LE ROUTAGE DANS LE RÉSEAU

TASSONE Laura

DEFRANCE Baptiste

Table des matières

Quesque le réseau

Le réseaux internet c'est l'échange de données via différents protocoles entre différentes machines. Le but du réseau est de permettre le partage de fichiers et d'application, la communication entre différents postes etc… Un réseau est structuré de manière simple, permettant la communication entre un client et un serveur. Pour faire simple, le serveur est une machine qui fournira les informations à une machine client. A l'inverse, le client est une machine qui va demander des informations à une machine serveur. Par exemple, quand vous vous connecter sur votre messagerie mail, votre ordinateur demande des informations à un autre ordinateur qui contient un serveur de messagerie mail. Votre ordinateur est donc considéré comme machine client et l'ordinateur ayant la messagerie mail comme machine serveur.

Le routage statique

Dans un réseau, les routeurs doivent communiquer normalement et s'échanger des informations telles que le contenu de la table de routage, que nous avons déjà évoquée. Le processus d'échange d'informations entre routeurs dépend du genre de routage utilisé. Dans un routage statique, c'est vous, l'administrateur réseau, qui devez construire et mettre à jour manuellement vos tables de routage. Donc, dans un routage statique, le contenu des tables de routage est également statique. Ce genre de routage n'est pas vraiment pratique pour des raisons évidentes. * Les routeurs ne découvriront pas automatiquement les network ID des autres réseaux, ce sera à vous de les leur indiquer par une configuration manuelle. Les routeurs ne pourront pas communiquer entre eux pour s'échanger des informations, ce sera à vous de modifier les changements des données de votre réseau dans chaque routeur, manuellement. Les routeurs ne seront pas intelligents et pourront garder des données erronées dans leur table. Étant donné qu'ils ne communiquent pas entre eux, si un chemin vers un réseau n'est plus praticable, ils continueront à le considérer valable tant que vous ne l'aurez pas changé. En bref, le routage statique est défini manuellement par l'administrateur.

Le routage dynamique

Le routage dynamique est exactement le contraire du routage statique. Tout se fait automatiquement grâce à un protocole de routage. Nous allons voir ici ce qu'est le routage dynamique pour pouvoir comprendre la suite de notre présentation. Il est possible d'avoir un réseau composé de plusieurs dizaines de routeurs. Ces derniers doivent constamment communiquer en s'échangeant des informations sur les routes. En réseau, ce sont des protocoles qui permettent la communication entre les hôtes. Le rôle d'un protocole de routage consiste donc à définir les règles et principes de communication entre routeurs, pour ce qui concerne le seul routage. En résumé, un protocole de routage, c'est l'intelligence

qui régit la manière dont les routeurs communiquent entre eux pour nous offrir le meilleur service de routage possible, c'est-à-dire le moins coûteux, le plus rapide, le plus pratique. Différents protocoles de routage Il existe de nombreux protocoles de routage. Un routeur peut en supporter plusieurs en même temps. Pourquoi en avoir plusieurs, s'ils servent tous à faire la même chose ? La réponse se trouve dans la méthodologie. Ces protocoles font certes la même chose, mais certains sont plus pratiques, d'autres ont des contraintes plus coûteuses par exemple. Citons les protocoles les plus célèbres : RIPv1 et RIPv2, OSPF, EIGRP, IGRP, BGP, IS-IS. Ces protocoles peuvent se classer dans deux « familles » : IGP (Interior Gateway Protocol, protocole de routage interne) C'est la famille des protocoles qui peuvent échanger des informations de routage avec des systèmes autonomes (AS, Autonomous Systems). Il s'agit, pour faire simple, d'un ensemble de réseaux IP contrôlés par une organisation ou une entreprise. EGP (Exterior Gateway Protocol, protocole de routage externe) C'est la famille des protocoles qui déterminent la disponibilité d'un réseau entre deux systèmes autonomes et permettent le routage entre eux. Les fournisseurs d'accès à Internet, par exemple, utilisent un protocole de cette famille pour effectuer un routage externe. C'est la famille du principal protocole de routage utilisé par Internet, BGP (Border Gateway Protocol). Nous avons schématisé un réseau constitué de deux systèmes autonomes (Myrtille et Citron).

RIP

On parle ici de protocole d'information de routage (Routing Information Protocol). Il sert à réaliser du routage dynamique, c'est-à-dire sans intervention humaine. Les routeurs peuvent s'échanger dynamiquement les informations de routage au moyen de ce protocole. Il est défini par la RFC 1 058 et utilise un algorithme de routage dit à vecteur de distance (distance vector). Retenez ce nom, nous étudierons cette notion par la suite. RIP est classé dans la famille des protocoles de routage interne (IGP), que nous avons évoquée dans le précédent chapitre. Les protocoles de routage à vecteur de distance, comme RIP, sont basés sur l'algorithme de Bellman-Ford. Il existe deux versions de ce protocole. Commençons par étudier la différence entre ces versions avant de plonger dans la technique.

Première version La toute première version de ce protocole ne pouvait fonctionner que dans un réseau utilisant l'adressage par classes. Cela veut donc dire que, dans un réseau utilisant RIPv1 pour le routage, on ne peut pas utiliser des techniques telles que l'implémentation des masques de sous-réseaux à longueur variable (VLSM) ou l'agrégation des routes (supernetting). Une autre faiblesse de cette version est qu'elle ne peut supporter qu'un maximum de 15 sauts. Au-delà, RIP ne pourra pas assurer son devoir de routage. Ce n'est pas tout : RIPv1 ne supporte pas l'authentification. Ainsi, il accepte et intègre tous les messages qu'il reçoit de tout le monde sans sourciller. Cela fait donc de RIPv1 un protocole très vulnérable. Pour terminer sur les caractéristiques de cette version, les routeurs utilisant RIPv1 mettent à jour leurs tables de routage en les broadcastant (diffusant) sur tous les routeurs adjacents (ou voisins).

Ces présentations étant faites, explorons un peu ce protocole d'un point de vue technique. Nous avons déjà vu que l'unité de métrique du protocole IP était appelée « saut ». Voilà une caractéristique de RIP pour empêcher les boucles de routage, RIP limite à 15 le nombre de sauts par chemin de la source à la destination. Par ailleurs, RIP utilise le protocole UDP que nous avons étudié dans la couche transport et le port 520. Le principal rôle des protocoles de routage est l'échange d'informations sur les routes. Que se passe-t-il alors dans un réseau si une route ne fonctionne plus ? Les routeurs continueront à s'échanger des tables de routage. Cela veut donc dire que des informations fausses pourront être transmises à d'autres routeurs. Pour empêcher la diffusion de ces informations inexactes, RIP utilise trois mécanismes distinct, split horizon (séparation horizontale), route poisoning (empoisonnement de route) et finalement holddown (rétention).

RIPV2

Comme nous l'avons vu, la version 1 est limitée. Elle était pratique jusqu'à un certain moment, alors ses créateurs ont décidé de la faire évoluer, donnant naissance à RIPv2. Cette dernière supporte l'implémentation des masques de sous-réseaux, ce qui veut dire qu'elle peut efficacement router les paquets dans un réseau basé sur l'adressage CIDR. L'échange des tables de routage se fait par multicast. Les tables de routage sont transmises aux autres routeurs adjacents à l'adresse 224.0.0.9. L'autre grande avancée de RIPv2 est qu'on peut désormais sécuriser l'accès à un routeur en utilisant une authentification chiffrée.

OSPF

OSPF RIP, c'est bien pour de petits réseaux avec peu d'exigences, c'est facile à mettre en place et simple à configurer. OSPF, c'est tout l'inverse. On peut passer des heures sur le sujet tellement il est complexe. Dans ce chapitre, nous resterons en surface et nous vous orienterons vers d'autres ressources pour compléter. Pour commencer, OSPF est un protocole de routage dynamique de type IGP. C'est à peu près le seul point commun avec RIP. Il rentre dans la catégorie des protocoles à état de liens (link state protocoe) et utilise l'algorithme de Dijkstra. Gardons ces notions de côté pour le moment, on va rester sur l'aspect purement réseau de la bête.

Comme ce protocole est conçu pour de vastes réseaux, il introduit la notion de zone, aussi parfois appelée aire (area). Chaque zone porte un numéro. La principale porte toujours le numéro 0. Toutes les zones ne sont pas nécessairement reliées entre elles directement, mais une zone OSPF ne peut pas être isolée par des routeurs non OSPF, sinon elle n'est pas visible du reste du réseau. Et pour cause : les informations sont transmises de proche en proche, directement d'un routeur à l'autre.

OSPF a son vocabulaire propre et, franchement, ce n'est pas très grave si vous ne le retenez pas. L'important, c'est que vous compreniez comment ça marche ! vous pouvez voir des ABR (Area Border Router): ce sont des routeurs à cheval sur plusieurs aires. On aperçoit

également un ASBR (Autonomous System Boundary Router): il s'agit d'un routeur qui est en limite d'un réseau OSPF et qui assure les échanges avec un réseau utilisant un autre protocole de routage, comme RIP ou BGP. Pour découvrir son environnement, OSPF envoie des paquets Hello à ses voisins. Cela permet d'identifier sur quelles interfaces il va avoir à communiquer.

Une fois les voisins découverts, OSPF émet un Link-State Advertisement (LSA) en leur direction pour leur communiquer les informations de routage dont il dispose. Les voisins propagent l'information à leurs propres voisins avec un Link-State Update (LSU) et ainsi de suite. Chaque changement dans un routeur génère un LSA, chaque mise à jour dans une table de routage génère un LSU. Contrairement à RIP, aucune information de routage n'est transmise par OSPF s'il n'y a pas eu de changement. Tout au plus, il envoie des paquets Hello régulièrement. Cela signale aux voisins qu'il est toujours là, bien que discret. Quand un routeur ne donne plus de nouvelles après un certain temps (de 40 secondes à 2 minutes selon les configurations), il est considéré comme ne faisant plus partie du réseau par OSPF et ne reçoit plus les mises à jour. Pour attribuer un coût à une liaison, nous avons vu que RIP se base sur le nombre de sauts. OSPF, lui, se base sur la bande passante : plus elle est élevée, plus le coût est faible. Une technique utilisée par Cisco consiste à diviser une bande passante de référence par la bande passante réelle. Initialement, la référence était de 100 Mb/s. Vu les débits d'aujourd'hui, cette valeur n'a plus grand intérêt. On peut la configurer pour qu'elle soit, par exemple, de 10 Gb/s, ce qui serait plus pertinent. Ainsi, un lien de 10 Mb/s aura un coût de 1 000 (10 G / 10 M = 1 000), un lien de 200 Mb/s aura un coût de 50, etc. Il faut ensuite interpréter toutes ces valeurs reçues pour construire une table de routage.

EIGRP :

Protocole EIGRP Enhanced Interior Gateway Routing Protocol (EIGRP) est un protocole de routage propriétaire développé par Cisco en 1994. EIGRP est un protocole de routage à vecteur de distance IP, avec une optimisation permettant de minimiser l'instabilité de routage due aussi bien au changement de topologie qu'à l'utilisation de la bande passante et la puissance du processeur du routeur. En 2013, il s’est ouvert à la communauté Internet et est même décrit dans une RFC de l’IETF. Cependant, il reste sous le contrôle de CISCO, qui est le seul à pouvoir le modifier. Les autres constructeurs sont seulement autorisés à l’utiliser. EIGRP à plusieurs caractéristiques : -Il résout un des problèmes majeurs des protocoles de routage à vecteur de distance, celui des boucles (comme pour les switchs). S’il peut le faire, c’est qu’il a connaissance du réseau et non pas seulement de ses voisins directs (comme un protocole à état de lien). -La convergence des informations est relativement rapide comparé à d’autres protocoles de la même famille (RIP, Routing Information Protocol). -Il utilise la métrique, en prenant en compte la bande passante et le délai, et non

pas les sauts (d'où le nom d'hybride). -Il possède, en plus d'une route vers le plus court chemin, une seconde route de secours. Ce qui est très efficace lors de panne. Notez qu'il est le seul à avoir cette route de secours. -Il peut faire du load-balancing sur des bandes passantes égales ou inégales (que deux câbles n'est pas la même capacité), ce qu'il est le seul à faire. -Il a une distance administrative de 90. Comment fonctionne EIGRP ? EIGRP commence par établir son voisinage en leur envoyant des messages « Hello ». S'il reçoit à son tour des messages « Hello », il enregistre les données de ses voisins. Il stocke son voisinage dans ce que l'on appelle une table de voisinage. Vous pouvez la consulter avec la commande : show ip eigrp neighbors. Le routeur envoie ensuite ses données au reste du système autonome. Un système autonome, c'est un réseau interne (IGP donc), connecté à Internet et qui a un fonctionnement (un protocole) cohérent. Il s'agit d'un réseau d'entreprise ou de celui d'un fournisseur d'accès. À la réception de ces données, chaque routeur a connaissance du réseau : Show ip eigrp topology Grâce à l'algorithme DUAL, les routeurs sont en mesure de choisir la meilleure route vers un réseau donné. Vous pouvez voir ses informations en tapant la commande : Show ip route. Voilà une vue d'ensemble de ce protocole très puissant et assez simple à configurer qu'est EIGRP. Nous verrons comment le mettre en pratique dans le prochain chapitre. Passons maintenant à un de ces concurrents, de la famille de protocoles à état de lien, OSPF.

BGP

Nous abordons maintenant un protocole particulier. BGP (Border Gateway Protocol) est très différent de ce que nous avons vu jusqu'à présent. Voyons ses caractéristiques dans les grandes lignes. D'abord, c'est un fondement d'Internet. Son utilité principale est d'assurer l'échange de routes entre fournisseurs d'accès à Internet et autres opérateurs de télécommunications. Ensuite, il fonctionne sur un mode pair à pair, en établissant une connexion TCP sur le port 179. Contrairement à RIP ou OSPF qui émettent des messages et découvrent le réseau qui les entoure, BGP doit être spécifiquement configuré sur un routeur pour travailler avec un seul autre routeur voisin. On peut avoir plusieurs liaisons BGP (on parle de sessions) sur un même routeur, mais elles sont indépendantes et doivent être configurées manuellement. Un routeur qui exécute BGP fait le lien entre un réseau dit interne (les clients d'un FAI par exemple) et le réseau d'interconnexion dit externe (Internet). Ce protocole intervient à la frontière entre ces réseaux (figure 14-22). La partie interne est considérée comme un système autonome (autonomous system - AS). Chaque AS dispose d'un numéro qui lui est attribué par une autorité pour éviter les conflits. Comme on peut s'en douter, sur Internet, le nombre de routes est conséquent. BGP a recours à l'agrégation de routes, que nous avons étudiée précédemment, pour alléger un peu les transmissions. Selon le constructeur Cisco, en 2015, une table BGP complète sur Internet compte plus de 570 000 entrées ! Vu le volume, il vaut mieux ne pas transmettre toute sa table de routage à son voisin. Pour éviter la saturation, BGP doit être relativement lent. Chaque routeur envoie à ses voisins les modifications de sa table avec un intervalle minimum de 30 secondes par voisin et par préfixe, c'est-à-dire par route agrégée. Cette valeur est seulement une recommandation et peut être modifiée. Si une route devient inaccessible, l'annonce est immédiate. Toute route reçue par BGP n'est pas forcément intégrée à la table de routage : des comparaisons sont effectuées avec les entrées existantes pour déterminer si une

modification est pertinente. Comme avec OSPF, s'il n'a rien à dire, BGP envoie des messages régulièrement à ses voisins pour dire qu'il est en vie. Si un pair n'émet rien durant 90 secondes (valeur par défaut), la session est considérée close par son voisin. 90 secondes, c'est long, mais une fréquence plus élevée implique mécaniquement une augmentation du trafic et donc augmente le risque de congestion. En revanche, en cas de coupure brute, comme une clôture de session niveau TCP ou un câble débranché, la session BGP prend fin immédiatement.

Analyse de communication réseau

Le principal intérêt de ces logiciels est de visualiser les trames qui transitent par les interfaces réseau d'un appareil. Cela est utile pour comprendre et résoudre un dysfonctionnement, mais c'est aussi très instructif pour connaître finement un protocole. On peut aussi s'en servir pour de la rétro-ingénierie, c'est-à-dire déterminer le fonctionnement d'une application en observant son comportement. Les analyseurs permettent de capturer les flux qui passent en temps réel, de les sauvegarder au format pcap (un format de fichier permettant de stocker des trames réseau), de lire des enregistrements, de les filtrer et de les analyser finement. Pour les hôtes ne disposant pas d'une interface graphique, comme souvent les serveurs, nous recommandons tcpdump. L'installation se fait au moyen du gestionnaire de paquets.