Réseaux informati

Nouvelle édition en français

Cisco CCNA

Guide de préparation à l'examen de certification CCNA 200-301

Volume 3

Technologies Ethernet et Wi-Fi

Cisco CCNA 200-301 Volume 3

Guide de préparation au Cisco CCNA 200-301 en français, Volume 3 Technologies Ethernet et Wi-Fi

François-Emmanuel Goffinet

Ce livre est en vente à http://leanpub.com/cisco-ccna-3

Version publiée le 2021-09-19

Aussi par François-Emmanuel Goffinet

Cisco CCNA 200-301 Volume 1

Cisco CCNA 200-301 Volume 2

Cisco CCNA 200-301 Volume 4

Linux Administration Volume 1

Linux Administration Volume 2

Linux Administration Volume 3

Linux Administration Volume 4

Protocole SIP

Table des matières

Avertissement

Le projet lié à cet ouvrage est conçu principalement pour des candidats francophones à l'examen de certification Cisco CCNA 200-301.

Le document sera probablement utile comme *support de formation* dans d'autres contextes tels que celui de l'autoapprentissage, de l'enseignement ou de la formation professionnelle.

Si le document peut sans doute contribuer à mieux connaître les réseaux d'entreprise dans la perspective du CCNA, il ne peut aucunement garantir la réussite de l'examen. Aussi, ce projet n'a jamais poursuivi l'ambition de remplacer d'autres sources d'information/formation issues des canaux officiels tels que *Cisco Press*, *Cisco Learning Network*, les *Cisco Systems Learning Partners*, *Cisco Academy* ou encore la documentation officielle du fabricant. D'ailleurs l'auteur est totalement indépendant de tout fabricant cité. Celles-ci, toutes mieux présentées les unes que les autres, ne manquent pas au contraire, mais il est rare de trouver des sources de qualité et fiables en français.

Copyrights

Dédicace

À mes parents qui m'ont toujours apporté un soutien sans faille dans tous mes projets.

Remerciements

Merci aux milliers de visiteurs quotidiens du site cisco.goffinet.org.

Merci aux centres de formation et aux écoles qui m'accordent leur confiance et qui me permettent de rencontrer mon public en personne.

Merci à Wendell Odom, mon mentor sur le sujet Cisco CCNA. N'hésitez pas à vous procurer ses livres en anglais chez Cisco Press.

Merci à Stéphane Bortzmeyer dont la prose prolifique m'inspire et m'aide à vulgariser les technologies de l'Internet.

Merci enfin à Cisco Systems d'être aussi ouvert depuis tant d'années dans sa documentation et pour son effort à rendre les technologies des réseaux plus accessibles, mieux comprises et plus populaires.

Avant-Propos

François-Emmanuel Goffinet est formateur IT et enseignant depuis 2002 en Belgique et en France. Outre Cisco CCNA, il couvre de nombreux domaines des infrastructures informatiques, du réseau à la virtualisation des systèmes, du nuage à la programmation d'infrastructures hétérogènes en ce y compris DevOps, Docker, K8s, chez AWS, GCP ou Azure, etc. avec une forte préférence et un profond respect pour l'Open Source, notamment pour Linux.

On trouvera ici un des résultats d'un projet d'autopublication en mode *agile* plus large lié au site web cisco.goffinet.org. La documentation devrait évoluer dans un format vidéo. Les sujets développés devraient trouver des questionnaires de validation de connaissances. Enfin, une solution accessible et abordable de simulation d'exercices pratiques mériterait réflexion.

Cisco CCNA 200-301

L'examen Cisco CCNA 200-301[1] est disponible en anglais uniquement. Il se déroule sous surveillance dans un centre de test VUE après une inscription sur leur site vue.com et un paiement (de maximum 300 EUR) avec un bon de réduction (*voucher*) ou par carte de crédit.

Cet examen de niveau fondamental sur la théorie des réseaux évalue votre niveau avec un examen sur ordinateur en anglais constitué d'une centaine de questions théoriques et pratiques. Cet examen a une durée de 120 minutes. Il est interdit de revenir sur une question à laquelle on a déjà répondu. Le seuil de réussite est fixé entre 82,5% et 85%. Tout diplômé d'un premier cycle de l'enseignement supérieur en informatique devrait être en mesure de réussir cet examen dans un délai de trois mois. Tout qui voudrait entrer dans une carrière dans les réseaux ne perd pas son temps en passant cet examen. Certains prétendent même que c'est fortement recommandé.

Sujets et objectifs de l'examen Cisco CCNA 200-301

On trouve 53 objectifs dans six sujets[2] : Fondamentaux des Réseaux (20%), Accès au Réseau (20%), Connectivité IP (25%), Services IP (10%), Sécurité de base (15%), Automation et Programmabilité (10%).

On trouve aussi dix verbes dans les objectifs de la certification CCNA 200-301 qui correspondent à certaines compétences à valider :

1. "Expliquer" (6)
2. "Décrire" (15)
3. "Comparer" (6)
4. "Identifier" (1)
5. "Reconnaître" (1)
6. "Interpréter" (2)
7. "Déterminer" (1)
8. "Définir" (1)
9. "Configurer" (17)
10. "Vérifier" (1)

On peut considérer que seuls les objectifs qui demandent à "Configurer" et à "Vérifier" seraient purement pratiques. Toutefois, "Identifier", "Interpréter" et "Déterminer" pourraient aussi trouver leur application opérationnelle. Les autres objectifs comme "Expliquer", "Décrire", "Définir", "Reconnaître" seraient validés par des questions d'examen plus théoriques.

Les objectifs développés dans ce volume sont indiqués en gras.

1. La page officielle de la certification se trouve à cette adresse.
2. La page officielle des sujets et des objectifs du Cisco CCNA 200-301 se trouve à cette adresse.

1.0 Fondamentaux des Réseaux - 20%

- 1.1 Expliquer le rôle et la fonction des composants réseau
  - 1.1.a Routeurs
  - 1.1.b Commutateurs (switches) L2 et L3
  - 1.1.c Pare-feu NG (Next-generation firewalls) et IPS
  - 1.1.d Point d'accès (Access points)
  - 1.1.e Controlleurs (Cisco DNA Center et WLC)
  - 1.1.f Points terminaux (Endpoints)
  - 1.1.g Serveurs
- 1.2 Décrire les caractéristiques des architectures et topologies réseau
  - 1.2.a 2 tier
  - 1.2.b 3 tier
  - 1.2.c Spine-leaf
  - 1.2.d WAN
  - 1.2.e Small office/home office (SOHO)
  - 1.2.f On-premises et cloud
- 1.3 Comparer les interfaces physiques et les types de câble
  - 1.3.a Fibre monmode (Single-mode) et fibre multimode, cuivre
  - 1.3.b Connexions (Ethernet shared media et point-to-point)
  - 1.3.c Concepts sur PoE
- 1.4 Identifier les problèmes d'interface et de câbles (collisions, errors, mismatch duplex, et/ou speed)
- 1.5 Comparer TCP à UDP
- 1.6 Configurer et vérifier l'adressage et le sous-réseautage (subnetting) IPv4
- 1.7 Décrire la nécessité d'un adressage IPv4 privé
- 1.8 Configurer et vérifier l'adressage et les préfixes IPv6
- 1.9 Comparer les types d'adresses IPv6
  - 1.9.a Global unicast
  - 1.9.b Unique local
  - 1.9.c Link local
  - 1.9.d Anycast
  - 1.9.e Multicast
  - 1.9.f Modified EUI 64
- 1.10 Vérifier les paramètres IP des OS clients (Windows, Mac OS, Linux)
- 1.11 Décrire les principes des réseaux sans-fil
  - 1.11.a Nonoverlapping Wi-Fi channels
  - 1.11.b SSID
  - 1.11.c RF
  - 1.11.d Encryption
- 1.12 Expliquer les fondamentaux de la virtualisation (virtual machines)
- 1.13 Décrire les concepts de la commutation (switching)
  - 1.13.a MAC learning et aging
  - 1.13.b Frame switching
  - 1.13.c Frame flooding
  - 1.13.d MAC address table

2.0 Accès au Réseau - 20%

- 2.1 Configurer et vérifier les VLANs (normal range) couvrant plusieurs switches
  - 2.1.a Access ports (data et voice)
  - 2.1.b Default VLAN
  - 2.1.c Connectivity
- 2.2 Configurer et vérifier la connectivité interswitch
  - 2.2.a Trunk ports
  - 2.2.b 802.1Q
  - 2.2.c Native VLAN
- 2.3 Configurer et vérifier les protocoles de découverte Layer 2 (Cisco Discovery Protocol et LLDP)
- 2.4 Configurer et vérifier (Layer 2/Layer 3) EtherChannel (LACP)
- 2.5 Décrire la nécessité et les operations de base de Rapid PVST+ Spanning Tree Protocol
  - 2.5.a Root port, root bridge (primary/secondary), et les autres noms de port
  - 2.5.b Port states (forwarding/blocking)
  - 2.5.c Avantages PortFast
- 2.6 Comparer les architectures Cisco Wireless Architectures et les modes des APs
- 2.7 Décrire les connexions physiques d'infrastructure des composants WLAN (AP,WLC, access/trunk ports, et LAG)
- 2.8 Décrire les connexions des accès de gestion des APs et du WLC (Telnet, SSH, HTTP,HTTPS, console, et TACACS+/RADIUS)
- 2.9 Configurer les composants d'un accès au LAN sans-fil pour la connectivité d'un client en utilisant un GUI seulement pour la création du WLAN, les paramètres de sécurité, les profiles QoS et des paramètres WLAN avancés

3.0 Connectivité IP - 25%

- 3.1 Interpréter les composants d'une table de routage
  - 3.1.a Routing protocol code
  - 3.1.b Prefix
  - 3.1.c Network mask
  - 3.1.d Next hop
  - 3.1.e Administrative distance
  - 3.1.f Metric
  - 3.1.g Gateway of last resort
- 3.2 Déterminer comment un routeur prend une décision de transfert par défaut
  - 3.2.a Longest match
  - 3.2.b Administrative distance
  - 3.2.c Routing protocol metric
- 3.3 Configurer et vérifier le routage statique IPv4 et IPv6
  - 3.3.a Default route
  - 3.3.b Network route

  - 3.3.c Host route
  - 3.3.d Floating static

- 3.4 Configurer et vérifier single area OSPFv2
  - 3.4.a Neighbor adjacencies
  - 3.4.b Point-to-point
  - 3.4.c Broadcast (DR/BDR selection)
  - 3.4.d Router ID

- 3.5 Décrire le but des protocoles de redondance du premier saut (first hop redundancy protocol)

4.0 Services IP - 10%

- 4.1 Configurer et vérifier inside source NAT (static et pools)
- 4.2 Configurer et vérifier NTP dans le mode client et le mode server
- 4.3 Expliquer le rôle de DHCP et de DNS au sein du réseau
- 4.4 Expliquer la fonction de SNMP dans les opérations réseau
- 4.5 Décrire l'utilisation des fonctionnalités de syslog features en ce inclus les facilities et niveaux
- 4.6 Configurer et vérifier DHCP client et relay
- 4.7 Expliquer le forwarding per-hop behavior (PHB) pour QoS comme classification, marking, queuing, congestion, policing, shaping
- 4.8 Configurer les périphériques pour un accès distant avec SSH
- 4.9 Décrire les capacités la fonction de TFTP/FTP dans un réseau

5.0 Sécurité de base - 15%

- 5.1 Définir les concepts clé de la sécurité (menaces, vulnerabilités, exploits, et les techniques d'atténuation)
- 5.2 Décrire les éléments des programmes de sécurité (sensibilisation des utilisateurs, formation, le contrôle d'accès physique)
- 5.3 Configurer l'accès aux périphériques avec des mots de passe
- 5.4 Décrire les éléments des politiques de sécurité comme la gestion, la complexité, et les alternatives aux mots de passe (authentications multifacteur, par certificats, et biométriques)
- 5.5 Décrire les VPNs remote access et site-to-site
- 5.6 Configurer et vérifier les access control lists
- 5.7 Configurer les fonctionnalités de sécurité Layer 2 (DHCP snooping, dynamic ARP inspection, et port security)
- 5.8 Distinguer les concepts authentication, authorization, et accounting
- 5.9 Décrire les protocoles de sécurité sans-fil (WPA, WPA2, et WPA3)
- 5.10 Configurer un WLAN en utilisant WPA2 PSK avec un GUI

6.0 Automation et Programmabilité - 10%

- 6.1 Expliquer comment l'automation impacte la gestion du réseau
- 6.2 Comparer les réseaux traditionnels avec le réseau basé contrôleur (controller-based)
- 6.3 Décrire les architectures basées contrôleur (controller-based) et software defined (overlay, underlay, et fabric)
  - 6.3.a Séparation du control plane et du data plane
  - 6.3.b APIs North-bound et south-bound
- 6.4 Comparer la gestion traditionnelle les périphériques campus avec une gestion des périphériques avec Cisco DNA Center
- 6.5 Décrire les caractéristiques des APIs de type REST (CRUD, verbes HTTP, et encodage des données)
- 6.6 Reconnaître les capacités des mécanismes de gestion des configuration comme Puppet, Chef, et Ansible
- 6.7 Interpréter des données encodées en JSON

Introduction

Ce troisième volume du guide de préparation à la certification Cisco CCNA 200-301 porte principalement sur les technologies Ethernet et Wi-Fi. Il complète le propos de l'examen sur des sujets comme les commutateurs Ethernet, les VLANs, le Trunking, Etherchannel, Rapid Spanning-Tree, HSRP, les technologies sans fil (WLAN). L'ouvrage couvre un seul sujet essentiel de la certification CCNA : Accès au Réseau.

Ce volume peut occuper une activité intellectuelle de 16 à 35 heures, voir plus.

L'objectif opérationnel est de concevoir une architecture réseau fiable.

Dans une première partie, on étudiera le protocole d'accès LAN Ethernet, son câblage, son format de trames. On présentera les principes de la commutation Ethernet et les architectures LAN. Enfin, on apprendra à configurer un commutateur Cisco et à comprendre la notion d'interfaces.

La seconde partie est consacrée aux technologies VLANs (IEEE 802.1q) dans leur implémentation Cisco Systems (VTP et DTP) avec "Trunking" et du routage inter-VLANs. Ces chapitres complètent une première topologie d'entreprise avec la virtualisation du réseau local.

Les deux parties suivantes exposent les protocoles LAN qui visent à assurer la disponibilité du réseau dans des architectures traditionnelles. La troisième partie expose les principes fondamentaux des protocoles Spanning-Tree et Rapid Spanning-Tree au niveau de la couche 2 (L2) et ainsi que ceux du protocole de couche physique (L1) Etherchannel qui permet d'agréger les liaisons sur le plan logique. La quatrième partie tente de répondre à la question de la robustesse des liaisons au sein des réseaux locaux au niveau des passerelles par défaut avec HSRP, au niveau de la couche 2 (L2) avec Spanning-Tree, au niveau de la couche physique (L1) avec Etherchannel et au niveau de la couche 3 (L3) avec le routage (statique) IPv4 et IPv6. Il reprend des principes d'architecture hiérarchique et modulaire des réseaux.

La cinquième et dernière partie porte sur les technologies Wireless LAN (WLAN) des réseaux sans-fil locaux, dont fait partie ce qu'on appelle le Wi-Fi. On y trouvera un exposé de présentation générale du domaine, des informations sur les aspects normatifs (IEEE 802.11), sur les topologies logiques et les modèles de déploiement, sur les aspects physiques (bande de fréquence, non-overlapping, antennes), sur les aspects de configuration des clients, sur les aspects de sécurité WPA, et enfin sur les aspects de gestion au sein d'un réseau local.

Première partie Commutation Ethernet

La technologie Ethernet (IEEE 802.3) est la technologie de réseau local (LAN) par excellence pour connecter les stations de travail au sein des organisations mais aussi les ressources des centres de données (*data centers*). Mais la technologie Ethernet est aujourd'hui de plus en plus proposée comme mode de transport sur de la fibre optique dans le déploiement de la boucle locale haut-débit. Comme technologie filaire LAN/MAN du groupe IEEE 802, elle pourrait être comparées aux technologies IEEE 802.11 (Wi-Fi) ou Bluethooth.

Le succès de la technologie Ethernet tient à une adoption large du marché, une inter-opérabilité éprouvée entre les versions du protocole et entre les constructeurs. Mais elle s'explique aussi avec le retour sur investissement sur l'infrastructure physique, avec le choix des supports cuivre ou fibre optique, avec des vitesses qui décuplent à chaque version, avec le support du matériel (switches) et celui des protocoles IEEE 802.1 pour assurer des services de commutation performants.

Le rôle du commutateur a optimisé la méthode d'accès au support Ethernet sans toucher au principe du transport du protocole. En bref, alors qu'Ethernet est une technologie a support partagé, le commutateur distribue la connectivité en dédiant les connexions de poste à poste et en les "multiplexant". Dans les cadre des organisations à partir d'une certaine taille, les architectures constituées de commutateurs (*switches*) doivent être construites de manière systématique en respectant un modèle de conception pour assurer sa robustesse, sa résilience et un niveau de service à 100 % de disponibilité. On a alors l'habitude de placer ce matériel dans des couches de conception : *Access*, *Distribution* et *Core* .

Aussi, on apprendra dans cette partie à configurer un commutateur Cisco de manière basique.

1. Technologie Ethernet

La technologie Ethernet dispose de ses propres caractéristiques en matière de câblage, de normes, de formats de trame et de méthode d'accès. Aussi avec PoE, Ethernet est capable d'alimenter les périphériques. Enfin, on fournira dans ce chapitre la méthode de diagnostic de couche 1 (L1) concernant les câbles utilisés en technologie Ethernet avec un périphérique Cisco.

1. Supports de transmission et protocoles LAN

1.1. Câblage et environnements bruités

Le câble cuivre ou en fibre optique et l'air transportent les données transmises. Mais ces supports exigent une connectique et un placement correct sans quoi le signal risque de se dégrader.

Tous les supports peuvent connaître des sources de bruit qui dégradent le signal.

Les supports ont aussi leurs caractéristiques en vitesse et en portée.

1.2. Cuivre

Les supports en cuivre comme la paire torsadée ou le câble coaxial sont sensibles aux interférences électromagnétiques : ascenseurs, néons, engins de puissance, etc. peuvent engendrer des interférences sur les câbles de données proches.

La longueur d'un segment physique d'un câble à paires torsadées est limitée à quelques dizaines de mètres voire quelques centaines de mètres dans certains formats, mais avec des pertes assez fortes qui nécessitent la répétition du signal.

Les supports en cuivre sont relativement bon marché, populaires, faciles à déployer.

1.3. Fibre optique

La fibre optique est insensible aux interférences électromagnétiques et convient aux environnements industriels fortement bruités. Mais la fibre optique peut connaître des interférences dues à un mauvais placement du câble en fibre optique, une soudure mal réalisée, des connecteurs défectueux, etc.

Avec la fibre optique, il n'y a pas de limite théorique sur la distance (plusieurs Km) et sur la vitesse (plusieurs Gb/s).

En soi, la fibre optique n'est pas coûteuse. Par contre, le matériel de connexion et de déploiement est certainement plus coûteux (en compétences, en argent).

1.4. Air

L'air a l'avantage de permettre des connexions au réseau de manière non mécanique. On parle alors de technologies "sans fil".

Toutefois, c'est un environnement fortement bruité qui peut être corrigé par :

- des mécanismes de fiabilité protocolaires (réservation de ressources, accusés de réception, reprise sur erreur, etc.)
- des mécanismes physiques comme MIMO.
- Leur portée dépend du type d'onde et de la puissance d'émission.

1.5. Protocoles IEEE 802

Les thèmes d'étude du groupe de travail IEEE 802 sont (dans l'ordre où le groupe de normalisation les énumère) :

- IEEE 802.1 : Gestion des réseaux locaux, VLAN, authentification, etc.
- IEEE 802.2 : Distinction entre couche Logical Link Control (LLC) et Media Access Control (MAC)
- IEEE 802.3 : Couche média CSMA/CD Ethernet
- IEEE 802.4 : Couche média CSMA/CA Token Bus et AppleTalk (utilisée en informatique industrielle) (dissous)
- IEEE 802.5 : Couche média Token Ring (IBM)
- IEEE 802.6 : Groupe de conseils sur les réseaux à grande distance (Réseau métropolitain ou MAN) (dissous)
- IEEE 802.7 : Groupe de conseils sur les réseaux à large bande (dissous)
- IEEE 802.8 : Groupe de conseils sur les réseaux sur fibre optique (dissous)
- IEEE 802.9 : Réseaux à intégration de services comme RNIS (dissous)
- IEEE 802.10 : Interopérabilité de la sécurité des LAN/MAN (dissous)
- IEEE 802.11 : Réseaux sans fil : réseau sans fil, Wi-Fi
- IEEE 802.12 : Réseaux locaux utilisant le mécanisme de demande de priorité
- IEEE 802.13 : Inutilisé (À l'origine réseaux Mapway (dissous))
- IEEE 802.14 : Réseaux et modems câble (dissous)
- IEEE 802.15 : Réseaux privés sans fil (WPAN) comme le Bluetooth
- IEEE 802.16 : Réseaux sans fil à large bande par exemple le WiMAX
- IEEE 802.17 : Réseaux de fibres optiques en anneau (Resilient Packet Ring)
- IEEE 802.18 : Groupe de conseils pour la normalisation des communications radioélectriques
- IEEE 802.19 : Groupe de conseils sur la cohabitation avec les autres standards
- IEEE 802.20 : Accès sans fil à bande large
- IEEE 802.21 : Transfert automatique des liaisons indépendamment du média
- IEEE 802.22 : Réseaux régionaux sans fil

Source : https ://fr.wikipedia.org/wiki/IEEE_802.

2. Technologie Ethernet

Ethernet est actuellement la technologie filaire LAN L2 dominante. Son succès s'explique notamment par divers facteurs tels que :

- Diversité des supports : **Cuivre** (paire torsadée) et **Fibre** ;

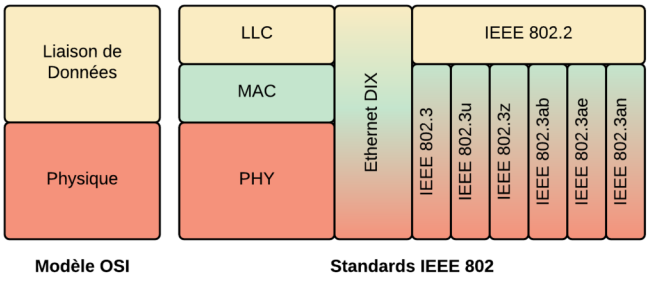
- Interopérabilité (vers IP, vers les protocoles IEEE 802) ;
- Stabilité des infrastructures (supports) / Évolutivité de la technologie (services) ;
- Bon marché ;
- Facilité de déploiement ;
- Fiabilité assurée par l'infrastructure et par la commutation.

Nom commercial	Ethernet
Portée	**Locale (LAN)**
Norme	IEEE 802.3
Supports	**paire torsadée ou fibre optique**

2.1. Ethernet dans les modèles de communication

Du point de vue du modèle TCP/IP, Ethernet remplit la couche "Accès au Réseau". Dans le modèle OSI, Ethernet couvre les couches "Liaison de données" (L2) et "Physique" (L1).

Les trames IEEE 802.3 utilisent le protocole "Logical Link Control" (LLC) pour embarquer des protocoles de couches supérieures.



OSI et standards IEEE 802

Les caractéristiques de la technologie Ethernet sont les suivantes :

- 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)

2.2. Versions de la technologie Ethernet

On trouvera ici le nom commercial, la vitesse théorique, la dénomination physique, le standard IEEE et des caractéristiques physiques sommaires des technologies Ethernet les plus courantes.

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	1 Gbps	1000BASE-SX, 1000BASE-LX	IEEE 802.3z	Fibre, 550 m, <5 Km
Gigabit Ethernet	1 Gbps	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
40Gigabit Ethernet	40 Gbps	40GBASE-SR, 40GBASE-LR	IEEE 802.3ba	Fibre, 125 m, <10 Km
100Gigabit Ethernet	100 Gbps	100GBASE-SR, 100GBASE-LR	IEEE 802.3ba	Fibre, 125 m, <10 Km

Avec Ethernet, un câble à paires torsadées est toujours déployé sur un segment physique de maximum 100 mètres, quel que soit sa catégorie ou son blindage. Au-delà de cette distance, la gestion des collisions (qui sont intrinsèques à la technologie) ne sera plus gérée de manière correcte.

En fibre optique, selon sa catégorie, on trouvera plusieurs options en support de longueurs et en vitesse qui ne sont pas détaillées ici.

2.3. Autonégociation

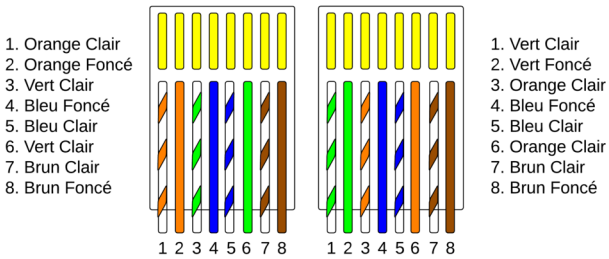
Les vitesses Ethernet et les modes half-duplex / Full Duplex sont autonégiociés par les interfaces des cartes réseau et des commutateurs avec des impulsions électriques qui définissent un mode commun. Il est conseillé de laisser les interfaces autonégocier la vitesse et le mode.

Par exemple sur un commutateur Cisco :

```
Switch(config-if)#speed ?
  10    Force 10 Mbps operation
  100   Force 100 Mbps operation
  1000  Force 1000 Mbps operation
  auto  Enable AUTO speed configuration
```

3. Câble à paire torsadée

3.1. Norme EIA 568A/568B



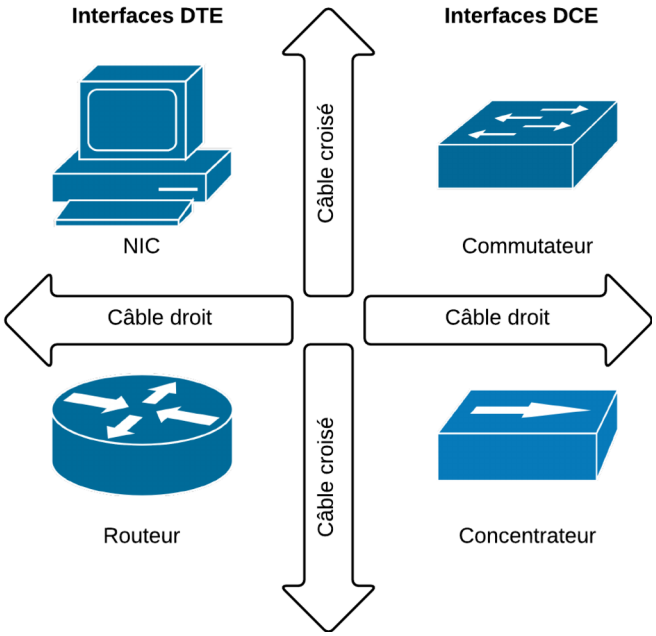
Norme EIA 568A/568B

On utilise ce câble en catégories récentes avec une prise modulaire RJ45 (8P8C). Les schémas de brochage répondent aux normes de câblage structuré T568A et T568B.

3.2. Câbles droits et câbles croisé

Les commutateurs (switches) et concentrateurs (hubs) sont identifiés comme étant des DCE (Data Connexion Equipement) alors que les stations terminales et les routeurs sont des périphériques DTE (Data Terminal Equipment). Les équipements identiques DTE/DTE ou DCE/DCE se connectent avec un câble croisé (qui croise les paires d'émission et de réception). Les équipements de type différents se connectent avec un câble droit car la position émission/réception sur leurs interfaces est déjà inversée.

- Câble droit (*straight*)
- Câble croisé (*cross-over*)



Câble droit/câble croisé

Outre le fait que les nouvelles gammes de matériel actif s'adaptent automatiquement aux câbles en reconnaissant les positions du signal, on utilisera soit du câble croisé ou droit selon le type de matériel que l'on connecte. Cette fonctionnalité s'appelle "Auto-MDIX".

Câbles droits

- PC à Hub
- PC à Switch
- Switch à Routeur

Câbles croisés

- Switch à Switch
- Hub à Hub
- Routeur à Routeur
- PC à PC
- Hub à Switch
- PC à Routeur

3.3. Règles d'or du câblage à paire torsadée

Respecter les règles du câblage structuré pour le câblage horizontal sur des connexions T568A/T568B est élémentaire :

- 6 mètres de la station terminale à la prise murale.
- 90 mètres en câblage horizontal jusqu'au panneau de brassage.
- 3 mètres jusqu'au commutateur.
- éloigner le câble de tout élément de puissance.

Aussi, on aura une préférence pour les câbles préfabriqués et certifiés sans blindage, des choix de couleurs, des solutions d'étiquetage, etc.

3.4. Câbles inversés

- Câble inversé (*roll-over*), console

3.5. Types de blindage et catégorie de câbles à paires torsadées

Les câbles à paires torsadées peuvent disposer de différents types de blindages et sont organisés en catégories en fonction des versions d'Ethernet à supporter[1]. On conseille toujours de prendre la catégorie courante voire la dernière selon son budget. Quoi qu'il en soit, les bonnes pratiques de câblage sont en dehors des objectifs vérifiés par le CCNA.

Les types de blindages

- Paire torsadée non blindée
- Paire torsadée écrantée
- Paire torsadée blindée
- Paire torsadée écrantée et blindée
- Paire torsadée super blindée

Les catégories de câbles

- Catégorie 5
- Catégorie 5e / classe D
- Catégorie 6 / classe E
- Catégorie 6a / classe Ea
- Catégorie 7a / classe Fa
- Catégorie 8

4. Fibre optique

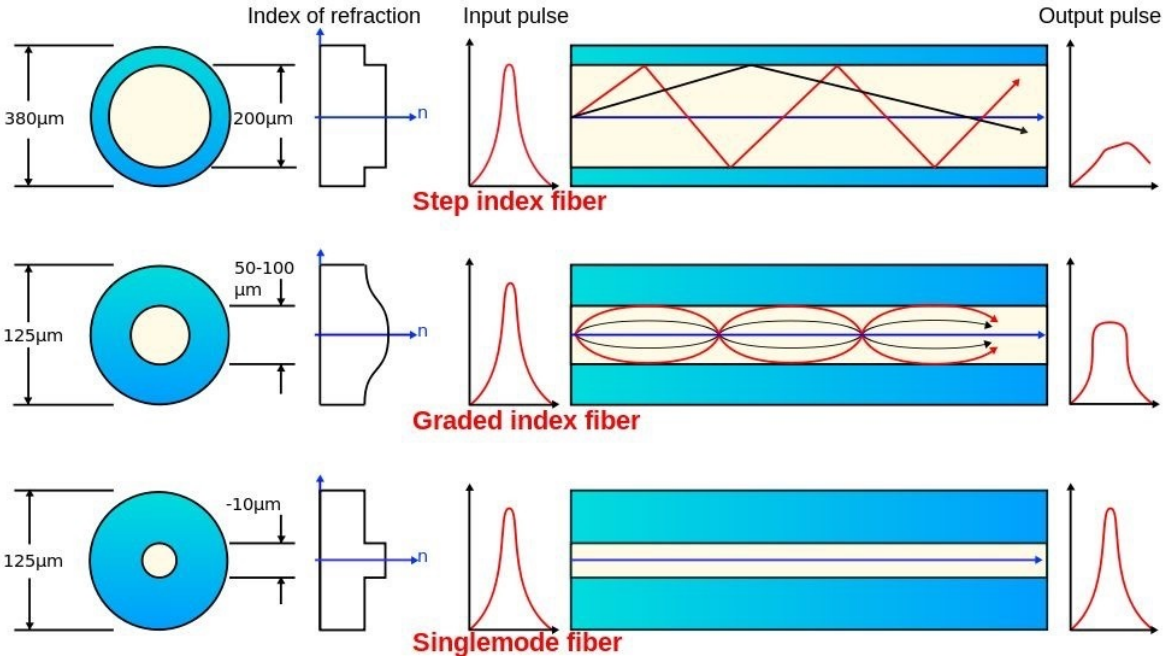
4.1. La fibre optique multimode

Les rayons lumineux peuvent suivre des trajets différents suivant l'angle de réfraction. Les rayons peuvent donc arriver au bout de la ligne à des instants différents, d'une certaine dispersion du signal. Elles sont généralement utilisées pour de courtes distances, elles ont pour émetteur une diode électroluminescente et des performances d'environ 1 gigabit/Km. La fibre optique multimode est généralement utilisée pour de courtes distances (de l'ordre de la centaine de mètres). Elle est la plus employée pour les réseaux privés.

1. https ://en.wikipedia.org/wiki/Twisted_pair

4.2. La fibre optique monomode

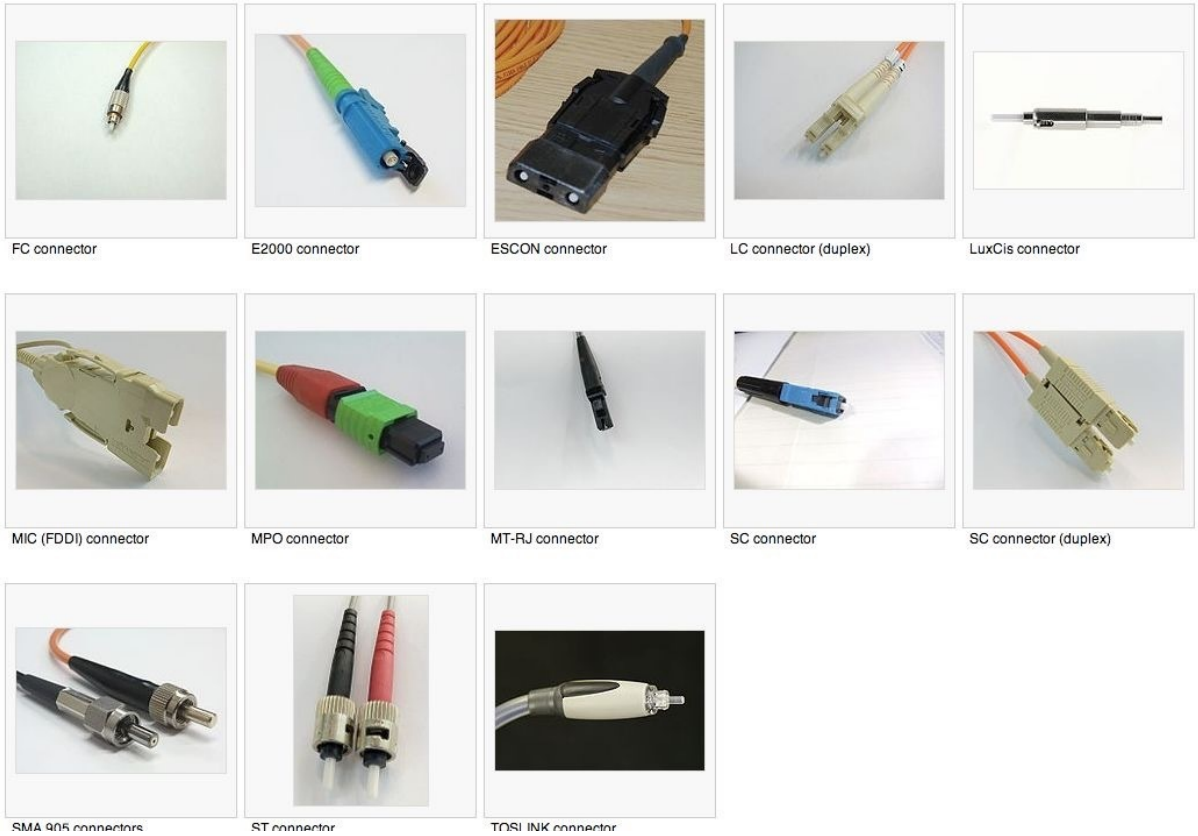
Les rayons suivent un seul chemin. La fibre optique monomode a le coeur si fin (de l'ordre de la longueur d'onde du signal transmis) que le chemin de propagation des différents modes est pratiquement direct. La dispersion du signal est quasiment nulle, le signal est donc très peu déformé. Ses performances sont d'environ 100 gigabits/km, l'indice de réfraction peut être constant ou décroissant. Cette fibre optique est utilisée essentiellement pour les sites à distance. Le petit diamètre du coeur nécessite une grande puissance d'émission, donc des diodes au laser qui sont relativement onéreuses (ce qui rend la fibre optique monomode plus chère que la fibre optique multimode). Du fait de ses débits très importants, mais de son coût élevé, cette fibre est utilisée essentiellement pour les sites à grande distance et très grande distance.



Fibre monomode, fibre multimode

4.3. Types de connecteurs fibres

On trouvera un grand nombre de connecteurs fibres.



[Connecteurs fibre](https ://en.wikipedia.org/wiki/Optical_fiber_connector)

4.4. DWDM (Dense Wavelength-Division Multiplexing)

DWDM (Dense Wavelength-Division Multiplexing) est une technologie de fibre optique qui multiplie la quantité de bande passante dans un seul brin de fibre. DWDM permet des communications bidirectionnelles sur un même brin. Il est capable de multiplexer jusqu'à 80 canaux de 10 Gbps sur une seule fibre. Il supporte les standards SONET et SDH.

Les circuits DWDM sont utilisés dans tous les câbles sous-marins de communication et longue distance.

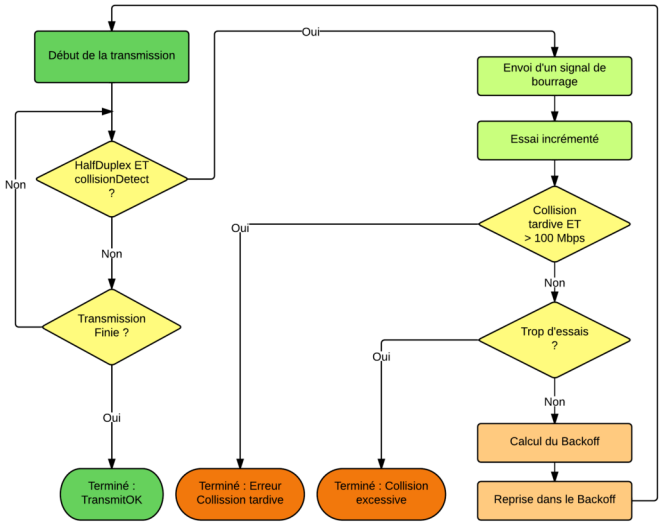
[Séries de modules SFP+ pour des communications 10 GHz WDM](https ://commons.wikimedia.org/wiki/File :SFP_WDM_2.jpg)

5. Ethernet (CSMA/CD) IEEE 802.3

Ethernet est une technologie à support partagé. L'accès au support est donc concurrentiel.

La technologie Ethernet répond au principe "premier arrivé, premier servi" et se propose de gérer le phénomène intrinsèque des collisions.

Ethernet ne met en oeuvre aucun mécanisme de fiabilité ou de connexion. Tout au plus, une interface (destination finale ou commutateur intermédiaire) va vérifier la trame reçue. En cas de trame corrompue, le trafic est abandonné, sans plus.



Algorithme CSMA/CD

5.1. Topologie logique et topologie physique

La topologie logique est la méthode d'accès (MAC) au support physique.

On distingue :

- Les méthodes stochastiques, premier arrivé premier servi (Ethernet, Wi-Fi).
- Les méthodes déterministes, par passage de jeton, contrôlé (Token-Ring).

5.2. CSMA/CD

La méthode d'accès MAC est appelée : Carrier Sense Multiple Access with Collision Detection (CSMA/CD) :

- Principe premier arrivé premier servi.
- Si le canal est libre, la station place son trafic.
- Si ce n'est pas le cas, elle attend.
- Le protocole se propose de gérer les collisions.
- Pas de fonction de fiabilité (ACK), pas de fonctions de gestions d'erreur, de contrôle de flux, etc.
- CSMA/CD = Ethernet Legacy (10BASE2, 10BASE5, 10BASE-T)

5.3. Principe CSMA (Carrier Sense Multiple Access)

1. Une interface qui tente de placer une trame écoute le support.
2. En cas de porteuse, elle retarde 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 collisions 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 un média 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.

5.4. Gestion des collisions (CD)

Sur un support partagé, une collision peut survenir lorsque deux ou plusieurs interfaces tentent de placer une trame en même temps alors qu'elles ont constaté un support libre (absence de porteuse).

Parce qu'il faut un certain délai pour qu'une trame arrive d'une extrémité à l'autre du support, l'interface émettrice va rester attentive pendant ce temps à d'éventuelles collisions. Les standards 802.3 définissent précisément ce temps. Il est appelé le slot time. Jusqu'en 100 Mbps, il s'agit du temps de placement de 512 bits ou 64 octets.

- En cas de collision, les stations impliquées la renforcent en envoyant un signal de bourrage afin que toutes les interfaces du réseau l'entendent.
- Elles attendent alors de reprendre la procédure de placement de la trame dans un délai aléatoire. C'est ce qu'on appelle le mécanisme de Backoff prévu par le protocole.

- Précisément, les stations impliquées reprendront aléatoirement dans une fourchette variant de 0 à un multiple du slot time.

Le support partagé par du matériel de couche 1 (Hub, concentrateur, câble en bus) est appelé domaine de collision. La bande passante est partagée dans un domaine de collision.

5.5. Délais

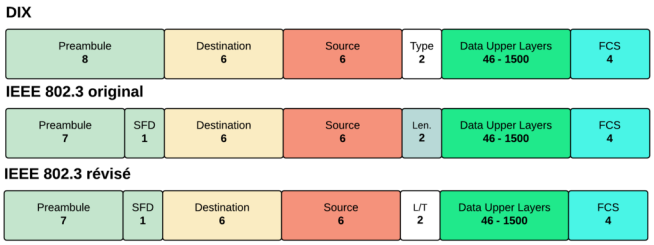
Les délais dans la technologie Ethernet dépendant de la qualité de l'infrastructure. Si celle-ci connaît des défaillances physiques dans le câblage, les connecteurs, les prises de connexion ou les panneaux de brassages, on aura des délais et une expérience diminuée de la technologie, voire une incapacité.

C'est parce que le signal se propage dans un délai certain encodé dans les cartes réseau Ethernet que taille maximale d'un segment est fixée à 100 mètres sur du câble à paires torsadées.

6. Trame Ethernet 802.3

On trouvera deux types de trames Ethernet : IEEE 802.3 standard et Ethernert II (DIX). Les trames DIX sont celles qui sortent des cartes réseau de nos ordinateurs terminaux (stations de travail, imprimantes, serveurs traditionnels). Les trames IEEE 802.3 sont émises par du matériel "*legacy*" d'infrastructure de type commutateur ou routeur.

6.1. Format de trame Ethernet 802.3



Formats de trames Ethernet

Une trame Ethernet dispose de deux champs d'adresses : "destination" et "source" codées sur 48 bits chacune.

Ensuite, on y trouve soit un champ "longueur" **ou** un champ "type". Le champ "type" annonce la charge contenue dans la trame. Dans une trame IEEE 802.3, le protocole LLC (Logical Link Control) s'occupe d'interfacer des protocoles de couche 2 comme CDP ou Spanning-Tree par exemple.

Enfin, en "en queue" de trame, on trouve un champ de 4 bits "FCS" (Frame Check Sequency) qui vérifie l'intégrité de la trame. L'hôte émetteur fabrique une somme de contrôle et l'inscrit dans ce champ ; à la réception, les hôtes Ethernet vérifient cette valeur. Quand les valeurs ne correspondent pas, Ethernet ne propose aucun mécanisme de reprise, la trame est abandonnée. La fiabilité pourrait être assurée par un protocole de couche supérieure comme TCP.

A titre d'exercice, quelle est la différence entre ces deux types de trames ?

- des trames IEEE 802.3 CDP émises d'un commutateur Cisco
- des trames Ethernet ARP émises d'un hôte quelconque.

6.2. Champ "Ethertype"

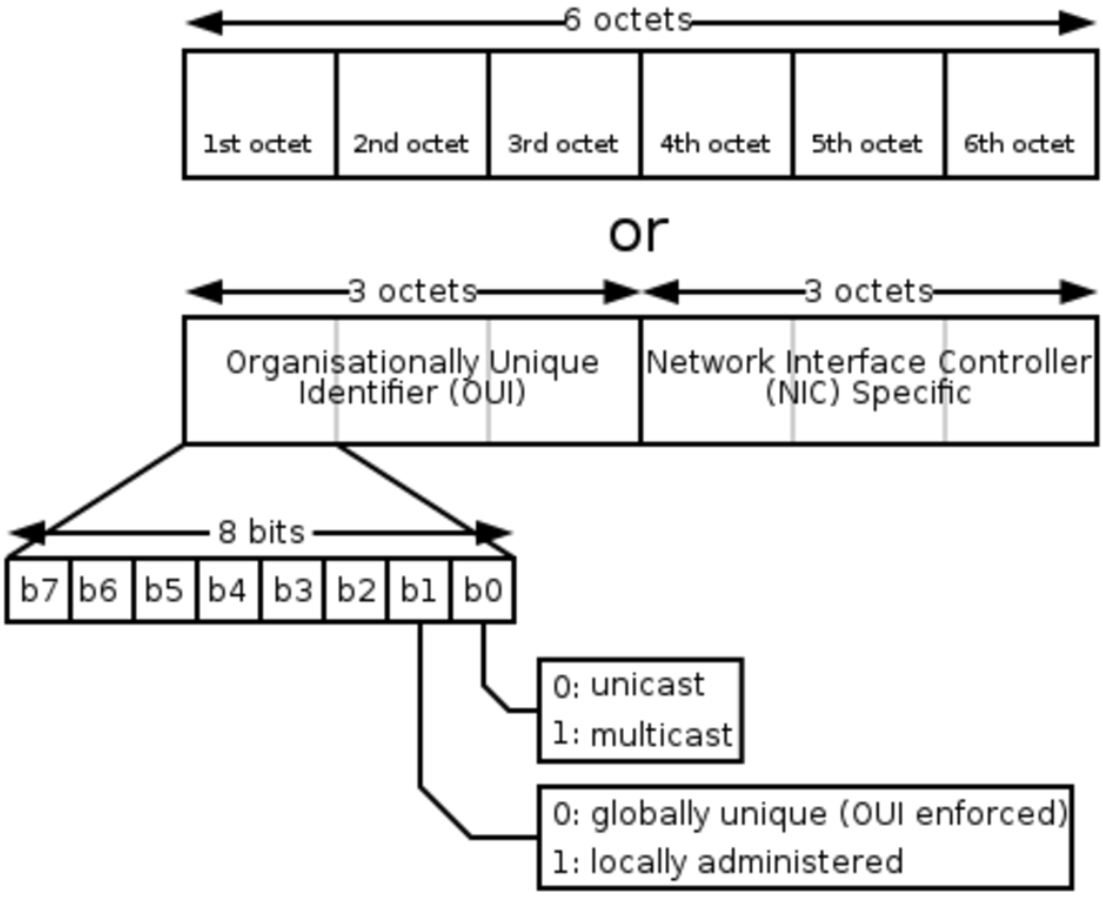
Le champ "type" d'une trame Ethernet annonce la charge qu'elle comprend. On trouve une liste sommaire dans le tableau suivant.

Ethertype	Protocole
0x0800	Internet Protocol version 4 (IPv4)
0x0806	Address Resolution Protocol (ARP)
0x8100	VLAN-tagged frame (IEEE 802.1Q)
0x86DD	Internet Protocol Version 6 (IPv6)
0x8863	PPPoE Discovery Stage
0x8864	PPPoE Session Stage
0x8870	Jumbo Frames
0x888E	EAP over LAN (IEEE 802.1X)
0x9100	Q-in-Q

6.3. Adressage MAC 802

L'adresse MAC 802 est un adressage de livraison locale, de couche 2, on peut le caractériser comme étant un adressage "physique".

- Une adresse MAC est fondée dans la carte.
- Elle est codée en 48 bits notés en hexadécimal `AA :BB :CC :DD :EE :FF`
- Les 24 premiers bits d'une adresse MAC identifient le constructeur de l'interface réseau et sont appelés *Organizationaly Unique Identifier* (OUI). Les préfixes OUI sont enregistrés auprès de l'IEEE.
- Les 24 derniers bits sont laissés à la discrétion du constructeur.
- L'adressage MAC-EUI64 est un adressage étendu de 16 bits `FFFE : AA :BB :CC :FF :FE :DD :EE :FF`



Adressage MAC IEEE 802

Source de l'image : Adressage MAC IEEE 802.

Note : Lors de l'opération de transformation de 48 à 64 bits, il est nécessaire de renverser le bit "Universal/Local" ("U/L bit") à la septième position du premier octet. Le bit "u" bit est fixé à 1 (Universal) et il est fixé à zéro (0) pour indiquer une portée locale de l'adresse.

6.4. Préfixes d'adresses MAC

Comme en IP on trouve un adressage MAC Unicast, Broadcast et Multicast.

L'adressage Unicast est celui qui est à destination d'*une seule* interface. On trouvera la liste des préfixes IEEE MAC dans ce fichier : Sanitized IEEE OUI Data (oui.txt).

Une adresse de (diffusion) Broadcast est à destination de *toutes* les interfaces :

```
FF:FF:FF:FF:FF:FF
```

L'adressage Multicast (CDP/VTP, STP, IPv4, IPv6) est celui qui est à destination de *certaines* interfaces :

- CDP/VTP : `01:00:0C :CC :CC :CC`
- STP : `01:80:C2:00:00:00`
- Multicast IPv4 : `01:00:5E :00:00:00 - 01:00:5E :7F :FF :FF`
- Multicast IPv6 : `33:33:00:00:00:00 - 33:33:FF :FF :FF :FF`

7. Power over Ethernet

La technologie “Power over Ethernet” ou PoE, normalisée IEEE 802.3af permet d’alimenter en courant continu (DC) des périphériques du réseau comme des téléphones IP, des caméras IP, des points d’accès Wi-Fi[2] grâce aux câbles à paires torsadées utilisés par Ethernet en même temps que la transmission de données.

7.1. Alimentation électrique via le câble de données

Le PoE fournit environ 48 V en courant continu à travers deux fils non utilisés des quatre fils disponibles avec du câble de catégorie 3 ou 5e, pour du 10BASE-T et du 100BASE-TX. Une technique dite “phantom power” permet également de transporter le courant à travers une paire utilisée pour la transmission de données. Ceci permet donc l’utilisation du PoE avec du 1000BASE-T, en utilisant toutes les paires (catégorie 5e ou plus).

Le PoE original fournit un maximum de 350 mA et une puissance maximale de 15,4 W. Seulement 13 W sont disponibles après décompte de la déperdition de 10 à 20 % de l’énergie disponible dans les câbles (résistance des câbles d’où déperdition de chaleur par effet joule). Cela est d’ailleurs l’un des problèmes à résoudre par les constructeurs de câblage, car la concentration des passages de câbles occasionne un échauffement accru, ce qui implique un vieillissement accéléré et des caractéristiques physiques différentes.[3]

Habituellement, l’alimentation peut être fournie soit par les ports de commutateurs Ethernet compatibles (et plus coûteux), soit par des injecteurs PoE qui s’insèrent sur le câble de données pour y placer un courant électrique.

7.2. Avantages et objectifs de PoE

PoE permet de faire des économies de coûts d’installation :

- Supprime la nécessité d’installer des prises électriques
- Réduit considérablement les coûts de déploiement
- Pas besoin de gros adaptateurs de courant alternatif

PoE simplifie l’installation :

- Utilise un seul câble Cat5/5e/6 pour les données et l’alimentation

PoE permet d’assurer une sauvegarde centralisée de l’alimentation :

- Fonctionnement continu pendant les interruptions de courant

PoE permet une gestion centralisée de l’alimentation :

- Les appareils peuvent être mis hors tension à distance pendant les périodes de faible utilisation ou pour des raisons de sécurité

PoE permet de sécuriser l’alimentation :

- PoE n’endommagera pas les dispositifs non-PoE ou les périphériques existants

2. Cas d’usage PoE.
3. Alimentation électrique par câble Ethernet et Introduction to PoE and the IEEE802.3af and 802.3at Standards.

7.3. Fonctionnement de PoE

On trouvera deux types de périphériques PoE :

- Les “Powered Devices (PDs)”, ceux qui sont alimentés comme les téléphones IP, les caméras IP ou encore les points d’accès Wi-Fi.
- Les “Power Sourcing Equipments (PSEs)” comme des commutateurs PoE ou des injecteurs de puissance PoE.

Pour éviter qu’un périphérique reçoive une puissance inappropriée, le standard PoE met en oeuvre un mécanisme d’autonégociation qui permet d’adapter le niveau de puissance (voire de ne pas l’envoyer) selon certaines “classes” entre le Powered Device (PD) et le “Power Sourcing Equipment (PSE)”. Ensuite, des protocoles comme LLDP ou CDP peuvent être utilisés par les PSE pour compléter la configuration.

7.4. Normes PoE

Depuis les années 2000, Cisco Systems a développé des normes d’alimentation par le câble de données qui sont ensuite devenus des standards interopérables ratifiés par l’IEEE. En voici un tableau récapitulatif.

Nom	Standard	Watts Max. (PSE)	Paires alimentées
Cisco Inline Power	Cisco	7	2
PoE	IEEE 802.3af	15	2
PoE+	IEEE 802.3at	30	2
UPoE (4PPoE)	IEEE 802.3bt (Type 3)	60	4
UpoE+	IEEE 802.3bt (Type 4)	100	4

8. Identifier les problèmes d’interface et de câbles Ethernet sur le matériel Cisco

Pour identifier des problèmes physiques (L1) tels que des câbles (ou d’interfaces) défectueux, des câbles trop longs, des collisions locales ou tardives, on apprendra à interpréter les sorties de la commande IOS `show interfaces`.

8.1. Commande show interfaces

La commande `show interfaces` offre un diagnostic de couche 2 complet que l’on peut décomposer en plusieurs parties :

- Statut de l’interface (L1) et protocole de ligne (L2).
- Des paramètres d’adresses L2 et d’encapsulation, de mode, de vitesse et de type de support, l’interval keepalive.
- Des paramètres de qualité de service (QoS).
- Des statistiques de succès et d’erreurs sur les trames vues par l’interface.

```
Switch#show interfaces GigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
  Hardware is iGbE, address is 0c10.2a8e.1c00 (bia 0c10.2a8e.1c00)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto Duplex, Auto Speed, link type is auto, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 03:21:22, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     67 packets input, 10022 bytes, 0 no buffer
     Received 62 broadcasts (62 multicasts)
     6 runts, 0 giants, 0 throttles
     6 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 62 multicast, 0 pause input
     10911 packets output, 817382 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     1 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

8.2. Statut d'interface

Le statut d'interface peut prendre trois valeurs[^2] et signifie un problème de couche 1, soit de signal sur le câble :

- `administratively down` : interface désactivée
- `down` : l'interface ne reçoit pas de signal
- `up` : l'interface reçoit du signal

Statut d'interface	Signification	Remède
`administratively down`	l'interface est "shutdown"	monter l'interface avec la commande `no shutdown`
`down`	l'interface ne reçoit pas de signal	problème physique, l'interface connectée est désactivée, le câble est "pendant"
`up`	l'interface reçoit du signal	interface opérationnelle au niveau de la couche 1

8.3. Protocole de ligne

Le diagnostic "line protocol is" est un diagnostic de couche 2 (L2) qui indique si le protocole Ethernet est opérationnel. Étant donné qu'il est totalement discret, on aura des erreurs indiquées à cet endroit. Mais par exemple, en PPPoE avec un défaut d'authentification empêche le protocole de se monter.

Line Protocole prend deux valeurs possibles :

- `up` : le protocole de couche 2 est opérationnel.
- `down` : le protocole de couche 2 ne répond pas.

Voici les cas de diagnostic de “line protocol is down” :

Statut d’interface	Protocole de ligne	Signification
`administratively down`	`down`	sans couche 1, pas de couche 2
`down`	`down`	sans couche 1, pas de couche 2
`up`	`down`	L’interface reçoit du signal, mais n’arrive pas négocier un paramètre de couche 2

8.4. Problèmes d’interfaces et de câbles Ethernet

Dans la dernière partie du résultat de la commande `show interafces`, sur les statistiques, on retiendra la signification quelques valeurs comme *runts*, *CRC* ou *collisions* :

Valeur de la statistique	Signification
runts	Donne le nombre de paquets qui sont rejetés parce qu’ils sont plus petits que la taille minimale de paquet du support. Par exemple, tout paquet Ethernet de moins de 64 octets est considéré comme un avorton.
CRC	Indique que la somme de contrôle de redondance cyclique (CRC, “cyclic redundancy checksum”) générée par la station LAN d’origine ou le dispositif distant ne correspond pas à la somme de contrôle calculée à partir des données reçues. Sur un réseau local, cela indique généralement des problèmes de bruit ou de transmission sur l’interface du réseau local ou sur le bus du réseau local lui-même. Un nombre élevé de CRC est généralement le résultat de collisions ou d’une station transmettant de mauvaises données.
collisions	Donne le nombre de messages retransmis à la suite d’une collision Ethernet. Ceci est généralement le résultat d’une extension excessive du réseau local (câble Ethernet ou émetteur-récepteur trop long, plus de deux répéteurs entre les stations, ou trop d’émetteurs-récepteurs multiports en cascade). Un paquet qui entre en collision n’est compté qu’une seule fois dans les paquets de sortie.

Différents problèmes de câblage peuvent intervenir sur des interfaces Ethernet :

- Bruit excessif (Excessive noise)
- Collisions excessives (Excessive collisions)
- Trames avortons excessives (Excessive runt frames)
- Collisions tardives (Late collisions)
- “No link integrity”

8.5. Bruit excessif (Excessive noise)

Avec du bruit excessif (Excessive noise) les valeurs d’erreurs CRC sont en grand nombre par rapport aux erreurs de collision.

8.6. Collisions excessives (Excessive collisions)

Le taux de collision, qui correspond au nombre de collisions par rapport au nombre de paquets sortants, ne devrait jamais être inférieur à 0,1%.

8.7. Trames avortons excessives (Excessive runt frames)

Dans un environnement Ethernet partagé, les trames avortons sont presque toujours causées par des collisions. Si les trames avortons se produisent lorsque les collisions ne sont pas élevées ou dans un environnement Ethernet commuté, elles sont alors le résultat de sous-exécutions (underruns) ou de mauvais logiciels d’une carte d’interface réseau.

8.8. Collisions tardives (Late collisions)

Les collisions tardives ne devraient jamais se produire dans un réseau Ethernet correctement conçu. Elles se produisent généralement lorsque les câbles Ethernet sont trop longs ou lorsqu'il y a trop de répéteurs dans le réseau.

8.9. "No link integrity"

Ce type d'erreur "No link integrity" suggère de vérifier le type de câble.

Deuxième partie Technologies VLANs

On trouvera ici un premier chapitre qui explique les principes fondamentaux des VLANs et la terminologie Cisco.

Un second chapitre expose les commandes de configuration des VLANs, du protocole DTP (Dynamic Trunking Protocol), du protocole VTP (Virtual Trunking Protocol) ainsi que des recommandations de bonnes pratiques.

Enfin, cette partie se termine par des exercices pratiques qui met en oeuvre tout ce qui a été exposé.

2. Concepts VLAN (Cisco IOS)

Ce chapitre est une présentation de la technologie VLAN, du concept de “Trunk” VLAN selon Cisco Systems, du routage “inter-VLANs”, de l’implémentation de la technologie en général et de la nomenclature Cisco en particulier.

1. Technologie VLAN

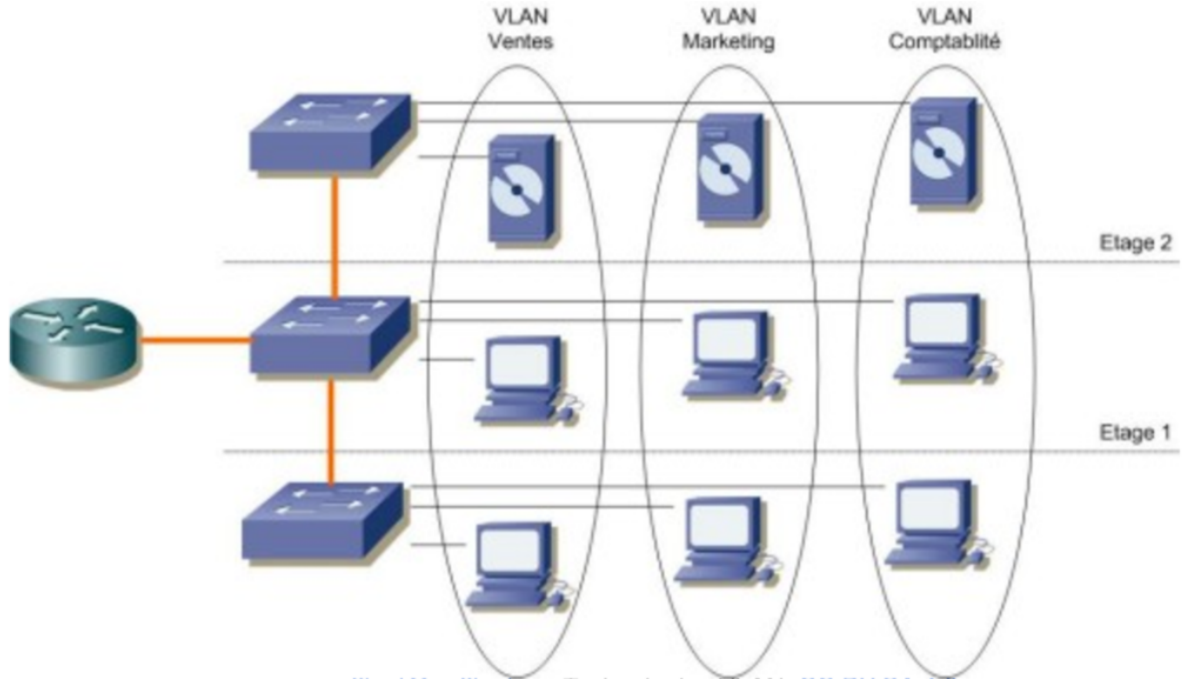
La technologie VLAN “virtualise” un LAN, un réseau local.

> La virtualisation d’un LAN consiste en la séparation entre, d’une part, l’infrastructure physique et, d’autre part, les services de couche 2 “liaison de données” fournis par les commutateurs.
>
> Soit une seule infrastructure physique supporte plusieurs LAN distincts (VLANs).

1.1. Utilité des VLANs

La technologie VLAN (LAN virtuel) permet de gérer et de maintenir plusieurs réseaux locaux (LANs), soit séparés par du routage, sur une seule et même infrastructure physique commutée.

Par analogie, on peut considérer qu’**un VLAN est un commutateur virtuel** sur plusieurs commutateurs physiques. On peut aussi considérer qu’**un VLAN correspond à un domaine de diffusion (*Broadcast*)** dans lequel on déploie un adressage IP cohérent comme un LAN.



Utilité des VLANs.

1.2. Avantages et inconvénients de la technologie VLAN

On citera brièvement les avantages acquis de la technologie VLAN :

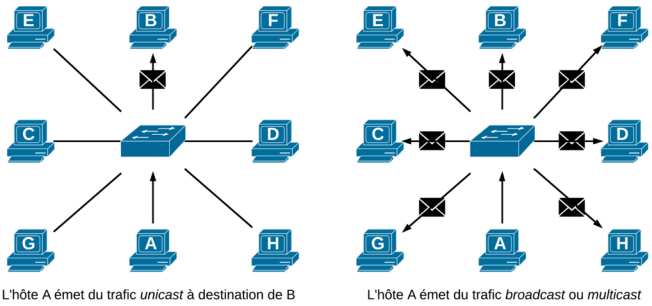
- Indépendance de la couche physique

- Contribue à la séparation des flux et la sécurité de l'infrastructure.
- Flexibilité : allocation dynamique des utilisateurs dans un réseau indépendamment de l'emplacement
- Facilité de gestion : QoS, classification, routage, filtrage
- Performances : diminution de la taille des domaines de Broadcast
- Coût abordable

A titre d'inconvénients, on peut citer :

- Architecture adaptées
- Investissements dans l'infrastructure
- Montées en compétences du personnel

1.3. Fonctionnement d'un LAN



Un LAN défini comme une infrastructure commutée.

Au sein d'un LAN défini comme une infrastructure commutée, soit un réseau composé de commutateurs, toutes les interfaces hôtes disposent d'une adresse unique : une adresse physique MAC du protocole IEEE 802.

Un commutateur (un "*switch*") tient une table de correspondance entre ses ports et les adresses MAC des hôtes afin de leur transférer rapidement le trafic. Cette opération de transfert est prise en charge au niveau matériel par des puces spécialisées appelées des ASICs.

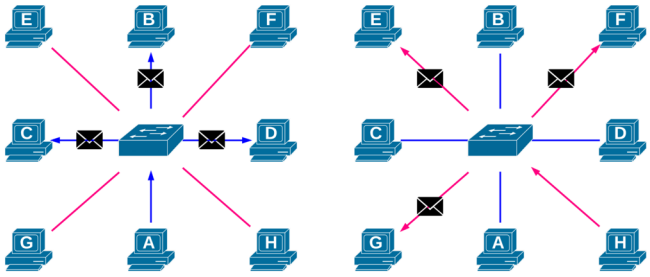
Sur ces réseaux, on connaît du trafic Unicast (à destination d'un seul hôte), du trafic de Broadcast (diffusion, à destination de tous les hôtes) et du trafic Multicast (à destination de certains hôtes).

Un commutateur transfère le trafic de diffusion (Broadcast) et Multicast à travers tous ses ports sauf celui d'origine ; un routeur "filtre" le trafic de diffusion en ne le transférant pas. Le trafic Unicast connu du commutateur est directement transféré par le bon port de sortie.

1.4. LAN Virtuel (VLAN)

Un VLAN est donc un LAN logique fonctionnant sur une infrastructure LAN physique commutée.

Une infrastructure physique commune peut supporter plusieurs VLANs. Chaque LAN virtuel fonctionnera comme n'importe quel LAN distinct.



Du trafic de Broadcast émane des stations A et H.

Concrètement, les ports du commutateur prennent un identifiant VLAN. Cet identifiant logique définit l'étendue du domaine de diffusion : le trafic de diffusion ne sera transféré que sur les ports ayant le même identifiant. Autrement dit, par exemple, le trafic de diffusion venant d'un port appartenant au VLAN 66 ne se sera transféré que sur les ports ayant pour attribution le VLAN 66.

La séparation fonctionnelle entre deux ports ayant des identifiants VLAN différents correspond à une séparation physique. En quelque sorte, la technologie VLAN permet de diviser logiquement les ports du commutateur, soit l'infrastructure physique elle-même.

1.5. Définition

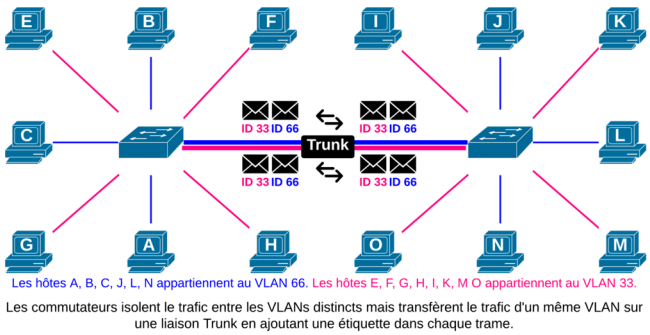
La virtualisation d'un LAN consiste à séparer l'infrastructure physique des services de transfert rapide fournis par les commutateurs.

L'objectif fondamental d'un VLAN est de rendre la fonction d'un LAN (tel que décrit plus haut) indépendante de l'infrastructure physique. Cette technologie s'intègre pleinement dans les marchés des environnements virtualisés, des déploiements de réseaux sans fil, de la VoIP, des passerelles Internet d'entreprise et familiales.

De plus, cette fonctionnalité peut être étendue sur des ports de commutateurs distants à travers toute l'infrastructure. Dans ce cas, les commutateurs devront transporter entre eux du trafic appartenant à plusieurs VLANs sur une ou plusieurs liaisons spécifiques …

2. Trunking

2.1. Trunk ou Liaison d'agrégation



Les commutateurs isolent le trafic entre les VLANs distincts mais transfèrent le trafic de plusieurs VLANs sur une liaison Trunk

… Les ports d'une liaison qui agrègent le trafic de plusieurs VLANs s'appellent un "Trunk" chez le constructeur Cisco Systems et "liaison d'agrégation" chez d'autres. Sur ce type de liaison, le commutateur ajoute des champs supplémentaires dans ou autour de la trame Ethernet. Ils servent notamment à distinguer le trafic de VLANs différents car ils contiennent entre autres le numéro d'identification du VLAN.

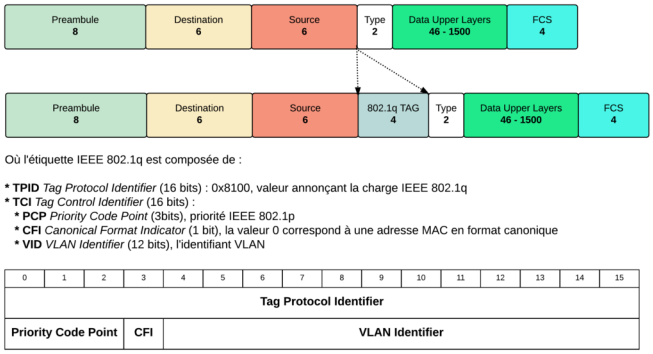
Une liaison “Trunk” transporte les trames de plusieurs VLANs. On imagine aisément que la liaison doit être dimensionnée en port “uplink” avec des capacités supérieures (bande passante) à celles des hôtes qui placent du trafic. Enfin, sauf exception, une liaison “Trunk” se monte entre des ports de commutateurs.

2.2. Protocoles “Trunk”

On trouvera deux protocoles de “Trunk” ou de “liaison d’agrégation” VLAN qui permettent de distinguer le trafic de VLANs distincts. Il agissent au niveau de la couche 2 “liaison de données” (L2). Ils opèrent sous les couches TCP/IP.

- Inter-Switch Link (ISL) : protocole propriétaire Cisco qui encapsule la trame d’origine avec un en-tête spécifique qui contient entre autres le numéro de VLAN et un nouveau champ FCS. Il est indépendant de la technologie sous-jacente. Il est de moins en moins rencontré au profit de IEEE 802.1q.
- **IEEE 802.1q** : Standardisé et interopérable, il ajoute une étiquette dans l’en-tête de la trame (un ensemble de champs juste après le champ d’adresse MAC d’origine). Cette étiquette a une taille de 4 octets ou 32 bits dont 12 bits sont consacrés au numéro de VLAN. Le standard supporte les technologies IEEE 802.3 (Ethernet), IEEE 802.11 (WIFI), IEEE 802.5 (Token-Ring), etc. en tant que protocole de “pontage” (bridging, IEEE 802.1). Vu que la trame sera modifiée, le commutateur recalculera la valeur du champ CRC/FCS.

2.3. Etiquette IEEE 802.1q



Etiquette 802.1q

Où l’étiquette IEEE 802.1q est composée de :

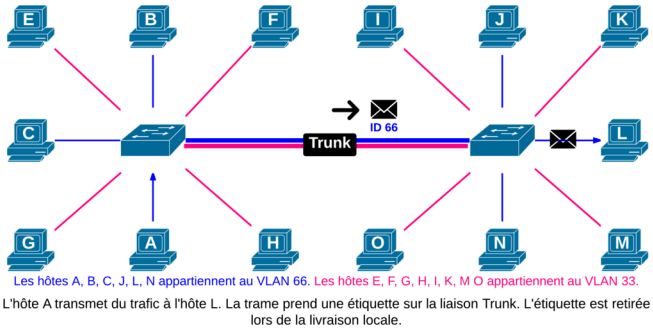
- TPID Tag Protocol Identifier (16 bits) : 0x8100, valeur annonçant la charge IEEE 802.1q
- TCI Tag Control Identifier (16 bits) :
  - PCP Priority Code Point (3bits), priorité IEEE 802.1p
  - CFI Canonical Format Indicator (1 bit), la valeur 0 correspond à une adresse MAC en format canonique
  - **VID VLAN Identifier (12 bits)**, l’identifiant VLAN

```
Frame 408: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)
Ethernet II, Src: 00:de:a2:0c:c7:00 (00:de:a2:0c:c7:00), Dst: 00:de:a2:83:4c:00 (00:de:a2:83:4c:00)
    Destination: 00:de:a2:83:4c:00 (00:de:a2:83:4c:00)
    Source: 00:de:a2:0c:c7:00 (00:de:a2:0c:c7:00)
    Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 10
    000. .... .... .... = Priority: Best Effort (default) (0)
    ...0 .... .... .... = CFI: Canonical (0)
    .... 0000 0000 1010 = ID: 10
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000
    Trailer: 00000000
Address Resolution Protocol (request)
```

Capture : https ://www.cloudshark.org/captures/e1fa27f2ec12

2.4. Encapsulation IEEE 802.1q

Quand est-ce que cette encapsulation IEEE 802.1q intervient-elle ?

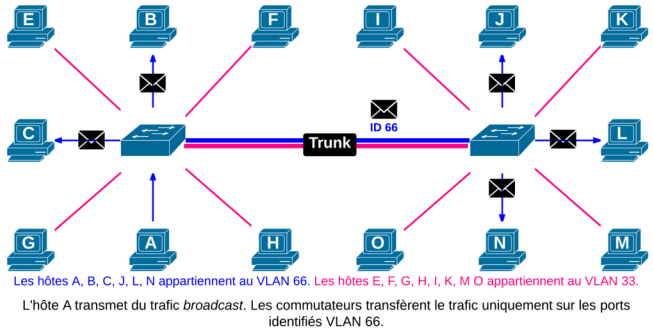


Un hôte A veut joindre un hôte L connecté à un commutateur distant.

Un hôte A veut joindre un hôte L connecté à un commutateur distant. Les commutateurs sont interconnectés par une “liaison d’agrégation” ou “Trunk”. La trame sera étiquetée seulement si elle quitte le commutateur sur un port qui connecte une “liaison d’agrégation” ou “Trunk”. Lors de la livraison locale de la trame à la station destinataire, elle sort du port du commutateur de destination sans étiquette.

2.5. Multicast/Diffusion

Le trafic de diffusion (Broadcast) comme celui de Multicast sera porté à la destination de tous les ports ayant le même identifiant VLAN, mais aussi à travers des ports “Trunk”.



Broadcast sur un port Trunk

Les hôtes connectés à un port d’un identifiant VLAN différent ne seront pas affectés par ce trafic. En ce sens, la taille des domaines de diffusion peut être contrôlée sur une infrastructure commutée à des fins de performance, d’administration du trafic et du contrôle des flux des machines et finalement de leurs utilisateurs.

2.6. Domaines IP

Comme dans tout LAN, le réseau IP est homogène et correspond à un adressage marqué par un préfixe et un masque de réseau.

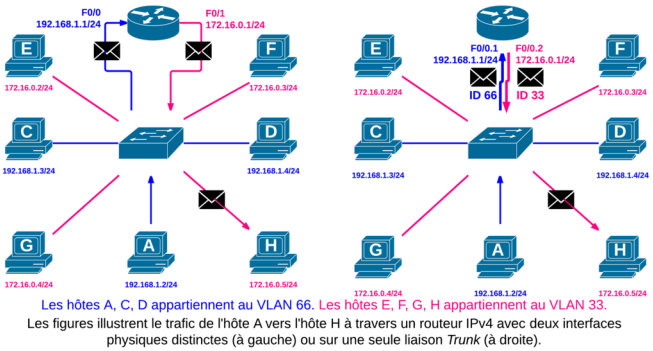
Au sein d’un LAN, toutes les interfaces qui participent à IP partagent le même adressage.

Un routeur constitue la limite d’un VLAN comme celle d’un LAN. En conséquence, pour que des VLANs communiquent ensemble, en tant que réseaux logiques différents, une fonction de routage est nécessaire. On parle alors dans la littérature de “routage inter-VLAN”.

Cette fonction peut être remplie par des plates-formes d’entreprise comme des routeurs d’accès, des routeurs Linux/BSD mais de préférence avec des commutateurs LAN disposant d’un logiciel de routage (commutateurs L3,

commutateurs mulicouches, *Multilayer switches*). Ces “routeurs” sont capables de transférer du trafic de VLANs différents à partir d’un seul port physique reconnu comme port d’agrégation VLAN.

2.7. Routage inter-VLAN



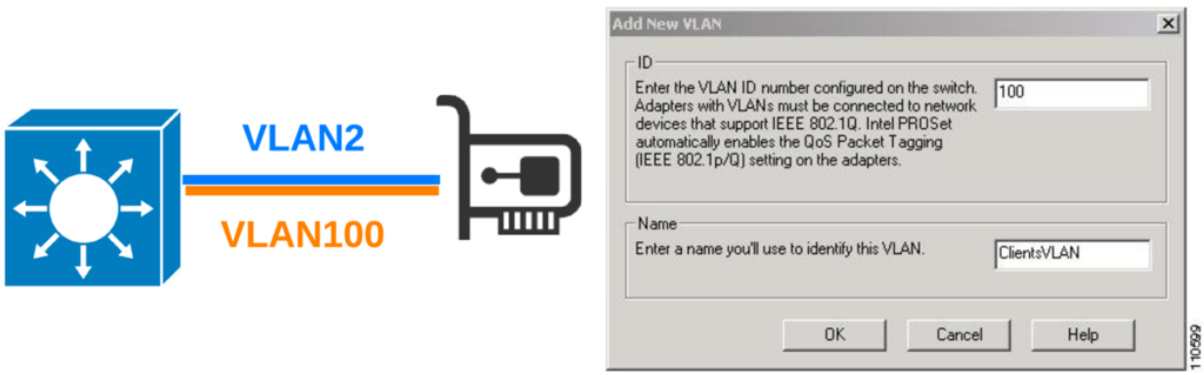
Routage Inter-VLAN

Dans cet exemple, une seule interface du routeur est nécessaire. Elle sera configurée en mode “trunk” en créant pour chaque VLAN une sous-interface logique différente. Évidemment, l’interface physique ne prend pas d’adresse IP.

Cette configuration de lab que l’on ne souhaitera pas rencontrer dans la réalité, est appelée “routeur-on-a-stick”.

3. Implémentation de la technologie

3.1. Cartes IEEE 802.1q



Les serveurs professionnels intègrent des cartes réseaux compatibles IEEE 802.1q.

Si le standard est largement disponible sur les commutateurs d’entreprise, les hôtes tels que les serveurs ou du matériel embarqué peuvent supporter la technologie VLAN en fonction des pilotes développés pour l’interface physique. Alors que les systèmes d’exploitation Linux/BSD supportent un grand nombre de cartes, les cartes Intel (ou Broadcom) sont bien supportées sous Microsoft Windows ; elles sont proposées d’emblée par les grands assembleurs comme HP ou Dell.

3.2. Implémentation VLAN

On trouvera différents types d’implémentations sur les commutateurs, à savoir :

- Les **VLANs statiques** ou dits “port-based” ou “port-centric” : un port de commutateur appartient “statiquement” à un VLAN. Ce type de configuration nécessite un configuration manuelle de chaque port. **C’est encore l’implémentation la plus courante**.

- Les **VLANs dynamiques** : où l'attribution d'un VLAN est effectuée dynamiquement sur base d'une adresse physique (MAC), logique (IP) ou de crédits quelconques avec **IEEE 802.1X / EAP**. Ce type d'implémentation est nécessairement la plus coûteuse et demande d'autant plus de composants d'infrastructure et de compétence.

4. Modes opérationnels des ports sur les commutateurs Cisco

Sur un port de commutateur Cisco (pas chez les autres), un "switchport", on rencontre deux modes opérationnels de ports :

- "access"
- "trunk"

4.1. Mode des ports "access"

Sur un commutateur Cisco, on distinguera les ports dits "access" des ports dits "trunk".

Un port "access" est un port qui ne transportera des informations que d'un seul VLAN. A priori, ce type de port connectera un hôte terminal, une station de travail ou un serveur.

Un port "access" n'ajoute pas d'étiquette au trafic qu'il délivre.

4.2. Mode des ports "trunk"

Un port "trunk" est un port qui transportera des informations de plusieurs VLANs. On y connectera un autre commutateur, un routeur ou même la carte réseau IEEE 802.1q d'un serveur configuré en port "trunk".

Un port "trunk" ajoute des étiquettes au trafic puisqu'il est destiné à un autre commutateur. Le VLAN natif est celui pour lequel il n'y aura pas d'étiquette ajoutée sur le port "trunk". Ce paramètre se définit d'ailleurs sur le port "trunk".

Autrement dit, un port "access" n'est pas un port "trunk" et inversement.

5. Nomenclature des VLANs

Dans sa documentation, Cisco Systems distinguent plusieurs types de VLANs. Cette nomenclature n'est pas stricte.

En voici une liste non-exhaustive.

- VLAN 1
- VLAN par défaut (Default VLAN)
- VLANs utilisateur (User VLAN)
- VLAN de gestion (Management VLAN)
- VLAN natif (Native VLAN)
- VLAN Voice
- VLANs réservés

5.1. VLAN 1

Le VLAN 1 est un VLAN spécial. Il est le VLAN par défaut de tous les ports, y compris l'interface de gestion (SVI). En plus, une série de protocoles de couche 2 comme CDP (Cisco Discovery Protocol), VTP (VLAN Trunk Protocol), PAgP (Port Aggregation Protocol) et DTP doivent impérativement transiter à travers ce VLAN spécifique.

Pour ces raisons, le VLAN 1 ne peut jamais être supprimé, il existe d'office.

Pour ces raisons, il recommandé d'éviter d'utiliser dans tous les cas le VLAN 1 dans ses déploiements en production.

Notons que les VLANs 1002 à 1005 sont des VLANs par défaut réservés aux technologies FDDI et Token-Ring. Ils sont donc inutilisables sur un commutateur Cisco Ethernet.

5.2. Vlan par défaut

Par défaut, le VLAN 1 est celui qui assigné à tous les ports d'un commutateur tant qu'ils n'ont pas été configurés autrement. Cela signifie que tous les autres types de VLANs (utilisateur, gestion et natif, etc.) sont membres du VLAN 1 par défaut.

5.3. VLAN utilisateur

On dira que ce type de VLAN est un VLAN "normal" dans le sens où il est celui qui a été configuré pour rendre une segmentation logique du commutateur dans le cadre de l'utilité des VLAN. La numérotation des VLANs est disponible sur 12 bits. Ceci dit, chaque modèle de switch aura ses limites en nombre total à créer et à gérer. Pour connecter des utilisateurs et leurs services, on évitera d'utiliser le VLAN 1.

5.4. VLAN de gestion

Le VLAN de gestion est un VLAN spécifique attribué aux commutateurs pour qu'ils soient accessibles via une adresse IP (ICMP, Telnet, SNMP, HTTP).

Qu'il existe ou non une interface physique appartenant au VLAN de gestion désigné, on joindra le commutateur en IP via une interface virtuelle (SVI) de type VLANx. Tous ports "access" associés à ce VLANx répondent en IP pour l'interface virtuelle VLANx.

Dans les bonnes pratiques de configuration, on le distinguera du VLAN par défaut d'un VLAN utilisateur ou du VLAN natif. On changera donc le numéro du VLAN de gestion.

Dans le cas d'une tempête de diffusion ou d'un souci de convergence avec Spanning-Tree, l'administrateur devrait toujours avoir accès au matériel pour résoudre les problèmes via ce VLAN.

Aussi, une bonne raison de séparer le VLAN de gestion des autres tient au fait évident de séparer logiquement les périphériques "dignes de confiance" des autres. Il s'agit alors d'appliquer les règles de sécurité nécessaires afin d'éviter, par exemple, que des utilisateurs classiques ou tout simplement "non-autorisés" n'accèdent au matériel.

5.5. VLAN natif

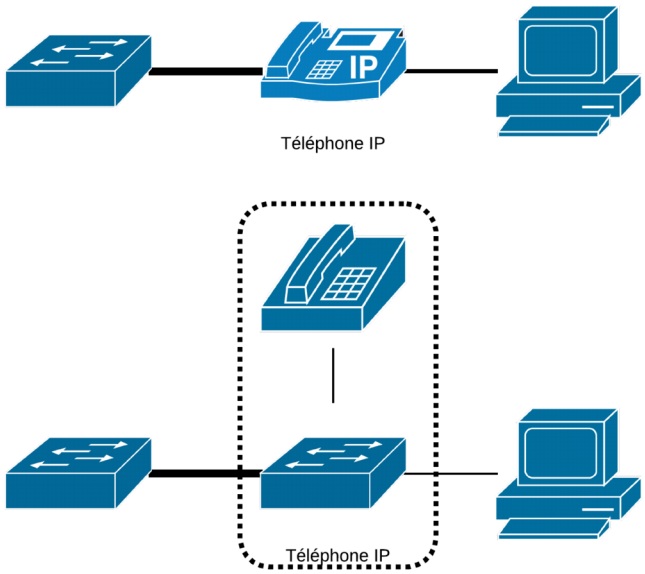
La notion de VLAN natif n'intervient que lorsque l'on configure un port "Trunk". Quand un port est configuré en tant que tel, le commutateur insère une "étiquette" dans l'en-tête de la trame avec le numéro de VLAN approprié.

Toutes les trames passant par un "Trunk" sont ainsi étiquetées sauf les trames appartenant au VLAN natif. Donc, les trames du VLAN natif, par défaut le VLAN 1, ne sont pas étiquetées. Ce type de VLAN existe pour assurer une inter-opérabilté avec du trafic ne supportant pas l'étiquetage. On recommandera de changer le numéro du VLAN natif.

Aussi, les protocoles de contrôles tels que CDP, VTP, PAgP et DTP sont toujours transmis par le VLAN natif. Si on change l'identifiant du VLAN natif, ce qui est conseillé, il faut le faire sur toutes les liaisons "Trunk", sur toute la topologie.

5.6. VLAN Voice

Pour assurer la Qualité de Service (QoS) des communications vocales, le VLAN Voice se configure sur un port Access et crée une sorte de mini-Trunk vers un téléphone IP.



VLAN Voice Cisco

5.7. VLANs réservés

Puisque le VLAN ID est codé sur 12 bits dans les étiquettes 802.1q, offrant de la sorte 4096 possibilités, le premier ID VLAN disponible `0` et le dernier `4095` sont réservés et ne peuvent donc pas être utilisés.

En retirant les VLANs par défaut et les VLANs réservés, la plage de VLANs disponibles varie de 1 à 1001 et de 1006 à 4094.

Troisième partie Redondance de liens

Cette partie expose les principes fondamentaux des protocoles Spanning-Tree et Rapid Spanning-Tree au niveau de la couche 2 (L2) et ainsi que ceux du protocole de couche physique (L1) Etherchannel qui permet d'agréger les liaisons sur le plan logique.

Spanning-Tree est un protocole L2 formalisé IEEE 802.1D qui vise à créer un chemin unique entre les commutateurs interconnectés d'un LAN. La solution vise à se prémunir de la problématique des boucles de commutation (*bridging loops*). Toutefois Spanning-Tree dispose de plusieurs désavantages : il converge lentement, il est limité dans le diamètre du réseau (sept commutateurs en cascade) et il est très crédule rendant l'architecture vulnérable aux attaques internes. Aussi, pendant qu'un chemin unique est créé pour le réseau local, les autres liens redondants ne sont pas utilisés.

Heureusement, il est possible d'optimiser l'anti-bouclage de couche 2 (L2) avec Rapid Spanning-Tree. On le déploiera uniquement entre la couche Access et Distribution en tentant aujourd'hui de dédier les VLANs sur les commutateurs de couche Access. Spanning-Tree reste vulnérable à des attaques locales sur les commutateurs. Cisco Systems (mais aussi les autres fabricants de commutateurs) propose une série de contre-mesures comme "BPDU Guard".

La technologie Etherchannel (IEEE 802.3ad) permet d'agréger des liens sur le plan physique en assurant la reprise sur erreur et en augmentant la capacité des interconnexions. Elle trouve certainement son utilité en simplifiant les topologies Spanning-Tree dans les "switch blocks" tout en augmentant la tolérance aux pannes.

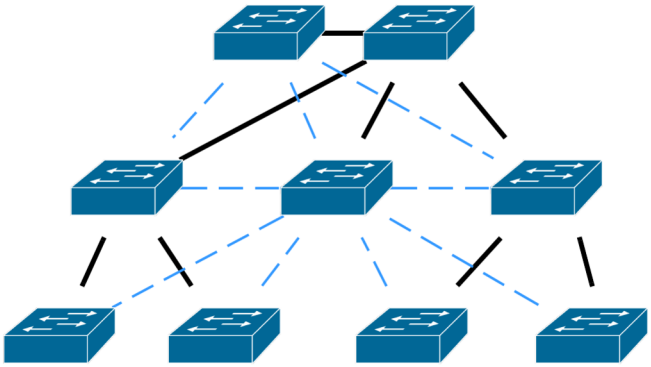
3. Spanning-Tree et Rapid Spanning-tree Cisco

1. Spanning-Tree

Spanning-Tree est un protocole L2 formalisé IEEE 802.1D qui permet de garder une topologie physique redondante tout en créant un chemin logique unique.

Spanning-Tree envoie régulièrement des annonces (BPDU) pour élire un commutateur principal (root).

En fonction de cette information, les commutateurs “coupent” des ports et une topologie de transfert à chemin unique converge (de quelques secondes à 50 secondes selon les versions).



Activé par défaut sur les commutateurs Cisco, Spanning-Tree crée une topologie de transfert sans boucle dans un réseau commuté (L2)

1.1. Variantes STP

Sur du matériel Cisco, Spanning-Tree fonctionne en mode propriétaire avec PVST+ (Per-VLAN Spanning Tree) ou avec PVRST+ (Per-VLAN Rapid Spanning Tree).

Nom	Standard
Spanning-Tree (STP)	IEEE 802.1D
PVST+	STP Cisco
Rapid Spanning-Tree (RSTP)	IEEE 802.1w
PVRST+	RSTP Cisco
MIST	IEEE 802.1s

1.2. Protocoles 802

IEEE 802.1 est un groupe de travail du projet IEEE 802.

Les thèmes d’étude du groupe de travail IEEE 802 sont (dans l’ordre où le groupe de normalisation les énumère) :

- **IEEE 802.1 : Gestion des réseaux locaux, VLAN, authentification, etc.**
- IEEE 802.2 : Distinction entre couche Logical Link Control (LLC) et Media Access Control (MAC)
- **IEEE 802.3 : Couche média CSMA/CD Ethernet**

- IEEE 802.4 : Couche média CSMA/CA Token Bus et AppleTalk (utilisée en informatique industrielle) (dissous)
- IEEE 802.5 : Couche média Token Ring (IBM)
- IEEE 802.6 : Groupe de conseils sur les réseaux à grande distance (Réseau métropolitain ou MAN) (dissous)
- IEEE 802.7 : Groupe de conseils sur les réseaux à large bande (dissous)
- IEEE 802.8 : Groupe de conseils sur les réseaux sur fibre optique (dissous)
- IEEE 802.9 : Réseaux à intégration de services comme RNIS (dissous)
- IEEE 802.10 : Interopérabilité de la sécurité des LAN/MAN (dissous)
- **IEEE 802.11** : **Réseaux sans fil** : **réseau sans fil**, **Wi-Fi**
- IEEE 802.12 : Réseaux locaux utilisant le mécanisme de demande de priorité
- IEEE 802.13 : Inutilisé (À l'origine réseaux Mapway (dissous))
- IEEE 802.14 : Réseaux et modems câble (dissous)
- **IEEE 802.15** : **Réseaux privés sans fil (WPAN) comme le Bluetooth**
- IEEE 802.16 : Réseaux sans fil à large bande par exemple le WiMAX
- IEEE 802.17 : Réseaux de fibres optiques en anneau (Resilient Packet Ring)
- IEEE 802.18 : Groupe de conseils pour la normalisation des communications radioélectriques
- IEEE 802.19 : Groupe de conseils sur la cohabitation avec les autres standards
- IEEE 802.20 : Accès sans fil à bande large
- IEEE 802.21 : Transfert automatique des liaisons indépendamment du média
- IEEE 802.22 : Réseaux régionaux sans fil

1.3. Protocoles 802.1

Parmi les standards IEEE 802.1 les plus populaires, on trouvera :

- **802.1D** : **MAC Bridges**
- 802.1Q : Virtual LANs
- 802.1X : Port Based Network Access Control
- 802.1AB : Station and Media Access Control Connectivity Discovery (LLDP)
- 802.1AE : MAC Security
- 802.1AX : Link Aggregation

Sources : https ://fr.wikipedia.org/wiki/IEEE_802, http ://fr.wikipedia.org/wiki/IEEE_802.1, http ://en.wikipedia.org/wiki/IEEE_-802.1#802.1D

1.4. Terminologie Spanning-Tree

- Bridge
- MAC bridges
- BID
- BPDU
- États STP
- commutateur (switch) Root
- commutateur non-Root
- port Désigné
- port Root
- port Non-désigné
- délais
- RSTP
- PVST+
- PVRST+
- rapid-pvst

2. Problématique des boucles de commutation

Pour assurer la fiabilité des liaisons entre des commutateurs du LAN il est utile de multiplier les connexions physiques (redondance) entre ces périphériques, notamment entre la couche Acces et la couche Distribution.

Toutefois,

1. Si les commutateurs transfèrent le trafic de diffusion et Multicast par tous les ports sauf celui d'origine et
2. si les trames Ethernet ne disposent pas de durée de vie,

plusieurs problèmes peuvent alors survenir :

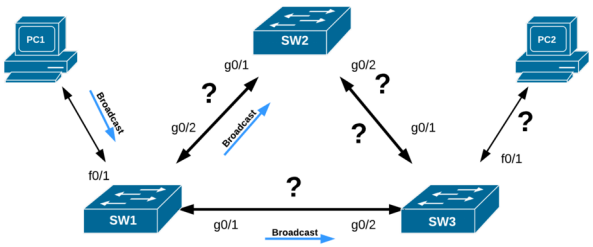
- des tempêtes de diffusion (de *Broadcast*),
- des trames dupliquées,
- une instabilité des tables de commutation.

2.1. Tempête de diffusion

Lorsque des trames de diffusion (`FF :FF :FF :FF :FF :FF` en destination par exemple, du trafic ARP Req) ou de Multicast sont reçues, les commutateurs les transfèrent par tous les ports, sauf le port d'origine.

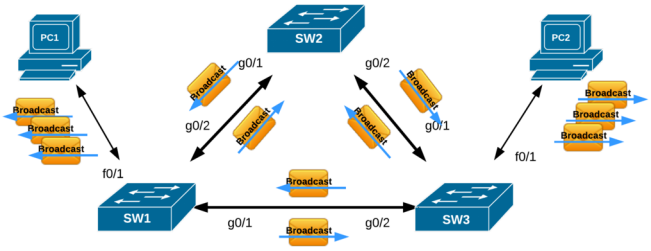
Les trames circulent en boucle et sont multipliées à chaque passage sur un commutateur. Ces données de couche 2 (L2) n'ayant pas de durée de vie (un Time to Live (TTL) comme les paquets IP traités par les routeurs), elles vont tourner indéfiniment entre les commutateurs.

Quel est le sort réservé par les commutateurs à la trame dont la destination est une adresse de diffusion ou Multicast dans un réseau bouclé ?



Quel est le sort d'une trame de Broadcast ou Multicast sur un commutateur ?

Dans ces conditions, une trame de diffusion est multipliée en boucle sur tous les ports jusqu'à rendre le réseau inutilisable.



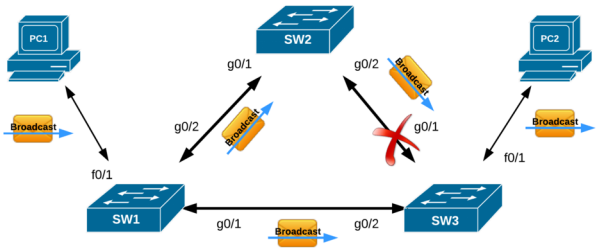
Les commutateurs transfèrent les trames de Broadcast / Multicast par tous ses ports sauf le port d'origine

Mais comment mettre fin à ce phénomène ?

2.2. Couper la boucle de commutation

Ce problème de bouclage dans un réseau commuté trouve sa solution avec la rupture de la boucle.

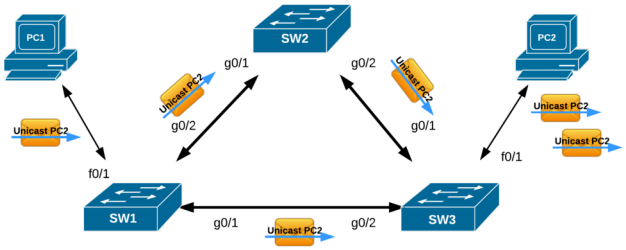
En coupant la boucle, un seul chemin est possible d'une extrémité à l'autre du réseau.



Couper la boucle de commutation

2.3. Trames dupliquées

Dans cet autre exemple, PC1 envoie une trame à PC2, elle arrive en double exemplaire à sa destination.



PC1 envoie une trame à PC2, elle arrive en double exemplaire à sa destination.

3. Spanning-Tree : Principe

Afin de profiter de la redondance tout en évitant la problématique des boucles, Spanning-Tree crée un chemin sans boucle basé sur le chemin le plus court.

- Ce chemin est établi en fonction de la somme des **coûts** de liens entre les commutateurs.
- Ce coût est une valeur inverse à la vitesse d'un port, car un lien rapide aura un coût moins élevé qu'un lien lent. Aussi, un chemin sans boucle suppose que certains ports soient bloqués (**état Blocking**) et pas d'autres (**état Forwarding**), certains transférant du trafic et d'autres pas.

Les commutateurs Spanning-Tree échangent régulièrement (2s. par défaut, en Multicast `01:80:c2:00:00:00`) des informations (appelées des **BPDU - Bridge Protocol Data Unit**) afin qu'une éventuelle modification de la topologie puisse être adaptée sans boucle.

3.1. BID : Bridge ID

Chaque commutateur Cisco prendra un identifiant unique appelé BID (Bridge ID) composé :

1. d'une priorité configurable (4 bits, multiples de 4096), par défaut cisco 32768 (0100)
2. d'une "Bridge System ID Extension" de 12 bits (numéros de VLAN)
3. de l'adresse MAC du commutateur

Par exemple :

```
Bridge ID  Priority       32769  (priority 32768 sys-id-ext 1)
Address                          0001.96C7.DC42
```

Le BID permet à STP de choisir un commutateur Root dans la topologie.

3.2. Bridge System ID Extension

Le "Bridge System ID Extension" qui compose le "Bridge ID" Spanning-Tree du commutateur le rend unique pour chaque VLAN.

4. Algorithme Spanning-Tree

Spanning-Tree calcule une topologie sans boucle en 4 étapes :

1. Sélection d'**un commutateur Root**, un seul par topologie, qui sera le commutateur racine de la topologie, tous ses ports transfèrent le trafic (**ports Designated**). Le commutateur avec **l'identifiant "Bridge ID" (BID) le plus faible** remporte l'élection.

2. Sélection d'**un seul port Root** sur les (autres) **commutateurs non-Root**, qui dispose de la liaison dont le coût vers le commutateur Root est le plus faible. Il est le seul à transférer du trafic.

3. Sélection d'**un port Designated pour chaque segment physique** qui connecte deux commutateurs quand c'est nécessaire. C'est le port qui a le coût vers le commutateur Root le plus faible qui est sélectionné, il est le seul à transférer le trafic.

4. Les ports Root et Designated transfèrent du trafic (**état "Forwarding"**) et **les autres ports coupent la liaison (état "Blocking")**.

4.1. Sélection d'un commutateur Root

Le **commutateur Root (principal)** sera le point central de l'arbre STP. Le choix de celui-ci dans l'architecture du réseau peut avoir son importance. Idéalement, on le choisira dans la couche Distribution.

Par défaut, le commutateur qui aura l'identifiant "Bridge ID" (**BID**) le plus faible sera élu Root.

Si la **priorité STP du commutateur** reste à sa valeur par défaut (32768, `0x08`), la valeur de l'adresse MAC du commutateur sera déterminante.

Le commutateur Root est unique dans la topologie.

Tous ses ports sont en état "Forwarding", transfèrent du trafic.

4.2. Influencer la sélection du commutateur Root

Il est conseillé de choisir laisser l'IOS choisir la priorité du commutateur root principal (`root primary`) et son backup (`root secondary`). On désigne chaque commutateur root principal et secondaire sur les périphériques concernés par ces rôles (en général deux commutateurs redondants de la couche Distribution).

```
(config)#spanning-tree vlan vlan-id root [primary|secondary]
```

Toutefois, on peut toujours fixer la priorité du commutateur (par VLAN) :

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

4.3. Sélection d'un seul port Root sur chaque commutateur non-Root

Les autres **commutateurs non-Root** vont sélectionner **un seul port Root** qui aura le chemin le plus court vers le commutateur Root.

Un port Root est en état "forwarding".

Le coût est calculé inversement à la vitesse de la liaison avec une référence de 20 Gbps. Le coût d'une interface STP est normalement codée par défaut sur 16 bits dans sa version courte (short-mode) qui est le mode de calcul par défaut. Une autre méthode dite "long-mode" utilise une valeur de 32 bits avec une valeur de référence de coût de 20 Tbps. La commande `spanning-tree pathcost method long` en mode de configuration globale active la méthode "long-mode". Cette opération doit alors être réalisée sur tous les commutateurs STP de la topologie.

Vitesse du lien	Coût (short-mode)	Coût (long-mode)
10 Mbps	100 (50 à 600)	2000000
100Mbps	19 (10 à 60)	200000
1Gbps	4 (3 à 10)	20000
10Gbps	2 (1 à 5)	2000
20Gbps	1	1000
100Gbps	1	200
1Tbps	1	20
10Tbps	1	2
20Tbps	1	1

Coût des liaisons

Ce coût peut être modifié.

S'il s'agit d'un port configuré en mode Access (qui connecte un périphérique terminal), la commande de configuration est :

```
(config-if)#spanning-tree cost <cost>
```

S'il s'agit d'un port **en mode Trunk** (qui connecte un autre commutateur pour transporter du trafic de plusieurs VLANs), la commande de configuration est :

```
(config-if)#spanning-tree vlan <vlan-id> cost <cost>
```

Ports Root ex aequo

Sur un commutateur non-Root, pour des interfaces STP en cas de coûts égaux vers le commutateur Root, c'est leur priorité la plus faible (d'une valeur de 0 à 255) qui emporte le choix du port Root (elle est de 128 par défaut) en déterminant l'ID du port composé de 2 octets (priorité + numéro STP du port) :

Sur un port en mode Access :

```
(config-if)#spanning-tree port-priority <priority>
```

Sur un port **en mode trunk** :

```
(config-if)#spanning-tree vlan <vlan-id> port-priority <priority>
```

4.4. Un port Désigné par segment

Pour chaque segment physique, domaine de collision ou lien, il y a **un port Designated**.

Le port Designated d'un segment est celui qui a le chemin le plus court vers le commutateur Root.

Un port Designated est normalement en état "Forwarding", autrement dit, envoie et reçoit du trafic de données.

Tous les autres sont des ports Non-Designated en état "Blocking", c'est-à-dire bloquant tout trafic de données mais restant à l'écoute des BPDU.

5. Spanning-Tree en résumé

- 1 commutateur Root par réseau dont tous les ports sont Designated (Forwarding)
- 1 port Root (Forwarding) par commutateur Non-Root
- 1 port Designated (Forwarding) par domaine de collision (liaison)
- tous les autres ports sont Non-Designated (Blocking)

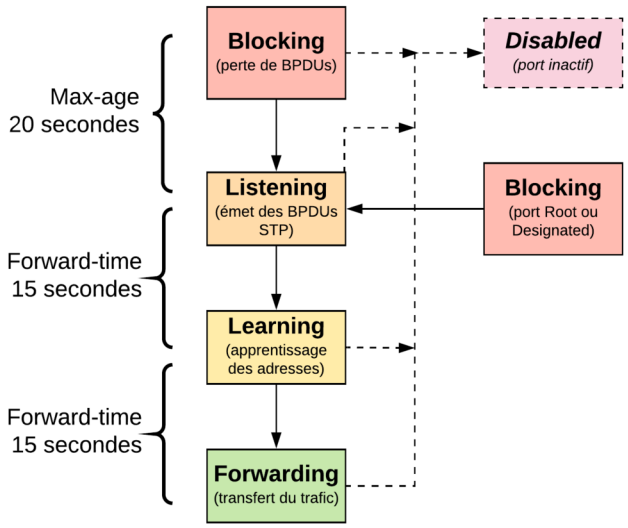
Port	⇋	Port	État	⇋	État	Commutateur	⇋	Commutateur
Root	⇋	Designated	Forwarding	⇋	Forwarding	Non-root	⇋	Root
Designated	⇋	Root	Forwarding	⇋	Forwarding	Non-root	⇋	Non-root
Designated	⇋	Non-Designated	Forwarding	⇋	Blocking	Non-root	⇋	Non-root

6. États Spanning-Tree

Un port démarre en état “Blocking” et peut atteindre l’état “Forwarding” en fonction des BPDUs reçus. L’état “Disabled” est une désactivation administrative ou fait suite à une erreur de sécurité.

États	Délais	Transfert data	Apprentissage MAC	Envoie des BPDUs	A l’écoute des BPDUs, SNMP
Blocking	Max Age = 20 sec.	non	non	non	oui, en attente de BPDUs
Listening	Forwarding Delay = 15 sec.	non	non	oui	oui
Learning	Forwarding Delay = 15 sec.	non	oui	oui	oui
Forwarding	-	oui	oui	oui	oui

6.1. Délais Spanning-Tree



Délais Spanning-Tree

Par défaut, sur les commutateurs Cisco, tous les ports (*switchports*) sont activés en PVST+. Cela signifie qu’un port de commutateur qui se connecte connait les états successifs “Disabled”, “Blocking”, “Listening”, “Learning” et “Forwarding” jusqu’à atteindre un délai de 50 secondes avant de commencer à transférer du trafic. Ce comportement peut être modifié sur les ports Access qui connectent des postes de travail avec la fonction “spanning-tree portfast”.

Mais pourquoi manipuler des délais Spanning-Tree ? À une époque lointaine, on pouvait réaliser du “fine tuning” sur les délais Spanning-Tree pour étendre une topologie ou améliorer sensiblement ses performances. Ce type de projet n’a plus de sens aujourd’hui dans les conceptions hiérarchiques. On aura plutôt tendance à limiter l’étendue de Spanning-Tree entre la couche Access et Distribution et à utiliser sa version rapide, Rapid Spanning-Tree.

On notera enfin que ces délais font partie des informations partagées par les commutateurs. En conséquence, ils doivent être identiques sur tous les commutateurs de la topologie au risque de détériorer le fonctionnement du protocole.

Âge maximum (Max Age)

“Max-Age”, délais avant lequel un port attend avant d’entrer en état “Listening” :

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

De 6 à 200 secondes, 20 secondes par défaut.

Forward Delay

“Forward-time”, élais pour atteindre l’état “Forwarding” :

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

De 4 à 200 secondes, 15 secondes par défaut.

Hello STP

“Hello-time”, fréquence des Hellos STP :

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

De 1 à 10 secondes, 2 secondes par défaut.

7. Messages Spanning-Tree

Les commutateurs s’échangent des “Bridge Protocol Data Units” (BPDU) de deux types :

- **type Configuration** : utilisés lors des élections, pour maintenir la connectivité entre les commutateurs
- **type Topology Change Notification (TCN)** : envoyés auprès d’un commutateur Root pour signaler des ruptures de liens. Quand un commutateur reçoit un TCN, il l’accuse de réception.

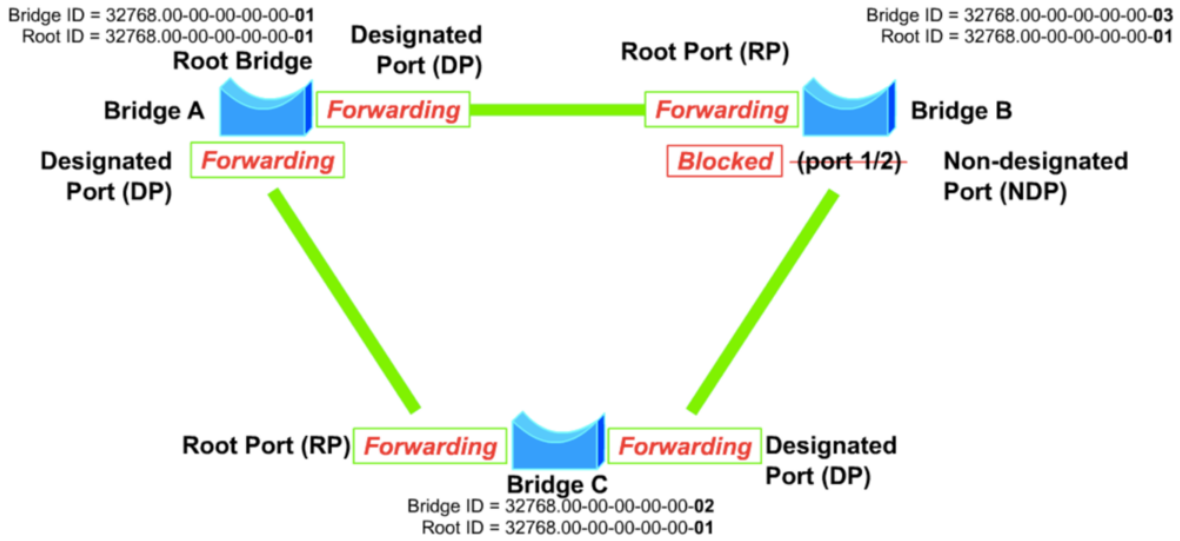
Capture de trafic STP : https ://www.cloudshark.org/captures/add9bb6a43f9

7.1. Charge Spanning-tree

```
IEEE 802.3 Ethernet
Logical-Link Control
Spanning Tree Protocol
    Protocol Identifier: Spanning Tree Protocol (0x0000)
    Protocol Version Identifier: Spanning Tree (0)
    BPDU Type: Configuration (0x00)
    BPDU flags: 0x00
    Root Identifier: 32768 / 1 / 00:19:06:ea:b8:80
    Root Path Cost: 0
    Bridge Identifier: 32768 / 1 / 00:19:06:ea:b8:80
    Port identifier: 0x8005
    Message Age: 0
    Max Age: 20
    Hello Time: 2
    Forward Delay: 15
```

8. Convergence Spanning-Tree

Cette animation historique en flash illustre le fonctionnement de Spanning-Tree :



[Animation Spanning-Tree](images/spanning_tree1.swf)

9. Variantes STP

Protocole	Standard	Convergence	Instances /VLANs
Spanning-Tree (STP)	IEEE 802.1D	Lente	Unique
PVST+	STP Cisco	Lente	Multiple
Rapid Spanning-Tree (RSTP)	IEEE 802.1w	Rapide	Unique
PVRST+	RSTP Cisco	Rapide	Multiple
MST	IEEE 802.1s	Rapide	Multiple

9.1. PVST+

PVST+ est la version Cisco améliorée de STP IEEE 802.1D-2004.

Avec PVST+, il y a une instance STP par VLAN.

PVRST+ est la version améliorée de Rapid Spanning-tree (RSTP).

MST est un standard IEEE 802.1s de l'implémentation propriétaire Cisco de "Multiple Instances Spanning Tree Protocol" (MISTP). MST distribue la charge de plusieurs VLANs sur plusieurs liens STP.

9.2. Rapid Spanning-Tree : RSTP / PVRST+

RSTP / PVRST+ font fait passer le temps de convergence à 6 secondes maximum ce qui les rend beaucoup plus opérationnels que STP.

Pour l'activer, en mode de configuration globale :

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

9.3. Points communs entre RSTP et STP

En général, RSTP fonctionne de la même manière que STP :

- Mêmes règles d'élection du commutateur Root
- Mêmes règles de sélection d'un port Root sur un commutateur non-Root
- Mêmes règles d'un unique port Designated sur un segment physique et les autres en état "Blocking".

9.4. Différences entre RSTP et STP

Les différences par rapport à STP :

1. Il n'y a plus que trois états pour les ports RSTP :
   - **Discarding** (au lieu de Disabled, Blocking et Listening)
   - **Learning** et **Forwarding** (gardant la même fonction)
2. Les rôles port Root et port Designated subsitent. 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. Types. Les ports connectant des périphériques terminaux s'appellent des ports Edge qui remplissent la même fonction que la fonction Portfast en PVST+. Les ports Point-to-Point connectent des commutateurs entre eux. Alors que STP attend passivement des BPDUs pour agir, RSTP négocie le statut des liens rapidement (3 X le Hello Time = 6 secondes).

États Spanning-Tee (802.1d)	**États Rapid STP (802.1w)**
Blocking	Discarding
Listening	Discarding
Learning	Learning
Forwarding	Forwarding

9.5. Captures Rapid Spanning-Tree

On peut voir des paquets RSTP ici : https ://www.cloudshark.org/captures/4d3b1f118872

10. Sécurité et bonnes pratique STP

La commande `Portfast` est une fonctionnalité propriétaire Cisco. Elle s'exécute uniquement sur des ports connectant des périphériques terminaux et dans une infrastructure VLAN uniquement sur des ports en mode Access.

Lorsqu'il est connecté, le port configuré en mode "**Spanning-Tree Portfast**" passe directement de l'état "Blocking" à l'état "Forwarding". STP Portfast comporte aussi l'avantage de ne pas transférer de BPDUs TCN inutiles et de monter une interface sans passer par les délais STP.

La commande d'activation s'exécute en configuration d'interface :

```
(config-if)#spanning-tree portfast
```

Le message qui suivra indique la précaution d'usage afin d'éviter des boucles.

```
%Warning: portfast should only be enabled on ports connected to a single host. Connecting hubs, concen\
trators, switches, bridges, etc... to this interface  when portfast is enabled, can cause temporary br\
idging loops. Use with CAUTION %Portfast has been configured on FastEthernet0/X but will only have eff\
ect when the interface is in a non-trunking mode.
```

10.1. Portfast BPDU Guard

La fonctionnalité “Portfast” n’empêche pas de connecter un commutateur “pirate”.

Afin de limiter plus strictement sa topologie STP, on peut utiliser le mode Portfast “**BPDU Guard**” : le port Portfast qui reçoit des BPDU se mettra en mode “err-Disabled”.

Ce mode est désactivé par défaut et s’active sur un modèle C2960 :

```
(config-if)# spanning-tree bpduguard enable
```

On notera que les commandes `spanning-tree portfast default` et `spanning-tree bpduguard default` en configuration globale activent par défaut ces modes sur tous les ports Access.

```
(config)#spanning-tree portfast default
(config)#spanning-tree portfast bpduguard default
```

10.2. BPDU Filter, Root Guard, Loop Guard, UplinkFast

Alors que “Porfast” force un port Access à passer d’un état Blocking ou Discarding à l’état Forwarding et “BPDU guard” protège le port de la réception de BPDU, on trouvera d’autres fonctionnalités que l’on peut citer : BPDU Filter, Root guard, Loop Guard et UplinkFast.

- “**BPDU Filter**” : élimine tous les BPDU sur le port du commutateur (fonctionnalité rarement déployée et incompatible avec BPDU Guard)
- “**Root Guard**” : empêche qu’un nouveau Switch Root soit élu à travers ce port. On l’applique sur toutes les interfaces des switches Root qui connectent des switches non-Root, sur des interfaces en mode access, soit sur toute interface de laquelle il ne peut pas y avoir de commutateur Root à élire : `(config)#interface GigabitEthernet0/0 (config-if)#spanning-tree guard root`
- “**Loop Guard**” : on l’applique sur toutes interfaces qui sont ou qui pourraient devenir nondesignated. Loop Guard ne peut pas être utilisé avec Root Guard.
- “**UplinkFast**” : active la convergence rapide quand un lien direct vers un autre commutateur tombe.

11. Diagnostic Spanning-Tree

- Vérification du protocole *ieee* (pvst) ou *rstp* (rapid-pvst)
- Identification du VLAN
- Identification du BID du commutateur
- Identification du Root ID
- Correspondance des délais (Hello Time, Fordward Delay, Max Age)
- État des ports
- Rôle des ports

11.1. Diagnostic de base

```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     0001.96C7.DC42
             Cost        4
             Port        26(GigabitEthernet1/2)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0001.4373.1102
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/1            Altn BLK 4         128.25   P2p
Gi1/2            Root FWD 4         128.26   P2p
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p


AS1#show spanning-tree vlan 10 active

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    24586
             Address     0c2a.e87a.9300
             Cost        3
             Port        65 (Port-channel1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     0c2a.e823.3800
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi2/0               Desg FWD 4         128.9    P2p Edge
Po1                 Root FWD 3         128.65   P2p
Po2                 Altn BLK 3         128.66   P2p
```

Où on identifie :

- Version de Spanning-Tree : `protocol ieee` ou `protocol rstp`
- Le Root ID sur la ligne `Root ID`
- Les délais `Hello Time`, `Max Age` et `Forward Delay`
- le `Bridge ID` local
- Le rôle des interfaces
- Le statut des interfaces
- Le coût des interfaces `Cost`, ainsi que leur priorité locale `Prio.Nbr`

La sortie de cette commande `show spanning-tree` fournit la plupart du temps les informations nécessaires à la vérification et au dépannage du protocole Spanning-Tree en Cisco IOS.

11.2. 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
```

Vérification générale de Spanning-Tree :

```
S1#show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
Extended system ID                     is enabled
Portfast Default                       is edge
Portfast Edge BPDU Guard Default       is disabled
Portfast Edge BPDU Filter Default      is disabled
Loopguard Default                      is disabled
PVST Simulation Default                is enabled but inactive in pvst mode
Bridge Assurance                       is enabled but inactive in pvst mode
EtherChannel misconfig guard           is enabled
Configured Pathcost method used is short
UplinkFast                             is disabled
BackboneFast                           is disabled

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                    0         0        0          2          2
VLAN0010                    0         0        0          3          3
VLAN0099                    0         0        0          2          2
---------------------- -------- --------- -------- ---------- ----------
3 vlans                     0         0        0          7          7
```

12. Références STP

- IEEE 802.1D™-2004 IEEE Standard for Local and Metropolitan Area Networks—Media access control (MAC) Bridges (Incorporates IEEE 802.1t™-2001 and IEEE 802.1w™)
- http ://packetlife.net/captures/protocol/stp/
- Understanding Multiple Spanning Tree Protocol (802.1s)
- Understanding Rapid Spanning Tree Protocol (802.1w)
- Understanding and Tuning Spanning Tree Protocol Timers

Quatrième partie Disponibilité dans le LAN

Cette partie tente de répondre à la question de la robustesse des liaisons au sein des réseaux locaux au niveau des passerelles par défaut avec HSRP, au niveau de la couche 2 (L2) avec Spanning-Tree, au niveau de la couche physique (L1) avec Etherchannel et au niveau de la couche 3 (L3) avec le routage (statique) IPv4 et IPv6. Il reprend des principes d'architecture hiérarchique et modulaire des réseaux.

Pour visualiser correctement l'enjeu de ces solutions dans les réseaux commutés, on rappellera ce tableau récapitulatif des solutions de haute disponibilité dans le LAN.

Couche	Protocole/Solutions	Délais de reprise
L1	Etherchannel	Plus ou moins 1 seconde pour rediriger le trafic sur un lien alternatif
L2	Rapid Spanning Tree	Quelques secondes
L3	First Hop Redundancy Protocols comme HSRP, VRRP, GLBP	10 secondes par défaut (Cisco) mais le constructeur conseille 1s hello time, 3s Hold Time
L3	Protocoles de routage	En dessous de la seconde avec OSPF ou EIGRP

4. Solutions de disponibilité dans le LAN

Dans ce chapitre introductif de conception des réseaux locaux, on identifiera les différents modèles de conception dans lesquels interviennent les solutions de disponibilité dans le réseau local (LAN) telles que Etherchannel, Rapid Spanning-Tree, HSRP et le routage IP. Le propos développé ici invite au déploiement de ces topologies dans des exercices de laboratoires. On ne manquera enfin de rappeler le principe de la sécurité par conception.

1. Solutions de disponibilité dans le LAN

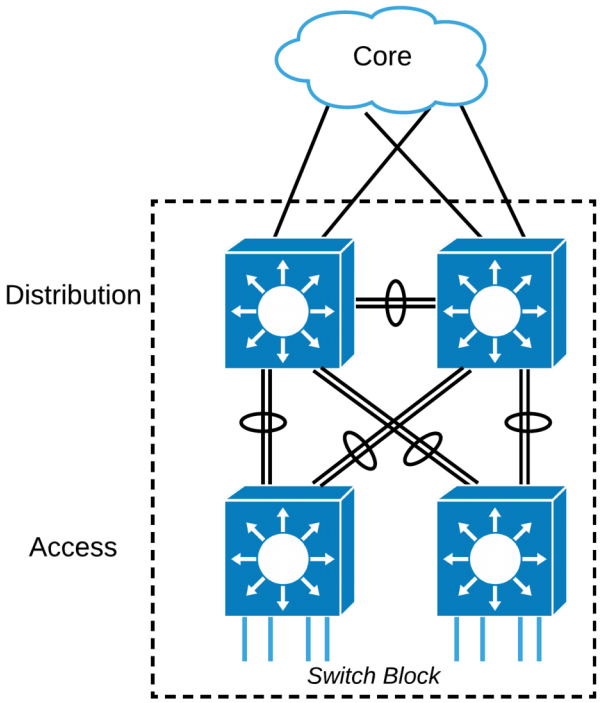
Les solutions de redondance dans le LAN qui contribuent à la haute disponibilité[1] dans les réseaux LAN sont les suivantes : Etherchannel, Rapid Spanning Tree, HSRP ou VRRP et les protocoles de routage.

Couche	Protocole/Solutions	Délais de reprise
L1	Etherchannel	Plus ou moins 1 seconde pour rediriger le trafic sur un lien alternatif
L2	Rapid Spanning Tree	Quelques secondes
L3	First Hop Redundancy Protocols comme HSRP, VRRP, GLBP	10 secondes par défaut (Cisco) mais le constructeur conseille 1s hello time, 3s Hold Time
L3	Protocoles de routage	En dessous de la seconde avec OSPF ou EIGRP

2. Redondance de couche 1

Etherchannel peut cumuler plusieurs liaisons physiques (L1) en terme de fiabilité et de charge. Chaque groupe Etherchannel est vu comme une interface logique pour le commutateur. Du point de vue de Spanning-Tree, ce sont les interfaces “Port-Channel” qui seront prisent en compte dans le calcul d’une topologie sans boucle. Dans ce cadre, Etherchannel contribue à simplifier les topologies Spanning-Tree.

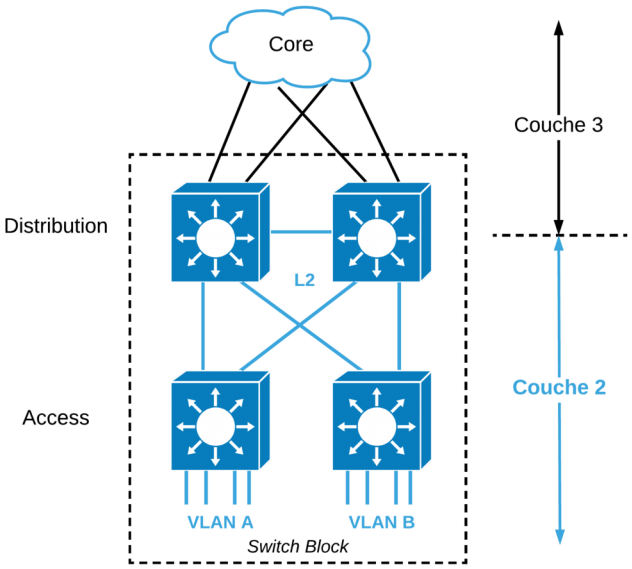
1. Le jargon disponibilité, haute disponibilité (HA), Tolérance aux pannes (FT), redondance, robutesse, résilience, taux de disponibilité ou d’indisponibilté, point unique de rupture (single point of failure), isolation des pannes, plan de reprise d’activité, plan de continuité d’activité est un sujet en soi.



Redondance couche 1

3. Redondance de couche 2

Spanning-Tree est activé par défaut sur les commutateurs Cisco. Il se déploie habituellement pour assurer la redondance entre la couche Access et la couche Distribution. Le routage IP — soit la couche 3 (L3) — intervient entre la couche Distribution et la couche Core. On activera de préférence des protocoles comme Rapid STP ou MST dont les délais de reprise pourraient en satisfaire certains.

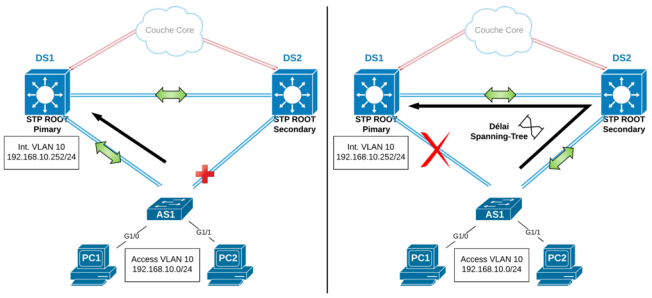


Redondance de couche 2

Ici, les VLANs *peuvent* s'étaler sur les commutateurs Access et le réseau est physiquement "bouclé". Dans une situation idéale, une seule liaison est activée entre la couche Access et la couche Distribution. Grâce à Spanning-

Tree avec les deux commutateurs configurés “Root Primary” pour certains VLANs et “Root Secondary” pour d’autres, l’un peut reprendre le rôle “root” pour l’autre et on peut distribuer la charge de plusieurs VLANs sur des liaisons alternatives. Toutefois, si une connexion vers la couche Distribution tombe, le trafic du VLAN impliqué passera par le “Trunk” alternatif cumulant le trafic de tous les VLANs et passera par un commutateur intermédiaire pour joindre son ancien commutateur “root”. On imagine que la rapidité de Spanning-Tree est un enjeu dans ce type de topologie.

Dans la figure suivante, le trafic du VLAN 10 passe de manière optimale par DS1. En effet, DS1 est “root primary” pour le VLAN 10. L’interface de AS1 qui pointe sur DS2 est nécessairement “non-designated” et en état STP “Blocking”. Toutefois, si la connexion entre AS1 et DS1 venait à tomber, le trafic du VLAN 10 vers DS1 passerait de bout en bout par le “trunk” entre AS1 et DS2 et puis par le “trunk” entre DS2 et DS1.



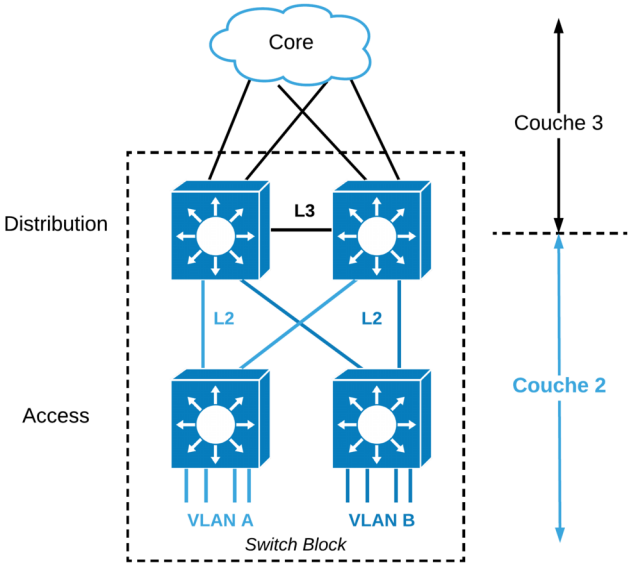
Les VLANs “éparpillés” continuent à communiquer entre eux mais leur passerelle reste un point unique de rupture. Dans ce cadre, un protocole de redondance du premier saut (First Hop redundancy Protocols, FHRP) comme HSRP, VRRP ou GLBP assure la redondance de la passerelle et le nouveau commutateur root (secondaire) peut prendre en charge le routage des paquets.

4. Redondance de couche 3

Si l’on imagine que l’un peut devenir passerelle pour l’autre de manière cohérente grâce à HSRP, on disposera d’une mesure de protection en cas de passerelle totalement indisponible. S’il ne s’agit jamais que d’une rupture entre le commutateur Distribution et le commutateur Access, c’est Spanning-Tree qui entrera jeu de manière relativement rapide mais toujours moins que le routage ou HSRP. La passerelle sera toujours joignable mais le trafic passera par un chemin sous-optimal dépendant de Rapid Spanning-Tree et de son délai (jusqu’à 6 secondes). Dans ce type d’architecture courante, il est nécessaire que les commutateurs Root et la passerelle par défaut (HSRP ou VRRP) correspondent.

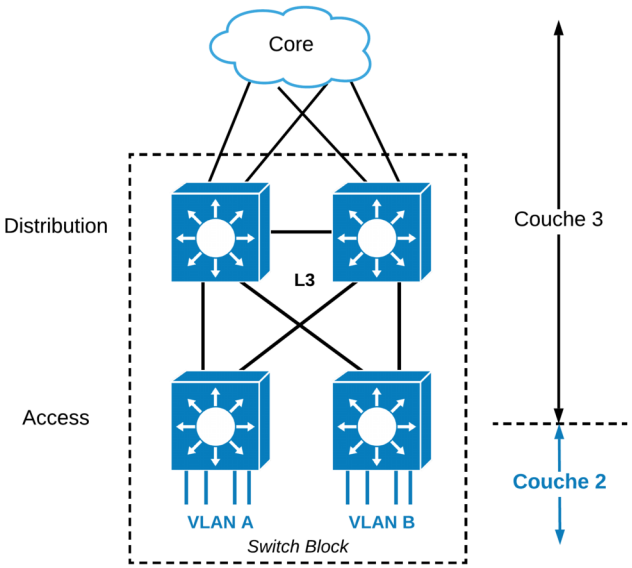
Une autre solution de conception consiste à diminuer l’étendue de la couche 2, soit de Spanning-Tree dans la couche distribution, une “topologie sans boucle de couche 2”. Spanning-Tree est toujours présent par mesure de précaution et éventuellement pour répondre à une bonne pratique. On sera attentif au fait que ce type d’architecture exige que les IDs VLANs ne s’étendent pas sur plusieurs commutateurs de couche Access, ces IDs devant être alors uniques sur chacun d’eux. La gestion des VLANs devient alors locale aux commutateurs d’accès.

Dans la figure suivante, chaque VLAN est strictement déployé sur un commutateur Access. Un lien L3 entre les commutateurs Distribution coupe naturellement la boucle Spanning-Tree L2 selon un “modèle HSRP” (Layer 2 Loop-Free Topology). Les routeurs HSRP redondants dans la couche Distribution se voient à travers la couche Access.



Redondance de couche 2 sans boucle

Aussi, pourquoi maintenir des liaisons L2 entre la couche Access et Distribution si les VLANs se limitent localement sur les commutateurs d'accès et ne s'éparpillent pas ? On peut alors considérer du routage IP statique par défaut vers les commutateurs de couche Distribution à partir des commutateurs Access. Par défaut Spanning-Tree sera maintenu, mais il ne disposera plus de rôle critique dans une infrastructure entièrement routée dans le réseau local.



Redondance de couche via routage IP

Dans ce type de déploiement, la couche Access assure les fonctions de routage IP.

5. Redondance des liaisons L3 (Routage)

Des interfaces routées redondante, c'est-à-dire des liaisons redondantes auxquelles on a attribué des adresses IP comme les interfaces des routeurs ou encore des interfaces `no switchport` des commutateurs pourraient aider à atteindre un niveau de disponibilité suppérieur.

Dès qu'une interface IP connait des problèmes L1/L2 comme une interruption physique, le routeur ou le commutateur retirera immédiatement l'interface problématique de sa table de routage comme interface de sortie. Toutes les routes associées à cette interface seront supprimées, ce qui aura pour effet de répartir le trafic sur les meilleures

liaisons alternatives. Si des routes statiques étaient associées à cette interface, elles seront supprimées (voir routes flottantes) ; si des routes apprises par un protocole de routage étaient associées à cette interface, elles disparaîteront également de la table de routage mais cela ne signifie pas nécessairement que le chemin alors choisi sera optimal.

Faudra-t-il encore que la méthode de routage puisse s'adapter de manière efficace afin de créer **une topologie de transfert sans boucle** dans **les plus brefs délais**, réduisant ce que l'on appelle le délai de convergence. Plus la convergence est lente, plus le taux de disponibilté chutera. Seuls OSPF ou EIGRP peuvent répondre à ces deux critères anti-bouclage et rapidité. RIP, quel que soit sa version, sera à la fois particulièrement sensible aux boucles de routage et lent à "converger".

Aussi, le routage dynamique et ses protocoles comme OSPF ou EIGRP sur matériel Cisco sont capables de répartir la charge du trafic vers une même destination sur plusieurs liaisons équivalentes de manière efficace. EIGRP est même capable d'utiliser des liaisons plus coûteuses à condition que celles-ci soient réputées sans boucle. Cette technique appelée dans le jargon "Unequal Load Balancing" permettrait de répartir la charge de trafic proportionnellement au coût des meilleures laisons alors que celle-ci n'aurait jamais été utilisée avec une répartion de charge égale (la seule disponible en OSPF). Cette fonctionnalité EIGRP remarquable, associée concept de *variance*, demande réflexion avant déploiement car son usage pourrait avoir des effets secondaires ("effets de bord"), indésirables, coûteux ou inattendus. En cas de doute, le support technique de Cisco Systems est à votre écoute.

6. La sécurité par conception

Enfin, la mise en oeuvre de tous ces protocoles L1/L2/L3 exigerait que l'on se pose une question préalable, bien réelle : si des éléments extérieurs venaient à se connecter à l'infrastructure, est-ce qu'ils pourraient discuter librement avec ces protocoles CDP, VTP, 802.1q, DTP, HSRP, VRRP, EIGRP, OSPF ? Si cela était le cas, ces éléments extérieurs pourraient endommager l'infrastructure, redigirer du trafic sur de mauvais chemins ou encore s'immiscer dans les communications de manière involaire ou malveillante.

Nombreux sont les cas de rupture de service connus suite à la connexion d'un périphérique externe (pirate ou non) au réseau qui devient STP Root détruisant ainsi la topologie initiale. Des périphériques de communication domestiques ou venant d'opérateurs sont parfaitement capables de fonctionner en Spanning-Tree par exemple. Qui des professionels des réseaux n'a jamais connu l'expérience d'une tempête de Broadcast ? Les commutateurs pirates et les périphériques non autorisés sont légions dans certains réseaux d'entreprise, surtout s'ils sont hétérogènes.

Dans leur plus simple configuration, telle que certains diplômes CCNA les présentent, ces protocoles d'infrastructure et de contrôle sont particulièrement crédules. Au moment de la conception, et il n'est probablement jamais assez tôt comme trop tard pour y penser, on se souciera des interactions autorisées sur le plan du contrôle et de la gestion : authentification des message, filtrage basé sur la provenance ou la nature des messages, etc. Cette démarche demande simplement d'intégrer l'aspect sécurité dans la conception.

Il est d'ailleurs trivial de démontrer les vulnérabilités des configurations faibles en sécurité, des configurations qui laissent subsister des paramètres par défaut ou des environnements qui n'ont pas été audités. Les contre-mesures des fabricants comme Cisco sont à diposition des utilisateurs, bien souvent disponibles sans frais supplémentaires. Mais leur mise en place demandent un investissement en matière de compétences techniques et culturelles, et surtout en temps.

Alors que les commutateurs ont pour fonction principale de transférer le plus rapidement possible le trafic L2 au sein du réseau, ceux-ci ont acquis au fil du temps des fonctions L3 de routage et de services IP, et puis des fonctions de sécurité et de vérification du trafic de plus en plus avancées. Si les fonctions de bas niveau sont assurées par des puces dédiées comme des ASICs, les commutateurs d'entreprise deviennent de puissants ordinateurs du réseau, notamment dans les gammes de périphériques Cisco.

Enfin, la mise en place d'une solution de surveillance qui journalise les événements et qui est capable de les rapporter afin de remonter des alertes, de les analyser pour vérifier l'état de santé de l'infrastructure entière, ou encore pour remédier automatiquement ou non aux problèmes constatés, etc. est partie intégrante d'une conception sécurisée du réseau. Mais de nouveau, ce type de projet aussi avancé demande un certain investissement en compétences et en temps.

De nouveaux modèles d'infrastructures comme SDN ou des solutions basées sur les technologies en nuage ou qui s'en inspirent facilitent réellement ce type de gestion. Il y a toujours de la place pour des outils de surveillance comme

Nagios ou Zabbix par exemple, mais de nouveau outils dotés de capacités de collecte, d'analyse, de présentation et de réaction aux événements du réseau ont fait récemment leur apparition. Ces derniers s'intègrent aux solutions traditionnelles de surveillance qui utilisent Syslog et SNMP mais ajoutent des nouvelles méthodes de collecte, de stockage, de traitement et de présentation de données qui correspondent aux attentes du marché. On imagine alors les capacités nécessaires et la maintenance en soi de telles solutions. Heureusement, l'Open Source démocratise des solutions qu'à une époque seules les entreprises les plus fortunées pouvaient se payer. On citera par exemple projet netdata.io.

Cinquième partie Technologies WLAN

Cette partie porte sur les technologies Wireless LAN (WLAN) des réseaux sans-fil locaux, dont fait partie ce qu'on appelle le Wi-Fi. On y trouvera un exposé de présentation générale du domaine, des informations sur les aspects normatifs (IEEE 802.11), sur les topologies logiques et les modèles de déploiement, sur les aspects physiques (bande de fréquence, non-overlapping, antennes), sur les aspects de configuration des clients, sur les aspects de sécurité WPA, et enfin sur les aspects de gestion au sein d'un réseau local.

5. Introduction aux technologies WLAN

Ce chapitre d'introduction tente de présenter rapidement le concept de Wireless LAN (WLAN), les standards IEEE 802.11 et celui de Wi-Fi. On positionnera également ces technologies dans le modèle OSI au niveau de la couche (L1) et la couche 2 accès au réseau (L2) qui détermine les méthodes d'accès au support (MAC). Le standard IEEE 802.11i embarque nativement la sécurité de couche 2 en matière d'authentification et de chiffrement. On évoquera enfin des questions de déploiement opérationnel.

1. Technologies Wireless LAN (WLAN), IEEE 802.11 et Wi-Fi

Les technologies sans-fil (de réseau local), dites communément Wireless LAN (WLAN), reposent essentiellement sur un seul standard, celui du groupe de travail IEEE 802.11.

La *Wi-Fi Alliance* est une autre organisation, un consortium commercial qui s'occupe d'assurer l'interopérabilité du matériel respectant le standard IEEE 802.11 venant de différents fabricants.

Organismes de régulation, standardisation et compatibilité

On parlera plus volontiers de "IEEE 802.11" dans le cadre de discussions sur le protocole et son fonctionnement.

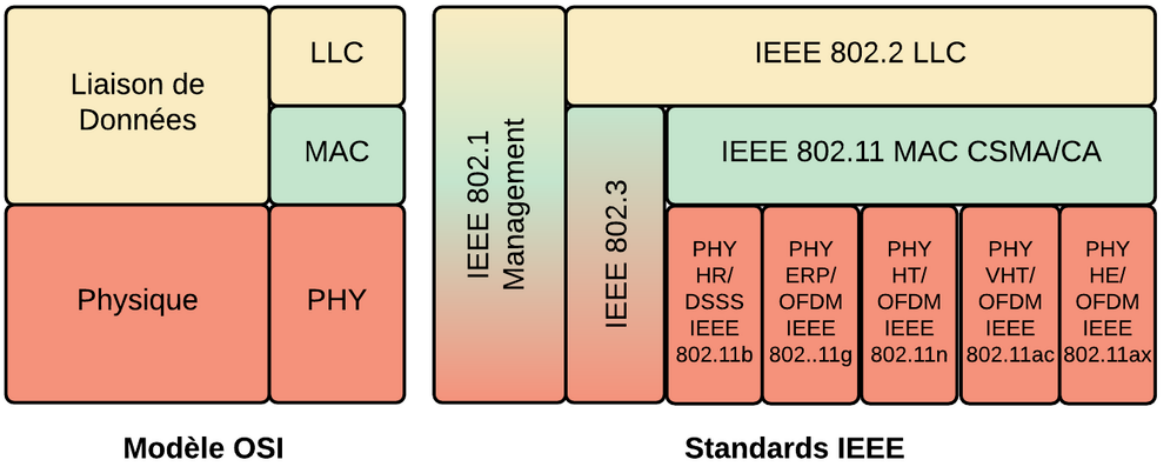
On lira dans la documentation le terme "WLAN" ("Wireless LAN") à propos d'architectures de déploiement et de solutions de fabricants tels que Cisco ou HPE/Aruba.

On utilisera le terme "Wi-fi" ou encore "Wifi" pour désigner une technologie sans fil ou un périphérique respectant le standard IEEE 802.11 de manière interopérable. Toutes ces désignations font référence aux technologies d'Accès qui permettent de se connecter à un réseau local sans-fil de manière mobile en cette nouvelle décennie 2020.

On notera enfin que d'autres technologies utilisent aussi les ondes radio sur les mêmes fréquences ou sur d'autres fréquences que le Wi-Fi. Elles peuvent être issues du même groupe de travail IEEE 802, comme *Bluetooth* (IEEE 802.15) pour le WPAN (Personal, mais aussi avec *Zigbee* ou *Z-Wave*) ou *WiMax* (IEEE 802.16) pour le WWAN (Wide) pour des objectifs différents. Il existe bon nombre d'autres technologies qui utilisent l'air comme support de transmission : les satellites, les réseaux cellulaires, etc.

2. Protocoles IEEE 802.11

La technologie WLAN du standard IEEE 802.11 couvre la couche "Accès au réseau" du modèle TCP/IP ou les couches "Physique" (L1) et "Liaison de données" (L2) du modèle OSI.



Couche Accès IEEE 802.11

Tout comme IEEE 802.3 (Ethernet), IEEE 802.11 précise la couche physique par des caractéristiques de bande de fréquence, de modulation et d'encodage qui offrent des capacités de transport. On trouvera dans ce tableau les standards IEEE 802.11, leur génération, leur bande de fréquence, la vitesse pour un flux et le nombre de flux simultanés supportés (en théorie).

Standard IEEE 802.11	Génération	Bande de fréquence	Vitesse négociée (1 flux)	Flux MIMO
IEEE 802.11b	Wi-Fi 1	2,4GHz	11 Mbps	-
IEEE 802.11a	Wi-Fi 2	5GHz	54 Mbps	-
IEEE 802.11g	Wi-Fi 3	2,4GHz	54 Mbps	-
IEEE 802.11n	Wi-Fi 4	2,4GHz (5GHz)	150 Mbps	4
IEEE 802.11ac	Wi-Fi 5	5GHz	866 Mbps	8
IEEE 802.11ax	Wi-Fi 6	2,4GHz-5GHz	1147 Mbps	8

Au niveau de la sous-couche MAC, le standard IEEE 802.11 propose une méthode d'accès au support (medium) qui est bien différente de celle d'Ethernet. Sur le plan strictement protocolaire, alors que le standard Ethernet IEEE 802.3 utilise CSMA/CD (Carrier Sense Multiple Access with Collision Detection) qui vise à détecter des accès concurrents sur un fil, le standard Wi-Fi IEEE 802.11 se propose d'éviter les collisions avec **CSMA/CA** pour "Collision Avoidance" sur un support partagé comme l'air, avec des mécanismes de contention.

3. Sécurité IEEE 802.11i

Par nature, les transmissions des réseaux sans-fil se propagent en dehors du confinement d'une zone physique telle qu'un bâtiment ou un niveau d'étage. Ces transmissions pourraient parvenir de manière indiscrète à des interfaces tierces à l'organisation, car elles seraient situées dans la zone de couverture radio de l'oragnisation.

À la suite des premières faiblesses publiées du WEP (Wired Equivalent Privacy), la sécurité embarquée du protocole

IEEE 802.11 (1999), un nouveau standard de sécurité **IEEE 802.11i** a été ratifié en “draft standard” en 2004 en remplacement du protocole vulnérable.

L’implémentation du protocole IEEE 802.11i est assurée par la Wi-Fi Alliance à travers les programmes de certification WPA, WPA2, WPA3 en vue d’assurer la transition matérielle et opérationnelle vers de nouveaux protocoles de sécurité. WPA, WPA2, WPA3 assurent au niveau de la couche 2 (L2) les fonctions de sécurité suivante :

- l’authentification comme contrôle d’accès
- le chiffrement du trafic pour la confidentialité
- l’intégrité des messages (MIC, Message Integrity Check)

4. Caractéristiques des technologies d’accès au réseau sans fil (WLAN)

Un réseau sans-fil devrait répondre à différentes caractéristiques en ce qui concerne :

- l’expérience utilisateur essentielle en terme de mobilité, de sécurité et de qualité de service
- la nature du support comme l’air
- les architectures WLAN en termes d’intégration et de gestion

5. Expérience utilisateur

- Mobilité : les utilisateurs devraient accéder aux facilités du réseau à partir de n’importe quel périphérique, d’autant plus s’il est mobile. L’expérience mobile devrait être comparable à celle du LAN filaire.
- Sécurité : les utilisateurs devraient être authentifiés et leur trafic devrait être sécurisé (chiffré et authentifié) de manière forte selon des politiques de sécurité définies.
- Qualité de service : la disponibilité du réseau est assurée par de la redondance, de la gestion des congestions et un dimensionnement adapté des liaisons et de la couverture radio.

6. Support comme l’air

Le support de transmission des technologies sans fil est l’air, comme espace physique partagé par un ensemble d’utilisateurs. Cet espace dispose de limites par rapport aux réseaux filaires d’entreprise :

- L’accès au support est partagé en Half-Duplex entre les candidats au placement du trafic.
- Le support est sensible aux interférences radio.
- Il offre un accès ouvert, par nature : les ondes radio ne sont pas confinées sur un câble qui serait intrinsèquement privé (pas nécessairement confidentiel ou chiffré), les écoutes, indiscrétions et usurpations étant aisées à mettre en oeuvre.
- Un réseau Wi-Fi d’entreprise se passe difficilement d’une infrastructure filaire sous-jacente.

7. Architectures WLAN

En entreprise, différents éléments font que des architectures de réseau sans fil soient adaptées au-delà du protocole initial IEEE 802.11 :

- L'intégration aux environnements filaires,
- le grand nombre de points d'accès à gérer,
- la gestion des profils des utilisateurs,
- la gestion de la qualité de service et
- la gestion de la sécurité.

Le marché et notamment Cisco Systems, en titre de "Leader" parmi beaucoup d'acteurs, construisent et proposent des solutions qui se fondent sur le standard et sur bien d'autres protocoles et mises en oeuvre. Cisco Systems propose aussi ses solutions propriétaires qui peuvent être portées en standard IEEE ou IETF.

Avec le temps, les fabricants de matériel deviennent des fournisseurs de services de connectivité LAN/WLAN : avec du matériel d'infrastructure propriétaire et adpaté, les clients sont invités à profiter des fonctionnalités avancées avec des abonnements à des services. Les solutions deviennent de plus en plus ouvertes, offrant des APIs bien documentées et de nombreuses facilités.

8. Éléments d'architecture WLAN

Pour construire une architecture Wireles LAN d'entreprise, différents éléments d'infrastructure doivent être présents :

- Pontage IEEE 802.1 et Etherchannel
- Composants des réseaux WLAN
- Protocole de contrôle et Overlay WLC-AP
- Protocoles d'authentification

8.1. Pontage IEEE 802.1 et Etherchannel

Le standard IEEE 802.11 est supporté par le cadre des protocoles de pontage IEEE 802.1 pour l'infrastructure.

- IEEE 802.1D : MAC Bridges (Spanning-Tree)
- IEEE 802.1p : mutualisé avec 802.1D-2004, Traffic Class Expediting and Dynamic Multicast Filtering
- IEEE 802.1Q : Virtual LANs
- IEEE 802.1s : mutualisé avec 802.1Q-2003, Multiple Spanning Trees
- IEEE 802.1t : mutualisé avec 802.1D-2004, 802.1D Maintenance
- IEEE 802.1v : mutualisé avec 802.1Q-2003, VLAN Classification by Protocol and Port
- IEEE 802.1w : mutualisé avec 802.1D-2004, Rapid Reconfiguration of Spanning Tree
- IEEE 802.1X : 2001 Port Based Network Access Control

- IEEE 802.1AB : Station and Media Access Control Connectivity Discovery (LLDP)
- IEEE 802.1ad : Provider Bridging
- IEEE 802.1AE : MAC Security

Etherchannel IEEE 802.3ad.

8.2. Composants des réseaux WLAN

- Périphériques Clients
- Points d'accès
- Un environnement physique
- Wireless Controller LAN

8.3. Protocole de contrôle et Overlay WLC-AP

- CAPWAP
- LWAPP

8.4. Protocoles d'authentification

- EAP : PEAP, …
- Une infrastructure à clé publique (PKI)
- Serveur d'authentification Radius
- Base de donnée d'utilisateurs (Local, LDAP, Annuaire fédéré, …)

Révisions

Ethernet

- ~~Connexions (Ethernet shared media et point-to-point)~~
- ~~Concepts sur PoE~~
- ~~Identifier les problèmes d'interface et de câbles (collisions, errors, mismatch duplex, et/ou speed)~~

WLAN

- ~~Décrire les principes des réseaux sans-fil (Nonoverlapping Wi-Fi channels, SSID, RF, Encryption)~~
- ~~Comparer les architectures Cisco Wireless Architectures et les modes des APs~~
- ~~Décrire les connexions physiques d'infrastructure des composants WLAN (AP,WLC, access/trunk ports, et LAG)~~
- Décrire les connexions des accès de gestion des APs et du WLC (Telnet, SSH, HTTP,HTTPS, console, et TACACS+/RADIUS)
- Configurer les composants d'un accès au LAN sans-fil pour la connectivité d'un client en utilisant un GUI seulement pour la création du WLAN, les paramètres de sécurité, les profiles QoS et des paramètres WLAN avancés