Adaptation - Réseaux

Lucas Nussbaum
lucas.nussbaum@univ-lorraine.fr

Licence professionnelle ASRALL

Administration de systèmes, réseaux et applications à base de logiciels libres

Adaptation - Réseaux

- 5 séances de 2 heures
- Un examen (sur papier)
- Contenu : des rappels (en théorie)
  - Généralités
  - Adressage
  - Routage
  - Interactions adressage et routage $\rightsquigarrow$ ARP
  - Configuration réseau sous Linux

Les réseaux aujourd'hui

- Haut débit pour tout le monde
  - 100 Mb/s ou 1 Gb/s à la maison
  - backbone Tb/s
- Transport des données multimédia
  - Téléphone, télévision, jeux, ...
- Terminaux connectés en permanence
  - WiFi, 3G/4G
- Information partout, n'importe quand

Architecture de communication

- Grand nombre de machines à connecter
- Interconnexion de systèmes (ou de réseaux) différents
  - ordinateur, téléphone portable
  - réseaux filaires, sans-fils
- Connexions non fiables
- Multiplexage de communications
  - Congestion ?
- ...

Comment faire fonctionner tout ça en pratique ?

- Protocoles
- Architectures en couches

Protocoles

Déf. : Règles de communication entre 2 parties (*peers*) de même niveau
Les protocoles définissent le **format**, l'**ordre des messages** envoyés et reçus, et les **actions possibles** lors de la transmission et de la réception.

- Protocole humains
  - Exemples :
    - Quelle heure est-il ?
    - Introductions (Bonjour, ça va ?)
- Protocoles réseaux
  - Machines à la place des humains

Toutes les communications sur Internet sont dirigées par des protocoles

Protocoles (2)

Protocoles d'Internet :

- Décrits par des **RFC** (Request For Comment)
  - Plus de 6000 RFCs
  - Mais certains protocoles ne sont pas standardisés
- organisme de standardisation :
  IETF (Internet Engineering Task Force)

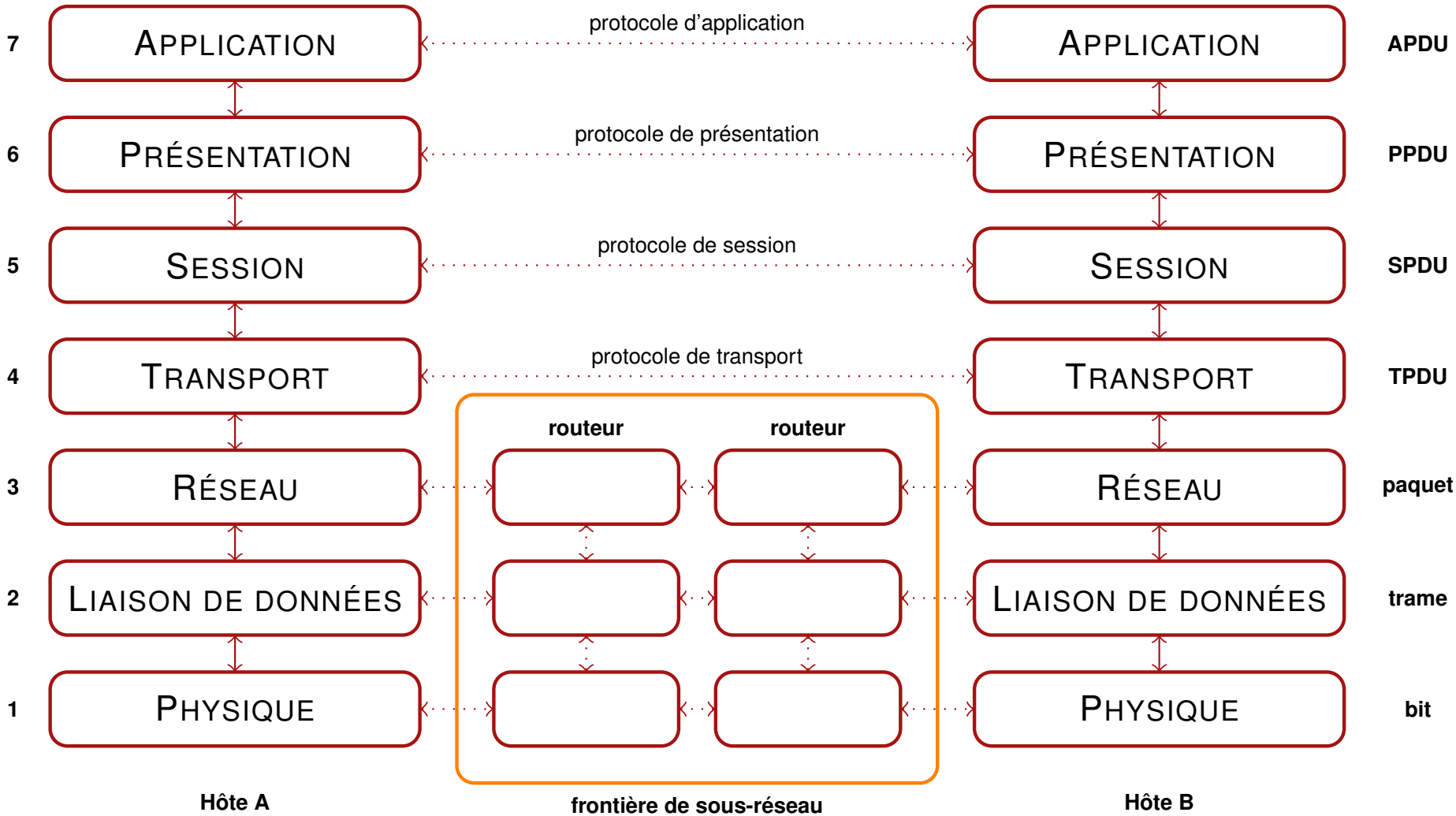
Architecture en couche

- "*chaque couche fait une chose, mais la fait bien, et fournit une interface plus simple à la couche au-dessus*"
  - Fournit des services à la couche supérieure (via un ensemble de primitives)
  - Utilise les services de la couche inférieure
  - Ajoute éventuellement un *header* et/ou *trailer* aux données, avant de transmettre les données à la couche inférieure
- Permet de séparer la spécification et l'implémentation

Communications :

- **horizontale** : entre parties (peers), qui comprennent et parlent le même protocole
- **verticale** : entre couches, qui utilisent un protocole d'interface (pas un protocole réseau)

Modèle OSI (*Open Systems Interconnection*)



Modèle OSI (*Open Systems Interconnection*) - 2

- **Application** : programmes d'application
- **Présentation** : interprétation des données (encodage)
- **Session** : notions de connexions, multiplexage, ...
- **Transport** : gère le transfert de bout en bout
- **Réseau** : gère le transfert entre les extrémités (routage)
- **Liaison** : contrôle d'erreur, contrôle de flux
- **Physique** : interface avec le support physique

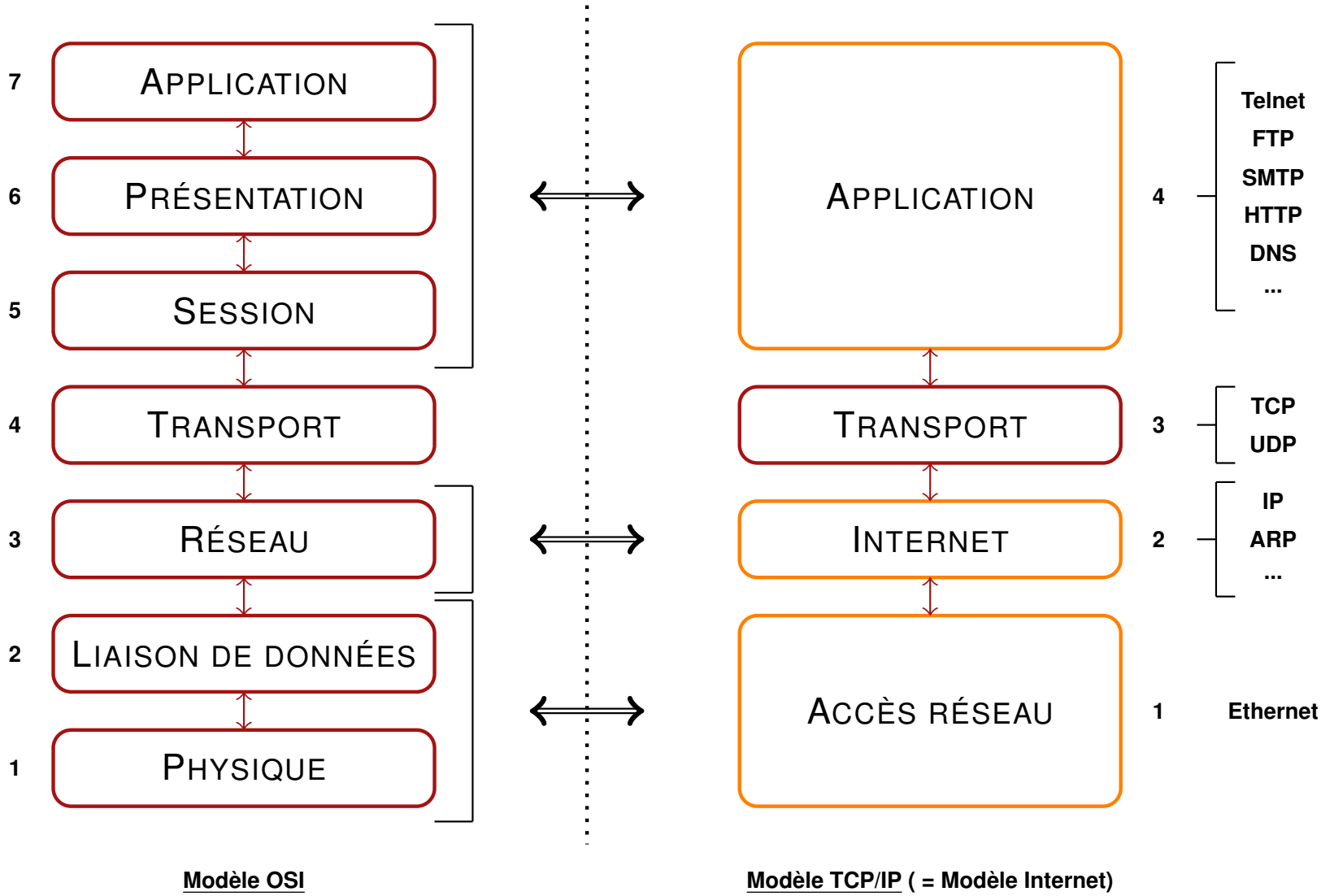
TCP/IP

Ensemble des protocoles utilisés sur Internet

Organisés en couche, mais certaines couches du modèle OSI sont fusionnées :

- **Applications** : HTTP, DNS, SMTP, peer-to-peer, ...
- **Transport** : TCP, UDP
- **Réseau** : IP
- **Transmission** : Ethernet, réseaux sans fil

Modèle OSI (1984) vs. Modèle TCP/IP (1976)



Modèle OSI

Modèle TCP/IP (= Modèle Internet)

Exercice : philosophes

Deux philosophes ne parlant pas la même langue et ne pouvant pas se déplacer souhaitent converser ensemble. L'un est kényan, l'autre indonésien. La seule possibilité pour eux est de faire appel à des traducteurs anglais et de télégraphier les courriers respectifs.

Modélisez cet exemple sous la forme d'un schéma s'inspirant du modèle OSI en donnant le rôle de chaque couche.

Rappels sur les unités

Temps : seconde **s**

- milliseconde *ms* (0.001*s*) : $10^{-3}s$
- microseconde μs (0.000001*s*) : $10^{-6}s$
- nanoseconde *ns* (0.000000001*s*) : $10^{-9}s$

Volume de données (émises, reçues) : bit : **b**, ou octet **o**.

- Kilobit **Kb** (1000) $10^3 b$
- Megabit **Mb** (1000000) $10^6 b$
- Gigabit **Gb** (1000000000) $10^9 b$
- Terabit **Tb** (1000000000000) $10^{12} b$
- 1 **o** (octet) = 8 **b** (bits) = 1 **B** (Byte)

Rappels sur les unités (2)

Attention :

- Réseaux : 1 K = 1000 (pour les débits)
- Mémoire : 1 K = 1024
- Volume de données (stockage) : ça dépend !

Pour lever l'ambiguïté : préfixes binaires (rarement utilisés)

- Kibi, Mebi, Gibi, ...
- $1KiB = 2^{10}B = 1024B$

Débit

Débit (D, en b/s) :

- Nombre de bits par unité de temps
- On parle parfois de *bande passante* (*bandwidth*)

Exemples :

- USB 2.0 : 480 Mb/s (ou Mbps)
- Wifi : 11 Mbps (802.11b) ou 54 Mbps (802.11g) ou plus

Temps d'émission, de propagation, de transfert

Temps d'émission (ou de transmission) **Te** : dépend du débit
Temps de propagation **Tp** : dépend de la vitesse de propagation **Vp** du signal (fonction du support), et de la distance

- Câble : $Vp = 2 * 10^8 m/s$
- Fibre optique : $Vp = 3 * 10^8 m/s$

Temps de transfert **Tt** : temps de transfert de bout en bout

$$Te = N/D$$

$$Tp = L/Vp$$

$$Tt = Te + Tp$$

(N : nb de bits ; D : débit ; L : distance)

Exercice : transfert de données

On souhaite transférer 100 Go de données entre l'IUT et le LORIA, distants de 2.5 km.

- La première solution est de réaliser le transfert à l'aide d'un disque dur et d'un vélo (à la vitesse moyenne de 18 km/h, soit 5 m/s). Calculez les temps d'émission ou de propagation (ou donnez-en une estimation, en justifiant). Calculez ensuite le débit moyen de cette solution.
- La deuxième solution est de transférer les données en utilisant un réseau en fibre optique, d'un débit de 1 Gbps (On rappelle la vitesse de propagation du signal dans la fibre optique : $3 * 10^8 m/s$). Calculez les temps d'émission ou de propagation (ou donnez-en une estimation, en justifiant). Calculez ensuite le débit moyen de cette solution.
- Quelle est la meilleure solution ?
- Sachant que la vitesse d'écriture sur un disque dur récent est d'environ 100 Mo/s, que pouvez-vous dire de ce calcul ?

Niveau 2 vs Niveau 3

- Niveau 2 (par exemple Ethernet) :
  - Réseau "local"
  - Équipements : hubs, switchs (commutation de trames)
  - Adresses MAC
- Niveau 3 (IP) :
  - Interconnexion de réseaux locaux
  - Équipements : routeurs
  - Adresses IP, tables de routage
- Protocole ARP : résolution de l'adresse MAC correspondant à une adresse IP

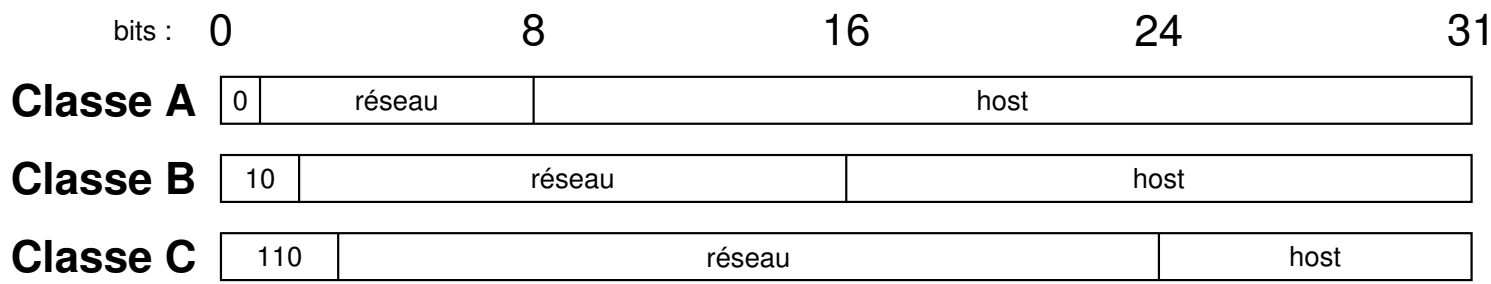
Adressage IP

- Adressage hiérarchique
  - Adresse de réseau IP
  - Adresse de chaque machine dans le réseau
- Réseau IP : suite d'adresses contigües
- Format d'adresse :
  - 32 bits : adresse réseau (n bits) + adresse machine (m bits)
  - Un réseau IP possède 2^m valeurs réparties entre :
    - l'adresse IP du réseau : les m bits sont à 0
    - les adresses des machines (max $2^m - 2$ machines)
    - une adresse de diffusion : les m bits sont à 1

Classes de réseaux

- Définit le nombre d'octets pour l'adresse réseau
  - classe A → 1 octet
  - classe B → 2 octets
  - classe C → 3 octets

- Historiquement :
  - classe A : 1er bit de l'adresse à 0
  - classe B : 2 premiers bits de l'adresse : 10
  - classe C : 2 premiers bits de l'adresse : 11



- Actuellement, on parle de classe A, B, C sans prendre en compte les premiers bits de l'adresse (uniquement le nombre d'octets)

Notation CIDR

- Classes de réseaux : grain trop gros
- Besoin d'attribuer des plages d'adresses de manière plus fine
- CIDR : Classless Interdomain Routing
  - Indication du nombre de bits de l'adresse réseau
  - Exemple : `charlemagne.iutnc.univ-lorraine.fr` : 194.214.170.56/22 ou 194.214.170.56/255.255.252.0

Adresses privées (RFC 1918)

- Réservées à un usage local (NAT, etc.)
- 10.0.0.0 - 10.255.255.255 (10/8)
- 172.16.0.0 - 172.31.255.255 (172.16/12)
- 192.168.0.0 - 192.168.255.255 (192.168/16)
- Autre adresse spéciale :
  - 127.0.0.1 - boucle locale

Exercices

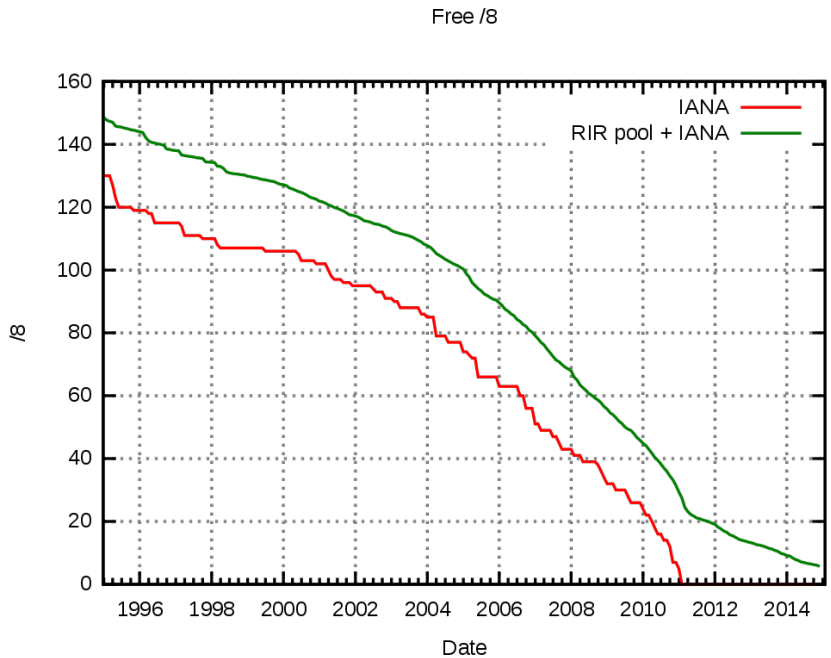
- Combien d'adresses utilisables par des machines comporte un réseau :
  - de masque 255.255.240.0 ?
  - de masque 255.255.255.192 ?
  - /12 ?
- Une machine d'adresse 129.88.61.10 appartient à un réseau /22. Donnez :
  - l'adresse du réseau
  - le masque de sous-réseau
  - l'adresse de diffusion (broadcast)
  - les adresses des premières et dernières machines du réseau
  - le nombre d'adresses utilisables par des machines
- Même question avec une machine d'adresse 152.81.15.82/20.
- Même question avec une machine d'adresse 100.64.85.152/28.

Attribution des adresses IP

- Une machine hôte obtient son adresse du bloc IP de son organisation
- Une organisation obtient son bloc IP à partir du bloc d'adresse de son ISP
- Un ISP obtient son bloc d'adresse de son propre provider ou de l'un des 5 RIR (*Regional Internet Registries*)
- Les RIR coopèrent avec l'ICANN (*Internet Cooperation for Assigned Names and Numbers*)

Épuisement des adresses IPv4

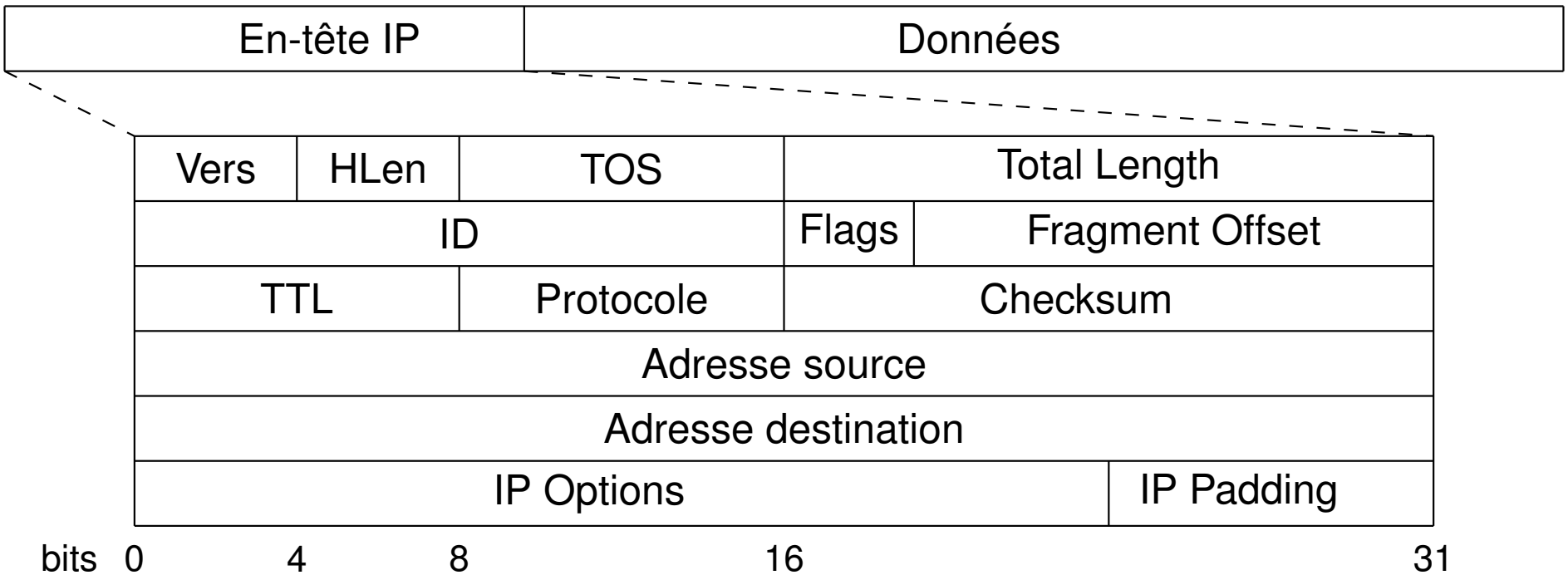
- Seulement (en théorie) 2^{32} adresses $\rightarrow$ 4.3 milliards !
- Beaucoup de besoins : terminaux mobiles, modems connectés en permanence, adressage inefficace (grandes entreprises, universités), virtualisation



Solution : IPv6 ?

- Adresses sur 128 bits
- exemple : www.google.com 2A00:1450:8006:0:0:0:0:93

Paquet IPv4 (1/3)



Paquet IPv4 (2/3)

- VERS : Version du protocole
  - 4 : IPv4
  - 5 : version expérimentale
  - 6 : IPv6
- HLEN : Longueur du header en unités de 32 bits (sans data)
- TOS : Qualité de service (QoS), etc. . .
- Total Length : Longueur totale (en octets), header et données
- ID : identifiant unique pour le réassemblage de paquets
- Flag : bits de contrôle
  - bit 1 : 0 (réservé)
  - bit 2, DF : 0 signifie fragmentation autorisée, 1 non
  - bit 3, MF : 0 signifie dernier fragment, 1 signifie d'autres fragments suivent

Paquet IPv4 (3/3)

- Fragment Offset : nombre de segments de 64 bits (sans header) déjà transmis dans des fragments précédents
- TTL (*Time To Live*) : nombre de routeurs que le paquet peut traverser
- Protocole :
  - 0 : réservé
  - 1 : Internet Control Message Protocol (ICMP)
  - 4 : IP (encapsulation IP)
  - 6 : TCP
  - 17 : UDP
  - ...
- Checksum

Exemple 1

```
45000047
d62c4000
401170c2
c0a83602
d41b28f1
b6c40100
...
```

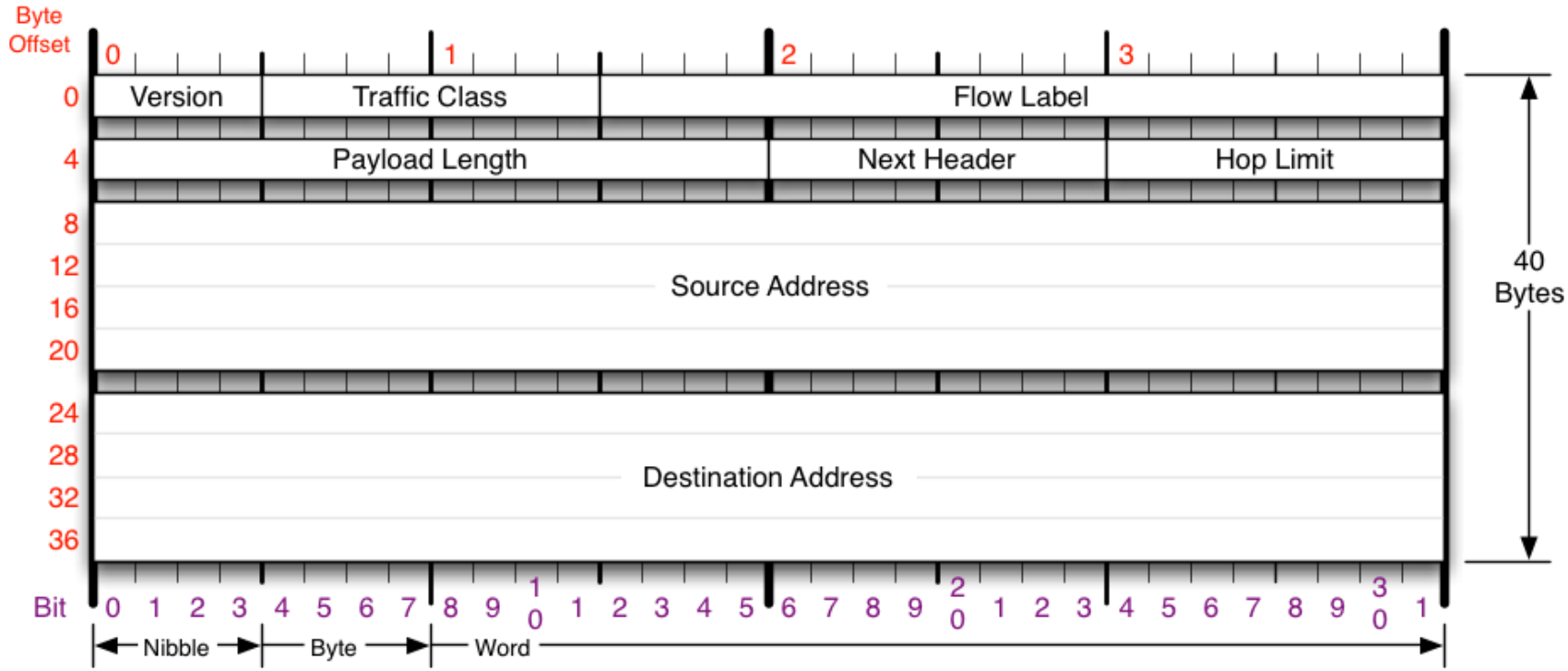
Exemple 2

```
450005dc
b0462000
4001b689
c0a836fe
c0a83602
00004205
...
```

Fragmentation IP

- Utilisée si le protocole de niveau 2 (e.g Ethernet) ne permet pas de transmettre des trames de taille suffisante
- **Flags :** indique si la fragmentation est autorisée, et si il y a d'autres fragments pour le paquet courant
- **Identification :** indique le numéro du paquet IP fragmenté
- **Fragment Offset :** indique la position du fragment (en octets depuis le début des informations)

IPv6 Header



Version

Version of IP Protocol. 4 and 6 are valid. This diagram represents version 6 structure only.

Traffic Class

8 bit traffic class field.

Flow Label

20 bit flow label.

Payload Length

16-bit unsigned integer. Length of the IPv6 payload, i.e., the rest of the packet following this IPv6 header, in octets. Any extension headers are considered part of the payload.

Source Address

128-bit address of the originator of the packet.

Next Header

8-bit selector. Identifies the type of header immediately following the IPv6 header. Uses the same values as the IPv4 Protocol field.

Destination Address

128-bit address of the intended recipient of the packet (possibly not the ultimate recipient, if a Routing header is present).

Hop Limit

8-bit unsigned integer. Decremented by 1 by each node that forwards the packet. The packet is discarded if Hop Limit is decremented to zero.

RFC 2460

Please refer to RFC 2460 for the complete Internet Protocol version 6 (IPv6) Specification.

Routage IP

Routeur : noeud intermédiaire connecté à 2+ réseaux

Lorsqu'un paquet arrive dans un routeur, celui-ci le retransmet :

- Soit à la machine destinaire si celle-ci est directement connectée au routeur
- Soit vers un autre routeur auquel il est directement connecté

Le choix de la *route* se fait à partir d'une **table de routage** :

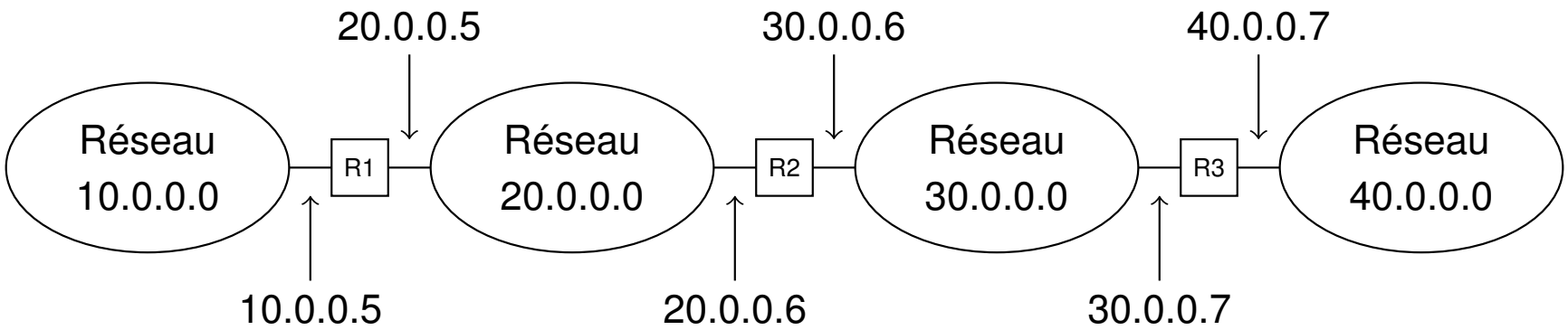
- Le routeur choisit la règle de préfixe le plus long correspondant à la destination

Table de routage

- Au moins 3 colonnes :
  - Adresse de réseau de destination
  - Passerelle à utiliser
  - Interface à utiliser pour joindre la passerelle
- Route par défaut : route utilisée lorsqu'il n'y a pas d'entrée correspondante dans la table de routage

```
$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   Iface
192.168.2.0     0.0.0.0         255.255.255.0   U       eth0
172.16.16.0     0.0.0.0         255.255.255.0   U       eth0
129.88.98.0     0.0.0.0         255.255.255.0   U       eth1
131.254.202.0   172.16.16.254   255.255.254.0   UG      eth0
138.96.20.0     172.16.16.254   255.255.252.0   UG      eth0
192.168.0.0     172.16.16.254   255.255.0.0     UG      eth0
172.16.0.0      172.16.16.254   255.240.0.0     UG      eth0
10.0.0.0        172.16.16.254   255.0.0.0       UG      eth0
0.0.0.0         129.88.98.254   0.0.0.0         UG      eth1
```

Table de routage : exemple



Destination	Passerelle
20.0.0.0	DIRECT
30.0.0.0	DIRECT
10.0.0.0	20.0.0.5
40.0.0.0	30.0.0.7

Table de routage de R2

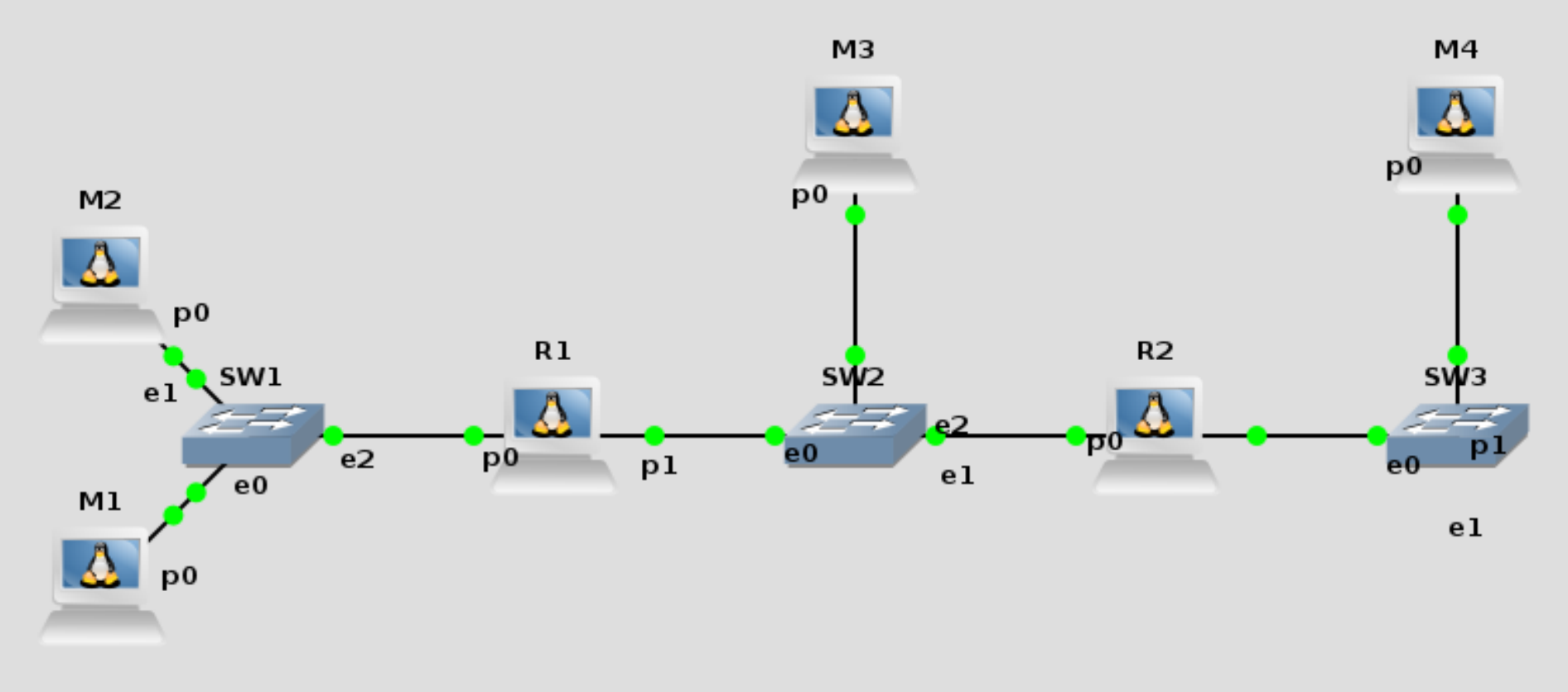
Exercice

Voici la table de routage d'une machine :
(G indique que la colonne Gateway contient une passerelle)

Destination	Gateway	Interface	Flags	Netmask
127.0.0.0	127.0.0.1	lo0	UH	255.0.0.0
152.16.2.0	152.16.2.254	eth0	U	255.255.255.0
152.16.3.0	152.16.3.254	fxp0	U	255.255.255.0
152.16.1.0	152.16.1.254	fxp1	U	255.255.255.0
128.121.0.0	152.16.2.253	eth0	UG	255.255.0.0
default	152.16.3.253	fxp0	UG	0.0.0.0

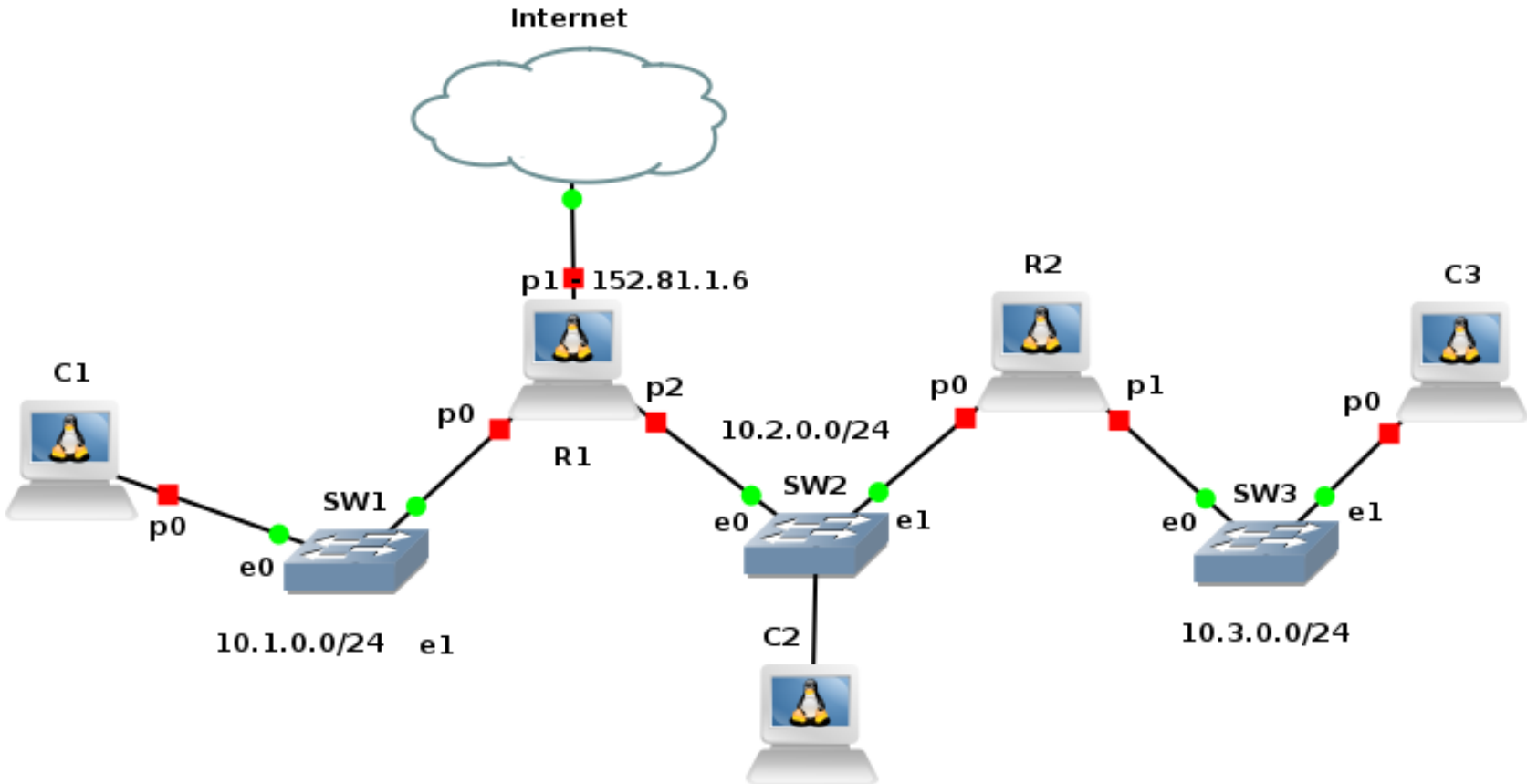
1. Combien de cartes réseaux y a-t-il sur cette machine ? Combien d'adresses IP ?
2. Dessiner la carte du réseau que vous pouvez déduire de cette table de routage.

Exercice



- Combien de réseaux de niveau 2 y a-t-il ?
- Proposez un plan d'adressage
- Donnez toutes les tables de routage (minimales)

Exercice : routage (1/2)



Exercice : routage (2/2)

Les tables de routage fournies doivent être minimales (pas de lignes inutiles), mais permettre à chaque machine ou routeur de joindre toutes les autres machines du réseau (et d'Internet).

- Sur le schéma de la page précédente, proposez un plan d'adressage en annotant le sujet. Les machines clientes doivent être en début de plage d'adresse ; les routeurs doivent être en fin de plage.
- Donner les tables de routage de C1, C2, R2

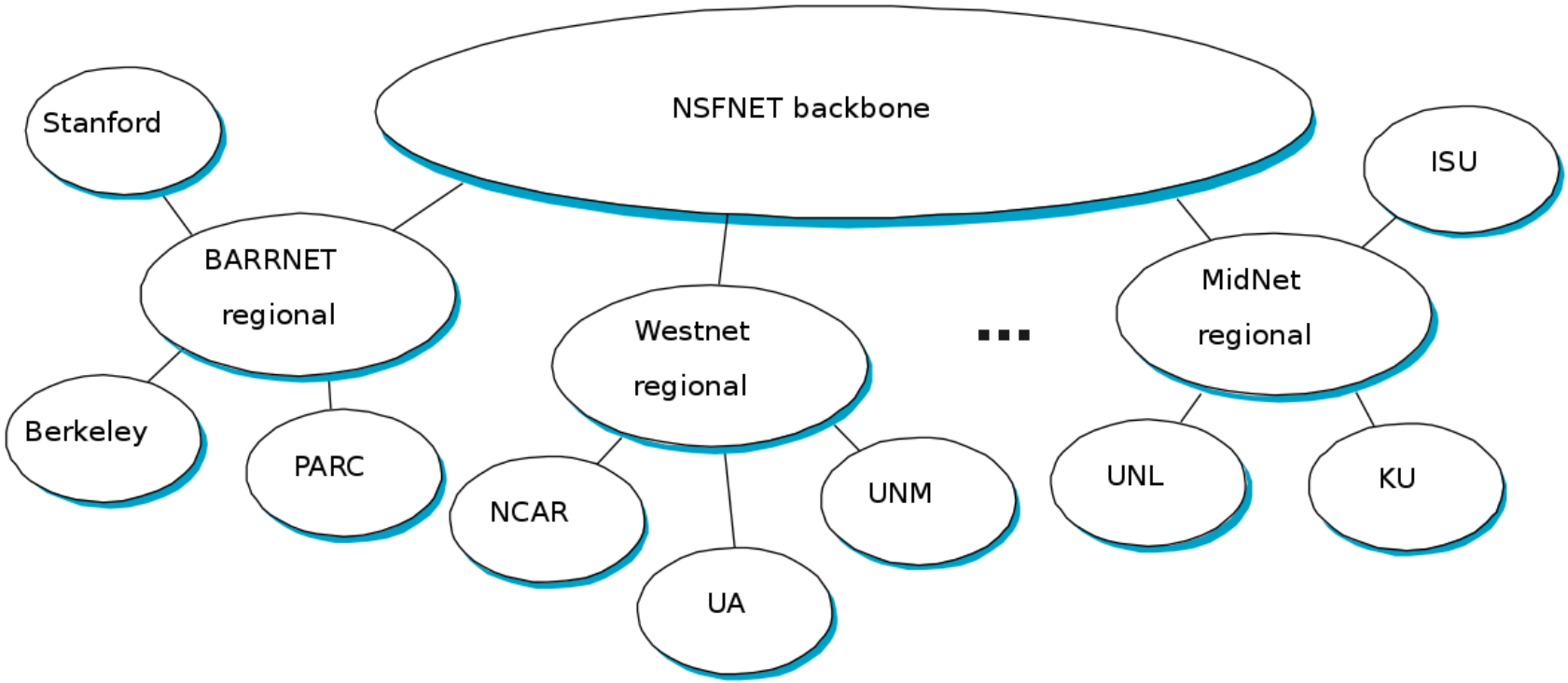
Remplissage de la table de routage

- Routage statique : table remplie manuellement
  - Ne permet pas de détecter les changements de topologie (pannes, liens engorgés)
- Routage dynamique :
  - Apprentissage automatique des différents réseaux accessibles
  - Protocole de routage :
    - À l'intérieur d'un réseau d'opérateur : RIP, OSPF, ISIS
    - Entre des opérateurs : BGP

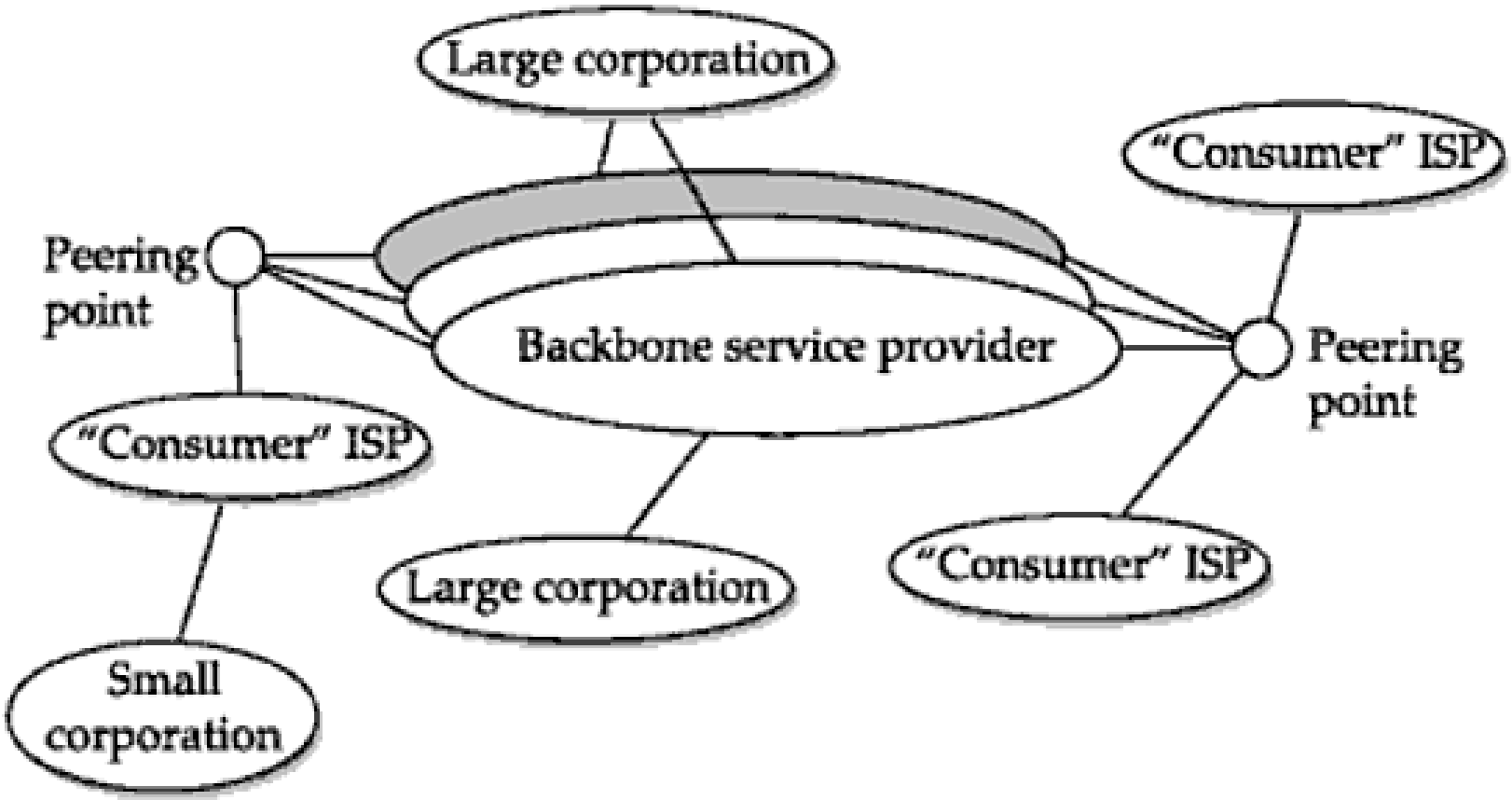
Pour éviter les boucles infinies dans le routage :

- Champ TTL (Time-to-live)
- Décrémenté à chaque passage par un routeur

Internet en 1990



Internet aujourd'hui



Interconnexion d'opérateurs

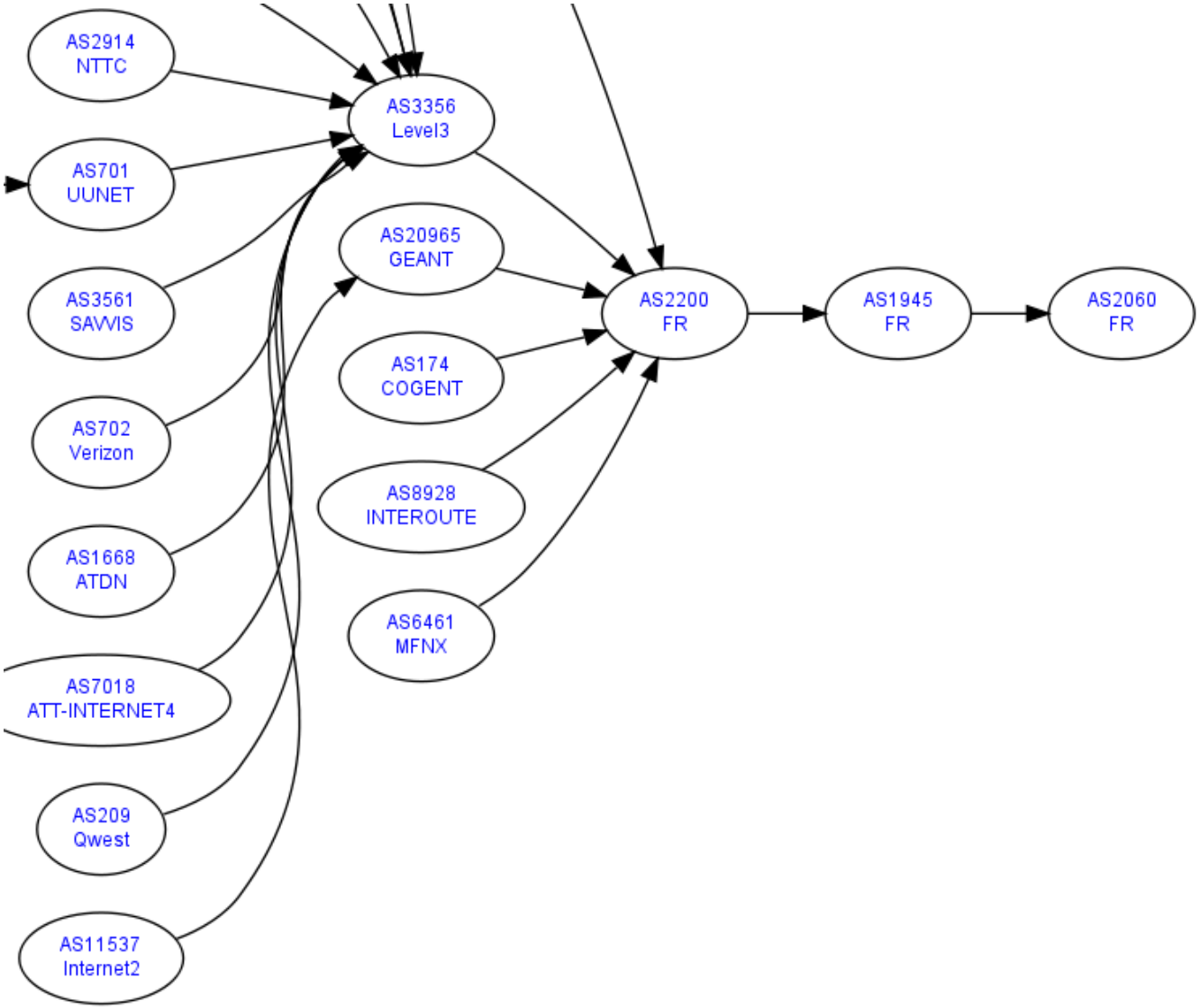
Quand on est opérateur, 2 solutions pour pouvoir atteindre d'autres réseaux :

- Payer un fournisseur de transit IP
- Passer des accords réciproques avec d'autres opérateurs (**peering**), souvent dans un Internet Exchange Point (IXP, GIX).
  En France : FranceIX, SFINX (Renater), etc.
- Possible source de conflits (2003 : Free vs France Telecom ; 2008 : Sprint vs Cogent ; 2012 : Free vs Youtube)

Internet "Tiers"

- Tier 1 network : Un réseau qui peut atteindre tous les autres réseaux sur Internet sans acheter du transit IP à un fournisseur ou payer un autre opérateur.
  AT&T, Global Crossing, Level 3, NTT (Verio), Qwest, Sprint, Verizon (ex-UUNET), SAVVIS, AOL, AboveNet, Cogent, TeliaSonera, Teleglobe, XO Communications, ...
- Tier 2 network : réseau qui a passé des accords de peering avec d'autres opérateurs, mais qui achète aussi du transit IP.
- Tier 3 network : réseau qui assure sa connectivité uniquement en achetant du transit.

Exemple



http://as.robtex.com/as2200.html

DHCP

- **Dynamic Host Configuration Protocol**
- Configuration automatique des machines
- Attribution d'une adresse IP, et d'autres paramètres :
  - Masque de sous-réseau
  - Passerelle par défaut
  - Serveurs DNS
  - ...
- Protocole (utilise UDP) :
  - DHCP Discover : demande par le client (diffusion)
  - DHCP Offer : offre du serveur
  - DHCP Request : acceptation de l'offre par le client
  - DHCP ACK : notification que l'IP a été attribuée au client
- Attribution temporaire : bail (*lease*) DHCP

Couche Transport : TCP et UDP

- Permet le multiplexage de plusieurs communications (numéros de ports, sur 16 bits)
- 2 protocoles de transport : UDP et TCP
  - UDP (*User Datagram Protocol*) :
    - Service de transport minimaliste et simple
    - Mode non-connecté (pas de sessions)
    - Pas de contrôle d'erreur ni de flux
    - Échange de **datagrammes**
    - Idéal pour les protocoles simples (DNS) ou ceux où le développeur veut tout contrôler lui-même (QUIC)
  - TCP (*Transmission Control Protocol*) :
    - Protocole complexe, masquant les contraintes du réseau aux applications
    - Mode connecté (**connexion TCP**), transport fiable d'un flot d'octets
    - Échange de **segments**
    - Le protocole de transport le plus utilisé (car facile du point de vue du développeur)

Quelques numéros de ports

Port	Service
22 / TCP	SSH
23 / TCP	telnet
25 / TCP	SMTP
53 / UDP	DNS
67 / UDP	BOOTP / DHCP
68 / UDP	BOOTP / DHCP
80 / TCP	HTTP
110 / TCP	POP3
137, 138, 139	NetBIOS
143 / TCP	IMAP
443 / TCP	HTTPS

ARP

- Address Resolution Protocol
- À l'interface entre couche Réseau et Liaison
- Problème : comment savoir à quelle adresse MAC envoyer un paquet IP ?
- ARP = Protocole de découverte des adresses MAC
- 2 types de paquets :
  - ARP request (broadcast) :
    Qui a l'IP 192.168.1.2 ?
  - ARP reply (unicast) :
    192.168.1.2 est à 00:07:cb:c7:52:5f
- Utilisation d'un cache
- Exercice : sur le réseau de l'exercice précédent, C1 envoie un paquet à C2. Toutes les tables ARP sont vides. quels sont toutes les trames échangées ?

Configuration réseau sous Linux

- Deux jeux de commandes pour les modifications transitoires :
  - Historiques : `ifconfig`, `route`

    ```
    ifconfig eth0 10.0.0.1/24
    route add default gw 10.0.0.254
    route add -net 2.2.2.0/24 gw 1.2.3.4
    netstat -rn # affiche la table de routage ; -n évite la résolution DNS
    route # affiche aussi la table de routage
    ```

  - Modernes (paquet `iproute2`, conseillé) : `ip`

    ```
    ip link show (peut être abrégé : ip l)
    ip addr show ⇝ ip a
    ip route show ⇝ ip r
    ip link set dev eth0 up ⇝ ip l s eth0 up
    ip addr add dev eth0 10.0.0.1/24
    ip route add 192.0.2.128/25 via 192.0.2.1
    ```

    voir `http://baturin.org/docs/iproute2/` et une cheat sheet de Red Hat

Configuration réseau persistante

- Dans `/etc/network/interfaces` (voir `interfaces(5)`)

```
auto eth1
iface eth1 inet static
     address 192.168.1.2/24
     gateway 192.168.1.1 # va ajouter une route par défaut
     # si nécessaire, pour ajouter des routes supplémentaires
     # (ou exécuter d'autres commandes)
     post-up ip route add 10.0.0.0/8 via 192.168.1.254
     # si le paquet resolvconf est installé, on peut indiquer
     # la configuration DNS
     dns-nameserver 8.8.8.8
     dns-search foo.com

auto eth2
iface eth2 dhcp
```

- Recharger toute la configuration : `service networking restart`
- Dé-configurer une interface : `ifdown eth1`
- Configurer une interface : `ifup eth1`

Configuration réseau persistante (2)

- D'autres outils
  - Orientés serveurs
    - `/etc/sysconfig/` (équivalent à `/etc/network/interfaces` dans le monde RedHat)
    - systemd-networkd (remplaçant intégré à systemd)
  - Orientés poste de travail
    - Network-Manager
    - wicd

Activation du routage sous Linux

- Par défaut, Linux ne route pas entre ses différentes interfaces
- Pour changer ce comportement :
  - De manière transitoire (oublié après un reboot) :
    - `echo 1 > /proc/sys/net/ipv4/ip_forward`
    - ou `sysctl -w net.ipv4.ip_forward=1`
  - De manière persistante :
    - Ajouter dans `/etc/sysctl.conf` : `net.ipv4.ip_forward=1`
    - Ou plus proprement, créer un fichier `/etc/sysctl.d/01-ipforwarding.conf` et y ajouter `net.ipv4.ip_forward=1`

Noms des interfaces

- Historiquement : eth0, eth1, ...
- Depuis récemment : noms prédictibles
  - Dépendent de la position physique de la carte réseau dans l'ordinateur
  - eno1 : sur la carte mère
  - ens1 : PCI slot 1
  - Voir `https://www.freedesktop.org/wiki/Software/systemd/PredictableNetworkInterfaceNames`

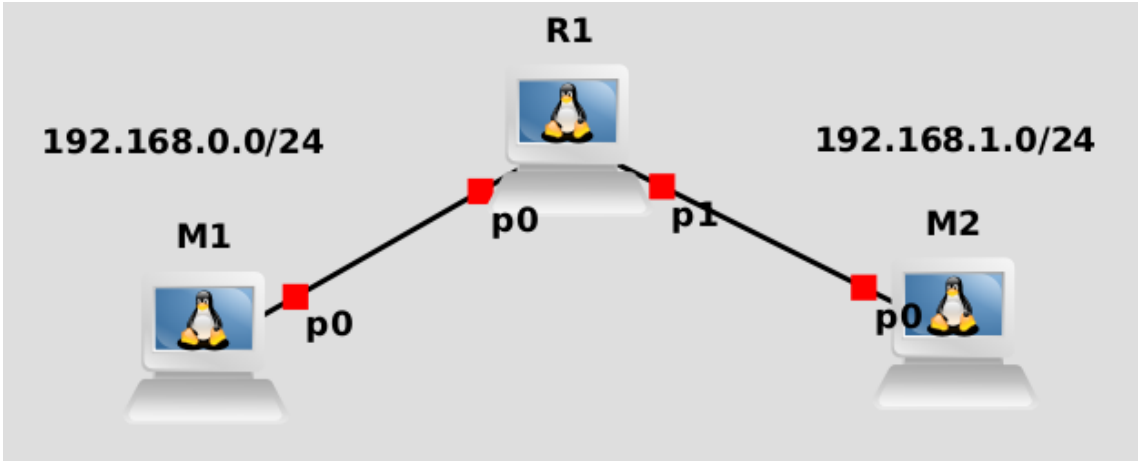
GNS3

- Simulateur réseau
- Par rapport à Vagrant
  - ☺ Topologies complexes, avec switches, routeurs, etc.
  - ☹ Pas adapté à des VM avec une configuration complexe de services réseaux

Installation de GNS3

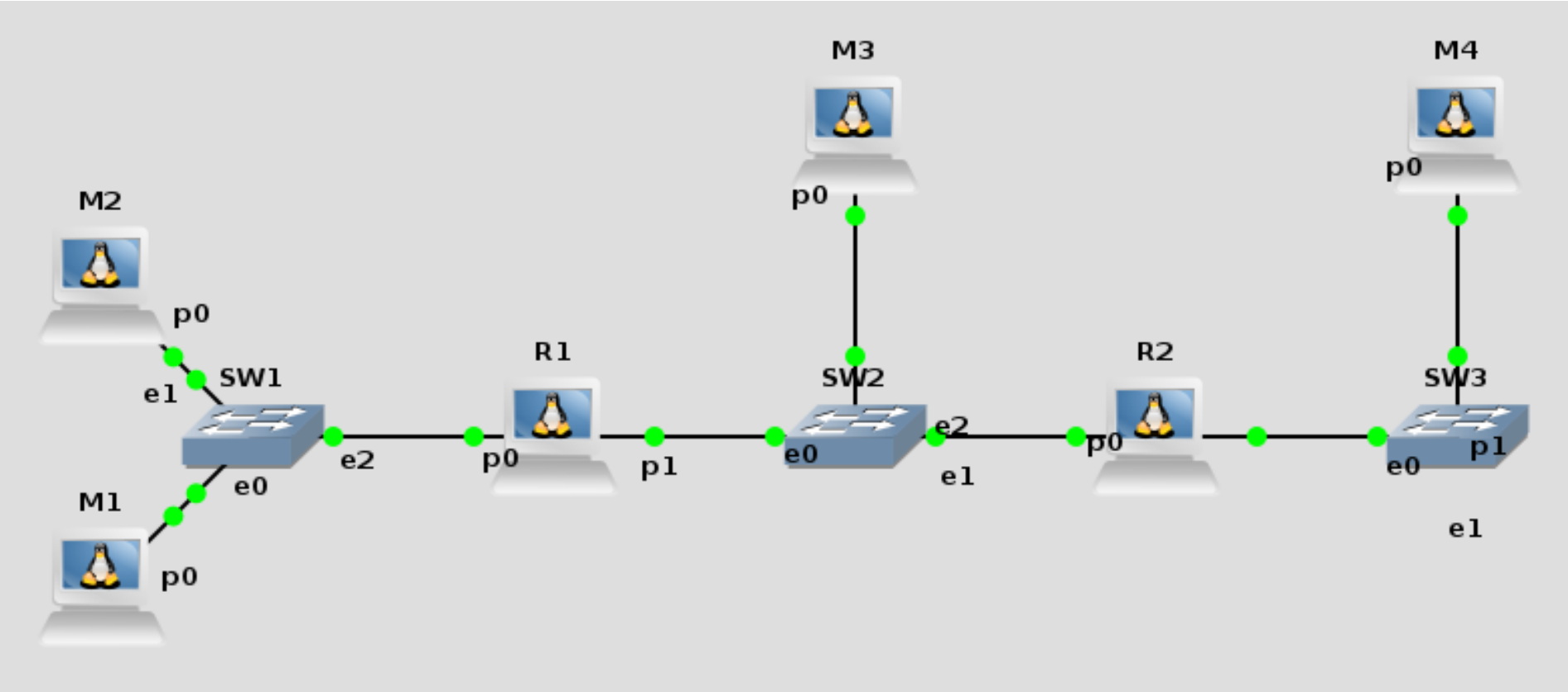
- Sous Debian 9 Stretch :
  `echo 'deb [trusted=true] http://ppa.launchpad.net/gns3/ppa/ubuntu xenial main' > /etc/apt/sources.list.d/gns3.list`
- Sous Debian 10 Buster : voir
  `https://people.debian.org/~lucas/gns3-buster/`
- Ensuite : `apt-get update ; apt-get -y install gns3-gui`
- S'ajouter au groupe `ubridge`, fermer/rouvrir la session
- Récupérer l'appliance Debian 9 :
  - `wget https://people.debian.org/~lucas/gns3/debian9.gns3a`
  - `wget https://people.debian.org/~lucas/gns3/debian9-0.5.qcow2.zip`
  - Décompresser le fichier .zip
- Lancer `gns3`
- Choisir "Run the topologies on my computer"
- Choisir "Import an appliance template file", sélectionner le fichier .gns3a

Exercice : routage (1)



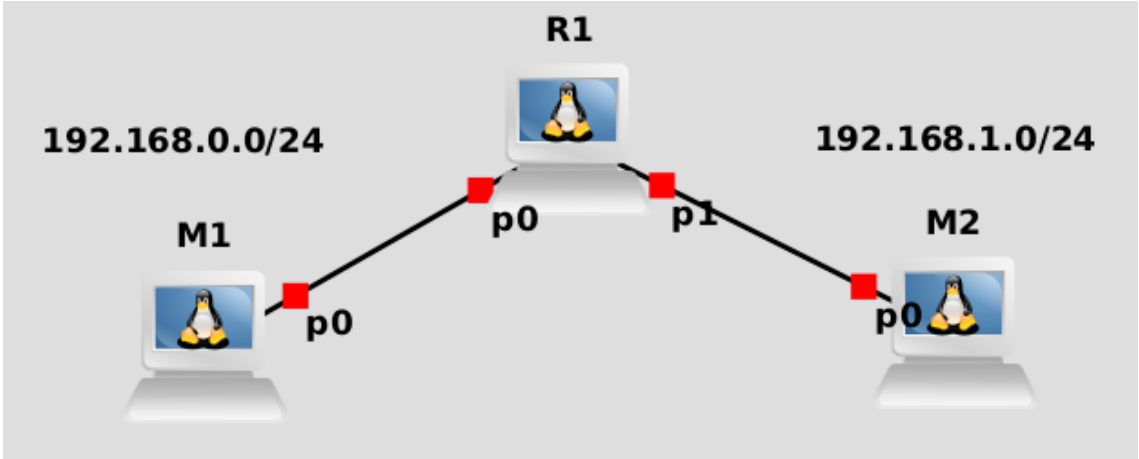
- Réaliser la topologie ci-dessus (R1 est une machine Debian 9 configurée comme un routeur), en configurant les machines d'abord de manière transitoire (avec les deux méthodes), puis de manière persistante
- Avec `ping` et `traceroute`, vérifiez que tout fonctionne bien (sinon, utilisez la fonction de capture de paquets dans GNS3 pour débugger)

Exercice : routage (2)



- Mêmes questions avec cette topologie (il est fortement conseillé de commencer par définir, sur papier, le plan d'adressage et les tables de routage à implémenter)

Exercices : firewall & ARP



- Consultez une introduction à `iptables` si vous n'êtes pas familier avec l'outil.
- Configurez des règles de filtrage sur R1, avec `iptables` :
  - SSH interdit depuis M1 vers M2
  - ICMP (`ping`) autorisé si, sur M2, on ping M1, mais pas l'inverse
- Configurez R1 pour que le réseau 192.168.0.0/24 soit NATé dessus. Utilisez Wireshark (fonction capture de paquets) pour confirmer.
- ARP : observez le contenu des tables ARP avec `ip neigh`, supprimez des entrées (`arp -d` ou `ip neigh`) et observez (avec Wireshark) les requêtes ARP nécessaires au re-peuplement de la table ARP

Exercices : firewall (2)

- Récupérez une appliance Debian 10 et importez là comme précédemment :
  - `wget https://people.debian.org/~lucas/gns3/debian10.gns3a`
  - `wget https://people.debian.org/~lucas/gns3/debian10-0.1.qcow2.zip`
- Debian 10 inclut `nftables`, qui remplace `iptables`. Refaites les questions précédentes sur le filtrage avec `nftables` au lieu de `iptables`.
- Documentation utile :
  - `https://wiki.nftables.org/`
  - `https://wiki.debian.org/nftables`

Notes diverses, FAQ, troubleshooting

- On peut changer le nom des machines avec :
  `hostnamectl set-hostname m1`
- Impossible d'ouvrir les consoles des VM : il faut installer les paquets `xterm` et `telnet`
- Erreur : failed to initialize KVM : Device or resource busy
  - Probablement dûe à un conflit entre KVM et une autre solution de virtualisation (Virtualbox par exemple).
  - Pour arrêter virtualbox, arrêtez toutes les machines virtuelles, puis :
    `rmmod vboxpci vboxnetflt vboxdrv`
- Capture de paquets
  - Il faut faire un clic droit sur le lien concerné
  - Pour que ça fonctionne, il faut que votre compte utilisateur soit ajouté au groupe `wireshark`
  - Autre solution : utiliser `tcpdump` (en console)
- Impossible d'ajouter un switch : installer le paquet `dynamips`