NetPractice

I. Introduction :

Ce projet à pour but de nous faire découvrir le **réseau** par des cas pratiques. Nous allons devoir **configurer des réseaux de petite taille.** Plus précisément, qu'il faudra **résoudre des problèmes liés à la mise en place d'un réseau fonctionnel.** Pour ce faire, il faudra comprendre le **fonctionnement des adresses avec le protocole TCP/IP.** Au cours de ce projet, nous allons devoir effectuer 10 exercices de 10 niveaux de difficulté. Dans le cadre de ce projet, il s'agit, bien évidemment, de réaliser des **réseaux fictifs** qui seront **disponibles dans une interface d'entraînement accessible par un navigateur web.**

II. Projet :

1. Première Étape - Connexion :

Dans un premier temps il faudra :

- Télécharger le fichier attaché au projet ;
- Extraire les fichiers dans un dossier au choix ;
- Exécuter le fichier “index.html” qui devrait ouvrir l’interface suivant dans un navigateur web :

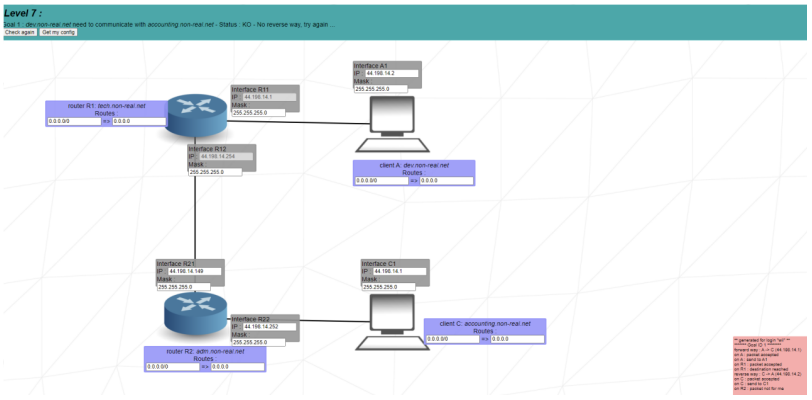
- Entrer votre login 42 dans le champ présent sur la page (ou utiliser la version “correction” en laissant le champ vide dans le cadre d’une évaluation).

2. Deuxième Étape - Exercices/Niveaux :

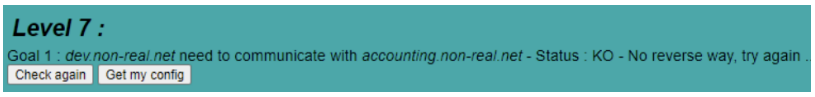
1. Représentation :

Les 10 exercices/niveaux se présenteront sous la forme suivant :

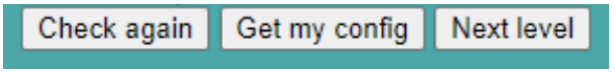
- Un **schéma réseau qui ne marche** pas du type :



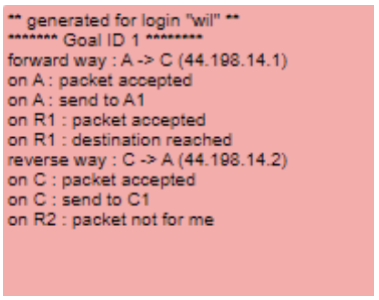
- **En haut de la fenêtre se trouve le but à atteindre pour rendre ce réseau fonctionnel**. Juste en dessous **deux boutons** sont à mis à notre disposition : **“Check again”** qui permet de voir si votre essai est correct ou non et **“Get my config”** qui permet de télécharger votre configuration à tout moment (ce qui sera utile tout au long des exercices/niveaux) :



- **Lorsqu'un exercice/niveau est réussi**, un **nouveau bouton** apparaît à la suite des boutons précédemment mentionnés : "**Next level**." Il suffit alors de cliquer sur celui-ci afin d'accéder au niveau suivant. Avant de passer au niveau, il faudra veiller à exporter la configuration de celui que nous venons de valider avec le bouton "Get my configuration", mentionné précédemment, afin de le mettre dans le dépôt git. Ex :

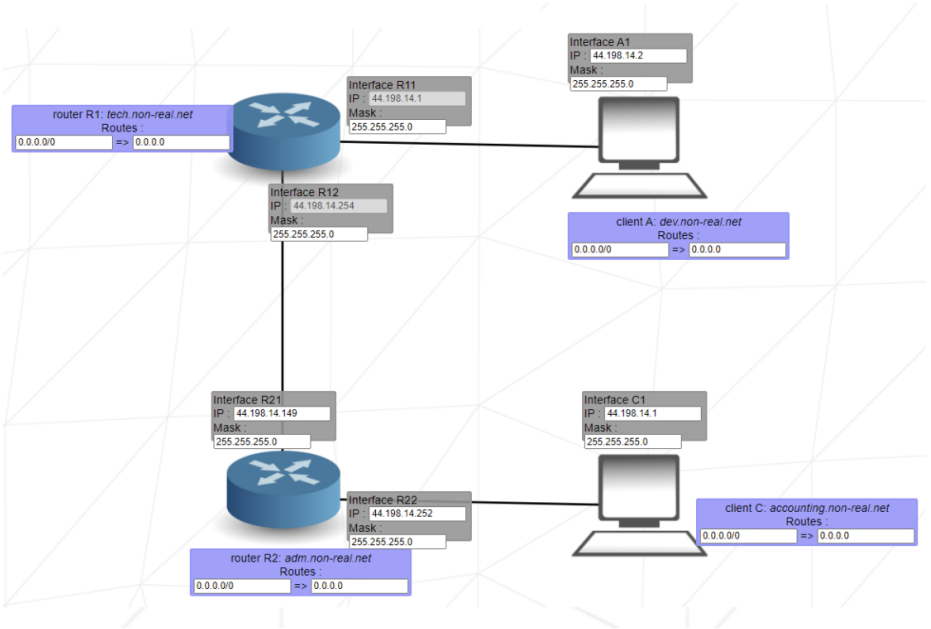


- **En bas, à droite de l'écran,** se trouve un **petite journal de log** qui aidera à comprendre pourquoi le but n'est pas atteint en cas de configuration incorrecte. Ex :



2. <u>Exemple :</u>

Le but de l'exemple ci-dessous et de modifier les champs non grisés afin de faire fonctionner la configuration représentée. Pour réussir ce projet, il faudra préalablement comprendre le **fonctionnement des adresses IP dans un réseau**, **avec un routeur ou une autre périphérique**, ainsi que tout ce qui est en lien avec le **fonctionnement de l'adressage TCP/IP.**



3. Troisième Étape - Rendu et Peer-evaluation :

   Une fois les 10 exercices/niveaux réalisés il faudra rendre nos configurations téléchargées tout au long dans un dépôt Git. Seul le travail présent sur le dépôt sera évalué en soutenance. Ainsi, il faudra bien vérifier les noms des dossiers et des fichiers du dépôt afin que ces derniers soient conformes aux demandes du sujet.

   Puisque 10 exercices/niveaux sont disponibles pour l'entraînement, il faudra rendre **10 fichiers à la racine du dépôt Git** (soit un fichier par excercices/niveaux). Pour ce faire, il faudra veiller à rentrer le bot login 42 dans l'interface d'entraînement et **exporter un fichier par niveaux en utilisant "Get my config."**

   Attention, durant la soutenance, il faudra valider trois exercices/niveaux aléatoires supplémentaires (comme indiqué dans l'interface d'entraînement). Bien entendu un **temps limité** sera accordé pour réaliser ces trois exercices/niveaux.

III. Notions :

1. Fonctionnement des Adresses IP :

A. Qu'est-ce qu'une adresse IP ?

Une adresse IP permet d'**identifier chaque équipement connecté) un réseau informatique** utilisant le **protocole IP** ("Internet Protocole"). Elle permet à l'équipement de **communiquer sur le réseau** auquel il est connecté.

Les adresses IP permettent également de c**ommuniquer entre des équipements qui sont sur des réseaux différents** grâce à la notion de "routeur." Le **routeur** va permettre, à son tour, de **faire le lien entre ces différents réseaux.**

De fait, **tout ce qui est connecté à un réseau IP à besoin d'une adresse IP pour communiquer avec le réseau** et communiquer avec Internet accessoirement.

Ci-dessous on trouve quelques exemples concrets :

- Un PC connecté en Wi-Fi sur la Box d'un domicile ;
- Une Smart TV connecté en câble sur la Box d'un domicile;
- Un smartphone connecté en Wi-Fi chez McDo';
- Un serveur connecté à un réseau d'entreprise;
- Etc.

B. Adresses IPv4 et IPv6 :

Il existe deux types d'adresse IP, les **adresse IPv4** (pour version 4), avec les caractéristiques suivantes :

- **Notation décimale avec 4 valeurs comprises entre 0 et 255, séparées par des points** ;
- Longueur de **32 bits**, c'est-à-dire **4 octets** ;
- **Notation la plus utilisée** à ce jour ;
- Exemple : **192.168.1.10** .

Les adresse IPv6 (pour version 6), avec les caractéristiques suivantes :

- **Notation hexadécimale avec 8 valeurs séparées par des ":"** ;
- Longueur de **128 bits**, c'est-à-dire **16 octet** (il existe ainsi, rien qu'à la notation, beaucoup plus d'adresses IPv6 que de version 4);
- Notation la moins utilisée mais qui r**emplacera dans les temps les adresses IPv4 (**celles-ci ont été créées afin de résoudre la pénurie d'adresses IPv4 qui ont atteint leurs limites depuis bien longtemps) ;
- Exemple : **1897:0c02:0000:84c2:0000:0000:cf2a:9077** .

C. Historique - Les Classes d'Adresses IPv4 :

Chaque adresse IP appartient à une classe qui correspond à une plage d'adresse IP. Il existe 5 classes différentes :

- La **classe A** de l'adresse IP 0.0.0.0 à 126.255.255.255 ;
- La **classe B** de l'adresse IP 128.0.0.0 à 191.255.255.255 ;
- La **classe C** de l'adresse IP 192.0.0.0 à 223.255.255.255 ;
- La **classe D** de l'adresse IP 224.0.0.0 à 239.255.255.255 ;
- La **classe E** de l'adresse IP 250.0.0.0 à 255.255.255.255.

Les c**lasses A, B et C sont privées et publiques**. La **classe D**, quant à elle, est **réservée pour le multicast** que l'on appelle également **multidiffusion,** ou **adresse de broadcast** (permet de diffuser un flux réseau à partir d'un serveur ou un PC un ensemble d'autres qui sont connectés au réseau et qui sont dits "abonnés" à ce flux). Enfin, la **classe E** est **réservée aux tests l'IUTF** ("Intelligent Use Task Force").

L'**adresse réseau** sera toujours la **première** adresse d'un réseau et l'**adresse broadcast** toujours la **dernière**. Par exemple pour une adresse de classe A :

- Son adresse réseau sera toujours 10.10.10.0 ;
- Et son adresse broadcast sera toujours 10.10.10.255.

D. Adresses IP Publiques et Privées :

a. Adresses IP Privées :

Les **adresses IP privées** sont les adresses IP que l'on peut u**tiliser pour les équipements sur un réseau local**. Une adresse IP privée ne peut pas être utilisée sur Internet, comme pour un site Web, car elles ne sont pas rouvertes sur Internet. Les adresses IP privées sont trouvée dans le réseau d'une entreprise, au niveau du réseau domestique

Le **choix d'une adresse réseau s'effectue en fonction de l'usage,** du besoin, et du nombre de PC serveur, de smartphones, de tablettes, **du nombre d'équipements qui ont besoin d'être connectés simultanément sur le réseau.** Ces adresses peuvent être **réutilisées plusieurs fois car elles sont contenues au niveau de réseau local**. De fait, les adresses IP privées, au sein d'une maison par exemple, ne sont **pas accessibles sur Internet**, elles sont privées.

Les adresses IP privées sont **retrouvées dans les classes A, B et C** : elles représentent, respectivement, **la moitié** de la classe A, la moitié de la classe B et la moitié de la classe C. Les **autres moitiées représentent les adresses IP publiques.** Par exemple, les adresses privées :

- De la classe A sont comprises entre 10.0.0.0 et 10.255.255.255 ;
- De la classe B sont comprises entre 172.16.0.0 et 172.32.255.255 ;
- De la classe C sont comprises entre 192.168.1.0 et 192.168.255.244.

b. Adresses IP publiques :

Les adresses IP publiques, à l'inverse, sont utilisées exclusivement sur Internet (comme sur une Box Internet, un site Web, etc). Une adresse IP publique est unique dans la montre, contrairement à une adresse IP privée. C'est notamment cette spécificité qui crée la pénurie d'adresse IPv4, malgré la présence de 4 294 967 296 adresses IP différentes. Par exemple, les adresses publiques :

- De la classe A sont toutes sauf 10.0.0.0 et 10.255.255.255 ;
- De la classe B ssont toutes sauf 172.16.0.0 et 172.32.255.255 ;
- De la classe C sont toutes sauf 192.168.1.0 et 192.168.255.244.

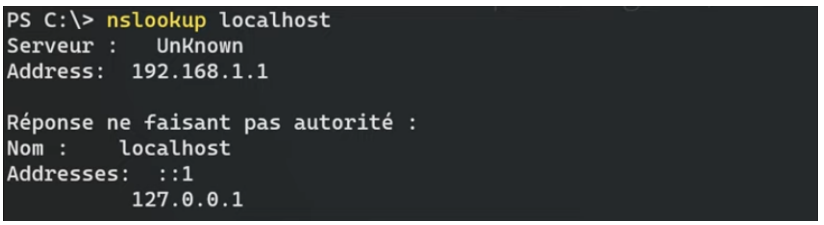
c. Exceptions :

Attention, il existe **2 exceptions** :

- Le **réseau 127.0.0.0** est réservé pour la **boucle locale** ;
- Le **réseau 0.0.0.0** est réservé pour **définir une route par défaut sur un routeur** (on dit au routeur que pour joindre tous les réseaux il doit passer par telle route).

d. Exemple :

Prenons l'exemple suivant :



Si on fait un "nslookup localhost" sur une machine, c'est-à-dire qu'on va demander au PC de résoudre le nom "localhost" pour retrouver l'adresse IP qui est associée, le compilateur retournera 2 adresses :

- L'adresse : ::1, qui est l'adresse de boucle locale en IPv6;
- L'adresse : 127.0.0.1, qui est l'adresse local de la machine, appelée la boucle locale. De fait, chaque machine, Windows, Linux ou bien MacOS, possède une adresse IP locale qui, sur n'importe quelle machine, est configurée par défaut.

E. CIDR - Classless InterDomain Routing :

a. Explications :

Internet est tellement énorme qu'il n'y a pas assez d'adresses IPv4, choses que l'on sait depuis les **années 90**. C'est à cette période là qu'est **intervenu le CIDR pour augmenter le nombre d'adresses IPv4 disponibles et éviter le gaspillage.**

Le CIDR introduit la **notion de sous-réseaux à travers le masque de sous-réseau**. Ce masque de sous-réseau va se **définir** non pas par sa valeur par défaut mais **en fonction du nombre d'hôtes à connecter.** Comme l'adresse IPv4, la **notation du masque sous-réseau** s'établit sur **4 octets** et la **valeur maximale est 255.255.255.255**. La **notation CIDR** s'effectue sous la forme **/<nombre-de-bits-pour-le- sous-raison>**, soit :

- Pour un masque 255.0.0.0, la notion CIDR est : /8;
- Pour un masque 255.255.254.0 , la notion CIDR est : /23;
- Pour un masque 255.255.255.0 , la notion CIDR est : /24.
-

Puisqu'il **détermine la limite entre la partie réseau et la partie hôte** dans le découpage de l'adresse IPv4.

b. Exemple :

Prenons l'exemple d'un réseau "10.10.10.0/24", c'est-à-dire le masque de sous-réseau "255.255.255.0." La notation CIDR, "/24", donne le nombre de bits à "1" d'où l'intérêt d'écrire le masque en bits pour bien comprendre. Puisque qu'un octet est égal à 8 bits, cela donne : 11111111.11111111.111111111.00000000. Il reste 8 bits à "0" à la fin donc ce réseau dispose de "2 puissance 8" adresses IP pour les hôtes, soit 254 adresses.

En effet, le réseau ne dispose pas de 256 adresses IPv4, comme le suggère le calcul "2 puissance 8", mais 256 - 2, soit 254 adresses IP. Cela est dû au fait que **2 adresses IPv4 sont automatiquement réservées**, et donc, non disponibles :

- L'**adresse réseau**, utilisée pour identifier le réseau (qui est toujours la première adresse, soit 10.10.10.0) ;
- L'**adresse de diffusion**, également appelée **adresse de broadcast**, pour la transmission de paquets à l'ensemble du réseau (qui est toujours la dernière, soit 10.10.10.255);
- Les machines connectées à ce réseau pourront donc avoir les adresses IP de 10.10.10.1 à 10.10.10.254 (classe A).

Il existe des calculateurs en ligne pour aider à trouver la bonne adresse de réseau et le bon masque de sous-réseau en fonction du nombre d'adresses IP dont on a besoin.

2. Calcul de Masque de Sous-Réseau :

   A. Pourquoi utiliser des calculs de masque de sous-réseau ?

      En faisant un calcul de masque de sous-réseau on va pouvoir **déterminer plusieurs informations** comme l'**adresse réseau** et l'**adresse broadcast** mais aussi déterminer **un ou plusieurs sous réseau du nombre d'équipement que l'on a à connecter à l'intérieur.**

      Par exemple, si on a besoin de connecter sur un réseau 50 machines au maximum, quel est l'intérêt d'avoir un réseau où on peut potentiellement connecter plus que 250.

      Ainsi, grâce aux calculs de masque de sous-réseau on va pouvoir déterminer des sous-réseaux au sein de son réseau local et donc de le segmenter. C'est-à-dire imaginer l'architecture de ce dernier pour ensuite suivre les bonnes pratiques et créer différents réseaux logiques. Par exemple, isoler les serveurs des imprimantes et des postes de travail.

      En bref, une adresse IP sans masque de sous-réseau n'a pas de sens.

   B. FLSM vs VLSM :

      Il existe **2 méthodes**, 2 manières de faire, de calcul de masque de sous-réseau:

      - La **méthode FLSM**, pour "Fixed Length Subnet Mask", est un **masque de sous-réseau fixe**. Dans ce cas, on va répondre le masque que l'on peut retrouver au sein des classes d'adresses IP.Une adresse IP de classe A, donc en 10.quelques-choses l'adresse fixe sera 255.0.0.0 ou alors un /8. Pour une adresse de classe B se sera 255.255.0.0 ou alors un /16. Et pour une adresse IP de classe C, se sera 255.255.255.0 ou alors un /24.
      - La **méthode VSL**, pour "Variable Length Subnet Mask", est une méthode qui s'appuie sur des **masques de sous-réseau à longueur variable**. De fait, il faut découper précisément son réseau en fonction de besoins réels. C'est justement cette méthode qui permet de découper précisément un réseau en plusieurs sous-réseaux, puisque qu'on va poser un masque qui répond aux besoins.

C. Qu’est-ce qu’un masque de sous-réseau ?

Un **masque de sous-réseau** est **la limite entre la partie réseau et la partie hôte**. Ses caractéristiques sont les suivantes :

- **Notation décimale** : 255.255.255, 255.0.0.0, 255.255.240.8, etc. ;
- **Notation CIDR** : /8, /16, /22, /24, etc. La notation CIDR d’un masque de sous-réseau est la **norme d’aujourd’hui** et **commence à /0,** pour 0.0.0.0, **et se termine à /32**, pour 255.255.255.255.

Par exemple, le masque de sous-réseau sur l’adresse IPv4 suivant 192.168.1.1/24, vient préciser un masque. C’est grâce à cette information combinée à l’adresse IP qui la précède que l’on va pouvoir ensuite déterminer la partie réseau et la partie hôte. Ainsi, on détermine tout un tas d'informations.

D. Calculer l’adresse IP d’un réseau à partir de son masque de sous-réseau :

a. Introduction :

Adresse IPv4	Bits
192.168.1.1/24	**24**
Problématique	L’adresse de sous-réseau /24 (ou 255.255.255.0) indique qu’**il y a 24 bits utiliser pour définir le réseau en lui-même**. Une indication importante, mais **comment l’interpréter** ?
Hypothèse	Un octet est égal à 8 bits, donc on peut déterminer que **les 3 octets (soit 24 bits) sont utilisés pour définir le réseau** de notre adresse IPv4. L**e dernier quatrième octet (soit 8 bits) sera utilisé pour la partie hôte.**
Conclusion	Le fait de connaître l’adresse IP que l’on utilise va nous permettre de savoir combien de machines on peut connecter sur le réseau en même temps.

b. Première étape - Traduire l'adresse IP en binaire :

Adresse IPv4	Bits
192.168.1.0/24	**24**
Problématique	**Comment calculer l'adresse d'un réseau qui contient l'adresse IPv5 ci-dessus ?**
Objectif	Convertir la valeur décimale en valeur binaire, c'est-à-dire de la base 10 vers la base 2.

Application sur le premier octet							
128	64	32	16	8	4	2	1
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
1	1	0	0	0	0	0	0
Remarques	Notre tableau est vide, nous allons le remplir pour chaque bit en indiquant 0 ou 1. Commençons par la valeur 192 : 128 + 64 = 192. Ainsi, 192 en binaire s'écrit 11000000.						

Application sur tous les octets								
	128	64	32	16	8	4	2	1
	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
192	1	1	0	0	0	0	0	0
168	1	0	1	0	1	0	0	0
1	0	0	0	0	0	0	0	1
0	0	0	0	0	0	0	0	0
Remarques	Ainsi, l'adresse IPv4 192.168.1.1, en binaire, s'écrit : 11000000.10100000.00000001.00000000							

c. Deuxième étape - Traduire le masque de sous-réseau en binaire :

Application sur tous les octets								
	128	64	32	16	8	4	2	1
	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
255	1	1	1	1	1	1	1	1
255	1	1	1	1	1	1	1	1
255	1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0	0
Remarques			Ainsi, le masque de sous-réseau /24 ou 255.255.255.0 , en binaire, s'écrit : 11111111.11111111.11111111..00000000					

d. Troisième étape - Déterminer l'adresse du réseau IP :

	1er Octet	2ème Octet	3ème Octet	4ème Octet
Adresse IPv4 binaire	11000000	10101000	00000001	00000000
Masque de sous-réseau binaire	11111111	11111111	11111111	00000000
Adresse IP du réseau	11000000	10101000	00000001	00000000

e. Quatrième étape - Convertir la valeur binaire de l'adresse IP du réseau :

Adresse IPv4 et masque de sous-réseau	192.168.1.0/24
Valeur binaire de l'adresse IPv4	11000000.10100000.00000001.00000000
Valeur binaire du masque de sous réseau	11111111.11111111.11111111..00000000
Valeur binaire de l'adresse IP du réseau	11000000.10101000.00000001.00000000
Valeur décimale de l'adresse IP du réseau	192.168.1.0 (soit l'adresse IPv4 de base)

f. Conclusion :

L'adresse 192.168.1.0\24 fait partie du réseau 192.168.1.0. Ainsi grâce à ce calcul on a pu déterminer l'adresse IP de notre réseau.

E.

3.