

IP ROUTING

Routage IPv4/IPv6

[François-Emmanuel Goffinet](#)

Formateur IT

version 15.11

Sommaire

1. Le routeur
2. Prise en main d'un routeur
3. Structure d'une table de routage et routage statique
4. Gestion d'un réseau IPv4
5. Activation et vérification du routage IPv6
6. Protocoles de routage dynamique
7. Labs de routage statique

Objectifs (1/2)

- Décrire les concepts de base du routage
- Commandes permettant d'effectuer la configuration de base du routeur
- Configurer et vérifier l'état de fonctionnement d'une interface Ethernet
- Vérifier la configuration du routeur et la connectivité réseau
- Commandes pour examiner les informations de base du routeur et la connectivité réseau
- Configurer et vérifier la configuration du routage en route statique ou route par défaut
- Différencier les méthodes de routage et les protocoles de routage
- Table de routage IP

Objectifs (2/2)

- Configurer et vérifier DHCP
- Identifier le fonctionnement de base de NAT
- Configurer et vérifier le NAT pour en fonction de besoins donnés
- Configurer et vérifier le NTP comme un client
- Configuration de la connectivité IPv4/IPv6 double pile natif
- Configuration du routage IPv4/IPv6 double pile natif
- Activer le service DNS
- Activer DHCP Relay

Pré-requis

Pour votre meilleur confort de lecture, il est conseillé d'avoir une bonne connaissance des [modèles OSI et TCP/IP](#) ainsi que [la technologie Ethernet et des commutateurs](#) (Cisco).

Vous trouverez une initiation CLI IOS Cisco dans la présentation “[Prise en main d'un commutateur Cisco©](#)”.

1. Le routeur

Introduction

Un routeur est un ordinateur

- Les fonctions de base d'un routeur
 - un **ordinateur** spécialisé dans l'envoi de paquets à travers le réseau de données.
 - Ils sont responsables 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**
- Les routeurs sont le **centre** du réseau.
 - Les routeurs ont généralement (au minimum) deux connexions :
 - une connexion WAN (vers un ISP/FAI)
 - une connexion LAN

Routeurs

- Seuls les routeurs sont capables de transférer les paquets d'une interfaces à une autre.
- Les routeurs limitent les domaines de broadcast sur chacune de leur interface.
- Les routeurs échangent entre eux des informations concernant les différentes destinations (des réseaux à joindre) grâce à des protocoles de routage.

Détermination du chemin

- Les routeurs examinent la destination d'un paquet IP et déterminent le meilleur chemin en fonction des entrées disponibles dans leur table de routage.

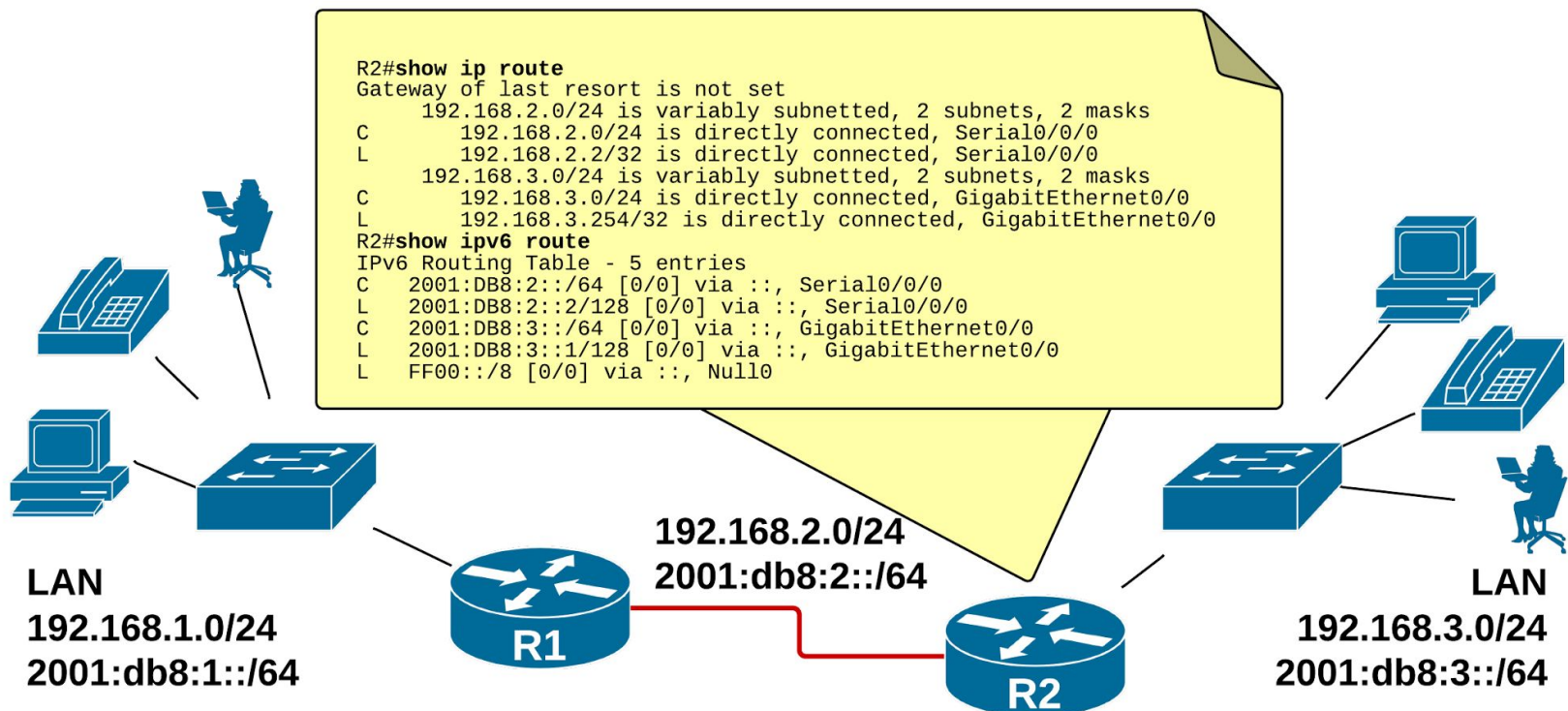
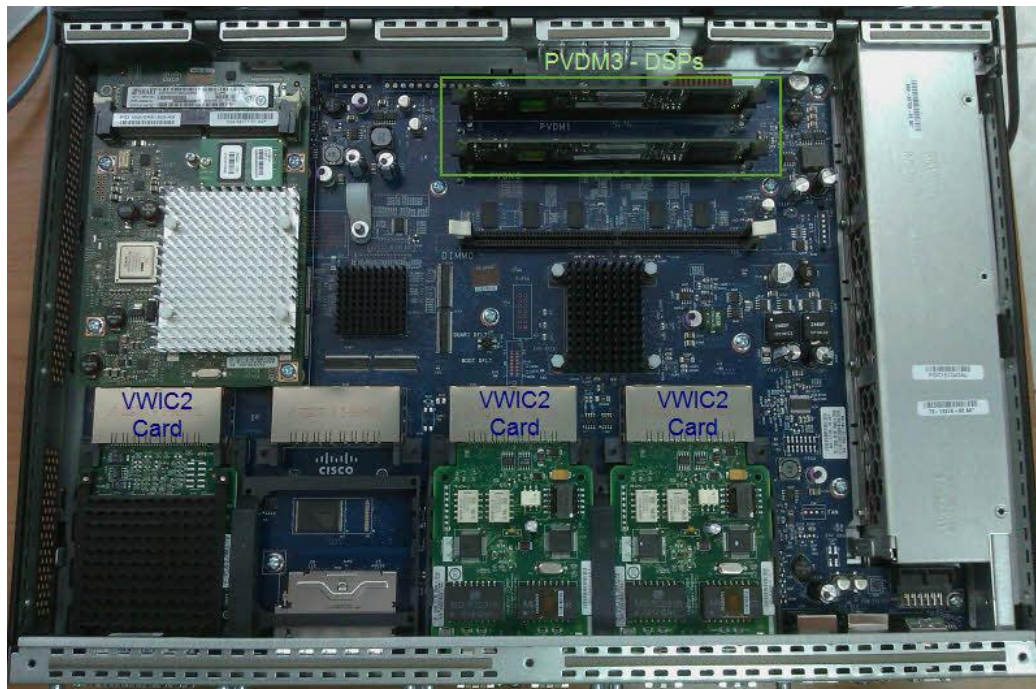


Table de routage par défaut sur R2

Composants d'un routeur

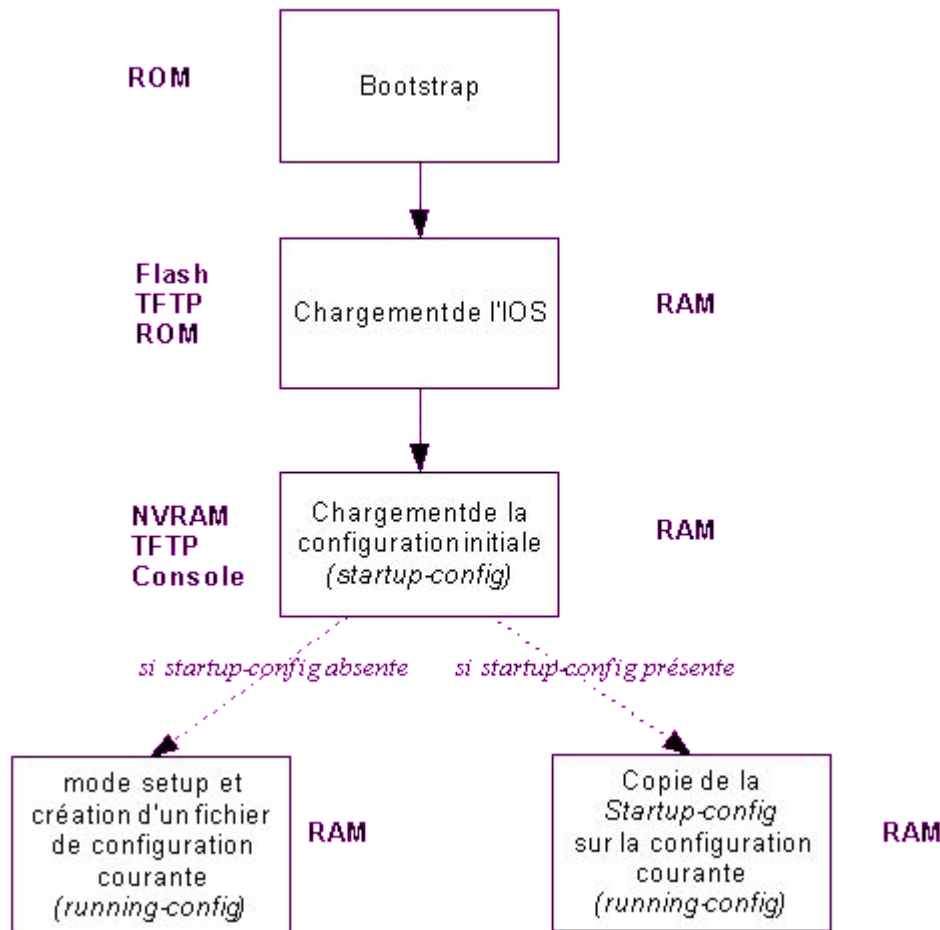
- Software :
 - une sorte de BIOS : ROM Monitor Mode
 - un OS : Cisco IOS
- Hardware :
 - CPU, RAM, NVRAM, Flash, ROM
 - Interfaces



Mémoires

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

Démarrage d'un routeur



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

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 NVRAM
 - La quantité de Flash
 - La licence installée
 - La valeur du registre de configuration

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 CISC01941/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)
```

```
Cont. ...
```

Commande show version

Cont. ...

License Info:

License UDI:

Device#	PID	SN
---------	-----	----

*0	CISCO1941/K9	FTX152420YE
----	--------------	-------------

Technology Package License Information for Module:'c1900'

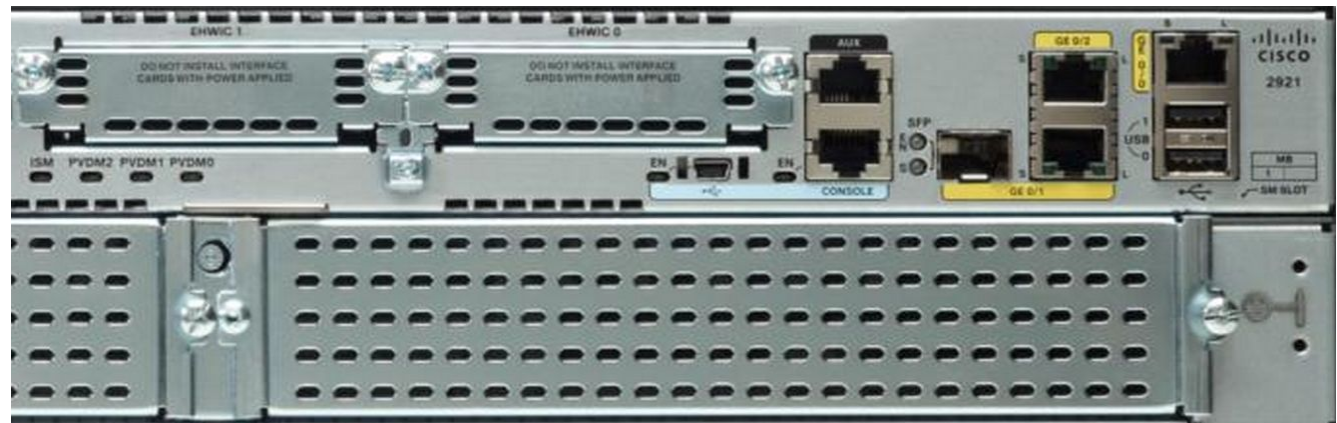
Technology	Technology-package		Technology-package
	Current	Type	Next reboot

ipbase	ipbasek9	Permanent	ipbasek9
security	None	None	None
data	None	None	None

Configuration register is 0x2102

Interface 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
 - Fastethernet
 - Serial
 - DSL
 - ISDN
 - Cable



Interfaces LAN et WAN

- Deux groupes d'interfaces
 - Interface LAN
 - se connecte au réseau LAN
 - Dispose d'une adresse MAC
 - Peut se voir assigné une adresse IPv4 et IPv6
 - Format RJ-45 jack
 - 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



Routeur et couche réseau

Les routeurs utilisent l'adresse IP de destination des paquets pour prendre leur décision de transfert :

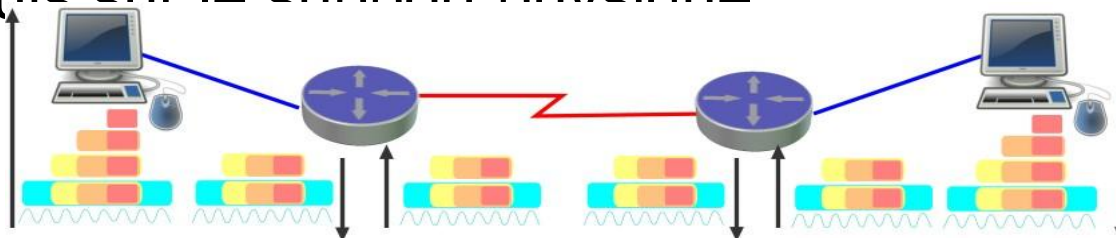
1. Le chemin pris par un paquet est déterminé après consultation de table de routage
2. Ensuite le routeur détermine le meilleur chemin
3. Le paquet est encapsulé en trame, et puis la trame en signal binaire

Encapsulation L1, L2, L3

Les routeurs couvrent les couches 1, 2 et 3 :

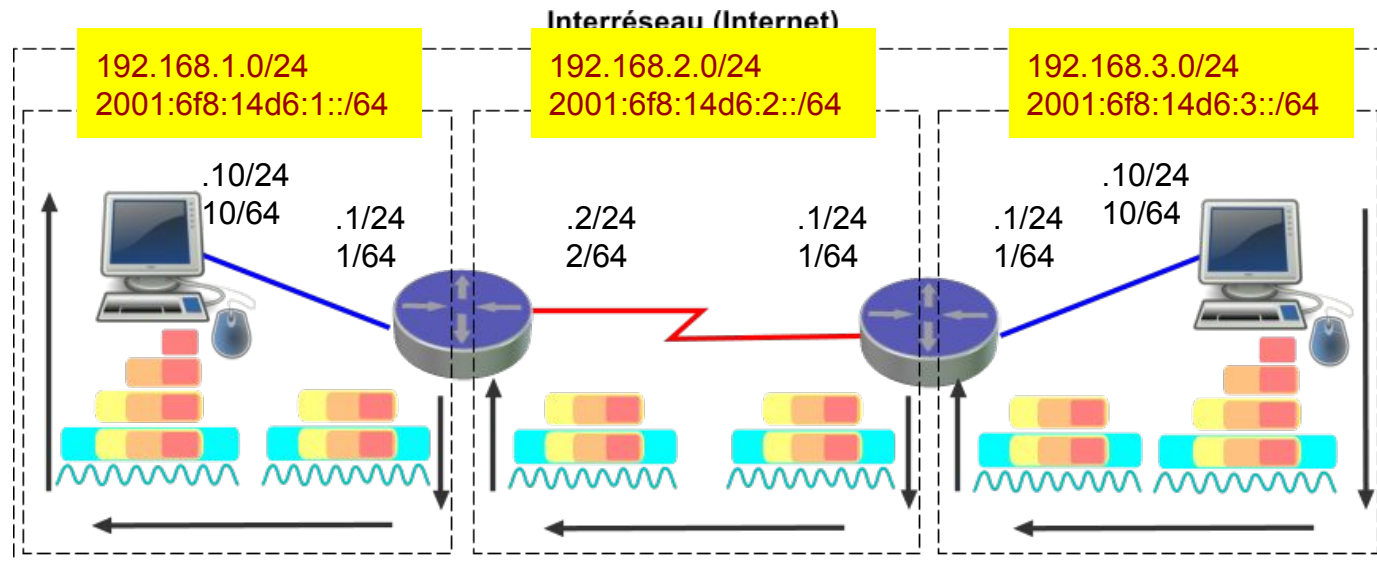
- Ils reçoivent du signal binaire
- Les bits sont décodés et passés à la couche 2
- Il dés-encapsule la trame
- le paquet passe à la couche 3
 - Décision de routage en fonction de l'adresse IP de destination

Le paquet est ré-encapsulé L2 et placé sur l'interface de sortie et puis sur le support physique



Domaine 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.



Routage

Chaque machine de l'intér-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

Sous Windows : `route print`

Sous GNU/Linux/MacOSX : `netstat -r`

Sous Cisco IOS : `show ip route`

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

La passerelle par défaut est configurée statiquement, dynamiquement (IPv4) ou automatiquement (IPv6)

Table de routage

Une table de routage sous Microsoft Windows

```
C:\Windows\system32\cmd.exe
Microsoft Windows [version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\francois>route print -4
=====
Liste d'Interfaces
15...02 50 f2 00 00 01 .....gogo6 Virtual Multi-Tunnel Adapter
11...00 0c 29 5f 11 9f .....Connexion réseau Intel(R) PRO/1000 MT
1.....Software Loopback Interface 1
12...00 00 00 00 00 00 e0 Carte Microsoft ISATAP
13...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
16...00 00 00 00 00 00 e0 Carte Microsoft ISATAP #2
=====

IPv4 Table de routage
=====
Itinéraires actifs :
Destination réseau    Masque réseau    Adr. passerelle    Adr. interface    Métrique
0.0.0.0                0.0.0.0          172.16.124.2       172.16.124.165    10
127.0.0.0              255.0.0.0        On-link            127.0.0.1         306
127.0.0.1              255.255.255.255  On-link            127.0.0.1         306
127.255.255.255        255.255.255.255  On-link            127.0.0.1         306
172.16.124.0           255.255.255.0    On-link            172.16.124.165    266
172.16.124.165         255.255.255.255  On-link            172.16.124.165    266
172.16.124.255         255.255.255.255  On-link            172.16.124.165    266
224.0.0.0              240.0.0.0        On-link            127.0.0.1         306
224.0.0.0              240.0.0.0        On-link            172.16.124.165    266
255.255.255.255        255.255.255.255  On-link            127.0.0.1         306
255.255.255.255        255.255.255.255  On-link            172.16.124.165    266
=====
Itinéraires persistants :
Aucun

C:\Users\francois>
```

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 (`net.ipv4.ip_forward`), cette activation est triviale.
- Sur un routeur Cisco le routage IPv4 est activé par défaut. Par contre, il est désactivé en IPv6.

Modèles de routeurs

On peut s'informer sur les différents catégorie de routeurs chez :

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

Autres informations

- [Câblage sériel, modules et interfaces](#)
- [Commandes IOS de base](#)
- [Configuration générale des routeurs](#)
- [Convention de dénomination des images IOS](#)
- [Exercice de configuration basique des routeurs](#)
- [Le mot de passe 'enable'](#)
- [Méthodes de diagnostic](#)
- [Notions de base sur les routeurs](#)
- [Procédure "Password Recovery"](#)

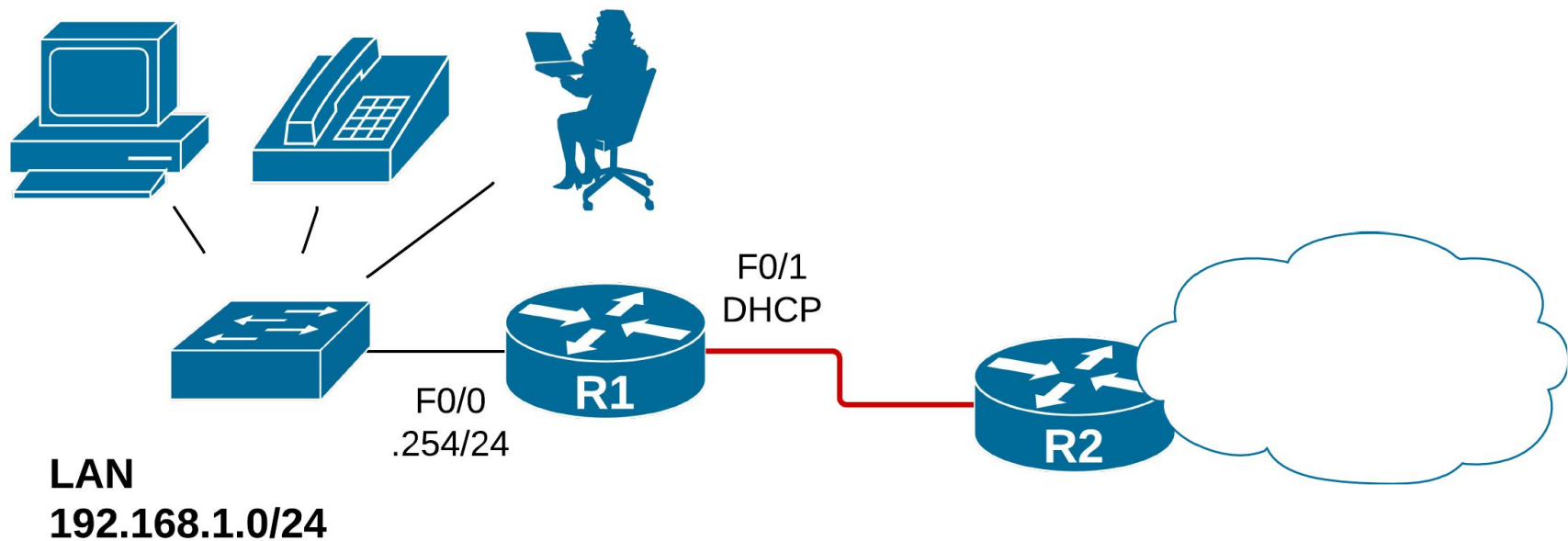
Questions/Réponses

- Séance de question/réponse
- Exercice personnel : examen d'une table de routage locale

2. Prise en main d'un routeur

Configuration IPv4 sans NAT

Topologie IPv4 sans NAT



Dans cette topologie, la passerelle R1 doit être configurée par assurer un service de routage IP vers R2 comme passerelle par défaut. Une configuration NAT n'est pas envisagée ici.

Imaginons que R1 est le routeur connecté en IP/MPLS au routeur central R2.

Méthodologie

1. Configuration de l'infrastructure physique
 - a. Connectique WAN et LAN
 - b. Connectique console (pilotes, putty)
2. Configuration de la connectivité IPv4 sur le routeur :
 - a. Remise à zéro de la configuration
 - b. Configuration IPv4

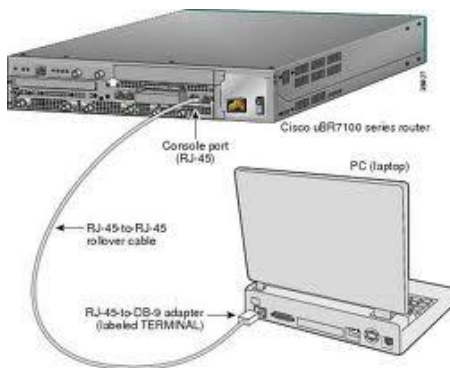
Password Recovery

- A vrai dire, la procédure "password recovery", "recouvrement de mot de passe", ne permet pas de retrouver un mot de passe d'un routeur Cisco.
- Tout au plus, elle permet de reprendre la main sur un routeur dont l'accès est limité par un mot de passe, de le changer ou de le lire si celui-ci n'est pas chiffré.
- En laboratoire, cette procédure nous permettra de travailler sur des machines dont la configuration est vierge.

Voir : http://cisco.goffinet.org/s2/password_recovery

Connexion à la console du routeur

- Câble inversé (roll-over) du port COM1 du PC au routeur sur le port console.
- Lancer un logiciel d'émulation de terminal (putty/hyperterminal) 9600 bauds



Navigation CLI

Passage en mode privilège

```
>enable
```

```
#
```

Passage en mode de configuration globale

```
#configure terminal
```

```
(config) #
```

Configuration d'une interface

```
(config) #interface FastEthernet 0/1
```

```
(config-if) #
```

Passage aux modes inférieurs

```
(config-if) #exit
```

```
(config) #exit
```

```
#
```


Aide au CLI

- Une aide est accessible via le point d'interrogation.
- Les commandes s'auto-complètent avec la touche de tabulation.
- L'environnement indique l'endroit d'une erreur.
- Les commandes s'abrègent si il n'y pas d'ambiguïté.
- En cas d'ambiguïté, l'environnement propose les choix.
- Par défaut les logs apparaissent dans la console, pas en terminal distant.
- raccourcis clavier : on peut faire défiler l'historique des commandes avec les flèches du haut et du bas, on peut revenir au mode privilège directement (CTRL-Z), etc.
- La commande do permet d'exécuter une commande du mode privilège dans un autre mode.

Navigation CLI

Toutes les commandes d'administration s'exécutent en mode privilège :

Commande IOS	Signification
<code>#show running-config</code>	Visualise la configuration courante (RAM)
<code>#show ip interface brief</code>	Visualise l'état des interfaces IPv4
<code>#show ipv6 interface brief</code>	Visualise l'état des interfaces IPv6
<code>#show ipv6 route</code>	Visualise la table de routage IPv6
<code>#copy running-config startup-config</code>	Enregistre la configuration courante
<code>#write memory</code>	Enregistre la configuration courante

Vérification des interfaces

1. Accéder au mode privilège :

```
Router>enable
```

```
Router#
```

2. Vérifier les interfaces :

```
Router#show ip interface brief
```

Interface Protocol	IP-Address	OK?	Method	Status
FastEthernet0/0	unassigned	YES	unset	<u>administratively down</u> <u>down</u>
FastEthernet0/1	unassigned	YES	unset	<u>administratively down</u> <u>down</u>
Vlan1	unassigned	YES	unset	administratively down down

Configuration IPv4

1. Configuration globale
2. Clé SSH
3. Configuration IPv4
 - a. LAN
 - b. WAN (DHCP)
 - c. IP Routing (DHCP)
 - d. DHCP LAN
4. Test de connectivité IPv4

Configuration globale

```
conf t
!  
hostname R1  
enable secret mon_mot_de_passe  
ip domain name entreprise.lan  
!  
line vty 0 4  
    login local  
    transport input ssh  
!  
username root secret mon_autre_mot_de_passe  
!  
ip ssh version 2  
crypto key generate rsa
```

Clé SSH

The name for the keys will be: 0xX00.goffinet.org
Choose the size of the key modulus in the range of 360 to 4096 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 10 seconds)

0xX00(config)#
*Dec 6 00:41:38.574: %SSH-5-ENABLED: SSH 1.99 has been enabled

Commandes de confort

Pour éviter les résolutions DNS inutiles dans la console :

```
(config)#no ip domain-lookup
```

Pour éviter que les messages de logs interrompent votre frappe dans la console :

```
(config)#line con 0
```

```
(config-line)#logging synchronous
```

Pour commenter les interfaces :

```
(config-if)#description Vers le LAN
```

Pour filter des sorties :

```
#show interfaces | include shutdown
```

Connectivité IPv4

```
interface FastEthernet0/0
  description Interface LAN
  ip address 192.168.1.254 255.255.255.0
  no shutdown
```

!

```
interface FastEthernet0/1
  description interface WAN
  ip address dhcp
  no shutdown
```

!

```
ip dhcp excluded-address 192.168.1.1 192.168.1.99
ip dhcp pool LAN_IPv4
  network 192.168.1.0 255.255.255.0
  default-router 192.168.1.254
  dns-server 8.8.8.8
```

!

```
end
```

```
wr
```


Test de la connectivité IPv4

#ping

Protocol [ip]:

Target IP address: www.google.com

Repeat count [5]: Datagram size [100]: Timeout in seconds [2]:

Extended commands [n]: **y**

Source address or interface: **192.168.1.254**

Type of service [0]: Set DF bit in IP header? [no]: Validate reply data?

[no]: Data pattern [0xABCD]: Loose, Strict, Record, Timestamp, Verbose

[none]: Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 173.194.41.146, timeout is 2 seconds:

Packet sent with a source address of 192.168.1.254

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 24/32/52 ms

Vérification de la table de routage IPv4

```
Gateway#show ip route
```

```
Codes: C - connected, S - static, I - IGRP, 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, E - EGP  
       i - IS-IS, 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
```

```
Gateway of last resort is 195.238.2.22 to network 0.0.0.0
```

```
C    192.168.1.0/24 is directly connected, FastEthernet0/0  
    195.238.2.0/30 is subnetted, 1 subnets  
C      195.238.2.20 is directly connected, FastEthernet0/1  
S*    0.0.0.0/0 [1/0] via 195.238.2.22
```

Vérification L2 sur le routeur

show ip interface brief

```
Gateway#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
			L3	L1	L2
FastEthernet0/0	192.168.1.254	YES	manual	up	up
FastEthernet0/1	195.238.2.21	YES	DHCP	up	up
Vlan1	unassigned	YES	unset	administratively down	down

6. Vérification L2 sur le routeur

show interface f0/0

```
Gateway#show interface Fa0/0
FastEthernet0/0 is up, line protocol is up (connected)
  Hardware is Lance, address is 0002.4a05.e001 (bia 0002.4a05.e001)
  Internet address is 192.168.1.254/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 29 bits/sec, 0 packets/sec
  5 minute output rate 26 bits/sec, 0 packets/sec
    13 packets input, 1235 bytes, 0 no buffer
    Received 2 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    11 packets output, 1177 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

adresse MAC
adresse IPv4
Erreurs

3. Structure d'une table de routage

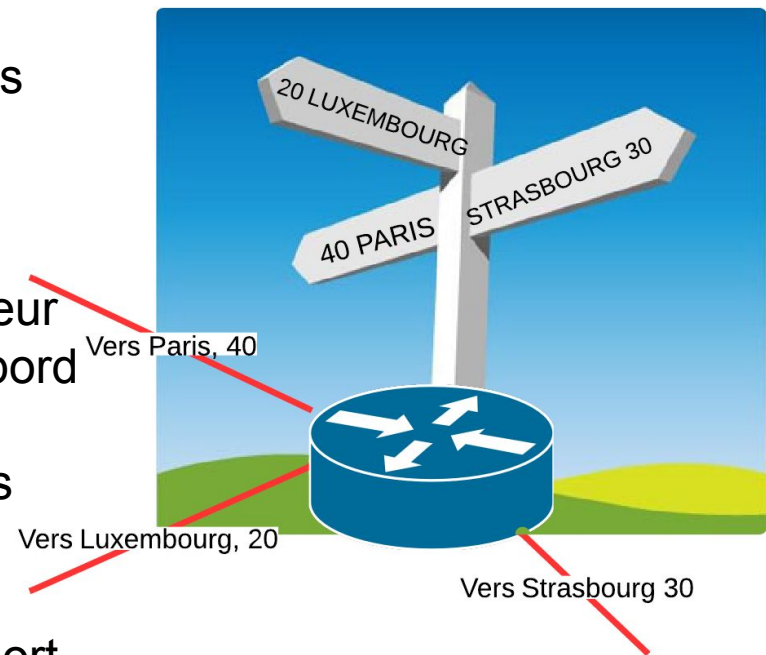
Cisco IOS

Routage

- Les machines qui s'occupent d'acheminer les paquets d'une extrémité à l'autre de l'interréseau sont les **routeurs**
- Ils fondent leurs décisions sur base des **adresses IP** contenues dans les paquets
- Un routeur est un sorte de carrefour muni d'un panneau indicateur (table de routage)
- Ils sont optimisés pour ces tâches (logiciel et matériel)
- Ils commutent les paquets sur la meilleure interface de sortie

Table de routage d'un routeur

Une table de routage est une sorte de "panneau indicateur" qui donne les routes (les réseaux) joignables à partir du "carrefour" que constitue un routeur. Les paquets arrivent sur une interface de la machine. Pour "router" le paquet, le routeur fondera sa décision en deux temps : d'abord il regarde dans l'en-tête IP le réseau de destination et compare toutes les entrées dont il dispose dans sa table de routage; ensuite, si le réseau de destination est trouvé, il commute le paquet sur le bon port de sortie; si ce réseau n'est pas trouvé, le paquet est jeté.



Éléments d'un table de routage

- Un réseau de destination et son masque =
 - une ville
- Une distance administrative/métrique =
 - un kilométrage
- Une passerelle/une interface de sortie =
 - une direction

Les routes avec la métrique la plus faible toujours préférée.

Structure d'une table de routage

- La table de routage fonctionne en RAM et comprend des informations :
 - **Les réseaux directement connectés** - pour tout réseau directement connecté à une interface
 - **Les réseaux distants joignables** - pour tout réseau qui n'est pas directement connecté au routeur
 - **Des informations détaillées** à propos de ces destinations incluent l'adresse du réseau, son masque et l'adresse du prochain saut (routeur) vers la destination
- `show ip route` ou `show ipv6 route` pour afficher la table (activation du routage IPv6
`ipv6 unicast-routing`)

Routes directement connectées

- Comment ajouter un réseau à la table de routage ?
 - en activant une interfaces du routeur
 - Chaque interface d'un routeur est membre d'un réseau différent
 - Activé avec la commande *no shutdown (ipv6 enable)*
 - Notée par un **C** dans la table de routage
 - Pour qu'une route statique ou dynamique soit installée dans la table de routage, il faut au minimum un réseau directement connecté (pour transférer les paquets vers une passerelle)

Routes statiques

- Routes statiques dans la table de routage :
 - la destination: le réseau à joindre et son masque
 - La direction : l'adresse IP de la passerelle ou l'interface de sortie
 - Dénnotée par un **S** dans la table de routage
 - La table doit contenir au moins un réseau directement connecté
- Quand utiliser des routes statiques ?
 - Quand l'inter-réseau n'est constitué que de quelques routeurs
 - Quand le routeur connecte un LAN à un FAI
 - Dans les topologies Hub-and-Spoke (en étoile)

Route statique par défaut

- Une route statique par défaut est celle qui prendra en charge tout trafic qui n'a pas de correspondance spécifique
- Utile au routage Internet
- Dénotée par S^* dans la table :

S^* 0.0.0.0/0 [1/0] via 195.238.2.22

Examen d'une table de routage

● Routes Connected et Static :

Gateway#show ip route

Codes: C - connected, S - static, I - IGRP, 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, E - EGP
i - IS-IS, 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

Gateway of last resort is 195.238.2.22 to network 0.0.0.0

C 192.168.1.0/24 is directly connected, FastEthernet0/0
195.238.2.0/30 is subnetted, 1 subnets
C 195.238.2.20 is directly connected, FastEthernet0/1
S* 0.0.0.0/0 [1/0] via 195.238.2.22

Configuration d'une route statique

```
(config)#ip route network mask {address|interface} [AD]
```

où :

- network : est l'adresse du réseau à joindre
- mask : est le masque du réseau à joindre
- address : est l'adresse du prochain routeur directement connecté pour atteindre le réseau
- interface : est l'interface de sortie du routeur pour atteindre le réseau
- AD : distance administrative optionnelle (1, par défaut)

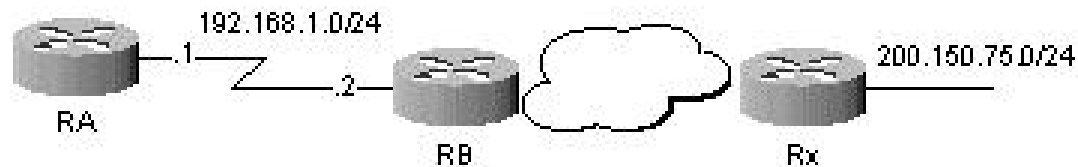
Configuration d'une route statique

Par exemple, à partir du routeur A, le réseau 200.150.75.0/24 est joignable par l'interface de Serial 0/0 par la passerelle (prochaine adresse IP) 192.168.1.2 :

```
RA(config)#ip route 200.150.75.0 255.255.255.0 serial 0/0
```

ou

```
RA(config)#ip route 200.150.75.0 255.255.255.0 192.168.1.2
```



On peut vérifier le routage statique dans la configuration courante du routeur via la commande `#show running-config` .

Notons qu'une route a toujours une métrique de 0. Le réseau à joindre est censé être directement connecté.

Routes dynamiques

- Protocoles de routage dynamique
 - Ajoutent des destinations dans la table de routage
 - Découvrent de nouveaux réseaux
 - Mettent à jour et maintiennent les tables de routage
- Découverte automatique des réseaux
 - Les routeurs sont capables de découvrir de nouveaux réseaux en partageant des informations sur les tables de routage.

Protocoles de routage

- Maintenance de la table de routage
 - Les protocoles de routage dynamiques sont utilisés pour se partager des informations sur la topologie du réseau et maintenir leur table de routage.
- Exemple de protocoles de routage :
 - RIP
 - EIGRP
 - OSPFv2
 - OSPFv3

En conclusion : 3 principes

1. Les routeurs prennent leurs décisions de manière autonome, en se basant sur les informations de la table de routage
2. Chaque table de routage peut contenir des informations différentes
3. Une table de routage peut indiquer comment atteindre une destination mais pas son retour

4. Gestion d'un réseau IPv4

Services IPv4 à déployer sur le LAN

Services IPv4 à déployer sur le LAN :

- Adressage double : privé/public
- NAT overload
- DHCP
- DNS (cache pour le LAN)
- NTP (client)
- Auto Secure

NAT

Le NAT permet de traduire :

les adresses *internes* (inside)

privée (local) en

publique (global)

les adresses externes (outside)

Le routeur NAT tient une table de traduction

Il transforme le trafic : il remplace les en-têtes IPv4 et de couche transport (UDP/TCP).

Rôle du NAT/PAT

Ici, établir la connectivité IPv4 entre un réseau privé et l'Internet adressé globalement :

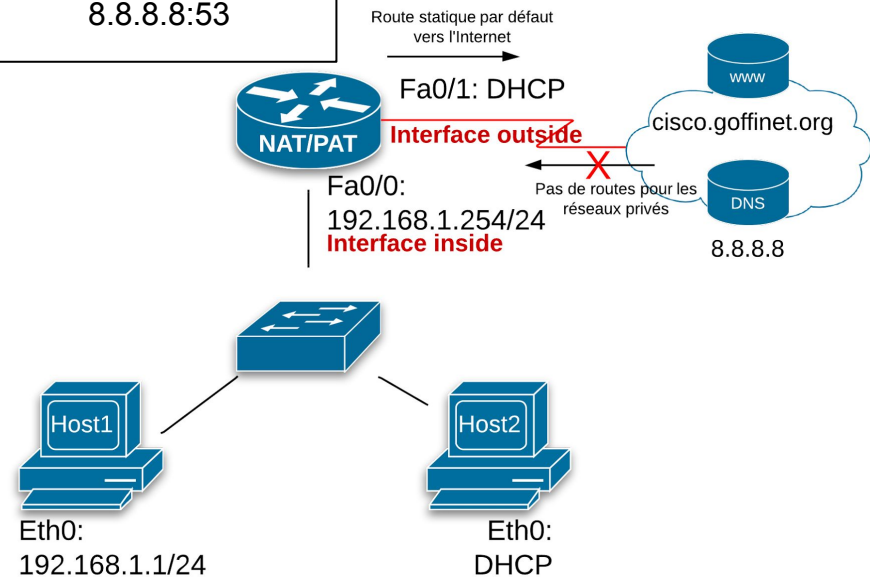
Pro	Inside global	Inside local	Outside local	Outside global
udp	195.238.2.21:1029	192.168.1.11:1029	8.8.8.8:53	8.8.8.8:53
udp	195.238.2.21:1025	192.168.1.12:1025	8.8.8.8:53	8.8.8.8:53
udp	195.238.2.21:1024	192.168.1.13:1025	8.8.8.8:53	8.8.8.8:53

En maintenant une table de correspondance

- Protocole
- Adresse
- Port

Deux côtés :

- Inside
- Outside



Configuration du NAT/PAT

1. Quel trafic à traduire ?

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

2. Création de la règle :

```
Gateway(config) #ip nat inside source list 1 interface f0/1  
overload
```

3. Définition Inside / Outside :

```
Gateway(config) #interface f0/0  
Gateway(config-if) #ip nat inside  
Gateway(config-if) #exit  
Gateway(config) #interface f0/1  
Gateway(config-if) #ip nat outside  
Gateway(config-if) #exit  
Gateway(config) #
```

Logique de configuration sur Cisco IOS

1. Quel trafic à traduire ?

- Le trafic ayant pour IP_SOURCE 192.168.1.0/24

2. Création de la règle :

- **Traduire** dans le trafic venant de l'**intérieur**
- ayant pour IP_SOURCE 192.168.1.0/24
- par l'adresse IP de l'interface f0/1 (195.238.2.21)
- avec du PAT.

3. Définition Inside / Outside :

- L'interface f0/0 sera du côté "intérieur".
- L'interface f0/1 sera du côté "extérieur".

Vérification du NAT

A partir du routeur, générer du trafic prenant l'adresse IP de l'interface LAN F0/0 comme origine avec la commande ping.

Vérification du NAT/PAT

```
Gateway#ping
Protocol [ip]:
Target IP address: 195.238.2.21
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.1.254
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 195.238.2.21, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.254
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/6 ms
```

Vérification du NAT/PAT

Gateway#**show ip nat translations**

Pro	Inside global	Inside local	Outside local	Outside
global				
icmp	195.238.2.21:11	192.168.1.254:11	195.238.2.22:11	195.238.2.22:
11				
icmp	195.238.2.21:12	192.168.1.254:12	195.238.2.22:12	195.238.2.22:
12				
icmp	195.238.2.21:13	192.168.1.254:13	195.238.2.22:13	195.238.2.22:
13				
icmp	195.238.2.21:14	192.168.1.254:14	195.238.2.22:14	195.238.2.22:
14				
icmp	195.238.2.21:15	192.168.1.254:15	195.238.2.22:15	195.238.2.22:
15				

- Inside = Champs IP_SOURCE
- Local = interface inside
- Global = interface outside

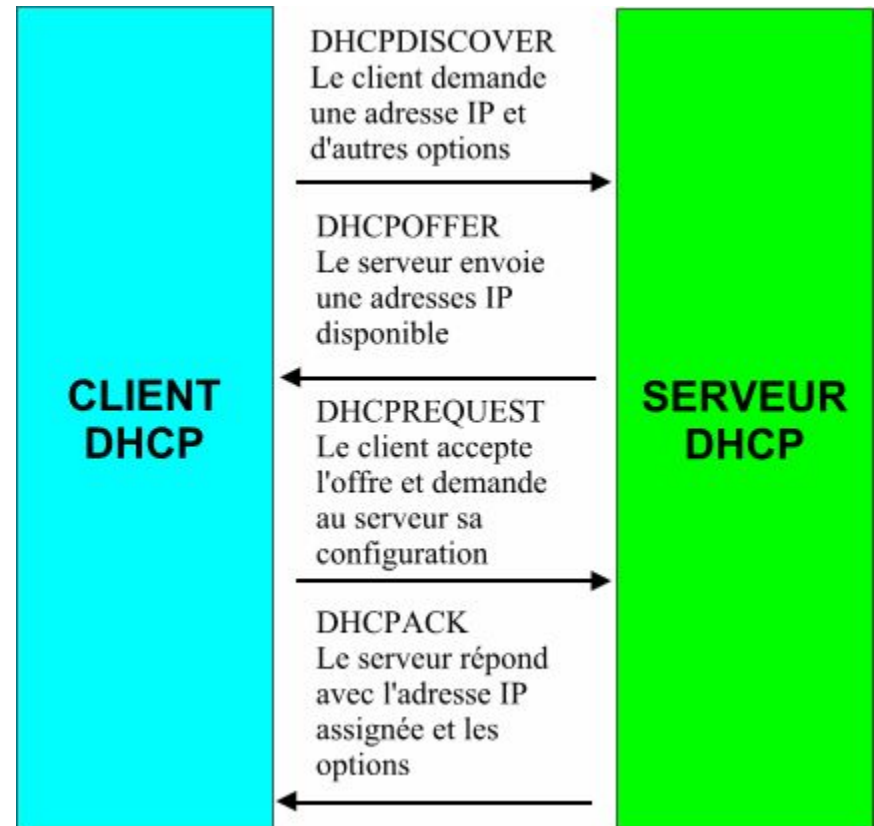
Rôle du service DHCP

Dynamic Host Configuration Protocol (DHCP)

Un serveur (UDP 67) offre aux clients qui le demandent un bail pour des paramètres et des options TCP/IP :

- Adresse IP
- Masque
- Passerelle
- Adresse du serveur de noms
- et d'autres

La négociation débute en broadcast.



Échanges DHCP

N ▼	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	314	DHCP Discover - Transaction ID 0x3d1d
2	0.000295	192.168.0.1	192.168.0.10	DHCP	342	DHCP Offer - Transaction ID 0x3d1d
3	0.070031	0.0.0.0	255.255.255.255	DHCP	314	DHCP Request - Transaction ID 0x3d1e
4	0.070345	192.168.0.1	192.168.0.10	DHCP	342	DHCP ACK - Transaction ID 0x3d1e

▼ Bootstrap Protocol (Offer)

Message type: Boot Reply (2)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x00003d1d
Seconds elapsed: 0
‣ Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0 (0.0.0.0)
Your (client) IP address: 192.168.0.10 (192.168.0.10)
Next server IP address: 192.168.0.1 (192.168.0.1)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: Grandstr_01:fc:42 (00:0b:82:01:fc:42)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP

- Option: (53) DHCP Message Type (Offer)
- Option: (1) Subnet Mask
- Option: (58) Renewal Time Value
- Option: (59) Rebinding Time Value
- Option: (51) IP Address Lease Time
- Option: (54) DHCP Server Identifier
- Option: (255) End

Serveur DHCP Cisco IOS

```
Gateway(config)#ip dhcp pool GW  
Gateway(dhcp-config)#network 192.168.1.0 255.255.255.0  
Gateway(dhcp-config)#default-router 192.168.1.254  
Gateway(dhcp-config)#dns-server 8.8.8.8  
Gateway(dhcp-config)#exit  
Gateway(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
```

Diagnostic DHCP

- Dans la console du routeur :
show ip dhcp bindings
- Analyse de paquets DHCP

Cache DNS pour le LAN

Activer la résolution de nom et le service :

```
(config)# ip domain lookup  
(config)# ip name-server x.x.x.x  
(config)# ip dns server
```

Adapter la configuration DHCP :

```
(config)#ip dhcp pool GW  
(dhcp-config)#dns-server 192.168.1.254  
(dhcp-config)#exit
```


Network Time Protocol

Le Protocole d'Heure Réseau (Network Time Protocol ou NTP) est un protocole qui permet de synchroniser, via un réseau informatique, l'horloge locale d'ordinateurs sur une référence d'heure.

La version 3 de NTP est la plus répandue à ce jour. Elle est formalisée par la RFC 1305.

http://fr.wikipedia.org/wiki/Network_Time_Protocol

<http://www.pool.ntp.org/fr/>

Configuration de NTP (client)

Configuration client NTP :

```
ntp server <ip_address>
```

Vérification du statut NTP :

```
show clock
```

```
show calendar
```

```
show ntp status
```

```
show ntp associations
```

Auto Secure

```
#auto secure
```

```
--- AutoSecure Configuration ---
```

```
*** AutoSecure configuration enhances the security of  
the router, but it will not make it absolutely resistant  
to all security attacks ***
```

AutoSecure will modify the configuration of your device.
All configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
Autosecure documentation.

At any prompt you may enter '?' for help.

Use ctrl-c to abort this session at any prompt.

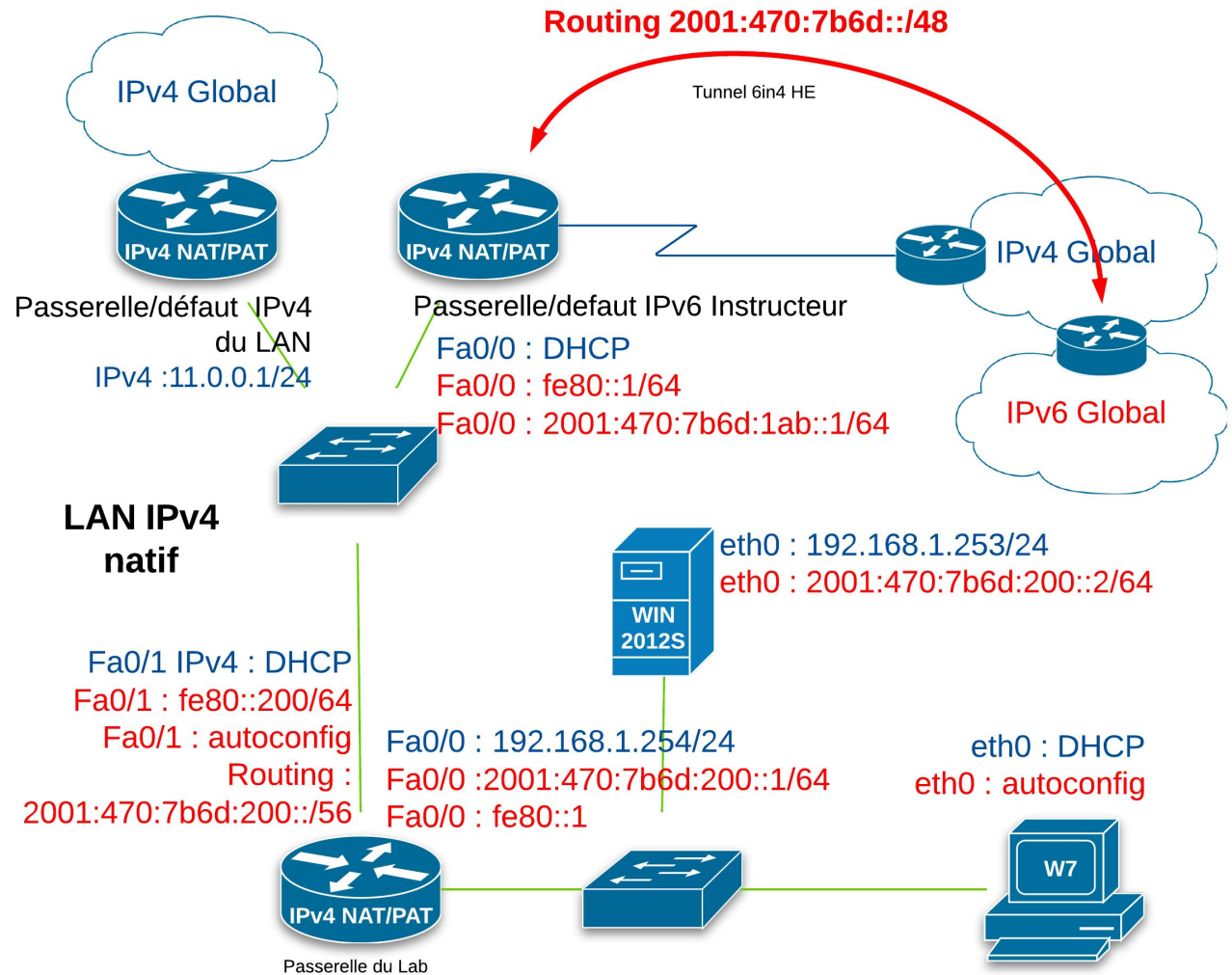
Gathering information about the router for AutoSecure

...

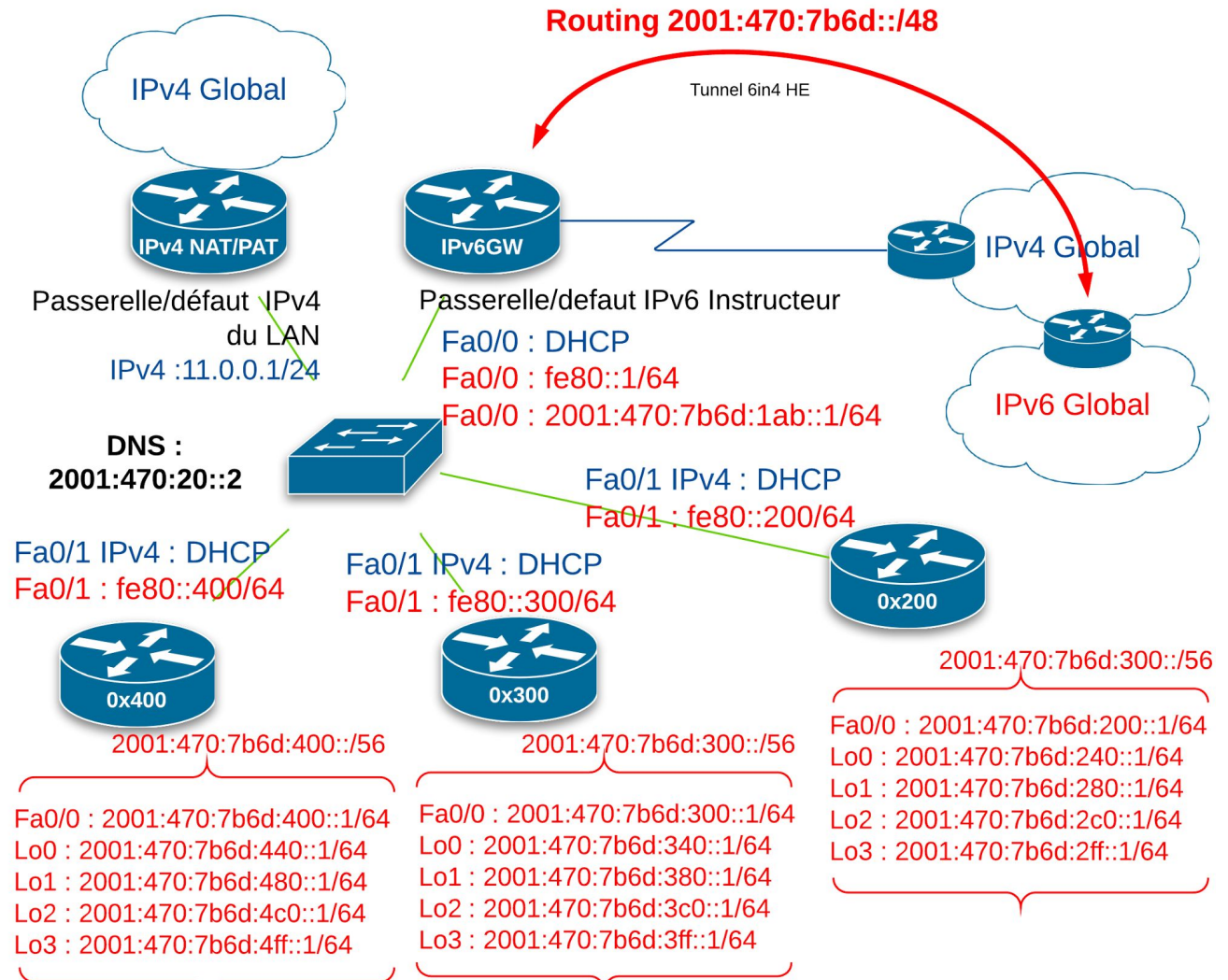
5. Activation et vérification du routage IPv6

Topologie personnelle

Pour l'équipe
0x200



Topologie du lab



Plan d'adressage

Équipe	Réseau routé	Fa0/1 WAN	Fa0/0 LAN	
0x100	0x100::/56 (Réservé)	-	fe80::1/64 2001:470:7b6d:1lab::1/64	
0x200	0x200::/56	fe80::200/64 autoconfig	fe80::1/64 2001:470:7b6d:200::1/64	2001:470:7b6d:280::1/64 2001:470:7b6d:2ff::1/64
0x300	0x300::/56	fe80::300/64 autoconfig	fe80::1/64 2001:470:7b6d:300::1/64	2001:470:7b6d:380::1/64 2001:470:7b6d:3ff::1/64
0x400	0x400::/56	fe80::400/64 autoconfig	fe80::1/64 2001:470:7b6d:400::1/64	2001:470:7b6d:480::1/64 2001:470:7b6d:4ff::1/64
0x500	0x500::/56	fe80::500/64 autoconfig	fe80::1/64 2001:470:7b6d:500::1/64	2001:470:7b6d:580::1/64 2001:470:7b6d:5ff::1/64
0x600	0x600::/56	fe80::600/64 autoconfig	fe80::1/64 2001:470:7b6d:600::1/64	2001:470:7b6d:680::1/64 2001:470:7b6d:6ff::1/64
0x700	0x700::/56	fe80::700/64 autoconfig	fe80::1/64 2001:470:7b6d:700::1/64	2001:470:7b6d:780::1/64 2001:470:7b6d:7ff::1/64

Configuration IPv4

1. Configuration globale
2. Clé SSH
3. Configuration IPv4
 - a. LAN
 - b. WAN (DHCP)
 - c. IP Routing (DHCP)
 - d. NAT
 - e. DHCP LAN
 - f. DNS LAN
4. Test de connectivité IPv4

Configuration IPv6

- Interface WAN IPv6
- Interface LAN IPv6
- Routage IPv6

Interface WAN IPv6

```
interface FastEthernet0/1
```

```
ipv6 enable
```

```
do sh ipv6 int brie
```

```
!
```

```
ipv6 address FE80::X00 link-local
```

```
do sh ipv6 int brie
```

```
!
```

```
ipv6 address autoconfig
```

```
do sh ipv6 int brie
```

Interface LAN IPv6

```
interface FastEthernet0/0  
  ipv6 enable  
  ipv6 address 2001:470:7B6D:200::1/64  
  ipv6 address FE80::1 link-local
```

Route IPv6

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

```
(config)#
```

```
ipv6 route ::/0 FastEthernet0/1 FE80::1
```

Table de routage IPv6

```
#show ipv6 route
```

```
IPv6 Routing Table - default - 10  
entries
```

```
Codes: C - Connected, L - Local, S  
- Static, NDp - ND Prefix
```

```
S    ::/0 [1/0]
```

```
    via FE80::1, FastEthernet0/1
```

```
NDp 2001:470:7B6D:1AB::/64 [2/0]
```

```
    via FastEthernet0/1, directly  
connected
```

```
L    2001:470:7B6D:1AB::200/128  
[0/0]
```

```
    via FastEthernet0/1, receive
```

```
C    2001:470:7B6D:200::/64 [0/0]
```

```
    via FastEthernet0/0, directly  
connected
```

```
L    2001:470:7B6D:200::1/128 [0/0]
```

```
    via FastEthernet0/0, receive
```

```
C    2001:470:7B6D:201::/64 [0/0]
```

```
    via Loopback0, directly  
connected
```

```
L    2001:470:7B6D:201::1/128 [0/0]
```

```
    via Loopback0, receive
```

```
C    2001:470:7B6D:2FF::/64 [0/0]
```

```
    via Loopback1, directly  
connected
```

```
L    2001:470:7B6D:2FF::1/128 [0/0]
```

```
    via Loopback1, receive
```

```
L    FF00::/8 [0/0]
```

```
    via Null0, receive
```

Vérification du routage

```
#ping
Protocol [ip]: ipv6
Target IPv6 address: www.google.com
Repeat count [5]: Datagram size [100]: Timeout in seconds [2]:
Extended commands? [no]: y
Source address or interface: fastethernet0/0
UDP protocol? [no]: Verbose? [no]: Precedence [0]: DSCP [0]: Include hop
by hop option? [no]: Include destination option? [no]: Sweep range of
sizes? [no]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2A00:1450:4007:803::1014, timeout is 2
seconds:
Packet sent with a source address of 2001:470:7B6D:200::1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 136/276/408 ms
```

Adresse IPv6 (1/2)

```
#show ipv6 interface f0/0
```

```
FastEthernet0/0 is up, line protocol is up
```

```
IPv6 is enabled, link-local address is FE80::C802:CFF:FE9D:8
```

```
No Virtual link-local address(es):
```

```
Global unicast address(es):
```

```
2001:470:CBF7:200::1, subnet is 2001:470:7B6D:200::/64
```

```
Joined group address(es):
```

```
FF02::1
```

```
FF02::2
```

```
FF02::1:FF00:1
```

```
FF02::1:FF9D:8
```

```
MTU is 1500 bytes
```

```
ICMP error messages limited to one every 100 milliseconds
```

```
ICMP redirects are enabled
```

```
ICMP unreachablees are sent
```

```
ND DAD is enabled, number of DAD attempts: 1
```

```
ND reachable time is 30000 milliseconds (using 30000)
```

```
ND RAs are suppressed (periodic)
```

Hosts use stateless autoconfig for addresses.

Adresses IPv6

```
#sh ipv6 interface f0/0
```

```
FastEthernet0/0 is up, line protocol is up
```

```
IPv6 is enabled, link-local address is FE80::1
```

```
No Virtual link-local address(es):
```

```
Global unicast address(es):
```

```
2001:470:CBF7:200::1, subnet is 2001:470:7B6D:200::/64
```

```
Joined group address(es):
```

```
FF02::1
```

```
FF02::2
```

```
FF02::1:FF00:1
```

```
MTU is 1500 bytes
```

```
ICMP error messages limited to one every 100 milliseconds
```

```
ICMP redirects are enabled
```

```
ICMP unreachablees are sent
```

```
ND DAD is enabled, number of DAD attempts: 1
```

```
ND reachable time is 30000 milliseconds (using 30000)
```

```
ND RAs are suppressed (periodic)
```

```
Hosts use stateless autoconfig for addresses.
```


Vérification terminale

Test de base IPv6 :

ipconfig, netsh interface ipv6 ..., ping, tracert

Firefox, plugin show IP, google, <http://test-ipv6.com/>, youtube, lesoir

1. Test Dual-Stack
2. Fixez l'adresse IPv4 sans DNS IPv4
3. Désactivez IPv4

Etapes suivantes ..

- Configuration des clients IPv6
- DHCPv6 Stateless
 - Configuration RA flag O
- DHCPv6 Stateful
 - Configuration RA flag M et O
 - Désactivation de l'autoconfiguration
- Pare-feu IPv4/IPv6

Dans les présentations :

- [ICND1 Protocole IPv6](#)
- [ICND1 Firewalls et ACLs IPv4 IPv6](#)

6. Protocoles de routage dynamique

Principes, classification, métrique, distance administrative

Objectifs

- Décrire le rôle des protocoles de routage dynamiques.
- Catégoriser les protocoles de routage.
- Identifier, décrire et expliquer les notions de métrique et de distance administrative

Objectifs des protocoles de routage

- Découvrir dynamiquement les routes vers les réseaux d'un interréseau et les inscrire dans la table de routage.
- S'il existe plus d'une route vers un réseau, inscrire la meilleure route dans la table de routage.
- Détecter les routes qui ne sont plus valides et les supprimer de la table de routage.
- Ajouter le plus rapidement possible de nouvelles routes ou remplacer le plus rapidement les routes perdues par la meilleure route actuellement disponible.

Fonctionnement

Un protocole de routage transporte notamment des informations sur les différentes routes dans l'intér-réseau mais aussi des messages de maintien de relations de voisinage

Chaque routeur reçoit et envoie des informations de routage.

Il applique un algorithme qui optimise ces informations en chemins cohérents.

Statique c. dynamique

Avantages du routage statique

- Peut servir de mécanisme de backup
- Facile à configurer
- Aucune ressource supplémentaire nécessaire
- Plus sécurisé

Désavantages du routage statique

- Chaque changement dans la topologie nécessite une intervention manuelle sur les routeurs
- Cette méthode ne convient à la croissance des réseaux larges

AS, routage intérieur et extérieur

- Un système autonome (AS) est un ensemble de réseaux sous la même autorité administrative (autorité de gestion).
- Au sein d'un système autonome, les routes sont générées par des protocoles de routage intérieurs comme RIP, EIGRP, OSPF ou ISIS.
- Les protocoles de routage qui permettent de connecter les systèmes autonomes entre eux sont des protocoles de routage extérieurs comme EGP ou BGP.
- Dans le contexte de l'interconnexion mondiale des réseaux, l'IANA assigne un numéro d'AS (16/32 bits).

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. Ils 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 comme étant représentatif. EIGRP est aussi un protocole à vecteur de distance entièrement optimisé par Cisco Systems.

Protocole de routage à état de liens

Un protocole de routage à état de liens utilise un algorithme plus efficace (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. On citera OSPF et IS-IS. Ils convergent très rapidement. Les routeurs entretiennent des relations de voisinage maintenues.

EIGRP

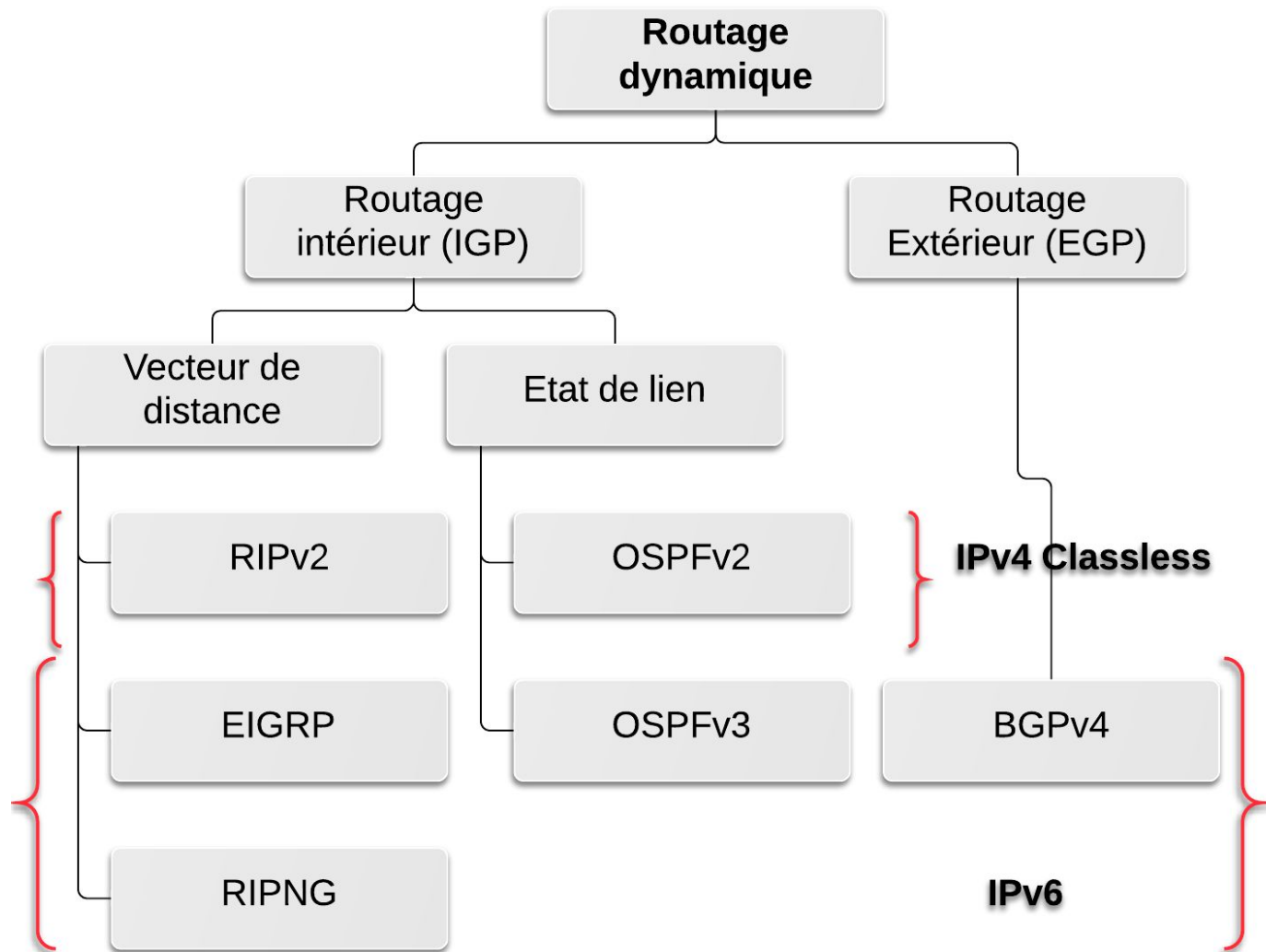
- Protocole propriétaire Cisco
- Protocole à vecteur de distance (algorithme DUAL) sans boucles
- Multi-protocoles
- Simple à configurer et à maintenir
- Relations de voisinage
- Routes de backup
- Répartition de charge inégale
- Convergence rapide

Routage Classful

Les protocoles classful n'embarquent pas d'informations sur les masques des réseaux.

RIPv1 et IGRP (Cisco) sont aujourd'hui des protocoles obsolètes.

Classification des protocoles de routage



Convergence

La convergence est le temps pour qu'un ensemble de routeurs puissent avoir une vision homogène, complète et efficace de l'ensemble des routes d'un interrèseau. Le temps de convergence est particulièrement éprouvé lorsqu'il y a des modifications topologiques dans l'interrèseau.

Métrique

La métrique d'une route est la valeur d'une route en comparaison d'autres routes apprises par le protocole de routage. Plus sa valeur est faible, meilleure est la route. Chaque protocole dispose de sa méthode de valorisation. On peut trouver toute une série de composante de métrique parmi :

- nombre de sauts (RIP)
- bande passante (EIGRP)
- délai (EIGRP)
- charge (EIGRP)
- fiabilité (EIGRP)
- coût (OSPF)

Répartition de charge

Ce que l'on appelle communément “Load Balancing” est la capacité pour un routeur de supporter plusieurs chemins à coût égaux vers une destination. Il en résulte que les paquets vers une même destination sont répartis sur plusieurs interfaces.

Le protocole EIGRP est capable de répartir la charge sur des liens inégaux sous certaines conditions.

Distance administrative d'un route

La distance administrative est la préférence dans une table de routage pour des routes apprises par un protocole de routage par rapport aux mêmes routes apprises par un autre protocole de routage.

Plus la valeur est faible et plus le protocole est préféré.

Par défaut, une route EIGRP sera préférée à une route RIP; une route statique sera préférée à toute autre route dynamique.

Valeurs par défaut

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

Identification dans la table de routage

1.0.0.0/32 is subnetted, 3 subnets

R 1.1.1.1 [120/1] via 10.1.1.1, 00:00:15, FastEthernet0/0

R 1.3.3.3 [120/1] via 10.1.1.1, 00:00:15, FastEthernet0/0

R 1.2.2.2 [120/1] via 10.1.1.1, 00:00:15, FastEthernet0/0

2.0.0.0/32 is subnetted, 1 subnets

C 2.2.2.2 is directly connected, Loopback0

33.0.0.0/32 is subnetted, 1 subnets

O 33.33.33.33 [110/2] via 10.2.2.3, 00:01:08, FastEthernet1/0

111.0.0.0/32 is subnetted, 1 subnets

D 111.111.111.111 [90/156160] via 10.1.1.1, 00:01:23,
FastEthernet0/0

10.0.0.0/24 is subnetted, 2 subnets

C 10.2.2.0 is directly connected, FastEthernet1/0

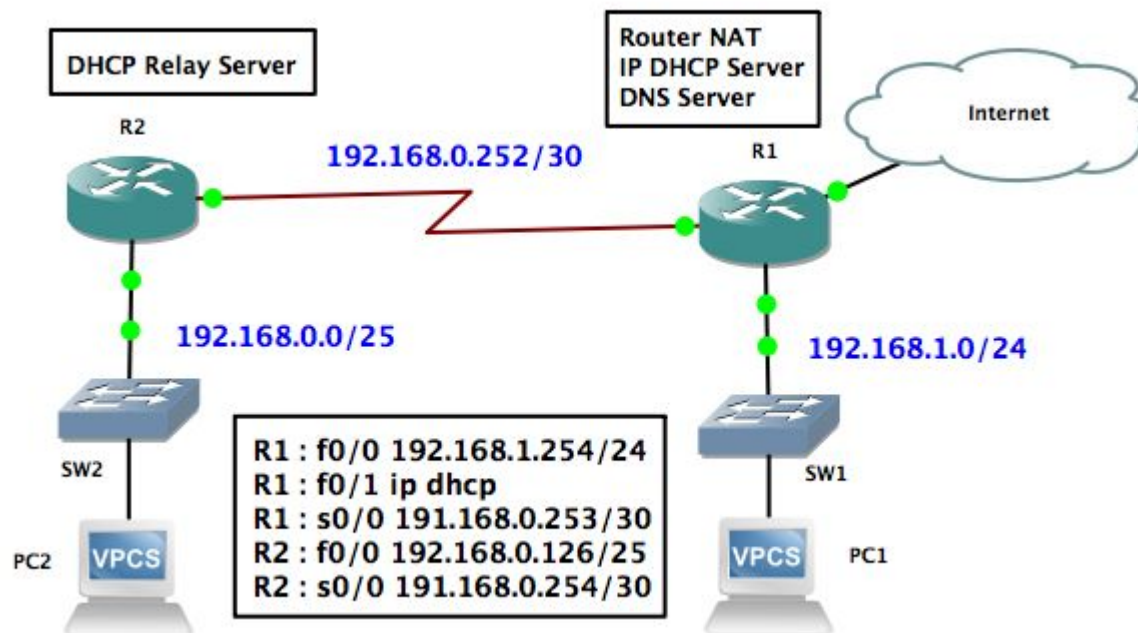
C 10.1.1.0 is directly connected, FastEthernet0/0

Synthèse IGP

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 <i>areas</i>
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)	OSPFv2/v3 - IP89 - 224.0.0.5, 224.0.0.6, FF02::5, FF02::6 IS-IS

7. Labs de routage statique

Topologie de Lab IPv4



On combine ici les deux exemples IPv4 de la présentation pour déployer le routage et les services internes.

R1 est le routeur central qui connecte l'Internet, Il fait office de routeur PAT overload, de serveur DHCP pour les deux LANs, et de serveur DNS pour la topologie. Le pare-feu n'est pas envisagé ici.

R2 est un routeur distant sur une connexion privée. Il fait office de serveur DHCP Relay. Le routage statique IPv4 est configuré sur les deux routeurs.

Etapes de configuration

Sur R1 :

- Configuration des interfaces
- Configuration du routage statique
- Configuration du NAT
- Configuration du service DNS
- Configuration du service NTP
- Configuration du service DHCP

Sur R2 :

- Configuration des interfaces
- Configuration du routage statique
- Configuration DHCP relay

R1 : Interfaces et routage

```
hostname R1
interface FastEthernet0/0
  ip address 192.168.1.254 255.255.255.0
  no shutdown
interface Serial0/0
  ip address 192.168.0.253 255.255.255.252
  no shutdown
interface FastEthernet0/1
  ip address dhcp
  no shutdown
ip route 192.168.0.0 255.255.255.128 192.168.0.254
```


R1 : NAT

```
ip nat inside source list nat interface
FastEthernet0/1 overload
ip access-list standard nat
    permit 192.168.1.0 0.0.0.255
    permit 192.168.0.0 0.0.0.255
interface FastEthernet0/0
    ip nat inside
interface FastEthernet0/1
    ip nat outside
```

R1 : DNS et NTP

```
no ip domain-lookup
```

```
!
```

```
ip dns server
```

```
!
```

```
ip name-server 8.8.8.8
```

```
!
```

```
ntp server pool.ntp.org
```

R1 : DHCP

```
ip dhcp pool LAN
    network 192.168.1.0 255.255.255.0
    default-router 192.168.1.254
    dns-server 192.168.1.254
!
ip dhcp pool LAN2
    network 192.168.0.0 255.255.255.128
    default-router 192.168.0.126
    dns-server 192.168.1.254
```

R2 : Solution

```
hostname R2
interface FastEthernet0/0
  ip address 192.168.0.126 255.255.255.128
  ip helper-address 192.168.0.253
  no shutdown
interface Serial0/0
  ip address 192.168.0.254 255.255.255.252
  no shutdown
ip route 0.0.0.0 0.0.0.0 192.168.0.253
end
```

DHCP Relay

Un choix de conception centralise le service DHCP sur R1. Par défaut le R2 bloque les requêtes DHCP adressée en broadcast (255.255.255.255).

Pour “relayer” en Unicast le message DHCP Discover auprès de R1, on réalise la tâche suivante :

```
R2(config)# interface FastEthernet0/0
```

```
R2(config-if)# ip helper-address 192.168.0.253
```

On peut observer le processus de démarrage DHCP sur [R2 à partir son interface f0/0](#) et [de son interface s0/0](#).

Veuillez comparer les deux captures.

Diagnostic PC2

```
PC2> ip dhcp
```

```
DDORA IP 192.168.0.1/25 GW 192.168.0.126
```

```
PC2> ping www.google.com
```

```
www.google.com resolved to 194.78.99.180
```

```
84 bytes from 194.78.99.180 icmp_seq=1 ttl=126 time=40.344 ms
```

```
84 bytes from 194.78.99.180 icmp_seq=2 ttl=126 time=95.318 ms
```

```
84 bytes from 194.78.99.180 icmp_seq=3 ttl=126 time=21.551 ms
```

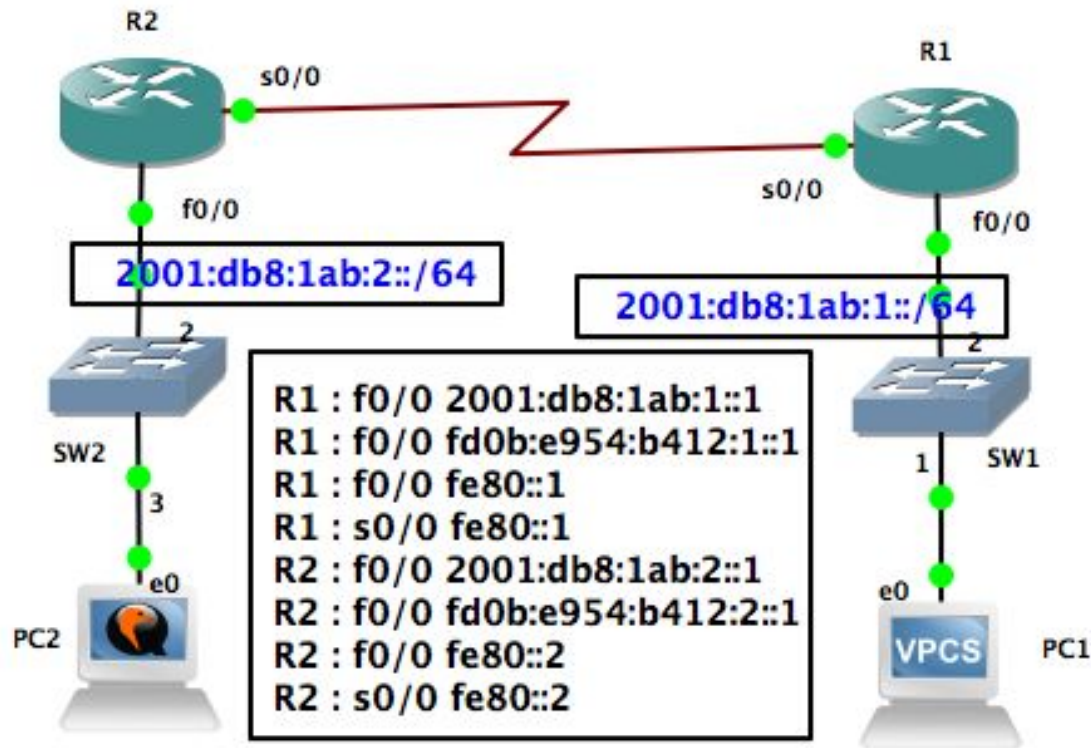
```
84 bytes from 194.78.99.180 icmp_seq=4 ttl=126 time=31.208 ms
```

```
84 bytes from 194.78.99.180 icmp_seq=5 ttl=126 time=23.841 ms
```

Diagnostic routeurs

```
# show interface f0/0
# show interface s0/0
# show controllers s0/0
# show ip interface brief
# show ip interface f0/0
# show ip route
# show ip nat translations
# show ip dhcp binding
# show ntp status
```

Topologie routage IPv6



Voici un lab de routage IPv6 minimal avec de l'adressage global, ULA et Link-local. SLAAC est automatiquement activé !

Étapes de configuration

1. Configuration de interfaces LAN et WAN
2. Activation du routage IPv6
3. Configuration du routage statique
4. Vérifications IPv6
5. Configuration DHCPv6 stateless

Solution R1

```
hostname R1
ipv6 unicast-routing
interface FastEthernet0/0
    ipv6 address FE80::1 link-local
    ipv6 address 2001:DB8:1AB:1::1/64
    ipv6 address FD0B:E954:B412:1::1/64
    no shutdown
interface Serial0/0
    ipv6 address FE80::1 link-local
    no shutdown
ipv6 route 2001:DB8:1AB:2::/64 Serial0/0 FE80::2
ipv6 route FD0B:E954:B412:2::/64 Serial0/0 FE80::2
end
```

Solution R2

```
hostname R2
ipv6 unicast-routing
interface FastEthernet0/0
    ipv6 address FE80::2 link-local
    ipv6 address 2001:DB8:1AB:2::1/64
    ipv6 address FD0B:E954:B412:2::1/64
    no shutdown
interface Serial0/0
    ipv6 address FE80::2 link-local
    no shutdown
ipv6 route ::/0 Serial0/0 FE80::1
end
```

Diagnostic IPv6 sur le routeur

```
# show ipv6 interface brief  
# show ipv6 interface f0/0  
# show ipv6 route
```

show ipv6 interface brief

R2#show ipv6 interface brief

```
FastEthernet0/0          [up/up]
    FE80::2
    2001:DB8:1AB:2::1
    FD0B:E954:B412:2::1
Serial0/0                [up/up]
    FE80::2
```

show ipv6 interface f0/0 (1/2)

```
R2#show ipv6 interface f0/0
```

```
FastEthernet0/0 is up, line protocol is up
```

```
IPv6 is enabled, link-local address is FE80::2
```

```
No Virtual link-local address(es):
```

```
Global unicast address(es):
```

```
2001:DB8:1AB:2::1, subnet is 2001:DB8:1AB:2::/64
```

```
FD0B:E954:B412:2::1, subnet is FD0B:E954:B412:2::/64
```

```
Joined group address(es):
```

```
FF02::1
```

```
FF02::2
```

```
FF02::1:FF00:1
```

```
FF02::1:FF00:2
```

show ipv6 interface f0/0 (1/2)

MTU is 1500 bytes

ICMP error messages limited to one every 100 milliseconds

ICMP redirects are enabled

ICMP unreachable are sent

ND DAD is enabled, number of DAD attempts: 1

ND reachable time is 30000 milliseconds

ND advertised reachable time is 0 milliseconds

ND advertised retransmit interval is 0 milliseconds

ND router advertisements are sent every 200 seconds

ND router advertisements live for 1800 seconds

ND advertised default router preference is Medium

Hosts use stateless autoconfig for addresses.

show ipv6 route

R1#show ipv6 route

IPv6 Routing Table - 7 entries

```
C   2001:DB8:1AB:1::/64 [0/0]      via ::, FastEthernet0/0
L   2001:DB8:1AB:1::1/128 [0/0]    via ::, FastEthernet0/0
S   2001:DB8:1AB:2::/64 [1/0]    via FE80::2, Serial0/0
C   FD0B:E954:B412:1::/64 [0/0]    via ::, FastEthernet0/0
L   FD0B:E954:B412:1::1/128 [0/0]  via ::, FastEthernet0/0
S   FD0B:E954:B412:2::/64 [1/0]    via FE80::2, Serial0/0
L   FF00::/8 [0/0]      via ::, Null0
```


Configuration DHCPv6 Stateless

```
ipv6 dhcp pool LAN
  dns-server 2001:DB8:1AB:AAA::1
interface FastEthernet0/0
  ipv6 nd other-config-flag
```

Vérification ND

```
R1#show ipv6 interface f0/0
```

```
FastEthernet0/0 is up, line protocol is up
```

```
IPv6 is enabled, link-local address is FE80::1
```

```
!!!!!!! Sortie omise !!!!!!!!
```

```
ND DAD is enabled, number of DAD attempts: 1
```

```
ND reachable time is 30000 milliseconds
```

```
ND advertised reachable time is 0 milliseconds
```

```
ND advertised retransmit interval is 0 milliseconds
```

```
ND router advertisements are sent every 200 seconds
```

```
ND router advertisements live for 1800 seconds
```

```
ND advertised default router preference is Medium
```

Hosts use stateless autoconfig for addresses.

Hosts use DHCP to obtain other configuration.

Droits

[Cisco Systems est une marque réservée.](#)

Routage IPv4/IPv6 de goffinet@goffinet.eu est mis à disposition selon les termes de la [licence Creative Commons Attribution - Partage dans les Mêmes Conditions 4.0 International](#)