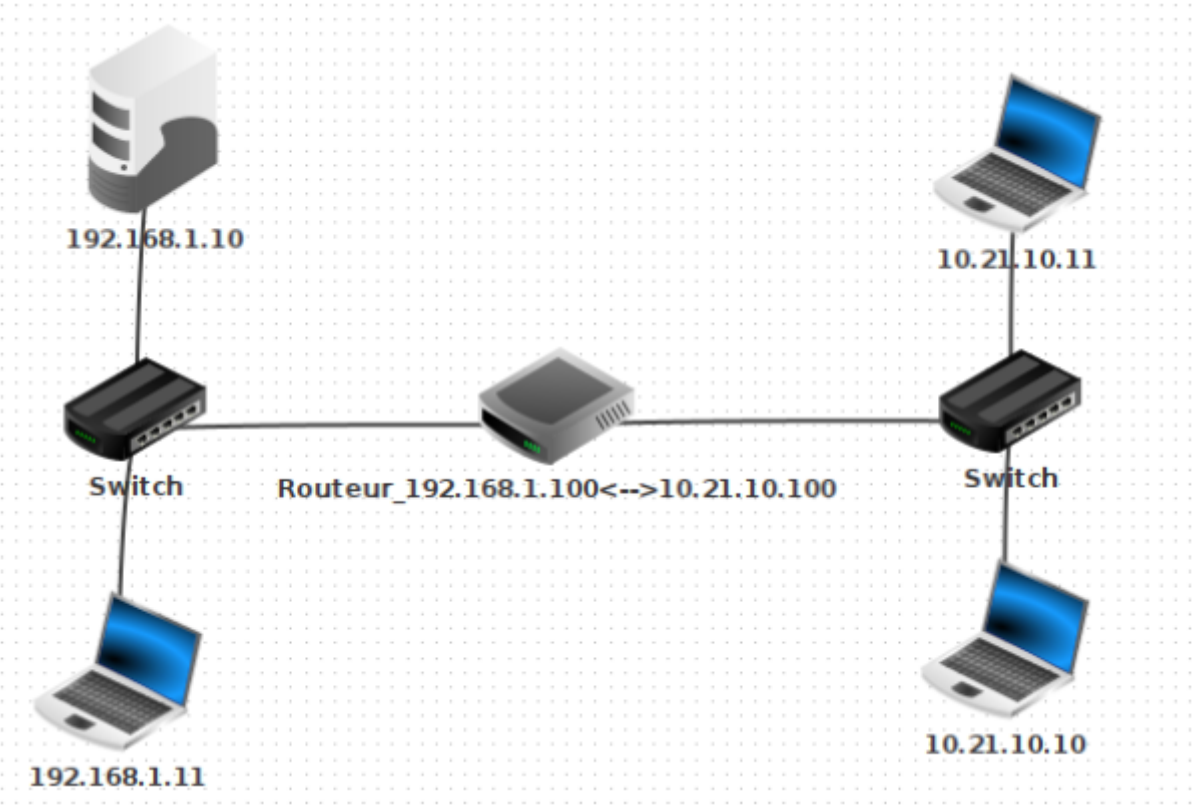
Filius : Apprentissage réseaux IPV4

Filius site AL



Reseaux : exemple avec Filius FR

filius_guide_du_debutant_2022.pdf

filius.deb pour Linux

filius pour Windows

(Enlever .tar)

Utilisation Filius 1

Utilisation Filius 2

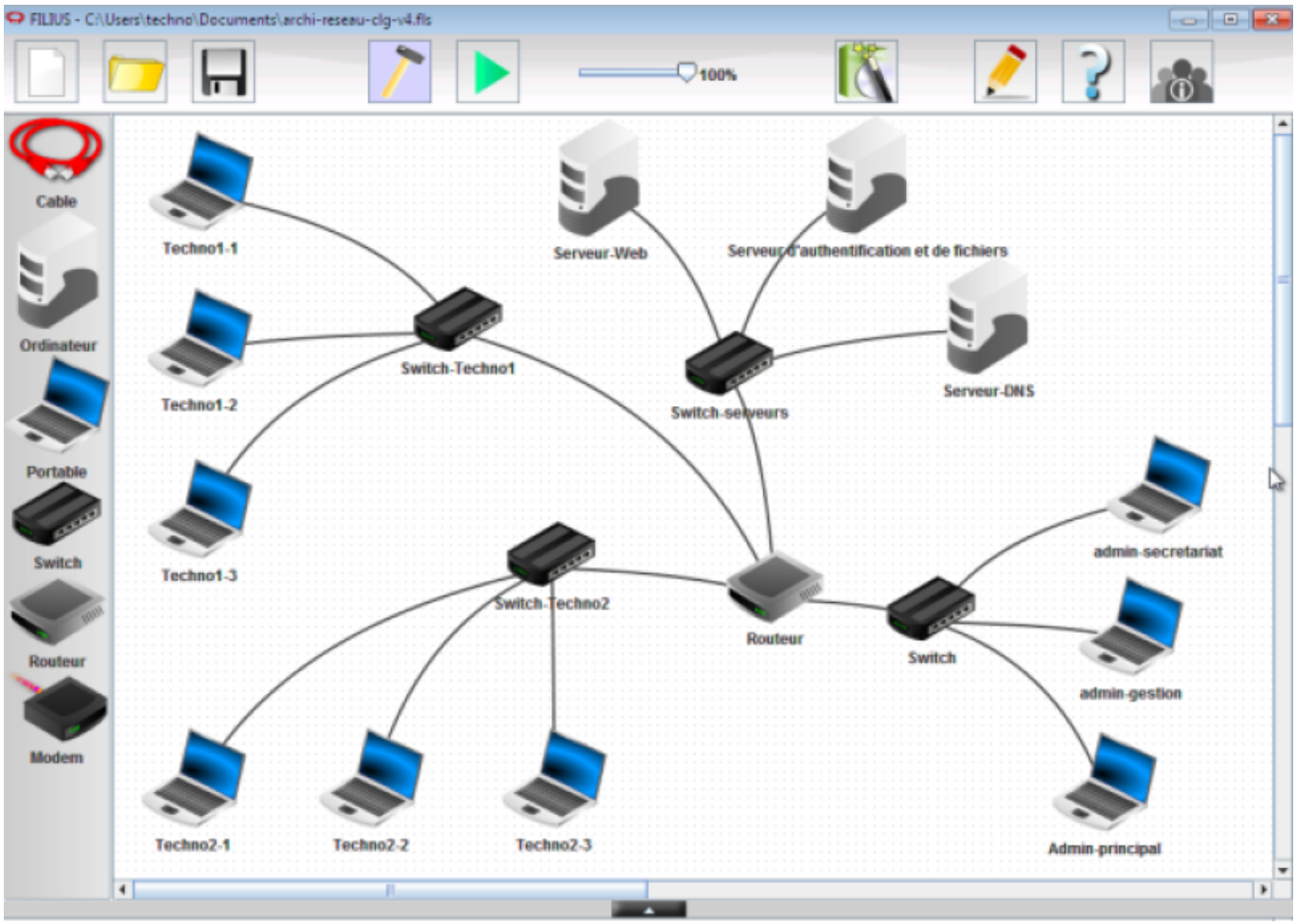
TP1 - Modélisation de réseaux avec Filius

TP2 - Les serveurs DNS avec Filius

Simulation (1) Reseaux avec Filius FR

Simulation (2) Reseaux avec Filius FR

TP Filius .pdf



Démarrer un serveur web avec python

Tp Filius

Masque Reseau IPV4

Le concept de bloc CIDR

CIDR (Classless Inter-Domain Routing : Routage Inter-Domaine Sans Classe) est une méthode d'allocation et de notation des adresses IP qui a été introduite en 1993 pour remplacer le système d'adressage classique basé sur les classes (Class A, B, C). Principes fondamentaux

Un bloc CIDR est représenté par une adresse IP suivie d'une barre oblique (/) et d'un nombre qui indique la longueur du préfixe réseau. Par exemple : 192.168.1.0/24

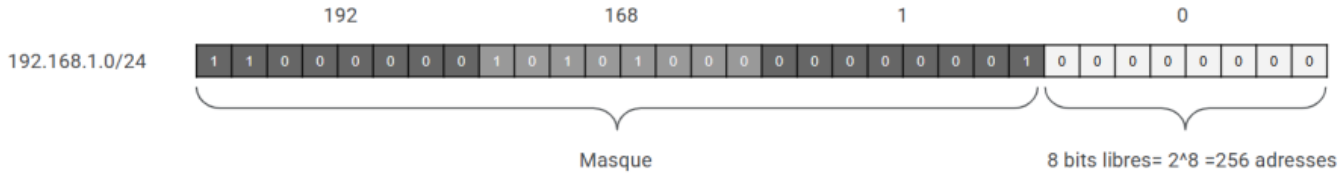
- L'adresse IP 192.168.1.0 représente l'adresse de base du réseau
- Le nombre après la barre oblique (24) indique combien de bits, en partant de la gauche, sont utilisés pour identifier le réseau

Comment ça fonctionne

Une adresse IPv4 est composée de 32 bits, généralement exprimée comme une suite de 4 chiffres compris entre 0 et 255, séparés par des points (exemple: 10.123.12.217)

Par exemple, pour 192.168.1.0/24:

- Les 24 premiers bits (192.168.1) identifient le réseau (le masque)
- Les 8 derniers bits (<taille de l'adresse IP: 32> - <taille du masque: 24> = 8) sont libres, et peuvent être utilisés pour les hôtes



Exemples courants

```
/32: Une seule adresse IP
/24: Un réseau local standard (256 adresses)
/16: Un grand réseau d'entreprise
/8: Un très grand bloc (16 millions d'adresses)
```

Le CIDR est fondamental pour la gestion efficace de l'espace d'adressage IP et pour le routage sur Internet.

RFC 1918

Avec l'explosion du nombre de périphériques connectés sur Internet, le nombre maximal d'adresse (2^32) aurait vite été atteint.

Pour palier ce problème, la RFC 1918, intitulée “Address Allocation for Private Internets”, a été publiée en février 1996 par l'IETF (Internet Engineering Task Force).

Cette norme définit les plages d'adresses IP réservées pour une utilisation dans les réseaux privés, sans être routées sur Internet public. Elle a introduit trois blocs d'adresses spécifiques :

- 10.0.0.0/8 (permettant environ 16,7 millions d'adresses)
- 172.16.0.0/12 (environ 1 million d'adresses) et
- 192.168.0.0/16 (65 536 adresses).

Pour contourner la limite du nombre d'adresses IPv4 c'est de passer à l'IPv6

Les masques de sous reseaux en IPV4 FR

CIDR : masque de sous reseaux IPV4 FR

Formule pour trouver le nombre de machines(hotes) par réseaux = 2^(32-masque CIDR)-2 : exemple

: 2^(32-24)-2 = 254

Notation décimale	Notation binaire	Notation CIDR	Nombre de bits pour hôtes	Hôtes possibles (total – 2)
255.0.0.0	11111111.00000000.00000000.00000000	/8	24	(2^24)-2 soit 16 777 214
255.128.0.0	11111111.10000000.00000000.00000000	/9	23	8 388 606
255.192.0.0	11111111.11000000.00000000.00000000	/10	22	4 194 302
255.224.0.0	11111111.11100000.00000000.00000000	/11	21	2 097 150
255.240.0.0	11111111.11110000.00000000.00000000	/12	20	1 048 574
255.248.0.0	11111111.11111000.00000000.00000000	/13	19	524 286
255.252.0.0	11111111.11111100.00000000.00000000	/14	18	262 142
255.254.0.0	11111111.11111110.00000000.00000000	/15	17	131 070
255.255.0.0	11111111.11111111.00000000.00000000	/16	16	65 534
255.255.128.0	11111111.11111111.10000000.00000000	/17	15	32 766
255.255.192.0	11111111.11111111.11000000.00000000	/18	14	16 382
255.255.224.0	11111111.11111111.11100000.00000000	/19	13	8 190
255.255.240.0	11111111.11111111.11110000.00000000	/20	12	4 094
255.255.248.0	11111111.11111111.11111000.00000000	/21	11	2 046
255.255.252.0	11111111.11111111.11111100.00000000	/22	10	1 022
255.255.254.0	11111111.11111111.11111110.00000000	/23	09	510
255.255.255.0	11111111.11111111.11111111.00000000	/24	08	254
255.255.255.128	11111111.11111111.11111111.10000000	/25	07	126
255.255.255.192	11111111.11111111.11111111.11000000	/26	06	62
255.255.255.224	11111111.11111111.11111111.11100000	/27	05	30
255.255.255.240	11111111.11111111.11111111.11110000	/28	04	14
255.255.255.248	11111111.11111111.11111111.11111000	/29	03	6
255.255.255.252	11111111.11111111.11111111.11111100	/30	02	2

Le routage réseau IPV4 /Nat

Qu'est-ce qu'un routeur ?

Un routeur est un équipement réseau physique responsable de l'acheminement des paquets vers leur destination. Les routeurs se connectent à deux ou plusieurs réseaux ou sous-réseaux IP et se transmettent des paquets de données entre eux selon les besoins. Ils sont utilisés pour les particuliers et les bureaux pour établir les connexions au réseau local. Des routeurs plus puissants sont présents partout sur Internet, afin d'aider les paquets de données à atteindre leur destination.

Comment fonctionne le routage ?

Les routeurs s'appuient sur des **tables de routage** internes pour prendre des décisions concernant l'acheminement des paquets le long des chemins réseau. Une table de routage enregistre les chemins que les paquets doivent emprunter pour atteindre chaque destination dont le routeur est responsable.

Les **tables de routage** peuvent être statiques ou dynamiques. Les statiques ne changent pas et sont établies manuellement par un administrateur réseau. Dans les grandes lignes, elles fixent les itinéraires que les paquets de données empruntent sur le réseau,

Les tables de routage dynamiques se mettent à jour automatiquement. Les routeurs dynamiques s'appuient sur divers protocoles de routage pour déterminer les chemins les plus courts et les plus rapides. Ils déterminent également le temps nécessaire aux paquets pour atteindre leur destination.

Quels sont les principaux protocoles de routage ?

Pour les réseaux, un protocole constitue un ensemble de règles normalisées de formatage des données conçu pour permettre à n'importe quel ordinateur connecté de comprendre les données. Un protocole de routage est un protocole utilisé pour identifier ou annoncer les chemins réseau.

Les protocoles suivants aident les paquets de données à trouver leur chemin sur Internet :

IP : l'Internet Protocol ou protocole Internet (IP) spécifie l'origine et la destination de chaque paquet de données. Les routeurs inspectent l'en-tête IP de chaque paquet pour savoir où les envoyer.

BGP : le protocole de routage BGP (Border Gateway Protocol, protocole de passerelle en bordure) sert à annoncer quels réseaux contrôlent quelles adresses IP et quels réseaux se connectent entre eux. (Les grands réseaux qui effectuent ces annonces BGP sont appelés systèmes autonomes.) Le BGP est un protocole de routage dynamique.

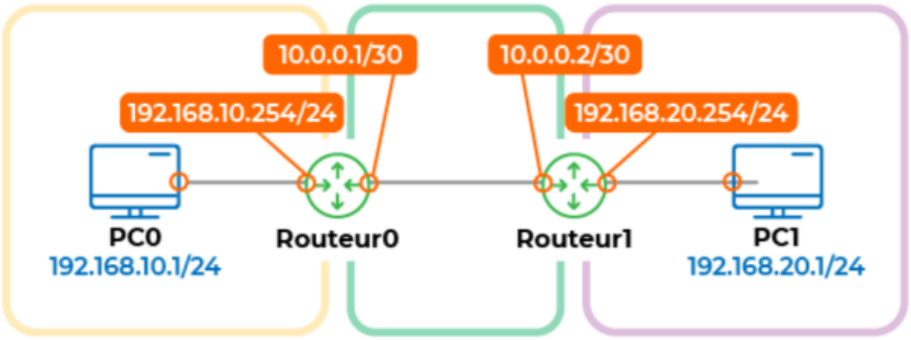
Les protocoles ci-dessous acheminent les paquets au sein d'un AS :

OSPF : le protocole OSPF (Open Shortest Path First, itinéraire ouvert le plus court en premier) est couramment utilisé par les routeurs réseau pour identifier dynamiquement les itinéraires disponibles les plus rapides et les plus courts afin d'envoyer les paquets vers leur destination.

RIP : le protocole RIP (Routing Information Protocol, protocole d'informations de routage) s'appuie sur le « nombre de sauts » pour trouver le chemin le plus court d'un réseau à un autre. Le « nombre de sauts » désigne ici le nombre de routeurs par lesquels un paquet doit passer pendant son trajet. (Lorsqu'un paquet passe d'un réseau à l'autre, on parle de « saut ».)

Les autres protocoles de routage interne comprennent l'**EIGRP** (Enhanced Interior Gateway Routing Protocol, protocole de routage par passerelle intérieure renforcé, principalement utilisé pour les routeurs Cisco) et l'**IS-IS** (Intermediate System to Intermediate System, système intermédiaire à système intermédiaire).

Exemple routage statique



Architecture composée de 2 routeurs et de 3 réseaux.

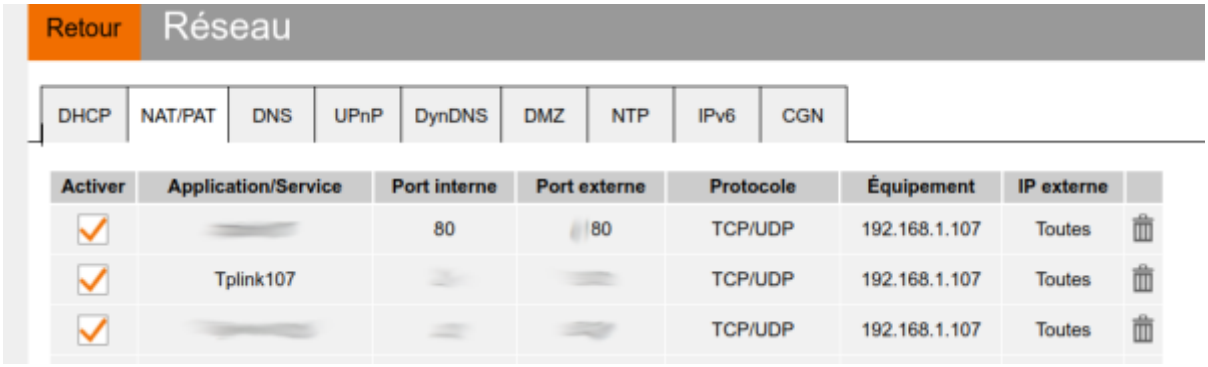
Cette architecture est composée de 2 routeurs et de 3 réseaux. Si on regarde la table de routage du Router0, voilà à quoi elle ressemble :

Réseau de destination	Réseau directement connecté	Interface de sortie	Prochain saut
192.168.10.0/24	Oui	192.168.10.254	
10.0.0.0/30	Oui	10.0.0.1	
192.168.20.0/24	Non	10.0.0.1	10.0.0.2

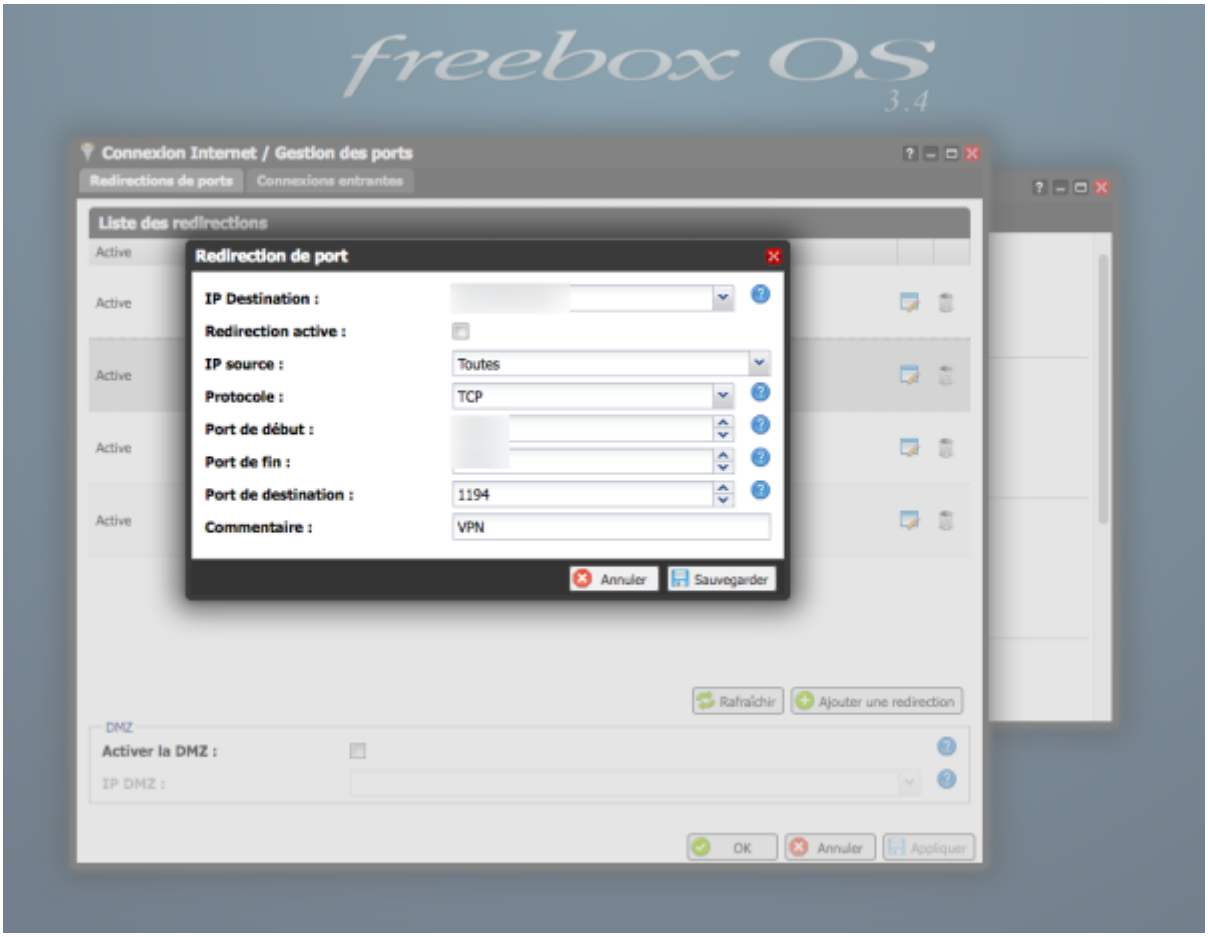
Cette table contient 3 routes vers les 3 réseaux de notre architecture.
Cette fois, si un paquet à destination de 192.168.20.1 arrive sur le Router0, celui-ci voit que le réseau associé est 192.168.20.0/24. Le routeur n'est pas directement connecté à ce réseau, et pour l'atteindre il sait qu'il va devoir faire passer le paquet par un autre routeur dont l'adresse est 10.0.0.2. Dans une table de routage, cet autre routeur est souvent identifié comme "prochain saut" ou "passerelle".

Exemple de routage NAT sur Box

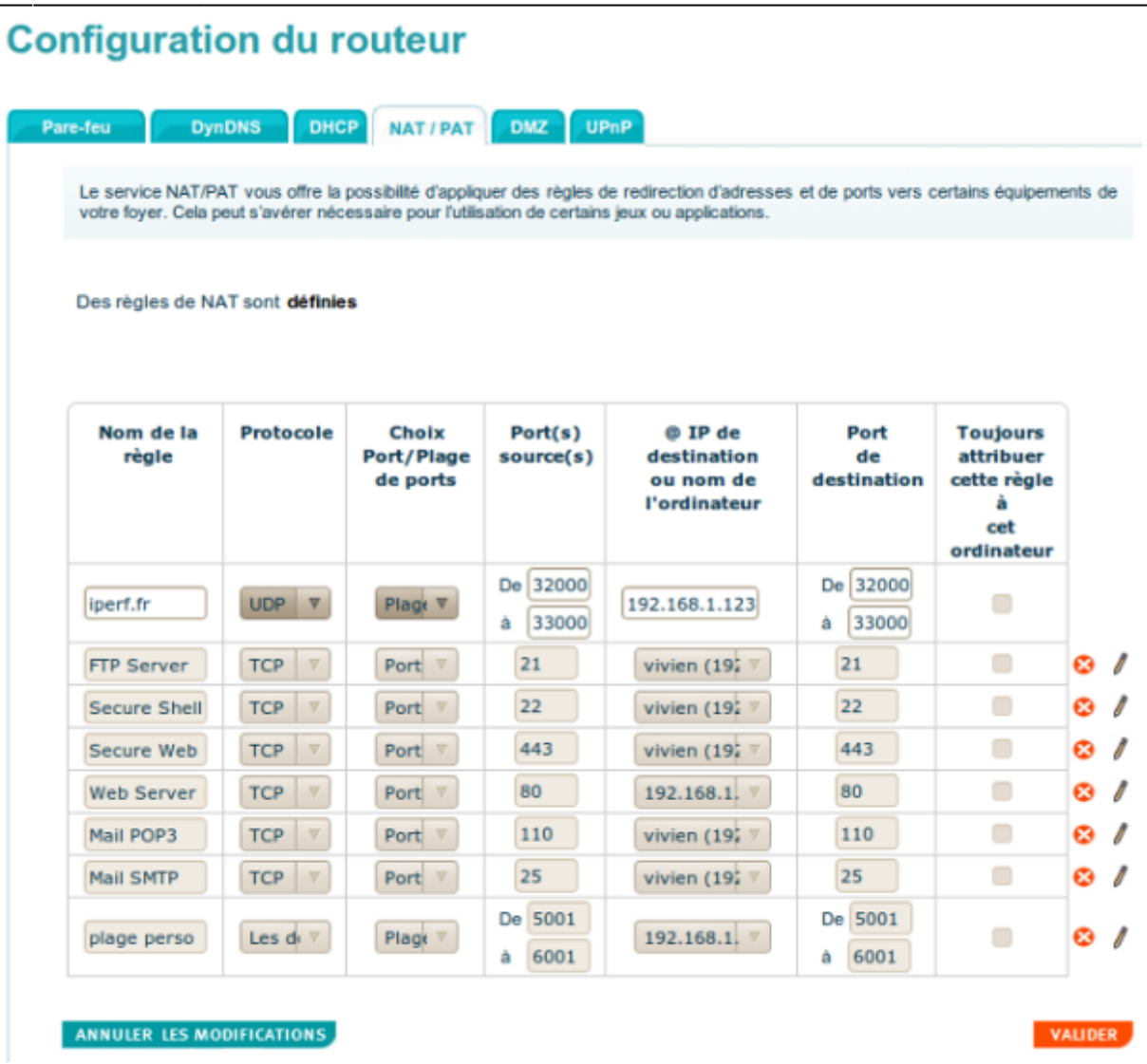
Orange


Retour
Réseau
DHCP
NAT/PAT
DNS
UPnP
DynDNS
DMZ
NTP
IPv6
CGN
Activer
Application/Service
Port interne
Port externe
Protocole
Équipement
IP externe
80
80
TCP/UDP
192.168.1.107
Toutes
Tplink107
TCP/UDP
192.168.1.107
Toutes
TCP/UDP
192.168.1.107
Toutes

Free


freebox OS
3.4
Connexion Internet / Gestion des ports
Redirections de ports
Connexions entrantes
Liste des redirections
Redirection de port
IP Destination :
Redirection active :
IP source :
Toutes
Protocole :
TCP
Port de début :
Port de fin :
Port de destination :
1194
Commentaire :
VPN
Annuler
Sauvegarder
Rafraîchir
Ajouter une redirection
DMZ
Activer la DMZ :
IP DMZ :
OK
Annuler
Appliquer

bbox


Configuration du routeur
Pare-feu
DynDNS
DHCP
NAT / PAT
DMZ
UPnP
Le service NAT/PAT vous offre la possibilité d'appliquer des règles de redirection d'adresses et de ports vers certains équipements de votre foyer. Cela peut s'avérer nécessaire pour l'utilisation de certains jeux ou applications.
Des règles de NAT sont définies
Nom de la règle
Protocole
Choix Port/Plage de ports
Port(s) source(s)
@ IP de destination ou nom de l'ordinateur
Port de destination
Toujours attribuer cette règle à cet ordinateur
iperf.fr
UDP
Plage
De 32000 à 33000
192.168.1.123
De 32000 à 33000
FTP Server
TCP
Port
21
vivien (19
21
Secure Shell
TCP
Port
22
vivien (19
22
Secure Web
TCP
Port
443
vivien (19
443
Web Server
TCP
Port
80
192.168.1.
80
Mail POP3
TCP
Port
110
vivien (19
110
Mail SMTP
TCP
Port
25
vivien (19
25
plage perso
Les d
Plage
De 5001 à 6001
192.168.1.
De 5001 à 6001
ANNULER LES MODIFICATIONS
VALIDER

SFR


http://192.168.1.1/network/nat
neufbox - NAT
SFR
neufbox
Etat
Réseau
Wifi
Hotspot
Applications
Maintenance
Eco
Général
WAN
DynDNS
DNS
DHCP
NAT
Route
Filtrage
Translation de ports
Nom Protocole Type Ports externes Adresse IP de destination Ports de destination Activation
1 BO2 les deux Port 3074 192.168.1.48 3074 Désactiver
2 Nom aléatoire TCP Port 3074 192 168 1 3074 Activer
Choisir les deux
Cliquer ici pour trouver l'adresse IP de votre console

Serveur DNS

DNS, c'est l'abréviation de **D**omain **N**ame **S**ystem — ou, en bon français, **système de noms de domaine**.

Il permet de traduire des noms de domaine lisibles par l'humain (comme fablab37110.ovh) en adresses IP compréhensibles par les machines (comme 192.0.2.1).

Comment fonctionne le DNS ?

1. La requête DNS

Lorsqu'un utilisateur tape fablab37110.ovh dans son navigateur, celui-ci interroge d'abord le cache DNS local (souvent géré par le système d'exploitation).

2. Les serveurs récursifs

Si l'information n'est pas dans le cache, la requête est envoyée à un serveur DNS récursif, souvent fourni par votre fournisseur d'accès à Internet (FAI) ou Google (8.8.8.8).

3. La hiérarchie DNS

Le serveur récursif consulte ensuite :

- Le serveur racine (root DNS),
- Puis le serveur de domaine de premier niveau (TLD), comme .fr,
- Et enfin le serveur faisant autorité pour fablab37110.ovh

4. La résolution finale

Le serveur faisant autorité renvoie l'adresse IP correspondante à fablab37110.ovh , et celle-ci est utilisée pour établir la connexion au serveur web.

Les types d'enregistrements DNS

Voici les principaux types d'enregistrements DNS utilisés pour gérer un nom de domaine :

Type	Fonction principale
A	Associe un nom de domaine à une adresse IPv4
AAAA	Associe à une adresse IPv6
CNAME	Alias d'un autre nom de domaine
MX	Indique les serveurs de messagerie

Type	Fonction principale
TXT	Contient des informations diverses (SPF, vérifications Google...)
NS	Spécifie les serveurs DNS autoritaires

Puis-je changer mes DNS pour accélérer ma connexion ?

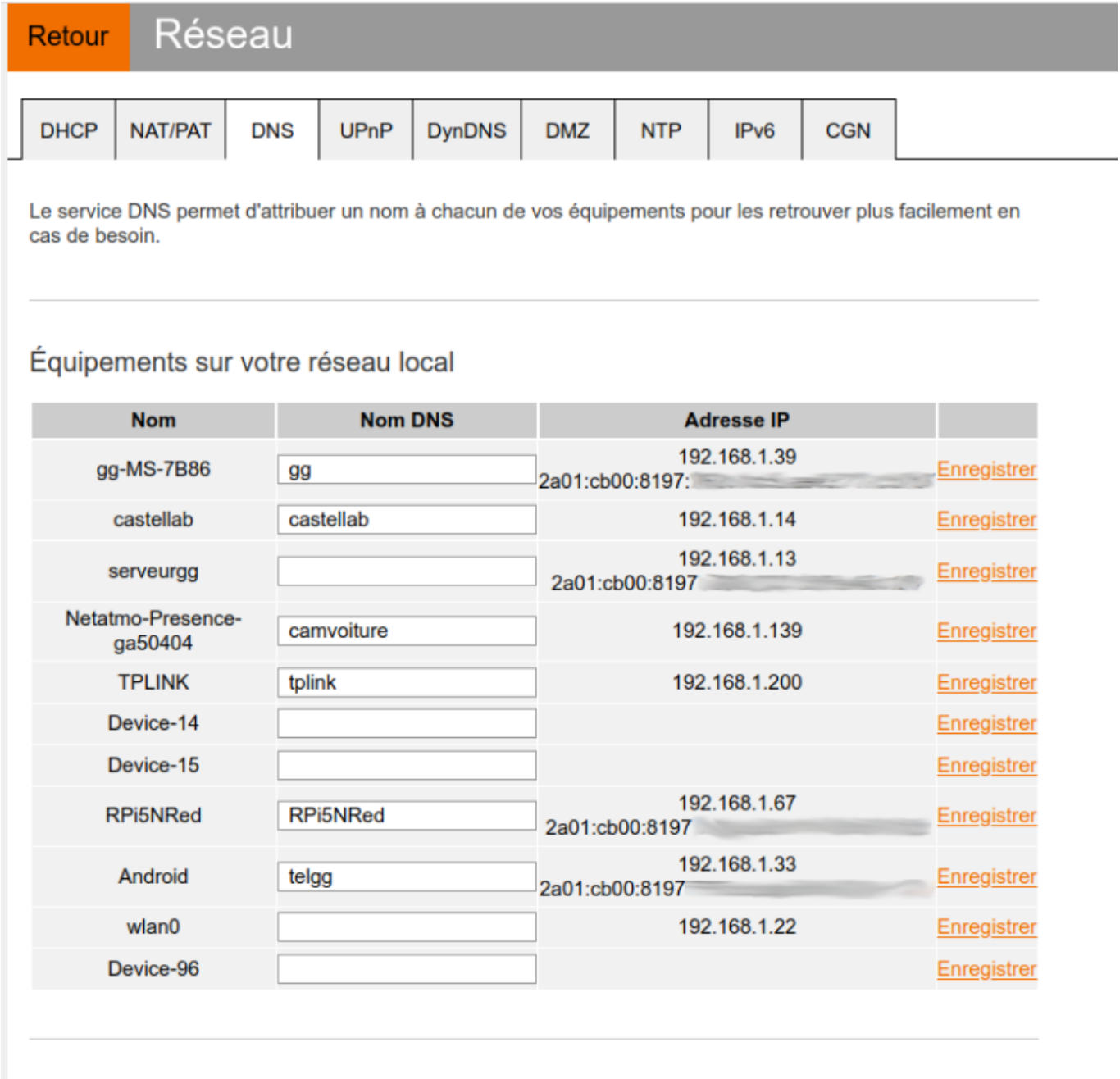
Oui. CertainsDNS publics sont plus rapides que ceux de votre FAI.

DNS les plus rapides en 2025

#	DNS	Adresses IPv4	Adresses IPv6
1	Cloudflare 1.1.1.1	1.1.1.1 - 1.0.0.1	2606:4700:4700::1111 - 2606:4700:4700::1001
2	Cisco OpenDNS Home	208.67.222.222 - 208.67.220.220	2620:119:35::35 - 2620:119:53::53
3	Neustar UltraDNS Public	64.6.64.6 - 64.6.65.6	2620:74:1b::1:1 - 2620:74:1c::2:2
4	NextDNS	45.90.28.0 - 45.90.30.0	2a07:a8c0:: - 2a07:a8c1::
5	Google Public DNS	8.8.8.8 - 8.8.4.4	2001:4860:4860::8888 - 2001:4860:4860::8844
6	Quad9	9.9.9.9 - 149.112.112.112	2620:fe::fe - 2620:fe::9
7	Comodo Secure DNS	8.26.56.26 - 8.20.247.20	–
8	Yandex.DNS	77.88.8.8 - 77.88.8.1	2a02:6b8::feed:0ff - 2a02:6b8:0:1::feed:0ff
9	SafeDNS	195.46.39.39 - 195.46.39.40	2001:67c:2778::3939 - 2001:67c:2778::3940
10	FDN	80.67.169.12 et 80.67.169.40	2001:910:800::12 et 2001:910:800::40

Utiliser les noms pour se connecter à vos serveurs interne

sur une Live Box



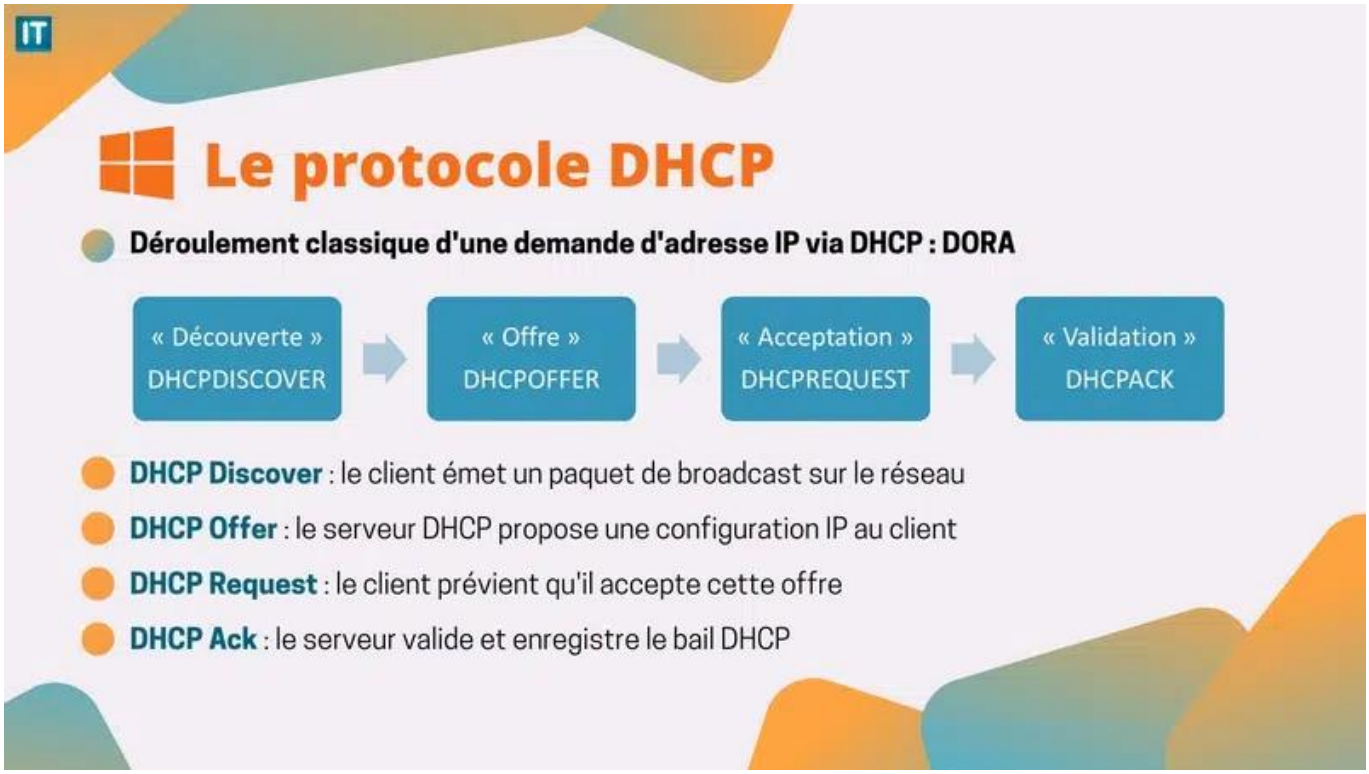
Serveur DHCP

DHCP : Présentation et définitions

Le DHCP (Dynamic Host Configuration Protocol) est un protocole réseau essentiel pour attribuer dynamiquement des adresses IP à chaque hôte sur le réseau local, que ce soit le réseau d'une entreprise ou le réseau du logement d'un particulier.

Le protocole DHCP a été utilisé la première fois en 1993. Il est défini par la RFC1531 et a été, par la suite, modifié et complété par les RFC1534, RFC2131 et RFC2132. Ce protocole fonctionne aussi bien en IPv4 qu'en IPv6. Dans ce cas, il s'appelle DHCPv6 et les adresses peuvent être auto configurées, sans DHCP.

Le protocole fonctionne en mode client/serveur et s'appuie essentiellement sur un mécanisme de requêtes DHCP, traitées par le serveur et émises par les clients. Le moteur principal de ce protocole est adossé à la communication BOOTP (utilisant des trames UDP).



Le serveur DHCP va distribuer une configuration réseau complète à la machine : une adresse IP, un masque de sous-réseau, une passerelle par défaut, un ou plusieurs serveurs DNS, etc... Tout dépend des options DHCP configurées dans les paramètres de l'étendue DHCP.

En ce qui concerne l'attribution des adresses IP des serveurs et des imprimantes, il est conseillé de leur attribuer une adresse IP fixe. Ainsi, les adresses contenues dans une étendue prédéfinie ne seront pas affectées par inadvertance, à un autre périphérique.

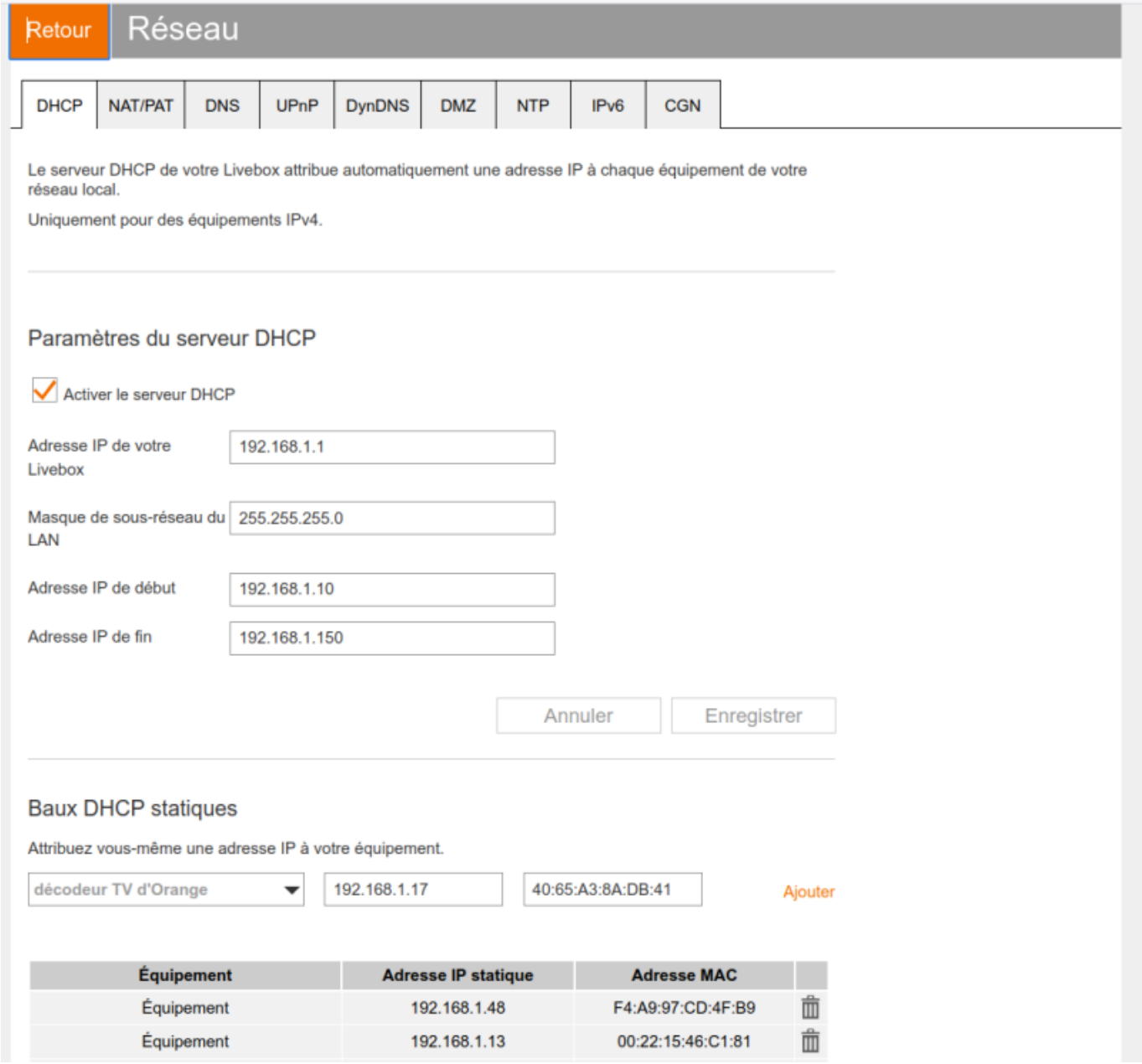
Le protocole DHCP 1

Le protocole DHCP 2

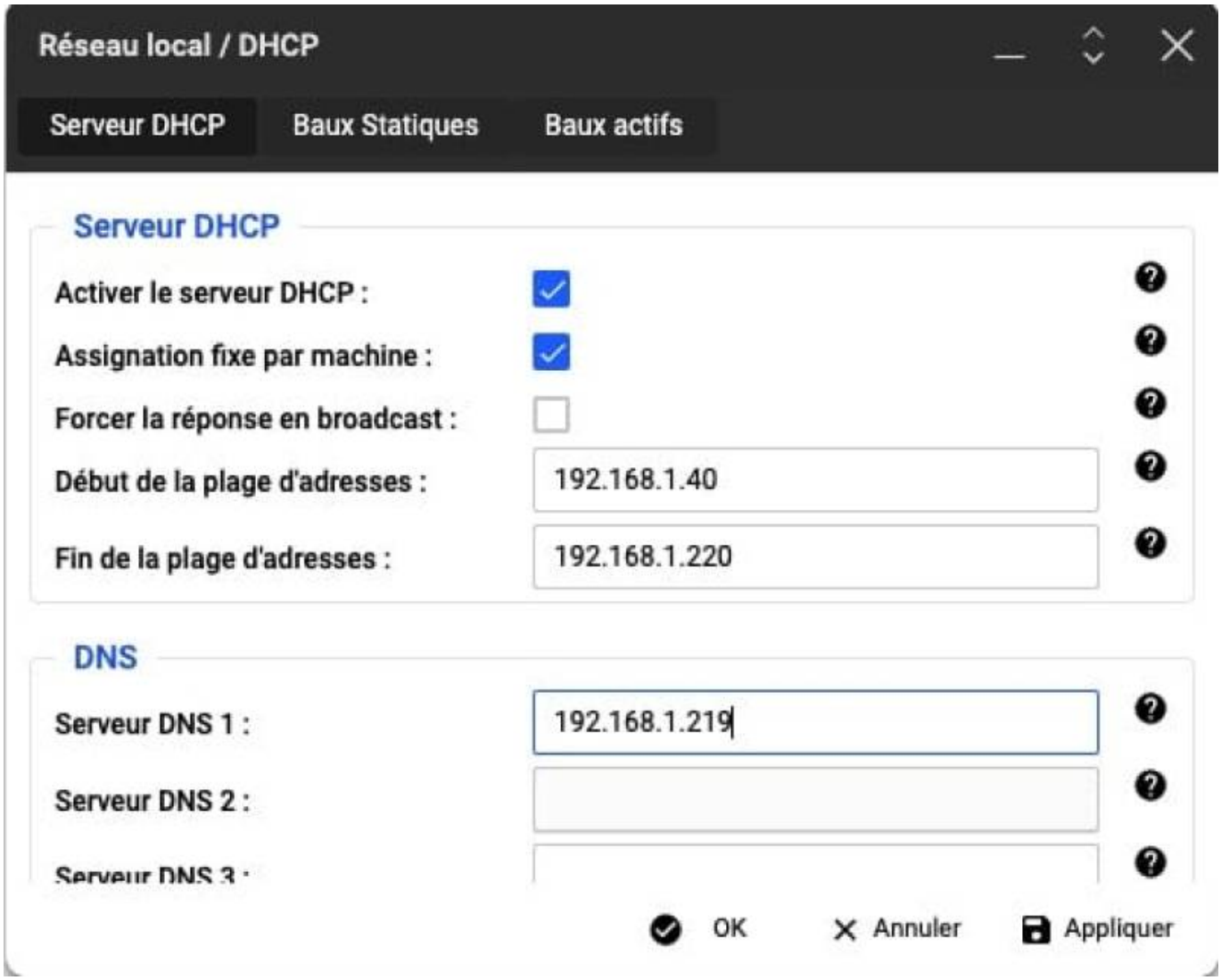
Activer le DHCP sous Windows11

Configurer le DHCP sur un poste Linux Mint

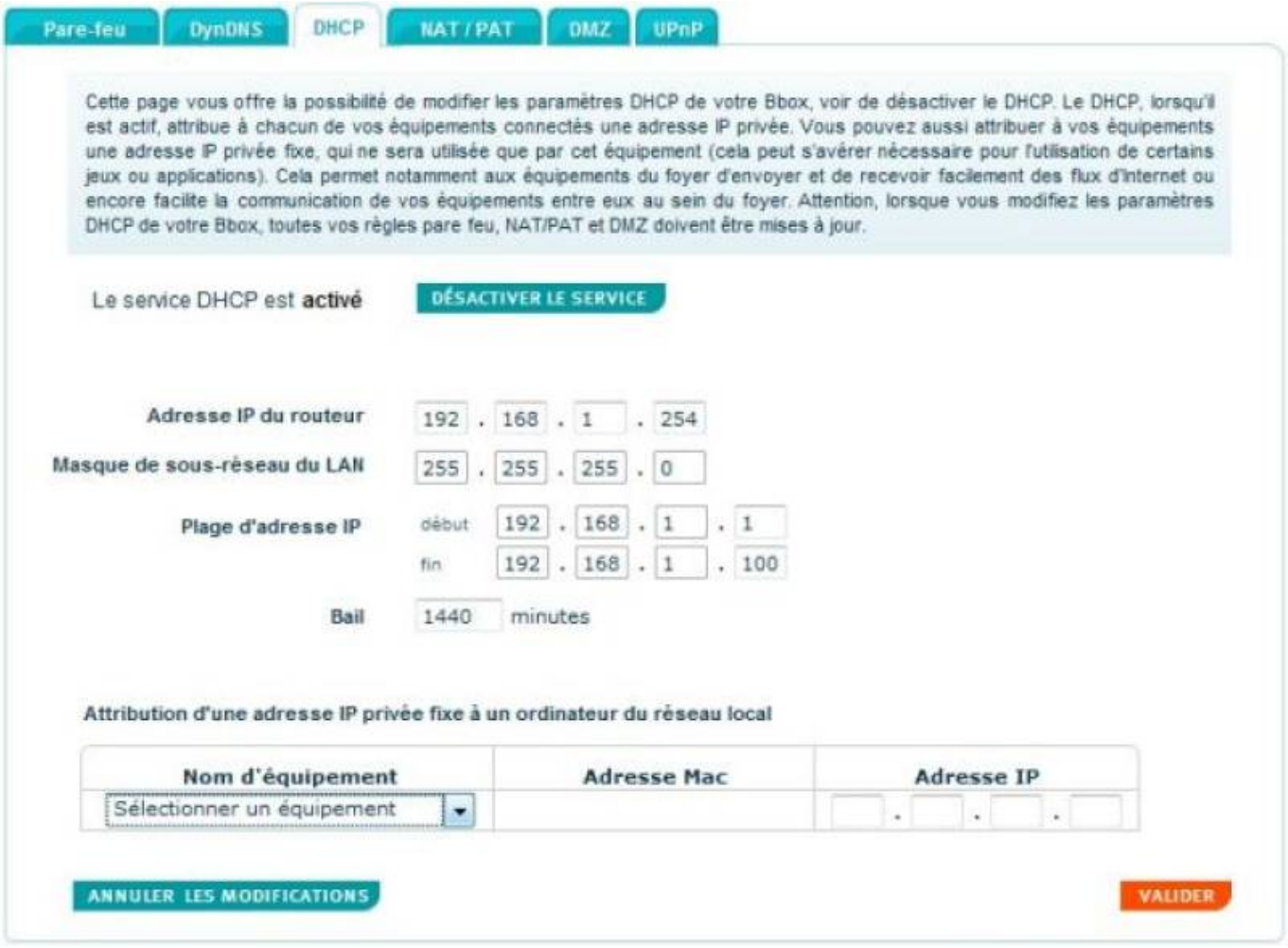
DHCP sur Box Orange



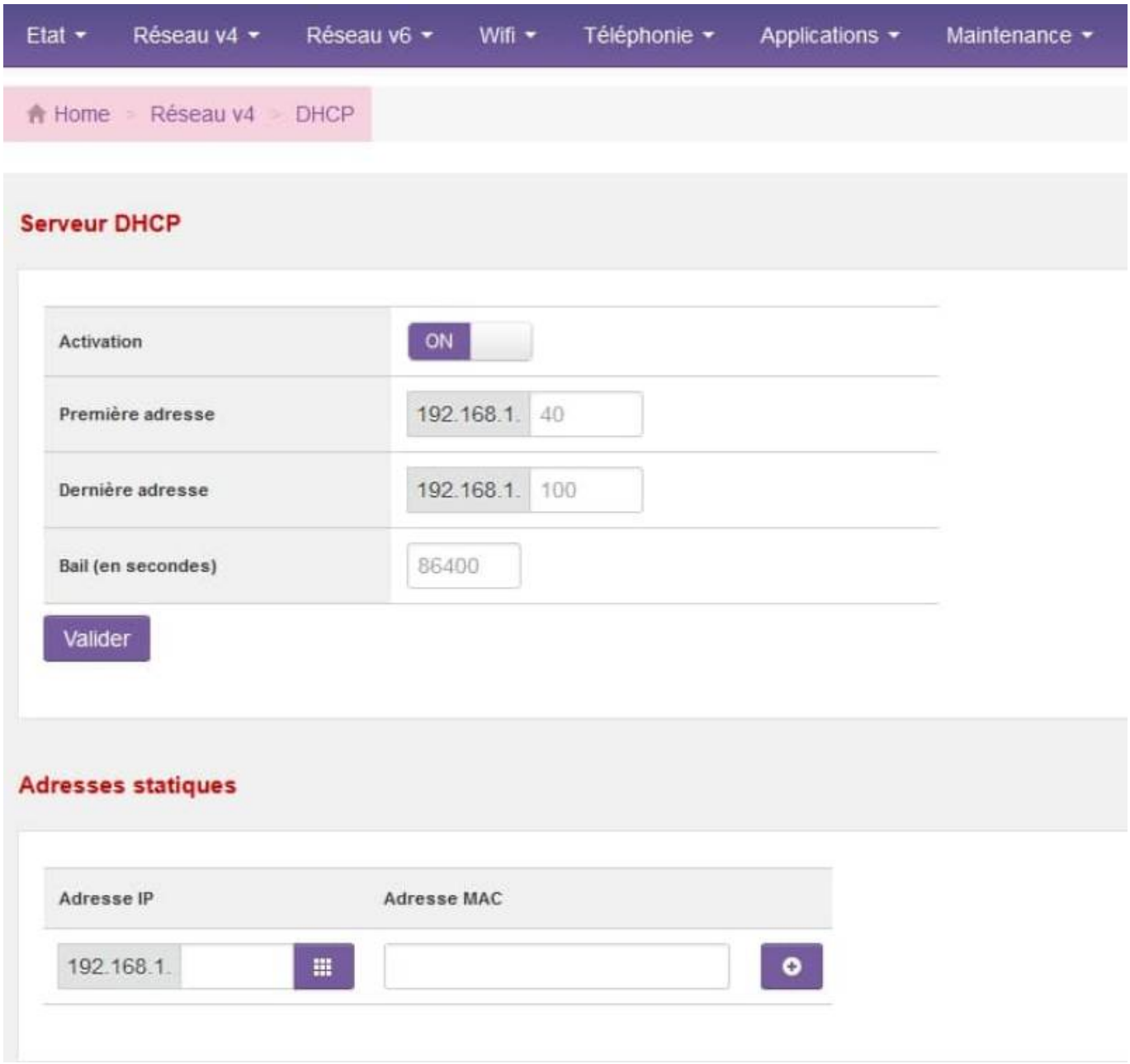
DHCP sur FreeBox



DHCP sur bbox



DHCP sur box SFR



Noms de domaines

Nom de domaine en .fr

Structure d'une adresse internet

Une adresse internet ou nom de domaine est l'équivalent de votre adresse postale sur internet. C'est la manière dont vos contacts et clients vont trouver votre site internet sur le web.

Pour communiquer entre eux, les périphériques reliés à internet sont identifiés par une adresse internet unique, dite adresse IP (Internet Protocol). Cette adresse se présente sous forme d'une suite de chiffres, par exemple : 192.134.4.20. Le nom de domaine permet de traduire en un nom intelligible et facilement mémorisable une adresse IP, et ainsi accéder à un site web (afnic.fr) ou adresser un courrier électronique (support@afnic.fr).

Le nom de domaine est composé d'une chaîne de caractères (nom propre, marque ou association de mots clés) et d'une extension qui indique l'espace de nommage. Il existe plusieurs types d'extensions :

- Des extensions nationales (ccTLD, "Country Code Top Level Domain"), comme le .fr, le .re ou les autres noms de domaine ultramarins gérés par l'Afnic ;
- Des extensions génériques (gTLD, "Generic Top Level Domain") dont les plus connues sont le .com, .net, .info, .biz. Depuis quelques années, de nombreuses nouvelles extensions génériques ont fait leur apparition, comme .paris, .bzh, .alsace, .corsica.

Un nom de domaine est unique dans un espace de nommage (comme le .fr) et attribué au premier qui en fait la demande, s'il satisfait aux conditions d'attribution de l'extension.

Quand choisir son nom de domaine ?

Le nom de domaine profite à la première personne qui en demande la réservation auprès d'un bureau d'enregistrement de nom de domaine aussi appelé registrar. C'est donc la règle du « premier arrivé, premier servi » qui s'applique puisque techniquement, il ne peut y avoir deux noms de domaine identiques.

Toutefois, il vous est fortement recommandé de vérifier préalablement que le nom de domaine ne porte pas atteinte à des droits antérieurs de tiers (travail que les registrars ne font pas). Il est donc essentiel de penser le plus tôt possible à la réservation de son nom de domaine, et idéalement au même moment que l'enregistrement de sa marque.

Nom de domaine Gratuit

La technologie DNS dynamique vous permet de donner votre PC ou un serveur une adresse permanente sur Internet. Les fournisseurs de services Internet changent régulièrement votre adresse IP, mais avec le DNS dynamique, vous pouvez pointer un nom de domaine fixe à l'adresse IP actuelle de votre serveur.

Nom de domaine de troisième niveau (yourname.dynudomain.com) Vous pouvez utiliser le service DNS dynamique avec des noms de domaine de troisième niveau gratuitement.

1. dynu.com , Nom de sous domaine gratuit
2. Dyn6
3. Noip
4. Freedns
5. Cloudns
6. Duckdns

- Nom de domaine de premier niveau (yourname.com)(Non gratuit)

Fournisseurs de nom de domaine (payant)

Liste non exhausive (et totalement subjective):

1. OVH
2. Ionos
3. Gandi
4. Amen
5. Lws
6. Afnic
7. Nordnet
8. Mon domaine
9. ....

Les ports Réseaux

Qu’est-ce qu’un port réseau ?

Un **port réseau** est un numéro (entre **0 et 65535**) utilisé pour identifier un **service ou une application** sur un appareil (ordinateur, serveur, routeur…). Il permet à plusieurs applications d'utiliser la même connexion réseau sans interférer.

Analogie simple

* L’adresse IP = l’adresse d’un immeuble * Le port = le numéro d’un appartement

```
→ On sait à quelle « porte » livrer les données.
```

—

Pourquoi les ports existent-ils ?

Parce qu'un appareil peut avoir **plusieurs applications** utilisant le réseau en même temps :

* Navigateur web * Messagerie * Jeux en ligne * Serveur web * Téléchargements

Les ports permettent de savoir **à quel programme** envoyer les données.

—

Classification des ports

Les ports sont divisés en 3 catégories :

Catégorie	Numéros	Description
——————————-	———	————————————
Ports connus (Well-known)	0 à 1023	Réservés aux services système et protocoles standards
Ports enregistrés (Registered)	1024 à 49151	Utilisés par des applications et services utilisateurs
Ports dynamiques / privés	49152 à 65535	Utilisés temporairement (ex : connexions sortantes)

—

Ports les plus courants (à connaître absolument)

Service	Port	Protocole	Rôle
———	—-	———	——————————-
HTTP	80	TCP	Navigation web non sécurisée
HTTPS	443	TCP	Navigation web sécurisée
FTP	21	TCP	Transfert de fichiers
SSH	22	TCP	Connexion distante sécurisée
DNS	53	UDP/TCP	Résolution des noms de domaine
SMTP	25	TCP	Envoi d’emails
POP3	110	TCP	Récupération d’emails
IMAP	143	TCP	Consultation d’emails
RDP	3389	TCP	Connexion bureau à distance Windows

DHCP	67/68	UDP	Attribution automatique d’adresses IP

—

TCP vs UDP : quelles différences ?

Les ports peuvent utiliser **TCP**, **UDP**, ou les deux.

□ TCP (Transmission Control Protocol)

* Connexion fiable * Contrôle d’erreurs * Reprise des paquets perdus

```
→ Idéal pour : web, emails, SSH, transferts importants.
```

□ UDP (User Datagram Protocol)

* Plus rapide * Pas de contrôle d’erreur * Moins fiable

```
→ Idéal pour : streaming, jeux en ligne, VoIP.
```

—

Comment voir les ports ouverts sur un appareil ?

Sous **Windows**

```sh netstat -ano ```

Sous **Linux**

```sh sudo netstat -tulnp ```

ou

```sh sudo ss -tulnp ```

Sous **macOS**

```sh sudo lsof -i ```

—

Sécurité et ports

Les ports ouverts peuvent représenter une **porte d’entrée pour des attaques**, d’où :

* Filtrage via **pare-feu** * Masquage des ports inutilisés * Utilisation de ports non standards pour des

services sensibles

—

Port forwarding (redirection de port)

Utilisé dans les routeurs pour rendre un service accessible depuis Internet.

Exemple :

* On redirige le **port 80** vers un serveur web interne.

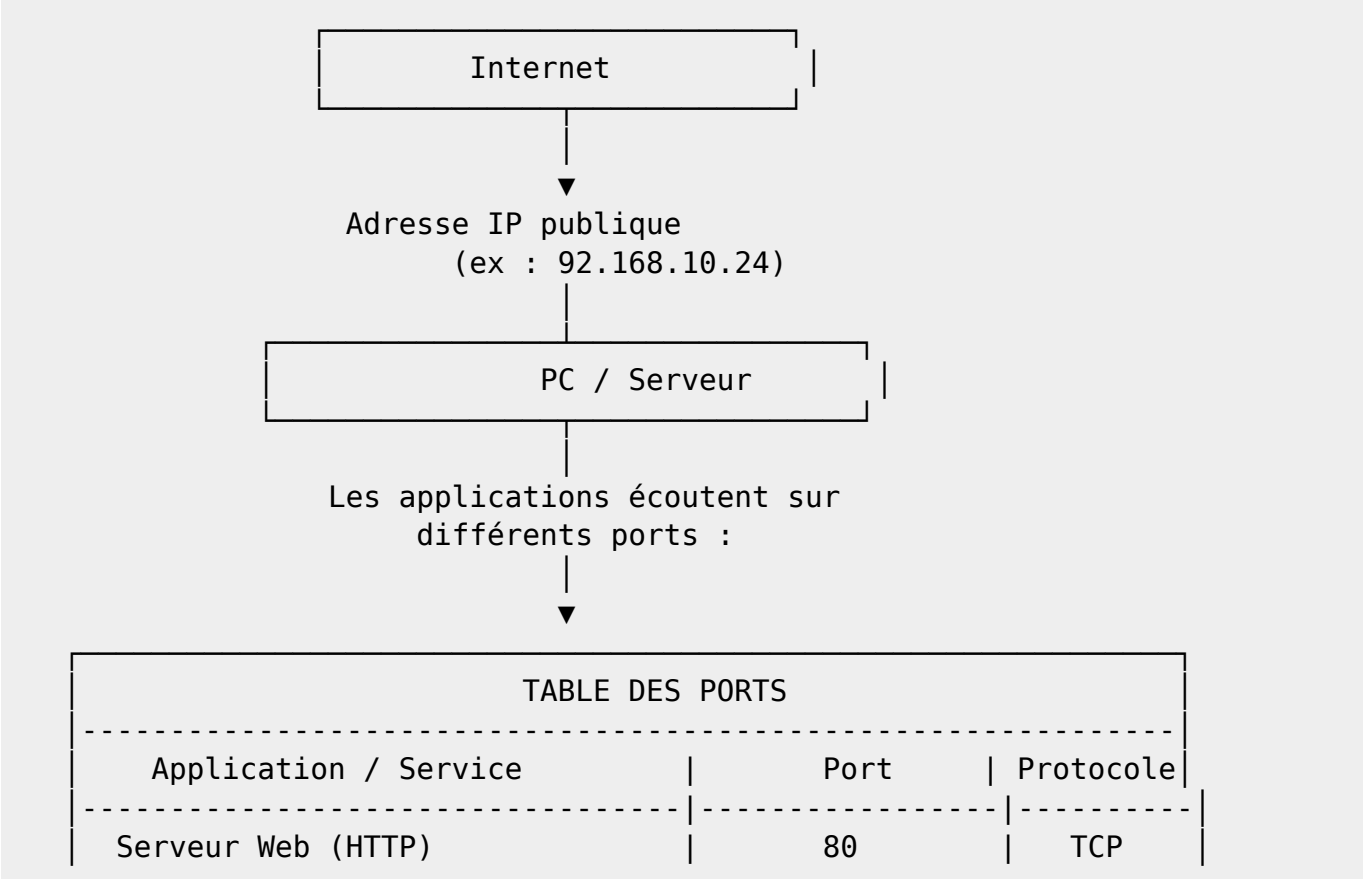
—

Résume simple

- Un port identifie **un service** sur un appareil.
- Il y en a **65 536**.
- Certains sont standardisés (HTTPS 443, SSH 22…).
- TCP et UDP sont les deux types principaux.
- Les ports ouverts doivent être surveillés pour la **sécurité**.

—

Un schema



```
    |  Serveur Web sécurisé (HTTPS)    |      443        |   TCP    |
    |  Connexion distante SSH          |       22        |   TCP    |
    |  DNS                              |       53        | UDP/TCP  |
    |  Jeu en ligne                    |    27015        |   UDP    |
    └──────────────────────────────────────────────────────────────┘
                                  |
                                  ▼
                Les données arrivent sur l'IP
            → le port indique **à quel programme** les envoyer.
```

Les adresses IP IPV4 et IPV6

IPV6

Norme RFC_2460 IPV6 1999 EN

Norme RFC_2460 IPV6 1999 FR

Protocole IPV4

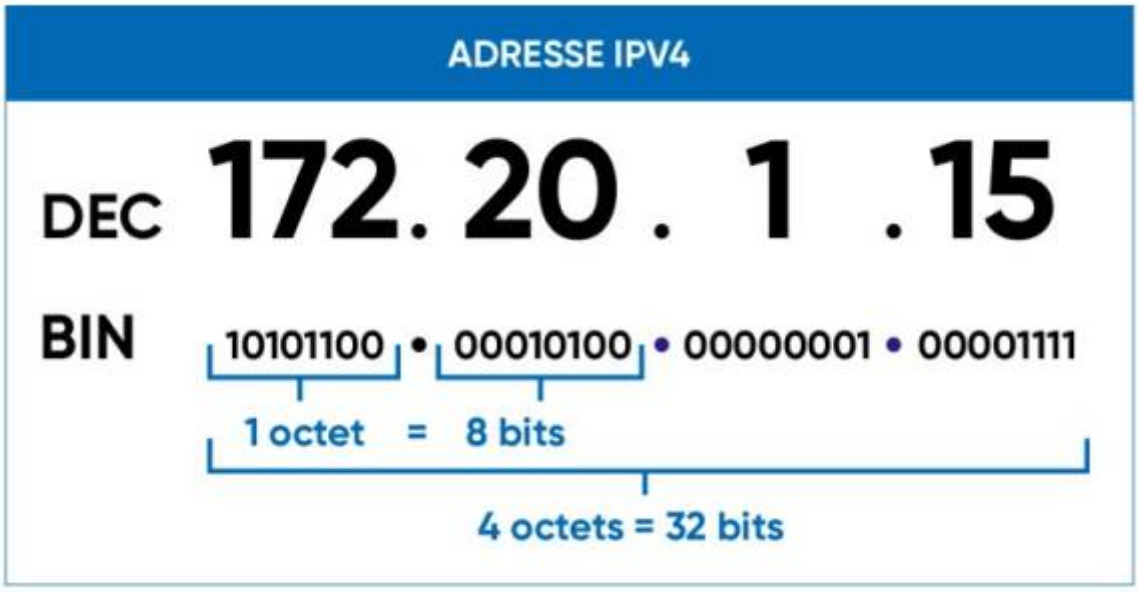
Norme RFC_791 IPV4 1981 EN

Norme RFC_791 IPV4 1981 FR

Adresse IPv4 - Définition

Une adresse IPv4 est une adresse IP dans la version 4 du protocole IP (IPv4). Cette adresse permet d'identifier chaque machine connectée sur un réseau informatique utilisant le protocole IP version 4.

Cette adresse est composée de quatre octets, chacun ayant leur valeur décimale comprise entre 0 et 255, séparés par des points ; exemple : 212.85.150.133.



L'IPv4 est la version la plus couramment utilisée d'adresse IP. Elle est représentée sous la forme de quatre groupes de quatre nombres en base 10 séparés par des points. Une adresse IPv4 est codée sur 4×8 = 32 bits. Une adresse IPv4 peut varier en :

```
  base 10 de 0.0.0.0 à 255.255.255.255 ;
  base 2 de 00000000.00000000.00000000.00000000 à
11111111.11111111.11111111.11111111 .
```

L'IPv4 permet de représenter 232 c'est-à-dire un peu plus de 4,2 milliards d'adresses uniques, mais en raison de l'épuisement des adresses, l'IPv6 a été introduite.

Pourquoi IPv4 reste encore indispensable ?

Même si l'IPv6 est destiné à remplacer l'IPv4, ce dernier demeure extrêmement répandu, notamment en raison :

- de la compatibilité historique,
- d'équipements encore non compatibles IPv6,
- de la facilité d'administration,
- de la présence de solutions contournant le manque d'adresses (NAT, PAT, CIDR…).

Bases sur les réseaux

comprendre-bases-sur-les-reseaux

guidedautodefensenumérique.pdf

Qu’y a-t-il dans ma box ?

Jusqu’à présent nous avons parlé de routeur, de pare-feu, de modem et de box, mais quelle est la différence entre tous ces appareils ? Disons qu’ils ont tous une fonction utile pour faire fonctionner un réseau et lui permettre de communiquer avec d’autres réseaux, en particulier sur internet. Mots clés :

1. Box
2. Modem
3. Routeur
4. Switch
5. Borne d’accès Wi-Fi
6. Pare-feu
7. Serveur

La box, quant à elle est l’élément qui regroupe tous les autres. C’est un appareil inventé par les fournisseurs d’accès pour vous éviter d’avoir quatre ou cinq appareils branchés dans votre salon, tout ca pour accéder à internet et avoir la télé. Une box internet c’est donc une boite dans laquelle il y a : un modem, un routeur, une borne d’accès Wi-Fi, un switch, un pare-feu, un serveur (web, ftp, voip) qui permet d’orchestrer tout ca mais aussi de vous fournir une interface de paramétrage, de mettre votre voix sous forme numérique pour être envoyée sur internet etc… Comme vous le voyez il y a fort à dire sur la box !

Nos box Internet, riches en équipements

Le modem

C’est l’élément le plus important dans l’interconnexion des réseaux et nous n’en avons encore pas parlé ! C’est parce qu’aujourd’hui pratiquement plus personne n’utilise un modem autre que celui intégré à sa box. Modem est un raccourci pour « Modulateur – Démodulateur ». C’est un appareil qui transforme un signal numérique en signal analogique et vice-versa. Pour quoi faire ? Pour le faire voyager pardi ! A la suite des réseaux locaux (LAN) dont les limites géographiques sont visibles à l’œil nu, les modems donnent accès à un monde beaucoup plus vaste : celui des grands réseaux (WAN : Wide Area Network).

Pour connecter deux réseaux, soit vous utilisez un câble si les deux réseaux sont suffisamment proches, soit vous utilisez un autre réseau qui les relie : le réseau téléphonique. Jusqu’à l’avènement de l’ADSL (Asymetric Digital Subscriber Line) les communications utilisaient le Réseau Téléphonique Commuté (RTC). Les communications voix étaient coupées pendant que le modem faisait passer d’horribles sons sur la ligne pour parler à un serveur. Les débits étaient alors de quelques Ko/s. Désormais les technologies DSL permettant non seulement de ne plus monopoliser les lignes téléphoniques mais aussi d’atteindre des débits beaucoup plus importants. Cela est rendu possible par l’utilisation de fréquences très élevées qui voyagent non plus à l’intérieur des fils du téléphone mais à leur périphérie. Il y a donc plusieurs signaux qui voyagent sur le réseau téléphonique, un peu comme dans les réseau CPL.

Par conséquent, le modem est une interface entre votre box et votre réseau téléphonique.

Le routeur

Comme nous l'avons vu précédemment, pour interconnecter deux réseaux il faut un routeur qui est connecté sur deux réseaux en même temps et qui fait passer les communications de l'un à l'autre. Dans votre box, le routeur reçoit les données qui sont transmises sur votre réseau et pour lesquelles personne ne se reconnaît comme destinataire et les donne au modem qui les transforme en signaux analogiques à destination du réseau internet.

Le switch

Celui-ci permet de mettre tous les ordinateurs d'un réseau ensemble afin qu'ils s'envoient des données. Il est lié à la norme Ethernet (voir la fiche sur les réseaux). Le routeur est bien entendu branché sur le switch car c'est un élément du réseau.

La borne d'accès Wi-Fi

En Wi-fi vous n'êtes pas connecté physiquement au réseau, mais il faut bien qu'un élément fasse la liaison entre votre ordinateur et le routeur. C'est le rôle de la borne d'accès qui est elle-même reliée au switch et qui capte toutes les communications qui circulent dans les airs, les filtre afin de vérifier qu'elle est bien concernée et les met sur le réseau via le switch. Il va de soi que la borne d'accès elle-même doit disposer d'une interface du type modem pour transformer les informations numériques en signaux radio-électriques à envoyer dans les airs.

Le pare-feu

C'est un élément dont la fonction n'est pas indispensable au fonctionnement du réseau. Sans lui les communications se font normalement et il n'apporte aucun gain en performances. Son rôle est simplement de filtrer les communications qui viennent de l'extérieur de votre réseau (d'internet donc) et vérifier qu'il peut laisser entrer les données. Nous verrons dans un autre chapitre comment un pare-feu s'y prend pour protéger votre réseau.

Le serveur

C'est le chef d'orchestre de votre box. C'est un ordinateur qui possède un système d'exploitation (basé sur un noyau Linux dans la plupart des cas) et des logiciels développés pour partie par votre fournisseur d'accès. Les services les plus couramment installés sur ce serveur sont :

1. **Un serveur web** pour la configuration de tous les éléments cités ci-dessus ainsi que pour des informations de diagnostic ou plus simplement pour vous permettre d'effectuer la mise à jour de votre box.
2. **Un serveur DHCP** qui vous permet de ne faire pratiquement aucune configuration sur votre ordinateur lorsque vous le connectez au réseau. C'est lui qui fournira automatiquement à votre ordinateur une adresse IP afin qu'il puisse communiquer avec les autres ordinateurs possédant

une adresse IP dont, bien évidemment la box elle-même (le routeur).

3. **Un serveur de VoIP** dont le rôle est de transformer votre voix qui passe à travers le micro du téléphone en signaux numériques qui seront à nouveau transformés en signaux analogiques et transmis à un autre serveur qui se chargera d'acheminer votre voix à votre interlocuteur… et vice-versa. Il vous donne aussi un certain nombre d'autres fonctionnalités qui dépendent de votre fournisseur d'accès.