Réseaux informati

Nouvelle édition en français

Cisco CCNA

Guide de préparation à l'examen de certification CCNA 200-301

Volume 2

Routage et connectivité IP

© 2021 François-Emmanuel Goffinet

Cisco CCNA 200-301 Volume 2

Guide de préparation au Cisco CCNA 200-301 en français, Volume 2 Routage et connectivité IP

François-Emmanuel Goffinet

Ce livre est en vente à http://leanpub.com/cisco-ccna-2

Version publiée le 2021-09-19

Ce livre est publié par Leanpub. Leanpub permet aux auteurs et aux éditeurs de bénéficier du Lean Publishing. Lean Publishing consiste à publier à l'aide d'outils très simples de nombreuses itérations d'un livre électronique en cours de rédaction, d'obtenir des retours et commentaires des lecteurs afin d'améliorer le livre.

© 2020 - 2021 François-Emmanuel Goffinet

Table des matières

© 2021 François-Emmanuel Goffinet

© 2021 François-Emmanuel Goffinet

© 2021 François-Emmanuel Goffinet

Avertissement

Le projet lié à cet ouvrage est conçu principalement pour des candidats francophones à l'examen de certification Cisco CCNA 200-301.

Le document sera probablement utile comme *support de formation* dans d'autres contextes tels que celui de l'autoapprentissage, de l'enseignement ou de la formation professionnelle.

Si le document peut sans doute contribuer à mieux connaître les réseaux d'entreprise dans la perspective du CCNA, il ne peut aucunement garantir la réussite de l'examen. Aussi, ce projet n'a jamais poursuivi l'ambition de remplacer d'autres sources d'information/formation issues des canaux officiels tels que *Cisco Press*, *Cisco Learning Network*, les *Cisco Systems Learning Partners*, *Cisco Academy* ou encore la documentation officielle du fabricant. D'ailleurs l'auteur est totalement indépendant de tout fabricant cité. Celles-ci, toutes mieux présentées les unes que les autres, ne manquent pas au contraire, mais il est rare de trouver des sources de qualité et fiables en français.

Copyrights

Les entreprises suivantes et leurs marques protégées sont citées dans le document :

- Cisco Systems
- HP/Aruba
- VMWare
- Microsoft
- Red Hat
- Canonical
- Linux Foundation
- Wikimedia
- Wikipedia
- Docker
- GNS3

Dédicace

À mes parents qui m'ont toujours apporté un soutien sans faille dans tous mes projets.

Remerciements

Merci aux milliers de visiteurs quotidiens du site cisco.goffinet.org.

Merci aux centres de formation et aux écoles qui m'accordent leur confiance et qui me permettent de rencontrer mon public en personne.

Merci à Wendell Odom, mon mentor sur le sujet Cisco CCNA. N'hésitez pas à vous procurer ses livres en anglais chez Cisco Press.

Merci à Stéphane Bortzmeyer dont la prose prolifique m'inspire et m'aide à vulgariser les technologies de l'Internet.

Merci enfin à Cisco Systems d'être aussi ouvert depuis tant d'années dans sa documentation et pour son effort à rendre les technologies des réseaux plus accessibles, mieux comprises et plus populaires.

Avant-Propos

François-Emmanuel Goffinet est formateur IT et enseignant depuis 2002 en Belgique et en France. Outre Cisco CCNA, il couvre de nombreux domaines des infrastructures informatiques, du réseau à la virtualisation des systèmes, du nuage à la programmation d'infrastructures hétérogènes en ce y compris DevOps, Docker, K8s, chez AWS, GCP ou Azure, etc. avec une forte préférence et un profond respect pour l'Open Source, notamment pour Linux.

On trouvera ici un des résultats d'un projet d'autopublication en mode *agile* plus large lié au site web cisco.goffinet.org. La documentation devrait évoluer dans un format vidéo. Les sujets développés devraient trouver des questionnaires de validation de connaissances. Enfin, une solution accessible et abordable de simulation d'exercices pratiques mériterait réflexion.

Cisco CCNA 200-301

L'examen Cisco CCNA 200-301[1] est disponible en anglais uniquement. Il se déroule sous surveillance dans un centre de test VUE après une inscription sur leur site vue.com et un paiement (de maximum 300 EUR) avec un bon de réduction (*voucher*) ou par carte de crédit.

Cet examen de niveau fondamental sur la théorie des réseaux évalue votre niveau avec un examen sur ordinateur en anglais constitué d'une centaine de questions théoriques et pratiques. Cet examen a une durée de 120 minutes. Il est interdit de revenir sur une question à laquelle on a déjà répondu. Le seuil de réussite est fixé entre 82,5% et 85%. Tout diplômé d'un premier cycle de l'enseignement supérieur en informatique devrait être en mesure de réussir cet examen dans un délai de trois mois. Tout qui voudrait entrer dans une carrière dans les réseaux ne perd pas son temps en passant cet examen. Certains prétendent même que c'est fortement recommandé.

Sujets et objectifs de l'examen Cisco CCNA 200-301

On trouve 53 objectifs dans six sujets[2] : Fondamentaux des Réseaux (20%), Accès au Réseau (20%), Connectivité IP (25%), Services IP (10%), Sécurité de base (15%), Automation et Programmabilité (10%).

On trouve aussi dix verbes dans les objectifs de la certification CCNA 200-301 qui correspondent à certaines compétences à valider :

1. "Expliquer" (6)
2. "Décrire" (15)
3. "Comparer" (6)
4. "Identifier" (1)
5. "Reconnaître" (1)
6. "Interpréter" (2)
7. "Déterminer" (1)
8. "Définir" (1)
9. "Configurer" (17)
10. "Vérifier" (1)

On peut considérer que seuls les objectifs qui demandent à "Configurer" et à "Vérifier" seraient purement pratiques. Toutefois, "Identifier", "Interpréter" et "Déterminer" pourraient aussi trouver leur application opérationnelle. Les autres objectifs comme "Expliquer", "Décrire", "Définir", "Reconnaître" seraient validés par des questions d'examen plus théoriques.

Les objectifs développés dans ce volume sont indiqués en gras.

1. La page officielle de la certification se trouve à cette adresse.
2. La page officielle des sujets et des objectifs du Cisco CCNA 200-301 se trouve à cette adresse.

1.0 Fondamentaux des Réseaux - 20%

- 1.1 Expliquer le rôle et la fonction des composants réseau
  - 1.1.a Routeurs
  - 1.1.b Commutateurs (switches) L2 et L3
  - 1.1.c Pare-feu NG (Next-generation firewalls) et IPS
  - 1.1.d Point d'accès (Access points)
  - 1.1.e Controlleurs (Cisco DNA Center et WLC)
  - 1.1.f Points terminaux (Endpoints)
  - 1.1.g Serveurs
- 1.2 Décrire les caractéristiques des architectures et topologies réseau
  - 1.2.a 2 tier
  - 1.2.b 3 tier
  - 1.2.c Spine-leaf
  - 1.2.d WAN
  - 1.2.e Small office/home office (SOHO)
  - 1.2.f On-premises et cloud
- 1.3 Comparer les interfaces physiques et les types de câble
  - 1.3.a Fibre monmode (Single-mode) et fibre multimode, cuivre
  - 1.3.b Connexions (Ethernet shared media et point-to-point)
  - 1.3.c Concepts sur PoE
- 1.4 Identifier les problèmes d'interface et de câbles (collisions, errors, mismatch duplex, et/ou speed)
- 1.5 Comparer TCP à UDP
- 1.6 Configurer et vérifier l'adressage et le sous-réseautage (subnetting) IPv4
- 1.7 Décrire la nécessité d'un adressage IPv4 privé
- 1.8 Configurer et vérifier l'adressage et les préfixes IPv6
- 1.9 Comparer les types d'adresses IPv6
  - 1.9.a Global unicast
  - 1.9.b Unique local
  - 1.9.c Link local
  - 1.9.d Anycast
  - 1.9.e Multicast
  - 1.9.f Modified EUI 64
- 1.10 Vérifier les paramètres IP des OS clients (Windows, Mac OS, Linux)
- 1.11 Décrire les principes des réseaux sans-fil
  - 1.11.a Nonoverlapping Wi-Fi channels
  - 1.11.b SSID
  - 1.11.c RF
  - 1.11.d Encryption
- 1.12 Expliquer les fondamentaux de la virtualisation (virtual machines)
- 1.13 Décrire les concepts de la commutation (switching)
  - 1.13.a MAC learning et aging
  - 1.13.b Frame switching
  - 1.13.c Frame flooding
  - 1.13.d MAC address table

© 2021 François-Emmanuel Goffinet

2.0 Accès au Réseau - 20%

- 2.1 Configurer et vérifier les VLANs (normal range) couvrant plusieurs switches
  - 2.1.a Access ports (data et voice)
  - 2.1.b Default VLAN
  - 2.1.c Connectivity
- 2.2 Configurer et vérifier la connectivité interswitch
  - 2.2.a Trunk ports
  - 2.2.b 802.1Q
  - 2.2.c Native VLAN
- 2.3 Configurer et vérifier les protocoles de découverte Layer 2 (Cisco Discovery Protocol et LLDP)
- 2.4 Configurer et vérifier (Layer 2/Layer 3) EtherChannel (LACP)
- 2.5 Décrire la nécessité et les operations de base de Rapid PVST+ Spanning Tree Protocol
  - 2.5.a Root port, root bridge (primary/secondary), et les autres noms de port
  - 2.5.b Port states (forwarding/blocking)
  - 2.5.c Avantages PortFast
- 2.6 Comparer les architectures Cisco Wireless Architectures et les modes des APs
- 2.7 Décrire les connexions physiques d'infrastructure des composants WLAN (AP,WLC, access/trunk ports, et LAG)
- 2.8 Décrire les connexions des accès de gestion des APs et du WLC (Telnet, SSH, HTTP,HTTPS, console, et TACACS+/RADIUS)
- 2.9 Configurer les composants d'un accès au LAN sans-fil pour la connectivité d'un client en utilisant un GUI seulement pour la création du WLAN, les paramètres de sécurité, les profiles QoS et des paramètres WLAN avancés

3.0 Connectivité IP - 25%

- 3.1 Interpréter les composants d'une table de routage
  - 3.1.a Routing protocol code
  - 3.1.b Prefix
  - 3.1.c Network mask
  - 3.1.d Next hop
  - 3.1.e Administrative distance
  - 3.1.f Metric
  - 3.1.g Gateway of last resort
- 3.2 Déterminer comment un routeur prend une décision de transfert par défaut
  - 3.2.a Longest match
  - 3.2.b Administrative distance
  - 3.2.c Routing protocol metric
- 3.3 Configurer et vérifier le routage statique IPv4 et IPv6
  - 3.3.a Default route
  - 3.3.b Network route

© 2021 François-Emmanuel Goffinet

  - 3.3.c Host route
  - 3.3.d Floating static

- 3.4 Configurer et vérifier single area OSPFv2
  - 3.4.a Neighbor adjacencies
  - 3.4.b Point-to-point
  - 3.4.c Broadcast (DR/BDR selection)
  - 3.4.d Router ID

- 3.5 Décrire le but des protocoles de redondance du premier saut (first hop redundancy protocol)

4.0 Services IP - 10%

- 4.1 Configurer et vérifier inside source NAT (static et pools)
- 4.2 Configurer et vérifier NTP dans le mode client et le mode server
- 4.3 Expliquer le rôle de DHCP et de DNS au sein du réseau
- 4.4 Expliquer la fonction de SNMP dans les opérations réseau
- 4.5 Décrire l'utilisation des fonctionnalités de syslog features en ce inclus les facilities et niveaux
- 4.6 Configurer et vérifier DHCP client et relay
- 4.7 Expliquer le forwarding per-hop behavior (PHB) pour QoS comme classification, marking, queuing, congestion, policing, shaping
- 4.8 Configurer les périphériques pour un accès distant avec SSH
- 4.9 Décrire les capacités la fonction de TFTP/FTP dans un réseau

5.0 Sécurité de base - 15%

- 5.1 Définir les concepts clé de la sécurité (menaces, vulnerabilités, exploits, et les techniques d'atténuation)
- 5.2 Décrire les éléments des programmes de sécurité (sensibilisation des utilisateurs, formation, le contrôle d'accès physique)
- 5.3 Configurer l'accès aux périphériques avec des mots de passe
- 5.4 Décrire les éléments des politiques de sécurité comme la gestion, la complexité, et les alternatives aux mots de passe (authentications multifacteur, par certificats, et biométriques)
- 5.5 Décrire les VPNs remote access et site-to-site
- 5.6 Configurer et vérifier les access control lists
- 5.7 Configurer les fonctionnalités de sécurité Layer 2 (DHCP snooping, dynamic ARP inspection, et port security)
- 5.8 Distinguer les concepts authentication, authorization, et accounting
- 5.9 Décrire les protocoles de sécurité sans-fil (WPA, WPA2, et WPA3)
- 5.10 Configurer un WLAN en utilisant WPA2 PSK avec un GUI

© 2021 François-Emmanuel Goffinet

6.0 Automation et Programmabilité - 10%

- 6.1 Expliquer comment l'automation impacte la gestion du réseau
- 6.2 Comparer les réseaux traditionnels avec le réseau basé contrôleur (controller-based)
- 6.3 Décrire les architectures basées contrôleur (controller-based) et software defined (overlay, underlay, et fabric)
  - 6.3.a Séparation du control plane et du data plane
  - 6.3.b APIs North-bound et south-bound
- 6.4 Comparer la gestion traditionnelle les périphériques campus avec une gestion des périphériques avec Cisco DNA Center
- 6.5 Décrire les caractéristiques des APIs de type REST (CRUD, verbes HTTP, et encodage des données)
- 6.6 Reconnaître les capacités des mécanismes de gestion des configuration comme Puppet, Chef, et Ansible
- 6.7 Interpréter des données encodées en JSON

© 2021 François-Emmanuel Goffinet

Introduction

Ce second volume du guide de préparation à la certification Cisco CCNA 200-301 est la deuxième étape dans votre projet de formation. Il couvre les objectifs de la certification sur des fondamentaux des réseaux mais surtout sur la connectivité IP et les services associés. Il porte essentiellement sur le routage ÌPv4/IPv6, les protocole de routage comme OSPF, RIP et EIGRP, les services IP comme le NAT, les protocoles DNS, DHCP, RA et DHCPv6.

L'ouvrage couvre les sujets suivants de la certification CCNA : Fondamentaux des Réseaux, Connectivité IP et Services IP (en partie).

Ce volume peut occuper une activité intellectuelle de 16 à 35 heures, voir plus.

L'objectif opérationnel de ce document est de mettre en place la connectivité IP dans un interréseau d'entreprise.

La première partie de ce volume de préapration au CCNA s'intéresse au routage IPv4/IPv6. Les routeurs sont au coeur du réseau Internet car ce sont eux qui interconnectent les points d'extrémités entre eux. Dans ce cinquième chapitre, on trouvera une introduction aux routeurs Cisco, on apprendra à lire une table de routage IPv4 et IPv6 d'un routeur et à distinguer les concepts de base du routage. Ensuite, on apprendra enfin à configurer, à vérifier et à diagnostiquer le routage statique en Cisco IOS.

Une seconde partie présente les services d'infrastructure qui permettent que cette connectivité IP soit "bien vécue" par l'utilisateur final. On entend ici par connectivité "bien vécue" la mise à disposition d'un service d'accès au réseau de qualité et évident pour quiconque. DNS, DHCP, NAT et les ACLs Cisco sont les principaux chapitres développés. On y trouvera aussi des compléments pour la gestion des adresses IPv6. Nous répondons à la question : comment implémente-t-on la connectivité Internet d'un réseau d'entreprise ?

Les trois dernières parties s'intéressent aux protocoles de routage intérieurs. On trouvera un chapitre sur un grand classique comme RIP (en version 1 et en version 2) comme protocole de routage à vecteur de distance de l'IETF. Un chapitre est consacré aux protocoles de routage intérieurs de l'IETF à état lien : OSPFv2 et OSPFv3. Enfin, un dernier chapitre expose le protocole à vecteur de distance optimisé par Cisco Systems EIGRP, récemment publié en RFC Informational. Alors que l'actuelle certification vérifie uniquement le sujet OSPFv2, il est recommandé de porter un regard sur l'ensemble des protocoles de routage intérieurs notamment sur EIGRP.

Première partie Routage et routeurs

Les routeurs sont au coeur du réseau Internet car ce sont eux qui interconnectent les points d'extrémités entre eux. Dans cette partie, on trouvera une introduction aux routeurs Cisco, on apprendra à lire une table de routage IPv4 et IPv6 d'un routeur et à distinguer les concepts de base du routage. Ensuite, on apprendra enfin à configurer, à vérifier et à diagnostiquer le routage statique en Cisco IOS.

1. Introduction aux routeurs Cisco

Dans ce chapitre, on tentera d'identifier et de décrire les composants matériels et logiciels des routeurs Cisco Systems.

Au préalable de la lecture de ce document il est conseillé d'avoir pris connaissance des chapitres du chapitre 2. Cisco IOS CLI.

1. Un routeur est un ordinateur

Un routeur est un ordinateur spécialisé dans l'envoi de paquets à travers le réseau de données.

Il est responsable de l'interconnexion des réseaux en sélectionnant le meilleur chemin pour qu'un paquet soit acheminé jusqu'à sa destination.

Il transfère les paquets qui ne lui sont pas spécifiquement destinés, par définition.

Les routeurs sont le centre du réseau en son coeur.

Un routeur a généralement (au minimum) deux connexions :

- une connexion WAN (vers un ISP/FAI)
- une connexion LAN

Seuls les routeurs sont capables de transférer les paquets d'une interface à une autre.

Le routeur transfère le trafic en fonction de l'adresse IP destination trouvée dans le paquet ; précisément, il compare cette destination à une entrée de sa table de routage qui indique une interface de sortie qui emprunte le meilleur chemin.

Le routeur limite les domaines de *Broadcast* / *Multicast* sur chacune de ses interfaces.

En IPv6, le routeur configure le réseau grâce à des *Router Advertisements* (ICMPv6 134) envoyés régulièrement.

Les routeurs arrivent à s'échanger entre eux des informations concernant les différentes destinations (des réseaux à joindre) grâce à des protocoles de routage.

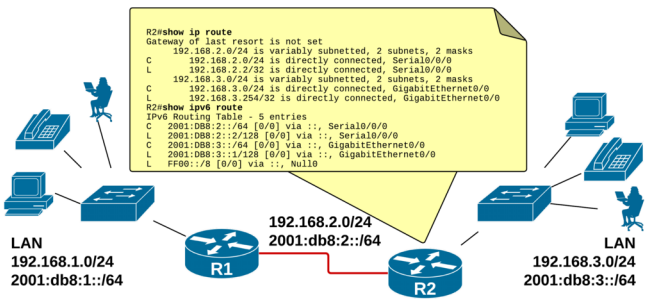


Table de routage par défaut sur R2

Table de routage par défaut du routeur R2

2. Composants d'un routeur Cisco : Logiciel

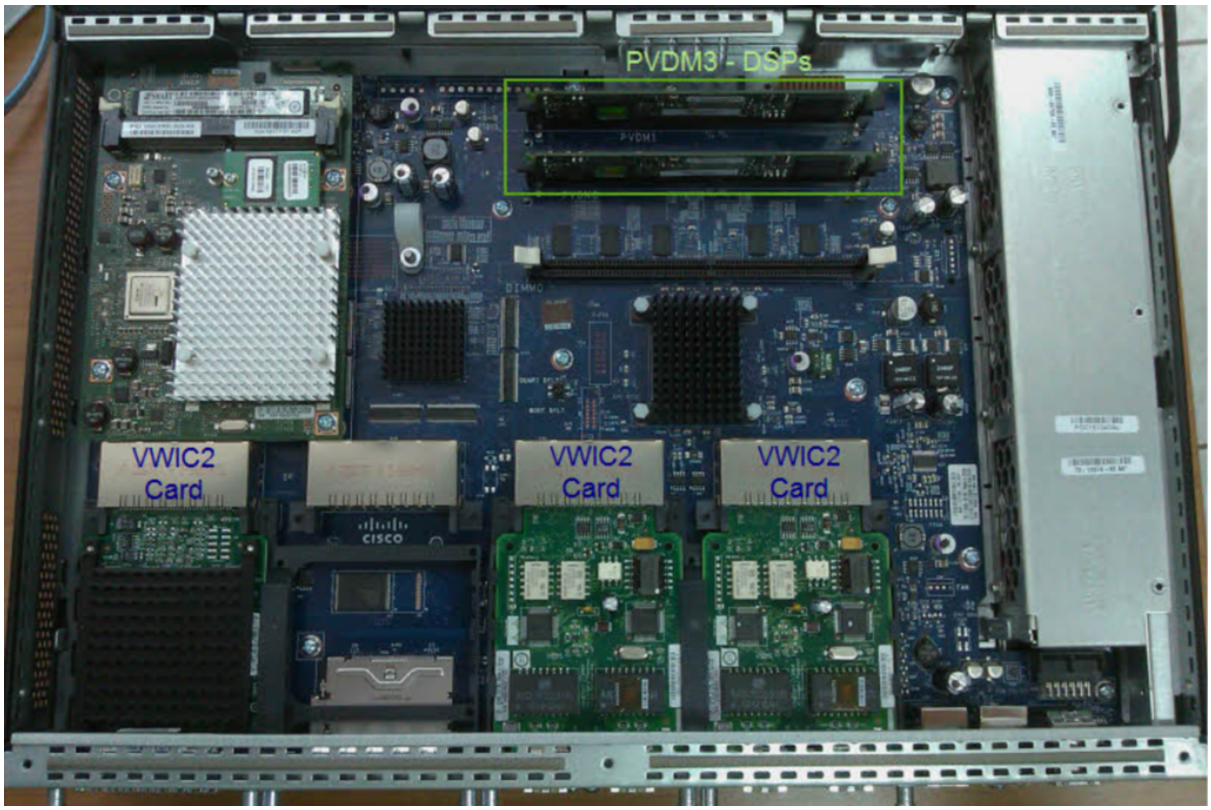
Un routeur Cisco fonctionne grâce à des logiciels :

- une sorte de BIOS : ROM Monitor Mode
- un système d'exploitation : Cisco IOS (*Internetwork Operating System*)

3. Composants d'un routeur Cisco : Matériel

Sur le plan matériel, les routeurs Cisco sont principalement composés de :

- CPU, RAM, NVRAM, Flash, ROM
- Interfaces



A l'intérieur d'un C2600

- Aujourd'hui, Cisco Systems propose des routeurs matériels et logiciels basés sur des plateformes Intel qui ne disposent pas de "ROM Monitor Mode".
- IOS XR est une nouvelle version d'IOS entièrement réécrite qui profite d'une architecture Microkernel (QNX) performante (Multitâche préemptif et protection mémoire).

4. Mémoires

Mémoire	exemple	commande
RAM	Fichier de configuration courante	`show running-config`
RAM	Tables de routage	`show ip [ipv6] route`
RAM	Cache ARP Cache ND	`show arp` / `show ipv6 neighbors`
RAM	Mémoire de travail	`show memory`
Flash	Emplacement de l'image IOS	`show flash`
Flash	Fichiers de configuration supplémentaires	`show flash`
Flash	Images supplémentaires de l'IOS	`show flash`
NVRAM	Fichier de configuration de démarrage	`show startup-config`
NVRAM	Registre de configuration	`show version`
ROM	POST, Bootstrap, Trouve et charge l'IOS, la configuration initiale	Mode ROM Monitor ou RXBoot

© 2021 François-Emmanuel Goffinet

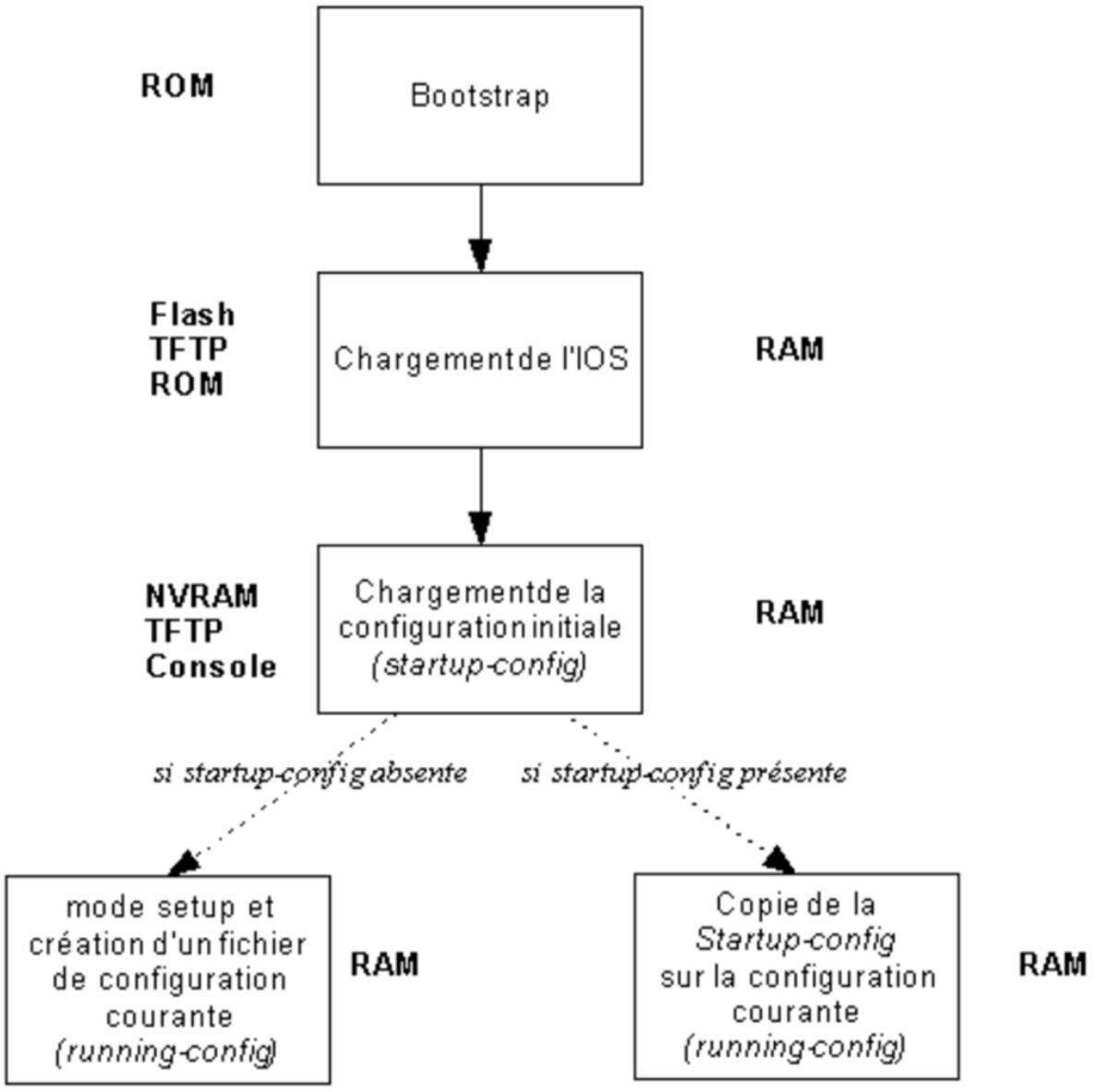
5. Démarrage d'un routeur

Pour redémarrer un routeur Cisco :

```
Router#reload
```

Lors de son redémarrage le routeur passe différentes étapes :

1. Test matériel
    - Power-On Self Test (POST)
    - Exécution bootstrap loader
    - Localisation et chargement de l'IOS
    - Localisation et chargement du fichier de configuration initiale (`startup-config`)
    - Ou mode "setup" et configuration courante vierge



Démarrage d'un routeur Cisco

© 2021 François-Emmanuel Goffinet

5.1. Vérification du démarrage

La commande `show version` permet de connaître :

- Le modèle exact de la plateforme
- Le nom de l'image et la version de l'IOS
- La version du Bootstrap dans la ROM
- Le nom du fichier d'image et son emplacement
- Le nombre et le type d'interfaces
- La quantité de RAM
- La quantité de NVRAM
- La quantité de Flash
- La licence installée
- La valeur du registre de configuration

5.2.Commande `show version`

```
R2#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 23-Feb-11 14:19 by pt_team
ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco1941 uptime is 1 hours, 13 minutes, 25 seconds
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.151-1.M4.bin"
Last reload type: Normal Reload
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)
License Info:
License UDI:
------------------------------------------------
Device#   PID                 SN
------------------------------------------------
*0        CISCO1941/K9        FTX152420YE
Technology Package License Information for Module:'c1900'
-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      None          None          None
data          None          None          None

Configuration register is 0x2102
```

© 2021 François-Emmanuel Goffinet

6. Interfaces d’un routeur

Le *plan data* est constitué d’interfaces qui sont des portes physiques qui activent la transmission de données. On y connecte des câbles avec des connecteurs.

Chaque interface connecte un réseau IP différent.

Types d’interfaces :

- Wi-Fi
- Ethernet
- Serial
- DSL
- ISDN
- Cable (DOCSIS)
- …

6.1. Interfaces LAN et WAN

On trouve deux catégories d’interfaces :

Interface LAN :

- Se connecte au réseau LAN
- Dispose d’une adresse MAC
- Peut se voir assigné une adresse IPv4 et des adresses IPv6
- Format RJ-45 jack

Panneau avant d’un C2921

Interface WAN :

- Utilisée pour offrir une connectivité extérieure au LAN
- Selon la technologie WAN, une adresse de couche 2 peut être utilisée
- Supporte IPv4/IPv6

© 2021 François-Emmanuel Goffinet

Modules WIC-2T avec interfaces Smart Serial

6.2. Commandes de vérification des interfaces

Couche	Commande	Description
L1	`show controllers S0/0`	-
L1/L2	`show interface G0/0`	-
L1/L2/L3	`show ip interface brief`, `show ipv6 interface brief`	-
L3	`show ip interface`, `show ipv6 interface`	-

6.3. “Status” et “Protocol” des interfaces

```
Router#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            11.1.2.1        YES manual up                    up
Serial0/0                  11.1.3.1        YES manual up                    down
FastEthernet0/1            unassigned      YES unset  down                  down
Serial0/1                  unassigned      YES unset  administratively down down
Loopback0                  8.8.8.8         YES manual up                    up
```

La colonne “Status” dans les sorties fournit une information de couche physique L1. Elle peut connaître trois états :

Etat “Status”	Description	Remède
`administratively down`	Administrativement désactivée	`no shutdown`
`down`	Activée mais ne reçoit aucun signal	Vérifier les connecteurs et câbles
`up`	fonctionnel sur le plan physique	-

La colonne “Protocol” indique si le protocole L2 (Ethernet, PPP, HDLC, …) est opérationnel. Elle connaît deux états :

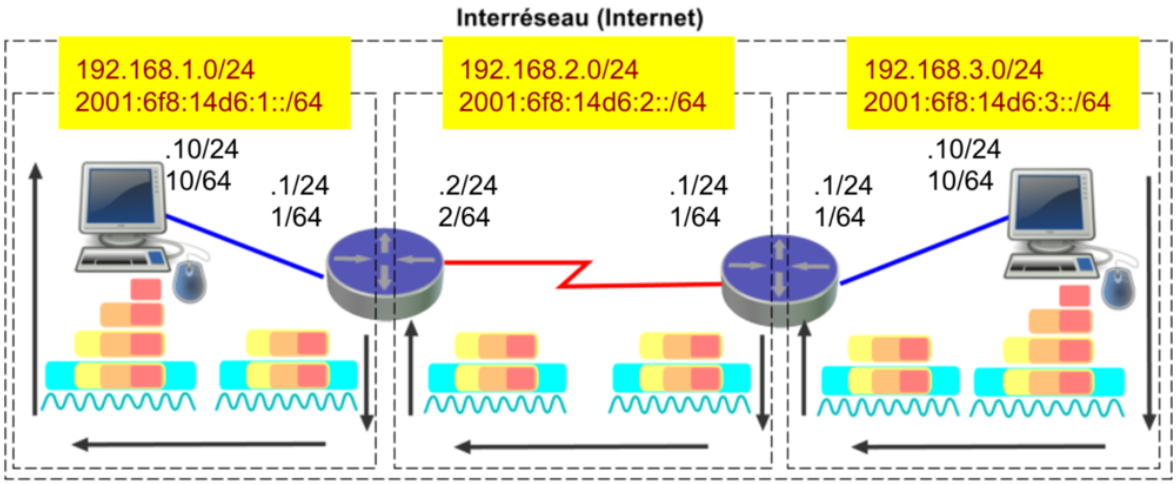
© 2021 François-Emmanuel Goffinet

Etat “Protocol”	Description	Remède
down	problème d’encapsulation, de chiffrement, d’authentification	vérifier les paramètres d’encapsulation et de configuration des utilisateurs et des mots de passe de la liaison
up	fonctionnel sur le plan de la couche 2	-

7. Domaines IP

Deux noeuds (hôtes, interfaces, cartes réseau, PC, smartphone, etc.) doivent appartenir au même réseau, au même domaine IP, pour communiquer directement entre eux.

Quand les noeuds sont distants, ils ont besoin de livrer leur trafic à une passerelle, soit un routeur.



Ré-encapsulation L2 au passage de chaque routeur

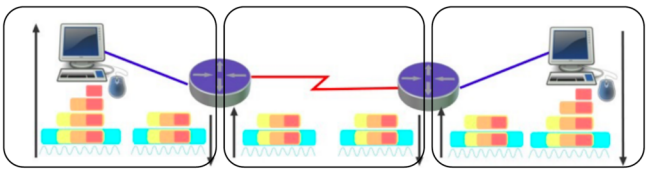
Les routeurs utilisent l’adresse IP de destination des paquets pour prendre la décision de transfert :

- Le chemin pris par un paquet est déterminé après consultation de table de routage
- Ensuite le routeur détermine le meilleur chemin
- Le paquet est encapsulé en trame, et puis la trame en signal binaire

Les routeurs couvrent les couches 1, 2 et 3 :

- Les routeurs reçoivent du signal binaire
- Les bits sont décodés et passés à la couche 2
- Le routeur dés-encapsule la trame
- Le paquet passe à la couche 3
- Une décision de routage est prise en fonction de l’adresse IP de destination
- Le paquet est ré-encapsulé au niveau L2 et il est placé sur l’interface de sortie et puis sur le support physique.

© 2021 François-Emmanuel Goffinet



Ré-encapsulation L2 au passage de chaque routeur

8. Table de routage

Chaque machine de l'inter-réseau dispose de sa table de routage, soit pour chaque entrée :

- Un réseau de destination et son masque
- une interface de sortie et une passerelle

Commandes :

- Sous Windows : `route print`, `netsh interface ip show route`
- Sous GNU/Linux/MacOSX : `netstat -r`, `ip route`
- Sous Cisco IOS : `show ip route`

Cette table sert à encapsuler le paquet (L3) sur la liaison (L2) la plus proche de la destination.

La passerelle par défaut est configurée sur les hôtes de manière **statique**, **dynamique (IPv4)** ou **automatique (IPv6)**

9. Logiciel de routage

Le fait qu'un ordinateur dispose de plusieurs interfaces connectées à différents réseaux n'en fait pas nécessairement un routeur.

Faut-il qu'un logiciel se charge de cette tâche.

Sur une machine Linux, cette activation est triviale (`net.ipv4.ip_forward`).

Aujourd'hui, Cisco a porté ses plateformes matérielles en machines virtuelles IOS : CSR1000v, NX-OS, vIOS, … mais à la concurrence aussi. Le Marketplace Appliance de GNS3 donne une idée du développement attendu des routeurs en machine virtuelle dans les *data centers* et les solutions en nuage (cloud).

Sur un routeur Cisco, le routage IPv4 est activé par défaut. Par contre, il est désactivé par défaut en IPv6.

10. Routage IPv6

Le routage IPv6 est désactivé par défaut en Cisco IOS. Pour l'activer en configuration globale :

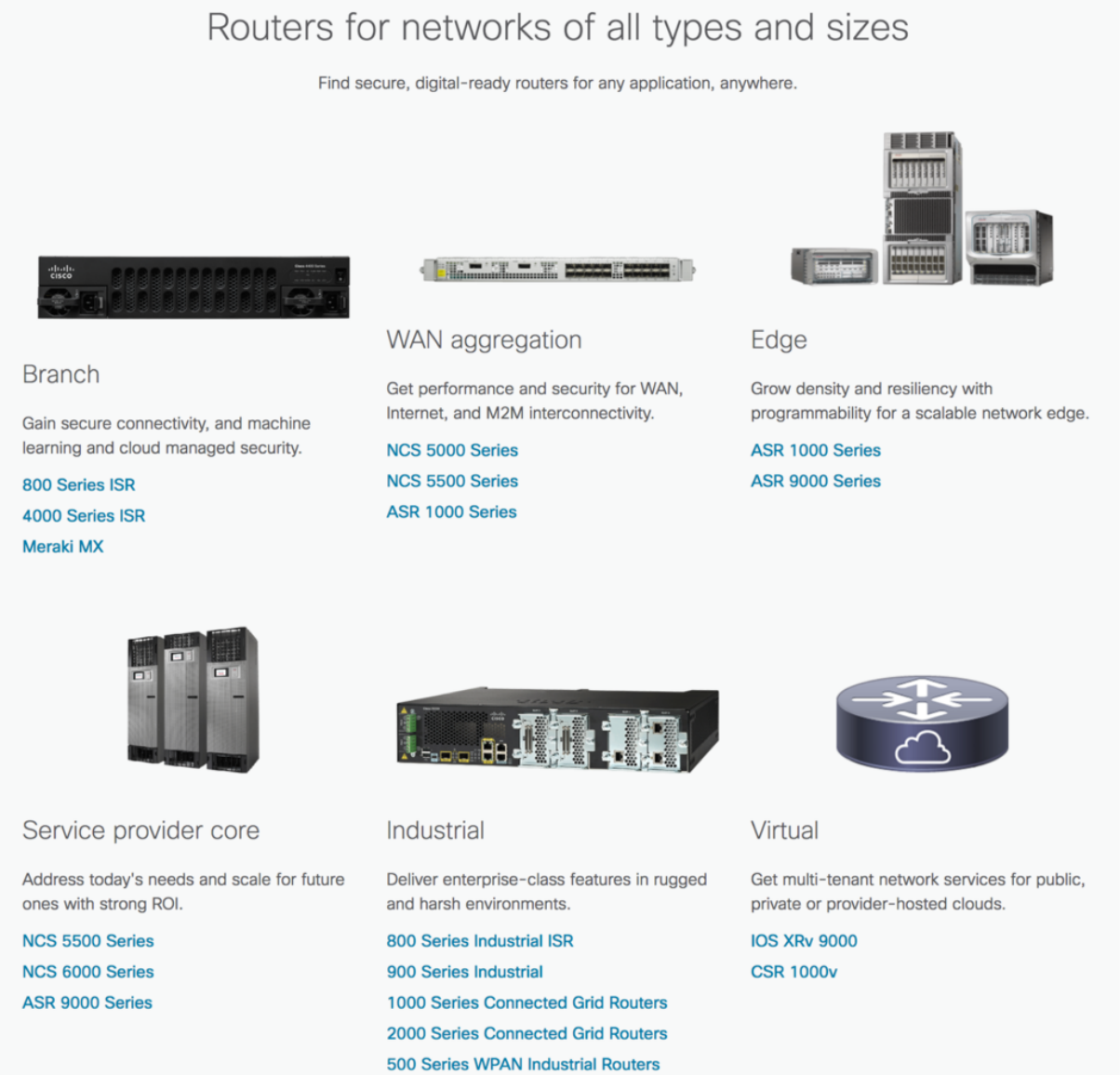
```
#configure terminal
(config)#ipv6 unicast-routing
```

© 2021 François-Emmanuel Goffinet

11. Modèles de routeurs

On peut s'informer sur les différentes catégories de routeurs chez différents fabricants :

- Cisco Systems
- Juniper Networks
- HP
- et bien d'autres



Catalogue de modèles de routeurs Cisco

12. Formes de routeur

- Routeur grand public

© 2021 François-Emmanuel Goffinet

- Routeurs d'accès
- Routeur à services intégrés
- Pare-feux NG
- Routeur de datacenter
- Routeur virtuel

© 2021 François-Emmanuel Goffinet

Deuxième partie Services d'infrastructure

Si l'on veut se faire une bonne idée des opérations qui se déroulent dans un réseau, notamment en bordure sur les routeurs mais aussi dans le LAN, il faut se s'intéresser à d'autres domaines que le routage ou la commutation. Un série de services peuvent s'implémenter sur un routeur Cisco comme le NAT/PAT (Network Address Translation / Port Address Translation), mais pas obligatoirement. On en trouvera d'autres, indispensables à une connectivité "bien vécue" comme DNS, DHCP ou DHCPv6. Cette partie aborde aussi les concepts de configuration des ACLs aui sont des listes de filtrage IP en Cisco IOS. Il s'agit toujours ici de configurations simples et fondamentales.

Sans NAT, l'Internet que nous connaissons aujourd'hui n'aurait jamais existé et notre expérience de l'Internet se vivrait depuis longtemps en IPv6. L'appréciation que l'on peut faire de la technologie dépend du point de vue et surtout de son expérimentation personnelle. Quoi qu'il en soit, il a permis le développement rapide de l'Internet IPv4 pourtant extrêmement contraint.

Que feraient les administrateurs de réseaux locaux sans le service DHCP d'attribution dynamique d'adresses IPv4 ? Qu'en est-il en IPv6 ? Il n'y aucune raison de ne pas profiter des anciennes et nouvelles fonctionnalités du nouveau protocole DHCPv6. A cette occasion, un article détaille les mécanismes d'auto-configuration automatique en IPv6.

Autant nos machines peuvent se contenter d'IPv4 ou d'IPv6, comme dans les topologies de lab Cisco, autant dans la réalité les utilisateurs et les solutions d'échanges entre les machines ne peuvent plus se passer de DNS. Pour un utilisateur final, accéder à son réseau social favori avec une expérience positive sans résolution de noms est impossible. Il en va de même dans les solutions d'infrastructure, dans les centres de données, etc. Beaucoup de retours d'expérience malheureuse sur le réseau relève de la qualité du service DNS utilisé. DNS est certainement aujourd'hui un pré-requis dans tous les réseaux.

Avant de proposer des exercices pratiques supplémentaires avec des adressages et des connexions différentes qui implémentent ces solutions, on trouvera un exposé sur les ACLs Cisco, sujet central et fondamental des certifications Cisco.

2. Network Address Translation (NAT44)

Dans ce chapitre on parlera du Inside Source NAT44 (Statique, Pool et PAT) et de son implémentation en Cisco IOS.

1. Introduction

Le NAT, pour "Network Address Translation", Traduction d'Adresses Réseau, a été proposé en 1994 sous le RFC 1631 comme solution à court terme face au manque d'adresses IPv4. Son objectif principal était de permettre aux adresses IP d'être partagées par un grand nombre de périphériques réseau. Envisagé comme un palliatif au manque d'adresses IPv4, il montre aujourd'hui ses limites à la croissance de l'Internet. Ce que l'on appelle "IP Masquerading", pour masquage d'adresses IP est synonyme du NAT dans le jargon. On parlera ici uniquement de l'implétentation du NAT en Cisco IOS.

2. Définition

Le NAT est défini dans le RFC 3022. Le NAT permet d'utiliser des adresses n'ayant pas de signification globale (par exemple des adresses privées définies dans le RFC 1918, non globalement routables) pour les connecter à travers l'Internet en traduisant celles-ci en adresses globales routables. Le NAT permet aussi de fournir une solution de re-numérotation pour les organisations qui changent de fournisseur de service par exemple.

3. Portée

On peut utiliser le NAT dans différents cas :

- On dispose d'une multitude d'hôtes adressés de manière privée et le routeur externe dispose d'une seule ou de quelques adresses IPv4 globales (publiques). Le NAT est configuré sur un routeur en bordure d'un réseau d'extrémité (un LAN), étant identifié comme étant le côté interne ("inside"), qui connecte un réseau public comme l'Internet, identifié comme étant le côté externe ("outside"). Le NAT traduit les adresses locales internes en une adresse globale unique avant d'envoyer les paquets vers le réseau externe.
- On doit changer des adresses internes. Au lieu de les changer, on les traduit par du NAT.
- On veut rendre accessible des hôtes qui sont localement et globalement dans le même adressage, autrement dit on permet une connectivité d'adresses qui se chevauchent ("overlapping") de part et d'autre du routeur NAT.
- On peut utiliser également le NAT pour distribuer la charge TCP vers un hôte virtuel qui répond à la place de plusieurs serveurs réels selon un principe de type round-robin.
- Il *contribue* à améliorer la sécurité des réseaux internes en les rendant opaques aux autres organisations, mais il n'est jamais une mesure de filtrage de sécurité.

4. Limites

- Le NAT contredit le principe fondamental d'IP qui demande une communication de bout en bout (les stations d'extrémité établissent et gèrent elles-mêmes leur communication). Le NAT pose donc des problèmes dans l'établissement de communications utilisant certains protocoles de sécurité assurant une authentification et un chiffrement (IPSEC), des applications peer-to-peer (VOIP) et autres tels que FTP.

- En matière de sécurité, il n'est jamais qu'une option qui ne remplace pas un filtrage IP pertinent (pare-feu, *firewall*).
- Par ailleurs, son utilisation répandue rend opaque l'étendue réelle de l'Internet IPv4. Rappelons que ce principe a été mis en place pour répondre de manière temporaire au manque d'adresses IPv4.

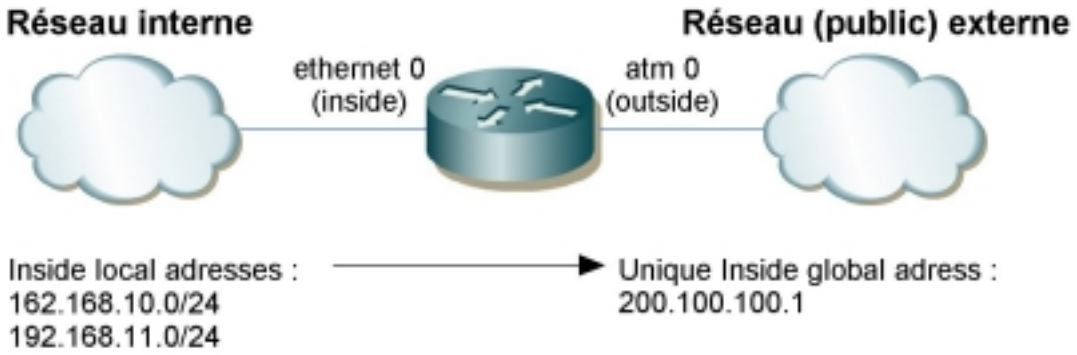
5. Terminologie Cisco

On fera la distinction entre interne ("inside") et externe ("outside"). Les adresses internes sont celles qui sont maîtrisées par l'administrateur du réseau d'extrémité. Les adresses externes sont celles dont on n'a pas la maîtrise et qui font partie d'un réseau public tel que l'Internet.

On fera aussi la distinction entre adresses locales et globales. Les adresses locales sont celles qui ne sont pas nécessairement des adresses légitimes et les adresses globales sont celles qui sont routables, qui ont une signification à portée globale.

Concrètement, on trouvera dans les tables NAT jusqu'à quatre types d'adresses :

- **Inside local address** - L'adresse IP assignée à un hôte à l'intérieur d'un réseau d'extrémité. Il s'agit probablement d'une adresse privée, non routable globalement.
- **Inside global address** - La ou les adresses IP publiques qui représentent les adresses IP locales internes, les adresses IP routables du routeur NAT.
- **Outside local address** - L'adresse IP d'un hôte telle qu'elle apparaît aux hôtes d'un réseau interne. Il ne s'agit pas nécessairement d'une adresse légitime routable.
- **Outside global address** - L'adresse IP réelle routable d'un hôte qui se situe à l'extérieur du réseau du routeur NAT.



Inside local address et Inside global address

```
#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
udp 122.168.122.106:59856 192.168.1.100:59856 194.57.169.1:123 194.57.169.1:123
udp 122.168.122.106:43050 192.168.1.101:43050 195.154.105.147:123 195.154.105.147:123
tcp 122.168.122.106:43516 192.168.1.101:43516 216.58.204.132:443 216.58.204.132:443
```

Dans cette sortie, la colonne `Inside local` correspond à l'adresse et au port source original qui est traduit dans une entrée correspondante `122.168.122.106:59856`. L'adresse `Inside global` est l'adresse de traduction que la destination va recevoir. L'adresse de destination n'est traduite dans aucune direction, soit la colonne `Outside local` et la colonne `Outside global` sont équivalentes.

© 2021 François-Emmanuel Goffinet

6. Traduction d'adresses IP

On trouvera deux grands types de traduction d'adresses internes :

- **Les traductions statiques** : une correspondance de type un à un entre une adresse IPv4 locale interne et une adresse IPv4 globale interne. Elles sont utiles lorsqu'un hôte interne doit être accessible de l'extérieur. On peut également établir des correspondances de ports TCP/UDP pour réaliser ce que l'on appelle communément le transfert de ports.
- **Les traductions dynamiques** : une correspondance de plusieurs-à-plusieurs entre un ensemble d'adresses IP locales (définies par une ACL) et un groupe d'adresses IP globales (définies par un "pool", une plage d'adresses).

On trouvera deux variantes aux traductions dynamiques :

- **Overloading** : la correspondance de plusieurs adresses IP locales internes (définies par une ACL) et une adresse IP globale interne (définie par le nom d'une interface) ou plusieurs adresses IP globales internes (définies par un "pool") en utilisant comme critère distinctif du trafic les ports TCP/UDP. Cette solution est aussi appelée PAT ("Port Address Translation"), "single-address NAT" ou encore "port-level multiplexed NAT".
- **Overlapping** : la correspondance entre adresses IP internes qui se chevauchent avec des adresses externes et inversement.

7. Méthodes de configuration de traduction d'adresses IP internes

Au préalable, il est utile d'être informé sur les liste d'accès (ACLs) Cisco IOS.

7.1. Traduction statique

Définition du NAT

```
(config)#ip nat inside source static <local_inside_ip> <global_inside_ip>
```

Définition des interfaces Inside/Outside

```
(config)#interface <type> <number>
(config-if)#ip nat inside
(config)# interface <type> <number>
(config-if)#ip nat outside
```

7.2. Traduction dynamique simple

Adresses locales soumises au NAT

```
(config)#access-list <access-list_number> permit <source_ip> <wildcard_mask>
```

Pool d'adresses globales

© 2021 François-Emmanuel Goffinet

```
(config)#ip nat pool <name> <start_ip> <end_ip>
```

Definition du NAT

```
(config)#ip nat inside source list <access-list_number> pool <name>
```

Définition des interfaces Inside/Outside

```
(config)#interface <type> <number>
(config-if)#ip nat inside
(config)# interface <type> <number>
(config-if)#ip nat outside
```

7.3. Traduction dynamique overload (PAT) avec une seule IP globale

Adresses locales soumises au NAT

```
(config)#access-list <access-list_number> permit <source_ip> <wildcard_mask>
```

Definition du NAT

```
(config)#ip nat inside source list <access-list_number> interface <type> <number> overload
```

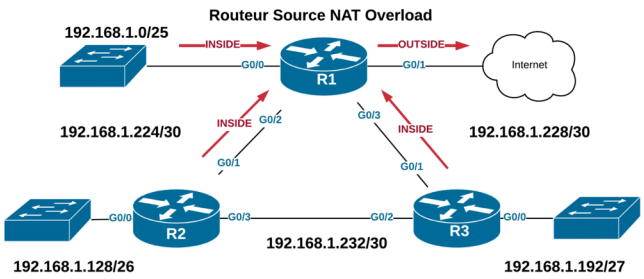
Définition des interfaces Inside/Outside

```
(config)#interface <type> <number>
(config-if)#ip nat inside
(config)# interface <type> <number>
(config-if)#ip nat outside
```

Diagnostic

```
#clear ip nat translation *
#show ip nat translations [verbose]
#show ip nat statistics
#debug ip nat
```

8. Mise en place du Source NAT overload



Mise en place du Source NAT overload

À partir d'une topologie représentative telle que celle-ci, on configure le Source NAT overload (PAT) sur R1 qui connecte l'Internet.

© 2021 François-Emmanuel Goffinet

```
(config)#interface g0/1
(config-if)#ip address dhcp
(config-if)#no shutdown
```

En premier lieu, la procédure consiste à identifier les paquets dont l'adresse IPv4 source correspond à une adresse `192.168.1` par une ACL. En configuration globale sur R1 :

```
(config)#access-list 1 permit 192.168.1.0 0.0.0.255
```

Ensuite, une règle NAT traduira l'adresse IPv4 source correspondant à l'ACL définie précédemment par l'adresse IPv4 de l'interface externe G0/1.

```
(config)#ip nat inside source list 1 interface g0/1 overload
```

Enfin, il faut indiquer chaque interface qui choisira le trafic à traduire, ici G0/2, G0/3 et G0/0 (`inside`) et le côté des destinations qui pourraient être traduites (`outside`).

```
(config)#interface g0/0
(config-if)#ip nat inside
(config-if)#interface g0/2
(config-if)#ip nat inside
(config-if)#interface g0/3
(config-if)#ip nat inside
(config-if)#interface g0/1
(config-if)#ip nat outside
```

9. Diagnostic NAT

On retiendra les commandes suivantes :

- `show running-config | include nat`
- `show access-list`
- `show ip nat translations`
- `show ip nat statistics`
- ...

9.1. Vérification de la configuration

```
gateway#show running-config | include nat
 ip nat inside
 ip nat outside
ip nat inside source list lan interface GigabitEthernet0/1 overload


gateway#show access-list lan
Standard IP access list lan
    10 permit 192.168.1.0, wildcard bits 0.0.0.255 (41 matches)
```

9.2. Vérification des traductions

C'est la commande `show ip nat translations` qui offre la table de traduction.

© 2021 François-Emmanuel Goffinet

```
gateway#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
udp 192.168.122.106:59856 192.168.1.100:59856 194.57.169.1:123 194.57.169.1:123
udp 192.168.122.106:38009 192.168.1.101:38009 194.57.169.1:123 194.57.169.1:123
udp 192.168.122.106:39792 192.168.1.101:39792 80.74.64.1:123 80.74.64.1:123
udp 192.168.122.106:40591 192.168.1.101:40591 178.33.123.180:123 178.33.123.180:123
udp 192.168.122.106:40824 192.168.1.101:40824 194.57.169.1:123 194.57.169.1:123
udp 192.168.122.106:41218 192.168.1.101:41218 195.154.105.147:123 195.154.105.147:123
udp 192.168.122.106:41499 192.168.1.101:41499 80.74.64.1:123 80.74.64.1:123
udp 192.168.122.106:43050 192.168.1.101:43050 195.154.105.147:123 195.154.105.147:123
tcp 192.168.122.106:43516 192.168.1.101:43516 216.58.204.132:443 216.58.204.132:443
udp 192.168.122.106:44933 192.168.1.101:44933 178.33.123.180:123 178.33.123.180:123
udp 192.168.122.106:46438 192.168.1.101:46438 80.74.64.1:123 80.74.64.1:123
udp 192.168.122.106:49243 192.168.1.101:49243 195.154.105.147:123 195.154.105.147:123
udp 192.168.122.106:51454 192.168.1.101:51454 195.154.105.147:123 195.154.105.147:123
udp 192.168.122.106:52567 192.168.1.101:52567 178.33.123.180:123 178.33.123.180:123
```

9.3. Statistiques NAT

La commande `show ip nat statistics` offre les statistiques du service de traduction.

```
gateway#show ip nat statistics
Total active translations: 41 (0 static, 41 dynamic; 41 extended)
Peak translations: 41, occurred 00:00:35 ago
Outside interfaces:
  GigabitEthernet0/1
Inside interfaces:
  GigabitEthernet0/0
Hits: 80  Misses: 0
CEF Translated packets: 80, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list lan interface GigabitEthernet0/1 refcount 41

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

9.4. Déboggage NAT en Cisco IOS

La commande `debug ip nat` peut être utilisée simplement ou avec un paramètre spécifique.

```
gateway#debug ip nat ?
  <1-99>      Access list
  detailed    NAT detailed events
  error       NAT error events
  fragment    NAT fragment events
  generic     NAT generic ALG handler events
  h323        NAT H.323 events
  ipsec       NAT IPSec events
  multipart   NAT Multipart support events
  nvi         NVI events
  piggyback   NAT Piggyback support events
```

© 2021 François-Emmanuel Goffinet

```
port         NAT PORT events
pptp         NAT PPTP events
redundancy   NAT HA redundancy
route        NAT Static route events
sbc          NAT SIP Session Border Controller events
sip          NAT SIP events
skinny       NAT skinny events
tcp-alg      NAT-ALG segmentation using common TCP Proxy
test         TEST Code event
vrf          NAT VRF events
wlan-nat     WLAN NAT events
<cr>
```

10. Lectures et références

- Anatomy : A Look Inside Network Address Translators, par Geoff Huston, APNIC, IPJ, Volume 7, Number 3, p. 2, September 2004.

© 2021 François-Emmanuel Goffinet

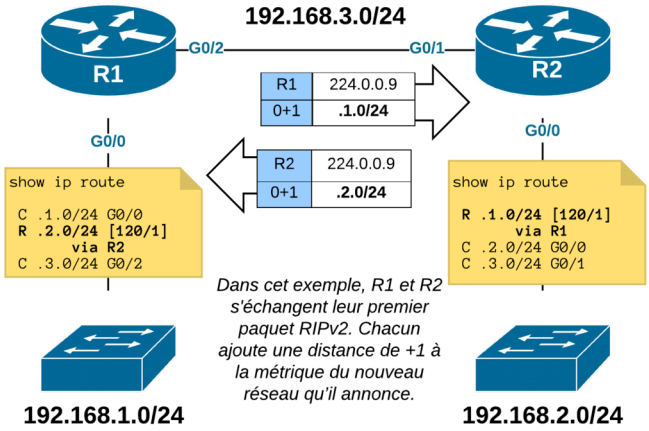
Troisième partie Routage RIP

Bien que le protocole de routage RIP ait été retiré des objectifs de l'examen CCNA et qu'il n'est plus conseillé de le déployer dans les nouvelles infrastructures, il reste un grand classique. En effet, il s'agit d'un standard IETF qui en met en oeuvre le principe du routage à vecteur de distance. Cette partie propose d'étudier les protocoles de routage RIPv1 et RIPv2.

3. Lab routage RIPv2 simple

Cet exercice reprend la topologie de deux routeurs interconnectés entre eux (R1 et R2) connectent chacun un LAN adressé en IPv4 et en IPv6. L'exercice consiste à implémenter le routage dynamique RIPv2, à le configurer et à le dépanner. On invitera le lecteur à jouer avec la distance administrative des routes statiques et à réfléchir aux configurations assez simples qui sont proposées.

1. Topologie



Topologie : routage RIPv2 simple

2. Configuration des interfaces sur R1

```
hostname R1
!
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 no shutdown
!
interface GigabitEthernet0/2
 ip address 192.168.3.1 255.255.255.0
 no shutdown
!
ip dhcp pool LAN
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
!
end
```

3. Configuration des interfaces sur R2

```
hostname R2
!
interface GigabitEthernet0/0
 ip address 192.168.2.1 255.255.255.0
 no shutdown
!
interface GigabitEthernet0/1
 ip address 192.168.3.2 255.255.255.0
 no shutdown
!
ip dhcp pool LAN
 network 192.168.2.0 255.255.255.0
 default-router 192.168.2.1
!
end
```

4. Vérification des interfaces

Sur R1 :

```
R1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         192.168.1.1     YES NVRAM  up                    up
GigabitEthernet0/1         unassigned      YES NVRAM  administratively down down
GigabitEthernet0/2         192.168.3.1     YES NVRAM  up                    up
GigabitEthernet0/3         unassigned      YES NVRAM  administratively down down
```

Sur R2 :

```
R2#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         192.168.2.1     YES NVRAM  up                    up
GigabitEthernet0/1         192.168.3.2     YES NVRAM  up                    up
GigabitEthernet0/2         unassigned      YES NVRAM  administratively down down
GigabitEthernet0/3         unassigned      YES NVRAM  administratively down down
```

Test de connectivité sur le voisinage :

```
R1#ping 192.168.3.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/7 ms
```

5. Activation du routage RIPv2

Respectivement, sur chaque routeur :

- activation la version 2
- l'interface LAN est passive
- déclaration des réseaux directement connectés

Sur R1 :

© 2021 François-Emmanuel Goffinet

```
router rip
 version 2
 passive-interface GigabitEthernet0/0
 network 192.168.1.0
 network 192.168.3.0
```

Sur R2 :

```
router rip
 version 2
 passive-interface GigabitEthernet0/0
 network 192.168.2.0
 network 192.168.3.0
```

6. Vérification de la configuration RIPv2

Sur R1 :

```
R1#show ip protocols | begin rip
Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 27 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: rip
  Default version control: send version 2, receive version 2
    Interface             Send  Recv  Triggered RIP  Key-chain
    GigabitEthernet0/2    2     2
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    192.168.1.0
    192.168.3.0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.3.2          120      00:00:27
  Distance: (default is 120)
```

Sur R2 :

```
R2#show ip protocols | begin rip
Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 18 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: rip
  Default version control: send version 2, receive version 2
    Interface             Send  Recv  Triggered RIP  Key-chain
    GigabitEthernet0/1    2     2
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
```

© 2021 François-Emmanuel Goffinet

```
    192.168.2.0
    192.168.3.0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.3.1          120      00:00:01
  Distance: (default is 120)
```

7. Vérification de la table de routage

Sur R1 :

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/0
L        192.168.1.1/32 is directly connected, GigabitEthernet0/0
R     192.168.2.0/24 [120/1] via 192.168.3.2, 00:00:18, GigabitEthernet0/2
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, GigabitEthernet0/2
L        192.168.3.1/32 is directly connected, GigabitEthernet0/2
```

Sur R2 :

```
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

R     192.168.1.0/24 [120/1] via 192.168.3.1, 00:00:16, GigabitEthernet0/1
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, GigabitEthernet0/0
L        192.168.2.1/32 is directly connected, GigabitEthernet0/0
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, GigabitEthernet0/1
L        192.168.3.2/32 is directly connected, GigabitEthernet0/1
```

© 2021 François-Emmanuel Goffinet

8. Vérification de la base de donnée RIP

Sur R2 :

```
R2#show ip rip database
192.168.1.0/24    auto-summary
192.168.1.0/24
    [1] via 192.168.3.1, 00:00:04, GigabitEthernet0/1
192.168.2.0/24    auto-summary
192.168.2.0/24    directly connected, GigabitEthernet0/0
192.168.3.0/24    auto-summary
192.168.3.0/24    directly connected, GigabitEthernet0/1
```

9. Debug RIP

En production, on redigera les logs ailleurs que dans la console.

```
R2#debug ip rip ?
  bfd       RIP BFD Events
  database  RIP database events
  events    RIP protocol events
  trigger   RIP trigger extension
  <cr>


R2#debug ip rip
RIP protocol debugging is on

*Oct 22 13:48:15.686: RIP: received v2 update from 192.168.3.1 on GigabitEthernet0/1
*Oct 22 13:48:15.686:      192.168.1.0/24 via 0.0.0.0 in 1 hops
*Oct 22 13:48:39.979: RIP: sending v2 update to 224.0.0.9 via GigabitEthernet0/1 (192.168.3.2)
*Oct 22 13:48:39.980: RIP: build update entries
*Oct 22 13:48:39.980:         192.168.2.0/24 via 0.0.0.0, metric 1, tag 0
*Oct 22 13:48:44.050: RIP: received v2 update from 192.168.3.1 on GigabitEthernet0/1
*Oct 22 13:48:44.051:      192.168.1.0/24 via 0.0.0.0 in 1 hops
*Oct 22 13:48:39.979: RIP: sending v2 update to 224.0.0.9 via GigabitEthernet0/1 (192.168.3.2)
*Oct 22 13:48:39.980: RIP: build update entries
*Oct 22 13:48:39.980:         192.168.2.0/24 via 0.0.0.0, metric 1, tag 0
*Oct 22 13:48:44.050: RIP: received v2 update from 192.168.3.1 on GigabitEthernet0/1
*Oct 22 13:48:44.051:      192.168.1.0/24 via 0.0.0.0 in 1 hops
*Oct 22 13:49:06.592: RIP: sending v2 update to 224.0.0.9 via GigabitEthernet0/1 (192.168.3.2)
*Oct 22 13:49:06.593: RIP: build update entries
*Oct 22 13:49:06.593:         192.168.2.0/24 via 0.0.0.0, metric 1, tag 0
*Oct 22 13:49:09.792: RIP: received v2 update from 192.168.3.1 on GigabitEthernet0/1
*Oct 22 13:49:09.792:      192.168.1.0/24 via 0.0.0.0 in 1 hops
```

On peut arrêter tout debug :

```
R2#undebug all
All possible debugging has been turned off
```

10. Routes flottantes

À compléter.

© 2021 François-Emmanuel Goffinet

Quatrième partie Routage OSPF

Le protocole OSPF est le protocole de routage dynamique intérieur TCP/IP de l'IETF. Il fonctionne selon le principe des protocoles à état de lien qui utilisent l'algorithme Dijkstra. Contrairement à un protocole de routage à vecteur de distance, OSPF collecte l'état de toutes les liaisons au sein d'une zone (*area*) et calcule de son point de vue toutes les routes pour les destinations de la zone. Le protocole fonctionne en connectant les zones entre elles mais il reste néanmoins un protocole de routage intérieur. Il existe en version 2 pour IPv4 et en version 3 principalement pour IPv6.

Après une introduction sur le protocole de routage, on verra comment le configurer, le vérifier et le dépanner dans un contexte multi-zones (*multi-area*) avec une attention particulière sur l'établissement des relations de voisinage et sur l'élection DR-BR.

4. Introduction au protocole de routage dynamique OSPF

1. Introduction à OSPF

1.1 Protocole de routage à état de lien

Un protocole de routage à état de lien utilise un algorithme (plus) efficace (autre que RIP, comme “Dijkstra” ou “Shortest Path First”). Les routeurs collectent l’ensemble des coûts des liens et construisent de leur point de vue l’arbre de tous les chemins possibles. Les meilleures routes sont alors intégrées à la table de routage.

- On parlera de routage hiérarchique (à deux niveaux).
- On citera OSPF et IS-IS.
- Ils convergent très rapidement.
- Les routeurs entretiennent des relations de voisinage maintenues.

1.2. Protocole à vecteur de distance

Un protocole de routage à vecteur de distance est celui qui utilise un algorithme de routage qui additionne les distances pour trouver les meilleures routes (Bellman-Ford).

- Les routeurs envoient l’entièreté de leur table de routage aux voisins.
- Ces protocoles sont sensibles aux boucles de routage.
- Dans ce type de protocole, aucun routeur ne remplit de fonction particulière. On parlera de connaissance “plate” de l’inter-réseau ou de routage non-hiérarchique.
- Ils convergent lentement.

On citera RIP et IGRP (propriétaire obsolète) comme étant représentatifs. EIGRP est aussi un protocole à vecteur de distance avancé entièrement optimisé par Cisco Systems qui ne présente pas ces désavantages.

1.3. Distances administratives (par défaut)

La **distance administrative** est le poids administratif d’une route apprise par un protocole de routage. Une distance administrative faible donne la préférence pour une route apprise quelle que soit la méthode de routage. Les distances administratives ont une valeur par défaut. Une route EIGRP sera préférée à une route RIP. Par défaut, une route statique sera préférée à toute autre route dynamique.

Méthode de routage	Distance administrative
Réseau connecté	0
Route statique	1
Ext-BGP	20
Int-EIGRP	90
OSPF	110
IS-IS	115
RIP	120
Int-BGP	200
Inconnu	255

1.4. Comparatif protocoles de routage

Vecteur de distance	Etat de lien
Algorithme Bellman-Ford (RIP)	Algorithme Dijkstra (OSPF)
Facile à configurer	Compétences requises
Partage des tables de routage	Partage des liaisons
Réseaux plats	Réseaux conçus (design) organisés en areas
Convergence plus lente	Convergence rapide, répartition de charge
Topologies limitées	Topologies complexes et larges
Gourmand en bande passante	Relativement discret
Peu consommateur en RAM et CPU	Gourmand en RAM et CPU
Mises à jour régulière en Broadcast/Multicast	Mises à jour immédiate
Pas de signalisation	Signalisation fiable et en mode connecté
RIPv1 - UDP520 - `255.255.255.255`, RIPv2 - UDP520 - `224.0.0.9`, EIGRP - Cisco Systems (DUAL)- `224.0.0.10` - `FF02::A`	OSPFv2/v3 - IP89 - `224.0.0.5`, `224.0.0.6`, `FF02::5`, `FF02::6`, IS-IS

1.5. OSPF (Open Shortest Path First)

Le protocole OSPF (Open Shortest Path First) a été développé par l'IETF pour répondre au besoin d'un protocole de routage intérieur (IGP, "Internal Gateway Protocol") dans la pile des protocoles TCP/IP, non-propriétaire et hautement fonctionnel.

Les discussions sur la création d'un IGP commun et inter-opérable pour l'Internet commencèrent en 1987.

La version actuelle d'OSPFv2 est décrite dans le RFC 2328 (1998). Une version 3 est définie dans le RFC 5340 qui permet l'utilisation de OSPF dans un réseau IPv6 (2008) et même d'embarquer des routes IPv4.

Son principal concurrent sur les infrastructures homogènes d'entreprises est EIGRP, propriétaire Cisco.

OSPF est un protocole de routage à états de liens.

1.6. Comparatif OSPF/RIP

En OSPF, il n'y a pas de limite du nombre de sauts comme en RIP. OSPF étant un protocole de routage à état de lien, chaque routeur possède une connaissance complète des réseaux au sein d'une zone (*area*). Aussi, le danger des boucles de routage n'étant *a priori* plus présent, la limite du nombre de sauts n'est plus nécessaire.

L'utilisation intelligente du "VLSM" (masques à longueur variable) améliore les plans d'adressage (allocations d'adresses IP). OSPF supporte aussi l'agrégation et la "summarization" de routes.

Il utilise le Multicast pour envoyer ses mises à jour d'état de lien. Aussi, ces mises à jour sont envoyées uniquement lors d'un changement de topologie. On économise la bande passante. Les mises à jour sont seulement incrémentielles et opportunes.

OSPF offre une meilleure convergence que RIP parce que les changements de routage sont propagés instantanément et (non périodiquement) de manière incrémentielle grâce aux relations de voisinage entretenues.

OSPF est meilleur pour la répartition de charge (*load balancing*). Le choix du meilleur chemin est basé sur le coût (la bande passante inversée). Cette métrique peut être définie manuellement sur les interfaces.

© 2021 François-Emmanuel Goffinet

OSPF permet une définition logique des réseaux où les routeurs peuvent être répartis en zones (*area*). Cette fonctionnalité empêche une explosion de mises à jour d'états de lien sur l'ensemble du réseau. C'est aussi au niveau des zones que l'on peut agréger les routes et stopper la propagation inutile des informations de sous-réseaux existants.

OSPF autorise l'authentification des informations de routage par l'utilisation de différentes méthodes d'identification avec mots de passe.

Il permet le transfert et l'étiquetage des routes extérieures injectées dans un Système Autonome (AS) pour permettre de les maintenir par des "EGPs" comme BGP.

1.7. Les éléments clés de OSPF

Les routeurs OSPF entretiennent une relation orientée connexion avec les routeurs d'un même segment physique. Dans la terminologie OSPF, on parlera d'*adjacency*, en français, d'adjacence ou de contiguïté.

Au lieu d'envoyer des mises à jour entières lors d'un changement topologique, OSPF envoie des mises à jour incrémentielles.

OSPF n'est pas limité par une segmentation dépendante de l'adressage IP ou des sous-réseaux, il utilise la notion d'*area* (zone) pour désigner un groupe de routeurs.

OSPF supporte entièrement les possibilités du "VLSM" et de la "summarization" manuelle des routes.

Grâce à la possibilité de donner des rôles particuliers aux routeurs, la communication "inter-area/inter-routeurs" est efficace.

Bien que OSPF permette une communication "inter-area", il reste un protocole de routage intérieur (IGP).

1.8. Que signifie Link-States / Etats de liens ?

OSPF est un protocole à état de lien.

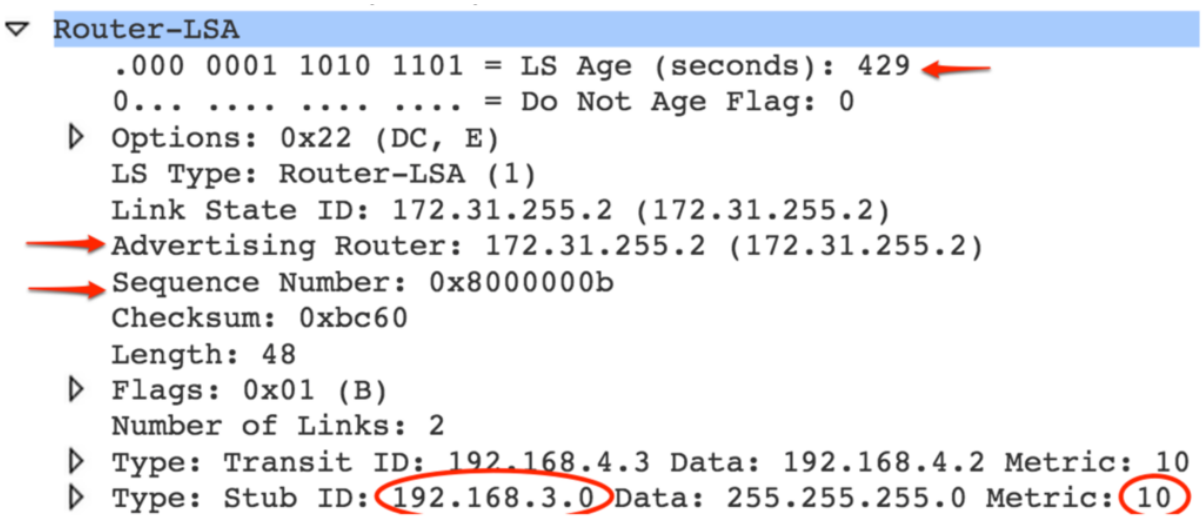
- Nous pouvons penser qu'un lien est l'interface d'un routeur.
- L'état d'un lien est une description de cette interface et de la relation qu'elle entretient avec ses routeurs voisins.
- Une description de cette interface pourrait comprendre, par exemple, son adresse IP, le masque, le type de réseau connecté, les routeurs connectés, etc.

L'ensemble de ces états de liens forme la *link-state database*. La *link-state database* ou *topology table*, est identique sur tous les routeurs d'une *area* (zone).

1.9. Exemple d'état de lien OSPF

Un *Link State Advertisement (LSA)* est l'information de routage échangée par les routeurs dans des messages *Link State Update (LSU).*

© 2021 François-Emmanuel Goffinet



LSA OSPF

1.10. Support d'IPv6 : OSPFv3

OSPFv2 et OSPFv3 ont des messages, un algorithme et un fonctionnement très proches.

Parmi d'autres, on notera au moins deux différences entre OSPFv2 et OSPFv3. En OSPFv3 :

- Des messages renommés et nouveaux
- Deux approches de configuration OSPFv3 sous Cisco IOS :
  - Une configuration traditionnelle (uniquement IPv6)
  - L'approche par *address-family* (supportant **le transport en IPv6** des routes IPv4 **et** des routes IPv6)

2. Zone OSPF

2.1. "Area" ou zone OSPF

Une caractéristique principale d'OSPF est de supporter des interréseaux très larges grâce au regroupement des routeurs dans des entités logiques appelées *areas* ou zones.

La communication *inter-areas* ne laisse passer que les échanges d'information minimale de routage dans le seul objectif de connecter les zones entre elles.

Il en résulte que les efforts de calcul de routes ne s'opèrent qu'au sein d'une même zone.

Les routeurs d'une zone ne sont pas affectés (en calcul) par les changements intervenus dans une autre zone.

Dans un contexte où OSPF demande beaucoup de ressources en CPU et en mémoire, cette notion de conception est très importante.

2.2. Opérations et rôles OSPF

Un routeur OSPF peut prendre en charge trois types d'opérations :

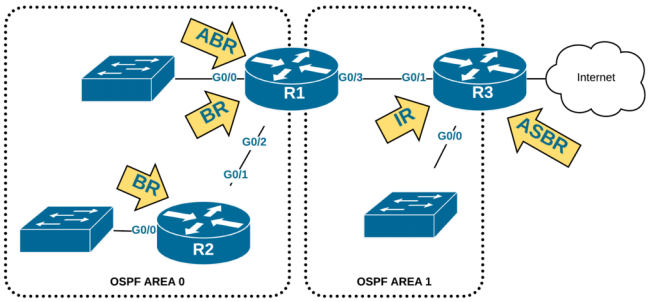
1. opérations dans une zone,
2. connexions inter-zones

© 2021 François-Emmanuel Goffinet

3. et connexions avec d'autres systèmes autonomes (AS).

Un routeur OSPF remplit un rôle et une responsabilité particulière qui dépend de la hiérarchie OSPF établie :

1. Internal Router (IR)
2. Backbone Router (BR)
3. Area Border Router (ABR)
4. Autonomous System Boundary Router (ASBR)



IR BR ABR ASBR OSPF

OSPF Internal Router (IR)

Un **IR** remplit des fonctions au sein d'une zone (*area*) uniquement, autre que la zone *Backbone*.

Sa fonction primordiale est d'entretenir à jour avec tous les réseaux de sa zone (*area*) sa base de données d'états de lien (*link-state database*) qui est identique sur chaque IR.

Il renvoie toute information aux autres routeurs de sa zone (area), le routage ou L'inondation (*flooding*) des autres zones requiert L'intervention d'un *Area Border Router* (**ABR**).

OSPF Backbone Router (BR)

Une des règles de conception OSPF est que chaque zone (area) dans l'interréseau doit être connectée à une seule zone, **la zone 0** ou la ***backbone area***.

Les **BR** ont une interface connectée à la *backbone area*.

OSPF Area Border Router (ABR)

Un **ABR** connecte au moins deux zones (area) dont l'*area* 0.

Un ABR possède autant de bases de données d'états de lien qu'il y a d'interfaces connectées à des zones différentes.

Chacune de ces bases de données contient la topologie entière de la zone connectée et peut donc être "summarizée", c'est-à-dire agrégée en une seule route IP.

Ces informations peuvent être transmises à la zone de backbone pour la distribution.

Un élément clé est qu'un ABR est l'endroit où l'agrégation doit être configurée pour réduire la taille des mises à jour de routage qui doivent être envoyées ailleurs.

Donc quand on parle des capacités de OSPF de minimiser les mises à jour de routage, on peut directement penser au rôle rempli par les ABR.

© 2021 François-Emmanuel Goffinet

OSPF Autonomous System Boundary Router (ASBR)

OSPF est un IGP (Interior Gateway Protocol), autrement dit il devra être connecté au reste de l'Internet par d'autres AS.

Ce type de routeur fera en quelque sorte office de passerelle vers un ou plusieurs AS. L'échange d'information entre un AS OSPF et d'autres AS est le rôle d'un **ASBR**.

Les informations qu'il reçoit de l'extérieur seront redistribuées au sein de l'AS OSPF.

2.3. Fonctionnement dans une zone

1. Pour chaque zone (*area*) une table d'états de lien est construite et maintenue.
2. La table de routage est construite à partir de cette base de données.
3. Ce résultat est obtenu grâce à l'application de l'algorithme de routage SPF.

Étape 1 : Découverte des voisins

D'abord, l'interface d'un routeur doit trouver ses voisins et entretenir une relation avec chaque voisin L2.

Il utilise des paquets Hello.

Dès son initialisation ou à la suite d'un changement dans la topologie, un routeur va générer un *link-state advertisement (LSA).*

Cette annonce va représenter la collection de tous les états de liens de voisinage du routeur.

Étape 2 : Inondations et mises à jour

Tous les routeurs de la zone (*area*) vont s'échanger ces états de liens par inondation (*flooding*).

Chaque routeur qui reçoit des mises à jour d'état de lien (*link-state update*), en gardera une copie dans sa *link-state database* et propagera la mise à jour auprès des autres routeurs.

Étape 3 : Calcul des routes

Après que la base de données de chaque routeur a été complétée, chacun va calculer l'arbre du chemin le plus court ("Shortest Path Tree") vers toutes les destinations avec l'algorithme "Dijkstra".

Il construira alors la table de routage (*routing table*), appelée aussi *forwarding database*, en choisissant les meilleures routes à inscrire.

Étape 4: Maintenance des routes

S'il n'y a pas de modification topologique, OSPF sera très discret.

Par contre en cas de changement, il y aura échange d'informations (par des paquets d'état de lien) et l'algorithme "Dijkstra" recalculera les chemins les plus courts à inscrire dans la table de routage.

© 2021 François-Emmanuel Goffinet

Cinquième partie Routage EIGRP

Concurrent immédiat du protocole de routage à états de lien OSPF de l'IETF, EIGRP est le protocole préféré dans les infrastructures homogènes Cisco. EIGRP est documenté depuis 2016 dans le RFC7868 informational. EIGRP s'oppose aussi à OSPF au moins à deux égards : c'est un protocole de routage à vecteur de distance ultra-performant d'une part, et d'autre part, il supporte nativement les deux protocoles IPv4 et IPv6. Du point de vue de la performance, il tout aussi performant voir plus performant qu'OSPF. Enfin, il est simple à configurer et à maintenir.

À titre d'exemple, on démontrera aussi la capacité de EIGRP de répartir la charge de trafic entre des chemins inégaux. Ce sera l'occasion d'illustrer le concept de variance.

5. Protocole EIGRP

Le protocole de routage dynamique propriétaire EIGRP est la solution préférée dans les infrastructures Cisco Systems. EIGRP est un protocole de routage dynamique intérieur hautement fonctionnel. Il converge très rapidement et il est multi-protocoles IPv4/IPv6. Il permet de contrôler finement la métrique de manière à influencer les entrées de la table de routage. EIGRP est alors capable de répartir la charge de trafic sur des liaisons à coûts inégaux.

1. Présentation du protocole EIGRP

- Protocole de routage à **vecteur de distance** avancé propriétaire (IP88).
- Utilisant l'algorithme DUAL, Diffusing Update Algorithm mentionné comme "Loop-Free Routing Using Diffusing Computations", (Garcia-Luna-Aceves 1993, SRI International).
- Préféré dans les infrastructures homogènes Cisco, il est concurrent au standard IETF OSPF.
- Performant et évolutif.
- RFC 7868 informational (mai 2016), Cisco's Enhanced Interior Gateway Routing Protocol (EIGRP)[1].

1.1. Fonctionnalités

Le protocole EIGRP dispose de caractéristiques fonctionnelles modernes :

- Établit des relations de voisinage.
- Mises à jour opportunes, incrémentielles, partielles avec des demandes, des réponses et des accusés de réception (économie de bande passante).
- Il est multi-protocoles : il supporte aussi bien qu'IPv4/IPv6.
- Il utillise l'Unicast et le Multicast `224.0.0.10` et `FF02::A`, Il est directement embarqué dans IP (protocole IP 88).
- Convergence très rapide par nature.
- Calcul anticipé de routes alternatives sans boucle (algorithme DUAL).
- Métrique fine "composite" (c'est-à-dire composées de plusieurs éléments dans une formule de calcul).
- Répartition de charge égale des routes, mais aussi répartition de charge inégale de routes.
- Redistribution de routes.
- "Summarization" automatique/manuelle des routes.
- Authentification des messages de routage.

1. Le démon de routage Open Source FRRouting version 4 (22/03/2018) supporte nativement EIGRP en implémentant son RFC 7868.

1.2. Composants clés d'EIGRP

- EIGRP découvre les routeurs voisins et prend en charge la maintenance des relations de voisinage avec des paquets Hello envoyés périodiquement.
- Une machine à état quelques fois déjà nommée "RTP" (pour Reliable Transport Protocol) assure le contrôle, l'envoi, le suivi et assure la fiabilité des messages EIGRP.
- L'algorithme d'optimisation des routes est "Diffusing Update Algorithm" (DUAL) qui détermine le meilleur chemin sans boucle.

1.3. Tables EIGRP

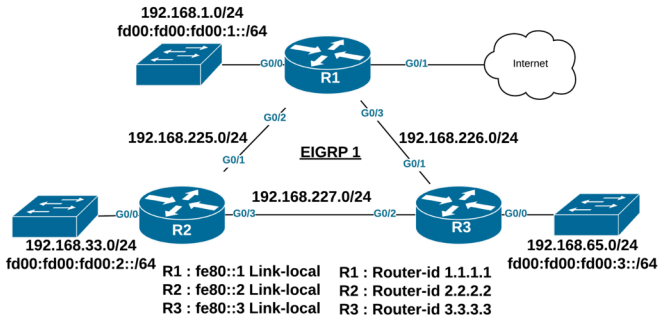
EIGRP gère trois tables :

1. *Neighbor Table* : une table de voisinage est utilisée pour une livraison fiable des messages.
2. *Topology Table* : une table topologique qui contient toutes les routes EIGRP sans boucles.
3. La table de routage pouvant contenir les meilleures routes EIGRP.

2. Configuration EIGRP en IPv4 et en IPv6

Chaque routeur est identifié par un routeur ID, même s'il est conseillé qu'il soit unique, cet élément est moins critique dans les calculs EIGRP (en comparaison au router ID OSPF), sauf pour les routes externes[2]. Il s'agit d'un mot de 32 bits qu'il est obligatoire de configurer manuellement en IPv6. Comme en OSPF, l'adresse IPv4 d'une interface de loopback peut prévaloir pour déterminer cet identifiant.

2.1. Topologie d'étude



Topologie d'étude EIGRP en IPv4 et en IPv6

2.2. Configuration de base IPv4

2. Preventing Duplicate EIGRP Router IDs

© 2021 François-Emmanuel Goffinet

```
hostname R1
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
interface GigabitEthernet0/0
 no shutdown
 ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet0/2
 no shutdown
 ip address 192.168.225.1 255.255.255.0
!
interface GigabitEthernet0/3
 no shutdown
 ip address 192.168.226.1 255.255.255.0
```

2.3. Configuration du routage IPv4

```
router eigrp 1
 passive-interface GigabitEthernet0/0
 eigrp router-id 1.1.1.1
 network 192.168.1.0
 network 192.168.225.0
 network 192.168.226.0
```

Note sur la commande `network`, il est possible de préciser un masque pour choisir des interfaces participantes :

```
R1(config-router)#network ?
  A.B.C.D  Network number

R1(config-router)#network 192.168.0.0 ?
  A.B.C.D  EIGRP wild card bits
  <cr>

R1(config-router)#network 192.168.0.0 0.0.0.255 ?
  <cr>
```

Sans masque générique, c'est le réseau de classe (classful) qui est pris en compte.

2.4. Vérification de la configuration IPv4

```
R1#show ip protocols | begin eigrp
Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(1)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    Soft SIA disabled
    NSF-aware route hold timer is 240
    Router-ID: 1.1.1.1
    Topology : 0 (base)
      Active Timer: 3 min
```

© 2021 François-Emmanuel Goffinet

```
      Distance: internal 90 external 170
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1
  Automatic Summarization: disabled
  Maximum path: 4
  Routing for Networks:
    192.168.1.0
    192.168.225.0
    192.168.226.0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.225.2         90      00:04:29
  Distance: internal 90 external 170
```

2.5. Configuration de base IPv6

```
hostname R1
!
interface GigabitEthernet0/0
 no shutdown
 ipv6 address FE80::1 link-local
 ipv6 address FD00:FD00:FD00:1::1/64
!
interface GigabitEthernet0/2
 no shutdown
 ipv6 address FE80::1 link-local
!
interface GigabitEthernet0/3
 no shutdown
 ipv6 address FE80::1 link-local
```

2.6. Configuration du routage IPv6

```
ipv6 unicast-routing
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
ipv6 router eigrp 1
 eigrp router-id 1.1.1.1
 passive-interface GigabitEthernet0/0
!
interface GigabitEthernet0/0
 ipv6 eigrp 1
!
interface GigabitEthernet0/2
 ipv6 eigrp 1
!
interface GigabitEthernet0/3
 ipv6 eigrp 1
```

Note : La configuration administrative du `router-id` est obligatoire en EIGRP IPv6.

© 2021 François-Emmanuel Goffinet

2.7. Vérification de la configuration IPv6

```
R1#sh ipv6 protocols | begin eigrp
IPv6 Routing Protocol is "eigrp 1"
EIGRP-IPv6 Protocol for AS(1)
  Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  Soft SIA disabled
  NSF-aware route hold timer is 240
  Router-ID: 1.1.1.1
  Topology : 0 (base)
    Active Timer: 3 min
    Distance: internal 90 external 170
    Maximum path: 16
    Maximum hopcount 100
    Maximum metric variance 1
  Interfaces:
    GigabitEthernet0/2
    GigabitEthernet0/3
    GigabitEthernet0/0 (passive)
  Redistribution:
    None
```

2.8. Commandes de configuration EIGRP

On reconnaîtra les commandes :

- `router eigrp 1` où le chiffre signifie le numéro de système autonome (AS).
- `passive-interface` qui empêche l'envoi d'informations de routage à travers l'interface désignée.
- `router-id` qui fixe l'identifiant du routeur EIGRP (**obligatoire en IPv6**)

2.9. Déclaration des réseaux

Pour déclarer des réseaux dans le processus de routage EIGRP IPv4, on utilisera habituellement la commande `network` avec ou sans masque générique (réseau de classe pris en compte), selon le niveau de précision dans le choix des interfaces qui participent au routage :

```
R1(config)#router eigrp 1
R1(config-router)#network 192.168.1.0 0.0.0.255
R1(config-router)#network 192.168.225.0
R1(config-router)#network 192.168.226.0
```

Pour déclarer des réseaux dans le processus de routage EIGRP IPv6, on indique qu'une interface participe au routage :

```
R1(config)#interface G0/0
R1(config-if)#ipv6 eigrp 1
```

3. Voisinage EIGRP

3.1. Cinq types de paquets EIGRP

EIGRP cinq types de paquets :

© 2021 François-Emmanuel Goffinet

- **Hello** : identifie les voisins et sert de mécanisme de “keepalive”.
- **Update** : Envoie des informations de routage de manière fiable
- **Query** : Demande des informations de routage de manière fiable
- **Reply** : Répond à un Query de manière fiable
- **ACK** : Accusé de réception

3.2. Hello EIGRP

Les routeurs EIGRP s’annoncent dans des paquets Hello envoyés aux adresses `224.0.0.10` et `FF02::A` toutes les 5 secondes sur des liaisons rapides et 60 secondes sur des connexions série. Des délais différents sur les interfaces n’empêchent pas les relations de voisinage EIGRP. Toutefois,

- L’adresse source doit être dans le même réseau que le voisin.
- Le poids des métriques doit correspondre.
- Le processus EIGRP doit être dans le même système autonome.

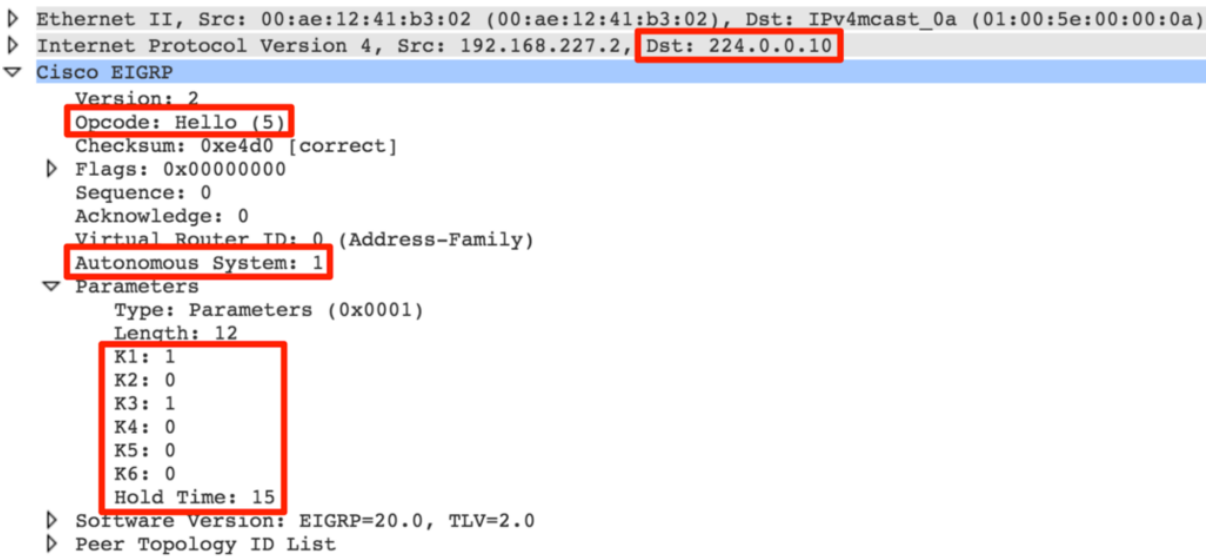
On configure le délai des “Hello” en configuration d’interface :

```
(config-if)#ip hello-interval eigrp <instance-tag> <seconds>
```

Le délai Hold Time est celui après lequel un voisin est considéré comme injoignable (*down*). On le configure sur une interface :

```
(config-if)#ip hold-time eigrp <instance-tag> <seconds>
```

3.3. Paquet EIGRP Hello IPv4



Paquet EIGRP Hello IPv4

3.4. Relations de voisinage

© 2021 François-Emmanuel Goffinet

```
R1#show ipv6 eigrp neighbors
EIGRP-IPv6 Neighbors for AS(1)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
1   Link-local address:     Gi0/3                    10 00:20:28  231  1386  0  5
    FE80::3
0   Link-local address:     Gi0/2                    13 00:20:40  933  5000  0  6
    FE80::2
```

```
R1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
0   192.168.225.2           Gi0/2                    14 00:15:58  520  3120  0  6
1   192.168.226.2           Gi0/3                    13 00:21:57   14   100  0  12
```

La valeur dans la colonne “Hold” de la sortie ne doit jamais excéder le “Hold Time” et ne doit jamais être inférieure au “Hello Interval”. La colonne “Hold” comprend des valeurs normales entre 10 et 15 secondes si le “Hold Time” est de 15 secondes et si le “Hello Interval” est de 5 secondes. La valeur normale sera comprise entre 120 et 180 secondes si le “Hello Interval” est de 60 secondes avec un “Hold Time” de 180 secondes. En cas de discordance, il y a lieu de vérifier les interfaces voisines, voire de configurer manuellement les délais.

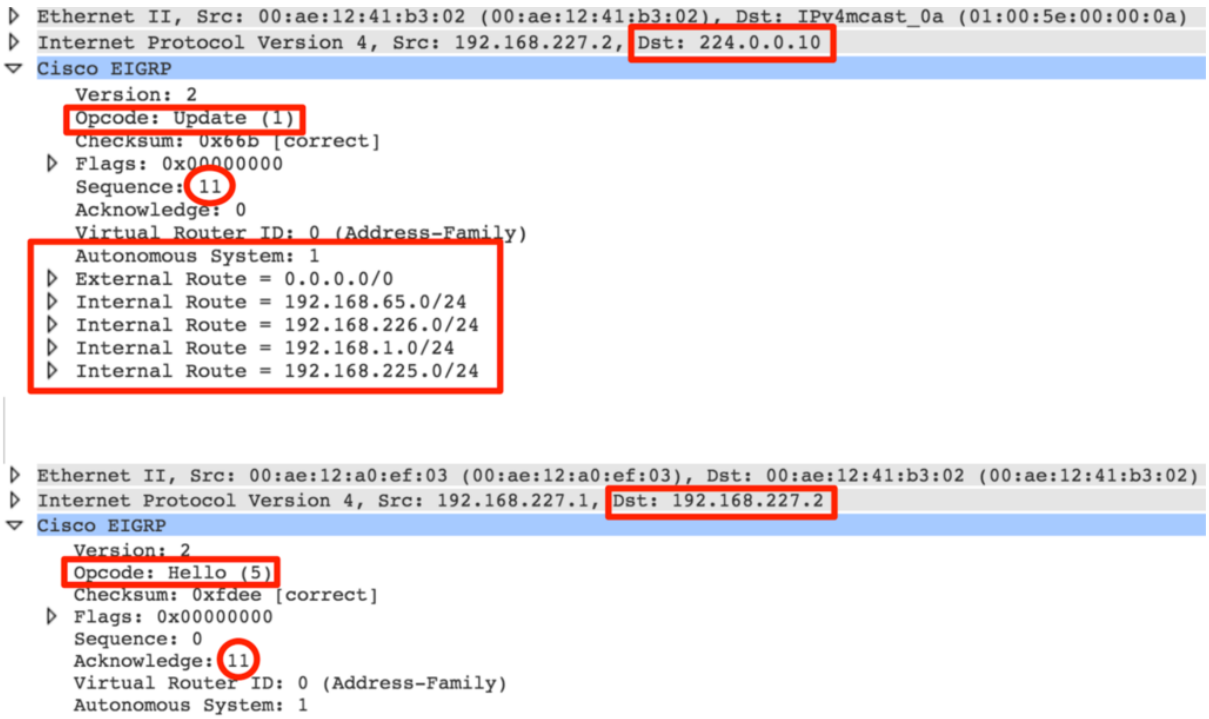
On trouvera ici la signification des colonnes.

- **H** : liste les voisins dans l’ordre appris par le routeur.
- **Address** : L’adresse IP des voisins.
- **Interface** : l’interface de laquelle le paquet Hello a été reçu.
- **Hold (sec)** : le temps restant avant lequel le voisin est considéré comme “down”.
- **Uptime** : le temps depuis lequel l’adjacence a été établie.
- **SRTT** (Smooth Round Trip Timer) : le temps moyen en millisecondes entre la transmission d’un paquet à un voisin et la réception d’un accusé de réception.
- **RTO** (Retransmission Timeout) : si la livraison Multicast échoue, alors la livraison Unicast est utilisée ; le RTO est le temps en millisecondes que le routeur patiente pour recevoir un accusé de réception à des messages livrés en Unicast.
- **Q Cnt** (Queue count) : le nombre de paquets EIGRP mis en file d’attente. `0` est la meilleure valeur. Toute valeur supérieure à 0 est problématique.
- **Seq Num** (Sequence Number) : le numéro de séquence du dernier message de mise-à-jour EIGRP (chaque message EIGRP dispose d’une numéro de séquence incrémenté).

3.5. EIGRP Update/ACK

EIGRP connaît un échange de messages dès que le voisinage est établi. Les routes sont transmises dans messages *EIGRP Update* adressés en multicast/unicast confirmés par des Hello ACK adressés en Unicast. Leur point commun est le numéro de séquence et le numéro “ack”.

© 2021 François-Emmanuel Goffinet



EIGRP Update/ACK

On trouve aussi des paquets Update avec un flag “init” en Unicast préalables à l’échange des routes.

3.6. Message GOODBYE

Un message “Goodbye” est une fonctionnalité conçue pour améliorer la convergence EIGRP. Ce message informe immédiatement les voisins de la fin d’un processus de routage EIGRP et d’un changement dans la topologie. Cette fonctionnalité permet aussi aux voisins EIGRP de se synchroniser et de recalculer leurs relations de voisinage de manière plus efficace qu’au terme de l’expiration d’un compteur de retenue (“Hold Time”).

Un message “Goodbye” reçu par un routeur : `*Apr 26 13:48:42.523: %DUAL-5-NBRCHANGE : IP-EIGRP(0) 1: Neighbor 10.1.1.1 (Ethernet0/0) is down : Interface Goodbye received`

Reference : http ://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfeigrp.html

4. Tables de routage EIGRP

4.1. Formule de métrique EIGRP

La métrique EIGRP est obtenue à partir d’une formule mathématique où k est un poids qui permet d’inclure les composantes suivantes :

- bande passante (bandwidth, BW) : $(10^7/bandwidth_i) \times 256$
- délais (delay) : $delay_i \times 256$
- charge (load)
- fiabilité (reliability)

$$Metric = \left[\left(k1 \times BW_m + \frac{k2 \times BW_m}{256 - load} + k3 \times delay \right) \times \frac{k5}{k4 + reliability} \right] \times 256$$

© 2021 François-Emmanuel Goffinet

Où la bande passante minimum est $BW_m = \frac{10^7}{least\_bandwidth}$

Si la bande passante et le délai sont seulement activés par défaut comme l'indique la commande `show ip protocols` :

```
Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
```

$$Metric = \left[\left(\frac{10^7}{least\_bandwidth} \right) + cumultative\_delay \right] \times 256$$

4.2. Table de routage IPv4

```
R1#show ip route eigrp | begin Gateway
Gateway of last resort is not set
D     192.168.33.0/24
           [90/3072] via 192.168.225.2, 00:43:43, GigabitEthernet0/2
D     192.168.65.0/24
           [90/3072] via 192.168.226.2, 00:43:43, GigabitEthernet0/3
D     192.168.227.0/24
           [90/3072] via 192.168.226.2, 00:43:43, GigabitEthernet0/3
           [90/3072] via 192.168.225.2, 00:43:43, GigabitEthernet0/2
```

On constate que le réseau `192.168.227.0/24` entre R2 et R3 est joignable via R2 ou R3. Les deux routes disposent d'une valeur de métrique équivalente (3072). Le routeur répartira la charge sur les deux liaisons pour du trafic pour cette destination.

4.3. Table de routage IPv6

```
R1#show ipv6 route eigrp | begin 90
D   FD00:FD00:FD00:2::/64 [90/3072]
     via FE80::2, GigabitEthernet0/2
D   FD00:FD00:FD00:3::/64 [90/3072]
     via FE80::3, GigabitEthernet0/3
```

4.4. Diagnostic EIGRP

On retiendra les commandes de diagnostic suivante et la signification de leur sortie.

Pour IPv4 :

```
show ip protocols
show ip eigrp neighbors
show ip route eigrp
show ip eigrp interface <interface>
show ip eigrp topology
```

Pour IPv6 :

© 2021 François-Emmanuel Goffinet

```
show ipv6 protocols
show ipv6 eigrp neighbors
show ipv6 route eigrp
show ipv6 eigrp interface <interface>
show ipv6 eigrp topology
```

5. Algorithme DUAL

La table topologique EIGRP contient toutes les routes sans boucles calculées grâce à l'algorithme DUAL. Les routes Actives sont celles qui sont en cours d'apprentissage et **les routes Passives sont des routes apprises et valides**.

La notion de "successor" correspond à celle de passerelle, soit le routeur disposant d'un chemin sans boucle pour un réseau de destination.

La Feasible Distance (FD) est la meilleure métrique pour cette destination.

Par défaut EIGRP installe un "successor" avec la "feasible distance", soit la meilleure route sans boucle.

5.1. Condition de faisabilité

Une route alternative pour une destination pourrait être apprise d'avance alors qu'elle n'aurait pas la meilleure métrique à condition que sa distance reportée (Reported Distance) soit inférieure à la meilleure métrique (Feasible Distance) locale.

On trouve la "reported distance" à côté de la métrique calculée.

La Reported Distance est la meilleure métrique du "successor" potentiel pour la même destination.

Si cette valeur est inférieure à la FD locale, le chemin est certainement sans boucle.

On vérifie ces valeurs dans la table topologique EIGRP

5.2. Table topologique

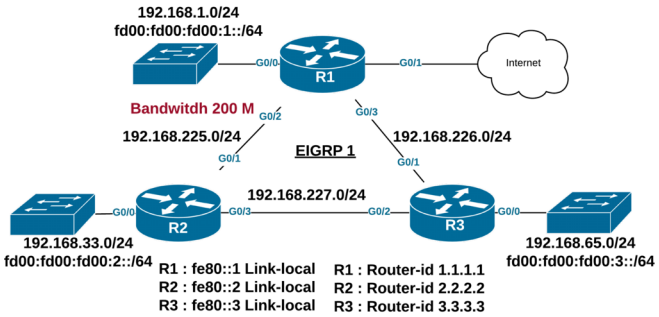
```
R1#show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(1)/ID(1.1.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 192.168.225.0/24, 1 successors, FD is 2816
        via Connected, GigabitEthernet0/2
P 192.168.227.0/24, 2 successors, FD is 3072
        via 192.168.225.2 (3072/2816), GigabitEthernet0/2
        via 192.168.226.2 (3072/2816), GigabitEthernet0/3
P 192.168.33.0/24, 1 successors, FD is 3072
        via 192.168.225.2 (3072/2816), GigabitEthernet0/2
P 192.168.1.0/24, 1 successors, FD is 2816
        via Connected, GigabitEthernet0/0
P 192.168.226.0/24, 1 successors, FD is 2816
        via Connected, GigabitEthernet0/3
P 192.168.65.0/24, 1 successors, FD is 3072
        via 192.168.226.2 (3072/2816), GigabitEthernet0/3
```

© 2021 François-Emmanuel Goffinet

6. Manipuler les distances

6.1. Deuxième topologie EIGRP



Seconde topologie EIGRP

Dans cette topologie la bande passante est fixée de manière administrative à 200 Mbps entre R1 et R2.

6.2. Manipuler les distances

On peut manipuler la métrique EIGRP en fixant une bande passante administrative en Kbps sur les interfaces respectives, ici 200 Mbps entre R1 et R2 :

```
R1(config)#interface G0/2
R1(config-if)#bandwidth 200000
R2(config)#interface G0/1
R2(config-if)#bandwidth 200000
```

6.3. Seconde table de routage IPv4

La meilleure route pour le réseau `192.168.227.0/24` passe par R3 seulement (G0/3) :

```
R1#sh ip route eigrp | begin Gateway
Gateway of last resort is not set

D     192.168.33.0/24
           [90/3328] via 192.168.226.2, 00:04:28, GigabitEthernet0/3
D     192.168.65.0/24
           [90/3072] via 192.168.226.2, 00:04:28, GigabitEthernet0/3
D     192.168.227.0/24
           [90/3072] via 192.168.226.2, 00:04:28, GigabitEthernet0/3
```

6.4. Seconde table topologique

La meilleure route pour la destination `192.168.227.0/24` dispose d'une FD de 3072. Elle passe par R3 (G0/3).

Une route alternative pour cette même destination `192.168.227.0/24` passe par R2 (G0/2) avec une métrique calculée à 13312. Elle ne peut pas être incluse dans la table de routage car cette valeur est plus élevée que la meilleure métrique.

La "Reported Distance" 2816 de la route alternative est inférieure à la FD 3072 : c'est une route sans boucle.

© 2021 François-Emmanuel Goffinet

```
R1#sh ip eigrp topology
P 192.168.227.0/24, 1 successors, FD is 3072
        via 192.168.226.2 (3072/2816), GigabitEthernet0/3
        via 192.168.225.2 (13312/2816), GigabitEthernet0/2
```

6.5. Unequal Load balancing

Il est possible d'inclure une route alternative à métrique plus élevée dans la table de routage pour une réparation de charge proportionnelle, "inégale" (unequal load balancing) si :

- la route répond à la condition de faisabilité
- la variance permet d'inclure cette route

6.6. Variance

La variance est le multiplicateur de la meilleure métrique qui permet d'inclure des routes sans boucles à métriques plus élevées. Par défaut, la variance fixée à 1 n'autorise que la prise en charge de la meilleure route. C'est un donc un rapport exprimé en nombre entier.

En divisant la métrique de la route alternative 13312 par la FD 3072, on obtient la valeur de la variance nécessaire à l'inclusion de notre route alternative, soit 5.

Il sera nécessaire d'exécuter la commande sur tous les routeurs pour assurer un routage cohérent :

```
(config)#router eigrp 1
(config-router)#variance 5
```

6.7. Troisième table de routage

```
R1#show ip route eigrp | begin Gateway
Gateway of last resort is not set

D     192.168.33.0/24
           [90/3328] via 192.168.226.2, 00:00:54, GigabitEthernet0/3
           [90/13312] via 192.168.225.2, 00:00:54, GigabitEthernet0/2
D     192.168.65.0/24
           [90/3072] via 192.168.226.2, 00:00:54, GigabitEthernet0/3
D     192.168.227.0/24
           [90/3072] via 192.168.226.2, 00:00:54, GigabitEthernet0/3
           [90/13312] via 192.168.225.2, 00:00:54, GigabitEthernet0/2
```

7. Captures et documentation EIGRP

- R2 redémarre en IPv4 : https ://www.cloudshark.org/captures/3d6c6fe03771?filter=ip
- R2 redémarre en IPv6 : https ://www.cloudshark.org/captures/3d6c6fe03771?filter=ipv6
- Documentation Cisco : Cisco Enhanced Interior Gateway Routing Protocol, Document ID :16406
- RFC 7868 : https ://tools.ietf.org/html/rfc7868

© 2021 François-Emmanuel Goffinet