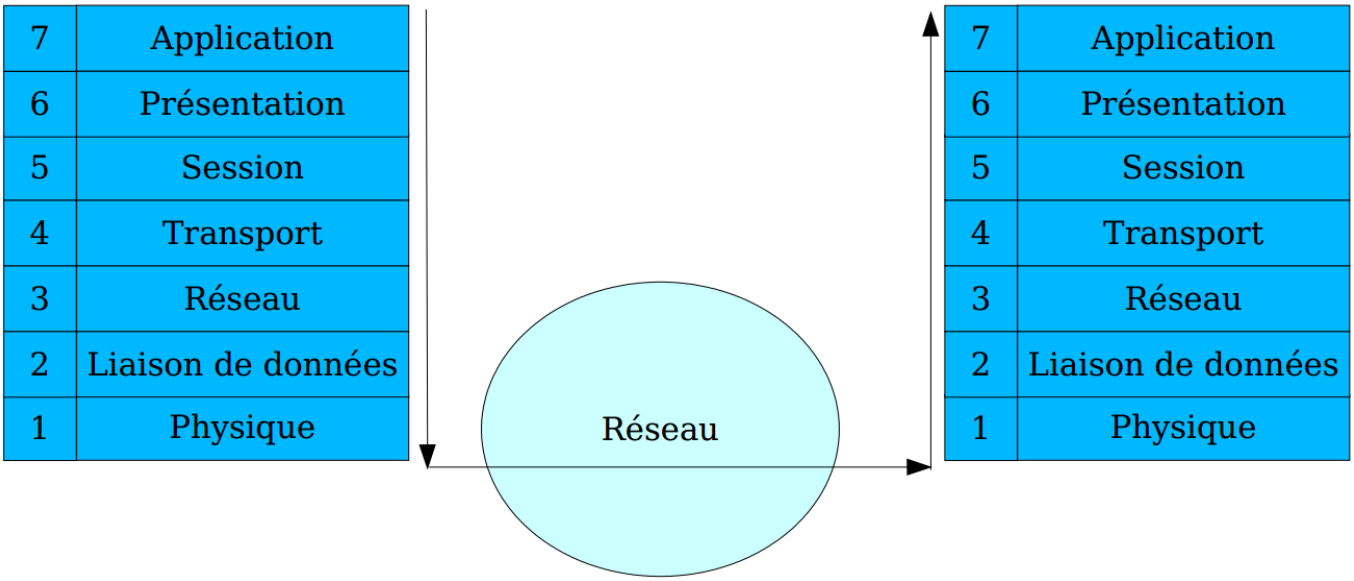
UVSQ ISTY	SNPI – Réseau 3
	TP1

Petit rappel :

Communication d'une application à une autre via le réseau



A) Le câble réseau

Objectif : Nous étudions la couche 1 du modèle OSI et le câble est le support de transmission le plus usité.

Les normes EIA/TIA (Electronic Industries Association / Telephony IndustriesAssociation) définissent des catégories de câbles en fonction de leur atténuation et affaiblissement paradiaphonie

Il existe 6 catégories qui normalisent le connecteur, la bande passante du câble et le nombre max. de paires pouvant être utilisées :

cat 1 : téléphone traditionnel (voix)
cat 2 : transmission des données 4Mbit/s (RNIS) [4 paires torsadées]
cat 3 : 10 Mbit/s max. [4 paires torsadées et de 3 torsions par pied]
cat 4 : 16 Mbit/s max. [4 paires torsadées en cuivre]
cat 5 : 100 Mbit/s max. [4 paires torsadées en cuivre]
cat 5e : 1 Gbit/s max sur 100m, utilisation des 4 paires torsadées des câbles en classe D
cat 6 : 2.5 Gbit/s sur 100m, 10 Gbit/s sur 25m pouvant aller jusque 100m en changeant le type de codage du protocole utilisé
cat 6a : jusqu'à 10Gb/s
cat 7 : Il existe encore des problèmes avec les connecteurs. Les connecteurs validés sont en cuivre.

Q1. **Regardez** sur le câble Ethernet connecté sur votre PC, quelle est sa catégorie et donc, sa vitesse de transfert maximale.

Q2. **Recherchez** les significations de conducteurs **multibrins** et **monobrins.** Décrivez-les et donnez les avantages de chacun d'eux.

Q3. **Explicitez** les désignations des différents types de câbles comme les câbles U/UTP, F/UTP, SF/UTP et S/FTP. Donnez le prix pour 100 mètres (prix sur le site de votre choix) et leurs particularités. Donnez les distances maximales admissibles et la section des conducteurs. Si vous voyez d'autres types de blindage, n'hésitez pas….

B) La fibre optique

Utilisation de la FO :

- Liaison entre répartiteur (backbone), centraux téléphoniques urbains et interurbains
- Couplage de segments dans une ville, entre deux villes, entre les continents

Avantages

- Légèreté
- Immunité au bruit
- Isolation galvanique parfaite
- Faible atténuation
- Tolère des débits de l'ordre de 100Mbps
- Largeur de bande de quelques dizaines de mégahertz à plusieurs gigahertz (fibre monomode)
- Sécurité (difficile à mettre sur écoute)

Inconvénients

- Peu pratique dans des réseaux locaux (installation difficile)
- Coût relativement élevé
- Relative fragilité
- Distributeur central de la fibre optique

Constitution de FO (Fibre Optique):

Une fibre optique est composée de 3 éléments principaux :

- Le cœur dans lequel se propagent les ondes optiques
- La gaine optique d'indice de réfraction inférieur à celui du cœur, qui confie les ondes optiques dans le cœur
- Le revêtement de protection qui assure la protection mécanique de la fibre

Les fibres (appelées brins au sein d'un câble) sont regroupées dans des câbles par multiples de 2, de 8 ou de 12.

La qualité d'une fibre optique est caractérisée par 2 valeurs :

- Bande passante exprimée en MHz.km
- Affaiblissement linéique exprimé en dB/km

La transmission des données s'effectue par modulation numérique de la puissance optique de l'onde émise à une longueur donnée.

Il existe 2 types de fibres optiques : la **fibre multimode** et la **fibre monomode**.

Q4. **Donnez** le principe de fonctionnement des 2 types de FO (monomode et multimode), leurs avantages, leurs utilisations et donnez des valeurs physiques (taille du cœur, taille de la gaine, longueur d'onde, distances)

Activités sur l'ordinateur :

Partie 1 : Relever les informations suivantes

1.1°) Combien de cartes réseau sont installées sur votre ordinateur ? Donnez leur(s) nom(s), leur(s) fabricant(s) ? Est-ce des cartes réseaux filaire ou sans fil ?

1.2°) Que signifie le cadenas sur l'icône de la carte réseau ?

1.3°) Quel message avez-vous quand le câble est débranché ?

1.4°) Indiquez les informations quand vous placez votre souris sur l'icône réseau (en bas à droite) ?

1.5°) Lancez l'invite de commande (*menu Démarrer ≻ Tous les programmes ≻ Accessoires ≻ Invite de commande*). Tapez « net user ». Combien y-a-t-il de compte utilisateur pour votre ordinateur ?

1.6°) Tapez « ipconfig ». Retrouvez l'adresse IP de votre ordinateur ?

1.7°) Tapez « ipconfig /all ». Quelle est la différence avec la commande précédente ?

1.8°) Quel est le nom de votre ordinateur sur le réseau *(Nom de l'hôte)* ?

1.9°) Relevez l'adresse MAC (*adresse physique*) la carte réseau de votre ordinateur.

1.10°) Relevez les paramètres réseaux de votre carte réseau :

1.11°) Retrouvez votre adresse IP internet (http://www.adresseip.com ou http://www.whatismyip.com/, http://monip.org/, http://www.connaitresonip.com/, http://www.monip.com/, ou encore http://www.monip.biz

1.12°) Quelle est votre adresse publique ?

1.12°) Quelle est votre adresse privée ?

Partie 2 : Tests de communication.

L'outil couramment utilisé pour tester la communication entre les machines s'appelle ping. Par exemple, la commande ping 172.1.1.99 permet de vérifier que votre PC communique avec le poste 172.1.1.99.

2.1°) Testez la communication avec le poste de votre voisin (indiquez la commande et le résultat obtenu). La communication est-elle établie ?

Testez la communication avec un ordinateur éteint. La communication est-elle établie ?

2.2°) Testez la communication avec la passerelle (indiquez la commande et le résultat obtenu). La communication est-elle établie ?

2.3°) Testez la communication avec le 127.0.0.1 (indiquez la commande et le résultat obtenu). À quoi correspond cette adresse IP ?
La communication est-elle établie ?

2.4°) Tapez la commande ping –a « IP de votre choix » ? Donnez le nom de l'ordinateur qui a l'adresse 192.168.231.125 :

2.5°) Par défaut, la commande ping envoie 4 requêtes d'échos. Quelle commande doit-on taper pour envoyer 2 requêtes d'échos ?

2.6°) Testez la communication avec le site www.google.fr (indiquez la commande et le résultat obtenu).

Quelle est l'adresse IP internet du site www.google.fr ?

2.7°) Tapez l'adresse 54.38.34.189 dans la barre d'adresse de votre navigateur internet.
A quel site correspond cette adresse ?

2.8°) Ce site est hébergé chez OVH : recherchez whois 54.38.34.189. Observez et Concluez

2.9°) Le nom du site est enregistré au travers de LWS : recherchez whois « nom du site internet ». Observez et concluez

2.10°) Les noms de domaine sont attribués par l'ICANN : proposez une fiche « résumé » de cette société

Partie 3 : Mémorisation des adresses MAC.

Pour communiquer entre elles, les machines utilisent à la fois l'adresse IP et l'adresse MAC de la carte réseau. Chaque ordinateur mémorise la correspondance entre adresse MAC et adresse IP dans ce qu'on appelle le cache ARP. La commande utilisée pour voir son contenu est : arp -a

3.1°) Visualisez le cache arp en tapant arp –a. Quelles informations contient cette table ?

3.2°) Générez du trafic en faisant un ping vers le Pc voisin puis visualisez la table arp.
Que constatez-vous ?

3.3°) Faire un ping vers www.google.fr. Visualisez la table arp. Que constatez-vous ?

3.4°) Peut-on connaître l'adresse MAC d'une machine située hors de notre réseau local ?

Partie 4 : J'ai la VM (Virtual Machine) de Pierre Blazevic. Il a une capacité de 17,3Go.
Calculez sa capacité en Gio en expliquant la différence de notation. Explicitez la différence entre le Go et le Gio. Quelle est la différence entre l'octet et le byte ?

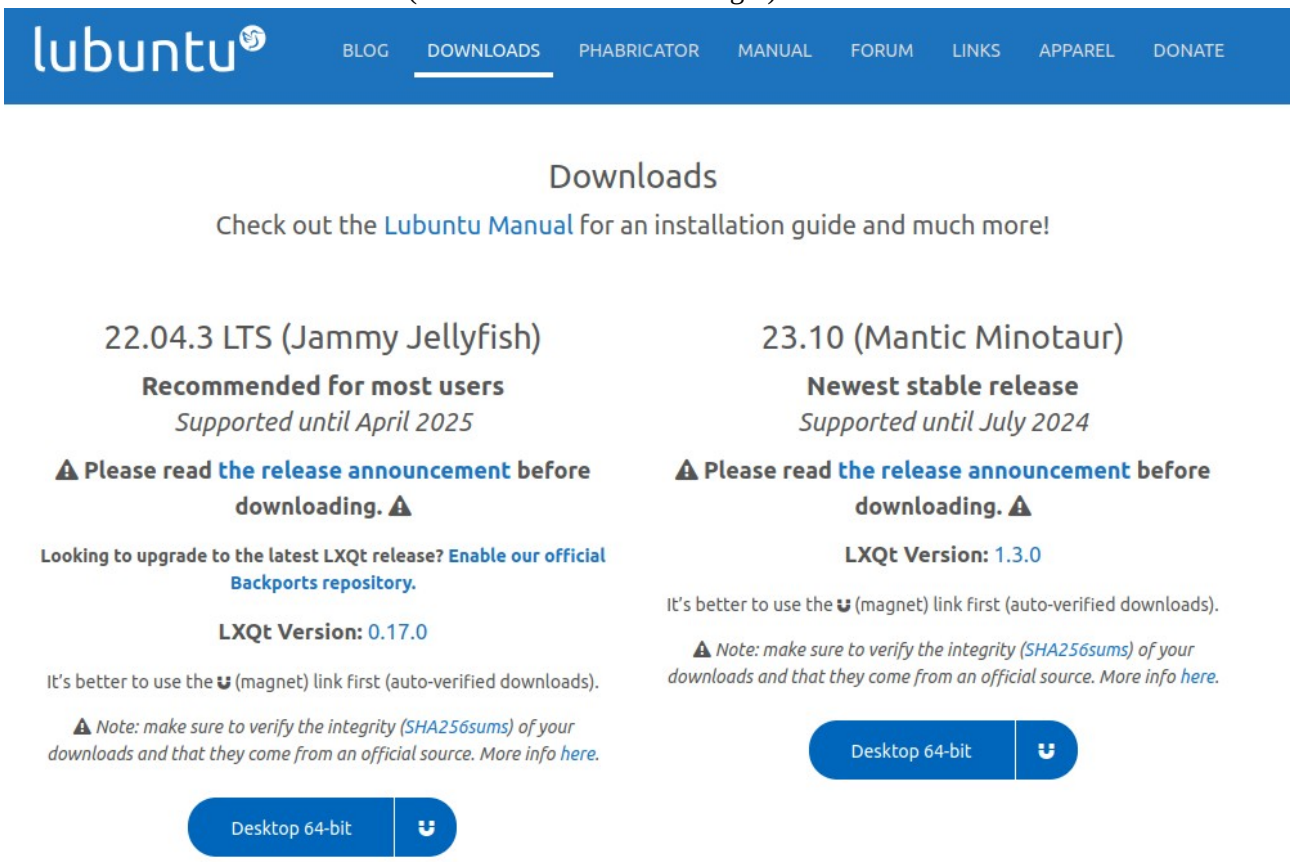
Calculez le temps de transfert que mettra cette VM en fonction de différentes technologies :

- Réseau 100Mbits/s
- Réseau 1000Mbits/s
- Réseau fibré en fibre multi mode Gbits/s

http://cisco.goffinet.org/s1/fibre_optique#.VpF9pVKj9c8
https://fr.wikipedia.org/wiki/Fibre_optique
https://fr.wikipedia.org/wiki/Paire_torsad%C3%A9e
http://www.commentcamarche.net/forum/affich-1185896-quel-est-la-dif-entre-le-cable-stp-et-ftp
http://www.ybet.be/hardware2_ch4/hard2_ch4.php
http://www.commentcamarche.net/contents/1128-transmission-de-donnees-le-cablage
http://hautrive.free.fr/reseaux/supports/cables-paires-torsadees.html

Partie 5 : Installation du VM (Virtual Machine) avec le logiciel VirtualBox.

Vous allez installer l'OS Lubuntu (Ubuntu mais en version Light) :



La version LTS signifie Long-Term Support qui désigne une version de logiciel (ici un OS) dont le support est assuré pour une période de temps plus longue que la normale : ici, 5 ans en théorie mais qui vient d'être diminué à 3 ans
L'édition 22.04.3 signifie qu'elle est sortie en 2022 et au mois de mars
L'édition 23.10 signifie qu'elle est sortie en 2023 et au mois d'octobre

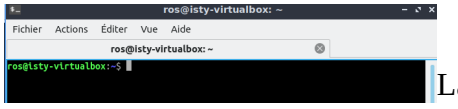
Installez la version 22.04.03 que je vous ai distribué sur la VM. Pour cela, regardez la vidéo ici

Il nous reste à :

1. installer le fichier de add-on
2. paramétrer le réseau correctement pour faire les commandes spécifiques au réseau

I. Le terminal :

Le terminal de commande s'ouvre par : Super () + « terminal » ou CTRL+ALT+T



La fenêtre du terminal est très utile et permet de constater que l'utilisateur se nomme « ros » et que la machine se nomme « isty-virtualbox »
avec CTRL+MAJ+N, on ouvre une nouvelle fenêtre de terminal
avec CTRL+MAJ+T, on ouvre un nouvel onglet dans le même terminal

II. Les utilisateurs et leur pouvoir

- La commande **who** permet de connaître qui est connecté : sur la machine virtuelle Lubuntu, il y a 2 utilisateurs :

```
ros@isty-virtualbox:~$ who
ros      tty1         2022-03-07 11:10 (:0)
ros@isty-virtualbox:~$
```

  l'utilisateur « ros » et l'utilisateur « tty1 » qui est le terminal et ils se sont connectés à 11h10 le 7 mars 2022.
- Le terminal peut-être le terminal natif : CTRL+ALT+F1 pour un terminal natif et CTRL+ALT+F7 pour revenir au GUI (Graphical User Interface) : je ne conseille pas son utilisation car il y a 6 terminaux natifs mais c'est c….t
- Pour ouvrir ou exécuter avec tous les droits (les privilèges du super utilisateur) : sudo….
- Pour lire un fichier : nano est un éditeur de texte très léger : nano toto.txt ou sudo toto.txt si on veut des privilèges supplémentaires (à manipuler avec précautions)
- Le copié/collé est maintenant : SHIFT+CTRL+C et SHIFT+CTRL+V

III. Les commandes de bases

le shell : c'est un langage de programmation (exécute des commandes, fait de la redirection d'entrées / sorties, permet les processus de connexion, permet la création de scripts, permet l'accès aux variables d'environnements)

1. **history :** cette commande permet de lister toutes les commandes déjà effectuées

2. **clear :** permet d'effacer le terminal

3. **la commande « cd » : c**hange **d**irectory : permet de se déplacer dans l'arborescence
   cd /*home*/ros/Téléchargements : ici c'est un chemin absolu
   cd Téléchargements : ici, c'est un chemin relatif (si je suis dans le répertoire ros)
   cd .. : je reviens au répertoire parent (immédiatement au dessus du répertoire actuel
   cd ../.. : je reviens donc au répertoire parent du répertoire parent de notre répertoire actuel
   cd - : je reviens au répertoire précédent (celui que j'ai visité juste avant)
   cd ~ : je vais au répertoire personnel (il y a les répertoires Documents, Téléchargement,...

4. **la commande « ls » : L**ist Files and Directorie**s**
   ls : affiche le contenu du répertoire courant
   ls -a : affiche en + les fichiers cachés
   ls /home : affiche le contenu du répertoire home
   ls -l : affiche sous la forme verticale le contenu du répertoire mais aussi le type de fichier.
   Exemple :
   drwxr-xr-x 2 ros ros 4096 déc. 10 11:08 Téléchargements
   -rwxrwx--- 1 ros ros 3448200 nov. 3 15:08 test_1_2021-07-16-17-30-56.bag
   drwxr-xr-x 2 ros ros 4096 avril 21 2021 Vidéos
   qlq explications ??
   1ère lettre : type de fichier : d, c'est un répertoire et -, c'est un fichier
   rwx : droits en fonction des utilisateurs : r pour read, w pour write et w pour execute
   le 1er ros : utilisateur propriétaire du fichier ou du répertoire
   le 2ème ros : le groupe propriétaire du fichier ou du répertoire

puis, la date de la dernière modification puis le nom du fichier ou du répertoire

ls -la : affiche sous la forme verticale le contenu du répertoire (même les cachés) mais aussi le type de fichier

5. **la commande « rm » : rem**ove (effacer)
   rm : supprime définitivement un fichier
   rmdir : supprime définitivement un répertoire
   rm -r : suppression récursive

6. **la commande «mkdir» : m**a**k**e a **dir**ectory (créer un répertoire)

7. **la commande « mv » : m**o**v**e (déplacer)

8. **la commande « cp » : c**o**p**y (…)
   cp [source][destination] pour un fichier
   cp -r [source][destination] pour un répertoire

9. **la commande «more» :** more est un filtre permettant de se déplacer dans un texte, écran par écran : Cette version est particulièrement primitive.

10. **la commande «less» :** cette commande vous permet de parcourir un fichier texte, affichant un écran plein de texte à chaque fois et on peut se déplacer (molette, page down, page up, espace,)
    less -N …. : on affiche le contenu du fichier avec des numéros de ligne
    less fichier puis /motàrechercher : on affiche le fichier et le mot « motàrechercher » sera en surbrillance

11. **la commande «cat» :** cette commande permet d'afficher mais aussi de concaténer plusieurs fichiers

12. **la commande «find»** : recherche de fichier par son nom, par sa taille ou par son type,….

13. **la commande «grep» :**
    grep motif nomfichier : on recherche le mot « motif » dans le fichier « monfichier »
    cat nomfichier | grep motif : même chose que ci-dessus

14. **la commande « man » :** permet d'avoir un manuel, une aide sur une commande
    exemple : man mkdir

15. **la commande « shutdown » :** une commande que j'utilise fréquemment pour éteindre un serveur à une heure voulue
    shutdown -h 23:07 : le PC / serveur s'éteindra à 23h07
    shutdown +10 : le PC / serveur s'éteindra dans 10 minutes

Exercices sur la partie Linux

a) en vous aidant de la commande « man », redémarrez votre machine dans 1 minute (man shutdown)

b) Créez un fichier dans Documents avec la commande nano

c) Copier/coller ce fichier dans un autre répertoire avec les lignes de commande

d) Écrire un script qui demande à l'utilisateur de saisir son age et qui affiche un message en fonction de son age :

- "jeune pour être en MT4" si l'age est entre 17 et 20
- "beaucoup trop jeune pour être en MT4" lorsqu'il est entre 14 et 16
- "commence à être âgé pour être en MT4 " si l'age est entre 21 et 25
- "beaucoup trop vieux pour être en MT4" si l'age est supérieur à 25

un petit exemple de script :

```
#!/bin/bash

echo "Entrez votre note :"
read note

if [ $note -ge 16 ]
then
    echo "très bien"
elif [ $note -ge 14 ]
then
    echo "bien"
elif [ $note -ge 12 ]
then
    echo "assez bien"
elif [ $note -ge 10 ]
then
    echo "moyen"
else
    echo "insuffisant"
fi
```

Partie 6 : Quelques manipulations

1. Ping : déjà faites
2. ipconfig : déjà faites (ifconfig sous linux)
3. ipconfig /all : déjà faites
4. arp -a : déjà faites

Testez ces commandes et complétez les informations obtenues sous la commande. Observez et concluez

5. getmac : pour obtenir l'adresse MAC rapidement
6. ipconfig /release : relâche l'adresse IP actuelle
7. ipconfig /renew : redemande une adresse IP au serveur DHCP

Quelques commandes internet :

L'utilitaire traceroute

On va prendre pour exemple de tracer la route vers le serveur web de l'université. Pour cela, il y a 3 choix possibles de l'utilitaire traceroute :

- mode UDP : traceroute www.uvsq.fr
- mode ICMP : traceroute I www.uvsq.fr
- mode TCP : traceroute T www.uvsq.fr

1. Rappelez ce qu'est les protocoles UDP, ICMP et TCP. Le protocole HTTP (les pages web) sont basées sur quel protocole ?
2. Testez les 3 modes et qu'observez-vous ? Concluez ?
3. Lorsque vous utilisez l'utilitaire Traceroute, il y existe des options. Expliquez les et testez les :
   traceroute Tn
   traceroute AT

L'utilitaire NMAP :

nmap est un logiciel de balayage des réseaux. L'outil est disponible, sous licence de logiciel libre sur le site http://insecure.org. Cet outil est utilisé par les pirates pour préparer des attaques (attaques par balayage), et par les administrateurs systèmes pour tester la vulnérabilité de leurs systèmes (ex. études d'audit système)

Attention : tout acte de balayage de réseau non-autorisé est assimilé à une attaque et donc répréhensible selon la loi française. Nous nous limitons à faire des balayages des machines dans la salle.

Le principe de map est de solliciter des machines à balayer des réponses montrant l'état des différents ports. Différentes techniques de balayages sont possibles et s'appuient sur l'utilisation des protocoles de base : tcp, udp, ip et icmp. Par défaut, nmap balaye les ports systèmes (numéro de port < 1024). Selon nmap un port d'une machine peut être dans un des états suivants :

- open (ouvert) : port associé à un service actif.
- closed (fermé) : port associé à un service inactif.
- filtered (filtré) : Port inaccessible à cause d'un pare-feu par exemple.
- unfiltered (non filtré) : port accessible mais nmap n'arrive par à déterminer s'il est ouvert ou fermé.

Le balayage d'une machine destination se fait en quatre étapes (qui peuvent être modifiées en utilisant des options appropriées) :

1. Si l'adresse de la machine cible est donnée sous forme symbolique, une résolution DNS est déclenchée (à moins que l'adresse IP de la machine est été donnée dans le fichier local hosts)
2. nmap envoie un paquet ICMP et attends le retour (opération ping). Cette phase peut être évitée en utilisant l'option -P0.
3. Si la destination est spécifiée sous forme d'adresse IP, une phase de résolution inverse DNS est déclenchée. Cette phase peut être évitée en utilisant l'option -n.
4. Le balayage spécifié est exécuté.

La syntaxe générale d'une commande nmap est la suivante :
→ nmap [types de scans] [options] cibles

Spécification de cibles :
Les cibles peuvent être désignées par adresses symboliques ou adresses IP. L'adressage CIDR peut être utilisée afin de désigner des sous-réseaux. Il est aussi possible d'utiliser des intervalles pour designer des pans de réseaux. Par exemple : 192.168.34.1-17 désigne l'intervalle d'adresses [192.168.34.1, 192.168.34, 17]. Des virgules peuvent être employées aussi pour désigner un ensemble de valeurs non-ordonnées. Exemple : 192.168.34.1,2 désigne les deux machines 1 et 2 sur le réseau 192.168.34.0/24.
L'option -p permet de spécifier aussi le numéro de ports à utiliser. Des intervalles et des virgules peuvent aussi être utilisées pour désigner des ensembles de numéro de ports. Des exemples sont :

- nmap -p80,443 localhost
- nmap -p1-1023 192.168.34,1-4

Exercices :

1. Installer si nécessaire, les logiciels nmap, zenmap (un client graphique pour nmap) et wireshark.
2. Comparer et justifier les différences des résultats entre les deux commandes suivantes :
   « nmap @unpc » et « netstat -a » exécutée sur votre machine.
3. Exécuter chacune des commandes suivantes et capturer et justifier le trafic généré pour chaque exécution :
   (a) nmap -p80 scanme.nmap.org
   (b) nmap -p113 scanme.nmap.org
   (c) nmap -p113 -P0 scanme.nmap.org
4. Recommandiez vous l'emploi de l'option -P0 ?
5. Comment faire pour éviter les résolutions DNS ?
6. Sur un PC, donner une commande qui permet de tester l'état de ports web sur une autre machine en générant le minimum de paquets
7. Donner une commande qui permet de retourner les adresses des machines actives sur votre réseau local.
8. Combien de paquets sont générés suite à l'exécution sur votre PC de la commande nmap -P0 -r -sS @unautrePC. Est ce que la balayage des ports se fait dans l'ordre de leurs numéros ?
9. Donner la configuration des paquets générés par les balayages suivants : -sF, -sX. Expliquer le fonctionnement de ces attaques. Quel est l'avantage de ce type de balayage ? (indice : tester sur un port ouvert et un autre fermé)
10. Donner une commande qui permet de donner la liste des machines actives sur le réseau local
11. Peut-on combiner différents type de balayages ?
12. Quel est l'effet de la commande nmap -sV -p80 scanme.nmap.org. Expliquer le fonctionnement après observation du trafic généré.
13. Consulter la page de manuel de la commande nmap et donner la finalité du balayage de type -sO. Tester ce mode de balayage sur le routeur auquel la machine est connectée. Donner les résultats obtenus.
14. Quel type de paquets est généré par un balayage de type -sA. Peut on détecter les ports ouverts avec ce type de balayage ?
15. Comparer les résultats obtenus de l'exécution de ces deux commandes et tenter de justifier une éventuelle différence dans les résultats :
    — sudo nmap -sW -p80 -P0 scanme.nmap.org
    — sudo nmap -sS -p80 -P0 scanme.nmap.org
16. Tester et expliquer le fonctionnement de la commande : nmap -sI @PC2 scanme.nmap.org
17. Que fait la commande nmap -O PC2. Tester aussi avec scanme.nmap.org ?