

Modèle OSI et routage **(Révision)**

Guy Roman, mars 2002

Table des matières.

<i>Le modèle de référence OSI</i>	3
<i>La couche physique du modèle OSI</i>	5
<i>La couche liaison de données du modèle OSI</i>	6
<i>La couche réseau</i>	6
<i>Le routage et les catégories de protocoles de routage.</i>	9
Les deux fonctions de base d'un routeur.	9
Les routes statiques et dynamiques.	9
La route par défaut.	10
Les protocoles routés et de routage.	10
Les protocoles de routage IP.	10
La convergence réseau.	10
Le routage à vecteur de distance.	10
Le routage à état de liens.	10
Comparaison des protocoles de routage à vecteur de distance et à état de liens.	10
Activation d'un processus de routage IP.	11
Configuration du protocole RIP.	11
<i>La couche de transport du modèle OSI.</i>	11
Un transport fiable.	11
La segmentation de la couche 4.	12
L'échange en trois étapes.	12
Utilisation d'une mémoire tampon dans la transmission.	12
Fenêtrage.	12
La fiabilité par accusé de réception.	12
<i>Résumé.</i>	13

Modèle OSI et routage

Révision : Le modèle de référence OSI et le routage

Le modèle de référence OSI

Les modèles de réseau utilisent des couches pour simplifier les fonctions réseau. Cette répartition des fonctions réseau est appelée organisation en couche. Pour comprendre l'importance de l'organisation en couche, examinons le modèle de référence OSI, un modèle en couche permettant de mettre en œuvre les communications entre ordinateurs. Les couches du modèle de référence OSI contribuent à simplifier les tâches nécessaires pour que deux ordinateurs puissent communiquer entre eux.

Comme **chaque couche peut être dédiée à des fonctions spécifiques**, le concepteur de réseau a la possibilité de choisir les fonctions et les équipements de réseau appropriés à chacune d'elles. Les sept couches du modèle de référence OSI correspondent chacune à une fonction distincte. Les raisons de cette répartition des fonctions réseau sont les suivantes :

- Les couches divisent les aspects du fonctionnement d'un réseau en éléments moins complexes.
- Elles définissent les interfaces standard pour la compatibilité " plug-and-play ".
- Elles permettent aux ingénieurs de concentrer leurs efforts de conception et de développement sur des fonctions modulaires.
- Elles favorisent la symétrie entre les différentes fonctions réseau modulaires pour assurer leur interopérabilité.
- Elles évitent que les modifications apportées à une zone affectent les autres zones, afin que chaque zone puisse évoluer rapidement.
- Elles répartissent la complexité du réseau en opérations distinctes, faciles à exécuter.

Chaque couche du modèle de référence OSI a une fonction spécifique :

- La couche application (**couche 7**) fournit des services réseau aux applications utilisateur. Par exemple, elle fournit des services de transfert de fichiers à un programme de traitement de texte.
- La couche présentation (**couche 6**) assure la représentation des données et le formatage du code. Elle traite également la syntaxe de transfert des données. Elle veille à ce que les données en provenance du réseau puissent être utilisées par l'application et que les informations envoyées par l'application soient transmises au réseau.
- La couche session (**couche 5**) établit, maintient et gère les sessions entre les applications.
- La couche transport (**couche 4**) segmente et réassemble les données en un flux de données. Elle peut garantir une connexion et assure un transport fiable.
- La couche réseau (**couche 3**) détermine le meilleur chemin pour déplacer des données d'un endroit à un autre. Le routeur fonctionne au niveau de cette couche. Elle recourt à des méthodes d'adressage logique qui peuvent être gérées par un administrateur. Elle utilise les méthodes d'adressage IP, Apple-Talk, DECnet, VINES et IPX.

- La couche liaison de données (**couche 2**) assure la transmission physique par le biais d'un média. Elle traite les notifications d'erreur, la topologie du réseau et le contrôle de flux. Elle utilise des adresses MAC (*Media Access Control*), qui sont aussi appelées adresses physiques ou matérielles.
- La couche physique (**couche 1**) fournit les procédures ainsi que les moyens électriques, mécaniques et fonctionnels pour établir et maintenir la liaison physique entre les systèmes. Elle utilise un média physique, tel qu'un câble à paires torsadées, un câble coaxial ou un câble à fibre optique.

Le modèle de référence **OSI décrit la façon dont les informations circulent** entre les programmes d'application de différents ordinateurs par le biais d'un média réseau. Lorsque les informations à envoyer descendent à travers les couches d'un système donné, elles ressemblent de moins en moins au langage humain et de plus en plus aux 1 et aux 0 que l'ordinateur comprend. Chaque couche utilise son propre protocole pour communiquer avec la couche homologue de l'autre système. Les informations échangées entre des couches homologues par le protocole de chaque couche sont appelées unités de données de protocole.

L'organisation en couche du modèle de référence OSI interdit la communication directe entre les couches homologues de différents hôtes. Par conséquent, chaque couche de l'hôte A doit compter sur les services fournis par les couches adjacentes de l'hôte A pour communiquer avec la couche homologue de l'hôte B. **Par exemple**, si couche 4 de l'hôte A doit communiquer avec la couche 4 de l'hôte B, elle doit utiliser les services de la couche 3 de l'hôte A.

L'encapsulation des données s'effectue en cinq étapes afin que le courrier électronique soit transmis à la destination appropriée :

Étape 1

Lorsqu'un utilisateur envoie un message électronique, les caractères alphanumériques sont convertis en **données** depuis la **couche 7 jusqu'à la couche 5**.

Étape 2

À l'aide des **segments à la couche 4**, la fonction de transport prépare les données en vue de leur transport sur le réseau et vérifie que les hôtes à chaque extrémité du système de messagerie peuvent communiquer de façon fiable.

Étape 3

Au niveau de la **couche 3**, les données sont placées dans un **paquet** (ou datagramme) contenant un en-tête réseau constitué des adresses logiques d'origine et de destination. Ensuite, les équipements transmettent les paquets au réseau via un chemin déterminé.

Étape 4

Chaque équipement de réseau doit placer le paquet dans une **trame au niveau de la couche 2** afin d'assurer la connexion à l'équipement suivant de la liaison directement connecté. Chaque équipement se trouvant sur le chemin sélectionné doit effectuer un verrouillage de trame pour se connecter à l'équipement suivant.

Étape 5

La trame doit être convertie en une **configuration de 1 et de 0** en vue de la **transmettre via le média** (souvent un fil de cuivre ou une fibre optique) au niveau de la **couche 1**. Une fonction de synchronisation permet aux équipements de distinguer ces bits lorsqu'ils circulent dans le média. Le média du réseau physique peut varier tout au long du chemin sélectionné. Par exemple, le message électronique peut provenir d'un réseau local, traverser le backbone (fédérateur) d'un campus et sortir par une liaison WAN pour atteindre sa destination sur un autre LAN distant.

La couche physique du modèle OSI

Les normes Ethernet et IEEE 802.3 se partagent la plus grande part du marché des protocoles de réseau local actuellement disponibles. Aujourd'hui, le terme Ethernet désigne souvent tous les réseaux locaux à détection de porteuse avec accès multiple (**CSMA/CD**) qui sont généralement conformes aux normes Ethernet, y compris la norme IEEE 802.3.

La technologie Ethernet a été initialement conçue pour combler le vide entre les réseaux longue distance à débit lent et les réseaux informatiques spécialisés à haut débit qui transportaient les données sur des distances très limitées. Elle convient particulièrement bien aux applications dans lesquelles un média de communication local doit gérer occasionnellement un trafic dense à des débits maximaux.

Le terme **Ethernet** désigne les mises en œuvre LAN comprenant les **trois catégories** principales suivantes :

- Les spécifications de réseau local Ethernet et IEEE 802.3 fonctionnant à 10 Mbits/s sur câble coaxial ou à paires torsadées.
- La spécification de réseau local Ethernet 100 Mbits/s, également appelée Fast Ethernet, fonctionnant à 100 Mbits/s sur câble à paires torsadées.
- La spécification de réseau local Ethernet 1 000 Mbits/s, également appelée Gigabit Ethernet, fonctionnant à 1 000 Mbits/s (1 Gbit/s) sur câble à paires torsadées ou à fibre optique.

Ethernet a survécu en tant que technologie de média essentielle, car elle est remarquablement **souple, simple** à mettre en œuvre et **facile à comprendre**. Les gestionnaires de réseau ont préféré Ethernet et ses dérivés aux autres technologies proposées, car elle répond efficacement aux besoins d'un grand nombre de mises en œuvre de campus. Pour remédier aux limites d'Ethernet, des utilisateurs inventifs (et des organismes de normalisation) ont créé des canaux Ethernet de plus en plus larges. Certains critiquent la technologie Ethernet parce qu'elle ne peut pas évoluer, mais sa méthode de transmission sous-jacente continue d'être l'un des principaux moyens de transport de données pour les applications de campus actuelles.

Les **normes de câblage Ethernet et IEEE 802.3** définissent un réseau local à **topologie en bus** fonctionnant à un débit de 10 Mbits/s. Les trois normes de câblage :

- 10Base2 - Appelée Ethernet à câble fin, cette norme autorise des segments de réseau pouvant atteindre 185 mètres sur câble coaxial.
- 10Base5 - Appelée ThickEthernet, cette norme autorise des segments de réseau pouvant atteindre 500 mètres sur câble coaxial.
- 10BaseT - Permet de transporter des trames Ethernet sur des câbles à paires torsadées bas de gamme.

Les normes de câblage Ethernet et IEEE 802.3 définissent un réseau à topologie en bus, avec un câble de connexion entre les stations d'extrémité et le média réseau réel. Dans le cas d'Ethernet, ce câble est appelé câble émetteur-récepteur. Il est connecté à un équipement émetteur-récepteur relié au média physique. La configuration IEEE 802.3 est similaire, sauf que le câble de connexion est appelé AUI (*Attachment Unit Interface*) et l'émetteur-récepteur, MAU (*Media Attachment Unit*). Dans les deux cas, le câble de connexion est relié à une carte d'interface (ou à un circuit d'interface) dans la station d'extrémité.

Les stations sont connectées au segment par un câble reliant une AUI de la station à un MAU directement raccordé au câble coaxial Ethernet. Comme la norme **10BaseT** ne donne accès qu'à une seule station, les **stations connectées** à un réseau local Ethernet selon cette norme sont presque toujours reliées **à un concentrateur ou à un commutateur LAN**.

La couche liaison de données du modèle OSI

L'accès au média réseau a lieu au niveau de la **couche liaison de données** du modèle de référence OSI. La couche liaison de données où réside l'**adresse MAC** est adjacente à la couche physique. Il n'existe **jamais deux adresses MAC identiques**. Par conséquent, dans un réseau, un équipement se connecte au média par la carte réseau et chaque carte réseau est dotée d'une adresse MAC unique.

Avant qu'une carte réseau quitte l'usine, le fabricant lui attribue une adresse MAC unique. Cette adresse est programmée sur une puce de la carte réseau. Comme l'adresse MAC se trouve sur la carte réseau, l'adresse physique de l'ordinateur sera modifiée si la carte réseau dont il est équipé est remplacée. Les **adresses MAC** sont **représentées** par des nombres **hexadécimaux** (base 16). Il existe deux formats d'adresse MAC : 0000.0c12.3456 et 00-00-0c-12-34-56.

Dans un **réseau Ethernet**, lorsqu'un équipement veut envoyer des données à un autre équipement, il peut ouvrir une voie de communication vers l'autre équipement en utilisant l'adresse MAC de celui-ci. Lorsqu'une **source envoie des données** sur un réseau, les données **transportent l'adresse MAC de leur destination**. Pendant que les données traversent le média réseau, la carte réseau de chaque équipement vérifie si son adresse MAC correspond à l'adresse physique de destination transportée par la trame. S'il n'existe **pas de correspondance**, la carte réseau **ignore la trame**, qui poursuit son chemin jusqu'à la prochaine station. S'il existe une **correspondance**, la carte réseau **copie la trame et place la copie dans l'ordinateur** dans lequel elle réside au niveau de la couche liaison de données. **Même si** la carte réseau effectue **une copie** de la trame et la stocke dans l'ordinateur, la **trame d'origine poursuit son chemin sur le réseau** où d'autres cartes réseau peuvent l'examiner et déterminer s'il existe une correspondance ou non.

La couche réseau

Plusieurs **protocoles** fonctionnent au niveau de la **couche réseau** du modèle de référence OSI.

- Le protocole IP assure l'acheminement au mieux des datagrammes, dans un réseau non orienté connexion. Il ne se préoccupe pas du contenu des datagrammes (paquets), mais il recherche un moyen de les acheminer à destination.
- Le protocole **ICMP (Internet Control Message Protocol)** offre des fonctions de messagerie et de contrôle.
- Le protocole **ARP (Address Resolution Protocol)** **détermine** les adresses de la couche liaison (**MAC**) de données **pour** les adresses **IP connues**.
- Le protocole de **résolution inverse d'adresse (RARP)** **détermine** les adresses réseau (**IP**) **lorsque** les adresses de la couche liaison de données (**MAC**) sont **connues**.

Dans un **environnement TCP/IP**, les stations d'extrémité communiquent avec des serveurs, des hôtes ou d'autres stations d'extrémité. La communication n'est **possible que si chaque nœud** utilisant la pile de protocoles TCP/IP **comporte une adresse logique unique de 32 bits**, appelée adresse **IP**.

Les **réseaux** peuvent être **segmentés en** plusieurs réseaux plus petits appelés **sous-réseaux**. L'adresse **IP** est donc **subdivisée** en numéro de **réseau**, numéro de **sous-réseau** et numéro d'**hôte**. Les **sous-réseaux** utilisent des adresses uniques de 32 bits qui sont **créées en empruntant des bits au champ d'hôte**. Les adresses de **sous-réseau** sont **visibles** par les autres équipements du **même réseau**, mais **pas par les réseaux externes**. Les sous-réseaux ne sont **pas visibles de l'extérieur**, car les réseaux externes ne peuvent faire référence qu'à l'adresse réseau complète d'un sous-réseau. Les **sous-réseaux** permettent d'**utiliser plus efficacement les adresses réseau**.

La **détermination du chemin** consiste à **sélectionner le meilleur chemin** que le trafic doit emprunter dans le nuage de réseaux. Ce sont les **routeurs** qui **évaluent le meilleur chemin** connu pour le trafic. La détermination du chemin

s'effectue **au niveau** de la couche 3, la **couche réseau**. Les **services de routage utilisent** les **informations de topologie du réseau** lors de **l'évaluation** des **chemins**. Ces **informations** peuvent être **configurées** par **l'administrateur** réseau **ou** collectées **par** des **processus dynamiques** s'exécutant sur le réseau.

La **couche réseau** se connecte aux réseaux et **fournit des services** d'acheminement au mieux (best-effort) de **bout en bout** des paquets à son utilisateur, **la couche transport**. La couche réseau **envoie les paquets** du réseau source au réseau de destination **en se basant sur la table de routage IP**. Une fois que le **routeur** a déterminé le chemin à utiliser, il peut **commuter le paquet**. La commutation **consiste à prendre le paquet** accepté sur une **interface du routeur et à le transmettre à une autre interface** ou à un port représentant le meilleur chemin vers la destination du paquet.

Pour que la **communication d'acheminement** soit utile, un réseau doit représenter de façon cohérente les chemins disponibles entre les routeurs. Il faut donc procéder avec **l'adresse réseau** (adressage IP).

L'adresse réseau contient **une partie chemin et une partie hôte**. La **partie chemin identifie** une portion du **chemin utilisée par le routeur** au sein du nuage de réseaux et la **partie hôte identifie** un **équipement spécifique du réseau**. Le **routeur** se sert de l'adresse réseau pour **identifier** le **réseau source ou de destination** d'un paquet.

La **cohérence des adresses** de couche 3 sur l'ensemble du réseau **améliore** l'utilisation de la **bande passante** en évitant la diffusion des broadcasts inutiles. Les broadcasts créent un trafic inutile et gaspillent la capacité des équipements ou des liaisons qui n'ont pas besoin de les recevoir.

L'une des **fonctions** du **routeur** consiste à **déterminer le chemin** à utiliser pour **transmettre une trame donnée**. La trame arrive sur une interface du routeur. **La trame de couche liaison** de données est **retirée et éliminée**. Quant à la trame de couche réseau (le **paquet**), elle est **envoyée** au processus de **couche réseau appropriée**. **L'en-tête** de protocole réseau est alors examiné afin de **déterminer la destination du paquet**. Le processus de couche réseau **consulte** ensuite la **table de routage**, qui **indique** l'interface connectée au **meilleur saut** vers la destination. Le **paquet** est ensuite retransmis à la couche liaison de données, où il est **encapsulé** dans une **nouvelle trame**. Ensuite, il est placé **en file d'attente** afin d'**être acheminé** par l'interface appropriée. Enfin, la trame est mise dans le réseau et voyage jusqu'au routeur du saut suivant, où le processus se répète.

Pour **déterminer l'adresse réseau**, le routeur **extraît** l'adresse **IP de destination** du paquet entrant et **recupère** le **masque de sous-réseau** interne. Le routeur effectue ensuite une opération **ET logique** pour **obtenir le numéro de réseau**. Pendant l'opération ET logique, la **portion hôte** de l'adresse IP de destination est **retirée**. Enfin, le **routeur recherche** le **numéro du réseau de destination**, **établit** une **correspondance** avec une **interface de sortie** et **achemine** la **trame** à l'adresse **IP de destination**.

Les messages **ICMP** sont transportés dans des datagrammes IP et sont utilisés pour **envoyer des messages d'erreur et de contrôle**. Le protocole ICMP (*Internet Control Message Protocol*) utilise les types de message contenus dans la liste ci-dessous, mais il en existe d'autres.

- Destination inaccessible
- Dépassement du délai
- Problème de paramètre
- Épuisement de la source
- Rediriger
- Écho
- Réponse à l'écho
- Horodater

- Réponse horodatée
- Demande d'informations
- Réponse à une demande d'informations
- Demande d'adresse
- Réponse à une demande d'adresse

Si un **routeur** est **incapable** de remettre un **paquet à destination**, il envoie un **message ICMP** « destination inaccessible » à l'unité **source** pour l'informer du problème. Le routeur **abandonne** le **paquet initial**. Une destination peut être inaccessible parce que l'hôte a indiqué une adresse inexistante ou, plus rarement, parce que le routeur ne connaît pas le chemin à la destination. **Si** un **routeur** ne peut **pas remettre** un message **ICMP** pour un motif quelconque, il **n'enverra pas** de message **ICMP** pour signaler l'**échec**, car cela pourrait saturer le réseau d'un flux sans fin de messages ICMP. C'est pourquoi un message ICMP qui n'a pu être remis est éliminé.

Pour **vérifier l'accessibilité** d'une unité dans un interréseau, un hôte TCP/IP peut envoyer une **requête d'écho ICMP**, qui est **générée par** la commande « **Ping** ».

Pour **communiquer sur un réseau** Ethernet, la station **source doit connaître** les adresses **MAC** et **IP** de la station de **destination**. Une fois que la **source a déterminé** l'adresse **IP** de **destination**, son **protocole IP consulte** sa table **ARP** (Address Resolution Protocol) pour **rechercher** l'adresse **MAC** de **destination**. Si le protocole IP trouve dans sa table une **correspondance de l'adresse IP de destination à l'adresse MAC de destination**, il **relie** ces deux **adresses** et les utilise pour encapsuler les données.

Si l'adresse **MAC** est **inconnue**, la source doit envoyer une **requête ARP**. Si **l'adresse ne figure pas** dans la table du routeur, le protocole **ARP envoie** un message de **broadcast** pour rechercher la station de destination.

Le routage et les catégories de protocoles de routage.

La **couche réseau** doit être en mesure d'**interopérer avec** les diverses **couches inférieures**. Les **routeurs** doivent être capables de **traiter** en toute transparence les **paquets encapsulés** dans les **différentes trames** de niveau inférieur sans modifier l'adressage de couche 3 des paquets.

En règle générale, les **routeurs transmettent** un **paquet** d'une **liaison de données à une autre**. Pour transmettre un paquet, le routeur effectue **deux opérations de base** : la **sélection du chemin** et une **commutation**. La fonction de **commutation permet** au routeur d'**accepter** un **paquet** sur une interface **et** de **acheminer** sur une autre. La fonction de **détermination du chemin permet** au routeur de **sélectionner** l'**interface** appropriée **pour acheminer** un paquet.

Les deux fonctions de base d'un routeur.

En règle générale, les routeurs transmettent un paquet d'une liaison de données à une autre. Pour transmettre un paquet, le routeur effectue deux opérations de base : la **sélection du chemin** et une **commutation**.

La fonction de **commutation** permet au routeur d'accepter un paquet sur une interface et de l'acheminer sur une autre.

La fonction de **détermination du chemin** permet au routeur de sélectionner l'interface appropriée pour acheminer un paquet.

Le processus de transmission de données de la **couche réseau examine l'en-tête** de la trame pour déterminer le réseau de destination, puis **consulte la table de routage** qui associe les réseaux aux interfaces sortantes. La trame d'origine est éliminée et ignorée. Le paquet est de nouveau encapsulé dans la trame de liaison de données de l'interface sélectionnée, puis il est placé en file d'attente pour être transmis au saut suivant du chemin.

Les routes statiques et dynamiques.

Le routage **statique** est **géré manuellement**. C'est l'administrateur réseau qui définit la route dans la configuration du routeur. Les routes statiques réduisent la charge du système, car **aucune mise à jour** de routage n'est envoyée.

Une fois que l'administrateur réseau a entré les commandes de configuration pour lancer le **routage dynamique**, les informations de route sont **mises à jour automatiquement**.

Le routage **statique** permet à l'administrateur, pour des raisons de sécurité, de **masquer des parties du réseau**. De plus, lorsque le réseau n'est **accessible que par un seul chemin**, une route statique vers le réseau peut suffire. Ce type de partition est appelé **réseau d'extrémité**.

Le routage **dynamique** tend à révéler toutes les **informations** connues **relatives à un réseau**.

La route par défaut.

Une route par **défaut** consiste en une entrée de table de routage permettant de diriger les paquets pour lesquels le **prochain saut** n'est **pas explicitement indiqué** dans la table de routage.

Les protocoles routés et de routage.

Les protocoles **routés** définissent le format et l'utilisation des champs dans un paquet. Les paquets sont généralement transmis d'un système d'extrémité à un autre. Le **protocole IP** est un exemple de protocole routé.

Un protocole de **routage** permet aux routeurs de communiquer avec d'autres routeurs pour **tenir à jour les tables de routage**. Les protocoles **RIP** (*Routing Information Protocol*), **IGRP** (*Interior Gateway Routing Protocol*), **EIGRP** (*Enhanced Interior Gateway Routing Protocol*) et **OSPF** (*Open Shortest Path First*) sont des exemples de protocoles de routage TCP/IP.

Les protocoles de routage IP.

La plupart des protocoles de routage entrent dans l'une des **deux catégories de base** : à **vecteur de distance** ou à **état de liens**. Le protocole de routage à **vecteur de distance détermine la direction** (le vecteur) **et la distance** d'une liaison du réseau. Le protocole de routage à **état de liens** (aussi appelé protocole du plus court chemin d'abord) **recrée la topologie** exacte de tout le **réseau** (ou au moins de la partie où se trouve le routeur).

Un troisième type de protocole, le protocole **hybride symétrique**, **combine** des aspects des protocoles à **vecteur** de distance **et** des protocoles à **état de liens**.

La convergence réseau.

Chaque fois que la topologie change en raison de la **croissance du réseau**, d'une **reconfiguration** ou d'une **panne**, la **base de connaissances** du réseau doit également être **modifiée**. Les connaissances doivent refléter une **vue juste et cohérente** de la nouvelle topologie. Cette vue est **appelée convergence**.

Le routage à vecteur de distance.

Les protocoles de routage à **vecteur de distance transmettent** régulièrement des **copies** d'une table de routage **d'un routeur à l'autre**. Chaque routeur reçoit une **table** de routage de son **voisin immédiat**.

Le même **processus** est **répété** étape par étape **dans toutes les directions entre les routeurs** immédiatement **voisins**. Ainsi, le protocole cumule les distances réseau afin de **tenir à jour la base de données** contenant les informations sur la topologie **du réseau**. Les protocoles à vecteur de distance **ne permettent pas** à un routeur de **connaître la topologie exacte** d'un réseau. Les protocoles **RIP** et **IRGP** sont utilisés.

Le routage à état de liens.

Il **gère** une **base de données complexe** d'informations **topologiques** et a une **connaissance complète** des routeurs distants et de leurs interconnexions, donc **du réseau**.

Le routage à état de liens utilise les mises à jour du routage à état de liens dans le routage **OSPF**.

Comparaison des protocoles de routage à vecteur de distance et à état de liens.

Vecteur à distance :

- Voit la topologie du réseau dans la perspective du voisin.
- Additionne les vecteurs de distance d'un routeur à l'autre.
- Mises à jour périodiques fréquentes : convergence lente.
- Passe des copies de la table de routage aux routeurs voisins.

État de liens :

- Vue commune de l'ensemble de la topologie du réseau.
- Calcule le plus court chemin vers les autres routeurs.
- Mises à jour déclenchées par événements : convergence plus rapide.
- Passe les mises à jour du routage à état de liens aux autres routeurs.

Activation d'un processus de routage IP.

La sélection du protocole routé IP implique la **sélection** d'un protocole de routage tel que le protocole **RIP ou IGRP**, ainsi que l'**attribution** de numéros de **réseau IP sans préciser** de valeurs de **sous-réseau**.

Configuration du routage dynamique

Pendant le routage dynamique, les routeurs s'envoient des **messages périodiques de mise à jour** du routage. Chaque fois qu'un routeur reçoit un message contenant de nouvelles informations, il **recalcule le meilleur chemin** et **envoie** la nouvelle **mise à jour aux autres routeurs**.

Configuration du protocole RIP.

Les principales **caractéristiques** du protocole **RIP** sont les suivantes :

- Il utilise le nombre de sauts comme métrique pour la sélection du chemin.
- Le nombre de sauts maximum autorisé est de 15.
- Par défaut, les mises à jour du routage sont diffusées toutes les 30 secondes.

La couche de transport du modèle OSI.

Un transport fiable.

Lorsque la couche transport (**TCP**) envoie ses segments de données, elle vérifie **l'intégrité des données**. Pour ce faire, elle recourt à un **procédé** appelé **contrôle de flux**. Le contrôle de flux permet d'**éviter** le problème du **dépassement de capacité des mémoires tampons de l'hôte de destination**. Les dépassements de capacité peuvent constituer de graves problèmes car ils **entraînent des pertes de données**.

Les services de la couche transport permettent également aux utilisateurs de demander un transport de données fiable entre les hôtes et les destinations. Pour assurer la **fiabilité** du transport, une **relation orientée connexion** est utilisée entre les systèmes d'extrémité en cours de communication. Un transport fiable exécute les opérations suivantes :

- il segmente les applications de couche supérieure,
- il établit une connexion,
- il transfère les données,
- il utilise le fenêtrage,
- il utilise les techniques d'accusé de réception.

Les protocoles routés et de routage. Les protocoles de routage IP. La convergence réseau.

La fonctionnalité de transport est assurée segment par segment. Autrement dit, **plusieurs applications** peuvent **envoyer** des **segments** de données suivant la **méthode du premier arrivé, premier servi**. Ces segments peuvent être adressés à la même destination ou à des destinations différentes.

L'échange en trois étapes.

Étape 1 : établissement de la connexion.

- Un **chemin** est **déterminé** entre les unités d'origine et de destination pour assurer un débit de services constant.

Étape 2 : Transfert de données.

- Les **données** sont **transmises** de manière **séquentielle** par le chemin établi et arrivent à destination dans l'ordre où elles ont été envoyées.

Étape 3 : fermeture de la connexion.

- Consiste à mettre **fin** à la **connexion** entre la source et la destination lorsqu'elle n'est plus nécessaire.

Utilisation d'une mémoire tampon dans la transmission de données.

Pendant le transfert des données, deux raisons peuvent entraîner une congestion.

Premièrement, le **trafic généré** par un ordinateur peut être **plus rapide que** la capacité de **transfert** du réseau.

Deuxièmement, si plusieurs ordinateurs doivent envoyer **simultanément** des **datagrammes** à une **même destination**, celle-ci peut devenir encombrée, même si le problème ne provient pas d'une source.

Lorsque des **datagrammes** arrivent trop rapidement et que l'ordinateur ou la passerelle ne peut les traiter, ils sont **stockés temporairement en mémoire**. **Si le trafic continue**, l'hôte ou la passerelle **sature** éventuellement sa **mémoire** et doit **abandonner** les **datagrammes** qui arrivent. Dans ce cas, un indicateur agit comme un **signal d'arrêt** et prévient l'émetteur de **cesser d'envoyer des données**. Lorsque le **récepteur peut accepter** d'autres **données**, il envoie un **indicateur** de transport " **prêt** " qui agit comme un feu vert. Lorsque l'émetteur reçoit cet indicateur, il **reprend la transmission** des segments.

Fenêtrage.

Le **fenêtrage** est un mécanisme de **contrôle de flux** selon lequel la source doit recevoir un **accusé de réception** de la destination après avoir transmis une certaine quantité de données.

Par exemple, si la taille de la **fenêtre est de 3**, la **source** peut **envoyer 3 octets** à la destination. Elle doit ensuite **attendre un accusé de réception**. **Si la destination reçoit les 3 octets**, elle doit envoyer un **accusé de réception à la source**, qui peut alors envoyer 3 autres octets. **Si** pour une raison quelconque, la destination **ne reçoit pas les 3 octets** (à cause du dépassement de la taille de la mémoire tampon, par exemple), elle n'envoie **pas d'accusé de réception**. Comme la **source** ne reçoit pas d'accusé de réception, elle sait qu'elle **retransmettre** les données à un **débit plus lent**.

La fiabilité par accusé de réception.

La technique **PAR** (**P**ositive **A**cknowledgement and **R**etransmission) **garantit la fiabilité**. Selon cette technique, la **source envoie un paquet**, **démarré un compteur** et **attend un accusé de réception** avant d'envoyer un nouveau paquet. Si le **compteur** arrive à **expiration avant** que la source n'est reçu un **accusé de réception**, elle **retransmet** le **paquet** et **redémarre le compteur**.

Résumé.

Voici un **résumé du résumé** qui retrace les **grandes lignes des sujets traités dans les pages précédentes** :

- Grâce aux couches, le modèle de référence OSI simplifie la communication entre deux ordinateurs.
 - Le protocole de chaque couche échange des informations, appelées unités de données de protocole, entre les couches homologues.
 - Chaque couche dépend de la fonction de service de la couche du modèle de référence OSI immédiatement inférieure. La couche inférieure utilise l'encapsulation pour placer l'unité de données de protocole de la couche supérieure dans son champ de données, puis elle ajoute les informations d'en-tête et de fin dont elle a besoin pour remplir sa fonction.
 - Le terme *Ethernet* est souvent utilisé pour désigner des réseaux locaux à détection de porteuse avec accès multiple (CSMA/CD), qui sont généralement conformes aux spécifications Ethernet, y compris à la norme IEEE 802.3.
 - Les liaisons de données Ethernet et 802.3 assurent le transport des données par la liaison physique qui relie deux équipements.
 - Le protocole IP assure l'acheminement au mieux des datagrammes, non orienté connexion. Il ne se préoccupe pas du contenu des datagrammes, mais il recherche une façon de les acheminer à destination.
 - Les messages ICMP sont transportés dans des datagrammes IP et permettent d'envoyer des messages d'erreur et de contrôle.
 - Le protocole ARP sert à mettre en correspondance une adresse IP connue et une adresse de sous-couche MAC pour permettre la communication sur un média à accès multiples tel qu'Ethernet.
 - La fonction de commutation permet au routeur d'accepter un paquet sur une interface et de l'acheminer sur une autre.
 - Les protocoles routés sont des protocoles réseau qui fournissent suffisamment d'informations dans l'adresse de couche réseau pour permettre l'acheminement d'un paquet d'un hôte à un autre en fonction de la méthode d'adressage.
 - Les protocoles de routage prennent en charge les protocoles routés en fournissant des mécanismes de partage des informations de routage. Les routeurs échangent des messages de protocole de routage.
 - La plupart des protocoles de routage entrent dans l'une des deux catégories de base : à vecteur de distance ou à état de liens.
 - Les routeurs doivent être capables de traiter en toute transparence les paquets encapsulés dans différentes trames de niveau inférieur sans modifier l'adressage de couche 3 des paquets.
 - RIP, IGRP, OSPF et EIGRP sont des exemples de protocoles de routage.
 - Les services de la couche transport permettent aux utilisateurs de demander un transport de données fiable entre les hôtes et les destinations.
-