Chapitre 3: Notions de base sur le routage et les sous-réseaux

3.1 Protocole routé

3.1.1 Protocole routé et protocole routable

3.1.2 IP comme protocole routé

3.1.3 Propagation d'un paquet et commutation au sein d'un routeur

3.1.4 Transmission orientée connexion et transmission non orientée connexion

3.1.5 Anatomie d'un paquet IP

3.2 Protocoles de routage IP

3.2.1 Vue d'ensemble du routage

3.2.2 Routage et commutation

3.2.3 Protocole routé et protocole de routage

3.2.4 Détermination du chemin

3.2.5 Tables de routage

3.2.6 Algorithmes et métriques de routage

3.2.7 Protocoles IGP et EGP

3.2.8 État de liens et vecteur de distance

3.2.9 Protocoles de routage

3.3 Mécanisme de découpage en sous-réseaux

3.3.1 Classes d'adresses réseau IP

3.3.2 Introduction au découpage en sous-réseaux

3.3.3 Détermination de l'adresse d'un masque de sous-réseau

3.3.4 Application du masque de sous-réseau

3.3.5 Découpage de réseaux de classe A et B en sous-réseaux

3.3.6 Calcul du sous-réseau via l'opération AND

Le protocole IP (*Internet Protocol*) est le principal protocole routé d'Internet. Les adresses IP permettent d'acheminer les paquets depuis une source vers une destination en empruntant le meilleur chemin possible. La propagation des paquets, les modifications de l'encapsulation et les protocoles orientés et non orientés connexion sont également essentiels à la bonne livraison des données. Ce module présente chacun de ces éléments.
La différence entre les protocoles de routage et les protocoles routés est souvent source de confusion. Les deux concepts, bien que similaires en apparence, sont en fait très différents. Les routeurs se servent des protocoles de routage pour créer les tables qui leur permettront de déterminer le meilleur chemin vers un hôte sur Internet.
Les organisations ne peuvent pas toutes être classées dans les trois classes d'adresses (A, B et C). La subdivision en sous-réseaux apporte de la flexibilité à ce système de classes. Elle permet aux administrateurs réseau de déterminer la taille du réseau dont ils auront besoin. Une fois qu'ils ont choisi le type de segmentation de leurs réseaux, ils emploient des masques de sous-réseau pour définir l'emplacement de chacune des machines sur le réseau.

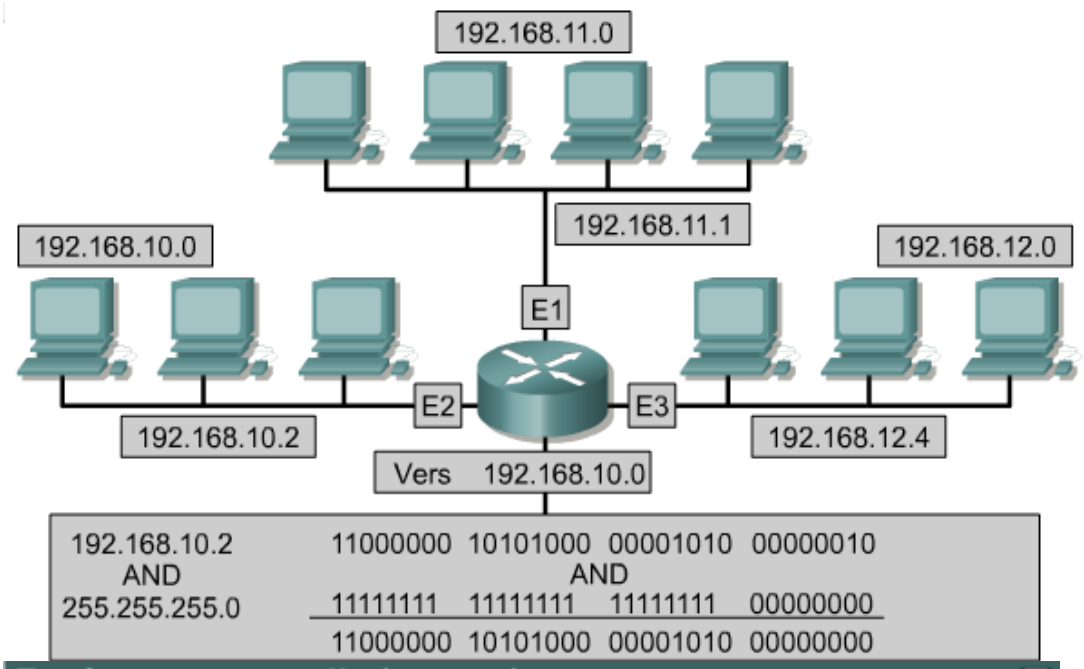
-

3.1 Protocole routé

3.1.1 Protocole routé et protocole

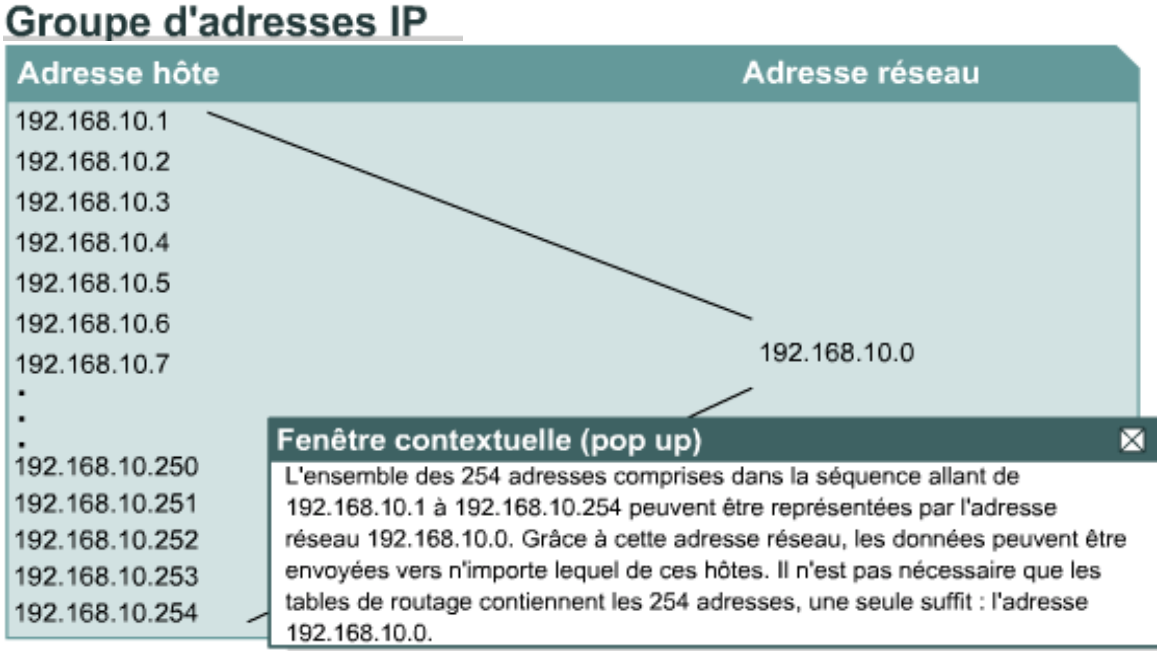
Un protocole est un ensemble de règles qui définit le mode de communication entre les différents ordinateurs sur les réseaux. Pour communiquer entre eux, les ordinateurs échangent des messages. Afin de pouvoir accepter et traiter ces messages, il leur faut disposer d'ensembles de règles qui déterminent la manière de les interpréter. Les messages utilisés pour établir une connexion avec une machine distante, les messages électroniques et les fichiers transférés sur un réseau sont autant d'exemples de ces messages.
Un protocole décrit les éléments suivants:

- Le format de message requis.
- La manière dont les ordinateurs doivent échanger les messages d'activités spécifiques.



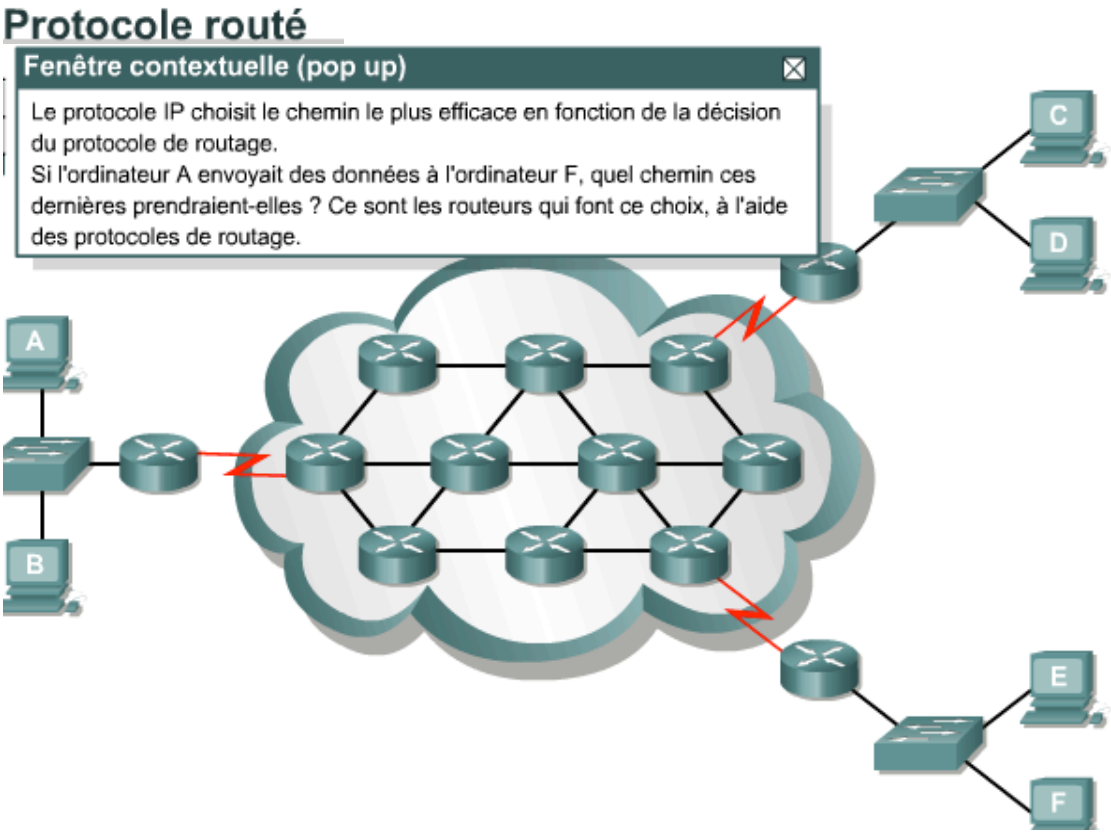
Un protocole routé permet au routeur de transmettre des données entre les nœuds de différents réseaux. Un protocole routable doit impérativement permettre d'attribuer un numéro de réseau et un numéro d'hôte à chacune des machines. Certains protocoles, à l'instar du protocole IPX, ne requièrent que

le numéro de réseau. Ils utilisent alors l'adresse MAC de l'hôte à la place de son numéro. D'autres protocoles, comme IP, nécessitent que l'adresse comporte une partie réseau et une partie hôte. Dans ce cas, un masque de réseau est nécessaire pour différencier ces deux numéros. L'adresse réseau est ensuite obtenue en effectuant une opération AND logique sur l'adresse et le masque de réseau.



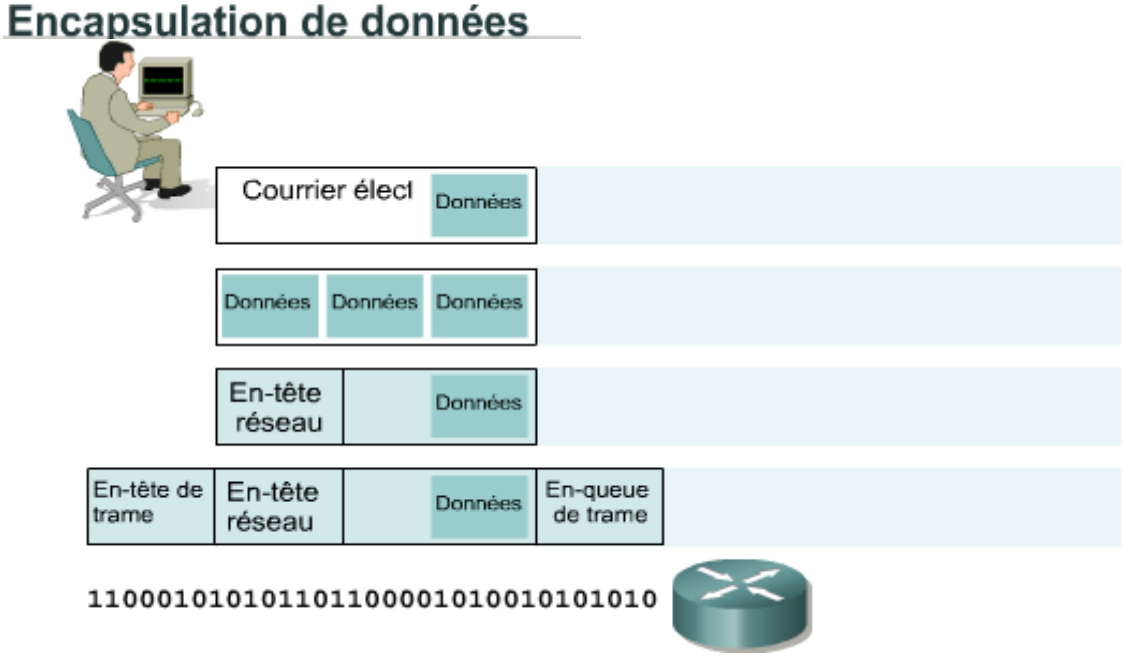
L'objectif du masque de réseau est de permettre à des groupes d'adresses IP séquentielles d'être traités en tant qu'une seule et même unité. Sans ce regroupement, chaque hôte devrait être mappé individuellement pour le routage, ce qui est impossible à réaliser. En effet, selon le consortium ISC (*Internet Software Consortium*), il existerait quelque 233 101 500 hôtes sur Internet.

10.1.2 IP comme protocole routé

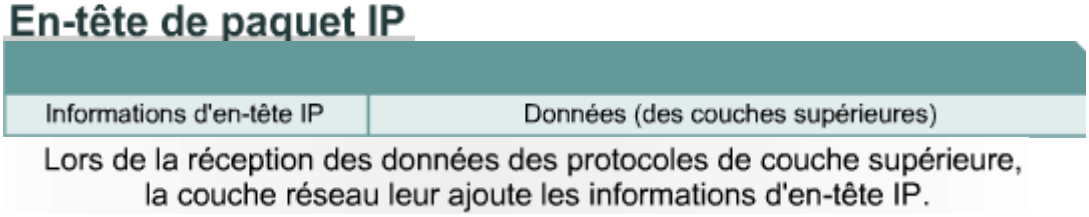


IP est le système d'adressage hiérarchique des réseaux le plus largement utilisé. ��C'est un protocole non orienté connexion, peu fiable et axé sur l'acheminement au mieux (best-effort delivery). Le terme «non orienté connexion» signifie qu'aucune connexion à un circuit dédié n'est établie avant la transmission. Le protocole IP détermine le meilleur chemin pour les données en fonction du protocole de routage. Les

termes «peu fiable» et «au mieux» ne signifient pas que le système n'est pas fiable et qu'il fonctionne mal, mais plutôt que le protocole IP ne s'assure pas de la bonne livraison des données envoyées sur le réseau. Si cette vérification est nécessaire, elle est effectuée par les protocoles de couche supérieure.

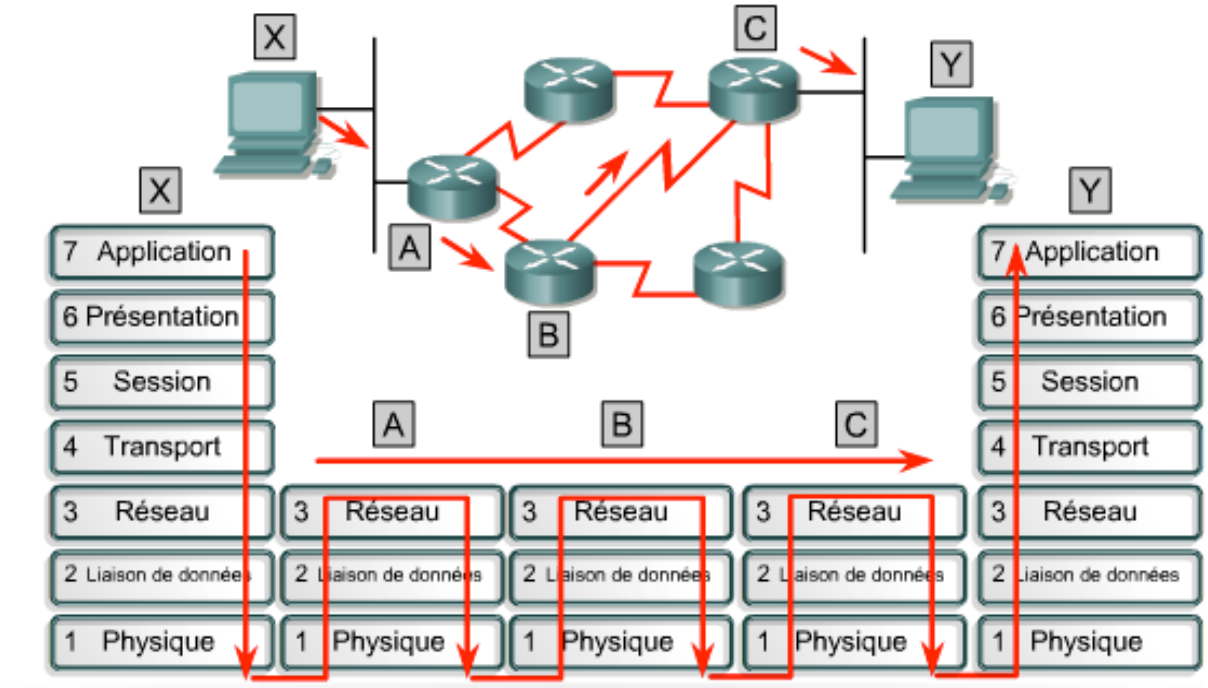


Les données sont traitées au niveau de chaque couche du modèle OSI au fur et à mesure qu'elles circulent vers le bas du modèle. Au niveau de la couche réseau, les données sont encapsulées dans des paquets. Ces paquets sont appelés des datagrammes. IP détermine le contenu de l'en-tête du paquet IP, qui contient les informations d'adressage. Il ne se préoccupe toutefois pas des données proprement dites. Il se contente de les accepter lorsqu'il les reçoit des couches supérieures.



3.1.3 Propagation d'un paquet et commutation au sein d'un routeur

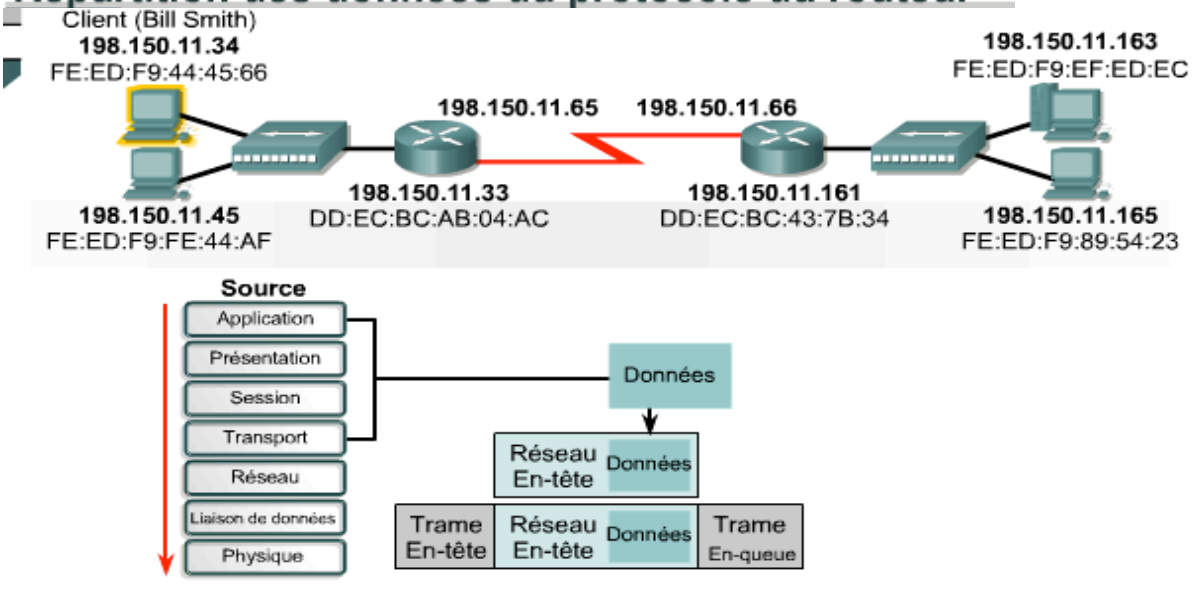
Équipements de la couche réseau dans un flux de données



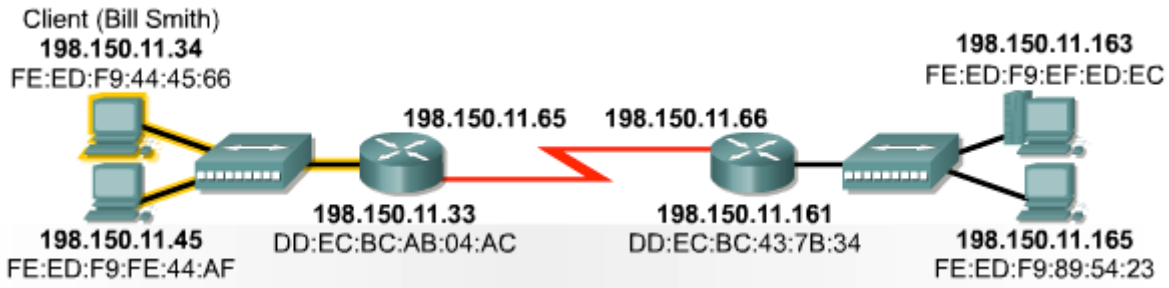
Chaque routeur fournit ses services pour la prise en charge des fonctions de la couche supérieure.

Au cours de l'acheminement d'un paquet sur un inter réseau jusqu'à sa destination finale, les en-queues et les en-têtes de trame de la couche 2 sont retirés et remplacés au niveau de chacune des unités de couche 3. Cela s'explique par le fait que les unités de données de la couche 2, ou trames, sont destinées à l'adressage local, tandis que les unités de données de la couche 3, ou paquets, sont destinées à l'adressage de bout en bout.

Répartition des données du protocole du routeur



La couche transport segmente, séquence et ajoute le contrôle d'erreur au message électronique. Les adresses source et de destination de la couche réseau sont ajoutées au datagramme. Le cache ARP fournit l'adresse MAC correspondant à l'adresse IP de destination. Ainsi, la trame Ethernet est ajoutée et comprend les adresses source et de destination.



Trame En-tête		Réseau En-tête		Données	Trame En-queue
Destination	Source	Source	Destination		
DD:EC:BC:AB:04:AC	FE:ED:F9:44:45:66	198.150.11.34	198.150.11.163	Courrier électronique Données	CRC-32

Les trames de données sont ensuite transmises sur le segment Ethernet. Toutes les stations de travail prennent la trame et vérifient si elle leur est destinée. Toutes les unités, à l'exception du routeur, rejettent la trame.

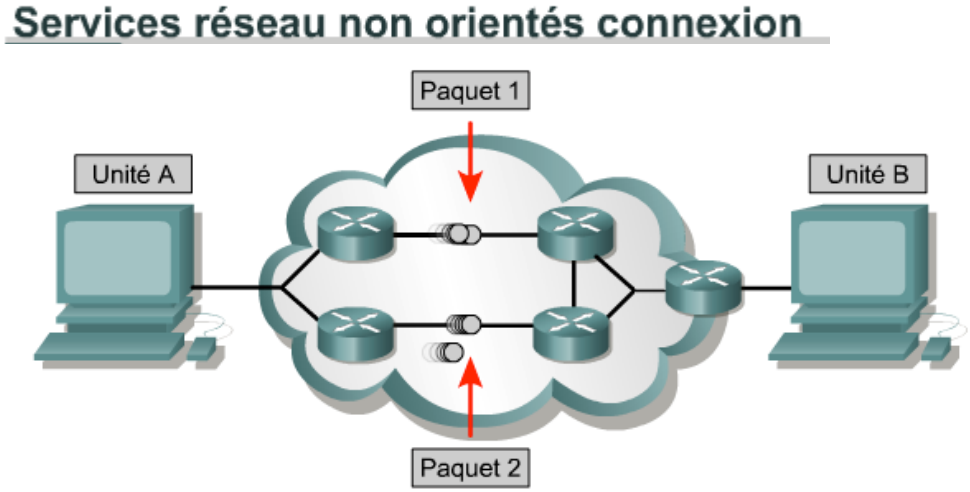
Les trames Ethernet de la couche 2 sont conçues pour circuler au sein d'un domaine de broadcast grâce à l'adresse MAC gravée sur le matériel. Les autres types de trames de la couche 2 comprennent les liaisons série PPP et les connexions Frame Relay, qui utilisent différents systèmes d'adressage de couche 2. Quel que soit le type d'adressage de couche 2 utilisé, les trames sont conçues pour circuler dans un domaine de broadcast de couche 2. Lorsque les données sont envoyées vers une unité de couche 3, les informations de couche 2 sont modifiées.

Lorsqu'une interface du routeur reçoit une trame, elle en extrait l'adresse MAC de destination. Cette adresse est vérifiée afin de savoir si la trame est destinée directement à l'interface du routeur ou s'il s'agit d'un broadcast. Dans les deux cas, la trame est acceptée. Si elle est destinée à une autre unité du domaine de collision, elle est rejetée.

Lorsqu'elle est acceptée, les informations de code de redondance cyclique (CRC, *Cyclic Redundancy Check*) sont extraites de son en-queue. Le CRC est calculé pour vérifier l'intégrité des données de la trame. Si la vérification échoue, la trame est rejetée. Si elle réussit, l'en-queue et l'en-tête de trame sont retirés, et le paquet est transmis à la couche 3. Ce paquet est ensuite examiné pour savoir s'il est destiné au routeur ou s'il doit être acheminé vers un autre équipement de l'interréseau. Si l'adresse IP de destination correspond à l'un des ports du routeur, l'en-tête de la couche 3 est retiré et les données sont transmises à la couche 4. Dans le cas contraire, l'adresse est comparée à la table de routage. Si une correspondance est établie ou s'il existe un chemin par défaut, le paquet est envoyé à l'interface indiquée dans l'entrée mise en correspondance de la table de routage. Lors de la commutation du paquet vers l'interface de sortie, une nouvelle valeur CRC est ajoutée en en-queue de trame et l'en-tête de trame approprié est ajouté au paquet. La trame est ensuite transmise au domaine de broadcast suivant et continue sa route jusqu'à la destination finale.

3.1.4 Transmission orientée connexion et transmission non orientée connexion

Ces deux services constituent la véritable transmission des données de bout en bout sur un interréseau.



La plupart des services réseau utilisent un système de livraison non orienté connexion. Les paquets peuvent emprunter différentes routes pour circuler sur le réseau. Ils sont ensuite rassemblés à leur arrivée. Dans un système non orienté connexion, la destination n'est pas contactée avant l'envoi d'un paquet. Le système postal constitue une bonne analogie, puisque le destinataire du courrier n'est pas contacté pour savoir s'il acceptera la lettre avant son envoi. De même, l'expéditeur ne sait pas si sa lettre est arrivée à bon port.

Dans les systèmes orientés connexion, une connexion est établie entre l'émetteur et le récepteur avant le transfert des données. Le système téléphonique est un exemple de système orienté connexion. L'appelant initie l'appel, une connexion s'établit, puis la communication a lieu.

Les processus réseau sans connexion sont souvent appelés processus à commutation de paquets. Au cours de leur acheminement, les paquets peuvent emprunter différents chemins et arriver de manière désordonnée. Le chemin emprunté par chaque paquet est déterminé par divers critères. Certains de ces critères, tels que la bande passante disponible, peuvent varier d'un paquet à l'autre.

Les processus réseau orientés connexion sont souvent appelés processus à commutation de circuits. Une connexion avec le destinataire est établie avant que le transfert des données ne commence. Tous les paquets circulent de manière séquentielle sur le même circuit virtuel ou physique.

Internet est un réseau sans connexion gigantesque, dans lequel la majorité des transmissions de paquets sont traitées par le protocole IP. Le protocole TCP ajoute les services orientés connexion et fiables de la couche 4 au protocole IP.

3.1.5 Anatomie d'un paquet IP

Champs de la couche réseau

0 4	8		16 19	24 31
VERS	HLEN	Type de service	Longueur totale	
Identification			Indicateurs	Décalage de fragment
Durée de vie		Protocole	Somme de contrôle d'en-tête	
Adresse IP source				
Adresse IP de destination				
Options IP (s'il y a lieu)				Remplissage
Données				
. . .				

Il s'agit des champs d'un en-tête de paquet IP. Leur longueur est fixe, sauf dans le cas des options IP et des champs de remplissage.

Les paquets IP comprennent les données des couches supérieures et un en-tête IP. Cette page présente le contenu de cet en-tête:

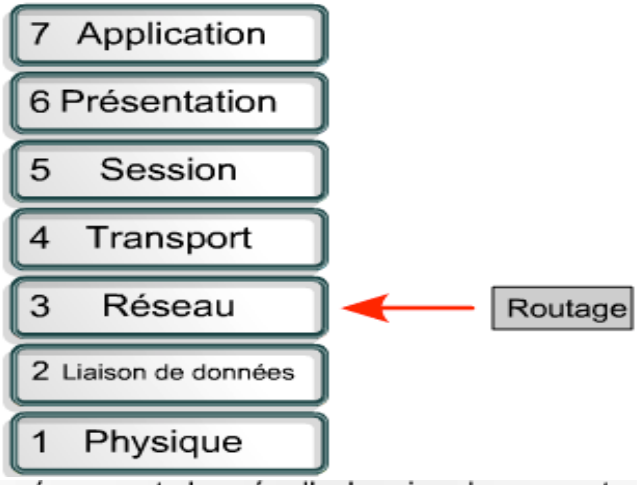
- **Version:** indique le format de l'en-tête du paquet IP. Le champ Version (4 bits) contient le numéro 4 s'il s'agit d'un paquet IPv4 ou le numéro 6 s'il s'agit d'un paquet IPv6. Ce champ n'est toutefois pas utilisé pour faire la distinction entre des paquets IPv4 et IPv6. C'est le rôle du champ relatif au type de protocole présent dans l'enveloppe de couche 2.
- **Longueur d'en-tête IP (HLEN):** indique la longueur de l'en-tête du datagramme en mots de 32 bits. Ce champ représente la longueur totale des informations d'en-tête et inclut les deux champs d'en-tête de longueur variable.
- **Type de service (ToS):** ce champ codé sur 8 bits indique le niveau d'importance attribué par un protocole de couche supérieure particulier.
- **Longueur totale (16 bits):** ce champ spécifie la taille totale du paquet en octets, données et en-tête inclus. Pour obtenir la taille des données proprement dites, soustrayez la longueur de l'en-tête IP de cette longueur totale.
- **Identification (16 bits):** identifie le datagramme actuel. Ce champ comporte le numéro de séquence.
- **Drapeaux (3 bits):** champ dans lequel les deux bits de poids faible contrôlent la fragmentation. Un bit indique si le paquet peut être fragmenté ou non, et l'autre si le paquet est le dernier fragment d'une série de paquets fragmentés.

- **Décalage de fragment (13 bits):** champ permettant de rassembler les fragments du datagramme. Il permet au champ précédent de se terminer sur une frontière de 16 bits.
- **Durée de vie (TTL):** champ indiquant le nombre de sauts par lesquels un paquet peut passer. Ce nombre est décrémenté à chaque passage du paquet dans un routeur. Lorsque le compteur atteint zéro, le paquet est éliminé. Cela empêche les paquets de circuler indéfiniment en boucle.
- **Protocole (8 bits):** indique quel protocole de couche supérieure, tel que TCP ou UDP, reçoit les paquets entrants une fois les processus IP terminés.
- **Somme de contrôle de l'en-tête (16 bits):** champ qui aide à garantir l'intégrité de l'en-tête IP.
- **Adresse source (32 bits):** : champ indiquant l'adresse IP du nœud à partir duquel a été envoyé le paquet.
- **Adresse de destination (32 bits):** champ indiquant l'adresse IP du nœud vers lequel sont envoyées les données.
- **Options:** permet au protocole IP de prendre en charge diverses options, telles que la sécurité. La longueur de ce champ peut varier.
- **Remplissage:** des zéros sont ajoutés à ce champ pour s'assurer que l'en-tête IP est toujours un multiple de 32 bits.
- **Données:** ce champ contient les informations de couche supérieure. Sa longueur est variable.

Si les adresses IP source et de destination sont des champs capitaux, les autres champs de l'en-tête font du protocole IP un protocole très souple. Les champs de l'en-tête répertorient les informations d'adressage source et de destination du paquet et indiquent souvent la longueur des données du message. Les informations de routage sont également contenues dans les en-têtes IP, qui, de ce fait, peuvent devenir longs et complexes.

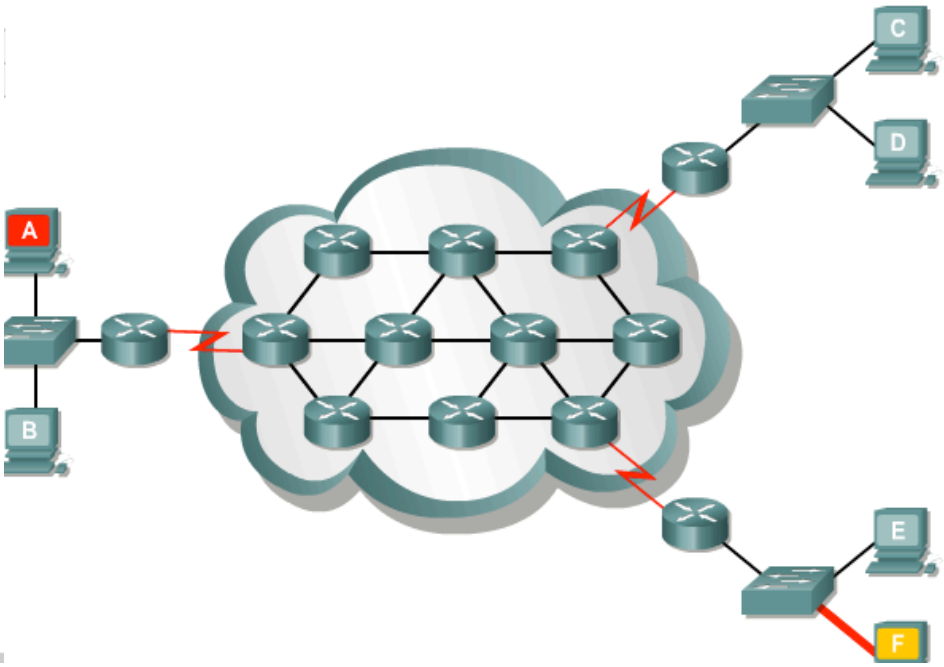
3.2 Protocoles de routage IP

3.2.1 Vue d'ensemble du routage



La couche réseau est chargée d'acheminer les paquets sur un réseau.

Le routage est une fonction de la couche 3 du modèle OSI. C'est un système d'organisation hiérarchique qui permet de regrouper des adresses individuelles. Ces dernières sont traitées comme un tout jusqu'à ce que l'adresse de destination soit requise pour la livraison finale des données.



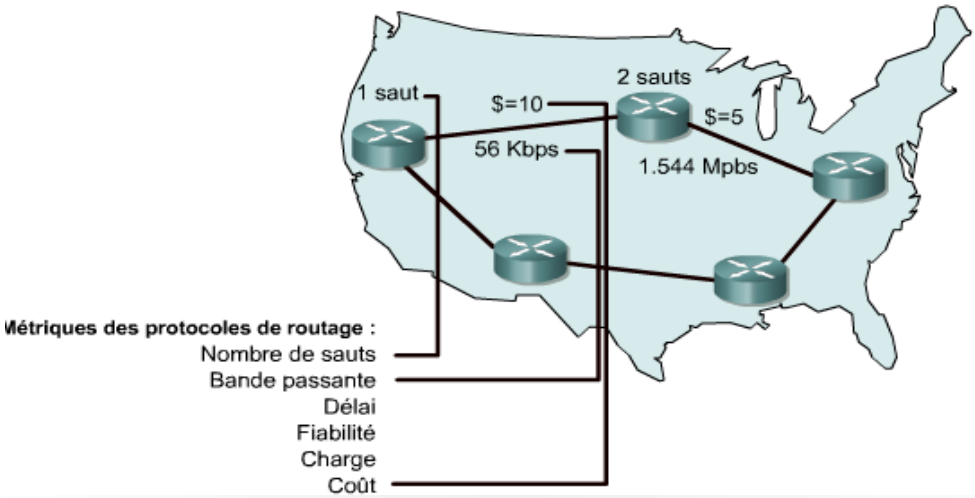
Routage

Le routage cherche le chemin le plus efficace d'une unité à une autre. Le matériel au centre du processus de routage est le routeur.

Il possède les deux fonctions principales suivantes:

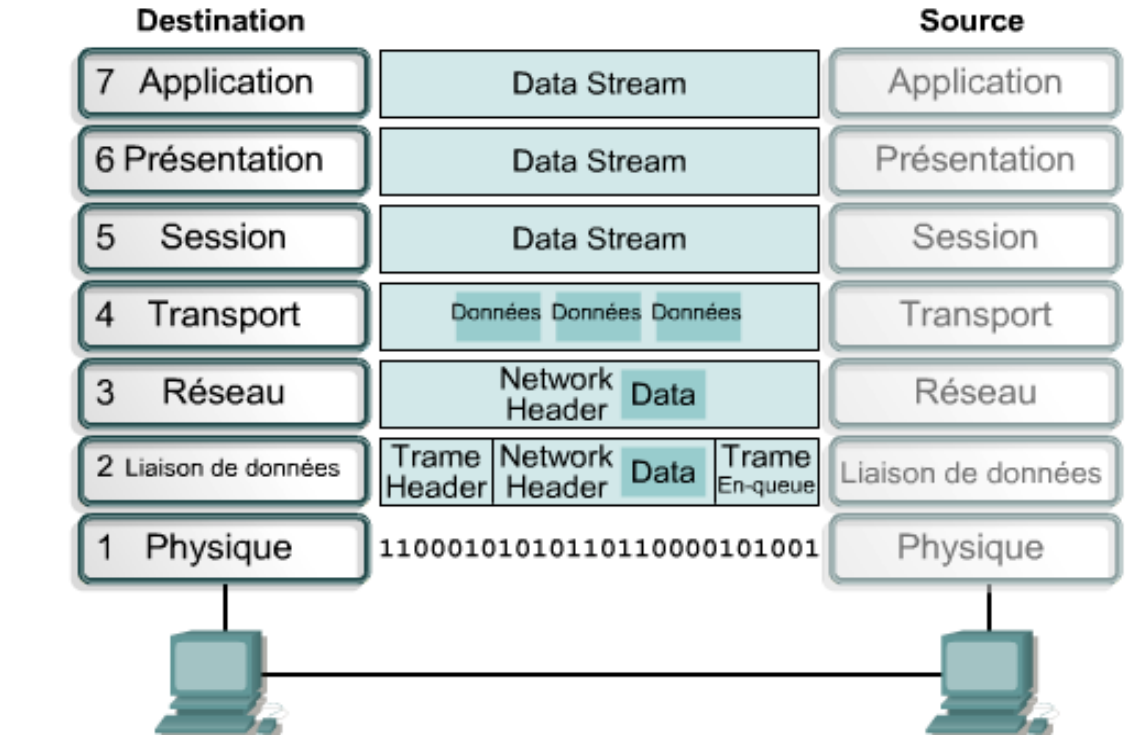
- Le routeur gère les tables de routage et s'assure que les autres routeurs ont connaissance des modifications apportées à la topologie du réseau. Il se sert des protocoles de routage pour échanger les informations de réseau.
- Le routeur détermine la destination des paquets à l'aide de la table de routage lorsque ceux-ci arrivent à l'une de ses interfaces. Il les transfère vers la bonne interface, ajoute les informations de trame de cette interface, puis transmet la trame.

Métriques de routage



La couche réseau est chargée d'acheminer les paquets sur un réseau.

Un routeur est une unité de couche réseau qui utilise une ou plusieurs métriques pour déterminer le chemin optimal par lequel acheminer le trafic réseau. Les métriques de routage sont les valeurs qui permettent de définir le meilleur chemin. Les protocoles de routage utilisent diverses combinaisons de ces métriques pour établir la meilleure route possible des données.



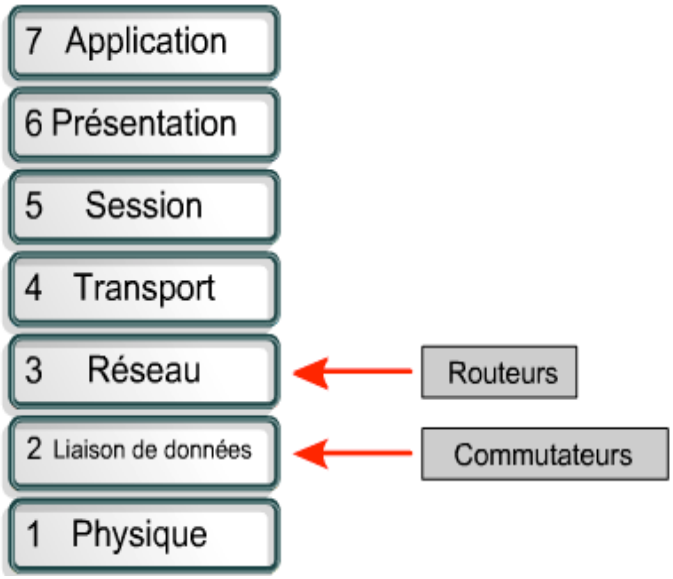
Les routeurs permettent d'interconnecter les segments d'un réseau ou des réseaux entiers. Leur rôle consiste à acheminer les trames de données entre les réseaux, en fonction des informations de la couche 3. Ils prennent des décisions logiques quant au meilleur acheminement possible des données, puis redirigent les paquets vers le port de sortie approprié afin qu'ils soient encapsulés pour la transmission. Les phases d'encapsulation et de désencapsulation se produisent à chaque passage d'un paquet dans un routeur. Le routeur doit en effet désencapsuler la trame de données de la couche 2 pour accéder à l'adresse de couche 3 et l'examiner. Comme vous pouvez le voir dans la figure , le processus intégral d'envoi des données implique des phases d'encapsulation et de désencapsulation au niveau des sept couches du modèle OSI. L'encapsulation consiste à fractionner le flux de données en segments et à ajouter les en-têtes et les en-queues appropriés avant de transmettre les données. Le processus de désencapsulation, quant à lui, consiste à retirer les en-têtes et les en-queues, puis à recombiner les données en un flux continu.

Ce cours présente le protocole routable le plus répandu, à savoir IP. D'autres protocoles routables existent, comme par exemple IPX/SPX et AppleTalk. Ces protocoles prennent en charge la couche 3. Ceux qui ne la prennent pas en charge sont des protocoles non routables.

Le plus connu d'entre eux est NetBEUI. Il s'agit d'un petit protocole rapide et efficace qui se contente de livrer les trames sur un seul segment.

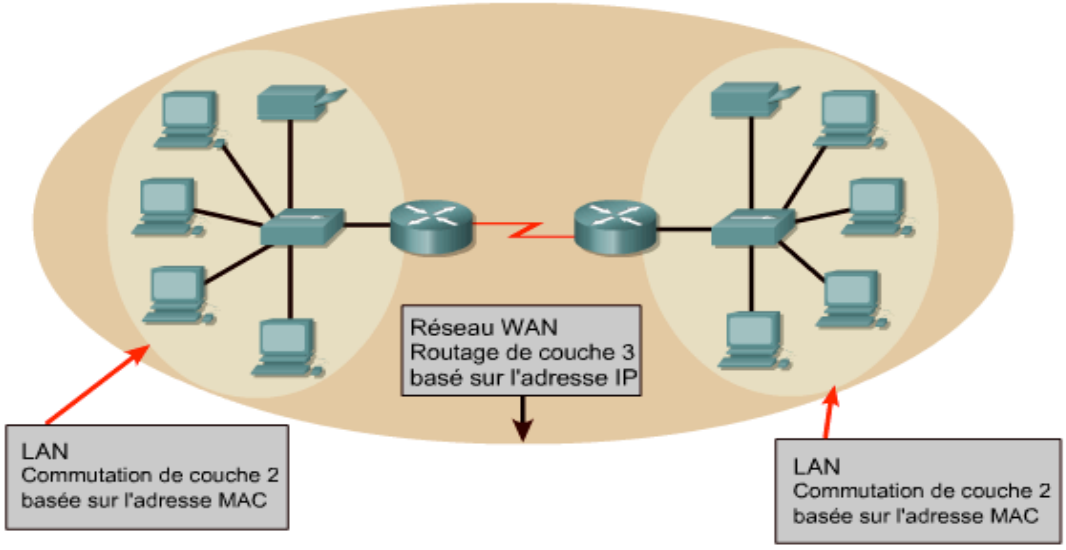
3.2.2 Routage et commutation

Cette page effectue une comparaison entre le routage et la commutation. En apparence, les routeurs et les commutateurs semblent jouer le même rôle. La principale différence entre les deux repose sur le fait que les commutateurs opèrent au niveau de la couche 2 du modèle OSI alors que les routeurs fonctionnent sur la couche 3. Autrement dit, ces deux matériels utilisent des informations différentes pour envoyer les données de la source à la destination.



La relation existant entre la commutation et le routage peut être comparée aux appels téléphoniques locaux et longue distance. Lorsqu'un appel est passé à un numéro comportant le même indicatif régional, il est traité par un commutateur local. Ce dernier ne peut effectuer le suivi que des numéros locaux. Il ne peut pas gérer l'ensemble des numéros de téléphone du monde entier. Lorsque le commutateur reçoit une demande pour un appel hors de sa zone, il transfère cet appel vers un commutateur de niveau supérieur à même de reconnaître les indicatifs régionaux. Celui-ci commute ensuite l'appel de sorte qu'il atteigne le commutateur local correspondant à son indicatif.

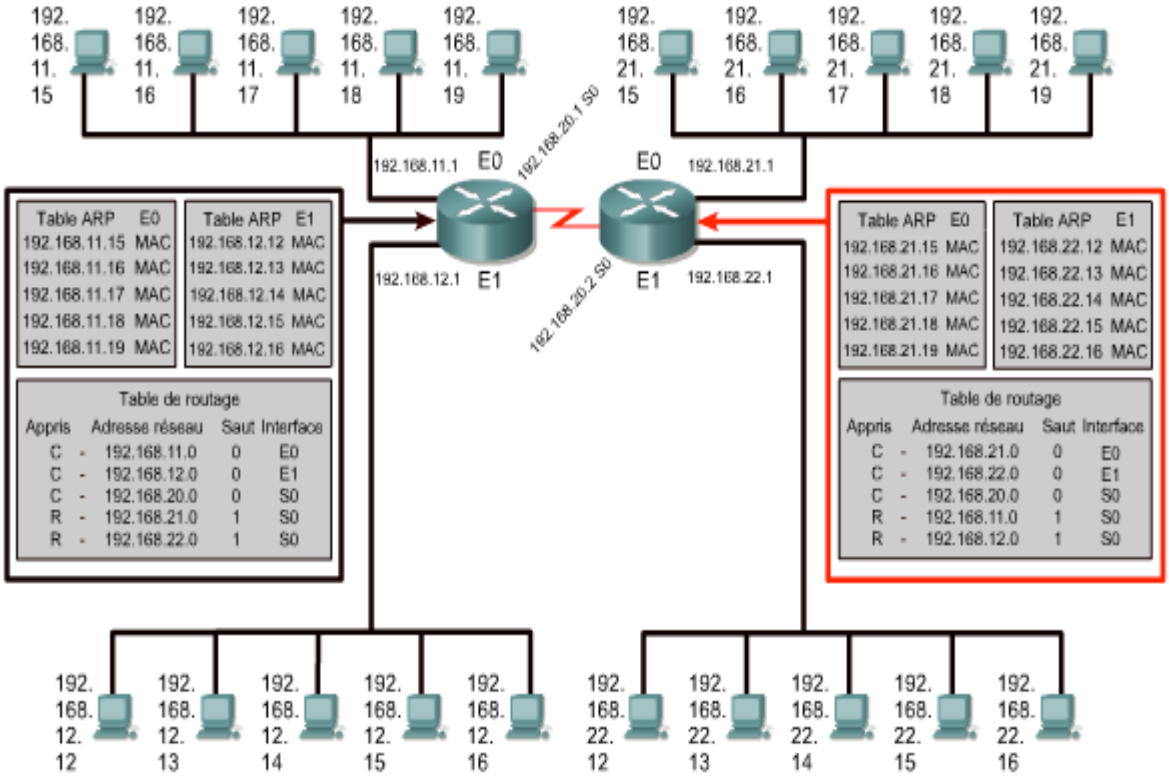
Commutation de la couche 2 et routage de la couche 3



La commutation de couche 2 s'effectue au sein du réseau LAN. Le routage de couche 3 achemine le trafic entre les domaines de broadcast. Cela nécessite le format d'adressage hiérarchique d'un système d'adressage de couche 3, tel que IP.

Le routeur joue un rôle similaire à celui du commutateur de niveau supérieur. La figure montre les tables ARP des adresses MAC de la couche 2 et les tables de routage des adresses IP de la couche 3. Chaque ordinateur et chaque interface de routeur gèrent une table ARP pour la communication de couche 2. La table ARP n'est utile que pour le domaine de broadcast auquel elle est connectée. Le routeur est également doté d'une table de routage qui lui permet d'acheminer les données hors du domaine de broadcast. Chaque entrée de table ARP contient une paire d'adresses IP-MAC.

Tables ARP et tables de routage



Fenêtre contextuelle (pop up)

Chaque ordinateur et chaque interface de routeur gèrent une table ARP pour la communication de couche 2. La table ARP n'est utile que pour le domaine de broadcast auquel elle est connectée. Le routeur est également doté d'une table de routage qui lui permet d'acheminer les données hors du domaine de broadcast. Chaque table ARP contient une paire d'adresses IP-MAC. Les adresses MAC sont représentées dans le schéma avec l'acronyme MAC, les adresses réelles étant trop longues pour pouvoir figurer ici. Les tables de routage cherchent également à savoir comment la route a été apprise. Dans cet exemple, elles sont directement connectées (représentées par un C) ou apprises par le biais du protocole RIP (représentées par un R). Les tables permettent de déterminer l'adresse IP des réseaux à atteindre, le nombre de sauts ou la distance jusqu'à ces réseaux, ainsi que l'interface à partir de laquelle les données doivent être acheminées pour atteindre le réseau de destination.

Le commutateur de couche 2 établit sa table de transmission à l'aide d'adresses MAC. Lorsqu'un hôte possède des données pour une adresse IP non locale, il envoie la trame au routeur le plus proche. Ce routeur est également appelé « passerelle par défaut ». L'hôte se sert de l'adresse MAC du routeur comme adresse MAC de destination.

Un commutateur interconnecte des segments appartenant au même réseau ou sous-réseau logique. Dans le cas d'hôtes non locaux, le commutateur transfère la trame au routeur en fonction de l'adresse MAC de destination. Le routeur analyse alors l'adresse de destination de couche 3 du paquet afin de déterminer l'acheminement de la trame. L'hôte X connaît l'adresse IP du routeur parce que sa configuration IP contient l'adresse IP de la passerelle par défaut.

À l'instar du commutateur qui gère une table d'adresses MAC connues, le routeur possède une table d'adresses IP connue sous le nom de table de routage. Les adresses MAC ne sont pas organisées de manière logique, tandis que l'organisation des adresses IP est, elle, hiérarchique. Un commutateur se contentant de rechercher les adresses appartenant à son segment dans sa table, il ne traite qu'un nombre limité d'adresses MAC non organisées. Les routeurs, quant à eux, ont besoin d'un système d'adressage hiérarchique qui va permettre de regrouper les adresses similaires et de les traiter en tant qu'une seule et même unité réseau, et ce jusqu'à ce que les données atteignent le segment de destination.

Sans cette organisation, Internet ne pourrait fonctionner. Vous pourriez comparer ce dernier à une bibliothèque dans laquelle des millions de pages imprimées s'entasseraient. Cette documentation serait tout simplement inutile puisqu'il serait impossible de localiser un seul de ces documents. Lorsque ces pages sont identifiées et assemblées en un livre et que chacun de ces livres est répertorié dans un index, la recherche et l'utilisation des données deviennent alors possibles.

Comparaison entre les fonctions du routeur et celles du commutateur

Fonctions	Routeur	Commutateur
Vitesse	Lente	Rapide
Couches OSI	Couche 3	Couche 2
Adressage utilisé	IP	MAC
Broadcasts	Bloqués	Transmis
Sécurité	Élevée	Faible

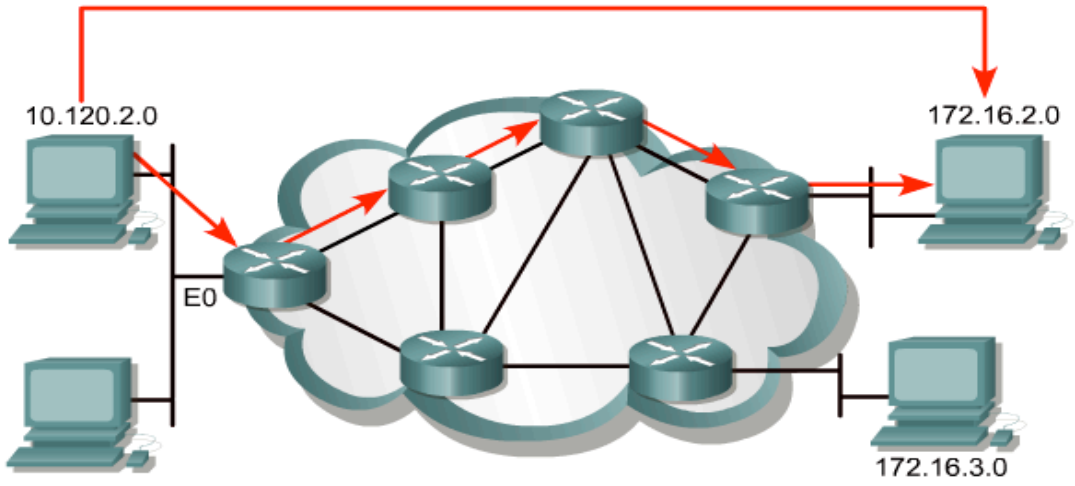
La vitesse et la sécurité sont relatives et dépendent de la configuration de l'équipement.

Une autre différence entre les réseaux routés et commutés réside dans le fait que ces derniers ne bloquent pas les broadcasts. Les commutateurs peuvent par conséquent voir leur fonctionnement perturbé par des tempêtes de broadcasts. Les routeurs bloquant les broadcasts LAN, les tempêtes n'affectent que le domaine de broadcast dont elles sont issues. Du fait de ce blocage, les routeurs offrent une meilleure sécurité et un meilleur contrôle de la bande passante que les commutateurs.

3.2.3 Protocole routé et protocole de routage

Les protocoles routés ou routables sont utilisés au niveau de la couche réseau afin de transférer les données d'un hôte à l'autre via un routeur. Les protocoles routés transportent les données sur un réseau. Les protocoles de routage permettent aux routeurs de choisir le meilleur chemin possible pour acheminer les données de la source vers leur destination.

Protocole routé



Les protocoles routés transportent les données d'une station d'extrémité à une autre.

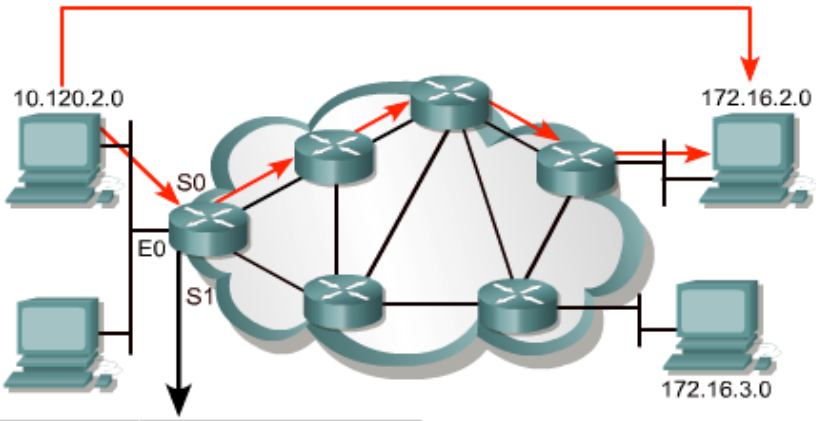
Le protocole routé englobe notamment les fonctions suivantes:

- Il inclut n'importe quelle suite de protocoles réseau capable de fournir assez d'informations dans l'adresse de couche réseau pour permettre au routeur d'effectuer le transfert vers l'unité suivante, jusqu'à la destination finale.
- Il définit le format et l'usage des champs dans un paquet.

Le protocole IP (*Internet Protocol*) et le protocole IPX (*Internetwork Packet Exchange*) de Novell, mais aussi DECnet, AppleTalk, Banyan VINES et Xerox Network Systems (XNS), sont des exemples de protocoles routés.

Les routeurs utilisent des protocoles de routage pour échanger des tables de routage et partager d'autres informations d'acheminement. En d'autres termes, les protocoles de routage permettent aux routeurs d'acheminer les protocoles routés.

Protocole de routage



Protocole réseau	Réseau de destination	Interface de sortie
Connecté	10.120.2.0	E0
RIP	172.16.2.0	S0
IGRP	172.16.3.0	S1

Les protocoles de routage sont utilisés par les routeurs pour déterminer les chemins et gérer les tables de routage.
Une fois le chemin déterminé, le routeur peut acheminer le protocole routé.

Protocole de routage = RIP, IGRP

Les fonctions du protocole de routage sont en partie les suivantes:

- Il fournit les processus utilisés pour partager les informations d'acheminement.
- Il permet aux routeurs de communiquer entre eux afin de mettre à jour et de gérer les tables de routage.

Les protocoles de routage prenant en charge le protocole routé IP sont par exemple les protocoles RIP, IGRP, OSPF, BGP et EIGRP

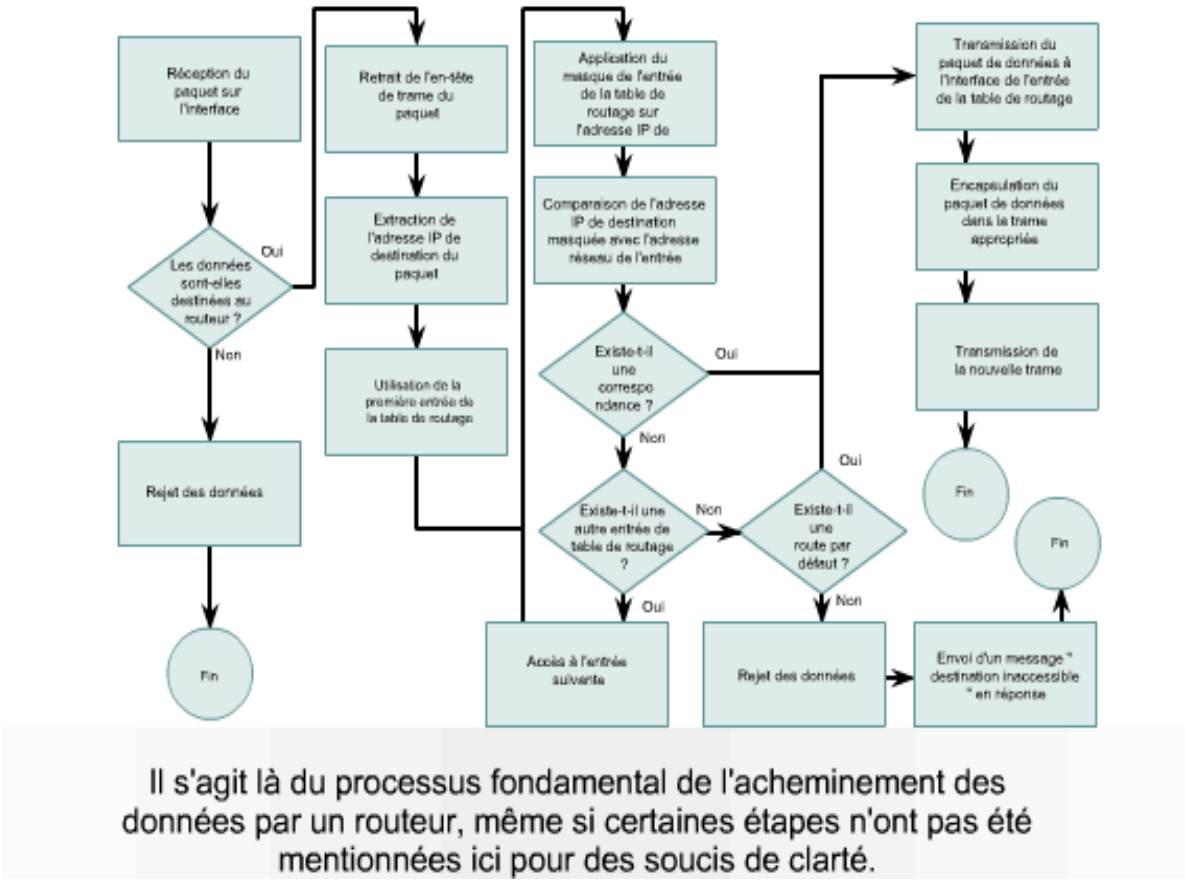
3.2.4 Détermination du chemin

La détermination du chemin se produit au niveau de la couche réseau. Ce processus permet au routeur de comparer l'adresse de destination aux routes disponibles dans sa table de routage et de choisir le meilleur chemin possible. Les routeurs acquièrent ces chemins soit par l'intermédiaire du routage statique, soit par l'intermédiaire du routage dynamique. Les chemins configurés manuellement par l'administrateur réseau sont appelés «routes statiques». Ceux que le routeur a acquis d'autres routeurs à l'aide d'un protocole de routage sont dits «routes dynamiques».

La détermination du chemin permet au routeur de choisir le port à partir duquel envoyer un paquet pour que celui-ci arrive à destination. On appelle ce processus le routage d'un paquet. Chaque routeur rencontré sur le chemin du paquet est appelé un saut. Le nombre de sauts constitue la distance parcourue. La détermination du chemin peut être comparée à la situation où une personne conduit sa voiture d'un endroit de la ville à un autre. Le conducteur consulte une carte qui lui indique les rues par lesquelles passer pour arriver à sa destination, tout comme le routeur consulte sa table de routage. Il passe d'un carrefour à un autre, de la même façon qu'un paquet circule d'un routeur à un autre lors de chaque saut. À chaque carrefour, le conducteur peut choisir de prendre à gauche, à droite ou de continuer tout droit. Il en va de même pour le routeur lorsqu'il choisit le port de sortie à partir duquel le paquet sera envoyé.

Le conducteur prend ses décisions en fonction de certains facteurs, comme l'état du trafic, la limitation de vitesse, le nombre de voies, les péages et si une route est fréquemment fermée ou pas. Il est parfois plus rapide de prendre le chemin le plus long en passant par des petites routes peu fréquentées que de prendre l'autoroute embouteillée. De même, les routeurs vont prendre leurs décisions en fonction de la charge, de la bande passante, du délai, du coût et de la fiabilité d'une liaison de réseau.

Processus de routage



Il s'agit là du processus fondamental de l'acheminement des données par un routeur, même si certaines étapes n'ont pas été mentionnées ici pour des soucis de clarté.

Les processus impliqués dans la sélection du chemin pour chaque paquet sont les suivants:

- Le routeur compare l'adresse IP du paquet reçu avec ses tables IP.
- Il extrait l'adresse de destination du paquet.
- Le masque de la première entrée dans la table de routage est appliqué à l'adresse de destination.
- La destination masquée est comparée avec l'entrée de la table de routage.
- Si une correspondance est établie, le paquet est transmis au port associé à cette entrée de table.
- Si aucune correspondance n'est établie, l'entrée suivante de la table est examinée.
- Si le paquet ne correspond à aucune des entrées de la table, le routeur recherche l'existence d'une route par défaut.
- Si une route par défaut a été définie, le paquet est transmis au port qui lui est associé. La route par défaut est le chemin qui doit être utilisé lorsque aucune correspondance n'a pu être établie avec la table de routage. Elle est configurée par l'administrateur réseau.

Si aucun chemin par défaut n'existe, le paquet est éliminé. Un message est alors souvent envoyé à l'unité émettrice des données pour signaler que la destination n'a pu être atteinte.

3.2.5 Tables de routage

Les routeurs emploient des protocoles de routage pour construire et gérer les tables de routage contenant les informations d'acheminement. Le processus de sélection du chemin en est ainsi facilité. Les protocoles de routage placent diverses informations d'acheminement dans les tables de routage. Le contenu de ces informations varie selon le protocole de routage utilisé. Les tables de routage contiennent les informations nécessaires à la transmission des paquets de données sur les réseaux connectés. Les équipements de couche 3 interconnectent les domaines de broadcast ou les réseaux LAN. Le transfert des données nécessite un système d'adressage hiérarchique.

Tables de routage

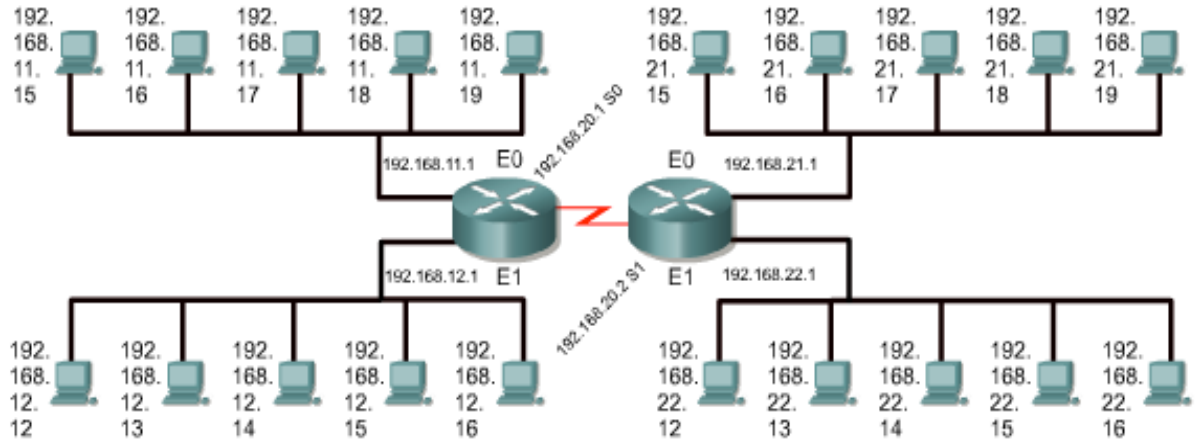


Table de routage

Appris	Adresse réseau	Saut	Interface
C -	192.168.11.0	0	E0
C -	192.168.12.0	0	E1
C -	192.168.20.0	0	S0
R -	192.168.21.0	1	S0
R -	192.168.22.0	1	S0

Table de routage

Appris	Adresse réseau	Saut	Interface
C -	192.168.21.0	0	E0
C -	192.168.22.0	0	E1
C -	192.168.20.0	0	S1
R -	192.168.11.0	1	S1
R -	192.168.12.0	1	S1

Les routeurs conservent les informations suivantes dans leurs tables de routage:

- **Type de protocole:** cette information identifie le type de protocole de routage qui a créé chaque entrée.
- **Associations du saut suivant:** indique au routeur que la destination lui est directement connectée, ou qu'elle peut être atteinte par le biais d'un autre routeur appelé le «saut suivant» vers la destination finale. Dès réception d'un paquet, le routeur vérifie l'adresse de destination et tente de trouver une correspondance dans sa table de routage.
- **Métrique de routage:** les métriques utilisées varient selon les protocoles de routage et permettent de déterminer les avantages d'une route sur une autre. Par exemple, le protocole RIP se sert d'une seule métrique de routage : le nombre de sauts. Le protocole IGRP crée une valeur de métrique composite à partir des métriques de fiabilité, de délai, de charge et de bande passante.
- **Interfaces de sortie:** cette information désigne l'interface à partir de laquelle les données doivent être envoyées pour atteindre leur destination finale.

Les routeurs s'envoient des messages afin de mettre à jour leurs tables de routage. Certains protocoles de routage transmettent ces messages de manière périodique. D'autres ne les envoient que lorsque des changements sont intervenus dans la topologie du réseau. Certains transmettent l'intégralité de la table dans leurs messages de mise à jour alors que d'autres se contentent d'envoyer les modifications. L'analyse des mises à jour de routage provenant de routeurs directement connectés permet aux routeurs de créer et de gérer leur table de routage

3.2.6 Algorithmes et métriques de routage

Un algorithme est une solution détaillée d'un problème. Les algorithmes utilisés pour définir le port auquel envoyer un paquet diffèrent selon les protocoles de routage. Ils reposent sur l'utilisation de métriques pour prendre ce type de décision.

Les protocoles de routage sont conçus pour répondre à un ou plusieurs des objectifs suivants:

- **Optimisation:** capacité d'un algorithme de routage à sélectionner le meilleur chemin. Ce dernier sera choisi en fonction des métriques et de la pondération utilisées dans le calcul. Par exemple, un algorithme peut utiliser à la fois le nombre de sauts et le délai comme métriques, mais considérer que le délai doit prévaloir dans le calcul.
- **Simplicité et réduction du temps-système:** plus l'algorithme est simple et plus il sera traité efficacement par le processeur et la mémoire du routeur. Ce paramètre est important si le réseau veut pouvoir évoluer vers des proportions plus conséquentes, comme Internet.

- **Efficacité et stabilité:** un algorithme de routage doit pouvoir fonctionner correctement dans des circonstances inhabituelles ou imprévues, comme les défaillances de matériels, les surcharges et les erreurs de mise en œuvre.
- **Flexibilité:** : un algorithme de routage doit pouvoir s'adapter rapidement à toutes sortes de modifications du réseau, touchant par exemple la disponibilité et la mémoire du routeur, la bande passante ou le délai réseau.
- **Rapidité de convergence:** la convergence est le processus par lequel tous les routeurs s'entendent sur les routes disponibles. Lorsqu'un événement sur le réseau entraîne des modifications au niveau de la disponibilité d'un routeur, des mises à jour sont nécessaires afin de rétablir la connectivité du réseau. Une convergence lente des algorithmes de routage peut empêcher la livraison des données.

Algorithmes et métriques de routage

Protocole	Métrique	Nombre maximum de routeurs	Origines
Protocole RIP	Nombre de sauts	15	Xerox
Protocole IGRP	• Bande passante • Charge • Délai • Fiabilité	255	Cisco

Les métriques de routage sont les valeurs utilisées pour déterminer le meilleur chemin jusqu'au saut suivant.

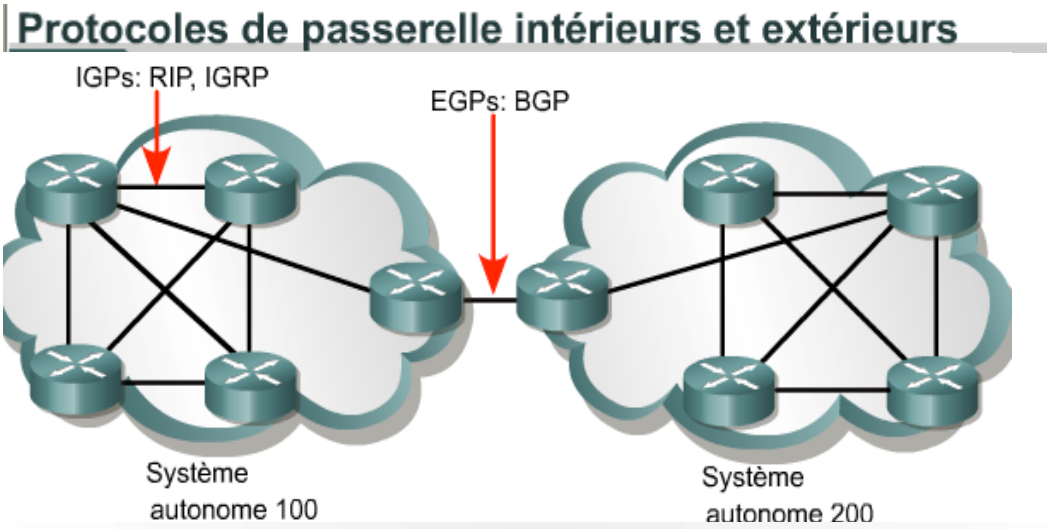
Les algorithmes de routage utilisent différentes métriques pour déterminer la meilleure route. Chacun d'eux interprète à sa façon ce qui est le mieux. L'algorithme génère un nombre, appelé valeur métrique, pour chaque chemin traversant le réseau. Les algorithmes de routage perfectionnés effectuent la sélection du chemin en fonction de plusieurs métriques combinées en une valeur composite. Généralement, les valeurs métriques faibles indiquent le meilleur chemin.
Les métriques peuvent être calculées sur la base d'une seule caractéristique de chemin, comme elles peuvent l'être sur la base de plusieurs. Les métriques les plus communément utilisées par les protocoles de routage sont les suivantes:

- **Bande passante:** la bande passante représente la capacité de débit d'une liaison. Une liaison Ethernet de 10 Mbits/s est généralement préférable à une ligne louée de 64 Kbits/s.
- **Délai:** le délai est le temps nécessaire à l'acheminement d'un paquet, pour chaque liaison, de la source à la destination. Il dépend de la bande passante des liaisons intermédiaires, de la quantité de données pouvant être temporairement stockées sur chaque routeur, de la congestion du réseau et de la distance physique.
- **Charge:** la charge est la quantité de trafic sur une ressource réseau telle qu'un routeur ou une liaison.
- **Fiabilité:** la fiabilité se rapporte habituellement au taux d'erreurs de chaque liaison du réseau.
- **Nombre de sauts:** le nombre de sauts est le nombre de routeurs par lesquels un paquet doit passer avant d'arriver à destination. Chaque routeur équivaut à un saut. Un nombre de sauts égal à 4 signifie que les données doivent passer par quatre routeurs pour atteindre leur destination. Lorsque plusieurs chemins sont possibles, c'est le chemin comportant le moins de sauts qui est privilégié.
- **Tops:** délai d'une liaison de données utilisant les tops d'horloge d'un PC IBM, un top d'horloge correspondant environ à 1/18 seconde.

Coût: le coût est une valeur arbitraire, généralement basée sur la bande passante, une dépense monétaire ou une autre mesure, attribuée par un administrateur réseau.

3.2.7 Protocoles IGP et EGP

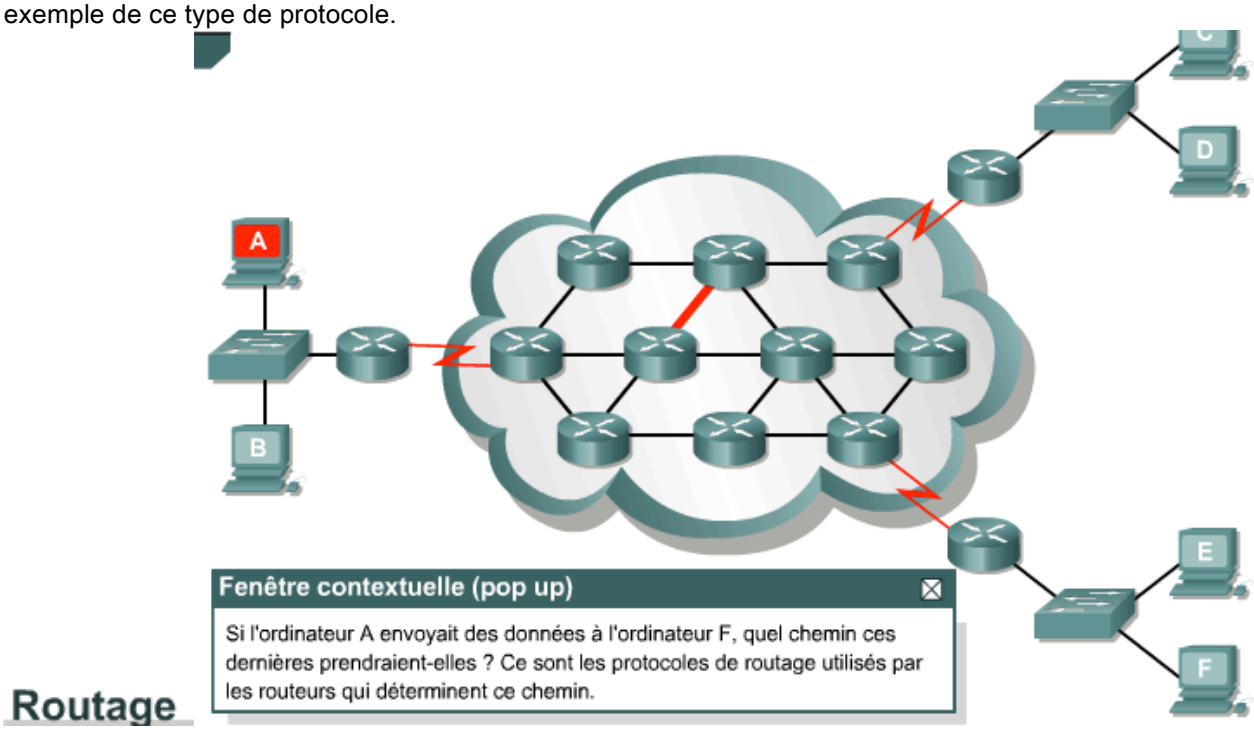
Un système autonome est un réseau ou un ensemble de réseaux placés sous un même contrôle administratif, tel que le domaine cisco.com. Un tel système est constitué de routeurs qui présentent une vue cohérente du routage vers l'extérieur.
Il existe deux familles de protocoles de routage : les protocoles IGP (*Interior Gateway Protocol*) et les protocoles EGP (*Exterior Gateway Protocol*).



Les protocoles IGP acheminent les données au sein d'un système autonome. Il s'agit:

- Des protocoles RIP et RIPv2.
- Du protocole IGRP.
- Du protocole EIGRP.
- Du protocole OSPF.
- Du protocole IS-IS (*Intermediate System-to-Intermediate System*).

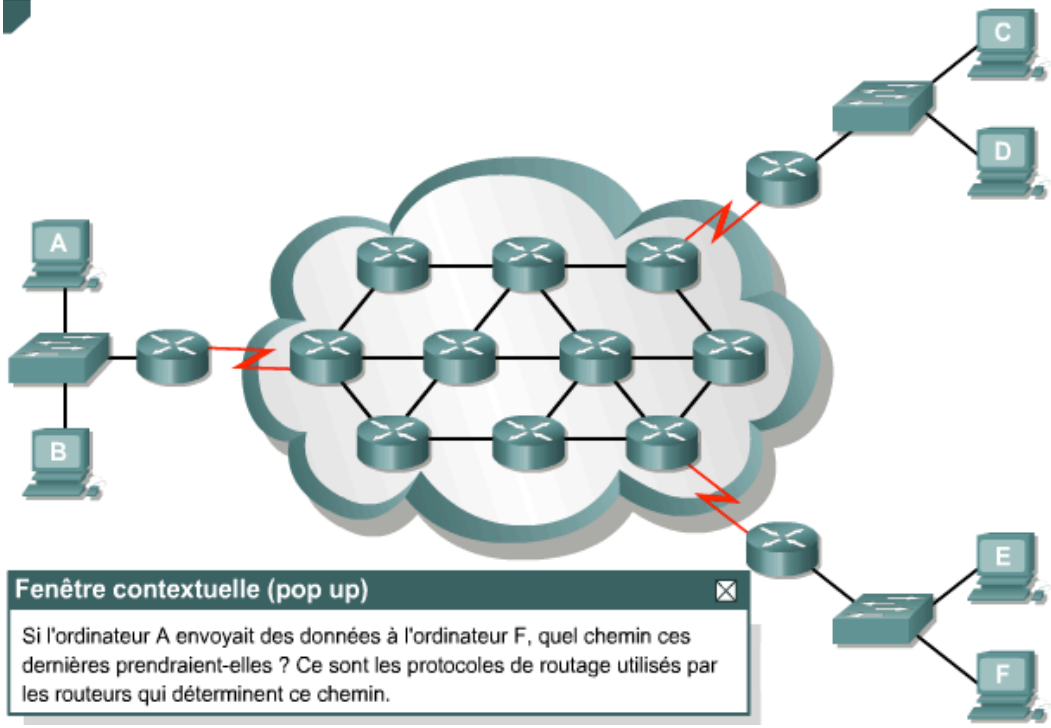
Les protocoles EGP acheminent les données entre les systèmes autonomes. Le protocole BGP est un exemple de ce type de protocole.



3.2.8 État de liens et vecteur de distance

Les protocoles de routage peuvent être classés en protocoles IGP ou EGP. Le type utilisé va dépendre de l'administration du groupe de routeurs, notamment s'ils sont placés sous une seule et même administration ou pas. Les protocoles IGP peuvent être subdivisés en protocoles à vecteur de distance et en protocoles à état de liens. Cette page présente le routage à vecteur de distance et à état de liens, et explique quand ces différents types de protocoles de routage sont utilisés.

Routage



La méthode de routage à vecteur de distance détermine la direction (vecteur) et la distance vers n'importe quelle liaison de l'interréseau. La distance peut être représentée par le nombre de sauts vers cette liaison. Les routeurs faisant appel aux algorithmes de vecteur de distance envoient périodiquement l'intégralité ou une partie des entrées de leur table de routage aux routeurs adjacents, que des modifications aient été ou non apportées au réseau. Lorsqu'un routeur reçoit une mise à jour de routage, il vérifie tous les chemins connus et modifie le cas échéant sa propre table de routage. Ce processus est également appelé «routage par rumeur». La connaissance qu'a un routeur du réseau dépend de la vue dont dispose le routeur adjacent sur la topologie du réseau.
Les exemples suivants sont des exemples de protocoles à vecteur de distance:

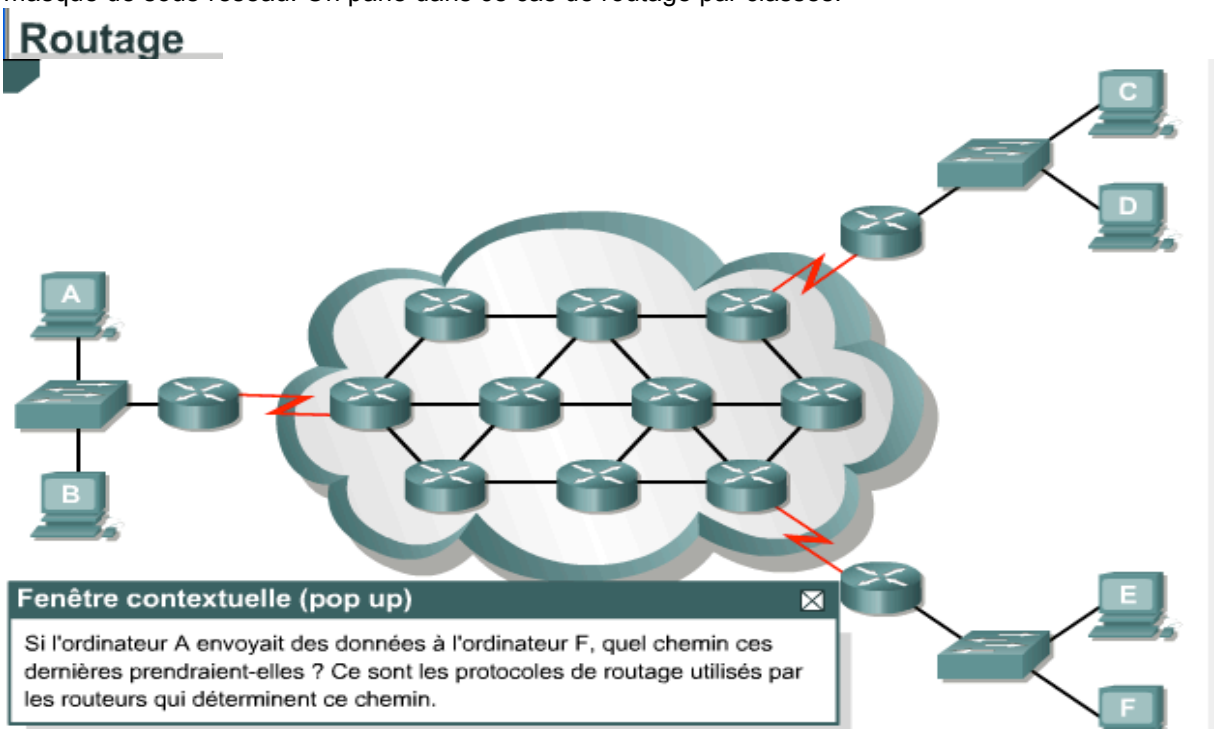
- **Routing Information Protocol (RIP):** le protocole RIP est le protocole IGP le plus utilisé sur Internet. Son unique métrique de routage est basée sur le nombre de sauts.
- **Interior Gateway Routing Protocol (IGRP):** ce protocole IGP a été développé par Cisco afin de résoudre les problèmes associés au routage dans des réseaux hétérogènes étendus.
- **Enhanced IGRP (EIGRP):** ce protocole IGP, propriété de Cisco, inclut un grand nombre des caractéristiques d'un protocole de routage à état de liens. Il est, de ce fait, également appelé «protocole hybride symétrique», bien qu'il soit véritablement à classer dans les protocoles de routage à vecteur de distance avancés.

Les protocoles à état de liens ont été conçus pour pallier les limitations des protocoles de routage à vecteur de distance. Ils ont pour avantage de répondre rapidement aux moindres changements sur le réseau en envoyant des mises à jour déclenchées uniquement après qu'une modification soit survenue. Ces protocoles envoient par ailleurs des mises à jour périodiques, connues sous le nom d'actualisations à état de liens, à des intervalles moins fréquents, par exemple toutes les 30 minutes.
Dès qu'une unité a détecté la modification d'une liaison ou d'une route, elle crée une mise à jour de routage à état de liens (LSA, *link-state advertisement*) concernant cette liaison. Cette mise à jour LSA est ensuite transmise à tous les équipements voisins. Chacun d'eux en prend une copie, met à jour sa base de données à état de liens et transmet la mise à jour LSA aux autres unités voisines. Cette diffusion de mises à jour LSA est nécessaire afin que tous les équipements de routage puissent créer des bases de données transcrivant de manière précise la topologie du réseau et mettre à jour leur table de routage.
Les algorithmes à état de liens se servent généralement de leurs bases de données pour créer des entrées dans la table de routage qui privilégient le chemin le plus court. Les protocoles OSPF (*Open Shortest Path First*) et IS-IS (*Intermediate System-to-Intermediate System*) sont des exemples de protocoles à état de liens.

L'activité de média interactive souligne les différences entre les protocoles de routage à vecteur de distance et les protocoles à état de liens.

3.2.9 Protocoles de routage

Le protocole RIP est un protocole de routage à vecteur de distance qui utilise le nombre de sauts comme métrique pour déterminer la direction et la distance vers n'importe quelle liaison de l'interréseau. S'il existe plusieurs chemins vers une destination, le protocole RIP sélectionne celui qui comporte le moins de sauts. Toutefois, le nombre de sauts étant la seule métrique de routage utilisée par ce protocole, il ne sélectionne pas toujours le chemin le plus rapide. En outre, le protocole RIP ne peut acheminer un paquet au-delà de 15 sauts. La version 1 du protocole RIP (RIPv1) n'incluant pas les informations de masque de sous-réseau dans les mises à jour de routage, tous les équipements du réseau doivent nécessairement utiliser le même masque de sous-réseau. On parle dans ce cas de routage par classes.



La version 2 (RIPv2) fournit un routage par préfixe et envoie les informations de masque de sous-réseau dans ses mises à jour de routage. On parle ici de routage sans classe. Avec les protocoles de routage sans classe, les sous-réseaux d'un même réseau peuvent comporter des masques différents. Cette technique fait référence à l'utilisation de masques de sous-réseau de longueur variable (VLSM).

Le protocole IGRP est un protocole de routage à vecteur de distance mis au point par Cisco. Il a été spécifiquement développé pour résoudre les problèmes associés au routage dans de grands réseaux qui dépassaient la portée des protocoles tels que RIP. IGRP peut sélectionner le chemin disponible le plus rapide en fonction du délai, de la bande passante, de la charge et de la fiabilité. Le nombre de sauts maximal autorisé est par ailleurs considérablement plus élevé que celui défini dans le protocole RIP. Le protocole IGRP utilise uniquement le routage par classes.

Le protocole OSPF est un protocole de routage à état de liens mis au point par l'IETF (*Internet Engineering Task Force*) en 1988. Il a été écrit pour permettre la gestion de vastes interréseaux évolutifs hors de portée du protocole RIP.

Le protocole IS-IS (*Intermediate System-to-Intermediate System*) est un protocole de routage à état de liens utilisé pour les protocoles routés autres qu'IP. Il existe une extension du protocole IS-IS, Integrated IS-IS, qui, elle, prend en charge plusieurs protocoles routés dont IP.

À l'instar du protocole IGRP, EIGRP est un protocole développé par Cisco. Il constitue une version perfectionnée du protocole IGRP. Plus précisément, ce protocole offre de meilleures performances d'exploitation comme une convergence plus rapide et une bande passante moins surchargée. C'est un protocole à vecteur de distance avancé qui a également recours à certaines fonctions des protocoles à état de liens. Il est, par conséquent, parfois classé dans les protocoles de routage hybrides.

Le protocole BGP (*Border Gateway Protocol*) est un exemple de protocole EGP (*External Gateway Protocol*). Il permet l'échange d'informations de routage entre systèmes autonomes tout en garantissant une sélection de chemins exempts de boucle. Le protocole BGP est le protocole de mises à jour de routage le plus utilisé par les grandes sociétés et les FAI sur Internet. BGP4 est la première version de BGP à

prendre en charge le routage interdomaine sans classes (CIDR) et le regroupement de routes. À la différence des protocoles IGP courants, comme RIP, OSPF et EIGRP, le protocole BGP ne se sert pas de métriques tels que le nombre de sauts, la bande passante ou le délai. Il prend à la place ses décisions de routage selon des stratégies de réseau (ou règles utilisant divers attributs de chemin BGP).

3.3 Mécanisme de découpage en sous-réseaux

3.3.1 Classes d'adresses réseau IP

Cette page permet de revoir les classes d'adresses IP. La combinaison des différentes classes d'adresses IP offre une plage d'hôtes comprise entre 256 et 16,8 millions.

Pour permettre une gestion efficace d'un nombre limité d'adresses IP, il est possible de subdiviser toutes les classes en sous-réseaux plus petits. La figure donne une vue d'ensemble de la division réseaux-hôtes.

Configurations de bits d'adresses IP

Classe A	Réseau	Hôte		
Octet	1	2	3	4

Classe B	Réseau		Hôte	
Octet	1	2	3	4

Classe C	Réseau			Hôte
Octet	1	2	3	4

Classe D	Hôte			
Octet	1	2	3	4

Les adresses de classe D sont utilisées pour les groupes de multicast. Il n'est pas nécessaire d'allouer des octets ou des bits pour séparer les adresses réseau et hôte. Les adresses de classe E sont réservées à la recherche.

3.3.2 Introduction au découpage en sous-réseaux

Pour effectuer un découpage en sous-réseaux, des bits de la partie hôte doivent être réattribués au réseau. Cette opération est souvent appelée « emprunt » de bits. Il serait en fait plus juste de parler de « prêt ». L'emprunt se fait toujours à partir du bit d'hôte situé le plus à gauche, à savoir celui le plus proche du dernier octet de la partie réseau.

Subdivision des octets hôte d'une adresse de classe C

Adresse réseau de classe C 192.168.10.0

11000000.10101000.00001010.00000000
N . N . N . H

11000000.10101000.00001010.00000000
N . N . N . sN H

Dans cet exemple, trois bits ont été alloués pour désigner le sous-réseau.

Les adresses de sous-réseau contiennent une partie réseau de classe A, B ou C, plus un champ de sous-réseau et un champ d'hôte. Le champ de sous-réseau et le champ d'hôte sont créés à partir de la partie hôte d'origine de l'adresse IP principale. Cette opération s'effectue en réattribuant des bits de la partie hôte à la partie réseau d'origine de l'adresse. Le fait de pouvoir diviser la partie hôte d'origine de l'adresse en nouveaux champs de sous-réseau et d'hôte permet à l'administrateur réseau de gagner en flexibilité au niveau de l'adressage.

Subdivision des octets hôte d'une adresse de classe B

Adresse réseau de classe B 147.10.0.0
10010011.00001010.00000000.00000000 N . N . H . H
10010011.00001010.00000000.00000000 N . N . sN H. H Dans cet exemple, cinq bits ont été alloués pour désigner le sous-réseau.

En plus de faciliter la gestion du réseau, le découpage en sous-réseaux permet à l'administrateur réseau de confiner le broadcast et de garantir une certaine sécurité sur le réseau LAN. Ce dernier point est rendu possible du fait que l'accès aux autres sous-réseaux ne peut se faire qu'à travers les services d'un routeur. Les accès peuvent par ailleurs être sécurisés grâce à l'utilisation de listes de contrôle d'accès qui autorisent ou refusent l'accès à un sous-réseau en fonction de plusieurs critères. Ces listes feront l'objet d'une étude plus loin dans le cursus. Certains propriétaires de réseaux de classes A et B ont également découvert que le découpage en sous-réseaux était source de revenus du fait de la vente ou de la location d'adresses IP jusqu'alors inutilisées.

Subdivision des octets hôte d'une adresse de classe A

Adresse réseau de classe A 28.0.0.0
00011100.00000000.00000000.00000000 N . H . H . H
00011100.00000000.00000000.00000000 N . sN . sN H . H Dans cet exemple, douze bits ont été alloués pour désigner le sous-réseau.

Le découpage en sous-réseaux est une opération purement interne à un réseau. Vu de l'extérieur, un réseau LAN est un réseau unique qui ne donne aucune information sur sa structure interne. Cette perspective permet de conserver des tables de routage de petite taille et efficaces. Supposons l'adresse de nœud locale 147.10.43.14 sur le sous-réseau 147.10.43.0. À l'extérieur du réseau LAN, seul le numéro de réseau principal 147.10.0.0 est visible. La raison en est simple : l'adresse de sous-réseau locale 147.10.43.0 n'est valable qu'au sein du réseau LAN subdivisé en sous-réseaux.

10.3.3 Détermination de l'adresse d'un masque de sous-réseau

Le nombre de bits à sélectionner dans le processus de découpage en sous-réseaux dépend du nombre maximal d'hôtes requis par sous-réseau. Pour calculer le nombre de sous-réseaux et d'hôtes créés par l'emprunt de bits, il est nécessaire d'avoir des notions de base en calculs binaires et de connaître la valeur de position des bits dans un octet.

Tableau de découpage en sous-réseaux (valeur et position des bits)

Bits empruntés	1	2	3	4	5	6	7	8
Valeur	128	64	32	16	8	4	2	1

Quelle que soit la classe d'adresse IP, les deux derniers bits du dernier octet ne doivent jamais être attribués au sous-réseau. Ces bits constituent les deux derniers bits significatifs. Si vous utilisez tous les bits disponibles, à l'exception de ces deux derniers, pour créer des sous-réseaux, les sous-réseaux créés ne comporteront que deux hôtes utilisables. Il s'agit d'une méthode de conservation d'adresses pratique pour l'adressage des liaisons de routeur série. Toutefois, pour un réseau LAN effectif, cela impliquerait des coûts en équipement dépassant l'entendement.

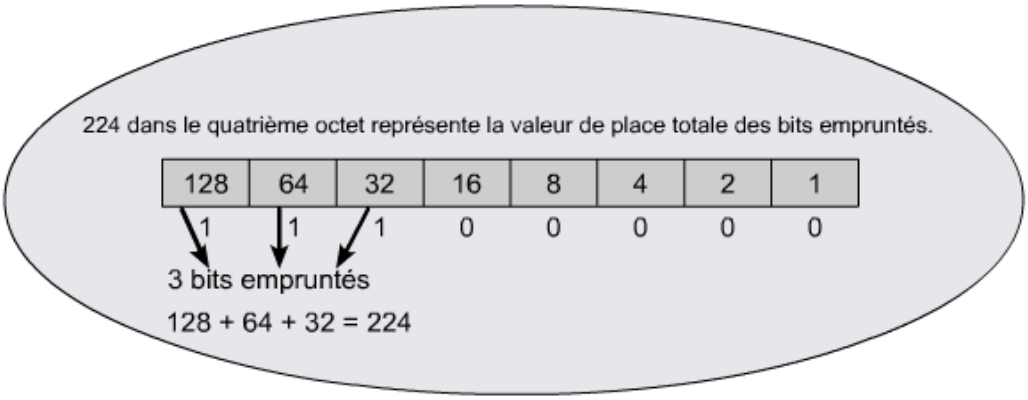
Tableau de découpage en sous-réseaux (identificateur du masque de sous-réseau)

Format /#	/25	/26	/27	/28	/29	/30	N/A	N/A
Masque	128	192	224	240	248	252	254	255
Bits empruntés	1	2	3	4	5	6	7	8
Valeur	128	64	32	16	8	4	2	1

Une adresse de classe C avec le masque /25 emprunte uniquement un bit, comme indiqué dans le tableau ci-dessus. Toutefois, une adresse de classe B avec le même masque va emprunter neuf bits.

Le masque de sous-réseau apporte au routeur l'information dont il a besoin pour déterminer le réseau et le sous-réseau auxquels un hôte donné appartient. Le masque de sous-réseau est créé en utilisant des 1 dans les positions binaires du réseau. Les bits du sous-réseau sont déterminés en ajoutant la valeur de position des bits empruntés. Ainsi, si trois bits sont empruntés, le masque d'une adresse de classe C donne 255.255.255.224. Au format de barre oblique, ce masque est représenté par /27. Le nombre situé après la barre oblique correspond au nombre total de bits utilisés pour les parties réseau et sous-réseau.

Découpage en sous-réseaux



Pour savoir combien de bits doivent être utilisés, le concepteur du réseau doit d'abord calculer le nombre d'hôtes nécessaires à son sous-réseau le plus vaste ainsi que le nombre de sous-réseaux requis. Supposons que le réseau requiert 30 hôtes et cinq sous-réseaux. La méthode la plus simple pour déterminer le nombre de bits à réattribuer est de se reporter au tableau de découpage en sous-réseaux. Si vous consultez la ligne intitulée « Hôtes utilisables », vous constatez que trois bits sont nécessaires pour 30 hôtes. Le tableau vous informe également que six sous-réseaux utilisables sont en même temps créés, ce qui répond tout à fait à vos besoins actuels. Il existe une différence entre les hôtes utilisables et le nombre total d'hôtes qui tient à l'utilisation de deux adresses spécifiques pour chaque sous-réseau : l'ID du réseau (représenté par la première adresse disponible) et l'adresse de broadcast (représentée par la dernière adresse disponible). Savoir emprunter le nombre de bits appropriés nécessaires aux sous-réseaux et aux hôtes de chacun des sous-réseaux constitue un exercice périlleux qui peut être à l'origine d'un certain nombre d'adresses hôtes inutilisées dans les divers sous-réseaux. Le routage par classes ne permet pas de limiter la perte de ces adresses. En revanche, le routage sans classe (qui sera abordé un peu plus loin dans ce cours) peut vous aider à récupérer un bon nombre de ces adresses perdues.

Tableau de découpage en sous-réseaux

Format /#	/25	/26	/27	/28	/29	/30	N/A	N/A
Masque	128	192	224	240	248	252	254	255
Bits empruntés	1	2	3	4	5	6	7	8
Valeur	128	64	32	16	8	4	2	1
Nombre total de		4	8	16	32	64		
Sous-réseaux u		2	6	14	30	62		
Nombre total d'l		64	32	16	8	4		
Hôtes utilisables		62	30	14	6	2		

Une adresse de classe C avec le masque /25 emprunte uniquement un bit, comme indiqué dans le tableau ci-dessus. Toutefois, une adresse de classe B avec le même masque va emprunter neuf bits.

Pour résoudre les problèmes liés à la subdivision en sous-réseaux, vous pouvez faire appel à la même méthode que celle utilisée pour la création du tableau des sous-réseaux. Cette méthode se base sur la formule suivante :

Nombre de sous-réseaux utilisables = deux à la puissance du nombre de bits attribués au sous-réseau ou nombre de bits empruntés, moins deux. La soustraction correspond aux deux adresses réservées que sont l'adresse du réseau et l'adresse de broadcast du réseau.

$(2^{\text{nombre de bits empruntés}}) - 2 =$ sous-réseaux utilisables

$(2^3) - 2 = 6$

Nombre d'hôtes utilisables = deux à la puissance des bits restants, moins deux (pour les adresses réservées que sont l'adresse du sous-réseau et l'adresse de broadcast du sous-réseau).

$(2^{\text{nombre de bits hôtes restants}}) - 2 =$ hôtes utilisables

$(2^5) - 2 = 30$

3.3.4 Application du masque de sous-réseau

Système de sous-réseaux

Numéro du sous-réseau	ID du sous-réseau	Plage d'hôtes	ID de broadcast
0	192.168.10.0	.1--.30	192.168.10.31
1	192.168.10.32	.33--.62	192.168.10.63
2	192.168.10.64	.65--.94	192.168.10.95
3	192.168.10.96	.97--.126	192.168.10.127
4	192.168.10.128	.129--.158	192.168.10.159
5	192.168.10.160	.161--.190	192.168.10.191
6	192.168.10.192	.193--.222	192.168.10.223
7	192.168.10.224	.225--.254	192.168.10.255

Une fois le masque de sous-réseau défini, vous pouvez l'utiliser pour établir le mod��le de sous-réseau. Le tableau de la figure donne un exemple du nombre de sous-réseaux et d'adresses qui peuvent être créés en attribuant trois bits au champ de sous-réseau. Cela permet en fait de créer huit sous-réseaux comportant chacun 32 hôtes. La numérotation des sous-réseaux commence à zéro (0), et le premier sous-réseau est donc toujours le sous-réseau zéro.

Le remplissage du tableau se fait automatiquement pour trois de ses champs mais demande quelques calculs pour les autres. L'adresse du sous-réseau zéro est identique à celle du réseau principal, ici 192.168.10.0. L'adresse de broadcast pour l'ensemble du réseau est le nombre le plus élevé, soit 192.168.10.255 dans notre cas. Le troisième nombre directement obtenu est l'ID du sous-réseau numéro sept. Il est constitué des trois octets du réseau et du numéro de masque de sous-réseau inséré au niveau

du quatrième octet. Trois bits ont été attribués au champ de sous-réseau donnant la valeur 224. L'ID du sous-réseau 7 est 192.168.10.224. L'insertion de ces nombres entraîne la définition de points de contrôle qui vérifieront l'exactitude du tableau une fois celui-ci complété.

Tableau de découpage en sous-réseaux

Format /#	/25	/26	/27	/28	/29	/30	N/A	N/A
Masque	128	192	224	240	248	252	254	255
Bits empruntés	1	2	3	4	5	6	7	8
Valeur	128	64	32	16	8	4	2	1
Nombre total de sous-réseaux		4	8	16	32	64		
Sous-réseaux utilisables		2	6	14	30	62		
Nombre total d'hôtes		64	32	16	8	4		
Hôtes utilisables		62	30	14	6	2		

Une adresse de classe C avec le masque /25 emprunte uniquement un bit, comme indiqué dans le tableau ci-dessus. Toutefois, une adresse de classe B avec le même masque va emprunter neuf bits.

En consultant le tableau de découpage en sous-réseaux ou en appliquant la formule, on constate que les trois bits attribués au champ de sous-réseau donne un résultat total de 32 hôtes dans chacun des sous-réseaux. À partir de ces informations, vous pouvez calculer l'adresse de chacun des sous-réseaux. Il vous suffit en effet d'ajouter 32 à chacun des numéros précédents, en commençant par le sous-réseau zéro. Notez que la partie hôte de l'adresse de sous-réseau ne comporte que des bits à 0.

Le champ de broadcast est le dernier numéro de chaque sous-réseau et il ne comporte que des 1 dans la partie hôte. Cette adresse ne permet la diffusion que vers les hôtes d'un même sous-réseau. L'adresse du sous-réseau zéro étant 192.168.10.0 et le nombre total d'hôtes s'élevant à 32 hôtes, l'adresse de broadcast est la suivante : 192.168.10.31. En effet, si l'on commence à calculer à partir de zéro, le 32ème numéro séquentiel est le numéro 31. Il est important de garder à l'esprit qu'en gestion de réseaux, zéro (0) constitue un vrai nombre.

Vous pouvez renseigner la colonne relative à l'adresse de broadcast de la même manière que vous avez indiqué l'adresse des sous-réseaux. Ajoutez simplement 32 à l'adresse de broadcast précédente du sous-réseau. Une autre méthode consiste à partir du bas de cette colonne et à remonter vers le haut en soustrayant 1 de l'adresse de sous-réseau précédente.

3.3.5 Découpage de réseaux de classe A et B en sous-réseaux

La méthode de découpage en sous-réseaux des réseaux de classes A et B est identique à celle utilisée pour les réseaux de classe C, à l'exception du nombre de bits impliqués qui est considérablement plus élevé. Le nombre de bits disponibles à attribuer au champ de sous-réseau dans une adresse de classe A est de 22 bits, tandis qu'il est de 14 bits pour une adresse de classe B.

Subdivision des octets hôte d'une adresse réseau de classe B

Adresse réseau de classe B 147.10.0.0 (14 bits disponibles)
11001011.00001010.00000000.00000000 N . N . H . H
10010011.00001010.00000000.00000000 N . N . sN . sN H Dans cet exemple, 12 bits ont été alloués pour désigner le sous-réseau.

Subdivision des octets hôte d'une adresse réseau de classe A

Adresse réseau de classe A 28.0.0.0 (22 bits disponibles)
00011100.00000000.00000000.00000000 N . H . H . H
00011100.00000000.00000000.00000000 N . sN . sN . sN H
Dans cet exemple, 20 bits ont été alloués pour désigner le sous-réseau.

En attribuant 12 bits d'une adresse de classe B au champ de sous-réseau, vous créez le masque de sous-réseau 255.255.255.240 ou /28. L'ensemble des huit bits ont été attribués dans le troisième octet donnant 255, la valeur totale des huit bits. Quatre bits ont été attribués dans le quatrième octet donnant le résultat 240. Petit rappel : le masque de format /# correspond à la somme totale des bits attribués au champ de sous-réseau en plus des bits fixes du réseau.

Découpage en sous-réseaux

Masque	128	192	224	240	248	252	254	255
Bits empruntés	1	2	3	4	5	6	7	8
Valeur	128	64	32	16	8	4	2	1
Sous-réseaux	2	4	8	16	32	64	128	256

Une adresse de classe C avec le masque /25 emprunte uniquement un bit, comme indiqué dans le tableau ci-dessus. Toutefois, une adresse de classe B avec le même masque va emprunter neuf bits.

L'attribution de 20 bits d'une adresse de classe A au champ de sous-réseau crée le masque de sous-réseau 255.255.255.240 ou /28. L'ensemble des huit bits des deuxième et troisième octets sont affectés au champ de sous-réseau, ainsi que quatre bits du quatrième octet.
Ici, il apparaît clairement que les masques de sous-réseau des adresses de classes A et B sont identiques. À moins d'associer le masque à une adresse réseau, il est impossible de savoir combien de bits ont été affectés au sous-réseau.
Quelle que soit la classe sur laquelle porte la subdivision, les règles sont les mêmes:

Nombre total de sous-réseaux = $2^{\text{nombre de bits empruntés}}$

Nombre total d'hôtes = $2^{\text{nombre de bits restants}}$

Sous-réseaux utilisables = $2^{\text{nombre de bits empruntés}}$ moins 2

Hôtes utilisables = $2^{\text{nombre de bits restants}}$ moins 2

3.3.6 Calcul du sous-réseau via l'opération AND

Les routeurs se servent des masques de sous-réseau pour déterminer le sous-réseau de chacun des nœuds. On parle alors d'opération AND logique. Il s'agit d'un processus binaire par lequel le routeur calcule l'ID de sous-réseau d'un paquet entrant. L'opération AND est similaire à une multiplication.
Ce processus s'effectue au niveau binaire. Il est par conséquent nécessaire d'afficher l'adresse IP et le masque au format binaire. L'opération AND est appliquée à l'adresse IP et à l'adresse du sous-réseau avec pour résultat l'ID du sous-réseau. Cette information permet au routeur de transférer le paquet à l'interface appropriée.

Adresse du paquet	201.10.11.65	11001001.00001010.00001011.01000001
AND		
Masque	255.255.255.224	11111111.11111111.11111111.11100000
ID du sous-réseau	201.10.11.64	11001001.00001010.00001011.01000000

Le découpage en sous-réseaux est une opération qui s'apprend. Il vous faudra vous exercer de nombreuses heures avant de pouvoir développer des systèmes flexibles et exploitables. Vous pouvez trouver de nombreux outils de calcul de sous-réseaux sur le Web. Un administrateur réseau se doit cependant de savoir créer manuellement ces sous-réseaux afin de pouvoir élaborer de manière efficace le système de réseaux adéquat et de pouvoir vérifier la validité des résultats d'un outil de calcul. Ce dernier se

contente en effet de fournir le système d'adressage final, sans indiquer le système initial. En outre, l'utilisation d'outils de calcul, quels qu'ils soient, est interdite pendant l'examen de certification.

Résumé

- Un protocole est un ensemble de règles qui déterminent le mode de communication entre ordinateurs sur les réseaux.
- Les protocoles routés transportent les données sur un réseau.
- Les protocoles de routage permettent aux routeurs de choisir le meilleur chemin pour acheminer les données de la source vers leur destination.
- Le découpage en sous-réseaux permet aux administrateurs réseau de subdiviser les réseaux en segments.

Le protocole IP est dit protocole non orienté connexion parce qu'aucune connexion à un circuit dédié n'est établie entre la source et la destination avant la transmission. Il est considéré comme non fiable car il ne vérifie pas la bonne livraison des données. S'il est nécessaire de vérifier la bonne livraison des données, il faut combiner le protocole IP à un protocole de transport orienté connexion, tel que TCP. S'il n'est pas nécessaire de vérifier l'intégrité des données à la livraison, IP peut être utilisé avec un protocole sans connexion, tel que UDP. Les processus réseau sans connexion sont souvent appelés processus à commutation de paquets, tandis que les processus réseau orientés connexion sont dits processus à commutation de circuits.

Les protocoles ajoutent des informations de contrôle aux données au niveau de chaque couche du modèle OSI tout au long de leur transmission sur le réseau. Ces informations étant ajoutées au début et à la fin des données, on parle d'encapsulation des données. La couche 3 ajoute des informations d'adresse réseau ou logique aux données et la couche 2 des informations d'adresse locale ou physique.

Le routage de la couche 3 et la commutation de la couche 2 permettent d'acheminer et de livrer les données sur le réseau. Au départ, le routeur reçoit une trame de couche 2 avec un paquet de couche 3 encapsulé en son sein. Il doit retirer la trame de couche 2 et examiner le paquet de couche 3. Si ce dernier est destiné à une adresse locale, le routeur doit l'encapsuler dans une nouvelle trame dotée de la bonne adresse MAC locale de destination. Si les données doivent être transmises vers un autre domaine de broadcast, le routeur encapsule le paquet de couche 3 dans une nouvelle trame de couche 2 contenant l'adresse MAC de l'unité d'interconnexion de réseaux suivante. La trame est ainsi transférée sur le réseau de domaine de broadcast en domaine de broadcast jusqu'à sa livraison finale à l'hôte approprié.

Les protocoles routés, comme IP, transportent les données sur un réseau. Les protocoles de routage, quant à eux, permettent aux routeurs de choisir le meilleur chemin pour acheminer les données de la source à leur destination. Ce chemin peut être une route statique, entrée manuellement, ou une route dynamique, connue par le biais des protocoles de routage. Dans le cas du routage dynamique, les routeurs s'échangent des mises à jour de routage afin de gérer leur table. Les algorithmes de routage mettent en œuvre des métriques pour traiter les mises à jour de routage et informer les tables de routage des meilleurs chemins possibles. La convergence décrit la vitesse à laquelle tous les routeurs acquièrent une même vue du réseau après qu'il ait subi une modification.

Les protocoles IGP (*Interior Gateway Protocol*) sont des protocoles de routage qui acheminent les données au sein de systèmes autonomes, tandis que les protocoles EGP (*Exterior Gateway Protocol*) acheminent les données entre les différents systèmes autonomes. Les protocoles IGP peuvent être subdivisés en protocoles à vecteur de distance et en protocoles à état de liens. Les routeurs faisant appel aux protocoles à vecteur de distance envoient périodiquement des mises à jour de routage constituées de l'intégralité ou d'une partie de leur table de routage. Les routeurs utilisant les protocoles à état de liens, pour leur part, se servent des mises à jour de routage à état de liens (LSA) pour envoyer des mises à jour uniquement lorsque des modifications surviennent dans la topologie du réseau. Ils peuvent en outre, mais moins fréquemment, envoyer les tables de routage complètes.

Lors de la transmission des paquets sur le réseau, il est nécessaire que les unités puissent distinguer la partie réseau de la partie hôte de l'adresse IP. Un masque d'adresse de 32 bits, appelé masque de sous-réseau, permet d'indiquer les bits d'une adresse IP utilisés pour l'adresse réseau. Le masque de sous-réseau par défaut pour une adresse de classe A est 255.0.0.0. Pour une adresse de classe B, le masque de sous-réseau commence toujours par 255.255.0.0 et celui d'une adresse de classe C par 255.255.255.0. Le masque de sous-réseau peut être utilisé pour diviser un réseau existant en plusieurs « sous-réseaux ».

Le découpage d'un réseau en sous-réseaux permet de réduire la taille des domaines de broadcast, permet aux segments LAN situés dans plusieurs zones géographiques différentes de communiquer par le biais de routeurs et améliore la sécurité en isolant les segments LAN les uns des autres.
Les masques de sous-réseau personnalisés utilisent plus de bits que les masques par défaut en les empruntant à la partie hôte de l'adresse IP. Une adresse en trois parties est ainsi créée:

- L'adresse réseau d'origine;
- L'adresse de sous-réseau composée des bits empruntés;
- L'adresse hôte composée des bits restants après l'emprunt des bits servant à créer les sous-réseaux.

Les routeurs utilisent les masques de sous-réseau pour déterminer la partie sous-réseau d'une adresse d'un paquet entrant. On parle alors d'opération AND logique.