Défense périmétrique

- Comprendre les caractéristiques des principaux modules de sécurité *switch*, *router*, *firewall*, *proxy*, *gateway*, …
- Modèle en couches "du bas vers le haut"
- Lab Hacking (vol de mot de passe telnet et https)
- Lab Firewall & DMZ (tests avec VirtualBox)
- Network scanners (tests de pénétration)
- Web Proxies

Principaux composants du labo → Schéma L

- **Firewall pfSense** et 3 réseaux : Intranet – DMZ – Internet (failover)
- **Serveur de fichiers** 10.2.1.1 CentOS6 2TB

  Interface utilisateur de type CLI

  Simplicité et stabilité

  Excellente documentation (anglais et français)

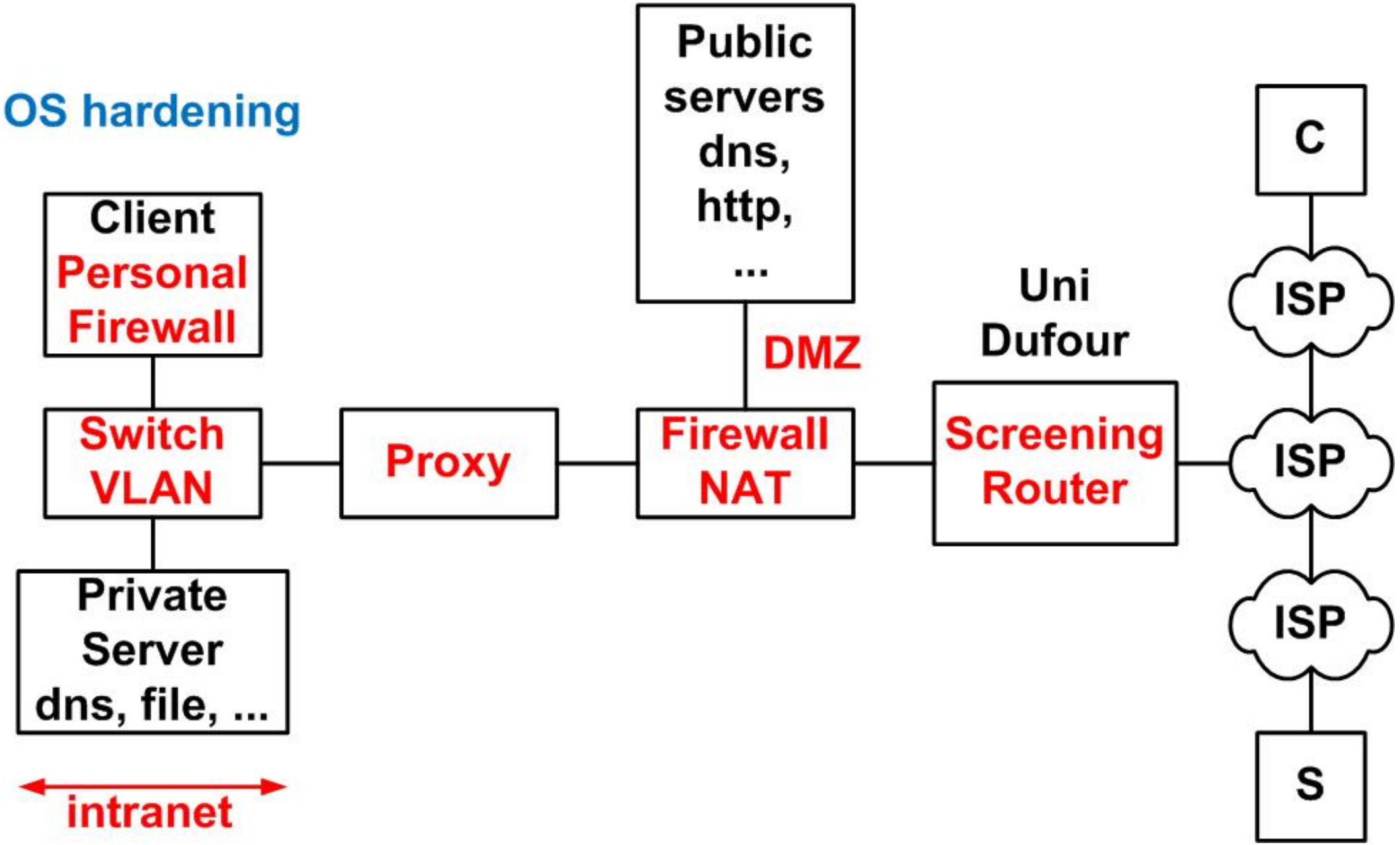
  Services Samba = serveur de fichiers compatible Windows
- **Commutateurs Ethernet 1 Gbit/s**

  Netgear 24 ports

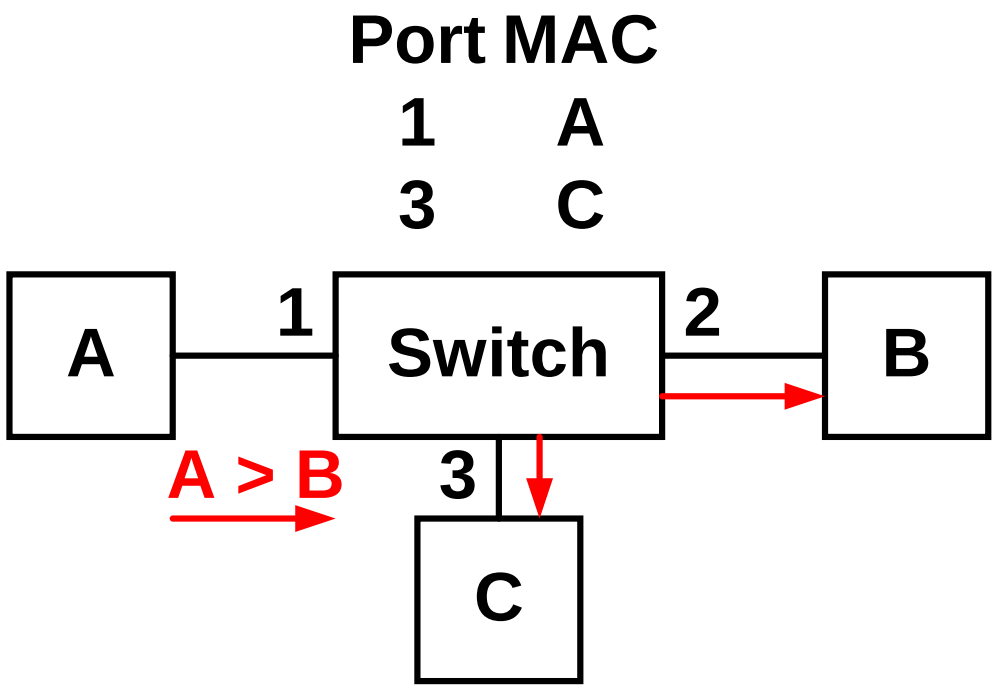
  Netgear 16 ports

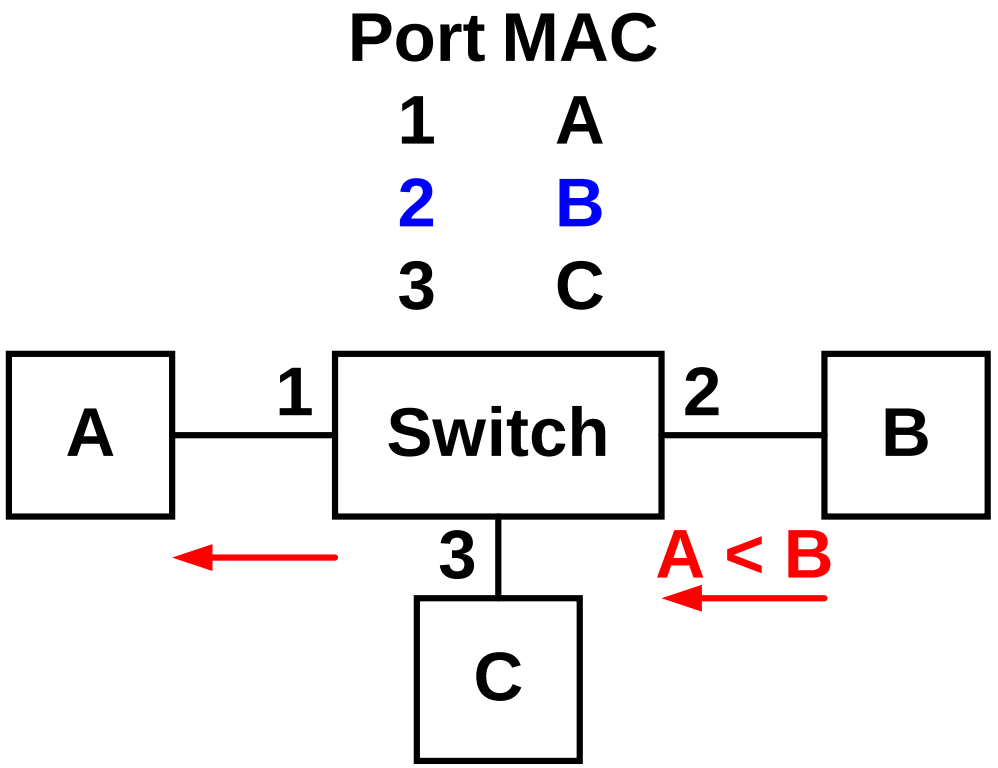
- **PC Windows 7 – VirtualBox (Ubuntu) – Fedora**

Défense en profondeur et modèle en couches



Switch : Table (rappel)



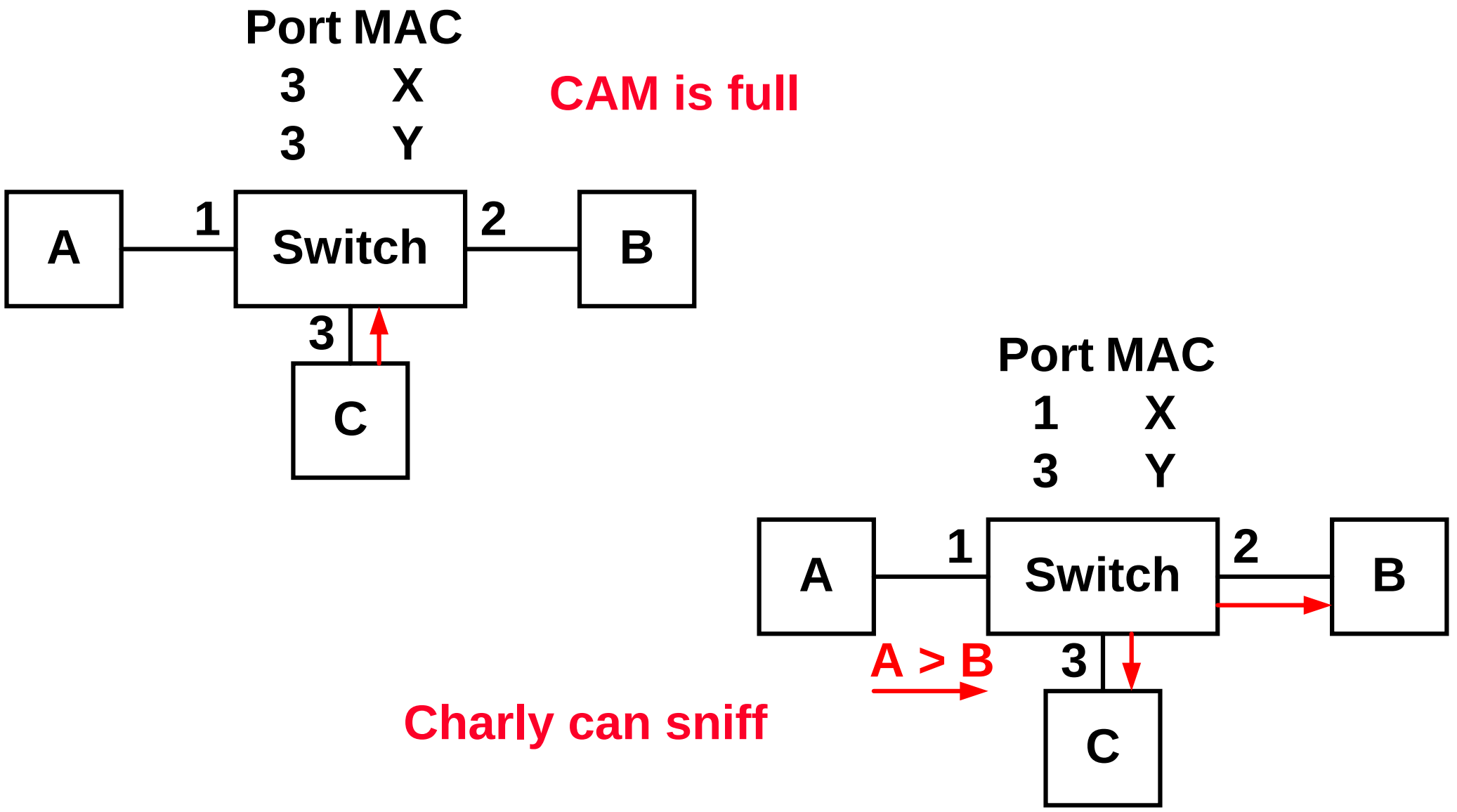


CAM (Cisco)

Content Addressable Memory

Max 8000 MAC addr (2950)

MAC flooding → CAM overflow



Switch Port Security

- Static port → Specify MAC addresses for each port
  Only 1 MAC address per port

- Dyn. Port → Learn limited number of MAC addresses / port

- Switch can block or shutdown

ARP cache (rappel)

A

B

Empty cache

Empty cache

ARP req →

DA_eth = FF FF FF FF FF FF

IP_A : MAC_A

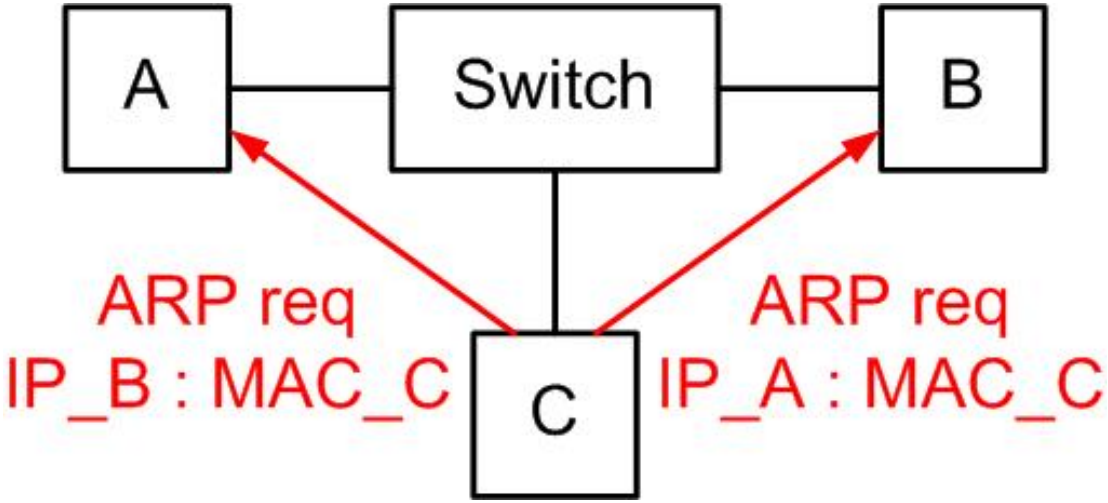
← ARP resp

IP_B : MAC_B

Ex 1 → slide 108

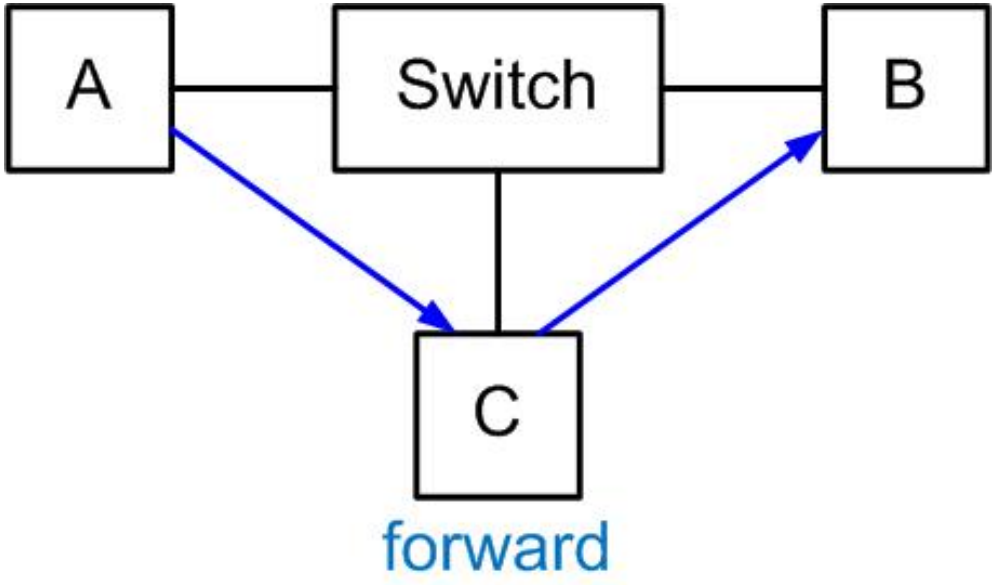
- Déterminer l'algorithme de mise en mémoire dans le cache ARP (slide 7)

ARP poisoning (corruption de cache)



C modifie le contenu des caches ARP des victimes A,B
Avec des cibles Windows, C peut utiliser des paquets ARP request pour créer l'équivalence IP : MAC voulue

Le paquet destiné à B émis par A est d'abord envoyé à C
C peut le lire et le modifier
C l'émet vers B
→ Attaque Man in the Middle
Outils Cain (Win) & dsniff (Linux)



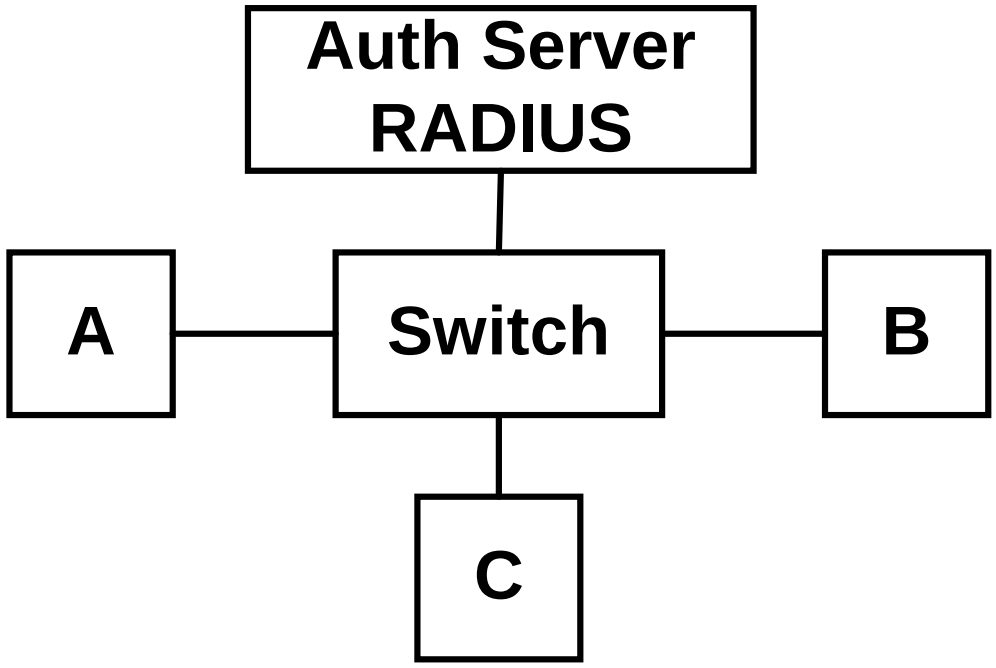
ARP Security

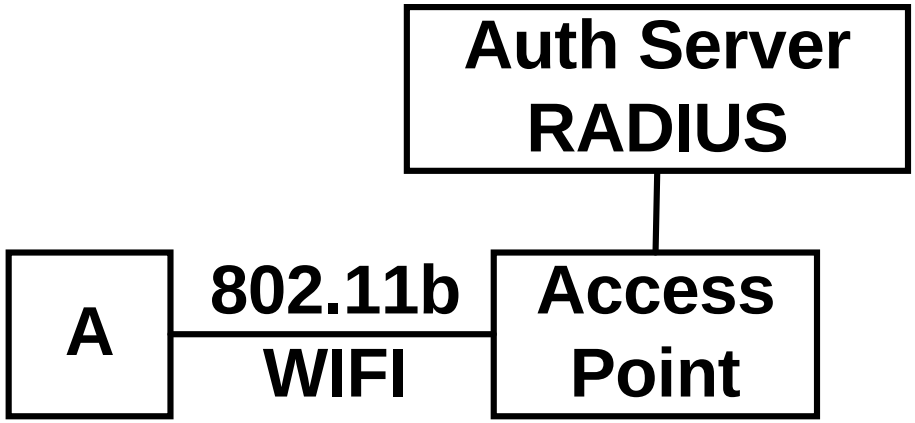
- Disable dynamic ARP cache

  `arp –s IP MAC` entry is permanent

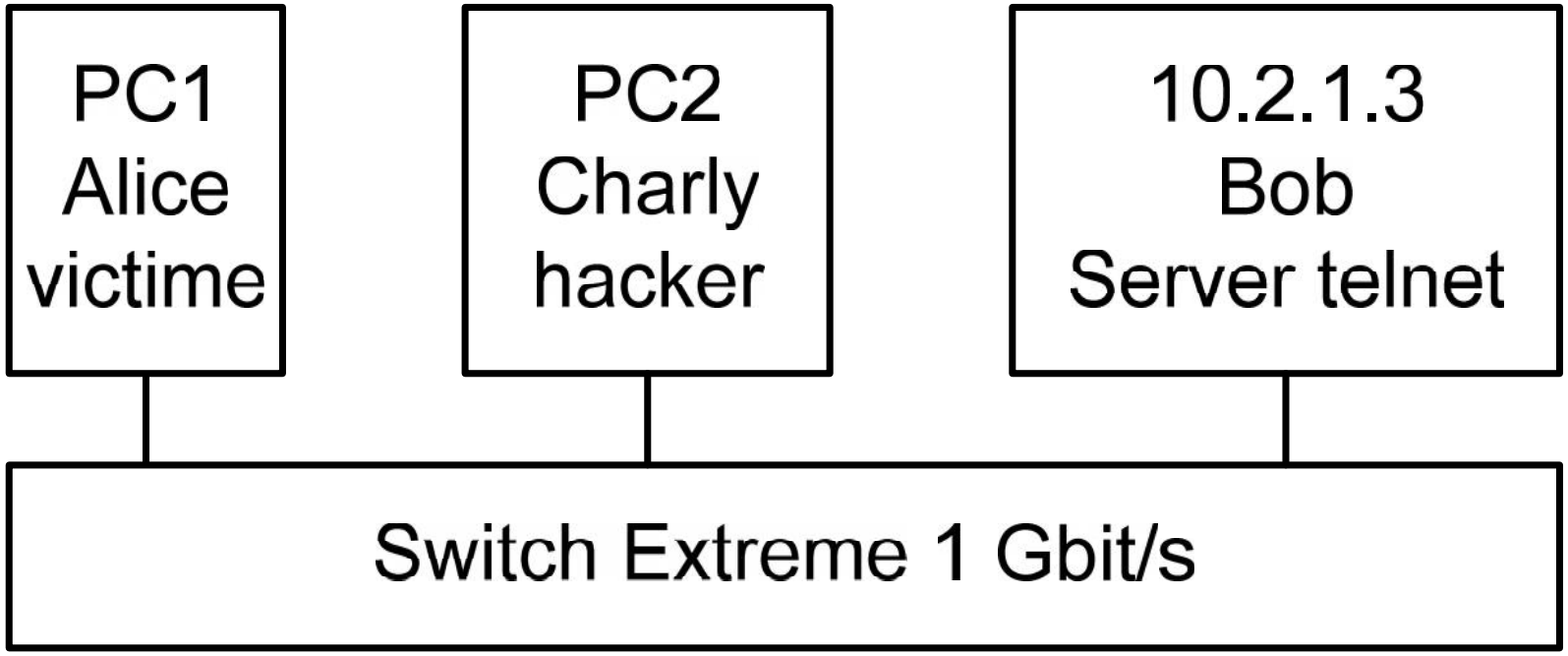
  bug dans Win7; ok avec SP1

- Authentification 802.1x depuis client XP



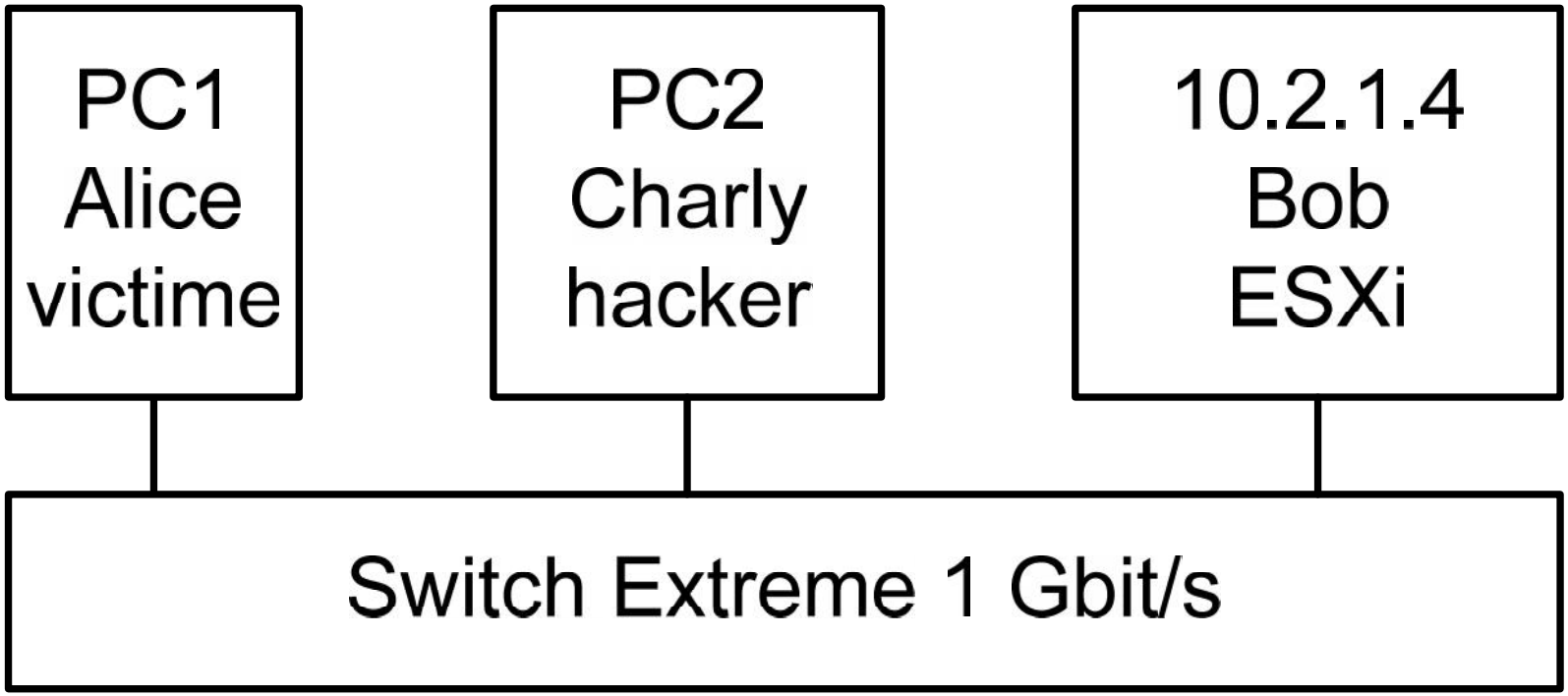


Labo Hacking



- §2 : Charly veut voler les paramètres username et password donnant à Alice l'accès au serveur telnet 10.2.1.3
- §2.1 : Trouver les adresses Eth & IP (Alice & Charly)
- §2.2 : Utiliser Cain pour effectuer l'attaque ARP poisoning

Labo Hacking



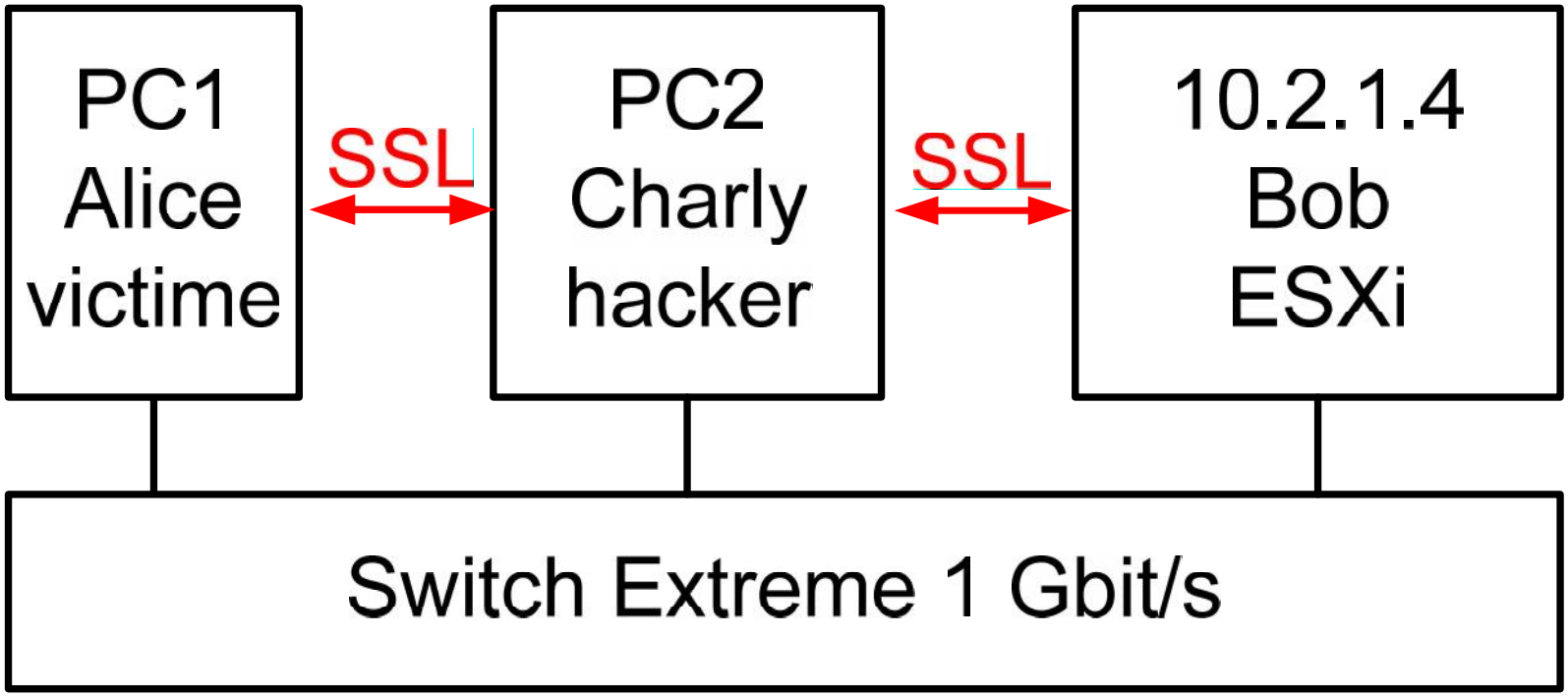
- §3 : Charly veut voler les paramètres username et password protégés par une session SSL (https)

  ESXi est un hyperviseur (virtualisation)

- §3.1 : Utiliser Cain pour effectuer l'attaque ARP poisoning

  suite slide 13

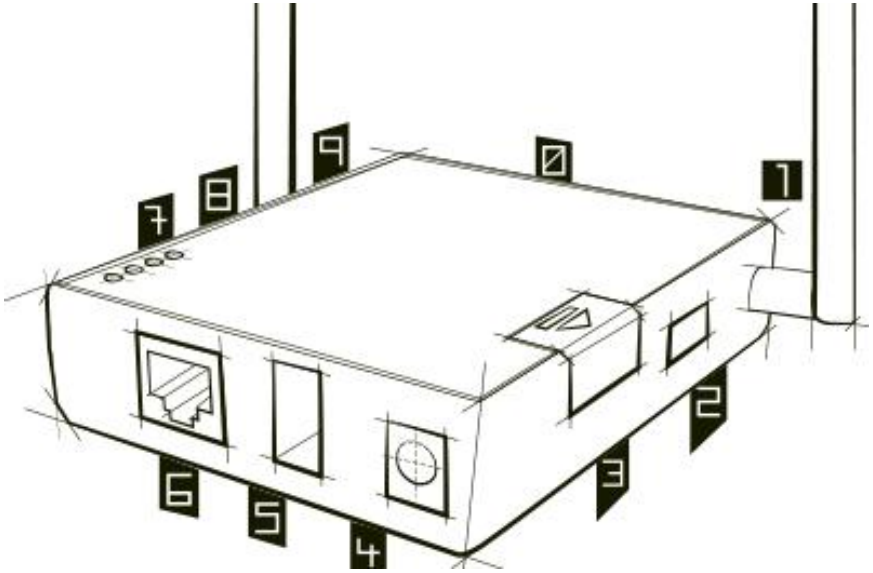
Labo Hacking



1. Alice : https://10.2.1.4
2. Bob envoie son certificat
3. Charly prend le rôle de **client SSL**
4. Charly prend le rôle de **serveur SSL** en envoyant un certificat malicieux
5. Alice (naïve) installe ce certificat
6. Charly **(Man in the Middle)** récupère username - password

WiFi auditing and penetration testing → risques !!!

- The WiFi Pineapple is a unique device developed by Hak5 for the purpose of WiFi auditing and penetration testing. Since 2008 the WiFi Pineapple has grown to encompass the best rogue access point features, unique purpose-built hardware, intuitive web interfaces, versatile deployment options, powerful software and hardware development aids, a modular application ecosystem and a growing community of passionate penetration testers.



1. SMA Antenna Connector
2. Mode Selection Switches
3. Expansion Bus Door
4. DC Power Port
5. USB 2.0 Host Port
6. 10/100 Ethernet Port
7. Indicator LEDs
8. MicroSD Storage Slot
9. SMA Antenna Connector

- https://www.wifipineapple.com/

Virtual LAN (VLAN) : motivation

- Grouper des ordinateurs (postes de travail, serveurs, …) par secteur d'activité

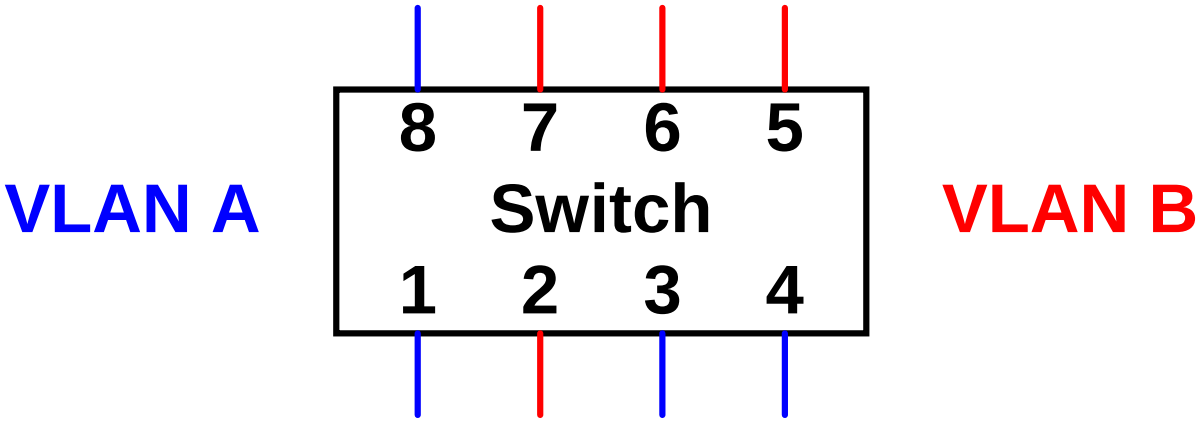
  Isoler les groupes → un domaine de diffusion par groupe

  Exemple : le flux du département R&D n'est plus visible sur le réseau de la comptabilité

- Les flux de diffusion *(broadcast)* ne sont plus propagés sur l'ensemble du site

- Certains groupes n'ont volontairement aucun accès à l'extérieur pour des motifs de sécurité *(intranet)*

VLAN basé sur le numéro de port



- Ports du VLAN A 1 3 4 …
- Ports du VLAN B 2 5 …
- Exige une reconfiguration du commutateur si le poste de travail est déplacé du port 1 sur le port 2

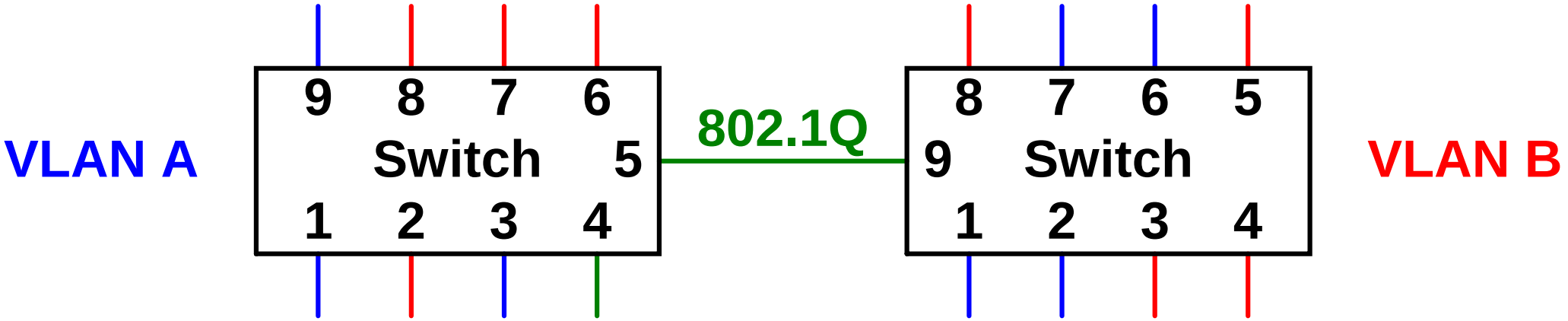
VLAN basé sur l'adresse physique

- Adresse physique = *MAC address*
- Adresses du VLAN A 20 56 78 AE 10 A6

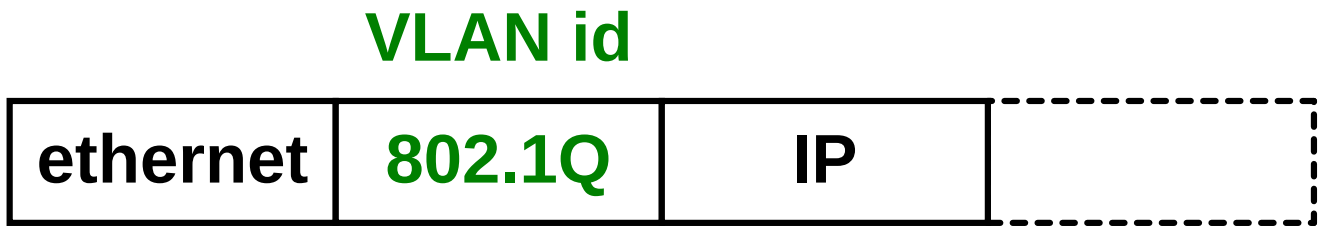
  ...
- Adresses du VLAN B 5E D3 6A F8 92 C7

  ...
- Pas de reconfiguration si le poste de travail est déplacé
- Variantes basées sur adresses IP, ports UDP-TCP, …

VLAN : interconnexion



- Le protocole 802.1Q permet d'étendre des VLANs sur plusieurs commutateurs



Best Practices for switches & VLAN

- Assigner un mode à chaque port pour éviter qu'il soit en mode automatique (le commutateur détecte le partenaire = *endpoint* ou *switch* pour placer le port dans le bon mode)

- Limiter le nb d'adresse Ethernet par port (idéalement à 1)

```
#  switchport port-security maximum 1
```

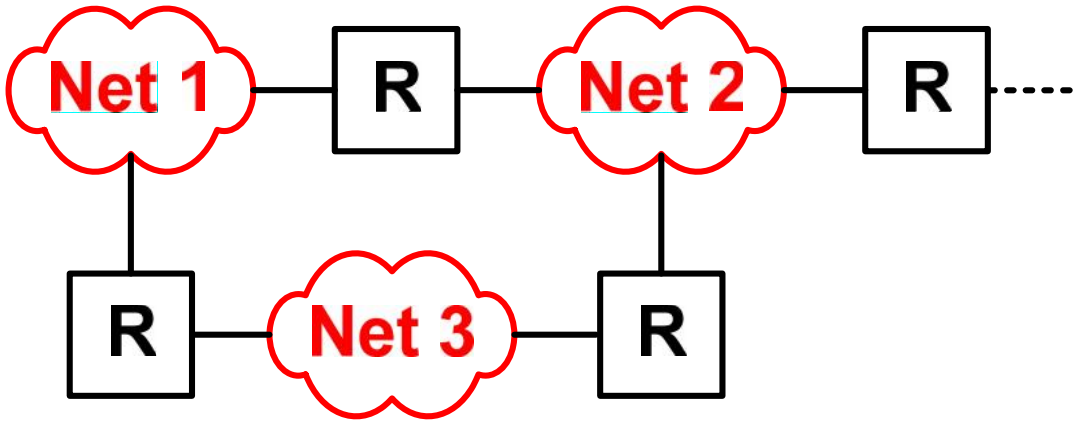
- Désactiver le cache dynamique de certains équipements critiques comme *firewall* (slide 3), …

- Détecter les changements adresse Ethernet : adresse IP (arpwatch)

- Configurer un port en mode écoute pour un analyseur (Wireshark)

Internet : routeurs

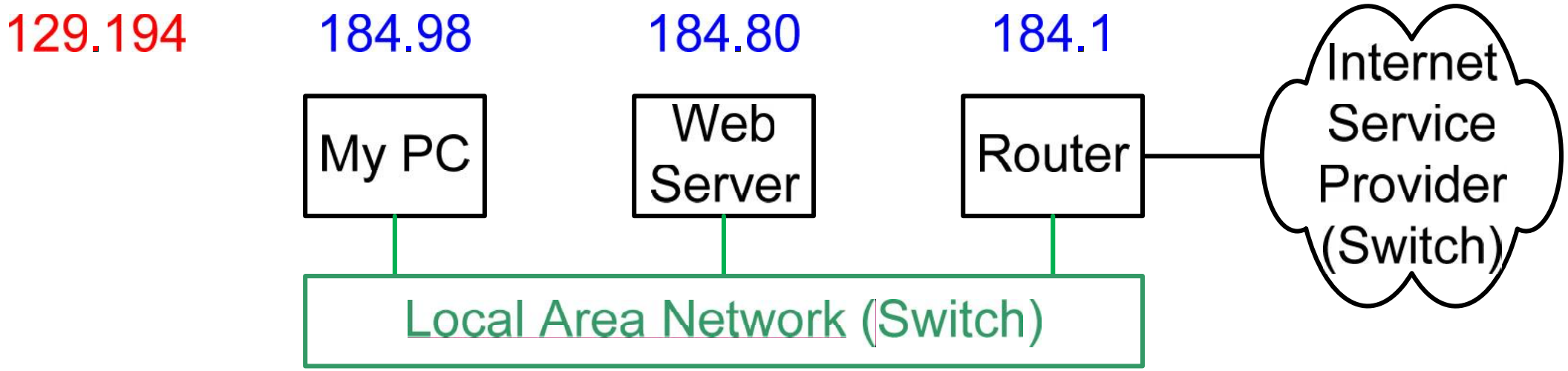
- *Internet* est constitué de réseaux *(Network)* reliés par des routeurs



- Adresse IP (32 bits) = network + host
  Serveur web du labo = 129.194.184.80 http://129.194.184.80/
  → adresse de classe B
  → network = 129.194
  → host = 184.80

Configuration de mon PC

- UniGE dispose de la classe B = 129.194.H.H



• *IP address*	129.194.184.98	Adresse IP
• *Subnet mask*	255.255.0.0	Masque
• *Router*	129.194.184.1	Routeur
• *DNS*	129.194.4.6	Serveur DNS

Subnet Mask (1)

- Valeur par défaut (adresse de classe B dans notre cas)

255.255.0.0

255	255	0	0
11111111	11111111	00000000	00000000

- Ce masque permet de distinguer, parmi toutes les destinations possibles, entre **destination directe** ou **indirecte**

- Notation CIDR pour mon PC : 129.194.184.98/16 (16 bits à 1)

Subnet Mask (2)

- **Destination directe**

  ping 129.194.184.80

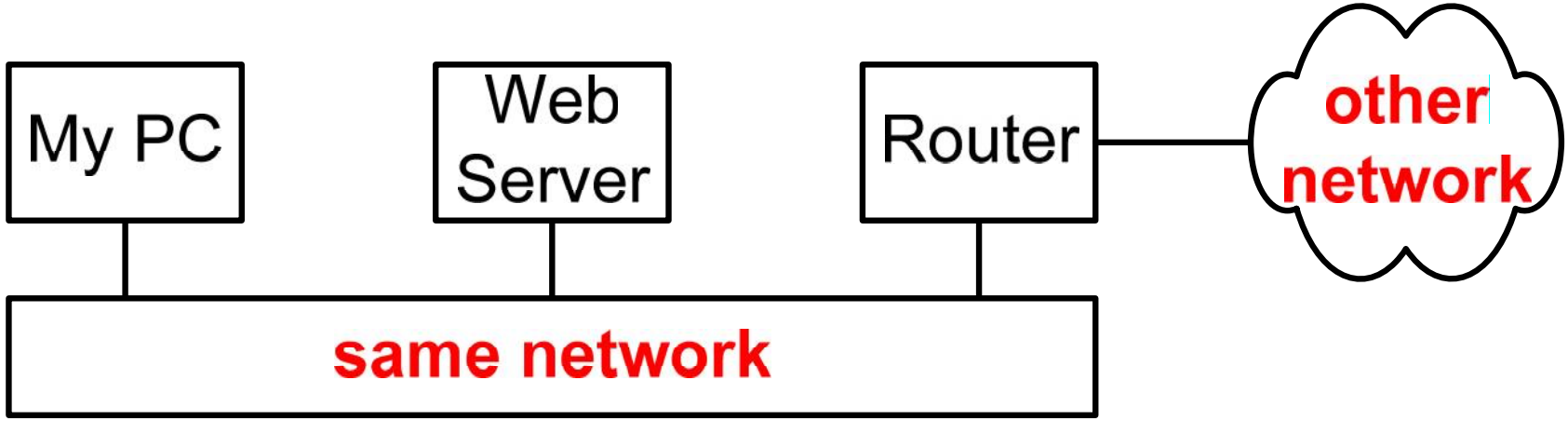
  subnet mask 255.255.0.0 → same network

- **Destination indirecte**

  ping 130.59.1.40

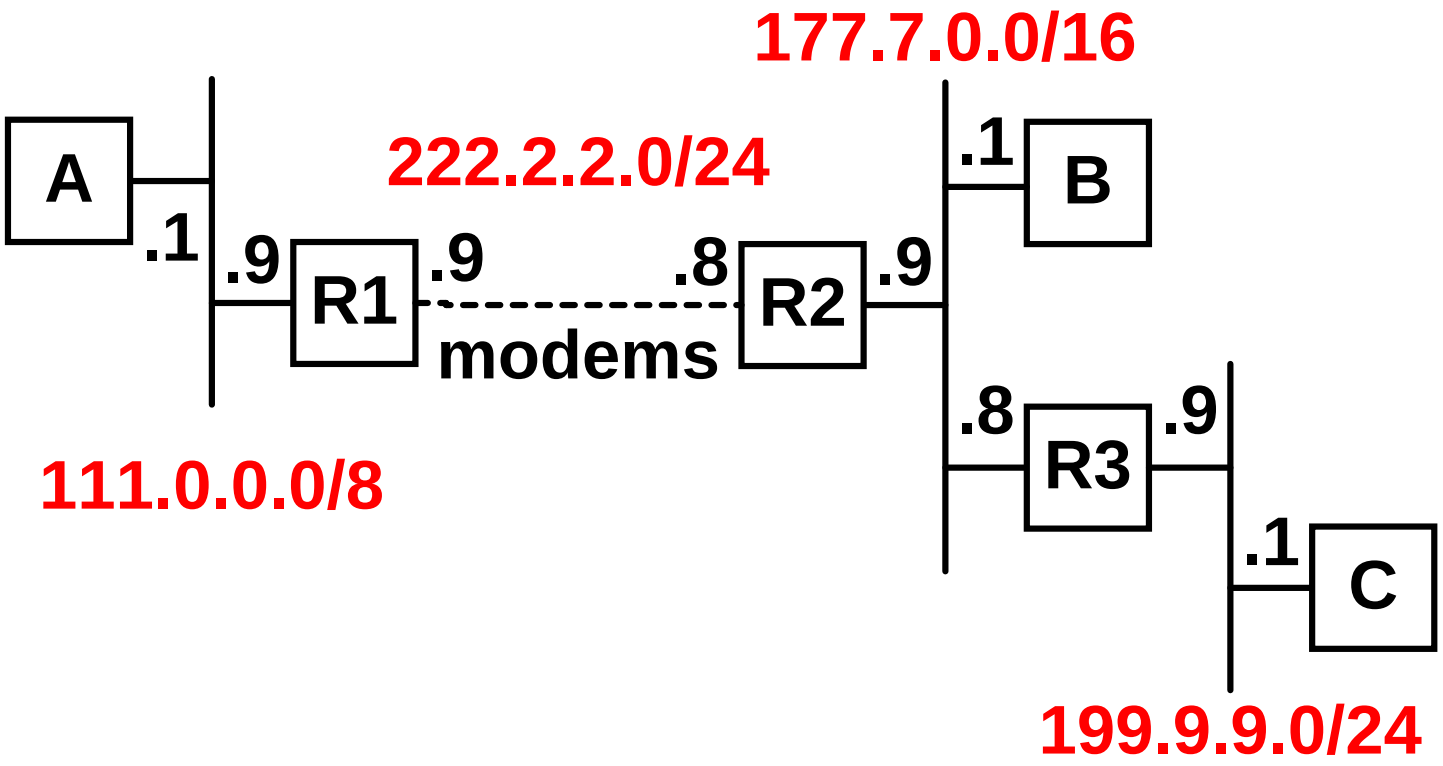
  subnet mask 255.255.0.0 → other network

  router = 129.194.184.1



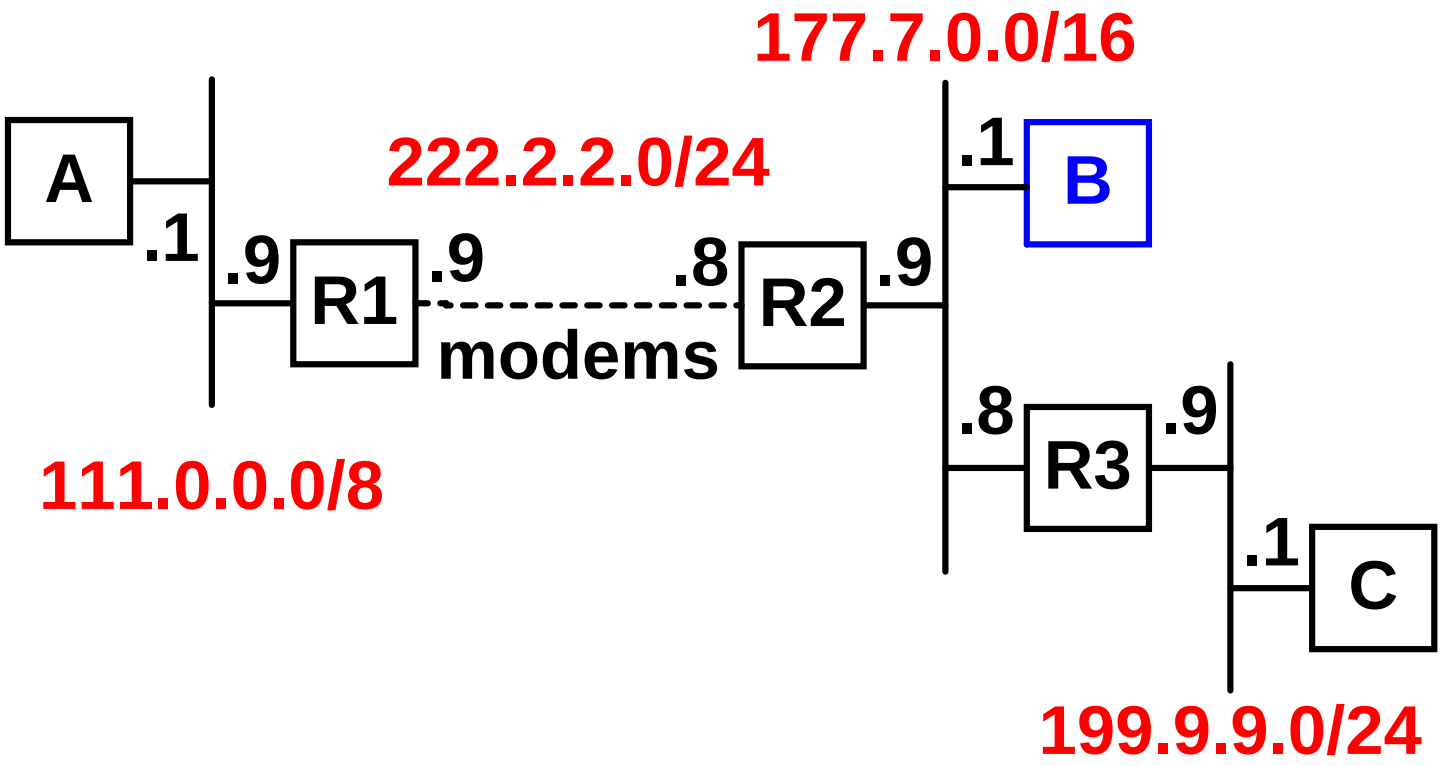
Routage statique

- Dans cet exemple, chaque équipement est configuré manuellement (commandes Unix)



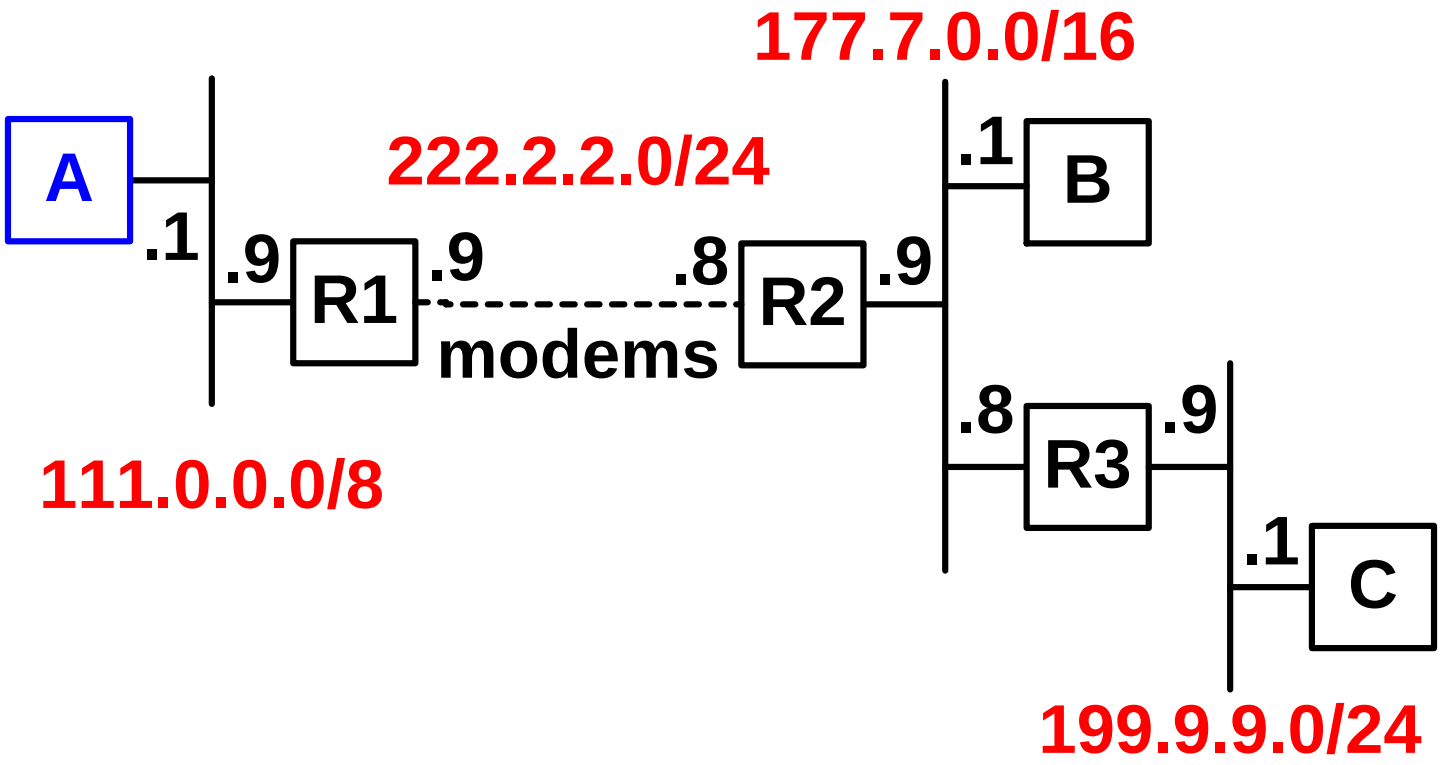
Sur la machine B

- `ifconfig eth0 177.7.0.1  mask 255.255.0.0`
- `route add 111.0.0.0  177.7.0.9`
- `route add 199.9.9.0  177.7.0.8`



Sur la machine A

- `ifconfig eth0 111.0.0.1  mask 255.0.0.0`
- `route add default 111.0.0.9`



Sur le routeur R1

- **`ifconfig eth0 111.0.0.9  mask 255.0.0.0`**
- **`ifconfig le0 222.2.2.9  mask 255.255.255.0`**
- **`route add default 222.2.2.8`**
- **`sysctl -w net.ipv4.ip_forward=1`** activer routage

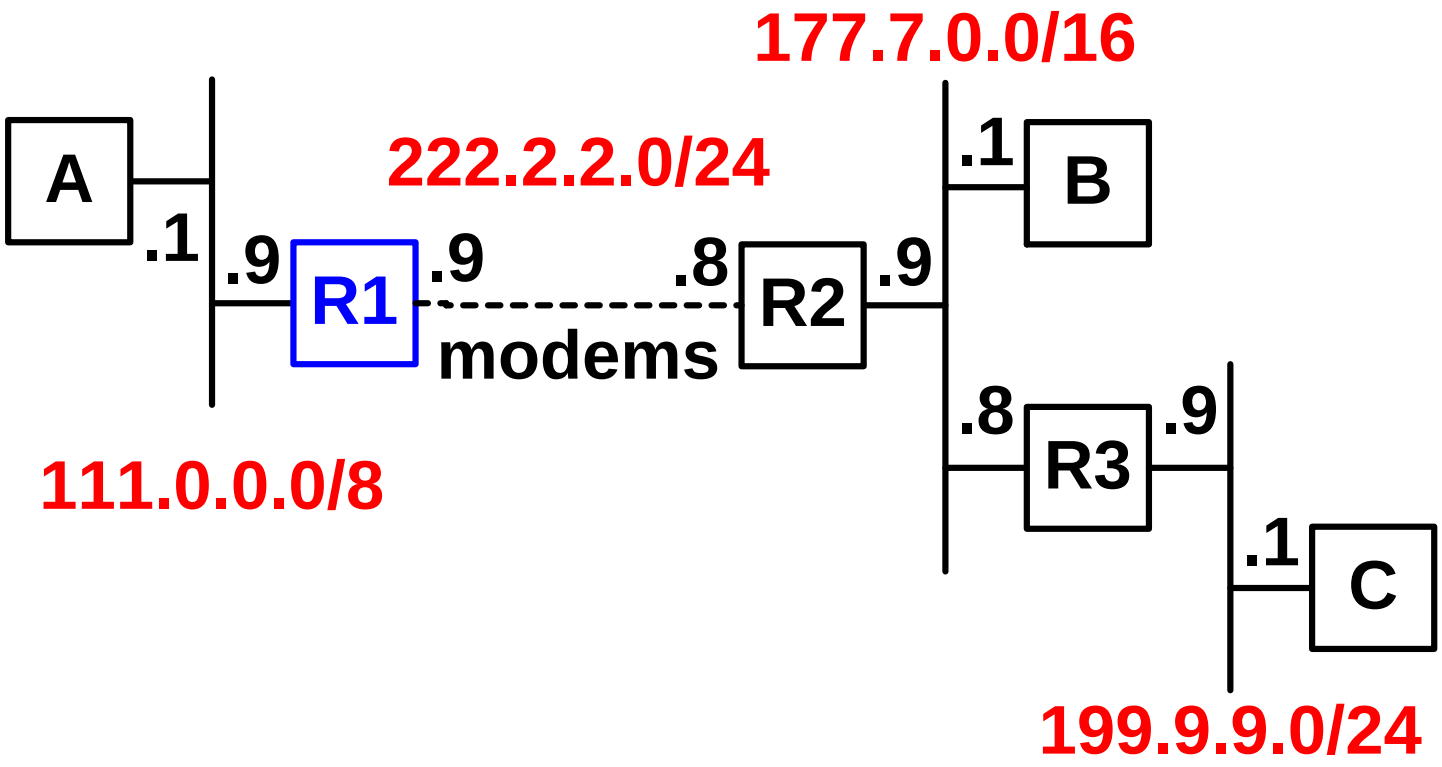


Table de routage de R1

- Chaque routeur gère une table de routage IP (*IP routing table*) qu'il consulte à chaque fois qu'il reçoit un paquet

- Pour R1

Destination	Routeur	Interface
111.0.0.0	connecté	eth0
222.2.2.0	connecté	le0
0.0.0.0	222.2.2.8	

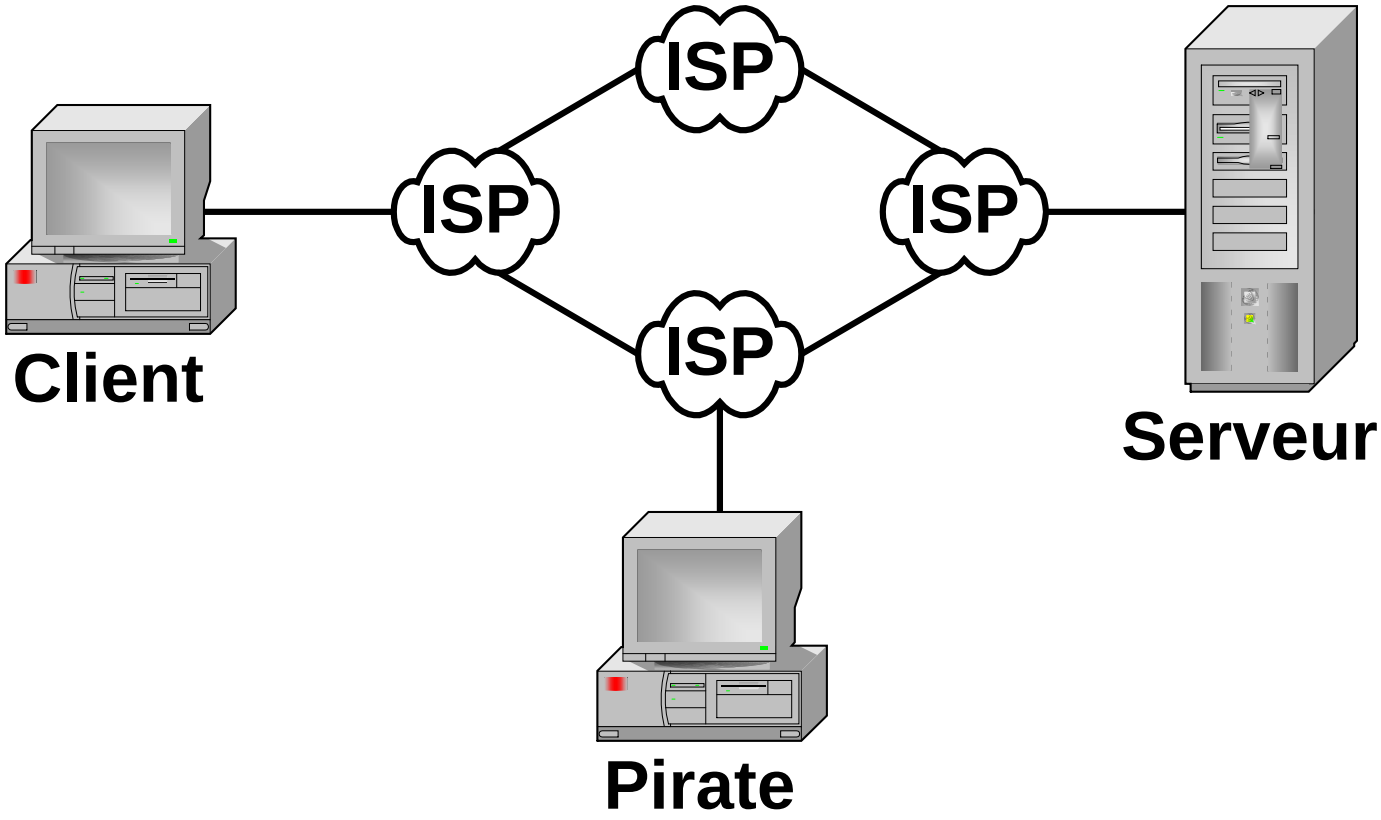
- Chaque routeur possède généralement une route par défaut

Ex2 : déterminer les commandes pour R2 → slide 109

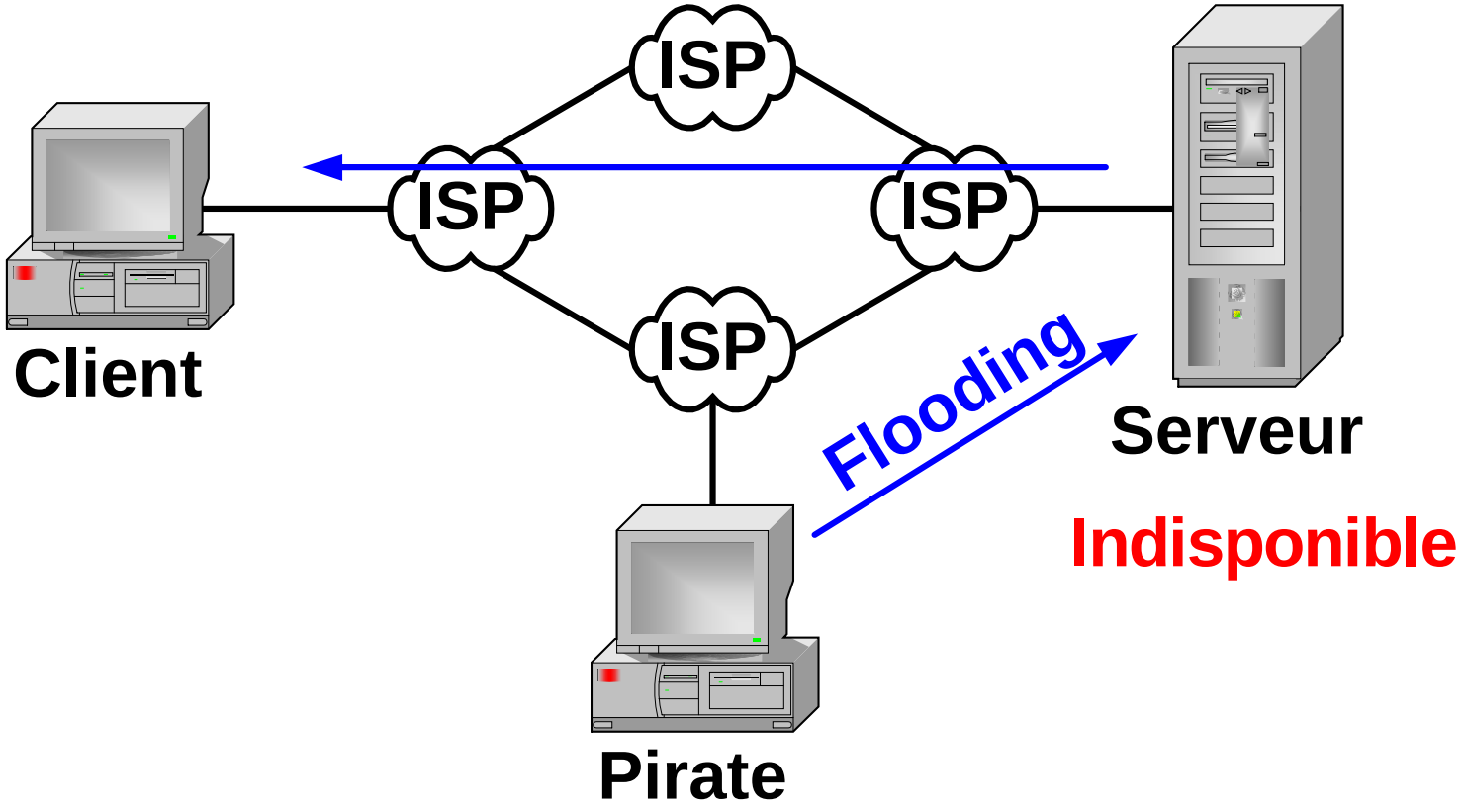
IP Spoofing

- Utiliser une fausse adresse IP source

  Se faire passer pour autrui *(impersonation)*



Denial of Service : TCP SYN Flooding & IP Spoofing

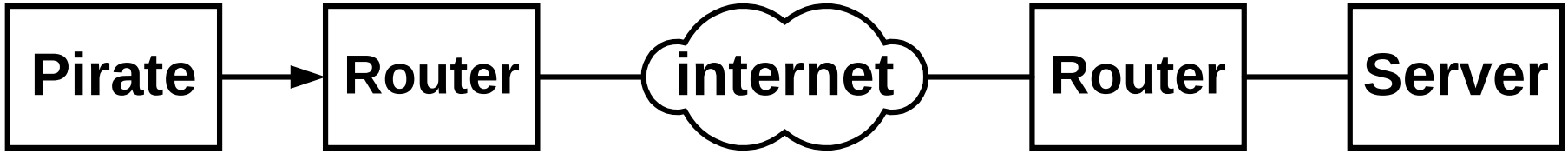


Denial of Service : TCP SYN Flooding & IP Spoofing

Pirate		**Server**
IP Spoofing	→ SYN	
		allocation mémoire
	← ACK, SYN	
		temporisateur d'établissement de connexion
IP Spoofing	→ SYN	
IP Spoofing	→ SYN	
IP Spoofing	→ SYN	
		plus de mémoire disponible

Denial of Service (DoS)

- Solution Bloquer la source (RFC 2267 – 1998)
  Exige la participation active des ISPs



forward if
valid IP Source Address

- https://www.ovh.com/fr/anti-ddos/principe-anti-ddos.xml
- http://www.zdnet.fr/actualites/ovh-noye-par-une-attaque-ddos-sans-precedent-39842490.htm un botnet composé de 145'000 caméras produit un DDOS de 1.5 Tbps !!! (sept 2016)

Private IP addresses

- Certaines plages d'adresse ip sont réservées à un usage privé *(intranet)* et définies dans la RFC 1918 *(Address Allocation for Private Internets)* :

10.0.0.0	–	10.255.255.255	1 réseau classe A
172.16.0.0	–	172.31.255.255	16 rés. classe B
192.168.0.0	–	192.168.255.255	256 rés. classe C

- Les routeurs d'*internet* doivent être configurés pour ignorer ces adresses → adresses non routables

- NAT *(Network Address Translation)*

  PAT *(Port Address Translation)*

Plan d'adressage IP privées du labo

- **10.2.x.x Labo A409**

- **10.2.0.x Composants réseau**
- **10.2.0.1 pfSense LAN interface**
- **10.2.0.1x Switch Extreme**
- **10.2.0.2x Switch Netgear**

- **10.2.1.x Server**
- **10.2.1.1 A1 = File Server Ubuntu 12**
- **10.2.1.10 G16 Admin (4 serveurs virtualisés)**

- **10.2.2.x PC liste pfSense – Status – DHCP lease**
- **10.2.3.x Client DHCP hors liste**

- **10.10.10.x DMZ**

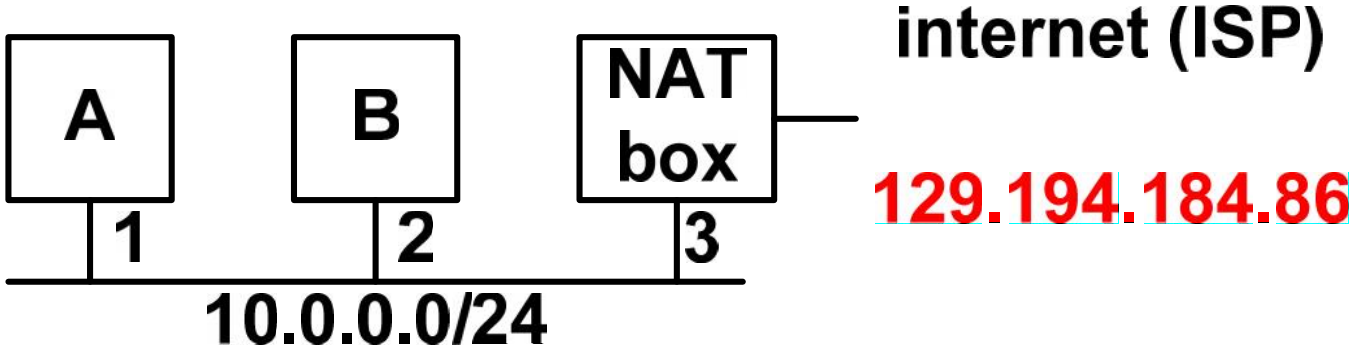
Ex 3 → *slide 110*

- En notation CIDR *(Classless Inter-Domain Routing)*, les réseaux précédents correspondent à 10.2.0.0/16 et 10.10.0.0/16

- Déterminer l'intervalle du réseau IP = 11.0.0.0/8

Dynamic NAT (1)

- Plusieurs ordinateurs et une seule adresse IP routable



- Adressage privé et translation d'adresse

- Configuration de A

IP address	10.0.0.1
Subnet mask	255.255.255.0
Router	10.0.0.3
DNS	

Dynamic NAT (2)

- Demande de connexion A → S

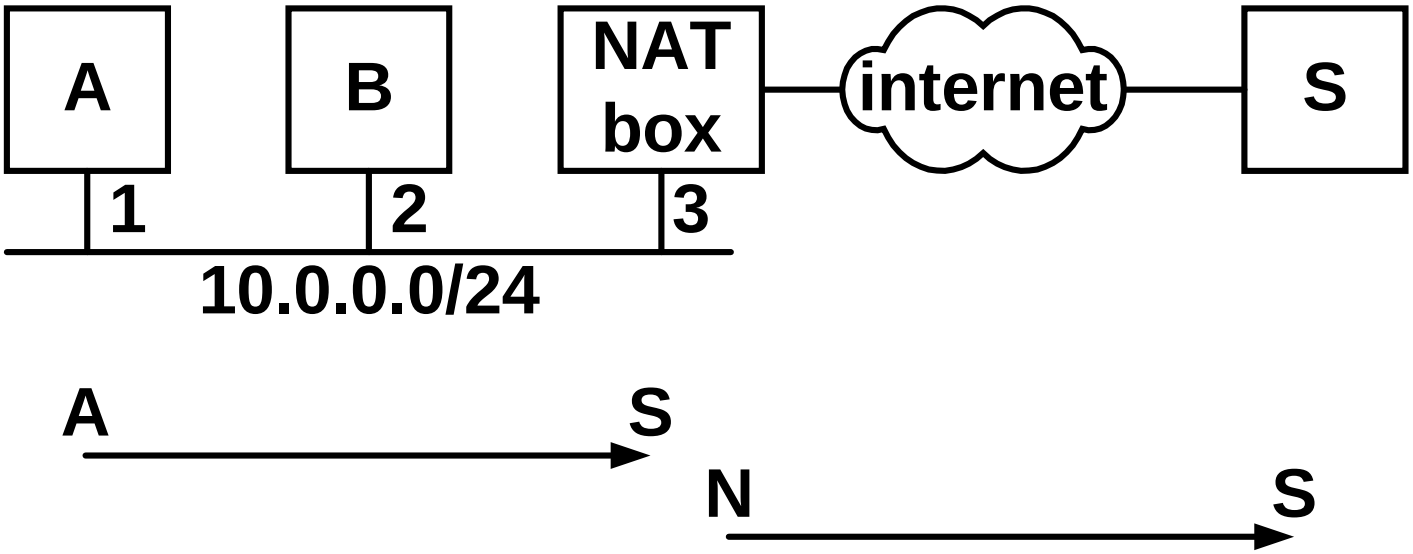
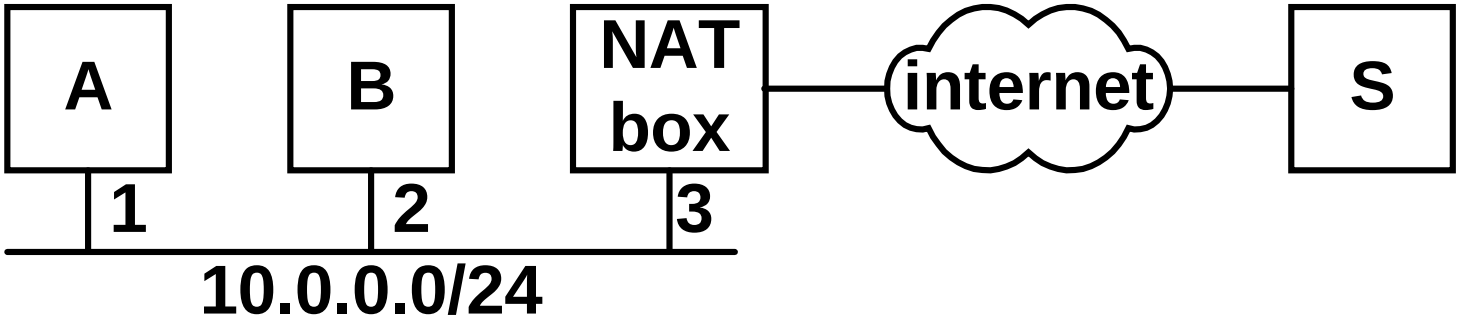


Table dynamique

10.0.0.1:1024 ← → 129.194.184.86:63450

PAT *(Port Address Translation)*

Dynamic NAT (3)



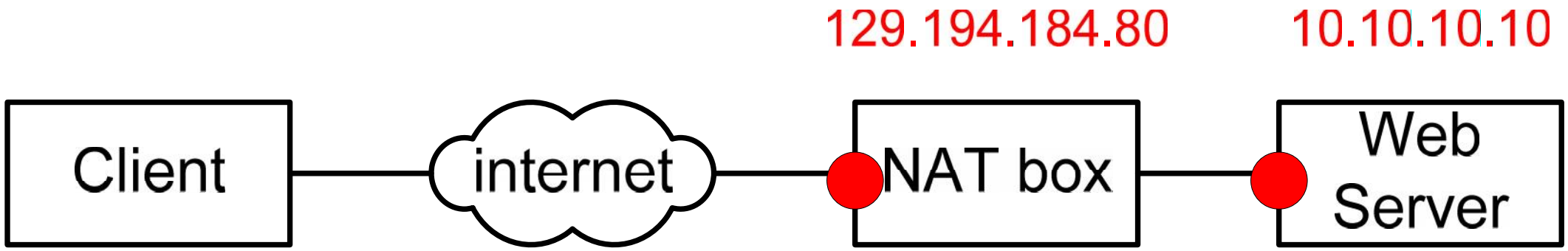
- Ce module NAT cache (mascarade) un réseau interne, utilisant une plage d'adresses privées, derrière une seule adresse ip publique

- Il peut offrir un service DHCP du côté interne

- Un client du réseau *internet* ne peut pas accéder aux serveurs du réseau privé (adresses privées non routables)

Accès au serveur du réseau privé (Static NAT)

- Illustration avec le serveur web du labo

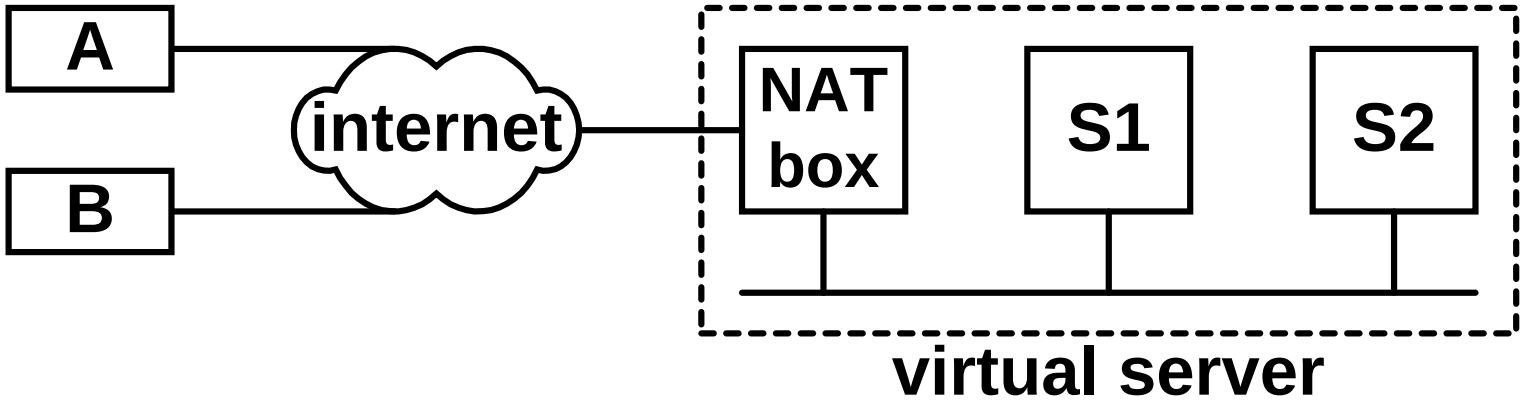


- La redirection doit être entrée manuellement → Static NAT

- Table statique
  129.194.184.80:80 ← → 10.10.10.10:80

- Suite dans labo DMZ

Load balancing



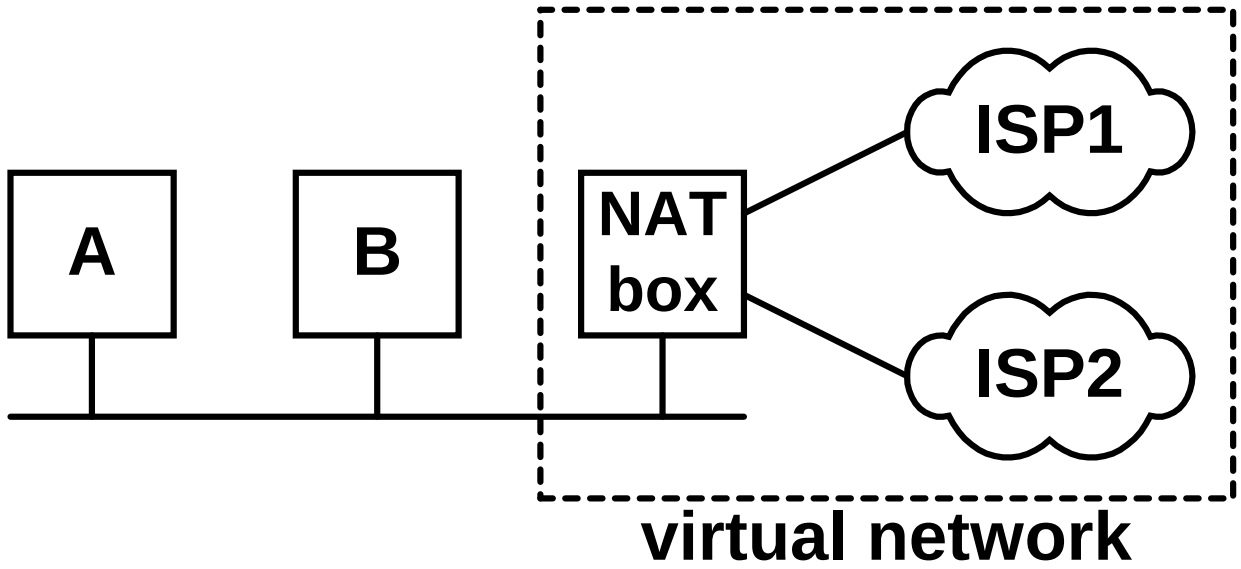
- Les serveurs S1 et S2 associés au module NAT forment un serveur virtuel *(virtual server)*

  Ainsi le premier client utilisera le serveur S1, le second client S2,…

- Suite dans cous Réseaux Avancés

NAT router

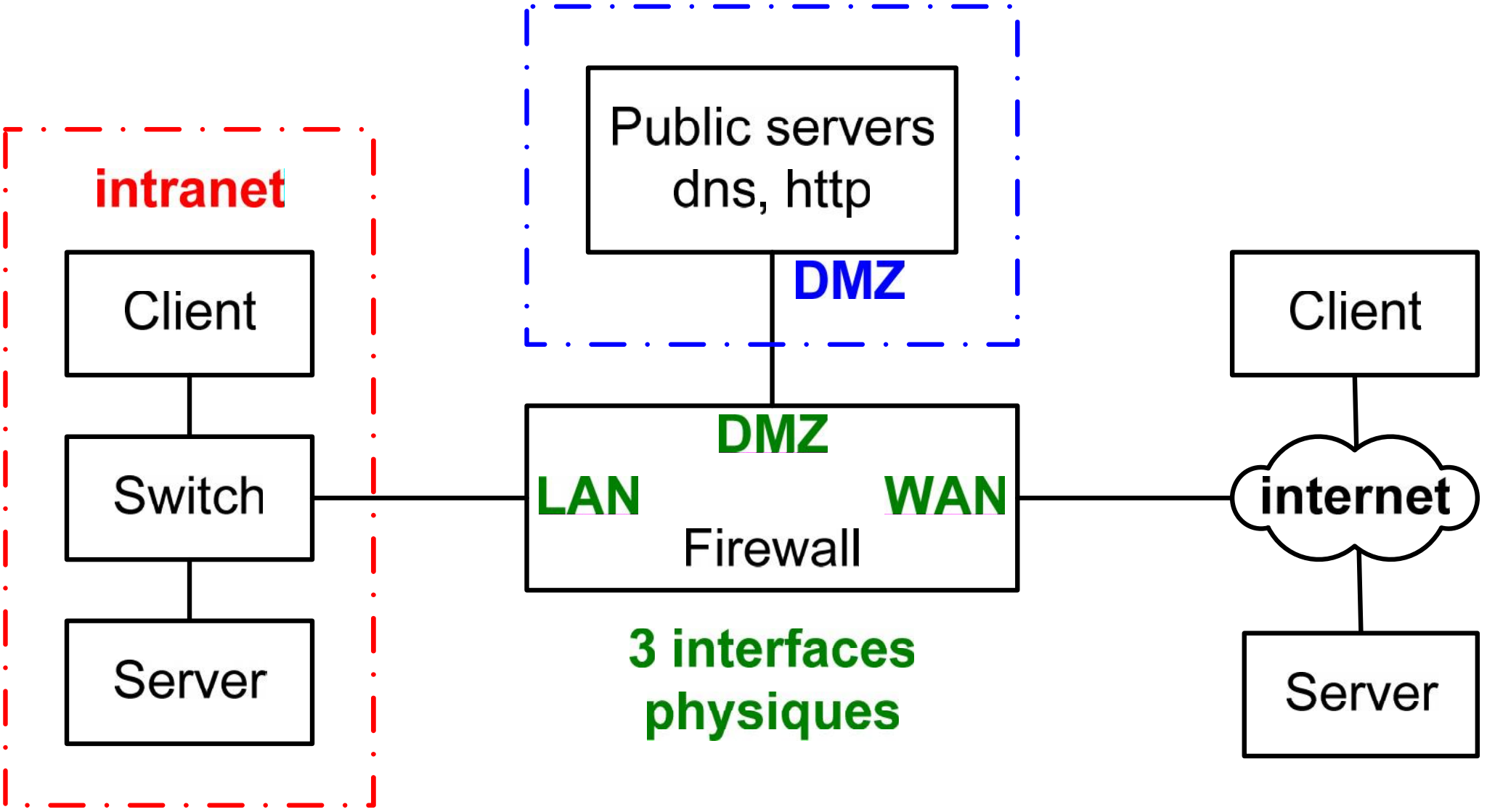
- Imaginons une PME qui dispose de 2 accès à *internet* pour des raisons de sécurité



- Le module NAT peut décider d'utiliser ISP1 ou ISP2 selon différents critères de disponibilité, taux de charge, tarification, temps de réponse, …
- Chaque poste de travail ne voit qu'un seul routeur

Firewall : introduction (1)

- Etude basée sur le produit **pfSense** qui protège le labo.



Firewall : introduction (2)

- *Firewall* (pare-feu) avec **3 interfaces physiques**

- **Intranet** composé de clients et serveurs

  Les clients doivent pouvoir accéder aux serveurs publics

  Les serveurs ne doivent pas être accessibles depuis internet

- Le réseau intermédiaire est appelé DeMilitarized Zone → **DMZ**

  Il accueille les serveurs publics tels que http://www.tdeig.ch et dns qui gère le domaine (la zone) tdeig.ch

- Un client de l'intranet peut accéder à un serveur de la DMZ

  Depuis la DMZ, un éventuel client *(malware)* ne doit pas pouvoir accéder à l'intranet

Firewall : règles (rules)

	Source		Destination			
No	IF	adr_IP	adr_IP	Service	Action	Log
1	LAN	10.2.0.0/16	129.194.0.0/16	dns	NAT	Log
2	LAN	10.2.0.0/16	Any	http	NAT	
3	Any	Any	Any	Any	Drop	

- Chaque nouveau paquet est comparé à la règle 1, 2, …
- Action – Log sont exécutés si le paquet respecte les conditions Source – Destination – Service
- Int = interface physique = LAN ou DMZ ou WAN ou All (Any)

Firewall : Rules based on IP, TCP, … headers

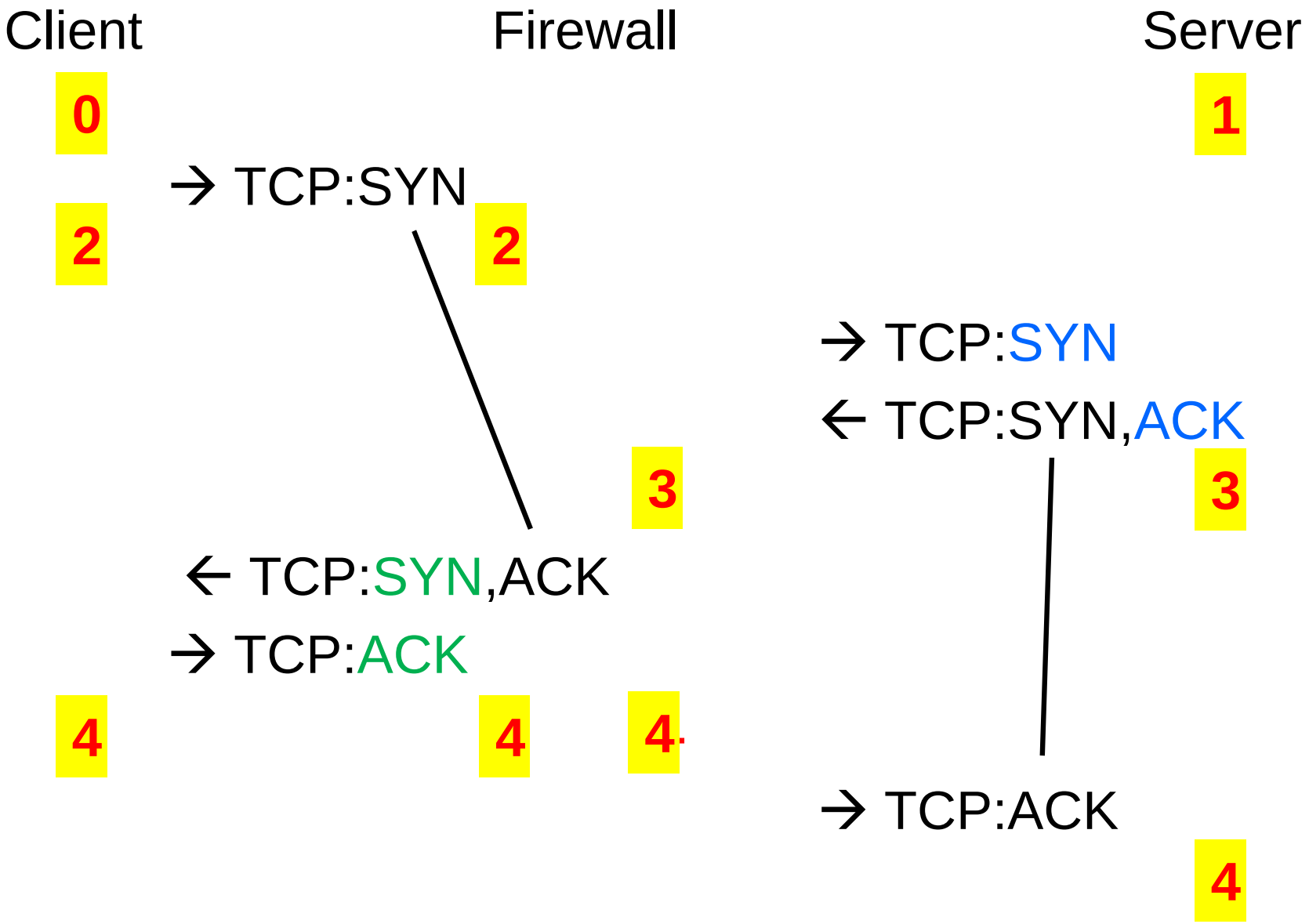
IP header

Version	Header Length	Type of service	Total length
Identification			Fragmentation
Time To Live		Protocol	Header checksum
Source address			
Destination address			

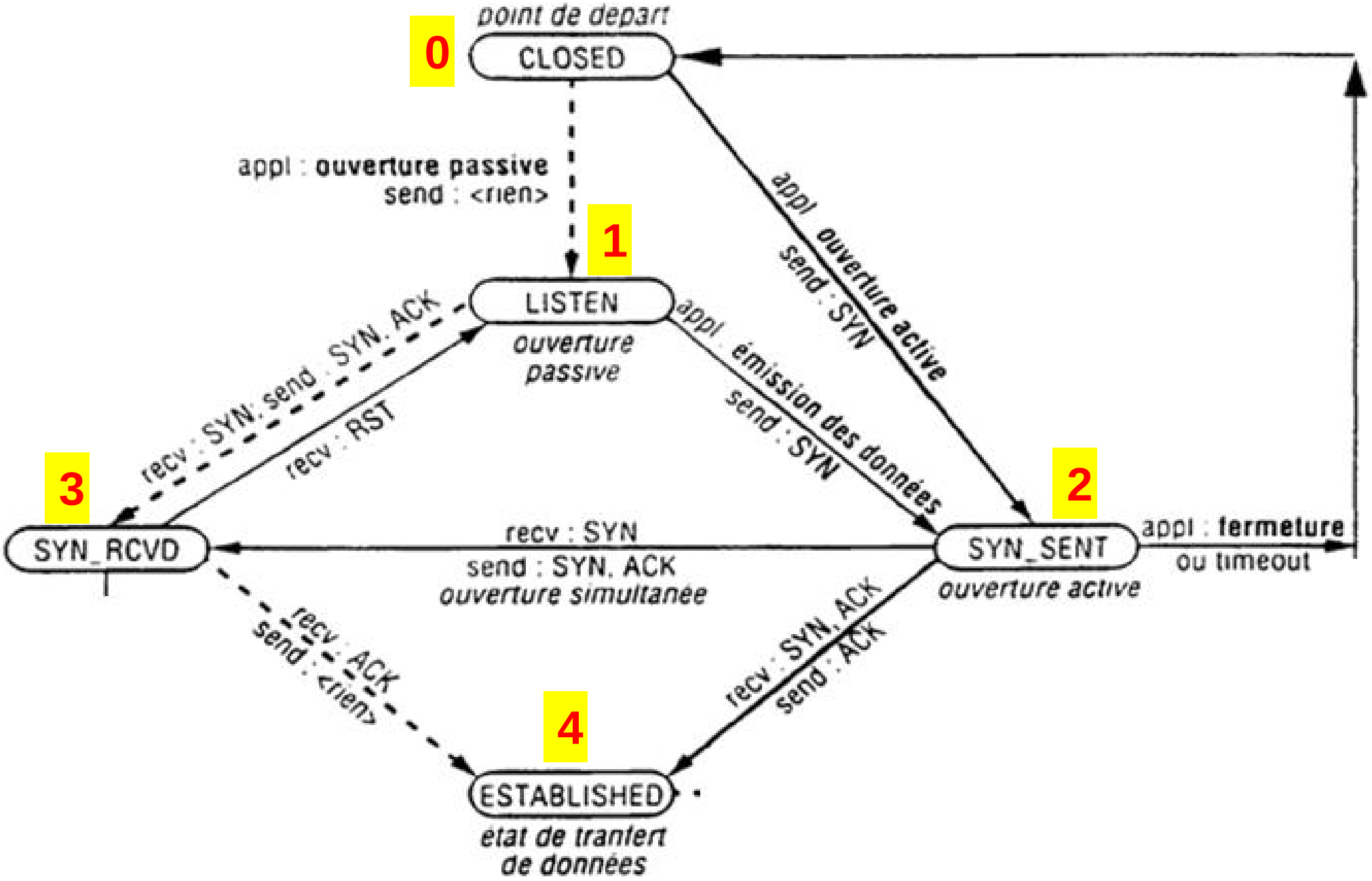
TCP header

Source port			Destination port
Sequence number			
Acknowledgment number			
Length		Flag	Window
Checksum			

Etablissement TCP



TCP : State Diagram



Stateful Firewall

	Source		Destination			
No	IF	adr_IP	adr_IP	Service	Action	Log
2	LAN	10.2.0.0/16	Any	http	NAT	

- Cette règle cache une certaine complexité !

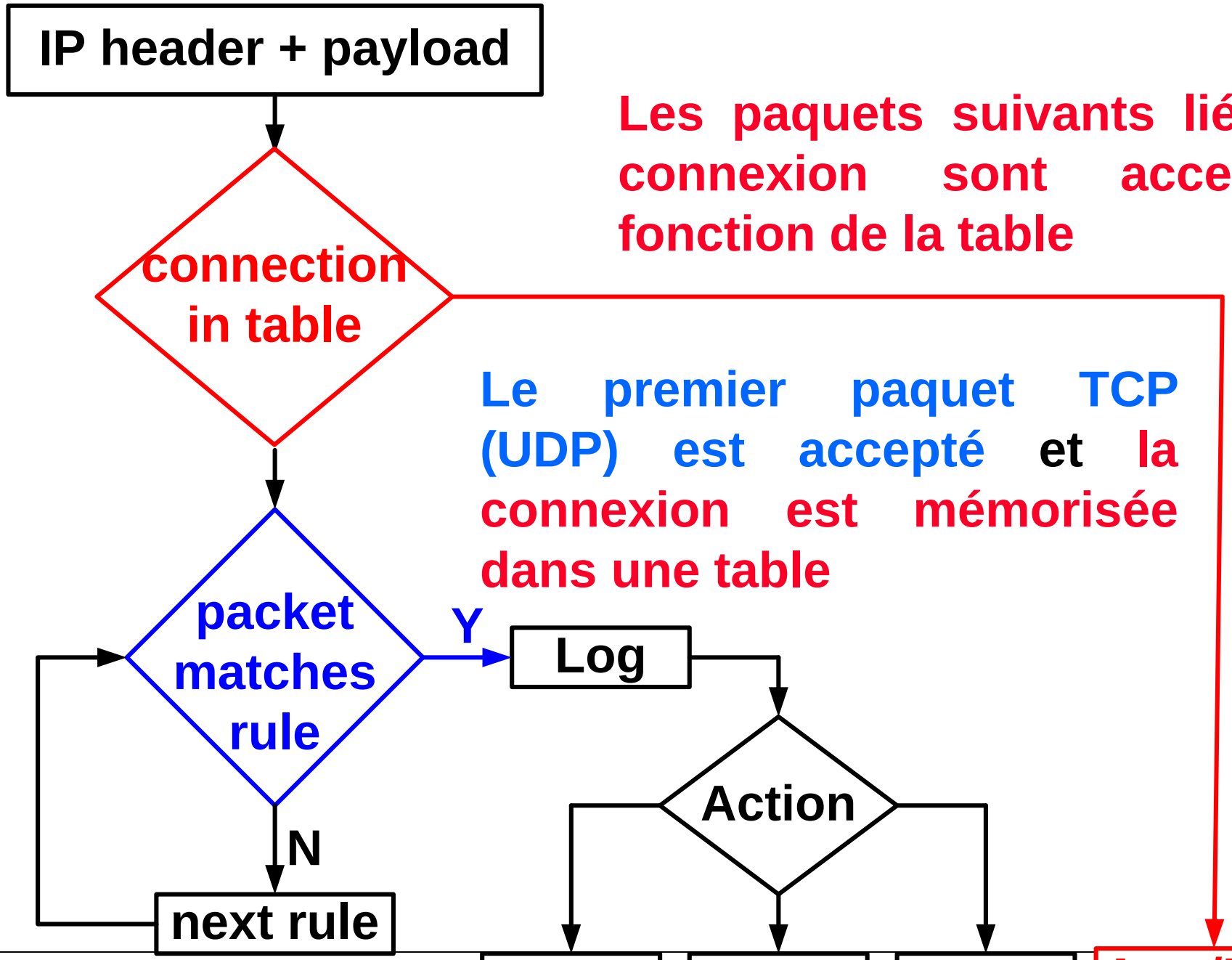
  Par quelle magie, les réponses issues du serveur sont-elles autorisées à traverser le *firewall* ?

- Réponse

  Tous les *firewalls* actuels (y compris les *firewalls* personnels) sont du type ***stateful firewall***

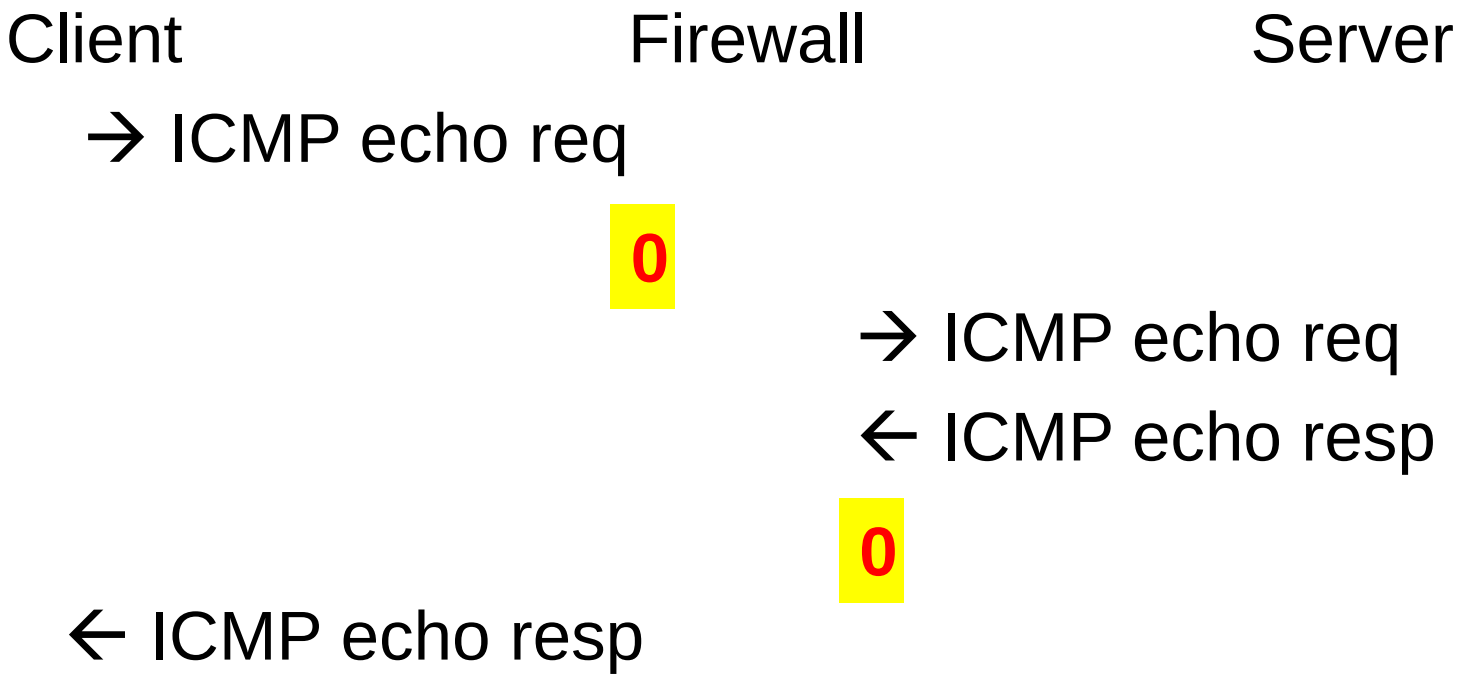
- Voir labo iptables (RPI)

Stateful Firewall : connection in table



Flux ICMP

- Bien que ce protocole soit **sans connexion**, un firewall dit stateful est capable de mémoriser l'échange ICMP dans sa table d'état



- Idem pour flux UDP
- Labo §5 : mesure du timeout ICMP

Firewall pfSense (qui protège le labo)

- Basé sur le système d'exploitation FreeBSD http://www.freebsd.org
- *Features : Router, **DHCP server**, DNS server, **Firewall**, Wireless Access Point, VPN, Proxy, Reverse Proxy*
- Matériel : PC bas de gamme et ancien
- Installation : LiveCD (USB) / Full Install / Embedded
- Administration via **interface web** / SSH / console physique
  → http://www.pfsense.org/screenshots/ démo
- Sauvegarde du seul fichier de configuration **/cf/conf/config.xml**
- Produit dont la robustesse est éprouvée
  → http://secunia.com/community/advisories/search/
- Travail de Bachelor 2012 de Michaël Golliet

Service DHCP (Dynamic Host Configuration Protocol)

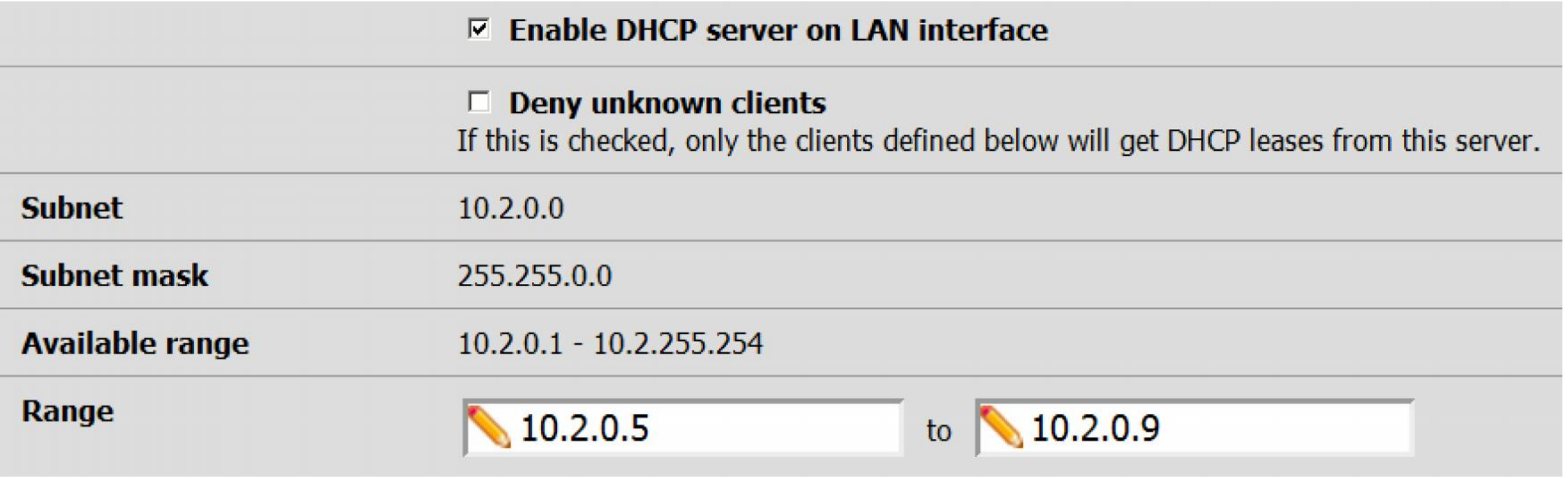
- Rfc 1531 (1993), rfc 2131 (1997), …
- Nombreuses extensions : BOOTP Vendor Extensions, PXE, …

- Diag. en flèches

		Client en mode DHCP (défaut)
→	DHCP Discover	Recherche d'un serveur
←	DHCP Offer	Un serveur est présent
→	DHCP Request	Demande des paramètres
←	DHCP Ack	IP_Addr, mask, IP_router, IP_DNS
	…	lease time
→	DHCP Request	
←	DHCP Ack	

DHCP : liste des clients autorisés

- Je ne souhaite pas configurer manuellement chaque PC du labo
- Je veux une adresse IP fixe en fonction de l'adresse Ethernet
- pfSense : Services – DHCP Server



- Démo → Status – DHCP leased (labo §7)

Labo Firewall pfSense : Config. par défaut & DHCP (90')

§2 Démarrer pfSense (chargement via le réseau)

§3 Modifier le câblage : PC-Win – PC-Firewall – Intranet LaboTD

§4 Administration distante (WebGUI)
Interfaces, DHCP Server, Routage, DNS, Services actifs
Règles par défaut, Logs par défaut, Config logs

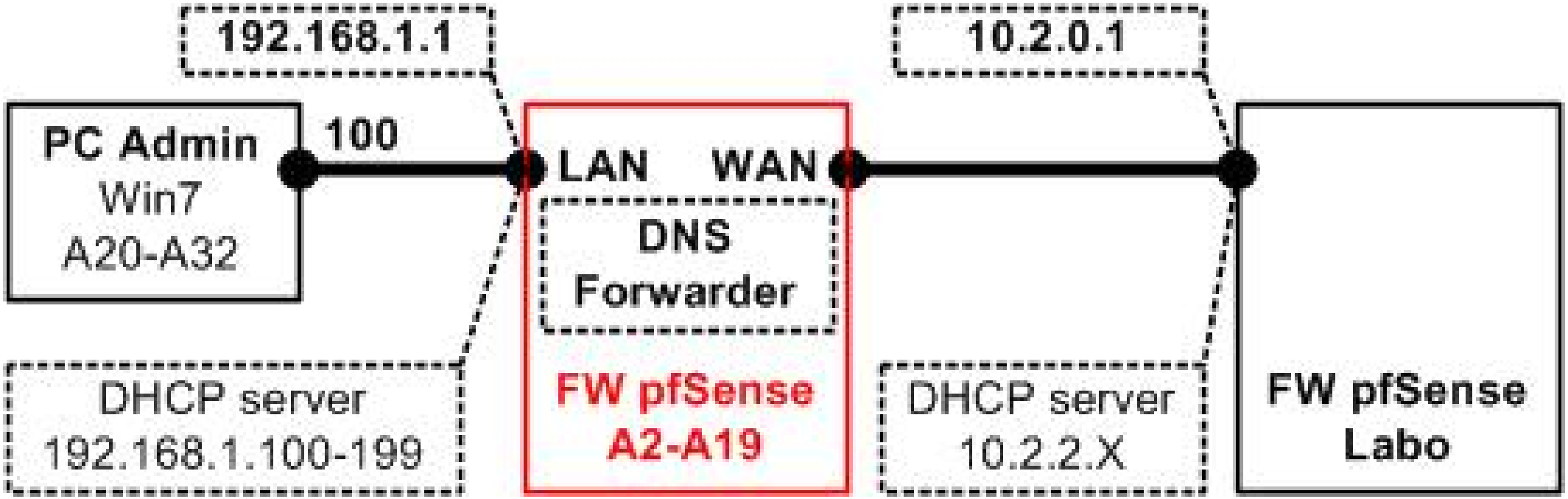
§5 Afficher la table d'état

§6 Configuration réseau de VirtualBox (Vbox) = Bridge

§7 Fonctions évoluées du serveur DHCP
IP fixe en fonction de l'adresse Ethernet
Liste blanche (qui exclut toute adresse Eth inconnue)
Test avec Vbox

Synthèse du labo Firewall pfSense

- Schéma : adr IP, DHCP, router, DNS

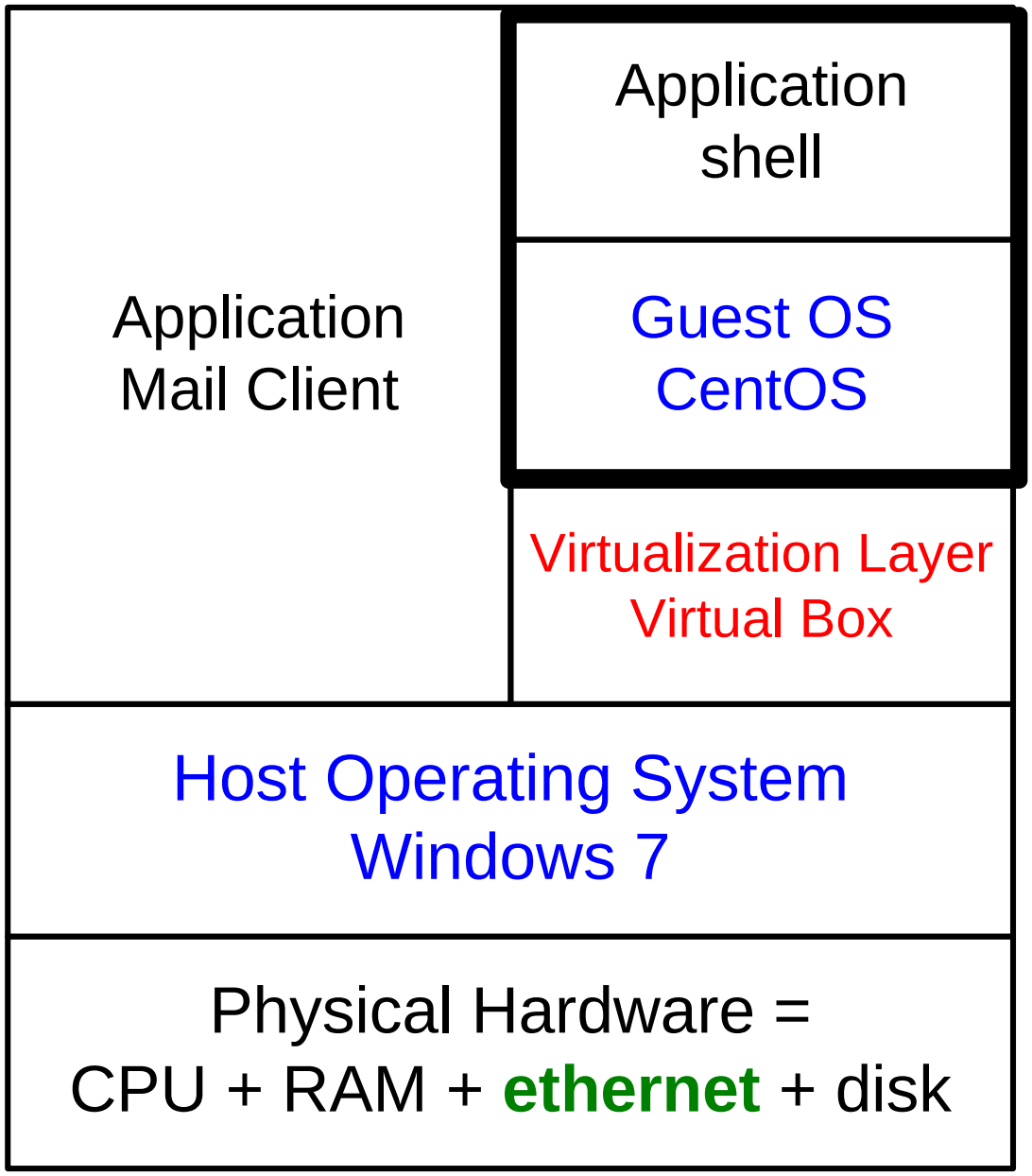


- Règles par défaut

  Administration depuis client web

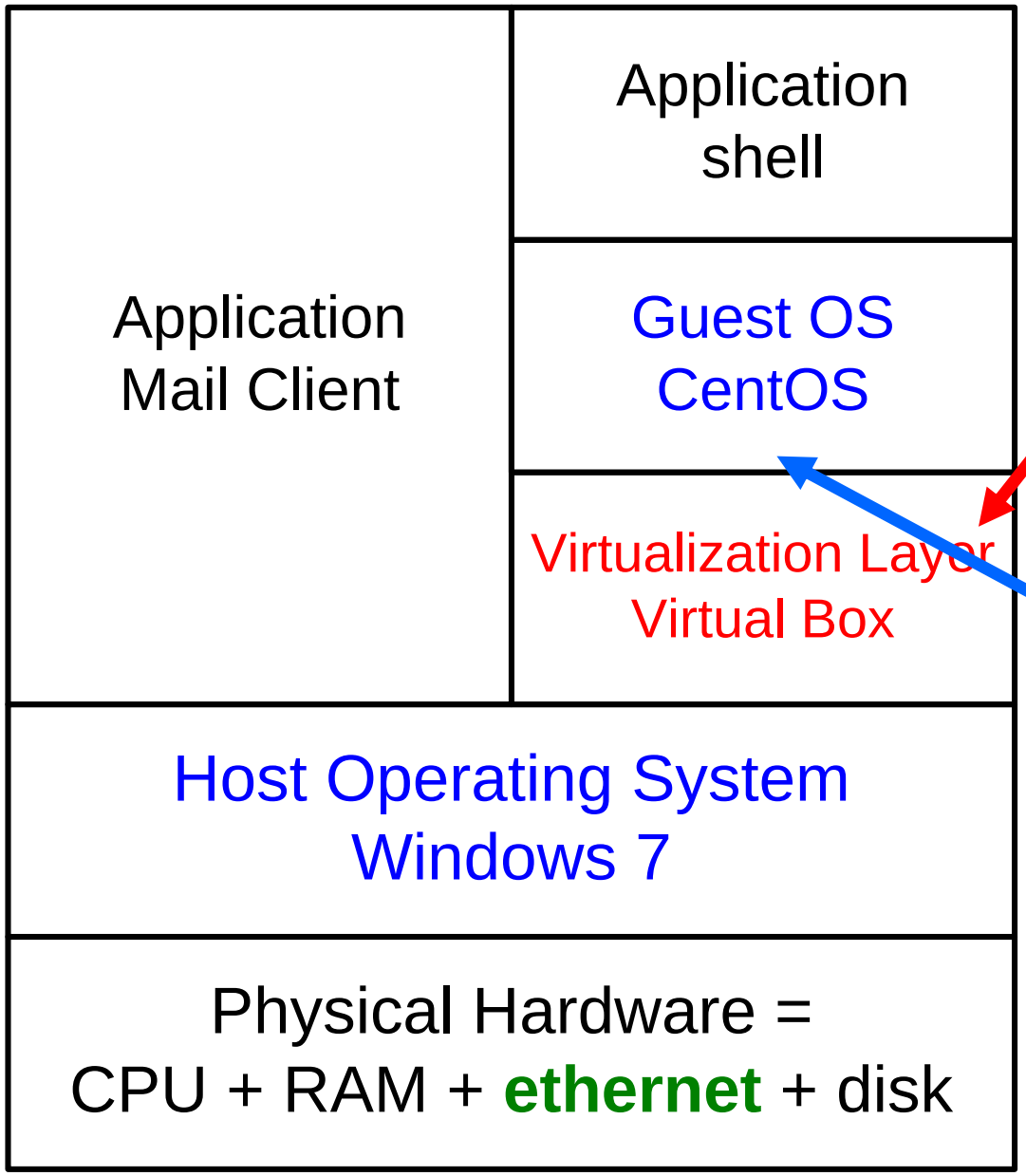
  Clients LAN peuvent accéder à internet (WAN); NAT activé

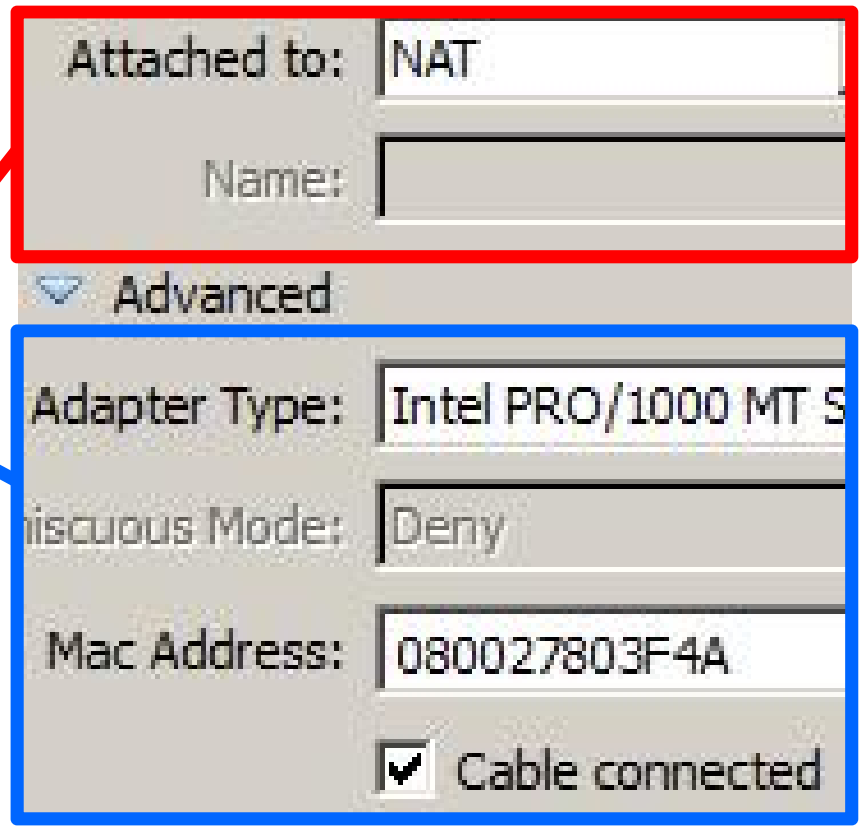
VirtualBox : Architecture



- Excellent support du matériel grâce à Host OS
- Choix des Guest OS grâce à VirtualBox (Vbox)
- VM (machine virtuelle) contient Guest OS + applications
- On parle d'une architecture de Type 2 (sans hyperviseur)

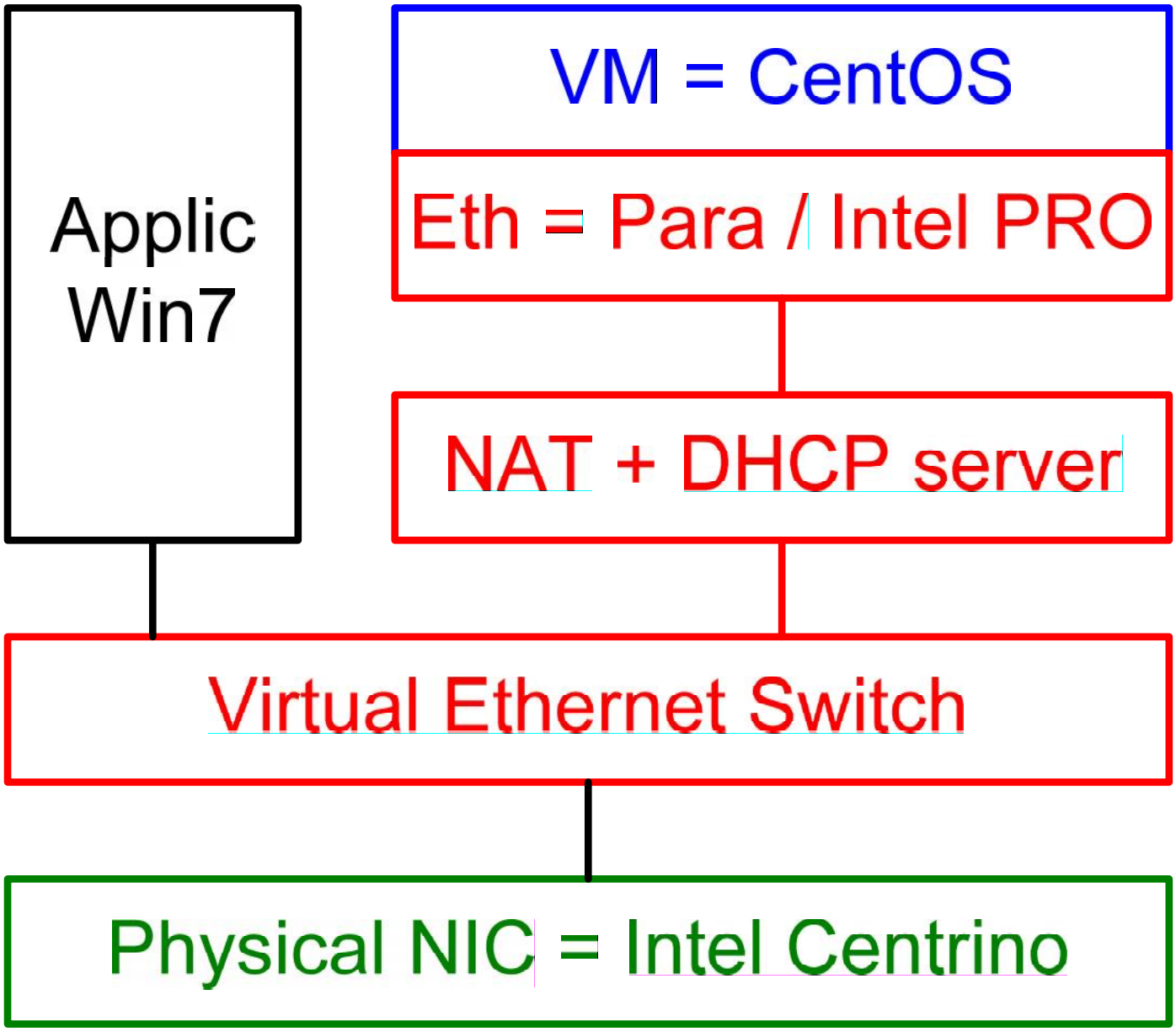
NAT networking (default mode)





Réseau émulé par Vbox

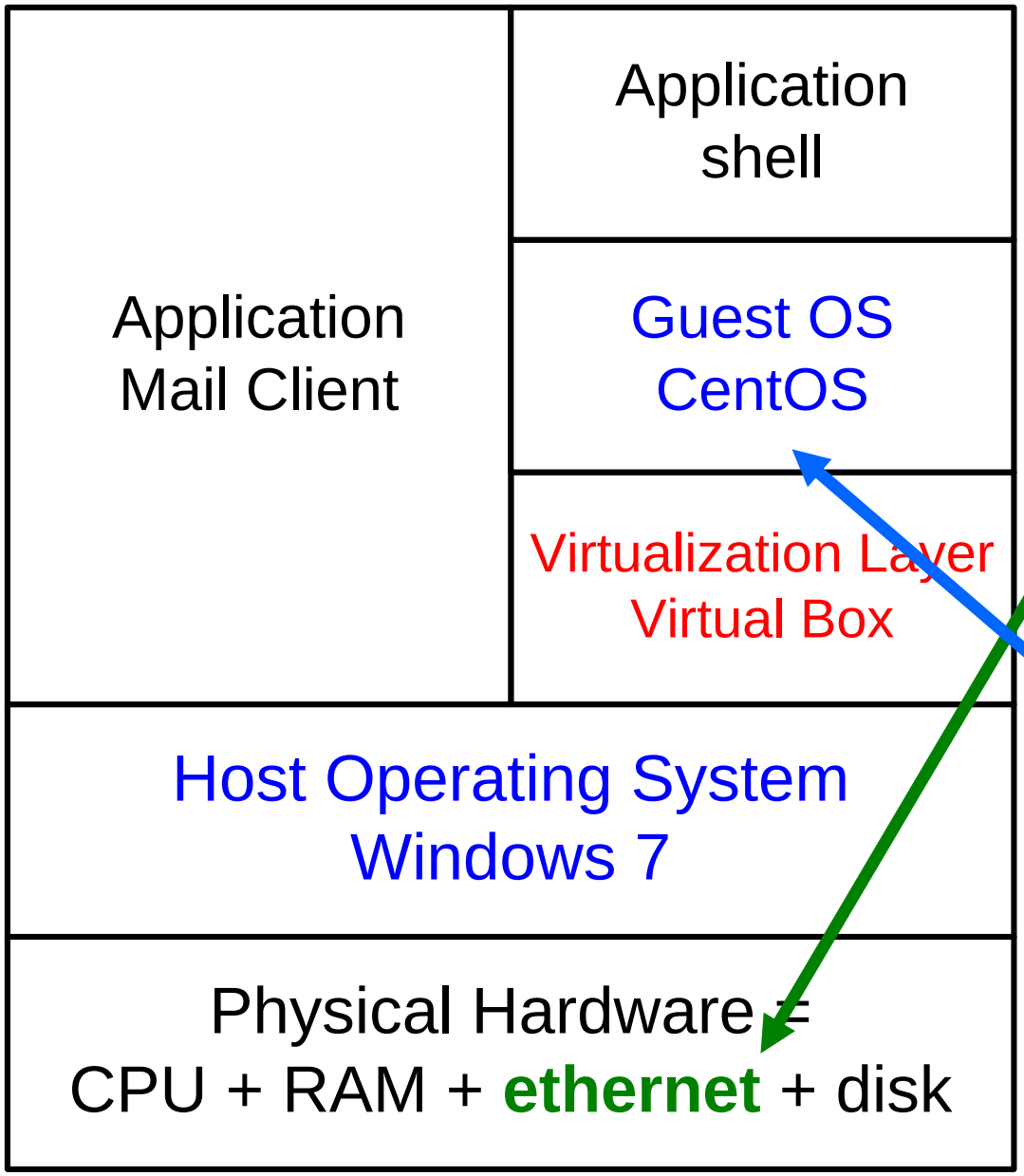
Réseau émulé par Vbox

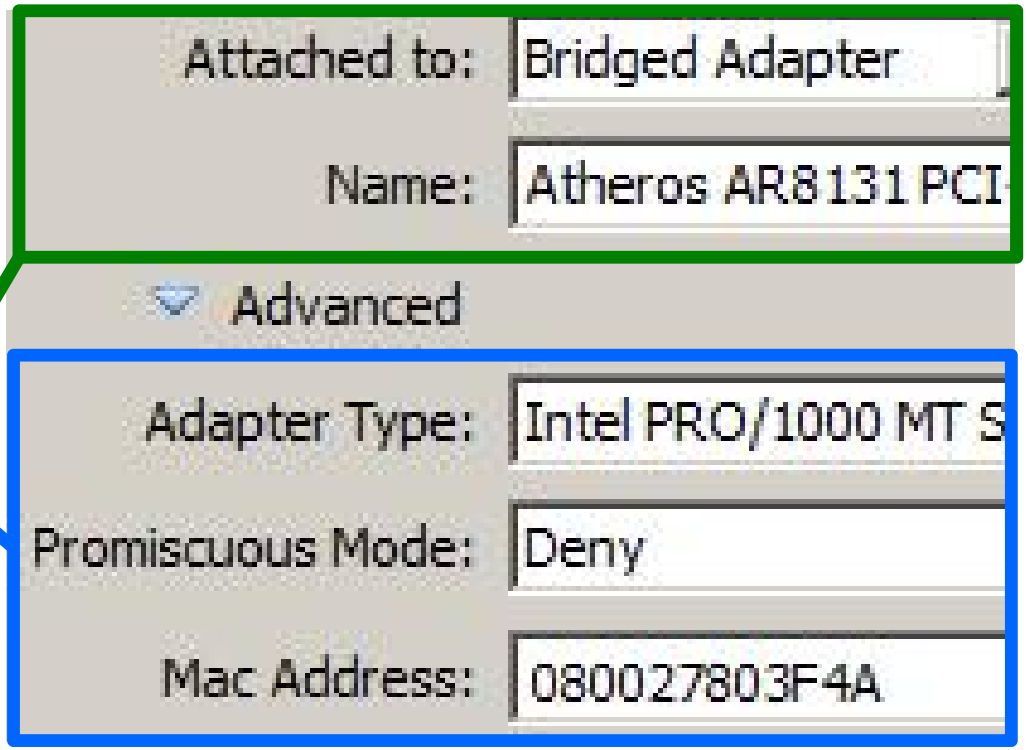


Réseau émulé par Vbox

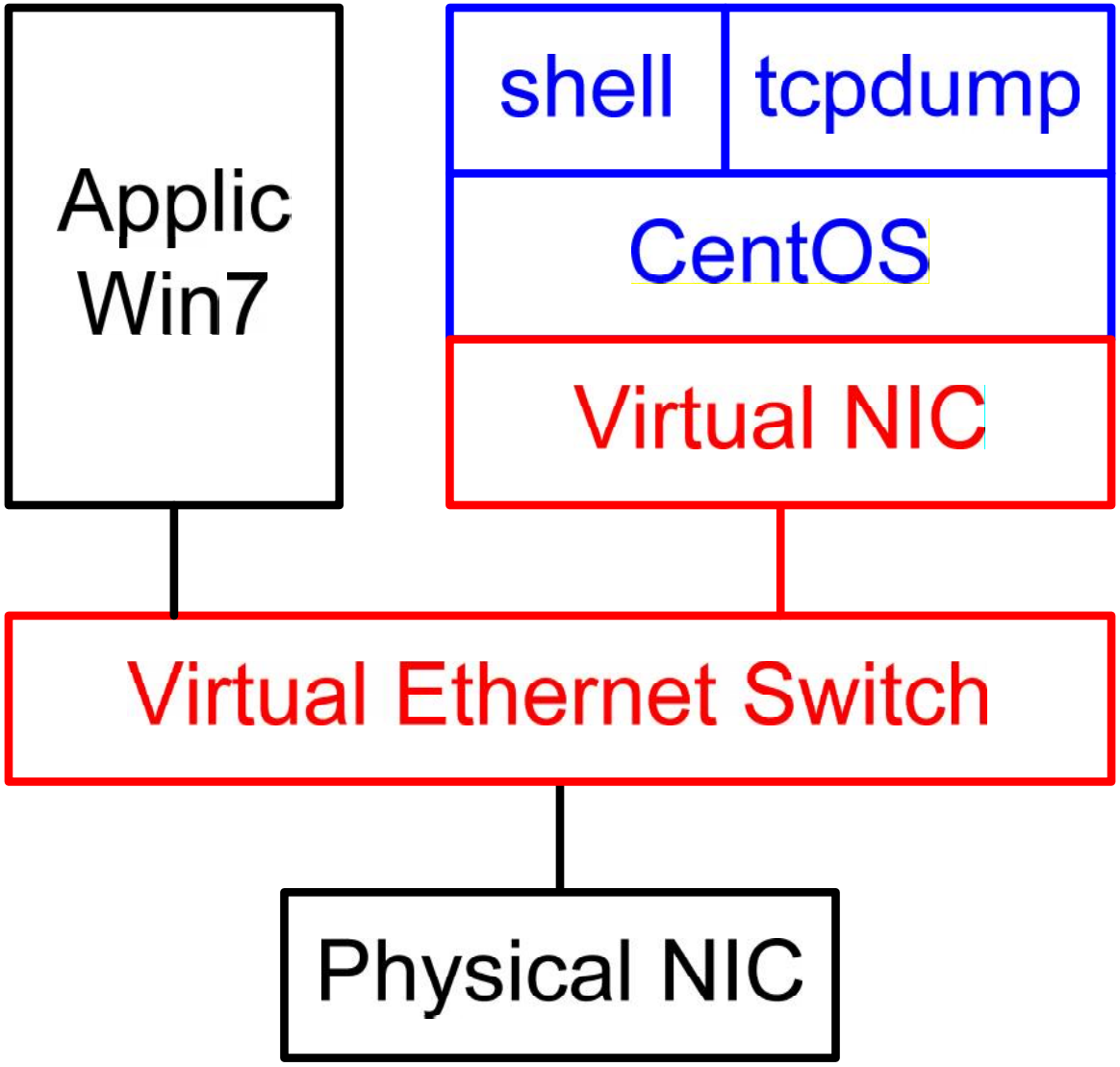
Physical Network Interface Card

Bridged networking





Bridged networking



- Utilisons l'outil tcpdump (Wireshark) pour comprendre le rôle de WinPcap utilisé dans l'architecture Vbox

Travail personnel difficile : Problématique DNS → 106

4 A quoi sert le serveur DNS Debian 5.0 (voir schéma) ?

5 Comment est-il connu de Root ?

6 Quelle valeur(s) de serveur DNS faut-il donner au client de l'intranet ? **Tenir compte du mécanisme de Failover**

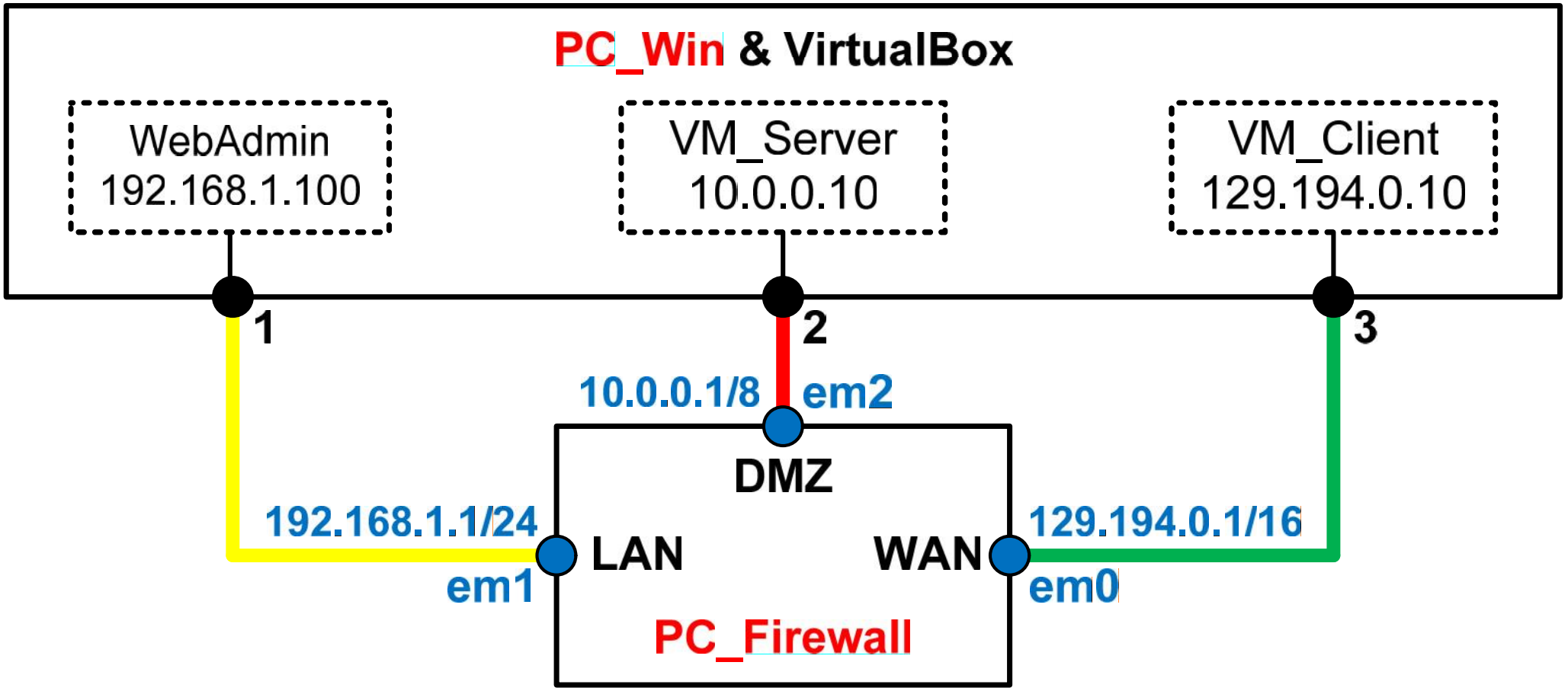
7 Un serveur DNS est-il utile dans l'intranet ?

Si oui pour quelles fonctions ?

Si non expliquer le fonctionnement

Labo DMZ

- Configurer et tester une DMZ avec 2 PCs selon le schéma suivant



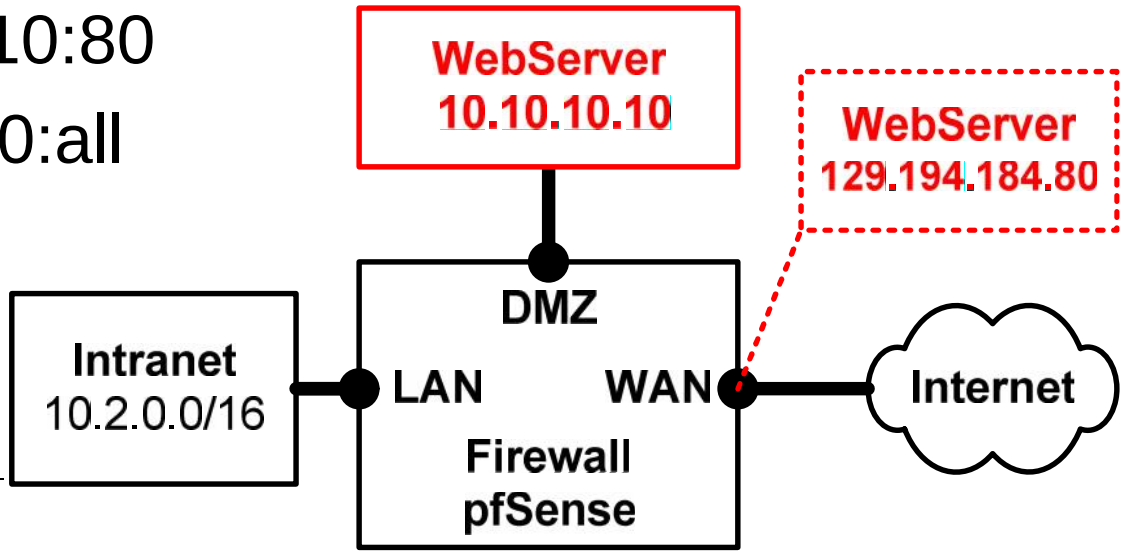
- **Aucune connexion à l'intranet du labo** (3 câbles à disposition)
- Test final depuis VM_Client : ping 129.194.0.2

Plan d'adressage et translation d'adresse du FW labo

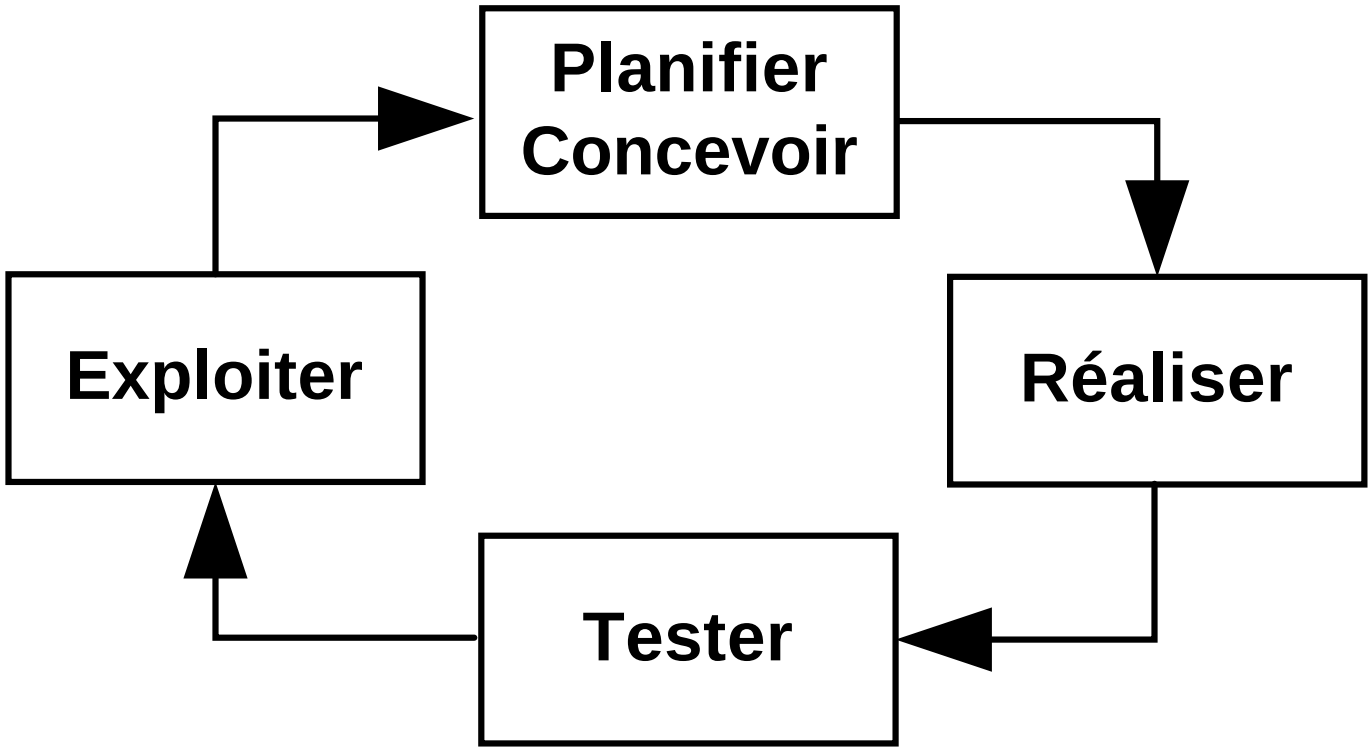
- Le firewall sépare (route) 3 réseaux → **Schéma**
  Intranet = 10.2.0.0/16 DMZ = 10.10.10.0/24 Internet = public IP

- Intranet – DMZ (sans NAT), Intranet – Internet (avec dyn NAT)

- Internet – DMZ (avec NAT statique) → **Labo DMZ**
  Ajouter interface DMZ
  Activer ProxyARP pour 129.194.184.80
  Redirection (NAT) de 129.194.184.80:80 to to 10.10.10.10:80
  Rule1 : WAN pass to 10.10.10.10:80
  Rule2 : LAN pass to 10.10.10.10:all



Labo DMZ & Roue de Deming



- Planifier – Concevoir → Analyse
- Réaliser – Tester

Labo DMZ : Principales difficultées

- Identifier les ports physiques

  Où se trouvent les ports Ethernet de Windows ?

  Les identifiants affichés par VirtualBox et ipconfig sont différents !

  Où se trouvent em0, em1 et em2 ?

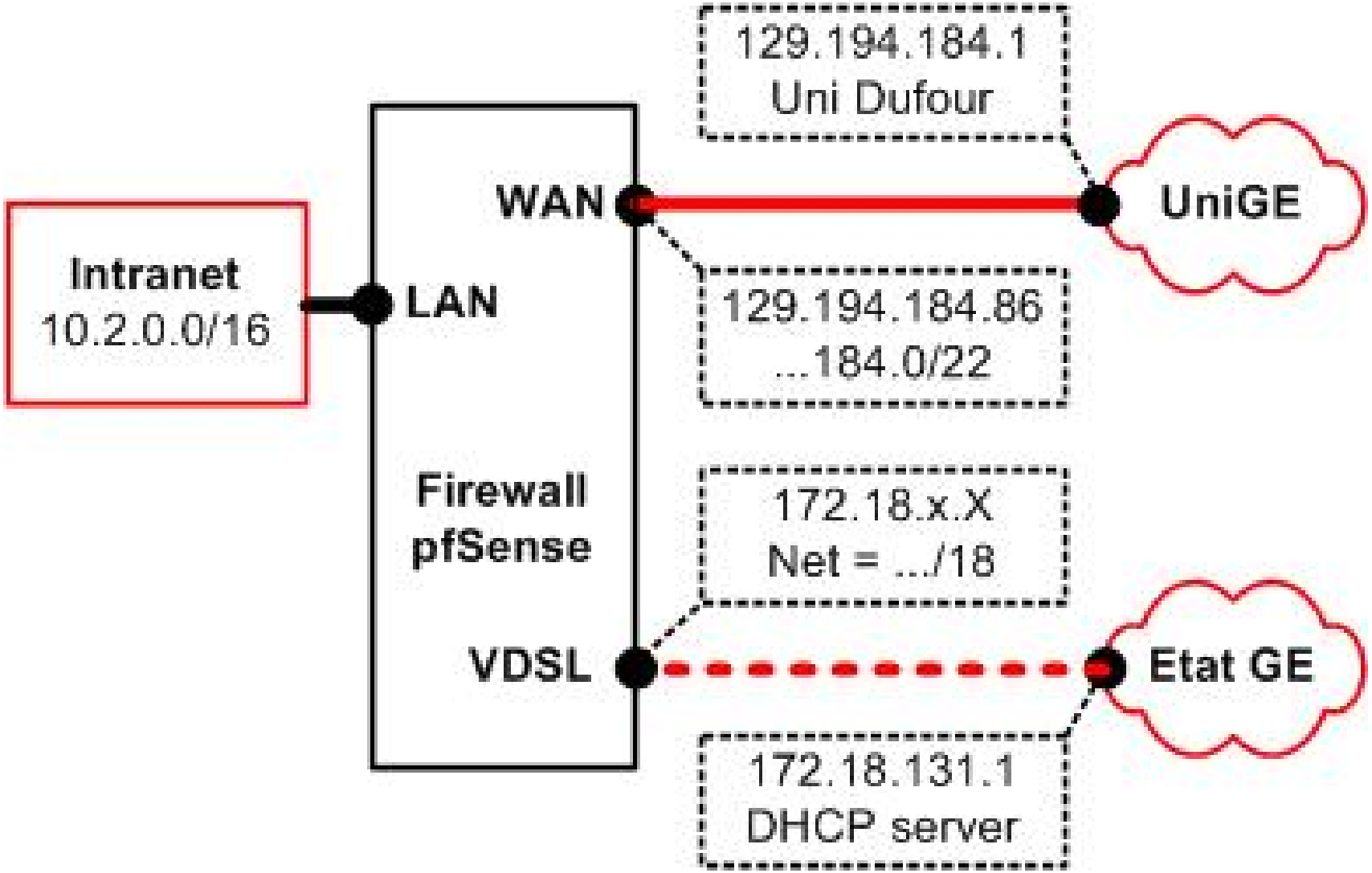
- VM_Cient + VM_Server à disposition

- Compréhension des affichages pfSense

- Utiliser le corrigé après 45 min

Failover : Principe de fonctionnement

- **Un seul lien actif : vers UniGE ou vers EtatGE**



Failover : Problématique

- Offrir une connexion redondante
  Accès à internet via 2 chemins possibles

- Comment détecter la coupure du lien principal ?

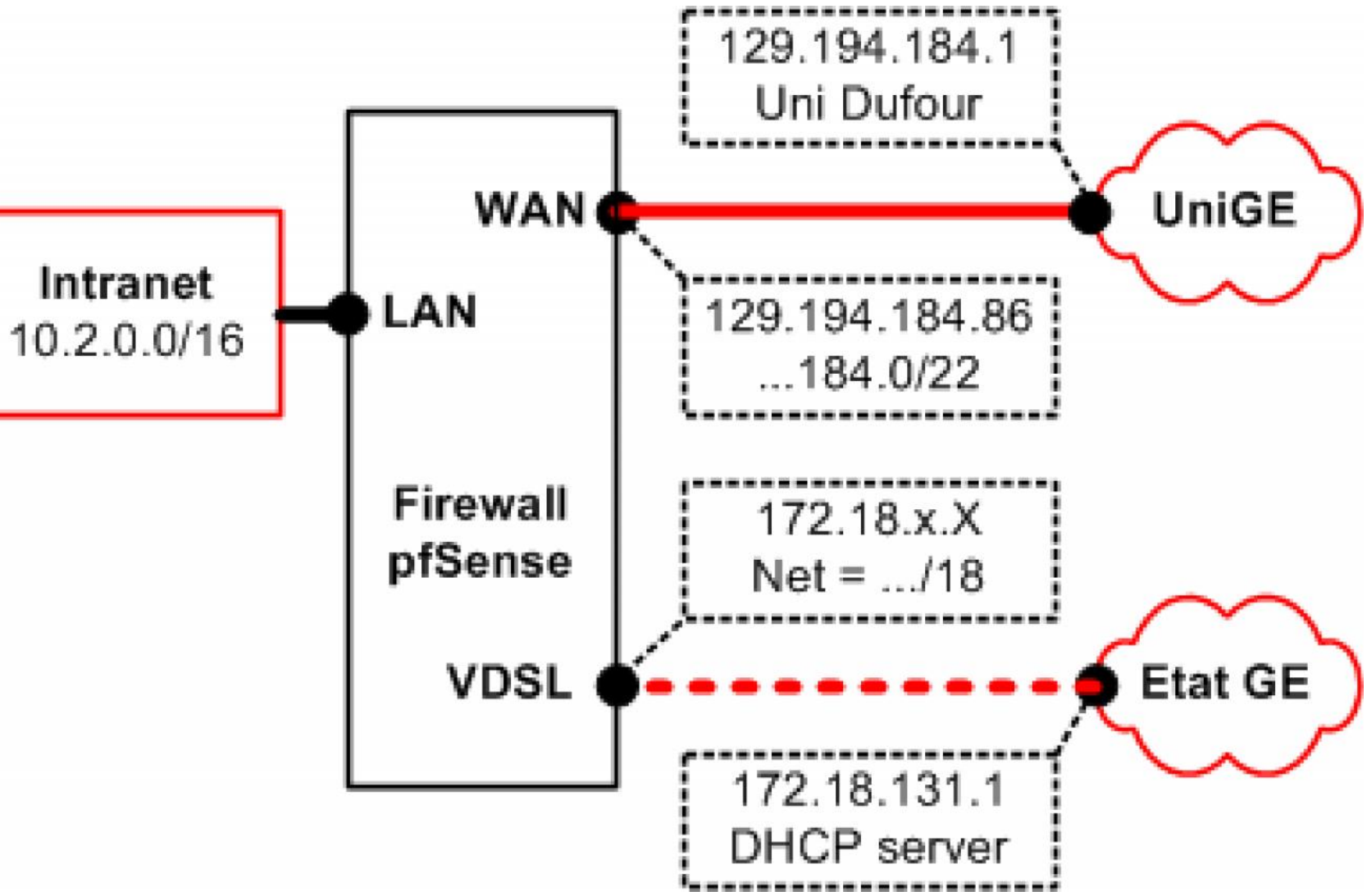
- Comment écrire une règle autorisant un accès à internet ?

- Comment connaître les basculements des 6 derniers mois ?

- Qui (intranet - internet) peut bénéficier de cette redondance ?

Failover avec pfSense (1/3)

- **Un seul lien actif : vers UniGE ou vers EtatGE**



Ajouter int VDSL mode DHCP

Créer le GatewayGroup Failover

Autoriser le failover (System)

Redirect

Failover avec pfSense (2/3)

- La surveillance (IPMonitor) avec paquets ICMP (ve 21 sept – 15h)

Name	Gateway	Monitor	RTT	Loss	Status	Description
HEPIA	129.194.184.1	129.194.184.1	0.777ms	100.0%	Offline	UniGE Router
GW_OPT1	172.18.131.1	172.18.131.1	0.532ms	0.0%	Online	VDSL Router

- **`# ping -t 5 -oqc 5 -i 0.7 <ip address>`**

  `-t 5 Wait 5 seconds`

  `-o Exit successfully after 1 reply packet received`

  `-q Quiet (summary) output`

  `-c 5 Send 5 packets`

  `-i 0.7 Wait 0.7 seconds between each packet sended`

- **Indisponibilité de 5-6 secondes**

  Est-il possible de modifier ces valeurs ? → projet de semestre

Failover avec pfSense (3/3)

- Firewall utilise le lien (privilégié) vers UniGE
- Depuis intranet : **`ping -t www.cern.ch`**

```
Réponse de 137.138.144.168 : octets=32 temps=1 ms TTL=118
```

- Imaginons une **coupure de 8 secondes**

```
Réponse de 137.138.144.168 : octets=32 temps=1 ms TTL=118
Délai d'attente de la demande dépassé.       6 rép ident
Réponse de 137.138.144.168 : octets=32 temps=32 ms TTL=112
```

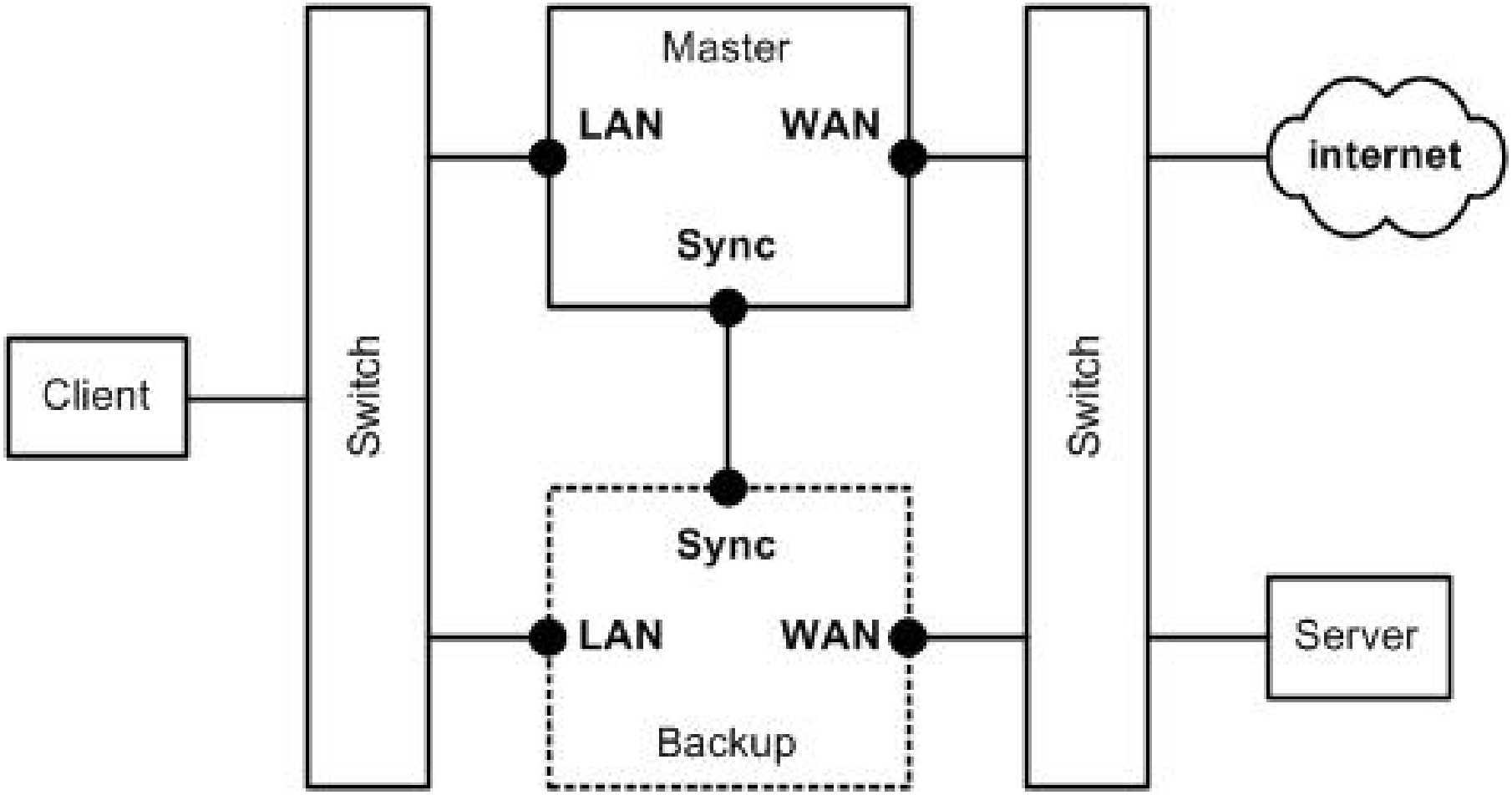
- **Je reconnecte le câble mais les paquets ICMP continuent d'utiliser le lien de secours !!!**

```
Réponse de 137.138.144.168 : octets=32 temps=32 ms TTL=112
```

- Attendre 10 s (timeout ICMP) pour effacer l'élément dans la state table

```
Réponse de 137.138.144.168 : octets=32 temps=1 ms TTL=118
```

Dual Firewall (Master & Backup)



- Un seul firewall actif à la fois
- Solution transparente pour client – internet – serveur
- Mémoire Golliet → http://www.tdeig.ch/linux/Golliet_RTB.pdf

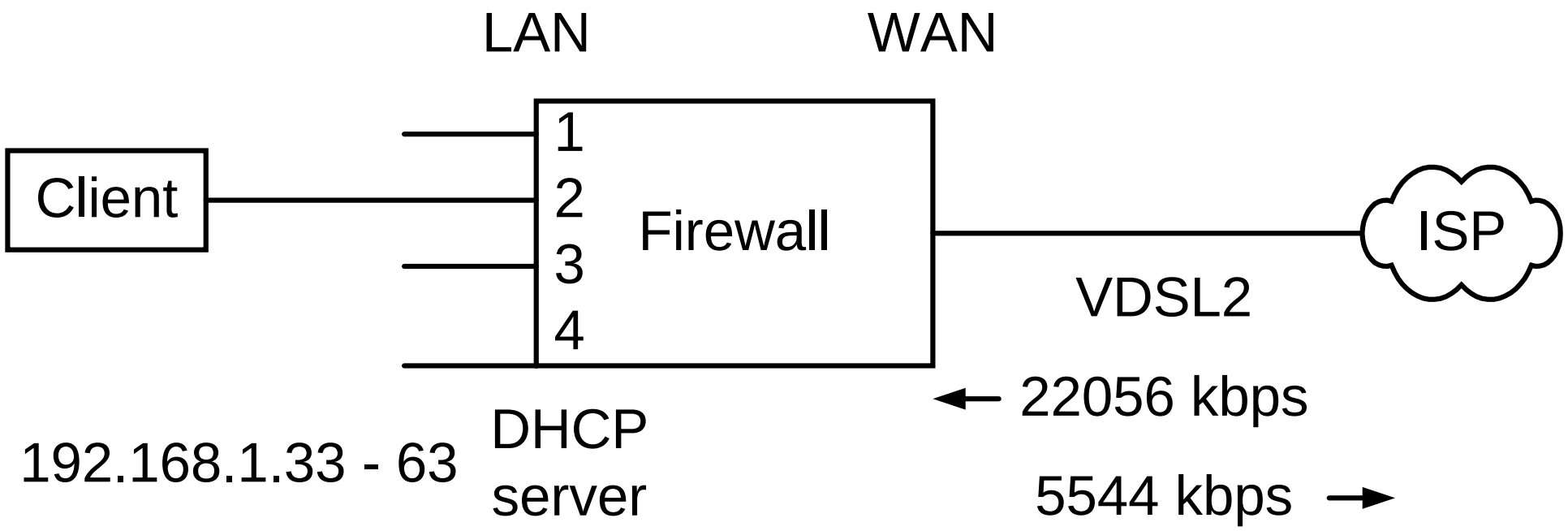
Dual Firewall : Fonctionnement

- **pfSync**
- Protocole garantissant la réplication des données (config, tables, …)
- Interfaces dédiées

- **CARP (Common Address Redundant Protocol)**
- Groupes de redondance côté LAN et WAN
- Chaque groupe possède une adresse IP virtuelle
- Client & Server utilisent l'adresse IP virtuelle
- Le FW master envoie chaque seconde un paquet d'annonce
- Le FW backup devient master après 3 secondes s'il n'a rien reçu

- Alternative aux protocoles VRRP & HSRP protégés par Cisco
- Voir Mémoire Golliet §3.5 et §4.1
- Suite dans cours Réseaux Avancés

Mon modem-routeur ADSL Bluewin TV (Netopia 3397)



accept outgoing connection (NAT)

refuse all incoming connection

Haute disponibilité

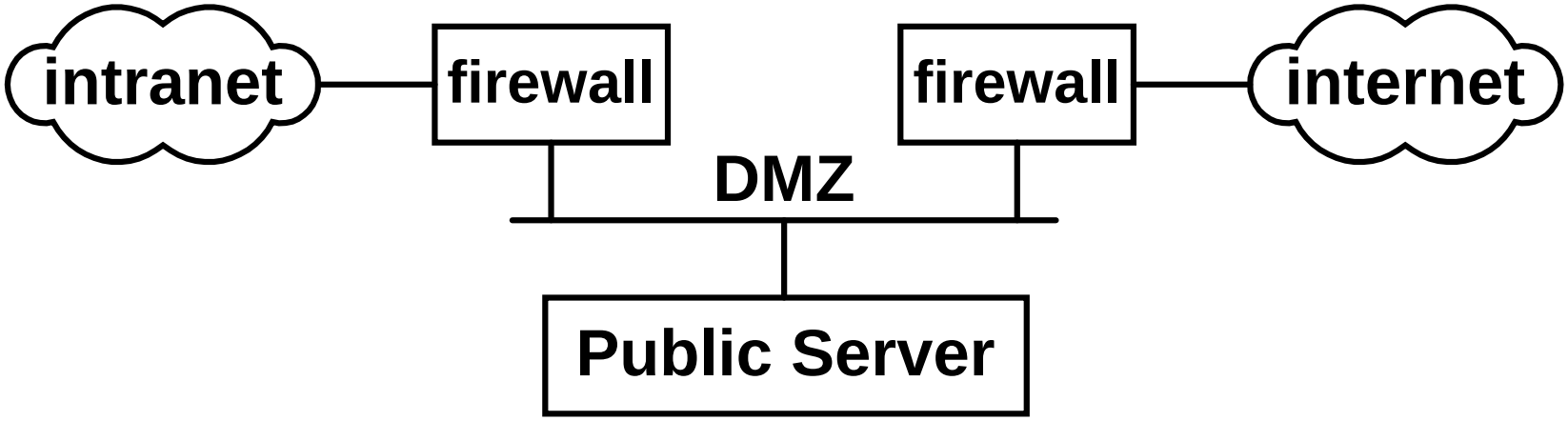
- Disponibilité Temps d'arrêt annuel
  99,9% 8,75 heures
  99,99% 52 minutes
  99,999% 5 min

- Mode de fonctionnement
  Load balancing → répartition de charge :
  N x Domain Controlers, N x serveurs DNS, N x serveurs Web
  Hot swapping → commutation suite à incident :
  backup ligne louée via RNIS, *firewalls*, …

- Suite dans cours Réseaux Avancés

DMZ (DeMilitarized Zone)

- Défense en profondeur avec 2 *firewalls* :

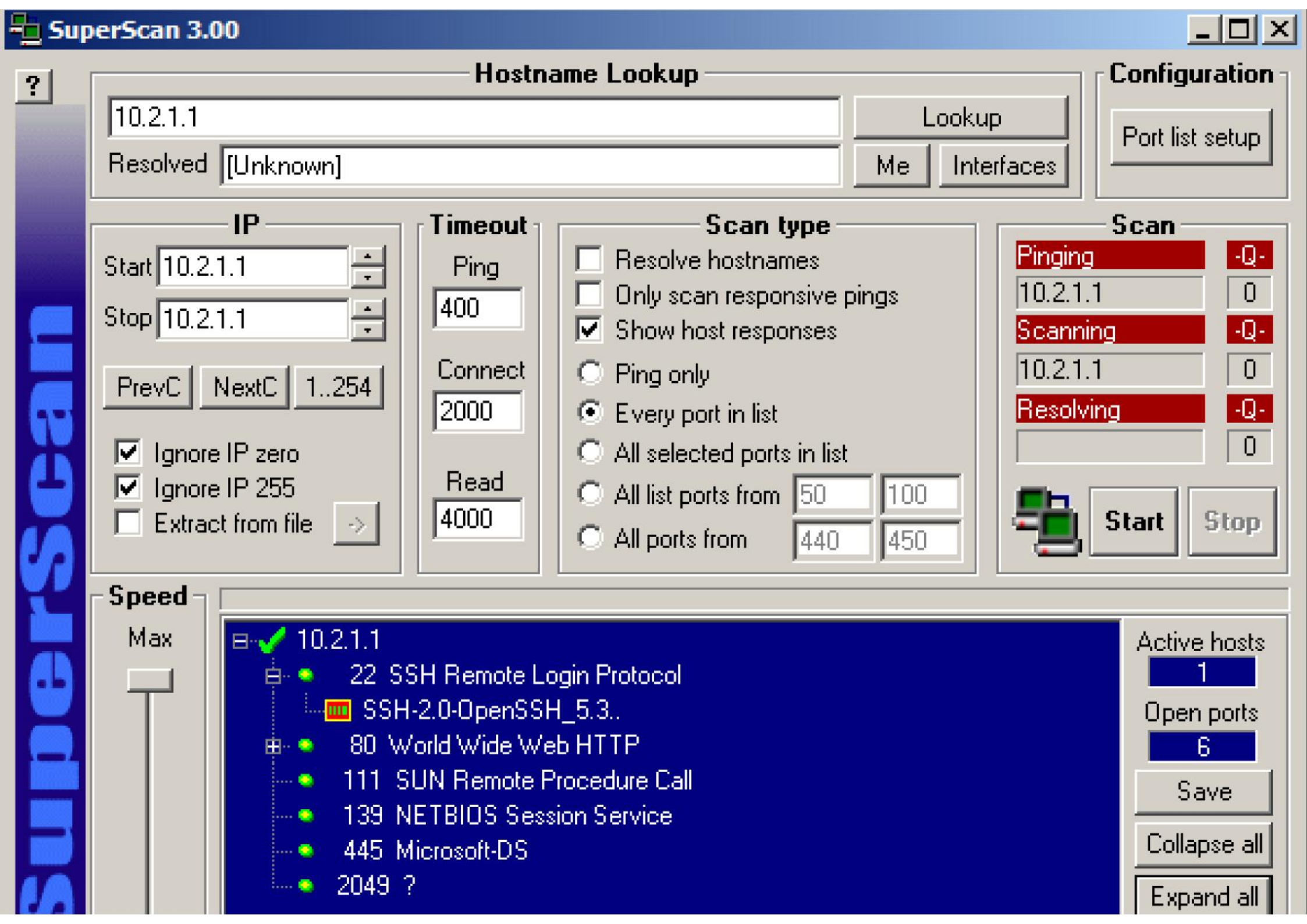


- Des entreprises peuvent comporter plusieurs DMZs :

  DMZ pour l'accès à distance *(remote access)*, DMZ pour VPN *(Virtual Private Network)*

Network scanners

- Outils qui testent si un port (TCP-UDP) est ouvert
- Capables de scruter une plage d'adresses IP et / ou une plage de ports
- Capables d'identifier à distance le système d'exploitation utilisé
- A utiliser pour tester (auditer) la configuration du *firewall*
- A utiliser lors d'un test de pénétration pour identifier les services disponibles et les équipements *(firewalls)* intermédiaires
- Automatisation facile *(scripts)* → très présents sur internet


SuperScan 3.00
?
Hostname Lookup
10.2.1.1
Lookup
Resolved
[Unknown]
Me
Interfaces
Configuration
Port list setup
IP
Start
10.2.1.1
Stop
10.2.1.1
PrevC
NextC
1..254
Ignore IP zero
Ignore IP 255
Extract from file
->
Timeout
Ping
400
Connect
2000
Read
4000
Scan type
Resolve hostnames
Only scan responsive pings
Show host responses
Ping only
Every port in list
All selected ports in list
All list ports from
50
100
All ports from
440
450
Scan
Pinging
-Q-
10.2.1.1
0
Scanning
-Q-
10.2.1.1
0
Resolving
-Q-
0
Start
Stop
Speed
Max
10.2.1.1
22 SSH Remote Login Protocol
SSH-2.0-OpenSSH_5.3..
80 World Wide Web HTTP
111 SUN Remote Procedure Call
139 NETBIOS Session Service
445 Microsoft-DS
2049 ?
Active hosts
1
Open ports
6
Save
Collapse all
Expand all
SuperScan

Nmap : Ping scan

`nmap 10.2.1.1`

→ ICMP echo request

→ TCP ACK port 80

← ICMP echo reply

← TCP RST port 80

→ DNS req inverse (10.2.1.1)

← DNS resp (FQDN)

`Host is up`

`nmap www.tdeig.ch`

→ ICMP echo request

→ TCP ACK port 80

`Host seems down`

- Il est donc important de bien comprendre le fonctionnement d'un outil comme nmap
- Utilisé au labo iptables (RPI)

Nmap : don’t ping

```
nmap –Pn –p80-81 www.tdeig.ch
```

don’t ping

port

→ TCP SYN port 80

→ TCP SYN port 81

← TCP SYN-ACK port 80

```
Host is up
PORT   STATE    SERVICE
80/tcp open     http
81/tcp closed   hosts2-ns
```

Nmap : <port> <addr>

```
nmap –p80-81 www.tdeig.ch
     2276 ports utilisés par défaut nmap-services

     –p 20-25, 80, 443

          192.168.1.0/24      256 ip addresses
          192.168.1.4–26           interval
          192.168.1.6,13,24–26
          www.unige.ch          FQDN
```

Nmap : TCP connect

```
nmap -sT -p80-81 www.tdeig.ch
```

→ TCP SYN port 80
← TCP ACK, SYN port ouvert
→ TCP ACK
→ TCP RST

→ TCP SYN port 81
← TCP ACK, RST or no packet port fermé

- **Résultats en 1,5 secondes**

Nmap : TCP SYN stealth

```
nmap -sS -p80-81 www.tdeig.ch
```

→ TCP SYN port 80
← TCP ACK, SYN — port ouvert
→ TCP RST — **pas de trace dans le fichier log**

→ TCP SYN port 81
← TCP ACK, RST or No packet — port fermé

- **Résultats en 0.3 secondes**

Nmap : UDP port scan

```
nmap -sU -p53-54 129.194.184.84
```

→ UDP port 53

← No packet port ouvert

→ UDP port 54

← ICMP destination unreachable or No packet port fermé

```
Interesting ports on 129.194.184.84
PORT   STATE      SERVICE
53/udp open       domain
54/udp closed     xns-ch
```

Nmap : OS –O & Service detections –sV

```
nmap -A 129.194.184.80        -A = -O -sV

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 5.3
80/tcp   open  http    Apache httpd 2.2.14
445/tcp   open         Samba smbd 3.X

Running: Linux 2.6.X
OS details: Linux 2.6.32 – 2.6.33
Network distance: 2 hops
```

Récupérer la bannière (Grab banner)

- **telnet <addr>**

- **telnet <addr> 25** **SMTP server**

  220 eig.unige.ch -- Server ESMTP (PMDF V5.2)

- **telnet <addr> 80** **HTTP server**

  HEAD / HTTP/1.0<CR><CR> **démo**

  Server: Apache/2.2.14 (Ubuntu)

- **telnet <addr> 21** **FTP server**

- La bannière peut être modifiée

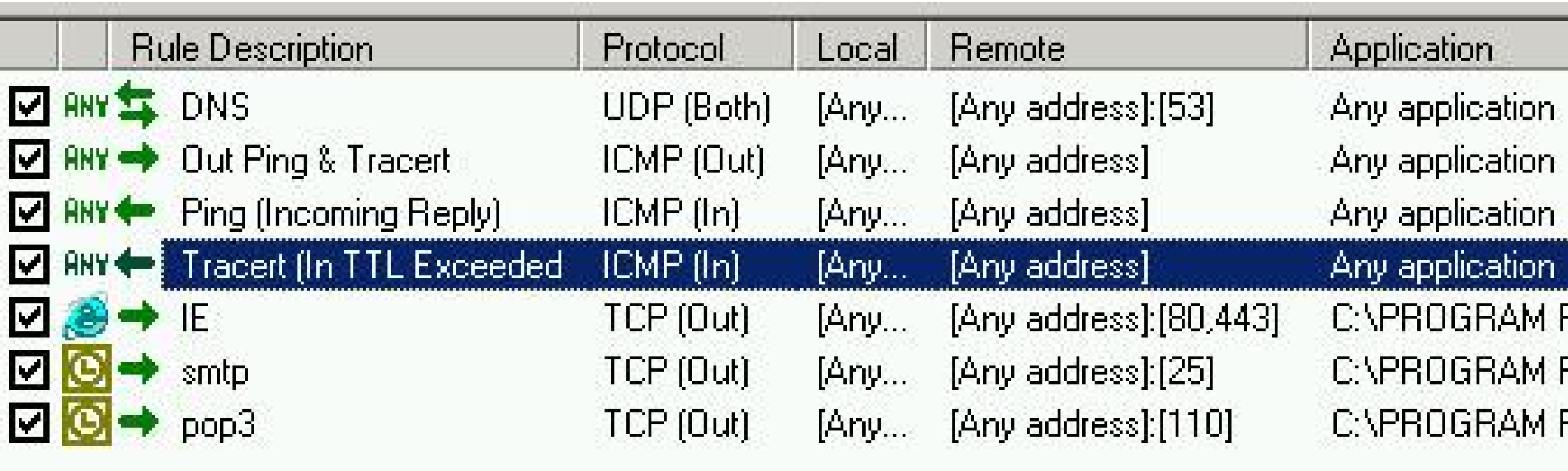
Eléments de comparaison

- Simplicité comme Superscan
  GUI, utilise la pile TCP/IP de Windows
  Mode TCP uniquement

- Richesse avec nmap http://insecure.org/nmap/
  CLI, différents modes (– sT –sS –sU –sO –sV …)
  Exige une librairie WinPcap pour forger les paquets → droits admin
  Outil complexe qui demande des connaissances et de la réflexion

Personal firewall (1)

- *Firewall* au niveau du poste de travail – du serveur
- Règle semblable à celle d'un *firewall* traditionnel

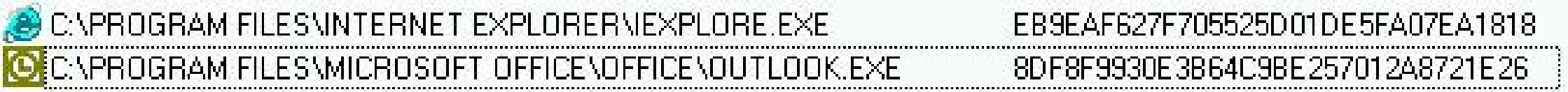


	Rule Description	Protocol	Local	Remote	Application
☑	ANY DNS	UDP (Both)	[Any...	[Any address]:[53]	Any application
☑	ANY Out Ping & Tracert	ICMP (Out)	[Any...	[Any address]	Any application
☑	ANY Ping (Incoming Reply)	ICMP (In)	[Any...	[Any address]	Any application
☑	ANY Tracert (In TTL Exceeded	ICMP (In)	[Any...	[Any address]	Any application
☑	IE	TCP (Out)	[Any...	[Any address]:[80,443]	C:\PROGRAM F
☑	smtp	TCP (Out)	[Any...	[Any address]:[25]	C:\PROGRAM F
☑	pop3	TCP (Out)	[Any...	[Any address]:[110]	C:\PROGRAM F

Personal firewall (2)

- **Protection des applications**

  Empêcher l'exécution de code non autorisé (com, dll, drv, exe, ocx, scr, sys, vxd)



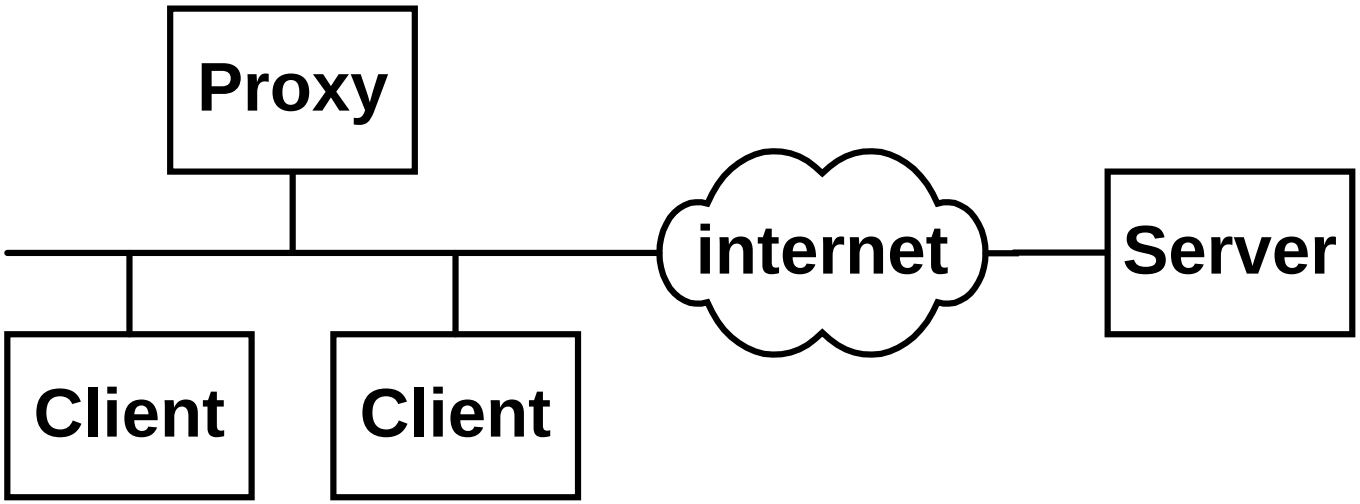
  Détecter l'attaque par substitution (renommer malvare.exe en iexplore.exe) → Protection contre cheval de Troie

- **L'utilisateur ne doit pas pouvoir le désactiver, ni modifier les règles**

- **Attaque possible avec code malicieux**

  http://www.tdeig.ch/windows/contournement_pfw.pdf

Proxy : principe



- Le client adresse toutes ses demandes au proxy qui conserve en mémoire une copie des pages visitées
- Gain lorsque les clients accèdent aux mêmes pages statiques
- Le poste client doit être configuré en conséquence
  L'utilisateur peut parfois décider de ne pas l'utiliser
- Le proxy se charge d'effectuer les requêtes DNS

Proxy : protocole

```
Client                                  Proxy                    Server
→ TCP SYN dst:8000
                          TCP ACK ←
→ HTTP: Get ...
          Host: S
          Proxy Connection = Keep-Alive

                                  → TCP SYN dst:80
                                                       TCP ACK ←
                                  → HTTP: Get ...
                                      Via: P
                                      Host: S
```

IE :
Tools
Internet Options
Connections
LAN Settings

Proxy functions

- Caching

  Mise en mémoire des pages html, résolutions DNS, …ftp

- Tracking, logging

  Enregistrement des sessions … surveiller les utilisateurs

- Filtering

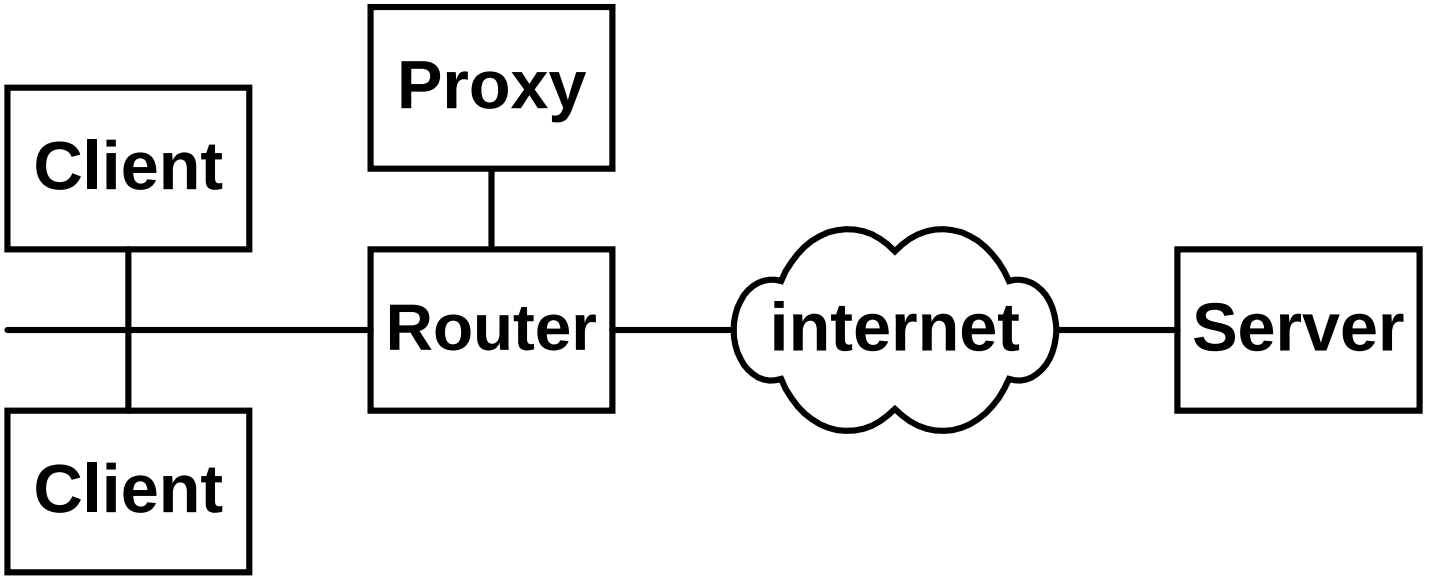
  Filtrage de sites (sport, violence, sexe, …)

- Anonymizing

  Protéger l'anonymat de l'internaute

- Security

Transparent Proxy



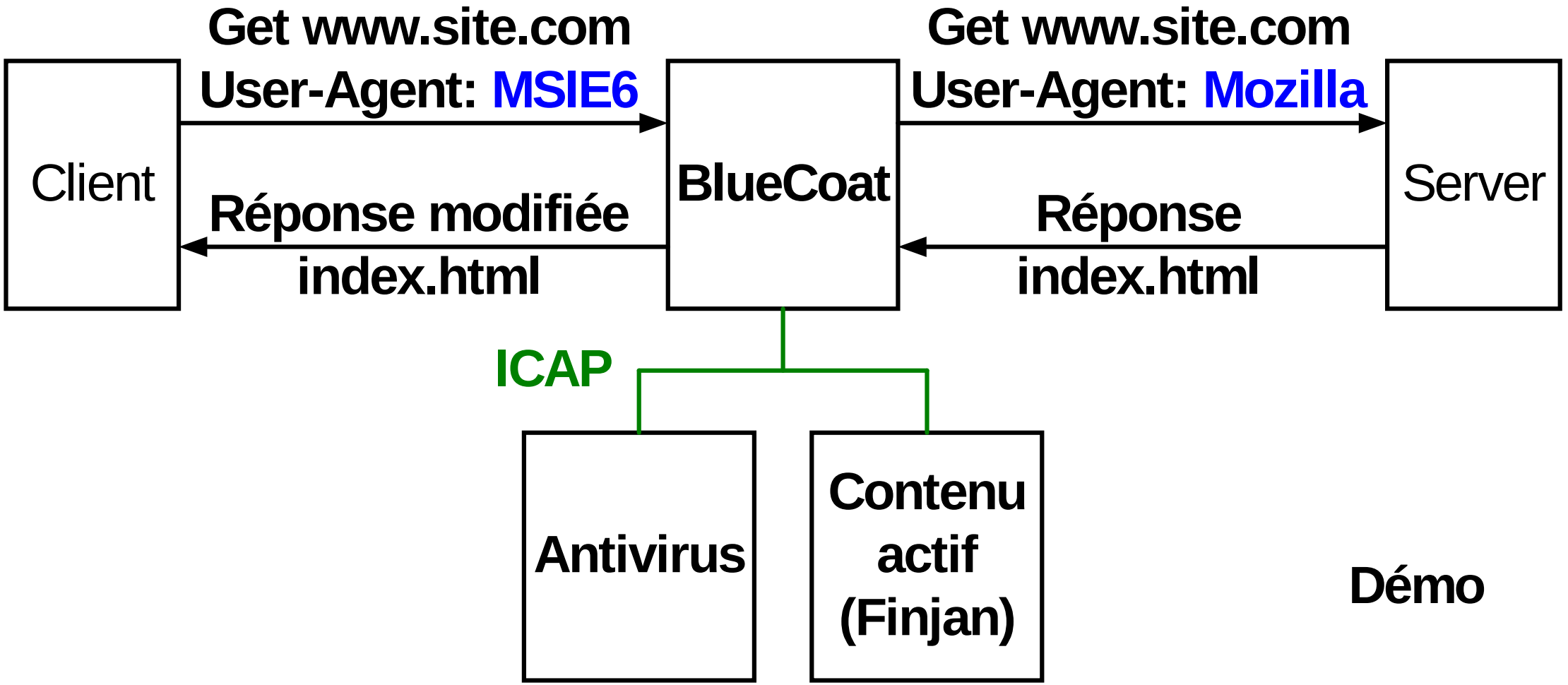
- Routage du flux TCP:80 vers le proxy
- Obligation de passer par le proxy
- Utilisé par les ISP (Point Of Presence)
- Le poste client ne doit pas être configuré spécifiquement
- Le système de cache est transparent
- Intégration des fonctions dans un Firewall applicatif

Firewall Proxy

Proxy Blue Coat

Connect www.site.com

Get www.malware.com



Démo

Proxy HTTP : Opérations à effectuer

- Lors de la requête

  Authentifier l'utilisateur (si possible)

  Limitation des méthodes HTTP acceptées (get, …)

  Vérifications URL (*Pattern matching*, catégorie *Websense*, …)

  Limitation des extensions (.exe)

  Filtrage (modification ou supression) des entêtes User-Agent, Referer, en-tête propriétaire X-Bluecoat-Via (anonymat)

- Lors de la réponse

  Suppression du contenu actif (Javascript, Applet, ActiveX, …)

  Filtrage des entêtes types MIME (Content-Type: text/html, …)

Champs à inspecter

- Bloquage de méthode PUT, POST, …

  `HTTP: Request Method = GET`

- Bloquage de sites (mots clé, sites spécifiques, …)

  `HTTP: Host = www.xyz.ch`

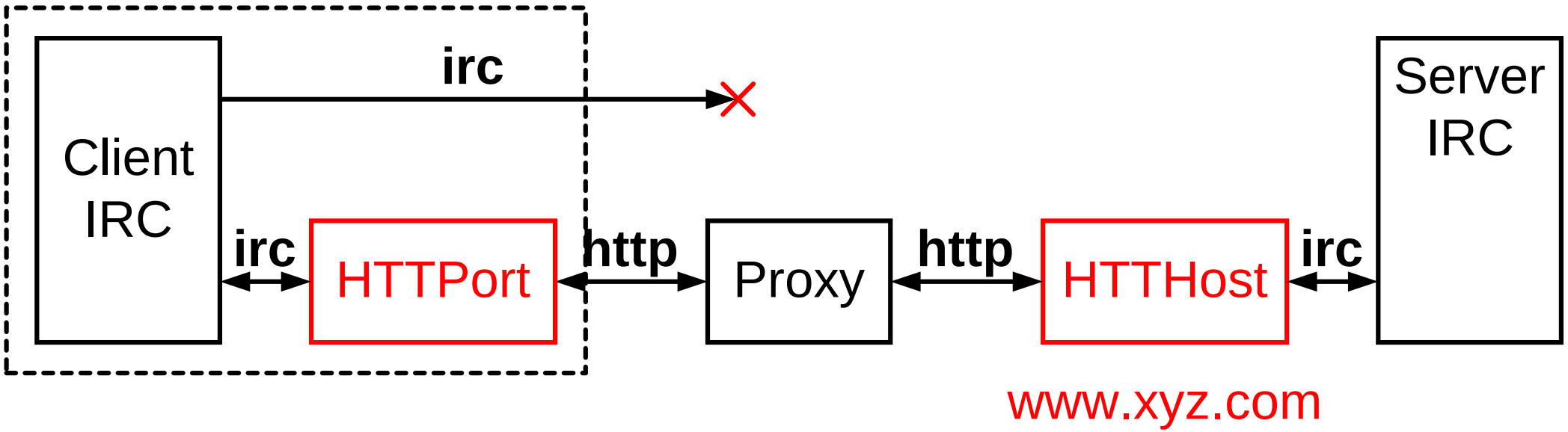
- Bloquage de type MIME

  `HTTP: Content-Type: video/mpeg`

- *URL filtering with regular expression*

  http://www.example.com:80/cgi-bin/search.pl?q=xyz#abc

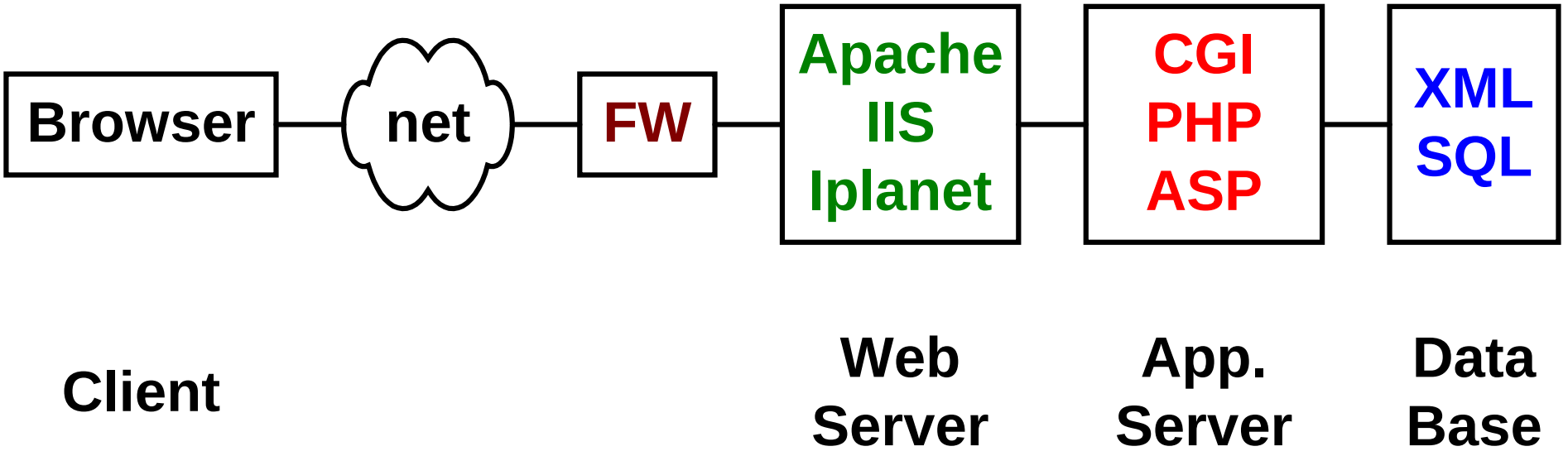
HTTP tunneling



- Seul le flux http est autorisé par le *proxy*
- HTTPort s'installe sur le poste client
- Les requêtes IRC *(Internet Relay Chat)* sont encapsulées
  http://www.xyz.com:80/script.pl?aX6..aTz (query)
  en-tête aléatoire : flux irc codé en base 64 (évent. chiffré)
- Nécessité de disposer d'un serveur HTTHost
- Mécanisme similaire pour les réponses IRC

Interprétation de l'URL (RFC 1808 Relative URL)

http://FQDN:80/chemin/script.asp?a=bob&b=123

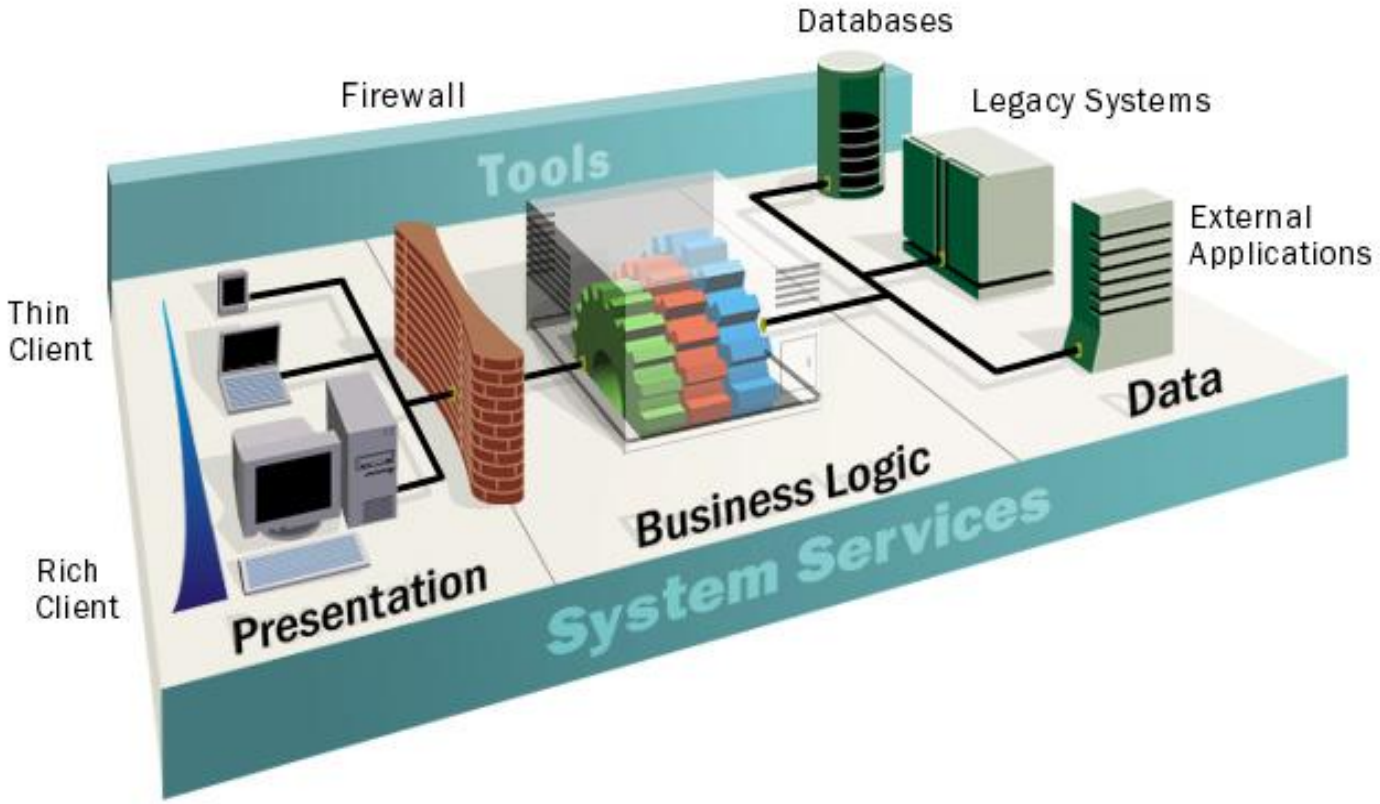


<scheme>://<net_loc>/<path>;<params>?<query>#<fragment>

http://www.example.com:80/cgi-bin/search.pl?q=xyz#abc

Composants d'un SI

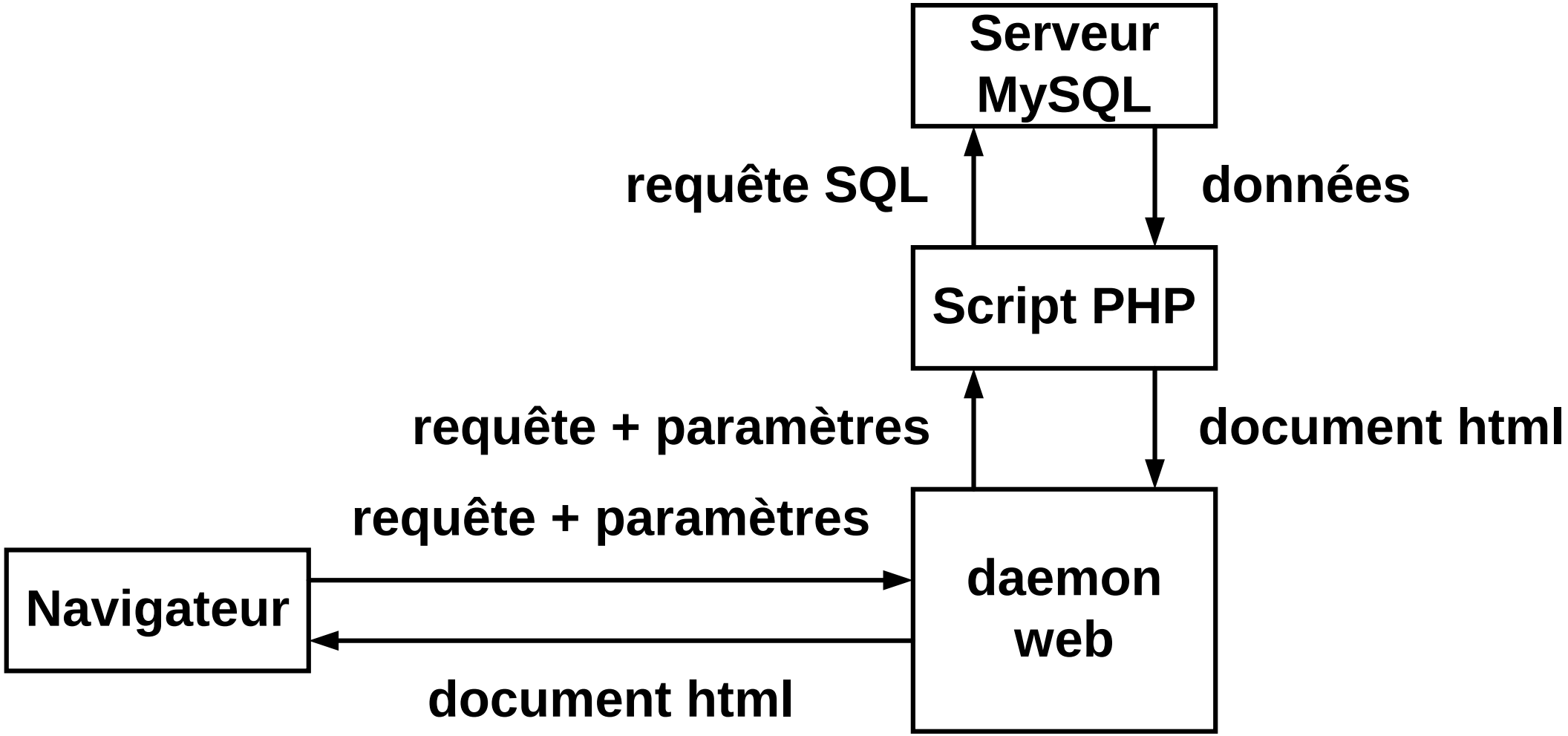
- Personnes
- Données
- Logiciels
- Matériels
- Réseaux



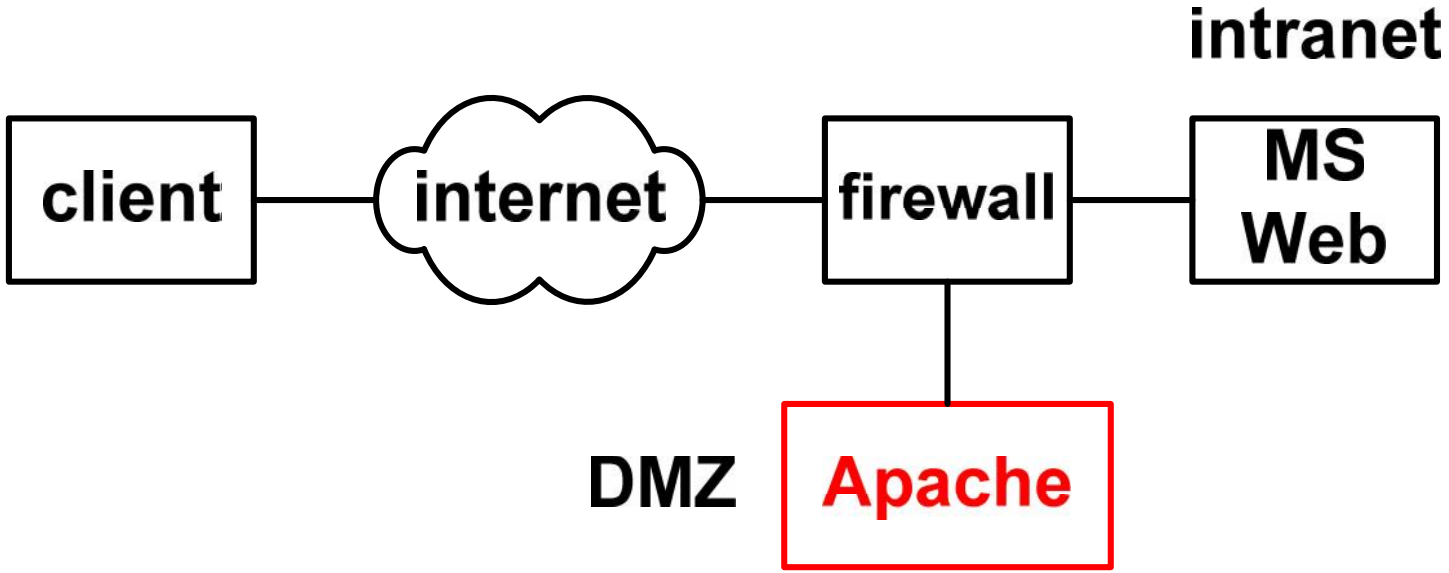
→ Risques à tous les niveaux !

World-Wide Web

- Configuration du travail de diplôme Dizon 2003 :



Reverse Proxy



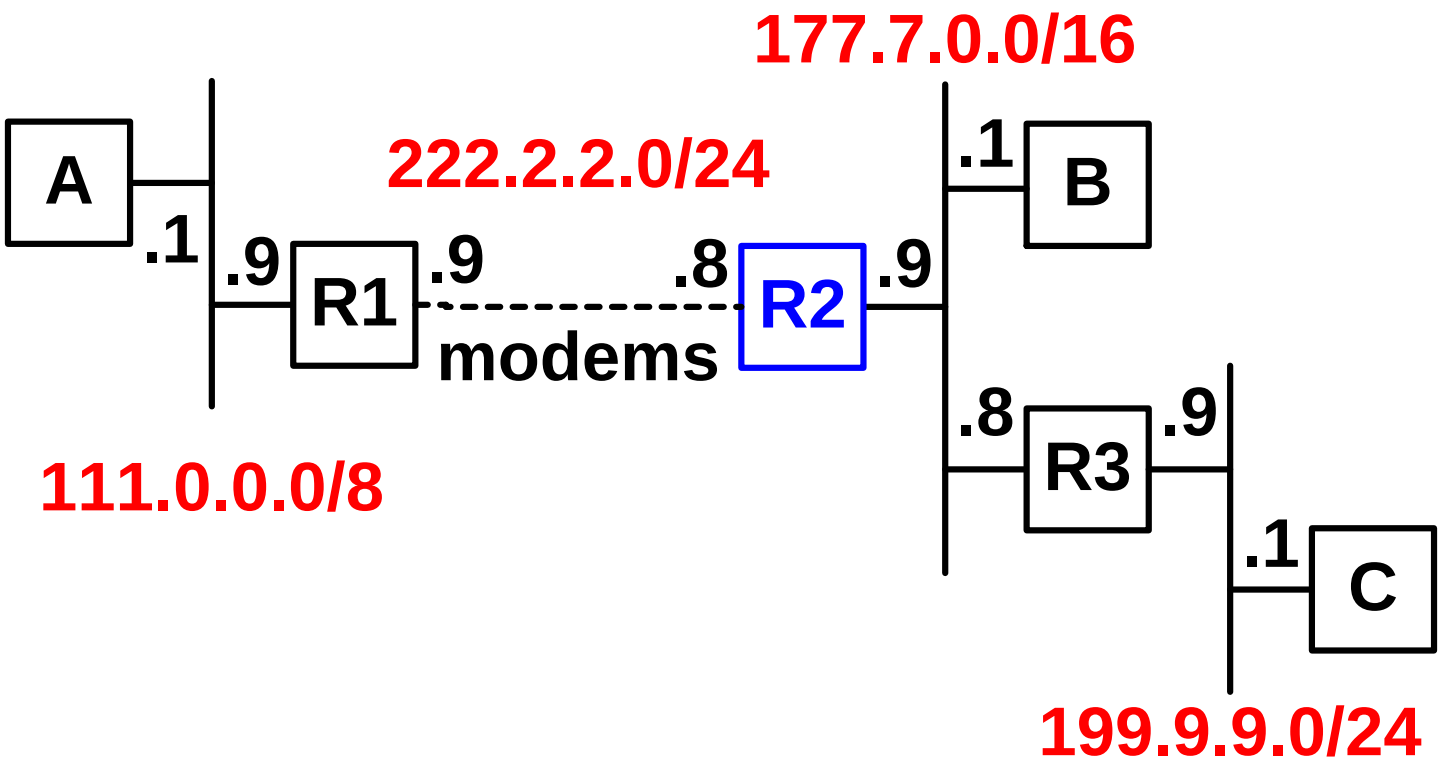
- Echange http entre Client et serveur Apache
- Echange http entre Client Apache et serveur Web MS
- Le **reverse proxy** (Apache) se fait passer pour le serveur web
- Les données applicatives (html, …) se trouvent dans l'intranet (serveur Web MS)

Ex 1

- Déterminer l'alg. de mise en mémoire dans le cache ARP (slide 7)
- if (trame ARP request) → créer ou mettre à jour équivalence adr **source** IP : Eth
- If (trame ARP response) → idem
- Implémentation Windows : XP – Vista – Seven
- On parle dans ce cas de failles conceptuelles car le protocole ARP peut être utilisé pour produire des équivalences malicieuses
  → *ARP cache poisoning*

Ex2 : déterminer les commandes pour R2

- `ifconfig eth0 177.7.0.9  mask 255.255.0.0`
- `ifconfig le0 222.2.2.8  mask 255.255.255.0`
- `route add 111.0.0.0  222.2.2.9`
- `route add 199.9.9.0  177.7.0.8`



Ex 3

- En notation CIDR *(Classless Inter-Domain Routing)*, le réseau précédent correspond à 10.1.0.0/16

- Déterminer l'intervalle du réseau IP = 11.0.0.0/8

- IP range 11.0.0.0 à 11.255.255.255
- Adresse de *subnet* 11.0.0.0
- Adresse de diffusion IP 11.255.255.255
- Intervalle disponible 11.0.0.1 → 11.255.255.254

Problématique DNS : Correction (1/2)

4 A quoi sert le serveur DNS Debian 5.0 (voir schéma) ?

A résoudre www.tdeig.ch envoyé par un étudiant depuis son domicile. Ce serveur est dit **autoritaire** pour la zone **tdeig.ch**

5 Comment est-il connu de Root ?

Grâce à une inscription chez www.nic.ch CHF 17.- / an

6 Quelle(s) valeur(s) de serveur DNS faut-il donner au client de l'intranet ? **Tenir compte du mécanisme de Failover**

10.2.0.1 pour utiliser la fonction DNS forwarder (proxy implémenté dans pfSense)

§21.3 : DNS Forwarder uses the DNS servers configured in System - General Setup, or those obtained from your ISP for dynamically configured WAN interfaces

Problématique DNS : Correction (2/2)

7 Un serveur DNS est-il utile dans l'intranet ?

Si oui pour quelles fonctions ? Associer FQDN à **private IP**

www.tdeig.ch : 10.10.10.10

Si non expliquer le fonctionnement

Pas besoin de serveur DNS public puisque le FW (proxy DNS) s'en occupe

```
ipconfig /all
Router          = 10.2.0.1
Serveur DNS = 10.2.0.1
```