l'environnement

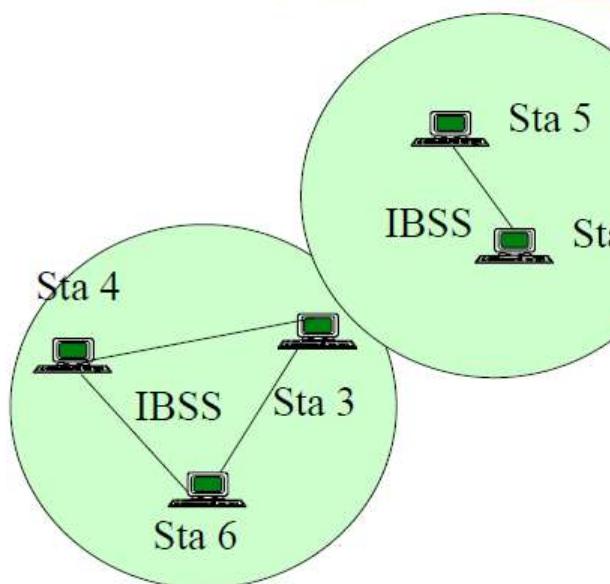
- Type de construction (cloisons, murs, matériaux)
- Implantation des antennes
- Interférences (bluetooth, micro-ondes, autres réseaux WiFi)

► Comparaison des débits en fonction de la distance

Norme	débit théorique	portée en intérieur	usage
802.11a	54 Mbit/s	25 mètres	Accès au haut débit mais à courte portée.
802.11b	11 Mbit/s	35 mètres	Norme assez courante, utile pour le surf sur Internet. À éviter pour le streaming de vidéos ou le jeu en ligne.
802.11g	54 Mbit/s	25 mètres	Norme la plus répandue. Permet de jouer et de regarder des vidéos sur le Net avec un certain confort. Le transfert de fichiers volumineux reste long.
802.11n	540 Mbit/s	50 mètres	La norme à venir. Le très haut débit sans fil.

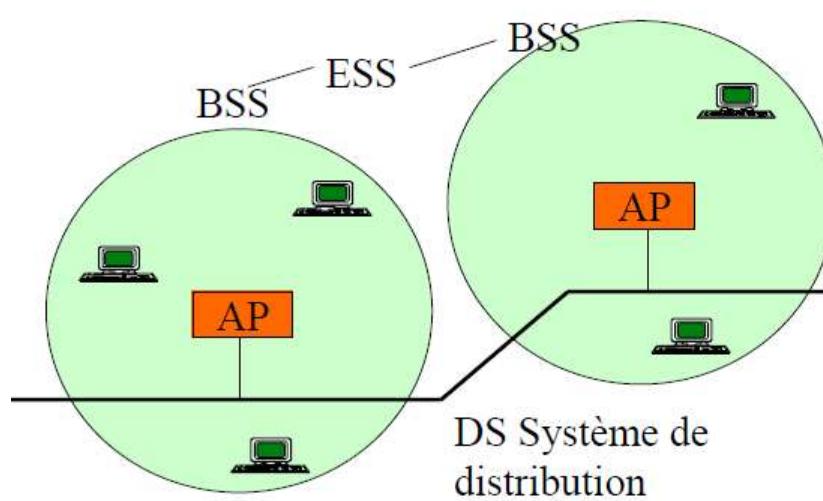
- **1) WIFI : un réseau local radio.**
 - | Définition sur les deux niveaux **physique** et **liaison**.
- **2) WIFI : deux organisations architecturales.**
 - | Le mode **infrastructure (centralisé)**.
 - | Le mode **ad 'hoc (distribué)**.
- **3) WIFI : deux protocoles différents** d'accès au médium.
 - | **PCF** 'Point Coordination Function' (**en coopération**).
 - | **DCF** 'Distributed Coordination Function' (**en compétition**)
 - | Pouvant être utilisés simultanément par une station.
- **4) WIFI : différents niveaux physiques** selon le débit, le codage, la bande de fréquences utilisée.
 - | 802.11, 802.11a , **802.11b** , **802.11g**, en cours 802.11n.
- **5) Consortium de développement : WIFI Alliance** 99

Le niveau liaison Wifi : **Le mode ad'hoc (distribué)**



- | IBSS 'Independent Basic Service Set' : ensemble de stations avec coupleurs sans fils, communicantes dans la même bande.
- | Terminologie: mode ad 'hoc, 'peer to peer'
- | Protocole DCF : Distributed Coordination Function.

Le niveau liaison Wifi : Le mode 'infrastructure' (centralisé)



- AP 'Access Point' commutateur.
- Station de travail avec un coupleur WIFI.
- **BSS** (Basic Service Set): un seul AP.
- **ESS** ('Extended Service Set') : plusieurs AP connectés par un autre réseau (réseau Ethernet ou sans fil).
- Changement de point d'accès: **handover/roaming** (itinérance).
103

Le niveau liaison Wifi : DCF ' Distributed Coordination Function '

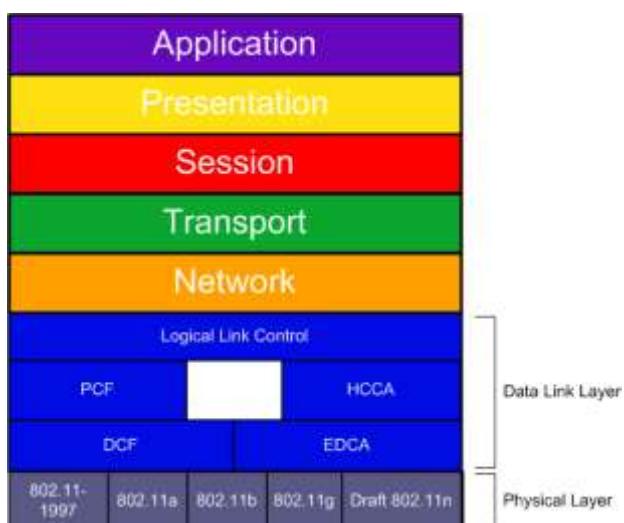
- | 1) Protocole en **compétition** avec **écoute** (CSMA).
- | 2) Ajournement **non persistant**.
- | 3) **Détection** de collisions par accusé de réception.
- | 4) **Retransmission** sur collision (binary backoff).
- | 5) Gestion de la **fragmentation**.
- | 6) Pas de **gestion de connexion**.
- | 7) Pas de **contrôle de flux**.
- | 8) Pas de garantie de livraison **sans erreurs**.
- | 9) Pas de **qualité de service** (en version de base)

Le niveau liaison Wifi : PCF ' Point Coordination Function '

- ▶ 1) Fonctionnement en **scrutation ('polling')** par le PC ('Point Coordinator').
- ▶ 2) Une station **émet** si elle est **autorisée par le PC**.
- ▶ 3) Le PC **sélectionne** une station en plaçant son adresse dans la trame.
- ▶ 4) Les trames sont acquittées. Si l'acquittement ne revient pas le **PC ou la station effectuent la retransmission**.
- ▶ 5) **PCF** a plutôt été destiné à des échanges à **qualité de service**.

Les risques liés à la mauvaise protection d'un réseau sans fil sont multiples :

1. **L'interception de données** consistant à écouter les transmissions des différents utilisateurs du réseau sans fil
2. **Le détournement de connexion** dont le but est d'obtenir l'accès à un réseau local ou à internet
3. **Le brouillage des transmissions** consistant à émettre des signaux radio de telle manière à produire des interférences
4. **Les dénis de service** rendant le réseau inutilisable en envoyant des commandes factices



Les normes WiFi

Normes	Débit max	Fréquence	Date	Description
802.11	1 à 2 Mb/s	2,4 Ghz	1997	Première norme WiFi
802.11a	54 Mb/s	5 GHz	1999	- haut-débit sur 8 canaux - de 50Mbps jusqu'à 10m à 6Mbps jusqu'à 70m
802.11b	11 Mb/s	2,4 GHz	1999	- fixe un débit moyen maximum à 11 Mb/s théorique - portée de 50m en intérieur à 300 mètres en extérieur - spécifie 3 canaux radio (1, 6 et 11)
802.11g	54 Mb/s	2,4 GHz	2001	- fixe un débit moyen maximum à 54 Mbits/s théorique une - portée de 25m en intérieur à 75 mètres en extérieur - spécifie 3 canaux radio (1, 6 et 11)
802.11i			2004	- améliore la sécurité (authentification, cryptage et distribution des clés) en s'appuyant sur la norme Advanced Encryption Standard.
802.11n	270 Mb/s	2,4 GHz ou 5 GHz	2009	- regroupement des canaux - agrégation des paquets de données
802.11s	1 G/s	5 GHz	2012	- en cours de normalisation - améliore 802.11n

802.11x – Amendements

- **802.11a** - Vitesse de 54 Mbits/s (bande 5 GHz)
- **802.11b** - Vitesse de 11 Mbits/s (bande ISM 2,4 GHz)
- **802.11g** - Vitesse de 54 Mbits/s (bande ISM)
- **802.11n** - Vitesse de 100 Mbits/s (bande ISM)
- **802.11e** - Qualité de service
- **802.11x** – Amélioration de la sécurité (court terme) : WEP
- **802.11i** - Amélioration de la sécurité (long terme) : AES
- **802.11f** – itinérance : Inter-Access point roaming protocol

Les différentes normes WiFi

La norme *IEEE 802.11* est en réalité la norme initiale offrant des débits de 1 ou 2 Mbps. Des révisions ont été apportées à la norme originale afin d'optimiser le débit (c'est le cas des normes 802.11a, 802.11b et 802.11g, appelées normes 802.11 physiques) ou bien préciser des éléments afin d'assurer une meilleure sécurité ou une meilleure interopérabilité. Voici un tableau présentant les différentes révisions de la norme 802.11 et leur signification :

Nom de la norme	Nom	Description
802.11a	Wifi5	La norme 802.11a (baptisé <i>WiFi 5</i>) permet d'obtenir un haut débit (54 Mbps théoriques, 30 Mbps réels). La norme 802.11a spécifie 8 canaux radio dans la bande de fréquence des 5 GHz.
802.11b	Wifi	La norme 802.11b est la norme la plus répandue actuellement. Elle propose un débit théorique de 11 Mbps (6 Mbps réels) avec une portée pouvant aller jusqu'à 300 mètres dans un environnement dégagé. La plage de fréquence utilisée est la bande des 2.4 GHz, avec 3 canaux radio disponibles.
802.11c	Pontage 802.11 vers 802.1d	La norme 802.11c n'a pas d'intérêt pour le grand public. Il s'agit uniquement d'une modification de la norme 802.1d afin de pouvoir établir un pont avec les trames 802.11 (<i>niveau liaison de données</i>).
802.11d	Internationalisation	La norme 802.11d est un supplément à la norme 802.11 dont le but est de permettre une utilisation internationale des réseaux locaux 802.11. Elle consiste à permettre aux différents équipements d'échanger des informations sur les plages de fréquence et les puissances autorisées dans le pays d'origine du matériel.
802.11e	Amélioration de la qualité de service	La norme 802.11e vise à donner des possibilités en matière de qualité de service au niveau de la couche <i>liaison de données</i> . Ainsi cette norme a pour but de définir les besoins des différents paquets en terme de bande passante et de délai de transmission de telle manière à permettre notamment une meilleure transmission de la voix et de la vidéo.
802.11f	Itinérance (roaming)	La norme 802.11f est une recommandation à l'intention des vendeurs de point d'accès pour une meilleure interopérabilité des produits. Elle propose le protocole <i>Inter-Access point roaming protocol</i> permettant à un utilisateur itinérant de changer de point d'accès de façon transparente lors d'un déplacement, quelles que soient les marques des points d'accès présentes dans l'infrastructure réseau. Cette possibilité est appelée <i>itinérance</i> (ou <i>roaming en anglais</i>)

802.11g		La norme 802.11g offre un haut débit (54 Mbps théoriques, 30 Mbps réels) sur la bande de fréquence des 2.4 GHz. La norme 802.11g a une compatibilité ascendante avec la norme 802.11b, ce qui signifie que des matériels conformes à la norme 802.11g peuvent fonctionner en 802.11b
802.11h		La norme 802.11h vise à rapprocher la norme 802.11 du standard Européen (HiperLAN 2, où le <i>h</i> de 802.11h) et être en conformité avec la réglementation européenne en matière de fréquence et d'économie d'énergie.
802.11i		La norme 802.11i a pour but d'améliorer la sécurité des transmissions (gestion et distribution des clés, chiffrement et authentification). Cette norme s'appuie sur l'AES(<i>Advanced Encryption Standard</i>) et propose un chiffrement des communications pour les transmissions utilisant les technologies 802.11a, 802.11b et 802.11g.
802.11lr		La norme 802.11r a été élaborée de telle manière à utiliser des signaux infra-rouges. Cette norme est désormais dépassée techniquement.
802.11j		La norme 802.11j est à la réglementation japonaise ce que le 802.11h est à la réglementation européenne.

D'autres amendements qui concernent principalement la couche MAC du standard ont aussi été validés :

Amendement	Date de publication	Description
802.11d	2001	Permet la récupération dynamique des contraintes de transmissions (puissance max., canaux autorisés) en fonction des régulations locales.
802.11h	2003	Décrit des mécanismes permettant de mesurer et de sélectionner dynamiquement les canaux afin de respecter leurs conditions d'utilisations locales (notamment nécessaires pour l'utilisation de la bande ISM à 5 GHz en Europe ¹).
802.11i	2004	Ajoute des mécanismes d'identification et de chiffrement des données (WPA), afin de remplacer l'algorithme initial WEP de la norme 802.11 qui est obsolète.
802.11j	2004	Décrit les modifications nécessaires à l'utilisation des bandes de fréquences à 4.9 GHz et 5 GHz en conformité avec la régulation japonaise.
802.11e	2005	Ajoute des mécanismes de QoS dans les réseaux 802.11.
802.11r	2008	Vise à améliorer la mobilité entre les cellules d'un réseau Wi-Fi (le handover) et permettre à un appareil connecté de basculer plus vite d'un point d'accès vers un autre.
802.11u	2007	Elle vise à faciliter la reconnaissance et la sélection des réseaux et l'interfonctionnement avec d'autres réseaux externes tels les réseaux mobiles pour permettre l'interopérabilité entre différents fournisseurs de services.
802.11y	2008	L'intérêt de cette version tient à sa grande portée jusqu'à 5 000 m en extérieur. La fréquence utilisée est de 3.7 GHz, ce qui la rend incompatible avec les cartes "usuelles" (a/b/g/n/ac).
802.11w	2009	Augmente la sécurité des trames de management.

En 2007, puis en 2012², la plupart des amendements principaux à la norme 802.11 (a,b,d,e,g,h,i,j puis n) ont été directement intégrés dans la norme par le groupe IEEE 802.11ma et sont disponibles sous la forme d'un unique document².

IEEE 802.11 fait partie d'un ensemble de normes édictées sous l'égide du comité de standardisation IEEE 802 à partir de 1997. Celui-ci constitue un tout cohérent servant de base de travail aux constructeurs développant des équipements et les services chargés de l'implémentation des infrastructures réseaux à liaison filaire et sans fil.

Le schéma ci-dessous est une adaptation du synopsis du standard IEEE 802 consigné dans la section "introduction" de la plupart des normes publiées sous ce standard. Celui-ci est articulé autour de la norme IEEE 802.11 qui donne des spécifications relatives à l'implémentation de la couche PHY et de la sous-couche MAC (Couche liaison de données du modèle OSI) pour les réseaux locaux à liaison sans fil (WLAN).

L'ensemble articulé autour de la norme IEEE 802.11 se décompose en éléments identifiés comme suit :

- **802** : standard général de base pour le déploiement de réseaux numériques locaux ou métropolitains à liaison filaire ou sans fil ;
- **802.1** : gestion des réseaux ;
- **802.10** : sécurisation des échanges pour les systèmes à liaison filaire ou sans fil (Token Ring, Ethernet, Wi-Fi, WiMAX) ;
- **802.11** : spécifications pour l'implémentation de réseaux numériques locaux à liaison sans fil ;
- **802.2** : description générale de la sous-couche Logical Link Control.

Protocole	Date de normalisation	Fréquence	Taux de transfert (Typ)	Taux de transfert (Max)	Portée moyenne (intérieur) [réf. nécessaire]	Portée (étranger) [réf. nécessaire]
Norme initiale	1997	2,4-2,5 GHz	1 Mbit/s	2 Mbit/s	?	?
802.11a	1999	5,15-5,35/5,47-5,725/5,725-5,875 GHz	25 Mbit/s	54 Mbit/s	~25 m	~75 m
802.11b	1999	2,4-2,5 GHz	6,5 Mbit/s	11 Mbit/s	~35 m	~100 m
802.11g	2003	2,4-2,5 GHz	25 Mbit/s	54 Mbit/s	~25 m	~75 m
802.11n	2009	2,4 GHz ou 5 GHz	200 Mbit/s	450 Mbit/s	~50 m	~125 m
802.11ac	janvier 2014	5 GHz	433 Mbit/s	1300 Mbit/s	~20 m	~50 m

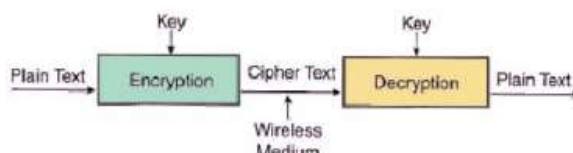
Clé WEP

► Le WEP (Wired Equivalent Privacy) est un mécanisme de cryptage des données

- ▶ Basé sur une clé secrète de 64 ou 128 bits Cette clé doit être connue de la station et du point d'accès.
- ▶ Une clé de session générée de façon aléatoire.
- ▶ Ce protocole a été cassé en 2001 via sa clé de session

► Authentification par clé partagée

- ▶ Clé secrète partagée par toutes les stations (doit être renseigné par un autre canal, le plus souvent à la main)
- ▶ WEP 64 : clé de 40 bit, WEP 128 : clé de 104 bits
- ▶ Confidentialité par cryptage



► une authentification du terminal par clé partagée

- ▶ selon le mode « challenge-response »

► et le chiffrement des données

- ▶ avec algorithme de chiffrement symétrique: RC4 (Rivest Cipher)

WEP – les points faibles

- Clés statiques partagées (40 bits "64", 104 bits "128")
 - Rarement changées
 - Vol de machine => vol de clef
 - Les autres qui partagent la clef peuvent lire vos trames
 - Possède une durée de vie longue
 - Diffusion d'une nouvelle clé difficile si le parc de mobile est important.
- Possibilité de choisir la clé dans l'espace des caractères imprimables.
 - Avec une clé de 40 bits et un jeu de 70 caractères :
 - ~ 1.500 millions de combinaisons différentes.
 - => Attaque par force brute possible.

WEP : Authentification des stations

- Envoi d'une requête d'authentification par la station vers l'AP
- l'AP envoie un « challenge » à la station mobile
- Le mobile chiffre le challenge avec l'algorithme WEP et la clé secrète et transmet le résultat (la réponse) au AP
- Le point d'accès déchiffre la réponse à l'aide de la clé secrète et l'algorithme WEP et compare la valeur obtenue.

• Si valeur identique alors mobile authentifié.

Open System Authentication



Shared Key Authentication



31

- La procédure de chiffrement WEP utilise 3 éléments en entrée :
 - ➔ Un vecteur d'initialisation (IV) de 24 bits (nombre pseudo aléatoire)
 - ➔ une clé secrète partagée (K) de 40 bits ou 104 bits
 - ➔ Le texte en clair (P) à chiffrer
- Etape 1 : le vecteur d'initialisation est concaténé à la clé pour former une sous-clé (seed) de 64 bits ou 128 bits.
- Etape 2 : La sous-clé est utilisée par l'algorithme RC4 pour générer une séquence de clé de chiffrement
- Etape 3 : une valeur d'intégrité (ICV) de 32 bits est calculée sur le texte en clair (P) en utilisant l'algorithme CRC-32.
- Etape 4 : ICV est concaténé à P
- Etape 5 : (P+ICV) est XORé avec la clé
- Etape 6 : message chiffré + IV en clair sont envoyés

RC4: Principes

RC4: Rivest Cipher 4

- Algorithme simple permettant le cryptage et le décryptage
- Repose sur la génération d'un flot aléatoire (key stream) et l'opérateur OU Exclusif (XOR)
- Cryptage: Message en clair XOR key stream = Message crypté
- Décryptage : Message crypté XOR key stream = Message en clair

RC4: fonctionnement

2 phases:

- Initialisation
- Génération d'un nombre pseudo-aléatoire

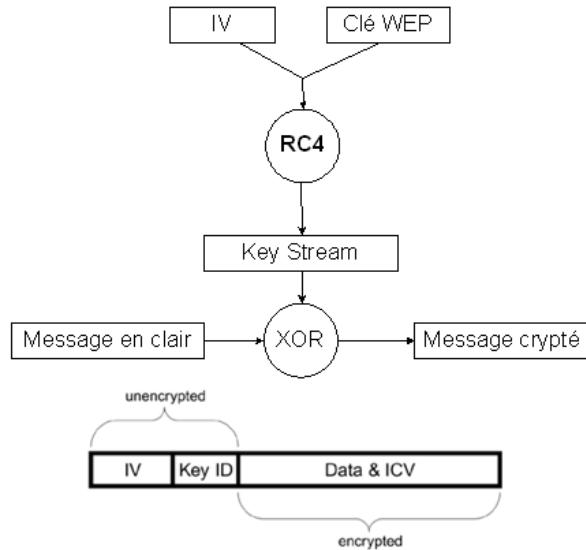
Initialisation grâce à un vecteur d'initialisation concaténé avec la clé WEP

- Génération d'un tableau de 256 octets
- permutations grâce à la clé

Génération d'un nombre pseudo-aléatoire

- Nouvelle permutation
- octet choisi dans le tableau (R)

Ensuite, chaque octet du message est XORé avec la valeur R choisie



La clef RC4 est symétrique.

Dans WEP :

- pas de protocole de gestion des clés : une unique clé partagée entre tous les utilisateurs.

AUTHENTIFICATION

Deux méthodes :

- Ouvert : pas de clef demandée. Association faite par le serveur à une requête du client. Les messages peuvent ensuite éventuellement être chiffrés avec la clef WEP.
- À clef partagé :
 - le client envoie une requête d'authentification au point d'accès (AP)
 - le point d'accès envoie un texte en clair pour un challenge
 - le client doit chiffrer le texte en clair en utilisant la clef WEP et la renvoyer à l'AP.
 - le point d'accès déchiffre le texte et le compare au texte en clair envoyé et renvoie une réponse positive ou négative
 - Après authentification et association, WEP peut être utilisé pour chiffrer les données.

WAP/WAP2

- ▶ juin 2004
- ▶ norme 802.11i
- ▶ WPA Wireless Protected Access
- ▶ WPA2 et le nom commercial de wpa
- ▶ 4 phases
 - 1) Mise en accord sur la politique de sécurité
 - 2) Authentification
 - 3) Dérivation et distribution des clés
 - 4) Chiffrement et intégrité de la RSNA (robust security network association)

Problèmes avec WEP

- Plusieurs attaques possibles :
 - Accès non autorisé.
 - Modification des messages.
 - Attaque par dictionnaire.
 - Etc.
- 15 minutes pour casser une clé de 40 bits en attaque passive, pas beaucoup plus long pour une clé de 128 bits !

Le protocole WPA offre une protection d'un niveau bien supérieur à WEP. Il utilise pourtant le même algorithme de chiffrement et est basé sur le même principe de vecteur d'initialisation. En revanche le TKIP (Temporal Key Integrity Protocol ou Protocole d'intégrité par clé temporelle) a été ajouté, permettant ainsi une permutation plus importante des clés sans que le vecteur d'initialisation ne puisse être reconstitué de manière utile. Dans les configurations les plus courantes, le mode Personnel est utilisé avec la PSK (Pre-Shared Key ou clé pré-partagée). Cela permet d'utiliser une clé alphanumérique normale d'une longueur d'au moins 32 caractères. Ce qui offre un niveau de protection tout à fait acceptable.

Le protocole WPA2 quant à lui utilise un algorithme de chiffrement beaucoup plus puissant, utilisé dans le cryptage des documents sensibles et possédant une clé très forte. Il s'agit de la dernière norme du protocole WPA permettant de protéger votre réseau WLAN.

Malheureusement une faille très importante a été découverte au mois de juillet 2010 dans ce protocole qui reste néanmoins considéré comme le plus sécurisé.

La Wi-Fi Alliance a ainsi créé une nouvelle certification, baptisée **WPA2**, pour les matériels supportant le standard 802.11i ([ordinateur portable](#), [pda](#), [carte réseau](#), etc.).

Contrairement au WPA, le WPA2 permet de sécuriser aussi bien les réseaux sans fil en [mode infrastructure](#) que les réseau en [mode ad hoc](#).

Architectures WPA

La norme IEEE 802.11i définit deux modes de fonctionnement :

- **WPA Personal** : le mode « WPA personnel » permet de mettre en oeuvre une infrastructure sécurisée basée sur le WPA sans mettre en oeuvre de serveur d'authentification. Le WPA personnel repose sur l'utilisation d'une clé partagée, appelées **PSK** pour *Pre-shared Key*, renseignée dans le point d'accès ainsi que dans les postes clients. Contrairement au WEP, il n'est pas nécessaire de saisir une clé de longueur prédéfinie. En effet, le WPA permet de saisir une « *passphrase* » (*phrase secrète*), traduite en *PSK* par un algorithme de hachage.
- **WPA Enterprise** : le mode entreprise impose l'utilisation d'une infrastructure d'authentification 802.1x basée sur l'utilisation d'un serveur d'authentification, généralement un serveur RADIUS (*Remote Authentication Dial-in User Service*), et d'un contrôleur réseau (le point d'accès)

WPA-1 (2004 - IEEE 802.11i) utilise

- **Confidentialité** : l'algorithme de chiffrement par flot RC4 avec une clef de 154 bits (128 bits + 48 bits IV)
- **Intégrité** : la somme de contrôle MIC (Message Integrity Code - "Michael" dérivé de MAC) plus sécurisé que CRC32 + compteur de trame pour empêcher les attaques par rejet.
- **Protocole de gestion des clefs** : protocole Temporal Key Integrity Protocol (TKIP), qui échange de manière dynamique les clés lors de l'utilisation du système.

WPA2

- **Confidentialité** : chiffrement basé sur AES plutôt que sur RC4.
- **Protocole de gestion des clefs** : protocole CCMP

Le TKIP (*Temporal Key Integrity Protocol*) est proposé en 2002 sous le nom de WPA

4 modifications principales:

1. un **compteur** (incrémental) sur 48 bits pour les IV
2. la **génération périodique d'une nouvelle clé** dérivée temporaire
3. **une clé pour chaque paquet**, longue de 128 bits et dérivée de la clé temporaire, de l'IV et du compteur
4. un **vrai mécanisme d'intégrité (MAC)**

EAP (Extended Authentication Protocol) RFC 2284.

- Protocole général qui supporte de multiples méthodes (carte à puce, token cards, one-time passwords, kerberos, public key encryption, etc) d'authentification.
- EAP peut :
 - Renouveler les clés.
 - Authentifier utilisateur.
 - Faire une authentification mutuelle.

Extensible Authentication Protocol (EAP)

est un mécanisme d'identification universel, fréquemment utilisé dans les réseaux sans fil et les liaisons Point-A-Point



LE WPA2: AMÉLIORATIONS

Pour compatibilité, le WPA utilise RC4 comme algorithme de chiffrement.

Bien que plus sûr que WEP, le WPA utilise un algo faible

IEEE adopte le WPA en 2004 après quelques modifications:

- ▶ support de l'AES pour le chiffrement
- ▶ mode confidentialité-authenticité: CCMP (*Counter mode, CBC-MAC, Protocol*)
- ▶ inclut une gestion de clé plus soignée (liens *ad-hoc*...)

IEEE 802.11i = WPA2 = TKIP-AES

- WPA : *Wireless Protected Access*
 - Solution du WECA pour corriger les erreurs du WEP
- Profil de 802.11i promu par le WECA
 - Permet de combler une partie des problèmes du WEP
 - Utilisation du mécanisme TKIP
 - Changement des clefs de chiffrement de façon périodique
 - 10ko de données échangées
 - Clef à 128 bits
 - Vecteur d'initialisation de 48bits (281 474 976 710 656 possibilités)
 - Impossibilité de réutiliser un même IV avec la même clef
 - Utilisation du MIC qui est un contrôle d'intégrité de tout le message
- 2 modes de fonctionnement
 - Mode PSK (*PreShared Key*) : secret partagé
 - Mode à base de 802.1X pour une authentification centralisée

- Le WPA n'intègre pas les sécurisation que le 802.11i apporte :
 - La sécurisation des réseaux multi-point Ad-Hoc
 - N'implémente pas AES comme algorithme de chiffrement
- Nécessite des équipements capables de l'implémenter
 - Les anciens équipements ont la plupart du temps la possibilité de mettre à jour leur software
 - Infrastructure à base de Radius (sauf en mode PSK)
 - C'est du 802.1X



- Définition d'un RSN (*Robust Security Network*) permettant de garantir :
 - Sécurité et mobilité
 - Authentification du client indépendamment du lieu où il se trouve
 - Intégrité et Confidentialité
 - Garantie d'une confidentialité forte avec un mécanisme de distribution dynamique des clefs
 - Passage à l'échelle et flexibilité
 - Ré-authentification rapide et sécurisée en cas de « handover », séparation du point d'accès et du processus d'authentification pour le passage à l'échelle, architecture de sécurité flexible
- Associations construites autour d'authentifications fortes : RSNA (*Robust Security Network Association*) – dépendantes de 802.1x
 - PMKSA : Pairwise Master Key Authentication Security Association (contexte post 802.1x)
 - PTKSA : Pairwise Transient Key Security Association (contexte post 4 Way Handshake)
 - GTKSA : Group Transient Key Security Association (contexte post Grouk Key Handshake)
 - STAKeySA : Station Key Security Association (contexte post STAKey Handshake)
- Sécurité au niveau MAC :
 - TKIP (*Temporal Key Integrity Protocol*) - Optionnel
 - CCMP (*Counter-mode/CBC-MAC-Protocol*) - Obligatoire
 - Le TSN (*Transition Security Network*) permet une compatibilité avec les anciens mécanismes (*Open Authentication, Shared Key Authentication, WEP*)



TKIP – Généralités

- Algorithme de chiffrement sous jacent : RC4, utilisé correctement (au sens cryptographique du terme)
- Les apports de TKIP par rapport au WEP :
 - Utilisation d'un algorithme de hachage cryptographique non linéaire : MIC (*Message Integrity Code*) basé sur Michael (Niels Ferguson)
 - Impossibilité de réutiliser un même IV avec la même clef (l'IV joue maintenant un rôle de compteur appelé TSC (*TKIP Sequence Counter*)) et augmentation de la taille de l'IV à 48 bits
 - Utilisation de clés de 128 bits (et non 40 ou 104 bits pour le WEP)
 - Intègre des mécanismes de distribution et de changement de clés
 - Utilise une clé différente pour le chiffrement de chaque paquet : PPK (*Per Packet Key*)

TKIP

- ★ Utilisation de RC4 comme algorithme de chiffrement (pour des raisons économiques).
- ★ Utilisation d'un algorithme de hachage cryptographique non-linéaire : MIC (*Message Integrity Code*) basé sur Michael.
- ★ Impossibilité d'utiliser le même IV avec la même clé (l'IV joue maintenant le rôle d'un compteur appelé TSC (*TKIP Sequence Counter*)) et augmentation de la taille de l'IV à 48 bits.
- ★ Utilisation de clé à 128 bits.
- ★ Intégration de mécanisme de distribution et de changement des clés.
- ★ Utilisation de clés différentes pour le chiffrement de chaque paquet.

Le fonctionnement du protocole EAP est basé sur l'utilisation d'un contrôleur d'accès (en anglais *authenticator*), chargé d'établir ou non l'accès au [réseau](#) pour un utilisateur (en anglais *supplicant*). Le contrôleur d'accès est un simple garde-barrière servant d'intermédiaire entre l'utilisateur et un serveur d'authentification (en anglais *authentication server*), il ne nécessite que très peu de ressources pour fonctionner. Dans le cas d'un [réseau sans fil](#), c'est le point d'accès qui joue le rôle de contrôleur d'accès.

Le serveur d'authentification (appelé parfois *NAS*, pour *Network Authentication Service*, traduisez *Service d'authentification réseau*, voire *Network Access Service*, pour *Serveur d'accès réseau*) permet de valider l'identité de l'utilisateur, transmis par le contrôleur réseau, et de lui renvoyer les droits associés en fonction des informations d'identification fournies. De plus, un tel serveur permet de stocker et de comptabiliser des informations concernant les utilisateurs afin, par exemple, de pouvoir les facturer à la durée ou au volume (dans le cas d'un fournisseur d'accès par exemple).

La plupart du temps le serveur d'authentification est un serveur [RADIUS](#) (*Remote Authentication Dial In User Service*), un serveur d'authentification standard défini par les RFC 2865 et 2866, mais tout autre service d'authentification peut être utilisé.

Ainsi, le schéma global suivant récapitule le fonctionnement global d'un réseau sécurisé avec le standard 802.1x :

- Le contrôleur d'accès, ayant préalablement reçu une demande de connexion de la part de l'utilisateur, envoie une requête d'identification ;
- L'utilisateur envoie une réponse au contrôleur d'accès, qui la fait suivre au serveur d'authentification ;
- Le serveur d'authentification envoie un « challenge » au contrôleur d'accès, qui le transmet à l'utilisateur. Le challenge est une méthode d'identification. Si le client ne gère pas la méthode, le serveur en propose une autre et ainsi de suite ;
- L'utilisateur répond au challenge. Si l'identité de l'utilisateur est correcte, le serveur d'authentification envoie un accord au contrôleur d'accès, qui acceptera l'utilisateur sur le réseau ou à une partie du réseau, selon ses droits. Si l'identité de l'utilisateur n'a pas pu être vérifiée, le serveur d'authentification envoie un refus et le contrôleur d'accès refusera à l'utilisateur d'accéder au réseau.

Echange de clés de chiffrement

Outre l'authentification des utilisateurs, le standard 802.1x est un support permettant de changer les clés de chiffrement des utilisateurs de manière sécurisé, afin d'améliorer la sécurité globale.

Advanced Encryption Standard ou AES (soit « standard de chiffrement avancé » en français), aussi connu sous le nom de Rijndael, est un algorithme de chiffrement symétrique. Il remporta en octobre 2000 le concours AES, lancé en 1997 par le NIST et devint le nouveau standard de chiffrement pour les organisations du gouvernement des États-Unis. Il a été approuvé par la NSA (National Security Agency) dans sa suite B¹ des algorithmes cryptographiques.

L'algorithme prend en entrée un bloc de 128 bits (16 octets), la clé fait 128, 192 ou 256 bits. Les 16 octets en entrée sont permutsés selon une table définie au préalable. Ces octets sont ensuite placés dans une matrice de 4x4 éléments et ses lignes subissent une rotation vers la droite. L'incrément pour la rotation varie selon le numéro de la ligne. Une transformation linéaire est ensuite appliquée sur la matrice, elle consiste en la multiplication binaire de chaque élément de la matrice avec des polynômes issus d'une matrice auxiliaire, cette multiplication est soumise à des règles spéciales selon GF(2⁸) (groupe de Galois ou corps fini). La transformation linéaire garantit une meilleure diffusion (propagation des bits dans la structure) sur plusieurs tours. Finalement, un XOR entre la matrice et une autre matrice permet d'obtenir une matrice intermédiaire. Ces différentes opérations sont répétées plusieurs fois et définissent un « tour ». Pour une clé de 128, 192 ou 256, AES nécessite respectivement 10, 12 ou 14 tours.

VRRP : Créé par l'IETF en 1999 (donc compatible multi vendeurs), identique à HSRP (toutefois VRRP utilise des timers plus petit par défaut le rendant plus rapide).

Virtual Router Redundancy Protocol (protocole de redondance de routeur virtuel, VRRP) est un protocole standard dont le but est d'augmenter la disponibilité de la passerelle par défaut des hôtes d'un même réseau.

Il est basé sur le protocole de redondance Cisco HSRP et il est le seul moyen de fournir de la redondance entre des routeurs de constructeurs différents.

Le routeur ayant la priorité VRRP la plus haute est élu comme maître (master). Ce dernier détient l'adresse MAC du format 00-00-5E-00-01-XX qui correspondant à l'adresse IP virtuelle VRRP.

VRRP utilise la notion de [routeur](#) virtuel, auquel est associée une [adresse IP](#) virtuelle ainsi qu'une [adresse MAC](#) virtuelle.

Parmi un groupe de routeurs participant à VRRP dans un réseau, le protocole va élire un *maître*, qui va répondre aux requêtes [ARP](#) pour l'adresse IP virtuelle, ainsi qu'un ou plusieurs routeurs de secours, qui reprendront l'adresse IP virtuelle en cas de défaillance du routeur maître.

VRRP peut être utilisé sur [Ethernet](#), [MPLS](#)] et les réseaux [Token Ring](#). Une implémentation pour le protocole [IPv6](#) est définie par la [RFC 5798](#) avec la version 3 du protocole VRRP.

Le protocole VRRP est plus déployé que d'autres protocoles similaires.[\[réf. nécessaire\]](#) VRRP est un standard IETF pris en charge par de nombreux vendeurs de routeurs ainsi que par des systèmes d'exploitation comme Linux¹.

HSRP, signifiant Hot Standby Routing Protocol, est un protocole qui permet à un routeur d'être le secours d'un autre routeur situé sur le même réseau Ethernet. HSRP est décrit par la [Rfc 2281](#) "Cisco Hot Standby Router Protocol (HSRP)". HSRP est le protocole propriétaire de Cisco inspiré du protocole normalisé VRRP.

Le principe de fonctionnement est que tous les routeurs émulent une adresse IP virtuelle qui sera utilisée comme passerelle par les équipements du réseau LAN. Pour cela, chacun des routeurs configurera son protocole HSRP avec un niveau de priorité. Celui qui disposera du plus grand se verra élu et sera actif. Les autres seront passifs en attendant la perte du premier routeur.

La communication lié au protocole HSRP entre les routeurs se fait par l'envoi de paquets Multicast à l'adresse IP 224.0.0.2 vers le [port UDP 1985](#). Cela permet principalement d'élire le routeur actif et de tester (track) sa présence.

HSRP permet qu'un routeur de secours (ou Spare) prenne immédiatement, de façon transparente, le relais dès qu'un problème physique apparaît.

En partageant une seule et même adresse IP et MAC, plusieurs routeurs peuvent être considérés comme un seul routeur "Virtuel". Les membres du groupe de ce routeur virtuel sont capables de s'échanger (Multicast) des messages d'état et des informations.

Un routeur physique peut donc être "responsable" du routage et un autre en redondance. Si le routeur, que nous appellerons primaire, a un problème, le routeur secondaire prendra sa place automatiquement. Les paquets continueront de transiter de façon transparente car les 2 routeurs partagent les mêmes adresses IP et MAC !

Le processus d'élection se déroule pendant la mise en place des liens, une fois ce processus terminé, seul le routeur primaire (Active) va envoyer des messages HSRP multicast en UDP aux autres afin de minimiser le trafic réseau. Si ces messages ne sont plus reçus par le routeur secondaire (Standby), c'est que le routeur primaire à un problème et le secondaire devient donc Actif.

L'élection se fait un peu à la manière de spanning-tree, en prenant en compte une priorité. Cette priorité est composée d'un paramètre "priority" compris entre 1 et 255 (255 étant le plus prioritaire) et de l'adresse IP de l'interface.

A priorités statiques égales, la plus haute adresse IP sera élue. Plusieurs groupes HSRP peuvent exister au sein d'un même routeur sans que cela ne pose problème (depuis l'IOS 10.3). Seuls les routeurs du même numéro de groupe s'échangeront les messages HSRP.

Ensute nous configurons notre interface FastEthernet 0/0 :

```
R1(config)#interface fastethernet 0/0
R1(config-if)#ip address 30.0.0.251 255.0.0.0
R1(config-if)#no shutdown
```

Puis nous activons le HSRP sur nos interfaces : (ROUTEUR 1)

```
R1(config)#interface fastethernet 0/0
R1(config-if)#standby 1 ip 30.0.0.254
R1(config-if)#standby 1 priority 130
R1(config-if)#standby 1 preempt
R1(config-if)#standby 1 track FastEthernet 0/1 30
```

Quelques petites explications :

- ▶ standby 1 ==> Déclare le groupe HSRP.
- ▶ standby 1 ip 30.0.0.254 ==> Déclare l'adresse IP du routeur virtuel.
- ▶ standby 1 priority 130 ==> Déclare la priority du routeur.
- ▶ standby 1 preempt ==> Permet d'augmenter la rapidité d'élection.
- ▶ standby 1 track FastEthernet 0/1 30 ==> Surveille la deuxième interface du routeur, si l'interface tombe le HSRP fera en sorte qu'un autre routeur prenne sa place.

Puis nous activons le HSRP sur nos interfaces : (ROUTEUR 2)

```
R2(config)#interface fastethernet 0/0
R2(config-if)#standby 1 ip 30.0.0.254
R2(config-if)#standby 1 priority 120
R2(config-if)#standby 1 preempt
R2(config-if)#standby 1 track FastEthernet 0/1 20
```

Puis nous activons le HSRP sur nos interfaces : (ROUTEUR 3)

```
R3(config)#interface fastethernet 0/0
R3(config-if)#standby 1 ip 30.0.0.254
R3(config-if)#standby 1 priority 110
R3(config-if)#standby 1 preempt
R3(config-if)#standby 1 track FastEthernet 0/1 20
```

Avant d'étudier les pannes, nous observons le statut du HSRP sur nos routeurs.

show standby

R2 est en **Standby** prêt à prendre le routage si R1 a un problème.

R3 est en mode "**Listen**", il écoute le réseau en attendant que R1 et R2 tombe.

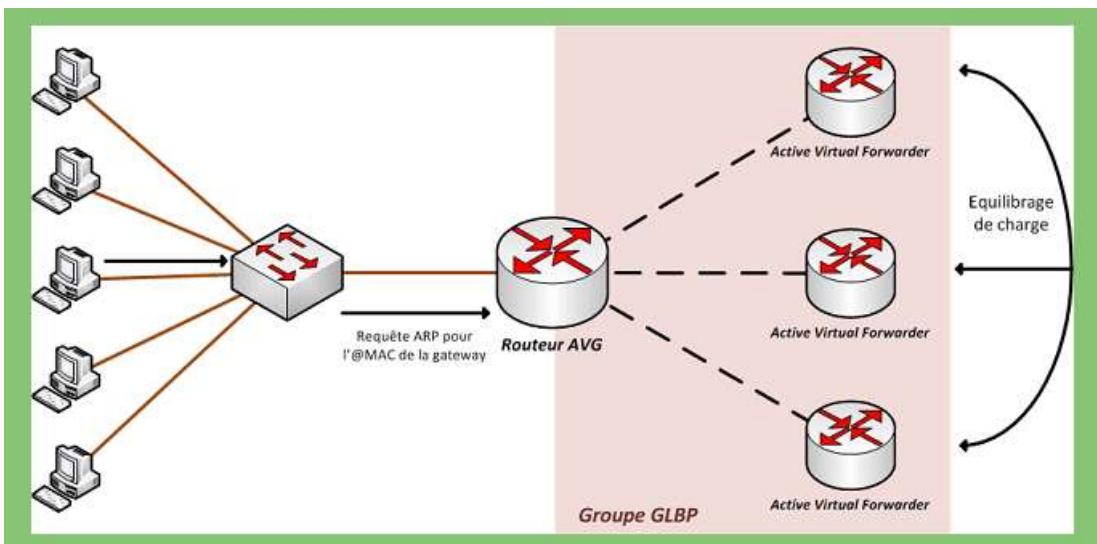
GLBP

Gateway Load Balancing Protocol est un protocole propriétaire Cisco qui permet de faire de la redondance ainsi que de la répartition de charge sur plusieurs routeurs en utilisant une adresse IP virtuelle, qui sera associée à plusieurs adresses MAC virtuelles.

Ainsi, tous les routeurs du groupe GLBP défini participent activement alors que dans VRRP ou HSRP, il n'y a qu'un qui est en mode actif tandis que les autres patientent.

Le protocole GLBP élit un Active Virtual Gateway (AVG) qui va répondre aux requêtes ARP pour l'adresse IP virtuelle. GLBP permet de donner un poids variable à chacun des routeurs participants pour la répartition de la charge entre ces routeurs. La charge est donc répartie par hôte dans le sous-réseau.

GLBP est un protocole propriétaire Cisco qui reprend les concepts de base de HSRP et VRRP. Contrairement à ces 2 protocoles, tous les routeurs du groupe GLBP participent activement au routage alors que dans VRRP ou HSRP, il n'y en a qu'un qui est en mode actif, tandis que les autres patientent. Plus concrètement, à l'intérieur du groupe GLBP, le routeur ayant la plus haute priorité ou la plus haute adresse IP du groupe prendra le statut de « AVG » (active virtual gateway). Ce routeur va intercepter toutes les requêtes ARP effectuées par les clients pour avoir l'adresse MAC de la passerelle par défaut, et grâce à l'algorithme d'équilibrage de charge préalablement configuré, il va renvoyer l'adresse MAC virtuelle d'un des routeurs du groupe GLBP. C'est d'ailleurs le Routeur AVG qui va assigner les adresses MAC virtuelles aux routeurs du groupe, Ainsi ils ont le statut « AVF » (Active Virtual Forwarder). Un maximum de 4 adresses MAC virtuelle est défini par groupe, les autres routeurs ayant des rôles de backup en cas de défaillance des AVF.



Les timers de GLBP sont :

- ▶ Hello : 3s
- ▶ Dead : 10s est le temps à partir duquel un AVF sera Dead, son adresse mac sera associée à un autre AVF
- ▶ Redirect (Temps à partir duquel on arrêtera de rediriger l'adresse mac d'une AVF Dead vers une autre AVF) : 600s
- ▶ Timeout (Temps à partir duquel un routeur est considéré comme inactif, son adresse MAC ne sera plus utilisée) : 14400s (4 heures), doit être supérieur au temps de conservation entrées ARP des clients.

On pourra vérifier la configuration GLBP de nos routeurs via la commande suivante :

```
1 show glbp brief
```

Voici les commandes qui vont permettre de configurer le GLBP :

```
R1(config-if)#glbp 1 ip 192.168.0.254
R1(config-if)#glbp 1 priority 255
R1(config-if)#glbp 1 preempt
R1(config-if)#glbp 1 name glbp-lan
```

Quelques

explications :

- ▶ **glbp 1** : Correspond au groupe 1.
- ▶ **glbp 1 ip** : Permet d'attribuer une adresse IP à l'interface GLBP.
- ▶ **glbp 1 priority** : Permet d'attribuer une priorité au routeur, qui va servir à élire un routeur AVG. Nous voulons que R1 soit AVG donc nous mettons la plus haute valeur (255).
- ▶ **glbp 1 preempt** : Si un routeur entre dans le groupe GLBP avec une valeur de priorité plus forte que les autres, il doit quand même attendre la prochaine élection (qui aura lieu lorsque le routeur AVG actuel sera hors service). La commande "preempt" permet d'éviter ce problème. Pour affiner le réglage nous pouvons régler le délai avant que le routeur ne reprenne le contrôle du groupe (délai par défaut = 30s) via la commande "glbp 1 preemp delay XXX" où XXX est un nombre de seconde.
- ▶ **glbp 1 name glbp-lan** : Permet simplement de donner un nom au groupe.

Un **domaine de collision** désigne une partie du réseau dans laquelle toutes les trames sont vues par tous les équipements. Il comprend les bus et les « hubs » ou concentrateurs et est limité par les « switchs » ou commutateurs et les routeurs.

Un **domaine de diffusion** désigne la partie du réseau dans laquelle les trames de « broadcast » sont vues par tous les équipements. Il est constitué des bus, des « hubs » et des « switchs », il est limité par les routeurs. Les domaines de collisions appartiennent au même domaine de diffusion.

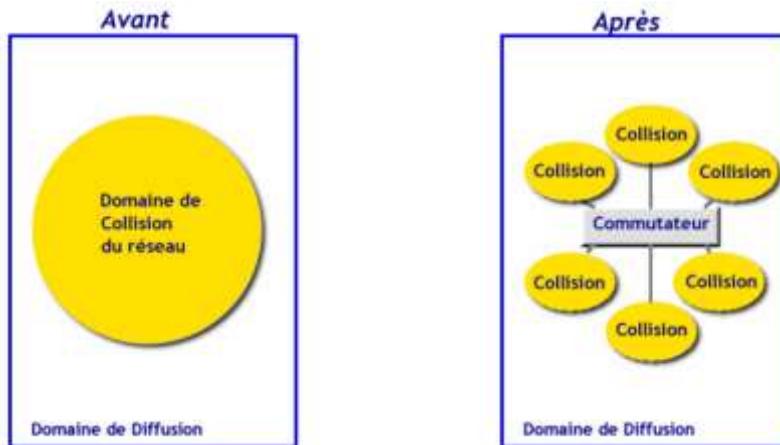
Segmentation

Les facultés des commutateurs et des routeurs à segmenter les réseaux sont une source de confusion. Comme chacun des 2 dispositifs opère à un niveau différent du modèle OSI, chacun réalise un type de segmentation différent.

5.1. Un commutateur segmente des domaines de collision

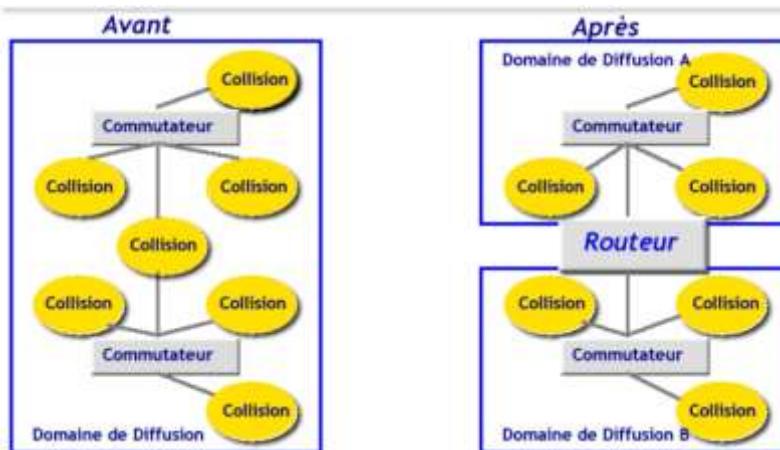
La segmentation au niveau 2 réduit le nombre de stations en compétition sur le même réseau local. Chaque domaine de collision possède la bande passante délivrée par le port du commutateur.

Les domaines de collisions appartiennent au même domaine de diffusion.



5.2. Un routeur segmente des domaines de diffusion

La segmentation au niveau 3 réduit le trafic de diffusion en divisant le réseau en sous-réseaux indépendants.



5.3. Synthèse

C'est grâce aux progrès de l'électronique qui ont permis d'augmenter les densités d'intégration et les fréquences, que les commutateurs ont pu se développer.

Dans le même temps, les fonctions réalisées par les routeurs n'ont cessé d'augmenter en quantité et en qualité. Il ne faut pas oublier que toute la sécurité d'un système d'information se «joue» sur les équipements d'interconnexion. Une règle de sécurité sur une équipement réseau est évaluée à chaque nouveau paquet tandis qu'une règle de sécurité applicative n'est évaluée qu'à l'authentification.

Il était donc inévitable que l'on aboutisse à des équipements «hybrides». Aujourd'hui, les routeurs les plus performants associent une électronique rapide (celle du commutateur) au niveau 2 et un logiciel complet (les fonctions du routeur) au niveau 3.

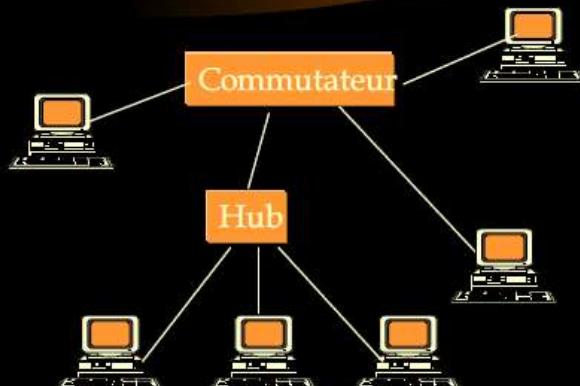
Pour parvenir à ce résultat, on trouve 2 approches :

- **Les équipements haut de gamme.** Les ténors du marché de l'interconnexion réseau proposent des appareils avec une électronique de commutation et de chiffrement spécifique. Les fonctions de routage sont assurées par des systèmes d'exploitation propriétaires. C'est la solution la plus complète et la plus efficace mais elle a un coût très élevé.
- **Les réseaux virtuels ou VLANs.** La norme IEEE 802.1Q permet une segmentation dynamique des sous-réseaux. C'est une solution attrayante du point de vue gestion de parc mais incomplète du point de vue contrôle d'accès. Il est possible d'exploiter les informations des trames IEEE 802.1Q en les associant à un adressage réseau de niveau 3. On parle alors de *routage inter-vlan*.

¶

La commutation

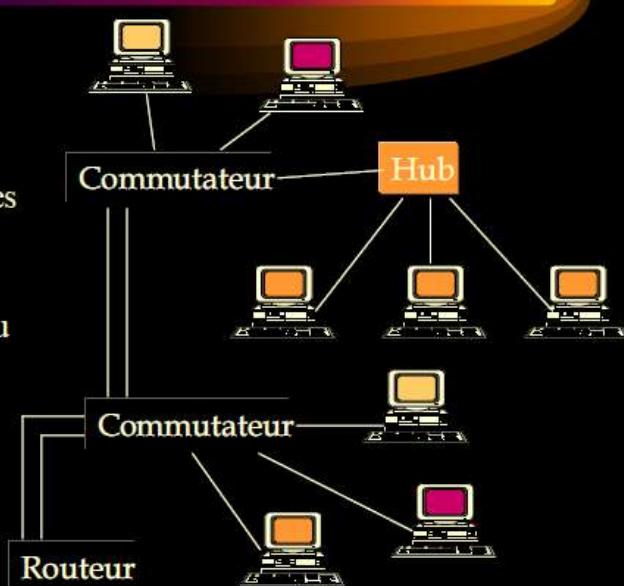
- Meilleur accès au média
 - bande passante dédiée,
 - moins de conflits d'accès
 - collisions réduites
- Le trafic est dirigé vers la station spécifiée
- Les "broadcast" sont diffusés plus vite
- L'évolutivité reste un problème



¶

Le réseau local commuté

- Domaines de collisions réduits
- Intelligence dans le port du commutateur
- Les frontières physiques disparaissent
- Regroupement logique des utilisateurs
- Meilleur contrôle de la bande passante et des changements dans le réseau
- Centralisation de l'administration
- Routeur pour la communication inter-réseau



Les avantages offerts par les VLAN

- flexibilité de la segmentation du réseau (dynamique) : les utilisateurs et les ressources entre lesquels les communications sont fréquentes peuvent être regroupés sans contrainte due leur localisation.
- simplification de la gestion du réseau : l'ajout de nouveaux éléments ou le déplacement d'éléments existants peut être réalisé rapidement sans devoir manipuler les connexions physiques dans une local technique.
- augmentation des performances du réseau : traffic réseau segmenté, limitation des broadcast
- meilleure utilisation des serveurs réseaux : le serveur peut appartenir à plusieurs VLAN en même temps. ce qui permet de réduire le trafic qui doit être routé (traité IP)
- renforcement de la sécurité du réseau : les frontières (virtuelles) entre les VLAN ne peuvent être franchies que par le biais d'un routage.

VLAN: un réseau local (LAN) est défini par un domaine de diffusion. Tous les hôtes d'un réseau local reçoivent les messages de diffusion émis par n'importe quel autre hôte de ce réseau. Par définition, un réseau local est délimité par des équipements fonctionnant au niveau 3 du modèle OSI : la couche réseau.

Un réseau local virtuel (VLAN) est un réseau local (LAN) distribué sur des équipements fonctionnant au niveau 2 du modèle OSI : la couche liaison. Dès que l'on a besoin de communiquer entre domaines de diffusion, il est absolument nécessaire de passer par les fonctions de routage du niveau réseau du modèle OSI.

Le réseau local est distribué sur différents équipements via des liaisons dédiées appelées *trunks*. Un *trunk* est une connexion physique unique sur laquelle on transmet le trafic de plusieurs réseaux virtuels. Les trames qui traversent le *trunk* sont complétées avec un identificateur de réseau local virtuel (VLAN id). Grâce à cette identification, les trames sont conservées dans un même VLAN (ou domaine de diffusion).

Les *trunks* peuvent être utilisés :

entre deux commutateurs

C'est le mode de distribution des réseaux locaux le plus courant.

entre un commutateur et un hôte

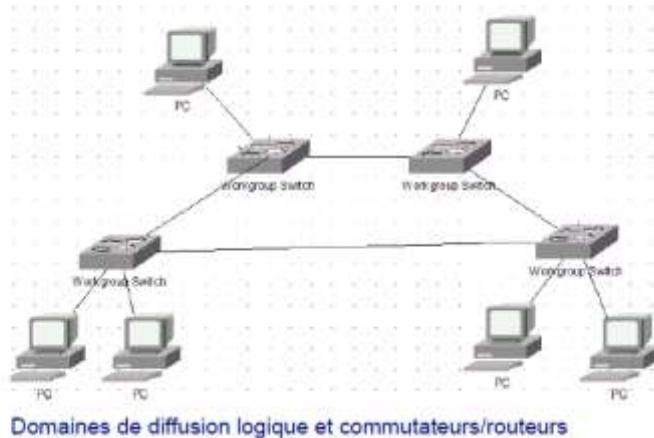
C'est le mode de fonctionnement à surveiller étroitement. Un hôte qui supporte le *trunking* a la possibilité d'analyser le trafic de tous les réseaux locaux virtuels.

entre un commutateur et un routeur

C'est le mode fonctionnement qui permet d'accéder aux fonctions de routage ; donc à l'interconnexion des réseaux virtuels par routage inter-VLAN. La mise en œuvre de ce type de routage est l'objet de ce document.

Enfin, il ne faut pas oublier que tous les VLANs véhiculés dans le même *trunk* partagent la bande passante du média utilisé. Si un *trunk* utilise un lien 100Mbps Full-Duplex, la bande passante de tous les VLANs associés est limitée à ces 100Mbps Full-Duplex.

Un VLAN permet de créer des domaines de diffusion (domaines de *broadcast*) gérés par les commutateurs indépendamment de l'emplacement où se situent les nœuds, ce sont des domaines de diffusion gérés logiquement.



Domaines de diffusion logique et commutateurs/routeurs

- Trois nécessités pour introduire le concept
 - Limiter les domaines de broadcast
 - Garantir la sécurité
 - Permettre la mobilité des utilisateurs

Objectifs des VLAN

- Avoir des fonctions de la couche 3 avec la vitesse de la couche 2
- Faciliter la gestion de la mobilité des postes
- Supprimer la possibilité de communication entre certaines parties du réseau, sécurisé des domaines
- Pouvoir facilement attribuer des autorisations différentes, en fonction des droits et rôles de chaque groupe de personnes

VLANs par ports

Cette technique fournit une méthode de division d'un équipement de niveau 2 (un commutateur) en plusieurs domaines de diffusion. La réalisation de cette division est spécifique à chaque plateforme.

Le coût d'administration de ce genre de réseaux locaux est très important puisqu'il faut gérer manuellement sur chaque équipement la distribution des réseaux locaux.

Ceci dit, cette technique ne dépend pas d'une gestion propriétaire de l'affectation des ports dans les différents VLANs. C'est la raison principale pour laquelle elle est très répandue. Le commutateur assure une isolation complète entre la station et le VLAN auquel elle appartient.

VLANs du type Cisco Inter-Switch Link, ISL VLANs

Cette technique a été développée spécifiquement pour les équipements Cisco™. Elle complète les en-têtes de trames avec 30 octets répartis en 13 champs. Ce type d'encapsulation n'est plus beaucoup utilisé du fait de son incompatibilité avec le standard IEEE 802.1Q.

VLANs IEEE 802.1Q

Le standard IEEE 802.1Q fournit un mécanisme d'encapsulation très répandu et implanté dans de nombreux équipements de marques différentes. C'est sur ce standard que s'appuie ce document. Comme dans le cas de l'encapsulation ISL précédente, l'en-tête de trame est complété par une balise de 4 octets.

Les Vlan par port (Vlan de niveau 1)

On affecte chaque port des commutateurs à un VLAN.

L'appartenance d'une trame à un VLAN est alors déterminée par la connexion de la carte réseau à un port du commutateur.

Les ports sont donc affectés statiquement à un VLAN.

Si on déplace physiquement une station il faut désaffecter son port du Vlan puis affecter le nouveau port de connexion de la station au bon Vlan. Si on déplace logiquement une station (on veut la changer de Vlan) il faut modifier l'affectation du port au Vlan.

Les Vlan par adresse MAC (Vlan de niveau 2)

On affecte chaque adresse MAC à un VLAN.

L'appartenance d'une trame à un VLAN est déterminée par son adresse MAC. En fait il s'agit, à partir de l'association Mac/VLAN, d'affecter dynamiquement les ports des commutateurs à chacun des VLAN en fonction de l'adresse MAC de l'hôte qui émet sur ce port.

L'intérêt principal de ce type de VLAN est l'indépendance vis-à-vis de la localisation géographique. Si une station est déplacée sur le réseau physique, son adresse physique ne changeant pas, elle continue d'appartenir au même VLAN (ce fonctionnement est bien adapté à l'utilisation de machines portables).

Si on veut changer de Vlan il faut modifier l'association Mac / Vlan.

Les Vlan par adresse de Niveau 3 (VLAN de niveau 3)

On affecte une adresse de niveau 3 à un VLAN.

L'appartenance d'une trame à un VLAN est alors déterminée par l'adresse de niveau 3 ou supérieur qu'elle contient (le commutateur doit donc accéder à ces informations).

En fait, il s'agit à partir de l'association adresse niveau 3/VLAN d'affecter dynamiquement les ports des commutateurs à chacun des VLAN.

Dans ce type de VLAN, les commutateurs apprennent automatiquement la configuration des VLAN en accédant aux informations de couche 3. Ceci est un fonctionnement moins rapide que le Vlan de niveau 2.

Quand on utilise le protocole IP on parle souvent de Vlan par sous-réseau.

Installation des VLANs sur les switchs

Pour tous les switchs

```
enable
Conf t
vlan 20
Name direction
vlan 30
Name commercial
vlan 40
Name serveurs
```

Attribution des ports pour les VLANs entre switchs :

```
Sur switch4 :
Enable
Conf t
Interface FastEthernet0/2
Switchport mode trunk
Exit
Interface FastEthernet0/3
Switchport mode trunk
Exit
Interface FastEthernet0/4
Switchport mode trunk
Exit
Interface FastEthernet0/5
Switchport mode trunk
exit
Interface FastEthernet0/1
Switchport mode trunk
```

Attribution des ports entre switchs et appareils finaux :

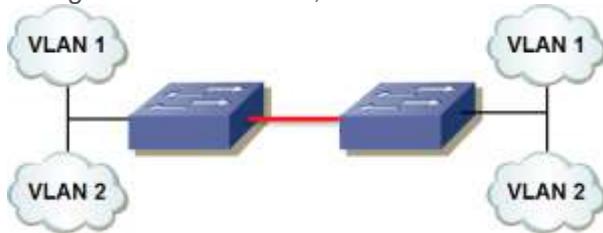
```
Sur tous les switchs finaux:
Interface Fa0/2
Switchport access vlan 20

Interface Fa0/3
Switchport access vlan 30
```

Configuration des sous-interfaces du routeur :

```
Conf t
Interface FastEthernet0/0.1
Encapsulation dot1Q 20
Ip address 10.0.0.1 255.255.255.0
Exit
Interface FastEthernet0/0.2
Encapsulation dot1Q 30
Ip address 10.0.1.1 255.255.255.0
Exit
Interface FastEthernet0/0.3
Encapsulation dot1Q 40
Ip address 10.0.2.1 255.255.255.0
```

Prenons par exemple l'exemple où deux switch sont reliés l'un à l'autre, chacun ayant été configuré avec 2 VLANs, le VLAN 1 et le VLAN 2...



Le but ici est que le trafic du VLAN1 de gauche puisse circuler sur le VLAN1 de droite et idem pour le VLAN2. Afin que cela soit possible, il faut configurer la liaison entre les deux switch en « trunk »... ou plus précisément configurer une encapsulation des trames lorsqu'elles transitent sur le lien de sorte que le switch qui la reçoit peut ensuite la relayer dans le bon VLAN.

Quand on parle d'encapsulation, on doit forcément faire appel à un protocole. Du côté de Cisco, deux protocoles existent pour l'encapsulation des données sur un trunk:

1. ISL (Inter Switch Link) qui est un protocole propriétaire Cisco qui tend à disparaître.
2. dot1Q (IEEE 802.1Q) le protocole standard défini par l'IEEE.

Nous nous contenterons de voir dot1q dans le cas présent. Toutefois il est bon de savoir que chacun a son propre fonctionnement. ISL pour sa part encapsule toute les trames, quelque soit le VLAN. dot1Q, lui ne fait qu'insérer un tag (un marqueur) dans l'en-tête de la trame ethernet ... et uniquement sur les VLANs autres que le VLAN natif. (Le VLAN natif est celui utilisé par les protocoles comme CDP par exemple pour s'échanger les informations).

Quels sont les techniques de diffusion de configuration ?

On utilise VTP en manuel.

Si tu utilises mrp tu utiliseras mvrp.

Quels sont les différences entre le VTP et MRP ?

VTP en manuel pour diffuser et MRP en dynamique pour configurer.

Typologie VLAN

Routage : Legacy inter-VLAN

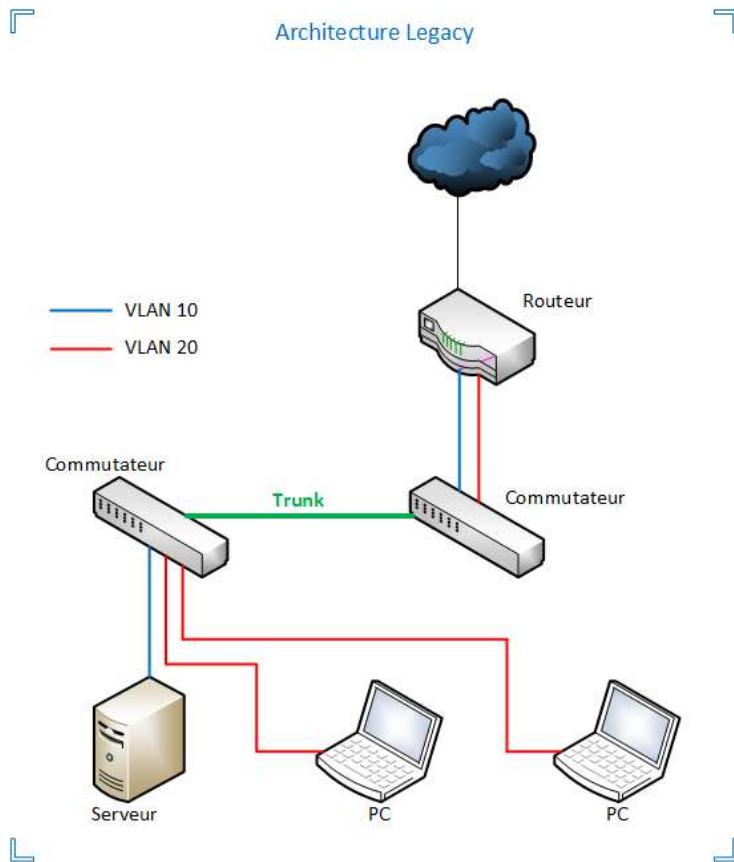
Dans l'approche Legacy, le routage inter-VLAN est effectué en connectant différentes interfaces physiques du routeur sur différentes interfaces physiques du commutateur. Les ports du

commutateur connectés au routeur ne sont pas en mode trunk mais en mode accès (*access*), chaque interface physique est assignée à un VLAN différent.

Cette méthode requiert autant d'interfaces physiques que vous avez de VLANs, ce qui peut vite devenir gênant. Cette méthode est certainement très peu utilisé et n'est plus implémentée.

Si plusieurs commutateurs sont présents dans votre architecture, ils doivent être reliés entre eux par un lien trunk, contrairement au cas de la liaison routeur – commutateur.

Voici un exemple d'architecture :



Vous remarquerez qu'il y a deux VLANs, le VLAN 10 et le VLAN 20 chacun dispose de son propre lien dédié entre le routeur et le commutateur. Entre les deux commutateurs on trouve un lien trunk pour tagguer les trames Ethernet.

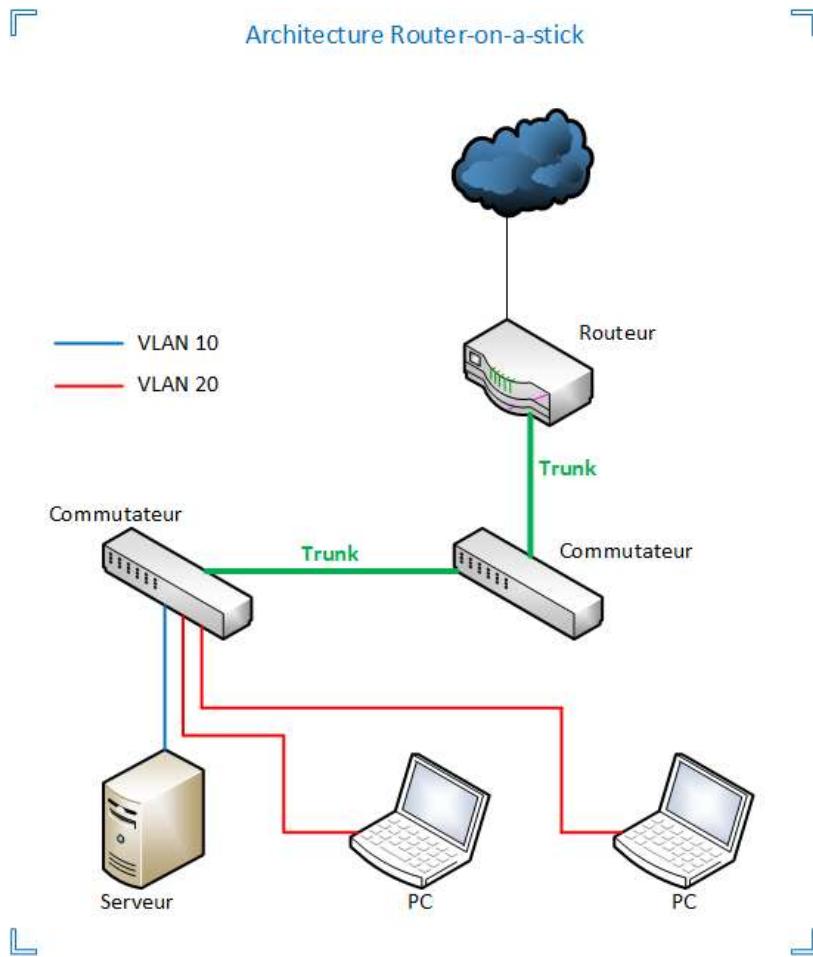
III. Routage : Router-on-a-stick

L'architecture Router-on-a-stick est une évolution de l'architecture Legacy, notamment au niveau du lien commutateur – routeur puisqu'au lieu d'avoir un lien par VLAN, un seul lien suffira. Le lien entre le routeur et le commutateur est désormais un lien trunk.

De plus, sur l'interface du routeur connectée au commutateur, il faudra créer une sous-interface virtuelle pour chaque VLAN en activant l'encapsulation 802.1Q pour le VLAN pour que le tagguage des trames Ethernet opère correctement.

Chaque sous-interface sera la passerelle des postes du VLAN, il faudra donc penser à attribuer une adresse IP à ces interfaces virtuelles et à les rendre active (*no shutdown*).

Ce type d'architecture est toujours utilisé de nos jours, voici un schéma représentatif :



Les liens trunk agissent comme des tuyaux capables de transporter le flux de données de chacun des VLANs autorisés.

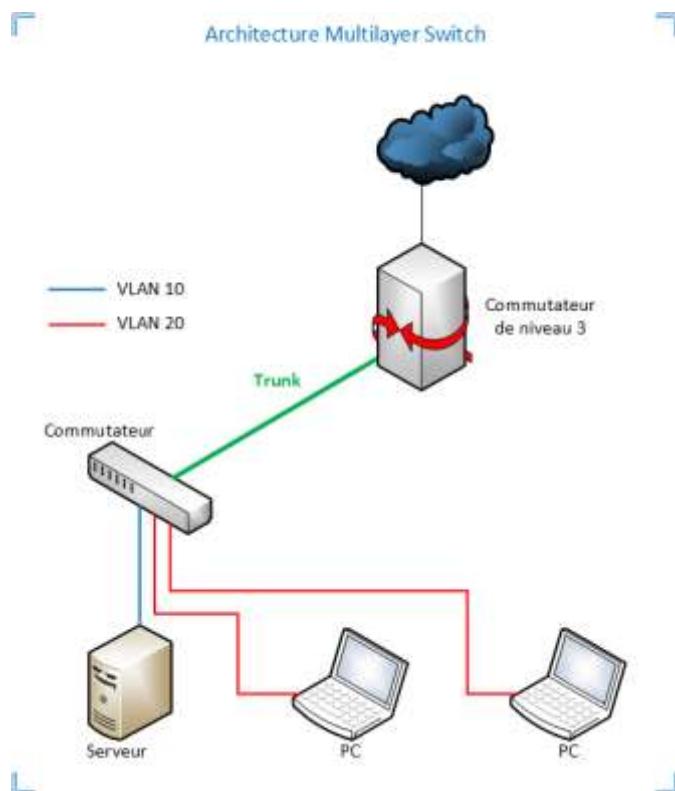
IV. Routage : Multilayer Switch

La mise en place de routage inter-VLAN avec une architecture Multilayer Switch que l'on peut traduire par "Commutateur multicouches" correspond à une architecture qui n'utilise pas de routeur pour effectuer le routage. La fonctionnalité de routage est assurée par un commutateur de niveau 3 et donc avec des fonctions de niveau 3 comme le routage, ces *multilayer switch* sont capables d'assurer les fonctions de niveau 2 et de niveau 3.

Le commutateur qui effectue le routage doit avoir l'ip routing d'activé pour que cela fonctionne. Il effectuera le routage directement en interne.

Ce type d'architecture est plus évolutif que n'importe que les deux autres architectures présentées dans cet article. Tout simplement car les routeurs ont un nombre limité d'interfaces alors que les commutateurs en ont beaucoup plus.

Néanmoins, ce type de commutateur ne remplace pas toutes les fonctionnalités d'un routeur, notamment au niveau de la sécurité.



Propriétés

C'est un protocole propriétaire Cisco de niveau 2. De part sa simplicité et sa puissance, l'IEEE a sorti un protocole similaire afin de permettre cette fonctionnalité entre switchs de constructeurs différents: GVRP (GARP VLAN Registration Protocol). La norme est IEEE [802.1ak](#).

Fonctionnement

Les messages VTP diffusent des annonces de création, de suppression ou de modification de VLAN. Cette diffusion s'effectue à travers tous les switchs grâce à une trame niveau 2 avec une adresse de destination MAC multicast bien particulière qui est 01-00-0C-CC-CC-CC.

Architecture du VTP

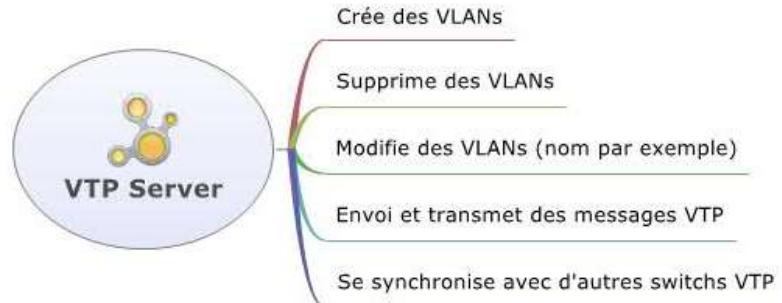
Le switch possède 3 modes VTP: client, transparent ou server (actif par défaut):

- VTP Server: switch qui crée les annonces VTP
- VTP Client: switch qui reçoit, se synchronise et propage les annonces VTP
- VTP Transparent: switch qui ne traite pas les annonces VTP

Switch en mode VTP Server

Le switch en mode Server permet à l'administrateur de faire toute modification sur les VLANs et de propager automatiquement ses modifications vers tous les switchs du réseau.

Mind à télécharger:



Switch en mode VTP Client

Le switch en mode Client **ne permet pas** à l'administrateur de faire des modifications sur les VLANs. Vous recevez un message d'erreur quand vous essayez de créer un VLAN.

Mind à télécharger:

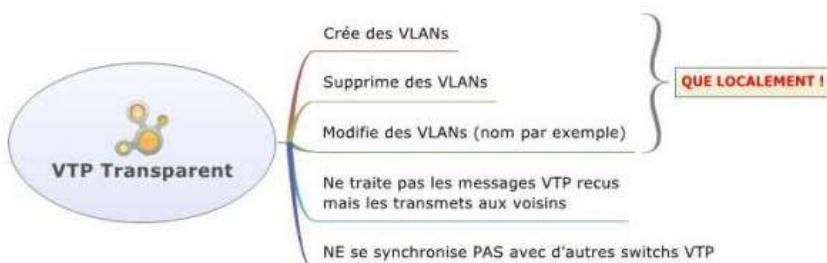


- VTP server et client : lien Trunk.

Switch en mode VTP Transparent

Le switch en mode Transparent permet à l'administrateur de faire toute modification sur les VLANs en **local uniquement** et donc **ne propage pas** ses modifications vers tous les switchs du réseau. Très pratique pour des maquettes!

Mind à télécharger:

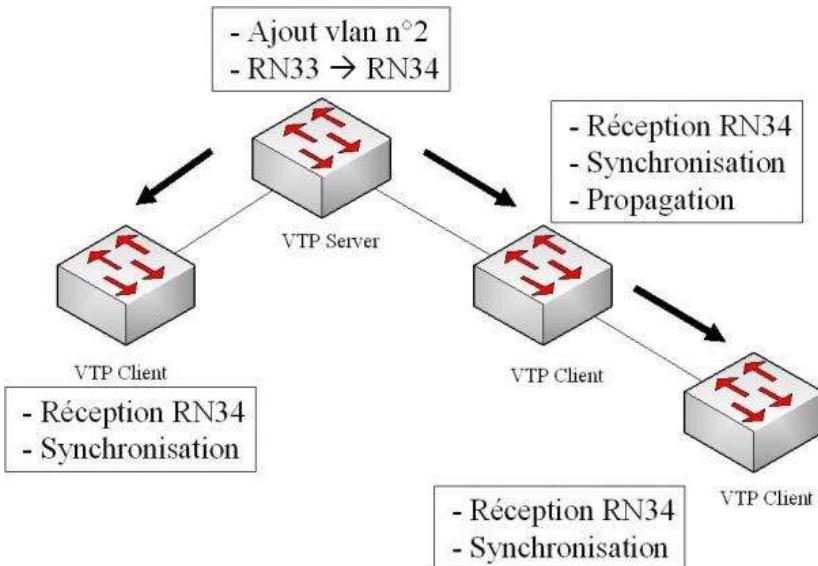


Synchronisation

A chaque création/suppression/modification de VLAN, une variable appelée RN – Revision Number – s'incrémente (initialement 0 puis 1 puis 2 puis 3...). A chaque création/suppression/modification de

VLAN, le switch Server envoi un message VTP avec la nouvelle valeur du RN. Les autres switchs compare le RN reçu du switch Server avec le RN qu'ils stocke en local, si ce dernier est plus petit (logiquement) alors les switchs se synchronisent avec le Server et récupère la nouvelle base de données des VLANs.

Par défaut, le RN est envoyé automatiquement dès une création/suppression/modification de VLAN puis envoyé toutes les 5 minutes.



Remarques importantes

- Les messages VTP se propagent sur les liens configurés en Trunk (norme [802.1Q](#)) et pas en Access
- VTP ne gère que la plage de VLAN comprise entre 1 et 1005. La plage étendue 1006 à 4096 n'est pas supportée. Pour cela, il faut basculer en mode Transparent sur tous les switchs et créer ses VLANs étendus à la main
- Il existe 3 versions de VTP, bien vérifier qu'une et une seule version est active sur son réseau pour éviter les surprises (v1 et v2 incompatibles entre elles)
- La configuration VTP n'est pas visualisable dans la running-config mais est stockée dans le fichier `vlan.dat` situé dans la flash (faites un `show flash:` pour voir le fichier)

Pour configurer le VTP, voici les étapes:

1. obligatoire: configurer un domaine VTP qui permet à tous les switchs d'être dans le même « groupe d'amis »
2. obligatoire: configurer le mode de votre switch (client, transparent ou server)
3. optionnel: activer la fonction pruning
4. optionnel: configurer un mot de passe pour sécuriser les messages VTP
5. optionnel: activer la version 2 ou 3 de VTP (version 1 active par défaut)

Mind à télécharger:



Avantages de VTP

- Le VTP permet d'avoir une configuration de VLAN cohérente en gérant :
 - Addition
 - Effacement
 - Renommer
- Les avantages du VTP :

VTP Benefits

- VLAN configuration consistency across the network
- Accurate tracking and monitoring of VLANs
- Dynamic reporting of added VLANs across a network
- Dynamic trunk configuration when VLANs are added to the network

Inconvénients de VTP

Un grand domaine STP et les potentiels risques et instabilités de STP. Le plus grand risque est une boucle STP à travers le réseau entier.

Considérer le risque d'insérer un switch ayant un numéro de révision supérieur.

VTP est propriétaire Cisco ce qui limite son utilisation!

	Serveur VTP	Client VTP	VTP transparent
Description	Gère les configurations de domaine et de VLAN	Met à jour la configuration VTP. Les commutateurs client VTP ne peuvent pas changer la configuration des VLANs.	Capable de gérer les configurations de VLANs locaux. Les configurations de VLANs ne sont pas partagées avec le VTP.
Répond aux annonces VTP?	Participe totalement	Participe totalement	Achemine uniquement les annonces VTP
Configuration globale des VLANs récupérée au démarrage?	Oui car la configuration des VLANs est stockée en NVRAM flash.	Non car la configuration des VLANs est stockée en RAM.	Non car seule la configuration des VLANs locaux est stockée en NVRAM flash.
Met à jour d'autres commutateurs opérant avec VTP.	Oui	Oui	Non

CDP : Le **Cisco Discovery Protocol (CDP)** est un protocole de découverte de réseau de niveau 2 développé par [Cisco Systems](#) qui permet, avec [SNMP](#), de trouver d'autres périphériques voisins directement connectés ([routeur](#), [switch](#), [pont](#), etc.). Il s'utilise avec des commandes [IOS](#). CDP est indépendant des médias qu'il parcourt. Par défaut, les annonces CDP sont envoyées toutes les 60 secondes sur les interfaces qui prennent en charge [SNAP](#), ce qui comprend les médias physiques comme les [LAN](#) Ethernet, [Frame Relay](#) et l'[Asynchronous transfer mode](#) (ATM). Les informations sont envoyées par une adresse [multicast](#). La version la plus récente est la CDPv2.

Le protocole CDP (Cisco Discovery Protocol) est un protocole propriétaire de la couche OSI 2 développé par Cisco Systems.

Il tourne sur les équipements Cisco et certains équipements HP.

Il est utile pour deux raisons:

- Obtenir des informations sur les équipements CDP directement connectés comme le système d'exploitation et l'adresse IP.
- Vérifier que la connectivité OSI de couche trois est fonctionnelle en cas de problèmes au niveau de la couche IP (couche OSI 3).

Les annonces CDP sont envoyées vers l'adresse multicast 01-00-0c-cc-cc-cc.

MRP: Multiple Registration Protocol (MRP), autrefois connu sous les noms **Generic Attribute Registration Protocol (GARP)** et **GARP VLAN Registration Protocol (GVRP)** est un protocole standard de [niveau 2](#) pour la configuration automatique des [VLAN](#) dans un [réseau communiqué](#). Il est défini par la norme IEEE 802.1ak¹.

La norme IEEE 802.1D mentionne l'idée d'enregistrement dynamique de l'appartenance aux groupes entre [ponts](#).

Les [commutateurs réseaux](#) peuvent utiliser GVRP pour dynamiquement gérer l'enregistrement des VLAN.

Dans un réseau de niveau 2, MRP fournit une méthode pour partager dynamiquement les informations sur les VLAN et configurer les VLAN au besoin. Par exemple, pour ajouter un port d'un [switch](#) à un VLAN, seul le port nécessaire doit être configuré. Tous les [trunks](#) sont créés dynamiquement sur les commutateurs où MRP est activé. Sans MRP (ou le protocole propriétaire équivalent chez [Cisco Systems](#), [VTP](#)), tout devrait être configuré manuellement.

MVRP : Les VLANs peuvent être déclarés manuellement ou dynamiquement. Dans la déclaration dynamique, l'administrateur définit les VLANs sur un switch et un seul. Le

protocole : Multiple VLAN Registration Protocol (MVRP) permet la diffusion de ces informations aux autres switchs du réseau.

La norme IEEE 802.1D mentionne l'idée d'enregistrement dynamique de l'appartenance aux groupes entre ponts.

Les commutateurs réseaux peuvent utiliser GVRP pour dynamiquement gérer l'enregistrement des VLAN.

Dans un réseau de niveau 2, MRP fournit une méthode pour partager dynamiquement les informations sur les VLAN et configurer les VLAN au besoin. Par exemple, pour ajouter un port d'un switch à un VLAN, seul le port nécessaire doit être configuré. Tous les trunks sont créés dynamiquement sur les commutateurs où MRP est activé. Sans MRP (ou le protocole propriétaire équivalent chez Cisco Systems, VTP), tout devrait être configuré manuellement.

Résumé des caractéristiques de PVST+, RSTP et rapid PVST+ variantes de STP

Cisco et variantes du STP

Cisco et variantes du STP	
Propriétaire Cisco	PVST <ul style="list-style-type: none">Utilise le protocole ISL propriétaire Cisco.Chaque VLAN a une instance de spanning-tree.Capacité d'équilibrage de charge de couche 2Inclut les extensions BackboneFast, UplinkFast et PortFast.
	PVST+ <ul style="list-style-type: none">Supporte ISL et IEEE 802.1QSupporte les extensions propriétaires CiscoAjout des améliorations BPDU Guard et Root Guard
	rapid-PVST+ <ul style="list-style-type: none">Basé sur le standard IEEE 802.1wConvergence plus rapide que IEEE 802.1D
Standard IEEE	RSTP <ul style="list-style-type: none">Introduit en 1982 fournit une convergence plus rapide que 802.1DImplémente les versions génériques des extensions propriétaires Cisco.L'IEEE a incorporé RSTP dans 802.1D en identifiant la spécification comme IEEE 802.1D-2004 MSTP <ul style="list-style-type: none">Plusieurs VLANs peuvent être incorporés dans la même instance spanning-treeInspiré du MISTP (Multiple Instances Spanning Tree Protocol) de Cisco,l'IEEE 802.1Q-2003 inclut maintenant MSTP.

spanning-tree vlan 1-100 priority 24576

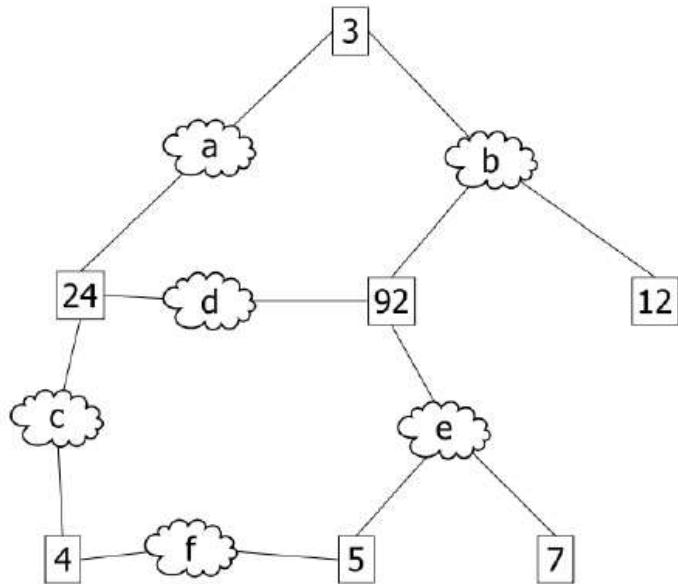
spanning-tree vlan 1-100 root primary

spanning-tree vlan 10 root secondary

spanning-tree vlan 40 root secondary

Le Spanning Tree Protocol (aussi appelé STP) est un protocole réseau permettant une topologie réseau sans boucle dans les LAN avec pont. Il est défini dans la norme IEEE 802.1D.

Le principe est simple, voici un exemple de topologie :



Il est plus qu'évident que nous avons ici un nombre important de boucles.

Les trames BPDU (Bridge Protocol Data Unit) :

Cette trame spécifique est émise par tout switch implémentant le protocole Spanning Tree, elle sert à calculer « l'arbre », à notifier les changements de topologie et à acquitter ces changements.

Par défaut, elles sont émises toutes les 2 secondes.

Sélection du « Root Bridge » (« Pont Racine » en français) :

Dans tout réseau intégrant le Spanning Tree, un « Root Bridge » est désigné (qui constitue la racine de l'arbre) de la manière suivante :

Le switch désigné comme « Root Bridge » est celui ayant le « bridge ID » le plus faible. Cette valeur est composée d'une priorité et de l'adresse MAC du switch.

Si la priorité est laissée par défaut, tout sera automatique. Il est cependant possible à l'administrateur de la modifier afin de privilégier un switch par rapport à un autre.

Bien entendu, si pour une raison ou une autre le « Root Bridge » venait à ne plus répondre, le processus de « Root Bridge » reprendrait immédiatement pour en élire un nouveau.

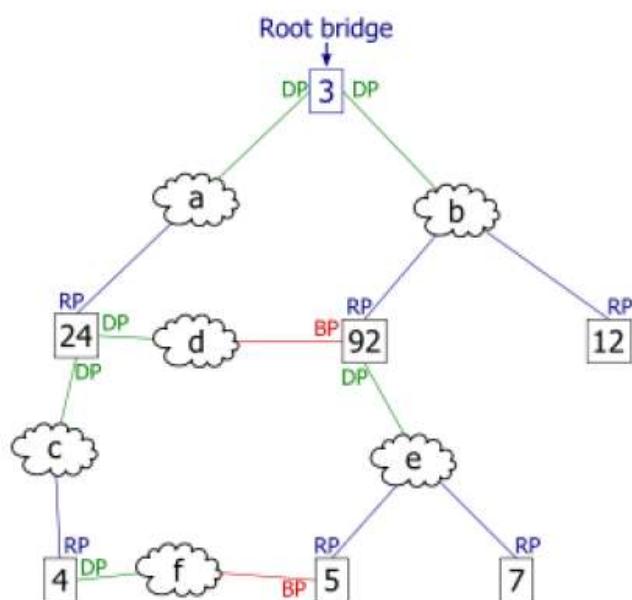
Sélection du « Root Port » :

Ce port est défini et désigné de la manière suivante :

Le « Root Port » est le port permettant d'atteindre le « Root Bridge » avec le coût le plus faible en termes de bande passante. S'il venait à y avoir une égalité, le port ayant l'ID le plus faible est élu (l'ID le plus faible est généralement le port 1 ... et en suivant).

Voici donc le réseau obtenu :

- **RP** : Root Port
- **DP** : Forwarding Port (oui, je sais ... vous ne voyez pas le rapport entre le « D » et Forwarding mais vous comprendrez mieux cela en 2^{ème} partie de sujet !!)
- **BP** : Blocked Port



- Construction **distribuée** de l'arbre par l'**ensemble des commutateurs**
- **Transparent** pour les machines
- **Sans pré-configuration** particulière des commutateurs
- **Convergence rapide** (de l'ordre de la dizaine de secondes)
- **Tolérance aux changements de topologie**
- **Trafic généré négligeable**

Règles de base de STP

- ① A la **convergence de l'algorithme**, la **racine est le commutateur de plus petit identifiant**
 - Partie « priorité » utile pour imposer l'élu
- ② Si un **commutateur reçoit une configuration lui proposant une meilleure racine** que celle qu'il considère, **il change d'avis**
- ③ Si **plusieurs ports permettent d'atteindre la racine**, seul **celui qui minimise le coût vers la racine est conservé actif = port racine**
 - **Blocage des ports redondants (plus de retransmission de trames)**
- ④ Si **plusieurs ports permettent d'atteindre le même segment**, seul **celui qui minimise le coût est conservé actif = port désigné**

Le “Spanning tree”

Arbre de recouvrement :

- . construction d'un arbre recouvrant tous les ponts
- . en déactivant certains ports de certains ponts, on élimine les cycles
- . il existe plusieurs arbres recouvrants pour une même topologie !
==> ‘l’arbre des plus courts chemins’

Algorithme de construction d'un arbre de recouvrement total :

- . algorithme d'élection basé sur les **adresses + coût + n° port.**
 - . la racine de l'arbre sera le pont de + petite adresse
 - . les liaisons actives seront celles de + faible coût à partir de cette racine.
 - . en cas d'égalité, on choisit
 - le chemin passant par le pont de plus petite adresse
 - le + petit n° de port (interface de communication).

Structure des messages de configuration [valeur lors de l'initialisation]:

- . Identité de la racine (proposée) [l'émetteur].
- . Coût de la liaison entre l'émetteur et la racine [0].
- . Identité de l'émetteur.
- . Numéro du port de l'émetteur.

Coût des liens, en fonction inverse de leur débit :

- . $\text{Coût(lien)} = 10^9/\text{débit(lien)}$ (il existe une version adaptée aux débits supérieurs à 1 Gbit/s)

L'arbre couvrant est construit en 3 étapes :

1. Sélection d'un Switch Racine (Commutateur Racine)
2. Sélection d'un port Racine pour les Switch non-Root (Port Root)
3. Sélection d'un port désigné pour chaque segment

Commandes de diagnostic STP

Pour le diagnostic STP sur un VLAN :

```
#show spanning-tree vlan vlan-id
```

Pour le diagnostic STP d'une interface :

```
#show spanning-tree interface interface
```

Pour des informations détaillées :

```
#show spanning-tree detail
```

Pour vérifier uniquement les interfaces actives :

```
#show spanning-tree active
```

8. Commandes de configuration de STP

Désactivation de STP :

```
(config)#no spanning-tree vlan vlan-id
```

Priorité du commutateur :

```
(config)#spanning-tree vlan vlan-id priority priority
```

Coût et priorité d'un port :

```
(config-if)#spanning-tree [vlan vlan-id] cost cost
(config-if)#spanning-tree [vlan vlan-id] port-priority priority
```

Paramètres de délais :

```
(config)#spanning-tree [vlan vlan-id] max-age seconds
```

6 à 200 secondes, 20 secondes par défaut

```
(config)#spanning-tree [vlan vlan-id] forward-time seconds
```

4 à 200 secondes, 15 secondes par défaut

```
(config)#spanning-tree [vlan vlan-id] hello-time seconds
```

1 à 10 secondes, 2 secondes par défaut

Activation du rapid spanning-tree sur le switch

```
2960-RG(config)#spanning-tree mode rapid-pvst
```

Vérification des informations

```
2960-RG#sh spanning-tree
```

Fixer le switch root

Dans la copie d'écran suivante le switch est root pour les vlans 1 à 100. Puis on affiche les données spanning-tree pour le vlan 4.

```
switch(config)#spanning-tree vlan 1-100 root primary
switch(config)#end
switch#show spanning-tree vlan 4
```

Configurer une priorité sur un port

Dans l'exemple, l'interface prioritaire sera gi0/1 pour les vlans 1 à 100. On affiche ensuite les informations pour le vlan 4.

```
switch(config)#interface gigabitEthernet 0/1
switch(config-if)#spanning-tree vlan 1-100 port-priority 64
switch(config-if)#end
switch#show spanning-tree vlan 4
```

Configuration des ports d'accès reliés à un switch

Lors du démarrage d'un switch, la recherche de la meilleure topologie prend un peu de temps. La commande suivante fait passer directement le port de l'état **blocking** à l'état **forwarding**, le démarrage de l'interface est donc plus rapide. On appliquera cette commande sur les ports reliés à des machines terminales (PC, imprimante, ...).

```
2960-RG(config)#int range fa0/1 - 8
2960-RG(config-if-range)#spanning-tree portfast
```

Vérification

```
2960-RG#sh run int fa0/1
```

Fonctionnement

Afin d'éviter les boucles, le processus spanning-tree place les ports des switches dans un état, soit '**FORWARDING**', soit '**BLOCKING**'.

En état '**FORWARDING**', le switch forwarda les trames ethernet et suit son processus normal d'apprentissage de sa table de forwarding.

En état '**BLOCKING**', le switch ne forwarda pas les trames ethernet et n'est pas dans un état d'apprentissage. Néanmoins, le switch est toujours capable de recevoir des trames

appelées **BPDU** (Bridge Protocol Data Unit).

Le passage d'un état 'BLOCKING' à 'FORWARDING' d'un port ne peut s'opérer qu'en passant par les états '**LISTENING**' et '**LEARNING**'.

L'état 'LISTENING' correspond à un état où la table de correspondance MAC/interface de sortie va expirer.

L'état 'LEARNING' correspond à un état où le switch va remplir sa table de correspondance MAC/interface de sortie, mais ne forwardera toujours pas de trame.

Le passage d'un état 'LISTENING' à 'LEARNING' et de 'LEARNING' à 'FORWARDING' se fait dans un délai de **15s**. Ce délai est appelé : **Forward Delay**.

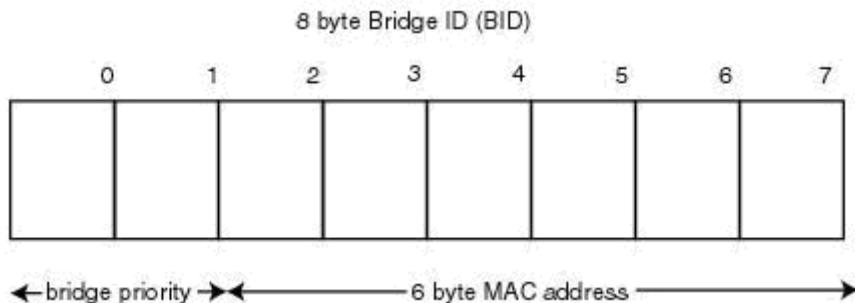
Une fois que le processus spanning-tree est complètement déroulé, une topologie stable est établie. Cette topologie reste stable tant que les messages BPDU envoyés tous les 2s (**Hello BPDU**) indiquent toujours le même état et que le temps **Max Age(20s)** n'est pas expiré. Si la topologie n'est plus stable, le processus de résolution et de création d'une topologie non-bouclée peut commencer après le délai Max Age(20s) (avec Max Age = 10 * Hello BPDU, soit 10 * 2s).

Le temps de convergence d'une topologie à une autre est donc d'environ : $10 * 2 + 15 + 15 = 50s$.

Afin d'établir une topologie le processus spanning-tree effectue les étapes suivantes :

Etape 1:

Sélectionner le 'Root Bridge' au moyen de son BID(Bridge ID)



Tous les switches émettent des BPDU avec pour Root ID leur Bridge ID. Le root ID indique le switch qui est la racine de la topologie. Celui qui a le plus bas BID gagne l'élection. Une fois, le 'Root Bridge' élu, celui-ci continue d'émettre des BPDU, alors que les autres switchs retransmettent ces derniers.

Etape 2:

Ensuite, pour les switchs non-root, il faut élire un 'Root-port (RP)'. Ce port est le port qui reçoit les BPDU avec un root-path-cost le plus faible. Le root-path-cost est le coût indiqué dans le BPDU afin d'atteindre le Root Bridge. Depuis le Root Bridge, le path-cost est de 0. Chaque port selon son type possède un coût.

Coûts révisés IEEE:

Vitesse	Coût
10Mbits	100

100Mbits	19
1Gbits	4
10Gbits	2

Chaque switch réémet aux autres switchs le BPDU en ajoutant au 'Root Path Cost', le coût de l'interface sur laquelle il a reçu le BPDU. Les ports depuis lesquels le 'root-path-cost' est le plus faible sont élu 'Root Port'. Ces ports sont passés en état '**FORWARDING**'.

Etape 3:

Finalement pour tous les segments LAN du réseau de switch, il faut déterminer les 'Designated'Port (DP)'. On identifie ces ports en utilisant de nouveau le path-cost et le Bridge-ID(==BID) du switch qui forwarde les BPDU émis par le Root Bridge, ceci depuis chaque bout du segment. Suivant le path-cost(le plus faible), on identifie le DP, si égalité le BID le plus faible gagne. Les ports qui ne sont ni 'Root Port', ni 'Designated Port' sont des 'Non-Designated Port'. Ils se trouvent dans un état bloqué.

A la fin de ce processus, il n'y a plus de boucle dans le réseau de switch.

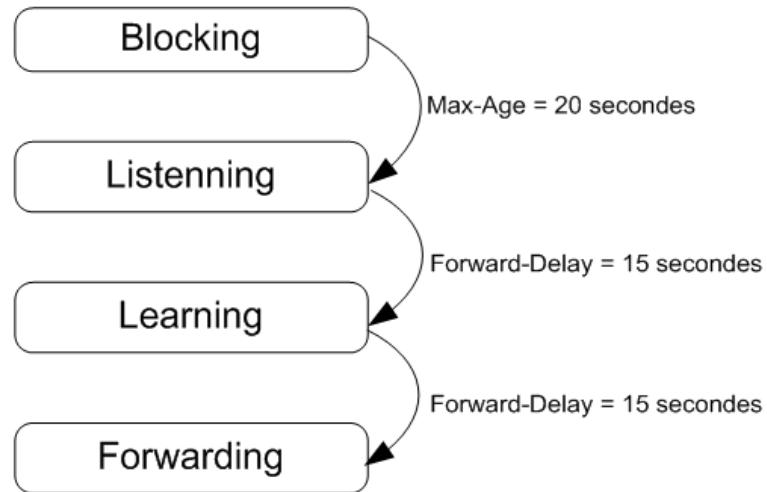
Convergence STP

- Afin de communiquer, STP utilise des BPDU
- Les BPDU Hello sont transmises toutes les 2 secondes

- Protocole STP:
 - Branchement d'un nouveau switch
 - Le port s'active, le protocole STP se met en marche
 - Max age (20 secondes) Temps de sécurité à attendre en cas de changement topologique
 - Listennning (15 secondes) Temps pour que le commutateur écoute les trames qu'il peut recevoir, sans émettre
 - Learning (15 secondes) Temps pour apprendre les informations de la topologie STP

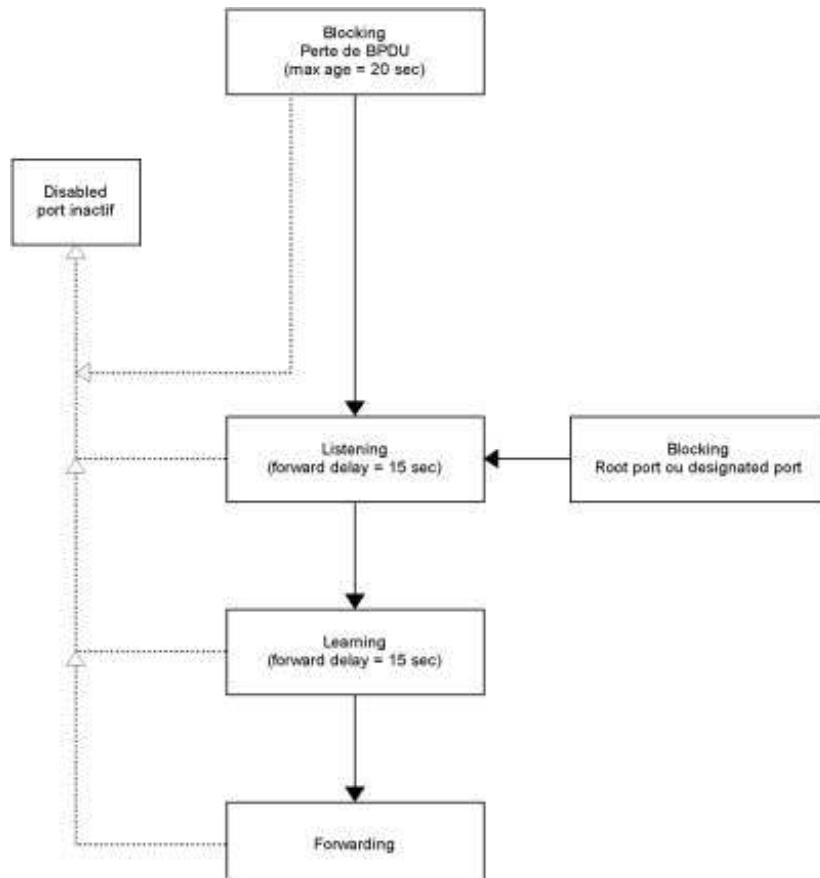
- Le port met donc 50 secondes à s'initialiser

- Temps de convergence = 50s :



- Lorsqu'une modification topologique est détectée :
 - Arbre STP recalculé
 - Trafic stoppé

Cinq états de ports peuvent rencontrés consécutivement sur un port avant que STP ait convergé. Chaque état comporte un délai qui varie en fonction de la version de STP utilisée sur le commutateur Cisco. En voici les propriétés.



Le compteur "age maximum" (Max Age) de 20 secondes par défaut est le temps maximal avec que STP effectue de nouveaux calculs quand une interface ne reçoit plus de BPDUs. Le temps de "forwarding" de 15 secondes par défaut est le temps de passage d'un état "listening" à "learning" et de "learning" à "forwarding". Bref, une topologie peut prendre jusqu'à 50 secondes avant de converger et de transférer du trafic. Aussi, la fréquence d'envoi de BPDUs Hello est de 2 secondes par défaut

Etat « Blocking »/ Reste dans cet état pendant 20 secondes max.

Rejette toutes les trames de données venant du segment attaché
Rejette toutes les trames de données venant d'un autre port de transfert
N'intègre aucune emplacement de station dans sa MAC table (il n'y pas d'apprentissage)
Reçoit les BPDUs et les transmet à son système
N'envoie pas de BPDUs reçus de son système
Répond à SNMP

Etat « Listening »/ Reste dans cet état pendant 15 secondes max.

Rejette toutes les trames de données venant du segment attaché
Rejette toutes les trames de données venant d'un autre port de transfert
N'intègre aucune emplacement de station dans sa MAC table (il n'y pas d'apprentissage)
Reçoit les BPDUs et les transmet à son système
Envie les BPDUs reçus de son système
Répond à SNMP

Etat « Learning »/ Reste dans cet état pendant 15 secondes max.

Rejette toutes les trames de données venant du segment attaché
Rejette toutes les trames de données venant d'un autre port de transfert
Intègre les emplacements de station dans sa MAC table (apprentissage)
Reçoit les BPDUs et les transmet à son système
Envie les BPDUs reçus de son système
Répond à SNMP

Etat « Forwarding »

Commute toutes les trames de données venant du segment attaché
Commute toutes les trames de données venant d'un autre port de transfert
Intègre les emplacements de station dans sa MAC table (apprentissage)
Reçoit les BPDUs et les transmet à son système
Envie les BPDUs reçus de son système
Répond à SNMP

Etat « Disabled »

Cet état est similaire à l'état « blocking » sauf que le port est considéré physiquement non opérationnel (*shut down ou problème physique*).

Rapid Spanning Tree (RSTP)

RSTP fait passer le temps de convergence à 6 secondes maximum ce qui le rend beaucoup plus opérationnel que STP.

Pour l'activer, en mode de configuration globale :

```
(config)#spanning-tree mode rapid-pvst
```

RSTP fonctionne de la même manière que STP. Il y a toutefois quelques différences.

1. Il n'y a plus que trois états pour les ports RSTP :

- Discarding (au lieu de Disabled, Blocking et Listening)
- Learning et Forwarding (ayant la même fonction)

2. Les rôles port Root et port Designated subsistent. Les meilleurs ports alternatifs prennent le nom de lien de sauvegarde de ces derniers : port Alternate et port Backup. Ils prennent le rôle port Root et port Designated en cas de défaillance.

3. Les ports connectant des périphériques terminaux s'appellent des ports Edge qui remplissent la même fonction que la fonction Portfast en PVST+.

MSTP (1)

- ⇒ Création du MSTP (Multiple Spanning Tree Protocol)
 - 802.1s
 - évolution du STP/RPVST et 802.1q
- ⇒ 802.1s a été ajouté au 802.1q en 2003
- ⇒ Compatibilité ascendante avec le STP/RSTP (802.1d / 802.1w)
- ⇒ Certains constructeurs n'ont pas attendu et ont implémenté des alternatives
 - PVST / Rapid-PVST chez Cisco (Per VLAN Spanning Tree)
- ⇒ MSTP de Cisco sorti avant la norme
 - ⇒ incompatible avec le MSTP standard (802.1s)
- ⇒ Avec MSTP on crée une MSTP region (CST)
- ⇒ Chaque region peut faire tourner plusieurs instances nommées MSTI (dans laquelle on place un ou plusieurs VLAN(s))
- ⇒ Principes
 - si un seul VLAN : même principe que le RSTP (et compatible)
 - si plusieurs VLANs
 - 1 arbre de recouvrement par MSTI
- ⇒ BPDU contenant le numéro de l'instance sur les liens taggés

PVST

Le **Per VLAN Spanning-Tree** est une amélioration propriétaire de Cisco qui permet d'avoir une instance ST par VLAN (ça permet de faire de la répartition de flux puisqu'on peut ainsi définir un root bridge différent pour chaque VLAN).

Cependant son inconvénient est que ce n'est pas un standard (donc concrètement ça ne tourne qu'entre équipements Cisco) et qui cela consomme beaucoup de ressources (CPU et réseau).

Comme ce protocole utilise une instance par VLAN, chaque BID doit contenir le numéro de VLAN : la priorité du STP (**bridge priority**, sur 16 bits) a été décomposée en 2 champs pour devenir l'**extended bridge priority** 4+12 bits : 4 pour la priorité du switch et 12 bits pour identifier le VLAN ($2^{12} = 4096$, le compte est bon). Cela permet donc de ne pas changer le format du champs, mais implique d'utiliser une priorité multiple de 4096 (on joue sur les 4 bits de poids fort du BID).

R-PVSTP

Rapid-PVST Protocol ou **Rapid Per VLAN Spanning Tree Protocol** permet de combiner le "rapide" et le "par VLAN" ST :

- **Rapid** : de converger plus vite lors d'un changement de topologie (2 secondes au lieu de 50 environ)
- **Per VLAN** : d'utiliser une instance STP par VLAN

C'est un protocole propriétaire CISCO à la différence du MSTP (**Multiple STP**, extension du RSTP, qui permet de créer plusieurs instances de STP avec un ou plusieurs VLAN rattaché).

Configuration (idem pour le PVSTP activé par défaut) :

On active le RPVST :

```
Switch1(config)#spanning-tree mode rapid-pvst
Switch2(config)#spanning-tree mode rapid-pvst
```

La priorité par défaut est de 32768 : on va déclarer le Switch1 en "root primaire" et le 2 en "root secondaire" backup, ce qui va avoir comme effet de passer la priorité du Switch1 à 24576 et du Switch2 à 28672.

```
Switch1(config)#spanning-tree vlan 445 root primary
Switch2(config)#spanning-tree vlan 445 root secondary
```

NB : quand on configure un switch en **root primary** sur un **vlan**, il va modifier dynamiquement sa priorité pour devenir **root** sur ce **VLAN** ; en revanche la commande **root secondary** fixe une priorité statique de 28672 (juste prioritaire à la priorité d'un switch lambda configuré par défaut).

On aurait pu gérer les priorités statiques à la main :

```
Switch1(config)#spanning-tree vlan 445 priority 8192
Switch2(config)#spanning-tree vlan 445 priority 16384
```

Vérification :

```
Switch1#sh spanning-tree vlan 445
```

MSTP

Le **Multiple Spanning-tree** (IEEE 802.1s) permet de créer des groupes (instances) de VLANs qui partageront une même topologie spanning-tree. On diminue ainsi la charge du réseau et des CPUs des commutateurs par rapport au PVST (moins de BPDUs et moins de calculs d'arbres). Cela permet par exemple de faire du partage de charge en déterminant des chemins différents pour différentes instances.

L'inconvénient est qu'un problème de ST sur une instance impacte tous les VLANs de celle-ci ; de plus le MST doit se configurer sur chaque switch d'une instance.

On associe donc un groupe de VLAN à une instance (numérotées de 1 à 15 max), contenue dans une région ; ces VLANs partageront leur topologie ST (ou plutôt RST car chez Cisco le MST implique de fonctionner en RST).

Par défaut l'instance 0 (MST0) contient tous les VLANs.

Les switchs appartenant à une même région MST apparaissent comme un seul “gros” switch par rapport aux autres ; ils doivent avoir en commun :

- les mêmes numéros d'instance
- le même mapping de VLAN par instance
- le même numéro de révision

Le BID (Bridge ID) du MST a le même format qu'en PVST, à ceci près que l'extended system ID contient le numéro de l'instance à la place du numéro de VLAN.

Configuration

On va créer 2 instances dans la région region1 avec un n° de révision de 1 :

```
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#instance 1 vlan 1-500
Switch(config-mst)#instance 2 vlan 501-1000
Switch(config-mst)#revision 1
Switch(config-mst)#name region1
Switch(config-mst)#exit
```

Puis on active le MST :

```
Switch(config)#spanning-tree mode mst
```

Chaque commutateur doit avoir la même configuration de région sous peine de ne pas pouvoir communiquer avec les autres commutateurs “régionaux”.

Pour réinitialiser la détection des protocoles ST, il faut passer la commande :

```
clear spanning-tree detected-protocols
```

Dans certains cas (à déterminer) il faut passer la directive suivante sur les interfaces physiques reliées à certains commutateurs :

```
Switch(config-if)#spanning-tree mst pre-standart
```

Vérification

```
show spanning-tree mst configuration
show spanning-tree mst
```

La question piège au CCNA !



Tout d'abord, rectifions une erreur que Cisco s'amuse à poser pendant l'examen; Qu'est ce que le Wifi ? Ah bonne question, ben c'est les réseaux sans fil? Et ben non!

Les réseaux sans fil sont les réseaux qui contiennent des équipements qui communiquent par des ondes radios, on parle alors de WLAN – Wireless LAN. Si vous avez du mal avec la notion de LAN, je vous invite à lire [cet article](#).

Mais alors qu'est ce que le Wifi, ou plutôt la Wireless Fidelity Alliance? C'est une association mondiale qui certifie l'interopérabilité des équipements. Bien évidemment, cette association à but non lucratif est constituée des acteurs majeurs des réseaux dont les constructeurs de cartes sans-fil, de clé USB sans-fil, de bornes d'accès... dont Cisco. Vous pouvez trouver la liste complète sur le site officiel: <http://www.wi-fi.org/who-we-are/member-companies>

Maintenant que l'erreur est corrigée, si on vous pose la question « à quoi correspond le sigle WiFi? », ne répondez pas que c'est la technologie des réseaux sans fil ! Pour la suite de l'article, soyez indulgent avec moi car désormais je parlerai plus souvent de Wifi car c'est le terme le plus connu.

Fonctionnement

Avant de commencer à décrire le fonctionnement du WLAN, il faut comprendre ce qu'est la méthode CSMA/CD décrite [dans cet article](#). Une fois cette notion assimilée, vous pouvez continuer la lecture.

Le WLAN utilise la technologie **CSMA/CA** au lieu du CSMA/CD. **CA** pour **Collision Avoidance** ou en français évitement (ou annulation) des collisions.

Le WLAN utilise des ondes radios pour communiquer entre les équipements. Au lieu d'envoyer des impulsions électriques (sur câble cuivre) ou de la lumière (sur fibre optique), on utilise les fréquences radios dont l'unité est le Hertz. Si on reprend le **modèle OSI** ou le **modèle TCP/IP**, on place les ondes radios au niveau de la couche physique (niveau 1).

Malheureusement, de nouveaux problèmes sont apparus avec le WLAN comme la **couverture** (je capte plus dès que je m'éloigne trop de la borne), les **interférences** avec d'autres équipements qui utilisent les mêmes fréquences (comme le four à micro-onde!).

Obligation légale

Comme nous émettons des ondes radios dans tous les sens, le WLAN est soumis à des réglementations qui dépendent de chaque pays. C'est pourquoi, quand on configure une borne d'accès Wifi Cisco, il y a un champ où on sélectionne le pays dans lequel on se trouve, ça permet à la borne de se caler par rapport à des paramètres définis par la réglementation du pays.

Voici les principaux organismes à connaître pour le CCNA ainsi que leurs fonctions:

- **IEEE – Institute of Electrical and Electronics Engineers** : organisme professionnel technique, non commercial qui se charge, entre autre, de la rédaction de standards internationaux, que ce soit WLAN ou autres. Chaque standard à un dénomination, pour le WLAN c'est la norme **802.11**. Leur site est [ici](#).
- **ETSI – European Telecommunications Standards Institute** : comme l'IEEE mais pour la rédaction de standards propres à l'Europe (ETSI a rédigé l'HiperLAN, l'IEEE a rédigé le 802.11 ou WLAN WiFi). Leur site est [ici](#).
- **ITU-R – International Telecommunication Union**: Secteur des radiocommunications que ce soit filaire ou sans-fil. Le R de ITU-R désigne RadioCommunication. Cet organisme régule les radiofréquences utilisées par les communications sans fil. Leur site est [ici](#).
- **ISM – Industrial Scientific & Medical** : Ce n'est pas un organisme mais c'est important de savoir ce que c'est. Les bandes ISM sont des bandes de fréquences qui ne sont pas soumises à des réglementations nationales et qui peuvent être utilisées librement (gratuitement et sans autorisation) pour des applications industrielles, scientifiques et médicales. Les seules obligations à observer sont la **puissance d'émission** et la **perturbation de fréquences voisines**. C'est sur ces fréquences-çi que la WLAN fonctionne.

Les 3 technologies 802.11

Voici un tableau qui récapitule les 3 technologies à connaître pour le CCNA. Beaucoup de personnes m'ont demandé si le 802.11n est au programme de l'examen. A ce jour, juin 2012, la réponse est non.

Historiquement, les 2 normes 802.11b et 802.11a sont sorties le même mois en 1999 mais elles fonctionnent sur des plages de fréquences différentes. La norme 802.11g est sorti plus tard en 2003 et fonctionne **sur les mêmes fréquences** que le 802.11b (question classique du CCNA).

On remarque qu'en fonction de la technologies utilisées, on atteint des débits plus ou moins élevés.

	802.11b	802.11a	802.11g	
Bande de fréquence	2,4 GHz	5 GHz	2,4 GHz	
Transmission	DSSS	OFDM	DSSS	OFDM
Débits [Mbps]	1, 2, 5.5, 11	6, 9, 12, 18, 24, 36, 48, 54	1, 2, 5.5, 11	6, 9, 12, 18, 24, 36, 48, 54

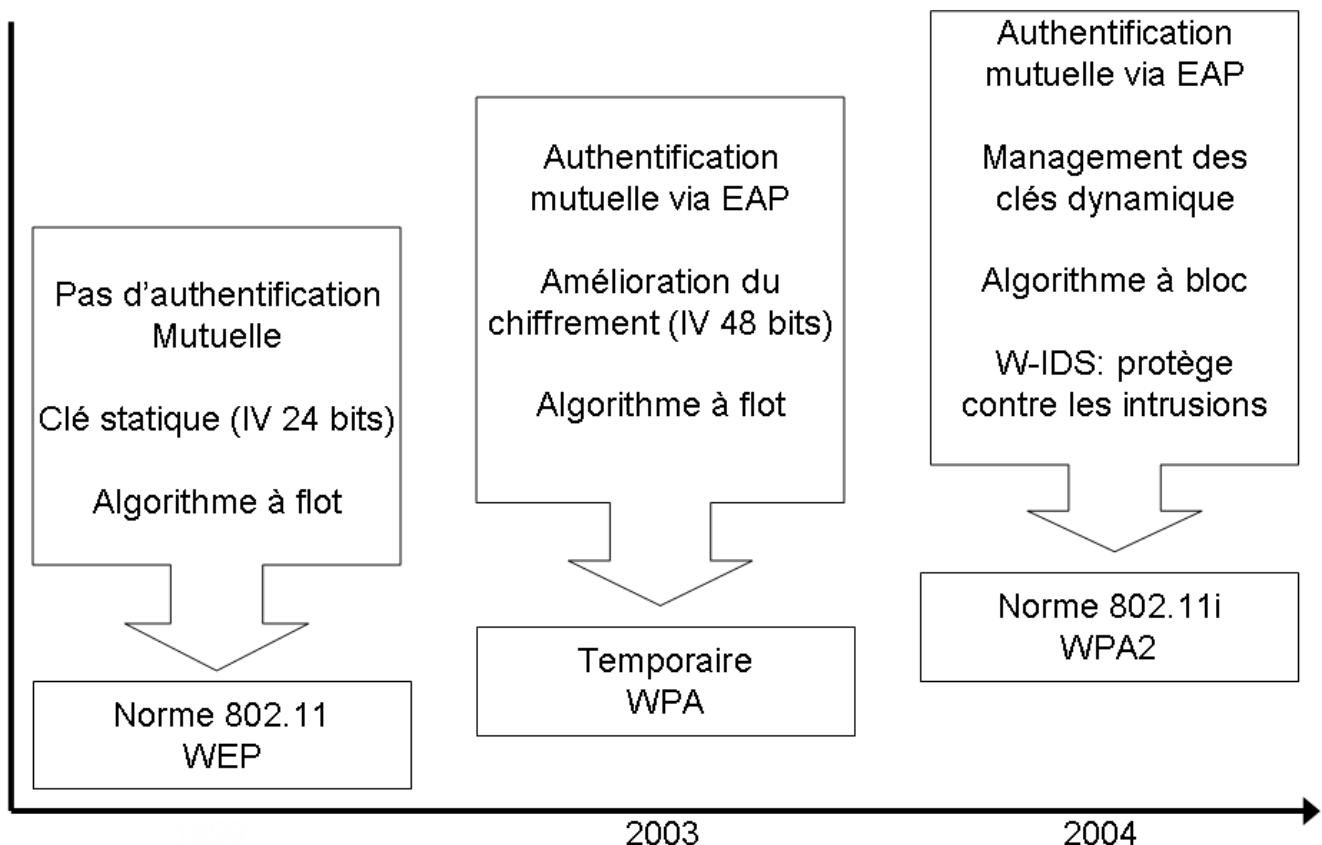
Et la sécurité dans tout cas?

Les ondes radio ne s'arrêtent pas à vos murs, elles les traversent et vont chez vos voisins. On assimile souvent une borne WLAN à un hub avec un câble cuivre qui arrive chez votre voisin, il ne lui reste plus qu'à se « brancher » sur votre borne pour accéder à votre réseau, sic!

De plus, la norme 802.11 (WLAN) a été établie pour une facilité d'implémentation, ne se souciant pas de la sécurité des données dans un premier temps. Sur un réseau WLAN qui s'apparente à un Hub, tout le monde peut écouter ce que vous envoyez/recevez car la plupart des protocoles transitent en clair comme la messagerie (POP, SMTP, IMAP), le Web (HTTP), MSN... et beaucoup de sniffers sont disponibles sur Internet (Ethereal, Wireshark, Kisnet,...) pour analyser ces protocoles.

Il est très facile par exemple de récupérer une communication MSN, une conversation vocale... oui ça fait peur et pour conclure, sachez qu'une clé WEP se casse en moins d'une heure.

Des mécanismes de sécurité ont été pensés et implémentés pour palier à ces problèmes. On pourrait résumer l'évolution de la sécurité WLAN avec le schéma suivant:



Remarques importantes

- Approximativement, le débit pratique est équivalent à la moitié du débit théorique pour les 3 technos (a, b et g) due aux overheads (surcharge de service : données utilisées pour le control par exemple):

	Débit théorique (Mbps)	Débit réel (Mbps)
802.11b	11	6
802.11g (avec aucun client 802.11b dans la cellule)	54	22
802.11a	54	25

- L'avantage du 802.11g est l'interopérabilité avec les clients 802.11b qui sont les plus déployés au niveau mondial. Mais le débit des clients 802.11g est fortement diminué lors de la présence de clients 802.11b raccordé sur une même borne Wifi.
- Les fréquences de la bande des 2,4Ghz ont une propagation plus intéressante que celles de la bande des 5GHz.

A quoi sert-il?

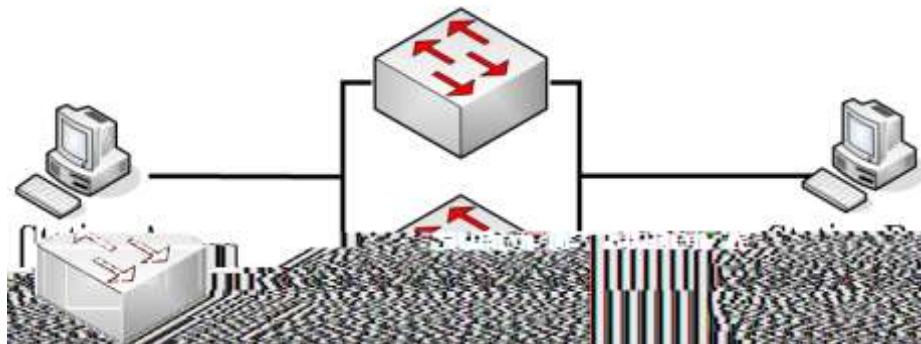
L'objectif des réseaux est de faire en sorte que les paquets arrivent à destination. Une solution est de dupliquer les équipements physique pour qu'en cas de panne sur l'un d'eux, l'autre équipement prenne le relai; **on appelle ça la redondance ou la résilience**.

Architecture non redondée

Sur le schéma ci-dessus, on voit bien que si le switch tombe (panne électrique, bug...), plus aucune communication entre les ordinateurs A et B n'est possible.

Architecture redondée

Maintenant que l'on souhaite que les paquets entre les ordinateurs A et B transitent même en cas de panne matériel, créons cette nouvelle architecture:



Avec cette architecture, on voit bien que si le switch du haut ne fonctionne plus, le switch du bas peut tout même transmettre les paquets de A vers B et de B vers A.

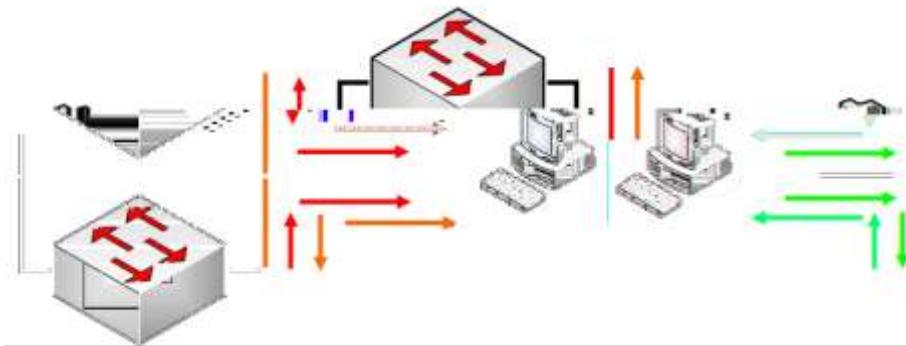
Les 3 problèmes à savoir pour le CCNA

Lors de l'examen, vous allez tomber sur des questions propre au fonctionnement intrinsèque du spanning-tree et de ses différentes versions mais aussi sur les problèmes rencontrés par la mise en place d'une redondance physique dans un LAN commuté.

Retenez bien ces 3 problèmes car c'est une question classique du CCNA.

1er problème: Tempête de broadcast

Sur l'architecture redondée précédente, imaginons que la station A envoi un message de broadcast (trame niveau 2 avec comme adresse MAC de destination FFFF.FFFF.FFFF). *Que se passe-t-il?*



- Le switch du haut reçoit la trame sur son port, **extrait l'adresse MAC** de destination (FFFF.FFFF.FFFF) et **la duplique sur tous ses ports** car c'est une adresse de broadcast. La trame sort donc du switch du haut et se dirige vers le switch du bas
- idem pour le switch du bas; il reçoit la trame sur son port, **extrait l'adresse MAC** de destination (FFFF.FFFF.FFFF) et **la duplique sur tous ses ports** car c'est une adresse de broadcast. La trame sort donc du switch du bas et se dirige vers le switch du haut
- et ces trames **tournent sans arrêt** entre les 2 switchs, faisant monter leur CPU à 100% et les font plus ou moins planter (souvent un reboot est nécessaire)

Ce phénomène s'appelle la **tempête de broadcast**, ou **broadcast storm** en anglais.

2ème problème: Duplication de trame

Maintenant, imaginons que la station A envoi une trame vers la station B, donc la trame sera forgée avec les informations suivantes:

- adresse MAC source: A
- adresse MAC destination: B

Que se passe-t-il?

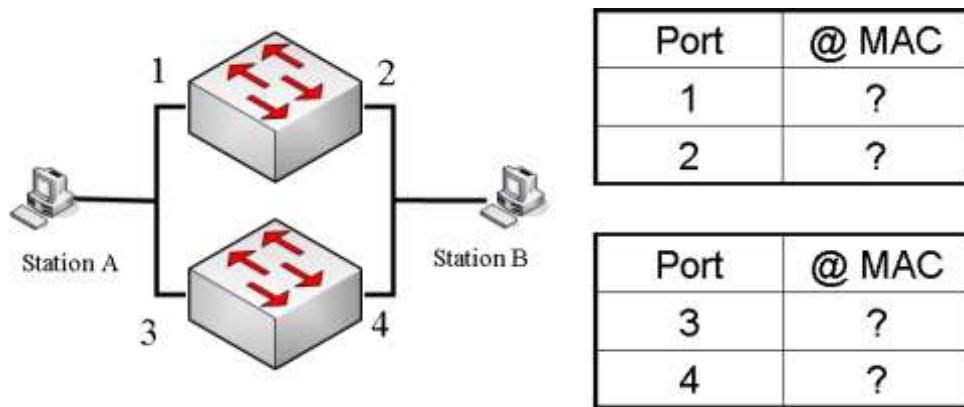
- Le switch du haut reçoit la trame sur son port (flèche rouge), **extrait l'adresse MAC** de destination (B) et la commute sur le port de droite. La station B reçoit bien la trame de la station A
- Mais le switch du bas reçoit aussi la trame sur son port (flèche orange), **extrait l'adresse MAC** de destination (B) et la commute sur le port de droite. La station B reçoit donc pour une deuxième fois la trame de la station A

Ce phénomène s'appelle la **duplication de trame** (pas top comme optimisation réseau 😊)

3ème problème: Instabilité de la table CAM

Maintenant, regardons un peu ce qu'il se passe côté table CAM – Content Addressable Memory – du switch.

Pour ceux qui ont oublié cette notion, je vous renvoi vers ce chapitre ([switch](#)).



Reprendons la trame précédente (message de A vers B):

- la trame arrive sur le port 1 du switch du haut. Le switch **extrait l'adresse MAC source et l'insère dans sa table CAM** [port 1 = adresse MAC A]
- la trame arrive aussi sur le port 3 du switch du bas. Le switch **extrait l'adresse MAC source et l'insère dans sa table CAM** [port 3 = adresse MAC A]

Maintenant que chaque switch a extrait l'adresse MAC source pour l'insérer dans sa table, chacun **extrait l'adresse MAC de destination (B) et la compare à sa table**. Comme aucune entrée n'est trouvée, chaque switch va dupliquer la trame sur tous ses ports:

- le switch du haut envoie la trame sur son port 2
- le switch du bas envoie la trame sur son port 4

Et c'est là où ça devient cocasse car chaque switch reçoit la trame de l'autre switch...

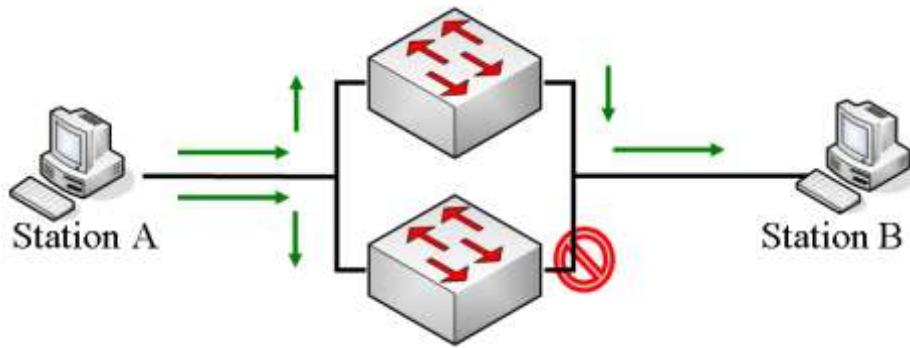
- le switch du haut reçoit sur son port 2 la trame du switch du bas
 - le switch **extrait l'adresse MAC source et l'insère dans sa table CAM** [port 2 = adresse MAC A]. Pour cela, **il supprime l'entrée précédente** qui était [port 1 = adresse MAC A]
- le switch du bas reçoit sur son port 4 la trame du switch du haut
 - le switch **extrait l'adresse MAC source et l'insère dans sa table CAM** [port 4 = adresse MAC A]. Pour cela, **il supprime l'entrée précédente** qui était [port 3 = adresse MAC A]

On voit ici que les switchs mettent à jour leur table CAM à chaque fois qu'ils reçoivent une trame.

Ce phénomène s'appelle **l'instabilité de la table CAM**.

Résolution des 3 problèmes

Pour éviter ces 3 problèmes (**tempête de broadcast**, **duplication de trame** et **instabilité de la table CAM**), le protocole spanning-tree a été créé. Comme ces problèmes proviennent du fait que le réseau commuté est face à une boucle physique, le spanning-tree permet d'identifier cette boucle et de la bloquer « logiciellement ».



Dans notre exemple, tout le trafic passera par le switch du haut pour joindre la station B, le chemin du bas étant bloqué au niveau du port du switch du bas.

Si le switch du haut tombe en panne, le protocole spanning-tree va le détecter et va débloquer le port du bas. A ce moment, tout le trafic passera pour le switch du bas.

Voilà à quoi sert le spanning-tree !

A retenir pour le CCNA

Dans un prochain chapitre, je détaillerai en profondeur le fonctionnement de ce protocole et ses différentes versions jusqu'au MSTP .

Mais pour le moment, retenez que les points suivants pour l'examen:

- en mettant en place une architecture redondée, on est face à 3 problèmes majeurs:
 1. tempête de broadcast
 2. duplication de trame
 3. instabilité de la table CAM
- Pour résoudre ces problèmes, le spanning-tree a été créé et permet d'éviter les boucles physiques en désactivant un port logiciellement, et le réa-active au besoin pour assurer la résilience du réseau

Sécurisation WEP

On a une possibilité pour **retreindre l'accès** à la borne Wifi ainsi que de **rendre les communications illisibles** entre clients légitimes et la borne d'accès: c'est l'utilisation du **chiffrement**.

Si on **définit un mot de passe** commun entre les clients et la borne d'accès alors seuls les clients qui connaissent le mot de passe peuvent transiter par la borne WiFi. Ce même mot de passe va être utilisé pour **chiffrer les trames WiFi** pour les rendre illisibles pendant le transport dans les airs.

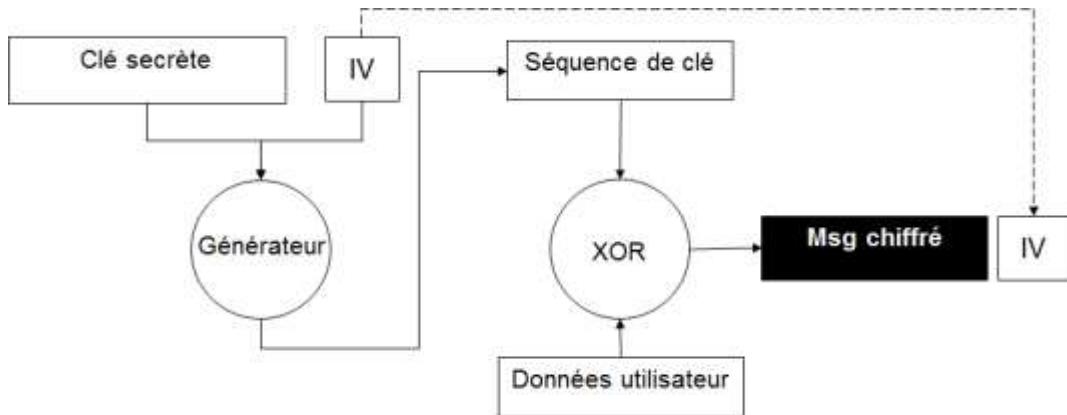
La première application de cette notion de chiffrement pour le WLAN s'appelle la clé **WEP – Wired Equivalency Privacy**. On définit un **mot de passe** qu'on appelle (à tort) clé WEP et on la configure sur la borne d'accès et sur les clients WiFi. Lors de la communication, seuls ceux qui ont la bonne clé WEP sont acceptés par la borne.

Pour reprendre **l'exemple de la porte d'une maison**, c'est comme si la borne d'accès était la porte de maison et la clé WEP était la clé de la serrure, vous distribuez la clé de la serrure à chaque client légitime.

Celui qui n'a pas cette clé ne peut pas ouvrir la porte. Logique et efficace ! Même si on va voir que **ce n'est plus aujourd'hui** une bonne solution de sécurité.

Remarque: beaucoup d'administrateurs ont la flegme de retenir le mot de passe alors il arrive que la clé WEP soit inscrits sur le dos de la borne Wifi ou sur un post-it 😊

Si on fait un schéma simplifié du fonctionnement du chiffrement utilisé pour une clé WEP, ce serait le suivant:



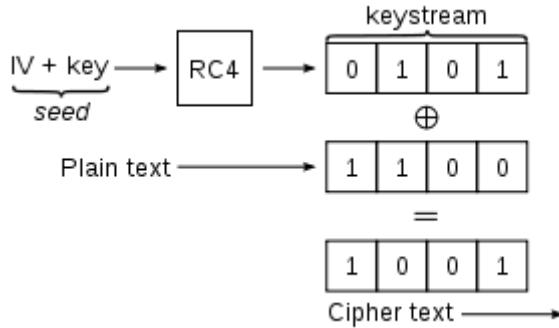
Explications du schéma:

- **clé secrète:** c'est ici que vous définissez votre mot de passe
- **IV pour Vecteur d'Initialisation:** pour ajouter un peu plus de complexité à votre mot de passe, l'ordinateur **concatène** à la clé secrète un**nombre aléatoire** qui est calculé automatiquement
- **Générateur:** l'algorithme (ici **RC4**) va générer à partir de la clé secrète et de l'IV **une séquence de clé**. Dites vous que c'est un méga mot de passe 😊
- **Données utilisateur:** ici se trouve les données utilisateur (la trame Ethernet) à transférer dans les airs
- **XOR:** c'est la fonction logique « **OU exclusif** » qui prend la **séquence de clé** et les **données utilisateur** et effectue un XOR entre eux
- Le résultat de ce XOR donne un message binaire dit « **chiffré** » car incompréhensible

Une fois le XOR calculé, la carte WiFi envoie les données dans les airs en encapsulant le message chiffré dans l'entête WiFi, ou plus précisément dans l'entête 802.11 pour les puristes.

Vous remarquerez que **l'IV est ajouté en clair** à coté du message chiffré.

C'est tout à fait logique: l'IV est calculé automatiquement par celui qui va chiffrer le message, par exemple votre carte WiFi. Il faut bien que la borne d'accès qui va recevoir ce message puisse le déchiffrer. Et pour le déchiffrer il lui faut 2 paramètres, la **clé secrète** que vous avez configurée manuellement des deux cotés et l'**IV** que la carte WiFi du client a **généré automatiquement**. Voilà pourquoi l'IV est **transmis en clair**, c'est pour le **destinataire**.



Important à comprendre: Le XOR est une fonction réversible:

- [séquence de clé] XOR [message en clair] = message chiffré
- [séquence de clé] XOR [message chiffré] = message en clair

Donc on voit bien que **dés qu'on connaît la séquence de clé** alors on peut déchiffrer un message chiffré !

Donc pour résumer:

- le chiffrement WEP est un protocole chargé du **chiffrement des trames** et utilise l' algorithme symétrique **RC4**
- la clé secrète a une longueur de **40 ou 104 bits**.
- Cette clé secrète doit être déclarée au niveau du point d'accès et des clients
- A cela s'ajoute **24 bits d'IV** (d'où le fait que l'on voit souvent dans les configuration, clé WEP de **40+24=64 bits ou 104+24=128 bits**)

Pourquoi le WEP est considéré comme obsolète?

```
Terminal
File Edit View Terminal Tabs Help

[82:34:54] Tested 627488 Keys (got 55118 IVs)

# depth byte(vote)
0 0/ 1 FC(70000) E7(06304) 58(62976) A0(62728) 2A(62464)
1 0/ 1 81(72980) 45(64512) 3F(63744) 1C(62728) 3A(62328)
2 0/ 2 A2(66568) A6(66208) B0(64708) E8(64256) ED(64256)
3 0/ 1 C8(79616) 3C(66816) B9(64888) D7(64888) 55(63488)
4 0/ 2 9B(65288) 4F(64256) 3E(63232) 7D(63232) 2F(63232)
5 0/ 1 B3(76280) 50(66568) 13(66304) 3F(65208) 87(63280)
6 0/ 1 2E(72192) 94(64256) B0(63744) 90(63408) 98(63232)
7 0/ 1 1A(72704) 80(66304) 16(64708) 53(64760) D3(64760)
8 0/ 2 4A(65328) 7D(66016) 3B(65536) 9B(65624) 56(64512)
9 0/ 1 14(66568) C0(64096) 89(63488) EF(63488) 47(62976)
10 0/ 1 58(67328) 59(67328) 00(66304) B4(66948) EE(66648)
11 1/ 1 10(66568) 34(65256) B0(64256) 00(64256) 49(63488)
12 1/ 2 A8(64444) B9(63700) 3E(63228) C7(62428) 30(62368)

KEY FOUND! | F0:01:A2:C8:83:2E:1A:00:14:C9:0F:AA |
Decrypted correctly: 100%
root@dehim:kootha#
```

Aujourd'hui, **on n'utilise plus** le WEP car le fait que son **IV** n'aît une taille que de 24 bits permet à des pirates de calculer toutes les possibilités de

valeurs de cet IV très rapidement. Et oui, 24 bits, ça ne fait « **que** » 2^{24} possibilités et avec les ordinateurs d'aujourd'hui, ça prends quelques secondes.

Authentification 802.1x

Le **standard 802.1x** est une solution de sécurisation, mise au point par l'IEEE en juin 2001, permettant **d'authentifier** (identifier) un utilisateur souhaitant accéder à un réseau (filaire ou WiFi) grâce à un **serveur d'authentification**. Ce serveur est souvent appelé **Serveur RADIUS**. De plus cette authentification est mutuelle dans le sens où le client identifie aussi le réseau dans lequel il entre.

Quand vous allez à la banque, vous allez dans une agence de **vos** banque et pas dans une agence d'une autre banque, c'est pareil ici.

Le standard 802.1x repose sur des protocoles **EAP (Extensible Authentication Protocol)** défini par l'IETF dont le rôle est de transporter les informations d'identification des utilisateurs.

Pourquoi je précise « des » protocoles EAP?



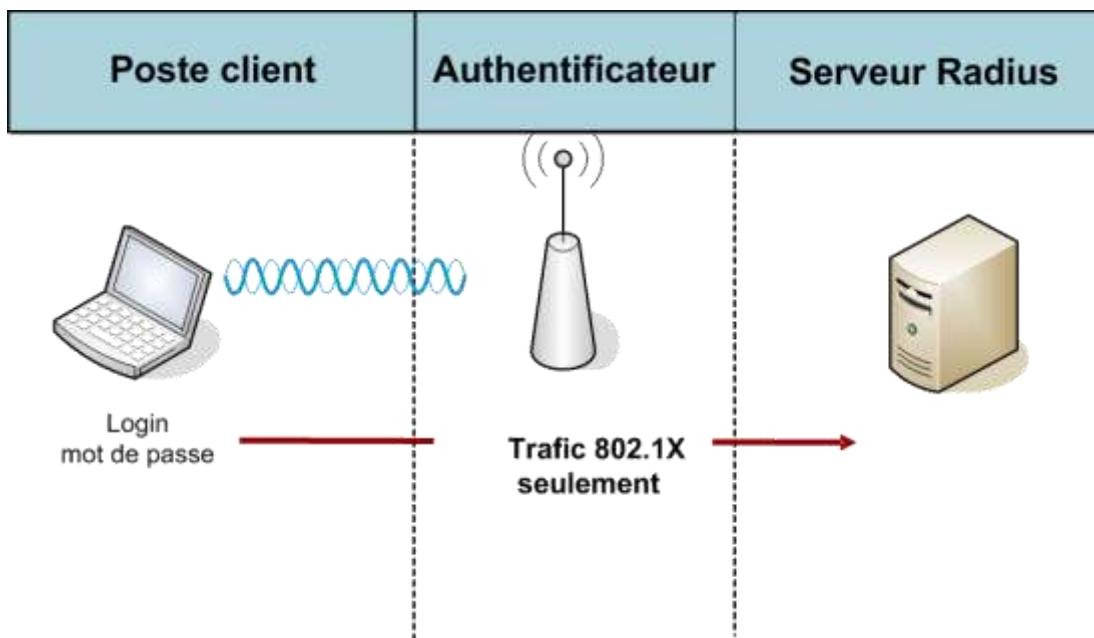
Car en fonction de votre infrastructure, vous allez peut être vouloir mettre en place une authentification des utilisateurs par un **mot de passe**, par des **certificats numériques**, par des **Token**... ce sont des **protocoles EAP différents** qui seront utilisés en fonction du mode d'authentification souhaité:

- EAP-LEAP
- EAP-FAST
- EAP-PEAP
- EAP-TLS
- ...

En cliquant sur l'image de droite pour l'agrandir, on peut voir la configuration d'une carte WiFi en **EAP-PEAP**. En fonction du type d'authentification, vous choisissez tel ou tel protocole EAP.

Fonctionnement du 802.1x

Le fonctionnement du standard 802.1x est en fait très simple malgré son nom barbare:



1. Le **client** (votre ordinateur portable) **se connecte** en WiFi à la borne d'accès
2. Cette borne d'accès est configurée pour appliquer le standard **802.1x** via le protocole **EAP**, la borne vous demande de rentrer vos identifiants
3. Dans la fenêtre Windows qui s'est affichée, **vous entrez vos identifiants** (par exemple: *login = cyril et mode passe = toto*)
4. Une fois que la borne a reçue vos identifiants, **elle les transmet** à un serveur d'authentification, dit **serveur RADIUS**
5. C'est ce serveur qui va **valider ou non** vos identifiants. Supposons qu'il accepte vos identifiants, **il avertit** la borne d'accès qu'elle peut vous autoriser à entrer dans le réseau
6. Vous avez désormais accès au réseau et vous pouvez surfer sur l'intranet et l'internet 😊



Prenons un exemple dans la vraie vie pour faire un comparatif explicite:

- Après un vol international, vous débarquez de l'avion et arrivez au contrôle d'immigration
- la personne vous demande de vous identifier en vous demandant votre passeport, que vous lui donnez
- elle scan le passeport, votre identité est transmise à un serveur qui vérifie si vous n'êtes pas sur une liste noire
- il vous rend le passeport et vous entrez officiellement dans le pays

Dans cet exemple on identifie les 3 composants relatif au standard 802.1x:

- le **client** (*supplicant* en anglais): c'est votre ordinateur portable qui souhaite accéder au réseau (ou vous qui descendez de l'avion)

- la **borne d'accès** (*authenticator* en anglais): elle va vous demander de vous identifier afin de laisser vos trames transiter dans le réseau (c'est la personne du contrôle d'immigration)
- le **serveur d'authentification Radius** (*authentication server* en anglais): c'est le serveur qui décide si vous avez le droit ou non d'utiliser le réseau (c'est le serveur de la douane avec sa liste noire)

Sécurisation WPA

Pour la petite histoire, lorsque les entreprises se sont rendues compte que le chiffrement WEP était inefficace, elles ont arrêté de déployer du WiFi. A ce moment là, un groupe d'étude appelé **802.11i** a été créé pour définir une sécurité plus élevée que le WEP, ce groupe a sorti la norme du même nom.

Aujourd'hui la **norme 802.11i** est **la référence** pour la sécurisation du WiFi.

Mais à l'époque, ce groupe n'avait pas encore sorti leurs recommandations (fainéants!) alors l'**alliance WiFi** les a doublé et a préféré sortir une **solution temporaire** en attendant le **802.11i**. Cette solution temporaire s'appelle le **WPA** !

Le **WPA** est une sorte de rustine en attendant le 802.11i. Il utilise:

- le **802.1x** pour **l'authentification** (mais reste optionnel)
- l'algorithme de chiffrement **TKIP (Temporary Key Integrity Protocol)**, plus robuste que l'algorithme **RC4** du WEP. Il permet la **génération aléatoire** de clés et offre la possibilité de modifier la clé de chiffrement plusieurs fois pour une sécurité plus forte.

On a vu que l'utilisation de 802.1x **impose** la mise en place d'un serveur Radius, ce qui peut poser problème pour les petites entreprises car ça reste cher. On a donc **2 modes de fonctionnement** du WPA (comme pour le WPA2):

- **Mode Personnel:** dans ce mode, on définit un **mot de passe partagé** entre le client et la borne d'accès, ce mot de passe s'appelle **PSK** pour **Pre-Shared Key**. C'est quasiment le même principe que la clé WEP mais avec un algorithme plus puissant. Pas besoin d'un serveur Radius.
- **Mode Entreprise:** dans ce mode, on utilise le **standard 802.1x** donc la mise en place d'un serveur Radius est **nécessaire**.

Sécurisation WPA2

Le 802.11i a été ratifié le 24 juin 2004 afin de fournir une solution de sécurisation poussée des réseaux WiFi. Il s'appuie sur l'algorithme de chiffrement **TKIP**, comme le WPA, mais **supporte également** le chiffrement symétrique **AES (Advanced Encryption Standard)**, beaucoup plus robuste que TKIP.

La **Wi-Fi Alliance** a alors créé une nouvelle sécurisation baptisée **WPA2** pour les nouveaux matériels supportant le standard 802.11i.

Et comme pour le WPA, on peut l'utiliser selon que l'on souhaite mettre en place un serveur Radius ou non pour l'authentification 802.1x:

- **Mode Personnel:** utilisation d'un PSK
- **Mode Entreprise:** utilisation du 802.11x donc d'un serveur Radius

Résumé WPA et WPA2

Ce tableau résume les 2 modes de configuration que l'on peut trouver dans les sécurisations WPA et WPA2.

Mode de configuration	WPA	802.11i / WPA2
Mode Personal	Authentification: PSK	Authentification: PSK
	Chiffrement : TKIP	Chiffrement : AES
Mode Enterprise	Authentification: 802.1x / EAP	Authentification: 802.1x / EAP
	Chiffrement : TKIP	Chiffrement : AES

Mais il existe aussi des attaques qui impacte le Wifi, non pas dans le sens **vol de données** et **pénétration** dans le réseau mais plutôt dans le sens de la la **disponibilité** du service.

Conclusion

La sécurité pour le Wifi est importante du fait que n'importe qui peut analyser les trames niveau 2, il faut alors protéger son infrastructure sans-fil selon les principes suivants:

- le **filtrage** par adresse MAC est facilement contournable
- **cacher** le SSID ne sert strictement à rien car en analysant le trafic, on le retrouve en clair dans les trames Wifi

- la sécurisation WEP est aujourd'hui **à bannir** car cassable en quelques minutes avec n'importe quel portable
- l'**authentification 802.1x** est aujourd'hui recommandée pour une authentification mutuelle (serveur radius et client) et utilise des protocoles dit EAP: EAP-PEAP, EAP-Fast...
- la sécurisation WPA est une **solution temporaire** qui utilise l'authentification robuste 802.1x mais un chiffrement pas optimal
- la sécurisation **WPA2** qui suit la norme 802.11i est la **solution optimale**
- la protection contre les attaques extérieures par la mise en place de **W-IDS**

Trunk 802.1Q et ISL, ce qu'il faut savoir pour le CCNA

Avec les chapitres précédents, nous savons comment **créer un VLAN** (cf chapitre [VLAN](#)), comment **propager cette création** de VLAN sur tous les switchs du réseau (cf chapitre [VTP](#)) et **comment attribuer un port** dans un VLAN (cf fin du chapitre [VLAN](#)).

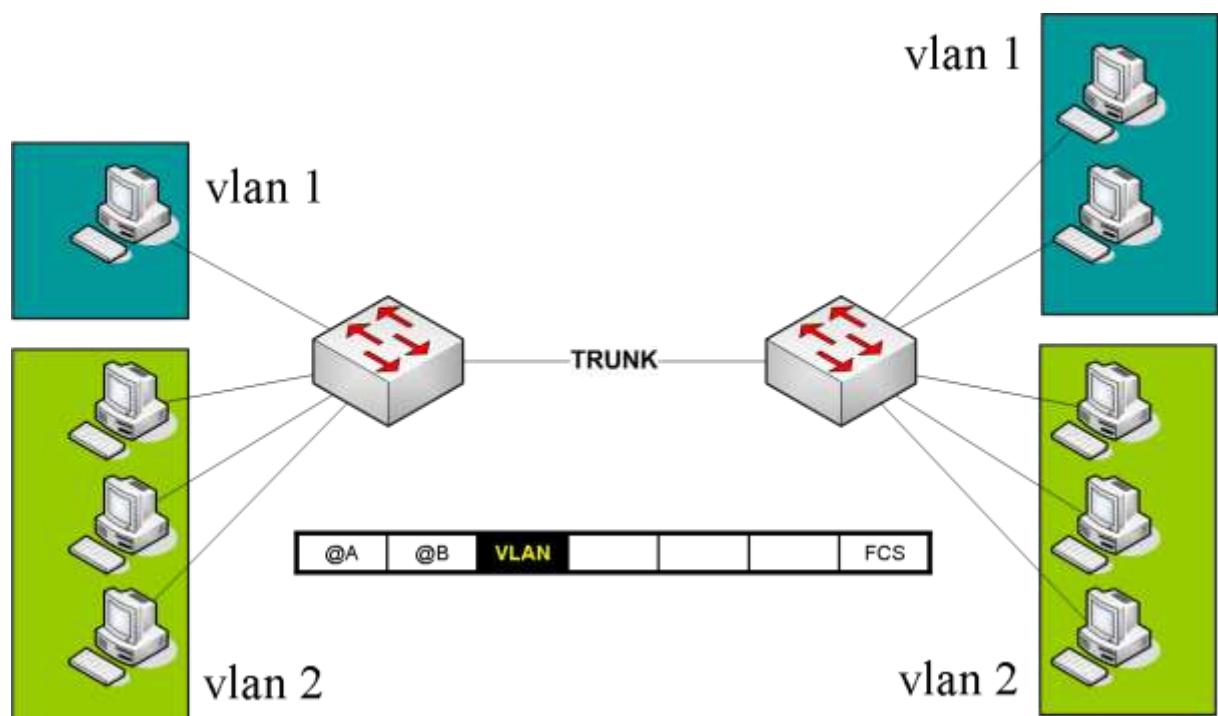
Maintenant, la question qui tue: *quand une trame provenant d'un switch voisin arrive sur notre switch, comment sait-il à quel VLAN appartient la trame reçue?*

Et bien, si on ne fait rien, le switch considérera que la trame appartient au VLAN configuré sur le port (VLAN 1 par défaut). Il faut donc configurer les switchs pour qu'à chaque fois qu'une trame sort d'un port pour joindre un autre switch, on y rajoute l'identifiant du VLAN auquel la trame appartient. C'est la notion de **Trunk!**

Définition

Le trunk est le mécanisme qui permet d'**insérer l'identifiant du VLAN** sur une trame utilisateur. Toute trame se propageant sur plusieurs switchs conservera toujours l'information de son appartenance à son VLAN. Et le switch de destination saura avec quels ports la trame peut être commutée (ports appartenant au même VLAN).

Cette configuration de lien Trunk s'effectue sur les liens entre switchs, souvent appelés **uplink**.



Dans le schéma ci dessous, on configure le lien inter-switch en Trunk. Toutes les trames qui sortiront sur ce lien (switch de droite ou de gauche), se verront appliquer une étiquette supplémentaire qui contient l'identifiant du VLAN (en **noir** sur la trame).

Historiquement, Cisco avait créé son propre protocole de Trunk entre ses switchs, nommé **ISL – Inter-Switch Link**. Mais très rapidement, cette fonctionnalité plus qu'essentielle, demanda une interopérabilité avec d'autres constructeurs.

La norme **Trunk 802.1Q** fut sortie et Cisco l'implémenta aussi dans ses switchs. D'où la possibilité sur certains switchs Cisco de décider quel trunk on souhaite faire, ISL ou 802.1Q.

A retenir pour le CCNA, le tableau suivant :

ISL Inter Switch Link	802.1Q
Propriétaire	Normalisé
Encapsulation	Tag
Indépendant du niveau 2	Dépend du protocole Ethernet
Encapsule l'ancienne trame dans une nouvelle	Ajoute un champ dans l'entête de la trame initiale

Trunk ISL

Le trunk propriétaire Cisco ISL a la particularité **d'encapsuler toute la trame** de l'utilisateur dans une nouvelle trame, nommée trame ISL. Voici à quoi ressemble une trame ISL:

Entête ISL 26 octets	Trame Ethernet Utilisateur 0 – 1500 octets	FCS 4 octets
---------------------------------------	-------------------------------------------------------------	-------------------------------

Remarque: comme cette trame a un format particulier, il est obligatoire que le switch d'en face puisse comprendre ce formatage. Il faut donc configurer le port du switch d'en face en trunk ISL.

Voici ci dessous la configuration à effectuer sur les ports des switchs interconnectés entre eux:

```
Switch(config)# interface fastethernet 0/0
Switch(config-if)# shutdown
Switch(config-if)# switchport trunk encapsulation isl
Switch(config-if)# switchport mode trunk
Switch(config-if)# no shutdown
```

Vérifions que le port en question est bien configuré:

```
Switch# show interfaces fastethernet 0/0 trunk

  Port      Mode       Encapsulation  Status      Native VLAN
  Fa0/0    trunk      isl           trunking   1

  Port      VLANs allowed on trunk
  Fa0/0    1,1002-1005

  Port      VLANs allowed and active in management domain
  Fa0/0    1,1002-1005

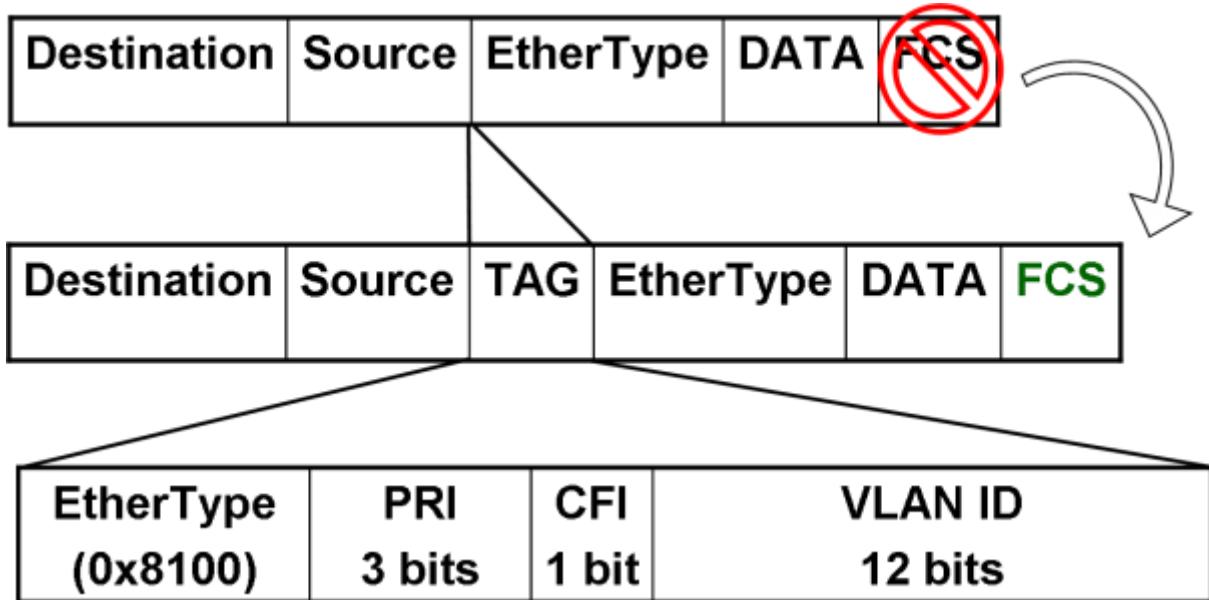
  Port      VLANs in spanning tree forwarding state and not pruned
  Fa0/0    1,1002-1005
```

Avec cette commande, on peut vérifier que le port Fa0/0 est bien en mode **Trunk ISL** via le status **trunking**.

Pour information, la colonne **native VLAN** permet de mettre dans le VLAN 1 une trame qui arriverait non encapsulée ISL sur ce port (on en reparle un peu plus loin).

Trunk 802.1Q

Le trunk normalisé **802.1Q** n'encapsule pas toute la trame de l'utilisateur comme ISL mais casse la trame et y **insère** une étiquette ou tag, nommée **TAG 802.1Q**. Voici à quoi ressemble une trame utilisateur avec le rajout du **TAG 802.1Q**:



La première trame est celle de l'utilisateur qui arrive sur le switch. Dès que cette trame sort vers un port configuré en Trunk 802.1Q, le switch insère l'étiquette TAG (trame n°2 dans le schéma).

En inspectant le contenu de ce TAG, on remarque les champs suivants (trame n°3 dans le schéma):

- EtherType**: permet de préciser que c'est une trame 802.1Q, la valeur en hexa est **0x8100**
- PRI**: champs de priorité sur 3 bits qui permet de classifier le trafic utilisateur pour lui appliquer de la qualité de service (voix, vidéo...). Ce champ est aussi appelé **802.1P** ou **COS – Class Of Service**.
- CFI – Canonical Format Identifier**: permet la compatibilité d'un réseau Ethernet avec un réseau TokenRing. Champ à oublier pour le CCNA car il n'existe quasiment plus du réseau TokenRing aujourd'hui.
- VLAN ID – VLAN Identifier**: codé sur 12bits: valeur numérique du VLAN auquel la trame utilisateur appartient. **C'est le champ le plus important à connaître!**

Voici ci dessous la configuration à effectuer sur les ports des switchs interconnectés entre eux:

```

Switch(config)# interface fastethernet 0/1
Switch(config-if)# shutdown
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no shutdown

```

On peut remarquer qu'il n'y a qu'une seule variable qui change par rapport à une configuration Trunk ISL (la variable **dot1q** en rouge).

Vérifions que le port en question est bien configuré:

```

Switch# show interfaces fastethernet 0/0 trunk
      Port        Mode       Encapsulation  Status        Native VLAN
      Fa0/0      trunk      dot1q          trunking     1

```

Port	VLANs allowed on trunk
Fa0/0	1,1002-1005
Port	VLANs allowed and active in management domain
Fa0/0	1,1002-1005
Port	VLANs in spanning tree forwarding state and not pruned
Fa0/0	1,1002-1005

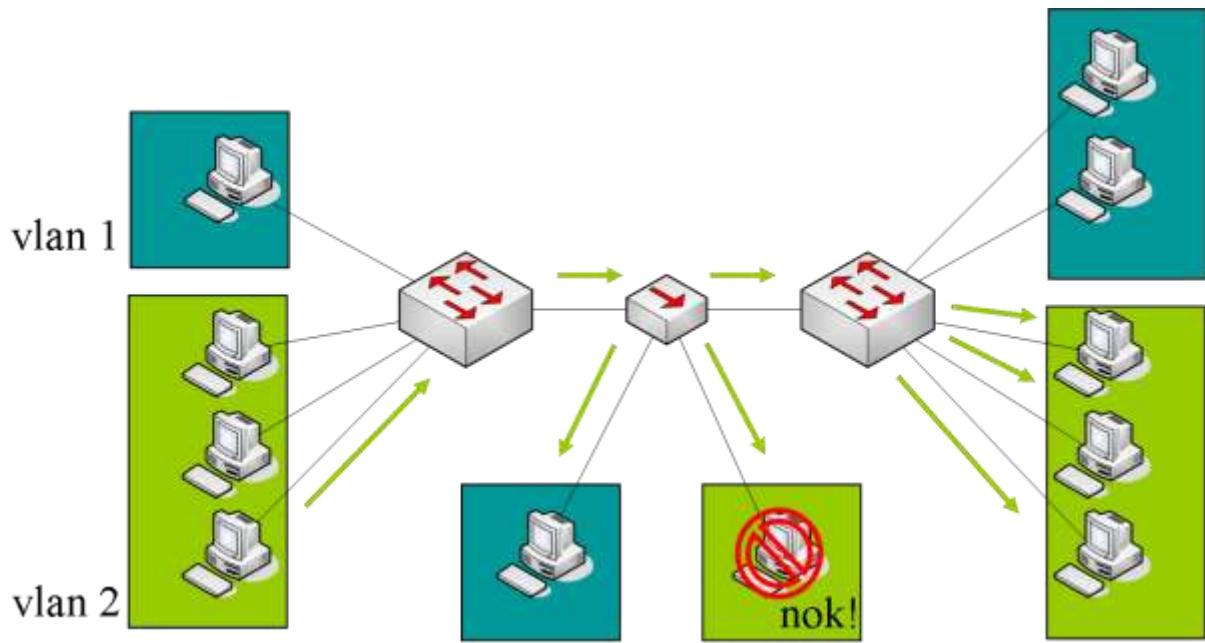
Avec cette commande, on peut vérifier que le port Fa0/0 est bien en mode Trunk **802.1Q** avec le status **trunking** et l'encapsulation **dot1q**.

Important – VLAN natif

La particularité du Trunk 802.1Q vient du fait que **pour un VLAN en particulier**, le Trunk **ne casse pas** la trame de l'utilisateur et donc **ne lui rajoute pas le TAG**. Le trunk laisse la trame transiter sans aucun changement.

Pourquoi?

Il faut revenir sur l'historique des réseaux: jadis (sic!) on pouvait se trouver dans le cas où des PC connectés à un HUB était lui même connecté à 2 switchs. On se trouvait alors dans le schéma suivant:



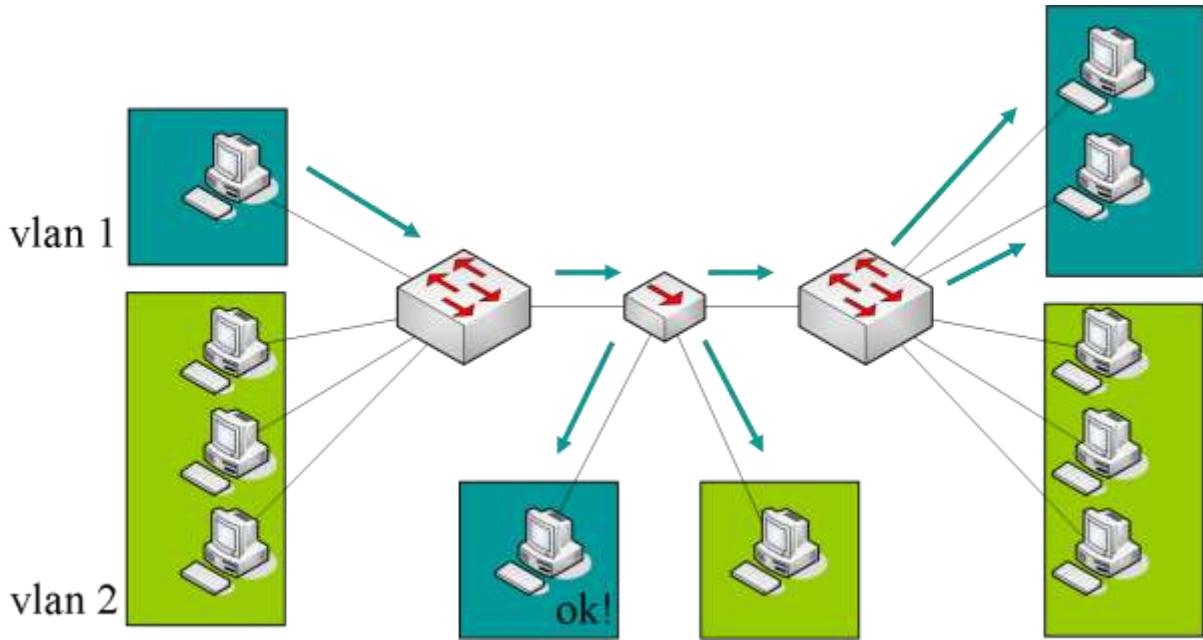
Prenons le cas où les PC dans le VLAN 2 souhaitent communiquer:

1. un PC de gauche envoi du trafic;
2. le switch de gauche **ajoute** le TAG VLAN=2 dans la trame et envoi la trame au HUB;
3. le HUB diffuse la trame taguée sur tous ses ports;
4. le switch de droite reçoit la **trame taguée, enlève le TAG** et commute la trame vers les ports appartenant au même VLAN (2 ici);
5. le PC du bas reçoit une **trame taguée!** Comme le PC ne sait pas lire le TAG, il rejette la trame.

On voit ici que le PC du bas ne pourra jamais recevoir de trame provenant d'autres PC qui appartiennent au même VLAN que lui.

Donc dans la norme 802.1Q, il a été défini que pour un VLAN en particulier, appelé **VLAN natif**, les switchs laisseraient passer la trame initiale sans ajouter de TAG.

Regardons maintenant le même comportement avec un PC appartenant au VLAN n°1, configuré comme VLAN natif:



Reprendons le cas où les PC souhaitent communiquer mais cette fois ci ils appartiennent au VLAN natif 1:

1. un PC de gauche envoi du trafic;
2. le switch de gauche **n'ajoute pas** le TAG VLAN=1 dans la trame et envoi la trame au HUB;
3. le HUB diffuse la **trame non taguée** sur tous ses ports;
4. le switch de droite reçoit la **trame non taguée**, donc sait qu'elle appartient au VLAN natif (1 ici) et commute la trame vers les ports appartenant au même VLAN;
5. le PC du bas reçoit une **trame non taguée** donc la traite comme toute trame classique.

On voit ici que le PC du bas peut communiquer sans aucun souci avec d'autres PC qui appartiennent au même VLAN que lui.

A retenir pour le CCNA

Donc, parmis les choses à savoir pour l'examen CCNA, essayez de retenir les informations suivantes:

- Trunk propriétaire → ISL de Cisco avec une **encapsulation complète** de la trame
- Trunk normalisé → 802.1Q avec un **ajout de TAG** dans la trame
- **par défaut**, le VLAN natif est le VLAN 1 (attention à ne pas confondre VLAN natif et VLAN par défaut!)
- dans une configuration 802.1Q, le VLAN natif **doit être identique des deux côtés**

Remarque hors CCNA: la notion de Trunk chez d'autres constructeurs est différente: c'est la capacité d'agrégier plusieurs liens physiques entre 2 switchs pour en faire qu'un seul virtuel. On active alors les protocoles PAGP ou LACP. Donc il faut faire attention quand vous parlez à des techniciens à propos du Trunk, certaines personnes ne comprendront pas car vous parlerez de 2 notions différentes.