

Routeurs et routage

L'interconnexion de réseaux consiste à les relier physiquement et à proposer un moyen d'acheminer l'information en la rapprochant progressivement de sa destination.

C'est le rôle des routeurs et de la technique de routage.

L'objectif de la constitution du protocole TCP/IP est, dès le départ, de permettre de faire circuler des informations découpées en paquets (datagrammes) en empruntant un chemin parmi plusieurs. La technique adoptée est celle du routage déjà utilisée dans l'acheminement du courrier postal par exemple.

Contrairement à la commutation utilisée au cœur des réseaux de téléphonie et qui repose sur l'établissement d'un chemin unique pour l'ensemble d'une communication, le routage calcule la voie à emprunter à chaque paquet. On peut alors gérer dynamiquement la congestion en redirigeant des paquets vers des routes moins sollicitées. Fonctions des routeurs

Le système repose sur des tables de routage et le principe d'une passerelle (un autre routeur) connue pour chaque direction. Cette passerelle permet de se rapprocher de la destination attendue.

Pour renseigner ces tables, on pourra procéder manuellement, mais des protocoles de communication inter-routeur permettent d'automatiser la mise à jour.

Les routeurs assurent aussi une autre fonction qui consiste à être un point de passage sécurisé entre le réseau interne et l'extérieur grâce à la translation d'adresses (et de port).

I Routage

La fonction de routage repose sur une connaissance de voisinage et un système de référents mieux avertis.

Le routage est la fonction fondamentale du niveau 3. Sans elle, toute communication entre deux postes situés sur des réseaux distants nécessiterait de connaître tous les éléments à traverser.

Le routage repose donc sur une organisation logique des adresses déjà évoquée, et sur un travail de redirection réalisé par des **passerelles** ou **gateways**.

Une machine ne connaissant pas une direction donnée aura donc un ou plusieurs **redirecteurs** de référence susceptibles de connaître plus de chose et donc d'acheminer le message.

1.1 Poste et Passerelle

Lors de la configuration d'un poste, on doit préciser :





- son adresse IP,
- le masque qu'on lui applique
- dans le cas d'un accès à un réseau externe, l'adresse IP du routeur jouant le rôle de passerelle

par défaut.

Le principe de la communication depuis un poste est donc le suivant :



1.2 Table de routage et passerelle

Une table de routage est constituée de quatre ensembles sur 5 colonnes (voir illustrations ci-dessous).  

Sur un routeur, la table présente :

- les routes vers les réseaux directement connectés (ceux sur lesquels le routeur possède une adresse)
- des routes connues qui ne sont pas directement connectées et ne sont pas sur la « route par défaut
- une route par défaut (0.0.0.0/0) vers laquelle renvoyer tous les paquets ne correspondant pas à des routes connues



Contrôle /Lecture

Quelques règles de base permettent de lire une table, d'en vérifier la validité, de construire les routes adaptées.

- La passerelle et l'interface sont toujours sur le même réseau
- La colonne interface ne comporte que les adresses IP présentes sur la machine dont on étudie la table, plus 127.0.0.1.
- Dans la colonne Adresse réseau, on ne trouve que des adresses de réseau (0 sur les bits de l'hôte), des adresses de diffusion (broadcast [1 sur les bits de l'hôte] et multicast [224.0.0.0]) et éventuellement les adresses IP de l'équipement.
- Un masque à 255.255.255.255 indique une adresse exacte dans la colonne adresse réseau.
- Les lignes 0.0.0.0/0 indiquent des routes par défaut

Exploitation de la table

La table est lue par le routeur, du plus précis (généralement un broadcast) au plus général (0.0.0.0).

Le routeur compare successivement les routes possibles avec l'adresse de destination de la trame qu'il a reçue.

Lorsqu'il trouve une correspondance (éventuellement par la route par défaut), il redirige le datagramme.

Les colonnes passerelle et interface vont servir à préciser vers qui la trame devra s'adresser au niveau 2 : une passerelle (prochain routeur) ou le poste destinataire (interface=passerelle).

Algorithme de routage des datagrammes pour un routeur

le principe de l'algorithme de routage est de déterminer l'adresse MAC de la prochaine machine à contacter (un routeur ou un poste)

- **A travers un seul réseau** : IP s'arrange pour déterminer l'adresse physique (Carte Ethernet ou Token Ring) correspondant à l'adresse IP du destinataire (grâce à ARP). Il passe alors cette valeur à la couche Liaison qui encapsule le tout dans une trame Ethernet (ou un autre protocole de niveau 2 en Wifi, pour les réseaux Apple, etc). Le routage est terminé, le récepteur recevant une information qui lui est destinée.
- **A travers plusieurs réseaux** : lorsque le routeur étudie l'adresse IP du destinataire, son premier travail est de comparer les valeurs de l'adresse IP du destinataire et des réseaux destination connus dans la table. Dans le cas où le réseau destinataire n'est pas directement relié au matériel, il est nécessaire de passer par une machine spécifique, citée dans la colonne passerelle IP, qui est chargée de rediriger les datagrammes vers d'autres réseaux.

Cet algorithme repose sur des tables renseignées de manière suffisamment complètes pour permettre d'atteindre toute destination possible depuis un point déterminé.

Un poste connaît son routeur, qui renvoie vers le fournisseur d'accès, qui redirige ensuite vers le cœur de son réseau ou des partenaires, etc.

[Algorithme de routage](#)



II Protocoles de routage

Les protocoles de routage permettent aux routeurs de s'échanger leurs informations sans intervention humaine et de garder une information à jour.

Les routeurs doivent être reconfigurés régulièrement pour prendre en compte la défektivité d'un lien, l'ajout d'un routeur dans le maillage, la modification du débit d'une liaison, etc.

Si le nombre de matériels est peu conséquent, que les évolutions sont rares et l'ensemble fiable, le paramétrage peut se faire manuellement. Le routage est alors dit statique.

Mais lorsque l'infrastructure se complexifie, qu'elle devient mouvante ou que les besoins de qualité se font ressentir, les routeurs peuvent assurer une automatisation des mises à jour grâce à un routage dynamique réalisé par des algorithmes d'échange de tables entre routeurs organisés en domaines.

2.1 Métrique et distance administrative

Les protocoles de routage ont pour vocation de rendre automatique le paramétrage des tables de routage en s'appuyant sur la colonne métrique qui précisera le coût d'usage d'une route parmi plusieurs.

Métrique

Pour choisir la meilleure route, les routeurs vont s'appuyer sur la notion de métrique. Cette information est valorisée selon des critères propres à chaque algorithme (ou protocole).

Notamment, elle peut prendre en compte le nombre d'intermédiaires (sauts ou hop) entre le routeur et le réseau distant, comme c'est le cas dans le protocole RIP, ou la bande passante pour atteindre le lien distant comme c'est le cas du protocole OSPF.

On peut aussi valoriser la métrique par des notions de coût financier (par exemple entre une liaison forfaitaire DSL et un lien de secours RNIS).

Distance administrative

Les routeurs peuvent implémenter des protocoles de routage différents, parmi lesquels il faudra effectuer un choix selon la fiabilité de l'algorithme, sa rapidité de traitement, le temps de convergence (temps mis par l'ensemble du domaine administré pour prendre en compte une évolution), etc.

Un indice est associé à chaque route enregistrée dans la table. Cet indice est nommé **distance administrative**.

Lorsqu'il reçoit une table d'un routeur distant, le routeur récepteur se reconfigurera si la route proposée est sur un protocole plus efficace que celui actuellement utilisé.

Pour les routeurs Cisco on trouve par exemple :

Protocole de routage (route source)	Distance administrative
Connected interface	0
Static route	1
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route	5
External Border Gateway Protocol (BGP)	20
Internal EIGRP	90
IGRP	100
OSPF	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140
On Demand Routing (ODR)	160
External EIGRP	170
Internal BGP	200
Unknown	255

On observera que les algorithmes concernent deux grands types de composants :

- ceux situés à la périphérie d'un domaine (éléments d'interconnexion entre opérateurs, par exemple) ou BGP (Border Gateway Protocol)
- ceux situés au sein même de ces domaines, les IGP (Interior Gateway Protocol). RIP et OSPF

sont des IGP. Leurs informations n'ont d'intérêt qu'à l'intérieur d'une structure, et ne vaut pas pour d'autres *domaines réseau* (autre opérateur ou entreprise).

Algorithme de mise à jour

Qu'il s'agisse de la métrique ou de la distance administrative, les routeurs retiendront toujours les valeurs les plus petites (les moins coûteuses) de manière intelligente.

Principe pour 1 ligne de routage sur un protocole de routage unique.

Un routeur reçoit d'un autre matériel une table de routage. Il en extrait une ligne et ajoute à la métrique fournie par l'autre équipement le coût (selon le protocole de routage retenu) pour atteindre cet autre équipement → nouvelle métrique.



2.2 Protocoles de routage RIP et OSPF

Les protocoles définissent la manière dont la métrique est mise à jour, ainsi que les techniques d'échange, la détection de boucle, etc. Bien que globalement peu efficace à l'interconnexion des réseaux, ces protocoles sont pertinents sur une structure où on a la maîtrise des routeurs.

Nous verrons les deux protocoles de référence dans un réseau local : RIP (Routing Internet Protocol) et OSPF (Open Shortest Path First), qui vous sont décrits de manière plus détaillée sur le site CISCO www.labo-cisco.com.

RIP (Routing Internet Protocol)

Défini dans les RFC 1058, 1388, et 1723 (RIPv2).

C'est le protocole de routage interne historiquement le plus utilisé car très simple.

La valeur TTL de l'entête IP est positionnée à une valeur prédéterminée au moment de l'émission. Chaque intermédiaire RIP (chaque routeur traversé) diminue le TTL de 1, évitant les boucles infinies ou la propagation de messages perdus. Métrique et Mise à jour des tables

RIP fonctionne sur une métrique calculée en nombre de sauts (hop), c'est à dire le nombre de routeurs séparant un équipement réseau destinataire. Cette valeur est limitée au chiffre 15 pour éviter les routes trop longues ou les boucles.

Le travail de mise à jour s'effectue par un échange régulier entre les routeurs, indépendant du travail d'acheminement.

Toutes les 30s (compteur *routing-update*), les tables sont mises à jour par *broadcast* en *UDP*. Si un routeur ne communique pas, une deuxième mise en attente de 180s est démarrée. Si le routeur défectueux n'a toujours pas communiqué au bout de ce temps, les routes qui l'utilisent en tant que passerelle sont bloquées et un nouveau chrono démarre pour 240s. En cas de panne persistante, les routes correspondantes sont détruites.

Si une mise à jour parvient, le routeur qui reçoit ajoute 1 à toutes les métriques (il est à 1 routeur de

distance supplémentaire que son prédécesseur). Si une métrique atteint la valeur 16, la route est considérée comme non joignable et n'est pas enregistrée.

Bilan

Ce protocole est très simple dans sa conception, dans son paramétrage. Toutefois, l'information de métrique produite (nombre de sauts) n'est pas toujours pertinente sur l'efficacité d'une route.

Le nombre de matériel n'indique pas nécessairement le chemin le plus rapide (ne prend pas en compte la congestion, le débit, etc).

Par ailleurs, les échanges entre routeurs paramétrés selon ce protocole utilisent beaucoup de bande passante pour leurs échanges.

OSPF (Open Shortest Path First)

Défini dans les RFC 1131, mis à jour par les RFC 1245 à 1247. OSPFv2 dans la RFC 2178 et 2328.

Métrique et coût Ce protocole est destiné à remplacer RIP car il diminue le temps de convergence, et fonctionne sur des temps de réponse (donc sur les débits) pour la valorisation de la métrique.

À la création du protocole (années 80), des valeurs standard ont été attribuées aux principales connexions :

- FDDI (100 Mbps) : coût 1
- Gigabit / 100BaseT : coût 1
- Token Ring : coût 6
- Ethernet 10baseT : coût 10
- T1 : coût 128
- Ligne série 56 Kbps : coût 1785

Ces valeurs sont aujourd'hui obsolètes, elles peuvent alors être paramétrées différemment par le responsable de l'infrastructure réseau.

Pour calculer le coût d'un chemin, on ajoutera l'ensemble des métriques. Le plus court sera retenu dans le cas de multiples parcours possibles.

Organisation

Pour éviter une gestion trop vaste, des interconnexions trop lourdes, OSPF organise un système de routage en zones (area) indépendantes interconnectées par un backbone. Ainsi, le schéma ci-dessous issu du site labo-cisco (lien obsolète) montre trois zones reliées.



Les éléments présents dans la zone 1 n'ont aucune vision du reste, seul le routeur en contact avec le backbone permet l'interconnexion.

Les routeurs OSPF se signalent par la production régulière de messages hello indiquant leur état, leurs voisins (par le biais d'extraits de la table de routage) et leur priorité dans la zone.

Pour éviter les communications trop nombreuses, un système a un rôle de référence (DR - Designated

Router). Il centralise l'état des tables de routage des différents matériels et redistribue le schéma (technique d'inondation) lorsque nécessaire.

Le calcul des routes est effectué par un principe d'échange entre les routeurs (envoi de l'état et mise à jour des tables aux voisins).

Bilan

Le protocole OSPF améliore RIP en diminuant le trafic réseau, en produisant une information plus pertinente sur l'état réel du réseau et l'efficacité des liaisons.

Toutefois, il demande des ressources de calcul plus importantes sur les routeurs, ce qui a retardé son déploiement.

2.3 Conclusion sur le routage

Le routage est la fonction permettant l'acheminement de paquets à travers une infrastructure non connecté (on parle du mode datagramme).

Il repose sur des algorithmes de traitement des paquets permettant de définir la route à suivre, et sur des algorithmes de mise à jour des tables de routage entre matériels d'un domaine.

La multiplication des réseaux ayant alourdi les tables, la notation CIDR a permis de limiter leur saturation en rassemblant de multiples lignes contiguës en une version compacte (voir sur-réseaux dans la fiche sur l'adressage). En complément du routage, la plupart des matériels d'interconnexion de niveau 3 joue un rôle d'intermédiaire et de porte d'entrée/sortie unique pour les réseaux locaux.

Les fonctions de translations sont aujourd'hui indissociables de ces composants.

IV ROUTAGE, NAT et PAT

1 NAT

Fonction quasi naturelle des routeurs, la translation d'adresse (Network Address Translation - NAT) consiste à remplacer les adresses IP du réseau interne par la ou les adresses IP visibles sur le réseau externe.

Transparent pour l'émetteur, ce travail en sortie a un intérêt évident pour les réseaux utilisant des adresses privées. On parle alors de **NAT dynamique** ou **IP Masquerading**.

NAT statique

Toutefois, la translation d'adresse peut aussi être utilisée pour assurer une forme de sécurité en masquant l'adresse d'une machine de l'extérieur (par exemple un serveur interne accessible depuis l'extérieur, remplacé par l'adresse du routeur).

On parle alors de NAT statique, le paramétrage étant fourni par l'administrateur.

2 PAT

Ce même travail de sécurisation peut être réalisé au niveau des ports TCP/UDP.

On demandera aux machines externes de s'adresser au port standard (par exemple, 80 pour HTTP), le routeur réalisant une translation de port (Port Address Translation – PAT) vers une valeur interne particulière (par exemple 8080). On ne pourra pas alors attaquer le port du serveur, seul le routeur se verra bloqué.

Cette fonction est toujours faite en statique. Le couplage des deux parades peut aussi être noté NPAT.

From:

<https://wiki.sio.bts/> - **WIKI SIO : DEPUIS 2017**

Permanent link:

<https://wiki.sio.bts/doku.php?id=routage>

Last update: **2020/07/26 16:27**

