

Sous-réseaux IP

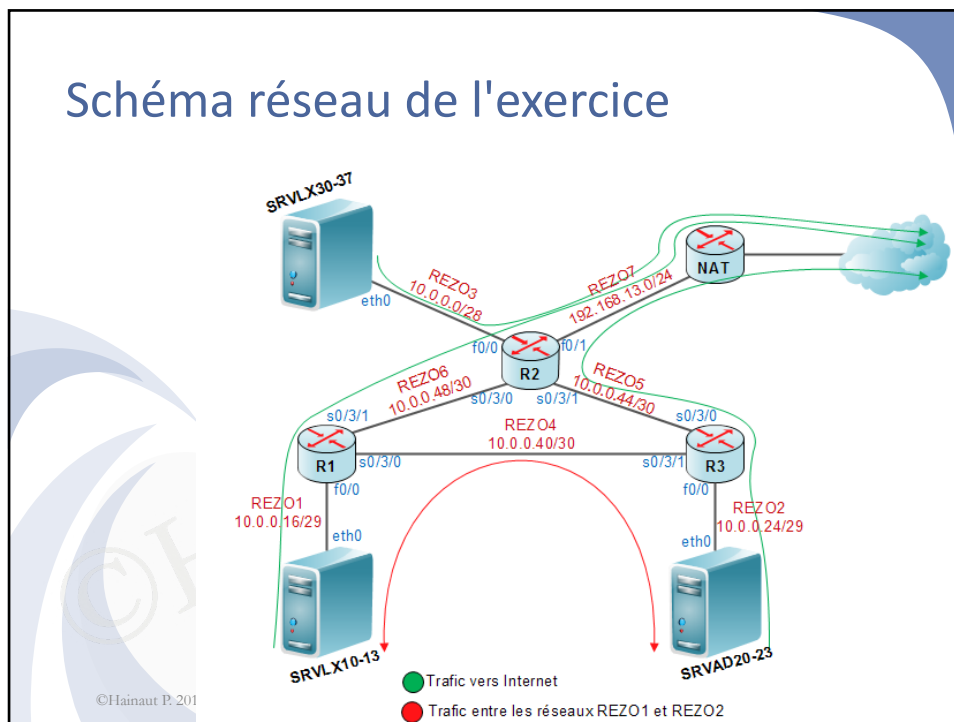
Exercice récapitulatif

Hainaut Patrick 2015

But de cette présentation

- L'adressage et le routage IP sont des notions importantes
- Il est intéressant d'utiliser ces notions dans un exercice récapitulatif qui vous permettra de faire le point sur vos connaissances
- Des infos complémentaires seront apportées, au besoin

Schéma réseau de l'exercice



Données de l'exercice

- Nous avons 3 serveurs interconnectés par un ensemble de 3 routeurs, lui-même connecté à Internet via un 4^{ème} routeur
- Nous nous intéressons ici à l'aspect IP, aussi nous n'installerons pas de services sur les serveurs
- SRVLX10-13 et SRVAD20-23 doivent pouvoir communiquer ensemble
- Les 3 serveurs doivent pouvoir accéder à Internet

Environnement de test réel

- Cet exercice peut être réalisé avec du matériel réel:
 - Serveur SRVLX10-13 sous Linux CentOS
 - Serveur SRVAD20-23 sous Windows 2008 Server
 - serveur SRVLX30-37 sous Ubuntu Linux
 - routeurs Cisco 2811
- Ca permet de travailler en groupe en se coordonnant, de câbler correctement et de manipuler du "vrai" matériel

Environnement de test réel

- Tâches à faire:
 - En fonction des données sur le schéma, configurer des paramètres IP valides sur les différentes interfaces réseaux
Toutes les interfaces ont une adresse IP statique sauf sur f0/1 de R2
 - Il faut ensuite configurer les différentes tables de routage sur R1, R2 et R3
Le routeur NAT n'est pas directement accessible, vous savez qu'il est serveur DHCP, NAT et qu'il est connecté à Internet (Il n'est donc pas à configurer !)
 - Vérifier que les trois serveurs ont accès à Internet (ping google) et que SRVLX10-13 et SRVAD20-23 peuvent se pinguer

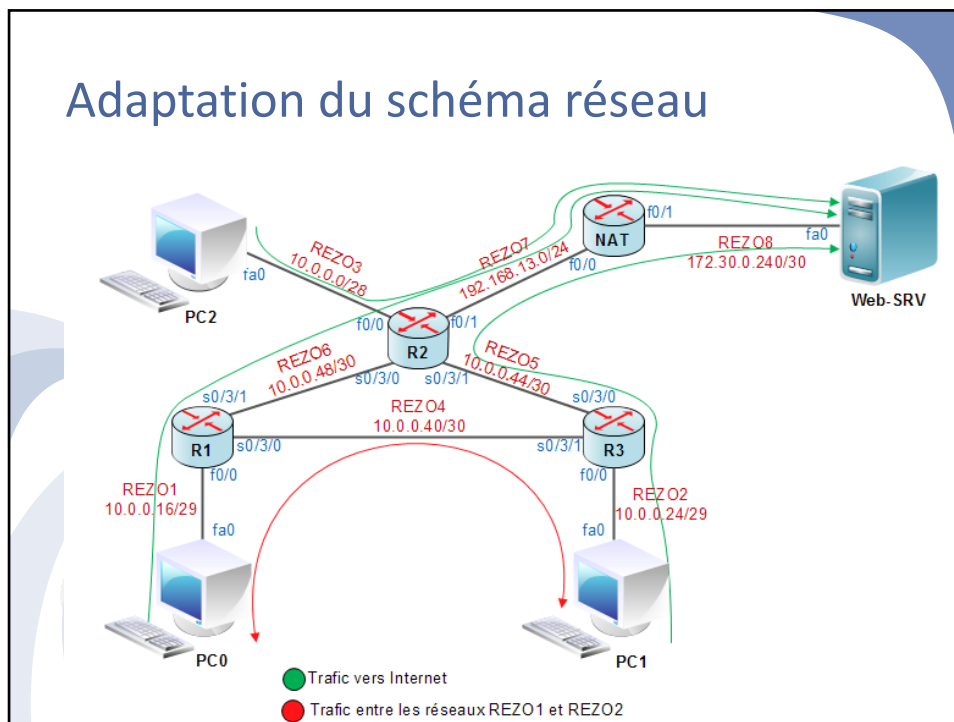
Environnement de test réel

- Ce qui est connu:
 - Les câbles à utiliser (Theo4 et Cisco1)
 - La configuration d'interfaces réseau sous les différentes plateformes (Manip5, Ex5, Manip11 et Cisco1)
 - La configuration de routes statiques (Cisco1)
- Reste la configuration d'une interface réseau en client DHCP sur les routeurs Cisco:
Pour un 2811: router (if-config)# ip address dhcp
- Vérifiez via traceroute, le trajet des différentes trames

Environnement de test sous Packet Tracer

- Cet exercice peut être réalisé sous Cisco Packet Tracer avec:
 - Des PC virtuels
 - Des routeurs Cisco 2811 virtuels
 - Un serveur Web virtuel pour simuler Internet
- Cela permet d'utiliser le puissant simulateur réseau de Cisco qui permettra une résolution très rapide de cet exercice en vous permettant de maîtriser tous les aspects du problème

Adaptation du schéma réseau



Environnement de test sous Packet Tracer

- Tâches à faire:
 - En fonction des données sur le schéma, configurer des paramètres IP valides sur les différentes interfaces réseaux
Toutes les interfaces ont une adresse IP statique (l'adressage dynamique n'est pas disponible sous Packet Tracer)
 - Internet sera simulé par un serveur (disponible dans la liste des périphériques finaux)
 - Il faut ensuite configurer les différentes tables de routage sur R1, R2 et R3 et NAT
 - Vérifier que les trois serveurs ont accès à Internet (ping Web-SRV) et que PC0 et PC1 peuvent se pinguer

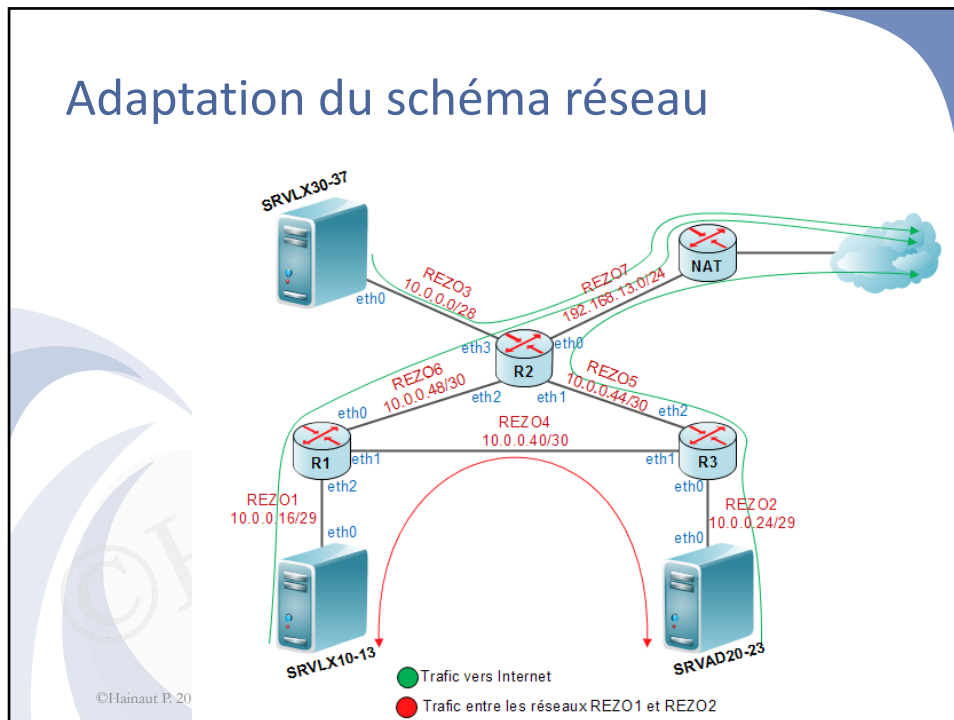
Environnement de test sous Packet Tracer

- Ce qui est connu:
 - Les câbles à utiliser (Theo4 et Cisco1)
 - La configuration d'interfaces réseau sous Packet Tracer (Cisco1)
 - La configuration de routes statiques (Cisco1)
- Si certaines choses vous sont inconnues, l'interface est très intuitive et votre débrouillardise devrait combler ces manques
- Vérifiez via `tracert` (tracert sous émulation Windows), le trajet des différentes trames

Environnement de test sous VirtualBox

- Cet exercice peut être réalisé sous VirtualBox avec:
 - Serveur SRVLX10-13 sous Linux CentOS
 - Serveur SRVAD20-23 sous Windows 2008 Server
 - serveur SRVLX30-37 sous Ubuntu Linux
 - Les routeurs sous Linux CentOS
- Cela permet maîtriser tous les aspects du problème tout en expérimentant des configurations réelles et la configuration de routeurs sous Linux

Adaptation du schéma réseau



Environnement de test sous VirtualBox

- Tâches à faire:
 - En fonction des données sur le schéma, configurer des paramètres IP valides sur les différentes interfaces réseaux
Toutes les interfaces ont une adresse IP statique sauf sur eth0 de R2
 - Il faut ensuite configurer les différentes tables de routage sur R1, R2 et R3
Le routeur NAT n'est pas directement accessible, vous savez qu'il est serveur DHCP, NAT et qu'il est connecté à Internet
 - Vérifier que les trois serveurs ont accès à Internet (ping google) et que SRVLX10-13 et SRVAD20-23 peuvent se pinguer

Environnement de test sous VirtualBox

- Ce qui est connu:
 - La création des différentes machines virtuelles (Manip2)
 - La liaison entre les différentes machines virtuelles (Manip2)
 - La configuration d'interfaces réseau sous les différentes plateformes (Manip5, Ex5 et Manip11)
- Ce qui reste à connaître
 - Indication de la passerelle au niveau d'une interface Linux
 - La gestion des tables de routage sous Linux
 - La gestion des tables de routage sous Windows

Passerelle sous Linux Ubuntu

- Il suffit d'utiliser le mot clé `gateway` au niveau de la configuration d'une interface dans le `/etc/network/interfaces`

- Exemple:

```
# The eth1 network interface
iface eth1 inet static
address 10.0.0.17
netmask 255.255.255.248
gateway 10.0.0.22
```

- N'oubliez pas de redémarrer le réseau ...

Tables de routage sous Linux Ubuntu

- La commande `route` est vue en détail dans Manip4
- Comme expliqué dans la présentation en question, les routes configurées par cette commande sont supprimées au redémarrage
- Pour les rendre permanentes, c'est assez facile sous Ubuntu; il suffit d'éditer le fichier `/etc/network/interfaces` et de taper les commandes `route ...` avec le mot clé `up` devant

Tables de routage sous Linux Ubuntu

- Exemple:

```
# The eth1 network interface
iface eth1 inet static
address 10.0.0.22
netmask 255.255.255.248
# static route
up route add -net 10.0.0.24 netmask 255.255.255.248 gw 10.0.0.22 dev eth1
```

Passerelle sous Linux CentOS

- On peut spécifier une passerelle pour une interface spécifique (comme pour les autres OS)
- Si on veut spécifier une passerelle pour eth0, on modifiera le fichier `/etc/sysconfig/network-scripts/ifcfg-eth0`

Exemple:

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=1A:2B:3C:4E:5F:00
IPADDR=10.0.0.17
NETMASK=255.255.255.248
ONBOOT=yes
GATEWAY=10.0.0.22
```

- N'oubliez pas de redémarrer le réseau ...

©Hainaut P. 2015 - www.coursonline.be

19

Passerelle sous Linux CentOS

- Les paramètres réseau globaux se trouvent dans le fichier `/etc/sysconfig/network`

Exemple:

```
NETWORKING=yes
HOSTNAME=R1.atc.lan
NOZEROCONF=yes
GATEWAY=10.0.0.22
```

- On peut ainsi activer le réseau, spécifier le nom DNS de la machine, désactiver l'auto-configuration (169.254. ...) et spécifier la passerelle
- Il est cependant préférable d'indiquer la passerelle au niveau de la configuration de l'interface ...

©Hainaut P. 2015 - www.coursonline.be

20

Tables de routage sous Linux CentOS

- La commande `route` est vue en détail dans Manip4
- Comme expliqué dans la présentation en question, les routes configurées par cette commande sont supprimées au redémarrage
- Pour les rendre permanentes, il faut créer un fichier par interface dans `/etc/sysconfig/network-scripts`
- Ce fichier sera nommé `route-interface`
Exemple: `route-eth0`

Tables de routage sous Linux CentOS

- Dans ce fichier, pour écrire une route, il faut respecter la syntaxe suivante:
network address/netmask via gateway
- Exemple:
10.0.0.24/29 via 10.0.0.22
- Comme les routes sont définies par interface, il n'y a pas lieu de préciser l'interface de sortie

Linux: remarques

- Pour Ubuntu et CentOS, on aurait pu préciser la passerelle par la route par défaut:

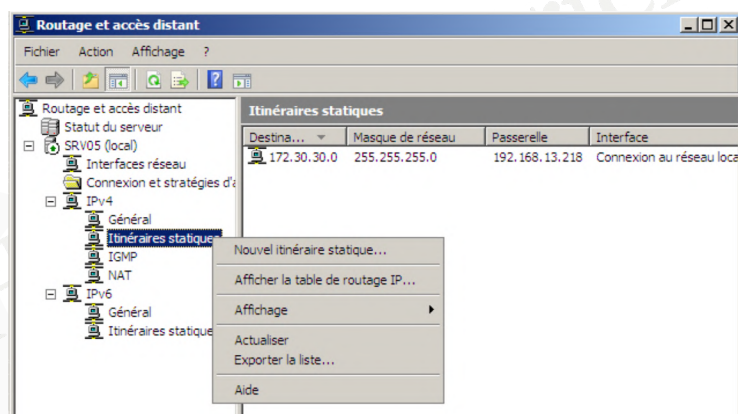
Exemple:

up route add default gw 10.0.0.22 dev eth1 sous Ubuntu
default 10.0.0.22 sous CentOS ou 0.0.0.0/0 10.0.0.22 si le mot clé default n'est pas reconnu par votre version

- C'est plus "propre" de le faire dans la configuration de l'interface

Tables de routage sous 2008 Server

- Dans le rôle "Routage et Accès distant", on peut ajouter sous l'item IPv4 des itinéraires statiques



Tables de routage sous 2008 Server

- On peut aussi, via l'invite de commande, afficher la table de routage avec la commande `route print`
- On ajoute une route persistante (qui reste après redémarrage) par la commande
`route add -p network address mask netmask gateway`

Exemple:

```
route add -p 10.0.0.24 mask 255.255.255.248 10.0.0.30
```

- On l'enlève par `route del ...`
- Remarque: comme on est dans un OS contrôlé par souris, on préférera la méthode de la dia précédente ...

Solution partielle - Avertissement

- Avant d'aller plus loin dans cette présentation, faites l'effort d'avoir cherché et réfléchi à une solution
- Vous ne tirerez bénéfice des dias qui suivent que si vous avez essayé, et pas juste 10 minutes ...
- On établira la liaison de SRVLX10-13 à Internet

Solution partielle - Création des machines

- Pour créer les machines sous VirtualBox, on crée et installe une machine de chaque type (Ubuntu, CentOS, ...) puis on la clone
- Il faut changer le nom de chaque machine
- Dans le cas de la liaison étudiée, ce sont toutes des machines CentOS
- Pour cette distribution, il faut éditer le fichier `/etc/sysconfig/network` et modifier la directive **HOSTNAME=**
- Après avoir sauvegarder les modifications, on redémarre le service réseau par `service network restart`

©Hainaut P. 2015 - www.coursonline.be

27

Solution partielle - Cartes réseaux

- Si vous utilisez des machines clonées, il y a beaucoup de chance que vos cartes réseaux aient été renommées par le système
- Pour le savoir: `ifconfig -a`
- Si c'est le cas, et si vous voulez revenir à la situation du schéma, il faut éditer le fichier `/etc/udev/rules.d/70-persistent-net.rules` et modifier la variable **name=**
- Pour que le changement soit pris en compte, on redémarre `udev` par la commande `start_udev`

©Hainaut P. 2015 - www.coursonline.be

28

Solution partielle - R2

- Partons d'Internet et revenons progressivement jusque SRVLX10-13
- Le routeur NAT à accès à Internet et est serveur DHCP et NAT
- Ce routeur n'est pas à créer, c'est le routeur de l'école distribuant l'accès Internet
- Si vous refaites l'exercice chez vous, ce routeur correspond à votre box vous donnant accès à Internet, la configuration reste donc la même

Solution partielle - R2

- R2 reçoit donc une IP dynamique sur son interface eth0
- Pour le reste, on prendra comme convention arbitraire, d'attribuer la première adresse disponible au routeur et la dernière au PC
- Dans le cas de deux routeurs, on attribue la première adresse disponible au premier routeur rencontré

Solution partielle - IP sur R2

- R2 doit avoir accès à Internet grâce aux paramètres dynamiques reçu sur eth0, on peut tester cela par un **ping**
- Il faut maintenant configurer l'interface eth2
- On va donc éditer le fichier `/etc/sysconfig/network-scripts/ifcfg-eth2` (à créer s'il n'existe pas)
- On retrouvera: **IPADDR=10.0.0.49**
NETMASK=255.255.255.252
- On redémarre le service réseau par: **service network restart**

Solution partielle - firewall sur R2

- En CentOS, le firewall est activé par défaut
- Pour les besoins de la manipulation, nous allons le désactiver
- Il faut taper:
iptables --flush -t filter suivi de **service iptables save**

Solution partielle - ip_forward sur R2

- Pour que la communication passe à travers R2, on doit activer le passage des trames d'une interface à l'autre
- On doit, pour cela, mettre à 1 la variable **ip_forward**
- Cela se fait en éditant le fichier `/etc/sysctl.conf` et en modifiant la ligne `net.ipv4.ip_forward=0` par `net.ipv4.ip_forward=1`
- On doit recharger ce fichier de configuration par la commande:
`sysctl -p`

Solution partielle - route sur NAT

- Deux cas possibles: soit on contrôle le routeur NAT, soit pas
- Si on contrôle le routeur NAT, on va implémenter une route de retour sur ce routeur: **10.0.0.16/29 via lan**
- Quand SRVLX10-13 fait une requête sur Internet, il le fait avec une adresse du réseau 10.0.0.16/29
- Le routeur NAT met en œuvre le NAT, en échangeant les adresses du réseau 10.0.0.16/29 avec son adresse publique pour la requête, puis dans l'autre sens pour la réponse, avec comme adresse de destination une adresse du réseau 10.0.0.16/29
- Il faut donc une route sur NAT vers ce réseau

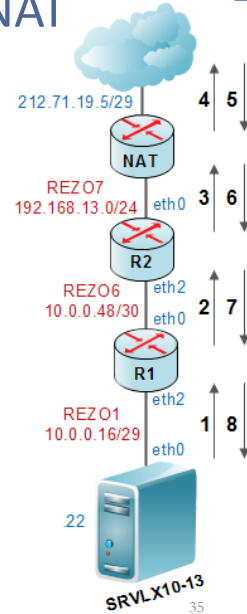
Solution partielle - route sur NAT

- ping 8.8.8.8, sans NAT sur R2 ...

Trame Ethernet

Paquet IP

	MAC d:	MAC s:	IP des:	IP src:	Datas
1	R1	SRV	8.8.8.8	10.0.0.22	
2	R2	R1	8.8.8.8	10.0.0.22	
3	NAT	R2	8.8.8.8	10.0.0.22	
4	Web	NAT	8.8.8.8	212.71.19.5	
5	NAT	Web	212.71.19.5	8.8.8.8	
6	R2	NAT	10.0.0.22	8.8.8.8	
7	R1	R2	10.0.0.22	8.8.8.8	
8	SRV	R1	10.0.0.22	8.8.8.8	



© Hainaut P. 2013 - www.coursonline.be

Solution partielle - NAT sur R2

- Bien que la solution des routes soit toujours préférable, si on ne contrôle pas le routeur NAT, on n'a pas d'autre choix que de faire du NAT sur R2
- En effet, le réseau 10.0.0.16/29 n'étant pas connu du routeur NAT, il ne saura pas retourner le résultat de la requête
- Il faut donc que la requête soit faite avec un réseau connu, en l'occurrence, le réseau 192.168.13.0/24
- Pour cela, il suffit de mettre en œuvre le NAT sur R2, qui va échanger les adresses du réseau 10.0.0.16/29 avec l'adresse du réseau 192.168.13.0 présente sur eth0 de R2

© Hainaut P. 2015 - www.coursonline.be

36

Solution partielle - NAT sur R2

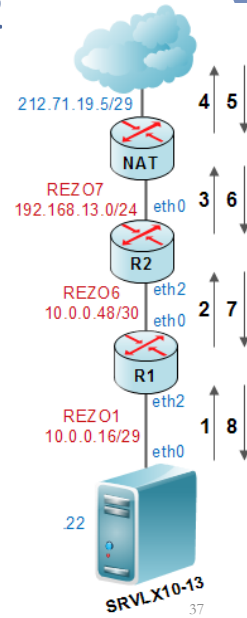
- ping 8.8.8.8, avec NAT sur R2 ...

Trame Ethernet

Paquet IP

	MAC d:	MAC s:	IP des:	IP src:	Datas
1	R1	SRV	8.8.8.8	10.0.0.22	
2	R2	R1	8.8.8.8	10.0.0.22	
3	NAT	R2	8.8.8.8	192.168.13.8	
4	Web	NAT	8.8.8.8	212.71.19.5	
5	NAT	Web	212.71.19.5	8.8.8.8	
6	R2	NAT	192.168.13.8	8.8.8.8	
7	R1	R2	10.0.0.22	8.8.8.8	
8	SRV	R1	10.0.0.22	8.8.8.8	

© Hainaut P. 2013 - www.coursonline.be



Solution partielle - NAT sur R2

- Il faut taper:

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

et sauver cette commande par `service iptables save`

- eth0 est bien l'interface de sortie vers Internet

© Hainaut P. 2015 - www.coursonline.be

38

Solution partielle - Route sur R2

- Quelque soit la solution choisie plus haut, une fois le paquet de retour sur R2, il faut l'acheminer vers R1
- De nouveau, deux solutions: soit une route de retour sur R2, soit la mise en œuvre du NAT sur R1
- Comme on contrôle R2, on choisira la première solution, plus professionnelle

Solution partielle - route sur R2

- L'effet de la commande `route add -net 10.0.0.16 netmask 255.255.255.248 gw 10.0.0.50` étant disparu au redémarrage, on préférera créer le fichier **route-eth2** dans lequel on écrira:
10.0.0.16/29 via 10.0.0.50
- 10.0.0.50 est l'adresse du prochain nœud (R1) par lequel on doit passer pour acheminer le paquet de retour
- On redémarre le service réseau pour que le fichier **route-eth2** soit pris en compte, ce qu'on vérifie par `route -n` qui affiche la table de routage

Solution partielle - IP sur R1

- Pour **ifcfg-eth0**, on aura: **IPADDR=10.0.0.50**
NETMASK=255.255.255.252
GATEWAY=10.0.0.49
- Pour **ifcfg-eth2**, on aura: **IPADDR=10.0.0.17**
NETMASK=255.255.255.248
- Après avoir redémarré le service réseau, on doit pouvoir faire un ping d'une adresse sur Internet (pas besoin de rajouter de route sur R2, c'est un réseau directement connecté et par la passerelle sur eth0 pour R1, on indique la sortie ...)

©Hainaut P. 2015 - www.coursonline.be

41

Solution partielle - IP sur R2

- Pour **ifcfg-eth0**, on aura: **IPADDR=10.0.0.22**
NETMASK=255.255.255.248
GATEWAY=10.0.0.17
- Le service réseau redémarré, on faire un **ping** d'une adresse sur Internet (IP uniquement car pas de DNS installé ou renseigné)
- Pour suivre le trajet des trames, rendez-vous à la dia 35 ou 37 suivant votre configuration

©Hainaut P. 2015 - www.coursonline.be

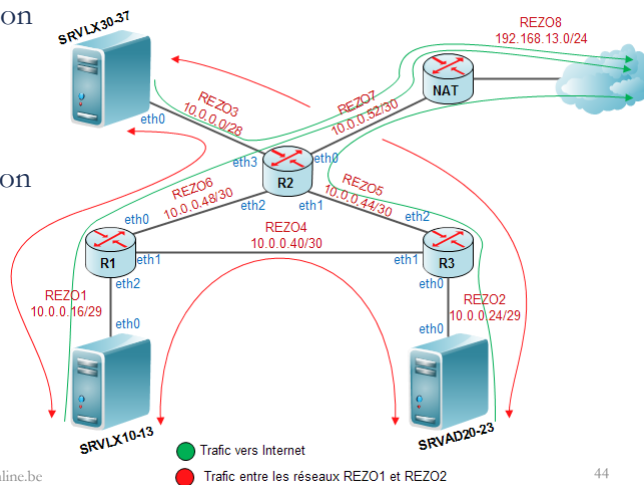
42

Solution partielle - Conclusion

- Voilà, il reste à faire de même pour le reste des liaisons
- Je veux pouvoir faire un ping de www.google.be mais sans installer **bind**. Comment procéder ?

Extension de l'exercice

- On rajoute un routeur NAT -> Qu'est-ce qui change au niveau de la configuration
- Les 3 serveurs doivent être en communication -> rajoutez les routes nécessaires



Conclusion

- Voici un exercice qui permet de mettre en œuvre l'adressage IP, de configurer les interfaces réseau des différentes machines et de créer les routes nécessaires aux communications réseau demandées
- Le fait de réaliser cet exercice de plusieurs façons et sur des plateformes différentes permet une bonne révision