



Ateliers SI-F AFNOG 2009

OSPF

Eric Assi

AFNOG 2009



OSPF : Chapitre 1

INTRODUCTION AUX IGP

AFNOG 2009



Protocole de routage interne (IGP)

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

AFNOG 2009

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 2009

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 2009

RIP

- Pour "Routing Information Protocol"
- Plusieurs problèmes d'évolutivités
- RIPv1 est "classful", officiellement obsolete
- RIPv2 est "classless"
 - Plus de performances et de fonctionnalités que RIPv1
 - N'est pas utilisé à grande échelle dans au niveau 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 2009

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 2009

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 2009

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 in 1988
 - NSFnet a déployé, son IGP en se basant sur une version récente du draft ISIS-IP

AFNOG 2009

IS-IS

- Dans l'environnement IS-IS tout est soit un intermédiaire système (IS) ou un End Système (ES)
 - ES : Host
 - IS : Router
- IS-IS : Est un protocole qui permet aux (IS) de communiquer avec d'autres (IS), donc aux routeurs de communiquer entre eux.
- IS-IS transporte les informations de routage du protocole OSI
- Très facile de le modifier et transporter d'autres protocoles tels que IPv4 et IPv6.

AFNOG 2009

IS-IS (cont)

- Les motivations du développement d'IS-IS
 - Un protocole non propriétaire, large 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

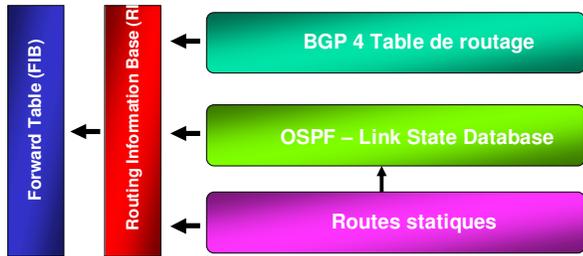
AFNOG 2009

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 2009

La table de transmission



AFNOG 2009

Note : Distance administrative (cisco)

Route Source	Default Distance
Connected Interface	0
Static Route	1
Enhanced IGRP Summary Route	5
External BGP	20
Internal Enhanced IGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
External Enhanced IGRP	170
Internal BGP	200
Unknown	255

AFNOG 2009

OSPF : Chapitre 2

LES BASES D'OSPF

AFNOG 2009



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 2009



Historique de l'OSPF

Développé par IETF – RFC1247

- Destiné pour les réseaux TCP/IP sur Internet
- OSPF v2 version recente 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 2009



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 2009



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 2009



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 2009

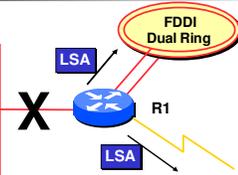


Routage basé sur l'état de lien

- 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 2009

Faible bande passante



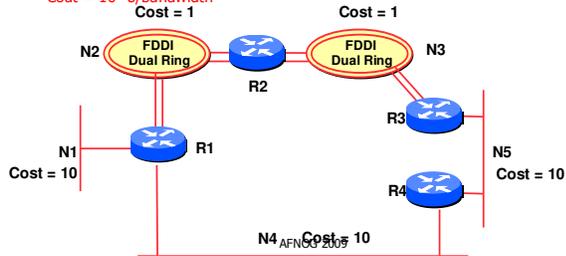
- Seuls les changements sont propagés
- Le Multicast est utilisé sur les réseaux multi-accès à diffusion
 - 224.0.0.5 est utilisé pour tous les routeurs parlant OSPF
 - 224.0.0.6 est utilisé par les DR (designated router) et les BDR (backup designated router) routeurs

AFNOG 2009

"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 2009

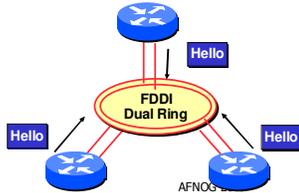
Les paquets OSPF

- 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
- Hello
- Database description (DDP)
- Link-state request (LSR)
- Link-state update (LSU)
- Link-state acknowledgment (LSA)

AFNOG 2009

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



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 2009

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 2009

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 mises à jour à chaque changement d'état du réseau

AFNOG 2009

Routeurs désignés

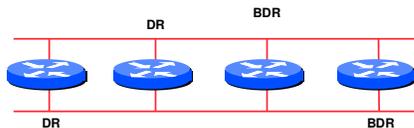
Ces routeurs contrôlent les mises à jour des informations de routage sur les réseaux à diffusion et d'accès multiple (Ethernet, token ring, FDDI,..)

- 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 2009

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



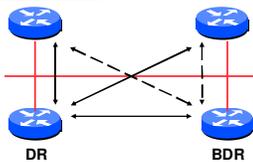
AFNOG 2009

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 2009

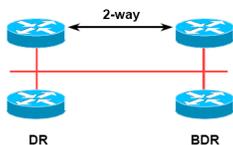
Routeur désigné (suite)



- Diffusion de LSA (routeurs adjacents)
- DR et BDR etat "FULL" avec les autres routeurs parlant OSPF

AFNOG 2009

Routeur désigné (suite)

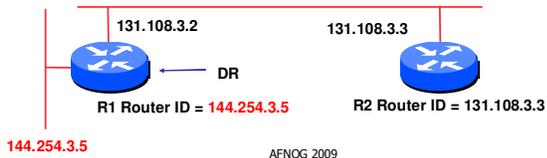


- DR et BDR etat "FULL" avec les autres routeurs parlant OSPF
- Les autres routeurs sont dans un état "2-way"

AFNOG 2009

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 2009

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 2009

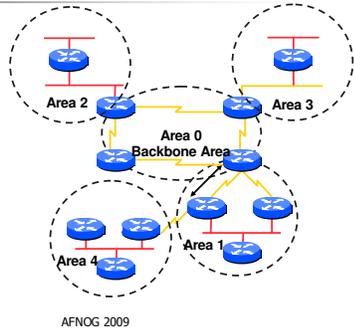
Topologie de réseaux OSPF

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

AFNOG 2009

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



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 2009

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 2009

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

AFNOG 2009

Classification des routeurs

- Internal Router (IR)
- Area Border Router (ABR)
- Backbone Router (BR)
- Autonomous System Border Router (ASBR)

AFNOG 2009

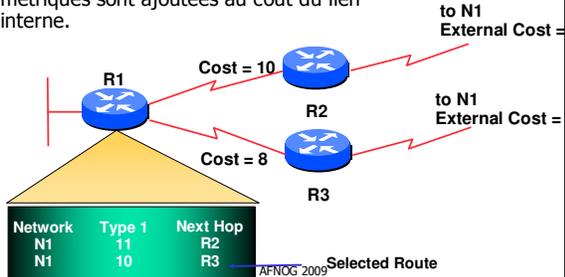
Différents types LSA

- 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 2009

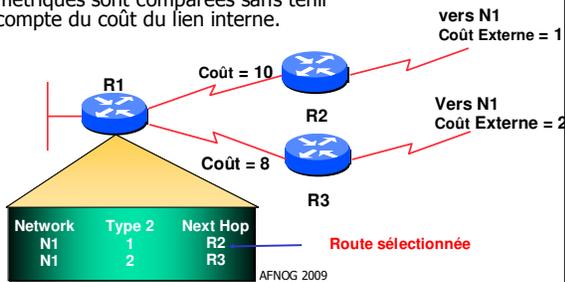
Routes Externes

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



Routes externes

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



Authentication de route

- Il est recommandé d'utiliser l'authentification OSPF
 - ...et pour tous les autres protocoles de routage
Exposer aux attaques de denis de service
 - OSPF utilise TCP/IP

AFNOG 2009

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** (partage de charge)
- 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 2009

OSPFv3 Introduction

- Les specifications du protocole sont publiées dans le RFC 2740
- Link-state IGP (cout tinterface additive)
- Principe de base identique à OSPF pour IPV4
- Distribue les prefixes IPV6
- IPv4/IPv6 OSPF fonctionne en "ships in the night"

AFNOG 2009

OSPFv3/OSPFv2 Similarités

- Les memes types de packets de base
 - Hello, DBD, LSR, LSU, LSA
- Mecanisme de decouverte de voisin et de formation de relation d'adjacent.
- Types d'interfaces
 - P2P, P2MP, Broadcast, NBMA, Virtual
- Diffusion de LSA
- Types LSA presqu'identique

AFNOG 2009

OSPFv3/OSPFv2 differences

- **OSPFv3 est activé sur un lien** et non par sous-réseaux
- Un lien par definition est un medium de communication de deux noeuds au niveau de la couche liaison.
- Dans IPv6 plusieurs sous-reseaux IP peuvent être assignés à un lien et deux noeuds de differents sous-réseaux peuvent communiquer au niveau de la couche liaison, OSPFv3 s'appuie sur ce principe.

AFNOG 2009

OSPFv3/OSPFv2 differences

- **Support de plusieurs instances par lien**
- Un nouveau champ dans l'en-tête du paquet OSPF permet d'activer plusieurs instances par lien.
- Les identifiants des instances (ID) doivent correspondre pour que le paquet soit accepté.

AFNOG 2009

OSPFv3/OSPFv2 Differences

- Utilisation des adresses "link-local"
- Deux nouveaux types de LSA
 - Link-LSA (type 8)
 - Inter-area-prefix-LSA (type 9)
- Utilise des adresses multicast :
 - FF02::5 (ALLDRRouter)
 - FF02::6 (ALLSPFRouter)

AFNOG 2009

OSPFv3 Link-state LSA

■ LSA "Link-state" par lien :

- Les "scope" du lien local sont diffusés que sur le lien auquel ils sont associés
- Fourni l'adresse router "link-local"
- Liste tous les préfixes IPV6 attachés au lien
- une collection de bit d'option pour les "Router-LSA"

AFNOG 2009



AFNOG 2009

OSPFv3 les commandes IOS

Visualiser le voisinage OSPF:

show ipv6 ospf neighbor

show ipv6 ospf [<process ID>]

clear ipv6 ospf [<process ID>]

Visualiser les informations des LSA:

show ipv6 ospf [<process ID>] database link

show ipv6 ospf [<process ID>] database prefix

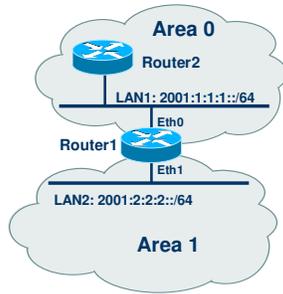
Commande de debug:

debug ipv6 ospf ...

AFNOG 2009

OSPFv3 exemple de configuration

```
Router1#  
interface Ethernet0  
  ipv6 address 2001:1:1:1::1/64  
  ipv6 ospf 1 area 0  
  
interface Ethernet1  
  ipv6 address 2001:2:2:2::2/64  
  ipv6 ospf 1 area 1  
  
ipv6 router ospf 1  
  router-id 1.1.1.1  
  area 1 range 2001:2:2::/48
```



AFNOG 2009

Résumé

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

AFNOG 2009
