

OSPF

Ateliers Afnog: F2

Eric Assi

AFNOG 2006

OSPF : Chapitre 1

INTRODUCTION AUX IGP

AFNOG 2006

Protocole de routage interne (IGP)

- Avantages des IGP
- Convergence
- RIP
- EIGRP
- ISIS
- OSPF

AFNOG 2006

Les avantages du routage dynamique

- Detection automatique et adaptation aux changements de topologie
- Routage optimal
- Evolutif
- Robuste
- Simple
- Convergence rapide
- Controle sur le choix des routes

AFNOG 2006

Notion de convergence

- On parle de convergence lorsque tous les routeurs ont la même information de routage
- En cas de non convergence, les ressources du réseau peuvent être inaccessibles
 - Les paquets sont acheminés vers d'autres destinations.
 - On parle de trou noir "Black holes" (les paquets disparaissent)
 - Bouclage du processus de routage (routing loops)
 - Le processus de convergence est déclenché après changement de status d'un routeur ou d'un lien.

AFNOG 2006

RIP

- Pour "Routing Information Protocol"
- Plusieurs problèmes d'évolutivité
- RIPv1 est "classful", officiellement obsolète
- RIPv2 est "classless"
 - Plus de performances et de fonctionnalités que RIPv1
 - N'est pas utilisé à grande échelle dans le réseau d'internet
 - Utiliser seulement aux limites de l'internet, entre le réseau d'accès (dial-up access) configuré en RIPv2 et la couche suivante du réseau.

AFNOG 2006

Les inconvénients de RIP

- RIP est basé sur l'algorithme du "vecteur distant"
 - Ecoute toutes les routes du voisinage
 - Installe toutes les routes dans sa table routage
 - Le plus petit nombre de saut vers une destination X l'emporte
 - Annonce toutes les routes de sa table de routage
 - très simple, très stupide
- La seule métrique est le nombre de saut
- Le nombre maximum de saut sur un réseau 16 (pas plus)
- convergence lente (bouclage de route)
- Pas assez robuste

AFNOG 2006

IGRP/EIGRP

- "Enhanced Interior Gateway Routing Protocol"
- Nouvelle version de IGRP qui était "classful"
 - IGRP développé par Cisco en 1980s pour résoudre les problèmes inhérents à RIP
- Protocole de routage propriétaire Cisco
- Basé sur l'algorithme du "Vecteur distant"
 - Bon contrôle de la métrique
- Largement utilisé sur le réseau de plusieurs entreprises et quelques ISP.
 - Multiprotocole (supporte IP, IPX, APPLE TALK,)
 - Très évolutifs et convergence rapide
 - Supporte l'équilibrage de charge (load balancing) pour des chemins de coûts différents.

AFNOG 2006

IS-IS

- "Intermediate System to Intermediate System"
- Choisi en 1987 by ANSI comme un protocole de routage intra-domaine OSI (CLNP – connectionless network protocol)
 - Basé sur les travaux de DEC pour DECnet/OSI (DECnet Phase V)
 - IS-IS est basé sur l'algorithme de Dijkstra
- Extensions vers IP développées en 1988
 - NSFnet a déployé, son IGP en se basant sur une version récente du draft ISIS-IP
 - Côte d'Ivoire Telecom utilise IS-IS comme IGP sur son réseau MPLS

AFNOG 2006

IS-IS (cont)

- Les motivations du développement d'IS-IS
 - Un protocole non propriétaire
 - Un grand espace d'adressage
 - Un adressage hiérarchisé
- Similarités entre IS-IS et OSPF
 - Protocoles d'état de lien basés l'algorithme de Dijkstra
 - Topologie à deux niveaux
 - OSPF est plus déployé comme solution d'entreprise
 - IS-IS plus utilisé sur des réseaux d'ISP ou opérateurs télécom
- Différences entre IS-IS et OSPF
 - Identification des aires
 - Un routeur dans IS-IS n'appartient qu'à une seule aire
 - Il n'existe pas de routeur désigné backup avec IS-IS

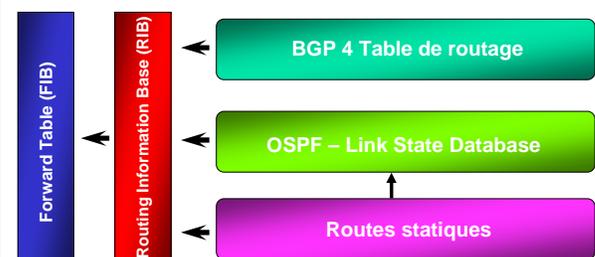
AFNOG 2006

Note: Routage et transmission

- Le routage est différent de la transmission
- Le routage permet de constituer une carte du réseau
 - Chaque protocole de routage a sa base de données de routage
 - Les protocoles de routage annoncent les tables de transmission
- La transmission consiste à acheminer le paquet vers l'équipement adjacent
 - La table de transmission contient le meilleur chemin vers le prochain saut pour chaque préfixe.
 - Il existe toujours une seule table de transmission

AFNOG 2006

La table de transmission



AFNOG 2006

OSPF : Chapitre 2

LES BASES D'OSPF

AFNOG 2006

LES BASES D'OSPF

- Historique de l'OSPF
- Le protocole d'état de lien
- Les paquets OSPF
- Le protocole Hello
- routeur désigné
- Topologie de réseaux OSPF

AFNOG 2006

Historique de l'OSPF

- Développé par IETF – RFC1247
 - Destiné pour les réseaux TCP/IP sur Internet
- OSPF v2 version récente publiée 1998 dans le RFC2328/STD54
- OSPF V3 (extension à IPv6) publié en 1999 dans le RFC2740
- Etat de lien/Technologie du chemin le plus court (SPF)
- Le routage dynamique
- La convergence
- L'authentification de route

AFNOG 2006

Le protocole d'état de lien

- Basé sur l'algorithme de Dijkstra
 - Détermination du chemin le plus court
- Tous les routeurs calculent le meilleur chemin vers une destination donnée
- Tout changement d'état de lien est diffusé à travers le réseau

AFNOG 2006

Le protocole d'état de lien

- Chaque routeur détient une base de données contenant toute la cartographies du réseau
 - Les liens
 - Leur état (avec leur coût)
- Tous les routeurs ont la même information
- Tous les routeurs calculent le meilleur chemin vers toute destination
- Tout changement d'état de lien est diffusé à travers le réseau

AFNOG 2006

Routage basé sur l'état de lien

- Identification automatique de voisin (équipement adjacent)
 - Les voisins sont des routeurs physiquement connectés
- Chaque routeur construit un paquet d'état de lien (LSP: Link State Packet)
 - Distribue les paquets LSP aux voisins...
 - En utilisant des LSA (Link State Advertisement)

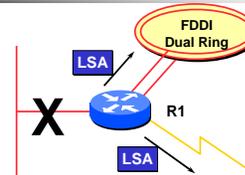
AFNOG 2006

Routage basé sur l'état de lien

- Chaque routeur calcule le meilleur chemin vers toute destination
- En cas de rupture d'un lien
 - De nouveaux paquets d'état de lien (LSP: Link state packet) sont diffusés
 - Tous les routeurs recalculent leur table de routage

AFNOG 2006

Faible bande passante



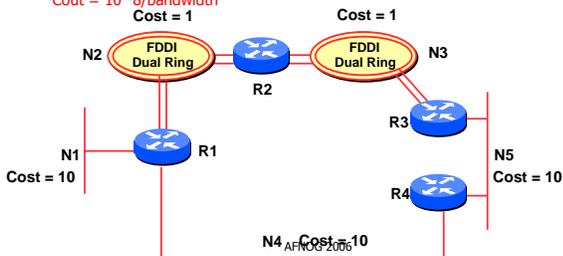
- Seuls les changements sont propagés
- Le Multicast est utilisé sur les réseaux multi-accès à diffusion
 - 224.0.0.5 est utilisé pour tous les routeurs parlant OSPF
 - 224.0.0.6 est utilisé par les DR (designated router) et les BDR (backup designated router) routeurs

AFNOG 2006

"Shortest Path First"

- Le chemin optimal est déterminé par la Somme des coûts des différents interfaces.
- La métrique est calculée à partir de la bande passante

$$\text{Coût} = 10^8 / \text{bandwidth}$$



AFNOG 2006

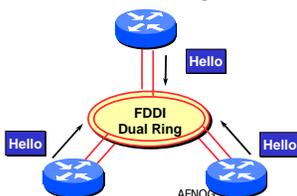
Les paquets OSPF

- 5 types de paquets utilisés par OSPF :
 - L'établissement des relations de voisinage, étape transitoire des routeurs adjacents
 - Mise à jour des tables de routage de routage
 - Hello
 - Database description (DDP)
 - Link-state request (LSR)
 - Link-state update (LSU)
 - Link-state acknowledgment (LSA)

AFNOG 2006

Le protocole Hello

- Le Protocole Hello
 - Responsable de l'établissement et la maintenance du dialogue en routeurs voisins
 - Election de routeur désigné sur les réseaux à diffusion



AFNOG 2006

Les paquets Hello OSPF

- Le Protocole Hello
 - les paquets Hello sont périodiquement transmis sur toutes les interfaces OSPF
 - Multicast des paquets (224.0.0.5) sur toutes les interfaces des routeurs
 - Périodicité 10s sur les LAN, 30s sur les NBMA
 - Dead interval 40s sur les LAN, 120s sur les NBMA
- Le paquet Hello
 - Contient les informations telles que la Priorité du routeur, les intervalles d'annonce d'Hello, une liste des voisins reconnus, etc

AFNOG 2006

Les paquets Hello OSPF

- Utilisation des annonces LSA (Link state advertisement)
 - Les LSAs sont ajoutés à la base de données OSPF
 - Les LSAs sont transmis vers les voisins OSPF
- Chaque routeur construit une base de donnée d'état de lien identique
- l'algorithme SPF s'appuie sur cette base de donnée
- Création de la table transmission à partir "SPF tree"

AFNOG 2006

L'Algorithme OSPF

- Lorsqu'un changement survient :
 - Le changement est annoncé à tous les voisins
 - Tous les routeurs exécutent l'algorithme SPF en utilisant la nouvelle base de données
 - Le protocole reste passive lorsque que réseau est stable
 - Une mise à jour périodique des LSA **chaque 30 minutes**, dans le cas contraire, les mis à jour à chaque changement d'état du réseau

AFNOG 2006

Routeurs désignés

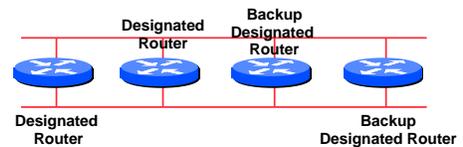
Ces routeurs contrôlent les mises à jour des informations de routage sur les réseaux à diffusion et d'accès multiple (Ethernet, token ring, FDDI,..)

- Seuls les DR et les BDR peuvent être totalement adjacents avec les autres routeurs
- Les autres routeurs restent dans un état "2-way" en eux.
- Si le DR ou le BDR "disparaît", une re-elections du routeur disparu s'opère.

AFNOG 2006

Routeurs désignés (suite)

- Un seul DR par réseau d'accès multiple
 - Génère des paquets LSA sur le réseau
 - Le BDR écoute mais ne génère aucun paquet
 - Accélère la synchronisation des bases de données
 - Réduit le trafic sur le réseau d'accès



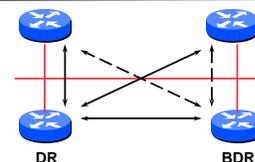
AFNOG 2006

Routeur désigné (suite)

- Les DR/BDR permettent d'éviter la surcharge du réseau
 - relation entre routeurs sans DR/BDR parlant OSPF $n(n-1)/2$ contre $2n-2$ avec DR/BDR
 - Réduit l'utilisation des CPU des routeurs
- Tous les routeurs sont adjacents au routeur DR/BDR
- Le routeur DR met à jour la base de données de tous ses voisins

AFNOG 2006

Routeur désigné (suite)



- Diffusion de LSA (routeurs adjacents)

AFNOG 2006

routeur désigné (suite)

- Déterminée par la priorité de l'interface
- Par le routeur ayant le plus grand ID
 - Pour Cisco IOS, c'est l'adresse IP de l'interface loopback
 - En l'absence de loopback, la plus grande adresse IP d'une interface physique sur le routeur



AFNOG 2006

routeur désigné (suite)

- Peut être forcée en changeant l'ID du routeur :
 - router-id <ip address>
- Peut être forcée en changeant la priorité du routeur :
 - ip ospf priority 100 (default "1", candidat non éligible "0")

AFNOG 2006

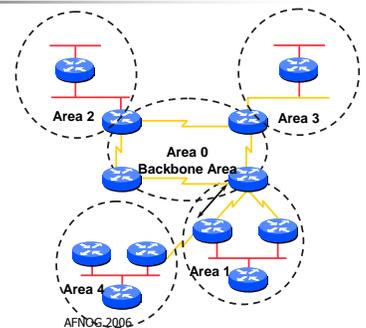
Topologie de réseaux OSPF

- Aires OSPF
- Liens virtuels
- Types de Routeurs
- Types de routes OSPF
- Différents types de LSA
- Route avec authentification
- Plusieurs chemins de couts identiques

AFNOG 2006

Aires OSPF

- Groupe de réseaux et d'hotes contigus
- Base de données définie par aire
 - Invisible hors de la aire
 - Réduction du trafic de routage
- Backbone d'aires contigues
 - Toutes les aires doivent être connectées au backbone
- Liens virtuels



AFNOG 2006

Aires OSPF (suite)

- Réduit le trafic de routage au niveau du backbone aire 0
- Quand doit-on subdiviser le réseau en aires ?
 - lorsque le backbone a plus de 10 à 15 routeurs
 - Lorsque la topologie du backbone devient complexe
- Le design des aires s'apparente à l'architecture des backbones d'ISP

AFNOG 2006

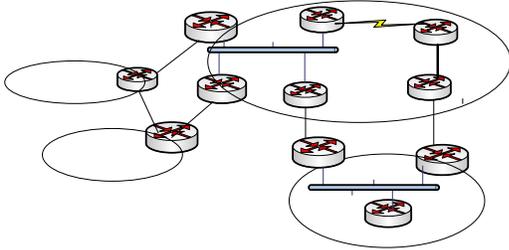
Liens virtuels

- Pas recommandés
- A quoi servent-ils ?
 - Utiliser dans un scénario de backup
 - Permet d'assurer la connectivité d'une aire à une aire autre que le backbone
 - Permet d'assurer la connectivité d'une aire déconnectée

AFNOG 2006

Liens Virtuels

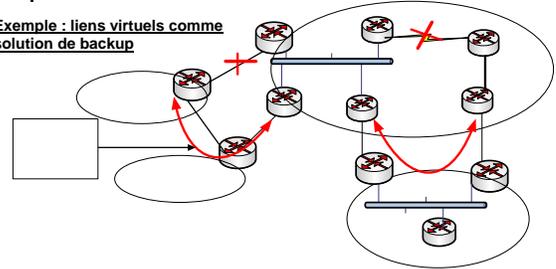
Exemple : liens virtuels



AFNOG 2006

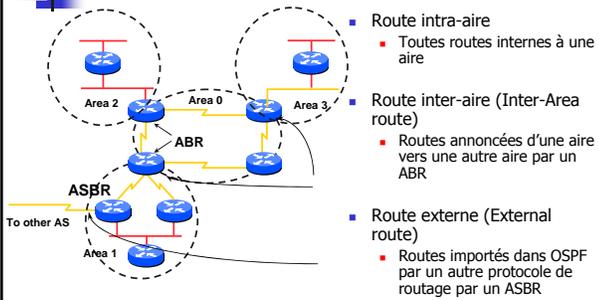
Liens virtuels

Exemple : liens virtuels comme solution de backup



AFNOG 2006

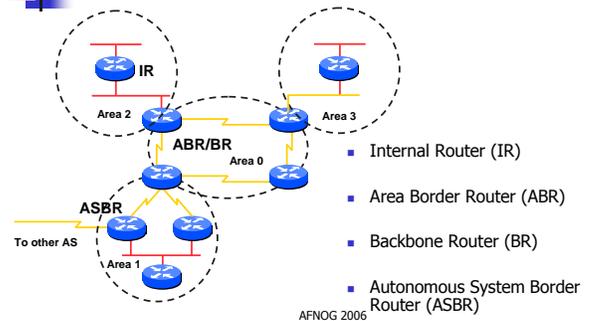
Routes OSPF



- Route intra-aire
 - Toutes routes internes à une aire
- Route inter-aire (Inter-Area route)
 - Routes annoncées d'une aire vers une autre aire par un ABR
- Route externe (External route)
 - Routes importés dans OSPF par un autre protocole de routage par un ASBR

AFNOG 2006

Classification des routeurs



AFNOG 2006

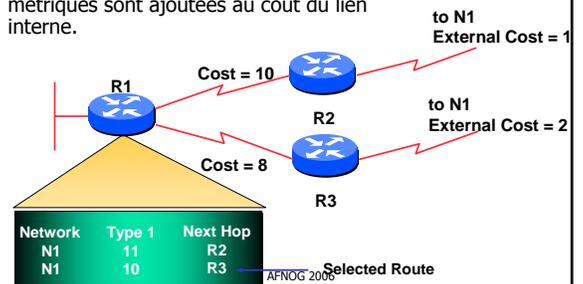
Différents types LSA

- LSA type 1 : Descrit l'état et le coût des liens d'un routeur vers l'aire
- LSA type 2 : Généré par le DR décrit, les routeurs rattachés à un réseau à diffusion
- LSA type 3 : Généré par un ABR, définit une destination hors de l'aire mais interne à l'AS
- LSA type 4 : détient les informations sur l'ASBR
- LSA type 5 : routes externes, routes hors de l'AS, la route par défaut est considérée comme une route externe

AFNOG 2006

Routes Externes

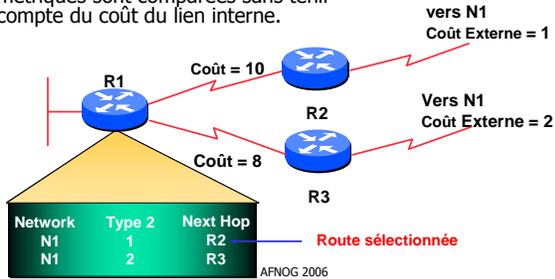
- LSA Type 5 (E1) métrique externe: les métriques sont ajoutées au coût du lien interne.



AFNOG 2006

Routes externes

- LSA Type 5 (E2) métrique externe: les métriques sont comparées sans tenir compte du coût du lien interne.



Authentication de route

- La recommandation actuelle est l'utilisation de l'authentification pour l'OSPF
 - ...et pour tous les autres protocoles de routage exposer aux attaques de denis de service
 - OSPF utilise TCP/IP

AFNOG 2006

Chemins multiples à coûts identiques

- Lorsque n chemins vers une même destination ont des coûts égaux, OSPF installe n entrées dans la table de transmission
 - On a une repartition de la charge du réseau vers les n chemins
 - Solution idéale pour étendre les capacités des liens sur les backbones d'ISP
 - Evite l'utilisation d'équipement de multiplexage
 - Evite l'utilisation de route statique

AFNOG 2006

Résumé

- Les IGP: RIP obsolète, IS-IS pour les ISP, OSPF plus utilisé par les entreprises
- Table de transmission \neq table routage
- Le protocole Hello: maintient la base de donnée OSPF
- Topologie OSPF est hiérachisée basées sur des aires : Backbone et aires secondaires
- Authentication de route obligatoire
- Exécution d'OSPF : Consomatrice en CPU

AFNOG 2006