

LAN – conception Cisco

Principes de conception LAN

Les principes de conception des réseaux LAN (LAN Design) de Cisco propose un modèle de conception hiérarchique et modulaire à trois couches :

Access, Distribution et Core.

Modèles de conception

L'infrastructure LAN devrait être :

- Robuste
- Évolutive
- Sécurisée
- Gérée

L'infrastructure devrait répondre à plusieurs critères.

Elle est documentée et basée sur un modèle de conception.

Elle est robuste avec une redondance L1, L2 et L3.

Elle est évolutive avec une possibilité de déployer une architecture VLAN.

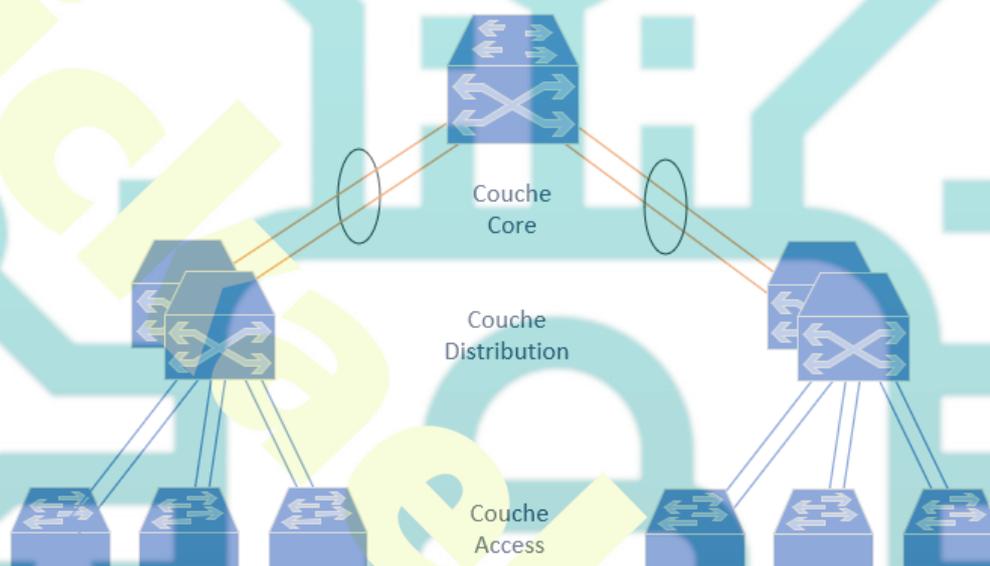
Elle est sécurisée, documentée et dispose de mécanismes d'authentification forte.

But d'un modèle de conception

Que ce soit OSI, IEEE, TCI/IP ou Cisco, un modèle de conception sert à construire des réseaux en respectant certaines règles d'architecture qui leur permettent de répondre aux besoins actuels et futurs des entreprises et de leurs utilisateurs.

Si un modèle de conception facilite le déploiement, la configuration, la maintenance et la mise à jour des infrastructures, on considérera aussi que l'usage d'un tel modèle facilite les achats de matériels et de services.

Modèle hiérarchique en 3 couches

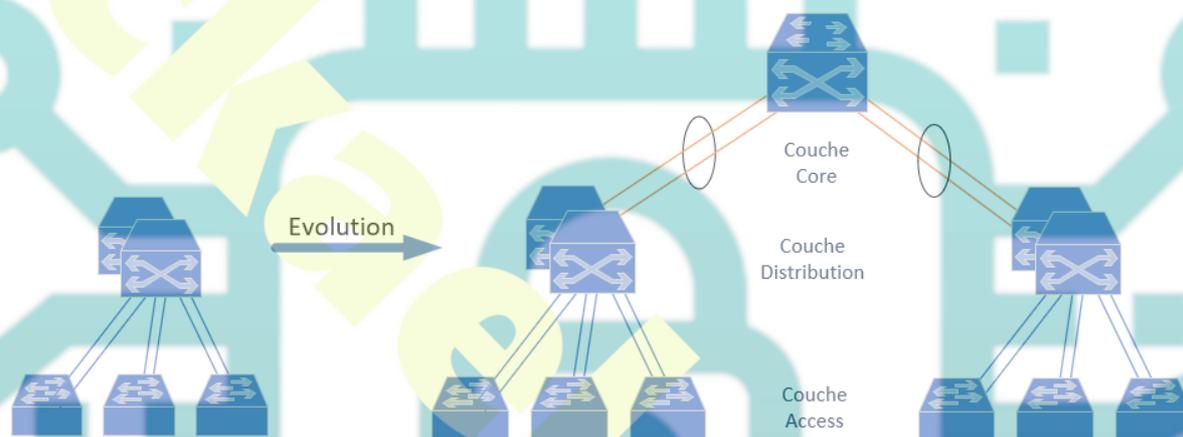


- La couche **Core** est la couche supérieure (backbone à haute vitesse). Elle fournit de la haute disponibilité et s'adapte rapidement aux changements. **Son rôle est simple, elle doit relier entre eux les différents segments du réseau, comme Internet, les sites distants via des WAN ou des MAN, les LAN ou les étages d'une société.** Elle doit transférer les données le plus rapidement possible. On y trouve des routeurs et/ou gros switches.
- La couche **Distribution** qui agrège les connexions des locaux techniques. **Son rôle est simple : limiter les zones de broadcast, filtrer, router, autoriser ou non les paquets...** Nous sommes entre la couche Core et la couche Access, c'est-à-dire entre la partie « liaison » et la partie « utilisateurs ». Ici, on commence à diviser le réseau en segment, en ajoutant plusieurs routeurs/switches de distribution, chacun étant connecté au Core d'un côté, et à la couche Access de l'autre. On utilise des commutateurs pour segmenter et organiser le système d'information en groupes, profils utilisateurs et afin d'isoler les problèmes. On y trouve soit des routeurs, soit des switches en fonction de la taille du réseau.
- La couche **Access** qui permet aux utilisateurs d'accéder aux périphériques du réseau. **Doit attribuer des VLAN, sécuriser les ports.**

Architecture modulaire et évolutive

Chaque couche fournit différentes fonctionnalités et capacités du réseau. Selon la taille du réseau, on aura besoin d'une, deux ou trois couches. Quel que soit le nombre de couches nécessaires, le plus important est que chaque couche fournisse les mêmes services selon les mêmes règles de conception.

Concevoir un réseau de manière modulaire permet de le faire évoluer de manière robuste et redondante.



Cette conception répond à une situation réelle d'un "Campus LAN", soit une architecture du réseau qui correspond à plusieurs bâtiments contigus interconnectés entre eux sous une même administration. On y trouve du trafic utilisateur, du trafic de communications unifiées, du trafic de gestion, du trafic VDi (virtualisation), du trafic critique et des accès aux utilisateurs mobiles, etc.

La couche Core interconnecte les bâtiments et les services offerts sur le réseau. La couche Access offre la connectivité aux utilisateurs alors que la couche Distribution agrège le trafic utilisateur vers d'autres réseaux. L'objectif d'une telle méthode de conception est de faire évoluer le réseau de manière la plus efficace et de faire face aux problèmes de disponibilité.

La couche ACCESS

La couche Access est celle qui connecte les utilisateurs finaux (*end users*) au réseau. Les commutateurs (*switches*) de couche Access ont une connectivité de type L2, notamment avec la technologie VLAN.

Un périphérique de la couche Access fournit par les fonctionnalités suivantes :

Connectivité aux périphériques terminaux, haute densité de ports, interfaces montantes

Haute Disponibilité – alimentation redondante et support des First Hop Redundancy Protocols (FHRP).

Convergence – fournit du Power over Ethernet (PoE) pour les téléphones IP et les points d'accès sans fils, quality of service (QoS).

Sécurité – comprend d'office les fonctionnalités port security, DHCP snooping, Dynamic ARP inspection, IP source guard.

La couche DISTRIBUTION

La couche Distribution fournit l'interconnexion entre les couches Access et Core.

Un périphérique de la couche Distribution fournit par les fonctionnalités suivantes :

Lieu d'agrégation : disponibilité et réduction de complexité.

Haute disponibilité, “fast path recovery”, répartition de charge, qualité de service (QoS), et sécurité.

Route summarization et manipulation de paquets, point de redistribution entre des domaines de **roulage**, **filtrage** de paquets et politiques de routage.

Termine les VLAN.

Redondance de la passerelle : First Hop Redundancy Protocol (HSRP, VRRP, GLBP).

Les liaisons montantes (*uplinks*) des tous les commutateurs Access sont toutes “agrégées” dans la couche distribution. Les commutateurs de la couche Distribution doivent être capables de supporter la charge de traitement de tout le trafic venant des périphériques Access. Ces commutateurs devraient disposer d'une haute densité de ports à vitesse élevée pour assurer son service d'interconnexion.

Les VLAN et les domaines Broadcast/Multicast convergent au niveau de la couche Distribution nécessitant du roulage, du filtrage et de la sécurité. Ces commutateurs doivent être capables de router les paquets avec un taux de transfert très élevé.

Habituellement, la couche Distribution est une limite L3 qui assure le routage des VLAN.

La couche CORE

La couche Core fournit la connectivité entre tous les périphériques de la couche Distribution. On l'appelle aussi le "Backbone", la dorsale du réseau dont le rôle principal est de transférer de la manière la plus efficace un gros volume de trafic du réseau.

Agrège le trafic des commutateurs de distribution

Implémente des protocoles et des technologies évolutives et de la **répartition de la charge**

Transfert "haute vitesse" L3.

Utilise de la **redondance de L3.**

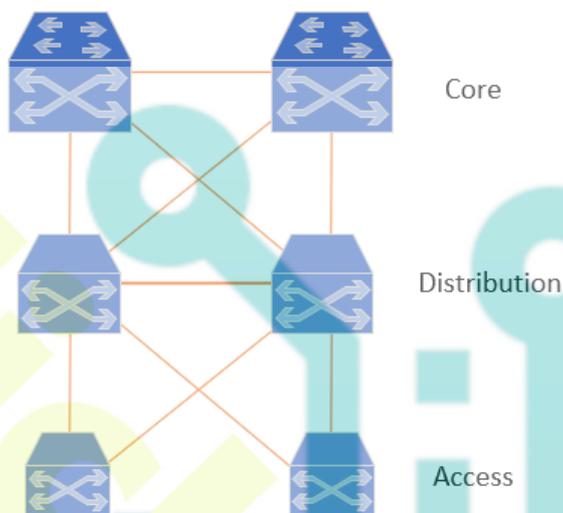
Sans une couche **core** les commutateurs de couche distribution devraient être entièrement maillés entre eux. Ce choix de conception est difficile à faire évoluer sans compter les besoins en câblage entre les commutateurs de distribution.

Pour les plus petites topologies, on peut combiner la couche core et distribution dans une topologie appelée "collapsed LAN Core".

Conception modulaire du réseau

Pour assurer la disponibilité de l'architecture et la faire évoluer aisément, Cisco recommande une conception modulaire du réseau qui organise le réseau en différents "blocks".

Pour améliorer la disponibilité du réseau, on ajoutera de la redondance dans la couche Distribution et dans la couche Core pour obtenir un *design* entièrement redondant.



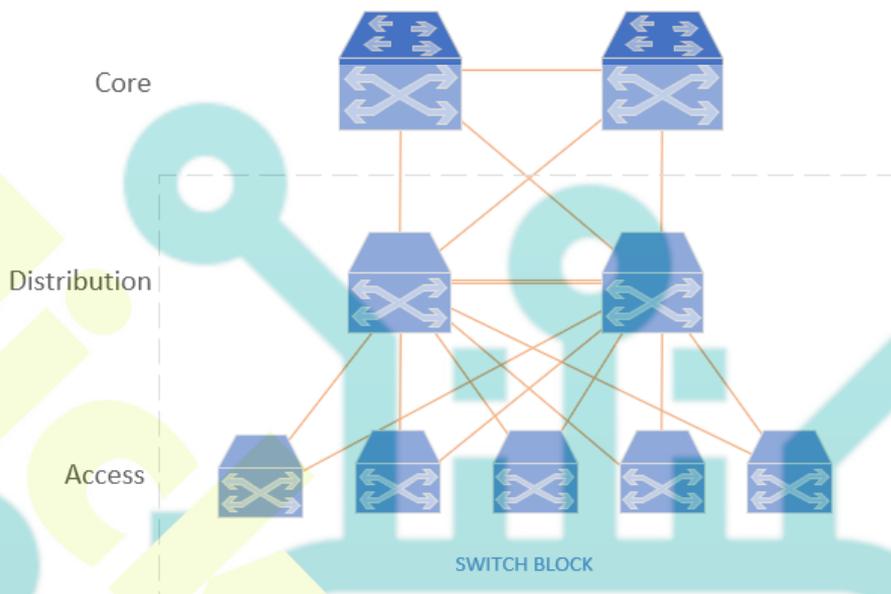
Une conception du réseau totalement redondante

On considérera ici un réseau de type Campus que l'on peut diviser en deux "blocks" :

Un Building Blocks: groupe de commutateurs Access et leurs commutateurs Distribution.

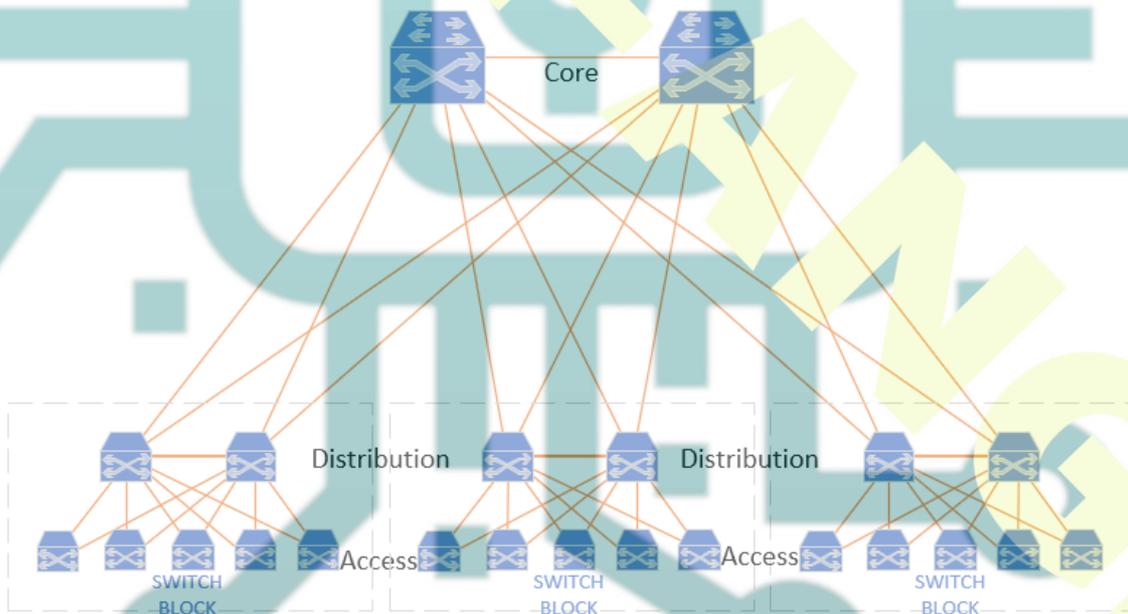
Le "Backbone": groupe de core du réseau Campus qui connecte tous les "Switch Blocks".

Dans le diagramme suivant on fait évoluer le réseau en ajoutant des commutateurs Access dans un "Switch Block".



Évolutivité de la couche Access

Dans la figure suivante, le réseau grandit par l'ajout de "switch blocks".

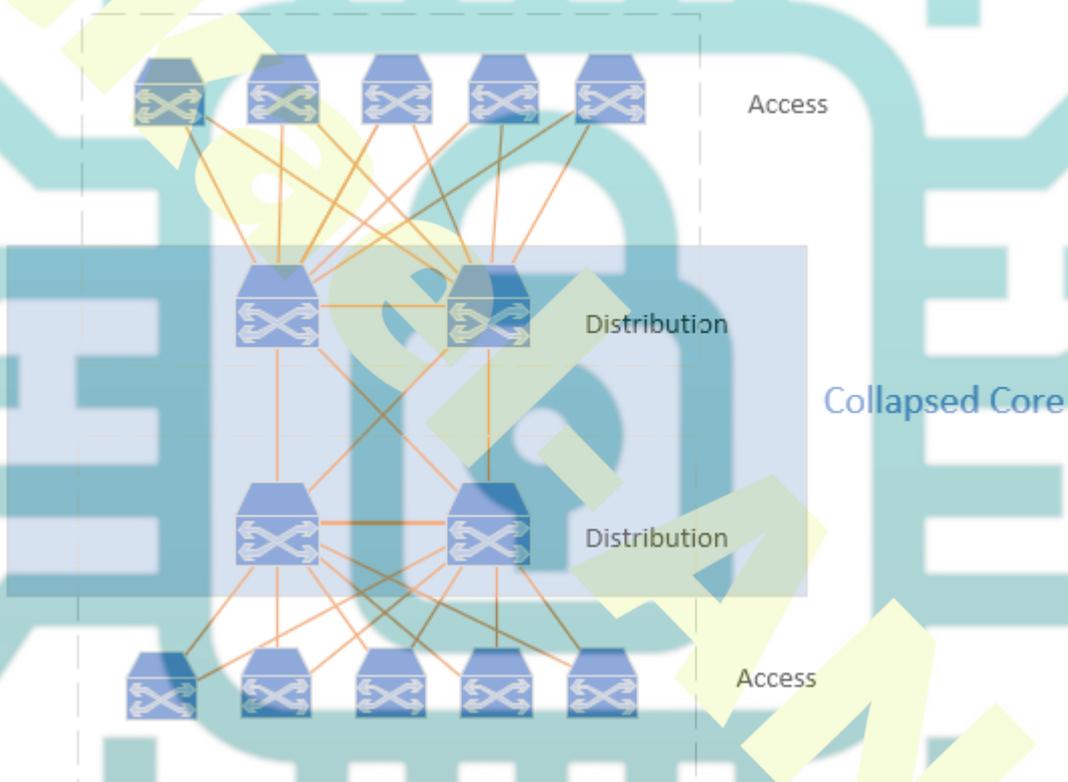


Les autres composants du réseau Campus qui donne accès un centre de données, à l'Internet, aux sites distant, les accès externes, la DMZ, etc. sont conçus comme des modules respectant le modèle hiérarchique.

Collapsed Core

Toutes les situations ne nécessitent pas une couche Core dédiée. Dans ce cas, on peut simplifier la topologie en “Collapsed Core”.

Dans une topologie collapsed core, chaque commutateur de couche Access dispose d'un lien redondant vers chaque commutateur de couche Distribution. Tous les sous-réseaux L3 sont présents dans la couche Access et se terminent sur les commutateurs de couche Distribution. Les commutateurs de couche Distribution se connectent les uns aux autres avec des liens redondants.



Architecture Collapsed Core

- **Redondance L1, L2 et L3 dans les “Switch blocks”**

Afin d'assurer la redondance et sa gestion (en évitant du bouclage dans le transfert du trafic), chaque couche pourrait avoir sa préférence sur le niveau de la solution L1 et/ou L2 ou encore L3.

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

On mettra dans la couche Access une redondance L1 avec une redondance L2 voire même du routage statique (L3). Le routage dynamique opère au niveau des couches Distribution et Core. Etherchannel ajoute de la redondance sans alourdir les topologies logiques.

Règles de Conception

Chaque couche devrait contenir une paire de commutateurs.

Connecter chaque commutateur à la couche supérieure avec deux liens pour la redondance.

Connecter chaque paire de commutateurs de couche Distribution avec un lien mais ne pas connecter les commutateurs Access entre eux.

Ne pas étendre les VLAN au-delà de la couche Distribution.

Choix et catalogues de commutateurs

Critères de choix de commutateurs

- Fonctionnalités Access/Distribution/Core
- Fonctionnalités L2 / L3
- Type d'interface/technologies
- Contraintes physiques
- Nombre d'interfaces
- Conformité protocolaire
- Form Factor : Fixed ports, Modular, Stackable
- Gestion, facilités
- Prix

- Garantie/support

Stacking de commutateurs et agrégation de châssis

Un switch “stackable” est un commutateur qui peut aussi s’agrèger avec d’autres commutateurs “stackable” pour offrir une seule plateforme de gestion.

Les commutateurs sont connectés entre eux en anneau par un câble spécial. Ils peuvent être ajoutés de manière transparente dans un “stack” sans interrompre les opérations sur le réseau. Ceux-ci se configurent automatiquement avec l’image et la configuration appropriée.

Avec le “stacking” l’administration du réseau est simplifiée : une seule adresse de gestion, un seul fichier de configuration, une seule table d’adresses MAC ...

On peut trouver certains avantages avec le “stacking” :

- Plus haute densité de ports.
- Usage efficace des ressources.
- Administration simplifiée du réseau.
- Évolutivité facilitée.
- Flexibilité de déploiement.
- Connexions résilientes.

L’agrégation de châssis de châssis est une technologie Cisco Systems qui fait fonctionner un seul commutateur. L’agrégation de châssis est semblable au “stacking” sauf que la technologie est disponible sur de gros châssis tels que des C6500 ou des C6800 utilisés dans la couche Core ou Distribution alors que le “stacking” serait plus utilisé dans la couche Access.

Modèles de commutateurs Cisco Campus LAN couche Access

- Cisco Catalyst 3850 Series Switches
- Cisco Catalyst 3650 Series Switches
- Cisco Catalyst 4500E Series Switches
- Cisco Catalyst 2960-X and 2960-XR Series Switches

Modèles de commutateurs Cisco Campus LAN couche Distribution

Cisco Catalyst 3850 Series Switches

Cisco Catalyst 6807-XL Series Switches with Supervisor Engine 6T

Cisco Catalyst 6880-X Series Switches

Cisco Catalyst 4500-X Series Switches

Cisco Catalyst 4500E Series Switches

Modèles de commutateurs Cisco Campus LAN couche Core

Cisco Nexus 7700 Series Switches with Supervisor 2E

Cisco Catalyst 6807-XL Switches

Cisco Catalyst 6500 Supervisor Engine 6T

Matériel routeur

Les routeurs jouent un rôle essentiel dans la mise en réseau en connectant les particuliers et les entreprises à Internet, en interconnectant plusieurs sites au sein d'un réseau d'entreprise, en fournissant des chemins redondants et en connectant des fournisseurs de services Internet sur Internet. Ils agissent également en tant que traducteur entre différents types de supports et protocoles.

Il existe trois catégories de routeurs: **Succursale, Edge réseau et Fournisseur de services.**

Les routeurs viennent également dans de nombreux facteurs de forme. Les administrateurs réseau dans un environnement d'entreprise doivent pouvoir prendre en charge divers routeurs, du petit routeur de bureau au modèle monté en rack ou en lame.

Modèle pour les petites entreprises ou individuels

Cisco 800 series

Modèle pour les succursales, petite et moyennes entreprises

Cisco 1900 series

cisco 2900 series

Cisco 3900 series

Modèle pour les grandes entreprises et fournisseurs

Cisco 7600 series

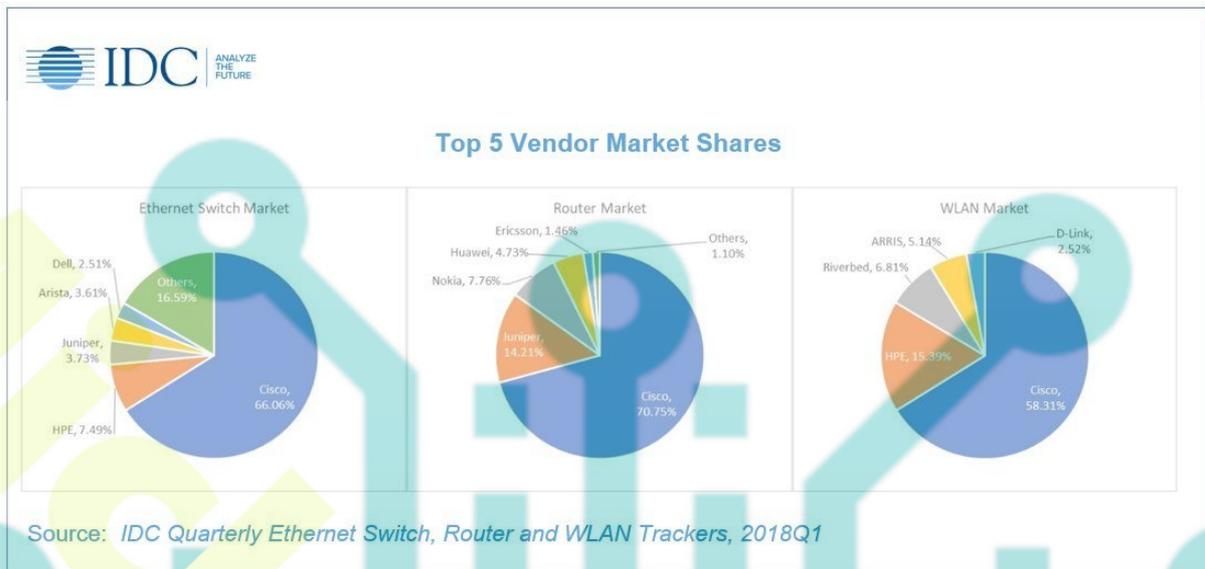
Gestion des périphériques

IOS désigne l'ensemble des technologies de routage, de commutation, de sécurité et autres technologies d'inter réseau intégrées dans un système d'exploitation multitâche unique. La gestion hors bande est utilisée pour la configuration initiale ou lorsqu'une connexion réseau n'est pas disponible. La gestion intra bande est utilisée pour surveiller et modifier la configuration d'un périphérique réseau via une connexion réseau.

Une configuration de commutateur de base comprend le nom d'hôte pour l'identification, les mots de passe pour la sécurité, l'attribution d'adresses IP aux interfaces pour la connectivité et le routage de base.

Le Marché

Cisco Systems est le leader du marché infrastructures d'entreprise sur les switches et les routeurs.



Cisco a continué de dominer le centre de données en tant que premier fournisseur d'entreprise dans presque tous les segments, malgré une chute de la part de marché de 2 points de pourcentage au cours des quatre trimestres précédents, pour atteindre 23% de part de marché.

Synergy attribue le positionnement de Cisco à une croissance substantielle du nombre de serveurs, Cisco se situant à la cinquième place en tant que fournisseur. Dans le même temps, il convient de noter que, dans les autres segments du marché, la part de marché de Cisco est restée relativement constante.

En décembre, Synergy a annoncé que la part de Cisco dans le marché mondial total des commutateurs et des routeurs s'élevait à 53%, son plus haut niveau depuis 2016. La part de marché de Cisco allant de 63% pour les routeurs d'entreprise à 40% pour les routeurs de fournisseurs de services .

Avec une part de marché globale de 11% pour l'infrastructure informatique, HPE se classait au deuxième rang derrière Cisco. Par segment, HPE est en tête de la catégorie des serveurs de centre de données, se classe n° 2 en WLAN et se classe au troisième rang pour les commutateurs et les routeurs.

Après Cisco et HPE, les autres fournisseurs qui se classent au deuxième rang des segments sont : Dell EMC pour les serveurs de centre de données d'entreprise, Huawei pour les commutateurs et les routeurs, Microsoft pour la collaboration et Check Point pour la sécurité du réseau.