ROUTAGE STATIQUE :

Limitations du routage statique

- Ne s'adapte pas à l'augmentation de la taille du réseau : Nécessite une configuration complexe dans le cas de plusieurs sites
- Ne s'adapte pas aux pannes dans le réseau : Nécessite l'intervention de l'administrateur pour rétablir le routage
- Ne s'adapte pas aux conditions de trafic sur le réseau : Nécessite l'intervention de l'administrateur pour router le trafic sur les chemins les moins chargés

Utiliser dans :

- passerelle par défaut
- Petite installation

ROUTAGE DYNAMIQUE :

Caractéristiques du routage dynamique :

- Apprendre automatiquement les réseaux des sites distants
- Réagir dynamiquement aux changements du réseau : pannes, congestions, …

Envoi de messages protocolaires spécifiques entre les routeurs pour apprendre les réseaux distants

L'algorithme de routage permet de calculer le meilleur chemin vers chacun des réseaux IP appris par le routeur

La métrique du routage dynamique permet d'évaluer la qualité des différents chemins qui mènent vers un même réseau IP afin de choisir le meilleur

RIP : Routing Information Protocol = 120

- Protocole de routage RIP : Échange d'informations de routage entre routeurs adjacents (routeurs voisins connectés directement)
- Algorithme de routage RIP
  - Chaque routeur calcule le meilleur chemin vers chacun des réseaux IP appris
  - Le meilleur chemin correspond au plus court, en comptant le nombre de routeurs traversés
    - La métrique RIP est le nombre de sauts (hop number)
- Chaque information de routage reçue est comparée aux entrées de la table de routage
  - Le routeur décide s'il intègre l'information de routage reçue dans sa table de routage

Mise à jour de table :

- Si le réseau IP reçu dans un message RIP n'existe pas dans la table de routage d'un routeur, il est alors ajouté dans cette table de routage
- Si le réseau IP reçu dans un message RIP existe dans la table de routage mais la métrique reçue est plus petite, la table de routage est alors mise à jour
- Si le réseau IP reçu dans un message RIP provient de la même source que l'entrée de la table de routage, la table de routage est alors mise à jour (même si la métrique est plus grande !)

- Si aucun des trois cas précédents ne se présente, alors il n'y a pas de mise à jour de la table de routage

Périodicité des échanges RIP

- En régime stable (pas de changement dans les tables) :
  - Messages RIP échangés toutes les 30s ± 0 à 5s
- Principe des mises à jour déclenchées (triggered update ou flash update)
  - Un message RIP est diffusé à 0 à 5s dès que la table de routage locale est modifiée
  - Permet une prise en compte rapide des modifications
- Principe du route time-out
  - Un routeur dont on ne reçoit plus de messages RIP depuis 180s devient inaccessible (métrique = ∞)
  - Les entrées de la table de routage apprises via RIP sont donc valables 3 minutes

Un routeur ne renvoie pas une information de routage vers le routeur qui lui a appris cette information.

Accélérer la convergence RIP :

- Afin de réduire le temps de convergence, on «limite» la valeur de l'infini
  - Dans RIP, infini = 16
  - Un «domaine» de routage RIP n'excède pas 15 sauts de routage, ce qui limite l'usage de RIP à des petites configurations
- Utilisation de l'horizon partagé ou split horizon (A ne doit pas envoyer de mise à jour vers B concernant le réseau 10.0.4.0/24 (qui a été appris via B) => split horizon)
- Utilisation de l'horizon partagé avec retour empoisonné ou poison reverse (B envoie une mise à jour vers A concernant le réseau 10.0.4.0/24 avec une métrique de 16 => poison reverse)
- Utilisation des mises à jour déclenchées ou triggered update

RIPv1 :

Message envoyé en diffusion → Adresse destination 255.255.255.255

RIP est encapsulé dans UDP → port source = port destination = 520

Champ commande :

• Requête (request): utilisée par un routeur pour réclamer les informations de routage d'un voisin sans attendre la diffusion programmée (par exemple au démarrage du routeur).

• Réponse (response): utilisée par un routeur pour envoyer ses informations de routage

RPV2 :

Message envoyé en multicast → Adresse destination 224.0.0.9 (le groupe de tous les routeurs RIPv2)

RIP est encapsulé dans UDP → port source = port destination = 520

- Address Family: type des adresses de réseau échangées (en général IP)
- Route tag: indique si les réseaux IP ont été appris via d'autres protocoles et injectés dans RIP

- Adresse et masque de réseau
- Métrique: nombre de sauts
- Next Hop: si ce champ est égal à 0.0.0.0, l'information inscrite dans la table de
- routage d'un routeur B

Protocoles de routage propriétaires: IGRP et EIGRP

Protocoles propriétaires Cisco

• IGRP : Interior Gateway Routing Protocol

• EIGRP (successeur de IGRP) : Enhanced IGRP

Dépassent les limitations de RIP

• Pas de limite à 15 sauts

• Possibilité d'équilibrer la charge sur plusieurs routes

• Moins de messages échangés

Métrique plus intéressante qui combine la bande passante d'un lien, la charged'un lien, le délai, …

RIPng :

RIPng est le premier protocole de routage dynamique proposé pour IPv6

• Simple extension à IPv6 du protocole RIPv2 d'IPv4

• Hérite les mêmes limitations d'utilisation (maximum de 15 sauts par exemple)

Les paquets RIPng sont émis vers l'adresse de multicast all-riprouter FF02::9 et encapsulés dans un paquet UDP avec le numéro de port 521

OSPF (Open Shortest Path First) : OSPF 110

- Algorithme à état de liens ou Link State (utilisé par OSPF)
    - Le routeur A dispose d'une information détaillée sur les réseaux distants
        - Il peut reconstituer le schéma global du réseau
    - Le routeur A utilise cette information pour calculer le meilleur chemin

Avantages des algorithmes à état de lien

• Calcul qui prend en compte les caractéristiques de tous les liens traversés

• Chaque routeur dispose d'une vision actualisée de tout le réseau et calcule le meilleur chemin vers un réseau IP en prenant en compte les caractéristiques de tous les liens traversés

• Calcul rapide de la table de routage en cas de changements (convergence rapide)

• Chaque routeur dispose d'une vision actualisée de tout le réseau et réagit plus rapidement à tout changement (par exemple une panne ou une reconfiguration)

Les algorithmes à état de lien sont plus adaptés aux grands réseaux que les algorithmes vecteur distance

Fonctionnement du protocole de routage OSPF

- Découverte de voisins OSPF
- Échange d'information de routage
- Calcul des meilleurs chemins
- Mise à jour de l'information de routage

Algorithme de routage OSPF : Algorithme des plus courts chemins SPF (par E. Dijkstra)

Un routeur OSPF maintient trois tables d'information

- La table des voisins OSPF : Une table qui contient les adresses des routeurs OSPF voisins
- La table des états de liens appelée Link State DataBase (LSDB) : Une table d'information qui contient les caractéristiques de tous les liens du réseau (de ses interfaces (état, coût, ...) et des réseaux directement connectés)
- La table de routage : Une table qui contient les réseaux appris et une passerelle par réseau destination

Découverte automatique des routeurs OSPF voisins :

- Envoi périodique de messages OSPF de type Hello
- Permet de maintenir une liste de voisins OSPF

Un message Hello est envoyé périodiquement par un routeur OSPF sur chacune de ses interfaces

Principaux champs du message Hello

- Router ID: identifiant du routeur qui correspond à l'adresse IP la plus élevée parmi les interfaces du routeur
- Hello interval: période des envois de messages Hello (10 s)
- Dead interval: temps au bout duquel le routeur supprime le voisin de sa liste, s'il n'a pas reçu de message Hello (40 s)
- Neighbor: liste des identifiants des routeurs voisins que le routeur a découvert via des échanges de messages Hello

Init (initialisation)
2Way (voisinage bidirectionnel)
Exstart (début d'échange)
Exchange
LS Request (réclame des informations)
LS Update (envoie infos)
LS Acknowledge (acquittement)
Full (synchronisés)
La métrique OSPF se présente sous la forme d'un coût associé à chaque interface d'un routeur

- Le coût est choisi par l'administrateur
- Le coût est un entier positif
- Le meilleur chemin a le coût le plus bas
- Le coût d'un chemin est égal à la somme des coûts des interfaces sortantes des routeurs traversés

108/Débit (en bits/s)

Un changement d'état de lien se produit lorsque:

- Le protocole OSPF est déclenché sur un routeur
- Le coût d'une interface OSPF change

- L'état d'une interface change : par exemple une interface qui tombe en panne

Si un changement d'état de lien se produit

- Le routeur concerné
    - Génère ou met un jour l'information dans sa table LSDB
    - Recalcule les meilleurs chemins
    - Envoie un message Link State Update vers ses voisins
- Les voisins
    - Mettent à jour leur base
    - Acquittent l'information par un message Link State Acknowledge
    - Envoient l'information vers leurs voisins

Diffusion fiable ou Reliable flooding lors d'un changement d'état de lien ou périodiquement toutes les 30 minutes

Les aires OSPF

Objectif :

- Réduire la charge des routeurs OSPF sur un réseau de grande taille
- Réduire le nombre d'échanges OSPF sur un réseau de grande taille

Méthode :

- Mettre en place plusieurs aires de routage sur un même réseau
- Les informations d'état de lien sont échangées à l'intérieur d'une aire

Propriétés :

- Chaque aire est identifiée par un numéro
- Chaque routeur maintient une table LSDB relative à l'aire à laquelle il appartient
- Un routeur de bordure d'aire (ABR : Area Border Router) possède des interfaces attachées à plusieurs aires, et assure ainsi le passage d'informations de routage résumées entre aires
- Un ABR possède une table LSDB pour chacune des aires à laquelle il est connecté

Une aire backbone (area 0) doit être configurée sur un réseau OSPF

- Elle assure le lien entre les différentes aires secondaires
- Toutes les aires secondaires doivent être connectées à l'aire backbone

DR (routeur désigné)

Routeur élu lors de l'établissement du voisinage (messages Hello)

- Comparaison de la priorité du routeur envoyée dans le message Hello
- Le DR a la priorité la plus élevée
- Tous les routeurs, sur le réseau Ethernet, synchronisent leurs LSDB avec le DR

BDR (Routeur désigné de secours)

Routeur élu lors de l'établissement du voisinage (messages Hello)

- Comparaison de la priorité du routeur envoyée dans le message Hello
- Le BDR a la deuxième priorité la plus élevée (après celle du DR)
- Tous les routeurs sur le réseau Ethernet synchronisent leurs LSDB avec le DR et le BDR
- Si le DR tombe en panne, le BDR prend la relève

Router ID

- Identifiant du routeur qui correspond à l'adresse IP la plus élevée parmi les interfaces du routeur
- Sauf si on configure une interface loopback sur le routeur, dans ce cas, l'identifiant du routeur correspond à l'adresse IP de l'interface loopback
- L'interface loopback est une interface virtuelle (logicielle) joignable par n'importe quel port physique

INTER-VLAN :

Transport de VLAN: utilisation de liens trunk

Objectif

- Assurer le transport de VLAN entre commutateurs
- Simplifier la mise en place basique qui nécessite une interface par VLAN sur chacun des équipements

Méthode

- Utiliser un seul lien entre commutateurs pour transporter plusieurs VLAN

Utilisation du protocole IEEE 802.1Q

- Ajout d'un numéro de VLAN appelé aussi VLAN TAG dans les trames sur un lien trunk pour identifier l'appartenance à un VLAN

Mise en place d'un routeur pour interconnecter les VLAN: routage inter-VLAN

- Chaque VLAN correspond à un réseau IP
- Les interfaces du commutateur sont configurées en mode access

Bilan de l'interconnexion des VLAN

Nécessité d'un équipement de niveau 3

- Routeur => routage inter-VLAN
    - Utilisé dans les petites installations
- Commutateur de niveau 3 => commutation inter-VLAN
    - Utilisé dans les grandes installations en raison de ses hautes performances

Positionnement

- Les VLAN permettent de séparer le trafic
- Le routage ou la commutation inter-VLAN permettent aux équipements dans des VLAN différents de communiquer !
- Mais offrent aussi la possibilité de filtrer le trafic d'une manière intelligente en se basant sur les adresses IP, les numéros de ports, les applications, …

NAT

Différentes formes de NAT

- Statique :

Configuration d'une table fixe de traduction par l'administrateur

- Adresse IP privée <=> adresse IP publique

Utile quand une station du réseau privé doit être accessible depuis Internet

- Dynamique :

Traduit une adresse IP privée en une adresse IP publique « libre », choisie dans une plage d'adresses configurée dans le routeur

- Les traductions actives adresse IP privée <=> adresse IP publique sont conservées par le routeur dans une table
- Une adresse publique sort de la table et redevient libre, si aucun trafic relatif à cette adresse n'est détecté par le routeur au bout d'un temps prédéfini

- Overloading (NAT/PAT) :

Le routeur dispose d'une seule adresse IP publique (ex. un routeur ADSL)

- Chaque adresse privée est traduite vers cette adresse unique

Pour distinguer les différentes connexions, on traduit cette fois-ci les ports source au niveau TCP et UDP, ou le champ « identifiant » d'un message ICMP

- Les traductions actives sont conservées par le routeur dans une table
- Une entrée de la table est purgée, si aucun trafic relatif à cette entrée n'est détecté par le routeur au bout d'un certain temps
- Le routeur traite directement les éventuels conflits de ports

Redirection de ports

Un serveur du réseau privé peut être rendu accessible via un mécanisme de port forwarding (par ex. tout paquet destiné au port 80 est traduit vers la même adresse IP)

Listes d'accès ACL / Filtrage des paquets IP

Le filtrage des paquets IP permet de mettre en place une décision simple

- Autoriser le paquet IP
- Interdire le paquet IP

L'autorisation d'un paquet IP ne garantit pas sa livraison

- Le routage doit être bien configuré sur le réseau !

Mise en place du filtrage sur un routeur

- Déclaration d'un ensemble de règles (autorisation, interdiction)
    - Access-list ou ACL sur un routeur Cisco

- Configuration de l'ACL comme filtre d'entrée ou de sortie sur le routeur (Une ACL est un ensemble de règles désignées par un numéro ou une chaîne de caractères)

Ex :

access-list 100 deny/permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

- 100: numéro de l'ACL
- deny ou permit: action de la règle
- 192.168.1.0 0.0.0.255: source des paquets avec un masque inversé
- 192.168.2.0 0.0.0.255: destination des paquets avec un masque inversé

Définition d'une source ou d'une destination

- Plage d'adresses IP avec un masque inversé
    - 192.168.1.0 0.0.0.255
- Toutes les adresses IP
    - Mot clé: any
- Adresse IP unique
    - host 192.58.38.62 ou 192.58.38.62 0.0.0.0

Les règles d'une ACL deviennent actives quand elles sont affectées à une interface

- Entrée = in
- Sortie = out

Accès à l'Internet et transition vers IPv6

Duplicate Address Detection (DAD)
Paquet Neighbor Solicitation
Paquet Router Solicitation
Paquet Router Advertisement