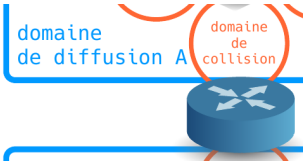
# Segmentation des réseaux locaux

**Philippe Latu**
philippe.latu(at)inetdoc.net

*https://www.inetdoc.net*

**Résumé**

Les commutateurs sont aujourd'hui des outils essentiels dans la conception des architectures réseau. La garantie sur la bande passante délivrée par port a fortement contribué au développement des réseaux locaux. Pour autant, la commutation de trames Ethernet associée aux réseaux virtuels (VLANs) peut-elle supplanter à elle seule le routage dans la gestion des réseaux ? Pour concevoir correctement une architecture, il faut considérer les besoins des application, les types de trafic (données, voix, vidéo) et la composition des groupes logiques. Cet article donne quelques éléments sur le choix entre routage et commutation.




# Table des matières



## 1. Copyright et Licence

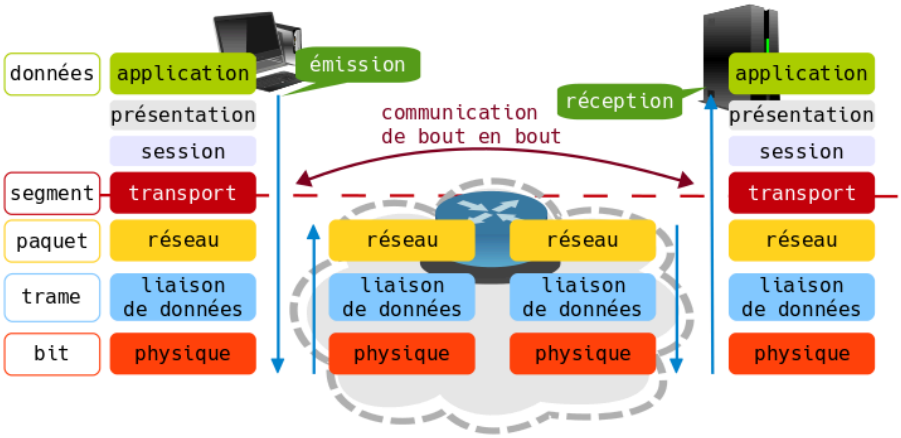


## Meta-information

Cet article est écrit avec DocBook XML sur un système Debian GNU/Linux. Il est disponible en version imprimable au format PDF : `lan-segmentation.pdf`.

## 2. Introduction

D'après la modélisation OSI, c'est la couche réseau (niveau 3) qui assure l'interconnexion entre les réseaux hétérogènes. Qu'en est-il de l'interconnexion entres des réseaux homogènes qui reposent pratiquement tous sur Ethernet ?




La conception d'une architecture d'interconnexion de réseaux a toujours été l'art de trouver le bon équilibre entre rapidité et qualité. Les commutateurs répondent parfaitement au critère rapidité tandis que les routeurs répondent parfaitement au critère qualité. Ce document est une introduction aux deux techniques : commutation et routage. Il fait suite à la présentation des Modélisations réseau et il se termine par une synthèse succincte sur la segmentation des réseaux locaux avec le modèle hiérarchique.

## 3. La commutation

La technologie de commutation opère au niveau 2 du modèle de référence OSI. À l'origine, la popularité des commutateurs pouvait être vue comme la résurgence de la technologie des ponts.

- Tout comme un pont, le commutateur prend ses décisions de transmission à partir de l'adresse MAC source contenue dans chaque trame.
- À la différence d'un pont, le commutateur transmet les trames avec des temps de latence extrêmement courts grâce à des algorithmes intégrés directement dans ses composants.

La commutation permet de répartir la bande passante à la fois sur des segments partagés et des segments dédiés. Tous les hôtes raccordés directement à un port de commutateur appartiennent à un segment dédié, tandis que tous les hôtes associés à un point d'accès radio Wifi appartiennent à un segment partagé.

Pour simplifier, on peut définir un commutateur comme une machine à fabriquer des circuits full-duplex à la demande.

À l'intérieur d'un commutateur, la commutation de circuits utilise des composants qui manipulent un type de mémoire particulier appelé Content-addressable memory. Ces composants permettent d'accélérer considérablement la transmission des données en recherchant directement les adresses MAC connues d'un ou plusieurs ports.

### Modèles de propagation

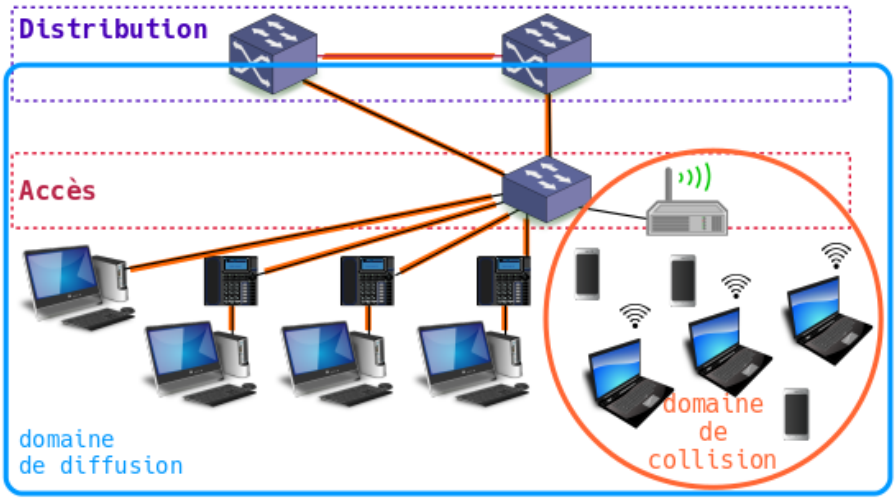
Commutation cut-through

> Elle démarre le processus propagation à partir de l'adresse MAC du destinataire avant que la totalité de la trame soit reçue. Avec ce modèle, les temps d'attente sont aussi courts quelle que soit la longueur des trames. Cependant, les trames erronées sont transmises sans aucun contrôle.

Commutation store and forward

> La totalité de la trame est lue et validée avant sa retransmission. Ceci permet de supprimer les trames corrompues et de définir des filtres pour contrôler le trafic à travers le commutateur. Les temps d'attente augmentent avec la longueur des trames.

## Où utiliser des commutateurs ?




Où utiliser des commutateurs ? - vue complète

Les commutateurs doivent être considérés comme fournisseurs de bande passante et non comme une amélioration de la sécurité et du contrôle du réseau. Les besoins en bande passante proviennent :

- du nombre toujours croissant du nombre d'hôtes (ou d'adresses MAC) raccordés,
- des besoins toujours croissants en débit réseau de chaque hôte,
- de l'émergence de nouveaux services Internet qui nécessitent des échanges toujours plus fréquents,
- de la densité du nombre des serveurs dans les centres de données.

Dans l'exemple du schéma ci-dessus, les hôtes et les commutateurs des couches Accès et Distribution appartiennent à un même domaine de diffusion. Les tables CAM ( Content-addressable memory) de tous les commutateurs contiennent les adresses MAC source ainsi que les numéros de ports via lesquels lesquels les hôtes sont joignables.

Chaque liaison surlignée en orange constitue un segment dédié ou encore une partie de circuit full-duplex sur lequel toute collision est impossible puisque le canal de transmission est réservé au seul usage de l'hôte ou équipement concerné.

En revanche, le point d'accès Wifi situé à droite du schéma ouvre un segment partagé. Le canal de transmission est partagé entre tous les hôtes associés à ce point d'accès. Ceux-ci sont en concurrence dans la zone de couverture radio du point d'accès pour émettre et recevoir des données. Plus le nombre d'hôtes est important plus il y a de collisions et plus les temps de communication deviennent aléatoires.

Pour conclure cette section, il faut noter qu'il existe au niveau liaison de données un protocole qui permet de se protéger contre les «orages de diffusion» provoqués par la présence d'au moins une boucle dans les liaisons entre commutateurs des couches Accès et Distribution : le Spanning Tree Protocol. L'étude de ce protocole sort du cadre de cet article et le schéma ci-dessus est exemple de topologie sans boucle puisque la liaison horizontale entre les deux commutateurs de couche distribution utilise le routage au niveau réseau. Il faut simplement noter à ce niveau que des solutions, permettant de garantir que le chemin entre deux hôtes est unique, existent. Dans une architecture contemporaine, le recours à la redondance pour augmenter la tolérance aux pannes, impose l'étude de la protection contre les boucles.

## 4. Le routage

Les routeurs opèrent au niveau 3 du modèle de référence OSI. Ils ont beaucoup plus de fonctions logicielles qu'un commutateur. En fonctionnant à un niveau plus élevé qu'un commutateur, un routeur distingue les différents protocoles de la couche réseau : IPv4 et IPv6. Cette connaissance permet au routeur de prendre des décisions plus sophistiquées pour l'acheminement des flux réseau.

- Comme un commutateur, un routeur fournit aux utilisateurs une communication transparente entre des segments différents.

- À la différence d'un commutateur, un routeur détermine les limites logiques entre les différents segments de réseaux.

Un routeur fournit un service de contrôle d'accès parce qu'il ne transmet que le trafic destiné à le traverser. Pour traiter les flux réseau, un routeur doit assurer deux fonctions de base :

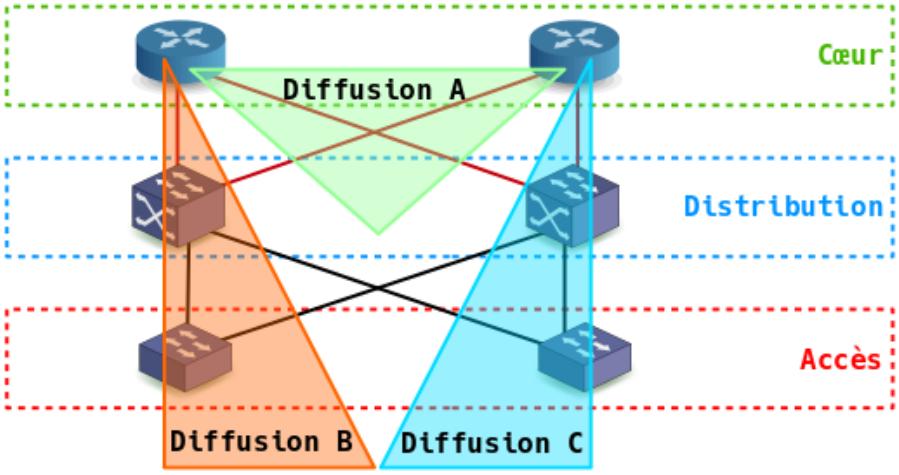
1. Créer et maintenir une table de routage pour chaque protocole de couche réseau (IPv4 et IPv6). Ces tables peuvent être mises à jour grâce à des protocoles de routage dynamiques.

2. Identifier le protocole contenu dans chaque paquet, extraire l'adresse de destination réseau et prendre la décision de propagation en fonction des données de la table de routage.

Les fonctionnalités étendues d'un routeur lui permettent de choisir le meilleur chemin à partir de plus d'éléments qu'une simple adresse MAC : comptage des « sauts », vitesse de transmission, coût, délais et conditions de trafic.

Ces améliorations conduisent à une meilleure sécurité, une meilleure utilisation de la bande passante et plus de contrôle sur les opérations réseau. Cependant, les temps de traitement supplémentaires peuvent réduire les performances comparativement à un commutateur.

## Où utiliser des routeurs ?




Où utiliser un routeur ? - vue complète

Les routeurs sont conçus pour gérer les architectures réseau en assurant les besoins suivants :

1. Segmenter les réseaux en domaines de diffusion isolés. La hiérarchie qui en résulte permet de déléguer l'autorité et la gestion des réseaux.

2. Filtrer intelligemment les paquets et supporter les chemins multiples redondants en assurant une «balance de charge».

Dans l'exemple du schéma ci-dessus, les triangles désignent trois domaines de diffusion (A, B et C). Ces domaines de diffusions sont distribués sur les différents commutateurs à partir des deux routeurs de la couche Cœur. Ainsi, le trafic issu d'un hôte du domaine C (triangle bleu) doit transiter par le domaine A (triangle vert) avant d'atteindre un hôte du domaine B (triangle orange). Ces domaines correspondent à des périmètres à l'intérieur desquels les trames et les paquets de diffusion restent cloisonnés. Les tables CAM ( Content-addressable memory) des commutateurs de chacun des domaines (triangle de couleur) ne contiennent que les adresses MAC des hôtes du domaine en question. On limite de cette façon le nombre circuits full-duplex à fabriquer par chaque commutateur.

À une époque où le nombre d'hôtes Wifi présents dans une même zone de couverture radio géographique explose, le fait de définir correctement les limites de la diffusion devient une question très sensible.

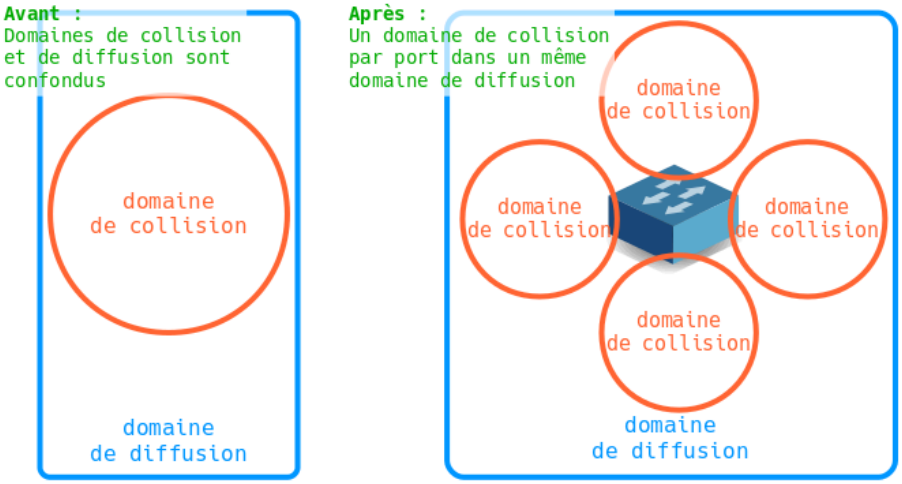
## 5. Segmentation

Les aptitudes des commutateurs et des routeurs à segmenter les réseaux sont une source de confusion. Comme chacun de ces équipements opère jusqu'à un niveau différent du modèle OSI, chacun réalise un type de segmentation différent.

## 5.1. Un commutateur segmente des domaines de collision

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

Les domaines de collisions appartiennent au même domaine de diffusion.

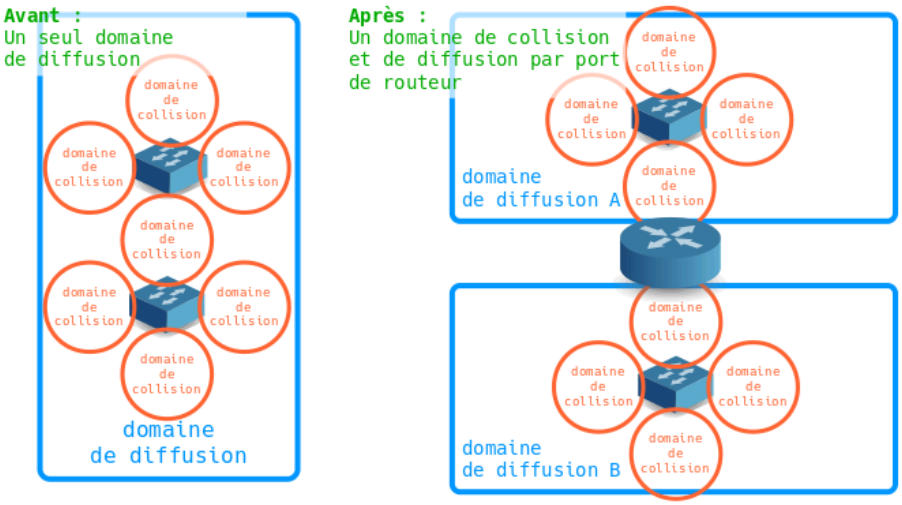



Segmenter avec un commutateur - vue complète

## 5.2. Un routeur segmente des domaines de collision et de diffusion

La segmentation au niveau de la couche réseau (3) limite la portée du trafic de diffusion en divisant le réseau en sous-réseaux indépendants.

Comme un routeur opère aussi au niveau liaison de données (2), ses interfaces ont aussi pour rôle la délimitation d'un domaine de collision.




Segmenter avec un routeur - vue complète

## 5.3. Principe du routage inter-VLAN

C'est grâce aux progrès de l'électronique, qui ont permis d'augmenter les densités d'intégration et les fréquences, que les commutateurs ont pu se développer. On peut maintenant affirmer qu'un commutateur est une machine à fabriquer des circuits full-duplex. En effet, à un instant donné, deux hôtes raccordés au même commutateur disposent d'un canal de transmission réservé sans risque de collision avec un débit et une latence connue.

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

Il était donc inévitable que l'on aboutisse à des équipements qui associent la commutation de circuits et la commutation de paquets. Aujourd'hui, les routeurs les plus performants associent les champs des en-têtes des couches application, transport et réseau à une électronique rapide de commutation de circuit au niveau liaison de données.

Pour parvenir à ce résultat, il a fallu dépasser la difficulté liée aux définitions des formats d'adressage :

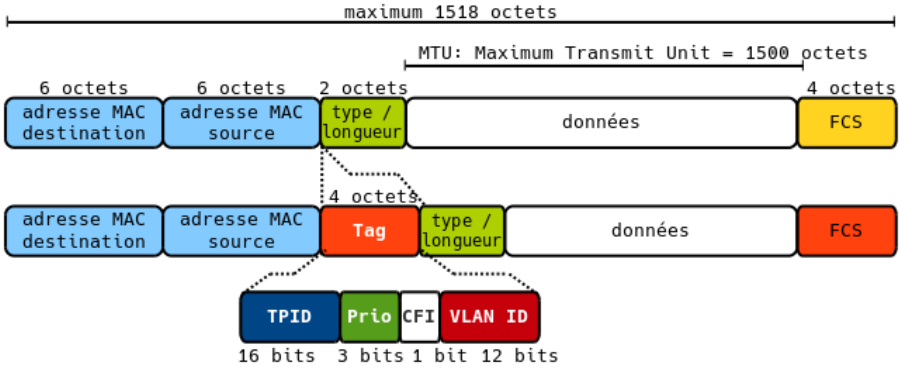
- Les adresses du niveau liaison de données.
  Les adresses MAC sont communément désignées comme adresses physiques parce qu'elles sont définies ou «gravées» directement dans le composant d'interface réseau. Cependant, il n'est pas très difficile les modifier au niveau logiciel. Il existe deux Types d'adresses MAC qui sont présentés dans le document : Routage Inter-VLAN.

  Le point important ici, c'est que l'espace des adresses MAC est «à plat» sans aucune hiérarchie. Le format de ces adresses ne permet pas de constituer des groupes logiques. Ainsi, une trame de diffusion avec l'adresse MAC destination `ff:ff:ff:ff:ff:ff` sera recopiée sur tous les ports des commutateurs d'un même domaine de diffusion.

- Les adresses du niveau réseau.
  Les adresses IPv4 et IPv6 utilisent la notion de masque réseau de façon à distinguer un hôte et le réseau auquel il appartient. Le réseau peut ainsi correspondre au groupe logique qui limite la portée des trames ou des paquets de diffusion.

  L'espace des adresses IPv4 ou IPv6 est hiérarchisé par nature et contrairement à l'espace des adresses MAC il est possible de diviser l'espace total en groupes géographiques ou logiques. La distribution de l'espace d'adressage entre les organismes tels que l'IANA et les RIR illustre bien cette aptitude au découpage en groupes.

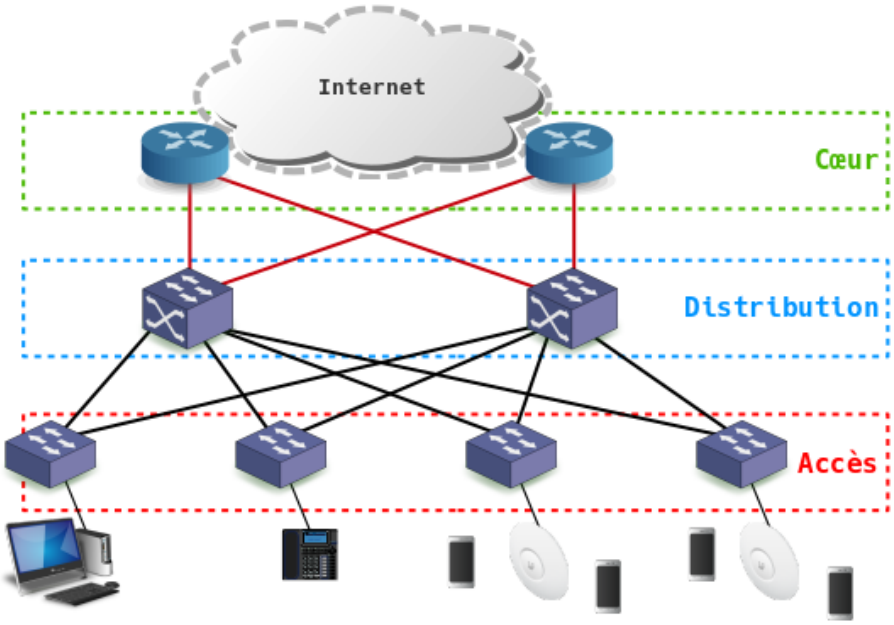
Jusqu'à l'apparition de la notion de VLAN, il était impossible de faire correspondre les deux espaces d'adressage des couches liaison et réseau. La norme IEEE 802.1Q a introduit de nouveaux champs dans le format de trame Ethernet. Celui qui nous intéresse ici est le champ VLAN ID.




En faisant correspondre un identifiant de VLAN à une sous-interface réseau avec un préfixe IPv4 et/ou IPv6 propre, on constitue un groupe logique dans lequel la diffusion a une portée limitée. On parle alors de Routage Inter-VLAN.

## 6. Modèle hiérarchique de conception

En tenant compte des notions abordées ci-dessus, voici un exemple d'architecture type basé sur le modèle hiérarchique. Il s'agit de concilier la fourniture de bande passante pour le réseau local et les contrôles de flux et d'accès vers l'Internet.




Exemple de conception - vue complète

Ce découpage type d'une architecture réseau en trois couches distinctes est en grande partie basé sur la répartition des rôles entre routage et commutation. Cette répartition a pour but de satisfaire plusieurs critères :

- La création de domaines de diffusion dont les limites sont connues aide à structurer l'architecture de façon à obtenir un modèle déterministe des flux réseaux.
- La création de blocs d'équipements redondants rend l'architecture tolérante aux pannes, reproductible et plus facile à personnaliser.
- La hiérarchisation permet de limiter la complexité en divisant l'architecture en blocs fonctionnels avec un rôle bien défini.

Cœur

Cette couche correspond à la dorsale du réseau de l'entreprise qui relie entre eux les blocs fonctionnels d'équipements. Les objectifs à ce niveau sont les performances, la stabilité et le moins de complexité possible. C'est la raison pour laquelle on ne trouve généralement que deux routeurs redondants à ce niveau.

Le débit binaire utile est le critère de dimensionnement d'un routeur qui conditionne les performances. Par débit binaire utile, on entend la transmission de flux réseau classifiés, routés et filtrés.

Distribution

Cette couche repose sur la convergence, l'équilibrage de charge, la qualité de service et la haute disponibilité. On y trouve l'isolation vis-à-vis de la couche accès avec le moins de commutation de circuits (ou d'adresses MAC) possible. Vue de la couche accès, c'est à ce niveau que l'on offre la redondance des passerelles réseau par défaut des hôtes.

Accès

Plus les usages réseau évoluent, plus cette couche doit être riche en fonctionnalités diverses. Elle ne se limite plus à fournir des ports de commutateur en vis-à-vis de postes de travail fixes qui utilisent tous le même système. On y trouve maintenant des fonctions de gestion de l'alimentation des équipements raccordés au commutateur (téléphones, points d'accès Wifi, etc.) via la technologie PoE ( Power over Ethernet). On y trouve aussi les fonctions d'authentification de ces mêmes hôtes ou équipements raccordés à l'aide du protocole IEEE 802.1X. Pour optimiser l'utilisation de la bande passante radio, les commutateurs intègrent de plus en plus des logiciels de contrôle radio qui permettent par exemple de réguler les puissances rayonnées par les antennes des points d'accès Wifi.