Internet - Outils

Nicolas Delestre

À partir des cours « Outils réseaux » de Paul Tavernier et Nicolas Prunier

Plan

DHCP

Objectifs

- Automatiser et centraliser l'affectation des adresses IP
- L'attribution peut être permanente (association adresse MAC adresse IP) ou temporaire (attribution d'une adresse IP disponible)

Principe (attribution temporaire)

1. Le client DHCP émet en diffusion un premier message de demande de bail
2. S'il existe plusieurs serveurs DHCP atteints par la diffusion et si ces serveurs disposent d'une adresse IP libre, ces serveurs DHCP proposent au client cette adresse IP associée à une durée d'utilisation possible de l'adresse (une durée de bail). Ce message contient aussi l'adresse IP du serveur proposant l'offre.
3. S'il a reçu plusieurs propositions, le client en choisit une et retourne une demande d'utilisation de cette adresse. Cette demande est également diffusée pour que les autres serveurs DHCP apprennent qu'ils n'ont pas été sélectionnés.
4. Le protocole se termine par la transmission d'un message par lequel le serveur DHCP sélectionné accuse réception de la demande et accorde l'adresse selon la durée de bail prévue.

Firewall 1 / 2

Objectifs

- Élément permettant de trier les flux réseaux, en bloquant certains, en autorisant d'autres
- Le tri peut se faire sur :
  - les adresses IP source et/ou destination
  - les ports source et/ou destination

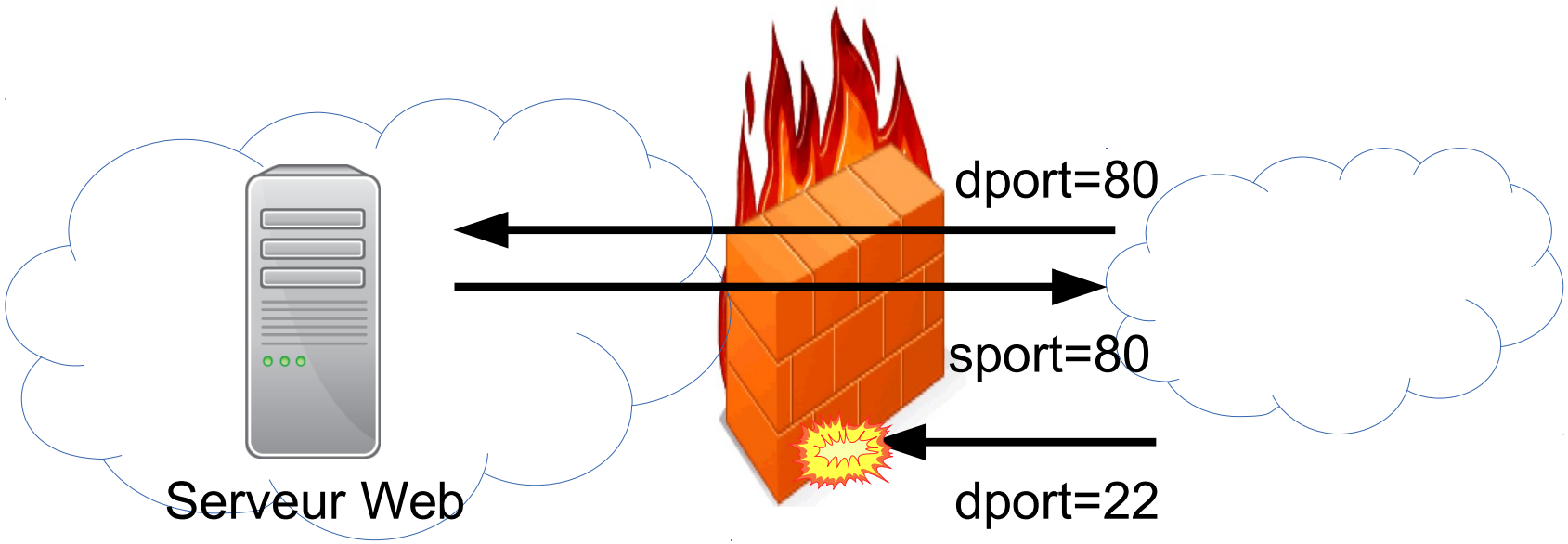
Deux types de firewall

1. Firewall personnel
   - Protège la machine sur laquelle il est installé
   - Bloque par défaut les flux venant de l'extérieur
   - Prévient/demande à l'utilisateur lorsqu'une application veut initier des flux vers l'extérieur
2. **Firewall réseau**
   - Effectue le routage inter-zones tout en appliquant des règles de filtrage
   - En général, il se place en coupure entre les zones de niveau de sécurité diffèrents (LAN / Datacenter / DMZ / Internet)

Firewall 2 / 2

Principe de configuration

- On interdit tout et on filtre le reste



Statefull et stateless

Firewall sans état (*stateless*)

- Un firewall stateless ne sait pas si un paquet appartient à une connexion déjà établie
  - Rappel pour un flux TCP : SYN, SYN-ACK et ACK
- Incomplet en terme de sécurité : générer des paquets TCP dont le port source ou destination est autorisé

Firewall avec état (*statefull*)

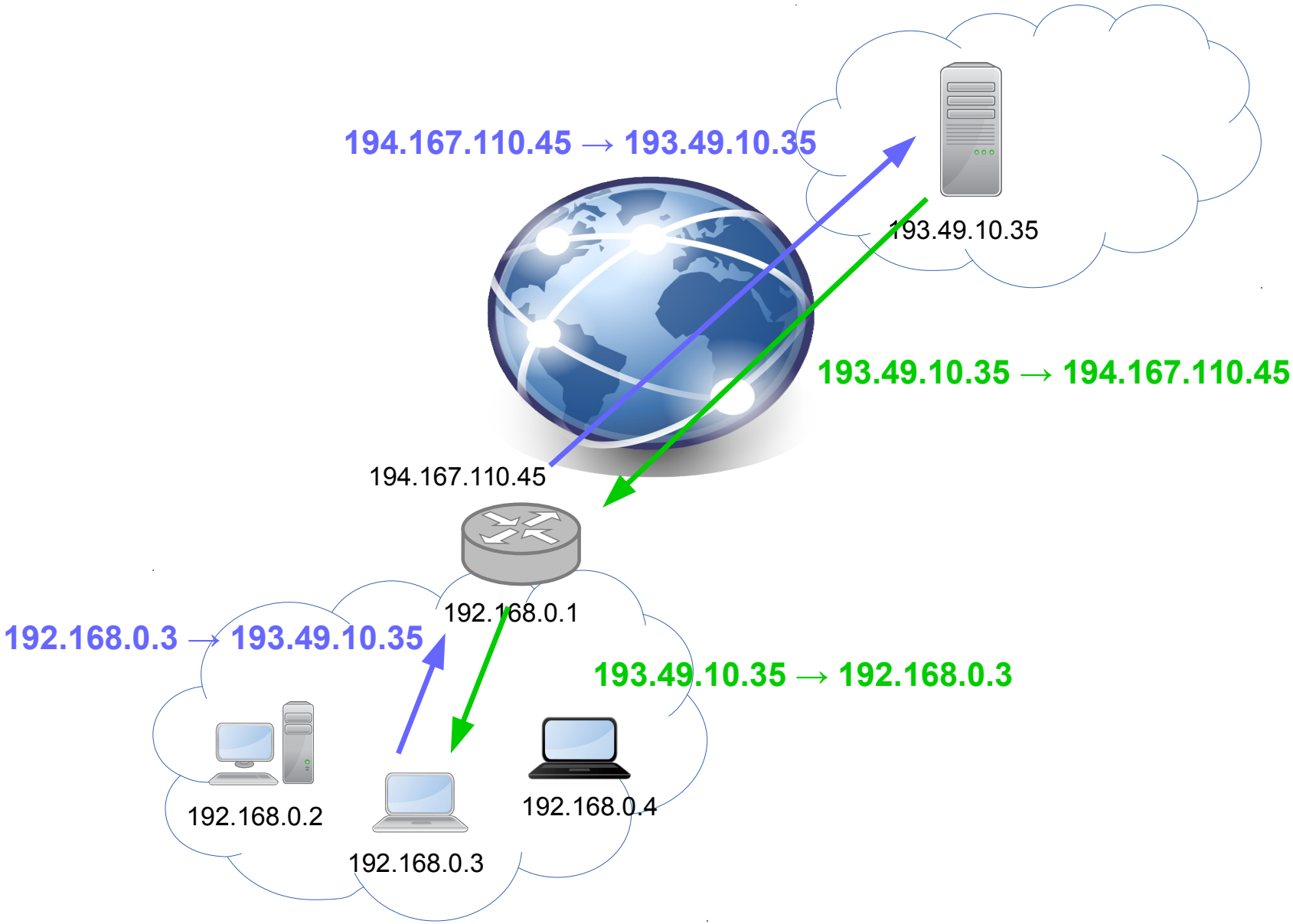
- Un firewall statefull connaît l'état de chaque connexion
- Plus sécurisé et plus simple à gérer
- Mais demande plus de ressource CPU et de mémoire

NAT 1 / 2

Objectifs

- Problèmes :
  - Il n'y a plus assez d'adresses IPv4 disponibles pour le nombre de machines reliées à internet sur la planète
  - Les adresses IP coûtent cher
- Solution : NAT
  - Le réseau interne est en adressage privé (RFC1918), un routeur/firewall « translate » les adresses des connexions sortantes
- Avantages/inconvénients :
  - Certains protocoles fonctionnent pas ou mal avec les mécanismes de translation d'adresse (H323, SIP, ...)
  - On économise nombre d'adresses IP publiques
  - Les machines nattées ne sont pas accessibles de l'extérieur

NAT 2 / 2


194.167.110.45 → 193.49.10.35
193.49.10.35
193.49.10.35 → 194.167.110.45
194.167.110.45
192.168.0.1
192.168.0.3 → 193.49.10.35
193.49.10.35 → 192.168.0.3
192.168.0.2
192.168.0.3
192.168.0.4

Translation de port

Objectif

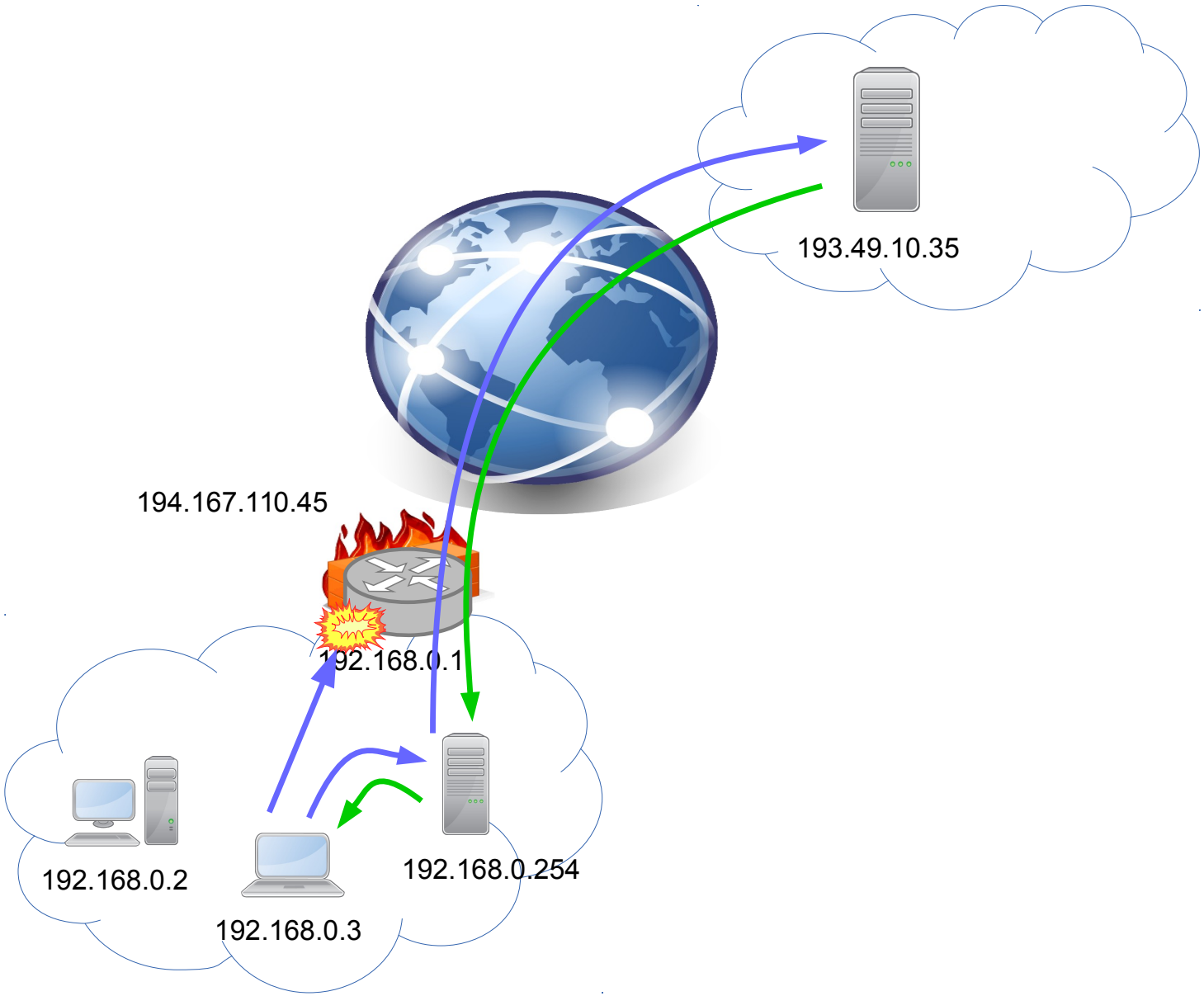
- Transmettre certaines communications entrantes (détérminées par le port destination) vers une machine appartenant à un serveur natté
- Il peut y avoir une modification du port

Proxy 1 / 2

Objectifs

- Pour sortir sur internet, obliger le client à passer par un « mandataire »
- Avantages :
  - Possibilité d'analyser plus finement le trafic
  - Des journaux de connexions
  - Sur les flux HTTP, possibilité de filtrer certains sites, de faire du contrôle anti-virus
- Inconvénients :
  - Moins performant en terme de débit
  - Ne fonctionne que pour quelques protocoles

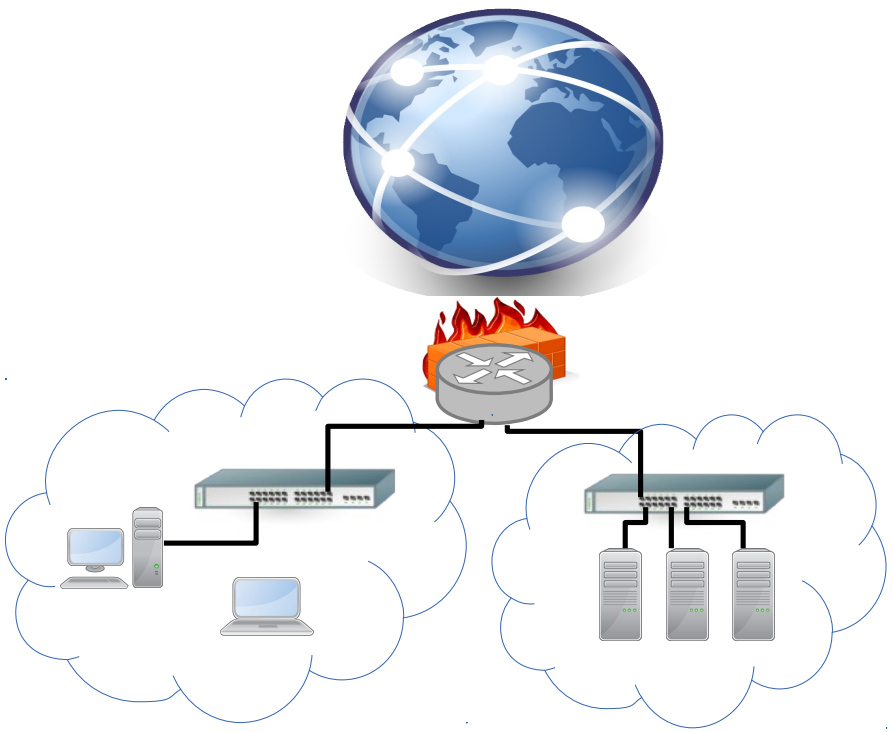
Proxy 2 / 2


193.49.10.35
194.167.110.45
192.168.0.1
192.168.0.2
192.168.0.3
192.168.0.254

DMZ

Zone démilitarisé

- Mettre les machines accessibles depuis internet dans un réseau différent des machines du réseau local
- Objectif : si un serveur publique est piraté, le pirate n'a pas accès au réseau local



VLAN 1 / 6

Rappel sur les switchs

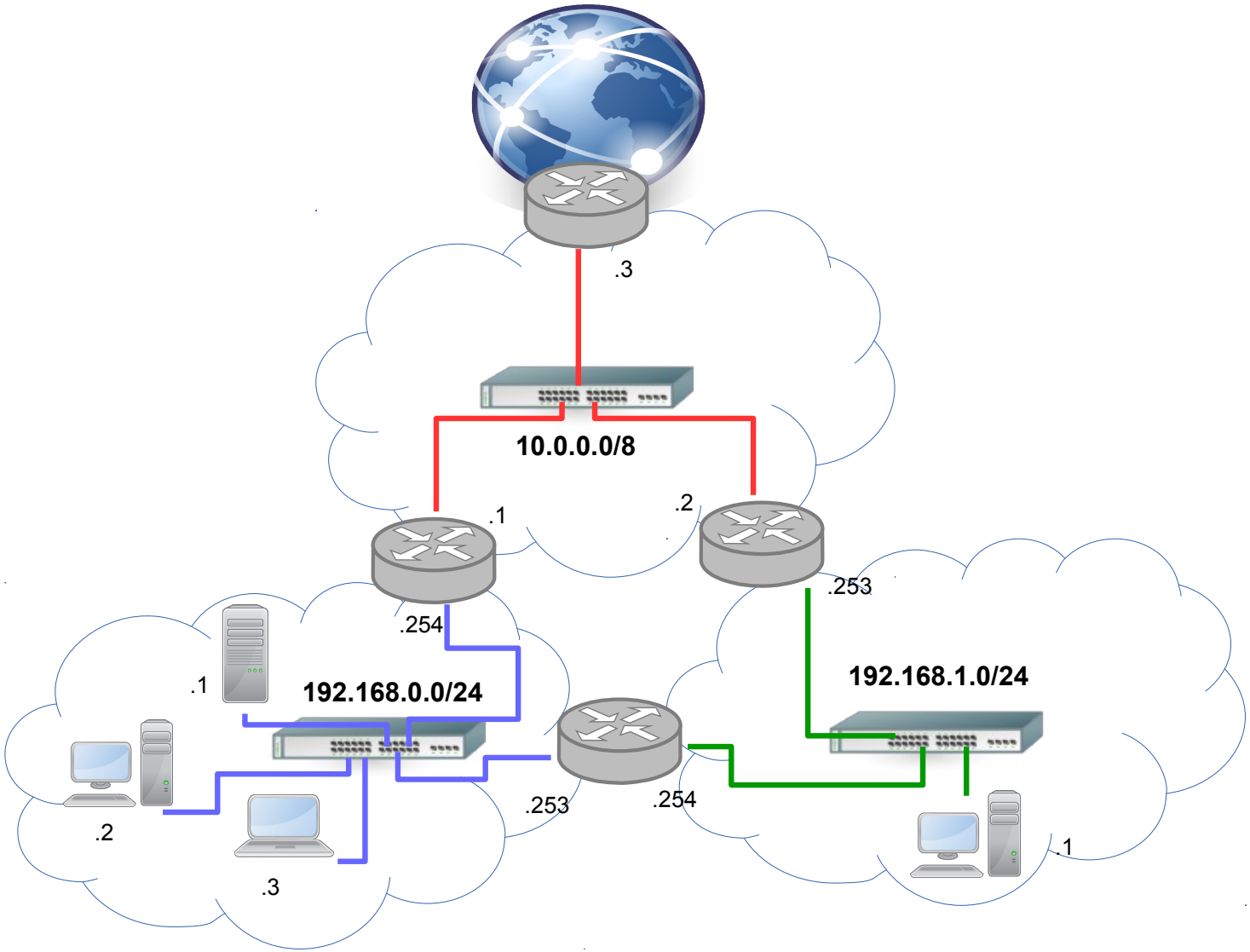
- Équipement de niveau 2 (OSI)
- Il « connaît » pour chacun de ses ports, la liste des équipements reliés en niveau 2, c'est à dire les adresses MAC
- La connaissance de la liste de ces adresses MAC se fait par apprentissage au fur et à mesure des trames
- Quand il reçoit une trame, il regarde l'adresse de niveau 2 de destination (i.e. adresse MAC) et transmet la trame sur le port où se trouve la machine avec cette adresse MAC
- Il n'a (théoriquement) aucune connaissance des adresses IP

VLAN 2 / 6

Rappel sur les routeurs

- Un routeur permet de relier (au moins) deux (sous-)réseaux différents. C'est à dire deux classes d'adresses différentes
- Il reçoit un paquet sur une interface et en consultant sa table de routage le transmet sur une autre
- On dit qu'un routeur « adosse » des domaines de broadcast

VLAN 3 / 6



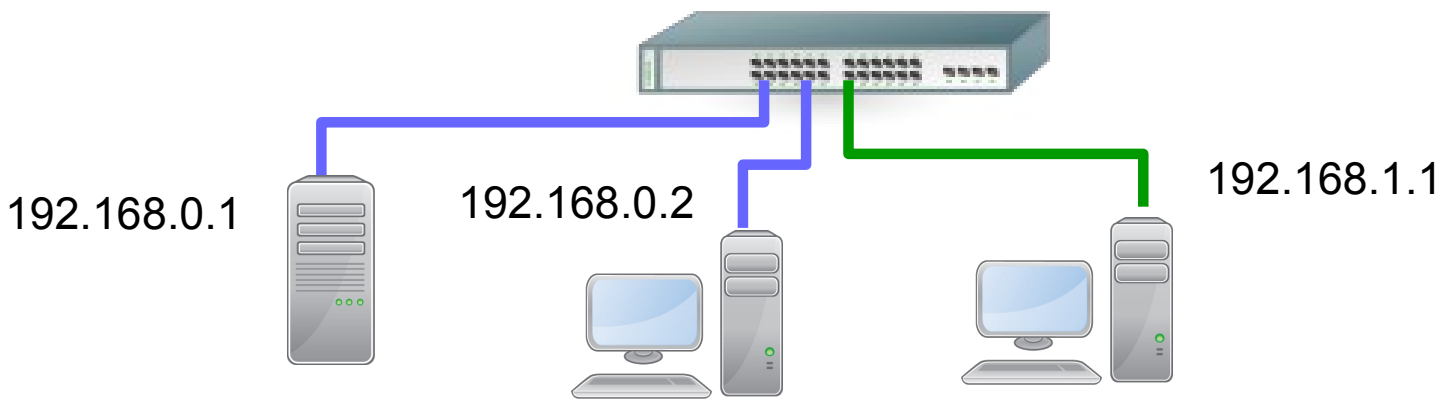
VLAN 4 / 6

Questions ?

- Je veux placer dans la salle machine (ou la baie) du réseau 192.168.0.0/24 une machine du réseau 192.168.1.0/24

Réponses

- Tirer un câble ou déplacer la machine
- Utiliser les VLAN : Ils permettent de faire coexister de manière étanche plusieurs domaines de broadcast sur un même switch.



VLAN 5 / 6

Avantages

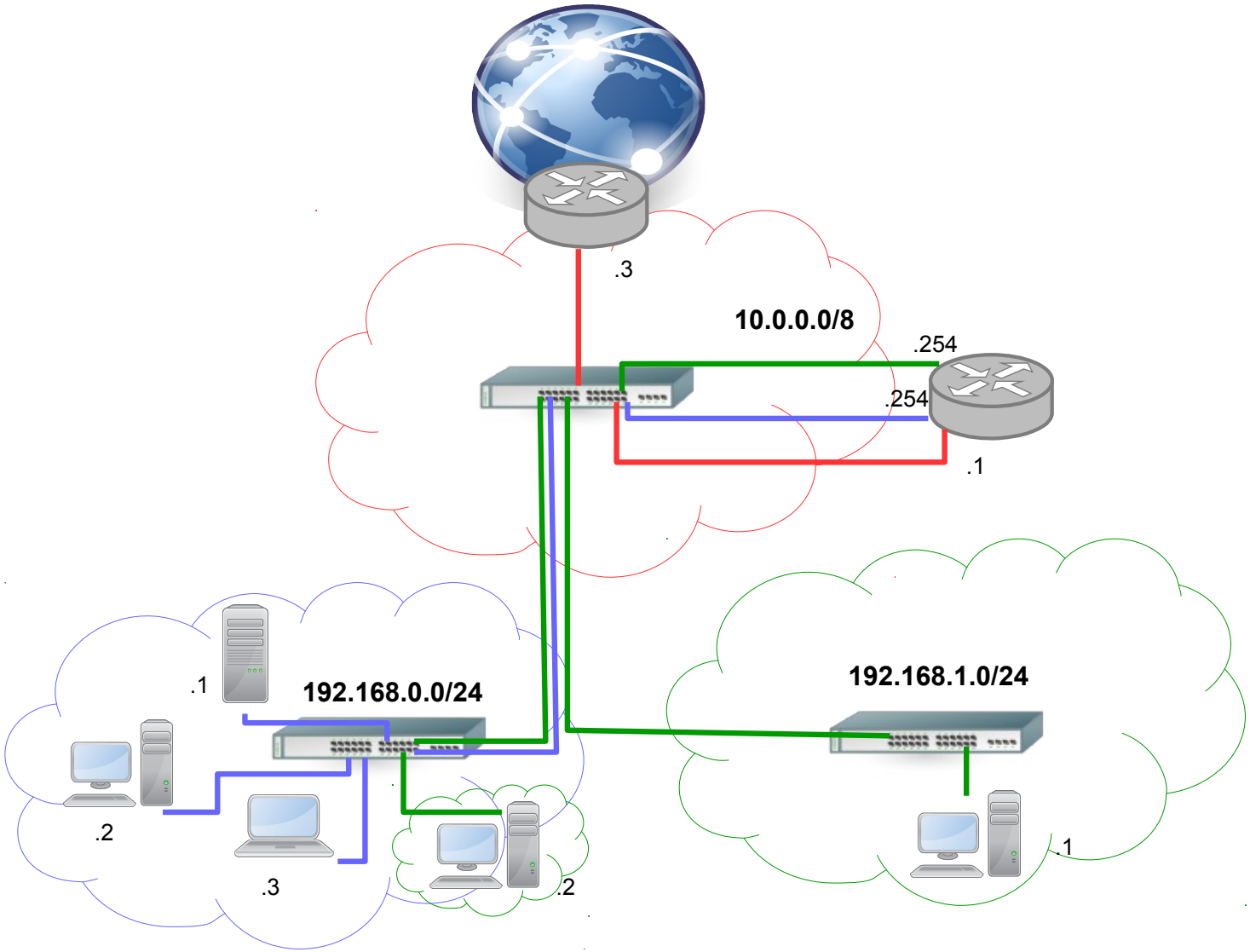
- Simplifier le brassage. « Comment changer un poste de réseau sans avoir à déplacer le poste » ?
- Ne pas multiplier le nombre de routeurs.
- Ne pas multiplier le nombre de ports sur les routeurs et firewalls.
- Rentabiliser l'investissement des switches

Trame

Préambule 7octets 10101010	Délimiteur de début 10101011	Adresse destination 6 octets	Adresse source 6 octets	TPID 2 octets	TCI 2 octets	EtherType / Longueur	*Données LLC*	Bourrage si L<46 octets	FCS 4 octets

- TPID : protocole utilisé
- TCI : 3bits pour la priorité (au regard des autres VLAN, indépendant de la priorité IP), 1 bit pur compatibilité avec Token Ring, 12 bits d'identification du VLAN

VLAN 6 / 6



Wake on Line

- Objectif : allumer une machine à distance
- Nécessité : carte mère et carte Ethernet compatible
- Principe :
  - envoi d'un paquet « magique », une trame Ethernet broadcastée suivie de 16 fois l'adresse MAC destination, suivi optionellement d'un mot de passe de 4 ou 6 octets
  - la trame Ethernet est générée par l'émission d'un paquet UDP (port 0, 7 ou 9)
- Il est possible d'envoyer un paquet « magique » sur Internet. Dans ce cas le port utilisé doit être redirigé vers la machine qui doit être réveillée.